Cisco Content Services Gateway Installation and Configuration Guide

Release 3.1(3)C6(2)
December 13, 2012

Corporate 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: 408 526-4100

Text Part Number: OL-7283-01

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)

Cisco Content Services Gateway Installation and Configuration Guide

About This Book

This preface describes who should read the *Cisco Content Services Gateway Installation and Configuration Guide*, how it is organized, and its document conventions.

This publication does not contain the instructions to install the Catalyst 6000 series switch or Cisco 7600 series router. For information on installing the switch or router, see the *Installation Guide* that came with your switch or router.

Note For translations of the warnings in this publication, see the "Safety Overview" section on page 17.

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-7283-01	May 16, 2005	Introduced the following features with Cisco IOS 12.2(18)SXE [3.1(3)C6(2)]: • CSG Interface Awareness, page 1-2 • Quota Push, page 1-2 • Tariff Switch, page 1-2 • Prepaid Support for POP3, page 1-3 • Prepaid Support for IMAP, page 1-3 • Transaction Support for IMAP, page 1-3 • Enhanced Interoperability with Cisco Service-Aware GGSN, page 1-5 • CSG RADIUS Proxy Enhancements, page 1-6 • Supplemental Usage Reports, page 1-6 • Quota Balance Replacement, page 1-7 • Delayed Quota Reauthorization, page 1-7 • Configurable Reauthorization Threshold, page 1-7
OL-7283-01	May 16, 2005	Consolidated the descriptions of CDR support into one section: • CDR Support, page 1-10

Revision	Date	Change Summary
OL-7283-01	May 16, 2005	Consolidated the descriptions of Advice of Charge (AoC) features into one section: • Advice of Charge and Related Features, page 1-13
OL-7283-01	May 16, 2005	Consolidated the descriptions of RADIUS features into one section: • RADIUS Features, page 1-17
OL-7283-01	May 16, 2005	Consolidated the descriptions of HTTP features into one section: • HTTP Features, page 1-22
OL-7283-01	May 16, 2005	Consolidated the descriptions of WAP features into one section: • WAP Features, page 1-23
OL-7283-01	May 16, 2005	Added the following new commands to the Command Reference: • **meter imap** • **radius ack error** • **report usage** • **table (module CSG VLAN)**
OL-7283-01	May 16, 2005	Changed the following existing commands in the Command Reference: • **quota server** • **radius endpoint** • **radius proxy** • **retcode** • **show module csg accounting** • **variable (module csg)**

Revision	Date	Change Summary
OL-6028-02	December 15, 2004	Introduced the following features with Cisco IOS 12.2(18)SXD [3.1(3)C5(5)]: • Advice of Charge and Related Features, page 1-13 • HTTP Pipelining and Chunked Transfer Encoding, page 1-22 • URL Rewriting, page 1-15 • Service Verification, page 1-16 • RADIUS Handoff, page 1-21 • Fixed CDR Support for HTTP, page 1-10 • Fixed CDR Support for RTSP, page 1-11 • Single CDR Support for WAP Connectionless and HTTP, page 1-12 • Fixed CDR Support for IMAP, page 1-11 • Prepaid/Envelope Support for SMTP, page 1-12 • SMTP Content Authorization, page 1-16 • POP3 Support, page 1-31 • RADIUS Packet of Disconnect, page 1-21 • RADIUS Endpoint, page 1-20 • RADIUS Proxy, page 1-20 • Service-Level CDR Summarization, page 1-12 • Passthrough Mode and the Default Quota, page 1-32 • Fragment Support, page 1-44 • Connection Duration Billing, page 1-35 • Header Mapping and URL Mapping, page 1-32 (RTSP URL Mapping) • Postpaid Service Tagging, page 1-36 • Stateful Redundancy and Failover, page 1-36 • “Default” Policy, page 1-37 Documentation of these new features includes feature descriptions, configuration tasks, configuration examples, and all associated new and changed commands.
OL-6028-02	December 15, 2004	Moved prepaid configuration tasks into a separate chapter: • Configuring Prepaid Support, page 6-1
OL-6028-02	December 15, 2004	Documented protocol compliance statements in a new appendix: • Protocol Compliance Statements for the CSG 3.1(3)C6(2), page D-1

Revision	Date	Change Summary
OL-6028-02	December 15, 2004	Added the following new commands to the Command Reference: • **activation** • **ip csg snmp timer** • **next-hop** • **passthrough** • **pending** • **radius endpoint** • **radius handoff** • **radius pod attribute** • **radius pod nas** • **radius pod timeout** • **records granularity** • **verify** • **verify confirmation**
OL-6028-02	December 15, 2004	Changed the following existing commands in the Command Reference: • **accounting (CSG policy)** • **aoc confirmation** • **basis** • **client (CSG content)** • **debug ip csg** • **flags** • **match (header map)** • **match (URL map)** • **mode** • **radius proxy** • **records format** • **show module csg tech-support** • **show module csg variable** • **variable (module csg)**

Audience

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

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 (CSG).
Chapter 2, "Installing the Hardware"	Describes how to install the CSG.
Chapter 3, "Configuring the Content Services Gateway"	Describes how to configure VLANs, virtual servers, billing, and other configuration tasks on the CSG.
Chapter 4, "Configuring Secure (Router) Mode, Redundancy, Fault Tolerance, and HSRP"	Describes how to configure secure router mode, redundancy, fault tolerance, and Hot Standby Router Protocol (HSRP) on the CSG.
Chapter 5, "Configuring RADIUS Support: Learning Who the Subscriber Is"	Describes RADIUS configuration details and features.
Chapter 6, "Configuring Prepaid Support"	Describes prepaid configuration details and features.
Appendix A, "PSD Configuration for the CSG"	Describes how to configure the CSG to communicate with the PSD.
Appendix B, "Command Reference"	Describes the commands that allow you to set up and monitor content billing on the CSG.
Appendix C, "Standards Compliance Specifications"	Lists the standards with which Catalyst 6000 series switches or Cisco 7600 series routers comply, when installed in a system.
Appendix D, "Protocol Compliance Statements for the CSG 3.1(3)C6(2)"	Provides protocol compliance statements for the CSG 3.1(3)C6(2).
Appendix E, "Translated Safety Warnings"	Provides translated safety warnings for the CSG.

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.
{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 the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.

Convention	Description
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.

Safety Overview

Safety warnings appear throughout this publication in procedures that, if performed incorrectly, might harm you. A warning symbol precedes each warning statement.

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Waarschuwing **BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van de standaard praktijken om ongelukken te voorkomen. Gebruik het nummer van de verklaring onderaan de waarschuwing als u een vertaling van de waarschuwing die bij het apparaat wordt geleverd, wilt raadplegen.

BEWAAR DEZE INSTRUCTIES

Varoitus **TÄRKEITÄ TURVALLISUUSOHJEITA**

Tämä varoitusmerkki merkitsee vaaraa. Tilanne voi aiheuttaa ruumiillisia vammoja. Ennen kuin käsittelet laitteistoa, huomioi sähköpiirien käsittelemiseen liittyvät riskit ja tutustu onnettomuuksien yleisiin ehkäisytapoihin. Turvallisuusvaroitusten käännökset löytyvät laitteen mukana toimitettujen käännettyjen turvallisuusvaroitusten joukosta varoitusten lopussa näkyvien lausuntonumeroiden avulla.

SÄILYTÄ NÄMÄ OHJEET

Attention **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement.

CONSERVEZ CES INFORMATIONS

Warnung **WICHTIGE SICHERHEITSHINWEISE**

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung vor Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.

BEWAHREN SIE DIESE HINWEISE GUT AUF.

Avvertenza **IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero di istruzione presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze riportate in questo documento.

CONSERVARE QUESTE ISTRUZIONI

Advarsel **VIKTIGE SIKKERHETSINSTRUKSJONER**

Dette advarselssymbolet betyr fare. Du er i en situasjon som kan føre til skade på person. Før du begynner å arbeide med noe av utstyret, må du være oppmerksom på farene forbundet med elektriske kretser, og kjenne til standardprosedyrer for å forhindre ulykker. Bruk nummeret i slutten av hver advarsel for å finne oversettelsen i de oversatte sikkerhetsadvarslene som fulgte med denne enheten.

TA VARE PÅ DISSE INSTRUKSJONENE

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você está em uma situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha conhecimento dos perigos envolvidos no manuseio de circuitos elétricos e familiarize-se com as práticas habituais de prevenção de acidentes. Utilize o número da instrução fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham este dispositivo.

GUARDE ESTAS INSTRUÇÕES

¡Advertencia! **INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Al final de cada advertencia encontrará el número que le ayudará a encontrar el texto traducido en el apartado de traducciones que acompaña a este dispositivo.

GUARDE ESTAS INSTRUCCIONES

Varning! **VIKTIGA SÄKERHETSANVISNINGAR**

Denna varningssignal signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanliga förfaranden för att förebygga olyckor. Använd det nummer som finns i slutet av varje varning för att hitta dess översättning i de översatta säkerhetsvarningar som medföljer denna anordning.

SPARA DESSA ANVISNINGAR

Figyelem **FONTOS BIZTONSÁGI ELOÍRÁSOK**

Ez a figyelmezeto jel veszélyre utal. Sérülésveszélyt rejto helyzetben van. Mielott bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplo figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján keresheto meg.

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Предупреждение **ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ**

Этот символ предупреждения обозначает опасность. То есть имеет место ситуация, в которой следует опасаться телесных повреждений. Перед эксплуатацией оборудования выясните, каким опасностям может подвергаться пользователь при использовании электрических цепей, и ознакомьтесь с правилами техники безопасности для предотвращения возможных несчастных случаев. Воспользуйтесь номером заявления, приведенным в конце каждого предупреждения, чтобы найти его переведенный вариант в переводе предупреждений по безопасности, прилагаемом к данному устройству.

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告 重要的安全性说明

此警告符号代表危险。您正处于可能受到严重伤害的工作环境中。在您使用设备开始工作之前，必须充分意识到触电的危险，并熟练掌握防止事故发生的标准工作程序。请根据每项警告结尾提供的声明号码来找到此设备的安全性警告说明的翻译文本。

请保存这些安全性说明

警告 安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。警告の各国語版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。

これらの注意事項を保管しておいてください。

주의 중요 안전 지침

이 경고 기호는 위험을 나타냅니다. 작업자가 신체 부상을 일으킬 수 있는 위험한 환경에 있습니다. 장비에 작업을 수행하기 전에 전기 회로와 관련된 위험을 숙지하고 표준 작업 관례를 숙지하여 사고를 방지하십시오. 각 경고의 마지막 부분에 있는 경고문 번호를 참조하여 이 장치와 함께 제공되는 번역된 안전 경고문에서 해당 번역문을 찾으십시오.

이 지시 사항을 보관하십시오.

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você se encontra em uma situação em que há risco de lesões corporais. Antes de trabalhar com qualquer equipamento, esteja ciente dos riscos que envolvem os circuitos elétricos e familiarize-se com as práticas padrão de prevenção de acidentes. Use o número da declaração fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham o dispositivo.

GUARDE ESTAS INSTRUÇÕES

Advarsel **VIGTIGE SIKKERHEDSANVISNINGER**

Dette advarselssymbol betyder fare. Du befinder dig i en situation med risiko for legemesbeskadigelse. Før du begynder arbejde på udstyr, skal du være opmærksom på de involverede risici, der er ved elektriske kredsløb, og du skal sætte dig ind i standardprocedurer til undgåelse af ulykker. Brug erklæringsnummeret efter hver advarsel for at finde oversættelsen i de oversatte advarsler, der fulgte med denne enhed.

GEM DISSE ANVISNINGER

تحذير **إرشادات الأمان الهامة**

يوضح رمز التحذير هذا وجود خطر. وهذا يعني أنك متواجد في مكان قد ينتج عنه التعرض لإصابات. قبل بدء العمل، احذر مخاطر التعرض للصدمات الكهربائية وكن على علم بالإجراءات القياسية للحيلولة دون وقوع أي حوادث. استخدم رقم البيان الموجود في أخر كل تحذير لتحديد مكان ترجمته داخل تحذيرات الأمان المترجمة التي تأتي مع الجهاز.
قم بحفظ هذه الإرشادات

Upozorenje **VAŽNE SIGURNOSNE NAPOMENE**

Ovaj simbol upozorenja predstavlja opasnost. Nalazite se u situaciji koja može prouzročiti tjelesne ozljede. Prije rada s bilo kojim uređajem, morate razumjeti opasnosti vezane uz električne sklopove, te biti upoznati sa standardnim načinima izbjegavanja nesreća. U prevedenim sigurnosnim upozorenjima, priloženima uz uređaj, možete prema broju koji se nalazi uz pojedino upozorenje pronaći i njegov prijevod.

SAČUVAJTE OVE UPUTE

Upozornění

DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY

Tento upozorňující symbol označuje nebezpečí. Jste v situaci, která by mohla způsobit nebezpečí úrazu. Před prací na jakémkoliv vybavení si uvědomte nebezpečí související s elektrickými obvody a seznamte se se standardními opatřeními pro předcházení úrazům. Podle čísla na konci každého upozornění vyhledejte jeho překlad v přeložených bezpečnostních upozorněních, která jsou přiložena k zařízení.

USCHOVEJTE TYTO POKYNY

Προειδοποίηση

ΣΗΜΑΝΤΙΚΕΣ ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

Αυτό το προειδοποιητικό σύμβολο σημαίνει κίνδυνο. Βρίσκεστε σε κατάσταση που μπορεί να προκαλέσει τραυματισμό. Πριν εργαστείτε σε οποιοδήποτε εξοπλισμό, να έχετε υπόψη σας τους κινδύνους που σχετίζονται με τα ηλεκτρικά κυκλώματα και να έχετε εξοικειωθεί με τις συνήθεις πρακτικές για την αποφυγή ατυχημάτων. Χρησιμοποιήστε τον αριθμό δήλωσης που παρέχεται στο τέλος κάθε προειδοποίησης, για να εντοπίσετε τη μετάφρασή της στις μεταφρασμένες προειδοποιήσεις ασφαλείας που συνοδεύουν τη συσκευή.

ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ

אזהרה

הוראות בטיחות חשובות

סימן אזהרה זה מסמל סכנה. אתה נמצא במצב העלול לגרום לפציעה. לפני שתעבוד עם ציוד כלשהו, עליך להיות מודע לסכנות הכרוכות במעגלים חשמליים ולהכיר את הנהלים המקובלים למניעת תאונות. השתמש במספר ההוראה המסופק בסופה של כל אזהרה כד לאתר את התרגום באזהרות הבטיחות המתורגמות שמצורפות להתקן.

שמור הוראות אלה

Opomena

ВАЖНИ БЕЗБЕДНОСНИ НАПАТСТВИЈА
Симболот за предупредување значи опасност. Се наоѓате во ситуација што може да предизвика телесни повреди. Пред да работите со опремата, бидете свесни за ризикот што постои кај електричните кола и треба да ги познавате стандардните постапки за спречување на несреќни случаи. Искористете го бројот на изјавата што се наоѓа на крајот на секое предупредување за да го најдете неговиот период во преведените безбедносни предупредувања што се испорачани со уредот.
ЧУВАЈТЕ ГИ ОВИЕ НАПАТСТВИЈА

Ostrzeżenie **WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA**

Ten symbol ostrzeżenia oznacza niebezpieczeństwo. Zachodzi sytuacja, która może powodować obrażenia ciała. Przed przystąpieniem do prac przy urządzeniach należy zapoznać się z zagrożeniami związanymi z układami elektrycznymi oraz ze standardowymi środkami zapobiegania wypadkom. Na końcu każdego ostrzeżenia podano numer, na podstawie którego można odszukać tłumaczenie tego ostrzeżenia w dołączonym do urządzenia dokumencie z tłumaczeniami ostrzeżeń.

NINIEJSZE INSTRUKCJE NALEŻY ZACHOWAĆ

Upozornenie **DÔLEŽITÉ BEZPEČNOSTNÉ POKYNY**

Tento varovný symbol označuje nebezpečenstvo. Nachádzate sa v situácii s nebezpečenstvom úrazu. Pred prácou na akomkoľvek vybavení si uvedomte nebezpečenstvo súvisiace s elektrickými obvodmi a oboznámte sa so štandardnými opatreniami na predchádzanie úrazom. Podľa čísla na konci každého upozornenia vyhľadajte jeho preklad v preložených bezpečnostných upozorneniach, ktoré sú priložené k zariadeniu.

USCHOVAJTE SI TENTO NÁVOD

Related Documentation

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

- *Site Preparation and Safety Guide*
- *Regulatory Compliance and Safety Information for the Catalyst 6500 Series Switches*
- *Catalyst 6500 Series Switch Installation Guide*
- *Catalyst 6500 Series Quick Software Configuration*
- *Catalyst 6500 Series Switch Module Installation Guide*
- *Catalyst 6500 Series Software Configuration Guide*
- *Catalyst 6500 Series Command Reference*
- *Catalyst 6000 Family IOS Software Configuration Guide*
- *Catalyst 6500 Series Cisco IOS Command Reference*
- *Catalyst 6000 Family Flash Card Install Note*
- *ATM Configuration and Command Reference—Cisco Catalyst 6500 Series Switches*
- *System Message Guide - Catalyst Family Switches—Cisco Catalyst 6500 Series Switches*
- *Regulatory Compliance and Safety Information for the Cisco 7600 Series Routers*
- *Cisco 7609 Router Installation Guide*
- *Cisco 7600 Series Cisco IOS Software Configuration Guide*
- *Cisco 7600 Series Cisco IOS Command Reference*

- For information about MIBs, see:

  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml
- *Release Notes for Cisco Content Services Gateway*, Release 3.1(3)C6(2)
- Cisco IOS Configuration Guides and Command References, Release 12.1—Use these publications to help you configure the Cisco IOS software that runs on the MSFC and on the MSM and ATM modules.

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.

Overview

The Cisco Content Services Gateway (CSG) is a high-speed processing module that brings content billing and user awareness to the Cisco Catalyst 6500 series switch or Cisco 7600 series router platforms. The CSG is typically located at the edge of a network in an Internet service provider (ISP) Point of Presence (POP), or Regional Data Center.

The CSG offers more than standard IP flow accounting; the CSG also examines various protocol requests (Wireless Application Protocol [WAP], Mail, FTP, RTSP, and HTTP) to gather URLs and other header information for accounting purposes. Additionally, the CSG gathers information on usernames and usage statistics, and enables differentiated billing for individual transactions based on hostname, on the directory accessed, or on individual files.

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

This section includes the following information:

What's New

The CSG 3.1(3)C6(2) includes the following new features:

Additional features are described in the "Features from Previous Releases" section on page 1-8.

CSG Interface Awareness

Many provider networks offer data access, control over user addressing, and dedicated Virtual Routing and Forwarding (VRF) over the wireless network to enterprises and Mobile Virtual Network Operators (MVNOs). Interface awareness enables the CSG to distinguish between users and sessions that share the same IP address on different VLANs (that is, users and sessions with overlapping IP addresses).

The CSG binds contents to specific VLANs, and configures those VLANs with a table ID. When user packets match a content and a session is created, the CSG uses the table ID of the content as part of the user search. When a table is configured on a VLAN, the contents that are bound to each VLAN are associated with the table ID of that VLAN.

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

To associate a table name with a VLAN, use the **table** command in module CSG VLAN configuration mode.

To associate a table name with a particular RADIUS proxy or endpoint, use the **radius proxy** and **radius endpoint** commands in module CSG configuration mode.

Quota Push

This feature enables operators to "push" quota for a user or service to the CSG. This enables quota servers to provide quota for a user or service before traffic from that user or service reaches the CSG. 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 CSG accepts a quota push for a user at any point after the user and billing plan are known to the CSG (that is, when a User Table element exists for the user). For example, the CSG accepts a quota push after receiving an accounting start but does not require an existing service for the user (one is created). The CSG 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.

There are no commands required to enable quota push.

Tariff Switch

Tariff switch is a prepaid feature in which the CSG 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 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 CSG 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. The CSG 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 should choose the timeout carefully to avoid causing a flood of Quota Return messages at a given time. At any given time, the CSG 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.

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 CSG sends intermediate records to the BMA for transactions that span a tariff switch time and do not terminate quickly.

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

Prepaid Support for POP3

The CSG supports prepaid billing for POP3. For **basis fixed** prepaid billing, the CSG treats each e-mail download as a transaction and a prepaid debit subject to weighting.

The CSG 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 CSG to provide refunding for POP3, specify return code **554** on the **retcode** command in CSG refund configuration mode for the POP3 refund definition.

Prepaid Support for IMAP

The CSG supports prepaid billing for IMAP.

There are no commands required to enable prepaid support for IMAP.

Transaction Support for IMAP

The CSG provides transaction support for IMAP. The CSG 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 CSG includes IMAP transaction counts in the Completed Transactions TLV. The CSG 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 CSG accumulates the bytes and includes them in the next transaction. When the IMAP session ends, the CSG reports any remaining bytes.

Consider the following simple example of an IMAP transaction with BODY:

Client request: 1 FETCH 5 BODY[]

Server response: * 5 FETCH (BODY[]{55}cr-lf-55-bytes-of-e-mail-followed-by-cr-lf)cr-lf

1 OK FETCH COMPLETE

The CSG handles this request and response as follows:

Step 1 The client request is tagged **1**. The CSG parses the request and increments the body up byte counts, because the request was for a **BODY[]**.

Step 2 The CSG parses the untagged response from the server and notes that it contains TEXT (**BODY[]**).

Step 3 The CSG 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:

Client request: 8 FETCH 1:100 BODY[]<0.5>

Server 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 CSG handles this request and response as follows:

Step 1 The client request is tagged **8**. The CSG parses the request and increments the body up byte counts, because the request was for a **BODY[]**.

Step 2 The server sends 100 untagged responses which the CSG parses, noting that the response contains TEXT (**BODY[]**).

Step 3 The CSG 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 CSG 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.

To specify which IMAP bytes are billed for when doing prepaid debits (BODY only, BODY and HEADER only, or BODY and OTHER only), use the **meter imap** command in CSG service configuration mode.

Because IMAP metering is byte-based, you cannot configure both **meter imap** and **basis fixed** or **basis second** in the same service. Only **basis byte** is meaningful with **meter imap**.

If you specify **basis fixed**, each IMAP transaction counts as a quadran, subject to weights.

To specify that the CSG is to refund quota for IMAP quota for application return codes, use the **retcode** command in CSG refund configuration mode.

Note Any IMAP transaction that is not an OK tagged response (such as **1 OK FETCH COMPLETE**) is subject to a prepaid refund.

Enhanced Interoperability with Cisco Service-Aware GGSN

The CSG can couple with a Cisco GGSN to form a service-aware GGSN. When operating in this mode, the CSG 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.

CSG RADIUS Proxy Enhancements

The CSG RADIUS interface recognizes the following Cisco-specific VSAs:

- Sub-attribute 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 sub-attribute in order for the CSG to act on this VSA. If the quota server is not configured, the CSG 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.
- Sub-attribute 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 CSG.

For RADIUS endpoint and RADIUS proxy configurations, you can prevent the CSG from acknowledging the following errors by entering the **no** form of the **radius ack error** command in CSG user group configuration mode:

1. The User Table entry cannot be created due to resource constraints.
2. The CSG parses the Accounting Request and encounters RADIUS protocol errors.
3. The CSG parses the Accounting Request and a billing plan is specified in the Accounting Request, but it does not match a billing plan in the CSG configuration.
4. The CSG parses the Accounting Request and a quota server is specified in the Accounting Request, but it does not match a quota server in the CSG configuration.
5. The CSG parses the Accounting Request and a connect service is specified in the Accounting Request, but it does not match a connect service in the CSG configuration.

   For errors 3, 4, and 5, the CSG can parse the configuration VSA from the Access-Accept. If the CSG uses any attribute from the Access-Accept that does not match the CSG configuration, the CSG does not send a RADIUS response to the Accounting Request.

For RADIUS accounting requests processed as a result of matching a **radius endpoint** command, the CSG does not send a RADIUS acknowledgement.

For RADIUS accounting requests processed as a result of matching a **radius proxy** command, the CSG does not forward the Accounting Request to the RADIUS server.

Supplemental Usage Reports

You can configure the CSG 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. The data is incremental from the last report.

If a tariff switch timeout occurs during the interval, the CSG 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, use the **report usage** command in CSG accounting configuration mode.

Quota Balance Replacement

By default, when the CSG receives a quota grant from the quota server, the CSG adds the granted quota to the current balance for a subscriber's service. Quota balance replacement enables the quota server to instruct the CSG to replace the current quota balance with the amount of granted quota for a subscriber's service. Note that if the replacement grant is provided in a Service Authorization Response, the CSG 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.

Delayed Quota Reauthorization

The CSG accepts the Reauthorization Delay TLV, which specifies the number of seconds the CSG delays its next reauthorization request to the quota server for the service specified in the message. This TLV also specifies the action the CSG is to take for the service between the time the message is received and the next reauthorization:

- Wait—The CSG keeps transactions in a pending state during the delay period. In pending state, the CSG maintains the transaction state but drops packets.
- Deny—The CSG drops new transactions during the delay period. Existing transactions are dropped if quota expires during the delay period. The CSG does not maintain the session state; the user 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 CSG 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.

Configurable Reauthorization Threshold

You can configure the thresholds of available quota that trigger service reauthorization by specifying the following CSG variables on the **variable** command in module CSG configuration mode:

- CSG_BASIS_BYTE_LOW_QUOTA_MAX
- CSG_BASIS_FIXED_LOW_QUOTA_MAX
- CSG_BASIS_SEC_LOW_QUOTA

You can configure the thresholds for volume-, time-, and transaction-based billing, and the CSG can also accept a threshold specified by the quota server in a quota grant to the CSG.

Enhanced Quota Reconciliation

During internal quota reconciliation, the CSG might drop packets for some prepaid users, which can affect user throughput.

To prevent this problem, set the CSG_QUOTA_BLOCK environment variable to 0, using the **variable** command in module CSG configuration mode. Setting this variable to 0 enables the CSG to forward packets for a prepaid user during quota reconciliation, regardless of whether quota is available for the user. When quota reconciliation is complete, if the CSG determines that the user has no quota available, the CSG terminates the connection.

The CSG supports enhanced quota reconciliation for all accounting types.

If you want the CSG to continue to drop packets that arrive during quota reconciliation, set the CSG_QUOTA_BLOCK to 1. This is the default setting.

Features from Previous Releases

In addition to new features introduced in this release, the CSG provides the following features and functionality that were introduced prior to the CSG 3.1(3)C6(2):

CDR Support

The CSG provides the following Call Detail Record (CDR) support:

Fixed CDR Support for HTTP

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

The single CDR contains all fields 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 **report radius attribute** command in CSG accounting configuration mode. This is a change from the CSG 3.1(3)C5(1), in which you hard-coded up to 10 specific RADIUS attributes which were included in the CDR in a predefined order. This scheme is very flexible, enabling you to add RADIUS attributes as you go. This change in the handling of RADIUS TLVs applies to both WAP and HTTP fixed CDRs.

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 in itself variable. Therefore, a predefined “fixed” list of attributes cannot be determined when RADIUS attribute 26 is configured.

To enable the fixed format feature for HTTP and for WAP, use the **records format fixed** command in CSG accounting configuration mode.

The CSG 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 CSG now supports postpaid billing for the Internet Message Access Protocol (IMAP), in addition to postpaid billing for Post Office Protocol, version 3 (POP3) and Simple Mail Transfer Protocol (SMTP). This feature enables the CSG to report service-level fixed format CDRs for IMAP. The service-level CDR includes the following IMAP-specific counts:

- Number of header retrievals. That is, the number of times the CSG 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 the CSG 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 CSG 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 CSG generates intermediate CDRs every 15 minutes, then the CSG reports the delta of the total byte count from the point in which the last CDR was reported to the point at which the current CDR is reported. So, the first CDR would report 100 KB and the second would report 50 KB.

With fixed format CDRs, they 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.)

To enable the CSG to support IMAP, use the **records format fixed** command in CSG accounting configuration mode, and the **accounting type imap** command in CSG policy configuration mode.

When configuring CSG support for IMAP, keep in mind the following considerations:

- The CSG supports only postpaid billing for IMAP. IMAP transactions for a prepaid user are treated as postpaid.
- The CSG does not support AoC for IMAP. If AoC is configured for an IMAP user, AoC is ignored for that user.
- The CSG cannot examine IMAP flows sent over an encrypted tunnel, such as Secure Socket Layer (SSL) or Transport Layer Security (TLS). Therefore, when an encrypted tunnel is used for IMAP traffic, the CSG records only IP and TCP upstream and downstream byte counts. No other counts are provided.

Fixed CDR Support for RTSP

This feature enables the CSG 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.

To enable the fixed format feature for RTSP, use the **records format fixed** command in CSG accounting configuration mode.

Single CDR Support for WAP Connectionless and HTTP

The CSG already reduces the multiple CDRs generated for WAP connection-oriented traffic down to a single CDR, which is reported at the end of the transaction. This feature is extended to WAP connectionless traffic and 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.

To enable single CDR support for WAP connection-oriented, WAP connectionless, and HTTP traffic, use the **variable-single-cdr** keyword on the **records format** command in CSG accounting configuration mode.

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

Service-Level CDR Summarization

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

For example, if a user is accessing the open Internet service, and the data is billed solely on the basis of volume, generating records for each HTTP transaction is of little use. With service-level CDR summarization enabled, the CSG generates only consolidated records containing service-level usage. Information from individual events is no reported (for example, no URLs).

The CSG supports the following protocols in both fixed and variable format: IP, HTTP, SMTP, POP3, and IMAP. (POP3 and IMAP are supported in postpaid mode only.)

Service-level CDRs are generated only for subscribers with entries in the CSG User Table entry. If a subscriber does not have an entry in the User Table, the CSG generates transaction-level CDRs.

To enable service-level CDR summarization, use the **records granularity** command in CSG service configuration mode.

Note If you specify both **type http** and any other type (**type other**, **type ftp**, **type imap**, and so on) for a service, and you enable service-level CDR summarization for the service, the CSG's incremental and cumulative byte counts are not valid. This is because they are a mix of TCP bytes (for the HTTP traffic) and IP bytes (for all other traffic).

Prepaid/Envelope Support for SMTP

The CSG provides SMTP postpaid and prepaid support, including the addition of 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 mail envelope information as well as IP byte counts, TCP byte counts, and mail data (X-CSG-SIZE) byte counts for each mail message. When multiple e-mails are sent over a single TCP connection, each mail message is assigned byte counts until the start of the next mail message. The last mail is assigned bytes from the start of that 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 mail message. If the CSG 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 mail not being sent). If the CSG receives a QUIT before receiving any return code, it reports a default return code of **554** (Transaction failed). This enables the CSG to apply refunding via the SMTP return code value.

If the user 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 mail was received, and the authentication failure bit is set in the TCP **flags** field.

The CSG no longer uses the TCP Stats CDR, which was generated at the end of the TCP connection, because the information in the TCP Stats CDR duplicates the information in the SMTP CDR.

Fixed Attribute CDRs for WAP

In support of some legacy billing systems, the CSG provides a fixed attribute format for WAP CDRs. The same set of attributes are reported in each CDR regardless of 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.

Advice of Charge and Related Features

Advice of Charge (AoC) is a function that enables a service provider to provide messaging and authorization prompts to its subscribers. The CSG'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 CSG to block client requests and redirect them to the notification server when the client must make a decision to pay for the service. It is also responsible for telling the CSG to allow the client request to flow when the client has agreed to pay.
- The notification server is responsible for communicating fees to the client and providing the option to pay. The client's payment decision must be communicated from the notification server to the quota server.

The CSG's role in the AoC process is to redirect user data requests to the notification server. The CSG provides two modes for redirecting to the notification server. The choice of mode, and the requirements that mode imposes on the notification server, varies by protocol. The two modes supported by the CSG are:

- URL-redirect—Supported for HTTP and WAP/WSP
- NAT-redirect—Supported for all other protocols

A complete AoC implementation depends heavily on the notification server. With URL-redirect, the notification server can be a standard Web server, because the CSG does the redirection at the protocol level. This is the easiest deployment to implement. With NAT-redirect, the CSG just forwards the connection directly to the notification server. The notification server must therefore be able to accept the packets, interpret the protocol, drive an AoC on its own, and properly manage the rest of that user's flow for that connection.

The CSG 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 CSG's service verification function, the latter using the CSG'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 CSG 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 CSG's role in the process. However, the CSG does provide some additional assists for URL-redirects that greatly ease the burden on the backend systems. For example, the CSG 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 user HTTP request when redirecting the subscriber to the final requested content. The CSG 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 CSG strips the token from the request so that the content server is not confused by the extra data.

You can instruct the CSG to get authorization from the quota server for each subscriber request for content.

The CSG's support for AoC has the following restrictions:

- The CSG supports AoC via content authorization and URL-redirect for only HTTP and WAP/WSP.
- The CSG does not support AoC for IMAP. If AoC is configured for an IMAP user, AoC is ignored for that user.
- The CSG does not support AoC for Connection Duration services.
- When performing AoC for a TCP connection carrying pipelined HTTP requests, the CSG 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.

To enable the CSG's support for AoC, use the **authorize content** command in CSG service configuration mode.

The CSG provides the following AoC-related features:

- URL Redirect, page 1-14
- URL Rewriting, page 1-15
- WAP URL Appending, page 1-15
- SMTP Content Authorization, page 1-16
- Redirect Flexibility, page 1-16
- Service Verification, page 1-16

URL Redirect

In a redirect scenario, the CSG responds to the HTTP or WAP client with response code and a URL to which the client should redirect. You can configure the redirect URL using the **redirect** command in CSG user group configuration mode, or the quota server can provide the redirect URL during service authorization (or reauthorization) or content authorization processing.

In the case of 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 a single redirect URL for both WAP and HTTP. 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 returned from the quota server in a service authorization response, or in a content authorization response with the REDIRECT_URL action code, takes precedence over a redirect URL that is configured using the **redirect** command. The CSG uses the **redirect**-specified URL when the quota server responds with the FORWARD action code.

To control the amount of time and the number of redirects that the CSG allows, specify the following environment variables using the **variable** command in module CSG configuration mode:

- CSG_REDIRECTS_INTERVAL—Defines the length of time for which the CSG should redirect.
- CSG_REDIRECTS_MAX—Defines the number of requests that are redirected before the CSG stops redirecting, but within the interval time.

The CSG starts the interval timer when the first request is redirected after it has received no quota. This counter is reset, and the timer is stopped after another quota grant of zero is given.

For example, if CSG_REDIRECTS_MAX is set to 15 and CSG_REDIRECTS_INTERVAL is set to 8 seconds, and you receive a Service Auth Response with zero quadrans, and you have redirect information, then redirection occurs when you run out of quota (assuming you have not received quota since). The CSG_REDIRECTS_INTERVAL 8-second timer starts after your first redirect. Therefore, request 1 is redirected, and up to 14 more requests can be redirected, if they occur within the 8 seconds after the first redirect.

URL Rewriting

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 client request. The notification server appends a string beginning with a token to the originally requested URL and sends it to the client as part of a redirect reply after the client has agreed to pay. The CSG 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 client has agreed to pay for the request. It responds to the CSG with a FORWARD action code in the content authorization response. The CSG detects the token, creates a new GET request containing the original URL with the token and any characters following it removed, and sends the GET on behalf of the client. The token must be known by the CSG, the quota server, and the notification server. It is administratively defined on the CSG using the CLI. The token should be chosen carefully to ensure that it is only present in URLs rewritten by the notification server and not in other client requests.

The CSG supports URL rewriting for HTTP, WAP 1.x, and WAP 2.x.

To define a URL-rewriting token for CSG, use one of the following commands in CSG user group configuration mode:

- **aoc confirmation**
- **verify confirmation**

WAP URL Appending

Whenever a content authorization response contains a REDIRECT_URL action code for a WAP content authorization request, the CSG can optionally append the originally requested URL to the one returned by the quota server.

For example, if the client originally requested the following URL:

http://www.yahoo.com/home.wml

and the quota server returns the following URL in a REDIRECT_URL content authorization response:

http://www.yahoo.com/charges.wml

then the CSG would send the following URL as part of a redirect message to the client:

http://www.yahoo.com/charges.wml?www.yahoo.com/home.wml

The default behavior is to pass the redirect URL to the client as specified by the quota server without modification.

To enable WAP URL appending, set the CSG_WAP_APPEND_AOC_URL environment variable using the **variable** command in module CSG configuration mode.

SMTP Content Authorization

The CSG handles content authorization for SMTP in a slightly different manner than for other protocols.

Typically, the CSG sends the content authorization request immediately after performing service authorization. The CSG can do this because all of the information in the content authorization request is contained in the initial flow received by the CSG.

However, for SMTP, the information needed in the content authorization request—number of recipients with a good return code, number of recipients with a bad return code, size of mail in bytes (if present) and the sender of the e-mail—are not known until after the CSG processes the SMTP envelope. Therefore, when content authorization is configured, the CSG allows all envelope information to flow through, even if the user has no quota (however, access is not permitted if the user is not authorized). The CSG initiates the content authorization request when it receives the DATA command. The CSG queues the packet containing the DATA command until content authorization processing is resolved.

If the CSG receives a DROP or REDIRECT in the content authorization response, it drops the DATA command packet, terminates the session, and generates a CDR containing the envelope information and an invalid application return code.

If the CSG receives a FORWARD, it uses the weight that is returned in the response for prepaid processing.

Multiple e-mails over the same TCP connection result in multiple content authorization requests. Each mail is treated as a separate transaction.

To enable content authorization for SMTP, use the **authorize content** command in CSG service configuration mode.

Redirect Flexibility

A quota server can request a redirect for multiple reasons (for example, top-up, “sorry” indication, login request, and so on). The CSG allows the quota server to return the IP address and port number for each redirect. Thus, a different port number, or even a different server, can be used for every reason that the quota server might request the redirect. The CSG stores the most recent redirect address and port number for each service under each user, and uses that address and port instead of the globally defined default.

Service Verification

Service verification is a capability like AoC, provided the first time a user accesses a service using HTTP or WAP. A Service Verify Request quota management message supplies the quota server with content from the user request (the URL, header information, user 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 CLI to define the service confirmation token that is used in URL-rewriting.

To enable or disable service verification, use the **verify** command in CSG service configuration mode. Service verification is also disabled when the quota server sends a Service Verify Tag-Length-Value (TLV) in a Service Authorization Response or Service Verification Response.

Service verification is supported only for HTTP and WAP.

As long as service verification is enabled, sessions of any type for this user do not trigger service reauthorization requests. Service reauthorization resumes for the user 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 user in a Service Verification Response. The CSG 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 (user 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.

RADIUS Features

The CSG provides the following RADIUS features:

- User Profile Retrieval from RADIUS Access Accept or Accounting Request, page 1-17
- Reporting RADIUS Attributes, page 1-18
- User Cleanup on RADIUS Accounting Start, page 1-19
- Processing Multiple RADIUS Accounting Stops, page 1-19
- RADIUS Monitor, page 1-19
- RADIUS Endpoint, page 1-20
- RADIUS Proxy, page 1-20
- RADIUS Handoff, page 1-21
- RADIUS Packet of Disconnect, page 1-21

See "Configuring RADIUS Support: Learning Who the Subscriber Is" section on page 5-1 for more information on configuring RADIUS features.

User Profile Retrieval from RADIUS Access Accept or Accounting Request

The user profile (billing plan) can be specified in a RADIUS message using the Cisco subattribute 1 VSA. The format of the VSA is:

csg:billing_plan= *billing_plan_name*

The *billing_plan_name* can be null, to indicate a postpaid user. Otherwise, the billing plan name must be sent as an uppercase string to match a configured billing plan on the CSG.

The billing plan is included in the RADIUS Access-Accept or RADIUS Accounting-Request message.

If the RADIUS Access-Accept includes the billing plan, the user ID (RADIUS attribute 1 or 31, as configured) must also be included; otherwise, the CSG is not able to associate the billing plan with the user.

Use the **user-profile server radius** command to retrieve the billing plan from the RADIUS message.

Reporting RADIUS Attributes

You can specify a set of attributes to be extracted from RADIUS Accounting Start messages for each subscriber, and reported with each transaction record. The CSG reports these attributes to the BMA and to the quota server. The CSG extracts these attributes from the RADIUS Accounting Start, and refreshes (replaces) its stored attributes whenever a RADIUS Interim Accounting message is received, to ensure that the latest user information is stored.

You can use Arbitrary RADIUS attributes to understand where a user is connecting to the network, and for correlation purposes. Examples of these attributes and their uses include:

- NAS-IP-Address (4) identifies the gateway that provides accounting control for the subscriber. Examples of such devices include the gateway GPRS support node (GGSN), Packet Data Serving Node (PDSN), HomeAgent, Cisco AS5300, and so on.
- SGSN IP (26/10415/6) identifies the SGSN the subscriber is accessing, if the CSG is configured to report all RADIUS attribute 26 (the Vendor-Specific Attribute, or VSA) instances.
- Acct-session-ID (44) uniquely identifies the session on this NAS and can be used for correlation to GGSN accounting records. The CSG cannot separate the RADIUS attribute 26s—it sends all of them.

The attributes are configured by their standard number, as shown in the following example:

```
ip csg accounting USER-BMA1
  user-group GROUP1
  agent activate 2 sticky 30
  agent 210.0.0.102 3386 1
  report radius attribute 3
  report radius attribute 5
  report radius attribute 7
  report radius attribute 44
  inservice
```

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 CSG supports continuation messages. A continuation message includes a correlator, a continuation number (so messages received out of order can be reordered), and an indication of the final message.

Note The CSG examines only the standard RADIUS attribute number and is not aware of any special formatting or subclassing for Vendor-Specific Attributes (VSAs). If a VSA is desired, then the CSG reports all VSAs (that is, attribute 26s).

If the configured attributes change, only new RADIUS requests are subject to the new attributes. Attributes already saved for a user continue to be reported.

When a RADIUS Start request is received, any attributes received from a previous Start request are deleted. If there are multiple instances of an attribute, they are all reported. Attributes are reported in the order they exist in the RADIUS message.

User Cleanup on RADIUS Accounting Start

A subscriber's connectivity attributes might change over time without a RADIUS Accounting Stop arriving to close down the previous accounting. Instead, it is possible that a new RADIUS Accounting Start or Interim Accounting message might arrive with the updated information. Some customers might choose to close all of the user's services if a significant change has occurred in the user's status.

With the **radius start restart session-id** command configured, the CSG deletes the user entry as if it had received a stop, closes all of the subscriber's services, and creates a new entry.

To avoid deleting the user entry because of a retransmission of the RADIUS message, the **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.

Processing Multiple RADIUS Accounting Stops

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 CSG removes the subscriber from the User Table when it receives the final stop, which contains an attribute indicating it is final. The CSG support for this functionality allows the specific attribute to be configured. If this function is configured, the CSG processes only the RADIUS Accounting Stop that contains the configured attribute. The contents of the specified attribute are not examined.

RADIUS Monitor

RADIUS monitor provides a way to insert the CSG into the RADIUS flow without changing the authentication, authorization, and accounting (AAA) or Network Access Server (NAS) addresses in the network. The CSG monitors the traffic between the RADIUS client and the RADIUS server, and watches for RADIUS messages flowing through it that match the configured rule. The address of the server must be configured.

Optionally, a RADIUS key is configured. If the key is configured, the CSG parses and acts on the message only if the RADIUS Authenticator is correct. If the key is not configured, the CSG always parses the message. The message is forwarded regardless of the key being configured or correct.

Here is a sample configuration:

```
ip csg user-group U1
  radius userid User-Name
  radius monitor 10.2.3.4 1234 key cisco --> Address, Port, and Key for RADIUS AAA Server.
  radius monitor 10.2.3.9 1234 key cisco2
  radius monitor 10.2.7.4 3901 key cisco --> Multiple AAA destinations can be monitored.
```

All RADIUS messages, including Access messages, are forwarded, except when the IP or UDP headers specify a length larger than the physical packet size.

All RADIUS messages, including access messages, are forwarded, except when the IP or UDP headers specify a length larger than the physical packet size.

When configuring RADIUS monitor for a server that is in the same subnet as a CSG interface, you must first configure a dummy route for that server, such as:

route *ip-address* **255.255.255.255 gateway** *gw-ip-address*

where:

- *ip-address* is any IP address that is not used in the network

- *gw-ip-address* is the gateway IP address

Add a RADIUS monitor configuration only after you have added the dummy route.

RADIUS Endpoint

To configure the CSG as a RADIUS Accounting endpoint, and to use RADIUS PoD with RADIUS endpoint, use the **radius endpoint** command in module CSG configuration mode.

To support RADIUS endpoint, the CSG requires a route to 255.255.255.255. You can configure the route by using the **gateway (module CSG VLAN)** command or the **route (module CSG VLAN)** command. For example:

gateway 31.0.0.6

or:

route 255.255.255.255 255.255.255.255 gateway 31.0.0.6

RADIUS Proxy

The CSG can act as a RADIUS proxy, forwarding all RADIUS accounting messages it receives to a configured RADIUS server. When the RADIUS server acknowledges a message with an ACK, the CSG forwards the ACK back to the client. RADIUS proxy supports both RADIUS Access and RADIUS Accounting.

The CSG allows you to specify only one RADIUS server, and the same RADIUS password must be used throughout.

RADIUS proxy can operate with clients that use large numbers of port numbers. The RADIUS client sends messages to the configured CSG (virtual) address. The CSG accepts messages for all ports on the configured address. The address of the RADIUS server is also configured. Optionally, a RADIUS key is configured. If the key is configured, the CSG parses and acts on the message only if the RADIUS Authenticator is correct. If the key is not configured, the CSG parses the message with no conditions. The message is forwarded regardless of the key being configured or correct.

All RADIUS messages (including Access messages) are forwarded except when the IP or UDP headers specify a length larger than the physical packet size.

To configure a CSG as a RADIUS proxy, use the **radius proxy** command in module CSG configuration mode. Keep in mind the following considerations:

- We recommend that you use this support with a small number (approximately 20) of RADIUS senders, where a sender is defined by its IP address and port.
- You can define up to 64,511 clients, where a client is defined by its IP address and port.
- The CSG IP address must be a virtual IP address, and it must be unique. The CSG IP address must not be specified in other CSG commands, and it must not match any real IP address, virtual IP address, or alias IP address configured on the CSG or in a /32 content configuration.
- You can configure a source IP address using the **radius proxy** command in module CSG configuration mode. The CSG uses the source IP address when it forwards a RADIUS message to the server.
- If you are load-balancing more than one CSG, you must configure the CSG's as RADIUS proxies, not RADIUS monitors.

RADIUS Handoff

In networks that do not use Cisco Home Agents (HAs), the CSG's RADIUS handoff feature can manage handoffs for roaming users.

The User Table identifies all users known to the CSG. The 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. When RADIUS handoff is configured, and a RADIUS Accounting Stop is received, the CSG starts a handoff timer instead of deleting the CSG User Table entry for the roaming user immediately.

- When a handoff occurs, the CSG detects an accounting start for the same user with a different NAS IP address. The CSG then uses the existing User Table entry for the user, to preserve the user information, and turns off the timer.
- If the handoff timer expires before the CSG detects an accounting start for the user, the CSG assumes a handoff did not occur and deletes the User Table entry for the user.
- In the event of a failover, all handoff timers are restarted.

To configure RADIUS handoff support, use the **radius handoff** command in CSG user group configuration mode.

RADIUS Packet of Disconnect

The quota server can instruct the CSG to disconnect a user. The CSG then sends a RADIUS Packet of Disconnect (PoD) message to the NAS identifying the user, and the NAS then sends a RADIUS Accounting Stop message, which also clears the User Table entry.

The quota server instructs the CSG to disconnect a user using one of the following methods:

- The quota server can send the UserDisconnectRequest message to the CSG. This message uses the UserIndex TLV to identify the user to be disconnected.
- The quota server can use Action Code 4 in the Action TLV in one of the following requests and responses:
  - The ServiceAuthResponse (indicating that the CSG is to send the PoD message when the quota runs out)
  - The ServiceStopRequest (indicating that the CSG is to send the PoD message immediately)
  - The UserProfileResponse (indicating that the CSG is to send the PoD message immediately)

The CSG sends the PoD message to the NAS that is specified by the NAS-IP-Address attribute (4) in the Accounting Start.

To configure RADIUS PoD support, use the following commands in CSG user group configuration mode:

- Use the **radius pod attribute** command to specify the RADIUS attributes to be copied from the RADIUS Start message and sent to the NAS in the PoD message.
- Use the **radius pod nas** command to specify the NAS port to which the CSG should send the PoD message, and the key to use in calculating the Authenticator.
- Use the **radius pod timeout** command to specify the number of times to retry the RADIUS PoD message if it is not acknowledged, and the interval between retries.

The CSG can send PoD messages only if the CSG received the user information on a virtual interface configured using the **radius proxy** or **radius endpoint** command in module CSG configuration mode.

HTTP Features

The CSG provides the following HTTP features:

HTTP Pipelining and Chunked Transfer Encoding

The CSG supports full HTTP pipelining and chunked transfer encoding.

Support for full HTTP pipelining and chunked transfer encoding required extensive redesign of the TCP engine and of HTTP parsing, which in turn impacted the way the CSG counts bytes. For HTTP billing, the CSG reports only TCP byte counts. To maintain backward compatibility, the CSG still reports IP byte counts, but the values reported are the same as the TCP byte counts. 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 CSG, and a failover occurs, the CSG does not increment the content counters for traffic flowing through these connections. The CSG 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 CSG 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.

HTTP 1.0 Content Billing

The CSG enables you to bill users for individual transactions by discriminating on a per-object basis, and on a per-user 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 end user.

HTTP 1.1 Content Billing

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

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 (as well as by IP address) immediately, without having to wait for the HTTP Statistics record.

You can configure the CSG to send the HTTP Header message as soon as it is generated, rather than batching it until an entire packet is filled. This reduces latency and notifies the BMA about the client's transaction as quickly as possible. This type of reporting is more efficient, but provides less information, and should be used only when the BMA needs to react to the client's activity very quickly.

You can configure the CSG to not send the HTTP Statistics message. This 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 CSG 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 CSG reports HTTP-specific information about the request, such as the URL, as well as HTTP error codes (that is, response codes of 300 or higher).

WAP Features

The CSG provides the following WAP features:

- WAP Traffic, page 1-23
- WAP 2.0, page 1-24
- WAP Cutoff, page 1-25
- Concatenated WAP PDUs, page 1-25

WAP Traffic

The CSG 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 WTP and WSP in support of WAP 1.2—The ability to generate billing records for each WAP GET, POST, PUSH/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 MMS, and to exclude charging for MMS.
- Top-up capability using URL redirect.
- URL-map support for WAP.
- Support for multiple services.
- WAP 1.2.1 HTTP support: The CSG HTTP support is compatible with WAP 1.2.1 (HTTP over WP-TCP) 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 CSG supports WAP 2.0—a specific dialect of XML that can be transported over HTTP to convey content to the mobile devices. The incomplete WAP 2.0 standard specification defines five network flows in which mobile devices might participate. The first four flows described below are generally implemented over WAP 2/HTTP/TCP across a WAP 2.0 Proxy/Push Proxy Gateway (PPG). The last flow (Flow number 5, TO-TCP) is not supported.

General flows supported in the CSG

1. Retrieve a message from the network using HTTP.request-method: GET
2. Post a message into the network using HTTP.request-method: POST
3. Acknowledge a PUSH indication using HTTP.request-method: POST

Push flows generally implemented as WAP 2 over SMS OTA-Push

These flows are generally implemented as WAP 2/SMS rather than WAP 2/HTTP.

4. PO-TCP: The PPG establishes a direct connection to the mobile device using prior knowledge of the mobile device's IP address. The PPG negotiates an understanding of the mobile device's identity and capabilities using HTTP.request-method: OPTIONS, then uses HTTP.request-method: POST to deliver the push notification as a WAP 2.0 XML message. The WAP 2.0 XML might wrap other content such as MMS-encoded notifications or URLs.
5. TO-TCP: This form of PUSH is a hybrid between the conventional pure Short Message Service (SMS) notification and previous flow. It provides a bridge during a transition period where the PPG does not have prior knowledge of the mobile device's IP address. This push is implemented as a WAP 2 Session Initiation Request (SIR) over SMS. Upon receipt of the SIR, the mobile device connects to the PPG via TCP. The PPG then begins the HTTP exchange described in flow 4 above.

Note The TO-TCP flow is not supported, but is provided for informational purposes.

The CSG supports billing WAP 2.0 traffic (the first three flows above) using existing configuration commands. WAP 2.0 mobile devices might be configured to use or to ignore the WAP 2.0 proxy; 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 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/HTTP and MMS/WAP 2.0/HTTP.

Differentiated Billing of MMS Over WAP 2.0

WAP 2.0 mobile devices generally implement support for extensive Multimedia Messaging Service (MMS). This is generally implemented over WAP 2.0. Service providers use MMS to differentiate and promote their products, which necessitates differentiating the billing of MMS over WAP 2.0 from other WAP 2.0 billing.

The CSG supports the ability to bill MMS over the supported WAP 2.0 flows at a differentiated rate. When WAP 2.0 billing is configured, MMS might be differentiated by using the capabilities of the **http** accounting type to detect some or all of the following characteristics of MMS/WAP 2/HTTP 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 three types of notification:

1. SMS-based notification carrying the URI for the MMS. The handset then initiates a GET request to that URI to retrieve the information.
2. TO-TCP (Terminal-Originated TCP) starts with SMS, but only provides 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 and must succeed before the handset can retrieve the notification.
3. PO-TCP (PPG Originated TCP) is similar to TO-TCP except the TCP connection is opened by the PPG, and is followed by the OPTIONS method.

The CSG Layer 7 billing for MMS relies entirely on options one and three. 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.

WAP Cutoff

When a user’s quota is entirely depleted in the middle of a transaction, the corresponding action varies depending on the protocol. For WAP, the current transaction is allowed to complete, and the user is charged for all bytes used in the transaction. The result is that the user has a negative quota balance. On the next transaction request, the user is redirected to the top-off server. While this behavior provides the best user experience, it also allows some leakage. For small transactions, the leakage is minimal; however, for large transactions the leakage can be significant.

Because there is a trade-off between end-user experience and leakage, a CSG configuration option allows you to choose what behavior you want to enforce. To configure this feature, enter the **zero-quota abort type** command in global configuration mode. The configuration option is enabled on a per-service basis. This option is only supported for WAP, and the default is to not terminate a transaction midstream when the user runs out of quota. For all other protocols, the user is cut off midstream.

Note Configuring the cut-off option for WAP affects only connection-oriented sessions, and not connectionless traffic.

When configured, this condition causes the existing transaction to be aborted. The CSG sends aborts to both the client and server, terminating the transaction. A BMA record for the transaction is generated with a flag setting in the Wireless Transaction Protocol (WTP) information record that indicates the transaction was intentionally aborted. In the report, the user is charged for the number of bytes that were processed for the transaction, including the bytes that caused it to exceed the quota balance. Typically, the user should not be charged for this transaction because it was not allowed to complete. The user is reimbursed by the billing agent for transactions with the 0x04 flag set, or by the prepaid refund feature.

Concatenated WAP PDUs

The CSG 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 should be assigned. Here is how the CSG 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

RTSP Features

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

- RTSP Billing, page 1-26
- Per-Click Authorization, page 1-27
- Correlation, page 1-27

RTSP Billing

The RTSP Billing feature adds the following functionality to the CSG:

- Correlates various streams associated with an RTSP session.
- Reports application-level information (for example, filename) to the billing system.

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

- RTSP requires a control TCP connection to server port 554.
- 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 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 resends 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:

- Client sends SETUP request suggesting one or more modes it can support.
- Server responds with mode 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 CSG sends a contentAuthorizationRequest at the beginning of the TCP session. For each transaction involving a data stream, the CSG sends a contentAuthorizationRequest before allowing the data stream. This request allows the quota server to inspect the filename before granting authorization.

The CSG only allows Network Address Translation (NAT-based) redirection for RTSP traffic.

RTSP allows multiplexing multiple data streams over the same transport. For example, audio and video presentations can be multiplexed over the same UDP flows. In these cases, the quota server must ensure that it does not send contradictory responses to the various contentAuthorizationRequests. For example, if one request is allowed and the other one denied, the CSG's behavior is undefined.

Correlation

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

The CSG 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 audio and video stream for a movie. For instance, if M is the media server, a client (C) can perform the following operations over the same RTSP session:

Table 1-1 Multiple Streams Controlled by Single RTSP Session

Client	Server	Protocol	Method/URL
C	M	RTSP	DESCRIBE rtsp://a.ex.com/movie.sdp Client requests description of a movie. The server assigns a session ID to the client, and sends the.sdp file containing information about the movie.
C	M	RTSP	SETUP rtsp://a.ex.com/movie/audio Client requests setup of a stream.
C	M	RTSP	SETUP rtsp://a.ex.com/movie/video Client requests setup of a second stream. This results in setting up of four UDP flows.
C	M	RTSP	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, and four UDP streams associated with it. The CSG is able to correlate all these four UDP streams together 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 CSG has no easy way to find out that these two streams are related. A typical situation is when 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. The following interactions take place:

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 three concurrent sessions:

- HTTP 1.1 sessions: 1
- RTSP Video Session: 2, 4
- RTSP Audio Session: 3, 5

All of the sessions (TCP and UDP) 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 no correlation 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 end-user presentation are present. A container file represents an RTSP presentation, with each of its components being RTSP streams. 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 describing the contents of a container file.

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

Interleaved RTSP

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

To avoid a bottleneck, the CSG does the following for interleaved RTSP sessions:

- Wait for a SETUP request/reply to determine whether this is an interleaved RTSP session.
- Remember the URL information.
- After determining interleaved RTSP, report RTSP information to BMA/quota server, and shortcut the connection to fastpath. Any subsequent transactions on the same RTSP control connection is not visible to the CSG's billing function.

This method provides some RTSP level information, but avoids making the RTSP path a target of DoS attacks. If most of the RTSP streaming billing applications are in the walled garden, customers have some control over the servers to ensure that the use of interleaved RTSP is not too much.

CDRs

The CSG generates the following the 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 CSG does not generate any UDP CDRs.

RTSP billing in the CSG is based on inspection of the RTSP SETUP and TEARDOWN messages that are exchanged between the client and server. The CSG builds the RTSP CDR immediately after the RTSP TEARDOWN signal if the URL exactly matches that from the RTSP SETUP signal. Otherwise, the CSG builds the CDR after any condition that causes the flows to be terminated. Examples include:

- When the idle content timer expires. By default, this timer is set to 3600 seconds (1 hour). To receive the RTSP CDRs sooner, set the timer to a smaller value, such as 60 seconds, using the **idle** command in CSG content configuration mode.
- When a service_stop is triggered (for example, when the access server sends a RADIUS Accounting Stop for the user).

Session Processing

RTSP control session processing is similar to FTP control sessions. The RTSP control session is assigned an 8-byte correlator. 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 CSG keeps track of RTSP sessions and an RTSP session is used to correlate multiple streams associated with the session.

Note An RTSP session might be comprised of more than one TCP session; alternatively, the RTSP session can exist without a TCP session between client and server.

When the client sends a **setup** command, the CSG notes the client ports and extracts server ports 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 CSG actions are annotated after various steps.

In this example, client C requests a presentation from 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 CSG makes sure that X+i is even. 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 the various flows for an RTSP transaction together, and also enable 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, so the CSG lets the streams idle out and sends usage records when the streams idle out.

POP3 Support

The CSG 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 CSG no longer generates a final TCP Stats record. If a user downloads multiple e-mails during a single TCP session, the CSG generates a CDR for the previous e-mail each time it processes a new RETR or TOP command. The CSG generates a CDR for the last e-mail when it processes the STATS command (for TCP termination).

The CSG supports POP3 in both prepaid and postpaid mode.

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

To define the POP3 accounting type for a billing policy, use the **accounting type pop3** command in CSG policy configuration mode.

SMTP and POP3 Data Mining

SMTP is the Internet mail transfer protocol that operates over TCP with port 25. End users send messages using SMTP, and it is also used to transfer messages between SMTP gateways (or relays). POP3 is a common protocol used to retrieve Internet mail from a 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— RFC2822 headers that appear as contents to the SMTP and POP3 protocols. The RFC2822 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 CSG 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, with the exception of 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 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 CSG 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 CSG Report String Attribute reports also has a continuation option. This means that information for a single header might span multiple CSG Report String Attribute reports which might span multiple CSG Data Records.

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

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 Mapping and URL Mapping

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

- The CSG provides header mapping and filtering for HTTP. For more information about header mapping, see the description of the **match (header map)** command.
- The CSG provides URL mapping and filtering for HTTP, RTSP, and WAP. For more information about URL mapping, see the description of the **match (URL map)** command.

Passthrough Mode and the Default Quota

For prepaid users, when a quota server is not available for authorization grant of quota, sessions are blocked. In passthrough mode, the CSG grants quota for services and their sessions when a quota server is not available. The CSG allows all traffic to pass, and CDRs are flagged for special consideration by the BMA.

For each service that you want to use passthrough mode, you must enable it using the **passthrough** command in CSG service configuration mode.

If you enable passthrough mode for a service, do not disable quota server reassignment for user groups associated with that service. That is, do not configure **no quota server reassign** in CSG user group configuration mode for user groups associated with the 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 CSG 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 CSG continues to grant quota as long as a quota server is inactive.

When the service becomes idle, the CSG generates and stores a ServiceStopRequest message, containing the total usage for this instance of the service. When a quota server becomes active, the CSG forwards all stored ServiceStopRequest messages to the quota server.

This section contains the following additional information about passthrough mode:

- Flagging of Messages, page 1-33
- User Profile Requests, page 1-33
- Quota Server Recovery, page 1-33

Flagging of Messages

To facilitate billing recovery, some messages to the quota server and the BMA include a QuotaServerFlags TLV. The CSG adds this TLV whenever it grants a passthrough mode quota to a service.

User Profile Requests

When the CSG learns of new users, it typically sends a UserProfileRequest to an active quota server. This enables the CSG to learn the billing plan to use for each user. If the quota server returns a NULL billing plan, a user is postpaid.

When passthrough mode is in use for any service, the CSG changes the way it processes UserProfileRequests. When there is no active quota server, the CSG assigns all new users to postpaid processing. The CSG reports all sessions for these users as postpaid, and does not flag generated CDRs with a QuotaServerFlags TLV.

If a user is still on the network when the quota server becomes active, the CSG sends a normal UserProfileRequest to the quota server for the user. When the CSG receives a response, it updates the user's billing plan. If the updated billing plan is now a prepaid billing plan, the CSG blocks new IP sessions started by the user 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 CSG forwards stored ServiceStopRequests to it. Additional actions taken by the CSG depend on user traffic.

When a user who was forced to postpaid while the quota server was absent creates a new IP session, the CSG issues a UserProfileRequest followed by a ServiceAuthorizationRequest, and blocks new traffic until quota has been granted.

Prepaid users might have some services that were granted quota in passthrough mode. For those services, when quota runs low, the CSG sends a ServiceReauthorizationRequest 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 CSG in passthrough mode. The requested quadrans TLV contains a request for an additional quota amount.

When the quota server responds to a ServiceStopRequest or a ServiceReauthorizationRequest, the CSG moves the service out of passthrough mode. If the quota server denies quota when it sends a ServiceAuthorizationResponse message, the CSG blocks the traffic. The CSG also flags CDRs generated by traffic for these services, which received passthrough mode quota grants, with QuotaServerFlags TLVs, until a ServiceStop is sent. That is, once a service is granted a passthrough mode quota, the CSG flags all CDRs for that serviced, up to and including the ServiceStop. Again, this only applies to prepaid users. Postpaid users CDRs are never flagged.

Service Duration Billing

The Service Duration Billing feature enables the CSG to deduct quota based on the time of network usage for prepaid (or “managed”) users. With this feature, the user is charged for the time duration of the CSG service. The charging is performed 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 with content idleness. Because non-TCP sessions (such as UDP) do not have a Layer 4 session termination mechanism, the LBST for non-TCP sessions is the last packet forwarded for the IP session.
- 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 non-zero quota.
- The Last Billable Time (LBT) is the greatest timestamp (in seconds) of the LBST for all IP sessions mapping to the service for this user. Optionally (and by default), the value for service idle is added to the maximum interval of the LBST when calculating the LBT. The reason for adding the service idle timeout to the duration is because the duration calculation already includes the intermediate (between IP sessions) idle intervals, so the last idle interval should also be included.
- If the service object is destroyed due to service idleness, the calculation for usage is:

  Usage = LBT - FBT

  If the service object is destroyed due to an asynchronous event such as user logoff, the calculation for usage is:

  Usage = LBT - FBT

  or

  Usage = Async Event Timestamp - FBT

  whichever is smaller.

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

  Usage = LBT - FBT

  or

  Usage = OutOfQuota Timestamp - FBT

  whichever is smaller.

Note If the user runs out of quota, but the user refreshes the quota before the service idles out, the periods (or gaps) of zero quota is 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 CSG module, you cannot modify the basis or meter configuration. You are instructed at the console to configure **no inservice** on the downloaded Accounting definitions.

Reporting to the BMA

For service duration billing, the unit for quadrans reported to the quota server and BMA is 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 individual sessions or the sum of durations of individual sessions.

Out of Quota

When a subscriber runs out of quota, the CSG terminates the user sessions mapped to the service using the same asynchronous session kill mechanism that is used when a subscriber User Table entry is deleted. The CSG 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 CSG to deduct quota based on the time that a user is logged on to the IP network. That differs from Service Duration Billing, which charges based on the duration of a service. Because the service measures the duration of subscriber access, the service is never idle—it is destroyed only when the user logs out, or when a Service Stop Request is received from the quota server.

The CSG charges based on 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 due to 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 user has quota, the FBT is typically the same time as the RADIUS Accounting-Start.
- The Last Billable Time (LBT) is the timestamp, in seconds, when the User Table entry is destroyed. During the service lifetime, the CSG updates the LBT when either of the following situations occurs:
  - An IP session starts or ends.
  - A Service Reauthorization Request is sent by the CSG. This results in an update to the service balance and usage before the Service Reauthorization Request is sent. The CSG uses the following algorithm to calculate the usage:

    Usage = LBT - FBT

    or

    Usage = OutOfQuota Timestamp - FBT

    whichever is smaller.

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

    Usage = LBT - FBT

    If the user 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 user runs out of quota, existing prepaid and postpaid IP sessions for the subscriber are terminated. If the user does not have quota to proceed, no IP sessions for the user are allowed to proceed. The CSG provides enforcement for only those policies that have accounting configured.

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

Postpaid Service Tagging

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

The service must be associated with a billing plan configured for postpaid mode. As in the case of prepaid billing plans, the user 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 user is automatically associated with any billing plan configured for postpaid mode. In such cases, we strongly recommend that you configure only one billing plan for postpaid mode.

Stateful Redundancy and Failover

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

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

As described in the "Configuring Fault Tolerance" section on page 4-4, the primary and backup CSGs use a private VLAN to exchange connection and billing status information. The configurations must be the same on each CSG. The quota server, BMA, and user ID database definitions should also be the same, although this is not required.

During normal operation, connection and billing state information is sent by the primary CSG to the backup CSG, and from the primary quota server to the backup quota server. Both the primary and the backup CSGs maintain state information for the configured BMAs, and the primary CSG keeps the backup CSG informed as to which BMAs and quota servers are being used. If the primary CSG fails, the backup CSG takes over operation and tries to use the same BMAs or quota servers, if it has connectivity. Otherwise, the backup CSG selects the BMAs or quota servers with the highest priority.

The primary CSG also informs the backup CSG when user IDs are added to or removed from the User Table, and sends the correlators to the backup CSG 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 CSG, and a failover occurs, the CSG does not increment the content counters for traffic flowing through these connections. The CSG does increment the content counters for new connections created after the failover.

The CSG provides full stateful failover for FTP and IMAP sessions.

The CSG provides limited stateful failover for HTTP, POP3, SMTP, and WAP sessions. User information and quota information is maintained on the backup CSG; however, in-flight transactions are not. If the primary CSG fails, the user transaction completes on the backup, but no quota is charged for the transaction. Normal billing resumes with the user's next transaction.

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

The CSG does not support stateful redundancy for IP, RTSP, or UDP connections.

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

"Default" Policy

The CSG matches content on a best-match basis, based on Layer 3 and Layer 4 information. When there is a successful content match, the CSG then matches against the policies configured within that content, linearly, on a first-match basis. If no policy within the content matches, the CSG 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.

For example, given the following policy and content configuration:

```
ip csg policy PHTTP1
  accounting type http customer-string HTTP-POL1
ip csg policy PHTTP1
  accounting type http customer-string HTTP-POL2
ip csg content HTTP
  policy PHTTP1
  policy PHTTP2
```

The output from the **show module contentServicesGateway 5 content name HTTP detail** command is as follows:

```
HTTP, state = OPERATIONAL, index = 10
  destination = 198.133.219.0/24:80, TCP
  idle = 3600, replicate = none, vlan = ALL, pending = 30
  max parse len = 4000, persist rebalance = TRUE
  conns = 0, total conns = 0

  policy          total conn   client pkts  server pkts
  ------------------------------------------------------
  PHTTP1          0            0            0
  PHTTP2          0            0            0
  (default)    4760        30056        26534
```

In this example, any TCP traffic that does not match either the PHTTP1 policy or the HTTP2 policy matches the "default" policy, and is reflected in the **(default)** row.

Prepaid Error Reimbursement

The Prepaid Error Reimbursement feature allows the CSG to automatically refund quota for failed transactions, as defined by the CLI. Refund conditions can be configured using session flag (IP, TCP or WAP) settings and application return codes.

The CSG also adds a refund TLV to the statistics records on the BMA interface. The refund TLV is added for transactions that meet one of the refund conditions. 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 For duration-based services, error reimbursement is not possible.

If refund is enabled for a CSG prepaid service, you cannot download more than 0x6FFFFFFF bytes of data in a given transaction.

Support for the Cisco Persistent Storage Device

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

Under normal conditions, the CSG sends content billing records to the mediation partners' servers. If, for any reason, those servers become unreachable, records are sent to the PSD for safekeeping until contact is reestablished with the Billing Mediation Agent (BMA). Once contact is reestablished, the CSG retrieves the records from the PSD, and forwards them to the BMA.

Storage

Under normal conditions, the PSD provides backup 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.

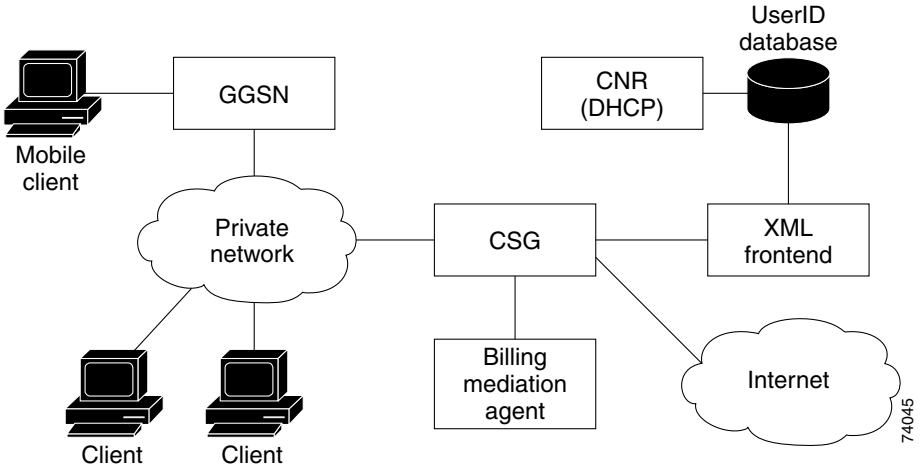
Retrieval

Once the CSG 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 CSG in the same order and form as it was deposited. The CSG is responsible for maintaining order, if necessary, or of mixing retrieved data with incoming "live" records. Once the CSG acknowledges to the PSD that it has successfully sent the data to the client server (the BMA), the PSD deletes that data. The PSD stores the data until it receives this acknowledgement.

Postpaid Billing

Figure 1-1 illustrates simple traffic flows between the various components in a simple postpaid CSG environment.

Figure 1-1 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 CSG monitors data flows and generates accounting records that can be used to bill customers at a content-level granularity. The CSG 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.

BMA Load Sharing

The CSG can support multiple BMAs. This is useful in environments in which the number of billing records sent by the CSG could overwhelm a single BMA.

Note Multiple BMAs cannot have the same IP address.

The CSG maintains GTP' sequence numbers for each BMA.

All of the billing records for a given user are sent to the same BMA.

Quota Server Load Sharing

The CSG supports multiple quota servers. This is useful in environments in which the number of quota transactions sent by the CSG could overwhelm a single quota server. Multiple quota servers can be simultaneously active, and the CSG assigns a quota server to each user. All quota transactions for the user are done with the same quota server.

When a quota server fails, all users associated with that quota server are distributed among other quota servers.

Note Multiple quota servers cannot have the same IP address.

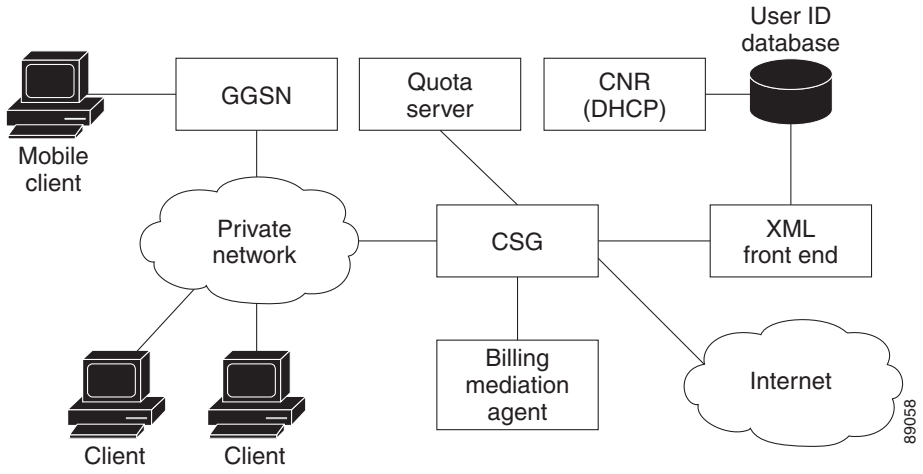
Prepaid Content Billing and Accounting

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

The CSG uses a quota server to keep track of the quota that is left in the user's account. Each CSG supports one quota server and multiple idle backup quota servers. The CSG allows multiple groups of users on each quota server, with one quota manager for each user. Figure 1-2 illustrates a typical CSG prepaid content billing network.

Figure 1-2 CSG Prepaid Content Billing Network



Quota is provided by the Quota Manager, on request for quota by the CSG. This quota is either for an initial service connection, or for subsequent re-authorization when the original/last quota grant is depleted. The Quota Manager is allowed to provide a value in the range of 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 user can no longer access the service.

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

Once the user finishes a session by closing the bearer session (a RADIUS Accounting Stop 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.

The following example flow illustrates a basic prepaid flow between the CSG and the Quota Manager:

1. The NAS/GGSN sends an Access Request to the RADIUS Server.
2. On receipt of an Access Accept from the RADIUS Server, the NAS/GGSN sends an Accounting Start to the RADIUS Server.

3. The CSG creates a user entry, and links the user IP address to either the username or Calling Station ID (depending upon the configuration of the CSG).
4. The CSG sends a User Authorization Request to the Quota Manager.
5. The Quota Manager replies to the CSG with a valid billing plan for the user (User Authorization Response).
6. User traffic begins to flow from the NAS/GGSN toward the requested server.
7. The CSG 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 it has quota to give).
9. The user traffic passes the CSG to the service, and prepaid billing begins.
10. A Service Stop occurs if either the NAS/GGSN sends a RADIUS Accounting Stop, or if the content and service idle out.
11. Service Stop provides the quota used and returns any remaining quota.

Obtaining User IDs

The CSG uses two methods to obtain user IDs:

- The CSG can use an external user ID database to map IP addresses to user IDs. When the CSG 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 CSG generates an accounting record without it.
- The CSG can act as a RADIUS Accounting Server or a proxy for RADIUS accounting messages. The CSG can examine the accounting messages to determine user IDs. (The CSG does not support full RADIUS accounting.)

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

Filtering Accounting

Filtering lets you configure the following functionality:

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

Per-Event Filtering

The CSG supports the following per-event actions that require instruction from the billing system, and are supported as variations of the same design:

- Per-Event Filtering—Permits or denies a transaction as directed by the quota server.

To enable these functions, use the **authorize content** command in CSG service configuration mode.

Intermediate Billing Records

Typically, the CSG sends two billing records for each HTTP session. The CGS 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 CSG to send intermediate billing records after a specified number of seconds, or after a specified number of bytes, whichever occurs first.

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

The CSG supports intermediate billing for FTP, HTTP, IP, TCP, and UDP. The CSG does not support intermediate billing for WAP or e-mail protocols (such as IMAP, POP3, and SMTP). The CSG does not support intermediate billing for RTSP control sessions unless the video/audio traffic is also transported over the control session.

Packet Forwarding

The CSG configurations allow users to specify multiple gateways; one for each of the VLANs. However, only one default gateway can be in effect at a time. So, the second default gateway configured does not take effect until the first default gateway is unconfigured. Generally, you should only specify one default gateway to avoid confusing which default gateway is being used by the CSG at any given moment.

All traffic that passes through the CSG (including the traffic to and from the CSG [GTP' traffic]) is routed and forwarded based on the VLAN interface, route, and gateway statements specified under the **module CSG** commands.

For example:

```
Module ContentServicesGateway 6

vlan 10 server
ip address 10.250.0.1 255.255.0.0
gateway 10.250.1.1

vlan 251 client
ip address 10.251.0.1 255.255.0.0
route 10.200.0.0 255.254.0.0 gateway 10.251.2.11
```

For packet forwarding, the following logic applies:

1. If the destination IP address of the packet is a subnet adjacent to one of the VLAN interfaces configured, the CSG tries to map the destination IP address to a MAC address, using the Address Resolution Protocol (ARP), and forwards the packet.
2. If the destination IP address of the packet is not subnet-adjacent, the CSG forwards it based on the routes specified.
3. If there are no matching routes, the CSG forwards the destination IP address of the packet based on the default gateway as defined. If no default gateway is specified, and if the CSG does not have an ARP entry in its ARP cache for the MAC address, the CSG drops the packet.

For packets that originated from the CSG (GTP'), the CSG uses the VLAN interface that resulted from the above forwarding logic to forward the packet. In the configuration example above, if a packet is forwarded using the default gateway, it uses the source interface of 10.250.0.1 to forward the packet.

In general, the default gateway is used to specify on the server VLAN to direct client traffic to the Internet. This prevents you from having to specify lots of subnets, as some of them are not easily identified. However, the default gateway can be placed in either the client or server VLAN.

In addition to using route/gateway to forward the traffic, client/server traffic can also be forwarded using next-hop as specified in the billing policy. For example:

```
ip csg policy FORWARD_PKT
      accounting customer-string CLIENT-TRAFFIC
      next-hop 1.1.1.1

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

In the above example, if traffic hits this content and policy, the traffic is forwarded to next-hop router that has an IP address of 1.1.1.1.

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

Miscellaneous Features

The CSG provides the following miscellaneous features:

Support for the CSG MIB

The CSG supports the CISCO-CSG-MIB implemented in Cisco IOS.

Note The CISCO-CSG-MIB agent queries every CSG module on the chassis, so minor delays in responses to SNMP queries are to be expected. To prevent potential problems, you might need to increase the SNMP walk timeout.

Non-HTTP Traffic

For non-HTTP traffic, the CSG records information about data transfer based on flow information.

Fragment Support

The CSG supports IP fragments for both TCP and non-TCP flows, including fragments that arrive out of order.

Report Billing Plan ID to BMA and Quota Server

The CSG reports the billing plan identifier string in BMA records, and in messages to the quota server.

Asynchronous Quota Return

The Asynchronous Quota Return feature allows the quota server to request the CSG return quota for a defined user and service, and send a Quota Return.

Prior to CSG 3.1(3)C6(2), the quota returned via a Quota Return message did not include quota reserved for ongoing transactions. Beginning in CSG 3.1(3)C6(2), the quota reserved for ongoing transactions is recalled from the transactions and included in the quota returned in the Quota Return message.

Asynchronous Service Stop

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

Support for Port Number Ranges

When you define content on the CSG, you can define a single port number, or a range of port numbers. This eliminates the need to define 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 **accounting type http** means that the CSG 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 CSG, as well as generating many CDRs that the customer had not planned for.

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

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

Packet Counts

The CSG 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 CSG 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 CSG might report this negative balance to the quota server as a negative number in the Remaining Quota TLV.

Dependencies and Restrictions

- The CSG supports only Internet Protocol version 4 (IPv4). It does not support Internet Protocol version 6 (IPv6).
- The CSG does not support IP packets larger than 1500 bytes.
- The CSG supports up to 256 total VLANs (client and server).
- The CSG supports up to 1024 content/policy pairs configured under services within a billing plan. Note that if two billing plans contain the same service, the content/policy pairs are counted multiple times.
- The CSG supports up to 4000 content definitions (or virtual server definitions in postpaid); up to 1000 unique IP addresses (virtual IP addresses plus VLAN IP addresses and alias IP addresses); and up to 127 contents for each unique IP address (each content counts as one and each VLAN/alias IP address counts as four).
- The CSG supports up to 255 services and up to 1024 services rules.
- The CSG supports up to 16,000 access control list (ACL) items.
- Up to six Cisco CSGs and/or CSMs can be installed in a Catalyst 6500 series switch or Cisco 7600 series router chassis.
- You cannot cascade two or more CSGs. For more information, see the TCP compliance exceptions in the "Layer 7 Inspection (accounting type=specific protocol)" section on page D-1.
- The CSG runs with Cisco IOS Release 12.1(12c)E4 or later.
- More than one CSG can run in a Catalyst 6000 series switch or Cisco 7600 series router chassis.
- The CSG 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 CSG fault-tolerance support allows two CSG modules (in the same or in different chassis) to be configured in the active and standby modes.
- For IP Layer 4 and Layer 7 inspection, the CSG volume counters wrap at 0xFFFFFFFF (4294967295 bytes). The volume counters are 32 bits unsigned.
- During chunked POST processing, the CSG can buffer up to 29,696 packets for all users. Therefore, the maximum theoretical POST size for a single user would be 44.5MB (29,696 packets at 1,500 bytes/packet). However, this theoretical maximum is reduced if other users have active chunked POSTs in process.
- The CSG reports all times in Coordinated Universal Time (UTC), regardless of the setting of the **clock timezone** or **clock summer-time** command.
- For RTSP, keep the following considerations in mind:
  - RTSP requires a control TCP connection to server port 554.

  - RTSP offers minimal support for TCP-interleaved and HTTP-tunneled transport: only the first stream URL is reported. 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 terminated/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 such choice is to interleave the stream with the control channel. In this mode, the CSG cannot map the transport connection to a different policy, and URL mapping cannot be supported.

    The other shared mode for RTSP is to use a single HTTP connection. RTSP tunneled over HTTP has the same limitation as interleaved RTSP: The stream cannot be mapped to a policy different from the control connection, as both of them share the same transport.
  - The CSG does not support multicast RTSP.
  - The CSG does not correlate streams described in a container file, for instance, SMIL.
  - The CSG parses only the RTSP control session. When multiple RTSP streams are multiplexed over the same transport, the CSG reports cumulative statistics for all such streams.
  - If RTSP URL mapping and filtering is used, and multiple RTSP streams share the same transport channel, the CSG generates a single content authorization request, and the request contains all URLs carried over that stream. Also, the RTSP stream CDR contains URLs for all streams that are multiplexed over the same transport channel.
  - If an RTSP proxy is used, the CSG should be placed on the client side of the proxy. If the CSG is placed on the network side of the proxy, the CSG sees packets originating from the proxy, and the CDRs reported contain the proxy's IP address, instead of the client's.
  - After a CSG failover, existing RTSP UDP streams continue to operate if a catch-all content rule was defined to pass unknown UDP flows. However, RTSP correlation for those streams ceases, and billing is limited only to the parameters defined for the catch-all content rule. New RTSP connections are processed normally.
  - For RTSP, all policies must use the same access control list (ACL) and the same next-hop IP address.
  - For RTSP, the policy used to determine the next hop address is chosen based solely on ACLs, not URL maps. As a result, you can choose the next hop from one policy for routing and from a different policy for billing.

- For fault-tolerant (FT) CSG pairs:
  - Each FT CSG pair must use a different FT VLAN.
  - If you have pairs of CSG cards and pairs of CSM cards in your network, each pair must use a different FT VLAN. Do not configure a CSG pair and a CSM pair to use the same FT VLAN.
  - The CSG does support trunked FT VLANs, but each pair of CSGs must use a unique FT VLAN and a unique group ID. In addition, make sure that the number of high availability messages between all pairs of CSGs on the trunk does not overwhelm the CSG card.
  - A single CSG environment does not require a route in the Content Services Module (CSM) pointing to the CSG RADIUS virtual IP address. However, in a fault-tolerant setup, or a multiple-CSG setup, a route to the CSG RADIUS virtual IP address is required. This route must point to the Alias IP of the appropriate CSG.
- Traffic coming from an unknown source MAC address on the client-side or server-side VLAN is dropped by the CSG.

- The IP address in the content definition cannot be in the same subnet as the IP address of the client VLANs.
- When you configure redundant CSGs, the backup CSG must use the same software release as the primary CSG, or a later software release. If your CSGs act as backups for each other, they must all use the same software release.
- Advice of Charge (AoC) via content authorization and URL-redirect is supported for only HTTP and WAP/WSP.
- When a CSG prepaid service is configured for Advice of Charge (AoC), the weighting value for charging the content is not determined until the CSG processes the Content Authorization Response. For SMTP billing (**accounting type smtp**), the CSG does not send the Content Authorization Request until it processes the SMTP DATA command. If the CSG does not process the SMTP DATA command for a session, then the CSG does not charge the session for volume and event billing.
- The CSG does not support multiple protocols under a single service definition. Do not configure a CSG service with more than one accounting protocol type.
- Service verification is supported for only HTTP and WAP.
- FTP requires a control TCP connection to well-known server port 21.
- For WAP, keep the following considerations in mind:
  - All policies must use the same access control list (ACL) and the same next-hop IP address.
  - For WAP1.x, the policy used to determine the next hop address is chosen based solely on ACLs, not URL maps. As a result, you can choose the next hop from one policy for routing and from a different policy for billing.
  - The CSG supports only URL maps for WAP; header maps are not supported. You cannot use the CLI to configure header maps for WAP services. Policies defined as accounting type **wap** can accept only URL map definitions. For WAP 1.x, URL maps take precedence over access lists.
- For IMAP support, message tags cannot be longer than 100 bytes. If the CSG encounters a message with a tag length greater than 100 bytes, only IP and TCP upstream and downstream byte counts are reported.
- The CSG does not support the CLOSING or TIME-WAIT states for TCP connections. After the end-points exchange FIN_ACK messages, the connection is terminated immediately, and the CSG does not process any out-of-order packets for the connection.
- The RADIUS Accounting Start message which specifies the NAS IP to which to send the PoD message must be received on an IP address specified by the **radius proxy** or **radius endpoint** command configured in module CSG configuration mode.
- For CSG type=HTTP parsing, the CSG imposes the following restrictions:
  - The HTTP method must be initiated by the same endpoint that initiated the TCP connection (by the same side that sent the TCP SYN); the impact is that the client request transfers no data.
  - The maximum HTTP transaction volume is 268435455 bytes. If this length is exceeded, the CSG invokes Layer 4 billing for the remainder of the connection.
  - HTTP request parsing is limited to 64,000 bytes. Any headers beyond this limit are not recognized and are not used in matching URL or header maps.
  - Sharing of the same port for both HTTP and HTTPS is not supported. However, SSL can be tunneled over HTTP using the Connect method.
  - There are two types of maps for HTTP, URLs and headers.

  - If policy type=http, the only TCP option that is passed through the CSG is the Maximum Segment Size (MSS). The other options are dropped. This includes Wireless Profiled TCP Options (example: SACK) that are used with WAP2.0 implementations.
  - With RFC2818, an HTTP session can become encrypted via the UPGRADE method. If Layer 7 billing is defined for the HTTP port, then the session might time out when the UPGRADE occurs, because the CSG code cannot parse the encrypted data after TLS negotiation.
  - For an HTTP transaction, if any quota is granted, the CSG always sends the following packets, even if there is insufficient quota:

    - The first request (GET, POST, any other method) from the client—headers plus the part of the message that arrives before quota is granted.

    - The headers plus one packet of the response from the server.
  - For HTTP Layer 7 inspection, the CSG supports up to 65,535 concurrent HTTP TCP connections.
  - Some HTTP Layer 7 methods and content types cause the CSG to invoke Layer 4 processing for the remainder of the TCP connection. For details, see the HTTP compliance exceptions in the "Layer 7 Inspection (accounting type=specific protocol)" section on page D-1.

- For the CSG/Hybrid (that is, the CSG running in hybrid mode, with CatOS on the Supervisor Engine and Cisco IOS on the Multilayer Switch Feature Card (MSFC)):
  - Runs with Cisco IOS Release 12.1(13)E or later and CatOS 7.6.1 or later.
  - Supports only the CSG Release 2.2(3)C2(1) command-line interface (CLI), not the CSG Release 3.1(1)C3(1) CLI.
  - Does not support the **hw-module module** *slot* **reset** command. To reset the CSG/Hybrid, enter the **set module power** [**up** | **down**] *slot* command at the CatOS console.
- When replacing an adjacent device but retaining the same IP address (such that there is a different MAC address but the same IP address as before), you must either enter the **clear module csm** *slot* **connections** command in privileged EXEC mode, or you must recycle the CSG.

Note The **clear module csm** *slot* **connections** command clears all connections for the specified CSM; you cannot use this command to clear selected connections.

- Services configured for **basis second connect** (Connection Duration Billing) are subject to the following restrictions:
  - Service verification is not supported for Connection Duration services.
  - Advice of Charge (AoC) 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 CSG redirects must map to a policy that does not have accounting configured. This is due to the fact that 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:
  - Content idle is not included for non-TCP connections. Therefore, the idle timeout for non-TCP content definitions is restricted to be less than the service idle timeout of any service that includes the non-TCP content definition, and that is configured for **basis second**.
  - The CSG does not allow you to specify weights for Service Duration Billing.

- If the CSG does not have an ARP entry in its ARP cache for the MAC address of a device or firewall, it drops packets received from that device or firewall.
- If you define content with a network mask of 255.255.255.255 or /32 (that is, all subnets), a virtual server is created and the CSG's MAC address is entered as the host's address in the CSG's ARP cache. Because of this, you cannot have hosts directly connected to the CSG, coupled with content with a network mask of 255.255.255.255 or /32 that matches those hosts.
- The CSG does not decrement the time to live (TTL) of an IP packet.
- For Interface Awareness:
  - To enable the CSG to route network-initiated connections correctly, the AAA or NAS must send the downlink_nexthop VSA.
  - All downlink next-hop addresses must be configured as gateways in the CSG's routing table.
  - To avoid routing ambiguity on the uplink (or server VLAN) side of the CSG, next hops must override the CSG's routing table.
  - Table IDs and names are not supported or reported in fixed-format TLVs.
  - If a content definition 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 definitions must handle all traffic from users arriving on a VLAN marked with a table name. The CSG uses the VLAN table name to locate user entries. Therefore, if you want to apply the same contents to multiple tables, you must redefine all of your contents.
  - Configurations with overlapping IP address requirements must use CSG RADIUS proxy or RADIUS endpoint to populate the User Table. RADIUS monitor, user database, and old-style RADIUS proxy and endpoint configuration do not support table names or overlapping IP addresses.
  - To identify a user within a CSG table, the quota server-initiated messages must contain the Extended User Index TLV to identify or trigger action on a user within a CSG table.
  - The CSG supports overlapping subscriber IP addresses, but does not support overlap in interface or gateway configuration. The entities that assign IP addresses to subscribers within the VRF must be aware of all of the restricted addresses which belong to the CSG and to adjacent network devices.
  - Network-initiated connections are routed via the default routing table, unless the RADIUS VSA containing the downlink gateway is present in the initial RADIUS flows.
- For Quota Push, the CSG rejects the Quota Push message if the "Replace current balance" flag is not set in the Granted Quadrans TLV.
- For Tariff Switch:
  - If CSG 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.
  - If a transaction spans multiple tariff switches, but the CSG does not support intermediate records for that protocol, the CSG reports only the most recent tariff switch information.
  - If a transaction is configured for BMA reporting using a fixed-format record, the tariff switch usage information is not reported in the record.

- For Enhanced Radius Proxy, in order for the CSG to act on the optional Quota Server TLV in a Radius Start Accounting message, the referenced quota server must be manually configured prior to receiving the Accounting Start message that contains the TLV.
- In a Home Agent (HA) configuration in which the active CSG is running at 3.1(3)C6(2) and the backup CSG is running at 3.1(3)C5(5) or 3.1(3)C5(4), time-based billing might result in over-charging.
- With the **replicate connection tcp** command configured, when a connection is established or terminated, the active CSG sends a dummy SYN or RST, respectively, to the fault-tolerant VLAN. This is normal operation. The extra packets are not billed and the destination MAC address is unknown, so the packets do not reach the server. The destination MAC address for the dummy SYN or RST frame is structured as follows:

  0x03:*xx*:*yy*:00:*zz*:*zz*

  where:

  - **0x03:*xx*:*yy*** is the Cisco Organizational Unique Identifier (OUI).
  - *zz* is the VLAN of the SYN that initiated the connection.

Installing the Hardware

Note Before you install the CSG into the Catalyst 6000 series switch, make sure the switch meets the hardware and software requirements listed in the *Release Notes for Cisco Content Services Gateway 3.1(3)C6(2)*.

This chapter describes how to install the CSG into the Catalyst 6500 series switch or Cisco 7600 series router, and contains these sections:

Front Panel Description

Figure 2-1 shows the CSG front panel. (The RJ-45 connector is covered by a removable plate.)

Figure 2-1 The CSG Front Panel

Status LED

When the CSG powers up, it initializes various hardware components and communicates with the supervisor engine. The Status LED indicates the supervisor engine operations and the initialization results.

During the normal initialization sequence, the status LED changes from off to red, to orange, and then to green. Table 2-1 describes the Status LED operation.

Table 2-1 Content Services Gateway Status LED

Color	Description
Off	• The module is waiting for the supervisor engine to provide power. • The module is not online. • The module is not receiving power, which could be caused by the following: – Power is not available to the CSG. – Module temperature is over the limit. Enter the **show environment temperature** *mod* command to display the temperature of each of four sensors on the CSG.
Red	• The module is released from reset by the supervisor engine and is booting. • If the boot code fails to execute, the LED stays red after power up.
Orange	• The module is initializing hardware or communicating with the supervisor engine. • A fault occurred during the initialization sequence. • The module has failed to download its Field Programmable Gate Arrays (FPGAs) on power up, but continues with the remainder of the initialization sequence and provides the module online status from the supervisor engine. • The module has not received module online status from the supervisor engine. This problem could be caused by the supervisor engine detecting a failure in an external loopback test that it issued to the CSG.
Green	• The module is operational; the supervisor engine has provided module online status.
Green goes off and stays off	• The module is disabled through the supervisor engine CLI using the following commands: – **config terminal** – **no power enable module** *mod*

RJ-45 Connector

The RJ-45 connector, which is covered by a removable plate, is used to connect a management station device or a test device. This connector is used by field engineers to perform testing and to obtain dump information.

Installing the CSG

The following sections describe how to install the CSG:

Note Before installing the CSG, you must install the Catalyst 6000 series switch or Cisco 7600 series router chassis and at least one supervisor engine. For information on installing the switch chassis, see the *Catalyst 6000 Series Switch Installation Guide,* or the *Cisco 7609 Router Installation Guide*.

Before installing the CSG, make sure that the following items are available:

- Catalyst 6000 series switch or Cisco 7600 series router chassis
- Management station that is available through a Telnet or a console connection to perform configuration tasks

- Flat-blade screwdriver
- Wrist strap or other grounding device
- Antistatic mat or antistatic foam

When you install the CSG, keep the following considerations in mind:

- See the *Cisco 7600 Series Router Module Installation Guide* if you are installing the CSG module into a Cisco 7600 series router.
- All modules, including the supervisor engine (if you have redundant supervisor engines), support hot swapping. You can add, replace, or remove modules without interrupting the system power or causing other software or interfaces to shut down. For more information about hot-swapping modules, see the *Catalyst 6500 Series Switch Module Installation Guide*.

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.**

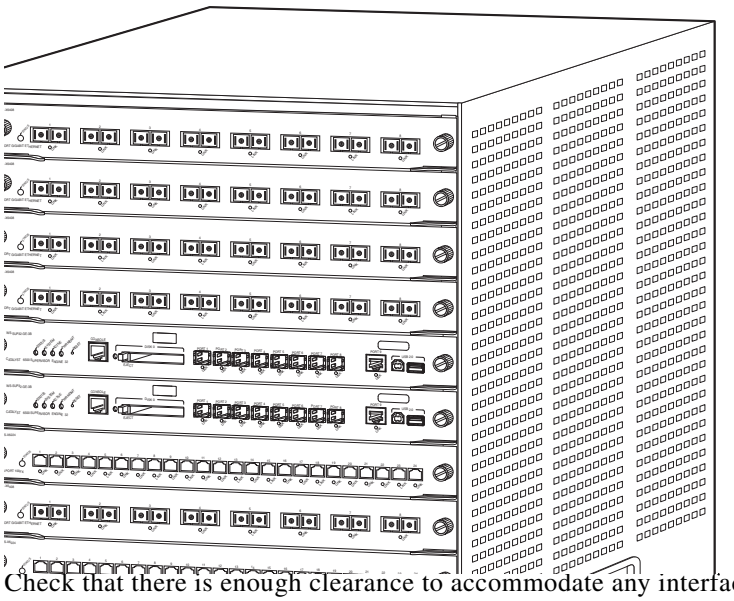
To install the CSG into the Catalyst 6000 series switch, perform these steps:

Step 1 Make sure you take the necessary precautions to prevent ESD damage.

Step 2 Choose a slot for the CSG. See Figure 2-2 for slot numbers on a Catalyst 6000 series switch.

Note Slot 1 is reserved for the supervisor engine. Slot 2 can contain an additional supervisor engine in case the supervisor engine in slot 1 fails. If a redundant supervisor engine is not required, you can insert the CSG in slots 2 through 6 on the 6-slot chassis, slots 2 through 9 on a 9-slot chassis, or slots 2 through 13 on the 13-slot chassis.

Figure 2-2 Slot Numbers on Catalyst 6000 Series Switches



Step 3 Check that there is enough clearance to accommodate any interface equipment that you are connecting directly to the supervisor engine or switching module ports.

Tip If possible, place switching modules between empty slots that contain only switching-module filler plates (Cisco part number 800-00292-01).

Warning **Blank faceplates (filler panels) serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards and faceplates are in place.**

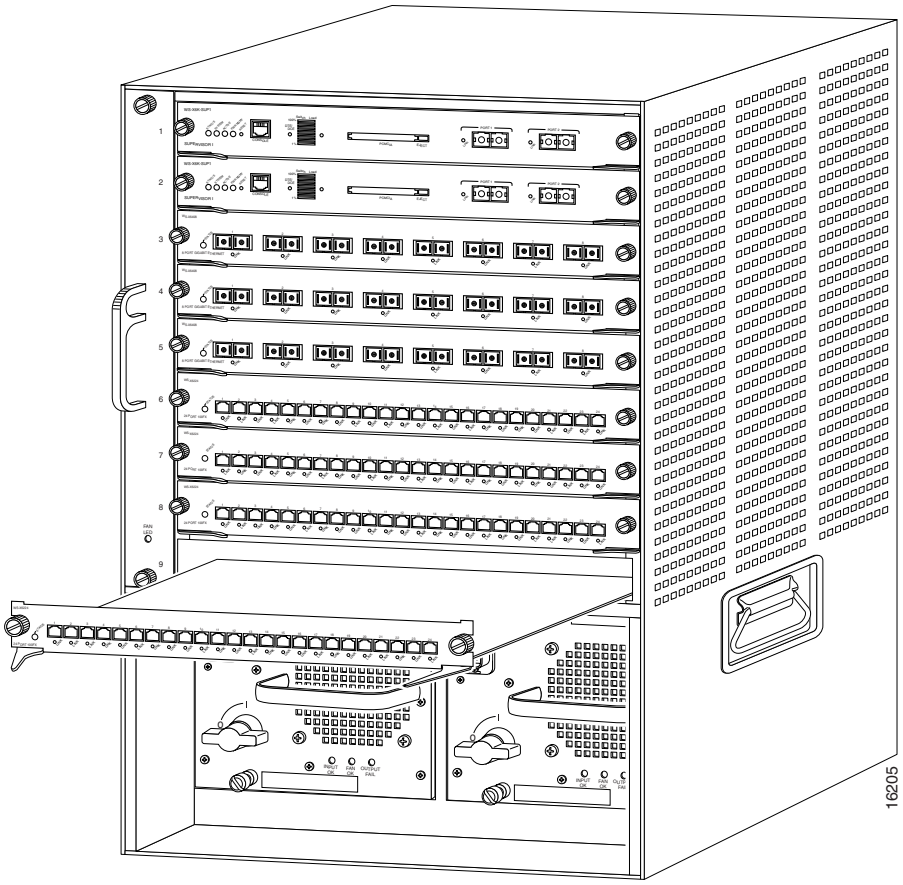
Step 4 Loosen the captive installation screws that secure the switching module filler plate (or an existing switching module) to the desired slot.

Step 5 Remove the switching module filler plate (or an existing switching module).

Step 6 Hold the face of the CSG with one hand, and place your other hand under the carrier support. Do not touch the printed circuit boards or connector pins.

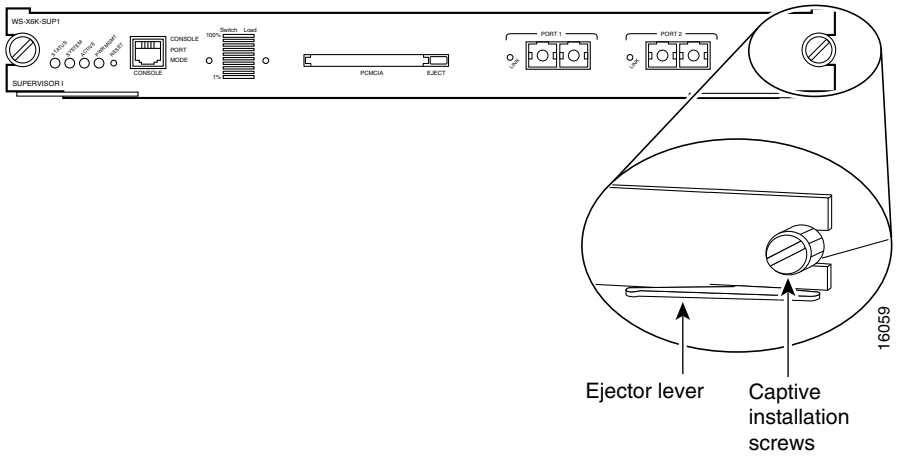
Step 7 Place the CSG in the slot. Align the notch on the sides of the switching module carrier with the groove in the slot. (See Figure 2-3.)

Figure 2-3 Installing Modules in the Catalyst 6000 Series Switch



Step 8 Keep the CSG at a 90-degree angle to the backplane and carefully slide the CSG into the slot until the switching module faceplate contacts the ejector levers. See Figure 2-4.

Figure 2-4 Ejector Levers and Captive Installation Screws



Step 9 Using the thumb and forefinger of each hand, simultaneously push in the left and right levers to fully seat the CSG in the backplane connector.

Caution Always use the ejector levers when installing or removing the CSG. A module that is partially seated in the backplane can cause system problems.

If you perform a hot swap, the console displays the message "Module *n* has been inserted." This message does not appear, however, if you are connected to the Catalyst 6000 series switch through a Telnet session.

Step 10 Use a screwdriver to tighten the captive installation screws on the left and right ends of the CSG.

This completes the CSG installation procedure.

Verifying the Installation

When you install the CSG into the Catalyst 6000 series switch or Cisco 7600 series router, the module goes through a boot sequence that requires no intervention. At the successful conclusion of the boot sequence, the green Status LED lights and remains on. If the Status LED does not show green, or shows a different color, see Table 2-1 on page 2-2 to determine the module's status.

Configuring the Content Services Gateway

This chapter describes how to configure the CSG and contains these sections:

Preparing to Configure the CSG

Before you configure the CSG, take the following actions:

- Make sure that the Cisco IOS version for the switch matches that of the module. You must use Cisco IOS Release 12.1(12c)E4 or later.
- Configure VLANs on the Catalyst 6000 series switch or Cisco 7600 series router *before* you configure VLANs for the CSG. VLAN IDs must be the same for the switch and the module. Refer to the *Catalyst 6000 Series IOS Software Configuration Guide* or the *Cisco 7600 Series Cisco IOS Software Configuration Guide* for details.

  The following example shows how to configure VLANs:

```
Router> enable
Router# vlan database
Router(vlan)# vlan 130
VLAN 130 added:
    Name: VLAN130
Router(vlan)# vlan 150
VLAN 150 added:
    Name: VLAN150
Router(vlan)# exit
```

- Place physical interfaces that connect to the servers and to the clients in the corresponding VLAN.

  The following example shows how to configure a physical interface as a Layer 2 interface and assign it to a VLAN:

```
Router> enable
Router# config
Router(config)# interface 3/1
Router(config-if)# switchport
Router(config-if)# switchport access vlan 150
Router(config-if)# no shutdown
Router(vlan)# exit
```

- If the Multilayer Switch Function Card (MSFC) is used on the next-hop router on either the client-side or the server-side VLAN, then you must configure the corresponding Layer 3 VLAN interface.

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

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

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

Using the CLI

The software interface for the CSG is the Cisco IOS command-line interface (CLI). For more information about using the CLI and Cisco IOS command modes, see Chapter 2 in the *Catalyst 6000 Series IOS Software Configuration Guide*, and Chapter 2 in the *Cisco 7600 Series Cisco IOS Software Configuration Guide.*

Accessing Online Help

In any command mode, you can get a list of available commands by entering a question mark (?) as follows:

```
Router> ?
```

or

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

Online help shows the default configuration values and ranges available to commands.

Upgrading to a New CSG Release

This section describes three methods for upgrading the CSG:

During the upgrade, enter all commands on a console connected to the supervisor engine. Enter each configuration command on a separate line.

Note To complete the upgrade, enter the **exit** command to return to the supervisor engine prompt. If you do not terminate the session, and you remove the CSG from the Catalyst 6000 series chassis, you cannot enter configuration commands to the CSG unless you press **Ctrl** + **^**, enter **x**, and enter the **disconnect** command at the prompt.

The CSG can run in hybrid mode, with CatOS on the Supervisor Engine and Cisco IOS on the MSFC. In the CSG/Hybrid, you can only upgrade the CSG from the MSFC. To enter the MSFC console from CatOS, enter **switch console**. After you enter the MSFC console, you can configure the CSG the same as in native mode. To exit from the MSFC console, enter **^C** three times.

In a redundant MSFC configuration, you cannot upgrade older versions of the CSG from the MSFC in slot 2 with the keyword **slot0:**. To work around this problem, you can either upgrade from the MSFC in slot 1, or you can upgrade with IP address 127.0.0.22.

Upgrading from the Supervisor Engine Bootflash

For instructions on loading images into bootflash, see the *Catalyst 6000 Family Flash Card Install Note* or the *Cisco 7600 Series Cisco IOS Software Configuration Guide*.

To upgrade the CSG from the supervisor engine bootflash, perform these steps:

Step 1 Enable the TFTP server to supply the image from bootflash:

```
Router> enable
Router# configure terminal
Router(config)# tftp-server bootflash:name
```

where *name* is the CSG image name, such as c6csg-apc.31-3.c6.2.

Step 2 Set up a session between the supervisor engine and the CSG:

```
Router# session slot slot-number processor 0
```

where *slot-number* is the slot number for the CSG to be upgraded.

Step 3 Load the image from the supervisor engine to the CSG:

```
CSM# upgrade 127.0.0.yz name
```

where:

- *y* is the slot number—**1** for slot 1, **2** for slot 2, and so on.
- *z* identifies the Supervisor Engine—**1** for Supervisor Engine 720, **2** for Supervisor Engine 32.
- *name* is the CSG2 image name, such as c6csg-apc.31-3.c7.1.

Step 4 Reboot the CSG by turning it off, then back on, or by entering the following command on the supervisor engine console:

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

where *slot-number* is the slot number for the CSG that has been upgraded.

Upgrading from a Flash PC Card

To upgrade the CSG from a removable Flash PC card inserted in the supervisor engine, perform these steps:

Step 1 Enable the TFTP server to supply the image from the removable Flash PC card:

```
Router> enable
Router# configure terminal
Router(config)# tftp-server slotx:name
```

where:

- *x* is the slot number for the CSG2 that you want to upgrade.
- *name* is the CSG2 image name, such as c6csg-apc.31-3.c7.1.

Step 2 Set up a session between the supervisor engine and the CSG:

```
Router# session slot slot-number processor 0
```

where *slot-number* is the slot number for the CSG to be upgraded.

Step 3 Load the image from the supervisor engine to the CSG:

```
CSM# upgrade 127.0.0.yz name
```

where:

- *y* is the slot number—**1** for slot 1, **2** for slot 2, and so on.
- *z* identifies the Supervisor Engine—**1** for Supervisor Engine 720, **2** for Supervisor Engine 32.
- *name* is the CSG2 image name, such as c6csg-apc.31-3.c7.1.

Step 4 Reboot the CSG by turning it off then back on, or by entering the following commands on the supervisor engine console:

```
Router# configure terminal
Router# hw-module module slot-number reset
```

where:

- *slot-number* is the slot number for the CSG that has been upgraded.

Upgrading from an External TFTP Server

To upgrade the CSG from an external TFTP server, perform these steps:

Step 1 Create a VLAN on the supervisor engine for the TFTP CSG runtime image download.

Note You can use an existing VLAN. However, for a reliable download, we recommend that you create a VLAN specifically for the TFTP connection.

Step 2 Configure the interface that is connected to your TFTP server.

Step 3 Add the interface to the VLAN.

Step 4 Enter the CSG **vlan** command. See the *"Configuring VLANs" section on page 3-37* for more information.

Step 5 Add an IP address to the VLAN for the CSG.

Step 6 (Optional) Add a route to the TFTP server for the CSG, if necessary.

Step 7 Enter the **show csg** *slot* **vlan detail** command to verify your configuration. See the *"Configuring VLANs" section on page 3-37* for more information.

Step 8 Make a Telnet connection into the CSG with the **session** *slot-number* **0** command.

Step 9 Upgrade the image using the **upgrade** *TFTP-server-IP-address* **c6csg-apc.***revision***.bin** command, where *revision* is **31-3.c6.2** if you are using the CSG 3.1(3)C6(2).

Step 10 Reboot the CSG.

For the CSG/Hybrid, you must enable the VLAN for the CSG from the CatOS console. To do so, enter the following command:

set vlan *vlan-list*

To add a VLAN:

set trunk *slot*/**1** *vlan-list*

To reset a VLAN:

clear trunk *slot*/**1** *vlan-list*

Upgrading from CSG 3.1(3)C5(5) to the CSG 3.1(3)C6(2)

The CSG 3.1(3)C6(2) requires one of the following supervisor engines running Cisco IOS Release 12.2(18)SXE:

- Supervisor Engine 2 with an MSFC2 (SUP2-MSFC2)
- Supervisor Engine 720 with an MSFC3-BXL (SUP720-MSFC3-BXL)

The CSG 3.1(3)C6(2) does not support Cisco IOS Releases 12.2(17d)SXB, 12.2(17d)SXB1, and 12.2(18)SXD. Therefore, you must upgrade to a supervisor engine running Cisco IOS Release 12.2(18)SXE, either before you upgrade the CSG or at the same time.

Even if you keep your existing configuration and you do not enable any new CSG 3.1(3)C6(2) features, you must be aware of the following differences between the CSG 3.1(3)C6(2) and CSG 3.1(3)C5(5):

- All new CSG 3.1(3)C6(2) TLVs are optional. They cause no backward compatibility issues with entities that support previous releases of the interface, provided those entities ignore unrecognized TLVs and messages.

Performing a Hitless Upgrade

A hitless upgrade allows you to upgrade to a new version without any major service disruption due to the downtime for the upgrade. To perform a hitless upgrade, perform these steps:

Step 1 Perform a write memory on standby.

Step 2 Upgrade the standby system with the new release, and then reboot the CSG. The standby CSG boots as standby with the new release.

Step 3 After rebooting, wait for all of the information to propagate to the standby. Be aware that it might take up to an hour for this process to complete.

Step 4 Upgrade the active CSG with the new release, and then reboot the active CSG. When the active CSG reboots, the standby CSG becomes the new active CSG and takes over the service responsibility.

The rebooted CSG comes up as standby.

Saving and Restoring Configurations

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

Configuring the CSG

This section identifies the tasks you must perform before you can use the content billing feature on the CSG. It provides information on the following topics:

Other Configuration Tasks

This section provides information on the following topics

Specifying CSG Locations

Before you can enter CSG configuration commands on the switch, you must specify the CSG that you want to configure.

To specify the slot number of a CSG in module CSG configuration mode, perform this task:

	Command	Purpose
Step 1	`Router# config t`	Enters configuration mode.
Step 2	`Router(config)# module csg` *slot-number*	Enters module CSG configuration mode for a specified slot.

The **module csg** command places you in module CSG configuration mode. All further configuration commands that you enter apply to the CSG installed in the slot you have specified.

Note Unless otherwise specified, all the examples in this publication assume that you have already entered this command and entered the configuration mode for the CSG you are configuring.

Configuring User Groups

To configure the CSG to record and generate accounting records, you must specify the user groups you want to generate accounting records for, as well as the user database that the CSG queries for user IDs.

To configure user groups on the CSG; to specify the user database, RADIUS endpoint, and quota servers; and to configure redirect NAT, perform the following steps:

	Command	Purpose
Step 1	`Router(config)# ip csg user-group` *group-name*	Defines a CSG user group and specifies a user database name.
Step 2	`Router(config-csg-group)# database` *ip-address port-number*	Specifies the location of the user database, including the IP address and port number of the user database.
Step 3	`Router(config-csg-group)# entries max` *entries-number*	(Optional) Defines the maximum number of entries in the CSG User Table.
Step 4	`Router(config-csg-group)# quota local-port` *port-number*	(Optional) Configures the local port on which the CSG receives communications from quota servers.
Step 5	`Router(config-csg-group)# quota server` {*ip-address port-number priority* | **reassign**}	(Optional) Configures the quota servers that return billing quota values for users. **Note** The CSG does not support multiple quota servers with the same IP address.

	Command	Purpose
Step 6	`Router(config-csg-group)# quota activate number`	(Optional) Allows load balancing of quota servers, similar to the BMA load balancing feature. Multiple quota servers can be simultaneously active, and the CSG assigns a quota server to each user. All quota transactions for the user are done with the same quota server. When a quota server fails, all users associated with that quota server are distributed among other quota servers. The valid range for the *number* argument is 1 through 10. **Note** Multiple quota servers cannot have the same IP address.
Step 7	`Router(config-csg-group)# radius acct-port port-number`	Specifies the port number for the RADIUS accounting endpoint.
Step 8	`Router(config-csg-group)# radius handoff [duration]`	(Optional) Configures RADIUS handoff support.
Step 9	`Router(config-csg-group)# radius key secret`	Configures the CSG to be the RADIUS endpoint for accounting records, and provides the key.
Step 10	`Router(config-csg-group)# radius parse strict`	(Optional) Tightens the parsing rules for RADIUS flows.
Step 11	`Router(config-csg-group)# radius pod attribute radius_attribute_number`	(Optional) Specifies the RADIUS attributes to be copied from the RADIUS Start message and sent to the NAS in the Packet of Disconnect (PoD).
Step 12	`Router(config-csg-group)# radius pod nas [start-ip end-ip] port key [encrypt] secret-string`	(Optional) Specifies the NAS port to which the CSG should send the Packet of Disconnect (PoD) message, and the key to use in calculating the Authenticator.
Step 13	`Router(config-csg-group)# radius pod timeout timeout retransmit retransmit`	(Optional) Specifies the number of times to retry the RADIUS Packet of Disconnect (PoD) message if it is not ACKed, and the interval between retransmissions.
Step 14	`Router(config-csg-group)# radius server ip-address [port-number]`	(Optional) Enables RADIUS proxy.
Step 15	`Router(config-csg-group)# radius userid {1 | 31 | User-Name | Calling-Station-Id}`	(Optional) RADIUS attribute used to extract the user IDs from a RADIUS record.
Step 16	`Router(config-csg-group)# radius start restart session-id {attr_number | {26 | vsa} {vendor_id | 3gpp} sub-attr_number}`	(Optional) Deletes an existing User Table entry for a specific user (when a RADIUS Accounting Start is received), and creates a new entry for that user (similar to when a RADIUS Accounting Stop has been received).
Step 17	`Router(config-csg-group)# radius stop purge {attr_number | {26 | vsa} {vendor_id | 3gpp} sub-attr_number}`	(Optional) Specifies the attribute (which might be a vendor-specific attribute) that must be included in the RADIUS Accounting Stop request in order for the User Table entry to be deleted.
Step 18	`Router(config-csg-group)# radius monitor server_addr server_port [key [encrypt] secret-string]`	Specifies that the CSG should monitor the RADIUS flows to the specified server.
Step 19	`Router(config-csg-group)# redirect nat ip-address [port-number]`	(Optional) Redirects client NAT flows to an alternate IP address when the client's quota is exhausted.
Step 20	`Router(config-csg-group)# redirect http url`	(Optional) Redirects client HTTP flows to an alternate URL when the client's quota is exhausted.
Step 21	`Router(config-csg-group)# redirect wap url`	(Optional) Redirects client WAP flows to an alternate URL when the client's quota is exhausted.

	Command	Purpose
Step 22	`Router(config-csg-group)# aoc confirmation`	Configures a token for use in advice of charge (AoC) URL-rewriting.
Step 23	`Router(config-csg-group)# user-profile server {quota | radius {remove | pass}}`	(Optional) Specifies which server is used to obtain the user profile or billing plan. **Note** The VSA is removed from the Access-Accept message only if **remove** is specified. We recommend that you use **pass** to reduce processing time on the CSG. You should use **remove** only if the RADIUS client cannot tolerate the Cisco VSA in the message. Additionally, the user ID must be in the message containing the billing plan.

The following example shows how to configure a CSG user group, including a database, a RADIUS endpoint, quota servers, and redirect NAT:

```
ip csg user-group G1
 entries max 100000
 database 10.1.2.3 11111
 quota local-port 6666
 quota server 10.1.4.5 888 1
 quota server 10.1.6.7 999 2
 radius acct-port 7777
 radius key SECRET_PASSWORD
 radius parse strict
 radius server 10.13.14.15
 radius userid User-Name
 redirect nat 10.33.33.3
!
ip csg user-group U1
 radius userid User-Name
 radius monitor 10.2.3.4 1234 key cisco
 radius monitor 10.2.3.9 1234 key cisco2
 radius monitor 10.2.7.4 3901 key cisco
```

Configuring Accounting Policies

To configure the CSG to record and generate accounting records, you must define content-based client accounting as a service. This includes specifying the user groups you want to generate accounting records for, as well as the Billing Mediation Agent to send accounting records to.

To configure the accounting policies on the CSG, perform the following steps:

	Command	Purpose
Step 1	`Router(config)# ip csg accounting` *name*	Defines content-based client accounting as a policy.
Step 2	`Router(config-csg-accounting)# user-group` *name*	Associates a user group with a specific accounting service.

	Command	Purpose
Step 3	`Router(config-csg-accounting)# agent ip-address port-number priority`	Defines the primary and backup Billing Mediation Agents (BMAs) to which billing records are to be sent. **Note** The CSG does not support multiple agents with the same IP address.
Step 4	`Router(config-csg-accounting)# agent activate [number [sticky seconds]]`	(Optional) Enables support for multiple active BMAs
Step 5	`Router(config-csg-accounting)# agent local-port port-number`	(Optional) Defines the port on which the CSG is to listen for packets from the BMAs.
Step 6	`Router(config-csg-accounting)# keepalive number-of-seconds`	(Optional) Defines the keepalive time interval (in seconds) used to test the health of BMAs.
Step 7	`Router(config-csg-accounting)# records batch`	(Optional) Batches billing records into a single message before sending them to the BMA.
Step 8	`Router(config-csg-accounting)# records http-statistics`	(Optional) Sends the HTTP Statistics data record to the BMA.
Step 9	`Router(config-csg-accounting)# records intermediate {bytes bytes | time seconds | bytes bytes time seconds}`	(Optional) Enables the generation of intermediate billing records.
Step 10	`Router(config-csg-accounting)# records max`	(Optional) Defines the maximum number of billing records that can be stored or queued in the CSG before they are forwarded to the Billing Mediation Agent (BMA).
Step 11	`Router(config-csg-accounting)# records format`	(Optional) Specifies variable, fixed, or variable-single CDR format.
Step 12	`Router(config-csg-accounting)# record-storage ip-address [port]`	(Optional) Defines a PSD to associate with this accounting group.
Step 13	`Router(config-csg-accounting)# record-storage local-port port`	(Optional) Defines the source port to be used by the CSG when communicating with the record store.
Step 14	`Router(config-csg-accounting)# report http header header_name`	(Optional) Defines the inclusion of multiple HTTP request headers in the CSG HTTP_Header CDR.
Step 15	`Router(config-csg-accounting)# report radius attribute radius_attribute_number`	(Optional) Specifies the RADIUS attributes to be copied from the RADIUS Start message and sent to the BMA in each billing record.
Step 16	`Router(config-csg-accounting)# report usage {bytes ip | seconds}`	(Optional) Enables supplemental usage reporting.
Step 17	`Router(config-csg-accounting)# inservice`	Activates the accounting service on a CSG.

Step 18	`Router# show module csg slot accounting {agent | database | error | quota-server | radius | users {all | statistics | ip-address [ipmask] | userid userid}} [detail] [module num]`
	or
	`Router# show ip csg accounting {agent | database | error | quota-server | radius | users {all | statistics | ip-address [ipmask] | userid userid}} [detail] [module num]`
		Displays information for the CSG billing feature.

The following example shows how to define the CSG accounting policy:

```
ip csg accounting A1
 user-group G1
 agent activate 2
 agent local-port 3775
 agent 10.1.2.4 11112 1
 agent 10.1.2.5 11113 2
 keepalive 3
 records batch
 records http-statistics
 records intermediate bytes 100000 time 3600
 records max 250
 record-storage local-port 5002
 record-storage 172.18.12.226
 report http header x-subno
 report http header x-al-session-id
 report radius attribute 3
 report radius attribute 5
 inservice
```

Activating the Accounting Policy on the CSG

To activate the accounting policy on the CSG, enter the following command in module CSG configuration mode:

Command	Purpose
`Router(config-csg-module)# accounting service-name`	Downloads a configured accounting service to a CSG card.

Defining Client/Server Connectivity

To properly configure the CSG, you must create VLANs for both the client side and server side of the switch. You must do this so that the CSG knows where to forward the traffic it receives. The minimal configuration requires one client-side VLAN and one server-side VLAN. Additionally, you must configure IP addresses for the VLANs, and all gateway IP addresses.

To configure server-side VLANs on the CSG, enter the following command in module CSG configuration mode:

Command	Purpose
`Router(config-csg-module)# vlan vlan-id server [vlan-name]`	Configures the server-side VLANs and enters the server VLAN mode. **Note** You cannot use VLAN 1 as a server-side VLAN for the CSG.

Then configure an IP address on this VLAN.

To configure client-side VLANs on the CSG, enter the following commands, beginning in module CSG configuration mode:

Command	Purpose
`Router(config-csg-module)# vlan vlan-id client [vlan-name]`	Configures the client-side VLANs and enters the client VLAN mode. **Note** You cannot use VLAN 1 as a client-side VLAN for the CSG.

Then configure an IP address on this VLAN.

The following example shows how to configure client and server VLANs:

```
vlan 10 server
 ip address 10.250.0.1 255.255.0.0
 gateway 10.250.1.1

vlan 251 client
 ip address 10.251.0.1 255.255.0.0
 route 10.200.0.0 255.254.0.0 gateway 10.251.2.11
```

Downloading an Accounting Service

Before you can configure the CSG to perform content billing, you must enable it to reference and download a specific accounting service configuration.

To install the accounting service in a specific CSG, enter the following command in module CSG configuration mode:

Command	Purpose
`Router(config-csg-module)# accounting service-name`	Assigns a specific accounting service to a specific CSG.

Downloading Ruleset Content

A CSG billing ruleset is a list of all content names that are to be downloaded to a specific CSG card.

To download all content defined by a ruleset to a CSG card, enter the following command in module CSG configuration mode:

Command	Purpose
`Router(config-csg-module)# ruleset ruleset-name`	Downloads all content defined by a ruleset to a CSG card.

Configuring Policies and Traffic Types

Policies are access rules that traffic must match for a server farm. Policies allow the CSG to apply filters to certain types of traffic subject to the accounting service.

When the CSG is able to match 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 correct order.

To configure accounting records policies in module CSG configuration mode, perform this task:

	Command	Purpose
Step 1	`Router(config-csg-module)# ip csg policy policy-name`	Defines a policy for qualifying flows for CSG accounting services, and enters CSG policy configuration mode.
Step 2	`Router(config-csg-policy)# accounting [type {http | ftp | wap {connection-oriented | connectionless} | rtsp | ftp | smtp | pop3 | other}] [customer-string string]`	Defines the accounting type and customer string for all flows that comply with a CSG billing policy.
Step 3	`Router(config-csg-policy)# client-group {std-access-list-number | std-access-list-name}`	References a standard access list that is part of a CSG billing policy.
Step 4	`Router(config-cag-policy)# client-ip http-header x-forwarded-for`	Specifies that the user's IP address is to be obtained from the URL header after the **x-forwarded-for** keyword.
Step 5	`Router(config-cag-policy)# header-map header-map-name`	References a header map that is part of a CSG billing policy.
Step 6	`Router(config-cag-policy)# next-hop ip-address`	Defines a next-hop IP address.
Step 7	`Router(config-cag-policy)# url-map url-map-name`	References a URL map that is part of a CSG billing policy.

The following example shows how to define a policy:

```
ip csg policy MOVIES_COMEDY
 accounting type http customer-string MOVIES_COMEDY
 client-group 44
 client-ip http-header x-forwarded-for
 header-map MOVIES
 next-hop 33.0.0.150
 url-map MOVIES
```

Configuring a Content Billing Service

A CSG content billing service is a component of a billing plan that is subscribed to by users.

You can configure one or more content billing services for the CSG. 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 user's quota. Grouping content into one or more services enables you to separate, for example, a user's prepaid quota for Internet browsing from his quota for e-mails.

For each service, the CSG downloads a separate quota, and deducts from that quota. Quotas are specified in units called *quadrans*. A quadran is a generic unit whose exact "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), and a byte for a per-volume service. The value of a quadran is transparent to the CSG; it simply requests and downloads quadrans as needed from quota servers.

The CSG requests an additional quota grant when a user's per-click quota falls below a specified percentage of the last quota grant, or when a user'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 user tries to access, the CSG maintains a separate logical accounting session. When a user's quota is divided among multiple services, the CSG requests an additional quota grant for each service individually, based on its usage.

If a user fails authorization for a service, but continues to send new requests for that service, the CSG waits a specified time before sending a reauthorization request for that user to the quota server. This ensures that the quota server is not inundated with reauthorization requests from unauthorized users.

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.
- The **exclude mms** option specifies that MMS content over WAP is not billed.

To configure a content billing service, perform this task:

	Command	Purpose
Step 1	`Router(config-csg-module)# ip csg service` *service-name*	Defines a content billing service, and enters CSG service configuration mode.
Step 2	`Router(config-csg-service)# content` *content-name* `policy` *policy-name* `[weight` *weight-name*`]`	Defines content as a member of a CSG billing service, identifies a policy to apply to this content, and optionally assigns a weight to this content.
Step 3	`Router(config-csg-service)# basis {byte {ip | tcp} | {fixed | second [connect] [exclude mms]}`	(Optional) Specifies the billing basis for a CSG content billing service. **Note** When changing the basis for a service, the content must be taken out of service.
Step 4	`Router(config-csg-service)# idle` *duration*	(Optional) Specifies the minimum amount of time that the CSG maintains a service with no user sessions.

The CSG allows you to define a pool of up to 255 services. You can authorize each user for any number of services from that pool, but we recommend that the billing system not authorize each user for more than 10 active services. Exceeding this guideline could lead to the following problems:

- The increase in the number of quota authorizations per user can overload the quota server, as well as the CSG.
- As the number of services for which a user is actively authorized increases, the user's quota becomes fragmented. Although the CSG allows the billing system to recall and redistribute the quota, so that the user is not denied service due to quota fragmentation, the process increases overhead in both the quota server and the CSG.

The following example shows how to define a content billing service:

```
ip csg service MOVIES
 basis fixed
 content MOVIES_COMEDY policy MOVIES_COMEDY
 content MOVIES_ACTION policy MOVIES_ACTION weight DOUBLE
 idle 120
```

Configuring Content

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

A CSG content specification 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 UDP port numbers.

If the content specification does not match any service listed under a user's billing plan, the CSG considers the service to be either free or postpaid. The CSG does not try to authorize the user with the quota server for the service.

To specify content for a CSG accounting service, perform the following tasks, beginning in module CSG configuration mode:

	Command	Purpose
Step 1	`Router(config-csg-module)# ip csg content` *content-name*	Defines content for CSG accounting services, and enters CSG content configuration mode.
Step 2	`Router(config-csg-content)# policy` *policy-name*	References a CSG billing policy.
Step 3	`Router(config-csg-content)# ip {any | ip-address [netmask]} [protocol [port-number last-port-number]]`	Defines the Layer 3/Layer 4 subset of flows that can be processed by the CSG accounting services. You can define *port-number* as a single value or a range of numbers.
Step 4	`Router(config-csg-content)# client [include | exclude] {any | ip-address [netmask]`	(Optional) Defines the client IP address spaces that can use the CSG content server.
Step 5	`Router(config-csg-content)# idle` *duration*	(Optional) Specifies the minimum amount of time the CSG maintains an idle content connection.
Step 6	`Router(config-csg-content)# pending` *timeout*	(Optional) Sets the pending connection timeout.
Step 7	`Router(config-csg-content)# replicate connection tcp`	(Optional) Replicates the connection state for all TCP connections to the CSG content servers on the backup system.

	Command	Purpose
Step 8	`Router(config-csg-content)# vlan vlan-name`	(Optional) Restricts CSG billing content to a single source VLAN.
Step 9	`Router(config-csg-content)# inservice`	Activates the content service on each CSG.
Step 10	`Router # show module csg slot content [name content-name] [detail]`	Displays statistics and counters for CSG content.

The following example shows how to define content for a CSG accounting service:

```
ip csg content MOVIES_COMEDY
 policy POLICY1
 client 10.4.4.0 255.255.255.0
 idle 120
 ip 172.18.45.0/24 tcp 8080
 pending 300
 replicate connection tcp
 vlan MOVIES_COMEDY
 inservice
```

The following example shows how to define a range of port numbers:

```
ip csg content MULTI_PORT
 policy WAP_SRV_POLICY
 ip any udp 30000 30150
 inservice
```

Configuring Fixed or Variable Format CDR Support

The CSG supports both variable and fixed format CDR generation, including a fixed variable format for WAP CDRs. The same set of variables are reported in each CDR regardless of WSP 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. To configure a specific format, perform the following tasks:

	Command	Purpose
Step 1	`Router(config)# ip csg accounting records format [variable | fixed | variable-single-cdr]`	Specifies variable, fixed, or variable single CDR format.
Step 2	`Router(config)# module csg 3 hostname MYHOST`	Specifies a variable hostname for a CSG module
Step 3	`Router(config)# ip csg billing FOO mode postpaid service X service Y`	Specifies that a billing plan is postpaid or prepaid.
Step 4	`Router(config)# ip csg service FOO owner name ABC_CORP owner id ABC123456`	Specifies the owner responsible for the content associated with a 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.

	Command	Purpose
Step 5	`Router(config)# ip csg service FOO` `class 7`	Specifies a service class value.

Step 6	`Router(config)# ip csg transport-type`
	`assign 1.2.3.4 6`
	`assign 2.5.3.1 7`
	`assign 6.6.7.5 0`
		Classifies data traffic based on its access path using the NAS-IP reported in RADIUS. Use the **assign** command to associate IP addresses with transport-type values. Transport-type information is reported in fixed record format CDRs.

Configuring a Refund Policy on the CSG

The prepaid error reimbursement feature allows the CSG to automatically refund quota for failed transactions, as defined by the CLI. The CSG checks them in the following order: TCP/WAP flags, ApplicationReturnCode.

Note If refund is enabled for a CSG prepaid service, you cannot download more than 0x6FFFFFFF bytes of data in a given transaction.

To configure a refund policy on the CSG, perform the following tasks:

	Command	Purpose
Step 1	`Router(config)# ip csg refund`	Specifies a refund policy that can then be applied to the various services, and enters CSG refund configuration mode.

Step 2	`Router(config)# ip csg refund COMPANY-REFUND`
	`retcode http 500 509`
	`retcode wap 0x44 0x50`
	`retcode ftp 454`
		Specifies the range of application return codes for which the CSG refunds quota.

Step 3	`Router(config)# ip csg refund COMPANY-REFUND`
	`retcode http 500 509`
	`retcode wap 0x44 0x50`
	`retcode ftp 454`
	`flags tcp 43 00`
	`flags tcp 63 01`
	`flags tcp 80 80`
	`flags ip 80 80`
	`flags wap 0 8`
		Specifies a mask of interesting TCP, IP, or WAP flag bits and values for which the CSG refunds quota.

The following example shows how to configure a refund policy on the CSG:

```
ip csg refund COMPANY-REFUND
  retcode http 500 509
  retcode wap 0x44 0x50
  retcode ftp 454
  flags tcp FF 14
  flags wap FF 08
```

To enable and specify the refunding policy for a CSG prepaid service, specify the following command in CSG service configuration mode:

	Command	Purpose
Step 1	`Router(config-csg-service)# refund-policy` *policy-name*	Enables and specifies the refunding policy for a CSG prepaid service.

The following example shows how to configure the **refund-policy** command:

```
ip csg service BILLPERCLICK
  basis fixed
  refund-policy COMPANY-REFUND
  content ADVERTISEMENTS policy ADVERTISEMENTS weight PAYBACK
  content BOOKS policy BOOKSALES
  content BOOKS policy BOOKFREE weight FREE
  content CORPORATE policy CORPORATE weight FREE
!
ip csg service BILLBYVOLUME
  basis byte tcp
  refund-policy COMPANY-REFUND
  content BILLBYVOLUME policy BILLBYVOLUME
!
ip csg service BILLBYIPVOLUME
  basis byte
  refund-policy COMPANY-REFUND
  content INTERNET policy INTERNET
```

Configuring RADIUS Accounting Attribute Reporting

The CSG allows you to configure a list of RADIUS accounting attributes that are to be reported to the BMA and quota server in every CDR. To configure these attributes using their standard numbers, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip csg accounting` *name*	Defines content-based client accounting as a service, and enters CSG accounting configuration mode.
Step 2	`Router(config-csg-accounting)# report radius attribute 3`	Defines which attributes you want to report.

You can specify as many attributes as you desire. The attributes are copied from the RADIUS accounting message and sent in each billing message to the BMA.

Note The CSG examines only the standard RADIUS attribute number. The CSG is not aware of any special formatting or subclassing for Vendor-Specific Attributes (VSAs). If a VSA is desired, then the CSG reports all VSAs (attribute 26).

If the list of configured attributes changes, only new RADIUS requests are subject to the new attributes. Attributes already saved for a user continue to be reported.

When a RADIUS start request is received, any attributes received from a previous start request are deleted. If there are multiple instances of an attribute, they are all reported. Attributes are reported in the order they exist in the RADIUS message.

The following example shows how to define multiple RADIUS attributes:

```
Router(config)# ip csg accounting a1
Router(config-csg-accounting)# report radius attribute 3
Router(config-csg-accounting)# report radius attribute 5
Router(config-csg-accounting)# report radius attribute 7
Router(config-csg-accounting)# report radius attribute 44
```

Configuring RADIUS Proxy

The RADIUS proxy feature lets you specify that the CSG should be a proxy for RADIUS messages. To configure the RADIUS proxy feature, enter the following command in module CSG configuration mode:

Command	Purpose
`Router(config-csg-module)# radius proxy` *csg_addr server addr* [*csg_source_addr*] [**key** [*encrypt*] *secret-string*] [**table** *table-name*]	Specifies that the CSG should be a proxy for RADIUS messages.

Note If you specify the **user-profile server radius remove** command, you might also need to configure a key.

Configuring RADIUS Endpoint

To configure the CSG as a RADIUS Accounting endpoint, enter the following command in module CSG configuration mode:

Command	Purpose
`Router(config-csg-module)# radius endpoint` *csg_addr* **key** [*encrypt*] *secret-string* [**table** *table-name*]	Identifies the CSG as an endpoint for RADIUS Accounting messages.

Configuring HTTP Header Reporting

The CSG allows you to include multiple HTTP request headers in the CSG HTTP_Header CDR. To define HTTP reporting on the CSG, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip csg accounting` *name*	Defines content-based client accounting as a service, and enters CSG accounting configuration mode.
Step 2	`Router(config-csg-accounting)# report http header` *x_header*	Defines the inclusion of multiple HTTP request headers in the CSG HTTP_Header CDR. You can specify any number of headers up to 256, and header names cannot exceed 224 characters.

The following example shows how to enable HTTP header reporting for virtual server VS1:

```
Router(config)# ip csg accounting a1
```

```
report http header x-subno
report http header x-al-session-id
```

Configuring a Ruleset

A CSG billing ruleset is a list of all content names that are to be downloaded to a specific CSG card.

To define a ruleset for CSG billing, perform this task:

	Command	Purpose
Step 1	`Router(config-csg-module)# ip csg ruleset` *ruleset-name*	Configures a CSG billing ruleset, and enters CSG ruleset configuration mode.
Step 2	`Router(config-csg-ruleset)# content` *content-name*	Adds a content reference to a CSG ruleset.

If you have defined more than one content name using multiple **ip csg content** commands, you can configure more than one **content** command in CSG ruleset configuration mode.The following example shows how to define a CSG billing ruleset:

```
ip csg ruleset R1
 content MOVIES_COMEDY
 content MOVIES_ACTION
```

Configuring Maps for Pattern-Matching

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

To define the CSG billing content filters (URL maps and header maps), perform this task:

	Command	Purpose
Step 1	`Router(config-csg-module)# ip csg map` *map-name* {**url** | **header**}	Defines the CSG billing content filters (URL maps and header maps), and enters CSG map configuration mode.
Step 2	`Router(config-csg-map-header)# match protocol` *protocol* **header** *header-name* [**value** *pattern*]	Specifies a header match pattern for a CSG billing map.
Step 3	`Router(config-csg-map-url)# match protocol` *protocol* [**method** *method*] **url** *pattern*	Specifies a URL match pattern for a CSG billing map.

Note For WAP, the CSG supports URL maps, but not header maps.

Header Maps

You can specify more than one **match** command in CSG header map configuration mode to specify multiple header match expressions for a given header map:

- 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 value www.cisco.com
   match header User-Agent valuemyagent
  ```

  But the following is not a valid configuration, because both **match header** commands reference header **Host**:

  ```
  ip csg map HDR1
   match header Host valuewww.cisco.com
   match header Host valuemy.cisco.com
  ```

- If the header matches *all* of the header match expressions, then the match is TRUE and the flows can be processed by the CSG accounting services (unless there is another map associated with this policy that is FALSE).
- If the header *does not* match *even one* of the header match expressions, then the match is FALSE and the flows are not processed by the CSG accounting services, even if other maps for this policy match TRUE.
- The CSG 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. The more wildcard matches you use, the fewer header maps and header match patterns the CSG can handle, depending on your configuration. Therefore, to optimize the performance of the CSG, minimize the number of header match patterns that are applied to a CSG content configuration, and minimize the number of wildcards used in header match patterns.
- The header match expressions are case-sensitive. For example, if you define the following header match expression:

  match header host1 value *.2.*.44

  but the actual HTTP header keyword is **HOST1**, the header *does not* match the header match expression, the match is FALSE, and the flow is not processed by the CSG accounting services.

The following example shows how to specify 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 value www.cisco.com
 match header User-Agent value myagent
```

URL Maps

You can specify more than one **match** command in CSG URL map configuration mode to specify multiple URL match expressions for a given URL map:

- If the URL matches *any* of the URL match expressions, then the match is TRUE and the flows can be processed by the CSG accounting services (unless there is another map associated with this policy that is FALSE).
- If the URL *does not* match any of the URL match expressions, then the match is FALSE and the flows are not processed by the CSG accounting services, even if other maps for this policy match TRUE.
- The URL match expressions are case-sensitive. For example, if you define the following URL match expression:

  match protocol http url http://*url-string*

  but a subscriber enters the following URL in a Web browser:

  HTTP://*url-string*

  the URL *does not* match the URL match expression, the match is FALSE, and the flow is not processed by the CSG accounting services.

  Therefore, consider upper- and lowercase combinations carefully when creating URL match expressions.
- When you configure URL match patterns for RTSP streams, keep in mind that you must 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***.
- Depending on your configuration, the CSG can handle up to 1000 single-wildcard URL match patterns (for example, ***movies** or **movies***, but not ***movies***) or up to 11 double-wildcard URL match patterns (for example, ***movies*** or **http://test.*movies.com/*.mpeg**). Double-wildcard URL match patterns are also known as keyword URL match patterns. If you want to use keyword URL match patterns, keep the following considerations in mind in order to optimize the CSG's performance:
  - Minimize the number of URL match patterns that are applied to a given CSG content definition.
  - 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 pattern.
  - Combine multiple keyword URL match patterns into a single pattern 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 the following 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**

Remember that the entire pattern, including wildcards and UNIX string-matching special characters, cannot exceed 128 characters.

- When adding or changing URL match patterns, check their impact on the CSG's memory:
  1. Enter the **show module csg status** command in privileged EXEC mode to check the status of the configuration change.
  2. When the status changes from PENDING (the change has not yet downloaded) to COMPLETE, SUCCESS (the change has downloaded successfully), enter the **show module csm memory** command in privileged EXEC mode. This command displays the CSG's total memory used versus total memory available.

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**, and for any other URLs that match the pattern:

```
ip csg map MOVIES url
 match url *.movies_(comedy|action|drama).com/*.mpeg
```

Configuring a Symbolic Weight Name

The same weight can occur in multiple rules, specified in multiple billing services. If a weight changes, and you use numeric constants for weights, each occurrence of the weight must be updated. However, if you define symbolic weight names, you need only update a single definition for each weight. The result is a more readable configuration, and price lists that are easier to manage.

The weight-name is referenced in the **content** command in CSG service configuration mode.

To define a symbolic name for a CSG billing weight, perform this task:

Command	Purpose
`Router(config-csg-module)#` **ip csg weight** *weight-name weight-value*	Defines a symbolic name for a CSG billing weight, and enters CSG weight configuration mode.

The following example shows how to define a CSG weight:

```
ip csg weight DOUBLE 2
```

Configuring Advice of Charge, Filtering, and Other Per-Event Authorizations

To configure content authorization, perform this task:

	Command	Purpose
Step 1	`Router(config)#` **ip csg service** *service name*	Defines a content billing service, and enters CSG service configuration mode.
Step 2	`Router(config-csg-service)#` **authorize content**	Instructs the CSG to get authorization from the quota server for each subscriber request for content.

The following example shows how to configure content authorization for the CSG:

```
Router(config)# ip csg service service_name
   authorize content
```

To define the token used for the URL-rewriting feature of AoC, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip csg user-group group name`	Creates a group of end-users for which you want to generate accounting records, and enters CSG user group configuration mode.
Step 2	`Router(config-csg-group)# aoc confirmation token`	Configures a token for use in advice of charge (AoC) URL-rewriting.

The following example shows how to specify a token for AoC URL-rewriting:

```
ip csg user-group A1
    aoc confirmation ?CSG_AOC_OK
```

Configuring Quota Server Load-Sharing

The CSG allows load sharing among quota servers, similar to its BMA load-balancing feature. Multiple quota servers can be simultaneously active, and the CSG assigns a quota server to each user.

To configure quota server load-sharing, perform this task:

	Command	Purpose
Step 1	`Router(config)# ip csg user group` *group name*	Creates a group of end-users for which you want to generate accounting records, and enters CSG user group configuration mode.
Step 2	`Router(config-csg-group)# quota activate` *number*	Assigns a quota server to each user. All quota transactions for the user are done with the same quota server. When a quota server fails, all users associated with that quota server are distributed among other quota servers. The valid range for the *number* argument is 1 through 10.

The following example shows how to define quota server load-sharing:

```
router(config)# ip csg user u1
router(config-csg-group)# quota activate 5
```

Configuring Service-Level CDR Summarization

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

To configure service-level CDR summarization, perform this task:

	Command	Purpose
Step 1	`Router(config-csg-module)# ip csg service` *service-name*	Defines a content billing service, and enters CSG service configuration mode.
Step 2	`Router(config-csg-service)# records granularity {transaction | service {bytes` *bytes* `| time` *seconds* `| bytes` *bytes* `time` *seconds*`}}`	Specifies the granularity at which billing records (CDRs) should be generated. For service-level CDR summarization, specify the **service** keyword.

Note If you specify both **type http** and any other type (**type other**, **type ftp**, **type imap**, and so on) for a service, and you enable service-level CDR summarization for the service, the CSG's incremental and cumulative byte counts are not valid. This is because they are a mix of TCP bytes (for the HTTP traffic) and IP bytes (for all other traffic).

Service-level CDRs are generated only for subscribers with entries in the CSG User Table entry. If a subscriber does not have an entry in the User Table, the CSG generates transaction-level CDRs.

If there are no quota servers configured on the CSG, 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 url
  match protocol http url http://www.nhl.com/*
!
ip csg map MOVIES url
  match protocol http url http://www.hollywood.com/*
!
ip csg policy SPORTS
  accounting type http
  url-map SPORTS
!
ip csg policy MOVIES
  accounting type http
  url-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 byte 128000
!
ip csg billing EVERYBODY
  mode postpaid
  service SPORTS
  service MOVIES
```

Configuring Quota Server Reauthorization

After the CSG receives a grant of zero quadrans in a Service Authorization Response, the CSG waits for an interval of time before it requests quota in a Service Reauthorization Request. To configure the initial minimum interval before the CSG sends a Service Reauthorization Request, perform this task:

	Command	Purpose
Step 1	`Router(config)# module csg` *slot*	Enters module CSG configuration mode for a specified slot.
Step 2	`Router(config-csg-module)# variable CSG_ZERO_QUOTA_TIMEOUT_INIT` *timeout*	Sets the initial timeout for reauthorization after quota grant of zero.

For each consecutive grant of zero quadrans in a Service Authorization Response from the quota server, the CSG doubles the retry timeout. If the quota server grants any value for quota greater than zero in a Service Authorization Response, the CSG uses the initial value for retry interval after the next zero quota grant.

Note Service Authorization messages have a usage of zero for RTSP traffic.

A quota push can provide a zero grant and cause a reauthorization wait of CSG_ZERO_QUOTA_TIMEOUT_INIT.

To configure the maximum retry timeout value, perform the following task:

	Command	Purpose
Step 1	`Router(config)# module csg slot`	Enters module CSG configuration mode for a specified slot.
Step 2	`Router(config-csg-module)# variable CSG_ZERO_QUOTA_TIMEOUT_MAX timeout`	Sets the maximum timeout for reauthorization after quota grant of zero.

Note If the INIT value is greater than the MAX value, the MAX value is used as the minimum retry interval and the INIT value is ignored.

To configure the maximum values for the threshold of available quota for sending a Service Reauthorization Request, perform the following task:

	Command	Purpose
Step 1	`Router(config)# module csg slot`	Enters module CSG configuration mode for a specified slot.
Step 2	`Router(config-csg-module)# variable CSG_BASIS_BYTE_LOW_QUOTA_MAX max_threshold`	Sets the maximum value for the available quota threshold that triggers reauthorization for basis byte.
Step 3	`Router(config-csg-module)# variable CSG_BASIS_FIXED_LOW_QUOTA_MAX max_threshold`	Sets the maximum value for the available quota threshold that triggers reauthorization for basis fixed.

The formula for calculating the reauthorization thresholds are:

- For volume-basis billing, the threshold is the smallest of the following values:
  - CSG_BASIS_BYTE_LOW_QUOTA_MAX
  - last_quota_grant /4
  - 32 KB
- For fixed-basis billing, the threshold is the smallest of the following values:
  - CSG_BASIS_FIXED_LOW_QUOTA_MAX
  - last_quota_grant /4

Protocol-Specific Configuration Details

This section provides information about the following tasks:

Configuring WAP/WSP Support

The CSG 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

The CSG 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 downloaded from destination to source.

Incomplete WAP Transactions

When the internal session representing a WAP flow for the CSG expires (due to inactivity or because a WAP DISCONNECT packet is received), any outstanding elements in the WAP transaction queue are reported. These are transactions that were not completed for some reason. Examples include a GET request for which a full REPLY was not received, or 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 (MMS)

Multimedia Messaging Service (MMS) traffic running over WAP is differentiated 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 due to 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. In situations where prepaid WAP with free MMS is configured, some packets still flow (even if a user has insufficient quota) in order to make this determination. But the transaction does not complete, and the user 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 users.

Configuring the CSG to Monitor and Generate WAP Reports

To enable the CSG to monitor and generate reports for WAP traffic, perform the following task:

	Command	Purpose
Step 1	`Router(config-csg-module)# ip csg policy POLICY_NAME`	Defines a policy for qualifying flows for the CSG accounting services, and enters CSG policy configuration mode.
Step 2	`Router(config-csg-policy)# accounting type wap {connection-oriented | connectionless} [customer-string string value]`	Defines the accounting type and customer string for all flows that comply with a CSG billing policy.

The following example shows how to enable the CSG to monitor and generate reports for WAP traffic:

```
ip csg policy WAP_CLT_POLICY
  accounting type wap connection-oriented customer-string to_wap_client
```

Note You cannot mix **type wap** with any other types. If one of the policies is **wap** they all must be **wap**.

WAP is only supported for CSG-style configurations—using content and not virtual servers.

Configuring Connection-Oriented and Connectionless WAP

The accounting types **wap connection-oriented** and **wap connectionless** specify how the WAP traffic for that port should be interpreted. To configure **wap connection-oriented** or **wap connectionless**, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip csg policy policy-name`	Defines a policy for qualifying flows for the CSG accounting services, and enters CSG policy configuration mode.
Step 2	`Router(config-csg-policy)# accounting type wap {connection-oriented | connectionless} [customer-string string]`	Defines the accounting type and customer string for all flows that comply with a CSG billing policy.

The following example shows how to define both connection-oriented and connectionless WAP accounting:

```
ip csg policy WSP_CON_P
 accounting type wap connection-oriented

ip csg policy WAP_NOCON_P
 accounting type wap connectionless

ip csg content WAP_CON
 ip any udp 9201
 policy WAP_CON_P
```

```
ip csg content WAP_CONLESS
 ip any udp 9200
 policy WAP_NOCON_P
```

Prepaid Support

Some upstream WAP browsing traffic occurs because the CSG must inspect the reply before determining that 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.

Redirect

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

To configure the redirect option, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip csg user-group` *group-name*	Creates a group of end-users for which you want to generate accounting records, and allows you to enter CSG user group configuration mode.
Step 2	`Router(config-csg-group)# redirect nat` *ip-address*	Redirects NAT client flows to an alternate IP address when the client's quota is exhausted.
Step 3	`Router(config-csg-group)# redirect wap` *url*	Redirects WAP client flows to an alternate URL when the client's quota is exhausted.
Step 4	`Router(config-csg-group)# redirect http` *url*	Redirects HTTP client flows to an alternate URL when the client's quota is exhausted.

WAP redirect requires that you configure a policy and service so a client who has exhausted quota can access the server specified in the redirect URL.

The following example shows how to define the redirect option for WAP, and to allow redirected WAP traffic to pass without charge:

```
ip csg user-group A1
 database 10.18.12.214 3311
 radius key secret-key
 quota local-port 7788
 redirect wap http://www.topoff.com
 quota server 10.10.1.203 7777 1
ip csg map TOPOFF url
  match protocol http url http://www.topoff.com*
!
ip csg policy URL_TOPOFF
  accounting type wap connection-oriented customer-string topoff
  url-map TOPOFF
!
ip csg content WAP_WTP_CONTENT
  ip any udp 9201
  policy URL_TOPOFF
```

```
  inservice
!
ip csg weight ZERO 0
!
ip csg service FREE
  content WAP_WTP_CONTENT policy URL_TOPOFF weight ZERO
```

Disabling Prepaid MMS Billing

By default the CSG treats MMS traffic like any other WAP 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:

	Command	Purpose
Step 1	`Router(config)# ip csg service service-name`	Defines a content billing service, and enters CSG service configuration mode.
Step 2	`Router(config-csg-service)# basis byte {ip exclude mms | fixed exclude mms}`	Specifies the billing basis for a CSG content billing service. This example illustrates how to exclude prepaid billing of MMS content for volume- or fixed-basis users.
Step 3	`Router(config-csg-service)# content content-name policy policy-name`	Defines content as a member of a CSG billing service, identifies a policy to apply to this content, and optionally assigns a weight to this content.

The following example shows how to disable MMS traffic from prepaid volume billing:

```
ip csg service SERVIN_WAP
 basis byte ip exclude mms
 content WAP_CLIENT policy WAP_CLT_POLICY
 content WAP_WSP_SRV policy WAP_SRV_POLICY
 content WAP_WTP_SRV policy WAP_SRV_POLICY
```

Note You can also use **basis fixed exclude mms** to disable prepaid billing for fixed-basis billing.

Configuring the CSG SMTP and POP3 Data Mining

The CSG can report SMTP and POP3 data records. To configure SMTP or POP3 data mining on the CSG, perform the following tasks:

	Command	Purpose
Step 1	`Router(config)# ip csg policy policy-name`	Defines a policy for qualifying flows for the CSG accounting services, and enters CSG policy configuration mode.
Step 2	`Router(config-csg-policy)# accounting type [smtp | pop3] [customer-string string]`	Defines the accounting type and customer string for all flows that comply with a CSG billing policy.

The following example shows how to enable the reporting of SMTP and POP3 data records on the CSG:

```
ip csg policy SMTP
  accounting type smtp

ip csg policy POP3
```

```
  accounting type pop3

ip csg content SMTP
  ip any tcp 25
  policy SMTP
  inservice


ip csg content POP3
  ip any tcp 110
  policy POP3
  inservice
```

Configuring RTSP Billing

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

To configure RTSP billing on the CSG, enter the following command in CSG policy configuration mode:

Command	Purpose
`Router(config-csg-policy)# accounting type rtsp [customer-string string]`	Defines the accounting type as RTSP, and optionally the customer string for all flows that comply with a CSG billing policy. Prepaid service matches are based on the IP address and port number of the control connection to the RTSP server IP.

The following example shows how to configure RTSP billing:

```
ip csg policy RTSP
  accounting type rtsp

ip csg content RTSP
  ip any tcp 554
  policy RTSP
  inservice
```

When configuring RTSP billing, keep the following considerations in mind:

- The CSG supports only port 554 for RTSP billing.
- RealPlayer clients 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 CSG does not bill the stream as RTSP. Therefore, for RTSP billing, you must block TCP and HTTP connections to the server network on ports 80, 8080 and 7070. For more information about blocking ports, see the "Blocking Ports" section on page 3-34.
- HTTP should be your last choice for RTSP transport.
- When using HTTP as the transport for RTSP, the control connection might time out, causing the stream to hang.

- This occurs because, when handling RTSP over HTTP, the client opens two TCP connections, one for the main content and one for control. The client uses the control connection sparingly, which can result in the connection timing out. To prevent this problem, ensure that the idle content timer has a duration of at least 60 seconds (the default setting is 3600 seconds). For more information on setting the idle content timer, see the description of the **idle** command in CSG content configuration mode.

  This is not an issue when using UDP or TCP as the transport.

Blocking Ports

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

```
ip csg policy RTSP
  accounting type rtsp
!
ip csg policy RTSP-BLOCK
  next-hop 10.10.10.1
!
ip csg content BLOCK7070
  ip 1.1.1.0 255.255.255.0 tcp 7070
  policy RTSP-BLOCK
  inservice
!
ip csg content BLOCK80
  ip 1.1.1.0 255.255.255.0 tcp 80
  policy RTSP-BLOCK
  inservice
!
ip csg content BLOCK8080
  ip 1.1.1.0 255.255.255.0 tcp 8080
  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 Connection Duration Billing

Connection Duration Billing enables the CSG to deduct quota based on the time that a user is logged on to the IP network.

To configure the Connection Duration Billing feature on the CSG, specify the following commands in CSG service configuration mode:

	Command	Purpose
Step 1	`Router(config-csg-service)# basis second connect [exclude mms]`	Specifies Connection Duration Billing for a CSG content billing service. **Note** When changing the basis for a service, the content must be taken out of service.
Step 1	`Router(config-csg-service)# activation [automatic | user-profile]`	Specifies the activation mode for a Connection Duration service.

The following commands are used to configure Connection Duration Billing for the **OFF_NET** service, with **automatic** activation:

```
ip csg service OFF_NET
  basis second connect
  activation automatic
```

Enabling Passthrough Mode for a Service

To enable passthrough mode for a service, specify the following command in CSG service configuration mode:

	Command	Purpose
Step 1	`Router(config-csg-service)# passthrough` *quota-grant*	Enables passthrough mode for a service.

The following example specifies that the CSG grants 65,535 quadrans of quota to the service NAME each time the service runs low on quota:

```
ip csg service NAME
  passthrough 65535
```

Configuring SNMP Timers

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

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

Command	Purpose
`Router(config)# ip csg snmp timer {agent | quota-server} [`*interval*`]`	Defines SNMP timers for lost CSG records, and enter s CSG SNMP timer configuration mode.

The following example defines a 300-second CSG SNMP agent timer and enters CSG SNMP timer configuration mode:

```
ip csg snmp timer agent 300
```

Configuring the Idle Content Timer for UDP and WAP 1.x

To configure an idle content timer, specify the following command in CSG content configuration mode:

Command	Purpose
`Router(config-csg-content)# idle` *duration*	Specifies the minimum amount of time that the CSG maintains an idle content connection.

The following example shows how to configure a 120-second idle timer for the CSG content MOVIES_COMEDY:

```
ip csg content MOVIES_COMEDY
 idle 120
```

The CSG tracks usage on a per-session basis. UDP protocols do not have an end-of-session indicator and simply idle out. For that reason, for UDP and WAP 1.x, setting the content idle timer to a low value (for example, 30 seconds) allows the CSG to quickly recognize that a session has ended and generate billing records accordingly. Other service-level features of the CSG that count sessions (such as passthrough mode and service-level CDRs) are similarly affected by the content idle timer setting.

Other Configuration Tasks

The following sections provide additional information to help you configure the CSG. The sections include:

Configuring the CSG and PSD

The configuration tasks required to establish communication between the CSG and the PSD involve several steps that go beyond the scope of this chapter. For specific information on how to configure the CSG and the PSD, see Appendix A, “PSD Configuration for the CSG.”

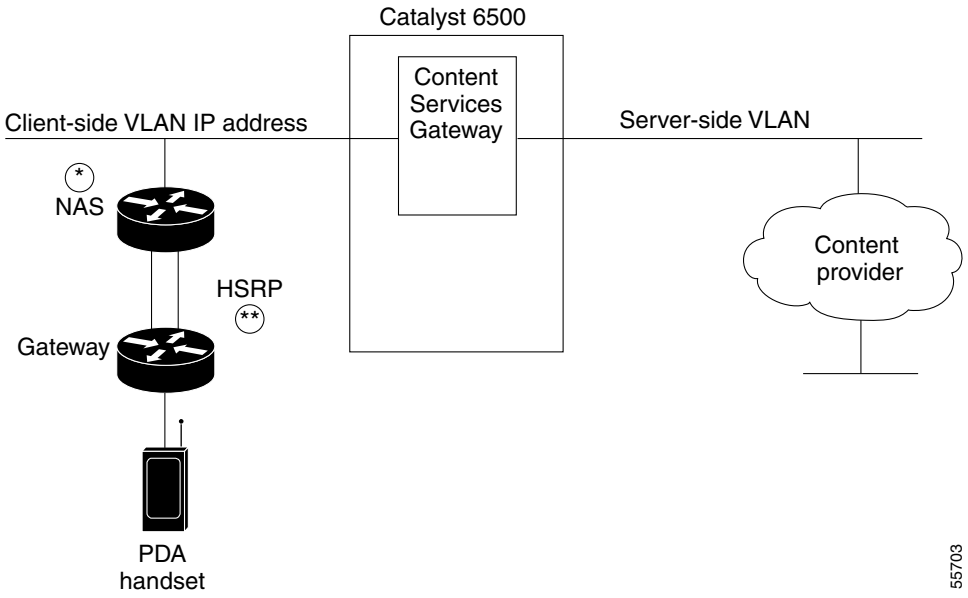
Configuring VLANs

Clients and servers communicate through the CSG using Layer 2 and Layer 3 technology in a specific VLAN configuration. Clients connect to the client-side VLAN, and servers connect to the server-side VLAN. Servers and clients exist on different subnets. Servers can also be located one or more Layer 3 hops away and connect to the server-side VLAN through routers. This section describes how to configure VLANs for the CSG.

A client sends a request to one of the module's server addresses. The CSG extracts the URL—if applicable—and records the statistics. When properly configured, the CSG records statistics for flows in both directions. When a connection ends, the CSG builds an accounting record and sends it to the BMA.

When you install the CSG in a Catalyst 6500 series switch, you must configure client-side and server-side VLANs. (See Figure 3-1.)

Figure 3-1 Configuring VLANs



*Any router configured as a client-side gateway, or a next-hop router for servers more than one hop away, must have ICMP redirects disabled. The CSG does not perform a Layer 3 lookup to forward traffic; the CSG cannot act upon ICMP redirects.

** You can configure up to seven gateways per VLAN for up to 256 VLANs and up to 224 gateways for the entire system. If an HSRP/VRRP gateway is configured, the CSG uses three gateway entries out of the 224 gateway entries because traffic can come from the virtual and physical MAC addresses of the HSRP group. (See the "HSRP Configuration Overview" section on page 4-9.)

Note You must configure VLANs on the Catalyst 6000 series switch or Cisco 7600 series router *before* you configure VLANs for the CSG. VLAN IDs must be the same for the switch and the module.

You must create both a client-side and server-side VLAN:

- Configuring Client-Side VLANs, page 3-38
- Configuring Server-Side VLANs, page 3-38

- Associating a Table Name with a VLAN, page 3-39

Configuring Client-Side VLANs

To configure client-side VLANs, perform this task:

	Command	Purpose
Step 1	`Router(config-csg-module)# vlan vlan-id client [vlan-name]`	Configures the client-side VLANs and enters the client VLAN mode. **Note** Do not use VLAN 1 as a client-side VLAN for the CSG.
Step 2	`Router(config-csg-vlan-client)# ip address ip-address netmask`	Configures an IP address to the CSG used by probes and Address Resolution Protocol (ARP) requests on this particular VLAN.
Step 3	`Router(config-csg-vlan-client)# gateway ip-address`	Configures the gateway IP address.

Note You cannot use VLAN 1 as a client-side or server-side VLAN for the CSG.

The following example shows how to configure the CSG for client-side VLANs:

```
Router(config-module-csg)# vlan 130 client
Router(config-csg-vlan-client)# ip address 123.44.50.6 255.255.255.0
Router(config-csg-vlan-client)# gateway 123.44.50.1
Router(config-csg-vlan-client)# exit
```

Configuring Server-Side VLANs

To configure server-side VLANs, perform this task:

	Command	Purpose
Step 1	`Router(config-csg-module)# vlan vlan-id server [vlan-name]`	Configures the server-side VLANs and enters the server VLAN mode. **Note** Do not use VLAN 1 as a server-side VLAN for the CSG.
Step 2	`Router(config-csg-vlan-server)# ip address ip-address netmask`	Configures an IP address for the server VLAN.
Step 3	`Router(config-csg-vlan-server)# alias ip-address netmask`	(Optional) Configures multiple IP addresses to the CSG as alternate gateways for the real server. The alias is required in the redundant configuration.
Step 4	`Router(config-csg-vlan-server)# route ip-address netmask gateway gw-ip-address`	Configures a static route to reach the real servers if they are more than one Layer 3 hop away from the CSG. **Note** If you are adding a new route to an existing gateway, the new route might not take effect until you remove the gateway and reconfigure it to clear the gateway cached entries.

The following example shows how to configure the CSG for server-side VLANs:

```
Router(config-module-csg)# vlan 150 server
Router(config-csg-vlan-server)# ip address 123.46.50.6 255.255.255.0
Router(config-csg-vlan-server)# alias 123.60.7.6 255.255.255.0
Router(config-csg-vlan-server)# route 123.50.0.0 255.255.0.0 gateway 123.44.50.1
Router(config-csg-vlan-server)# exit
```

Associating a Table Name with a VLAN

Interface awareness enables the CSG to distinguish between users and sessions that share the same IP address on different VLANs (that is, users and sessions with overlapping IP addresses). Interface awareness requires that each VLAN be associated with a table name.

To associate a table name with a VLAN, enter the following command in module CSG VLAN configuration mode:

Command	Purpose
`Router(config-csg-vlan-client)# table` *table-name* or `Router(config-csg-vlan-server)# table` *table-name*	Associates a table name with a VLAN.

Preventing Pipelined Requests

Note This procedure is no longer necessary in the CSG 3.1(3)C5(5) and later. It is made obsolete by the CSG's full HTTP pipelining support.

Some customers have handsets that attempt to make pipelined HTTP requests. Because this is not supported prior to CSG 3.1(3)C5(5), the CSG enables you to prevent HTTP pipelined requests by disabling HTTP persistence. This is done by applying TCP FIN to the final response packet to force establishing a new session for each request. The final response packet is identified using the Content-Length: field in the HTTP header, and support was not added to detect the final packet when Content-Length: is not present (as when using Transfer-Encoding: chunked). So, the CSG prevents chunked encoded responses by overwriting the HTTP version in the request to HTTP/1.0. Because chunked encoding is not supported in HTTP/1.0, an HTTP/1.1 server is not allowed to respond with chunked data.

To disable persistence, enter the following commands in module CSG configuration mode:

	Command	Purpose
Step 1	`Router(config-csg-module)# variable CSG_HTTP_PERSISTENCE_DISABLE 0`	Configures setting the FIN bit at end of responses. To disable this variable and prevent HTTP pipelined requests, set this variable to 0.
Step 2	`Router(config-csg-module)# variable CSG_HTTP_1_0_OPERATION 0`	Overwrites the HTTP version to 1.0 on GETs and responses. To disable this variable and prevent HTTP pipelined requests, set this variable to 0.

Configuring Layer 2-Adjacent Devices

Note If a CSG receives a packet with a Layer 2 address it does not recognize, from a device that has a layer 3 address that is not on the same IP subnet as the CSG, it drops the packet. If the CSG already has an Address Resolution Protocol (ARP) cache entry for the Layer 2 source address, it processes the packet normally. This behavior can be a problem if there are Layer 2-adjacent devices that are performing redundancy (for example, HSRP or Virtual Router Redundancy Protocol [VRRP] firewalls).

In a typical network environment, all traffic flows between clients and servers and uses the primary device/firewall. When traffic is coming *from* the device/firewall to the CSG, the source MAC can be that of the physical interface on that device rather than the MAC associated with the virtual IP address that is shared between the two devices/firewalls. If there is a failover of the second device/firewall, traffic is routed through the backup device/firewall. If the CSG does not have an ARP entry in its ARP cache for the MAC address of the now-active device/firewall, it drops packets received from that device/firewall.

To avoid this behavior, configure static routes on the CSG that point to the IP addresses on the interfaces of the adjacent devices/firewalls. For example, if the CSG is Layer 2-adjacent to two firewalls, and the IP addresses on those firewalls are 1.1.1.5 and 1.1.1.6, configure the following on the CSG:

route *IP address not-in-use on the network* 255.255.255.255 gateway 1.1.1.5
route *IP address not-in-use on the network* 255.255.255.255 gateway 1.1.1.6

This causes the CSG to spawn an ARP for 1.1.1.5 and 1.1.1.6 so that it has an ARP entry in its ARP cache for both firewalls. In the event of a failover, the packets received from the now-active firewall have a source MAC that is in the ARP cache of the CSG.

Configuration Examples

This section includes the following examples:

Sample CSG Billing Rules

Table 3-1 shows sample CSG billing rules.

Table 3-1 Sample CSG Billing Rules

Content Specification	Service/Billing Basis	Quadrans per Unit
IP/Netmask = 1.2.3.4/24 Protocol/Port Number = TCP/80 HostName = *.books-co-inc.com URL = *.jpg	Service = BillByVolume Basis = TCP Volume	1
IP/Netmask = 1.2.3.4/24 Protocol/Port Number = TCP/80 HostName = *.books-co-inc.com URL = *freecontent*	Service = BillPerClick Basis = Constant	0
IP/Netmask = 1.2.3.4/24 Protocol/Port Number = TCP/80 HostName = *.advt-co.com URL = *	Service = Advertisements Basis = Constant	-1

Table 3-1 Sample CSG Billing Rules (continued)

Content Specification	Service/Billing Basis	Quadrans per Unit
IP/Netmask = 198.133.219.0/24 Protocol/Port Number = TCP/80 HostName = *bigcorp* URL = *	Service = Corporate Basis = Constant	0
IP/Netmask = 0.0.0.0/0 Protocol/Port Number = TCP/80 HostName = * URL = *	Service = Internet Basis = IP Volume	1

The following example shows how to configure these CSG billing rules:

```
ip csg user-group U1
 entries max 10000
 radius key cisco
 radius acct-port 23385
 radius userid User-Name
 quota local-port 4095
 quota server 20.20.50.13 3386 5
 quota server 20.20.50.130 3386 6
 quota server 20.20.52.13 3386 7
!
ip csg accounting CSGBILL
 user-group U1
 records max 2000
 agent activate 2 sticky 30
 records intermediate bytes 50000
 agent 9.15.72.5 3386 2
 agent 10.76.86.2 3386 5
!
 agent 20.20.50.131 3386 8
 inservice
!
ip csg map ADVERTISEMENTS header
 match header Host header-value *.advt-co.com
!
ip csg map ALLHOSTS header
 match header Host header-value *
!
ip csg map BOOKS header
 match header Host header-value *.books-co-inc.com
!
ip csg map CORPORATE header
 match header Host header-value *bigcorp*
!
ip csg map ALLURLS url
 match url *
!
ip csg map BOOKFREE url
 match url *freecontent*
!
ip csg map JPGS url
 match url *.jpg
!
ip csg map GIF url
```

```
 match url *.gif
!
ip csg policy ADVERTISEMENTS
 accounting type http
 url-map ALLURLS
 header-map ADVERTISEMENTS
!
ip csg policy BOOKFREE
 accounting type http
 url-map BOOKFREE
 header-map BOOKS
!
ip csg policy BOOKSALES
 accounting type http
 url-map JPGS
 header-map BOOKS
!
ip csg policy CORPORATE
 accounting type http
 url-map ALLURLS
 header-map CORPORATE
!
ip csg policy INTERNET
 accounting type http
 url-map ALLURLS
 header-map ALLHOSTS
!
ip csg content ADVERTISEMENTS
 ip 1.2.5.0 255.255.255.0 tcp 80
 policy ADVERTISEMENTS
 inservice
!
ip csg content BOOKS
 ip 1.2.3.0 255.255.255.0 tcp 80
 policy BOOKSALES
 policy BOOKFREE
 inservice
!

ip csg content CORPORATE
 ip 198.133.219.0 255.255.255.0 tcp 80
 policy CORPORATE
 inservice
!
ip csg content INTERNET
 ip any tcp 80
 policy INTERNET
 inservice
!
ip csg ruleset R1
 content ADVERTISEMENTS
 content BOOKS
 content CORPORATE
 content INTERNET
!
ip csg weight FREE 0
ip csg weight PAYBACK -1
!
ip csg service BILLPERCLICK
 basis fixed
 content ADVERTISEMENTS policy ADVERTISEMENTS weight PAYBACK
 content BOOKS policy BOOKSALES
 content BOOKS policy BOOKFREE weight FREE
 content CORPORATE policy CORPORATE weight FREE
```

```
!
ip csg service BILLBYVOLUME
 basis byte tcp
 content BILLBYVOLUME policy BILLBYVOLUME
!
ip csg service BILLBYIPVOLUME
 basis byte
 content INTERNET policy INTERNET
!
ip csg billing PLAN1
 service BILLPERCLICK
 service BILLBYVOLUME
 service BILLBYIPVOLUME
!

module ContentServicesGateway 5
 vlan 30 client AUCTION_HOUSE
  ip address 123.44.50.6 255.255.255.0
  gateway 123.44.50.1
!
 vlan 40 server
  ip address 123.46.50.6 255.255.255.0
!
 ruleset R1
 accounting CSGBILL
```

Simple Postpaid Billing Configuration Example

The following example shows a simple postpaid billing CSG configuration:

```
ip csg policy POLICY1
 accounting type http
!
ip csg content MOVIES_COMEDY
 ip 172.18.45.0/24 tcp 8080
 policy POLICY1
 inservice
!
ip csg content AUCTION_HOUSE
 ip 216.32.120.0/24 tcp 8080
 policy POLICY1
 vlan AUCTION_HOUSE
 inservice
!
ip csg content WAKETECH
 ip 48.33.0.0/16 tcp 80
 policy POLICY1
 inservice
!
ip csg ruleset R1
 content MOVIES_COMEDY
 content AUCTION_HOUSE
 content WAKETECH
!
ip csg user-group G1
 entries max 100000
 database 10.1.2.3 11111
 radius key secretpassword
!
ip csg accounting A1
 user-group G1
 agent localport 3775
```

```
 agent 10.1.2.4 11112 1
 agent 10.1.2.5 11113 2
 agent activate 2
 records max 250
 inservice
!
mod csg 4
 vlan 30 client AUCTION_HOUSE
  ip address 123.44.50.6 255.255.255.0
  gateway 123.44.50.1
 vlan 40 server
  ip address 123.46.50.6 255.255.255.0
  alias 123.60.7.6 255.255.255.0
  route 123.50.0.0 255.255.0.0 gateway 123.44.50.1
 ruleset R1
 accounting A1
```

Basic WAP Configuration Example

The following example illustrates a basic CSG WAP configuration that provides the following functions:

- Charges a fixed rate for all WAP and MMS transactions for which a URL is used.
- Allows requests that are not content-based (control flows) to go through for free.
- Uses a single service for all traffic.

```
ip csg map DEFAULT_URL url
 match protocol http url http://*
!
ip csg policy WAP_URL
 accounting type wap connection-oriented
 url-map DEFAULT_URL
!
ip csg policy WAP_CONTROL
 accounting type wap connection-oriented customer-string control_flow
!
ip csg content WAP_WTP_CONTENT
 ip any udp 9201
 idle 30
 policy WAP_URL
 policy WAP_CONTROL
 inservice
!
ip csg weight ZERO 0
!
ip csg service WAP
 basis fixed
 content WAP_WTP_CONTENT policy WAP_URL
 content WAP_WTP_CONTENT policy WAP_CONTROL weight ZERO
```

Redirect to Top-Off Server Configuration Example

The following example illustrates a WAP configuration with additions to support redirect to a top-off server. This configuration provides the following functions:

- Allows redirect requests to the top-off server to go through for free.
- Defines a second service to be used only for free transactions.

Note This configuration is required to allow redirect to work properly.

Users must also be authorized to use this service by the quota server.

No quota needs to be given out for this service, but a cause code of 0x04 (user authorized) must be returned for the transaction to be allowed through.

```
ip csg map TOPOFF url
 match protocol http url http://www.topoff.com*
!
ip csg map DEFAULT_URL url
 match protocol http url http://*
!
ip csg policy URL_TOPOFF
 accounting type wap connection-oriented customer-string topoff
 url-map TOPOFF
!
ip csg policy WAP_URL
 accounting type wap connection-oriented customer-string
 url-map DEFAULT_URL
!
ip csg policy WAP_CONTROL
 accounting type wap connection-oriented customer-string control_flow
!
ip csg content WAP_WTP_CONTENT
 ip any udp 9201
 idle 30
 policy URL_TOPOFF
 policy WAP_URL
 policy WAP_CONTROL
 inservice
!
ip csg weight ZERO 0
!
ip csg service WAP
 basis fixed
 content WAP_WTP_CONTENT policy WAP_URL
!
ip csg service FREE
 content WAP_WTP_CONTENT policy URL_TOPOFF weight ZERO
 content WAP_WTP_CONTENT policy WAP_CONTROL weight ZERO
```

Free MMS Transactions Configuration Example

Specific MMS Transactions

The following example illustrates a WAP 1 or MMS/WAP1.x configuration in which MMS transactions to servers mms1 and mms2 are free, while third-party MMS transactions are charged.

```
ip csg map TOPOFF url
 match protocol http url http://www.topoff.com*
!
ip csg map OUR_MMS url
 match protocol http url http://www.mms1*
 match protocol http url http://www.mms2*
!
ip csg map DEFAULT_URL url
 match protocol http url http://*
!
```

```
ip csg policy URL_TOPOFF
 accounting type wap connection-oriented customer-string topoff
 url-map TOPOFF
!
ip csg policy FREE_MMS
 accounting type wap connection-oriented customer-string free_mms
 url-map OUR_MMS
!
ip csg policy WAP_URL
 accounting type wap connection-oriented customer-string
 url-map DEFAULT_URL
!
ip csg policy WAP_CONTROL
 accounting type wap connection-oriented customer-string control_flow
!
ip csg content WAP_WTP_CONTENT
 ip any udp 9201
 idle 30
 policy URL_TOPOFF
 policy FREE_MMS
 policy WAP_URL
 policy WAP_CONTROL
 inservice
!
ip csg weight ZERO 0
!
ip csg service WAP
 basis fixed
 content WAP_WTP_CONTENT policy WAP_URL
!
ip csg service FREE
 content WAP_WTP_CONTENT policy URL_TOPOFF weight ZERO
 content WAP_WTP_CONTENT policy FREE_MMS weight ZERO
 content WAP_WTP_CONTENT policy WAP_CONTROL weight ZERO
```

All MMS Transactions

The following example illustrates a WAP 1 or MMS/WAP1.x configuration in which all MMS transactions are free. In this example, MMS content is free for service WAP (the user must be authorized for this service).

```
ip csg map TOPOFF url
 match protocol http url http://www.topoff.com*
!
ip csg map DEFAULT_URL url
 match protocol http url http://*
!
ip csg policy URL_TOPOFF
 accounting type wap connection-oriented customer-string topoff
 url-map TOPOFF
!
ip csg policy WAP_URL
 accounting type wap connection-oriented customer-string
 url-map DEFAULT_URL
!
ip csg policy WAP_CONTROL
 accounting type wap connection-oriented customer-string control_flow
!
ip csg content WAP_WTP_CONTENT
 ip any udp 9201
 idle 30
 policy URL_TOPOFF
 policy WAP_URL
 policy WAP_CONTROL
```

```
 inservice
!
ip csg weight ZERO 0
!
ip csg service WAP
  basis fixed exclude mms
  content WAP_WTP_CONTENT policy WAP_URL
!
ip csg service FREE
  content WAP_WTP_CONTENT policy URL_TOPOFF weight ZERO
  content WAP_WTP_CONTENT policy WAP_CONTROL weight ZERO
```

Differentiating MMS Over WAP 2 Example

The following example assumes that the quota server and the accounting agent are already configured for the system. It also assumes that the WAP proxy can be found on port 9401 on a host addressable using a server VLAN configured to access the subnet 10.10.2.0/24. This example illustrates the differences in a working configuration necessary to differentiate billing WAP2/HTTP and MMS/WAP2/HTTP.

```
ip csg map WAP2MMS_GET_MAP url
 match protocol http method GET url /wap/mms*

ip csg map WAP2MMS_POSTMAP url
 match protocol http method POST url /wap/mms*

ip csg map WAP2MMSPOSTMAPH header
 match protocol http header Content-Type header-value application/vnd.wap.mms-message

ip csg policy WAP2_MMS_GET
! match all wap2/http gets of mms
  accounting type http customer-string wap2mms-get
  url-map WAP2MMS_GET_MAP

ip csg policy WAP2_MMS_POST
! match all wap2/http posts that are mms related
! This catches handset-initiated MMS sends and acknowledgements of
! network-initiated MMS pushes.
  accounting type http customer-string wap2mms-post
  header-map WAP2MMSPOSTMAPH  ! recommended
! or
! url-map WAP2MMS_POSTMAP  ! optional
! The header-map catches MMS even when it goes to an unknown URL,
! so it is recommended over the url-map.

ip csg policy WAP2
! You might choose to differentiate non-MMS wap2 get/posts and URLs/headers
! here, if relevant. In this case, we just label all remaining traffic as
! wap2.
  accounting type http customer-string wap2

ip csg content WAP2
! 10.10.2.0 255.255.255.0 represents the network where WAP 2 Proxies are
! located. Port 9401 is the port the WAP 2 Proxies are configured to use.
 ip 10.10.2.0 255.255.255.0 tcp 9401
 policy WAP2_MMS_GET
 policy WAP2_MMS_POST
 policy WAP2
 inservice

! Adjust these to change the pre-paid weight associated with each flow:
ip csg weight WEIGHT_WAP2 3
```

```
ip csg weight WEIGHT_WAP2GET 1
ip csg weight WEIGHT_WAP2POST 2

ip csg service WAP2MMSGET
 basis fixed
 idle 10000
 content WAP2 policy WAP2_MMS_GET weight WEIGHT_WAP2GET

ip csg service WAP2MMSPOST
 basis fixed
 idle 10000
 content WAP2 policy WAP2_MMS_POST weight WEIGHT_WAP2POST

ip csg service WAP2
 basis fixed
 idle 10000
 content WAP2 policy WAP2 weight WEIGHT_WAP2

ip csg ruleset R
! other contents
 content WAP2

ip csg billing BILL1
 service WAP2MMSGET
 service WAP2MMSPOST
 service WAP2
```

Pricing by Quota Server Configuration Example

The following example shows a CSG configuration in which all pricing is done by a quota server. In this example:

- Assume that User X has $10.00 in his account.
- There are two types of content:
  - C1—This is billed per object (for example, URL GET), where each object costs $0.01.
  - C2—This is billed per byte, where each KB 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 User X, with a subscription to billing plan REGULAR, tries to access content that matches C1, the CSG tries to download quota for User X for service PERCLICK.

The quota server borrows money from User X's $10.00, and returns some quadrans to the CSG. Each quadran is good for one object download, or one click. If the quota server wants the CSG to query for each click, it can choose to send just one quadran at a time, so that the CSG queries the quota server each time. On the other hand, if the quota server wants to grant $2.00 worth to the CSG in one shot, it can send 200 quadrans to the CSG, which the CSG keeps using for User X's access to C1.

When User X tries to access content that matches C2, the CSG makes another request to the quota server to get User X's quota for C2. C2 is billed per IP byte. The quota server borrows another $5.00 from User X's account, and sends 500000 quadrans to the CSG. As User X continues to access C2, his traffic is metered for volume, and for each byte the CSG deducts one quadran.

Differentiating Prices Configuration Example

The following example extends the previous example by adding an additional content type that is priced differently. In this example:

- Assume that User X has $10.00 in his account.
- There are three types of content:
  - C1—This is billed per *.jpg file, where each JPG file costs $0.01.
  - C2—This is billed per byte, where each KB costs $0.01.
  - C3—This 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 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 User X tries to download an MP3 file (that is, a file that matches content MP3), the CSG requests the MP3 quota for User X. Each download of an MP3 file costs $0.05, so the quota server borrows $1.00 from User X's account, and returns 20 quadrans to the CSG for service MP3. The CSG can use the quadrans for 20 downloads of MP3 files.

Alternatively, the quota server could send just one quadran, which is good for only one transaction. This would force the CSG 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 3-50 showed that you can create a new service for a content and differentiate its billing from other types of content.

However, with each new service, the user's quota fragments further, and traffic between the CSG and the quota server increases.

You can improve this situation by specifying a symbolic weight on the CSG. In this 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, reducing the overall number of services and reducing the traffic between the CSG and the quota server.

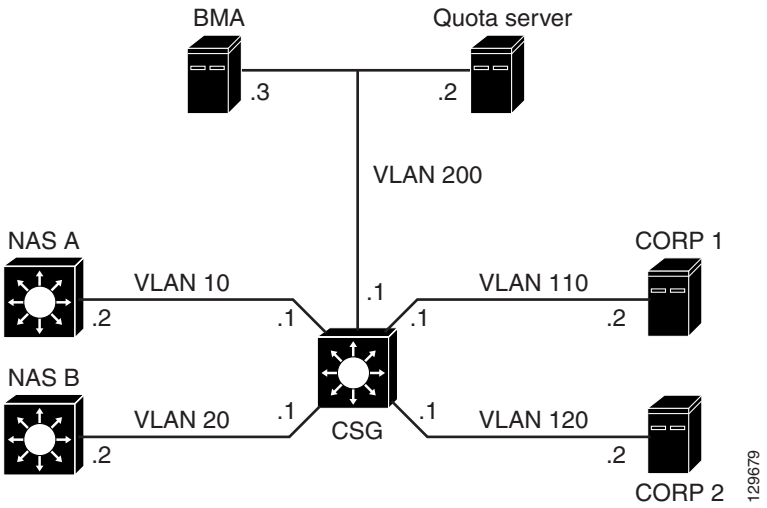
```
ip csg content C1
 policy P1
 inservice
!
ip csg content C2
 policy P2
 inservice
!
ip csg content MP3
 policy P1
 inservice
!
ip csg weight MP3 5
!
ip csg service PERBYTE
 basis byte ip
 content C2 policy P2
!
ip csg service PERCLICK
 basis fixed
 content C1 policy P1
 content MP3 policy P1 weight MP3
!
ip csg billing REGULAR
 service PERCLICK
 service PERBYTE
```

When the quota server borrows $1.00 from User X's account, and sends 100 quadrans for service PERCLICK, the CSG can use the quadrans for 100 JPG files, or for 20 MP3 files, or for a mix of the two.

Interface Awareness Example

The following example provides a sample configuration for interface awareness.

Figure 3-2 Interface Awareness




```
ip csg user-group GROUP1
 radius userid Calling-Station-Id
 user-profile server radius pass
 quota server 10.10.200.2 3386 1
!
ip csg accounting USER-BMA1
 user-group GROUP1
 agent 10.10.200.3 3386 1
 inservice
!
ip csg policy CORP1-POLICY
 accounting type other customer-string CORP1
 next-hop 10.10.110.2
!
ip csg policy CORP2-POLICY
 accounting type other customer-string CORP2
 next-hop 10.10.120.2
!
ip csg content CORP1-CONTENT
 ip any
 vlan CORP1-CLIENT
 policy CORP1-POLICY
 inservice
!
ip csg content CORP2-CONTENT
 ip any
 vlan CORP2-CLIENT
 policy CORP2-POLICY
 inservice
!
ip csg ruleset R1
 content CORP1-CONTENT
 content CORP2-CONTENT
!
ip csg service CORP1
```

```
 content CORP1-CONTENT policy CORP1-POLICY
!
ip csg service CORP2
 content CORP2-CONTENT policy CORP2-POLICY
!
ip csg billing CORP1
 service CORP1
!
ip csg billing CORP2
 service CORP2
!
module ContentServicesGateway 9
 vlan 10 server
  name CORP1-CLIENT
  table C1
  ip address 10.10.10.1 255.255.255.0
!
 vlan 20 server
  name CORP2-CLIENT
  table C2
  ip address 10.10.20.1 255.255.255.0
!
 vlan 110 server
  name CORP1-SERVER
  table C1
  ip address 10.10.110.1 255.255.255.0
!
 vlan 120 server
  name CORP2-SERVER
  table C2
  ip address 10.10.120.1 255.255.255.0
!
 vlan 200 server
  name CSG-TO-BMA-QS
  ip address 10.10.200.1 255.255.255.0
!
 ruleset R1
 accounting USER-BMA1
 radius proxy 10.10.10.3 10.10.110.3 key cisco table C1
 radius proxy 10.10.20.3 10.10.120.3 key cisco table C2
```

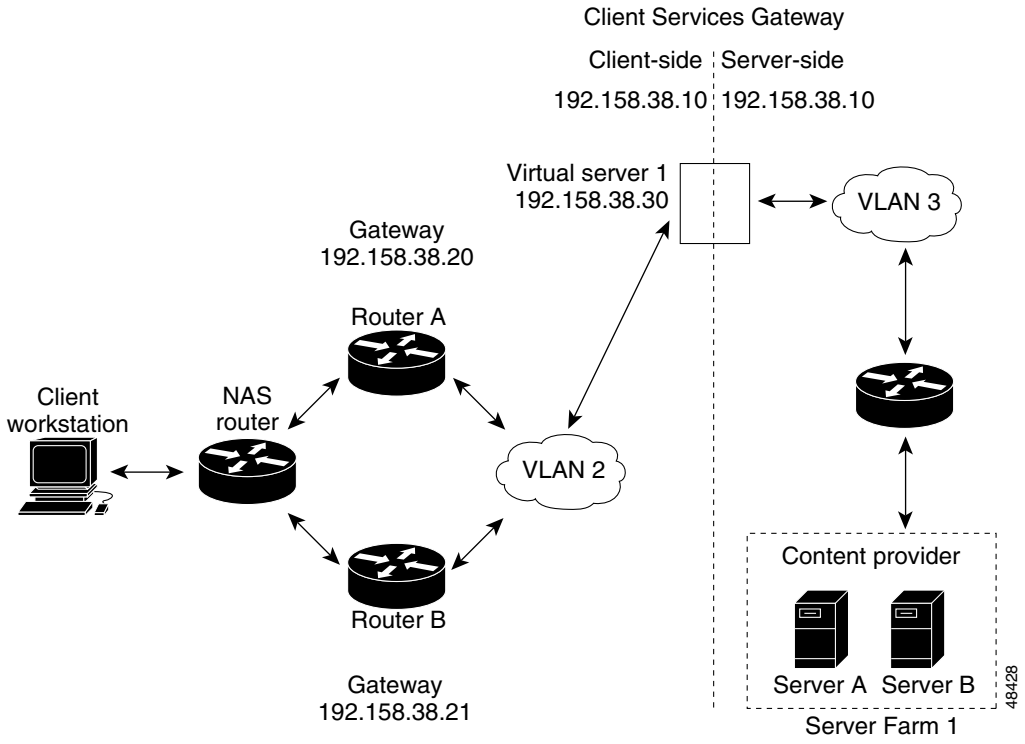
Configuring Secure (Router) Mode, Redundancy, Fault Tolerance, and HSRP

This chapter describes how to configure some aspects of content switching that are necessary for the Content Services Gateway to function properly. This information is contained in the following sections:

Configuring the Single Subnet (Bridge) Mode

In a single subnet (bridge) mode configuration, the client-side and server-side VLANs are on the same subnets. Figure 4-1 illustrates a typical single subnet (bridge) mode configuration.

Figure 4-1 Single Subnet (Bridge) Mode Configuration



To configure single subnet (bridge) mode content switching, first configure a client-side VLAN and a server-side VLAN, using the following procedure:

	Command	Purpose
Step 1	`Router# vlan database`	Enters the VLAN configuration mode.
Step 2	`Router(vlan)# vlan 2`	Configures a client-side VLAN.
Step 3	`Router(vlan)# vlan 3`	Configures a server-side VLAN.

After you have configured a client-side VLAN and a server-side VLAN, assign the same IP address to the VLANs, using the following procedure:

	Command	Purpose
Step 1	`Router(config-module-csg)# vlan 2 client`	Creates the client-side VLAN 2 and enters module CSG VLAN client configuration mode.
Step 2	`Router(config-csg-vlan-client)# ip addr 192.158.38.10 255.255.255.0`	Assigns the CSG IP address on VLAN 2.
Step 3	`Router(config-csg-vlan-client)# gateway 192.158.38.20`	Defines the client-side VLAN gateway to Router A.
Step 4	`Router(config-module-csg)# vlan 3 server`	Creates the server-side VLAN 3 and enters the CSG VLAN server configuration mode.
Step 5	`Router(config-csg-vlan-server)# ip addr 192.158.38.10 255.255.255.0`	Assigns the CSG IP address on VLAN 3.

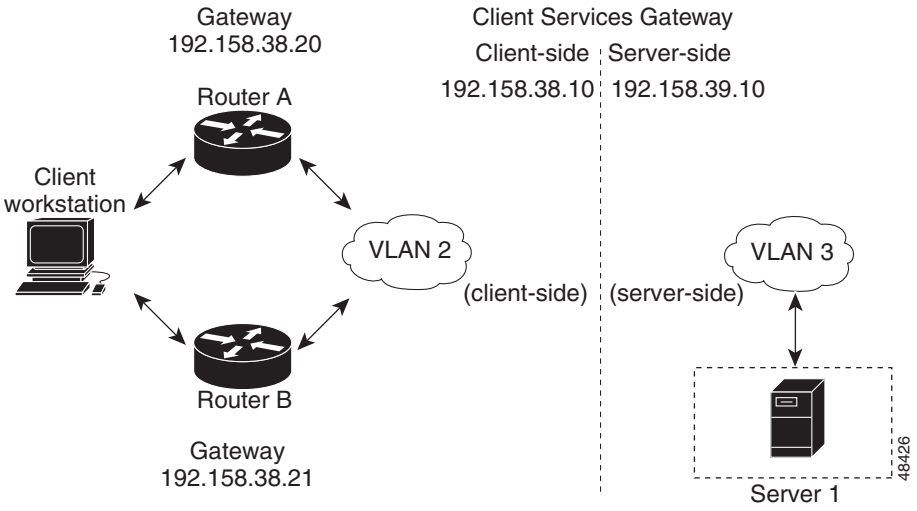
	Command	Purpose
Step 6	`Router(config-csg-vlan-server)# exit`	Exits the configuration mode.
Step 7	`Router(config-module-csg)# vserver VIP1`	Creates a virtual server and enters the CSG virtual server mode.

After you have assigned the IP addresses, set the server's default routes to Server A's gateway (192.158.38.20) or Server B's gateway (192.158.38.21).

Configuring the Secure (Router) Mode

Because the client-side and server-side VLANs are on different subnets, you can configure the CSG to operate in a secure (router) mode. Figure 4-2 shows how to set up the secure (router) mode configuration.

Figure 4-2 Secure (Router) Mode Configuration



To configure content switching in secure (router) mode, first configure a client-side VLAN and a server-side VLAN, using the following procedure:

	Command	Purpose
Step 1	`Router# vlan database`	Enters the VLAN configuration mode.
Step 2	`Router(vlan)# vlan 2`	Configures a client-side VLAN.
Step 3	`Router(vlan)# vlan 3`	Configures a server-side VLAN.

After you have configured a client-side VLAN and a server-side VLAN, assign IP addresses to the VLANs, using the following procedure:

	Command	Purpose
Step 1	`Router(config-module-csg)# vlan 2 client`	Creates the client-side VLAN 2 and enters module CSG VLAN client configuration mode.
Step 2	`Router(config-csg-vlan-client)# ip address 192.158.38.10 255.255.255.0`	Assigns the CSG IP address on VLAN 2.
Step 3	`Router(config-csg-vlan-client)# gateway 192.158.38.20`	Defines the client-side VLAN gateway to Router A.
Step 4	`Router(config-module-csg)# vlan 3 server`	Creates the server-side VLAN 3 and enters the CSG VLAN server configuration mode.
Step 5	`Router(config-csg-vlan-server)# ip address 192.158.39.10 255.255.255.0`	Assigns the CSG IP address on VLAN 3.

Configuring Fault Tolerance

This section describes a fault-tolerant (FT) configuration. In this configuration, two separate Catalyst 6000 series chassis each contain a CSG. The configuration can also apply to two separate Cisco 7600 series router chassis containing CSGs.

Note You can also create a fault-tolerant configuration with two CSGs in a single Catalyst 6000 series switch or Cisco 7600 series router chassis. You can create a fault-tolerant configuration in the secure (router) mode.

In the secure (router) mode, the client-side and server-side VLANs provide the fault-tolerant (redundant) connection paths between the CSG and the routers on the client side and the servers on the server side. In a redundant configuration, two CSGs perform active and standby roles. Each CSG contains the same IP, virtual server, and server farm. From the client-side and server-side networks, each CSG is configured identically. The network sees the fault-tolerant configuration as a single CSG.

Configuring fault-tolerance requires the following:

- Two CSGs that are installed in the Catalyst 6000 series switch or Cisco 7600 series router chassis.
- Identically configured CSGs. One CSG is negotiated at run time to be the active; the other is negotiated to be the standby.
- Each CSG connected to the same client-side and server-side VLANs.
- Communication between the CSGs provided by a shared private VLAN.
- Each FT CSG pair must use a different FT VLAN.
- If you have pairs of CSG cards and pairs of CSM cards in your network, each pair must use a different FT VLAN. Do not configure a CSG pair and a CSM pair to use the same FT VLAN.
- The CSG does support trunked FT VLANs, but each pair of CSGs must use a unique FT VLAN and a unique group ID. In addition, make sure that the number of high availability messages between all pairs of CSGs on the trunk does not overwhelm the CSG card.
- A network that sees the redundant CSGs as a single entity.

- Connection redundancy by configuring a link that has a 1-GB per-second capacity. Enable the calendar in the switch Cisco IOS software so that the CSG state change gets stamped with the correct time.

  The following command enables the calendar:

```
Cat6k-2# configure terminal
Cat6k-2(config)# clock timezone WORD offset from UTC
Cat6k-2(config)# clock calendar-valid
```

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

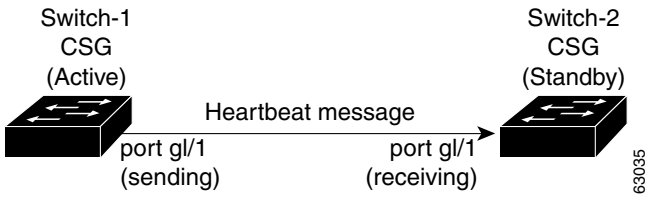
- Quality of service (QoS) configured on each CSG in the fault-tolerant pair with Cisco IOS Release 12.1(12c)E4 and later. Table 4-1 lists the QoS requirements.

Table 4-1 QoS Enabling Matrix

CSG Release	Cisco IOS Release	Supervisor Engine/MSFC	Configure QoS?
3.1(1)C3(1)	12.1(12c)E4	SUP1-MSFC2	No
3.1(1)C3(1)	12.1(12c)E4	SUP2-MSFC2	Yes
3.1(1)C4(1)	12.1(12c)E4	SUP2-MSFC2	Yes
3.1(3)C5(1)	12.2(14)ZA7	SUP2-MSFC2	Yes
3.1(3)C5(5)	12.2(18)SXD	SUP720-MSFC3-BXL SUP2-MSFC2	Yes
3.1(3)C6(2)	12.2(18)SXE	SUP720-MSFC3-BXL SUP2-MSFC2	Yes

Figure 4-3 shows the QoS configuration topology.

Figure 4-3 QoS Configuration Topology



Without the secure (router) mode configuration shown in Figure 4-2, 802.1Q priority information is not preserved in packets traversing to the switch. Heartbeat messages sent from the active to the standby CSG must contain this priority information so that they are transmitted without delay. When an excessive delay occurs, an unnecessary takeover might occur.

You can overcome this limitation by configuring the sending port g1/1 to retain priority information upon transmission and the receiving port g1/1 to trust the class of service (CoS) (priority bits) for the incoming packets.

Configure the switch with the **permit any any** command to enable it to accept incoming packets with any MAC address from any MAC address.

To configure QoS for a fault-tolerant configuration, enter these commands:

```
Router(config)# mls qos
Router(config)# interface g1/1
Router(config-if)# no shutdown
Router(config-if)# mls qos cos 7
Router(config-if)# switchport
Router(config-if)# switchport access vlan 200
Router(config-if)# switchport trunk encapsulation dot1q
Router(config-if)# switchport trunk allowed vlan 1,2,1002-1005
Router(config-if)# switchport mode trunk
```

Table 4-2 lists CSG fault-tolerant configuration requirements.

Table 4-2 The CSG Fault-Tolerant Configuration Requirements

Configuration Parameter	On Both CSG Modules	
	Same	Different
VLAN name	X	
VLAN address		X
Gateway[1] address	X	
Content name	X	
Content IP address	X	
Alias IP addresses	X	
Redundancy group name	X	
Redundancy VLAN ID	X	

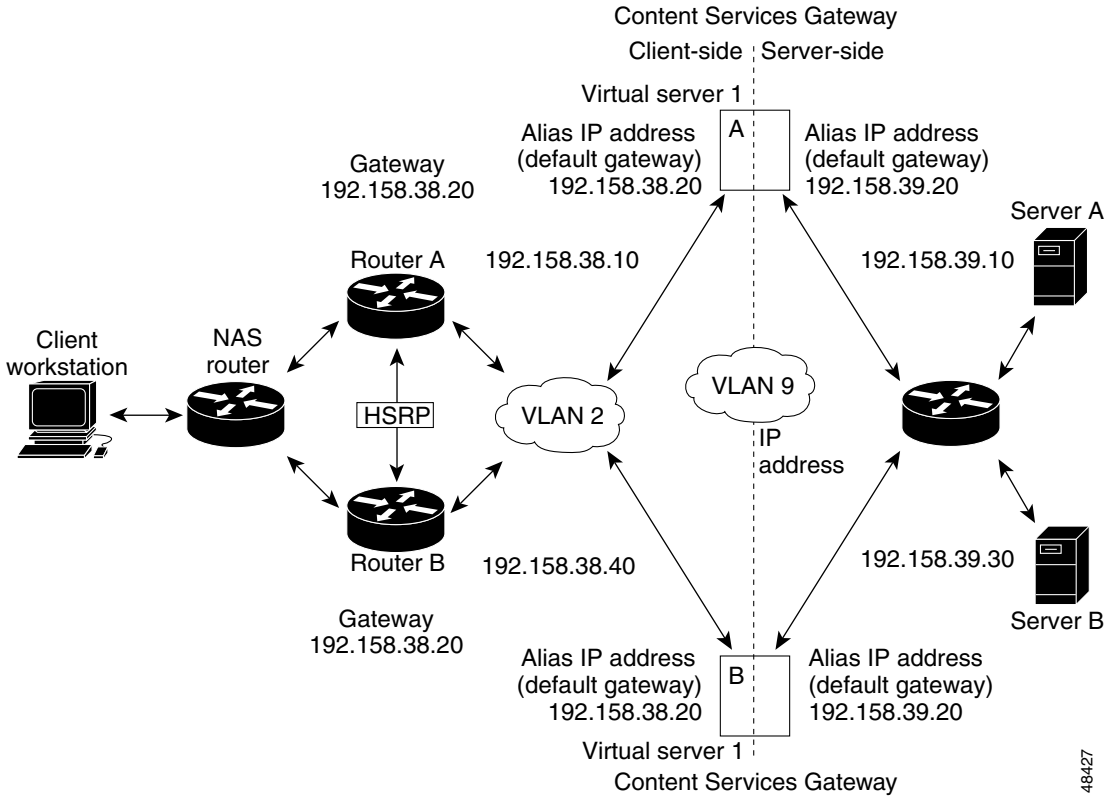
1. Server default gateways must point to the alias IP address.

Enter the **replicate connection tcp** command in content configuration mode to configure replication for the CSGs. (The default setting for the **replicate** command is disabled.)

If no router is present on the server-side VLAN, then each server's default route points to the alias IP address.

Figure 4-4 shows how to set up a secure (router) mode fault-tolerant configuration.

Figure 4-4 Fault-Tolerant Configuration



To configure the active (A) CSG for fault tolerance, use the following procedure:

	Command	Purpose
Step 1	`Router(config-module-csg)# vlan 2 client`	Creates the client-side VLAN 2 and enters CSG VLAN client configuration mode.
Step 2	`Router(config-csg-vlan-client)# ip address 192.158.38.10 255.255.255.0`	Assigns an IP address to the CSG VLAN.
Step 3	`Router(config-csg-vlan-client)# alias 192.158.38.30 255.255.255.0`	Assigns an alias address to the CSG.
Step 4	`Router(config-csg-vlan-client)# gateway 192.158.38.20 255.255.255.0`	(Optional) Defines the client-side VLAN gateway for an HSRP enabled gateway.
Step 5	`Router(config-module-csg)# ip csg content content1`	Creates a CSG content definition and enters the CSG content configuration mode.
Step 6	`Router(config-csg-content)# ip any tcp www`	Defines Layer 3/Layer 4 parameters of the content.
Step 7	`Router(config-csg-content)# inservice`	Enables the server.
Step 8	`Router(config-module-csg)# vlan 3 server`	Creates the server-side VLAN that defines the Layer 2 paths for the CSG accounting service flows, assigns a VLAN ID and optional name, and enters module CSG VLAN configuration mode.
Step 9	`Router(config-csg-vlan-server)# ip address 192.158.39.10 255.255.255.0`	Assigns the CSG IP address on VLAN 2.

	Command	Purpose
Step 10	`Router(config-csg-vlan-server)# alias 192.158.39.20 255.255.255.0`	Assigns an alias address to the CSG.
Step 11	`Router(config-module-csg) vlan 9 ft`	Defines VLAN 9 as a fault-tolerant VLAN.
Step 12	`Router(config-module-csg)# ft group` *ft-group-number* `vlan 9`	Enters fault-tolerant configuration mode and configures fault tolerance.
Step 13	`Router(config-module-csg)# end`	Ends module CSG configuration mode.
Step 14	`Router# vlan database`	Enters VLAN configuration mode.
Step 15	`Router(vlan)# vlan 2`	Configures a client-side VLAN 2.
Step 16	`Router(vlan)# vlan 3`	Configures a server-side VLAN 3.
Step 17	`Router(vlan)# vlan 9`	Configures a fault-tolerant VLAN 9.
Step 18	`Router(vlan)# exit`	Exits. The configuration takes affect.

To configure the standby (B) CSG for fault tolerance, perform this task (see Figure 4-4):

	Command	Purpose
Step 1	`Router(config-module-csg)# vlan 2 client`	Creates the client-side VLAN that defines the Layer 2 paths for the CSG accounting service flows, assigns a VLAN ID and optional name, and enters module CSG VLAN configuration mode.
Step 2	`Router(config-csg-vlan-client)# ip address 192.158.38.40 255.255.255.0`	Assigns an IP address to the CSG VLAN.
Step 3	`Router(config-module-csg) vlan 9 ft`	Defines VLAN 9 as a fault-tolerant VLAN.
Step 4	`Router(config-csg-vlan-client)# gateway 192.158.38.20`	Defines the client-side VLAN gateway.
Step 5	`Router(config-module-csg)# ip csg content content1`	Creates a CSG content definition and enters the CSG content configuration mode.
Step 6	`Router(config-csg-content)# ip any tcp www`	Defines Layer 3/Layer 4 parameters of the content.
Step 7	`Router(config-csg-vserver)# inservice`	Enables the server.
Step 8	`Router(config-module-csg)# vlan 3 server`	Creates the server-side VLAN that defines the Layer 2 paths for the CSG accounting service flows, assigns a VLAN ID and optional name, and enters module CSG VLAN configuration mode.
Step 9	`Router(config-csg-vlan-server)# ip address 192.158.39.30 255.255.255.0`	Assigns an IP address to the CSG VLAN.
Step 10	`Router(config-csg-vlan-server)# alias 192.158.39.20 255.255.255.0`	Assigns an alias address to the CSG.
Step 11	`Router(config-module-csg)# ft group` *ft-group-number* `vlan 9`	Enters fault-tolerant configuration mode and configures fault tolerance.
Step 12	`Router(config-module-csg)# show module csg ft`	Displays the state of the fault tolerant system.

To configure fault tolerance in module CSG configuration mode, perform this task:

	Command	Purpose
Step 1	`Router(config-module-csg)# ft group` *group-id* `vlan` *vlanid*	Configures fault tolerance and enters fault-tolerance configuration mode.
Step 2	`Router(config-csg-ft)# priority` *value*	Sets the priority of the CSG.
Step 3	`Router(config-csg-ft)# failover` *failover-time*	(Optional) Sets the time for a standby CSG to wait before becoming an active CSG.
Step 4	`Router(config-csg-ft)# heartbeat-time` *heartbeat-time*	(Optional) Sets the time before heartbeat messages are transmitted by the CSG.

This example shows how to set fault tolerance for connection redundancy in module CSG configuration mode:

```
Router(config-module-csg)# ft group 90 vlan 111
Router(config-csg-ft)# priority 10
Router(config-csg-ft)# failover 3
Router(config-cag-ft)# heartbeat-time 2
```

Configuring HSRP

This section provides an overview of a Hot Standby Router Protocol (HSRP) configuration (see Figure 4-5) and describes how to configure the CSGs with HSRP and failover on the Catalyst 6000 series switches.

HSRP Configuration Overview

Figure 4-5 shows that two Catalyst 6000 series switches, Switch 1 and Switch 2, are configured to route from a client-side network (10.100/16) to an internal CSG client network (10.6/16, VLAN 136) through an HSRP gateway (10.100.0.1). The configuration shows the following:

- The client-side network is assigned an HSRP group ID of HSRP ID 2.
- The internal CSG client network is assigned an HSRP group ID of HSRP ID 1.

Note HSRP group 1 must have tracking turned on so that it can track the client network ports on HSRP group 2. When HSRP group 1 detects any changes in the active state of those ports, it duplicates those changes so that both the HSRP active (Switch 1) and HSRP standby (Switch 2) switches share the same knowledge of the network.

In the example configuration, two CSGs (one in Switch 1 and one in Switch 2) are configured to forward traffic between a client-side and a server-side VLAN:

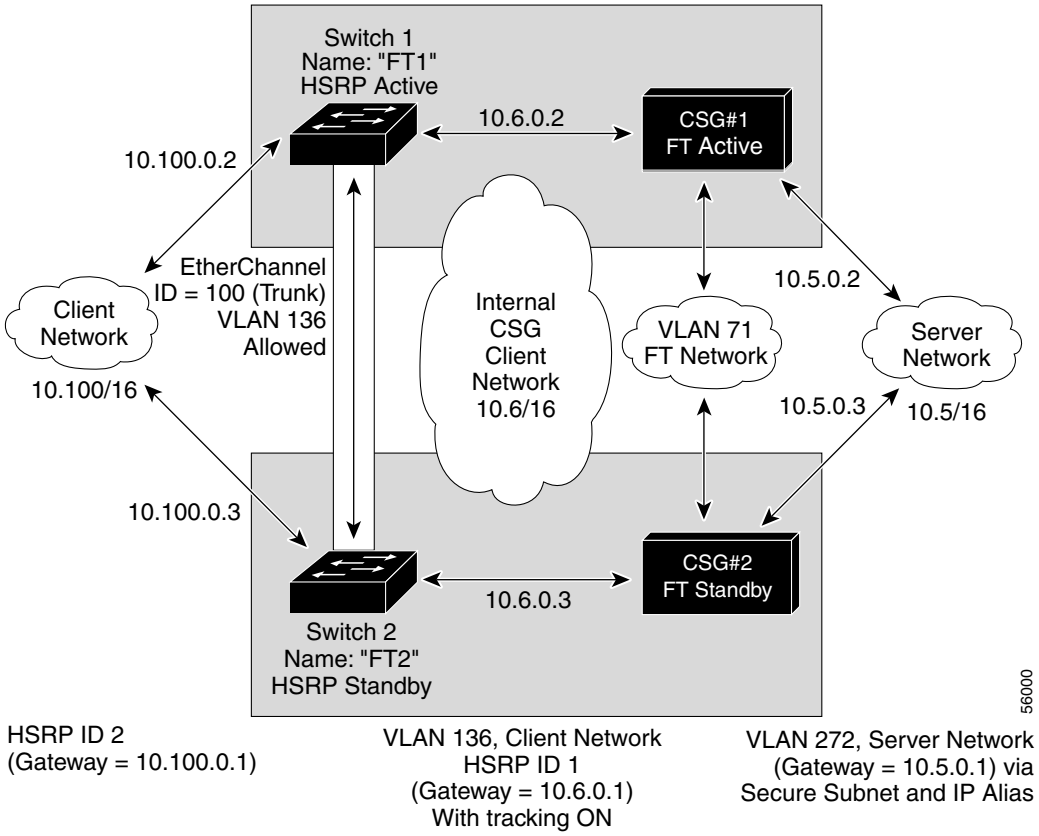
- Client VLAN 136 (The client VLAN is actually an internal CSG VLAN network; the actual client network is on the other side of the switch.)
- Server VLAN 272

The actual servers on the server network point to the CSG server network through an aliased gateway (10.5.0.1), allowing the servers to run a secure subnet.

In the example configuration, an EtherChannel is set up with trunking enabled, allowing traffic on the internal CSG client network to travel between the two Catalyst 6000 series switches.

Note EtherChannel protects against a severed link to the active switch and a failure in a non-CSG component of the switch. EtherChannel also provides a path between an active CSG in one switch and another switch, allowing the CSGs and switches to failover independently, providing an extra level of fault tolerance.

Figure 4-5 HSRP Configuration



Creating the HSRP Gateway

The following procedure describes how to create an HSRP gateway for the client-side network. The gateway is HSRP ID 2 for the client-side network. In this example, HSRP is set on Fast Ethernet ports 3/6.

To create an HSRP gateway, follow these steps:

Step 1 Configure Switch 1—FT1 (HSRP active) as follows:

```
Router(config)# interface FastEthernet3/6
Router(config)# ip address 10.100.0.2 255.255.0.0
Router(config)# standby 2 priority 110
Router(config)# standby 2 ip 10.100.0.1
```

Step 2 Configure Switch 2—FT2 (HSRP standby) as follows:

```
Router(config)#interface FastEthernet3/6
Router(config)# ip address 10.100.0.3 255.255.0.0
Router(config)# standby 2 priority 100
Router(config)# standby 2 ip 10.100.0.1
```

Creating Fault-Tolerant HSRP Configurations

This section describes how to create a fault-tolerant HSRP secure mode configuration. To create a nonsecure mode configuration, enter the commands described with these exceptions:

- Assign the same IP address to both the server-side and client-side VLANs.
- Do not use the **alias** command to assign a default gateway for the server-side VLAN.

To create fault-tolerant HSRP configurations, follow these steps.

Step 1 Configure VLANs on HSRP FT1 as follows:

```
Router(config)# module csg 5
Router(config-module-csg)# vlan 136 client
Router(config-csg-vlan-client)# ip address 10.6.0.245 255.255.0.0
Router(config-csg-vlan-client)# gateway 10.6.0.1
Router(config-csg-vlan-client)# exit

Router(config-module-csg)# vlan 272 server
Router(config-csg-vlan-server)# ip address 10.5.0.2 255.255.0.0
Router(config-csg-vlan-server)# alias 10.5.0.1 255.255.0.0
Router(config-csg-vlan-server)# exit

Router(config-module-csg)# vlan 71 ft

Router(config-module-csg)# ft group 88 vlan 71
Router(config-csg-ft)# priority 30
Router(config-csg-ft)# exit

Router(config-module-csg)# interface Vlan136
ip address 10.6.0.2 255.255.0.0
standby 1 priority 100
standby 1 ip 10.6.0.1
standby 1 track Fa3/6 10
```

Step 2 Configure VLANs on HSRP FT2 as follows:

```
Router(config)# module csg 6
Router(config-module-csg)# vlan 136 client
Router(config-csg-vlan-client)# ip address 10.6.0.246 255.255.0.0
Router(config-csg-vlan-client)# gateway 10.6.0.1
Router(config-csg-vlan-client)# exit

Router(config-module-csg)# vlan 272 server
Router(config-csg-vlan-server)# ip address 10.5.0.3 255.255.0.0
Router(config-csg-vlan-server)# alias 10.5.0.1 255.255.0.0
Router(config-csg-vlan-server)# exit

Router(config-module-csg)# vlan 71 ft
Router(config-module-csg)# ft group 88 vlan 71
Router(config-csg-ft)# priority 20
```

```
Router(config-csg-ft)# exit

Router(config-module-csg)# interface Vlan136
ip address 10.6.0.3 255.255.0.0
standby 1 priority 100
standby 1 ip 10.6.0.1
standby 1 track Fa3/6 10
```

Step 3 Configure EtherChannel on both switches as follows:

```
Router(console)# interface Port-channel100
Router(console)# switchport
Router(console)# switchport trunk encapsulation dot1q
Router(console)# switchport trunk allowed vlan 136
```

Note By default, all VLANs are allowed on the port channel.

Step 4 (Optional) To prevent problems, remove the server and the FT CSG VLANs as follows:

```
Router(console)# switchport trunk remove vlan 71
Router(console)# switchport trunk remove vlan 272
```

Step 5 Add ports to the EtherChannel as follows:

```
Router(console)# interface FastEthernet3/25
Router(console)# switchport
Router(console)# channel-group 100 mode on
```

Configuring Connection Redundancy

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

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

Stateful redundancy is not supported for RTSP connections. For all other connections, a new session is created when the backup CSG becomes active.

To configure connection redundancy, perform this task:

	Command	Purpose
Step 1	`Router(config)# ip csg content` *content-name*	Defines content for CSG accounting services, and enters CSG content configuration mode.
Step 2	`Router(config-csg-content)# ip` *ip-address* [*ip-mask*] *protocol port-number*	Defines the Layer 3/Layer 4 flows that can be processed by the CSG accounting services.
Step 3	`Router(config-csg-content)# replicate connection tcp`	Replicates the connection state for all TCP connections to the CSG content servers on the backup system.
Step 4	`Router(config-csg-content)# inservice`	Enables the content definition.

This example shows how to configure connection redundancy:

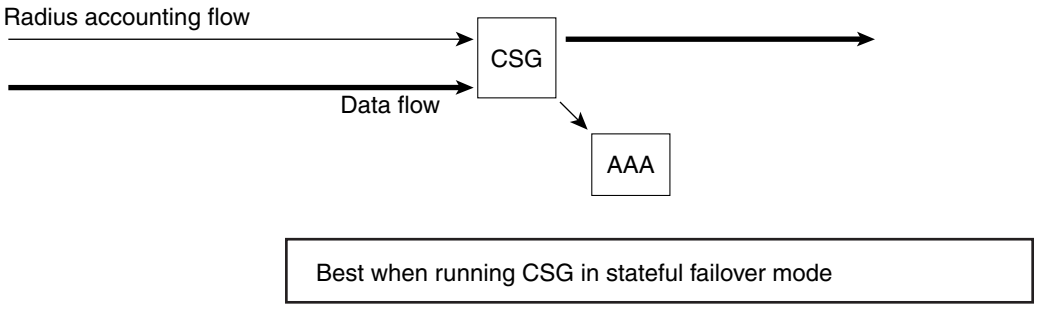
```
Router(config)# ip csg content CISCO
Router(config-csg-content)# ip 10.10.10.10 tcp telnet
Router(config-csg-content)# replicate connection tcp
Router(config-csg-content)# inservice
```

Configuring RADIUS Support: Learning Who the Subscriber Is

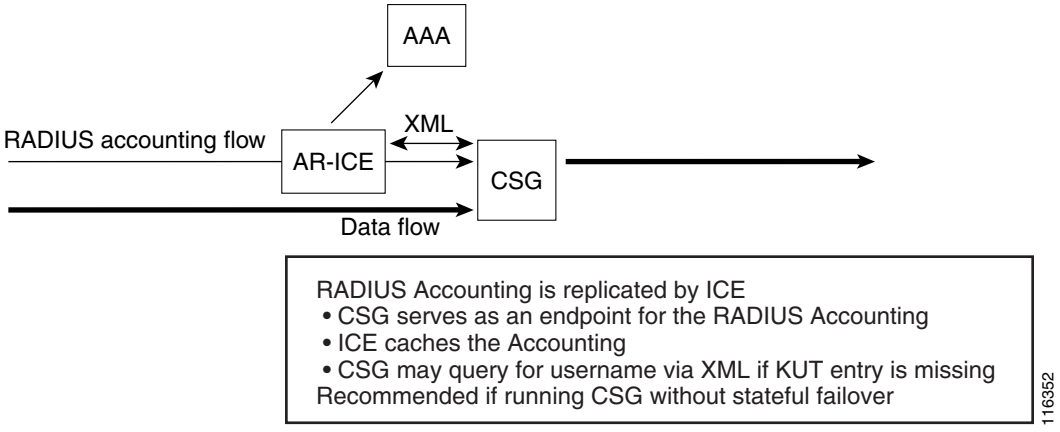
Figure 5-1 illustrates the placement of the CSG in the RADIUS accounting and data flows.

Figure 5-1 RADIUS Accounting and Data Flows

RADIUS accounting proxy or monitor



RADIUS accounting endpoint
plus Access Registrar - Identity Cache Engine (ICE)



This chapter contains the following information:

Configuring RADIUS Inspection: Endpoint

This configuration specifies the port number for the RADIUS accounting endpoint.

The CSG RADIUS features require that you configure the NAS to direct RADIUS messages to the CSG IP address (or to the alias address if this is a redundant configuration). You must also configure your NAS to the specific CSG port number. The following example illustrates the configuration:

```
module csg 3
  radius endpoint 1.2.3.4 key secret
```

To support RADIUS endpoint, the CSG requires a route to 255.255.255.255. You can configure the route by using the **gateway (module CSG VLAN)** command or the **route (module CSG VLAN)** command. For example:

gateway 31.0.0.6

or:

route 255.255.255.255 255.255.255.255 gateway 31.0.0.6

Note When the CSG2 is configured as a RADIUS endpoint, the CSG2 drops all RADIUS packets other than RADIUS Accounting-Request messages.

Configuring RADIUS Inspection: Proxy

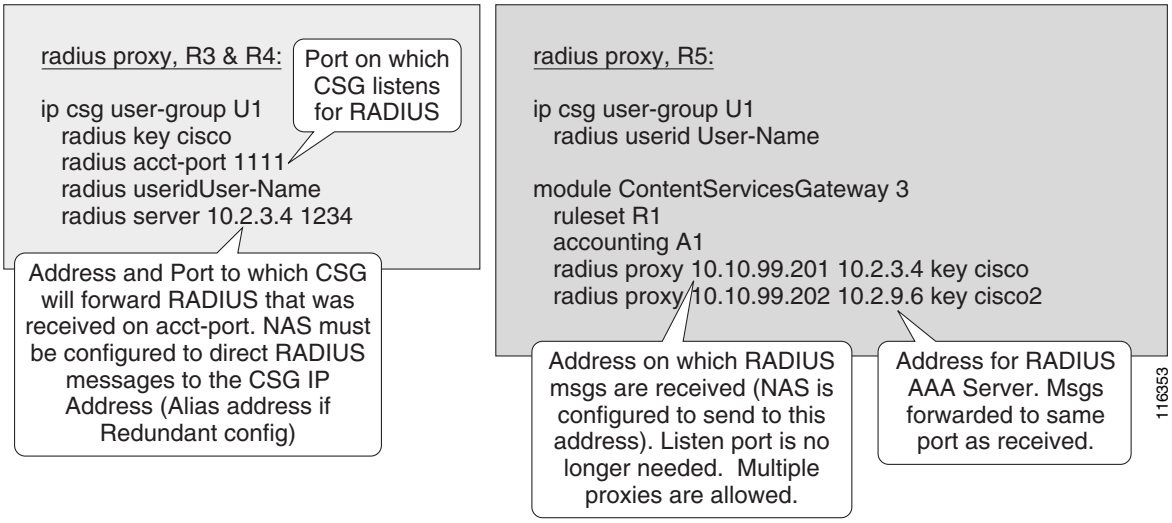
The CSG enhances the proxy function to allow operation with clients that use large numbers of port numbers. RADIUS proxy provides a way to remove the chance of routing errors (RADIUS is targeted at the CSG IP addresses directly), and must be used in place of RADIUS monitor when the CSGs are being load-balanced.

RADIUS proxy supports both RADIUS Access and RADIUS Accounting.

Note The old proxy function is still supported, and operates as before if you configure it in the old way. However, we strongly recommend that you use the new proxy support.

Figure 5-2 illustrates the differences between configurations.

Figure 5-2 RADIUS Proxy Configuration Changes



Using a CSG 3.1(3)C4(1) RADIUS configuration on the CSG 3.1(3)C5(1) or later results in the CSG 3.1(3)C4(1) behavior.

Configuring RADIUS Inspection: Monitor

RADIUS monitor provides a way to insert the CSG without changing the AAA or NAS addresses in the network. The CSG monitors the traffic between the RADIUS client and the RADIUS server, looking for RADIUS messages flowing through it that match the configured rule. The address of the server must be configured.

Optionally, a RADIUS key is configured. If the key is configured, the CSG parses and acts on the message only if the RADIUS Authenticator is correct. If the key is not configured, the CSG always parses the message. The message is forwarded regardless of the key being configured or correct. Here is a sample configuration:

```
ip csg user-group U1
  radius userid User-Name
  radius monitor 10.2.3.4 1234 key cisco --> Address, Port, and Key for RADIUS AAA Server.
  radius monitor 10.2.3.9 1234 key cisco2
  radius monitor 10.2.7.4 3901 key cisco --> Multiple AAA destinations can be monitored.
```

All RADIUS messages, including access messages, are forwarded, except when the IP or UDP headers specify a length larger than the physical packet size.

When configuring RADIUS monitor for a server that is in the same subnet as a CSG interface, you must first configure a dummy route for that server, such as:

route *ip-address* **255.255.255.255 gateway** *gw-ip-address*

where:

- *ip-address* is any IP address that is not used in the network
- *gw-ip-address* is the gateway IP address

Add a RADIUS monitor configuration only after you have added the dummy route.

Configuring RADIUS Inspection: Packet of Disconnect

This 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 CSG should 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 user-group G1
  radius userid User-Name
  radius pod attribute 44
  radius pod nas 1.1.1.0 1.1.1.255 1700 key secret
  radius pod nas 1701 key password
  radius pod timeout 30 retransmits 5

mod csg 3
  radius proxy 1.2.3.4 5.6.7.8 key secret
```

Configuring RADIUS Inspection: Associating a Table Name with a RADIUS Proxy or Endpoint

Interface awareness enables the CSG to distinguish between users and sessions that share the same IP address on different VLANs (that is, users and sessions with overlapping IP addresses). Interface awareness requires that each VLAN be associated with a table name. You can also associate the table name with a particular RADIUS proxy or endpoint.

To associate the table name with a particular RADIUS proxy, enter the following command in module CSG configuration mode, specifying the **table** keyword and a table name:

Command	Purpose
Router(config-csg-module)# **radius proxy** *csg_addr server addr* [*csg_source_addr*] [**key** [*encrypt*] *secret-string*] [**table** *table-name*]	Specifies that the CSG should be a proxy for RADIUS messages.

To associate the table name with a particular RADIUS endpoint, enter the following command in module CSG configuration mode, specifying the **table** keyword and a table name:

Command	Purpose
Router(config-csg-module)# **radius endpoint** *csg_addr* **key** [*encrypt*] *secret-string* [**table** *table-name*]	Identifies the CSG as an endpoint for RADIUS Accounting messages.

Configuring RADIUS Inspection: Preventing the CSG from Acknowledging Errors

By default, the CSG acknowledges the following errors:

1. The User Table entry cannot be created due to resource constraints.
2. The CSG parses the Accounting Request and encounters RADIUS protocol errors.
3. The CSG parses the Accounting Request and a billing plan is specified in the Accounting Request, but it does not match a billing plan in the CSG configuration.
4. The CSG parses the Accounting Request and a quota server is specified in the Accounting Request, but it does not match a quota server in the CSG configuration.
5. The CSG parses the Accounting Request and a connect service is specified in the Accounting Request, but it does not match a connect service in the CSG configuration.

   For errors 3, 4, and 5, the CSG can parse the configuration VSA from the Access-Accept. If the CSG uses any attribute from the Access-Accept that does not match the CSG configuration, the CSG does not send a RADIUS response to the Accounting Request.

For RADIUS endpoint and RADIUS proxy configurations, you can prevent the CSG from acknowledging these errors by entering the **no** form of the **radius ack error** command in CSG user group configuration mode.

For RADIUS accounting requests processed as a result of matching a **radius endpoint** command, the CSG does not send a RADIUS acknowledgement.

For RADIUS accounting requests processed as a result of matching a **radius proxy** command, the CSG does not forward the Accounting Request to the RADIUS server.

Extracting the Billing Plan ID Using RADIUS

Prior to the CSG 3.1(3)C5(1), the CSG required that the quota server provide the Billing Plan ID. The information had to be provisioned to the quota server, or the quota server had to act as a surrogate (retrieving from the authentication, authorization, and accounting (AAA) server in order to send to the CSG). It was not possible to distinguish between prepaid and postpaid users if the quota server was unavailable.

The CSG now adds the ability to extract the Billing Plan ID from RADIUS Access Accept using a CSG VSA. The following information is included:

- Attribute number: 26 (=vendor specific)
- Vendor ID: 9 (=Cisco)
- Subattribute: 1 (=Cisco generic)
- Format: csg:billing_plan= where the billing plan name appears after the equal sign (=). If the attribute is present, but no billing plan is specified, the user is postpaid.

The new **user-profile** command enables the billing plan function. If the CSG is configured to get the billing plan from RADIUS, and the billing plan sub-attribute is included in the RADIUS messages, the CSG does not query the quota server (that is, no User Profile Request). If the billing plan attribute is not present in the RADIUS messages by the time the CSG receives the Accounting Start with the user ID, the CSG queries the quota server.

Reporting Arbitrary RADIUS Attributes

The operator can specify a set of attributes to be extracted from RADIUS Accounting Start messages for each subscriber and reported with each transaction record.

Note VSAs (attribute 26) are not separable (all are sent).

The CSG saves these attributes for each subscriber and replaces them when a new Accounting Start is received.

For example, in a GPRS environment you can use this capability as follows:

- NAS-IP-Address (4) identifies the GGSN to which the subscriber is tunneled.
- SGSN IP (26/10415/6) identifies the SGSN the subscriber is accessing.
- Acct-session-ID (44) uniquely identifies the session on this NAS and can be used for correlation to GGSN accounting records.

RADIUS Attributes Required for CSG User Table

The User Table identifies all users known to the CSG. The 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 CSG requires the following RADIUS attributes in the RADIUS Accounting Start in order to build an entry for a user in the CSG User Table 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

When the CSG 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 CSG receives the RADIUS Accounting Start message with the user ID, it builds a User Table entry using the cached information.

Note Cached information is not displayed in the output of the **show module csg accounting users** command.

Configuring Prepaid Support

This chapter contains the following information related to the CSG support for prepaid billing:

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, perform this task:

	Command	Purpose
Step 1	`Router (config-csg-module)# ip csg billing` *billing-plan-name*	Defines a billing plan to be used for prepaid billing, and enters CSG billing configuration mode.
Step 2	`Router (config-csg-billing)# service` *service-name*	Associates a service with a CSG billing plan.
Step 3	`Router # show module csg` *slot* `billing [detail] {all | plan` *billing-plan-name*`}`	Displays statistics and counters for the CSG billing.

The following example shows how to define a prepaid billing plan:

```
ip csg billing REGULAR
 service MOVIES
 service BROWSING
```

When a CSG prepaid user 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**. Often, the reservation 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 CSG might make additional requests for quota from the quota server.

Prior to this enhancement, the CSG would limit the reservation size to the size of the intermediate byte count, which resulted in additional records sent to the BMA. Now, you can limit the size of the reservation per IP session to reduce the number of requests to the quota server.

To configure a maximum amount of quota reserved for a prepaid IP user session, configure the following in module CSG configuration mode:

`Router (config-module-csg)# variable CSG_BASIS_BYTE_RESERVED_MAX` *quota*

Prepaid Billing with Policies Configuration Example

The following example shows a CSG configuration for prepaid billing with policies:

```
ip csg map TRAINING url
 match url *.edu/*
!
ip csg policy TRAINING
 report radius attribute type http
 url-map TRAINING
!
ip csg map AUCTION_HOUSE url
 match url *.auction_house.com/*
!
ip csg policy AUCTION_HOUSE
 accounting type http customer-string AUCTION_HOUSE
 url-map AUCTION_HOUSE
!
ip csg map MOVIES url
 match url *.movies_(comedy|action|drama).com/*.mpeg
!
ip csg policy MOVIES_COMEDY
 accounting type http customer-string MOVIES_COMEDY
 url-map MOVIES
!
ip csg policy MOVIES_ACTION
 accounting type http customer-string MOVIES_ACTION
 url-map MOVIES
!
ip csg content MOVIES_COMEDY
 ip 172.18.45.0/24 tcp 8080
 policy MOVIES_COMEDY
 inservice
!
ip csg content MOVIES_ACTION
 ip 66.33.78.0/24 tcp 80
 policy MOVIES_ACTION
 inservice
!
ip csg content AUCTION_HOUSE
 ip 216.32.120.0/24 tcp 8080
 policy AUCTION_HOUSE
 vlan AUCTION_HOUSE
 inservice
!
ip csg content WAKETECH
 ip 48.33.0.0/16 tcp 80
 policy TRAINING
 inservice
!
ip csg ruleset R1
 content MOVIES_COMEDY
 content MOVIES_ACTION
 content AUCTION_HOUSE
 content WAKETECH
!
ip csg weight DOUBLE 2
!
ip csg service MOVIES
 content MOVIES_COMEDY policy MOVIES_COMEDY
 content MOVIES_ACTION policy MOVIES_ACTION weight DOUBLE
!
ip csg service BROWSING
```

```
 basis fixed
 content AUCTION_HOUSE policy AUCTION_HOUSE
 content WAKETECH policy TRAINING
!
ip csg billing FREE_BROWSING
 service MOVIES
!
ip csg billing REGULAR
 service MOVIES
 service BROWSING
!
ip csg user-group G1
 entries max 100000
 database 10.1.2.3 11111
 quota server 10.1.4.5 888 1
 quota server 10.1.6.7 999 2
 radius key secretpassword
 redirect nat 10.33.33.3
!
ip csg accounting A1
 user-group G1
 agent local-port 3775
 agent 10.1.2.4 11112 1
 agent 10.1.2.5 11113 2
 records max 250
 inservice
!
mod csg 5
 vlan 30 client AUCTION_HOUSE
  ip address 123.44.50.6 255.255.255.0
  gateway 123.44.50.1
 vlan 40 server
  ip address 123.46.50.6 255.255.255.0
  alias 123.60.7.6 255.255.255.0
  route 123.50.0.0 255.255.0.0 gateway 123.44.50.1
 ruleset R1
 accounting A1
```

PSD Configuration for the CSG

Communicating Between the PSD and the CSG

This appendix offers one example of how to configure a CSG to communicate with the Cisco Persistent Storage Device (PSD). There are other variations that also work.

Before you configure the CSG to communicate with the PSD, you must determine the following configuration details:

- PSD VLAN number
- PSD IP address
- CSG IP address
- VLAN interface IP address

Note The PSD, the CSG, and VLAN interface IP addresses must be unused addresses in the same subnet. Additionally, if you want to perform software upgrades and FTP recovery of data files, the selected IP addresses must be in the same subnet as your default gateway.

If you plan to configure a Domain Name System (DNS) on the PSD, you must determine the following configuration details.

- PSD host name
- Domain name
- Domain name server addresses

There are additional CSG commands that are used to set up user groups, agents, quota servers, inservice, and so on. This appendix presents a minimal sample of what is required to configure the CSG that the PSD is to use.

This appendix provides the following information:

Setting up the CSG to Communicate with the PSD

To enable the CSG to communicate with the PSD, perform the following tasks on the Supervisor:

Step 1 If you have not already done so, create a VLAN on which the CSG and PSD can communicate, using the following commands:

```
Router> enable
Router# vlan database
Router(vlan)# vlan 55
Router(vlan)# exit
```

Note You can use an existing client VLAN on the CSG rather than creating a client VLAN, but we do not recommend doing so. If you do so, you tie communication with the PSD to a virtual server whose configuration (or unconfiguration) is driven by content billing requirements. If that VLAN is disabled to meet content billing requirements, communication with the PSD is interrupted.

Step 2 Use the following commands to associate a specific PSD to a CSG accounting group. This is the same IP address that is to be assigned to the PSD.

```
Router(config)# ip csg accounting name
Router(config-csg-acct)# record-storage local-port 2000
Router(config-csg-acct)# record-storage 172.18.12.1 255.255.255.0
Router(config-csg-acct)# exit
Router(config)#
```

You must use a **record-storage** command to specify the *local-port* before you use a second **record-storage** command to specify the *ip address* and *port* of the record-storage server.

In this example, the first **record-storage** command sets the local port, which is the source port from which the CSG sends packets to the record-storage server and the port on which it listens for responses. You can set this local-port to any available port.

The second **record-storage** command sets the destination address for packets going to the PSD.

Unless you are using a record-storage server other than the PSD, you need not specify the *port* parameter. However, if you omit the *port* argument in the second **record-storage** command, the CSG defaults to port 3386. (The PSD listens only on port 3386.) If you are using a record-storage server other than the PSD, and that server is listening on another port, then you must specify that port in the first **record-storage** command.

Step 3 Use the following commands to define a client VLAN over which the CSG and PSD can communicate.

```
Router(config)# module csg number
Router(config-csg-module)# vlan 55 client name
Router(config-csg-vlan-client)# ip address 172.18.12.2 255.255.255.0
Router(config-csg-vlan-client)# end
```

When you define the client VLAN, keep the following considerations in mind:

- The client VLAN on the CSG must have the same VLAN number as the corresponding VLAN interface on the Supervisor, and their IP addresses must be in the same subnet.
- Do not target billable client traffic to client VLAN on the CSG.
- If you are configuring more than one CSG, you must allow enough IP addresses to cover the number of CSGs in your chassis, plus two—one for the PSD IP address, and one for the VLAN interface IP address. Additionally, the subnet you choose must have room for all of the CSGs, plus one.

Step 4 (Optional) Use the following commands to allow traffic to be routed from the VLAN on which the PSD is configured to your default gateway. This step, which requires access to an FTP server, is necessary if you intend to upgrade the software on the PSD. In addition, if you are using DNS, this configuration allows you to perform name resolution to your name servers:

```
Router# conf t
Router(config)# interface FastEthernet 5/12
Router(config-if)# no ip address
Router(config-if)# switchport
Router(config-if)# switchport access vlan 55
Router(config-if)# switchport mode access
Router(config-if)# exit
Router(config)# interface vlan 55
Router(config-if)# ip address 172.18.12.3 255.255.255.0
Router(config-if)# end
```

Setting Up the PSD to Communicate with the CSG

To enable the PSD to communicate with the CSG, perform the following tasks on the Supervisor:

Step 1 Assign the PSD to a VLAN, using the following commands:

```
Router# config term
Router(config)# persistent-store module 3 vlan 55
```

Step 2 Assign an IP address to the PSD, using the following commands:

```
Router# session slot 3 proc 1
root@localhost.localdomain# ip address 172.18.12.2 255.255.255.0
root@localhost.localdomain# ip gateway 172.18.12.3
root@localhost.localdomain# ip host psd1 *
root@psd1.localdomain# ip domain cisco.com *
root@psd1.cisco.com# ip nameserver 64.11.22.1 64.11.22.2 *
root@psd1.cisco.com# exit
```

When assigning an IP address to the PSD, keep the following considerations in mind:

- This IP address must be in the same subnet as the IP address of the VLAN configured in Step 3 in the "Setting up the CSG to Communicate with the PSD" section on page A-2.
- The IP address used in the **ip gateway** command must be the same IP address that was assigned to the VLAN interface configured in Step 3 in the "Setting up the CSG to Communicate with the PSD" section on page A-2.

Note If you change the PSD address, and you are already billing on your CSGs, you must also change the record storage destination.

Command Reference

This appendix documents only new or modified commands necessary to configure and monitor the CSG for content billing. All other commands used with this product (those that already exist and have not been modified) are documented in either the Cisco IOS Release 12.2 command reference publications or in the IOS Server Load Balancing feature module.

- **show module csg accounting, page B-163** (modified command)
- **show module csg arp, page B-167**
- **show module csg billing, page B-168**
- **show module csg clock, page B-169**
- **show module csg conns, page B-170**
- **show module csg content, page B-172**
- **show module csg ft, page B-174**
- **show module csg stats, page B-175**
- **show module csg status, page B-176**
- **show module csg tech-support, page B-177**
- **show module csg variable, page B-184**
- **show module csg vlan, page B-185**
- **snmp-server enable traps csg, page B-186**
- **table (module CSG VLAN), page B-187** (new command)
- **url-map, page B-188**
- **user-group, page B-190**
- **user-profile server, page B-191**
- **variable (module csg), page B-193** (modified command)
- **verify, page B-198**
- **verify confirmation, page B-199**
- **vlan (CSG content), page B-200**
- **vlan (module CSG), page B-201**
- **zero-quota abort type, page B-203**

accounting (CSG policy)

To define the accounting type and customer string for all flows that comply with a CSG billing policy, use the **accounting** command in CSG policy configuration mode. To delete the rules, use the **no** form of this command.

accounting [**type** {**http** | **ftp** | **other** | **wap** {**connection-oriented** | **connectionless**}| **smtp** | **pop3** | **rtsp** | **imap**} [**customer-string** *string*]

no accounting [**type** {**http** | **ftp** | **other** | **wap** {**connection-oriented** | **connectionless**}| **smtp** | **pop3** | **rtsp** | **imap**} [**customer-string** *string*]

Syntax Description

type http	Indicates HTTP accounting. For HTTPS, use **type other** for port number 443.
type ftp	Indicates FTP accounting, and enables Layer 7 inspection of FTP control sessions.
type other	Indicates some other type of IP accounting, such as IP, TCP, or UDP. This is the default setting. For HTTPS, use **type other** for port number 443.
type wap	Indicates WAP accounting.
connection-oriented	Defines the type of WAP traffic as connection-oriented.
connectionless	Defines the type of WAP traffic as connectionless.
type smtp	Enables reporting of SMTP data records.
type pop3	Enables reporting of POP3 data records.
type rtsp	Enables reporting of RTSP data records.
type imap	Enables reporting of IMAP Data Records.
customer-string *string*	(Optional) 1-to-16-byte string to be output to the generated accounting records.

Defaults

The default accounting type is **other**.

Command Modes

CSG policy configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.
3.1(1)C4(1)—12.2(14)ZA	The **type wap** keyword was added.
3.1(1)C4(3)—12.2(14)ZA2	The **smtp** and **pop3** keywords were added
3.1(3)C5(1)—12.2(17d)SXB	The **rtsp** keyword was added.
3.1(3)C5(5)—12.2(17d)SXD	The **imap** keyword was added.

Usage Guidelines

This command is required if accounting records are to be generated for content that satisfies the associated CSG billing policy.

Prepaid service matches are based on the IP address and port number of the control connection to the RTSP server IP.

The default setting for this command (**accounting type other**) is displayed in the output of the **show run** command.

Specifying **type ftp** requires a control TCP connection to server port 21.

Specifying **type rtsp** requires a control TCP connection to server port 554.

If you specify both **type http** and any other type (**type other**, **type ftp**, **type imap**, and so on) for a service, and you enable service-level CDR summarization for the service, the CSG's incremental and cumulative byte counts are not valid. This is because they are a mix of TCP bytes (for the HTTP traffic) and IP bytes (for all other traffic).

When configuring header and URL maps, keep the following considerations in mind:

- Header and URL maps are valid only with accounting types HTTP, RTSP, and WAP.
- If you do not specify an accounting type, the CSG assumes that the session is an HTTP session, and packets matching the policy are not billed (that is, no quota is used, and no CDR is generated).

Examples

The following example shows how to define accounting types and customer strings:

```
ip csg policy WSP_CON_P
    accounting type wap connection-oriented

ip csg policy WAP_NOCON_P
    accounting type wap connectionless

ip csg content WAP_CON
    ip any udp 9201
    policy WAP_CON_P

ip csg content WAP_CONLESS
    ip any udp 9200
    policy WAP_NOCON_P

ip csg policy SMTP
    accounting type smtp

ip csg policy POP3
    accounting type pop3

ip csg content SMTP
    ip any tcp 25
    policy SMTP
    inservice

ip csg content POP3
    ip any tcp 110
    policy POP3
    inservice

ip csg policy RTSP
    accounting type rtsp

ip csg content RTSP
    ip any tcp 554
```

```
    policy RTSP
    inservice

ip csg policy IMAP
    accounting type imap

ip csg content IMAP
    ip any tcp 143
    policy IMAP
    inservice
```

Related Commands

Command	Description
ip csg policy	Defines a policy for qualifying flows for the CSG accounting services, and enters CSG policy configuration mode.

accounting (module CSG)

To download a configured accounting service to a CSG card, use the **accounting** command in module CSG configuration mode. To delete the downloaded accounting service, use the **no** form of this command.

accounting *service-name*

no accounting *service-name*

Syntax Description

service-name	Name of the configured accounting service to be downloaded.

Defaults

No default behavior or values.

Command Modes

Module CSG configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

You must specify at least one client VLAN and one server VLAN in order for the accounting service to be placed inservice. Otherwise, no traffic can flow to the accounting service.

You must configure at least one ruleset in order for the accounting service to be placed INSERVICE.

Examples

The following example shows how to download the CSG accounting service A1 to the CSG card in slot 4:

```
module csg 4
 accounting A1
 ruleset R1
```

Related Commands

Command	Description
module csg	Enters module CSG configuration mode for a specified slot.

activation

To specify the activation mode for a Connection Duration service, use the **activation** command in CSG service configuration mode. To restore the default setting, use the **no** form of this command.

activation [**automatic** | **user-profile**]

no activation

Syntax Description

automatic	Activate the Connection Duration service, unless the billing profile indicates that no service should be activated. If you specify the **automatic** keyword, the CSG activates the Connection Duration service in the user'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	Activate 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 CSG 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 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

CSG service configuration mode

Command History

Release	Modification
3.1(3)C5(5)—12.2(18)SXD	This command was introduced.

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	Defines a content billing service, and enters CSG service configuration mode.

agent (CSG accounting)

To define the primary and backup Billing Mediation Agents (BMAs) to which billing records are to be sent, use the **agent** command in CSG accounting configuration mode. To remove a BMA from the list of agents, use the **no** form of this command.

agent *ip-address port-number priority*

no agent *ip-address port-number priority*

Syntax Description

ip-address	IP address of the BMA you wish to define. The CSG differentiates BMAs based on IP addresses. When you configure a BMA, make sure its IP address matches on both the active CSG and on the backup CSG.
port-number	Port number of the BMA you wish to define. The valid range is 1 to 65535. The CSG differentiates BMAs based on port numbers. When you configure a BMA, make sure its port number matches on both the active CSG and on the backup CSG.
priority	Allows you to define primary and backup BMAs. You must specify at least one agent. The priority specifies the order of preference of the agents. A lower number indicates a higher priority. If the current agent becomes unusable, the CSG uses the highest priority BMA available. Priorities for different agents do not have to be contiguous. That is, you can have three agents with priorities 1, 5, and 10. The valid range of priorities is 1 to 1000.

Defaults

Primary and backup BMAs are not defined.

Command Modes

CSG accounting configuration

Command History

Release	Modification
2.2(1)C(1)—12.1(11b)E3	This command was introduced.

Usage Guidelines

Accounting records are sent to only those agents identified in the **agent** command. This provides a measure of security to ensure that records are not sent to unauthorized systems.

Note The CSG does not support multiple agents with the same IP address.

Examples

The following example shows how to configure a primary BMA with priority 1, and a backup BMA with priority 2, for the CSG accounting service A1:

```
ip csg accounting A1
 user-group G1
 agent activate 2
 agent local-port 3775
 agent 10.1.2.4 11112 10
 agent 10.1.2.5 11113 20
 keepalive 3
 records batch
 records http-statistics
 records intermediate bytes 100000 time 3600
 records max 250
 inservice
```

Related Commands

Command	Description
ip csg accounting	Defines content-based accounting as a service.
agent activate	Enables support for multiple active BMAs.
agent local-port	Defines the port on which the CSG listens for packets from the BMAs.

agent activate

To enable support for multiple active Billing Mediation Agents (BMAs), use the **agent activate** command in CSG accounting configuration mode. To disable support for multiple active BMAs, use the **no** form of this command.

agent activate [*number* [**sticky** *seconds*]]

no agent activate [*number* [**sticky** *seconds*]]

Syntax Description

number	Number of BMAs that the CSG 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 valid range is 1 through 10. The default value is 1.
sticky *seconds*	Number of seconds of inactivity after which a sticky object is to be deleted. The CSG creates a sticky object to ensure that all the billing records for a user 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 CSG cannot access the user ID database), the CSG creates two sticky objects, one for the source IP address and one for the destination IP address. These entries are removed from the table based on inactivity. Note that entries that contain a user ID do not age out; they are removed only by RADIUS messages. The valid range is 1 second through 64,000 seconds. The default value is 30 seconds.

Defaults

The default value for *number* is 1.

The default value for *seconds* is 30 seconds.

Command Modes

CSG accounting configuration

Command History

Release	Modification
2.2(3)C2(1)—12.1(13)E	This command was introduced.

Examples

The following example shows how to enable support for multiple active BMAs for the CSG accounting service A1. In this example, up to two BMAs can be active at the same time:

```
ip csg accounting A1
 user-group G1
 agent activate 2
 agent local-port 3775
 agent 10.1.2.4 11112 10
 agent 10.1.2.5 11113 20
 keepalive 3
 records batch
 records http-statistics
 records intermediate bytes 100000 time 3600
 records max 250
 inservice
```

Related Commands

Command	Description
agent (CSG accounting)	Defines the primary and backup BMAs to which to send billing records.
agent local-port	Defines the port on which the CSG listens for packets from the BMAs.
ip csg accounting	Defines content-based accounting as a service.

agent local-port

To define the port on which the CSG is to listen for packets from the Billing Mediation Agents (BMAs), use the **agent local-port** command in CSG accounting configuration mode. To revert to the default value, use the **no** form of this command.

agent local-port *port-number*

no agent local-port

Syntax Description

port-number	Port number on which the BMA is to listen. The valid range is 1 to 65535. The default value is 3386, the port number prescribed by GTP', the protocol used to send accounting records.

Defaults

The default port number is 3386.

Command Modes

CSG accounting configuration

Command History

Release	Modification
2.2(1)C(1)—12.1(11b)E3	This command was introduced.

Usage Guidelines

This command accommodates BMAs that configure a port number that is different from the GTP' default.

This local port must be unique with respect to any other local port configured, such as the quota server local port.

Note The CSG drops requests (such as nodealive, echo, and redirect requests) unless they come from a configured BMA IP address. The CSG also verifies IP addresses contained in NodeAddress IEs against the configured list of BMAs. If there is no match, the CSG drops the request. The CSG does not look at a request's source port, replying to the same port from which the request came.

Examples

The following example shows how to specify local port 3775 as the port on which the CSG listens, instead of the default port, for the CSG accounting service A1:

```
ip csg accounting A1
 user-group G1
 agent activate 2
 agent local-port 3775
 agent 10.1.2.4 11112 10
 agent 10.1.2.5 11113 20
 keepalive 3
 records batch
 records http-statistics
 records intermediate bytes 100000 time 3600
```

```
records max 250
inservice
```

Related Commands

Command	Description
agent (CSG accounting)	Defines the primary and backup BMAs to which to send billing records.
agent activate	Enables support for multiple active BMAs.
ip csg accounting	Defines content-based accounting as a service.

alias (module CSG VLAN)

To assign multiple IP addresses to the CSG, use the **alias** command in module CSG VLAN configuration mode. To remove an alias IP address from the configuration, use the **no** form of this command.

alias *ip-address netmask*

no alias *ip-address netmask*

Syntax Description

ip-address	Alias IP address; a maximum of 256 addresses are allowed.
netmask	Network mask.

Defaults

No default behavior or values.

Command Modes

Module CSG VLAN configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

This command allows you to place the CSG on a different IP network than real servers without using a router.

You can also use this command in redundant configurations to ensure that the gateway can access the same IP address regardless of which the CSG is active.

You can specify more than one **alias** command for each VLAN.

Examples

The following example shows how to use the **alias** command to assign multiple IP addresses to the CSG:

```
vlan 301 client
 name TO-GGSN-MS-APN
 gateway 31.0.0.10
 ip address 31.0.0.21 255.255.255.0
 route 11.0.0.0 255.255.0.0 gateway 31.0.0.1
 route 11.1.0.0 255.255.0.0 gateway 31.0.0.2
 route 11.2.0.0 255.255.0.0 gateway 31.0.0.3
 route 11.3.0.0 255.255.0.0 gateway 31.0.0.4
 alias 31.0.0.51 255.255.255.0
```

Related Commands

Command	Description
show module csg variable	Displays the list of VLANs.
vlan (module CSG)	Creates a client or server VLAN that defines the Layer 2 paths for the CSG accounting service flows, assigns a VLAN ID and optional name, and enters module CSG VLAN configuration mode.

aoc confirmation

To configure a token for use in advice of charge (AoC) URL-rewriting, use the **aoc confirmation** command in CSG user group configuration mode. To remove the token, use the **no** form of this command.

aoc confirmation *token*

no aoc confirmation

Syntax Description

token	A string of up to 15 alphanumeric characters. To insert a question mark (?) in the string, enter Ctrl-V, then the question mark. To insert a question mark in an editing document, use ASCII code 22. Use TFTP instead of copy-and-paste to keep the question mark.

Defaults

No default behavior or values.

Command Modes

CSG user group configuration

Command History

Release	Modification
3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.
3.1(3)C5(5)—12.2(18)SXD	Support was added for WAP content authorization URL-rewriting.

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 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 both HTTP and WAP content authorization URL-rewriting.

Examples

The following example specifies a token for advice of charge (AoC) URL-rewriting:

```
ip csg user-group A1
    aoc confirmation ?CSG_AOC_OK
```

Related Commands

Command	Description
authorize content	Enables content authorization for a service.

assign

To associate an IP address with a transport-type value, use the **assign** command in CSG transport-type configuration mode. To remove the association, use the **no** form of this command.

assign *ip-address value*

no assign *ip-address value*

Syntax Description

ip-address	IP address.
value	Transport-type value in the range 1 to 255.

Defaults

No default behavior or values.

Command Modes

CSG transport-type configuration

Command History

Release	Modification
3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.

Usage Guidelines

The transport-type is used to classify data traffic based on its access path using the NAS-IP reported in RADIUS. Use the **assign** command to associate IP addresses with transport-type values. Transport-type information is reported in fixed record format CDRs.

Examples

The following example associates an IPv4 address with a transport-type value:

```
ip csg transport-type
  assign 1.2.3.4 34
```

Related Commands

Command	Description
records format	Specifies **variable** or **fixed** CDR format.
hostname	Specifies a variable hostname for a CSG module.
owner name	Specifies the name of a service owner.
owner id	Specifies an identifier for a service owner.
ip csg transport-type	Classifies data traffic based on its access path.
class	Specifies a service class value.

authorize content

To enable Advice of Charge and Per-Event Filtering for the CSG, use the **authorize content** command in CSG service configuration mode.

authorize content

Syntax Description

There are no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

CSG service configuration mode

Command History

Release	Modification
3.1(3)C4(1)—12.2(14)ZA2	This command was introduced.

Usage Guidelines

If this command is configured, the CSG uses the new ContentAuthReq to alert the quota server of a new transaction, and allows it to direct the CSG (using ContentAuthResp) to perform any of four mutually exclusive actions:

- FORWARD: Instructs the CSG to forward the flow without altering the destination.
- DROP: Instructs the CSG to drop all packets for this flow.
- REDIRECT-NAT: Instructs the CSG to forward all packets for this flow to the IP address provided in the ContentAuthResp. The CSG translates the packet to the IP address and port that were provided.
- REDIRECT-URL: Instructs the CSG to redirect the client request to the URL provided in the ContentAuthResp. The CSG sends a Layer 7 redirect to the client (for example, HTTP 302 response) that contains the redirect URL.

Examples

The following example illustrates the **authorize content** command:

```
Router(config)# ip csg service service_name
Router(config-csg-service)# authorize content
```

Related Commands

Command	Description
ip csg service	Defines a content billing service, and enters CSG service configuration mode.
aoc confirmation	Configures a token for use in advice of charge (AoC) URL-rewriting.

basis

To specify the billing basis for a CSG content billing service, use the **basis** command in CSG service configuration mode. To use the default billing basis, use the **no** form of this command.

basis [**byte** [**exclude mms**] {**ip** | **tcp**} | {**fixed** [**exclude mms**] | **second** [**connect**]}]

no basis [**byte** {**ip** [**exclude mms**] | **tcp**} | {**fixed** [**exclude mms**] | **second** [**connect**]}]

Syntax Description

byte ip	Billing charge is a function of the IP data volume processed during the user's session. This is the default setting. **Note** We strongly recommend that you do not specify **basis byte ip** for HTTP billing. If you do so, the byte counts are the same as if you had specified **basis byte tcp**.
exclude mms	(Optional) MMS traffic is not counted against quota for prepaid users when **exclude mms** is configured, and the user is authorized for the service. You can configure **exclude mms** with both **byte ip** and **fixed**, but not with **byte tcp** or **second**.
byte tcp	Billing charge is a function of the TCP data volume processed during the user's session. **Note** Supplemental usage reporting always reports IP bytes, even if the billing basis is configured for TCP bytes.
fixed	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	Billing charge is duration-based for the CSG service. Unless the **connect** keyword is also configured, the billing is for the service duration time.
connect	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 module csg accounting** command are updated only when there is a Service Reauthorization Request for new quota.

Defaults

The default setting is **byte ip** (billing charge is a function of the IP data volume processed).

Command Modes

CSG service configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.
3.1(1)C4(1)—12.2(14)ZA	The **exclude mms** keyword was added.

Release	Modification
3.1(3)C5(1)—12.2(17d)SXB	The **second** keyword was added.
3.1(3)C5(5)—12.2(18)SXD	The **connect** keyword was added.

Usage Guidelines

By default the CSG treats MMS traffic like any other WAP traffic, and generates appropriate prepaid and postpaid WAP statistics reports. The content type distinguishes it as MMS traffic. MMS traffic is not counted against quota for prepaid users when either **basis byte ip exclude mms**, or **basis fixed exclude mms** is configured on the service.

For HTTP billing, configuring **basis byte tcp** allows counting of only TCP payload and exclusion of overhead for network retransmission. With this option, the CSG excludes IP and TCP headers from volume counts:

- Prior to the CSG 3.1(3)C5(5), the byte counting is limited to TCP payload plus one byte representing each SYN, and one byte representing the first FIN.
- In the CSG 3.1(3)C5(5) and later, the byte counting is limited to TCP payload.

Retransmitted packets are also not counted.

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

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 CSG billing configuration mode, then enter the **basis second connect** command in CSG service configuration mode.

Because IMAP metering is byte-based, you cannot configure both **meter imap** and **basis fixed** or **basis second** in the same service. Only **basis byte** is meaningful with **meter imap**.

Examples

The following example shows how to specify fixed billing for the CSG service MOVIES:

```
ip csg service MOVIES
  basis fixed
  content MOVIES_COMEDY policy MOVIES_COMEDY
  content MOVIES_ACTION policy MOVIES_ACTION weight DOUBLE
  idle 12
```

The following commands are used to configure Service Duration Billing for the OFF_NET service.

```
ip csg service OFF_NET
  basis second
  meter minimum 60
  content ANY policy HTTP
  content ANY policy ANY
```

Related Commands

Command	Description
ip csg service	Defines a content billing service, and enters CSG service configuration mode.
meter increment	Specifies the increments for debiting quota upon completion of a service configured for Service Duration Billing.

class

To specify a service class value, use the **class** command in CSG service configuration mode. To remove the owner ID, 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

No default behavior or values.

Command Modes

CSG service configuration

Command History

Release	Modification
3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.

Usage Guidelines

Class is used with fixed-record format to identify a service class value. This value is opaque to the CSG and only has meaning for the administrator. It is reported as tariff-class in fixed record format 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	Defines a content billing service, and enters CSG service configuration mode.
ip csg transport-type	Classifies data traffic based on its access path.
mode	Specifies that a billing plan is postpaid or prepaid.
records format	Specifies **variable** or **fixed** CDR format.
hostname	Specifies a variable hostname for a CSG module.
owner name	Specifies the name of a service owner.
owner id	Specifies an identifier for a service owner.
assign	Associates an IPv4 address with a transport-type value.

clear module csg

To clear the CSG, use the **clear module csg** command in privileged EXEC mode.

clear module csg {*slot* | **all**} {**core-dump** | **counters**}

Syntax Description

slot	Indicates the CSG's location in the switch. The range is from 1 through 9.
all	Indicates that the command is to apply to all CSGs in the switch.
core-dump	Clears the CSG core dump.
counters	Clears all CSG statistics.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Examples

The following example clears all statistics for all of the CSGs in the switch:

```
clear module csg all counters
```

clear module csm

To clear the CSG, use the **clear module csm** command in privileged EXEC mode.

clear module csm {*slot* | **all**} {**arp-cache** *ip-address* | **connections** [**real** | **vserver**] | **counters** | **ft active** | **linecard-configuration** | **sticky** [*sticky-group* | **all**]}

Syntax Description

slot	Indicates the CSG's location in the switch. The range is 1 through 9.
all	Indicates that the command is to apply to all CSGs in the switch.
arp-cache *ip-address*	Clears the Address Resolution Protocol (ARP) cache for the specified CSG.
connections	Clears connections for the specified CSG. All connections are cleared for the specified CSG; use this command to clear selected connections.
real	(Optional) Clears connections for only the real servers.
vserver	(Optional) Clears connections for only the virtual servers.
counters	Clears all statistics for the specified CSG.
ft active	This keyword does not apply in a CSG environment.
linecard-configuration	This keyword does not apply in a CSG environment.
sticky	This keyword does not apply in a CSG environment.
sticky-group	This argument does not apply in a CSG environment.
all	This keyword does not apply in a CSG environment.

Defaults

If you specify the **connections** keyword and you do not specify **real** or **vserver**, all connections are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

When a connection is closed, a reset (RST) is sent to both the client and the server. Counters reset all the CSG statistics information, except for the **show module csg tech-support** counters, which are reset any time you run the **show** command.

Examples

The following example clears all connections for all the CSGs in the switch:

```
clear module csm all connections
```

client (CSG content)

To define the client IP address spaces that can use the CSG content server, use the **client** command in CSG content configuration mode. To remove a client definition, use the **no** form of this command.

client [**include** | **exclude**] {**any** | *ip-address* [*netmask*]}

no client [**include** | **exclude**] {**any** | *ip-address* [*netmask*]}

Syntax Description

include	(Optional) Indicates that the specified client can use the CSG content server. This is the default setting.
exclude	(Optional) Indicates that the specified client cannot use the CSG content server. Flows from excluded clients are blocked.
any	Identifies all clients. This is the default setting.
ip-address	Client IP address. The default is 0.0.0.0 (all clients).
netmask	(Optional) Client IP network mask. 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 client IP network mask is 0.0.0.0 or /0.

Defaults

All clients are included and can use the CSG content server.

The default client IP address is 0.0.0.0 (all clients).

The default client IP network mask is 0.0.0.0 or /0.

Command Modes

CSG content configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.
3.1(3)C5(3)—12.2(18)SXD	The usage guidelines were modified.

Usage Guidelines

You can use more than one **client** command to define more than one client.

The **include** and **exclude** settings are used only with the “default” policy, which is used only if all customer-defined policies fail to match.

The *netmask* argument is applied to the source IP address of incoming connections. The result must match the *ip-address* argument, or the **include** and **exclude** settings are not applied to the user packet.

The **include** and **exclude** settings are not applied at all if the **ip csg block** command is configured.

If you define content with a network mask of 255.255.255.255 or /32 (that is, all subnets), a virtual server is created and the CSG's MAC address is entered as the host's address in the CSG's ARP cache. Because of this, you cannot have hosts directly connected to the CSG, coupled with content with a network mask of 255.255.255.255 or /32 that matches those hosts.

Examples

The following example allows only clients from 10.4.4.x access to the CSG content server:

```
ip csg content MOVIES_COMEDY
 client 10.4.4.0 255.255.255.0
 idle 120
 ip 172.18.45.0/24 tcp 8080
 policy POLICY1
 replicate connection tcp
 vlan MOVIES_COMEDY
 inservice
```

Related Commands

Command	Description
ip csg content	Defines content for the CSG accounting services, and enters CSG accounting configuration mode.

client-group (CSG policy)

To reference a standard access list that is part of a CSG billing policy, use the **client-group** command in CSG policy 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 valid range is 1 to 99.
std-access-list-name	Standard access list name.

Defaults

All clients can access the content.

Command Modes

CSG policy configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

The **client-group** command is used to qualify clients for the CSG accounting service. The conditions specified in the referenced access list must be true in order for the flows to be processed by the CSG accounting services. If the conditions are not true, the flows are not processed (that is, traffic flows through with no accounting).

If you reference an access list that includes a **deny** statement, and that **deny** statement is matched, then traffic is blocked, there is no accounting, and the CSG does not check the next policy.

The referenced access list is applied to the VLAN interfaces.

You can reference more than one access list for a single policy by using multiple **client-group** commands in CSG policy configuration mode.

For WAP 1.x, URL maps take precedence over access lists.

For WAP1.x and RTSP, the policy used to determine the next hop address is chosen based solely on access control lists (ACLs), not URL maps. As a result, you can choose the next hop from one policy for routing and from a different policy for billing.

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 policy. For example, the following configuration is valid, because both policies use **client group 1** and **next-hop 1**:

```
policy A
  accounting type wap connection-oriented
  url A
  client group 1
  next-hop 1
policy B
  accounting type wap connection-oriented
  url B
```

```
  client group 1
  next-hop 1
content WAP-CON
  policy A
  policy B
```

The following configuration is not valid, because policy A uses **client group 1** and **next-hop 1**, but policy B uses **client group 1** and **next-hop 2**:

```
policy A
  accounting type wap connection-oriented
  url A
  client group 1
  next-hop 1
policy B
  accounting type wap connection-oriented
  url B
  client group 1
  next-hop 2
content WAP-CON
  policy A
  policy B
```

Examples

The following example shows how to reference client group 44 for the CSG policy MOVIES_COMEDY:

```
ip csg policy MOVIES_COMEDY
 accounting type http customer-string MOVIES_COMEDY
 client-group 44
 client-ip http-header x-forwarded-for
 header-map MOVIES
 url-map MOVIES
```

Related Commands

Command	Description
ip csg policy	Defines a policy for qualifying flows for the CSG accounting services, and enters CSG policy configuration mode.
next-hop	Defines a next-hop IP address.

client-ip (CSG policy)

To specify that the user's IP address is to be obtained from the URL header after the **x-forwarded-for** keyword, use the **client-ip** command in CSG policy configuration mode. To specify that the user's IP address is to be obtained from the IP header, use the **no** form of this command.

client-ip http-header x-forwarded-for

no client-ip http-header x-forwarded-for

Syntax Description

http-header x-forwarded-for	Specifies that the user's IP address is to be obtained from the URL header after the **x-forwarded-for** keyword.

Defaults

No default behavior or values.

Command Modes

CSG policy configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

The conditions specified in the referenced header map must be true in order for the flows to be processed by the CSG accounting services. If the conditions are not true, the flows are not processed.

Examples

The following example shows how to reference a client IP address specification in a CSG policy:

```
ip csg policy MOVIES_COMEDY
 accounting type http customer-string MOVIES_COMEDY
 client-group 44
 client-ip http-header x-forwarded-for
 header-map MOVIES
 url-map MOVIES
```

Related Commands

Command	Description
ip csg policy	Defines a policy for qualifying flows for the CSG accounting services, and enters CSG policy configuration mode.

content (CSG ruleset)

To add a content reference to a CSG ruleset, use the **content** command in CSG ruleset configuration mode. To remove a content reference, use the **no** form of this command.

content *content-name*

no content *content-name*

Syntax Description

content-name	Name of a configured content for this ruleset.

Defaults

No default behavior or values.

Command Modes

CSG ruleset configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

The *content-name* argument must match the *content-name* argument on an **ip csg content** command.

If you configure more than one content name using multiple **ip csg content** commands, you can configure more than one **content** command in CSG ruleset configuration mode. Each content must be associated with a different Layer 3/Layer 4 definition, as configured with **ip** commands in CSG content configuration mode.

Note If you assign an inbound VLAN to each content, using the VLAN to differentiate the contents within the same ruleset, the contents can be associated with the same Layer 3/Layer 4 definition.

Examples

The following example shows how to add references to contents MOVIES_COMEDY and MOVIES_ACTION to ruleset R1:

```
ip csg ruleset R1
 content MOVIES_COMEDY
 content MOVIES_ACTION
```

Related Commands

Command	Description
ip csg ruleset	Configures a CSG billing ruleset, and enters CSG ruleset configuration mode.

content (CSG service)

To define a content and policy as a member of a CSG billing service, and optionally to assign a weight to this content, use the **content** command in CSG 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-name*]

no content *content-name* **policy** *policy-name* [**weight** *weight-name*]

Syntax Description

content-name	Name of the content for this service. The name can be 1 to 15 characters long, uppercase or lowercase letters (The CSG 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-name*	(Optional) Name of a configured billing weight.

Defaults

No default behavior or values.

Command Modes

CSG service configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

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, reference a *weight-name* that has a *weight-value* of 0.

Examples

The following example shows how to define content for the CSG 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 named DOUBLE.

```
ip csg service MOVIES
 basis fixed
 content MOVIES_COMEDY policy MOVIES_COMEDY
 content MOVIES_ACTION policy MOVIES_ACTION weight DOUBLE
 idle 120
```

Related Commands

Command	Description
ip csg service	Defines a content billing service, and enters CSG service configuration mode.

database

To identify the server that answers user ID queries, use the **database** command in CSG user group configuration mode. To disable the database server, use the **no** form of this command.

database *ip-address port-number*

no database *ip-address port-number*

Syntax Description

ip-address	The IP address of the server that answers user ID queries.
port-number	The port number of the server that answers user ID queries. The valid range is 1 to 65535.

Defaults

No default behavior or values.

Command Modes

CSG user group configuration

Command History

Release	Modification
2.2(1)C(1)—12.1(11b)E3	This command was introduced.

Examples

The following example shows how to specify user database IP address 10.1.2.3 and port number 11111 for the CSG user-group G1:

```
ip csg user-group G1
 entries max 100000
 database 10.1.2.3 11111
 quota local-port 6666
 quota server 10.1.4.5 888 1
 quota server 10.1.6.7 999 2
 radius acct-port 7777
 radius key SECRET_PASSWORD
 radius parse strict
 radius server 10.13.14.15
 radius userid User-Name
 redirect nat 10.33.33.3
```

debug ip csg

To set the flags to obtain debugging output for the various CSG 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** | **agent** | **api** | **cpu** | **ftp** | **gtp** | **imap** | **module** *number* | **pop3** | **quota** | **radius** | **record storage** *slot* | **rtsp** | **smtp** | **timer** | **tlv** | **udb** | **users** [**prepaid**] | **wap** | **xml**}

no debug ip csg {**all** | **agent** | **api** | **cpu** | **ftp** | **gtp** | **imap** | **module** *number* | **pop3** | **quota** | **radius** | **record storage** *slot* | **rtsp** | **smtp** | **timer** | **tlv** | **udb** | **users** [**prepaid**] | **wap** | **xml**}

Syntax Description

all	Generates debugging output for all CSG components.
agent	Generates debugging output for the agent component.
api	Generates debugging output for the API call trace component.
cpu	Generates debugging output for the CPU component.
ftp	Generates debugging output for the FTP component.
gtp	Generates debugging output for the GTP component.
imap	Generates debugging output for the IMAP component.
module *number*	Restricts debugging output to only the specified CSG module.
pop3	Generates debugging output for the POP3 component.
quota	Generates debugging output for the quota server component.
radius	Generates debugging output for the RADIUS component.
record storage *slot*	Sets the flag to generate debugging output for the Persistent Storage Device (PSD) module, and denotes PSD slot number.
rtsp	Generates debugging output for the RTSP component.
smtp	Generates debugging output for the SMTP component.
timer	Generates debugging output for the timer component.
tlv	Generates debugging output for the TLV component.
udb	Generates debugging output for the UDB component.
users	Generates debugging output for the user component.
prepaid	Generates debugging output for only the prepaid users component.
xml	Generates debugging output for the XML component.
wap	Generates debugging output for the WAP component.

Defaults

The default values apply to all active CSG modules (cards). The **module** option restricts debugging to a specific card. If you enter the **module** command, debugging is turned off for all other cards; however, the debugging flags set remains in effect for the selected module.

If you want to see most but not all debugging output, you can use the **all** option to turn on all debugging flags, then use the **no** form of this command to turn off any options that do not interest you.

Command Modes

Privileged EXEC

Command History

Release	Modification
2.2(1)C(1)—12.1(11b)E3	This command was introduced.
3.1(1)C3(1)—12.2(14)ZA	The **cpu**, **quota**, **prepaid**, and **users** keywords were added.
3.1(3)C4(1)—12.2(14)ZA2	The **record storage** keyword and *slot* argument was added.
3.1(3)C5(1)—12.2(17d)SXB	The **rtsp** keyword was added.
3.1(3)C5(3)—12.2(18)SXD	The **ftp** keyword was added.
3.1(3)C5(5)—12.2(18)SXD	The **imap** keyword was added.

Usage Guidelines

Once the debug flags are set, they are automatically sent to the CSG card when a configuration is downloaded. Similarly, changes in the debug settings are sent to the CSGs being debugged.

You can use the **show debug** command to display the debug flag settings.

Examples

The following example shows how to turn on debugging for **rtsp** and **udb** on module 3:

```
debug ip csg module 3
debug ip csg rtsp
debug ip csg udb
```

entries max

To define the maximum number of entries allowed in the CSG User Table, use the **entries max** command in CSG user group configuration mode. To return to the default value, use the **no** form of this command.

entries max *entries-number*

no entries max *entries-number*

Syntax Description

entries-number	The maximum number of entries allowed in the User Table. If the User Table is full, or if there is no memory left for new entries, the CSG uses a Least Recently Used (LRU) algorithm to purge the oldest idled entries. The oldest idled entries are those that have idled the longest since all of the user's sessions were terminated or timed out. The valid range is 0 to an unlimited number of entries. The default number of entries is 25,000. A value of 0 specifies an unlimited number of entries. The actual number of entries in the User Table depends on several variables, including the traffic model being used, the number of RADIUS attributes reported, and so on. Even if you set *entries-number* to a very large number, such as 300,000, the CSG might never store that many entries in the User Table.

Defaults

The default number of entries is 25,000.

Command Modes

CSG user group configuration

Command History

Release	Modification
2.2(1)C(1)—12.1(11b)E3	This command was introduced.

Usage Guidelines

The User Table identifies all users known to the CSG. The 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.

Examples

The following example shows how to specify a maximum of 100,000 cache entries for the CSG user-group G1:

```
ip csg user-group G1
 entries max 100000
 database 10.1.2.3 11111
 quota local-port 6666
 quota server 10.1.4.5 888 1
 quota server 10.1.6.7 999 2
 radius acct-port 7777
 radius key SECRET_PASSWORD
 radius parse strict
```

```
radius server 10.13.14.15
radius userid User-Name
redirect nat 10.33.33.3
```

Related Commands

Command	Description
database	Server that answers user ID queries.
radius key	Specifies the CSG to be the RADIUS endpoint for accounting records, and specifies the secret key.

failover

To set the time for a standby CSG to wait before becoming an active CSG, use the **failover** command in fault-tolerant configuration mode. To remove the failover configuration, use the **no** form of this command.

failover *failover-time*

no failover *failover-time*

Syntax Description

failover-time	Amount of time, in seconds, the CSG must wait after the last heartbeat message is received before assuming the other CSG is not operating. The valid range is 1 to 65535 seconds. The default value is 3 seconds.

Defaults

The default failover time is 3 seconds.

Command Modes

Fault-tolerant configuration

Command History

Release	Modification
2.2(1)C(1)—12.1(11b)E3	This command was introduced.

Examples

The following example shows how to set a failover period of 6 seconds:

```
ft group 123 vlan 5
 failover 6
 heartbeat-time 2
 priority 12
```

Related Commands

Command	Description
ft group (module CSG)	Enters fault-tolerant configuration mode and configures fault tolerance.
show module csg ft	Displays statistics and counters for the CSG fault-tolerant pair.

flags

To specify IP, TCP, or WAP flag bit masks and values for CSG quota refund, use the **flags** command in CSG 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 BMA for connection termination. The range for *mask* is 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

No default behavior or values.

Command Modes

CSG refund configuration

Command History

Release	Modification
3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.
3.1(3)C5(5)—12.2(18)SXD	Combined the **flags** and **flags wap** commands.

Usage Guidelines

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 due to 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 HTTP1.1).
  - 0: The connection has been closed.
  - 1: The connection is not closed yet, and TCP close bits have no meaning.
- 0x80: Connection terminated due to 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
  retcode http 500 509
  retcode wap 0x44 0x50
  retcode ftp 454
  flags tcp 43 00
  flags ip 80 80
  flags wap 08
```

Related Commands

Command	Description
ip csg refund	Specifies the refund policy that can then be applied to the various services, and enters CSG refund configuration mode.
retcode	Specifies the range of application return codes for which the CSG refunds quota.

ft group (module CSG)

To enter fault-tolerant configuration mode and configure fault tolerance, use the **ft group** command in module CSG configuration mode. To remove the fault-tolerant configuration, use the **no** form of this command.

ft group *group-id* **vlan** *vlan-id*

no ft group

Syntax Description

group-id	ID of the fault-tolerant group. Both of the CSGs must have the same group ID. The range is from 1 to 254.
vlan *vlan-id*	VLAN, identified by its VLAN ID, over which heartbeat messages are to be sent. Both of the CSGs must have the same VLAN ID. The valid range is 2 to 4095.

Defaults

No default behavior or values.

Command Modes

Module CSG configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

A fault-tolerant group is comprised of two Catalyst 6000 series switches, each containing a CSG configured for fault-tolerant operation. Each fault-tolerant group appears to network devices as a single device. A network might have more than one fault-tolerant group, but the CSG supports only one fault-tolerant group per VLAN trunk.

The characteristics of each fault-tolerant group are defined by the following commands:

- **failover**
- **heartbeat-time**
- **priority**

Examples

The following example shows how to configure a fault-tolerant group named 123, with heartbeat messages sent over VLAN 5:

```
module csg 4
 accounting A1
 ft group 123 vlan 5
  failover 6
  heartbeat-time 2
  priority 12
 ruleset R1
 vlan 30 client
 vlan 40 server
```

Related Commands

Command	Description
failover	Sets the time for a standby CSG to wait before becoming an active CSG.
heartbeat-time	Sets the time before heartbeat messages are transmitted by the CSG.
priority	Sets the priority of the CSG.
show module csg ft	Displays statistics and counters for the CSG fault-tolerant pair.

gateway (module CSG VLAN)

To configure a gateway IP address, use the **gateway** command in module CSG VLAN configuration mode. To remove the gateway from the configuration, use the **no** form of this command.

gateway *ip-address*

no gateway *ip-address*

Syntax Description

ip-address	IP address of the client-side gateway.

Defaults

No default behavior or values.

Command Modes

Module CSG VLAN configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

You can configure up to 7 gateways per VLAN with a total of up to 255 gateways for the entire system. A gateway must be in the same network as specified in the **ip address** VLAN command.

To support RADIUS endpoint, the CSG requires a route to 255.255.255.255. You can configure the route by using the **gateway (module CSG VLAN)** command or the **route (module CSG VLAN)** command. For example:

gateway 31.0.0.6

or:

route 255.255.255.255 255.255.255.255 gateway 31.0.0.6

Note If you already have a gateway configured, you do not need to configure an additional gateway for the RADIUS endpoint.

Examples

The following example shows how to configure a client-side gateway IP address:

```
vlan 301 client
 name TO-GGSN-MS-APN
 gateway 31.0.0.10
 ip address 31.0.0.21 255.255.255.0
 route 11.0.0.0 255.255.0.0 gateway 31.0.0.1
 route 11.1.0.0 255.255.0.0 gateway 31.0.0.2
 route 11.2.0.0 255.255.0.0 gateway 31.0.0.3
 route 11.3.0.0 255.255.0.0 gateway 31.0.0.4
 alias 31.0.0.51 255.255.255.0
```

Related Commands

Command	Description
ip address (module CSG VLAN)	Assigns an IP address to the CSG VLAN.
show module csg variable	Displays the list of VLANs.
vlan (module CSG)	Creates a client or server VLAN that defines the Layer 2 paths for the CSG accounting service flows, assigns a VLAN ID and optional name, and enters module CSG VLAN configuration mode.

header-map

To reference a header map that is part of a CSG billing policy, use the **header-map** command in CSG policy configuration mode. To delete the reference, use the **no** form of this command.

header-map *header-map-name*

no header-map *header-map-name*

Syntax Description

header-map-name	Name of a header map, as configured with an **ip csg map** command.

Defaults

No default behavior or values.

Command Modes

CSG policy configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

The conditions specified in the referenced header map must be true in order for the flows to be processed by the CSG accounting services. If the conditions are not true, the flows are not processed.

Examples

The following example shows how to reference header map MOVIES for the CSG policy MOVIES_COMEDY:

```
ip csg policy MOVIES_COMEDY
 accounting type http customer-string MOVIES_COMEDY
 client-group 44
 client-ip http-header x-forwarded-for
 header-map MOVIES
 url-map MOVIES
```

Related Commands

Command	Description
ip csg map	Defines the CSG billing content filters (URL and header maps), and enters CSG map configuration mode.
ip csg policy	Defines a policy for qualifying flows for the CSG accounting services, and enters CSG policy configuration mode.
match (header map)	Specifies a header match pattern for a CSG billing map.
match (URL map)	Specifies a URL match pattern for a CSG billing map.
url-map	References a URL map that is part of a CSG billing policy.

heartbeat-time

To set the time before heartbeat messages are transmitted by the CSG, use the **heartbeat-time** command in fault-tolerant configuration mode. To restore the default heartbeat interval, use the **no** form of this command.

heartbeat-time *heartbeat-time*

no heartbeat-time *heartbeat-time*

Syntax Description

heartbeat-time	Time interval between heartbeat transmissions, in seconds. The valid range is 1 to 65535 seconds. The default value is 1 second.

Defaults

The default heartbeat time is 1 second.

Command Modes

Fault-tolerant configuration

Command History

Release	Modification
2.2(1)C(1)—12.1(11b)E3	This command was introduced.

Examples

The following example shows how to set the heartbeat time to 2 seconds:

```
ft group 123 vlan 5
 failover 6
 heartbeat-time 2
 priority 12
```

Related Commands

Command	Description
ft group (module CSG)	Enters fault-tolerant configuration mode and configures fault tolerance.
show module csg ft	Displays statistics and counters for the CSG fault-tolerant pair.

hostname

To specify a variable hostname for a CSG module, use the **hostname** command in module CSG configuration mode. To remove the hostname, use the **no** form of this command.

hostname *name*

no hostname

Syntax Description

name	1- to 20-character hostname for the CSG module.

Defaults

No default behavior or values.

Command Modes

Module CSG configuration

Command History

Release	Modification
3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.

Usage Guidelines

This command assigns a hostname to a CSG module that is reported in fixed-record format.

Examples

The following example specifies a hostname for the CSG module in slot 3:

```
module ContentServicesGateway 3
       hostname MYHOST
```

Related Commands

Command	Description
assign	Associates an IPv4 address with a transport-type value.
class	Specifies a service class value.
ip csg transport-type	Classifies data traffic based on its access path.
mode	Specifies that a billing plan is postpaid or prepaid.
owner id	Specifies an identifier for a service owner.
owner name	Specifies the name of a service owner.
records format	Specifies **variable** or **fixed** CDR format.

idle (CSG content)

To specify the minimum amount of time that the CSG maintains an idle content connection, use the **idle** command in CSG 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	Idle content timer duration in seconds. If there are no flows on a content connection for more than *duration* seconds, the CSG assumes the connection is idle and ends the connection. Valid values range from 4 to 65535 seconds. The default is 3600 seconds (1 hour).

Defaults

The default idle duration is 3600 seconds (1 hour).

Command Modes

CSG content configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

RTSP billing in the CSG is based on inspection of the RTSP SETUP and TEARDOWN messages that are exchanged between the client and server. The CSG builds the RTSP CDR immediately after the RTSP TEARDOWN signal if the URL exactly matches that from the RTSP SETUP signal. Otherwise, the CSG builds the CDR after any condition that causes the flows to be terminated. Examples include:

- When the idle content timer expires. By default, this timer is set to 3600 seconds (1 hour). To receive the RTSP CDRs sooner, set the timer to a smaller value, such as 60 seconds. (Do not set the timer to less than 60 seconds for RTSP.)
- When a service_stop is triggered (for example, when the access server sends a RADIUS Accounting Stop for the user).

The CSG tracks usage on a per-session basis. UDP protocols do not have an end-of-session indicator and simply idle out. For that reason, for UDP and WAP 1.x, setting the content idle timer to a low value (for example, 30 seconds) allows the CSG to quickly recognize that a session has ended and generate billing records accordingly. Other service-level features of the CSG that count sessions (such as passthrough mode and service-level CDRs) are similarly affected by the content idle timer setting.

Examples

The following example shows how to configure a 120-second idle timer for the CSG content MOVIES_COMEDY:

```
ip csg content MOVIES_COMEDY
 client 10.4.4.0 255.255.255.0
 idle 120
 ip 172.18.45.0/24 tcp 8080
 policy POLICY1
 replicate connection tcp
 vlan MOVIES_COMEDY
 inservice
```

Related Commands

Command	Description
ip csg content	Defines content for the CSG accounting services, and enters CSG content configuration mode.

idle (CSG service)

To specify the minimum amount of time that the CSG maintains a service with no user sessions, use the **idle** command in CSG 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	Idle service timer duration in seconds. If a user's quota for a service is unused for more than *duration* seconds, the CSG assumes the service is idle and sends a ServiceStop to free up the resources. Valid values range from 10 to 65535 seconds. The default is 300 seconds (5 minutes).

Defaults

The default idle duration is 300 seconds.

Command Modes

CSG service configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

For RTSP, do not set the timer to less than 60 seconds.

Examples

The following example shows how to configure a 120-second idle timer for the CSG service MOVIES:

```
ip csg service MOVIES
 basis fixed
 content MOVIES_COMEDY policy MOVIES_COMEDY
 content MOVIES_ACTION policy MOVIES_ACTION weight DOUBLE
 idle 120
```

Related Commands

Command	Description
ip csg service	Defines a content billing service, and enters CSG service configuration mode.

inservice (CSG content)

To activate the content service on each CSG, use the **inservice** command in CSG 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

CSG content configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

When you activate the **inservice** command, the CSG verifies the parameters semantically. If the CSG detects an error, the command fails.

Examples

The following example shows how to place the CSG content MOVIES_COMEDY in service:

```
ip csg content MOVIES_COMEDY
 client 10.4.4.0 255.255.255.0
 idle 120
 ip 172.18.45.0/24 tcp 8080
 policy POLICY1
 replicate connection tcp
 vlan MOVIES_COMEDY
 inservice
```

Related Commands

Command	Description
ip csg content	Defines content for the CSG accounting services, and enters CSG accounting configuration mode.

ip

To define the Layer 3/Layer 4 subset of flows that can be processed by the CSG accounting services, use the **ip** command in CSG content configuration mode. To delete the content definition, use the **no** form of this command.

ip {**any** | *ip-address* [*netmask*]} [*protocol* [*port-number*]]

no ip {**any** | *ip-address* [*netmask*]} [*protocol* [*port-number*]]

Syntax Description

any	All Layer 3/Layer 4 flows can be processed. This is the default setting.
ip-address	IP address for which Layer 3/Layer 4 flows can be processed.
netmask	Mask identifying the network from which Layer 3/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.
protocol	Protocol type of Layer 3/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 UDP flows can be processed. • *protocol-number*—Number identifying the protocol whose flows can be processed. The valid range is 0 to 255, where 0 means the same as **any**.
port-number	Port number from which Layer 3/Layer 4 flows can be processed. The valid range is 0 to 65535, where 0 means flows from any port number can be processed.

Defaults

All Layer 3/Layer 4 flows can be processed.

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 flows from any port number can be processed.

Command Modes

CSG content configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

This command is required to place content in service.

UDP ports 9200 and 9201 are well-known WSP and WTP WAP ports. When a policy with **accounting type wap** is associated with a content, use even-numbered UDP ports to designate WSP traffic, and 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 CSG does not support Layer 3 content rules. The CSG ignores the specified port number, and the **show module 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 CSG accounting services:

```
ip csg content MOVIES_COMEDY
 client 10.4.4.0 255.255.255.0
 idle 120
 ip 172.18.45.0/24 tcp 8080
 policy POLICY1
 replicate connection tcp
 vlan MOVIES_COMEDY
 inservice
```

Related Commands

Command	Description
ip csg content	Defines content for the CSG accounting services, and enters CSG content configuration mode.

ip address (module CSG VLAN)

To assign an IP address to the CSG VLAN, use the **ip address** command in module CSG VLAN configuration mode. To remove the CSG IP address from the configuration, use the **no** form of this command.

ip address *ip-address netmask*

no ip address *ip-address netmask*

Syntax Description

ip-address	IP address for the CSG; only one management IP address is allowed per VLAN.
netmask	Network mask.

Defaults

No default behavior or values.

Command Modes

Module CSG VLAN configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

This command is applicable for both server-side and client-side VLANs.

Examples

The following example shows how to assign an IP address to the CSG VLAN:

```
vlan 301 client
 name TO-GGSN-MS-APN
 gateway 31.0.0.10
 ip address 31.0.0.21 255.255.255.0
 route 11.0.0.0 255.255.0.0 gateway 31.0.0.1
 route 11.1.0.0 255.255.0.0 gateway 31.0.0.2
 route 11.2.0.0 255.255.0.0 gateway 31.0.0.3
 route 11.3.0.0 255.255.0.0 gateway 31.0.0.4
 alias 31.0.0.51 255.255.255.0
```

Related Commands

Command	Description
show module csg variable	Displays the list of VLANs.
vlan (module CSG)	Creates a client or server VLAN that defines the Layer 2 paths for the CSG accounting service flows, assigns a VLAN ID and optional name, and enters module CSG VLAN configuration mode.

ip csg accounting

To define content-based client accounting as a service, and to enter CSG accounting configuration mode, use the **ip csg accounting** command in global configuration mode. To turn off the service, use the **no** form of this command.

ip csg accounting *service-name*

no ip csg accounting *service-name*

Syntax Description

service-name	Name of the accounting service: • In the CSG Releases 2.2.(1)C(1) through 2.2(3)C2(1), the name can be 1 to 15 characters, uppercase or lowercase letters (the CSG changes all letters to uppercase), numbers, underscores, and the special characters #, @, and $. The first character must be a letter. • In the CSG Release 3.1(1)C3(1) or later, the name can be 1 to 15 characters, uppercase or lowercase letters (the CSG changes all letters to uppercase), numbers, and any special characters.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
2.2(1)C(1)—12.1(11b)E3	This command was introduced.

Usage Guidelines

The characteristics of each accounting service are defined by the following commands:

- **agent (CSG accounting)**
- **agent activate**
- **agent local-port**
- **keepalive**
- **records batch**
- **records format**
- **records http-statistics**
- **records intermediate**
- **records max**
- **record-storage**
- **record-storage local-port**
- **report http header**

- **report radius attribute**
- **report usage**
- **user-group**

Examples

The following example shows how to configure a CSG accounting service named A1:

```
ip csg accounting A1
 user-group G1
 agent activate 2
 agent local-port 3775
 agent 10.1.2.4 11112 10
 agent 10.1.2.5 11113 20
 keepalive 3
 records batch
 records http-statistics
 records intermediate bytes 100000 time 3600
 records max 250
 inservice
```

Related Commands

Command	Description
agent (CSG accounting)	Defines the BMA to which to send billing records.
agent activate	Enables support for multiple active BMAs.
agent local-port	Defines the port on which the CSG listens for packets from the BMAs.
inservice (CSG content)	Starts the accounting service in each CSG configuration.
keepalive	Defines the keepalive time interval (in seconds). The time in which a message from the BMA must be received.
records batch	Batches billing records into a single message before sending them to the BMA.
records http-statistics	Sends the HTTP Statistics data record to the BMA.
records intermediate	Enables the generation of intermediate billing records.
records max	Defines the maximum number of billing records that can be stored or queued in the CSG before they are forwarded to the Billing Mediation Agent (BMA).
user-group	Associates a user group with a specific accounting service.

ip csg billing

To define a billing plan to be used for prepaid billing, and to enter CSG 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 CSG encounters a new client, the CSG retrieves its billing plan. The name can be 1 to 64 characters, uppercase or lowercase letters (the CSG changes all letters to uppercase), numbers, and any special characters.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

The characteristics of each billing plan are defined by the following commands:

- **mode**
- **service**

Examples

The following example shows how to define a CSG billing plan named REGULAR:

```
ip csg billing REGULAR
 service MOVIES
 service BROWSING
```

Related Commands

Command	Description
service	Associates a service with a CSG billing plan.

ip csg block

To force the CSG to drop packets that do not match a configured billing policy, use the **ip csg block** command in global configuration mode. To restore the default behavior, enabling the CSG to forward the packets without billing, use the **no** form of this command.

ip csg block

no ip csg block

Syntax Description

There are no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
3.1(3)C5(5)—12.2(18)SXD	This command was introduced.

Usage Guidelines

By default, if packets do not match any billing policy, the CSG forwards the packets without billing. This command causes the CSG to drop the packets instead.

Examples

The following example shows how to force the CSG to drop packets that do not match any billing policy:

```
ip csg block
```

ip csg content

To define content for the CSG accounting services, and to enter CSG content configuration mode, use the **ip csg content** command in global configuration mode. To delete the content definition, use the **no** form of this command.

ip csg content *content-name*

no ip csg content *content-name*

Syntax Description

content-name	Name that identifies the content. The name can be 1 to 15 characters, uppercase or lowercase letters (the CSG changes all letters to uppercase), numbers, and any special characters.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

The characteristics of each content definition are defined by the following commands:

- **client (CSG content)**
- **idle (CSG content)**
- **inservice (CSG content)**
- **ip**
- **pending**
- **policy (CSG content)**
- **replicate connection tcp**
- **vlan (CSG content)**

If the content specification does not match any service listed under a user's billing plan, the CSG considers the service to be either free or postpaid. The CSG does not try to authorize the user with the quota server for the service.

If multiple policies are defined under **ip csg content**, they must all have the same accounting type. As an example, if one of the policies is configured with **accounting type wap**, they all must have **accounting type wap**.

Examples

The following example shows how to define the CSG content named MOVIES_COMEDY:

```
ip csg content MOVIES_COMEDY
 client 10.4.4.0 255.255.255.0
 idle 120
 ip 172.18.45.0/24 tcp 8080
 policy POLICY1
 replicate connection tcp
 vlan MOVIES_COMEDY
 inservice
```

Related Commands

Command	Description
client (CSG content)	Defines the client IP address spaces that can use the CSG content server.
idle (CSG content)	Specifies the minimum amount of time that the CSG maintains an idle content connection.
inservice (CSG content)	Activates the content service on each CSG.
ip	Defines the Layer 3/Layer 4 subset of flows that can be processed by the CSG accounting services.
policy (CSG content)	References a CSG billing policy.
replicate connection tcp	Replicates the connection state for all TCP connections to the CSG content servers on the backup system.
vlan (CSG content)	Restricts the CSG billing content to a single source VLAN.

ip csg map

To define the CSG billing content filters (URL maps and header maps), and to enter CSG URL map or header 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* {**url** | **header**}

no ip csg map *map-name* {**url** | **header**}

Syntax Description

map-name	Name of the map. The name can be 1 to 15 characters, uppercase or lowercase letters (the CSG changes all letters to uppercase), numbers, and any special characters.
url	Defines a URL content filter, and enters CSG URL map configuration mode.
header	Defines a header content filter, and enters CSG header map configuration mode.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

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

The URLs or headers that are to be matched against a pattern are defined by the following commands:

- **match (header map)**
- **match (URL map)**

When configuring a map, keep the following considerations in mind:

- When you enter a new or changed URL match pattern using the **match (URL map)** command, the CSG console becomes non-responsive while the CSG downloads the entire configuration, which can take a long time. Therefore, 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 map)** statements, but it cannot include both **match (header map)** statements and **match (url map)** statements.

- You can specify up to two maps in a given policy: one for header 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
 header-map HOSTMAP
 url-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 CSG URL map named MOVIES:

```
ip csg map MOVIES url
  match url *.movies_(comedy|action|drama).com/*.mpeg
```

Related Commands

Command	Description
header-map	References a header map that is part of a CSG billing policy.
ip csg policy	Defines a policy for qualifying flows for the CSG accounting services, and enters CSG policy configuration mode.
match (header map)	Specifies a header match pattern for a CSG billing map.
match (URL map)	Specifies a URL match pattern for a CSG billing map.
url-map	References a URL map that is part of a CSG billing policy.

ip csg policy

To define a policy for qualifying flows for the CSG accounting services, and to enter CSG 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 1 to 15 characters, uppercase or lowercase letters (the CSG changes all letters to uppercase), numbers, and any special characters.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

The characteristics of each policy are defined by the following commands:

- **accounting (CSG policy)**
- **client-group (CSG policy)**
- **client-ip (CSG policy)**
- **header-map**
- **next-hop**
- **url-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 map)** statements, but it cannot include both **match (header map)** statements and **match (url map)** statements.
- You can specify up to two maps in a given policy: one for header 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
 header-map HOSTMAP
 url-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 CSG policy named MOVIES_COMEDY:

```
ip csg policy MOVIES_COMEDY
 accounting type http customer-string MOVIES_COMEDY
 client-group 44
 client-ip http-header x-forwarded-for
 header-map MOVIES
 url-map MOVIES
```

Related Commands

Command	Description
accounting (CSG policy)	Defines the accounting type and customer string for all flows that comply with a CSG billing policy.
client-group (CSG policy)	References a standard access list that is part of a CSG billing policy.
client-ip (CSG policy)	Specifies that the user's IP address is to be obtained from the URL header after the **x-forwarded-for** keyword.
header-map	References a header map that is part of a CSG billing policy.
url-map	References a URL map that is part of a CSG billing policy.

ip csg refund

To specify the refund policy that can then be applied to the various services, and to enter CSG 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 a policy that applies to the content for this service.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.

Usage Guidelines

The characteristics of each policy are defined by the following commands:

- **flags**
- **retcode**

If refund is enabled for a CSG prepaid service, you cannot download more than 0x6FFFFFFF bytes of data in a given transaction.

Examples

The following example shows how to configure the **ip csg refund** command:

```
ip csg refund COMPANY-REFUND
  retcode http 500 509
  retcode wap 0x44 0x50
  retcode ftp 454
  flags tcp FF 14
  flags wap FF 08
```

Related Commands

Command	Description
flags	Specifies IP, TCP, or WAP flag bit masks and values for which the CSG refunds quota.
retcode	Specifies the range of application return codes for which the CSG refunds quota.

ip csg ruleset

To configure a CSG billing ruleset, and to enter CSG ruleset configuration mode, use the **ip csg ruleset** command in global configuration mode. To delete the ruleset, use the **no** form of this command.

ip csg ruleset *ruleset-name*

no ip csg ruleset *ruleset-name*

Syntax Description

ruleset-name	Name of the CSG billing ruleset. A ruleset is a list of all content names that are to be downloaded to a specific CSG card. The name can be 1 to 15 characters, uppercase or lowercase letters (the CSG changes all letters to uppercase), numbers, and any special characters.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

The characteristics of each ruleset are defined by the **content (CSG ruleset)** command.

Examples

The following example shows how to configure a CSG billing ruleset named R1:

```
ip csg ruleset R1
 content MOVIES_COMEDY
 content MOVIES_ACTION
```

Related Commands

Command	Description
content (CSG ruleset)	Adds a content reference to a CSG ruleset.

ip csg service

To define a content billing service, and to enter CSG service configuration mode, use the **ip csg service** command in global configuration mode. To turn off the 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 users. The name can be 1 to 15 characters, uppercase or lowercase letters (the CSG changes all letters to uppercase), numbers, and any special characters.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

The CSG allows you to define a pool of up to 255 services. You can authorize each user for any number of services from that pool, but we recommend that the billing system not authorize each user for more than 10 active services. Exceeding this guideline could lead to the following problems:

- The increase in the number of quota authorizations per user can overload the quota server, as well as CSG.
- As the number of services for which a user is actively authorized increases, the user's quota becomes fragmented. Although the CSG allows the billing system to recall and redistribute the quota so that the user is not denied service due to quota fragmentation, the process increases overhead in both the quota server and the CSG.

The characteristics of each content billing service are defined by the following commands:

- **activation**
- **authorize content**
- **basis**
- **class**
- **content (CSG service)**
- **idle (CSG service)**
- **meter exclude service-idle**
- **meter imap**

- **meter increment**
- **meter initial**
- **meter minimum**
- **owner id**
- **owner name**
- **passthrough**
- **records granularity**
- **refund-policy**
- **verify**
- **zero-quota abort type**

Examples

The following example shows how to define a CSG content billing service named MOVIES:

```
ip csg service MOVIES
 basis fixed
 content MOVIES_COMEDY policy MOVIES_COMEDY
 content MOVIES_ACTION policy MOVIES_ACTION weight DOUBLE
 idle 120
```

Related Commands

Command	Description
basis	Specifies the billing basis for a CSG content billing service.
content (CSG service)	Defines content as a member of a CSG billing service, identifies a policy to apply to this content, and optionally assigns a weight to this content.
idle (CSG service)	Specifies the minimum amount of time that the CSG maintains a service with no user sessions.

ip csg snmp timer

To define SNMP timers for lost CSG records, and to enter CSG SNMP timer configuration mode, 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 {**agent** | **quota-server**} *interval*

no ip csg snmp timer {**agent** | **quota-server**} *interval*

Syntax Description

agent	Defines an SNMP timer for lost CSG agent records.
quota-server	Defines an SNMP timer for lost CSG quota server records.
interval	Interval, in seconds, of the CSG SNMP timer. The valid range is 1 second to 2,147,483,647 seconds. The default setting is 60 seconds.

Defaults

The default SNMP timer interval is 60 seconds.

Command Modes

Global configuration

Command History

Release	Modification
3.1(3)C5(3)—12.2(18)SXD	This command was introduced.

Examples

The following example defines a 300-second CSG SNMP agent timer and enters CSG SNMP timer configuration mode:

```
ip csg snmp timer agent 300
```

ip csg transport-type

To classify data traffic based on its access path, and to enter CSG transport-type configuration mode, use the **ip csg transport-type** command in global configuration mode. To remove transport-type information, use the **no** form of this command.

ip csg transport-type

no class ip csg transport-type

Syntax Description

There are no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.

Usage Guidelines

Transport-type is used to classify data traffic based on its access path using the NAS-IP reported in RADIUS. Use the **assign** command to associate IP addresses with transport-type values. Transport-type information is reported in fixed record format CDRs.

Usage Guidelines

The characteristics of each ruleset are defined by the **assign** command.

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
  assign 2.5.3.1 7
  assign 6.6.7.5 0
```

Related Commands

Command	Description
records format	Specifies **variable** or **fixed** CDR format.
hostname	Specifies a variable hostname for a CSG module.
owner name	Specifies the name of a service owner.
owner id	Specifies an identifier for a service owner.
assign	Associates an IPv4 address with a transport-type value.

Command	Description
class	Specifies a service class value.
mode	Specifies that a billing plan is postpaid or prepaid.

ip csg user-group

To create a group of end users for which you want to generate accounting records, and to enter CSG user group configuration mode, use the **ip csg user-group** command in global configuration mode. To delete a group of users, use the **no** form of this command.

ip csg user-group *group-name*

no ip csg user-group *group-name*

Syntax Description

group-name	Name of the group you want to create: • In the CSG Releases 2.2.(1)C(1) through 2.2(3)C2(1), the name can be 1 to 15 characters, uppercase or lowercase letters (the CSG changes all letters to uppercase), numbers, underscores, and the special characters #, @, and $. The first character must be a letter. • In the CSG Release 3.1(1)C3(1), the name can be 1 to 15 characters, uppercase or lowercase letters (the CSG changes all letters to uppercase), numbers, and any special characters.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
2.2(1)C(1)—12.1(11b)E3	This command was introduced.

Usage Guidelines

The **ip csg user-group** command configures parameters related to mapping IP addresses to user IDs.

You cannot delete a user group that is referenced by an accounting service. First, you must disassociate the user group from the accounting service. See the **user-group** command in CSG accounting configuration mode for more details.

The characteristics of this group of users are defined by the following commands:

- **aoc confirmation**
- **database**
- **entries max**
- **quota activate**
- **quota local-port**
- **quota server**
- **radius acct-port**
- **radius ack error**

- **radius handoff**
- **radius key**
- **radius monitor**
- **radius parse strict**
- **radius pod attribute**
- **radius pod nas**
- **radius pod timeout**
- **radius server**
- **radius start restart session-id**
- **radius stop purge**
- **radius userid**
- **redirect**
- **user-profile server**
- **verify confirmation**

Examples

The following example shows how to create the CSG user-group G1:

```
ip csg user-group G1
 entries max 100000
 database 10.1.2.3 11111
 quota local-port 6666
 quota server 10.1.4.5 888 1
 quota server 10.1.6.7 999 2
 radius acct-port 7777
 radius key SECRET_PASSWORD
 radius parse strict
 radius server 10.13.14.15
 radius userid User-Name
 redirect nat 10.33.33.3
 redirect wap www.topoff.com/wap
 redirect http www.topoff.com/http
 aoc confirmation AOC_OK
```

Related Commands

Command	Description
database	Server that answers user ID queries.
entries max	Defines the maximum number of entries in the memory cache to retain information about users belonging to this group.
quota local-port	Configures the local port on which the CSG receives communications from quota servers.
quota server	Configures the quota servers that return billing quota values for users.
radius acct-port	Configures the RADIUS listening port when it is different from the established RADIUS default of 1813.
radius key	Specifies that the CSG is the RADIUS accounting server to obtain user ID accounting records.
radius monitor	Tightens the parsing rules for RADIUS flows.

Command	Description
radius proxy	Enables RADIUS proxy.
radius start restart session-id	RADIUS attribute used to extract the user IDs from a RADIUS record.
redirect	Redirects client flows to an alternate IP address when the client's quota is exhausted.

ip csg weight

To define a symbolic name for a CSG billing weight, and to enter CSG weight configuration mode, use the **ip csg weight** command in global configuration mode. To remove the weight name, use the **no** form of this command.

ip csg weight *weight-name weight-value*

no ip csg weight *weight-name weight-value*

Syntax Description

weight-name	Name of the billing weight. The name can be 1 to 15 characters, uppercase or lowercase letters (the CSG changes all letters to uppercase), numbers, and any special characters.
weight-value	Number of quadrans to deduct for each billable object that uses this billing weight. The valid range is -32768 quadrans to +32767 quadrans. The default billing weight is 1 quadran, which means 1 quadran is deducted for each billable object. A value of 0 means the associated content is free.

Defaults

The default billing weight is 1 quadran.

Command Modes

Global configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

To make a content free, assign a *weight-value* of 0.

The same weight can occur in multiple rules, specified in multiple billing services. If a weight changes, and you use numeric constants for weights, each occurrence of the weight must be updated. However, if you define symbolic weight names, you need only update a single definition for each weight. The result is a more readable configuration, and price lists that are easier to manage.

Examples

The following example shows how to define a CSG billing weight named DOUBLE with a weight value of 2 quadrans:

```
ip csg weight DOUBLE 2
```

keepalive

To define the keepalive time interval used to test the health of Billing Mediation Agents (BMAs) and quota servers, use the **keepalive** command in CSG accounting configuration mode. To reset the keepalive timer to the default value, use the **no** form of this command.

keepalive *number-of-seconds*

no keepalive

Syntax Description

number-of-seconds	Time, in seconds, that is used to determine the health of BMAs and quota servers. The valid ranges is 1 to 86,400 seconds. The default value is 60 seconds.

Defaults

The default value is 60 seconds.

Command Modes

CSG accounting configuration

Command History

Release	Modification
2.2(1)C(1)—12.1(11b)E3	This command was introduced.

Examples

The following example shows how to specify a keepalive time of 3 seconds for the CSG accounting service A1:

```
ip csg accounting A1
 user-group G1
 agent activate 2
 agent local-port 3775
 agent 10.1.2.4 11112 10
 agent 10.1.2.5 11113 20
 keepalive 3
 records batch
 records http-statistics
 records intermediate bytes 100000 time 3600
 records max 250
 inservice
```

Related Commands

Command	Description
agent (CSG accounting)	Defines the primary and backup BMAs to which to send billing records.

match (header map)

To specify a header match pattern for a CSG billing map, use the **match** command in CSG header map configuration mode. To delete the header match pattern, use the **no** form of this command.

match protocol *protocol* **header** *header-name* [**value** *pattern*]

no match protocol *protocol* **header** *header-name* [**value** *pattern*]

Syntax Description

protocol *protocol*	Default application protocol: **http**—This is the only supported application protocol, and it is the default setting.
header *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 **host**.
value	(Optional) Specific value corresponding to the header that is to be matched against the input header.
pattern	(Optional) Regular expression that is to be matched against the input header.

Defaults

The default protocol is HTTP.

If you specify a *header-name* argument and you do not specify a *pattern* argument, then the header match is TRUE if *header-name* is present in the HTTP flow.

Command Modes

CSG header map configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.
3.1(3)C5(3)—12.2(18)SXD	The usage guidelines were modified.

Usage Guidelines

Header maps are valid only with accounting types HTTP, RTSP, and WAP (specified using the **accounting** command in CSG policy configuration mode). If you do not specify an accounting type, the CSG assumes that the session is an HTTP session, and packets matching the policy are not billed (that is, no quota is used, and no CDR is generated).

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 map)** statements, but it cannot include both **match (header map)** statements and **match (url map)** statements.

- You can specify up to two maps in a given policy: one for header 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
 header-map HOSTMAP
 url-map URLMAP
```

  In this example, a flow must match both HOSTMAP and URLMAP in order to match policy MAP-POLICY.

- If you have configured too many maps, or if your maps are too complex, the CSG generates the following syslog message:

  %CSM_SLB-3-UNEXPECTED: Module 3 unexpected error:
  Current configuration exceed memory limit for rule table.

  If you see this message, you must reduce the number and complexity of the maps in your configuration.

  To ensure that your maps are configured correctly, use the following command:

  show module csg *slot* **tech-support processor 4 | include LB common pool**

  If the **last config change** field in the output is zero, your maps are configured correctly.

You can specify more than one **match** command in CSG header map configuration mode to specify multiple header match expressions for a given header map:

- 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 value www.cisco.com
 match header User-Agent valuemyagent
```

  But the following is not a valid configuration, because both **match header** commands reference header **Host**:

```
ip csg map HDR1
 match header Host valuewww.cisco.com
 match header Host valuemy.cisco.com
```

- If the header matches *all* of the header match expressions, then the match is TRUE and the flows can be processed by the CSG accounting services (unless there is another map associated with this policy that is FALSE).
- If the header *does not* match *even one* of the header match expressions, then the match is FALSE and the flows are not processed by the CSG accounting services, even if other maps for this policy match TRUE.
- The CSG 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. The more wildcard matches you use, the fewer header maps and header

match patterns the CSG can handle, depending on your configuration. Therefore, to optimize the performance of the CSG, minimize the number of header match patterns that are applied to a CSG content configuration, and minimize the number of wildcards used in header match patterns.

- The header match expressions are case-sensitive. For example, if you define the following header match expression:

  match header host1 value *.2.*.44

  but the actual HTTP header keyword is **HOST1**, the header *does not* match the header match expression, the match is FALSE, and the flow is not processed by the CSG accounting services.

Table B-1 shows the special characters that you can use in header match expressions.

Table B-1 Special Characters for Matching String Expressions

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.

Examples

The following example shows how to specify 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 value www.cisco.com
 match header User-Agent value myagent
```

Related Commands

Command	Description
header-map	References a header map that is part of a CSG billing policy.
ip csg map	Defines the CSG billing content filters (URL and header maps), and enters CSG map configuration mode.
ip csg policy	Defines a policy for qualifying flows for the CSG accounting services, and enters CSG policy configuration mode.

Command	Description
match (URL map)	Specifies a URL match pattern for a CSG billing map.
url-map	References a URL map that is part of a CSG billing policy.

match (URL map)

To specify a URL match pattern for a CSG billing map, use the **match** command in CSG URL map configuration mode. To delete the match pattern, use the **no** form of this command.

match protocol *protocol* [**method** *method*] **url** *pattern*

no match protocol *protocol* [**method** *method*] **url** *pattern*

Syntax Description

protocol *protocol*	Default application protocol: **http**—This is the only supported application protocol, and it is the default setting.
method *method*	Method to be matched. Valid methods are: • Extension method name of 1 to 15 characters • **connect**—CONNECT method • **delete**—DELETE method • **get** —GET method • **head**—HEAD method • **options**—OPTIONS method • **post**—POST method • **put**—PUT method • **trace**—TRACE method
url *pattern*	Regular URL expression to be matched against the input URL. The pattern can include up to 128 characters, including wildcards and UNIX string-matching special characters.

Defaults

The default application protocol is HTTP.

Command Modes

CSG URL map configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.
3.1(3)C5(3)—12.2(18)SXD	The usage guidelines were modified.

Usage Guidelines

URL maps are valid only with accounting types HTTP, RTSP, and WAP (specified using the **accounting** command in CSG policy configuration mode). If you do not specify an accounting type, the CSG assumes that the session is an HTTP session, and packets matching the policy are not billed (that is, no quota is used, and no CDR is generated).

When configuring a map, keep the following considerations in mind:

- When you enter a new or changed URL match pattern using the **match (URL map)** command, the CSG console becomes non-responsive while the CSG downloads the entire configuration, which can take a long time. Therefore, 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 map)** statements, but it cannot include both **match (header map)** statements and **match (url map)** statements.
- You can specify up to two maps in a given policy: one for header 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
 header-map HOSTMAP
 url-map URLMAP
```

  In this example, a flow must match both HOSTMAP and URLMAP in order to match policy MAP-POLICY.

- If you have configured too many maps, or if your maps are too complex, the CSG generates the following syslog message:

  %CSM_SLB-3-UNEXPECTED: Module 3 unexpected error:
  Current configuration exceed memory limit for rule table.

  If you see this message, you must reduce the number and complexity of the maps in your configuration.

  To ensure that your maps are configured correctly, use the following command:

  show module csg *slot* **tech-support processor 4 | include LB common pool**

  If the **last config change** field in the output is zero, your maps are configured correctly.

You can specify more than one **match** command in CSG URL map configuration mode to specify multiple URL match expressions for a given URL map:

- If the URL matches *any* of the URL match expressions, then the match is TRUE and the flows can be processed by the CSG accounting services (unless there is another map associated with this policy that is FALSE).
- If the URL *does not* match any of the URL match expressions, then the match is FALSE and the flows are not processed by the CSG accounting services, even if other maps for this policy match TRUE.
- The URL match expressions are case-sensitive. For example, if you define the following URL match expression:

  match protocol http url http://*url-string*

  but a subscriber enters the following URL in a Web browser:

  HTTP://*url-string*

  the URL *does not* match the URL match expression, the match is FALSE, and the flow is not processed by the CSG accounting services.

Therefore, consider upper- and lowercase combinations carefully when creating URL match expressions.

- When you configure URL match patterns for RTSP streams, keep in mind that you must 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***.
- Depending on your configuration, the CSG can handle up to 1000 single-wildcard URL match patterns (for example, ***movies** or **movies***, but not ***movies***) or up to 11 double-wildcard URL match patterns (for example, ***movies*** or **http://test.*movies.com/*.mpeg**). Double-wildcard URL match patterns are also known as keyword URL match patterns. If you want to use keyword URL match patterns, keep the following considerations in mind in order to optimize the CSG's performance:
  - Minimize the number of URL match patterns that are applied to a given CSG content definition.
  - 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 pattern.
  - Combine multiple keyword URL match patterns into a single pattern 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 the following 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**

    Remember that the entire pattern, including wildcards and UNIX string-matching special characters, cannot exceed 128 characters.
- When adding or changing URL match patterns, check their impact on the CSG's memory:
  1. Enter the **show module csg status** command in privileged EXEC mode to check the status of the configuration change.
  2. When the status changes from PENDING (the change has not yet downloaded) to COMPLETE, SUCCESS (the change has downloaded successfully), enter the **show module csm memory** command in privileged EXEC mode. This command displays the CSG's total memory used versus total memory available.
- For WAP 1.x, URL maps take precedence over access lists.
- For WAP1.x and RTSP, the policy used to determine the next hop address is chosen based solely on access control lists (ACLs), not URL maps. As a result, you can choose the next hop from one policy for routing and from a different policy for billing.

Table B-2 shows the special characters that you can use in URL match expressions.

Table B-2 Special Characters for Matching String Expressions

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.

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 url
  match url *.movies_(comedy|action|drama).com/*.mpeg
```

Related Commands

Command	Description
header-map	References a header map that is part of a CSG billing policy.
ip csg map	Defines the CSG billing content filters (URL and header maps), and enters CSG map configuration mode.
ip csg policy	Defines a policy for qualifying flows for the CSG accounting services, and enters CSG policy configuration mode.
match (header map)	Specifies a header match pattern for a CSG billing map.

Command	Description
url-map	References a URL map that is part of a CSG billing policy.
show module csg status	Displays whether the CSG is online and, if so, the CSG chassis slot location and whether the configuration download is complete.

meter exclude service-idle

To exclude the final service idle from the usage calculation when the service is configured for Service Duration Billing, use the **meter exclude service-idle** command in CSG service configuration mode. To return to the default behavior, use the **no** form of the command.

meter exclude service-idle

no meter exclude service-idle

Syntax Description

This command has no arguments or keywords

Defaults

The default behavior is to include the service-idle in the usage.

Command Modes

CSG service configuration

Command History

Release	Modification
3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.

Usage Guidelines

Configuration of this command can lead to situations where charging is reduced because the next service access occurs after the service idles, instead of before the service idles.

Examples

The following example shows how to configure Service Duration Billing for the OFF_NET service:

```
ip csg service OFF_NET
  meter exclude service-idle
```

Related Commands

Command	Description
ip csg service	Defines a content billing service, and enters CSG service configuration mode.

meter imap

To specify which Internet Message Access Protocol (IMAP) bytes are billed for when doing prepaid debits, use the **meter imap** command in CSG service configuration mode. To return to the default behavior, use the **no** form of the command.

meter imap [**body-only** | **body-header** | **body-other**]

no meter imap

SyntaxDescription

body-only	Only BODY IMAP bytes are to be counted when performing prepaid debits.
body-header	Only BODY and HEADER 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

CSG service configuration

Command History

Release	Modification
3.1(1)C6(2)—12.2(18)SXE	This command was introduced.

Usage Guidelines

You can configure only one **meter 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 imap** and **basis fixed** or **basis second** in the same service. Only **basis byte** is meaningful with **meter imap**.

Examples

The following example shows how to configure IMAP to count only BODY bytes when performing prepaid debits:

```
ip csg service S1
  meter imap body-only
```

meter increment

To specify the increments for debiting quota upon completion of a service configured for Service Duration Billing, use the **meter increment** command in CSG 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	Specifies the increment, in seconds, for debiting quota upon completion of a service configured for Service Duration Billing. For example, to enable the CSG to charge quota per-minute instead of per-second, specify **meter increment 60**. The valid range is 1 to 65535. The default value is 1. **Note** The value for quadrans is always denoted as seconds.

Defaults

The default value is 1.

Command Modes

CSG service configuration

Command History

Release	Modification
3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.

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 CSG does not round up 120 seconds of network usage, but does round up 163 seconds or 173 seconds of network usage to 180 quadrans before calculating total usage for reporting in the Service Stop.

Note The round-up of network usage is not reflected in calculations for the Usage TLV in Service Reauthorization Requests.

The increment value is considered when determining if 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 meter increments for Service Duration Billing for the OFF_NET service.

```
ip csg service OFF_NET
  basis second
  meter minimum 60
  meter increment 100
  content ANY policy HTTP
  content ANY policy ANY
```

Related Commands

Command	Description
ip csg service	Defines a content billing service, and enters CSG service configuration mode.

meter initial

To specify the initial quota debited from the balance at the beginning of a service when the service is configured for Service Duration Billing, use the **meter initial** command in CSG 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	Specifies 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 CSG grants the first network access for a session mapped to the service. The initial value is not rounded up to the nearest increment value. The valid range is 0 to 65535. The default value is 0.

Defaults

The default value is 0.

Command Modes

CSG service configuration

Command History

Release	Modification
3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.

Usage Guidelines

This command allows “connection set-up charges” to be applied to a service.

Examples

The following example shows how to configure **meter initial** values for Service Duration Billing for the OFF_NET service.

```
ip csg service OFF_NET
  basis second
  meter initial 60
  content ANY policy HTTP
  content ANY policy ANY
```

Related Commands

Command	Description
ip csg service	Defines a content billing service, and enters CSG service configuration mode.

meter minimum

To specify the minimum number of quadrans debited for a service or session, excluding the value in **meter initial**, use the **meter minimum** command in CSG 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	Specifies minimum number of quadrans debited for a service or session, excluding the value in **meter initial**. For example, to force the CSG 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 valid range is 0 to 65535. The default value is 0.

Defaults

The default value is 0.

Command Modes

CSG service configuration

Command History

Release	Modification
3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.

Usage Guidelines

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, 63 seconds of network usage is rounded up to 90 quadrans for calculating usage in the Service Stop, but 150 seconds of network usage is not rounded up.

Note The round-up of network usage is not reflected in calculations for the Usage TLV in Service Reauthorization Requests.

Examples

The following example shows how to configure **meter minimum** values for Service Duration Billing for the OFF_NET service.

```
ip csg service OFF_NET
  basis second
  meter minimum 60
  content ANY policy HTTP
  content ANY policy ANY
```

Related Commands

Command	Description
ip csg service	Defines a content billing service, and enters CSG service configuration mode.

mode

To specify that a billing plan is postpaid or prepaid, use the **mode** command in CSG billing configuration mode. To return to the default mode, use the **no** form of this command.

mode [**postpaid** | **prepaid**]

no mode

Syntax Description

postpaid	Specifies a postpaid billing service.
prepaid	Specifies a prepaid billing service. This is the default setting.

Defaults

The default setting is **prepaid**.

Command Modes

CSG billing configuration

Command History

Release	Modification
3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.
3.1(3)C5(3)—12.2(18)SXD	Support for using variable record format with **mode postpaid** to enable service correlation of postpaid CDRs was added.

Usage Guidelines

Mode postpaid is used with both fixed- and variable-record format to enable service correlation of postpaid CDRs.

Examples

The following example specifies **mode postpaid**.

```
ip csg billing FOO
  mode postpaid
```

Related Commands

Command	Description
assign	Associates an IP address with a transport-type value.
class	Specifies a service class value.
hostname	Specifies a variable hostname for a CSG module.
ip csg transport-type	Classifies data traffic based on its access path.
owner id	Specifies an identifier for a service owner.
owner name	Specifies the name of a service owner.
records format	Specifies **variable** or **fixed** CDR format.

module csg

To enter module CSG configuration mode for a specified slot, use the **module csg** command in global configuration mode. To remove the **module csg** configuration, use the **no** form of this command.

module csg *slot-number*

no module csg *slot-number*

Caution For Cisco IOS releases prior to 12.2(18)SXD, entering the **no** form of this command (**no module csg** *slot-number*) removes your existing **module csg** configuration with no warning message!

For Cisco IOS releases 12.2(18)SXD and later, the CSG issues a warning message and does not remove your existing **module csg** configuration unless you have already removed all underlying accounting.

Syntax Description

slot-number	Slot number where the CSG resides.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

The full syntax for this command is **module ContentServicesGateway** *slot-number*; **module csg** *slot-number* is a valid shortcut.

The following commands in module CSG configuration mode specify which accounting services to download, as well as the binding of VLANs with the accounting service:

- **accounting (module CSG)**
- **ruleset**
- **vlan (module CSG)**

Examples

The following example shows how to configure the CSG in slot 4:

```
module csg 4
 accounting A1
 ft group 123 vlan 5
 ruleset R1
 vlan 30 client
 vlan 32 client
 vlan 40 server
```

Related Commands

Command	Description
accounting (module CSG)	Downloads a configured accounting service to a CSG card.
ft group (module CSG)	Enters fault-tolerant configuration mode and configures fault tolerance.
ruleset	Downloads all content defined by a ruleset to a CSG card.
vlan (module CSG)	Creates a client or server VLAN that defines the Layer 2 paths for the CSG accounting service flows, assigns a VLAN ID and optional name, and enters module CSG VLAN configuration mode.

next-hop

To define a next-hop IP address, use the **next-hop** command in CSG policy configuration mode. To return to the default mode, use the **no** form of this command.

next-hop *ip-address*

no next-hop *ip-address*

Syntax Description

ip-address	IP address of the next hop.

Defaults

No default behavior or values.

Command Modes

CSG policy configuration

Command History

Release	Modification
3.1(3)C5(3)—12.2(18)SXD	This command was introduced.

Usage Guidelines

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 policy. For example, the following configuration is valid, because both policies use **client group 1** and **next-hop 1**:

```
policy A
  accounting type wap connection-oriented
  url A
  client group 1
  next-hop 1
policy B
  accounting type wap connection-oriented
  url B
  client group 1
  next-hop 1
content WAP-CON
  policy A
  policy B
```

The following configuration is not valid, because policy A uses **client group 1** and **next-hop 1**, but policy B uses **client group 1** and **next-hop 2**:

```
policy A
  accounting type wap connection-oriented
  url A
  client group 1
  next-hop 1
policy B
  accounting type wap connection-oriented
  url B
  client group 1
  next-hop 2
content WAP-CON
```

```
policy A
policy B
```

If you associate more than one policy with the same content definition, the CSG determines the next-hop based on the first policy match within any data flow (TCP connection). The CSG reports all subsequent policy matches within that flow as configured, but ignores the next-hop information.

- For **type http** accounting, the first policy match is based on the first HTTP request within a persistent connection.
- For other Layer 7 inspection, the first policy match is based on the first packet. For example for **type wap** accounting, the first policy match is based on the WSP connection request.

Traffic initiated from a next-hop does not require a virtual server/content definition in order to be routed through the CSG.

Examples

The following example specifies **next-hop**.

```
ip csg policy FTP-MS-APN
  accounting type ftp customer-string FTP-POL
  client-group 11
  next-hop 33.0.0.150
```

Related Commands

Command	Description
client-group (CSG policy)	References a standard access list that is part of a CSG billing policy.
ip csg policy	Defines a policy for qualifying flows for the CSG accounting services, and enters CSG policy configuration mode.

owner id

To specify an identifier for a service owner, use the **owner id** command in CSG service configuration mode. To remove the owner ID, use the **no** form of this command.

owner id *id*

no owner id *id*

Syntax Description

id	1- to 15-character string identifying a service owner.

Defaults

No default behavior or values.

Command Modes

CSG service configuration

Command History

Release	Modification
3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.

Usage Guidelines

Use this command with fixed-record format to identify a service owner.

Examples

The following example specifies an owner ID for the service:

```
ip csg service FOO
  owner id ABC123456
```

Related Commands

Command	Description
assign	Associates an IPv4 address with a transport-type value.
class	Specifies a service class value.
hostname	Specifies a variable hostname for a CSG module.
ip csg service	Defines a content billing service, and enters CSG service configuration mode.
ip csg transport-type	Classifies data traffic based on its access path.
mode	Specifies that a billing plan is postpaid or prepaid.
owner name	Specifies the name of a service owner.
records format	Specifies **variable** or **fixed** CDR format.

owner name

To specify the name of a service owner, use the **owner name** command in CSG service configuration mode. To remove the owner name, use the **no** form of this command.

owner name *name*

no owner name

Syntax Description

name	1- to 38-character string specifying the name of the service.

Defaults

No default behavior or values.

Command Modes

CSG service configuration

Command History

Release	Modification
3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.

Usage Guidelines

Owner name is used with fixed-record format to identify a service owner.

Examples

The following example specifies an owner name for the service:

```
ip csg service FOO
  owner name ABC_CORP
```

Related Commands

Command	Description
assign	Associates an IPv4 address with a transport-type value.
class	Specifies a service class value.
hostname	Specifies a variable hostname for a CSG module.
ip csg service	Defines a content billing service, and enters CSG service configuration mode.
ip csg transport-type	Classifies data traffic based on its access path.
mode	Specifies that a billing plan is postpaid or prepaid.
owner id	Specifies an identifier for a service owner.
records format	Specifies **variable** or **fixed** CDR format.

passthrough

To enable passthrough mode for a service, use the **passthrough** command in CSG service configuration mode. To disable passthrough mode, use the **no** form of this command.

passthrough *quota-grant*

no passthrough *quota-grant*

Syntax Description

quota-grant	Size of each quota grant to give to the service. The *quota-grant* is also called the default quota. Range is 1 to 2147483647.

Defaults

No default behavior or values.

Command Modes

CSG service configuration

Command History

Release	Modification
3.1(3)C5(5)—12.2(18)SXD	This command was introduced.

Usage Guidelines

Use this command to enable the CSG to grant quota to the service when at least one quota server is configured, but none are active.

If you enable passthrough mode for a service, do not disable quota server reassignment for user groups associated with that service. That is, do not configure **no quota server reassign** in CSG user group configuration mode for user groups associated with the service.

Examples

The following example specifies that the CSG 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	Defines a content billing service, and enters CSG service configuration mode.

pending

To set the pending connection timeout, use the **pending** command in CSG 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 before a connection is considered unreachable. The valid range is 4 seconds to 65535 seconds. The default value is 30 seconds.

Defaults

The default pending timeout is 30 seconds.

Command Modes

CSG content configuration

Command History

Release	Modification
3.1(3)C5(3)—12.2(18)SXD	This command was introduced.

Usage Guidelines

The pending connection timeout sets the response time for terminating connections if a switch becomes flooded with traffic. The pending connections are configurable on a per-content basis.

Examples

This example shows how to set the pending timer:

```
ip csg content MOVIES_COMEDY
  pending 300
```

Related Commands

Command	Description
ip csg content	Defines content for the CSG accounting services, and enters CSG accounting configuration mode.
show module csg content	Displays statistics and counters for the CSG content.

policy (CSG content)

To reference a CSG billing policy, use the **policy** command in CSG content configuration mode. To delete a policy reference, use the **no** form of this command.

policy *policy-name*

no policy *policy-name*

Syntax Description

policy-name	Name of a configured CSG billing policy.

Defaults

No default behavior or values.

Command Modes

CSG content configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

If accounting records are to be generated for this content definition, you must reference at least one policy that contains the **accounting** command.

You can reference more than one policy in a given content definition, using multiple **policy** commands.

If multiple policies are defined under **ip csg content**, they must all have the same accounting type. For example, if one of the policies is configured with **accounting type wap**, they all must have **accounting type wap**.

Examples

The following example shows how to reference a policy named POLICY1:

```
ip csg content MOVIES_COMEDY
 client 10.4.4.0 255.255.255.0
 idle 120
 ip 172.18.45.0/24 tcp 8080
 policy POLICY1
 replicate connection tcp
 vlan MOVIES_COMEDY
 inservice
```

Related Commands

Command	Description
ip csg content	Defines content for the CSG accounting services, and enters CSG accounting configuration mode.
show module csg content	Displays statistics and counters for the CSG content.

priority

To set the priority of the CSG, use the **priority** command in fault-tolerant configuration mode. To restore the priority default value, use the **no** form of this command.

priority *value*

no priority

Syntax Description

value	Priority of the CSG. The valid range is 1 to 254. The default value is 10. A higher number indicates a higher priority.

Defaults

The default priority value is 10.

Command Modes

Fault-tolerant configuration

Command History

Release	Modification
2.2(1)C(1)—12.1(11b)E3	This command was introduced.

Usage Guidelines

The CSG with the largest priority value is the primary CSG in the fault-tolerant pair when the modules are both operating.

Examples

The following example shows how to set the priority value to 12:

```
ft group 123 vlan 5
 failover 6
 heartbeat-time 2
 priority 12
```

Related Commands

Command	Description
ft group (module CSG)	Enters fault-tolerant configuration mode and configures fault tolerance.
show module csg ft	Displays statistics and counters for the CSG fault-tolerant pair.

quota activate

To simultaneously activate multiple quota servers, and to assign a quota server to each user, use the **quota activate** command in CSG user group configuration mode. To deactivate quota servers, use the **no** form of this command.

quota activate *number*

no quota activate *number*

Syntax Description

number	Identifies a specific quota server to activate, or to assign to a specific user. You can use any number from 1 through 10.

Defaults

The default value is 1.

Command Modes

CSG user group configuration.

Command History

Release	Modification
3.1(1)C4(1)—12.2(14)ZA	This command was introduced.

Examples

The following example shows how to activate quota 2 and assign it to user U1:

```
ip csg user U1
(config-csg-group)# quota activate 2
```

quota local-port

To configure the local port on which the CSG receives communications from quota servers, use the **quota local-port** command in CSG user group configuration mode. To remove a quota local-port configuration, use the **no** form of this command.

quota local-port *port-number*

no quota local-port *port-number*

Syntax Description

port-number	The port number on which the CSG is to receive communications from quota servers. The valid range is 1 to 65535. The quota local port and the agent local port cannot be the same.

Defaults

No quota local ports are configured.

Command Modes

CSG user group configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

For prepaid billing, you must specify a quota local port.

Note The CSG drops requests (such as nodealive, echo, and redirect requests) unless they come from a configured quota server IP address. The CSG also verifies IP addresses contained in NodeAddress IEs against the configured list of quota servers. If there is no match, the CSG drops the request. The CSG does not look at a request's source port, replying to the same port from which the request came.

Examples

The following example configures quota local port 6666 for the CSG user-group G1:

```
ip csg user-group G1
 entries max 100000
 database 10.1.2.3 11111
 quota local-port 6666
 quota server 10.1.4.5 888 1
 quota server 10.1.6.7 999 2
 radius acct-port 7777
 radius key SECRET_PASSWORD
 radius parse strict
 radius server 10.13.14.15
 radius userid User-Name
 redirect nat 10.33.33.3
```

Related Commands

Command	Description
ip csg user-group	Creates a group of end users for which you want to generate accounting records

quota server

To configure the quota servers that return billing quota values for users, use the **quota server** command in CSG user group configuration mode. To remove a quota server configuration, use the **no** form of this command.

quota server {*ip-address port-number priority* | **reassign**}

no quota server {*ip-address port-number priority* | **reassign**}

Syntax Description

ip-address	IP address of the quota server. The CSG differentiates quota servers based on IP addresses. When you configure a quota server, make sure its IP address matches on both the active CSG and on the backup CSG.
port-number	Port number of the quota server. The valid range is 1 to 65535. The CSG differentiates quota servers based on port numbers. When you configure a quota server, make sure its port number matches on both the active CSG and on the backup CSG.
priority	Allows you to define primary and backup 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 CSG 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.
reassign	Enables quota server reassignment after a failure.

Defaults

No quota servers are configured, and quota servers are reassigned after a failure.

Command Modes

CSG user group configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.
3.1(1)C6(2)—12.2(18)SXE	The **reassign** keyword was added.

Usage Guidelines

For prepaid billing, you must specify at least one quota server. You can specify up to 10 quota servers, each with a unique IP address and a unique priority.

A quota server can recognize a duplicate quota-download request, as when general packet radio service (GPRS) tunnelling 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.

Note The CSG does not support multiple quota servers that have the same IP address.

To disable quota server reassignment (that is, to prevent the CSG from assigning a new quota server to a user if the original quota server fails), use the **no** form of this command with the **reassign** keyword.

If you enable passthrough mode for a service (by using the **passthrough** command in CSG service configuration mode), do not disable quota server reassignment for user groups associated with that service. That is, do not configure **no quota server reassign** for user groups associated with the service.

Examples

The following example configures two quota servers for the CSG user-group G1 with priorities 1 and 2:

```
ip csg user-group G1
 entries max 100000
 database 10.1.2.3 11111
 quota local-port 6666
 quota server 10.1.4.5 888 1
 quota server 10.1.6.7 999 2
 radius acct-port 7777
 radius key SECRET_PASSWORD
 radius parse strict
 radius server 10.13.14.15
 radius userid User-Name
 redirect nat 10.33.33.3
```

Related Commands

Command	Description
ip csg user-group	Creates a group of end users for which you want to generate accounting records

radius acct-port

To configure the RADIUS listening port when it is different from the established RADIUS default of 1813, use the **radius acct-port** command in CSG user group configuration mode. To return to the default value, use the **no** form of this command.

radius acct-port *port-number*

no radius acct-port

Syntax Description

port-number	Listening port number of the RADIUS server. The valid range is 1 to 65535. The default port number is 1813.

Defaults

The default port number is 1813.

Command Modes

CSG user group configuration

Command History

Release	Modification
2.2(1)C(1)—12.1(11b)E3	This command was introduced.

Examples

The following example shows how to configure RADIUS listening port 7777 for the CSG user-group G1:

```
ip csg user-group G1
 entries max 100000
 database 10.1.2.3 11111
 quota local-port 6666
 quota server 10.1.4.5 888 1
 quota server 10.1.6.7 999 2
 radius acct-port 7777
 radius key SECRET_PASSWORD
 radius parse strict
 radius server 10.13.14.15
 radius userid User-Name
 redirect nat 10.33.33.3
```

Related Commands

Command	Description
radius key	Specifies the CSG to be the RADIUS endpoint for accounting records, and specifies the secret key.
radius start restart session-id	Specifies the RADIUS attribute used to extract the user identifier from a RADIUS record.

radius ack error

To enable the CSG to generate a RADIUS response to an Accounting Start Request or Accounting Interim Request when it encounters an error condition, use the **radius ack error** command in CSG user group configuration mode. To prevent RADIUS responses to errors, use the **no** form of this command.

radius ack error

no radius ack error

Syntax Description

There are no arguments or keywords.

Defaults

The CSG generates a RADIUS response to an Accounting Start Request or Accounting Interim Request when it encounters an error condition.

Command Modes

CSG user group configuration

Command History

Release	Modification
3.1(1)C6(2)—12.2(18)SXE	This command was introduced.

Usage Guidelines

Use the **no** form of this command to prevent the CSG from acknowledging the following errors:

1. The User Table entry cannot be created due to resource constraints.
2. The CSG parses the Accounting Request and encounters RADIUS protocol errors.
3. The CSG parses the Accounting Request and a billing plan is specified in the Accounting Request, but it does not match a billing plan in the CSG configuration.
4. The CSG parses the Accounting Request and a quota server is specified in the Accounting Request, but it does not match a quota server in the CSG configuration.
5. The CSG parses the Accounting Request and a connect service is specified in the Accounting Request, but it does not match a connect service in the CSG configuration.

   For errors 3, 4, and 5, the CSG can parse the configuration VSA from the Access-Accept. If the CSG uses any attribute from the Access-Accept that does not match the CSG configuration, the CSG does not send a RADIUS response to the Accounting Request.

For RADIUS accounting requests processed as a result of matching a **radius endpoint** command, the CSG does not send a RADIUS acknowledgement.

For RADIUS accounting requests processed as a result of matching a **radius proxy** command, the CSG does not forward the Accounting Request to the RADIUS server.

To prevent existing entries from being reused for new users when the User Table is full, use the **no** form of this command, **no radius ack error**.

Examples

The following examples shows how to prevent RADIUS responses to RADIUS Accounting Start Requests and Accounting Interim Requests when errors are encountered.

```
ip csg usergroup UGROUP
  no radius ack error
```

Related Commands

Command	Description
radius endpoint	Identifies the CSG as an endpoint for RADIUS Accounting messages.
radius proxy	Specifies that the CSG should be a proxy for RADIUS messages.

radius endpoint

To identify the CSG as an endpoint for RADIUS Accounting messages, use the **radius endpoint** command in module CSG configuration mode. To remove the endpoint identification, use the **no** form of this command.

radius endpoint *csg_addr* **key** [*encrypt*] *secret-string* [**table** *table-name*]

no radius endpoint *csg_addr* **key** [*encrypt*] *secret-string* [**table** *table-name*]

Syntax Description

csg_addr	Specifies the CSG IP address. The CSG IP address must be a virtual IP address, and it must be unique. The CSG IP address must not be specified in other CSG commands, and it must not match any real IP address, virtual IP address, or alias IP address configured on the CSG.
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, **wr mem**). 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 plus the encrypted text. See the Cisco IOS **service** command for more details.
secret-string	1- to 64-character clear password. All characters are valid; case is significant. The *secret-string* is always sent in plain text to the CSG module when the configuration is downloaded. *Secret-string* must match the secret specified on the RADIUS client (for example, the GGSN).
table *table-name*	(Optional) Associates the specified table name with the RADIUS endpoint. The *table-name* argument is a 1-to-15 character string identifying the table. The CSG stores the table name as all-uppercase ASCII characters.

Defaults

The *secret-string* is stored in plain text.

Command Modes

Module CSG configuration

Command History

Release	Modification
3.1(3)C5(5)—12.2(18)SXD	This command was introduced.
3.1(1)C6(2)—12.2(18)SXE	The **table** keyword and *table-name* argument were added.

Usage Guidelines

A RADIUS Accounting message sent to the specified *csg_addr* (and any port) is parsed, and then acknowledged, by the CSG.

The User Table identifies all users known to the CSG. The 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. User table entries created as a result of RADIUS messaging through **radius endpoint** definition with a **table** configured are indexed by the configured *table-name*. This enables the CSG to segment the user space and removes ambiguity if multiple users share the same IP address, provided that their entries were instantiated by RADIUS flows to CSG radius definitions bound to different table-names.

To change the RADIUS endpoint *table-name* associated with a given *csg_addr*, you must first enter the **no** form of the **radius endpoint** command for that *csg_addr*, then enter the command with the new *table-name*.

To support RADIUS endpoint, the CSG requires a route to 255.255.255.255. You can configure the route by using the **gateway (module CSG VLAN)** command or the **route (module CSG VLAN)** command. For example:

gateway 31.0.0.6

or:

route 255.255.255.255 255.255.255.255 gateway 31.0.0.6

Note If you already have a gateway configured, you do not need to configure an additional gateway for the RADIUS endpoint.

When the CSG2 is configured as a RADIUS endpoint, the CSG2 drops all RADIUS packets other than RADIUS Accounting-Request messages.

Examples

The following example shows how to identify the CSG as a RADIUS endpoint:

```
module csg 3
  radius endpoint 1.2.3.4 key secret
```

The following example illustrates how to use the **radius endpoint** command to create an endpoint point that maps to table ACME_VLAN, to be used as part of a user index for users created as a result of traffic to this **radius endpoint** definition.

```
module csg 3
  radius endpoint 1.2.3.4 key secret table ACME_VLAN
```

Related Commands

Command	Description
radius userid	Specifies the RADIUS attribute used to extract the user identifier from a RADIUS record.

radius handoff

To configure RADIUS handoff support, use the **radius handoff** command in CSG user group configuration mode. To turn off the timer, use the **no** form of this command.

radius handoff [*duration*]

no radius handoff

Syntax Description

duration	Handoff timer duration in seconds. The handoff timer is started when an Accounting Stop is received. If the handoff timer expires before an accounting start for a user is seen, the CSG assumes a handoff did not occur and deletes the User Table entry for the user. Valid values range from 0 to 43200 seconds. The default is 0 seconds (no handoff timer).

Defaults

The default *duration* is 0 seconds (no handoff timer).

Command Modes

CSG user group configuration

Command History

Release	Modification
3.1(3)C5(5)—12.2(18)SXD	This command was introduced.

Usage Guidelines

The User Table identifies all users known to the CSG. The 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.

Examples

The following example shows how to specify a RADIUS handoff timer duration of 1000 seconds:

```
ip csg user-group G1
  radius handoff 1000
```

radius key

To specify and configure the CSG to be the RADIUS endpoint for accounting records, and to designate that the CSG is to use the accounting records to maintain user IDs, use the **radius key** command in CSG user group configuration mode. To delete the key and disable RADIUS, use the **no** form of this command.

radius key [*encrypt*] *secret-string*

no radius key

Syntax Description

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, **wr mem**). 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 plus the encrypted text. See the Cisco IOS **service** command for more details.
secret-string	1- to 64-character clear password. All characters are valid; case is significant. The *secret-string* is always sent in plain text to the CSG module when the configuration is downloaded. *Secret-string* must match the secret specified on the RADIUS client (for example, the GGSN).

Defaults

The *secret-string* is stored in the plain text.

Command Modes

CSG user group configuration

Command History

Release	Modification
2.2(1)C(1)—12.1(11b)E3	This command was introduced.

Examples

The following example shows how to specify the RADIUS key SECRET_PASSWORD for the CSG user-group G1:

```
ip csg user-group G1
 entries max 100000
 database 10.1.2.3 11111
 quota local-port 6666
 quota server 10.1.4.5 888 1
```

```
quota server 10.1.6.7 999 2
radius acct-port 7777
radius key SECRET_PASSWORD
radius parse strict
radius server 10.13.14.15
radius userid User-Name
redirect nat 10.33.33.3
```

Related Commands

Command	Description
radius start restart session-id	Specifies the search RADIUS attribute used to extract the user identifier from a RADIUS record.
radius acct-port	Configures the RADIUS listening port when it is different from the RADIUS default of 1813.

radius monitor

To specify that the CSG should monitor the RADIUS flows to the specified server, use the **radius monitor** command in CSG user group configuration mode. To stop monitoring the RADIUS flows, use the **no** form of this command.

radius monitor *server_addr server_port* [**key** [*encrypt*] *secret-string*]

no radius monitor *server_addr server_port* [**key** [*encrypt*] *secret-string*]

Syntax Description

server_addr	Specifies the server address to monitor.
server_port	Specifies the port number 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, **wr mem**). 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 plus the encrypted text. See the Cisco IOS **service** command for more details.
secret-string	(Optional) 1- to 64-character clear password. All characters are valid; case is significant. The *secret-string* is always sent in plain text to the CSG module when the configuration is downloaded. *Secret-string* must match the secret specified on the RADIUS client (for example, the GGSN).

Defaults

The *secret-string* is stored in plain text.

Command Modes

CSG user group configuration

Command History

Release	Modification
3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.

Usage Guidelines

The RADIUS key and encryption level are optional; the CSG always forwards the message. If specified, the CSG parses the message only if the RADIUS authenticator was created using encryption. If the key is not configured, the CSG always parses the message.

All RADIUS messages, including access messages, are forwarded, except when the IP or UDP headers specify a length larger than the physical packet size.

Note The CSG is not a proxy. The network must be set up so that packets are sent through the CSG, not to the CSG.

Examples

The following example illustrates the use of the **radius monitor** command:

```
ip csg user-group G1
  radius userid User-Name
  radius monitor 1.2.3.4 1813 key secret
```

Related Commands

Command	Description
radius userid	Specifies the RADIUS attribute used to extract the user identifier from a RADIUS record.

radius parse strict

To tighten the parsing rules for RADIUS flows, use the **radius parse strict** command in CSG user group configuration mode. To relax the parsing rules, use the **no** form of this command.

radius parse strict

no radius parse strict

Syntax Description

This command has no arguments or keywords.

Defaults

The parsing rules are relaxed.

Command Modes

CSG user group configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

When you configure this command, the CSG fails parsing if the length of the user ID (RADIUS Attribute 1 [User-Name] or RADIUS Attribute 31 [Calling-Station-Id], as configured) is less than the minimum (3).

Examples

The following example tightens the parsing rules for RADIUS flows for the CSG user-group G1:

```
ip csg user-group G1
 entries max 100000
 database 10.1.2.3 11111
 quota local-port 6666
 quota server 10.1.4.5 888 1
 quota server 10.1.6.7 999 2
 radius acct-port 7777
 radius key SECRET_PASSWORD
 radius parse strict
 radius server 10.13.14.15
 radius userid User-Name
 redirect nat 10.33.33.3
```

Related Commands

Command	Description
radius start restart session-id	Specifies the search RADIUS attribute used to extract the user identifier from a RADIUS record.
radius acct-port	Configures the RADIUS listening port when it is different from the RADIUS default of 1813.

radius pod attribute

To specify the RADIUS attributes to be copied from the RADIUS Start message and sent to the NAS in the Packet of Disconnect (PoD) message, use the **radius pod attribute** command in CSG user group configuration mode. To disable this feature, use the **no** form of this command.

radius pod attribute *radius_attribute_number*

no radius pod attribute *radius_attribute_number*

Syntax Description

radius_attribute_number	Specifies the number of the RADIUS attribute to be copied from the RADIUS Start message and sent to the NAS in the PoD message.

Defaults

No RADIUS attributes are sent in the PoD message.

Command Modes

CSG user group configuration

Command History

Release	Modification
3.1(3)C5(5)—12.2(18)SXD	This command was introduced.

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. If the list of configured attributes changes, only new RADIUS messages are subject to the new attributes. Attributes already saved continue to be included in the PoD message.

When a RADIUS Start request is received, any attributes received from a previous Start request are deleted.

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:

```
ip csg user-group G1
  radius pod attribute 44
  radius pod attribute 26
```

Related Commands

Command	Description
radius pod nas	Specifies the NAS port to which the CSG should send the Packet of Disconnect (PoD) message, and the key to use in calculating the Authenticator.
radius pod timeout	Specifies the number of times to retry the RADIUS Packet of Disconnect (PoD) message if it is not ACKed, and the interval between retransmissions.

radius pod nas

To specify the NAS port to which the CSG should send the Packet of Disconnect (PoD) message, and the key to use in calculating the Authenticator, use the **radius pod nas** command in CSG user group configuration mode. To restore the default settings, use the **no** form of this command.

radius pod nas [*start-ip end-ip*] *port* **key** [*encrypt*] *secret-string*

no radius pod nas [*start-ip end-ip*] *port* **key** [*encrypt*] *secret-string*

Syntax Description

start-ip	Specifies the first NAS IP address in a range of addresses.
end-ip	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, **wr mem**). 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 plus the encrypted text. See the Cisco IOS **service** command for more details.
secret-string	1- to 64-character clear password. All characters are valid; case is significant. The *secret-string* is always sent in plain text to the CSG module when the configuration is downloaded. *Secret-string* must match the secret specified on the RADIUS client (for example, the GGSN).

Defaults

The *secret-string* is stored in plain text.

Command Modes

CSG user group configuration

Command History

Release	Modification
3.1(3)C5(5)—12.2(18)SXD	This command was introduced.

Usage Guidelines

The PoD message is sent to the NAS IP address specified in the NAS-IP-Address attribute (4) in the Accounting Start message. This command specifies the NAS listen port, as well as the key to use in calculating the Authenticator.

The Accounting Start must have been received on an IP address specified in the enhanced proxy or endpoint (**radius proxy** or **radius endpoint**) command configured in module CSG configuration mode.

In some networks, many NASs might use the same listen 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 NASs. 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 user-group G1
  radius userid User-Name
  radius pod attribute 44
  radius pod nas 1.1.1.0 1.1.1.255 1700 key secret
  radius pod nas 1701 key password

mod csg 3
  radius proxy 1.2.3.4 5.6.7.8 key secret
```

Related Commands

Command	Description
radius pod attribute	Specifies the RADIUS attributes to be copied from the RADIUS Start message and sent to the NAS in the Packet of Disconnect (PoD).
radius pod timeout	Specifies the number of times to retry the RADIUS Packet of Disconnect (PoD) message if it is not ACKed, and the interval between retransmissions.

radius pod timeout

To specify the number of times to retry the RADIUS Packet of Disconnect (PoD) message if it is not ACKed, and the interval between retransmissions, use the **radius pod timeout** command in CSG user group configuration mode. To restore the default timeout, use the **no** form of this command.

radius pod timeout *timeout* **retransmit** *retransmit*

no 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 default timeout is 5 seconds.
retransmit *retransmit*	Number of times to retransmit the message. The default setting is 3 retransmits.

Defaults

The default timeout is 5 seconds.

The default number of retransmits is 3 retransmits.

Command Modes

CSG user group configuration

Command History

Release	Modification
3.1(3)C5(5)—12.2(18)SXD	This command was introduced.

Examples

The following example shows how to specify a RADIUS PoD timeout and retries:

```
ip csg user-group G1
  radius pod timeout 30 retransmits 5
```

Related Commands

Command	Description
radius pod attribute	Specifies the RADIUS attributes to be copied from the RADIUS Start message and sent to the NAS in the Packet of Disconnect (PoD).
radius pod nas	Specifies the NAS port to which the CSG should send the Packet of Disconnect (PoD) message, and the key to use in calculating the Authenticator.

radius proxy

To specify that the CSG should be a proxy for RADIUS messages, use the **radius proxy** command in module CSG configuration mode. to stop the CSG from proxying for RADIUS messages, use the **no** form of this command.

radius proxy *csg_addr server_addr* [*csg_source_addr*] [**key** [*encrypt*] *secret-string*] [**table** *table-name*]

no radius proxy *csg_addr server_addr* [*csg_source_addr*] [**key** [*encrypt*] *secret-string*] [**table** *table-name*]

Syntax Description

csg_addr	Specifies the CSG IP address. The CSG IP address must be a virtual IP address, and it must be unique. The CSG IP address must not be specified in other CSG commands, and it must not match any real IP address, virtual IP address, or alias IP address configured on the CSG or in a /32 content configuration.
server_addr	Specifies the server IP address.
csg_source_addr	Specifies the source IP address the CSG is to use when sending packets to the server. By default, *csg_source_addr* is set to *csg_addr*.
key	(Optional) Specifies a RADIUS key. Specify no more than one **key** for each CSG 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, **wr mem**). 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 plus the encrypted text. See the Cisco IOS **service** command for more details.
secret-string	(Optional) 1- to 64-character clear password. All characters are valid; case is significant. The *secret-string* is always sent in plain text to the CSG module when the configuration is downloaded. *Secret-string* must match the secret specified on the RADIUS client (for example, the GGSN).
table *table-name*	Associates the specified table name with the RADIUS proxy. The *table-name* argument is a 1-to-15 character string identifying the table. The CSG stores the table name as all-uppercase ASCII characters.

Defaults

The *secret-string* is stored in plain text.

The CSG_*source_addr* is set to *csg_addr.*

Command Modes

Module CSG configuration

Command History

Release	Modification
3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.
3.1(3)C5(5)—12.2(18)SXD	The CSG_*source_addr* argument was added.
3.1(1)C6(2)—12.2(18)SXE	The **table** keyword and *table-name* argument were added.

Usage Guidelines

A message sent to the specified *csg_addr* (and any port) is parsed and then forwarded to the specified server. When forwarded to the server, the source IP address is the CSG_*source_addr*, if configured, or the CSG_*addr* otherwise.

The source port is arbitrarily chosen by the CSG, and the destination port remains unchanged. When a message is received from the server and forwarded to the client, the source IP address is the CSG_*addr* 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 client.

You can configure an optional RADIUS key. If you configure a key, the CSG parses and acts on the message only if the RADIUS authenticator is correct. If the key is not configured, the CSG always parses the message. Whether you configure a key or not, and whether it is correct or not, the CSG always forwards the message.

You can specify up to 32 **radius proxy** commands.

You can specify more than one RADIUS **key** by specifying more than one **radius proxy** command, but each command must specify a unique CSG IP address.

All RADIUS messages are forwarded, except when the IP or UDP headers specify a length larger than the physical packet size.

The User Table identifies all users known to the CSG. The 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. User table entries created as a result of RADIUS messaging through **radius proxy** definition with a **table** configured are indexed by the configured *table-name*. This enables the CSG to segment the user space and removes ambiguity if multiple users share the same IP address, provided that their entries were instantiated by RADIUS flows to CSG radius definitions bound to different table-names.

You can define up to 64,511 clients, where a client is defined by its IP address and port.

Note If your network is designed to check the authorization string in RADIUS messages, you should enter a secret-string. Additionally, if you configure the **user-profile server radius remove** command, you might need to configure a secret-string.

To change the RADIUS proxy *table-name* associated with a given *csg_addr*, you must first enter the **no** form of the **radius proxy** command for that *csg_addr*, then enter the command with the new *table-name*.

Examples

The following example illustrates how to use the **radius proxy** command:

```
ip csg user-group G1
  radius userid User-Name
!
mod csg 3
  radius proxy 1.2.3.4 5.6.7.8 key secret
```

The following example illustrates how to use the **radius proxy** command to create a proxy point that maps to table ACME_VLAN, to be used as part of a user index for users created as a result of traffic to this **radius proxy** definition.

```
ip csg user-group G1
  radius userid User-Name
!
mod csg 3
  radius proxy 1.2.3.4 5.6.7.8 key secret table ACME_VLAN
```

Related Commands

Command	Description
radius userid	Specifies the RADIUS attribute used to extract the user identifier from a RADIUS record.

radius server

To enable RADIUS proxy, use the **radius server** command in CSG user group configuration mode. To remove the RADIUS server configuration, use the **no** form of this command.

radius server *ip-address* [*port-number*]

no radius server *ip-address* [*port-number*]

Syntax Description

ip-address	The IP address of the RADIUS server.
port-number	(Optional) The port number of the RADIUS server. The valid range is 1 to 65535. The default port number is 1813 (the default RADIUS port).

Defaults

The default port number is 1813.

Command Modes

CSG user group configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

When the CSG acts as a RADIUS proxy, proxied messages are forwarded to this RADIUS server.

Examples

The following example configures a RADIUS server for the CSG user-group G1, with IP address 10.13.14.15 and the default RADIUS port, 1813:

```
ip csg user-group G1
 entries max 100000
 database 10.1.2.3 11111
 quota local-port 6666
 quota server 10.1.4.5 888 1
 quota server 10.1.6.7 999 2
 radius acct-port 7777
 radius key SECRET_PASSWORD
 radius parse strict
 radius server 10.13.14.15
 radius userid User-Name
 redirect nat 10.33.33.3
```

Related Commands

Command	Description
radius start restart session-id	Specifies the search RADIUS attribute used to extract the user identifier from a RADIUS record.
radius acct-port	Configures the RADIUS listening port when it is different from the RADIUS default of 1813.

radius start restart session-id

To delete an existing CSG User Table entry for a specific user, and to create a new entry for that user, use the **radius start restart session-id** command in CSG user group configuration mode.

radius start restart session-id {*attr_number* | {**26** | **vsa**} {*vendor_id* | **3gpp**} *sub-attr_number*}

Syntax Description

attr_ number	Specifies the RADIUS attribute number.
26	RADIUS attribute number 26.
vsa	Specifies the vendor-specific attribute.
vendor_id	Specifies the vendor ID number
3gpp	Specifies the 3gpp vendor ID.
sub-attr_number	Specifies the sub-attribute number.

Defaults

The default behavior is that existing User Table entries are not deleted.

Command Modes

CSG user group configuration

Command History

Release	Modification
3.1(3)C4(9)—12.2(14)ZA2	This command was introduced.

Usage Guidelines

This command:

- Deletes an existing CSG User Table entry for a specific user (when a RADIUS Accounting Start or RADIUS Intermediate Accounting is received).
- Creates a new entry for that user (similar to when a RADIUS Accounting Stop has been received).
- Terminates all sessions for that user.

In order to detect duplicate RADIUS requests (which dictates that the existing entry is not deleted), specify the attribute (which might be a vendor-specific attribute) 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 **radius start restart session-id** command:

```
ip csg user-group U1
  radius start restart session-id 44
```

radius stop purge

To specify the attribute (which might be a vendor-specific attribute) that must be included in the RADIUS Accounting Stop request in order for the User Table entry to be deleted, use the **radius stop purge** command in CSG user group configuration mode.

radius stop purge {*attr_number* | **{26 | vsa}** {*vendor_id* | **3gpp}** *sub-attr_number*}

Syntax Description

attr_ number	Specifies the RADIUS attribute number.
26	RADIUS attribute number 26.
vsa	Specifies the vendor specific attribute.
vendor_id	Specifies the vendor's ID number
3gpp	Specifies the 3gpp vendor ID.
sub-attr_number	Specifies the sub-attribute number.

Defaults

The user entry is deleted when a stop is received.

Command Modes

CSG user group configuration

Command History

Release	Modification
3.1(3)C4(9)—12.2(14)ZA2	This command was introduced.

Usage Guidelines

The **radius stop purge** command specifies the attribute (which might be a vendor-specific attribute) that must be included in the RADIUS Accounting Stop request in order for the User Table entry to be deleted. The contents of the specified attribute are not examined.

The User Table identifies all users known to the CSG. The 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.

Examples

The following example shows how to enable the **radius stop purge** command for the CSG user-group U1:

```
ip csg user-group U1
 radius stop purge vsa 3gpp 11
```

radius userid

To specify the RADIUS attribute used to extract the user identifier from a RADIUS record, use the **radius userid** command in CSG user group configuration mode. To specify that no RADIUS attributes are to be used, use the **no** form of this command.

radius userid {**1** | **31** | **User-Name** | **Calling-Station-Id**}

no 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

No default behavior or values.

Command Modes

CSG user group configuration

Command History

Release	Modification
2.2(1)C(1)—12.1(11b)E3	This command was introduced.

Usage Guidelines

The **radius userid** command specifies that the CSG obtains the user ID from either attribute 1 or 31. If **no radius userid** is specified, user IDs are not obtained from RADIUS messages.

Examples

The following example shows how to specify RADIUS attribute User-Name for the CSG user-group G1:

```
ip csg user-group G1
 entries max 100000
 database 10.1.2.3 11111
 quota local-port 6666
 quota server 10.1.4.5 888 1
 quota server 10.1.6.7 999 2
 radius acct-port 7777
 radius key SECRET_PASSWORD
 radius parse strict
 radius server 10.13.14.15
 radius userid User-Name
 redirect nat 10.33.33.3
```

Related Commands

Command	Description
radius key	Specifies the CSG to be the RADIUS endpoint for account records.
radius acct-port	Configures the RADIUS listening port when it is different from the established RADIUS default of 1813.

records batch

To batch billing records into a single message before sending them to the Billing Mediation Agent (BMA), use the **records batch** command in CSG accounting configuration mode. To send billing records to the BMA as soon as they are created, use the **no** form of this command.

records batch

no records batch

Syntax Description

This command has no arguments or keywords.

Defaults

The default is **records batch**, which batches billing records into a single message.

Command Modes

CSG accounting configuration

Command History

Release	Modification
2.2(3)C2(1)—12.1(13)E	This command was introduced.

Usage Guidelines

The **records batch** command batches billing records into a single message. The message is sent when it is full, or when a short time has elapsed. Batching records reduces network overhead and increases the CSG performance.

Examples

The following example batches billing records for the CSG accounting service A1:

```
ip csg accounting A1
 user-group G1
 agent activate 2
 agent local-port 3775
 agent 10.1.2.4 11112 10
 agent 10.1.2.5 11113 20
 keepalive 3
 records batch
 records http-statistics
 records intermediate bytes 100000 time 3600
 records max 250
 inservice
```

Related Commands

Command	Description
ip csg accounting	Defines content-based client accounting as a service, and enters CSG accounting configuration mode.

records format

To specify variable, fixed, or variable single CDR format, use the **records format** command in CSG accounting configuration mode. To return to the default, use the **no** form of this command.

records format [**fixed | variable | variable-single-cdr**]

no records format

Syntax Description

fixed	Specifies fixed CDR format.
variable	Specifies variable CDR format.
variable-single-cdr	Specifies variable single CDR format.

Defaults

The default setting is **variable**.

Command Modes

CSG accounting configuration

Command History

Release	Modification
3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.
3.1(3)C5(5)—12.2(18)SXD	The **variable-single-cdr** keyword was added.

Usage Guidelines

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

Examples

The following example specifies fixed record format:

```
ip csg accounting
  records format fixed
```

Related Commands

Command	Description
hostname	Specifies a variable hostname for a CSG module
mode	Specifies that a billing plan is postpaid or prepaid.
owner name	Specifies the name of a service owner.
owner id	Specifies an identifier for a service owner.
class	Specifies a service class value.
ip csg transport-type	Classifies data traffic based on its access path.

records granularity

To specify the granularity at which billing records (CDRs) should be generated, use the **records granularity** command in CSG service configuration mode. To restore the default granularity, use the **no** form of this command.

records granularity {**transaction** | **service** {**bytes** *bytes* | **time** *seconds* | **bytes** *bytes* **time** *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. • For HTTP billing, the CSG counts TCP bytes. • For all other billing protocols, the CSG counts IP bytes. The difference between bytes sent and received in two records might not exactly equal the *bytes* argument, because updates must occur on packet boundaries. The range is from 5000 to 4294967295; however, we recommend an upper limit of 4000000. The default value, if the **bytes** keyword is not specified, is 0 bytes, indicating no maximum.
time *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 60 to 4294967295; however, we recommend an upper limit of 65535. The default value, if the **time** keyword is not specified, is 0 seconds, indicating 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 **time** keyword, or both:

- If you specify both the **bytes** keyword and the **time** keyword, a billing record is sent as soon as either limit is reached, and both limits are reset.
- If you specify only the **bytes** keyword and not the **time** keyword, the maximum time between billing records for a session is set to 0 seconds, indicating no time limit.
- If you specify only the **time** keyword and not the **bytes** keyword, the number of bytes of data that triggers the sending of a billing record is set to 0 bytes, indicating no maximum.

Command Modes

CSG service configuration

Command History

Release	Modification
3.1(3)C5(3)—12.2(18)SXD	This command was introduced.

Usage Guidelines

You can use this command to reduce the number of records for a service in which transaction level billing is not required.

For example, if a user is accessing the Internet, and the data is billed solely on the basis of volume, generating records for each HTTP transaction is of little use. With service-level CDR summarization enabled, the CSG generates only consolidated records containing service-level usage.

If you specify both **type http** and any other type (**type other**, **type ftp**, **type imap**, and so on) for a service, and you enable service-level CDR summarization for the service, the CSG's incremental and cumulative byte counts are not valid. This is because they are a mix of TCP bytes (for the HTTP traffic) and IP bytes (for all other traffic).

Service-level CDRs are generated only for subscribers with entries in the CSG User Table entry. If a subscriber does not have an entry in the User Table, the CSG 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 time 120
```

Related Commands

Command	Description
ip csg service	Defines a content billing service, and enters CSG service configuration mode.

records http-statistics

To send the HTTP Statistics data record to the Billing Mediation Agent (BMA), use the **records http-statistics** command in CSG accounting configuration mode. To not send the HTTP Statistics data record to the BMA unless the session fails (for example, if an RST without FIN is received, or if the session times out), use the **no** form of this command.

records http-statistics

no records http-statistics

Syntax Description

This command has no arguments or keywords.

Defaults

The default is **records http-statistics**, which causes the HTTP Statistics data record to be sent to the BMA whenever the session terminates.

Command Modes

CSG accounting configuration

Command History

Release	Modification
2.2(3)C2(1)—12.1(13)E	This command was introduced.

Examples

The following example sends the HTTP Statistics data record to the BMA for the CSG accounting service A1:

```
ip csg accounting A1
 user-group G1
 agent activate 2
 agent local-port 3775
 agent 10.1.2.4 11112 10
 agent 10.1.2.5 11113 20
 keepalive 3
 records batch
 records http-statistics
 records intermediate bytes 100000 time 3600
 records max 250
 inservice
```

records intermediate

To enable the generation of intermediate billing records, use the **records intermediate** command in CSG accounting configuration mode. To disable the generation of intermediate billing records, use the **no** form of this command.

records intermediate {**bytes** *bytes* | **time** *seconds* | **bytes** *bytes* **time** *seconds*}

no records intermediate {**bytes** *bytes* | **time** *seconds* | **bytes** *bytes* **time** *seconds*}

Syntax Description

bytes *bytes*	Number of bytes of data, sent and received by a session, that triggers the sending of an intermediate billing record: • For HTTP billing, the CSG counts TCP bytes. • For all other billing protocols, the CSG counts IP bytes. 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; however, we recommend an upper limit of 4000000. The default value, if the **bytes** keyword is not specified, is 0 bytes, indicating that the number of bytes sent and received will not trigger an intermediate record.
time *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 65535. The default value, if the **time** keyword is not specified, is 0 seconds, indicating no time limit.

Defaults

If you do not specify the **records intermediate** command, intermediate billing records are not generated.

If you specify the **bytes** keyword but not the **time** keyword, the maximum time between billing records for a session is set to 0 seconds, indicating no time limit.

If you specify the **time** keyword but not the **bytes** keyword, the number of bytes of data that triggers the sending of an intermediate billing record is set to 0 bytes, indicating no maximum.

If you specify both the **bytes** keyword and the **time** keyword, a billing record is sent as soon as either limit is reached, and both limits are reset.

Command Modes

CSG accounting configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.
3.1(1)C5(5)—12.2(18)SXD	This command was introduced.

Examples

The following example shows how to enable intermediate billing records for the CSG accounting plan A1. In this example, intermediate records are generated after 100,000 IP bytes of data are sent and received, or after 3600 seconds (1 hour), whichever comes first:

```
ip csg accounting A1
 user-group G1
 agent activate 2
 agent local-port 3775
 agent 10.1.2.4 11112 10
 agent 10.1.2.5 11113 20
 keepalive 3
 records batch
 records http-statistics
 records intermediate bytes 100000 time 3600
 records max 250
 inservice
```

Related Commands

Command	Description
ip csg accounting	Defines content-based client accounting as a service, and enters CSG accounting configuration mode.

records max

To define the maximum number of billing records that can be stored or queued in the CSG before they are forwarded to the Billing Mediation Agent (BMA), use the **records max** command in CSG accounting configuration mode. To revert to the default setting, use the **no** form of this command.

records max *number*

no records max *number*

Syntax Description

number	Defines the maximum number of billing records that can be stored or queued in the CSG before they are forwarded to the BMA. If the number of queued records exceeds the *number* argument, the CSG tries to forward the records to the Persistent Storage Device (PSD), if one is available. Otherwise, the CSG discards the billing records. The valid range is 1 to 65535 records. The default value is 10,000 records.

Defaults

The default value is 10,000 records.

Command Modes

CSG accounting configuration

Command History

Release	Modification
2.2(1)C(1)—12.1(11b)E3	This command was introduced.

Usage Guidelines

This command sets:

- The maximum number of BMA records among all BMAs
- The maximum number of quota server records among all quota servers
- The maximum number of Cisco Persistent Storage Device (PSD) records in the PSD

For example, if you set the **records max** command to 5000, the CSG can store or queue:

- Up to 5,000 total BMA records, shared among all BMAs
- Up to 5,000 total quota server records, shared among all quota servers
- Up to 5,000 total PSD records

If the value configured on the **records max** command is very high, the CSG might crash or be unable to communicate with IOS when its memory is exhausted. The following message might appear on the syslog:

%ICC-4-HEARTBEAT: Card 9 failed to respond to heartbeat

If you see this message, you need to reduce the maximum number of billing records that the CSG is allowed to buffer in memory. To do so, set **records max** to a smaller value, such as 10,000 (the default setting).

Examples

The following example shows how to specify that a maximum of 250 billing records can be can be queued in the CSG before they are forwarded to the BMA, for the CSG accounting service A1:

```
ip csg accounting A1
 user-group G1
 agent activate 2
 agent local-port 3775
 agent 10.1.2.4 11112 10
 agent 10.1.2.5 11113 20
 keepalive 3
 records batch
 records http-statistics
 records intermediate bytes 100000 time 3600
 records max 250
 inservice
```

Related Commands

Command	Description
agent (CSG accounting)	Defines the primary and backup BMAs to which to send billing records

record-storage

To define a Persistent Storage Device (PSD) to associate with this accounting group, use the **record-storage** command in CSG accounting configuration mode. To disable the record store, use the **no** form of the command.

record-storage *ip-address* [*port*]

no record-storage *ip-address* [*port*]

Syntax Description

ip-address	The destination address for packets going to the storage device.
port	(Optional) The source port to be used by the CSG when communicating with a record storage server other than the Persistent Storage Device/Call Data Record Backup (PSD/CDRB).

Defaults

No default behavior or values.

Command Modes

CSG accounting configuration

Command History

Release	Modification
3.1(3)C4(1)—12.2(14)ZA2	This command was introduced.

Usage Guidelines

The **record-storage** command sets the destination address for packets going to the storage device (PSD/CDRB). The PSD/CDRB only listens on port 3386. When the **record-storage** command omits the *port* parameter, the CSG defaults to port 3386. If a storage device is listening on another port, then you should specify that port in the **record-storage local-port** command.

Note Unless you are using a record-storage server other than the PSD, you need not specify the *port* parameter. Additionally, you must use the **record-storage local-port** command to specify the local port before you use the **record-storage** command to specify the IP address and port of the record-storage server.

Examples

The following example shows how to define a record store destination address of 172.18.12.226:

```
ip csg accounting D
  record-storage local-port 5002
  record-storage 172.18.12.226
```

Related Commands

Command	Description
record-storage local-port	Defines the source port to be used by the CSG when communicating with the record store.

record-storage local-port

To define the source port to be used by the CSG when communicating with the record store, use the **record-storage local-port** command in CSG accounting configuration mode. To disable the record store, use the **no** form of the command.

record-storage local-port *port*

no record-storage local-port *port*

Syntax Description

port	The source port to be used by the CSG when communicating with the record store.

Defaults

No default behavior or values.

Command Modes

CSG accounting configuration

Command History

Release	Modification
3.1(3)C4(1)—12.2(14)ZA2	This command was introduced.

Usage Guidelines

The local port is the source port from which the CSG sends packets to the record-storage server, and the port on which the CSG listens for responses.

Note The record-storage local port must not conflict with the quota server, nor with the agent local port.

Examples

The following example shows how to define a record store local port of 5002:

```
ip csg accounting D
  record-storage local-port 5002
  record-storage 172.18.12.226
```

Related Commands

Command	Description
record-storage	Defines a Persistent Storage Device (PSD) to associate with this accounting group.

redirect

To redirect client flows to an alternate IP address when the client's quota is exhausted, use the **redirect** command in CSG user group configuration mode. To remove the redirect, use the **no** form of this command.

redirect [**nat** *ip-address* [*port-number*]] [**wap** *url*] [**http** *url*]

no redirect [**nat** *ip-address* [*port-number*]] [**wap** *url*] [**http** *url*]

Syntax Description

nat	Redirects NAT client flows to an alternate IP address when quota is depleted.
wap	Redirects WAP client flows to a configured redirect URL when quota is depleted.
http	Redirects HTTP client flows to a configured redirect URL when quota is depleted, and configures the default URL for use in HTTP redirection.
ip-address	The IP address to which client flows are to be redirected.
port-number	(Optional) Port number to which client flows are to be redirected. The valid range is 1 to 65535. If you do not specify a port number, the port number in the user packet is not changed.
url	The URL to which client flows are redirected.

Defaults

No redirect IP address is defined.

If you do not specify a port number, the port number in the user packet is not changed.

Command Modes

CSG user group configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.
3.1(3)C4(1)—12.2(14)ZA2	The **wap** variable was added.
3.1(3)C5(1)—12.2(17d)SXB	The **http** variable was added.

Examples

The following example configures redirect NAT for the CSG user-group G1, with flows redirected to IP address 10.33.33.3:

```
ip csg user-group G1
 entries max 100000
 database 10.1.2.3 11111
 quota local-port 6666
 redirect wap http://172.18.12.219:80/redirect/topoff.wml/
 quota server 10.1.4.5 888 1
 quota server 10.1.6.7 999 2
 radius acct-port 7777
 radius key SECRET_PASSWORD
```

```
radius parse strict
radius server 10.13.14.15
radius userid User-Name
redirect nat 10.33.33.3
redirect http http://172.18.12.219:80/redirect/topoff.html/
```

refund-policy

To enable and specify the refunding policy for a CSG prepaid service, use the **refund-policy** command in CSG service configuration mode. To disable the refunding policy, use the **no** form of this command.

refund-policy *policy-name*

no refund-policy *policy-name*

Syntax Description

policy-name	Name of the refunding policy to be enabled.

Defaults

The default is for refunding to be disabled.

Command Modes

CSG service configuration

Command History

Release	Modification
3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.

Usage Guidelines

If refund is enabled for a CSG prepaid service, you cannot download more than 0x6FFFFFFF bytes of data in a given transaction.

Examples

The following example enables refund policy **COMPANY-REFUND**:

```
ip csg service BILLBYVOLUME
  basis byte tcp
  refund-policy COMPANY-REFUND
  content BILLBYVOLUME policy BILLBYVOLUME
```

Related Commands

Command	Description
ip csg service	Defines a content billing service, and enters CSG service configuration mode.

replicate connection tcp

To replicate the connection state for all TCP connections to the CSG content servers on the backup system, use the **replicate connection tcp** command in CSG content configuration mode. To disable connection redundancy, use the **no** form of this command.

replicate connection tcp

no replicate connection tcp

Syntax Description

This command has no arguments or keywords.

Defaults

Connection redundancy is not enabled.

Command Modes

CSG content configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

This command is required for stateful failover for replicated TCP connections.

For replication to occur, you must enable Cisco IOS Server Load Balancing (SLB) fault tolerance with the **ft group** command.

With the **replicate connection tcp** command configured, when a connection is established or terminated, the active CSG sends a dummy SYN or RST, respectively, to the fault-tolerant VLAN. This is normal operation. The extra packets are not billed and the destination MAC address is unknown, so the packets do not reach the server. The destination MAC address for the dummy SYN or RST frame is structured as follows:

0x03:*xx*:*yy*:00:*zz*:*zz*

where:

- **0x03:*xx*:*yy*** is the Cisco Organizational Unique Identifier (OUI).
- *zz* is the VLAN of the SYN that initiated the connection.

Examples

The following example shows how to enable TCP replication for the CSG content MOVIES_COMEDY:

```
ip csg content MOVIES_COMEDY
 client 10.4.4.0 255.255.255.0
 idle 120
 ip 172.18.45.0/24 tcp 8080
 policy POLICY1
 replicate connection tcp
 vlan MOVIES_COMEDY
 inservice
```

Related Commands

Command	Description
ip csg content	Defines content for the CSG accounting services, and enters CSG content configuration mode.

report http header

To define the inclusion of multiple HTTP request headers in the CSG HTTP_Header CDR, use the **report http header** command in CSG accounting configuration mode. To disable this configuration, use the **no** form of this command.

report http header *header_name*

no report http header *header_name*

Syntax Description

header_name	The name of the request header you want to include in the CSG HTTP_Header CDR. You can specify any number of headers; header names cannot exceed 224 characters.

Defaults

The default is to only copy the "host," "user-agent," and "from" HTTP headers into the CDRs. Any number of headers (up to 256) can be configured.

Command Modes

CSG accounting configuration

Command History

Release	Modification
3.1(3)C4(1)—12.2(14)ZA2	This command was introduced.

Examples

The following example shows how to enable reporting HTTP header information:

```
Router(config)# ip csg accounting name
Router(config-csg-accounting)# report http header x-subno
Router(config-csg-accounting)# report http header x-al-session-id
```

report radius attribute

To specify the RADIUS attributes to be copied from the RADIUS Start message into CDRs, use the **report radius attribute** command in CSG accounting configuration mode. To disable this feature, use the **no** form of this command.

report radius attribute *radius_attribute_number*

no report radius attribute *radius_attribute_number*

Syntax Description

radius_attribute_number	Specifies the RADIUS attribute number to be copied from the RADIUS Start message.

Defaults

The default setting is that no RADIUS attributes are reported.

Command Modes

CSG accounting configuration

Command History

Release	Modification
2.2(1)C(4)—12.1(11b)E3	This command was introduced.
3.1(3)C4(1)—12.2(14)ZB2	This command was moved to the CSG accounting configuration mode

Usage Guidelines

You can specify as many attributes as you want.

If the attribute is not present in the RADIUS message, the attribute is not present in the CDRs, unless **records format fixed** is configured. If the list of configured attributes changes, only new RADIUS requests are subject to the new attributes. Attributes already saved continue to be reported.

When a RADIUS Start request is received, any attributes received from a previous Start request are deleted.

If there are multiple instances of an attribute, they are all reported.

Attributes are reported in the order they exist in the RADIUS message.

Examples

The following example shows how to enable the **report radius attribute** command:

```
ip csg accounting A1
  report radius attribute 3
  report radius attribute 5
  report radius attribute 7
  report radius attribute 44
```

Related Commands

Command	Description
ip csg accounting	Defines content-based client accounting as a service, and to enter CSG accounting configuration mode.

report usage

To enable supplemental usage reporting, use the **report usage** command in CSG accounting configuration mode. To disable supplemental usage reporting, use the **no** form of this command.

report usage {**bytes ip** | **seconds**}

no 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

No default behavior or values.

Command Modes

CSG accounting configuration

Command History

Release	Modification
3.1(3)C6(2)—12.2(18d)SXE	This command was introduced.

Usage Guidelines

Interval report TLVs are generated for SvcReauthorizationRequest, ServiceStop, and QuotaReturn messages. Reports contain statistics since the last report.

If you want to report both IP bytes and usage in seconds, you can specify both **report usage bytes ip** and **report usage seconds**.

Examples

The following example shows how to enable supplemental usage reporting for both IP bytes and seconds:

```
ip csg accounting NAME
  report usage bytes ip
  report usage seconds
```

retcode

To specify the range of application return codes for which the CSG refunds quota, use the **retcode** command in CSG refund configuration mode. Use the **no** form of this command to disable this feature.

retcode {**ftp** | **http** | **imap** | **pop3** | **smtp** | **wap**} *rc-start* [*rc-end*]

no retcode {**ftp** | **http** | **imap** | **pop3** | **smtp** | **wap**} *rc-start* [*rc-end*]

Syntax Description

ftp	The CSG refunds quota for File Transfer Protocol (FTP) application return codes.
http	The CSG refunds quota for Hypertext Transfer Protocol (HTTP) and Wireless Application Protocol (WAP) 2.x application return codes. **Note** The **http** keyword affects only HTTP and WAP 2.x. For WAP 1.x refunds, use the **wap** keyword.
imap	The CSG refunds quota for Internet Message Access Protocol (IMAP) application return codes.
pop3	The CSG refunds quota for Post Office Protocol, version 3 (POP3) application return codes.
smtp	The CSG refunds quota for Simple Mail Transfer Protocol (SMTP) application return codes.
wap	The CSG refunds quota for Wireless Application Protocol (WAP) 1.x application return codes. **Note** The **wap** keyword affects only WAP 1.x. For WAP 2.x refunds, use the **http** keyword.
rc-start	Specifies the beginning of the range of values for specific application return codes. Valid values are 1 to 65535 (0xffff).
rc-end	(Optional) Specifies the end of the range of values for specific application return codes. Valid values are the value of *rc-start* to 65535 (0xffff). If you are specifying a single value as the range, do not specify *rc-end*.

Defaults

No default behavior or values.

Command Modes

CSG refund configuration

Command History

Release	Modification
3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.
3.1(1)C6(2)—12.2(18)SXE	The **imap** keyword was added.

Usage Guidelines

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 CSG does not support refunding for IMAP. If configured, refunding for IMAP has no effect.

Examples

The following example shows how to enable the **retcode** command:

```
ip csg refund COMPANY-REFUND
  retcode http 500 509
  retcode wap 0x44 0x50
  retcode ftp 454
```

Related Commands

Command	Description
flags	Specifies IP, TCP, or WAP flag bit masks and values for which the CSG refunds quota.
ip csg refund	Specifies the refund policy that can then be applied to the various services, and enters CSG refund configuration mode.

route (module CSG VLAN)

To configure networks that are not Layer 2-adjacent to the CSG, use the **route** command in module CSG VLAN configuration mode. To remove the subnet or gateway IP address from the configuration, use the **no** form of this command.

route *ip-address netmask* **gateway** *gw-ip-address*

no route *ip-address netmask* **gateway** *gw-ip-address*

Syntax Description

ip-address	Subnet IP address.
netmask	Network mask.
gateway	Keyword to specify that the gateway is configured.
gw-ip-address	Gateway IP address.

Defaults

No default behavior or values.

Command Modes

Module CSG VLAN configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

Specify the Layer 3 network's subnet address and the gateway IP address to reach the next-hop router. The gateway address must be in the same network as specified in the **ip address** VLAN command.

You can specify up to 4095 **route** commands for each VLAN.

If you are adding a new route to an existing gateway, the new route might not take effect until you remove the gateway and reconfigure it to clear the gateway cached entries.

To support RADIUS endpoint, the CSG requires a route to 255.255.255.255. You can configure the route by using the **gateway (module CSG VLAN)** command or the **route (module CSG VLAN)** command. For example:

gateway 31.0.0.6

or:

route 255.255.255.255 255.255.255.255 gateway 31.0.0.6

Note If you already have a gateway configured, you do not need to configure an additional gateway for the RADIUS endpoint.

Examples

The following example shows how to configure a network to the CSG:

```
vlan 301 client
 name TO-GGSN-MS-APN
 gateway 31.0.0.10
 ip address 31.0.0.21 255.255.255.0
 route 11.0.0.0 255.255.0.0 gateway 31.0.0.1
 route 11.1.0.0 255.255.0.0 gateway 31.0.0.2
 route 11.2.0.0 255.255.0.0 gateway 31.0.0.3
 route 11.3.0.0 255.255.0.0 gateway 31.0.0.4
 alias 31.0.0.51 255.255.255.0
```

Related Commands

Command	Description
ip address (module CSG VLAN)	Assigns an IP address to the CSG VLAN.
show module csg variable	Displays the list of VLANs.
vlan (module CSG)	Creates a client or server VLAN that defines the Layer 2 paths for the CSG accounting service flows, assigns a VLAN ID and optional name, and enters module CSG VLAN configuration mode.

ruleset

To download all content defined by a ruleset to a CSG card, use the **ruleset** command in module CSG configuration mode. To delete the downloaded content, use the **no** form of this command.

ruleset *ruleset-name*

no ruleset *ruleset-name*

Syntax Description

ruleset-name	Name of a configured CSG billing ruleset.

Defaults

No default behavior or values.

Command Modes

Module CSG configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

Configuration commands are sent to the CSG card to provision each content referenced in the ruleset.

Examples

The following example shows how to download the CSG ruleset R1 to the CSG card in slot 4:

```
module csg 4
 accounting A1
 ft group 123 vlan 5
 ruleset R1
 vlan 30 client
 vlan 32 client
 vlan 40 server
```

Related Commands

Command	Description
module csg	Enters module CSG configuration mode for a specified slot.

service

To associate a service with a CSG billing plan, use the **service** command in CSG 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 CSG billing service.

Defaults

No default behavior or values.

Command Modes

CSG billing configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

You can associate more than one service with the same billing plan by using multiple **service** commands.

Examples

The following example shows how to associate a service with a billing plan:

```
ip csg billing REGULAR
 service MOVIES
 service BROWSING
```

Related Commands

Command	Description
ip csg billing	Defines a billing plan to be used for prepaid billing.

show ip csg accounting

To monitor and display configuration, operation, and statistical information for the CSG billing feature, use the **show ip csg accounting** command in privileged EXEC mode.

show ip csg accounting {**agent | database | error | quota-server | radius | users** {**all | statistics |** *ip-address* [*ip-mask*] **| userid** *userid*}} [**detail**] [**module** *num*] [**psd module** *slot*]

Syntax Description

agent	Displays information about the Billing Mediation Agent (BMA) to which to send billing records.
database	Displays information about the server that answers user ID queries.
error	Displays error messages.
quota-server	Displays information about the quota server.
radius	Displays information related to RADIUS.
users	Displays information from the User Table.
all	Displays information for all users.
statistics	Displays performance statistics.
ip-address	Displays information for the specified user IP address.
ip-mask	Displays information for the specified user IP address mask.
userid *userid*	Displays information for the specified user ID.
detail	Lists detailed statistics for each BMA, followed by a summary of statistics for all BMAs.
module *num*	Displays information for the specified CSG module.
psd module *slot*	Displays information pertaining to Persistent Storage Device (PSD) functionality residing on the CSG.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
2.2(1)C(1)—12.1(11b)E3	This command was introduced.
2.2(3)C2(1)—12.1(13)E	This command was modified to support multiple BMAs.
3.1(1)C3(1)—12.2(14)ZA	The **quota-server** keyword was added.
3.1(3)C5(1)—12.2(17d)SXB	Added new output for RADIUS in the **users detail** variable.

Usage Guidelines

BMA statistics are kept for each BMA, as well as an aggregate count for all BMAs.

Note Invoking the **show ip csg accounting users all** command might flood your screen with output.

Examples

The following example shows how to display information about the quota server:

```
Router# show ip csg accounting quota-server

---------------------- CSG in slot 4 ----------------------
charging gateway      priority state
-----------------------------------------
10.10.99.1:6923              2 NAWAIT
```

The following example displays the RADIUS attributes being sent to the BMA and quota server, including a short description of the fields.

Note A good understanding of RADIUS protocol is needed to decode these RADIUS values.

The length of the RADIUS VSA is not included in the output; this command shows the value field. In the case of VSA (26), the first four octets are the Vendor ID code.

```
Router# show ip csg accounting users all detail

---------------------- CSG in slot 4 ----------------------
192.168.215.15  31608920094
  bma = 192.168.200.22:3338
  qs = 192.168.221.97:3338, nas = 192.168.210.170, flags = 0x01, sessions = 0
  billing = PREPAID, plan = PLAN1
  004:c0a8d2aa                 - NAS IP Address (192.168.210.170)
  030:41504e31                 - Called Station ID (APN1)
  007:00000007                 - Framed Protocol (GPRS PDP Context)
  008:c0a8d70f                 - Framed IP Address (192.168.215.15)
  026:000028af0111313038303133303038393230303934 (3GPP VSA 10415, IMSI 108013008920094)
  031:3331363038393230303934   - Calling Station ID (31608920094)
```

show module csg accounting

To monitor and display configuration, operation, and statistical information for the CSG billing feature, use the **show module csg accounting** command in privileged EXEC mode.

show module csg *slot* **accounting** {**agent | database | error | quota-server | radius | users** {**all | statistics |** *ip-address* [*ip-mask*] **| userid** *userid*}} [**detail**]

Syntax Description

slot	Slot where the CSG resides.
agent	Displays information about the Billing Mediation Agent (BMA) to which to send billing records.
database	Displays information about the server that answers user ID queries.
error	Displays error messages.
quota-server	Displays information about the quota server.
radius	Displays information related to RADIUS.
users	Displays information from the User Table.
all	Displays information for all users.
statistics	Displays performance statistics.
ip-address	Displays information for the specified user IP address.
ip-mask	Displays information for the specified user IP address mask.
userid *userid*	Displays information for the specified user ID.
detail	Lists detailed statistics for each BMA, followed by a summary of statistics for all BMAs.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.
3.1(3)C5(1)—12.2(17d)SXB	Output for the **detail** argument was modified.
3.1(3)C6(2)—12.2(18)SXE	Output was modified to support the tariff switch feature.

Usage Guidelines

BMA statistics are kept for each BMA, as well as an aggregate count for all BMAs.

Note Invoking the **show module csg accounting users all** command might flood your screen with output.

Examples

The following example shows how to display detailed information about all accounting users on CSG 3:

```
c6k-csg# show module csg 3 accounting users all detail
10.10.10.2      USER_1
  table name = None
  bma = 0.0.0.0:0, qs = 10.10.20.2:5000
  nexthop dl ip = 0.0.0.0, nas = 10.10.10.10, flags = 0x00000011, sessions = 0
  billing = PREPAID, plan = BILLBYTES, handoff timer OFF
  service = SERVICEBYTES, basis = IP bytes, verify = Disabled
   balance = 96607, consumed = 3393
   reserved = 0, pending = 0, trigger = 32768
   current time    = TUE MAR 22 18:22:00 2005
   quota expiry    = TUE MAR 22 18:25:57 2005
   idle  expiry    = TUE MAR 22 18:26:57 2005
   earliest reauth = TUE MAR 22 18:22:00 2005
   service id = 0x4240624800000000, transactions = 0, flags = 0x0020
   interval bytes up = 125
   interval bytes down = 3268
   interval seconds = 1
   interval first billable = TUE MAR 22 18:21:57 2005
   interval last billable = TUE MAR 22 18:21:57 2005
  Report attributes:
   008:0a0a0a02
   040:00000001
   044:303031
   004:0a0a0a0a
   001:555345525f31
```

Table B-3 describes the fields shown in the display.

Table B-3 show module csg accounting users all detail Field Descriptions

Field	Description
table name	Table name of the VLAN.
bma	IP address of the BMA.
qs	IP address of the quota server.
nexthop dl ip	IP address of the next-hop downlink.
nas	IP address of the Network Access Server (NAS).
flags	Internal CSG field.
sessions	Total number of sessions.
billing	Type of billing plan: • If the billing plan is prepaid, this field is set to PREPAID. • If the billing plan is postpaid, or if it has a length of zero, this field is set to POSTPAID. • If the CSG cannot determine whether the billing plan is prepaid or postpaid, this field is set to UNKNOWN.
plan	Specific billing plan, or (none) if the billing plan is zero-length or is not known to the CSG.
handoff timer	Indicates whether the RADIUS handoff timer is on or off.
service	Name of the service.

Table B-3 show module csg accounting users all detail Field Descriptions (continued)

basis	Billing basis for the service. Possible values are: • IP bytes—Billing charge is a function of the IP data volume processed during the user's session. • TCP bytes—Billing charge is a function of the TCP data volume processed during the user's session. • Fixed—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—Billing charge is duration-based for the CSG service. • Second connect—Billing charge is based on connection duration time, not service duration time.
verify	Indicates whether service verification is enabled or disabled.
balance	Amount of quota remaining. **Note** If the **basis second connect** command is configured, the **balance** field is updated only when there is a service reauthorization request for new quota.
consumed	Amount of quota used. **Note** If the **basis second connect** command is configured, the **consumed** field is updated only when there is a service reauthorization request for new quota.
reserved	Amount of quota reserved for ongoing transactions.
pending	Amount of quota that has been consumed but is not yet been charged against **consumed** or **balance**. Quota is typically in **pending** state to prevent charging until refund conditions are evaluated at the end of the transaction.
trigger	Threshold for quota reauthorization.
current time	Current timestamp.
quota expiry	Timestamp for the quota to expire.
idle expiry	Timestamp for the idle timer to expire.
earliest reauth	Timestamp for the earliest service reauthorization request for the service.
service id	Identifier for the service.
transactions	Number of open transactions mapped to the service.
flags	Internal CSG field.
tariff_switch time	Timestamp of the tariff switch.
t/sw consumed	Amount of consumed quota at the time of the tariff switch.
t/sw interval bytes up	Number of tariff switch interval usage bytes uploaded since last report.
t/sw interval bytes down	Number of tariff switch interval usage bytes downloaded since last report.
t/sw interval seconds	Number of tariff switch interval usage seconds since last update.
t/sw interval first billable	Timestamp of the first billable session time for this tariff switch report interval.
t/sw interval last billable	Timestamp of the last billable session time for this tariff switch report interval.
interval bytes up	Number of interval usage bytes uploaded since last report.
interval bytes down	Number of interval usage bytes downloaded since last report.
interval seconds	Number of interval usage seconds since last update.

Table B-3 show module csg accounting users all detail Field Descriptions (continued)

interval first billable	Timestamp of the first billable session time for this report interval.
interval last billable	Timestamp of the last billable session time for this report interval.
Report attributes	Values of any RADIUS attributes associated with the user. For example, **008:0a0a0a02** indicates that RADIUS attribute **8** is associated with the user, with a value of **0a0a0a02**.

The following example shows how to display performance statistics for accounting users on CSG 4:

```
c6k-csg# show module csg 4 accounting users statistics
Module  Max Entries  Highwater  Current   Overflow
------  -----------  ---------  --------  --------
4       250000       215282     212452    5778149
```

Table B-4 describes the fields shown in the display.

Table B-4 show module csg accounting users statistics Field Descriptions

Field	Description
Module	CSG module number.
Max Entries	Maximum number of entries allowed in the User Table, as configured with the **entries max** command in CSG user group configuration mode.
Highwater	Largest number of entries in the User Table since bootup.
Current	Current number of entries in the User Table.
Overflow	Number of entries reallocated for a new user because the User Table was full or no more storage was available.

show module csg arp

To display the CSG Address Resolution Protocol (ARP) cache, use the **show module csg** *slot* **arp** command in privileged EXEC mode.

show module csg *slot* **arp**

Syntax Description

slot	Slot where the CSG resides.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Examples

The following example shows how to display the CSG ARP cache:

```
Router# show module csg 4 arp

Internet Address  Physical Interface  VLAN      Type       Status
------------------------------------------------------------------
 10.10.99.244     00-01-64-F9-1A-45   99        LEARNED    up(0 misses)
 10.10.99.250     00-02-7E-39-2B-13   99        LEARNED    up(0 misses)
 20.20.20.10      00-90-BF-99-B8-1C   820       LEARNED    up(0 misses)
 20.20.20.103     00-02-7E-39-25-98   820       --SLB--    local
 20.20.30.103     00-02-7E-39-25-98   830       --SLB--    local
 20.20.20.240     00-00-00-00-00-00   820       ROUTER     down(4 misses)
 20.20.30.250     00-00-00-00-00-00   830       ROUTER     down(4 misses)
 10.10.99.1       08-00-20-B6-3E-7B   99        LEARNED    up(0 misses)
 10.10.99.3       08-00-20-B6-27-7E   99        LEARNED    up(0 misses)
 10.10.99.40      00-07-EC-CC-54-8A   99        LEARNED    up(0 misses)
 10.10.99.41      00-02-7E-39-2B-14   99        LEARNED    up(0 misses)
 10.10.99.52      00-02-FC-BD-70-0A   99        LEARNED    up(0 misses)
 10.10.99.55      00-E0-34-B7-20-65   99        LEARNED    up(0 misses)
 10.10.99.62      00-09-43-51-26-0A   99        LEARNED    up(0 misses)
 10.10.99.67      00-02-FC-E0-80-4A   99        LEARNED    up(0 misses)
 10.10.99.103     00-02-7E-39-25-98   99        --SLB--    local
```

show module csg billing

To display statistics and counters for CSG billing, use the **show module csg** *slot* **billing** command in privileged EXEC mode.

show module csg *slot* **billing** {**all** | **plan** *billing-plan-name*}

Syntax Description

slot	Slot where the CSG resides.
all	Displays statistics for all CSG billing plans.
plan *billing-plan-name*	Displays statistics for only the specified CSG billing plan.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Examples

The following example shows how to display the statistics and counters for all CSG billing plans:

```
C6K-csg# show module csg 3 billing all
CSG billing plan PLAN_A
    service = OFF_NET, basis = seconds (svc), idle = 300
      initial = 0, increment = 0, minimum= 60, exclude-svc-idle = 0
      rule = (TELNET, VANILLA), weight = 1
      rule = (BROWSE, ANYHTTP), weight = 1
```

Related Commands

Command	Description
ip csg billing	Defines a billing plan to be used for prepaid billing, and enters CSG billing configuration mode.

show module csg clock

To display time information for the CSG, use the **show module csg** *slot* **clock** command in privileged EXEC mode.

show module csg *slot* **clock**

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
3.1(3)C5(5)—12.2(18)SXD	This command was introduced.

Usage Guidelines

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

Examples

The following example shows how to display time information for the CSG:

```
C6K-csg# show module csg 1 clock
seconds = 1123757186, base = 1122382560, uptime = 1374626
adjusted time = THU AUG 11 10:46:45 2005 UTC
last sync time = THU AUG 11 10:46:11 2005 UTC
```

Table B-5 describes the fields shown in the display.

Table B-5 show module csg clock Field Descriptions

Field	Description
seconds	Seconds since January 1, 1970.
base	Internal, unadjusted number of seconds since January 1, 1970.
uptime	Seconds since the CSG was last booted.
adjusted time	Current date and time. The adjusted time is used as the time stamp TLV for CDRs.
last sync time	Date and time of last synchronization update from the Supervisor Engine.

show module csg conns

To display active connections, use the **show module csg** *slot* **conns** command in privileged EXEC mode.

show module csg *slot* **conns** [**vserver** *virtserver-name*] [**client** *ip-address*] [**detail**]

Syntax Description

slot	Slot where the CSG resides.
vserver	(Optional) Keyword to specify the connections associated with a particular virtual server.
virtserver-name	(Optional) Name of the virtual server to be monitored.
client	(Optional) Keyword to specify the connections associated with a particular client IP address.
ip-address	(Optional) IP address of the client to be monitored.
detail	(Optional) Keyword to specify detailed connection information.

Defaults

If no options are specified, the command displays output for all active connections.

Command Modes

Privileged EXEC

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

Entering this command might result in a sudden increase in CSG CPU utilization (that is, the percent of the CSG CPU that is in use).

Examples

The following example shows how to display active connection data:

```
Router# show module csg 4 conns
    prot vlan source               destination          state
------------------------------------------------------------------------
In  TCP  11   100.100.100.2:1754    10.10.3.100:80       ESTAB
Out TCP  12   100.100.100.2:1754    10.10.3.20:80        ESTAB

In  TCP  11   100.100.100.2:1755    10.10.3.100:80       ESTAB
Out TCP  12   100.100.100.2:1755    10.10.3.10:80        ESTAB

Router# show module csg 4 conns detail
    prot vlan source               destination          state
------------------------------------------------------------------------
In  TCP  11   100.100.100.2:1754    10.10.3.100:80       ESTAB
Out TCP  12   100.100.100.2:1754    10.10.3.20:80        ESTAB
    vs = WEB_VIP, ftp = No, csrp = False
```

```
In  TCP  11   100.100.100.2:1755    10.10.3.100:80        ESTAB
Out TCP  12   100.100.100.2:1755    10.10.3.10:80         ESTAB
    vs = WEB_VIP, ftp = No, csrp = False
```

show module csg content

To display statistics and counters for the CSG content, use the **show module csg** *slot* **content** command in privileged EXEC mode.

show module csg *slot* **content** [**name** *content-name*] [**detail**]

Syntax Description

slot	Slot where the CSG resides.
name *content-name*	(Optional) Name of a configured content.
detail	(Optional) Keyword to display more detailed information.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Examples

The following example shows how to display the statistics and counters for the CSG content:

```
Router# show module csg 4 content
content         prot destination              vlan state        conns
------------------------------------------------------------------
HTTP            TCP  20.20.0.0/16:80          ALL  OPERATIONAL  0
OTHER           any  20.20.0.0/16             ALL  OPERATIONAL  0
```

Table B-6 describes the fields shown in the display.

Table B-6 show module csg content Field Descriptions

Field	Description
content	Name of the configured CSG billing content.
prot	Protocol type of Layer 3/Layer 4 flows that can be processed by the content: • **any**—Flows of any protocol type can be processed. • **tcp**—Only TCP flows can be processed. • **udp**—Only UDP flows can be processed. • *protocol-number*—Number identifying the protocol whose flows can be processed. The valid range is 0 to 255, where 0 means the same as **any**.
destination	The destination address for packets going to the content.
vlan	Name of the source VLAN for the content, or ALL if the content is not restricted to a single VLAN.

Table B-6 show module csg content Field Descriptions (continued)

state	Current state of the content.
conns	Number of connections currently using the content.

The following example shows how to display detailed statistics and counters for the CSG HTTP content named **HTTP-MS**:

```
Router# show module csg 4 content name HTTP-MS detail
HTTP-MS, state = OPERATIONAL, index = 11
  destination = 0.0.0.0/0:80, TCP
  idle = 10, replicate = connection, vlan = ALL, pending = 30
  max parse len = 4000, persist rebalance = TRUE
  conns = 2, total conns = 3
  policy          total conn   client pkts  server pkts
  ------------------------------------------------------
  HTTP-MS-AHTML   0            0            0
  HTTP-MS-BJPG    1            3            1
  HTTP-FREE       0            0            0
  HTTP-DOUBLE     0            0            0
  HTTP-MS         10           71           59
  (default)       0            0            0
```

Note For HTTP accounting, the “client pkts” and “server pkts” columns might show incorrect values. Therefore, ignore the values in the “client pkts” and “server pkts” columns.

Related Commands

Command	Description
ip csg content	Defines content for the CSG accounting services, and enters CSG content configuration mode.

show module csg ft

To display statistics and counters for the CSG fault-tolerant pair, use the **show module csg** *slot* **ft** command in privileged EXEC mode.

show module csg *slot* **ft** [**detail**]

Syntax Description

slot	Slot where the CSG resides.
detail	(Optional) Keyword to display more detailed information.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Examples

The following example shows how to display the statistics and counters for the CSG fault-tolerant pair:

```
Router# show module csg 4 ft
FT group 2, vlan 30
 This box is active
 priority 10, heartbeat 1, failover 3, preemption is off
```

Related Commands

Command	Description
ft group (module CSG)	Enters fault-tolerant configuration mode and configures fault tolerance.

show module csg stats

To display statistics, use the **show module csg** *slot* **stats** command in privileged EXEC mode.

show module csg *slot* **stats**

Syntax Description

slot	Slot where the CSG resides.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Examples

The following example shows how to display the CSG statistics:

```
Router# show module csg 4 stats

Connections Created:        0
Connections Destroyed:      0
Connections Current:        0
Connections Timed-Out:      0
Connections Failed:         0
Server initiated Connections:
      Created: 25, Current: 0, Failed: 24
L4 Load-Balanced Decisions: 0
L4 Rejected Connections:    25
L7 Load-Balanced Decisions: 0
L7 Rejected Connections:
      Total: 0, Parser: 0,
      Reached max parse len: 0, Cookie out of mem: 0,
      Cfg version mismatch: 0, Bad SSL2 format: 0
L4/L7 Rejected Connections:
      No policy: 0, No policy match 0,
      No real: 0, ACL denied 0,
      Server initiated: 25
Checksum Failures: IP: 0, TCP: 0
Redirect Connections: 0, Redirect Dropped: 0
FTP Connections:            0
MAC Frames:
      Tx: Unicast: 15103, Multicast: 4, Broadcast: 25808,
          Underflow Errors: 0
      Rx: Unicast: 7618, Multicast: 2548994, Broadcast: 44518,
          Overflow Errors: 0, CRC Errors: 0
```

show module csg status

To display whether the CSG is online and, if so, the CSG chassis slot location and whether the configuration download is complete, use the **show module csg** *slot* **status** command in privileged EXEC mode.

show module csg *slot* **status**

Syntax Description

slot	Slot where the CSG resides.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

If the CSG is online, this command shows the CSG chassis slot location and indicates whether the configuration download is complete.

Examples

The following example shows how to display the CSG status:

```
Router# show module csg 4 status
SLB Module is online in slot 4.
Configuration Download state:COMPLETE, SUCCESS
```

show module csg tech-support

To display technical support information for the CSG, use the **show module csg** *slot* **tech-support** command in privileged EXEC mode.

show module csg *slot* **tech-support** [**all** | **core-dump** | **csg** | **fpga** | **ft** | **processor** *number* | **slowpath** | **utilization**]

Syntax Description

slot	Slot where the CSG resides.
all	(Optional) Keyword to display all of the available statistics.
core-dump	(Optional) Keyword to display all of the most recent statistics for the process that experienced a core dump.
csg	(Optional) Keyword to display all of the CSG statistics.
fpga	(Optional) Keyword to display all of the FPGA statistics.
ft	(Optional) Keyword to display all of the statistics related to fault tolerance.
processor *number*	(Optional) Keyword to display the statistics for the specified processor.
slowpath	(Optional) Keyword to display all of the slowpath statistics.
utilization	(Optional) Keyword to display all of the utilization statistics (total memory usage).

Defaults

If no options are specified, the command displays all information.

Command Modes

Privileged EXEC

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.
3.1(3)C5(5)—12.2(18)SXD	Added support for IMAP and RADIUS Packet of Disconnect (PoD) statistics.

Examples

The following example shows how to display utilization statistics for the CSG:

```
Router# show module csg 4 tech-support utilization
Resource Utilization:
  Memory
    Available Memory     62%     156M
    Allocated Memory     30%      76M
    OS Static Memory      8%      22M
```

Note If **Available Memory** is near zero, there might be a buffer leak.

The following example shows how to display buffer pool statistics for the CSG:

```
Router# show module csg 4 tech-support csg
CSG KUT Stats:
  max = 25000, current = 0, highwater = 0, LRU-steals = 0
  requests = 0, responses = 0, resends = 0, timeouts = 0

CSG Radius Stats:
  starts = 0, stops = 0, other = 0
  client messages received = 0, client messages sent = 0
  max proxy clients exceeded = 0

CSG LogGen Stats:
  session: dups= 0, create err= 0, seq err= 0 (persist 0)
  no session= 0, bad ixp msg= 0
  alloc fail= 0, alloc interm fail= 0
  billing records= 0, no reserve= 0
  msg rcv err= 0, msg send err= 0
  csg_billing_url_rcv= 0, csg_billing_stat_rcv= 0
  csg_billing_ft_notify_rcv= 0, csg_billing_retcode_rcv= 0
  null buffer addr= 0, invalid vsid= 0
  dup url= 0, wap_url_no_sess= 0, wap_url_no_app= 0
  wap url req= 0, wap url resp= 0, wap url frag resp= 0
  nokut duplicate= 0 negative avail= 0 sess delete err= 0
  up-range= 0, down-range= 0
  gtp-rej-error= 0

CSG record storage stats:
  Writes:        = 0,  Write Errors:  = 0
  Reads:         = 0,  Read Errors:   = 0
  Reads Pending: = 0,  Alloc Errors:  = 0

CSG QM Stats:
  Errors: Alloc Error = 0, Too Many Requests = 0
  Badly formatted message = 0, No Active QS: 0

GTP Application: CSG Billing Agent, Local Port: 3386, TID: b3025f0
  alloc failures = 0, no standby on CG failure = 0
  packets sent = 0, received = 3, failed acks = 0
  packets dropped = 0, rejected = 0, retransmissions = 0
  packets outstanding: current = 0, highwater = 1
  bad records = 0, unknown CG = 0, CG failures = 0
  Charging Gateways: defined = 1, max active = 1
    10.10.99.1:2369             2       ACTIVE

GTP Application: CSG Quota Manager, Local Port: 0, TID: 0
  alloc failures = 0, no standby on CG failure = 0
  packets sent = 0, received = 0, failed acks = 0
  packets dropped = 0, rejected = 0, retransmissions = 0
  packets outstanding: current = 0, highwater = 0
  bad records = 0, unknown CG = 0, CG failures = 0
  Charging Gateways: defined = 0, max active = 1

GTP Application: CSG record storage, Local Port: 0, TID: 0
  alloc failures = 0, no standby on CG failure = 0
  packets sent = 0, received = 0, failed acks = 0
  packets dropped = 0, rejected = 0, retransmissions = 0
  packets outstanding: current = 0, highwater = 0
  bad records = 0, unknown CG = 0, CG failures = 0
  Charging Gateways: defined = 0, max active = 1

CSG HTTP Stats:
  packets= 0, requests= 0, parse failures= 0
  alloc failures= 0, redirects= 0
```

```
CSG FTP Stats:
  vserver: add = 0/0, remove = 0/0, lookup errors = 0
  ftp details: alloc = 0/0, no details = 0
  session lookup errors = 0, dropped data conns = 0
  killed data conns = 0

CSG WAP Stats:
  parses= 0, wap sessions= 0, mms sessions= 0
  connection oriented packets= 0, connectionless packets= 0
  curr trans= 0, total trans= 0, incomplete trans= 0
  billing reports= 0, dup packets= 0, redirects= 0
  disconnects= 0, unknown packets= 0, concat packets= 0
  parse err= 0, alloc fail= 0, drops= 0, refunds= 0
  forced aborts= 0 concat frags= 0 aoc reqs= 0

CSG Mail Stats:
  SMTP messages          = 0
  SMTP packets           = 0
  MAIL retransmits       = 0
  MAIL tcp gaps          = 0
  MAIL ip frags          = 0
  MAIL aoc bypass        = 0
  MAIL alloc fails       = 0
  POP3 messages          = 0
  POP3 packets           = 0
  IMAP header retrievals = 0
  IMAP body retrievals   = 0
  IMAP packets           = 0

CSG RTSP Stats:
  Conns: add = 0, fail = 0, cleanups = 0
  Allocs: sessions = 0, ctl_conns = 0, streams = 0,
  secondary = 0
  Timeouts: sessions = 0, ctl_conns = 0, streams = 0
  Misc: reuse = 0, reuse term = 0, teardowns = 0,
  suspends = 0, patches = 0, interleaved = 0,
  http = 0, no_policy = 0
  Errors: alloc = 0, dups = 0, session = 0,
  patch = 0, rejects = 0

CSG Fragment Stats:
  creates= 0, destroys= 0, timeouts= 0, invalids= 0
  leaders= 0, trailers= 0, drops= 0, unknown= 0
  alloc failures= 0

pkt_drive_bill_drop stats:
  kut_prepaid_nokut = 0, kut_prepaid = 0
  session = 0, session_kill = 0
  brec_url_msg_1 = 0, brec_url_msg_2 = 0, brec_stat_prepaid = 0
  brec_stat_msg_1 = 0, brec_stat_msg_2 = 0, brec_wap_url_msg = 0
  pkt_drive_drain = 0, pkt_drive_redir = 0
  mail_1 = 0, mail_2 = 0, mail_3 = 0
  mail_session_close = 0
  frag_1 = 0, frag_2 = 0, frag_3 = 0, frag_4 = 0
  http_resolved = 0

pkt_drive_bill_queue stats:
  bill_q_ndx_in        =0, bill_q_ndx_out =0
  csg_q_elem_hiwater   =0, csg_q_elem_count       =0
  send_threshold       =520, BILL_MAX_SEND_QUEUE  =65536
  csg_relinquish       =0, csg_relinquish_cnt     =2
  pkt_drops_q_full     =0
```

```
CSG Clock Stats:
  seconds = 1130322752, base = 1130322529, uptime = 223
  adjusted time = WED OCT 26 10:32:32 2005 UTC
  last sync time = WED OCT 26 10:28:49 2005 UTC

Timer Wheel Stats:
  ticks = 228, starts = 126, stops = 4, timeouts = 119, longest = 2

Tracebacks:
None recorded.

Buffer pools:
        Pool Name     total    in-use      free       max   largest     flags
 ------------------------------------------------------------------------------
         CSG BRec      5000         0      5000    200000      5000 DYN
        CSG NoKut         0         0         0    200000         0 DYN
 CSG IntermBackup         0         0         0   1000000         0 DYN
 CSG Intermediate         0         0         0   1000000         0 DYN
      CSG Session         0         0         0   1000000         0 DYN
  CSG GTP Signals        50         0        50         0        50 DYN
     CSG GTP Data     10000         1      9999         0     10000 DYN
    CSG KUT Elems     12500         0     12500         0     12500 DYN
    CSG IMAP Data         0         0         0    200000         0 DYN
     CSG MAIL aoc         0         0         0      5000         0 DYN
 CSG Mail Details         0         0         0    200000         0 DYN
     CSG WAP URLs         0         0         0     50000         0 DYN
  CSG WAP session         0         0         0     50000         0 DYN
  CSG WAP details         0         0         0     50000         0 DYN
    CSG RTSP Buff         0         0         0      1000         0 DYN
   CSG RTSP Fixed         0         0         0    100000         0 DYN
     CSG RTSP Str         0         0         0    200000         0 DYN
     CSG RTSP Ctl         0         0         0    100000         0 DYN
    CSG RTSP Sess         0         0         0    100000         0 DYN
          CSG FTP         0         0         0     50000         0 DYN
   CSG HTTP FIXED         0         0         0    100000         0 DYN
 CSG HTTP Details         0         0         0   1600000         0 DYN
     CSG HTTP REQ         1         0         1   1600000         1 DYN
  CSG HTTP Header         4         0         4   6400000         4 DYN
      CSG buffers         0         0         0     10240         0 DYN
         CSG Frag         0         0         0     16384         0 DYN
 CSG AOC TokenPkt         0         0         0     10000         0 DYN
 CSG AOC TokenReq         0         0         0     10000         0 DYN
 CSG HTTPRedirDet         0         0         0         0         0 DYN
 CSG HTTPRedirUrl         0         0         0         0         0 DYN
     CSG PT Grant         0         0         0         0         0 DYN
 CSG KUT RedirNAT         0         0         0         0         0 DYN
 CSG KUT RedirURL         0         0         0         0         0 DYN
 CSG IMAPSvcStats         0         0         0         0         0 DYN
 CSG KUT SvcStats         0         0         0   1000000         0 DYN
      CSG KUT Svc      8000         0      8000   1000000      8000 DYN
  CSG Svc Connect         0         0         0      1024         0 DYN
     CSG Svc Name         8         3         5       255         8 DYN
     CSG Svc Rule        16         4        12      1024        16 DYN
   CSG QM Request         0         0         0     10000         0 DYN
   CSG BPlan Name         8         5         3       128         8 DYN
```

Table B-7 describes the fields shown in the Buffer Pools table in the display.

Table B-7 show module csg tech-support utilization Field Descriptions

Field	Description
Pool Name	Name of the CSG buffer pool.
total	Total number of buffers currently in the pool.
in-use	Total number of buffers currently being used. If the values in the **in-use** column are growing continuously, even during periods of low usage, and are never declining, there might be a buffer leak. **Note** It is normal for the values in the **GTP Data** row to grow if the Billing Mediation Agent (BMA) is not available. The growth is limited by the setting of the **records max** command.
free	Total number of buffers currently available.
max	Maximum possible number of buffers in the pool. A value of 0 indicates that the buffer is unbounded as long as overall memory is available.
largest	Highwater mark for the number of buffers in the pool.
flags	Additional information about the specific metric: • DYN—Pool can grow dynamically. • GRW—Pool has grown. • SHR—Pool is shrinking. • MAX—Pool is at maximum size.

The following example shows how to display processor statistics for the CSG:

```
Router# show module csg 4 tech-support processor 2
------------------------------------------------------------
---------------------- TCP Statistics ----------------------
------------------------------------------------------------
     Aborted rx                                 3350436013  66840864
     New sessions rx                            180         0
     Total Packets rx                           16940       0
     Total Packets tx                           0           0
     Packets Passthrough                        697         0
     Packets Dropped                            0           0
     Persistent OOO Packets Dropped             0           0
     Persistent Fastpath Tx                     0           0
     Total Persistent Requests                  0           0
     Persistent Same Real                       0           0
     Persistent New Real                        0           0

     Data Packets rx                            877         0
     L4 Data Packets rx                         877         0
     L7 Data Packets rx                         0           0
     Slowpath Packets rx                        7851        0
     Relinquish Requests rx                     8031        0

     TCP xsum failures                          0           0

     Session Mismatch                           0           0
     Session Reused while valid                 0           0
     Unexpected Opcode rx                       0           0
     Unsupported Proto                          0           0
```

```
     Session Queue Overflow                    0           0
     Control->Term Queue Overflow              0           0
     t_fifo Overflow                           0           0

     L7 Analysis Request Sent                  0           0
     L7 Successful LB decisions                0           0
     L7 Need More Data decisions               0           0
     L7 Unsuccessful LB decisions              0           0
     L4 Analysis Request Sent                180           0
     L4 Successful LB decisions              180           0
     L4 Unsuccessful LB decisions              0           0

Transmit:
       SYN                                     0           0
       SYN/ACK                                 0           0
       ACK                                     0           0
       RST/ACK                                 0           0
       data                                    0           0
     Retransmissions:                          0           0
Receive:
       SYN                                   180           0
       SYN/ACK                                 0           0
       ACK                                   340           0
       FIN                                     0           0
       FIN/ACK                               340           0
       RST                                    17           0
       RST/ACK                                 0           0
       data                                    0           0

Session Redundancy Standby:
     Rx Fake SYN                               0           0
     Rx Repeat Fake SYN                        0           0
     Rx Fake Reset                             0           0
     Fake SYN Sent to NAT                      0           0
     Tx Port Sync                              0           0
     Encap Not Found                           0           0
     Fake SYN, TCP State Invalid               0           0

Session Redundancy Active:
     L4 Requests Sent                          0           0
     L7 Requests Sent                          0           0
     Persistent Requests Sent                  0           0
     Rx Fake SYN                               0           0
     Fake SYN Sent to NAT                      0           0

     Sessions torn down                      180           0
     Rx Close session                          1           0
     Slowpath(low pri) buffer allocs        7843           0
     Slowpath(high pri) buffer allocs          8           0
     Small buffer allocs                     180           0
     Medium buffer allocs                      0           0
     Large buffer allocs                       0           0
     Session table allocs                    180           0

     Slowpath(low pri) buffer alloc failures   0           0
     Slowpath(high pri) buffer alloc failures  0           0
     Small buffer allocs failures              0           0
     Medium buffer allocs failures             0           0
     Large buffer allocs failures              0           0
     Session table allocs failures             0           0

     Outstanding slowpath(low pri) buffers     0           0
     Outstanding slowpath(high pri) buffers    0           0
     Outstanding small buffers                 0           0
```

```
Outstanding medium buffers                0           0
Outstanding large buffers                 0           0
Outstanding sessions                      0           0
```

show module csg variable

To display the environmental variables in the configuration, use the **show module csg variable** command in privileged EXEC mode.

show module csg *slot* **variable** [**name** *name*] [**detail**]

Syntax Description

slot	Slot where the CSG resides.
name	(Optional) Keyword to display the named variable information.
detail	(Optional) Keyword to display the map configuration details.

Defaults

If no variable name is specified, the command displays information about all variables.

Command Modes

Privileged EXEC

Command History

Release	Modification
3.1(1)C4(1)—12.2(14)ZA1	This command was introduced.
3.1(3)C5(5)—12.2(18)SXD	Added support for several new variables.

Examples

The following example shows how to display the variable configurations:

```
Router# show module csg 3 variable detail

Name: CSG_BASIS_BYTE_LOW_QUOTA_MAX  Rights: RW
Value: 10000000
Default: 10000000
Valid values: Integer (0 to 10000000)
Description:
Maximum value for the available quota threshold that triggers reauthorization for basis
byte.
.
.
.
```

For a list of all valid variables, see the description of the **variable (module csg)** command.

Related Commands

Command	Description
variable (module csg)	Specifies the environmental variables in the configuration.

show module csg vlan

To display the list of VLANs, use the **show module csg** *slot* **vlan** command in privileged EXEC mode.

show module csg *slot* **vlan** [**client** | **server** | **ft**] [**id** *vlan-id*] [**detail**]

Syntax Description

slot	Slot where the CSG resides.
client	(Optional) Keyword to display only the client VLAN configuration.
server	(Optional) Keyword to display only the server VLAN configuration.
ft	(Optional) Keyword to display only the fault-tolerant configuration.
id	(Optional) Keyword to display the VLAN.
vlan-id	(Optional) Keyword to display the specified VLAN.
detail	(Optional) Keyword to display the map configuration details.

Defaults

If no options are specified, the command displays information about all VLANs.

Command Modes

Privileged EXEC

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Examples

The following example shows how to display the VLAN configurations:

```
Router# show module csg 4 vlan

vlan   IP address       IP mask          type
-------------------------------------------------
11     10.10.4.2        255.255.255.0    CLIENT
12     10.10.3.1        255.255.255.0    SERVER
30     0.0.0.0          0.0.0.0          FT

Router# show module csg 4 vlan detail
vlan   IP address       IP mask          type
-------------------------------------------------
11     10.10.4.2        255.255.255.0    CLIENT
  GATEWAYS
  10.10.4.1
12     10.10.3.1        255.255.255.0    SERVER
30     0.0.0.0          0.0.0.0          FT
```

Related Commands

Command	Description
vlan (module CSG)	Creates a client or server VLAN that defines the Layer 2 paths for the CSG accounting service flows, assigns a VLAN ID and optional name, and enters module CSG VLAN configuration mode.

snmp-server enable traps csg

To enable Simple Network Management Protocol (SNMP) notification types that are available on the CSG, use the **snmp-server enable traps csg** command in global configuration mode. To disable CSG notifications, use the **no** form of this command.

snmp-server enable traps csg {**agent** | **database** | **quota-server**}

no snmp-server enable traps csg {**agent** | **database** | **quota-server**}

Syntax Description

agent	Enable SNMP agent server traps.
database	Enable SNMP CSG database traps.
quota-server	Enable SNMP quota server traps.

Command Default

If you do not enter the **snmp-server enable traps csg** command, no CSG notifications controlled by this command are sent.

Command Modes

Global configuration

Command History

Release	Modification
3.1(1)C4(3)—12.2(14)ZA2	This command was introduced.

Examples

The following example enables CSG database traps:

```
Router(config)# snmp-server enable traps csg database
```

table (module CSG VLAN)

To associate a table name with a VLAN, use the **table** command in module CSG VLAN configuration mode. To remove the table association for the VLAN, use the **no** form of this command.

table *table-name*

no table *table-name*

Syntax Description

table-name	1-to-15 character string identifying the table. The CSG stores the table name as all-uppercase ASCII characters.

Defaults

No default behavior or values.

Command Modes

Module CSG VLAN configuration

Command History

Release	Modification
3.1(1)C6(2)—12.2(18)SXE	This command was introduced.

Usage Guidelines

The User Table identifies all users known to the CSG. The 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. When a table name is associated with a VLAN, User Table entries for user traffic arriving on the VLAN are classified using the configured table name as part of the User Table entry search.

You can associate only one table name with each VLAN.

Examples

The following example associates the ACME_VLAN table with VLAN 254 on module 5:

```
module csg 5
  vlan 254 client
    table ACME_VLAN
```

Related Commands

Command	Description
radius endpoint	Identifies the CSG as an endpoint for RADIUS Accounting messages.
radius proxy	Specifies that the CSG should be a proxy for RADIUS messages.
show module csg variable	Displays the list of VLANs.
vlan (module CSG)	Creates a client or server VLAN that defines the Layer 2 paths for the CSG accounting service flows, assigns a VLAN ID and optional name, and enters module CSG VLAN configuration mode.

url-map

To reference a URL map that is part of a CSG billing policy, use the **url-map** command in CSG policy configuration mode. To delete the reference, use the **no** form of this command.

url-map *url-map-name*

no url-map *url-map-name*

Syntax Description

url-map-name	Name of a URL map, as configured with the **ip csg map** command.

Defaults

No default behavior or values.

Command Modes

CSG policy configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

The conditions specified in the referenced URL map must be true in order for the flows to be processed by the CSG accounting services. If the conditions are not true, the flows are not processed.

For WAP 1.x, URL maps take precedence over access lists.

For WAP1.x and RTSP, the policy used to determine the next hop address is chosen based solely on access control lists (ACLs), not URL maps. As a result, you can choose the next hop from one policy for routing and from a different policy for billing.

Examples

The following example shows how to reference a URL map:

```
ip csg policy MOVIES_COMEDY
 accounting type http customer-string MOVIES_COMEDY
 client-group 44
 client-ip http-header x-forwarded-for
 header-map MOVIES
 url-map MOVIES
```

Related Commands

Command	Description
header-map	References a header map that is part of a CSG billing policy.
ip csg map	Defines the CSG billing content filters (URL and header maps), and enters CSG map configuration mode.
ip csg policy	Defines a policy for qualifying flows for the CSG accounting services, and enters CSG policy configuration mode.

Command	Description
match (header map)	Specifies a header match pattern for a CSG billing map.
match (URL map)	Specifies a URL match pattern for a CSG billing map.

user-group

To associate a user group with a specific accounting service, use the **user-group** command in CSG accounting configuration mode. To disassociate a user group in order to delete it, use the **no** form of this command.

user-group *group-name*

no user-group *group-name*

Syntax Description

group-name	Name of a configured user group to be associated with this accounting service. Only one user group can be associated with each accounting service.

Defaults

No default behavior or values.

Command Modes

CSG accounting configuration

Command History

Release	Modification
2.2(1)C(1)—12.1(11b)E3	This command was introduced.

Examples

The following example associates user-group G1 with the CSG accounting group A1:

```
ip csg accounting A1
 user-group G1
 agent activate 2
 agent local-port 3775
 agent 10.1.2.4 11112 10
 agent 10.1.2.5 11113 20
 keepalive 3
 records batch
 records http-statistics
 records intermediate bytes 100000 time 3600
 records max 250
 inservice
```

Related Commands

Command	Description
ip csg accounting	Defines content-based accounting as a service.
ip csg user-group	Creates a group of end users for which you want to generate accounting records, and enters CSG user group configuration mode.

user-profile server

To specify which server is used to obtain the user profile (or billing plan), use the **user-profile server** command in CSG user group configuration mode. To restore the default setting, use the **no** form of this command

user-profile server {**quota** | **radius** {**remove** | **pass**}}

no user-profile server {**quota** | **radius** {**remove** | **pass**}}

Syntax Description

quota	Obtains the billing plan from the quota server.
radius	Obtains the billing plan from the RADIUS message.
remove	Removes the VSA containing the billing plan from the Access-Accept message.
pass	Does not remove the VSA containing the billing plan from the Access-Accept message.

Defaults

If not configured, the default behavior is to obtain the billing plan from the quota server.

Command Modes

CSG user group configuration

Command History

Release	Modification
3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.

Usage Guidelines

If not specified, the quota server is used to obtain the billing plan. If **radius** is specified, the RADIUS Access-Accept and RADIUS Accounting-Request messages are parsed for the Cisco VSA, sub-attribute 1, which contains the billing plan name. The VSA is optionally removed from the RADIUS Access-Accept message before the message is sent to the RADIUS client or server.

Keep the following considerations in mind:

- The VSA is removed from the RADIUS Access-Accept message only if **remove** is specified. You should use **remove** only if the RADIUS client cannot tolerate the Cisco VSA in the message.
- We recommend that you use **pass** to reduce processing time on the CSG.
- The user ID must be in the message containing the billing plan.

Examples

The following example illustrates the **user-profile server** command:

```
ip csg user-group G1
  radius userid User-Name
  user-profile server radius pass
```

Related Commands

Command	Description
radius userid	Specifies the RADIUS attribute used to extract the user identifier from a RADIUS record.

variable (module csg)

To specify the environmental variables in the configuration, use the **variable** command in module CSG configuration mode. To remove environmental variables from the configuration, use the **no** form of this command.

variable *name value*

no variable *name value*

Syntax Description

name	Specifies a name string for the variable. See Table B-8 for a list of valid variable names.
value	Specifies a value string for the variable.

Defaults

No default behavior or values.

Command Modes

Module CSG configuration

Command History

Release	Modification
3.1(1)C4(1)—12.2(14)ZA1	This command was introduced.
3.1(3)C5(1)—12.2(17d)SXB	Added support for the MAX_PARSE_LEN_MULTIPLIER variable.
3.1(3)C5(3)—12.2(18)SXD	Added support for several new variables.
3.1(3)C5(5)—12.2(18)SXD	Added support for several new variables.
3.1(3)C6(2)—12.2(18)SXD	Added support for the CSG_FT_CONTENT variable.

Usage Guidelines

Table B-8 lists the environmental values used by the CSG.

Table B-8 Environmental Variables

Name	Default	Valid Values	Description
ARP_INTERVAL	300	Integer (15 to 31536000)	Time (in seconds) between ARPs for configured hosts.
ARP_LEARNED_INTERVAL	14400	Integer (60 to 31536000)	Time (in seconds) between ARPs for learned hosts.
ARP_GRATUITOUS_INTERVAL	15	Integer (10 to 31536000)	Time (in seconds) between gratuitous ARPs.
ARP_RATE	10	Integer (1 to 60)	Seconds between ARP retries.
ARP_RETRIES	3	Integer (2 to 15)	Count of ARP attempts before flagging a host as down.

Table B-8 Environmental Variables (continued)

Name	Default	Valid Values	Description
ARP_LEARN_MODE	1	Integer (0 or 1)	Indicates whether the CSG learns the MAC address on responses only (0) or on all traffic (1).
CSG_BASIS_BYTE_LOW_QUOTA_MAX	10000000	Integer (0 to 10000000)	Maximum value for the available quota threshold that triggers reauthorization for basis byte.
CSG_BASIS_BYTE_RESERVED_ MAX	10000000	Integer (2048 to 10000000)	Maximum unaccounted quota (basis byte) reserved per IP session.
CSG_BASIS_FIXED_LOW_QUOTA_MAX	10000000	Integer (0 to 10000000)	Maximum value for the available quota threshold that triggers reauthorization for basis fixed.
CSG_BASIS_SEC_LOW_QUOTA	10	Integer (5 to 300)	Value for the available quota threshold that triggers reauthorization for basis second.
CSG_BILL_Q_HI_THRESHOLD	5000	Integer (5000 to 65535)	Threshold for throttling the CSG billing queue.
CSG_BILL_Q_LO_THRESHOLD	3000	Integer (3000 to 65535)	Threshold for resetting the throttling of the CSG billing queue.
CSG_EXTRA_DEBUG	-	String (0 to 255 chars)	String to define extra debugs.
CSG_FAST_FIN_TIMEOUT	10	Integer (10 to 65535)	Timeout (in seconds) for connection reset after FIN is detected.
CSG_FRAG_BUFFER_MAX	100	Integer (0 to 65535)	Maximum number of buffered trailers.
CSG_FRAG_LIFETIME	10	Integer (1 to 255)	Fragment database entry lifetime (seconds).
CSG_FRAG_POOL_MAX	16384	Integer (1 to 50000)	Maximum fragment database size.
CSG_FREE_CONTENT_ACCESS_PERMIT	0	Integer (0 or 1)	Permit forwarding of free content in a prepaid service when access to the service is denied.
CSG_FT_CONTENT	0	Integer (0 or 1)	Replicate session only if configured in content (1) or always (0).
CSG_FTP_HA_WAIT_DELAY	10	Integer (1 to 60)	Delay, in sixtieths of a second, after sending FTP content information to the backup.
CSG_FTP_PWD	0	Integer (0 or 1)	Disables injection of the PWD command into the FTP control connection.
CSG_GTP_MAX_RETRIES	3	Integer (1 to 4294967295)	Maximum number of GTP repolls before link failure.

Table B-8 Environmental Variables (continued)

Name	Default	Valid Values	Description
CSG_GTP_RETRY_TIME	4	Integer (2 to 4294967295)	GTP retransmit delay time (in seconds).
CSG_GTP_TX_WINDOW	128	Integer (1 to 4294967295)	GTP transmit window size.
CSG_HTTP_FIXED_INTERM_CDRS	0	Integer (0 or 1)	Control the generation of fixed intermediate CDRs for HTTP when **records format fixed** is configured.
CSG_HTTP_PERSISTENCE_ DISABLE	0	Integer (0 or 1)	Disable HTTP persistent connections. **Note** This variable is no longer necessary in the CSG. It is made obsolete by the CSG's full pipelining support.
CSG_HTTP_1_0_OPERATION	0	Integer (0 or 1)	Overwrite HTTP version to 1.0. **Note** This variable is no longer necessary in the CSG. It is made obsolete by the CSG's full pipelining support.
CSG_IXP_FPGA_TRAP_ENABLED	0	Integer (0 or 1)	Enable IXP FPGA hang detection.
CSG_IXP_WATCHDOG_ENABLED	1	Integer (0 or 1)	Enable IXP Watchdog processing.
CSG_IXP_WATCHDOG_TIMEOUT	60	Integer (30 to 3600)	IXP Watchdog timeout (in seconds).
CSG_MAX_BPLANS	128	Integer (128; read-only)	Maximum number of CSG billing plans.
CSG_PERSISTENT_PARSE	0	Integer (0 or 1)	Disables parsing for multiple requests in persistent HTTP connections. **Note** This variable is no longer necessary in the CSG. It is made obsolete by the CSG's full pipelining support.
CSG_QUOTA_BLOCK	1	Integer (0 or 1)	Drop (1) or forward (0) packets during quota reconciliation.
CSG_RADIUS_PROXY_CLIENT_REUSE	7200	Integer (0 to 1000000)	Reuse RADIUS proxy blocks if idle for the specified number of seconds. Specify 0 if you do not want to reuse blocks.
CSG_REDIRECTS_INTERVAL	8	Integer (0 to 3600)	Time interval, in seconds, for redirecting an out-of-quota subscriber. The start of the interval is the time of the first redirect after a quota grant of zero.

Table B-8 Environmental Variables (continued)

Name	Default	Valid Values	Description
CSG_REDIRECTS_MAX	15	Integer (0 to 255)	Maximum number of times a redirect is to be performed for an out-of-quota subscriber during a redirect interval.
CSG_RPR_PLUS_DELAY	90	Integer (1 to 1200)	Delay (in seconds) after an RPR+ switchover before the CSG detects timeouts.
CSG_SVC_CDR_MODE_QGRANT	65535	Integer (5000 to 16777216)	Amount of quota reservation for a session matching a service with service-level CDR granularity.
CSG_WAP_APPEND_AOC_URL	0	Integer (0 or 1)	Append the original URL to the redirect URL sent by the quota server on a Content Authorization REDIRECT_URL response.
CSG_WAP_REDIRECTS_MAX	15	Integer (1 to 255)	Maximum number of times a redirect attempt is to be performed for a single WAP session. **Note** This variable is no longer necessary in the CSG. It is replaced by CSG_REDIRECTS_MAX .
CSG_WAP_REPORT_ACTUAL_PDU_TYPE	0	Integer (0 or 1)	Report the real PDU types parsed in WAP packets.
CSG_ZERO_QUOTA_TIMEOUT_ INIT	4	Integer (1 to 3600)	Initial timeout for reauthorization after quota grant of zero. The value specified for CSG_ZERO_QUOTA_TIMEOUT _ INIT must be less than or equal to the value specified for CSG_REDIRECTS_INTERVAL.
CSG_ZERO_QUOTA_TIMEOUT_MAX	60	Integer (1 to 3600)	Maximum timeout for reauthorization after quota grant of zero.
DEBUG_BILL_URL	1	Integer (0 or 1)	Enable (1) or disable (0) debugging messages for bill URL messages.
DEST_UNREACHABLE_MASK	0xffff	Integer (0 to 65535)	Bitmask defining which ICMP destination unreachable codes are to be forwarded.
HTTP_CASE_SENSITIVE_MATCHING	1	Integer (0 or 1)	Indicates whether the URL (cookie, header) matching and sticky are case-sensitive.

Table B-8 Environmental Variables (continued)

Name	Default	Valid Values	Description
MAX_PARSE_LEN_MULTIPLIER	1	Integer (1 to 16)	Multiply the configured MAX_PARSE_LEN by this integer. If you specify too large an integer, you might limit the number of requests that can be processed at one time.
ROUTE_UNKNOWN_FLOW_PKTS	0	Integer (0 or 1)	Indicates whether to route non-SYN packets that do not match any existing flows.

Examples

This example shows how to enable the environmental variables configuration:

```
Router (config-module-csg)# variable CSG_BASIS_FIXED_LOW_QUOTA_MAX 1000000
```

Related Commands

Command	Description
module csg	Enters module CSG configuration mode for a specified slot.
show module csg variable	Displays the environmental variables in the configuration.

verify

To enable service verification, use the **verify** command in CSG service configuration mode. To disable this feature, use the **no** form of this command.

verify

no verify

Syntax Description

There are no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

CSG service configuration

Command History

Release	Modification
3.1(3)C5(5)—12.2(18)SXD	This command was introduced.

Usage Guidelines

If this command is configured, the CSG uses the ServiceVerificationRequest to perform the following actions:

- Alert the quota server of a new transaction.
- Allow the quota server to direct the CSG to perform one of the following mutually exclusive actions:
  - **DROP**—Drop all packets for this flow.
  - **FORWARD**—Forward the flow without altering the destination.
  - **REDIRECT-NAT**—Forward all packets for this flow to the IP address provided in the ContentAuthResp. The CSG NATs the packet to the IP address and port provided in the ContentAuthResp.
  - **REDIRECT-URL**—Redirect the client request to the URL provided in the ContentAuthResp. The CSG sends a Layer 7 redirect (for example, an HTTP 302 response) to the client that contains the redirect URL.

Examples

The following example specifies a token for service verification URL-rewriting:

```
ip csg service SERVICE_NAME
    verify
```

Related Commands

Command	Description
ip csg service	Defines a content billing service, and enters CSG service configuration mode.
verify confirmation	Configures a token for use in service verification URL-rewriting.

verify confirmation

To configure a token for use in service verification URL-rewriting, use the **verify confirmation** command in CSG user group configuration mode. To remove the token, use the **no** form of this command.

verify confirmation *token*

no verify confirmation *token*

Syntax Description

token	A string of up to 15 alpha numeric characters.

Defaults

No default behavior or values.

Command Modes

CSG user group configuration

Command History

Release	Modification
3.1(3)C5(5)—12.2(18)SXD	This command was introduced.

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 server.

The token is used for both HTTP and WAP service verification URL-rewriting.

Examples

The following example specifies a token for service verification URL-rewriting:

```
ip csg user-group A1
    verify confirmation ?CSG_VERIFY_OK
```

Related Commands

Command	Description
verify	Enables service verification.

vlan (CSG content)

To restrict the CSG billing content to a single source VLAN, use the **vlan** command in CSG content configuration mode. To remove the restriction, use the **no** form of this command.

vlan *vlan-name*

no vlan *vlan-name*

Syntax Description

vlan-name	Name of the source VLAN for the CSG billing content.

Defaults

No default behavior or values.

Command Modes

CSG content configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

The VLAN number is dependent on the CSG card that receives the content definition. When the content is downloaded to a CSG card, the *vlan-name* argument is mapped to a specific VLAN number.

Examples

The following example shows how to restrict the CSG content billing to a single-source VLAN named MOVIES_COMEDY:

```
ip csg content MOVIES_COMEDY
 client 10.4.4.0 255.255.255.0
 idle 120
 ip 172.18.45.0/24 tcp 8080
 policy POLICY1
 replicate connection tcp
 vlan MOVIES_COMEDY
 inservice
```

Related Commands

Command	Description
ip csg content	Defines content for the CSG accounting services, and enters CSG content configuration mode.

vlan (module CSG)

To create a client or server VLAN that defines the Layer 2 paths for the CSG accounting service flows, assign a VLAN ID and optional name, and enter module CSG VLAN configuration mode, use the **vlan** command in module CSG configuration mode. To remove the VLAN from the configuration, use the **no** form of this command.

vlan *vlan-id* {**client** | **server**} [*vlan-name*]

no vlan *vlan-id* {**client** | **server**} [*vlan-name*]

Syntax Description

vlan-id	Number of the VLAN. The valid range is 2 to 4095. There is no default value. This VLAN defines the Layer 2 paths for the CSG accounting service flows as well as all filters defined by the service. **Note** You cannot use VLAN 1 as a client-side or server-side VLAN for the CSG.
client	Keyword to specify a client-side VLAN.
server	Keyword to specify a server-side VLAN.
vlan-name	(Optional) Unique symbolic name of the VLAN. The name can be 1 to 15 characters, uppercase or lowercase letters (the CSG changes all letters to uppercase), numbers, and any special characters. The *vlan-name* argument is required if the content specification includes the **vlan** command in CSG content configuration mode.

Defaults

No default behavior or values.

Command Modes

Module CSG configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

A VLAN database entry should exist for the given VLAN ID.

When a content configuration is downloaded that includes a **vlan** command that specifies the same *vlan-name* argument, the CSG translates the *vlan-name* argument to the correct *vlan-id* argument when the content is installed on the CSG card.

If the downloaded content configuration does not include a **vlan** command, or if the **vlan** command does not specify a valid *vlan-name* argument, then the content configuration cannot be brought inservice because no source VLAN is defined.

The characteristics of each VLAN are defined by the following commands:

- **alias (module CSG VLAN)**
- **gateway (module CSG VLAN)**
- **ip address (module CSG VLAN)**
- **route (module CSG VLAN)**
- **table (module CSG VLAN)**

Examples

The following example shows how to create client-side VLANs with IDs 301, 320, and 400 for the CSG in slot 4:

```
module csg 4
 accounting A1
 ft group 123 vlan 5
 ruleset R1
 vlan 301 client
  name TO-GGSN-MS-APN
  gateway 31.0.0.10
  ip address 31.0.0.21 255.255.255.0
  route 11.0.0.0 255.255.0.0 gateway 31.0.0.1
  route 11.1.0.0 255.255.0.0 gateway 31.0.0.2
  route 11.2.0.0 255.255.0.0 gateway 31.0.0.3
  route 11.3.0.0 255.255.0.0 gateway 31.0.0.4
  alias 31.0.0.51 255.255.255.0
 vlan 320 client
 vlan 400 server
```

Related Commands

Command	Description
alias (module CSG VLAN)	Assigns multiple IP addresses to the CSG.
gateway (module CSG VLAN)	Configures a gateway IP address.
ip address (module CSG VLAN)	Assigns an IP address to the CSG VLAN.
module csg	Enters module CSG configuration mode for a specified slot.
route (module CSG VLAN)	Configures networks that are not Layer 2 adjacent to the CSG.
show module csg vlan	Displays the list of VLANs.

zero-quota abort type

To force WAP transactions to be aborted midstream when the user's quota has been depleted, use the **zero-quota abort type** command in CSG service configuration mode. To return to the default behavior, use the **no** form of the command.

zero-quota abort type {**wap**}

no zero-quota abort type {**wap**}

Syntax Description

wap	Keyword to specify that WAP transactions be aborted midstream when user's quota is depleted.

Defaults

No default behavior or values.

Command Modes

CSG service configuration

Command History

Release	Modification
3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.

Usage Guidelines

This command is configured on a per-service basis.

This command configures the WAP cutoff feature.

Examples

The following example shows how to enable the **zero-quota abort type** command:

```
ip csg service SERVIN_WAP
  zero-quota abort type wap
  content WAP_WTP_CONTENT policy WAP_WTP
```

Related Commands

Command	Description
ip csg service	Defines a content billing service, and enters CSG service configuration mode.

Standards Compliance Specifications

Catalyst 6000 series switches and Cisco 7600 series routers, when installed in a system, comply with the standards listed in Table C-1.

Table C-1 Regulatory Standards Compliance

Agency Approvals	Description
Compliance	CE[1] Marking
Safety	UL[2] 1950, CSA[3]-C22.2 No. 950, EN[4] 60950, IEC[5] 950, TS[6] 001, AS/NZS[7] 3260
Electromagnetic compatibility (EMC)	FCC[8] Part 15 (CFR[9] 47) Class A, ICES[10]-003 Class A, EN55022 Class A, CISPR22 Class A, AS/NZS 3548 Class A, and VCCI Class A, EN55024, EN300 386, EH50082-1, EN55022 Class B, CISPR22 Class B, VCCI Class B, AS/NZ 3548 Class B

1. CE = European Compliance
2. UL = Underwriters Laboratory
3. CSA = Canadian Standards Association
4. EN = European Norm
5. IEC = International Electrotechnical Commission
6. TS = Technical Specification
7. AS/NZS = Standards Australia/Standards New Zealand
8. FCC = Federal Communications Commission
9. CFR = Code of Federal Regulations
10. ICES = Interference-Causing Equipment Standard

Protocol Compliance Statements for the CSG 3.1(3)C6(2)

This appendix provides protocol compliance statements for the CSG 3.1(3)C6(2). Any RFCs that are not explicitly listed are not supported.

Layer 4 Inspection (accounting type=other)

The CSG differentiates TCP and UDP, and classifies all other protocols simply as IP. All protocols can be billed in this manner if further protocol-specific processing is not desired (or if deeper inspection for such protocols is not supported).

- IP—Compliant with RFC791. To avoid leakage, the CSG drops packets on a service for a prepaid user while reconciling the user's quota for that service. The frequency depends on how quickly the user is consuming quota on that service and generally amounts to a few packets. This is controlled by setting the CSG_BASIS_BYTE_RESERVED_MAX variable up to a setting of 256000. Settings above this value have no effect.

  The CSG volume counters wrap at 0xFFFFFFFF (268435455 bytes). The volume counters are 32 bits unsigned.

  The CSG supports IP fragmentation for generic Layer 4 flows, regardless of protocol and regardless of the order in which the flows arrive.
- UDP—Compliant with RFC768.
- TCP—Compliant with standard TCP (RFC3168).

Layer 7 Inspection (accounting type=specific protocol)

- IP—Compliant with RFC791.

  The CSG supports IP fragmentation for HTTP, WAP2.0, and WAP1.x, regardless of the order in which the flows arrive. The CSG does not support IP fragmentation for SMTP, POP3, IMAP4, FTP, and RTSP control connection, nor for RADIUS flows. The CSG drops IP fragments for those unsupported protocols.

To avoid leakage, the CSG drops packets on a service for a prepaid user while reconciling the user's quota for that service. The frequency depends on how quickly the user is consuming quota on that service and generally amounts to a few packets. This is controlled by setting the CSG_BASIS_BYTE_RESERVED_MAX variable up to a setting of 256000. Settings above this value have no effect.

The CSG volume counters wrap at 0xFFFFFFFF (268435455 bytes). The volume counters are 32 bits unsigned.

- UDP—Compliant with RFC768.

  See IP compliance for further restrictions.

- TCP—Compliant with standard TCP (RFC793), with the following exceptions:
  - The CSG does not pass TCP header options when performing deep packet inspection, other than MSS.
  - When performing Layer 7 inspection of TCP-based protocols, the CSG drops packets that arrive out of order, relying on retransmission to provide them again after the missing packets are received. Those packets that require inspection, and that are therefore subject to this dropping, vary per protocol. For HTTP, the CSG parses only HTTP headers, so the packets carrying HTTP headers must be in order. After the header parsing is complete and the CSG has detected the body, the CSG no longer enforces the order of the packets. This repeats for each transaction in a persistent or pipelined connection. There are two important exceptions to this: for chunked encoding, and for multipart content, every packet must be analyzed and therefore is dropped if not in order. For e-mail protocols (that is, SMTP, POP3, and IMAP4), all packets must be in order.

  See IP compliance for further restrictions.

- WP-TCP—Compliant with mandatory elements of Wireless Profiled TCP (WP-TCP) (WAP-225-TCP-20010331-a at http://www.wapforum.org/what/technical.htm), with the exception of SACK (RFC2018).

  Impact: End-user latency for lossy transmissions.

  See TCP compliance for further restrictions.

- HTTP—Compliant with RFC1945 (HTTP 1.0) and RFC2616 (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: Client requests transfer no data (that is, they hang). See TO-TCP in MMS for WAP 2.0 compliance for an example.

  2. The maximum HTTP transaction volume is 268435455 bytes. If this length is exceeded, the CSG invokes Layer 4 billing for the remainder of the connection.

  3. HTTP request parsing is limited to 64000 bytes.

     Impact: Any headers beyond this limit are not recognized and therefore are not used in matching URL or header maps.

  4. The CSG supports up to 65535 concurrent HTTP TCP connections.

  5. If the HTTP server or client causes improper parsing, the CSG reverts to Layer 4 billing for the remainder of the TCP connection.

     For example, the CSG requires that all HTTP responses begin with the string "HTTP". If an HTTP response does not begin with "HTTP", the CSG increments a Layer 7 error statistic, "HTTP invalid msgs", and invokes Layer 4 billing.

Also, when parsing the response for an HTTP return code, the CSG accepts only ASCII decimal digits (0x30 - 0x39). If the response contains any other characters, the CSG increments the "HTTP invalid msgs" statistic and invokes Layer 4 billing.

If the CSG cannot parse the HTTP HEAD method, it invokes Layer 4 billing for all subsequent traffic.

6. HTTP status 101 (switching protocols) is not supported. The CSG expects all subsequent requests to be unencrypted and parsable by HTTP rules (see HTTPS compliance for further restrictions).

   Impact: The user TCP connection might hang until the content idle timer expires, or until the connection closes for some other reason.

7. Error codes 204, 205, and 304 do not require a body. If a response contains one of these error codes, the CSG ignores "Content-Type:", "Content-Length:", and "Transfer-Encoding:chunked" headers that might be present in error.

8. The CSG does not support the CLOSING or TIME-WAIT states for TCP connections. After the end-points exchange FIN_ACK messages, the connection is terminated immediately, and the CSG does not process any out-of-order packets for the connection.

9. The existence of a Head method in a persistent HTTP TCP connection causes the CSG to invoke Layer 4 billing for the remainder of the connection. This Layer 4 charging is reported via the HTTPstatistics CDR for the Connect transaction. The CSG will not discern any additional transactions after the Head 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 CSG passes the traffic without charge.

10. Multipart content causes the CSG to invoke Layer 4 billing for the remainder of the connection.

Compliant with RFC2774 (HTTP Extension Framework), subject to the restrictions above.

See TCP compliance for further restrictions.

- HTTPS—Because HTTPS URLs and other headers are encrypted, the CSG 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 (RFC2817) is supported. The CSG detects the Connect method and invokes Layer 4 billing for the remainder of the TCP connection. This Layer 4 charging is reported via the HTTPstatistics CDR for the Connect transaction. The CSG 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 CSG passes the traffic without charge.

  – Switching via the "Upgrade" header (RFC2817) is ignored. The CSG attempts to parse the traffic as normal HTTP. When parsing fails, the CSG invokes Layer 4 billing for all subsequent traffic on the TCP connection, charging against the last matching Policy.

  See HTTP compliance for further restrictions.

- WAP 2.0 (HTTP over WP-TCP transport)—The CSG supports the billing of WAP 2.0 over clear text HTTP and the differential billing of MMS over WAP 2.0 over clear text HTTP (see MMS for WAP 2.0 compliance for details) as specified by the WapForum (wapforum.org - http://www1.wapforum.org/tech/terms.asp?doc=Technical_WAP2_0-20021106.zip), with the following exceptions:

  - There are two variants of Push OTA-HTTP: TO-TCP and PO-TCP. The CSG does not support TO-TCP, as described in WAP-235-PushOTA-20010425-a, for flows billed at Layer 7 (that is, those with HTTP policies). PO-TCP can be configured but requires more complex configuration (see MMS for WAP 2.0 compliance for details).
  - The CSG cannot bill TLS (encrypted connections) as WAP 2.0 flows. In WAP-235-PushOTA-20010425-a, TLS is referenced as OTA-HTTP-TLS.
  - See HTTPS compliance for restrictions regarding 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 RFC2817 pertaining to Upgrade requests or responses are not supported by WAP 2.0 clients).
  - Because the CSG does not currently pass TCP options, the CSG does not support the <WAP-GW-STD-11>, <WAP-GW-STD-13>, <WAP-GW-STD-14>, <WAP-GW-STD-15>, and <WAP-GW-STD-17> standards.

  See HTTP 1.1, HTTPS, and WP-TCP compliance for further restrictions.

- MMS for WAP 2.0 (HTTP transport)—At the current time, the MMS standard is very incomplete.
  - For MMS differentiation, the CSG requires that the “Content-Type” header in the request be set to “application/vnd.wap.mms-message” on all MMS/WAP2/HTTP exchanges, other than message retrieval.
  - For message retrieval, the “Content-Type” header is not present in the GET request, so the CSG 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 would be the canonical technique for MMS differentiation per the standard.

MMS over WAP 2.0 allows three types of notification:

1. SMS-based notification carrying the URI for the MMS. The handset then initiates a GET request to that URI to retrieve the information.
2. TO-TCP (Terminal-Originated TCP). TO-TCP starts with SMS but provides only the IP address of the 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 (PPG-Originated TCP). PO-TCP is similar to TO-TCP, except the TCP connection is opened by the PPG and is followed by the OPTIONS method.

The CSG Layer 7 billing for MMS relies entirely on options 1 and 3. The CSG 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 TCP retry attempts expire.

See WAP 2.0 compliance for further restrictions.

- POP3—Compliant with RFC1939. The CSG reports the RFC2822 (Internet-Message Format) headers in the body of the POP3 message.

  See TCP compliance for further restrictions.

- IMAP4—Compliant with RFC3501.

  See TCP compliance for further restrictions.

- SMTP—Compliant with RFC 2821 - Simple Mail Transfer Protocol. Reports headers in the SMTP body formatted in accordance with RFC 2822 - Internet Message Format.

  The CSG 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 either incomplete or no SMTP envelope and RFC 2822 headers are reported (depending on the e-mail content).

  See TCP compliance for further restrictions.

- FTP—Compliant with RFC959. The CSG requires that the control connection use port 21 on the server.

  See TCP compliance for further restrictions.

- RTSP—Compliant with RFC2326, except that the RFC allows RTSP control flows on either TCP or UDP, but the CSG supports RTSP control flows only on TCP. The CSG requires that the control connection use port 554 on the server, even though some servers allow other ports to be used. The CSG does not parse SMIL or SDP files, so correlation is not supported across multiple elements in the file.

  For Interleaved RTSP (Control and Stream both sharing the control connection), and for RTSP over HTTP:554 (with policy of type=rtsp), the CSG parses only the first SETUP command.

  See TCP compliance for further restrictions.

- WAP 1.x (WSP/WTP)—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 WSP is identified via WSP Content Type values 0X3E or application/vnd.wap.mms-message.

See UDP compliance for further restrictions.

- RADIUS—Compliant with RFC2865 and RFC2866. The CSG can inspect RADIUS Access and RADIUS Accounting messages.

  For RADIUS inspection, the CSG does not support fragmented RADIUS messages nor messages that exceed an Ethernet frame size (approximately 1470 bytes). Also, the CSG 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 CSG 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 CSG 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 CSG 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 CSG 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 should be sent. The CSG allows the customer to configure the NAS port. Also, note specific actions to be taken when the Ack or Nak is received—The CSG uses the Ack or Nak only to determine whether it should send the Request. The CSG does not use, process, or report any attributes included in the Ack or Nak. Attributes that the CSG sends in the Request are defined by the customer.

    The CSG does not support any other message types in this RFC.

  See UDP compliance for further restrictions.

APPENDIX E

Translated Safety Warnings

Safety Information Referral Warning

Warning **Before you install, operate, or service the system, read the *Site Preparation and Safety Guide*. This guide contains important safety information you should know before working with the system.**

Waarschuwing **Lees de handleiding *Voorbereiding en veiligheid van de locatie Handleiding* voordat u het systeem installeert of gebruikt of voordat u onderhoud aan het systeem uitvoert. Deze handleiding bevat belangrijke beveiligingsvoorschriften waarvan u op de hoogte moet zijn voordat u met het systeem gaat werken.**

Varoitus **Ennen kuin asennat järjestelmän tai käytät tai huollat sitä, lue *Asennuspaikan valmistelu-jaturvaopas* -opasta. Tässä oppaassa on tärkeitä turvallisuustietoja, jotka tulisi tietää ennen järjestelmän käyttämistä.**

Attention **Avant d'installer le système, de l'utiliser ou d'assurer son entretien, veuillez lire le *Guide de sécurité et de préparation du site*. Celui-ci présente des informations importantes relatives à la sécurité, dont vous devriez prendre connaissance.**

Warnung **Warnhinweis Bevor Sie das System installieren, in Betrieb setzen oder warten, lesen Sie die *Anleitung zur Standortvorbereitung und Sicherheitshinweise*. Dieses Handbuch enthält wichtige Informationen zur Sicherheit, mit denen Sie sich vor dem Verwenden des Systems vertraut machen sollten.**

Avvertenza **Prima di installare, mettere in funzione o effettuare interventi di manutenzione sul sistema, leggere le informazioni contenute nella documentazione sulla *Guida alla sicurezza*. Tale guida contiene importanti informazioni che è necessario acquisire prima di iniziare qualsiasi intervento sul sistema.**

Advarsel **Før du installerer, tar i bruk eller utfører vedlikehold på systemet, må du lese *Veiledning for stedsklargjøring og sikkerhet*. Denne håndboken inneholder viktig informasjon om sikkerhet som du bør være kjent med før du begynner å arbeide med systemet.**

Aviso **Antes de instalar, funcionar com, ou prestar assistência ao sistema, leia o *Guia de Preparação e Segurança do Local*. Este guia contém informações de segurança importantes que deve conhecer antes de trabalhar com o sistema.**

¡Advertencia! **Antes de instalar, manejar o arreglar el sistema, le aconsejamos que consulte la *Guía de prevención y preparación de una instalación*. Esta guía contiene importante información para su seguridad que debe saber antes de comenzar a trabajar con el sistema.**

Varning! **Innan du installerar, använder eller utför service på systemet ska du läsa *Förberedelser och säkerhet Handbok*. Denna handbok innehåller viktig säkerhetsinformation som du bör känna till innan du arbetar med systemet.**

Wrist Strap Warning

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.**

Waarschuwing **Draag tijdens deze procedure aardingspolsbanden om te vermijden dat de kaart beschadigd wordt door elektrostatische ontlading. Raak het achterbord niet rechtstreeks aan met uw hand of met een metalen werktuig, omdat u anders een elektrische schok zou kunnen oplopen.**

Varoitus **Käytä tämän toimenpiteen aikana maadoitettuja rannesuojia estääksesi kortin vaurioitumisen sähköstaattisen purkauksen vuoksi. Älä kosketa taustalevyä suoraan kädelläsi tai metallisella työkalulla sähköiskuvaaran takia.**

Attention **Lors de cette procédure, toujours porter des bracelets antistatiques pour éviter que des décharges électriques n'endommagent la carte. Pour éviter l'électrocution, ne pas toucher le fond de panier directement avec la main ni avec un outil métallique.**

Warnung **Zur Vermeidung einer Beschädigung der Karte durch elektrostatische Entladung während dieses Verfahrens ein Erdungsband am Handgelenk tragen. Bei Berührung der Rückwand mit der Hand oder einem metallenen Werkzeug besteht Elektroschockgefahr.**

Avvertenza **Durante questa procedura, indossare bracciali antistatici per evitare danni alla scheda causati da un'eventuale scarica elettrostatica. Non toccare direttamente il pannello delle connessioni, né con le mani né con un qualsiasi utensile metallico, perché esiste il pericolo di folgorazione.**

Advarsel **Bruk jordingsarmbånd under prosedyren for å unngå ESD-skader på kortet. Unngå direkte berøring av bakplanet med hånden eller metallverktøy, slik at di ikke får elektrisk støt.**

Aviso **Durante este procedimento e para evitar danos ESD causados à placa, use fitas de ligação à terra para os pulsos. Para evitar o risco de choque eléctrico, não toque directamente na parte posterior com a mão ou com qualquer ferramenta metálica.**

¡Advertencia! **Usartiras conectadas a tierra en las muñecas durante este procedimiento para evitar daños en la tarjeta causados por descargas electrostáticas. No tocar el plano posterior con las manos ni con ninguna herramienta metálica, ya que podría producir un choque eléctrico.**

Varning! **Använd jordade armbandsremmar under denna procedur för att förhindra elektrostatisk skada på kortet. Rör inte vid baksidan med handen eller metallverktyg då detta kan orsaka elektrisk stöt.**

Blank Faceplate Installation Requirement Warning

Warning **Blank faceplates (filler panels) serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards and faceplates are in place.**

Waarschuwing **Lege vlakplaten (vulpanelen) vervullen drie belangrijke functies: ze voorkomen blootstelling aan gevaarlijke voltages en elektrische stroom binnenin het chassis; ze beperken elektromagnetische storing hetgeen andere apparaten kan storen en ze leiden een stroom van koellucht door het chassis. Bedien het systeem niet tenzij alle kaarten en vlakplaten zich op hun plaats bevinden.**

Varoitus **Tyhjillä kansilaatoilla (peitelevyillä) on kolme tehtävää: ne suojaavat vaarallisilta asennuspohjan sisäisiltä jännitteiltä ja virroilta; suojaavat sähkömagneettiselta häiriöltä (EMI), joka voi haitata muiden laitteiden toimintaa; ja ohjaavat jäähdytysilmavirran asennuspohjan läpi. Laitetta ei saa käyttää, jos kaikki kortit ja peitelevyt eivät ole paikoillaan.**

Attention **Les caches blancs remplissent trois fonctions importantes : ils évitent tout risque de choc électrique à l'intérieur du châssis, ils font barrage aux interférences électromagnétiques susceptibles d'altérer le fonctionnement des autres équipements et ils dirigent le flux d'air de refroidissement dans le châssis. Il est vivement recommandé de vérifier que tous les caches et plaques de protection sont en place avant d'utiliser le système.**

Warnung **Unbeschriftete Aufspannplatten (Füllpaneelen) erfüllen drei wichtige Funktionen : sie schützen vor gefährlichen Spannungen und Elektrizität im Innern der Chassis; sie halten elektromagnetische Interferenzen (EMI) zurück, die andere Geräte stören könnten; und sie lenken die Kühlluft durch das Chassis. Nehmen Sie das System nur in Betrieb, wenn alle Karten und Aufspannplatten an vorgesehener Stelle odnungsgemäß installiert sind.**

Avvertenza **Le piastre di protezione (panelli di riempimento) hanno tre funzioni molto importanti:Impediscono di esporvi ai voltaggi e le tensioni elettriche pericolose del chassis; trattengono le interferenze elettromagnetiche (EMI) che possono scombussolare altri apparati; e avviano il flusso d'aria di raffreddamento attraverso il chassis. Non operate il sistema se le schede e i pannelli non sono in posizione.**

Advarsel **Blanke ytterplater (deksler) har tre viktige funksjoner: De forhindrer utsettelse for farlig spenning og strøm inni kabinettet; de inneholder elektromagnetisk forstyrrelse (EMI) som kan avbryte annet utstyr, og de dirigerer luftavkjølingsstrømmen gjennom kabinettet. Betjen ikke systemet med mindre alle kort og ytterplater sitter på plass.**

Aviso **As placas em bruto (painéis de enchimento) desempenham três funções importantes: evitam a exposição a voltagens e correntes perigosas no interior do chassi; protegem de interferências electromagnéticas (IEM) passíveis de afectar outro equipamento; e orientam o fluxo do ar de refrigeração através do chassi. Não pôr o sistema a funcionar sem que todos os cartões e placas estejam no devido lugar.**

¡Advertencia! **Los platos en blanco (paneles de relleno) ofrecen tres funciones importantes: previenen la exposición a voltajes peligrosos y corrientes dentro del chasis; contienen interferencias electromagnéticas (EMI) que pueden interrumpir otros equipos; y dirigen el flujo de aire refrigerante a través del chasis. No opere el sistema a menos que todas las tarjetas y platos estén en su lugar.**

Varning! **Tomma planskivor (fyllnadspaneler) fyller tre viktiga funktioner: de förhindrar utsättning för farliga spänningar och elströmmar inuti chassit; de förhindrar elektromagnetisk störning (EMI) som skulle kunna rubba annan utrustning; samt de riktar flödet av kylluft genom chassit. Använd inte systemet om inte alla kort och planskivor finns på plats.**

Qualified Personnel Warning

Warning **Only trained and qualified personnel should be allowed to install or replace this equipment.**

Waarschuwing **Installatie en reparaties mogen uitsluitend door getraind en bevoegd personeel uitgevoerd worden.**

Varoitus **Ainoastaan koulutettu ja pätevä henkilökunta saa asentaa tai vaihtaa tämän laitteen.**

Avertissement **Tout installation ou remplacement de l'appareil doit être réalisé par du personnel qualifié et compétent.**

Achtung **Gerät nur von geschultem, qualifiziertem Personal installieren oder auswechseln lassen.**

Avvertenza **Solo personale addestrato e qualificato deve essere autorizzato ad installare o sostituire questo apparecchio.**

Advarsel **Kun kvalifisert personell med riktig opplæring bør montere eller bytte ut dette utstyret.**

Aviso **Este equipamento deverá ser instalado ou substituído apenas por pessoal devidamente treinado e qualificado.**

¡Atención! **Estos equipos deben ser instalados y reemplazados exclusivamente por personal técnico adecuadamente preparado y capacitado.**

Varning **Denna utrustning ska endast installeras och bytas ut av utbildad och kvalificerad personal.**