



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 Cisco IOS Server Load Balancing feature module.

- [accounting \(CSG policy\)](#), page B-5
- [accounting \(module CSG\)](#), page B-8
- [activation](#), page B-9
- [agent \(CSG accounting\)](#), page B-10
- [agent activate](#), page B-12
- [agent local-port](#), page B-14
- [alias \(module CSG VLAN\)](#), page B-16
- [aoc confirmation](#), page B-17
- [assign](#), page B-18
- [authorize content](#), page B-19
- [basis](#), page B-20
- [class](#), page B-23
- [clear module csg](#), page B-24
- [clear module csm](#), page B-25
- [client \(CSG content\)](#), page B-27
- [client-group \(CSG policy\)](#), page B-29
- [client-ip \(CSG policy\)](#), page B-31
- [content \(CSG ruleset\)](#), page B-32
- [content \(CSG service\)](#), page B-33
- [copy](#), page B-34
- [database](#), page B-35
- [debug ip csg](#), page B-36
- [entries](#), page B-38 (modified command)
- [entries idle \(CSG billing\)](#), page B-41 (new command)
- [failover](#), page B-43

- flags, page B-44
- ft group (module CSG), page B-47
- gateway (module CSG VLAN), page B-49
- header-map, page B-51
- heartbeat-time, page B-52
- hostname, page B-53
- idle (CSG content), page B-54
- idle (CSG service), page B-56
- inservice (CSG content), page B-58
- ip, page B-59
- ip address (module CSG VLAN), page B-61
- ip csg accounting, page B-62
- ip csg billing, page B-64
- ip csg block, page B-66
- ip csg content, page B-67
- ip csg map, page B-69
- ip csg policy, page B-71
- ip csg refund, page B-73
- ip csg ruleset, page B-74
- ip csg service, page B-75
- ip csg snmp timer, page B-77
- ip csg transport-type, page B-78
- ip csg user-group, page B-80
- ip csg weight, page B-83
- keepalive, page B-84
- match (header map), page B-85
- match (URL map), page B-90
- meter exclude, page B-95 (modified command)
- meter imap, page B-97
- meter increment, page B-99
- meter initial, page B-101
- meter minimum, page B-102
- mode, page B-104
- module csg, page B-106
- next-hop, page B-108
- owner id, page B-110
- owner name, page B-111
- passthrough, page B-112

- [pending](#), page B-113
- [ping](#), page B-114
- [policy \(CSG content\)](#), page B-115
- [priority](#), page B-116
- [quota activate](#), page B-117
- [quota local-port](#), page B-118
- [quota server](#), page B-120
- [radius acct-port](#), page B-122
- [radius ack error](#), page B-123
- [radius endpoint](#), page B-125
- [radius handoff](#), page B-127
- [radius key](#), page B-128
- [radius monitor](#), page B-130
- [radius parse strict](#), page B-132
- [radius pod attribute](#), page B-133 (modified command)
- [radius pod nas](#), page B-135
- [radius pod timeout](#), page B-137
- [radius proxy](#), page B-138
- [radius server](#), page B-141
- [radius start restart session-id](#), page B-143
- [radius stop purge](#), page B-144
- [radius userid](#), page B-145
- [records batch](#), page B-147
- [records format](#), page B-148
- [records granularity](#), page B-149
- [records http-statistics](#), page B-151
- [records intermediate](#), page B-152
- [records max](#), page B-154
- [record-storage](#), page B-156
- [record-storage local-port](#), page B-157
- [redirect](#), page B-158
- [refund-policy](#), page B-160
- [replicate connection tcp](#), page B-161
- [report http header](#), page B-163
- [report radius attribute](#), page B-164 (modified command)
- [report usage](#), page B-166
- [retcode](#), page B-167
- [route \(module CSG VLAN\)](#), page B-169

- [ruleset](#), page B-171
- [service](#), page B-172
- [show](#), page B-173 (modified command)
- [show ip csg accounting](#), page B-175
- [show module csg accounting](#), page B-177
- [show module csg arp](#), page B-181
- [show module csg billing](#), page B-182
- [show module csg clock](#), page B-183
- [show module csg conns](#), page B-184
- [show module csg content](#), page B-186
- [show module csg ft](#), page B-188
- [show module csg stats](#), page B-189
- [show module csg status](#), page B-190
- [show module csg tech-support](#), page B-191
- [show module csg variable](#), page B-197
- [show module csg vlan](#), page B-198
- [snmp-server enable traps csg](#), page B-200
- [table \(module CSG VLAN\)](#), page B-201
- [upgrade](#), page B-202
- [url-map](#), page B-203
- [user-group](#), page B-205
- [user-profile server](#), page B-206
- [variable \(module csg\)](#), page B-208 (modified command)
- [verify](#), page B-216
- [verify confirmation](#), page B-218
- [vlan \(CSG content\)](#), page B-219
- [vlan \(module CSG\)](#), page B-220
- [zero-quota abort type](#), page B-222

accounting (CSG policy)

To define the accounting type and a 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 {ftp | http | imap | other | pop3 | rtsp | smtp | wap {connection-oriented |
connectionless}}] [customer-string string]
```

```
no accounting [type {ftp | http | imap | other | pop3 | rtsp | smtp | wap {connection-oriented |
connectionless}}] [customer-string string]
```

Syntax Description

type ftp	Indicates FTP accounting, with Layer 7 inspection of FTP control sessions.
type http	Indicates HTTP accounting. For HTTPS, use type other for port number 443.
type imap	Enables reporting of Internet Message Access Protocol (IMAP) data records.
type other	Indicates some other type of IP accounting, such as IP, TCP, or User Datagram Protocol (UDP). This is the default setting. For HTTPS, use type other for port number 443.
type pop3	Enables reporting of Post Office Protocol, version 3 (POP3) data records.
type rtsp	Enables reporting of Real Time Streaming Protocol (RTSP) data records.
type smtp	Enables reporting of Simple Mail Transfer Protocol (SMTP) data records.
type wap	Indicates wireless application protocol (WAP) accounting.
connection-oriented	Defines the type of WAP traffic as connection-oriented.
connectionless	Defines the type of WAP traffic as connectionless.
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 on the basis of 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.

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	<i>service-name</i>	Name of the configured accounting service to be downloaded.
---------------------------	---------------------	---

Defaults	None
-----------------	------

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 in service. 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 in service.

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	Activates the Connection Duration service, unless the billing profile indicates that no service is to 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	Activates the Connection Duration service only if the billing profile specifies this service as the connect service. This is the default setting. If you specify the user-profile keyword, the 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 authentication, authorization, and accounting (AAA) Access-Accept, an AAA Accounting-Start, or a Quota Server User-Profile Response.

Defaults

The Connection Duration service is activated only if the billing profile specifies this service as the connect service.

Command Modes

CSG service configuration

Command History

Release	Modification
3.1(3)C5(5)—12.2(17d)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	Configures a content billing service, and enters CSG service configuration mode.

agent (CSG accounting)

To define the active and standby 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 agent** form of this command.

agent *ip-address port-number priority*

no agent *ip-address port-number priority*

Syntax Description

<i>ip-address</i>	IP address of the BMA you wish to define. The CSG differentiates BMAs on the basis of their IP addresses. When you configure a BMA, make sure its IP address matches on both the active CSG and on the standby CSG.
<i>port-number</i>	Port number of the BMA you wish to define. The range is from 1 to 65535. The CSG differentiates BMAs on the basis of their port numbers. When you configure a BMA, make sure its port number matches on both the active CSG and the standby CSG.
<i>priority</i>	Defines active and standby 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 sequential. That is, you can have three agents with priorities 1, 5, and 10. The range of priorities is 1 to 1000.

Defaults

Active and standby BMAs are not defined.

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 only to the 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 an active BMA with priority 1, and a standby 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
agent activate	Enables support for multiple active BMAs.
agent local-port	Defines the port on which the CSG listens for packets from the BMAs.
ip csg accounting	Configures content-based accounting as a service.

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

<i>number</i>	Number of BMAs that the CSG tries to activate at the same time. If you have defined more BMAs than <i>number</i> , and an active BMA fails, the BMA with the highest priority (lowest number) that is not already active is made active. The range is from 1 to 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. Entries that contain a user ID do not age out; they are removed only by RADIUS messages. The range is from 1 to 64000. The default value is 30.

Defaults

The default value for *number* is 1.
The default value for *seconds* is 30.

Command Modes

CSG accounting configuration

Command History

Release	Modification
2.2(3)C2(1)—12.1(13)E	This command was introduced.

Usage Guidelines

Use this command to load-balance CDRs among multiple active BMAs.

When the CSG uses multiple active BMAs, it sends all CDRs for a given user to a particular BMA. The CSG stores that BMA assignment in the CSG User Table entry for that user.

For example, if a configuration has four active BMAs, and one of those BMAs fails, the CSG looks for a suitable standby BMA. If the CSG finds a suitable standby BMA, it transfers all of the CDRs from the failed BMA to the new BMA, and updates all of the affected User Table entries to reflect the new BMA assignment.

However, if the CSG cannot find a suitable standby BMA, it redistributes all of the CDRs from the failed BMA among the remaining three active BMAs. It does so by finding the User Table entries for the affected users in the CDRs. The CSG then assigns one of the active BMAs to each affected user, and updates the User Table entries to reflect the new BMA assignments. The CSG reassigns all CDRs for a given user to the same BMA.

If the CSG cannot find a User Table entry for a user (for example, the user has logged off), it creates a temporary sticky object as a placeholder and assigns a new BMA to the sticky object. This ensures that the remaining CDRs for that user are sent to the same BMA.

**Note**

This command is valid only if your CSG uses multiple active BMAs. If your CSG uses one and only one active BMA, the default settings are sufficient (that is, **agent activate 1 sticky 30**).

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 active and standby 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	Configures content-based accounting as a service.

agent local-port

To define the port on which the CSG will 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 will listen. The range is from 1 to 65535. The default value is 3386, the port number prescribed by general packet radio service (GPRS) tunneling protocol (GTP) prime (GTP'), which is the protocol used for sending accounting records.

The agent local port number cannot be the same as the the quota local port number (configured with the **quota local-port** command in CSG user group configuration mode).

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 not 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 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; instead, the CSG replies 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 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 active and standby BMAs to which to send billing records.
agent activate	Enables support for multiple active BMAs.
ip csg accounting	Configures 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	
<i>ip-address</i>	Alias IP address; a maximum of 256 addresses is allowed.
<i>netmask</i>	Network mask.

Defaults None

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 configure 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 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 VLAN or server VLAN that defines the Layer 2 paths for the CSG accounting service flows, assigns a VLAN ID and an 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	<p><i>token</i></p> <p>A string of up to 15 alphanumeric characters.</p> <p>To insert a question mark (?) in the string, press Ctrl-v and then press the question mark (?) key. To insert a question mark in an editing document, use ASCII code 22. To retain the question mark, use TFTP instead of copy-and-paste.</p>
---------------------------	---

Defaults	None
-----------------	------

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(17d)SXD	Support was added for wireless application protocol (WAP) content authorization URL-rewriting.

Usage Guidelines	<p>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.</p>
-------------------------	--

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	<i>ip-address</i>	IP address.
	<i>value</i>	Transport-type value in the range 1 to 255.

Defaults	None
----------	------

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 the traffic's access path, using the Network Access Server (NAS) IP address reported in the RADIUS Accounting Start message. Use the assign command to associate IP addresses with transport-type values. Transport-type information is reported in fixed record format call detail records (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
	class	Specifies a service class value.
	hostname	Specifies a variable hostname for a CSG module.
	ip csg transport-type	Classifies data traffic on the basis of its access path.
	owner name	Specifies the name of a service owner.
	owner id	Specifies an identifier for a service owner.
	records format	Specifies variable or fixed CDR format.

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 This command has no arguments or keywords.

Defaults None

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 Content Authorization Request to alert the quota server of a new transaction, and allows it to direct the CSG (using Content Authorization Response) 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 Content Authorization Response. 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 Content Authorization Response. 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
	aoc confirmation	Configures a token for use in AoC URL-rewriting.
	ip csg service	Configures a content billing service, and enters CSG service configuration mode.

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.
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.
3.1(3)C5(1)—12.2(17d)SXB	The second keyword was added.
3.1(3)C5(5)—12.2(17d)SXD	The connect keyword was added.

Usage Guidelines

By default the CSG treats MMS traffic like any other wireless application protocol (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 synchronization sequence number (SYN), and one byte representing the first Finish (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 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.

**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 Internet Message Access Protocol (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**.

You cannot configure both **meter exclude svc-idle** and **basis byte** or **basis fixed** in the same service. Only **basis second** is meaningful with **meter exclude svc-idle**.

Examples

The following example shows how to specify fixed billing for the 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	Configures a content billing service, and enters CSG service configuration mode.
meter exclude	Excludes timers from the usage calculation duration billing.

Command	Description
meter imap	Specifies which Internet Message Access Protocol (IMAP) bytes are billed for when doing prepaid debits.
meter increment	Specifies the increments for debiting quota upon completion of a service configured for Service Duration Billing.

class

To specify a service class value, use the **class** command in CSG service configuration mode. To remove the owner ID, use the **no class** form of this command.

class *value*

no class *value*

Syntax Description	<i>value</i>	Specifies a value in the range 1 to 255.
---------------------------	--------------	--

Defaults	None
-----------------	------

Command Modes	CSG service configuration
----------------------	---------------------------

Command History	Release	Modification
	3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.

Usage Guidelines	The class command is used with fixed-record format to identify a service class value. This value is opaque to the CSG and has meaning only for the administrator. It is reported as tariff-class in fixed-record format call detail records (CDRs).
-------------------------	--

Examples	The following example specifies a class value for the service:
-----------------	--

```
ip csg service FOO
class 7
```

Related Commands	Command	Description
	ip csg service	Configures a content billing service, and enters CSG service configuration mode.
	ip csg transport-type mode	Classifies data traffic on the basis of 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		
<i>slot</i>		Indicates the CSG's location in the switch. The range is from 1 through 9.
all		Indicates that the command applies 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		
<i>slot</i>		Indicates the CSG's location in the switch. The range is from 1 through 9.
all		Indicates that the command applies to all CSGs in the switch.
arp-cache <i>ip-address</i>		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.
<i>sticky-group</i>		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.

When the CSG is processing a large number of requests for new pipelined HTTP connections, processing high amounts of RTSP traffic, or clearing a large number of sessions, the message processing levels might exceed the CSG processing capability, entering the **clear module csm arp-cache** command or the **clear module csm connections** command might force the CSG to stop forwarding traffic and reboot.

Examples

The following example clears all connections for all of 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.
<i>ip-address</i>	Client IP address. The default is 0.0.0.0 (all clients).
<i>netmask</i>	(Optional) Client IP network mask. You can express the network mask in either IP dotted notation (<i>n.n.n.n</i>) or prefix notation (<i>/nn</i> , where <i>nn</i> 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 none of the customer-defined policies match.
	The <i>netmask</i> argument is applied to the source IP address of incoming connections. The result must match the <i>ip-address</i> argument; otherwise, the include and exclude settings are not applied to the user packet.
	The include and exclude settings are not applied if the ip csg block command is configured.

If you configure content with a network mask of 255.255.255.255 or /32, then a virtual server is created and the CSG's MAC address is entered as the host address in the CSG Address Resolution Protocol (ARP) cache. Therefore, 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
  pending 300
  replicate connection tcp
  vlan MOVIES_COMEDY
  inservice
```

Related Commands

Command	Description
ip csg content	Configures CSG content, 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

<i>std-access-list-number</i>	Standard IP access list number. The range is from 1 to 99.
<i>std-access-list-name</i>	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 wireless application protocol (WAP) 1.x, URL maps take precedence over access lists.

For WAP 1.x and Real Time Streaming Protocol (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 (CSG policy)

```

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	None				
Command Modes	CSG policy configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>3.1(1)C3(1)—12.2(14)ZA</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	3.1(1)C3(1)—12.2(14)ZA	This command was introduced.
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	<p>The following example shows how to reference a client IP address specification in a CSG policy:</p> <pre>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</pre>				
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>ip csg policy</td> <td>Defines a policy for qualifying flows for the CSG accounting services, and enters CSG policy configuration mode.</td> </tr> </tbody> </table>	Command	Description	ip csg policy	Defines a policy for qualifying flows for the CSG accounting services, and enters CSG policy configuration mode.
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

<i>content-name</i>	Name of a configured content for this ruleset.
---------------------	--

Defaults

None

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 have used multiple **ip csg content** commands to define more than one content name, you can configure more than one **content** command in CSG ruleset configuration mode. Each content must be associated with a different Layer 3 or 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 or 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 configure 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

<i>content-name</i>	Name of the content for this service. The name can be from 1 to 15 characters long, and can include uppercase or lowercase letters (the CSG changes all letters to uppercase), numbers, and any special characters.
policy <i>policy-name</i>	Name of a configured policy to apply to the content for this service.
weight <i>weight-name</i>	(Optional) Name of a configured billing weight.

Defaults

None

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 configure 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	Configures a content billing service, and enters CSG service configuration mode.

copy

To copy the CSG core dump to a file, use the **copy** command on the CSG console.

```
copy core dump {tftp ip-address filename | rcp ip-address filename [rcp-user]}
```

Syntax Description	
core dump tftp <i>ip-address filename</i>	Copies the CSG core dump using TFTP. Use the <i>ip-address</i> argument to specify the IP address of the TFTP server. Use the <i>filename</i> argument to specify the destination filename.
core dump rcp <i>ip-address filename</i>	Copies the CSG core dump using Remote Copy Protocol (RCP). Use the <i>ip-address</i> argument to specify the IP address of the RCP server. Use the <i>filename</i> argument to specify the destination filename.
<i>rcp-user</i>	(Optional) Name used when connecting to the RCP server.

Defaults None

Command Modes CSG console

Command History	Release	Modification
	2.2(1)C(1)	This command was introduced.

Examples The following example uses TFTP server 1.2.3.4 to copy the CSG core dump to file core dump1:

```
CSG> copy core dump 1.2.3.4 core dump1
```

Related Commands	Command	Description
	ping	Determines whether the CSG can reach a remote host.
	show	Displays information about the CSG.
	upgrade	Upgrades the CSG by loading a CSG image from the Supervisor Engine.

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	<i>ip-address</i>	IP address of the server that answers user ID queries.
	<i>port-number</i>	Port number of the server that answers user ID queries. The range is from 1 to 65535.

Defaults	None
----------	------

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 idle 3600
  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 general packet radio service (GPRS) tunneling protocol (GTP) component.
imap	Generates debugging output for the Internet Message Access Protocol (IMAP) component.
module <i>number</i>	Restricts debugging output to only the specified CSG module.
pop3	Generates debugging output for the Post Office Protocol, version 3 (POP3) component.
quota	Generates debugging output for the quota server component.
radius	Generates debugging output for the RADIUS component.
record storage <i>slot</i>	Sets the flag to generate debugging output for the Cisco Persistent Storage Device (PSD) module, and denotes PSD slot number.
rtsp	Generates debugging output for the Real Time Streaming Protocol (RTSP) component.
smtp	Generates debugging output for the Simple Mail Transfer Protocol (SMTP) component.
timer	Generates debugging output for the timer component.
tlv	Generates debugging output for the Tag-Length-Value (TLV) component.
udb	Generates debugging output for the User Database (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 wireless application protocol (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.

To see most but not all debugging output, use the **all** option to turn on all debugging flags, and then use the **no** form of this command to exclude debugging output for any options that are not of interest to you.

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 <i>slot</i> 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(17d)SXD	The imap keyword was added.

Usage Guidelines

Once the debug flags are set, they are automatically sent to the CSG cards when a configuration is downloaded. Similarly, changes in the debug settings are sent to the CSG cards that are being debugged.

You can use the **show debug** command to display the debug flag settings.

All CSG usage information has been consolidated into one number, CSG CPU Utilization (that is, the percent of the CSG CPU that is currently in use), which presents a good overall picture of CSG capacity. To display CSG CPU Utilization, first enable debugging output for the CPU, using the **debug ip csg cpu** command, then enter the **show module csg slot tech-support utilization** command. To calculate the remaining CSG CPU capacity, subtract the CSG CPU Utilization from 100%. So, if the CSG CPU Utilization is 32%, the CSG has 68% CPU capacity remaining.

**Note**

You must re-enter the **debug** command after every reload because it is not saved in the startup configuration.

Examples

The following example shows how to turn on debugging for **rtsp** and **udb** on module 3:

```
debug ip csg module 3
debug ip csg rtsp
debug ip csg udb
```

entries

To define settings for the CSG User Table, use the **entries** command in CSG user group configuration mode. To use the default settings, use the **no** form of this command.

```
entries { idle duration [pod] | max entries-number }
```

```
no entries { idle | max }
```

Syntax Description

idle <i>duration</i>	Number of seconds after which entries for idle users are deleted from the CSG User Table. The range is from 0 (entries never idle out) to 2147483647. The default setting is 0.
pod	(Optional) Specifies whether the CSG is to send the RADIUS Packet of Disconnect message when an entry idles out.
max <i>entries-number</i>	<p>Maximum number of entries allowed in the CSG 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 the user's sessions were all terminated or timed out.</p> <p>The range is from 0 to 4294967295. The default number of entries is 25000. A value of 0 specifies an unlimited number of entries.</p> <p>The actual number of entries in the User Table depends on several variables, including the traffic model being used and the number of RADIUS attributes reported. Even if you set <i>entries-number</i> to a very large number, such as 300000, the CSG might never store that many entries in the User Table.</p>

Defaults

The default idle duration is 0 seconds, and the CSG does not send the RADIUS Packet of Disconnect message when an entry idles out.

The default maximum 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.
3.1(3)C7(1)—12.2(18)SXF1 or 12.2(18)SRA	The idle and pod keywords and <i>duration</i> argument were added.

Usage Guidelines

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

When setting the entry idle timer, keep the following considerations in mind:

- You can set the entry idle timer in either the user group or the billing plan. If you do not set the timer in the billing plan, the CSG uses the timer set in the user group. That is, if there is an entry idle timer value in the billing plan, it is used; otherwise, if there is a global entry idle timer value configured, it is used.
- If set, the idle timer starts when there are no billable sessions, and restarts whenever a RADIUS Accounting Start or an Interim Accounting message is received. The timer stops when a billable session is started.
- If you do not specify the **pod** keyword, the CSG deletes the idle entry when the timer expires.
- If you specify the **pod** keyword, and if RADIUS Packet of Disconnect (PoD) is configured for the CSG, the CSG sends a PoD message when the idle timer expires. The CSG deletes the idle entry when the PoD message is ACKed, NAKed, or when all retries have been sent.
- The idle timer enables the CSG to eliminate an idle User Table entry if the Network Access Server (NAS) fails to deliver a RADIUS Accounting Stop request for an idle user. Eliminating idle entries from the User Table frees up CSG resources.
- If Connection Duration Billing is enabled, you can use either the billing plan entry idle timer or the user group entry idle timer to release a user connection.

Examples

The following example shows how to specify an entry idle time of 1 hour and a maximum of 100,000 cache entries for CSG user group G1:

```
ip csg user-group G1
  entries idle 3600
  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.
entries idle (CSG billing)	Sets the time after which entries for idle users are deleted from the CSG User Table.
ip csg user-group	Creates a group of users for which you want to generate accounting records, and enters CSG user group configuration mode.
radius key	Specifies the CSG to be the RADIUS endpoint for accounting records, and specifies the secret key.
radius pod attribute	Specifies the RADIUS attributes to be copied from the RADIUS Start message and sent to the NAS in the PoD message.

Command	Description
radius pod nas	Specifies the NAS port to which the CSG is to send the PoD message, and the key to use in calculating the Authenticator.
radius pod timeout	Specifies the number of times to retry the RADIUS PoD message if it is not acknowledged by means of an ACK message, and the interval between retransmissions.
radius proxy	Specifies that the CSG is to be a proxy for RADIUS messages.

entries idle (CSG billing)

To set the time after which entries for idle users are deleted from the CSG User Table, use the **entries idle** command in CSG billing configuration mode. To use the default settings, use the **no** form of this command.

```
entries idle duration [pod]
```

```
no entries idle
```

Syntax Description

idle duration	Number of seconds after which entries for idle users are deleted from the CSG User Table. The range is from 0 (entries never idle out) to 2147483647. The default setting is 0.
pod	(Optional) Specifies whether the CSG is to send the RADIUS Packet of Disconnect message when an entry idles out.

Defaults

The default idle duration is 0 seconds, and the CSG does not send the RADIUS Packet of Disconnect message when an entry idles out.

Command Modes

CSG billing configuration

Command History

Release	Modification
3.1(3)C7(1)—12.2(18)SXF1 or 12.2(18)SRA	This command was introduced.

Usage Guidelines

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

When setting the entry idle timer, keep the following considerations in mind:

- You can set the entry idle timer in either the user group or the billing plan. If you do not set the timer in the billing plan, the CSG uses the timer set in the user group. That is, if there is an entry idle timer value in the billing plan, it is used; otherwise, if there is a global entry idle timer value configured, it is used.
- If set, the idle timer starts when there are no billable sessions, and restarts whenever a RADIUS Accounting Start or an Interim Accounting message is received. The timer stops when a billable session is started.
- If you do not specify the **pod** keyword, the CSG deletes the idle entry when the timer expires.
- If you specify the **pod** keyword, and if RADIUS Packet of Disconnect (PoD) is configured for the CSG, the CSG sends a PoD message when the idle timer expires. The CSG deletes the idle entry when the PoD message is ACKed, NAKed, or when all retries have been sent.
- If Connection Duration Billing is enabled, you can use either the billing plan entry idle timer or the user group entry idle timer to release a user connection.

Examples

The following example shows how to specify an entry idle time of 1 hour for CSG billing plan REGULAR:

```
ip csg billing REGULAR
  entries idle 3600
  mode postpaid
  service MOVIES
  service BROWSING
```

Related Commands

Command	Description
entries	Defines settings for the CSG User Table.
ip csg billing	Defines a billing plan, and enters CSG billing configuration mode.
mode	Specifies that a billing plan is postpaid or prepaid.
radius pod attribute	Specifies the RADIUS attributes to be copied from the RADIUS Start message and sent to the NAS in the PoD message.
radius pod nas	Specifies the NAS port to which the CSG is to send the PoD message, and the key to use in calculating the Authenticator.
radius pod timeout	Specifies the number of times to retry the RADIUS PoD message if it is not acknowledged by means of an ACK message, and the interval between retransmissions.
radius proxy	Specifies that the CSG is to be a proxy for RADIUS messages.
service	Associates a service with a CSG billing plan.

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	<i>failover-time</i>	Amount of time, in seconds, that the CSG must wait after receiving the last heartbeat message before the CSG assumes that the other CSG is not operating. The range is from 1 to 65535. The default value is 3.
---------------------------	----------------------	---

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 wireless application protocol (WAP) flag bit masks and values for CSG Prepaid Error Reimbursement, 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.
<i>mask</i>	The <i>mask</i> for an ip or tcp flag must match that reported to the Billing Mediation Agent (BMA) for connection termination. The range for <i>mask</i> is from 0x01 to 0xFF.
<i>value</i>	The <i>value</i> for an ip , tcp , or wap flag, which must match that reported to the BMA for connection termination. <ul style="list-style-type: none"> For an ip or tcp flag, the range for <i>value</i> is from 0x00 to 0xFF. For a wap flag, <i>value</i> can be 0x00, 0x01, 0x02, or 0x04.

Defaults

None

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(17d)SXD	Combined the flags and flags wap commands.

Usage Guidelines

The CSG supports flag-based refunding for all protocols.

The **ip** flag *values* are:

- 0x01: Connection initiator.
 - 0: The connection was initiated by the subscriber. The source address is associated with the user ID.
 - 1: The connection was initiated by the network. The destination address is associated with the user ID.
- 0x80: Connection terminated because of lack of authorization failure.
 - 0: The connection was not terminated as a result of an authorization failure.
 - 1: The connection was terminated as a result of an authorization failure.

- 0x7E: Reserved.

The **tcp** flag *values* are:

- 0x01: Connection initiator.
 - 0: The connection was initiated by the subscriber. The source address is associated with the user ID.
 - 1: The connection was initiated by the network. The destination address is associated with the user ID.
- 0x02: TCP termination type.
 - 0: Normal TCP termination (FIN or RST).
 - 1: Connection timed out.
- 0x04: Persistent Connection (multiple sequential transactions per TCP connection).
 - 0: The reported connection is not a persistent connection.
 - 1: The reported connection is a persistent connection.
- 0x08: Destination Initiated Close (valid only if TCP termination type is 0).
 - 0: The connection teardown was initiated by the source IP in the flow.
 - 1: The connection teardown was initiated by the destination IP in the flow.
- 0x10: Destination Side FIN (valid only if TCP termination type is 0).
 - 0: The destination side never sent a FIN (it might have sent an RST).
 - 1: The destination side sent a FIN.
- 0x20: Source Side FIN (valid only if TCP termination type is 0).
 - 0: The source side never sent a FIN (it might have sent an RST).
 - 1: The source side sent a FIN.
- 0x40: Connection not closed (valid only for HTTP 1.1).
 - 0: The connection has been closed.
 - 1: The connection is not closed yet, and TCP close bits have no meaning.
- 0x80: Connection terminated because of lack of authorization failure.
 - 0: The connection was not terminated as a result of an authorization failure.
 - 1: The connection was terminated as a result of an authorization failure.

The **wap** flag *values* are:

- 0x00: Normal.
- 0x01: Aborted.
- 0x02: Incomplete.
- 0x04: Forced abort.

Examples

The following example shows how to set flags for IP, TCP, and WAP:

```
ip csg refund COMPANY-REFUND
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 to apply to the various services, and enters CSG refund configuration mode.
retcode	Specifies the range of application return codes for which the CSG refunds quota for Prepaid Error Reimbursement.

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		
<i>group-id</i>		ID of the fault-tolerant group. Both CSGs must have the same group ID. The range is from 1 to 254.
vlan <i>vlan-id</i>		VLAN, identified by its VLAN ID, over which heartbeat messages are to be sent. Both CSGs must have the same VLAN ID. The range is from 2 to 4095.

Defaults	
None	

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 comprises 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
```

■ ft group (module CSG)

```
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	<i>ip-address</i>	IP address of the client-side gateway.
--------------------	-------------------	--

Defaults	None
----------	------

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 VLAN or server VLAN that defines the Layer 2 paths for the CSG accounting service flows, assigns a VLAN ID and an 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	<i>header-map-name</i> Name of a header map, as configured with an ip csg map command.
---------------------------	---

Defaults	None
-----------------	------

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	<i>heartbeat-time</i>	Time interval between heartbeat transmissions, in seconds. The range is from 1 to 65535. The default value is 1.
---------------------------	-----------------------	--

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	<i>name</i>	1- to 20-character hostname for the CSG module.
--------------------	-------------	---

Defaults	None
----------	------

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 on the basis of 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

<i>duration</i>	Content idle timer duration in seconds. If there are no flows on a content connection for more than <i>duration</i> seconds, the CSG assumes the connection is idle and ends the connection. The range is from 4 to 65535. The default is 3600.
-----------------	--

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

Real Time Streaming Protocol (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 call detail record (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 content idle 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. (For RTSP, do not set the timer to less than 60 seconds.)
- 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. User Datagram Protocol (UDP) does not have an end-of-session indicator and simply idles out. For that reason, for UDP and wireless application protocol (WAP) 1.x, setting the content idle timer to a low value (for example, 30) allows the CSG to quickly recognize that a session has ended and to 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.

For a service configured with **basis second**, make sure the idle timeout value for the content configuration, set using the **idle** command in CSG content configuration mode, does not exceed the service idle timeout value, set using the **idle** command in CSG service configuration mode. Examples of these contents include:

- Non-TCP contents
- TCP contents with policies for HTTP or WAP2 where the client or server does not close the TCP connection at the end of the transaction

Content that is configured with **ip any** requires two upstream packets to trigger the **idle (CSG content)** timer. Therefore, if content is configured with **ip any** and the CSG receives only one upstream packet (as for a UDP session), the content timer is never triggered, and downstream traffic matches the **ip any** content connection entry until the timer expires. After the timer expires, the CSG treats all downstream traffic as server-initiated traffic and might block the traffic in certain configurations. To avoid this problem, configure a new content to match UDP traffic (**ip any udp**), referencing the same policy referenced by the **ip any** content.

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
pending 300
replicate connection tcp
vlan MOVIES_COMEDY
inservice
```

Related Commands

Command	Description
ip csg content	Configures CSG content, 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

<i>duration</i>	Service idle timer duration, in seconds. The timer begins when there are no sessions. If a user's quota for a service is unused for more than <i>duration</i> seconds, the CSG assumes that the service is idle and sends a Service Stop to free up the resources. The range is from 10 to 65535. The default is 300.
-----------------	--

Defaults

The default idle duration is 300 seconds (5 minutes).

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 services configured with **basis second**, make sure the idle timeout value for the content configurations, set using the **idle** command in CSG content configuration mode, does not exceed the service idle timeout value, set using the **idle** command in CSG service configuration mode. Examples of these contents include:

- Non-TCP contents
- TCP contents with policies for HTTP or wireless application protocol (WAP) 2.x where the client or server does not close the TCP connection at the end of the transaction

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	Configures 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
pending 300
replicate connection tcp
vlan MOVIES_COMEDY
inservice
```

Related Commands	Command	Description
	ip csg content	Configures CSG content, and enters CSG accounting configuration mode.

ip

To define the subset of Layer 3 and Layer 4 flows that can be processed by the CSG accounting services, use the **ip** command in CSG content configuration mode. To delete the flow definition, use the **no** form of this command.

```
ip {any | ip-address [netmask]} [any | protocol [port-number [last-port-number]]]
```

```
no ip {any | ip-address}
```

Syntax Description

any	All Layer 3 and Layer 4 flows can be processed. This is the default setting.
<i>ip-address</i>	IP address for which Layer 3 and Layer 4 flows can be processed.
<i>netmask</i>	Mask that identifies the network from which Layer 3 and Layer 4 flows can be processed. You can express the network mask in either IP dotted notation (<i>n.n.n.n</i>) or prefix notation (<i>/nn</i> , where <i>nn</i> is the number of leading 1-bits). For example, 255.255.0.0 and /16 are equivalent network masks. The default network mask is 255.255.255.255 or /32, which means flows to a specific host can be processed.
any	All protocol types of Layer 3 and Layer 4 flows can be processed. This is the default setting.
<i>protocol</i>	Protocol type of Layer 3 and Layer 4 flows that can be processed: <ul style="list-style-type: none"> any—Flows of any protocol type can be processed. This is the default setting. tcp—Only TCP flows can be processed. udp—Only User Datagram Protocol (UDP) flows can be processed. <i>protocol-number</i>—Number identifying the protocol whose flows can be processed. The range is from 0 to 255, where 0 means the same as any.
<i>port-number</i>	Port number from which Layer 3 and Layer 4 flows can be processed, or first port number in a contiguous range. The range is from 0 to 65535, where 0 indicates that flows from any port number can be processed.
<i>last-port-number</i>	Last port number in a contiguous range. The range is from <i>port-number</i> to 65535.

Defaults

If you specify an IP address but no network mask, the default network mask is 255.255.255.255 or /32 (flows to a specific host can be processed).

If you do not specify a protocol, flows of any protocol type can be processed.

If you specify a protocol but no port number, the default port number is 0, which means that flows from any port number can be processed.

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 Wireless Session Protocol (WSP) and Wireless Transaction Protocol (WTP) wireless application protocol (WAP) ports. When a policy with **accounting type wap** is associated with a content, use even-numbered UDP ports to designate WSP traffic, and use odd-numbered ports to designate WTP traffic.

Although you can use this command to specify a port number for Layer 3 content (**ip any any port-number**), the 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.

Content that is configured with **ip any** requires two upstream packets to trigger the **idle (CSG content)** timer. Therefore, if content is configured with **ip any** and the CSG receives only one upstream packet (as for a UDP session), the content timer is never triggered, and downstream traffic matches the **ip any** content connection entry until the timer expires. After the timer expires, the CSG treats all downstream traffic as server-initiated traffic and might block the traffic in certain configurations. To avoid this problem, configure a new content to match UDP traffic (**ip any udp**), referencing the same policy referenced by the **ip any** content.

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
  pending 300
  replicate connection tcp
  vlan MOVIES_COMEDY
  inservice
```

Related Commands

Command	Description
ip csg content	Configures CSG content, 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		
	<i>ip-address</i>	IP address for the CSG; only one management IP address is allowed per VLAN.
	<i>netmask</i>	Network mask.

Defaults None

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 VLANs 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 VLAN or server VLAN that defines the Layer 2 paths for the CSG accounting service flows, assigns a VLAN ID and an optional name, and enters module CSG VLAN configuration mode.

ip csg accounting

To configure 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 accounting service, use the **no** form of this command.

ip csg accounting *service-name*

no ip csg accounting *service-name*

Syntax Description

<i>service-name</i>	Name of the accounting service. The name can be from 1 to 15 characters long, and can include uppercase or lowercase letters (the CSG changes all letters to uppercase), numbers, and any special characters.
---------------------	---

Defaults

None

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 that will be used to test the health of BMAs and quota servers.
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.
user-group	Associates a user group with a specific accounting service.

ip csg billing

To define a billing plan, 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 from 1 to 64 characters long, and can include uppercase or lowercase letters (the CSG changes all letters to uppercase), numbers, and any special characters.

Defaults

None

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:

- [entries idle \(CSG billing\)](#)
- [mode](#)
- [service](#)

Examples

The following example shows how to define a CSG billing plan named REGULAR:

```
ip csg billing REGULAR
  entries idle 3600
  mode postpaid
  service MOVIES
  service BROWSING
```


Related Commands	Command	Description
	entries idle (CSG billing)	Sets the time after which entries for idle users are deleted from the CSG User Table.
	mode	Specifies that a billing plan is postpaid or prepaid.
	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 This command has no arguments or keywords.

Defaults None

Command Modes Global configuration

Command History

Release	Modification
3.1(3)C5(5)—12.2(17d)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 configure CSG content, and to enter CSG content configuration mode, use the **ip csg content** command in global configuration mode. To delete the content configuration, use the **no** form of this command.

ip csg content *content-name*

no ip csg content *content-name*

Syntax Description	<i>content-name</i>	Name of the content. The name can be from 1 to 15 characters long, and can include uppercase or lowercase letters (the CSG changes all letters to uppercase), numbers, and any special characters.
---------------------------	---------------------	--

Defaults	None
-----------------	------

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 configuration 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 configuration 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. For example, if one of the policies is configured with **accounting type wap**, the policies 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
  pending 300
  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 subset of Layer 3 and Layer 4 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 standby 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

<i>map-name</i>	Name of the map. The name can be from 1 to 15 characters long, and can include 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

None

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	<i>policy-name</i>	Name of a policy that applies to the content for this service. The name can be from 1 to 15 characters long, and can include uppercase or lowercase letters (the CSG changes all letters to uppercase), numbers, and any special characters.				
Defaults	None					
Command Modes	Global configuration					
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Release</th> <th style="text-align: left;">Modification</th> </tr> </thead> <tbody> <tr> <td>3.1(1)C3(1)—12.2(14)ZA</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	3.1(1)C3(1)—12.2(14)ZA	This command was introduced.	
Release	Modification					
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.					

Usage Guidelines Because of limitations on the number of URL match patterns that the CSG can handle, do not define more than 16,000 policies. For more information on URL match patterns, see the description of the **match (URL map)** command.

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 a 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.
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 refund

To specify the refund policy to apply 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	<i>refund-policy-name</i> Name of a policy that applies to the content for this service.
---------------------------	--

Defaults	None
-----------------	------

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**—The CSG supports flag-based refunding for all protocols.
- **retcode**—The CSG supports return code-based refunding for all protocols except RTSP.

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 wireless application protocol (WAP) flag bit masks and values for CSG Prepaid Error Reimbursement.
retcode	Specifies the range of application return codes for which the CSG refunds quota for Prepaid Error Reimbursement.	

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	<i>ruleset-name</i>	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 from 1 to 15 characters long, and can include uppercase or lowercase letters (the CSG changes all letters to uppercase), numbers, and any special characters.
---------------------------	---------------------	--

Defaults	None
-----------------	------

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 configure 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 content billing service, use the **no** form of this command.

ip csg service *service-name*

no ip csg service *service-name*

Syntax Description

<i>service-name</i>	Name of the content billing service, which is a component of a billing plan that is subscribed to by users. The name can be from 1 to 15 characters long, and can include uppercase or lowercase letters (the CSG changes all letters to uppercase), numbers, and any special characters.
---------------------	--

Defaults

None

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 1024 services. You can authorize, for each user, any number of services from that pool, but we recommend that the billing system not authorize more than 10 active services for each user. Exceeding this guideline could lead to the following problems:

- The increase in the number of quota authorizations per user can overload both the quota server and 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 because of 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](#)

- [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)	Configures 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 Simple Network Management Protocol (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.
<i>interval</i>	Interval, in seconds, of the CSG SNMP timer. The range is from 1 to 2,147,483,647. The default setting is 60.

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 on the basis of 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 ip csg transport-type

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Global configuration

Command History	Release	Modification
	3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.

Usage Guidelines Use the **ip csg transport-type** command to classify data traffic on the basis of its access path, using the Network Access Server (NAS) IP address reported in the RADIUS Accounting Start message. Use the **assign** command to associate IP addresses with transport-type values. Transport-type information is reported in fixed record format call detail records (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
	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.
	owner name	Specifies the name of a service owner.
	owner id	Specifies an identifier for a service owner.

Command	Description
assign	Associates an IPv4 address with a transport-type value.
class	Specifies a service class value.
mode	Specifies that a billing plan is postpaid or prepaid.
records format	Specifies variable or fixed CDR format.

ip csg user-group

To create a group of 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

<i>group-name</i>	Name of the group that you want to create. The name can be from 1 to 15 characters long, and can include uppercase or lowercase letters (the CSG changes all letters to uppercase), numbers, and any special characters.
-------------------	--

Defaults

None

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](#)
- [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 idle 3600
  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
aoc confirmation	Configures a token for use in AoC URL-rewriting.
database	Server that answers user ID queries.
entries	Defines settings for the CSG User Table.
quota activate	Simultaneously activates multiple quota servers, and assigns a quota server to each user.
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 not the established RADIUS default of 1813.
radius ack error	Enables the CSG to generate a RADIUS response to an RADIUS Accounting Start Request or a RADIUS Accounting Interim Request when it encounters an error condition.
radius handoff	Configures RADIUS handoff support.
radius key	Specifies that the CSG is the RADIUS Accounting server to obtain user ID accounting records.

Command	Description
aoc confirmation	Configures a token for use in AoC URL-rewriting.
radius monitor	Specifies that the CSG is to monitor the RADIUS flows to the specified server.
radius parse strict	Tightens the parsing rules for RADIUS flows.
radius pod attribute	Specifies the RADIUS attributes and VSA subattributes to be copied from the RADIUS Start message and sent to the Network Access Server (NAS) in the Packet of Disconnect (PoD) message.
radius pod nas	Specifies the Network Access Server (NAS) port to which the CSG is to 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 acknowledged by means of an ACK message, and the interval between retransmissions.
radius proxy	Enables RADIUS proxy.
radius server	Configures a RADIUS server.
radius start restart session-id	Deletes an existing CSG User Table entry for a specific user, and creates a new entry for that user.
radius stop purge	Specifies the attribute that must be included in the RADIUS Accounting Stop request in order for the User Table entry to be deleted.
radius userid	Specifies the RADIUS attribute used to extract the user identifier from a RADIUS record.
redirect	Redirects client flows to an alternate IP address when the client's quota is exhausted.
user-profile server	Specifies which server is used to obtain the user profile (or billing plan).
verify confirmation	Configures a token for use in service verification URL-rewriting.

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

<i>weight-name</i>	Name of the billing weight. The name can be from 1 to 15 characters long, and can include uppercase or lowercase letters (the CSG changes all letters to uppercase), numbers, and any special characters.
<i>weight-value</i>	Weight multiplier to apply to each billable object that uses this billing weight. The range is from -32768 to +32767. The default billing weight multiplier is 1. A value of 0 means that the associated content is free.

Defaults

The default billing weight multiplier is 1.

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 update only a single definition for each weight. The results are 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 that will be 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	<i>number-of-seconds</i>	Time, in seconds, that is used to determine the health of BMAs and quota servers. The range is 1 to 86,400. The default value is 60.
---------------------------	--------------------------	--

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 active and standby BMAs to which billing records are to be sent.

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 <i>protocol</i>	Default application protocol: http —This is the only supported application protocol, and it is the default setting.
header <i>header-name</i>	Header field that is to be matched against the input header. The <i>header-name</i> 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.
<i>pattern</i>	(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 another map associated with this policy matches 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 and describes 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.
<code>\character</code>	Escaped character. Examples: <code>\?</code> Match on a question mark (<code>\<ctrl-v>?</code>) <code>\+</code> Match on a plus sign <code>*</code> Match on an asterisk <code>\a</code> Alert (ASCII 7) <code>\b</code> Backspace (ASCII 8) <code>\f</code> Form-feed (ASCII 12) <code>\n</code> New line (ASCII 10) <code>\r</code> Carriage return (ASCII 13) <code>\t</code> Tab (ASCII 9) <code>\v</code> Vertical tab (ASCC 11) <code>\0</code> Null (ASCII 0) <code>\\</code> 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.
<code>.\x##</code>	Any ASCII character as specified in two-digit hex notation. For example, <code>\x3f</code> 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 <i>protocol</i>	Default application protocol:	http —This is the only supported application protocol, and it is the default setting.
method <i>method</i>	Method to be matched. Valid methods are:	<ul style="list-style-type: none"> • 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 <i>pattern</i>	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 use more than one **match** command in CSG URL map configuration mode to specify multiple URL match expressions for a 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 another map associated with this policy matches 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 uppercase and lowercase combinations carefully when you create URL match expressions.

- When you configure URL match patterns for Real Time Streaming Protocol (RTSP) streams, be sure to account for trailing stream IDs in RTSP stream names. For example, URL match pattern ***.mpeg** does not match **rtsp://1.1.1.254:554/movie.mpeg/streamid=0** because the stream name has a trailing **/streamid=0**. To match such RTSP stream names, use a URL match pattern such as ***.mpeg***.
- Depending on your configuration, the CSG can handle up to 1000 single-wildcard URL match patterns (such as ***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, observe the following guidelines to optimize the performance of the CSG:
 - Minimize the number of URL match patterns that are applied to a CSG content configuration.
 - Minimize the number of keyword URL match patterns that you use. In general, it is better to use multiple single-wildcard URL match patterns instead of individual keyword URL match patterns.
 - Combine several keyword URL match patterns into a single pattern by using UNIX string-matching special characters. For example, ***.movies_comedy.com/*.mpeg**, ***.movies_action.com/*.mpeg**, and ***.movies_drama.com/*.mpeg** can be combined into the following single pattern:


```
*.movies_(comedy|action|drama).com/*.mpeg
```

 And these patterns


```
*.movies_comedy.com/*.mpeg
*.movies_action.com/*.mpeg
*.movies_drama.com/*.mpeg
*.clips_comedy.com/*.mpeg
*.clips_action.com/*.mpeg
*.clips_drama.com/*.mpeg
```

 can be combined into the following single pattern:


```
*(.movies|clips)*?*(comedy|action|drama).com/*.mpeg
```
 - Do not forget that the entire pattern, including wildcards and UNIX string-matching special characters, cannot exceed 128 characters.
- When you add or change URL match patterns, check their effect on the CSG memory:
 1. To check the status of the configuration change, enter the **show module csg status** command in privileged EXEC mode.
 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 both the total memory used and the total memory available.
- For wireless application protocol (WAP) 1.x, URL maps take precedence over access lists.
- For WAP 1.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 and describes 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.
<i>\character</i>	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

To exclude timers from the usage calculation duration billing, use the **meter exclude** command in CSG service configuration mode. To return to the default behavior, use the **no** form of the command.

```
meter exclude {pause rtsp | svc-idle}
```

```
no meter exclude {pause rtsp | svc-idle}
```

Syntax

Keyword	Description
pause rtsp	Excludes the Real Time Streaming Protocol (RTSP) PAUSE time from the duration billing calculation when RTSP session is used.
svc-idle	Excludes the final service idle from the usage calculation when the service is configured for Service Duration Billing.

Defaults

The default behavior is to include the RTSP PAUSE time and the service-idle in the usage calculation.

Command Modes

CSG service configuration

Command History

Release	Modification
3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.
3.1(3)C7(1)—12.2(18)SXF1 or 12.2(18)SRA	The pause rtsp keyword was added, and the service-idle keyword was changed to svc-idle .

Usage Guidelines

Configuration of this command with the **svc-idle** keyword specified can result in reduced charging because the next service access occurs after the service idles, rather than occurring before the service idles.

Examples

The following example shows how to exclude the RTSP PAUSE time from the duration billing calculation for the SERVICE-A service:

```
ip csg service SERVICE-A
  basis second
  meter exclude pause rtsp
  content RTSP policy RTSP-POLICY
```

The following example shows how to exclude the final service idle from the usage calculation for the OFF_NET service:

```
ip csg service OFF_NET
  meter exclude svc-idle
```

Related Commands	Command	Description
	basis	Specifies the billing basis for a CSG content billing service.
	ip csg content	Configures CSG content, and enters CSG content configuration mod.
	ip csg service	Configures a content billing service, and enters CSG service configuration mode.
	policy (CSG content)	References a CSG billing policy.

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

Syntax	Description
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

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 range is from 1 to 65535. The default value is 1.

Note The value for quadrans is always denoted as seconds.

Defaults

The default increment is 1 second.

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; however, the CSG does round up, say, 163 seconds of network usage to 180 quadrans before it calculates total usage for reporting in the Service Stop.



Note

The rounding-up of network usage is not reflected in calculations for the Usage Tag-Length-Value (TLV) in Service Reauthorization Requests.

The increment value is considered when determining whether sufficient quota exists for granting network access for a session. For instance, if the increment is 60, the network usage is 50, and the balance is 10, network access is permitted. However, if the increment is 60, the network usage is 70, and the balance is 10, network access is not permitted because the balance is not sufficient to satisfy the entire increment (that is, a minimum of 1 minute of quota would be required to allow access for a portion of the minute).

Examples

The following example shows how to configure quota debit increments for Service Duration Billing for the OFF_NET service.

```
ip csg service OFF_NET
basis second
meter minimum 60
meter increment 100
content ANY policy HTTP
content ANY policy ANY
```

Related Commands

Command	Description
ip csg service	Configures 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

<i>value</i>	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 that has been mapped to the service. The initial value is not rounded up to the nearest increment value. The range is from 0 to 65535. The default value is 0.
--------------	---

Defaults

The default quota is 0 quadrans.

Command Modes

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 setup 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	Configures 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

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 range is from 0 to 65535. The default value is 0.

Defaults

The default number is 0 quadrans.

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, 150 seconds of network usage is not rounded up for the purpose of calculating usage in the Service Stop, but, for example, 63 seconds of network usage is rounded up to 90 quadrans.



Note The rounding-up of network usage is not reflected in calculations for the Usage Tag-Length-Value (TLV) in Service Reauthorization Requests.

Examples

The following example shows how to configure **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	Configures 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 use 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 mode 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 call detail records (CDRs) was added.

Usage Guidelines

The **mode** command with the **postpaid** keyword is used with both fixed-record format and variable-record format to enable service correlation of postpaid CDRs.

Examples

The following example specifies postpaid mode for CSG billing plan REGULAR

```
ip csg billing REGULAR
  entries idle 3600
  mode postpaid
  service MOVIES
  service BROWSING
```

Related Commands

Command	Description
assign	Associates an IP address with a transport-type value.
class	Specifies a service class value.
entries idle (CSG billing)	Sets the time after which entries for idle users are deleted from the CSG User Table.
hostname	Specifies a variable hostname for a CSG module.
ip csg billing	Defines a billing plan, and enters CSG billing configuration mode.
ip csg transport-type	Classifies data traffic on the basis of its access path.

Command	Description
owner id	Specifies an identifier for a service owner.
owner name	Specifies the name of a service owner.
records format	Specifies variable or fixed call detail record (CDR) format.
service	Associates a service with a CSG billing plan.

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 in which the CSG resides.

Defaults

None

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 configured by a ruleset to a CSG card.
	vlan (module CSG)	Creates a client VLAN or server VLAN that defines the Layer 2 paths for the CSG accounting service flows, assigns a VLAN ID and an 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 delete the next-hop IP address, use the **no** form of this command.

next-hop *ip-address*

no next-hop *ip-address*

Syntax Description	<i>ip-address</i>	IP address of the next hop.
Defaults	None	
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 configuration, the CSG determines the next-hop on the basis of 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 Wireless Session Protocol (WSP) connection request.

**Note**

Even if you have defined a next-hop IP address, traffic that matches the “default” policy of a content might not be routed with next-hop.

Examples

The following example specifies a 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	<i>id</i>	1- to 15-character string that identifies a service owner.
---------------------------	-----------	--

Defaults	None
-----------------	------

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	Configures a content billing service, and enters CSG service configuration mode.
	ip csg transport-type	Classifies data traffic on the basis of 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	<i>name</i>	1- to 38-character string that specifies the name of the service.
--------------------	-------------	---

Defaults	None
----------	------

Command Modes	CSG service configuration
---------------	---------------------------

Command History	Release	Modification
	3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.

Usage Guidelines	The owner name command 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	Configures a content billing service, and enters CSG service configuration mode.
	ip csg transport-type	Classifies data traffic on the basis of 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	<i>quota-grant</i> Size of each quota grant to give to the service. The <i>quota-grant</i> is also called the default quota. The range is from 1 to 2147483647.				
Defaults	None				
Command Modes	CSG service configuration				
Command History	<table border="1"> <thead> <tr> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Release</th> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border-bottom: 1px solid black;">3.1(3)C5(5)—12.2(17d)SXD</td> <td style="border-bottom: 1px solid black;">This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	3.1(3)C5(5)—12.2(17d)SXD	This command was introduced.
Release	Modification				
3.1(3)C5(5)—12.2(17d)SXD	This command was introduced.				
Usage Guidelines	<p>Use this command to enable the CSG to grant quota to the service when when at least one quota server is configured, but none are active.</p> <p>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 the no quota server reassign command in CSG user group configuration mode for user groups associated with the service.</p>				
Examples	<p>The following example specifies that the CSG grants 65535 quadrans of quota to the service NAME each time the service runs low on quota:</p> <pre>ip csg service NAME passthrough 65535</pre>				
Related Commands	<table border="1"> <thead> <tr> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Command</th> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Description</th> </tr> </thead> <tbody> <tr> <td style="border-bottom: 1px solid black;">ip csg service</td> <td style="border-bottom: 1px solid black;">Configures a content billing service, and enters CSG service configuration mode.</td> </tr> </tbody> </table>	Command	Description	ip csg service	Configures a content billing service, and enters CSG service configuration mode.
Command	Description				
ip csg service	Configures 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	<i>timeout</i>	Time, in seconds, for the pending connection timeout, which is the time to wait before a connection is considered unreachable. The range is from 4 to 65535. The default value is 30.
---------------------------	----------------	---

Defaults The default pending connection 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 connection timer:

```
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
  pending 300
  replicate connection tcp
  vlan MOVIES_COMEDY
  inservice
```

Related Commands	Command	Description
	ip csg content	Configures CSG content, and enters CSG accounting configuration mode.
	show module csg content	Displays statistics and counters for the CSG content.

ping

To determine whether the CSG can reach a remote host, use the **ping** command on the CSG console.

ping *ip-address*

Syntax Description	<i>ip-address</i>	IP address of the remote host.
---------------------------	-------------------	--------------------------------

Defaults	None
-----------------	------

Command Modes	CSG console
----------------------	-------------

Command History	Release	Modification
	2.2(1)C(1)	This command was introduced.

Examples The following example pings the remote host at IP address 1.2.3.4:

```
CSG> ping 1.2.3.4
```

Related Commands	Command	Description
	copy	Copies the CSG core dump.
	show	Displays information about the CSG.
	upgrade	Upgrades the CSG by loading a CSG image from the Supervisor Engine.

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	
<i>policy-name</i>	Name of a configured CSG billing policy.

Defaults	None
----------	------

Command Modes	CSG content configuration
---------------	---------------------------

Command History	Release	Modification
	3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines	<p>If accounting records are to be generated for flows matching this policy, you must configure the accounting command. If you do not want to bill for flows matching this policy, do not configure the accounting command.</p> <p>To reference more than one policy in a content configuration, use multiple policy commands.</p> <p>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.</p>
------------------	---

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
  pending 300
  replicate connection tcp
  vlan MOVIES_COMEDY
  inservice
```

Related Commands	Command	Description
	ip csg content	Configures CSG content, 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 with respect to its peer fault-tolerant CSGs, 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	<i>value</i>	Priority of the CSG with respect to its peer fault-tolerant CSGs. The range is from 1 to 254. A higher number indicates a higher priority. The default value is 10.
---------------------------	--------------	---

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 highest priority value is the active CSG in its set of fault-tolerant CSGs.
-------------------------	--

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	<i>number</i>	Identifies a specific quota server to activate or assign to a specific user. The range is from 1 to 10. The default value is 1.
---------------------------	---------------	---

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
  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 range is from 1 to 65535.

The quota local port number cannot be the same as the the agent local port number (configured with the **agent local-port** command in CSG accounting configuration mode).

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 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; the CSG replies to the 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 idle 3600
  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 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

<i>ip-address</i>	IP address of the quota server. The CSG differentiates quota servers on the basis of their IP addresses. When you configure a quota server, make sure that its IP address matches on both the active CSG and the standby CSG.
<i>port-number</i>	Port number of the quota server. The range is from 1 to 65535. The CSG differentiates quota servers on the basis of their port numbers. When you configure a quota server, make sure that its port number matches on both the active CSG and the standby CSG.
<i>priority</i>	Defines active and standby quota servers. The priority specifies the order of preference of the quota servers. A lower number indicates a higher priority. If the current quota server becomes unusable, the 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) tunneling protocol (GTP) retransmits a packet. When the quota server detects a duplicate quota-download request, it resends the same quota that it sent for the original request.

**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 the **no quota server reassign** command 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 idle 3600
  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 users for which you want to generate accounting records

radius acct-port

To configure the RADIUS listening port when it is not the established RADIUS default of 1813, use the **radius acct-port** command in CSG user group configuration mode. To use the default port number, use the **no** form of this command.

radius acct-port *port-number*

no radius acct-port

Syntax Description

<i>port-number</i>	Listening port number of the RADIUS server. The range is from 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 idle 3600
  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 a RADIUS Accounting Start Request or a RADIUS 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

This command has no arguments or keywords.

Defaults

The CSG generates a RADIUS response to a RADIUS Accounting Start Request or a RADIUS 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 because of resource constraints.
2. The CSG parses the RADIUS Accounting Request and encounters RADIUS protocol errors.
3. The CSG parses the RADIUS Accounting Request and a billing plan is specified in the RADIUS Accounting Request, but it does not match a billing plan in the CSG configuration.
4. The CSG parses the RADIUS Accounting Request and a quota server is specified in the RADIUS Accounting Request, but it does not match a quota server in the CSG configuration.
5. The CSG parses the RADIUS Accounting Request and a connect service is specified in the RADIUS 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 vendor-specific attribute (VSA) from the RADIUS Access-Accept. If the CSG uses any attribute from the RADIUS 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 RADIUS 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 RADIUS 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 is to 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

<i>csg-addr</i>	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.
<i>encrypt</i>	(Optional) Indicates how the <i>secret-string</i> is represented when the configuration is displayed (for example, show run), or how it is written to nonvolatile memory (for example, write memory). The possible values are 0 and 7 : <ul style="list-style-type: none"> 0—The <i>secret-string</i> is stored in plain text. This is the default setting. 7—The <i>secret-string</i> is encrypted before it is displayed or written to nonvolatile memory. <p>Note If your router is configured to encrypt all passwords, then the password is represented as 7 followed by the encrypted text. See the Cisco IOS service command for more details.</p>
<i>secret-string</i>	1- to 64-character clear password value for MD5 authentication. All characters are valid; case is significant. The <i>secret-string</i> is always sent in plain text to the CSG module when the configuration is downloaded. The <i>secret-string</i> must match the secret that is specified on the RADIUS client (for example, the gateway general packet radio service [GPRS] support node [GGSN]).
table <i>table-name</i>	(Optional) Associates the specified table name with the RADIUS endpoint. The <i>table-name</i> 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(17d)SXD	This command was introduced.
3.1(1)C6(2)—12.2(18)SXE	The table keyword and <i>table-name</i> argument were added.

Usage Guidelines

A RADIUS Accounting message sent to the specified *csg-addr* (and any port) is parsed, and is then acknowledged, by the CSG.

CSG 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

<i>duration</i>	Handoff timer duration, in seconds. The handoff timer is started when a RADIUS Accounting Stop is received. If the handoff timer expires before a RADIUS Accounting Start for a user is seen, the CSG assumes that a handoff did not occur and deletes the User Table entry for the user. The range is from 0 to 43200. The default is 0 (no handoff timer).
-----------------	--

Defaults

The default is that no handoff timer is configured.
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(17d)SXD	This command was introduced.

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

<i>encrypt</i>	Indicates how the <i>secret-string</i> is represented when the configuration is displayed (for example, show run), or how it is written to nonvolatile memory (for example, write memory). The possible values are 0 and 7 : <ul style="list-style-type: none"> 0—The <i>secret-string</i> is stored in plain text. This is the default setting. 7—The <i>secret-string</i> is encrypted before it is displayed or written to nonvolatile memory. <p>Note If your router is configured to encrypt all passwords, then the password is represented as 7 followed by the encrypted text. See the Cisco IOS service command for more details.</p>
<i>secret-string</i>	1- to 64-character clear password value for MD5 authentication. All characters are valid; case is significant. The <i>secret-string</i> is always sent in plain text to the CSG module when the configuration is downloaded. The <i>secret-string</i> must match the secret that is specified on the RADIUS client (for example, the gateway general packet radio service [GPRS] support node [GGSN]).

Defaults

The *secret-string* is stored in 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 use the **radius key** command to specify a secret password for CSG user group G1:

```
ip csg user-group G1
  entries idle 3600
  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 not the RADIUS default of 1813.

radius monitor

To specify that the CSG is to 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

<i>server-addr</i>	Specifies the server address to monitor.
<i>server-port</i>	Specifies the port number to monitor.
key	(Optional) Specifies a RADIUS key.
<i>encrypt</i>	<p>(Optional) Indicates how the <i>secret-string</i> is represented when the configuration is displayed (for example, show run), or how it is written to nonvolatile memory (for example, write memory).</p> <p>The possible values are 0 and 7:</p> <ul style="list-style-type: none"> 0—The <i>secret-string</i> is stored in plain text. This is the default setting. 7—The <i>secret-string</i> is encrypted before it is displayed or written to nonvolatile memory. <p>Note If your router is configured to encrypt all passwords, then the password is represented as 7 followed by the encrypted text. See the Cisco IOS service command for more details.</p>
<i>secret-string</i>	<p>(Optional) 1- to 64-character clear password value for MD5 authentication. All characters are valid; case is significant.</p> <p>The <i>secret-string</i> is always sent in plain text to the CSG module when the configuration is downloaded.</p> <p>The <i>secret-string</i> must match the secret that is specified on the RADIUS client (for example, the gateway general packet radio service [GPRS] support node [GGSN]).</p>

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 the RADIUS key and encryption level are 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 User Datagram Protocol (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 shows how to use the **radius monitor** command to enable the CSG to monitor the RADIUS flows:

```
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 CSG user group G1:

```
ip csg user-group G1
  entries idle 3600
  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 not the RADIUS default of 1813.

radius pod attribute

To specify the RADIUS attributes and vendor-specific attribute (VSA) subattributes to be copied from the RADIUS Start message and sent to the Network Access Server (NAS) in the Packet of Disconnect (PoD) message, use the **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 | {26 | vsa} } {vendor-id | 3gpp}
radius-subattribute-number}
```

```
no radius pod attribute {radius-attribute-number | {26 | vsa} } {vendor-id | 3gpp}
radius-subattribute-number}
```

Syntax Description

<i>radius-attribute-number</i>	RADIUS attribute number to be copied from the RADIUS Start message and sent to the Network Access Server (NAS) in the Packet of Disconnect (PoD) message.
26	RADIUS attribute number 26.
vsa	Specifies the VSA.
<i>vendor-id</i>	Specifies the vendor ID number. The range is from 1 to 16777215.
3gpp	Specifies the Third Generation Partnership Project (3GPP) vendor ID.
<i>radius-subattribute-number</i>	Specifies the subattribute number. The range is from 1 to 255.

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(17d)SXD	This command was introduced.
3.1(3)C7(1)—12.2(18)SXF1 or 12.2(18)SRA	The 26 , vsa , and 3gpp keywords and <i>vendor-id</i> and <i>radius-subattribute-number</i> arguments were added.

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 affected by the new attributes. Attributes that are already saved will 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 is to send the PoD message, and the key to use in calculating the Authenticator.
radius pod timeout	Specifies the number of times to retry the RADIUS PoD message if it is not acknowledged by means of an ACK message, and the interval between retransmissions.

radius pod nas

To specify the Network Access Server (NAS) port to which the CSG is to send the Packet of Disconnect (PoD) message, and to specify 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	
<i>start-ip</i>	Specifies the first NAS IP address in a range of addresses.
<i>end-ip</i>	Specifies the last NAS IP address in a range of addresses.
<i>port</i>	Specifies the NAS port number to which the PoD message is sent.
key	Specifies a RADIUS key.
<i>encrypt</i>	<p>(Optional) Indicates how the <i>secret-string</i> is represented when the configuration is displayed (for example, show run), or how it is written to nonvolatile memory (for example, write memory).</p> <p>The possible values are 0 and 7:</p> <ul style="list-style-type: none"> 0—The <i>secret-string</i> is stored in plain text. This is the default setting. 7—The <i>secret-string</i> is encrypted before it is displayed or written to nonvolatile memory. <p>Note If your router is configured to encrypt all passwords, then the password is represented as 7 followed by the encrypted text. See the Cisco IOS service command for more details.</p>
<i>secret-string</i>	<p>1- to 64-character clear password value for MD5 authentication. All characters are valid; case is significant.</p> <p>The <i>secret-string</i> is always sent in plain text to the CSG module when the configuration is downloaded.</p> <p>The <i>secret-string</i> must match the secret that is specified on the RADIUS client (for example, the gateway general packet radio service [GPRS] support node [GGSN]).</p>

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(17d)SXD	This command was introduced.

Usage Guidelines

The PoD message is sent to the NAS IP address that is specified in the NAS-IP-Address attribute (4) in the RADIUS Accounting Start message. This command specifies the NAS listening port, as well as the key to use in calculating the Authenticator.

The RADIUS Accounting Start must be received on an IP address that is specified in the enhanced proxy or endpoint (**radius proxy** or **radius endpoint**) command that is configured in module CSG configuration mode.

In some networks, many NASs might use the same listening port and key. In such networks, you can use this command to specify the range of NAS IP addresses.

If no IP addresses are specified, the port number and key apply to all NASes. The “global” definition is used if a specific range is not configured for the NAS when the PoD message is sent.

Examples

The following example shows how to specify NAS ports and keys:

```
ip csg 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 PoD.
radius pod timeout	Specifies the number of times to retry the RADIUS PoD message if it is not acknowledged by means of an ACK message, and the interval between retransmissions.

radius pod timeout

To specify the number of times to retry the RADIUS Packet of Disconnect (PoD) message if it is not acknowledged by means of an ACK message, and the interval between retransmissions, use the **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		
<i>timeout</i>		Number of seconds to wait for an ACK or NAK before sending another PoD message. The default timeout is 5 seconds.
retransmit <i>retransmit</i>		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(17d)SXD	This command was introduced.

Examples

The following example shows how to specify a RADIUS PoD timeout and the number of times to retransmit the message:

```
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 PoD.
radius pod nas	Specifies the NAS port to which the CSG is to send the PoD message, and specifies the key to use in calculating the Authenticator.

radius proxy

To specify that the CSG is to 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	
<i>csg-addr</i>	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.
<i>server-addr</i>	Specifies the server IP address.
<i>csg-source-addr</i>	Specifies the source IP address that the CSG is to use when sending packets to the server. By default, <i>csg-source-addr</i> is set to <i>csg-addr</i> .
key	(Optional) Specifies a RADIUS key. Note Specify no more than one key for each CSG IP address.
<i>encrypt</i>	(Optional) Indicates how the <i>secret-string</i> is represented when the configuration is displayed (for example, show run), or how it is written to nonvolatile memory (for example, write memory). The possible values are 0 and 7 : <ul style="list-style-type: none"> 0—The <i>secret-string</i> is stored in plain text. This is the default setting. 7—The <i>secret-string</i> is encrypted before it is displayed or written to nonvolatile memory. Note If your router is configured to encrypt all passwords, then the password is represented as 7 followed by the encrypted text. See the Cisco IOS service command for more details.
<i>secret-string</i>	(Optional) 1- to 64-character clear password value for MD5 authentication. All characters are valid; case is significant. The <i>secret-string</i> is always sent in plain text to the CSG module when the configuration is downloaded. The <i>secret-string</i> must match the secret that is specified on the RADIUS client (for example, the gateway general packet radio service [GPRS] support node [GGSN]).
table <i>table-name</i>	Associates the specified table name with the RADIUS proxy. The <i>table-name</i> 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(17d)SXD	The <i>csg-source-addr</i> argument was added.
3.1(1)C6(2)—12.2(18)SXE	The table keyword and <i>table-name</i> 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; otherwise, the source IP address is the *csg-addr*.

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 User Datagram Protocol (UDP) headers specify a length larger than the physical packet size.

CSG 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; a client is defined by its IP address and port.

**Note**

If your network is designed to check the authorization string in RADIUS messages, we recommend that you enter a *secret-string*. Additionally, if you configure the **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 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 configure a RADIUS server, 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	<i>ip-address</i>	IP address of the RADIUS server.
	<i>port-number</i>	(Optional) Port number of the RADIUS server. The range is from 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 is configured 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 the IP address 10.13.14.15 and with the default RADIUS port, which is port number 1813:

```
ip csg user-group G1
  entries idle 3600
  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 not 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 {radius-attribute-number | {26 | vsa} {vendor-id | 3gpp}
radius-subattribute-number}
```

Syntax Description		
<i>radius-attribute-number</i>		Specifies the RADIUS attribute number.
26		RADIUS attribute number 26.
vsa		Specifies the vendor-specific attribute (VSA).
<i>vendor-id</i>		Specifies the vendor ID number. The range is from 1 to 16777215.
3gpp		Specifies the Third Generation Partnership Project (3GPP) vendor ID.
<i>radius-subattribute-number</i>		Specifies the subattribute number. The range is from 1 to 255.

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.

To detect duplicate RADIUS requests (in this situation, the existing entry is not deleted), specify the attribute (which might be a VSA) to be used. If the contents of the specified attribute in the original request match the contents of the attribute in the current request, the request is a duplicate and the existing entry is not deleted.

Examples The following example shows how to enable the **radius start restart session-id** command:

```
ip csg user-group U1
  radius start restart session-id 44
```

radius stop purge

To specify the 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 {radius-attribute-number | {26 | vsa} {vendor-id | 3gpp}
radius-subattribute-number}
```

Syntax Description

<i>radius-attribute-number</i>	Specifies the RADIUS attribute number.
26	RADIUS attribute number 26.
vsa	Specifies the vendor-specific attribute (VSA).
<i>vendor-id</i>	Specifies the vendor ID number. The range is from 1 to 16777215.
3gpp	Specifies the Third Generation Partnership Project (3GPP) vendor ID.
<i>radius-subattribute-number</i>	Specifies the subattribute number. The range is from 1 to 255.

Defaults

The user entry is deleted when a RADIUS Accounting 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 VSA) 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.

Examples

The following example shows how to enable the **radius stop purge** command for 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

None

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 the **no radius userid** command is used, 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 idle 3600
  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 acct-port	Configures the RADIUS listening port when it is not the established RADIUS default of 1813.
	radius key	Specifies the CSG to be the RADIUS endpoint for account records.

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 improves 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	Configures content-based client accounting as a service, and enters CSG accounting configuration mode.

records format

To specify variable, fixed, or variable-single call detail record (CDR) format, use the **records format** command in CSG accounting configuration mode. To use the default setting, 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(17d)SXD	The variable-single-cdr keyword was added.

Usage Guidelines

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

Examples

The following example specifies fixed record format:

```
ip csg accounting
 records format fixed
```

Related Commands

Command	Description
class	Specifies a service class value.
hostname	Specifies a variable hostname for a CSG module
ip csg transport-type	Classifies data traffic on the basis of its access path.
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.

records granularity

To specify the granularity at which billing call detail records (CDRs) are to 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	<p>Number of bytes of data, sent and received by a session, that triggers a CDR.</p> <ul style="list-style-type: none"> For HTTP billing, the CSG counts TCP bytes. For all other billing protocols, the CSG counts IP bytes. <p>The difference between bytes sent and bytes received in two records might not exactly equal the <i>bytes</i> argument, because updates must occur on packet boundaries.</p> <p>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, indicating no maximum.</p>
time seconds	<p>Maximum time, in seconds, between billing records for a session. Records can be sent more frequently if the number of bytes is reached.</p> <p>When a record is sent because the maximum time has been reached, the byte counts reported in the record are approximate.</p> <p>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, indicating no time limit.</p>

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 when either limit is reached. Then 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

records granularity

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 services for which transaction-level billing is not required. For example, if a user is accessing the Internet, and the data is to be billed solely on the basis of volume, then generating records for each HTTP transaction is of little use. With service-level CDR summarization enabled, the CSG generates only consolidated records that contain service-level usage.

To enable service-level CDR summarization in postpaid mode, you must specify that the associated billing plan is postpaid by using the **mode postpaid** command in CSG billing configuration mode.

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	Configures 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 send the HTTP Statistics data record to the BMA only when a session fails (for example, if a Reset [RST] without Finish [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 <i>bytes</i>	<p>Number of bytes of data, sent and received by a session, that triggers the sending of an intermediate billing record:</p> <ul style="list-style-type: none"> For HTTP billing, the CSG counts TCP bytes. For all other billing protocols, the CSG counts IP bytes. <p>The difference between bytes sent and received in two records might not exactly equal the <i>bytes</i> 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.</p> <p>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, indicating that the number of bytes sent and received will not trigger an intermediate record.</p>
time <i>seconds</i>	<p>Maximum time, in seconds, between billing records for a session. Records can be sent more frequently if the number of bytes is reached.</p> <p>When a record is sent because the maximum time has been reached, the byte counts reported in the record are approximate.</p> <p>The range is from 5 to 65535. The default value, if the time keyword is not specified, is 0, indicating no time limit.</p>

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 when either limit is reached. Then 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) elapse, whichever occurs 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	Configures 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, 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

<i>number</i>	Maximum number of billing records that can be stored or queued in the CSG. If the number of queued records exceeds the <i>number</i> 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 range is from 1 to 65535. The default value is 10000.
---------------	--

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 10000 (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, 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 active and standby BMAs to which billing records are to be sent.

record-storage

To define a Cisco 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

<i>ip-address</i>	Destination address for packets going to the storage device.
<i>port</i>	(Optional) Source port that the CSG will use for communicating with a record storage server other than the Persistent Storage Device/Call Data Record Backup (PSD/CDRB).

Defaults

None

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 that are going to the storage device (PSD/CDRB). The PSD/CDRB listens only on port 3386. Therefore, when the **record-storage** command omits the *port* parameter, the CSG defaults to port 3386. If a storage device is listening on another port, you must 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 use the **record-storage** command to define a record storage 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 that the CSG will use for communicating with record storage.

record-storage local-port

To define the source port that the CSG will use for communicating with record storage, use the **record-storage local-port** command in CSG accounting configuration mode. To remove the source port for record storage, use the **no** form of the command.

record-storage local-port *port*

no record-storage local-port *port*

Syntax Description	<i>port</i>	Source port that the CSG will use for communicating with the record store.
---------------------------	-------------	--

Defaults	None
-----------------	------

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; the local port is also the port on which the CSG listens for responses.
-------------------------	--



Note	The record-storage local port must not conflict with either the quota server or 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 Cisco 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 Network Address Translation (NAT) client flows to an alternate IP address when quota is depleted.
wap	Redirects wireless application protocol (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.
<i>ip-address</i>	The IP address to which client flows are to be redirected.
<i>port-number</i>	(Optional) Port number to which client flows are to be redirected. The range is from 1 to 65535. If you do not specify a port number, the port number in the user packet is not changed.
<i>url</i>	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 redirects NAT client flows for the CSG user group G1; the flows are redirected to IP address 10.33.33.3:

```
ip csg user-group G1
entries idle 3600
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

<i>policy-name</i>	Name of the refunding policy to be enabled.
--------------------	---

Defaults

Refunding is not enabled.

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	Configures 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 standby 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 synchronization sequence number (SYN) or Reset (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
  pending 300
  replicate connection tcp
```

■ replicate connection tcp

```
vlan MOVIES_COMEDY
inservice
```

Related Commands

Command	Description
ip csg content	Configures CSG content, and enters CSG content configuration mode.

report http header

To define the inclusion of multiple HTTP request headers in the CSG HTTP_Header call detail record (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

<i>header-name</i>	Name of the request header that 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 copy only 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:

```
ip csg accounting name
  report http header x-subno
  report http header x-al-session-id
```

report radius attribute

To specify the RADIUS attributes to be copied from the RADIUS Start message into call detail records (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 | 26 | vsa} {vendor-id | 3gpp}
radius-subattribute-number
```

```
no report radius attribute {radius-attribute-number | 26 | vsa} {vendor-id | 3gpp}
radius-subattribute-number
```

Syntax Description

<i>radius-attribute-number</i>	RADIUS attribute number to be copied from the RADIUS Start message.
26	RADIUS attribute number 26.
vsa	Specifies the vendor-specific attribute (VSA).
<i>vendor-id</i>	Specifies the vendor ID number. The range is from 1 to 16777215.
3gpp	Specifies the Third Generation Partnership Project (3GPP) vendor ID.
<i>radius-subattribute-number</i>	Specifies the subattribute number. The range is from 1 to 255.

Defaults

No RADIUS attributes are reported.

Command Modes

CSG accounting configuration

Command History

Release	Modification
2.2(1)C(4)—12.2(11b)E3	This command was introduced.
3.1(3)C4(1)—12.2(14)ZA2	This command was moved to the CSG accounting configuration mode
3.1(3)C7(1)—12.2(18)SXF1 or 12.2(18)SRA	The 26 , vsa , and 3gpp keywords and <i>vendor-id</i> and <i>radius-subattribute-number</i> arguments were added.

Usage Guidelines

You can specify as many attributes as you want.

If an attribute is not present in the RADIUS message, it is not present in the CDRs, unless **records format fixed** is configured. If the list of configured attributes changes, only new RADIUS messages are affected by the new attributes. Attributes that are already saved will continue to be included in the PoD message.

When a RADIUS Start request is received, any attributes that were 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 in which they are presented 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	Configures content-based client accounting as a service, and enters CSG accounting configuration mode.
ip csg service	Configures a content billing service, and enters CSG service 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	seconds
	Report the number of IP bytes uploaded and downloaded for each interval.	Report usage in seconds for the interval, as well as the timestamps of the start of the first and last billable sessions in the interval.

Defaults	None
----------	------

Command Modes	CSG accounting configuration
---------------	------------------------------

Command History	Release	Modification
	3.1(3)C6(2)—12.2(18d)SXE	This command was introduced.

Usage Guidelines

Interval report Tag-Length-Values (TLVs) are generated for Service Reauthorization Request, Service Stop, and Quota Return messages. Reports contain statistics since the last report.

If you want to report both IP bytes and usage in seconds, you can specify both **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 for Prepaid Error Reimbursement, 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 FTP application return codes.
http	The CSG refunds quota for 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.
<i>rc-start</i>	Specifies the beginning of the range of values for specific application return codes. Valid values are 1 to 65535 (0xffff).
<i>rc-end</i>	(Optional) Specifies the end of the range of values for specific application return codes. Valid values are the value of <i>rc-start</i> to 65535 (0xffff). If you are specifying a single value as the range, do not specify <i>rc-end</i> .

Defaults

None

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

The CSG supports return code-based refunding for all protocols except RTSP.

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 use the **retcode** command to specify ranges of application return codes:

```
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 wireless application protocol (WAP) flag bit masks and values for CSG Prepaid Error Reimbursement.
ip csg refund	Specifies the refund policy to apply 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		
<i>ip-address</i>		Subnet IP address.
<i>netmask</i>		Network mask.
gateway		Specifies that the gateway is configured.
<i>gw-ip-address</i>		Gateway IP address.

Defaults None

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 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 VLAN or server VLAN that defines the Layer 2 paths for the CSG accounting service flows, assigns a VLAN ID and an optional name, and enters module CSG VLAN configuration mode.

ruleset

To download all content configured 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	<i>ruleset-name</i>	Name of a configured CSG billing ruleset.
--------------------	---------------------	---

Defaults	None
----------	------

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 that is 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

<i>service-name</i>	Name of a configured CSG billing service.
---------------------	---

Defaults

None

Command Modes

CSG billing configuration

Command History

Release	Modification
3.1(1)C3(1)—12.2(14)ZA	This command was introduced.

Usage Guidelines

To associate more than one service with the same billing plan, use multiple **service** commands.

Examples

The following example shows how to associate services MOVIES and BROWSING with billing plan REGULAR:

```
ip csg billing REGULAR
  entries idle 3600
  mode postpaid
  service MOVIES
  service BROWSING
```

Related Commands

Command	Description
entries idle (CSG billing)	Sets the time after which entries for idle users are deleted from the CSG User Table.
ip csg billing	Defines a billing plan, and enters CSG billing configuration mode.
mode	Specifies that a billing plan is postpaid or prepaid.

show

To display information about the CSG, use the **show** command on the CSG console.

show [**buffer** | **cpu** | **csg** | **encap** *ip-address netmask* | **processes** [**detail**] | **version**]

Syntax Description		
buffer		Displays memory allocation for the CSG.
cpu		Displays memory and CPU utilization for the CSG.
csg		Displays all of the CSG statistics.
encap		Displays encapsulation information for misdirected packets.
<i>ip-address</i>		IP address for which to display encapsulation information. The default is 0.0.0.0 (all clients).
<i>netmask</i>		IP network mask for which to display encapsulation information. You can express the network mask in either IP dotted notation (<i>n.n.n.n</i>) or prefix notation (<i>/nn</i> , where <i>nn</i> is the number of leading 1 bits). For example, 255.255.0.0 and /16 are equivalent network masks.
processes		Displays information about the CSG processes.
detail		Displays the traceback for each CSG process.
version		Displays the version of the CSG.

Defaults None

Command Modes CSG console

Command History	Release	Modification
	2.2(1)C(1)	This command was introduced.
	3.1(3)C7(1)	The encap keyword and the <i>ip-address</i> and <i>netmask</i> arguments were added.

Usage Guidelines You cannot use the **encap** keyword to display encapsulation information for locally defined interfaces. If you enter this command for a locally defined interface, the CSG displays an error message, as shown in the following example:

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

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

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

Examples

The following example displays encapsulation information for IP address 172.18.45.1:

```
CSG> show encap 172.18.45.1 255.255.255.255  
  
172.18.45.1      /32      00-d0-00-33-a8-0a
```

Related Commands

Command	Description
copy	Copies the CSG core dump.
ping	Determines whether the CSG can reach a remote host.
upgrade	Upgrades the CSG by loading a CSG image from the Supervisor Engine.

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.
<i>ip-address</i>		Displays information for the specified user IP address.
<i>ip-mask</i>		Displays information for the specified user IP address mask.
userid <i>userid</i>		Displays information for the specified user ID.
detail		Lists detailed statistics for each BMA, followed by a summary of statistics for all BMAs.
module <i>num</i>		Displays information for the specified CSG module.
psd module <i>slot</i>		Displays information pertaining to Cisco Persistent Storage Device (PSD) functionality residing on the CSG.

Defaults None

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, in addition to 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 that are sent to the BMA and the quota server, including a short description of the fields.



Note A good understanding of RADIUS protocol is needed to understand these RADIUS values.

The length of the RADIUS vendor-specific attribute (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		
<i>slot</i>		Slot in which 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.
<i>ip-address</i>		Displays information for the specified user IP address.
<i>ip-mask</i>		Displays information for the specified user IP address mask.
userid <i>userid</i>		Displays information for the specified user ID.
detail		Lists detailed statistics for each BMA, followed by a summary of statistics for all BMAs.

Defaults None

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(18d)SXE	Output was modified to support the tariff switch feature.

Usage Guidelines BMA statistics are kept for each BMA, in addition to 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:

```
Router# 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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	<i>slot</i>	Slot in which the CSG resides.
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 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		
	<i>slot</i>	Slot in which the CSG resides.
	all	Displays statistics for all CSG billing plans.
	plan <i>billing-plan-name</i>	Displays statistics for only the specified CSG billing plan.

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 shows how to display the statistics and counters for all CSG billing plans:

```
Router# 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, 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 None

Command Modes Privileged EXEC

Command History	Release	Modification
	3.1(3)C5(5)—12.2(17d)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:

```
Router# 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 Tag-Length-Value (TLV) for call detail records (CDRs).
last sync time	Date and time of last synchronization update from the Supervisor Engine.

show module csg conns

To display active CSG 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		
<i>slot</i>		Slot in which the CSG resides.
vserver		(Optional) Specifies the connections associated with a particular virtual server.
<i>virtserver-name</i>		(Optional) Name of the virtual server to be monitored.
client		(Optional) Specifies the connections associated with a particular client IP address.
<i>ip-address</i>		(Optional) IP address of the client to be monitored.
detail		(Optional) Specifies 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		
<i>slot</i>		Slot in which the CSG resides.
name <i>content-name</i>		(Optional) Name of a configured content.
detail		(Optional) Displays more detailed information.

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 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 and Layer 4 flows that can be processed by the content: <ul style="list-style-type: none"> any—Flows of any protocol type can be processed. tcp—Only TCP flows can be processed. udp—Only User Datagram Protocol (UDP) flows can be processed. <i>protocol-number</i>—Number identifying the protocol whose flows can be processed. The range is from 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 = 10
destination = 0.0.0.0/0:80, TCP
idle = 10, replicate = connection, vlan = ALL, pending = 30
max parse len = 4000, persist rebalance = TRUE
conns = 0, total conns = 7
policy          total conn  client pkts  server pkts
-----
HTTP-MS-AHTML   1             0             0
HTTP-MS-BJPG    2             0             0
HTTP-FREE        0             0             0
HTTP-DOUBLE      0             0             0
HTTP-MS         28            0             0
(default)        0             0             0
```

**Note**

For HTTP accounting, the “client pkts” and “server pkts” columns always display zeros.

Related Commands

Command	Description
ip csg content	Configures CSG content, 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	
<i>slot</i>	Slot in which the CSG resides.
detail	(Optional) Displays more detailed information.

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 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	<i>slot</i>	Slot in which the CSG resides.
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 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 the status of the CSG and, if it is online, its chassis slot location and the status of the configuration download, use the **show module csg slot status** command in privileged EXEC mode.

show module csg slot status

Syntax Description	<i>slot</i>	Slot in which the CSG resides.
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 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

<i>slot</i>	Slot in which the CSG resides.
all	(Optional) Displays all of the available statistics.
core-dump	(Optional) Displays all of the most recent statistics for the process that experienced a core dump.
csg	(Optional) Displays all of the CSG statistics.
fpga	(Optional) Displays all of the field programmable gate array (FPGA) statistics.
ft	(Optional) Displays all of the statistics related to fault tolerance.
processor number	(Optional) Displays the statistics for the specified processor.
slowpath	(Optional) Displays all of the slowpath statistics.
utilization	(Optional) Displays 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(17d)SXD	Added support for Internet Message Access Protocol (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    61%    153M
  Allocated Memory   31%     79M
  OS Static Memory    8%     22M

  Lowest Memory Available    153M THU MAR 23 21:53:31 2006
```

You can also use this command to display the CSG CPU Utilization number (that is, the percent of the CSG CPU that is currently in use), which presents a good overall picture of CSG capacity. To do so, first enable debugging output for the CPU, using the **debug ip csg cpu** command in privileged EXEC mode, then enter the **show module csg slot tech-support utilization** command. To calculate the remaining CSG CPU capacity, subtract the CSG CPU Utilization from 100%. So, if the CSG CPU Utilization is 32%, the CSG has 68% CPU capacity remaining.

**Note**

You must re-enter the **debug** command after every reload because it is not saved in the startup configuration.

```
Router# debug ip csg cpu

CSG CPU Utilization debugging is on

Router# show module csg 3 tech-support utilization

Resource Utilization:
  Memory
  Available Memory      61%    153M
  Allocated Memory     31%     79M
  OS Static Memory      8%     22M

  Lowest Memory Available      153M THU MAR 23 21:53:31 2006

  CSG CPU Utilization: 1m (55.0%), 5m (32.0%)
```

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, exceed_sess_max= 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

```

show module csg tech-support

```
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

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
```

show module csg tech-support

```

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 CSG 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	
<i>slot</i>	Slot in which the CSG resides.
name	(Optional) Displays the named variable information.
detail	(Optional) Displays the map configuration details.

Defaults If no variable name is specified, the command displays information for all variables.

Command Modes Privileged EXEC

Command History	Release	Modification
	3.1(1)C4(1)—12.2(14)ZA	This command was introduced.
	3.1(3)C5(5)—12.2(17d)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 for a CSG, 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

<i>slot</i>	Slot in which the CSG resides.
client	(Optional) Displays only the client VLAN configuration.
server	(Optional) Displays only the server VLAN configuration.
ft	(Optional) Displays only the fault-tolerant configuration.
id	(Optional) Displays the VLAN.
<i>vlan-id</i>	(Optional) Displays the specified VLAN.
detail	(Optional) Displays the map configuration details.

Defaults

If no options are specified, the command displays information about all the 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 VLAN or server VLAN that defines the Layer 2 paths for the CSG accounting service flows, assigns a VLAN ID and an 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:

```
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	<i>table-name</i>	1- to 15-character string identifying the table. The CSG stores the table name as all-uppercase ASCII characters.
Defaults	None	
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	<p>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.</p> <p>You can associate only one table name with each VLAN.</p>	
Examples	<p>The following example associates the ACME_VLAN table with VLAN 254 on module 5:</p> <pre>module csg 5 vlan 254 client table ACME_VLAN</pre>	
Related Commands	Command	Description
	radius endpoint	Identifies the CSG as an endpoint for RADIUS Accounting messages.
	radius proxy	Specifies that the CSG is to be a proxy for RADIUS messages.
	show module csg variable	Displays the list of VLANs.
	vlan (module CSG)	Creates a client VLAN or server VLAN that defines the Layer 2 paths for the CSG accounting service flows, assigns a VLAN ID and an optional name, and enters module CSG VLAN configuration mode.

upgrade

To upgrade the CSG by loading a CSG image from the Supervisor Engine, use the **upgrade** command on the CSG console.

```
upgrade {slot0: | 127.0.0.yz} filename
```

Syntax Description	upgrade <i>slot0:</i> <i>filename</i>	Loads the specified CSG image, such as <code>c6csg-apc.31-3.c7.1</code> , from the Supervisor Engine in slot 0 to the CSG.
	upgrade 127.0.0.yz <i>filename</i>	Loads the specified CSG image, such as <code>c6csg-apc.31-3.c7.1</code> , from the specified Supervisor Engine to the CSG. The Supervisor Engine is identified as 127.0.0.yz , where: <ul style="list-style-type: none"> • <i>y</i> is the slot number—1 for slot 1, 2 for slot 2, and so on. • <i>z</i> identifies the Supervisor Engine—1 for Supervisor Engine 720, 2 for Supervisor Engine 32. • <i>filename</i> is the CSG image name, such as <code>c6csg-apc.31-3.c7.1</code>.

Defaults	None
----------	------

Command Modes	CSG console
---------------	-------------

Command History	Release	Modification
	2.2(1)C(1)	This command was introduced.

Examples	The following example loads CSG image <code>c6csg-apc.31-3.c7.1</code> from the Supervisor Engine 32 in slot 1 to the CSG:
----------	--

```
CSG> upgrade 127.0.0.12 c6csg-apc.31-3.c7.1
```

Related Commands	Command	Description
	copy	Copies the CSG core dump.
	ping	Determines whether the CSG can reach a remote host.
	show	Displays information about the CSG.

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	<i>url-map-name</i>	Name of a URL map, as configured with the ip csg map command.
---------------------------	---------------------	--

Defaults	None
-----------------	------

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 wireless application protocol (WAP) 1.x, URL maps take precedence over access lists.

For WAP 1.x and Real Time Streaming Protocol (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

<i>group-name</i>	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

None

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	Configures content-based accounting as a service.
ip csg user-group	Creates a group of users for which you want to generate accounting records, and enters CSG user group configuration mode.

user-profile server

To specify which server to use 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 vendor-specific attribute (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

The billing plan is obtained 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 that contains 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 the specified environmental variables from the configuration, use the **no** form of this command.

variable *name value*

no variable *name value*

Syntax Description

<i>name</i>	Name string for the variable. See Table B-7 for a list of valid variable names.
<i>value</i>	Value string for the variable.

Defaults

None

Command Modes

Module CSG configuration

Command History

Release	Modification
3.1(1)C4(1)—12.2(14)ZA	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(17d)SXD	Added support for several new variables.
3.1(3)C6(2)—12.2(18d)SXE	Added support for the CSG_FT_CONTENT variable.
3.1(3)C7(1)—12.2(18)SXF1 or 12.2(18)SRA	Added support for several new variables.

Usage Guidelines

[Table B-7](#) lists the environmental values used by the CSG.

Table B-7 Environmental Variables

Name	Default	Valid Values	Description
ARP_INTERVAL	300	Integer (15 to 31536000)	Time (in seconds) between Address Resolution Protocols (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.

Table B-7 Environmental Variables (continued)

Name	Default	Valid Values	Description
ARP_RATE	10	Integer (1 to 60)	Time (in seconds) between ARP retries.
ARP_RETRIES	3	Integer (2 to 15)	Count of ARP attempts before a host is flagged as down.
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 fixed-cost billing (basis fixed).
CSG_BASIS_SEC_LOW_QUOTA	10	Integer (5 to 300)	Value for the available quota threshold that triggers reauthorization for duration-based billing (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. Note Do not change the setting of this variable unless directed to do so by Cisco personnel.
CSG_FAST_FIN_TIMEOUT	10	Integer (10 to 65535)	Timeout (in seconds) for connection reset after a Finish (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).

Table B-7 Environmental Variables (continued)

Name	Default	Valid Values	Description
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_FT_SESSION_DELAY	0	Integer (0 to 3600)	Delay, in seconds, before replicating session information.
CSG_FTP_HA_WAIT_DELAY	10	Integer (1 to 60)	Delay, in sixtieths of a second, after sending FTP content information to the standby.
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 general packet radio service (GPRS) tunneling protocol (GTP) repolls before link failure.
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 call detail records (CDRs) for HTTP when the records format fixed command is configured.
CSG_HTTP_STATS_DELAY	0	Integer (0 to 1234)	Delay in seconds before sending the HTTP Statistics CDR.
CSG_IXP_FPGA_TRAP_ENABLED	0	Integer (0 or 1)	Enable Internet Exchange Point (IXP) field programmable gate array (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.

Table B-7 Environmental Variables (continued)

Name	Default	Valid Values	Description
CSG_MEM_FAILOVER_THRESHOLD	0	Integer (0 to 98)	Perform a core dump, failover to the standby CSG, and issue a message when CSG memory usage exceeds the failover threshold. By default (0), the CSG does not perform a core dump or failover, nor does it issue this failover message.
CSG_MEM_MAX_FREQUENCY	1	Integer (1 to 99)	Set the time, in minutes, between depletion messages for CSG memory usage exceeded.
CSG_MEM_MAX_THRESHOLD	85	Integer (1 to 98)	Issue a message when CSG memory usage exceeds the depletion threshold.
CSG_MEM_WARN_FREQUENCY	1	Integer (1 to 99)	Set the time, in minutes, between warning messages for CSG memory usage exceeded.
CSG_MEM_WARN_THRESHOLD	85	Integer (1 to 98)	Issue a message when CSG memory usage exceeds the warning threshold.
CSG_OBSCURE_X_FORWARDED_FOR	0	Integer (0 or 1)	Overwrite (1) or retain (0) the contents of the X-Forwarded-For header.
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.
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 Route Processor Redundancy Plus (RPR+) switchover before the CSG detects timeouts.

Table B-7 Environmental Variables (continued)

Name	Default	Valid Values	Description
CSG_SESSION_MAX	1000000	Integer (1 to 1000000)	Set the maximum number of sessions that the CSG can support. When the number of active sessions reaches the specified maximum number of sessions, the CSG begins dropping incoming new sessions.
CSG_SMTP_CDR_HEADER_REDUCTION	0	Integer (0 or 1)	Remove (1) or include (0) RFC 2822 header Tag-Length-Values (TLVs) in the Simple Mail Transfer Protocol (SMTP) CDR.
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_DROP_UNKNOWN_PACKETS	0	Integer (0 or 1)	Drop (0) or forward without charge (1) wireless application protocol (WAP) 1.x packets that cannot be parsed as type wap .
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 a 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 a quota grant of zero.
DEBUG_BILL_URL	1	Integer (0 or 1)	Enable (1) or disable (0) debugging messages for bill URL messages.

Table B-7 Environmental Variables (continued)

Name	Default	Valid Values	Description
DEST_UNREACHABLE_MASK	0xffff	Integer (0 to 65535)	Bitmask that defines which Internet Control Message Protocol (ICMP) destination unreachable codes are to be forwarded.
HTTP_CASE_SENSITIVE_MATCHING	1	Integer (0 or 1)	Indicates whether URL matching (cookie, header) and sticky objects are case-sensitive.
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 packets that do not include synchronization sequence numbers (SYNs) and do not match any existing flows.
TRAP_CODES	-	String (1 to 128 chars)	<p>If CSG debug traps are enabled using the TRAP_USER_ENABLE variable, this variable specifies the list of trap codes, in hex notation, to be enabled for debugging.</p> <p>Note Do not change the setting of this variable unless directed to do so by Cisco personnel.</p>

Table B-7 Environmental Variables (continued)

Name	Default	Valid Values	Description
TRAP_USER	-	String (1 to 30 chars)	<p>If CSG debug traps are enabled using the TRAP_USER_ENABLE variable, this variable specifies the user ID for remote command (RCMD), which allows the router to receive remote shell protocol (rsh) and remote command protocol (rcp) requests.</p> <p>Note Do not change the setting of this variable unless directed to do so by Cisco personnel.</p>
TRAP_USER_ENABLE	0	Integer (0 or 1)	<p>Enable (1) or disable (0) additional trap information for debugging.</p> <p>Note Do not change the setting of this variable unless directed to do so by Cisco personnel.</p>

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

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

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

By default, the CSG issues this warning message when memory usage exceeds 85%. To change that threshold, change the setting of the **CSG_MEM_WARN_THRESHOLD** variable. The valid range for this variable is 1% to 98%; the default setting is 85%.

By default, the CSG issues this warning message once a minute after the threshold has been exceeded. To change the time between warning messages, change the setting of the **CSG_MEM_WARN_FREQUENCY** variable. The valid range for the variable is 1 minute to 99 minutes; the default setting is 1 minute.

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

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

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

By default, the CSG issues this depletion message once a minute after the threshold has been exceeded. To change the time between depletion messages, change the setting of the **CSG_MEM_MAX_FREQUENCY** variable. The valid range for the variable is 1 minute to 99 minutes; the default setting is 1 minute.

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

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

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



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

If you see any of the preceding messages, you need to reduce the maximum number of billing records that the CSG is allowed to buffer in memory. To do so, set the **records max** command in CSG accounting configuration mode to a smaller value, such as 10,000.

Examples

This example shows how to enable the environmental variables configuration:

```
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 This command has no arguments or keywords.

Defaults None

Command Modes CSG service configuration

Command History	Release	Modification
	3.1(3)C5(5)—12.2(17d)SXD	This command was introduced.

Usage Guidelines If this command is configured, the CSG uses the Service Verification Request to perform the following actions:

- Alert the quota server of a new transaction.
- Allow the quota server to direct the 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 Content Authorization Response. The CSG uses NAT to translate the packet to the IP address and port provided in the Content Authorization Response.
 - **REDIRECT-URL**—Redirect the client request to the URL provided in the Content Authorization Response. The CSG sends a Layer 7 redirect (for example, an HTTP 302 response) to the client; the Layer 7 redirect 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	Configures 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	<i>token</i>	A string of up to 15 alphanumeric characters.
Defaults	None	
Command Modes	CSG user group configuration	
Command History	Release	Modification
	3.1(3)C5(5)—12.2(17d)SXD	This command was introduced.
Usage Guidelines	<p>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.</p> <p>The token is used for both HTTP and wireless application protocol (WAP) service verification URL-rewriting.</p>	
Examples	<p>The following example specifies a token for service verification URL-rewriting:</p> <pre>ip csg user-group A1 verify confirmation ?CSG_VERIFY_OK</pre>	
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	<i>vlan-name</i>	Name of the source VLAN for the CSG billing content.
Defaults	None	
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. When the content is downloaded to a CSG card, the <i>vlan-name</i> argument is mapped to a specific VLAN number.	
Examples	<p>The following example shows how to restrict the CSG content billing to a single-source VLAN named MOVIES_COMEDY:</p> <pre>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 pending 300 replicate connection tcp vlan MOVIES_COMEDY inservice</pre>	
Related Commands	Command	Description
	ip csg content	Configures CSG content, and enters CSG content configuration mode.

vlan (module CSG)

To create a client VLAN or server VLAN that defines the Layer 2 paths for the CSG accounting service flows, assign a VLAN ID and an 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		
<i>vlan-id</i>		Number of the VLAN. The range is from 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		Specifies a client-side VLAN.
server		Specifies a server-side VLAN.
<i>vlan-name</i>		(Optional) Unique symbolic name of the VLAN. The name can be from 1 to 15 characters long, and can include uppercase or lowercase letters (the CSG changes all letters to uppercase), numbers, and any special characters. The <i>vlan-name</i> argument is required if the content configuration includes the vlan command in CSG content configuration mode.

Defaults	
	None

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 must 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 into service 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 wireless application protocol (WAP) transactions to be terminated midstream when the user's quota is 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	Specifies that WAP transactions be ended midstream when user's quota is depleted.
Defaults	None	
Command Modes	CSG service configuration	
Command History	Release	Modification
	3.1(3)C5(1)—12.2(17d)SXB	This command was introduced.
Usage Guidelines	<p>This command is configured on a per-service basis.</p> <p>This command configures the WAP cutoff feature.</p>	
Examples	<p>The following example shows how to enable the zero-quota abort type command:</p> <pre>ip csg service <i>SERVIN_WAP</i> zero-quota abort type wap content <i>WAP_WTP_CONTENT</i> policy <i>WAP_WTP</i></pre>	
Related Commands	Command	Description
	ip csg service	Configures a content billing service, and enters CSG service configuration mode.