



# APPENDIX **A**

## CSG2 Command Reference

---

This appendix documents the commands necessary to configure and monitor the CSG2. Other commands used with the CSG2 are documented in the following publications:

- *Service and Application Module for IP User Guide* for the following commands:
  - Supervisor console commands
  - Power PC console commands
  - Power PC ROM-monitor (ROMmon) console commands
  - Broadcom BCM Linux-based Storage Area Network Operation System (SanOS) console commands
  - Broadcom BCM ROMmon console commands
  - Line Card Processor (LCP) console commands
- Cisco IOS Server Load Balancing feature module for IOS SLB-specific commands
- Cisco IOS Release 12.2 command reference publications for other IOS commands

All of the CSG2 commands are listed below in alphabetical order:

- [accounting, page A-6](#)
- [activation, page A-7](#)
- [aoc append url, page A-9](#)
- [aoc confirm, page A-10](#)
- [aoc enable, page A-12](#)
- [basis, page A-14](#)
- [block, page A-17](#)
- [class, page A-18](#)
- [clear ip csg, page A-19](#)
- [clear ip iscsi statistics, page A-21](#)
- [clear record-storage-module stats, page A-22](#)
- [client-group \(CSG2 content\), page A-23](#)
- [content \(CSG2 service\), page A-25](#)
- [debug ip csg, page A-27](#)
- [entries user idle, page A-31](#)

- [flags](#), page A-33
- [idle \(CSG2 content\)](#), page A-36
- [idle \(CSG2 service\)](#), page A-38
- [inservice \(CSG2 content\)](#), page A-40
- [ip \(CSG2 content\)](#), page A-41
- [ip \(iSCSI\)](#), page A-43
- [ip csg billing](#), page A-45
- [ip csg bma](#), page A-46
- [ip csg bma activate](#), page A-48
- [ip csg bma keepalive](#), page A-50
- [ip csg bma local-port](#), page A-51
- [ip csg bma messages](#), page A-53
- [ip csg bma retransmit](#), page A-55
- [ip csg bma retries](#), page A-56
- [ip csg bma window](#), page A-58
- [ip csg case-sensitive](#), page A-59
- [ip csg content](#), page A-60
- [ip csg database](#), page A-62
- [ip csg entries fragment](#), page A-63
- [ip csg entries session user max](#), page A-65
- [ip csg entries user idle](#), page A-67
- [ip csg entries user max](#), page A-69
- [ip csg entries user profile](#), page A-71
- [ip csg ipc crashdump](#), page A-73
- [ip csg ipc keepalive](#), page A-74
- [ip csg ipc retransmit](#), page A-75
- [ip csg ipc retries](#), page A-76
- [ip csg iscsi drain delay](#), page A-77
- [ip csg iscsi drain packet](#), page A-78
- [ip csg iscsi profile](#), page A-80
- [ip csg map](#), page A-81
- [ip csg mode single-tp](#), page A-83
- [ip csg policy](#), page A-84
- [ip csg psd](#), page A-86
- [ip csg psd drain delay](#), page A-88
- [ip csg psd drain packet](#), page A-89
- [ip csg psd keepalive](#), page A-90
- [ip csg psd local-port](#), page A-91

- [ip csg psd margin, page A-93](#)
- [ip csg psd retransmit, page A-94](#)
- [ip csg psd retries, page A-95](#)
- [ip csg psd window, page A-97](#)
- [ip csg quota-server, page A-98](#)
- [ip csg quota-server activate, page A-100](#)
- [ip csg quota-server keepalive, page A-101](#)
- [ip csg quota-server local-port, page A-102](#)
- [ip csg quota-server messages, page A-104](#)
- [ip csg quota-server reassign, page A-105](#)
- [ip csg quota-server retransmit, page A-106](#)
- [ip csg quota-server retries, page A-107](#)
- [ip csg quota-server window, page A-109](#)
- [ip csg radius ack error parse, page A-111](#)
- [ip csg radius correlation, page A-115](#)
- [ip csg radius endpoint, page A-117](#)
- [ip csg radius handoff, page A-120](#)
- [ip csg radius monitor, page A-122](#)
- [ip csg radius monitor nas, page A-124](#)
- [ip csg radius on-off purge, page A-125](#)
- [ip csg radius pod attribute, page A-126](#)
- [ip csg radius pod nas, page A-128](#)
- [ip csg radius pod timeout, page A-130](#)
- [ip csg radius proxy, page A-131](#)
- [ip csg radius reauthorization attribute, page A-135](#)
- [ip csg radius start restart session-id, page A-137](#)
- [ip csg radius stop purge, page A-139](#)
- [ip csg radius userid, page A-141](#)
- [ip csg records format, page A-143](#)
- [ip csg redirect, page A-144](#)
- [ip csg refund, page A-146](#)
- [ip csg replicate, page A-147](#)
- [ip csg report http header, page A-149](#)
- [ip csg report radius attribute, page A-151](#)
- [ip csg report smtp rfc2822, page A-153](#)
- [ip csg report usage, page A-154](#)
- [ip csg report wap actual-pdu, page A-156](#)
- [ip csg service, page A-157](#)

- [ip csg snmp timer, page A-160](#)
- [ip csg subscriber, page A-161](#)
- [ip csg transport-type assign, page A-162](#)
- [ip iscsi target-profile, page A-163](#)
- [map, page A-165](#)
- [match header, page A-167](#)
- [match method, page A-171](#)
- [match url, page A-174](#)
- [meter exclude control sip, page A-178](#)
- [meter exclude mms wap, page A-180](#)
- [meter exclude network-init sip, page A-182](#)
- [meter exclude pause rtsp, page A-184](#)
- [meter exclude svc-idle, page A-186](#)
- [meter include imap, page A-188](#)
- [meter increment, page A-191](#)
- [meter initial, page A-193](#)
- [meter minimum, page A-195](#)
- [mode, page A-197](#)
- [mode tep, page A-198](#)
- [name \(iSCSI\), page A-199](#)
- [next-hop, page A-201](#)
- [owner, page A-203](#)
- [parse length, page A-204](#)
- [parse protocol, page A-205](#)
- [passthrough, page A-207](#)
- [pending, page A-208](#)
- [policy \(CSG2 content\), page A-209](#)
- [port \(iSCSI\), page A-211](#)
- [reauthorization threshold, page A-213](#)
- [reauthorization timeout, page A-215](#)
- [records delay, page A-217](#)
- [records granularity, page A-218](#)
- [records intermediate, page A-220](#)
- [refund, page A-222](#)
- [replicate, page A-223](#)
- [retcode, page A-225](#)
- [sami rate all, page A-227](#)
- [service, page A-228](#)

- [show ip csg](#), page A-229
- [show ip iscsi](#), page A-243
- [show record-storage-module](#), page A-246
- [snmp-server enable traps csg](#), page A-248
- [subscriber-ip http-header forwarded-for](#), page A-250
- [verify confirm](#), page A-252
- [verify enable](#), page A-254
- [vlan \(CSG2 content\)](#), page A-255
- [vrf](#), page A-256

# accounting

To specify accounting and an optional customer string for a CSG2 policy, use the **accounting** command in CSG2 policy configuration mode. To remove accounting for a policy, use the **no** form of this command.

**accounting** [**customer-string** *string*]

**no accounting** [**customer-string** *string*]

## Syntax Description

**customer-string** *string* (Optional) 1- to 16-byte string to be output to the generated accounting records.

## Defaults

The default is no accounting.

## Command Modes

CSG2 policy configuration

## Command History

| Release    | Modification  |
|------------|---|
| 12.4(11)MD | This command was migrated from CSG1.  |
|            | Changes from CSG1: All keywords and arguments except <b>customer-string</b> <i>string</i> were removed. |
| 12.4(15)MD | Support for FTP was added.  |

## Usage Guidelines

This command is required if the CSG2 is to generate call detail records (CDRs) for content that matches the CSG2 policy.

This command is required to enable billing functions (such as CDR generation and prepaid charging) for content that matches a CSG2 policy.

For FTP and Real Time Streaming Protocol (RTSP) accounting, the CSG2 matches prepaid services on the basis of the IP address and port number of the control connection to the FTP or RTSP network IP address.

## Examples

The following example shows how to specify accounting and customer strings for a CSG2 policy:

```
ip csg policy MOVIES
  accounting customer-string MOVIES
```

## Related Commands

| Command                       | Description   |
|-------------------------------|---|
| <a href="#">ip csg policy</a> | Defines a policy for qualifying flows for the CSG2 billing services, and enters CSG2 policy configuration mode. |

# activation

To specify the activation mode for a CSG2 Connection Duration service, use the **activation** command in CSG2 service configuration mode. To restore the default setting, use the **no** form of this command.

**activation** [**automatic** | **user-profile**]

**no activation**

## Syntax Description

|                     |  |
|---------------------|--|
| <b>automatic</b>    | (Optional) Activates the Connection Duration service, unless the billing profile indicates that no service is to be activated.<br><br>If you specify the <b>automatic</b> keyword, the CSG2 activates the Connection Duration service in the subscriber's billing plan automatically, unless the service name is specified with a zero length as the connect service in the billing profile information. The connect service information must be specified in the same message as the subscriber's billing plan.                 |
| <b>user-profile</b> | (Optional) Activates the Connection Duration service only if the billing profile specifies this service as the connect service. This is the default setting.<br><br>If you specify the <b>user-profile</b> keyword, the CSG2 activates the Connection Duration service for a subscriber only if the service name is specified as a connect service in the billing profile information in an authentication, authorization, and accounting (AAA) Access-Accept, an AAA Accounting-Start, or a Quota Server User-Profile Response. |

## Defaults

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

## Command Modes

CSG2 service configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: None. |

## Usage Guidelines

This command requires that the service be configured with **basis second connect**.

## Examples

The following example specifies **automatic** activation for Connection Duration service CONNECT.

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

| Related Commands | Command                        | Description  |
|------------------|--------------------------------|--|
|                  | <a href="#">ip csg service</a> | Configures a CSG2 content billing service, and enters CSG2 service configuration mode. |



# aoc append url

To specify that the CSG2 is to append the original URL to the redirect URL sent by the quota server on a Content Authorization REDIRECT\_URL response for use in Advice of Charge (AoC) URL-rewriting, use the **aoc append url** command in CSG2 service configuration mode. To restore the default setting, use the **no** form of this command.

**aoc append url**

**no aoc append url**

**Syntax Description** This command has no arguments or keywords.

**Defaults** The CSG2 does not append the original URL to the redirect URL.

**Command Modes** CSG2 service configuration

| Command History | Release    | Modification                 |
|-----------------|------------|------------------------------|
|                 | 12.4(11)MD | This command was introduced. |

**Usage Guidelines** Before configuring this command, you must enable AoC by configuring the **aoc enable** command. The CSG2 performs this function only for content parsed as connectionless or connection-oriented wireless application protocol (WAP 1.x). For other protocols, the CSG2 ignores this configuration option.

**Examples** The following example specifies that the CSG2 is to append the original URL to the redirect URL for use in AoC URL-rewriting:

```
ip csg service MOVIES
 aoc enable
 aoc append url
```

| Related Commands | Command                        | Description  |
|------------------|--------------------------------|--|
|                  | <a href="#">aoc confirm</a>    | Configures a token for use in Advice of Charge (AoC) URL-rewriting.                    |
|                  | <a href="#">aoc enable</a>     | Enables Advice of Charge (AoC) URL-rewriting for the CSG2.                             |
|                  | <a href="#">ip csg service</a> | Configures a CSG2 content billing service, and enters CSG2 service configuration mode. |

# aoc confirm

To configure a token for use in Advice of Charge (AoC) URL-rewriting, use the **aoc confirm** command in CSG2 service configuration mode. To remove the token, use the **no** form of this command.

**aoc confirm** *token*

**no aoc confirm**

## Syntax Description

|              |  |
|--------------|--|
| <b>token</b> | <p>A string of up to 15 alphanumeric characters. The string is not case-sensitive.</p> <p>Acceptable characters include alphanumeric characters and any of the following special characters: \$-_.+!*'(),?/:@&amp;=~%. To enter other special characters not listed, use the URL-escape format with the percent sign (%).</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

CSG2 service configuration

## Command History

| Release    | Modification  |
|------------|---|
| 12.4(11)MD | <p>This command was migrated from CSG1.</p> <p>Changes from CSG1:</p> <ul style="list-style-type: none"> <li>• The name of this command changed from <b>aoc confirmation</b> to <b>aoc confirm</b>.</li> <li>• The configuration mode for this command changed from CSG user group configuration to CSG2 service configuration.</li> <li>• The list of supported special characters changed.</li> </ul> |

## Usage Guidelines

Before configuring this command, you must enable AoC by configuring the **aoc enable** command.

URL-rewriting allows a top-off server to append parameters to a URL in order to convey state information to the quota server during a Content Authorization Request. Whenever a Content Authorization Response contains the forward action code, and the URL contains the AoC confirmation token, the token and all trailing characters are removed from the URL before the request is forwarded to the server.

The token is used for HTTP and WAP 1.x content authorization URL-rewriting.

If the token uses the URL-escape format, the redirect URL to which the token is being matched must also use the URL-escape format.

**Examples**

The following example specifies a token for Advice of Charge (AoC) URL-rewriting:

```
ip csg service MOVIES
aoc enable
aoc confirm ?CSG_AOC_OK
```

**Related Commands**

| Command                        | Description   |
|--------------------------------|---|
| <a href="#">aoc append url</a> | Specifies that the CSG2 is to append the original URL to the redirect URL sent by the quota server for use in Advice of Charge (AoC) URL-rewriting. |
| <a href="#">aoc enable</a>     | Enables Advice of Charge (AoC) URL-rewriting for the CSG2.  |
| <a href="#">ip csg service</a> | Configures a CSG2 content billing service, and enters CSG2 service configuration mode.  |

# aoc enable

To enable Advice of Charge (AoC) URL-rewriting for the CSG2, use the **aoc enable** command in CSG2 service configuration mode. To restore the default setting, use the **no** form of this command.

**aoc enable**

**no aoc enable**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The CSG2 does not append the original URL to the redirect URL.

## Command Modes

CSG2 service configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.<br><br>Changes from CSG1: The name of this command changed from <b>authorize content</b> to <b>aoc enable</b> . |

## Usage Guidelines

This command is not valid if the service is configured with **basis second connect**.

If this command is configured, the CSG2 alerts the quota server of a new transaction, and allows it to direct the CSG2 to perform any of the following mutually exclusive actions:

- **DROP**: Instructs the CSG2 to drop all packets for this flow.
- **FORWARD**: Instructs the CSG2 to forward the flow without altering the destination (a weight might be specified).
- **REDIRECT-URL**: Instructs the CSG2 to redirect subscriber requests to the URL provided by the quota server. The CSG2 sends a Layer 7 redirect to the subscriber (for example, HTTP 302 response) that contains the redirect URL. This applies to both HTTP and WAP 1.x protocols.

## Examples

The following example enables AoC URL-rewriting for the CSG2:

```
ip csg service MOVIES
aoc enable
```

## Related Commands

| Command                        | Description   |
|--------------------------------|---|
| <a href="#">aoc append url</a> | Specifies that the CSG2 is to append the original URL to the redirect URL sent by the quota server for use in Advice of Charge (AoC) URL-rewriting. |

| Command                        | Description  |
|--------------------------------|--|
| <a href="#">aoc confirm</a>    | Configures a token for use in Advice of Charge (AoC) URL-rewriting.                    |
| <a href="#">ip csg service</a> | Configures a CSG2 content billing service, and enters CSG2 service configuration mode. |

# basis

To specify the billing basis for a CSG2 content billing service, use the **basis** command in CSG2 service configuration mode. To use the default billing basis, use the **no** form of this command.

```
basis [byte {ip | tcp} | {fixed | second [connect | transaction]}]
```

```
no basis [byte {ip | tcp} | {fixed | second [connect | transaction]}]
```

## Syntax Description

|                    |  |
|--------------------|--|
| <b>byte ip</b>     | (Optional) Billing charge is a function of the IP data volume processed during the subscriber's session. This is the default setting.  |
| <b>byte tcp</b>    | (Optional) Billing charge is a function of the TCP data volume processed during the subscriber's session.<br><br><b>Note</b> Supplemental usage reporting always reports IP bytes, even if the billing basis is configured for TCP bytes.  |
| <b>fixed</b>       | (Optional) Billing charge is a fixed cost, which is deducted each time the first packet for a transaction hits a content-policy pair (that is, deducted for each request).   |
| <b>second</b>      | (Optional) Billing charge is duration-based for the CSG2 service. Unless the <b>connect</b> keyword is also configured, the billing is for the service duration time.  |
| <b>connect</b>     | (Optional) Billing charge is based on connection duration time, not service duration time.<br><br><b>Note</b> If you specify the <b>connect</b> keyword, the <b>balance</b> and <b>consumed</b> fields in the output of the <b>show ip csg users</b> command are updated only when there is a Service Reauthorization Request for new quota. |
| <b>transaction</b> | (Optional) Billing charge is based on transaction duration time.<br><br><b>Note</b> The <b>transaction</b> keyword is valid for Session Initiation Protocol (SIP) only.  |

## Defaults

The default setting is **byte ip** (billing charge is a function of the IP data volume processed).

## Command Modes

CSG2 service configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.<br><br>Changes from CSG1: The <b>exclude mms</b> keyword was removed. |
| 12.4(15)MD | The <b>transaction</b> keyword was added.  |

**Usage Guidelines**

For TCP billing, configuring **basis byte tcp** allows counting of only TCP payload and exclusion of overhead for network retransmission. With this option, the CSG2 excludes IP and TCP headers from volume counts. The byte counting is limited to TCP payload. Retransmitted packets are not counted.

Services that are configured with the **basis second connect** command (that is, for Connection Duration Billing) are subject to the following restrictions:

- Service verification is not supported for Connection Duration services.
- If redirect is to be performed when the Connection Duration service runs out of quota, the URL location to which the CSG2 redirects must map to a policy that does not have accounting configured. This is because all IP sessions mapped to policies with accounting configured (postpaid or prepaid) are dropped when the Connection Duration service has no quota.

For Service Duration Billing:

- When a Service Duration Billing Service is a member of a billing plan, and an accounting definition is in service and downloaded to a CSG2 module, you cannot modify the basis or meter configuration. You are instructed at the console to configure **no inservice** on the downloaded Accounting definitions.
- If a content configuration is included in a service configured for **basis second**, the CSG2 restricts the content idle timeout to less than or equal to the service idle timeout for the service. The content idle time is not included in the last billable time for the service.
- The CSG2 does not allow you to specify weights for Service Duration Billing.

**Note**

We recommend that you first remove the service from each billing plan, make the basis changes, and add it back to each billing plan. If you delete it, the service is automatically removed from each billing plan, and you must add it back to each plan after configuring it.

To enable Connection Duration Billing for a service, configure the service name as a service under one or more billing plans in CSG2 billing configuration mode, then enter the **basis second connect** command in CSG2 service configuration mode.

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

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

**Examples**

The following example shows how to specify fixed billing for the CSG2 service MOVIES:

```
ip csg service MOVIES
  basis fixed
```

The following commands are used to configure Service Duration Billing for the OFF\_NET service.

```
ip csg service OFF_NET
  basis second
```

**Related Commands**

| Command                             | Description   |
|-------------------------------------|---|
| <code>ip csg service</code>         | Configures a CSG2 content billing service, and enters CSG2 service configuration mode.                            |
| <code>meter exclude svc-idle</code> | Excludes timers from the usage calculation.   |
| <code>meter include imap</code>     | Specifies which Internet Message Access Protocol (IMAP) bytes are billed for when doing prepaid debits.           |
| <code>meter increment</code>        | Specifies the increments for debiting quota upon completion of a service configured for Service Duration Billing. |



# block

To force the CSG2 to drop packets that do not match a configured billing policy, use the **block** command in CSG2 content configuration mode. To restore the default behavior, enabling the CSG2 to forward the packets without billing, use the **no block** form of this command.

**block**

**no block**

**Syntax Description** This command has no arguments or keywords.

**Defaults** None

**Command Modes** CSG2 content configuration

| Command History | Release    | Modification  |
|-----------------|------------|---|
|                 | 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: <ul style="list-style-type: none"> <li>The name of this command changed from <b>ip csg block</b> to <b>block</b>.</li> <li>The configuration mode for this command changed from global to CSG2 content configuration.</li> </ul> |

**Usage Guidelines** By default, if packets do not match any billing policy, the CSG2 forwards the packets without billing. This command causes the CSG2 to drop the packets instead.

**Examples** The following example shows how to force the CSG2 to drop packets that do not match any billing policy:

```
ip csg content MOVIES
  block
```

| Related Commands | Command                        | Description  |
|------------------|--------------------------------|--|
|                  | <a href="#">ip csg content</a> | Configures content for CSG2 services, and enters CSG2 content configuration mode.                                  |
|                  | <a href="#">ip csg policy</a>  | Defines a policy for qualifying flows for the CSG2 accounting services, and enters CSG2 policy configuration mode. |
|                  | <a href="#">parse length</a>   | Defines the maximum number of Layer 7 bytes that the CSG2 is to parse when attempting to assign a policy.          |

# class

To specify a service class value, use the **class** command in CSG2 service configuration mode. To remove the service class value, use the **no class** form of this command.

**class** *value*

**no class** *value*

## Syntax Description

**value** Specifies a value in the range 1 to 255.

## Defaults

None

## Command Modes

CSG2 service configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: None. |

## Usage Guidelines

The **class** command is used with fixed-record format to identify a service class value. This value is opaque to the CSG2 and has meaning only for the administrator. It is reported as tariff-class in fixed-record format call detail records (CDRs).

## Examples

The following example specifies a class value for the service:

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

## Related Commands

| Command                                      | Description  |
|--|--|
| <a href="#">ip csg service</a>               | Configures a CSG2 content billing service, and enters CSG2 service configuration mode. |
| <a href="#">ip csg transport-type assign</a> | Classifies data traffic on the basis of its access path.                               |
| <a href="#">mode</a>                         | Specifies the mode for a CSG2 billing plan.  |
| <a href="#">ip csg records format</a>        | Specifies <b>variable</b> or <b>fixed</b> CDR format.                                  |
| <a href="#">owner</a>                        | Specifies an identifier or name for a service owner.                                   |

# clear ip csg

To clear the CSG2, use the **clear ip csg** command in privileged EXEC mode.

```
clear ip csg {counters | sessions user [application] [ip-address ip-mask] |
user [all | ip ip-address {global | vrf vrf-name}]}
```

| Syntax Description          |  |  |
|-----------------------------|--|--|
| <b>counters</b>             |  | Clears all CSG2 cumulative counters and statistics, but not CSG2 “state” counters. For example, counters such as “current number of sessions” are not cleared.   |
| <b>sessions user</b>        |  | Closes all subscriber sessions.  |
| <i>application</i>          |  | (Optional) Closes subscriber sessions for only the specified application: <ul style="list-style-type: none"> <li>• <b>ftp</b>—Closes FTP subscriber sessions.</li> <li>• <b>http</b>—Closes HTTP subscriber sessions.</li> <li>• <b>imap</b>—Closes IMAP subscriber sessions.</li> <li>• <b>other</b>—Closes other subscriber sessions.</li> <li>• <b>pop3</b>—Closes POP3 subscriber sessions.</li> <li>• <b>rtsp</b>—Closes RTSP subscriber sessions.</li> <li>• <b>smtp</b>—Closes SMTP subscriber sessions.</li> <li>• <b>wap</b>—Closes WAP subscriber sessions.</li> </ul> |
| <i>ip-address ip-mask</i>   |  | (Optional) Closes subscriber sessions for only the specified subscriber IP address and subscriber IP address mask.<br><br>Specify IP address 0.0.0.0 to close subscriber sessions for all subscriber IP addresses.<br><br>Specify IP address mask 0 to close subscriber sessions for all subscriber IP address masks.  |
| <b>user</b>                 |  | Closes all subscriber entries in the CSG2 User Table.  |
| <b>all</b>                  |  | (Optional) Closes all subscriber entries in the CSG2 User Table.   |
| <b>ip</b> <i>ip-address</i> |  | (Optional) Closes only those subscriber entries in the CSG2 User Table that are associated with the specified IP address.  |
| <b>global</b>               |  | (Optional) Closes all subscriber entries that are associated with the specified IP address.  |
| <b>vrf</b> <i>vrf-name</i>  |  | (Optional) Closes only those subscriber entries that are associated with the specified IP address and that are associated with the specified Virtual Routing and Forwarding (VRF) table.   |

**Defaults** None

**Command Modes** Privileged EXEC

| Command History | Release    | Modification                      |
|-----------------|------------|-----------------------------------|
|                 | 12.4(11)MD | This command was introduced.      |
|                 | 12.4(15)MD | The <b>ftp</b> keyword was added. |

**Usage Guidelines** By default, the CSG2 deletes 1000 User Table entries per second in response to the **clear ip csg user all** command. To specify a different deletion rate, use the **ip csg radius on-off purge** command in global configuration mode.

**Examples** The following example clears all counters and statistics for the CSG2:

```
clear ip csg counters
```

The following example clears all subscriber entries from the CSG2 User Table that are associated with IP address **1.2.3.4**:

```
clear ip csg user ip 1.2.3.4
```

The following example clears all subscriber entries from the CSG2 User Table that are associated with IP address **1.2.3.4** and that are also associated with VRF table **AAA**:

```
clear ip csg user ip 1.2.3.4 vrf AAA
```

The following example clears all sessions for application **http** and IP address mask **1.2.3.4/32**:

```
clear ip csg sessions user http 1.2.3.4/32
```

| Related Commands | Command                     | Description                          |
|------------------|-----------------------------|--------------------------------------|
|                  | <a href="#">show ip csg</a> | Displays information about the CSG2. |

# clear ip iscsi statistics

To clear current iSCSI statistics, use the **clear ip iscsi statistics** command in privileged EXEC configuration mode.

**clear ip iscsi statistics**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC

| Command History | Release    | Modification                 |
|-----------------|------------|------------------------------|
|                 | 12.4(15)MD | This command was introduced. |

**Examples** The following example clears iSCSI-related statistics:

```
clear ip iscsi statistics
```

| Related Commands | Command                       | Description                           |
|------------------|-------------------------------|---------------------------------------|
|                  | <a href="#">show ip iscsi</a> | Displays information about the iSCSI. |

# clear record-storage-module stats

To clear current record storage module (RSM) statistics, use the **clear record-storage-module stats** command in privileged EXEC configuration mode.

**clear record-storage-module stats**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC

| Command History | Release    | Modification                 |
|-----------------|------------|------------------------------|
|                 | 12.4(15)MD | This command was introduced. |

**Examples** The following example clears RSM-related statistics:

```
clear record-storage-module stats
```

| Related Commands | Command                                    | Description   |
|------------------|--|---|
|                  | <a href="#">show record-storage-module</a> | Displays information about the record storage module (RSM). |

# client-group (CSG2 content)

To reference a standard access list that is part of a CSG2 content, use the **client-group** command in CSG2 content configuration mode. To delete the reference, use the **no** form of this command.

**client-group** { *std-access-list-number* | *std-access-list-name* }

**no client-group** { *std-access-list-number* | *std-access-list-name* }

| Syntax Description |                               |  |
|--------------------|-------------------------------|--|
|                    | <i>std-access-list-number</i> | Standard IP access list number. The ranges are from 1 to 99 and from 1300 to 1999. |
|                    | <i>std-access-list-name</i>   | Standard access list name.   |

**Defaults** All subscribers can access the content.

**Command Modes** CSG2 content configuration

| Command History | Release    | Modification   |
|-----------------|------------|--|
|                 | 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: <ul style="list-style-type: none"> <li>The configuration mode for this command changed from CSG policy configuration to CSG2 content configuration.</li> <li>The range for the <i>std-access-list-number</i> argument increased from 1300 to 1999.</li> </ul> |

**Usage Guidelines** The **client-group** command is used to qualify subscribers for the CSG2 content. The conditions specified in the referenced access list must be true in order for the flows to be processed by the CSG2 content. If the conditions are not true, the CSG2 determines this to be a content mismatch, and normal content match processing continues (that is, the CSG2 tries to match a less specific content). If no contents are matched, the CSG2 does not process the flow (that is, the CSG2 blocks this traffic flow).

If you reference an access list that includes a **deny** statement, and that **deny** statement is matched, then the CSG2 treats the traffic as a content mismatch and normal content processing continues, allowing the traffic to match another less specific content. For example, in the following configuration, packets from from IP address 1.1.1.1 do not match CONTENT1, but they do match CONTENT2:

```
ip csg content CONTENT1
 ip any
  client-group 99
  inservice
!
ip csg content CONTENT2
 ip any
  inservice
!
```

```
access-list 99 deny 1.1.1.1
access-list 99 permit any
```

You can use next-hop with client groups as long as a given client group is always sent to the same next hop. You cannot send a given client group to two or more different next hops based on a content.

The CSG2 searches contents with the same IP and VLAN configuration, but different client groups, in numerical order. For example, given two contents with the same IP/VLAN configuration, one referencing client group 4 and the other client group 7, the CSG2 matches the content that references client group 4.

### Examples

The following example shows how to reference client group 44 for the CSG2 content MOVIES:

```
ip csg content MOVIES
  client-group 44
```

### Related Commands

| Command                        | Description   |
|--------------------------------|---|
| <a href="#">ip csg content</a> | Configures content for CSG2 services, and enters CSG2 content configuration mode. |
| <a href="#">next-hop</a>       | Defines a next-hop IP address.  |



## content (CSG2 service)

To configure a content and policy as a member of a CSG2 billing service, and optionally to assign a weight to this content, use the **content** command in CSG2 service configuration mode. To remove a content name from the billing service, use the **no** form of this command.

```
content content-name policy policy-name [weight weight-value]
```

```
no content content-name policy policy-name
```

### Syntax Description

|                                   |  |
|-----------------------------------|--|
| <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 CSG2 changes all letters to uppercase), numbers, and any special characters. |
| <b>policy</b> <i>policy-name</i>  | Name of a configured policy to apply to the content for this service.  |
| <b>weight</b> <i>weight-value</i> | (Optional) Number of quadrans to deduct for each transaction. The range is from 0 to 32767. The default <i>weight-value</i> is 1 quadrans.   |

### Defaults

The default *weight-value* is 1 quadrans.

### Command Modes

CSG2 service configuration

### Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.<br><br>Changes from CSG1: The <i>weight-name</i> argument was replaced with the <i>weight-value</i> argument. |

### Usage Guidelines

You must configure a policy before configuring this command.

Content can reference more than one policy. Therefore, you can have multiple **content** commands with the same *content-name* argument, but different *policy-name* arguments.

To make a specific content free, specify a *weight-value* of 0.

### Examples

The following example shows how to configure content for the CSG2 service MOVIES. In this example:

- Policy MOVIES\_COMEDY is applied to content MOVIES\_COMEDY.
- Policy MOVIES\_ACTION is applied to content MOVIES\_ACTION.
- Content MOVIES\_ACTION is given a billing weight of 2.

```
ip csg service MOVIES
content MOVIES_COMEDY policy MOVIES_COMEDY
content MOVIES_ACTION policy MOVIES_ACTION weight 2
```

| Related Commands | Command                        | Description  |
|------------------|--------------------------------|--|
|                  | <a href="#">ip csg content</a> | Configures content for CSG2 services, and enters CSG2 content configuration mode.                                  |
|                  | <a href="#">ip csg policy</a>  | Defines a policy for qualifying flows for the CSG2 accounting services, and enters CSG2 policy configuration mode. |
|                  | <a href="#">ip csg service</a> | Configures a CSG2 content billing service, and enters CSG2 service configuration mode.                             |

## debug ip csg

To set the flags to obtain debugging output for the various CSG2 components, use the **debug ip csg** command in privileged EXEC mode. To disable the debugging feature, use the **no** form of this command.

```
debug ip csg {all | acl number [vrf vrf-name | global] | configuration sync | content | crashinfo |
error | frag | ftp | gtp {any | bma [priority] | ipc | psd | quota-server [priority]} | http [detail]
| imap | interm | ipc [detail] | iscsi [detail] | other | packet [dump] | policy | pop3 |
psd [detail] | qs [detail] | radius [detail] | replicate | rtsp [detail] | service [detail | ha] |
session {event | state [detail]} | sip | smtp | stats | tlv | udb [xml] | users | wap [detail] | xml}
```

```
no debug ip csg {all | acl number [vrf vrf-name | global] | configuration sync | content | crashinfo |
error | frag | ftp | gtp {any | bma [priority] | ipc | psd | quota-server [priority]} | http [detail]
| imap | interm | ipc [detail] | iscsi [detail] | other | packet [dump] | policy | pop3 |
psd [detail] | qs [detail] | radius [detail] | replicate | rtsp [detail] | service [detail | ha] |
session {event | state [detail]} | sip | smtp | stats | tlv | udb [xml] | users | wap [detail] | xml}
```

### Syntax Description

|                           |   |
|---------------------------|---|
| <b>all</b>                | Generates debugging output for all CSG2 components.   |
| <b>acl number</b>         | Generates debugging output for all subscribers in a simple access control list (ACL).   |
| <b>vrf vrf-name</b>       | (Optional) Generates debugging output for the Virtual Routing and Forwarding (VRF) table with the ACL.  |
| <b>global</b>             | (Optional) Generates debugging output for the default routing table with the ACL.   |
| <b>configuration sync</b> | Generates debugging output for the configuration synchronization component.   |
| <b>content</b>            | Generates debugging output for the CSG2 content debug messages, indicating the results of the content match algorithm. This output is filtered if <b>debug ip csg acl</b> has been configured.  |
| <b>crashinfo</b>          | Generates debugging output for the crash information component.   |
| <b>error</b>              | Generates debugging output for situations that might indicate a problem.  |
| <b>frag</b>               | Generates debugging output for the CSG2 fragment database.  |
| <b>ftp</b>                | Generates debugging output for the FTP component.   |
| <b>gtp any</b>            | Generates debugging output for the general packet radio service (GPRS) tunneling protocol (GTP) component's interaction with components other than the Billing Mediation Agent (BMA), the Interprocessor Communication (IPC) component, the Persistent Storage Device (PSD) component, or the quota server. |
| <b>gtp bma [priority]</b> | Generates debugging output for the GTP component's interaction with the BMA.<br><br>To generate detailed debugging output for the GTP component's interaction with a specific BMA, specify the quota server's <i>priority</i> .   |
| <b>gtp ipc</b>            | Generates debugging output for the GTP component's interaction with the IPC component.  |
| <b>gtp psd</b>            | Generates debugging output for the GTP component's interaction with the PSD component.  |

|  |   |
|--|---|
| <b>gtp quota-server</b><br>[ <i>priority</i> ] | Generates debugging output for the GTP component's interaction with the quota server.<br><br>To generate detailed debugging output for the GTP component's interaction with a specific quota server, specify the quota server's <i>priority</i> .   |
| <b>http [detail]</b>                           | Generates debugging output for the HTTP component.<br><br>To generate detailed debugging output for the HTTP component, specify the optional <b>detail</b> keyword.   |
| <b>imap</b>                                    | Generates debugging output for the Internet Message Access Protocol (IMAP) component.   |
| <b>interm</b>                                  | Generates debugging output for the intermediate billing component.  |
| <b>ipc [detail]</b>                            | Generates debugging output for the IPC component.<br><br>To generate detailed debugging output for the IPC component, specify the optional <b>detail</b> keyword.   |
| <b>iscsi [detail]</b>                          | Generates debugging output for the iSCSI component.<br><br>To generate detailed debugging output for the iSCSI component, specify the optional <b>detail</b> keyword.   |
| <b>mail</b>                                    | Generates debugging output for the mail component.  |
| <b>other</b>                                   | Generates debugging output for other components.  |
| <b>packet [dump]</b>                           | Generates debugging output for e-mail packets.<br><br>To generate a dump of all inbound packets in hexadecimal format, specify the optional <b>dump</b> keyword.  |
| <b>policy</b>                                  | Generates debugging output for the policy component.  |
| <b>pop3</b>                                    | Generates debugging output for the Post Office Protocol, version 3 (POP3) component.  |
| <b>psd [detail]</b>                            | Generates debugging output for the PSD component.<br><br>To generate detailed debugging output for the PSD component, specify the optional <b>detail</b> keyword.   |
| <b>qs [detail]</b>                             | Generates debugging output for the quota server component.<br><br>To generate detailed debugging output for the quota server component, including all packets to and from the quota server in both hexadecimal and ASCII formats, specify the optional <b>detail</b> keyword.   |
| <b>radius [detail]</b>                         | Generates debugging output for the RADIUS component.<br><br>To generate detailed debugging output for the RADIUS component, specify the optional <b>detail</b> keyword.   |
| <b>replicate</b>                               | Generates debugging output for the high availability (HA) component, including stateful messages as well as stateless transitions and the dump/bulk synchronization processes.<br><br>You can also use the following commands to debug the redundancy facility (RF), the RF for Interdevice redundancy (RF Interdev), and the Hot Standby Router Protocol (HSRP): <ul style="list-style-type: none"> <li>• <b>debug redundancy progression</b></li> <li>• <b>debug redundancy interdev</b></li> <li>• <b>debug standby</b></li> </ul> |

|                               |  |
|-------------------------------|--|
| <b>service [detail]</b>       | <p>Generates debugging output for the subscriber services component.</p> <p>To generate detailed debugging output for the subscriber services component, specify the optional <b>detail</b> keyword.</p> <p><b>Note</b> If you specify the <b>detail</b> keyword, the CSG2 might generate debugging output for every packet mapped to the service.</p> |
| <b>service [ha]</b>           | <p>Generates debugging output for the subscriber services component.</p> <p>To generate debugging output for high availability (HA) replication for the subscriber services component, specify the optional <b>ha</b> keyword.</p>   |
| <b>session event</b>          | Generates debugging output for the session event component.  |
| <b>session state [detail]</b> | <p>Generates debugging output for the session state component.</p> <p>To generate detailed debugging output for the session state component, specify the optional <b>detail</b> keyword.</p>   |
| <b>rtsp [detail]</b>          | <p>Generates debugging output for the Real Time Streaming Protocol (RTSP) component.</p> <p>To generate detailed debugging output for the RTSP component, specify the optional <b>detail</b> keyword.</p>  |
| <b>sip</b>                    | Generates debugging output for the Session Initiation Protocol (SIP) component.  |
| <b>smtp</b>                   | Generates debugging output for the Simple Mail Transfer Protocol (SMTP) component.   |
| <b>stats</b>                  | Generates debugging output for the statistics component.   |
| <b>tlv</b>                    | Generates debugging output for the Tag-Length-Values (TLVs) component.   |
| <b>udb [xml]</b>              | <p>Generates debugging output for the User Database (UDB) component.</p> <p>To generate debugging output for only the XML component, specify the optional <b>xml</b> keyword.</p>  |
| <b>users</b>                  | Generates debugging output for the subscriber component.   |
| <b>wap [detail]</b>           | <p>Generates debugging output for the wireless application protocol (WAP) component.</p> <p>To generate detailed debugging output for the WAP component, specify the optional <b>detail</b> keyword.</p>   |

**Defaults**

The CSG2 generates no debugging output.

**Command Modes**

Privileged EXEC

| Command History | Release    | Modification   |
|-----------------|------------|--|
|                 | 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: <ul style="list-style-type: none"> <li>The <b>acl number, configuration sync, detail, dump, error, frag, global, ha, http, interm, ipc, mail, other, packet, priority, qs, replicate, service, session event, session state, stats</b>, and <b>vrf vrf-name</b>, keywords and arguments were added.</li> <li>The <b>any, bma, ipc, psd</b>, and <b>quota-server</b> keywords were added for the <b>gtp</b> keyword.</li> <li>The <b>agent, api, cpu, module number, quota, prepaid, record storage slot</b>, and <b>timer</b> keywords and arguments were removed.</li> </ul> |
|                 | 12.4(15)MD | The <b>crashinfo, ftp, iscsi, mail</b> , and <b>sip</b> keywords were added.   |

### Usage Guidelines

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

Restrict the output of other CSG2 debugging commands to subscribers specified in the ACL.

Once the debug flags are set, they are automatically sent to the CSG2 cards when a configuration is downloaded. Similarly, changes in the debug settings are sent to the CSG2 cards that are being debugged.

Generating debugging output for ACL (that is, configuring the **acl** keyword) disables all of the following types of debugging:

- Configuration
- Error
- GTP
- IPC
- PSD
- RADIUS
- Replicate
- Statistics
- TLV
- UDB

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



#### Note

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

### Examples

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

```
debug ip csg rtsp
debug ip csg udb
```

# entries user idle

To set the time after which entries for idle subscribers are deleted from the CSG2 User Table, use the **entries user idle** command in CSG2 billing configuration mode. To use the default settings, use the **no** form of this command.

**entries user idle** *duration* [**pod**]

**no entries user idle**

## Syntax Description

|                             |   |
|-----------------------------|---|
| <b>idle</b> <i>duration</i> | Number of seconds after which entries for idle subscribers are deleted from the CSG2 User Table. The range is from 0 (entries never idle out) to 2147483647. The default setting is 0 (entries never idle out). |
| <b>pod</b>                  | (Optional) Specifies whether the CSG2 is to send the RADIUS Packet of Disconnect message when an entry idles out.   |

## Defaults

The default idle duration is 0 seconds, and the CSG2 does not send the RADIUS Packet of Disconnect message when an entry idles out.

## Command Modes

CSG2 billing configuration

## Command History

| Release    | Modification  |
|------------|---|
| 12.4(11)MD | This command was migrated from CSG1.<br><br>Changes from CSG1: The name of this command changed from <b>entries idle (CSG2 billing)</b> to <b>entries user idle</b> . |

## Usage Guidelines

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

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

- You can set the entry idle timer either globally, using the **ip cs g entries user idle** command in global configuration mode, or in each billing plan, using the **entries user idle** command. If you do not set the timer in the billing plan, the CSG2 uses the global timer. That is, if there is an entry idle timer value in the billing plan, it is used; otherwise, if there is a global entry idle timer value configured, it is used.
- If set, the idle timer starts when there are no billable sessions, and restarts whenever a RADIUS Accounting Start or an Interim Accounting message is received. The timer stops when a billable session is started.
- If you do not specify the **pod** keyword, the CSG2 deletes the idle entry when the timer expires.
- If you specify the **pod** keyword, and if RADIUS Packet of Disconnect (PoD) is configured for the CSG2, the CSG2 sends a PoD message when the idle timer expires. The CSG2 deletes the idle entry when the PoD message is ACKed, NAKed, or when all retries have been sent.

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

---

**Examples**

The following example shows how to specify an entry idle time of 1 hour for CSG2 billing plan REGULAR:

```
ip csg billing REGULAR
  entries user idle 3600
```

---

**Related Commands**

| Command                                     | Description   |
|---|---|
| <a href="#">ip csg billing</a>              | Defines a CSG2 billing plan, and enters CSG2 billing configuration mode.  |
| <a href="#">ip csg entries user idle</a>    | Specifies how long the CSG2 is to retain entries in the CSG2 User Table.  |
| <a href="#">ip csg radius pod attribute</a> | Specifies the RADIUS attributes to be copied from the RADIUS Start message and sent to the NAS in the PoD message.  |
| <a href="#">ip csg radius pod nas</a>       | Specifies the NAS port to which the CSG2 is to send the PoD message, and the key to use in calculating the Authenticator.                                     |
| <a href="#">ip csg radius pod timeout</a>   | 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. |
| <a href="#">ip csg radius proxy</a>         | Specifies that the CSG2 is to be a proxy for RADIUS messages.   |
| <a href="#">mode</a>                        | Specifies the mode for a CSG2 billing plan.   |
| <a href="#">service</a>                     | Associates a service with a CSG2 billing plan.  |



# flags

To specify IP, TCP, or wireless application protocol (WAP) flag bit masks and values for CSG2 Prepaid Error Reimbursement, use the **flags** command in CSG2 refund configuration mode. To remove the flags, use the **no** form of this command.

**flags** {**ip** *mask* | **tcp** *mask* | **wap**} *value*

**no flags** {**ip** *mask* | **tcp** *mask* | **wap**} *value*

| Syntax Description |   |
|--------------------|---|
| <b>ip</b>          | All IP protocol connections other than TCP or WAP.  |
| <b>tcp</b>         | TCP connections   |
| <b>wap</b>         | WAP connections.  |
| <i>mask</i>        | The <i>mask</i> for an <b>ip</b> or <b>tcp</b> 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 <b>ip</b> , <b>tcp</b> , or <b>wap</b> flag, which must match that reported to the BMA for connection termination. <ul style="list-style-type: none"> <li>For an <b>ip</b> or <b>tcp</b> flag, the range for <i>value</i> is from 0x00 to 0xFF.</li> <li>For a <b>wap</b> flag, <i>value</i> can be 0x00, 0x01, 0x02, or 0x04.</li> </ul> |

**Defaults** None

**Command Modes** CSG2 refund configuration

| Command History | Release    | Modification   |
|-----------------|------------|--|
|                 | 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: None. |

**Usage Guidelines** The CSG2 supports flag-based refunding for all protocols.

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

- 0x01: Connection initiator.
  - 0: The connection was initiated by the subscriber. The source address is associated with the user ID.
  - 1: The connection was initiated by the network. The destination address is associated with the user ID.

- 0x80: Connection terminated because of lack of authorization failure.
  - 0: The connection was not terminated as a result of an authorization failure.
  - 1: The connection was terminated as a result of an authorization failure.
- 0x7E: Reserved.

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

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

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

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

**Examples**

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

```
ip csg refund COMPANY-REFUND
  flags tcp 43 00
  flags ip 80 80
  flags wap 04
```

**Related Commands**

| Command                       | Description   |
|-------------------------------|---|
| <a href="#">ip csg refund</a> | Specifies the CSG2 refund policy to apply to the various services, and enters CSG2 refund configuration mode.     |
| <a href="#">retcode</a>       | Specifies the range of application return codes for which the CSG2 refunds quota for Prepaid Error Reimbursement. |

## idle (CSG2 content)

To specify the minimum amount of time that the CSG2 maintains an idle content connection, use the **idle** command in CSG2 content configuration mode. To restore the default idle duration value, use the **no** form of this command.

**idle** *duration*

**no idle** *duration*

### Syntax Description

|                 |   |
|-----------------|---|
| <i>duration</i> | Content idle timer duration in seconds. If no packets are received on a content connection for more than <i>duration</i> seconds, the CSG2 assumes the connection is idle and ends the connection.<br><br>The range is from 4 to 65535. The default is 300. |
|-----------------|---|

### Defaults

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

### Command Modes

CSG2 content configuration

### Command History

| Release    | Modification  |
|------------|---|
| 12.4(11)MD | This command was migrated from CSG1.<br><br>Changes from CSG1: The default setting for the <i>duration</i> argument changed from 3600 seconds to 300 seconds. |

### Usage Guidelines

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

For RTSP, do not set the idle timer duration to less than 60 seconds.

When using HTTP as the transport for RTSP, the control connection is used sparingly and might time out, causing the stream to become unresponsive. This occurs because the subscriber opens two TCP connections, one for the main content and one for control. The subscriber uses the control connection sparingly, which can cause the connection to time out. To prevent this problem, ensure that the content idle timer has a duration of at least 60 seconds (the default setting is 300 seconds). This is not an issue when using UDP or TCP as the transport.

The CSG2 tracks usage on a per-session basis. User Datagram Protocol (UDP) does not have an end-of-session indicator and simply idles out. For that reason, for UDP and wireless application protocol 1.x (WAP 1.x), setting the content idle timer to a low value (for example, 30) allows the CSG2

to quickly recognize that a session has ended and to generate billing records accordingly. Other service-level features of the CSG2 that count sessions (such as passthrough mode and service-level CDRs) are similarly affected by the content idle timer setting.

For TCP, the CSG2 does not send a reset (RST) until a packet is received.

For a service configured with **basis second**, make sure the idle timeout value for the content configuration, set using the **idle** command in CSG2 content configuration mode, does not exceed the service idle timeout value, set using the **idle** command in CSG2 service configuration mode. Examples of these contents include:

- Non-TCP contents
- TCP contents with policies for HTTP or WAP 2.0 where the subscriber or network does not close the TCP connection at the end of the transaction

### Examples

The following example shows how to configure a 120-second idle timer for the CSG2 content MOVIES\_COMEDY:

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

### Related Commands

| Command                             | Description   |
|-------------------------------------|---|
| <a href="#">idle (CSG2 service)</a> | Specifies the minimum amount of time that the CSG2 maintains a service with no subscriber sessions. |
| <a href="#">ip csg content</a>      | Configures content for CSG2 services, and enters CSG2 content configuration mode.                   |
| <a href="#">pending</a>             | Sets the pending connection timeout.  |

## idle (CSG2 service)

To specify the minimum amount of time that the CSG2 maintains a service with no subscriber sessions, use the **idle** command in CSG2 service configuration mode. To restore the default idle duration value, use the **no** form of this command.

**idle** *duration*

**no idle** *duration*

### Syntax Description

|                 |  |
|-----------------|--|
| <i>duration</i> | Service idle timer duration, in seconds. The timer begins when there are no sessions. If a subscriber's quota for a service is unused for more than <i>duration</i> seconds, the CSG2 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

CSG2 service configuration

### Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: None. |

### Usage Guidelines

For services configured with **basis second**, make sure the idle timeout value for the content configurations, set using the **idle** command in CSG2 content configuration mode, does not exceed the service idle timeout value, set using the **idle** command in CSG2 service configuration mode. Examples of these contents include:

- Non-TCP contents
- TCP contents with policies for HTTP or WAP 2.0 where the subscriber or network does not close the TCP connection at the end of the transaction

If a subscriber's quota for a service is unused for more than the service idle timer duration, the CSG2 assumes that the service is idle and sends a ServiceStop to free up quota.

For RTSP, do not set the idle timer duration to less than 60 seconds.

### Examples

The following example shows how to configure a 120-second idle timer for the CSG2 service MOVIES:

```
ip csg service MOVIES
idle 120
```

| Related Commands | Command                             | Description  |
|------------------|-------------------------------------|--|
|                  | <a href="#">idle (CSG2 content)</a> | Specifies the minimum amount of time that the CSG2 maintains an idle content connection. |
|                  | <a href="#">ip csg service</a>      | Configures a CSG2 content billing service, and enters CSG2 service configuration mode.   |
|                  | <a href="#">pending</a>             | Sets the pending connection timeout.   |

## inservice (CSG2 content)

To activate the content service on each CSG2, use the **inservice** command in CSG2 content configuration mode. To suspend the content service, use the **no** form of this command.

**inservice**

**no inservice**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** The default value is **no inservice**.

---

**Command Modes** CSG2 content configuration

---

| Command History | Release    | Modification   |
|-----------------|------------|--|
|                 | 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: None. |

---



---

**Usage Guidelines** When you activate the **inservice** command, the CSG2 verifies the parameters semantically. If the CSG2 detects an error, the command fails.

---

**Examples** The following example shows how to place the CSG2 content MOVIES\_COMEDY in service:

```
ip csg content MOVIES_COMEDY
inservice
```

---

| Related Commands | Command                        | Description   |
|------------------|--------------------------------|---|
|                  | <a href="#">ip csg content</a> | Configures content for CSG2 services, and enters CSG2 content configuration mode. |

---



## ip (CSG2 content)

To define the subset of Layer 3 and Layer 4 flows that can be processed by the CSG2 accounting services, use the **ip** command in CSG2 content configuration mode. To delete the flow definition, use the **no** form of this command.

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

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

### Syntax Description

|                         |  |
|-------------------------|--|
| <b>any</b>              | 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>          | (Optional) Mask that identifies the network for which Layer 3 and Layer 4 flows can be processed.<br><br>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.<br><br>The default network mask is 255.255.255.255 or /32, which means flows to a specific host can be processed.   |
| <b>any</b>              | (Optional) All protocol types of Layer 3 and Layer 4 flows can be processed. This is the default setting.  |
| <i>protocol</i>         | (Optional) Protocol type of Layer 3 and Layer 4 flows that can be processed: <ul style="list-style-type: none"> <li><b>any</b>—Flows of any protocol type can be processed. This is the default setting.</li> <li><b>tcp</b>—Only TCP flows can be processed.</li> <li><b>udp</b>—Only User Datagram Protocol (UDP) flows can be processed.</li> <li><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 <b>any</b>.</li> </ul> |
| <i>port-number</i>      | (Optional) Specifies the beginning of the range of port numbers for which Layer 3 and Layer 4 flows can be processed. The range is 0 to 65535, where 0 indicates that flows from any port number can be processed.   |
| <i>last-port-number</i> | (Optional) Specifies the end of the range of port numbers, The range is <i>port-number</i> to 65535. If you are specifying a single port number, do not specify <i>last-port-number</i> .  |

### Defaults

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

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

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

The CSG2 parses port numbers only when processing TCP and UDP traffic. For all other protocols, the CSG2 does not track the layer 4 port.

**Command Modes** CSG2 content configuration

| Command History | Release    | Modification   |
|-----------------|------------|--|
|                 | 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: None. |

**Usage Guidelines** This command is required to place content in service.

UDP ports 9200 and 9201 are well-known Wireless Session Protocol (WSP) and Wireless Transaction Protocol (WTP) wireless application protocol (WAP) ports. When a policy with **parse protocol wap** is associated with a content, use even-numbered UDP ports to designate WSP traffic, and use odd-numbered ports to designate WTP traffic.

Although you can use this command to specify a port number for Layer 3 content (**ip any any port-number**), the CSG2 does not support Layer 3 content rules. The CSG2 ignores the specified port number, and the **show ip csg content** command displays the port number as 0.

**Examples** The following example shows how to specify that, for content MOVIES\_COMEDY, only flows for IP address 172.18.45.0/24 and TCP port 8080 are to be processed by the CSG2 accounting services:

```
ip csg content MOVIES_COMEDY
ip 172.18.45.0/24 tcp 8080
```

| Related Commands | Command                        | Description   |
|------------------|--------------------------------|---|
|                  | <a href="#">ip csg content</a> | Configures content for CSG2 services, and enters CSG2 content configuration mode. |

# ip (iSCSI)

To specify the IP address of an iSCSI target in the target interface profile on the CSG2, use the **ip** command in iSCSI configuration mode. To remove the IP address configuration, use the **no ip** form of the command.

**ip** *ip-address*

**no ip** *ip-address*

|                           |                   |                                 |
|---------------------------|-------------------|---------------------------------|
| <b>Syntax Description</b> | <i>ip-address</i> | IP address of the iSCSI target. |
|---------------------------|-------------------|---------------------------------|

|                        |                                |
|------------------------|--------------------------------|
| <b>Command Default</b> | No default behavior or values. |
|------------------------|--------------------------------|

|                      |                     |
|----------------------|---------------------|
| <b>Command Modes</b> | iSCSI configuration |
|----------------------|---------------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|------------------------|----------------|------------------------------|
|                        | 12.4(15)MD     | This command was introduced. |

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | Only one target can be defined per profile. |
|-------------------------|---|

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following example configures an iSCSI target interface profile with the name <b>targetA</b> to a SCSI target with the IP address <b>10.0.0.1</b> . |
|-----------------|--|

```
gprs iscsi targetA
  name ign.2002-10.edu.abc.io1.iscsi.draft20-target:1
  ip 10.0.0.1
  port 3260
```

| <b>Related Commands</b> | <b>Command</b>                            | <b>Description</b>   |
|-------------------------|---|--|
|                         | <a href="#">ip csg iscsi drain delay</a>  | Defines the delay interval, in seconds, before draining packets from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) when the Billing Mediation Agent (BMA) becomes active.      |
|                         | <a href="#">ip csg iscsi drain packet</a> | Defines the number of packets to be drained from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) per drain delay interval when the Billing Mediation Agent (BMA) becomes active. |
|                         | <a href="#">ip csg iscsi profile</a>      | Specifies the Internet Small Computer Systems Interface (iSCSI) target to be used as backup storage for the CSG2.  |

| Command                        | Description  |
|--------------------------------|--|
| <b>ip iscsi target-profile</b> | Creates an iSCSI profile for an iSCSI target on the CSG2, and enters iSCSI configuration mode.                           |
| <b>name (iSCSI)</b>            | Specifies the name of an iSCSI target in the target profile on the CSG2  |
| <b>port (iSCSI)</b>            | Specifies the number of the port on which to listen for iSCSI traffic in the iSCSI target interface profile on the CSG2. |

# ip csg billing

To define a CSG2 billing plan, and to enter CSG2 billing configuration mode, use the **ip csg billing** command in global configuration mode. To delete the billing plan, use the **no** form of this command.

**ip csg billing** *billing-plan-name*

**no ip csg billing** *billing-plan-name*

|                           |                          |   |
|---------------------------|--------------------------|---|
| <b>Syntax Description</b> | <i>billing-plan-name</i> | Name of the billing plan, which is a set of services. When the CSG2 encounters a new subscriber, the CSG2 retrieves its billing plan.<br><br>The name can be from 1 to 64 characters long, and can include uppercase or lowercase letters (the CSG2 changes all letters to uppercase), numbers, and any special characters. |
|---------------------------|--------------------------|---|

|                 |      |
|-----------------|------|
| <b>Defaults</b> | None |
|-----------------|------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | Global configuration |
|----------------------|----------------------|

|                        |                |  |
|------------------------|----------------|--|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>  |
|                        | 12.4(11)MD     | This command was migrated from CSG1.<br><br>Changes from CSG1: None. |

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | You can define up to 128 billing plans.<br><br>The characteristics of each billing plan are defined by the following commands: <ul style="list-style-type: none"> <li>• <a href="#">entries user idle</a></li> <li>• <a href="#">mode</a></li> <li>• <a href="#">service</a></li> </ul> |
|-------------------------|---|

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example shows how to define a CSG2 billing plan named REGULAR:<br><br><pre>ip csg billing REGULAR</pre> |
|-----------------|---|

|                         |                                   |  |
|-------------------------|-----------------------------------|--|
| <b>Related Commands</b> | <b>Command</b>                    | <b>Description</b>   |
|                         | <a href="#">entries user idle</a> | Sets the time after which entries for idle subscribers are deleted from the CSG2 User Table. |
|                         | <a href="#">mode</a>              | Specifies the mode for a CSG2 billing plan.  |
|                         | <a href="#">service</a>           | Associates a service with a CSG2 billing plan.   |

## ip csg bma

To configure the Billing Mediation Agents (BMAs) to which the CSG2 is to send billing records, use the **ip csg bma** command in CSG2 global configuration mode. To remove a BMA from the list of agents, use the **no** form of this command.

```
ip csg bma [vrf vrf-name] ip-address port-number priority
```

```
no ip csg bma [vrf vrf-name] ip-address port-number
```

### Syntax Description

|                            |  |
|----------------------------|--|
| <b>vrf</b> <i>vrf-name</i> | (Optional) Virtual Routing and Forwarding (VRF) table which the CSG2 is to use to communicate with the BMA.  |
| <i>ip-address</i>          | IP address of the BMA you wish to define.<br><br>The CSG2 differentiates BMAs on the basis of their IP addresses. When you configure a BMA, make sure its IP address matches on both the active CSG2 and on the standby CSG2.  |
| <i>port-number</i>         | Port number of the BMA you wish to define. The range is from 1 to 65535.<br><br>The CSG2 differentiates BMAs on the basis of their port numbers. When you configure a BMA, make sure its port number matches on both the active CSG2 and the standby CSG2.   |
| <i>priority</i>            | Priority of the BMA you wish to define.<br><br>The priority specifies the order of preference of the agents. A lower number indicates a higher priority. If the current agent becomes unusable, the CSG2 uses the highest priority BMA available.<br><br>Priorities for different agents do not have to be sequential. That is, you can have three agents with priorities 1, 5, and 10.<br><br>The range of priorities is 1 to 1000. |

### Defaults

Active and standby BMAs are not defined.  
If no VRF table is specified, the CSG2 uses the global routing table to communicate with the BMA.

### Command Modes

Global configuration

### Command History

| Release    | Modification  |
|------------|---|
| 12.4(11)MD | This command was migrated from CSG1.<br><br>Changes from CSG1: <ul style="list-style-type: none"> <li>The name of this command changed from <b>agent (CSG2 accounting)</b> to <b>ip csg bma</b>.</li> <li>The <b>vrf vrf-name</b> keyword and argument were added.</li> </ul> |

**Usage Guidelines**

You must specify the BMA local port using the **ip csg bma local-port** command before you enter the **ip csg bma** command.

Accounting records are sent only to the agents identified in the **ip csg bma** command. This provides a measure of security to ensure that records are not sent to unauthorized systems.

General packet radio service (GPRS) tunneling protocol (GTP) prime (GTP') does not support nodealive or redirect for multiple agents with the same IP address.

**Note**

The CSG2 does not support multiple BMAs with the same IP address.

**Examples**

The following example shows how to configure a BMA with priority 10 that uses VRF table BMAVRF:

```
ip csg bma vrf BMAVRF 1.2.3.4 5555 10
```

**Related Commands**

| Command                               | Description  |
|---------------------------------------|--|
| <a href="#">ip csg bma activate</a>   | Enables support for multiple active BMAs.  |
| <a href="#">ip csg bma keepalive</a>  | Defines the Billing Mediation Agent (BMA) keepalive time interval for the CSG2.  |
| <a href="#">ip csg bma local-port</a> | Defines the port on which the CSG2 listens for packets from the BMAs.  |
| <a href="#">ip csg bma messages</a>   | Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages that the CSG2 can buffer for all Billing Mediation Agents (BMAs). |
| <a href="#">ip csg bma retransmit</a> | Defines the Billing Mediation Agent (BMA) retransmit time interval for the CSG2.   |
| <a href="#">ip csg bma retries</a>    | Defines the maximum number of Billing Mediation Agent (BMA) retries allowed before the CSG2 determines that the link has failed.   |
| <a href="#">ip csg bma window</a>     | Defines the Billing Mediation Agent (BMA) transmit window size for the CSG2.   |

# ip csg bma activate

To enable support for multiple active Billing Mediation Agents (BMAs), use the **ip csg bma activate** command in CSG2 global configuration mode. To disable support for multiple active BMAs, use the **no** form of this command.

**ip csg bma activate** [*number* [**sticky seconds**]]

**no ip csg bma activate** [*number* [**sticky seconds**]]

## Syntax Description

|                       |  |
|-----------------------|--|
| <i>number</i>         | <p>(Optional) Number of BMAs that the CSG2 tries to activate at the same time.</p> <p>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.</p> <p>The range is from 1 to 32. The default value is 1.</p>  |
| <b>sticky seconds</b> | <p>(Optional) Number of seconds of inactivity after which a sticky object is to be deleted.</p> <p>The CSG2 creates a sticky object to ensure that all the billing records for a subscriber are sent to the same BMA. If the user ID is not available (for example, if the internal table is too small to hold all user ID entries, or if the CSG2 cannot access the user ID database), the CSG2 creates a sticky object for the subscriber IP address.</p> <p>This entry is removed from the table based on inactivity.</p> <p>Entries that contain a user ID do not age out; they are removed only by RADIUS messages.</p> <p>The range is from 1 to 64000. The default value is 30.</p> |

## Defaults

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

## Command Modes

Global configuration

## Command History

| Release    | Modification  |
|------------|---|
| 12.4(11)MD | <p>This command was migrated from CSG1.</p> <p>Changes from CSG1:</p> <ul style="list-style-type: none"> <li>The name of this command changed from <b>agent activate</b> to <b>ip csg bma activate</b>.</li> <li>The range of the <i>number</i> argument changed from 1 to 10, to 1 to 32.</li> </ul> |



**Usage Guidelines**

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

When the CSG2 uses multiple active BMAs, it sends all CDRs for a given user to a particular BMA. The CSG2 stores that BMA assignment in the CSG2 User Table entry for that user.

For example, if a configuration has four active BMAs, and one of those BMAs fails, the CSG2 looks for a suitable standby BMA. If the CSG2 finds a suitable standby BMA, it transfers all of the CDRs from the failed BMA to the new BMA, and updates all of the affected User Table entries to reflect the new BMA assignment.

However, if the CSG2 cannot find a suitable standby BMA, it redistributes all of the CDRs from the failed BMA among the remaining three active BMAs. It does so by finding the User Table entries for the affected users in the CDRs. The CSG2 then assigns one of the active BMAs to each affected user, and updates the User Table entries to reflect the new BMA assignments. The CSG2 reassigns all CDRs for a given user to the same BMA.

If the CSG2 cannot find a User Table entry for a user (for example, the user has logged off), it creates a temporary sticky object as a placeholder and assigns a new BMA to the sticky object. This ensures that the remaining CDRs for that user are sent to the same BMA.

**Note**

This command is valid only if your CSG2 uses multiple active BMAs. If your CSG2 uses one and only one active BMA, the default settings are sufficient (that is, **ip csg bma activate 1 sticky 30**).

**Examples**

The following example shows how to enable support for multiple active BMAs for the CSG2 accounting service A1. In this example, up to two BMAs can be active at the same time, and the CSG2 deletes inactive sticky objects after 60 seconds:

```
ip csg bma activate 2 sticky 60
```

**Related Commands**

| Command                                      | Description  |
|--|--|
| <a href="#">ip csg bma</a>                   | Defines the Billing Mediation Agents (BMAs) to which the CSG2 is to send billing records |
| <a href="#">ip csg quota-server activate</a> | Activates one or more quota servers.   |

# ip csg bma keepalive

To define the Billing Mediation Agent (BMA) keepalive time interval for the CSG2, use the **ip csg bma keepalive** command in global configuration mode. To reset the BMA keepalive timer to the default value, use the **no** form of this command.

**ip csg bma keepalive** *number-of-seconds*

**no ip csg bma keepalive**

## Syntax Description

*number-of-seconds* Time, in seconds, between BMA keepalives. The range is 1 to 65535. The default value is 60.

## Defaults

The default value is 60 seconds.

## Command Modes

Global configuration

## Command History

| Release    | Modification  |
|------------|---|
| 12.4(11)MD | This command was migrated from CSG1.<br><br>Changes from CSG1: <ul style="list-style-type: none"> <li>The name of this command changed from <b>keepalive</b> to <b>ip csg bma keepalive</b>.</li> <li>The configuration mode for this command changed from CSG accounting to global configuration.</li> </ul> |

## Usage Guidelines

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

## Examples

The following example shows how to specify a BMA keepalive time of 300 seconds:

```
ip csg bma keepalive 300
```

## Related Commands

| Command                                       | Description  |
|---|--|
| <a href="#">ip csg bma</a>                    | Defines the Billing Mediation Agents (BMAs) to which the CSG2 is to send billing records |
| <a href="#">ip csg ipc keepalive</a>          | Defines the Interprocessor Communication (IPC) keepalive time interval for the CSG2.     |
| <a href="#">ip csg psd keepalive</a>          | Defines the Cisco Persistent Storage Device (PSD) keepalive time interval for the CSG2.  |
| <a href="#">ip csg quota-server keepalive</a> | Defines the quota-server keepalive time interval for the CSG2.                           |

# ip csg bma local-port

To define the port on which the CSG2 communicates with the Billing Mediation Agent (BMA), use the **ip csg bma local-port** command in CSG2 global configuration mode. To remove the port, use the **no** form of this command.

```
ip csg bma local-port port-number
```

```
no ip csg bma local-port
```

## Syntax Description

|                    |   |
|--------------------|---|
| <i>port-number</i> | Port number on which the BMA will listen. The range is from 1024 to 65535. 5000 is not a valid port number.<br><br>The BMA local port number must be different from the Persistent Storage Device (PSD) local port number and from the quota server local port number (configured with the <b>ip csg psd local-port</b> command and the <b>ip csg quota-server local-port</b> command, respectively). |
|--------------------|---|

## Defaults

No BMA local ports are configured.

## Command Modes

Global configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.<br><br>Changes from CSG1: The name of this command changed from <b>agent local-port</b> to <b>ip csg bma local-port</b> . |

## Usage Guidelines

You must specify the BMA local port using the **ip csg bma local-port** command before you enter the **ip csg bma** command.

This command accommodates BMAs that configure a port number that is not the general packet radio service (GPRS) tunneling protocol (GTP) prime (GTP') default port (3386).

You must configure a local port to activate BMAs. The local port must be unique with respect to all other configured local ports, such as the quota server local port.



### Note

The CSG2 drops requests (such as nodealive, echo, and redirect requests) unless they come from a configured BMA IP address. The CSG2 also verifies IP addresses against the configured list of BMAs. If there is no match, the CSG2 drops the request. The CSG2 does not look at a request's source port; instead, the CSG2 replies to the same port from which the request came.

**Examples**

The following example shows how to specify local port 5555 as the port on which the CSG2 listens for the CSG2 accounting service A1:

```
ip csg bma local-port 5555
```

**Related Commands**

| Command  | Description  |
|--|--|
| <a href="#">ip csg bma</a>                     | Defines the Billing Mediation Agents (BMAs) to which the CSG2 is to send billing records                 |
| <a href="#">ip csg psd local-port</a>          | Configures the local port on which the CSG2 communicates with the Cisco Persistent Storage Device (PSD). |
| <a href="#">ip csg quota-server local-port</a> | Configures the local port on which the CSG2 communicates with quota servers.                             |

## ip csg bma messages

To specify the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages that the CSG2 can buffer for all Billing Mediation Agents (BMAs), use the **ip csg bma messages** command in global configuration mode. To restore the default setting, use the **no** form of this command.

**ip csg bma messages** *number*

**no ip csg bma messages**

|                           |               |  |
|---------------------------|---------------|--|
| <b>Syntax Description</b> | <i>number</i> | Maximum number of GTP' messages that can be buffered for all BMAs. The range is from 1 to 65535. The default is 10000. |
|---------------------------|---------------|--|

**Defaults** The CSG2 buffers up to 10000 GTP' messages.

**Command Modes** Global configuration

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>  |
|------------------------|----------------|--|
|                        | 12.4(11)MD     | This command was migrated from CSG1.<br>Changes from CSG1: <ul style="list-style-type: none"> <li>The name of this command changed from <b>records max</b> to <b>ip csg bma messages</b>.</li> <li>The configuration mode for this command changed from CSG accounting to global configuration.</li> </ul> |

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

The CSG2 can buffer GTP' messages in either the Cisco Persistent Storage Device (PSD) or in the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI), as configured. (For more information, see the [“Configuring PSD Support” section on page 7-1](#) and the [“Configuring iSCSI Support” section on page 8-1](#).)

If the BMA GTP' message buffer exceeds 75% of the *number* specified on this command, the CSG2 stops reading GTP' messages from the PSD or SAN. When the buffer drops below the 75% threshold, the CSG2 again begins reading from the PSD or SAN, placing the buffered GTP' messages in the BMA queue. For example, using the default setting for this command of 10,000 messages, the CSG2 can read from the PSD or SAN as long as the buffer contains less than 7,500 GTP' messages—75% of 10,000 messages.

By default, the CSG2 limits the rate at which GTP' messages are read from the PSD to 500 packets/second, and from the SAN to 167 packets/second. However, you can change those default rates. For more information, see the [“Configuring the PSD Packet Drain Settings” section on page 7-2](#) and the [“Configuring the iSCSI Packet Drain Settings” section on page 8-4](#).

### Examples

The following example shows how to configure the CSG2 to buffer up to 12345 GTP' messages:

```
ip csg bma messages 12345
```

### Related Commands

| Command                                      | Description   |
|--|---|
| <a href="#">ip csg bma</a>                   | Defines the Billing Mediation Agents (BMAs) to which the CSG2 is to send billing records  |
| <a href="#">ip csg iscsi drain delay</a>     | Defines the delay interval, in seconds, before draining packets from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) when the Billing Mediation Agent (BMA) becomes active.                             |
| <a href="#">ip csg iscsi drain packet</a>    | Defines the number of packets to be drained from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) per drain delay interval when the Billing Mediation Agent (BMA) becomes active.                        |
| <a href="#">ip csg psd drain delay</a>       | Defines the delay interval, in seconds, before draining packets from the Cisco Persistent Storage Device (PSD) when the Billing Mediation Agent (BMA) becomes active.   |
| <a href="#">ip csg psd drain packet</a>      | Defines the number of packets to be drained from the Cisco Persistent Storage Device (PSD) per drain delay interval when the Billing Mediation Agent (BMA) becomes active.  |
| <a href="#">ip csg psd margin</a>            | Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages, beyond the size of the Billing Mediation Agent (BMA) message queue, that the CSG2 can buffer for the Cisco Persistent Storage Device (PSD). |
| <a href="#">ip csg quota-server messages</a> | Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages that the CSG2 can buffer for all quota servers.  |

# ip csg bma retransmit

To define the Billing Mediation Agent (BMA) retransmit time interval for the CSG2, use the **ip csg bma retransmit** command in global configuration mode. To reset the BMA retransmit timer to the default value, use the **no** form of this command.

```
ip csg bma retransmit number-of-seconds
```

```
no ip csg bma retransmit
```

## Syntax Description

|                          |   |
|--------------------------|---|
| <i>number-of-seconds</i> | Time, in seconds, between BMA retransmits. The range is 2 to 65535. The default value is 4. |
|--------------------------|---|

## Defaults

The default value is 4 seconds.

## Command Modes

Global configuration

## Command History

| Release    | Modification                                     |
|------------|--|
| 12.4(11)MD | This command was introduced.                     |
| 12.4(15)MD | The range changed from 1 to 65535 to 2 to 65535. |

## Usage Guidelines

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

## Examples

The following example shows how to specify a BMA retransmit time of 2 seconds:

```
ip csg bma retransmit 2
```

## Related Commands

| Command  | Description  |
|--|--|
| <a href="#">ip csg bma</a>                     | Defines the Billing Mediation Agents (BMAs) to which the CSG2 is to send billing records |
| <a href="#">ip csg ipc retransmit</a>          | Defines the Interprocessor Communication (IPC) retransmit time interval for the CSG2.    |
| <a href="#">ip csg psd retransmit</a>          | Defines the Cisco Persistent Storage Device (PSD) retransmit time interval for the CSG2. |
| <a href="#">ip csg quota-server retransmit</a> | Defines the quota server retransmit time interval for the CSG2.                          |

## ip csg bma retries

To define the maximum number of Billing Mediation Agent (BMA) retries allowed before the CSG2 determines that the link has failed, use the **ip csg bma retries** command in global configuration mode. To reset the number of BMA retries to the default value, use the **no** form of this command.

```
ip csg bma retries [packet] number-of-retries
```

```
no ip csg bma retries
```

### Syntax Description

|                          |  |
|--------------------------|--|
| <b>packet</b>            | (Optional) Attempt to send a packet to the BMA the specified number of times, then discard the packet. |
| <i>number-of-retries</i> | Maximum number of BMA retries allowed by the CSG2. The range is 1 to 65535. The default value is 3.    |

### Defaults

The default value is 3 retries.

### Command Modes

Global configuration

### Command History

| Release    | Modification                         |
|------------|--------------------------------------|
| 12.4(11)MD | This command was introduced.         |
| 12.4(15)MD | The <b>packet</b> keyword was added. |

### Usage Guidelines

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

By default, the CSG2 retries a packet forever; it never discards a packet. If you configure the **ip csg bma retries packet** command, the CSG2 tries to send a packet to the BMA the specified number of times, then discards the packet. (The first attempt to send a packet to the BMA is not counted as a retry.) For example, if you configure **ip csg bma retries packet 4**, the CSG2 tries to send a packet to the BMA five times before discarding it (the initial attempt plus four retries).

### Examples

The following example shows how to allow two BMA retries:

```
ip csg bma retries 2
```

The following example shows how to allow the CSG2 to try to send a packet to the BMA four times, in addition to the initial attempt:

```
ip csg bma retries packet 4
```



| Related Commands | Command                                     | Description  |
|------------------|---|--|
|                  | <a href="#">ip csg bma</a>                  | Defines the Billing Mediation Agents (BMAs) to which the CSG2 is to send billing records   |
|                  | <a href="#">ip csg ipc retries</a>          | Defines the maximum number of Interprocessor Communication (IPC) retries allowed before the CSG2 determines that the link has failed.    |
|                  | <a href="#">ip csg psd retries</a>          | Defines the maximum number of Cisco Persistent Storage Device (PSD) retries allowed before the CSG2 determines that the link has failed. |
|                  | <a href="#">ip csg quota-server retries</a> | Defines the maximum number of quota server retries allowed before the CSG2 determines that the link has failed.                          |

# ip csg bma window

To define the Billing Mediation Agent (BMA) transmit window size for the CSG2, use the **ip csg bma window** command in global configuration mode. To reset the BMA transmit window size to the default value, use the **no** form of this command.

```
ip csg bma window {max window-size | min window-size | min auto}
```

```
no ip csg bma window {max | min}
```

## Syntax Description

|                               |  |
|-------------------------------|--|
| <b>max</b> <i>window-size</i> | Maximum size, in packets, of the BMA transmit window. The range is 1 to 65535. The default value is 128.   |
| <b>min</b> <i>window-size</i> | Minimum size, in packets, of the BMA transmit window. The range is 1 to 65535.   |
| <b>min auto</b>               | Specifies that the CSG2 is to determine the minimum size of the BMA transmit window automatically. The CSG2 keeps track of the maximum number of ACKs received in one response and sets that number as the minimum window. |

## Defaults

The default maximum window size is 128 packets.  
The default minimum window size is automatically determined by the CSG2.

## Command Modes

Global configuration

## Command History

| Release    | Modification                 |
|------------|------------------------------|
| 12.4(11)MD | This command was introduced. |

## Usage Guidelines

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

## Examples

The following example shows how to set the maximum BMA transmit window to 64 packets:

```
ip csg bma window max 64
```

## Related Commands

| Command                                    | Description  |
|--|--|
| <a href="#">ip csg bma</a>                 | Defines the Billing Mediation Agents (BMAs) to which the CSG2 is to send billing records |
| <a href="#">ip csg psd window</a>          | Defines the Cisco Persistent Storage Device (PSD) transmit window size for the CSG2.     |
| <a href="#">ip csg quota-server window</a> | Defines the quota server transmit window size for the CSG2.                              |

# ip csg case-sensitive

To specify whether to treat CSG2 header, method, and URL match patterns as case-sensitive, use the **ip csg case-sensitive** command in global configuration mode. To disable case-sensitivity for CSG2 match patterns, use the **no** form of this command.

**ip csg case-sensitive**

**no ip csg case-sensitive**

**Syntax Description** This command has no arguments or keywords.

**Defaults** CSG2 match patterns are case-sensitive.

**Command Modes** Global configuration

| Command History | Release    | Modification                 |
|-----------------|------------|------------------------------|
|                 | 12.4(11)MD | This command was introduced. |

**Examples** The following example shows how to disable case-sensitivity for CSG2 match patterns:

```
no ip csg case-sensitive
```

| Related Commands | Command                      | Description  |
|------------------|------------------------------|--|
|                  | <a href="#">match header</a> | Specifies a header match pattern for a CSG2 billing map. |
|                  | <a href="#">match method</a> | Specifies a method match pattern for a CSG2 billing map. |
|                  | <a href="#">match url</a>    | Specifies a URL match pattern for a CSG2 billing map.    |

# ip csg content

To configure content for CSG2 services, and to enter CSG2 content configuration mode, use the **ip csg content** command in global configuration mode. To delete the content configuration, use the **no** form of this command.

**ip csg content** *content-name*

**no ip csg content** *content-name*

## Syntax Description

|                     |   |
|---------------------|---|
| <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 CSG2 changes all letters to uppercase), numbers, and any special characters. |
|---------------------|---|

## Defaults

None

## Command Modes

Global configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: None. |

## Usage Guidelines

You can define up to 2048 contents.

The characteristics of each content configuration are defined by the following commands:

- **block**
- **client-group (CSG2 content)**
- **idle (CSG2 content)**
- **inservice (CSG2 content)**
- **ip (CSG2 content)**
- **mode tcp**
- **next-hop**
- **parse length**
- **parse protocol**
- **pending**
- **policy (CSG2 content)**
- **records delay**
- **records intermediate**
- **replicate**

- [subscriber-ip http-header forwarded-for](#)
- [vlan \(CSG2 content\)](#)
- [vrf](#)

You cannot change characteristics for a content while it is in service.

If the content configuration does not match any service listed under a subscriber's billing plan, the CSG2 considers the service to be either free or postpaid. The CSG2 does not try to authorize the subscriber with the quota server for the service.

### Examples

The following example shows how to define the CSG2 content named MOVIES\_COMEDY:

```
ip csg content MOVIES_COMEDY
```

### Related Commands

| Command   | Description  |
|---|--|
| <a href="#">block</a>                                   | Forces the CSG2 to drop packets that do not match a configured billing policy.                             |
| <a href="#">client-group (CSG2 content)</a>             | References a standard access list that is part of a CSG2 content.  |
| <a href="#">idle (CSG2 content)</a>                     | Specifies the minimum amount of time that the CSG2 maintains an idle content connection.                   |
| <a href="#">inservice (CSG2 content)</a>                | Activates the content service on each CSG2.  |
| <a href="#">ip (CSG2 content)</a>                       | Defines the subset of Layer 3 and Layer 4 flows that can be processed by the CSG2 accounting services.     |
| <a href="#">mode tcp</a>                                | Specifies the mode for CSG2 TCP sessions.  |
| <a href="#">next-hop</a>                                | Defines a next-hop IP address.   |
| <a href="#">parse length</a>                            | Defines the maximum number of Layer 7 bytes that the CSG2 is to parse when attempting to assign a policy.  |
| <a href="#">parse protocol</a>                          | Defines how the CSG2 is to parse traffic for a content.  |
| <a href="#">policy (CSG2 content)</a>                   | References a CSG2 billing policy.  |
| <a href="#">records delay</a>                           | Specifies the delay before the CSG2 is to send the HTTP Statistics CDR.                                    |
| <a href="#">records intermediate</a>                    | Enables the generation of CSG2 intermediate billing records.   |
| <a href="#">replicate</a>                               | Replicates the connection state for all TCP connections to the CSG2 content servers on the standby system. |
| <a href="#">subscriber-ip http-header forwarded-for</a> | Specifies that the CSG2 is to obtain the subscriber's IP address from the HTTP X-Forwarded-For header.     |
| <a href="#">vlan (CSG2 content)</a>                     | Restricts the CSG2 billing content to a single source VLAN.  |
| <a href="#">vrf</a>                                     | Restricts the CSG2 content to packets within a single Virtual Routing and Forwarding (VRF) table.          |

# ip csg database

To identify the database server that answers CSG2 user ID queries, use the **ip csg database** command in global configuration mode. To disable the database server, use the **no** form of this command.

```
ip csg database [vrf vrf-name] ip-address port-number local-port
```

```
no ip csg database
```

## Syntax Description

|                            |  |
|----------------------------|--|
| <b>vrf</b> <i>vrf-name</i> | (Optional) Specifies the Virtual Routing and Forwarding (VRF) table to be used for communication with the database server. |
| <i>ip-address</i>          | IP address of the database server that answers user ID queries.  |
| <i>port-number</i>         | Port number of the database server that answers user ID queries. The range is from 1 to 65535.                             |
| <i>local-port</i>          | Local port number that the CSG2 is to use to send queries to the database server. The range is from 1 to 65535.            |

## Defaults

If no VRF table is specified, the CSG2 uses the global routing table to communicate with the database server.

## Command Modes

Global configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.<br><br>Changes from CSG1: <ul style="list-style-type: none"> <li>• The name of this command changed from <b>database</b> to <b>ip csg database</b>.</li> <li>• The configuration mode for this command changed from CSG user group to global configuration.</li> <li>• The <b>vrf</b> <i>vrf-name</i> and <i>local-port</i> keywords and arguments were added.</li> </ul> |

## Usage Guidelines

You can configure one and only one database server to answer CSG2 user ID queries.

The subscriber traffic must flow on an interface in the global routing table (not the VRF table).

## Examples

The following example shows how to specify a user database server with IP address 10.1.2.3, port number 11111, and local port number 22222:

```
ip csg database 10.1.2.3 11111 22222
```

# ip csg entries fragment

To define the maximum number of entries in the CSG2 fragment database, or to define how long the CSG2 is to retain the entries, use the **ip csg entries fragment** command in global configuration mode. To restore the default settings, use the **no** form of this command.

```
ip csg entries fragment {idle duration | maximum entries-number}
```

```
no ip csg entries fragment {idle | max}
```

## Syntax Description

|                                      |  |
|--------------------------------------|--|
| <b>idle</b> <i>duration</i>          | Number of seconds after which entries are deleted from the CSG2 fragment database. The range is from 1 to 255. The default setting is 5. |
| <b>maximum</b> <i>entries-number</i> | Maximum number of entries allowed in the CSG2 fragment database. The range is from 1 to 65535. The default number of entries is 16384.   |

## Defaults

The default idle duration is 5 seconds.  
The default maximum number of entries is 16384.

## Command Modes

Global configuration

## Command History

| Release    | Modification                 |
|------------|------------------------------|
| 12.4(11)MD | This command was introduced. |

## Usage Guidelines

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

## Examples

The following example shows how to specify a maximum CSG2 fragment database size of 32,768 entries:

```
ip csg entries fragment maximum 32768
```

## Related Commands

| Command                                  | Description  |
|--|--|
| <a href="#">ip csg database</a>          | Server that answers user ID queries.                                     |
| <a href="#">ip csg entries user idle</a> | Specifies how long the CSG2 is to retain entries in the CSG2 User Table. |
| <a href="#">ip csg entries user max</a>  | Specifies the maximum number of entries allowed in the CSG2 User Table.  |

| Command                                | Description   |
|--|---|
| <b>ip csg entries user profile</b>     | Specifies the location from which the CSG2 is to obtain the subscriber profile and billing plan when generating entries for the CSG2 User Table.  |
| <b>ip csg entries session user max</b> | Specifies the maximum number of entries allowed in the CSG2 session table.  |
| <b>ip csg psd margin</b>               | Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages, beyond the size of the Billing Mediation Agent (BMA) message queue, that the CSG2 can buffer for the Cisco Persistent Storage Device (PSD). |
| <b>ip csg quota-server messages</b>    | Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages that the CSG2 can buffer for all quota servers.  |



# ip csg entries session user max

To specify the maximum number of entries allowed in the CSG2 session table, use the **ip csg entries session user max** command in global configuration mode. To restore the default settings, use the **no** form of this command.

**ip csg entries session user max** *entries*

**no ip csg entries session user max**

## Syntax Description

|                |   |
|----------------|---|
| <i>entries</i> | Maximum number of entries allowed in the session table. This is the maximum number of sessions that the CSG2 can support. When the number of active sessions reaches the specified maximum, the CSG2 begins dropping incoming new sessions. The range is from 1 to 1800000. The default number of entries is 1000000. |
|----------------|---|

## Defaults

The default maximum number of entries is 1000000.

## Command Modes

Global configuration

## Command History

| Release    | Modification                 |
|------------|------------------------------|
| 12.4(11)MD | This command was introduced. |

## Usage Guidelines

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

## Examples

The following example shows how to specify a maximum CSG2 session table size of 100,000 entries:

```
ip csg entries session user max 100000
```

## Related Commands

| Command                                     | Description  |
|---|--|
| <a href="#">ip csg database</a>             | Server that answers user ID queries.   |
| <a href="#">ip csg entries fragment</a>     | Defines the maximum number of entries in the CSG2 fragment database, or how long the CSG2 is to retain the entries.                              |
| <a href="#">ip csg entries user idle</a>    | Specifies how long the CSG2 is to retain entries in the CSG2 User Table.   |
| <a href="#">ip csg entries user max</a>     | Specifies the maximum number of entries allowed in the CSG2 User Table.  |
| <a href="#">ip csg entries user profile</a> | Specifies the location from which the CSG2 is to obtain the subscriber profile and billing plan when generating entries for the CSG2 User Table. |

| Command                                      | Description   |
|--|---|
| <a href="#">ip csg psd margin</a>            | Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages, beyond the size of the Billing Mediation Agent (BMA) message queue, that the CSG2 can buffer for the Cisco Persistent Storage Device (PSD). |
| <a href="#">ip csg quota-server messages</a> | Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages that the CSG2 can buffer for all quota servers.  |

# ip csg entries user idle

To specify how long the CSG2 is to retain entries in the CSG2 User Table, use the **ip csg entries user idle** command in global configuration mode. To restore the default settings, use the **no** form of this command.

**ip csg entries user idle** *duration* [**pod**]

**no ip csg entries user idle**

## Syntax Description

|                 |  |
|-----------------|--|
| <i>duration</i> | Number of seconds after which the CSG2 is to delete entries for idle subscribers from the CSG2 User Table. The range is from 0 (entries never idle out) to 2147483647. The default setting is 0. |
| <b>pod</b>      | (Optional) Specifies whether the CSG2 is to send the RADIUS Packet of Disconnect message when an entry idles out.  |

## Defaults

The default idle duration is 0 seconds (entries never idle out), and the CSG2 does not send the RADIUS Packet of Disconnect message when an entry idles out.

## Command Modes

Global configuration

## Command History

| Release    | Modification                 |
|------------|------------------------------|
| 12.4(11)MD | This command was introduced. |

## Usage Guidelines

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

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

- You can set the entry idle timer either globally, using the **ip csg entries user idle** command, or in each billing plan, using the **entries user idle** command in CSG2 billing configuration mode. If you do not set the timer in the billing plan, the CSG2 uses the global timer. That is, if there is an entry idle timer value in the billing plan, it is used; otherwise, if there is a global entry idle timer value configured, it is used.
- If set, the idle timer starts when there are no billable sessions, and restarts whenever a RADIUS Accounting Start or an Interim Accounting message is received. The timer stops when a billable session is started.
- If you do not specify the **pod** keyword, the CSG2 deletes the idle entry when the timer expires.
- If you specify the **pod** keyword, and if RADIUS Packet of Disconnect (PoD) is configured for the CSG2, the CSG2 sends a PoD message when the idle timer expires. The CSG2 deletes the idle entry when the PoD message is ACKed, NAKed, or when all retries have been sent.

## ip csg entries user idle

- If Connection Duration Billing is enabled, you can use either the billing plan entry idle timer or the global entry idle timer to release a subscriber connection.
- The idle timer does not affect sticky user entries.

### Examples

The following example shows how to specify a CSG2 User Table entry idle time of 86,400 seconds:

```
ip csg entries user idle 86400
```

### Related Commands

| Command   | Description   |
|---|---|
| <a href="#">entries user idle</a>               | Sets the time after which entries for idle subscribers are deleted from the CSG2 User Table.  |
| <a href="#">ip csg database</a>                 | Server that answers user ID queries.  |
| <a href="#">ip csg entries fragment</a>         | Defines the maximum number of entries in the CSG2 fragment database, or how long the CSG2 is to retain the entries.   |
| <a href="#">ip csg entries user max</a>         | Specifies the maximum number of entries allowed in the CSG2 User Table.   |
| <a href="#">ip csg entries user profile</a>     | Specifies the location from which the CSG2 is to obtain the subscriber profile and billing plan when generating entries for the CSG2 User Table.  |
| <a href="#">ip csg entries session user max</a> | Specifies the maximum number of entries allowed in the CSG2 session table.  |
| <a href="#">ip csg psd margin</a>               | Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages, beyond the size of the Billing Mediation Agent (BMA) message queue, that the CSG2 can buffer for the Cisco Persistent Storage Device (PSD). |
| <a href="#">ip csg quota-server messages</a>    | Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages that the CSG2 can buffer for all quota servers.  |

# ip csg entries user max

To specify the maximum number of entries allowed in the CSG2 User Table, use the **ip csg entries user max** command in global configuration mode. To restore the default settings, use the **no** form of this command.

**ip csg entries user max** *entries*

**no ip csg entries user max**

## Syntax Description

|                |  |
|----------------|--|
| <i>entries</i> | <p>Maximum number of entries allowed in the CSG2 User Table.</p> <ul style="list-style-type: none"> <li>For the 2 GB-SAMI option, the range is from 1 to 1250000. The default number of entries is 300000.</li> <li>For the 1 GB-SAMI option, the range is from 1 to 500000. The default number of entries is 300000.</li> </ul> <p>The actual number of entries in the CSG2 User Table depends on several variables, including the traffic model being used and the number of RADIUS attributes reported. Even if you set entries-number to a very large number, such as 300000, the CSG2 might never store that many entries in the CSG2 User Table.</p> |
|----------------|--|

## Defaults

The default maximum number of entries is 300000 for both the 1 GB-SAMI and the 2 GB-SAMI options.

## Command Modes

Global configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was introduced.   |
| 12.4(15)MD | <p>The range was changed to reflect the differences between the 2 GB-SAMI and 1 GB-SAMI options:</p> <ul style="list-style-type: none"> <li>For the 2 GB-SAMI option, the range is from 1 to 1250000.</li> <li>For the 1 GB-SAMI option, the range is from 1 to 500000.</li> </ul> |

## Usage Guidelines

The maximum number of entries is not enforced on the buffer pool maximum size, it is enforced during allocation of individual entries to the CSG2 User Table.

## Examples

The following example shows how to specify a maximum CSG2 User Table size of 500000 entries:

```
ip csg entries user max 500000
```

| Related Commands | Command   | Description   |
|------------------|---|---|
|                  | <a href="#">ip csg database</a>                 | Server that answers user ID queries.  |
|                  | <a href="#">ip csg entries fragment</a>         | Defines the maximum number of entries in the CSG2 fragment database, or how long the CSG2 is to retain the entries.   |
|                  | <a href="#">ip csg entries user idle</a>        | Specifies how long the CSG2 is to retain entries in the CSG2 User Table.  |
|                  | <a href="#">ip csg entries user profile</a>     | Specifies the location from which the CSG2 is to obtain the subscriber profile and billing plan when generating entries for the CSG2 User Table.  |
|                  | <a href="#">ip csg entries session user max</a> | Specifies the maximum number of entries allowed in the CSG2 session table.  |
|                  | <a href="#">ip csg psd margin</a>               | Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages, beyond the size of the Billing Mediation Agent (BMA) message queue, that the CSG2 can buffer for the Cisco Persistent Storage Device (PSD). |
|                  | <a href="#">ip csg quota-server messages</a>    | Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages that the CSG2 can buffer for all quota servers.  |

# ip csg entries user profile

To specify the location from which the CSG2 is to obtain the subscriber profile and billing plan when generating entries for the CSG2 User Table, use the **ip csg entries user profile** command in global configuration mode. To restore the default settings, use the **no** form of this command.

```
ip csg entries user profile {quota-server | radius {pass | remove | timeout timeout}}
```

```
no ip csg entries user profile
```

## Syntax Description

|                               |  |
|-------------------------------|--|
| <b>quota-server</b>           | The CSG2 obtains the subscriber profile and billing plan from the quota server.  |
| <b>radius</b>                 | The CSG2 obtains the Cisco vendor-specific attribute (VSA) subattribute 1, which contains the billing plan name, from the RADIUS Access-Accept and RADIUS Accounting-Request messages.         |
| <b>pass</b>                   | Does not remove the VSA containing the billing plan from the RADIUS Access-Accept message.   |
| <b>remove</b>                 | Removes the VSA containing the billing plan from the RADIUS Access-Accept message.   |
| <b>timeout <i>timeout</i></b> | Number of seconds to retain cached billing plan data while waiting for a RADIUS Accounting Start message for a user. The range is from 10 to 65535 seconds. The default timeout is 20 seconds. |

## Defaults

If you do not specify the **ip csg entries user profile** command, the CSG2 obtains the subscriber profile and billing plan from the quota server.  
If you do not specify a timeout, the default timeout is 20 seconds.

## Command Modes

Global configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: <ul style="list-style-type: none"> <li>The name of this command changed from <b>user-profile server</b> to <b>ip csg entries user profile</b>.</li> <li>The configuration mode for this command changed from CSG user group to global configuration.</li> </ul> |
| 12.4(15)MD | The <b>timeout</b> keyword and <i>timeout</i> argument were added.   |

**Usage Guidelines**

Keep the following considerations in mind:

- The VSA is removed from the RADIUS Access-Accept message only if **remove** is specified. Use the **remove** argument only if the RADIUS client cannot accept the Cisco VSA in the message.
- We recommend that you use **pass** to reduce processing time on the CSG2.
- The user ID must be included in the message that contains the billing plan.

The CSG2 obtains billing plan data from authentication, authorization, and accounting (AAA) RADIUS Access response packets.

- When the CSG2 receives a RADIUS Access response for a user, it caches the billing plan data for that user.
- When the CSG2 receives a RADIUS Accounting Start message from a Network Access Server (NAS) for that same user, it frees the cached billing plan data.
- If the cache timeout expires before the CSG2 receives the RADIUS Accounting Start message, the CSG2 frees the cached billing plan data. If the RADIUS Accounting Start message arrives after the cached billing plan data has been freed, the CSG2 creates the user with an unknown billing plan and sends a User Authorization Request to the quota server.

In most cases, the default timeout of 20 seconds is far greater than the delay between the receipt of the RADIUS Access response and the receipt of the RADIUS Accounting Start message. If the default timeout is not large enough, you can use the **ip csg entries user profile timeout *timeout*** command to increase the timeout.

**Examples**

The following example shows how to specify that the CSG2 is to obtain billing plan names from the RADIUS Access-Accept and RADIUS Accounting-Request messages, and that the CSG2 is not to remove the VSA containing the billing plan from the messages:

```
ip csg entries user profile radius pass
```

**Related Commands**

| Command   | Description   |
|---|---|
| <a href="#">ip csg database</a>                 | Server that answers user ID queries.  |
| <a href="#">ip csg entries fragment</a>         | Defines the maximum number of entries in the CSG2 fragment database, or how long the CSG2 is to retain the entries.   |
| <a href="#">ip csg entries user idle</a>        | Specifies how long the CSG2 is to retain entries in the CSG2 User Table.  |
| <a href="#">ip csg entries user max</a>         | Specifies the maximum number of entries allowed in the CSG2 User Table.   |
| <a href="#">ip csg entries session user max</a> | Specifies the maximum number of entries allowed in the CSG2 session table.  |
| <a href="#">ip csg psd margin</a>               | Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages, beyond the size of the Billing Mediation Agent (BMA) message queue, that the CSG2 can buffer for the Cisco Persistent Storage Device (PSD). |
| <a href="#">ip csg quota-server messages</a>    | Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages that the CSG2 can buffer for all quota servers.  |
| <a href="#">ip csg radius userid</a>            | Specifies the RADIUS attribute used to extract the user identifier from a RADIUS record.  |



# ip csg ipc crashdump

To define the action to be taken by the CSG2 if an Interprocessor Communication (IPC) link fails, use the **ip csg ipc crashdump** command in global configuration mode. To restore the default setting, use the **no** form of this command.

```
ip csg ipc crashdump [never | tolerance [number-of-seconds]]
```

```
no ip csg ipc crashdump
```

## Syntax Description

|   |  |
|---|--|
| <b>never</b>                              | (Optional) Never generate a crash dump in an IPC link fails. This is the default setting.  |
| <b>tolerance</b> <i>number-of-seconds</i> | (Optional) Time, in seconds, that the CSG2 is to wait after an IPC link fails before generating a crash dump. The range is 60 to 600. The default value is 60. |

## Defaults

The default setting is to never generate a crash dump. If you specify the tolerance keyword without specifying a time, the CSG2 generates a crash dump 60 seconds after an IPC link fails.

## Command Modes

Global configuration

## Command History

| Release    | Modification                 |
|------------|------------------------------|
| 12.4(11)MD | This command was introduced. |

## Usage Guidelines

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

## Examples

The following example shows how to specify that the CSG2 is to generate a crash dump 120 seconds after an IPC link fails:

```
ip csg ipc crashdump tolerance 120
```

# ip csg ipc keepalive

To define the Interprocessor Communication (IPC) module keepalive time interval for the CSG2, use the **ip csg ipc keepalive** command in global configuration mode. To reset the IPC keepalive timer to the default value, use the **no** form of this command.

**ip csg ipc keepalive** *number-of-seconds*

**no ip csg ipc keepalive**

## Syntax Description

*number-of-seconds* Time, in seconds, between IPC keepalives. The range is 1 to 65535. The default value is 8.

## Defaults

The default value is 8 seconds.

## Command Modes

Global configuration

## Command History

| Release    | Modification                 |
|------------|------------------------------|
| 12.4(11)MD | This command was introduced. |

## Usage Guidelines

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

## Examples

The following example shows how to specify an IPC keepalive time of 300 seconds:

```
ip csg ipc keepalive 300
```

## Related Commands

| Command                                       | Description   |
|---|---|
| <a href="#">ip csg bma keepalive</a>          | Defines the Billing Mediation Agent (BMA) keepalive time interval for the CSG2.         |
| <a href="#">ip csg psd keepalive</a>          | Defines the Cisco Persistent Storage Device (PSD) keepalive time interval for the CSG2. |
| <a href="#">ip csg quota-server keepalive</a> | Defines the quota-server keepalive time interval for the CSG2.                          |

# ip csg ipc retransmit

To define the Interprocessor Communication (IPC) retransmit time interval for the CSG2, use the **ip csg ipc retransmit** command in global configuration mode. To reset the IPC retransmit timer to the default value, use the **no** form of this command.

```
ip csg ipc retransmit number-of-seconds
```

```
no ip csg ipc retransmit
```

|                           |                          |   |
|---------------------------|--------------------------|---|
| <b>Syntax Description</b> | <i>number-of-seconds</i> | Time, in seconds, between IPC retransmits. The range is 1 to 65535. The default value is 4. |
|---------------------------|--------------------------|---|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | The default value is 4 second. |
|-----------------|--------------------------------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | Global configuration |
|----------------------|----------------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|------------------------|----------------|------------------------------|
|                        | 12.4(11)MD     | This command was introduced. |

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | We recommend that you change the retransmit time interval only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting. |
|-------------------------|--|

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example shows how to specify an IPC retransmit time of 2 seconds:<br><pre>ip csg ipc retransmit 2</pre> |
|-----------------|---|

| <b>Related Commands</b> | <b>Command</b>                                 | <b>Description</b>   |
|-------------------------|--|--|
|                         | <a href="#">ip csg bma retransmit</a>          | Defines the Billing Mediation Agent (BMA) retransmit time interval for the CSG2.         |
|                         | <a href="#">ip csg psd retransmit</a>          | Defines the Cisco Persistent Storage Device (PSD) retransmit time interval for the CSG2. |
|                         | <a href="#">ip csg quota-server retransmit</a> | Defines the quota server retransmit time interval for the CSG2.                          |

## ip csg ipc retries

To define the maximum number of Interprocessor Communication (IPC) retries allowed before the CSG2 determines that the link has failed, use the **ip csg ipc retries** command in global configuration mode. To reset the number of IPC retries to the default value, use the **no** form of this command.

**ip csg ipc retries** *number-of-retries*

**no ip csg ipc retries**

### Syntax Description

|                          |  |
|--------------------------|--|
| <i>number-of-retries</i> | Maximum number of IPC retries allowed by the CSG2. The range is 1 to 65535. The default value is 20. |
|--------------------------|--|

### Defaults

The default value is 20 retries.

### Command Modes

Global configuration

### Command History

| Release    | Modification                 |
|------------|------------------------------|
| 12.4(11)MD | This command was introduced. |

### Usage Guidelines

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

### Examples

The following example shows how to allow two IPC retries:

```
ip csg ipc retries 2
```

### Related Commands

| Command                                     | Description  |
|---|--|
| <a href="#">ip csg bma retries</a>          | Defines the maximum number of Billing Mediation Agent (BMA) retries allowed before the CSG2 determines that the link has failed.         |
| <a href="#">ip csg psd retries</a>          | Defines the maximum number of Cisco Persistent Storage Device (PSD) retries allowed before the CSG2 determines that the link has failed. |
| <a href="#">ip csg quota-server retries</a> | Defines the maximum number of quota server retries allowed before the CSG2 determines that the link has failed.                          |

# ip csg iscsi drain delay

To define the delay interval, in seconds, before draining packets from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) when the Billing Mediation Agent (BMA) becomes active, use the **ip csg iscsi drain delay** command in global configuration mode. To delete the drain delay interval, use the **no** form of this command.

**ip csg iscsi drain delay** *number-of-seconds*

**no ip csg iscsi drain delay**

|                           |                          |   |
|---------------------------|--------------------------|---|
| <b>Syntax Description</b> | <i>number-of-seconds</i> | Delay interval, in seconds, before draining packets from the SAN. The range is 0 to 3. The default value is 3. A value of 0 means no delay. |
|---------------------------|--------------------------|---|

|                 |                                 |
|-----------------|---------------------------------|
| <b>Defaults</b> | The default value is 3 seconds. |
|-----------------|---------------------------------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | Global configuration |
|----------------------|----------------------|

|                        |                |                              |
|------------------------|----------------|------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|                        | 12.4(15)MD     | This command was introduced. |

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | The CSG2 can buffer GTP' messages in the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI), if so configured. (For more information, see the <a href="#">“Configuring iSCSI Support” section on page 8-1.</a> ) By default, the CSG2 limits the rate at which GTP' messages are read from the SAN to 167 packets/second (500 packets/3 seconds). However, you can use the <b>ip csg iscsi drain delay</b> command to change that rate. For example, specifying an interval of 2 seconds yields a rate of 250 packets/second (500 packets/2 seconds). |
|-------------------------|--|

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example shows how to specify a SAN drain delay interval of 2 seconds: |
|-----------------|---|

```
ip csg iscsi drain delay 2
```

|                         |   |  |
|-------------------------|---|--|
| <b>Related Commands</b> | <b>Command</b>                            | <b>Description</b>   |
|                         | <a href="#">ip csg iscsi drain packet</a> | Defines the number of packets to be drained from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) per drain delay interval when the Billing Mediation Agent (BMA) becomes active. |
|                         | <a href="#">ip csg iscsi profile</a>      | Specifies the Internet Small Computer Systems Interface (iSCSI) target to be used as backup storage for the CSG2.  |
|                         | <a href="#">ip iscsi target-profile</a>   | Creates an iSCSI profile for an iSCSI target on the CSG2, and enters iSCSI configuration mode.   |

# ip csg iscsi drain packet

To define the number of packets to be drained from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) per drain delay interval when the Billing Mediation Agent (BMA) becomes active, use the **ip csg iscsi drain packet** command in global configuration mode. To delete the drain packet, use the **no** form of this command.

**ip csg iscsi drain packet** *number-of-packets*

**no ip csg iscsi drain packet**

|                           |                          |  |
|---------------------------|--------------------------|--|
| <b>Syntax Description</b> | <i>number-of-packets</i> | Number of packets to be drained from the SAN per drain delay interval. The range is from 1 to 64000. The default is 500. |
|---------------------------|--------------------------|--|

|                 |                                   |
|-----------------|-----------------------------------|
| <b>Defaults</b> | The default value is 500 packets. |
|-----------------|-----------------------------------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | Global configuration |
|----------------------|----------------------|

|                        |                |                              |
|------------------------|----------------|------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|                        | 12.4(15)MD     | This command was introduced. |

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | The CSG2 can buffer GTP' messages in the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI), if so configured. (For more information, see the <a href="#">“Configuring iSCSI Support” section on page 8-1.</a> ) By default, the CSG2 limits the rate at which GTP' messages are read from the SAN to 167 packets/second (500 packets/3 seconds). However, you can use the <b>ip csg iscsi drain packet</b> command to change that rate. For example, specifying that 600 packets are to be drained per interval yields a rate of 200 packets/second (600 packets/3 seconds). |
|-------------------------|--|

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example shows how to specify that 1000 packets are to be drained from the SAN per drain delay interval: |
|-----------------|---|

```
ip csg iscsi drain packet 1000
```

|                         |  |   |
|-------------------------|--|---|
| <b>Related Commands</b> | <b>Command</b>                           | <b>Description</b>  |
|                         | <a href="#">ip csg iscsi drain delay</a> | Defines the delay interval, in seconds, before draining packets from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) when the Billing Mediation Agent (BMA) becomes active. |

| Command                              | Description   |
|--------------------------------------|---|
| <code>ip csg iscsi profile</code>    | Specifies the Internet Small Computer Systems Interface (iSCSI) target to be used as backup storage for the CSG2. |
| <code>ip iscsi target-profile</code> | Creates an iSCSI profile for an iSCSI target on the CSG2, and enters iSCSI configuration mode.                    |

# ip csg iscsi profile

To specify the Internet Small Computer Systems Interface (iSCSI) target to be used as backup storage for the CSG2, use the **ip csg iscsi profile** command in global configuration mode. To delete the iSCSI target, use the **no** form of this command.

**ip csg iscsi profile** *target-profile-name*

**no ip csg iscsi profile**

## Syntax Description

|                            |  |
|----------------------------|--|
| <i>target-profile-name</i> | Name of the iSCSI target profile to be used as backup storage. |
|----------------------------|--|

## Defaults

No iSCSI target is specified.

## Command Modes

Global configuration

## Command History

| Release    | Modification                 |
|------------|------------------------------|
| 12.4(15)MD | This command was introduced. |

## Usage Guidelines

You can associate one and only one iSCSI target profile with each CSG2.

## Examples

The following example shows how to specify CSG\_BACKUP as the iSCSI target:

```
ip csg iscsi profile CSG_BACKUP
```

## Related Commands

| Command                                   | Description  |
|---|--|
| <a href="#">ip csg iscsi drain delay</a>  | Defines the delay interval, in seconds, before draining packets from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) when the Billing Mediation Agent (BMA) becomes active.      |
| <a href="#">ip csg iscsi drain packet</a> | Defines the number of packets to be drained from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) per drain delay interval when the Billing Mediation Agent (BMA) becomes active. |
| <a href="#">ip iscsi target-profile</a>   | Creates an iSCSI profile for an iSCSI target on the CSG2, and enters iSCSI configuration mode.   |



# ip csg map

To define the CSG2 billing content filters (header, method, and URL maps), and to enter CSG2 map configuration mode, use the **ip csg map** command in global configuration mode. To turn off the service, use the **no** form of this command.

```
ip csg map map-name
```

```
no ip csg map map-name
```

## Syntax Description

|                 |   |
|-----------------|---|
| <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 CSG2 changes all letters to uppercase), numbers, and any special characters. |
|-----------------|---|

## Defaults

None

## Command Modes

Global configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.                                       |
|            | Changes from CSG1: The <b>header</b> and <b>url</b> keywords were removed. |

## Usage Guidelines

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

The headers, methods, or URLs that are to be matched against a pattern are defined by the following commands:

- [match header](#)
- [match method](#)
- [match url](#)

When configuring a map, keep the following considerations in mind:

- We recommend that you configure the URL match pattern during your maintenance window, or during off-peak hours.
- You cannot specify different types of match patterns in a given map. For example, a map can include one or more **match header** statements, but it cannot include both **match header** statements and **match url** statements.
- You can specify up to three maps in a given policy: one for header matching, one for method matching, and one for URL matching. For example, the following is a valid configuration:

```
ip csg map HOSTMAP
  match header host1 value *.2.*.44
!
```

```

ip csg map URLMAP
  match url */mobile/index.wml
!
ip csg policy MAP-POLICY
  map HOSTMAP
  map URLMAP

```

In this example, a flow must match both HOSTMAP and URLMAP in order to match policy MAP-POLICY.

## Examples

The following example shows how to configure a CSG2 URL map named MOVIES:

```

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

```

## Related Commands

| Command                               | Description   |
|---------------------------------------|---|
| <a href="#">ip csg case-sensitive</a> | Specifies whether to treat CSG2 sticky objects and header, method, and URL match patterns as case-sensitive.        |
| <a href="#">ip csg policy</a>         | Defines a policy for qualifying flows for the CSG2 accounting services, and enters CSG2 policy configuration mode,. |
| <a href="#">map</a>                   | References a header, method, or URL map that is part of a CSG2 billing policy.                                      |
| <a href="#">match header</a>          | Specifies a header match pattern for a CSG2 billing map.  |
| <a href="#">match method</a>          | Specifies a method match pattern for a CSG2 billing map.  |
| <a href="#">match url</a>             | Specifies a URL match pattern for a CSG2 billing map.   |

# ip csg mode single-tp

To enable the CSG2 to use a single traffic processor (TP) instead of multiple TPs, use the **ip csg mode single-tp** command in global configuration mode. To restore the default setting, use the **no** form of this command.

**ip csg mode single-tp**

**no ip csg mode single-tp**

**Syntax Description** This command has no arguments or keywords.

**Defaults** The CSG2 operates in multiple-TP mode.

**Command Modes** Global configuration

| Command History | Release    | Modification                 |
|-----------------|------------|------------------------------|
|                 | 12.4(11)MD | This command was introduced. |

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

Single-TP mode is required for HTTP X-Forwarded-For operation. Before configuring the CSG2 for X-Forwarded-For operation, configure the CSG2 for single-TP mode by entering the **ip csg mode single-tp** command, then performing a **write memory**, then restarting the CSG2.

To switch out of single-TP mode, enter the **no ip csg mode single-tp** command, then perform a **write memory**, then restart the CSG2.

If you intend to operate in single-TP mode, the **ip csg mode single-tp** command must be the first command in your CSG2 configuration.

**Examples** The following example shows how to configure single-TP mode for the CSG2:

```
ip csg mode single-tp
```

| Related Commands | Command   | Description  |
|------------------|---|--|
|                  | <a href="#">subscriber-ip http-header forwarded-for</a> | Specifies that the CSG2 is to obtain the subscriber's IP address from the HTTP X-Forwarded-For header. |

# ip csg policy

To define a policy for qualifying flows for the CSG2 billing services, and to enter CSG2 policy configuration mode, use the **ip csg policy** command in global configuration mode. To turn off the service, use the **no** form of this command.

**ip csg policy** *policy-name*

**no ip csg policy** *policy-name*

## Syntax Description

|                    |   |
|--------------------|---|
| <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 CSG2 changes all letters to uppercase), numbers, and any special characters. |
|--------------------|---|

## Defaults

None

## Command Modes

Global configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: None. |

## Usage Guidelines

Because of limitations on the number of URL match patterns that the CSG2 can handle, do not define more than 16,000 policies. For more information on URL match patterns, see the description of the [match url](#) command.

The characteristics of each policy are defined by the following commands:

- [accounting](#)
- [map](#)

When configuring a map, keep the following considerations in mind:

- You cannot specify different types of match patterns in a given map. For example, a map can include one or more **match header** statements, but it cannot include both **match header** statements and **match url** statements.
- You can specify up to three maps in a given policy: one for header matching, one for method matching, and one for URL matching. For example, the following is a valid configuration:

```
ip csg map HOSTMAP
  match header host1 value *.2.*.44
!
ip csg map URLMAP
  match url */mobile/index.wml
!
```

```
ip csg policy MAP-POLICY
map HOSTMAP
map URLMAP
```

In this example, a flow must match both HOSTMAP and URLMAP in order to match policy MAP-POLICY.

### Examples

The following example shows how to configure a CSG2 policy named MOVIES\_COMEDY:

```
ip csg policy MOVIES_COMEDY
```

### Related Commands

| Command                        | Description  |
|--------------------------------|--|
| <a href="#">accounting</a>     | Specifies accounting and an optional customer string for a CSG2 policy.  |
| <a href="#">ip csg content</a> | Configures content for CSG2 services, and enters CSG2 content configuration mode.                                |
| <a href="#">ip csg map</a>     | Defines the CSG2 billing content filters (header, method, and URL maps), and enters CSG2 map configuration mode. |
| <a href="#">ip csg service</a> | Configures a CSG2 content billing service, and enters CSG2 service configuration mode.                           |
| <a href="#">map</a>            | References a header, method, or URL map that is part of a CSG2 billing policy.                                   |
| <a href="#">match header</a>   | Specifies a header match pattern for a CSG2 billing map.   |
| <a href="#">match method</a>   | Specifies a method match pattern for a CSG2 billing map.   |
| <a href="#">match url</a>      | Specifies a URL match pattern for a CSG2 billing map.  |

# ip csg psd

To configure a Cisco Persistent Storage Device (PSD), use the **ip csg psd** command in global configuration mode. To remove the PSD, use the **no** form of this command.

**ip csg psd** [**vrf** *vrf-name*] *ip-address* *port-number*

**no ip csg psd** [**vrf** *vrf-name*] *ip-address* *port-number*

## Syntax Description

|                            |  |
|----------------------------|--|
| <b>vrf</b> <i>vrf-name</i> | (Optional) Virtual Routing and Forwarding (VRF) table which the CSG2 is to use to communicate with the PSD.  |
| <i>ip-address</i>          | IP address for packets destined for the PSD.<br><br>The CSG2 differentiates PSDs on the basis of their IP addresses. When you configure a PSD, make sure that its IP address matches on both the active CSG2 and the standby CSG2.   |
| <i>port-number</i>         | Port number for packets destined for the PSD.<br><br>The CSG2 differentiates PSDs on the basis of their port numbers. When you configure a PSD, make sure that its port number matches on both the active CSG2 and the standby CSG2. |

## Defaults

No PSDs are configured.  
If no VRF table is specified, the CSG2 uses the global routing table to communicate with the PSD.

## Command Modes

Global configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.<br><br>Changes from CSG1: <ul style="list-style-type: none"> <li>• The name of this command changed from <b>records-storage</b> to <b>ip csg psd</b>.</li> <li>• The configuration mode for this command changed from CSG accounting configuration to global configuration.</li> <li>• The <b>vrf</b> <i>vrf-name</i> keyword and argument were added.</li> </ul> |

## Usage Guidelines

You must specify the PSD local port using the **ip csg psd local-port** command before you enter the **ip csg psd** command.

You can configure only one PSD.

## Examples

The following example configures a PSD with IP address 1.2.3.4 and port number 7777, that uses VRF table PSDVRF to communicate with the CSG2:

```
ip csg psd vrf PSDVRF 1.2.3.4 7777
```

| Related Commands | Command                                 | Description   |
|------------------|---|---|
|                  | <a href="#">ip csg psd drain delay</a>  | Defines the delay interval, in seconds, before draining packets from the Cisco Persistent Storage Device (PSD) when the Billing Mediation Agent (BMA) becomes active.   |
|                  | <a href="#">ip csg psd drain packet</a> | Defines the number of packets to be drained from the Cisco Persistent Storage Device (PSD) per drain delay interval when the Billing Mediation Agent (BMA) becomes active.  |
|                  | <a href="#">ip csg psd keepalive</a>    | Defines the Cisco Persistent Storage Device (PSD) keepalive time interval for the CSG2.   |
|                  | <a href="#">ip csg psd local-port</a>   | Configures the local port on which the CSG2 communicates with the Cisco Persistent Storage Device (PSD).  |
|                  | <a href="#">ip csg psd margin</a>       | Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages, beyond the size of the Billing Mediation Agent (BMA) message queue, that the CSG2 can buffer for the Cisco Persistent Storage Device (PSD). |
|                  | <a href="#">ip csg psd margin</a>       | Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages, beyond the size of the Billing Mediation Agent (BMA) message queue, that the CSG2 can buffer for the Cisco Persistent Storage Device (PSD). |
|                  | <a href="#">ip csg psd retransmit</a>   | Defines the Cisco Persistent Storage Device (PSD) retransmit time interval for the CSG2.  |
|                  | <a href="#">ip csg psd retries</a>      | Defines the maximum number of Cisco Persistent Storage Device (PSD) retries allowed before the CSG2 determines that the link has failed.  |
|                  | <a href="#">ip csg psd window</a>       | Defines the Cisco Persistent Storage Device (PSD) transmit window size for the CSG2.  |

# ip csg psd drain delay

To define the delay interval, in seconds, before draining packets from the Cisco Persistent Storage Device (PSD) when the Billing Mediation Agent (BMA) becomes active, use the **ip csg psd drain delay** command in global configuration mode. To delete the drain delay interval, use the **no** form of this command.

**ip csg psd drain delay** *number-of-seconds*

**no ip csg psd drain delay**

|                           |                          |   |
|---------------------------|--------------------------|---|
| <b>Syntax Description</b> | <i>number-of-seconds</i> | Delay interval, in seconds, before draining packets from the PSD. The range is 0 to 3. The default value is 1. A value of 0 means no delay. |
|---------------------------|--------------------------|---|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | The default value is 1 second. |
|-----------------|--------------------------------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | Global configuration |
|----------------------|----------------------|

|                        |                |                              |
|------------------------|----------------|------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|                        | 12.4(11)MD     | This command was introduced. |

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | The CSG2 can buffer GTP' messages in the Cisco Persistent Storage Device (PSD), if so configured. (For more information, see the <a href="#">“Configuring PSD Support” section on page 7-1.</a> ) By default, the CSG2 limits the rate at which GTP' messages are read from the PSD to 500 packets/second. However, you can use the <b>ip csg psd drain delay</b> command to change that rate. For example, specifying an interval of 2 seconds yields a rate of 250 packets/second (500 packets/2 seconds). |
|-------------------------|--|

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example shows how to specify a PSD drain delay interval of 2 seconds: |
|-----------------|---|

```
ip csg psd drain delay 2
```

|                         |   |  |
|-------------------------|---|--|
| <b>Related Commands</b> | <b>Command</b>                          | <b>Description</b>   |
|                         | <a href="#">ip csg psd</a>              | Configures a Cisco Persistent Storage Device (PSD).  |
|                         | <a href="#">ip csg psd drain packet</a> | Defines the number of packets to be drained from the Cisco Persistent Storage Device (PSD) per drain delay interval when the Billing Mediation Agent (BMA) becomes active. |



# ip csg psd drain packet

To define the number of packets to be drained from the Cisco Persistent Storage Device (PSD) per drain delay interval when the Billing Mediation Agent (BMA) becomes active, use the **ip csg psd drain packet** command in global configuration mode. To delete the drain packet, use the **no** form of this command.

**ip csg psd drain packet** *number-of-packets*

**no ip csg psd drain packet**

|                           |                          |  |
|---------------------------|--------------------------|--|
| <b>Syntax Description</b> | <i>number-of-packets</i> | Number of packets to be drained from the PSD per drain delay interval. The range is from 1 to 64000. The default is 500. |
|---------------------------|--------------------------|--|

|                 |                                   |
|-----------------|-----------------------------------|
| <b>Defaults</b> | The default value is 500 packets. |
|-----------------|-----------------------------------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | Global configuration |
|----------------------|----------------------|

|                        |                |                              |
|------------------------|----------------|------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|                        | 12.4(11)MD     | This command was introduced. |

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | The CSG2 can buffer GTP' messages in the Cisco Persistent Storage Device (PSD), if so configured. (For more information, see the <a href="#">“Configuring PSD Support” section on page 7-1.</a> ) By default, the CSG2 limits the rate at which GTP' messages are read from the PSD to 500 packets/second. However, you can use the <b>ip csg psd drain packet</b> command to change that rate. For example, specifying that 1000 packets are to be drained per interval yields a rate of 1000 packets/second (1000 packets/1 second). |
|-------------------------|--|

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example shows how to specify that 1000 packets are to be drained from the PSD per drain delay interval: |
|-----------------|---|

```
ip csg psd drain packet 1000
```

|                         |  |   |
|-------------------------|--|---|
| <b>Related Commands</b> | <b>Command</b>                         | <b>Description</b>  |
|                         | <a href="#">ip csg psd</a>             | Configures a Cisco Persistent Storage Device (PSD).   |
|                         | <a href="#">ip csg psd drain delay</a> | Defines the delay interval, in seconds, before draining packets from the Cisco Persistent Storage Device (PSD) when the Billing Mediation Agent (BMA) becomes active. |

# ip csg psd keepalive

To define the Cisco Persistent Storage Device (PSD) keepalive time interval for the CSG2, use the **ip csg psd keepalive** command in global configuration mode. To reset the PSD keepalive timer to the default value, use the **no** form of this command.

**ip csg psd keepalive** *number-of-seconds*

**no ip csg psd keepalive**

|                           |                          |  |
|---------------------------|--------------------------|--|
| <b>Syntax Description</b> | <i>number-of-seconds</i> | Time, in seconds, between PSD keepalives. The range is from 1 to 65535. The default value is 60. |
|---------------------------|--------------------------|--|

|                 |                                  |
|-----------------|----------------------------------|
| <b>Defaults</b> | The default value is 60 seconds. |
|-----------------|----------------------------------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | Global configuration |
|----------------------|----------------------|

|                        |                |                              |
|------------------------|----------------|------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|                        | 12.4(11)MD     | This command was introduced. |

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | We recommend that you change the keepalive time interval only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting. |
|-------------------------|---|

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example shows how to specify a PSD keepalive time of 300 seconds: |
|-----------------|---|

```
ip csg psd keepalive 300
```

|                         |   |  |
|-------------------------|---|--|
| <b>Related Commands</b> | <b>Command</b>                                | <b>Description</b>   |
|                         | <a href="#">ip csg bma keepalive</a>          | Defines the Billing Mediation Agent (BMA) keepalive time interval for the CSG2.      |
|                         | <a href="#">ip csg ipc keepalive</a>          | Defines the Interprocessor Communication (IPC) keepalive time interval for the CSG2. |
|                         | <a href="#">ip csg psd</a>                    | Configures a Cisco Persistent Storage Device (PSD).                                  |
|                         | <a href="#">ip csg quota-server keepalive</a> | Defines the quota-server keepalive time interval for the CSG2.                       |

# ip csg psd local-port

To configure the local port on which the CSG2 communicates with the Cisco Persistent Storage Device (PSD), use the **ip csg psd local-port** command in global configuration mode. To remove a quota server local port configuration, use the **no** form of this command.

**ip csg psd local-port** *port-number*

**no ip csg psd local-port**

## Syntax Description

|                    |   |
|--------------------|---|
| <i>port-number</i> | Port number on which the CSG2 is to communicate with the PSD. The range is from 1024 to 65535. 5000 is not a valid port number.<br><br>The PSD local port number must be different from the Billing Mediation Agent (BMA) local port number and from the quota server local port number (configured with the <b>ip csg bma local-port</b> command and the <b>ip csg quota-server local-port</b> command, respectively). |
|--------------------|---|

## Defaults

No PSD local port is configured.

## Command Modes

Global configuration

## Command History

| Release    | Modification  |
|------------|---|
| 12.4(11)MD | This command was migrated from CSG1.<br><br>Changes from CSG1: <ul style="list-style-type: none"> <li>The name of this command changed from <b>records-storage local-port</b> to <b>ip csg psd local-port</b>.</li> <li>The configuration mode for this command changed from CSG accounting configuration to global configuration.</li> </ul> |

## Usage Guidelines

You must specify the PSD local port using the **ip csg psd local-port** command before you enter the **ip csg psd** command.

You can configure only one PSD.

## Examples

The following example configures a PSD with local port number 7777:

```
ip csg psd local-port 7777
```

| Related Commands | Command  | Description  |
|------------------|--|--|
|                  | <a href="#">ip csg bma local-port</a>          | Configures the local port on which the CSG2 communicates with the Billing Mediation Agent (BMA). |
|                  | <a href="#">ip csg psd</a>                     | Configures a Cisco Persistent Storage Device (PSD).  |
|                  | <a href="#">ip csg quota-server local-port</a> | Configures the local port on which the CSG2 communicates with quota servers.                     |

# ip csg psd margin

To specify the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages, beyond the size of the Billing Mediation Agent (BMA) message queue, that the CSG2 can buffer for the Cisco Persistent Storage Device (PSD), use the **ip csg psd margin** command in global configuration mode. To restore the default setting, use the **no** form of this command.

**ip csg psd margin** *number*

**no ip csg psd margin**

|                           |               |   |
|---------------------------|---------------|---|
| <b>Syntax Description</b> | <i>number</i> | Maximum number of GTP' messages, beyond the size of the BMA message queue, that can be buffered for the PSD. The range is from 100 to 65535. The default is 2000. |
|---------------------------|---------------|---|

**Defaults** The CSG2 buffers up to 2000 GTP' messages, beyond the size of the BMA message queue.

**Command Modes** Global configuration

|                        |                |                              |
|------------------------|----------------|------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|                        | 12.4(11)MD     | This command was introduced. |

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

**Examples** The following example shows how to configure the CSG2 to buffer up to 3000 GTP' messages, beyond the size of the BMA message queue:

```
ip csg psd margin 2000
```

|                         |                                     |  |
|-------------------------|-------------------------------------|--|
| <b>Related Commands</b> | <b>Command</b>                      | <b>Description</b>   |
|                         | <a href="#">ip csg bma messages</a> | Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages that the CSG2 can buffer for all Billing Mediation Agents (BMAs). |
|                         | <a href="#">ip csg psd</a>          | Configures a Cisco Persistent Storage Device (PSD).  |

# ip csg psd retransmit

To define the Cisco Persistent Storage Device (PSD) retransmit time interval for the CSG2, use the **ip csg psd retransmit** command in global configuration mode. To reset the PSD retransmit timer to the default value, use the **no** form of this command.

```
ip csg psd retransmit number-of-seconds
```

```
no ip csg psd retransmit
```

|                           |                          |   |
|---------------------------|--------------------------|---|
| <b>Syntax Description</b> | <i>number-of-seconds</i> | Time, in seconds, between PSD retransmits. The range is 1 to 65535. The default value is 4. |
|---------------------------|--------------------------|---|

|                 |                                 |
|-----------------|---------------------------------|
| <b>Defaults</b> | The default value is 4 seconds. |
|-----------------|---------------------------------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | Global configuration |
|----------------------|----------------------|

|                        |                |                              |
|------------------------|----------------|------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|                        | 12.4(11)MD     | This command was introduced. |

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | We recommend that you change the retransmit time interval only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting. |
|-------------------------|--|

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following example shows how to specify a PSD retransmit time of 2 seconds: |
|-----------------|--|

```
ip csg psd retransmit 2
```

| <b>Related Commands</b> | <b>Command</b>                                 | <b>Description</b>  |
|-------------------------|--|---|
|                         | <a href="#">ip csg bma retransmit</a>          | Defines the Billing Mediation Agent (BMA) retransmit time interval for the CSG2.      |
|                         | <a href="#">ip csg ipc retransmit</a>          | Defines the Interprocessor Communication (IPC) retransmit time interval for the CSG2. |
|                         | <a href="#">ip csg psd</a>                     | Configures a Cisco Persistent Storage Device (PSD).                                   |
|                         | <a href="#">ip csg quota-server retransmit</a> | Defines the quota server retransmit time interval for the CSG2.                       |

# ip csg psd retries

To define the maximum number of Cisco Persistent Storage Device (PSD) retries allowed before the CSG2 determines that the link has failed, use the **ip csg psd retries** command in global configuration mode. To reset the number of PSD retries to the default value, use the **no** form of this command.

```
ip csg psd retries [packet] number-of-retries
```

```
no ip csg psd retries
```

## Syntax Description

|                          |  |
|--------------------------|--|
| <b>packet</b>            | (Optional) Attempt to send a packet to the PSD the specified number of times, then discard the packet. |
| <i>number-of-retries</i> | Maximum number of PSD retries allowed by the CSG2. The range is 1 to 65535. The default value is 3.    |

## Defaults

The default value is 3 retries.

## Command Modes

Global configuration

## Command History

| Release    | Modification                         |
|------------|--------------------------------------|
| 12.4(11)MD | This command was introduced.         |
| 12.4(15)MD | The <b>packet</b> keyword was added. |

## Usage Guidelines

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

By default, the CSG2 retries a packet forever; it never discards a packet. If you configure the **ip csg psd retries packet** command, the CSG2 tries to send a packet to the PSD the specified number of times, then discards the packet. (The first attempt to send a packet to the PSD is not counted as a retry.) For example, if you configure **ip csg psd retries packet 4**, the CSG2 tries to send a packet to the PSD five times before discarding it (the initial attempt plus four retries).

## Examples

The following example shows how to allow two PSD retries:

```
ip csg psd retries 2
```

The following example shows how to allow the CSG2 to try to send a packet to the PSD four times, in addition to the initial attempt:

```
ip csg psd retries packet 4
```

| Related Commands | Command                                     | Description   |
|------------------|---|---|
|                  | <a href="#">ip csg bma retries</a>          | Defines the maximum number of Billing Mediation Agent (BMA) retries allowed before the CSG2 determines that the link has failed.      |
|                  | <a href="#">ip csg ipc retries</a>          | Defines the maximum number of Interprocessor Communication (IPC) retries allowed before the CSG2 determines that the link has failed. |
|                  | <a href="#">ip csg psd</a>                  | Configures a Cisco Persistent Storage Device (PSD).   |
|                  | <a href="#">ip csg quota-server retries</a> | Defines the maximum number of Billing Mediation Agent (BMA) retries allowed before the CSG2 determines that the link has failed.      |



# ip csg psd window

To define the Cisco Persistent Storage Device (PSD) transmit window size for the CSG2, use the **ip csg psd window** command in global configuration mode. To reset the PSD transmit window size to the default value, use the **no** form of this command.

```
ip csg psd window {max window-size | min window-size | min auto}
```

```
no ip csg psd window {max | min}
```

## Syntax Description

|                               |  |
|-------------------------------|--|
| <b>max</b> <i>window-size</i> | Maximum size, in packets, of the PSD transmit window. The range is 1 to 65535. The default value is 128.   |
| <b>min</b> <i>window-size</i> | Minimum size, in packets, of the PSD transmit window. The range is 1 to 65535.   |
| <b>min auto</b>               | Specifies that the CSG2 is to determine the minimum size of the PSD transmit window automatically. The CSG2 keeps track of the maximum number of ACKs received in one response and sets that number as the minimum window. |

## Defaults

The default maximum window size is 128 packets.  
The default minimum window size is automatically determined by the CSG2.

## Command Modes

Global configuration

## Command History

| Release    | Modification                 |
|------------|------------------------------|
| 12.4(11)MD | This command was introduced. |

## Usage Guidelines

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

## Examples

The following example shows how to set the maximum PSD transmit window to 64 packets:

```
ip csg psd window max 64
```

## Related Commands

| Command                                    | Description  |
|--|--|
| <a href="#">ip csg bma window</a>          | Defines the Billing Mediation Agent (BMA) transmit window size for the CSG2. |
| <a href="#">ip csg psd</a>                 | Configures a Cisco Persistent Storage Device (PSD).                          |
| <a href="#">ip csg quota-server window</a> | Defines the quota server transmit window size for the CSG2.                  |

## ip csg quota-server

To configure the CSG2 quota servers that return billing quota values for subscribers, use the **ip csg quota-server** command in global configuration mode. To remove a quota server configuration, use the **no** form of this command.

```
ip csg quota-server [vrf vrf-name] ip-address port-number priority
```

```
no ip csg quota-server [vrf vrf-name] ip-address port-number
```

### Syntax Description

|                     |   |
|---------------------|---|
| <i>vrf vrf-name</i> | (Optional) Virtual Routing and Forwarding (VRF) table which the CSG2 is to use to communicate with the quota server.  |
| <i>ip-address</i>   | IP address of the quota server.<br><br>The CSG2 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 CSG2 and the standby CSG2.<br><br>You can configure up to 10 quota servers. Each quota server must have a unique IP address (or a unique IP address-VRF name combination, if VRF is configured).   |
| <i>port-number</i>  | Port number of the quota server. The range is from 1 to 65535.<br><br>The CSG2 differentiates quota servers on the basis of their port numbers. When you configure a quota server, make sure that its port number matches on both the active CSG2 and the standby CSG2.   |
| <i>priority</i>     | Defines active and standby quota servers.<br><br>The priority specifies the order of preference of the quota servers. A lower number indicates a higher priority. If the current quota server becomes unusable, the CSG2 uses the highest priority quota server available.<br><br>The range of priorities is from 1 to 1000, but you can configure only up to 10 quota servers. Each quota server must be configured with a unique priority. Priorities for different quota servers do not have to be sequential. That is, you can have three quota servers with priorities 1, 5, and 10, respectively. |

### Defaults

No quota servers are configured.  
If no VRF table is specified, the CSG2 uses the global routing table to communicate with the quota server.

### Command Modes

Global configuration

**Command History**

| Release    | Modification  |
|------------|---|
| 12.4(11)MD | <p>This command was migrated from CSG1.</p> <p>Changes from CSG1:</p> <ul style="list-style-type: none"> <li>• The name of this command changed from <b>quota server</b> to <b>ip csg quota-server</b>.</li> <li>• The configuration mode for this command changed from CSG user group configuration to global configuration.</li> <li>• The <b>vrf</b> <i>vrf-name</i> keyword and argument were added.</li> <li>• The <b>reassign</b> keyword was removed.</li> </ul> |

**Usage Guidelines**

For prepaid billing, you must configure at least one quota server.

You can configure up to 10 quota servers. Each quota server must have a unique priority and a unique IP address (or a unique IP address-VRF name combination, if VRF is configured).

**Note**

The CSG2 does not support multiple quota servers that have the same IP address.

A quota server can recognize a duplicate quota-download request, as when general packet radio service (GPRS) tunneling protocol (GTP) retransmits a packet. When the quota server detects a duplicate quota-download request, it resends the same quota that it sent for the original request.

To disable quota server reassignment (that is, to prevent the CSG2 from assigning a new quota server to a subscriber if the original quota server fails), use the **no** form of the **ip csg quota-server reassign** command.

**Examples**

The following example configures a quota server with IP address 1.2.3.4, port number 6666, and priority 10, that uses VRF table QSVRF to communicate with the CSG2:

```
ip csg quota-server vrf QSVRF 1.2.3.4 6666 10
```

**Related Commands**

| Command                               | Description  |
|---------------------------------------|--|
| <b>ip csg quota-server activate</b>   | Activates one or more quota servers.   |
| <b>ip csg quota-server keepalive</b>  | Defines the quota server keepalive time interval for the CSG2.   |
| <b>ip csg quota-server local-port</b> | Configures the local port on which the CSG2 communicates with quota servers.   |
| <b>ip csg quota-server messages</b>   | Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages that the CSG2 can buffer for all quota servers. |
| <b>ip csg quota-server reassign</b>   | Reassigns subscribers to a different CSG2 quota server after a failure.  |
| <b>ip csg quota-server retransmit</b> | Defines the quota server retransmit time interval for the CSG2.  |
| <b>ip csg quota-server retries</b>    | Defines the maximum number of quota server retries allowed before the CSG2 determines that the link has failed.  |
| <b>ip csg quota-server window</b>     | Defines the quota server transmit window size for the CSG2.  |

# ip csg quota-server activate

To activate one or more quota servers, use the **ip csg quota-server activate** command in global configuration mode. To deactivate quota servers, use the **no** form of this command.

**ip csg quota-server activate** *number*

**no ip csg quota-server activate**

|                           |               |   |
|---------------------------|---------------|---|
| <b>Syntax Description</b> | <i>number</i> | Number of quota servers to activate. The range is from 1 to 32. The default value is 1. |
|---------------------------|---------------|---|

|                 |                         |
|-----------------|-------------------------|
| <b>Defaults</b> | The default value is 1. |
|-----------------|-------------------------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | Global configuration |
|----------------------|----------------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>  |
|------------------------|----------------|--|
|                        | 12.4(11)MD     | This command was migrated from CSG1.<br>Changes from CSG1: <ul style="list-style-type: none"> <li>• The name of this command changed from <b>quota activate</b> to <b>ip csg quota-server activate</b>.</li> <li>• The configuration mode for this command changed from CSG user group configuration to global configuration.</li> <li>• The range for the <i>number</i> argument changed from 1 to 10, to 1 to 32.</li> </ul> |

**Examples** The following example shows how to activate two quota servers:

```
ip csg quota-server activate 2
```

| <b>Related Commands</b> | <b>Command</b>                      | <b>Description</b>  |
|-------------------------|-------------------------------------|---|
|                         | <a href="#">ip csg bma activate</a> | Enables support for multiple active Billing Mediation Agents (BMAs)                 |
|                         | <a href="#">ip csg quota-server</a> | Configures the CSG2 quota servers that return billing quota values for subscribers. |

# ip csg quota-server keepalive

To define the quota server keepalive time interval for the CSG2, use the **ip csg quota-server keepalive** command in global configuration mode. To reset the quota server keepalive timer to the default value, use the **no** form of this command.

**ip csg quota-server keepalive** *number-of-seconds*

**no ip csg quota-server keepalive**

|                           |                          |  |
|---------------------------|--------------------------|--|
| <b>Syntax Description</b> | <i>number-of-seconds</i> | Time, in seconds, between quota server keepalives. The range is 1 to 65535. The default value is 60. |
|---------------------------|--------------------------|--|

|                 |                                  |
|-----------------|----------------------------------|
| <b>Defaults</b> | The default value is 60 seconds. |
|-----------------|----------------------------------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | Global configuration |
|----------------------|----------------------|

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|------------------------|----------------|------------------------------|
|                        | 12.4(11)MD     | This command was introduced. |

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | We recommend that you change the keepalive time interval only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting. |
|-------------------------|---|

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following example shows how to specify a quota server keepalive time of 300 seconds:<br><pre>ip csg quota-server keepalive 300</pre> |
|-----------------|--|

| <b>Related Commands</b> | <b>Command</b>                       | <b>Description</b>  |
|-------------------------|--------------------------------------|---|
|                         | <a href="#">ip csg bma keepalive</a> | Defines the Billing Mediation Agent (BMA) keepalive time interval for the CSG2.         |
|                         | <a href="#">ip csg ipc keepalive</a> | Defines the Interprocessor Communication (IPC) keepalive time interval for the CSG2.    |
|                         | <a href="#">ip csg psd keepalive</a> | Defines the Cisco Persistent Storage Device (PSD) keepalive time interval for the CSG2. |
|                         | <a href="#">ip csg quota-server</a>  | Configures the CSG2 quota servers that return billing quota values for subscribers.     |

# ip csg quota-server local-port

To configure the local port on which the CSG2 communicates with quota servers, use the **ip csg quota-server local-port** command in global configuration mode. To remove a quota server local port configuration, use the **no** form of this command.

**ip csg quota-server local-port** *port-number*

**no ip csg quota-server local-port**

## Syntax Description

|                    |  |
|--------------------|--|
| <i>port-number</i> | Port number on which the CSG2 is to communicate with quota servers. The range is from 1024 to 65535. 5000 is not a valid port number.<br><br>The quota server local port number must be different from the Billing Mediation Agent (BMA) local port number and from the Persistent Storage Device (PSD) local port number (configured with the <b>ip csg bma local-port</b> command and the <b>ip csg psd local-port</b> command, respectively). |
|--------------------|--|

## Defaults

No quota server local ports are configured.

## Command Modes

Global configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.<br><br>Changes from CSG1: <ul style="list-style-type: none"> <li>The name of this command changed from <b>quota local-port</b> to <b>ip csg quota-server local-port</b>.</li> <li>The configuration mode for this command changed from CSG user group configuration to global configuration.</li> <li>The range for the <i>port-number</i> argument changed from 1 to 65535, to 1024 to 65535.</li> </ul> |

## Usage Guidelines

For prepaid billing, you must configure a quota server local port.



### Note

The CSG2 drops requests (such as nodealive, echo, and redirect requests) unless they come from a configured quota server IP address. The CSG2 also verifies IP addresses against the configured list of quota servers. If there is no match, the CSG2 drops the request. The CSG2 does not look at a request's source port; the CSG2 replies to the port from which the request came.

**Examples**

The following example configures quota server local port 6666:

```
ip csg quota-server local-port 6666
```

**Related Commands**

| Command                               | Description  |
|---------------------------------------|--|
| <a href="#">ip csg bma local-port</a> | Configures the local port on which the CSG2 communicates with the Billing Mediation Agent (BMA).         |
| <a href="#">ip csg psd local-port</a> | Configures the local port on which the CSG2 communicates with the Cisco Persistent Storage Device (PSD). |
| <a href="#">ip csg quota-server</a>   | Configures the CSG2 quota servers that return billing quota values for subscribers.                      |

## ip csg quota-server messages

To specify the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages that the CSG2 can buffer for all quota servers, use the **ip csg quota-server messages** command in global configuration mode. To restore the default settings, use the **no** form of this command.

**ip csg quota-server messages** *number*

**no ip csg quota-server messages**

### Syntax Description

|               |   |
|---------------|---|
| <i>number</i> | Maximum number of GTP' messages that can be buffered for all quota servers. The range is from 1 to 65535. The default is 10000. |
|---------------|---|

### Defaults

The CSG2 buffers up to 10000 GTP' messages.

### Command Modes

Global configuration

### Command History

| Release    | Modification                 |
|------------|------------------------------|
| 12.4(11)MD | This command was introduced. |

### Usage Guidelines

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

### Examples

The following example shows how to configure the CSG2 to buffer up to 12345 GTP' messages:

```
ip csg quota-server messages 12345
```

### Related Commands

| Command                             | Description   |
|-------------------------------------|---|
| <a href="#">ip csg bma messages</a> | Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages that the CSG2 can buffer for all Billing Mediation Agents (BMAs).  |
| <a href="#">ip csg psd margin</a>   | Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages, beyond the size of the Billing Mediation Agent (BMA) message queue, that the CSG2 can buffer for the Cisco Persistent Storage Device (PSD). |
| <a href="#">ip csg quota-server</a> | Configures the CSG2 quota servers that return billing quota values for subscribers.   |



# ip csg quota-server reassign

To reassign subscribers to a different CSG2 quota server after a failure, use the **ip csg quota-server reassign** command in global configuration mode. To disable quota server reassignment for subscribers, use the **no** form of this command.

**ip csg quota-server reassign**

**no ip csg quota-server reassign**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Subscribers are reassigned to a different quota server after a failure.

## Command Modes

Global configuration

## Command History

| Release    | Modification                 |
|------------|------------------------------|
| 12.4(11)MD | This command was introduced. |

## Examples

The following example reassigns subscribers after a quota server failure:

```
ip csg quota-server reassign
```

## Related Commands

| Command                             | Description   |
|-------------------------------------|---|
| <a href="#">ip csg quota-server</a> | Configures the CSG2 quota servers that return billing quota values for subscribers. |

# ip csg quota-server retransmit

To define the quota server retransmit time interval for the CSG2, use the **ip csg quota-server retransmit** command in global configuration mode. To reset the quota server retransmit timer to the default value, use the **no** form of this command.

**ip csg quota-server retransmit** *number-of-seconds*

**no ip csg quota-server retransmit**

|                           |                          |  |
|---------------------------|--------------------------|--|
| <b>Syntax Description</b> | <i>number-of-seconds</i> | Time, in seconds, between quota server retransmits. The range is 1 to 65535. The default value is 4. |
|---------------------------|--------------------------|--|

**Defaults** The default value is 4 seconds.

**Command Modes** Global configuration

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|------------------------|----------------|------------------------------|
|                        | 12.4(11)MD     | This command was introduced. |

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

**Examples** The following example shows how to specify a quota server retransmit time of 2 seconds:

```
ip csg quota-server retransmit 2
```

| <b>Related Commands</b> | <b>Command</b>                        | <b>Description</b>   |
|-------------------------|---------------------------------------|--|
|                         | <a href="#">ip csg bma retransmit</a> | Defines the Billing Mediation Agent (BMA) retransmit time interval for the CSG2.         |
|                         | <a href="#">ip csg ipc retransmit</a> | Defines the Interprocessor Communication (IPC) retransmit time interval for the CSG2.    |
|                         | <a href="#">ip csg psd retransmit</a> | Defines the Cisco Persistent Storage Device (PSD) retransmit time interval for the CSG2. |
|                         | <a href="#">ip csg quota-server</a>   | Configures the CSG2 quota servers that return billing quota values for subscribers.      |

# ip csg quota-server retries

To define the maximum number of quota server retries allowed before the CSG2 determines that the link has failed, use the **ip csg quota-server retries** command in global configuration mode. To reset the number of quota server retries to the default value, use the **no** form of this command.

```
ip csg quota-server retries [packet] number-of-retries
```

```
no ip csg quota-server retries
```

## Syntax Description

|                          |   |
|--------------------------|---|
| <b>packet</b>            | (Optional) Attempt to send a packet to the quota server the specified number of times, then discard the packet. |
| <i>number-of-retries</i> | Maximum number of quota server retries allowed by the CSG2. The range is 1 to 65535. The default value is 3.    |

## Defaults

The default value is 3 retries.

## Command Modes

Global configuration

## Command History

| Release    | Modification                         |
|------------|--------------------------------------|
| 12.4(11)MD | This command was introduced.         |
| 12.4(15)MD | The <b>packet</b> keyword was added. |

## Usage Guidelines

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

By default, the CSG2 retries a packet forever; it never discards a packet. If you configure the **ip csg quota-server retries packet** command, the CSG2 tries to send a packet to the quota server the specified number of times, then discards the packet. (The first attempt to send a packet to the quota server is not counted as a retry.) For example, if you configure **ip csg quota-server retries packet 4**, the CSG2 tries to send a packet to the quota server five times before discarding it (the initial attempt plus four retries).

## Examples

The following example shows how to allow two quota server retries:

```
ip csg quota-server retries 2
```

The following example shows how to allow the CSG2 to try to send a packet to the quota server four times, in addition to the initial attempt:

```
ip csg quota-server retries packet 4
```

| Related Commands | Command                             | Description  |
|------------------|-------------------------------------|--|
|                  | <a href="#">ip csg bma retries</a>  | Defines the maximum number of Billing Mediation Agent (BMA) retries allowed before the CSG2 determines that the link has failed.         |
|                  | <a href="#">ip csg ipc retries</a>  | Defines the maximum number of Interprocessor Communication (IPC) retries allowed before the CSG2 determines that the link has failed.    |
|                  | <a href="#">ip csg psd retries</a>  | Defines the maximum number of Cisco Persistent Storage Device (PSD) retries allowed before the CSG2 determines that the link has failed. |
|                  | <a href="#">ip csg quota-server</a> | Configures the CSG2 quota servers that return billing quota values for subscribers.  |

# ip csg quota-server window

To define the quota server transmit window size for the CSG2, use the **ip csg quota-server window** command in global configuration mode. To reset the quota server transmit window size to the default value, use the **no** form of this command.

```
ip csg quota-server window {max window-size | min window-size | min auto}
```

```
no ip csg quota-server window {max | min}
```

## Syntax Description

|                               |   |
|-------------------------------|---|
| <b>max</b> <i>window-size</i> | Maximum size, in packets, of the quota server transmit window. The range is 1 to 65535. The default value is 128.   |
| <b>min</b> <i>window-size</i> | Minimum size, in packets, of the quota server transmit window. The range is 1 to 65535.   |
| <b>min auto</b>               | Specifies that the CSG2 is to determine the minimum size of the quota server transmit window automatically. The CSG2 keeps track of the maximum number of ACKs received in one response and sets that number as the minimum window. |

## Defaults

The default maximum window size is 128 packets.  
The default minimum window size is automatically determined by the CSG2.

## Command Modes

Global configuration

## Command History

| Release    | Modification                 |
|------------|------------------------------|
| 12.4(11)MD | This command was introduced. |

## Usage Guidelines

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

## Examples

The following example shows how to set the maximum quota server transmit window to 64 packets:

```
ip csg quota-server window max 64
```

## Related Commands

| Command                           | Description  |
|-----------------------------------|--|
| <a href="#">ip csg bma window</a> | Defines the Billing Mediation Agent (BMA) transmit window size for the CSG2. |

| Command                             | Description  |
|-------------------------------------|--|
| <a href="#">ip csg psd window</a>   | Defines the Cisco Persistent Storage Device (PSD) transmit window size for the CSG2. |
| <a href="#">ip csg quota-server</a> | Configures the CSG2 quota servers that return billing quota values for subscribers.  |

# ip csg radius ack error parse

To enable the CSG2 to generate a RADIUS response to a RADIUS Accounting Start Request or a RADIUS Accounting Interim Request when it encounters a RADIUS parse error condition, use the **ip csg radius ack error parse** command in global configuration mode. To prevent RADIUS responses to errors, use the **no** form of this command.

**ip csg radius ack error parse**

**no ip csg radius ack error parse**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The CSG2 generates a RADIUS response to a RADIUS Accounting Start Request or a RADIUS Accounting Interim Request when it encounters a RADIUS parse error condition.

## Command Modes

Global configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: <ul style="list-style-type: none"> <li>The <b>radius ack error</b> command split into two new commands—<b>ip csg radius ack error parse</b> and <b>ip csg radius ack error user</b>.</li> <li>The configuration mode for this command changed from CSG user group configuration to global configuration.</li> </ul> |

## Usage Guidelines

Use the **no** form of this command, **no ip csg radius ack error parse**, to prevent the CSG2 from acknowledging the following RADIUS parse errors:

- Invalid RADIUS message or attribute length
- RADIUS Authenticator does not match what the CSG2 calculates
- Incorrect RADIUS attribute length
- User profile information such as billing plan or quota server does not match the CSG2 configuration

## Examples

The following example shows how to prevent RADIUS responses when RADIUS parse errors are encountered.

```
no ip csg radius ack error parse
```

| Related Commands | Command  | Description  |
|------------------|--|--|
|                  | <a href="#">ip csg radius ack error user</a>           | Enables the CSG2 to generate a RADIUS response to a RADIUS Accounting Start Request or a RADIUS Accounting Interim Request when it encounters a user resource error condition. |
|                  | <a href="#">ip csg radius endpoint</a>                 | Identifies the CSG2 as an endpoint for RADIUS Accounting messages.   |
|                  | <a href="#">ip csg radius handoff</a>                  | Configures RADIUS handoff support.   |
|                  | <a href="#">ip csg radius proxy</a>                    | Specifies that the CSG2 is to be a proxy for RADIUS messages.  |
|                  | <a href="#">ip csg radius start restart session-id</a> | Deletes an existing CSG2 User Table entry for a specific subscriber, and creates a new entry for that subscriber.  |
|                  | <a href="#">ip csg radius stop purge</a>               | Specifies the attribute that must be included in the RADIUS Accounting Stop request in order for the CSG2 User Table entry to be deleted.                                      |



# ip csg radius ack error user

To enable the CSG2 to generate a RADIUS response to a RADIUS Accounting Start Request or a RADIUS Accounting Interim Request when it encounters a user resource error condition, use the **ip csg radius ack error user** command in global configuration mode. To prevent RADIUS responses to errors, use the **no** form of this command.

**ip csg radius ack error user**

**no ip csg radius ack error user**

**Syntax Description** This command has no arguments or keywords.

**Defaults** The CSG2 generates a RADIUS response to a RADIUS Accounting Start Request or a RADIUS Accounting Interim Request when it encounters a user resource error condition.

**Command Modes** Global configuration

| Command History | Release    | Modification   |
|-----------------|------------|--|
|                 | 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: <ul style="list-style-type: none"> <li>The <b>radius ack error</b> command split into two new commands—<b>ip csg radius ack error parse</b> and <b>ip csg radius ack error user</b>.</li> <li>The configuration mode for this command changed from CSG user group configuration to global configuration.</li> </ul> |

**Usage Guidelines** Use the **no** form of this command, **no ip csg radius ack error user**, to prevent the CSG2 from acknowledging the following user resource errors:

- Maximum number of users reached
- Unable to allocate memory for creating a user entry or for storing RADIUS attribute information (such as report attributes or parsed billing plan information)
- Unable to communicate user information via inter-processor communication
- Load manager prevents allocation of a user

**Examples** The following example shows how to prevent RADIUS responses when user resource errors are encountered.

```
no ip csg radius ack error user
```

| Related Commands | Command  | Description   |
|------------------|--|---|
|                  | <a href="#">ip csg radius ack error parse</a>          | Enables the CSG2 to generate a RADIUS response to a RADIUS Accounting Start Request or a RADIUS Accounting Interim Request when it encounters a RADIUS parse error condition. |
|                  | <a href="#">ip csg radius endpoint</a>                 | Identifies the CSG2 as an endpoint for RADIUS Accounting messages.  |
|                  | <a href="#">ip csg radius handoff</a>                  | Configures RADIUS handoff support.  |
|                  | <a href="#">ip csg radius proxy</a>                    | Specifies that the CSG2 is to be a proxy for RADIUS messages.   |
|                  | <a href="#">ip csg radius start restart session-id</a> | Deletes an existing CSG2 User Table entry for a specific subscriber, and creates a new entry for that subscriber.   |
|                  | <a href="#">ip csg radius stop purge</a>               | Specifies the attribute that must be included in the RADIUS Accounting Stop request in order for the CSG2 User Table entry to be deleted.                                     |

# ip csg radius correlation

To enable RADIUS correlation processing by the CSG2, use the **ip csg radius correlation** command in global configuration mode. To disable RADIUS correlation processing, use the **no** form of this command.

**ip csg radius correlation**

**no ip csg radius correlation**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The CSG2 does not perform RADIUS correlation processing.

## Command Modes

Global configuration

## Command History

| Release    | Modification                 |
|------------|------------------------------|
| 12.4(11)MD | This command was introduced. |

## Usage Guidelines

A retransmitted RADIUS Stop might cause the CSG2 to remove a subscriber entry from the CSG2 User Table when the entry should not be removed.

To avoid this problem, the CSG2 must be able to associate a session correlator from the RADIUS Start message with a subscriber entry in the User Table, and compare that correlator with the correlator in the RADIUS Stop message. If the correlators match, the CSG2 deletes the subscriber entry; otherwise, the CSG2 retains the entry in the User Table.

The CSG2 can use the Acct-Session-Id (attribute 44) as the correlator, or it can use the following vendor-specific attribute (VSA) subattribute (attribute 26, Vendor-Id 9, subattribute 1):

**csg:user\_session\_correlator=<string>**

If both attributes are included in the RADIUS Start or RADIUS Stop message, the CSG2 uses the VSA subattribute.

To enable this capability, enter the **ip csg radius correlation** command.

- If there is no correlator saved in the User Table entry, the CSG2 deletes the entry.
- If there is a correlator saved in the User Table entry, the CSG2 compares it to the correlator in the RADIUS Stop. If the correlators match, the CSG2 deletes the entry; if they do not match, or if there is no correlator in the RADIUS Stop, the CSG2 retains the entry in the User Table.

To disable this capability, enter the **no ip csg radius correlation** command. The CSG2 deletes User Table entries without subscriber session correlation.

## Examples

The following example shows how to enable RADIUS correlation processing by the CSG2.

```
ip csg radius correlation
```

| Related Commands | Command  | Description   |
|------------------|--|---|
|                  | <a href="#">ip csg radius handoff</a>                  | Configures RADIUS handoff support.  |
|                  | <a href="#">ip csg radius start restart session-id</a> | Deletes an existing CSG2 User Table entry for a specific subscriber, and creates a new entry for that subscriber.                         |
|                  | <a href="#">ip csg radius stop purge</a>               | Specifies the attribute that must be included in the RADIUS Accounting Stop request in order for the CSG2 User Table entry to be deleted. |
|                  | <a href="#">replicate</a>                              | Replicates the connection state for all connections to the CSG2 content servers on the standby system.                                    |

## ip csg radius endpoint

To identify the CSG2 as an endpoint for RADIUS Accounting messages, use the **ip csg radius endpoint** command in global configuration mode. To remove the endpoint identification, use the **no** form of this command.

```
ip csg radius endpoint [vrf csg-vrf-name] csg-address key [encrypt] secret-string
[vrf sub-vrf-name]
```

```
no ip csg radius endpoint [vrf csg-vrf-name] csg-address
```

| Syntax Description             |  |
|--------------------------------|--|
| <b>vrf</b> <i>csg-vrf-name</i> | (Optional) Virtual Routing and Forwarding (VRF) table which the CSG2 IP address is to use for RADIUS communication.  |
| <i>csg-address</i>             | <p>Specifies the CSG2 IP address.</p> <p>The CSG2 IP address must be a virtual IP address, and it must be unique (or the IP address-VRF name combination must be unique, if VRF is configured). The CSG2 IP address (or the IP address-VRF name combination) must not be specified in other CSG2 commands, and it must not match any real IP address, virtual IP address, or alias IP address (or IP address-VRF name combination) configured on the CSG2.</p> <p>If you want the CSG2 RADIUS endpoint IP address to be a member of a CSG2 interface subnet, you must configure the CSG2 IP address as follows:</p> <ul style="list-style-type: none"> <li>In non-redundant configurations, you must configure the CSG2 IP address as a secondary IP address configured on the appropriate interface.</li> <li>In redundant configurations, you must configure the CSG2 IP address as a standby secondary IP address on the appropriate interface.</li> </ul> <p><b>Note</b> The CSG2 performs radius endpoint processing only on User Datagram Protocol (UDP) traffic that is destined for the server IP address. The server IP address cannot be used for any other UDP communication with the CSG2.</p> |
| <b>key</b>                     | 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, <b>show run</b>), or how it is written to nonvolatile memory (for example, <b>write memory</b>).</p> <p>The valid values are:</p> <ul style="list-style-type: none"> <li><b>0</b>—The <i>secret-string</i> is stored in plain text. This is the default setting.</li> <li><b>7</b>—The <i>secret-string</i> is encrypted before it is displayed or written to nonvolatile memory.</li> </ul> <p><b>Note</b> 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 <b>service</b> 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 CSG2 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> |
| <b>vrf</b> <i>sub-vrf-name</i> | (Optional) Virtual Routing and Forwarding (VRF) table which the subscriber is to use for RADIUS communication.   |

### Defaults

The *secret-string* is stored in plain text.

If no VRF table is specified for the CSG2, the CSG2 uses the global routing table for RADIUS communication.

If no VRF table is specified for the subscriber, the subscriber uses the global routing table for RADIUS communication.

### Command Modes

Global configuration

### Command History

| Release    | Modification  |
|------------|---|
| 12.4(11)MD | <p>This command was migrated from CSG1.</p> <p>Changes from CSG1:</p> <ul style="list-style-type: none"> <li>The name of this command changed from <b>radius endpoint</b> to <b>ip csg radius endpoint</b>.</li> <li>The configuration mode for this command changed from module CSG configuration to global configuration.</li> <li>The <b>vrf</b> <i>csg-vrf-name</i> and <b>vrf</b> <i>sub-vrf-name</i> keywords and arguments were added.</li> <li>The <b>table</b> <i>table-name</i> keyword and argument were removed.</li> </ul> |

### Usage Guidelines

A RADIUS Accounting message sent to the specified *csg-address* (and any port) is parsed, and is then acknowledged, by the CSG2.

CSG2 User Table entries created as a result of RADIUS messaging through the **ip csg radius endpoint** definition with a VRF configured are indexed by the configured *sub-vrf-name*. This enables the CSG2 to segment the subscriber space and removes ambiguity if multiple subscribers share the same IP address, provided that their entries were instantiated by RADIUS flows to CSG2 radius definitions bound to different VRFs. If the *sub-vrf-name* is not configured, the User Table entries are indexed via the global routing table.

To change the RADIUS endpoint *csg-vrf-name* or *sub-vrf-name* associated with a given *csg-address*, you must first enter the **no** form of the **ip csg radius endpoint** command for that *csg-address*, then enter the command with the new *csg-vrf-name* or *sub-vrf-name*.

You can also configure an optional RADIUS key.

- If you configure a RADIUS key, the CSG2 parses and acts on a message only if the RADIUS Authenticator is correct.
- If you do not configure a RADIUS key, the CSG2 always parses and forwards every message.

---

**Examples**

The following example shows how to identify the CSG2 as a RADIUS endpoint:

```
ip csg radius endpoint vrf RADIUSVRF 1.2.3.4 key secret vrf SUBVRF
```

---

**Related Commands**

| Command                                   | Description  |
|---|--|
| <a href="#">ip csg radius monitor nas</a> | Specifies that the CSG2 is to monitor the RADIUS flows to the specified server.          |
| <a href="#">ip csg radius proxy</a>       | Specifies that the CSG2 is to be a proxy for RADIUS messages.                            |
| <a href="#">ip csg radius userid</a>      | Specifies the RADIUS attribute used to extract the user identifier from a RADIUS record. |

# ip csg radius handoff

To configure the CSG2 RADIUS handoff timer, use the **ip csg radius handoff** command in global configuration mode. To turn off the timer, use the **no** form of this command.

**ip csg radius handoff *duration***

**no ip csg radius handoff**

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <p><i>duration</i> Handoff timer duration, in seconds.</p> <p>The handoff timer is started when a RADIUS Accounting Stop is received. If the handoff timer expires before a RADIUS Accounting Start for a subscriber is seen, the CSG2 assumes that a handoff did not occur and deletes the CSG2 User Table entry for the subscriber.</p> <p>The range is from 1 to 43200.</p> |
|---------------------------|--|

|                 |                             |
|-----------------|-----------------------------|
| <b>Defaults</b> | RADIUS handoff is disabled. |
|-----------------|-----------------------------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | Global configuration |
|----------------------|----------------------|

| <b>Command History</b> | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.4(11)MD</td> <td> <p>This command was migrated from CSG1.</p> <p>Changes from CSG1:</p> <ul style="list-style-type: none"> <li>The name of this command changed from <b>radius handoff</b> to <b>ip csg radius handoff</b>.</li> <li>The configuration mode for this command changed from CSG user group configuration to global configuration.</li> </ul> </td> </tr> </tbody> </table> | Release | Modification | 12.4(11)MD | <p>This command was migrated from CSG1.</p> <p>Changes from CSG1:</p> <ul style="list-style-type: none"> <li>The name of this command changed from <b>radius handoff</b> to <b>ip csg radius handoff</b>.</li> <li>The configuration mode for this command changed from CSG user group configuration to global configuration.</li> </ul> |
|------------------------|--|---------|--------------|------------|--|
| Release                | Modification   |         |              |            |  |
| 12.4(11)MD             | <p>This command was migrated from CSG1.</p> <p>Changes from CSG1:</p> <ul style="list-style-type: none"> <li>The name of this command changed from <b>radius handoff</b> to <b>ip csg radius handoff</b>.</li> <li>The configuration mode for this command changed from CSG user group configuration to global configuration.</li> </ul>   |         |              |            |  |

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | The handoff timer is started when a RADIUS Accounting Stop is received. If the handoff timer expires before a RADIUS Accounting Start is received for a subscriber, the CSG2 assumes a handoff did not occur and deletes the CSG2 User Table entry for the subscriber. |
|-------------------------|--|

|                 |  |
|-----------------|--|
| <b>Examples</b> | <p>The following example shows how to specify a RADIUS handoff timer duration of 1000 seconds:</p> <pre>ip csg radius handoff 1000</pre> |
|-----------------|--|



| Related Commands | Command  | Description  |
|------------------|--|--|
|                  | <a href="#">ip csg radius ack error parse</a>          | Enables the CSG2 to generate a RADIUS response to a RADIUS Accounting Start Request or a RADIUS Accounting Interim Request when it encounters a RADIUS parse error condition.  |
|                  | <a href="#">ip csg radius ack error user</a>           | Enables the CSG2 to generate a RADIUS response to a RADIUS Accounting Start Request or a RADIUS Accounting Interim Request when it encounters a user resource error condition. |
|                  | <a href="#">ip csg radius proxy</a>                    | Specifies that the CSG2 is to be a proxy for RADIUS messages.  |
|                  | <a href="#">ip csg radius start restart session-id</a> | Deletes an existing CSG2 User Table entry for a specific subscriber, and creates a new entry for that subscriber.  |
|                  | <a href="#">ip csg radius stop purge</a>               | Specifies the attribute that must be included in the RADIUS Accounting Stop request in order for the CSG2 User Table entry to be deleted.                                      |

## ip csg radius monitor

To specify that the CSG2 is to monitor the RADIUS flows to the specified server, use the **ip csg radius monitor** command in global configuration mode. To stop monitoring the RADIUS flows, use the **no** form of this command.

```
ip csg radius monitor [vrf vrf-name] server-address server-port [key [encrypt] secret-string]
[vrf sub-vrf-name]
```

```
no ip csg radius monitor [vrf vrf-name] server-address server-port
```

### Syntax Description

|                                |  |
|--------------------------------|--|
| <b>vrf</b> <i>csg-vrf-name</i> | (Optional) Virtual Routing and Forwarding (VRF) table which the CSG2 IP address is to use for RADIUS communication.  |
| <i>server-address</i>          | Specifies the server address to monitor.   |
| <i>server-port</i>             | Specifies the server port to monitor.  |
| <b>key</b>                     | (Optional) Specifies a RADIUS key.   |
| <i>encrypt</i>                 | (Optional) Indicates how the <i>secret-string</i> is represented when the configuration is displayed (for example, <b>show run</b> ), or how it is written to nonvolatile memory (for example, <b>write memory</b> ).<br><br>The valid values are: <ul style="list-style-type: none"> <li><b>0</b>—The <i>secret-string</i> is stored in plain text. This is the default setting.</li> <li><b>7</b>—The <i>secret-string</i> is encrypted before it is displayed or written to nonvolatile memory.</li> </ul> <p><b>Note</b> 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 <b>service</b> command for more details.</p> |
| <i>secret-string</i>           | (Optional) 1- to 64-character clear password value for MD5 authentication. All characters are valid; case is significant.<br><br>The <i>secret-string</i> is always sent in plain text to the CSG2 module when the configuration is downloaded.<br><br>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]).   |
| <b>vrf</b> <i>sub-vrf-name</i> | (Optional) Virtual Routing and Forwarding (VRF) table which the subscriber is to use for RADIUS communication.   |

### Defaults

The *secret-string* is stored in plain text.

If no VRF table is specified for the CSG2, the CSG2 uses the global routing table for RADIUS communication.

If no VRF table is specified for the subscriber, the subscriber uses the global routing table for RADIUS communication.

### Command Modes

Global configuration

| Command History | Release    | Modification                 |
|-----------------|------------|------------------------------|
|                 | 12.4(15)MD | This command was introduced. |

**Usage Guidelines**

You can configure an optional RADIUS key.

- If you configure a RADIUS key, the CSG2 parses and acts on a message only if the RADIUS Authenticator is correct.
- If you do not configure a RADIUS key, the CSG2 always parses and forwards every message.
- Even if you configure a key, the CSG2 forwards all RADIUS messages (including Access messages), regardless of the configuration or accuracy of the key, unless the IP or UDP headers specify a length larger than the physical packet size.

**Examples**

The following example shows how to use the **ip csg radius monitor** command to enable the CSG2 to monitor the RADIUS flows:

```
ip csg radius monitor 1.2.3.4 1813 key KEY_TABLE
```

**Related Commands**

| Command                                   | Description  |
|---|--|
| <a href="#">ip csg radius endpoint</a>    | Identifies the CSG2 as an endpoint for RADIUS Accounting messages.                                   |
| <a href="#">ip csg radius monitor nas</a> | Specifies that the CSG2 is to monitor the RADIUS flows to the specified Network Access Server (NAS). |
| <a href="#">ip csg radius proxy</a>       | Specifies that the CSG2 is to be a proxy for RADIUS messages.  |

# ip csg radius monitor nas

To specify that the CSG2 is to monitor the RADIUS flows to the specified Network Access Server (NAS), use the **ip csg radius monitor nas** command in global configuration mode. To stop monitoring the RADIUS flows, use the **no** form of this command.

```
ip csg radius monitor nas nas-ip-address [vrf nas-vrf-name]
```

```
no ip csg radius monitor nas nas-ip-address [vrf nas-vrf-name]
```

## Syntax Description

|                                |  |
|--------------------------------|--|
| <i>nas-ip-address</i>          | Specifies the NAS IP address to monitor.<br><br><b>Note</b> The CSG2 performs radius monitor processing only on User Datagram Protocol (UDP) traffic that is destined for the NAS IP address. The NAS IP address cannot be used for any other UDP communication with the CSG2. |
| <b>vrf</b> <i>nas-vrf-name</i> | (Optional) Virtual Routing and Forwarding (VRF) table which the NAS IP address is to use for RADIUS communication.   |

## Defaults

If no VRF table is specified for the NAS, the CSG2 uses the global routing table for RADIUS communication.

## Command Modes

Global configuration

## Command History

| Release    | Modification                 |
|------------|------------------------------|
| 12.4(15)MD | This command was introduced. |

## Usage Guidelines

This command is required whenever a RADIUS monitor is configured. Use this command to identify each NAS that is to communicate with the RADIUS monitor server. Each interface on which a NAS server resides must be marked as a subscriber interface.

## Examples

The following example shows how to use the **ip csg radius monitor nas** command to enable the CSG2 to monitor the RADIUS flows:

```
ip csg radius monitor nas 1.2.3.4 vrf NAS_TABLE
```

## Related Commands

| Command                                | Description  |
|--|--|
| <a href="#">ip csg radius endpoint</a> | Identifies the CSG2 as an endpoint for RADIUS Accounting messages. |
| <a href="#">ip csg radius proxy</a>    | Specifies that the CSG2 is to be a proxy for RADIUS messages.      |

## ip csg radius on-off purge

To specify the rate at which the CSG2 is to delete CSG2 User Table entries in response to a RADIUS Accounting On or RADIUS Accounting Off message, or in response to the **clear ip csg user all** command, use the **ip csg radius on-off purge** command in global configuration mode. To restore the default setting, use the **no** form of this command.

```
ip csg radius on-off purge deletions-per-second
```

```
no ip csg radius on-off purge
```

|                           |                             |   |
|---------------------------|-----------------------------|---|
| <b>Syntax Description</b> | <i>deletions-per-second</i> | Number of User Table entry deletions per second. The range is from 50 to 65535. The default rate is 1000. |
|---------------------------|-----------------------------|---|

**Defaults** The default rate is 1000 User Table entry deletions per second.

**Command Modes** Global configuration

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|------------------------|----------------|------------------------------|
|                        | 12.4(15)MD     | This command was introduced. |

**Usage Guidelines** The actual rate at which the CSG2 deletes User Table entries might be slightly higher or lower than the specified rate.

**Examples** The following example shows how to specify a User Table deletion rate of 875 entries per second:

```
ip csg radius on-off purge 875
```

## ip csg radius pod attribute

To specify the RADIUS attributes and vendor-specific attribute (VSA) subattributes to be copied from the RADIUS Start message and sent to the Network Access Server (NAS) in the Packet of Disconnect (PoD) message, use the **ip csg radius pod attribute** command in global configuration mode. To disable this feature, use the **no** form of this command.

```
ip csg radius pod attribute {radius-attribute-number | vsa {vendor-id | 3gpp}  
radius-subattribute-number}
```

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

### Syntax Description

|                                   |   |
|-----------------------------------|---|
| <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. The range is from 1 to 255. |
| <b>vsa</b>                        | Specifies the VSA.  |
| <i>vendor-id</i>                  | Specifies the vendor ID number. The range is from 1 to 16777215.  |
| <b>3gpp</b>                       | 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

RADIUS attributes sufficient to identify the NAS and subscriber (RFC3576) are sent in the PoD message.

### Command Modes

Global configuration

### Command History

| Release    | Modification  |
|------------|---|
| 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: <ul style="list-style-type: none"> <li>The name of this command changed from <b>radius pod attribute</b> to <b>ip csg radius pod attribute</b>.</li> <li>The configuration mode for this command changed from CSG user group configuration to global configuration.</li> <li>The <b>26</b> keyword was removed.</li> </ul> |

### Usage Guidelines

You can specify up to 256 RADIUS attributes.

If the RADIUS message does not contain an attribute, the PoD message attribute does not contain the attribute, either.

The CSG2 saves and reports attribute and subattribute information for each subscriber.

When the CSG2 receives a new RADIUS Accounting Start or RADIUS Interim Accounting Request, it saves the attribute and subattribute information parsed from the new request.

The CSG2 saves only those attributes or subattributes which meet both of the following criteria:

- They are present in the new RADIUS Accounting Start or RADIUS Interim Accounting Request.
- They are configured for reporting at the time the new request arrives at the CSG2.

All previously stored attribute and subattribute information from previous requests is destroyed, even if the new RADIUS Accounting Start or RADIUS Interim Accounting Request does not contain all of the attributes and subattributes that were present in the previous request. Only the currently stored attributes are reported in CDRs.

If there are multiple instances of an attribute, all instances are included. Attributes are included in the PoD message in random order.

### Examples

The following example shows how to specify RADIUS attributes 44 and 26:

```
ip csg radius pod attribute 44
ip csg radius pod attribute 26
```

### Related Commands

| Command                                   | Description   |
|---|---|
| <a href="#">ip csg radius pod nas</a>     | Specifies the NAS port to which the CSG2 is to send the PoD message, and the key to use in calculating the Authenticator.                                     |
| <a href="#">ip csg radius pod timeout</a> | Specifies the number of times to retry the RADIUS PoD message if it is not acknowledged by means of an ACK message, and the interval between retransmissions. |

## ip csg radius pod nas

To specify the Network Access Server (NAS) port to which the CSG2 is to send the Packet of Disconnect (PoD) message, and to specify the key to use in calculating the Authenticator, use the **ip csg radius pod nas** command in global configuration mode. To restore the default settings, use the **no** form of this command.

```
ip csg radius pod nas [vrf vrf-name] [start-ip end-ip] port key [encrypt] secret-string
```

```
no ip csg radius pod nas [vrf vrf-name] [start-ip end-ip] port key [encrypt] secret-string
```

### Syntax Description

|                            |  |
|----------------------------|--|
| <b>vrf</b> <i>vrf-name</i> | (Optional) Virtual Routing and Forwarding (VRF) table which the CSG2 is to use for RADIUS communication.   |
| <i>start-ip</i>            | (Optional) Specifies the first NAS IP address in a range of addresses.   |
| <i>end-ip</i>              | (Optional) 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.  |
| <b>key</b>                 | 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, <b>show run</b>), or how it is written to nonvolatile memory (for example, <b>write memory</b>).</p> <p>The possible values are <b>0</b> and <b>7</b>:</p> <ul style="list-style-type: none"> <li><b>0</b>—The <i>secret-string</i> is stored in plain text. This is the default setting.</li> <li><b>7</b>—The <i>secret-string</i> is encrypted before it is displayed or written to nonvolatile memory.</li> </ul> <p><b>Note</b> 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 <b>service</b> 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 CSG2 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.  
If no VRF table is specified, the CSG2 uses the global routing table for RADIUS communication.

### Command Modes

Global configuration



| Command History | Release    | Modification   |
|-----------------|------------|--|
|                 | 12.4(11)MD | <p>This command was migrated from CSG1.</p> <p>Changes from CSG1:</p> <ul style="list-style-type: none"> <li>The name of this command changed from <b>radius pod nas</b> to <b>ip csg radius pod nas</b>.</li> <li>The configuration mode for this command changed from CSG user group configuration to global configuration.</li> <li>The <b>vrf vrf-name</b> keyword and argument were added.</li> </ul> |

### Usage Guidelines

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

The RADIUS Accounting Start message which specifies the NAS IP address to which to send the PoD message must be received on an IP address specified by the **ip csg radius proxy** or **ip csg radius endpoint** command configured in global configuration mode.

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

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

### Examples

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

```
ip csg radius pod nas 1.1.1.0 1.1.1.255 1700 key secret
ip csg radius pod nas 1701 key password
```

### Related Commands

| Command                                     | Description   |
|---|---|
| <a href="#">ip csg radius pod attribute</a> | Specifies the RADIUS attributes to be copied from the RADIUS Start message and sent to the NAS in the PoD.  |
| <a href="#">ip csg radius pod timeout</a>   | Specifies the number of times to retry the RADIUS PoD message if it is not acknowledged by means of an ACK message, and the interval between retransmissions. |

# ip csg radius pod timeout

To specify the number of times to retry the RADIUS Packet of Disconnect (PoD) message if it is not acknowledged by means of an ACK message, and the interval between retransmissions, use the **ip csg radius pod timeout** command in global configuration mode. To restore the default timeout, use the **no** form of this command.

**ip csg radius pod timeout** *timeout* **retransmit** *retransmit*

**no ip csg radius pod timeout** *timeout* **retransmit** *retransmit*

| Syntax Description | Parameter                           | Description  |
|--------------------|-------------------------------------|--|
|                    | <i>timeout</i>                      | Number of seconds to wait for an ACK or NAK before sending another PoD message. The range is from 1 to 1000. The default timeout is 5 seconds. |
|                    | <b>retransmit</b> <i>retransmit</i> | Number of times to retransmit the message. The range is from 1 to 100. The default setting is 3 retransmits.                                   |

**Defaults**

The default timeout is 5 seconds.  
The default number of retransmits is 3 retransmits.

**Command Modes**

Global configuration

| Command History | Release    | Modification  |
|-----------------|------------|---|
|                 | 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: <ul style="list-style-type: none"> <li>The name of this command changed from <b>radius pod timeout</b> to <b>ip csg radius pod timeout</b>.</li> <li>The configuration mode for this command changed from CSG user group configuration to global configuration.</li> </ul> |

**Examples**

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

```
ip csg radius pod timeout 30 retransmit 5
```

| Related Commands | Command                                     | Description   |
|------------------|---|---|
|                  | <a href="#">ip csg radius pod attribute</a> | Specifies the RADIUS attributes to be copied from the RADIUS Start message and sent to the NAS in the PoD.                          |
|                  | <a href="#">ip csg radius pod nas</a>       | Specifies the NAS port to which the CSG2 is to send the PoD message, and specifies the key to use in calculating the Authenticator. |

## ip csg radius proxy

To specify that the CSG2 is to be a proxy for RADIUS messages, use the **ip csg radius proxy** command in global configuration mode. To stop the CSG2 from proxying for RADIUS messages, use the **no** form of this command.

```
ip csg radius proxy [vrf csg-vrf-name] csg-address [vrf server-vrf-name] server-address
csg-source-address [key [encrypt] secret-string] [vrf sub-vrf-name]
```

```
no ip csg radius proxy [vrf csg-vrf-name] csg-address server-address
```

### Syntax Description

|                                   |   |
|-----------------------------------|---|
| <b>vrf</b> <i>csg-vrf-name</i>    | (Optional) Virtual Routing and Forwarding (VRF) table which the CSG2 IP address is to use for RADIUS communication.   |
| <i>csg-address</i>                | Specifies the CSG2 IP address.<br><br>The CSG2 IP address must be a virtual IP address, and it must be unique (or the IP address-VRF name combination must be unique, if VRF is configured). The CSG2 IP address (or the IP address-VRF name combination) must not be specified in other CSG2 commands, and it must not match any real IP address, virtual IP address, or alias IP address (or IP address-VRF name combination) configured on the CSG2.<br><br>If you want the CSG2 RADIUS proxy IP address to be a member of a CSG2 interface subnet, you must configure the CSG2 IP address as follows: <ul style="list-style-type: none"> <li>• In non-redundant configurations, you must configure the CSG2 IP address as a secondary IP address configured on the appropriate interface.</li> <li>• In redundant configurations, you must configure the CSG2 IP address as a standby secondary IP address on the appropriate interface.</li> </ul> <p><b>Note</b> The CSG2 performs radius proxy processing only on User Datagram Protocol (UDP) traffic that is destined for the server IP address. The server IP address cannot be used for any other UDP communication with the CSG2.</p> |
| <b>vrf</b> <i>server-vrf-name</i> | (Optional) Virtual Routing and Forwarding (VRF) table which the server IP address is to use for RADIUS communication.   |
| <i>server-address</i>             | Specifies the server IP address.  |

|                                |  |
|--------------------------------|--|
| <i>csg-source-address</i>      | <p>Specifies the source IP address that the CSG2 is to use when sending packets to the RADIUS server.</p> <p>The CSG2 source IP address must be unique (or the IP address-VRF name combination must be unique, if VRF is configured).</p> <p>If you want the CSG2 RADIUS proxy IP address to be a member of a CSG2 interface subnet, you must configure the CSG2 source IP address as follows:</p> <ul style="list-style-type: none"> <li>• In non-redundant configurations, you must configure the CSG2 source IP address as a secondary IP address configured on the appropriate interface.</li> <li>• In redundant configurations, you must configure the CSG2 source IP address as a standby secondary IP address on the appropriate interface.</li> </ul> <p><b>Note</b> The CSG2 performs radius proxy processing only on User Datagram Protocol (UDP) traffic that is destined for the <i>csg-source-address</i>. The <i>csg-source-address</i> cannot be used for any other UDP communication with the CSG2.</p> |
| <b>key</b>                     | <p>(Optional) Specifies a RADIUS key.</p> <p><b>Note</b> Specify no more than one <b>key</b> for each CSG2 IP address.</p>   |
| <i>encrypt</i>                 | <p>(Optional) Indicates how the <i>secret-string</i> is represented when the configuration is displayed (for example, <b>show run</b>), or how it is written to nonvolatile memory (for example, <b>write memory</b>).</p> <p>The possible values are <b>0</b> and <b>7</b>:</p> <ul style="list-style-type: none"> <li>• <b>0</b>—The <i>secret-string</i> is stored in plain text. This is the default setting.</li> <li>• <b>7</b>—The <i>secret-string</i> is encrypted before it is displayed or written to nonvolatile memory.</li> </ul> <p><b>Note</b> 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 <b>service</b> 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 CSG2 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>  |
| <b>vrf</b> <i>sub-vrf-name</i> | <p>(Optional) Virtual Routing and Forwarding (VRF) table which the subscriber is to use for RADIUS communication.</p>  |

## Defaults

The *secret-string* is stored in plain text.

The *csg-source-address* is set to *csg-address*.

If no VRF table is specified for the CSG2, the CSG2 uses the global routing table for RADIUS communication.

If no VRF table is specified for the RADIUS server, the RADIUS server uses the global routing table for RADIUS communication.

If no VRF table is specified for the subscriber, the subscriber uses the global routing table for RADIUS communication.

**Command Modes** Global configuration

| Command History | Release    | Modification  |
|-----------------|------------|---|
|                 | 12.4(11)MD | <p>This command was migrated from CSG1.</p> <p>Changes from CSG1:</p> <ul style="list-style-type: none"> <li>• The name of this command changed from <b>radius proxy</b> to <b>ip csg radius proxy</b>.</li> <li>• The configuration mode for this command changed from module CSG configuration to global configuration.</li> <li>• The <b>vrf csg-vrf-name</b>, <b>vrf server-vrf-name</b>, and <b>vrf sub-vrf-name</b> keywords and arguments were added.</li> <li>• The <b>table table-name</b> keyword and argument were removed.</li> </ul> |

**Usage Guidelines** A message sent to the specified *csg-address* (and any port) is parsed and then forwarded to the specified RADIUS server. When forwarded to the RADIUS server, the source IP address is the *csg-source-address*.

The source port is arbitrarily chosen by the CSG2, and the destination port remains unchanged. When a message is received from the network and forwarded to the subscriber, the source IP address is the *csg-address*, and the source port remains unchanged. The source IP address and port are taken from the destination IP address and port in the original message from the subscriber.

You can configure an optional RADIUS key. If you configure a key, the CSG2 parses and acts on the message only if the RADIUS authenticator is correct. If the key is not configured, the CSG2 always parses the message. Whether you configure a key or not, and whether it is correct or not, the CSG2 always forwards the message.

You can specify up to 64 **ip csg radius proxy** commands.

You can also configure an optional RADIUS key.

- If you configure a RADIUS key, the CSG2 parses and acts on a message only if the RADIUS Authenticator is correct.
- If you do not configure a RADIUS key, the CSG2 always parses and forwards every message.

You can specify more than one RADIUS **key** by specifying more than one **ip csg radius proxy** command, but each command must specify a unique CSG2 IP address (or IP address-VRF name combination, if VRF is configured).

All RADIUS messages are forwarded, unless the IP or User Datagram Protocol (UDP) headers specify a length larger than the physical packet size.

CSG2 User Table entries created as a result of RADIUS messaging through the **ip csg radius endpoint** definition with a VRF configured are indexed by the configured *sub-vrf-name*. This enables the CSG2 to segment the subscriber space and removes ambiguity if multiple subscribers share the same IP address, provided that their entries were instantiated by RADIUS flows to CSG2 radius definitions bound to different VRFs. If the *sub-vrf-name* is not configured, the User Table entries are indexed via the global routing table.

**Note**

If your network is designed to check the authorization string in RADIUS messages, we recommend that you enter a *secret-string*. Additionally, if you configure the **ip csg entries user profile radius remove** command, you might need to configure a *secret-string*.

To change the RADIUS proxy *csg-vrf-name*, *server-vrf-name*, or *sub-vrf-name* associated with a given *csg-address*, you must first enter the **no** form of the **ip csg radius endpoint** command for that *csg-address*, then enter the command with the new *csg-vrf-name*, *server-vrf-name*, or *sub-vrf-name*.

**Examples**

The following example illustrates how to create a RADIUS proxy point:

```
ip csg radius proxy vrf RADIUSVRF 1.2.3.4 vrf SERVERVRF 5.6.7.8 1.2.3.4 key secret vrf
SUBVRF
```

**Related Commands**

| Command                                   | Description  |
|---|--|
| <a href="#">ip csg radius endpoint</a>    | Identifies the CSG2 as an endpoint for RADIUS Accounting messages.                       |
| <a href="#">ip csg radius monitor nas</a> | Specifies that the CSG2 is to monitor the RADIUS flows to the specified server.          |
| <a href="#">ip csg radius userid</a>      | Specifies the RADIUS attribute used to extract the user identifier from a RADIUS record. |

# ip csg radius reauthorization attribute

To define the RADIUS attributes and VSA subattributes to be monitored by the CSG2, and to enable Roaming Service Control, use the **ip csg radius reauthorization attribute** command in global configuration mode. To delete a RADIUS attribute, use the **no** form of this command.

```
ip csg radius reauthorization attribute {radius-attribute-number | vsa {vendor-id | 3gpp}  
radius-subattribute-number}
```

```
no ip csg radius reauthorization attribute {radius-attribute-number | vsa {vendor-id | 3gpp}  
radius-subattribute-number}
```

| Syntax Description                |  |  |
|-----------------------------------|--|--|
| <i>radius-attribute-number</i>    |  | Specifies the RADIUS attribute number. The range is from 1 to 255.   |
| <b>vsa</b>                        |  | Specifies the vendor-specific attribute (VSA).                       |
| <i>vendor-id</i>                  |  | Specifies the vendor ID number. The range is from 1 to 16777215.     |
| <b>3gpp</b>                       |  | 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 no RADIUS attribute is defined.

**Command Modes** Global configuration

| Command History | Release    | Modification                 |
|-----------------|------------|------------------------------|
|                 | 12.4(15)MD | This command was introduced. |

**Usage Guidelines** Roaming Service Control, also known as seamless roaming or RADIUS reauthorization, enables the CSG2 to reauthorize prepaid users when specified RADIUS attributes change, rather than ending the users' sessions.

When a RADIUS Start request is received, the specified attributes are saved. When a subsequent Start or Intermediate Accounting message is received, the specified attributes in the new message are compared with the saved attributes. If any attribute is different, each service is reauthorized, as new traffic for the service arrives.

If both Roaming Service Control and the reporting of RADIUS attributes are enabled, the CSG2 monitors both sets of attributes, but only changes in the Roaming Service Control attributes trigger reauthorization. For more information about the reporting of RADIUS attributes, see the [“Reporting RADIUS Attributes and VSA Subattributes”](#) section on page 9-7.

---

**Examples**

The following example illustrates how to create a RADIUS proxy point:

```
ip csg radius reauthorization attribute 14
ip csg radius reauthorization attribute vsa 7777 44
ip csg radius reauthorization attribute 26 7778 4
```

---

**Related Commands**

| Command                             | Description   |
|-------------------------------------|---|
| <a href="#">ip csg radius proxy</a> | Specifies that the CSG2 is to be a proxy for RADIUS messages. |

---



# ip csg radius start restart session-id

To delete an existing CSG2 User Table entry for a specific subscriber, and to create a new entry for that subscriber, use the **ip csg radius start restart session-id** command in global configuration mode.

```
ip csg radius start restart session-id {radius-attribute-number | vsa {vendor-id | 3gpp}
radius-subattribute-number}
```

| Syntax Description                |  |  |
|-----------------------------------|--|--|
| <i>radius-attribute-number</i>    |  | Specifies the RADIUS attribute number. The range is from 1 to 255.   |
| <b>vsa</b>                        |  | Specifies the vendor-specific attribute (VSA).                       |
| <i>vendor-id</i>                  |  | Specifies the vendor ID number. The range is from 1 to 16777215.     |
| <b>3gpp</b>                       |  | 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 CSG2 User Table entries are not deleted.

## Command Modes

Global configuration

## Command History

| Release    | Modification  |
|------------|---|
| 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: <ul style="list-style-type: none"> <li>The name of this command changed from <b>radius start restart session-id</b> to <b>ip csg radius start restart session-id</b>.</li> <li>The configuration mode for this command changed from module CSG configuration to global configuration.</li> <li>The <b>26</b> keyword was removed.</li> </ul> |

## Usage Guidelines

This command:

- Deletes an existing CSG2 User Table entry for a specific subscriber (when a RADIUS Accounting Start or RADIUS Intermediate Accounting is received).
- Creates a new entry for that subscriber (similar to when a RADIUS Accounting Stop has been received).
- Terminates all sessions for that subscriber.

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

**ip csg radius start restart session-id****Examples**

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

```
ip csg radius start restart session-id 44
```

**Related Commands**

| Command                                  | Description   |
|--|---|
| <a href="#">ip csg radius stop purge</a> | Specifies the attribute that must be included in the RADIUS Accounting Stop request in order for the CSG2 User Table entry to be deleted. |

## ip csg radius stop purge

To specify the attribute that must be included in the RADIUS Accounting Stop request in order for the CSG2 User Table entry to be deleted, use the **ip csg radius stop purge** command in global configuration mode.

```
ip csg radius stop purge {radius-attribute-number | vsa {vendor-id | 3gpp}
radius-subattribute-number}
```

| Syntax Description                |  |  |
|-----------------------------------|--|--|
| <i>radius-attribute-number</i>    |  | Specifies the RADIUS attribute number. The range is from 1 to 255.   |
| <b>vsa</b>                        |  | Specifies the vendor-specific attribute (VSA).                       |
| <i>vendor-id</i>                  |  | Specifies the vendor ID number. The range is from 1 to 16777215.     |
| <b>3gpp</b>                       |  | 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 subscriber entry is deleted when a RADIUS Accounting Stop is received.

### Command Modes

Global configuration

### Command History

| Release    | Modification  |
|------------|---|
| 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: <ul style="list-style-type: none"> <li>The name of this command changed from <b>radius stop purge</b> to <b>ip csg radius stop purge</b>.</li> <li>The configuration mode for this command changed from module CSG configuration to global configuration.</li> <li>The <b>26</b> keyword was removed.</li> </ul> |

### Usage Guidelines

The **ip csg 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 CSG2 User Table entry to be deleted. The contents of the specified attribute are not examined.

### Examples

The following example shows how to enable the **ip csg radius stop purge** command:

```
ip csg radius stop purge 44
```

## ■ ip csg radius stop purge

| Related Commands | Command  | Description   |
|------------------|--|---|
|                  | <a href="#">ip csg radius start restart session-id</a> | Deletes an existing CSG2 User Table entry for a specific subscriber, and creates a new entry for that subscriber. |

# ip csg radius userid

To specify the RADIUS attribute used to extract the user identifier from a RADIUS record, use the **ip csg radius userid** command in global configuration mode. To specify that no RADIUS attributes are to be used, use the **no** form of this command.

```
ip csg radius userid {1 | 31 | User-Name | Calling-Station-Id}
```

```
no ip csg radius userid
```

## Syntax Description

|                           |   |
|---------------------------|---|
| <b>1</b>                  | RADIUS attribute number 1.                |
| <b>31</b>                 | RADIUS attribute number 31.               |
| <b>User-Name</b>          | Equivalent to RADIUS attribute number 1.  |
| <b>Calling-Station-Id</b> | Equivalent to RADIUS attribute number 31. |

## Defaults

None

## Command Modes

Global configuration

## Command History

| Release    | Modification  |
|------------|---|
| 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: <ul style="list-style-type: none"> <li>The name of this command changed from <b>radius userid</b> to <b>ip csg radius userid</b>.</li> <li>The configuration mode for this command changed from module CSG configuration to global configuration.</li> </ul> |

## Usage Guidelines

The **ip csg radius userid** command specifies that the CSG2 obtains the user ID from either attribute 1 or 31. If the **no** form of this command, **no ip csg radius userid**, is used, user IDs are not obtained from RADIUS messages.

## Examples

The following example shows how to specify RADIUS attribute User-Name:

```
ip csg radius userid User-Name
```

| Related Commands | Command  | Description  |
|------------------|--|--|
|                  | <a href="#">ip csg radius ack error parse</a>          | Enables the CSG2 to generate a RADIUS response to a RADIUS Accounting Start Request or a RADIUS Accounting Interim Request when it encounters a RADIUS parse error condition.  |
|                  | <a href="#">ip csg radius ack error user</a>           | Enables the CSG2 to generate a RADIUS response to a RADIUS Accounting Start Request or a RADIUS Accounting Interim Request when it encounters a user resource error condition. |
|                  | <a href="#">ip csg radius handoff</a>                  | Configures RADIUS handoff support.   |
|                  | <a href="#">ip csg radius start restart session-id</a> | Deletes an existing CSG2 User Table entry for a specific subscriber, and creates a new entry for that subscriber.  |
|                  | <a href="#">ip csg radius stop purge</a>               | Specifies the attribute that must be included in the RADIUS Accounting Stop request in order for the CSG2 User Table entry to be deleted.                                      |

# ip csg records format

To specify variable, fixed, or combined (variable-single) call detail record (CDR) format, use the **ip csg records format** command in global configuration mode. To use the default setting, use the **no** form of this command.

```
ip csg records format [fixed | variable [combined {http | wap}]]
```

```
no ip csg records format [fixed | variable [combined {http | wap}]]
```

## Syntax Description

|                      |   |
|----------------------|---|
| <b>fixed</b>         | (Optional) Specifies fixed CDR format.  |
| <b>variable</b>      | (Optional) Specifies variable CDR format.   |
| <b>combined http</b> | (Optional) Specifies combined (variable-single) CDR format for HTTP traffic.                                |
| <b>combined wap</b>  | (Optional) Specifies combined (variable-single) CDR format for wireless application protocol (WAP) traffic. |

## Defaults

The default setting is **variable**.

## Command Modes

Global configuration

## Command History

| Release    | Modification  |
|------------|---|
| 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: <ul style="list-style-type: none"> <li>The name of this command changed from <b>records format</b> to <b>ip csg records format</b>.</li> <li>The configuration mode for this command changed from CSG accounting configuration to global configuration.</li> <li>The <b>variable-single-cdr</b> keyword was replaced with the <b>combined</b> keyword.</li> <li>The <b>http</b> and <b>wap</b> keywords were added.</li> </ul> |

## Usage Guidelines

This command is valid only for transaction-based CDRs. It is not valid for service-level CDRs.

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

## Examples

The following example shows how to specify combined CDR record format for HTTP traffic:

```
ip csg records format variable combined http
```

# ip csg redirect

To redirect subscriber flows to an alternate IP address when the subscriber's quota is exhausted, use the **ip csg redirect** command in global configuration mode. To remove the redirect, use the **no** form of this command.

```
ip csg redirect {http url | interval seconds | maximum number | sip url | wap url}
```

```
no ip csg redirect [http | sip | wap]
```

## Syntax Description

|                         |  |
|-------------------------|--|
| <b>http url</b>         | (Optional) Redirects HTTP subscriber flows to the specified redirect URL when quota is depleted, and configures the default URL for use in HTTP redirection.   |
| <b>interval seconds</b> | (Optional) Length of time, in seconds, during which the CSG2 redirects an out-of-quota subscriber. After this interval, the CSG2 drops the requests until quota can be requested again.<br><br>The start of the interval is the time of the first redirect after a quota grant of zero. The range is from 0 to 3600. The default is 8. |
| <b>maximum number</b>   | (Optional) Maximum number of times a redirect is to be performed for an out-of-quota subscriber during a redirect interval. The range is from 0 to 255. The default is 15.   |
| <b>sip url</b>          | (Optional) Redirects Session Initiation Protocol (SIP) call requests (INVITE methods) to the specified redirect URL when quota is depleted.  |
| <b>wap url</b>          | (Optional) Redirects wireless application protocol (WAP) subscriber flows to the specified redirect URL when quota is depleted.  |

## Defaults

If you do not specify an interval, the CSG2 redirects subscriber flows after 8 seconds.  
If you do not specify a maximum, the CSG2 allows up to 15 redirects during the interval.

## Command Modes

Global configuration

## Command History

| Release    | Modification  |
|------------|---|
| 12.4(11)MD | This command was migrated from CSG1.<br><br>Changes from CSG1: <ul style="list-style-type: none"> <li>The name of this command changed from <b>redirect</b> to <b>ip csg redirect</b>.</li> <li>The configuration mode for this command changed from CSG user group configuration to CSG2 service configuration.</li> <li>The <b>interval seconds</b> and <b>maximum number</b> keywords and arguments were added.</li> <li>The <b>nat ip-address</b> and <b>port-number</b> keyword and arguments were removed.</li> </ul> |
| 12.4(15)MD | The <b>sip</b> keyword and <b>url</b> argument were added.  |



---

**Examples**

The following example shows how to configure CSG2 redirects:

```
ip csg redirect http http://server/topoff.html
ip csg redirect sip sip: 1.2.3.4
ip csg redirect wap http://server/topoff.wml
ip csg redirect interval 30
ip csg redirect maximum 10
```

# ip csg refund

To specify the CSG2 refund policy to apply to the various services, and to enter CSG2 refund configuration mode, use the **ip csg refund** command in global configuration mode. To disable this feature, use the **no** form of the command.

**ip csg refund** *refund-policy-name*

**no ip csg refund** *refund-policy-name*

## Syntax Description

|                           |  |
|---------------------------|--|
| <i>refund-policy-name</i> | Name of the refund policy that applies to the content for this service. The name can be from 1 to 15 characters long, and can include uppercase or lowercase letters (the CSG2 changes all letters to uppercase), numbers, and any special characters. |
|---------------------------|--|

## Defaults

None

## Command Modes

Global configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: None. |

## Usage Guidelines

The characteristics of each policy are defined by the following commands:

- **flags**—The CSG2 supports flag-based refunding for all protocols.
- **retcode**—The CSG2 supports return code-based refunding for all protocols except RTSP.

## Examples

The following example shows how to specify CSG2 refund policy COMPANY-REFUND:

```
ip csg refund COMPANY-REFUND
```

## Related Commands

| Command               | Description   |
|-----------------------|---|
| <b>flags</b>          | Specifies IP, TCP, or wireless application protocol (WAP) flag bit masks and values for CSG2 Prepaid Error Reimbursement. |
| <b>ip csg policy</b>  | Defines a policy for qualifying flows for the CSG2 accounting services, and enters CSG2 policy configuration mode.        |
| <b>ip csg service</b> | Configures a CSG2 content billing service, and enters CSG2 service configuration mode.                                    |
| <b>retcode</b>        | Specifies the range of application return codes for which the CSG2 refunds quota for Prepaid Error Reimbursement.         |

# ip csg replicate

To enable high availability (HA) state replication between redundant CSG2 systems, use the **ip csg replicate** command in global configuration mode. To disable state replication, use the **no** form of this command.

```
ip csg replicate [vrf vrf-name] local-ip remote-ip base-port
```

```
no ip csg replicate
```

## Syntax Description

|                     |   |
|---------------------|---|
| <b>vrf vrf-name</b> | (Optional) Virtual Routing and Forwarding (VRF) table which the redundant CSG2s are to use when sending state synchronization messages.   |
| <b>local-ip</b>     | Local IP address on the CSG2 used as the source IP address for outgoing state synchronization messages, and as the listen IP address for incoming state synchronization messages. You must configure this IP address on the local CSG2 as either an interface or as a secondary IP address.   |
| <b>remote-ip</b>    | Remote IP address used as the destination IP address for outgoing state synchronization messages.   |
| <b>base-port</b>    | User Datagram Protocol (UDP) port number used as the source and destination port for state synchronization messages.<br><br>The specified port number is the first of six sequential UDP ports that the CSG2 uses for state synchronization. For example, if you specify port number 2000, the CSG2 uses ports 2000 through 2005 for state synchronization. |

## Defaults

Replication is not enabled.

## Command Modes

Global configuration

## Command History

| Release    | Modification                 |
|------------|------------------------------|
| 12.4(11)MD | This command was introduced. |

## Usage Guidelines

The **ip csg replicate** command enables stateful replication of the CSG2 state data structures, such as the CSG2 User Table.

To enable replication of session and flows, use the **replicate** command in CSG2 content configuration mode.

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

## Examples

The following example shows how to enable CSG2 replication to a peer using local IP address 10.10.10.1, remote IP address, 10.10.10.2, and UDP ports 2000 through 2005:

```
Ip csg replicate 10.10.10.1 10.10.10.2 2000
```

## ■ ip csg replicate

| Related Commands | Command                   | Description  |
|------------------|---------------------------|--|
|                  | <a href="#">replicate</a> | Replicates the connection state for all connections to the CSG2 content servers on the standby system. |

# ip csg report http header

To define the inclusion of multiple HTTP request headers in the CSG2 HTTP\_Header call detail record (CDR), use the **ip csg report http header** command in global configuration mode. To disable this configuration, use the **no** form of this command.

**ip csg report http header** *header-name*

**no ip csg report http header** *header-name*

## Syntax Description

|                    |  |
|--------------------|--|
| <i>header-name</i> | Name of the request header that you want to include in the CSG2 HTTP_Header CDR.<br><br>The header name can be from 1 to 224 characters long, and can include uppercase or lowercase letters (the CSG2 changes all letters to uppercase), numbers, and any special characters. |
|--------------------|--|

## Defaults

The default is to copy only the “host,” “user-agent,” and “from” HTTP headers into the CDRs.

## Command Modes

Global configuration

## Command History

| Release    | Modification  |
|------------|---|
| 12.4(11)MD | This command was migrated from CSG1.<br><br>Changes from CSG1: <ul style="list-style-type: none"> <li>The name of this command changed from <b>report http header</b> to <b>ip csg report http header</b>.</li> <li>The configuration mode for this command changed from CSG accounting configuration to global configuration.</li> </ul> |

## Examples

The following example shows how to enable reporting HTTP header information:

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

## Related Commands

| Command  | Description  |
|--|--|
| <a href="#">ip csg report radius attribute</a> | Specifies the RADIUS attributes to be copied from the RADIUS Start message into CSG2 call detail records (CDRs).                                   |
| <a href="#">ip csg report smtp rfc2822</a>     | Specifies that the CSG2 is to include RFC 2822 header Tag-Length-Values (TLVs) in Simple Mail Transfer Protocol (SMTP) call detail records (CDRs). |

| Command                                      | Description  |
|--|--|
| <a href="#">ip csg report usage</a>          | Enables CSG2 supplemental usage reporting to the quota server.   |
| <a href="#">ip csg report wap actual-pdu</a> | Specifies whether actual wireless application protocol (WAP) protocol data units (PDUs) are to be reported in CSG2 call detail records (CDRs). |

# ip csg report radius attribute

To specify the RADIUS attributes and VSA subattributes to be copied from the RADIUS Start message and sent to the Billing Mediation Agent (BMA) in CSG2 call detail records (CDRs), use the **ip csg report radius attribute** command in global configuration mode. To disable this feature, use the **no** form of this command.

```
ip csg report radius attribute {radius-attribute-number | vsa {vendor-id | 3gpp}  
radius-subattribute-number}
```

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

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

**Defaults** No RADIUS attributes are copied into CDRs.

**Command Modes** Global configuration

| Command History | Release    | Modification  |
|-----------------|------------|---|
|                 | 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: <ul style="list-style-type: none"> <li>The name of this command changed from <b>report radius attribute</b> to <b>ip csg report radius attribute</b>.</li> <li>The configuration mode for this command changed from CSG accounting configuration to global configuration.</li> <li>The <b>26</b> keyword was removed.</li> </ul> |

**Usage Guidelines** You can specify up to 256 attributes.

If an attribute is not present in the RADIUS message, it is not present in the CDRs, unless **ip csg records format fixed** is configured.

The CSG2 saves and reports attribute and subattribute information for each subscriber.

When the CSG2 receives a new RADIUS Accounting Start or RADIUS Interim Accounting Request, it saves the attribute and subattribute information parsed from the new request.

The CSG2 saves only those attributes or subattributes which meet both of the following criteria:

- They are present in the new RADIUS Accounting Start or RADIUS Interim Accounting Request.
- They are configured for reporting at the time the new request arrives at the CSG2.

All previously stored attribute and subattribute information from previous requests is destroyed, even if the new RADIUS Accounting Start or RADIUS Interim Accounting Request does not contain all of the attributes and subattributes that were present in the previous request. Only the currently stored attributes are reported in CDRs.

If there are multiple instances of an attribute, they are all reported. Attributes are reported in the order in which they are presented in the RADIUS message.

If both the reporting of RADIUS attributes and Roaming Service Control are enabled, the CSG2 monitors both sets of attributes, but only changes in the Roaming Service Control attributes trigger reauthorization. For more information about Roaming Service Control, see the [“Enabling Roaming Service Control”](#) section on page 9-9.

### Examples

The following example shows how to specify the RADIUS attributes to be copied from the RADIUS Start message into CDRs:

```
ip csg report radius attribute 3
ip csg report radius attribute 5
ip csg report radius attribute 7
ip csg report radius attribute 44
```

### Related Commands

| Command                                      | Description  |
|--|--|
| <a href="#">ip csg report http header</a>    | Defines the inclusion of multiple HTTP request headers in the CSG2 HTTP_Header call detail record (CDR).   |
| <a href="#">ip csg report smtp rfc2822</a>   | Specifies that the CSG2 is to include RFC 2822 header Tag-Length-Values (TLVs) in Simple Mail Transfer Protocol (SMTP) call detail records (CDRs). |
| <a href="#">ip csg report usage</a>          | Enables CSG2 supplemental usage reporting to the quota server.   |
| <a href="#">ip csg report wap actual-pdu</a> | Specifies whether actual wireless application protocol (WAP) protocol data units (PDUs) are to be reported in CSG2 call detail records (CDRs).     |



# ip csg report smtp rfc2822

To specify that the CSG2 is to include RFC 2822 header Tag-Length-Values (TLVs) in Simple Mail Transfer Protocol (SMTP) call detail records (CDRs), use the **ip csg report smtp rfc2822** command in global configuration mode. To exclude SMTP headers from CDRs, use the **no** form of this command.

```
ip csg report smtp rfc2822
```

```
no ip csg report smtp rfc2822
```

**Syntax Description** This command has no arguments or keywords.

**Defaults** RFC 2822 header TLVs are included in SMTP CDRs.

**Command Modes** Global configuration

| Command History | Release    | Modification                 |
|-----------------|------------|------------------------------|
|                 | 12.4(11)MD | This command was introduced. |

**Examples** The following example shows how to exclude RFC2822 headers from SMTP CDRs:

```
no ip csg report smtp rfc2822
```

| Related Commands | Command  | Description  |
|------------------|--|--|
|                  | <a href="#">ip csg report http header</a>      | Defines the inclusion of multiple HTTP request headers in the CSG2 HTTP_Header call detail record (CDR).                                       |
|                  | <a href="#">ip csg report radius attribute</a> | Specifies the RADIUS attributes to be copied from the RADIUS Start message into CSG2 call detail records (CDRs).                               |
|                  | <a href="#">ip csg report usage</a>            | Enables CSG2 supplemental usage reporting to the quota server.   |
|                  | <a href="#">ip csg report wap actual-pdu</a>   | Specifies whether actual wireless application protocol (WAP) protocol data units (PDUs) are to be reported in CSG2 call detail records (CDRs). |

## ip csg report usage

To enable CSG2 supplemental usage reporting to the quota server, use the **ip csg report usage** command in global configuration mode. To disable supplemental usage reporting, use the **no** form of this command.

```
ip csg report usage { bytes ip | seconds }
```

```
no ip csg report usage { bytes ip | seconds }
```

### Syntax Description

|                 |   |
|-----------------|---|
| <b>bytes ip</b> | Report the number of IP bytes uploaded and downloaded for each interval.  |
| <b>seconds</b>  | Report usage in seconds for the interval, as well as the timestamps of the start of the first and last billable sessions in the interval. |

### Defaults

None

### Command Modes

Global configuration

### Command History

| Release    | Modification  |
|------------|---|
| 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: <ul style="list-style-type: none"> <li>• The name of this command changed from <b>report usage</b> to <b>ip csg report usage</b>.</li> <li>• The configuration mode for this command changed from CSG accounting configuration to global configuration.</li> </ul> |

### Usage Guidelines

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

If you want to report both IP bytes and usage in seconds, you can specify both **ip csg report usage bytes ip** and **ip csg report usage seconds**.

### Examples

The following example shows how to enable supplemental usage reporting for both IP bytes and seconds:

```
ip csg report usage bytes ip
ip csg report usage seconds
```

| Related Commands | Command  | Description  |
|------------------|--|--|
|                  | <a href="#">ip csg report http header</a>      | Defines the inclusion of multiple HTTP request headers in the CSG2 HTTP_Header call detail record (CDR).   |
|                  | <a href="#">ip csg report radius attribute</a> | Specifies the RADIUS attributes to be copied from the RADIUS Start message into call detail records (CDRs).  |
|                  | <a href="#">ip csg report smtp rfc2822</a>     | Specifies that the CSG2 is to include RFC 2822 header Tag-Length-Values (TLVs) in Simple Mail Transfer Protocol (SMTP) call detail records (CDRs). |
|                  | <a href="#">ip csg report wap actual-pdu</a>   | Specifies whether actual wireless application protocol (WAP) protocol data units (PDUs) are to be reported in CSG2 call detail records (CDRs).     |

# ip csg report wap actual-pdu

To specify whether actual protocol data units (PDUs) are to be reported in CSG2 wireless application protocol (WAP) call detail records (CDRs), use the **ip csg report wap actual-pdu** command in global configuration mode. To exclude actual PDUs from WAP CDRs, use the **no** form of this command.

**ip csg report wap actual-pdu**

**no ip csg report wap actual-pdu**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Actual PDUs are not reported in WAP CDRs.

**Command Modes** Global configuration

| Command History | Release    | Modification                 |
|-----------------|------------|------------------------------|
|                 | 12.4(11)MD | This command was introduced. |

**Examples** The following example shows how to report actual PDUs in WAP CDRs:

```
ip csg report wap actual-pdu
```

| Related Commands | Command  | Description  |
|------------------|--|--|
|                  | <a href="#">ip csg report http header</a>      | Defines the inclusion of multiple HTTP request headers in the CSG2 HTTP_Header call detail record (CDR).   |
|                  | <a href="#">ip csg report radius attribute</a> | Specifies the RADIUS attributes to be copied from the RADIUS Start message into call detail records (CDRs).  |
|                  | <a href="#">ip csg report smtp rfc2822</a>     | Specifies that the CSG2 is to include RFC 2822 header Tag-Length-Values (TLVs) in Simple Mail Transfer Protocol (SMTP) call detail records (CDRs). |
|                  | <a href="#">ip csg report usage</a>            | Enables CSG2 supplemental usage reporting to the quota server.   |

# ip csg service

To configure a CSG2 content billing service, and to enter CSG2 service configuration mode, use the **ip csg service** command in global configuration mode. To turn off the content billing service, use the **no** form of this command.

**ip csg service** *service-name*

**no ip csg service** *service-name*

|                           |                     |   |
|---------------------------|---------------------|---|
| <b>Syntax Description</b> | <i>service-name</i> | Name of the content billing service, which is a component of a billing plan that is subscribed to by subscribers. The name can be from 1 to 16 characters long, is not case-sensitive, and can include uppercase or lowercase letters (the CSG2 changes all letters to uppercase), numbers, and any special characters. |
|---------------------------|---------------------|---|

|                 |      |
|-----------------|------|
| <b>Defaults</b> | None |
|-----------------|------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | Global configuration |
|----------------------|----------------------|

|                        |                |  |
|------------------------|----------------|--|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>  |
|                        | 12.4(11)MD     | This command was migrated from CSG1.<br>Changes from CSG1: None. |

**Usage Guidelines**

The CSG2 allows you to define a pool of up to 1024 services. You can authorize, for each subscriber, any number of services from that pool, but we recommend that the billing system not authorize more than 10 active services for each subscriber. Exceeding this guideline could lead to the following problems:

- The increase in the number of quota authorizations per subscriber can overload both the quota server and the CSG2.
- As the number of services for which a subscriber is actively authorized increases, the subscriber's quota becomes fragmented. Although the CSG2 allows the billing system to recall and redistribute the quota so that the subscriber is not denied service because of quota fragmentation, the process increases overhead in both the quota server and the CSG2.

The CSG2 supports multiple protocols under a single service definition.

The characteristics of each content billing service are defined by the following commands:

- [activation](#)
- [aoc append url](#)
- [aoc confirm](#)
- [aoc enable](#)

- [basis](#)
- [class](#)
- [content \(CSG2 service\)](#)
- [idle \(CSG2 service\)](#)
- [meter exclude mms wap](#)
- [meter exclude pause rtsp](#)
- [meter exclude svc-idle](#)
- [meter include imap](#)
- [meter increment](#)
- [meter initial](#)
- [meter minimum](#)
- [owner](#)
- [passthrough](#)
- [reauthorization threshold](#)
- [reauthorization timeout](#)
- [records granularity](#)
- [refund](#)
- [verify confirm](#)
- [verify enable](#)

---

**Examples**

The following example shows how to define a CSG2 content billing service named MOVIES:

```
ip csg service MOVIES
```

---

**Related Commands**

| Command                                | Description  |
|--|--|
| <a href="#">activation</a>             | Specifies the activation mode for a CSG2 Connection Duration service.  |
| <a href="#">aoc append url</a>         | Specifies that the CSG2 is to append the original URL to the redirect URL sent by the quota server for use in Advice of Charge (AoC) URL-rewriting.      |
| <a href="#">aoc confirm</a>            | Configures a token for use in Advice of Charge (AoC) URL-rewriting.  |
| <a href="#">aoc enable</a>             | Enables Advice of Charge (AoC) URL-rewriting for the CSG2.   |
| <a href="#">basis</a>                  | Specifies the billing basis for a CSG2 content billing service.  |
| <a href="#">content (CSG2 service)</a> | Configures content as a member of a CSG2 billing service, identifies a policy to apply to this content, and optionally assigns a weight to this content. |
| <a href="#">idle (CSG2 service)</a>    | Specifies the minimum amount of time that the CSG2 maintains a service with no subscriber sessions.  |
| <a href="#">ip csg billing</a>         | Defines a CSG2 billing plan, and enters CSG2 billing configuration mode.   |

| Command                          | Description   |
|----------------------------------|---|
| <b>ip csg refund</b>             | Specifies the CSG2 refund policy to apply to the various services, and enters CSG2 refund configuration mode.   |
| <b>meter exclude mms wap</b>     | Excludes bytes for a WAP 1.x Multimedia Messaging Service (MMS) session from the CSG2 usage calculation.  |
| <b>meter exclude pause rtsp</b>  | Excludes the Real Time Streaming Protocol (RTSP) PAUSE time from the CSG2 usage calculation.  |
| <b>meter exclude svc-idle</b>    | Excludes the final service idle from the CSG2 usage calculation.  |
| <b>meter include imap</b>        | Specifies which Internet Message Access Protocol (IMAP) bytes are billed for by the CSG2 when doing prepaid debits.   |
| <b>meter increment</b>           | Specifies the increments for debiting quota by the CSG2 upon completion of a service configured for Service Duration Billing.                               |
| <b>meter initial</b>             | Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing. |
| <b>meter minimum</b>             | Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing. |
| <b>owner</b>                     | Specifies an identifier or name for a CSG2 service owner.   |
| <b>passthrough</b>               | Enables passthrough mode for a CSG2 service.  |
| <b>reauthorization threshold</b> | Specifies the CSG2 reauthorization threshold.   |
| <b>reauthorization timeout</b>   | Specifies the CSG2 reauthorization timeout.   |
| <b>records granularity</b>       | Specifies the granularity at which CSG2 billing call detail records (CDRs) are to be generated.   |
| <b>refund</b>                    | Specifies the refund policy for a CSG2 prepaid service.   |
| <b>verify confirm</b>            | Configures a token for use in CSG2 service verification URL-rewriting.  |
| <b>verify enable</b>             | Enables CSG2 service verification.  |

# ip csg snmp timer

To define Simple Network Management Protocol (SNMP) timers for lost CSG2 records, use the **ip csg snmp timer** command in global configuration mode. To restore the default setting, use the **no** form of this command.

```
ip csg snmp timer { bma | psd | quota-server } interval
```

```
no ip csg snmp timer { bma | psd | quota-server } interval
```

## Syntax Description

|                     |  |
|---------------------|--|
| <b>bma</b>          | Defines an SNMP timer for lost CSG2 Billing Mediation Agent (BMA) records.                             |
| <b>psd</b>          | Defines an SNMP timer for lost CSG2 Persistent Storage Device (PSD) records.                           |
| <b>quota-server</b> | Defines an SNMP timer for lost CSG2 quota server records.  |
| <i>interval</i>     | Interval, in seconds, of the CSG2 SNMP timer. The range is from 1 to 2,147,483,647. The default is 60. |

## Defaults

The default SNMP timer interval is 60 seconds.

## Command Modes

Global configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: <ul style="list-style-type: none"> <li>The <b>psd</b> keyword was added.</li> <li>The <b>agent</b> keyword was replaced with the <b>bma</b> keyword.</li> </ul> |

## Examples

The following example defines a 300-second CSG2 SNMP BMA timer:

```
ip csg snmp timer bma 300
```

## Related Commands

| Command                                      | Description   |
|--|---|
| <a href="#">snmp-server enable traps csg</a> | Enable Simple Network Management Protocol (SNMP) notification types that are available on the CSG2. |



# ip csg subscriber

To define a subscriber interface as a CSG2 subscriber interface, use the **ip csg subscriber** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

**ip csg subscriber**

**no ip csg subscriber**

---

**Syntax Description**

This command has no arguments or keywords.

---

**Defaults**

The interface is not a CSG2 subscriber interface.

---

**Command Modes**

Interface configuration

---

**Command History**

| Release    | Modification                 |
|------------|------------------------------|
| 12.4(11)MD | This command was introduced. |

---

**Usage Guidelines**

All traffic routed through the CSG2, including peer-to-peer traffic, must flow from a subscriber interface to a network interface, or from a network interface to a subscriber interface. Therefore, configure the **ip csg subscriber** command on only the subscriber interface, never on the network interface.

---

**Examples**

The following example defines interface GigabitEthernet0/0.69 as a CSG2 subscriber interface:

```
interface GigabitEthernet0/0.69
 ip csg subscriber
```

# ip csg transport-type assign

To classify data traffic on the basis of its access path, use the **ip csg transport-type assign command** in global configuration mode. To remove transport-type information, use the **no** form of this command.

**ip csg transport-type assign** *ip-address value*

**no ip csg transport-type assign** *ip-address value*

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

**Defaults** None

**Command Modes** Global configuration

| Command History | Release    | Modification   |
|-----------------|------------|--|
|                 | 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: <ul style="list-style-type: none"> <li>The name of the command changed from <b>ip csg transport-type</b> to <b>ip csg transport type assign</b>.</li> <li>The <i>ip-address</i> and <i>value</i> arguments were added.</li> </ul> |

**Usage Guidelines** Use the **ip csg transport-type assign** command to classify data traffic on the basis of its access path, using the Network Access Server (NAS) IP address reported in the RADIUS Accounting Start message. Transport-type information is reported in fixed record format call detail records (CDRs).

**Examples** The following example creates a transport-type table and enters transport-type configuration mode:

```
ip csg transport-type assign 1.2.3.4 6
```

| Related Commands | Command                               | Description   |
|------------------|---------------------------------------|---|
|                  | <a href="#">class</a>                 | Specifies a service class value.                      |
|                  | <a href="#">owner</a>                 | Specifies an identifier or name for a service owner.  |
|                  | <a href="#">mode</a>                  | Specifies the mode for a CSG2 billing plan.           |
|                  | <a href="#">ip csg records format</a> | Specifies <b>variable</b> or <b>fixed</b> CDR format. |

# ip iscsi target-profile

To create an iSCSI profile for an iSCSI target on the CSG2, and enter iSCSI configuration mode, use the **ip iscsi target-profile** command in global configuration mode. To remove the iSCSI profile, use the **no** form of the command.

**ip iscsi target-profile** *target-profile-name*

**no ip iscsi target-profile** *target-profile-name*

## Syntax Description

*target-profile-name* Name of the iSCSI profile.

## Command Default

No default behavior or values.

## Command Modes

Global configuration

## Command History

| Release    | Modification                 |
|------------|------------------------------|
| 12.4(15)MD | This command was introduced. |

## Usage Guidelines

You can configure one and only one iSCSI profile on a given CSG2.

The iSCSI profile enables the CSG2 to read/write to a remote iSCSI device (target) on a SAN via an iSCSI.



### Note

The CSG2 supports only one type of backup device, either a PSD or an iSCSI device. The PSD and iSCSI features can coexist, but only one can be enabled at a time.

The characteristics of each content billing service are defined by the following commands:

- [ip \(iSCSI\)](#)
- [name \(iSCSI\)](#)
- [port \(iSCSI\)](#)

## Examples

The following example configures an iSCSI profile with the name **targetA** to use to store and retrieve CDRs when a charging gateway (CG) is not available:

```
ip iscsi target-profile targetA
  name ign.2002-10.edu.abc.io1.iscsi.draft20-target:1
  ip 10.0.0.1
  port 3260
```

| Related Commands | Command                          | Description  |
|------------------|----------------------------------|--|
|                  | <b>ip (iSCSI)</b>                | Specifies the IP address of an iSCSI target in the target interface profile on the CSG2.   |
|                  | <b>ip csg iscsi drain delay</b>  | Defines the delay interval, in seconds, before draining packets from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) when the Billing Mediation Agent (BMA) becomes active.      |
|                  | <b>ip csg iscsi drain packet</b> | Defines the number of packets to be drained from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) per drain delay interval when the Billing Mediation Agent (BMA) becomes active. |
|                  | <b>ip csg iscsi profile</b>      | Specifies the Internet Small Computer Systems Interface (iSCSI) target to be used as backup storage for the CSG2.  |
|                  | <b>name (iSCSI)</b>              | Specifies the name of an iSCSI target in the target profile on the CSG2  |
|                  | <b>port (iSCSI)</b>              | Specifies the number of the port on which to listen for iSCSI traffic in the iSCSI target interface profile on the CSG2.   |

# map

To reference a header, method, or URL map that is part of a CSG2 billing policy, use the **map** command in CSG2 policy configuration mode. To delete the reference, use the **no** form of this command.

**map** *map-name*

**no map** *map-name*

|                           |                           |   |
|---------------------------|---------------------------|---|
| <b>Syntax Description</b> | <i>map-name</i>           | Name of a header, method, or URL map, as configured with an <b>ip csg map</b> command.  |
| <b>Defaults</b>           | None                      |   |
| <b>Command Modes</b>      | CSG2 policy configuration |   |
| <b>Command History</b>    | <b>Release</b>            | <b>Modification</b>   |
|                           | 12.4(11)MD                | This command was migrated from CSG1.<br>Changes from CSG1: This command incorporated the following CSG1 commands: <ul style="list-style-type: none"> <li>• <b>header-map</b></li> <li>• <b>url-map</b></li> </ul> |

## Usage Guidelines

The conditions specified in the referenced header, method, or URL map must be true in order for the flows to be processed by the CSG2 accounting services. If the conditions are not true, the flows are not processed.

When configuring a map, keep the following considerations in mind:

- You cannot specify different types of match patterns in a given map. For example, a map can include one or more **match header** statements, but it cannot include both **match header** statements and **match url** statements.
- You can specify up to three maps in a given policy: one for header matching, one for method matching, and one for URL matching. For example, the following is a valid configuration:

```
ip csg map HOSTMAP
  match header host1 value *.2.*.44
!
ip csg map URLMAP
  match url */mobile/index.wml
!
ip csg policy MAP-POLICY
  map HOSTMAP
  map URLMAP
```

In this example, a flow must match both HOSTMAP and URLMAP in order to match policy MAP-POLICY.

**Examples**

The following example shows how to reference maps for CSG2 policies MOVIES and GAMES:

```
ip csg policy MOVIES
  map HORROR
  map COMEDY
ip csg policy GAMES
  map GAMES
```

**Related Commands**

| Command                       | Description  |
|-------------------------------|--|
| <a href="#">ip csg map</a>    | Defines the CSG2 billing content filters (header, method, and URL maps), and enters CSG2 map configuration mode. |
| <a href="#">ip csg policy</a> | Defines a policy for qualifying flows for the CSG2 billing services, and enters CSG2 policy configuration mode.  |
| <a href="#">match header</a>  | Specifies a header match pattern for a CSG2 billing map.   |
| <a href="#">match method</a>  | Specifies a method match pattern for a CSG2 billing map.   |
| <a href="#">match url</a>     | Specifies a URL match pattern for a CSG2 billing map.  |

# match header

To specify a header match pattern for a CSG2 billing map, use the **match header** command in CSG2 map configuration mode. To delete the header match pattern, use the **no** form of this command.

**match header** *header-name value*

**no match header** *header-name value*

## Syntax Description

|                    |  |
|--------------------|--|
| <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 <b>Content-Type</b> , <b>Host</b> , <b>Referer</b> , <b>User-Agent</b> , or an arbitrary header name from 1 to 63 characters long. The header name can include uppercase or lowercase letters (the CSG2 changes all letters to uppercase), numbers, and any special characters. |
|                    | <b>Note</b> For Session Initiation Protocol (SIP), you must enter the long form of the header name. The CSG2 does not support the short form of the header name.   |
| <i>value</i>       | Regular header pattern that is to be matched against the input header. The pattern can include up to 127 characters, including wildcards and UNIX string-matching special characters.  |

## Defaults

None.

## Command Modes

CSG2 map configuration

## Command History

| Release    | Modification  |
|------------|---|
| 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: <ul style="list-style-type: none"> <li>The name of this command changed from <b>match (header map)</b> to <b>match header</b>.</li> <li>The configuration mode for this command changed from CSG header map configuration to CSG2 map configuration.</li> <li>The <b>protocol</b> <i>protocol</i> and <b>value</b> keywords and arguments were removed.</li> <li>The <i>pattern</i> argument was replaced with the <i>value</i> argument.</li> </ul> |
| 12.4(15)MD | Support for Session Initiation Protocol (SIP) headers was added.  |

**Usage Guidelines**

This command is valid only for HTTP and Session Initiation Protocol (SIP).

You can use more than one **match header** command in CSG2 map configuration mode to specify multiple header match patterns for a header map as follows:

- You can configure more than one **match header** command in a given header map, but they must reference different headers.

For example, the following is a valid configuration, because the first **match header** command references header **Host** and the other references header **User-Agent**:

```
ip csg map HDR1
  match header Host www.cisco.com
  match header User-Agent myagent
```

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

```
ip csg map HDR1
  match header Host www.cisco.com
  match header Host my.cisco.com
```

- If a flow matches *all* of a map's header match patterns, then the CSG2 accepts and processes the flow (unless another map associated with the flow does not match, of course).
- If a flow *does not* match *even one* of a map's header match patterns, then the match fails and the CSG2 does not accept or process the flow.
- The CSG2 treats each header match pattern as a double-wildcard match, which means that a header match pattern that includes even a single wildcard, such as **match header host\* 1.2.3.4**, is treated as a triple-wildcard match. The more wildcard matches you use, the fewer header maps and header match patterns the CSG2 can handle, depending on your configuration. Therefore, to optimize the performance of the CSG2, minimize the number of header match patterns that are applied to a CSG2 content configuration, and minimize the number of wildcards used in header match patterns.
- By default, the header match patterns are case-sensitive. For example, if you define the following header match pattern:

```
match header host1 *.2.*.44
```

but the actual HTTP header keyword is **HOST1**, then the match fails and the CSG2 does not accept or process the flow.

If you do not want the header match patterns to be case-sensitive, configure the **no ip csg case-sensitive** command.

You can specify up to 8192 match patterns.

The following table shows and describes the special characters that you can use in the *value* argument in header match patterns.

| Convention | Description   |
|------------|---|
| *          | Zero or more characters.                                      |
| +          | Zero or more repeated instances of the token preceding the +. |
| ?          | Zero or one character.  |



| Convention                          | Description   |
|-------------------------------------|---|
| <code>\character</code>             | Escaped character.<br>Examples:<br><code>\?</code> Match on a question mark ( <code>\&lt;ctrl-v&gt;?</code> )<br><code>\+</code> Match on a plus sign<br><code>\*</code> Match on an asterisk<br><code>\a</code> Alert (ASCII 7)<br><code>\b</code> Backspace (ASCII 8)<br><code>\f</code> Form-feed (ASCII 12)<br><code>\n</code> New line (ASCII 10)<br><code>\r</code> Carriage return (ASCII 13)<br><code>\t</code> Tab (ASCII 9)<br><code>\v</code> Vertical tab (ASCC 11)<br><code>\0</code> Null (ASCII 0)<br><code>\\</code> Back slash |
| Bracketed range [0-9]               | Matching any single character from the range.   |
| A leading <code>^</code> 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.<br>For example, <code>\x3f</code> yields a <code>?</code> for a one-character wild card match.  |

When configuring a map, keep the following considerations in mind:

- You cannot specify different types of match patterns in a given map. For example, a map can include one or more **match header** statements, but it cannot include both **match header** statements and **match url** statements.
- You can specify up to three maps in a given policy: one for header matching, one for method matching, and one for URL matching. For example, the following is a valid configuration:

```
ip csg map HOSTMAP
  match header host1 value *.2.*.44
!
ip csg map URLMAP
  match url */mobile/index.wml
!
ip csg policy MAP-POLICY
  map HOSTMAP
  map URLMAP
```

In this example, a flow must match both HOSTMAP and URLMAP in order to match policy MAP-POLICY.

## Examples

The following example shows how to specify HTTP header match patterns for map HDR1. In this example, the header match is TRUE *only* for host **www.cisco.com** and user agent **myagent**. Any other combination of host and IP address matches FALSE:

```
ip csg map HDR1
  match header Host www.cisco.com
```

```
match header User-Agent myagent
```

The following example shows how to specify SIP header match patterns for map SIP-HDR1. In this example, the header match is TRUE *only* for Event **presence** and Content-Type **application/sdp**. Any other combination of Event and Content-Type matches FALSE:

```
ip csg map SIP-HDR1
match header Event presence
match header Content-Type application/sdp
```

#### Related Commands

| Command                               | Description  |
|---------------------------------------|--|
| <a href="#">ip csg case-sensitive</a> | Specifies whether to treat CSG2 header, method, and URL match patterns as case-sensitive.                        |
| <a href="#">ip csg map</a>            | Defines the CSG2 billing content filters (header, method, and URL maps), and enters CSG2 map configuration mode. |
| <a href="#">ip csg policy</a>         | Defines a policy for qualifying flows for the CSG2 billing services, and enters CSG2 policy configuration mode.  |
| <a href="#">map</a>                   | References a header, method, or URL map that is part of a CSG2 billing policy.                                   |
| <a href="#">match method</a>          | Specifies a method match pattern for a CSG2 billing map.   |
| <a href="#">match url</a>             | Specifies a URL match pattern for a CSG2 billing map.  |

# match method

To specify a method match pattern for a CSG2 billing map, use the **match method** command in CSG2 map configuration mode. To delete the match pattern, use the **no** form of this command.

**match method** *method-name*

**no match method** *method-name*

## Syntax Description

|                    |  |
|--------------------|--|
| <i>method-name</i> | Method to be matched. Valid methods are: <ul style="list-style-type: none"> <li>• Extension method name of 1 to 15 characters</li> <li>• <b>connect</b>—HTTP CONNECT method</li> <li>• <b>get</b>—HTTP GET method</li> <li>• <b>head</b>—HTTP HEAD method</li> <li>• <b>post</b>—HTTP POST method</li> </ul> |
|--------------------|--|

## Defaults

None.

## Command Modes

CSG2 map configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was introduced.                                     |
| 12.4(15)MD | Support for Session Initiation Protocol (SIP) methods was added. |

## Usage Guidelines

This command is valid only for HTTP and SIP.

You can use more than one **match method** command in CSG2 map configuration mode to specify multiple method match patterns for a method map:

- If a flow matches *any* of a map's method match patterns, then the CSG2 accepts and processes the flow (unless another map associated with the flow does not match, of course).
- If a flow *does not* match *any* of a map's method match patterns, then the match fails and the CSG2 does not accept or process the flow.
- By default, the method match patterns are case-sensitive. For example, if you define the following method match pattern:

**match method get**

but the actual method keyword is **GET**, then the match fails and the CSG2 does not accept or process the flow.

If you do not want the method match patterns to be case-sensitive, configure the **no ip csg case-sensitive** command.

You can specify up to 8192 match patterns.

The following table shows and describes the special characters that you can use in the *method-name* argument in method match patterns.

| Convention             | Description  |
|------------------------|--|
| *                      | Zero or more characters.   |
| +                      | Zero or more repeated instances of the token preceding the +.  |
| ?                      | Zero or one character.   |
| <i>\character</i>      | Escaped character.<br>Examples:<br>\? Match on a question mark (\<ctrl-v>?)<br>\+ Match on a plus sign<br>\* Match on an asterisk<br>\a Alert (ASCII 7)<br>\b Backspace (ASCII 8)<br>\f Form-feed (ASCII 12)<br>\n New line (ASCII 10)<br>\r Carriage return (ASCII 13)<br>\t Tab (ASCII 9)<br>\v Vertical tab (ASCC 11)<br>\0 Null (ASCII 0)<br>\\ 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.<br>For example, \x3f yields a ? for a one-character wild card match.   |

When configuring a map, keep the following considerations in mind:

- You cannot specify different types of match patterns in a given map. For example, a map can include one or more **match header** statements, but it cannot include both **match header** statements and **match url** statements.
- You can specify up to three maps in a given policy: one for header matching, one for method matching, and one for URL matching. For example, the following is a valid configuration:

```
ip csg map HOSTMAP
  match header host1 value *.2.*.44
!
ip csg map URLMAP
  match url */mobile/index.wml
!
ip csg policy MAP-POLICY
  map HOSTMAP
  map URLMAP
```

In this example, a flow must match both HOSTMAP and URLMAP in order to match policy MAP-POLICY.

### Examples

The following example shows how to specify a GET method match pattern for map MOVIES:

```
ip csg map MOVIES
match method GET
```

### Related Commands

| Command                               | Description  |
|---------------------------------------|--|
| <a href="#">ip csg case-sensitive</a> | Specifies whether to treat CSG2 header, method, and URL match patterns as case-sensitive.                        |
| <a href="#">ip csg map</a>            | Defines the CSG2 billing content filters (header, method, and URL maps), and enters CSG2 map configuration mode. |
| <a href="#">ip csg policy</a>         | Defines a policy for qualifying flows for the CSG2 billing services, and enters CSG2 policy configuration mode.  |
| <a href="#">map</a>                   | References a header, method, or URL map that is part of a CSG2 billing policy.                                   |
| <a href="#">match header</a>          | Specifies a header match pattern for a CSG2 billing map.   |
| <a href="#">match url</a>             | Specifies a URL match pattern for a CSG2 billing map.  |

# match url

To specify a URL match pattern for a CSG2 billing map, use the **match url** command in CSG2 map configuration mode. To delete the match pattern, use the **no** form of this command.

**match url** *pattern*

**no match url** *pattern*

## Syntax Description

|                |   |
|----------------|---|
| <i>pattern</i> | Regular URL pattern to be matched against the input URL. The pattern can include up to 127 characters, including wildcards and UNIX string-matching special characters. |
|----------------|---|

## Command Modes

CSG2 map configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: <ul style="list-style-type: none"> <li>The name of this command changed from <b>match (URL map)</b> to <b>match url</b>.</li> <li>The configuration mode for this command changed from CSG2 URL map configuration to CSG2 map configuration.</li> <li>The <b>protocol</b> <i>protocol</i> and <b>method</b> <i>method</i> keywords and arguments were removed.</li> </ul> |
| 12.4(15)MD | Support for Session Initiation Protocol (SIP) URLs was added.  |

## Usage Guidelines

You can use more than one **match url** command in CSG2 map configuration mode to specify multiple URL match patterns for a URL map:

- If a flow matches *any* of a map's URL match patterns, then the CSG2 accepts and processes the flow (unless an attribute, header, or method map associated with the flow does not match, of course).
- If a flow *does not* match *any* of a map's URL match patterns, then the match fails and the CSG2 does not accept or process the flow.
- By default, the URL match patterns are case-sensitive, and you must consider uppercase and lowercase combinations carefully when you create URL match patterns. For example, if you define the following URL match pattern:

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

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

**HTTP://url-string**

then the match fails and the CSG2 does not accept or process the flow.

If you do not want the URL match patterns to be case-sensitive, configure the **no ip csg case-sensitive** command.

- As a further example, by default the following URLs do not match:

**http://www.cisco.com/index.html**

**http://www.cisco.com/INDEX.html**

However, if you have disabled case-sensitivity by entering the **no ip csg case-sensitive** command, then all of the following URLs match:

**http://www.cisco.com/index.html**

**http://www.cisco.com/INDEX.html**

**http://www.cisco.com/Index.html**

**http://www.cisco.com/IndeX.html**

**http://www.cisco.com/INdex.html**

- When you configure URL match patterns for Real Time Streaming Protocol (RTSP) streams, be sure to account for trailing stream IDs in RTSP stream names. For example, URL match pattern **\*.mpeg** does not match **rtsp://1.1.1.254:554/movie.mpeg/streamid=0** because the stream name has a trailing **/streamid=0**. To match such RTSP stream names, use a URL match pattern such as **\*.mpeg\***.
- You can include up to two wildcards in each URL match pattern, but the more wildcard matches you use, the fewer URL maps and URL match patterns the CSG2 can handle, depending on your configuration. For example, the CSG2 can handle the following combinations of URL maps and URL match patterns:
  - If you have one content and 1023 policies, then the CSG2 can handle up to 1023 URL maps, each with one URL match pattern and no wildcards.
  - If you have 2000 contents, each with the same policy and the same URL map, then the CSG2 can handle up to 100 URL match patterns for that map, with one wildcard in each pattern (such as **\*movies** or **movies\***, but not **\*movies\***).
  - If you have one content, one policy, and one URL map, then the CSG2 can handle up to 17 match patterns for that map, with two wildcards in each pattern (such as **\*movies\***).
- When using wildcards in URL match patterns, observe the following guidelines to optimize the performance of the CSG2:
  - Minimize the number of URL match patterns that are applied to a CSG2 content configuration.
  - Minimize the number of keyword URL match patterns that you use. In general, it is better to use multiple single-wildcard URL match patterns instead of individual keyword URL match patterns.
  - Combine several keyword URL match patterns into a single pattern by using UNIX string-matching special characters. For example, **\*.movies\_comedy.com/\*.mpeg**, **\*.movies\_action.com/\*.mpeg**, and **\*.movies\_drama.com/\*.mpeg** can be combined into the following single pattern:

**\*.movies\_(comedy|action|drama).com/\*.mpeg**

And these patterns

**\*.movies\_comedy.com/\*.mpeg**

**\*.movies\_action.com/\*.mpeg**

**\*.movies\_drama.com/\*.mpeg**

**\*.clips\_comedy.com/\*.mpeg**

**\*.clips\_action.com/\*.mpeg**

**\*.clips\_drama.com/\*.mpeg**

can be combined into the following single pattern:

**\*.(movies|clips)\*?\*(comedy|action|drama).com/\*.mpeg**

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

You can specify up to 8192 match patterns.

The following table shows and describes the special characters that you can use in the *pattern* argument in URL match patterns.

| Convention             | Description  |
|------------------------|--|
| *                      | Zero or more characters.   |
| +                      | Zero or more repeated instances of the token preceding the +.  |
| ?                      | Zero or one character.   |
| <i>\character</i>      | Escaped character.<br>Examples:<br>\? Match on a question mark (\<ctrl-v>?)<br>\+ Match on a plus sign<br>\* Match on an asterisk<br>\a Alert (ASCII 7)<br>\b Backspace (ASCII 8)<br>\f Form-feed (ASCII 12)<br>\n New line (ASCII 10)<br>\r Carriage return (ASCII 13)<br>\t Tab (ASCII 9)<br>\v Vertical tab (ASCC 11)<br>\0 Null (ASCII 0)<br>\\ 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.<br>For example, \x3f yields a ? for a one-character wild card match.   |

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



When configuring a map, keep the following considerations in mind:

- We recommend that you configure the URL match pattern during your maintenance window, or during off-peak hours.
- You cannot specify different types of match patterns in a given map. For example, a map can include one or more **match header** statements, but it cannot include both **match header** statements and **match url** statements.
- You can specify up to three maps in a given policy: one for header matching, one for method matching, and one for URL matching. For example, the following is a valid configuration:

```
ip csg map HOSTMAP
  match header host1 value *.2.*.44
!
ip csg map URLMAP
  match url */mobile/index.wml
!
ip csg policy MAP-POLICY
  map HOSTMAP
  map URLMAP
```

In this example, a flow must match both HOSTMAP and URLMAP in order to match policy MAP-POLICY.

### Examples

The following example shows how to specify URL match patterns for map MOVIES. In this example, the URL match is TRUE for **\*.movies\_comedy.com/\*.mpeg**, for **\*.movies\_action.com/\*.mpeg**, for **\*.movies\_drama.com/\*.mpeg**, and for any other URLs that match the pattern:

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

### Related Commands

| Command                               | Description  |
|---------------------------------------|--|
| <a href="#">ip csg case-sensitive</a> | Specifies whether to treat CSG2 header, method, and URL match patterns as case-sensitive.                        |
| <a href="#">ip csg map</a>            | Defines the CSG2 billing content filters (header, method, and URL maps), and enters CSG2 map configuration mode. |
| <a href="#">ip csg policy</a>         | Defines a policy for qualifying flows for the CSG2 billing services, and enters CSG2 policy configuration mode.  |
| <a href="#">map</a>                   | References a header, method, or URL map that is part of a CSG2 billing policy.                                   |
| <a href="#">match header</a>          | Specifies a header match pattern for a CSG2 billing map.   |
| <a href="#">match method</a>          | Specifies a method match pattern for a CSG2 billing map.   |

# meter exclude control sip

To exclude call control packets for a Session Initiation Protocol (SIP) session from the CSG2 usage calculation, use the **meter exclude control sip** command in CSG2 service configuration mode. To return to the default behavior, use the **no** form of the command.

**meter exclude control sip**

**no meter exclude control sip**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The default behavior is to include the SIP call control packets in the usage calculation.

## Command Modes

CSG2 service configuration

## Command History

| Release    | Modification                 |
|------------|------------------------------|
| 12.4(15)MD | This command was introduced. |

## Usage Guidelines

The **meter exclude control sip** command and the **basis second** command in CSG2 service configuration mode are mutually exclusive. If you configure the **meter exclude control sip** command, do not configure the **basis second** command.

## Examples

The following example shows how to exclude the call control packets for a SIP session from the usage calculation for the SERVICE-A service:

```
ip csg service SERVICE-A
meter exclude control sip
```

## Related Commands

| Command  | Description  |
|--|--|
| <a href="#">ip csg service</a>                 | Configures a CSG2 content billing service, and enters CSG2 service configuration mode.   |
| <a href="#">meter exclude mms wap</a>          | Excludes bytes for a WAP 1.x Multimedia Messaging Service (MMS) session from the CSG2 usage calculation.   |
| <a href="#">meter exclude network-init sip</a> | Excludes incoming Session Initiation Protocol (SIP) transactions (that is, those that are initiated from the network) from the CSG2 usage calculation. |
| <a href="#">meter exclude pause rtsp</a>       | Excludes the Real Time Streaming Protocol (RTSP) PAUSE time from the CSG2 usage calculation.   |
| <a href="#">meter exclude svc-idle</a>         | Excludes the final service idle from the CSG2 usage calculation.   |

| Command                   | Description   |
|---------------------------|---|
| <b>meter include imap</b> | Specifies which Internet Message Access Protocol (IMAP) bytes are billed for by the CSG2 when doing prepaid debits.   |
| <b>meter increment</b>    | Specifies the increments for debiting quota by the CSG2 upon completion of a service configured for Service Duration Billing.                               |
| <b>meter initial</b>      | Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing. |
| <b>meter minimum</b>      | Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing. |

# meter exclude mms wap

To exclude bytes for a WAP 1.x Multimedia Messaging Service (MMS) session from the CSG2 usage calculation, use the **meter exclude mms wap** command in CSG2 service configuration mode. To return to the default behavior, use the **no** form of the command.

**meter exclude mms wap**

**no meter exclude mms wap**

**Syntax Description** This command has no arguments or keywords.

**Defaults** The default behavior is to include the MMS in the usage calculation.

**Command Modes** CSG2 service configuration

| Command History | Release    | Modification  |
|-----------------|------------|---|
|                 | 12.4(11)MD | This command was migrated from CSG1.  |
|                 |            | Changes from CSG1: The <b>meter exclude</b> command split into three new commands— <b>meter exclude mms wap</b> , <b>meter exclude pause rtsp</b> , and <b>meter exclude svc-idle</b> . |

**Examples** The following example shows how to exclude the bytes for a WAP 1.x MMS session from the usage calculation for the SERVICE-A service:

```
ip csg service SERVICE-A
  meter exclude mms wap
```

| Related Commands | Command  | Description  |
|------------------|--|--|
|                  | <a href="#">ip csg service</a>                 | Configures a CSG2 content billing service, and enters CSG2 service configuration mode.   |
|                  | <a href="#">meter exclude control sip</a>      | Excludes call control packets for a Session Initiation Protocol (SIP) session from the CSG2 usage calculation.   |
|                  | <a href="#">meter exclude network-init sip</a> | Excludes incoming Session Initiation Protocol (SIP) transactions (that is, those that are initiated from the network) from the CSG2 usage calculation. |
|                  | <a href="#">meter exclude pause rtsp</a>       | Excludes the Real Time Streaming Protocol (RTSP) PAUSE time from the CSG2 usage calculation.   |
|                  | <a href="#">meter exclude svc-idle</a>         | Excludes the final service idle from the CSG2 usage calculation.   |
|                  | <a href="#">meter include imap</a>             | Specifies which Internet Message Access Protocol (IMAP) bytes are billed for by the CSG2 when doing prepaid debits.                                    |

| Command                | Description   |
|------------------------|---|
| <b>meter increment</b> | Specifies the increments for debiting quota by the CSG2 upon completion of a service configured for Service Duration Billing.                               |
| <b>meter initial</b>   | Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing. |
| <b>meter minimum</b>   | Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing. |

# meter exclude network-init sip

To exclude incoming Session Initiation Protocol (SIP) transactions (that is, those that are initiated from the network) from the CSG2 usage calculation, use the **meter exclude network-init sip** command in CSG2 service configuration mode. To return to the default behavior, use the **no** form of the command.

**meter exclude network-init sip**

**no meter exclude network-init sip**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The default behavior is to include incoming SIP transactions in the usage calculation.

## Command Modes

CSG2 service configuration

## Command History

| Release    | Modification                 |
|------------|------------------------------|
| 12.4(15)MD | This command was introduced. |

## Examples

The following example shows how to exclude incoming SIP transactions from the usage calculation for the SERVICE-A service:

```
ip csg service SERVICE-A
  meter exclude network-init sip
```

## Related Commands

| Command                                   | Description   |
|---|---|
| <a href="#">ip csg service</a>            | Configures a CSG2 content billing service, and enters CSG2 service configuration mode.  |
| <a href="#">meter exclude control sip</a> | Excludes call control packets for a Session Initiation Protocol (SIP) session from the CSG2 usage calculation.                |
| <a href="#">meter exclude mms wap</a>     | Excludes bytes for a WAP 1.x Multimedia Messaging Service (MMS) session from the CSG2 usage calculation.                      |
| <a href="#">meter exclude pause rtsp</a>  | Excludes the Real Time Streaming Protocol (RTSP) PAUSE time from the CSG2 usage calculation.                                  |
| <a href="#">meter exclude svc-idle</a>    | Excludes the final service idle from the CSG2 usage calculation.  |
| <a href="#">meter include imap</a>        | Specifies which Internet Message Access Protocol (IMAP) bytes are billed for by the CSG2 when doing prepaid debits.           |
| <a href="#">meter increment</a>           | Specifies the increments for debiting quota by the CSG2 upon completion of a service configured for Service Duration Billing. |

| Command              | Description   |
|----------------------|---|
| <b>meter initial</b> | Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing. |
| <b>meter minimum</b> | Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing. |

# meter exclude pause rtsp

To exclude the Real Time Streaming Protocol (RTSP) PAUSE time from the CSG2 usage calculation, use the **meter exclude pause rtsp** command in CSG2 service configuration mode. To return to the default behavior, use the **no** form of the command.

**meter exclude pause rtsp**

**no meter exclude pause rtsp**

**Syntax Description** This command has no arguments or keywords.

**Defaults** The default behavior is to include the RTSP PAUSE time in the usage calculation.

**Command Modes** CSG2 service configuration

| Command History | Release    | Modification  |
|-----------------|------------|---|
|                 | 12.4(11)MD | This command was migrated from CSG1.  |
|                 |            | Changes from CSG1: The <b>meter exclude</b> command split into three new commands— <b>meter exclude mms wap</b> , <b>meter exclude pause rtsp</b> , and <b>meter exclude svc-idle</b> . |

**Usage Guidelines** You must configure **basis second** before configuring this command.

**Examples** The following example shows how to exclude the RTSP PAUSE time from the usage calculation for the SERVICE-A service:

```
ip csg service SERVICE-A
  basis second
  meter exclude pause rtsp
```

| Related Commands | Command  | Description  |
|------------------|--|--|
|                  | <a href="#">ip csg service</a>                 | Configures a CSG2 content billing service, and enters CSG2 service configuration mode.   |
|                  | <a href="#">meter exclude control sip</a>      | Excludes call control packets for a Session Initiation Protocol (SIP) session from the CSG2 usage calculation.   |
|                  | <a href="#">meter exclude mms wap</a>          | Excludes bytes for a WAP 1.x Multimedia Messaging Service (MMS) session from the CSG2 usage calculation.   |
|                  | <a href="#">meter exclude network-init sip</a> | Excludes incoming Session Initiation Protocol (SIP) transactions (that is, those that are initiated from the network) from the CSG2 usage calculation. |



| Command                                | Description   |
|--|---|
| <a href="#">meter exclude svc-idle</a> | Excludes the final service idle from the CSG2 usage calculation.  |
| <a href="#">meter include imap</a>     | Specifies which Internet Message Access Protocol (IMAP) bytes are billed for by the CSG2 when doing prepaid debits.   |
| <a href="#">meter increment</a>        | Specifies the increments for debiting quota by the CSG2 upon completion of a service configured for Service Duration Billing.                               |
| <a href="#">meter initial</a>          | Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing. |
| <a href="#">meter minimum</a>          | Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing. |

# meter exclude svc-idle

To exclude the final service idle from the CSG2 usage calculation, use the **meter exclude svc-idle** command in CSG2 service configuration mode. To return to the default behavior, use the **no** form of the command.

**meter exclude svc-idle**

**no meter exclude svc-idle**

**Syntax Description** This command has no arguments or keywords.

**Defaults** The default behavior is to include the service-idle in the usage calculation.

**Command Modes** CSG2 service configuration

| Command History | Release    | Modification  |
|-----------------|------------|---|
|                 | 12.4(11)MD | This command was migrated from CSG1.  |
|                 |            | Changes from CSG1: The <b>meter exclude</b> command split into three new commands— <b>meter exclude mms wap</b> , <b>meter exclude pause rtsp</b> , and <b>meter exclude svc-idle</b> . |

**Usage Guidelines** Configuration of this command can result in reduced charging because the next service access occurs after the service idles, rather than occurring before the service idles.

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

**Examples** The following example shows how to exclude the final service idle from the usage calculation for the OFF\_NET service:

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

| Related Commands | Command                                   | Description  |
|------------------|---|--|
|                  | <a href="#">ip csg service</a>            | Configures a CSG2 content billing service, and enters CSG2 service configuration mode.                         |
|                  | <a href="#">meter exclude control sip</a> | Excludes call control packets for a Session Initiation Protocol (SIP) session from the CSG2 usage calculation. |
|                  | <a href="#">meter exclude mms wap</a>     | Excludes bytes for a WAP 1.x Multimedia Messaging Service (MMS) session from the CSG2 usage calculation.       |

| Command                               | Description   |
|---------------------------------------|---|
| <b>meter exclude network-init sip</b> | Excludes incoming Session Initiation Protocol (SIP) transactions (that is, those that are initiated from the network) from the CSG2 usage calculation.      |
| <b>meter exclude pause rtsp</b>       | Excludes the Real Time Streaming Protocol (RTSP) PAUSE time from the CSG2 usage calculation.  |
| <b>meter include imap</b>             | Specifies which Internet Message Access Protocol (IMAP) bytes are billed for by the CSG2 when doing prepaid debits.   |
| <b>meter increment</b>                | Specifies the increments for debiting quota by the CSG2 upon completion of a service configured for Service Duration Billing.                               |
| <b>meter initial</b>                  | Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing. |
| <b>meter minimum</b>                  | Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing. |

# meter include imap

To specify which Internet Message Access Protocol (IMAP) bytes are billed for by the CSG2 when doing prepaid debits, use the **meter include imap** command in CSG2 service configuration mode. To return to the default behavior, use the **no** form of the command.

**meter include imap body {header | only | other}**

**no meter include imap**

## Syntax Description

|                    |   |
|--------------------|---|
| <b>body header</b> | Only BODY and HEADER IMAP bytes are to be counted when performing prepaid debits. |
| <b>body only</b>   | Only BODY IMAP bytes are to be counted when performing prepaid debits.            |
| <b>body other</b>  | Only BODY and OTHER IMAP bytes are to be counted when performing prepaid debits.  |

## Defaults

All IMAP bytes are to be counted when performing prepaid debits.

## Command Modes

CSG2 service configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: <ul style="list-style-type: none"> <li>The name of this command changed from <b>meter imap</b> to <b>meter include imap</b>.</li> <li>The <b>body-header</b>, <b>body-only</b>, and <b>body-other</b> keywords changed to <b>body header</b>, <b>body only</b>, and <b>body other</b>, respectively.</li> </ul> |

## Usage Guidelines

You can configure only one **meter include imap** command per service. The billing basis for the service must be **byte**. The three categories of bytes are BODY, HEADER, and OTHER, determined as follows:

- BODY—The bytes are classified as BODY if a fetch request or response is encountered for one of the following specifications (including any appended “<>” subset variants):
  - BODY[]
  - BODY[#]
  - BODY[TEXT]
  - BODY[#.TEXT]
  - BODY.PEEK[]
  - BODY.PEEK[#]
  - BODY.PEEK[TEXT]

- BODY.PEEK[#.TEXT]
- RFC822
- RFC822.TEXT
- HEADER—If the bytes cannot be classified as BODY, then they are classified as HEADER if a fetch request or response is encountered for one of the following specifications (including any appended “<>” subset variants):
  - BODY[HEADER]
  - BODY[#.HEADER]
  - BODY.PEEK[HEADER]
  - BODY.PEEK[#.HEADER]
  - RFC822.HEADER
- OTHER—If request or response cannot be classified as BODY or HEADER, then it is classified as OTHER. OTHER examples include:
  - SYN/FIN/ACK/RST packets that do not contain a payload
  - Non-HEADER or BODY IMAP commands such as **3 select inbox**
  - Retransmitted packets
  - Anything else that is not considered BODY or HEADER
  - If the session becomes encrypted or enters PASSTHRU mode, subsequent packets for the session cannot be parsed and are treated as OTHER.

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

### Examples

The following example shows how to configure IMAP to count only BODY bytes when performing prepaid debits:

```
ip csg service S1
meter include imap body only
```

### Related Commands

| Command  | Description  |
|--|--|
| <a href="#">ip csg service</a>                 | Configures a CSG2 content billing service, and enters CSG2 service configuration mode.   |
| <a href="#">meter exclude control sip</a>      | Excludes call control packets for a Session Initiation Protocol (SIP) session from the CSG2 usage calculation.   |
| <a href="#">meter exclude mms wap</a>          | Excludes bytes for a WAP 1.x Multimedia Messaging Service (MMS) session from the CSG2 usage calculation.   |
| <a href="#">meter exclude network-init sip</a> | Excludes incoming Session Initiation Protocol (SIP) transactions (that is, those that are initiated from the network) from the CSG2 usage calculation. |
| <a href="#">meter exclude pause rtsp</a>       | Excludes the Real Time Streaming Protocol (RTSP) PAUSE time from the CSG2 usage calculation.   |
| <a href="#">meter exclude svc-idle</a>         | Excludes the final service idle from the CSG2 usage calculation.   |

| Command                | Description   |
|------------------------|---|
| <b>meter increment</b> | Specifies the increments for debiting quota by the CSG2 upon completion of a service configured for Service Duration Billing.                               |
| <b>meter initial</b>   | Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing. |
| <b>meter minimum</b>   | Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing. |

# meter increment

To specify the increments for debiting quota by the CSG2 upon completion of a service configured for Service Duration Billing, use the **meter increment** command in CSG2 service configuration mode. To restore the default behavior, use the **no** form of the command.

**meter increment** *value*

**no meter increment** *value*

## Syntax Description

*value*

Increment, in seconds, for debiting quota upon completion of a service configured for Service Duration Billing. For example, to enable the CSG2 to charge quota per minute instead of per second, specify **meter increment 60**.

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

## Defaults

The default increment is 1 second.

## Command Modes

CSG2 service configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: None. |

## Usage Guidelines

If **basis second** is configured for the service, the network usage (usage excluding the initial charge) is rounded up to the nearest integer multiple of the increment value when the Service Stop is sent. For an increment value of 60, the CSG2 does not round up 120 seconds of network usage; however, the CSG2 does round up, say, 163 seconds of network usage to 180 quadrans before it calculates total usage for reporting in the Service Stop.



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

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

**Examples**

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

```
ip csg service OFF_NET
meter increment 100
```

**Related Commands**

| Command  | Description   |
|--|---|
| <a href="#">ip csg service</a>                 | Configures a CSG2 content billing service, and enters CSG2 service configuration mode.  |
| <a href="#">meter exclude control sip</a>      | Excludes call control packets for a Session Initiation Protocol (SIP) session from the CSG2 usage calculation.  |
| <a href="#">meter exclude mms wap</a>          | Excludes bytes for a WAP 1.x Multimedia Messaging Service (MMS) session from the CSG2 usage calculation.  |
| <a href="#">meter exclude network-init sip</a> | Excludes incoming Session Initiation Protocol (SIP) transactions (that is, those that are initiated from the network) from the CSG2 usage calculation.      |
| <a href="#">meter exclude pause rtsp</a>       | Excludes the Real Time Streaming Protocol (RTSP) PAUSE time from the CSG2 usage calculation.  |
| <a href="#">meter exclude svc-idle</a>         | Excludes the final service idle from the CSG2 usage calculation.  |
| <a href="#">meter include imap</a>             | Specifies which Internet Message Access Protocol (IMAP) bytes are billed for by the CSG2 when doing prepaid debits.   |
| <a href="#">meter initial</a>                  | Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing. |
| <a href="#">meter minimum</a>                  | Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing. |



# meter initial

To specify the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing, use the **meter initial** command in CSG2 service configuration mode. To restore the default behavior, use the **no** form of the command.

**meter initial** *value*

**no meter initial** *value*

## Syntax Description

|              |  |
|--------------|--|
| <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 CSG2 grants the first network access for a session that has been mapped to the service. The initial value is not rounded up to the nearest increment value.<br><br>The range is from 0 to 65535. The default value is 0. |
|--------------|--|

## Defaults

The default quota is 0 quadrans.

## Command Modes

CSG2 service configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.<br><br>Changes from CSG1: None. |

## Usage Guidelines

This command allows “connection setup charges” to be applied to a service.

The debit occurs when the CSG2 grants the first access for the service. The initial value is not rounded up to the nearest increment value.

## Examples

The following example shows how to configure an initial quota debit for the OFF\_NET service.

```
ip csg service OFF_NET
meter initial 60
```

## Related Commands

| Command                                   | Description  |
|---|--|
| <a href="#">ip csg service</a>            | Configures a CSG2 content billing service, and enters CSG2 service configuration mode.                         |
| <a href="#">meter exclude control sip</a> | Excludes call control packets for a Session Initiation Protocol (SIP) session from the CSG2 usage calculation. |

| Command                               | Description   |
|---------------------------------------|---|
| <b>meter exclude mms wap</b>          | Excludes bytes for a WAP 1.x Multimedia Messaging Service (MMS) session from the CSG2 usage calculation.  |
| <b>meter exclude network-init sip</b> | Excludes incoming Session Initiation Protocol (SIP) transactions (that is, those that are initiated from the network) from the CSG2 usage calculation.      |
| <b>meter exclude pause rtsp</b>       | Excludes the Real Time Streaming Protocol (RTSP) PAUSE time from the CSG2 usage calculation.  |
| <b>meter exclude svc-idle</b>         | Excludes the final service idle from the CSG2 usage calculation.  |
| <b>meter include imap</b>             | Specifies which Internet Message Access Protocol (IMAP) bytes are billed for by the CSG2 when doing prepaid debits.   |
| <b>meter increment</b>                | Specifies the increments for debiting quota by the CSG2 upon completion of a service configured for Service Duration Billing.                               |
| <b>meter minimum</b>                  | Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing. |

# meter minimum

To specify the minimum number of quadrans debited by the CSG2 for a service or session, use the **meter minimum** command in CSG2 service configuration mode. To return to the default behavior, use the **no** form of the command.

**meter minimum** *value*

**no meter minimum** *value*

## Syntax Description

*value*

Minimum number of quadrans debited for a service or session, excluding the value in **meter initial**. For example, to force the CSG2 to debit 90 quadrans when less than 90 quadrans of network usage were used for the service, specify **meter minimum 90**. If the initial value is 20 quadrans and the minimum is 90 quadrans, then the minimum total charge is 110 quadrans. The minimum value is applied only if at least 1 session is granted network access for the service.

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

## Defaults

The default number is 0 quadrans.

## Command Modes

CSG2 service configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: None. |

## Usage Guidelines

If **meter initial** is set to 20 quadrans, and **meter minimum** is set to 90 quadrans, then the minimum total charge is 110 quadrans.

If service duration is configured in the **basis** command, the usage is rounded up to the minimum value when the Service Stop is sent. For a minimum value of 90, 150 seconds of network usage is not rounded up for the purpose of calculating usage in the Service Stop, but, for example, 63 seconds of network usage is rounded up to 90 quadrans.



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

**Examples**

The following example shows how to configure a minimum debit for the OFF\_NET service.

```
ip csg service OFF_NET
meter minimum 60
```

**Related Commands**

| Command  | Description   |
|--|---|
| <a href="#">ip csg service</a>                 | Configures a CSG2 content billing service, and enters CSG2 service configuration mode.  |
| <a href="#">meter exclude control sip</a>      | Excludes call control packets for a Session Initiation Protocol (SIP) session from the CSG2 usage calculation.  |
| <a href="#">meter exclude mms wap</a>          | Excludes bytes for a WAP 1.x Multimedia Messaging Service (MMS) session from the CSG2 usage calculation.  |
| <a href="#">meter exclude network-init sip</a> | Excludes incoming Session Initiation Protocol (SIP) transactions (that is, those that are initiated from the network) from the CSG2 usage calculation.      |
| <a href="#">meter exclude pause rtsp</a>       | Excludes the Real Time Streaming Protocol (RTSP) PAUSE time from the CSG2 usage calculation.  |
| <a href="#">meter exclude svc-idle</a>         | Excludes the final service idle from the CSG2 usage calculation.  |
| <a href="#">meter include imap</a>             | Specifies which Internet Message Access Protocol (IMAP) bytes are billed for by the CSG2 when doing prepaid debits.   |
| <a href="#">meter increment</a>                | Specifies the increments for debiting quota by the CSG2 upon completion of a service configured for Service Duration Billing.                               |
| <a href="#">meter initial</a>                  | Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing. |

# mode

To specify the mode for a CSG2 billing plan, use the **mode** command in CSG2 billing configuration mode. To use the default mode, use the **no** form of this command.

**mode** [**postpaid** | **prepaid**]

**no mode**

| Syntax Description |   |
|--------------------|---|
| <b>postpaid</b>    | (Optional) Specifies a postpaid billing plan.                             |
| <b>prepaid</b>     | (Optional) Specifies a prepaid billing plan. This is the default setting. |

**Defaults** The default mode is **prepaid**.

**Command Modes** CSG2 billing configuration

| Command History | Release    | Modification   |
|-----------------|------------|--|
|                 | 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: None. |

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

**Examples** The following example specifies postpaid mode for CSG2 billing plan REGULAR

```
ip csg billing REGULAR
mode postpaid
```

| Related Commands | Command                                      | Description  |
|------------------|--|--|
|                  | <a href="#">class</a>                        | Specifies a service class value.   |
|                  | <a href="#">entries user idle</a>            | Sets the time after which entries for idle subscribers are deleted from the CSG2 User Table. |
|                  | <a href="#">ip csg billing</a>               | Defines a CSG2 billing plan, and enters CSG2 billing configuration mode.                     |
|                  | <a href="#">ip csg transport-type assign</a> | Classifies data traffic on the basis of its access path.                                     |
|                  | <a href="#">owner</a>                        | Specifies an identifier or name for a service owner.   |
|                  | <a href="#">ip csg records format</a>        | Specifies <b>variable</b> or <b>fixed</b> call detail record (CDR) format.                   |
|                  | <a href="#">service</a>                      | Associates a service with a CSG2 billing plan.   |

# mode tcp

To specify the mode for CSG2 TCP sessions, use the **mode tcp** command in CSG2 content configuration mode. To use the default mode, use the **no** form of this command.

**mode tcp {datagram | transparent [zero]}**

**no mode tcp**

## Syntax Description

|                    |  |
|--------------------|--|
| <b>datagram</b>    | Specifies that the CSG2 is to treat TCP sessions as datagrams.                           |
| <b>transparent</b> | Specifies that the CSG2 is to treat TCP sessions as transparent.                         |
| <b>zero</b>        | (Optional) Specifies that TCP bytes are not to be reported for transparent TCP sessions. |

## Defaults

If you do not configure this command, the CSG2 treats TCP sessions as transparent, forwarding all TCP packets, including out-of-order packets, and reporting all new and retransmitted TCP payload bytes.

## Command Modes

CSG2 content configuration

## Command History

| Release     | Modification                 |
|-------------|------------------------------|
| 12.4(11)MD6 | This command was introduced. |

## Usage Guidelines

The **mode tcp** command is valid only if the **parse protocol other** command is also specified for the content.

If you configure the **mode tcp transparent** command, the CSG2 forwards all TCP packets, including out-of-order packets, and reports all new and retransmitted TCP payload bytes. If you also configure the optional **zero** keyword, the CSG2 reports zero TCP bytes. The CSG2 uses TCP signals to establish and terminate the TCP sessions.

If you configure the **mode tcp datagram** command, the CSG2 forwards all TCP packets, including out-of-order packets, and reports zero TCP payload bytes. Each TCP session is established by the first SYN, and terminated by the content's idle timer.

## Examples

The following example specifies transparent mode for TCP sessions for CSG2 content VPN:

```
ip csg content VPN
ip any tcp 10000
mode tcp transparent
```

## Related Commands

| Command                        | Description   |
|--------------------------------|---|
| <a href="#">ip csg content</a> | Configures content for CSG2 services, and enters CSG2 content configuration mode. |

## name (iSCSI)

To specify the name of an iSCSI target in the target profile on the CSG2, use the **name** command in iSCSI configuration mode. To remove the IP address configuration, use the **no** form of the command.

**name** *target-name*

**no name** *target-name*

| Syntax Description | <i>target-name</i> | Name of the iSCSI target. |
|--------------------|--------------------|---------------------------|
|--------------------|--------------------|---------------------------|

| Command Default | No default behavior or values. |
|-----------------|--------------------------------|
|-----------------|--------------------------------|

| Command Modes | iSCSI configuration |
|---------------|---------------------|
|---------------|---------------------|

| Command History | Release    | Modification                 |
|-----------------|------------|------------------------------|
|                 | 12.4(15)MD | This command was introduced. |

**Examples** The following example configures an iSCSI target interface profile with the name **targetA** to a SCSI target named **eftcompany.com**.

```
ip iscsi target-profile targetA
  name iqn.2002-10.edu.abc.io1.iscsi.draft20-target:1
  ip 10.0.0.1
  port 3260
```

| Related Commands | Command                                   | Description  |
|------------------|---|--|
|                  | <a href="#">ip (iSCSI)</a>                | Specifies the IP address of an iSCSI target in the target interface profile on the CSG2.   |
|                  | <a href="#">ip csg iscsi drain delay</a>  | Defines the delay interval, in seconds, before draining packets from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) when the Billing Mediation Agent (BMA) becomes active.      |
|                  | <a href="#">ip csg iscsi drain packet</a> | Defines the number of packets to be drained from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) per drain delay interval when the Billing Mediation Agent (BMA) becomes active. |
|                  | <a href="#">ip csg iscsi profile</a>      | Specifies the Internet Small Computer Systems Interface (iSCSI) target to be used as backup storage for the CSG2.  |

| Command                                 | Description  |
|---|--|
| <a href="#">ip iscsi target-profile</a> | Creates an iSCSI profile for an iSCSI target on the CSG2, and enters iSCSI configuration mode.                           |
| <a href="#">port (iSCSI)</a>            | Specifies the number of the port on which to listen for iSCSI traffic in the iSCSI target interface profile on the CSG2. |



# next-hop

To define a next-hop IP address, use the **next-hop** command in CSG2 content configuration mode. To delete the next-hop IP address, use the **no** form of this command.

```
next-hop ip-address [reverse] [subscriber media]
```

```
no next-hop ip-address [reverse] [subscriber media]
```

| Syntax Description |                         |   |
|--------------------|-------------------------|---|
|                    | <i>ip-address</i>       | IP address of the next hop for packets sourced by the flow initiator.   |
|                    | <b>reverse</b>          | (Optional) IP address of the next hop for packets sent to the flow initiator.   |
|                    | <b>subscriber media</b> | (Optional) IP address of the next hop for packets sent from the subscriber for Session Initiation Protocol (SIP) media. |

**Defaults** None

**Command Modes** CSG2 content configuration

| Command History | Release    | Modification   |
|-----------------|------------|--|
|                 | 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: <ul style="list-style-type: none"> <li>The configuration mode for this command changed from CSG policy configuration to CSG2 content configuration.</li> <li>The <b>reverse</b> keyword was added.</li> </ul> |
|                 | 12.4(15)MD | The <b>subscriber media</b> keywords were added.   |

**Usage Guidelines** You can configure one forward next-hop, and one reverse next-hop.



**Note**

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

The **subscriber media** option affects only SIP media sessions (used for subscriber-to-subscriber traffic). If the **subscriber media** option is not configured, SIP media sessions use the values defined for **next-hop** or **next-hop reverse**.

**Examples** The following example specifies next-hop for CSG2 content MOVIES:

```
ip csg content MOVIES
next-hop 1.2.3.4
next-hop 9.8.7.6 reverse
Next-hop 2.3.4.5 subscriber media
```

| Related Commands | Command                                     | Description   |
|------------------|---|---|
|                  | <a href="#">client-group (CSG2 content)</a> | References a standard access list that is part of a CSG2 content.                 |
|                  | <a href="#">ip csg content</a>              | Configures content for CSG2 services, and enters CSG2 content configuration mode. |

# owner

To specify an identifier or name for a CSG2 service owner, use the **owner** command in CSG2 service configuration mode. To remove the owner ID or name, use the **no** form of this command.

```
owner {id id | name name}
```

```
no owner {id | name}
```

| Syntax Description | id <i>id</i>     | 1- to 15-character string that identifies a service owner.        |
|--------------------|------------------|---|
|                    | name <i>name</i> | 1- to 38-character string that specifies the name of the service. |

| Defaults | None |
|----------|------|
|----------|------|

| Command Modes | CSG2 service configuration |
|---------------|----------------------------|
|---------------|----------------------------|

| Command History | Release    | Modification   |
|-----------------|------------|--|
|                 | 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: This command incorporated the following CSG1 commands: <ul style="list-style-type: none"> <li>• <b>owner id</b></li> <li>• <b>owner name</b></li> </ul> |

| Usage Guidelines | Use this command with fixed-record format to identify a service owner. |
|------------------|--|
|------------------|--|

| Examples | The following example specifies an owner ID for the CSG2 service A1: |
|----------|--|
|----------|--|

```
ip csg service A1
  owner id ABC123456
```

| Related Commands | Command                                      | Description  |
|------------------|--|--|
|                  | <a href="#">class</a>                        | Specifies a service class value.   |
|                  | <a href="#">ip csg service</a>               | Configures a CSG2 content billing service, and enters CSG2 service configuration mode. |
|                  | <a href="#">ip csg transport-type assign</a> | Classifies data traffic on the basis of its access path.                               |
|                  | <a href="#">mode</a>                         | Specifies the mode for a CSG2 billing plan.  |
|                  | <a href="#">ip csg records format</a>        | Specifies variable or fixed CDR format.  |

# parse length

To define the maximum number of Layer 7 bytes that the CSG2 is to parse when attempting to assign a policy, use the **parse length** command in CSG2 content configuration mode. To restore the default setting, use the **no** form of this command.

**parse length** *number*

**no parse length**

|                           |               |  |
|---------------------------|---------------|--|
| <b>Syntax Description</b> | <i>number</i> | Maximum number of Layer 7 bytes to parse. The range is from 1 to 65535. The default value is 4000. |
|---------------------------|---------------|--|

**Defaults** The CSG2 parses up to 4000 Layer 7 bytes when attempting to assign a policy.

**Command Modes** CSG2 content configuration

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|------------------------|----------------|------------------------------|
|                        | 12.4(11)MD     | This command was introduced. |

**Usage Guidelines** If the parse length is exceeded, the CSG2 blocks or forwards packets on the basis of the **block** command. This command is valid only if **parse protocol http** is also configured.

**Examples** The following example specifies that the CSG2 is to parse up to 1234 Layer 7 bytes when attempting to assign a policy:

```
ip csg content MOVIES
  parse protocol http
  parse length 1234
```

| <b>Related Commands</b> | <b>Command</b>                 | <b>Description</b>  |
|-------------------------|--------------------------------|---|
|                         | <a href="#">block</a>          | Forces the CSG2 to drop packets that do not match a configured billing policy.    |
|                         | <a href="#">ip csg content</a> | Configures content for CSG2 services, and enters CSG2 content configuration mode. |
|                         | <a href="#">parse protocol</a> | Defines how the CSG2 is to parse traffic for a content.                           |

# parse protocol

To define how the CSG2 is to parse traffic for a content, use the **parse protocol** command in CSG2 content configuration mode. To restore the default setting, use the **no** form of this command.

```
parse protocol {ftp | http | imap | other | pop3 | rtsp | sip | smtp | wap {connection-oriented |
connectionless}}
```

```
no parse protocol
```

## Syntax Description

|                            |   |
|----------------------------|---|
| <b>ftp</b>                 | FTP traffic, with Layer 7 inspection of FTP control sessions.   |
| <b>http</b>                | HTTP traffic.   |
| <b>imap</b>                | Internet Message Access Protocol (IMAP) traffic.  |
| <b>other</b>               | Some other type of IP traffic, such as IP, TCP, or User Datagram Protocol (UDP). This is the default setting. |
| <b>pop3</b>                | Post Office Protocol, version 3 (POP3) traffic.   |
| <b>rtsp</b>                | Real Time Streaming Protocol (RTSP) traffic.  |
| <b>sip</b>                 | Session Initiation Protocol (SIP) traffic.  |
| <b>smtp</b>                | Simple Mail Transfer Protocol (SMTP) traffic.   |
| <b>wap</b>                 | Wireless application protocol traffic.  |
| <b>connection-oriented</b> | Defines the WAP traffic as connection-oriented.   |
| <b>connectionless</b>      | Defines the WAP traffic as connectionless.  |

## Defaults

The CSG2 parses the traffic as some other type of IP traffic, such as IP, TCP, or User Datagram Protocol (UDP).

## Command Modes

CSG2 content configuration

## Command History

| Release    | Modification                                       |
|------------|--|
| 12.4(11)MD | This command was introduced.                       |
| 12.4(15)MD | The <b>ftp</b> and <b>sip</b> keywords were added. |

## Examples

The following example specifies that the CSG2 is to parse traffic for this content as HTTP traffic:

```
ip csg content MOVIES
  parse protocol http
```

| Related Commands | Command   | Description   |
|------------------|---|---|
|                  | <a href="#">ip csg content</a>                          | Configures content for CSG2 services, and enters CSG2 content configuration mode.                         |
|                  | <a href="#">parse length</a>                            | Defines the maximum number of Layer 7 bytes that the CSG2 is to parse when attempting to assign a policy. |
|                  | <a href="#">subscriber-ip http-header forwarded-for</a> | Specifies that the CSG2 is to obtain the subscriber's IP address from the HTTP X-Forwarded-For header.    |

# passthrough

To enable passthrough mode for a CSG2 service, use the **passthrough** command in CSG2 service configuration mode. To disable passthrough mode, use the **no** form of this command.

**passthrough** *quota-grant*

**no passthrough**

|                           |   |  |
|---------------------------|---|--|
| <b>Syntax Description</b> | <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. |
| <b>Defaults</b>           | None  |  |
| <b>Command Modes</b>      | CSG2 service configuration  |  |
| <b>Command History</b>    | <b>Release</b>  | <b>Modification</b>  |
|                           | 12.4(11)MD  | This command was migrated from CSG1.<br>Changes from CSG1: None.   |
| <b>Usage Guidelines</b>   | Use this command to enable the CSG2 to grant quota to the service when at least one quota server is configured, but none are active.  |  |
| <b>Examples</b>           | <p>The following example specifies that the CSG2 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> |  |
| <b>Related Commands</b>   | <b>Command</b>  | <b>Description</b>   |
|                           | <a href="#">ip csg service</a>  | Configures a CSG2 content billing service, and enters CSG2 service configuration mode.   |

# pending

To set the pending connection timeout, use the **pending** command in CSG2 content configuration mode. To restore the default, use the no form of this command.

**pending** *timeout*

**no pending**

## Syntax Description

|                |   |
|----------------|---|
| <i>timeout</i> | Time, in seconds, to wait for a response to an initial synchronization sequence number (SYN) on a TCP session. The range is from 4 to 65535. The default value is 30. |
|----------------|---|

## Defaults

The default pending connection timeout is 30 seconds.

## Command Modes

CSG2 content configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: None. |

## Examples

This example shows how to set the pending connection timer for a CSG2 content:

```
ip csg content MOVIES_COMEDY
pending 300
```

## Related Commands

| Command                             | Description  |
|-------------------------------------|--|
| <a href="#">idle (CSG2 content)</a> | Specifies the minimum amount of time that the CSG2 maintains an idle content connection. |
| <a href="#">ip csg content</a>      | Configures content for CSG2 services, and enters CSG2 content configuration mode.        |
| <a href="#">show ip csg</a>         | Displays information about the CSG2.   |



## policy (CSG2 content)

To reference a CSG2 billing policy, use the **policy** command in CSG2 content configuration mode. To delete a policy reference, use the **no** form of this command.

**policy** *policy-name* [**priority** *priority-number*]

**no policy** *policy-name*

### Syntax Description

|  |   |
|--|---|
| <i>policy-name</i>                     | Name of a configured CSG2 billing policy.   |
| <b>priority</b> <i>priority-number</i> | (Optional) Priority of the policy.<br><br>The priority specifies the order of preference of the policy. A lower number indicates a higher priority. If the current policy becomes unusable, the CSG2 uses the highest priority policy (that is, the policy with the lowest priority number) available.<br><br>In the same content, all policies must have different priorities.<br><br>Priorities for different policies do not have to be sequential. That is, you can have three policies with priorities 1, 5, and 10.<br><br>The range of priorities is 1 to 511. |

### Defaults

No policy is configured.  
If you do not specify a priority for the policy, no priority is configured. The CSG2 lists and prioritizes the policy sequentially, in the order in which it was configured.

### Command Modes

CSG2 content configuration

### Command History

| Release    | Modification  |
|------------|---|
| 12.4(11)MD | This command was migrated from CSG1.<br><br>Changes from CSG1: None.            |
| 12.4(15)MD | The <b>priority</b> keyword and the <i>priority-number</i> argument were added. |

### Usage Guidelines

If accounting records are to be generated for flows matching this policy, you must configure the **accounting** command in CSG2 policy configuration mode. If you do not want to bill for flows matching this policy, do not configure the **accounting** command.

To reference more than one policy in a content configuration, use multiple **policy** commands.

All policies in a given content configuration must be configured the same way, either all with priorities, or all without priorities. Policies in the same content configuration must have different priorities.

**Examples**

The following example shows how to reference policies with and without priorities:

```
ip csg content MOVIES
  policy COMEDY
  policy HORROR

ip csg content MUSIC
  policy HIPHOP priority 1
  policy COUNTRY priority 10000
```

**Related Commands**

| Command                        | Description  |
|--------------------------------|--|
| <a href="#">ip csg content</a> | Configures content for CSG2 services, and enters CSG2 content configuration mode.                                  |
| <a href="#">ip csg policy</a>  | Defines a policy for qualifying flows for the CSG2 accounting services, and enters CSG2 policy configuration mode. |
| <a href="#">show ip csg</a>    | Displays information about the CSG2.   |

# port (iSCSI)

To specify the number of the port on which to listen for iSCSI traffic in the iSCSI target interface profile on the CSG2, use the **port** command in iSCSI configuration mode. To remove the port number, use the **no** form of the command.

**port** *port-number*

**no port** *port-number*

## Syntax Description

|                    |   |
|--------------------|---|
| <i>port-number</i> | Number of the port on which to listen for iSCSI traffic. We recommend that you use port 3260. |
|--------------------|---|

## Command Default

No default behavior or values.

## Command Modes

iSCSI configuration

## Command History

| Release    | Modification                 |
|------------|------------------------------|
| 12.4(15)MD | This command was introduced. |

## Examples

The following example configures an iSCSI target interface profile with the name **targetA** to a iSCSI target with which the CSG2 will communicate using port number **3260**.

```
ip iscsi target-profile targetA
  name iqn.2002-10.edu.abc.io1.iscsi.draft20-target:1
  ip 10.0.0.1
  port 3260
```

## Related Commands

| Command                                   | Description  |
|---|--|
| <a href="#">ip (iSCSI)</a>                | Specifies the IP address of an iSCSI target in the target interface profile on the CSG2.   |
| <a href="#">ip csg iscsi drain delay</a>  | Defines the delay interval, in seconds, before draining packets from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) when the Billing Mediation Agent (BMA) becomes active.      |
| <a href="#">ip csg iscsi drain packet</a> | Defines the number of packets to be drained from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) per drain delay interval when the Billing Mediation Agent (BMA) becomes active. |
| <a href="#">ip csg iscsi profile</a>      | Specifies the Internet Small Computer Systems Interface (iSCSI) target to be used as backup storage for the CSG2.  |

| Command                                 | Description  |
|---|--|
| <a href="#">ip iscsi target-profile</a> | Creates an iSCSI profile for an iSCSI target on the CSG2, and enters iSCSI configuration mode. |
| <a href="#">name (iSCSI)</a>            | Specifies the name of an iSCSI target in the target profile on the CSG2                        |

# reauthorization threshold

To configure the CSG2 reauthorization threshold, use the **reauthorization threshold** command in CSG2 service configuration mode. To restore the default setting, use the **no** form of this command.

**reauthorization threshold** *threshold*

**no reauthorization threshold**

| Syntax Description | <i>threshold</i>   |
|--------------------|--|
|                    | Number of remaining quadrans or seconds to trigger reauthorization. <ul style="list-style-type: none"> <li>For fixed-cost billing (<b>basis fixed</b>) or volume-based billing (<b>basis byte</b>), the range (in quadrans) is from 0 to 10000000. The default is 10000000.</li> <li>For duration-based billing (<b>basis second</b>), the range (in seconds) is from 0 to 10000000. The default is 10.</li> </ul> |

| Defaults | For fixed-cost billing ( <b>basis fixed</b> ) or volume-based billing ( <b>basis byte</b> ), the default reauthorization threshold is 10000000 quadrans.<br>For duration-based billing ( <b>basis second</b> ), the default reauthorization threshold is 10 seconds. |
|----------|--|
|----------|--|

| Command Modes | CSG2 service configuration |
|---------------|----------------------------|
|---------------|----------------------------|

| Command History | Release    | Modification                 |
|-----------------|------------|------------------------------|
|                 | 12.4(11)MD | This command was introduced. |

| Usage Guidelines | <p>Setting the threshold to 0 means that reauthorization is triggered when there are no remaining quadrans or seconds. The quota server can override these settings.</p> <p>For services configured for fixed-cost billing (<b>basis fixed</b>), the reauthorization trigger is the smallest of the following values:</p> <ul style="list-style-type: none"> <li>The threshold configured using the <b>reauthorization threshold</b> command</li> <li>25% of the last quota grant returned from the quota server</li> </ul> <p>For services configured for volume-based billing (<b>basis byte</b>), the reauthorization trigger is the smallest of the following values:</p> <ul style="list-style-type: none"> <li>The threshold configured using the <b>reauthorization threshold</b> command</li> <li>25% of the last quota grant returned from the quota server</li> <li>32 KB</li> </ul> <p>For services configured for duration-based billing (<b>basis second</b>), the reauthorization trigger is the threshold configured using the <b>reauthorization threshold</b> command.</p> |
|------------------|---|
|------------------|---|

**reauthorization threshold****Examples**

The following example shows how to specify a reauthorization threshold of 75 quadrans:

```
ip csg service A1
 reauthorization threshold 75
```

**Related Commands**

| Command                                 | Description  |
|---|--|
| <a href="#">ip csg service</a>          | Configures a CSG2 content billing service, and enters CSG2 service configuration mode. |
| <a href="#">reauthorization timeout</a> | Specifies the CSG2 reauthorization timeout.  |

# reauthorization timeout

To specify the CSG2 reauthorization timeout, use the **reauthorization timeout** command in CSG2 service configuration mode. To restore the default setting, use the **no** form of this command.

**reauthorization timeout** [**initial** *initial-timeout*] [**maximum** *maximum-timeout*]

**no reauthorization timeout**

| Syntax Description | initial <i>initial-timeout</i> | (Optional) Initial timeout, in seconds, for reauthorization after a quota grant of zero. The range is from 1 to 3600 seconds. The default is 4.  |
|--------------------|--------------------------------|--|
|                    |                                | The value specified for must be less than or equal to the value specified for <b>maximum</b> maximum-timeout.                                    |
|                    | maximum <i>maximum-timeout</i> | (Optional) Maximum timeout, in seconds, for reauthorization after a quota grant of zero. The range is from 1 to 3600 seconds. The default is 60. |

## Defaults

The default initial reauthorization timeout is 4 seconds.  
The default maximum reauthorization timeout is 60 seconds.

## Command Modes

CSG2 service configuration

## Command History

| Release    | Modification                 |
|------------|------------------------------|
| 12.4(11)MD | This command was introduced. |

## Usage Guidelines

The quota server can override these settings.

For every quota grant of zero, the reauthorization time doubles, until the maximum timeout is reached. For example, if the initial timeout is set to 30 seconds, and the maximum timeout is set to 250 seconds, the reauthorization times (assuming quota grants of zero) would be:

- 30 seconds
- 60 seconds
- 120 seconds
- 240 seconds
- 250 seconds
- 250 seconds

And so on.

**Examples**

The following example shows how to specify an initial reauthorization timeout of 10 seconds and a maximum reauthorization timeout of 20 seconds:

```
ip csg service A1
  reauthorization timeout initial 10 maximum 20
```

**Related Commands**

| Command                                   | Description  |
|---|--|
| <a href="#">ip csg service</a>            | Configures a CSG2 content billing service, and enters CSG2 service configuration mode. |
| <a href="#">reauthorization threshold</a> | Specifies the CSG2 reauthorization threshold.  |



# records delay

To specify the delay before the CSG2 is to send the HTTP Statistics CDR, use the **records delay** command in CSG2 content configuration mode. To restore the default setting, use the **no** form of this command.

**records delay** *seconds*

**no records delay**

| <b>Syntax Description</b>      | <i>seconds</i>   | Time, in seconds, that the CSG2 is to delay before sending the HTTP statistics CDR. The range is from 0 to 1234 seconds. The default is 0 (no records delay). |              |                                |   |  |
|--------------------------------|--|---|--------------|--------------------------------|---|--|
| <b>Defaults</b>                | The default value is 0 (no records delay).   |   |              |                                |   |  |
| <b>Command Modes</b>           | CSG2 content configuration   |   |              |                                |   |  |
| <b>Command History</b>         | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.4(11)MD</td> <td>This command was introduced.</td> </tr> </tbody> </table>   | Release   | Modification | 12.4(11)MD                     | This command was introduced.  |  |
| Release                        | Modification   |   |              |                                |   |  |
| 12.4(11)MD                     | This command was introduced.   |   |              |                                |   |  |
| <b>Usage Guidelines</b>        | Specifying a records delay enables CSG2 accounting for retransmitted packets and ACKs after the transaction closes, but before the connection closes.  |   |              |                                |   |  |
| <b>Examples</b>                | <p>The following example shows how to specify a records delay of 5 seconds:</p> <pre>ip csg content MOVIES  records delay 5</pre>  |   |              |                                |   |  |
| <b>Related Commands</b>        | <table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><a href="#">ip csg content</a></td> <td>Configures content for CSG2 services, and enters CSG2 content configuration mode.</td> </tr> </tbody> </table> | Command   | Description  | <a href="#">ip csg content</a> | Configures content for CSG2 services, and enters CSG2 content configuration mode. |  |
| Command                        | Description  |   |              |                                |   |  |
| <a href="#">ip csg content</a> | Configures content for CSG2 services, and enters CSG2 content configuration mode.  |   |              |                                |   |  |

## records granularity

To specify the granularity at which CSG2 billing call detail records (CDRs) are to be generated, use the **records granularity** command in CSG2 service configuration mode. To restore the default granularity, use the **no** form of this command.

```
records granularity { transaction | service { bytes bytes | seconds seconds | bytes bytes
seconds seconds } }
```

```
no records granularity
```

| Syntax Description            |  |
|-------------------------------|--|
| <b>transaction</b>            | Generate CDRs for each transaction. This is the default setting.   |
| <b>service</b>                | Generate summarized, service-level CDRs.   |
| <b>bytes</b> <i>bytes</i>     | Number of bytes of data, sent and received by a session, that triggers a CDR.<br><br>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.<br><br>The range is from 5000 to 2147483647. The default value, if the <b>bytes</b> keyword is not specified, is 0, indicating no maximum.      |
| <b>seconds</b> <i>seconds</i> | Maximum time, in seconds, between billing records for a session. Records can be sent more frequently if the number of bytes is reached.<br><br>When a record is sent because the maximum time has been reached, the byte counts reported in the record are approximate.<br><br>The range is from 5 to 86400. The default value, if the <b>time</b> keyword is not specified, is 0, indicating no time limit. |

### Defaults

If you do not specify the **records granularity** command, CDRs are generated for each transaction.

If you specify **records granularity service**, you must also specify the **bytes** keyword, the **seconds** keyword, or both:

- If you specify both the **bytes** keyword and the **seconds** keyword, a billing record is sent when either limit is reached. Then both limits are reset.
- If you specify only the **bytes** keyword and not the **seconds** keyword, the maximum time between billing records for a session is set to 0 seconds, indicating no time limit.
- If you specify only the **seconds** 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

CSG2 service configuration

| Command History | Release    | Modification   |
|-----------------|------------|--|
|                 | 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: <ul style="list-style-type: none"> <li>The <b>time</b> keyword changed to <b>seconds</b>.</li> <li>The range for the <i>seconds</i> argument changed from 60 to 4294967295, to 5 to 86400.</li> </ul> |

### Usage Guidelines

You can use this command to reduce the number of records for services for which transaction-level billing is not required. For example, if a subscriber is accessing the Internet, and the data is to be billed based only on volume, then generating records for each HTTP transaction is of little use. With service-level CDR summarization enabled, the CSG2 generates only consolidated records that contain service-level usage.

To enable service-level CDR summarization in postpaid mode, you must specify that the associated billing plan is postpaid by using the **mode postpaid** command in CSG2 billing configuration mode.

Service-level CDRs are generated only for subscribers with entries in the CSG2 User Table entry. If a subscriber does not have an entry in the User Table, the CSG2 generates transaction-level CDRs.

### Examples

The following example shows how to specify a service granularity in both IP bytes and seconds:

```
ip csg service A1
  records granularity service byte 10000 seconds 120
```

### Related Commands

| Command                        | Description  |
|--------------------------------|--|
| <a href="#">ip csg service</a> | Configures a CSG2 content billing service, and enters CSG2 service configuration mode. |

# records intermediate

To enable the generation of CSG2 intermediate billing records, use the **records intermediate** command in CSG2 content configuration mode. To disable the generation of intermediate billing records, use the **no** form of this command.

**records intermediate** { **bytes** *bytes* | **seconds** *seconds* | **bytes** *bytes* **seconds** *seconds* }

**no records intermediate** { **bytes** *bytes* | **seconds** *seconds* | **bytes** *bytes* **seconds** *seconds* }

## Syntax Description

|                               |  |
|-------------------------------|--|
| <b>bytes</b> <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> <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. The default value, if the <b>bytes</b> keyword is not specified, is 0, indicating that the number of bytes sent and received will not trigger an intermediate record.</p> |
| <b>seconds</b> <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 86400. The default value, if the <b>seconds</b> keyword is not specified, is 0, indicating no time limit.</p>   |

## Defaults

If you do not specify the **records intermediate** command, or if you specify the **records intermediate** command for a content for a protocol handler that does not support intermediate statistics, intermediate billing records are not generated.

If you specify the **bytes** keyword but not the **seconds** keyword, the maximum time between billing records for a session is set to 0 seconds, indicating no time limit.

If you specify the **seconds** keyword but not the **bytes** keyword, the number of bytes of data that triggers the sending of an intermediate billing record is set to 0 bytes, indicating no maximum.

If you specify both the **bytes** keyword and the **seconds** keyword, a billing record is sent when either limit is reached. Then both limits are reset.

## Command Modes

CSG2 content configuration

| Command History | Release    | Modification  |
|-----------------|------------|---|
|                 | 12.4(11)MD | <p>This command was migrated from CSG1.</p> <p>Changes from CSG1:</p> <ul style="list-style-type: none"> <li>• The configuration mode for this command changed from CSG accounting configuration to CSG2 content configuration.</li> <li>• The <b>time</b> keyword changed to <b>seconds</b>.</li> <li>• The range for the <i>seconds</i> argument changed from 5 to 65535, to 5 to 86400.</li> </ul> |

### Usage Guidelines

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

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

The CSG2 does not support intermediate billing for RTSP control sessions unless the video/audio traffic is also transported over the control session.

### Examples

The following example shows how to enable intermediate billing records for the CSG2 content MOVIES. In this example, intermediate records are generated after 100,000 IP bytes of data are sent and received, or after 3600 seconds (1 hour) elapse, whichever occurs first:

```
ip csg content MOVIES
 records intermediate bytes 100000 seconds 3600
```

### Related Commands

| Command                        | Description   |
|--------------------------------|---|
| <a href="#">ip csg content</a> | Configures content for CSG2 services, and enters CSG2 content configuration mode. |

# refund

To specify the refund policy for a CSG2 prepaid service, use the **refund** command in CSG2 service configuration mode. To disable the refund policy, use the **no** form of this command.

**refund** *policy-name*

**no refund** *policy-name*

## Syntax Description

|                    |                            |
|--------------------|----------------------------|
| <i>policy-name</i> | Name of the refund policy. |
|--------------------|----------------------------|

## Defaults

Refunding is not enabled.

## Command Modes

CSG2 service configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.   |
|            | Changes from CSG1: The name of this command changed from <b>refund-policy</b> to <b>refund</b> . |

## Examples

The following example specifies refund policy COMPANY-REFUND:

```
ip csg service BILBYVOLUME
refund COMPANY-REFUND
```

## Related Commands

| Command                        | Description   |
|--------------------------------|---|
| <a href="#">ip csg refund</a>  | Specifies the CSG2 refund policy to apply to the various services, and enters CSG2 refund configuration mode. |
| <a href="#">ip csg service</a> | Configures a CSG2 content billing service, and enters CSG2 service configuration mode.                        |

# replicate

To replicate the connection state for all connections to the CSG2 content servers on the standby system, use the **replicate** command in CSG2 content configuration mode. To disable connection redundancy, use the **no** form of this command.

**replicate** [*delay seconds*]

**no replicate** [*delay*]

## Syntax Description

**delay seconds** (Optional) Number of seconds to delay state replication. The range is from 1 to 3600. The default value is no delay.

## Defaults

Connection redundancy is not enabled.  
If you do not specify a delay, there is no delay.

## Command Modes

CSG2 content configuration

## Command History

| Release    | Modification   |
|------------|--|
| 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: <ul style="list-style-type: none"> <li>The name of this command changed from <b>replicate connection tcp</b> to <b>replicate</b>.</li> <li>The <b>delay seconds</b> keyword and argument were added.</li> </ul> |

## Usage Guidelines

Replication is not supported for the wireless application protocol 1.x (WAP 1.x) and Real Time Streaming Protocol (RTSP) protocols. Therefore, the CSG2 generates an error message if either of the following situations occurs:

- You have already configured RTSP or WAP 1.x using the **parse protocol** command and you try to enter the **replicate** command.
- You have already configured **replicate** and you try to configure RTSP or WAP 1.x using the **parse protocol** command.

For HTTP, the replicated session is treated as Layer 4. No HTTP parsing is performed when the replicated session on the standby CSG2 becomes active.

## Examples

The following example shows how to enable replication for the CSG2 content MOVIES, and replication with a delay of 30 seconds for the CSG2 content GAMES:

```
ip csg content MOVIES
  replicate
ip csg content GAMES
  replicate delay 30
```

| Related Commands | Command                          | Description   |
|------------------|----------------------------------|---|
|                  | <a href="#">ip csg content</a>   | Configures content for CSG2 services, and enters CSG2 content configuration mode. |
|                  | <a href="#">ip csg replicate</a> | Enables state replication between redundant CSG2 systems.                         |



# retcode

To specify the range of application return codes for which the CSG2 refunds quota for Prepaid Error Reimbursement, use the **retcode** command in CSG2 refund configuration mode. To disable this feature, use the **no** form of this command.

```
retcode {ftp | http | imap | pop3 | sip | smtp | wap} rc-start [rc-end]
```

```
no retcode {ftp | http | imap | pop3 | sip | smtp | wap} rc-start [rc-end]
```

## Syntax Description

|                 |  |
|-----------------|--|
| <b>ftp</b>      | The CSG2 refunds quota for FTP application return codes.   |
| <b>http</b>     | The CSG2 refunds quota for HTTP and WAP 2.0 application return codes.<br><br><b>Note</b> The <b>http</b> keyword affects only HTTP and WAP 2.0. For WAP 1.x refunds, use the <b>wap</b> keyword.   |
| <b>imap</b>     | The CSG2 refunds quota for Internet Message Access Protocol (IMAP) application return codes.   |
| <b>pop3</b>     | The CSG2 refunds quota for Post Office Protocol, version 3 (POP3) application return codes.  |
| <b>sip</b>      | The CSG2 refunds quota for Session Initiation Protocol (SIP) application return codes.<br><br><b>Note</b> For SIP calls, only the return code to the INVITE method is used.<br><br>For SIP events, each event is a transaction associated with a single return code. |
| <b>smtp</b>     | The CSG2 refunds quota for Simple Mail Transfer Protocol (SMTP) application return codes.  |
| <b>wap</b>      | The CSG2 refunds quota for WAP 1.x application return codes.<br><br><b>Note</b> The <b>wap</b> keyword affects only WAP 1.x. For WAP 2.0 refunds, use the <b>http</b> keyword.   |
| <i>rc-start</i> | Specifies the beginning of the range of values for specific application return codes. The range is 1 to 65535 (0xffff).  |
| <i>rc-end</i>   | (Optional) Specifies the end of the range of values for specific application return codes. The range is 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

CSG2 refund configuration

| Command History | Release    | Modification   |
|-----------------|------------|--|
|                 | 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: None. |
|                 | 12.4(15)MD | The <b>ftp</b> and <b>sip</b> keywords were added.               |

### Usage Guidelines

The CSG2 supports return code-based refunding for all protocols except RTSP.

The return codes are protocol-specific.

For IMAP, keep in mind the following considerations:

- Only return code 554 is used. Return code 554 is used when a transaction ending in an IMAP tagged response was not flagged **OK**.
- The CSG2 does not support refunding for IMAP. If configured, refunding for IMAP has no effect.

### Examples

The following example shows how to **specify ranges of application return codes**:

```
ip csg refund COMPANY-REFUND
retcode http 500 509
retcode sip 300 999
retcode wap 0x44 0x50
```

### Related Commands

| Command                       | Description   |
|-------------------------------|---|
| <a href="#">flags</a>         | Specifies IP, TCP, or wireless application protocol (WAP) flag bit masks and values for CSG2 Prepaid Error Reimbursement. |
| <a href="#">ip csg refund</a> | Specifies the CSG2 refund policy to apply to the various services, and enters CSG2 refund configuration mode.             |

# sami rate all

To specify the bit rate limit to be used by the Service and Application Module for IP (SAMI) for each PowerPC's (PPC's) traffic, CSG2 use the **sami rate all** command in global configuration mode. Use the **no** form of this command to disable this feature.

**sami rate** *bits-per-second* **all**

**no sami rate** *bits-per-second* **all**

|                           |                        |   |
|---------------------------|------------------------|---|
| <b>Syntax Description</b> | <i>bits-per-second</i> | Number of bits per second that the SAMI rate-limiting code is to allow to be forwarded to an individual PPC. The range is 1 bps to 2 Gbps (0x80000000). The default value is 1.9 Gbps (0x70000000). |
|---------------------------|------------------------|---|

|                 |  |
|-----------------|--|
| <b>Defaults</b> | The default rate is 1.9 Gbps (0x70000000). |
|-----------------|--|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | Global configuration |
|----------------------|----------------------|

|                        |                |                              |
|------------------------|----------------|------------------------------|
| <b>Command History</b> | <b>Release</b> | <b>Modification</b>          |
|                        | 12.4(11)MD     | This command was introduced. |

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following example shows how to <b>specify a bit rate limit of 1 Gbps (0x40000000)</b> :<br><br><code>sami rate 0x40000000 all</code> |
|-----------------|--|

# service

To associate a service with a CSG2 billing plan, use the **service** command in CSG2 billing configuration mode. To remove the association, use the **no** form of this command.

**service** *service-name*

**no service** *service-name*

|                           |   |  |
|---------------------------|---|--|
| <b>Syntax Description</b> | <i>service-name</i>   | Name of a configured CSG2 billing service.   |
| <b>Defaults</b>           | None  |  |
| <b>Command Modes</b>      | CSG2 billing configuration  |  |
| <b>Command History</b>    | <b>Release</b>  | <b>Modification</b>  |
|                           | 12.4(11)MD  | This command was migrated from CSG1.<br>Changes from CSG1: None.                             |
| <b>Usage Guidelines</b>   | To associate more than one service with the same billing plan, use multiple <b>service</b> commands.  |  |
| <b>Examples</b>           | <p>The following example shows how to associate services MOVIES and BROWSING with billing plan REGULAR:</p> <pre>ip csg billing REGULAR   service MOVIES   service BROWSING</pre> |  |
| <b>Related Commands</b>   | <b>Command</b>  | <b>Description</b>   |
|                           | <a href="#">entries user idle</a>   | Sets the time after which entries for idle subscribers are deleted from the CSG2 User Table. |
|                           | <a href="#">ip csg billing</a>  | Defines a CSG2 billing plan, and enters CSG2 billing configuration mode.                     |
|                           | <a href="#">ip csg service</a>  | Configures a CSG2 content billing service, and enters CSG2 service configuration mode.       |
|                           | <a href="#">mode</a>  | Specifies the mode for a CSG2 billing plan.  |

# show ip csg

To display information about the CSG2, use the **show ip csg** command in privileged EXEC mode.

```
show ip csg { billing [plan billing-plan-name] | bma | content [name content-name]
[detail | internal] | database | gtp | iscsi | load [history] | psd | quota-server | radius |
sessions { database | gtp | imap | ipc | radius | replicate | user [application [internal]]
[ip-address ip-mask] } | stats | users { ip-address ip-mask | id user-name | all | sip [internal] }
[detail]
```

## Syntax Description

|                                      |  |
|--------------------------------------|--|
| <b>billing</b>                       | Displays information about billing plans.  |
| <b>plan</b> <i>billing-plan-name</i> | (Optional) Displays information about only the specified billing plan.   |
| <b>bma</b>                           | Displays information about the Billing Mediation Agents (BMAs) to which the CSG2 sends billing records. BMA statistics are reported for each BMA, in addition to an aggregate count for all BMAs.                    |
| <b>content</b>                       | Displays information about the CSG2 content table.   |
| <b>name</b> <i>content-name</i>      | (Optional) Displays information about only the specified content.  |
| <b>detail</b>                        | (Optional) Displays detailed information about the CSG2 content.   |
| <b>internal</b>                      | (Optional) Displays internal CSG2 data structure information for use in debugging.<br><br>We recommend that you enter this keyword only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. |
| <b>database</b>                      | Displays information about the server that answers CSG2 user ID queries.   |
| <b>gtp</b>                           | Displays information about the general packet radio service (GPRS) tunneling protocol (GTP).   |
| <b>iscsi</b>                         | Displays information about the Internet Small Computer Systems Interface (iSCSI).  |
| <b>load</b>                          | Displays information about load management.  |
| <b>history</b>                       | (Optional) Displays histograms of recent load management activity.   |
| <b>psd</b>                           | Displays information about the Cisco Persistent Storage Device (PSD) functionality residing on the CSG2.   |
| <b>quota-server</b>                  | Displays information about the quota servers.  |
| <b>radius</b>                        | Displays information about RADIUS.   |
| <b>sessions</b>                      | Displays information about sessions.   |
| <b>database</b>                      | Displays information about only the user database sessions.  |
| <b>gtp</b>                           | Displays information about only the GTP sessions.  |
| <b>imap</b>                          | Displays information about only the Internet Message Access Protocol (IMAP) sessions.  |
| <b>ipc</b>                           | Displays information about only the Interprocessor Communication (IPC) sessions.   |
| <b>other</b>                         | Displays information about all other Layer 3 and Layer 4 sessions.   |
| <b>pop3</b>                          | Displays information about only the Post Office Protocol, version 3 (POP3) sessions.   |
| <b>radius</b>                        | Displays information about only the RADIUS sessions.   |

|                           |  |
|---------------------------|--|
| <b>replicate</b>          | Displays information about only high availability (HA) sessions.   |
| <b>smtp</b>               | Displays information about only the Simple Mail Transfer Protocol (SMTP) sessions.   |
| <b>user</b>               | Displays information about only subscriber sessions.   |
| <i>application</i>        | (Optional) Displays information about only the specified application: <ul style="list-style-type: none"> <li>• <b>ftp</b>—Closes FTP subscriber sessions.</li> <li>• <b>http</b>—Closes HTTP subscriber sessions.</li> <li>• <b>imap</b>—Closes IMAP subscriber sessions.</li> <li>• <b>other</b>—Closes other subscriber sessions.</li> <li>• <b>pop3</b>—Closes POP3 subscriber sessions.</li> <li>• <b>rtsp</b>—Closes RTSP subscriber sessions.</li> <li>• <b>smtp</b>—Closes SMTP subscriber sessions.</li> <li>• <b>wap</b>—Closes WAP subscriber sessions.</li> </ul> |
| <b>internal</b>           | (Optional) Displays internal CSG2 data structure information for use in debugging.<br><br>We recommend that you enter this keyword only when directed to do so by Cisco Technical Assistance Center (TAC) engineers.   |
| <i>ip-address ip-mask</i> | (Optional) Displays information about only the specified subscriber IP address and subscriber IP address mask.<br><br>Specify IP address 0.0.0.0 to display information about all subscriber IP addresses.<br><br>Specify IP address mask 0 to display information about all subscriber IP address masks.  |
| <b>stats</b>              | Displays performance statistics for the CSG2.<br><br>You can also use the following commands to monitor CSG2 high availability (HA) configurations: <b>show redundancy state</b> , <b>show redundancy interdev</b> , and <b>show ipc sctp</b> .  |
| <b>users</b>              | Displays information about subscribers.<br><br><b>Note</b> If the <b>basis second connect</b> command is configured, the <b>balance</b> and <b>consumed</b> fields in the output of the <b>show ip csg users</b> command are updated only when there is a Service Reauthorization Request for new quota.   |
| <i>ip-address ip-mask</i> | Displays information about only the specified subscriber IP address and subscriber IP address mask.<br><br>Specify IP address 0.0.0.0 to display information about all subscriber IP addresses.<br><br>Specify IP address mask 0 to display information about all subscriber IP address masks.   |
| <b>id user-name</b>       | Displays information about the specified user ID.  |
| <b>all</b>                | Displays information about all subscribers.  |
| <b>sip</b>                | Displays information about the Session Initiation Protocol (SIP).  |

|                 |  |
|-----------------|--|
| <b>internal</b> | (Optional) Displays internal CSG2 data structure information for use in debugging.<br><br>We recommend that you enter this keyword only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. |
| <b>detail</b>   | (Optional) Displays more detailed information.   |

**Command Default** None

**Command Modes** Privileged EXEC

| Command History | Release    | Modification  |
|-----------------|------------|---|
|                 | 12.4(11)MD | This command was migrated from CSG1.<br><br>Changes from CSG1: This command incorporated the following CSG1 commands: <ul style="list-style-type: none"> <li>• <b>show ip csg accounting</b></li> <li>• <b>show module csg content</b></li> <li>• <b>show module csg stats</b></li> </ul> |
|                 | 12.4(15)MD | The <b>billing, ftp, gtp, history, iscsi, load, plan,</b> and <b>sip</b> keywords and <i>billing-plan-name</i> argument were added.   |

**Usage Guidelines** In the output for the **show ip csg content** command, the CSG2 might truncate some fields, such as the VRF name and the domain name.

Entering the **show ip csg users all** command might flood your screen with output.

**Examples** The following example shows how to display the statistics and counters for CSG2 content:

```
Router# show ip csg content
```

```

name                prot destination                vlan state
-----
ANY                 Any  0.0.0.0/0                    ALL  OUTFSERVICE
CONTENT             Any  0.0.0.0/0                    ALL  INSTALLED
CsgCg01             UDP  0.0.0.0/0:16000              ALL  INSTALLED
CsgCg11             UDP  0.0.0.0/0:16001              ALL  INSTALLED
CsgRadProxy1       UDP  10.18.28.34/32:0             ALL  INSTALLED
CsgRadProxy2       UDP  10.18.28.36/32:0             ALL  INSTALLED
CsgRadProxy3       UDP  10.18.28.37/32:0             ALL  INSTALLED
CsgRadProxy4       UDP  10.18.28.39/32:0             ALL  INSTALLED
CsgRadProxy5       UDP  10.18.28.254/32:0            ALL  INSTALLED
CsgRadProxy6       UDP  10.18.28.2/32:0              ALL  INSTALLED
CsgReplicate       UDP  10.18.28.8/32:6000           ALL  INSTALLED
CsgUDB             UDP  0.0.0.0/0:4444               ALL  INSTALLED
HTTP               TCP  0.0.0.0/0:80                 ALL  INSTALLED
HTTP82             TCP  0.0.0.0/0:82                 ALL  INSTALLED
RADIUS             UDP  11.18.28.16/32:1812          ALL  INSTALLED
RTSP               TCP  0.0.0.0/0:554                ALL  INSTALLED
SMTP               TCP  0.0.0.0/0:2025               ALL  INSTALLED

```

```
TCP          TCP 0.0.0.0/0:0          ALL INSTALLED
WAPCONN      UDP 0.0.0.0/0:9201         ALL INSTALLED
WAPCONNLESS  UDP 0.0.0.0/0:9200         ALL INSTALLED
```

The following example shows how to display detailed statistics and counters for the CSG2 HTTP content named **HTTP**:

```
Router# show ip csg content name HTTP detail
```

```
HTTP, parse type = http, state = INSTALLED, index = 13
destination = 0.0.0.0/0:80, protocol = TCP, vlan = ANY
idle = 10, pending = 30, replicate = Session, max parse len = 4000
total sessions = 48347288, current sessions = 153
regex memory usage = 98352
subscriber paks = 187932310, network paks = 261526365
```

| policy  | transactions |
|---------|--------------|
| -----   | -----        |
| FILE0K  | 0            |
| FILE16K | 0            |
| FILE1K  | 374104       |
| FILE4K  | 364817       |
| FILE8K  | 365168       |
| GIF     | 4462769      |
| JPEG    | 2982911      |
| HTML    | 13569080     |
| HTTP    | 8535         |
| (none)  | 0            |

The following example shows how to display the CSG2 statistics:

```
Router# show ip csg stats
```

```
CSG Replication Stats:
```

```
State: ACTIVE
Transmit: Packets = 1725627, current sequence = 268220
Received: Packets = 12014, current sequence = 12015, errors = 0
Last Bulk Sync Sent: 07:15:01 UTC Jun 6 2007
Bulk sync in progress on:
  Processor 5
  Processor 8
```

```
CSG Clear Stats:
```

```
counters = 0, kut = 0, sessions = 0
```

```
IPC PPC Stats:
```

```
init alloc fail = 0
message block alloc fail = 0
message block alloc denied = 0
correlator alloc fail = 0
message blocks currently allocated = 5020, max allocated = 5200
message blocks currently queued = 5020, max queued = 5200
message blocks currently tx queued = 5020, max tx queued = 5200
message blocks currently hashed = 3600, max hashed = 3663
dropped messages = 0, null msgs = 0
failure to respond = 0
acks = 11251929, timed out responses = 231567
interrupt acks = 1898906, process acks = 25, no ack = 0
sent to peer
  unreliable sends = 0, unreliable send failures = 0
  reliable sends = 436, reliable send failures = 0
  request sends = 1902531, request send failures = 0
```



```

    response sends = 11252888, response send failures = 0
received from peer
    unreliable = 51626, reliable = 97224994, request = 11254924, response =
1667364
    unsupported ipc port = 0, unsupported ipc request port = 0
    uncorrelated = 1138193
errors
    rtx list = 0, hash list = 0, dealloc = 0
    msg type = 0, ack miss = 0
-----
destination = 127.1.0.4:0, localport = 0
connection failures = 0
priority = 0, ACTIVE
packet rate = 351/sec, ack rate = 351/sec
data packets sent = 3086282, retransmits = 76, failed acks = 0
queued = 0, highwater = 586, tx win = 32
unacked = 0, ack = 138, count = 4

-----
destination = 127.1.0.5:0, localport = 0
connection failures = 0
priority = 0, ACTIVE
packet rate = 304/sec, ack rate = 23/sec
data packets sent = 1230533, retransmits = 523322, failed acks = 0
queued = 2490, highwater = 2669, tx win = 32
unacked = 32, ack = 5, count = 4

-----
destination = 127.1.0.6:0, localport = 0
connection failures = 0
priority = 0, ACTIVE
packet rate = 831/sec, ack rate = 831/sec
data packets sent = 5280267, retransmits = 114, failed acks = 0
queued = 0, highwater = 191, tx win = 32
unacked = 0, ack = 14, count = 1

-----
destination = 127.1.0.7:0, localport = 0
connection failures = 0
priority = 0, ACTIVE
packet rate = 191/sec, ack rate = 191/sec
data packets sent = 3339431, retransmits = 39339, failed acks = 0
queued = 0, highwater = 1649, tx win = 32
unacked = 0, ack = 105, count = 4

-----
destination = 127.1.0.8:0, localport = 0
connection failures = 0
priority = 0, ACTIVE
packet rate = 257/sec, ack rate = 0/sec
data packets sent = 1281140, retransmits = 506285, failed acks = 0
queued = 2530, highwater = 2716, tx win = 31
unacked = 31, ack = 4, count = 0

CSG Distributed Config Stats:
    poll msg sent = 16, online msg rcvd = 5, ack sent = 5
    ack not sent = 4, cmd distributed = 0, rollback = 0
    'no' cmd success = 0, 'no' cmd failure = 0

CSG Load Management Stats:
Radius Start
    Allowed (per second) = 367872 (21)
    IPC: Queue Depth Tolerance 24000 / 100000 (24 percent)
    Denied (per second) = 0 (0)
Database Request
    Allowed (per second) = 75197 (10)
    IPC: Queue Depth Tolerance 24000 / 100000 (24 percent)

```

```

    Denied (per second) = 5065121 (0)
    Rate: Limit 1800 per traffic processor
    Denied (per second) = 25193314 (0)
Session Create
    Allowed (per second) = 49802545 (1872)
    IPC: Queue Depth Tolerance 36000 / 100000 (36 percent)
    Denied (per second) = 21971 (6)
BMA Messages
    Allowed (per second) = 94475805 (11138)
    IPC: Queue Depth Tolerance 60000 / 100000 (60 percent)
    Denied (per second) = 0 (0)
Quota Server
    Allowed (per second) = 13725076 (837)
    IPC: Queue Depth Tolerance 60000 / 100000 (60 percent)
    Denied (per second) = 0 (0)

```

## CSG Buffer Management Stats:

| Category    | Create   | Copy    | Free     | Deny |
|-------------|----------|---------|----------|------|
| Radius      | 0        | 1858818 | 1854161  | 0    |
| Application | 0        | 9422790 | 9422649  | 0    |
| Fragments   | 161      | 1127    | 1288     | 0    |
| Unlimited   | 95979756 | 0       | 95979750 | 0    |

## CSG User Database Stats:

```
errors = 0
```

## CSG Session L4 Stats:

```

alloc fail ooo node = 0
alloc fail pak copy enqueue = 0
general errors = 0
FSM errors = 262
standby FSM errors = 0
count errors = 0
term idle = 838696
term short timer = 10179

```

## Network interface:

```

TCP packets = 266880460
TCP frags = 0
datagram packets = 4932124
datagram frags = 161
out of order      = 93841
out of order get  = 91870
out of order flushed = 1971
retransmitted = 94873
set aside        = 56824
set aside get    = 56412
set aside flushed = 412
term closed     = 1003483
term RST        = 10
term not SYN    = 259
term mid SYN    = 0
term error      = 0
dropped OOW    = 323808
dropped set aside = 292592
dropped queue size = 0
dropped error  = 259

```

## Subscriber interface

```

TCP packets = 192907977
TCP frags = 0
datagram packets = 13347893
datagram frags = 0

```

```

out of order          = 412
out of order get      = 384
out of order flushed = 28
retransmitted        = 485
set aside            = 9504977
set aside get        = 9418614
set aside flushed    = 86222
term closed          = 1362349
term RST             = 457991
term not SYN         = 0
term mid SYN         = 0
term error           = 0
dropped OOW          = 0
dropped set aside    = 692663
dropped queue size   = 0
dropped error        = 0

```

## CSG Fragment Stats:

```

creates = 161, destroys = 161, timeouts = 0,
invalids = 0, locked = 0
Leaders: rx = 161, tx = 161, dropped = 0, creates = 161
Trailers: rx = 966, tx = 966, dropped = 0, creates = 0
Reassemble: invalid = 0
alloc failures = 0, overlap = 0, missing leader = 0
failed tx = 0, requeues = 0, failed requeues = 0

```

## CSG Packet Stats:

```

packet rcv = 509381050, drop invalid = 0,
protocol drop = 26408409, no handler = 0, no handler options = 0,
drop no content = 3, drop no session = 31791002
local enqueue = 2187, local enqueue failed = 0
local enqueue copy = 18

```

## CSG Distributed KUT Stats:

```

requests = 75197, responses = 62442, resends = 23430
timeouts = 11652, idle timeouts = 0, corr mismatch = 0
corr missing = 0, unknown IP = 11652
unknown ha vrf = 0, tx fail ipc = 0
alloc failures:
  kut = 0, kut_delete_event = 0, rad attr = 0
  int_stats = 0, kut_svc = 0, svc_stats = 0
  tariff = 0, redir_info = 0, passthru_grant = 0
  refund = 0, txn_abort = 0, ipc = 0

```

## CSG Session Stats:

```

user sessions = 531, highwater = 169455, ha_overrun = 0
max limit = 0, wc fail = 0, no content = 0
appl fail = 30314998, denied = 1487001, ha no content = 0
ha no session = 17529
Resets : subscriber = 46196262, network = 15603410
Alloc failures : wc = 0, session = 0
  prof event = 0, resolve event = 0, pend quota = 0
  pend aoc = 0
Resolve : no sess = 1, event fail = 3042, enq fail = 0
dup quota = 0, dup aoc = 0, aoc fail = 79
sess lookup fail = 0

```

## CSG LogGen Stats:

```

alloc fail = 0, gtp reject = 405
Billing records: sent = 94591046, fail = 0
IPC: alloc fail = 0, sent = 94475805, fail = 0, rcv = 94591043

```

GTP Application: CSG ipc, Local Port: 0

```

alloc failures = 0, no standby on CG failure = 0
packets sent = 14217667, received = 122537872, failed acks = 0
packets dropped = 0, rejected = 0, retransmits = 1069136, no ip = 0
packets outstanding: current = 5022, highwater = 5200
bad records = 0, unknown CG = 0, CG failures = 0
send skipped = 0, records dropped during drain = 0
Charging Gateways: defined = 5, max active = 5
  127.1.0.4:00ACTIVE
  127.1.0.5:00ACTIVE
  127.1.0.6:00ACTIVE
  127.1.0.7:00ACTIVE
  127.1.0.8:00ACTIVE

GTP Application: CSG Billing Agent, Local Port: 16000
  alloc failures = 0, no standby on CG failure = 0
  packets sent = 8096890, received = 809759, failed acks = 0
  packets dropped = 0, rejected = 0, retransmits = 261, no ip = 0
  packets outstanding: current = 4, highwater = 3262
  bad records = 0, unknown CG = 0, CG failures = 0
  send skipped = 0, records dropped during drain = 0
  Charging Gateways: defined = 1, max active = 1
    10.18.28.10:33331ACTIVE

GTP Application: CSG Quota Server, Local Port: 16001
  alloc failures = 0, no standby on CG failure = 81
  packets sent = 4054366, received = 4054405, failed acks = 294
  packets dropped = 2245665, rejected = 405, retransmits = 49, no ip = 0
  packets outstanding: current = 9304, highwater = 10001
  bad records = 0, unknown CG = 0, CG failures = 81
  send skipped = 0, records dropped during drain = 0
  Charging Gateways: defined = 1, max active = 1
    10.18.28.10:33851ACTIVE

GTP Application: CSG PSD, Local Port: 0
  alloc failures = 0, no standby on CG failure = 0
  packets sent = 0, received = 0, failed acks = 0
  packets dropped = 0, rejected = 0, retransmits = 0, no ip = 0
  packets outstanding: current = 0, highwater = 0
  bad records = 0, unknown CG = 0, CG failures = 0
  send skipped = 0, records dropped during drain = 0
  Charging Gateways: defined = 0, max active = 1

CSG User Stats:
  max = 300000, current = 148916, highwater = 169990
  exceed-max = 0
  kut current = 148916, kut highwater = 169990
  sticky current = 0, sticky highwater = 318
  ipc tx fail = 0, ipc response timeouts = 231557
  alloc failures:
    aff = 0, pend event = 0, delete event = 0
    ipc = 0
  ha receive drops:
    no aff = 22, unknown vrf = 0, state = 0

CSG Radius Stats:
  starts = 1548210, stops = 2015870, other = 0
  client msg rcv = 0, client msg sent = 0
  incorrect authentication = 0
  alloc failures:
    billplan = 0, auth = 0, user info = 0
    nas info = 0, pod port = 0, pod info = 0
    proxy elem = 0, proxy port = 0
  proxy source port = 1037
  proxy errors:

```

```

invalid message size = 0, unable to find client = 0
unable to send to client = 0, unable to send to server = 0
unable to find proxy blk = 0
proxy CSG ip = 10.18.28.34,
server ip = 11.18.28.17
client->server = 386484, server->client = 385459
parse errors = 0, pkt not proxied = 0
proxy CSG ip = 10.18.28.36,
server ip = 11.18.28.18
client->server = 230290, server->client = 229610
parse errors = 0, pkt not proxied = 0
proxy CSG ip = 10.18.28.37,
server ip = 11.18.28.19
client->server = 304504, server->client = 303612
parse errors = 0, pkt not proxied = 0

proxy CSG ip = 10.18.28.39,
server ip = 11.18.28.20
client->server = 0, server->client = 0
parse errors = 0, pkt not proxied = 0
proxy CSG ip = 10.18.28.254,
server ip = 11.18.28.16
client->server = 0, server->client = 0
parse errors = 0, pkt not proxied = 0
endpoint CSG ip = 10.18.28.2
client->CSG = 2642802, CSG->client = 2640636
unable to send ACK = 0, parse errors = 0
no ack sent = 0, non-Acct-Req = 0

CSG QS Stats:
alloc fail:
req = 0, redir = 0, defer ack = 0, req token = 0
too frequent requests = 12129585, called on standby = 0
no defer ack data = 0, no cg affinity = 0
passthru = 7404738, response no kut svc = 969, no quota = 10034067
svc auth fail = 6, aoc-verify fail = 0
badly formatted message:
aoc verify response = 0, cont auth redir = 458607
usr auth rsp = 0, svc auth rsp = 0
svc verify resp = 0, quota return accept = 0
svc stop req = 0, quota return req = 0
user disconnect req = 0, quota push req = 0
invalid req = 0
QS requests received from QS:
request = 0, fail to send to tp = 0
QS responses received from QS:
response = 4053620, fail to send to tp = 0
no request = 0, missing request data = 0
IPC:
CP alloc fail = 0, sent = 11252881, fail = 0, rcv = 13790207
TP alloc fail = 0, sent = 13725076, fail = 0, rcv = 11186359
response no request = 0
user profile req = 862466, rsp = 181435
svc auth req = 2533171, re-auth req = 1151422, rsp = 1499012
quota return = 118566, quota return accept = 0
auth content req = 6528274, rsp = 1832535
svc verify req = 0, rsp = 0
svc stop = 2531177, fail to enqueue qm request process = 0
svc stop req = 0, user disconnect req = 0
quota return req = 0, quota push req = 0, rsp = 0
negative quota grant = 0

```

## CSG OTHER Stats:

```
total sessions = 40344, alloc fail = 0
aoc fail = 0, frags = 0, aborts = 6521, init fail = 2513
reports = 39937, standby no uid = 0, errors = 0
```

## CSG HTTP Stats:

```
sess = 18052044, txn = 22158257, set-aside resolved = 9367313
packets:
  sub new = 22418621, retx = 53, payload less = 164830871
  net new = 238215919, retx = 94709, payload less = 22597153
billing reports:
  header = 6075882, stats = 79933600
alloc failures = 0
downgrade:
  parse failures = 8460, status code = 0
  rsp > req = 0, 0.9 method = 3007
fin terminated = 342, https = 20967, x4 = 0
redirects = 450449, redirect failures = 1075
reset:
  error = 0, no user = 30295243, no quota = 10025299
  exceed max parse len = 0, no policy = 0
  auth drop = 5577073
svc verify = 0, aoc = 6480351
unassigned bytes updates:
  no txn = 59360, downgrade = 26308, leak = 16082230
billing not resolved on standby = 0
```

## CSG RTSP Stats:

```
Dyn Sess: add = 32386, fail = 32, delete = 32374, unused = 38
Allocs: sessions = 8131, ctl_conns = 10405, streams = 16226,
Timeouts: control = 10402, data = 31359, streams = 1
Misc: reuse = 0, reuse kills = 0, teardowns = 0
  suspend = 96, patches = 0, interleaved = 0, sess = 0
  http = 0, pauses = 0, no_policy = 0, mismatch = 0
  ip frags = 0, retransmits = 29, resegments = 0
  no user = 4030
Errors: alloc = 0, dups = 0, ddrops = 0, cdrops = 32
  patch = 0, parse = 0, aoc = 0, reject = 0
  misc = 0
Reports: tcp = 10402, udp = 32336, stream = 16172
```

## CSG Mail Stats:

```
SMTP: messages = 457898, packets = 8701512, reports = 457898
  fsm error = 0
POP3: messages = 0, packets = 0, reports = 0
  fsm error = 0
IMAP: header fetches = 0, body fetches = 0
  packets = 0, reports = 0, fsm error = 0
MAIL: ip frags = 0, aoc bypass = 0, alloc fails = 0
  error = 0, no user = 6754, no policy = 0
  txn drop = 0, aoc drop = 0
```

## CSG WAP Stats:

```
parses = 6026562, wap sessions = 978999, mms sessions = 0
connection oriented paks = 2629846, connectionless paks = 3396716
total trans = 2087358, incomplete trans = 2962
billing reports = 3755797, dup packets = 718748, redirects = 972
disconnects = 0, unknown packets = 98, concat packets = 0
parse err = 275, alloc fail = 0, refunds = 0
forced aborts = 19015, concat frags = 0, uid wait = 65571
seg att = 0, seg succ = 0, seg comp = 0, frags = 161
send fail = 0, send ok = 50279, no policy = 0
stateless = 732269, verifys = 0, cont fail = 0
user fail = 6458, err = 0, pre policy = 0
```

```
Aoc: reqs = 47923, drop = 14006, redir = 6778, fail = 0  
Drops: err = 0, quota = 14290, block = 0, queue = 2521
```

## Timer Stats:

```
tmr_intialized = 1  
tmr_ticks = 7160  
tmr_starts = 4067359  
tmr_stops = 3487837  
tmr_timeouts = 574960  
tmr_active = 4562  
tmr_longest_chain = 505
```

The following example shows how to display information about the quota server:

```
Router# show ip csg quota-server
```

| charging gateway | vrf | priority | state  |
|------------------|-----|----------|--------|
| 10.18.28.10:3385 |     | 1        | ACTIVE |

The following example shows how to display information about sessions:

```
Router# show ip csg sessions
```

| subscriber       | network          | prot | vrf    | state |
|------------------|------------------|------|--------|-------|
| 10.18.28.37:1028 | 11.18.28.19:1812 | 17   | <none> | ESTAB |
| 10.18.28.34:1029 | 11.18.28.17:1812 | 17   | <none> | ESTAB |
| 10.18.28.11:1813 | 10.18.28.2:1812  | 17   | <none> | ESTAB |
| 10.18.28.14:1813 | 10.18.28.2:1812  | 17   | <none> | ESTAB |
| 10.18.28.15:1813 | 10.18.28.2:1812  | 17   | <none> | ESTAB |
| 10.18.28.13:1813 | 10.18.28.2:1812  | 17   | <none> | ESTAB |
| 10.18.28.11:1810 | 10.18.28.2:5555  | 17   | <none> | ESTAB |
| 10.18.28.13:1810 | 10.18.28.2:5555  | 17   | <none> | ESTAB |
| 10.18.28.14:1810 | 10.18.28.2:5555  | 17   | <none> | ESTAB |
| 10.18.28.15:1810 | 10.18.28.2:5555  | 17   | <none> | ESTAB |
| 10.18.28.34:1030 | 11.18.28.17:1812 | 17   | <none> | ESTAB |
| 10.18.28.13:1814 | 10.18.28.36:1812 | 17   | <none> | ESTAB |
| 10.18.28.14:1814 | 10.18.28.36:1812 | 17   | <none> | ESTAB |
| 10.18.28.11:1814 | 10.18.28.36:1812 | 17   | <none> | ESTAB |
| 10.18.28.34:1031 | 11.18.28.17:1812 | 17   | <none> | ESTAB |
| 10.18.28.11:1815 | 10.18.28.2:5555  | 17   | <none> | ESTAB |
| 10.18.28.12:1815 | 10.18.28.2:5555  | 17   | <none> | ESTAB |
| 10.18.28.13:1815 | 10.18.28.2:5555  | 17   | <none> | ESTAB |
| 10.18.28.14:1815 | 10.18.28.2:5555  | 17   | <none> | ESTAB |
| 10.18.28.15:1815 | 10.18.28.2:5555  | 17   | <none> | ESTAB |
| 10.18.28.36:1025 | 11.18.28.18:1812 | 17   | <none> | ESTAB |
| 10.18.28.34:1026 | 11.18.28.17:1812 | 17   | <none> | ESTAB |
| 10.18.28.37:1027 | 11.18.28.19:1812 | 17   | <none> | ESTAB |
| 10.18.28.11:1812 | 10.18.28.2:5555  | 17   | <none> | ESTAB |
| 10.18.28.13:1812 | 10.18.28.2:5555  | 17   | <none> | ESTAB |
| 10.18.28.14:1812 | 10.18.28.2:5555  | 17   | <none> | ESTAB |
| 10.18.28.15:1812 | 10.18.28.2:5555  | 17   | <none> | ESTAB |
| 10.18.28.37:1036 | 11.18.28.19:1812 | 17   | <none> | ESTAB |
| 10.18.28.34:1032 | 11.18.28.17:1812 | 17   | <none> | ESTAB |
| 10.18.28.13:1816 | 10.18.28.37:1812 | 17   | <none> | ESTAB |
| 10.18.28.15:1816 | 10.18.28.37:1812 | 17   | <none> | ESTAB |
| 10.18.28.14:1816 | 10.18.28.37:1812 | 17   | <none> | ESTAB |
| 10.18.28.11:1816 | 10.18.28.37:1812 | 17   | <none> | ESTAB |
| 10.18.28.36:1033 | 11.18.28.18:1812 | 17   | <none> | ESTAB |
| 10.18.28.36:1034 | 11.18.28.18:1812 | 17   | <none> | ESTAB |
| 10.18.28.11:1818 | 10.18.28.34:1812 | 17   | <none> | ESTAB |
| 10.18.28.14:1818 | 10.18.28.34:1812 | 17   | <none> | ESTAB |
| 10.18.28.15:1818 | 10.18.28.34:1812 | 17   | <none> | ESTAB |
| 10.18.28.12:1818 | 10.18.28.34:1812 | 17   | <none> | ESTAB |
| 10.18.28.13:1818 | 10.18.28.34:1812 | 17   | <none> | ESTAB |
| 10.18.28.37:1035 | 11.18.28.19:1812 | 17   | <none> | ESTAB |



**Note**

The **prot** column displays the IP protocol as described in the Assigned Numbers RFC.



The following table lists and describes the possible states for the **show ip csg sessions user** command:

| <b>State<sup>1</sup></b>                  | <b>Description</b>   |
|---|--|
| <b>CSG_S SVC_STATE_INIT</b>               | The session has been created but no packet has been processed.<br>Short timer. <sup>2</sup>  |
| <b>CSG_S SVC_STATE_SYN_SUB</b>            | A SYN packet has been received from the subscriber interface.<br>Short timer. <sup>2</sup>   |
| <b>CSG_S SVC_STATE_SYN_NET</b>            | A SYN packet has been received from the network interface.<br>Short timer. <sup>2</sup>  |
| <b>CSG_S SVC_STATE_SYN_BOTH</b>           | The session has received a SYN packet from both the subscriber and network interfaces.<br>Short timer. <sup>2</sup>  |
| <b>CSG_S SVC_STATE_SETUP_ACK_SUB_WAIT</b> | The session has received a SYN-ACK from the network interface and is waiting for the ACK from the subscriber interface to complete the TCP 3-way handshake.<br>Short timer. <sup>2</sup> |
| <b>CSG_S SVC_STATE_SETUP_ACK_NET_WAIT</b> | The session has received a SYN-ACK from the subscriber interface and is waiting for the ACK from the network interface to complete the TCP 3-way handshake.<br>Short timer. <sup>2</sup> |
| <b>CSG_S SVC_STATE_ESTAB</b>              | The TCP session has been established.<br>UDP sessions enter this state on the first packet. This is the only state for UDP sessions after INIT.  |
| <b>CSG_S SVC_STATE_FIN_SUB</b>            | The session has received a FIN from the subscriber interface   |
| <b>CSG_S SVC_STATE_FIN_NET</b>            | The session has received a FIN from the network interface  |
| <b>CSG_S SVC_STATE_FIN_SUB_WAIT</b>       | The session has received an ACK from the subscriber interface and is waiting for a FIN from the subscriber interface   |
| <b>CSG_S SVC_STATE_FIN_NET_WAIT</b>       | The session has received an ACK from the network interface and is waiting for a FIN from the network interface   |
| <b>CSG_S SVC_STATE_FIN_BOTH</b>           | The session has received a FIN from both the subscriber and network interfaces   |

| State <sup>1</sup>                          | Description  |
|---|--|
| <b>CSG_S SVC_STATE_CLOSING_ACK_NET_WAIT</b> | The session has received a FIN-ACK or a FIN and an ACK from the subscriber interface and is waiting for the ACK from the network interface to close the connection.<br><br>Short timer. <sup>2</sup> |
| <b>CSG_S SVC_STATE_CLOSING_ACK_SUB_WAIT</b> | The session has received a FIN-ACK or a FIN and an ACK from the network interface and is waiting for the ACK from the subscriber interface to close the connection.<br><br>Short timer. <sup>2</sup> |
| <b>CSG_S SVC_STATE_CLOSED</b>               | The session is closed. Note that closed sessions are destroyed so it is very unlikely that show session will display a session in this state.  |

1. TCP sessions use all these states. UDP sessions move from INIT state directly to ESTAB state.
2. "Short timer" indicates that the state uses a 5-second idle time regardless of what is configured in the content. All other states use the configured idle time.

The following example displays detailed information about the subscriber at **10.18.28.0/24**:

```
Router# show ip csg users 10.18.28.0/24 detail

10.18.28.11      C-10.18.28.11
  sessions = 1, traffic proc id = 4
  nexthop downlink ip = 0.0.0.0, flags = 0x00000001
  nas = <none>
  idle = 10000, PoD = no
  billing = PREPAID, plan = PERF, handoff timer OFF, idle timer OFF
  bma: ip = 10.18.28.10, port = 3333
  quota-server: ip = 0.0.0.0, port = 0
  affinity state = OPEN
10.18.28.14      C-10.18.28.14
  sessions = 1, traffic proc id = 4
  nexthop downlink ip = 0.0.0.0, flags = 0x00000001
  nas = <none>
  idle = 10000, PoD = no
  billing = PREPAID, plan = PERF, hand
```

#### Related Commands

| Command                        | Description   |
|--------------------------------|---|
| <a href="#">ip csg billing</a> | Defines a CSG2 billing plan, and enters CSG2 billing configuration mode.          |
| <a href="#">ip csg content</a> | Configures content for CSG2 services, and enters CSG2 content configuration mode. |

# show ip iscsi

To display information about the iSCSI, use the **show ip iscsi** command in privileged EXEC mode.

**show ip iscsi {name | session [*session-id*] [detail] | stats [detail] | target}**

| Syntax Description | name              | Displays the name of an iSCSI initiator.                              |
|--------------------|-------------------|---|
|                    | session           | Displays the status of iSCSI sessions on the CSG2.                    |
|                    | <i>session-id</i> | (Optional) Displays information for only the specified iSCSI session. |
|                    | detail            | (Optional) Displays detailed information about the iSCSI session.     |
|                    | stats             | Displays iSCSI statistics.  |
|                    | detail            | (Optional) Displays detailed iSCSI statistics.                        |
|                    | target            | Displays information about an iSCSI target.                           |

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC

| Command History | Release    | Modification                 |
|-----------------|------------|------------------------------|
|                 | 12.4(15)MD | This command was introduced. |

## Examples

The following example shows output from the **show ip iscsi name** command:

```
Router# show ip iscsi name
iSCSI initiator name: iqn.1987-07.com.cisco:wtbg-sup-09-3
```

The following example shows output from the **show ip iscsi session** command:

```
Router# show ip iscsi session
ID  TARGET  STATE      CONNECTIONS
-----
12  LINUX   Logged In  1
```

The following example shows output from the **show ip iscsi session detail** command:

```
Router# show ip iscsi session detail
ID: 12
Profile: LINUX
State: Logged In
Connections: 1
First Burst Length: 16384
Max Burst Length: 16384
Max Recv Data Segment: 32768
Max Xmit Data Segment: 8192
Initial R2T: Yes
Immediate data: Yes
Data PDU in order: Yes
Data PDU in order: Yes
```

The following example shows output from the **show ip iscsi stats** command:

```
Router# show ip iscsi stats
iSCSI Stats:
  Login Requests - 2, Login Responses - 2
  Logout Requests - 0, Logout Responses - 0
  Login Timeouts - 0, Logout Timeouts - 0
  SCSI Commands - 27, SCSI Responses - 27
  Data In PDUs - 25, Data Out PDUs - 0
  Immed Data - 1, Unsolicited Data - 0
  NOP Ins - 35, NOP Outs - 35
  Async Requests - 0, Async Req Logout - 0
  Async Drop Conn - 0, Async Drop Conns - 0
  R2t Requests - 0, Rejects - 0

System Stats:
  TX Queue Overflow - 0, RX Queue Overflow - 0
  Connection Resets - 0, Tasks aborted - 0

SCSI Stats:
  Total Requests - 27
  Test Unit Ready Requests - 1, Test Unit Ready Failures - 0
  Report Luns Requests - 1, Report Luns Failures - 0
  Lun Inquiry Requests - 5, Lun Inquiry Failures - 0
  Read Capacity Requests - 5, Read Capacity Failures - 0
  Read Requests - 14, Read Failures - 0
  Write Requests - 1, Write Failures - 0
  Blocks Read- 49, Blocks Written - 8
```

The following example shows output from the **show ip iscsi stats detail** command:

```
Router# show ip iscsi stats detail
iSCSI Stats:
  Login Requests - 2, Login Responses - 2
  Logout Requests - 0, Logout Responses - 0
  Login Timeouts - 0, Logout Timeouts - 0
  SCSI Commands - 27, SCSI Responses - 27
  Data In PDUs - 25, Data Out PDUs - 0
  Immed Data - 1, Unsolicited Data - 0
  NOP Ins - 36, NOP Outs - 36
  Async Requests - 0, Async Req Logout - 0
  Async Drop Conn - 0, Async Drop Conns - 0
  R2t Requests - 0, Rejects - 0

System Stats:
  TX Queue Overflow - 0, RX Queue Overflow - 0
  Connection Resets - 0, Tasks aborted - 0

SCSI Stats:
  Total Requests - 27
  Test Unit Ready Requests - 1, Test Unit Ready Failures - 0
  Report Luns Requests - 1, Report Luns Failures - 0
  Lun Inquiry Requests - 5, Lun Inquiry Failures - 0
  Read Capacity Requests - 5, Read Capacity Failures - 0
  Read Requests - 14, Read Failures - 0
  Write Requests - 1, Write Failures - 0
  Blocks Read- 49, Blocks Written - 8
```

The following example shows output from the **show ip iscsi target** command:

```
Router# show ip iscsi target
Target Profile= TARGET_LINUX IN_USE
Target: name= iqn.2002-10.edu.unh.iol.iscsi.draft20-target:1
Target: ip= 10.76.43.233, port= 3260, portal group= 0
vrf= , sync read offset= 100, batch write= 100
write interval= 5 sec, file size= 100 MB #
```

# show record-storage-module

To display information about the record storage module (RSM), use the **show record-storage-module** command in privileged EXEC mode.

```
show record-storage-module {stats | target-info [all | target-profile profile-name] [detail]}
```

| Syntax Description |   |  |
|--------------------|---|--|
|                    | <b>stats</b>                              | Displays current RSM statistics.   |
|                    | <b>target-info</b>                        | Displays the number of RSM disks available, and their current status.        |
|                    | <b>all</b>                                | (Optional) Displays statistics for all targets for which there are profiles. |
|                    | <b>target-profile</b> <i>profile-name</i> | (Optional) Displays statistics for a specific profile.                       |
|                    | <b>detail</b>                             | (Optional) Displays detailed information about the RSM drives.               |

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC

| Command History | Release    | Modification                 |
|-----------------|------------|------------------------------|
|                 | 12.4(15)MD | This command was introduced. |

**Usage Guidelines** Use the **show record-storage-module stats** command to display RSM statistics.

**Examples** The following example shows output from the **show record-storage-module stats** command:

```
Router# show record-storage-module stats
RSM Appl Stats:
requests:
  open= 1, read= 0, write= 0
  ping= 0, close= 0
request fail:
  open= 0, read= 0, write= 0
  ping= 0, close= 0 | ta
alloc fail:
  appl info= 0, appl msg= 0, appl req= 0,
  data buffer= 0, drive= 0
RSM Clear:
  Statistics = 1
```

The following example shows output from the **show record-storage-module target-info all detail** command:

```
Router# show record-storage-module target-info all detail
Target profile = TARGET_LINUX
Application name = GGSN, Target State = Active, Disk = Usable
Application id = 2, iSCSI handle = 2
```

```
Number of drives = 5, Read drive = sda3, Write drive = sda3
Active drives:
  Drive = sda3
  File system id = 19
  Descriptors: read = -1, write = -1, master = -1
  Current File: bytes written = 0, bytes read = 0
  Master file in memory:
  Drive full = No
  Write: dir = 1, file = 1
  Read: dir = 1, file = 1, offset = 62675
  Salvage file = 0, CRC = 0x91C816C0
Failed drives:
  Drive = sda0
  Reason = Unexpected IFS error (Invalid DOS media or no media in slot)
  Drive = sda1
  Reason = Unexpected IFS error (Invalid DOS media or no media in slot)
  Drive = sda2
  Reason = Unexpected IFS error (Invalid DOS media or no media in slot)
  Drive = sda4
  Reason = Unexpected IFS error (Invalid DOS media or no media in slot)
```

## snmp-server enable traps csg

To enable Simple Network Management Protocol (SNMP) notification types that are available on the CSG2, use the **snmp-server enable traps csg** command in global configuration mode. To disable CSG2 notifications, use the **no** form of this command.

```
snmp-server enable traps csg [bma [records | state] | database | quota-server [records | state]]
```

```
no snmp-server enable traps csg [bma [records | state] | database |
quota-server [records | state]]
```

| Syntax Description  |            |   |
|---------------------|------------|---|
| <b>bma</b>          | (Optional) | Enables traps for only the Billing Mediation Agents (BMAs) to which the CSG2 sends billing records. |
| <b>records</b>      | (Optional) | Enables only lost records traps for the BMAs.   |
| <b>state</b>        | (Optional) | Enables only state change traps for the BMAs.   |
| <b>database</b>     | (Optional) | Enables traps for only the database server that answers CSG2 user ID queries.                       |
| <b>quota-server</b> | (Optional) | Enables traps for only the CSG2 quota servers.  |
| <b>records</b>      | (Optional) | Enables only lost records traps for the quota servers.  |
| <b>state</b>        | (Optional) | Enables only state change traps for the quota servers.  |

**Command Default** If you do not enter the **snmp-server enable traps csg** command, no CSG2 notifications controlled by this command are sent.

**Command Modes** Global configuration

| Command History | Release    | Modification   |
|-----------------|------------|--|
|                 | 12.4(11)MD | This command was migrated from CSG1.   |
|                 |            | Changes from CSG1:   |
|                 |            | <ul style="list-style-type: none"> <li>The <b>bma</b>, <b>database</b>, <b>quota-server</b>, <b>records</b>, and <b>state</b> keywords were added.</li> <li>The <b>agent</b>, <b>database</b>, and <b>quota-server</b> keywords were removed.</li> </ul> |

**Usage Guidelines** Entering the **snmp-server enable traps csg** command enables all CSG2 SNMP traps.

If you then enter the **snmp-server enable traps csg bma** command, the BMA lost records and state change traps are enabled.

If you then enter the **snmp-server enable traps csg quota-server records** command, the quota server lost records trap is enabled.



---

**Examples**

The following example enables CSG2 traps:

```
snmp-server enable traps csg
```

---

**Related Commands**

| Command                           | Description  |
|-----------------------------------|--|
| <a href="#">ip csg snmp timer</a> | Defines Simple Network Management Protocol (SNMP) timers for lost CSG2 records, and enters CSG2 SNMP timer configuration mode. |

---

# subscriber-ip http-header forwarded-for

To specify that the CSG2 is to obtain the subscriber's IP address from the HTTP X-Forwarded-For header, use the **subscriber-ip http-header x-forwarded-for** command in CSG2 content configuration mode. To specify that the CSG2 is to obtain the subscriber's IP address from the IP header, use the **no** form of this command.

**subscriber-ip http-header x-forwarded-for [obscure]**

**no subscriber-ip http-header x-forwarded-for**

## Syntax Description

|                |  |
|----------------|--|
| <b>obscure</b> | (Optional) Overwrite the IP address in the X-Forwarded-For header with blanks. |
|----------------|--|

## Defaults

The CSG2 obtains the subscriber's IP address from the IP header. If you enter the **subscriber-ip http-header x-forwarded-for** command without the **obscure** keyword, the IP address in the X-Forwarded-For header is not obscured with blanks.

## Command Modes

CSG2 content configuration

## Command History

| Release    | Modification                 |
|------------|------------------------------|
| 12.4(11)MD | This command was introduced. |

## Usage Guidelines

If the CSG2 is configured to obtain the subscriber's IP address from the HTTP X-Forwarded-For header, it also automatically recognizes the variant X-UP-Forwarded-For header.

Only content that is configured with **parse protocol http** can be configured with **subscriber-ip http-header x-forwarded-for**.

Single-TP mode is required for HTTP X-Forwarded-For operation.

- Before configuring the CSG2 for X-Forwarded-For operation, configure the CSG2 for single-TP mode by entering the **ip csg mode single-tp** command, then performing a **write memory**, then restarting the CSG2.
- If the CSG2 is not operating in single-TP mode, and you attempt to enter the **subscriber-ip http-header x-forwarded-for** command, the CSG2 rejects the command and issues a warning message.
- If the CSG2 is operating in single-TP mode and you attempt to switch to multiple-TP mode, the CSG2 checks the configuration for the **subscriber-ip http-header x-forwarded-for** command. If the configuration does contain the command (that is, X-Forwarded-For operation is enabled), the CSG2 does not switch to multiple-TP mode, and it issues a warning message.

To prevent exposure of potentially sensitive IP addresses, the CSG2 can obscure the contents of X-Forwarded-For headers, overwriting the contents with blanks.

- If you want to obscure the contents of the X-Forwarded-For header, enter the **subscriber-ip http-header x-forwarded-for** command with the **obscure** keyword.
- If you do not want to obscure the contents of the X-Forwarded-For header, enter the **subscriber-ip http-header x-forwarded-for** command without the **obscure** keyword (the default setting).
- When obscuring the IP address in X-Forwarded-For headers, keep the following considerations in mind:
  - The CSG2 does not obscure the IP address in fragmented request packets that have X-Forwarded-For headers, because the CSG2 does not reassemble the fragments and therefore cannot modify the packets.
  - The CSG2 does not obscure the X-Forwarded-For header for traffic that is downgraded from Layer 7 inspection to Layer 4 inspection.
  - If the active CSG2 fails over to the standby CSG2, the standby CSG2 does not obscure the IP address in X-Forwarded-For header for existing HTTP sessions. However, the standby CSG2 does obscure the IP address in X-Forwarded-For headers for new HTTP sessions.
  - If the subscriber sends more than one GET request with X-Forwarded-For headers, and the content host fails to send a TCP acknowledgement within five seconds, the CSG2 resets the subscriber side connection.

### Examples

The following example configures the CSG2 to obtain the subscriber's IP address from the HTTP X-Forwarded-For header, and obscures the IP address in the X-Forwarded-For header:

```
ip csg content MOVIES
  parse protocol http
  subscriber-ip http-header x-forwarded-for obscure
```

### Related Commands

| Command                               | Description   |
|---------------------------------------|---|
| <a href="#">ip csg content</a>        | Configures content for CSG2 services, and enters CSG2 content configuration mode.                         |
| <a href="#">ip csg mode single-tp</a> | Enables the CSG2 to use a single TP instead of multiple TPs.  |
| <a href="#">parse length</a>          | Defines the maximum number of Layer 7 bytes that the CSG2 is to parse when attempting to assign a policy. |
| <a href="#">parse protocol</a>        | Defines how the CSG2 is to parse traffic for a content.   |

# verify confirm

To configure a token for use in CSG2 service verification URL-rewriting, use the **verify confirm** command in CSG2 service configuration mode. To remove the token, use the **no** form of this command.

**verify confirm** *token*

**no verify confirm** *token*

| <b>Syntax Description</b> | <p><i>token</i></p> <p>A string of up to 15 alphanumeric characters. The string is not case-sensitive.</p> <p>Acceptable characters include alphanumeric characters and any of the following special characters: \$-_.+!*'(),?!:@&amp;=;%~. To enter other special characters not listed, use the URL-escape format with the percent sign (%).</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>   |         |              |            |                                      |  |                    |  |   |
|---------------------------|---|---------|--------------|------------|--------------------------------------|--|--------------------|--|---|
| <b>Defaults</b>           | None  |         |              |            |                                      |  |                    |  |   |
| <b>Command Modes</b>      | CSG2 service configuration  |         |              |            |                                      |  |                    |  |   |
| <b>Command History</b>    | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.4(11)MD</td> <td>This command was migrated from CSG1.</td> </tr> <tr> <td></td> <td>Changes from CSG1:</td> </tr> <tr> <td></td> <td> <ul style="list-style-type: none"> <li>The name of this command changed from <b>verify confirmation</b> to <b>verify confirm</b>.</li> <li>The configuration mode for this command changed from CSG user group configuration to CSG2 service configuration.</li> <li>The list of supported special characters changed.</li> </ul> </td> </tr> </tbody> </table>   | Release | Modification | 12.4(11)MD | This command was migrated from CSG1. |  | Changes from CSG1: |  | <ul style="list-style-type: none"> <li>The name of this command changed from <b>verify confirmation</b> to <b>verify confirm</b>.</li> <li>The configuration mode for this command changed from CSG user group configuration to CSG2 service configuration.</li> <li>The list of supported special characters changed.</li> </ul> |
| Release                   | Modification  |         |              |            |                                      |  |                    |  |   |
| 12.4(11)MD                | This command was migrated from CSG1.  |         |              |            |                                      |  |                    |  |   |
|                           | Changes from CSG1:  |         |              |            |                                      |  |                    |  |   |
|                           | <ul style="list-style-type: none"> <li>The name of this command changed from <b>verify confirmation</b> to <b>verify confirm</b>.</li> <li>The configuration mode for this command changed from CSG user group configuration to CSG2 service configuration.</li> <li>The list of supported special characters changed.</li> </ul>   |         |              |            |                                      |  |                    |  |   |
| <b>Usage Guidelines</b>   | <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 network.</p> <p>The token is used for HTTP and wireless application protocol (WAP) service verification URL-rewriting.</p> <p>If the token uses the URL-escape format, the redirect URL to which the token is being matched must also use the URL-escape format.</p> |         |              |            |                                      |  |                    |  |   |

**Examples**

The following example specifies a token for service verification URL-rewriting:

```
ip csg service MOVIES
  aoc enable
  verify confirm ?CSG_VERIFY_OK
```

**Related Commands**

| Command                        | Description  |
|--------------------------------|--|
| <a href="#">ip csg service</a> | Configures a CSG2 content billing service, and enters CSG2 service configuration mode. |
| <a href="#">verify enable</a>  | Enables CSG2 service verification.   |

# verify enable

To enable CSG2 service verification, use the **verify enable** command in CSG2 service configuration mode. To disable this feature, use the **no** form of this command.

**verify enable**

**no verify enable**

**Syntax Description** This command has no arguments or keywords.

**Defaults** None

**Command Modes** CSG2 service configuration

| Command History | Release    | Modification   |
|-----------------|------------|--|
|                 | 12.4(11)MD | This command was migrated from CSG1.<br>Changes from CSG1: The name of this command changed from <b>verify</b> to <b>verify enable</b> . |

**Usage Guidelines** If this command is configured, the CSG2 uses the Service Verification Request to perform the following actions:

- Alert the quota server of a new transaction.
- Allow the quota server to direct the CSG2 to perform one of the following mutually exclusive actions:
  - **DROP**—Drop all packets for this flow.
  - **FORWARD**—Forward the flow without altering the destination (a weight might be specified).
  - **REDIRECT-URL**—Redirect subscriber requests to the URL provided by the quota server. The CSG2 sends a Layer 7 redirect to the subscriber (for example, HTTP 302 response) that contains the redirect URL.

**Examples** The following example specifies a token for service verification URL-rewriting:

```
ip csg service SERVICE_NAME
verify enable
```

| Related Commands | Command                        | Description  |
|------------------|--------------------------------|--|
|                  | <a href="#">ip csg service</a> | Configures a CSG2 content billing service, and enters CSG2 service configuration mode. |
|                  | <a href="#">verify confirm</a> | Configures a token for use in CSG2 service verification URL-rewriting.                 |

## vlan (CSG2 content)

To restrict the CSG2 billing content to a single source VLAN, use the **vlan** command in CSG2 content configuration mode. To remove the restriction, use the **no** form of this command.

**vlan** *vlan-number*

**no vlan**

|                           |  |   |
|---------------------------|--|---|
| <b>Syntax Description</b> | <i>vlan-number</i>   | Dot1q encapsulation VLAN number.  |
| <b>Defaults</b>           | None   |   |
| <b>Command Modes</b>      | CSG2 content configuration   |   |
| <b>Command History</b>    | <b>Release</b>   | <b>Modification</b>   |
|                           | 12.4(11)MD   | This command was migrated from CSG1.<br><br>Changes from CSG1: The <i>vlan-name</i> argument was replaced with the <i>vlan-number</i> argument. |
| <b>Usage Guidelines</b>   | The VLAN number is dependent on the CSG2 card that receives the content. When the content is downloaded to a CSG2 card, the <i>vlan-number</i> argument is mapped to a specific VLAN number. |   |
| <b>Examples</b>           | The following example shows how to restrict the CSG2 content billing to single-source VLAN number 67:<br><br><pre>ip csg content MOVIES_COMEDY vlan 67</pre>                                 |   |
| <b>Related Commands</b>   | <b>Command</b>   | <b>Description</b>  |
|                           | <a href="#">ip csg content</a>   | Configures content for CSG2 services, and enters CSG2 content configuration mode.   |

# vrf

To restrict the CSG2 content to packets within a single Virtual Routing and Forwarding (VRF) table, use the **vrf** command in CSG2 content configuration mode. To remove the restriction, use the **no** form of this command.

**vrf** *vrf-name*

**no vrf**

## Syntax Description

|                 |  |
|-----------------|--|
| <i>vrf-name</i> | VRF within which the content should match packets. |
|-----------------|--|

## Defaults

None

## Command Modes

CSG2 content configuration

## Command History

| Release    | Modification                 |
|------------|------------------------------|
| 12.4(11)MD | This command was introduced. |

## Usage Guidelines

VRF configuration and filtering cannot be used in conjunction with VLAN filtering.

If you want to use VRF tables to restrict CSG2 content, we recommend that you define a VRF table for every content. If you do not configure a VRF table for a given content, then that content cannot match traffic to a VRF table, and you cannot use a global content to match traffic in different VRF tables.

## Examples

The following example shows how to restrict the CSG2 content to packets within VRF table CONTENTVRF:

```
ip csg content MOVIES_COMEDY
vrf CONTENTVRF
```

## Related Commands

| Command                        | Description   |
|--------------------------------|---|
| <a href="#">ip csg content</a> | Configures content for CSG2 services, and enters CSG2 content configuration mode. |