# ACS Charging Action Configuration Mode Commands

The ACS Charging Action Configuration Mode is used to configure Active Charging Service (ACS) charging actions.

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* **> charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Important**

The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

# allocation-retention-priority

This command allows you to configure the Allocation Retention Priority (ARP).

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* **> charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**allocation-retention-priority** *priority* **[ pci** *pci_value* **| pvi** *pvi_value* **]**
**no allocation-retention-priority**

**no**

If previously configured, disables ARP configuration in the current charging action.

***priority***

*priority* must be an integer from 1 through 15.

**pci *pci_value***

Specifies the Pre-emption Capability Indicator (PCI).

*pci_value* must be integer 0 or 1.

**Important** If not explicitly enabled, then the default value of 1 will hold true.

**pvi *pvi_value***

Specifies the Pre-emption Vulnerability Indicator (PVI).

*pvi_value* must be integer 0 or 1.

**Important** If not explicitly enabled, then the default value of 0 will hold true.

**Usage Guidelines**

This command configures the ARP, which indicates the priority of allocation and retention of the service data flow. The ARP resolves conflicts in demand for network resources. At the time of resource crunch, this parameter prioritizes allocation of resources during bearer establishment and modification. In a congestion situation, a lower ARP flow may be dropped to free up capacity. Once a service flow is successfully established, this parameter plays no role in quality of service (QoS) experienced by the flow.

**Example**

The following command sets the ARP to *10*:

```
allocation-retention-priority 10
```

# billing-action

This command allows you to configure the billing action for packets that match specific rule definitions (ruledefs).

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* > **charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

## Syntax Description

In StarOS 12.2 and later releases:

**billing-action { create-edrs { charging-edr** *charging_edr_format_name* **| reporting-edr** *reporting_edr_format_name* **} + [ wait-until-flow-ends ] | egcdr | exclude-from-udrs | radius | rf } +**
**no billing-action [ create-edrs | egcdr | exclude-from-udrs | radius | rf ] +**

In StarOS 12.1 and earlier releases:

**billing-action { edr** *edr_format_name* **[ wait-until-flow-ends ] | egcdr | exclude-from-udrs | radius | rf } +**
**no billing-action [ edr | egcdr | exclude-from-udrs | radius | rf ] +**

**no**

If previously configured, disables the specified configuration in the current charging action.

**edr *edr_format_name* [ wait-until-flow-ends ]**

**Important** This option is available only in 12.1 and earlier releases. In 12.2 and later releases, it is deprecated and is replaced by the **create-edrs charging-edr** option.

Enables EDR billing for packets matching this charging action.

*edr_format_name* must be the name of an existing EDR format, and must be an alphanumeric string of 1 through 63 characters.

**Important** If the EDR format name specified here is not configured in the EDR Format Configuration Mode, or has been deleted, the system accepts it without applying any EDR format for the billing action in this ACS service.

If this option is configured, the system generates an EDR immediately when a packet is received and it matches a ruledef that is associated with this charging action. Other events configured for flow end-condition, flow action, termination, and/or session control also create the triggers for EDR generation.

**wait-until-flow-ends**: By default, the EDR is generated immediately after a ruledef hit results in this charging action. When this keyword is specified, no EDR is generated on a ruledef hit. When the flow ends, an attempt is made to generate an EDR with the format specified.

**create-edrs { charging-edr *charging_edr_format_name* | reporting-edr *reporting_edr_format_name* } + [ wait-until-flow-ends ]**

**Important** This option is available only in 12.2 and later releases.

Enables EDR billing for packets matching this charging action.

- **charging-edr** *charging_edr_format_name*: Specifies to generate charging EDR.

*charging_edr_format_name* must be the name of a charging EDR format, and must be an alphanumeric string of 1 through 63 characters.

- **reporting-edr** *reporting_edr_format_name*: Specifies to generate reporting EDR.

  *reporting_edr_format_name* must be the name of a reporting EDR format, and must be an alphanumeric string of 1 through 63 characters.

If the above options are configured, the system generates an EDR immediately when a packet is received and it matches a ruledef that is associated with this charging action. Other events configured for flow end-condition, flow action, termination, and/or session control also creates the triggers for EDR generation.

- **wait-until-flow-ends**: By default, the EDR is generated immediately after a ruledef hit results in this charging action. When this keyword is specified, no EDR is generated on a ruledef hit. When the flow ends, an attempt is made to generate an EDR with the format specified.

#### egcdr

Enables eG-CDR billing for packets matching this charging action.

If this option is configured, the system generates an eG-CDR when the subscriber session ends or an interim trigger condition occurs. The interim triggers are configurable in the ACS Rulebase Configuration Mode. In addition, whenever there is an SGSN-to-SGSN handoff the system treats that as a trigger.

To generate an eG-CDR the **accounting-mode** command in the APN Configuration Mode must be configured with the "none" option.

The format of enhanced G-CDRs is controlled by the **inspector** CLI command in the Context Configuration Mode.

#### exclude-from-udrs

By default, statistics are accumulated on a per content ID basis for possible inclusion in UDRs. The **exclude-from-udrs** keyword causes the system to not include the packet's statistics in UDRs.

When this option is disabled, (the default setting) UDRs will be generated based on the UDR format specified in the rulebase.

Default: Disabled.

#### radius

Enables billing action as RADIUS Charging Data Records (CDRs) for packets matching this charging action, and the data packet statistics will be included in the postpaid RADIUS accounting.

Default: Disabled.

#### rf

Enables Rf accounting.

Rf accounting is applicable only for dynamic and predefined rules that are marked for it. Dynamic rules have a field offline-enabled to indicate this. To mark a predefined rule as offline-enabled, use this keyword and the **billing-records** CLI in the ACS Rulebase Configuration Mode.

### Usage Guidelines

Use this command to enable an EDR, eG-CDR and/or RADIUS CDR type of billing for content matching this charging action.

### Example

In 12.1 and earlier releases, the following command enables the EDR billing type with EDR format *charge1_format*:

```
billing-action edr charge1_format
```

In 12.2 and later releases, the following command is applied to both charging and reporting EDRs since the trigger for both the EDRs is the same:

```
billing-action create-edrs charging-edr charging_edrformat1 reporting-edr
 reporting_edrformat1 wait-until-flow-ends
```

# cca charging credit

This command allows you to enable/disable Credit Control Application (CCA) and configure the RADIUS/Diameter prepaid charging behavior.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* **> charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**cca charging credit [ rating-group** *coupon_id* **] [ preemptively-request ] { default | no } cca charging**

#### no

If previously configured, disables RADIUS/Diameter Prepaid Credit Control Charging in the current charging action.

#### default

Disables RADIUS/Diameter Prepaid Credit Control Charging.

#### credit

Specifies RADIUS/Diameter Prepaid Credit Control Charging Credit behavior.

#### preemptively-request

Specifies RADIUS/Diameter prepaid credit preemptively requested charging credit behavior. If this option is used, a quota is requested for the specific type of content during session initialization.

**rating-group *coupon_id***

Specifies the coupon ID used in prepaid charging as rating-group which maps to the coupon ID for prepaid customer.

*coupon_id* must be an integer from 0 through 65535.

This option also assigns different content-types for the same charging action depending upon whether or not prepaid is enabled.

**Important** This rating-group overrides the content ID, if present in the same charging-action for the prepaid customer in Diameter Credit Control Application (DCCA). But only the content IDs will be used in eG-CDRs irrespective of the presence of rating-group in that charging action.

**Usage Guidelines** Use this command to configure RADIUS/Diameter Prepaid Credit Control Charging behavior.

This command selects reservation based credit control. A CCR-Initial is used to reserve quota upon the first traffic, then a series of CCR-updates are issued as the traffic proceeds and quota dwindles. A CCR-Terminate is issued at the end of the session or at the end of the quota-hold-time.

**Example**

The following is an example of this command:

```
cca charging credit
```

# charge-units

This command allows you to configure the charge units for RADIUS/DCCA charging calculation.

**Product** GGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* > **charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

```
charge-units units
{ default | no } charge-units
```

**default**

Configures this command with its default setting.

Default: 0; disables the counter, same as **no charge-units**

**no**

If previously configured, disables the charge-units configuration in the current charging action.

***units***

Specifies the service-specific fixed unit counter per content ID for RADIUS/DCCA charging.

*units* is the value set for charging unit, and must be an integer from 1 through 65535.

**Usage Guidelines**

This command configures the unit amount counters for charging calculation on per content ID basis for different protocols and packets regardless of packet direction (uplink or downlink).

**Important**

For more information on content ID, refer to the **if-protocol** command in the *ACS Ruledef Configuration Mode Commands* chapter.

**Example**

The following command sets the charging unit to *1024*:

```
charge-units 1024
```

# charge-volume

This command allows you to configure how the volume amount counter for eG-CDRs, UDRs, and DCCA charging are calculated.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* **> charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

```
charge-volume { { dns | ftp-control | ftp-data | http | icmp | imap | ip
 | mms | pop3 | pptp | rtcp | rtp | rtsp | sdp | secure-http | sip | smtp
 | tcp | tftp | udp | wsp | wtp } { bytes | packet-length | packets } [
downlink | uplink ] | constant fixed_value }
{ default | no } charge-volume
```

**default**

Configures this command with its default setting.

Default: **charge-volume ip bytes**

**no**

If previously configured, deletes the charge-volume configuration in the current charging action.

**{ dns | ftp-control | ftp-data | http | icmp | imap | ip | mms | pop3 | pptp | rtcp | rtp | rtsp | sdp | secure-http | sip | smtp | tcp | tftp | udp | wsp | wtp }**

Specifies the charge volume method for the specific rule definition.

- **dns**: Charge volume for DNS
- **ftp-control**: Charge volume for FTP-Control
- **ftp-data**: Charge volume for FTP-Data
- **http**: Charge volume for HTTP
- **icmp**: Charge volume for ICMP
- **imap**: Charge volume for Internet Message Access Protocol (IMAP)
- **ip**: Charge volume for IP
- **mms**: Charge volume for MMS
- **pop3**: Charge volume for POP3
- **pptp**: Charge volume for PPTP
- **rtcp**: Charge volume for RTCP
- **rtp**: Charge volume for RTP
- **rtsp**: Charge volume for RTSP
- **sdp**: Charge volume for SDP
- **secure-http**: Charge volume for secure-https
- **sip**: Charge volume for SIP
- **smtp**: Charge volume for SMTP
- **tcp**: Charge volume for TCP
- **tftp**: Charge volume for TFTP
- **udp**: Charge volume for UDP
- **wsp**: Charge volume for WSP
- **wtp**: Charge volume for WTP

**bytes**

Sets charge volume for bytes.

**packet-length**

Sets charge volume for packet length.

### packets

Sets charge volume for packets.

### constant *fixed_value*

This sets the fixed increment value for charging.

*fixed_value* is the value set for charging, and must be an integer from 0 through 65535.

If **constant** *3* is configured for every invocation of this Charging Action, the system adds 3 to the downlink/uplink volume counter, depending on the direction of packet.

## Usage Guidelines

This command provides the method for charging volume calculation for different protocols and packets.

For information on supported protocols see the *ACS Ruledef Configuration Mode Commands* chapter.

If **charge-volume rtp packets** is configured, system computes volume amounts for different options for RTP as follows:

| Volume | Description |
|---|---|
| Volume amount | Total (downlink and uplink) RTP packets |
| Volume amount uplink | Uplink RTP packets |
| Volume amount downlink | Downlink RTP packets |
| Volume amount uplink packets | Uplink RTP packets |
| Volume amount downlink packets | Downlink RTP packets |
| Volume amount uplink bytes | Uplink RTP bytes |
| Volume amount downlink bytes | Downlink RTP bytes |

**Important** Whenever service counts volume, it counts all packets that the relevant analyzers accepted.

**Important** If a TCP packet is routed to the HTTP analyzer but there is no HTTP payload, then the TCP statistics will be updated but the HTTP statistics will not be updated (except for the "packets ignored by the HTTP analyzer" statistic).

### Example

Following command sets the charging volume of downlink packets for RTP:

```
charge-volume rtp packets downlink
```

# content-filtering processing server-group

This command allows you to enable/disable Category-based Content Filtering.

**Product**

CF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* **> charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

```
content-filtering processing server-group
{ default | no } content-filtering processing
```

**default**

Configures this command with its default setting.

Default: Content filtering configured for the rulebase is attempted

**no**

Specifies to bypass content filtering.

This configuration should only be specified for charging actions that are performed when known safe sites are being accessed.

**Usage Guidelines**

Use this command to enable or disable Category-based Content Filtering in the charging action.

This command works as second-level filter to process the HTTP/WAP GET request with Internet Content Adaptation Protocol (ICAP) after ruledef matching. The first-level filtering is in the rulebase configuration. This CLI command is only effective when the **content-filtering mode server-group** command is configured in the rulebase.

**Example**

The following command enables content filtering in the current charging action:

```
content-filtering processing server-group
```

# content-id

This command allows you to specify the content ID to use in the generated billing records, as well as the AVP used by the Credit Control Application, such as the "Rating-Group" AVP for use by the Diameter Credit Control Application (DCCA).

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* > **charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**content-id** *content_id*
**no content-id**

**no**

Removes the content ID configuration from the charging action.

***content_id***

Specifies the content ID for credit control service.

In 12.1 and earlier releases *content_id* must be an integer from 1 through 65535.

In 12.2 and later releases, *content_id* must be an integer from 1 through 2147483647.

**Usage Guidelines** This command specifies an optional content ID to use in the generated billing records. This identifier assists the carrier's billing post processing and also used by credit-control system to use independent quotas for different value of **content-id**.

If the specified ruledef uses the **if-protocol** command to select a value for content ID, then the *content_id* specified through this command is not used for billing record generation.

**Important** For more information on **content-id**, refer to the **if-protocol** command in the *ACS Ruledef Configuration Mode Commands* chapter.

**Example**

The following command sets the content ID in the current charging action to *23*:

```
content-id 23
```

# deactivate-predefined-rule

This command allows you to remove or deactivate the matched predefined rule/Group of Ruledefs (activated by PCRF via Gx) that selected this action to ensure one time redirection for the subscriber.

**Product** GGSN, P-GW

**Privilege** Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* > **charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**[ default | no ] deactivate-predefined-rule**

**default**

Configures this command with its default setting.

Default: Disabled; same as **no deactivate-predefined-rule**

**no**

If previously enabled, disables the predefined rule in the current charging action.

**Usage Guidelines**

Use this command to ensure that the predefined rule/Group of Ruledefs gets deactivated after applying the charging-action when configured. By default, the configuration is disabled. Static rules are not deactivated by this command.

This feature is added in the ECSv2 to redirect traffic when quota for a user expires. When quota expires, PCRF will install a rule for the redirection. In the charging-action for this redirection rule, an action to disable the same rule will ensure one time redirection. A charging-rule-report will be sent to PCRF indicating the PCC Rule Status as INACTIVE for the deactivated rule. Rule-Failure-Code sent is RESOURCE_ALLOCATION_FAILURE.

The deactivation will apply only for predefined rules/Group of Ruledefs. If a static rule is associated with the charging-action, it will not be deactivated.

# edns format

**Important** This is a licensed controlled feature. Contact your Cisco account representative for detailed information on specific licensing requirements.

This CLI command associates the device-id's with the security profiles to be applied. If any of the associated formats is not configured or the configured field value is not available for encoding, then the DNS request is sent unchanged and no EDNS translation is performed.

**Product**

P-GW

SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* > **charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

## Syntax Description

**`[ no ] edns format`** *`edns_format_name`* **`{ security-profile`** *`profile_name`* **`{ encryption rc4md5 encrypted key`** *`key_string`* **`} }`**

### no

If previously configured, deletes the specified EDNS Format configuration.

### edns-format

Enables EDNS format configuration.

### *format_name*

Defines the name of EDNS field or EDNS format.

### security-profile

Defines the security profile configuration in the EDNS to add mapping with the device-id.

### *security_profile_name*

Defines the name of the security profile. This is a string of size 1 to 50.

### encryption

Encrypts the EDNS header fields.

**Important** rc4md5 is hardcoded value as currently, encryption is not supported.

### encryption-key

Designates use of encryption.

### *key*

Defines key used to encrypt EDNS header fields. This is string of size 1 to 255.

## Usage Guidelines

Use this command to associate the device-id's with the security profiles to be applied. If any of the associated formats is not configured or the configured field value is not available for encoding, then the DNS request is sent unchanged and no EDNS translation is performed.

### Example

The following command associates the device-id's with the security profiles to be applied.:

```
edns format f1 security-profile s1 encryption rc4md5 encrypted key k1
```

# end

Exits the current configuration mode and returns to the Exec mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

Exits the current mode and returns to the parent configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

**Usage Guidelines** Use this command to return to the parent configuration mode.

# flow action

This command allows you to specify the action to take on packets that match rule definitions.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* **> charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-charging-action)#`

**Syntax Description** In StarOS 12.2 and later releases:

**flow action { conditional user-agent end-token** *end_token_name* **| discard [ downlink | uplink ] | random-drop interval** *interval_start* **to** *interval_end* **pkts-to-drop** *packet_min* **to** *packet_max* **| readdress [ [ server** *ipv4_address/ipv6_address* **[ discard-on-failure ] [ dns-proxy-bypass ] ] [ port** *port_number* **[ discard-on-failure ] [ dns-proxy-bypass ] ] | server-list** *server_list_name* **[ hierarchy ][ round-robin ] [ dns-proxy-bypass ] [ discard-on-failure ] ] | redirect-ocs-url | redirect-url** *redirect_url* **[ [**

**encryption { blowfish128 | blowfish64 }| { { aes128 | aes256 } [salt] } } [ encrypted ] key** *key* **] [ clear-quota-retry-timer ] [ first-request-only [ post-redirect { allow | discard | terminate } ] ] ] | rulebase-change** *rulebase_name* **| terminate-flow | terminate-session | url-readdress server** *ipv4_address* **[ port** *port_number* **] }**
**no flow action**

In StarOS 12.1 and earlier releases:

**flow action { conditional user-agent end-token** *end_token_name* **| discard [ downlink | uplink ] | random-drop interval** *interval_start* **to** *interval_end* **pkts-to-drop** *packet_min* **to** *packet_max* **| redirect-url** *redirect_url* **[ clear-quota-retry-timer ] | readdress [ server** *ipv4_address/ipv6_address* **] [ port** *port_number* **] | terminate-flow | terminate-session }**
**no flow action**

**no**

If previously configured, deletes the flow action configuration in the current charging action.

**conditional user-agent end-token *end_token_name***

Specifies to conditionally redirect the HTTP packets matched to a configured user-agent to a specified URL. The user agent is configured using the **redirect user-agent** command in the ACS Configuration Mode.

*end_token_name* must be an alphanumeric string of 1 through 32 characters, and is configured with this command to end the redirection condition.

**discard [ downlink | uplink ]**

Specifies to discard the specified packets.

- **downlink**: Downlink packets
- **uplink**: Uplink packets

If **downlink** or **uplink** keyword is not specified, both downlink and uplink packets will be discarded.

**random-drop interval *interval_start* to *interval_end* pkts-to-drop *packet_min* to *packet_max***

Specifies to drop a group of consecutive packets (**pkts-to-drop**) to be dropped in the specified time interval (**random-drop interval**). This will cause degradation in user experience. P2P VoIP would need more than one packet to be dropped, since that type of protocol is geared to handle occasional single packet drops.

- **random-drop interval** *interval_start* **to** *interval_end*: Specifies the random drop interval, in seconds, at which the voice packets will be dropped.

  *interval_start* and *interval_end* must be integers from 1 through 999.

- **pkts-to-drop** *packet_min* **to** *packet_max*: Specifies the number of voice packets to be dropped at a time in a flow when the packets have to be dropped.

  *packet_min* and *packet_max* must be integers from 1 through 100.

**readdress [ [ server *ipv4_address/ipv6_address* [ discard-on-failure ] [ dns-proxy-bypass ] ] [ port *port_number* [ discard-on-failure ] [ dns-proxy-bypass ] ] | server-list *server_list_name* [ hierarchy ][ round-robin ] [ discard-on-failure ] [ dns-proxy-bypass ] ]**

Specifies to readdress the location of the uplink packets for charging action.

- **server** *ipv4_address/Ipv6*: Specifies the re-address server's IPv4/IPv6 address.
- **port** *port_number*: Specifies the re-address server's port number.

  *port_number* must be an integer from 1 through 65535.

  **Important** You can optionally keep the original destination address and just change the destination TCP/UDP port number.

- **server-list** *server_list_name*

  **Important** This option is available only in StarOS 14.1 and later releases.

  This keyword is license dependent. For more information please contact your Cisco account representative.

  Specifies to readdress the packet flow to the DNS servers configured under the server list.

  For more information about configuring the server list, see the *ACS Readdress Server List Configuration Mode* chapter.

- **hierarchy**

  Specifies the hierarchy approach to select the server list from the readdress server list.

- **round-robin**

  Specifies the round-robin approach to select the server list from the readdress server list. This is the default approach.

- **discard-on-failure**

  **Important** This option is available only in StarOS 14.0 and later releases.

  Specifies to discard the packets if readdressing fails due to duplicate key. If this keyword is not configured, no action is taken and the packets are allowed to pass.

  If already configured, to revert the behavior, configure the **flow action readdress** command again without the **discard-on-failure** keyword.

- **dns-proxy-bypass**

  **Important** This option is available only in StarOS 12.3 and later releases.

Specifies the DNS packets to bypass interception at the session manager when readdressing for flow occurs, and go through ECS-based DNS redirection. If this keyword is not configured, DNS redirection from ECS is disabled.

**redirect-ocs-url**

**Important** This option is available only in StarOS 12.3 and later releases.

Specifies to redirect to the URL provided by OCS only for post-processing dynamic rules.

**redirect-url *redirect_url* [ [ encryption { blowfish128 | blowfish64 } | { { aes128 | aes256 } [salt] } } [ encrypted ] key *key* ] [ clear-quota-retry-timer ] [ first-request-only [ post-redirect { allow | discard | terminate } ] ] ]**

Specifies to return a redirect response to the subscriber, and terminate the TCP connections (to the subscriber and server). The subscriber's Web browser should automatically send the original HTTP packet to the specified URL. Redirection is only possible for certain types of HTTP packets (for example, GET requests), which typically are only sent in the uplink direction. If the flow is not HTTP, the **redirect-url** option is ignored, that is the packet is forwarded normally, except for SIP. For SIP, a Contact header with the redirect information is inserted.

The redirect-url consists of the redirect url and may additionally include one or more dynamic fields. Earlier, the dynamic fields could be encrypted using 128 and 256 bit blowfish encryption. The new functionality provides the additional AES-CBC encryption ofthe dynamic fields as well.

- *redirect_url* specifies the redirect URL. *redirect_url* must be an alphanumeric string of 1 through 511 characters. It may include one or more dynamic fields (up to 16 may be specified). For example, *http://search.com/subtarg=#HTTP.URL#*.

  Dynamic fields must be enclosed in "#" (hash).

  Up to 16 dynamic fields out of the following 23 are allowed:

  - #BEARER.CALLED-STATION-ID#
  - #BEARER.CALLING-STATION-ID#
  - #BEARER.NAS-IP-ADDRESS#
  - #BEARER.USER-NAME#
  - #BEARER.ACCT-SESSION-ID#
  - #BEARER.CORRELATION-ID#
  - #BEARER.RULEBASE#
  - #BEARER.SERVED-BSA-ADDR#
  - #BEARER.SERVICE-NAME#
  - #BEARER.SUBSCRIBER-ID#
  - #BEARER.MSISDN#
  - #HTTP.URL#

- #HTTP.URI#
- #HTTP.HOST#
- #RTSP.URI#
- #WSP.URL#
- #CONTENT-ID-LABEL#
- #CONTENT-ID-LABEL-CAUSING-REDIRECTION#
- #BEARER.HWID#
- #BEARER.IMSI#
- #BEARER.IMEI#
- #BEARER.ESN#
- #BEARER.MEID#

Concatenated fields separated by ; (semi colon) can also be inserted. For example, #BEARER.IMSI;BEARER.IMEI#

- **encryption { blowfish128 | blowfish64 }** [ | **{ { aes128 | aes256 } [salt] } }encrypted ] key** *key*

**Important** This option is available only in StarOS 12.2 and later releases.

  - **encryption**: Specifies to enable encryption for dynamic fields of the redirect URL.
    - **blowfish128**: Specifies to use Blowfish encryption with 128 bit key for encrypting the dynamic fields.
    - **blowfish64**: Specifies to use Blowfish encryption with 64 bit key for encrypting the dynamic fields.
    - **aes128**: Specifies to use AES-CBC encryption with 128 bit key for encrypting the dynamic fields
    - **aes256**: Specifies to use AES-CBC encryption with 256 bit key for encrypting the dynamic fields.
    - **salt**: Specifies to use salt with AES-CBC encryptions of the dynamic fields.
  - **encrypted**: Specifies to encrypt the key.
  - **key** *key*: Specifies the key to use for encryption of dynamic fields.

    *key* must be an alphanumeric string of 1 through 523 characters.

Note that encryption is supported only for the following fields:

- #BEARER.CALLING-STATION-ID#
- #BEARER.MSISDN#
- #BEARER.IMEI#

- #BEARER.MEID#
- #BEARER.IMSI#
- #BEARER.USERNAME#
- #BEARER.ESN#

Also, concatenated fields having any of the above will be encrypted.

%3furl= can be used as a delimiter between URL. As in http://search.com/subtarg/%3furl=#HTTP.URL# format.

- **clear-quota-retry-timer**: Specifies to reset Credit Control Application (CCA) Quota Retry Timer upon redirection.
- **first-request-only [ post-redirect { allow | discard | terminate } ]**

**Important** This option is available only in StarOS 12.3 and later releases.

  - **first-request-only**: Specifies the url-redirection to be performed only once per session after the first web traffic has been detected.
  - **post-redirect**: Specifies the action to be taken on subsequent flow packets that invoke this charging action after the first url-redirection has been performed for that session.

    The following are the different actions allowed on the flow packets:

    - **allow**: allows the packets subsequent to the first url-redirection to flow
    - **discard**: discards the packets subsequent to the first url-redirection
    - **terminate**: terminates the flow of packets on receiving packets subsequent to the first url-redirection

To disable this option if configured earlier, reuse the same **flow action redirect-url** *redirect_url* command without the **first-request-only** keyword.

**Important** Disabling the **first-request-only** keyword will not affect the existing subscriber calls.

### rulebase-change *rulebase_name*

Specifies the rulebase to change to when the charging action is applied. The new rulebase will be applied to the next packet on the call, and applied only to the current PDN.

### terminate-flow

Specifies to terminate the flow.

Terminates the TCP connection gracefully between the subscriber and external server and sends a TCP FIN to the subscriber and a TCP RST to the server. If the flow does not use TCP, this option simply discard the packets. This option is applicable only for flows that use TCP.

#### terminate-session

Specifies to terminate the session.

When a rule pointing to a charging action configured with the terminate-session keyword is hit, then the corresponding session will be terminated.

#### url-readdress server *ipv4_address* [ port *port_number* ]

Configures the URL server to re-address for the specified charging action.

- **server** *ipv4_address*: Specifies the re-address server's IPv4 address.
- **port** *port_number*: Specifies the re-address server's port number.

  *port_number* must be an integer from 1 through 65535.

## Usage Guidelines

Use this command to specify the action to take on packets, for example to discard, terminate, or redirect.

When a readdress server is configured for a charging action, the **show configuration** command will display the readdress related configuration only if server address is configured. The **show configuration verbose** command will display the readdress sever if configured, else will display "no flow action".

The redirect-url option can be used to redirect SIP requests as well. The following is a sample configuration:

```
configure
     active-charging service s1
          charging-action ca_sip_redir
               content-id 10
               flow action redirect-url sip:test@sip.org
               exit
          ruledef sip_req
               sip request packet = TRUE
               exit
          rulebase plan1
              action priority 08 ruledef sip_req charging-action ca_sip_redir

            /* other rules, routing rules for sip, etc */
               end
```

This would mean any SIP request that hits the *sip_req* ruledef, would get redirected to the url given in *ca_sip_redir*. This involves creating a redirection packet with the following response line and "Contact" header in the response.

*SIP/2.0 302 Moved Temporarily*

*302 Moved Temporarily*

Most of the header fields are copied directly from the request, so that the mandatory SIP headers are present. If content-length header was seen in the original message, it is replaced in the reply with "Content-Length: 0".

### Example

The following command sets the flow action to terminate:

```
flow-action terminate-flow
```

The following command resets quota retry timer upon redirection of flow to HTTP URL *http://search.com/?url=#http://msn.com#*:

```
flow action redirect-url http://search.com/%3url=#http://msn.com#
clear-quota-retry-timer
```

# flow idle-timeout

This command allows you to configure the maximum duration a flow can remain idle after which the system automatically terminates the flow.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* **> charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**flow idle-timeout { *idle_timeout* | flow-mapping *flow_timeout* }**
**{ default | no } flow idle-timeout [ flow-mapping ]**

#### no

Disables the idle-timeout configuration; sets the idle-timeout to 0 seconds.

#### default

Configures this command with its default setting.

Default: 300 seconds

#### idle-timeout *idle_timeout*

Specifies the maximum duration, in seconds, a flow can remain idle.

*idle_timeout* must be an integer from 0 through 86400.

#### flow-mapping *flow_timeout*

Specifies the maximum duration of flow-mapping timeout, in seconds.

*flow_timeout* must be an integer from 0 through 86400.

**Usage Guidelines** Use this command to configure the maximum duration a flow can remain idle after which the system automatically terminates the flow.

### Example

The following command configures the idle-timeout setting to *400* seconds:

```
flow idle-timeout 400
```

# flow limit-for-bandwidth

For Session Control functionality this command allows you to enable/disable bandwidth limiting and configure the uplink and downlink bandwidth limits for subscriber.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* > **charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

```
flow limit-for-bandwidth { { direction { downlink | uplink } peak-data-rate
 bps peak-burst-size bytes violate-action { discard | lower-ip-precedence
} [ committed-data-rate bps committed-burst-size bytes [ exceed-action {
discard | lower-ip-precedence } ] ] } | { id id } }
{ default | no } flow limit-for-bandwidth { direction { downlink | uplink
 } | id }
```

### no

If previously configured, disables bandwidth control traffic policing for the specified direction for the current subscriber.

### default

Configures this command with its default setting.

### direction { downlink | uplink }

Specifies the direction of flow to apply bandwidth limit:

- **downlink**: Flow of data towards subscriber.
- **uplink**: Flow of data from subscriber.

### peak-data-rate *bps*

Specifies the peak data-rate for the subscriber, in bps (bits per second).

*bps* must be an integer from 1 through 4294967295.

Default: 256000

**peak burst-size *bytes***

The peak burst size allowed, in bytes.

*bytes* must be an integer from 1 through 4294967295.

Default: 3000

**Important** It is recommended that this parameter be configured to at least the greater of the following two values: 1) three times greater than packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the "bucket" for the configured peak-data-rate.

**violate-action { discard | lower-ip-precedence }**

Specifies the action to take on packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

- **discard**: Discard the packet
- **lower-ip-precedence**: Transmit the packet after lowering the IP precedence

Default: **discard**

**committed-data-rate *bps***

The committed data rate (guaranteed-data-rate) in bits per second (bps).

In releases prior to 15.0, the committed-data-rate based policing was not effected for non-GBR bearers even if it is configured in Charging Action configuration mode. In 15.0 and later releases, the committed-data-rate policing can be implemented for both GBR bearers and non-GBR bearers. If the customer does not want to implement the committed-data-rate policing for non-GBR bearers, then the **committed-data-rate** keyword should not configured with the **flow limit-for-bandwidth** command in Charging Action configuration mode.

*bps* must be an integer from 1 through 4294967295.

Default: 144000

**committed-burst-size *bytes***

The committed burst size allowed, in bytes.

*bytes* must be an integer from 1 through 4294967295.

Default: 3000

**exceed-action { discard | lower-ip-precedence }**

The action to take on the packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:

- **discard**: Discard the packet

- **lower-ip-precedence**: Transmit the packet after lowering the ip-precedence

If exceed-action is not configured, the packets are forwarded.

Default: **lower-ip-precedence**

**id *id***

**Important** This option is available only in StarOS 8.1 and later releases.

Specifies the bandwidth limiting identifier.

*id* must be an integer from 1 through 65535.

This identifier enables traffic policing based on a separate identifier other than content ID. This identifier will always take priority over content ID. If this identifier is not configured, traffic policing will be based on the content ID.

## Usage Guidelines

Use this command to limit the bandwidth a subscriber uses in the uplink and downlink directions under Session Control.

**Important** If the exceed/violate action is set to "lower-ip-precedence", the TOS value for the outer packet becomes "best effort" for packets that exceed/violate the traffic limits regardless of what the **ip user-datagram-tos copy** command is configured to. In addition, the **lower-ip-precedence** option may also override the **ip qos-dscp** command configuration. Therefore, it is recommended that command not be used when specifying this option.

More information on the QoS feature is available in the *QoS Management* appendix of the *System Administration Guide*.

### Example

The following command sets an uplink peak data rate of *128000* bps and lowers the IP precedence when the committed-data-rate and the peak-data-rate are exceeded:

```
flow limit-for-bandwidth uplink peak-data-rate 128000 violate-action
lower-ip-precedence
```

The following command sets a downlink peak data rate of *256000* bps and discards the packets when the committed-data-rate and the peak-data-rate are exceeded:

```
flow limit-for-bandwidth downlink peak-data-rate 256000 violate-action
discard
```

# flow limit-for-flow-type

Use this command to specify the maximum number of similar flows that match the charging action, and the action to take if the limit is reached.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* > **charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**flow limit-for-flow-type** *limit* **over-limit-action { discard | redirect-url** *url* **| terminate-flow | terminate-session }**
**no flow limit-for-flow-type**

**no**

If previously configured, deletes the flow limit-for-flow-type configuration in the current charging action.

***limit***

Specifies the maximum number of flows of a type exceeding which the specified over-limit-action triggers.

*limit* must be an integer from 1 through 4000000000.

**over-limit-action { discard | redirect-url *url* | terminate-flow | terminate-session }**

Specifies the action to take on exceeding *limit* for a flow type:

- **discard**: Discards the packets
- **redirect-url** *url* : Redirects the flow to the specified URL. *url* must be an alphanumeric string of 1 through 511 characters. For example, http://search.com.
- **terminate-flow**: Terminates the flow to which this packet belongs
- **terminate-session**: Terminates the session to which this packet belongs

**Usage Guidelines**

Use this command to specify the number of simultaneous flows (of a type) that a subscriber may have, and the action to take if the limit is reached.

All flows with the same content-id are considered to be the same type. This limit applies to the total of all flows for a subscriber connection (that is, an individual PDP context or individual A10 tunnel).

If the flow is not HTTP, the **redirect-url** option is ignored, that is the packet is forwarded normally. Refer to the **flow action** CLI command.

If the limit specified by the **flow limit-across-applications** command in the Rulebase Configuration Mode is also exceeded, action is taken for that over-limit condition rather than the action configured here.

**Example**

The following command terminates the flow if total number of flows of a type exceeds *1024*:

**flow limit-for-flow-type 1024 over-limit-action terminate-flow**

# flow tethering-detection

This command allows required caching from DNS flows when the DNS-based tethering detection is configured.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* > **charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**`[ no ] flow tethering-detection dns-based host-table caching`**

**no**

If previously configured, deletes the specified configuration in the current charging action.

**dns-based**

Enables DNS-based tethering options.

**host-table**

Enables DNS-based tethering host table operations.

**caching**

Enables DNS-based tethering host table caching.

**Usage Guidelines**

Use this command to allow required caching from DNS flows to be done when the DNS-based tethering detection is enabled and required.

# ip tos

This command allows you to configure the IP Type of Service (ToS) octets.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* > **charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

## Syntax Description

```
ip tos { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 |
af41 | af42 | af43 | be | ef | lower-bits tos_value } [ uplink | downlink
]
{ default | no } ip tos [ uplink | downlink ]
```

### default

Configures this command with its default setting.

Default: IP ToS is not modified.

### no

If previously configured, deletes the IP ToS configuration in the current charging action.

### af *xx*

Specifies the use of an assured forwarding *xx* per hop behavior (PHB).

### be

Specifies the use of best effort forwarding PHB.

### ef

Specifies the use of expedited forwarding PHB.

### lower-bits *tos_value*

**Important** In StarOS 8.1 and later releases, this option is "**lower-bits** *tos_value*". In StarOS 8.0, it is *tos_value*.

Specifies the least-significant 6 bits in the TOS byte with the specified numeric value.

*tos_value* must be an integer from 0 through 63.

### downlink

Specifies the ToS only for downlink packets.

### uplink

Specifies the ToS only for uplink packets.

## Usage Guidelines

Use this command to specify the IP Type of Service (ToS) octets to use in the charging action. If one of the enumerated values is set, the DSCP bits which are the six most-significant bits in the TOS byte are marked. If the integer value is set, it will be written into the six least-significant bits of the TOS byte.

If **downlink** or **uplink** keywords are not specified, the command applies to both directions.

This command may be used multiple times. For example, the following sequence of commands will cause to set the ToS to af11 in the uplink direction, but not modify the ToS in the downlink direction:

```
ip tos af11
no ip tos downlink
```

### Example

The following command sets the IP ToS to *be* with *downlink*:

```
ip tos be downlink
```

# ip vlan

This command allows you to configure the VLAN identifier to be associated with the subscriber traffic in the destination context.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* **> charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**ip vlan** *vlan_id*
**{ default | no } ip vlan**

#### default

Configures this command with its default setting.

Default: Disable this IP VLAN configuration. Same as **no ip vlan** command.

#### no

If previously configured, deletes the IP VLAN configuration in the current charging action. Whatever value is configured for the VLAN tag in the subscriber configuration or IP pool configuration (or no VLAN tag if there is no configuration elsewhere) is used.

#### *vlan_id*

Specifies the VLAN ID.

*vlan_id* must be an integer from 1 through 4094.

**Usage Guidelines**

This command configures the subscriber VLAN ID which is used with the assigned address for the subscriber session to receive packets. If the IP pool from which the address is assigned is configured with a VLAN ID, then this subscriber configured VLAN ID overrides it.

Subscriber traffic can be routed to specific VLANs based on the configuration of their user profile. Using this functionality provides a mechanism for routing all traffic from a subscriber over the specified VLAN. All packets destined for the subscriber must also be sent using only IP addresses valid on the VLAN or they will be dropped.

### Example

The following command sets the IP VLAN range to go up to *500*:

```
ip vlan 500
```

The following command sets the IP VLAN range back to default.

```
default ip vlan
```

# nexthop-forwarding-address

This command allows you to configure the nexthop forwarding address.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* **> charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**nexthop-forwarding-address** *ipv4_address*
**no nexthop-forwarding-address**

#### no

If previously configured, deletes the nexthop-forwarding-address configuration in the current charging action.

#### *ipv4_address*

Specifies the nexthop-forwarding-address for the current charging action.

*ipv4_address* must be the nexthop forwarding address, and must be an IPv4 address.

**Usage Guidelines**

Use this command to configure the nexthop-forwarding-address for a charging action. When an uplink packet matches a rule and a charging action is applied to it this nexthop forwarding address is used.

There are different methods to configure a nexthop forwarding address, they are prioritized as follows:

- The nexthop forwarding address, if configured, in a redirect ACL is used
- Else, the nexthop address configured in the charging action is used
- Else, the nexthop address, if configured, in the IP pool is used

### Example

The following command sets the nexthop forwarding address for the current charging action to *10.1.1.1*:

```
nexthop-forwarding-address 10.1.1.1
```

# pco-custom1

This command configures the Protocol Configuration Options (PCO) value that will be sent to all UEs, and relates to the PCO for UE Notification feature.

**Product**

P-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* > **charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**pco-custom1** *custom1_value*
**{ no | default } pco-custom1**

**default**

Configures custom1 with the default setting.

Default: 0

**no**

If previously configured, resets the pco-custom1 value to the default setting.

***custom1_value***

Specifies the PCO custom1 value.

*custom1_value* must be an integer from 0 through 255.

**Usage Guidelines**

Use this command to configure the PCO custom1 value to be sent to the MS GTP messages. To enable or disable sending customized PCO options, use the **pco-options** command in the APN Configuration Mode.

**Example**

The following command configures PCO custom1 value to 5:

```
pco-custom1  5
```

# pco-custom2

This command configures the Protocol Configuration Options (PCO) value that will be sent to all UEs, and relates to the PCO for UE Notification feature.

**Product**

- GGSN
- P-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* **> charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**pco-custom2** *custom2_value*

***custom2_value***

Specifies the PCO custom2 value.

*custom2_value* must be an integer from 0 through 255.

**Usage Guidelines**

Use this command to configure the PCO custom value to be sent to the MS GTP messages. To enable or disable sending customized PCO options, use the **pco-options** command in the APN Configuration Mode.

**Example**

The following command configures PCO custom2 value to 5:

```
pco-custom2  5
```

# pco-custom3

This command configures the Protocol Configuration Options (PCO) value that will be sent to all UEs, and relates to the PCO for UE Notification feature.

**Product**

- GGSN
- P-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* **> charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**pco-custom3** *custom3_value*

***custom3_value***

Specifies the PCO custom3 value.

*custom3_value* must be an integer from 0 through 255.

**Usage Guidelines**

Use this command to configure the PCO custom value to be sent to the MS GTP messages. To enable or disable sending customized PCO options, use the **pco-options** command in the APN Configuration Mode.

**Example**

The following command configures PCO custom3 value to 6:

```
pco-custom3  6
```

# pco-custom4

This command configures the Protocol Configuration Options (PCO) value that will be sent to all UEs, and relates to the PCO for UE Notification feature.

**Product**

- GGSN
- P-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* > **charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**pco-custom4** *custom4_value*

***custom4_value***

Specifies the PCO custom4 value.

*custom4_value* must be an integer from 0 through 255.

**Usage Guidelines**

Use this command to configure the PCO custom value to be sent to the MS GTP messages. To enable or disable sending customized PCO options, use the **pco-options** command in the APN Configuration Mode.

**Example**

The following command configures PCO custom4 value to 7:

```
pco-custom4  7
```

# pco-custom5

This command configures the Protocol Configuration Options (PCO) value that will be sent to all UEs, and relates to the PCO for UE Notification feature.

**Product**

- GGSN
- P-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* **> charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**pco-custom5** *custom5_value*

***custom5_value***

Specifies the PCO custom5 value.

*custom5_value* must be an integer from 0 through 255.

**Usage Guidelines**

Use this command to configure the PCO custom value to be sent to the MS GTP messages. To enable or disable sending customized PCO options, use the **pco-options** command in the APN Configuration Mode.

### Example

The following command configures PCO custom5 value to 8:

```
pco-custom5  8
```

# product-offer-id-avp

This command enables sending the "Product-Offer-ID" AVP with traffic identifier for Home Agent (HA)/Content Charging Gateway (CCG) instead of the "Rating-Group" AVP. This allows to identify and report application service traffic interval or volume.

**Important** This command is customer-specific. For more information please contact your Cisco account representative.

**Product**

HA

PDSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* **> charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**product-offer-id-avp**

**Usage Guidelines**

Use this command to send the "Product-Offer-ID" AVP in Diameter message instead of the "Rating-Group" AVP for HA/CCG implementation. This implementation means that HA/CCG is deployed to work with both AAA server and OCS via Diameter Gy Online Charging Protocol for content based billing on both offline and online charging.

**Important**

If there is no mapping label configured for a content-id with the **label content-id** command in Active Charging Service Configuration Mode, the rating group will be sent in Product-Offer-ID AVP as Label.

# qos-class-identifier

This command allows you to configure the QoS Class Identifier (QCI).

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* **> charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**qos-class-identifier** *qos_class_identifier*
**no qos-class-identifier**

**no**

If previously configured, deletes the QCI configuration in the current charging action.

***qos_class_identifier***

Specifies the QCI.

*qos_class_identifier* must be an integer from 1 through 9 or from 128 through 254 (Operator specific).

**Usage Guidelines**

Use this command to configure the QCI for a charging action.

### Example

The following command configures the QCI as *3*:

```
qos-class-identifier 3
```

# qos-renegotiate

This command allows you to configure the QoS traffic class for the Layer 7 QoS Renegotiation feature, enabling the triggering of QoS renegotiation from a rule.

**Important** This command is license dependent. For more information please contact your Cisco account representative.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* **> charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

```
qos-renegotiate traffic-class { background | conversational | interactive
 priority | streaming }
no qos-renegotiate
```

#### no

If previously configured, deletes the qos-renegotiate traffic-class configuration in the current charging action.

#### background

Specifies the traffic class as Background, for traffic patterns in which the data transfer is not time-critical (for example e-mail exchange).

#### conversational

Specifies the traffic class as Conversational, for traffic patterns in which there is a constant flow of packets.

#### interactive *priority*

Specifies the traffic class as Interactive, for traffic patterns in which there is an intermittent flow of packets.

*priority* specifies the traffic handling priority, and must be an integer from 1 through 3.

#### streaming

Specifies the traffic class as Streaming, for traffic patterns in which there is a constant flow of data in one direction, either upstream or downstream.

### Usage Guidelines

Use this command to configure the QoS traffic class for a charging action for the Layer 7 QoS Renegotiation feature, enabling triggering QoS renegotiation from an active-charging rule.

Layer 7 QoS Renegotiation is an extension of the Dynamic QoS Renegotiation feature. Upon matching a particular layer 7 rule, for example the access of a particular URL, the GGSN triggers the renegotiation of the PDP context.

#### Example

The following command sets the QoS traffic class in the charging action to streaming:

```
qos-renegotiate traffic-class streaming
```

# retransmissions-counted

This command allows you to specify whether to count (for billing purposes) the number of packet retransmissions.

### Product

**Important** In release 17.0, this command has been deprecated. This configuration is available at rulebase level as **[local]host_name(config-rule-base)# [no] retransmissions-counted.**

All

### Privilege

Security Administrator, Administrator

### Command Modes

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* **> charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

### Syntax Description

```
[ default | no ] retransmissions-counted
```

#### default

Configures this command with its default setting.

Default: Disabled; same as **no retransmissions-counted**

#### no

If previously enabled, disables the retransmissions-counted configuration in the current charging action.

**Usage Guidelines**

Use this command to enable counting of the number of retransmissions.

If not enabled, retransmissions are automatically detected but discounted. The retransmissions will still be analyzed by the TCP analyzer (and higher layer analyzers), but the statistics (except for the count of retransmissions) will not be updated. Also, some higher layer analyzers (MMS, SIP, WSP, and WTP) can detect retransmissions when UDP is the transport layer.

### Example

The following is an example of this command:

```
retransmissions-counted
```

# service-chain

This command associates service-chain to the charging-action.

**Product**

P-GW

SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* **> charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

```
service-chain<service_chain_name>
no service-chain
```

### no

If previously configured, deletes the service-chain configuration in the current charging action.

### service-chain

Associates service-chain with active-charging.

### *service_chain_name*

Specifies service chain name

**Usage Guidelines**

Use this command to associate service chain name with active-charging.

### Example

The following command associates service chain name with active-charging.

```
service-chain sc1
```

# service-detection

The **service-detection session-update** command enables the support for users' QoS updation by PDSN/PCEF based on service start or stop.

## Product

**Important** This command is customer specific. For more information contact your Cisco account representative.

PDSN

## Privilege

Security Administrator, Administrator

## Command Modes

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* > **charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

## Syntax Description

```
service-detection session-update qos
no service-detection session-update
```

### no

If previously configured, deletes the service-detection configuration in the current charging action.

### service-detection

Detects start or end of service on PDSN

### session-update

Updates the subscriber session

### qos

Sets qos updation (upgrade/downgrade)

## Usage Guidelines

Use this command to configure the service detection to enable the support for users' QoS updation by PDSN/PCEF based on service start or stop.

### Example

The following command configures service detection for a subscriber session and sets the QoS updation.

```
service-detection session-update qos
```

# service-identifier

This command allows you to configure the service identifier to use in the generated billing records, as well as the AVP used by the Credit Control Application, such as the "Service-Identifier" AVP for use by DCCA. This is a more general classifier than content-id.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* **> charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**service-identifier** *service_id*
**no service-identifier**

**no**

If previously configured, deletes the service ID configuration in the current charging action.

***service_id***

Specifies the service identifier.

In 12.1 and earlier releases *service_id* must be an integer from 1 through 65535.

In 12.2 and later releases, *service_id* must be an integer from 1 through 2147483647.

**Usage Guidelines**

Use this command to configure the service identifier to use in generated billing records, as well as the AVP used by the Credit Control Application, such as the "Service-Identifier" AVP for use by DCCA. This is a more general classifier than content-id.

**Example**

The following command configures the service identifier in the current charging action to *99*:

```
service-identifier 99
```

# stripurl token

This command allows you to configure the token and value to be stripped from the HTTP URL.

**Important**

In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

**Product** MVG

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* **> charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

```
stripurl token token_name [ value token_value ]
no stripurl
```

**no**

If previously configured, disables the URL stripping configuration in the current charging action

**token *token_name***

Specifies the name of the token to be stripped from the URL. The **stripurl token** command is case-sensitive. Hence if the token name does not match, then charging action will not be applied.

*token_name* must be an alphanumeric string of 1 through 127 characters.

**value *token_value***

Specifies the value of the token to be stripped from the URL.

*token_value* must be an alphanumeric string of 1 through 127 characters.

**Usage Guidelines** Use this command to configure the token and value to be stripped from the HTTP URL.

**Example**

For the given URL: *http://www.videoserver.com?Name1=val1&Name2=val2&Name3=val3*, if the following CLI is used, this will strip parameter *Name2*and its optional value *val2* from the above URL and gives the following new URL: *http://www.videoserver.com?Name1=val1&Name3=val3*:

```
stripurl token Name2 value val2
```

# tft packet-filter

This command allows you to specify the packet filter to use in TFTs sent to the MS.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* **> charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**[ no ] tft packet-filter** *packet_filter_name*

**no**

If previously configured, removes the specified packet filter from the current charging action.

***packet_filter_name***

Specifies the packet filter to add/remove from the current charging action.

*packet_filter_name* must be the name of a packet filter, and must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to configure the packet filter to be sent to the MS. Up to eight packet filters can be specified in a charging action.

**Example**

The following command configures the packet filter *filter23* to be sent to the MS:

```
tft packet-filter filter23
```

# tft-notify-ue

This command allows you to to control whether TFT updates are sent to UE or not.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* **> charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**[ no ] tft-notify-ue**

**no**

If this option is configured, TFTs for that charging action are not sent to UE if certain trigger conditions are met.

**Usage Guidelines**

Use this command to suppress the selected TFT updates from being sent to the UE. This helps to identify if the appropriate TFT defined in the charging action needs to be sent to the UE or not. This CLI command is supported for both default and dedicated bearers.

The ability to include TFTs in the initial session creation are also controlled through this command. This way, the operator can suppress any unwanted TFTs to the UE.

Releases prior to 15.0, all predefined rules charging actions are associated with TFTs and the system includes TFTs towards the UE for all scenarios. In some scenarios it results in creating duplicate TFTs. This CLI-based approach is developed to overcome this situation.

NOTE: The TFT updates are not sent to UE based on certain trigger conditions.

# throttle-suppress

This command allows you to suppress bandwidth limiting at charging-action, bearer, and APN level.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* **> charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**throttle-suppress [ timeout** *suppress_timeout* **]**
**no throttle-suppress**

**no**

If configured, bandwidth limiting will continue from the next flow onwards.

**timeout *suppress_timeout***

Specifies the time for which bandwidth limiting is suppressed, in seconds.

*suppress_timeout* must be an integer from 10 through 300.

Default: 30 seconds

**Usage Guidelines**

Use this command to suppress bandwidth limiting (throttling) at charging-action, bearer, and APN level. When **throttle-suppress** is configured, the timeout will take the default value of 30 seconds and the flow will not be throttled for the next 30 seconds. When configured with the **timeout** keyword, bandwidth limiting is suppressed for the mentioned time.

### Example

The following command suppresses the flow (PDP context) for the next 155 seconds when traffic hits the charging-action:

```
throttle-suppress timeout 155
```

# tos

This command allows you to configure the Type of Service (ToS) octets.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* > **charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**tos { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef | lower-bits** *tos_value* **} [ downlink | uplink ]**
**no tos [ downlink | uplink ]**

**no**

Disables the ToS being used in the charging action.

**af *xx***

Specifies the use of an assured forwarding *xx* Per Hop Behavior (PHB).

**be**

Specifies use of Best Effort forwarding PHB.

**ef**

Specifies use of Expedited Forwarding PHB.

**lower-bits *tos_value***

**Important** In StarOS 8.1 and later releases, this option is "**lower-bits** *tos_value*". In StarOS 8.0 release, it is *tos_value*.

Sets the least-significant 6 bits in the ToS byte with the specified numeric value.

*tos_value* must be an integer from 0 through 63.

**downlink**

Specifies the ToS only for downlink packets.

**uplink**

Specifies the ToS only for uplink packets.

**Usage Guidelines**

Use this command to set the ToS octets used in the charging action. If one of the enumerated values is set, the Differentiated Services Code Point (DSCP) bits (the six most-significant bits (MSBs) in the ToS byte) are marked. If the integer value is set, it will be written into the six least-significant bits (LSBs) of the ToS byte.

### Example

The following command sets the ToS to *be* for downlink packets:

```
tos be downlink
```

# tpo profile

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

# video bitrate

This command allows you to specify the default target bit rate to use for the video pacing feature on the Mobile Video Gateway. This value is also used as the suggested maximum bit rate for the video optimization policy control feature.

**Important** In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

**Product**

MVG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* > **charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**[ default | no ] video bitrate** *bit_rate* **[ -noconfirm ]**

### default

Sets video bitrate to its default value.

### no

Deletes the video bit rate if previously configured.

**video bitrate *bit_rate***

Specifies the bit rate, in bits per second, at which the TCP video flow should be paced during video pacing. This value is also used as the suggested maximum bit rate for the video optimization policy control feature. For video pacing, this default bit rate is used on each video flow until the rate determination function calculates the optimal bit rate for pacing.

*bit_rate* must be an integer from 0 to 256000000.

Default: 0

**-noconfirm**

Specifies that the command must execute without prompting for confirmation.

**Usage Guidelines**

Use this command to specify the default bit rate to use for the video pacing feature, and the suggested maximum bit rate for the video optimization policy control feature.

**Example**

The following command sets the bit rate for the video flow at *300000* (300kbps):

```
video bitrate 300000
```

# video cae-readdressing

This command allows you to enable CAE (Content Adaptation Engine) re-addressing, allowing video traffic to be fetched from the CAEs in the CAE group. The CAE is an optional component of the Mobile Videoscape.

**Important** In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

**Product**

MVG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* **> charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**[ no ] video cae-readdressing [ xheader-format** *xheader_format_name* **]**

**no**

Disables CAE re-addressing if previously configured.

#### video cae-readdressing

Enables CAE re-addressing, allowing video traffic to be fetched from the CAEs in the CAE group.

#### xheader-format *xheader_format_name*

Specifies an HTTP x-header (Extension header) format for readdressing. When specified, the MVG inserts a destination IP address and TCP port number in a proprietary HTTP x-header in the HTTP request to the CAE. The CAE uses this information to connect to the OS (Origin Server) to retrieve selected video clips for adaptation.

*xheader_format_name* must be an alphanumeric string of 1 through 63 characters.

### Usage Guidelines

Use this command to enable CAE re-addressing on the Mobile Video Gateway.

#### Example

The following command enables CAE re-addressing:

```
video cae-readdressing xheader-format format_1
```

# video detailed-statistics

This command allows you to enable the collection of detailed video statistics.

**Important** In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

### Product

MVG

### Privilege

Security Administrator, Administrator

### Command Modes

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* > **charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

### Syntax Description

```
[ default | no ] video detailed-statistics [ -noconfirm ]
```

#### default

Sets video detailed-statistics to its default value, which is the same as **[ no ]**.

#### no

Disables the video statistics feature if previously enabled.

#### video detailed-statistics

Enables the video statistics feature. When a flow matches a rule definition for video during DPI (Deep Packet Inspection), the video statistics feature begins collecting detailed statistics for the video flow.

#### -noconfirm

Specifies that the command must execute without prompting for confirmation.

**Usage Guidelines**

Use this command to enable the video statistics feature.

#### Example

The following command enables the video statistics feature:

```
video detailed-statistics
```

# video optimization-preprocessing all

This command allows you to enable CAE re-addressing by enabling the Active Charging Service (ACS) to re-address video requests to the CAEs in the CAE group.

**Important** In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

**Product**

MVG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* **> charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

```
[ no ] video optimization-preprocessing all
```

#### no

Disables CAE re-addressing if currently enabled.

#### video optimization-preprocessing all

Enables CAE re-addressing by enabling the ACS to re-address video requests to the CAEs in the CAE group.

**Usage Guidelines**

Use this command to enable CAE re-addressing by enabling the ACS to re-address video requests to the CAEs in the CAE group.

### Example

The following command enables CAE re-addressing:

```
video optimization-preprocessing all
```

# video optimization-preprocessing cae-readdressing

This command allows you to enable CAE re-addressing by enabling the Active Charging Service (ACS) to re-address video requests to the CAEs in the CAE group.

**Important** In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

**Product**

MVG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* > **charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

```
[ no ] video optimization-preprocessing cae-readdressing
```

#### no

Disables CAE re-addressing if currently enabled.

#### video optimization-preprocessing cae-readdressing

Enables CAE re-addressing by enabling the ACS to re-address video requests to the CAEs in the CAE group.

**Usage Guidelines**

Use this command to enable CAE re-addressing by enabling the ACS to re-address video requests to the CAEs in the CAE group.

### Example

The following command enables CAE re-addressing:

```
video optimization-preprocessing cae-readdressing
```

# video pacing by-policing

This command allows you to enable the video pacing feature.

**Important** In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

**Product**

MVG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* > **charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**[ default | no ] video pacing by-policing [ initial-burst-duration** *value* **| normal-burst-duration** *value* **][ -noconfirm ]**

**default**

Sets video pacing by-policing to its default value, which is the same as **[ no ]**.

**no**

Deletes the video pacing by-policing settings and disables video pacing if previously configured.

**video pacing by-policing**

Enables the video pacing feature. When enabled, video pacing is applied per TCP video flow. The command syntax **by-policing** enables pacing enforcement by the policing method, which is the available method for this software release.

**initial-burst-duration *value***

Specifies the duration, in seconds, for the allowed initial burst of video content. Note that the initial burst is configured in terms of time, so that for video files with different encoding bit rates, the amount of bytes allowed without enforcing pacing gets adjusted accordingly. The amount of bytes allowed is calculated by (video encoding rate * initial-burst-duration).

*value* must be an integer between 1 and 30.

Default: 10 seconds

**normal-burst-duration *value***

Specifies the duration, in seconds, for the allowed normal burst of video content after the initial burst is completed. Like the initial burst, the normal burst is also configured in terms of time, so that for video files

with different encoding bit rates, the amount of bytes allowed without enforcing pacing gets adjusted accordingly. The amount of bytes allowed is calculated by (video encoding rate * normal-burst-duration).

*value* must be an integer between 1 and 30.

Default: 3 seconds

**-noconfirm**

Specifies that the command must execute without prompting for confirmation.

**Usage Guidelines**

Use this command to enable video pacing by policing.

**Example**

The following command enables video pacing by policing with an initial burst duration of 15 seconds and a normal burst duration of 3 seconds:

```
video pacing by-policing initial-burst-duration 15 normal-burst-duration
 3
```

# xheader-insert

This command allows you to specify the extension-header (x-header) format whose fields have to be inserted in HTTP request packets and HTTP response packets.

**Important**

This command is license dependent. For more information please contact your Cisco account representative.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**active-charging service** *service_name* > **charging-action** *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

**xheader-insert xheader-format** *xheader_format_name* **[ encryption { rc4md5 | aes-256-gcm-sha384 [ salt ]  [ encrypted ] key** *key* **] [ first-request-only ] [ msg-type { response-only | request-and-response } ] [ -noconfirm ]**
**no xheader-insert**

}

**no**

Removes previously configured x-header format name.

### xheader-format *xheader_format_name*

Enables x-header mode configuration, and specifies the x-header format whose fields are to be inserted in the packets.

*xheader_format_name* must be the name of an x-header format, and must be an alphanumeric string of 1 through 63 characters.

### encryption rc4md5 [ encrypted ] key *key*

If the x-header format has any encrypted fields defined, specifies to use RC4MD5 encryption.

After configuring this option, the fields in xheader format having "encrypt" enabled will be encrypted as follows:

1. The MD5 hash of the configure key will be calculated.
2. This MD5 hash will be used as a key for RC4 encryption.
3. This encrypted value will be base64 encoded to get the final X-header value. The final inserted X-header will be X-alias: base64(RC4(MD5(key),MSISDN)).

In the default case, if encryption is not enabled as above, the plain text value of the xheader field will be inserted.

Note that if the value of the key is changed on the fly, it will take effect only in case of new calls. Also, if the per rulebase RSA encryption is also enabled in the same config, per charging-action RC4MD5 encryption will take precedence over it.

*key* specifies the key as an alphanumeric string of 8 through 15 characters.

**encryption** specifies use of encryption.

The *key* can be configured either as plain text or encrypted. However, in the output of the **show configuration** command it will always be displayed as encrypted. And, in the output of the **show configuration showsecrets** command it will be displayed as plain text.

### encryption aes-256-gcm-sha384 [ salt ] [ encrypted ] key *key*

Use **aes-256-gcm-sha384** option to encrypt the x-header fields with AES-256-GCM algorithm and SHA384 to hash key in 384 bits.

Use the **[ salt ]** option for enhanced security. Use this additional option by generating new key each time the x-header is encrypted.

Use **key** option to enter the key that is used to encrypt and decrypt the x-header string. The key length for AES-256-GCM-SHA384 algorithm is 32 characters, which is equal to 256 bits.

### first-request-only

Specifies x-header insertion only for the first HTTP request in the IP flow. If not configured, the default behavior is insertion for all requests.

### msg-type { response-only | request-and-response }

Specifies the extension-header (x-header) format whose fields have to be inserted in HTTP Request and Response packets.

- **response-only**: X-header will be inserted in HTTP Response packets with specified x-header format.

- **request-and-response**: X-header will be inserted in both HTTP Request and Response packets with same x-header format.

### -noconfirm

Specifies that the command must execute without any prompts and confirmation from the user.

## Usage Guidelines

Use this command to enable x-header mode, and specify the x-header format name whose fields are to be inserted in HTTP GET and POST request packets and HTTP response packets.

Also, see the **xheader-format** command in the *ACS Configuration Mode Commands* and *ACS X-header Format Configuration Mode Commands* chapters.

### Example

The following command enables x-header mode, and specifies the x-header format name as *test12* for Request message:

```
xheader-insert xheader-format test12
```

The following command sets the x-header format name *format1* for both Request and Response messages:

```
xheader-insert xheader-format format1 msg-type request-and-response
```