Enhanced Charging Service Configuration

This chapter describes how to configure the Enhanced Charging Service (ECS) functionality, also known as Active Charging Service (ACS).

The following topics are covered in this chapter:

Initial Configuration

Initial configuration includes the following:

Step 1 Install the ECS license as described in Installing the ECS License, on page 2.

Step 2 Create the ECS administrative user account as described in Creating the ECS Administrative User Account, on page 1.

Step 3 Enable ECS as described in Enabling Enhanced Charging Service, on page 2.

Step 4 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Important Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

Creating the ECS Administrative User Account

At least one administrative user account with ECS privileges must be configured on the system. This is the account that is used to log on and execute ECS-related commands. For security purposes, it is recommended that these user accounts be created along with general system functionality administration.

To create the ECS administrative user account, use the following configuration:

```
configure
  context local
    administrator <user_name> password <password> ecs
    end
```

Notes:

- Aside from having ECS capabilities, an ECS Administrator account also has the same capabilities and privileges as any other system-level administrator account.
- You can also create system ECS user account for a config-administrator, operator, or inspector. ECS accounts have the same system-level privileges of normal system accounts except that they have full ECS command execution capability. For example, an ECS account has rights to execute every command that a regular administrator can in addition to all of the ECS commands.
- Note that only Administrator and Config-administrator level users can provision ECS functionality. Refer to the *Configuring System Settings* chapter of the *System Administration and Configuration Guide* for additional information on administrative user privileges.

Installing the ECS License

The ECS in-line service is a licensed Cisco product. Separate session and feature licenses may be required. Contact your Cisco account representative for detailed information on licensing requirements.

For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Enabling Enhanced Charging Service

Enhanced charging must be enabled before configuring charging services.

To enable Enhanced Charging Service, use the following configuration:

```
configure
  require active-charging
    context local
      interface <interface_name>
        ip address <ip_address/mask>
        exit
      server ftpd
      end
```

Notes:

- The **require active-charging** command must be configured before any services are configured, so that the resource subsystem can appropriately reserve adequate memory for ECS-related tasks. After configuring this command, the configuration must be saved and the system rebooted in order to allocate the resources for ECS on system startup.

Important After you configure this command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Configuring the Enhanced Charging Service

A charging service has analyzers that define which packets to examine and ruledefs (ruledefs) that define what packet contents to take action on and what action to take when the ruledef is matched. Charging services are configured at the global configuration level and are available to perform packet inspection on sessions in all contexts.

To configure the Enhanced Charging Service:

Step 1 Create the ECS service as described in Creating the Enhanced Charging Service, on page 3.

Step 2 Configure a ruledef as described in Configuring Rule Definitions, on page 3.

Step 3 Create a charging action as described in Configuring Charging Actions, on page 5.

Step 4 Define a rulebase as described in Configuring Rulebase, on page 6.

Step 5 *Optional*. Define a rulebase list in the ACS configuration mode and configure the rulebase list in an APN, as described in Configuring Rulebase Lists, on page 7.

Step 6 *Optional*. Enable dynamic collection of ruledef statistics as described in Configuring Ruledef Statistics Collection, on page 7.

Step 7 Set EDR formats as described in Setting EDR Formats.

Step 8 Set UDR formats as described in Setting UDR Formats.

Step 9 Enable charging record retrieval as described in Enabling Charging Record Retrieval, on page 9.

Step 10 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Important Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

Creating the Enhanced Charging Service

To create an Enhanced Charging Service, use the following configuration:

```
configure
  active-charging service <ecs_service_name>
  end
```

Notes:

- In this release, only one ECS service can be created in a system.

Configuring Rule Definitions

To create and configure a ruledef use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      ruledef <ruledef_name>
         <protocol> <expression> <operator> <condition>
         rule-application { charging | post-processing | routing }
         end
```

Notes:

- If the same ruledef is to be used for charging in one rulebase and for post-processing in another, then two separate identical ruledefs should be defined.
- For information on all the protocol types, expressions, operators, and conditions supported, refer to the *ACS Ruledef Configuration Mode Commands* chapter of the *Command Line Interface Reference*.
- The **rule-application** command specifies the ruledef type. By default, if not specified, the system considers a ruledef as a charging ruledef.
- In 14.1 and earlier releases, a maximum of 10 rule expressions (rule-lines) can be added in one ruledef.

  In 15.0 and later releases, a maximum of 32 rule expressions (rule-lines) can be added in one ruledef.

Verifying your Configuration

To verify your configuration, in the Exec Mode, enter the following command:

```
show active-charging
ruledef { all | charging | name ruledef_name | post-processing | routing }
```

Configuring Group of Ruledefs

A group-of-ruledefs enables grouping rules into categories, so that charging systems can base the charging policy on the category.

To create and configure a group-of-ruledefs, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      group-of-ruledefs <ruledef_group_name>
         add-ruledef priority <priority> ruledef <ruledef_name>
         group-of-ruledefs-application { charging | content-filtering |
gx-alias | post-processing }
         end
```

Notes:

- In releases prior to 20.1: A maximum of 128 ruledefs can be added to a group-of-ruledef.

  In 20.1 and later releases: A maximum of 512 ruledefs can be added to a group-of-ruledef.
- In 14.1 and earlier releases, a maximum of 64 group-of-ruledefs can be configured.

  In 15.0 and later releases, a maximum of 128 group-of-ruledefs can be configured.

  In 20.1 and later releases, a maximum of 384 group-of-ruledefs can be configured.

Important The total number of ruledefs supported for all GoRs must be used with caution due to the high memory impact. Any modifications to the ruledef or GoR configurations beyond the WARN state of the SCT Task memory may have adverse impact on the system.

- The **group-of-ruledefs-application** command specifies the group-of-ruledef type. By default, if not specified, the system considers a group-of-ruledef as a charging group-of-ruledef.

Verifying your Configuration

To verify your configuration, in the Exec Mode, enter the following command:

```
show active-charging group-of-ruledefs name <ruledef_group_name>
```

Configuring Charging Actions

Charging actions are used with rulebases and must be created before a rulebase is configured.

To create a charging action, use the following configuration:

```
configure
  active-charging service <ecs_service_name>
    charging-action <charging_action_name>
      content-id <content_id>
      retransmissions-counted
      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 } +
      end
```

Notes:

- Up to eight packet filters can be specified in a charging action.

Verifying your Configuration

To verify your configuration, in the Exec Mode, enter the following command:

```
show active-charging charging-action name <charging_action_name>
```

Configuring IP Readdressing

Readdressing of packets based on the destination IP address of the packets enables redirecting unknown gateway traffic to known/trusted gateways. This is implemented by configuring the re-address server in the charging action.

To configure the IP Readdressing feature, use the following configuration:

```
configure
  active-charging service <ecs_service_name>
    charging-action <charging_action_name>
      flow action readdress server  ipv4_address/ipv6_address [
```

```
discard-on-failure ]  [ dns-proxy-bypass ]  [ port port_number [
discard-on-failure ] [ dns-proxy-bypass ] ]
       end
```

To configure the IP Readdressing feature when the readdress server-list is defined under charging-action, use the following configuration:

```
configure
  active-charging service service_name
    charging-action  charging_action_name
      flow action readdress server-list  server_list_name [ hierarchy ] [
round-robin ] [ dns-proxy-bypass ] [ discard-on-failure ]
       end
```

Configuring Next Hop Address

To configure the Next Hop Address configuration feature, use the following configuration:

```
configure
  active-charging service <ecs_service_name>
    charging-action <charging_action_name>
      nexthop-forwarding-address <ip_address>
      end
```

Configuring Rulebase

A rulebase specifies which protocol analyzers to run and which packets are analyzed. Multiple rulebases may be defined for the Enhanced Charging Service. A rulebase is basically a subscriber's profile in a charging service.

To create and configure a rulebase, use the following configuration:

```
configure
  active-charging service <ecs_service_name>
    rulebase <rulebase_name>
      flow end-condition { content-filtering | hagr | handoff |
normal-end-signaling | session-end | tethering-signature-change |
url-blacklisting | timeout } [ flow-overflow ] + { charging-edr
<charging_edr_format_name> | reporting-edr <reporting_edr_format_name> }
      billing-records udr udr-format <udr_format_name>
     action priority <action_priority> { [ dynamic-only | static-and-dynamic
 | timedef <timedef_name> ] { group-of-ruledefs <ruledef_group_name> | ruledef
<ruledef_name> } charging-action <charging_action_name> [ monitoring-key
<monitoring_key> ] [ description <description> ] }
      route priority <route_priority> ruledef <ruledef_name> analyzer <analyzer>
 [ description <description> ]
      rtp dynamic-flow-detection
      udr threshold interval <interval>
      cca radius charging context <context> group <group_name>
      cca radius accounting interval <interval>
      end
```

Notes:

- When R7 Gx is enabled, "static-and-dynamic" rules behave exactly like "dynamic-only" rules. That is, they must be activated explicitly by the PCRF. When Gx is not enabled, "static-and-dynamic" rules behave exactly like static rules.
- In release 20.2, the **tethering-signature-change** keyword is added to create an EDR with the specified EDR format whenever a flow ends due to tethering signature change.

Verifying your Configuration

To verify your configuration, in the Exec Mode, enter the following command:

```
show active-charging rulebase name <rulebase_name>
```

Configuring Rulebase Lists

To create a rulebase list, use the following configuration:

```
configure
  active-charging service <ecs_service_name>
    rulebase-list <rulebase_list_name> <rulebase_name>[ <rulebase_name> + ]
    exit
```

Configuring a Rulebase List in an APN

To configure the rulebase list that was created in the ACS configuration mode in an APN, use the following configuration:

```
configure
  context <context_name>
    apn <apn_name>
      active-charging rulebase-list <rulebase_list_name>
      exit
```

Verifying your configuration

To verify your configuration for the rulebase list and APN, in the Exec mode, enter the following command:

```
show configuration
```

To verify your APN configuration, in the Exec mode, enter the following command:

```
show configuration apn <apn_name>
```

Configuring Ruledef Statistics Collection

To dynamically enable ruledef statistics collection in the ACS Configuration mode, use the following configuration:

```
configure
  active-charging service <ecs_service_name>
    statistics-collection { all | ruledef { all | charging | firewall |
 post-processing } }
    [ no ] statistics-collection
    end
```

Notes:

- By default, no statistics will be maintained.
- The **[no] statistics-collection all** and **[no] statistics-collection ruledef all** commands will result in the same output.
- If the command is not configured, statistics collection will not be enabled and the following error message will be displayed in the **show active-charging sessions full** CLI — "statistics collection disabled; not collecting <*charging/firewall/postprocessing*> ruledef stats".

To dynamically enable ruledef statistics collection in the Exec mode, use the following configuration:

```
statistics-collection active-charging { all | charging | firewall |
post-processing { callid call_id | imsi imsi_number } }
[ no ] statistics-collection active-charging { callid call_id | imsi
imsi_number }
```

Notes:

- The ruledef statistics will be maintained for a bearer only if this command is configured. By default, the statistics will not be maintained.
- If the command is not configured, statistics collection will not be enabled and the following error message will be displayed in the **show active-charging sessions full** CLI — "statistics collection disabled; not collecting <*charging/firewall/postprocessing*> ruledef stats".

To view subscriber statistics, in the Exec Mode, use the following command:

```
show active-charging subscribers { acsmgr instance instance_id | all | callid
 call_id | full | imsi imsi_number | rulebase rulebase_name }
```

Setting EDR Formats

ECS generates postpaid charging data files which can be retrieved from the system periodically and used as input to a billing mediation system for postprocessing.

EDRs are generated according to action statements in rule commands.

Up to 32 different EDR schema types may be specified, each composed of up to 32 fields or analyzer parameter names. The records are written at the time of each rule event in a comma-separated (CSV) format.

Important If you have configured RADIUS Prepaid Billing, configuring charging records is optional.

To set the EDR formats use the following configuration:

```
configure
  active-charging service <ecs_service_name>
    edr-format <edr_format_name>
      attribute <attribute> { [ format { MM/DD/YY-HH:MM:SS |
MM/DD/YYYY-HH:MM:SS | YYYY/MM/DD-HH:MM:SS | YYYYMMDDHHMMSS | seconds } ]
 [ localtime ] | [ { ip | tcp } { bytes | pkts } { downlink | uplink } ]
 priority <priority> }
      rule-variable <protocol> <rule> priority <priority>
      event-label <event_label> priority <priority>
      delimiter { comma | tab }
      end
```

For information on EDR format configuration and rule variables, refer to the *EDR Format Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

Verifying your Configuration

To verify your configuration, in the Exec Mode, enter the following command:

```
show active-charging edr-format name <edr_format_name>
```

Setting UDR Formats

ECS generates postpaid charging data files which can be retrieved from the system periodically and used as input to a billing mediation system for postprocessing.

UDRs are generated according to action statements in rule commands. Up to 32 different UDR schema types may be specified, each composed of up to 32 fields or analyzer parameter names. The records are written thresholds in a comma-separated (CSV) format.

Important If you have configured RADIUS Prepaid Billing, configuring charging records is optional.

To set the UDR format, use the following configuration:

```
configure
  active-charging service <ecs_service_name>
    udr-format <udr_format_name>
      attribute <attribute> { [ format { MM/DD/YY-HH:MM:SS |
MM/DD/YYYY-HH:MM:SS | YYYY/MM/DD-HH:MM:SS | YYYYMMDDHHMMSS | seconds } ]
 [ localtime ] | [ { bytes | pkts } { downlink | uplink } ] ] priority
<priority> }
      end
```

Important For information on UDR format configuration and rule variables, refer to the *UDR Format Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

Verifying your Configuration

To verify your configuration, in the Exec Mode, enter the following command:

```
show active-charging udr-format name <udr_format_name>
```

Enabling Charging Record Retrieval

To retrieve charging records you must configure the context that stores the charging records to accept SFTP connections.

To enable SFTP, use the following configuration:

```
configure
  context local
```

```
    administrator <user_name> [ encrypted ] password <password>
    config-administrator <user_name> [ encrypted ] password <password>
    exit
  context <context_name>
    ssh generate key
    server sshd
    subsystem sftp
    end
```

Notes:

- You must specify the **sftp** keyword to enable the new account to SFTP into the context to retrieve record files.

Optional Configurations

This section describes the following optional configuration procedures:

- Configuring a Rulebase for a Subscriber, on page 10
- Configuring a Rulebase within an APN, on page 10
- Configuring Charging Rule Optimization, on page 11

Important Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

Configuring a Rulebase for a Subscriber

This section describes how to apply an existing rulebase to a subscriber. For information on how to configure rulebases, see Configuring Rulebase, on page 6.

To configure a rulebase for a subscriber, use the following configuration:

```
configure
  context <context_name>
    subscriber name <subscriber_name>
      active-charging rulebase <rulebase_name>
      end
```

Configuring a Rulebase within an APN

This section describes how to configure an existing rulebase within an APN for a GGSN. For information on how to configure rulebases, see Configuring Rulebase, on page 6.

Important This information is only applicable to GGSN networks.

To configure a rulebase in an APN, use the following configuration:

```
configure
  context <context_name>
    apn <apn_name>
      active-charging rulebase <rulebase_name>
      end
```

Configuring Charging Rule Optimization

This section describes how to configure the internal optimization level for improved performance when the system evaluates each instance of the **action** CLI command.

To configure the rule optimization level, use the following configuration:

```
configure
  active-charging service <ecs_service_name>
    rulebase <rulebase_name>
      charging-rule-optimization { high | low | medium }
      end
```

Notes:

- In StarOS 14.0 and later releases, the **charging-rule-optimization** command is deprecated. Rule optimization is always enabled with the optimization level set to high as standard behavior.
- In 11.0 and later releases, the **medium** option is deprecated.
- Both the **high** and **medium** options cause reorganization of the entire memory structure whenever any change is made (for example, addition of another **action** CLI command).
- The **high** option causes allocation of a significant amount of memory for the most efficient organization.

Configuring Service-scheme Framework

The Service Scheme configuration is required to configure and enable features such as Response-based Charging, Response-based TRM, and Location QoS Override features for a subscriber. The configuration commands described in this section can be used to configure the service-scheme framework.

The following topics are covered in this section:

Configuring Subscriber Base

To configure the Active Charging Service (ACS) subscriber base, use the following configuration:

```
configure
  active-charging service service_name
    subscriber-base subs_base_name
      priority priority subs-class subs_class_name bind service-scheme
serv_scheme_name
      end
```

Notes:

- The **priority** command is used to assign priority to the service-scheme association within a subscriber base. This priority must be unique within a subscriber base.

Configuring Subscriber Class

To configure the Active Charging Service (ACS) subscriber class, use the following configuration:

```
configure
   active-charging service service_name
      subs-class subs_class_name
         [ no ] any-match operator condition
         [ no ] apn operator apn_name
         [ no ] multi-line-or all-lines
         [ no ] rulebase operator rulebase_name
         [ no ] v-apn operator v_apn_name
         end
```

Notes:

- The **any-match** command is used to enable or disable the wildcard configuration.
- The **apn** command is used to specify the APN name as a condition.
- The **multi-line-or** command is used to check if the OR operator must be applied to all lines in a subscriber class.
- The **rulebase** command is used to specify the rulebase name as a condition.
- The **v-apn** command is used to specify the virtual APN name as a condition.

Configuring Service Scheme

To enable the association of service-scheme based on subscriber class, use the following configuration:

```
configure
   active-charging service service_name
      service-scheme service_scheme_name
         [ no ] trigger { loc-update | sess-setup }
         end
```

Notes:

- The **trigger** command is used to configure the set of trigger events such as session-setup, location-update that will be handled under the service-scheme.

Configuring Service Scheme Trigger

To configure the set of triggers that will be handled under the associated service-scheme, use the following configuration:

```
configure
   active-charging service service_name
      service-scheme service_scheme_name
         [ no ] trigger { loc-update | sess-setup }
           priority priority trigger-condition trigger_condn_name trigger-action
 trigger_action_name
          end
```

Notes:

- The **priority** command is used to assign priority to the trigger events configured in service-scheme. The priority must be unique within a trigger.

Configuring Trigger Action

To configure the Active Charging Service (ACS) trigger actions, use the following configuration:

```
configure
  active-charging service service_name
    trigger-action trigger_action_name
      [ no ] charge-request-to-response http { all | connect | delete |
 get | head | options | post | put | trace }
      [ no ] throttle-suppress
      [ no ] transactional-rule-matching response http { all | connect
| delete | get | head | options | post | put | trace }
      end
```

Notes:

- The **charge-request-to-response** command is added in support of the Response-based Charging feature to delay charging till the HTTP response for the configured HTTP request method(s).
- The **throttle-suppress** command is added in support of the Location based QoS Override feature to perform throttle suppression to provide unlimited bandwidth based on trigger condition matched.
- The **transactional-rule-matching** command is added in support of the Response-based TRM feature to delayw-c engagement of TRM till the HTTP response for the configured HTTP request method(s).

Configuring Trigger Condition

To configure Active Charging Service (ACS) trigger conditions, use the following configuration:

```
configure
  active-charging service service_name
    trigger-condition trigger_condn_name
      [ no ] any-match operator condition
      [ no ] local-policy-rule = local_policy_rule
      [ no ] multi-line-or all-lines
      end
```

Notes:

- The **any-match** command is used to analyze all flows created after event activation.
- The **local-policy-rule** command is used to specify the local-policy rule within ECS for enabling trigger condition.
- The **multi-line-or** command is used to check if the OR operator must be applied to all lines in a trigger-condition.

Verifying Service Scheme Configuration

Use the following commands in the Exec Mode to verify your configuration:

- This command is used to display the number of subscribers associated with the configured service-scheme:

  show active-charging service-scheme { all | name *serv_scheme_name* **| statistics [name** *serv_scheme_name* **] } [service name** *service_name* **] [| { grep** *grep_options* **| more }]**

- This command displays the service-scheme selected for the particular subscriber:

  show active-charging subscribers full all

- This command displays information about the trigger action(s) configured in a service.

  show active-charging trigger-action { all | name *trigger_action_name* **[service** *acs_service_name* **] } [| { grep** *grep_options* **| more }]**

- This command displays information about the trigger condition(s) configured in a service.

  show active-charging trigger-condition { { all | name *trigger_condn_name* **[service** *acs_service_name* **] } | statistics [name** *trigger_condn_name* **] } [| { grep** *grep_options* **| more }]**

Sample Configuration

Use the sample configuration to enable features based on service-scheme framework for a subscriber.

```
configure
  active-charging service s1
    subscriber-base default
      priority 10 subs-class class1 bind service-scheme scheme1
      priority 20 subs-class class2 bind service-scheme scheme2
    #exit
    subs-class class1
      apn = cisco.com
      rulebase = plan1
      v-apn != some_virtual_apn
      multi-line-or
    #exit
    subs-class class2
      any-match
    #exit
    service-scheme scheme1
      trigger sess-setup
        priority 10 trigger-condition tc1 trigger-action ta1
        priority 20 trigger-condition tc2 trigger-action ta2
      #exit
    #exit
    service-scheme scheme2
      trigger sess-setup
        priority 10 trigger-condition tc1 trigger-action ta1
      #exit
```

```
#exit
trigger-condition tc1
  any-match
#exit
trigger-action ta1
  transactional-rule-matching response http all
  charge-request-to-response http all
#exit
trigger-action ta2
  throttle-suppress
#exit
```

Configuring Enhanced Features

The configuration examples in this section are optional and provided to cover the most common uses of ECS in a live network.

The following topics are covered in this section:

Configuring Prepaid Credit Control Application (CCA)

This section describes how to configure the Prepaid Credit Control Application for Diameter or RADIUS.

Important To configure and enable Diameter and DCCA functionality with ECS, you must obtain and install the relevant license on the chassis. Contact your Cisco account representative for detailed information on licensing requirements.

Important Before configuring Diameter or RADIUS CCA, you must configure AAA parameters. For more information, if you are using StarOS 12.3 or an earlier release, refer to the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

To configure Prepaid Credit Control Application:

Step 1 Configure the Prepaid Credit Control Application for Diameter or RADIUS as described in Configuring Prepaid CCA for Diameter or RADIUS, on page 16.

Step 2 Configure the required Prepaid Credit Control Mode:

- Configuring Diameter Prepaid Credit Control Application (DCCA), on page 18
- Configuring RADIUS Prepaid Credit Control Application, on page 20

Important Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

Configuring Prepaid CCA for Diameter or RADIUS

To configure the Prepaid Credit Control Application for Diameter or RADIUS, use the following configuration:

```
configure
  active-charging service <ecs_service_name>
    charging-action <charging_action_name>
     cca charging credit [ preemptively-request | rating-group <coupon_id>
]
      exit
    credit-control [ group <group_name> ]
      mode { diameter | radius }
      quota time-threshold { <absolute_value> | percent <percent_value> }
      quota unit-threshold { <absolute_value> | percent <percent_value> }
      quota volume-threshold { <absolute_value> | percent <percent_value> }
      end
```

Notes:

- <*ecs_service_name*> must be the name of the Enhanced Charging Service in which you want to configure Prepaid Credit Control Application.
- <*charging_action_name*> must be the name of the charging action for which you want to configure Prepaid Credit Control Application.
- *Optional:* To configure the redirection of URL for packets that match a ruledef and action on quota request timer, in the Charging Action Configuration Mode, enter the following command. This command also specifies the redirect-URL action on packet and flow for Session Control functionality.

  In 12.2 and later releases: **flow action 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 }]]**

  In 12.1 and earlier releases: **flow action redirect-url** <*redirect_url*> **[clear-quota-retry-timer]**

  The following example shows the redirection of a URL for packets that match a ruledef:

```
charging-action http-redirect
   content-id 3020
   retransmissions-counted
   billing-action exclude-from-udrs
   flow action redirect-url
"http://10.1.67.214/cgi-bin/aoc.cgi077imsi=#bearer.calling-station-id#

&url=http.url#&acctsessid=#bearer.acct-session-id#&correlationid=#bearer.correlation-id#

   &username=#bearer.user-name#&ip=#bearer.served-bsa-addr#&subid=#bearer.subscriber-id#

   &host=#http.host#&httpuri=#http.uri#" clear-quota-retry-timer
   end
```

- *Optional:* To configure credit control quota related parameters, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      rulebase <rulebase_name>
         cca quota { holding-time <holding_time> content-id <content_id> |
retry-time <retry_time> [ max-retries <max_retries> ] }
         cca quota time-duration algorithm { consumed-time <consumed_time>
 [ plus-idle ] [ content-id <content_id> ] | continuous-time-periods
<seconds> [ content-id <content_id> ] | parking-meter <seconds> [ content-id
 <content_id> ] }
         end
```

<*rulebase_name*> must be the name of the rulebase in which you want to configure Prepaid Credit Control configurables.

- *Optional:* To define credit control rules for quota state and URL redirect match rules with RADIUS AVP, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      ruledef <ruledef_name>
         cca quota-state <operator> { limit-reached | lower-bandwidth }
         cca redirect-indicator <operator> <indicator_value>
         end
```

<*ruledef_name*> must be the name of the ruledef that you want to use for Prepaid Credit Control Application rules.

cca redirect-indicator configuration is a RADIUS-specific configuration.

- *Optional:* This is a Diameter-specific configuration. To configure the failure handling options for credit control session, in the Credit Control Configuration Mode, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      credit-control [ group <group_name> ]
         failure-handling { ccfh-session-timeout <session_timeout> | {
initial-request | terminate-request | update-request } { continue [
go-offline-after-tx-expiry | retry-after-tx-expiry ] |
retry-and-terminate [ retry-after-tx-expiry ] | terminate }
         end
```

- *Optional:* To configure the triggering option for credit re-authorization when the named values in the subscriber session changes, use the following configuration:

```
configure
  active-charging service <ecs_service_name>
    credit-control [ group <group_name> ]
      trigger type { cellid | lac | qos | rat | sgsn } +
      end
```

- *Optional:* This is a Diameter-specific configuration. If the configuration is for 3GPP network, to configure the virtual or real APN name to be sent in Credit Control Application (CCA) message, use the following configuration:

```
configure
  active-charging service <ecs_service_name>
    credit-control [ group <group_name> ]
      apn-name-to-be-included { gn | virtual }
      end
```

Configuring Diameter Prepaid Credit Control Application (DCCA)

This section describes how to configure the Diameter Prepaid Credit Control Application.

Important To configure and enable Diameter and DCCA functionality with ECS, you must obtain and install the relevant license on the chassis. Contact your Cisco account representative for detailed information on licensing requirements.

Important It is assumed that you have already fully configured the AAA parameters, and Credit Control Application as described in Configuring Prepaid Credit Control Application (CCA), on page 15 for Diameter mode. For information on configuring AAA parameters, if you are using StarOS 12.3 or an earlier release, refer to the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

To configure Diameter Prepaid Credit Control Application, use the following configuration.

```
configure
  active-charging service <ecs_service_name>
    credit-control [ group <cc_group_name> ]
      mode diameter
      diameter origin endpoint <endpoint_name>
      diameter dictionary <dcca_dictionary>
      diameter peer-select peer peer_name [ realm realm_name ] [
secondary-peer secondary_peer_name [ realm realm_name ] ] [ imsi-based { { prefix
 | suffix } imsi/prefix/suffix_start_value } [ to imsi/prefix/suffix_end_value ] ] [
 msisdn-based { { prefix | suffix } msisdn-based/prefix/suffix_start_value } [
to msisdn-based/prefix/suffix_end_value ] ]
      end
```

Notes:

- Diameter peer configuration set with the **diameter peer-select** command can be overridden by the **dcca peer-select peer** command in the APN Configuration mode for 3GPP service networks, and in Subscriber Configuration mode in other service networks.
- The specific Credit Control Group to be used for subscribers must be configured in the APN Configuration Mode using the **credit-control-group** <*cc_group_name*> command.
- *Optional:* To configure the maximum time, in seconds, to wait for a response from Diameter peer, in the Credit Control Configuration Mode, enter the following command:

  diameter pending-timeout <*duration*>
- *Optional:* To configure Diameter Credit Control Session Failover, in the Credit Control Configuration Mode, enter the following command:

  diameter session failover

  When enabled, in the event of failure, failure handling action is based on the **failure-handling** CLI.
- *Optional:* If you want to configure the service for IMS authorization in 3GPP service network, you can configure dynamic rule matching with Gx interface and dynamic rule matching order in rulebase, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      rulebase <rulebase_name>
         dynamic-rule order { always-first | first-if-tied }
         action priority <action_priority> { [ dynamic-only |
static-and-dynamic | timedef <timedef_name> ] { group-of-ruledefs
<ruledef_group_name> | ruledef <ruledef_name> } charging-action
<charging_action_name> [ monitoring-key <monitoring_key> ] [ description
<description> ] }
         end
```

- *Optional:* To configure Diameter group AVP Requested-Service-Unit for Gy interface support to include a sub-AVP in CCRs using volume, time, and unit specific charging, in the Rulebase Configuration Mode, enter the following command:

  cca diameter requested-service-unit sub-avp { time cc-time <*duration*> **| units cc-service-specific-units** <*charging_unit*> **| volume { cc-input-octets** <*bytes*> **| cc-output-octets** <*bytes*> **| cc-total-octets** <*bytes*> **} + }**
- Ensure the Diameter endpoint parameters are configured. For information on configuring Diameter endpoint, if you are using StarOS 12.3 or an earlier release, refer to the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

Configuring Peer-Select in Subscriber Configuration Mode (Optional)

This section describes how to configure Diameter peer-select within a subscriber configuration.

Important The **dcca peer-select** configuration completely overrides all instances of **diameter peer-select** configured within the Credit Control Configuration Mode for an Enhanced Charging Service.

To configure DCCA peers within a subscriber configuration, use the following configuration:

```
configure
  context <context_name>
    subscriber name <subscriber_name>
      dcca peer-select peer <host_name> [ [ realm <realm_name> ] [
secondary-peer <host_name> [ realm <realm_name> ] ] ]
      end
```

Configuring Peer-Select in APN Configuration Mode (Optional)

This section describes how to configure Diameter peer-select within an APN configuration.

Important This information is only applicable to GGSN networks.

Important The **dcca peer-select** configuration completely overrides all instances of **diameter peer-select** configured within the Credit Control Configuration Mode for an Enhanced Charging Service.

To configure DCCA peers within an APN, use the following configuration:

```
configure
  context <context_name>
    apn <apn_name>
      dcca peer-select peer <host_name> [ [ realm <realm_name> ] [
secondary-peer <host_name> [ realm <realm_name> ] ] ]
      end
```

Configuring RADIUS Prepaid Credit Control Application

RADIUS prepaid billing operates on a per content-type basis. Individual content-types are marked for prepaid treatment. When a traffic analysis rule marked with prepaid content-types matches, it triggers prepaid charge management.

Important The RADIUS Prepaid feature of ECS has no connection to the system-level Prepaid Billing Support or the 3GPP2 Prepaid features that are enabled under different licenses.

Important It is assumed that you have already fully configured the AAA parameters, and Credit Control Application as described in Configuring Prepaid Credit Control Application (CCA), on page 15 for RADIUS mode. For information on configuring AAA parameters, if you are using StarOS 12.3 or an earlier release, refer to the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

To configure RADIUS Prepaid Charging with Enhanced Charging, use the following configuration.

```
configure
  active-charging service <ecs_service_name>
```

```
credit-control [ group <group_name> ]
  mode radius
  exit
rulebase <rulebase_name>
  cca radius charging context <vpn_context> [ group <group_name> ]
  end
```

Notes:

- <*rulebase_name*> must be the name of the rulebase in which you want to configure Prepaid Credit Control configurables.
- <*vpn_context*> must be the charging context in which the RADIUS parameters are configured:
- *Optional:* To specify the accounting interval duration for RADIUS prepaid accounting, in the ACS Rulebase Configuration Mode, enter the following command:

  cca radius accounting interval <*interval*>
- *Optional:* To specify the user password for RADIUS prepaid services, in the ACS Rulebase Configuration Mode, enter the following command:

  cca radius user-password [encrypted] password <*password*>
- Ensure the RADIUS server parameters are configured. For more information, if you are using StarOS 12.3 or an earlier release, refer to the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

Configuring Redirection of Subscriber Traffic to ECS

User traffic is directed through the ECS service inspection engine by using Access Control List (ACL) mechanism to selectively steer subscriber traffic.

To configure redirection of subscriber traffic to ECS:

Step 1 Create an ECS ACL as described in Creating an ECS ACL.

Step 2 Apply an ACL to an individual subscriber as described in Applying an ACL to an Individual Subscriber, on page 22.

Step 3 Apply an ACL to the subscriber named default as described in Applying an ACL to the Subscriber Named default, on page 22.

Step 4 Apply the ACL to an APN as described in Applying the ACL to an APN, on page 22.

Important Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

Creating an ECS ACL

To create an ACL to use in steering subscriber traffic through ECS, use the following configuration:

```
configure
  context <context_name>
    ip access-list <access_list_name>
      redirect css service <ecs_service_name> <keywords> <options>
      end
```

Notes:

- *<ecs_service_name>* must be the enhanced charging service's name; no CSS service needs to be configured.

Applying an ACL to an Individual Subscriber

IP ACLs are applied to subscribers via attributes in their profile. The subscriber profile could be configured locally on the system or remotely on a RADIUS server.

To apply an ACL to a RADIUS-based subscriber, use the Filter-Id attribute. For more information on this attribute, if you are using StarOS 12.3 or an earlier release, refer to the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

To apply an ACL to an individual subscriber, use the following configuration:

```
configure
  context <context_name>
    subscriber name <subscriber_name>
      ip access-group <acl_name> [ in | out ]
      end
```

Applying an ACL to the Subscriber Named default

To apply an ACL to the default subscriber, use the following configuration:

```
configure
  context <context_name>
    subscriber default
      ip access-group <acl_name> [ in | out ]
      end
```

Applying the ACL to an APN

To apply an ACL to an APN, use the following configuration:

Important This information is only applicable to UMTS networks.

```
configure
  context <context_name>
    apn <apn_name>
      ip access-group <acl_name> [ in | out ]
      end
```

Configuring GTPP Accounting

For information on configuring GTPP accounting, if you are using StarOS 12.3 or an earlier release, refer to the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

Configuring EDR/UDR Parameters

This section provides an example configuration to configure EDR/UDR file transfer and file properties parameters, including configuring hard disk support on SMC card on ASR 5500, transfer modes, transfer interval, etc.

To configure EDR/UDR file parameters:

```
configure
   context <context_name>
      edr-module active-charging-service  [ charging | reporting ]
         cdr { purge { storage-limit <storage_limit> | time-limit <time_limit> }
 [ max-files <max_records_to_purge> ] | push-interval <push_interval> |
push-trigger space-usage-percent <trigger_percentage> |
remove-file-after-transfer | transfer-mode { pull [ module-only ] | push
 primary { encrypted-url <encrypted_url> | url <url> } [ [ max-files <max_records>
 ] [ module-only ] [ secondary { encrypted-secondary-url
<encrypted_secondary_url> | secondary-url <secondary_url> } ] [ via local-context
 ] + ] | use-harddisk }
         file [ charging-service-name { include | omit } ] [ compression {
 gzip | none } ] [ current-prefix <string> ] [ delete-timeout <seconds> ] [
directory <directory_name> ] [ edr-format-name ] [ exclude-checksum-record
] [ field-separator { hyphen | omit | underscore } ] [ file-sequence-number
 rulebase-seq-num ] [ headers ] [ name <file_name> ] [ reset-indicator ] [
 rotation [ num-records <number> | time <seconds> | volume <bytes> ] ] [
sequence-number { length <length> | omit | padded | padded-six-length |
unpadded } ] [ storage-limit <limit> ] [ single-edr-format ] [ time-stamp
{ expanded-format | rotated-format | unix-format } ] [ trailing-text
<string> ] [ trap-on-file-delete ] [ xor-final-record ] +
         exit
      udr-module active-charging-service
         file [ charging-service-name { include | omit } ] [ compression {
 gzip | none } ] [ current-prefix <string> ] [ delete-timeout <seconds> ] [
directory <directory_name> ] [ exclude-checksum-record ] [ field-separator
{ hyphen | omit | underscore } ] [ file-sequence-number rulebase-seq-num
 ] [ headers ] [ name <file_name> ] [ reset-indicator ] [ rotation [
num-records <number> | time <seconds> | volume <bytes> ] ] [ sequence-number
{ length <length> | omit | padded | padded-six-length | unpadded } ] [
storage-limit <limit> ] [ time-stamp { expanded-format | rotated-format |
unix-format } ] [ trailing-text <string> ] [ trap-on-file-delete ] [
udr-seq-num ] [ xor-final-record ] +
         end
```

Notes:

- The **cdr** command keywords can be configured either in the EDR or the UDR Configuration Mode. Configuring in one mode prevents the configurations from being applied in the other mode.

- If the **edr-module active-charging-service** command is configured without the **charging** or **reporting** keywords, by default the EDR module is enabled for charging EDRs.
- When the configured threshold limit is reached on the hard disk drive, the records that are created dynamically in the */mnt/hd-raid/data/records/* directory are automatically deleted. Files that are manually created should be deleted manually.
- The **use-harddisk** keyword is only available on the ASR 5500.

Verifying your Configuration

To view EDR-UDR file statistics, in the Exec Mode, enter the following command:

```
show active-charging edr-udr-file statistics
```

Pushing EDR/UDR Files Manually

To manually push EDR/UDR files to the configured external storage, in the Exec mode, use the following command:

```
cdr-push { all | local-filename file_name }
```

NOTES:

- Before you can use this command, the CDR transfer mode and file locations must be set to push in the EDR/UDR Module Configuration Mode.
- The **cdr-push** command is available in the Exec Mode.
- <*file_name*> must be absolute path of the local file to push.

Retrieving EDR and UDR Files

To retrieve UDR or EDR files you must SFTP into the context that was configured for EDR or UDR file generation.

This was done with the FTP-enabled account that you configured in Enabling Charging Record Retrieval, on page 9.

The following commands use SFTP to log on to a context named **ECP** as a user named **ecpadmin**, through an interface configured in the ECS context that has the IP address *192.168.1.10* and retrieve all EDR or UDR files from the default locations:

```
sftp -oUser=ecpadminECP 192.168.1.10:/records/edr/*
sftp -oUser=ecpadminECP 192.168.1.10:/records/udr/*
```

Configuring RADIUS Analyzer

This section describes how to configure the RADIUS Analyzer. When a call is established, the pre-DFA-rulebase uses the traffic that has been authenticated by the RADIUS server. Until then all the normal traffic is denied and is resumed only after the additional RADIUS based authentication is successful. The success of RADIUS authentication is determined by a RADIUS analyzer.

To configure the RADIUS Analyzer, use the following configuration:

```
configure
  active-charging service  service_name
    ruledef  ruledef_name
      [ no ] radius [ any-match < != | = > < FALSE | TRUE  > | error < != | = >
 <FALSE | TRUE  > | state < != | = > < auth-req-rcvd | auth-rsp-fail |  auth-rsp-success
  > ]
      end
```

Notes:

- **radius:** RADIUS related configuration.
- **any-match:** This command allows you to define rule expressions to match all RADIUS packets.
- **error:** This command allows you to define rule expressions to match for errors in RADIUS packets and errors in the RADIUS analyzer.
- **state:** This command allows you to define rule expressions to match the current state of an RADIUS session.

Sample Radius Analyzer Configuration

This section describes how to configure the RADIUS Analyzer feature.

To configure the RADIUS Analyzer, use the following sample configuration:

```
configure
  active-charging service s1
    ruledef rt_radius
      udp dst-port = 1812
      rule-application routing
      exit
    ruledef  radius_accept
      radius state = auth-rsp-success
      exit
```

Sample Dual Factor Authentication Configuration

This section describes how to configure the the Dual Factor Authentication (DFA) feature.

To configure the DFA Analyzer, use the following sample configuration:

```
configure
  active-charging service s1
    rulebase pre-dfa-rulebase
      action priority 1 ruledef radius_server_radius_traffic
charging-action do_nothing
     action priority 2 ruledef radius_server_icmp_traffic charging-action
 do_nothing
      action priority 3 ruledef  radius_accept charging-action
change_rbase
      action priority 100 ruledef catch_all charging-action drop
      route priority 1 ruledef rt_radius analyzer radius
      exit
    rulebase post-dfa-rbase
    exit
```

Configuring Post Processing Feature

This section describes how to configure the Post-processing feature to enable processing of packets even if rule matching for them has been disabled.

To configure the Post-processing feature, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      ruledef <ruledef_name>
         <protocol> <expression> <operator> <condition>
         rule-application post-processing
         exit
      charging-action <charging_action_name>
         ...
         exit
      rulebase <rulebase_name>
       action priority <action_priority> { [ dynamic-only | static-and-dynamic
 | timedef <timedef_name> ] { group-of-ruledefs <ruledef_group_name> | ruledef
<ruledef_name> } charging-action <charging_action_name> [ monitoring-key
<monitoring_key> ] [ description <description> ] }
        post-processing priority <priority> ruledef <ruledef_name>
charging-action <charging_action_name>
        ...
        end
```

Notes:

- In the ACS Rulebase Configuration Mode, the ruledef configured for post-processing action must have been configured for post processing in the ACS Ruledef Configuration Mode.
- If the same ruledef is required to be a charging rule in one rulebase and a post-processing rule in another rulebase, then two separate identical ruledefs must be defined.
- Post processing with group-of-ruledefs is not supported.
- Delay charging with dynamic rules is not supported, hence there cannot be dynamic post-processing rules.

Configuring Service Group QoS Feature

To create and configure a QoS-Group-of-Ruledefs, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
     qos-group-of-ruledefs <qos_group_of_ruledefs_name> [ -noconfirm ] [
description <description> ]
        add-ruledef <ruledef_name>
        end
```

Notes:

- To configure flow action in the charging-action, in the ACS Charging Action Configuration Mode, use the **flow action** CLI command.

- To configure bandwidth limits for a flow, in the in the ACS Charging Action Configuration Mode use the **flow limit-for-bandwidth** CLI command.
- To view subscriber statistics and information on dynamic updates to charging parameters per call ID, in the Exec Mode, use the following command:

```
show active-charging
subscribers callid <call_id> charging-updates [ statistics ] [
charging-action [ name <charging_action_name> ] | qos-group [ name
<qos_group_of_ruledefs_name> ] ] [ | { grep <grep_options> | more } ]
```

Configuring Bandwidth Limiting

To suppress throttling at charging-action, bearer and APN level, use the following configuration:

```
configure
   active-charging service service_name
      charging-action charging_action_name
         throttle-suppress [ timeout suppress_timeout ]
         no throttle-suppress
         end
```

Notes:

- **timeout** *suppress_timeout*: Specifies the time for which throttling is suppressed, in seconds. *suppress_timeout* must be an integer from 10 through 300.
- When configured with the **timeout** keyword, bandwidth limiting is suppressed for the mentioned time.
- When configured without the **timeout** keyword, the default value of 30 seconds will apply.
- When **throttle-suppress** is configured, the timeout will take the default value of 30 seconds. The flow will not be throttled for the next 30 seconds.
- When **no throttle-suppress** is configured, bandwidth limiting will continue from the next flow onwards.

Verifying your Configuration

Verify your configuration in the Exec mode using the following commands.

- To verify the configured timeout value for suppress-throttle:

```
show active-charging charging-action name <charging_action_name> [ | { grep
 <grep_options> | more } ]
```

- To verify the number of uplink and downlink bytes that escaped bandwidth limiting due to suppressing functionality:

```
show active-charging charging-action statistics [ name
<charging_action_name> ] [ | { grep <grep_options> | more } ]
```

- To verify the total suppress time and elapsed time:

```
show active-charging flows full all [ | { grep <grep_options> | more } ]
```

- To verify the historical total and current number of flows for which bandwidth limiting is suppressed:

```
show active-charging subsystem all [ | { grep <grep_options> | more } ]
```

Configuring Flow Admission Control

To configure the TCP Proxy Flow Admission Control feature, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      fair-usage tcp-proxy max-flows-per-subscriber <max_flows>
      fair-usage tcp-proxy memory-share <memory_share>
      end
```

Notes:

- It is not necessary for the Fair Usage feature to be enabled before this configuration.
- <*max_flows*> specifies the maximum number of flows for which TCP Proxy can be used per subscriber. Note that this limit is per Session Manager.
- <*memory_share*> specifies what portion of ECS memory should be reserved for TCP Proxy flows. Note that it is a percentage value.

Verifying your Configuration

To verify your configuration, in the Exec mode, use the following command:

```
show active-charging tcp-proxy statistics [ rulebase <rulebase_name> ] [
verbose ] [ | { grep <grep_options> | more } ]
```

Configuring Time-of-Day Activation/Deactivation of Rules Feature

This section describes how to configure the Time-of-Day Activation/Deactivation of Rules feature to enable charging according to day/time.

To configure the Time-of-Day Activation/Deactivation of Rules feature, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      ruledef <ruledef_name>
         ...
         exit
      timedef <timedef_name>
       start day { friday | monday | saturday | sunday | thursday | tuesday
 | wednesday } time <hh> <mm> <ss> end day { friday | monday | saturday |
sunday | thursday | tuesday | wednesday } time <hh> <mm> <ss>
         start time <hh> <mm> <ss> end time <hh> <mm> <ss>
         exit
      charging-action <charging_action_name>
         ...
         exit
      rulebase <rulebase_name>
         action priority <action_priority> timedef <timedef_name> {
group-of-ruledefs <ruledef_group_name> | ruledef <ruledef_name> } charging-action
 <charging_action_name> [ description <description> ]
         ...
         end
```

Notes:

- In a timeslot if only the time is specified, that timeslot will be applicable for all days.
- If for a timeslot, "start time" > "end time", that rule will span the midnight, which means that rule is considered to be active from the current day till the next day.
- If for a timeslot, "start day" > "end day", that rule will span over the current week till the end day in the next week.
- In the following cases a rule will be active all the time:
  - A timedef is not configured in an action priority
  - A timedef is configured in an action priority, but the named timedef is not defined
  - A timedef is defined but with no timeslots

Verifying your Configuration

To verify your configuration, in the Exec Mode, enter the following command:

show active-charging timedef name *<timedef_name>*

Configuring Retransmissions Under Rulebase or Service Level CLI

To enable retransmission under Rulebase or Service Level base, use the following configuration:

```
configure
     active-charging service <ecs_service_name>
          rulebase <rulebase name>
               retransmissions-counted
              end
```

Notes:

- Use the **no retransmission counted** command to disable the retransmission counted feature.

To verify your configuration, in the Exec mode, enter the following command:

```
show active-charging rulebase name <rulebase_name>
```

Configuring Websockets

To enable the websocket flow detection feature, use the following configuration:

```
configure
  active-charging service <ecs_service_name>
    rulebase <rulebae name>
      websocket flow-detection  <protocol>
      end
```

Notes:

Use the **no websocket flow-detection** command or **default websocket flow-detection** command to disable websocket flow detection.

To verify your configuration, in the Exec mode, enter the following command:

show active-charging rulebase name *<rulebase_name>*

Configuring URL Filtering Feature

This section describes how to configure the URL Filtering feature to simplify rules for URL detection.

To create a group-of-prefixed-URLs, use the following configuration:

```
configure
  active-charging service <ecs_service_name>
    group-of-prefixed-urls <prefixed_urls_group_name>
    end
```

To configure the URLs to be filtered in the group-of-prefixed-URLs, use the following configuration:

```
configure
  active-charging service <ecs_service_name>
    group-of-prefixed-urls <prefixed_urls_group_name>
      prefixed-url <url_1>
      ...
      prefixed-url <url_10>
      end
```

To enable or disable the group in the rulebase for processing prefixed URLs, use the following configuration:

```
configure
  active-charging service <ecs_service_name>
    rulebase <rulebase_name>
      url-preprocessing bypass group-of-prefixed-urls
<prefixed_urls_group_name>
      ...
      url-preprocessing bypass group-of-prefixed-urls
<prefixed_urls_group_name>
      end
```

Notes:

- A maximum of 64 group-of-prefixed-urls can be created and configured.
- A maximum of 10 prefixed URLs can be configured in each group-of-prefixed-urls.
- In a rulebase, multiple group-of-prefixed-urls can be configured to be filtered.

Verifying your Configuration

To verify your configuration, in the Exec Mode, enter the following command:

show active-charging group-of-prefixed-urls name *<prefixed_urls_group_name>*

Configuring AES Encryption

This section describes how to redirect the flow to the redirect-url and encrypt the dynamic fields by using either blowfish encryption or AES encryption.

The flow action redirect-url specifies ASR to return a redirect response to the subscriber, and terminate the TCP connections (to the subscriber and server). The subscriber's Web browser automatically sends 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 of the dynamic fields as well.

To redirect-URL action on packet and flow for Session Control functionality, use this configuration.

```
configure
   active-charging service <ecs_service_name>
     flow action redirect-url redirect_url [ encryption { blowfish128 |
blowfish64 | { { aes128 | aes256 } [ salt ] } } [ encrypted ] key key ] ]

     end
```

Notes:

- **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