

ACS Configuration Mode Commands

The ACS Configuration Mode is used to manage active charging service (ACS)/enhanced charging service (ECS) configurations. ACS provides flexible, differentiated, and detailed billing to subscribers through Layer 3 through Layer 7 packet inspection and the ability to integrate with back-end billing mediation systems.

Important In this release only one active charging service can be configured per system.

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

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

- accelerate-flow, on page 4
- access-ruledef, on page 4
- bandwidth-policy, on page 6
- buffering-limit, on page 7
- charging-action, on page 8
- check-point accounting, on page 9
- content-filtering, on page 10
- content-filtering category match-method, on page 12
- content-filtering category policy-id, on page 13
- credit-control, on page 14
- diameter credit-control, on page 15
- edns, on page 15
- edr-format, on page 17
- edr-ipproto-port-map, on page 19
- edr-udr-flow-control, on page 20
- end, on page 21

- exit, on page 21
- extend-ruledef-limit, on page 21
- fair-usage deact-margin, on page 22
- fair-usage tcp-proxy, on page 23
- fair-usage threshold-percent, on page 24
- firewall dos-protection flooding, on page 25
- firewall dos-protection ip-sweep, on page 27
- firewall flooding, on page 28
- firewall flow-recovery, on page 29
- firewall icmp-destination-unreachable-message-threshold, on page 30
- firewall license, on page 30
- firewall max-ip-packet-size, on page 31
- firewall mime-flood, on page 31
- firewall nat-alg, on page 31
- firewall no-ruledef-matches, on page 32
- firewall port-scan, on page 33
- firewall protect-servers, on page 34
- firewall ruledef, on page 35
- firewall tcp-syn-flood-intercept, on page 37
- firewall track-list, on page 37
- fw-and-nat action, on page 38
- fw-and-nat policy, on page 39
- group-of-objects, on page 40
- group-of-prefixed-urls, on page 41
- group-of-ruledefs, on page 43
- h323 time-to-live, on page 44
- h323 timeout, on page 45
- h323 tpkt, on page 46
- h323 version, on page 47
- host-pool, on page 47
- idle-timeout, on page 49
- imsi-pool, on page 51
- ip dns-learnt-entries, on page 52
- ip max-fragments, on page 53
- label content-id, on page 54
- load-db, on page 54
- nat allocation-failure, on page 55
- nat allocation-in-progress, on page 56
- nat ip downlink reassembly-timeout, on page 57
- nat tcp-2msl-timeout, on page 58
- nat unsolicited-pkts, on page 59
- p2p-ads-group, on page 60
- p2p-detection attribute, on page 61
- p2p-detection behavioral, on page 62
- p2p-detection ecs-analysis, on page 63
- p2p-detection protocol, on page 64

- p2p detection debug parameters, on page 91
- packet-filter, on page 93
- passive-mode, on page 94
- pcp-service, on page 95
- policy-control bearer-bw-limit, on page 96
- policy-control bind-default-bearer, on page 97
- policy-control burst-size, on page 98
- policy-control charging-action-override, on page 99
- policy-control charging-rule-base-name, on page 99
- policy control def-bearer-qos-change, on page 100
- policy-control dynamic-rule-limit, on page 101
- policy-control l7-dynamic-rules, on page 102
- policy-control report-rule-failure-once, on page 103
- policy-control retransmissions-counted, on page 103
- policy-control time-based-pcc-rule, on page 104
- policy-control token-replenishment-interval , on page 105
- policy-control update-default-bearer, on page 106
- port-map, on page 107
- qos-group-of-ruledefs, on page 108
- radio-congestion, on page 109
- readdress-server-list, on page 110
- redirect user-agent, on page 111
- rulebase, on page 112
- rulebase-list, on page 113
- ruledef, on page 114
- service-scheme, on page 115
- sip advanced, on page 116
- statistics-collection, on page 117
- subs-class, on page 118
- subscriber-base, on page 119
- system-limit flow-chkpt-per-call, on page 120
- system-limit l4-flows, on page 121
- tcp-acceleration-profile, on page 122
- tcp-acceleration, on page 122
- tethering-database, on page 123
- tethering-detection, on page 125
- timedef, on page 126
- tpo policy, on page 127
- tpo profile, on page 127
- trigger-action, on page 128
- trigger-condition, on page 129
- udr-format, on page 130
- xheader-format, on page 131

accelerate-flow

This command allows you to create/configure/delete Flow Aware Packet Acceleration (FAPA) feature.

Product

GGSN

P-GW

PDSN

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
[ no ] accelerate-flow
```

no

If previously configured, disables the feature.

accelerate-flow

Enables and configures the FAPA feature.

Usage Guidelines

Use this command to create/configure/delete the FAPA feature.

Important Accelerated ECS Packet feature will be supported when TRM FastPath is enabled on the Rulebase.

Example

The following command enables the FAPA feature and enters the FAPA or accelerate-flow mode:

```
accelerate-flow
```

access-ruledef

This command allows you to create/configure/delete access rule definitions (ruledefs).

Important This command is available only in StarOS 8.1 and in StarOS 9.0 and later releases, and must be used to configure the Policy-based Stateful Firewall and NAT features.

Product

NAT

PSF

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

access-ruledef *access_ruledef_name* **[-noconfirm]**
no access-ruledef *access_ruledef_name*

no

If previously configured, deletes the specified access ruledef.

access_ruledef_name

Specifies the access ruledef to add/configure/delete.

access_ruledef_name must be the name of an access ruledef, and must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters. Each access ruledef must have a unique name.

If the named access ruledef does not exist, it is created, and the CLI mode changes to the Firewall-and-NAT Access Ruledef Configuration Mode wherein the ruledef can be configured.

If the named access ruledef already exists, the CLI mode changes to the Firewall-and-NAT Access Ruledef Configuration Mode for that access ruledef.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete an access ruledef. A ruledef contains different conditions/criteria to permit, drop, or reject a packet/connection/traffic based on one or more parameters. The ruledef name must be unique within the service. Host pool, port map, IMSI pool, and access/firewall, routing, and charging ruledefs configured in the active charging service must all have unique names.



Important An access ruledef can be referenced by multiple Stateful Firewall rulebases.



Important Access ruledefs are different from ACS ruledefs.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-acs-fw-ruledef)#

Also see the *Firewall-and-NAT Access Ruledef Configuration Mode Commands* chapter.

Example

The following command creates an access ruledef named *ruledef1*, and enters the Firewall-and-NAT Access Ruledef Configuration Mode:

```
access-ruledef ruledef1
```

bandwidth-policy

This command allows you to create/configure/delete bandwidth policies.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

bandwidth-policy *bandwidth_policy_name* **[-noconfirm]**
no bandwidth-policy *bandwidth_policy_name*

no

If previously configured, deletes the specified bandwidth policy from the active charging service.

bandwidth_policy_name

Specifies the bandwidth policy to add/configure/delete.

bandwidth_policy_name must be the name of a bandwidth policy, and must be an alphanumeric string of 1 through 63 characters. Each bandwidth policy must have a unique name.

If the named bandwidth policy does not exist, it is created, and the CLI mode changes to the ACS Bandwidth Policy Configuration Mode wherein the bandwidth policy can be configured.

If the named bandwidth policy already exists, the CLI mode changes to the ACS Bandwidth Policy Configuration Mode for that bandwidth policy.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete a bandwidth policy.

In 12.3 and earlier releases, a maximum of 64 bandwidth policies can be configured.

In 14.0 and later releases, a maximum of 256 bandwidth policies can be configured.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-bandwidth-policy)#

Also see the *ACS Bandwidth Policy Configuration Mode Commands* chapter.

Example

The following command creates a bandwidth policy named *test73*, and enters the ACS Bandwidth Policy Configuration Mode:

```
bandwidth-policy test73
```

buffering-limit

This command allows you to configure packet buffering limits.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

buffering-limit { far-max-packets *far_max_packets* **| flow-max-packets** *flow_max_packets* **| subscriber-max-packets** *subscriber_max_packets* **}**
{ default | no } buffering-limit { far-max-packets | flow-max-packets | subscriber-max-packets }

default

Configure this command with the default setting.

no

Disable the buffering limit configuration.

far-max-packets *far_max_packets*

Specify the maximum number of packets that can be buffered per FAR.

far_max_packets must be an integer from 1 to 128.

Default value: 5 packets

flow-max-packets *flow_max_packets*

Specify the maximum number of packets that can be buffered per flow.

flow_max_packets must be an integer from 1 to 255.

subscriber-max-packets *subscriber_max_packets*

Specify the maximum number of packets that can be buffered per subscriber.

subscriber_max_packets must be an integer from 1 to 255.

Usage Guidelines

Use this command to configure the limits for buffering packets sent by a subscriber, while waiting for a response from the Diameter server. Packets need to be buffered for various reasons, such as, waiting for Credit Control Authorization or waiting for the result of a content filtering rating request.

Example

The following command sets the buffering limit per flow to *55* packets:

```
buffering-limit flow-max-packets 55
```

charging-action

This command allows you to create/configure/delete ACS charging actions.

Important A maximum of 2048 charging actions can be configured in the active charging service.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

`[ no ] charging-action` *`charging_action_name`* **`[ -noconfirm ]`**

no

If previously configured, deletes the specified charging action from the active charging service.

charging_action_name

Specifies the charging action to add/configure/delete.

charging_action_name must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters and can contain punctuation characters. Each charging action must have a unique name.

If the named charging action does not exist, it is created, and the CLI mode changes to the ACS Charging Action Configuration Mode wherein the charging action can be configured.

If the named charging action already exists, the CLI mode changes to the ACS Charging Action Configuration Mode for that charging action.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete an ACS charging action.

A charging action represents actions to be taken when a configured rule is matched. Actions could range from generating an accounting record (for example, an EDR) to dropping the IP packet, etc. The charging action will also determine the metering principle—whether to count retransmitted packets and which protocol field to use for billing (L3/L4/L7 etc).

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-charging-action)#

Also see the *ACS Charging Action Configuration Mode Commands* chapter.

Example

The following command creates a charging action named *action123* and changes to the ACS Charging Action Configuration Mode:

```
charging-action action123
```

check-point accounting

This command configures micro checkpoint syncup timer for ICSR and Session Recovery for Rf-Gy synchronization.

Product

GGSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
check-point accounting sync-timer { icsr | sr } timer_value [ sr | icsr ]
timer_value
no check-point accounting sync-timer { icsr | sr }
```

no

If the micro checkpoint syncup timer is already configured, then the **no** variant will delete the configuration.

sr *timer_value*

Configures micro check-pointing timer for Session Recovery (SR). By default, the session recovery check-pointing will be done on 8 seconds.

timer_value: Time configured will be in multiples of 2 seconds. Note that the timer value less than 4 seconds and greater than 60 seconds will not be accepted.

icsr *timer_value*

Configures micro check-pointing timer for ICSR. By default, the ICSR check-pointing will be done on 18 seconds.

timer_value: Time configured will be in multiples of 2 seconds. Note that the timer value less than 4 seconds and greater than 60 seconds will not be accepted.

Usage Guidelines

Use this command to configure micro checkpoint syncup timer for ICSR and Session Recovery. Micro Checkpoint Sync-up timer is an internal timer utilized by Rf and Gy modules to check point corresponding billing information.

Releases prior to 17.0, micro checkpoint sync-up timer was hardcoded with a value of 18 seconds for ICSR and 8 seconds for Session Recovery (SR). In 17.0 and later releases, the micro checkpoint sync-up timer is made configurable with an expectation that it be set at a value as low as 4 seconds. The timer value is reduced to ensure the accurate billing information during the ICSR or SR switchover event.

This CLI is available at both active charging service level and rulebase level. If the timer value is configured at both service and rulebase level, then the service level value will be overridden with rulebase level values.

This feature provides the operator with the flexibility to provision timer for accurate billing information in case of session recovery or ICSR switchover. However, this is a performance impacting feature and the impact of the micro checkpoint sync timer reduction needs to be carefully considered by the operator before provisioning a lower value.

Example

The following command configures the micro checkpoint syncup timer for Session Recovery as *8* seconds:

```
check-point accounting sync-timer sr 8
```

content-filtering

Content Filtering Range, Trigger Action, Trigger Condition, edns static prefix, edns fields and edns tags under the active changing service. This option is disabled by default.

Product

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

Syntax Description

```
[default] content-filtering range range
          trigger-condition trigger_condition_name
             app-proto = dns
             external-content-filtering
```

default

By default, the content-filtering range is 1 to 4294967295. Any value in CF-Policy-ID AVP is considered for CF. It will not be shown by default and will be shown in verbose config. To restore default functionality, use the cli **default content-filtering range**

content-filtering

content-filtering range: Enter start number and end number for the **cf-policy-id**. *range_values* can be integers. For example, 1-4294967295.

If range parameter is set to 1-1000, any subscriber with a content filtering policy ID greater than or equal to 1 and lower than or equal to 1000 should use the standard content filtering functionality. And any subscriber profile with a content filter policy ID outside the range of 1-1000 can trigger the new EDNS0 functionality.

app-proto=dns

Avoids the IP readdressing of the non-DNS traffic. If this CLI is enabled with multiline-or cli, then all DNS traffic will be EDNS encoded.

external-content-filtering

Enables EDNS0 feature.When this flag is true along with the range criteria, EDNS0 feature is enabled. By default, this flag is disabled.

Usage Guidelines

Enter start number and end number for the **cf-policy-id**. *range_values* can be integers. For example, 1-4294967295.

If the content filter policy ID for any Subscriber profile is outside the range of 1 to 1000, use the following CF policy id range CLI commands to enable the new EDNS0 functionality.

Syntax Description

```
content-filtering
       category
       range
         content-filitering range range_start_number to range_end_number
         content-filtering range 1 to 1000
         [ default ] content-filtering
         [ no ] content-filtering
```

range

Specifies policy-id range for content filtering feature.

range

content-filtering range : Enter start number and end number for the content filtering *range_start_number* to *range_end_number* can be integers. For example, 1-4294967295.

no content-filitering range

When chassi comes up, the **no content-filitering range** CLI is displayed in verbose.

default

Configures the range between 1 to 4294967295. The CF-Policy-ID value that comes up in Gx event is considered for Content Filtering. You can view this range in both verbose and non- verbose mode.

content-filtering category match-method

This command allows you to specify the match method to look up URLs in the Category-based Content Filtering database.

Product

CF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
content-filtering category match-method { exact | generic }
default content-filtering category match-method
```

default

Configures this command with its default setting.

Default: **generic**

exact

Specifies the exact-match method, wherein URLs are rated only on exact match with URLs present in the Category-based Content Filtering database.

generic

Specifies the generic match method, wherein normalization, multi-lookups, and rollback algorithms are applied to URLs during look up. URLs are rated on generic match with URLs present in the Category-based Content Filtering database.

Usage Guidelines

Use this command to set the match method to look up URLs in the Category-based Content Filtering database.

Example

The following command sets the exact-match method to look up URLs in the Category-based Content Filtering database:

```
content-filtering category match-method exact
```

content-filtering category policy-id

This command allows you to create/configure/delete Content Filtering Category Policies for Category-based Content Filtering support.



Important A maximum of 64 Content Filtering Category Policies can be configured in the active charging service.

Product

CF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

content-filtering category policy-id *cf_policy_id* **[description [** *description_string* **]] [-noconfirm]**
no content-filtering category policy-id *cf_policy_id*

no

If previously configured, deletes the specified Content Filtering Category Policy from the active charging service.

cf_policy_id

Specifies the Content Filtering Category Policy ID to add/configure/delete.

cf_policy_id must be an integer from 1 through 4294967295.

If the specified policy ID does not exist, it is created and the CLI mode changes to the Content Filtering Policy Configuration Mode, wherein the policy can be configured.

If the specified policy ID already exists, the CLI mode changes to the Content Filtering Policy Configuration Mode for that policy.

description [*description_string*]

Specifies a description for the Content Filtering Category Policy.

description_string must be an alphanumeric string of 1 through 31 characters.

Note that both **description** and *description_string* are optional.

"**description** *description_string*" saves *description_string* as the new description.

"**description**" removes the previously specified description.

This description is displayed in the output of the "**show content-filtering category policy-id id** *id*" and "**show active-charging service name** *service_name*" commands.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete a Content Filtering Category Policy.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-acs-content-filtering-policy)#

Also see the *Content Filtering Policy Configuration Mode Commands* chapter.

Example

The following command creates a Content Filtering Policy with the ID *101*, and enters the Content Filtering Policy Configuration Mode:

```
content-filtering category policy-id 101
```

credit-control

This command allows you to enable/disable Prepaid Credit Control Configuration Mode.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
[ no ] credit-control [ group cc_group_name ]
     diameter credit-control group
      diameter map-mscc-rc-4999-to-2001
```

no

Disables the specified Prepaid Credit Control Application configuration.

group *cc_group_name*

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

Specifies the credit control group to add/configure/delete.

cc_group_name must be the name of a credit control group, and must be an alphanumeric string of 1 through 63 characters. Each credit control group must have a unique name.

If the named credit control group does not exist, it is created, and the CLI mode changes to the Credit Control Configuration Mode, wherein the credit control group can be configured.

If the named credit control group already exists, the CLI mode changes to the Credit Control Configuration Mode for that credit control group.

Creating different credit control groups enables applying different credit control configurations (DCCA dictionary, failure-handling, session-failover, Diameter endpoint selection, etc.) to different subscribers on the same system.

Without credit control groups, only one credit control configuration is possible on a system. All the subscribers in the system will have to use the same configuration.



Important ICSR support for credit-control group is limited to a maximum of three bearers (one default and two dedicated bearers).

Usage Guidelines

Use this command to enable/disable Prepaid Credit Control Configuration for RADIUS/Diameter charging mode.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-dcca)#

Also see the *Credit Control Configuration Mode Commands* chapter.

Example

The following command enables prepaid credit control accounting to use RADIUS and/or Diameter interface mode.

```
credit-control
```

diameter credit-control

This command has been deprecated, and is replaced by the credit-control, on page 14 command.

edns



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

This command allows you to configure EDNS format and fields. This configuration can be used whenever the DNS traffic needs to be converted to an EDNS request.

Product

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
edns
  security-profile  security_profile cf-policy-id-static-prefix
static_prefix_value
        fields fields_name
           [ default ] tag  number cf-policy-id  payload-length ( tcp | udp
 )
no edns
```

no

If previously configured, deletes the specified EDNS mode from the active charging service.

edns

This command allows you to configure EDNS format and fields.

security-profile

Specifies security profile is used to configure the 32 MS bit static value.

cf-policy-id-static-prefix *static_prefix_value*

Enter the integer value. The 32 bit static ID is used as MSB bytes in 64 bit device ID. If security-profile static prefix does not have any **cf-policy-id-prefix** defined, then device-id is encoded with only 32 bit **cf-policy-id**.

tag *val* cf-policy-id

This is a tag field to insert CF Policy ID in the EDNS0 Resource Record (RR) data.

payload-length (tcp | udp)

Specifies the RR UDP or TCP Payload-length value. You can enter the value ranging from 512 to 4096.

default tag

Resets the UDP or TCP payload-length field to an unconfigured default value of 1280.

Note If you enter a **default tag** *number* on a tag number that is not configured, the following error message is displayed:

Usage Guidelines

Use this command to configure EDNS format and fields.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-acs-edns)#

Also see the *EDNS Configuration Mode Commands* chapter.

Example

The following command enables EDNS Configuration Mode:

edns

The following command disables EDNS Configuration Mode:

no edns

edr-format

This command allows you to create/configure/delete ACS Event Data Record (EDR) formats.

Important A maximum of 256 EDR plus UDR formats can be configured in the active charging service.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Using this command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
edr-format edr_format_name [ -noconfirm ]
no edr-format edr_format_name
        attribute attribute_name
        attribute attribute_name
```

no

If previously configured, deletes the specified EDR format from the active charging service.

edr_format_name

Specifies the EDR format to add, configure, and delete.

edr_format_name must be an alphanumeric string of 1 through 63 characters. Each EDR format must have a unique name.

If the specific EDR format does not exist, it is created, and the CLI mode changes to the EDR Format Configuration Mode wherein the EDR format can be configured.

If the named EDR format already exists, the CLI mode changes to the EDR Format Configuration Mode for that EDR format.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create, configure, and delete an EDR format.

Upon entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-acs-edr)#

Also see the *EDR Format Configuration Mode Commands* chapter.

Example

The following command creates an EDR format named *edr_format1*, and enters the EDR Format Configuration Mode:

```
edr-format edr_format1
```

Example

The following example shows the warning message for **edr-format**:

```
no edr-format name
Are you sure? [  Yes | No ]  :  Yes
```

Note The previous warning message is displayed when you disable the following CLI commands in the active-charging service configuration:

- **ruledef**
- **rulebase**
- **charging-action**
- **packet-filter**
- **subscriber-base**
- **qos-group-of-ruledefs**
- **group-of-ruledefs**
- **trigger-condition**
- **trigger-action**
- **tcp-acceleration-init-params**
- **tcp-acceleration-profile**
- **subs-class**
- **readdress-server-list**
- **udr-format**
- **p2p-ads-group**
- **bandwidth-policy**

attribute *attribute_name*

Specifies the attribute to configure an EDR.

Usage Guidelines This command is used to create, configure, and delete the ACS Event Data Record (EDR) formats.

edr-ipproto-port-map

This command enables IP protocol and server port mapping for Event Data Records (EDR).

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

`[ default | no ] edr-ipproto-port-map`

default

Configures this command with its default setting.

Default: Disabled

no

If previously enabled, disables the IP protocol and server port mapping for EDR.

Usage Guidelines

Use this command to enable IP protocol and server port mapping for EDR. As part of EDR generation, packets can be mapped based on IP header protocol and Transport Header Port. Generating statistics based on IP Protocol and Transport Port number is an added advantage for offline packet analysis.

edr-udr-flow-control

This command allows you to enable/disable flow control between Session Managers (SessMgrs) and the CDRMOD process.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

`edr-udr-flow-control [ unsent-queue-size` *`unsent_queue_size`* **`]`**
`{ default | no } edr-udr-flow-control`

no

If previously enabled, disables the flow control configuration.

default

Configures this command with its default setting.

Default: Flow control is enabled; **unsent-queue-size**: 375

unsent-queue-size *unsent_queue_size*

Specifies the flow control unsent queue size at Session Manager (SessMgr) level.

unsent_queue_size must be an integer from 1 through 2500.

Usage Guidelines Use this command to enable Flow Control between SessMgr and the CDRMOD process, and configure the unsent queue size.

Example

The following command enable Flow Control between SessMgrs and the CDRMOD process, and configure the unsent queue size to *1000*:

```
edr-udr-flow-control unsent-queue-size 1000
```

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.

extend-ruledef-limit

This command allows you to configure the maximum hard limit extension for ruledef .

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

extend-ruledef-limit
no extend-ruledef-limit

no

If previously configured, disables the maximun hard limit configuration in the current charging action.

Usage Guidelines

This command configures the maximum hard limit extension for ruledef that is increased from 2500 to 3500.

fair-usage deact-margin

This command allows you to configure the deactivate margin for the Fair Usage feature.

Product



Important In release 17.0, this command has been deprecated.

ACS

ADC

CF

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

fair-usage deact-margin *deactivate_margin*
default fair-usage deact-margin

default

Configures this command with its default setting.

Default: 5 percent

deactivate_margin

Specifies that Fair Usage monitoring must be disabled when the instance-level credit usage goes *deactivate_margin* percentage below *usage_threshold*.

deactivate_margin is a percentage value, and must be an integer from 1 through 100.

Usage Guidelines

Use this command to configure when to disable the Fair Usage feature, which enables SessMgr instance-level load balancing for in-line service features, and resource usage control for subscribers. For additional information, refer to the feature description in the *Enhanced Charging Service Administration Guide*.

Example

The following command configures the deactivate margin to disable Fair Usage monitoring to 10% below the session resource usage threshold (65%):

```
fair-usage deact-margin 10
```

fair-usage tcp-proxy

This command allows you to configure the maximum number of flows for which TCP Proxy can be used per subscriber, and what portion of ECS memory should be reserved for TCP Proxy flows.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
fair-usage tcp-proxy { max-flows-per-subscriber max_flows_subscriber |
memory-share memory_share }
default fair-usage [ max-flows-per-subscriber | memory-share ]
```

default

Configures this command with its default setting.

max-flows-per-subscriber *max_flows_subscriber*

Specifies the maximum number of flows for which TCP Proxy can be used per subscriber.

This limit is per Session Manager.

max_flows_subscriber must be an integer from 1 through 1000.

Default: 5

memory-share *memory_share*

Specifies what portion of ECS memory should be reserved for TCP Proxy flows.

memory_share is a percentage value, and must be an integer from 1 through 100.

Default: 10%

Usage Guidelines Use this command to configure the maximum number of flows for which TCP Proxy can be used for a subscriber, and what portion of ECS memory should be reserved for TCP Proxy flows.

Example

The following command configures 100 as the maximum number of flows for which TCP Proxy can be enabled for the subscriber:

```
fair-usage tcp-proxy max-flows-per-subscriber 100
```

fair-usage threshold-percent

This command allows you to configure the usage threshold to start Fair Usage monitoring.

Product

Important In release 17.0, this command has been deprecated.

ACS

ADC

CF

PSF

NAT

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
fair-usage threshold-percent usage_threshold
default fair-usage threshold-percent
```

default

Configures this command with its default setting.

Default: 50 percent

usage_threshold

Specifies the threshold to start Fair Usage monitoring. Until the credit usage hits this threshold, all session resource allocation is allowed. On crossing this threshold, any new resource allocation request is evaluated before being allowed or denied.

usage_threshold is a percentage value, and must be an integer from 1 through 100.

Usage Guidelines

Use this command to configure the threshold to enable the Fair Usage feature, which enables SessMgr instance-level load balancing for in-line service features, and resource usage control for subscribers. For additional information, refer to the feature description in the *Enhanced Charging Service Administration Guide*.

Example

The following command enables the Fair Usage feature, and configures the session resource usage threshold to start Fair Usage monitoring to 75%:

```
fair-usage threshold-percent 75
```

firewall dos-protection flooding

This command is configured to protect servers from mobile subscribers in the uplink direction.

Product



Important In StarOS 17.0 and later releases, the uplink flooding feature is not enabled in the ACS Configuration mode, and must be enabled in the Firewall-and-NAT Policy Configuration mode. Hence, this command is no longer supported and left in place for backward compatibility.

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
firewall dos-protection flooding { { icmp | tcp-syn | udp } protect-servers
 { all | host-pool hostpool_name } packet limit packet_limit |
inactivity-timeout timeout | uplink-sample-interval interval }
default firewall dos-protection flooding { icmp | tcp-syn | udp |
inactivity-timeout | uplink-sample-interval }
no firewall dos-protection flooding { icmp | tcp-syn | udp }
```

no

Disables Stateful Firewall protection for subscribers against the specified Denial of Service (DoS) attack(s).

default

Disables Stateful Firewall protection for subscribers against all DoS attacks.

flooding { icmp | tcp-syn | udp } protect-servers { all | host-pool *hostpool_name*

Enables protection against the specified flooding attack:

- **icmp**: Enables ICMP uplink flooding protection.
- **tcp-syn**: Enables TCP Syn uplink flooding protection.
- **udp**: Enables UDP uplink flooding protection.

all: Enables protection for all the servers.

host-pool *hostpool_name*: Specifies the name of the host pool. *hostpool_name* must be an alphanumeric string of 1 through 63 characters.

packet limit *packet_limit*

Specifies the maximum number of packets allowed during a sampling interval.

packet_limit must be an integer from 1 through 4294967295.

Default: 1000 packets per sampling interval for all protocols.

inactivity-timeout *inactivity_timeout*

Specifies the inactivity timeout period, in seconds. This allows flooding traffic if the destination is inactive for more than the configured period.

inactivity_timeout must be an integer from 1 through 4294967295.

Default: 300 seconds

uplink-sample-interval *interval*

Specifies the uplink sampling interval, in seconds. The maximum sampling-interval configurable is 60 seconds.

interval must be an integer from 1 through 60.

Default: 1 second

Usage Guidelines

Use this command to enable Stateful Firewall protection from different types of DoS attacks for all servers or for those servers mentioned in the host pool. This allows users to safeguard their own servers and other hosts.

DoS attacks are also detected in the downlink direction. The **firewall dos-protection** command must be configured in the FW-and-NAT Policy Configuration mode.

Example

The following command enables ICMP uplink protection for all servers with packet limit set to *10*:

```
firewall dos-protection flooding icmp protect-servers all packet limit
10
```

firewall dos-protection ip-sweep

This command is configured to detect Source IP-based flooding attacks in the uplink direction.

Product



Important In StarOS 17.0 and later releases, the IPsweep feature is not enabled in the ACS Configuration mode, and must be enabled in the Firewall-and-NAT Policy Configuration mode. Hence, this command is no longer supported and left in place for backward compatibility.

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
firewall dos-protection ip-sweep { icmp | tcp-syn | udp } protect-servers
 { all | host-pool hostpool_name } packet limit packet_limit |
downlink-server-limit server_limit | inactivity-timeout timeout |
sample-interval interval }
default firewall dos-protection ip-sweep { downlink-server-limit | icmp
| inactivity-timeout | sample-interval | tcp-syn | udp }
no firewall dos-protection ip-sweep { icmp | tcp-syn | udp }
```

default

Disables Stateful Firewall protection for subscribers against all DoS attacks.

no

Disables Stateful Firewall protection for subscribers against the specified Denial of Service (DoS) attack(s).

ip-sweep { icmp | tcp-syn | udp } protect-servers { all | host-pool *hostpool_name*

Enables protection against the specified flooding attack:

- **icmp**: Enables source IP-based flood attack detection for ICMP.
- **tcp-syn**: Enables source IP-based flood attack detection for TCP-SYN.
- **udp**: Enables source IP-based flood attack detection for UDP.

all: Enables protection for all the servers.

host-pool *hostpool_name*: Specifies the name of the host pool. *hostpool_name* must be an alphanumeric string of 1 through 63 characters.

packet limit *packet_limit*

Specifies the maximum number of packets allowed during a sampling interval for uplink and downlink.

packet_limit must be an integer from 1 through 4294967295.

Default: 1000 packets per sampling interval for all protocols.

downlink-server-limit *server_limit*

Specifies the number of internet hosts that can be blocked in the uplink and downlink direction.

server_limit must be an integer from 2 through 999.

Default: 100

inactivity-timeout *inactivity_timeout*

Specifies the inactivity timeout period for uplink and downlink, in seconds. This allows flooding traffic if the destination is inactive for more than the configured period.

inactivity_timeout must be an integer from 1 through 4294967295.

Default: 300 seconds

sample-interval *interval*

Specifies the IP Sweep sample interval, in seconds. The maximum sampling-interval configurable is 60 seconds.

interval must be an integer from 1 through 60.

Default: 1 second

Usage Guidelines

Use this command to enable or disable IP Sweep Protection in the uplink direction for mobile subscribers and internet hosts on a per protocol basis. The purpose of the Uplink IP Sweep protection is to check whether a particular source IP address is generating more flows per sample interval than is permitted. If so, the first packets that come after the maximum packet limit during the particular time interval will be dropped.

IP Sweep attacks are also detected in the downlink direction. The **firewall dos-protection ip-sweep** command must be configured in the FW-and-NAT Policy Configuration mode. The configuration values for packet limit and sampling interval are common for both uplink and downlink.

Example

The following command enables ICMP uplink protection for all servers with packet limit set to *30*:

```
firewall dos-protection ip-sweep icmp protect-servers all packet limit
30
```

firewall flooding

Description In StarOS 8.1 and later releases, for Rulebase-based Stateful Firewall this command is available in the ACS Rulebase Configuration Mode, and for Policy-based Stateful Firewall in the Firewall-and-NAT

Policy Configuration Mode. In StarOS 8.3, this command is available in the ACS Rulebase Configuration Mode.

firewall flow-recovery

This command allows you to configure the Stateful Firewall's Flow Recovery feature.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

firewall flow-recovery { { downlink [[timeout *timeout* **] [no-flow-creation] +] } | { uplink [timeout** *timeout* **] } }**
{ default | no } firewall flow-recovery { downlink | uplink }

default

Configures this command with its default setting.

Default: Downlink and uplink flow recovery enabled, 300 seconds

no

Disables the flow recovery configuration.

downlink | uplink

Specifies the packets:

- **downlink**: Enables flow recovery for packets from the downlink direction.
- **uplink**: Enables flow recovery for packets from the uplink direction.

timeout *timeout*

Specifies the Stateful Firewall Flow Recovery Timeout setting, in seconds.

timeout must be an integer from 1 through 86400.

Default: 300 seconds

no-flow-creation

Specifies not to create data session/flow-related information for downlink-initiated packets (from the Internet to the subscriber) while the firewall downlink flow-recovery timer is running, but send to subscriber.

Usage Guidelines Use this command to configure Stateful Firewall Flow Recovery feature.

Important NAT flows will not be recovered.

Example

The following command configures Stateful Firewall Flow Recovery for packets in downlink direction with a timeout setting of *600* seconds:

```
firewall flow-recovery downlink timeout 600
```

firewall icmp-destination-unreachable-message-threshold

Description In StarOS 8.1 and later releases, for Rulebase-based Stateful Firewall this command is available in the ACS Rulebase Configuration Mode, and for Policy-based Stateful Firewall in the Firewall-and-NAT Policy Configuration Mode. In StarOS 8.3, this command is available in the ACS Rulebase Configuration Mode.

firewall license

This command allows you to configure the license related parameters for Stateful Firewall.

Product PSF

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description **firewall license exceed-action { disable-feature | drop-call | ignore }**

exceed-action { disable-feature | drop-call | ignore }

Configures one of the following parameters when license is exceeded.

- **disable-feature**: Disables the service when license is exceeded.
- **drop-call**: Drops the call if call fails to get a Stateful Firewall license.
- **ignore**: Continues using the Stateful Firewall license even if license is exceeded. This is the default behavior.

Usage Guidelines Use this command to configure the license related parameters for Stateful Firewall when license is exceeded.

firewall max-ip-packet-size

Description In StarOS 8.1 and later releases, for Rulebase-based Stateful Firewall this command is available in the ACS Rulebase Configuration Mode, and for Policy-based Stateful Firewall in the Firewall-and-NAT Policy Configuration Mode. In StarOS 8.3, this command is available in the ACS Rulebase Configuration Mode.

firewall mime-flood

Description In StarOS 8.1 and later releases, for Rulebase-based Stateful Firewall this command is available in the ACS Rulebase Configuration Mode, and for Policy-based Stateful Firewall in the Firewall-and-NAT Policy Configuration Mode. In StarOS 8.3, this command is available in the ACS Rulebase Configuration Mode.

firewall nat-alg

This command enables/disables Network Address Translation (NAT) Application Level Gateways (ALGs).

Product

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

`[ default | no ] firewall nat-alg { all | ftp | h323 | pptp | rtsp | sip } [ ipv4-and-ipv6 | ipv4-only | ipv6-only ]`

default

Configures this command with the default setting for the specified parameter.

Default:

- **ftp**: Enabled
- **h323**: Enabled
- **pptp**: Disabled
- **rtsp**: Disabled
- **sip**: Disabled

no

Disables all/ or the specified NAT ALG configuration. When disabled, the ALG(s) will not do any payload translation for NATd calls.

all | ftp | h323 | pptp | rtsp | sip

Specifies the NAT ALG to enable/disable.

- **all**: Enables/disables all of the following NAT ALGs.
- **ftp**: Enables/disables File Transfer Protocol (FTP) NAT ALG.
- **h323**: Enables/disables H323 NAT ALG.
- **pptp**: Enables/disables Point-to-Point Tunneling Protocol (PPTP) NAT ALG.
- **rtsp**: Enables/disables Real Time Streaming Protocol (RTSP) ALG.
- **sip**: Enables/disables Session Initiation Protocol (SIP) NAT ALG.

ipv4-and-ipv6 | ipv4-only | ipv6-only

Specifies to enable/disable NAT44/NAT64 ALG.

- **ipv4-and-ipv6**: Enables both NAT44 and NAT64 ALGs.
- **ipv4-only**: Enables only NAT44 ALG.
- **ipv6-only**: Enables only NAT64 ALG.

Usage Guidelines Use this command to enable/disable NAT ALGs.

To enable NAT ALG processing, in addition to this configuration, ensure that the routing rule for that particular protocol is added in the rulebase.

Example

The following command enables FTP NAT ALG:

```
firewall nat-alg ftp
```

The following command disables FTP NAT ALG:

```
no firewall nat-alg ftp
```

The following command enables FTP NAT ALG, and disables H.323, PPTP, RTSP, and SIP NAT ALGs:

```
default firewall nat-alg all
```

firewall no-ruledef-matches

Description In StarOS 8.1 and later releases, this command is available in the ACS Rulebase Configuration Mode.

firewall port-scan

This command allows you to configure Stateful Firewall's Port Scan Detection algorithm.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

firewall port-scan { connection-attempt-success-percentage { non-scanner | scanner } *percentage* **| inactivity-timeout** *inactivity_timeout* **| protocol { tcp | udp } response-timeout** *response_timeout* **| scanner-policy { block inactivity-timeout** *inactivity_timeout* **| log-only } }**
default firewall port-scan { connection-attempt-success- percentage { non-scanner | scanner } | inactivity-timeout | protocol { tcp | udp } response-timeout | scanner-policy }

default

Configures this command with its default setting.

connection-attempt-success-percentage { non-scanner | scanner } ***percentage***

Specifies the connection attempt success percentage.

- **non-scanner**: Specifies the connection attempt success percentage for a non-scanner.

  percentage must be an integer from 60 through 99.

  Default: 70%

- **scanner**: Specifies the connection attempt success percentage for a scanner.

  percentage must be an integer from 1 through 40.

  Default: 30%

inactivity-timeout ***inactivity_timeout***

Specifies the port scan inactivity timeout period, in seconds.

inactivity_timeout must be an integer from 60 through 1800.

Default: 300 seconds

protocol { tcp | udp } response-timeout ***response_timeout***

Specifies transport protocol and response-timeout period.

- **tcp**: Specifies response timeout for TCP.

  response_timeout must be an integer from 1 through 30.

- **udp**: Specifies response timeout for UDP.

  response_timeout must be an integer from 1 through 60.

Default: 3 seconds

scanner-policy { block inactivity-timeout *inactivity_timeout* | log-only }

Specifies how to treat packets from a source address that has been detected as a scanner.

- **block inactivity-timeout** *inactivity_timeout*: Specifies blocking any subsequent traffic from the scanner. If the scanner is found to be inactive for the inactivity-timeout period, then the scanner is no longer blocked, and traffic is allowed.

  inactivity_timeout specifies the scanner inactivity timeout period, in seconds, and must be an integer from 1 through 4294967295.

- **log-only**: Specifies logging scanner information without blocking scanner traffic.

Default: **log-only**

Usage Guidelines

Use this command to configure the Stateful Firewall Port Scan Detection algorithm enabled by the **firewall dos-protection port-scan** CLI command.

This protection tracks all uplink source addresses, and the packets they initiate towards all subscribers that have this protection enabled.

Example

The following command configures the Stateful Firewall Port Scan inactivity timeout setting to *900* seconds:

```
firewall port-scan inactivity-timeout 900
```

firewall protect-servers

This command is configured to protect ISP servers from mobile space devices.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

`firewall protect-servers { all | host-pool` *`hostpool_name`* **`} policy`** *`policy_name`*
`{ default | no } firewall protect-servers`

default

Configures this command with its default setting.

no

Disables protection of the servers.

all

Configured to protect all servers from attacking mobile nodes.

host-pool *hostpool_name*

Specifies the name of the host pool where all servers in that host pool need to protected.

hostpool_name must be an alphanumeric string of 1 through 63 characters.

policy *policy_name*

Specifies the Firewall-and-NAT policy to be applied to packets that are destined to the IPs mentioned in the host pool.

policy_name must be the name of a Firewall-and-NAT policy, and must be an alphanumeric string of 1 through 63 characters

Usage Guidelines

Use this command to protect all ISP servers or specific ISP servers from mobile space devices. All the uplink packets will be inspected, and the action will be taken based on the configuration in Firewall-and-NAT policy. Uplink protection can be enabled or disabled based on the server IP of the packet.

Example

The following command is configured to protect all servers within a Firewall-and-NAT policy named *test123*:

```
firewall protect-servers all policy test123
```

firewall ruledef

This command allows you to create/configure/delete Stateful Firewall ruledefs.

Important This command is available only in StarOS 8.1. This command must be used to configure the Rulebase-based Stateful Firewall and NAT features.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

firewall ruledef *firewall_ruledef_name* **[-noconfirm]**
no firewall ruledef *firewall_ruledef_name*

no

If previously configured, deletes the specified Stateful Firewall ruledef from the active charging service.

firewall_ruledef_name

Specifies the Stateful Firewall ruledef to add/configure/delete.

firewall_ruledef_name must be the name of a Stateful Firewall ruledef, and must be an alphanumeric string of 1 through 63 characters and can contain punctuation characters. Each ruledef must have a unique name.

If the named ruledef does not exist, it is created, and the CLI mode changes to the Firewall Ruledef Configuration Mode wherein the ruledef can be configured.

If the named Stateful Firewall ruledef already exists, the CLI mode changes to the Firewall Ruledef Configuration Mode for that ruledef.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete a Stateful Firewall ruledef. A Stateful Firewall ruledef contains different conditions to permit, drop, or reject a packet/connection/traffic based on one or more parameters. The ruledef name must be unique within the active charging service. Host pool, port map, IMSI pool, and Stateful Firewall, routing, and charging ruledefs must have unique names.

A Stateful Firewall ruledef can be referenced by multiple Stateful Firewall rulebases.



Important The Stateful Firewall ruledefs are different from the ACS ruledefs.

Also see the *Firewall-and-NAT Access Ruledef Configuration Mode Commands* chapter.

Example

The following command creates a Stateful Firewall ruledef named *fw_ruledef1*, and enters the Firewall Ruledef Configuration Mode:

```
firewall ruledef fw_ruledef1
```

firewall tcp-syn-flood-intercept

Description In StarOS 8.1 and later releases, for Rulebase-based Stateful Firewall this command is available in the ACS Rulebase Configuration Mode, and for Policy-based Stateful Firewall in the Firewall-and-NAT Policy Configuration Mode. In StarOS 8.3, this command is available in the ACS Rulebase Configuration Mode.

firewall track-list

This command allows you to configure the maximum number of server IP addresses to be tracked that are involved in any kind of denial-of-service (DoS) attacks.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

firewall track-list attacking-servers *no_of_servers*
{ default | no } firewall track-list attacking-servers

default

Configures this command with its default setting.

Default: 10 servers

no



Important This command variant is available only in StarOS 8.3 and later releases.

If previously configured, deletes the configuration from the active charging service.

attacking-servers *no_of_servers*

Specifies the maximum number of servers to track.

no_of_servers must be an integer from 1 through 100.

Usage Guidelines

Use this command to configure the maximum number of server IP addresses to be tracked that are involved in any kind of DoS attacks.

Example

The following command configures the maximum number of server IP addresses to be tracked that are involved in any kind of DoS attacks to *20*:

```
firewall track-list attacking-servers 20
```

fw-and-nat action

This command allows you to create/configure/delete Firewall-and-NAT actions.



Important This command is available only in 11.0 and later releases. This command must be used to configure the Stateful Firewall and NAT Action.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

fw-and-nat action *action_name* **[-noconfirm]**
no fw-and-nat action *action_name*

no

If previously configured, deletes the specified Firewall-and-NAT action from the active charging service.

action_name

Specifies the Firewall-and-NAT action to add/configure/delete.

action_name must be the name of a Firewall-and-NAT action, and must be an alphanumeric string of 1 through 63 characters. Each Firewall-and-NAT action must have a unique name.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete a Firewall-and-NAT action.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-fw-and-nat-action)#

Also see the *Firewall-and-NAT Action Configuration Mode Commands* chapter.

Example

The following command creates a Firewall-and-NAT action named *test1*, and changes to the Firewall-and-NAT Action Configuration Mode:

```
fw-and-nat action test1
```

fw-and-nat policy

This command allows you to create/configure/delete Firewall-and-NAT policies.



Important This command is available only in StarOS 8.1 and in StarOS 9.0 and later releases. This command must be used to configure the Policy-based Stateful Firewall and NAT features.

Product

PSF

NAT

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

fw-and-nat policy *policy_name* **[-noconfirm]**
no fw-and-nat policy *fw_nat_policy_name*

no

If previously configured, deletes the specified Firewall-and-NAT policy from the active charging service.



Important When a Firewall-and-NAT policy is deleted, for all subscribers using the policy, Stateful Firewall and NAT processing is disabled, also ACS sessions for the subscribers are dropped. In case of session recovery, the calls are recovered but with Stateful Firewall and NAT disabled.

fw_nat_policy_name

Specifies the Firewall-and-NAT policy to add/configure/delete.

fw_nat_policy_name must be the name of a Firewall-and-NAT policy, and must be an alphanumeric string of 1 through 63 characters. Each Firewall-and-NAT policy must have a unique name.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete a Firewall-and-NAT policy.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-fw-and-nat-policy)#

Also see the *Firewall-and-NAT Policy Configuration Mode Commands* chapter.

Example

The following command creates a Firewall-and-NAT policy named *test321*, and changes to the Firewall-and-NAT Policy Configuration Mode:

```
fw-and-nat policy test321
```

group-of-objects

This command allows you to create/configure/delete an ACS group-of-objects.

Important This command is available only in StarOS 10.2 and later releases.

Important A maximum of 16 object groups can be configured in the active charging service. And a maximum of 128 objects can be configured within each object group.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

group-of-objects *objects_group_name* **[type string [-noconfirm]]**
no group-of-objects *objects_group_name*

no

If previously configured, deletes the specified group-of-objects from the active charging service.

objects_group_name

Specifies the group-of-objects to add/configure/delete.

objects_group_name must be the name of a group-of-objects, and must be an alphanumeric string of 1 through 63 characters. Each group-of-objects must have a unique name.

If the named group-of-objects does not exist, it is created, and the CLI mode changes to the ACS Group-of-Objects Configuration Mode wherein the group can be configured.

If the named group-of-objects already exists, the CLI mode changes to the ACS Group-of-Objects Configuration Mode for that group.

type

Specifies the data type for the group-of-objects.



Important "string" is the only data type supported in this release.

string

Specifies the data type as string.

When creating a group, specifying the data type is mandatory.

When modifying an existing group, specifying the data type is optional.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete a group-of-objects.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-acs-group-of-objects)#

Also see the *ACS Group-of-Objects Configuration Mode Commands* chapter.

Example

The following command creates a group-of-objects named *test4* with the data type string, and enters the ACS Group-of-Objects Configuration Mode:

```
group-of-objects test4 type string
```

group-of-prefixed-urls

This command allows you to create/configure/delete an ACS group-of-prefixed-URLs.

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

Important A maximum of 64 group-of-prefixed-URL groups can be configured in the active charging service.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

group-of-prefixed-urls *prefixed_urls_group_name* **[-noconfirm]**
no group-of-prefixed-urls *prefixed_urls_group_name*

no

If previously configured, deletes the specified group-of-prefixed-urls from the active charging service.

prefixed_urls_group_name

Specifies the group-of-prefixed-urls to add/configure/delete.

prefixed_urls_group_name must be the name of a group-of-prefixed-urls, and must be an alphanumeric string of 1 through 63 characters. Each group-of-prefixed-urls must have a unique name.

If the named group-of-prefixed-urls does not exist, it is created, and the CLI mode changes to the ACS Group-of-Prefixed-URLs Configuration Mode wherein the group can be configured.

If the named group-of-prefixed-urls already exists, the CLI mode changes to the ACS Group-of-Prefixed-URLs Configuration Mode for that group.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete a group-of-prefixed-URLs.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-acs-grp-of-prefixed-urls)#

Also see the *ACS Group-of-Prefixed-URLs Configuration Mode Commands* chapter.

Example

The following command creates group-of-prefixed-urls named *test5*, and enters the ACS Group-of-Prefixed-URLs Configuration Mode:

```
group-of-prefixed-urls test5
```

group-of-ruledefs

This command allows you to create/configure/delete an ACS group-of-ruledefs.

Important A maximum of 512 ruledefs can be configured in one group-of-ruledefs in the active charging service. A maximum of 384 group-of-ruledefs can be configured.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
group-of-ruledefs ruledefs_group_name [ -noconfirm ]
no group-of-ruledefs ruledefs_group_name
```

no

If previously configured, deletes the specified group-of-ruledefs from the active charging service.

ruledefs_group_name

Specifies the group-of-ruledefs to add/configure/delete.

ruledefs_group_name must be unique within the active charging service, and must be an alphanumeric string of 1 through 63 characters. Each group-of-ruledefs must have a unique name.

If the named group-of-ruledefs does not exist, it is created, and the CLI mode changes to the ACS Group-of-Ruledefs Configuration Mode wherein the group can be configured.

If the named group-of-ruledefs already exists, the CLI mode changes to the ACS Group-of-Ruledefs Configuration Mode for that group.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete a group-of-ruledefs.

A group-of-ruledefs is a collection of rule definitions to use in access policy creation.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-group-of-ruledefs)#

Also see the *ACS Group-of-Ruledefs Configuration Mode Commands* chapter.

Example

The following command creates a group-of-ruledefs named *group1*, and enters the ACS Group-of-Ruledefs Configuration Mode:

group-of-ruledefs group1

h323 time-to-live

This command allows you to configure the time period for which an endpoint's registration to an H.323 gatekeeper is valid.

Product

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-acs)#`

Syntax Description

h323 time-to-live *timeout*
default h323 time-to-live

default

Configures this command with its default setting.

Default: 3600 seconds

timeout

Specifies the timeout setting, in seconds.

timeout must be an integer from 1 through 2147483647.

Usage Guidelines

Use this command to configure the time period for which an endpoint's registration to a gatekeeper is valid.

Example

The following command configures the time for an endpoint registration with a timeout setting of *5* seconds:

```
h323 time-to-live 5
```

h323 timeout

This command allows you to configure the timeout intervals for various H.323 requests.

Product

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

h323 timeout { admission *admission_timeout* **| discovery** *discovery_timeout* **| location** *location_timeout* **| registration** *registration_timeout* **| unregistration** *unregistration_timeout* **}**
default h323 timeout { admission | discovery | location | registration | unregistration }

default

Configures this command with the default setting for the specified parameters.

admission *admission_timeout*

Configures the timeout value for the admission request sent to the gatekeeper.

admission_timeout must be an integer from 1 through 20.

Default: 10 seconds

discovery *discovery_timeout*

Configures the timeout value for the gatekeeper request message sent to the Gatekeeper.

discovery_timeout must be an integer from 1 through 20.

Default: 10 seconds

location *location_timeout*

Configures the timeout value for the location request message sent to the Gatekeeper.

location_timeout must be an integer from 1 through 20.

Default: 10 seconds

registration *registration_timeout*

Configures the timeout value for the registration request message sent to the Gatekeeper.

registration_timeout must be an integer from 1 through 20.

Default: 6 seconds

unregistration *unregistration_timeout*

Configures the timeout value for the unregistration request message sent to the Gatekeeper.

unregistration_timeout must be an integer from 1 through 20.

Default: 3 seconds

Usage Guidelines Use this command to configure the timeout interval for the various H.323 requests.

Example

The following command configures the admission request message with a timeout value of *15* seconds:

```
h323 timeout admission 15
```

h323 tpkt

This command allows you to configure the maximum size of Transport Protocol Data Unit Packets (TPKT) that the H.323 Application Layer Gateway (ALG) can handle.

Product NAT

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
h323 tpkt max_tpkt_size
default h323 tpkt
```

default

Configures this command with its default setting.

Default: 2048 bytes

max_tpkt_size

Specifies the maximum TPKT size, in bytes.

max_tpkt_size must be an integer from 4 through 4096.

Usage Guidelines Use this command to configure the maximum packet size for the H.323 ALG.

Example

The following command configures a maximum TPKT packet size of *100* bytes:

```
h323 tpkt 100
```

h323 version

This command allows you to configure the H.323 version number supported by an H.323 Application Layer Gateway (ALG).

Product

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

h323 version *h323_version_number*
default h323 version

default

Configures this command with its default setting.

Default: 5

h323_version_number

Specifies the H.323 version number.

h323_version_number must be an integer from 1 through 7.

Usage Guidelines

Use this command to configure the H.323 version number supported by the H.323 ALG.

Example

The following command configures the H.323 version as *1*:

```
h323 version 1
```

host-pool

This command allows you to create/configure/delete host pools.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

host-pool *host_pool_name* **[-noconfirm]**
no host-pool *host_pool_name*

no

If previously configured, deletes the specified host pool from the active charging service.

host_pool_name

Specifies the host pool to add/configure/delete.

host_pool_name must be the name of a host pool, and must be an alphanumeric string of 1 through 63 characters and can contain punctuation characters. Each host pool must have a unique name.

If the named host pool does not exist, it is created, and the CLI mode changes to the ACS Host Pool Configuration Mode wherein the host pool can be configured.

If the named host pool already exists, the CLI mode changes to the ACS Host Pool Configuration Mode for that host pool.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Syntax Description

extend-host-pool-limit *host_pool_limit*
no extend-host-pool-limit *host_pool_limit*

extend_host_pool_limit

Increases the number of host pools from 512 to 1024 and IP related configuration lines per host pool from 20 to 32.

no

Unconfigures or disables the feature. If the configured hostpools are more than 512 or configured entries in hostpool are more than 20 then error is displayed.

Note Remove the hostpools manually and then try to disable the feature.

Usage Guidelines

Use this command to create/configure/delete ACS host pools.

A host pool is a collection of hosts and IP addresses to use in access policy creation. The host pool name must be unique with in the service. Host pool, port map, IMSI pool, and firewall, routing, and charging ruledefs must have unique names. A maximum of 512 host pools can be created. A maximum lines of 20 can be created inside the host pools.



Important Host pools configured in other ruledefs cannot be deleted.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-acs-host-pool)#

Also see the *ACS Host Pool Configuration Mode Commands* chapter.

Example

The following command creates a host pool named *hostpool1*, and enters the ACS Host Pool Configuration Mode:

```
host-pool hostpool1
```

idle-timeout

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

Product

ACS

NAT

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

idle-timeout { alg-media | flow-mapping { tcp | udp } | icmp | tcp [half-open] | udp } *idle_timeout*
{ default | no } idle-timeout { alg-media | flow-mapping { tcp | udp } | icmp | tcp [half-open] | udp }

default

Configures this command with the default setting for the specified parameter.

Default:

- **alg-media**: 120 seconds

- **flow-mapping { tcp | udp }**: 300 seconds for TCP and 0 seconds for UDP
- **icmp**, **tcp**, **udp**: 300 seconds
- **tcp half-open**: 200 seconds

no

Disables the idle-timeout configuration for the specified flow.

alg-media

Configures the ALG media for the specified flow.

flow-mapping { tcp | udp }

The Flow Mapping timer is an extension to the existing flow idle-timeout in ACS. This flow mapping timeout applies only for NAT enabled calls and is supported only for TCP and UDP flows. The purpose of this timer is to hold the resources (NAT IP, NAT port, Private IP NPU flow) associated with a 5-tuple flow until Mapping timeout expiry.

If the Flow Mapping timer is disabled, then the Mapping timeout will not get triggered for UDP/TCP idle timed out flows. The resources such as NAT mapping will be released along with the 5-tuple flow.

icmp

Configures the ICMP protocol for the specified flow.

tcp [half-open]

Configures the TCP protocol for the specified flow.

Use the **half-open** keyword to configure timeout interval for half-open TCP flows.

udp

Configures the UDP protocol for the specified flow.

idle_timeout

Specifies the timeout duration, in seconds, and must be an integer from 0 through 86400.

For **alg-media** specifies the media inactivity timeout. The *idle_timeout* value gets applied on RTP and RTCP media flows that are created for SIP/H.323 calls. The timeout is applied only on those flows that actually match the RTP and RTCP media pinholes that are created by the SIP/H.323 ALG.

A value of 0 disables the idle-timeout setting.

Usage Guidelines

Use this command to configure the maximum duration a flow can remain idle, in seconds, after which the system automatically terminates the flow.

Setting the value to 0 will cause the idle-timeout setting to be disabled.

For flows other than TCP, UDP and ICMP, timeout value will always be 300 seconds (unless configured in the charging-action). Charging action's flow idle-timeout will have precedence over ACS idle-timeout. If charging action's flow idle-timeout is default, then flows will have the value configured in the active charging service.

Example

The following command configures the maximum duration a TCP flow can remain idle to *3000* seconds, after which the system automatically terminates the flow:

```
idle-timeout tcp 3000
```

imsi-pool

This command allows you to create/configure/delete International Mobile Subscriber Identity (IMSI) pools.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

imsi-pool *imsi_pool_name* **[-noconfirm]**
no imsi-pool *imsi_pool_name*

no

If previously configured, deletes the specified IMSI pool from the active charging service.

imsi_pool_name

Specifies the IMSI pool to add/configure/delete.

imsi_pool_name must be the name of an IMSI pool, and must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters. Each IMSI pool must have a unique name.

If the named IMSI pool does not exist, it is created, and the CLI mode changes to the ACS IMSI Pool Configuration Mode wherein the IMSI pool can be configured.

If the named IMSI pool already exists, the CLI mode changes to the ACS IMSI Pool Configuration Mode for that IMSI pool.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete pools of International Mobile Subscriber Identifier (IMSI) numbers having group of single or range of IMSI numbers to use in access policy creation. The IMSI pool name must be unique with in the service. Host pool, port map, IMSI pool, and firewall, routing, and charging ruledefs must have unique names. A maximum of 256 IMSI pools can be created.

Important IMSI pools configured in other ruledefs cannot be deleted.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-acs-imsi-pool)#

Also see the *ACS IMSI Pool Configuration Mode Commands* chapter.

Example

The following command creates an IMSI pool named *imsipool1*, and enters the ACS IMSI Pool Configuration Mode:

```
imsi-pool imsipool1
```

ip dns-learnt-entries

This command allows you to configure how long to keep the snooped IPv4 addresses that were extracted from DNS responses.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

ip dns-learnt-entries timeout *timeout_period*
{ default | no } ip dns-learnt-entries timeout

default

Configures this command with the default DNS-learnt-entries timeout setting.

Default: 300 seconds

no

Specifies to always use the TTL value in the DNS response, and not the timeout configured with this command.

timeout_period

Specifies the DNS-learnt-entries timeout period, in seconds.

timeout_period must be an integer from 1 through 2147483647.

Usage Guidelines

Use this command to configure how long to keep the snooped IPv4 addresses that were extracted from DNS responses—for the TTL specified in the DNS response, or for the time period configured with this command, if greater.

The configurable timer will be at global ECS level and shared across all IP addresses. Internally, a five-minute (300 seconds, non configurable) timer will be started whenever DNS analyzer is enabled. On timeout of this timer, all the learnt IP addresses will be checked for TTL expiry and the expired entries will be flushed.

Example

The following command specifies to keep the snooped IPv4 addresses that were extracted from DNS responses for a time period of *900* seconds, or for the TTL value specified in the DNS response, whichever is greater:

```
ip dns-learnt-entries timeout 900
```

ip max-fragments

This command allows you to limit the maximum number of IPv4/IPv6 fragments per fragment chain.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

ip max-fragments *max_fragments*
default ip max-fragments

default

Configures this command with its default setting.

Default: 45

max_fragments

Specifies the maximum number of IPv4/IPv6 fragments per fragment chain.

max_fragments must be an integer from 1 through 300.

Usage Guidelines

Use this command to limit the maximum number of IPv4/IPv6 fragments.

Example

The following command limits the maximum number of IPv4/IPv6 fragments to *100*:

```
ip max-fragments 100
```

label content-id

This command allows you to specify a label (text string) to associate with a content ID for UDRs/EDRs/eG-CDRs.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

label content-id *content_id* **text** *label_text*
no label content-id *content_id*

no

If previously configured, deletes the specified label.

content-id *content_id*

Specifies the content ID to associate with the label.

content_id must be an integer from 1 through 65535.

text *label_text*

Specifies the label to associate with the specified content ID.

label_text must be an alphanumeric string of 1 through 64 characters.

Usage Guidelines

Use this command to create a text label to associate with a content ID.

A maximum of 2048 labels can be configured in the active charging service.

Example

The following command creates the label *test_charge1* to be associated with the content ID *1378*:

```
label content-id 1378 text test_charge1
```

load-db

This command allows you to load specified databases.

Product P-GW

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
load-db uidh wl-url-host-db
no load-db uidh
```

no

If configured, removes the database.

uidh

Configures the UIDH database.

wl-url-host-db

Loads URL Host database.

Usage Guidelines Use this command to load and configure the UIDH database and URL Host database.

nat allocation-failure

This command allows you to configure the action to take when NAT IP/Port allocation fails.

Important This command is available only in StarOS 8.3 and later releases.

Product NAT

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
nat allocation-failure send-icmp-dest-unreachable
{ default | no } nat allocation-failure
```

default

Configures this command with its default setting.

Default: Packets are dropped silently

no

If previously enabled, disables the NAT Allocation Failure configuration. Packets are dropped silently.

nat allocation-failure send-icmp-dest-unreachable

Specifies to send ICMP Destination Unreachable message when NAT IP/Port allocation fails.

Usage Guidelines Use this command to configure the action to take when NAT IP/port allocation fails—to send or not to send an "ICMP destination unreachable message" when a NAT IP/port cannot be assigned to a flow in data path.

Example

The following command configures sending ICMP Destination Unreachable message when NAT IP/Port allocation fails:

```
nat allocation-failure send-icmp-dest-unreachable
```

nat allocation-in-progress

This command allows you to configure the action to take on packets when NAT IP/NPU allocation is in progress.



Important This command is available only in StarOS 8.3 and later releases.

Product NAT

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
nat allocation-in-progress { buffer | drop }
default nat allocation-in-progress
```

default

Configures this command with its default setting.

Default: **buffer**

buffer | drop

Specifies the action to take on packets when NAT IP/NPU allocation is in progress:

- **buffer**: Buffers the packets.
- **drop**:Drops the packets.

Usage Guidelines

In On-demand NAT IP allocation (wherein NAT IP address is allocated to the subscriber when a packet is being sent), if no free NAT IP address is available, a NAT-IP Alloc Request is sent to the VPNMgr to get NAT-IP. During that time packets are dropped. This command enables buffering the packets received when IP Alloc Request is sent to VPNMgr.

Example

The following command specifies to buffer packets when NAT IP/NPU allocation is in progress:

```
nat allocation-in-progress buffer
```

nat ip downlink reassembly-timeout

This command configures the downlink IP reassembly timer.

Product

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

[default] nat ip downlink reassembly-timeout *timeout*

default

Configures this command with its default setting.

Default: 2000 milliseconds

timeout

The maximum duration for which IP packet fragments can be retained, in milliseconds.

timeout must be an integer from 1 through 30000.

Usage Guidelines

Use this command to configure the downlink IP reassembly timer by setting the duration for which IP packet fragments can be retained.

Example

The following command configures the duration for IP packet fragments with a timeout setting of *3000* seconds:

```
nat ip downlink reassembly-timeout 3000
```

nat tcp-2msl-timeout

This command allows you to configure the TCP 2MSL (Maximum Segment Lifetime) timeout value for NAT.

Important This command is available only in StarOS 8.3 and later releases.

Product

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

nat tcp-2msl-timeout *timeout*
default nat tcp-2msl-timeout

default

Configures this command with its default setting.

Default: 60 seconds

timeout

Specifies the TCP 2MSL timeout period, in seconds.

timeout must be an integer from 30 through 240.

Usage Guidelines

Use this command to configure the TCP 2MSL timeout value for NAT.

Example

The following command configures the TCP 2MSL timeout for NAT to *120* seconds:

```
nat tcp-2msl-timeout 120
```

nat unsolicited-pkts

This command allows you to configure unsolicited packets.

Product

ACS

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

nat unsolicited-pkts { icmp-host-unreachable { max-rate *packets_num* **} | server-list { max-limit** *servers_num* **} }**
[default | no] nat unsolicited-pkts { icmp-host-unreachable | server-list }

default

Configures this command with its default setting.

Default: Disabled

no

Configures this command with its default setting.

icmp-host-unreachable max-rate *packets_max*

Configures the maximum number of allowed ICMP response packets, in seconds.

packets_max must be an integer from 1 through 100.

server-list max-limit *servers_num*

Configures the maximum number of servers to be stored per Session Manager instance.

servers_num must be an integer from 2 through 50.

Usage Guidelines

Use the following command to configure the number of allowed ICMP responses and the number of servers where most number of unsolicited packets are received.

Example

The following command configures the number of allowed ICMP responses per second to *10*:

nat unsolicited-pkts host-unreachable max-rate 10

The following command configures the number of servers to be stored as *20*:

nat unsolicited-pkts server-list max-limit 20

p2p-ads-group

This command configures the P2P Advertisement server and associated protocols/applications.

Product

ADC

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-acs)#`

Syntax Description

`[ no ] p2p-ads-group` *`ads_group_name`* **`[ -noconfirm ]`**

no

If previously configured, disables the configured correlation group.

ads_group_name

Specifies the name of the P2P Advertisement correlation group. *ads_group_name* must be an alphanumeric string of 1 through 63 characters.

[-noconfirm]

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to configure the P2P Advertisement server and associated protocols/applications.

Important The maximum number of advertisement groups that can be configured is 100.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-acs-p2p-ads)#

Also see the *P2P Advertisement Server Group Configuration Mode Commands* chapter.

Example

The following command specifies to configure the ad-server correlation group named **group1**:

`p2p-ads-group group1`

p2p-detection attribute

This command enables or disables the detection of SSL renegotiation flows.

Product

ADC

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

`[ no ] p2p-detection attribute {` *`attribute_list`* **`[`** *`sub_attribute_name sub_attribute_value`* **`] }`**

no

If previously enabled, disables detection of SSL renegotiation flows.

attribute_list

List of configurable P2P detection attributes populated from the currently loaded P2P plugin.

Supported attribute: **ssl-renegotiation**

sub_attribute_name

List of configurable P2P detection sub-attributes related to the attribute selected from the attribute list. This list is populated from the currently loaded P2P plugin.

Supported sub-attributes if selected attribute is **ssl-renegotiation**:

- **max-entry-per-sessmgr**: Specifies maximum SSL Session IDs tracked per session manager.
- **id-reduce-factor**: Specifies by how much factor the SSL ID is stored in the SSL Session ID tracker table. Possible values are 1, 2, 4.

sub_attribute_value

Value of the selected sub-attribute. If sub-attribute is not specified, the default value set in the P2P plugin will be used.

The value for **max-entry-per-sessmgr** must be an integer from 1 through 65535. Default: 20000

Possible values for **id-reduce-factor** are 1,2,4. Default: 4

Usage Guidelines

Use this command to enable or disable the detection of SSL renegotiation flows.

Example

The following command enables SSL renegotiation with SSL session IDs as **40000** and factor as **4**
:

```
p2p-detection attribute ssl-renegotiation max-entry-per-sessmgr 40000
id-reduce-factor 4
```

p2p-detection behavioral

This command enables or disables behavioral detection for unidentified traffic.

Product

ADC

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

`[ no ] p2p-detection behavioral { ` *`behavioral_list`* **` | all }`**

no

If previously configured, disables the behavioral configuration.

behavioral_list

Specifies the behavior to match. The behavioral list is the list of supported behavioral detection logic populated from the currently loaded ADC plugin.

behavioral_list must be one of the following:

- **all**: Enables all behavioral detection types supported by the ADC plugin
- **download**: Detects unknown flows which are data download using behavioral analysis
- **p2p**: Detects P2P and file sharing protocols using behavioral analysis
- **upload**: Detects unknown flows which are data upload using behavioral analysis
- **video**: Detects video flows using behavioral analysis
- **voip**: Detects VoIP (voice and video) protocols using behavioral analysis

Usage Guidelines

Use this command to enable or disable behavioral detection for unidentified traffic. Behavioral VoIP is meant for zero day detection of VoIP traffic. Behavioral upload/download is similar to client-server upload/download using HTTP, FTP, SFTP, etc. It must also detect flows of non-standard ports which ECS cannot detect and falls under the client-server model. The behavioral feature is disabled by default.

Example

The following command specifies to configure behavioral VoIP:

```
p2p-detection behavioral voip
```

p2p-detection ecs-analysis

This command enables or disables ECS analysis for analyzers — FTP, HTPP, HTTPS, RTSP and SIP.

Product

ADC

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
[ no ] p2p-detection ecs-analysis { all | ftp | http | https | rtsp | sip }
```

no

If previously enabled, disables the configured analyzers.

all

ECS analysis for all analyzers — FTP, HTPP, RTSP and SIP.

ftp

ECS analysis for FTP analyzer.

http

ECS analysis for HTTP analyzer.

https

ECS analysis for HTTPS analyzer.

rtsp

ECS analysis for RTSP analyzer.

sip

ECS analysis for SIP analyzer.

Usage Guidelines Use this command to enable or disable the interworking of analyzers — FTP, HTPP, RTSP and SIP. This feature is enabled by default if P2P protocols are enabled.

Example

The following command enables ECS analysis for the **ftp** analyzer:

```
p2p-detection ecs-analysis ftp
```

p2p-detection protocol

This command enables/disables the detection of all or specified peer-to-peer (P2P) protocols.

Product ADC

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
[ no ] p2p-detection protocol [ 120Sports | 8tracks | abcnetworks | abscbn
 | accuradio |actionvoip | actsync | adobeconnect | aenetworks | aimini
| all | amazoncloud | amazonmusic | amazonvideo | android_messageantsp2p
 | anyconnect | apple-push | apple-store | applejuice | applemaps | ares
 | armagettron | avi | badoo | baeblemusic | baidumovie | battlefld | bbm
 | beatport | betternet | bitcasa | bittorrent | bittorrent-sync |
blackberry-store | blackberry | blackdialer | blackplanet-radio | box |
btn | callofduty | cbssports | chikka | cisco-jabber | citrix | clubpenguin
 | clubbox | comodounite | crackle | crossfire | crunchyroll |
curiosity-stream | cyberghost | dashradio | danzwave | ddlink | deezer
didi | directconnect | directv | discord | dish-anywhere | disneymovies
| dns-tunneling | dofus | dramafever | dropbox | ebuddy | edonkey | epix
 | eros | espn | expressvpn | facebook | facetime | fandor | fasttrack |
 feidian | ficall | fiesta | filetopia | filmontv | fitradio | flash |
flickr | florensia | foursquare | fox-business | fox-news | fox-now |
fox-sports | foxsportsgo | freenet | friendster | fring | fubotv | funshion
 | fxnow | gaana | gadugadu | gamekit | gmail | gnutella | go90 | goober
 | googlemaps | google-music | google-push | google | googleplay |
googleplus | gotomeeting |gtalk | guildwars | halflife2 | hamachivpn |
hayu | hbogo | hbonow | hbonordic | heytell | hgtv | hike-messenger | hls
 | hotspotvpn | http | hulu | hyves | iax | icall | icecast | icloud |
idrive | igo | iheartradio | imesh | imessage | imgur | imo | implus |
instagram | iplayer | iptv | irc | isakmp | iskoot | itunes | jabber |
jap | jumblo | kakaotalk | kidoodle | kik-messenger | kiswe | klowdtv |
kontiki | kugoo | kuro | linkedin | livestream | lync | magicjack |
manolito | mapfactor | mapi | maplestory | meebo | meetic | mega | mgcp
```

| mig33 | mlb | mojo | monkey3 | mozy | msn | msrp | mute | mxtp | mypeople | myspace | nateontalk | natgeotv | naverline | navigon | nbc-sports | nbc-tv | netflix | netmotion | newsy | nick | nimbuzz | nokia-store | nrktv | octoshape | odkmedia | odnoklassniki | off | ogg | ohiofm | oist | oovoo | opendrive | openft | openvpn | operamini | orb | oscar | outlook | paltalk | pando | pandora | path | pbs | pcanywhere | periscope | pinterest | playstation | plingm | poco | pokemon-go | popo | pplive | ppstream | ps3 | qello_concerts | qq | qqgame | qqlive | quake | quic | quicktime | radio-paradise | radiocom| rdp | rdt | redbulltv | regram | rfactor | rhapsody | rmstream | rodi | reddit | rynga | samsung-store | scydo | secondlife | shoutcast | showtime | silverlight | siri | skinny | skydrive | skype | slacker-radio | slingbox | slingtv | smartvoip | smashcast | smule |snapchat | softether | somafm | sopcast | soribada | soulseek | soundcloud | spark | spdy | spike| speedtest | splashfighter | spotify | ssdp | ssl | starz | stealthnet | steam | stun | sudaphone | svtplay | tagged | talkatone | tango | taxify | teamspeak | teamviewer | telegram | thunder | tinder | tidal | tmo-tv | tor | truecaller | truphone | tumblr | tunein-radio | tunnelvoice | turbovpn | tvants | tvland | tvuplayer | tv2sumotwitch | twitter | ufc | ultrabac | ultrasurf | univision | upc-phone | usenet | ustream | uusee | vchat | veohtv | vessel | vevo | viber | viki | vimeo | vine | voipdiscount | vopium | voxer | vpnmaster | vpnx | vtok | vtun | vudu | warcft3 | waze | webex | wechat | weibo | whatsapp | wii | willow | windows-azure | windows-store | winmx | winny | wmstream | wofkungfu | wofwarcraft | wuala | wwe | xbox | xdcc | xfinity | xing | yahoo | yahoomail | yogafree | youku | yiptv | yourfreetunnel | youtube | zattoo | zello +]

no

If previously enabled, disables the detection of the specific peer-to-peer protocol.

all

Specifies to detect all supported P2P protocols.

In 12.2 and earlier releases: Specifying **all** is the same as configuring each of the following protocols individually.

In 14.0 and later releases: Specifying **all** means all of the protocols supported by the currently loaded plugin.

120Sports

Specifies to detect 120Sports protocol.

8tracks

Specifies to detect 8tracks protocol.

abcnetworks

Specifies to detect Abcnetworks protocol.

abscbn

Specifies to detect ABSCBN protocol.

accuradio

Specifies to detect Accuradio protocol.

actionvoip

Specifies to detect ActionVoip protocol.

actsync

Specifies to detect ActiveSync protocol.

adobeconnect

Specifies to detect Adobe Connect protocol.

aenetworks

Specifies to detect AENetworks protocol.

aimini

Specifies to detect Aimini protocol.

amazoncloud

Specifies to detect AmazonCloud protocol.

amazonmusic

Specifies to detect Amazon Music protocol.

amazonvideo

Specifies to detect Amazon Video protocol.

android_messages

Specifies to detect Android Messages for Web P2P protocol.

antsp2p

Specifies to detect ANts P2P protocol.

anyconnect

Specifies to detect AnyConnect protocol.

apple-push

Specifies to detect Apple Push Notification protocol.

apple-store

Specifies to detect iPhone Appstore protocol.

applejuice

Specifies to detect Applejuice protocol.

applemaps

Specifies to detect Apple Maps protocol.

ares

Specifies to detect Ares Galaxy protocol.

armagettron

Specifies to detect Armagetron protocol.

avi

Specifies to detect AVI protocol.

badoo

Specifies to detect Badoo protocol.

baeblemusic

Specifies to detect Baeble Music protocol.

baidumovie

Specifies to detect Baidumovie protocol.

battlefld

Specifies to detect Battlefield protocol.

bbm

Specifies to detect BBM protocol.

beatport

Specifies to detect Beatport protocol.

betternet

Specifies to detect Betternet protocol.

bitcasa

Specifies to detect Bitcasa protocol.

bittorrent

Specifies to detect BitTorrent protocol.

bittorrent-sync

Specifies to detect BitTorrent Sync protocol.

blackberry-store

Specifies to detect Blackberry World protocol.

blackberry

Specifies to detect BlackBerry protocol.

blackdialer

Specifies to detect Blackdialer protocol.

blackplanet-radio

Specifies to detect BlackPlanet Radio protocol.

box

Specifies to detect BOX protocol.

btn

Specifies to detect BTN protocol.

callofduty

Specifies to detect Call of Duty protocol.

cbssports

Specifies to detect Cbs Sports protocol.

chikka

Specifies to detect Chikka protocol.

cisco-jabber

Specifies to detect Cisco Jabber protocol.

citrix

Specifies to detect Citrix Independent Computing Architecture (ICA) protocol.

clubbox

Specifies to detect Clubbox protocol.

clubpenguin

Specifies to detect Club Penguin protocol.

comodounite

Specifies to detect Comodo EasyVPN protocol.

cyberghost

Specifies to detect CyberGhost VPN protocol.

crackle

Specifies to detect Crackle protocol.

crossfire

Specifies to detect Crossfire protocol.

crunchyroll

Specifies to detect Crunchyroll protocol.

curiosity-stream

Specifies to detect CuriosityStream protocol.

dashradio

Specifies to detect Dashradio protocol.

danzwave

Specifies to detect Danzwave protocol.

ddlink

Specifies to detect DDLink protocol.

deezer

Specifies to detect Deezer protocol.

didi

Specifies to detect DiDi protocol.

directconnect

Specifies to detect Direct Connect protocol.

directv

Specifies to detect DirecTV protocol.

discord

Specifies to detect Discord protocol.

disneymovies

Specifies to detect Disney Movies protocol.

dish-anywhere

Specifies to detect Dish Anywhere protocol.

dns-tunneling

Specifies to detect DNS Tunneling protocol.

dofus

Specifies to detect DOFUS protocol.

dramafever

Specifies to detect DramaFever protocol.

dropbox

Specifies to detect Dropbox protocol.

ebuddy

Specifies to detect eBuddy protocol.

edonkey

Specifies to detect eDonkey protocol.

epix

Specifies to detect Epix protocol.

eros

Specifies to detect Eros Now protocol.

espn

Specifies to detect ESPN protocol.

expressvpn

Specifies to detect ExpressVPN protocol.

facebook

Specifies to detect Facebook protocol.

facetime

Specifies to detect FaceTime protocol.

fandor

Specifies to detect Fandor protocol.

fasttrack

Specifies to detect FastTrack protocol.

feidian

Specifies to detect Feidian protocol.

ficall

Specifies to detect Ficall protocol.

fiesta

Specifies to detect FIESTA protocol.

filetopia

Specifies to detect Filetopia protocol.

filmontv

Specifies to detect FilmOn TV protocol.

fitradio

Specifies to detect Fit Radio protocol.

flash

Specifies to detect Flash protocol.

flickr

Specifies to detect Flickr protocol.

flixea

Specifies to detect Flixea protocol.

florensia

Specifies to detect Florensia protocol.

foursquare

Specifies to detect Foursquare protocol.

fox-business

Specifies to detect Fox Business protocol.

fox-news

Specifies to detect Fox News protocol.

fox-now

Specifies to detect FoxNow protocol.

fox-sports

Specifies to detect Fox Sports protocol.

foxsportsgo

Specifies to detect Fox Sports Go protocol.

freenet

Specifies to detect Freenet protocol.

friendster

Specifies to detect Friendster protocol.

fring

Specifies to detect Fring SIP protocol.

fubotv

Specifies to detect fuboTV protocol.

funshion

Specifies to detect Funshion protocol.

fxnow

Specifies to detect FxNow protocol.

gaana

Specifies to detect Gaana protocol.

gadugadu

Specifies to detect Gadu-Gadu protocol.

gamekit

Specifies to detect GameKit protocol.

gmail

Specifies to detect Gmail protocol.

gnutella

Specifies to detect Gnutella protocol.

go90

Specifies to detect Go90 protocol.

goober

Specifies to detect Goober protocol.

googlemaps

Specifies to detect Google Maps protocol.

google-music

Specifies to detect Google Music protocol.

google-push

Specifies to detect Google Push Notification protocol.

google

Specifies to detect Google protocol.

googleplay

Specifies to detect GooglePlay protocol.

googleplus

Specifies to detect GooglePlus protocol.

gotomeeting

Specifies to detect Gotomeeting protocol.

gtalk

Specifies to detect Google Talk protocol.

guildwars

Specifies to detect GuildWars protocol.

halflife2

Specifies to detect Half-Life 2 protocol.

hamachivpn

Specifies to detect Hamachi VPN protocol.

hayu

Specifies to detect HAYU protocol.

hbogo

Specifies to detect HBO Go protocol.

hbonow

Specifies to detect HBO NOW protocol.

hbonordic

Specifies to detect HBO Nordic protocol.

heytell

Specifies to detect HeyTell protocol.

hgtv

Specifies to detect HGTV protocol.

hike-messenger

Specifies to detect Hike Messenger protocol.

hls

Specifies to detect HLS protocol.

hotspotvpn

Specifies to detect HotSpot VPN protocol.

http

Specifies to detect HTTP protocol.

hulu

Specifies to detect Hulu protocol.

hyves

Specifies to detect Hyves protocol.

iax

Specifies to detect Inter-Asterisk eXchange protocol.

icall

Specifies to detect iCall protocol.

icecast

Specifies to detect Icecast protocol.

icloud

Specifies to detect iCloud protocol.

idrive

Specifies to detect iDrive protocol.

igo

Specifies to detect IGO protocol.

iheartradio

Specifies to detect iHeartRadio protocol.

imesh

Specifies to detect iMesh protocol.

imessage

Specifies to detect iMessage protocol.

imgur

Specifies to detect Imgur protocol.

imo

Specifies to detect Imo.im instant messenger protocol.

implus

Specifies to detect IM+ protocol.

instagram

Specifies to detect Instagram protocol.

iplayer

Specifies to detect BBC iPlayer protocol.

iptv

Specifies to detect IPTV protocol.

irc

Specifies to detect Internet Relay Chat protocol.

isakmp

Specifies to detect Internet Security Association and Key Management Protocol.

iskoot

Specifies to detect iSkoot VoIP protocol.

itunes

Specifies to detect iTunes protocol.

jabber

Specifies to detect Jabber XMPP protocol.

jumblo

Specifies to detect Jumblo protocol.

jap

Specifies to detect Jap protocol.

kakaotalk

Specifies to detect Kakao Talk protocol.

kidoodle

Specifies to detect Kidoodle protocol.

kik-messenger

Specifies to detect Kik Messenger protocol.

kiswe

Specifies to detect Kiswe protocol.

klowdtv

Specifies to detect KlowdTV protocol.

kontiki

Specifies to detect Kontiki delivery protocol.

kugoo

Specifies to detect Kugoo protocol.

kuro

Specifies to detect Kuro protocol.

linkedin

Specifies to detect Linkedin protocol.

livestream

Specifies to detect Livestream protocol.

lync

Specifies to detect Microsoft Lync protocol.

magicjack

Specifies to detect MagicJack protocol.

manolito

Specifies to detect MANOLITO protocol.

mapfactor

Specifies to detect Mapfactor GPS Navigation protocol (Navigator Free, GPS Navigation).

mapi

Specifies to detect MAPI protocol.

maplestory

Specifies to detect MapleStory protocol.

meebo

Specifies to detect Meebo protocol.

meetic

Specifies to detect MEETIC protocol.

mega

Specifies to detect MEGA protocol.

mgcp

Specifies to detect Media Gateway Control Protocol.

mig33

Specifies to detect Mig33 protocol.

mlb

Specifies to detect MLB protocol.

mojo

Specifies to detect Mojo protocol.

monkey3

Specifies to detect Monkey3 protocol.

mozy

Specifies to detect Mozy protocol.

msn

Specifies to detect MSN Messenger protocol.

msrp

Specifies to detect MSRP protocol.

mute

Specifies to detect MUTE protocol.

mxtp

Specifies to detect My Mixtapez protocol.

mypeople

Specifies to detect My People protocol.

myspace

Specifies to detect MySpace protocol.

nateontalk

Specifies to detect NateOn Talk protocol.

natgeotv

Specifies to detect NatGeoTV protocol.

naverline

Specifies to detect Naver Line protocol.

navigon

Specifies to detect Navigon protocol.

nbc-sports

Specifies to detect NBC Sports protocol.

nbc-tv

Specifies to detect NBC TV protocol.

netflix

Specifies to detect Netflix protocol.

netmotion

Specifies to detect NetMotion Internet Mobility Protocol.

newsy

Specifies to detect Newsy protocol.

nick

Specifies to detect Nick and Noggin protocol.

nimbuzz

Specifies to detect Nimbuzz protocol.

nokia-store

Specifies to detect Nokia Ovi Store protocol.

nrktv

Specifies to detect NRK TV Store protocol.

odkmedia

Specifies to detect ODK Media protocol.

odnoklassniki

Specifies to detect Odnoklassniki protocol.

octoshape

Specifies to detect Octoshape protocol.

off

Specifies to detect Off-The-Record protocol.

ogg

Specifies to detect Ogg multimedia streaming protocol.

ohiofm

Specifies to detect Ohio FM streaming protocol.

oist

Specifies to detect Oist protocol.

oovoo

Specifies to detect ooVoo protocol.

opendrive

Specifies to detect Opendrive protocol.

openft

Specifies to detect OpenFT protocol.

openvpn

Specifies to detect OpenVPN protocol.

operamini

Specifies to detect Operamini protocol.

orb

Specifies to detect Internet Inter-ORB Protocol.

oscar

Specifies to detect Open System for CommunicAtion in Realtime protocol.

outlook

Specifies to detect Outlook protocol.

paltalk

Specifies to detect Paltalk protocol.

pando

Specifies to detect Pando protocol.

pandora

Specifies to detect Pandora protocol.

path

Specifies to detect Path protocol.

pbs

Specifies to detect PBS protocol.

pcanywhere

Specifies to detect PCAnywhere protocol.

periscope

Specifies to detect Periscope protocol.

pinterest

Specifies to detect Pinterest protocol.

playstation

Specifies to detect Playstation protocol.

plingm

Specifies to detect Plingm protocol.

poco

Specifies to detect Poco protocol.

pokemon-go

Specifies to detect Pokemon GO protocol.

popo

Specifies to detect Popo protocol.

pplive

Specifies to detect PPlive protocol.

ppstream

Specifies to detect PPstream protocol.

ps3

Specifies to detect PS3 protocol.

qello_concerts

Specifies to detect Qello Concerts instant messaging protocol.

qq

Specifies to detect Tencent QQ instant messaging protocol.

qqgame

Specifies to detect QQgame protocol.

qqlive

Specifies to detect QQlive protocol.

quake

Specifies to detect Quake network protocol.

quic

Specifies to detect QUIC protocol.

quicktime

Specifies to detect QuickTime protocol.

radiocom

Specifies to detect Radio.com protocol.

radio-paradise

Specifies to detect Radio Paradise protocol.

rdp

Specifies to detect Remote Desktop protocol.

rdt

Specifies to detect Real Data Transport (RDT) protocol.

redbulltv

Specifies to detect Red Bull TV protocol.

regram

Specifies to detect Regram protocol.

rfactor

Specifies to detect rFactor protocol.

rhapsody

Specifies to detect Rhapsody protocol.

rmstream

Specifies to detect RealMedia streaming protocol.

rodi

Specifies to detect Rodi protocol.

reddit

Specifies to detect Reddit protocol.

rynga

Specifies to detect Rynga protocol.

samsung-store

Specifies to detect Samsung App Store protocol.

scydo

Specifies to detect Scydo VoIP protocol.

secondlife

Specifies to detect Second Life protocol.

shalomworld

Specifies to detect Shalom World protocol.

shoutcast

Specifies to detect SHOUTcast protocol.

showtime

Specifies to detect Showtime protocol.

silverlight

Specifies to detect Silverlight protocol.

siri

Specifies to detect Apple Siri protocol.

skinny

Specifies to detect Skinny Call Control Protocol (SCCP).

skydrive

Specifies to detect Skydrive protocol.

skype

Specifies to detect Skype protocol.

slacker-radio

Specifies to detect Slacker Radio protocol.

slingbox

Specifies to detect Slingbox protocol.

slingtv

Specifies to detect Slingtv protocol.

smartvoip

Specifies to detect SmartVoip protocol.

smule

Specifies to detect Smule protocol.

snapchat

Specifies to detect SnapChat protocol.

softether

Specifies to detect Softether protocol.

somafm

Specifies to detect Soma FM protocol.

sopcast

Specifies to detect Sopcast streaming protocol.

soribada

Specifies to detect Soribada protocol.

soulseek

Specifies to detect Soulseek chat and file transfer protocol.

spark

Specifies to detect Spark protocol.

spdy

Specifies to detect SPDY protocol.

spike

Specifies to detect Spike protocol.

speedtest

Specifies to detect Speedtest protocol.

splashfighter

Specifies to detect SplashFighter protocol.

spotify

Specifies to detect Spotify music streaming protocol.

ssdp

Specifies to detect Simple Service Discovery Protocol.

ssl

Specifies to detect SSL Protocol.

starz

Specifies to detect Starz Play protocol.

stealthnet

Specifies to detect StealthNet RShare network protocol.

steam

Specifies to detect Steam file transfer protocol.

stun

Specifies to detect Session Traversal Utilities for NAT protocol.

subsplash

Specifies to detect Ligonier Ministries protocol.

sudaphone

Specifies to detect Sudaphone protocol.

svtplay

Specifies to detect SVTPlay protocol.

tagged

Specifies to detect Tagged protocol.

talkatone

Specifies to detect Talkatone protocol.

taxify

Specifies to detect Taxify protocol.

tango

Specifies to detect TAco Next Generation Objects hardware control system protocol.

teamspeak

Specifies to detect TeamSpeak VoIP gaming client protocol.

teamviewer

Specifies to detect TeamViewer remote control protocol.

telegram

Specifies to detect Telegram protocol.

thunder

Specifies to detect Thunder (Xunlei) download manager protocol.

tidal

Specifies to detect TIDAL protocol.

tinder

Specifies to detect Tinder protocol.

tmo-tv

Specifies to detect TMO TV protocol.

tor

Specifies to detect Tor hidden service (anonymizer) protocol.

truecaller

Specifies to detect Truecaller protocol.

truphone

Specifies to detect Truphone WiFi VoIP protocol.

tumblr

Specifies to detect Tumblr protocol.

tunein-radio

Specifies to detect TuneIn Radio protocol.

tunnelvoice

Specifies to detect Tunnel VoIP protocol.

turbovpn

Specifies to detect TurboVPN protocol.

tvants

Specifies to detect TVAnts protocol.

tvland

Specifies to detect TV Land protocol.

tvuplayer

Specifies to detect TVUPlayer protocol.

tv2sumo

Specifies to detect Tv2Sumo protocol.

twitch

Specifies to detect Twitch protocol.

twitter

Specifies to detect Twitter protocol.

ufc

Specifies to detect UFC and UFC Fight Pass protocols.

ultrabac

Specifies to detect UltraBac protocol.

ultrasurf

Specifies to detect UltraSurf protocol.

univision

Specifies to detect Univision Deportes protocol.

upc-phone

Specifies to detect UPC Phone protocol.

usenet

Specifies to detect Usenet Network News Transfer Protocol (NNTP) protocol.

ustream

Specifies to detect Ustream protocol.

uusee

Specifies to detect UUSee on-demand streaming protocol.

vchat

Specifies to detect VChat protocol.

veohtv

Specifies to detect VeohTV television via Internet protocol.

vessel

Specifies to detect Vessel protocol.

vevo

Specifies to detect Vevo protocol.

viber

Specifies to detect Viber VoIP protocol.

viki

Specifies to detect Viki protocol.

vimeo

Specifies to detect Vimeo protocol.

vine

Specifies to detect Vine protocol.

voipdiscount

Specifies to detect VoipDiscount protocol.

vopium

Specifies to detect Vopium protocol.

voxer

Specifies to detect Voxer Walkie Talkie protocol.

vpnmaster

Specifies to detect VPN Master protocol.

vpnx

Specifies to detect VPN-X cross-platform protocol.

vtok

Specifies to detect Vtok protocol.

vtun

Specifies to detect VTun (Virtual Tunnel) protocol.

vudu

Specifies to detect Vudu protocol.

warcft3

Specifies to detect Warcraft 3 game protocol.

waze

Specifies to detect Waze protocol.

webex

Specifies to detect Webex protocol.

wechat

Specifies to detect Wechat protocol.

weibo

Specifies to detect Weibo protocol.

whatsapp

Specifies to detect WhatsApp messaging protocol.

wii

Specifies to detect Wii Remote Bluetooth protocol.

windows-azure

Specifies to detect Windows Azure Cloud Services protocol.

windows-store

Specifies to detect Windows Phone App Store protocol.

winmx

Specifies to detect WinMX Peer Network Protocol (WPNP).

winny

Specifies to detect Winny anonymizing protocol.

wmstream

Specifies to detect Windows Media HTTP Streaming Protocol.

wofkungfu

Specifies to detect wofkungfu protocol.

wofwarcraft

Specifies to detect World of Warcraft gaming protocol.

wuala

Specifies to detect Wuala protocol.

wwe

Specifies to detect WWE protocol.

xbox

Specifies to detect Xbox protocol.

xdcc

Specifies to detect eXtended Direct Client-to-Client protocol.

xing

Specifies to detect Xing protocol.

xfinity

Specifies to detect Xfinity TV protocol.

yahoo

Specifies to detect Yahoo! Messenger protocol.

yahoomail

Specifies to detect Yahoo Mail protocol.

yiptv

Specifies to detect YipTV protocol.

yogafree

Specifies to detect Yogafree protocol.

youku

Specifies to detect Youku protocol.

yourfreetunnel

Specifies to detect your free Tunnel chat protocol.

youtube

Specifies to detect Youtube protocol.

zattoo

Specifies to detect Zattoo IPTV protocol.

zello

Specifies to detect Zello protocol.

+

More than one of the above keywords can be entered within a single command.

Usage Guidelines

Use this command to configure the detection of all or specific P2P protocol(s). Multiple keywords can be specified in a single command.

Example

The following command enables detection of all P2P protocols:

```
p2p-detection protocol all
```

p2p detection debug parameters

This command enables/disables the detection of all or specified peer-to-peer (P2P) debug parameters.

Product

ADC

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax

```
p2p-detection debug-param protocol-param  p2p_force_bailout_value value
```

snapchat_story_spotlight *value* **p2p_quic_ietf_decrypt** *value*
p2p_quic_ietf_frag_detection *value*
tls_quic_ch_frag_detection *value*

p2p_force_bailout_value

Specifies that based on the number of packets configured, p2p analysis will be forced to bailout. p2p uses maxmium packets per flow for analysis.The values are:

- Default value is 300
- Minimum value allowed is 2
- Maximum value allowed is 300

Note It is recommended to use 300 as the maximum value. Lower values will have an impact on detection.

fb_insta_video_detection *value*

Enables or disables subtype (unknown,streaming-video) detection for TLS flows in Facebook and IInstagram, with multiplex multiple media types in a single TCP 5-tuple.

- If value is set to 1, enables video detection for Facebook and Instagram. The flows with certain SNI for Instagram/ and Facebook will permanently remain in slow path to detect the media types exchanged in the flow.
- If value is set to 0, disables video detection for Facebook and Instagram.The flow is marked based on the first subtype exchanged in the flow and offloaded.

The values are:

- Default value is 0, which indicates disabled.
- Allowed values 0 (disable) or 1 (enable)

voip_subtype_detection *value*

Enable this keyword to differentiate audio and video flows in a VOIP call from Facebook and Viber application.

- If the **voip_subtype_detection** configuration iis disabled, both audio and video is detected as audio.
- To retain the **voip_subtype_detection** keyword across reloads, enter the configuration in the boot configuration file.

Values: Disabled by default. The allowed range value is 0 or 1, where 0 indicates **disabled**.

p2p_quic_ietf_decrypt*value*

Enables or disables the QUIC IETF decryption.

Note By default, the CLI is disabled and there's minimal impact on the performance due to TLS decryption.

The CLI needs to be entered manually to boot configuration as plugin CLI is not part of show/save configuration.

snapchat_story_spotlight *value*

The P2P parameter **snapchat_story_spotlight** *value* is added with the existing **snapchat** protocool to classify snapchat stories and spotlight to streaming-video. *value* indicates that the snapchat stories are classified based on the following specified values:

- 0: The snapchat streaming video is disabled. By default, the snapchat_story_spotlight value is 0 and it is disabled.

  1: The snapchat streaming video is enabled with minimum number of p2p packet analysis. This is the recommended value.

  2: The snapchat streaming video is enabled with more number of p2p packets.

p2p_quic_ietf_frag_detection *value*

The P2P parameter **p2p_quic_ietf_frag_detection***value* indicates that the QUIC IETF CH fragmented flows are processed based on the following specified values:

- 0: This value disables QUIC IETF of CH fragmented flows processing.

  1: This value enables QUIC IETF of CH fragmented flows processing. By default, it is enabled.

tls_quic_ch_frag_detection *value*

The P2P parameter **tls_quic_ch_frag_detection***value* distinctly identifies TLS and QUIC client hello initial fragmented packets, enabling the sharing of the Server Name Indication (SNI) once extracted for processing in the PGW.

- 0: This value disables both TLS and QUIC fragmented packets detection. By default, it is disabled.
- 1: This value enables only TLS fragmented packets detection.
- 2: This value enables only QUIC fragmented packets detection.
- 3: This value enables both TLS and QUIC fragmented packets detection.

packet-filter

This command allows you to create/configure/delete ACS packet filters.

Product ACS

Privilege Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-acs)#`

Syntax Description

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

no

If previously configured, deletes the specified packet filter from the active charging service.

packet_filter_name

Specifies the packet filter to add/configure/delete.

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

If the named packet filter does not exist, it is created, and the CLI mode changes to the ACS Packet Filter Configuration Mode wherein the packet filter can be configured.

If the named packet filter already exists, the CLI mode changes to the ACS Packet Filter Configuration Mode for that packet filter.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete an ACS packet filter.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-packet-filter)#

Also see the *ACS Packet Filter Configuration Mode Commands* chapter.

Example

The following command creates a packet filter named *filter3*, and enters the ACS Packet Filter Configuration Mode:

packet-filter filter3

passive-mode

This command allows you to configure the Active Charging Service to operate in passive mode, wherein ACS passively monitors copies of packets.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

`[ default | no ] passive-mode`

no

If previously enabled, disables the passive mode configuration.

default

Configures this command with its default setting.

Default: Disabled

Usage Guidelines

Use this command to put the active charging service in/out of passive mode operation, wherein ACS passively monitors copies of packets.

Example

The following command puts the active charging service into passive mode operation:

`passive-mode`

pcp-service

Creates or deletes a Port Control Protocol (PCP) service.



Important This command is customer specific. Contact your Cisco account representative for more information.

Product

ACS

NAT

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

`[ no ] pcp-service` *`pcp_service_name`* **`[ -noconfirm ]`**

no

If previously configured, deletes the specified PCP service.

pcp_service_name

Specifies the name of a PCP service.

pcp_service_name must be the name of a PCP service, and must be an alphanumeric string of 1 through 63 characters. A maximum of 5 PCP services can be configured in the active charging service.

If the named PCP service does not exist, it is created, and the CLI mode changes to the PCP Configuration Mode wherein the service can be configured. If the named PCP service already exists, the CLI mode changes to the PCP Configuration Mode.

-noconfirm

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

Usage Guidelines

Use this command to create or delete a PCP service.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-pcp-service)#

Also see the *PCP Configuration Mode Commands* chapter.

Example

The following command creates a PCP service named *pcp1*, and changes to the PCP Configuration mode:

```
pcp-service pcp1
```

policy-control bearer-bw-limit

This command allows you to enable/disable per-bearer MBR policing—bandwidth limiting.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
{ default | no } policy-control bearer-bw-limit
```

default

Configures this command with its default setting.

Default: Enable; by default, per-bearer MBR policing is enabled.

no

Disables per-bearer MBR policing.

Usage Guidelines This command allows you to enable/disable per-bearer bandwidth limiting based on bitrates received over Gx. Note that there are only two variants of this command, the default and no variants.

policy-control bind-default-bearer

For PCEF Bearer Binding in 3G and when BCM mode is UE only, this command allows you to enable/disable binding rules having QoS of default bearer to the default bearer and to not ignore/ignore other rules.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description **[default | no] policy-control bind-default-bearer**

default

Configures this command with its default setting.

Default: Disables only binding those rules having QoS of default bearer to the default bearer and specifies to not ignore other rules. Rules having respective QoS will get attached to the relevant bearers. Also TFT updates towards the UE (access side) will not be suppressed.

no

The **no** keyword functionality is same as the default setting.

Usage Guidelines This CLI command is used to bind all the PCC dynamic or predef rules received from PCRF (Bearer Control Mode (BCM) is UE_only) without QoS and ARP or with the same QoS and ARP as that of the default bearer, to the default bearer. This CLI is used for UE_Only mode.

In case no QoS is specified the rule gets attached to the default bearer. Also no TFT updates will be sent towards UE (access side). So only one default bearer will ever be created.

On receiving a PCC dynamic rule or predef rule from PCRF, having QoS/ARP other than the default bearer, then those rules are ignored and a response indicating that the rule could not be installed, is sent.

This CLI command will not work currently for dedicated bearers (secondary PDP contexts). Secondary bearers initiated by UE are not supported.

Releases prior to 12.2, when UE_Only BCM is received from PCRF, IMSA terminates the call for P-GW (GnGp setup). Release 12.2 onwards, the P-GW call is not terminated so as to be in compliance with 3GPP

standard specification TS 29.212, but Traffic Flow Template (TFT) updates towards UE (access side) will be supported.



Important This CLI is applicable to all the rulebases in the chassis configuration. If the rulebase is changed to some other rulebase in the interim period or anytime later, this CLI will continue to apply to the current new rulebase too.

policy-control burst-size

This command allows you to configure the burst size for bandwidth limiting per dynamic-rule or per bearer.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

policy-control burst-size { auto-readjust [duration *duration* **] | bytes** *bytes* **}**
{ default | no } policy-control burst-size

default | no

Configures this command with its default setting.

Default: 65535 bytes

duration *duration*

Configures the burst size equal to <seconds> of traffic.

duration must be an integer from 1 through 20.

Default: In 12.1 and earlier releases, 10 seconds. In 12.2 and later releases, 5 seconds.

bytes *bytes*

Specifies the burst size, in bytes.

bytes must be an integer from 1 through 4000000000.

Usage Guidelines

Use this command to configure the burst size for bandwidth limiting per dynamic-rule or per bearer.

Example

The following command configures the burst size for bandwidth limiting per dynamic-rule or per bearer equal to 10 seconds of traffic:

```
policy-control burst-size auto-readjust
```

policy-control charging-action-override

This command has been removed from the ACS Configuration Mode, and replaced by the **charging-action-override** command in the ACS Rulebase Configuration Mode.

policy-control charging-rule-base-name

This command allows you to configure how the Charging-Rule-Base-Name AVP from PCRF is interpreted, either as ACS rulebase or ACS group-of-ruledefs.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
policy-control charging-rule-base-name { active-charging-group-of-ruledefs
 | active-charging-rulebase [ ignore-when-removed ] [ use-first ]}
default policy-control charging-rule-base-name
no policy-control charging-rule-base-name active-charging-rulebase
use-first
```

default

Configures this command with its default setting(s).

Default:

- **charging-rule-base-name**: **active-charging-group-of-ruledefs**
- **use-first**: Disabled

no

If multiple Charging-Rule-Base-Name are received from the PCRF, specifies to select the last rulebase. This is the default behavior.

active-charging-group-of-ruledefs

Specifies interpreting Charging-Rule-Base-Name as ACS group-of-ruledefs.

active-charging-rulebase [ignore-when-removed][use-first]

Specifies interpreting Charging-Rule-Base-Name as ACS rulebase.

When Charging-Rule-Base-Name AVP is interpreted as ACS rulebase, if PCRF requests the removal of a Charging-Rule-Base-Name, which is the same as the rulebase used for that PDP context, the PDP context is terminated. This is because after removal of the rulebase, the PDP context will have no rulebase. This is the default behavior.

ignore-when-removed: Specifies to ignore PCRF request for removal of Charging-Rule-Base-Name, and take no action. If this keyword is not configured, the PDP context from which the rulebase is removed gets terminated.

use-first: If multiple Charging-Rule-Base-Name are received from the PCRF, since a call can only have one ACS rulebase applied, specifies to select the first rulebase. If previously enabled, to disable this configuration, use the **no policy-control charging-rule-base-name active-charging-rulebase use-first** command. If this keyword is not configured, by default, the last rulebase is selected.

For each call, this interpretation is decided at call setup, and will not be changed during the life of that call. Change will only apply to new calls coming up after the change.

Usage Guidelines

Use this command to configure interpretation of Charging-Rule-Base-Name AVP from PCRF either as ACS group-of-ruledefs or as ACS rulebase.

Example

The following command configures interpreting of Charging-Rule-Base-Name AVP as ACS rulebase:

```
policy-control charging-rule-base-name active-charging-rulebase
```

policy control def-bearer-qos-change

This command allows you to increase the buffer that is used for storing PCRF messages when the Default-Bearer-QoS change is in pending state.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

policy-control def-bearer-qos-change pending-buffer-size *buffer_size*
no policy-control def-bearer-qos-change

no

Configures this command with its default setting.

Default: 2

def-bearer-qos-change

Sets the Default-Bearer-QoS change parameters.

pending-buffer-size *buffer_size*

Specifies the buffer size for storing the PCRF messages when Default-Bearer-QoS change is pending. The *buffer_size* is an integer ranging from 2 through 4.

Usage Guidelines

The minimum configured value is 2 and maximum is 4.

Default value should suffice for most of the use cases. Increased value should be used as per use case and memory usage should also be considered.

The CLI command takes effect for new calls.

policy-control dynamic-rule-limit

This command allows you to enable/disable per-dynamic-rule MBR policing—bandwidth limiting.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

{ default | no } policy-control dynamic-rule-limit

default

Configures this command with its default setting.

Default: Enable; by default, per-dynamic-rule MBR policing is enabled.

no

Disables per-dynamic-rule MBR policing.

Usage Guidelines

This command allows you to enable/disable per-dynamic-rule bandwidth limiting based on bitrates received over Gx. Note that there are only two variants of this command, the default and no variants.

policy-control l7-dynamic-rules

This command allows you to enable/disable the L7 capabilities through Charging-Rule-Definition AVP received over Gx interface.

Product



Important This CLI command is license dependant. Contact your Cisco account representative for more information on the licensing requirements.

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

[default | no] policy-control l7-dynamic-rules

default

Configures this command with its default setting.

Default: Disabled i.e. activation of L7 dynamic rules through Charging-Rule-Definition AVP will be disabled.

no

Disables the activation of L7 dynamic rules through Charging-Rule-Definition AVP if already activated.

Usage Guidelines

This command allows you to enable/disable the L7 capabilities through Charging-Rule-Definition AVP received over Gx interface.

In releases prior to 20, only up to L4 dynamic rule provisioning and activation was supported by the gateway. In release 20, the dynamic rule is extended to support L7 capabilities. This is accomplished by introducing these two optional Diameter AVPs "L7-Application-Description" and "Rule-Condition-Action" as part of the grouped AVP "Charging-Rule-Definition".

When Out-of-Credit (OOC) trigger is sent from OCS to PCRF, L7 dynamic rule is sent from PCRF along with a condition and action which allow the subscriber to access specific URLs. The condition is the trigger when to apply the action. For example: If OOC (quota exhaustion condition) is sent from OCS, PCEF should allow (action) all the packets matching that rule (rating-group) to pass through. Once the relocation of credit occurs the gateway reverts back the special treatment for these URLs.

This feature is configured in such a way that PCEF/PCRF is able to fully support L7 dynamic rules and thereby enabling dynamic routes to redirect L7 traffic.



Important This feature requires a valid license to be installed prior to configuring this feature. Contact your Cisco account representative for more information on the licensing requirements.

For more information on this feature, refer to the *ECS Administration Guide*.

policy-control report-rule-failure-once

This command enables or disables the feature which prevents the rule failure loop between PCRF and PCEF.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

`[ default | no ] policy-control report-rule-failure-once`

default

Configures this command with its default setting.

Default: Disabled.

no

The **no** keyword functionality is same as the default setting.

Usage Guidelines

Use this command to send CCR-U only once for the same rule failure.

policy-control retransmissions-counted

This command allows you to enable/disable charging of retransmitted packets when they hit a dynamic rule.

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.**

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-acs)#`

Syntax Description

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

default | no

Disables charging of retransmitted packets when they hit a dynamic rule.

Default: Disabled; no retransmissions counted.

Usage Guidelines

Use this command to enable/disable charging of retransmitted packets when they hit a dynamic rule.

Example

The following command enables retransmissions to be charged when they hit a dynamic rule:

`policy-control retransmissions-counted`

policy-control time-based-pcc-rule

This command allows you to configure the PCC rule with activation or deactivation time.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-acs)#`

Syntax Description

`[ default | no ] policy-control time-based-pcc-rule install-on-activation-time remove-on-deactivation-time`

default | no

Configures the PCC rule with activation or deactivation time.

Default: Disabled.

Usage Guidelines

Use this command to configure a PCC rule with activation or deactivation time.

Example

The following command configures a PCC rule by installing the PCC rule only on activation time and removing the rule on deactivation time.

```
policy-control time-based-pcc-rule install-on-activation-time
remove-on-deactivation-time
```

policy-control token-replenishment-interval

This command configures token replenishment interval for MBR enforcement at the Active Charging Service level.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
[ no ] policy-control token-replenishment-interval { 10ms [
multiplication-factor < 2..100 > ] }
```

no

Disables token replenishment interval at Active Charging Service level.

token-replenishment-interval

Configures token-replenishment-interval. The available values range from 10ms to 1000ms (1 sec).

multiplication-factor

Configures multiplication factor of 10 ms as token replenishment interval. Multiplication-factor is configurable only if token replenishment interval is 10 ms.

Usage Guidelines

Use this command to configure token replenishment interval for MBR enforcement at the Active Charging Service level. By default, this CLI is disabled.

Example

The following commands generates peak-data-rate in Bytes of token every 1sec (1000ms).

```
policy-control token-replenishment-interval 10ms multiplication-factor
100
```

policy-control update-default-bearer

For PCEF Bearer Binding in 4G, this command allows you to enable/disable binding rules having QoS of default bearer to the default bearer and to not ignore/ignore other rules.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

[default | no] policy-control update-default-bearer

default

Configures this command with its default setting.

Disables only binding those rules having QoS of default bearer to the default bearer and specifies to not ignore other rules. Rules having respective QoS will get attached to the relevant bearers. Also TFT updates towards UE (access side) will not be suppressed.

no

Enables binding rules having QoS of default bearer to the default bearer and specifies to ignore other rules. In case no QoS is specified the rule gets attached to default bearer. Also TFT updates towards UE (access side) will be suppressed for default bearer. So only one default-bearer will ever be created.



Caution Upon executing this CLI command "**no policy-control update-default-bearer**", system crash is likely to occur if the TFT information is not added to the charging-action.

Usage Guidelines

This CLI command is used to bind all the PCC dynamic or predef rules received from PCRF without QoS and ARP or with the same QoS and ARP as that of the default bearer, to the default bearer.

On receiving a PCC dynamic rule or predef rule from PCRF, having QoS/ARP other than the default bearer, then those rules are ignored and a response indicating that the rule could not be installed, is sent.

This CLI command will not work currently for dedicated bearers (secondary PDP contexts). Secondary bearers initiated by UE are not supported.

Releases prior to 12.2 TFT updates were sent towards the UE (access side) on all bearers. Release 12.2 onwards, TFT updates will be suppressed towards the UE (access side) for default bearer, if the CLI is enabled.



Important This CLI is applicable to all the rulebases in the chassis configuration. If the rulebase is changed to some other rulebase in the interim period or anytime later, this CLI will continue to apply to the current new rulebase too.

port-map

This command allows you to create/configure/delete port maps.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

port-map *port_map_name* **[-noconfirm]**
no port-map *port_map_name*

no

If previously configured, deletes the specified port map from the active charging service.

port_map_name

Specifies the port map to add/configure/delete.

port_map_name must be the name of a port map, and must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters. Each port map must have a unique name.

If the named port map does not exist, it is created, and the CLI mode changes to the ACS Port Map Configuration Mode wherein the port map can be configured.

If the named port map already exists, the CLI mode changes to the ACS Port Map Configuration Mode for that port map.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete an ACS port map.

The port map name must be unique with in the service. Host pool, port map, IMSI pool, and firewall, routing, and charging ruledefs must have unique names. A maximum of the 256 port maps can be created.



Important Port maps in use in other ruledefs cannot be deleted.

Also see the *ACS Port Map Configuration Mode Commands* chapter.

Example

The following command creates a port map named *portmap1*, and enters the ACS Port Map Configuration Mode:

```
port-map portmap1
```

qos-group-of-ruledefs

This command allows you to create/configure/delete a qos-group-of-ruledefs.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

qos-group-of-ruledefs *qos_group_of_ruledefs_name* **[-noconfirm] [description** *description* **]**
no qos-group-of-ruledefs *qos_group_of_ruledefs_name*

no

If previously configured, deletes the specified qos-group-of-ruledefs from the active charging service.

qos_group_of_ruledefs_name

Specifies the qos-group-of-ruledefs to add/configure/delete.

qos_group_of_ruledefs_name must be the name of a qos-group-of-ruledefs, and must be an alphanumeric string of 1 through 63 characters. Each qos-group-of-ruledefs must have a unique name.

If the named qos-group-of-ruledefs does not exist, it is created, and the CLI mode changes to the ACS QoS-Group-of-Ruledefs Configuration Mode wherein the group can be configured.

If the named qos-group-of-ruledefs already exists, the CLI mode changes to the ACS QoS-Group-of-Ruledefs Configuration Mode for that group.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

description *description*

Specifies an optional description of the group, such as purpose of setting up the group, to be included in the configuration.

Usage Guidelines

Use this command to create/configure/delete a qos-group-of-ruledefs.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-qos-group-of-ruledefs)#

Also see the *ACS QoS-Group-of-Ruledefs Configuration Mode Commands* chapter.

Example

The following command creates a qos-group-of-ruledefs named *group1*, and enters the ACS QoS-Group-of-Ruledefs Configuration Mode:

```
qos-group-of-ruledefs group1
```

radio-congestion

This command allows you to create/configure/delete Radio Congestion policy.



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

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

radio-congestion policy *policy_name* **[-noconfirm]**
no radio-congestion policy *policy_name*

no

If previously configured, deletes the specified Radio Congestion policy from the active charging service.

policy_name

Specifies the Radio Congestion policy to add/configure/delete.

policy_name must be an alphanumeric string of 1 through 63 characters.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete a Radio Congestion policy.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-radio-congestion-policy)#

Also see the *Radio Congestion Policy Configuration Mode Commands* chapter.

Example

The following command creates a policy named *test123*, and changes to the Radio Congestion Policy Configuration Mode:

radio-congestion policy test123

readdress-server-list

This command allows you to create/delete server list for DNS redirection.



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

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-acs)#`

Syntax Description

[no] readdress-server-list *server_list_name* **[-noconfirm]**

no

If previously configured, deletes the specified readdress server list from the active charging service.

server_list_name

Specifies the server list to add/configure/delete for DNS redirection.

server_list_name must be an alphanumeric string of 1 through 63 characters and can contain punctuation characters. Each server list must have a unique name.

If the named server list does not exist, it is created, and the CLI mode changes to the ACS Readdress Server List Configuration Mode wherein the servers can be configured.

If the named server list already exists, the CLI mode changes to the ACS Readdress Server List Configuration Mode for that server list.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/delete server list for DNS redirection.

To add the servers to the server list, see the **server** command in the *ACS Readdress Server List Configuration Mode* chapter.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-readdress-server-list)#

Also see the *ACS Readdress Server List Configuration Mode* chapter.

Example

The following command creates a charging action named *homeDNSserver* and changes to the ACS Readdress Server List Configuration Mode:

```
readdress-server-list homeDNSserver
```

redirect user-agent

This command allows you to specify the user agent for conditional redirection of traffic flows.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

[no] redirect user-agent *user_agent_name*

no

If previously configured, deletes the specified user agent from the active charging service.

user_agent_name

Specifies the user agent to be used for redirecting traffic flow.

user_agent_name must be the name of a user agent, and must be an alphanumeric string of 1 through 32 characters.

A maximum of 16 user-agents can be configured in the active charging service.

Usage Guidelines

Use this command to redirect the traffic flow with conditions based on configured user-agent name. This user agent is used with **flow action** command in the ACS Charging Action Configuration Mode.

Example

The following command specifies the redirect user agent *user_rule1* for conditional redirection of traffic flow:

```
redirect user-agent user_rule1
```

rulebase

This command allows you to create/configure/delete ACS rulebases.

Important A maximum of 512 rulebases can be configured in the active charging service.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
rulebase rulebase_name [ -noconfirm ]
no rulebase rulebase_name
```

no

If previously configured, deletes the specified rulebase from the active charging service.

rulebase_name

Specifies the rulebase to add/configure/delete.

rulebase_name must be the name of an ACS rulebase, and must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters. Each rulebase must have a unique name.

If the named rulebase does not exist, it is created, and the CLI mode changes to the ACS Rulebase Configuration Mode wherein the rulebase can be configured.

If the named rulebase already exists, the CLI mode changes to the ACS Rulebase Configuration Mode for that rulebase.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete an ACS rulebase. A rulebase is a collection of protocol rules to match a flow and associated actions to be taken for matching flow.

The default rulebase is used when a subscriber/APN is not configured with a specific rulebase to use.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-rule-base)#

Also see the *ACS Rulebase Configuration Mode Commands* chapter.

Example

The following command creates a rulebase named *test1*, and enters the ACS Rulebase Configuration Mode:

```
rulebase test1
```

rulebase-list

This command allows you to create and delete ACS rulebase lists.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
rulebase-list rulebase_list_name rulebase_name [ rulebase_name + ] strip server-ipv6
 prefix_length prefix-set prefix_set_name
no rulebase-list rulebase_list_name
```

no

If previously configured, deletes the specified rulebase list from the active charging service.

rulebase_list_name

Specifies the rulebase list to add/modify/delete.

rulebase_list_name must be the name of an ACS rulebase list, and must be an alphanumeric string of 1 through 63 characters.

rulebase_name

Specifies the rulebase name(s) to add to the rulebase list.

Each rulebase list must contain a minimum of one rulebase name, and the cumulative length of all rulebase names must not exceed 256 bytes.

rulebase_name must be the name of an ACS rulebase, and each rulebase name must be an alphanumeric string of 1 through 63 characters.

strip_server ipv6 extracts IPv4 addtresses embedded in IPv6 addresses..

Prefix_Length uses the values 32,40,48,56,64 or 96.

prefix-set configures the active configuration for Well-known prefix and Network-specific prefix.

Usage Guidelines

Use this command to create or delete an ACS rulebase list. A rulebase list is a space-separated string of rulebase names supplied to the OCS, from which the OCS chooses the rulebase to use for the subscriber. The rulebase list to use for a subscriber is specified in the APN for the subscriber.

In 12.3 and earlier releases, a maximum of 20 rulebase lists can be configured.

In 14.0 and later releases, a maximum of 128 rulebase lists can be configured.

See the **active-charging rulebase-list** command in the *APN Configuration Mode Commands* chapter.

Example

The following command creates a rulebase list named *rblist*, and adds the rulebases named *rulebase1*, *rulebase3*, and *rulebase5* to it:

```
rulebase-list rblist rulebase1 rulebase3 rulebase5
```

The following command deletes the rulebase list named *rblist*:

```
no rulebase-list rblist
```

ruledef

This command allows you to create/configure/delete ACS rule definitions.

Important In releases prior to 21.1: A maximum of 2048 ruledefs can be configured in the active charging service.

In 21.1 and later releases: A maximum of 2500 ruledefs can be configured in the active charging service.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
ruledef ruledef_name [ -noconfirm ]
no ruledef ruledef_name
```

no

If previously configured, deletes the specified ruledef from the active charging service.

ruledef_name

Specifies the ruledef to add/configure/delete.

ruledef_name must be the name of an ACS ruledef, and must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters. Each ruledef must have a unique name. Host pool, port map, IMSI pool, and firewall, routing, and charging ruledefs must have unique names.

If the named ruledef does not exist, it is created, and the CLI mode changes to the ACS Ruledef Configuration Mode wherein the ruledef can be configured.

If the named ruledef already exists, the CLI mode changes to the ACS Ruledef Configuration Mode for that ruledef.



Important If there are any changes to ruledef and the Override Control/Inheritance feature is enabled, then execute the CLI command "update active-charging override-control rulebase-config". For more information on this command, see the *Command Line Interface Reference*.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete an ACS ruledef.

A ruledef represents a set of matching conditions across multiple L3 – L7 protocol based on protocol fields and state information. Each ruledef can be used across multiple rulebases within the active charging service.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-acs-ruledef)#

Also see the *ACS Ruledef Configuration Mode Commands* chapter.

Example

The following command creates an ACS ruledef named *test1*, and enters the ACS Ruledef Configuration Mode:

```
ruledef test1
```

service-scheme

This command allows you to enable association of service-scheme based on trigger events.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

`[ no ] service-scheme` *`service_scheme_name`* **`[ -noconfirm ]`**

no

If previously configured, deletes the specified service scheme configuration from the active charging service.

service_scheme_name

Specifies the service scheme to add/configure/delete.

service_scheme_name must be a service scheme name, and must be an alphanumeric string of 1 through 63 characters.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete a service-scheme and enable association of service-scheme based on trigger events.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-acs-servscheme)#

Also see the *ACS Service Scheme Configuration Mode Commands* chapter.

Example

The following command creates a service scheme named *ss1* and changes to the ACS Service Scheme Configuration Mode:

```
service-scheme ss1
```

sip advanced

This command enables SIP ALG to maintain the same tag parameters (from and to tag) for Authorization or Proxy Authentication requests.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

`[ default | no ] sip advanced out-of-dialog-request retain-tag`

default

Configures this command with its default setting.

Default: Disabled

no

If previously enabled, disables the SIP ALG configuration.

Usage Guidelines

Use this command to enable SIP ALG to maintain the same tag parameters (from and to tag) while processing 4xx responses for Authorization or Proxy Authentication requests as described in section 8.1.3.5 of RFC 3261 (SIP: Session Initiation Protocol).

statistics-collection

This command allows to dynamically enable collection of VPP offload statistics, Charging, Firewall or Post-processing ruledef statistics.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
statistics-collection { all | ruledef { all | charging | firewall |
post-processing | vpp }
{ default | no } statistics-collection { vpp }
```

default

Configures this command with its default setting. By default, statistics collection is disabled.

no

Disables dynamic statistics collection.

all

Specifies to collect all statistics.

ruledef

Specifies to collect ruledef statistics.

all | charging | firewall | post-processing

- **all**: Specifies to collect all ruledef statistics.

- **charging**: Specifies to collect charging ruledef statistics.
- **firewall**: Specifies to collect firewall ruledef statistics.
- **post-processing**: Specifies to collect post-processing ruledef statistics.

vpp

Configures VPP statistics collection. By default, this CLI is disabled.

Use the **no statistics-collection vpp** command to remove VPP statistics collection.

Usage Guidelines

Use this command to dynamically enable collection of ruledef statistics — Charging, Firewall or Post-processing. 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".

Example

The following command will collect firewall ruledef statistics:

```
statistics-collection ruledef firewall
```

The following command will collect vpp offload statistics:

```
statistics-collection vpp
```

subs-class

This command allows you to configure Active Charging Service subscriber class.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

[no] subs-class *subs_class_name* **[-noconfirm]**

no

If previously configured, deletes the specified configuration from the active charging service.

subs_class_name

Specifies the subscriber class to add/configure/delete.

subs_class_name must be an alphanumeric string of 1 through 63 characters.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete a subscriber class.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-acs-subsclass)#

Also see the *ACS Subscriber Class Configuration Mode Commands* chapter.

Example

The following command creates a subscriber class named *sc1* and changes to the ACS Subscriber Class Configuration Mode:

```
subs-class sc1
```

subscriber-base

This command allows you to configure Active Charging Service subscriber base.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

`[ no ] subscriber-base` *`subs_base_name`* **`[ -noconfirm ]`**

no

If previously configured, deletes the specified configuration from the active charging service.

subs_base_name

Specifies the subscriber base to add/configure/delete.

subs_base_name must be an alphanumeric string of 1 through 63 characters.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete a subscriber base. Only one subscriber-base configuration is currently allowed and it is recommended to use the subscriber base name as *default*.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-subscriber-base)#

Also see the *ACS Subscriber Base Configuration Mode Commands* chapter.

Example

The following command creates a subscriber base named *default* and changes to the ACS Subscriber Base Configuration Mode:

```
subscriber-base default
```

system-limit flow-chkpt-per-call

This command allows you to control the number of flows that can be checkpointed per call.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
system-limit flow-chkpt-per-call max_chkpt_flows
default system-limit flow-chkpt-per-call
```

default

Configures this command with its default setting.

Default value: 10

max_chkpt_flows

Specifies the maximum number of flows to be checkpointed per subscriber.

max_chkpt_flows must be an integer from 1 through 100.

Usage Guidelines

When this CLI command is configured, this sets the limit of flows per call to a value so that session level limits for recovered flows are not reached during initial calls or with subscribers having high number of flows.

The maximum number of flows that can be checkpointed per call are 100. A value of 0 indicates that there is no limit on the number of flows.

Example

The following command sets the number of flows to be checkpointed to *50*:

```
system-limit flow-chkpt-per-call 50
```

system-limit l4-flows

This command allows you to configure the system-wide Layer 4 flow limit.

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

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

system-limit l4-flows *limit*
{ default | no } system-limit l4-flows

default

Configures this command with its default setting.

Default: Disabled; same as **no system-limit l4-flows**

no

Disables the limit checking configuration.

limit

Specifies the Layer 4 flows limit.

limit must be an integer from 1 through 2147483647.

Usage Guidelines

Use this command to configure the system-wide limit for Layer 4 flows.

The System-wide L4 Flow Limiting feature provides the capability to limit the number of TCP and UDP flow over the system. This limiting can be applied to all subscribers attaching to the system and to all APNs. This feature is compatible with the existing per-subscriber limiting (configured using the flow limit-for-flow-type charging action). Both limiting can be active in the same time.

System-wide flow limiting is implemented by comparing the "Effective Flows" periodically (~ every 10 seconds) against the configurable "System-wide Flow Limit". Where "Effective Flows" is the number of active data sessions, each identified by the 5-tuple key. If the "Effective Flows" exceeds the "System-wide Flow Limit", the Resource Manager indicates it to the active charging service. When ACS is aware of the "System-wide Flow Limit" being reached, no more data sessions are setup. The packets are discarded. While processing a successive flow-usage update from active charging service a change in behavior is indicated to active charging service to start accepting data sessions. As this relies on periodic reporting there is an inherent delay in the detection of "exceeding/returning once exceeded" to the flow limit.

Example

The following command sets the system limit for L4 flows to *100*:

```
system-limit l4-flows 100
```

tcp-acceleration-profile

This command configures the TCP Acceleration profile for Inline TCP Optimization.

Product

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

tcp-acceleration-profile *profile_name*
no tcp-acceleration-profile

no

Disables the TCP Acceleration profile configuration.

Usage Guidelines

Use this command to configure a TCP Acceleration profile. Refer to *ACS TCP Acceleration Profile Configuration*mode for information on configuring the profile parameters.

tcp-acceleration

This command enables TCP Acceleration in the ACS Configuration mode.

Product

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

[no] tcp-acceleration

no

Disables TCP Acceleration.

tcp-acceleration

Enables TCP Acceleration feature.

Usage Guidelines Use this command to enable the TCP Acceleration feature.

tethering-database

This command allows you to enable/disable the Tethering Detection feature, and load the databases from the specified files into the service.



Important This command is available only if the *Smartphone Tethering Detection* license is enabled. Contact your Cisco account representative for more information.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

tethering-database [ipv6-os-signature *ipv6os_signature_db_file_name* **| os-signature** *os_signature_db_file_name* **| tac** *tac_db_file_name* **| ua-signature** *ua_signature_db_file_name* **] +**
{ default | no } tethering-database

default

Configures this command with its default setting.

Default: Tethering Detection feature is disabled, and the database file names are reset to their default values.

no

Disables Tethering Detection.

ipv6-os-signature *ipv6os_signature_db_file_name*

Specifies the IPv6 OS Signature database file to load.

ipv6os_signature_db_file_name must be the name of the IPv6 OS Signature database file, and must be an alphanumeric string of 1 through 255 characters.

Default filename: **v6-os-db**

os-signature *os_signature_db_file_name*

Specifies the OS Signature database file to load.

os_signature_db_file_name must be the name of the OS Signature database file, and must be an alphanumeric string of 1 through 255 characters.

Default filename: **os-db**

tac *tac_db_file_name*

Specifies the TAC database file to load.

tac_db_file_name must be the name of a TAC database file, and must be an alphanumeric string of 1 through 255 characters.

Default filename: **tac-db**

ua-signature *ua_signature_db_file_name*

Specifies the User Agent (UA) Signature database file to load.

ua_signature_db_file_name must be the name of a UA Signature database file, and must be an alphanumeric string of 1 through 255 characters.

Default filename: **ua-db**

+

Indicates that more than one of the preceding option can be entered in a single command.

Usage Guidelines

Use this command to enable the Tethering Detection feature, and load the OS, TAC, and UA databases from the specified files into the service.

Tethering refers to the use of a smartphone as a USB dongle/modem to provide Internet connectivity to laptops/PDAs/tablets like iPad, using the smartphone's data plan. Typically many operators have in place an eat-all-you-can-get data plan for smartphones, the usage of which is intended to be from the smartphone as a mobile device. However, some users use the low rate/unlimited usage of data plan to provide Internet connectivity to their laptops in places where normal Internet connection via broadband/WiFi might be more costly/not available/insecure.

Operators are interested in detecting such usage of a smartphone as a modem to better understand the usage across their networks and offer plans inline to that usage to their customers. They may also charge the tethered and non-tethered traffic separately.

After Tethering Detection has been enabled here (regardless, it must also be enabled within the rulebase), this CLI command may be used to change the databases with the specified databases.

The files are picked from the disk file system within the /databases directory. If a file name value is not configured, the default file names, *v6-os-db, os-db*, *tac-db*, and *ua-db*, are used.

For more information on the Tethering Detection feature, refer to the *Enhanced Charging Services Administration Guide*.

Example

The following command enables Tethering Detection and selects the UA Signature database file named *test*:

```
tethering-database ua-signature test
```

tethering-detection

This command allows you to enable tethering detection for TAC-db lookup, DNS-based lookup, and bypass tethering detection based on interface ID.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

[no] tethering-detection { bypass interface-id *ifid* **| dns-based nat64** *ipv6_network_prefix* **| tac-db }**
default tethering-detection

default

Configures this command with the default setting. DNS-based tethering detection is enabled by default.

no

If previously configured, disables the specified configuration for tethering detection.

bypass interface-id *ifid*

Specifies the IPv6 Interface ID from IPv6 address. When configured, all IPv6 flows having this interface ID in the source IP address will bypass IP-TTL and OS based tethering detection.

You can configure a maximum number of 10 interface IDs. If no interface IDs are present, then all the configured interface IDs will be removed.

By default, tethering detection bypass will be disabled.

ifid is a 64-bit unsigned integer from IPv6 address.

dns-based nat64 *ipv6_network_prefix*

Configure DNS-based lookup for tethering detection. The configured NAT64 prefixes are used to identify the IPv6 flows that will be considered for DNS-based tethering detection.

ipv6_network_prefix must be an IPv6 colon-separated-hexadecimal notation with subnet mask bit. IPv6 also supports :: notation.

tac-db

Enables TAC-db lookup for tethering detection. This is the default behavior.

Usage Guidelines

Use this command to enable TAC-db lookup for tethering detection, DNS-based lookup for tethering detection, or bypass tethering detection based on interface ID.

All the three options to enable tethering detection can be configured in a single line of CLI.

For more information on the Tethering Detection feature, refer to the *Enhanced Charging Services Administration Guide*.

Example

The following command enables TAC-db lookup for tethering detection:

```
tethering-detection tac-db
```

Example

The following command removes the specified *ifid1* and *ifidn* interface IDs:

```
no tethering-detection bypass interface-id ifid1 ifidn
```

timedef

This command allows you to create/configure/delete ACS Time Definitions (timedefs).

Important This command is available only in StarOS 8.1 and in StarOS 9.0 and later releases.

Important A maximum of 10 timedefs can be configured in the active charging service.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

timedef *timedef_name* **[-noconfirm]**
no timedef *timedef_name*

no

If previously configured, deletes the specified timedef from the active charging service.

timedef_name

Specifies the timedef to add/configure/delete.

timedef_name must be the name of a timedef, and must be an alphanumeric string of 1 through 63 characters. Each timedef must have a unique name.

If the named timedef does not exist, it is created, and the CLI mode changes to the ACS Timedef Configuration Mode wherein timeslots for the timedef can be configured.

If the named timedef already exists, the CLI mode changes to the ACS Timedef Configuration Mode for that timedef.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete ACS timedefs for the Time-of-Day Activation/Deactivation of Rules feature. Timedefs enable activation/deactivation of ruledefs/groups-of-ruledefs such that they are available for rule matching only when they are active.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-acs-timedef)#

Also see the *ACS Timedef Configuration Mode Commands* chapter.

Example

The following command creates a timedef named *test1*, and enters the ACS Timedef Configuration Mode:

timedef test1

tpo policy

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

tpo profile

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

trigger-action

This command allows you to configure ACS trigger actions.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
[ no ] trigger-action trigger_action_name [ -noconfirm ]
        edns-format format_name [ security-profile ] profile_name
        flow action readdress server-list  server_list_name  [ hierarchy ] [
 round-robin ][ discard-on-failure ]
```

no

If previously configured, deletes the specified trigger action from the active charging service.

trigger_action_name

Specifies the trigger action to add/configure/delete.

trigger_action_name must be the name of a trigger action, and must be an alphanumeric string of 1 through 63 characters.

If the named trigger action does not exist, it is created, and the CLI mode changes to the ACS Trigger Action Configuration Mode.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

edns-format*edns_format*

Specifies the EDNS format when EDNS is applied.

security-profile*profile_name*

Specifies the security profile configuration in the EDNS to add mapping with the Device-id. This is an optional keyword.

flow action readdress server-list

flow action readdress server-list *server_list_name* **[hierarchy] [round-robin][discard-on-failure]**: Specifies IP readdressing to readdress the packets to the configured server Ips. This CLI in trigger action supports only server list configuration. It does not support single server IP or port configuration like charging action.

Usage Guidelines

Use this command to create/configure/delete an ACS trigger action.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-acs-trig-action)#

Also see the *ACS Trigger Action Configuration Mode Commands* chapter.

Example

The following command creates a trigger action named *ta1* and changes to the ACS Trigger Action Configuration Mode:

```
trigger-action ta1
```

trigger-condition

This command allows you to configure ACS trigger conditions.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

[no]trigger-condition *trigger_condn_name* **[-noconfirm]**

no

If previously configured, deletes the specified trigger condition from the active charging service.

trigger_condn_name

Specifies the trigger condition to add/configure/delete.

trigger_condn_name must be an alphanumeric string of 1 through 63 characters.

If the named trigger condition does not exist, it is created, and the CLI mode changes to the ACS Trigger Condition Configuration Mode.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete an ACS trigger condition.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-acs-trig-condn)#

Also see the *ACS Trigger Condition Configuration Mode Commands* chapter.

Example

The following command creates a trigger condition named *tc1* and changes to the ACS Trigger Condition Configuration Mode:

```
trigger-condition tc1
```

udr-format

This command allows you to create/configure/delete a User Data Record (UDR) format.

Important A maximum of 256 UDR plus EDR formats can be configured in the active charging service.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

```
udr-format udr_format_name [ -noconfirm ]
no udr-format udr_format_name
```

no

If previously configured, deletes the specified UDR format from the active charging service.

udr_format_name

Specifies the UDR format to add/configure/delete.

udr_format_name must be the name of a UDR format, and must be an alphanumeric string of 1 through 63 characters. Each UDR format must have a unique name.

If the named UDR format does not exist, it is created, and the CLI mode changes to the UDR Format Configuration Mode wherein the UDR format can be configured.

If the named UDR format already exists, the CLI mode changes to the UDR Format Configuration Mode for that UDR format.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete a UDR format in the active charging service.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-acs-udr)#

Also see the *UDR Format Configuration Mode Commands* chapter.

Example

The following command creates an UDR format named *udr_fromat1* and changes to the UDR Format Configuration Mode:

```
udr-format udr_format1
```

xheader-format

This command allows you to create/configure/delete ACS extension-header (x-header) format specifications.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax Description

xheader-format *xheader_format_name* **[-noconfirm]**
no xheader-format *xheader_format_name*

no

If previously configured, deletes the specified x-header format from the active charging service.

xheader_format_name

Specifies the x-header format to add/configure/delete.

xheader_format_name must be the name of an xheader format, and must be an alphanumeric string of 1 through 63 characters. Each x-header format must have a unique name.

If the named x-header format does not exist, it is created, and the CLI mode changes to the ACS X-header Format Configuration Mode wherein the x-header format can be configured.

If the named x-header format already exists, the CLI mode changes to the ACS X-header Format Configuration Mode for that x-header format.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete an x-header format specification in the active charging service.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-acs-xheader)#

An x-header may be specified in a charging action to be inserted into HTTP GET and POST request packets. See **xheader-insert** CLI command in the *ACS Charging Action Configuration Mode Commands* chapter. Also see the *ACS X-header Format Configuration Mode Commands* chapter.

Example

The following command creates an x-header format named *test*, and enters the ACS X-header Format Configuration Mode:

```
xheader-format test
```