Credit Control Configuration Mode Commands

The Credit Control configuration Mode is used to configure prepaid services for Diameter/RADIUS applications.

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

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

apn-name-to-be-included

This command configures whether the virtual or real Access Point Name (APN) is sent in Credit Control Application (CCA) messaging.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
apn-name-to-be-included { gn | virtual }
default apn-name-to-be-included
```

default

Configures this command with the default setting.

Default: **gn**

gn

Sends the Gn APN name in the CCA messages.

virtual

Sends the virtual APN name, if configured in the APN Configuration Mode, in the CCA messages.

Usage Guidelines

Use this command to configure the APN information in CCA messages. Virtual APN name can be set to be sent in CCA messages if it is configured in the APN Configuration Mode.

Example

The following command sets the virtual APN name to be sent in CCA message:

```
apn-name-to-be-included virtual
```

app-level-retransmission

This command enables/disables application-level retransmissions with the "T" bit set.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
app-level-retransmission { set-retransmission-bit |
unset-retransmission-bit }
default app-level-retransmission
```

default

Configures this command with the default setting.

Default: **unset-retransmission-bit**

set-retransmission-bit

Sets the retransmission bit.

unset-retransmission-bit

Unsets the retransmission bit.

Usage Guidelines

Use this command to enable application-level transmission with "T" bit set.

'T' bit setting is done only for DIABASE protocol-based rerouting and not for application-based retransmissions. In order to identify such retransmissions, the server expects the T bit to be set at all levels (both DIABASE and application) of retransmission, which can be achieved with this CLI command.

Example

The following command specifies to set retransmission bit:

```
app-level-retransmission set-retransmission-bit
```

associate

This command associates/disassociates a failure handling template with the Diameter Credit Control Application (DCCA) service.

Product

GGSN

HA

HSGW

IPSG

PDSN

P-GW

S-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

associate failure-handling-template *template_name*
no associate failure-handling-template

no

Disassociates a failure handling template with the DCCA service.

failure-handling-template *template_name*

Associates a previously created failure handling template with the DCCA service. *template_name* specifies the name for a pre-configured failure handling template. *template_name* must be an alphanumeric string of 1 through 63 characters.

For more information on failure handling templates, refer to the **failure-handling-template** command in the *Global Configuration Mode Commands* chapter.

Usage Guidelines

Use this command to associate a configured failure handling template with the DCCA service.

The failure handling template defines the action to be taken when the Diameter application encounters a failure supposing a result-code failure, Tx-expiry or response-timeout. The application will take the action given by the template. For more information on failure handling template configurations, refer to the *Diameter Failure Handling Template Configuration Mode Commands* chapter.

Important Only one failure handling template can be associated with the DCCA service. The failure handling template should be configured prior to issuing this command.

If the association is not made to the template then failure handling behavior configured in the application with the **failure-handling** command will take its effect.

Example

The following command associates a pre-configured failure handling template called *fht1* to the DCCA service:

```
associate failure-handling-template fht1
```

charging-rulebase-name

This command allows static configuration of charging rulebase name to be sent to OCS through the CCR message.

Product

eHRPD

GGSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

charging-rulebase-name *rulebase_name*
no charging-rulebase-name

no

The **no** variant, when configured, sends the rulebase that was configured in APN/subscriber template to the OCS.

rulebase_name

Specifies the name for a charging rulebase to be sent to OCS via CCR message. *rulebase_name* must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to override/change the charging rulebase name in the Gy CCRs for eHRPD, GGSN and P-GW service types.

With this feature in 18.0 release, an APN/subscriber can have a single rulebase applied to it, but allowing a static configuration to always pass a different or same rulebase to the OCS through CCR messages.

The rulebase value configured in Credit Control (CC) group will be sent to OCS via CCR. If this CLI command is not configured, then the rulebase obtained from APN/subscriber template will be sent to OCS.

The configured value of rulebase under CC group is sent in all CCR (I/U/T) messages. This implies that any change in rulebase value in CC group during mid-session gets reflected in the next CCR message.

Example

The following command defines a charging rulebase name called *rb1* in the credit control group:

charging-rulebase-name rb1

diameter dictionary

This command configures the Diameter Credit Control dictionary for the Active Charging Service (ACS).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

diameter dictionary { dcca-custom1 | dcca-custom10 | dcca-custom11 | dcca-custom12 | dcca-custom13 | dcca-custom14 | dcca-custom15 | dcca-custom16 | dcca-custom17 | dcca-custom18 | dcca-custom19 | dcca-custom2 | dcca-custom20 | dcca-custom21 | dcca-custom22 |

```
dcca-custom23 | dcca-custom24 | dcca-custom25 | dcca-custom26 |
dcca-custom27 | dcca-custom28 | dcca-custom29 | dcca-custom3 |
dcca-custom30 | dcca-custom4 | dcca-custom5 | dcca-custom6 | dcca-custom7
 | dcca-custom8 | dcca-custom9 | dynamic-load | standard }
default diameter dictionary
```

default

Configures this command with the default setting.

Default: standard dictionary

dcca-custom1 ... dcca-custom30

Configures a custom Diameter dictionary.

dynamic-load

Configures the dynamically loaded Diameter dictionary. The dictionary name must be an alphanumeric string of 1 through 15 characters.

For more information on dynamic loading of Diameter dictionaries, see the **diameter dynamic-dictionary** in the *Global Configuration Mode Commands* chapter of this guide.

standard

Configures the standard Diameter dictionary.

Default: Enabled

Usage Guidelines

Use this command to select the Diameter dictionary for ACS.

Example

The following command selects the standard Diameter dictionary:

```
diameter dictionary standard
```

diameter disable-final-reporting-in-ccru

This command controls sending of CCR-U with reporting reason as FINAL immediately on receiving a 4012 or 4010 result-code at MSCC level.

Product

Important In StarOS release 16.0 and later, this command is obsolete and is only supported for backward compatibility reasons. Release 16.0 and beyond, use the diameter msg-type { ccru| ccrt } suppress-final-reporting command for this functionality.

GGSN

HA

IPSG

PDSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

diameter disable-final-reporting-in-ccru
{ default | no } diameter disable-final-reporting-in-ccru

default | no

Configures this command with the default setting. Default behavior is to send CCR-U with reporting reason as FINAL immediately on receiving 4010/4012 result-code.

Usage Guidelines

As per the current implementation, CCR-U is sent immediately on receiving 4010 or 4012 Result-Code at MSCC level. This new CLI command controls sending of immediate CCR-U with FINAL as Reporting-Reason. All other behaviors remain almost same like a Rating-group being blacklisted.

If this CLI command is configured, on receiving the result-code 4010/4012 at MSCC-level, immediate CCR-U with FINAL as Reporting-Reason will not be sent. All USU corresponding to that rating group is reported in CCR-T message.

Example

The following command specifies not to send immediate CCR-U with FINAL as Reporting-Reason:

diameter disable-final-reporting-in-ccru

diameter dynamic-rules request-quota

This command specifies to request quota immediately in the CCR sent to the Gy interface when the traffic matches the dynamic rules with Online AVP enabled and received over Gx interface.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
diameter dynamic-rules request-quota { on-traffic-match | on-receiving-rule }
default diameter dynamic-rules request-quota
```

default

Configures this command with the default setting.

Default: **on-receiving-rule**

on-traffic-match

Requests quota only when there is traffic matching the dynamic rules with Online AVP enabled.

on-receiving-rule

Requests quota on receiving a dynamic rule with Online AVP enabled.

Usage Guidelines

Use this command to request quota when the traffic matches the dynamic rules with Online AVP enabled.

Example

The following command specifies to request quota on receiving a dynamic rule with Online AVP enabled:

```
diameter dynamic-rules request-quota on-receiving-rule
```

diameter enable-quota-retry

This command enables/disables Quota Retry Timer for blockedlisted content.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ] diameter enable-quota-retry end-user-service-denied
```

no

Configures this command with the default setting.

Usage Guidelines

Quota-Retry-Time is currently not applicable to a Rating-Group which is blockedlisted with 4010 (END_USER_SERVICE_DENIED).

If this CLI command is configured, after the quota-retry timeout, CCR-U including the RSU is sent for blockedlisted content also. That is, quota will be requested for 4010 blacklisted content also.

Without the configuration of this CLI command, the old behavior persists that is, after quota retry-timer expiry, CCR-U is not sent for 4010 blacklisted category.

Example

In releases prior to StarOS 21.26:

The following command allows sending CCR-U requesting quota for blacklisted content:

diameter enable-quota-retry end-user-service-denied

diameter exclude-mscc-in-ccr-terminate

This command enables to exclude Multiple-Services-Credit-Control (MSCC) AVP in CCR-T message.

Product

GGSN

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-dcca)#`

Syntax Description

[default | no] diameter exclude-mscc-in-ccr-terminate

default

Includes MSCC AVP in CCR-T.

no

Includes MSCC AVP in CCR-T.

Usage Guidelines

Use this command to exclude MSCC AVP in CCR-T, which is included by default.

Also, see the **diameter mscc-per-ccr-update** command.

Example

The following command specifies to exclude MSCC AVP in CCR-T:

diameter exclude-mscc-in-ccr-terminate

diameter fui-redirected-flow

This command enables to control the behavior of marking redirected HTTP flow as free-of-charge.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] diameter fui-redirected-flow allow`

no

Disables the behavior of marking redirected HTTP flow as free-of-charge.

Default: **diameter fui-redirected-flow allow**

Usage Guidelines

Use this command to control the behavior of marking redirected HTTP flow as free-of-charge when the Final-Unit-Indication (FUI) Diameter AVP comes without Filter IDs.

Important Note that the default value, when configured, does not appear in the output of the **show configuration** command output; instead appear only in the output of the **show configuration verbose** command. When the HTTP redirection feature is disabled using the **no diameter fui-redirected-flow allow** command, it will be appear in the output of the **show configuration** command.

Example

The following command specifies to allow the packets free of charge, when matching the redirected-flow:

`diameter fui-redirected-flow allow`

diameter gsu-with-only-infinite-quota

This command configures whether to accept/reject CCA messages that contain Granted-Service-Unit AVP with only infinite quota grants from the server.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
diameter gsu-with-only-infinite-quota { accept-credit-control-answer |
reject-credit-control-answer }
default diameter gsu-with-only-infinite-quota
```

default

Configures this command with the default setting.

Default: **reject-credit-control-answer**

accept-credit-control-answer

Accepts the Credit-Control-Answer message.

reject-credit-control-answer

Rejects the Credit-Control-Answer message.

Usage Guidelines

Use this command to accept/reject CCA messages that contain the Granted-Service-Unit AVP with only infinite quota grants from the server.

Example

The following command specifies to accept CCA with the Granted-Service-Unit AVP containing only Infinite quota:

```
diameter gsu-with-only-infinite-quota accept-credit-control-answer
```

diameter hdd

This command enables/disables the Hard Disk Drive (HDD) to store the failed CCR-T messages for the corresponding credit control group.

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

Product

HA

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ] diameter hdd
```

no

Disables the HDD from storing the failed CCR-T messages for the corresponding credit control group.

Usage Guidelines

Use this command to enable the HDD to store the failed CCR-T messages. The Gy application sends the failed CCR-T messages to the CDR module for storing in the HDD. By default, this feature is disabled.

In the existing implementation with Assume Positive feature, there are high chances of losing the usage data reported through the CCR-T when the session is being terminated while in Assume Positive mode. This problem is addressed by allowing the DCCA module to write the CCR-T messages in the HDD of the chassis.

In cases where the Assume-Positive interim-quota is allocated, and CCR-T is not reported/answered, the CCR-T message is written to a local file, and saved in the HDD. This local file and directory information can be fetched and parsed to account for the lost bytes/usage. The retrieval of the file can be done with the PULL mechanism.

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.

Important This feature is applicable only when Assume Positive feature is enabled.

For more information on this feature, see the *AAA Interface Administration and Reference* document.

Limitations:

- When an ICSR event occurs unexpectedly before the CCR-T is written, the CCR-T will not written to the HDD and hence the usage will be lost.
- It is expected that the customers requiring this feature should monitor the HDD and periodically pull and delete the files so that the subsequent records can be buffered.

The **diameter-hdd-module** CLI command is used to configure the file characteristics for storing the Diameter records (CCR-Ts) in the HDD. For more information on this command, see the *Diameter HDD Module Configuration Mode Commands* chapter in this guide.

Example

The following command enables the HDD to store the failed CCR-T messages:

```
diameter hdd
```

diameter ignore-returned-rulebase-id

This command configures to accept/ignore the rulebase ID in the Rulebase-Id AVP returned by the Diameter server in CCA messages.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ default | no ] diameter ignore-returned-rulebase-id`

default

Configures this command with the default setting.

Default: Accept

no

Accepts the rulebase ID received from Diameter server in CCA.

Usage Guidelines

Use this command to ignore/accept rulebase ID returned from the Diameter server in CCA.

Example

The following command ignores the rulebase ID returned from the Diameter server in CCA:

`diameter ignore-returned-rulebase-id`

diameter ignore-service-id

This command enables to accept/ignore service ID in the Service-Identifier AVP defined in the Diameter dictionaries. This command is applicable to all products that use the Gy interface.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ default | no ] diameter ignore-service-id
```

default

Configures this command with the default setting.

Default: Accept

no

Specifies to accepts the service ID.

Usage Guidelines

Use this command to ignore/accept service ID value in the Service-Identifier AVP in the Diameter dictionaries for Gy interface implementations.

This command can be used to disable the usage of the Service-Identifier AVP for Gy interface implementations even if any of the Diameter dictionaries support the Service-Identifier AVP, and if this AVP should not be used for Gy interactions but must be present in GCDRs/eGCDRs.

Example

The following command specifies to ignore service ID in the Diameter dictionaries:

```
diameter ignore-service-id
```

diameter mscc-final-unit-action terminate

This command enables either to terminate a PDP session immediately when the Final-Unit-Action (FUA) in a particular Multiple Service Credit Control (MSCC) is set as TERMINATE and the quota is exhausted for that service, or to terminate the session after all other MSCCs (categories) have used up their available quota.

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

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
diameter mscc-final-unit-action terminate { category | session {
on-per-mscc-exhaustion | on-all-mscc-exhaustion } }
default diameter mscc-final-unit-action terminate
```

default

Configures this command with the default setting.

Default: Same as **diameter mscc-final-unit-action terminate category**

category

This is the standard behavior wherein the category is terminated if the Final-Unit-Indication AVP comes with TERMINATE for a given MSCC.

session { on-per-mscc-exhaustion | on-all-mscc-exhaustion }

Terminates the session depending on the quota usage of one MSCC or all the MSCCs.

on-per-mscc-exhaustion: When the FUA in a particular MSCC is set as TERMINATE and the quota is exhausted for that service, the session will be terminated immediately regardless of the state of the other MSCCs.

on-all-mscc-exhaustion: When the FUA in a particular MSCC is set as TERMINATE and the quota is exhausted for that service, the session termination will be initiated after all the other MSCCs (categories) have used up their available quota. There will no more CCR(U) messages sent requesting quota after receiving the FUA as TERMINATE in the MSCC level.

Usage Guidelines

Use this command to terminate a PDP session immediately when the FUA in a particular MSCC is set as TERMINATE and the quota is exhausted for that service, or to terminate the session after all other MSCCs (categories) have used up their available quota.

Example

The following command terminates the PDP session after quota exhausts for all MSCCs when MSCC FUA is set to TERMINATE:

```
diameter mscc-final-unit-action terminate session on-all-mscc-exhaustion
```

diameter mscc-per-ccr-update

This command configures sending single/multiple Multiple-Services-Credit-Control (MSCC) AVP in CCR-U messages.

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

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

diameter mscc-per-ccr-update { multiple | single }
default diameter mscc-per-ccr-update

default

Configures this command with the default setting.

Default: **multiple**

multiple

Sends multiple Multiple-Services-Credit-Control AVP in a single CCR-U message.

single

Sends only one Multiple-Services-Credit-Control AVP in a CCR-U message.

Usage Guidelines

Use this command to configure sending single/multiple Multiple-Services-Credit-Control AVP in CCR-U messages.

Example

The following command configures sending a single Multiple-Services-Credit-Control AVP in CCR-U messages:

diameter mscc-per-ccr-update single

diameter msg-type

This command controls sending of CCR-U/CCR-T with reporting reason as FINAL immediately on receiving a 4012 or 4010 result-code at MSCC level or when the MSCC is in FUI Redirect/Restrict-access state.

Product

GGSN

HA

IPSG

PDSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

In 18 and later releases:

```
[ no ] diameter msg-type { ccru { suppress-final-reporting } | ccrt {
suppress-final-reporting | suppress-blacklist-reporting } }
```

In 17 and earlier releases:

```
diameter msg-type { ccru | ccrt } suppress-final-reporting
[ no ] diameter msg-type ccru suppress-final-reporting
```

no

Depending on the configuration, this keyword will selectively send FINAL either in CCR-U or CCR-T even if MSCC is in FUI Redirect/Restrict-access state and USU is zero.

The default behavior is to not send CCR-T with reporting reason as FINAL even when MSCC is in FUI Redirect/Restrict-access state and USU is zero.

Important This default behavior is applicable to all dictionaries except for dcca-custom12 and dcca-custom13 dictionaries. In the case of dcca-custom12 and dcaa-custom13, the FINAL reporting will always be sent in CCR-T even if MSCC is in FUI Redirect/Restrict-access and USU is zero.

ccru

This keyword disables Immediate FINAL reporting for result code 4010/4012 in CCR-U message.

ccrt

This keyword disables FINAL reporting for MSCC which are in no-quota and FUI Redirect/Restrict-access state.

suppress-final-reporting

Important This keyword is available only in 18.3, 19.2 and later releases.

When used with the **diameter msg-type ccru** command, this keyword disables immediate FINAL reporting for result code 4010/4012. When used with the **diameter msg-type ccrt** command, this keyword disables FINAL reporting for no-quota FUA Redirect/Restrict-access.

suppress-blacklist-reporting

Important This keyword is available only in 18.3, 19.2 and later releases.

Disables FINAL reporting for blacklisted (4010/4012) content in CCR-T.

Usage Guidelines

With this CLI command "diameter msg-type ccrt suppress-final-reporting" configured:

Before MSCC enters into FUI Redirect or Restrict-Access state, all the used quota is reported using the Reporting-Reason as "OTHER_QUOTA_TYPE". Since all the quota is reported, there is no need to send any other FINAL reporting to OCS.

Releases prior to 16.0, even if there is no quota utilization, the gateway sends FINAL with USU as '0' octets in CCR-T. In this release, the FINAL reporting in CCR message is controlled when there is no quota usage to report to the OCS server during the FUI Redirect/Restrict-access scenario.

With this CLI command "diameter msg-type ccru suppress-final-reporting" configured:

In releases prior to 15.0, CCR-U is sent immediately on receiving 4010 or 4012 Result-Code at MSCC level. This new CLI command controls sending of immediate CCR-U with FINAL as Reporting-Reason. All other behaviors remain almost same like a Rating-group being blacklisted.

If this CLI command is configured, on receiving the result-code 4010/4012 at MSCC-level, immediate CCR-U with FINAL as Reporting-Reason will not be sent. All USU corresponding to that rating group is reported in CCR-T message.

In releases prior to 18, configuration control was available for filtering FINAL USU reporting in CCR-U for blacklisted content and in CCR-T for Final-Unit-Indication (REDIRECT/RESTRICT-ACCESS) activated content. In the case of CCR-T message, there is no way to ignore the FINAL reporting for blacklisted (4010/4012) content if the FINAL was previously disabled in CCR-U.

In 18 and later releases, the current CLI configuration is enhanced to disable FINAL reporting in CCR-T message for blacklisted (4010/4012) content. The **diameter msg-type ccrt** CLI command includes an additional keyword **suppress-blacklist-reporting** to support this enhancement. The default behavior of CCR-T is to send the FINAL reporting to be sent for blacklisted (4010/4012) content, if not reported already in CCR-U.

Important This feature is available only in 18.3, 19.2 and later releases.

This feature is used to selectively control the reporting of FINAL Used-Service-Unit (USU) in CCR-T for a Rating-Group (RG) which is blacklisted using 4010 and 4012 transient result-codes. This customization is required for a seamless integration with the operator network.

Example

The following command specifies not to send FINAL reporting for FUA Redirect/Restrict-access:

```
diameter msg-type ccrt suppress-final-reporting
```

diameter origin host

This command is obsolete. See the diameter origin endpoint, on page 19 command.

diameter origin endpoint

This command configures the Diameter Credit Control Origin Endpoint.

Product All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

diameter origin endpoint *endpoint_name* **[realm** *realm_name* **]**
no diameter origin endpoint

no

Removes the Diameter Credit Control Origin Endpoint configuration.

endpoint *endpoint_name*

Specifies the Diameter Credit Control Origin Endpoint name as an alphanumeric string of 1 through 63 characters.

realm *realm_name*

Specifies the Diameter Credit Control Realm ID as an alphanumeric string of 1 through 127 characters.

Usage Guidelines

Use this command to configure the Diameter Credit Control Origin Endpoint.

The endpoint to configure should be pre-configured. For information on creating and configuring a Diameter endpoint, see the **diameter endpoint** command in the Context Configuration mode.

Example

The following command configures a Diameter Credit Control Origin Endpoint named *test*:

```
diameter origin endpoint test
```

diameter peer-select

This command configures the Diameter credit control primary and secondary hosts for DCCA.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

In 8.x and earlier releases:

diameter peer-select peer *peer_name* **[realm** *realm_name* **] [secondary-peer** *secondary_peer_name* **[realm** *realm_name* **]] [imsi-based start-value** *imsi_start_value* **end-value** *imsi_end_value* **]**
no diameter peer-select [imsi-based start-value *imsi_start_value* **end-value** *imsi_end_value* **]**

In 9.0 and later releases, for UMTS deployments:

diameter peer-select peer *peer_name* **[realm** *realm_name* **] [secondary-peer** *secondary_peer_name* **[realm** *realm_name* **]] [imsi-based { { prefix | suffix }** *imsi/prefix/suffix_start_value* **} [to** *imsi/prefix/suffix_end_value* **]] [msisdn-based { { prefix | suffix }** *msisdn-based/prefix/suffix_start_value* **} [to** *msisdn-based/prefix/suffix_end_value* **]]**
no diameter peer-select [imsi-based { { prefix | suffix } *imsi/prefix/suffix_start_value* **} [to** *imsi/prefix/suffix_end_value* **]] | [msisdn-based { { prefix | suffix }** *msisdn-based/prefix/suffix_start_value* **} [to** *msisdn-based/prefix/suffix_end_value* **]]**

no

Removes previously configured Diameter credit control peer selection setting.

peer ***peer_name***

Specifies the primary host name. as an alphanumeric string of 1 through 63 characters that can contain punctuation characters.

imsi-based start-value ***imsi_start_value*** **end-value** ***imsi_end_value***

Important This section applies only to 8.3 and earlier releases.

Specifies peer selection based on International Mobile Subscriber Identification (IMSI) range.

start-value *imsi_start_value* specifies the start of range in integer value of IMSI, and **end-value** *imsi_end_value* specifies the end of range in integer value of IMSI.

imsi-based { { prefix | suffix } ***imsi/prefix/suffix_start_value*** **} [to** ***imsi/prefix/suffix_end_value*** **]**

Important This section applies only to 9.0 and later releases for UMTS deployments.

Selects peer based on IMSI prefix or suffix or IMSI range.

prefix: Specifies the prefix range

suffix: Specifies the suffix range

imsi/prefix/suffix_start_value: Specifies the IMSI/prefix/suffix start value. *prefix/suffix* must be an IMSI prefix/suffix, and must be an integer from 1 through 15 characters.

imsi/prefix/suffix_end_value: Specifies the IMSI/prefix/suffix end value. *prefix/suffix* must be an IMSI prefix/suffix, and must be an integer from 1 through 15 characters that must be greater than the start value.

Important If prefix/suffix is used, the lengths of both start and end prefix/suffix must be equal. If the **prefix** or **suffix** keyword is not specified, it will be considered as suffix.

msisdn-based { { prefix | suffix } *msisdn/prefix/suffix_start_value* } [to *msisdn/prefix/suffix_end_value*]

Specifies peer selection based on MSISDN prefix or suffix or MSISDN range.

prefix: Specifies the prefix range

suffix: Specifies the suffix range

msisdn/prefix/suffix_start_value: Specifies the MSISDN/prefix/suffix start value. *prefix/suffix* must be an MSISDN prefix/suffix, and must be an integer from 1 through 15 characters.

msisdn/prefix/suffix_end_value: Specifies the MSISDN/prefix/suffix end value. *prefix/suffix* must be an MSISDN prefix/suffix, and must be an integer from 1 through 15 characters that must be greater than the start value.

realm *realm_name*

The *realm_name* must be an alphanumeric string of 1 through 127 characters, and can contain punctuation characters. The realm may typically be a company or service name.

secondary-peer *secondary_peer_name*

Specifies a name for the secondary host to be used for failover processing. When the route-table does not find an AVAILABLE route, the secondary host performs a failover processing if the diameter session failover, on page 32 command is set.

secondary_peer_name must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters.

Usage Guidelines

Use this command to configure Diameter credit control host selection.

If the **diameter peer-select** command is not configured, and if multiple peers are configured in the endpoint, the available peers configured in the endpoint are automatically chosen in a load-balanced round-robin manner.

9.0 and later releases support peer selection using prefix or suffix of IMSI or IMSI range. Subscribers are now assigned to a primary OCS instance based on the value of the IMSI prefix or suffix of a length of 1 to 15 digits. If the prefix or suffix keyword is not specified, it will be considered as suffix. Up to 64 peer selects can be configured. At a time either prefix or suffix mode can be used in one DCCA config. If prefix or suffix mode is used, the lengths of all prefix/suffix must be equal.

In 12.2 and later releases, Diameter peer selection can also be performed based on the configurable prefix or suffix of MSISDN or MSISDN range.

Each primary OCS may have a designated secondary OCS in case of failure of the primary. It will be the responsibility of the GGSN to use the appropriate secondary OCS in case of primary failure. The secondary OCS for each primary OCS will be one of the existing set of OCSs.

Note Load-balancing is not supported if the **diameter peer-select** command is configured under the credit control group.

If the directly connected hosts/peers are configured under the credit control application, thenround-robin selection is not available even if the equal weighted peers are configured under the diameter end-point. In this scenario, the primary host/peer configured under the credit control group have precedence and selected always.

Example

The following command configures a Diameter credit control peer named *test* and the realm *companyx*:

```
diameter peer-select peer test realm companyx
```

The following command configures IMSI-based Diameter credit control peer selection in the IMSI range of *1234567890* to *1234567899*:

```
diameter peer-select peer star imsi-based start-value 1234567890 end-value
 1234567899
```

The following command configures IMSI-based DCCA peer selection with IMSI suffix of *100* through *200*:

```
diameter peer-select peer test_peer realm test_realm secondary-peer
test_sec_realm realm test_realm2 imsi-based suffix 100 to 200
```

diameter pending-timeout

This command configures the maximum time period to wait for response from a Diameter peer.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
diameter pending-timeout duration deciseconds msg-type { any | ccr-event |
 ccr-initial | ccr-terminate | ccr-update }
default diameter pending-timeout
```

default

Disables DCCA resending message at pending-timeout.

duration

Specifies the timeout duration (in deciseconds). The value must be an integer from 1 through 3000.

deciseconds msg-type { any | ccr-event | ccr-initial | ccr-terminate | ccr-update }

Specifies independent timers (in deciseconds) for all message types like CCR-I, CCR-U, CCR-T and CCR-E. The default time will be 100 deciseconds (10 seconds).

This keyword option provides additional flexibility for operator to configure independent timers with reduced granularity.

This feature implementation ensures that the timer configuration is backward compatible. If the CLI command is configured without "**desiseconds**" and "**msg-type**", the configured time will be taken as seconds and while displaying the CLI it will be converted to deciseconds and msg-type will be "**any**".

after-expiry-try-secondary-host

This keyword is deprecated. This can now be managed using the **retry-after-tx-expiry** and **go-offline-after-tx-expiry** keywords in the **failure-handling** command.

Usage Guidelines

Use this command to set the maximum time for Diameter credit control to receive a response from its peer.

DCCA refers to this as the Tx Timer. Typically, this should be configured to a value smaller than the response-timeout value of Diameter Endpoint Configuration Mode. That value is typically too large for DCCA's purposes.

If DCCA gets a "no available routes" error before pending-timeout expires, then DCCA tries to send to the secondary host (if one has been configured). If DCCA gets no response and pending-timeout expires, then DCCA either tries the secondary host or gives up. This can now be managed using the **failure-handling** command.

If routing has failed, i.e., the attempt to the primary host, as well as, the attempt to the secondary host (if that has been configured), then the processing configured by the **failure-handling** command is performed.

The routing (i.e., returning a good response, no response or an error response such as "no available routes") is controlled by Diameter Endpoint Configuration Mode. That uses a watchdog timer (called Tw Timer) to attempt a different route to a host. Multiple routes could be attempted. If there's no response before the endpoint's configured response-timeout expires, then "no available routes" is the routing result. The routing logic remembers the status of routes, so it can return "no available routes" immediately, without using any timers.

The default case will disable DCCA resending message at Tx (pending-timeout). So messages are retried only at Tw (device watchdog timeout) by diabase or at response-timeout by DCCA.

Example

The following command configures a Diameter Credit Control Pending Timeout setting of *20* seconds:

```
diameter pending-timeout 20
```

diameter reauth-blockedlisted-content

This command allows reauthorization of blockedlisted content (blacklisted with Result-Code like 4012, 4010, etc) when a Rating Group (RG) based Re-Authorization Request (RAR) or generic RAR is received.

Product

GGSN

HA

IPSG

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

In releases prior to StarOS 21.26:

```
diameter reauth-blacklisted-content [ content-based-rar ]
no diameter reauth-blacklisted-content
```

From StarOS 21.26 and later releases:

```
diameter reauth-blockedisted-content [ content-based-rar ]
no diameter reauth-blockedlisted-content
```

no

Configures this command with the default setting. That means, the reauthorization of blockedlisted RG will not happen.

content-based-rar

Reauthorizes blockedlisted RG only when RG specific RAR is received.

Usage Guidelines

The current Gy implementation does not allow reauthorization of Blockedlisted content (blacklisted with Result-Code like 4012, 4010, etc) when Gy receives an RAR (either a RG based RAR or generic RAR).

With this CLI based enhancement, it is possible to perform one of the following actions:

- to reauthorize blockedlisted RG only when RG specific RAR is received.
- to reauthorize blockedlisted RG on any kind of RAR (both RG specific or generic).
- do not reauthorize blockedlisted RG (default implementation).

This feature determines if the RAR received from OCS is generic or to any specific rating-group.

If it is a generic RAR:

Note From StarOS 21.26 and later releases, the term “blacklist” is replaced with “blockedlist” in the help string.

- If this CLI command "**diameter reauth-blacklisted-content**" is configured, then reauthorize all the Rating-Groups (RGs) which are blacklisted. CCR-U forced-reauthorization will be triggered all the RGs.
- If this CLI command "**diameter reauth-blacklisted-content content-based-rar**" is configured, then RG which are blacklisted will not be reauthorized. CCR-U forced-reauthorization will be triggered only for active RGs alone.

If Rating-Group information is received in RAR:

Note From StarOS 21.26 and later releases, the term “blacklist” is replaced with “blockedlist” in the help string.

- If either "**diameter reauth-blacklisted-content**" or "**diameter reauth-blacklisted-content content-based-rar**" is configured, then RG gets re-authorized even it is blacklisted. CCR-U forced-reauthorization will be triggered for the received RG.

If this CLI command is not configured, then the default behavior which is not to reauthorize blacklisted RG persists.

Example

In releases prior to StarOS 21.26:

The following command enables reauthorization of blacklisted content on receiving RG specific RAR:

```
diameter reauth-blacklisted-content [ content-based-rar ]
```

From StarOS 21.26 and later releases:

The following command enables reauthorization of blockedisted content on receiving RG specific RAR:

```
diameter reauth-blockedlisted-content [ content-based-rar ]
```

diameter redirect-url-token

This command allows configuring a token to be used for appending original URL to the redirect address.

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

Product GGSN

HA

IPSG

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

diameter redirect-url-token *string*
default diameter redirect-url-token

default

Configures this command with the default setting.

string

The redirect url token name must be an alphanumeric string of size 1 through 63 characters.

Usage Guidelines

The chassis should perform dynamic Advice of Charge (AoC) redirections (URL provided by Online Charging System (OCS)) for a particular Service ID/Rating Group combination without affecting the flows mapped to other Service ID/Rating Group combinations. Redirections can be removed by OCS for a particular MSCC (Service ID/Rating Group combination) using a RAR message containing a specific Service ID/Rating Group combination.

As part of redirection to an AoC or Top-UP server (302 Moved HTTP message) the PCEF should be able to append the original HTTP URL to the redirected session. This way, once the subscriber has successfully been redirected (and potentially topped up their prepaid account) they can be presented with an option to be redirected back to their original URL. The OCS can indicate to the PCEF if the original URL is to be appended to the redirection by specifying a special character to the end of the AoC redirection — for example, a "?" character.

Upon final unit indication a redirect server address will be returned together with the FUI.

On redirection, the redirect URL will be appended with the original URL information using the token name configured with the **diameter redirect-url-token** command so that on completion of AoC, the AoC server may redirect the client back to the original location.

The rules for appending the original URL before redirection are as follows:

1. The "?" character at the end of the AoC page provided by the OCS in the redirect URL will be replaced with the "&" character.
2. A configurable parameter will be appended after the "&" character. The parameter whose name will be defined in a command line in the chassis configuration. The parameter name is case sensitive.
3. An "=" will be appended to the parameter.

4. The subscriber's original URL will be appended to the "=" character.

For example:

When the original URL was http://homepage/

OCS provided URL:

http://test.dev.mms.ag/test/
admin?appName=Return&CODE=UPSELL&OCSCode=FWB&SessionID=4001-dmproxy40-gy2;1302019824;3;1021200;1200-HAOC12959754-UPSELL-N&transID=AOCPurchasepage?

The text in bold in the following sample indicates the current configuration for implementing the dynamic AoC redirection.

http://test.dev.mms.ag/test/
admin?appName=Return&CODE=UPSELL&OCSCode=FWB&SessionID=4001-dmproxy40-gy2;1302019824;3;1021200;1200-HAOC12959754-UPSELL-N&transID=AOCPurchasepage&returnUrl=http%3A%2F%2Fhomepage%2F

Example

The following command configures the redirect-url-token as *returnUrl*:

`diameter redirect-url-token returnUrl`

diameter redirect-validity-timer

This command allows you to control the starting of validity timer for the FUI-redirect scenario.

Product

GGSN

HA

IPSG

PDSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
diameter redirect-validity-timer { immediate | traffic-start }
default diameter redirect-validity-timer
```

default

Configures this command with the default setting. By default, the validity timer is started on receiving the first matching packet.

immediate

This keyword will make the redirect-validity-timer to get started immediately.

traffic-start

This keyword will make the redirect-validity-timer to get started only on receiving matchingtraffic. This is the default configuration.

Usage Guidelines

Use this CLI command to control the starting of validity timer on receipt of CCA in all cases. Based on the configuration value, DCCA decides when to start the redirect-validity-timer. By default, it is started on receiving the first matching packet.

Example

The following command configures the redirect-validity-timer to get started immediately on receiving CCA:

```
diameter redirect-validity-timer immediate
```

diameter result-code

This command enables sending a GTP Create-PDP-Context-Rsp message with cause code based on the DCCA result code.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
diameter result-code { authorization-rejected | credit-limit-reached |
end-user-service-denied | user-unknown } use-gtp-cause-code {
apn-access-denied-no-subscription | authentication-failure |
no-resource-available | system-failure }
default diameter result-code { authorization-rejected |
credit-limit-reached | end-user-service-denied | user-unknown }
use-gtp-cause-code
```

default

Configures this command with the default setting.

In 12.1 and earlier releases: **no-resource-available**

In 12.2 and later releases: **system-failure**

authorization-rejected

Result code received as DIAMETER_AUTHORIZATION_REJECTED(5003).

credit-limit-reached

Result code received as DIAMETER_CREDIT_LIMIT_REACHED(4012).

end-user-service-denied

Result code received as DIAMETER_END_USER_DENIED(4010).

user-unknown

Result code received as DIAMETER_USER_UNKNOWN(5030).

use-gtp-cause-code

Cause code to be sent in GTP response.

apn-access-denied-no-subscription

Sends the GTP cause code GTP_APN_ACCESS_DENIED_NO_SUBSCRIPTION in GTP response.

If this keyword is configured and if the CCR-U is received with auth-rejected(5003) or credit-limit-reached(4012) or user-unknown(5030) or end-user-service-denied(4010), then the GTP result-code is sent as "apn-access-denied-no-subscription".

authentication-failure

Sends the GTP cause code GTP_USER_AUTHENTICATION_FAILED in GTP response.

no-resource-available

Sends the GTP cause code GTP_NO_RESOURCES_AVAILABLE in GTP response.

system-failure

Sends the GTP cause code GTP_SYSTEM_FAILURE in GTP response.

Usage Guidelines

On receiving result-code as AUTHORIZATION-REJECTED, CREDIT_LIMIT_REACHED, END_USER_DENIED or USER_UNKNOWN from DCCA server, based on this CLI configuration, in GTP Create-PDP-Context Response message the cause code can either be sent as GTP_NO_RESOURCE_AVAILABLE or GTP_AUTHENTICATION_FAILED or GTP_SYSTEM_FAILURE or GTP_APN_ACCESS_DENIED_NO_SUBSCRIPTION.

Example

The following command sets the deny cause as user authentication failure when the CCA-Initial has the result code DIAMETER_AUTHORIZATION_REJECTED(5003):

```
diameter result-code authorization-rejected use-gtp-cause-code
authentication-failure
```

diameter send-ccri

This command configures when to send an initial Credit Control Request (CCR-I) for the subscriber session.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
diameter send-ccri { session-start | traffic-start }
default diameter send-ccri
```

default

Configures this command with the default setting.

Default: **session-start**

session-start

Sends CCR-I when the PDP context is being established (on receiving Create-PDP-Context-Request).

traffic-start

Delays sending CCR-I until the first data packet is received from the subscriber.

Important Please note that the CCR-I will be sent only with the default rulebase and not with Rulebase list even if the **rulebase-list** configuration is enabled. When the **rulebase-list** command is used in conjunction with **diameter send-ccri traffic-start** command, the former one's function is invalidated. The rulebase-list is used to allow the OCS to select one of the rulebases from the list configured during the session setup. But in case of **send-ccri traffic-start** the CLI causes the session setup to complete without OCS interaction. For more information on **rulebase-list** command, please see the *ACS Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

Usage Guidelines

Use this command to configure when to send CCR-Initial for the subscriber session.

Example

The following command configures to send CCR-I on traffic detection and not on context creation:

```
diameter send-ccri traffic-start
```

diameter service-context-id

This command configures the value to be sent in the Service-Context-Id AVP, which identifies the context in which DCCA is used.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

diameter service-context-id *service_context_id*
default diameter service-context-id

default

Configures this command with the default setting. Currently, the default value is encoded based on the dictionary wherever applicable; when not applicable, it is not encoded.

service_context_id

Specifies the service context as an alphanumeric string of 1 through 63 characters that can contain punctuation characters.

Usage Guidelines

If Service-Context-Id is applicable and configured using this command, it will be sent in the AVP Service-Context-Id in the Diameter CCR message.

Example

The following command specifies the value *version@customer.com* to be sent in the Service-Context-Id AVP in the Diameter CCR message:

```
diameter service-context-id version@customer.com
```

diameter session failover

This command enables or disables Diameter Credit Control Session Failover. When enabled, the secondary peer is used in the event the main peer is unreachable.

Product

GGSN

HA

IPSG

PDSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

[default | no] diameter session failover

default

Configures this command with the default setting.

Default: Depends on the **failure-handling** configuration

no

If the primary server is not reachable, failover is not triggered and the session is torn down. No failover action is taken.

Usage Guidelines

Use this command to enable/disable Diameter Credit Control Session Failover.

The failure-handling, on page 37 configuration comes into effect only if **diameter session failover** is present in the configuration. The failover can be overridden by the server in the response message, and it takes precedence.

Example

The following command enables Diameter Credit Control Session Failover:

diameter session failover

diameter suppress-avp

This command specifies to suppress the AVPs like the MVNO-subclass-id and MVNO-Reseller-Id AVPs.

Product

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
diameter suppress-avp reseller-id subclass-id
[no | default] diameter suppress-avp reseller-id subclass-id
```

no

Disables AVP suppression. Whenever PCRF sends the MVNO-subclassid and MVNO-Reseller-id AVPs in the Gx interface, the same is sent in the Gy message.

default

Sets the default configuration. AVPs are not suppressed by default. Whenever PCRF sends the MVNO-subclassid and MVNO-Reseller-id AVPs in the Gx interface, the same is sent in the Gy message.

uppress-avp

Suppresses both MVNO-subclassid and MVNO-Reseller-id AVPs.

reseller-id

Supresses the MVNO-Reseller-Id AVP.

subclass-id

Supresses the MVNO-Sub-Class-Id AVP.

Usage Guidelines

Use this command to suppress the AVPs like the MVNO-subclass-id and MVNO-Reseller-Id AVPs.

Example

The following command specifies to request quota on receiving a dynamic rule with Online AVP enabled:

```
diameter suppress-avp reseller-id subclass-id
```

diameter update-dictionary-avps

This command enables dictionary control of the AVPs that need to be added based on the version of the specification with which the Online Charging System (OCS) is compliant. This command is applicable to all products that use the dcca-custom8 dictionary for Gy interface implementation.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
diameter update-dictionary-avps { 3gpp-rel8 | 3gpp-rel9 | 3gpp-rel10 |
3gpp-rel11| 3gpp-rel13 }
[ default | no ] diameter update-dictionary-avps
```

default | no

Configures this command with the default setting.

Default: Compliant with the oldest release (Rel. 7) and send only Rel. 7 AVPs

3gpp-rel8

Select the 3GPP Rel. 8 AVPs for encoding.

3gpp-rel9

Selects the 3GPP Rel. 9 AVPs for encoding.

3gpp-rel10

Select the 3GPP Rel. 10 AVPs for encoding.

3gpp-rel11

Select the 3GPP Rel. 11 AVPs for encoding.

3gpp-rel13

Select the 3GPP Rel. 13 AVPs for encoding.

Usage Guidelines

Important This command is applicable ONLY to the dcca-custom8 dictionary. If, for any dictionary other than dcca-custom8, this command is configured with a value other than the default, configuration errors will be indicated in the output of the **show configuration errors section active-charging** command.

Use this command to encode the AVPs in the dictionary based on the release version of the specification to which the OCS is compliant with.

Example

The following command enables encoding of AVPs in the dictionary based on 3GPP Rel. 9:

```
diameter update-dictionary-avps 3gpp-rel9
```

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.

event-based-session

This command configures the parameters for event-based Gy session.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description **[no] event-based-session trigger type { location-any | mcc | mnc | timezone } +**
default event-based-session trigger type

default

Configures this command with the default setting.

Default: No triggers.

no

Removes the previously configured trigger type.

location-any

Sets the trigger based on change in user location.

mcc

Sets the trigger based on change in Mobile Country Code (MCC) of the serving node (for e.g. SGSN, S-GW).

mnc

Sets the trigger based on change in Mobile Network Code (MNC) of the serving node (for e.g. SGSN, S-GW).

timezone

Sets the trigger based on change in the timezone of UE.

+

Indicates that more than one of the previous keywords can be entered within a single command.

Usage Guidelines Use this command to enable the credit control reauthorization triggers for event-based-session in the credit-control group.

Example

The following command selects a credit control trigger as **mcc**:

```
event-based-session trigger type mcc
```

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.

failure-handling

This command configures Diameter Credit Control Failure Handling (CCFH) behavior in the event of communication failure with the prepaid server or on reception of specific error codes from prepaid server.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
failure-handling { initial-request | terminate-request | update-request
} { continue [ go-offline-after-tx-expiry | retry-after-tx-expiry ] |
retry-and-terminate [ retry-after-tx-expiry ] | terminate }
default failure-handling [ initial-request | terminate-request |
update-request ]
```

default failure-handling [initial-request | terminate-request | update-request]

Configures the default CCFH setting.

initial-request: The default setting is **terminate**.

update-request: The default setting is **retry-and-terminate**.

terminate-request: The default setting is **retry-and-terminate**.

initial-request

Specifies the message type as CCR-Initial.

terminate-request

Specifies the message type as CCR-Terminate.

update-request

Specifies the message type as CCR-Update.

continue

Specifies the CCFH setting as continue. The online session is converted into an offline session. The associated PDP Context is established (new sessions) or not released (ongoing sessions).

retry-and-terminate

Specifies the CCFH setting as retry-and-terminate. The user session will continue for the duration of one retry attempt with the prepaid server. If there is no response from both primary and secondary servers, the session is torn down.

terminate

Specifies the CCFH setting as terminate. All type of sessions (initial or update) are terminated in case of failure.

go-offline-after-tx-expiry

Starts offline charging after Tx expiry.

retry-after-tx-expiry

Retries after Tx expiry. Enables secondary-host, if up, to take over after Tx expiry.

Usage Guidelines

Use this command to select the CCFH behavior. The specified behavior is used for sessions when no behavior is specified by the prepaid server. By default, the CCFH is taken care at response-timeout except for terminate setting.

If the Credit-Control-Failure-Handling AVP is received from the server, the received setting will be applied to all the message types.

The following table indicates the CCFH behavior for the combination of different CCFH settings, and the corresponding CLI commands.

CCFH Setting	CLI Command	Behavior at Tx	Behavior at RT	Secondary is Up	Secondary is Down
Initial-request Message Type					
Continue	**initial-request continue**	N/A	Continue	Secondary takes over after RT	Offline after another RT. No more quota requests are performed for any rating group within the session after DCCA failure (even if connectivity to DCCA is restored)
	initial-request continue go-offline-after-tx-expiry	Offline	N/A	Offline at Tx	Offline at Tx
	initial-request continue retry-after-tx-expiry	Continue	N/A	Secondary takes over after Tx	Offline after another Tx
Retry-and-terminate	**initial-request retry-and-terminate**	N/A	Retry	Secondary takes over after RT	Terminate after another RT
	initial-request retry-and-terminate retry-after-tx-expiry	Retry	N/A	Secondary takes over after Tx	Terminate after another Tx
Terminate	**initial-request terminate**	Terminate	N/A	Terminate after Tx	Terminate after Tx
Update-request Message Type					
Continue	**update-request continue**	N/A	Continue	Secondary takes over after RT	Offline after another RT
	update-request continue go-offline-after-tx-expiry	Offline	N/A	Offline at Tx	Offline at Tx
	update-request continue retry-after-tx-expiry	Continue	N/A	Secondary takes over after Tx	Offline after another Tx
Retry-and-terminate	**update-request retry-and-terminate**	N/A	Retry	Secondary takes over after RT	Sends CCR-T after another RT
	update-request retry-and-terminate retry-after-tx-expiry	Retry	N/A	Secondary takes over after Tx	Sends CCR-T after another Tx

CCFH Setting	CLI Command	Behavior at Tx	Behavior at RT	Secondary is Up	Secondary is Down
Terminate	**update-request terminate**	Terminate	N/A	Sends CCR-T after Tx	Sends CCR-T after Tx
Terminate-request Message Type					
Continue	**terminate-request continue**	N/A	Retry	CCR-T is sent to secondary after RT	Terminate after another RT
	terminate-request continue go-offline-after-tx-expiry	Retry	N/A	CCR-T is sent to secondary after Tx	Terminate after another Tx
	terminate-request continue retry-after-tx-expiry	Retry	N/A	CCR-T is sent to secondary after Tx	Terminate after another Tx
Retry-and-terminate	**terminate-request retry-and-terminate**	N/A	Retry	CCR-T is sent to secondary after RT	Terminate after another RT
	terminate-request retry-and-terminate retry-after-tx-expiry	Retry	N/A	CCR-T is sent to secondary after Tx	Terminate after another Tx
Terminate	**terminate-request terminate**	Terminate	N/A	Terminate after Tx	Terminate after Tx

Example

The following command sets the Credit Control Failure Handling behavior for initial request message type to **retry-and-terminate**:

```
failure-handling initial-request retry-and-terminate
```

gy-rf-trigger-type

This command enables the Gy event triggers for configuration of matching Rf ACR containers.

Product

GGSN

HA

IPSG

PDSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

gy-rf-trigger-type { final | forced-reauthorization | holding-time | quota-exhausted | rating-condition-change | threshold | validity-time } { default | no } gy-rf-trigger-type

default | no

The "default/no" variant of this command will not enable any of the Gy event-triggers which means the containers would not be closed for any of the event-triggers.

final

Enables Gy trigger "final" for Rf

forced-reauthorization

Enables Gy trigger "forced-reauthorization" for Rf.

holding-time

Enables Gy trigger "qht" for Rf. The trigger "qht" indicates Quota Holding Time.

quota-exhausted

Enables Gy trigger "quota-exhausted" for Rf.

rating-condition-change

Enables Gy trigger "rating-condition-change" for Rf.

threshold

Enables Gy trigger "threshold" for Rf.

validity-time

Enables Gy trigger "validity-time" for Rf.

Usage Guidelines

Use this command to enable the Gy reporting reasons/event triggers.

For all the Gy event triggers a container will be cached at Rf and will be sent based on other events at Rf (for example, max-charging-change-condition, RAT-Change, etc).

Important The CLI command "gy-rf-trigger-type" is currently applicable only for CCR-U and not CCR-T.

For example, when the CLI for QUOTA_EXHAUSTED event trigger is configured under credit-control group configuration, if there is quota_exhausted event then the container should be cached with appropriate

change-condition value and ACR-I would be sent out based on other Rf event triggers. Similar behavior is applicable to other event triggers when configured.

Example

The following command specifies the validity-time event trigger to be enabled.

gy-rf-trigger-type validity-time

imsi-imeisv-encode-format

This command configures the encoding format of IMSI/IMEISV in the User-Equipment-Info, 3GPP-IMSI and 3GPP-IMEISV AVPs.

Product

GGSN

HA

IPSG

PDSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

[default | no] imsi-imeisv-encode-format { ascii | tbcd }

ascii

Sends IMSI/IMEISV as an octet string in ASCII encoded format. By default, the IMSI/IMEISV will be encoded in ASCII format.

tbcd

Sends IMSI/IMEISV as an octet string in Telephony Binary Coded Decimal (TBCD) format, i.e. the nibbles in an octet are inter-changed.

Usage Guidelines

Use this command to configure the encoding format of IMSI/IMEISV in User-Equipment-Info, 3GPP-IMSI and 3GPP-IMEISV AVPs.

Example

The following command specifies the encoding format of IMSI/IMEISV as ASCII:

imsi-imeisv-encode-format ascii

mode

This command configures the Prepaid Credit Control mode to RADIUS or Diameter.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
mode { diameter | radius }
default mode
```

default

Configures the default prepaid credit control mode.

Default: **diameter**

diameter

Enables Diameter Credit Control Application (DCCA) for prepaid charging.

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

radius

Enables RADIUS Credit Control for prepaid charging.

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

Usage Guidelines

Use this command to configure the prepaid charging application mode to Diameter or RADIUS credit control.

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

Example

The following command specifies to use RADIUS prepaid credit control application:

mode radius

offline-session re-enable

This command is configured to re-enable the offline Gy session after failure.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] offline-session re-enable

no

Disables the feature. This is the default behavior.

The default configuration is **no offline-session re-enable**.

Usage Guidelines

Use this command to re-enable the Offline Gy session back to Online charging, based on indication from PCRF. When **offline-session re-enable** is configured and the PCRF installs/modifies a rule with "Online" AVP value set to 1, then the Offline DCCA will be marked Online.

pending-traffic-treatment

This command controls the pass/drop treatment of traffic while waiting for definitive credit information from the server.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
pending-traffic-treatment { { { forced-reauth | trigger | validity-expired
 } drop | pass } | { noquota { buffer | drop | limited-pass volume | pass
 } } | { quota-exhausted { buffer | drop | pass } } }
default pending-traffic-treatment { forced-reauth | noquota |
quota-exhausted | trigger | validity-expired }
```

default

Configures this command with the default setting.

Default: **drop**

forced-reauth

Sets the Diameter credit control pending traffic treatment to forced reauthorization.

trigger

Sets the Diameter credit control pending traffic treatment to trigger.

validity-expired

Sets the Diameter credit control pending traffic treatment to validity expired.

noquota

Sets the Diameter credit control pending traffic treatment to no quota.

quota-exhausted

Sets the Diameter credit control pending traffic treatment to quota exhausted.

buffer

Specifies to tentatively count/time traffic, and then buffer traffic pending arrival of quota. Buffered traffic will be forwarded and fully charged against the quota when the quota is eventually obtained and the traffic is passed.

drop

Drops any traffic when there is no quota present.

limited-pass *volume*

Enables limited access for subscribers when the OCS is unreachable.

volume specifies the Default Quota size (in bytes) and must be an integer from 1 through 4294967295.

This feature allows the subscriber to use the network when the OCS response is slow. This configuration enables to set a Default Quota size from which the subscriber can consume quota until response from the OCS arrives. The traffic consumed by the subscriber from the Default Quota at the beginning of the session is reported and counted against the quota assigned from the OCS.

Important Default Quota is used only for **noquota** case (Rating Group (RG) seeking quota for the first time) and not for **quota-exhauste**d. Default Quota is not used for subsequent credit requests.

If the Default Quota is NOT exhausted before the OCS responds with quota, traffic is allowed to pass. Initial Default Quota usage is counted against initial quota allocated. If quota allocated is less than the actual usage, the actual usage and request additional quota are reported. If no additional quota is available, the traffic is denied.

If the Default Quota is NOT exhausted before the OCS responds with denial of quota, traffic is blocked after the OCS response. The gateway will report usage on Default Quota even in for CCR-U (FINAL) or CCR-T until the OCS responds.

If the Default Quota is exhausted before the OCS responds, the session is dropped.

The default pending-traffic-treatment for **noquota** is drop. The **default pending-traffic-treatment noquota** command removes any Default Quota limit configured.

pass

Passes all traffic more or less regardless of quota state.

Usage Guidelines

Use this command to set the Diameter credit control pending traffic treatment while waiting for definitive credit information from the server.

This CLI command is different than the **failure-handling** command, which specifies behavior in the case of an actual timeout or error, as opposed to the behavior while waiting. See also the **buffering-limit** command in the Active Charging Service Configuration Mode.

Example

The following command sets the Diameter credit control pending traffic treatment to drop any traffic when there is no quota present:

```
pending-traffic-treatment noquota drop
```

quota

This command sets various time-based quotas in the prepaid credit control service.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

quota *holding_time* **| validity-time** *validity_time* **}**
{ default | no } quota { holding-time | validity-time }

holding-time *holding_time*

Specifies the Quota Holding Time (QHT) in seconds. The value must be an integer from 1 through 4000000000.

validity-time *validity_time*

Specifies the validity lifetime of the quota, in seconds. The value must be an integer from 1 through 4000000.

Usage Guidelines

Use this command to set the prepaid credit control quotas.

Example

The following command sets the prepaid credit control request holding time to *30000* seconds:

quota holding-time 30000

quota request-trigger

This command configures the action on the packet that triggers the credit control application to request quota.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

quota request-trigger { exclude-packet-causing-trigger |
include-packet-causing-trigger }
{ default | no } quota request-trigger
default quota request-trigger

default

Configures this command with the default setting. Default: **include-packet-causing-trigger**

no

Same as the **default quota request-trigger** command.

Important In 10.0 and later releases, this keyword is deprecated.

exclude-packet-causing-trigger

Excludes the packet causing threshold limit violation trigger.

include-packet-causing-trigger

Includes the packet causing the threshold limit violation trigger.

Usage Guidelines

Use this command to configure action on the packet that triggers the credit control application to request quota, whether the packet should be excluded/included in the utilization information within the quota request.

Example

The following command sets the system to exclude the packets causing threshold limit triggers from accounting of prepaid credit of a subscriber:

```
quota request-trigger exclude-packet-causing-trigger
```

quota time-threshold

This command configures the time threshold limit for subscriber quota in the prepaid credit control service.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

quota time-threshold { *abs_time_value* **| percent** *percent_value* **}**
{ default | no } quota time-threshold

default

Configures this command with the default setting.

Default: Disabled

no

Disables time threshold for prepaid credit control quota.

abs_time_value

Specifies the absolute threshold time (in seconds) for configured time quota in prepaid credit control charging. *abs_time_value* must be an integer from 1 through 86400. To disable this assign 0. Default: 0 (Disabled)

percent_value

Specifies the time threshold value as a percentage of the configured time quota in DCCA. *percent_value* must be an integer from 1 through 100.

Usage Guidelines

Use this command to set the time threshold for prepaid credit control quotas.

Example

The following command sets the prepaid credit control time threshold to *400* seconds:

```
quota time-threshold 400
```

quota units-threshold

This command sets the unit threshold limit for subscriber quota in the prepaid credit control service.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

quota unit-threshold { *abs_unit_value* **| percent** *percent_value* **}**
{ default | no } quota units-threshold

default

Configures this command with the default setting.

Default: Disabled

no

Disables unit threshold for DCCA quota.

abs_unit_value

Specifies the absolute threshold value (in units) for the configured units quota in prepaid credit control application. *abs_unit_value* must be an integer from 1 through 4000000000. To disable this assign 0. Default: 0 (Disabled)

percent_value

Specifies the time threshold value as a percentage of the configured units quota in DCCA. *percent_value* must be an integer from 1 through 100.

Usage Guidelines Use this command to set the units threshold for prepaid credit control quotas.

Example

The following command sets the prepaid credit control time threshold to *160400* units:

```
quota units-threshold 160400
```

quota volume-threshold

This command sets the volume threshold limit for subscriber quota in the prepaid credit control service.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
quota volume-threshold { abs_vol_value | percent percent_value }
{ default | no } quota volume-threshold
```

default

Configures this command with the default setting.

Default: Disabled

no

Disables volume threshold for prepaid credit control quota.

abs_vol_value

Specifies the absolute threshold volume (in bytes) to the configured volume quota in prepaid credit control. *abs_vol_value* must be an integer from 1 through 4000000000. To disable this assign 0. Default: 0 (Disabled)

If configured, the Credit Control client will seek re-authorization from the server for the quota when the quota contents fall below the specified threshold.

percent *percent_value*

Specifies the volume threshold value as a percentage of the configured volume quota in prepaid credit control. *percent_value* must be an integer from 1 through 100.

Usage Guidelines Use this command to set the volume threshold for prepaid credit control quotas.

Example

The following command sets the prepaid credit control volume threshold to *160400* bytes:

```
quota volume-threshold 160400
```

radius usage-reporting-algorithm

This command configures the usage reporting algorithm for RADIUS prepaid using the Diameter Credit-Control Application (DCCA).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
radius usage-reporting-algorithm { cumulative | relative }
default radius usage-reporting-algorithm
```

default

Configures this command with the default setting.

Default: **cumulative**

cumulative

Reports the total accumulated usage of quota in every accounting interim.

relative

Reports the quota usage per accounting interim (since the previous usage report).

Usage Guidelines

Use this command to configure the usage reporting algorithm for RADIUS prepaid using DCCA.

Example

The following command configures the usage reporting algorithm for RADIUS prepaid using DCCA to *relative*:

```
radius usage-reporting-algorithm relative
```

redirect-indicator-received

This command configures the action on buffered packets when a redirect-indicator is received from the RADIUS server.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

redirect-indicator-received { discard-buffered-packet | reprocess-buffered-packet }
{ default | no } redirect-indicator-received

default

Configures this command with the default setting. Default: **discard-buffered-packet**

no

Disables the redirect-indicator-received configuration.

discard-buffered-packet

Discards the buffered packet.

reprocess-buffered-packet

Redirects the buffered packet on receiving a redirect-indicator from the RADIUS server.

Usage Guidelines

Use this command to configure the action taken on buffered packet when redirect-indicator is received.

Diameter can return a redirect URL but not a redirect indicator, however RADIUS can return a redirect indicator. In this situation, any subsequent subscriber traffic would match ruledefs configured with cca redirect-indicator, and charging actions that have flow action redirect-url should be configured. However, some handsets do not retransmit, so there will be no subsequent packets. On configuring reprocess-buffered-packet, the ruledefs are reexamined to find a new charging action, which may have flow action redirect-url configured.

Example

The following command configures the action taken on buffered packet when redirect-indicator is received to reprocess-buffered-packet:

redirect-indicator-received reprocess-buffered-packet

redirect-require-user-agent

This command conditionally verifies the presence of user-agents in the HTTP header, based on which HTTP URL redirection will be applied.

Product

GGSN

HA

IPSG

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] redirect-require-user-agent

no

Disables the "user-agent" check in the HTTP header.

Usage Guidelines

Use this command to conditionally verify the presence of configured user-agents in the HTTP header. The user agent is configured using the **redirect user-agent** command in the ACS Configuration Mode. The user agent could be, for example, Mozilla, Opera, Google Chrome, etc.

The default configuration is to enable the "user-agent" check, and compare it with the configured list of supported user-agents. The packet will be redirected only when the user-agent is matched with one of the configured user-agents.

If **no redirect-require-user-agent** is configured, the user-agent check is disabled. The packets will be redirected even if it does not contain a "user-agent" information in the HTTP header.

servers-unreachable

This command configures whether to continue or terminate calls when Diameter server or the OCS becomes unreachable.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

In 12.1 and earlier releases:

```
servers-unreachable { initial-request { continue | terminate [
after-timer-expiry timeout_period ] } | update-request { continue | terminate
 [ after-quota-expiry | after-timer-expiry timeout_period ] } }
no servers-unreachable { initial-request | update-request }
```

In 12.2 and later releases:

```
servers-unreachable { behavior-triggers { initial-request | update-request
 } result-code { any-error | result-code [ to end-result-code ] } |
transport-failure [ response-timeout | tx-expiry ] | initial-request {
continue [ { [ after-interim-time timeout_period ] [ after-interim-volume
quota_value ] } server-retries retry_count ] | terminate [ { [
after-interim-time timeout_period ] [ after-interim-volume quota_value ] }
server-retries retry_count | after-timer-expiry timeout_period ] } |
update-request { continue [ { [ after-interim-time timeout_period ] [
after-interim-volume quota_value ] } server-retries retry_count ] | terminate
 [ { [ after-interim-time timeout_period ] [ after-interim-volume quota_value
 ] } server-retries retry_count ] | after-quota-expiry | after-timer-expiry
 timeout_period ] } }
no servers-unreachable { initial-request | update-request }
default servers-unreachable behavior-triggers { initial-request |
update-request }
```

no

Deletes the current servers-unreachable configuration.

In 15.0 and later releases, to remove the error result code configuration, the **no** command syntax is **no servers-unreachable behavior-triggers { initial-request | update-request } result-code { any-error |** *result-code* **[to** *end-result-code* **] }**.

behavior-triggers { initial-request | update-request } { result-code { any-error | *result-code* [to *end-result-code*] } | transport-failure [response-timeout | tx-expiry] }

This keyword is used to determine when to apply server-unreachable action. This supports three configurable options to apply server-unreachable action either at transport failure, Tx expiry or at response timeout. Out of these three options, the transport failure is the default option.

- **initial-request**: Specifies the behavior when Diameter server(s)/OCS become unreachable during initial session establishment.
- **update-request**: Specifies the behavior when Diameter server(s)/OCS become unreachable during mid-session.
- **result-code { any-error |** *result-code* **[to** *end-result-code* **] }**: Specifies to configure any Diameter error result code or a range of result codes to trigger entering server unreachable mode.

result-code must be an integer ranging from 3000 to 5999.

- **transport-failure [response-timeout | tx-expiry]**: This keyword specifies to trigger the behavior either at transport failure or response timeout OR at Transport failure or Tx expiry.

initial-request { continue | terminate [after-timer-expiry *timeout_period*] }

Important This section applies only to 12.1 and earlier releases.

Specifies behavior when Diameter server(s)/OCS become unreachable during initial session establishment.

- **continue**: Specifies to continue call if Diameter server(s) becomes unreachable.
- **terminate**: Specifies to terminate call if Diameter server(s) becomes unreachable.

  after-timer-expiry *timeout_period*: On detecting transport failure, this keyword variable specifies the time limit for which the subscriber session will remain in offline state before the call is terminated.

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

initial-request { continue [{ [after-interim-time *timeout_period*] [after-interim-volume *quota_value*] } server-retries *retry_count*] | terminate [{ [after-interim-time *timeout_period*] [after-interim-volume *quota_value*] } server-retries *retry_count*] | after-timer-expiry *timeout_period* }

Important This section applies only to 12.2 and later releases.

Specifies behavior when Diameter server(s)/OCS become unreachable during initial session establishment.

- **continue**: Specifies to continue call if Diameter server(s) becomes unreachable.
- **terminate**: Specifies to terminate call if Diameter server(s) becomes unreachable.
  - **after-interim-time** *timeout_period*: Specifies to continue or terminate call after the interim timeout period expires.

    timeout_period specifies the timeout period, in seconds, and must be an integer from 1 through 4294967295.
  - **after-interim-volume** *quota_value*: Specifies to continue or terminate call on exhaustion of the assigned quota.

    quota_value specifies the volume-based quota value, in bytes, and must be an integer from 1 through 4294967295.

    The **after-interim-volume** and **after-interim-time** can be configured in one of the following ways:
    - **after-interim-volume** *quota_value* **server-retries** *retry_count*
    - **after-interim-time** *timeout_period* **server-retries** *retry_count*
    - **after-interim-volume** *quota_value* **after-interim-time** *timeout_period* **server-retries** *retry_count*

- **after-timer-expiry** *timeout_period*: On detecting transport failure, this keyword variable specifies the time limit for which the subscriber session will remain in offline state before the call is terminated.

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

- **server-retries** *retry_count*: Specifies the number of retries that should happen to OCS before allowing the session to terminate/offline.

  retry_count specifies the retries to OCS, and must be an integer from 0 through 65535. If the value 0 is defined for this keyword, the retry to OCS will not happen instead the configured action will be immediately applied.

update-request { continue | terminate [after-quota-expiry | after-timer-expiry *timeout_period*] }

Important This section applies only to 12.1 and earlier releases.

Specifies behavior when Diameter server(s)/OCS become unreachable during mid session.

- **continue**: Specifies to continue call if Diameter server(s) becomes unreachable.
- **terminate**: Specifies to terminate call if Diameter server(s) becomes unreachable.
  - **after-quota-expiry**: Specifies to terminate call on exhaustion of all available quota.
  - **after-timer-expiry** *timeout_period*: On detecting transport failure, this keyword variable specifies the time limit for which the subscriber session will remain in offline state before the call is terminated.

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

update-request { continue [{ [after-interim-time *timeout_period*] [after-interim-volume *quota_value*] } server-retries *retry_count*] | terminate [{ [after-interim-time *timeout_period*] [after-interim-volume *quota_value*] } server-retries *retry_count*] | after-quota-expiry | after-timer-expiry *timeout_period*] }

Important This section applies only to 12.2 and later releases.

Specifies behavior when Diameter server(s)/OCS become unreachable during mid session.

- **continue**: Specifies to continue call if Diameter server(s) becomes unreachable.
- **terminate**: Specifies to terminate call if Diameter server(s) becomes unreachable.
  - **after-interim-time** *timeout_period*: Specifies to continue or terminate call after the interim timeout period expires.

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

  - **after-interim-volume** *quota_value*: Specifies to continue or terminate call on exhaustion of the assigned quota.

quota_value specifies the volume-based quota value, in bytes, and must be an integer from 1 through 4294967295.

The **after-interim-volume** and **after-interim-time** can be configured in one of the following ways:

- **after-interim-volume** *quota_value* **server-retries** *retry_count*
- **after-interim-time** *timeout_period* **server-retries** *retry_count*
- **after-interim-volume** *quota_value* **after-interim-time** *timeout_period* **server-retries** *retry_count*

- **after-quota-expiry**: Specifies to terminate call on exhaustion of all available quota.
- **after-timer-expiry** *timeout_period*: On detecting transport failure, this keyword variable specifies the time limit for which the subscriber session will remain in offline state before the call is terminated.

  timeout_period specifies the timeout period, in seconds, and must be an integer from 1 through 4294967295.
- **server-retries** *retry_count*: Specifies the number of retries that should happen to OCS before allowing the session to terminate/offline.

  retry_count specifies the retries to OCS, and must be an integer from 0 through 65535. If the value 0 is defined for this keyword, the retry to OCS will not happen instead the configured action will be immediately applied.

Usage Guidelines

Use this command to configure whether to continue/terminate calls when Diameter server(s)/OCS are unreachable. This command can be used to verify the functionality of the configurable action if the OCS becomes unreachable.

In 12.1 and earlier releases, the OCS is considered down/unreachable when all transport/TCP connections are down for that OCS.

In 12.2 and later releases, the OCS is declared unreachable when all transport connections are down OR message timeouts happen (for example, a Tx expiry or response timeout, for all available OCS servers) owing to slow response from the OCS (may be due to network congestion or other network related issues).

The following set of actions are performed if the servers become unreachable:

- During initial session establishment:
  - Block traffic: Terminate the session.
  - Continue call: Continue by making the session offline.
  - Pass traffic until timer expiration post which terminates the call: Session would be offline while the timer is running.
  - Pass traffic until interim time expiration post which continues or terminates the call.
  - Pass traffic until interim volume expiration post which continues or terminates the call.
- During mid session:
  - Block traffic: Terminate the session.
  - Continue call: Continue by making the session offline.

- Run out of session quota post which terminates the call.
- Pass traffic until timer expiration post which terminates the call: Session would be offline while the timer is running.
- Pass traffic until interim time expiration post which continues or terminates the call.
- Pass traffic until interim volume expiration post which continues or terminates the call.

This command works on the same lines as the **failure-handling** command, which is very generic for each of the xxx-requests.

The **servers-unreachable** CLI command is specifically for TCP connection error. In the event of TCP connection failure, the **failure-handling** and/or **servers-unreachable** commands can be used. This way, the operator has the flexibility to configure CCFH independent of OCS-unreachable feature, that is having two different failure handlings for same request types.

Important Please note that the flexibility to configure CCFH independent of OCS-unreachable feature is applicable only to 12.1 and earlier releases. In 12.2 and later releases, if configured, the **servers-unreachable** takes precedence over the **failure-handling** command.

This command can also be used to control the triggering of behavior based on transport failure, response message timeouts or Tx expiry when OCS becomes unreachable. The OCS could be unreachable due to no TCP connection and the message timeout could be due to network congestion or any other network related issues.

The following are the possible and permissible configurations with respect to behavior triggering:

- **servers-unreachable behavior-triggers { initial-request | update-request } transport-failure**
- **servers-unreachable behavior-triggers { initial-request | update-request } transport-failure response-timeout**
- **servers-unreachable behavior-triggers { initial-request | update-request } transport-failure tx-expiry**

Of these configurations, the first one is considered to be the default configuration and it will take care of backward compatibility with 12.0 implementation.

If the server returns the CC-Failure-Handling AVP, it would apply for transport-failure/response-timeout/tx-expiry when the CLI command **servers-unreachable** is not configured. If the **servers-unreachable** is configured for a set of behavior-triggers, then servers-unreachable configuration will be applied for them. For those behavior-triggers for which servers-unreachable is not configured, the CC-Failure-Handling value provided by the server will be applied.

By default, Result-Code such as 3002 (Unable-To-Deliver), 3004 (Too-Busy) and 3005 (Loop-Detected) falls under delivery failure category and will be treated similar to response-timeout configuration.

Example

The following command configures the duration of *1111* seconds, for the subscriber session to be in offline state, after which the initial request calls will be terminated.

```
servers-unreachable initial-request terminate after-timer-expiry 1111
```

subscription-id service-type

This command enables required Subscription-Ids for various service types.

Product

GGSN

HA

IPSG

PDSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

subscription-id service-type { closedrp | ggsn | ha | ipsg | l2tplns | mipv6ha | pdsn | pgw } { e164 | imsi | nai }
[no] subscription-id service-type { closedrp | ggsn | ha | ipsg | l2tplns | mipv6ha | pdsn | pgw }

default

Configures the default timestamp-rounding setting.

Default: **floor**

closedrp | ggsn | ha | ipsg | l2tplns | mipv6ha | pdsn | pgw { e164 | imsi | nai }

Includes the Subscription-Id for the chosen service type. For example, if ipsg is configured as the keyword option, then the subscription-id is included for the IPSG service.

The following subscription-Id types are available:

- e164 - Include E164 information in the Subscription-Id AVP
- imsi - Include IMSI information in the Subscription-Id AVP
- nai - Include NAI information in the Subscription-Id AVP

Usage Guidelines

Currently, Subscription-Id AVP is encoded in the Gy CCRs based on dictionary and service-type checks. With the new CLI command, customers will have the provision of enabling required Subscription-Id types for various services.

Each service can have a maximum of three Subscription-Id types (e164, imsi & nai) that can be configured through this CLI command. The DCCA specific changes are made in such a way that, if the CLI command is configured for any particular service, then the CLI takes precedence. Else, it falls back to default (hard-coded) values configured for that service.

The advantage of this CLI command is that any further dictionary additions in DCCA can be minimized.

Important The CLI configured for any of the service will contain the most recent Subscription-Id-types configured for that service (i.e. overrides the previous values).

For an instance, if a customer wants IMSI value to be encoded in Gy CCRs (along with E164) for MIPv6HA service, then this CLI command **subscription-id service-type mipv6ha e164 imsi** should be configured in the Credit Control Configuration mode.

If only imsi is configured through the CLI, then Gy CCRs will only have imsi value.

Example

The following command configures imsi type for ggsn service:

```
subscription-id service-type ggsn imsi
```

timestamp-rounding

This command configures how to convert exact time into the units that are used in quotas.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
timestamp-rounding { ceiling | floor | roundoff }
default timestamp-rounding
```

default

Configures the default timestamp-rounding setting.

Default: **floor**

timestamp-rounding ceiling

Round off to the smallest integer greater than the fraction.

If the fractional part of the seconds is greater than 0, add 1 to the number of seconds and discard the fraction.

timestamp-rounding floor

Discard the fractional part of the second.

timestamp-rounding roundoff

Set the fractional part of the seconds to the nearest integer value. If the fractional value is greater than or equal to 0.5, add 1 to the number of seconds and discard the fractional part of second.

Usage Guidelines

Use this command to configure how to convert exact time into the units that are used in quotas for CCA charging.

The specified rounding will be performed before system attempts any calculation. For example using round-off, if the start time is 1.4, and the end time is 1.6, then the calculated duration will be 1 (i.e., 2 – 1 = 1).

Example

The following command sets the CCA timestamp to nearest integer value second (for example, 34:12.23 to 34:12.00):

```
timestamp-rounding roundoff
```

trigger type

This command enables/disables triggering a credit reauthorization when the named values in the subscriber session changes.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ] trigger type { cellid | lac | mcc | mnc | qos | rat | serving-node
 | sgsn | timezone } +
default trigger type
```

default

Configures this command with the default setting.

Default: No triggers.

no

Removes the previously configured trigger type.

cellid

Sets the trigger based on change in cell identity or Service Area Code (SAC).

lac

Sets the trigger based on change in Location Area Code.

mcc

Sets the trigger based on change in Mobile Country Code (MCC).

mnc

Sets the trigger based on change in Mobile Network Code (MNC).

qos

Sets the trigger based on change in the Quality of Service (QoS).

rat

Sets the trigger based on change in the Radio Access Technology (RAT).

serving-node

Sets the trigger based on change in serving node. The serving node change causes the credit control client to ask for a re-authorization of the associated quota.

Typically used as an extension to sgsn trigger in P-GW (SAEGW), however, may also be used alone.

sgsn

Sets the trigger based on change in the IP address of SGSN.

timezone

Sets the trigger based on change in the timezone of UE.

+

Indicates that more than one of the previous keywords can be entered within a single command.

Usage Guidelines

Use this command to set the credit control reauthorization trigger.

Example

The following command selects a credit control trigger as **lac**:

```
trigger type lac
```

usage-reporting

This command configures the ACS Credit Control usage reporting type.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
usage-reporting quotas-to-report based-on-grant {
report-only-granted-volume }
default usage-reporting quotas-to-report
```

default

Configures this command with the default setting.

Default: Disabled

usage-reporting quotas-to-report based-on-grant

Configures reporting usage only for granted quota.

Note When Gy server is unavailable, no grant (quota) is received. In this case, P-GW sends both CC-OCTET and CC-TIME AVPs in the usage report.

report-only-granted-volume

Suppresses the input and output octets. If the Granted-Service-Unit (GSU) AVP comes with CC-Total-Octets, then the device will send total, input and output octets in Used-Service-Unit (USU) AVP. If it comes with Total-Octets, the device will send only Total-Octets in USU.

Usage Guidelines

Use this command to configure reporting usage only for granted quota. On issuing this command, the Used-Service-Unit AVP will report quotas based on grant i.e, only the quotas present in the Granted-Service-Unit AVP.

With this command only the units for which the quota was granted by the DCCA server will be reported irrespective of the reporting reason.

Example

The following command configures to report usage based only on granted quota:

```
usage-reporting quotas-to-report based-on-grant
```