

Policy Control Configuration Mode Commands

Policy Control Configuration mode is used to configure the Diameter dictionary, origin host, host table entry and host selection algorithm for IMS Authorization service.

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands chapter.

- apn-name-to-be-included, on page 2
- arp-priority-level, on page 3
- associate, on page 4
- cc-profile, on page 6
- custom-reauth-trigger, on page 7
- diameter 3gpp-r9-flow-direction, on page 9
- diameter clear-session, on page 10
- diameter dictionary, on page 11
- diameter encode-event-avps, on page 13
- diameter encode-supported-features, on page 14
- diameter host-select reselect, on page 22
- diameter host-select row-precedence, on page 23
- diameter host-select table, on page 26
- diameter host-select-template, on page 28
- diameter map, on page 29

- diameter origin endpoint, on page 31
- diameter request-timeout, on page 31
- diameter session-prioritization, on page 32
- diameter sgsn-change-reporting, on page 34
- diameter update-dictionary-avps, on page 35
- encode-cc-in-r8-gx-dict, on page 38
- endpoint-peer-select, on page 39
- event-report-indication, on page 40
- event-update, on page 41
- failure-handling, on page 43
- li-secret, on page 47
- max-outstanding-ccr-u, on page 47
- subscription-id service-type, on page 48

apn-name-to-be-included

This command configures the APN name to be included in CCR Gx messages.

Product

GGSN

IPSG

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > **context** *context_name* > **ims-auth-service** *service_name* > **policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

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

gn | virtual

Specifies which APN name must be sent in the Gx messages.

gn: Specifies to send the real APN name.

virtual: Specifies to send the virtual APN name if present, else to send the real APN name.

default

Applies the default setting for this command.

Default: **gn**

Usage Guidelines

This feature is developed to implement a single global APN for the Enterprise services with the ability to have separate virtual APNs per single Enterprise, group of Enterprises sharing the same service group or per department.

To implement this feature, a configurable option is introduced per interface Rf, Gx, Gy and per APN. That is, a service specific CLI "**apn-name-to-be-included**" is configured for interfaces Rf, Gx, Gy separately. It can take values 'gn' or 'virtual'. Based on the value configured for this command, the Called-Station-Id AVP is populated.

This command is used to configure the APN name to be included in the CCR Gx messages to the PCRF — the real APN name or the virtual APN name.

The name of the virtual APN and the IP pool are signaled during the UE attach to the Enterprise PDN from the 3GPP AAA server over S6b interface with a new vendor-specific AVP "Virtual-APN-Name". The RADIUS Start, Gy CCR to OFCS and Rf ACR to OCS messages contain the Virtual APN name instead of the Enterprise APN.

This feature provides customers the desired granularity per enterprise and per department. This also allows bundling of number of small enterprises under the umbrella of single APN and logically separating them by virtual APN.

Example

The following command configures sending the real APN name in Gx messages:

```
apn-name-to-be-included gn
```

arp-priority-level

This command enables mapping of the ARP priority-level value received from PCRF to inter-user-priority value and be sent in A11 session update.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
arp-priority-level map-to inter-user-priority
{ default | no } arp-priority-level map-to
```

default

Configures the default setting for this command.

Default: arp-priority-level to inter-user-priority mapping not applicable

no

Disables arp-priority-level to inter-user-priority mapping.

Usage Guidelines



Important This command is for a customer-specific implementation to support IP-CAN policy control via Gx interface in PDSN, wherein the PCRF informs the subscriber's subscription level (such as gold, silver, bronze) to PDSN/PCEF via Priority-Level AVP, then PDSN maps the subscriber's subscription level to inter-user-priority and transmits it to PCF via A11 session update message. For more information on the use of this command contact your Cisco account representative.

associate

This command associates/disassociates a failure handling templateor a local policy template with the IMS authorization service.

Product

GGSN

HA

HSGW

IPSG

PDSN

P-GW

SAEGW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > **context** *context_name* > **ims-auth-service** *service_name* > **policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

associate { **failure-handling-template** *template_name* **| local-policy-service** *service_name* **[dual-mode] }**
no associate { **failure-handling-template | local-policy-service }**

no

Disassociates a failure handling templateor local policy template with the IMS authorization service.

failure-handling-template *template_name*

Associates a previously created failure handling template with the IMS authorization 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.

local-policy-service *service_name* [dual-mode]

Associates a previously created local policy service with the IMS authorization service. *service_name* specifies the name for a pre-configured local policy service. *service_name* must be an alphanumeric string of 1 through 63 characters.

dual-mode: This keyword enables both PCRF and local-policy to work together. When this CLI command is enabled, for a few set of events, PCRF will be contacted and for a few local-policy will be contacted.

This keyword is configured to provide load balancing support for PCRF, and failure-handling support when PCRF is down or any failure is detected.

By default, the **dual-mode** keyword will not enabled and only on PCRF failure the local-policy will be contacted.

For more information on local policy service configuration, refer to the **local-policy-service** command in the *Global Configuration Mode Commands* chapter.

Usage Guidelines

Use this command to associate a configured failure handling template or local policy service with the IMS authorization 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, refer to the *Failure Handling Template Configuration Mode Commands* chapter.



Important Only one failure handling template can be associated with the IMS authorization 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 effect.

To support fallback to local policy in case of failure at PCRF for CCFH continue, the local policy service should be associated with an IMS authorization service. In case of any failures, the local policy template associated with the ims-auth service will be chosen for fallback.

Example

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

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

cc-profile

This command configures the value of the **Offline** AVP sent to the PCRF based on the Charging Characteristics (CC) profile received from the SGSN.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

cc-profile *cc_profile_number* **[to** *cc_profile_number_range_end* **] map-to offline-avp { 0 | 1 }**
{ default | no } cc-profile

default

Configures the default setting for this command.

Default: Deletes all previously configured mappings.

no

Deletes all previously configured mappings.

cc_profile_number

Specifies the CC profile number to map.

For example, 1 for Hot Billing.

cc_profile_number must be an integer from 0 through 15.

cc_profile_number_range_end

Specifies, for a range of CC profile numbers to map, the end number. That is, from *cc_profile_number* through *cc_profile_number_range_end*.

cc_profile_number_range_end must be an integer from 1 through 15.

map-to offline-avp { 0 | 1 }

Specifies to map the CC profile number(s) to the **Offline** AVP value sent to the PCRF.

- **0**: Corresponds to the value DISABLE_OFFLINE (0).
- **1**: Corresponds to the value ENABLE_OFFLINE (1).

Usage Guidelines

Use this command to configure the CC Profile to **Offline** AVP value mapping. The **Offline** AVP's value (DISABLE_OFFLINE (0), ENABLE_OFFLINE (1)) is derived based on the CC profile received from the SGSN as specified by this mapping.

The following example shows how this command can be configured multiple times:

```
cc-profile 1 to 2 map-to offline-avp 1
cc-profile 4 map-to offline-avp 0
cc-profile 8 map-to offline-avp 1
```

On configuring the above set of commands, the Offline AVP value is sent as 1 (Offline enabled) for the CC profiles 1 (Hot Billing), 2 (Flat Rate), and 8 (Post-Paid). And, as 0 (Offline disabled) for the CC profile 4 (Pre-paid).

When configuring this command, overlapping of CC profile numbers is not permitted. In the following example, after configuring the first command, which specifies to send the **Offline** AVP's value as 1 (Offline enabled) for the CC profiles 1 through 15, the second command, which specifies to map CC profile 7, is not permitted:

```
cc-profile 1 to 15 map-to offline-avp 1
cc-profile 7 map-to offline-avp 0
```

Example

The following command specifies to send **Offline** AVP value as 1 (Offline enabled) for the CC profile 1 (Hot Billing):

```
cc-profile 1 map-to offline-avp 1
```

The following command specifies to delete all previously configured mappings:

```
no cc-profile
```

custom-reauth-trigger

This command enables custom reauthorization event triggers.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
custom-reauth-trigger { apn-ambr-mod-failure | default-bearer-qos-change
 | default-bearer-qos-mod-failure | qos-change |
resource-modification-request | ue-ip-addr-allocate | ue-ip-addr-release
 | none | { preservation-changed | reactivation-changed } + }
default custom-reauth-trigger
```

default

Configures the default setting for this command. The default setting is to enable all the event triggers.

none

Disables all custom event triggers.

apn-ambr-mod-failure

Enables APN AMBR Modification Failure event trigger.

default-bearer-qos-change

Enables Default EPS bearer QoS change event trigger.

default-bearer-qos-mod-failure

Enables Default EPS Bearer QOS Modification Failure event trigger.

qos-change

Enables QoS change trigger.

resource-modification-request

Enables Resource modification trigger.

ue-ip-addr-allocate

Enables UE IP address allocate trigger.

ue-ip-addr-release

Enables UE IP address release trigger.

preservation-changed

Enables preservation-changed event trigger.



Important This keyword is for use with a customer-specific implementation, and will be available only if a valid license is installed.

reactivation-changed

Enables reactivation-changed event trigger.



Important This keyword is for use with a customer-specific implementation, and will be available only if a valid license is installed.

Usage Guidelines

Use this command to enable/disable custom reauth event triggers.

It is recommended that the preservation-changed and reactivation-changed triggers both be enabled. As, when the bearer goes into preservation mode with the preservation-changed trigger, the reactivation-changed trigger must also be enabled for the bearer to get reactivated subsequently.

In 16.0 and later releases, this CLI command overwrites the previously configured triggers with the new event triggers. For example, if the following triggers are configured – QoS change, UE IP address allocation, UE IP address release, preservation-changed, reactivation-changed, then the APN-AMBR modification failure and Resource modification request triggers should be configured. This operation will overwrite all previously configured triggers and will configure only new APN-AMBR modification failure and Resource modification request triggers. By default, these event triggers are enabled.

Example

The following command disables all custom event triggers:

```
custom-reauth-trigger none
```

diameter 3gpp-r9-flow-direction

This command controls PCEF from sending Flow-Description, TFT-Filter, andPacket-Filter-Content AVPs in Rel. 9 format.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
[ no ] diameter 3gpp-r9-flow-direction
```

3gpp-r9-flow-direction

Encodes Flow-Direction, Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs based on 3GPP Rel. 9 specification.

no

Encodes Flow-Direction, Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs in Rel. 8 format. This is the default configuration.

Usage Guidelines

Use this command to enable Rel.9 changes for Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs sent by PCEF in CCR-U. This CLI command works in conjunction with **diameter update-dictionary-avps { 3gpp-r9 | 3gpp-r10 }**. When **diameter 3gpp-r9-flow-direction** is configured and negotiated supported feature is 3gpp-r9 or above, PCEF will send Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs in 3GPP Rel. 9 format.

Per the 3GPP Rel. 8 standards, the IPFilterRule in Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs is sent as "permit in" for UPLINK and "permit out" for DOWNLINK direction. From 3GPP Rel. 9 onwards, the Flow-Description AVP within the Flow-Information AVP will have only "permit out" and the traffic flow direction is indicated through Flow-Direction AVP. In 3GPP Rel. 9 format, both UPLINK and DOWNLINK are always sent as "permit out" and hence the usage of "permit in" is deprecated.

Backward compatibility is maintained, i.e. both Rel. 8 (permit in/out) and Rel. 9 (permit out with flow-direction) formats are accepted by PCEF.

This CLI command must be used only after the PCRF is upgraded to Rel. 9. For more information on this feature, see the *3GPP Rel.9 Compliance for IPFilterRule* section in the *Gx Interface Support* chapter in the administration guide for the product you are deploying.

Example

The following command enables Rel.9 changes for Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs:

```
diameter 3gpp-r9-flow-direction
```

diameter clear-session

This command enables the system to clear the subscriber sessions which are affected by session ID mapping mismatch.

Product

GGSN

HA

HSGW

IPSG

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
diameter clear-session sessid-mismatch
[ no ] diameter clear-session
```

sessid-mismatch

Clears the session with mismatched session ID. This CLI configuration is optional.

no

This keyword does not delete the subscriber sessions. This is the default configuration.

Usage Guidelines

Use this command to clear the subscriber sessions that are impacted due to the mismatch in the Diameter proxy-session manager mapping.

In the event of rapid back-to-back ICSR switchovers or extensive multiple process failures, the Diameter proxy-Session manager mapping information is not preserved across ICSR pairs. This mismatch in the Diameter proxy-Session ID results in rejection of RAR with 5002 - DIAMETER_UNKNOWN_SESSION_ID cause code. This behavior impacts the VoLTE call setup procedure. This CLI configuration is provided to control the behavior and delete the mismatched subscriber sessions.

When session manager sends an RAA with 5002 DIAMETER_UNKNOWN_SESSION_ID cause code, the dpca-rar-dp-mismatch bulk statistic counter in IMSA schema is incremented to indicate the session ID/Diamproxy grouping mismatch and also initiate the session termination. A Delete Bearer Request is sent to S-GW with a Reactivation Requested as the cause code while suppressing the CCR-T from being sent to PCRF. With this approach, the subscriber reattaches immediately without impacting the subsequent VoLTE calls, encountering only one failure instead of manual intervention.

Example

The following command enables the system to delete the mismatched subscriber sessions:

```
diameter clear-session sessid-mismatch
```

diameter dictionary

This command specifies the Diameter Policy Control Application dictionary to be used by the IMS Authorization Service for the policy control application.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
diameter dictionary { Standard | dpca-custom1 | dpca-custom10 |
dpca-custom11 | dpca-custom12 | dpca-custom13 | dpca-custom14 |
```

```
dpca-custom15 | dpca-custom16 | dpca-custom17 | dpca-custom18 |
dpca-custom19 | dpca-custom2 | dpca-custom20 | dpca-custom21 |
dpca-custom22 | dpca-custom23 | dpca-custom24 | dpca-custom25 |
dpca-custom26 | dpca-custom27 | dpca-custom28 | dpca-custom29 |
dpca-custom3 | dpca-custom30 | dpca-custom4 | dpca-custom5 | dpca-custom6
 | dpca-custom7 | dpca-custom8 | dpca-custom9 | dynamic-load |
gx-wimax-standard | gxa-3gpp2-standard | gxc-standard | pdsn-ty |
r8-gx-standard | std-pdsn-ty | ty-plus | ty-standard }
default diameter dictionary
```

dpca-custom1

Custom-defined Diameter dictionary for the Gx interface.

dpca-custom2

Custom-defined Diameter dictionary for Rel. 7 Gx interface.

dpca-custom3

Custom-defined Diameter dictionary for the Gx interface in conjunction with IP Services Gateway (IPSG).

dpca-custom4

Standard Diameter dictionary for 3GPP Rel. 7 Gx interface.

dpca-custom5

Custom-defined Diameter dictionary for Rel. 7 Gx interface.

dpca-custom6 ... dpca-custom30

Custom-defined Diameter dictionaries.

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.

gx-wimax-standard

Gx WiMAX standard dictionary.

gxa-3gpp2-standard

Gxa 3GPP2 standard dictionary.

gxc-standard

Gxc standard dictionary.

pdsn-ty

This keyword is restricted.

r8-gx-standard

R8 Gx standard dictionary.

Standard

Standard Diameter dictionary for the 3GPP Rel. 6 Gx interface.

Default: Enabled for Gx support in 3GPP networks.

std-pdsn-ty

This keyword is restricted.

ty-plus

This keyword is restricted.

ty-standard

This keyword is restricted.

default

Sets the default Diameter dictionary.

Default: **Standard**

Usage Guidelines

Use this command to specify the Diameter dictionary for IMS Authorization Service.

Example

The following command sets the **Standard** dictionary for Diameter Policy Control functions in 3GPP network:

```
diameter dictionary Standard
```

diameter encode-event-avps

This command enables encoding of all the event-related information AVPs in CCR-U messages.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
[ default ] diameter encode-event-avps { always | local-fallback }
```

default

Applies the default setting for this command.

Default: Sends AVPs relevant to the Event-Trigger subscribed by the PCRF.

always

This keyword option always sends the event-related AVPs in all CCR messages.

local-fallback

This keyword option sends the event-related AVPs in CCR-U messages in the event of local fallback scenario.

Usage Guidelines

Use this command to facilitate sending of all the event-related information AVPs in CCR-U messages.

In releases prior to 14.0, per the 3GPP standards for Gx, AVPs relevant to the Event-Trigger subscribed by the PCRF were always sent in the CCR messages. This release onwards, sending of event-related AVPs for all update (both access side and internal) and terminate requests is CLI controlled.

Note that the QoS-Info AVP will be encoded in all CCR-U messages if the CLI command "**diameter encode-event-avps always**" is enabled. This implementation impacts only the dpca-custom15 dictionary.

Example

The following command enables to always send the event-related AVPs in all CCR messages:

```
diameter encode-event-avps always
```

diameter encode-supported-features

This command enables/disables encoding and sending of Supported-Features AVP.

Product

GGSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
diameter encode-supported-features { adc-rules | cno-uli |
conditional-apn-policy-info | conditional-policy-info |
conditional-policy-info-default-qos | extended-bw-newradio |
mission-critical-qcis | multiple-pra | netloc | netloc-ran-nas-cause |
pcscf-restoration-ind | pending-transactions | session-recovery |
session-sync | sgw-restoration | sponsored-connectivity | trusted-wlan |
 netloc-trusted-wlan | netloc-untrusted-wlan | virtual-apn }
{ default | no } diameter encode-supported-features
```

adc-rules

This keyword enables configuration of Application Detection and Control (ADC) rules over Gx interface. For ADC 6th bit of supported feature will be set. By default, this supported feature will be disabled.

Important ADC Rule support is a licensed-controlled feature. Contact your Cisco account representative for detailed information on specific licensing requirements.

This keyword "**adc-rules**" will be available only when the feature-specific license is configured.

In release 18, the gateway node will use ADC functionality over Gx as defined in the Release 11 specification of 3GPP standard. ADC extension over Gx provides the functionality to notify PCRF about the start and stop of a specific protocol or a group of protocols, and provide the possibility to PCRF that with the knowledge of this information, change the QoS of the user when the usage of application is started and until it is finished.

The provision of ADC information is done through the ADC rule, the action initiated by PCRF is done through the PCC rule.

ADC rules are certain extensions to dynamic and predefined PCC rules in order to support specification, detection and reporting of an application flow. These rules are installed (modified/removed) by PCRF via CCA-I/CCA-U/RAR events. ADC rules can be either dynamic PCC or predefined PCC rules, and the existing attributes of dynamic and predefined rules will be applicable.

Dynamic PCC rule contains either traffic flow filters or Application ID. When Application ID is present, the rule is treated as ADC rule. Application ID is the name of the ruledef which is pre-defined in the boxer configuration. This ruledef contains application filters that define the application supported by P2P protocols.

PCEF will process and install ADC rules that are received from PCRF interface, and will detect the specified applications and report detection of application traffic to the PCRF. PCRF in turn controls the reporting of application traffic.

PCEF monitors the specified applications that are enabled by PCRF and generates Start/Stop events along with the Application ID. Such application detection is performed independent of the bearer on which the ADC PCC rule is bound to. For instance, if ADC rule is installed on a dedicated bearer whereas the ADC traffic is received on default bearer, application detection unit still reports the start event to PCRF.

cno-uli

This keyword enables the Presence Reporting Area (PRA) feature. Configuring cno-uli keyword enables feature bit in supported feature AVP and helps in negotiating with PCRF.

The Presence Reporting Area is an area defined within the 3GPP packet domain for the purpose of reporting of UE presence within that area. This is required for policy control and in charging scenarios.

During an IP-CAN session, the PCRF determines whether the reports for change of the UE presence in the PRA are required for an IP-CAN session. This determination is made based on the subscriber's profile configuration and the supported AVP features.

conditional-apn-policy-info

This keyword enables the Conditional APN Policy Information feature. This feature bit support is added to enable this feature for negotiation with PCRF. By default, this supported feature is disabled.

Use all three keywords—conditional-apn-policy-info, conditional-policy-info, conditional-policy-info-default-qos—to enable conditional Policy information feature on the P-GW. Using the no form of the command for all the three keywords, disables this feature.

Using only one of the keywords enables the feature bit in supported feature AVP.

Using no form of this command with only one of the keywords disables a specific feature bit in negotiation of this feature.



Important This keyword is customer-specific. For more information, contact your Cisco account representative.

conditional-policy-info

This keyword enables the Conditional Policy Information feature. This feature bit support is added to enable this feature for negotiation with PCRF. By default, this supported feature is disabled.

Use all three keywords—conditional-apn-policy-info, conditional-policy-info, conditional-policy-info-default-qos—to enable conditional Policy information feature on the P-GW. Using the no form of the command for all the three keywords, disables this feature.

Using only one of the keywords enables the feature bit in supported feature AVP.

Using no form of this command with only one of the keywords disables a specific feature bit in negotiation of this feature.



Important This keyword is customer-specific. For more information, contact your Cisco account representative.

conditional-policy-info-default-qos

This keyword enables the Conditional Policy Information Default QoS feature. This feature bit support is added to enable this feature for negotiation with PCRF. By default, this supported feature is disabled.

Use all three keywords—conditional-apn-policy-info, conditional-policy-info, conditional-policy-info-default-qos—to enable conditional Policy information feature on the P-GW. Using the no form of the command for all the three keywords, disables this feature.

Using only one of the keywords enables the feature bit in supported feature AVP.

Using no form of this command with only one of the keywords disables a specific feature bit in negotiation of this feature.



Important This keyword is customer-specific. For more information, contact your Cisco account representative.

extended-bw-newradio

This keyword enables Extended Bandwidth with New-Radio feature.

mission-critical-qcis

This keyword enables Mission Critical (MC)-Push to Talk (PTT) (MC-PTT) QCI feature. By default, this feature will not be enabled.



Important This keyword can be enabled only if the Wireless Priority Feature Set (WPS) license is configured. For licensing information, contact your Cisco account or support representative.

To support the MC-PTT services, a new set of standardized QoS Class Identifiers (QCIs) (65, 66, 69, 70) have been introduced. These are 65-66 (GBR) and 69-70 (non-GBR) network-initiated QCIs defined in 3GPP TS 23.203 v13.6.0 and 3GPP TS 23.401 v13.5.0 specifications. These QCIs are used for Premium Mobile Broadband (PMB)/Public Safety solutions.

In releases prior to 21, the gateway accepted only standard QCIs (1-9) and operator defined QCIs (128-254). If the PCRF sends QCIs with values between 10 and 127, then the gateway rejected the request. The MC QCI support was not negotiated with PCRF. In 21 and later releases, PCRF accepts the new standardized QCI values 69 and 70 for Default Bearer creation and 65, 66, 69 and 70 for Dedicated Bearer creation.

When **mission-critical-qcis** option is enabled, the gateway allows configuring MC QCIs as a supported feature and then negotiates the MC-PTT QCI feature with PCRF through Supported-Features AVP.

The gateway rejects the session create request with MC-PTT QCIs when the WPS license is not enabled and Diameter is not configured to negotiate MC-PTT QCI feature, which is part of Supported Feature bit.

To disable the negotiation of this feature, the existing **no diameter encode-supported-features** command needs to be configured. On executing this command, none of the configured supported features will be negotiated with the PCRF.

For more information on this feature, see the *Gx Interface Support* chapter in the administration guide of the product you are deploying.

multiple-pra

Enables the Multiple Presence Reporting Area Information Reporting.

netloc

Enables the NetLoc feature. The NetLoc feature indicates the support for reporting of the Access Network Information.



Important Network Provided Location Information (NPLI) feature is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

A new feature "netloc" (feature bit 10) has been added as part of the Supported-Features AVP to implement the Network provided Location Info (NPLI) feature for IMS. NPLI is used to support variety of applications like emergency call, Lawful intercept, charging, etc.



Important This feature works only if PCRF too supports netloc.

The netloc feature bit will be sent to PCRF on demand via CCR-I message. A new event trigger "ACCESS_NETWORK_INFO_REPORT (45)" and a new Diameter AVP "Required-Access-Info" have been added to support the NPLI enhancement.

The gateway node provides the required access network information (e.g. user location and/or user time zone information) to the PCRF within the 3GPP-User-Location-Info AVP, User-Location-Info-Time AVP (if available), and/or 3GPP-MS-TimeZone AVP as requested by the PCRF. The gateway also provides the ACCESS_NETWORK_INFO_REPORT event trigger within Event-Trigger AVP.

netloc-ran-nas-cause

Enables the Netloc-RAN-NAS-Cause feature. By default, this supported feature will be disabled.

This feature is used to send detailed RAN and/or NAS release cause code information from the access network to PCRF. This feature is added to be in compliance with Release 12 specification of 3GPP TS 29.212. It requires that the NetLoc feature is also supported.

A new feature "netloc-ran-nas-cause" (feature bit 22) has been added as part of the Supported-Features AVP to support the 3GPP RAN/NAS Release Cause Code Information Element (IE) on Gx interface. Starting from Release 21.2, this feature is supported on S5/S8, and S2b interfaces.



Important This feature can be enabled only when the NetLoc feature license is installed. However, from StarOS Release 21.1, you can enable the RAN/NAS feature without configuring the NetLoc feature. It is not mandatory to configure the "netloc" keyword to configure the "netloc-ran-nas-code" keyword.

If the supported features "netloc-ran-nas-code" and "netloc" are enabled, then netloc-ran-nas-cause code will be sent to PCRF via CCR-T message. A new Diameter AVP "RAN-NAS-Release-Cause" has been added to support this feature. This AVP will be included in the Charging-Rule-Report AVP and in CCR-T for bearer and session deletion events respectively.

pcscf-restoration-ind

Enables the P-CSCF Restoration Indication feature. By default, this feature is disabled.



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

This keyword, when enabled, allows the negotiation of P-CSCF Restoration feature support with PCRF. A new Diameter AVP "**PCSCF-Restoration-Indication**" is introduced to indicate to PCEF that a P-CSCF Restoration is requested. This is achieved by setting AVP value to 0.

For more information on this feature, see the *Gx Interface Support* chapter in the administration guide of the product you are deploying.

pending-transactions

Configures the Pending Transactions feature as part of supported features. This keyword addition is to handle race conditions on Gx i.e. process the Diameter messages in the order they are received.

Gx-based applications are vulnerable to certain race conditions (e.g. concurrent RAR/CCR). Enhancements are done on the Diameter protocol to deterministically handle the race conditions on Gx.

In a scenario wherein RAR is received while waiting for CCA-U, Gx application rejects RAR with Experimental-Result-Code AVP set to DIAMETER_PENDING_TRANSACTION. This should be done only if PCRF supports this functionality otherwise Gx client should continue with the current implementation.

If race conditions are not processed properly, it can lead to unpredictable behavior from each node, resulting in subscriber disconnection. With this feature, the outcome in such situation is deterministic and operator has the ability to influence the node behavior aligned with their policy.



Important Currently only one pending transaction is supported. So, all other transactions (like handoffs, etc) while one is pending will be rejected.

In 17.0 and later releases, in order to comply with 4G Network Upgrade 3GPP Standard, the following changes are implemented:

- Support for Negotiation of PT in initial session establishment.
- Support for receiving/sending 4144 with 3GPP Vendor ID in CCA/RAA.
- Retry of CCR-U when 4144 is received from PCRF.
- No Support for 4198 with Proprietary Vendor ID.
- Recovery of negotiated Supported features.

session-recovery

Enables the Session Recovery feature. This functionality helps ensure that the PCRF and P-GW can be in sync on session information and recover any lost Gx sessions. By default, session recovery and session sync features are not enabled.

Gx sessions typically tend to be long-lived. In case of session loss in PCRF (e.g. due to software failure), or a message loss in PCRF (e.g. Gx:RAA is dropped due to overload control), there is no existing mechanism to allow the PCRF and P-GW to sync-up on session state like Rules Status, APN-AMBR, QoS, Event Triggers, etc. In this release, the Gx interface between P-GW and PCRF has been enhanced to allow the PCRF and P-GW to sync-up. This is currently not part of 3GPP 29.212.



Important In this release, the Session Recovery and Sync will be supported only for the IMS APN.

This keyword is used to achieve the session recovery. When this feature is enabled, P-GW and PCRF will exchange session information and P-GW provides the complete subscriber session information to enable PCRF to build the session state.

session-sync

Enables the Session Synchronization feature. This functionality helps ensure that the PCRF and P-GW can be in sync on session information and recover any lost Gx sessions. By default, Session Recovery and Session Sync features will not be enabled.

Gx sessions typically tend to be long-lived. In case of session loss in PCRF (e.g. due to software failure), or a message loss in PCRF (e.g. Gx:RAA is dropped due to overload control), there is no existing mechanism to allow the PCRF and P-GW to sync-up on session state like Rules Status, APN-AMBR, QoS, Event Triggers, etc. The Gx interface between P-GW and PCRF is enhanced to allow the PCRF and P-GW to sync-up. This is currently not part of 3GPP 29.212.



Important In this release, the Session Recovery and Sync will be supported only for the IMS APN.

This keyword is used to achieve the session sync-up. When this feature is enabled, P-GW and PCRF will exchange session information and P-GW provides the complete subscriber session information to enable PCRF to build the session state.

sgw-restoration

This keyword enables configuration of S-GW Restoration feature.

P-GW is configured to support S-GW Restoration feature. P-GW sends S-GW Restoration feature in Supported-Features AVP through the CCR-I message during session creation. If P-GW receives S-GW Restoration feature in Supported-Features AVP in CCA-I message, then P-GW enables S-GW Restoration feature.

If P-GW and PCRF support S-GW Restoration feature, then the P-GW accepts CCA and RAR during S-GW restoration. Only Rule removal or RAR with session release cause is processed. Any rule install or modify is dropped. P-GW triggers CCR-U with PCC rule failure report and AN_GW_STATUS AVP to inform PCRF that S-GW is down. After receiving the SGW_Restoration indication, PCRF does not initiate any rule install or modification towards the P-GW. The P-GW informs the PCRF when the S-GW has recovered using the Event-Trigger AVP set to AN_GW_CHANGE and including the AN-GW-Address AVP related to the restored or new S-GW. If S-GW restoration is reported to PCRF, then the P-GW sends CCR-U with AN_GW_CHANGE trigger.

If S-GW Restoration feature is not negotiated through the Supported-Features AVP, then P-GW falls back to the old behavior as follows:

- Drops all internal updates towards PCRF
- Rejects CCA and RAR during S-GW Restoration
- Does not include AN_GW_STATUS as AN_GW_FAILED (0) AVP in CCR-U
- Sends an RAA command with the Experimental-Result-Code set to UNABLE_TO_COMPLY (5012) upon receiving RAR command

After configuring the S-GW Restoration feature on Gx interface, the failure is sent to PCRF with Rule-Failure-Code as AN_GW_FAILED in both failure and restoration scenarios.

sponsored-connectivity

Enables the Sponsored (data) Connectivity feature.

With sponsored data connectivity, the sponsor has a business relationship with the operator and the sponsor reimburses the operator for the user's data connectivity in order to allow the user access to an associated Application Service Provider's (ASP) services. Alternatively, the user pays for the connectivity with a transaction which is separate from the subscriber's charging. It is assumed the user already has a subscription with the operator.

The purpose of this feature is to identify the data consumption for a certain set of flows differently and charge it to sponsor. To support this, a new reporting level "SPONSORED_CONNECTIVITY_LEVEL" is added for reporting at Sponsor Connection level and two new AVPs "Sponsor-Identity" and "Application-Service-Provider-Identity" have been introduced at the rule level.

This CLI command "**diameter encode-supported-features**" has been added in Policy Control Configuration mode to send Supported-Features AVP with Sponsor Identity.

Sponsored Connectivity feature will be supported only when both P-GW and PCRF support 3GPP Rel. 10. P-GW advertises release as a part of supported features in CCR-I to PCRF. If P-GW supports Release 10 and also Sponsored Connectivity but PCRF does not support it (as a part of supported features in CCA-I), this feature is turned off.

This feature implementation impacts only the Gx dictionary "dpca-custom15".

trusted-wlan

Enables the Trusted WLAN feature.

netloc-trusted-wlan

Enables the NetLoc trusted WLAN feature over Gx interface.

This command takes effect when Gx is enabled on S2b call. By default, the feature is disabled and TWAN information will not be sent over Gx.

netloc-untrusted-wlan

Enables the NetLoc untrusted WLAN feature over Gx interface.

This command takes effect when Gx is enabled on S2b call. By default, the feature is disabled and UWAN information will not be sent over Gx.

virtual-apn

This keyword enables configuration of Gx-based Virtual APN (VAPN) feature. For VAPN 4th bit of supported feature will be set. By default, this supported feature will be disabled.



Important Gx-based VAPN is a licensed-controlled feature. Contact your Cisco account representative for detailed information on specific licensing requirements.

This keyword "**virtual-apn**" will be available only when the feature-specific license is configured.

In releases prior to 19, VAPN selection was possible through RADIUS or local configuration. In Release 19, ASR5K uses PCRF and Gx interface for Virtual APN selection to achieve signaling reduction.

This keyword enables Gx based Virtual APN Selection feature for a given IMS authorization service. When this configuration is enabled at P-GW/GGSN, then P-GW/GGSN advertises this feature to PCRF through the Supported-Features AVP in CCR-I. When the VAPN is selected, then the PCRF rejects the CCR-I message

with the Experimental-Result-Code AVP set to 5999 (DIAMETER_GX_APN_CHANGE), and sends a new APN through the Called-Station-Id AVP in CCA-I message. The existing call is then disconnected and established with the new virtual APN. Note that the Experimental Result Code 5999 will have the Cisco Vendor ID.



Important Enabling this feature might have CPU impact (depending on the number of calls using this feature).

Limitations:

- Virtual APN supported feature negotiation, Experimental Result Code (5999), Called-Station-Id AVP should be received to establish the call with new virtual APN. When any one of conditions is not met then the call will be terminated.
- Failure-handling will not be taken into account for 5999 result-code when received in the CCA-I message.
- When the Experimental Result Code 5999 is received in the CCA-U then failure-handling action will be taken.
- If the Called-Station-Id AVP is received in CCA-U or CCA-T, then the AVP will be ignored.
- If virtual-apn is received in local-policy initiated initial message then the call will be terminated.
- When PCRF repeatedly sends the same virtual-apn, then the call will be terminated.

default | no

This keyword removes the previously configured supported features.

Usage Guidelines This command is used to enable encoding and sending of Supported-Features AVP.

diameter host-select reselect

This command controls pacing of the reselection or switching of the PCRF after a change occurs in the table configuration for an IMS Authorization Service.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > **context** *context_name* > **ims-auth-service** *service_name* > **policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
diameter host-select reselect subscriber-limit subs_limit time-interval
duration
{ default | no } diameter host-select reselect
```

subscriber-limit *subs_limit*

Specifies the limit of subscribers to switch or reselect the PCRF for subscribers not more than *subs_limit* in time duration of *duration* second(s).

subs_limit must be an integer from 1 through 10000000.

time-interval *duration*

Specifies the time duration, in seconds, to reselect PCRF for subscribers not more than *subs_limit* in time duration of *duration* second(s).

duration must be an integer from 1 through 3600.

default

Applies the default setting for this command.

Sets the PCRF reselection or switching to default state.

no

Removes the configured PCRF reselection method and disables the reselection or switching of PCRF.

Usage Guidelines

Use this command to specify the pacing of reselection or switching of the PCRF in an IMS authorization service..

In case IMS authorization session have been opened on certain PCRF on the basis of the current selection table, and the current active table configuration is changed, the IMSA starts selection procedure for the PCRF. Existing sessions on current PCRF from earlier table is required to close and reopened on the selected PCRF from the new table. This reselection periodicity is controlled by this command and it indicates the number of subscriber sessions *subs_limit* to be reselected or moved in *duration* seconds.

For example, if this command is configured with *100* subscribers and *2* seconds, then the system reselects the PCRF for no more than *100* subscribers per *2* seconds.

Example

The following command sets the system to reselect the new PCRF for no more than *1000* subscriber in *15* seconds:

```
diameter host-select reselect subscriber-limit 1000 time-interval 15
```

diameter host-select row-precedence

This command adds/appends rows with precedence to a Diameter host table or MSISDN prefix range table.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > **context** *context_name* > **ims-auth-service** *service_name* > **policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
diameter host-select row-precedence precedence_value table { { { 1 | 2 } host
 host_name [ realm realm_id ] [ secondary host host_name [ realm realm_id ] ] }
| { prefix-table { 1 | 2 } msisdn-prefix-from msisdn_prefix_from
msisdn-prefix-to msisdn_prefix_to host host_name [ realm realm_id ] [ secondary
 host sec_host_name [ realm sec_realm_id ] algorithm { active-standby |
round-robin } ] } } [ -noconfirm ]
no diameter host-select row-precedence precedence_value table { { 1 | 2 } |
 prefix-table { 1 | 2 } }
```

diameter host-select row-precedence *precedence_value* table { 1 | 2 } host *host_name* [realm *realm_id*] [secondary host *sec_host_name* [realm *sec_realm_id*]]

This command adds/appends a row in the specified Diameter host table.

In 8.0, a maximum of 16 rows can be added to a table. In 8.1 and later releases, a maximum of 128 rows can be added per table.

row-precedence *precedence_value*: Specifies precedence of the row in the Diameter host table.



Important In 8.1 and later releases, *precedence_value* must be an integer from 1 through 128. In 8.0 and previous releases, *precedence_value* must be an integer from 1 through 100.

table { 1 | 2 }: Specifies the Diameter host table to add/append the primary and secondary Diameter host addresses.

host *host_name*: Specifies the primary host name. *host_name* must be an alphanumeric string of 1 through 127 characters in length.

realm *realm_id*: Specifies the primary realm ID. *realm_id* must be an alphanumeric string of 1 through 127 characters in length.

secondary host *sec_host_name* **[realm** *sec_realm_id* **]**: Specifies the secondary host name and realm ID:

host *sec_host_name*: Specifies the secondary host name. *host_name* must be an alphanumeric string of 1 through 127 characters in length.

realm *sec_realm_id*: Specifies the secondary realm ID. *realm_name* must be an alphanumeric string of 1 through 127 characters in length.

no diameter host-select row-precedence *precedence_value* table prefix-table { 1 | 2 } }

Removes the row with the specified precedence from the specified MSISDN prefix range table.

diameter host-select row-precedence *precedence_value* table prefix-table { 1 | 2 } msisdn-prefix-from *msisdn_prefix_from* msisdn-prefix-to *msisdn_prefix_to* host *host_name* [realm *realm_id*] [secondary host *sec_host_name* [realm *sec_realm_id*] algorithm { active-standby | round-robin }] [-noconfirm]

Use this command to configure the MSISDN prefix range based PCRF selection mechanism for Rel. 7 Gx interface support, wherein the PCEF is required to discover and select an appropriate PCRF to establish control relationship at primary PDP context activation.

This command adds a row in the specified MSISDN prefix range table. A maximum of 128 rows can be added per prefix range table.

row-precedence *precedence_value*: Specifies precedence of the row in the table.



Important In 8.1 and later releases, *precedence_value* must be an integer from 1 through 128. In 8.0 and previous releases, *precedence_value* must be an integer from 1 through 100.

prefix-table { 1 | 2 }: Specifies the MSISDN prefix range table to add the primary and/or secondary Diameter host addresses.

msisdn-prefix-from *msisdn_prefix_from*: For a range of MSISDNs, specifies the starting MSISDN.

msisdn-prefix-to *msisdn_prefix_to*: For a range of MSISDNs, specifies the ending MSISDN.



Important To enable the Gx interface to connect to a specific PCRF for a range of MSISDNs/subscribers configure *msisdn_prefix_from* and *msisdn_prefix_to* with the starting and ending MSISDNs respectively. The MSISDN ranges must not overlap between rows. To enable the Gx interface to connect to a specific PCRF for a specific MSISDN/subscriber, configure both *msisdn_prefix_from* and *msisdn_prefix_to* with the same MSISDN.

host *host_name*: Specifies the primary host name. *host_name* must be an alphanumeric string of 1 through 127 characters in length.

realm *realm_id*: Specifies the primary realm ID. *realm_id* must be an alphanumeric string of 1 through 127 characters in length.

secondary host *sec_host_name* **[realm** *sec_realm_id* **]**: Specifies the secondary host name and realm ID: **host** *sec_host_name*: Specifies the secondary host name. *sec_host_name* must be an alphanumeric string of 1 through 127 characters in length.

realm *sec_realm_id*: Specifies the secondary realm ID. *sec_realm_id* must be an alphanumeric string of 1 through 127 characters in length.

algorithm { active-standby | round-robin }: Specifies the algorithm for selection between primary and secondary servers in the MSISDN prefix range table.

Default: **active-standby**

active-standby: Specifies selection of servers in the Active-Standby fashion.

round-robin: Specifies selection of servers in the Round-Robin fashion.



Important The Round Robin algorithm for PCRF selection is effective only over a large number of PCRF selections, and not at a granular level.

[-noconfirm]

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

no diameter host-select row-precedence *precedence_value* table { 1 | 2 }

Removes the row with the specified precedence from the specified Diameter host table.

Usage Guidelines

Use this command to add, update, or delete rows specified with a precedence from a Diameter host table or MSISDN prefix range table.

In the Rel. 7 Gx implementation, when the Gateway interworks with multiple PCRFs, the Gateway can configure the primary and secondary server based on the MSISDN-prefix range in the MSISDN prefix range table. Using this command, you can add a new prefix row into the MSISDN prefix table.

If a row with the precedence that you add already exists in a table, the existing prefix row is removed and the new row is inserted with the same precedence.

Example

The following command adds a row with precedence *12* in table **2** with primary host name as *star_ims1* and secondary host name as *star_ims2* to Diameter host table.

```
diameter host-select row-precedence 12 table 2 host star_ims1 secondary host
 star_ims2
```

diameter host-select table

This command selects the Diameter host table or the MSISDN prefix range table, and the algorithm to select rows from the Diameter host table.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
diameter host-select table { { 1 | 2 } algorithm { ip-address-modulus [
prefer-ipv4 | prefer-ipv6 ] | msisdn-modulus | round-robin } | prefix-table
 { 1 | 2 } }
{ default | no } diameter host-select table
```

diameter host-select table { 1 | 2 } algorithm { ip-address-modulus | msisdn-modulus | round-robin }

table { 1 | 2 }: Specifies the Diameter host table to obtain the primary and secondary host names for PCRF.

algorithm { ip-address-modulus [prefer-ipv4 | prefer-ipv6] | msisdn-modulus | round-robin }: Specifies the algorithm to select row from the Diameter host table.

Default: **round-robin**

- **ip-address-modulus [prefer-ipv4 | prefer-ipv6]**: This algorithm divides the IP address, in binary, of the subscriber by the number of rows in the table, and the remainder is used as an index into the specified table to select the row.
- prefer-ipv4: Specifies that IPv4 addresses are to be used, if an IPv4v6 call is received, for selecting the rows in the host table.
- prefer-ipv6: Specifies that IPv6 addresses are to be used, if an IPv4v6 call is received, for selecting the rows in the host table.
- **msisdn-modulus**: This algorithm divides the MSISDN value in binary without the leading "+" of the subscriber by the number of rows in the table, and the remainder is used as an index in the specific table to select the row.
- **round-robin**: This algorithm rotates all rows in the active table for selection of the row in round-robin fashion. If no algorithm is specified this is the default behavior.



Important The Round Robin algorithm is effective only over a large number of selections, and not at a granular level.

diameter host-select table prefix-table { 1 | 2 }

Specifies the MSISDN Prefix Range table to be used in case of MSISDN prefix range based PCRF discovery mechanism.

default

Applies the default setting for this command.

no

Removes previous configuration.

When no table is selected, the system will not communicate with any PCRF for new sessions.

Usage Guidelines

Use this command to configure the Diameter host table and row selection methods to select host name or realm for PCRF.

When this command is used to change which table the system should be using, user must re-determine which E-PDF the system should be using for each subscriber. If a different E-PDF results from the configuration change in the table, the system will wait for all of the IMS sessions for the subscriber to be no longer active and then the system either closes/opens Gx sessions with the old/new PDFs respectively, or the system deactivates the PDP contexts of the subscriber.

Here is an example of how row selection is configured for three hosts that the system will use for load-balancing. Operator can configure six rows in a table, as follows.

Modulo 6	Primary Host	Secondary Host
0	1	2
1	1	3
2	2	1
3	2	3
4	3	1
5	3	2

In the above table, the three hosts are named 1, 2, and 3. When all hosts are working, the load will be distributed among all the three hosts. If host 1 fails, then the load will be distributed between the remaining two hosts. In this scenario, the modulo 6 results of 2 and 4 will return rows that have primary hosts but no working back-up host.

In the Rel. 7 Gx implementation, the GGSN/PCEF is required to discover and select an appropriate PCRF to establish control relationship at primary PDP context activation. The ip-address-modulus, msisdn-modulus, and round-robin algorithms are supported by the GGSN/PCEF for PCRF discovery. In addition, the active/standby and round-robin algorithms are used for selection between primary and secondary servers based on the MSISDN Prefix Range Table.

Example

The following command specifies **table 1** with **round-robin** algorithm to select the rows with host name for E-PDF in Diameter host table.

```
diameter host-select table 1 algorithm round-robin
```

diameter host-select-template

This command specifies the Diameter host server template to be associated with this IMS Authorization service. The service uses the specified template (and associated host-select table) to select a Diameter peer server. It then uses the returned host name(s) to contact the PCRF and establish the call.

Product

GGSN

HA

HSGW

IPSG

PDSN

P-GW

SAEGW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

diameter host-select-template *tmplt_name*
no diameter host-select-template

no

Removes the binding of the Diameter host select template with the IMS Authorization service.

tmplt_name

Specifies the name of an existing Diameter host server template (configured in Global Configuration mode) to bind with the IMS Authorization service. It is an alphanumeric string of 1 through 255 characters.

Usage Guidelines

Use this command to bind a configured Diameter host select template to the IMS Authorization service for DPCA. This IMS authorization service searches the associated host select table to select a Diameter peer server. For additional information refer to the *Diameter Host Select Configuration Mode Commands* chapter and the description of the **diameter-host-template** command in the *Global Configuration Mode Commands* chapter.

Important Prior to issuing this command, the Diameter host select template should be configured using the **diameter-host-template** command in the Global Configuration mode.

Important If no association is made to the template then the **diameter peer-select** command configured at the application level will be used for peer selection.

Example

The following command binds a configured Diameter host select template named *diamtemplate* to the IMS authorization service:

```
diameter host-select-template diamtemplate
```

diameter map

This command enables selecting the value to which the USAGE_REPORT and APN_AMBR_MOD_FAILURE Event-Trigger should be mapped to.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
diameter map usage-report { 29 | [ 26 | 33 ] [ 26 | 33 ] }
default diameter map usage-report
```

usage-report { 29 | [26 | 33] [26 | 33] }

Maps the USAGE_REPORT of Event-Trigger AVP to one or a combination of these values.

- 26 – Event-Trigger 26 will mapped to USAGE_REPORT. Note this will not affect any other Event-Trigger.
- 29 – Event-Trigger 29 will mapped to USAGE_REPORT, and 33 to APN_AMBR_MOD_FAILURE.
- 33 – Event-Trigger 33 will mapped to USAGE_REPORT, and 29 to APN_AMBR_MOD_FAILURE.

default

The default behavior is to configure the Event-Trigger USAGE_REPORT to be mapped to 26.

Usage Guidelines

The Event-Trigger AVP's USAGE_REPORT has been given different values in the 3GPP TS 29.212 standard spec. As a result of that, the releases of TS 29.212 are not backward compatible. To address this, this CLI command has been introduced in Policy Control configuration mode to map the USAGE_REPORT to either 26/29/33 or a combination of these values in order to be flexible enough to interoperate with various operators.

- TS 29.212 v9.5.0 - USAGE_REPORT (26)
- TS 29.212 v9.6.0 - USAGE_REPORT (29)
- TS 29.212 v9.7.0 - USAGE_REPORT (33)

If this CLI command **diameter map usage-report 29** is configured in the chassis and PCRF sends 29 event-trigger then on volume threshold breach CCR-U with volume-report and event-trigger 29 will be sent to the PCRF. Same is the case with the values 26 and 33.

In 17.1 and later releases, to be able to gracefully handle the change when moving between 3GPP releases supporting the different values for the Usage Report, the existing CLI command **diameter map usage-report** is modified to support configuration of multiple values of usage report mapping. While migrating from older versions to current version, all of the sessions created before the migration will continue to use 26 as usage report event trigger value. The new session will use usage-report value based on PCRF value or default value.

In releases prior to 17.1, when **diameter map usage-report** is mapped to 26, then APN AMBR modification failure event trigger is not supported. In 17.1 and later releases, APN AMBR modification failure event trigger is supported for all usage report trigger values (26, 33, 29).

Example

The following command maps the Event-Trigger USAGE_REPORT to 29 and APN_AMBR_MOD_FAILURE to 33:

```
diameter map usage-report 29
```

diameter origin endpoint

This command binds the origin endpoint configured in Context Configuration mode to the IMS Authorization service for Diameter Policy Control Application (DPCA).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

diameter origin endpoint *endpoint_name*
no diameter origin

endpoint *endpoint_name*

endpoint_name is the Diameter endpoint configured in Context Configuration Mode to bind with IMS authorization service, and must be an alpha/numeric string of 1 through 63 characters in length.

no

Removes the binding of Diameter origin endpoint with IMS Authorization service.

Usage Guidelines

Use this command to bind a configured Diameter origin endpoint to the IMS Authorization service for DPCA. This IMS authorization service searches all system contexts until it finds one with a matching Diameter origin endpoint name specified.

Example

The following command binds a configured endpoint named test to the IMS authorization service:

```
diameter origin endpoint test
```

diameter request-timeout

This command configures the request-timeout setting for Diameter-IMSA Gx interface.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
diameter request-timeout timeoutdeciseconds msg-type { any | ccr-initial
| ccr-terminate | ccr-update }
default diameter request-timeout
```

timeout

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

Default: 10 seconds

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

Specifies independent timers (in deciseconds) for all message types like CCR-I, CCR-U and CCR-T. 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**".

default

Applies the default setting for this command.

Usage Guidelines

Use this command to configure the request-timeout setting for Diameter-IMSA Gx interface. At the request-timeout value, DPCA will apply failure-handling to the subscriber. Action will be taken based on the failure-handling configuration (terminate/retry-terminate/continue).

Example

The following command configures the Diameter request-timeout setting to *20* seconds:

```
diameter request-timeout 20
```

diameter session-prioritization

This command enables prioritization of Gx messages based on eMPS state of the session. From Release 21.4, it also supports DRMP AVP with value 0 to be sent in Credit Control Request (Initial, Update and Terminate) messages over the Gx interface for P-GW eMPS sessions and for eMPS upgrade and downgrade transactions. Also the help string for “session prioritization” keyword is updated accordingly.

Product

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

`[ no ] diameter session-prioritization`

no

Disables the command and has the following implications:

- Disables prioritization of Gx messages for eMPS sessions and eMPS upgrade and downgrade.
- Disables encoding of DRMP AVP (value 0) in Credit Control Request (Initial, Update, and Terminate) messages for eMPS sessions and eMPS upgrade and downgrade.

By default, the CLI is disabled and Gx messages will not be prioritized based on eMPS value.

Usage Guidelines

Use this command to facilitate prioritization of Gx messages based on eMPS state of the session. From Release 21.4, it also supports DRMP AVP with value 0 to be sent in Credit Control Request (Initial, Update and Terminate) messages over the Gx interface for P-GW eMPS sessions and for eMPS upgrade and downgrade transactions. The help string is also changed for the existing command.

The Gx DRMP AVP is encoded when the **diameter session-prioritization** CLI is enabled in IMS Authorization Policy Control mode for policy control application. The following table summarizes the DRMP AVP values that are sent based on the different configurations and scenarios.

session prioritization CLI	eMPS Status of Session	Scenario	DRMP Encoding/Value
Off	Any	CCR Messages	Not Encoded
Any	Any	RAA response to RAR with DRMP X	Encoded/X
Off	eMPS	CCR Messages	Not Encoded
On	Yes	CCR Messages	Not Encoded
On	eMPS	CCR Messages	Encoded/0
On	Non-eMPS	CCR-U generated on eMPS state change from disabled to enabled.	Encoded/0

session prioritization CLI	eMPS Status of Session	Scenario	DRMP Encoding/Value
On	eMPS	CCR-U generated on eMPS state change from enabled to disabled.	Encoded/0
On	Non-eMPS	eMPS Upgrade failed and CCR-U follows	Encoded/0

This CLI takes affect when Gx, along with eMPS profile, is enabled in the configuration.

Example

The following command enables to prioritize Gx messages for sessions marked with eMPS:

```
diameter session-prioritization
```

diameter sgsn-change-reporting

This command enables reporting of SGSN_CHANGE event trigger and SGSN-Address AVP for 2G and 3G calls on GnGp P-GW.

Product

GGSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
diameter sgsn-change-reporting
no diameter sgsn-change-reporting
```

sgsn-change-reporting

This keyword specifies to detect SGSN change and send SGSN-Address AVP and SGSN_CHANGE event trigger for a subscriber in 2G/3G on Gx interface during GnGp scenario.

no

This variant specifies to send AN-GW-Address AVP during the call setup, when SGSN change happens, or during the handoff from 4G to 3G. This is the default setting.

Usage Guidelines

The current implementation does not send SGSN_CHANGE event trigger and SGSN- Address AVP. Instead it sends AN-GW-Address AVP and AN_GW_CHANGE event trigger for GnGp case. This behavior is not compliant to 3GPP standard TS 29.212 specification. Hence, in release 18, this CLI command "**diameter sgsn-change-reporting**" has been introduced to control this behavior.

This release provides, the GnGp P-GW users, the flexibility to configure detection of SGSN_CHANGE event trigger and to send SGSN-Address AVP for a subscriber in 2G/3G on Gx interface, so that PCRF can use this information to apply appropriate policies.

In releases prior to 18, AN-GW-Address AVP was sent in CCR-I message on GnGp scenario. AN_GW_CHANGE event trigger and AN-GW-Address AVP were sent when the inter-sgsn handoff or 4G to 2G/3G GnGp handoff happens.

When this CLI command is configured, SGSN-Address AVP will be sent in the CCR-I message for 2G/3G GnGp P-GW subscribers. SGSN_CHANGE event trigger and SGSN-Address AVP will be sent when the inter-sgsn handoff or 4G to 2G/3G GnGp handoff happens.



Important This feature is applicable only for SGSN IPv4 address. For SGSN IPv6 address, the SGSN-Address AVP will not be sent.

By default, AN-GW-Address AVP will be sent during the call setup, when SGSN change happens, or during the handoff from 4G to 3G.

Example

The following command configures to detect SGSN change and send SGSN-Address AVP in CCR-I :

```
diameter sgsn-change-reporting
```

diameter update-dictionary-avps

This command enables dictionary control of the AVPs that need to be added based on the version of the specification to which the PCEF is compliant with.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
diameter update-dictionary avps { 3gpp-r8 | 3gpp-r9 | 3gpp-r10 }
{ default | no } diameter update-dictionary avps
```

default | no

Configures this command with the default setting.

The default behavior is that R9 support will not be indicated as part of Supported-Features AVP in a R7/R8 dictionary and R8 support will not be indicated as part of Supported-Features AVP in a R7 dictionary.

3gpp-r8

Specifies to select the 3GPP Rel. 8 AVPs for encoding.

3gpp-r9

Specifies to select the 3GPP Rel. 9 AVPs for encoding.

3gpp-r10

Specifies to select the 3GPP Rel. 10 AVPs for encoding.

Usage Guidelines



Important This command is applicable only to Diameter dictionaries that support standard based volume reporting over Gx feature.

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

Release 12.0 onwards, if a 3GPP Rel. 7 based dictionary is already configured with **diameter dictionary dpca-custom4** command, and then if the **diameter update-dictionary-avps 3gpp-r9** command is applied, the Supported-Features AVP with feature bit 1 being set will be sent in the CCR-I to indicate that 3GPP Rel. 9 AVPs are also supported.

Both **default** and **no** command have the same behavior, as if the CLI command is not configured. Hence, in the output of **show configuration verbose** command, the **default** and **no** command is shown as **no diameter update-dictionary-avps**.

This CLI command when configured results in behavioral changes as indicated in the following table.

Possible Upgrade Scenarios	Behavior
3GPP Rel. 7 based dictionary upgraded to 3GPP Rel. 9 For example: **diameter dictionary dpca-custom4** **diameter update-dictionary-avps 3gpp-r9**	In the CCR-I, Supported-Features AVP will be encoded with value 2 for the Feature-List AVP. [V] [M] Supported-Features: [M] Vendor-Id: 10415 [V] [M] Feature-List-ID: 1 [V] [M] Feature-List: 2 The Feature-List AVP value suggest that it is 3GPP Rel. 9 compliant. But, it is not fully complaint to 3GPP Rel. 9. In the current release, for this upgrade scenario (3GPP Rel. 7 to 3GPP Rel. 9), only volume reporting related AVPs mentioned in the 3GPP Rel. 9 will be supported.

Possible Upgrade Scenarios	Behavior
3GPP Rel. 7 based dictionary upgraded to 3GPP Rel. 8 For example: **diameter dictionary dpca-custom4** **diameter update-dictionary-avps 3gpp-r8**	In the CCR-I, Supported-Features AVP will be encoded with value 1 for the Feature-List AVP. [V] [M] Supported-Features: [M] Vendor-Id: 10415 [V] [M] Feature-List-ID: 1 [V] [M] Feature-List: 1 The Feature-List AVP value suggest that it is 3GPP Rel. 8 compliant. But, it is not fully complaint to 3GPP Rel. 8. In the current release, for this upgrade scenario (3GPP Rel. 7 to 3GPP Rel. 8), none of the features mentioned in 3GPP Rel. 8 will be supported.
3GPP Rel. 8 based dictionary upgraded to 3GPP Rel. 9 For example: **diameter dictionary r8-gx-standard** **diameter update-dictionary-avps 3gpp-r9**	In the CCR-I, value for the Feature-List AVP in the Supported-Features AVP will be 2. [V] [M] Supported-Features: [M] Vendor-Id: 10415 [V] [M] Feature-List-ID: 1 [V] [M] Feature-List: 2 The Feature-List AVP value suggest that it is 3GPP Rel. 9 compliant. But, it is not fully complaint to 3GPP Rel. 9. Currently for this upgrade scenario (3GPP Rel. 8 to 3GPP Rel. 9), only volume reporting related AVPs mentioned in 3GPP Rel. 9 will be supported.
3GPP Rel. 9 based dictionary upgraded to 3GPP Rel. 10 For example: **diameter dictionary r8-gx-standard** **diameter update-dictionary-avps 3gpp-r10**	In the CCR-I, value for the Feature-List AVP in the Supported-Features AVP will be 8. [V] [M] Supported-Features: [M] Vendor-Id: 10415 [V] [M] Feature-List-ID: 1 [V] [M] Feature-List: 8 The Feature-List AVP value suggest that it is 3GPP Rel. 10 compliant. But, it is not fully complaint to 3GPP Rel. 10.

In 14.1 and later releases, Supported-Features AVP is extended to support 3GPP Rel. 10 in EPS 3.0 in addition to 3GPP Rel. 8 and Rel. 9. If the **diameter update-dictionary-avps 3gpp-r10** command is applied, the Supported-Features AVP with feature bit 1 being set will be sent in the CCR-I / CCA to indicate that 3GPP Rel. 10 AVPs are also supported. The 'M' bit setting for the Feature-List AVP and Feature-List-ID AVP must be the same as defined in 3GPP TS 29.229 and must not be affected by the 'M' bit setting of the Supported-Features AVP.

Example

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

```
diameter update-dictionary-avps 3gpp-r9
```

encode-cc-in-r8-gx-dict

This command enables r8-gx-standard dictionary configuration to send 3GPP-Charging-Characteristics AVP in CCR message.

Product

GGSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the preceeding command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
encode-cc-in-r8-gx-dict
{ default | no } encode-cc-in-r8-gx-dict
```

encode-cc-in-r8-gx-dict

Specifies to perform r8-gx-standard dictionary configuration by sending 3GPP-Charging-Characteristics AVP in CCR message.

default | no

Default/no behavior is to avoid r8-gx-standard dictionary configuration impacting other users. By default, this feature is disabled.

Usage Guidelines

Use this command to enable the inclusion of 3GPP-Charging-Characteristics AVP in CCR-I messages when using the r8-gx-standard dictionary.

Example

This command enables r8-gx-standard dictionary configuration to send 3GPP-Charging-Characteristics AVP in CCR message.

```
encode-cc-in-r8-gx-dict
```

endpoint-peer-select

This command enables Diabase to select the Diameter peers in all failure scenarios.

Product

GGSN

PGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

endpoint-peer-select [on-host-select-failure | on-inactive-host] { default | no } endpoint-peer-select

on-host-select-failure

Specifies to perform server selection at Diabase when the hosts could not be selected by IMS Authorization application.

on-inactive-host

Specifies to perform server selection at diabase when the hosts selected by application are inactive.

default | no

Default/no behavior is to terminate the call when the hosts could not be selected by application or when the hosts selected by application are inactive.

Usage Guidelines

Use this command to perform server selection at Diabase when the hosts could not be selected by application or when the hosts selected by the IMS Authorization application is inactive. For example, host table is not configured in IMSA service, host table is configured but not activated, none of the rows in prefix table match the subscriber, host template is not associated with IMSA service, host template could not select the hosts.

This CLI command is added in policy control configuration mode to maintain backward compatibility with the old behavior of terminating the call when server selection fails at application.

Example

The following command enables Diabase to select peers when the hosts selected by application are inactive.

```
endpoint-peer-select on-inactive-host
```

event-report-indication

This command enables event report indication.

Product

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
event-report-indication { all | pgw-trace-control | qos-change | rai-change
 | rat-change | sgsn-change | ue-timezone-change | user-loc-change } [
pgw-trace-control ] [ qos-change ] [ rai-change ] [ rat-change ] [
sgsn-change ] [ ue-timezone-change ] [ user-loc-change ]
{ default | no } event-report-indication
```

all | pgw-trace-control | qos-change | rai-change | rat-change | sgsn-change | ue-timezone-change | user-loc-change

Specifies which types of changes will trigger an event report from the PCRF.

- **all**: all triggers
- **pgw-trace-control**: P-GW trace control change trigger
- **qos-change**: QoS change trigger
- **rai-change**: RAI change trigger
- **rat-change**: RAT change trigger
- **sgsn-change**: SGSN change trigger
- **ue-timezone-change**: UE time zone change trigger
- **user-loc-change**: User location change trigger

default | no

Disables event report indication.

Usage Guidelines

Use this command to determine what type of event changes are reported from the PCRF.

Example

The following command enables event report indication for all triggers.

```
event-report-indication all
```

event-update

This command configures sending usage monitoring information in event updates either for all event triggers or for a specific event trigger.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
event-update send-usage-report [ reset-usage ] [ events { an-gw-change |
 apn-ambr-mod-failure | bearer-loss | bearer-rcvry |
charging-correlation-exchange | default-bearer-qos-change |
default-bearer-qos-mod-failure | ip-can-change | out-of-credit |
pgw-trace-control | plmn-change | qos-change | qos-excess-change |
rai-change | rat-change | reallocation-of-credit |
resource-modification-request | revalidation-timeout | sgsn-change |
successful-resource-alloc | tft-change | ue-ip-addr-allocate |
ue-ip-addr-release | ue-timezone-change| user-loc-change }+ ]
{ default | no } event-update
```

default

Configures the default setting for this command.

Default: Usage report is not sent in event update.

no

Disables sending usage report in event update.

reset-usage

Resets the usage at PCEF after reporting in event update.

events { an-gw-change | apn-ambr-mod-failure | bearer-loss | bearer-rcvry | charging-correlation-exchange | default-bearer-qos-change | default-bearer-qos-mod-failure | | ip-can-change | out-of-credit | pgw-trace-control | plmn-change | qos-change | qos-excess-change | rai-change | rat-change | reallocation-of-credit | resource-modification-request | revalidation-timeout | sgsn-change |

successful-resource-alloc | tft-change | ue-ip-addr-allocate | ue-ip-addr-release | ue-timezone-change| user-loc-change }+

Sends the custom usage report based on the following event triggers:

- an-gw-change — AN GW change event trigger
- apn-ambr-mod-failure — APN AMBR Modification Failure event trigger
- bearer-loss — Loss of bearer trigger
- bearer-rcvry — Recovery of bearer trigger
- charging-correlation-exchange — Charging Correlation Exchange trigger
- default-bearer-qos-change — Default EPS bearer QoS change event trigger
- default-bearer-qos-mod-failure — Default EPS Bearer QOS Modification Failure event trigger
- ip-can-change — IP-CAN Change trigger
- out-of-credit — Out of credit trigger
- pgw-trace-control — P-GW Trace Control
- plmn-change — PLMN change trigger
- qos-change — QoS change trigger
- qos-excess-change — Qos Change Exceeding Authorization trigger
- rai-change — RAI Change trigger
- rat-change — RAT change trigger
- reallocation-of-credit — Reallocation of credit trigger
- resource-modification-request — Resource modification trigger
- revalidation-timeout — Revalidation timeout trigger
- sgsn-change — SGSN change trigger
- successful-resource-alloc — Successful Resource Allocation event trigger
- tft-change — TFT change trigger
- ue-ip-addr-allocate — UE IP address allocate trigger
- ue-ip-addr-release — UE IP address release trigger
- ue-timezone-change — UE Time Zone Change event trigger
- user-loc-change — User Location Change trigger

Usage Guidelines

Use this command to send volume usage information when an event change is reported to the PCRF in a CCR-U message.

To send customized usage information based on specific event triggers, the event should be accordingly configured with the **event-update send-usage-report events** command. For example, if the usage report is

required whenever RAT change occurs, this can be accomplished using the **event-update send-usage-report events rat-change** command.

Example

The following command specifies to send volume usage report in event updates to the PCRF for all event triggers:

```
event-update send-usage-report reset-usage
```

The following command specifies to send volume usage report in event updates to the PCRF for RAT change scenarios:

```
event-update send-usage-report reset-usage events rat-change
```

The following command specifies to send volume usage report in event updates to the PCRF if either RAT change or QOS change occurs:

```
event-update send-usage-report reset-usage events rat-change qos-change
```

failure-handling

This command configures Diameter failure handling behavior.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > **context** *context_name* > **ims-auth-service** *service_name* > **policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

In Release 8.0:

```
failure-handling { continue | retry-and-terminate | terminate |
diameter-result-code { any-error | result_code } ccfh { continue |
retry-and-terminate | terminate } [ cc-request-type { initial-request |
terminate-request | update-request } ] }
no failure-handling diameter-result-code { any-error | integer result_code
 } [ cc-request-type { initial-request | terminate-request | update-request
 } ]
```

In 8.1 and later releases:

```
failure-handling cc-request-type { any-request | initial-request |
terminate-request | update-request } { diameter-result-code { any-error
| result_code [ to end_result_code ] } } { continue [ retry-server-on-event |
send-ccrt-on-call-termination ] | retry-and-terminate | terminate }
no failure-handling cc-request-type { any-request | initial-request |
terminate-request | update-request } [ diameter-result-code { any-error
```

```
| result_code [ to end_result_code] } ] [ continue {
send-ccrt-on-call-termination } ]
```

no

Disables previous failure-handling configuration.

retry-and-terminate

Specifies that in the event of a failure the user session continues for the duration of one retry attempt with the server. If this retry attempt also fails, the session is terminated.

terminate

Specifies that in the event of a failure the user session be terminated.

diameter-result-code { any-error | *result_code* [to *end_result_code*] }

Specifies failure handling behavior for any/specific result-code(s) to identify the type of failure and failure handling action for specific credit control request type.

any-error: Specifies failure handling behavior for those result-codes for which failure-handling behavior has not been specified.

result_code: Specifies a Diameter failure result code. *result_code* is the code returned for a failure handling action and must be an integer from 3000 through 4999.

to *end_result_code*: Use to specify a range of Diameter failure result codes. *end_result_code* must be an integer from 3000 through 4999, and must be greater than *result_code*.

continue [retry-server-on-event | send-ccrt-on-call-termination] | retry-and-terminate | terminate

As in 8.1 and later releases:

Specifies the credit control failure handling action.

- **continue**: In the event of a failure the user session continues. DPCA/Diameter will make periodic request and/or connection retry attempts and/or will attempt to communicate with a secondary peer depending on the peer config and session-binding setting.
  - **retry-server-on-event**: This optional keyword enables reconnecting with PCRF server on update and termination requests or re-authorization from server, for failure-handling CONTINUE sessions.



Important This keyword is valid only for **update-request** though it is allowed to configure for all the requests. The **failure-handling** command configuration will throw an error/warning message if it is configured for any request other than the update request.



Important Failure handling action "**continue retry-server-on-event**" will be taken only if failure happens to CCR-U message, not for CCR-I messages.

send-ccrt-on-call-termination: This optional keyword enables to send CCR-T on call termination if the failure action is **continue**.

Important This keyword is valid only for **update-request** though it is allowed to configure for all the requests. The **show configuration errors** command will throw an error/warning message if it is configured for any request other than the update request.

- **retry-and-terminate**: In the event of a failure the user session continues for the duration of one retry attempt with the server. If this retry attempt also fails, the session is terminated.
- **terminate**: In the event of a failure the user session is terminated.

ccfh { continue | retry-and-terminate | terminate }

As in 8.0 release:

Specifies the credit control failure handling (CCFH) action with or without credit control request type.

- **continue**: In the event of a failure the user session continues. DPCA/Diameter will make periodic request and/or connection retry attempts and/or will attempt to communicate with a secondary peer depending on the peer config and session-binding setting.
- **retry-and-terminate**: In the event of a failure the user session continues for the duration of one retry attempt with the server. If this retry attempt also fails, the session is terminated.
- **terminate**: In the event of a failure the user session is terminated.

cc-request-type

As in 8.0 release:

This optional keyword defines the type of credit control request with failure result code and credit control failure handling action for a session.

- **any-request**: Specifies the request type as any request for a new session.
- **initial-request**: Specifies the request type as initial request for a new session.
- **terminate-request**: Specifies the request type as terminate request for a session.
- **update-request**: Specifies the request type as update request for an active session.

Usage Guidelines

Use this command to configure the Diameter Policy Control Application (DPCA) failure handling behavior.

When an unknown rulebase comes in CCA, changing of rulebase and failure handling is managed in the following manner:

- If the new and existing rulebases have the same CCA policy, then switch to the new rulebase is successful.
- If the new rulebase is valid and has CCA-enabled, in CCA-Initial/Update request, switch to the new rulebase is successful.

- If the new rulebase is valid and does NOT have CCA enabled, whereas the existing rulebase has credit enabled, or vice versa, in CCA-Initial/Update request:
  - CCFH-Continue: Goes offline immediately after sending the CCR-T with termination cause as BAD_ANSWER.
  - CCFH-RETRY and TERMINATE: Goes offline immediately after sending the CCR-T with termination cause as BAD_ANSWER.
  - CCFH-TERMINATE: Goes offline immediately after sending the CCR-T with termination cause as BAD_ANSWER.
- If the new rulebase is invalid, in CCA-Initial/Update request:
  - CCFH-Continue: Goes offline immediately after sending the CCR-T with termination cause as BAD_ANSWER.
  - CCFH-RETRY and TERMINATE: Terminates on successful CCA-T, or terminates after successful/failed retry to secondary.
  - CCFH-TERMINATE: Terminates on successful/failed CCR-T to Primary.

The default failure handling behavior is:

failure-handling diameter-result-code any-error ccfh terminate

In StarOS release 14.1 and earlier, when an IP CAN session is up, if any CCR-U message delivery fails due to timeout or TCP link failure, the failure-handling action "**continue**" will be taken for the session and there will not be any further interaction with PCRF and RAR from PCRF is also not accepted (result code 5002 is sent in RAA). If the CCR-U that is triggered for reporting Usage-Monitoring-Information AVP fails, then the usage information is lost.

In 15.0 and later releases, after the IP-CAN session is up, if CCR-U message delivery fails due to timeout or TCP link failure, the failure-handling action "**continue retry-server-on-event**" will be taken at PCEF. Any request coming from session manager will be forwarded to PCRF, and if message delivery again fails session manager will be notified with status "SN_STATUS_NO_ACTIONS_TAKEN".

If CCR-U for reporting Usage-Monitoring-Information fails, then the unreported usage information is given back to ECS and the usage information is stored at ECS. Usage will be reported in CCR-T or in the next CCR-U (if CLI "**event-update send-usage-report**" is configured). Also, RAR message from PCRF will be processed and responded with result-code success in RAA.



Important Unreported usage will be lost, if CCR-U message delivery fails for last rule removal or usage reporting for monitoring stop indication from PCRF. Also, note that preserving unreported usage monitoring information is currently not supported for dpca-custom9 dictionary.

Example

The following command sets the DPCA failure handling to **retry-and-terminate** and return a result code of *3456* for credit control request type **initial-request**:

As in 8.0 release:

failure-handling diameter-result-code *3456* **ccfh retry-and-terminate cc-request-type initial-request**

As in 8.1 and later releases:

failure-handling cc-request-type initial-request diameter-result-code *3456* **retry-and-terminate**

li-secret

Refer to the *Cisco ASR 5000 Lawful Intercept Configuration Guide* for a description of this command.

max-outstanding-ccr-u

This command enables or disables the gateway to send multiple back-to-back CCR-Us to PCRF.

Product

GGSN

HA

PDSN

P-GW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-imsa-dpca)#`

Syntax Description

[default] max-outstanding-ccr-u *value*

default

This keyword sets the default value as 1 for the maximum number of outstanding CCR-U messages to be sent to PCRF.

value

This keyword configures a value for the maximum number of outstanding CCR-U messages to be sent to PCRF.

value must be an integer value from 1 through 12.

Usage Guidelines

This command enables the gateway to send multiple outstanding CCR-Us per session to PCRF.

In releases prior to 17.0, ASR5K node supports only one pending CCR-U message per session over Gx interface. Any request to trigger CCR-U (for access side updates/internal updates) were ignored/dropped, when there was already an outstanding message pending at the node. PCEF and PCRF were out of synch if CCR-U for critical update (like RAT change/ULI change) was dropped.

In 17.1 and later releases, this CLI command "**max-outstanding-ccr-u**" under IMS Authorization Service configuration mode allows multiple CCR-Us towards PCRF. That is, this CLI will allow the user to configure a value of up to 12 as the maximum number of CCR-U messages per session.

The CLI-based implementation allows sending request messages as and when they are triggered and processing the response when they are received. The gateway does re-ordering if the response messages are received out of sequence.

Example

The following command configures the maximum number of outstanding CCR-U messages as 2.

```
max-outstanding-ccr-u 2
```

subscription-id service-type

This command enables required subscription-id types for various services. The Subscription-ID AVP will be encoded based on the configured subscription-ID type.

Product

GGSN

HA

IPSG

PDSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > **context** *context_name* > **ims-auth-service** *service_name* > **policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
subscription-id service-type { closed_rp | ggsn | ha | ipsg | l2tplns |
mipv6ha | pdsn | pgw | samog-epdg } { e164 | imsi | nai } + |
lsm-emergency-imei-instead-of-uimsi
{ default | no } subscription-id service-type { closed_rp | ggsn | ha |
ipsg | l2tplns | mipv6ha | pdsn | pgw | samog-epdg }
```

default | no

Configures this command with the default setting.

The default behavior is that Subscription-ID AVP will be encoded based on service-type and Diameter dictionary.

{ closed_rp | ggsn | ha | ipsg | l2tplns | mipv6ha | pdsn | pgw | samog-epdg }{ e164 | imsi | nai }

Controls the encoding of Subscription-ID AVP based on the following service-types associated with services such as GGSN, HA, IPSG, PDSN, SaMOG, ePDG,etc.

- E164
- IMSI
- NAI
- lsm-emergency-imei-instead-of-uimsi

In Release 21, **samog-epdg** service type is added to allow encoding of Subscription-ID with a combination of MSISDN, NAI or IMSI in CCR for SaMOG (S2a) or ePDG (S2b) service for WLAN access types (trusted and untrusted 3GPP access types). This keyword is supported to send the Subscription-ID AVP with MSISDN in CCR-I or CCR-U towards PCRF. For more information on the functionality, see the *Gx Interface Support* chapter in the administration guide of the product you are deploying.

+

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

Usage Guidelines

In releases prior to 15.0, Subscription-ID AVP is encoded based on service-type and Diameter dictionary.

In 15.0 and later releases, when IMS Authorization service encodes the Subscription-ID AVP, IMSA will first check whether or not this CLI command **subscription-id service-type** is configured. If the CLI is configured for the current service, then IMSA will encode the Subscription-ID AVP based on the configured subscription-ID type. This CLI command takes more precedence than the default behavior.

If the CLI configuration does not encode any Subscription-ID AVP, then IMSA will encode this AVP based on the default behavior. For example, in GGSN/IPSG service, NAI support is not available. If this CLI command is configured for GGSN/IPSG service with NAI type, then based on CLI IMSA cannot encode any Subscription-ID AVP. By this time default behavior (old behavior based on service-type and dictionary) will add the subscription-ID.

Example

The following command enables encoding of the Subscription-ID AVP based on IMSI parameter for GGSN service:

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