

Overload Control

Ericsson Service-Aware Policy Controller

FACILITY DESCRIPTION

Copyright

© Ericsson España, S.A. 2017. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.

Abstract

This document provides a description of Overload Control function provided by the SAPC.



Contents

1	Overload Control Function	1
1.1	Load Regulation Mechanism	1
1.2	Massive Reauthorizations Mechanisms	2





1 Overload Control Function

The SAPC provides different mechanisms to control overload situations.

1.1 Load Regulation Mechanism

The SAPC detects that it is working in overload situation when any of the traffic processors is working at CPU load or memory load higher than a configured value.

In overload situation, the SAPC prioritizes the events handled with higher priority and rejects or discards events handled with lower priority.

The SAPC applies the following priority to the following events, in order from highest to lowest priority:

Table 1 Regulated Events

Event	Action performed when the SAPC is overloaded and event is not allowed
Gx/Rx session termination	The SAPC rejects the incoming Diameter messages to reduce its load answering with DIAMETER_TOO_BUSY.
Rx session modification for IMS emergency calls Gx session modification for emergency bearer services	The SAPC rejects the incoming Diameter messages to reduce its load answering with DIAMETER_TOO_BUSY.
Rx session establishment for IMS emergency calls	The SAPC rejects the incoming Diameter messages to reduce its load answering with DIAMETER_TOO_BUSY.
Gx session establishment for emergency bearer services	The SAPC rejects the incoming Diameter messages to reduce its load answering with DIAMETER_TOO_BUSY.
Gx/Rx session modification (non-emergency) Sy/ESy spending status notification request ⁽¹⁾ Incoming SOAP notification due to the subscriber profile update in external database deployments Gx session reauthorization due to Time Trigger function	<p>The SAPC rejects the incoming Diameter messages to reduce its load answering with DIAMETER_TOO_BUSY.</p> <p>The SAPC rejects the incoming SOAP notification messages to reduce its load answering with an HTTP Server Error.</p> <p>The SAPC discards the session reauthorization initiated by the SAPC due to Time Trigger function to reduce its load.</p>



Event	Action performed when the SAPC is overloaded and event is not allowed
Rx session establishment (non-emergency)	The SAPC rejects the incoming Diameter messages to reduce its load answering with DIAMETER_TOO_BUSY.
Gx session establishment (non-emergency) Smp session establishment ⁽²⁾	The SAPC rejects the incoming Diameter messages to reduce its load answering with DIAMETER_TOO_BUSY.
Provisioning REST API Request	The SAPC rejects the incoming REST API messages to reduce its load answering with an HTTP Service Unavailable Error.

(1) Sy/ESy session establishments are not explicitly regulated. If Gx session establishment is allowed, Sy/ESy session establishment is also allowed.

(2) Smp session modifications and terminations are not regulated.

When the SAPC is overloaded during the session inactivity cleanup process, the SAPC executes the session inactivity cleanup with low priority.

When the SAPC is overloaded and detects a PCEF or an AF restart, the SAPC executes massive clean up with low priority.

The SAPC provides a mechanism to avoid load peaks and signalling storm due to the massive cleanup or session inactivity cleanup, so incoming messages are not affected.

1.2 Massive Reauthorizations Mechanisms

The SAPC implements following Massive Reauthorization Congestion Control mechanisms to prevent an overload situation in the system that could degrade the SAPC performance.

— Disable Massive Reauthorizations Based on Subscriber Update

The sending of reauthorization messages to the enforcement function when massive changes on subscriber data are performed, can be disabled with a configured value to prevent network traffic overload.

— Disable Massive Reauthorizations Associated to Time Conditions

The SAPC policies can evaluate conditions based on date and time, so, the result is only applicable during a period. When the applicable period is reached or expired, the SAPC then triggers a particular action (refer to [Subscription and Policy Management](#)). The following mechanisms avoid congestion in the node because of a massive processing of reauthorizations owing to validity time expiration.

- Limit the maximum number of reauthorization due to Time of Day conditions that can be triggered per second.



This limit value is configured by Ericsson personnel (default value is 700) and depends on network traffic model and the SAPC capacity. For example, if a time condition that applies to 210.000 sessions is set to 12:00 and reauthorization throughput is set by default, the SAPC processes the reauthorizations from 12:00 to 12:05.

If the number of reauthorization messages to send is higher than this maximum number, the SAPC sends the additional messages at the next second that it is possible.

- Disable the sending of reauthorization messages associated to time conditions if network traffic overload is too high.

In this case, the new data is sent to the enforcement function when any message request is received from it.

— Disable Reauthorizations due to Session Inactivity Cleanup Mechanism

The sending of reauthorization messages to verify if the Gx session is still alive in the PCEF can be disabled with a configured value to prevent network traffic overload.

— Disperse Reauthorizations due to Fair Usage Reset on Specific Dates

If fair usage feature is active and it is configured reset on specific dates for postpaid subscriber groups, it is recommended not to specify the exact time in the configured period to avoid congestion situations. If not specified the SAPC calculates the expiration date for every subscriber of the subscriber group adding a random number of seconds (dispersion). In this way, it is avoided a massive reauthorization messages and the corresponding massive reception of IP session update messages at the same second for all the subscribers belonging to the same subscriber group.

The dispersion applied for every subscriber is a random number from 0 to the number of seconds of the period not specified:

- If hour is not specified: 23 hours, 59 minutes, and 59 seconds.
- If minute is not specified: 59 minutes and 59 seconds.
- If second is not specified: 59 seconds.