



Cisco ASR 5000 Series Mobile Service Edge Gateway - 3G Administration Guide

Version 12.2

Last Updated October 17, 2011

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-25592-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco ASR 5000 Series Mobile Service Edge Gateway - 3G Administration Guide

© 2011 Cisco Systems, Inc. and/or its affiliated entities. All rights reserved.

CONTENTS

About this Guide	V
Conventions Used.....	vi
Contacting Customer Support	vii
Mobile Service Edge Gateway-3G Overview	9
Product Overview.....	10
License Information.....	10
Network Deployment and Supported Interfaces.....	11
Supported Interfaces	11
Ga Interface.....	11
Gi Interface	12
Gn/Gp Interface	12
Features and Functionality.....	12
Traffic Offload.....	12
GTP Proxy Mode	13
Paging	13
Echo Processing/Path Failure.....	13
Restart Counter Handling	13
Session Recovery	14
Architecture	15
MSEG Manager	15
Session Manager.....	15
Charging	15
How it Works	16
PDP Context Activation	17
PDP Context Deactivation	19
GGSN-initiated PDP Context Deactivation	19
UE/SGSN-initiated PDP Context Deactivation	20
Update PDP Context.....	21
GGSN-initiated Update PDP Context.....	21
SGSN-initiated Update PDP Context	22
Configuration Overview	24
MSEG-3G Service Configuration.....	24
Mobile Service Edge Gateway-3G Configuration	25
Prerequisites and Initial Configuration.....	26
Installing the MSEG-3G License.....	26
Configuring MSEG-3G Service	27
Creating and Configuring the MSEG-3G Service	27
Configuring MSEG Global Parameters	28
Creating and Configuring MSEG APN Profiles	28
Creating and Configuring MSEG Associated Services Profiles	28
Creating and Configuring MSEG Criteria	29
Creating and Configuring MSEG IMEI Profiles	29
Creating and Configuring MSEG IMSI Profiles.....	30
Creating and Configuring MSEG Peer Profiles.....	30
Creating and Configuring MSEG RNC Profiles	30
Creating and Configuring MSEG Rulesets	31

Creating and Configuring Active-Charging Service Rulebases 31

Creating and Configuring Firewall-and-NAT Policies..... 31

Gathering MSEG-3G Statistics 32

Verifying and Saving Your Configuration 33

 Verifying the Configuration 34

 Feature Configuration..... 34

 Service Configuration..... 35

 Context Configuration 35

 System Configuration..... 36

 Finding Configuration Errors 36

 Saving the Configuration 37

 Saving the Configuration on the Chassis 38





Mobile Service Edge Gateway-3G Sample Configuration 41

About this Guide

This document pertains to the features and functionality that run on and/or that are related to the Cisco® ASR 5000 Chassis, formerly the Starent Networks ST40.

Conventions Used

The following tables describe the conventions used throughout this documentation.

Icon	Notice Type	Description
	Information Note	Provides information about important features or instructions.
	Caution	Alerts you of potential damage to a program, device, or system.
	Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.
	Electro-Static Discharge (ESD)	Alerts you to take proper grounding precautions before handling a product.

Typeface Conventions	Description
Text represented as a <i>screen display</i>	This typeface represents displays that appear on your terminal screen, for example: Login:
Text represented as commands	This typeface represents commands that you enter, for example: show ip access-list This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a command variable	This typeface represents a variable that is part of a command, for example: show card slot_number slot_number is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the File menu, then click New

Command Syntax Conventions	Description
{ keyword or <i>variable</i> }	Required keywords and variables are surrounded by grouped brackets. Required keywords and variables are those components that are required to be entered as part of the command syntax.
[keyword or <i>variable</i>]	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by square brackets.
	With some commands there may be a group of variables from which the user chooses one. These are called alternative variables and are documented by separating each variable with a vertical bar (also known as a pipe filter). Pipe filters can be used in conjunction with required or optional keywords or variables. For example: { nonce timestamp } OR [count <i>number_of_packets</i> size <i>number_of_bytes</i>]

Contacting Customer Support

Use the information in this section to contact customer support.

For New Customers: Refer to the support area of <http://www.cisco.com> for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

For Existing Customers with support contracts through Starent Networks: Refer to the support area of <https://support.starentnetworks.com/> for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.



Important: For warranty and repair information, please be sure to include the Return Material Authorization (RMA) tracking number on the outside of the package.

Chapter 1

Mobile Service Edge Gateway-3G Overview

This chapter provides an overview of the Cisco Mobile Service Edge Gateway-3G (MSEG-3G) service.

This chapter covers the following topics:

- [Product Overview](#)
- [Network Deployment and Supported Interfaces](#)
- [Architecture](#)
- [How it Works](#)

Product Overview



Important: In this release, the Cisco MSEG-3G solution is only available for Universal Mobile Telecommunications System (UMTS) wireless data networks.

The Cisco MSEG-3G solution provides GTP Proxy functionality with the option to offload Internet-based traffic, and provides the ability to police inbound roamer user traffic. This enables mobile network operators lower the cost of mobile data traffic, maintain quality service experience, and offer new applications.

The MSEG-3G provides service intelligence at the edge of the network to direct Internet-bound traffic at the edge of the network while retaining the control plane in the network core, enabling mobile operators to:

- Route low-value Internet-bound traffic straight to the Internet.
- Route high-priority or low-latency traffic without going deep into the packet core.
- Keep local traffic localized.
- Provide intelligent roaming options and secure connections to Mobile Virtual Network Operators (MVNOs).
- Create an architecture to enable new services and business models.

License Information

The MSEG-3G is a licensed product. To enable and configure MSEG-3G functionality, one of the following licenses must be obtained and installed on the chassis:

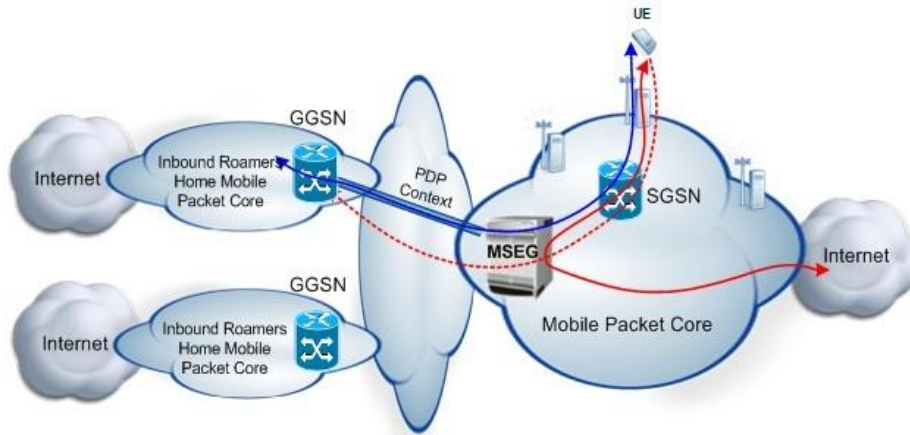
- Cisco PID [ASR5K-00-MSEG310] *MSEG 3G 10k Sessions*
- Cisco PID [ASR5K-00-MSEG301] *MSEG 3G 1k Sessions*

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

Network Deployment and Supported Interfaces

This section provides an overview of the network deployment and interfaces supported by MSEG-3G. The following illustration depicts MSEG-3G deployment in a mobile operator's network.

Figure 1. MSEG-3G Network Deployment



In the network the MSEG-3G is physically located on the Gn interface between the SGSN and the GGSN.

Important: All Iu for the same service area must be served by the same MSEG-3G.

Supported Interfaces

This section provides an overview of the interfaces supported by the MSEG-3G.

Ga Interface

When CDR generation is enabled, the MSEG-3G uses the Ga interface to communicate with the Charging Gateway (CG). The CG is responsible for sending GGSN Charging Data Records (G-CDRs) received from the GGSN, for each PDP context, to the billing system.

The MSEG-3G communicates with the CGs on the PLMN using GTP Prime (GTPP).

Important: When MSEG-3G CDR generation is enabled, in addition to the charging records generated by the GGSN, an additional charging record is generated. Operators must be aware of the issue of reconciliation of charging records that are generated by the MSEG-3G instead of/in addition to the GGSN.

Important: CDR generation at the MSEG-3G can be optionally enabled or disabled in the MSEG-3G Service configuration.

Gi Interface

The Gi interface plays the same role as on the GGSN, which is to serve as an exit/entry point to the public network. The primary difference is that if the anchor-proxy mode has not been enabled, and Network Address Translation (NAT) in-line service configuration is available, the IP packets exiting/entering the MSEG-3G on this interface will contain a locally-allocated NAT IP address instead of the GGSN-allocated subscriber IP address as the source/destination.

Gn/Gp Interface

The MSEG-3G supports the Gn interface control and data planes between the SGSN and the GGSN. All PDP establishments pass through the MSEG-3G so that a decision on whether the PDPs are of interest for offloading, either immediately or on meeting the offloading criteria later, can be made.

The initial criterion for offloading is the APN. That is, the MSEG-3G will track only those PDPs that either require offloading or may require offloading later. This initial eligibility decision is made on the basis of the APN/IMSI/IMEI. For Create PDP Context that meet the offloading criteria, the MSEG-3G will substitute the SGSN's IP address and TEID with a local IP address and TEID, before forwarding to the GGSN. On receiving the corresponding Create PDP Context Response, the MSEG-3G will swap the GGSN's IP address and TEID with a local IP address and TEID before forwarding to the SGSN. Thus, for these PDPs, the MSEG-3G will look like the SGSN to the GGSN and, the GGSN to the SGSN. All subsequent control and data plane events will now flow through the MSEG-3G, which will handle them in accordance with the call flows detailed later in this chapter.

The MSEG-3G also uses the Gn interface to selectively send downlink packets, for off-loaded PDPs, to the SGSN in order to either execute paging or to prevent inactivity timers from firing.

Features and Functionality

This section describes the MSEG-3G's base features.

Traffic Offload

The MSEG-3G depends on the SGSN to provide information on subscriber GTP endpoint identifiers (IP address/TEID) and mobility events. The MSEG-3G is not required to sniff the IuPS interface for control-plane events. For traffic to be offloaded, the NAT in-line service configuration must be available on the chassis. If not available the traffic is proxied to the GGSN.



Important: In this mode of operation, the APN resolution at the SGSN should point to an MSEG-3G.

GTP Proxy Mode

The GTP Proxy primary functionality is to provide the ability to apply policy enforcement to MVNO end-subscribers. This enables to offer a wider feature set to MVNO operators and to offer better conditions to MVNO by doing traffic enforcement on the GTP Proxy.

In the absence of NAT in-line service configuration, for all offloaded calls, by default the MSEG-3G behaves as a proxy.

The GTP Proxy functionality provides a point-of-intercept for operators to provide additional functionality on the data plane for MVNO and roaming scenarios, such as:

- Enforce local policies
- Provide analytics
- Provide local intercept
- Local charging
- Value added differentiated services

In this default proxy mode, all user packets are forwarded to/from over GTPU tunnels between the GGSN and the MSEG-3G for offloaded calls. This default data-plane proxy functionality for offloaded calls can be over-ridden by local configuration or policy application to provide data offload services using the NAT in-line service.

Paging

As data should not be sent directly to the RNC by the MSEG-3G when there is no established RAB for a PDP, the MSEG-3G needs to track the availability of a data connection to the RNC for the PDP.

When an RAB is not available and downlink data is incident at the MSEG, the data needs to be routed through the SGSN until the RAB has been established, after paging the UE if necessary.

This is taken care of by the SGSN by switching between single-tunnel and two-tunnel modes, depending on whether the PDP is active or has been preserved. MSEG-3G will simply forward any downlink data to the specified endpoint.

Echo Processing/Path Failure


The MSEG-3G supports selective enabling of the echo procedure towards each SGSN/GGSN/RNC it is connected to.

On an echo failure towards any of the peer nodes, the MSEG-3G will initiate PDP release procedures for all related PDPs. For example, if a GGSN has failed to respond to an echo on a given path, the MSEG-3G will request the release of all the PDPs corresponding to the path from the corresponding SGSNs.

Restart Counter Handling

If the restart counter value for an SGSN changes, the MSEG-3G will request deactivation of all PDP contexts, currently established via that SGSN, to the corresponding GGSNs.

If the restart counter value for a GGSN changes, the MSEG-3G will request deactivation of all PDP contexts, currently anchored at that GGSN, to the corresponding SGSNs.

 **Important:** In the current release, the MSEG-3G cannot cause the SGSN to request the corresponding UEs to activate after deactivation. It is possible to define a proprietary mechanism to do this, however it will require corresponding changes at the SGSN.

Session Recovery

The Session Recovery feature provides seamless failover and reconstruction of subscriber session information in the event of a hardware or software fault within the system preventing a fully connected user session from being disconnected.

Session recovery is performed by mirroring key software processes (for example, Session Manager and AAA Manager) within the system. These mirrored processes remain in an idle state (in standby-mode), wherein they perform no processing, until they may be needed in the case of a software failure (for example, a Session Manager task aborts). The system spawns new instances of “standby mode” session and AAA Managers for each active Control Processor (CP) being used.

Additionally, other key system-level software tasks, such as VPN Manager, are performed on a physically separate packet processing card to ensure that a double software fault (for example, Session Manager and VPN Manager fails at same time on same card) cannot occur. The packet processing card used to host the VPN Manager process is in active mode and is reserved by the operating system for this sole use when session recovery is enabled.

For more information on Session Recovery, refer to the *Session Recovery* chapter in the *System Administration Guide*.

Architecture

This section presents an overview of the MSEG-3G's architecture.

On the ASR 5000 chassis, the MSEG Manager and Session Manager subsystems are the key.

MSEG Manager

The MSEG Manager's (MSEGMgr) primary role is that of the Demux Manager for the MSEG-3G service, and is resident on the demux card, when available. There is a single MSEGMgr for the entire chassis, which handles all the MSEG-3G services configured in the chassis, irrespective of the context.

The MSEGMgr is the first point of entry for new PDP contexts. If the PDP matches one of the top-level off-loading criteria (APN/IMSI/IMEI), the MSEGMgr will load balance new PDP requests to a SessMgr. The MSEGMgr also handles all nodal GTPC messages for all the MSEG-3G services that are servicing UMTS networks. The MSEGMgr will install GTPC flows corresponding to the GTPC addresses specified for each of these services for the TEID-C value of 0. All GTPC/GTPU messages that cannot be matched to a session in the SessMgr will be directed to the MSEGMgr. That is, the MSEGMgr will be the default handler for such messages.

All flows installed by the MSEGMgr will need to be from the range specified for the MSEGMgr in the NPU subsystem.

Session Manager

The Session Managers (SessMgrs) handle all the subscriber sessions that meet the top-level MSEG-3G criterion. Calls will be load-balanced to the SessMgrs by the MSEGMgr using the standard add-session messaging functionality.

Each primary PDP context is considered to be a separate call, even if from the same subscriber. A callline will be allocated per primary PDP. A primary and the associated secondary's will be anchored by the same callline.

The credit allocation for a callline for the MSEG-3G service will be identical to that of the GGSN with NAT enabled. NAT of subscriber data sessions will be carried out at the SessMgrs.

The MSEG-3G uses a common GTP service flow (per service-ip-address per SessMgr) for all subscribers connecting via a given MSEG-3G service instance. Downlink data packets received from the GGSN will be forwarded to the RNC serving the subscriber. If the default GTP Proxy mode is overridden by configuration, the downlink data packets received on the public network will first pass through the NAT in-line service module before being sent to the MSEG-3G module. Uplink data packets will be either forwarded out to the public network via the NAT module, or sent to the GGSN if the packet does not match the NAT rules or if NAT configuration is not available.

Charging

The charging subsystem is responsible for collecting the charging information such as usage of radio and core network resources, the duration of time, uplink and downlink transfer rates and transferring the generated CDRs in ASN.1 format to the desired billing system. Based on the information provided, the billing system generates billing for the mobile subscriber according to predefined policies.

How it Works

This section describes how the MSEG-3G works.

When a new Create PDP Context Request reaches the MSEGMgr, it applies the “MSEG Criteria” configured for that service. If there is no criteria configured, the MSEGMgr will default to forwarding the Create PDP Context Request to the appropriate GGSN, after resolving the APN.

An “MSEG Criteria” configuration consists of the filters to match, that is a ruleset, their relative priorities, and the action to be taken on a match. The MSEG-3G can be configured to offload, terminate on a local GGSN, or forward the call without offloading at the MSEG-3G. This is decided at the MSEGMgr based on the first-level filters. Calls are anchored at the SessMgrs only if the MSEG-3G decided to offload the calls. Note that offloading a call does not necessarily mean all the data will also be offloaded. At this stage only the control plane offloading decision is made. The data plane maybe offloaded or not depending on the application of the second-level filters, which will include end-user application specific DPI and policy-based decisions.

PDP Context Activation

The following figure and steps explain the call flow for a successful PDP Context Activation.

Figure 2. MSEG-3G PDP Context Activation Call Flow

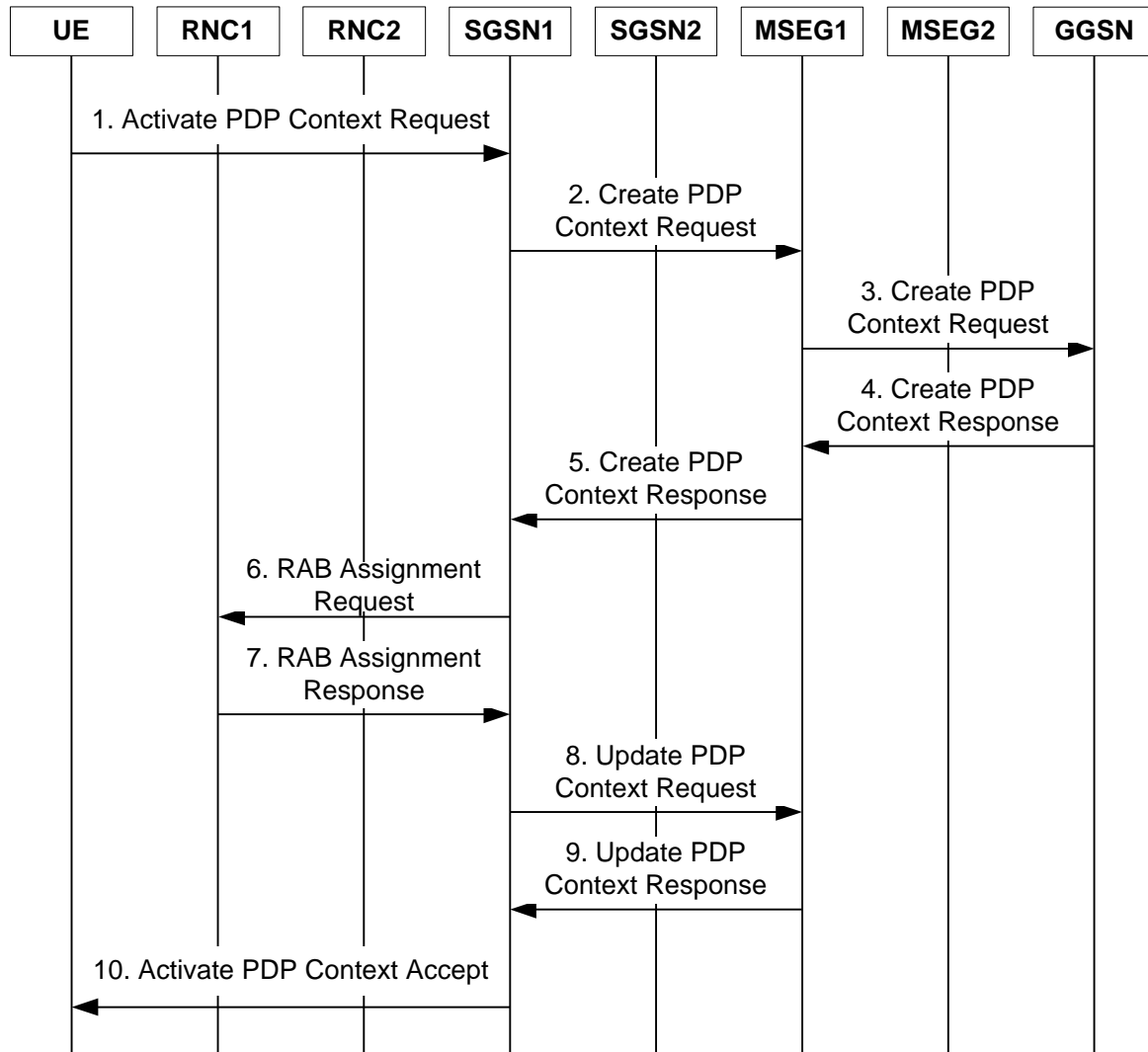


Table 1. MSEG-3G PDP Context Activation Call Flow Descriptions

Step	Description
1	The UE generates an Activate PDP Context Request. In the default mode, neither is this message available nor is it of interest to the MSEG-3G.

Step	Description
2	<i>SGSN</i> resolves the APN to <i>MSEG1</i> and sends the Create PDP Context Request with its TEIDs (C & U) and IP addresses (C & U) to be used by the GGSN as the destination identifiers in all subsequent messages for this PDP.
3	<p><i>MSEG1</i> breaks open the Create PDP Context Request to obtain the APN, the ULI and, RAT IEs. It uses the APN to resolve the real target GGSN(s). Further local processing, at <i>MSEG1</i>, is not proceeded with if:</p> <ol style="list-style-type: none"> 1. If the message is not a GTPv1 message, it is forwarded as is to the resolved GGSN. 2. The initial offload criteria—APN/IMSI/IMEI—are not met, <i>MSEG1</i> forwards the Create PDP Context Request as is to the resolved GGSN. 3. The ULI or the RAT IE is not included in the Create PDP Context Request and GTP Proxy mode has not been enabled for the APN and IMSI, <i>MSEG1</i> forwards the Create PDP Context Request as is to the resolved GGSN. 4. The RAT IE does not indicate UMTS access and GTP Proxy mode has not been enabled for the APN and IMSI, <i>MSEG1</i> forwards the Create PDP Context Request as is to the resolved GGSN. 5. The service-area-id in the ULI does not correspond to one of the RNCs that <i>MSEG1</i> is intercepting, <i>MSEG1</i> looks up the correct MSEG-3G — <i>MSEG2</i>— and forwards to that MSEG-3G for further processing. <p>If an initial offload criteria is met, <i>MSEG1</i> formulates a Create PDP Context Request with its TEIDs (C & U), IP addresses (C & U) and, recovery IE (if necessary), and sends the request to the resolved GGSN.</p>
4	The Create PDP Context Response received by <i>MSEG1</i> is first processed to check the status of the request. If the status indicates failure, <i>MSEG1</i> sends back a corresponding failure to the SGSN and subsequently releases any resources allocated for the Create PDP Context Request.
5	If the Create PDP Context Response indicates success, <i>MSEG1</i> returns a success to the SGSN with the GGSN's addresses and TEIDs replaced with the MSEG's addresses and TEIDs.
6	On a successful Create PDP Context setup, the SGSN seeks an RAB assignment for the PDP context. The RAB assignment is of no interest to the MSEG-3G.
7	After allocation of radio resources, the RNC sends out successful RAB assignment response.
8	By default, direct-tunnel is enabled at the SGSN. This will cause the SGSN to send an Update PDP Context Request to the GGSN (<i>MSEG1</i>). This request will be terminated at <i>MSEG1</i> and is not forwarded to the GGSN. <i>MSEG1</i> will note the GTP-U IP address and TEID being used for the data-session. For the proxy-anchored calls, this Update PDP Context is optional.
9	<i>MSEG1</i> responds to the Update PDP Context Request with a success cause.
10	The SGSN sends a PDP Context Activation Accept to the UE.

PDP Context Deactivation

This section presents call flows for the following scenarios:

- [GGSN-initiated PDP Context Deactivation](#)
- [UESGSN-initiated PDP Context Deactivation](#)

GGSN-initiated PDP Context Deactivation

The following figure and steps explain the call flow for a GGSN-initiated PDP Context Deactivation.

Figure 3. MSEG-3G GGSN-initiated PDP Context Deactivation Call Flow

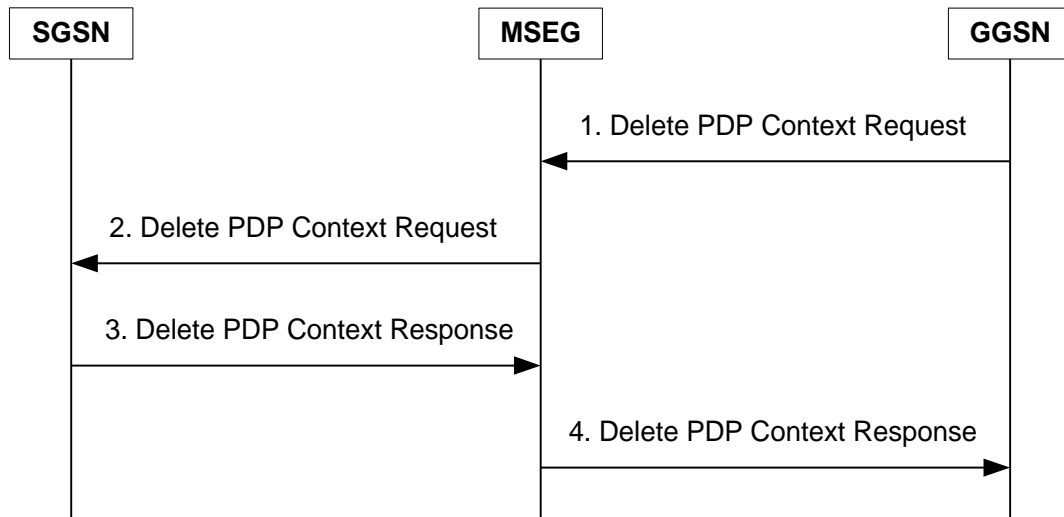


Table 2. MSEG-3G GGSN-initiated PDP Context Deactivation Call Flow Descriptions

Step	Description
1	The GGSN sends a Deactivate PDP Context Request to the SGSN, that is to the MSEG’s IP address/TEID.
2	The MSEG-3G forwards the request to the SGSN after switching the MSEG’s TEID and destination IP address/UDP port in the GTP header to the values provided by the SGSN during Create PDP Context setup.
3	The SGSN deletes the PDP context and sends the Deactivate PDP Context Response to the MSEG.
4	The MSEG-3G forwards the Deactivate PDP Context Response to the GGSN with the SGSN-side TEID and GTP-C endpoint as the target destination identifiers, and releases the session/resources corresponding to the PDP context.

UE/SGSN-initiated PDP Context Deactivation

The following figure and steps explain the call flow for a UE/SGSN-initiated PDP context deactivation. Note that from the MSEG’s perspective, deactivation whether initiated by the SGSN or the UE, is processed identically. Hence, the following call flow displays only the messages that will be visible on the Gn interface.

Figure 4. MSEG-3G UE/SGSN-initiated PDP Context Deactivation Call Flow

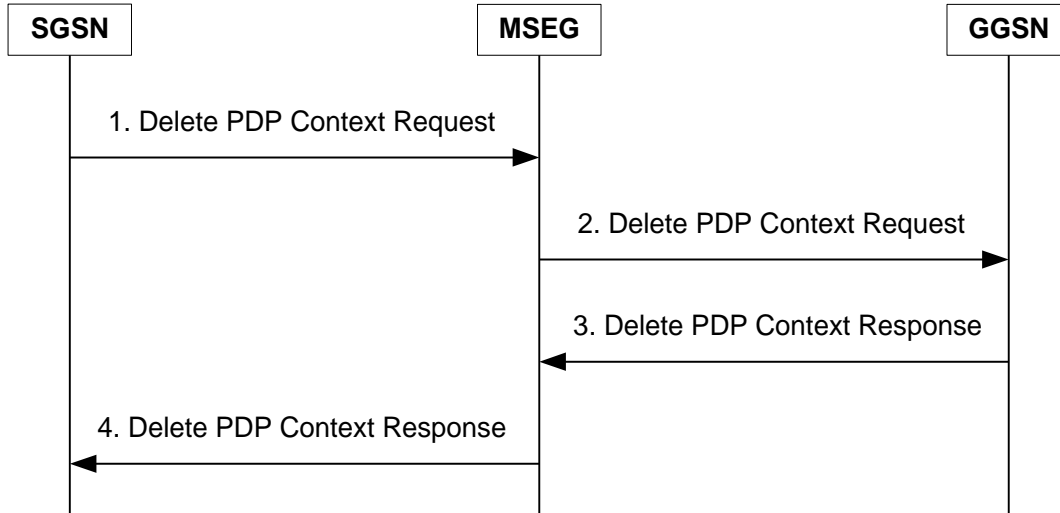


Table 3. MSEG-3G UE/SGSN-initiated PDP Context Deactivation Call Flow Descriptions

Step	Description
1	The SGSN sends a Deactivate PDP Context Request to the GGSN, that is to the MSEG’s GTP-C endpoint IP address/TEID for the PDP.
2	The MSEG-3G forwards the request to the GGSN after switching the MSEG’s TEID and destination IP address/UDP port in the GTP header to the values assigned by the GGSN during Create PDP Context setup.
3	The GGSN deletes the PDP context and sends the Deactivate PDP Context Response to the MSEG.
4	The MSEG-3G forwards the Deactivate PDP Context Response to the SGSN with the SGSN-side TEID and GTP-C endpoint as the target destination identifiers, and releases the session/resources corresponding to the PDP context.

Update PDP Context

This section presents call flows for the following scenarios:

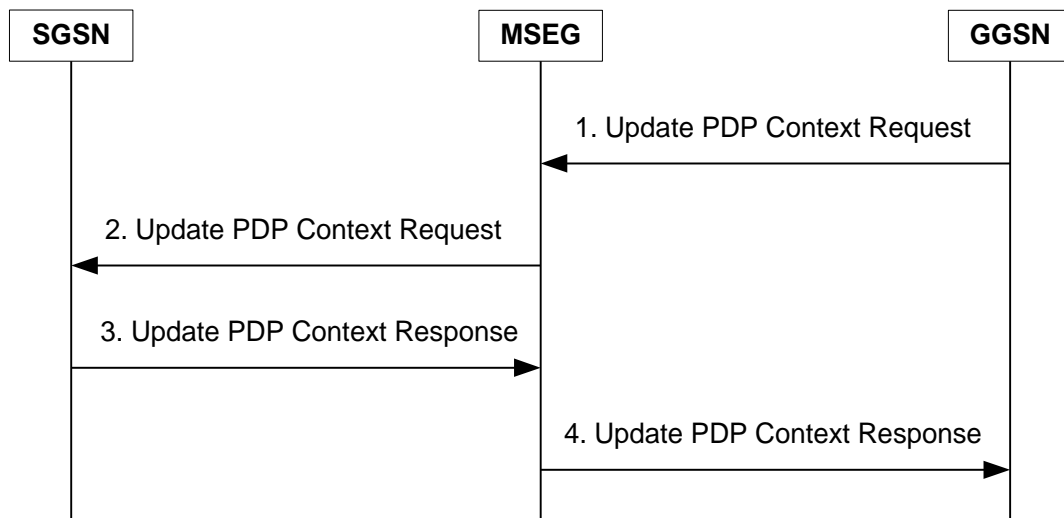
- [GGSN-initiated Update PDP Context](#)
- [SGSN-initiated Update PDP Context](#)

GGSN-initiated Update PDP Context

The GGSN can initiate Update PDP Context Requests either on a change of QoS or to assign an IP address for the subscriber (DHCP/MIP).

The following figure and steps explain the call flow for a GGSN-initiated Update PDP Context.

Figure 5. MSEG-3G GGSN-initiated Update PDP Context Call Flow



The MSEG-3G will process the Update PDP Context Request as has been specified for SGSNs.

Table 4. MSEG-3G GGSN-initiated Update PDP Context Call Flow Descriptions

Step	Description
1	The GGSN sends an Update PDP Context Request to the SGSN, that is to the MSEG’s IP address/TEID for the PDP context.

Step	Description
2	The MSEG-3G processes the Update PDP Context Request to remove/replace the following IEs, before forwarding to the SGSN: <ul style="list-style-type: none"> • Recovery IE will be removed, but can also be replaced by the MSEG’s value as necessary. • QoS modified by the MSEG’s policies, if necessary. • DTI Flags will be removed, if present. As the MSEG-3G is hiding the establishment of DT from the GGSN, this should not occur.
3	The SGSN sends an Update PDP Context Response to the MSEG-3G after processing the request.
4	The MSEG-3G processes the Update PDP Context Response for QoS and any other changes. The MSEG-3G forms and forwards a response to the GGSN with the following contents replaced/filtered out: <ul style="list-style-type: none"> • Recovery IE • Tunnel endpoint identified data IE is replaced to reflect the MSEG-3G allocated value to the GGSN. • DT Flags IE

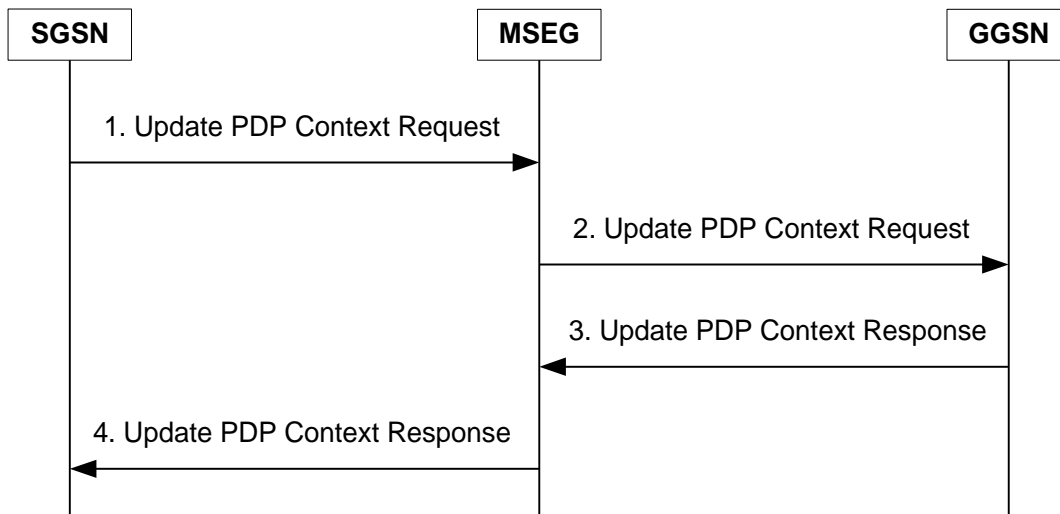
SGSN-initiated Update PDP Context

The SGSN can initiate Update PDP Context requests for the following reasons that are of significance to the MSEG:

- On Inter-SGSN RAU
- On Inter-RAT change
- On Direct-Tunnel change
- All other reasons including QoS change

The following figure and steps explain the call flow for an SGSN-initiated PDP update.

Figure 6. MSEG-3G SGSN-initiated Update PDP Context Call Flow



The MSEG-3G processes the Update PDP Context Request as specified for GGSNs. In addition, the actions taken by the MSEG-3G for specific conditions are described in the following table.

Table 5. MSEG-3G SGSN-initiated Update PDP Context Call Flow Descriptions

Step	Description
1	<p>The SGSN sends an Update PDP Context Request to the GGSN, that is to the MSEG’s IP address/TEID for the PDP context.</p> <ol style="list-style-type: none"> 1. From the SGSN control plane address and/or the service-area-id in the ULI, if included, the MSEG-3G gleans whether this will result in an inter-SGSN move or not. If an inter-MSEG move is called for, the MSEG looks up the new MSEG corresponding to the new RNC (service area ID/RNC IP address) and the call flow proceeds as outlined later in the inter-MSEG Relocation section. 2. If a direct-tunnel related change has occurred, the MSEG will proceed to Step 4. 3. On any other condition, the MSEG will forward the request to the GGSN as outlined in Step 2.
2	<p>The MSEG-3G processes the Update PDP Context Request as specified for GGSNs. If the processing is successful, the MSEG-3G forwards the request to the GGSN with the following elements filtered out/modified:</p> <ul style="list-style-type: none"> • Recovery IE will be removed, but can also be replaced by the MSEG’s value as necessary. • TEIDs (C & U) replaced with the MSEG-allocated values. • SGSN IP addresses/alternative addresses (C & U) replaced with the MSEG’s. • QoS modified by the MSEG’s policies, if necessary. • DTI Flags will be removed, if present. The MSEG-3G can skip to Step 4 if the Update PDP Context Request was solely DT related.
3	<p>The GGSN sends an Update PDP Context Response to the MSEG-3G after processing the request.</p>
4	<p>The MSEG-3G processes the Update PDP Context Response for QoS and any other changes. The MSEG-3G forms and forwards a response to the SGSN with the following contents replaced/filtered out:</p> <ul style="list-style-type: none"> • Recovery IE • GGSN address/alternative address for control and user plane. The MSEG-3G will update the corresponding fields in its records with the values now specified, if any. The MSEG’s TEIDs for the PDP context. If the MSEG-3G has itself changed, as maybe the case for an inter-RNC move, the MSEG-3G will replace the GGSN address/alternative address and TEID’s with its own. Else, this IE will be filtered out. • DT Flags IE

Configuration Overview

MSEG-3G configuration consists of both service instance specific and chassis global configuration. All configuration is expected to be administratively coordinated across the MSEGs deployed in an operator's domain.



Important: For MSEG-3G configuration procedures, refer to the *Mobile Service Edge Gateway-3G Configuration* chapter in the *Mobile Service Edge Gateway-3G Administration Guide*.

MSEG-3G Service Configuration

The MSEG-3G service for UMTS must have access to, at a minimum, the following configuration:

- GTPC address with an optional port configuration
- GTPU addresses with an optional port configuration
- RNC configuration
- APNs
- IMSI Ranges
- IMEI Ranges
- MSEG-3G Identifier

The GTPC/GTPU configuration is service instance specific.

The MSEGs, APNs, IMSI Range, IMEI Range configurations are global so as to be accessible by all MSEG-3G service instances. These global configurations will be associated as required with the individual MSEG-3G service instances from within the service configuration. Various other offload criterion such as QoS are also configured globally.

Chapter 2

Mobile Service Edge Gateway-3G Configuration

This chapter describes how to configure the Mobile Service Edge Gateway-3G (MSEG-3G) functionality.

The following topics are covered in this chapter:

- [Prerequisites and Initial Configuration](#)
- [Configuring MSEG-3G Service](#)
- [Gathering MSEG-3G Statistics](#)

Prerequisites and Initial Configuration

To configure MSEG-3G:

- Step 1** Ensure that the core network service GGSN is configured as described in the *Cisco ASR 5000 Series Gateway GPRS Support Node Administration Guide*.
- Step 2** Ensure that the core network services SGSN is configured as described in the *Cisco ASR 5000 Series Serving GPRS Support Node Administration Guide*.
- Step 3** Ensure that the Active Charging Service is configured.
For more information refer to the *Cisco ASR 5000 Series Enhanced Charging Services Administration Guide*.
- Step 4** Ensure that the Network Address Translation (NAT) in-line service is configured.
For more information refer to the *Cisco ASR 5000 Series Network Address Translation Administration Guide*.
- Step 5** Install the MSEG-3G license as described in the [Installing the MSEG-3G License](#) section.

Installing the MSEG-3G License

To enable and configure MSEG-3G functionality, one of the following licenses must be obtained and installed on the chassis:


- Cisco PID [ASR5K-00-MSEG310] *MSEG 3G 10k Sessions*
- Cisco PID [ASR5K-00-MSEG301] *MSEG 3G 1k Sessions*

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

Configuring MSEG-3G Service

To configure MSEG-3G service:

- Step 1** Create/configure the MSEG service as described in the [Creating and Configuring the MSEG-3G Service](#) section.
- Step 2** Create/configure MSEG global parameters as described in the [Configuring MSEG Global Parameters](#) section.
- Step 3** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

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

Creating and Configuring the MSEG-3G Service

To create and configure the MSEG-3G service, use the following configuration:

configure

```

context <context_name>

  mseg-service <mseg_service_name>

    mseg-id <mseg_id>

    mseg-criteria <mseg_criteria_name>

    path-failure detection-policy gtp { echo | non-echo + }

    gtpc echo-interval <echo_interval>

    gtpc max-retransmissions <max_retransmissions>

    gtpc retransmission-timeout <retransmission_timeout>

    gtpu echo-interval <echo_interval>

    gtpu max-retransmissions <max_retransmissions>

    gtpu retransmission-timeout <retransmission_timeout>

    bind gtpc-address <ipv4/ipv6_address> [ udp-port <port_number> ]

    bind gtpu-address <ipv4/ipv6_address>

    associate accounting-policy <accounting_policy_name>

  end

```

Configuring MSEG Global Parameters

This section describes how to configure the following MSEG global parameters:

- [Creating and Configuring MSEG APN Profiles](#)
- [Creating and Configuring MSEG Associated Services Profiles](#)
- [Creating and Configuring MSEG Criteria](#)
- [Creating and Configuring MSEG IMEI Profiles](#)
- [Creating and Configuring MSEG IMSI Profiles](#)
- [Creating and Configuring MSEG Peer Profiles](#)
- [Creating and Configuring MSEG RNC Profiles](#)
- [Creating and Configuring MSEG Rulesets](#)

Creating and Configuring MSEG APN Profiles

To create / configure an MSEG APN profile, use the following configuration:

```
configure
  mobile-services-edge-gateway
    apn-profile <apn_profile_name>
      apn <apn_name>
    end
```

Creating and Configuring MSEG Associated Services Profiles

To create / configure an MSEG associated services profile, use the following configuration:

```
configure
  mobile-services-edge-gateway
    associated-services-profile <asc_services_profile_name>
      active-charging-rulebase <acs_rulebase_name>
      fw-nat-policy <fw_nat_policy_name>
      ip access-group <access_group_name> in
      ip access-group <access_group_name> out
```

```
ip context-name <context_name>
end
```

Notes:

- For information on how to create and configure an active charging service rulebase, refer to the *Cisco ASR 5000 Series Enhanced Charging Services Administration Guide*.
- For information on how to create and configure a Firewall-and-NAT policy, refer to the *Cisco ASR 5000 Series Network Address Translation Administration Guide*.
- For information on how to create and configure IP access groups or Access Control Lists (ACL), refer to the *Cisco ASR 5000 Series System Administration Guide*.

Creating and Configuring MSEG Criteria

To create / configure an MSEG criteria, use the following configuration:

```
configure
mobile-services-edge-gateway
mseg-criteria <mseg_criteria_name>
    filter priority <priority> ruleset <ruleset_name> action { forward |
local-terminate | offload associated-services-profile
<asc_services_profile_name> }
end
```

Creating and Configuring MSEG IMEI Profiles

To create / configure an MSEG IMEI profile, use the following configuration:

```
configure
mobile-services-edge-gateway
imei-profile <imei_profile_name>
    imei-range start <imei_prefix_range_start> end <imei_prefix_range_end>
[ sv <imei_sw_version> ]
end
```

Creating and Configuring MSEG IMSI Profiles

To create / configure an MSEG IMSI profile, use the following configuration:

```
configure
  mobile-services-edge-gateway
    imsi-profile <imsi_profile_name>
      imsi-range mcc <mobile_country_code> mnc <mobile_network_code> msin
start <msin_start> end <msin_end>
    end
```

Creating and Configuring MSEG Peer Profiles

To create / configure an MSEG peer profile, use the following configuration:

```
configure
  mobile-services-edge-gateway
    peer-mseg-profile <peer_mseg_profile_name>
      mseg-gtpc <ipv4/ipv6_address> [ udp-port <port_number> ]
      mseg-gtpu <ipv4/ipv6_address>
      mseg-id <mseg_id>
    end
```

Creating and Configuring MSEG RNC Profiles

To create / configure an MSEG RNC profile, use the following configuration:

```
configure
  mobile-services-edge-gateway
    rnc-profile <rnc_profile_name>
      associate mseg-profile <mseg_profile_name>
      location mcc <mobile_country_code> mnc <mobile_network_code> lac
<location_area_code> sac <service_area_code>
      rnc-gtpu <ipv4/ipv6_address> [ udp-port <port_number> ]
      rnc-id <rnc_id>
    end
```

Creating and Configuring MSEG Rulesets

To create / configure an MSEG ruleset, use the following configuration:

```
configure
  mobile-services-edge-gateway
    mseg-ruleset <mseg_ruleset_name>
      access-type umts
      apn { if-match-profile <apn_profile_name> | if-no-match-profile
<apn_profile_name> }
      imei { if-match-profile <imei_profile_name> | if-no-match-profile
<imei_profile_name> }
      imsi { if-match-profile <imsi_profile_name> | if-no-match-profile
<imsi_profile_name> }
    end
```

Creating and Configuring Active-Charging Service Rulebases

For information on how to create and configure an active-charging service rulebase, refer to the *Cisco ASR 5000 Series Enhanced Charging Services Administration Guide*.

Creating and Configuring Firewall-and-NAT Policies

For information on how to create and configure a Firewall-and-NAT policy, refer to the *Cisco ASR 5000 Series Network Address Translation Administration Guide*.

Gathering MSEG-3G Statistics

The following table lists the commands that can be used to gather MSEG-related statistics.

In the following table, the first column lists what statistics to gather and the second column lists the command to use.

Table 6. Gathering MSEG Statistics and Information

Statistics/information to view	Command to use:
To view MSEG configuration information.	<code>show mseg-config all [{ grep <grep_options> more }]</code>
To view MSEG service specific configuration information.	<code>show mseg-service { all name <mseg_service_name> } [{ grep <grep_options> more }]</code>
To view GTPC statistics for the specified MSEG service.	<code>show gtpc statistics mseg-service <mseg_service_name>[[verbose] format1] [{ grep <grep_options> more }]</code>
To view GTPU statistics for specified MSEG service.	<code>show gtpu statistics mseg-service <mseg_service_name>[{ grep <grep_options> more }]</code>
To view MSEG-specific subscriber information.	<code>show subscribers mseg-only <filter_keywords>[{ grep <grep_options> more }]</code>
To view MSEG service specific subscriber information.	<code>show subscribers mseg-service <mseg_service_name> <filter_keywords>[{ grep <grep_options> more }]</code>
To view summary information for MSEG subscribers.	<code>show subscribers summary mseg-service <mseg_service_name><filter_keywords> [{ grep <grep_options> more }]</code>

Chapter 3

Verifying and Saving Your Configuration

This chapter describes how to save your system configuration.

Verifying the Configuration

You can use a number of commands to verify the configuration of your feature, service, or system. Many are hierarchical in their implementation and some are specific to portions of, or specific lines in, the configuration file.

Feature Configuration


In many configurations, you have to set and verify specific features. An example includes IP address pool configuration. Using this example, enter the following commands to verify proper feature configuration:

Enter the following command to display the IP address pool configuration:

```
show ip pool
```

The output from this command should look similar to the sample shown below. In this example, all IP pools were configured in the *isp1* context.

```
context : isp1:
+-----Type: (P) - Public (R) - Private
| (S) - Static (E) - Resource
|
|+-----State: (G) - Good (D) - Pending Delete (R)-Resizing
||
| |++--Priority: 0..10 (Highest (0) .. Lowest (10))
| | | |
| | | |+-Busyout: (B) - Busyout configured
| | | | | | | | | | vvvvv Pool Name Start Address Mask/End Address Used Avail
-----
PG00 ipsec 12.12.12.0 255.255.255.0 0 254 PG00
pool1 10.10.0.0 255.255.0.0 0 65534 SG00
vpnpool 192.168.1.250 192.168.1.254 0 5 Total Pool Count: 5
```

 **Important:** To configure features on the system, use the *show* commands specifically for these features. Refer to the *Cisco Systems ASR 5000 Command Line Interface Reference* for more information.

Service Configuration

Verify that your service was created and configured properly by entering the following command:

```
show <service_type> <service_name>
```

The output is a concise listing of the service parameter settings similar to the sample displayed below.

In this example, a P-GW service called *pgw* is configured.

```
Service name : pgw1
Service-Id : 1
Context : test1
Status : STARTED
Restart Counter : 8
EGTP Service : egtpl
LMA Service : Not defined
Session-Delete-Delay Timer : Enabled
Session-Delete-Delay timeout : 10000(msecs)
PLMN ID List : MCC: 100, MNC: 99
Newcall Policy : None
```

Context Configuration

Verify that your context was created and configured properly by entering the following command:

```
show context name <name>
```

The output shows the active context. Its ID is similar to the sample displayed below. In this example, a context named *test1* is configured.

Context Name	ContextID	State
-----	-----	-----
test1	2	Active

System Configuration

Verify that your entire configuration file was created and configured properly by entering the following command:

```
show configuration
```

This command displays the entire configuration including the context and service configurations defined above.

Finding Configuration Errors

Identify errors in your configuration file by entering the following command:

```
show configuration errors
```

This command displays errors it finds within the configuration. For example, if you have created a service named “service1”, but entered it as “srv1” in another part of the configuration, the system displays this error.

You must refine this command to specify particular sections of the configuration. Add the **section** keyword and choose a section from the help menu:

```
show configuration errors section ggsn-service
```

or


```
show configuration errors section aaa-config
```

If the configuration contains no errors, an output similar to the following is displayed:

```
#####
Displaying Global
AAA-configuration errors
#####
Total 0 error(s) in this section !
```

Saving the Configuration

Save system configuration information to a file locally or to a remote node on the network.

 **Caution:** Prior to loading 12.2, we recommend that copies of the original configuration file be made and stored (with unique release-identifying titles) both in the Flash and off the chassis. Configuration files created and saved in release 12.2 cannot be shared across multiple chassis due to a change in the encryption algorithm for passwords and secrets. These 12.2 changes modify encrypted data in the configuration file so that it cannot be recognized by previous software builds. If it is necessary to revert to a previous build, the chassis must be booted with the copy of the original configuration file. If this copy is not available, then the chassis will need to be loaded as if it is a new chassis.

Files saved locally can be stored in the CompactFlash or a PCMCIA memory card on the SMC. Files that are saved to a remote network node can be transmitted through FTP or TFTP.

Saving the Configuration on the Chassis

These instructions assume that you are at the root prompt for the Exec mode:

```
[local]host_name#
```

To save your current configuration, enter the following command:

```
save configuration url [-redundant] [-noconfirm] [showsecrets] [verbose]
```

Table 7. Command Syntax for Saving the Configuration

Keyword/Variable	Description
<i>url</i>	<p>Specifies the path and name to which the configuration file is to be stored. <i>url</i> may refer to a local or a remote file. <i>url</i> must be entered using one of the following formats:</p> <ul style="list-style-type: none"> <code>{ /flash /pcmcia1 /pcmcia2 } [/dir] /file_name</code> <code>file:/{ /flash /pcmcia1 /pcmcia2 } [/dir] /file_name</code> <code>tftp://{ ipaddress host_name [:port#] } [/directory] /file_name</code> <code>ftp://[username [:pwd] @] { ipaddress host_name } [:port#] [/directory] /file_name</code> <code>sftp://[username [:pwd] @] { ipaddress host_name } [:port#] [/directory] /file_name</code> <p><i>/flash</i> corresponds to the CompactFlash on the SMC. <i>/pcmcia1</i> corresponds to PCMCIA slot 1. <i>/pcmcia2</i> corresponds to PCMCIA slot 2. <i>ipaddress</i> is the IP address of the network server. <i>host_name</i> is the network server's <i>hostname</i>. <i>port#</i> is the network server's logical port number. Defaults are:</p> <ul style="list-style-type: none"> tftp: 69 - data ftp: 20 - data, 21 - control sftp: 115 - data <p>Note: <i>host_name</i> can only be used if the networkconfig parameter is configured for DHCP and the DHCP server returns a valid nameserver. <i>username</i> is the username required to gain access to the server if necessary. <i>password</i> is the password for the specified username if required. <i>/directory</i> specifies the directory where the file is located if one exists. <i>/file_name</i> specifies the name of the configuration file to be saved. Note: Configuration files should be named with a .cfg extension.</p>
-redundant	<p>Optional: This keyword directs the system to save the CLI configuration file to the local device, defined by the <i>url</i> variable, and then automatically copy that same file to the like device on the Standby SMC, if available. Note: This keyword will only work for like local devices that are located on both the active and standby SMCs. For example, if you save the file to the <i>/pcmcia1</i> device on the active SMC, that same type of device (a PC-Card in Slot 1 of the standby SMC) must be available. Otherwise, a failure message is displayed. Note: When saving the file to an external network (non-local) device, the system disregards this keyword.</p>

Keyword/Variable	Description
-noconfirm	Optional: Indicates that no confirmation is to be given prior to saving the configuration information to the specified filename (if one was specified) or to the currently active configuration file (if none was specified).
showsecrets	Optional: This keyword saves the CLI configuration file with all passwords in plain text, rather than their default encrypted format.
verbose	Optional: Specifies to display every parameter that is being saved to the new configuration file.



Important: The **-redundant** keyword is only applicable when saving a configuration file to local devices. This command does not synchronize the local file system. If you have added, modified, or deleted other files or directories to or from a local device for the active SMC, you must synchronize the local file system on both SMCs.

To save a configuration file called *system.cfg* to a directory that was previously created called *cfgfiles* on the CompactFlash in the SMC, enter the following command:

```
save configuration /flash/cfgfiles/system.cfg
```

To save a configuration file called *simple_ip.cfg* to a directory called *host_name_configs*, using an FTP server with an IP address of *192.168.34.156*, on which you have an account with a username of *administrator* and a password of *secure*, use the following command:

```
save configuration
ftp://administrator:secure@192.168.34.156/host_name_configs/
simple_ip.cfg
```

To save a configuration file called *init_config.cfg* to the root directory of a TFTP server with a hostname of *config_server*, enter the following command:

```
save configuration tftp://config_server/init_config.cfg
```


Appendix A

Mobile Service Edge Gateway-3G Sample Configuration

The following is a sample configuration for basic MSEG-3G functionality.

```
configure
  logging filter runtime facility all level debug critical-info
  license key "\
VER=1|C1M=SanDiskSDCFJ-4096|C1S=016822F1707V1720|DOI=1281687396|DOE=12\
=Y|SIG=MC0CFPHZlogEkfvv2jXHvV+3c/81QUaEAhUApTSFwxiQ5rKmMq2KHJuqx1p1jXo"
  gtp single-source private-extensions
  system hostname chassis12
  autoconfirm
  card 1
    mode active
  exit
  card 2
    mode active
  exit
  card 3
    mode active
  exit
  require session recovery
  require active-charging
  context local
    subscriber default
    exit
  aaa group default
    exit
```

■ Saving the Configuration on the Chassis

```
gtpv6 group default
  exit
exit
snmp engine-id local 800007e580bad6c7403bf7e746
task facility ipsecmgr max-crypto-maps-each-ipsecmgr 7400
task facility sessmgr max 10
task facility ipsecmgr ikev1 max 6
task facility ipsecmgr ikev2 max 6
context mseg
  interface Dns
    ip address 1.1.1.1 255.255.255.0
    exit
  interface Ga
    ip address 2.2.2.2 255.255.255.0
    exit
  interface ggsn
    ip address 3.3.3.3 255.255.255.0
    exit
  interface mseg1
    ip address 4.4.4.4 255.255.255.0
    ip address 5.5.5.5 255.255.255.255 secondary
    ip address 6.6.6.6 255.255.255.255 secondary
    ip address 7.7.7.7 255.255.255.255 secondary
    exit
  interface realgsn
    ip address 8.8.8.8 255.255.255.0
    exit
subscriber default
  exit
```

```
aaa group default
  exit

gtpv group default
  gtpv charging-agent address 2.2.2.2
  gtpv storage-server local aaamgr-wait-time 1
  gtpv attribute diagnostics
  gtpv attribute local-record-sequence-number
  gtpv dictionary custom6
  gtpv server 9.9.9.9 priority 1 max 1
  exit

policy accounting policy1
  accounting-level subscriber
  cc profile 0 interval 60
  cc profile 1 buckets 1
  cc profile 1 interval 61
  cc profile 2 interval 62
  cc profile 3 buckets 1
  cc profile 3 interval 63
  cc profile 4 interval 64
  cc profile 5 buckets 1
  cc profile 5 interval 65
  cc profile 6 buckets 1
  cc profile 6 interval 66
  cc profile 7 buckets 1
  cc profile 7 interval 67
  cc profile 8 buckets 1
  cc profile 8 interval 68
  cc profile 8 volume total 100000
  cc profile 9 interval 69
```

```
cc profile 10 interval 70
cc profile 11 interval 71
cc profile 12 interval 72
cc profile 13 interval 73
cc profile 14 interval 74
cc profile 15 interval 75

exit

gtpu-service ggsn1_gtpu
bind ipv4-address 7.7.7.7

exit

ggsn-service ggsn1
no echo-interval
no gtpc ran-procedure-ready-delay
plmn unlisted-sgsn home
associate gtpu-service ggsn1_gtpu
bind address 6.6.6.6

exit

mseg-service mseg1
mseg-id 1
mseg-criteria criterial
path-failure detection-policy gtp echo
gtpc max-retransmissions 4
no gtpc echo-interval
gtpc retransmission-timeout 5
gtpu max-retransmissions 4
no gtpu echo-interval
gtpu retransmission-timeout 5
bind gtpc-address 10.10.10.10
bind gtpu-address 5.5.5.5
```

```
    associate accounting-policy policyl
  exit

ip route 11.11.11.11 255.255.255.0 12.12.12.12 ggsn

ip domain-lookup

ip name-servers 13.13.13.13

udr-module active-charging-service
  file name udr-mseg rotation time 60 headers udr-seq-num
  exit

edr-module active-charging-service
  file name edr-mseg rotation time 60 headers edr-format-name
  exit

dns-client dnsclient1
  bind address 1.1.1.1
  cache ttl positive 100
  cache ttl negative 100
  exit

ip igmp profile default
  exit

exit

context isp
  ip access-list css-1
    redirect css service servicel ip any any
  exit

  ip pool natpool1 100.100.100.0 255.255.255.0 nat-one-to-one

  ip pool natpool2 101.101.0.0 255.255.0.0 napt-users-per-ip-address 2 port-
chunk-size 32256

  ip pool natpool3 102.102.0.0 255.255.0.0 napt-users-per-ip-address 2 on-
demand port-chunk-size 32256

  ip pool pp0 10.0.0.1 255.255.0.0 static

  ip pool pp1 11.1.2.1 255.255.255.0 static
```

■ Saving the Configuration on the Chassis

```
ip pool pp2 12.0.0.1 255.255.255.252 public 0
ip pool pp3 1.1.1.1 255.255.255.0 static
interface Gi
    ip address 192.168.40.1 255.255.255.0
    exit
subscriber default
    exit
aaa group default
    exit
gtp group default
    exit
ip igmp profile default
    exit
exit
active-charging service servicel
    idle-timeout tcp 300
    idle-timeout udp 300
    idle-timeout icmp 300
    ruledef ch_ip
        ip any-match = TRUE
        exit
    access-ruledef fw_ip
        ip any-match = TRUE
        exit
    edr-format edr1
        attribute sn-end-time format MM/DD/YYYY-HH:MM:SS priority 1
        attribute sn-start-time format MM/DD/YYYY-HH:MM:SS priority 2
        attribute sn-correlation-id priority 4
        rule-variable ip subscriber-ip-address priority 5
```

```
rule-variable ip server-ip-address priority 6
attribute sn-subscriber-port priority 7
attribute sn-server-port priority 8
attribute sn-volume-amt ip bytes uplink priority 9
attribute sn-volume-amt ip bytes downlink priority 10
attribute sn-volume-amt ip pkts uplink priority 11
attribute sn-volume-amt ip pkts downlink priority 12
rule-variable tcp payload-length priority 13
rule-variable ip protocol priority 14
attribute sn-direction priority 17
attribute sn-group-id priority 20
attribute sn-sequence-no priority 21
attribute sn-closure-reason priority 22
attribute sn-app-protocol priority 25
attribute sn-acct-session-id priority 26
attribute sn-charge-volume ip bytes downlink priority 27
attribute sn-charge-volume ip bytes uplink priority 28
attribute sn-flow-id priority 30
attribute sn-flow-start-time format MM/DD/YY-HH:MM:SS priority 31
attribute sn-format-name priority 32
attribute sn-parent-protocol priority 37
attribute sn-rulebase priority 38
attribute sn-volume-dropped-amt ip pkts uplink priority 46
attribute sn-volume-dropped-amt ip pkts downlink priority 47
attribute transaction-uplink-bytes priority 48
attribute transaction-downlink-bytes priority 49
exit

udr-format udr1

attribute sn-end-time format MM/DD/YYYY-HH:MM:SS priority 1
```

```
attribute sn-start-time format MM/DD/YYYY-HH:MM:SS priority 2
attribute sn-format-name priority 3
attribute sn-correlation-id priority 4
rule-variable bearer 3gpp2 release-indicator priority 6
attribute radius-nas-ip-address priority 7
attribute sn-start-time format YYYY/MM/DD-HH:MM:SS priority 8
event-label event1 priority 10
attribute sn-content-id priority 11
attribute sn-content-vol bytes downlink priority 12
attribute sn-content-vol pkts downlink priority 13
attribute sn-content-vol bytes uplink priority 14
attribute sn-content-vol pkts uplink priority 15
attribute radius-user-name priority 16
attribute sn-group-id priority 20
attribute sn-sequence-no priority 21
attribute sn-closure-reason priority 22
exit

charging-actionedr-egcdr
content-id 1
billing-action create-edrs charging-edr edr1
billing-action egcdr
exit

rulebase rulebase1
billing-records udr udr-format udr1
billing-records egcdr
action priority 1 ruledef ch_ip charging-actionedr-egcdr
fw-and-nat default-policy fw1
exit

fw-and-nat policy fw1
```

```
        access-rule priority 1 access-ruledef fw_ip permit nat-realm natpool1
        firewall policy ipv4-only
        exit
    exit
mobile-services-edge-gateway
    apn-profile apn1
        apn testapn1
        exit
    apn-profile apn2
        apn testapn2
        exit
    imsi-profile imsi-1
        imsi-range mcc 262 mnc 090 msin start 426000100 end 426000200
        exit
    imei-profile imei1
        imei-range start 12345678912300 end 12345678912500 sv 12
        exit
    associated-services-profile profile1
        ip context-name isp
        ip access-group css-1 in
        ip access-group css-1 out
        active-charging-rulebase rulebase1
        exit
    mseg-ruleset rule1
        apn if-match-profile apn1
        exit
    mseg-ruleset rule2
        imsi if-match-profile imsi-1
        exit
```

```
mseg-ruleset rule3
    imei if-match-profile imei1
    exit
mseg-ruleset rule4
    apn if-match-profile apn2
    exit
mseg-criteria criterial
    filter priority 1 ruleset rule1 action offload associated-services-
profile profile1
    filter priority 2 ruleset rule2 action offload associated-services-
profile profile1
    filter priority 3 ruleset rule3 action offload associated-services-
profile profile1
    filter priority 4 ruleset rule3 action forward
    exit
exit
port ethernet 18/1
    no shutdown
    bind interface mseg1 mseg
    exit
port ethernet 18/2
    no shutdown
    bind interface Gi isp
    exit
port ethernet 18/3
    no shutdown
    bind interface Dns mseg
    exit
port ethernet 18/4
    no shutdown
```

```
    bind interface ggsn mseg
    exit
port ethernet 18/5
    no shutdown
    bind interface Ga mseg
    exit
port ethernet 18/6
    no shutdown
    exit
port ethernet 18/7
    no shutdown
    exit
end
```