SaMOG Administration Guide, StarOS Release 21.14

First Published: 2019-06-27

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

CONTENTS

About This Guide

This preface describes the *SaMOG Administration Guide*, how it is organized, and its document conventions.

The guide provides information on the SaMOG (S2a-based Mobility over GTP) Gateway and includes network deployments and interfaces, feature descriptions, session establishment and disconnection flows, configuration instructions, and CLI commands for monitoring the system.

Conventions Used

The following tables describe the conventions used throughout this documentation.

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.

Typeface Conventions	Description
Text represented as a `screen display`	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.

Typeface Conventions	Description
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 *variable* **}**	Required keyword options and variables are those components that are required to be entered as part of the command syntax. Required keyword options and variables are surrounded by grouped braces { }. For example: **sctp-max-data-chunks { limit** *max_chunks* **| mtu-limit }** If a keyword or variable is not enclosed in braces or brackets, it is mandatory. For example: **snmp trap link-status**
[keyword or *variable* **]**	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by brackets.
|	Some commands support multiple options. These are documented within braces or brackets by separating each option with a vertical bar. These options can be used in conjunction with required or optional keywords or variables. For example: **action activate-flow-detection { intitiation | termination }** or **ip address [count** *number_of_packets* **| size** *number_of_bytes* **]**

Supported Documents and Resources

Related Common Documentation

The most up-to-date information for this product is available in the product Release Notes provided with each product release.

The following common documents are available:

- *AAA Interface Administration and Reference*
- *Command Line Interface Reference*
- *GTPP Interface Administration and Reference*
- *Installation Guide* (platform dependent)
- *Release Change Reference*
- *SNMP MIB Reference,*
- *Statistics and Counters Reference*
- *System Administration Guide* (platform dependent)
- *Thresholding Configuration Guide*

Related Product Documentation

The following product documents are also available and work in conjuction with SaMOG:

- *ECS Administration Guide*
- *GGSN Administration Guide*
- *SGSN Administration Guide*
- *S-GW Administration Guide*
- *P-GW Administration Guide*
- *MME Administration Guide*
- *NAT Administration Guide*

Obtaining Documentation

The most current Cisco documentation is available on the following website:

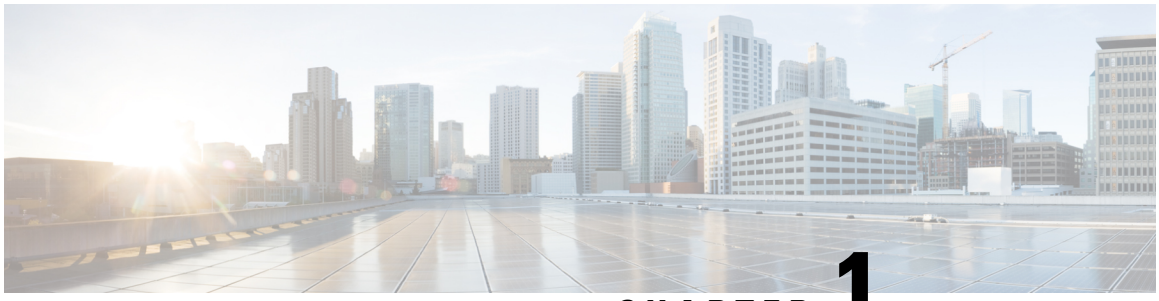
Use the following path selections to access the SaMOG documentation:

Products > Wireless > Mobile Internet> Network Functions > Cisco SaMOG S2a Mobility over GTP

Contacting Customer Support

Use the information in this section to contact customer support.

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 are required to access this site. Please contact your Cisco sales or service representative for additional information.



CHAPTER 1

SaMOG Gateway Overview

This chapter contains an overview of the SaMOG (S2a Mobility Over GTP) Gateway. This chapter covers the following topics:

Product Description

Until recently, Wireless LAN (WLAN) security was considered poor in strength and ease-of-use compared with that of LTE networks and devices, and operators used their core networks to add security layers such as IKEv2 for UE authentication and authorization and IPSec for network security between the UEs and the core network gateways. With the deployment of 802.1x, 802.11u, 802.11i, and Hotspot 2.0, operators now consider WLAN security strength and ease-of-use to be as acceptable as LTE security.

The Cisco® S2a Mobility Over GTP (SaMOG) Gateway addresses this next step in network evolution by enabling mobile operators to provide IP access from trusted non-3GPP access networks to the 3GPP EPC (Evolved Packet Core) network via. the S2a interface, including traffic from trusted WiFi, femtocell, metrocell, and small cell access networks. The SaMOG Gateway allows operators to provide services to 3G subscribers using GGSN (GTPv1) and 4G subscribers using P-GW (GTPv2, PMIPv6) via. PMIPv6, EoGRE or L3IP access-types.

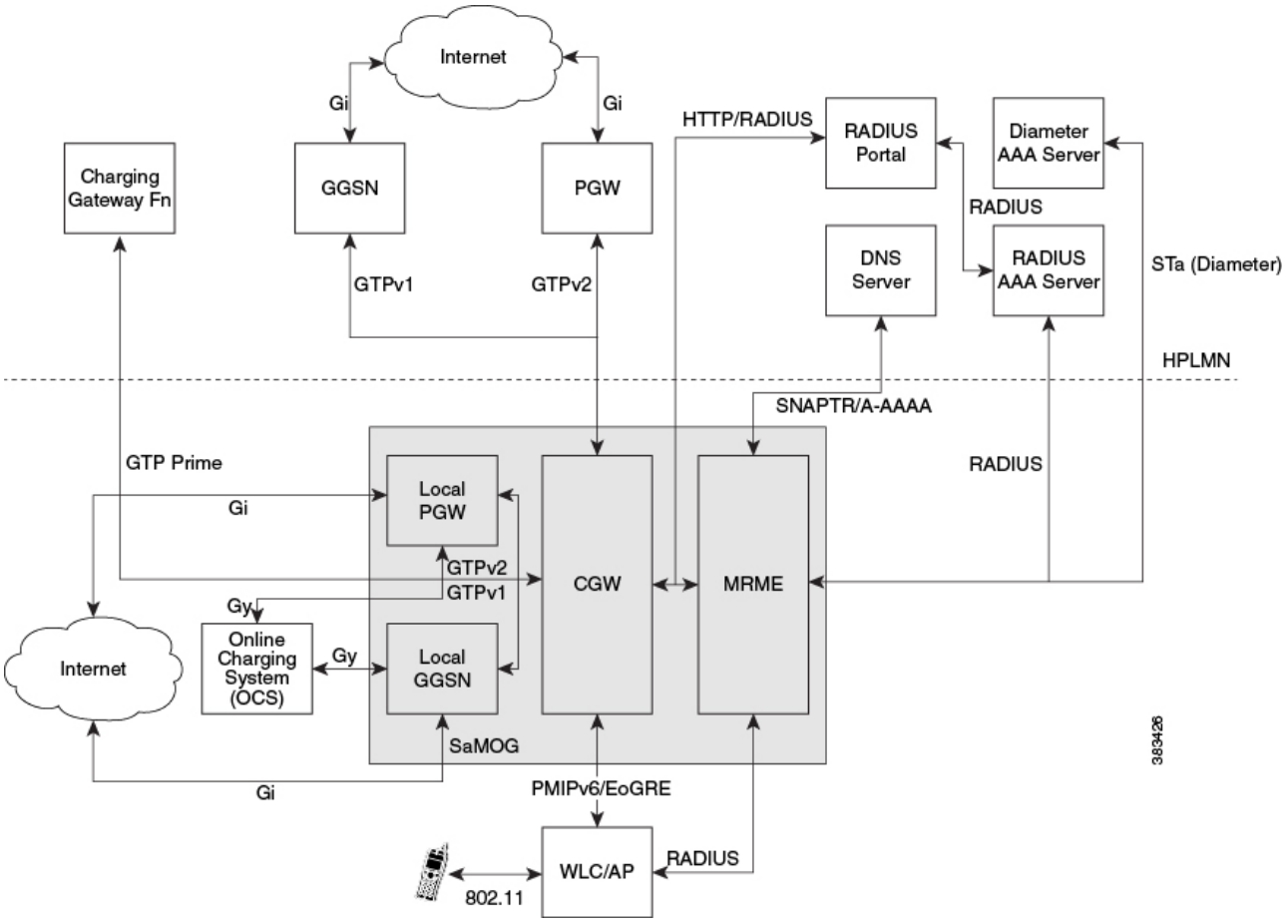
The SaMOG Gateway has the following key features:

- Provides seamless mobility between the 3GPP EPC network and WLANs for EPS (Evolved Packet System) services via. the GTPv1 based Gn interface, or GTPv2/PMIPv6-based S2a interface.
- Functions as a 3GPP Trusted WLAN Access Gateway (TWAG) as the Convergence Gateway (CGW) service. The CGW service terminates the S2a interface to the GGSN/P-GW and acts as the default router for the WLAN UEs on its access link.
- Functions as a 3GPP Trusted WLAN AAA Proxy (TWAP) as the Multi Radio Management Entity (MRME) service. The MRME service terminates the STa interface to the 3GPP AAA server and relays

the AAA information between the WLAN IP access network and the AAA server, or AAA proxy in the case of roaming.

The following figure provides the network architecture of the SaMOG Gateway:

Figure 1: SaMOG Gateway Network Architecture



Qualified Platforms

The SaMOG Gateway is a StarOS™ application that runs on Cisco ASR 5x00 and virtualized platforms. For additional platform information, refer to the appropriate *System Administration Guide* and/or contact your Cisco account representative.

DPC2 on ASR 5500

The SaMOG Gateway is fully qualified to run on the second generation Data Processing Card (DPC2) on the ASR 5500.

The DPC2 offers increased performance versus the first generation DPC, while maintaining backwards compatibility with other ASR 5500 cards. The raw input/output has been increased from 80Gbps (DPC/UDPC) to 150Gbps (DPC2).

The DPC2 has three CPU subsystems. Each subsystem consists of two CPUs with 24 cores each (maximum 144 cores) that are paired with a Platform Controller Hub (PCH). Each CPU is associated with 32 GB of DDR4 memory (total of 192 GB per DPC2) and a latest generation crypto offload engine.

For more information on the DPC2 card, refer the *System Administration Guide*.

MIO Demux Card on ASR 5500

The SaMOG Gateway is fully qualified to run on the Management Input/Output (MIO) card for demux functions. SaMOG can leverage on the additional card for user plane processing to increase the capacity of the chassis.

For more information on the MIO Demux card, refer the *System Administration Guide*.

Licenses

The SaMOG Gateway is a licensed Cisco product. Two mutually exclusive SaMOG base licenses are available for operators with different network deployment models:

- **SaMOG General License:** This base license is available for operators with a pure 4G deployment model or a Mixed Mode (running both 3G and 4G) deployment model. Operators can configure subscribers to setup 3G or 4G sessions based on the serving PLMN and the subscription of the subscriber.
- **SaMOG 3G License:** This base license is available for operators with a pure 3G deployment model. Operators can setup 3G (GTPv1) sessions through the SaMOG Gateway. This license does not permit configuration of a Diameter-based authentication.

In addition to the base license for running SaMOG services, separate session and feature licenses may also be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, see "Managing License Keys" in the *System Administration Guide*.

SaMOG Services

The SaMOG Gateway acts as the termination point of the WLAN access network. The SaMOG service enables the WLAN UEs in the trusted non-3GPP IP access network to connect to the EPC network via Wireless LAN Controllers (WLCs). During configuration, the SaMOG service gets associated with two services: the Convergence Gateway (CGW) service and the Multi Radio Mobility Entity (MRME) service. These collocated services combine to enable the SaMOG Gateway functionality.

CGW Service

The Convergence Gateway (CGW) service functions as a 3GPP Trusted WLAN Access Gateway (TWAG), terminating the S2a interface to the GGSN/P-GW and acts as the default router for the WLAN UEs on its access link.

The CGW service has the following key features and functions:

- Functions as a Local Mobility Anchor (LMA) towards the WLCs, which functions as a Mobile Access Gateway (MAG) with Proxy MIP capabilities per RFC 5213 and 3GPP TS 29.275 V11.5.
- Enables the S2a GTPv2 interface towards the P-GW for session establishment per 3GPP TS 29.274 V11.5.0.

- Enables the S2a PMIPv6 interface towards the P-GW for session establishment per 3GPP TS 29.275 V11.5.0.
- Enables the Gn interface towards the GGSN for session establishment per 3GPP TS 29.060 V11.5.0.
- Support for Layer 3 IP (L3IP) with out-of-band DHCP, and IP address assigned by the WLC (IP@W).
- Routing of packets between the P-GW and the WLAN UEs via the Wireless LAN Controllers (WLCs).
- Support for PDN type IPv4 and IPv6.
- Interacts with the MRME service to provide user profile information to establish the GTP-variant S2a interface towards the GGSN/P-GW per 3GPP TS 29.274.
- Provides a Generic Routing Encapsulation (GRE) data path towards the WLCs per RFCs 1701 and 1702 for tunneling of data towards the WLCs. Also follows RFC 5845 for exchanging GRE keys with WLC-based PMIP signaling.
- Receives and sends GTPU data packets towards the GGSN/P-GW per 3GPP TS 29.281 V11.5.

CGW Features and Functions

The CGW service includes the following features and functions:

DSCP Marking—CGW

Differentiated Services Code Point (DSCP) levels can be assigned to specific traffic patterns in order to ensure that data packets are delivered according to the precedence with which they are tagged. The DiffServ markings are applied to the IP header for every subscriber data packet transmitted in the downlink direction to the WLAN access network. The four traffic patterns have the following order of precedence:

1. Background (lowest)
2. Interactive
3. Streaming
4. Conversational (highest)

In addition, for class type Interactive, further categorization is done in combination with traffic handling priority and allocation-retention priority. Data packets falling under the category of each of the traffic patterns are tagged with a DSCP marking. Each traffic class is mapped to a QCI value according to mapping defined in TS 23.203. Therefore, DSCP values must be configured for different QCI values.

DSCP markings can be configured to control the DSCP markings for downlink packets. The IP header of the packet is updated with the value in TOS field. Note that there is no tunnel at the access side in SaMOG Gateway, hence the TOS field in the subscriber IP packet is marked with the DSCP value directly.

For more information on DSCP Marking on the SaMOG Gateway, refer DSCP Marking, on page 141.

GTPUv1 Support toward the P-GW—CGW

The SaMOG Gateway's CGW service supports GTPUv1 towards the P-GW as defined in 3GPP TS 29.281, V11, including the following functions:

- The SaMOG Gateway's CGW service supports fragmentation and reassembly of the outer IP packets that flow over the S2a interface via GRE tunnels, and supports reassembly of the incoming packets, including stripping the GRE encapsulation and tunneling the resultant packets to the GGSN/P-GW via GTP encapsulation. The CGW service supports GRE payloads over IPv4, IPv6, and IPv4v6 transports.
- Routing of packets between the GGSN/P-GW and the WLAN UE via the WLC.
- Tunnel management procedures for session creation and deletion.
- Path management procedures for path existence checks.
- Handling of the Recovery IE for detecting path failures.

GTP based Interface Support—CGW

The SaMOG Gateway's CGW service supports the GTPv2/GTPv1-based S2a/Gn interface towards the GGSN/P-GW for session establishment per 3GPP TS 29.274 and 29.060 Release 11.5, including the following functions:

- Routing of packets between the GGSN/P-GW and the WLAN UE via the WLC.
- Establishment of flows towards the WLC and the GGSN/P-GW.
- Tunnel management procedures for session creation and deletion.
- Path management procedures for path existence checks.
- Handling of the Recovery IE for detecting path failures.

Important SaMOG does not initiate any MODIFY_BEARER_COMMAND (to P-GW) or UPDATE_PDP_CONTEXT (to GGSN) message when a QoS update notification is received from the AAA server during reauthentication. SaMOG expects the AAA server to initiate an RAR for notification of any QoS updates (QoS changes are notified in the AA-Answer).

GRE Tunnel Support—CGW

The SaMOG Gateway's CGW service supports dynamic per-session Generic Routing Encapsulation (GRE) tunnels from the trusted 3GPP WLAN per RFC 5845.

P-GW Selection for LTE-to-WiFi Mobility—CGW

During LTE-to-WiFi mobility, the SaMOG Gateway's CGW service selects the same P-GW that anchored the session over LTE. The CGW service selects the GGSN/P-GW via an internal trigger from the SaMOG Gateway's MRME service.

Proxy MIP Support—CGW

The SaMOG Gateway's CGW service provides the underlying mechanism to terminate per-session Proxy Mobile IP (PMIPv6) tunnels from the WLAN infrastructure. To accomplish this, the CGW service acts as an Local Mobility Anchor (LMA) towards the Wireless LAN Controllers (WLCs), which acts as a Mobile Access Gateway (MAG) with PMIPv6 functionality as defined in RFC 5213. The LMA and MAG functions use Proxy Mobile IPv6 signaling to provide network-based mobility management on behalf of the UEs attached to the network. With this approach, the attached UEs are no longer involved in the exchange of signaling messages for mobility.

The LMA function on the SaMOG Gateway's CGW service and the MAG function on the WLCs maintain a single shared tunnel. To distinguish between individual subscriber sessions, separate GRE keys are allocated in the Proxy-MIP Binding Update (PBU) and Proxy-MIP Binding Acknowledgement (PBA) messages between the CGW service and the WLCs. To handle AAA server initiated disconnections, the CGW service supports RFC 5846 for Binding Revocation Indication (BRI) and Binding Revocation Acknowledgement (BRA) messaging with the WLCs.

EoGRE Support—CGW

CGW connects 3G/4G subscribers to EPC/Internet through the Trusted Wifi SSIDs served by EoGRE enabled Residential Gateways. CGW acts as the tunnel endpoint for the EoGRE tunnel initiated from the Residential Gateway. With the use of SSID-based WLAN access, the subscribers are authenticated based on the SSID they use in order to connect to the WLAN. The Residential-GW/WLC maintains a separate SSID for providing the 3G/4G access to help the UE in selecting the correct SSID for obtaining 3G/4G access through Wifi

network. SaMOG (MRME) act as the AAA server and DHCP server for the UE attaching to the WLAN network. This helps in processing all the control packets from the UE and maintaining the subscriber session to provide 3G/4G access. While acting as DHCP-Server, CGW creates the PDP-Context with GGSN/P-GW to obtain the IP Address to be allocated to UE through DHCP-Response in the access side. The DHCP and data packets generated by UE will be tunneled over EoGRE by Residential-GW/WLC node to SaMOG.

S2a Interface using PMIPv6—CGW

In StarOS Release 18 and later, the SaMOG Gateway can connect to the P-GW service over the S2a interface based on the PMIPv6 protocol as specified by 3GPP TS 29.275, Release 11 standards. The SaMOG Gateway performs a SNAPTR-based DNS query towards the DNS server to get the P-GW IP address, and initiates a PMIPv6-based registration procedure (acting as a Mobile Access Gateway (MAG)) by sending a Proxy Binding Update message to the P-GW. The IP address of the User Equipment (UE) allocated by P-GW (acting as the Local Mobility Anchor (LMA)) is then received in the Proxy Binding Acknowledge message.

How S2a Interface using PMIPv6 Works

The UE performs an 802.11 initial attach procedures and connect to Access Points (AP) and Wireless LAN Controllers (WLC), which in turn triggers a RADIUS-based authentication with the SaMOG Gateway. The SaMOG Gateway selects a RADIUS/Diameter-based AAA server or AAA proxy based on the local profile configuration and performs a RADIUS/Diameter-based authentication with the AAA server. After multiple rounds of authentication, the AAA server confirms the authentication status for the UE and shares the subscriber profile with the SaMOG Gateway. The SaMOG Gateway selects the P-GW based on the subscribers authorization information and setup a PMIPv6-based session with the P-GW. The data between the SaMOG Gateway and P-GW are exchanged through GRE tunnels using GRE keys for uplink and downlink data.

Limitations

The following are the current limitations for the SaMOG S2a interface using PMIPv6:

- As a PMIPv6-based S2a interface on the SaMOG Gateway cannot be used with a GGSN service, the SaMOG 3G license is not supported.
- The SaMOG Local Breakout - Enhanced model, and the SaMOG Web Authorization features are currently not supported.
- QoS negotiation and updates are not applicable for PMIPv6-based S2a interface, as there is no provision in the S2a interface PMIPv6 control messages to carry the requested QoS.

MRME Service

The Multi Radio Mobility Entity (MRME) service functions as a 3GPP Trusted WLAN AAA Proxy (TWAP), terminating the STa interface to the 3GPP AAA server and relays the AAA information between the WLAN IP access network and the AAA server, or AAA proxy in the case of roaming.

The MRME service has the following key features and functions:

- Relays the AAA information between the Wireless LAN Controllers (WLCs) and the 3GPP AAA server.
- Supports EAP-over-RADIUS between the SaMOG Gateway and the WLCs to authenticate the WLAN UEs per RFC 3579.
- Supports the Diameter-based STa interface between the 3GPP AAA server/proxy and the SaMOG Gateway per 3GPP TS 29.273 V11.4.0.
- Supports the exchange of EAP messages over the STa interface per RFC 4072.
- Functions as a RADIUS accounting proxy for WLC-initiated accounting messages as per RFC 2866.

- Supports RADIUS Dynamic Authorization Extensions per RFC 3576 to handle HSS/AAA-initiated detach and Diameter re-authorization procedures.
- Supports authentication between the WLAN UEs and the 3GPP AAA server using EAP-AKA, EAP-AKA', and EAP-SIM.
- Supports static and dynamic P-GW selection after the authentication procedures as per 3GPP TS 29.303 v 11.2.0.
- Support for PDN type IPv4 and IPv6.
- Maintains a username database to re-use existing resources when the CGW service receives PMIPv6 and EoGRE procedures initiated by the WLCs.
- Interacts with the CGW service to provide user profile information to establish the GTP-variant S2a/Gn interface towards the P-GW/GGSN per 3GPP TS 29.274 and 3GPP TS 29.060.

MRME Features and Functions

The MRME service includes the following features and functions.

EAP Authentication over RADIUS—MRME

The SaMOG Gateway's MRME service supports Extensible Authentication Protocol (EAP) over RADIUS to interact with the WLCs for authenticating the WLAN UEs based on RFC 3579. Two attributes, EAP-Message and Message-Authenticator, are used to transport EAP messages as defined in RFC 3579. The MRME service validates and processes these messages as follows:

- Validates the EAP header fields (Code, Identifier, and Length attributes) prior to forwarding an EAP packet.
- Discards Access-Request packets that include an EAP-Message attribute without a Message-Authenticator attribute.
- If multiple EAP-Message attributes are contained within an Access-Request or Access-Challenge packet, concatenates them to form a single EAP packet.
- For Access-Challenge, Access-Accept, and Access-Reject packets, calculates the Message-Authenticator attribute as follows: Message-Authenticator = HMAC-MD5 (Type, Identifier, Length, and Request Authenticator attributes).

EAP Identity of Decorated NAI Formats—MRME

The SaMOG Gateway supports the use of the EAP identity of the Decorated NAI in the following format:

homerealm!username@otherrealm

The username part of the Decorated NAI complies with RFCs 4187, 4816, and 5448 for EAP AKA, EAP SIM, and EAP AKA', respectively.

The following are examples of a typical NAI:

- **For EAP AKA authentication:**
  wlan.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org!0<IMSI>@wlan.mnc<visitedMNC>

  .mcc<visitedMCC>.3gppnetwork.org
- **For EAP SIM authentication:**
  wlan.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org!1<IMSI>@wlan.mnc<visitedMNC>

  .mcc<visitedMCC>.3gppnetwork.org
- **For EAP AKA' authentication:**
  wlan.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org!6<IMSI>@wlan.mnc<visitedMNC>

.mcc<visitedMCC>.3gppnetwork.org

EAP Identity of Emergency NAI Formats—MRME

The SaMOG Gateway's MRME service supports the use of the EAP identity of the Emergency NAI in the following format:

0<IMSI>@sos.wlan.mnc015.mcc234.3gppnetwork.org/1<IMSI>@sos.wlan.mnc015.mcc234.3gppnetwork.org

If the IMSI is not available, the Emergency NAI can include the IMEI/MAC address, as follows:

- imei<IMEI>@sos.wlan.mnc<visitedMNC>.mcc<visitedMCC>.3gppnetwork.org
- mac<MAC>@sos.wlan.mnc<visitedMNC>.mcc<visitedMCC>.3gppnetwork.org

As per RFC 29.273, UEs without an IMSI are not authorized via the STa Interface. If the Emergency NAI includes an IMEI or MAC username format, the authentication request will be rejected.

EAP Identity of Fast Reauthentication NAI Formats—MRME

Where the AAA server supports fast reauthentication, the AAA server assigns an identity to the subscriber which is used by the subscriber's UE to initiate a reattach or reauthentication. This authentication method is faster than the full reauthentication method as the AAA server and UE use the authentication key from a previous full authentication. The UE sends the assigned fast reauthentication NAI for subsequent authentication attempts, and the AAA server looks up the mapping between the fast reauthentication NAI and the identity of the subscriber.

The SaMOG gateway supports the use of the EAP identity of the Fast Reauthentication NAI in the following normal and decorated formats:

Normal: <prefix+fast-reauth-id>@nai.epc.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org

Decorated:
nai.epc.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org!<prefix+fast-reauth-id>@nai.epc.mnc<visitedMNC>.mcc<visitedMCC>.3gppnetwork.org

Important Currently, SaMOG does not support multi-PLMN. If the PLMN ID of a UE changes during a re-attach procedure, the User-Name changes from root to decorated NAI format or vice versa. The SaMOG service simply logs the event and continues with the session setup. The IPSG manager is updated with the permanent NAI (root format) and sent to the WLC to be included in the PBU for the PMIPv6 session. If the WLC does not use the NAI format in the PBU, call setup fails as the PBU is rejected. To avoid the change from root to decorated NAI or vice versa, specify a serving PLMN ID with an IMSI range. When a serving PLMN ID changes, the existing call is taken down and a re-attach procedure occurs.

The fast-reauth-id part of the Fast Reauthentication NAI complies with 3GPP 23.003 standards.

The following are examples of a typical NAI:

- **For EAP AKA authentication:**
  4<fast-reauth-id>@nai.epc.mnc<homeMNC>.mnc<homeMCC>.3gppnetwork.org

  nai.epc.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org!4<fast-reauth-id>@nai.epc.mnc<visitedMNC>.mcc<visitedMCC>.3gppnetwork.org
- **For SIM authentication:**
  5<fast-reauth-id>@nai.epc.mnc<homeMNC>.mnc<homeMCC>.3gppnetwork.org

nai.epc.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org!5<fast-reauth-id>@nai.epc.mnc<visitedMNC>.mcc<visitedMCC>.3gppnetwork.org

- **For EAP AKA' authentication:**
  8<fast-reauth-id>@nai.epc.mnc<homeMNC>.mnc<homeMCC>.3gppnetwork.org

  nai.epc.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org!8<fast-reauth-id>@nai.epc.mnc<visitedMNC>.mcc<visitedMCC>.3gppnetwork.org

EAP Identity of Pseudonym NAI Formats—MRME

The pseudonym NAI is a temporary identity provided to a user by the AAA server that the subscriber uses while connecting to the network. This enables the subscriber to connect and authenticate without revealing their IMSI information on the network. The AAA server maintains a mapping between the real identity and the pseudonym NAI of the subscriber, and uses the mapping to identify the subscriber.

The SaMOG gateway supports the use of the EAP identity of the Pseudonym NAI in the following normal and decorated formats:

Normal: <prefix+pseudonym-id>@nai.epc.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org

Decorated:
nai.epc.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org!<prefix+pseudonym-id>@nai.epc.mnc<visitedMNC>.mcc<visitedMCC>.3gppnetwork.org

Important Currently, SaMOG does not support multi-PLMN. If the PLMN ID of a UE changes during a re-attach procedure, the User-Name changes from root to decorated NAI format or vice versa. The SaMOG service simply logs the event and continues with the session setup. The IPSG manager is updated with the permanent NAI (root format) and sent to the WLC to be included in the PBU for the PMIPv6 session. If the WLC does not use the NAI format in the PBU, call setup fails as the PBU is rejected. To avoid the change from root to decorated NAI or vice versa, specify a serving PLMN ID with an IMSI range. When a serving PLMN ID changes, the existing call is taken down and a re-attach procedure is initiated.

The pseudonym-id part of the Pseudonym NAI complies with 3GPP 23.003 standards.

The following are examples of a typical NAI:

- **For EAP AKA authentication:**
  2<pseudonym-id>@nai.epc.mnc<homeMNC>.mnc<homeMCC>.3gppnetwork.org

  nai.epc.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org!2<pseudonym-id>@nai.epc.mnc<visitedMNC>.mcc<visitedMCC>.3gppnetwork.org

- **For SIM authentication:**
  3<pseudonym-id>@nai.epc.mnc<homeMNC>.mnc<homeMCC>.3gppnetwork.org

  nai.epc.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org!3<pseudonym-id>@nai.epc.mnc<visitedMNC>.mcc<visitedMCC>.3gppnetwork.org

- **For EAP AKA' authentication:**
  7<pseudonym-id>@nai.epc.mnc<homeMNC>.mnc<homeMCC>.3gppnetwork.org

  nai.epc.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org!7<pseudonym-id>@nai.epc.mnc<visitedMNC>.mcc<visitedMCC>.3gppnetwork.org

EAP Identity of Root NAI Formats—MRME

The SaMOG Gateway supports the use of the EAP identity of the Root NAI in the following format:

username@otherrealm

The username part of the Root NAI complies with RFCs 4187, 4816, and 5448 for EAP AKA, EAP SIM, and EAP AKA', respectively.

The following are examples of a typical NAI:

- **For EAP AKA authentication:** 0<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org
- **For EAP SIM authentication:** 1<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org
- **For EAP AKA' authentication:** 6<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org

EAP Agnostic Authentication—MRME

The SaMOG Gateway additionally supports EAP-based authentication where the inner layer of EAP protocols is agnostic. This enables SaMOG to support authentication mechanisms such as EAP-TLS and EAP-TTLS/MSCHAPv2, to connect non-UICC devices to the EPC core.

EAP-TLS

This authentication mechanism enables SaMOG to provide a certificate-based mutual authentication mechanism between the UE and the EAP Server for non-UICC devices.

EAP-TTLS/MSCHAPv2

SaMOG performs this authentication mechanism in two phases. During the first phase, SaMOG authenticates the server using a certificate that is used to create a secure tunnel. In the second phase, the subscriber is authenticated using MSCHAPv2 authentication mechanism within the secure tunnel.

Authentication

SaMOG considers the EAP-response/identity messages between the WLC and the AAA server as an uncategorized EAP authentication mechanism. SaMOG allows messages to be exchanged until a success/failure message is received from the AAA server, or the session setup timer expires.

NAI Usage

As with SIM-based authentications, in compliance to 3GPP 23.003 standard, SaMOG expects the NAI forwarded by the UE to be in the same format for P-GW selection, with the flexibility to support non-IMSI-based user-name in the AVP.

If the prefix for the user-name is uncategorized (not between 0 and 9), SaMOG considers the username portion of the NAI as non-IMSI based.

User Equipment (UE) Identity—MRME

In StarOS Release 18 and later, the SaMOG Gateway can receive the User Equipment's (UE) MAC address as the UE's identity in the Calling-Station-ID AVP in the Radius message (Access-Request). The UE's identity can then be forwarded over the GTPv1 or GTPv2 interface in the IMEI Software Version (SV) IE to GGSN, or Mobile Equipment Identity (MEI) IE to P-GW.

As the UE identity (MAC address) is 12 Bytes long (6 Bytes in the TBCD format), and the total length of the IMEIsV is 8 bytes, the additional 2 Bytes can be padded with an user configurable filler value.

Access Point (AP) Location—MRME

In StarOS Release 18 and later, the SaMOG Gateway can share the location information of the AP in the User Location Information (ULI) IE during the PDP context setup, and update the locations as Update Context Requests on the GTPv1 interface.When SaMOG detects a change in the AP's location during handovers, an Update PDP Context message is triggered.

SaMOG supports a new format to facilitate AP location in the Called-Station-ID AVP forwarded in the Radius messages. APs are assigned AP-Names which contain the location details and its MAC address (identity). The AP location (CGI) consists of the Location Area Code (LAC) and the Cell Identity (CI). SaMOG supports the following formats in the Called-Station-ID AVP:

- <MAC>
- mac<MAC>
- <MAC>:<SSID>
- mac<MAC>:<SSID>
- cgi<CGI>:<SSID>
- mac<MAC>:cgi<CGI>
- cgi<CGI>:mac<MAC>
- mac<MAC>:cgi<CGI>:<SSID>
- cgi<CGI>:mac<MAC>:<SSID>

For example, if an AP is assigned LAC = 1235, CI = 6789, AP-MAC = 11-22-33-44-55-66, and SSID = test, the Called-Station-ID AVP will contain cgi<12356789>:mac<112233445566>:test.

Access Point Group Name—MRME

The SaMOG Gateway supports access point (AP) group name format in the Called-Station-ID AVP to enable a way to apply policies based on WiFi AP groups . The AP/WLC forwards the AP group name to the SaMOG Gateway in the Access-Request message during initial attach, re-authentication, or handover. The SaMOG Gateway parses the AP group name and forwards it to:

- STa Diameter AAA server in the ANID AVP over DER/AAR messages
- RADIUS AAA server in the Called-Station-Id AVP over the Access-Request message
- External, co-located, or Local P-GW (LBO) in the TWAN-Identifier IE in the SSID sub-field over the Create Session Request message.

Important If the maximum length of the AP group name exceeds 32 octets, the SaMOG Gateway will not include the AP group name in the SSID field of the TWAN-Identifier IE.

The AAA server and P-GW can use the AP group name information to select Gx policies for the P-GW session. Different Gx policies can be chosen for different AP groups based on the AAA/PCRF configuration.

The AP group name information can be included with or without the "grp" prefix. When the AP Group name is included with the “grp” prefix, it can be present anywhere in the Called-Station-Id AVP. When the AP Group name is included without the "grp" prefix, it must be the last token preceded by the SSID token in the “Called-Station-Id” attribute.

The SaMOG Gateway currently supports the following AP group name formats in the Called-Station-ID AVP:

- mac<MAC>:grp<AP-Group-Name>
- grp<AP-Group-Name>:<SSID>
- cgi<CGI>:grp<AP-Group-Name>
- cgi<CGI>:mac<MAC>:grp<AP-Group-Name>
- <MAC>:<SSID>:<AP-Group-Name>

Diameter STa Interface Support—MRME

The SaMOG Gateway complies with 3GPP Release 11 SaMOG specifications for the STa interface as defined in TS 29.273 V11.4. The STa interface is defined between a non-3GPP access network and a 3GPP AAA server/proxy. The SaMOG Gateway uses the STa interface to authenticate and authorize the WLAN UEs. The SaMOG Gateway can communicate with the AAA Server/proxy over the IPv4 or IPv6 interface.

Operator Policy Support (IMSI-based Server Selection)—MRME

The SaMOG Gateway's MRME service supports the selection of a 3GPP AAA proxy based on the IMSI via the operator policy feature.

The operator policy provides mechanisms to fine tune the behavior of subsets of subscribers above and beyond the behaviors described in the user profile. It also can be used to control the behavior of visiting subscribers in roaming scenarios, enforcing roaming agreements and providing a measure of local protection against foreign subscribers.

An operator policy associates APNs, APN profiles, an APN remap table, and a call-control profile to ranges of IMSIs. These profiles and tables are created and defined within their own configuration modes to generate sets of rules and instructions that can be reused and assigned to multiple policies. In this manner, an operator policy manages the application of rules governing the services, facilities, and privileges available to subscribers. These policies can override standard behaviors and provide mechanisms for an operator to get around the limitations of other infrastructure elements, such as DNS servers and HSSs.

The operator policy configuration to be applied to a subscriber is selected on the basis of the selection criteria in the subscriber mapping at attach time. A maximum of 1,024 operator policies can be configured. If a UE was associated with a specific operator policy and that policy is deleted, the next time the UE attempts to access the policy, it will attempt to find another policy with which to be associated.

A default operator policy can be configured and applied to all subscribers that do not match any of the per-PLMN or IMSI range policies.

Changes to the operator policy take effect when the subscriber re-attaches and subsequent EPS Bearer activations.

P-GW Selection—MRME

The P-GW selection function enables the SaMOG Gateway's MRME service to allocate a P-GW to provide PDN connectivity to the WLAN UEs in the trusted non-3GPP IP access network. The P-GW selection function can employ either static or dynamic selection.

Static Selection

The PDN-GW-Allocation-Type AVP indicates whether the P-GW address is statically allocated or dynamically selected by other nodes, and is considered only if MIP6-Agent-Info is present.

The figure below shows the message exchange for static selection. The table that follows the figure describes each step in the flow.

Figure 2: P-GW Static Selection

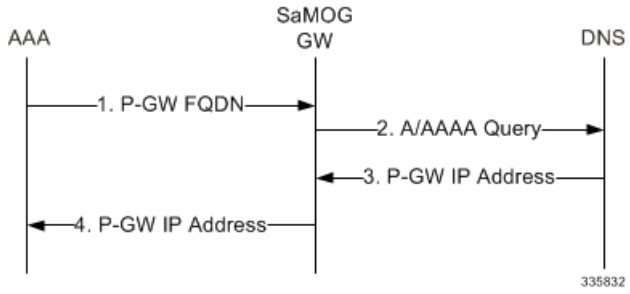


Table 1: P-GW Static Selection

Step	Description
1.	The SaMOG Gateway's MRME service receives the P-GW FQDN or P-GW IP address from the AAA server as part of the MIP-Home-Agent-Host AVP in the Diameter EAP Answer message.
2.	If it receives a P-GW FQDN, and if the FQDN starts with "topon", the MRME service removes the first two labels of the received FQDN to obtain the Canonical Node Name (ID) of the P-GW. The MRME service uses this P-GW ID to send an S-NAPTR query to the DNS.
3.	The MRME service receives the results of the query and selects the replacement string (P-GW FQDN) matching the Service Parameters of "x-3gpp-pgw:x-s2a-gtp".
4.	The MRME service then performs a DNS A/AAAA query with selected replacement string (P-GW FQDN). The DNS returns the IP address of the P-GW.

Dynamic Selection

For a given APN, when the HSS returns Dynamic Allocation Allowed for the P-GW ID and the selection is not for a 3GPP-to-non-3GPP handover, the MRME service ignores the P-GW ID and instead performs dynamic selection.

The figure below shows the message exchange for dynamic selection. The table that follows the figure describes each step in the flow.

Figure 3: P-GW Dynamic Selection

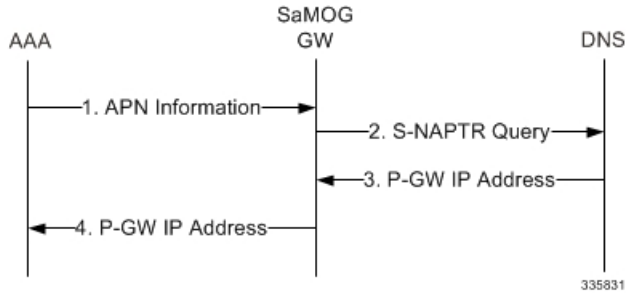


Table 2: P-GW Dynamic Selection

Step	Description
1.	The MRME service receives an APN name from the 3GPP AAA server.
2.	The MRME service constructs the APN FQDN from the received APN name and uses this as the query string to send to the DNS.
3.	The APN FQDN query returns NAPTR Resource Records (RRs) with an "s" flag.
4.	Result(s) from this operation are fed to a filter where only RRs with service-parameter "x-3gpp-pgw:x-s2a-gtp" are considered by the MRME service.
5.	Each of the resulting NAPTR RRs for that record set will be resolved further by performing DNS SRV queries using the replacement string pointed to by the NAPTR RRs.
6.	The MRME service receives a list of P-GW FQDNs from the DNS. After all the SRV queries are completed, the MRME service builds a candidate list of P-GW host names.
7.	The resulting P-GW entries are compared against the configured MRME service FQDN and the longest suffix-matching entry is chosen. If there are more than one pair of MRME service/P-GW combinations with the same degree of label match, attributes from the RR may be used to break the tie. The attributes include priority, weight, and order. Load-balancing of P-GWs occur based on weight, as per the procedure defined in RFC 2782.

Step	Description
8.	The selected P-GW FQDN is further resolved using a DNS A/AAAA query to resolve to the IPv4/IPv6 address of the S2a interface on the P-GW.
9.	The DNS returns the IP address of the P-GW.

Topology/Weight-based Selection

Topology/weight-based selection uses DNS requests to enable P-GW load balancing based on topology and/or weight.

For topology-based selection, once the DNS procedure outputs a list of P-GW hostnames for the APN FQDN, the SaMOG Gateway performs a longest-suffix match and selects the P-GW that is topologically closest to the SaMOG Gateway and subscriber. If there are multiple matches with the same suffix length, the Weight and Priority fields in the NAPTR resource records are used to sort the list. The record with the lowest number in the Priority field is chosen first, and the Weight field is used for those records with the same priority.

For weight-based selection, once the DNS procedure outputs a list of P-GW hostnames for the APN FQDN, if there are multiple entries with same priority, calls are distributed to these P-GWs according to the Weight field in the resource records. The Weight field specifies a relative weight for entries with the same priority. Larger weights are given a proportionately higher probability of being selected. The SaMOG Gateway uses the value of (65535 minus NAPTR preference) as the statistical weight for NAPTR resource records in the same way as the SRV weight is used for SRV records, as defined in RFC 2782.

When both topology-based and weight-based selection are enabled on the SaMOG Gateway, topology-based selection is performed first, followed by weight-based selection. A candidate list of P-GWs is constructed based on these, and the SaMOG Gateway selects a P-GW from this list for call establishment. If the selected P-GW does not respond, the MRME service selects the alternate P-GW(s) from the candidate list.

Local P-GW Selection

The SaMOG Gateway can configure and use local P-GW addresses either as a fall-back selection method to static and dynamic P-GW selection, or as the preferred selection method.

For more information, refer SaMOG Local P-GW Selection, on page 239

P-GW Selection Fall-back

The SaMOG Gateway currently supports the following P-GW selection mechanisms:

- AAA server provided P-GW address (static selection)
- DNS provided P-GW address for P-GW FQDN resolution (static selection)
- DNS provided P-GW addresses for APN FQDN resolution (dynamic selection)
- Locally configured P-GW addresses

When the AAA server provided P-GW address or DNS provided P-GW address for P-GW FQDN (static selection) fails, the SaMOG Gateway will perform P-GW selection using the following mechanisms over an S2a GTPv2 interface:

- Locally configured P-GW address
- DNS resolution using APN FQDN (dynamic selection)

The order of the P-GW fall-back selection mechanism can be configured using the **pgw-selection local-configuration-preferred** command under the MRME Service Configuration Mode. When this command is enabled, SaMOG first uses the locally configured P-GW addresses to fall-back to. When the locally configured P-GW addresses are not reachable, SaMOG then uses APN FQDN based P-GW address resolution. When this command is not enabled, SaMOG first uses APN FQDN based P-GW address resolution to fall-back to. When the P-GW address resolved using APN FQDN is not reachable, SaMOG then uses the locally configured P-GW addresses.

The SaMOG Gateway can also be configured with the maximum alternate P-GW attempts using the **gateway-selection max-alternate-pgw** *maximum_pgw_addresses* command under the APN Profile Configuration Mode. When the maximum alternate P-GW attempts is reached, P-GW addresses will not be resolved even if the next resolved address is reachable.

When a P-GW address or addresses are configured under the respective APN Profile Configuration Mode, the following table provides the various P-GW selection fall-back scenarios over a GTPv2 interface:

SL No.	pgw-selection local-configuration-preferred Enabled?	pgw-selection fallback pgw-id Enabled?	AAA - Address Location Type	Behavior
1	Yes/No	No	P-GW IP Address	If the P-GW address is not reachable, session setup is terminated. No fall-back occurs.
2	Yes/No	No	P-GW FQDN	SaMOG Gateway performs DNS resolution on the P-GW FQDN. If the resolved P-GW address is not reachable, session setup is terminated. No fall-back occurs.
3	Yes	Yes	P-GW IP Address	If the P-GW address is not reachable, SaMOG Gateway tries to establish session with the locally configured P-GW addresses. If the locally configured P-GW addresses are not reachable, SaMOG Gateway performs DNS resolution based on APN FQDN, and tries to establish session with the resolved P-GW addresses.

SL No.	pgw-selection local-configuration-preferred Enabled?	pgw-selection fallback pgw-id Enabled?	AAA - Address Location Type	Behavior
4	No	Yes	P-GW IP Address	If the P-GW address is not reachable, SaMOG Gateway performs DNS resolution based on APN FQDN, and tries to establish session with the resolved P-GW addresses. If the addresses resolved using APN FQDN are not reachable, SaMOG Gateway tries to establish session with the locally configured P-GW addresses, if available.
5	Yes	Yes	P-GW FQDN	SaMOG Gateway performs DNS resolution on the provided P-GW FQDN, and tries to establish session. If the address resolved using P-GW FQDN is not reachable, SaMOG Gateway tries to establish session with the locally configured P-GW addresses. If the locally configured P-GW addresses are not reachable, SaMOG Gateway performs DNS resolution based on APN FQDN, and tries to establish session with the resolved P-GW addresses.
6	No	Yes	P-GW FQDN	If the addresses resolved using APN FQDN are not reachable, SaMOG Gateway tries to establish session with the locally configured P-GW addresses, if available.

SL No.	pgw-selection local-configuration-preferred Enabled?	pgw-selection fallback pgw-id Enabled?	AAA - Address Location Type	Behavior
7	No	No/Yes	P-GW Dynamic Allocation (APN FQDN)	SaMOG Gateway performs DNS resolution based on APN FQDN, and tries to establish session with the resolved P-GW addresses. If the addresses resolved using APN FQDN are not reachable, SaMOG Gateway tries to establish session with the locally configured P-GW addresses, if available.
8	Yes	No/Yes	P-GW Dynamic Allocation (APN FQDN)	SaMOG Gateway tries to establish session with the locally configured P-GW addresses. If the locally configured P-GW addresses are not reachable, SaMOG Gateway performs DNS resolution based on APN FQDN, and tries to establish session with the resolved P-GW addresses.

GGSN Selection—MRME

The SaMOG Gateway uses the Gn' reference point between the SaMOG and GGSN. The SaMOG (acting like an SGSN) initiates the creation of PDP context a GTP tunnel with the GGSN for each UE. The SGTP is compliant to Release 7 for GTPv1 specification 29.060. The GGSN selection is based on the DNS query.

The GGSN node is selected as per the 3GPP standard for resolving the IP address using DNS query. The DNS query contains the dns-apn string in the form of ***<apn-name>.mncXXX.mccYYY.gprs***, and the apn-name is obtained from AAA-Server during Access-Accept message. The MCC and MNC values are derived in the following priority:

- From the NAI sent by UE in Access-Request message in the form of ***IMSI@wlan.mncXXX.mccYYY.3gppnetwork.org***.
- Local configuration

When SaMOG interacts with pre-release 7 network elements (RADIUS based interfaces) it uses A/AAA queries. When SaMOG interacts with post-release 7 network elements (Diameter based interfaces) it uses the NAPTR queries.

RADIUS Accounting Proxy—MRME

The SaMOG Gateway's MRME service proxies RADIUS accounting messages to a RADIUS accounting server and selects the server based on an IMSI range. Upon receiving an Accounting Stop message, the MRME service clears the subscriber session.

RADIUS Authentication Server—MRME

The SaMOG Gateway's MRME service terminates RADIUS authentication requests. IEEE 802.1X authenticators will function as RADIUS clients and generate Access Request messages to authenticate and authorize the WLAN UEs.

RADIUS Disconnection—MRME

The SaMOG Gateway's MRME service generates RADIUS disconnect messages that are sent to the WLCs over IPv4 or IPv6 transport for network or AAA initiated detach and admin disconnections. For a network initiated detach, the SaMOG Gateway's MRME service sends a RADIUS disconnect message to the WLC as per RFC 3576, which is the RADIUS client. Disconnect Message transactions between the WLC and SaMOG are authenticated using a shared secret mechanism. Statistics for these RADIUS disconnect messages can be retrieved via. bulk statistics or the output of CLI show commands.

Reauthorization Support—MRME

The SaMOG Gateway's MRME service uses an STa interface re-authorization procedure between the 3GPP AAA server and the trusted non-3GPP access network to enable the 3GPP AAA server to modify previously-provided authorization parameters, which may occur due to a modification of a subscriber profile in the HSS.

RADIUS Client Authentication—MRME

Transactions between the RADIUS client and the RADIUS server are authenticated through the use of a shared secret. To authenticate Access Request messages containing the EAP-Message attribute, the SaMOG Gateway's MRME service uses the Message-Authenticator as defined in RFC 3579. The Message-Authenticator is an HMAC-MD5 hash of the entire Access-Request packet, including Type, ID, Length and Authenticator attributes, using the shared secret as the key, as follows: Message-Authenticator = HMAC-MD5 (Type, Identifier, Length, and Request Authenticator attributes).

NAS-Identifier Support—MRME

SaMOG supports the RADIUS attribute "NAS-Identifier" in the RADIUS Authentication and Accounting messages, as defined by RFC 2865. The Access point/WLC can include the NAS-Identifier AVP either in the Authentication or Accounting messages (Start/Interim). SaMOG supports NAS-Identifier value as a 64-byte string value and validates string formats only. SaMOG includes the "NAS-Identifier" attribute in the Disconnect Message towards the WLC/Access point (if received from WLC) during UE (DHCP-release) initiated detach and network initiated disconnect procedures or admin clear.

TWAP Triggered PDN—MRME

With StarOS Release 18 and later, the Trusted WLAN AAA Proxy (TWAP) sends the Layer 2 attach trigger to the Trusted WLAN Access Gateway (TWAG) (with the MAC address and subscription data of the UE) after a successful EAP authentication. The SaMOG Gateway waits until a tunnel is established for S2a/Gn procedures before forwarding the EAP Success message to the UE.

For an EoGRE access-type, the IP address of the UE is communicated using tunneled DHCP procedure.

For L3IP access-type, the IP address of the UE is communicated using out-of-band DHCP.

For call flow information, refer SaMOG Gateway Session Establishment (StarOS Release 18 and later), on page 32 for PMIPv6 access-type, and SaMOG Gateway EoGRE Session Establishment (StarOS Release 18 and later), on page 51 for EoGRE access-type.

Network Deployment and Interfaces

The SaMOG Gateway provides IP access from the WLAN UEs to the P-GW and the Packet Data Network (PDN) in the Evolved Packet Core (EPC) network. From Release 16.0 and above, the SaMOG Gateway provides IP access from the WLAN UEs to GGSN/P-GW and the Packet Data Network (PDN) over PMIPv6 or EoGRE tunnel.

Deployment Scenarios

Operators deploying SaMOG in their WLAN offload scheme typically fall under one of the three categories described below:

- **4G Deployments:** The operator has already upgraded their core network elements to EPC specifications and wants to use SaMOG to provide services to PLMNs which have the network devices capable of setting up 4G calls. In addition, the deployed DNS server supports the post release 7 DNS procedures (S-NAPTR queries) to resolve the P-GW address from APN/P-GW FQDN.

  A 3G subscriber can connect to an SaMOG Gateway in 4G deployment as long as the STa based AAA server is capable of fetching the 3G policy from HSS/HLR and convert the 3G profile parameters to 4G parameters as per 3GPP specification 23.401 and provide the same to the SaMOG during authentication.

- **3G Deployments:** For operators with a 3G infrastructure, and wants to use SaMOG to provide services only to 3G subscribers using RADIUS authentication with a AAA server assuming that the AAA server is capable of fetching the 3G profile from HLR/HSS and provide the same to SaMOG. The network elements of all the PLMNs served by this SaMOG are pre-release 8. The DNS server in such a network is capable of doing pre-release 8 DNS procedures only to resolve GGSN address from APN FQDN.

  A 4G subscriber can connect to an SaMOG Gateway in 3G deployment as long as the RADIUS based AAA server can fetch 4G profiles from HSS, convert the 4G profile parameters to 3G values, and provide the same to SaMOG during authentication.

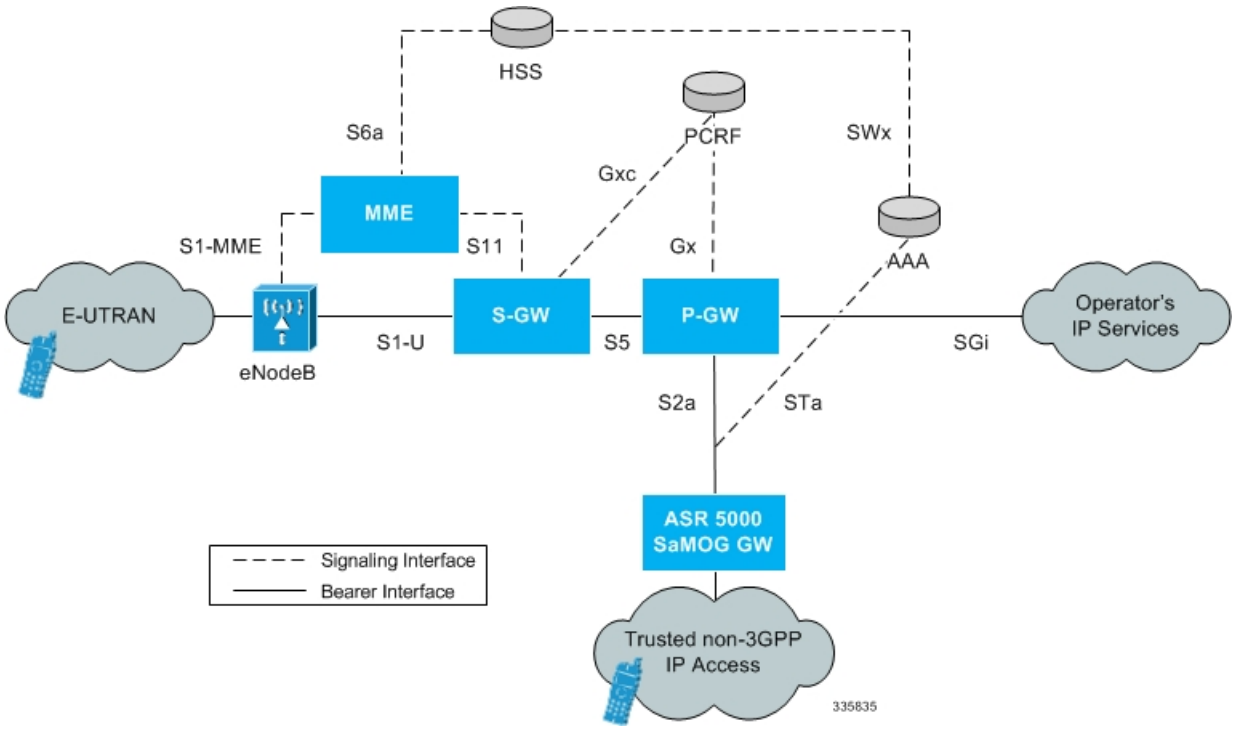
- **Mixed Mode Deployment:** For operators with infrastructure to deploy both 3G and 4G sessions, and wants to use SaMOG to provide services to both 3G and 4G subscribers.

  When a 3G/4G subscriber connects to a PLMN supporting 3G network elements, a GTPv1 session is established with GGSN for the subscriber.

  When a 3G subscriber connects to a PLMN supporting 4G network elements, if the DNS procedures result in a GGSN IP address, GTPv1 call is set for the subscriber. If the DNS query provides a P-GW, or both GGSN and P-GW interface IP address, a GTPv2 session is established with the P-GW. The AAA server will forward a 3G QoS profile or map it to a 4G QoS profile, and forward the same to SaMOG. The SaMOG Gateway converts the QoS back to 3G/4G parameters depending on whether GTPv1 or GTPv2 call is set.

The figure below shows the SaMOG Gateway terminating the WLAN interface from the trusted non-3GPP IP access network and providing access to the P-GW and the operator's IP services via GTPv2 over the S2a interface. It also shows the network interfaces used by the MME, S-GW, and P-GW in the EPC network.

Figure 4: SaMOG Gateway in the EPC Network



Network Elements

This section provides a description of the network elements that work with the SaMOG Gateway in the E-UTRAN/EPC network.

eNodeB

The evolved Node B (eNodeB) is the termination point for all radio-related protocols. As a network, E-UTRAN is simply a mesh of eNodeBs connected to neighboring eNodeBs via the X2 interface.

MME

The Mobility Management Entity (MME) is the key control node for the LTE access network. It works in conjunction with the eNodeB and the S-GW to control bearer activation and deactivation. The MME is typically responsible for selecting the P-GW for the UEs to access the PDN, but for access from trusted non-3GPP IP access networks, the SaMOG Gateway's MRME service is responsible for selecting the P-GW.

S-GW

The Serving Gateway (S-GW) routes and forwards data packets from the 3GPP UEs and acts as the mobility anchor during inter-eNodeB handovers. The S-GW receives signals from the MME that control the data traffic. All 3GPP UEs accessing the EPC network are associated with a single S-GW.

P-GW

The Packet Data Network Gateway (P-GW) is the network node that terminates the SGi interface towards the PDN. The P-GW provides connectivity to external PDNs for the subscriber UEs by being the point of entry and exit for all subscriber UE traffic. A subscriber UE may have simultaneous connectivity with more than one P-GW for accessing multiple PDNs. The P-GW performs policy enforcement, packet filtering, charging support, lawful interception, and packet screening. The P-GW is the mobility anchor for both trusted and untrusted non-3GPP IP access networks. For trusted non-3GPP IP access networks, the P-GW hosts the LMA (Local Mobility Anchor) function for the PMIP-based S2b interface, and the SaMOG Gateway's CGW service hosts the LMA function for the PMIP/EoGRE-based S2a interface.

GGSN

The GGSN works in conjunction with Serving GPRS Support Nodes (SGSNs) within the network and routes data traffic between the subscriber's Mobile Station (MS) and a Packet Data Networks (PDNs) such as the Internet or an intranet. GGSN can be configured to support Mobile IP and/or Proxy Mobile IP data applications to provide mobility for subscriber IP PDP contexts. When supporting these services, the system can be configured to either function as a GGSN and Foreign Agent (FA), a standalone Home Agent (HA), or a GGSN, FA, and HA simultaneously within the carrier's network.

3GPP AAA Server

The 3GPP Authentication, Authorization, and Accounting (AAA) server provides UE authentication via the Extensible Authentication Protocol - Authentication and Key Agreement (EAP-AKA) authentication method.

HSS

The Home Subscriber Server (HSS), is the master user database that supports the IP Multimedia Subsystem (IMS) network entities. It contains subscriber profiles, performs subscriber authentication and authorization, and provides information about the subscriber's location and IP information.

PCRF

The PCRF (Policy and Charging Rules Function) determines policy rules in the IMS network. The PCRF operates in the network core, accesses subscriber databases and charging systems, and makes intelligent policy decisions for subscribers.

Trusted Non-3GPP IP Access

The trusted non-3GPP IP access contains one or more WLAN access points. An access point terminates the UE's WLAN IEEE 802.11 link defined in IEEE standard 802.11-2007.

Logical Network Interfaces

The following table provides descriptions of the logical network interfaces supported by the SaMOG Gateway in the EPC network.

Table 3: Logical Network Interfaces on the SaMOG Gateway

Interface	Description
WLAN Interface	The interface to the WLCs and WLAN UEs in the trusted non-3GPP IP access network has not yet been defined in the 3GPP standards. The SaMOG Gateway uses Remote Access Dial In User Service (RADIUS) messages generated by the IP access network to provide session information such as the IP addresses of the WLAN UEs to the EPC network via the WLCs and to set up the access side associations.
STa Interface	The interface from the SaMOG Gateway's MRME service to the 3GPP AAA server, the STa interface is used for WLAN UE authentication. It supports the transport of mobility parameters, tunnel authentication, and authorization data. The EAP-AKA, EAP-SIM, and EAP-AKA' methods are used for authenticating the WLAN UEs over this interface.
S2a Interface	The interface from the SaMOG Gateway's CGW service to the GGSN/P-GW, the S2a interface runs the GTPv1/GTPv2 protocol to establish WLAN UE sessions with the GGSN/P-GW.

IPv6 and Dual-Stack (IPv4v6) Support

The SaMOG Gateway supports IPv6 and dual-stack (IPv4v6) address allocation for trusted Wi-Fi subscribers on the EPC core. This enables SaMOG Gateway to support a rapidly increasing number of subscribers accessing the internet via. mobile devices, and technologically advanced (example, Internet of Things) internet-enabled devices (sensors, machine-readable identifiers) that demand high network address assignment.

S2a GTPv2 Interface Towards the P-GW

SaMOG provides seamless mobility between the 3GPP EPC network and WLANs for EPS (Evolved Packet System) services via. GTPv2-based S2a interface using IPv4 and IPv6 addresses over the EoGRE and PMIPv6 access types. SaMOG can bind IPv4 and IPv6 addresses in the EGTP and GTPU services associated with the CGW service. SaMOG DNS can query P-GW IPv6 addresses and support static IPv6 address allocation from the AAA server.

Important Dual-stack (IPv4v6) bind address is currently not supported.

Supported Transport Combinations

The following table lists the supported IP transport combinations between P-GW and the EGTP service over the S2a GTPv2 interface.

P-GW Address (from DNS/AAA)	EGTP Bind Address	Session Transport Type
IPv4	IPv4	IPv4-C/ IPv4-Data
IPv6	IPv4	No session established
IPv4	IPv6	No session established
IPv6	IPv6	IPv6-C/ IPv6-Data
IPv4	IPv4v6	Dual-stack bind address not supported
IPv6	IPv4v6	Dual-stack bind address not supported

Supported EGTP Bind Addresses

Bind Address (EGTP Service)	Supported by SaMOG
Single IPv4 Address	Yes
Single IPv6 Address	Yes
Multiple IPv4 address	No
Multiple IPv6 address	No
Mix of IPv4 and IPv6 address	No

Supported GTPU Bind Addresses

Bind Address (GTPU Service)	Supported by SaMOG
Single IPv4 Address	Yes
Single IPv6 Address	Yes
Multiple IPv4 address	No
Multiple IPv6 address	No
Mix of IPv4 and IPv6 address	No

Access Types

Important In Release19, IPv6 transport using the PMIPv6 access type is supported as lab quality only.

The SaMOG gateway supports IPv6 transport for trusted Wi-Fi subscribers on the EPC core using the PMIPv6 and EoGRE access types. The access side peers (WLC/AP) and SaMOG communicate over an IPv6 transport, and data travels over the GRE tunnel between the IPv6 endpoints.

Limitations

- Though dual-stack binding is supported by the CGW service, only IPv6 transport is used for a PMIPv6 access type when a dual-stack configuration exists. To use both IPv4 and IPv6 tranports for the PMIPv6 access type, configure two different SaMOG contexts, one context for IPv4 CGW service binding, and the other context for an IPv6 CGW service binding.

Subscriber User Equipment (UE)

SaMOG can support IPv6 or dual-stack (IPv4v6) address allocation for both SIM and non-SIM (non-UICC) based subscriber's user equipment (UE) on the trusted Wi-Fi network. This is achieved using an external P-GW for SIM-based devices, and internal P-GW (Local Breakout - Heavy) for non-SIM-based devices to provide access to the EPC core. In this release, SaMOG supports IPv6/IPv4v6 address allocation over PMIPv6 and EoGRE access types along with GTPv2-based S2a interface.

Accepted PDN-Type for IPv4, IPv6, and IPv4v6 Subscribers on PMIPv6 and EoGRE Access Types

AAA Provided PDN-Type (Subscribed PDN-Type)	P-GW Provided PDN-Type	UE Requested PDN-Type	
		Requested by UE	Accepted by SaMOG
v6	v6	v6, v4v6	v6
v4	v4	v4, v4v6	v4
v4v6	v4	v4, v4v6	v4
	v6	v4, v4v6	v6
	v4v6	v4v6	v4v6

Inter-MAG Handoff for IPv4, IPv6, and IPv4v6 Subscribers Over PMIPv6 Access Type

UE Req WLC1	SaMOG v4	SaMOG v6	SaMOG v4v6
v4	PBA (v4)	Rejected Earlier v6 call continues	PBA (v4)
Handover WLC2			
v6	Rejected	No call	PBA (v6) send BRI to earlier MAG
v4v6	PBA (v4), send BRI to earlier MAG	No call	PBA (v4v6) send BRI to earlier MAG
v6	Rejected Earlier v4 call continues	PBA (v6)	PBA (v6)
Handover WLC2			
v4	No call	Rejected Earlier v6 call continues	PBA (v4) send BRI to earlier MAG

UE Req WLC1	SaMOG v4	SaMOG v6	SaMOG v4v6
v4v6	No call	PBA (v6) send BRI to earlier MAG	PBA (v4v6) send BRI to earlier MAG
v4v6	PBA (v4)	PBA (v6)	PBA (v4v6)
Handover WLC2			
v4	PBA (v4), BRI to old	Rejected Earlier v6 call continues	PBA (v4), BRI to old
v6	Rejected Earlier v4 call continues	PBA (v6), BRI to old	PBA (v6), BRI to old

Unsolicited Router Advertisement and Deprecation of IPv6 Prefix

SaMOG supports sending unsolicited router advertisements (RA) for the EoGRE access type.

IPv6 Prefix Advertisement

SaMOG can send unsolicited RA with a newly allocated IPv6 prefix when a session is established, and the AAA server has authorized the IPv6 or IPv4v6 PDN type for the session without waiting for an RS message from the UE.

The total number of retries and retry interval for RA to advertise an IPv6 prefix can be configured using the **ipv6 unsolicited-router-advt advertise** command under the APN Profile Configuration mode.

IPv6 Prefix Deprecation

SaMOG sends an RA with the preferred and valid lifetime as 0 to deprecate the IPv6 prefix in the following scenarios:

- When the network, SaMOG or the AAA server triggers a disconnect for an IPv6 or IPv4v6 PDN-type session.
- When a session receives an IPv6 packet with an old prefix (prefix that does not match the currently allocated prefix for the session), and the AAA server has authorized an IPv6 or IPv4v6 PDN-type for the session.

The total number of retries and retry interval for RA to deprecate an IPv6 prefix can be configured using the **ipv6 unsolicited-router-advt deprecate** command under the APN Profile Configuration mode.

DNS Support Over the IPv4 and IPv6 Transport

The SaMOG Gateway can perform SNAPTR, SRV, A/AAAA-based DNS queries towards the DNS server over the IPv4 or IPv6 transport to get the P-GW IP address.

The following are some use cases to resolve the P-GW IP address between the SaMOG Gateway and the DNS server:

- On an IPv4, IPv6 or IPv4v6 PDN, when the AAA server forwards the PGW-Allocation-Type value as Dynamic and Destination-Host, the DNS server responds with the P-GW IPv4 address.

The SaMOG Gateway performs SNAPTR DNS queries over the IP transport with the P-GW FQDN based on the Destination-Host received from the AAA Server to successfully resolve the P-GW IPv4 address.

- On an IPv4, IPv6 or IPv4v6 PDN, when the AAA server forwards the PGW-Allocation-Type value as Dynamic with no Destination-Host, the DNS server responds with the P-GW IPv6 address.

  The SaMOG Gateway performs SNAPTR DNS queries over the IP transport with the APN FQDN to successfully resolve the P-GW IPv6 address.

- On an IPv4, IPv6 or IPv4v6 PDN, when the AAA server forwards the PGW-Allocation-Type value as Dynamic and Destination-Host, the DNS server responds with more than one P-GW IPv4 addresses with different weights and priorities.

  The SaMOG Gateway performs SNAPTR DNS queries over the IP transport with the P-GW FQDN based on the Destination-Host received from the AAA Server, and selects the P-GW IPv4 address with the highest priority.

- On an IPv4, IPv6 or IPv4v6 PDN, when the AAA server forwards the PGW-Allocation-Type value as Dynamic and Destination-Host, the DNS server responds with more than one P-GW IPv6 addresses with different weights and priorities.

  The SaMOG Gateway performs SNAPTR DNS queries over the IP transport with the P-GW FQDN based on the Destination-Host received from the AAA Server, and selects the P-GW IPv6 address with the highest priority.

- On an IPv4, IPv6 or IPv4v6 PDN, when the AAA server forwards the PGW-Allocation-Type value as Dynamic and Destination-Host, the DNS server responds with P-GW IPv6 and IPv4 addresses with different weights and priorities.

  The SaMOG Gateway performs SNAPTR DNS queries over the IP transport with the P-GW FQDN based on the Destination-Host received from the AAA Server, and selects the P-GW IP address with the highest priority.

Transport Combinations

The table below lists the IPv4, IPv6 and IPv4v6 transport combinations for the SaMOG Gateway, and whether each combination is supported for deployment in this release.

Table 4: Transport Combinations for the SaMOG Gateway

IP Address Allocated by the P-GW for the WLAN UEs	RADIUS Authentication and Accounting (between the WLCs and the SaMOG Gateway)	PMIPv6 Interface (between the WLCs and the SaMOG Gateway)	EoGRE Interface (between the WLCs and the SaMOG Gateway)	Is this Combination Supported for Deployment?
IPv4	IPv4 IPv6	IPv4 IPv6 (Lab quality in Release 19)	IPv4 IPv6	Yes

IP Address Allocated by the P-GW for the WLAN UEs	RADIUS Authentication and Accounting (between the WLCs and the SaMOG Gateway)	PMIPv6 Interface (between the WLCs and the SaMOG Gateway)	EoGRE Interface (between the WLCs and the SaMOG Gateway)	Is this Combination Supported for Deployment?
IPv6	IPv4 IPv6	IPv4 IPv6 (Lab quality in Release 19)	IPv4 IPv6	Yes
IPv4v6	IPv4 IPv6	IPv4 IPv6 (Lab quality in Release 19)	IPv4 IPv6	Yes

Important In this release, SaMOG does not support IPv6 transport for PMIPv6 and L3IP access types.

How the SaMOG Gateway Works

This section describes the SaMOG Gateway during session establishment and disconnection.

SaMOG Gateway Session Establishment (StarOS Release 17 and earlier)

The figure below shows an SaMOG Gateway session establishment flow in Release 17 and earlier. The table that follows the figure describes each step in the flow.

Figure 5: SaMOG Gateway Session Establishment

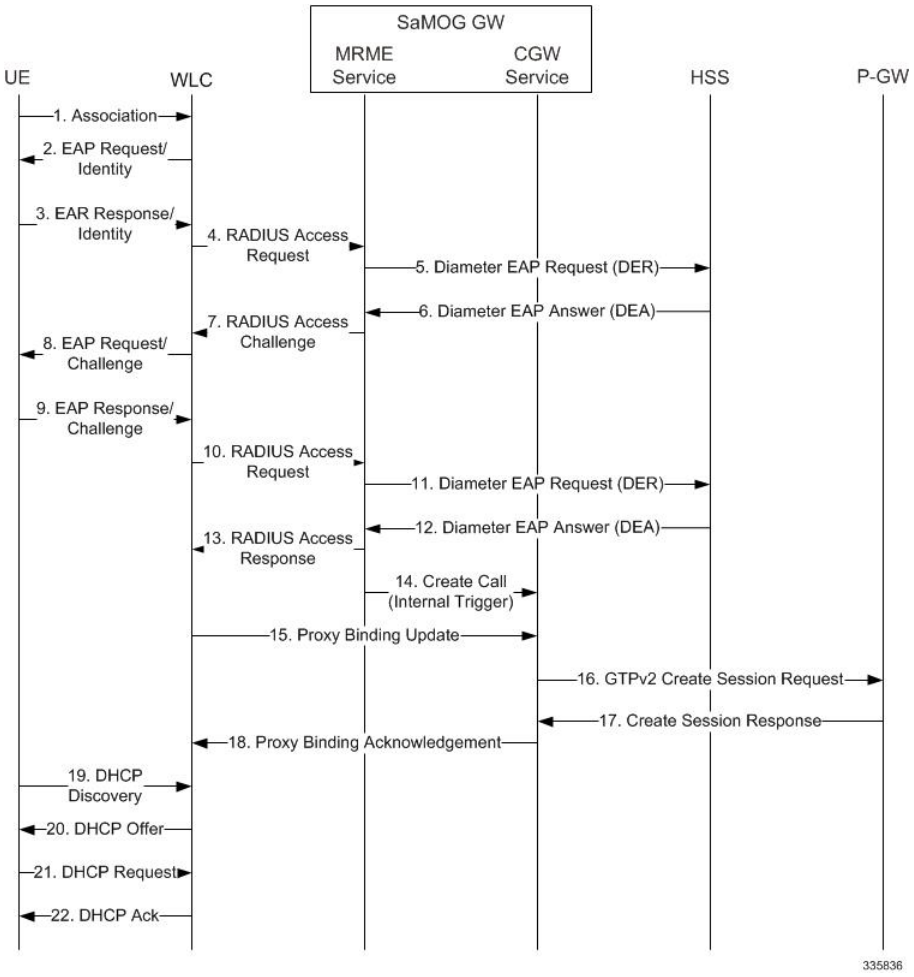


Table 5: SaMOG Gateway Session Establishment

Step	Description
1.	An association between the UE and WLC is established.
2.	The initial attach procedure starts with the authenticator sending an EAP Request/Identity message toward the supplicant.
3.	The UE responds to the EAP Request/Identity message with an EAP Response/Identity message, which contains the permanent identity (IMSI) on the SIM.

Step	Description
4.	The WLC requests MRME for authentication using EAP over RADIUS by sending an "Access- Request" message. The WLC includes the User-Name, EAP-Identity as part of the EAP-Message, Acct-Session-Id in the "Access-Request" message.
5.	The MRME initiates Authentication and Authorization procedures by sending "Diameter EAP Request" message to the 3GPP AAA Server, containing the user identity and EAP-Payload.
6.	The 3GPP AAA Server fetches the user profile and authentication vectors from the HSS/HLR (if these parameters are not available in the 3GPP AAA Server). The 3GPP AAA Server looks for the IMSI of the authenticated user based on the received user identity (root NAI or Decorated NAI), and includes the EAP-AKA as the requested authentication method in the request sent to the HSS. The HSS then generates authentication vectors and sends them back to the 3GPP AAA server. The 3GPP AAA Server checks if the user's subscription is authorized for a trusted non-3GPP access. The 3GPP AAA Server initiates the authentication challenge. The user identity is not requested again.
7.	The MRME responds to WLC with a "Radius Access-Challenge" message by including EAP-AKA AKA-Challenge in the EAP-Messages.
8.	WLC sends an authentication challenge towards the UE.
9.	The UE responds with a challenge response.
10.	The WLC forwards the "Radius Access-Request" by including EAP-Response/AKA-Challenge in the EAP-Message to MRME.
11.	The MRME forwards the EAP-Response/AKA-Challenge message to the 3GPP AAA Server by sending a "Diameter EAP Request" message. The AAA Server checks if the authentication response is correct.

Step	Description
12.	The 3GPP AAA Server forwards the final Authentication and Authorization answer by initiating "Diameter EAP Answer" (with a result code indicating success) including the relevant service authorization information, an EAP success and the key material to the MRME. The MRME performs P-GW Resolution (Steps 13-16) for dynamic P-GW selection by delaying the EAP-Response (Access-Accept) message to the WLC.
13.	The MRME sends a "DNS Request" with S-NAPTR Query by constructing an APN FQDN to the DNS Server.
14.	The MRME receives a "DNS Answer" with a list of A-Records from the DNS Server.
15.	The MRME sends a "DNS Request" by including the selected A-Record to get the P-GW IPv4 address.
16.	The MRME receives the resolved P-GW IPv4 address in the "DNS Response" from the DNS Server.
17.	The MRME sends the "Radius Access-Accept" message to the WLC by including the Shared Secret generated in the EAP exchange, and the User-Name.
18.	The WLC originates the "PMIPv6 Proxy-Binding-Update" message to the CGW. The information for the subscriber to form the PBU message is included. In addition, WLC also allocates a GRE tunnel ID for downlink data transfer, and includes it in the PBU message.
19.	The CGW originates a "GTPv2 Create Session Request" message on the S2a interface towards PDN-GW, by including S2a GTP-U TEID to be used for downlink data transfer, MSISDN, IMSI, APN, PAA, PDNType, Bearer-Context-List, APN-AMBR and Charging characteristic.
20.	The PDN-GW allocates the requested IP address for the subscriber and responds to the CGW with a "GTPv2 Create Session Response" message by including the Cause, PAA, Bearer-Context-List, APN-AMBR and GTP-U PGW TEID for uplink data transfer.
21.	The CGW responds with a "PMIPv6 PBA" to the WLC, by including the UEs IP address.

Step	Description
22.	A GTPv2 tunnel is established between the CGW and P-GW.
23.	A PMIPv6 tunnel is established between the WLC and CGW.
24.	The WLC initiates a "Radius Accounting-Request" with "Acct-Status-Type" as "Start" and by including the assigned UEs address.
25.	The MRME proxies the received "Radius Accounting-Request" towards the RADIUS accounting server.
26.	The MRME receives the "Radius Accounting-Response" from the Radius accounting server.
27.	The MRME proxies the received "Radius Accounting-Response" towards the WLC.

SaMOG Gateway Session Establishment (StarOS Release 18 and later)

The figure below shows an SaMOG Gateway session establishment flow in StarOS Release 18 and later. The table that follows the figure describes each step in the flow.

Figure 6: SaMOG Gateway Session Establishment Call Flow

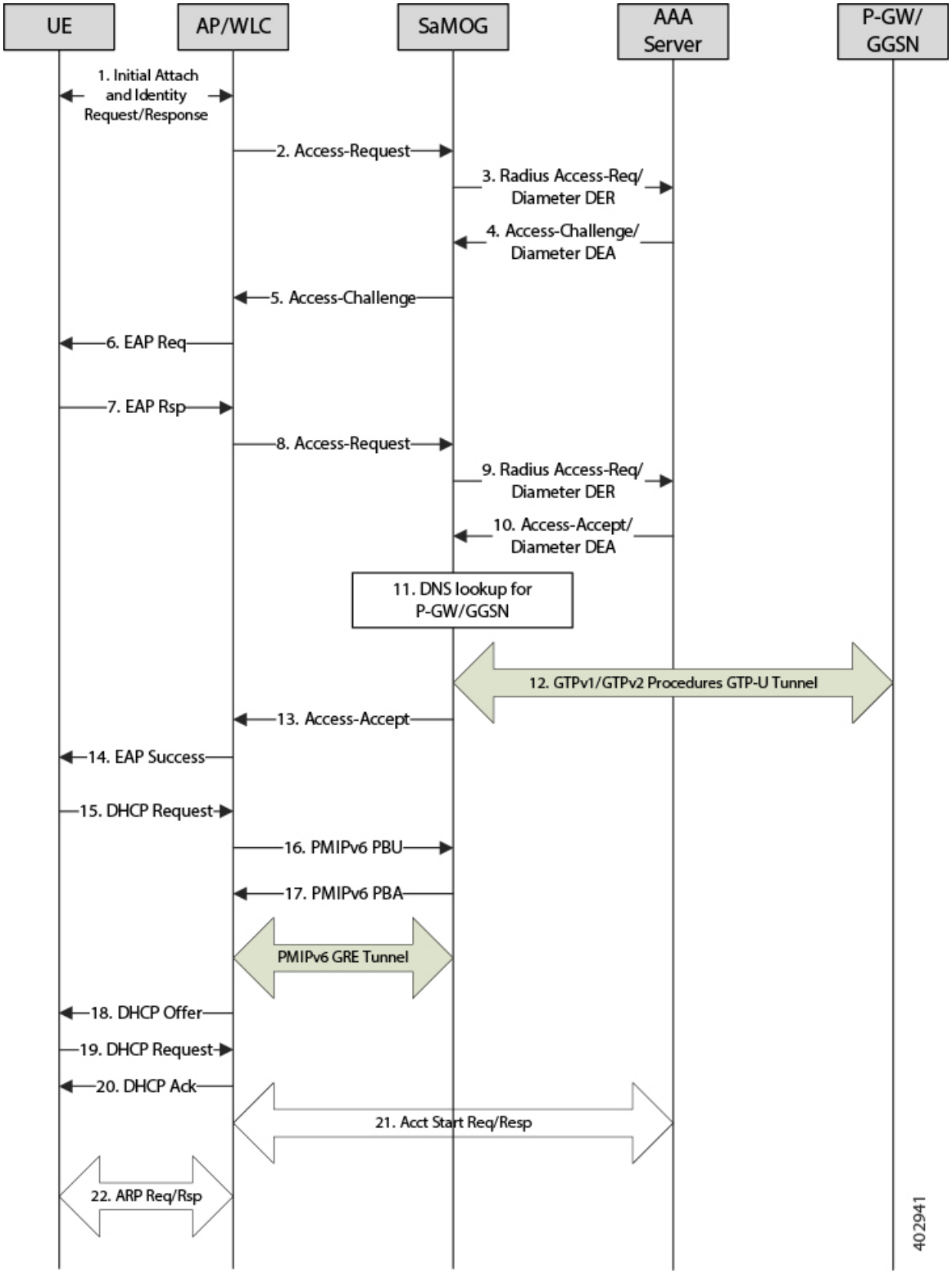


Table 6: SaMOG Gateway Session Establishment

Step	Description
1.	The UE initiates an initial attach procedure towards the WLC.
2.	The WLC forms an Access-Request message with the EAP-Identity payload, User-Name and Acct-Session-Id, and sends the same to SaMOG.
3.	SaMOG forms a Radius Access-Request or Diameter DEA message towards the AAA server using the attributes received from the WLC.
4.	The AAA server performs an EAP authentication and sends the Access-Challenge/DEA to SaMOG with the EAP payload.
5.	SaMOG copies the EAP payload to the Access-Challenge towards WLC.
6.	The WLC sends an EAP Request towards UE.
7.	The UE sends an EAP response.
8.	The WLC sends the Access-Request to SaMOG with the EAP payload received from the UE.
9.	SaMOG sends the Access-Request/DER to the AAA server with the EAP payload.
10.	The AAA server fetches the subscriber profile from HLR/HSS and validates the EAP Challenge response sent from the UE. The Access-Accept/DEA is sent to SaMOG with the user profile and EAP Success payload. SaMOG saves the user profile information.
11.	SaMOG performs DNS procedures towards the DNS server to get the P-GW/GGSN IP address.
12.	SaMOG delays sending the Access-Accept to the WLC and initiates S2a/Gn procedures towards P-GW/GGSN, by including the IMEIs V IE with the UE MAC value received as "Calling-Station-ID" AVP in the Access-Request if sending of IE is enabled (via. configuration).
13.	SaMOG sends Access-Accept to the WLC with EAP-Success payload after completion of S2a/Gn procedures.
14.	The WLC sends EAP-Success to the UE.

Step	Description
15.	The UE sends DHCP discover (broadcast) request to the WLC.
16.	The WLC acts as a DHCP server and initiates PMIPv6 PBU towards SaMOG for L3 Attachment by including the NAI and Service-Selection parameters.
17.	SaMOG will process the received PMIPv6 PBU and responds back with a PMIPv6 PBA by including the allocated home-address by P-GW/GGSN and the default gateway IP address.
18.	The WLC sends a DHCP offer towards the UE with the allocated UEs IP address and the default gateway.
19.	The UE sends DHCP request to the WLC for DHCP, by including router options and the allocated UE's IP address for further confirmation.
20.	The WLC sends DHCP Ack message to the UE.
21.	If proxy accounting is enabled, SaMOG will proxy accounting messages between the WLC and AAA server.
22.	The UE performs ARP request for the default gateway received from SaMOG. The WLC includes the virtual MAC address in the ARP response for the received Default gateway IP address in the ARP.

SaMOG Gateway IPv6 prefix Over PMIPv6 Using Stateless Address Auto-configuration (SLAAC)

The figure below shows the message flow to delegate an IPv6 prefix to the user equipment (UE) using SLAAC for PMIPv6 access type.The table that follows the figure describes each step in the message flow.

Figure 7: SaMOG Gateway IPv6 prefix Over PMIPv6 Using SLAAC

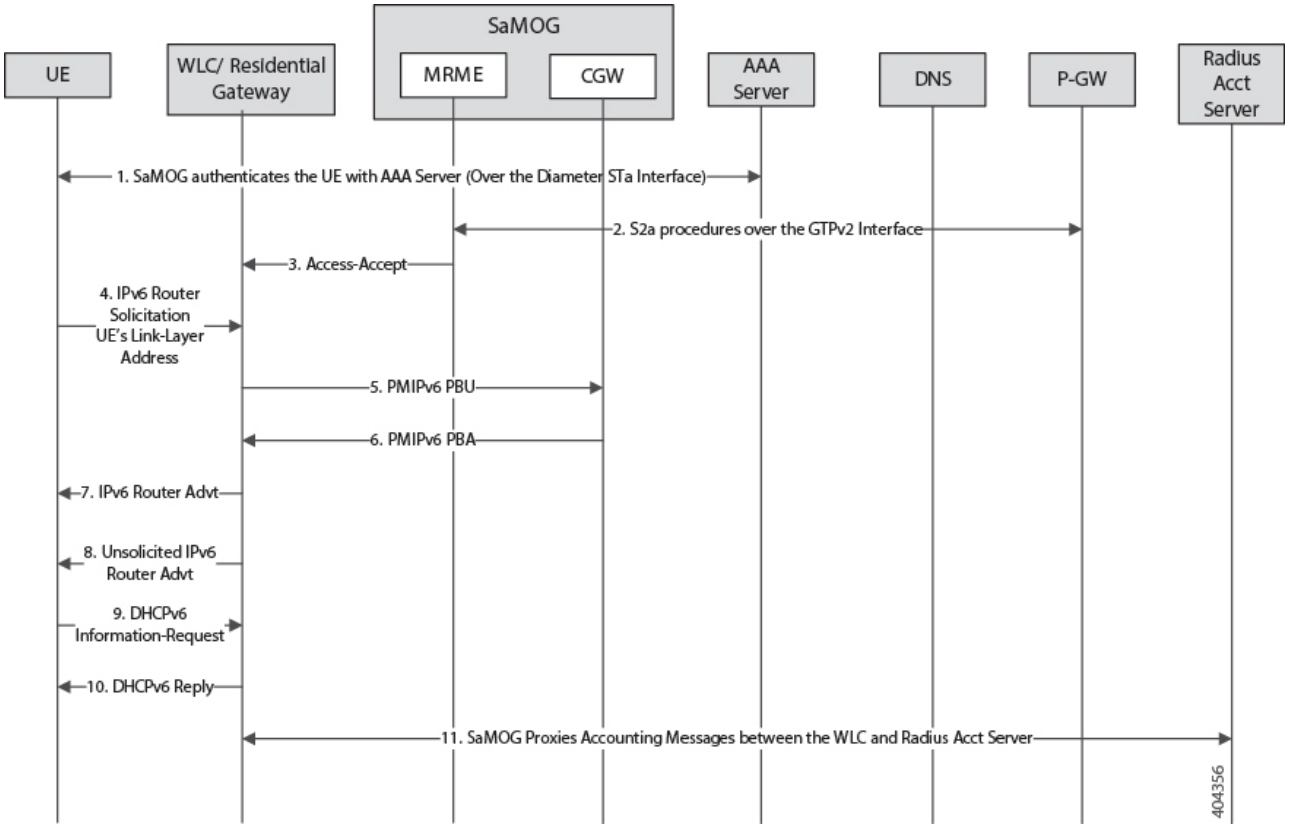


Table 7: SaMOG Gateway IPv6 prefix Over PMIPv6 Using SLAAC

Step	Description
1.	SaMOG authenticates between the UE and the AAA/Radius server via. WLC. During Authentication, SaMOG receives the PDN-Type IPv6 value as part of the APN-Profile AVP in the Diameter EAP Answer or Access-Accept message from the AAA/Radius server.
2.	After P-GW selection, SaMOG performs S2a procedures towards P-GW by including the PDN-Type, and receives the IPv6 Prefix for the subscriber's UE using S2a procedures as per APN subscription profile at P-GW
3.	SaMOG sends the Radius Access-Accept message towards WLC. SaMOG includes the PDN-Type (IPv6) in the Cisco-AVPair attribute.

Step	Description
4.	The UE sends the IPv6 ICMPv6 Router Solicitation (ICMPv6 Type 133) message to the destination as "Link-Local Scope multicast All Routers Address (ff02:2)" with the source address as UEs Link-Local address. The UE also includes the ICMPv6 option "source link-layer address", which is the MAC address of the UE.
5.	The WLC starts PMIPv6 procedures when any of the following triggers occur: • When an Access-Accept message is received from SaMOG and authentication is completed with the UE (Step 3). • When an IPv6 Router Solicitation message is received from the UE. For IPv6 Support, the WLC sends the PMIPv6 PBU towards SaMOG by including the Home Network Prefix: "::" and Link Local Address: "::".
6.	SaMOG processes the received PMIPv6 PBU and responds with a PMIPv6 PBA, by including the valid Home Network Prefix and Link Local Address provided by the P-GW during S2a procedures. SaMOG also includes the IPv6 DNS Primary/Secondary addresses in the PMIPv6 PBA message. SaMOG provides the DNS parameters in the PBA only when the WLC requests for it in the PBU. **Important**
7.	The WLC processes the received ICMPv6 Router Solicitation message over the CAP-WAP Tunnel and responds with an ICMPv6 Router Advertisement (ICMPv6 Type 134) message over CAP-WAP Tunnel towards the UE. The WLC also includes the RDNSS, DNSSL options as per *RFC 6106*.
8.	The WLC may optionally send the Unsolicited IPv6 Router Advertisement (RA) over CAP-WAP Tunnel based on the local configuration. The IPv6 options included would be same as in Step 7. **Important** For PMIPv6 access type, SaMOG silently drops unsolicited RA packets received from the WLC.

Step	Description
9.	The WLC receives the DHPCv6 Information-Request message over the CAP-WAP tunnel to fetch the configuration parameters based on the UE's behavior by including the Client-identifier and Option Request option with "DNS Recursive Name Server" and "Domain Search List".
10.	The WLC responds with a DHCPv6 Reply over the CAP-WAP Tunnel by including the "DNS Recursive Name Server" and "Domain Search List".
11.	SaMOG acts as an Accounting proxy between WLC and Radius Accounting Server where all Accounting messages will have "Framed-IPv6-Prefix" AVP.

SaMOG Gateway IPv6 prefix Over PMIPv6 using Stateful DHCPv6

The figure below shows the message flow to delegate an IPv6 prefix to the user equipment (UE) using stateful DHCPv6 for a PMIPv6 access type.The table that follows the figure describes each step in the message flow.

Figure 8: SaMOG Gateway IPv6 prefix Over PMIPv6 Using Stateful DHCPv6

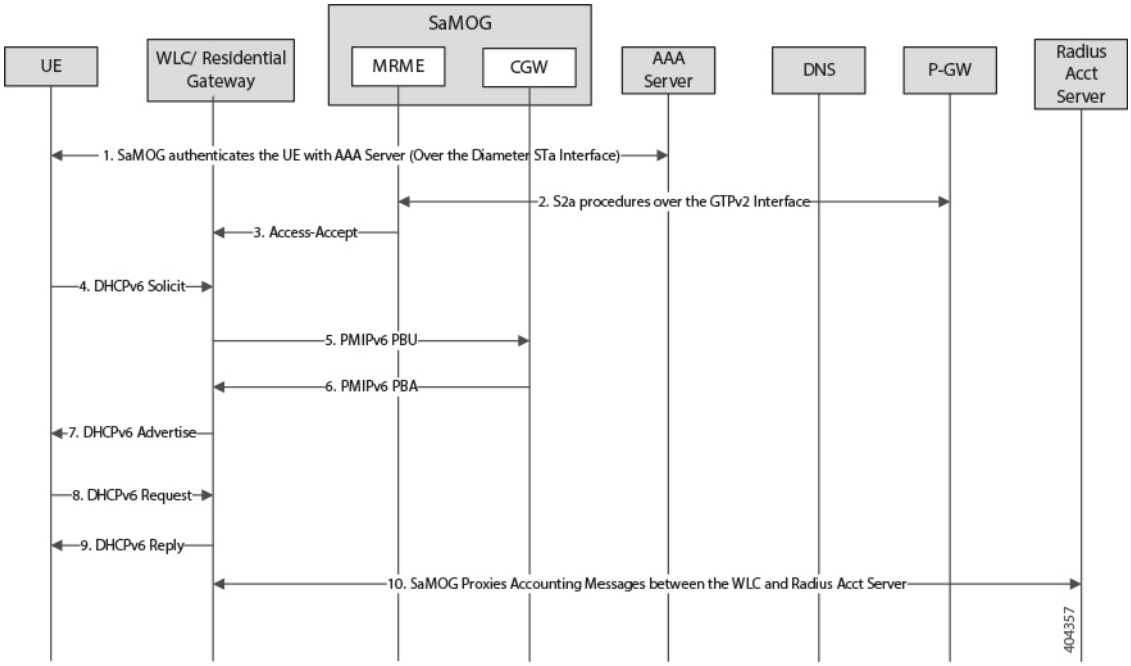


Table 8: SaMOG Gateway IPv6 prefix Over PMIPv6 Using Stateful DHCPv6

Step	Description
1.	SaMOG authenticates between the UE and the AAA/Radius server via. WLC. During Authentication, SaMOG receives the PDN-Type IPv6 value as part of the APN-Profile AVP in the Diameter EAP Answer or Access-Accept message from the AAA/Radius server.
2.	After P-GW selection, SaMOG performs S2a procedures towards GGSN/PGW by including the PDN-Type value received from the AAA/Radius server during authentication. SaMOG receives the IPv6 Prefix for the subscriber's UE using S2a procedures as per APN subscription profile at P-GW.
3.	SaMOG sends the Radius Access-Accept message towards WLC. SaMOG includes the PDN-Type (IPv6) in the Cisco-AVPair attribute.
4.	The UE sends the DHCPv6 Solicit message over the CAP-WAP tunnel by including the the Client Identifier (DUID), FQDN, Option Req:(DNSRNS Req, DNSSL Req), Elapsed Time, and IA_PD Option.
5.	The WLC starts PMIPv6 procedures when any of the following triggers occur: • When an Access-Accept message is received from SaMOG and authentication is completed with the UE (Step 3). • When a DHCPv6 Solicit message is received from the UE (Step 4). For IPv6 Support, the WLC sends the PMIPv6 PBU towards SaMOG by including the Home Network Prefix: "::" and Link Local Address: "::".
6.	SaMOG processes the received PMIPv6 PBU and responds with a PMIPv6 PBA, by including the valid Home Network Prefix and Link Local Address provided by the P-GW during S2a procedures. SaMOG also includes the IPv6 DNS Primary/Secondary addresses in the PMIPv6 PBA message.

Step	Description
7.	The WLC responds with a DHCPv6 Advertise message over the CAP-WAP tunnel by including the IA_PD (IA_PD prefix) Options, FQDN, Client Identifier, Server Identifier, Domain Search List, DNS Recursive Name Server options.
8.	The UE sends the DHCPv6 Request message over the CAP-WAP tunnel by including the Client Identifier (DUID), Server Identifier (DUID), Option Req:(DNSRNS Req, DNSSL Req), Elapsed Time, FQDN, IA_PD (IA_PD Prefix) Options.
9.	The WLC responds with a DHCPv6 Reply message over the CAP-WAP Tunnel by including the Client Identifier (DUID), Server Identifier (DUID), Elapsed Time, FQDN, IA_PD (IA_PD Prefix) Options.
10.	SaMOG acts as an Accounting proxy between WLC and Radius Accounting Server where all Accounting messages will have "Framed-IPv6-Address" AVP. **Important** For PMIPv6 access type, the SLAAC and stateful DHCPv6 process remains the same as the Radius server/DHCPv6-Inf-Req is exchanged between the UE and the WLC.

SaMOG Gateway Dual-stack Support Over PMIPv6

The table below describes the steps in the message flow for dual-stack support over PMIPv6.

Table 9: SaMOG Gateway Dual-stack Support Over PMIPv6 Using SLAAC

Step	Description
1.	Refer SaMOG Gateway IPv6 prefix Over PMIPv6 Using Stateless Address Auto-configuration (SLAAC), on page 35 and SaMOG Gateway IPv6 prefix Over PMIPv6 using Stateful DHCPv6, on page 38 for the sequence of messages between the WLC to SaMOG, and SaMOG to P-GW.
2.	SaMOG receives the PDN-Type as IPv4, IPv6, or IPv4v6 in the APN-Profile during authentication with the Radius/AAA Server.
3.	SaMOG starts S2a procedures based on the PDN-Type, towards P-GW/GGSN

Step	Description
4.	The WLC initiates PMIPv6 PBU by including the IPv4 Home Address and/or Home Network Prefix as per the received PDN-Type in the Cisco-AVPair from SaMOG.
5.	SaMOG provides the configuration parameters (DNS IPv4/IPv6 Addresses) in the PCO Mobility option of the PMIPv6 PBA.
6.	UE triggers the sequence of messages using SLAAC or Stateful DHCPv6 to get the IPv6 prefix and DHCPv4 to get the IPv4 address.

P-GW Initiated Session Disconnection

The figure below shows the message flow during a P-GW initiated session disconnection. The table that follows the figure describes each step in the message flow.

Figure 9: P-GW Initiated Session Disconnection

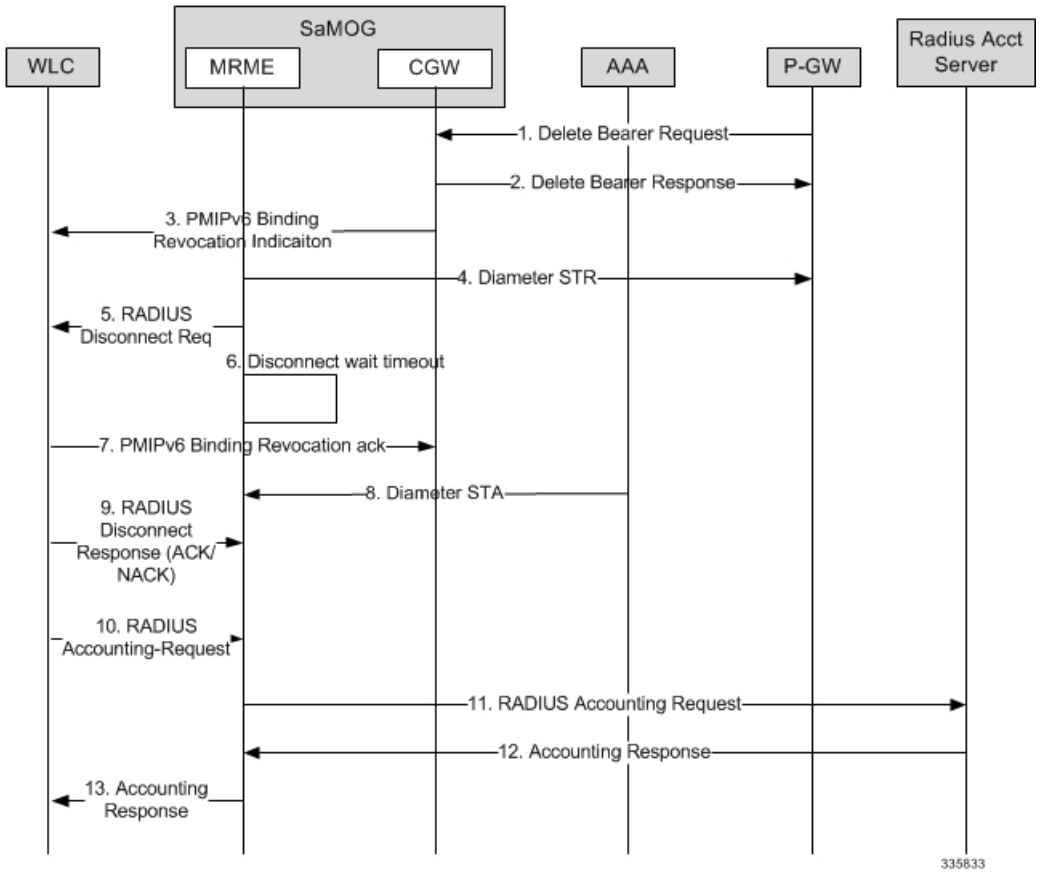


Table 10: P-GW Initiated Session Disconnection

Step	Description
1.	The P-GW initiates a "GTPv2 Delete Bearer Request" to remove the session resources from CGW.
2.	The CGW responds back with a "GTPv2 Delete Bearer Response" to P-GW.
3.	The CGW sends a "PMIPv6 Binding Revocation Indication" message to WLC to detach PMIPv6 GRE Tunnel between WLC and CGW.
4.	The MRME initiates a "Diameter Session-Termination-Request" message towards 3GPP AAA Server without waiting for GTPv2 Response procedures.
5.	The MRME also initiates a "Radius Disconnect Request" Message towards WLC to release the resources on WLC and towards UE.
6.	If the MRME had received Accounting Records for the session, then MRME initiates "Disconnect Wait Timer" to wait for "Accounting Request with Acct-Status-Type as Stop" message from WLC.
7.	The WLC responds with a "PMIPv6 Binding Revocation Ack" message to the CGW.
8.	The 3GPP AAA server responds with a "Diameter Session-Termination-Answer" message.
9.	The WLC respond back with a "Radius Disconnect Response ACK/NAK" message to the MRME. • If the MRME receives a "Radius Disconnect NAK" message, then MRME will stop the "Disconnect Wait Timer" and proceed to cleanup the call immediately. • If the MRME receives a "Radius Disconnect ACK" message, then MRME will wait for the "Accounting Stop" message based on the "Disconnect Wait Timer" value.
10.	The WLC triggers a "Radius Accounting-Request" message with "Acct-Status-Type" as "STOP" and an appropriate "Terminate-Cause".
11.	The MRME proxies the received "Radius Accounting-Request" message towards the RADIUS accounting server.

Step	Description
12.	The MRME receives the "Radius Accounting-Response" message from the RADIUS accounting server.
13.	The MRME proxies the received "Radius Accounting-Response" to the WLC.

WLC Initiated Session Disconnection

The figure below shows the message flow during a WLC initiated session disconnection. The table that follows the figure describes each step in the message flow.

Figure 10: WLC Initiated Session Disconnection

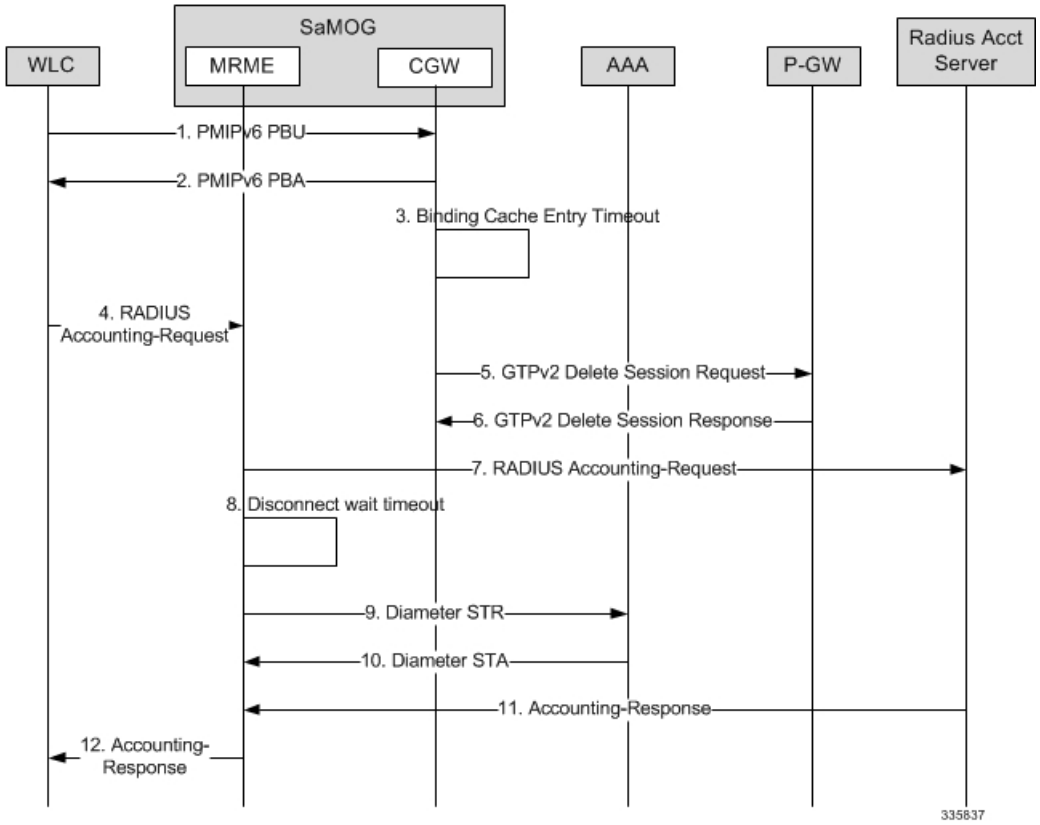


Table 11: WLC Initiated Session Disconnection

Step	Description
1.	The WLC sends a "PMIPv6 Proxy Binding Update" message with lifetime = 0 with NAI and the allocated IP-Address to the CGW.

Step	Description
2.	The CGW responds with a "PMIPv6 Proxy Binding Ack" message and cleans up the session and the associated GRE tunnel.
3.	The CGW initiates a "Binding Cache Entry" timer based on the configured "Binding Cache Entry Timeout" (session-delay-Timeout) value under the CGW Service Configuration Mode.
4.	The WLC triggers a "Radius Accounting-Request" message with the "Acct-Status-Type" as "STOP" and an appropriate "Terminate-Cause".
5.	The CGW initiates a "GTPv2 Delete Session Request" message to remove the session resources from the P-GW.
6.	The P-GW responds with a "GTPv2 Delete Session Response" message and intimates the MRME.
7.	The MRME proxies the received "Radius Accounting-Request" message to the RADIUS accounting server.
8.	The MRME service initiates a "Disconnect Delay" timer, based on the configured "Disconnect Delay Timeout" value under the MRME Service Configuration Mode.
9.	The MRME also initiates a "Diameter Session-Termination-Request" message to the 3GPP AAA server without waiting for the GTPv2 response procedures.
10.	The 3GPP AAA server responds with a "Diameter Session-Termination-Answer" message.
11.	The MRME receives the "Radius Accounting-Response" message from the RADIUS accounting server.
12.	The MRME responds to the WLC with a "Radius Accounting-Response" message.

AAA Server Initiated Session Disconnection

The figure below shows the message flow during an AAA server initiated session disconnection. The table that follows the figure describes each step in the message flow.

Figure 11: AAA Server Initiated Session Disconnection

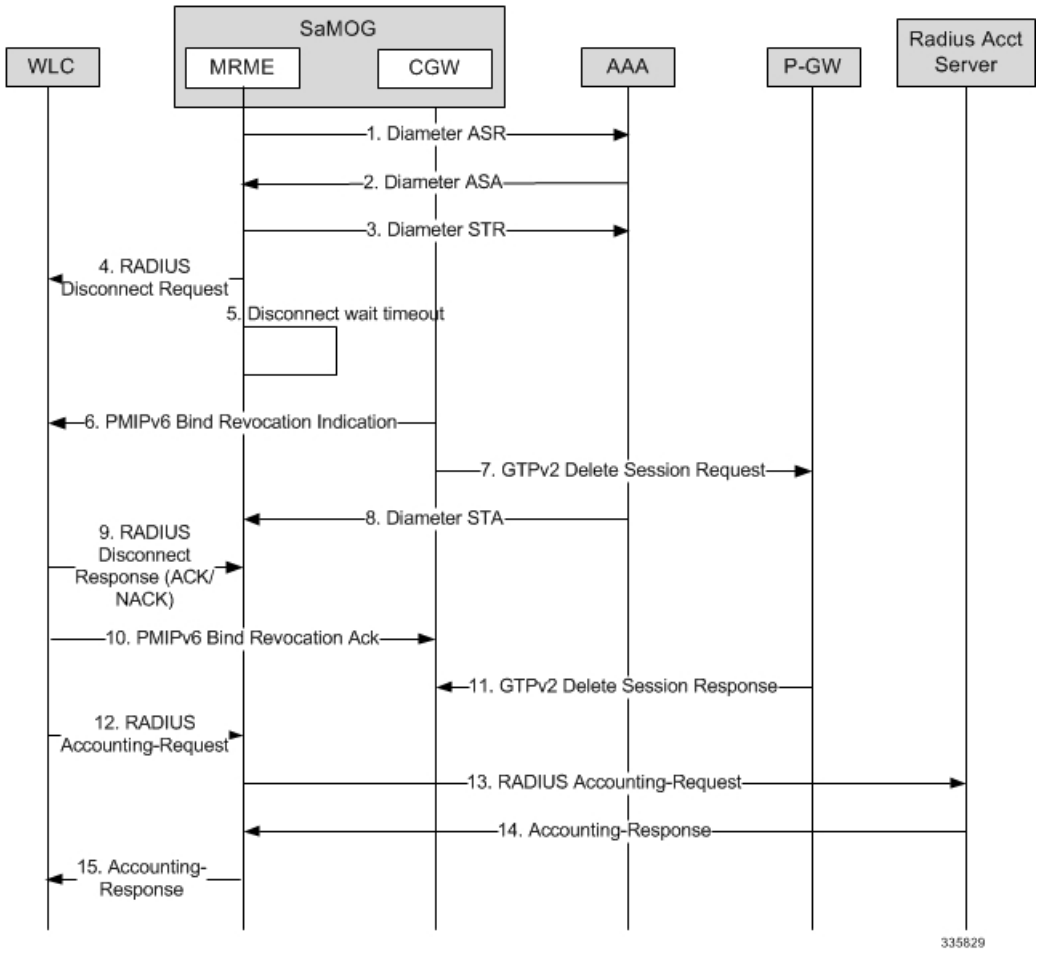


Table 12: AAA Server Initiated Session Disconnection

Step	Description
1.	The 3GPP AAA server initiates the STa disconnect procedures for trusted non-3GPP access UEs by sending a "Diameter Abort-Session-Request" message by including the Auth-Session-State.
2.	The MRME will process the received request, and if it is unable to proceed with the request, a "Diameter Abort-Session-Response" is sent with an appropriate Result-Code. Otherwise, the MRME will respond with a "Diameter Abort-Session-Request" message with a valid result code. Irrespective of the result on processing the "Diameter ASR" message, the MRME will tear down the session.

Step	Description
3.	The MRME initiates a "Diameter Session-Termination-Request" message to the 3GPP AAA server.
4.	The MRME also initiates a "Radius Disconnect Request" message to the WLC to release the resources on the WLC and to the UE.
5.	If the MRME receives accounting records for the session, then the MRME initiates "Disconnect Wait Timer" and waits for the "Accounting Request with Acct-Status-Type as Stop" message from the WLC.
6.	The CGW initiates a "PMIPv6 Binding Revocation Indication" message to the WLC to detach the PMIPv6 GRE tunnel between the WLC and the CGW.
7.	The CGW initiates a "GTPv2 Delete Session Request" message to remove the session resources from the P-GW.
8.	The 3GPP AAA server responds with a "Diameter Session-Termination-Answer" message.
9.	The WLC responds with a "PMIPv6 Binding Revocation Ack" message.
10.	WLC sends a "Radius Disconnect Response ACK/NAK" message to the MRME. • If the MRME receives a "Radius Disconnect NAK" message, then MRME stops the "Disconnect Wait Timer" and proceed to cleanup the call immediately. • If the MRME receives a "Radius Disconnect ACK" message, then MRME waits for the "Accounting Stop" message based on the "Disconnect Wait Timer" value.
11.	The P-GW responds with a "GTPv2 Delete Session Response" message.
12.	The WLC triggers a "Radius Accounting-Request" message with the "Acct-Status-Type" as "STOP", and an appropriate "Terminate-Cause".
13.	The MRME proxies the received "Radius Accounting-Request" message towards the RADIUS accounting server.

Step	Description
14.	The MRME receives the "Radius Accounting-Response" message from the RADIUS accounting server
15.	The MRME proxies the received "Radius Accounting-Response" message to the WLC.

SaMOG Gateway Data Flow

The figure below shows the user data flow on the SaMOG Gateway. The table that follows the figure describes each step in the flow.

Figure 12: SaMOG Gateway Data Flow

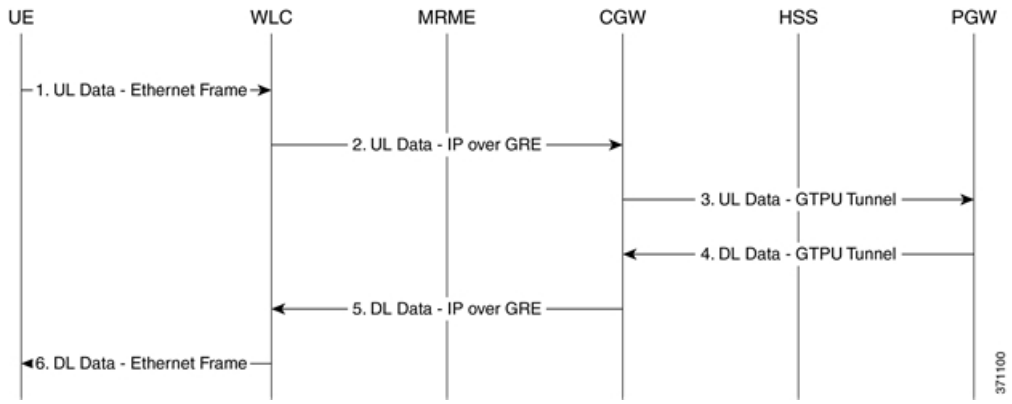


Table 13: SaMOG Gateway Data Flow

Step	Description
1.	The UE sends the uplink (UL) data to the WLC.
2.	The WLC sends the user data to the SaMOG Gateway's CGW service over the established bi-directional GRE tunnel.
3.	The CGW service sends the user data over a GTPU tunnel to the P-GW.
4.	The P-GW maps the downlink (DL) data on the GTPU tunnel to a GRE tunnel to the WLC.
5.	The CGW service sends the user data to the WLC over the GRE tunnel.
6.	The WLC sends the user data to the UE.

SaMOG Features and Functionality - Base Software

This section describes the SaMOG Gateway features and functions.

The following features and functions are supported:

Bulk Statistics

The system's support for CGW and MRME service bulk statistics allows operators to choose to view not only statistics that are of importance to them, but also to configure the format in which it is presented. This simplifies the post-processing of statistical data since it can be formatted to be parsed by external, back-end processors.

The system can be configured to collect bulk statistics and send them to a collection server called a receiver. Bulk statistics are collected in a group. The individual statistics are grouped by schema. The following is a partial list of supported schemas:

- **SaMOG:** Provides statistics to support the SaMOG Gateway.
- **System:** Provides system-level statistics.
- **Card:** Provides card-level statistics.
- **Port:** Provides port-level statistics.

The system supports the configuration of up to four sets of receivers. Each set can have primary and secondary receivers. Each set can be configured to collect specific sets of statistics from the various schemas. Bulk statistics can be periodically transferred, based on the transfer interval, using ftp/tftp/sftp mechanisms.

Bulk statistics are stored on the receivers in files. The format of the bulk statistic data files can be configured by the user. Users can specify the format of the file name, file headers, and/or footers to include information

such as the date, system host name, system uptime, the IP address of the system generating the statistics (available for headers and footers only), and/or the time that the file was generated.

When the Web Element Manager is used as the receiver, it is capable of further processing the statistics data through XML parsing, archiving, and graphing.

The Bulk Statistics Server component of the Web Element Manager parses collected statistics and stores the information in the PostgreSQL database. If XML file generation and transfer is required, this element generates the XML output and can send it to a northbound NMS or an alternate bulk statistics server for further processing.

Additionally, if archiving of the collected statistics is desired, the Bulk Statistics Server writes the files to an alternative directory on the server. A specific directory can be configured by the administrative user or the default directory can be used. Regardless, the directory can be on a local file system or on an NFS-mounted file system on the Web Element Manager server.

Important For more information on bulk statistics, see the *System Administration Guide.*

Congestion Control Support

SaMOG enhances on the StarOS framework to provide congestion control policies and threshold crossing alerts to ensure smooth performance of the SaMOG service and prevent congestion. The Congestion Control feature enables policies and thresholds to be configured to specify how the system should react in the event of a heavy load condition.

Congestion control monitors the system for conditions that could potentially degrade performance when the system is under heavy load. Typically, these conditions are temporary (for example, high CPU or memory utilization) and are quickly resolved. However, continuous or large numbers of these conditions within a specific time interval may have an impact the system's ability to service subscriber sessions. Congestion control helps identify such conditions and invokes policies for addressing the situation.

Congestion control operation is based on configuring the following:

- **Congestion Condition Thresholds:** Thresholds dictate the conditions for which congestion control is enabled and establish limits for defining the state of the system (congested or clear). These thresholds function in a way similar to operational thresholds that are configured for the system as described in the *Thresholding Configuration Guide*. The primary difference is that when congestion thresholds are reached, a service congestion policy and an SNMP trap, starCongestion, are generated.

  A threshold tolerance dictates the percentage under the configured threshold that must be reached in order for the condition to be cleared. An SNMP trap, starCongestionClear, is then triggered.

  - **Port Utilization Thresholds:** If you set a port utilization threshold, when the average utilization of all ports in the system reaches the specified threshold, congestion control is enabled.
  - **Port-specific Thresholds:** If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is enabled system-wide.

- **Service Congestion Policies:** Congestion policies are configurable for each service. These policies dictate how services respond when the system detects that a congestion condition threshold has been crossed.

For the SaMOG Gateway, congestion control monitors the following resources:

- Licensing utilization
- Maximum sessions per service utilization

- Demux message queue utilization
- Demux message queue wait time
- Port Rx specific utilization
- Port Tx specific utilization
- Average transmit port Tx utilization
- Process CPU utilization
- System CPU utilization
- System memory utilization

Note For more information on congestion control, refer to the *Congestion Control* chapter in the *System Administration Guide*. For configuration on congestion control specific to the SaMOG Gateway, refer to *Configuring the SaMOG Gateway* in this guide.

DHCP Trigger-based Session Creation

This feature enables the SaMOG Gateway to create sessions on receiving DHCP Discover or DHCP Request messages for a subscriber over the EoGRE tunnel.

For more information, refer DHCP Trigger-based Session Creation , on page 131.

Ethernet over GRE (EoGRE)

In addition to the PMIPv6 access type, SaMOG can use both Ethernet over GRE based access type from a trusted WLAN network to connect subscribers to 3G/4G networks.

4G/3G subscribers can connect to EPC/Internet using the trusted WiFi SSIDs served by EoGRE-enabled Residential Gateways in SaMOG. SaMOG acts as the tunnel endpoint for the EoGRE tunnel initiated from the Residential Gateway. Using the SSID-based WLAN access, users are authenticated based on the SSID they select to connect to WLAN. The Residential Gateway/WLC maintains separate SSIDs to provide 3G/4G access, and users can select the appropriate SSID based on their subscription to obtain 3G or 4G access through the WiFi network. EoGRE access type supports IPv4 , IPv6 and IPv4v6 addressing.

With this feature, SaMOG acts as the AAA server and DHCP server to the user equipment (UE) that connects to the WLAN network. SaMOG processes all the control packets from the UE and maintains the subscriber session to provide 3G/4G access. Acting as the DHCP-server, SaMOG creates the PDP context with GGSN/P-GW and obtains the IP address to allocate to the UE through DHCP-Response in the access-side. The interface with GGSN is similar to the TTG's Gn' interface with GGSN for 3G, and the existing SaMOG's S2a interface with P-GW for 4G. The DHCP and data packets originating from the UE are forwarded by the Residential Gateway/WLC node through the EoGRE tunnel to SaMOG.

The MRME service maintains all the access network parameters (Radius client and access client details) locally. The MRME service determines the session's access-type and if a request should be accepted or rejected, based on the NAS IP (AVP in the Access-Request/ Accounting-Request) or Source IP of the request (if NAS IP AVP is not available), by looking up the local configuration and conveys the same to CGW for session setup.

SaMOG as a Default Gateway

The SaMOG Gateway can act as the first-hop L3 router (default gateway) for the UE, and the UEs can forward data traffic directly to SaMOG using the EoGRE tunnel from the Residential Gateway/WLC. For 3G access, the default gateway IP address is obtained from the local configuration and supplied by P-GW for 4G access over the S2a interface.

UEs wanting to send data traffic will resolved the MAC address of the default gateway using an ARP request which is forwarded by the residential gateway/WLC over EoGRE using the mapped VLAN. The SaMOG Gateway responds with the virtual MAC address in the ARP response to enable data packets to reach SaMOG from the UE.

The SaMOG default gateway does not handle ICMP packets. The ICMP packets are considered as data and forwarded to GGSN/P-GW.

EoGRE Call Flows

This section describes the call flows for the EoGRE access-type.

SaMOG Gateway EoGRE Session Establishment (StarOS Release 18 and later)

The figure below shows an SaMOG Gateway session establishment flow using the EoGRE access type in StarOS Release 18 and later. The table that follows the figure describes each step in the flow.

Figure 13: SaMOG Gateway EoGRE Session Establishment

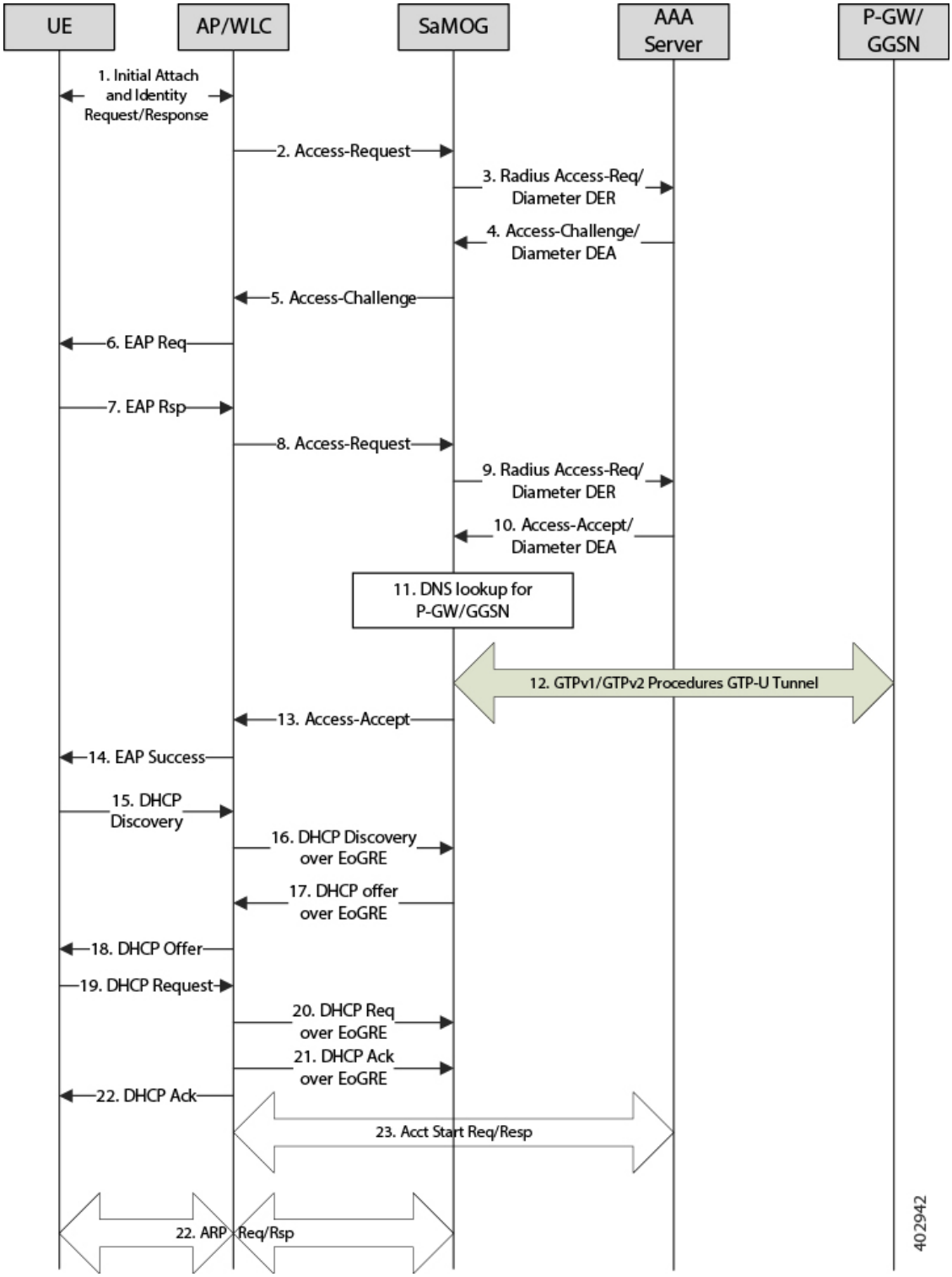


Table 14: SaMOG Gateway Session Establishment

Step	Description
1.	The UE initiates an initial attach procedure towards the WLC.
2.	The WLC forms an Access-Request message with the EAP-Identity payload, User-Name and Acct-Session-Id, and sends the same to SaMOG.
3.	SaMOG forms a Radius Access-Request or Diameter DEA message towards the AAA server using the attributes received from the WLC.
4.	The AAA server performs an EAP authentication and sends the Access-Challenge/DEA to SaMOG with the EAP payload.
5.	SaMOG copies the EAP payload to the Access-Challenge towards WLC.
6.	The WLC sends an EAP Request towards the UE.
7.	The UE sends an EAP response.
8.	The WLC sends the Access-Request to SaMOG with the EAP payload received from the UE.
9.	SaMOG sends the Access-Request/DER to the AAA server with the EAP payload.
10.	The AAA server fetches the subscriber profile from HLR/HSS and validates the EAP Challenge response sent from the UE. The Access-Accept/DEA is sent to SaMOG with the user profile and EAP Success payload. SaMOG saves the user profile information.
11.	SaMOG performs DNS procedures towards the DNS server to get the P-GW/GGSN IP address.
12.	SaMOG delays sending the Access-Accept to the WLC, and initiates S2a/Gn procedures towards P-GW/GGSN, by including the IMEIs V IE with the UE MAC value received as "Calling-Station-ID" AVP in the Access-Request, if sending of IE is enabled (via. configuration).
13.	SaMOG sends Access-Accept to the WLC with EAP-Success payload after completion of S2a/Gn procedures.
14.	The WLC sends EAP-Success to the UE.

Step	Description
15.	The UE sends DHCP discover (broadcast) request to the WLC.
16.	The WLC acts as a DHCP server and initiates DHCP discover over EoGRE tunnel towards SaMOG for L3 Attachment.
17.	SaMOG will process the received DHCP discover over EoGRE tunnel and responds back with a DHCP Offer over the EoGRE tunnel by including the allocated home-address by P-GW/GGSN and the default gateway IP address.
18.	The WLC sends a DHCP offer towards the UE with the allocated UE's IP address and the default gateway.
19.	The UE sends DHCP request to the WLC for DHCP, by including router options and the allocated UE's IP address for further confirmation.
20.	The WLC acts as a DHCP server and initiates a DHCP Request over the EoGRE tunnel towards SaMOG.
21.	SaMOG processes the received DHCP Request over the EoGRE tunnel and respond back with a DHCP Ack over the EoGRE tunnel by including the DNS Parameters in the router options.
22.	The WLC sends a DHCP Ack towards the UE.
23.	If proxy accounting is enabled, SaMOG will proxy the accounting messages between the WLC and the AAA server.
24.	The UE performs an ARP request for the default gateway received from SaMOG. The WLC sends the ARP request packets over the EoGRE tunnel and SaMOG responds back with an ARP Response over the EoGRE tunnel by including the virtual MAC address of the default gateway.

SaMOG Gateway IPv6 prefix Over EoGRE Using SLAAC

The figure below shows the message flow to delegate an IPv6 prefix to the user equipment (UE) using SLAAC for EoGRE access type. The table that follows the figure describes each step in the message flow.

Figure 14: SaMOG Gateway IPv6 prefix Over EoGRE Using SLAAC

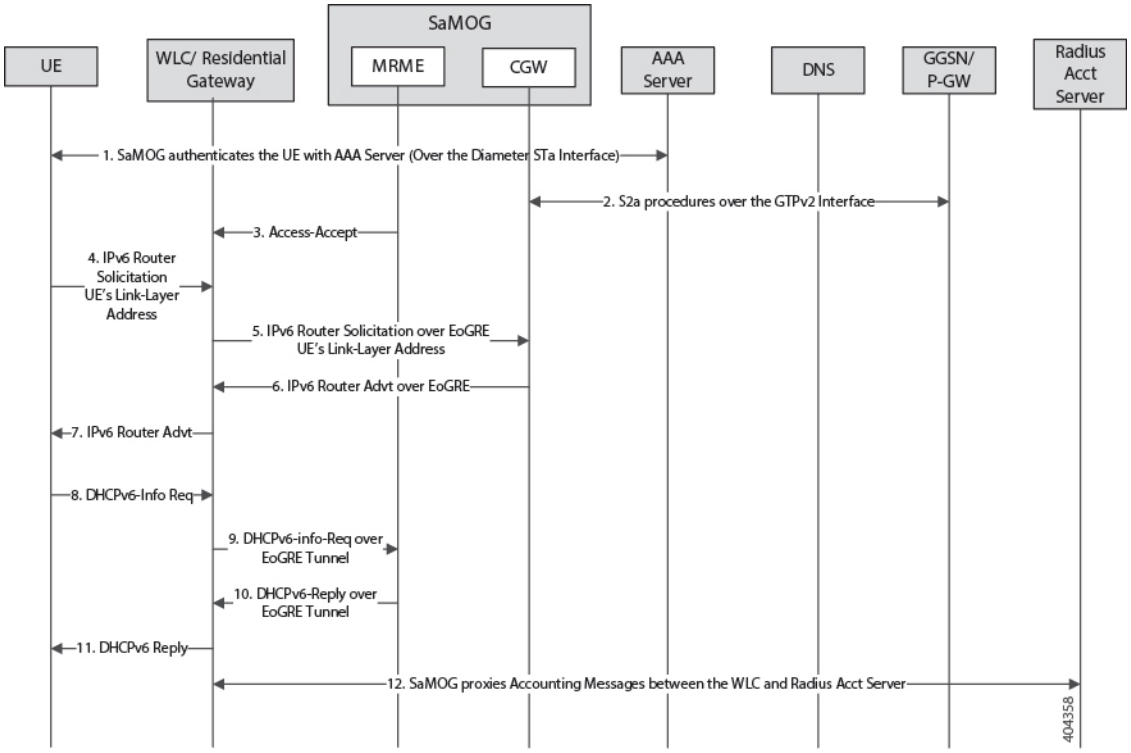


Table 15: SaMOG Gateway IPv6 prefix Over EoGRE Using SLAAC

Step	Description
1.	SaMOG authenticates between the UE and the AAA/Radius server via. WLC. During Authentication, SaMOG receives the PDN-Type IPv6 value as part of the APN-Profile AVP in the Diameter EAP Answer or Access-Accept message from the AAA/Radius server.
2.	After P-GW selection, SaMOG performs S2a procedures towards GGSN/PGW by including the PDN-Type, and receives the IPv6 Prefix for the subscriber's UE using S2a procedures as per APN subscription profile at P-GW
3.	SaMOG sends the Radius Access-Accept message towards WLC.

Step	Description
4.	The UE sends the IPv6 ICMPv6 Router Solicitation (ICMPv6 Type 133) message to the destination as "Link-Local Scope multicast All Routers Address (ff02:2)" with the source address as UEs Link-Local address. The UE also includes the ICMPv6 option "source link-layer address", which is the MAC address of the UE.
5.	For EoGRE access type sessions, the WLC is transparent between the UE and SaMOG for Neighbor Discovery and DHCPv6 messages. The WLC forwards the above messages to SaMOG by adding an EoGRE Tunnel Header received from the UE over CAP-WAP tunnel. Vice versa, the WLC discards the EoGRE tunnel header received from SaMOG and forwards the same to the UE over the CAP-WAP tunnel. The WLC sends the ICMPv6 Router Solicitation Message towards SaMOG by adding the EoGRE tunnel header.
6.	SaMOG processes the received ICMPv6 Router Solicitation message over the EoGRE tunnel and responds with an ICMPv6 Router Advertisement (ICMPv6 Type 134) message over the EoGRE tunnel towards WLC. The WLC also includes the RDNSS, DNSSL options as per *RFC 6106*.
7.	The WLC forwards the IPv6 Router Advertisement (RA) over the CAP-WAP tunnel based on the mapping maintained between the UE's MAC address and the CAP-WAP tunnel information.
8.	SaMOG sends unsolicited IPv6 Router Advertisement (RA) over the EoGRE tunnel by including the IPv6 options mentioned in Step 6.
9.	The WLC forwards the Unsolicited IPv6 Router Advertisement (RA) over CAP-WAP Tunnel based on the mapping maintained between the UE's MAC Address and CAP-WAP tunnel information.
10.	The WLC receives the DHPCv6 Information-Request message over the CAP-WAP tunnel to fetch the configuration parameters based on the UE's behavior by including the Client-identifier and Option Request option with "DNS Recursive Name Server" and "Domain Search List".

Step	Description
11.	The WLC forwards the DHCPv6 Information-Request towards SaMOG by adding the EoGRE tunnel header.
12.	SaMOG responds with a DHCPv6 Reply message over the EoGRE tunnel by including the "DNS Recursive Name Server" and "Domain Search List".
13.	The WLC forwards the DHCPv6 Reply message over the CAP-WAP tunnel based on the mapping maintained between the UE's MAC address and the CAP-WAP tunnel information.
13.	SaMOG acts as an Accounting proxy between the WLC and Radius Accounting Server where all Accounting messages will have "Framed-IP-Address" and "Framed-IPv6-Address" based on the PDN-Type.

SaMOG Gateway Dual-stack Support Using SLAAC Over EoGRE

The table below describes the steps in the message flow for dual-stack support using SLAAC over EoGRE.

Table 16: SaMOG Gateway Dual-stack Support Using SLAAC Over EoGRE

Step	Description
1.	Refer for the sequence of messages between the WLC to SaMOG, and SaMOG to P-GW.
2.	The UE triggers the sequence of messages using SLAAC to get the IPv6 prefix and DHCPv4 to get the IPv4 address.
3.	The WLC is transparent for the received SLAAC and DHCPv6 Info-req to get IPv6 Prefix and configuration parameters by encapsulating and decapsulating the EoGRE Tunnel header to and from SaMOG.
4.	WLC transparently receives DHCPv4 to get IPv4 address and configuration parameters by encapsulating and decapsulating the EoGRE Tunnel header to and from SaMOG.

MAC Address in Decimal Format for P-GW

This feature enables the SaMOG Gateway to encode the User Equipment's MAC address in the IMEISV IE value in decimal format, in order to support inter-operability with P-GW from third party vendors.

For more information, refer MAC Address in Decimal Format for P-GW , on page 149.

Newcall Policy Reject for SaMOG Service

During planned maintenance or congestion scenarios, this feature can either be used to restrict new calls on specified SaMOG service(s), or drop new calls on all SaMOG services. As this feature restricts new calls only, the existing established user sessions are not affected. This manner of restricting new calls, and clearing existing established sessions locally at SaMOG can ensure a graceful maintenance mode where no stale sessions on peer nodes (WLC/P-GW) exist.

This feature can be enabled using the **newcall policy samog-service { all | name** *service_name* **}** drop command under the Exec Mode, and disabled using the **no newcall policy samog-service { all | name** *service_name* **}** command. This configuration is disabled by default, and does not persist after a system reboot.

The output of the **show samog-service { all | name** *service_name* **}** command will indicate if newcall policy is enabled or disabled. Additionally, the output of the **show samog-service statistics** will indicate the total number of new calls dropped when the **newcall policy samog-service** command is enabled.

Offline Charging

The SaMOG Gateway supports generation of CDR files for offline charging. Offline charging works by collecting charging information concurrently with resource usage and passes the information through a chain of logical charging functions. At the end of the process, CDR files are generated by the network and transferred to the network operator's Billing Domain.

For more information on offline charging for the SaMOG Gateway, refer to the *SaMOG Gateway Offline Charging* chapter of this guide.

RADIUS Accounting-based Session Creation

This feature enables the SaMOG Gateway to create sessions on receiving a RADIUS Accounting-Start messages for subscribers.

For more information, refer RADIUS Accounting-based Session Creation, on page 173.

Rate Limiting Function (RLF) on STa Interface

The SaMOG Gateway supports the Rate Limiting Function (RLF) feature on the STa interface. The SaMOG Gateway rate limits the messages sent towards the AAA server when the RLF feature is enabled.

The RLF feature implements a generic framework that can be used by multiple interfaces and products for rate limiting/throttling outgoing messages like Diameter messages on Gx, Gy interface towards PCRF.

For more information on Rate Limiting Function (RLF), refer the *AAA Interface Administration and Reference guide*.

Sample Configuration

The following is a sample configuration to enable the use of RLF templates from the Global Configuration Mode:

```
config
    rlf-template rlf1
        msg-rate 1000 burst-size 100
        threshold upper 80 lower 60
        delay-tolerance 4
```

```
    exit
rlf-template rlf2
    msg-rate 20
    threshold upper 80 lower 60
    exit
rlf-template rlf3
    msg-rate 3000
    delay-tolerance 4
    exit
rlf-template rlf4
    msg-rate 4000
    threshold lower 60
    delay-tolerance 0
    end
```

SaMOG GTPP Using Same Source Address but Different Port

In multi-product deployment environments where CDRs are received from ePDG, SaMOG (pseudo) and P-GW (Local Breakout), the mediation server cannot differentiate between the products that provide the CDRs. With this feature, CDRs can easily be identified by mapping CDRs corresponding to each Gateway service to different ports of the same CGF server. This is achieved using CLI configurations for multiple GTPP groups with the same CGF server IP address and different port numbers. This configuration provides the flexibility to send ePDG, SaMOG and P-GW LBO CDRs to the same CGF server on different ports.

Whenever AAA proxy logs are displayed, it includes both CGF IP address and port, and can be filtered using the **port** keyword in the **gtpp test accounting**, **show gtpp counters**, **show gtpp statistics** and **clear gtpp statistics** CLI commands. If the port is not specified, then all GTPP servers with the specified IP address will be considered irrespective of the configured port.

SaMOG Wireless Access Gateway (WAG) Integration

Overview

The SaMOG Gateway supports additional deployment models and access-side connectivity by integrating various Wireless Access Gateway (WAG) functions. The WAG functions include:

- Deployment in environments where the WLC/RGs do not use bridge mode to forward packets between the User Equipment (UE) and the SaMOG Gateway.
- Receive IP packets in 'plain L3' or within GRE, MPLS or VLL tunnels.
- Route packets based on the IP address and the Layer 2 tunnel on the access-side to the GTP tunnel for the uplink, and vice versa for the downlink.
- Allow IP address allocation by either WLAN or SaMOG.

Layer 3 IP (L3IP)

The SaMOG Gateway supports out of band DHCP Layer 3 packet processing, and call setup with L3IP access type.

IP address assigned by the WLC (IP@W)

The User Equipment's (UE) IP address is assigned by WLC, and DHCP is not required in the call flow. WLC forwards the assigned IP address in the Accounting-Start message inside the Framed IP Address field. SaMOG NATs the IP@W with the IP address assigned by P-GW (IP@G).

IP over GRE (IPoGRE)

The SaMOG Gateway supports GRE encapsulation on the L3IP access-type to ensure a scalable deployment model. The SaMOG Gateway adds an extra IP and GRE header on top of the plain L3 IP. All control and data packets from one or more WLCs use the same IPoGRE tunnel. The SaMOG Gateway performs encapsulation and decapsulation before processing any control or data packets. After the packets are encapsulated or decapsulated, the session is handled in the same way as that of L3IP or IP@W deployment models. The IPoGRE functionality is achieved using the StarOS GRE tunnel feature, and one-to-one mapping between the GRE tunnel interfaces (or same TWAN profile multiple GRE tunnel interfaces) and VRFs.

Important The IP over GRE model requires a GRE Interface Tunneling license to create GRE tunnels. For more information on licenses, contact your Cisco account representative.

IP over VLAN (IPoVLAN)

The SaMOG Gateway supports VLAN encapsulation on the L3IP access-type to ensure a scalable deployment model. The SaMOG Gateway adds an extra VLAN header next to the Ethernet header and the session is handled in the same way as that of the L3IP or IP@W deployment models. The IPoVLAN functionality is achieved using the StarOS VLAN feature, and one-to-one mapping between the VLANs (or same TWAN profiles) and VRFs.

Authentication

SaMOG supports proxy-based authentication, and session creation based on the MAC address received in the Access-Request messages. SaMOG acts as both authentication and accounting proxy. In accordance to 3GPP 23.402 standards, a PDN connection establishment is completed before the Radius Access-Accept is sent to the WLC.

Accounting

The SaMOG Gateway functions in a server mode acting as a AAA accounting server in the uplink direction to receive the accounting requests. The accounting start message is used between the WLC and the SaMOG Gateway to communicate the IP@WLAN assigned by the WLC to the SaMOG Gateway. The server mode for the SaMOG Gateway is enabled when there is no accounting server configuration present in the Operator Policy Configuration Mode.

User Equipment's (UE) Address

The SaMOG Gateway provides support for different models for the UE Home Address (UE-HA) and UE Network Address (UE-NA) as follows:

- The WLAN assigns an address directly to the UE and communicates it to the SaMOG Gateway through an accounting start-request message with the Framed-IP-address set to IP@W.
- The WLC relays the DHCP requests to the SaMOG Gateway, and the SaMOG Gateway provides the address it receives from the P-GW.
- The WLC relays DHCP requests to the SaMOG Gateway, and the SaMOG Gateway assigns the address from its local pool and shares the same to the UE (For Local Breakout (Basic)).
- The SaMOG Gateway assigns the address from the P-GW to the UE.

Static NAT

The SaMOG gateway can perform static NAT when the UE-HA and the UE-Na are not the same. Static NAT is achieved through the Enhanced Charging Service's (ECSv2) Firewall and NAT functionality.

DHCP Server

SaMOG supports DHCP server at system level for L3IP models where the UE session is identified by parsing the DHCP options inside the DHCP packets (using DeMUX). SaMOG supports DHCP packets in-band where the VLAN or GRE tunnel from which the DHCP packets are received is considered to be the same tunnel to receive the data path traffic.

Access Type

The SaMOG Gateway supports the following access-types:

- Ethernet over GRE (EoGRE)
- PMIPv6
- Layer3 IP (L3IP)
- IP over VLAN (IPoVLAN)
- IP over GRE (IPoGRE)

The SaMOG Gateway determines the NPU flow for a session using the configured **access-type** CLI command under the TWAN Profile Configuration Mode. Although the SaMOG Gateway does not support a change in the access-type mid-session, the SaMOG Gateway drops the previous session and the access request message when a change is the access-type is detected, and the NPU flows are switched to the changed access-type.

Call Flows for WAG Models

This section describes the call flows for the different WAG models.

Session Establishment for Layer 3 IP with DHCP Server

The figure below shows an SaMOG Gateway session establishment flow for Layer 3 IP with a DHCP server in StarOS Release 18 and later. The table that follows the figure describes each step in the flow.

Figure 15: Session Establishment for Layer 3 IP with DHCP Server

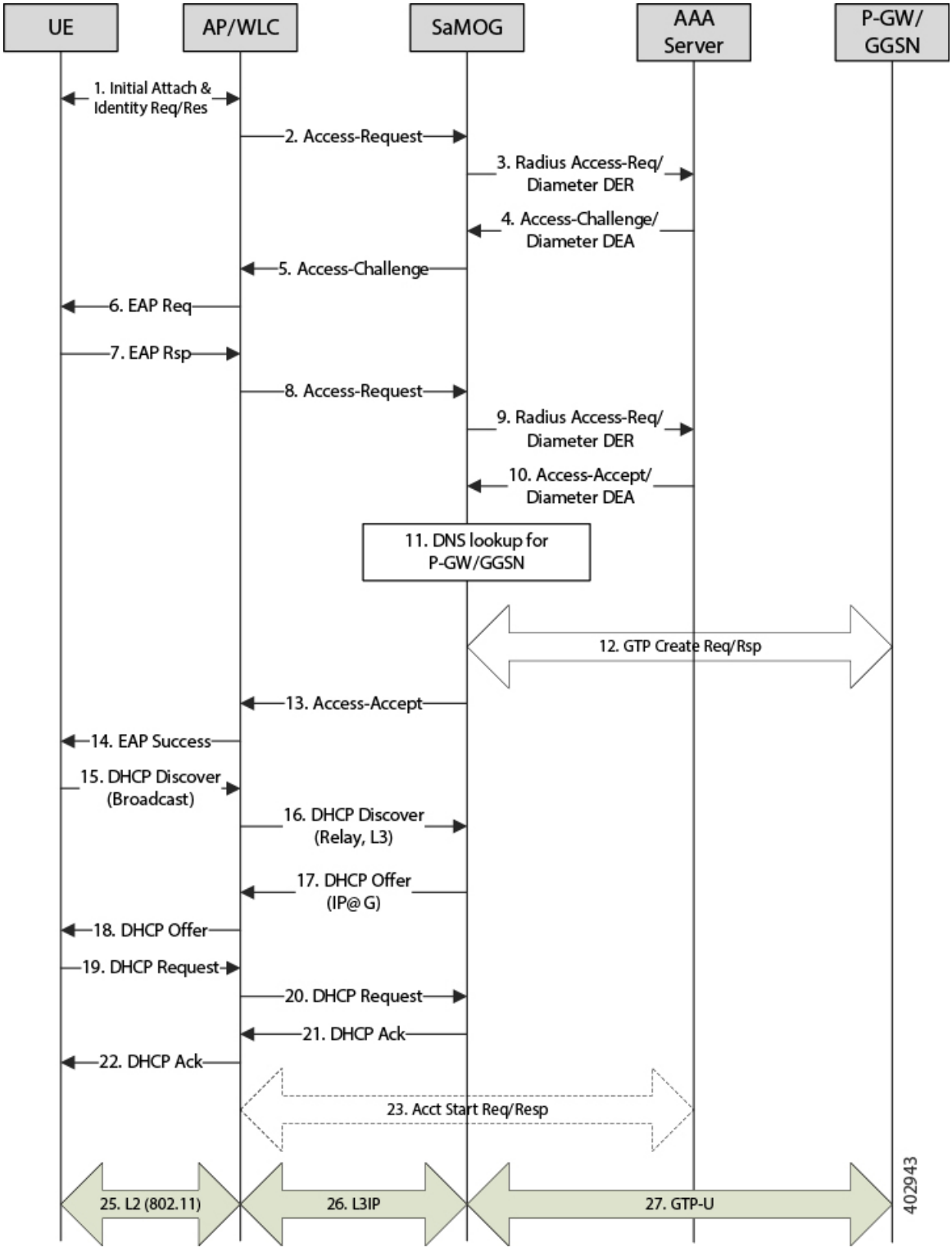


Table 17: Session Establishment for Layer 3 IP with DHCP Server

Step	Description
1.	The UE initiates an initial attach procedure towards the WLC.
2.	The WLC forms an Access-Request message with the EAP-Identity payload, User-Name and Acct-Session-Id, and sends the same to SaMOG.
3.	SaMOG forms a Radius Access-Request or Diameter DEA message towards the AAA server using the attributes received from the WLC.
4.	The AAA server performs an EAP authentication and sends the Access-Challenge/DEA to SaMOG with the EAP payload.
5.	SaMOG copies the EAP payload to the Access-Challenge message towards the WLC.
6.	The WLC sends an EAP Request towards the UE.
7.	The UE sends an EAP response.
8.	The WLC sends the Access-Request to SaMOG with the EAP payload received from the UE.
9.	SaMOG sends the Access-Request/DER to the AAA server with the EAP payload.
10.	The AAA server fetches the subscriber profile from HLR/HSS and validates the EAP Challenge response sent from the UE. The Access-Accept/DEA is sent to SaMOG with the user profile and EAP Success payload. SaMOG saves the user profile information.
11.	SaMOG performs DNS procedures towards the DNS server to get the P-GW/GGSN IP address.
12.	SaMOG sends a create request (GTPv2 or GTPv1) towards the P-GW/GGSN (or local P-GW/GGSN in case of LBO) and receives the IP Address of the UE in response (IP@G).
13.	SaMOG sends Access-Accept to the WLC with EAP-Success payload.
14.	The WLC sends EAP-Success to the UE.
15.	The UE sends DHCP discover (broadcast) request to the WLC.

Step	Description
16.	The WLC acts as a DHCP relay agent and relays the DHCP messages (unicast) towards SaMOG. The DHCP packets are in the form of plain L3 IP packets.
17.	SaMOG sends a DHCP offer with IP@G and the default G/W (may have received from P-GW) towards the UE.
18.	The WLC forwards the DHCP offer to the UE.
19.	The UE sends a DHCP request to the WLC.
20.	The WLC (acting as relay agent) forwards the DHCP request to SaMOG
21.	SaMOG sends DHCP Ack message to the WLC.
22.	The WLC forwards the DHCP Ack message to the UE.
23.	If proxy accounting is enabled, SaMOG proxies accounting messages between the WLC and the AAA server.
24.	Void.
25.	The UE sends/receives data packets over the 802.11 interface towards/from the Access Point (AP), and the AP sends/receives over CAP/WAP to/from WLC or intermediate routers.
26.	The WLC or one of the intermediate routers forwards/receives data packets as plain IP towards/from SaMOG.
27.	SaMOG forwards/receives the IP packets over the GTP-u tunnel towards/from P-GW/GGSN (Local P-GW/GGSN in case of LBO).

Session Establishment for Layer 3 IP, with IP Assigned by WLAN (IP@W)

The figure below shows an SaMOG Gateway session establishment flow for Layer 3 IP with the IP address assigned by WLAN (IP@W) using NAT in StarOS Release 18 and later. The table that follows the figure describes each step in the flow.

Figure 16: Session Establishment for Layer 3 IP, with IP@W

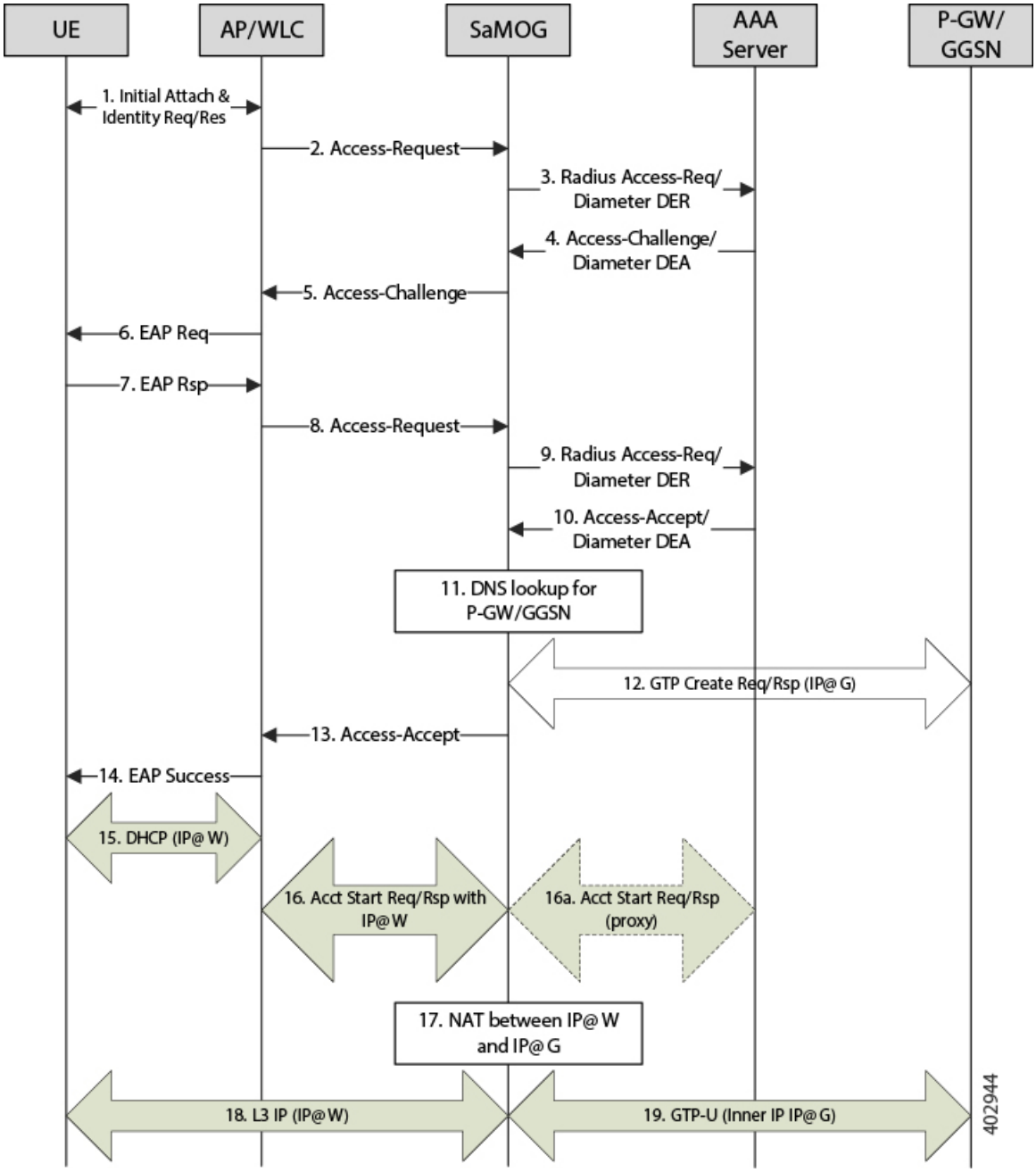


Table 18: Session Establishment for Layer 3 IP with IP@W

Step	Description
1.	The UE initiates an initial attach procedure towards the WLC.

Step	Description
2.	The WLC forms an Access-Request message with the EAP-Identity payload, User-Name and Acct-Session-Id, and sends the same to SaMOG.
3.	SaMOG forms a Radius Access-Request or Diameter DEA message towards the AAA server using the attributes received from the WLC.
4.	The AAA server performs an EAP authentication and sends the Access-Challenge/DEA to SaMOG with the EAP payload.
5.	SaMOG copies the EAP payload to the Access-Challenge message towards the WLC.
6.	The WLC sends an EAP Request towards the UE.
7.	The UE sends an EAP response.
8.	The WLC sends the Access-Request to SaMOG with the EAP payload received from the UE.
9.	SaMOG sends the Access-Request/DER to the AAA server with the EAP payload.
10.	The AAA server fetches the subscriber profile from HLR/HSS and validates the EAP Challenge response sent from the UE. The Access-Accept/DEA is sent to SaMOG with the user profile and EAP Success payload. SaMOG saves the user profile information.
11.	SaMOG performs DNS procedures towards the DNS server to get the P-GW/GGSN IP address.
12.	SaMOG sends a create request (GTPv2 or GTPv1) towards the P-GW/GGSN (or local P-GW/GGSN in case of LBO) and receives the IP Address of the UE in response (IP@G).
13.	SaMOG sends Access-Accept to the WLC with EAP-Success payload.
14.	The WLC sends EAP-Success to the UE.
15.	The UE performs DHCP with the WLC and obtains the IP address (IP@W).

Step	Description
16.	The WLC sends an Accounting Start Req with the Framed-IP-Address value (IP@W). If the Accounting Server is configured at SaMOG (SaMOG acting as an Accounting Proxy), the Accounting Start Req is forwarded to the Accounting server.
17.	SaMOG creates a NAT entry between the IP@W and IP@G.
18.	The UE sends/receives data packets with the IP address (IP@W) over the 802.11 interface towards/from the Access Point (AP), and the AP sends/receives data packets over CAP/WAP to/from WLC or intermediate routers. The WLC or the intermediate routers will forward/receive data packets as plain IP towards/from SaMOG.
19.	SaMOG performs NAT, changing the IP from IP@W to IP@G, and forwards the IP packets over GTP-u tunnel towards the P-GW/GGSN (Local P-GW/GGSN in case of LBO). Also, reverse NATing (IP@G to IP@W) occurs when the data is received from the P-GW/GGSN in the GTP-u tunnel and forwarded to the UE.

Limitations, Restrictions, and Dependencies

This section identifies limitations, restrictions, and dependencies for the SaMOG WAG integration:

- The AP location is sent from the WLC in the Called-Station-Id attribute. The WLC may include either the AP MAC, AP Name, AP MAC and SSID, or AP Name and SSID. If the WLC is configured to send the AP Name (for sending ULI on Gn interface), SaMOG will not be able to send the AP MAC in TWAN Identifier AVP over the S2a interface.
- The SaMOG Gateway does not support overlapping WLC-IP-Address for IPoVLAN and IPoGRE for Radius/DHCP packets.

Secondary P-GW or GGSN Fallback

The SaMOG Gateway supports session establishment between the GTP interface and an alternate P-GW or GGSN when connection establishment fails towards the primary P-GW or GGSN (response timeout or localized issues). Where SaMOG selects the P-GW or GGSN using DNS queries, the secondary P-GW or GGSN IP address is determined using the A/AAAA (Pre-release 8) or SNAPTR (Post-release 7) DNS procedure with the DNS server.

A/AAAA DNS Query-based Selection

The SaMOG Gateway performs the pre-release 8 DNS procedure when the local policy has A/AAAA configured as the DNS query type. As the DNS server returns a list of GGSN IP addresses that serve the APN, the SaMOG

Gateway selects the GGSN IP address from the list and tries to establish a GTPv1 session. The SaMOG Gateway will keep trying to establish a connection with the GGSN IP addresses from the list provided by the DNS server until a session is established. When the list is exhausted, or the session setup timer expires, the session setup attempt is aborted and the session is cleared.

SNAPTR DNS Query-based Selection

The SaMOG Gateway performs the post-release 7 DNS procedure when the local policy has SNAPTR configured as the DNS query type. The SNAPTR query is performed on an APN FQDN or P-GW FQDN with a service string mapped to the S2a-Gn, P-GW-Gn, and GGSN-Gn in the same order of preference. This results in a list of IP addresses of the P-GW or GGSN whose interfaces corresponds to the service string that currently serves the specified APN.

The SaMOG Gateway performs a topology or weight-based match (as configured) from the list and tries to establish a GTPv2 or GTPv1 connection with the matched P-GW or GGSN. On failure, SaMOG performs a topology or weight-based match with the rest of the IP addresses from the list until the list is exhausted. The SaMOG Gateway then builds a list from the next service parameter in preference. When the list is exhausted, or the session setup timer expires, the session setup attempt is aborted and the session is cleared.

Trigger for Secondary P-GW or GGSN Fallback

The SaMOG Gateway triggers fallback to the secondary P-GW or GGSN selection when the following GTP cause values are received in the Create Session Response (CSR) and Create PDP Context Response (CPCR) messages:

CSR/CPC Request Rejection Cause	GTPv2 Cause Code	GTPv1 Cause Code
Service not supported	68	200
No resources available	73	199
All dynamic addresses are occupied	84	211
Service denied	89	—
No memory available	91	212
APN congestion	113	229

The call setup attempt is terminated for all other cause values.

In addition to the above rejection causes, the P-GW or GGSN selection fallback is triggered when the primary P-GW or GGSN fails to respond to the CSR/CPCR Request message.

The fallback to secondary P-GW or GGSN is not applicable for SaMOG Local Break Out or Web Authorization features.

SNMP Traps

The SaMOG Gateway generates SNMP traps for the SaMOG service startup and shutdown events. For detailed descriptions of the traps, refer to the *SNMP MIB Reference* guide.

Threshold Crossing Alerts (TCA) Support

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e high CPU utilization, or packet collisions on a network) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

The system supports Threshold Crossing Alerts for certain key resources such as CPU, memory, IP pool addresses, etc. With this capability, the operator can configure threshold on these resources whereby, should the resource depletion cross the configured threshold, a SNMP Trap would be sent.

The following thresholding models are supported by the system:

- **Alert:** A value is monitored and an alert condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.
- **Alarm:** Both high and low threshold are defined for a value. An alarm condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.

In addition to the existing generic StarOS system level TCA thresholds, an SaMOG service session count threshold is available to check if the total number of subscribers have exceeded the high threshold.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps:** SNMP traps have been created that indicate the condition (high threshold crossing and clear) of each of the monitored values.

  Generation of specific traps can be enabled or disabled on the chassis. Ensuring that only important faults get displayed. SNMP traps are supported in both Alert and Alarm modes.

- **Logs:** The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.

  Logs are supported in both the Alert and the Alarm models.

- **Alarm System:** High threshold alarms generated within the specified polling interval are considered outstanding until a condition no longer exists or a condition clear alarm is generated. Outstanding alarms are reported to the systems's alarm subsystem and are viewable through the Alarm Management menu in the Web Element Manager.

Important For more information on threshold crossing alert configuration, refer to the *Thresholding Configuration Guide*.

Virtual MAC Validation

SaMOG can validate if the destination MAC address in the packet received over the EoGRE tunnel matches with its virtual MAC, broadcast, or multicast address. Packets whose address does not match are dropped. This validation can be enabled using the **violation drop** keywords in the **virtual-mac** command under the APN Profile Configuration Mode.

SaMOG Features and Functionality - License Enhanced Feature Software

This section describes the optional enhanced features and functions for SaMOG service.

Important The following features require the purchase of an additional feature license to implement the functionality with the SaMOG service. For more information on the feature licenses, contact your Cisco account representative.

This section describes the following enhanced features:

Inter-Chassis Session Recovery

SaMOG is capable of providing chassis-level and geographic-level redundancy and can recover fully created sessions in the event of a chassis failure.

The Cisco ASR 5x00 and virtualized platforms provide industry leading carrier class redundancy. The systems protects against all single points of failure (hardware and software) and attempts to recover to an operat ional state when multiple simultaneous failures occur.

For more information, refer the *Inter-Chassis Session Recovery* chapter of this guide.

Lawful Intercept

The Cisco Lawful Intercept feature is supported on the SaMOG (CGW, MRME) Gateway. Lawful Intercept is a license-enabled, standards-based feature that provides telecommunications service providers with a mechanism to assist law enforcement agencies in monitoring suspicious individuals for potential illegal activity. For additional information and documentation on the Lawful Intercept feature, contact your Cisco account representative.

SaMOG Local Break Out

The SaMOG Local Break Out (LBO) feature enables subscribers to access the Internet directly without connecting to the EPC or 3G core.

For more information on the Local Breakout feature for the SaMOG Gateway, refer to the *SaMOG Local Breakout* chapter of this guide.

Session Recovery

SaMOG has the ability to recover fully created sessions in the event of process level or card level failures.

This feature supports the following types of session recovery:

- **Task level recovery:** SaMOG sessions are recovered when a Session Manager task serving the session is terminated due to a software error.
- **Card level recovery:** SaMOG sessions are recovered when the entire PSC/DPC card hosting the Session Manager fails, and all the tasks running on that card have to be recovered. The SaMOG sessions can be recovered in the event of a PSC/DPC card failures in the following scenarios:
  - **Unplanned card failure:** SaMOG can recover tasks running on the failed card to the standby card by fetching the CRR information from the peer Session Managers and AAA Managers in the other card.
  - **Planned card migration:** The system administrator can migrate the sessions from one PSC/DPC card to a standby card using the CLI. Planned migration can be performed by transferring the entire memory contents from the source card to the destination card, re-opening the sockets, and updating the NPU flows.

Important In this release, card level recovery and npusim recovery are not supported on the virtualized platform (VPC).

When the Session Recovery feature is enabled for the SaMOG Gateway using the CLI, the Session Manager maintains a backup of the session critical information with the AAA Manager that has the same instance number. A paired AAA Manager with the same instance number as the Session Manager is started on a different PSC/DPC card. When a failure is detected, the Call Recovery Record (CRR) that contains the backed up information is fetched from the AAA Manager, and the sessions are re-created on the recovered Session Manager.

As the SaMOG session recovery feature makes use of the existing StarOS IPSG framework, new fields are added to the IPSG session recovery record to recover attributes specific to the SaMOG session (For example: GRE end point address, SaMOG EGTPC information, etc).

The Session Recovery feature requires a minimum of four PSC/DPC cards (3 active and 1 standby). One PSC/DPC card will be used the DEMUX managers and VPN manager, two PSC/DPC cards will be used by the Session manager and AAA manager, and one PSC/DPC card will be used for standby.

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

Web Authorization

The Web Authorization feature enables the SaMOG Gateway to authenticate a subscriber's user equipment (UE) over a web portal, based on a user ID and password combination, a one-time password, or a voucher. On successful authentication, the AAA server stores the subscriber profile (APN, IMSI, QoS) from the HLR/HSS for the subscriber's device, and SaMOG establishes the network connection for the UE.

Web-based authorization can be performed in the following scenarios:

- The UE with the Universal Integrated Circuit Card (UICC) does not support EAP-AKA, EAP-SIM, or EAP-AKA' based authentication.
- The UE with the UICC uses a prepaid voucher.
- The UE does not have a UICC (laptop, tablet, etc).

The SaMOG web-based authorization and session establishment for a non-EAP or non-UICC device occurs in two phases:

- Pre-Authentication Phase, on page 72
- Transparent Auto-logon (TAL) Phase, on page 72

Phases

The SaMOG web-based authorization and session establishment for a non-EAP or non-UICC device occurs in two phases:

Pre-Authentication Phase

During the pre-authentication phase, SaMOG supports local IP address assignment and redirects the UE traffic to a web portal where the subscriber authenticates with a username and password combination, a one-time password, or a voucher. On successful authentication, the subscriber's IMSI profile is associated with the MAC address of the UE and forwarded to the AAA server. SaMOG can allocate IPv4, IPv6, or IPv4v6 addresses to the UE during this phase.

The IP address to the UE is allocated from a locally configured IP address pool in order to communicate with the web portal. The pool name can either be locally configured or received from the AAA server. SaMOG then processes the HTTP(S) and DNS packets from the UE by using ACL filters on the traffic. All other packets are dropped. The ACL filter is locally configured, and the filter ID can either be locally configured or received from the AAA server. The received HTTP(S) packets are then redirected to the web portal using a locally configured ECS rulebase that provides the URL for redirection. The rulebase name can either be locally configured or received from the AAA server. SaMOG shares the primary and secondary DNS server address with the UE. The DNS server addresses can either be locally configured or received from the AAA server.

For assigning an IPv6 address, SaMOG uses the following AVPs in the Diameter AA-Answer message in the MRME STa dictionary:

- **Framed-IPv6-Pool**: The AAA server uses this attribute to send the IPv6 pool-name configured in the Gi context. SaMOG uses this IPv6 pool-name to allocate the IPv6 prefix during the pre-authentication phase.
- **SN1-IPv6-Primary-DNS**: The AAA server uses this attribute to send the IPv6 address of the primary DNS server in the ADDRESS format.
- **SN1-IPv6-Secondary-DNS**: The AAA server uses this attribute to send the IPv6 address of the secondary DNS server in the ADDRESS format.

Transparent Auto-logon (TAL) Phase

During the TAL phase, the subscriber profile is cached on the AAA server for a designated duration to enable subscribers to reconnect without further portal authentication, thus enabling a seamless user experience. During this phase, SaMOG can allocate IPv4, IPv6, or IPv4v6 addresses to the UE.

Multiple PDN Connections

Using web authorization, a subscriber can connect multiple non-EAP devices and one EAP based device using the same IMSI-based subscription at the same time. All PDN connections of a subscriber have different bearer IDs. The connections are routed to the same P-GW or GGSN in order to apply the APN level QoS on all the PDN connections. The SaMOG Gateway performs P-GW, GGSN, or L-GW selection for the first PDN connection for the subscriber, and all subsequent connections are routed to the same P-GW, GGSN, or L-GW.

DHCP Lease Time

When pre-authentication completes and on successful authentication of the UE through the external web portal, SaMOG disconnects the UE from the WiFi. The UE then automatically reconnects to WiFi, and SaMOG obtains a new IP address for the UE using a GTP tunnel towards P-GW (TAL phase). The UE is then expected to send a DHCP Request/Discover message to learn the new IP address (as WiFi was disconnected and reconnected).

The DHCP lease time for the IP address assigned during the pre-authentication and TAL phases can be configured using the **dhcp lease** command under the APN Profile Configuration Mode.

Session Recovery

The SaMOG gateway can recover AAA manager and Session manager failures for both pre-authentication phase and TAL phase as long as the sessions are fully connected. SaMOG maintains the MAC to IMSI mapping and MAC to Session manager mapping with the IPSG manager to ensure that the PDN connections of the subscriber is connected to the same Session manager.

Limitations, Restrictions, and Dependencies

This section identifies limitations, restrictions, and dependencies for the SaMOG Web Authorization feature:

- After a successful portal-based authentication, the UE will be disconnected and a new connection attempt is required to setup the TAL phase session.
- The Web Authorization feature cannot be configured with the pseudonym and fast reauthorization NAIs. If configured, the session for the same IMSI number might get established in a different GGSN, P-GW, or L-GW.
- The MAC to IMSI mapping table cannot be retrieved during an IPSG manager recovery.
- When two devices with the same IMSI number try to connect simultaneously, the sessions are sent to two different session managers. The device connecting later is locally dropped and its Access-Request message is ignored. However, a subsequent re-transmission of the Access-Request message succeeds as the IMSI session manager entry is found and the message is sent to the session manager.
- Only one IP context must be configured and all portal traffic routed from that VPN context.
- All IP pools must be under the same context.
- The timeout value for the pre-authentication phase (when the DM/ASR is not received) is 5 minutes and cannot be configured.
- For a MAC-based authentication, the AAA server is selected based on the SSID as no IMSI information is available in the Access-Request message. To avoid a different operation policy being selected when the IMSI is present, configure the SSID-based policy with a higher priority than the IMSI-based policy. Alternatively, configure both SSID and IMSI in the policy configuration.

Optimized Web Authorization

Optimized Web Authorization feature provides a seamless experience to the subscriber by continuing the SaMOG session with no session disconnection after the Pre-Authentication phase. The SaMOG Gateway uses the SaMOG Local Breakout – Enhanced feature where a P-GW (GTPv2) or GGSN (GTPv1) is collocated with SaMOG in the same chassis.

The address assigned to the subscriber's UE is retained by maintaining the same IP address range pools within a single Gi context, and shared across the P-GW or GGSN service and SaMOG service. The SaMOG service uses the VPNMgr address transfer feature to transfer the IP address or IPv6 prefix to the P-GW or GGSN service.

This feature is supported on both EoGRE and PMIPv6 access types, with IPv4 and IPv6 transports to the WLC.

SaMOG Features and Functionality - Inline Service Support

This section describes the features and functions of inline services supported on the SaMOG Gateway.

Important The following features require the purchase of an additional feature license to implement the functionality with the SaMOG service. For more information on the feature licenses, contact your Cisco account representative.

This section describes the following features:

• Network Address Translation (NAT), on page 74

Network Address Translation (NAT)

NAT translates non-routable private IP address(es) to routable public IP address(es) from a pool of public IP addresses that have been designated for NAT. This enables to conserve on the number of public IP addresses required to communicate with external networks, and ensures security as the IP address scheme for the internal network is masked from external hosts, and each outgoing and incoming packet goes through the translation process.

NAT works by inspecting both incoming and outgoing IP datagrams and, as needed, modifying the source IP address and port number in the IP header to reflect the configured NAT address mapping for outgoing datagrams. The reverse NAT translation is applied to incoming datagrams.

NAT can be used to perform address translation for simple IP and mobile IP. NAT can be selectively applied/denied to different flows (5-tuple connections) originating from subscribers based on the flows' L3/L4 characteristics—Source-IP, Source-Port, Destination-IP, Destination-Port, and Protocol.

NAT supports the following mappings:

- One-to-One
- Many-to-One

Important For more information on NAT, refer to the *Network Address Translation Administration Guide*.

Supported Standards

The SaMOG Gateway complies with the following standards:

- 3GPP References, on page 75
- IETF References, on page 76

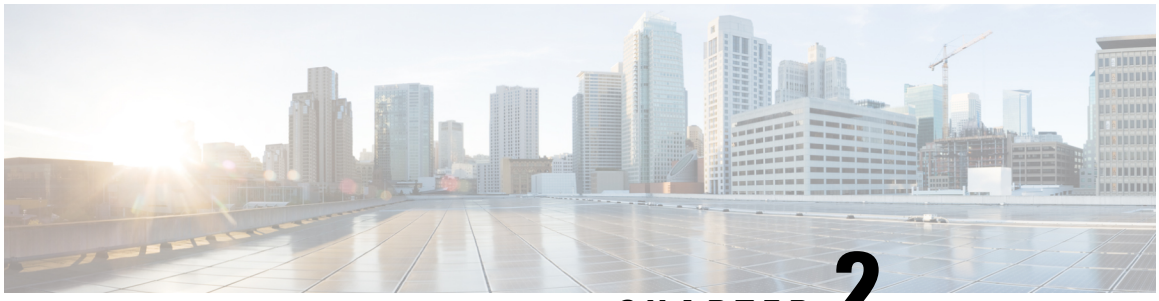
3GPP References

- 3GPP TS 23.234-a.0.0: "Universal Mobile Telecommunications System (UMTS); LTE; 3GPP system to Wireless Local Area Network (WLAN) interworking; System description (Release 10)".
- 3GGP TS 23.261-a.1.0: "Universal Mobile Telecommunications System (UMTS); LTE; IP flow mobility and seamless Wireless Local Area Network (WLAN) offload; Stage 2 (3GGP TS 23.261 version 10.1.0 Release 10)".
- 3GPP TS 23.401 (V10.4.0): "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 10)".
- 3GPP TS 23.402-b.5.1: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for non-3GPP accesses (Release 10)".
- 3GGP TS 24.302-a.4.0: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3 (Release 8)".
- 3GPP TS 24.312-a.3.0: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Access Network Discovery and Selection Function (ANDSF) Management Object (MO) (Release 10)".
- 3GPP TS 29.272: "3rd Generation Partnership Project; Technical Specification Group Core LTE; Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol".
- 3GPP TS 29.273-b.5.0: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Evolved Packet System (EPS); 3GPP EPS AAA interfaces (Release 9)".
- 3GPP TS 29.274-a.3.0: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 29.275-a.2.0: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols; Stage 3 (Release 8)".
- 3GGP TS 29.303 va.2.1: "Universal Mobile Telecommunications System (UMTS); LTE; Domain Name System Procedures; Stage 3 (3GGP TS 29.303 version 10.2.1 Release 10)".
- 3GPP TS 33.234-a.0.0: "3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; 3G Security; Wireless Local Area Network (WLAN) Interworking Security; (Release 6)".

- 3GPP TS 33.402-a.0.0: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses; (Release 8)."

IETF References

- RFC 2460 (December 1998): "Internet Protocol, Version 6 (IPv6) Specification".
- RFC 2461 (December 1998): "Neighbor Discovery for IP Version 6 (IPv6)".
- RFC 2473 (December 1998): "Generic Packet Tunneling in IPv6 Specification".
- RFC 3588 (September 2003): "Diameter Base Protocol".
- RFC 3602 (September 2003): The AES-CBC Cipher Algorithm and Its Use with IPsec".
- RFC 3715 (March 2004): "IPsec-Network Address Translation (NAT) Compatibility Requirements".
- RFC 3748 (June 2004): "Extensible Authentication Protocol (EAP)".
- RFC 3775 (June 2004): "Mobility Support in IPv6".
- RFC 3948 (January 2005): "UDP Encapsulation of IPsec ESP Packets".
- RFC 4072 (August 2005): "Diameter Extensible Authentication Protocol (EAP) Application".
- RFC 4187 (January 2006): "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".
- RFC 4303 (December 2005): "IP Encapsulating Security Payload (ESP)".
- RFC 4306 (December 2005): "Internet Key Exchange (IKEv2) Protocol".
- RFC 4739 (November 2006): "Multiple Authentication Exchanges in the Internet Key Exchange (IKEv2) Protocol".
- RFC 5213 (August 2008): "Proxy Mobile IPv6".
- RFC 5845 (June 2010): "Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6".
- RFC 5846 (June 2010): "Binding Revocation for IPv6 Mobility".
- RFC 5996 (September 2010): "Internet Key Exchange Protocol Version 2 (IKEv2)".



CHAPTER 2

Configuring the SaMOG Gateway

This chapter provides configuration instructions for the SaMOG (S2a Mobility Over GTP) Gateway. Information about the commands in this chapter can be found in the *Command Line Interface Reference.*

• Configuring the System to Perform as a SaMOG Gateway, on page 77

Configuring the System to Perform as a SaMOG Gateway

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to perform as a SaMOG Gateway in a test environment.

Required Information

The following sections describe the minimum amount of information required to configure and make the SaMOG Gateway operational in the network. To make the process more efficient, it is recommended that this information be available prior to configuring the system.

The following table lists the information that is required to configure the SaMOG Gateway context and service.

Table 19: Required Information for SaMOG Configuration

Required Information	Description
SaMOG Context and MRME, CGW and SaMOG Service Configuration	
SaMOG context name	The name of the SaMOG context, which can be from 1 to 79 alpha and/or numeric characters.
MRME service name	The name of the MRME service, which can be from 1 to 63 alpha and/or numeric characters.
IPv4 address	The IP address to which you want to bind the MRME service.
context DNS	The name of the context to use for PGW DNS.
IPV4_address/subnetmask	The IPv4 address and subnetmask for the destination RADIUS client the MRME service will use.

Required Information	Description
Key	The name of the encrypted key for use by the destination RADIUS server.
Port Number	The port number for RADIUS disconnect messages.
IPv4 address	The IPv4 address of the RADIUS client
Key	The encrypted key name for use by the RADIUS client.
Port	The port number used by the RADIUS client.
CGW service name	The name of the CGW service, which can be from 1 to 63 alpha and/or numeric characters.
IPv4 address	The IPv4 address to which the CGW service will bind.
Egress EGTP service name	The name of the egress EGTP service that the CGW service will use. This name must match the name of the EGTP service configured later in this procedure.
Timeout	The session delete delay timeout setting for use by CGW service.
SaMOG service name	The name of the SaMOG service, which can be from 1 to 63 alpha and/or numeric characters.
MRME service name	The name of the MRME service to associate with this SaMOG service. This is the MRME service name configured previously in this procedure.
CGW service name	The name of the CGW service to associate with this SaMOG service. This is the CGW service name configured previously in this procedure.
Subscriber map name	The subscriber map name to associate with the SaMOG service. This name must match the subscriber map name configured later in this procedure.
LTE Policy Configuration	
Subscriber map name	The name of the subscriber map to associate with the LTE policy, which can be from which can be from 1 to 64 alpha and/or numeric characters.
Precedence priority	Specifies the prcedence for the subscriber map. Must be an integer from 1 to 1024.
Service criteria type	Specifies the service criteria that must be matched for the subscriber map. Must be one of **imsi**, **service-plmnid** or **all**.
MCC number	The Mobile Country Code for use in this LTE policy.

Required Information	Description
MNC	The Mobile Network code for use in this LTE policy.
Operator policy name	The name of the operator policy use with the subscriber map, which can be from 1 to 64 alpha and/or numeric characters.
TAI mgmt db name	The name of the Tracking Area Identifier database for use with the LTE policy, which can be from 1 to 64 alpha and/or numeric characters.
GTPU and EGTP Service Configuration	
SaMOG context name	The name of the SaMOG context configured previously.
EGTP service name	The name for this EGTP service, which can be from 1 to 63 alpha and/or numeric characters.
EGTP service name	The name of the EGTP service name that you want to associate with the GTPU service. This is the EGTP service name configured previously.
IPv4 address	The IPv4 address to which you want to use to bind the EGTP service to the GTPU service.
GTPU service name	The name of the GTPU service, which can be from 1 to 63 alpha and/or numeric characters.
IPv4 address	The IP address to which the GTPU service will bind.
AAA and Diameter Endpoint Configuration	
AAA context name	The name assigned to the AAA context, which can be from 1 to 79 alpha and/or numeric characters.
AAA interface name	The name assigned to the AAA interface, which can be from 1 to 79 alpha and/or numeric characters.
IPv4 address/subnetmask	The primary IPv4 address and subnetmask for use by the AAA interface.
IPv4 address subnetmask	The secondary IPv4 address and subnetmask for use by the AAA interface.
SaMOG context name	The name of the SaMOG context configured earlier.
AAA DIAMETER STa1 group name	The primary AAA group name for use over the STa interface, which can be from 1 to 63 alpha and/or numeric characters.
DIAMETER endpoint name	The DIAMETER authentication endpoint name for use with this AAA group.

Required Information	Description
AAA DIAMETER STa2 group name	The secondary AAA group name for use over the STa interface, which can be from 1 to 63 alpha and/or numeric characters.
DIAMETER endpoint name	The DIAMETER authentication endpoint name for use with the secondary AAA group.
AAA Accounting Group Name	The name of the AAA Accounting group, which can be from 1 to 63 alpha and/or numeric characters.
Diameter authentication dictionary	The name of the Diameter dictionary used for authentication. This must be configured as the aaa-custom13 dictionary.
DIAMETER endpoint name	The name of the DIAMETER endpoint, which can be from 1 to 63 alpha and/or numeric characters. This is the name of the external 3GPP AAA server.
STa endpoint name	The name of the DIAMETER endpoint, which can be from 1 to 63 alpha and/or numeric characters. This is the name of the external 3GPP AAA server.
Origin real name	Name of the local Diameter realm, which can be a a string from 1 to 127 alpha and/or numeric characters.
Origin host STa endpoint IPv4 address	The IPv4 address of the origin host STa endpoint.
IPv4 address	The IPv4 address used for the origin host STa endpoint.
Port	The port used for the origin host STa endpoint.
Peer name	The name of the Diameter peer, which can be from 1 to 63 alpha and/or numeric characters.
SaMOG realm name	The name of the peer Diameter realm, which can be from 1 to 63 alpha and/or numeric characters.
IPv4 address	The IPv4 address for the peer STa endpoint.
Port	The port used for the peer STa endpoint.
DNS Configuration	
DNS context name	The name of the context in which DNS will be configured, which can be from 1 to 79 alpha and/or numeric characters.
DNS interface name	The name of the DNS interface, which can be from 1 to 79 alpha and/or numeric characters.
IPv4 address	The IPv4 address of the DNS server.

Required Information	Description
IP name server IP address	The IP name server IPv4 address.
DNS client	The name of the DNS client, which can be from 1 to 63 alpha and/or numeric characters.
IPv4 address	The IPv4 address to which you want to bind the DNS client service.
Configuring and Binding the Interfaces	
SaMOG service Interface port/slot	The slot and port number to which you want to bind the SaMOG service.
GTP SaMOG interface name and context	The SaMOG interface and context name that will be bound to the SaMOG interface port/slot.
STa Accounting service interface port/slot	The slot and port number to which you want to bind the STa accounting interface.
STa Accounting service name and context	The name and context name of the STa accounting interface that you want to bind to the STa accounting port/slot.
DNS service Interface slot/port	The slot and port number that to which you want to bind the DNS service.
DNS service interface name and context.	The name and context name that you want to bind to the DNS interface slot/port.
Radius PMIP-side service interface port/slot.	The slot and port number to which you want to bind the PMIP-side RADIUS interface.
Radius PMIP-side service interface name and context.	The name and context name of the PMIP side RADIUS interface you want to bind to the RADIUS interface port/slot.
Radius SaMOG-side service interface port/slot.	The slot and port number to which you want to bind the SaMOG-side RADIUS interface.
GTPU interface port/slot.	The slot and port number to which you want to bind the GTPU-interface.

SaMOG Gateway Configuration

The high-level steps below summarize the SaMOG gateway configuration tasks. Steps 1 through 8 are mandatory. Steps 8 through 11 are optional. Note that the SaMOG Gateway is a licensed Cisco product. Separate session and feature licenses may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, see "Managing License Keys" in the *System Administration Guide.*

Step 1 Set system configuration parameters such as activating PSC2s, ports, and enabling session recovery by following the configuration examples in the *System Administration Guide.*

Step 2 Create the SaMOG context by applying the example configuration in Creating the SaMOG Gateway Context , on page 82.

Step 3 Configure the MRME, CGW, and SaMOG services by applying the example configuration in Configuring the MRME, CGW and SaMOG Services, on page 83.

Step 4 Configure the LTE policy by applying the example configuration in Configuring the LTE Policy, on page 84.

Step 5 Create the GTPU and EGTP services by applying the example configuration in Configuring the GTPU and EGTP Services, on page 84.

Step 6 Create MAG services for a PMIPv6-based S2a interface by applying the example configuration in Configuring MAG Services, on page 85.

Step 7 Optional. Configure the IP over GRE (IPoGRE) encapsulation for processing DHCP Layer 3 IP packets by applying the example configuration in Configuring IPoGRE, on page 85.

Step 8 Optional. Configure the IP over VLAN (IPoVLAN) encapsulation for processing DHCP Layer 3 IP packets by applying the example configuration in Configuring IPoVLAN, on page 86.

Step 9 Create and configure the AAA group for Diameter and AAA authentication and accounting by applying the example configuration in Configuring AAA, on page 87.

Step 10 Configure the GTPP group consisting of the GTPP dictionary and CDR attributes, to be used for SGW and SGSN CDRs, and associate the GTPP group to the SaMOG Call Control Profile by applying the example configuration in Configuring GTPP Dictionary and CDR Attributes, on page 87.

Step 11 Configure the DNS service by applying the example configuration in Configuring DNS, on page 88.

Step 12 Optional. Enable Local breakout for an APN by applying the example configuration in Configuring Local Breakout, on page 88.

Step 13 Optional. Enable web-based authorization by applying the example configuration in Configuring Web-based Authorization, on page 91.

Step 14 Configure and bind interfaces to the relevant interfaces by applying the example configuration in Configuring and Binding the Interfaces, on page 94.

Step 15 Optional. Enable event logging by applying the example configuration in Enabling Logging, on page 94.

Step 16 Optional. Enable the sending of CGW and SaMOG SNMP traps by applying the example configuration in Enabling SNMP Traps, on page 95.

Step 17 Optional. Configure the system to gather and transfer bulk statistics by applying the example configuration in Configuring Bulk Statistics, on page 95.

Step 18 Save the completed configuration by following the instructions in Saving the Configuration, on page 96.

Creating the SaMOG Gateway Context

Create the context in which the SaMOG service will reside. The MRME, CGW, SaMOG and other related services will be configured in this context. Create the SaMOG context by applying the configuration example below.

```
config
      context  samog_context_name
      end
```

Configuring the MRME, CGW and SaMOG Services

The MRME and CGW services provide the SaMOG functionality. They must be configured in the SaMOG context and then associated with a SaMOG service name. Configure the MRME, CGW, and SaMOG services by applying the example configuration below.

```
            context context_name
                twan-profile twan_profile_name
                    radius client {  ipv4/ipv6_address [/mask ] } [ encrypted
 ] key value [ disconnect-message [ dest-port destination_port_number ] ] [
dictionary { custom70 | custom71 } ]
                     ue-address [ dhcp | twan ]
            exit
            mrme-service  mrme_service_name
# Release 18 and earlier:
                  bind address   ip4_address
# Release 19 and later:
                  bind { ipv4-address  ipv4_address [ ipv6-address ipv6_address
 ] | ipv6-address ipv6_address [ ipv4-address ipv4_address ] }
                   associate twan-profile twan_profile_name
                   dns-pgw context dns
 radius client  ip4_address/subnetmask encrypted key key  disconnect-message
dest-port  port_no
                   exit
            cgw-service  cgw_service_name
                bind { ipv4-address  ipv4_address [ ipv6-address ipv6_address
 ] | ipv6-address ipv6_address [ ipv4-address ipv4_address ] }
                   associate egress-egtp_service egress-egtp_service_name
                   revocation enable
                   session-delete-delay timeout  timeout_msecs
                   exit
            samog-service samog_service_name
 associate mrme-service  mrme_service_name
                   assoicate cgw-service  cgw_service_name
                   associate subscriber-map  subscriber_map_name
                   associate dhcp-service  dhcp_service_name [ level { system
 | user } ]
               # Associate a DHCPv6 service
                   associate dhcpv6-service  dhcpv6_service_name
                   exit
```

Important Configure the custom71 dictionary when Cisco WLC is used with PMIPv6 as the access-type. Configuring the custom71 dictionary enables attributes like the UE's permanent identity (NAI), subscribed APN, network protocol (PMIPv6), and LMA address (CGW service's bind address) to be sent in the Cisco Vendor-specific attributes to WLC. The WLC uses this information to build the PMIPv6 PBU to the SaMOG gateway when the **aaa-override** option is enabled on the Cisco WLC. These attributes are not sent when the custom70 dictionary is configured.

Notes:

- Use the **ue-address** command to configure Layer 3 IP access-type only.

- When the **associate dhcpv6-service** *dhcpv6_service_name* is configured, SaMOG will use the bind address configured under the DHCPv6 Service Configuration Mode for DHCPv6 server functionality.

Configuring the LTE Policy

Configure the LTE policy by applying the example configuration below.

```
config
      operator-policy policy-name
            apn network-identifier  apn_net_id apn-profile apn_profile_name
            associate call-control-profile   profile_id
            exit
      call-control-profile profile_name
            accounting mode gtpp
            authenticate context context_name aaa-group aaa_group_name
            accounting context context_name aaa-group aaa_group_name
            accounting context context_name gtpp-group gtpp_group_name
            assocaite accounting-policy  policy_name
            exit
      apn-profile profile_name
            accounting mode none
            local-offload
            address-resolution-mode local
            pgw-address IP_address
            qos default-bearer qci qci_id
            qos default-bearer arp arp_value preemption-capability may
vulnerability not-preemptable
            qos apn-ambr max-ul mbr-up max-dl mbr-dwn
            pdp-type-ipv4v6-override ipv4
            virtual-mac { mac_address | violation drop }
            twan default-gateway ipv4/ipv6_address/mask
            exit
      lte-policy
            subscriber-map   subscriber_map_name
                  precedence precedence_priority  match-criteria
service_criteria_type  mcc  mcc_number  mnc  mnc_number  operator-policy-name
operator_policy_name
                  precedence precedence_priority  match-criteria
service_criteria_type  operator-policy-name  operator_policy_name
                  exit
            tai-mgmt-db  tai_mgmt_db_name
           exit
```

Configuring the GTPU and EGTP Services

Configure the GTPU and EGTP services by applying the example configuration below.

```
config
      context samog_context_name
            egtp-service  egtp_service_name
            associate gtpu-service  egtp_service_name
```

```
        gtpc bind ipv4-address ipv4_address
        exit
    gtpu-service gtpu_service_name
        bind ipv4-address ipv4_address
        exit
```

Configuring MAG Services

Create MAG services to configure a PMIPv6-based S2a interface by applying the example configuration below.

```
config
    context context_name
        cgw-service cgw_service_name
            bind ipv4-address ipv4_address
            associate mag-service mag_service_name
            exit
        mag-service mag_service_name
            bind ipv4-address ipv4_address
            reg-lifetime max_reg_duration
            mobility-option-type-value standard
            end
```

Configuring IPoGRE

Important The IP over GRE functionality requires an additional GRE Interface Tunneling license to create IP-GRE tunnels. For more information, contact your Cisco account representative.

Configure IP over GRE (IPoGRE) encapsulation for processing DHCP Layer 3 IP packets by applying the example configuration below.

```
config
    context context_name
        ip vrf vrf_name
        exit
    interface interface_name
        ip address ip_address[/mask ]ipv4/v6_address
        exit
    interface interface_name1
        ip address ip_address[/mask ]ipv4/v6_address
        exit
    interface interface_tunnel_name tunnel
        ip vrf forwarding gre_vrf_name
        ip address ip_address[/mask ]ipv4/v6_address
        tunnel-mode gre
            source interface interface_name
            destination address ipv4_address
            exit
        exit
```

```
ip route ipv4_address ipv4_address tunnel interface_tunnel_name
port ethernet  port_number
     no shutdown
     bind interface   interface_name1 context_name
     vlan vlan_number
          no shutdown
          ingress-mode
          bind interface interface_name context_name
          end
```

Notes:

- Use the **interface** *interface_name1* configuration only if a VRF-GRE tunnel is required.
- Use the **ip vrf forwarding** command to associate a GRE tunnel with the VRF.

Configuring IPoVLAN

Configure IP over VLAN (IPoVLAN) encapsulation for processing DHCP Layer 3 IP packets by applying the example configuration below.

```
config
     context context_name
          ip vrf vrf_name
          exit
     interface interface_name
          ip address ip_address ip_address
          exit
     interface interface_name1
          ip vrf forwarding  vrf_name
          ip address ip_address ip_address
          exit
     ip route ip_address[/mask ] next-hop ip_address interface_name1 vrf vrf_name
     ip route ip_address[/mask ] next-hop ip_address interface_name1 vrf vrf_name
     port ethernet  port_number
          no shutdown
          ingress-mode
          bind interface   interface_name context_name
          vlan vlan_number
               ingress-mode
               bind interface interface_name1 context_name
               no shutdown
               end
config
     context context_name
          twan-profile twan_profile_name
               ue-address dhcp
               access-type client ipv4_address[/mask ] ip
               access-type ip vrf  vrf_name
               radius ip vrf  vrf_name
               radius client   ipv4_address[/mask ] key shared_secret_key
disconnect-message dest-port port_number dictionary custom71
               end
```

Notes:

- Use the **ip vrf forwarding** command to associate a GRE tunnel with the VRF.
- Use the **ingress-mode** command to process UL user packets for L3IP access-type.
- Each TWAN Profile creates a "aaa group" in all AAAMgrs with the name **samog_rad_grp_***twan_profile_name*.

Configuring AAA

Create the AAA group for DIAMETER authentication and then configure AAA accounting and authentication by applying the example configuration below.

```
config
      context aaa_context_name
            interface aaa_interface_name
                  ip address ipv4_address/subnetmask
                  ip address ipv4_address/subnetmask secondary
                  end
config
      context samog_context_name
            aaa group aaa_diameterSTa1_group_name
                  diameter authentication dictionary aaa-custom13
                  diameter authentication endpoint endpoint_name
                  exit
            aaa group aaa_group_diameter_STa2_name
                  diameter authentication dictionary aaa-custom13
                  diameter authentication endpoint endpoint_name
                  exit
            aaa group aaa_acct_group_name
                  radius attribute nas-ip-address address ipv4-address
                  radius accounting server ipv4_address encrypted key key
  port port_no
                  exit
            aaa group default
            exit
      gtpp group default
      exit
diameter endpoint STA_endpoint_name
      origin realm realm_name
      use-proxy
      origin host STa_endpoint_ipv4_address address ipv4_address port port_no
      no watchdog-timeout
      peer peer_name realm samog_realm_name address ipv4_address port port_no
      exit
```

Configuring GTPP Dictionary and CDR Attributes

Configure the GTPP dictionary to be used for SGW and SGSN CDRs and the CDR attributes for the SaMOG gateway by applying the example configuration below.

```
config
      context  samog_context_name
            gtpp group gttp_group_name
                  gtpp charging-agent IPv4/IPv6_Address
                  gtpp server Server_IPv4/IPv6_Address max Maximum_GTPP_Messages
                  gtpp trigger volume-limit
                  gtpp trigger time-limit
                  gtpp dictionary custom24
                  gtpp attribute local-record-sequence-number
                  gtpp attribute local-record-sequence-number
                  gtpp attribute msisdn
                  gtpp attribute diagnostics
                  gtpp attribute dynamic-flag
                  gtpp attribute record-type sgsnpdprecord
                  gtpp attribute record-type sgwrecord
                  gtpp attribute qos max-length qos_max_length
                  end
config
      call-control-profile call_control_profile_name
            accounting context samog_context_name gtpp group gtpp_group_name
```

Configuring DNS

Configure DNS for the SaMOG gateway by applying the example configuration below.

```
config
      context  dns_context_name
            interface  dns_interface_name
                  ip address  ipv4_address/subnetmask
 exit
            subscriber default
            exit
      aaa group default
      exit
      gtpp group default
      ip domain-lookup
      ip name-servers ipv4-address
      dns-client dns_client_name
            bind address ipv4_address
      exit
```

Configuring Local Breakout

Optionally, configure the local breakout - enhanced, or local breakout - basic, or flow-based (with or without external NAT) local breakout model for an APN (assuming that a P-GW service is configured) by applying the appropriate example configuration below:

Important The Local Breakout (LBO) feature is license dependent. Each LBO models require separate feature licenses. While the LBO - Basic and Flow-based LBO licenses can co-exist, they are mutually exclusive with the LBO - Enhanced license. Contact your local Cisco account representative for licensing requirements.

Local Breakout - Enhanced

```
config
      context context_name
            cgw-service service_name
                  associate pgw-service service_name
                  exit
            exit
      apn-profile profile_name
            local-offload
            end
```

Local Breakout - Basic

```
config
     apn-profile apn_profile_name
         local-offload
         ip address pool name pool_name
         ip context-name vpn_context_name
         dns primary ipv4_address
         dns secondary ipv4_address
         ip access-group access_list_name [ in | out ]
         active-charging rulebase rulebase_name
         exit
    context context_name
        ip pool pool_name ip_address/mask public priority subscriber-gw-address
 router_ip_address
         ip access-list access_list_name
              redirect css service acs_service_name any
              exit
         exit
    active-charging service acs_service_name
         access-ruledef access_ruledef_name
              ip any-match = TRUE
              exit
         fw-and-nat policy policy_name
             access-rule priority priority access-ruledef access_ruledef_name
 permit nat-realm nat_realm_name
              exit
         rulebase rulebase_name
              fw-and-nat default-policy policy_name
              end
```

Flow-based Local Breakout

```
config
     apn-profile apn_profile_name
          local-offload flow
          ip context-name vpn_context_name
          ip access-group access_list_name [ in | out ]
          active-charging rulebase rulebase_name
          exit
    context context_name
          ip access-list access_list_name
               redirect css service acs_service_name any
               exit
          exit
```

After applying the above initial configuration for Flow-based LBO, you can configure either a flow-based LBO whitelist or a blacklist.

Flow-based LBO with External NAT

SaMOG can also perform flow-based LBO with external NAT devices based on nex-hop. Configure flow-based LBO with an external NAT by applying the example configuration below:

```
config
 active-charging service acs_service_name
 rulebase rulebase_name
 action priority action_priority_1 ruledef ruledef_name_1 charging-action
charging_action_name
 action priority action_priority_2 ruledef ruledef_name_2 charging-action
charging_action_name
 exit
 ruledef ruledef_name_1
 ip dst-address = ipv6_address[/mask ]
 exit
 ruledef ruledef_name_2
 ip dst-address = ipv4_address[/mask ]
 exit
 charging-action charging_action_name
 nexthop-forwarding-address ipv4_address
 exit
 exit
    # To configure IPv6 Access List
 context context_name
 ipv6 access-list ipv6_acl_name
 redirect css service css_service_name any
 exit
 exit
    # To configure the APN profile to use the IPv6 access list
 apn-profile apn_profile_name
 ip access-group ipv6_acl_name in
 ip access-group ipv6_acl_name out
         # To configure IPv6 DNS servers for GTPv2 sessions on flow-based LBO
 dns ipv6 { primary | secondary } ipv6_address
 end
```

Flow-based LBO Whitelist

```
active-charging service acs_service_name
     access-ruledef access_ruledef_name
          ip dst-address = ipv4_destination_address[/mask ]
          exit
     fw-and-nat policy policy_name
         access-rule priority priority access-ruledef access_ruledef_name
permit bypass-nat
        access-rule no-ruledef-matches uplink action permit nat-realm
nat_realm_name
          access-rule no-ruledef-matches downlink action permit
nat-realm nat_realm_name
          exit
     rulebase rulebase_name
          fw-and-nat default-policy policy_name
          end
```

Notes:

- The *nat_realm_name* is the IP pool used by the NAT service for dynamic NATting. This IP pool may have one-to-one or many-to-one users mapping to conserve IP addresses.

Flow-based LBO Blacklist

```
active-charging service acs_service_name
     access-ruledef access_ruledef_name
          ip dst-address = ipv4_destination_address[/mask ]
          exit
     fw-and-nat policy policy_name
         access-rule priority priority access-ruledef access_ruledef_name
permit nat-realm nat_realm_name
          access-rule no-ruledef-matches uplink action permit
bypass-nat
          access-rule no-ruledef-matches downlink action permit
bypass-nat
          exit
     rulebase rulebase_name
          fw-and-nat default-policy policy_name
          end
```

Notes:

- The *nat_realm_name* is the IP pool used by the NAT service for dynamic NATting. This IP pool may have one-to-one or many-to-one users mapping to conserve IP addresses.

Configuring Web-based Authorization

Important The Web Authorization feature is license dependent. Contact your local Cisco account representative for licensing requirements.

Optionally, configure the SaMOG web-based authorization by applying the example configuration below.

HTTP Redirection for Web-based Authorization

For HTTP redirection, apply the following rulebase, ruledef and charging action example:

```
config
      active-charging service acs_service_name
             #Rule to analyze HTTP packets
             ruledef http_ruledef_name
                    tcp either-port = 80
                    tcp either-port = 8080
                    rule-application routing
                    exit
             #Rule to check if packet is a DNS packet
             ruledef is_DNS_ruledef_name
                    udp either-port = port_number
                    tcp either-port = port_number
                    multi-line-or all-lines
                    exit
            #Rule to check if packet is destined to HTTP portal (to avoid
 redirect loop)
             ruledef is_redirected_ruledef_name
                    ip server-ip-address = http_web_portal_ipv4_address/mask
                    exit
             #Rule for HTTP redirection to HTTP portal
             ruledef http_redirect_ruledef_name
                    http any-match = TRUE
                    ip any-match = TRUE
                    multi-line-or all-lines
                    exit
             #Action to allow packets without throttling at ECS
             charging-action allow_charging_action_name
                    content-id content_id_2
                    exit
             #Action to perform HTTP 302 redirection
             charging-action page_redirect_charging_action_name
                    content-id content_id_3
                    flow action redirect-url http_web_portal_url
                    exit
             #Rulebase with all above rules and actions
             rulebase rulebase_name
                    retransmissions-counted
                    #Run protocol analyzers
                    route priority route_priority ruledef http_ruledef_name
analyzer http
                    #Take action based on protocol analyzer result
                    action priority action_priority ruledef is_DNS_ruledef_name
 charging-action allow_charging_action_name
                    action priority action_priority ruledef
is_redirected_ruledef_name charging-action allow_charging_action_name
                    action priority action_priority ruledef
```

```
http_redirect_ruledef_name charging-action page_redirect_charging_action_name
                    end
```

HTTPS Redirection for Web-based Authorization

For HTTPS redirection, as the HTTPS packets are encrypted using SSL/TLS between the client and server, the ACS service will not be able to perform HTTP request inspection. All HTTPS packets are redirected to an external web portal using Layer 3/Layer 4 redirection rules. The web portal performs an SSL handshake with the UE and redirects for authenticaiton.

Apply the following rulebase, ruledef and charging action example for HTTPS redirection:

```
config
      active-charging service acs_service_name
            #Rule to allow DNS packets
            ruledef is_dns_ruledef_name
                  udp either-port = 53
                  tcp either-port = 53
                  multi-line-or all-lines
                  exit
            #Rule to check if the packet is destined to the web portal,
 to avoid redirect loop
            ruledef is_redirect_ruledef_name
                  ip server-ip-address = web_portal_ip_address
                  exit
            #Rule to check if the packet is an HTTPS packet
            ruledef is_https_ruledef_name
                  tcp either-port = 443
                  multi-line-or all-lines
                  exit
            #Action to allow packets without throttling at ECS
            charging-action allow_charging_action_name
                  content-id content_id_1
                  exit
            #Charging action to redirect all HTTPS packets (including
initial TCP SYN/SYNACK/ACK) to web portal
            charging-action l4_redirect_charging_action_name
                  content-id content_id_2
                  flow action readdress server web_portal_ip_address port
port_number
                  exit
            rulebase rulebase_name
                  action priority priority ruledef is_dns_ruledef_name
charging_action allow_charging_action_name
                  action priority priority ruledef
is_redirect_ruledef_namecharging_action allow_charging_action_name
                  action priority priority ruledef is_https_ruledef_name
charging_action l4_redirect_charging_action_name
```

Once the ruledef, charging action and rulebase are configured based on HTTP or HTTPS redirection, apply the rest of the configuration for web authorization as specified below:

```
configure
    operator-policy  { default | name  policy_name }
```

```
            apn  webauth-apn-profile apn_profile_name
            exit
        apn-profile  profile_name
            active-charging rulebase rulebase_name
            dns { primary | secondary } IPv4_address
            dhcp lease { short duration | time duration }
            ip address pool name  pool_name
            ip context-name  context_name
            ip access-group group_name [ in | out ]
            ipv6 address prefix-pool pool_name
            exit
        call-control-profile  profile_name
            timeout imsi cache  timer_value
            subscriber  multi-device
            authenticate context context_name auth-method { [ eap ] [non-eap]
}
            end
```

Configuring and Binding the Interfaces

The interfaces created previously now must be bound to physical ports. Bind the system interfaces by applying the example configuration below.

```
config
      port ethernet  slot no/port no
            no shutdown
            bind interface gtp_samog_interface_name  gtp_samog_context name
            exit
      port ethernet  slot no/port no
            bind interface interface  STa_acct_interface_name STa_acct_context_name
            exit
      port ethernet  slot no/port no
            bind interface dns_interface_name  dns_context name
            exit
      port ethernet  slot no/port no
            bind interface wlc_pmip_side_interface_name wlc_pmip_side_context_name
            exit
      port ethernet  slot no/port no
            bind interface wlc_side_samog_interface_name wlc_side_samog_context name

      port ethernet  slot no/port no
            bind interface gtpu_interface_name gtpu/gtpc_context name
            end
```

Enabling Logging

Optional. Enable event logging for the SaMOG Gateway by applying the example configuration below from the Command Line Interface Exec Mode.

```
[local]asr5000#  logging filter active facility mrme level  error_reporting_level
[local]asr5500#  logging filter active facility cgw level  error_reporting_level
```

```
[local]asr5500# logging filter active facility ipsgmgr level
error_reporting_level
[local]asr5500# logging filter active facility radius-coa level
error_reporting_level
[local]asr5500# logging filter active facility radius-auth level
error_reporting_level
[local]asr5500# logging filter active facility radius-acct level
error_reporting_level
[local]asr5500# logging filter active facility diabase level
error_reporting_level
[local]asr5500# logging filter active facility diameter-auth level
error_reporting_level
[local]asr5500# logging filter active facility aaamgr level error_reporting_level
[local]asr5500# logging filter active facility aaa-client level
error_reporting_level
[local]asr5500# logging filter active facility diameter level
error_reporting_level
[local]asr5500# logging filter active facility mobile-ipv6 level
error_reporting_level
[local]asr5500# logging filter active facility hamgr level error_reporting_level
[local]asr5500# logging filter active facility ham diameter-ecs level
error_reporting_level
[local]asr5500# logging filter active facility egtpc level error_reporting_level
[local]asr5500# logging filter active facility egtpmgr level
error_reporting_level
```

Enabling SNMP Traps

Optional. Enable the sending of SaMOG gateway-related SNMP traps by applying the example configuration below.

```
config
      context samog_context_name
            snmp trap enable SaMOGServiceStart
            snmp trap enable SaMOGServiceStop
            snmp trap enable CGWServiceStart
            snmp trap enable CGWServiceStop
            end
```

To disable the generation of an SNMP trap:

```
config
      contextsamog_context_name
            snmp trap suppress trap_name
            end
```

Configuring Bulk Statistics

Use the following configuration example to enable SaMOG bulk statistics:

```
config
      bulkstats collection
      bulkstats mode
 sample-interval minutes
```

```
                transfer-interval  minutes
                file  no
                      remotefile format  format
/localdisk/bulkstats/bulkstat%date%%time%.txt
                    receiver  ipv4_or_ipv6_address  primary mechanism sftp login
  login_name  encrypted password samog schema  schema_name  format  schema_format
```

Notes:

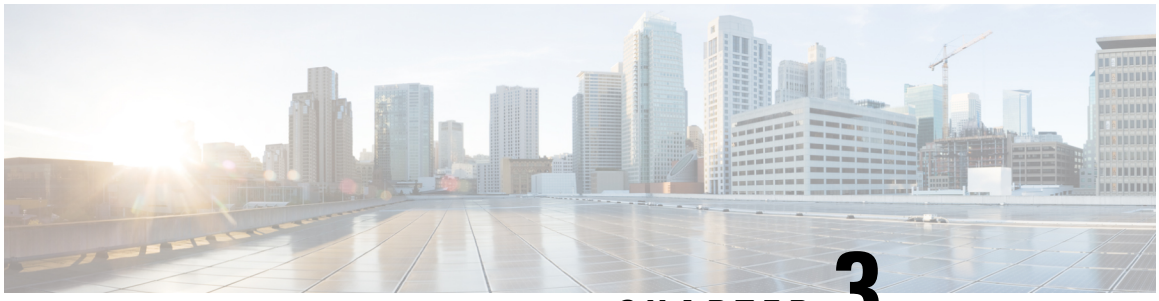
- The **bulkstats collection** command in this example enables bulk statistics, and the system begins collecting pre-defined bulk statistical information.
- The **bulkstats mode** command enters Bulk Statistics Configuration Mode, where you define the statistics to collect.
- The **sample-interval** command specifies the time interval, in minutes, to collect the defined statistics. The *minutes* value can be in the range of 1 to 1440 minutes. The default value is 15 minutes.
- The **transfer-interval** command specifies the time interval, in minutes, to transfer the collected statistics to the receiver (the collection server). The *minutes* value can be in the range of 1 to 999999 minutes. The default value is 480 minutes.
- The **file** command specifies a file in which to collect the bulk statistics. A bulk statistics file is used to group bulk statistics schema, delivery options, and receiver configuration. The *number* can be in the range of 1 to 4.
- The **receiver** command in this example specifies a primary and secondary collection server, the transfer mechanism (in this example, ftp), and a login name and password.
- The **samog schema** command specifies that the SaMOG schema is used to gather statistics. The *schema_name* is an arbitrary name (in the range of 1 to 31 characters) to use as a label for the collected statistics defined by the **format** option. The **format** option defines within quotation marks the list of variables in the SaMOG schema to collect. The format string can be in the range of 1 to 3599.

For descriptions of the SaMOG schema variables, see "SaMOG Schema Statistics" in the *Statistics and Counters Reference.* For more information on configuring bulk statistics, see the *System Administration Guide.*

Saving the Configuration

Save the SaMOG configuration file to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**.

For additional information on how to verify and save configuration files, see the *System Administration Guide* and the *Command Line Interface Reference.*



CHAPTER 3

Monitoring the SaMOG Gateway

This chapter provides information for monitoring the status and performance of the SaMOG (S2a Mobility Over GTP) Gateway using the **show** commands found in the CLI (Command Line Interface). These command have many related keywords that allow them to provide useful information on all aspects of the system ranging from current software configuration through call activity and status.

The selection of **show** commands listed in this chapter is intended to provided the most useful and in-depth information for monitoring the system. For additional information on these and other **show** commands and keywords, refer to the *Command Line Interface Reference.*

The system also supports the sending of Simple Network Management Protocol (SNMP) traps that indicate status and alarm conditions. See the *SNMP MIB Reference* for a detailed listing of these traps.

Monitoring SaMOG Gateway Status and Performance

The following table contains the CLI commands used to monitor the status of the SaMOG Gateway features and functions. Output descriptions for most of the commands are located in the *Statistics and Counters Reference.*

Table 20: SaMOG Gateway Status and Performance Monitoring Commands

To do this:	Enter this command:
View Service Information and Statistics	
View SaMOG service information and statistics.	**show samog-service { all | name** *service_name* }
View additional SaMOG service statistics.	**show samog-service statistics { all | samog-service** *service_name* }
View CGW service information and statistics.	**show cgw-service { all | name** *service_name* }
View MRME service information and statistics.	**show mrme-service { all | name** *service_name* }
View additional session statistics.	**show session disconnect-reasons** **show session duration**

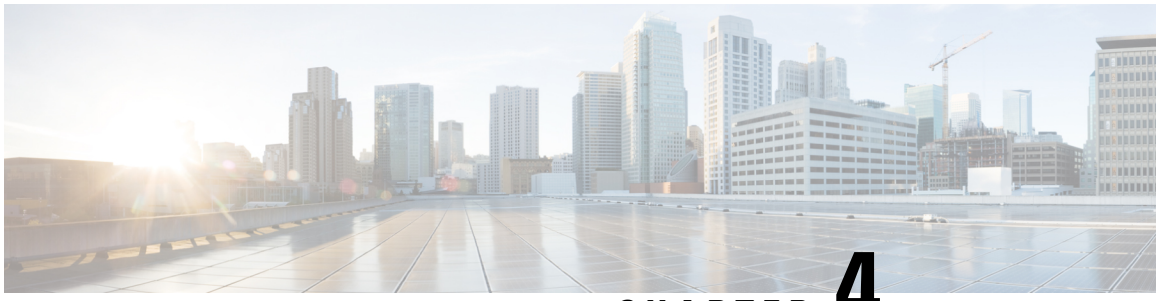
To do this:	Enter this command:
View SaMOG Gateway bulk statistics.	**show bulkstats variables samog**
View bulk statistics for the system.	**show bulkstats data**
View Diameter AAA Server Information	
View Diameter AAA server statistics.	**show diameter aaa-statistics all**
View Diameter message queue counters.	**show diameter message-queue counters { inbound | outbound }**
View Diameter statistics.	**show diameter statistics**
View Subscriber Information	
View Subscriber Configuration Information	
View locally configured subscriber profile settings (must be in the context where the subscriber resides).	**show subscribers configuration username** *subscriber_name*
View remotely configured subscriber profile settings.	**show subscribers aaa-configuration username** *subscriber_name*
View subscriber information based on IPv6 address.	**show subscribers ipv6-address** *ipv6_address*
View subscriber information based on IPv6 address prefix.	**show subscribers ipv6-prefix** *prefix*
View subscriber information based on caller ID.	**show subscribers callid** *call_id*
View subscriber information based on username.	**show subscribers username** *name*
View information for troubleshooting subscriber sessions.	**show subscribers debug-info**
View a summary of subscriber information.	**show subscribers summary**
View Subscribers Currently Accessing the System	
View a list of subscribers currently accessing the system.	**show subscribers all**
View a list of SaMOG Gateway subscribers currently accessing the system.	**show subscribers samog-only [all | full]**
View a list of SaMOG Gateway subscribers currently accessing the system per SaMOG service.	
View the P-CSCF addresses received from the P-GW.	**show subscribers full username** *subscriber_name*
View statistics for subscribers using a LMA service on the system.	**show subscribers lma-only [all | full | summary]**

To do this:	Enter this command:
View statistics for subscribers using a LMA service per LMA service.	**show subscribers lma-service** *service_name*
View Session Subsystem and Task Information	
View Session Subsystem Statistics **Important** Refer to the *System Administration Guide* for additional information on the Session subsystem and its various manager tasks.	
View AAA Manager statistics.	**show session subsystem facility aaamgr all**
View AAA Proxy statistics.	**show session subsystem facility aaaproxy all**
View Session Manager statistics.	**show session subsystem facility sessmgr all**
View LMA Manager statistics.	**show session subsystem facility magmgr all**
View session progress information for the SaMOG service.	**show session progress samog-service** *service_name*
View session duration information for the SaMOG service.	**show session duration samog-service** *service_name*
View Task Statistics	
View resource allocation and usage information for Session Manager.	**show task resources facility sessmgr all**
View Session Resource Status	
View session resource status.	**show resources session**
View Session Recovery Status	
View session recovery status.	**show session recovery status [verbose]**
View Session Disconnect Reasons	
View session disconnect reasons.	**show session disconnect-reasons**

Clearing Statistics and Counters

It may be necessary to periodically clear statistics and counters in order to gather new information. The system provides the ability to clear statistics and counters based on their grouping.

Statistics and counters can be cleared using the CLI **clear** command. Refer to the *Command Line Interface Reference* for detailed information on using this command.



CHAPTER 4

AAA Server-provided 3GPP-User-Location-Information Support

The following topics are discussed:

Feature Description

Overview

This feature enables the SaMOG Gateway to receive the last known LTE location of the subscriber in the 3GPP-User-Location-Info AVP from the Diameter-based AAA server over the STa interface. This information is then used by SaMOG in the Create Session Request (CSR) messages over the S2a interface. The 3GPP-User-Location-Info AVP is received by SaMOG when the **aaa-custom23** dictionary is available.

With the 3GPP-User-Location-Info AVP, SaMOG can then:

- Use the PLMN values (MCC/MNC) in the Serving-Network IE in the CSR messages.
- Populate the User-Location-Information (ULI) IE in the CSR messages.

Important The **aaa-custom23** dictionary is customer specific. For more information, contact your Cisco account representative.

Relationship to Other Features

Lawful Intercept

The PLMN values received in the 3GPP-User-Location-Information AVP will be used for lawful intercept purposes.

Offline Charging

The PLMN values received in the 3GPP-User-Location-Information AVP will be used for offline charging (CDR interface).

How AAA Server-provided 3GPP-User-Location-Information Works

Architecture

The AAA Server shares the last known LTE location of the subscriber through the Geographic Location Type field in the 3GPP-User-Location-Information AVP as specified in *3GPP TS 29.061*:

- **TAI** – When the value of the Geographic Location Type field is 128, the Geographic Location field will contain the PLMN and Tracking Area Code (TAC) values.
- **ECGI** – When the value of the Geographic Location Type field is 129, the Geographic Location field will contain the PLMN and E-UTRAN Cell Identifier (ECI) values.
- **TAI-ECGI** – Value of the Geographic Location Type field is 130.

On receiving the 3GPP-User-Location-Info AVP from the AAA Server, SaMOG can do one or both of the following:

- When the **samog-s2a-gtpv2 send uli** command under the Call Control Profile Configuration mode is enabled,SaMOG populates the ULI IE in the Create Session Request message over the S2a interface.
- When the **samog-s2a-gtpv2 send serving-network value uli** command under the Call Control Profile Configuration Mode is enabled, SaMOG forwards the Serving-Network Information Element (IE) in the Create Session Request message over the S2a interface.

The structure of the ULI IE, and ECGI and TAI values are as specified in *3GPP TS 29.274*.

The 3GPP-User-Location-Info AVP is non-standard over the STa interface, and ULI IE is non-standard over the S2a interface.

Standards Compliance

This feature complies with the following standards:

- **3GPP TS: 29.061** - "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)"
- **3GPP TS: 29.274** - "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3"

Configuring AAA Server-provided 3GPP-User-Location-Information

Configuring SaMOG to Forward the ULI IE

Use the following configuration to configure SaMOG to forward the User-Location-Information (ULI) Information Element (IE) in the CSR message over the S2a interface.

```
config
   call-control-profile profile_name
      samog-s2a-gtpv2 send uli
      end
```

Notes:

- **Default**: Disabled
- If previously configured, use the **no samog-s2a-gtpv2 send uli** command to disable the configuration.

Configuring SaMOG to Forward the Serving-Network IE

Use the following configuration to configure SaMOG to forward the Serving-Network Information Element (IE) in the CSR message over the S2a interface.

```
config
   call-control-profile profile_name
      [ no ] samog-s2a-gtpv2 send serving-network value uli
      end
```

Notes:

- **Default**: Disabled
- If previously configured, use the **no samog-s2a-gtpv2 send serving-network value uli** command to disable the configuration.

Monitoring and Troubleshooting

Show Command(s) and/or Outputs

show call-control-profile full name

The following fields are available to the output of the **show call-control-profile full name** *profile_name* command in support of this feature:

```
Samog-S2a-GTPv2:
Sending ULI IE                          : Enabled
```

```
ULI IE Content                      : 3gpp-user-location-info
Serving-network IE content          : ULI
```

*Table 21: **show call-control-profile full name** Command Output Descriptions*

Field	Description
Samog-S2a-GTPv2:	
Sending ULI IE	Indicates if SaMOG is configured to forward the value received from the 3GPP-User-Location-Info AVP. Values: • Enabled • Disabled
ULI IE Content	Indicates if SaMOG is configured to forward the ULI IE. Values: • 3gpp-user-location-info • None
Serving-network IE content	Indicates if SaMOG is configured to forward the Serving-Network IE. Values: • ULI • None

show subscribers samog-only full

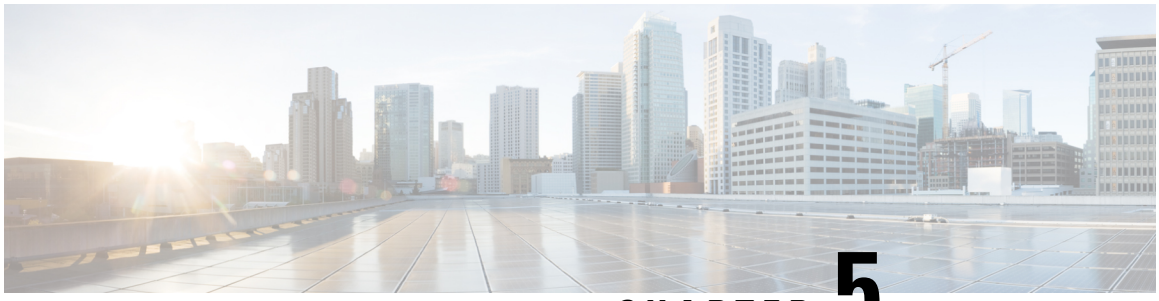
The following fields are available to the output of the **show subscribers samog-only full** command in support of this feature:

```
MRME Subscriber Info:
---------------------
uli: tai-ecgi
mcc: 412   mnc: 01   tac: 0001   eci: 0001
```

*Table 22: **show subscribers samog-only full** Command Output Descriptions*

Field	Description
MRME Subscriber Info:	
uli	The Geographic Location Type received in the 3GPP-User-Location-Info AVP for the subscriber.
mcc	Mobile Country Code (MCC) of the subscriber.
mnc	Mobile Network Code (MNC) of the subscriber.

Field	Description
tac	Tracking Area Code (TAC) of the subscriber.
eci	E-UTRAN Cell Identifier (ECI) of the subscriber.



CHAPTER 5

Civic Address in TWAN-Identifier IE

The following topics are discussed:

Feature Description

Overview

In earlier releases, SaMOG could send either the AP-Group-Name or the SSID value in the TWAN-Identifier IE in the Create Session Request (CSR) message. From Release 21.1 and later, operators can provision the SaMOG Gateway to forward AP-MAC, SSID, and AP-Group-Name triplet information in the TWAN-Identifier IE received from the access network to P-GW, Lawful Intercept (LI) services.

This feature enables the AP-Group-Name information to be encoded in the Civic-Address-Information IE within the TWAN-Identifier IE as defined in *RFC 4776*. The TWAN-Identifier will contain:

- AP-MAC to be encoded in the BSSID attribute
- SSID to be encoded in the SSID attribute
- AP-Group-Name to be encoded in the civic-addr attribute

On receiving the Civic Address Information IE within the TWAN-Identifier IE, P-GW can forward the IE towards PCRF (Gx) and OCS (Gy).

This feature is currently supported on the S2a GTPv2 protocol for RADIUS Authentication-based session triggers.

Important When this feature is enabled, the memory utilization of the AAAMgr will increase slightly.

How Civic Address in TWAN-Identifier IE Works

Architecture

SaMOG can receive the AP-Group-Name in the Called-Station-ID (RADIUS) AVP from the WLAN access network in following formats:

- mac<MAC>:grp<AP-Group-Name>
- grp<AP-Group-Name>:<SSID>
- cgi<CGI>:grp<AP-Group-Name>
- cgi<CGI>:mac<MAC>:grp<AP-Group-Name>
- <MAC>:<SSID>:<AP-Group-Name>

The AP group name is encoded in the Civic Address as per RFC 4776. For this feature, the Civic Address Type (CAType) format used is NAM (name).

Encoding

S2a Interface

The SaMOG Gateway encodes the TWAN-Identifier IE with the Civic-Address-Information field as specified in *RFC 4776*, and *3GPP TS: 29.274*. By default, the two digit country code in the civic location option will be encoded as IN.

LI Interface

Encoding for LI interface will be performed by SaMOG and P-GW as specified in *3GPP TS:29.274*, and *3GPP TS: 33.108*.

For more information, refer *Lawful Intercept with the SaMOG Service* chapter in the *Lawful Intercept Configuration* guide.

Gx Interface

The P-GW receives the Civic address IE in TWAN-Identifier IE from SaMOG over the S2a interface, and encodes the Civic address value in TWAN-Identifier attribute in Gx interface. Encoding for this AVP is as specified in *3GPP TS 29.274*. The standard Gx dictionary, **r8-gx-standard** is used.

Gy Interface

A Civic-Addr vendor specific AVP is used in the non-standard custom dictionary, **dcca-custom33** to encode the civic address value in the Gy interface by P-GW.

Important The **dcca-custom33** dictionary is customer specific. For more information, contact your Cisco account representative.

Gz Interface

P-GW (P-GW records) encodes the AP-Group-Name within the civicAddress attribute in the TWANUserLocationInfo and forwards it over the Gz interface using a non-standard custom dictionary, **custom53**.

Important The **custom53** dictionary is customer specific. For more information, contact your Cisco account representative.

Limitations

- If the maximum length of the AP-Group-Name exceeds 32 bytes, SaMOG will not include the AP group name in the Civic Address Information field of the TWAN-Identifier IE.
- It is recommended to avoid configuring SaMOG to send the AP-Group-Name in both SSID and Civic Address Information fields. If configured, SaMOG will send the AP-Group-Name in the SSID field and the Civic Address Information field.

Standards Compliance

This feature complies with the following standards:

- **RFC 4776**: "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information"
- **3GPP TS: 29.274**: "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C)"

Configuring Civic Address in TWAN-Identifier IE

Enabling Civic Address in TWAN-Identifier on the S2a Interface

Use the following configuration to enable SaMOG to forward the AP-Group-Name value in the Civic Address Information field of the TWAN-Identifier IE over the S2a interface.

```
config
   call-control-profile profile_name
      samog-s2a-gtpv2 send twan-identifier civic-addr-fld ca-type name
value ap-group-name
      end
```

Notes:

- If previously configured, use the **no samog-s2a-gtpv2 send twan-identifier civic-addr-fld** command to remove and restore the configuration to its default value.
- **Default**: Disabled

Monitoring and Troubleshooting

Civic Address in TWAN-Identifier IE Show Command(s) and/or Outputs

show call-control-profile full name

The following fields are available to the output of the **show call-control-profile full name** *profile_name* command in support of this feature:

```
Samog-S2a-GTPv2:
  TWAN-IDENTIFIER IE:
     SSID Value Type               : SSID
     Civic Address Information:
       CAtype-23 (NAME):  AP GROUP NAME
TWAN User Location Information:
   SSID Value Type                 : SSID
   Civic Address Information:
      CAtype-23 (NAME):  AP GROUP NAME
```

Table 23: show call-control-profile full name Command Output Descriptions

Field	Description
Samog-S2a-GTPv2:	
TWAN-IDENTIFIER IE:	
SSID Value Type	Indicates if the SSID field in the TWAN Identifier IE will contain SSID or AP group name value.
Civic Address Information:	
CAtype-23 (NAME)	The AP group name value for this Call Control Profile. Options: • AP group name • Disabled
TWAN User Location Information:	
SSID Value Type	Indicates if the SSID field in the TWAN Identifier IE will contain SSID or AP group name value.
Civic Address Information:	
CAtype-23 (NAME)	The AP group name value for this Call Control Profile. Options: • AP group name • Disabled

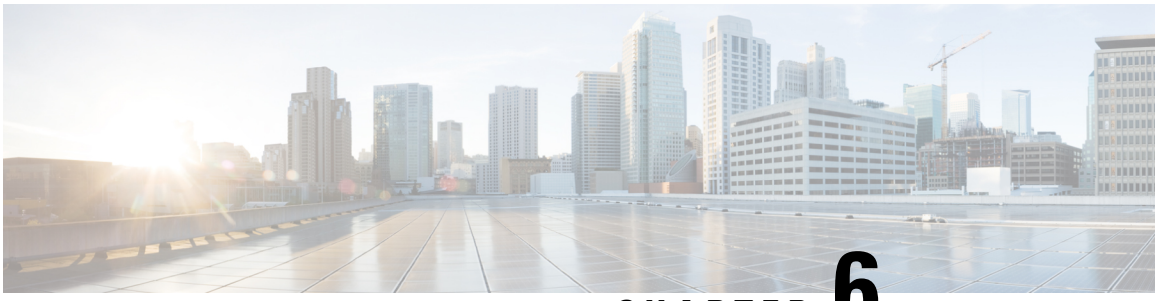
show subscribers

The following fields are available to the output of the **show subscribers { pgw-only | saegw-only } full all** command in support of this feature:

```
TWAN User Location Information:
   SSID  :   anmip
   BSSID :   64:D9:89:43:D4:A0
   CIVIC Address :   IN234grna
```

*Table 24: **show subscribers** Command Output Descriptions*

Field	Description
TWAN User Location Information	
SSID	SSID value for the subscriber in the TWAN ULI.
BSSID	BSSID value for the subscriber in the TWAN ULI.
Civic Address	The AP-Group-name value for the subscriber in the TWAN ULI.



CHAPTER 6

Dedicated Bearer Support

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SaMOG
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled – Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *ASR 5500 System Administration Guide* • *Command Line Interface Reference* • *SaMOG Administration Guide*

Revision History

Note Revision history details are not provided for features introduced before releases 21.2 and N5.5.

Revision Details	Release
First Introduced.	21.3

Feature Description

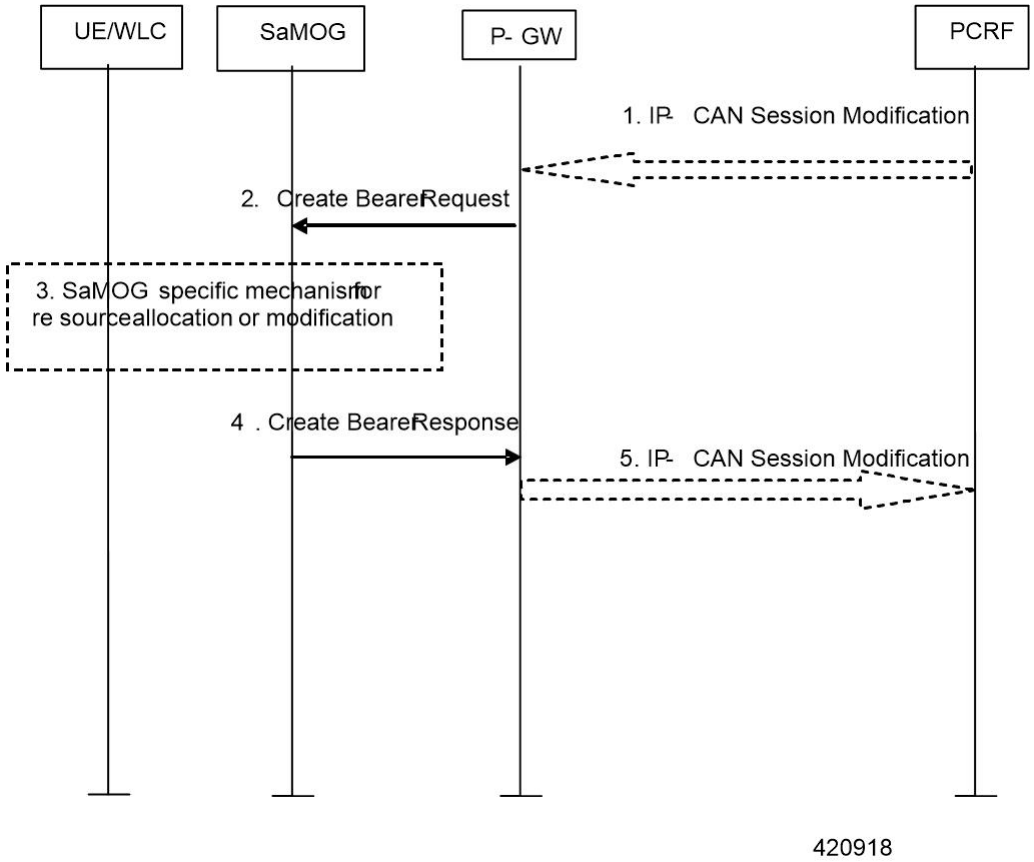
SaMOG supports dedicated bearer over S2A interface over GTPv2 protocol.

This release provides basic support for network initiated dedicated bearer. The additional procedures and features mentioned in release 13 3GPP TS 23.402/29.274 are not provided. SaMOG will support dedicated bearer creation in Transparent Single Mode.

Flows

This section provides various call flows that illustrate PGW and HSS initiated Bearer Modification.

PGW Initiated Bearer Modification (Dedicated Bearer Activation)

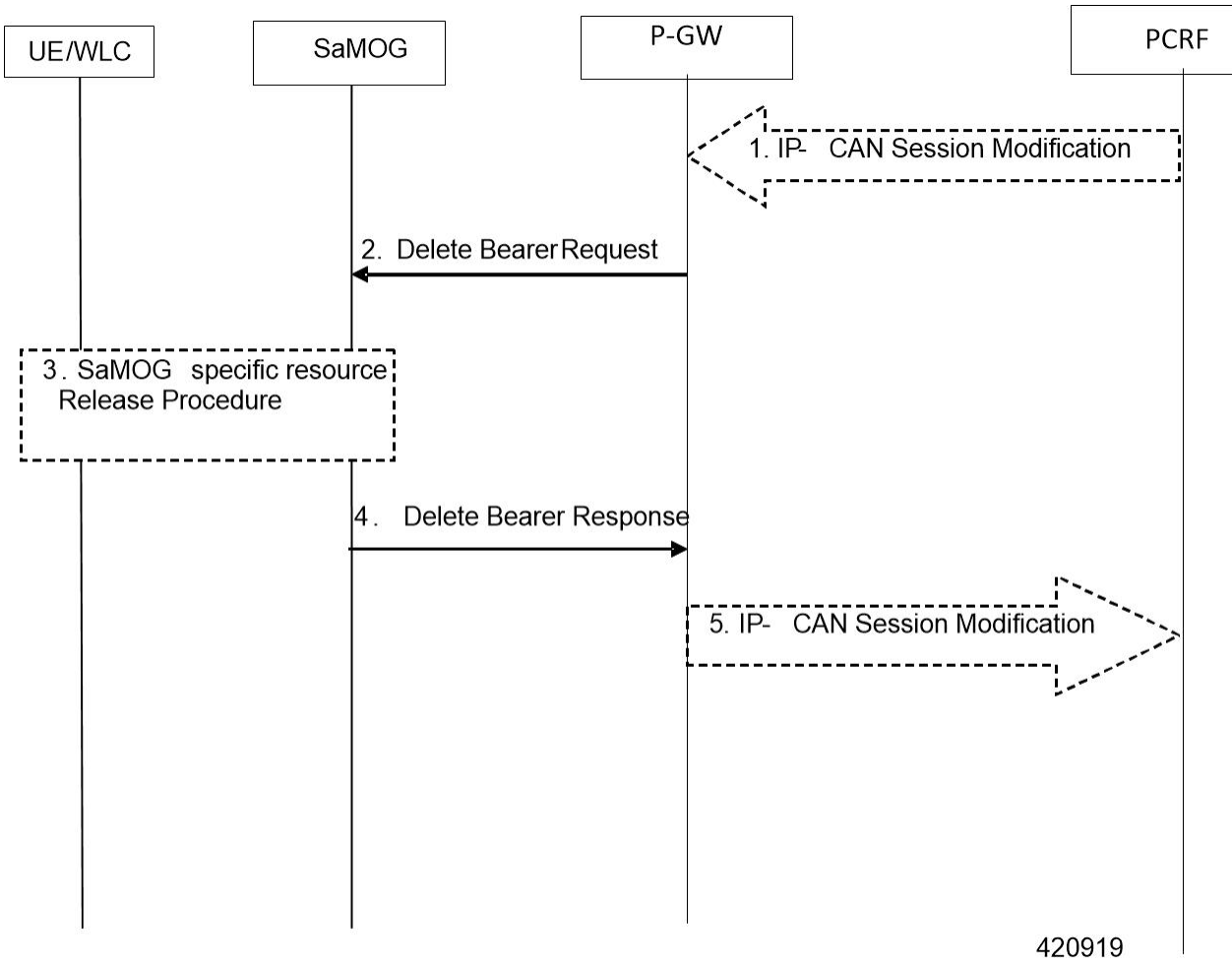


1. If dynamic PCC is deployed, the PCRF sends a PCC decision provision (QoS policy) message to the P-GW. If the Application function, (e.g. P-CSCF) requests it. If dynamic PCC is not deployed, the PDN GW may apply local QoS policy.
2. The P-GW uses this QoS policy to assign the S2a bearer QoS, i.e., it assigns the values to the bearer level QoS parameters QCI, ARP, GBR and MBR. If this dedicated bearer is created as part of the handover from 3GPP access with GTP-based S5/S8, then the PDN GW applies the Charging ID already in use for the corresponding dedicated bearer while the UE was in 3GPP access (i.e. bearer with the same QCI and

ARP as in 3GPP access). Otherwise, the PDN GW generates a new Charging ID for the dedicated bearer. The PDN GW sends a Create Bearer Request message (IMSI, EPS bearer QoS, TFT, PDN GW Address for the user plane, PDN GW TEID of the user plane, Charging Id, LBI) to the trusted WLAN access network - SaMOG. The Linked EPS bearer Identity (LBI) is the EPS bearer Identity of the default bearer.

3. SaMOG specific resource allocation/modification procedure are executed in this step.
4. The SaMOG selects an EPS bearer Identity, un assigned to the UE. Then stores the EPS bearer Identity and links the dedicated bearer to the default bearer indicated by the Linked Bearer Identity (LBI). SaMOG uses the uplink packet filter (UL TFT) to determine the mapping of uplink traffic flows to the S2a bearer. SaMOG then acknowledges the S2a bearer activation to the PGW by sending a Create Bearer Response (EPS bearer Identity, SaMOG Address for the user plane, SaMOG TEID of the user plane) message.
5. If the dedicated bearer activation procedure was triggered by a PCC Decision Provision message from the PCRF, the PDN GW indicates to the PCRF whether the requested PCC decision (QoS policy) could be enforced or not, allowing the completion of the PCRF-Initiated IP CAN Session Modification procedure.

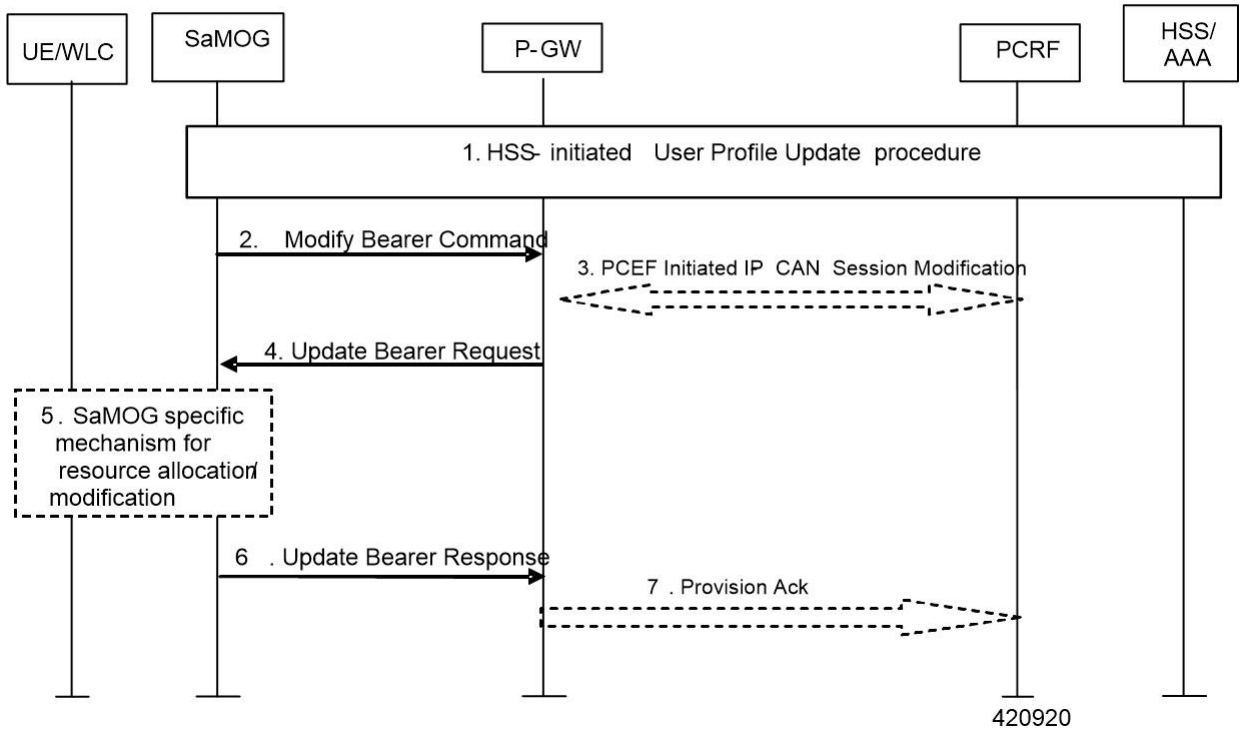
PGW Initiated Resource Allocation Deactivation



1. If dynamic PCC is deployed, the P-GW initiated Bearer Deactivation procedure may for example be triggered due to 'IP CAN session Modification procedure'. In this case, the resources associated with the PDN connection in the P-GW are released. If requested by the Application Function (e.g. P-CSCF).
2. The P-GW sends a Delete Bearer Request message (EPS Bearer Identity, Cause) to the SaMOG. This message can include an indication that all bearers belonging to that PDN connection shall be released.
3. SaMOG specific resources will be released for the bearer.
4. SaMOG deletes the bearer contexts related to the Delete Bearer Request, and acknowledges the bearer deactivation to the P-GW by sending a Delete Bearer Response (EPS Bearer Identity) message.
5. The P-GW deletes the bearer context related to the deactivated S2a bearer. If the dedicated bearer deactivation procedure was triggered by receiving a PCC decision message from the PCRF, the P-GW indicates to the PCRF whether the requested PCC decision was successfully enforced by completing the PCRF-initiated IP CAN Session Modification procedure or the PCEF initiated IP-CAN Session Modification procedure.

Important This procedure can be used to deactivate an S2a dedicated bearer or deactivate all S2a bearers belonging to a PDN address, for e.g., due to IP CAN session modification requests from the PCRF. If the default S2a bearer belonging to a PDN connection is deactivated, the P-GW deactivates all S2a bearers belonging to the PDN connection.

HSS Initiated Bearer Modification



1. The HSS updates the User Profile. (RAR from Diameter to SaMOG)
2. If the QCI and/or ARP and/or subscribed APN-AMBR has been modified and there is a related active PDN connection with the modified QoS Profile, then SaMOG sends the Modify Bearer Command (EPS bearer Identity, EPS bearer QoS, APN AMBR) message to the P-GW. The EPS bearer Identity identifies the default bearer of the affected PDN connection. The EPS bearer QoS contains the EPS subscribed QoS profile to be updated.
3. If PCC infrastructure is deployed, the P-GW informs the PCRF about the updated EPS bearer QoS. The PCRF sends the new updated PCC decision to the P-GW.
4. The PCRF may modify the APN-AMBR and the QoS parameters (QCI and ARP) associated with the default bearer in the response to the P-GW.
5. The P-GW modifies the default bearer of each PDN connection corresponding to the APN for which subscribed QoS has been modified. If the subscribed ARP parameter has been changed, the P-GW shall also modify all dedicated S2a bearers having the previously subscribed ARP value unless superseded by PCRF decision. The P-GW then sends the Update Bearer Request (EPS bearer Identity, EPS bearer QoS, TFT, APN AMBR) message to the SaMOG.
6. SaMOG will perform resource allocation/modification procedures.
7. SaMOG acknowledges the bearer modification to the P-GW by sending an Update Bearer Response (EPS bearer Identity) message. If the bearer modification fails the P-GW deletes the concerned S2a Bearer. P-GW indicates to the PCRF whether the requested PCC decision was enforced or not by sending a Provision Ack message

Limitations

Following are the know limitations of this feature:

- Support is available only for network-initiated dedicated bearer creation.
- LI and CDR support is not provided for dedicated bearer in SaMOG.
- Dedicated bearer support for LBO flow call model is not available.
- 3GPP-24.008 length field in TFT IE is only one Octet, as a result of this maximum length can be only 256, but in update bearer (message) more packet filters can be added to increase the size of TFT up to 960 (16 * 60 = 960). In this release, SaMOG only supports 504 size TFT per bearer.

Monitoring and Troubleshooting

Dedicated Bearer Support Show Command(s) and /or Outputs

show samog service statistic

Below show command output is introduced to support SaMOG Dedicated Bearer Feature:

The following new fields are added to the output of this command to display service statistics:

QCI Stats Total:

- Attempt
- Active
- Setup
- Released
- Rejected

QCI 1:

Bearers

- Attempt
- Active
- Setup
- Released
- Rejected

QCI 2:

Bearers

- Attempt
- Active
- Setup
- Released
- Rejected

QCI 3:

Bearers

- Attempt
- Active
- Setup
- Released
- Rejected

QCI 4:

Bearers

- Attempt
- Active
- Setup

- Released
- Rejected

QCI 5:

Bearers

- Attempt
- Active
- Setup
- Released
- Rejected

QCI 6:

Bearers

- Attempt
- Active
- Setup
- Released
- Rejected

QCI 7:

Bearers

- Attempt
- Active
- Setup
- Released
- Rejected

QCI 8:

Bearers

- Attempt
- Active
- Setup
- Released
- Rejected

QCI 9:

Bearers

- Attempt
- Active
- Setup
- Released
- Rejected

Non-Std QCI:

Bearers

- Attempt
- Active
- Setup
- Released
- Rejected

show samog subscribers samog only full

The following new fields are added to the output of this command to display the SaMOG Subscribers only full statistics:

CGW Subscriber Info:

- pgw c-addr
- pgw u-addr
- cgw s2a c-addr
- cgw s2a u-addr
- cgw s2a u-addr
- pgw c-teid
- samog s2a c-teid
- UE def-gw-addr
- UE Vlan ID
- UE VMAC Address
- APN AMBR Uplink(bps)
- APN AMBR Downlink(bps)
- Accounting mode

Bearer ID:

- pgw u-teid

- samog s2a u-teid
- Charging id
- Charging chars
- Total UL Bytes Sent
- Total UL Packets Sent
- Total DL Bytes Rcvd
- Total DL Packets Rcvd

QoS:

- QCI
- APR
- PCI
- PL
- PVI
- MBR Uplink (bps)
- MBR Downlink (bps)
- GBR Uplink(bps)
- GBR Downlink(bps)

Bearer ID:

- pgw u-teid
- samog s2a u-teid
- Charging id
- Charging chars
- Total UL Bytes Sent
- Total UL Packets Sent
- Total UL Bytes Rcvd
- Total DL Packets Rcvd

QoS:

- QCI
- APR
- PCI
- PL

- PVI
- MBR Uplink(bps)
- MBR Downlink(bps)
- GBR Uplink(bps)
- GBR Downlink(bps)

Bulk Statistics

The following bulk statistics are added in the SaMOG schema for Dedicated Bearer Support:

Counter	Descreption	Trigger
cgw-sessstat-dedicated-bearer-active	Total number of current active dedicated bearers.	Increments whenever the dedicated bearer is created on SaMOG and decrements whenever the dedicated bearer is released by SaMOG.
cgw-sessstat-dedicated-bearer-setup	Total number of dedicated bearers created on SaMOG.	Increments whenever the dedicated bearer is created on SaMOG.
cgw-sessstat-dedicated-bearer-released	Total number of dedicated bearers released by SaMOG.	Increments whenever the dedicated bearer is released by SaMOG.
cgw-sessstat-dedicated-bearer-rejected	Total number of dedicated bearers rejected by SaMOG.	Increments whenever the dedicated bearer is rejected by SaMOG.
cgw-sessstat-qci1-dedicated-bearer-attempted	Total number of QCI1 dedicated bearers attempted on SaMOG.	Increments whenever there is an attempt to make a QCI1 dedicated bearer on SaMOG.
cgw-sessstat-qci1-dedicated-bearer-active	Total number of current active QCI1 dedicated bearers on SaMOG.	Increments whenever the QCI1 dedicated bearer is created on SaMOG and decrements whenever the QCI1 dedicated bearer is released by SaMOG.
cgw-sessstat-qci1-dedicated-bearer-setup	Total number of QCI1 dedicated bearers created on SaMOG.	Increments whenever the QCI1 dedicated bearer is created on SaMOG.
cgw-sessstat-qci1-dedicated-bearer-released	Total number of QCI1 dedicated bearers released by SaMOG.	Increments whenever the QCI1 dedicated bearer is released by SaMOG.

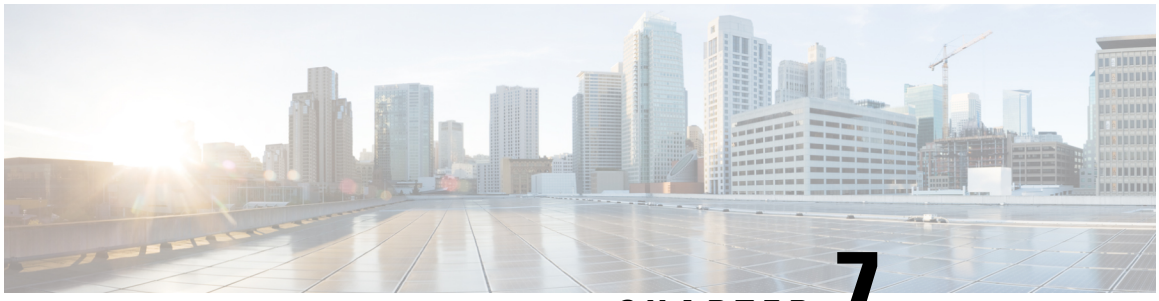
Counter	Descreption	Trigger
cgw-sessstat-qci1-dedicated-bearer-rejected	Total number of QCI1 dedicated bearers rejected by SaMOG.	Increments whenever the QCI1 dedicated bearer is rejected by SaMOG.
cgw-sessstat-qci2-dedicated-bearer-attempted	Total number of QCI2 dedicated bearers attempted on SaMOG.	Increments whenever there is an attempt to make a QCI2 dedicated bearer on SaMOG
cgw-sessstat-qci2-dedicated-bearer-active	Total number of current active QCI2 dedicated bearers on SaMOG.	SaMOG and decrements whenever the QCI2 dedicated bearer is released by SaMOG.
cgw-sessstat-qci2-dedicated-bearer-setup	Total number of QCI2 dedicated bearers created on SaMOG	Increments whenever the QCI2 dedicated bearer is created on SaMOG.
cgw-sessstat-qci2-dedicated-bearer-released	Total number of QCI2 dedicated bearers released by SaMOG.	Increments whenever the QCI2 dedicated bearer is released by SaMOG.
cgw-sessstat-qci2-dedicated-bearer-rejected	Total number of QCI2 dedicated bearers rejected by SaMOG.	Increments whenever the QCI2 dedicated bearer is rejected by SaMOG.
cgw-sessstat-qci3-dedicated-bearer-attempted	Total number of QCI3 dedicated bearers attempted on SaMOG.	Increments whenever there is an attempt to make a QCI3 dedicated bearer on SaMOG.
cgw-sessstat-qci3-dedicated-bearer-active	Total number of current active QCI3 dedicated bearers on SaMOG.	Increments whenever the QCI3 dedicated bearer is created on SaMOG and decrements whenever the QCI3 dedicated bearer is released by SaMOG.
cgw-sessstat-qci3-dedicated-bearer-setup	Total number of QCI3 dedicated bearers created on SaMOG.	Increments whenever the QCI3 dedicated bearer is created on SaMOG.
cgw-sessstat-qci3-dedicated-bearer-released	Total number of QCI3 dedicated bearers released by SaMOG.	Increments whenever the QCI3 dedicated bearer is released by SaMOG.
cgw-sessstat-qci3-dedicated-bearer-rejected	Total number of QCI3 dedicated bearers rejected by SaMOG.	Increments whenever the QCI3 dedicated bearer is rejected by SaMOG.
cgw-sessstat-qci4-dedicated-bearer-attempted	Total number of QCI4 dedicated bearers attempted on SaMOG.	Increments whenever there is an attempt to make a QCI4 dedicated bearer on SaMOG.

Counter	Description	Trigger
cgw-sessstat-qci4-dedicated-bearer-active	Total number of current active QCI4 dedicated bearers on SaMOG.	Increments whenever the QCI4 dedicated bearer is created on SaMOG and decrements whenever the QCI4 dedicated bearer is released by SaMOG.
cgw-sessstat-qci4-dedicated-bearer-setup	Total number of QCI4 dedicated bearers created on SaMOG.	Increments whenever the QCI4 dedicated bearer is created on SaMOG.
cgw-sessstat-qci4-dedicated-bearer-released	Total number of QCI4 dedicated bearers released by SaMOG.	Increments whenever the QCI4 dedicated bearer is released by SaMOG.
cgw-sessstat-qci4-dedicated-bearer-rejected	Total number of QCI4 dedicated bearers rejected by SaMOG.	Increments whenever the QCI4 dedicated bearer is rejected by SaMOG.
cgw-sessstat-qci5-dedicated-bearer-attempted	Total number of QCI5 dedicated bearers attempted on SaMOG.	Increments whenever there is an attempt to make a QCI5 dedicated bearer on SaMOG.
cgw-sessstat-qci5-dedicated-bearer-active	Total number of current active QCI5 dedicated bearers on SaMOG.	Increments whenever the QCI5 dedicated bearer is created on SaMOG and decrements whenever the QCI5 dedicated bearer is released by SaMOG.
cgw-sessstat-qci5-dedicated-bearer-setup	Total number of QCI5 dedicated bearers created on SaMOG.	Increments whenever the QCI5 dedicated bearer is created on SaMOG.
cgw-sessstat-qci5-dedicated-bearer-released	Total number of QCI5 dedicated bearers released by SaMOG.	Increments whenever the QCI5 dedicated bearer is released by SaMOG.
cgw-sessstat-qci5-dedicated-bearer-rejected	Total number of QCI5 dedicated bearers rejected by SaMOG.	Increments whenever the QCI5 dedicated bearer is rejected by SaMOG.
cgw-sessstat-qci6-dedicated-bearer-attempted	Total number of QCI6 dedicated bearers attempted on SaMOG.	Increments whenever there is an attempt to make a QCI6 dedicated bearer on SaMOG.

Counter	Descreption	Trigger
cgw-sessstat-qci6-dedicated-bearer-active	Total number of current active QCI6 dedicated bearers on SaMOG.	Increments whenever the QCI6 dedicated bearer is created on SaMOG and decrements whenever the QCI6 dedicated bearer is released by SaMOG.
cgw-sessstat-qci6-dedicated-bearer-setup	Total number of QCI6 dedicated bearers created on SaMOG.	Increments whenever the QCI6 dedicated bearer is created on SaMOG.
cgw-sessstat-qci6-dedicated-bearer-released	Total number of QCI6 dedicated bearers released by SaMOG.	Increments whenever the QCI6 dedicated bearer is released by SaMOG.
cgw-sessstat-qci6-dedicated-bearer-rejected	Total number of QCI6 dedicated bearers rejected by SaMOG.	Increments whenever the QCI6 dedicated bearer is rejected by SaMOG.
cgw-sessstat-qci7-dedicated-bearer-attempted	Total number of QCI7 dedicated bearers attempted on SaMOG.	Increments whenever there is an attempt to make a QCI7 dedicated bearer on SaMOG.
cgw-sessstat-qci7-dedicated-bearer-active	Total number of current active QCI7 dedicated bearers on SaMOG.	Increments whenever the QCI7 dedicated bearer is created on SaMOG and decrements whenever the QCI7 dedicated bearer is released by SaMOG.
cgw-sessstat-qci7-dedicated-bearer-setup	Total number of QCI7 dedicated bearers created on SaMOG.	Increments whenever the QCI7 dedicated bearer is created on SaMOG.
cgw-sessstat-qci7-dedicated-bearer-released	Total number of QCI7 dedicated bearers released by SaMOG.	Increments whenever the QCI7 dedicated bearer is released by SaMOG.
cgw-sessstat-qci7-dedicated-bearer-rejected	Total number of QCI7 dedicated bearers rejected by SaMOG.	Increments whenever the QCI7 dedicated bearer is rejected by SaMOG.
cgw-sessstat-qci8-dedicated-bearer-attempted	Total number of QCI8 dedicated bearers attempted on SaMOG.	Increments whenever there is an attempt to make a QCI8 dedicated bearer on SaMOG.

Counter	Descreption	Trigger
cgw-sessstat-qci8-dedicated-bearer-active	Total number of current active QCI8 dedicated bearers on SaMOG.	Increments whenever the QCI8 dedicated bearer is created on SaMOG and decrements whenever the QCI8 dedicated bearer is released by SaMOG.
cgw-sessstat-qci8-dedicated-bearer-setup	Total number of QCI8 dedicated bearers created on SaMOG.	Increments whenever the QCI8 dedicated bearer is created on SaMOG.
cgw-sessstat-qci8-dedicated-bearer-released	Total number of QCI8 dedicated bearers released by SaMOG.	Increments whenever the QCI8 dedicated bearer is released by SaMOG.
cgw-sessstat-qci8-dedicated-bearer-rejected	Total number of QCI8 dedicated bearers rejected by SaMOG.	Increments whenever the QCI8 dedicated bearer is rejected by SaMOG.
cgw-sessstat-qci9-dedicated-bearer-attempted	Total number of QCI9 dedicated bearers attempted on SaMOG.	Increments whenever there is an attempt to make a QCI9 dedicated bearer on SaMOG.
cgw-sessstat-qci9-dedicated-bearer-active	Total number of current active QCI9 dedicated bearers on SaMOG.	Increments whenever the QCI9 dedicated bearer is created on SaMOG and decrements whenever the QCI9 dedicated bearer is released by SaMOG.
cgw-sessstat-qci9-dedicated-bearer-setup	Total number of QCI9 dedicated bearers created on SaMOG.	Increments whenever the QCI9 dedicated bearer is created on SaMOG.
cgw-sessstat-qci9-dedicated-bearer-released	Total number of QCI9 dedicated bearers released by SaMOG.	Increments whenever the QCI9 dedicated bearer is released by SaMOG.
cgw-sessstat-qci9-dedicated-bearer-rejected	Total number of QCI9 dedicated bearers rejected by SaMOG.	Increments whenever the QCI9 dedicated bearer is rejected by SaMOG.
cgw-sessstat-non-std-qci-dedicated-bearer-attempted	Total number of non-standard QCI dedicated bearers attempted on SaMOG.	Increments whenever there is an attempt to make a non-standard QCI dedicated bearer on SaMOG.

Counter	Descreption	Trigger
cgw-sessstat-non-std-qci-dedicated-bearer-active	Total number of current active non-standard QCI dedicated bearers on SaMOG.	Increments whenever the non-standard QCI dedicated bearer is created on SaMOG and decrements whenever the non-standard QCI dedicated bearer is released by SaMOG.
cgw-sessstat-non-std-qci-dedicated-bearer-setup	Total number of non-standard QCI dedicated bearers created on SaMOG.	Increments whenever the non-standard QCI dedicated bearer is created on SaMOG.



CHAPTER 7

DHCP, RADIUS Accounting, and PMIPv6 based Session Triggers on GTPv2 over S2a Interface

The following topics are discussed:

Feature Description

This feature enables support for GTPv2 protocol on the S2a interface for DHCP, RADIUS Accounting, and PMIPv6-based session triggers for non-UICC devices.

For session triggers using the GTPv2 protocol over the S2a interface, the IMSI field in the Create-Session-Request (CSR) message will contain the decimal equivalent of the MAC address of the UE. The UE's MN-NAI value (from the AAA Server) in the PAP container within the PCO IE in the CSR message is sent to the local P-GW, and to the PCRF server over the Gx interface. SaMOG can be configured to send the MN-NAI value in the PAP-PCO IE using the **samog-s2a-gtpv2 send pco pap value mn-nai** command under the Call Control Profile Configuration Mode. The local P-GW can be configured to send the MN-NAI value in the Subscription-ID AVP with MSISDN in CCR-I or CCR-U towards PCRF on the Gx interface using the **subscription-id service-type samog-epdg nai** command under the Policy Control Configuration Mode.

Standards Compliance

This feature complies with the following standards:

- **3GPP TS 23.402** - "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for non-3GPP accesses"
- **3GPP TS 29.274** - "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3"

Configuring Session Triggers on GTPv2 Over S2a Interface

Enabling MN-NAI in PCO-PAP

Use the following configuration to enable SaMOG to forward the UE's MN-NAI value in the PAP container within the PCO IE in the CSR message to P-GW:

```
configure
   call-control-profile profile_name
      samog-s2a-gtpv2 send pco pap value mn-nai
      end
```

Notes:

- If previously configured, use the **no samog-s2a-gtpv2 send pco pap value mn-nai** command to remove and restore the configuration to its default value.
- **Default**: Disabled

Monitoring and Troubleshooting

Show Command(s) and/or Outputs

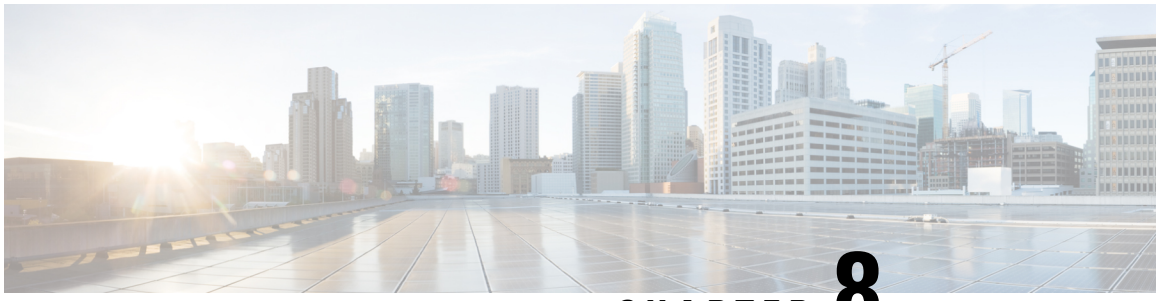
show call-control-profile full

The following fields are available to the output of the **show call-control-profile full name** *profile_name* command in support of this feature:

```
Samog-S2a-GTPv2:
    Sending PCO IE with PAP container       : Enabled with MN-NAI value
```

Table 25: show call-control-profile full Command Output Descriptions

Field	Description
SaMOG-S2a-GTPv2	
Sending PCO IE with PAP container	Indicates whether the configuration to forward the MN-NAI value in the PAP container within the PCO IE is enabled or disabled. Options: • Enabled with MN-NAI value • Disabled



CHAPTER 8

DHCP Trigger-based Session Creation

This feature enables the SaMOG Gateway to create sessions on receiving DHCP Discover or DHCP Request messages for a subscriber over the EoGRE tunnel.

The following sections provide more detailed information:

Feature Description

Overview

In traditional internet deployment architectures, the service provider provide WiFi access to subscribers based on web-based authentication. These deployment architecture might use access points (AP) which are incapable of RADIUS-based authentication triggers. These access points are only capable of relaying DHCP messages between the subscriber's user equipment (UE) and the DHCP server, to obtain the IP address for the UE, after which the AP forwards data packets between the UE and the default gateway.

With this feature, the SaMOG Gateway can initiate session creation when a DHCP message is received from the AP over the EoGRE tunnel. This feature integrates SaMOG as a gateway in deployment architectures where the AP/WLC cannot initiate RADIUS (Access-Request) messages.

DHCP Relay Agent Information Option

The SaMOG Gateway supports DHCP Relay Agent Information Option (option 82) to determine the AP's location information. This enables the SaMOG Gateway to select policies for the subscriber based on the location information, and share the serving AP's location information with the AAA server during authentication.

License Requirements

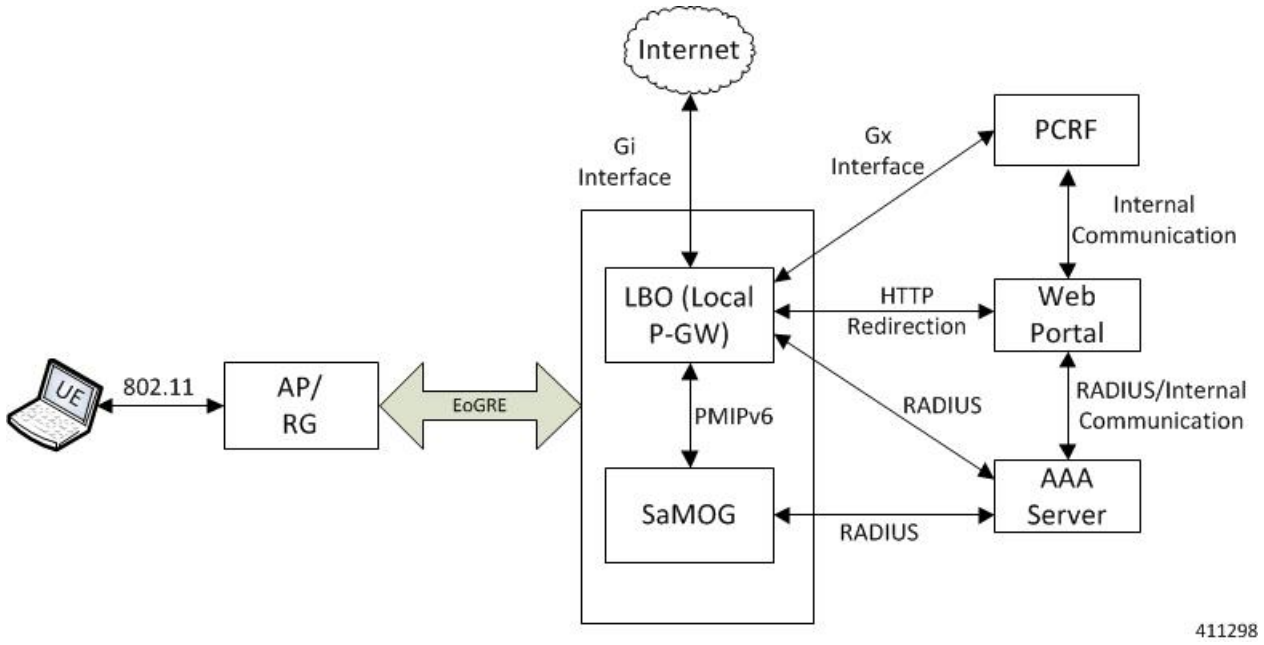
The DHCP trigger-based session creation feature does not require a separate license. However, a Local Breakout - Enhanced license is required to configure a local P-GW.

Contact your Cisco account representative for detailed information on specific licensing requirements.

How DHCP Trigger-based Session Creation Works

The following figure provides the deployment architecture for DHCP trigger-based session creation:

Figure 17: DHCP Trigger-based Session Creation Architecture



The following is the sequence of events for a DHCP trigger-based session creation deployment model:

1. The UE communicates with the AP/RG over the 802.11 link for WiFi association and data transmission. The AP receives the control (DHCP, ARP, etc.) and data packets from the UE and forwards them over the EoGRE tunnel to the SaMOG Gateway.
2. On receiving the DHCP Request or DHCP Discover message sent by the UE from the AP over the EoGRE tunnel, the SaMOG Gateway acts as the RADIUS client and sends a RADIUS Access-Request to the AAA server to obtain the subscriber information based on the UE MAC address (received in L2 DHCP packet).
3. On obtaining the subscriber information (APN name, NAI (in MAC@realm format), etc.) from the AAA server, the SaMOG Gateway uses the Local Breakout (LBO) - Enhanced feature and initiates a PMIPv6 based S2a session with the local P-GW.
4. The local P-GW obtains the HTTP redirection rules from the PCRF over the Gx interface. For more information on the Local Breakout feature, refer *Local Breakout-Enhanced* section of this guide.
5. The local P-GW assigns an IPv4 address and forwards it to the SaMOG Gateway. The SaMOG Gateway in turn forwards the IPv4 address in the DHCP Offer/Reply message to the AP over the EoGRE tunnel. The AP forwards this message to the UE.
6. Any UE initiated traffic is then forwarded to a web authentication portal through the AP, SaMOG Gateway, and the local P-GW (LBO).
7. The UE is presented with a web portal for subscriber authentication. The web portal authenticates the subscriber credentials with the AAA server, and informs the PCRF.

8. The PCRF responds to the web portal with an RAR message on the Gx interface to remove the HTTP redirection rules.
9. All UE traffic is henceforth directed to the Internet.

DHCP Relay Agent Information Option (option 82)

The SaMOG Gateway receives the location information in the AP-MAC or AP-MAC:SSID format in either the Circuit-ID (1) or Remote-ID (2) sub-option in the DHCP Relay Agent Information Option (option 82). Currently, the maximum supported length for DHCP option 82 is 64 bytes, and the maximum SSID value supported is 32 bytes. Formats other than AP-MAC or AP-MAC:SSID is considered as an opaque value. The SaMOG Gateway validates the Circuit-ID or Remote-ID sub-options based on the CLI configured under the TWAN Profile Configuration mode. For more configuration information, refer Configuring DHCP Trigger-based Session Creation, on page 135.

When the sub-option contains the location information in AP-MAC:SSID format, the SaMOG Gateway uses the SSID for policy selection, and selects the AAA server based on the policy.

During subscriber authentication with the AAA server, the SaMOG Gateway includes the processed Circut-ID or Remote-ID values (AP-MAC, AP-MAC:SSID, or opaque value) in Called-station-ID attribute in the Access-Request message towards the AAA server. While responding to the DHCP Discover/Request messages containing the DHCP Relay Agent Information Option (option 82), the SaMOG Gateway copies the DHCP option 82 value as it is in the DHCP-Offer/Ack messages.

Currently, the SaMOG Gateway supports AP-MAC and AP-MAC/SSID options in the following formats:

AP-MAC (separated by hyphen (-), colon (:), or period (.):

- XX-XX-XX-XX-XX-XX
- XX:XX:XX:XX:XX:XX
- XXXX.XXXX.XXXX

Other AP-MAC formats are not parsed.

AP-MAC and SSID (separated by colon (:) or semi-colon (;)):

- XX-XX-XX-XX-XX-XX:SSID
- XX-XX-XX-XX-XX-XX;SSID
- XX:XX:XX:XX:XX:XX:SSID
- XX:XX:XX:XX:XX:XX;SSID
- XXXX.XXXX.XXXX:SSID
- XXXX.XXXX.XXXX;SSID

Access Point without DHCP Relay Agent Information Option (option 82) Support

Where an access point does not support DHCP Relay Agent Information Option (option 82), the SaMOG Gateway maps the VLAN-ID with the NAS-Identifier AVP, and the EoGRE end point IP address with the NAS-Port-ID AVP. The NAS-Identifier and NAS-Port-ID AVPs are then shared with the RADIUS-based AAA server in the Access-Request message. The AAA server uses the information in these AVPs to identify

the AP location and select the appropriate portal for the subscriber. When the DHCP discover/request message does not contain VLAN tagging, the AAA server uses the NAS-Port-ID AVP to identify the AP location.

The SaMOG Gateway can be configured to send the mapped RADIUS attributes to the AAA server using the **radius attribute authentication nas-identifier** and **radius attribute authentication nas-port-id** commands under the Global Context Configuration or AAA Server Group Configuration Modes. For more information, refer Configuring DHCP-based Session Location (AP Without DHCP Relay Agent Information Option (option 82) Support), on page 135.

Limitations

Architectural Limitations

- Network initiated session disconnection cannot be communicated to the UE or AP as RADIUS support is not available on the AP.
- DHCP Trigger-based session creation can be achieved using a local P-GW (LBO - Enhanced) only. Using an external P-GW is not supported in this release.
- The SaMOG Gateway and P-GW communicate over the PMIPv6 protocol only. Other network protocols are currently not supported.
- The location attributes can be sent in either the Circuit-ID or the Remote-ID sub-option of option 82. Location attributes cannot be sent in both the sub-options.
- To support Cisco specific AVPs (mn-apn, mn-nai, etc), the recommended dictionary towards the RADIUS AAA server is Custom71.

Configuration Limitations

- The bind address for the MRME and CGW must be the same in order for the IPSGMGR to receive the MRME bind address and obtain the DHCP discover messages over the EoGRE tunnel with the tunnel end points as WLC and CGW/MRME bind address.
- The EoGRE access type configuration is mandatory for this feature. PMIPv6 or L3IP access type configuration will result in configuration error in the TWAN profile.
- Only one TWAN profile must have a DHCP session trigger enabled. If multiple TWAN profile configurations have DHCP session trigger enabled, the first configured TWAN profile with the DHCP session trigger is used.

Standards Compliance

This feature complies with the following standards:

- RFC 2131 (Handling of DHCP messages)
- RFC 3046 (DHCP Relay Agent Information Option)

The interface between the AP/WLC and the SaMOG Gateway is currently not standardized, and does not require any compliance.

Configuring DHCP Trigger-based Session Creation

Configuring TWAN Profile for DHCP Triggered Session Creation

Use the following configuration to enable DHCP trigger-based session creation:

```
configure
   twan-profile twan_profile_name
      access-type eogre
      session-trigger { dhcp location { circuit-id | remote-id } | radius
 }
      end
```

Notes:

- Use the **session-trigger** command under the TWAN Profile Configuration Mode to enable DHCP trigger-based session creation.
- Use the sub-option **circuit-id** or **remote-id** for the SaMOG Gateway to choose the UE location from the DHCP-Relay-Agent-Info option (DHCP option 82).
- Use the **default session-trigger** command to reset the configuration to its default value.
- If previously configured, use the **no session-trigger dhcp location** command to remove the configuration.
- Default: RADIUS-based session creation
- If the TWAN profile is configured with a DHCP session trigger, the access type must be EoGRE.
- At least one TWAN profile should have the DHCP session trigger enabled. If multiple TWAN profile configurations have DHCP session trigger enabled, the SaMOG Gateway will use the first configured TWAN profile with DHCP session trigger.

Configuring DHCP-based Session Location (AP Without DHCP Relay Agent Information Option (option 82) Support)

Use the following configuration to enable the SaMOG Gateway to send the mapped RADIUS attributes to the AAA server.

For Default AAA Server Group:

```
configure
   context context_name
      radius attribute authentication nas-identifier
      radius attribute authentication nas-port-id
      end
```

For Specific AAA Server Group:

```
configure
   context context_name
      aaa group group_name
```

```
radius attribute authentication nas-identifier
radius attribute authentication nas-port-id
end
```

Notes:

- If previously configured, use the **no radius attribute authentication nas-identifier** command and **no radius attribute authentication nas-port-id** commands to remove the configuration.
- By default, nas-identifier is enabled and nas-port-id is disabled.
- If these commands are configured under the Global Context Configuration Mode, the configuration will be applicable to the default AAA server group.
- If these commands are configured under the respective AAA server group, the configuration will be applicable to that AAA server group only.
- For expected functionality, both **nas-identifier** and **nas-port-id** keywords must be enabled.
- When **radius attribute authentication nas-identifier** is configured, also configuring **radius attribute nas-identifier** under the Global Context Configuration or AAA Server Group Configuration Mode will overwrite the VLAN ID received from the UE.

Verifying Configuration for DHCP Trigger-based Session Creation

Use the **show subscribers samog-only** command to verify if a subscriber session is triggered on receiving DHCP messages.

show subscribers samog-only full

```
Session Trigger Type: DHCP
```

Use the **shown twan-profile** command to verify if DHCP trigger-based session creation is enabled for the TWAN profile.

show twan-profile name *twan_profile_name*

```
Session Trigger Type: DHCP
```

Monitoring and Troubleshooting DHCP Trigger-based Session Creation

DHCP Trigger-based Session Creation Show Command(s) and/or Outputs

show samog-service statistics

The following counters are available to the output of the **show samog-service statistics** command in support of this feature:

```
DHCP Stats:
  DHCP Triggered Stats:
    Total Attempts:                                    0
      DHCP Discover :                                  0
```

```
    DHCP Request :                                  0
  DHCP Trigger Retransmission:                      0
DHCP Messages Discarded:                          0
  Max Size Exceeded:                              0
  Non-Existing Session:                           0
  GiAddr Mismatch:                                0
  Unsupported HW Type or Length:                  0
  Stale Packets:                                  0
  Service Not Supported:                          0
  Non-DHCP Packets:                               0
  Parsing Error :                                 0
  No Resource:                                    0
  Internal Error:                                 0
  License Limit Exceeded:                         0
  Service Limit Exceeded:                         0
  Congestion control policy applied:              0
```

*Table 26: **show samog-service statistics** Command Output Descriptions*

Field	Description
DHCP Stats	
DHCP Triggered Stat	
Total Attempts	Total number of session setup attempts.
DHCP Discover	Total number of session setup attempts from DHCP Discover message.
DHCP Request	Total number of Session setup attempts from DHCP Request message.
DHCP Trigger Retransmission	Total number of DHCP messages retransmitted.
DHCP Messages Discarded	Total number of DHCP messages discarded due to a failure.
Max Size Exceeded	Total number of DHCP messages discarded due to exceeding the maximum size.
Non-Existing Session	Total number of DHCP messages discarded due to a non-existing session.
GiAddr Mismatch	Total number of DHCP messages discarded due to mismatches in the Gi address.
Unsupported HW Type or Length	Total number of DHCP messages discarded due to unsupported hardware type or length.
Stale Packets	Total number of DHCP messages discarded due to stale packets.
Service Not Supported	Total number of DHCP messages discarded due to the service not being supported.
Non-DHCP Packets	Total number of messages discarded due to non-DHCP packets.
Parsing Error	Total number of DHCP messages discarded due to parsing errors.
No Resource	Total number of DHCP messages discarded due to lack of resources
Internal Error	Total number of DHCP messages discarded due to an internal error.

Field	Description
License Limit Exceeded	Total number of DHCP messages discarded after the license limit is reached.
Service Limit Exceeded	Total number of DHCP messages discarded after the service limit is reached.
Congestion control policy applied	Total number of DHCP messages discarded due to the applied congestion control policy.

show subscribers samog-only full

The following field is available to the output of the **show subscribers samog-only full** command in support of this feature:

```
MRME Subscriber Info:
    AP MAC    : <ap_mac_address>        SSID    : <ssid>
 Session Trigger Type: DHCP/Radius
```

Table 27: show subscribers samog-only full Command Output Descriptions

Field	Description
AP MAC	Specifies the AP MAC address from the DHCP option 82.
SSID	Specifies the SSID value from the DHCP option 82.
Session Trigger Type	Specifies the session trigger type as DHCP or Radius.

show twan-profile name

The following field is available to the output of the **show twan-profile name** *profile_name* command in support of this feature:

```
 Location reported from DHCP Option 82 : Circuit-ID/Remote-ID
```

Table 28: show twan-profile name Command Output Descriptions

Field	Description
Location reported from DHCP Option 82	Specifies the sub-option in DHCP option 82 from where the location is reported from.

show aaa group name

The following fields are available to the output of the **show aaa group name** *group_name* command to indicate if the nas-identifier and nas-port-id configurations are enabled or disabled:

```
nas-identifier  : Enabled | Disabled
nas-port-id  : Enabled | Disabled
```

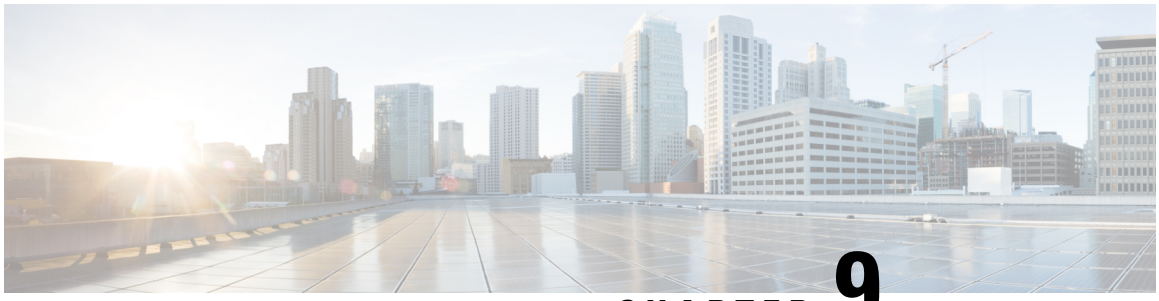
*Table 29: **show aaa group name** Command Output Descriptions*

Field	Description
nas-identifier	Indicates if the nas-identifier configuration is enabled/disabled for the SaMOG Gateway to send the nas-identifier attribute to the AAA server.
nas-port-id	Indicates if the nas-port-id configuration is enabled/disabled for the SaMOG Gateway to send the nas-port-id attribute to the AAA server.

DHCP Trigger-based Session Creation Bulk Statistics

The following bulks statistics included in the SaMOG schema support this feature:

Variable	Description	Data Type
mrme-dhcp-msg-discarded	**Description:** Total number of DHCP messages discarded by SaMOG. **Triggers:** Increments when DHCP messages are discarded. **Availability:** Per SaMOG Service **Type:** Counter	Int32
mrme-dhcp-discard-msgs-non-dhcp-pkts	**Description:** Total number of non-DHCP messages discarded by SaMOG. **Triggers:** Increments on receiving non-DHCP packets. **Availability:** Per SaMOG Service **Type:** Counter	Int32
mrme-dhcp-trigger-msgs-retransmitted-pkts	**Description:** Total number of retransmitted DHCP packets/messages received by SaMOG. **Triggers:** Increments on receiving retransmitted DHCP packets. **Availability:** Per SaMOG Service **Type:** Counter	Int32
mrme-dhcp-trigger-msgs-dhcp-request-pkts	**Description:** Total number of DHCP request packets received by SaMOG. **Triggers:** Increments on receiving DHCP request packets. **Availability:** Per SaMOG Service **Type:** Counter	Int32
mrme-dhcp-trigger-msgs-dhcp-discover-pkts	**Description:** Total number of DHCP Discover packets received by SaMOG. **Triggers:** Increments on receiving DHCP Discover packets. **Availability:** Per SaMOG Service **Type:** Counter	Int32



CHAPTER 9

DSCP Marking

This feature enables the SaMOG Gateway to perform DSCP marking on the uplink and downlink data packets on S2a and WLAN interfaces.

The following sections provide more detailed information:

Feature Description

Overview

The SaMOG Gateway supports DSCP marking on the uplink and downlink data packets. Service providers can use this feature to prioritize traffic across intermediate routers and deliver QoS services to subscribers. In an ePDG and SaMOG cascading network architecture for a Voice over WiFi (VoWiFi) over WLAN access, the SaMOG Gateway performs DSCP marking and prioritization to VoWiFi traffic using the Flow-based Local Breakout (LBO).

DSCP marking is supported on the EoGRE, PMIPv6, and L3-IP network access types, and GTP-U (GGSN-GTPv1 and PGW-GTPv2) and GRE (PMIPv6-based S2a) S2a-U variants on the network side. SaMOG can perform DSCP marking on IPv4, IPv6, and dual PDNs.

Relationship to Other Features

Flow-based Local Breakout

In an ePDG cascading architecture with SaMOG for VoWiFi over trusted WLAN access, DSCP marking in the SaMOG Flow-based LBO model ensures that the desired DSCP marking is performed by ePDG in the downlink packets towards the TWAN in the access network.

Session Recovery

The QCI-QoS-Map table will be restored for the recreated session after session recovery. DSCP values are applied to the consecutive traffic based on the QCI-QoS mapping table configuration during the time of session recovery.

Web Authorization

DSCP marking will not be performed to the traffic redirected to the web portal during the pre-authentication phase. The traffic from the UE session in this phase is intended for session establishment and authorization, and has no QCI value. DSCP marking will be performed on the subscriber traffic during the TAL phase.

During reauthorization, if the QCI value is modified for the subscriber call, the new QCI's DSCP value will be applied.

How DSCP Marking Works

Architecture

The SaMOG Gateway performs DSCP marking on the data traffic based on the QCI value derived for the subscriber's call. The QCI value is obtained based on the following order of priority:

- QoS negotiated with internal P-GW
- AAA server supplied QoS value

The QCI-QOS mapping table for DSCP marking can be configured using the **qci** *qci_value* **[{ uplink | downlink } encaps-header { copy-inner | copy-outer | dscp-marking** *dscp_hex_value* **}]** command under the QCI-QOS Mapping Table Configuration Mode. This configuration enables the SaMOG Gateway to mark the DSCP value in the outermost IP packet sent out of SaMOG (i.e, EoGRE/GRE/GTPU tunnel's IP header).

A default DSCP value of 0x00 is marked on all uplink and downlink data traffic during the following scenarios:

- • When no QCI-QoS mapping table is mapped (for the APN profile or CGW service).
- When no QCI-specific DSCP marking is configured under the QCI-QoS mapping table.

QCI-QoS Mapping Table Selection

The DSCP marking is performed based on the QCI-QoS mapping table configuration under the Context Configuration mode. The QCI-QoS mapping table is mapped to the subscriber call in the following order of priority:

- Mapping under the APN Profile Configuration Mode
- Mapping under the CGW Service Configuration Mode

The SaMOG Gateway will use the QCI-QoS mapping table configured for the APN profile for the subscriber session call. If no table is associated, SaMOG will look for the QCI-QoS mapping table configured for the CGW service.

For more configuration information, refer Configuring DSCP Marking, on page 143.

DSCP Configuration Change

When the DSCP configuration for a QCI changes, the new QCI/DSCP configuration will be applied to new calls only. The new DSCP marking will not be applied to subscriber calls that are currently active.

When session recovery occurs after the QCI-QoS mapping table is modified, the SaMOG gateway uses the latest CLI configuration.

Modifying the QCI Value

The QCI value for the SaMOG bearer can be modified in one of the following ways:

- From the AAA server using the RAR/CoA messages
- From the P-GW using the Update-Bearer-Request message

The new QCI value for the SaMOG bearer is then applied to all consecutive data traffic.

QCI Value for Flow-based LBO Model

The traffic sent to the flow-based LBO network uses the QCI value configured using the **local-offload flow qci** *qci_value* command under the APN Profile Configuration Mode.

If the configured QCI value is between 128 and 254, the DSCP configuration using the **operator-defined-qci** command under the QCI-QoS Mapping Table Configuration Mode mapped to the APN profile is used.

If the QCI value is between 1 and 9, the DSCP configuration using the **qci** command under the QCI-QOS Mapping Table Configuration Mode mapped to the APN profile is used.

For more configuration information, refer Configuring DSCP Marking, on page 143.

QCI Value for LBO – Enhanced Model

The QCI value for the LBO – Enhanced model is obtained based on the negotiated QCI-QoS value from the internal or external P-GW.

Limitations

This following limitations apply to the DSCP Marking feature:

- Currently, SaMOG supports DSCP marking on Flow-based LBO and LBO – Enhanced models. LBO Basic is not supported.
- DSCP marking cannot be performed on control signalling messages.

Configuring DSCP Marking

Associating the QCI-QoS Mapping Table

Use the following configuration to associate the QCI-QoS mapping table with the specified APN profile or CGW Service.

For APN Profile:

```
config
    apn-profile profile_name
        associate qci-qos-mapping mapping_table_name
        end
```

For CGW Service:

```
config
    context context_name
        cgw-service service_name
            associate qci-qos-mapping mapping_table_name
            end
```

Notes:

- By default, this configuration is disabled.
- To remove the configuration:
  - APN Profile Configuration mode: use the **remove associate qci-qos-mapping** command.
  - CGW Service Configuration mode: Use the **no associate qci-qos-mapping** command.
- *mapping_table_name* must be an alphanumeric string between 1 and 63 characters.

Configuring Downlink DSCP Marking

Use the following configuration to configure DSCP marking for downlink packets.

```
config
    qci-qos-mapping mapping_table_name
        qci qci_value downlink encaps-header { copy-inner | copy-outer |
dscp-marking dscp_hex_value }
        end
```

Notes:

- Use the **no qci** *qci_value* command to remove the configuration.
- *qci_value* must be an integer from 1 through 9.
- **encaps-header**: Specifies that the DSCP marking must be set on the encapsulation header for IP-in-IP, GRE, or GTP encapsulation.
- **copy-inner**: Specifies to copy the DSCP value from the inner IP packet's header in the S2a-u (GTP-U/PMIP-GRE) to the outer tunnel header towards UE (EoGRE/PMIP-GRE/Direct-IP).
- **copy-outer**: Specifies to copy the DSCP value from the outer tunnel header of the S2a-u (GTP-U/PMIP-GRE) to the outer tunnel header towards UE (EoGRE/PMIP-GRE/Direct-IP).
- **dscp-marking** *dscp_hex_value*: Specifies to enable marking of the specified *dscp_hex_value* in the downlink direction per QCI.
  - *dscp_hex_value* must be a hexadecimal number from 0x00 through 0x3F.

- When this configuration does not exist for the subscriber session's QCI, SaMOG will not perform DSCP marking to the downlink packets, and 0x00 (best effort) value will be marked.

Configuring Uplink DSCP Marking

Use the following configuration to configure DSCP marking for uplink packets

```
config
   qci-qos-mapping mapping_table_name
      qci qci_value uplink encaps-header { copy-inner | copy-outer |
dscp-marking dscp_hex_value }
      end
```

Notes:

- Use the **no qci** *qci_value* command to remove the configuration.
- *qci_value* must be an integer from 1 through 9.
- **encaps-header**: Specifies that the DSCP marking must be set on the encapsulation header for IP-in-IP, GRE, or GTP encapsulation.
- **copy-inner**: Specifies to copy the DSCP value from the inner IP packet's header from the UE (EoGRE/PMIP-GRE/Direct-IP) to the outer tunnel in the S2a-u (GTP-U/PMIP-GRE) towards P-GW.
- **copy-outer**: Specifies to copy the DSCP value from the outer tunnel header from the UE (EoGRE/PMIP-GRE/Direct-IP) to the outer tunnel in the S2a-u(GTP-U/PMIP-GRE) towards P-GW.
- **dscp-marking** *dscp_hex_value*: Specifies to enable marking of the specified *dscp_hex_value* in the uplink direction per QCI.
  - *dscp_hex_value* must be a hexadecimal number from 0x00 through 0x3F.
- When this configuration does not exist for the subscriber session's QCI, SaMOG will not perform DSCP marking to the uplink packets, and 0x00 (best effort) value will be marked.

Configuring QCI Value for Flow-based Local Breakout

Use the following configuration to specify the QCI for flow-based Local Breakout (LBO).

```
config
   apn-profile profile_name
      local-offload flow qci qci_value
      end
```

Notes:

- By default, this configuration is disabled.
- Use the **no local-offload flow qci** command to remove the configuration.
- *qci_value* must be an integer from 1 through 9, or 128 through 254.
  - For QCI range configured from 128 through 254, the DSCP configuration using the **operator-defined-qci** command (refer Configuring Downlink DSCP Marking for Flow-based Local Breakout, on page 146 and Configuring Uplink DSCP Marking for Flow-based Local Breakout, on

page 146) under the QCI-QoS Mapping Table Configuration Mode mapped to this APN profile is used.

- For QCI range configured from 1 through 9, the DSCP configuration using the **qci** command (refer Configuring Downlink DSCP Marking, on page 144 and Configuring Uplink DSCP Marking, on page 145) under the QCI-QoS Mapping Table Configuration Mode mapped to this APN profile is used.

Configuring Downlink DSCP Marking for Flow-based Local Breakout

Use the following configuration to configure DSCP marking for downlink packets using flow-based LBO.

```
config
   qci-qos-mapping mapping_table_name
     operator-defined-qci qci_value { gbr | non-gbr } downlink encaps-header
 { copy-inner | copy-outer | dscp-marking dscp_hex_value }
      end
```

Notes:

- Use the **no operator-defined-qci** *qci_value* command to remove the configuration.
- *qci_value* must be an integer from 128 through 254.
- **gbr**: Specifies that the QCI type is Guaranteed Bit Rate (GBR).
- **non-gbr**: Specifies that the QCI type is non-Garanteed Bit Rate (GBR).
- **encaps-header**: Specifies that the DSCP marking must be set on the encapsulation header for IP-in-IP, GRE, or GTP encapsulation.
- **copy-inner | copy-outer**: Specifies to copy the DSCP value from the IP packet's header from the LBO network towards the IP header in the access side network (EoGRE/PMIP-GRE/Direct-IP).
- **dscp-marking** *dscp_hex_value*: Specifies to enable marking of the specified *dscp_hex_value* in the downlink direction per LBO QCI.
  - *dscp_hex_value* must be a hexadecimal number from 0x00 through 0x3F.
- When this configuration does not exist, SaMOG will not perform DSCP marking to the downlink packets for the flow-based LBO.

Configuring Uplink DSCP Marking for Flow-based Local Breakout

Use the following configuration to configure DSCP marking for uplink packets using flow-based LBO.

```
config
   qci-qos-mapping mapping_table_name
     operator-defined-qci qci_value { gbr | non-gbr } uplink encaps-header
 { copy-inner | copy-outer | dscp-marking dscp_hex_value }
      end
```

Notes:

- Use the **no operator-defined-qci** *qci_value* command to remove the configuration.

- *qci_value* must be an integer from 128 through 254.
- **gbr**: Specifies that the QCI type is Guaranteed Bit Rate (GBR).
- **non-gbr**: Specifies that the QCI type is non-Garanteed Bit Rate (GBR).
- **encaps-header**: Specifies that the DSCP marking must be set on the encapsulation header for IP-in-IP, GRE, or GTP encapsulation.
- **copy-inner**: Specifies to copy the DSCP value from the inner IP packet's header from the UE (EoGRE/PMIP-GRE/Direct-IP) to the LBO IP header towards the LBO network.
- **copy-outer**: Specifies to copy the DSCP value from the IP packet's header from the outer tunnel header from the UE (EoGRE/PMIP-GRE/Direct-IP) to the LBO IP header towards the LBO network.
- **dscp-marking** *dscp_hex_value*: Specifies to enable marking of the specified *dscp_hex_value* in the uplink direction per LBO QCI.
  - *dscp_hex_value* must be a hexadecimal number from 0x00 through 0x3F.
- When this configuration does not exist, SaMOG will not perform DSCP marking to the uplink packets for the flow-based LBO.

Monitoring and Troubleshooting DSCP Marking

DSCP Marking Show Command(s) and/or Outputs

show apn-profile full

The information is available in the output of the **show apn-profile full { all | name** *profile_name* **}** command in support of this feature:

```
Local Offload              : Enabled
  Type                     : Flow
  QCI                      : 129
```

Table 30: show apn-profile full { all | name profile_name } Command Output Descriptions

Field	Description
Local Offload	Indicates if Local Offload is enabled.
Type	Indicates the type of LBO.
QCI	Configured QCI value.

show cgw-service all

The output of the **show cgw-service all** command displays the QCI-QOS mapping table name:

```
Service name                    : cgw1
  QCI-QOS mapping table         : map1
```

Table 31: show cgw-service all Command Output Descriptions

Field	Description
Service name	Displays the configured name of the service.
QCI-QOS mapping table	Displays the configured QCI-QOS mapping name for that CGW service.

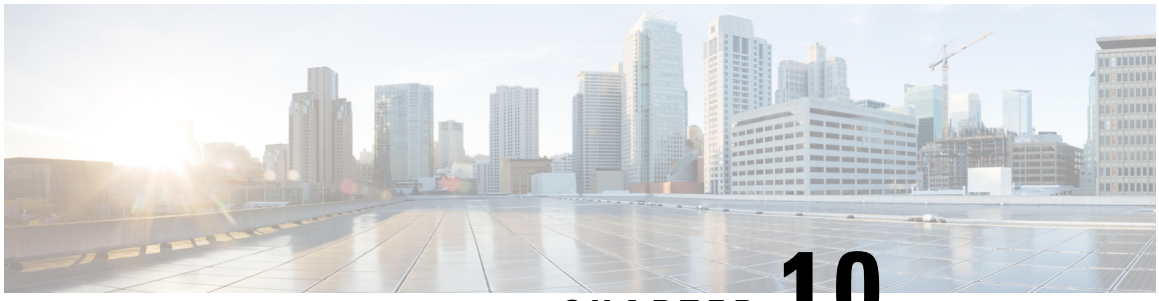
show subscribers samog-only full

The following counter is available to the output of the **show subscribers samog-only full** command in support of this feature:

```
Local Offload Flow Details:
    QCI                         : 129
```

Table 32: show subscribers samog-only full Command Output Descriptions

Field	Description
Local Offload Flow Details	
QCI	Configured QCI value.



CHAPTER 10

MAC Address in Decimal Format for P-GW

This feature enables the SaMOG Gateway to encode the User Equipment's MAC address in the IMEISV IE value in decimal format, in order to support inter-operability with P-GW from third party vendors.

The following sections provide more detailed information:

Feature Description

During call establishment, the SaMOG Gateway encodes the UE MAC address in the IMEISV IE value to decimal format and sends the Create Session Request message with the encoded value to P-GW. This ensures inter-operability between SaMOG and some third party vendor's P-GW that requires the UE MAC address in decimal format.

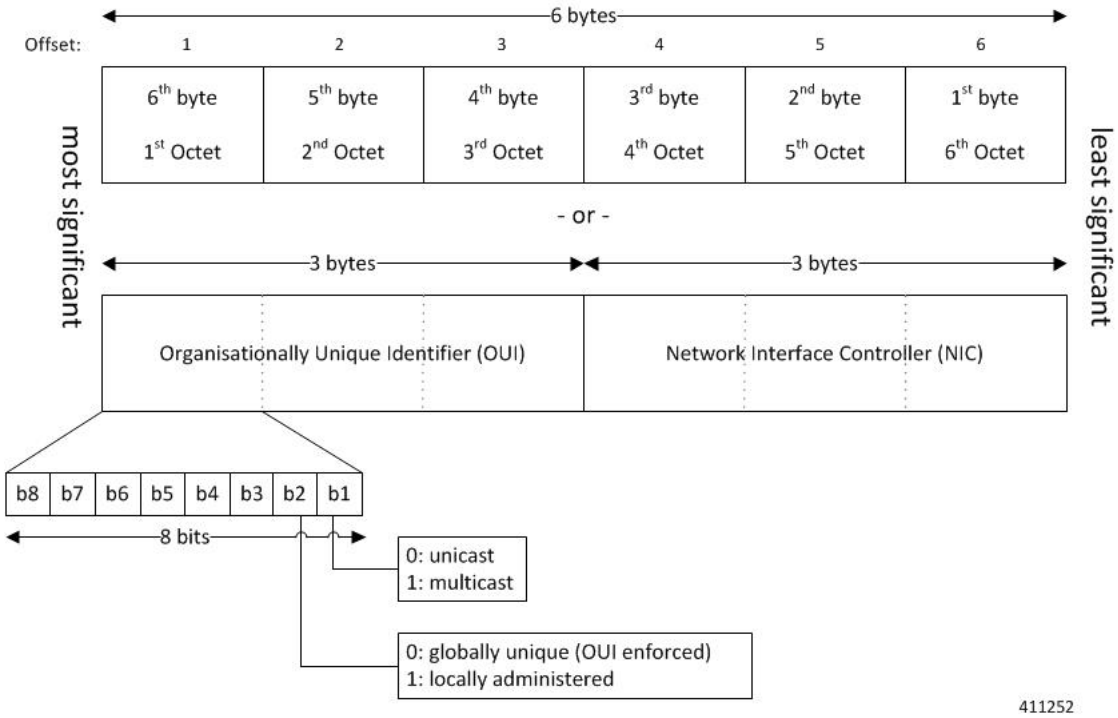
This feature can be configured by enabling the **decimal** keyword in the **samog-gtpv1** and **samog-s2a-gtpv2** commands under the Call Control Profile Configuration Mode. For more configuration information, refer Configuring MAC Address Encoding, on page 151.

How it Works

Architecture

The IMEI is a 15 digit decimal number that consists of a 14 digit value and 1 check digit, while the IMEISV field is a 16 digit decimal number that consists of a 14 digit value and 2 digit software version. The User Equipment's (UE) MAC address is a 6 byte or a 48 bit hexa-decimal value. As the maximum value of 6 bytes exceeds the 15 digit value in the IMEI field, 2 bits of the UE MAC address are removed and the remaining bits are left shifted. The SaMOG Gateway converts this value into decimal format and sends it to P-GW.

The following figure displays the bit representation and conversion of the MAC address:



The **b1 bit** represents the MAC address as unicast or multicast, and the **b2 bit** represents the MAC address as globally unique or locally administered.

Examples:

- UE MAC Address: 8AF9ABD5C613

  After bits 1 and 2 are removed: 22F9ABD5C613

  Decimal converted value: 38455725114899

  TBCD encoded value (sent to P-GW): 83547552118499F0

- UE MAC Address: FFFFFFFFFFFF

  After bits 1 and 2 are removed: 3FFFFFFFFFFF

  Decimal converted value: 70368744177663

  TBCD encoded value (sent to P-GW): 07637844716736F0

- UE MAC Address: 0034567890AB

  After bits 1 and 2 are removed: 0034567890AB

  Decimal converted value: 224789041323

  TBCD encoded value (sent to P-GW): 00227498403132F0

Standards Compliance

The interface between the SaMOG Gateway and P-GW complies with the following 3GPP standards:

- 3GPP TS 23.002

- 3GPP TS 29.060
- 3GPP TS 29.274

Configuring MAC Address Encoding in Decimal Format

Configuring MAC Address Encoding

Use the **decimal** keyword in the **samog-gtpv1** and **samog-s2a-gtpv2** commands under the Call Control Profile Configuration mode to enable SaMOG Gateway to encode the IMEI attribute in decimal format to send to P-GW.

```
configure
    call-control-profile profile_name
       samog-gtpv1 send imeisv value ue-mac decimal
       samog-s2a-gtpv2 send imeisv value ue-mac decimal
      end
```

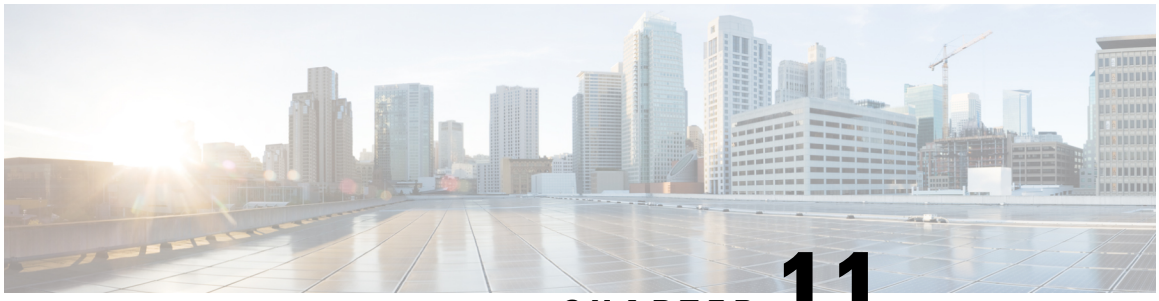
- By default, SaMOG sends the IMEISV value in hexa-decimal format.
- Use the **no samog-gtpv1 send imeisv** and **no samog-s2a-gtpv2 send imeisv** commands to disable decimal encoding.
- For further information on the other command keywords and the use of the command prefixes, refer to the *Command Line Interface Reference* for Release 20.0.

Verifying Configuration

Use the **show call-control-profile** command to verify the configuration of this feature.

show call-control-profile full name *profile_name*

```
Samog-GTPv1:
    Sending IMEI(SV) IE                                                 : Enabled
    IMEI(SV) IE Value Type                                              : UE MAC in Decimal
Samog-S2a-GTPv2:
    Sending IMEI(SV) IE                                                 : Enabled
    IMEI(SV) IE Value Type                                              : UE MAC in Decimal
```



CHAPTER 11

MN-NAI Support for Web Authorization Calls

This chapter describes MN-NAI support for web authorization calls in the following sections:

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SaMOG
Applicable Platform(s)	ASR 5500
Feature Default	Enabled - Always On
Related Changes in This Release	Not Applicable
Related Documentation	• *SaMOG Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
First introduced.	21.4

Feature Description

MN-NAI based authentication is supported for Web Authorization calls.

Earlier, SaMOG only supported IMSI based pre-authentication to post-authentication transition. Now, MN-NAI based pre-authentication to post-authentication transition is also supported.

SaMOG now supports pre-Authentication to post-Authentication transition for DHCP and PMIPv6 triggered sessions. The output for the **show subscribers samog-only full** command is modified to show the pre and post-authentication phases for DHCP and PMIPv6 triggered calls. For DHCP and PMIPv6 triggered calls, the UE-MAC is displayed as Username in the output when the **show subscribers samog-only full** and **show subscribers samog-only all** commands are executed.

For DHCP and PMIPv6 triggered sessions, SaMOG directs a TAL setup towards a local P-GW when an incoming Accept-Accept request contains an IMSI or MN-NAI value as a user identity. If the Accept-Accept request does not contain any user identity, the SaMOG processes the request as a pre-authentication call.

How It Works

The MN-NAI Web Authorization Calls supports:

- MN-NAI in the CoA request.
- Pre-authentication phase for DHCP and PMIPv6 triggered sessions.

The above implementations are applicable for both LBO-Basic and LBO-Enhanced models.

LBO Enhanced (also called as LBO Heavy): Uses a local P-GW/GGSN service locally to offload traffic to the internet. The UE's IP address is allocated by a local P-GW/GGSN service.

LBO Basic (also called as LBO Lite): Does not use a local P-GW/GGSN service. Here, the SaMOG itself offloads data to the internet. The UE's IP address is allocated by an SaMOG service.

MN-NAI is also applicable for DHCP and PMIPv6 triggered sessions. The session establishment call flows for DHCP and PMIPv6 triggered sessions are discussed in the *Call Flows* section.

Note From Release 21.4 onwards, the existing call flows for DHCP and PMIPv6 triggered sessions are not supported.

For more information on DHCP and PMIPv6 triggered sessions, refer to *DHCP Trigger-based Session Creation* and *PMIPv6-based Session Creation* chapters in the *SaMOG Administration Guide* respectively.

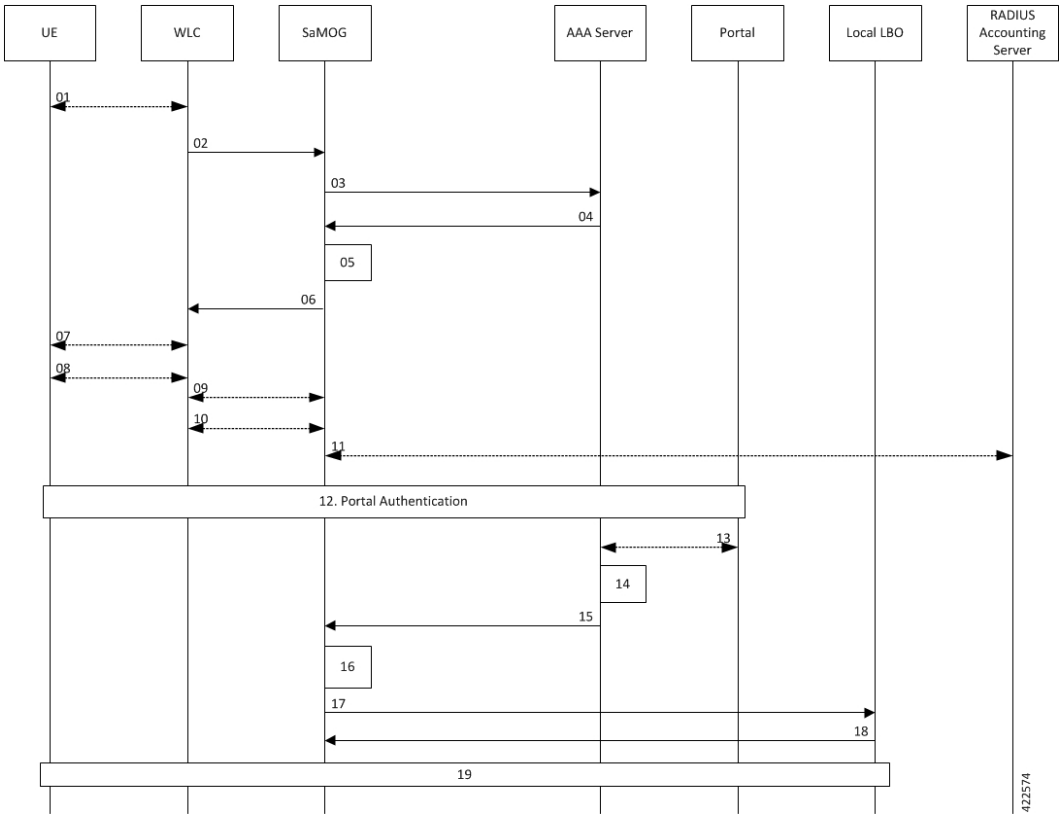
Call Flows

This section provides various call flows that illustrate the procedures used during DHCP and PMIPv6 triggered session establishment.

RADIUS Triggered - Web Authorization Call/Session Establishment

The figure below shows the detailed session establishment flow for a RADIUS triggered session. The table that follows the figure describes each step in the flow.

Figure 18: RADIUS Triggered Session Establishment Call Flow



Step	Description
01	UE sends 802.1x association request to AP/WLC with the SSID/Open-SSID information that it wishes to associate with.
02	WLC sends Access Request to SaMOG as the SSID on WLC is configured with MAC based authentication and the SaMOG is configured as RADIUS Server. Here, the EAP payload will not be present.
03	On SaMOG, SSID based policy is applied. If applicable operator policy allows Non-EAP based authentication, SaMOG fetches the AAA authentication server information from the policy and forwards Access-Request to AAA.
04	AAA sends Access-Accept request to SaMOG. The AAA server also sends a Session-Timeout AVP with a small value to allow web authentication.

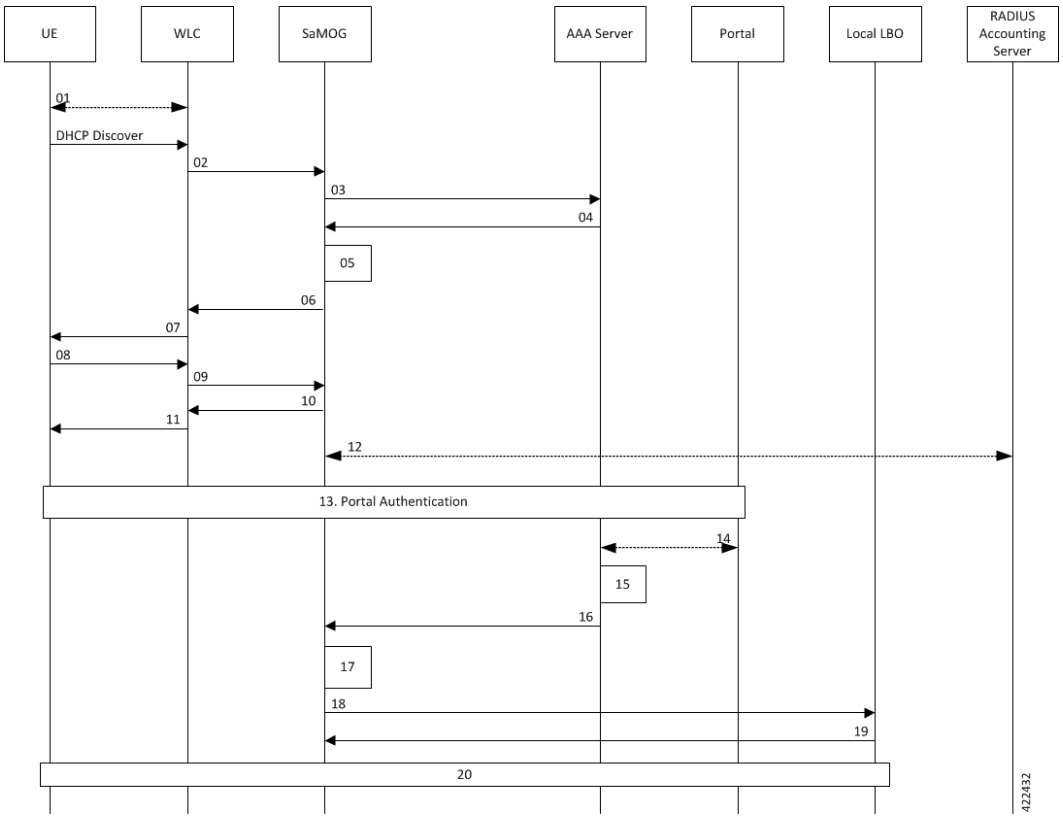
Step	Description
05	SaMOG triggers the following procedures before sending an Access-Accept message to WLC: • Allocate IP address from the local pool. • Initiate the Web-Auth and Pre-Auth timer. • Install L4/L7 Redirect Rules. The local P-GW assigns an IPv4 address and forwards it to the SaMOG Gateway.
06	SaMOG sends Access-Accept to WLC.
07	WLC sends 802.1x association response to UE. MAC based authentication between UE and AP/WLC is now complete.
08	UE performs L3 Attach procedures by initiating DHCP/IPv6-ND messages to WLC for fetching the IP Address or the IPv6-prefix.
09	WLC initiates EoGRE/PMIPv6 procedures towards SaMOG for L3 Attach.
10	Accounting is enabled on WLC and SaMOG is configured as an accounting server on the WLC.
11	SaMOG forwards an accounting start request towards AAA. AAA then associates the UE MAC Address and UE IP Address. AAA sends a Accounting Start Response, which will be forwarded by SaMOG towards WLC.
12	Web-based authentication takes place between UE and Portal Server.
13	After the user is authenticated, portal server fetches MSISDN, IMSI or MN-NAI information of the user. Portal sends CoA request (user-name, IMSI or MSISDN, UE IP Address) towards AAA. AAA associates the UE MAC Address and UE IP Address with the IMSI, MSISDN or MN-NAI value. It sends MAP request towards HSS to fetch the UE subscription details
14	AAA associates the UE MAC address, UE Subscription with the IMSI, MSISDN or MN-NAI value of the subscriber.
15	Further to this, AAA will be able to provide UE subscription details to SaMOG for a MAC based look-up. AAA caches this information as per operator policy, so that UE need not be redirected to the portal server every time.
16	SaMOG processes the received RADIUS CoA based on locally configured web-authentication APN-profile, SaMOG looks for IMSI or MN-NAI value in CoA. If IMSI or MN-NAI is part of CoA packet, SaMOG removes the L4-Redirection rules, and also removes the DL NPU flow for the allocated IP addresses.

Step	Description
17	es SaMOG initiates a GTPv2 CSReq for static IP address allocation with a.b.c.d and p:q:r:s::/64 for provided the IMSI or MN-NAI value towards Local LBO based on received subscriber profile or locally configured APN-profile in case subscriber-profile is not received as part of RADIUS CoA.
18	SaMOG receives a GTPv2 CSResp from Local LBO with the allocated IP addresses of end user.
19	SaMOG forwards the packet through the Local LBO; through the GTP-U Tunnel.

DHCP-triggered Web Authorization Call/Session Establishment

The following figure illustrates a detailed session establishment flow for a DHCP triggered session.

Figure 19: DHCP-triggered Session Establishment Call Flow



Step	Description
01	The UE communicates with the WLC over the 802.11 link for WiFi association and data transmission.
02	The WLC receives the control (DHCP, ARP, etc.) and data packets from the UE and forwards them over the EoGRE tunnel to the SaMOG gateway.

Step	Description
03	On receiving the DHCP Request or DHCP Discover message sent by the UE from the WLC over the EoGRE tunnel, the SaMOG gateway acts as the RADIUS client and sends a RADIUS Access-Request to the AAA server to obtain the subscriber information based on the UE MAC address (received in L2 DHCP packet).
04	AAA server determines that the UE MAC is not authenticated and sends an Access-Accept message without an IMSI or MN-NAI value in the MAC@realm format. These values are received using CS-AV pair attributes similar to DHCP/Radius Accounting triggered sessions.
05	SaMOG triggers the following procedures: • Allocate IP address from the local pool. • Initiate the Web-Auth and Pre-Auth timer. • Install L4/L7 Redirect Rules. The local P-GW assigns an IPv4 address and forwards it to the SaMOG gateway.
06	The SaMOG gateway in turn forwards the IPv4 address in the DHCP Offer/Reply message to the AP over the EoGRE tunnel.
07	The WLC forwards the DHCP offer with the allocated IP address towards the UE.
08	UE sends a DHCP request towards the WLC.
09	WLC forwards the DHCP request towards SaMOG.
10	SaMOG provides a DHCP acknowledgment.
11	The DHCP acknowledgment is forwarded to the UE.
12	SaMOG sends a RADIUS Accounting Request to the RADIUS accounting server and receives the corresponding response.
13	Web-based authentication takes place between UE and Portal Server.
14	After the user is authenticated, portal server fetches MSISDN, IMSI or MN-NAI information of the user. Portal sends CoA request (user-name, IMSI or MSISDN, UE IP Address) towards AAA. AAA associates the UE MAC Address and UE IP Address with the IMSI, MSISDN or MN-NAI value. It sends MAP request towards HSS to fetch the UE subscription details.
15	AAA associates the UE MAC address, UE Subscription with the IMSI, MSISDN or MN-NAI value of the subscriber.
16	Further to this, AAA will be able to provide UE subscription details to SaMOG for a MAC based look-up. AAA caches this information as per operator policy, so that UE need not be redirected to the portal server every time.

Step	Description
17	SaMOG processes the received RADIUS CoA based on locally configured web-authentication APN-profile, SaMOG looks for vIMSI or MN-NAI value in CoA. If IMSI or MN-NAI is part of CoA packet, SaMOG removes the L4-Redirection rules, and also removes the DL NPU flow for the allocated IP addresses. SaMOG retains the allocated IP addresses and stops the webauth_preauth_timer.
18	SaMOG initiates a GTPv2 CSReq for static IP address allocation with a.b.c.d and p:q:r:s::/64 for provided the vIMSI or MN-NAI value towards Local LBO based on received subscriber profile or locally configured APN-profile in case subscriber-profile is not received as part of RADIUS CoA.
19	SaMOG receives a GTPv2 CSResp from Local LBO with the allocated IP addresses of end user.
20	SaMOG forwards the packet through the Local LBO; through the GTP-U Tunnel.

PMIPv6-triggered Web Authorization Call/Session Establishment

The following figure illustrates a detailed session establishment flow for a PMIPv6-based session.

Figure 20: PMIPv6-triggered Session Establishment Call Flow

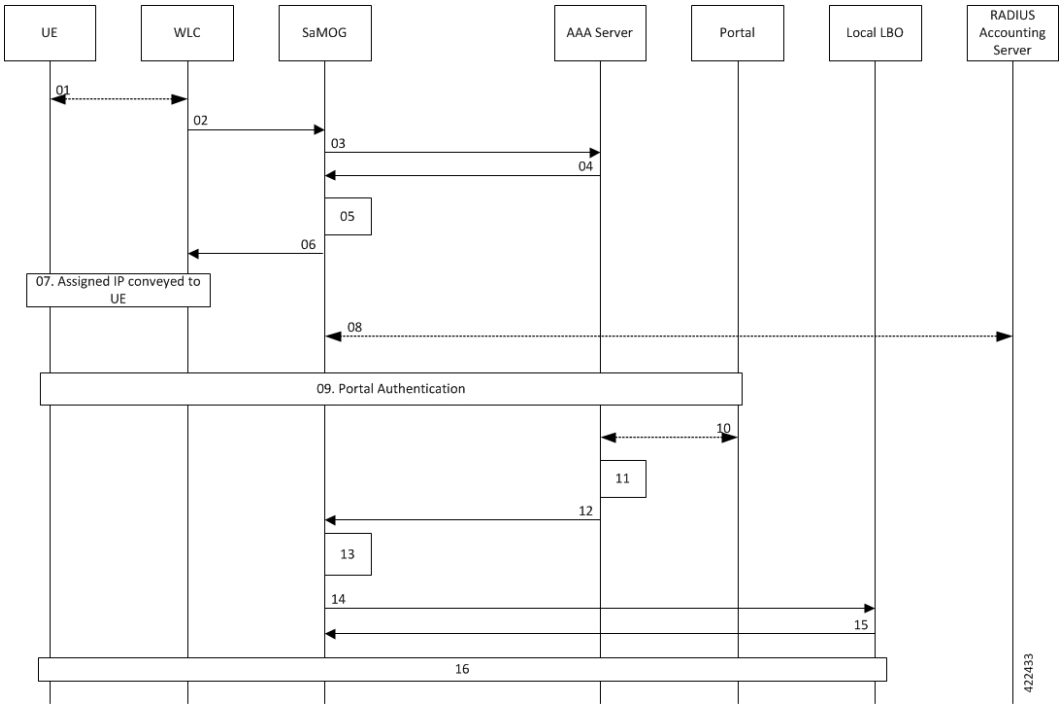


Table 33: PMIPv6-triggered Session Establishment Call Flow Descriptions

Steps	Description
01	UE performs 802.11 association with the WLC.
02	WLC forms a PMIPv6 Proxy Binding Update (PBU) and sends it to SaMOG. The message has the following parameter: UE MAC address in the Username part of NAI, or NAI can be only UE MAC (MAC@realm or MAC).
03	SaMOG caches the PBU message and maps its contents to the Radius Access-Request message towards the AAA server.
04	AAA server determines that the UE MAC is not authenticated and sends an Access-Accept message without an IMSI and MN-NAI value in the MAC@realm format. These values are received using CS-AV pair attributes similar to DHCP/Radius Accounting triggered sessions.
05	SaMOG triggers the following procedures: • Allocate IP address from the local pool. • Initiate the Web-Auth and Pre-Auth timer. • Install L4/L7 Redirect Rules.
06	SaMOG completes the session creation by sending the PBA message to the WLC.
07	UE attempts to access the HTTP page and the HTTP packet reaches the local gateway through SaMOG.
08	SaMOG sends a RADIUS Accounting Request to the RADIUS accounting server and receives the corresponding response.
09	Web-based authentication takes place between UE and Portal Server.
10	After the user is authenticated, portal server fetches MSISDN, IMSI or MN-NAI information of the user. Portal sends CoA request (user-name, IMSI or MSISDN, UE IP Address) towards AAA. AAA associates the UE MAC Address and UE IP Address with the IMSI, MSISDN or MN-NAI value. It sends MAP request towards HSS to fetch the UE subscription details.
11	AAA associates the UE MAC address, UE Subscription with the IMSI, MSISDN or MN-NAI value of the subscriber.
12	Further to this, AAA will be able to provide UE subscription details to SaMOG for a MAC based look-up. AAA caches this information as per operator policy, so that UE need not be redirected to the portal server every time.

Steps	Description
13	SaMOG processes the received RADIUS CoA based on locally configured web-authentication APN-profile. SaMOG looks for IMSI or MN-NAI value in CoA. If IMSI or MN-NAI is part of CoA packet, SaMOG removes the L4-Redirection rules, and also removes the DL NPU flow for the allocated IP addresses. SaMOG retains the allocated IP addresses, and stops the webauth_preauth_timer.
14	SaMOG initiates a GTPv2 CSReq for static IP address allocation with a.b.c.d and p:q:r:s::/64 for provided the vIMSI or MN-NAI value towards Local LBO based on received subscriber profile or locally configured APN-profile in case subscriber-profile is not received as part of RADIUS CoA.
15	SaMOG receives a GTPv2 CSResp from Local LBO with the allocated IP addresses of the end user.
16	SaMOG forwards the packet through the Local LBO; through the GTP-U Tunnel.

Limitations

SaMOG does not support RADIUS Accounting Triggered sessions for Web Authentication. This is under development and intended for future use. In Release 21.4, only TAL (post-authentication phase) is supported for RADIUS Accounting triggered sessions.

Monitoring and Troubleshooting

This section provides information on the show commands available to support the MN-NAI Support for Web Authorization Calls.

Show Command(s) and/or Outputs

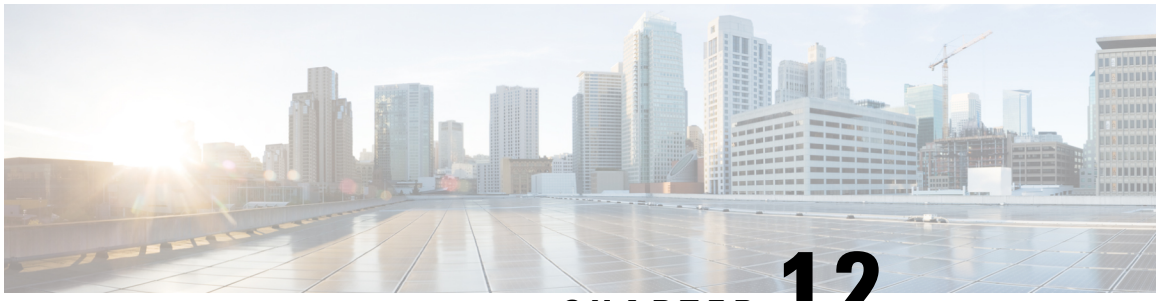
show subscribers samog-only full

The following new fields are added to the output of this command for DHCP and PMIPv6 session triggers during the pre-authentication phase:

- DHCP Trigger
  - Web authorization phase
  - IP pool name
  - IPv6 pool name
  - IP context name
  - Rulebase name
  - Access-list Name

    - Post-pre switch

- PMIPv6 Trigger
    - Web authorization phase
    - IP pool name
    - IPv6 pool name
    - IP context name
    - Rulebase name
    - Access-list Name
    - Post-pre switch



CHAPTER 12

PMIPv6-based Session Creation

The following topics are discussed:

Feature Description

Overview

SaMOG supports Radius Access-Request, Radius Accounting-Request and DHCP messages as the triggers for session creation.

Based on the AP/WLC capabilities, SaMOG can support session establishment in the following ways:

- When the AP/WLC is capable of RADIUS-based authentication, SaMOG acts as a AAA server and initiates session creation when it receives a RADIUS Access-Request from the AP/WLC.
- When the AP/WLC is capable of only forwarding DHCP messages from the UE through an EoGRE tunnel, SaMOG initiates session creation on receiving DHCP Discover and DHCP Request messages from the AP/WLC.
- When the AP/WLC is not capable of establishing EoGRE connections, is configured with a DHCP server, and the UE IP is allocated by the AP, SaMOG acts as an accounting server and allocates an IP. SaMOG then performs NAT between the IP allocated by the AP, and the IP allocated by SaMOG to establish a session for the subscriber.

With this feature, the SaMOG Gateway can also initiate session creation when it receives a PMIPv6 (PBU) message from the access point (AP). This feature integrates SaMOG as a gateway in deployment architectures where the AP/WLC can only initiate PMIPv6 messages, and not RADIUS or DHCP messages.

License Requirements

The following licenses are required for this feature:

- SaMOG General license (3G and 4G)

- SaMOG Local Breakout - Enhanced license to configure a local P-GW

Relationship to Other Features

DHCP-triggered and RADIUS-based Session Creation

DHCP-triggered and RADIUS (Access and Accounting) triggered sessions can co-exist with the PMIPv6-based sessions if the AP initiating the sessions are on different TWAN profiles. These TWAN profiles must have a corresponding session trigger configured.

Session Recovery

The PMIPv6-based sessions can be recovered for both unplanned failures and planned migrations.

How PMIPv6-based Session Creation Works

Architecture

The following is the sequence of events for a PMIP-based session creation deployment model:

- The UE communicates with the AP/WLC over the 802.11 link for WiFi association and data transmission. The AP/WLC forms a PMIPv6 Proxy Binding Update (PBU) message with the UE MAC in the Username part of NAI or UE MAC as NAI (MAC@realm or MAC).
- The AP/WLC sends the PBU message to SaMOG over the GRE (PMIPv6) tunnel.
- On receiving the PBU message, SaMOG performs RADIUS-based authentication with the 3GPP AAA server.
- The SaMOG Gateway then uses the Local Breakout (LBO) - Enhanced feature to allocate an IPv4 address and forwards it in the PBU message to the AP.
- The AP forwards this message to the UE.
- Any UE initiated traffic is then forwarded to a web authentication portal through the AP, SaMOG Gateway, and the local P-GW (LBO).
- The UE is presented with a web portal for subscriber authentication. The web portal authenticates the subscriber credentials with the AAA server, and informs the PCRF.
- The PCRF responds to the web portal with an RAR message on the Gx interface to remove the HTTP redirection rules.
- All UE traffic is henceforth directed to the Internet.

Limitations

Architectural Limitations

- This feature supports RADIUS-based authentication between SaMOG and the 3GPP AAA Server. Diameter-based authentication is currently not supported.
- With this feature, the AP will not send the SSID or location information in the PBU message.
- Only IPv4 address allocation is supported for the UE. IPv6 and IPv4v6 PDN types are currently not supported.
- All interfaces towards all external nodes will be IPv4 address only. IPv6 transport on any interface with external nodes is currently not supported.

Flows

PMIPv6-based Session Establishment

The figure below shows the detailed session establishment flow for a PMIPv6-based session. The table that follows the figure describes each step in the flow.

Figure 21: PMIPv6-based Session Establishment Call Flow

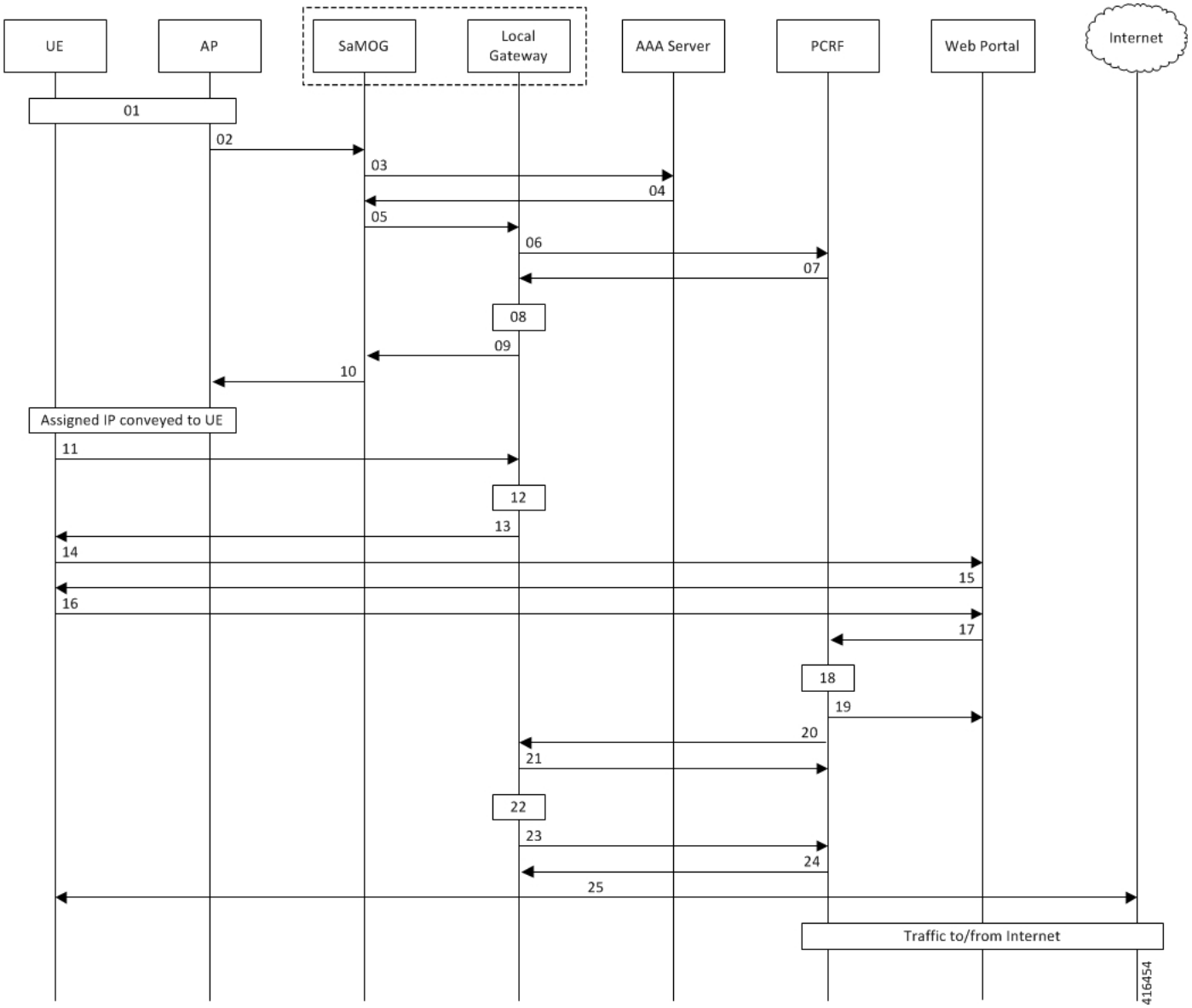


Table 34: PMIPv6-based Session Establishment

Step	Description
01	UE performs 802.11 association with the AP.
02	AP forms a PBU and sends it to SaMOG. The message has the following parameter: UE MAC address in the Username part of NAI, or NAI can be only UE MAC (MAC@realm or MAC).
03	SaMOG caches the PBU message and maps its contents to the Radius Access-Request message towards the AAA Server.

Step	Description
04	AAA server determines that the UE MAC is not authenticated and sends an Access-Accept message with an access point name (APN) and NAI in the MAC@realm format. These values are received using CS-AVPair attributes similar to DHCP/Radius Accounting triggered sessions.
05	SaMOG initiates a PMIPv6 Proxy Binding Update (PBU) message towards the Local Gateway (LGW) to setup the network side of the call. The MNID of the PBU is the NAI received from the AAA Server.
06	LGW sends CCR-I towards the PCRF, and includes the NAI/MNID received from SaMOG in the PBU.
07	PCRF determines that the subscriber is not authenticated and sends a CCA-I with Layer 7 (L7) redirection rulebase name.
08	LGW installs the L7 redirection rule and proceeds with session creation.
09	LGW allocates an IP address for the UE, and sends the same in Proxy Binding Answer (PBA) message towards SaMOG.
10	SaMOG completes the session creation by sending the PBA message to the AP.
11	UE attempts to access the HTTP page, and the HTTP packet reaches the LGW through SaMOG.
12	As the L7 redirection rule on the LGW is active, the LGW intercepts the HTTP packet.
13	LGW responds with a HTTP 302 response and provides the URL of the web authentication portal to the UE.
14	UE sends the HTTP GET request to the web portal through SaMOG and LGW.
15	The web portal presents the login page to the UE to enter the username and password.
16	Subscriber enters the username and password to perform web authentication.
17	The web portal invokes the PCRF API to share the username, password, and the source IP address of the packet.
18	PCRF validates the subscriber credentials and marks the UE MAC corresponding to the IP address as authenticated.
19	PCRF indicates authentication success to the web portal. The web portal then sends a HTTP 302 response to the UE with redirect to the originally accessed web page.
20	PCRF sends an RAR message on the Gx interface to indicate the removal of redirection rule.
21	LGW acknowledges with an RAA message.
22	LGW removes the L7 redirection rule for the UE session.
23	LGW sends a CCR-U message to PCRF to get quota information for the authenticated session.

Step	Description
24	PCRF sends the requested information in the CCA-U message.
25	UE attempts to connect to the originally accessed web page again. As the L7 rule is not present at the LGW this time, the packets are sent to the Internet.

Configuring PMIPv6-based Session Creation

Enabling PMIPv6-based Session Creation Trigger

Use the following configuration to enable PMIPv6-based session creation:

```
configure
   context context_name
      twan-profile profile_name
         session-trigger pmipv6
         end
```

Notes:

- Use the **default session-trigger** command to reset the configuration to its default value.
- **Default**: RADIUS (authentication)-based session trigger

Monitoring and Troubleshooting PMIPv6-based Session Creation

Show Command(s) and/or Outputs

show samog-service statistics

The following fields are available to the output of the **show samog-service statistics** command in support of this feature:

```
PMIP Trigger Session Stats:
  Total Attempted:               0
  Total Setup:                   0
  Total Current:                 0
  Total Released:                0
  Total Aborted:                 0
  Total Disconnected:            0
```

*Table 35: **show samog-service statistics** Command Output Descriptions*

Field	Description
PMIP Trigger Session Stats:	

Field	Description
Total Attempted	Total number of PMIP-triggered MRME calls attempted.
Total Setup	Total number of PMIP-triggered MRME calls that were successfully established.
Total Current	Total number of PMIP-triggered MRME calls that are currently present in the system.
Total Released	Total number of PMIP-triggered MRME calls aborted/disconnected.
Total Aborted	Total number of PMIP-triggered MRME sessions aborted before call establishment.
Total Disconnected	Total number of PMIP-triggered MRME sessions disconnected after call establishment.

show subscribers samog-only full

The following fields are available to the output of the **show subscribers samog-only full** command in support of this feature:

```
MRME Subscriber Info:
 ---------------------
    Session Trigger Type: pmip
```

*Table 36: **show subscribers samog-only full** Command Output Descriptions*

Field	Description
MRME Subscriber Info:	
Session Trigger Type	The session trigger type applied for the subscriber. Session Trigger type can be one of the following: • DHCP • Radius • Radius Acct • pmip

show twan-profile

The following fields are available to the output of the **show twan-profile { all | name** *profile_name* **}** command in support of this feature:

```
TWAN Profile Name                    : twan6
  Access-Type Client List
    Default Access Type              : PMIP
    Default Radius Dictionary        : custom70
    Session Trigger Type             : pmip
```

Table 37: show twan-profile Command Output Descriptions

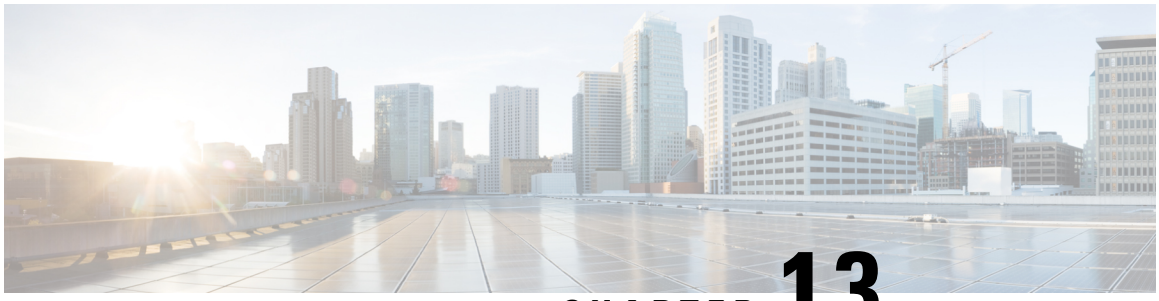
Field	Description
TWAN Profile Name	Name of the TWAN profile.
Access-Type Client List	
Default Access Type	Default access type set for the TWAN profile. Access type for the TWAN profile for PMIPv6-based session trigger must be PMIP.
Default Radius Dictionary	Default RADIUS dictionary used for the TWAN profile. The default RADIUS dictionary can be one of the following: • custom71 for Cisco WLC • custom70 for non-Cisco WLC
Session Trigger Type	The session trigger type set for the TWAN profile. Session Trigger type can be one of the following: • DHCP • Radius • Radius Acct • pmip

PMIPv6-based Session Creation Bulk Statistics

The following bulk statistics in the SaMOG schema provide PMIPv6-based session creation related information:

Variable	Description	Data Type
mrme-pmip-trigger-total-attempted	**Description:** Total number of PMIP-triggered MRME calls attempted. **Triggers:** Increments when an MRME call is attempted through PMIP-trigger. **Availability:** Per SaMOG Service **Type:** Counter	Int32
mrme-pmip-trigger-total-setup	**Description:** Total number of PMIP-triggered MRME calls that were successfully established. **Triggers:** Increments upon successful MRME call setup through PMIP-trigger. This does not decrement when the call is disconnected. **Availability:** Per SaMOG Service **Type:** Counter	Int32

Variable	Description	Data Type
mrme-pmip-trigger-total-current	**Description:** Total number of PMIP-triggered MRME calls that are currently present in the system. **Triggers:** Increments upon successful PMIP-triggered MRME call set up. Decrements upon successfuldisconnection of PMIP-triggered MRME call. **Availability:** Per SaMOG Service **Type:** Gauge	Int32
mrme-pmip-trigger-total-released	**Description:** Total number of PMIP-triggered MRME calls aborted/disconnected. **Triggers:** Increments when the PMIP-triggered MRME call is successfully disconnected. **Availability:** Per SaMOG Service **Type:** Counter	Int32
mrme-pmip-trigger-total-aborted	**Description:** Total number of PMIP-triggered MRME sessions aborted before call establishment. **Triggers:** Increments whenever PMIP-triggered MRME subscriber session is aborted by SaMOG due to various call setup failure such as authentication failure, pgw selection failure, and Session Setup Timeout. **Availability:** Per SaMOG Service **Type:** Counter	Int32
mrme-pmip-trigger-total-disconnected	**Description:** Total number of PMIP-triggered MRME sessions disconnected after call establishment. **Triggers:** Increments when PMIP-triggered MRME session gets disconnected. **Availability:** Per SaMOG Service **Type:** Counter	Int32



CHAPTER 13

RADIUS Accounting-based Session Creation

This feature enables the SaMOG Gateway to create sessions on receiving a RADIUS Accounting-Start messages for subscribers.

The following sections provide more detailed information:

Feature Description

Overview

The SaMOG Gateway can create sessions based on either of the following messages as a trigger:

RADIUS Access-Request messages: The Access Points (AP) or WLCs are configured with the SaMOG Gateway acting as the AAA Server. When the subscriber's user equipment (UE) performs an 802.11 association, these APs or WLCs trigger a RADIUS Access-Request message towards the SaMOG Gateway.

DHCP messages: The AP or WLC forwards DHCP messages (DHCP discover or DHCP Request) from the UE to the SaMOG Gateway over the EoGRE tunnel. The SaMOG Gateway uses this DHCP message as a trigger to initiate a session. This method of session creation is suited in networks where the AP or WLC is not capable of forwarding RADIUS messages.

RADIUS Accounting-based Session Creation

With the RADIUS Accounting-based Session Creation feature, sessions can be created when the APs forward a RADIUS Accounting-Start message with the allocated UE's IP address towards the accounting server. This method of session creation is suited in networks where the APs do not have EoGRE capabilities. These APs are configured with DHCP servers and the UE's IP address is allocated locally by the AP.

The SaMOG Gateway performs RADIUS-based authentication towards 3GPP AAA server by mapping parameters received in RADIUS Accounting request from the AP to a RADIUS Access-Request message towards the AAA server. The SaMOG Gateway perform APN-based local offload, using a Local P-GW for all accounting triggered sessions. The local P-GW allocates an IP address for the session. SaMOG performs

a static NAT between the UE's IP address (shared by the AP in the Framed-IP-Address attribute of the accounting message) and the IP address assigned by the local P-GW.

Relationship to Other Features

DHCP Triggered and RADIUS (Authentication)-based Session Creation

DHCP triggered and RADIUS (authentication) triggered sessions can co-exist with the RADIUS Accounting-based sessions if the AP initiating the sessions are on different TWAN profiles. These TWAN profiles must have a corresponding session trigger configured.

Session Recovery

The RADIUS Accounting-based sessions can be recovered for both unplanned failures and planned migrations.

Web Authorization

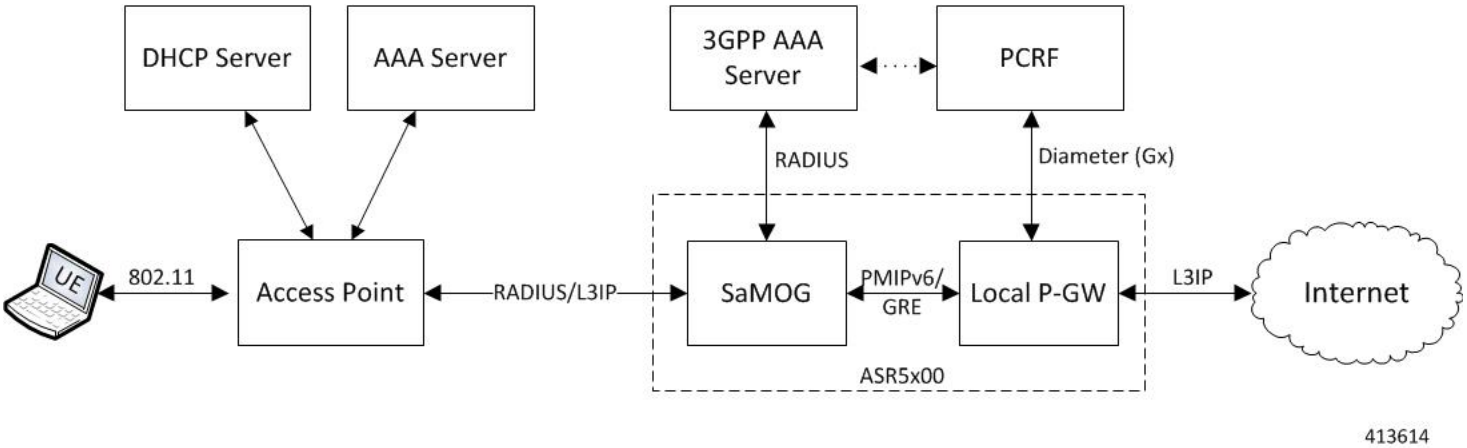
The SaMOG Gateway supports RADIUS Accounting-based session creation on the TAL phase of both Web Authorization and Optimized Web Authorization features. Session redirection is performed using the local P-GW.

How RADIUS Accounting-based Session Creation Works

Architecture

The following figure provides the deployment architecture for RADIUS Accounting-based session creation:

Figure 22: RADIUS Accounting-based Session Creation



The following are the sequence of events for a RADIUS Accounting-based session creation deployment model:

1. The AP allocates an IP address from a local DHCP server. SaMOG acts as an Accounting server for the AP.

2. Once the IP address is allocated, the AP sends an Accounting Start message to SaMOG with the allocated IP address in the Framed-IP-Address attribute.
3. SaMOG accepts the Radius Accounting Start message as a session trigger and performs authentication with a 3GPP AAA server.
4. The AAA server sends the UE details (received in the Accounting message) to the PCRF, and also forwards the NAI information to SaMOG based on the UE location.
5. On successful authentication, SaMOG establishes a connection with the local P-GW using PMIPv6 control protocol and obtains the IP address.
6. SaMOG uses the NAI information received from the AAA server in the PMIPv6 PBU message. This information is used by the local P-GW in the Gx messaging towards PCRF during session creation.
7. The local P-GW sends the redirection rules and other policies to the local P-GW based on the NAI information.
8. Once the session with the local P-GW is successfully established, SaMOG installs a static NAT between the UE's IP address and the IP address provided by the local P-GW.
9. SaMOG can now respond to Accounting Start messages, and the UE starts sending data over L3IP access towards SaMOG.
10. This data then NATTed towards the local P-GW and routed to the internet or redirected by the local P-GW as per the installed policy.
11. The downlink data is sent to SaMOG by the local P-GW and a reverse NAT is performed before forwarding the packets to the AP.

Flows

Session Establishment

The figure below shows the detailed session establishment flow for a RADIUS accounting-based session. The table that follows the figure describes each step in the flow.

Figure 23: RADIUS Accounting-based Session Establishment Call Flow

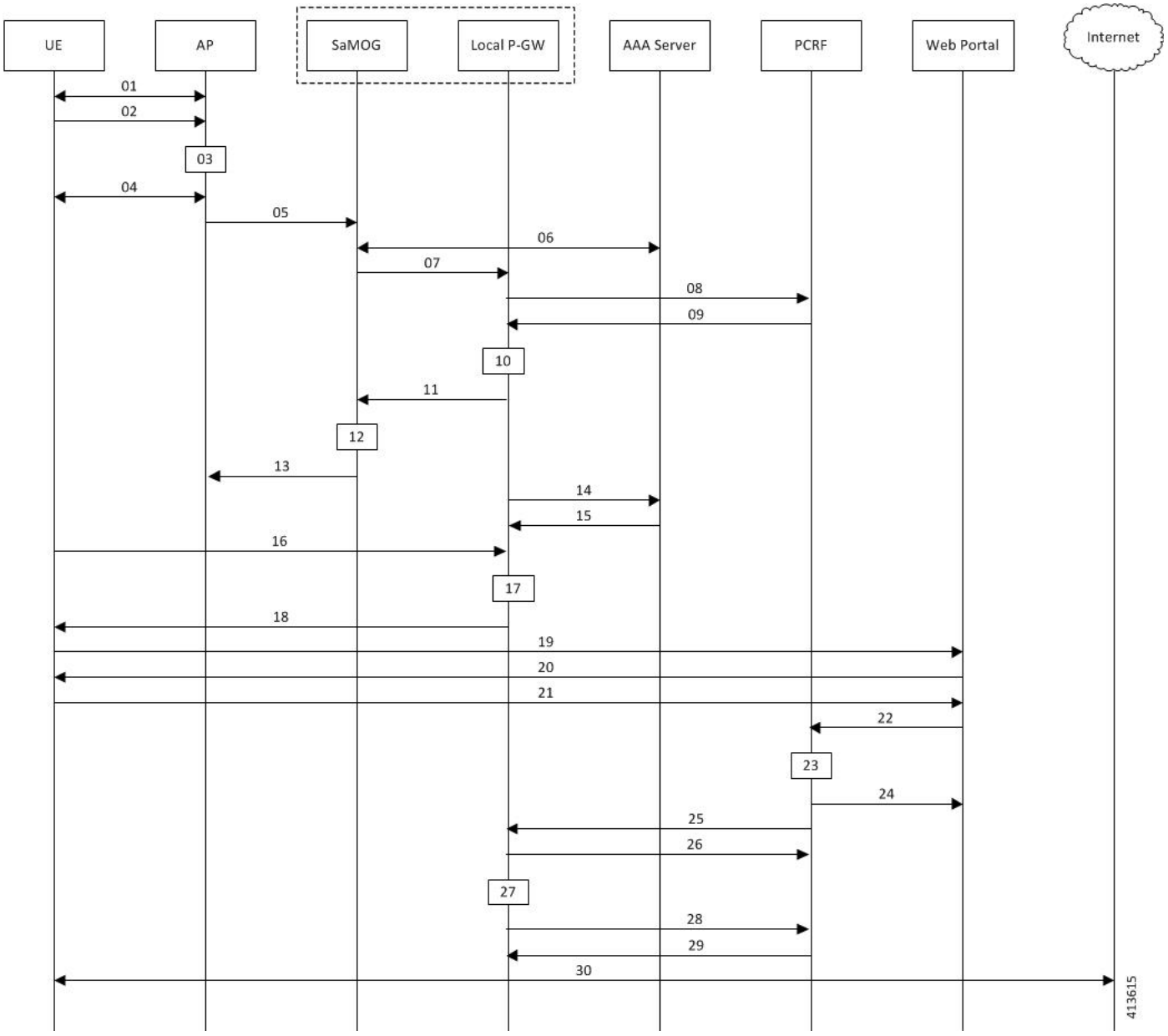


Table 38: RADIUS Accounting-based Session Establishment

Step	Description
01	UE performs 802.11 association with the AP and attaches to the open SSID.
02	UE sends DHCP Discover message to AP to get an IP address.
03	AP gets an IP address (For example, IP1) from a local DHCP server.

Step	Description
04	AP completes the DHCP transaction with the UE, and sends the IP (IP1) address to the UE in the DHCP offer/DHCP Reply message.
05	AP sends a Radius Accounting Start message to SaMOG with the following parameters: • UE MAC address in the Username and Calling Station-Id attribute. • Optional: VLAN ID in the NAS-Identifier attribute. • IP address (allocated by local DHCP server: IP1) in the Framed-IP-Address attribute. • AP-MAC and SSID in the Called-Station-Id attribute.
06	SaMOG caches the Accounting Start message and maps its contents to the Radius Access-Request message towards a AAA server. The Framed-IP-Address received in Accounting Start message is not sent towards the AAA server and the AP IP address (Radius endpoint address/source address of the Accounting Start message) is included in NAS-Port-Id attribute of the Access-Request. The AAA server determines that the UE MAC is not authenticated and sends Access-Accept message with an access point name (APN) and NAI in the MAC@realm format. These values are received using CS-AVPair attributes similar to DHCP triggered sessions.
07	SaMOG initiates a PMIPv6 Proxy Binding Update (PBU) message towards the local P-GW to setup the network side of the call. The MNID of the PBU is the NAI received from the AAA server.
08	The local P-GW sends CCR-I towards the PCRF, and includes the NAI/MNID received from SaMOG in the PBU message.
09	PCRF determines that the subscriber is not authenticated and sends a CCA-I with the L7 redirection rulebase name.
10	The local P-GW installs the L7 redirection rule and proceeds with session creation.
11	The local P-GW allocates an IP address (For example, IP2) for the UE and sends the IP address in the Proxy Binding Answer (PBA) message towards SaMOG.
12	SaMOG maps the static NAT between the IP address (IP1) received in the Accounting Start message from AP, and the IP address (IP2) sent by the local P-GW to the NAT table.
13	SaMOG completes session creation by sending the Accounting Response message to the AP.
14	The local P-GW sends an Accounting Start message towards the AAA server with the UE MAC and the Framed-IP-Address (with IP2).
15	The AAA server sends an Accounting Start response to the local P-GW.
16	The UE attempts to access the HTTP page, and the HTTP packet reaches the local P-GW through SaMOG. SaMOG performs static NAT to change the source IP address of the packet from IP1 to IP2 and forwards it to the local P-GW over the GRE tunnel.
17	As the L7 redirection rule on the local P-GW is active, HTTP packet is intercepted.

Step	Description
18	The local P-GW responds with a HTTP 302 response, and provides the URL of the authentication portal to the UE. SaMOG performs reverse NAT on this packet before forwarding it to the UE.
19	UE sends the HTTP GET request to the portal through SaMOG and the local P-GW.
20	The portal presents the login page to the UE to enter the username and password.
21	The subscriber enters the username and password to perform web authentication.
22	The portal shares the username, password and the source IP address (IP2) of the packet to the PCRF.
23	The PCRF validates the user credentials and marks the UE MAC corresponding to IP2 as authenticated.
24	The PCRF indicates authentication success to the portal. The portal then sends an HTTP 302 response to the UE with a redirect to the originally accessed web page.
25	The PCRF sends an RAR message on the Gx interface to indicate removal of redirection rule.
26	The local P-GW acknowledges the RAR message with an RAA message.
27	The local P-GW removes the L7 redirection rule for the UE session.
28	The local P-GW sends a CCR-U message to PCRF to get the quota information for the authenticated session.
29	The PCRF responds with a CCA-U message with the requested information.
30	UE now attempts to connect to the originally accessed web page again. As the L7 rule is not present at the local P-GW, the packets are sent to the Internet.

Standards Compliance

This feature complies with the following standard(s):

- RFC 2866 (RADIUS Accounting)

Configuring RADIUS Accounting-based Session Creation

Enabling RADIUS Accounting-based Session Creation Trigger

Use the following configuration to enable RADIUS Accounting-based session creation:

```
config
   context context_name
      twan-profile profile_name
```

```
session-trigger radius acct
end
```

Notes:

- Use the **default session-trigger** command to reset the configuration to its default value.
- **Default**: RADIUS (authentication)-based session trigger

Configuring Access Type and UE Address

Use the following configuration to configure the access type and UE address for RADIUS accounting-based session creation:

```
config
   context context_name
      twan-profile profile_name
         ue-address twan
         access-type ip
         end
```

Notes:

- Use the **ue-address twan** command to enable SaMOG to receive the TWAN UE address through the Accounting Start Framed-IP-Address message.
- • Use the **access-type ip** command to specify that all RADIUS clients under the TWAN profile will use the Layer 3 IP (L3IP) access type.

Monitoring and Troubleshooting RADIUS Accounting-based Session Creation

RADIUS Accounting-based Session Creation Show Command(s) and/or Outputs

show samog-service statistics

The following counters are available to the output of the **show samog-service statistics [** *service_name* **]** command in support of this feature:

```
MRME Service Stats:
Radius Accounting Trigger Session Stats:
Total Attempted:      0
Total Setup:          0
Total Current:        0
Total Released:       0
Total Aborted:        0
Total Disconnected:   0
```

Table 39: show samog-service statistics Command Output Descriptions

Field	Description
Radius Accounting Trigger Session Stats:	
Total Attempted	Total number of Accounting-triggered MRME calls attempted.
Total Setup	Total number of Accounting-triggered MRME calls that were successfully made.
Total Current	Total number of Accounting-triggered MRME calls that are currently present in the system.
Total Released	Total number of Accounting-triggered MRME calls disconnected/released.
Total Aborted	Total number of Accounting-triggered MRME sessions aborted.
Total Disconnected	Total number of Accounting-triggered MRME session disconnects.

show subscribers samog-only full

The following fields are available to the output of the **show subscribers samog-only full** command in support of this feature:

```
MRME Subscriber Info:
    Session Trigger Type:  Radius Acct
```

Table 40: show subscribers samog-only full Command Output Descriptions

Field	Description
MRME Subscriber Info	
Session Trigger Type	The session trigger type applied for the subscriber. Session Trigger type can be one of the following: • DHCP • Radius • Radius Acct

show twan-profile

The following fields are available to the output of the **show twan-profile { all | name** *profile_name* **}** command in support of this feature:

```
TWAN Profile Name         : prof1
    Access-Type Client List
        Default Access Type         : IP
        Default Radius Dictionary   : custom71 | custom 70
        UE-address Type             : TWAN
        Session Trigger Type        : Radius Acct
```

*Table 41: **show twan-profile** Command Output Descriptions*

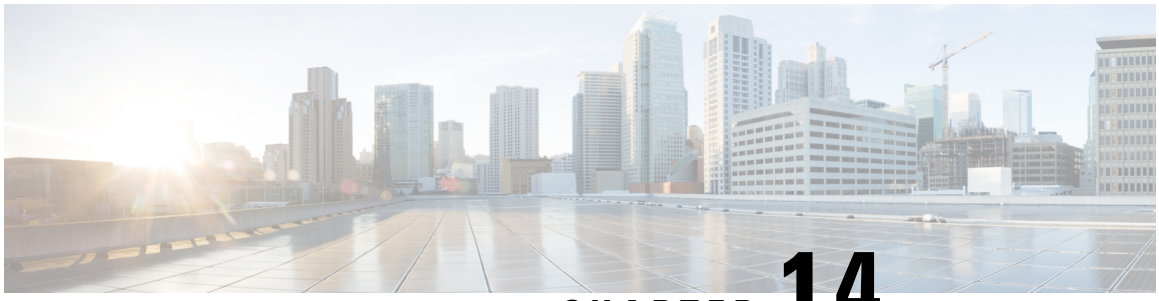
Field	Description
TWAN Profile Name	Name of the TWAN profile
Access-Type Client List	
Default Access Type	Default access type set for the TWAN profile. Access type for the TWAN profile for RADIUS-based session trigger must be IP.
Default Radius Dictionary	Default RADIUS dictionary used for the TWAN profile. The default RADIUS dictionary can be one of the following: • custom71 for Cisco WLC • custom70 for non-Cisco WLC
UE-address Type	UE's address type.
Session Trigger Type	The session trigger type set for the TWAN profile. Session Trigger type can be one of the following: • DHCP • Radius • Radius Acct

RADIUS Accounting-based Session Creation Bulk Statistics

The following bulks statistics included in the SaMOG schema support this feature:

Variable	Description	Data Type
mrme-acct-trigger-total-attempted	**Description**: Total number of Accounting-triggered MRME calls attempted. **Triggers**: Increments when there is an attempt to make an MRME call through accounting-trigger. **Availability**: Per SaMOG Service **Type**: Counter	Int32

Variable	Description	Data Type
mrme-acct-trigger-total-setup	**Description**: Total number of Accounting-triggered MRME calls that were successfully made. **Triggers**: Increments upon successful MRME call setup through accounting-trigger. This counter does not decrement when the call is disconnected. **Availability**: Per SaMOG Service **Type**: Counter	Int32
mrme-acct-trigger-total-current	**Description**: Total number of Accounting-triggered MRME calls that are currently present in the system. **Triggers**: Increments upon successful Accounting-triggered MRME call set up. Decrements upon successful disconnection of Accounting-Triggered MRME call. **Availability**: Per SaMOG Service **Type**: Gauge	Int32
mrme-acct-trigger-total-released	**Description**: Total number of Accounting-triggered MRME calls disconnected/released. **Triggers**: Increments when the Accounting-triggered MRME call is successfully disconnected. **Availability**: Per SaMOG Service **Type**: Counter	Int32
mrme-acct-trigger-total-aborted	**Description**: Total number of Accounting-triggered MRME sessions aborted. **Triggers**: Increments whenever Accounting-triggered MRME subscriber session is aborted by SaMOG due to various call setup failures such as authentication failure, P-GW selection failure, and Session Setup Timeout. **Availability**: Per SaMOG Service **Type**: Counter	Int32
mrme-acct-trigger-total-disconnected	**Description**: Total number of Accounting-triggered MRME session disconnects. **Triggers**: Increments when Accounting-triggered MRME session gets disconnected. **Availability**: Per SaMOG Service **Type**: Counter	Int32



CHAPTER 14

RADIUS Authentication-based non-UICC Sessions on PMIPv6 over S2a Interface

The following topics are discussed:

Feature Description

Overview

In Release 21.0 and earlier, for non-UICC devices, SaMOG supported the PMIPv6 protocol over the S2a interface for DHCP and RADIUS Accounting-based sessions.

In Release 21.1 and later, SaMOG supports the PMIPv6 protocol over the S2a interface for RADIUS Authentication triggered sessions also. This ensures that SaMOG can seamlessly handover non-UICC UE sessions that move from access points (AP) of one access type to another.

SaMOG forwards the MN-NAI value received from the AAA Server towards the Cisco WLC in the Access-Accept message. The Cisco WLC can use the same message in the PBU message towards SaMOG. For non-Cisco WLCs, the WLC may initiate a PBU message with the UE's MAC address (in any MAC format separated by '-', '.', ':') in the NAI attribute. SaMOG can then perform session lookup.

Web Authorization - Pre-Authentication Phase

In release 21.0 and earlier, during RADIUS authentication-based session creation, when the AAA server does not send the IMSI information in the Access-Accept message to SaMOG, SaMOG treats the call type as pre-authentication phase.

In release 21.1 and later, SaMOG applies the following logic to determine the call type as pre-authentication or Transparent Auto Logon (TAL) phase:

- If the IMSI information is included in the Access-Accept message from the AAA server, the call type will be considered as TAL phase (MN-NAI information can be included or excluded).
- If the IMSI information is not present and the MN-NAI information is present in the Acess-Accept message from the AAA server:

- SaMOG considers the call type to be TAL phase if the S2a protocol is PMIPv6.
- SaMOG considers the call type to be TAL phase, if the session trigger is DHCP or Accounting.
- SaMOG considers the call type to be pre-authentication phase if PMIPv6 is not the S2a protocol.

- If both IMSI and MN-NAI information is not present in the Access-Accept message from the AAA server, the call type will be considered as pre-authentication phase.

License Requirements

The following licenses are required for this feature:

- SaMOG General license (3G and 4G)
- SaMOG Local Breakout - Enhanced license to configure a local P-GW
- SaMOG Web Authorization license

Contact your Cisco account representative for detailed information on specific licensing requirements.

How RADIUS Authentication-based Sessions on PMIPv6 over S2a Interface Work

Flows

RADIUS PMIPv6-based Session Establishment with S2a-PMIPv6 LBO

The figure below shows the detailed session establishment flow for a RADIUS PMIPv6-based WLC with S2a-PMIPv6 Local Breakout session. The table that follows the figure describes each step in the flow.

Figure 24: RADIUS PMIPv6-based Session Establishment with S2a-PMIPv6 LBO Call Flow

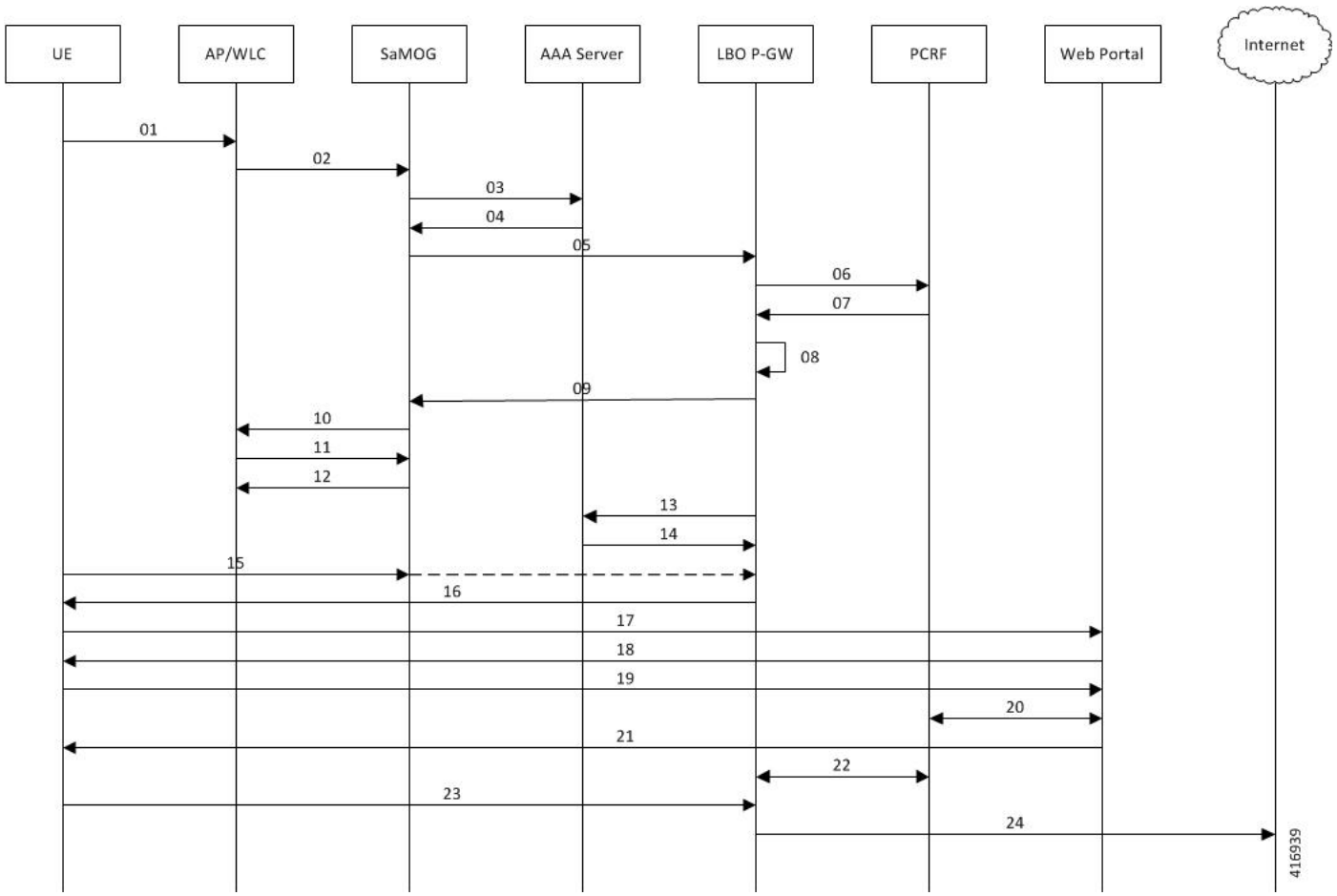


Table 42: RADIUS PMIPv6-based Session Establishment with S2a-PMIPv6 LBO

Step	Description
01	UE performs 802.11 association with the AP, and attaches to the open SSID.
02	AP forms a Radius Access Request (RAR) message and sends it to SaMOG. The RAR message has the following parameter: • UE MAC address in the Username and Calling-Station-Id attribute • (Optional) VLAN ID in the NAS-Identifier attribute • AP-MAC and SSID in the Called-Station-Id attribute
03	SaMOG caches the Access Request message from the AP/WLC and maps its contents to the Radius Access-Request message towards the AAA Server. The AP's IP address (Radius endpoint address/source address of the Access-Request message) is included in NAS-Port-Id attribute of the Access-Request message.

Step	Description
04	AAA server determines that the UE MAC is not authenticated and sends an Access-Accept message with an access point name (APN) and NAI in the MAC@realm format. These values are received using the CS-AVPair attributes similar to DHCP-triggered sessions.
05	SaMOG initiates a PMIPv6 Proxy Binding Update (PBU) message towards the Local Gateway (LGW) to setup the network side of the call. The MNID of the PBU is the NAI received from the AAA Server.
06	LGW sends CCR-I towards the PCRF, and includes the NAI/MNID received from SaMOG in the PBU.
07	PCRF determines that the subscriber is not authenticated and sends a CCA-I with Layer 7 (L7) redirection rulebase name.
08	LGW installs the L7 redirection rule and proceeds with session creation.
09	LGW allocates an IP address for the UE, and sends the same in Proxy Binding Answer (PBA) message towards SaMOG.
10	SaMOG completes the session creation by sending an Access-Accept message to the WLC with the MN-NAI attribute in MAC@realm format, as received from the AAA Server.
11	Cisco WLC sends a Proxy Binding Update (PBU) message with the NAI in MAC@realm format as received from SaMOG. Non-Cisco WLC sends a Proxy Binding Update (PBU) message with the NAI in MAC format.
12	SaMOG validates the NAI value received from the WLC. Upon successful validation of the NAI value, SaMOG sends a Proxy Binding Answer (PBA) message towards WLC.
13	LGW sends an Accounting Start message with the UE MAC and the Framed-IP-Address in the message towards the AAA Server.
14	AAA server sends Accounting Start response to the LGW.
15	UE attempts to access the HTTP page. The HTTP packet reaches the LGW through SaMOG. SaMOG forwards the packet to the LGW over the GRE tunnel.
16	As the L7 redirection rule on LGW is active, the HTTP packet is intercepted. LGW responds with an HTTP 302 response and provides the URL of the authentication portal to the UE. SaMOG forwards it to the UE.
17	UE sends an HTTP GET request to the portal through SaMOG and LGW.
18	The web portal presents the login page to the UE to enter the username and password.
19	Subscriber enters the username and password to perform web authentication.
20	The web portal invokes the PCRF API to share the username, password, and the source IP address of the packet. PCRF validates the user credentials and marks the UE MAC corresponding to the IP as authenticated.
21	The PCRF indicates an authentication success to the web portal. The web portal sends an HTTP 302 response to the UE with redirect to the originally accessed web page.

Step	Description
22	PCRF sends an RAR message on the Gx Interface to remove the redirection rule. LGW acknowledges the RAR with an RAA message. LGW removes the L7 redirection rule for the UE session. LGW sends a CCR-U message to the PCRF to get the quota information for the authenticated session. PCRF sends back a CCA-U message with the requested information.
23	UE attempts to reach the originally accessed web page again.
24	As the L7 rule is no longer present at the LGW, and the packets are sent to the Internet.

Limitations

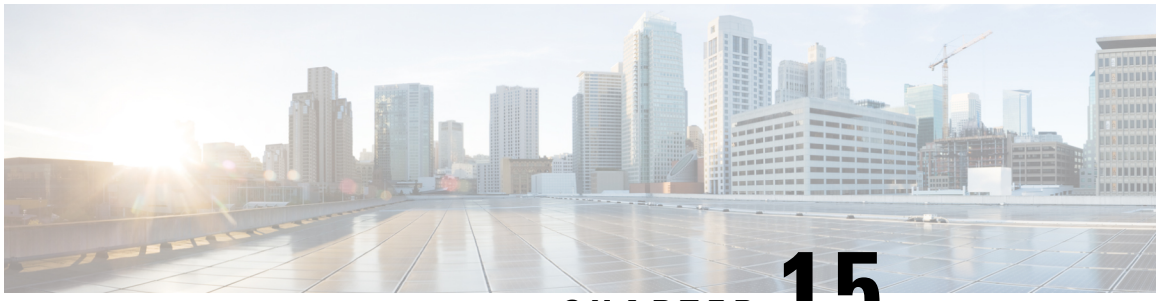
Architectural Limitations

- This feature currently supports RADIUS-based AAA Server only.
- Only IPv4 address allocation is supported for the UE. IPv6 and IPv4v6 PDN types are currently not supported.
- All interfaces towards all external nodes will be IPv4 address only. IPv6 transport on any interface with external nodes is currently not supported.

Standards Compliance

This feature complies with the following standards:

- **3GPP TS 23.402** - "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for non-3GPP accesses"
- **3GPP TS 29.274** - "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3"



CHAPTER 15

RADIUS-based Web Authorization with Local Breakout - Basic

The following topics are discussed:

Feature Description

Overview

In earlier releases, the SaMOG Gateway supports the Web Authorization and Local Breakout features:

- The Web Authorization feature enables SaMOG to register the subscriber's non-SIM UEs by authenticating the subscriber through a web portal (using username and password). In the pre-authentication phase, SaMOG allocates the IP address to the UE. In the TAL/post-authentication phase, the P-GW allocates the IP address to the UE.
- The Local Breakout – Basic feature enables SaMOG to connect subscriber's UE directly to the Internet without employing a local or external P-GW. The UE's IP address is allocated using an IP pool configured locally (or provided by the AAA Server).

For more information on the Web Authorization and Local Breakout – Basic features, refer the *SaMOG Administration Guide*.

This feature integrates SaMOG as a gateway in deployment architectures where service providers (such as cable operators) can connect subscriber's non-SIM UEs to the Internet without an external P-GW, using policies and rules provided by the RADIUS-based AAA server. Gx and Gy interface's capabilities are not required on these networks. The subscribers of the non-SIM devices are authenticated using web authorization, and connected to the Internet Service Provider (ISP) using Local Breakout – Basic.

License Requirements

The following licenses are required for RADIUS-based web authorization with LBO – Basic:

- SaMOG Local Breakout – Basic license
- SaMOG Web Authorization license
- Enhanced Charging Bundle (ECS) license
- (Optional) Application Detection and Control (ADC) license – To enable ADC related features

Contact your Cisco account representative for detailed information on specific licensing requirements.

Relationship to Other Features

Application Detection and Control (ADC)

This feature can support ADC functionalities when the ADC license is installed.

How RADIUS-based Web Authorization with LBO Basic Works

Architecture

Web Authorization

Pre-Authentication Phase

During the pre-authentication phase of web authorization, the Access-Accept message from the RADIUS-based AAA server contains the following attributes to enable SaMOG to assign IP address the UE and redirect the subscriber to the web portal:

- User-Name (UE MAC) – This is a mandatory attribute.
- SN1-Rulebase (Rulebase name in Starent VSA) – SaMOG redirects traffic to the web portal for subscriber authentication based on the configured rulebase, and its related ruledef and charging action. The rulebase can also be configured under the APN profile for SaMOG to use when the AAA Server does not share the rulebase. When both the rulebases exist, SaMOG will use the rulebase provided by the AAA Server.
- SN1-VPN-Name (Context name in the Starent VSA) – SaMOG allocates IPv4 or IPv6 address to the UE based on the IP pool configured for the context. The context can also be configured locally under the APN profile for SaMOG to use when the AAA Server does not share the context name.
- Framed-Pool (Pool name) – To indicate IPv4 and IPv6 pools, the AAA Server can send more than one IP pool name to SaMOG. SaMOG selects the pool configured under the context when the AAA Server does not share the pool name.
- Filter-ID (ACL name) – This attribute contains the allowed ACL for the UE.

Post-Authentication Phase

After the pre-authentication phase, SaMOG awaits the IMSI or MN-NAI attribute from the AAA Server in the CoA message. This CoA message acts as the post-authentication trigger. On receiving the CoA message,

SaMOG removes the redirection rule and installs new rules from the CoA message. If the CoA message is not received within 5 minutes (timer expiry of 300 seconds), SaMOG disconnects the session.

DSCP Marking

SaMOG supports DSCP marking in the web authorization post-authentication or direct TAL phase for uplink and downlink traffic. The QCI value is obtained in one of the following ways:

- The qci-qos-mapping table can be configured with the QCI value using the **qos default-bearer qci** *qci_value* under the APN Profile Configuration Mode. The QCI value can also be configured for the CGW service. Operator-defined DSCP marking, copy inner and copy outer options are supported.
- DSCP marking configured in the charging-action associated with a rulebase (using the Enhanced Charging Service). DSCP marking can be performed during pre-authentication and post-authentication phases.
- Default QCI value of 9.

When the qci-qos-mapping definition and configuration for DSCP marking under the charging-action exist, SaMOG will prefer the configuration for DSCP marking under the charging-action.

The following decision table provides various combinations of QCI configurations in the network, and the QCI value selection by SaMOG:

QCI received from AAA Server	QCI configured under APN profile	Charing action enabled with DSCP configuration	DSCP Marking (QCI value for the qci-qos-mapping table)
Yes	No	No	Value provided by the AAA Server
Yes	Yes	No	Value provided by the AAA Server
No	Yes	No	Value configured under the APN profile
No	No	No	Default QCI value of 9
Yes	No	Yes	Value configured under Charging Action
No	Yes	Yes	Value configured under Charging Action
Yes	Yes	Yes	Value configured under Charging Action
No	No	Yes	Value configured under Charging Action

SaMOG as an Accounting Client

SaMOG can perform the functionalities of an accounting client when access points do not have this capability. Use the **accounting mode radius-diameter** command under the Call Control Profile Configuration Mode to enable SaMOG to act as an accounting client. When enabled, SaMOG supports WLAN attributes like calling-station-id and called-station-id in the RADIUS accounting messages.

Flows

The figure below shows the detailed RADIUS-based web authorization flow with LBO – basic. The table that follows the figure describes each step in the flow.

Figure 25: RADIUS-based Web Authorization with LBO – Basic Call Flow

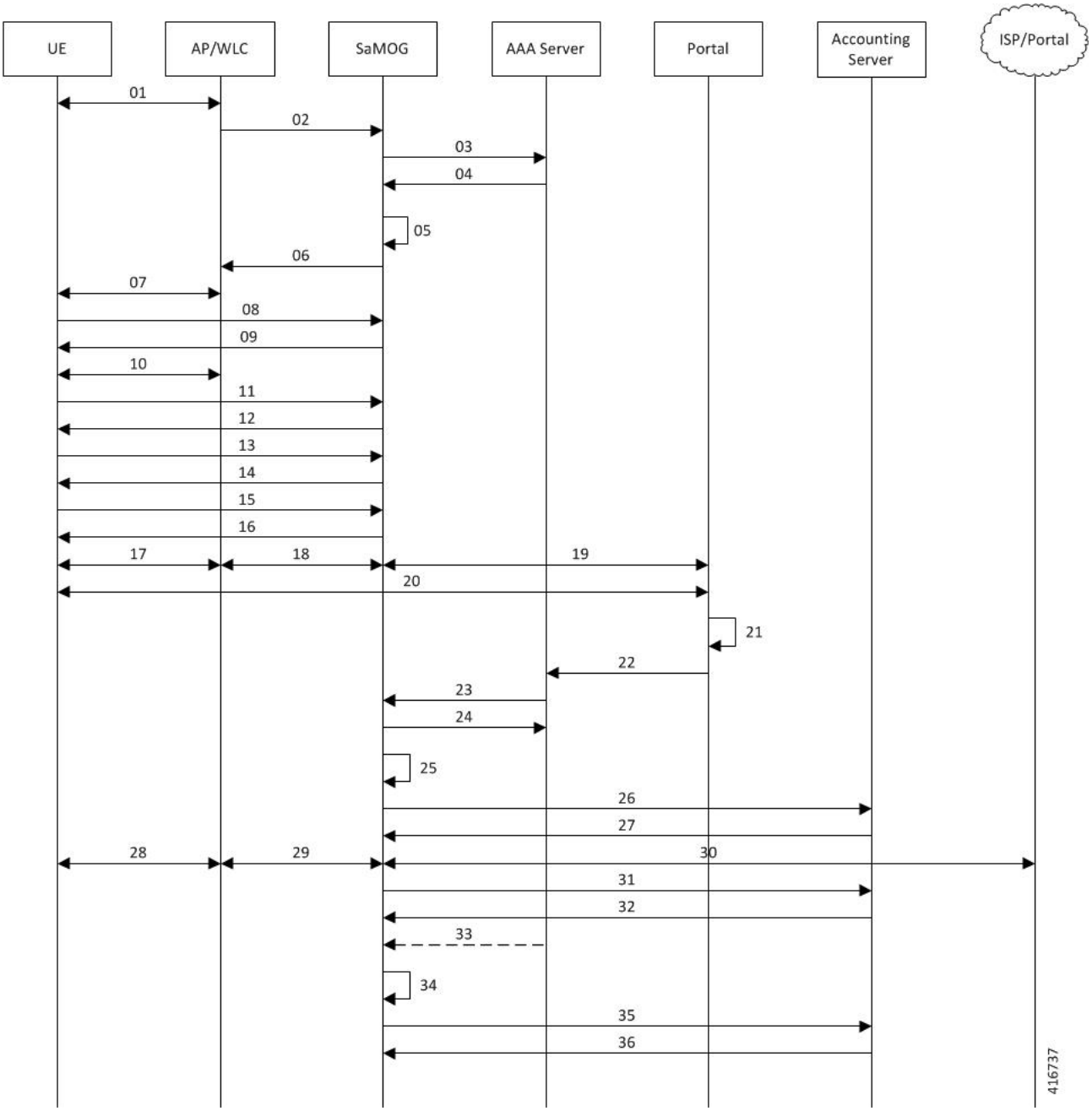


Table 43: RADIUS-based Web Authorization with LBO – Basic

Step	Description
01	UE sends 802.1x association request to AP/WLC with the SSID/Open-SSID information that it wishes to associate with.

Step	Description
02	On the WLC, the SSID is configured with MAC-based authentication, and SaMOG as the RADIUS Server. The WLC sends an Access-Request (user-name=UE-MAC, called-station-id=AP-MAC:SSID, Calling-Station-Id=UE-MAC) message to SaMOG without the EAP payload.
03	On SaMOG, an SSID-based policy is applied. If applicable, the operator policy allows Non-EAP based authentication. SaMOG fetches the AAA authentication server information from the policy. SaMOG initiates the authentication process by sending the Access-Request message received from the AP/WLC to the AAA server.
04	On the AAA Server, a MAC-based session lookup takes place as the user session is not found. Since the AAA Server is configured to allow user sessions, it sends an Access-Accept message to SaMOG. The subscription details will not be available on the AAA Server at this point. So the AAA Server sends only the user-name AVP in Access-Accept message. Optionally, the AAA server can provide the Filter-Id AVP and SN1-Rulebase AVPs for redirection along with SN1-IP-Pool-Name, SN1-VPN-Name, SN1-Primary/Secondary-DNS-Server, Framed-IPv6-Pool, SN1-IPv6-Primary/Secondary/DNS parameters.
05	Since the AAA Server does not provide the APN, SaMOG fetches the default web authorization APN profile associated to the operator policy. This APN profile is configured for IP address allocation and traffic redirection (if rulebase is not provided by the AAA Server). SaMOG performs the following procedures before sending the Access-Accept message to WLC: • Reserves IP Address (a.b.c.d and p:q:r:s::/64) from the local IP/IPv6 pool for UE. • Installs L4/L7 redirection rules to redirect the user traffic to the web portal and installs downlink NPU flow for the allocated ip-address and ipv6-prefix. • Initiates webauth_preauth_timer with a timeout value of 5 minutes. Post-authorization phase will be triggered within this timer.
06	SaMOG forwards the RADIUS Access-Accept message to the AP/WLC.
07	The WLC/AP sends an 802.1x association response to the UE. MAC-based authentication between the UE and AP/WLC is complete.
08	UE initiates an L3 attach procedure by sending a DHCP-Discover. SaMOG receives the same through the EoGRE tunnel.
09	SaMOG sends the allocated IPv4 address, default gateway address, and the lease duration through the DHCP-Offer message to the UE.
10	SaMOG sends DHCP-Request with a request IP as received in DHCP-Offer. SaMOG responds with a DHCP-Reply confirming the allotment of IP address.
11	UE sends the ARP-Request message to resolve the MAC address of the default gateway.

Step	Description
12	SaMOG sends ARP-Reply message to the UE with the virtual MAC address that is configured in the APN profile.
13	For IPv6/Dual stack, the UE sends a Router Solicitation to obtain the IPv6 address/prefix.
14	SaMOG responds to the UE with a Router Advertisement containing the IPv6 prefix.
15	UE sends a Neighbor Solicitation to determine the link-layer address of SaMOG.
16	SaMOG sends a Neighbor Advertisement to the UE with its link-layer address. The UE may also send a DHCPv6-Info-Request to obtain the DNS server addresses at this stage. If received, SaMOG sends a DHCPv6-Info-Reply with the DNS server addresses configured under the APN profile.
17	UE initiates data packets.
18	SaMOG receives the data packets from the UE through the EoGRE tunnel.
19	SaMOG redirects the traffic to a web portal as per the redirection rules installed (Step 5). If L4 rules are applied, SaMOG changes the destination address to the IP address of the portal, and forwards the packets. If L7 rules are applied, SaMOG redirects the packets to the IP address of the portal without modifying the destination address.
20	UE provides the subscriber's credentials for authorization.
21	Web-based authorization takes place between the UE and the portal server.
22	Portal server indicates the successful authentication status with the AAA server.
23	Post successful authentication, the AAA server triggers post-authorization phase by sending a CoA with the IMSI/MN-NAI and new rulebase in the SN1-Rulebase AVP. If CoA doesn't contain IMSI/MN-NAI identifier, SaMOG will not consider the CoA as a post-authorization trigger.
24	SaMOG sends CoA-Acknowledgement to the AAA Server.
25	SaMOG removes the redirection rules and installs the new rulebase received in the CoA message. SaMOG will offload the traffic locally with certain ECS capabilities.
26	SaMOG sends an Accounting-Request (Acct-Status-Type: Start) to the accounting server, if SaMOG has been configured to act as the Accounting client.
27	The Accounting Server sends an Accounting-Response to SaMOG.
28	UE initiates data packets.
29	SaMOG receives the data packets through the EoGRE tunnel.
30	SaMOG locally offloads the traffic to ISP without any redirection. SaMOG enforces any ECS capabilities like DSCP marking, rate limiting, MSS overwriting, and so on.

Step	Description
31	When the accounting interim conditions (volume/interval) configured under the AAA group are met, SaMOG sends an Accounting-Request (Acct-Status-Type: Interim) to the Accounting Server.
32	The Accounting Server sends an Accounting-Response to SaMOG.
33	(Optional) The AAA Server could send more CoA messages to SaMOG to install new rules.
34	SaMOG installs the new rules received in the CoA message.
35	Upon UE detach, SaMOG sends an Accounting-Request (Acct-Status-Type: Stop) message to the Accounting Server.
36	The Accounting Server sends an Accounting-Response message to SaMOG.

Configuring RADIUS-based Web Authorization with LBO – Basic

Configuring Local Breakout – Basic

The following is a sample configuration to enable Local Breakout – Basic:

```
lte-policy
    subscriber-map smap
      precedence 1 match-criteria all operator-policy-name oppolicywebauthdia

  operator-policy name oppolicywebauthdia
    associate call-control-profile cc-profwebauthdia
    apn webauth-apn-profile apnprfwebauth

  call-control-profile cc-profwebauthdia
    accounting context aaa aaa-group accounting1
    authenticate context aaa aaa-group STawebauth auth-method eap non-eap
#exit

apn-profile apnprfwebauth
    ip access-group acl-lbo-flow in
    ip access-group acl-lbo-flow out
    ip address pool name lbo-pool-1
    active-charging rulebase rb_lite
    ip context-name lbo-gi
    local-offload
    twan default-gateway 12.0.0.10/8
    accounting mode gtpp
    associate accounting-policy acctpolicy4g
    accounting context aaa gtpp group gtpp4g
  #exit

  context lbo-gi
    ip access-list acl-lbo-flow
      redirect css service acs1 any
    #exit
    ipv6 access-list acl-lbo-flow
      redirect css service acs1 any
    #exit
```

```
    ip pool lbo-pool-1 12.0.0.0 255.255.255.252 public 0 policy allow-static-allocation
subscriber-gw-address 12.0.0.2
    ipv6 pool pool_ipv6 prefix 1:2:3:5:5:6:7:9/48 public 0 policy allow-static-allocation
    interface ISP
      ip address 192.168.200.1 255.255.255.0
      ipv6 address bbbb::1/64 secondary
    #exit
    subscriber default
    exit
    aaa group default
    #exit
    gtpp group default
    #exit
```

Configuring DSCP Marking by SaMOG

The following is a sample configuration for SaMOG to mark DSCP values:

```
config
    qci-qos-mapping qci_qos_map_name
        qci qci_value_1 downlink encaps-header copy-inner
        qci qci_value_1 uplink encaps-header copy-inner
        qci qci_value_1 downlink encaps-header copy-outer
        qci qci_value_1 uplink encaps-header copy-outer
        qci qci_value_2 downlink encaps-header dscp-marking value1
        qci qci_value_2 uplink encaps-header dscp-marking value2
end

config
    apn-profile profile-name
      associate qci-qos-mapping qci_qos_map_name
        end

config
    context context_name
        cgw-service service_name
          associate qci-qos-mapping qci_qos_map_name
            end
```

Important The DSCP marking configuration under the APN Profile Configuration Mode takes priority over the DSCP marking configuration under the CGW Service Configuration Mode.

Configuring DSCP Marking by ECS

The following is a sample configuration for the AAA server to send a rulebase in the Access-Accept/CoA message. The APN profile can also be configured with the rulebase with DSCP marking as **ef** (expedite forwarding) in both uplink and downlink traffic:

```
rulebase rulebase_name
   action priority action_priority ruledef ruledef_name charging-action charging_action_name


ruledef ruledef_name
    ip any-match = TRUE

charging-action charging_action_name
    content-id id
```

```
    ip tos ef uplink
    ip tos ef downlink
```

Configuring SaMOG to act as the RADIUS Accounting Client

The following is a sample configuration to enable SaMOG to act as the RADIUS accounting client:

```
call-control-profile call_control_profile_name
    accounting mode radius-diameter
    associate accounting-policy accounting_policy_name
    accounting context aaa aaa-group aaa_group_name
    authenticate context aaa aaa-group aaa_group_name auth-type radius auth-method eap
non-eap
    exit

aaa group accounting_policy_name
    radius attribute nas-ip-address address ip_address
    radius dictionary custom71
    radius accounting server ip_address key key port port_number
    radius accounting interim interval interim_interval
    radius accounting interim volume total interim_volume
    exit

    policy accounting accounting_policy_name
        cc profile 2 interval interval
        cc profile 2 volume total total
        cc profile 8 interval interval
        cc profile 8 volume total total
    exit
```

Monitoring and Troubleshooting

RADIUS-based Web Authorization with LBO Basic Show Command(s) and/or Outputs

show subscriber samog-only full

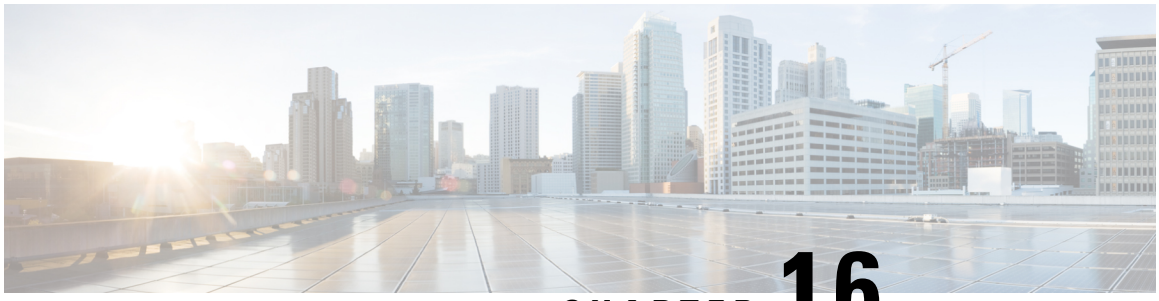
The following field is available in the output of the **show subscriber samog-only full** command in support of this feature:

```
CGW Subscriber Info:
---------------------
   QCI                 : 9
```

Table 44: show subscriber samog-only full Command Output Descriptions

Field	Description
CGW Subscriber Info	
QCI	Subscriber's QCI value.

show subscriber samog-only full

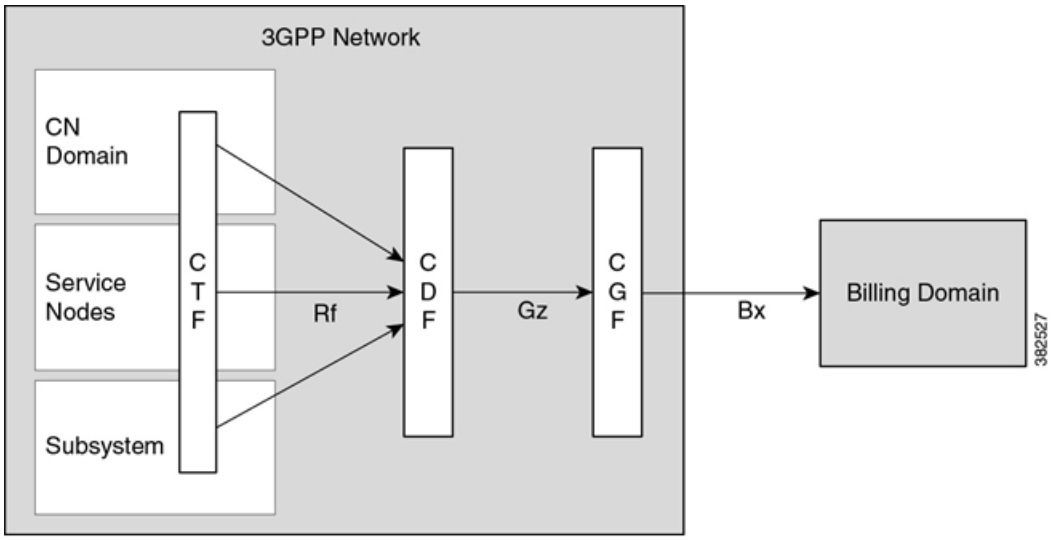


CHAPTER 16

SaMOG Gateway Offline Charging

The SaMOG Gateway supports generation of CDR files for offline charging. In Offline Charging, charging information is collected concurrently with resource usage and passed through a chain of logical charging functions. At the end of the process, CDR files are generated by the network and transferred to the network operator's Billing Domain.

Figure 26: 3GPP Offline Charging Architecture



The Charging Trigger Function (CTF) generates charging events and forwards them to the Charging Data Function (CDF). The CDF then generates CDRs and transfers it to the Charging Gateway Function (CGF). Finally, the CGF create CDR files and forwards them to the Billing Domain.

The SaMOG Gateway integrates with the CTF and CDF functions, generates CDRs based on the triggered events, and sends the same to the CGF over the Gz/Wz interface (using the GTPP protocol).

- SaMOG CDR Formats, on page 200
- Triggers for Generation of Charging Records, on page 209
- Configuring the SaMOG CDRs, on page 209

SaMOG CDR Formats

As 3GPP specifications does not define a CDR format for SaMOG, the S-GW CDR and SGSN CDR record formats are used to define the CDR formats. The record format can be selected using a CLI command under the GTPP Group Configuration Mode. By default, for an SaMOG general license, the S-GW record type is used, and for an SaMOG 3G license, the SGSN (SGSNPDPRecord) record type is used.

This section provides a reference for the S-GW and SGSN CDR fields supported by SaMOG.

The category column in all tables use keys described in the following table.

Table 45: Dictionary Table Key

Abbreviation	Meaning	Description
M	Mandatory	A field that must be present in the CDR.
C	Conditional	A field that must be present in the CDR if certain conditions are met.
OM	Operator Provisionable: Mandatory	A field that an operator has provisioned and must be included in the CDR for all conditions.
OC	Operator Provisionable: Conditional	A field that an operator has provisioned that must included in the CDR if certain conditions are met.

SaMOG S-GW CDR Format

The following table lists the S-GW CDR fields present in the available GTPP dictionary used by the SaMOG Gateway.

Table 46: SaMOG S-GW CDR Format

Field	Category	Description
Record Type	M	S-GW IP CAN bearer record. Set to S-GW record type.
Served IMSI	M	IMSI of the served party. Received in User name Radius AVP from WLC.
S-GW Address used	M	The control plane IP address of the S-GW used. CGW service IP address.

Field	Category	Description
PDN Connection Charging ID	OM	Charging ID of the EPS default bearer in GTP case. Set to befault bearer charging ID. SaMOG only supports default bearer setup. Therefore, the PDN connection charging ID and charging ID will be the same.
TWAN User Location Information	OC	UE location in a Trusted WLAN Access Network (TWAN) (SSID, and if available, BSSID of the access point), as defined in TS 29.274 [210] on an S2a GTP interface. For more information, refer **gtpp attribute twanuli** and **samog-cdr twanuli ap-group-name** commands under *Configuring the SaMOG CDRs* section of this chapter.
Charging ID	M	IP CAN bearer identifier used to identify this IP CAN bearer in different records created by PCNs. Provided by P-GW during Create session response.
Serving Node Address	OC	List of serving node control plane IP addresses (e.g. S-GW, SaMOG) used during record generation. MRME service IP address.
Serving Node IPv6 Address	OC	List of serving node control plane IPv6 addresses, in case of IPv4v6 dual stack used during record generation.
Serving Node Type	OC	List of serving node types in control plane.
PGW PLMN Identifier	OC	PLMN identifier (MCC MNC) of the P-GW used. Received in the APN OI part in PBU. For SaMOG 3G license, it will be set to GGSN PLMN ID.

Field	Category	Description
Access Point Name Network Identifier	OM	Logical name of the connected access point to the external Packet Data Network (network identifier part of APN). Received in Service Selection AVP in DER from AAA. If this field is not received in the DER, the session goes down.
PDP/PDN Type	OM	This field indicates PDN type (i.e IPv4, IPv6 or IPv4v6). Set to IPv4, IPv6, or IPv4v6. Received from AAA in DEA.
Served PDP/PDN Address	OC	IP address allocated for the PDP context/PDN connection, i.e. IPv4 or IPv6, if available. Allocated IP address.
Served PDP/PDN Address Extension	OC	IPv4 address of the served IMSI, if available, when PDN type is IPv4v6.
Dynamic Address Flag	OC	Indicates whether served PDP/PDN address is dynamic. This field will always set, as static address is not supported.
Dynamic Address Flag Extension	OC	Indicates whether the served IPv4 PDP/PDN address allocated during IP CAN bearer activation, initial attach (E-UTRAN or over S2x) and UE requested PDN connectivity with PDP/PDN type IPv4v6 is dynamic. This field will not be available if IPv4 address is static.
List of Traffic Data Volumes	OM	List of changes in charging conditions for IP CAN bearer, categorized based on traffic volumes/per traffic period or changed QoS. Generated by the SaMOG Gateway.

Field	Category	Description
Record Opening Time	M	Time stamp when IP CAN bearer is activated in S-GW, or record opening time on subsequent partial records. Generated by the SaMOG Gateway.
Duration	M	Duration of this record in the S-GW.
Cause for Record Closing	M	The reason for the release of record from S-GW. **Values:** • normalRelease • abnormalRelease • volumeLimit • timeLimit • maxChangeCond • managementIntervention
Diagnostics	OM	A more detailed reason for the release of the connection.
Record Sequence Number	C	Partial record sequence number, only present in case of partial records. A running sequence number with range of 1 through 4294967295 used to link partial records generated by the SaMOG for a specific bearer context (characterized with the same Charging ID and SaMOG address pair). This field will not be present if the first record is also the final record.
Node ID	OM	Name of the recording entity. This field contains an identifier string for the node that generates the CDR. On the SaMOG Gateway, the NodeID field is a printable string of the ndddSTRING format.

Field	Category	Description
Local Record Sequence Number	OM	Consecutive record number created by the node. The number is allocated sequentially including all CDR types. For each Node ID, the number with range 1 through 4294967295 is allocated sequentially for each CDR.
APN Selection Mode	OM	An index indicating how the APN was selected. Set to 0:MS or network provided APN, subscriber verified.
Served MSISDN	OM	The primary MSISDN of the subscriber. Received in the Subscription-ID AVP in DEA.
Charging Characteristics	M	The Charging Characteristics applied to the IP CAN bearer. Will be received from AAA in DEA 3GPP-Charging-Characteristics.
Charging Characteristics Selection Mode	OM	Holds information about how Charging Characteristics were selected. **Values:** • ServingNodeSupplied • homeDefault • roamingDefault • visitingDefault
P-GW Address Used	OC	P-GW IP address for the Control Plane The P-GW address received from the AVP MIP6-Agent-Info in DEA. If this value is not received, MRME performs DNS.
Serving Node PLMN Identifier	OC	Serving node PLMN Identifier (MCC and MNC) used during this record, if available. Received in NAI in Radius Access request.

Field	Category	Description
RAT Type	OC	Radio Access Technology (RAT) type currently used by the Mobile Station, when available. Set to WLAN.
Start Time	OC	Time when User IP-CAN session starts, available in the CDR for the first bearer in an IP-CAN session. Set by the SaMOG Gateway.
Stop Time	OC	Time when User IP-CAN session is terminated, available in the CDR for the last bearer in an IP-CAN session. Set by the SaMOG Gateway.

SaMOG SGSN CDR Format

The following table lists the SGSN (SGSNPDPRecord) CDR fields present in the available GTPP dictionary used by the SaMOG Gateway.

Table 47: SaMOG SGSN CDR Format

Field	Category	Description
Record Type	M	SGSN IP CAN bearer record. Set to SGSN record type.
Served IMSI	C	IMSI of the served party, if available. Received in User name Radius AVP from WLC.
SGSN Address used	OM	The IP address of the current SGSN. CGW service IP address.
Charging ID	M	IP CAN bearer identifier used to identify this IP CAN bearer in different records created by PCNs. Provided by GGSN in Create PDP context response.

Field	Category	Description
GGSN Address Used	M	The control plane IP addresses of the P-GW currently used. Set to GGSN address where PDP is context is created.
Access Point Name Network Identifier	OM	Logical name of the connected access point to the external Packet Data Network (network identifier part of APN). Received in Service Selection AVP in DER from AAA. If this field is not received in the DER, the session goes down.
PDP Type	OM	This field indicates PDN type (i.e IPv4, IPv6, IPv4v6, PPP, IHOSS:OSP). Set to IPv4.
Served PDP Address	OC	PDP address of the served IMSI, i.e. IPv4 address when PDP Type is IPv4, or IPv6 prefix when PDP Type is IPv6 or IPv4v6 Allocated UE IP address by GGSN.
List of Traffic Data Volumes	OM	List of changes in charging conditions for current IP CAN bearer, categorized based on traffic volumes/per traffic period, or initial and subsequently changed QoS. Set by the SaMOG Gateway.
Record Opening Time	M	Time stamp when IP CAN bearer is activated in the current SGSN, or record opening time on subsequent partial records. Set by the SaMOG Gateway.
Duration	M	Duration of current record in the SGSN. Set by the SaMOG Gateway.

Field	Category	Description
Cause for Record Closing	M	The reason for the release of record from current SGSN. **Values:** • normalRelease • abnormalRelease • volumeLimit • timeLimit • maxChangeCond • managementIntervention
Diagnostics	OM	A more detailed reason for the release of the connection.
Record Sequence Number	C	Partial record sequence number in the current SGSN, only present in case of partial records. A running sequence number with range of 1 through 4294967295 used to link partial records generated by the SaMOG for a specific bearer context (characterized with the same Charging ID and SaMOG address pair). This field will not be present if the first record is also the final record.
Node ID	OM	Name of the recording entity. This field contains an identifier string for the node that generates the CDR. On the SaMOG Gateway, the NodeID field is a printable string of the ndddSTRING format.
Record Extensions	OC	Set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.

Field	Category	Description
Local Record Sequence Number	OM	Consecutive record number created by the current node. The number is allocated sequentially including all CDR types. For each Node ID, the number with range from1 through 4294967295 is allocated sequentially for each CDR.
APN Selection Mode	OM	An index indicating how the APN was selected. Set to 0:MS or network provided APN, subscriber verified.
Access Point Name Operator Identifier	OM	The Operator Identifier part of the APN.
Served MSISDN	OM	The primary MSISDN of the subscriber. Received in the Subscription-ID AVP in DEA.
Charging Characteristics	M	The Charging Characteristics applied to the IP CAN bearer. Will be received from AAA in DEA 3GPP-Charging-Characteristics.
RAT Type	OC	Radio Access Technology (RAT) type currently used by the Mobile Station as defined TS 29.061 [205], when available. Set to WLAN.
Charging Characteristics Selection Mode	OM	Holds information about how Charging Characteristics were selected. **Values:** • AAASupplied • homeDefault • roamingDefault • visitingDefault

Field	Category	Description
Dynamic Address Flag	OC	Indicates whether the served PDP address that is allocated during IP CAN bearer activation, is dynamic. This field will not be available if the address is static. Always set.

Triggers for Generation of Charging Records

The following section describes the triggers for the generation of partial and final SaMOG CDRs.

SaMOG CDRs are updated (not closed) for any of the following conditions:

- QoS Change: When a QoS change is detected, the "List of Traffic Data Volumes" is added to the CDR.
- Tarrif Time Change: When the tarrif time changes, the "List of Traffic Data Volumes" is added to the CDR.
- CDR Closure: The "List of Traffic Data Volumes" is added to the CDR when this event occurs.

The "List of Traffic Volumes" attribute in the SaMOG CDR consists of a set of containers that are added when specific trigger conditions are met. The volume count per IP CAN bearer is also identified and separated for uplink and downlink traffic when the trigger condition occurs.

The SAMOG CDRs are closed as the final record for a subscriber session for the following events:

- End of IP-CAN bearer: The CDR is closed when the IP-CAN bearer is deactivated. The trigger condition includes:
  - UE detach
  - AAA detach
  - PGW/GGSN detach
  - any abnormal release
  - Admin clear

The following events trigger closure and sending of a partial SaMOG CDR:

- Volume Limit: The CDR is partially closed when the configured volume threshold is exceeded.
- Time Limit: The CDR is partially closed when the configured interval is reached.
- Maximum number of charging condition changes: The CDR is partially closed when the LOTV container exceeds its limit.
- Management intervention

Configuring the SaMOG CDRs

The SaMOG Gateway uses the custom24 GTPP dictionary to generate SGW and SGSN CDRs.

The following table lists the configuration commands related to creating and formatting the CDRs. These commands appear at different portions of the system configuration file.

- **gttp group** <*name*> - These are commands specified within the billing context.

Table 48: CDR Configuration Parameters

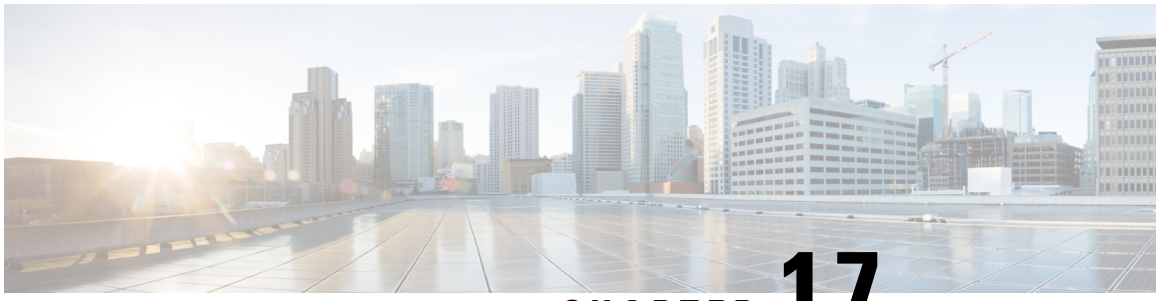
Command	Default	Comment
Trigger-related Configuration **gttp group<*name*>** in Billing Context		
gtpp trigger volume-limit	Enabled	When this trigger is disabled, no partial record closure occurs when the volume limit is reached.
gtpp trigger time-limit	Enabled	When this trigger is disabled, no partial record closure occurs when the configured time limit is reached.
gtpp trigger tariff-time-change	Enabled	When this trigger is disabled, container closure does not occur for a tariff-time change.
gtpp trigger qos-change	Enabled	Disabling this trigger ignores a qos-change and does not open a new CDR for it.
CDR Attribute-related Configuration		
gtpp attribute diagnostics	No	Includes the Diagnostic field in the CDR that is created when PDP contexts are released.
gtpp attribute duration-ms	No	Specifying this option results in mandatory "Duration" field in the CDR to be recorded in milliseconds rather than seconds.
gtpp attribute local-record-sequence-number	No	Specifying this option includes optional fields "Local Record Sequence Number" and "Node-ID" in the CDR. Since the "Local Record Sequence Number" has to be unique within one node (identified by "Node-ID"), "Node-ID" field will consist of sessMgr Recovery count + AAA Manager identifier + the name of the GSN service. Since each AAA Manager generate S-CDRs independently, the "Local Record Sequence Number" and "Node ID" fields will uniquely identify a CDR.

Command	Default	Comment
gtpp attribute msisdn	Enabled	Specifying this option includes field "MSISDN" in the CDR.
gtpp attribute node-id-suffix <*string*>	No String between 1 and 16 characters	Specifies the string suffix to use in the NodeID field of S- CDRs. With the default setting of "no", the SaMOG Gateway uses the GTPP context name for the Node ID field.
gtpp attribute record-type {sgwrecord | sgsnpdprecord }	No	If not explicitly configured, the record type selection is based on the SaMOG license used.
gtpp attribute twanuli	Disabled	Specifying this option includes the "TWAN User Location Information" in the S-GW CDRs. **Important** SaMOG services and standalone S-GW services must not share a GTTP group that has the **gtpp attribute twanuli** command configured. Instead, configure the command under different GTPP groups for each service.
Policy Accounting in Source Context		
cc profile <*index*> **buckets** <*number*>	index = 0-15 number = 4	Specifies the number of traffic volume container changes due to QoS changes or tariff time that can occur before an accounting record is closed.
cc profile <*index*> **interval** <*seconds*>	No	Specifies the normal time duration that must elapse before an accounting record is closed.

Command	Default	Comment
cc profile <*index*> **volume { downlink** <*vol_down_octets*> **uplink** <*vol-up_octets*> **| total** <*total_octets*> **}**	No	Specifies the downlink, uplink, and total volumes that must be met before closing an accounting record. • vol_down_octets is measured in octets and can be configured to any integer value from 100,000 to 4,000,000,000. • vol_up_octets is measured in octets and can be configured to any integer value from 100,000 to 4,000,000,000. • total_octets is the total traffic volume (up and downlink) measured in octets and can be configured to any integer value from 100,000 to 4,000,000,000.
cc profile <*index*> **tariff time1** *mins hours* **time2** *mins hours* **time3** *mins hours* **time4** *mins hours*	No	Specifies time-of-day time values to close the current traffic volume container (but not necessarily the accounting record). Four different tariff times may be specified. If less than four times are required, the same time can be specified multiple times.
Show Commands		
show gtpp counters	None	Displays GTPP counters for configured charging gateway functions (CGFs) within the given context.
show gtpp statistics	None	Displays GTPP statistics for configured CGFs within the context.
show gtpp storage-server counters	None	Displays counters pertaining to the configured GTPP storage server.
show gtpp storage-server statistics	None	Displays statistics pertaining to the configured GTPP storage server.
show gtpp group	None	Displays information pertaining to the configured GTPP storage server group.

Command	Default	Comment
Global Configuration Commands		
gtpp single-source	None	Configures the system to reserve a CPU for performing a proxy function for GTPP accounting. This command is mandatory for dispatching S-CDR. If not specified during bootup, the S-GW CDRs will be generated and buffered in the AAAMgr but not sent out. This is as similar to charging not being done. The maximum number of CDRs which will be buffered in AAAMgr is 128 MB (by size) or 26400 CDRs (by count), whichever comes first.
Call Control Profile Configuration		
accounting mode gtpp	gtpp Enabled	Enable this command to generate the bearer based SaMOG CDRs.
accounting context <*context*> **[gtpp group** <*group*> **]**	GTPP group Default	If GTPP group is not configured, the default value is used. If the accounting context is not configured, SaMOG service context is used.
cc { behavior-bit no-records *bit_value* **| local-value behavior** *bit_value* **profile index_bit** | *prefer { hlr-hss-value | local-value } }* **no cc behavior-bit no-records** remove cc { behavior-bit no-records | local-value | prefer }	None Enabled	Specifies how the Charging Characteristics should be selected in SaMOG. This command defines the charging characteristics to be applied for CDR generation when the handling rules are applied via. the Operator Policy feature.
associate accounting-policy <*name*>	Not associated	The accounting policy configured various SGW-CDR triggers for the CC profiles. If no policy is configured then triggers based on CC will not be generated and the Accounting policy in SaMOG service context is used.

Command	Default	Comment
samog-cdr twanuli ap-group-name **no samog-cdr twanuli ap-group-name**	SSID	Enable this command to send the AP Group Name in the SSID field of tWANUserLocationInformation in the S-GW CDR. To enable the SaMOG Gateway to send the TWAN ULI attribute in the GTPP requests, use the **gtpp attribute twanuli** command under the GTPP Group Configuration Mode. By default, when the **gtpp attribute twanuli** command is enabled and **samog-cdr twanuli ap-group-name** command is not configured, the SaMOG Gateway sends the SSID information in the TWANUserLocationInformation attribute.
APN Profile Configuration		
accounting mode gtpp	gtpp	Enable this command to generate the bearer based SaMOG CDRs. If not configured, the configuration under the CC profile is used.
accounting context <*context*> **[gtpp group** <*group*> **]**	GTPP group Default	If this command is not configured, the configuration under the CC profile is used.
associate accounting-policy <*name*>	Not associated	If this command is not configured, the configuration under the CC profile is used.



CHAPTER 17

SaMOG Inter-Chassis Session Recovery

This chapter describes the license-enabled inter-chassis session recovery feature on the SaMOG gateway.

Feature Description

SaMOG is capable of providing chassis-level and geographic-level redundancy and can recover fully created sessions in the event of a chassis failure.

The Cisco ASR 5x00 and virtualized platforms provide industry leading carrier class redundancy. The systems protects against all single points of failure (hardware and software) and attempts to recover to an operat ional state when multiple simultaneous failures occur.

The system provides several levels of system redundancy:

- Under normal N+1 packet processing card hardware redundancy, if a catastrophic packet processing card failure occurs all affected calls are migrated to the standby packet processing card if possible. Calls which cannot be migrated are gracefully terminated with proper call-termination signaling and accounting records are generated with statistics accurate to the last internal checkpoint.
- If the Session Recovery feature is enabled, any total packet processing card failure will cause a packet processing card switchover and all established sessions for supported call-types are recovered without any loss of session.

Even though Cisco provides excellent intra-chassis redundancy with these two schemes, certain catastrophic failures which can cause total chassis outages, such as IP routing failures, line-cuts, loss of power, or physical destruction of the chassis, cannot be protected by this scheme. In such cases, the SaMOG Inter-Chassis Session Recovery (ICSR) feature provides geographic redundancy between sites. This has the benefit of not only providing enhanced subscriber experience even during catastrophic outages, but can also protect other systems such as the RAN from subscriber reactivation storms.

ICSR allows for continuous call processing without interrupting subscriber services. This is accomplished through the use of redundant chassis. The chassis are configured as primary and backup with one being active and one in recovery mode. A checkpoint duration timer is used to control when subscriber data is sent from the active chassis to the inactive chassis. If the active chassis handling the call traffic goes out of service, the inactive chassis transitions to the active state and continues processing the call traffic without interrupting the subscriber session. The chassis determines which is active through a propriety TCP-based connection called a redundancy link. This link is used to exchange Hello messages between the primary and backup chassis and must be maintained for proper system operation.

How It Works

Inter-chassis Communication

Chassis configured to support ICSR communicate using periodic Hello messages. These messages are sent by each chassis to notify the peer of its current state. The Hello message contains information about the chassis such as its configuration and priority. A dead interval is used to set a time limit for a Hello message to be received from the chassis' peer. If the standby chassis does not receive a Hello message from the active chassis within the dead interval, the standby chassis transitions to the active state. In situations where the redundancy link goes out of service, a priority scheme is used to determine which chassis processes the session. The following priority scheme is used:

- route modifier
- chassis priority
- SPIO MAC address

Checkpoint Messages

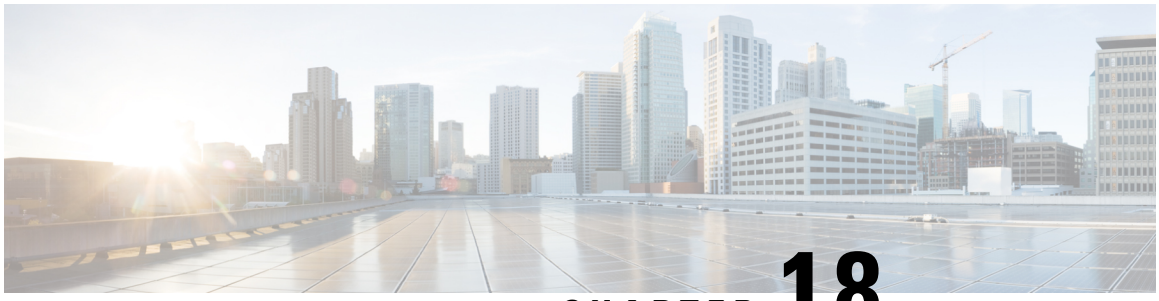
Checkpoint messages are sent from the active chassis to the inactive chassis at specific intervals and contain all the information needed to recreate the sessions on the standby chassis, if that chassis were to become active. Once a session exceeds the checkpoint duration, checkpoint data is collected on the session. The checkpoint parameter determines the amount of time a session must be active before it is included in the checkpoint message.

Important For more information on inter-chassis session recovery support, refer to the *Interchassis Session Recovery* chapter in the *System Administration Guide*.

Limitations

This section identifies limitations, restrictions, and dependencies for the SaMOG ICSR feature:

- In this release, ICSR support is available only for the following sessions types:
  - PMIPv6 access-type and GTPv2 network type sessions with DIAMETER-based authentication.
  - EoGRE access-type and GTPv2 network type sessions with DIAMETER-based authentication.
- ICSR support is not available for recovering CDR information and SaMOG Local Breakout (LBO) sessions (flow-based and LBO Basic).
- ICSR support is not available for multiple SaMOG services configuration.



CHAPTER 18

SaMOG Local Break Out

The SaMOG Local Breakout (LBO) feature enables subscribers to access the Internet without connecting to the EPC or 3G core. SaMOG currently supports the following LBO models:

- Local Breakout - Enhanced, on page 217
- Local Breakout - Basic, on page 225
- Flow-based Local Breakout, on page 228

Local Breakout - Enhanced

The Local Breakout (LBO) - Enhanced model is implemented by configuring a local P-GW or a local GGSN. All subscribers of a particular APN will be locally broken out without connecting to the P-GW or GGSN over the S2a interface. SaMOG performs IP allocation locally. This capability helps APNs whose data traffic can connect to the Internet immediately after authentication, instead of being sent to the 3GPP backbone.

License Requirements

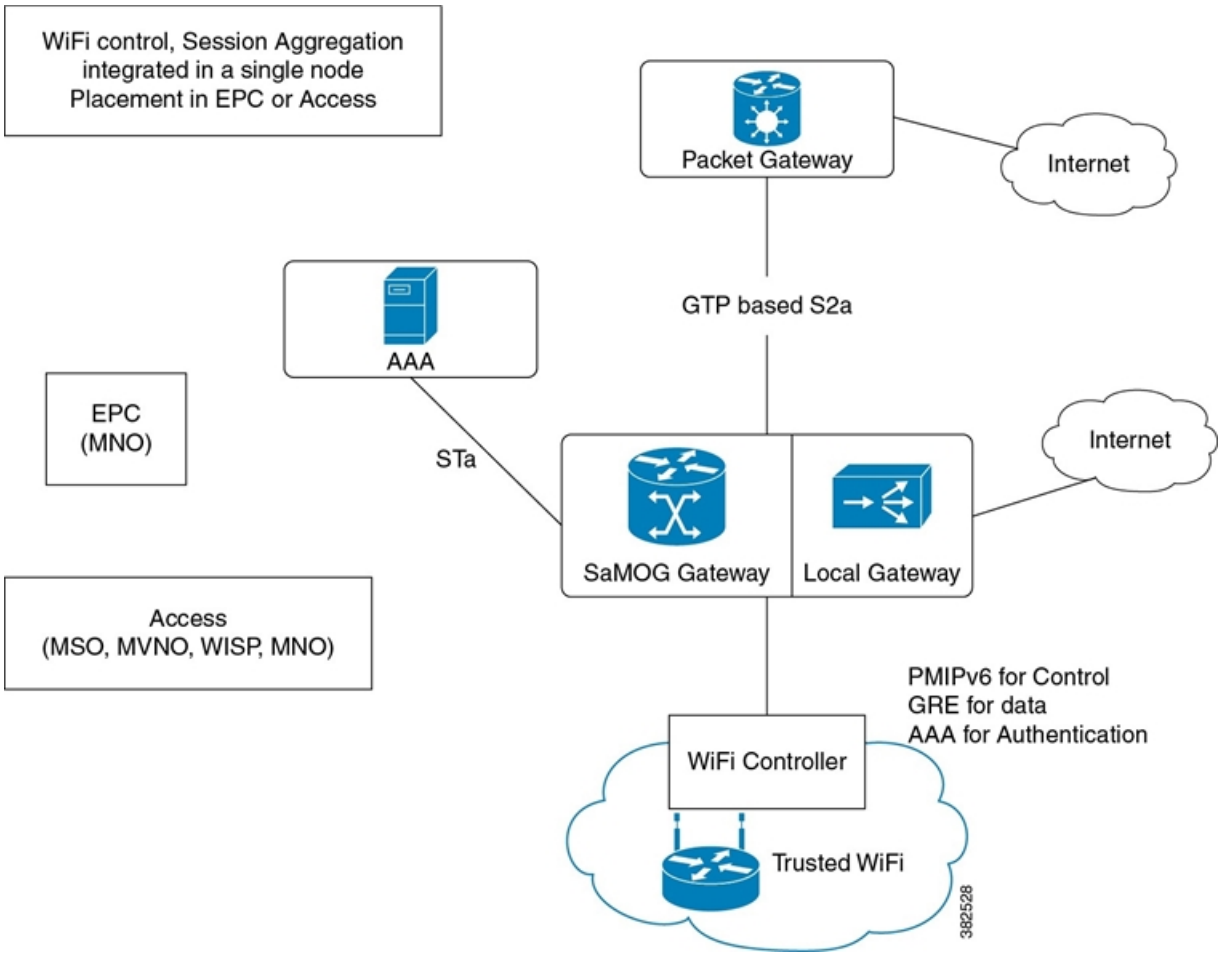
The Local Breakout - Enhanced model requires a separate LBO - Enhanced feature license. This license is mutually exclusive with the LBO - Basic and Flow-based LBO licenses.

SaMOG 3G license: Only a GGSN service can be configured and associated with the CGW service.

SaMOG general license: Either a GGSN service or a P-GW service can be configured and associated with the CGW service.

Overview

The following figure provides a high level architecture of the Local Breakout feature:



The APN provided by the AAA server is mapped to the locally configured P-GW or GGSN service IP. This eliminates the need for a DNS. The local P-GW or local GGSN assigns the IP using a locally configured IP pool after receiving the subscriber information from the AAA server. The subscriber information is received from the SaMOG service to the local P-GW service or local GGSN service through a GTP tunnel. This tunnel is set up within the same chassis.

The SaMOG Gateway decides whether an APN should be locally broken out based on the following parameters:

- A configuration in the APN profile indicating if LBO is enabled for the APN.
- Whether a "DEA-Flags" is received in the DEA messages on the STa interface. If DEA-Flags are received, SaMOG will verify if the "NSWO-Authorization" flag is set.

If the APN profile is configured for LBO, and either no "DEA-Flags" are received in the DEA messages, or "DEA-Flags" is received with the "NSWO-Authorization" flag set, SaMOG performs LBO for that APN.

LBO Decision based on AAA Policy and Local Policy

The decision on whether LBO can be done for a call is based on the following factors:

- A DIAMETER-based server can provide the following information:

- The MIP6_FEATURE_VECTOR AVP in DEA message can have the GTPV2_SUPPORTED flag set to indicate that the AAA server authorizes the GTP call through the EPC core (GGSN/PGW).
- The Bit 0 of the DEA_FLAG AVP (NSWO Authorization) is set to indicate that LBO is authorized for a session by the AAA server.

- The DIAMETER AAA server sends the APN information in the APN-Configuration AVP in DEA. This AVP may however be absent in case the AAA server authorizes only LBO, to indicate that any APN can be used for LBO for the subscriber.
- The operator can configure "local-offload" for each APN supporting LBO under the APN profile. However, the authorization from the AAA server will always be given preference over the local configuration. Local configuration will be used to take a decision when AAA server authorizes GTP as well as LBO for a call.

The following table indicates different scenarios where the occurance of LBO is determined:

AAA Indication	APN Received	Matching APN with LBO in the Local Configuration	LBO/GTP Call Decision
Both GTP and LBO NOT supported	—	—	Always an error condition
Only GTP Supported	No	—	Error Condition
	Yes	—	GTP Call setup with GGSN/P-GW
Only LBO Supported	No	Yes	LBO session established with the first APN with "local-offload" configured in local policy.
	No	No APN configured in local policy	Error Condition
	Yes	No	Error Condition
	Yes	Yes	LBO session established with received APN.
Both GTP and LBO Supported	No	—	Error Condition
	Yes	No	GTP session established with received APN.
	Yes	Yes	LBO session established with received APN.

Prepaid LBO Support

The SaMOG Gateway also supports Local Breakout (LBO) that enables time- and quota-based control to support prepaid subscribers. SaMOG interfaces with the Enhanced Charging Services (ECS) using the Gy interface for prepaid subscribers, and AAA for voucher-based subscribers. LBO for prepaid subscribers is supported on both PMIPv6 and EoGRE access types.

When a GTP session with the local P-GW or GGSN is set up, the local P-GW or GGSN service communicates with ECS to obtain the time and quota limits of the subscriber to establish connection. The time and quota limits are obtained with the Gy interface forwarding the CCR-I message to the Diameter Credit Control Application (DCCA) server. Until the time or volume quota is reached, the local P-GW or GGSN forwards the CCR-U message to DCCA in order to refresh the permitted time or volume quota allowed. When the UE terminates the session, the internal P-GW forwards the final service usage to ECS, and SaMOG completes the session.

Call Flows with Local Breakout - Enhanced

Attach Procedure

Figure 27: Attach Procedure Call Flow

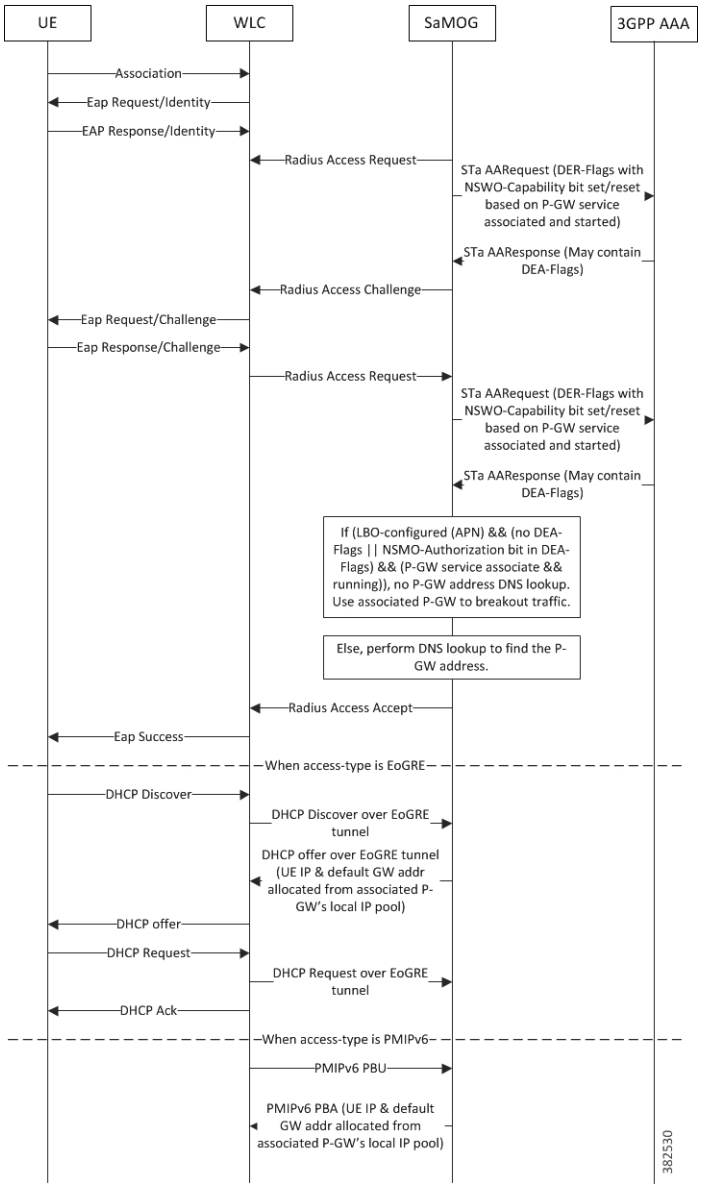


Table 49: Attach Procedure Call Flow Descriptions

Step	Description
1	UE associates with AP and WLC.
2	WLC starts EAP based authentication with UE and requests for the permanent identity of the user.
3	UE responds with the permanent identity (IMSI) stored on the SIM.
4	WLC requests SaMOG for authentication using Radius Access Request message.
5	SaMOG uses the STa interface towards 3GPP HSS to fetch subscriber authentication challenge. If LBO is enabled, SaMOG forwards DER-Flags (in the DER msg) with "NSWO-Capability" bit set to '1' to indicate to AAA that it supports LBO. Else, it sends the DER-Flags with "NSWO-Capability" bit set to '0'.
6	HSS returns the authentication parameters to SaMOG for the subscriber. The DEA message may contain DEA-Flags.
7	SaMOG sends Radius-Access-Challenge message to the WLC.
8	WLC in turn sends authentication challenge to UE.
9	UE responds with challenge response.
10	WLC initiates Radius Access Requests towards SaMOG with challenge response.
11	SaMOG originates STa AARequest towards HSS. If LBO is enabled, SaMOG sends DER-Flags (in the DER msg) with "NSWO-Capability" bit set to '1' to indicate to AAA that it supports LBO. Else, it sends the DER-Flags with "NSWO-Capability" bit set to '0'.
12	HSS authenticates the subscriber and also returns the subscriber profile information to MRME. The profile information will contain the Default QoS profile, Default APN, APN-AMBR, and Charging Characteristics.

Step	Description
13	If the APN profile requires LBO for the APN, either of the following conditions is met: • DEA-Flags not received • DEA-Flags received with the "NSWO-Authorization" bit set to 1. The P-GW service is then associated with the SaMOG service, and the associated P-GW IP address is used for LBO. Or, if a static IP address is provided by AAA, the address is used for allocation. If neither of the conditions above is met, DNS resolution is performed to determine the P-GW address.
14	SaMOG sends Radius-Access-Accept message towards WLC with some of the information mentioned in Step12 (APN Name, PDN-GW/LGW address).
15	EAP Success is sent to the UE.
16	For access-type EoGRE, UE sends DHCP Discover to SaMOG via. WLC. For access-type PIMP, WLC originates the PMIPv6 Proxy-Binding-Update message to SaMOG with the information from Step 13. Additionally, WLC allocates a GRE tunnel ID for downlink data transfer and includes it in PBU message.
17	For access-type EoGRE, the IP address allocated in Step 13 via. the associated P-GW is sent in the DHCP Offer msg. For access-type PIMPv6, the IP address allocated in Step 13 via. the associated P-GW is sent in the PBA message. The SaMOG service will setup the GRE tunnel and include the GRE tunnel ID for uplink data transfer.
18	For access-type EoGRE, the DHCP Request and DHCP Ack messages are forwarded to complete the IP address allocation. For access-type PMIPv6, WLC acts as DHCP server to the UE, and assigns the IP address received in PBA.

UE Initiated Detach

Figure 28: UE Initiated Detach Call Flow

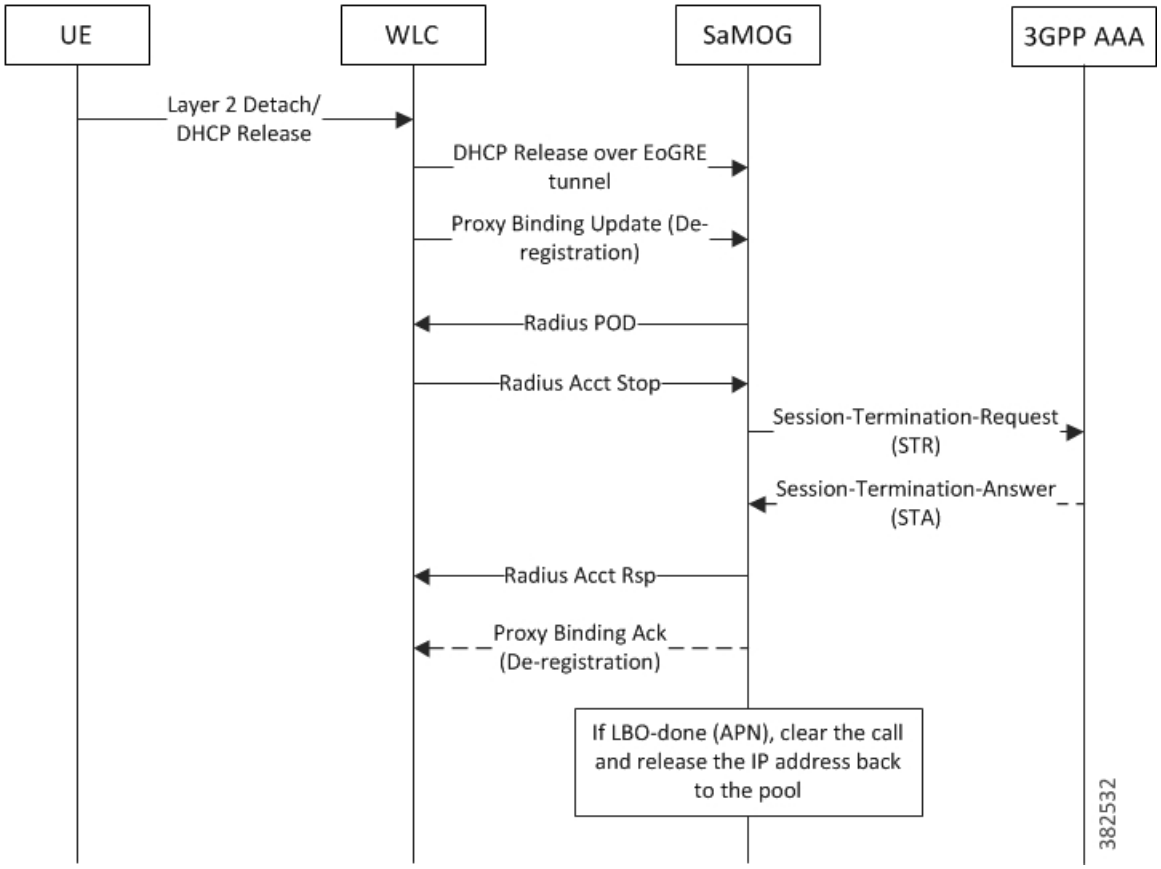


Table 50: UE Initiated Detach Call Flow Descriptions

Step	Description
1	UE initiates DHCP Release or L2 layer detach towards wireless network.
2	If access-type is EoGRE, UE sends a "DHCP Release" message to SaMOG. If the access-type is PMIPv6, WLC sends a PBU (De-registration) to SaMOG.
3	SaMOG sends a "Radius POD" to WLC.
4	WLC initiates Radius-Accounting-Stop message to SaMOG.
5-6	SaMOG in turn initiates STa Termination request to HSS, and receives a STa Termination response back from HSS.

Step	Description
7	SaMOG sends Radius-Accounting-Stop Response message to WLC.
8	For access-type PMIPv6, SaMOG sends back PMIPv6 Proxy Binding .
9	If the APN has been locally broken out, the allocated IP address is returned back to the P-GW IP pool. The session and associated IP-GRE/EoGRE tunnel is cleared.

AAA Initiated Detach

Figure 29: AAA Initiated Detach Call Flow

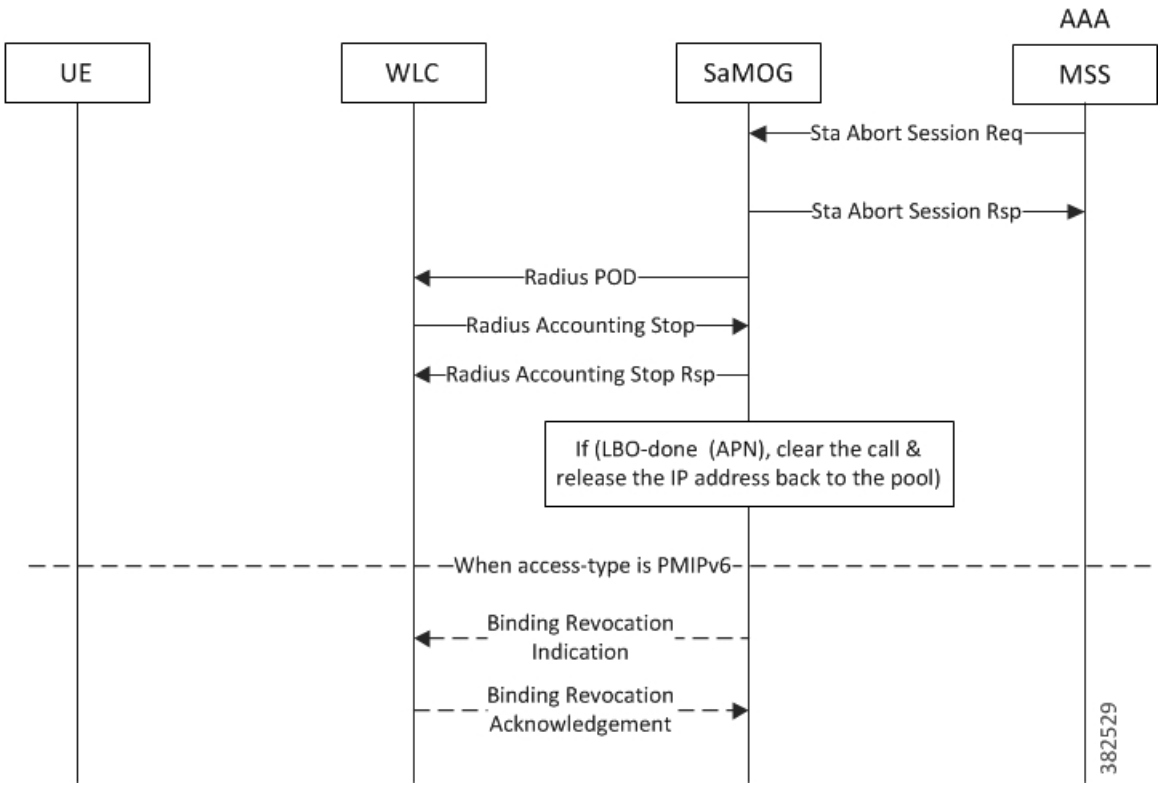


Table 51: AAA Initiated Detach Call Flow Descriptions

Step	Description
1	AAA sends STa Abort Session Req message to SaMOG.

Step	Description
2-3	SaMOG responds with an STa Abort Session Rsp message to AAA, and "Radius POD" message to WLC.
4	WLC initiates a Radius-Accounting-Stop Request message to SaMOG.
5	SaMOG sends Radius-Accounting-Stop Response message to WLC.
6	If the APN has been locally broken out, the allocated IP address is returned back to the P-GW IP pool. The session and associated IP-GRE/EoGRE tunnel is cleared.
7-8	If access-type is PMIPv6, SaMOG initiates a BRI message to WLC, and receives a BRA message back.

Limitations, Restrictions, and Dependancies

The following limitations, restrictions, and dependancies apply for the Local Breakout - Enhanced model:

- When an LBO session or GTP session is setup to an EPC/3G core, the mobility protocol or local breakout cannot be changed dynamically during reattach, even if the new authentication indicates the scope for such change. If the AAA server withdraws permission for the current mobility protocol/LBO, the session will be closed.
- In release 16.0, the Local Breakout feature supports 4G (GTPv2) sessions only.
- Prepaid support for Local Breakout feature using the AAA interface is limited to session-timeout AVP to control the session duration for voucher-based users. No additional support will be available on the AAA interface.
- For the LBO prepaid support, the SaMOG Gateway generates S-GW CDRs. Any packet drops on the interface P-GW service due to online credit control will still be counted in SGW-CDRs. However, operators can consider enabling P-GW CDRs in the internal P-GW as required.

Local Breakout - Basic

The Local Breakout (LBO) - Basic model enables SaMOG to connect the subscriber's User Equipment (UE) directly to the Internet without employing a local or external P-GW or GGSN service. The UE's IP address is allocated using an IP pool configured locally (or provided by the AAA server). The LBO basic model can be used with or without a Network Address Translation (NAT) service. If dynamic NAT is enabled for a subscriber, SaMOG allocates a global IP address from a pool, and replaces the source IP address of the data packet with this address.

License Requirements

The LBO - Basic model requires a separate feature license. This license is mutually exclusive with the LBO - Enhanced license, and can co-exist with the Flow-based LBO license.

Call Flows with Local Breakout - Basic

Local Breakout - Basic Session Setup

Figure 30: Local Breakout - Basic Session Setup Call Flow

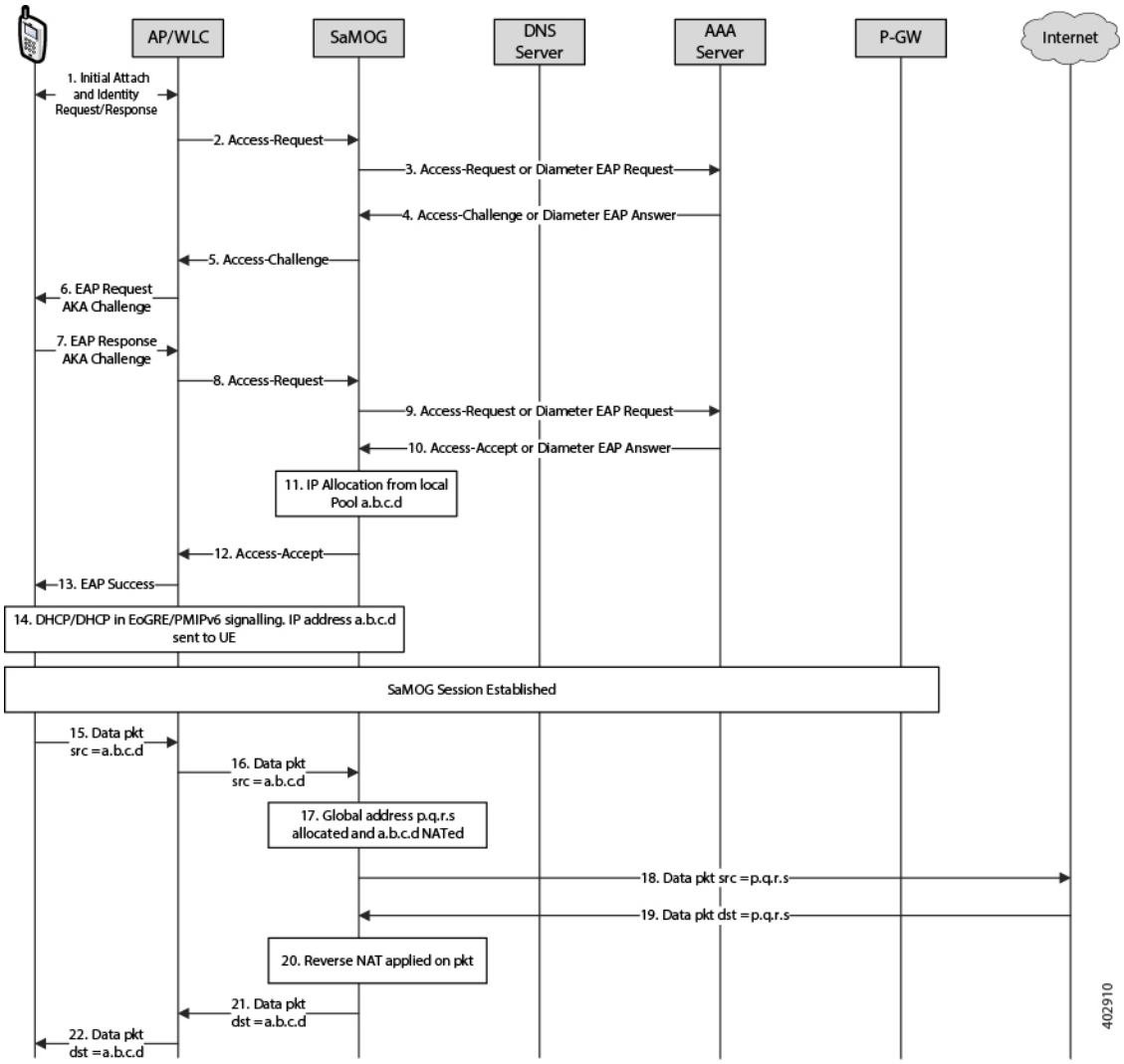


Table 52: Local Breakout - Basic Session Setup Call Flow Descriptions

Step	Description
1	UE initiates an initial attach procedure towards WLC.
2	WLC forms an Access-Request message with EAP-Identity payload, User-Name and Acct-Session-Id, and forwards the same to SaMOG.

Step	Description
3	SaMOG forms an Access-Request towards the RADIUS AAA server, or a Diameter EAP Request towards the STa AAA server using the attributes received from WLC.
4	AAA server performs EAP authentication and forwards the Access-Challenge/Diameter EAP Answer to SaMOG with the EAP payload.
5	SaMOG copies the EAP payload to the Access-Challenge towards WLC.
6	WLC forwards EAP Request with SIM Challenge towards UE.
7	UE sends EAP response with SIM Challenge response.
8	WLC sends Access-Request to SaMOG with EAP payload received from UE.
9	SaMOG sends Access-Request/Diameter EAP Request to AAA server with the EAP payload.
10	AAA server fetches the subscriber profile from HLR/HSS and validates the EAP Challenge response sent from UE. Access-Accept/Diameter EAP Answer is sent to SaMOG with user profile and EAP Success payload. SaMOG saves the user profile information. The AAA server authorizes local offload for the subscriber and the APN provided by AAA server has local-offload enabled.
11	SaMOG marks the session as an LBO - Basic candidate and allocates an IP address (a.b.c.d) from the local pool corresponding to the pool name received from AAA or configured under APN if the AAA server has not supplied any pool name.
12	SaMOG sends Access-Accept to the WLC with EAP-Success payload.
13	WLC forwards the EAP-Success to the UE.

Step	Description
14	DHCP or PMIPv6 messaging is then initiated to setup the data path. The UE IP address (a.b.c.d), DNS server address and default router address is supplied to the WLC/UE in DHCP or PMIPv6 (PBA) message. Once the WLC learns the UE IP address, it sends an Accounting-Start message containing the Framed-IP-Address attribute to SaMOG. SaMOG forwards it to the AAA accounting server, and the response from the accounting server is forwarded back to WLC.
15	Uplink data packet with the source IP address (a.b.c.d) is sent to WLC through the CAPWAP tunnel by UE.
16	WLC encapsulates the same packet into GRE/EoGRE tunnel or as L3IP, and sends it to SaMOG.
17	SaMOG performs dynamic NAT on this packet, allocates a global IP address from a pool (p.q.r.s), and replaces the source IP address of data packet with this address.
18	SaMOG routes the modified packet to the Internet.
19	The downlink packet contains the destination address set to p.q.r.s from the Internet to SaMOG.
20	SaMOG performs a reverse NAT, and replaces the address (a.b.c.d) as the destination address of the packet.
21	The modified packet is forwarded through the GRE/EoGRE tunnel or as L3IP to WLC.
22	WLC forwards the packet to the UE.

Important If NAT policy is not applied for the session (i.e. if ACLs are not provided, or if Rulebase is not provided, or if Rulebase doesn't contain NAT policy), the uplink data packets are directly offloaded to the Internet without NATting. and consequently reverse NAT is not applied for downlink packets from Internet, as NAT is not mandatory for LBO Basic.

Flow-based Local Breakout

The Flow-based Local Breakout (LBO) model enables SaMOG to selectively offload certain user data directly to the Internet without employing an external or internal P-GW or GGSN service, and forward the remaining traffic to an external P-GW or GGSN (via. the S2a tunnel) depending on configured Layer 4 rules. The User

Equipment's (UE) IP address is allocated by the external P-GW or GGSN service. SaMOG applies NAT addressing to all traffic that are offloaded directly to the Internet to differentiate between packets intended for local offload, and packets intended to be forwarded to P-GW or GGSN.

License Requirements

The Flow-based LBO model requires a separate feature license. This license is mutually exclusive with the LBO - Enhanced license, and can co-exist with the LBO - Basic license.

Flow-based LBO models

SaMOG applies Layer 4 rules to the data traffic using Access Control Lists (ACLs) to determine the part of traffic to be offloaded directly or sent to the P-GW or GGSN service. This decision can be based off an ACL whitelist or an ACL blacklist. While the ACL whitelist identifies the data to be forwarded to the P-GW or GGSN service, the ACL blacklist identifies the data to be locally offloaded.

Flow-based LBO using a Whitelist

A flow-based LBO using a whitelist is ideal in situations when a subscriber signs up for some premium content, and this content must be charged differently. SaMOG uses the ACL to route all traffic intended for the premium content server to be forwarded to P-GW or GGSN where special charging is applied using the Gx/Gy interface. SaMOG offloads the rest of the traffic that does not match the ACL directly to the Internet.

Flow-based LBO using a Blacklist

A flow-based LBO using blacklist is ideal in situations when SaMOG is deployed in a vicinity where a large number of subscribers access the same content (for example, a streaming video of an event in a stadium where the server is locally hosted). SaMOG offloads this content directly from the local server, and all other data traffic is routed to the P-GW or GGSN service.

Call Flows with Flow-based Local Breakout

Flow-based Local Breakout - Whitelist

Figure 31: Flow-based Local Breakout - Whitelist Call Flow

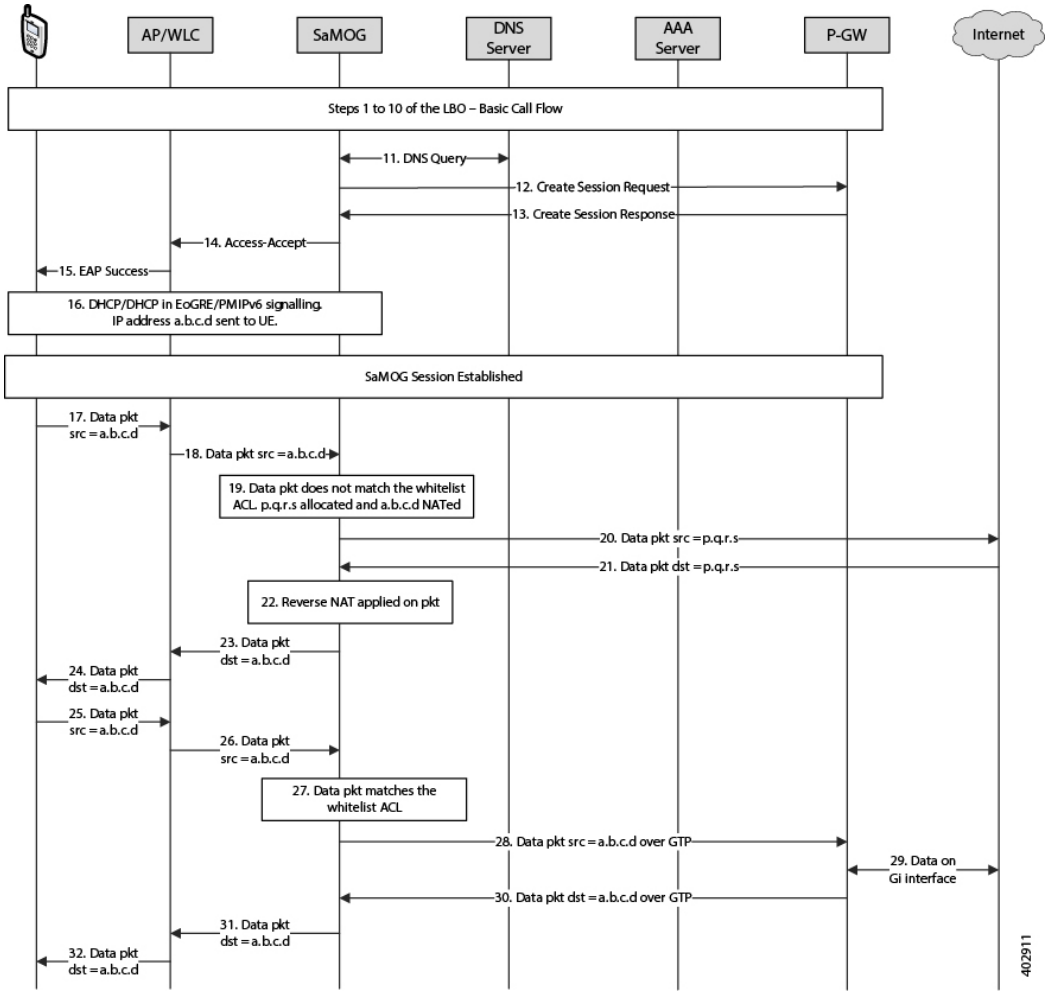


Table 53: Flow-based LBO - Whitelist Call Flow Descriptions

Step	Description
1	UE initiates an initial attach procedure towards WLC.
2	WLC forms an Access-Request message with EAP-Identity payload, User-Name and Acct-Session-Id, and forwards the same to SaMOG.
3	SaMOG forms an Access-Request towards the RADIUS AAA server, or a Diameter EAP Request towards the STa AAA server using the attributes received from WLC.

Step	Description
4	AAA server performs EAP authentication and forwards the Access-Challenge/Diameter EAP Answer to SaMOG with the EAP payload.
5	SaMOG copies the EAP payload to the Access-Challenge towards WLC.
6	WLC forwards EAP Request with SIM Challenge towards UE.
7	UE sends EAP response with SIM Challenge response.
8	WLC sends Access-Request to SaMOG with EAP payload received from UE.
9	SaMOG sends Access-Request/Diameter EAP Request to AAA server with the EAP payload.
10	AAA server fetches the subscriber profile from HLR/HSS and validates the EAP Challenge response sent from UE. Access-Accept/Diameter EAP Answer is sent to SaMOG with user profile and EAP Success payload. SaMOG saves the user profile information. The AAA server authorizes local offload for the subscriber and the APN provided by AAA server has flow-based LBO enabled. The AAA server may also provide a rulebase name that is configured in SaMOG and has the forwarding and NAT policy. The forwarding and NAT policy in turn has an ACL configured to identify the packets to be forwarded to the EPC core.
11	SaMOG performs DNS query with the DNS server and obtains the P-GW IP address.
12	SaMOG sets up the GTP session with PGW by sending a Create Session Request message to PGW.
13	PGW responds with a Create Session Response message and responds with the allocated UE IP address (a.b.c.d).
14	SaMOG sends Access-Accept to the WLC with EAP-Success payload.
15	WLC forwards the EAP-Success to the UE.

Step	Description
16	DHCP or PMIPv6 messaging is then initiated to setup the data path. The UE IP address (a.b.c.d), DNS server address and default router address is supplied to the WLC/UE in DHCP or PMIPv6 (PBA) message. Once the WLC learns the UE IP address, it sends an Accounting-Start message containing the Framed-IP-Address attribute to SaMOG. SaMOG forwards it to the AAA accounting server, and the response from accounting server is forwarded back to WLC.
17	The uplink data packet with the source IP address (a.b.c.d) is sent to WLC through the CAPWAP tunnel by UE
18	WLC encapsulates the same packet into GRE/EoGRE tunnel and forwards it to SaMOG.
19	SaMOG matches this packet with the ACL configured in the forward and NAT policy. Here, the packet does not match the ACL. SaMOG performs dynamic NAT on this packet. It allocates a global IP address from a pool (p.q.r.s) and replaces the source IP address of the data packet with this address.
20	SaMOG routes the modified packet to the Internet.
21	The downlink packet contains the destination address set to p.q.r.s from the Internet to SaMOG.
22	SaMOG performs a reverse NAT and replaces the address (a.b.c.d) as the destination address of the packet.
23	The modified packet is forwarded to the WLC over GRE/EoGRE tunnel.
24	The WLC forwards the packet to UE.
25	Another uplink data packet with the source IP address (a.b.c.d) is sent to WLC through the CAPWAP tunnel by UE.
26	WLC encapsulates the same packet into GRE/EoGRE tunnel and sends it to SaMOG
27	SaMOG matches this packet with the ACL configured in the forward and NAT policy. Here, the packet does match the ACL.

Step	Description
28	SaMOG then routes the packet to PGW over the GTP tunnel.
29	PGW processes the packet and sends it to the Internet over the Gi interface, and receives a downlink packet from the Internet.
30	The downlink packet comes with the destination address set to a.b.c.d from PGW to SaMOG over the GTP tunnel.
31	The packet is forwarded to the WLC through the GRE/EoGRE tunnel.
32	WLC forwards the packet to UE.

Flow-based Local Breakout - Blacklist

Figure 32: Flow-based Local Breakout - Blacklist Call Flow

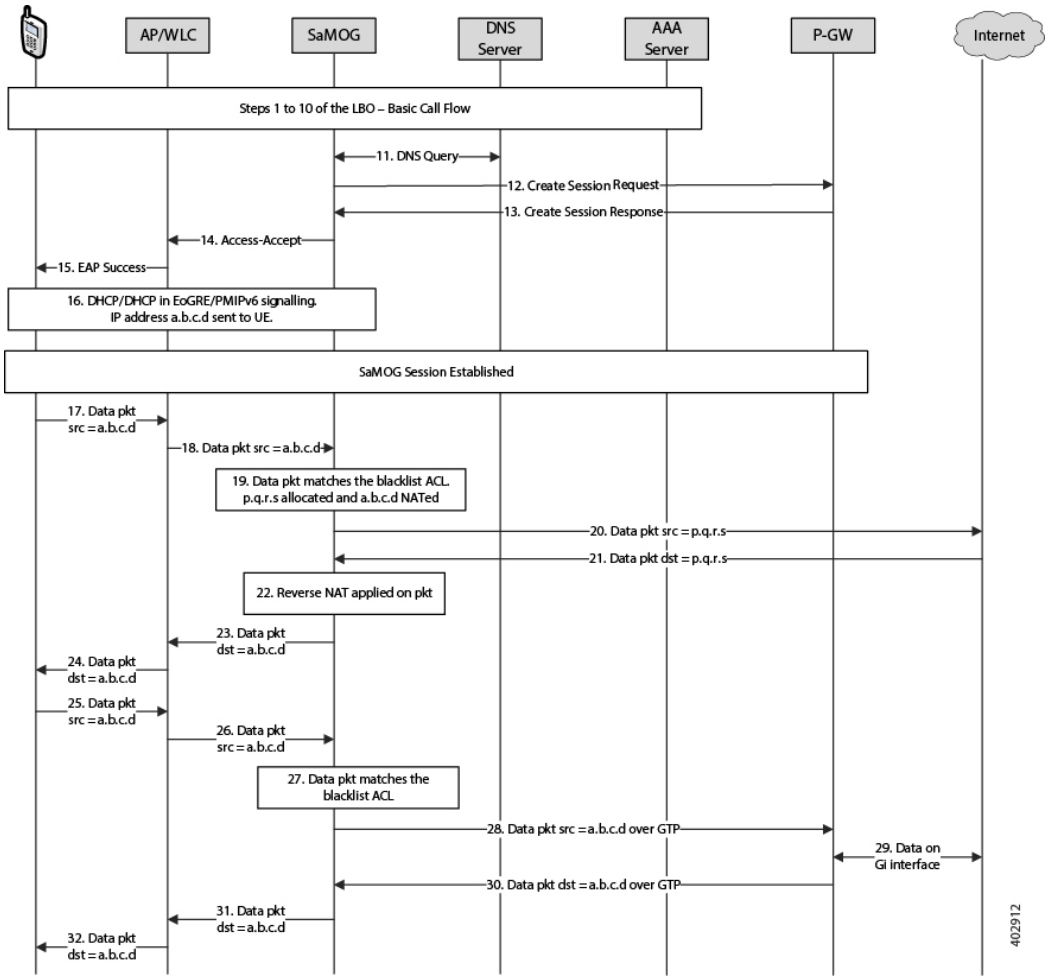


Table 54: Flow-based LBO - Blacklist Call Flow Descriptions

Step	Description
1	UE initiates an initial attach procedure towards WLC.
2	WLC forms an Access-Request message with EAP-Identity payload, User-Name and Acct-Session-Id, and forwards the same to SaMOG.
3	SaMOG forms an Access-Request towards the RADIUS AAA server, or a Diameter EAP Request towards the STa AAA server using the attributes received from WLC.

Step	Description
4	AAA server performs EAP authentication and forwards the Access-Challenge/Diameter EAP Answer to SaMOG with the EAP payload.
5	SaMOG copies the EAP payload to the Access-Challenge towards WLC.
6	WLC forwards EAP Request with SIM Challenge towards UE.
7	UE sends EAP response with SIM Challenge response.
8	WLC sends Access-Request to SaMOG with EAP payload received from UE.
9	SaMOG sends Access-Request/Diameter EAP Request to AAA server with the EAP payload.
10	AAA server fetches the subscriber profile from HLR/HSS and validates the EAP Challenge response sent from UE. Access-Accept/Diameter EAP Answer is sent to SaMOG with user profile and EAP Success payload. SaMOG saves the user profile information. The AAA server authorizes local offload for the subscriber and the APN provided by AAA server has flow-based LBO enabled. The AAA server may also provide a rulebase name that is configured in SaMOG and has the forwarding and NAT policy. The forwarding and NAT policy in turn has an ACL configured to identify the packets to be forwarded to the Internet directly.
11	SaMOG performs DNS query with the DNS server and obtains the P-GW IP address.
12	SaMOG sets up the GTP session with PGW by sending a Create Session Request message to PGW.
13	PGW responds with a Create Session Response message and responds with the allocated UE IP address (a.b.c.d).
14	SaMOG sends Access-Accept to the WLC with EAP-Success payload.
15	WLC forwards the EAP-Success to the UE.

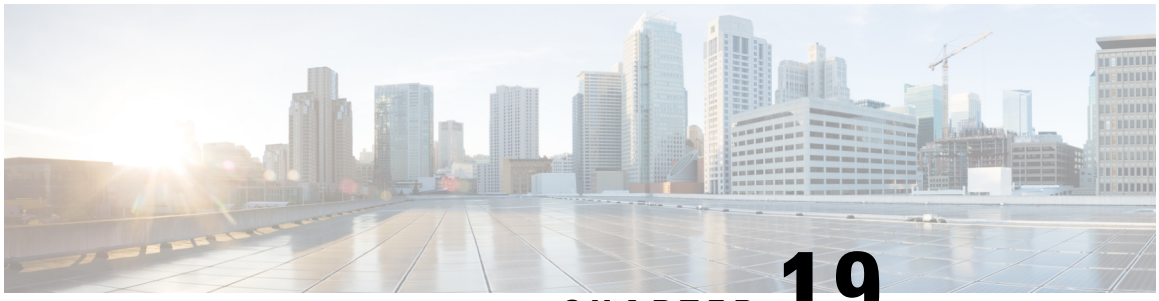
Step	Description
16	DHCP or PMIPv6 messaging is then initiated to setup the data path. The UE IP address (a.b.c.d), DNS server address and default router address is supplied to the WLC/UE in DHCP or PMIPv6 (PBA) message. Once the WLC learns the UE IP address, it sends Accounting-Start message containing the Framed-IP-Address attribute to SaMOG. SaMOG forwards it to the AAA accounting server, and the response from accounting server is forwarded back to WLC.
17	The uplink data packet with the source IP address (a.b.c.d) is sent to WLC through the CAPWAP tunnel by UE.
18	WLC encapsulates the same packet into GRE/EoGRE tunnel and forwards it to SaMOG.
19	SaMOG matches this packet with the ACL configured in the forward and NAT policy. Here, the packet matches the ACL. SaMOG performs dynamic NAT on this packet. It allocates a global IP address from a pool (p.q.r.s) and replaces the source IP address of the data packet with this address.
20	SaMOG routes the modified packet to the Internet.
21	The downlink packet contains the destination address set to p.q.r.s from the Internet to SaMOG.
22	SaMOG performs a reverse NAT and replaces the address (a.b.c.d) as the destination address of the packet.
23	The modified packet is forwarded to the WLC over GRE/EoGRE tunnel.
24	The WLC forwards the packet to UE.
25	Another uplink data packet with the source IP address (a.b.c.d) is sent to WLC through the CAPWAP tunnel by UE.
26	WLC encapsulates the same packet into GRE/EoGRE tunnel and sends it to SaMOG
27	SaMOG matches this packet with the ACL configured in the forward and NAT policy. Here, the packet does not match the ACL.

Step	Description
28	SaMOG then routes the packet to PGW over the GTP tunnel.
29	PGW processes the packet and sends it to the Internet over the Gi interface, and receives a downlink packet from the Internet.
30	The downlink packet comes with the destination address set to a.b.c.d from PGW to SaMOG over the GTP tunnel.
31	The packet is forwarded to the WLC through the GRE/EoGRE tunnel.
32	WLC forwards the packet to UE.

Limitations, Restrictions, and Dependancies

The following limitations, restrictions, and dependancies apply for the Local Breakout - Basic model:

- For an L3IP access type, the IP address assigned by the P-GW or GGSN must be routable on the WLAN. SaMOG does not assign a separate IP address for the UE.
- The Flow-based LBO model will always require NAT to route the UE packets on the Internet directly.



CHAPTER 19

SaMOG Local P-GW Selection

This feature enables the SaMOG Gateway to configure and use local P-GW addresses either as a fall-back selection method or as the preferred selection method.

The following sections provide more detailed information:

Feature Description

The SaMOG Gateway allocates P-GW to provide PDN connectivity to the User Equipment (UEs). The P-GW address is either selected based on the address provided by the AAA server (static selection) or by using DNS resolution (dynamic selection). With this feature, the SaMOG Gateway can support P-GW addresses that are configured locally under the APN Profile Configuration Mode. SaMOG can use these locally configured P-GW addresses in one of the following ways:

- As a fall-back selection method
- As preferred selection method

Local P-GW as a Fall-back Selection Method

1. When AAA Server identifies the P-GW selection method as Dynamic and if the local P-GW address is configured under the APN Profile, the SaMOG Gateway will perform local P-GW selection in the following scenarios:
   - The P-GW addresses received by DNS resolution are unreachable.
   - The DNS server is unreachable, or the DNS query is rejected.
   - DNS resolution is not configured, and/or the AAA server does not send the P-GW address.
2. When AAA Server identifies the P-GW selection method as static (P-GW IP Address or P-GW FQDN):

If the local P-GW address(es) are configured under the APN Profile and also P-GW selection fallback for P-GW ID is configured under mrme-service, the SaMOG Gateway will perform local P-GW selection in the following scenarios:

- The P-GW address mentioned by AAA server or received by DNS resolution (P-GW FQDN) is unreachable
- The DNS server is unreachable, or the DNS query is rejected (for P-GW FQDN).
- DNS resolution is not configured (for P-GW FQDN).

Local P-GW as the Preferred Selection Method

The SaMOG Gateway can be configured to use the local P-GW addresses for P-GW node selection as the preferred selection method.

This method is applicable only when the AAA server mentions the selection method as dynamic and the "local-configuration-preferred" configuration is enabled under mrme-service.

Note This configuration is not effective when the AAA server mentions the selection method as static.

How Local P-GW Address Support Works

The SaMOG Gateway performs local P-GW address selection based on the weight that is configured for each P-GW address (similar to DNS resolution of P-GW addresses). Only the first P-GW address is selected based on its weight. The rest of the addresses are selected on a round-robin basis starting from the next available P-GW address, rounding to the P-GW address before the first selected P-GW address. A maximum of 16 IPv4 and/or IPv6 local P-GW addresses can be configured.

Limitations

- In this release, the SaMOG Gateway does not support dual bind (IPv4 and IPv6) address for EGTP service (or GTPU service).
- The PGW-Fallback is supported only for GTPv2 Network Protocol.

Table 55: Truth Table Describing P-GW Fall Back Selection

SL No	Local Preferred Configuration	PGW-ID Fallback Configuration	AAA - Address Location Type	Behavior
1	Yes/No	No	PGW - IP Address	1. If PGW is not reachable then session setup is terminated, No Fallback

2	Yes/No	No	PGW FQDN	1. SaMOG performs DNS resolution on provided PGW FQDN, If resolved PGW is not reachable session setup is terminated, No Fallback
3	Yes	Yes	PGW - IP Address	1. If PGW is not reachable then 2. SaMOG tries to establish session with locally configured PGW Addresses If they are not reachable then 3. SaMOG performs DNS resolution based on APN FQDN and tries to establish session with resolved PGW addresses.
4	No	Yes	PGW- IP Address	1. If PGW is not reachable then 2. SaMOG performs DNS resolution based on APN FQDN and tries to establish session with resolved PGW addresses. If they are unreachable then. 3. If local configured PGW's are available, SaMOG tries to establish session with configured IP's
5	Yes	Yes	PGW FQDN	1. SaMOG performs DNS resolution on provided PGW FQDN, If resolved PGW is not reachable then 2. SaMOG tries to establish session with locally configured PGW Addresses If they are not reachable then 3. SaMOG performs DNS resolution based on APN FQDN and tries to establish session with resolved PGW addresses.

6	No	Yes	PGW FQDN	1. SaMOG performs DNS resolution on provided PGW FQDN, If resolved PGW is not reachable then 2. SaMOG performs DNS resolution based on APN FQDN and tries to establish session with resolved PGW addresses. If they are unreachable then. 3. If local configured PGW's are available, SaMOG tries to establish session with configured IP's
7	No	No/Yes	PGW - Dynamic Allocation (APN FQDN)	1. SaMOG performs DNS resolution on APN FQDN, If resolved PGWs are not reachable then 2. SaMOG tries to establish session with locally configured PGW Addresses.
8	Yes	No/Yes	PGW - Dynamic Allocation (APN FQDN)	1. SaMOG tries to establish session with locally configured PGW Addresses. If they are not reachable then 2. SaMOG performs DNS resolution based on APN FQDN and tries to establish session with resolved PGW addresses.
		Note Note: Fallback is applicable to only GTPv2 Network Protocol.		

Configuring Local P-GW Selection

Configuring Local P-GW Resolution

Use the **pgw-address** command under the APN Profile Configuration Mode to define local P-GW addresses for load balancing.

```
configure
   apn-profile profile-name
     pgw-address ipv4_address |  ipv6_address weight weight [ primary | secondary
 ]
      no pgw-address ipv4_address | ipv6_address
      end
```

Notes:

- Use the **no pgw-address** *ipv4_address* | *ipv6_address* command to disable the P-GW address(es) configured for an APN profile.

  ipv4_address must be an IPv4 address expressed in dotted-decimal notation.

  ipv6_address must be an IPv6 address expressed in colon (or double-colon) notation.

- **weight** *weight*

  Configures the weight for the IPv4 or IPv6 address.

  weight is an integer from 1 to 100.

- **primary | secondary**

  primary: Configures the primary P-GW for S2b interface.

  secondary: Configures the primary P-GW for S2b interface.

- A maximum of 16 P-GW IPv4 and/or IPv6 addresses can be configured for an APN profile.
- When multiple P-GW addresses are configured, only the first P-GW will be selected based on the weight. The rest of the P-GW addresses are selected using the round-robin mechanism

Configuring Preferred Selection as Local P-GW

Use the **pgw-selection** command under the MRME Service Configuration Mode to set the P-GW address selection from a local configuration as the preferred selection mechanism.

```
configure
   context context_name
      mrme-service service_name
         pgw-selection local-configuration-preferred
         end
```

Notes:

- Use the **no pgw-selection local-configuration-preferred** command to disable this command.
- By default, this command is disabled. The SaMOG Gateway uses DNS-based P-GW selection (dynamic selection) as the preferred selection method.

Configuring Local P-GW Fallback for Static Selection Method

Use the **pgw-selection** command under the MRME Service Configuration Mode to set the P-GW address selection from a local configuration as static selection method.

```
configure
   context context_name
      mrme-service service_name
         pgw-selection fallback pgw-id
         end
```

Notes:

- Use the **no pgw-selection fallback pgw-id** command to disable this command.
- By default, this command is disabled.

Verifying Configuration for Local P-GW Support

show apn-profile full all

Use the **show apn-profile** command to verify the configured P-GW IP address(es).

```
P-GW:
 IP-Address                      : 6666::200:1
 S5-S8-Protocol                  : N/A
 Weight                          : 1
IP-Address                       : 6666::a00:1
 S5-S8-Protocol                  : N/A
 Weight                          : 17
```

show mrme-service name *mrme_service_name*

Use the **show mrme-service name** command to verify the status of the local P-GW selection configuration.

```
Preferred PGW selection mechanism : Local
PGW-ID selection fallback : Enabled
```

Monitoring Local P-GW Selection

This section provides information on the show commands available to monitor the local P-GW selection.

Local P-GW Selection Show Command(s) and/or Outputs

show samog-service statistics

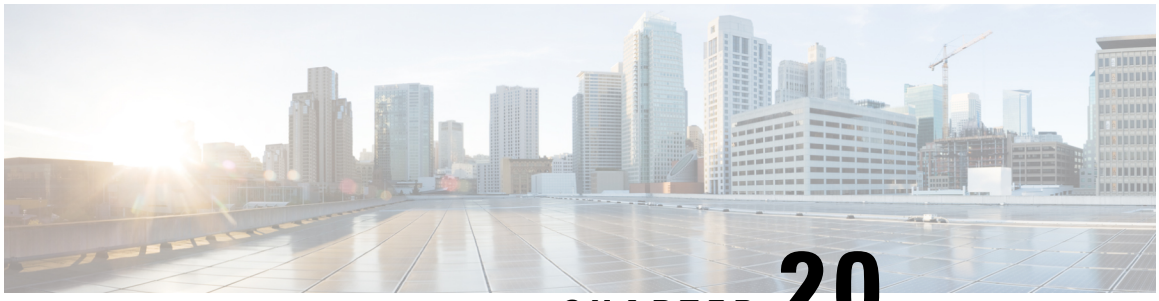
The following fields are available to the output of the **show samog-service statistics** command in support of this feature.

```
Local PGW Fallback Stats:
 Attempted:              0
  Success:               0        No Alternate GW:          0
```

Table 56: show samog-service statistics Command Output Descriptions

Field	Description
Local PGW Fallback Stats	

Attempted	Total number of local P-GW fall-back attempted.
Success	Total number of successful local P-GW fall-back achieved.
No Alternate GW	Total number of alternative Gateways available for fall-back.



CHAPTER 20

SaMOG Packet Capture (PCAP) Trace Support

Feature Information

Summary Data

Status	New Feature
Introduced-In Release	21.2
Modified-In Release(s)	Not Applicable
Applicable Product(s)	SaMOG
Applicable Platform(s)	ASR 5500 vPC-SI vPC-DI
Default Setting	Disabled
Related CDETS ID(s)	CSCva99100
Related Changes in This Release	Not Applicable
Related Documentation	SaMOG Administration Guide Command Line Interface Reference Guide

Revision History

Important Revision history details are not provided for features introduced before release 21.2.

Revision Details	Release	Release Date
New in this release.	21.2	April 27, 2017

Feature Description

The PCAP trace output of the **monitor subscriber** and **monitor protocol** commands can be exported as a hexdump file for SaMOG sessions. The hexdump capture can be stored in a text file in a hard disk, and later transferred to an external server through SFTP using a PUSH or PULL method.

PCAP trace and hexdump file collection can be enabled or disabled under the **monitor protocol** and **monitor subscriber** commands.

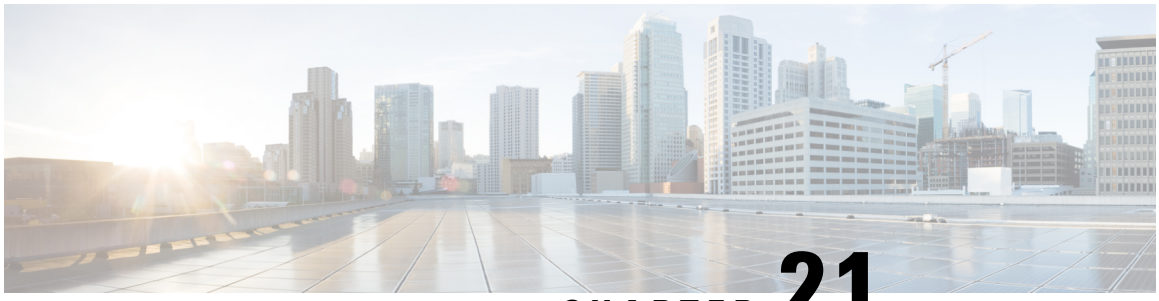
For SaMOG, hexdump captures can be enabled for the following protocols:

- GTPv1
- GTPv2
- GTPU
- User L3
- Diameter
- Radius
- EoGRE
- PMIPv6

SaMOG subscriber information for PCAP trace can be specified using the following filters:

- By MSID/IMSI
- By callid
- By username
- Next-Call
- By IMEI
- By MSISDN
- Next-SAMOG Call

For more information on PCAP Trace, Refer the *Packet Capture (PCAP) Trace* chapter in the *ASR5500 System Administration Guide*.



CHAPTER 21

Seamless Session Handover

The following topics are discussed:

Feature Description

Overview

This feature enables SaMOG to switch the access type (PMIPv6/EoGRE) seamlessly and preserve the session when subscribers move between access points with different session trigger types.

The SaMOG Gateway can:

- Seamlessly switch the access type from PMIPv6 (PMIPv6-based session creation) to EoGRE, based on the DHCP Discover, DHCP Request, or Direct Data Traffic on the EoGRE tunnel.
- Seamlessly switch the access type from EoGRE (DHCP trigger-based session creation) to PMIPv6, based on the PBU message from the AP.

How Seamless Session Handover Works

Flows

PMIPv6 to EoGRE (DHCP-triggered) Handover

The figure below shows the detailed handover procedure from PMIPv6 to EoGRE (DHCP-triggered).

Figure 33: PMIPv6 to EoGRE (DHCP-triggered) Handover Call Flow

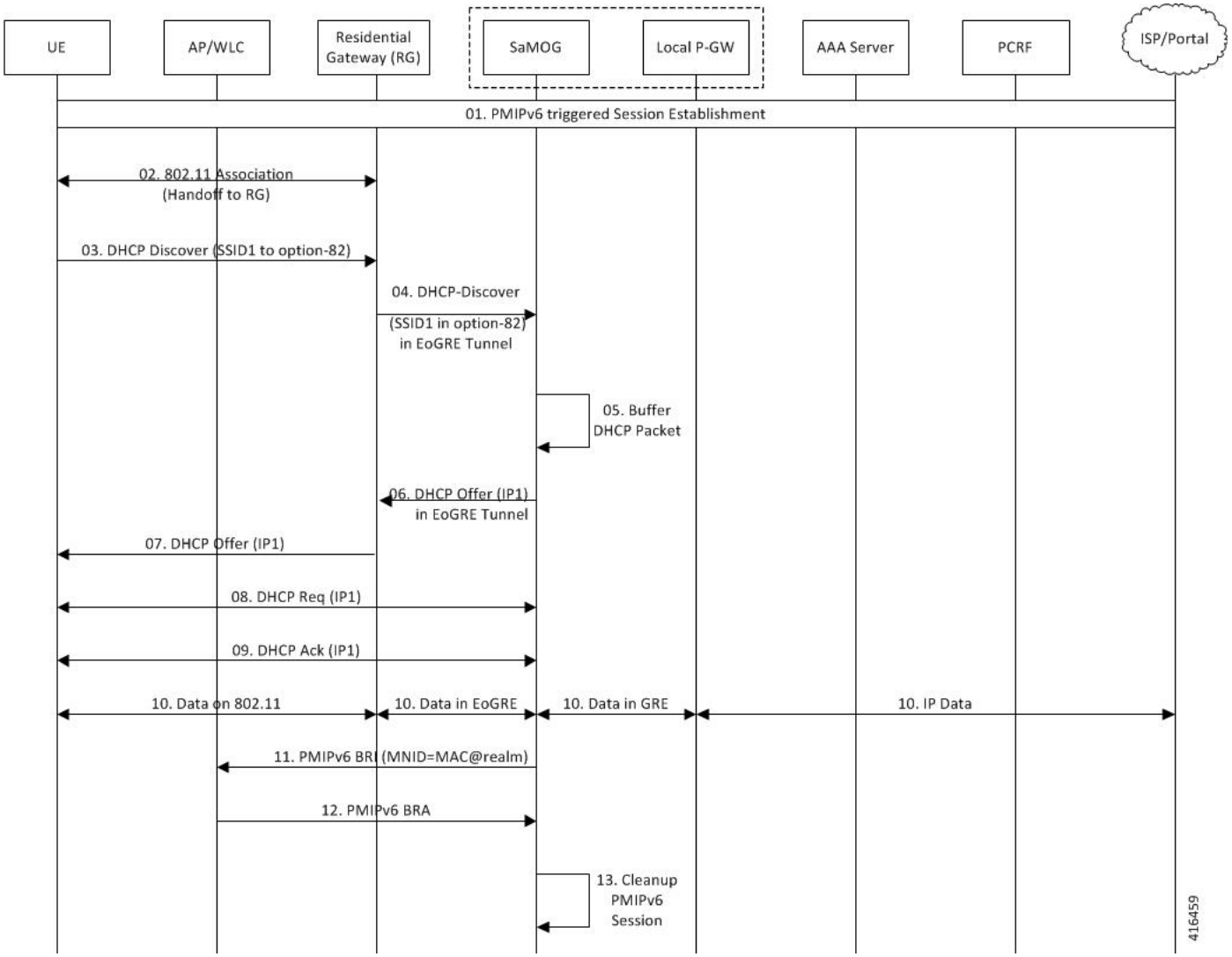


Table 57: PMIPv6 to EoGRE (DHCP-triggered) Handover

Step	Description
01	PMIPv6-triggered session is established. For more information on the PMIPv6-based session establishment, refer the *PMIPv6-based Session Creation* section of this guide. As the TWAN profile for DHCP-triggered session is associated with the MRME service, EoGRE (UE MAC) based flows are installed during the PMIPv6-triggered session setup.
02	UE moves (hand-off) to a new Residential Gateway (RG) that supports EoGRE.
03	UE send a DHCP-DISCOVER message towards the Residential Gateway (RG).
04	The RG forwards the DHCP-DISCOVER message to SaMOG on the EoGRE tunnel.

Step	Description
05	SaMOG detects that the UE has moved to a new RG (hand-off) and switches the data path from the PMIPv6 GRE tunnel to EoGRE tunnel for the UE session. SaMOG also updates the session type to EoGRE/DHCP-triggered.
06	SaMOG assigns the same IP address allocated during the PMIPv6 session to UE. DHCP-OFFER message is sent to the RG on the EoGRE tunnel.
07	RG forwards the DHCP-OFFER message to the UE.
08	A DHCP-Request message is sent from the UE to SaMOG (through the RG).
09	SaMOG sends a DHCP Ack message to the UE (through the RG).
10	Data is transferred between the UE and ISP (through SaMOG and the RG).
11	SaMOG initiates a clean-up of the previous PMIPv6 access side session with the old AP/WLC. SaMOG sends a Binding Revocation Indication (BRI) message to the old AP/WLC.
12	The old AP/WLC sends a BRI Ack message to SaMOG.
13	SaMOG cleans up the PMIPv6 session.

PMIPv6 to EoGRE (data-triggered) Handover

The figure below shows the detailed handover procedure from PMIPv6 to EoGRE (data-triggered).

Figure 34: PMIPv6 to EoGRE (data-triggered) Handover Call Flow

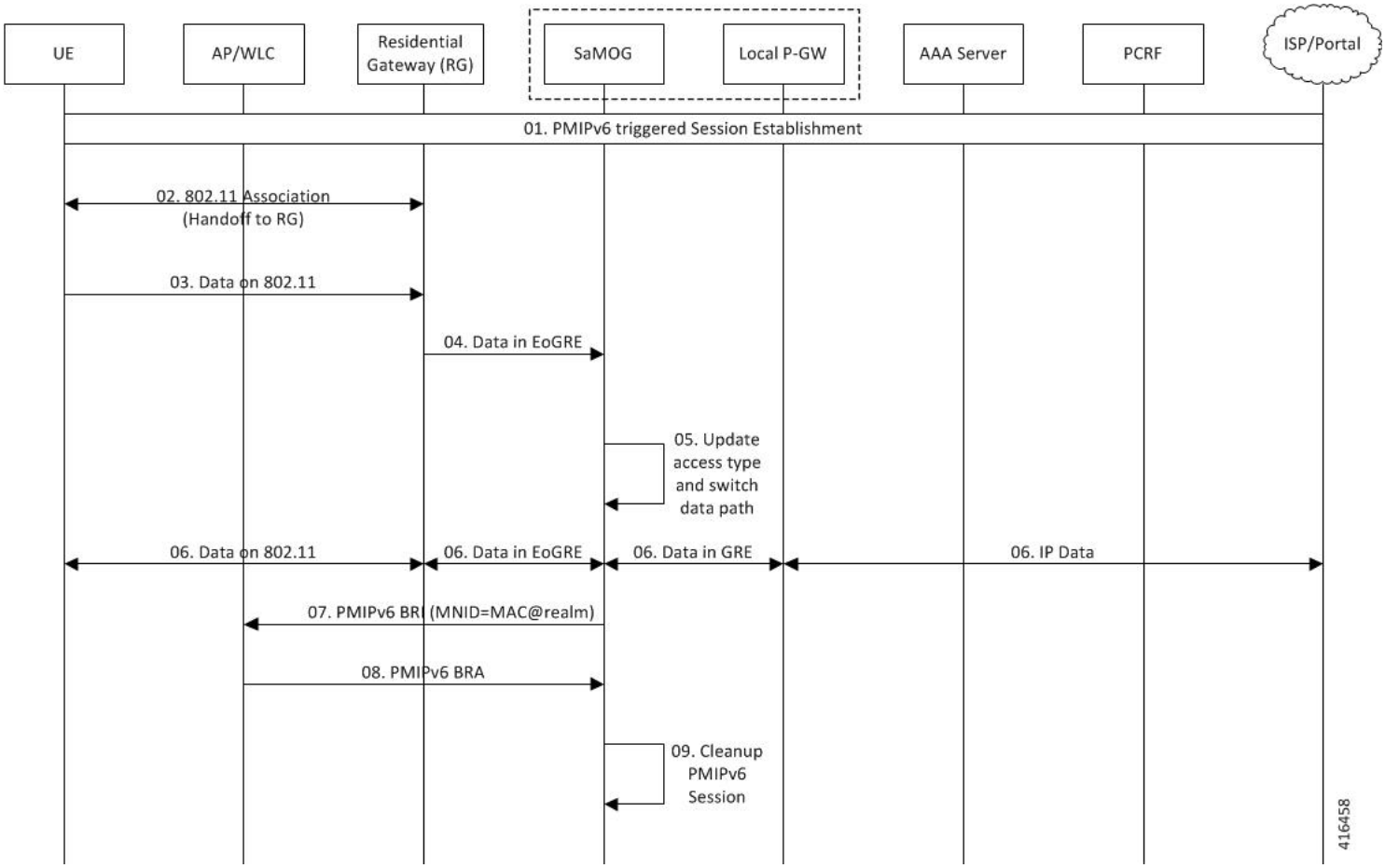


Table 58: PMIPv6 to EoGRE (data-triggered) Handover

Step	Description
01	PMIPv6-triggered session is established. For more information on the PMIPv6-based session establishment, refer the *PMIPv6-based Session Creation* section of this guide. As the TWAN profile for DHCP-triggered session is associated with the MRME service, EoGRE (UE MAC) based flows are installed during the PMIPv6-triggered session setup.
02	UE moves (hand-off) to a new Residential Gateway (RG) that supports EoGRE.
03	UE continues to send data traffic through the new RG.
04	RG forwards the data traffic to SaMOG through the EoGRE tunnel.
05	SaMOG detects that the UE has moved to a new RG (hand-off) and switches the data path from the PMIPv6 GRE tunnel to EoGRE tunnel for the UE session. SaMOG also updates the session type to EoGRE/DHCP-triggered.
06	Data is transferred between the UE and ISP (through SaMOG and the RG).

Step	Description
07	SaMOG initiates a clean-up of the previous PMIPv6 access side session with the old AP/WLC. SaMOG sends a Binding Revocation Indication (BRI) message to the old AP/WLC.
08	The old AP/WLC sends a BRI Ack message to SaMOG.
09	SaMOG cleans up the PMIPv6 session.

EoGRE to PMIPv6 (PBU-triggered) Handover

The figure below shows the detailed handover procedure from EoGRE to PMIPv6 (PBU-triggered).

Figure 35: EoGRE to PMIPv6 (PBU-triggered) Handover Call Flow

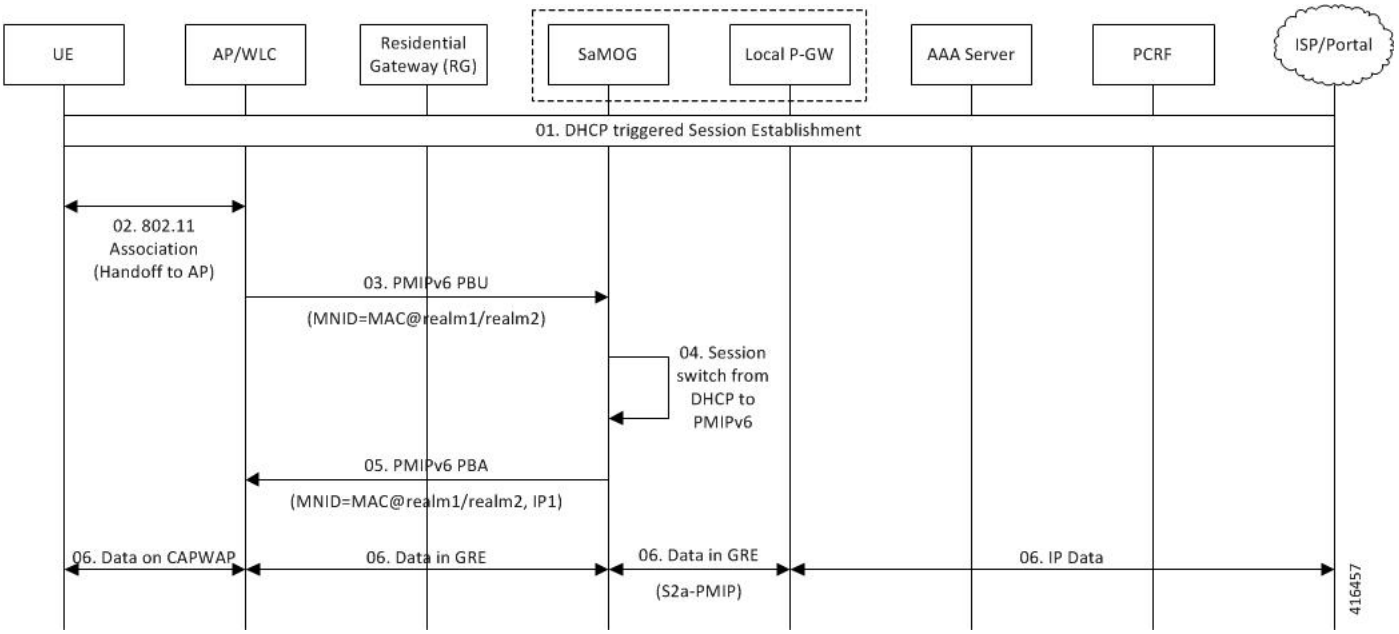


Table 59: EoGRE to PMIPv6 (PBU-triggered) Handover

Step	Description
01	DHCP-triggered session is established. For more information on DHCP trigger-based session, refer the *DHCP-Trigger Based Session Creation* chapter of the *SaMOG Administration Guide*.
02	UE moves (hand-off) to a new AP/WLC that supports the PMIPv6 access type.
03	The AP/WLC initiates a PBU message towards SaMOG on behalf of the UE (NAI is <MAC> or <MAC>@relam).
04	SaMOG receives the PBU message and detects that UE has moved to new AP (hand-off). SaMOG switches the data path from the EoGRE tunnel to a PMIPv6 GRE tunnel for the UE session, and also updates the session type to PMIPv6 triggered.

Step	Description
05	SaMOG initiates a PBA message towards the AP/WLC.
06	Data is transferred between the UE and ISP (through SaMOG).

Limitations

Architectural Limitations

- This feature supports RADIUS-based authentication between SaMOG and the 3GPP AAA Server. Diameter-based authentication is currently not supported.
- This feature supports PMIPv6-based S2a interface towards the local gateway. GTPv1 and GTPv2 are currently not supported.
- Only IPv4 address allocation is supported for the UE. IPv6 and IPv4v6 PDN types are currently not supported.
- All interfaces towards all external nodes will be IPv4 address only. IPv6 transport on any interface with external nodes is currently not supported.
- The AP will not convey the user location and SSID information to SaMOG.

Monitoring and Troubleshooting Seamless Session Handover

Show Command(s) and/or Outputs

show samog-service statistics

The following fields are available to the output of the **show samog-service statistics** command in support of this feature:

```
Handoff Statistics:
PMIP to PMIP Handoff Stats:
  Received:                   0            Accepted:                0
  Denied:                     0
DHCP to DHCP Handoff Stats:
  Received:                   0            Accepted:                0
  Denied:                     0
 PMIP to EoGRE Handoff Requests:
  Received:                   0            Accepted:                0
  Denied:                     0
 EoGRE to PMIP Handoff Requests:
  Received:                   0            Accepted:                0
  Denied:                     0
```

*Table 60: **show samog-service statistics** Command Output Descriptions*

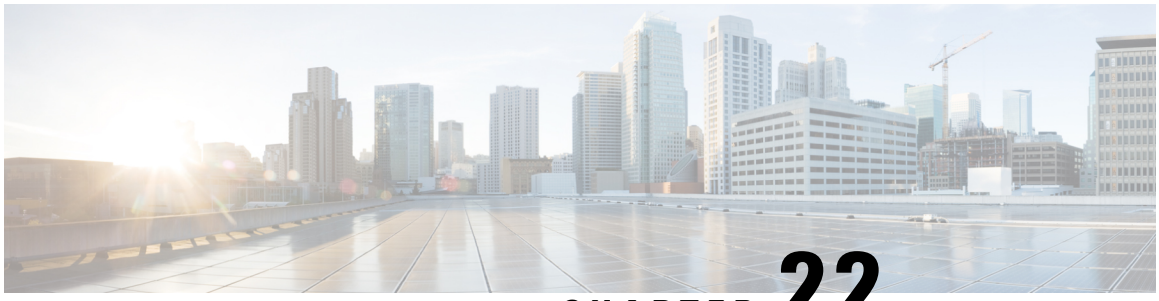
Field	Description
Handoff Statistics:	
PMIP to PMIP Handoff Stats:	
Received	Total number of PMIPv6 PBUs received for handoff for an existing PMIP session.
Accepted	Total number of PMIPv6 PBUs for Handoff accepted for an existing PMIP session.
Denied	Total number of PMIPv6 PBUs for handoff denied for an existing PMIP session.
DHCP to DHCP Handoff Stats:	
Received	Total number of DHCP Discover messages received during handoff for an existing DHCP session.
Accepted	Total number of DHCP Discover messages accepted during handoff for an existing DHCP session.
Denied	Total number of DHCP Discover messages denied during handoff for an existing DHCP session.
PMIP to EoGRE Handoff Requests:	
Received	Total number of EoGRE handoff messages received for a PMIP session.
Accepted	Total number of EoGRE handoff messages accpted for a PMIP session.
Denied	Total number of EoGRE handoff messages denied for a PMIP session.
EoGRE to PMIP Handoff Requests:	
Received	Total number of PMIP handoff messages received for an EoGRE session.
Accepted	Total number of PMIP handoff messages accepted for an EoGRE session.
Denied	Total number of PMIP handoff messages denied for an EoGRE session.

Seamless Session Handover Bulk Statistics

The following bulk statistics in the SaMOG schema provide information on seamless handovers between access types for a session:

Variable	Description	Data Type
cgw-binding-update-handoff-req-total-received	**Description:** Total number of PMIPv6 PBUs received for handoff for an existing PMIP session. **Triggers:** Increments whenever PMIPv6 PBU is received by SaMOG for handoff. **Availability:** Per SaMOG Service **Type:** Counter	Int32
cgw-binding-update-handoff-req-total-accepted	**Description:** Total number of PMIPv6 PBUs for Handoff accepted for an existing PMIP session. **Triggers:** Increments whenever PMIPv6 PBU is accepted by SaMOG for handoff. **Availability:** Per SaMOG Service **Type:** Counter	Int32
cgw-binding-update-handoff-req-total-denied	**Description:** Total number of PMIPv6 PBUs for handoff denied for an existing PMIP session. **Triggers:** Increments whenever PMIPv6 PBU received by SaMOG for handoff denied during processing. **Availability:** Per SaMOG Service **Type:** Counter	Int32
cgw-sessstat-dhcp-disc-handoff-received	**Description:** Total number of DHCP Discover messages received during handoff for an existing DHCP session. **Triggers:** Increments whenever a DHCP Discover message is received by SaMOG during handoff. **Availability:** Per SaMOG Service **Type:** Counter	Int32
cgw-sessstat-dhcp-disc-handoff-accepted	**Description:** Total number of DHCP Discover messages accepted during handoff for an existing DHCP session. **Triggers:** Increments whenever a DHCP Discover message is accepted by SaMOG during handoff. **Availability:** Per SaMOG Service **Type:** Counter	Int32
cgw-sessstat-dhcp-disc-handoff-denied	**Description:** Total number of DHCP Discover messages denied during handoff for an existing DHCP session. **Triggers:** Increments whenever a DHCP Discover message is denied by SaMOG during handoff. **Availability:** Per SaMOG Service **Type:** Counter	Int32

Variable	Description	Data Type
cgw-sessstat-pmip-to-eogre-handoff-received	**Description:** Total number of EoGRE handoff messages received for a PMIP session. **Triggers:** Increments whenever an EoGRE message is received by SaMOG for an existing PMIP session. **Availability:** Per SaMOG Service **Type:** Counter	Int32
cgw-sessstat-pmip-to-eogre-handoff-accepted	**Description:** Total number of EoGRE handoff messages accepted for a PMIP session. **Triggers:** Increments whenever an EoGRE message is accepted by SaMOG for handoff from a PMIP session. **Availability:** Per SaMOG Service **Type:** Counter	Int32
cgw-sessstat-pmip-to-eogre-handoff-denied	**Description:** Total number of EoGRE handoff messages denied for a PMIP session. **Triggers:** Increments whenever an EoGRE message is denied by SaMOG for handoff from a PMIP session. **Availability:** Per SaMOG Service **Type:** Counter	Int32
cgw-sessstat-eogre-to-pmip-handoff-received	**Description:** Total number of PMIP handoff messages received for an EoGRE session. **Triggers:** Increments whenever a PMIP message is received by SaMOG for an existing EoGRE session. **Availability:** Per SaMOG Service **Type:** Counter	Int32
cgw-sessstat-eogre-to-pmip-handoff-accepted	**Description:** Total number of PMIP handoff messages accepted for an EoGRE session. **Triggers:** Increments whenever a PMIP message is accepted by SaMOG for handoff from an EoGRE session. **Availability:** Per SaMOG Service **Type:** Counter	Int32
cgw-sessstat-eogre-to-pmip-handoff-denied	**Description:** Total number of PMIP handoff messages denied for an EoGRE session. **Triggers:** Increments whenever a PMIP message is denied by SaMOG for handoff from an EoGRE session. **Availability:** Per SaMOG Service **Type:** Counter	Int32



CHAPTER 22

Static Serving PLMN Configuration

The following topics are discussed:

Feature Description

Overview

The static serving PLMN configuration feature enables subscribers connecting from different operator sub-zones to be grouped and treated as a home user instead of a visited user. These subscribers can then be served by one SaMOG/P-GW for offloading traffic. This feature can be enabled using the **serving-plmn id** command under the Call Control Profile Configuration Mode.

How Static Serving PLMN Works

Architecture

When the serving PLMN ID (MNC/MCC) is configured under the Call Control Profile Configuration Mode (typically with the same serving PLMN ID of the serving P-GW), SaMOG provides higher priority to this configuration. The configured PLMN will be then be sent to P-GW in the Serving-Network IE of the Create Session Request (CSR) message. These subscribers will be treated as home users even if they belong to different operator sub-zones, and can be served by one SaMOG/P-GW.

In Release 21.1 and later, the PLMN ID for UICC and non-UICC devices is selected based on the following order of priority:

- The **serving-plmn id** configuration under the Call Control Profile Configuration Mode.
- The **plmn id** configuration under the SaMOG Service Configuration Mode.

- The User-Name from the EAP-Identity, Authentication, or Accounting messages if the realm (serving PLMN's realm) part of User-Name is in 3GPP format.

In Release 21.0 and earlier, the PLMN ID for UICC and non-UICC devices is selected based on the following order of priority:

- The User-Name from the EAP-Identity, Authentication, or Accounting messages if the realm (serving PLMN's realm) part of User-Name is in 3GPP format.
- The **plmn id** configuration under the SaMOG Service Configuration Mode.

Limitations

Architectural Limitations

- As there is no serving-plmn field in a PMIPv6 interface, static serving PLMN is not supported on the PMIPv6-based S2a interface.
- Static serving PLMN is not supported with DHCP trigger-based and Accounting-based session creation features as these features require PMIPv6-based S2a interface.

Configuring Static Serving PLMN

Use the following configuration to configure a static serving node PLMN Identifier (MCC and MNC) for a Call Control Profile:

```
configure
   call-control-profile profile_name
      serving-plmn id mcc mcc_value mnc mnc_value
      end
```

Notes:

- Use the **remove serving-plmn id** command to remove the static serving node PLMN ID configuration from the Call Control Profile.
- *mcc_value* must be an integer between 100 and 999.
- *mnc_value* must be an integer between 0 and 999.

Monitoring and Troubleshooting Static Serving PLMN Configuration

Static Serving PLMN Configuration Show Command(s) and/or Outputs

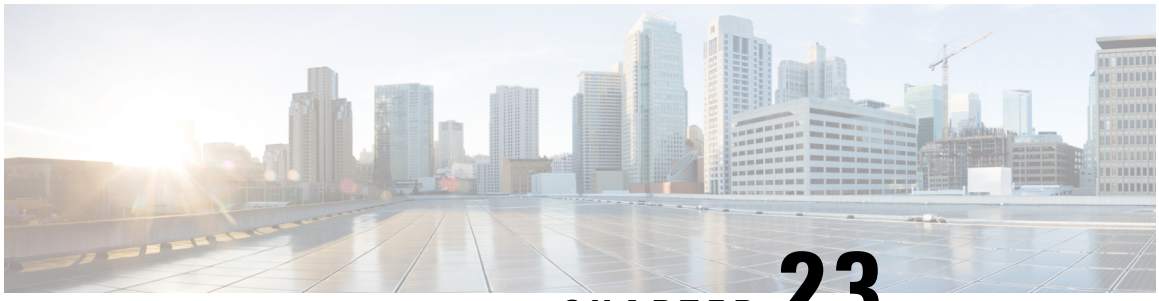
show call-control-profile full name

The following fields are available to the output of the **show call-control-profile full name** *profile_name* command in support of this feature:

```
Serving PLMN
    MCC                 : 777
    MNC                 : 109
```

Table 61: show call-control-profile full name Command Output Descriptions

Field	Description
Serving PLMN	
MCC	MCC value of the call control profile.
MNC	MNC value of the call control profile.



CHAPTER 23

Web Authorization Session Logout

Feature Information

Summary Data

Status	New Functionality
Introduced-In Release	21.2
Modified-In Release(s)	Not Applicable
Applicable Product(s)	SaMOG
Applicable Platform(s)	ASR 5500 vPC-SI vPC-DI
Default Setting	Enabled (depending on the response from the AAA Server)
Related CDETS ID(s)	CSCvc67377
Related Changes in This Release	Not Applicable
Related Documentation	SaMOG Administration Guide Command Line Interface Reference Guide

Revision History

Important Revision history details are not provided for features introduced before release 21.2.

Revision Details	Release	Release Date
New in this release.	21.2	April 27, 2017

Feature Description

Overview

The SaMOG Gateway supports the Web Authorization feature that enables SaMOG to register the subscriber's non-SIM UEs by authenticating the subscriber through a web portal (using username and password). On successful authentication, the AAA server stores the subscriber profile (APN, IMSI, QoS) from the HLR/HSS for the subscriber's device, and SaMOG establishes the network connection for the UE.

The Web Authorization feature has two phases:

- Pre-Authentication Phase – SaMOG allocates the IP address for the UE locally, and redirects the UE traffic to a web portal for subscriber authentication.
- Post-Authentication/Transparent Auto Logon (TAL) phase – P-GW allocates the IP address to the UE.

During transition between the two phases, the subscriber session disconnects. The Web Authorization feature can also be configured where the transition between the pre-authentication and post-authentication phases are achieved without session disconnection (optimized Web Authorization feature).

Refer the *Web Authorization* and *Optimized Web Authorization* sections in the *SaMOG Administration Guide* for more information on these features.

The Web Authorization Session Logout feature provides additional functionality to the Web Authorization feature. In release 21.1 and earlier, when the subscriber logs out of the portal or exhausts the quota, SaMOG clears the subscriber session on receiving a trigger from the P-GW or PCRF.

In Release 21.2 and later, SaMOG does not clear the subscriber session when the subscriber logs out of the portal or exhausts the quota. The subscriber session is instead moved from the post-authentication phase to the pre-authentication phase, and retained until the subscriber logs back in, or the timeout period (configurable) expires. This functionality enables operators to provide session stickiness for subscribers by retaining the subscriber’s Wi-Fi network connection.

License Requirements

The Web Authorization Session Logout feature requires the following licenses:

- SaMOG General license
- SaMOG Web Authorization feature license (to configure web authorization)
- SaMOG Local Breakout feature license (to configure a local P-GW)

Contact your Cisco account representative for detailed information on specific licensing requirements.

How Web Authorization Session Logout Works

Architecture

When the subscriber logs out from the web portal or exhausts the quota, the AAA Server initiates a subscription change request to SaMOG. The AAA Server does not include the APN subscription, vIMSI, or NAI information for the session (portal redirection rulebase, ACL name, IP pool name and Gi context names are optionally shared). On receiving the subscription change request without the user identity information, SaMOG verifies if the subscriber session is in post-authentication phase. SaMOG then switches the session back to the pre-authentication phase by initiating an address transfer from the local P-GW (through the VPN manager) to SaMOG, and installing the redirection rules and ACLs. CDRs used during the post-authentication phase are released when the session moves to the pre-authentication phase. New CDRs are used if the session moves back to the post-authentication phase.

The subscriber session will be retained in the pre-authentication phase until the subscriber re-authenticates through the web portal, or the session in the pre-authentication phase timeout period expires. The timeout period can be configured using the **disconnect preauth-wait-time** command under the MRME Configuration Mode.

Limitations

Architectural Limitations

- This feature is currently not support on GTPv1 and PMIPv6 towards P-GW.
- Only AAA Diameter-based authentication is supported. AAA Radius-based authentication is currently not supported.
- Inter-chassis session recovery (ICSR) is currently not supported with this feature.

Flows

Post-authentication to Pre-authentication

The figure below shows the detailed flow for the subscriber session moving from the post-authentication phase to the pre-authentication phase. The table that follows the figure describes each step in the flow.

Figure 36: Post-Authentication to Pre-Authentication Call Flow

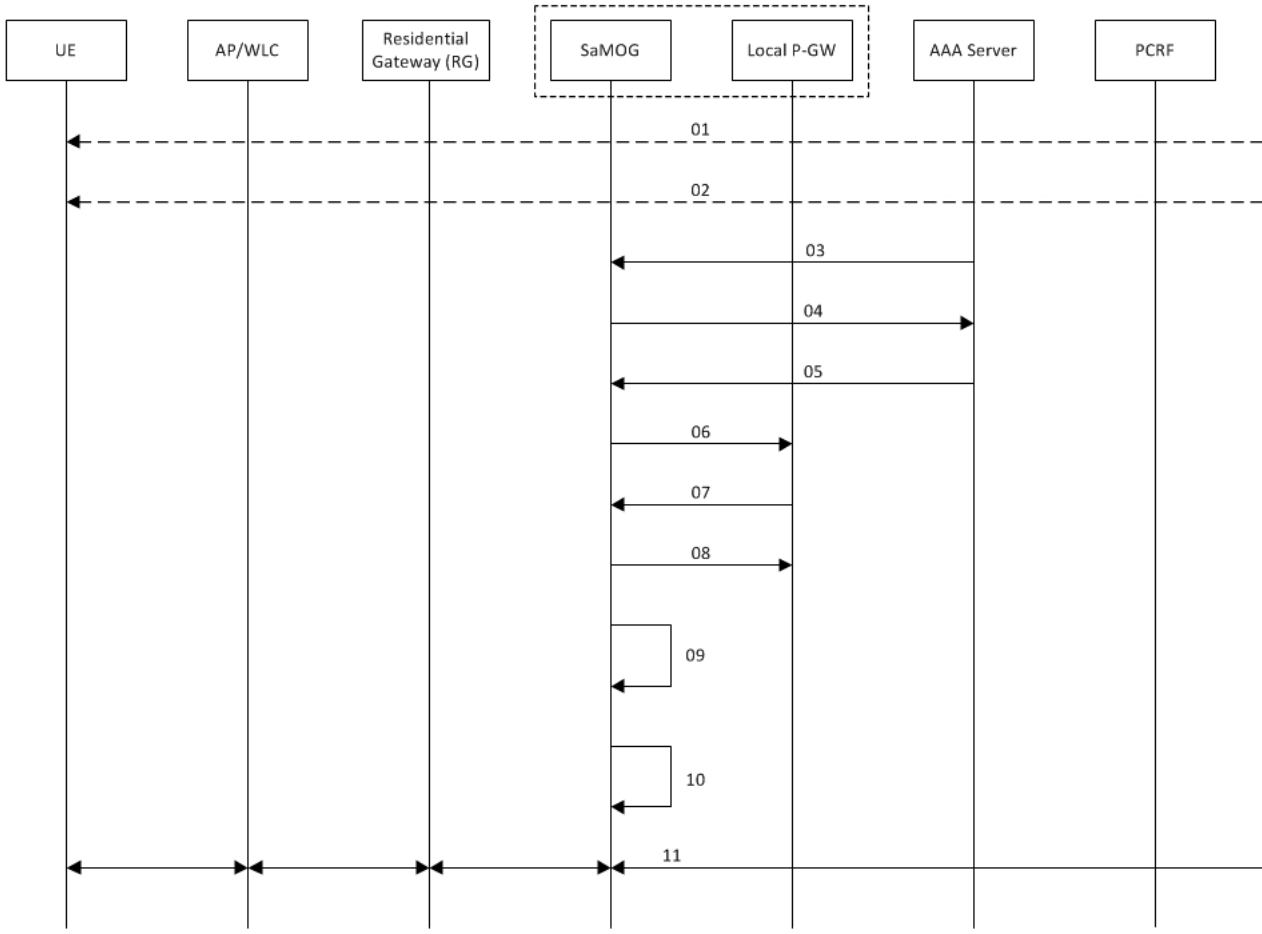


Table 62: Post-authentication to Pre-authentication

Step	Description
1	Subscriber session is established using web authorization.
2	Subscriber logs out from the portal, or exhausts the quota limit for the session.
3	The Diameter Server initiates an RAR message to SaMOG for the session.
4	SaMOG responds with an AAR message to the Diameter Server.
5	The Diameter Server initiates the AAA towards SaMOG where, • The Diameter Server does not share the user identity (no IMSI or NAI). • (optional) Parameters like the redirection rulename, ACL name, IP pool name (IPv4/IPv6) and Gi context name are included.

Step	Description
6	SaMOG receives the subscription change request without the user identity from the AAA Server. If the subscriber session is in the post-authentication phase, SaMOG initiates the process to move the session from post-authentication to pre-authentication phase. • If the AAA Server does not share the rulename, ACL name, IP pool name or context name, SaMOG takes these information from the Web authorization profile. • SaMOG transfers the user-allocated IP address (IPv4, IPv6, or IPv4v6) from the P-GW to SaMOG through the VPN manager. • SaMOG also initiates an ECS session creation with the redirection rulebase and ACLs. • On receiving the address allocation request, the VPN manager initiates an abort request to the P-GW.
7	On receiving the abort request from the VPN manager, P-GW sends a Delete Bearer Request (DBR) to SaMOG.
8	SaMOG responds to the DBR and cleans up the EGTPC/GTPU interfaces. The session, however, is not deleted.
9	The VPN manager provides the addresses requested by SaMOG. SaMOG initiates a FLOW creation for the IPs, and receives the downlink traffic from the ISP for the UE addresses.
10	SaMOG switches the session from post-authentication to pre-authentication on receiving the FLOW creation success notification from the NPU manager.
11	The subscriber is now redirected to the web portal for authorization. Once the subscriber successfully authenticates their identity, pre-authentication to post-authentication procedures are initiated. The AAA Server sends a re-authorization trigger to move the UE back to the post-authentication phase and provide the subscriber with access to the Internet.

Configuring Web Authorization Session Logout

Configuring the Pre-Authentication Wait Timer

Use the following configuration to configure the timeout for the subscriber's session after the session moves from the post-authentication phase to the pre-authentication phase:

```
config
   context context_name
      mrme-service service_name
         disconnect preauth-wait-time minutes
         end
```

Notes:

- Use the **default disconnect preauth-wait-time** command to restore the configuration to its default value.
- **Default:** 5 minutes

- *minutes* must be an integer from 1 through 60.

Monitoring and Troubleshooting Web Authorization Session Logout

Show Command(s) and/or Outputs

show samog-service statistics

The following fields are available to the output of the **show subscribers samog-service statistics** command in support of this feature:

```
MRME Service Stats:
Non-EAP Session Stats:
    Post-to-Pre:
        Attempted:    1               Success:        1
        Failure:    0
```

Table 63: show subscribers samog-service statistics Command Output Descriptions

Field	Description
MRME Service Stats:	
Non-EAP Session Stats:	
Post-to-Pre:	
Attempted	Total number of non-EAP sessions attempted to move from post to pre-authentication phase.
Success	Total number of non-EAP sessions successfully moved from post to pre-authentication phase.
Failure	Total number of non-EAP sessions that failed to be moved from post to pre-authentication phase.

show subscribers samog-only full

The following fields are available to the output of the **show subscribers samog-only full** command in support of this feature:

```
Web Authorization:    Yes
    Web authorization phase: Pre-Auth
     Post-pre switch: 1
```

Table 64: show subscribers samog-only full Command Output Descriptions

Field	Description
Web Authorization	Indicates if the web authorization is enabled for the subscriber.

Field	Description
Web authorization phase	Indicates the current web authorization phase for the subscriber session.
Post-pre switch	Total number of times the subscriber session was switched from post-authentication to pre-authentication phase.

Bulk Statistics

The following bulk statistics in the SaMOG schema support this feature:

Variable	Description	Data Type
mrme-non-eap-post-to-preauth-call-attempted	**Description:** Total number of non-EAP sessions attempted to move from post to pre-authentication phase. **Triggers:** Increments whenever a non-EAP session moves from post to pre-authentication phase is attempted. **Availability:** Per SaMOG Service **Type:** Counter	Int32
mrme-non-eap-post-to-preauth-call-success	**Description:** Total number of non-EAP sessions successfully moved from post to pre-authentication phase. **Triggers:** Increments whenever a non-EAP session successfully moved from post to pre- authorization phase. **Availability:** Per SaMOG Service **Type:** Counter	Int32
mrme-non-eap-post-to-preauth-call-failure	**Description:** Total number of non-EAP sessions that failed to be moved from post to pre-authentication phase due to internal errors, missing pre- authorization phase configurations, missing ACL, IP address pool, rulebase, and so on. **Triggers:** Increments whenever a non-EAP session fails to be created. **Availability:** Per SaMOG Service **Type:** Counter	Int32