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.

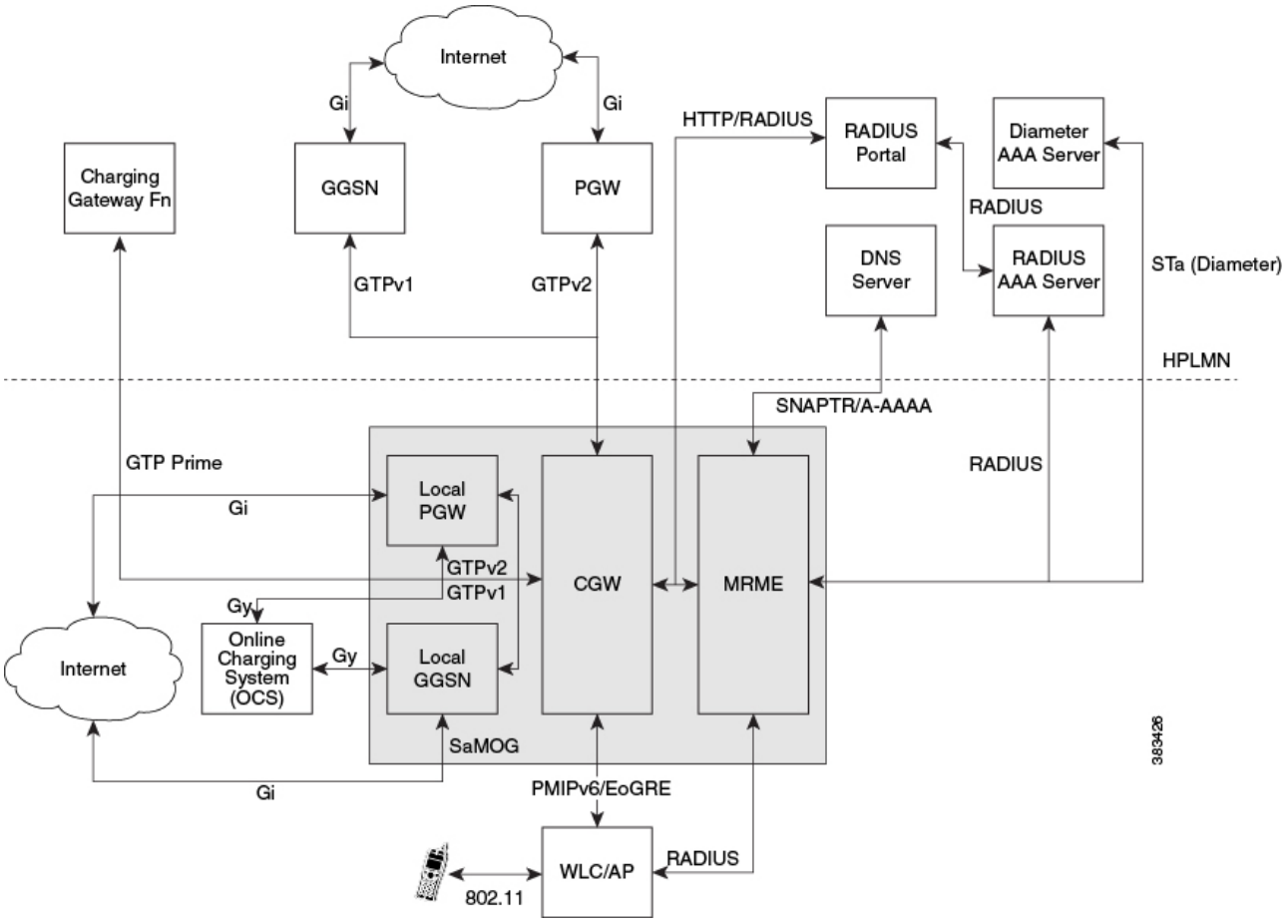
The SaMOG Gateway has the following key features:

- 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 ,VPC-DI, 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.

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

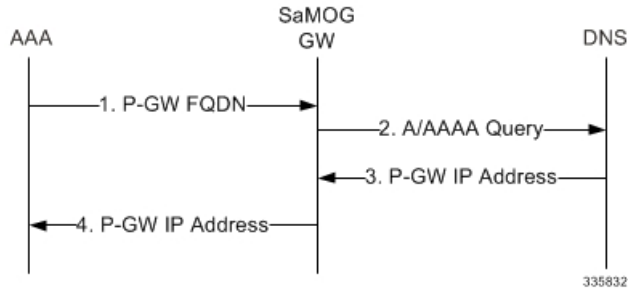


Table 1: P-GW Static Selection

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

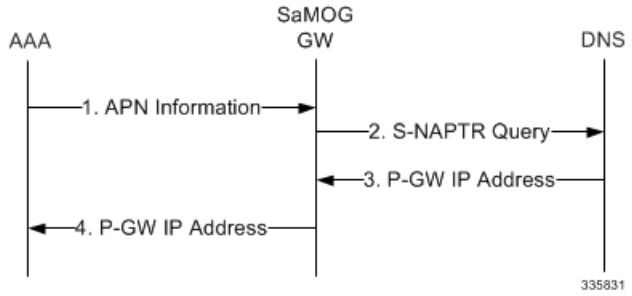


Table 2: P-GW Dynamic Selection

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

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.

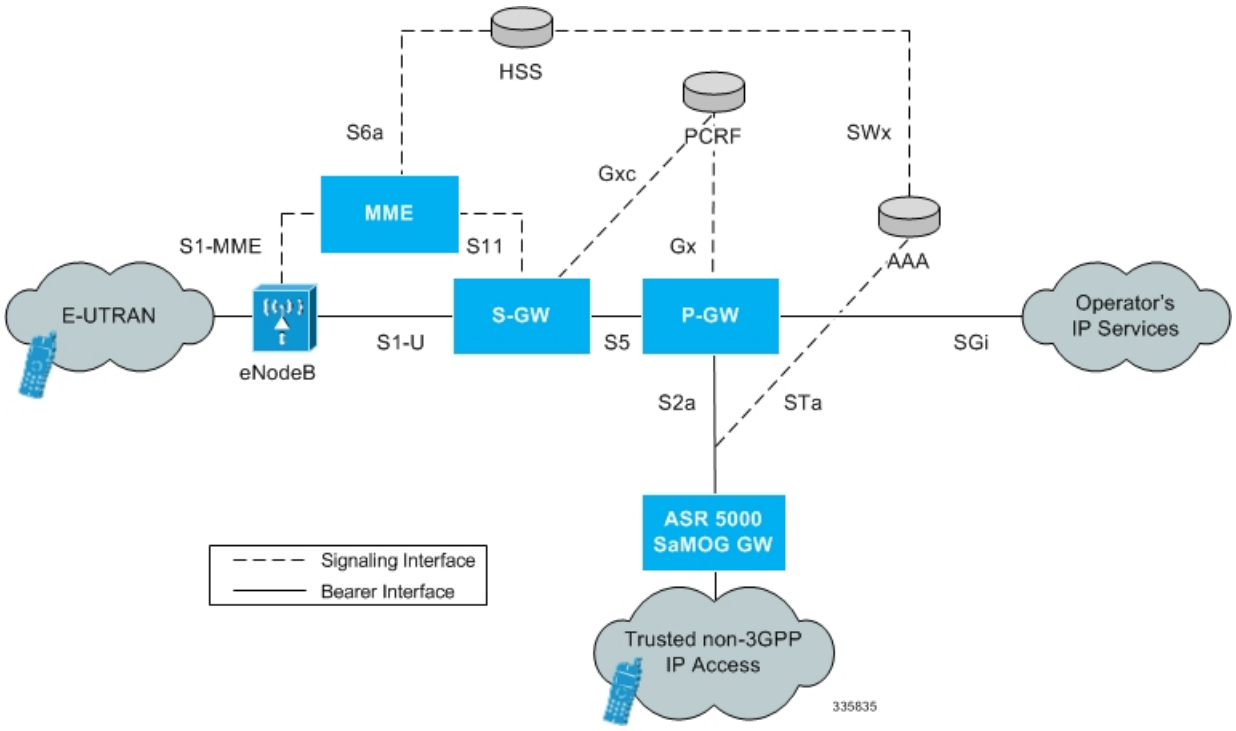
- **Mixed Mode Deployment:** For operators with infrastructure to deploy both 3G and 4G sessions, and wants to use SaMOG to provide services to both 3G and 4G subscribers.

  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

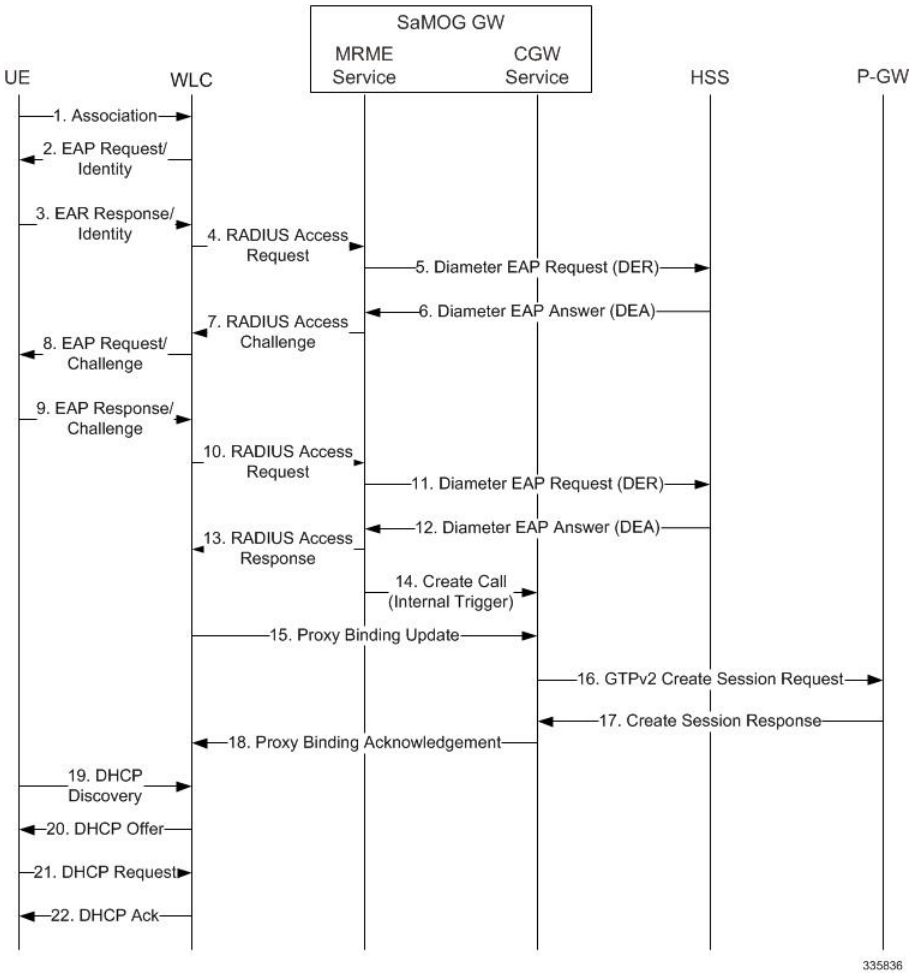


Table 5: SaMOG Gateway Session Establishment

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

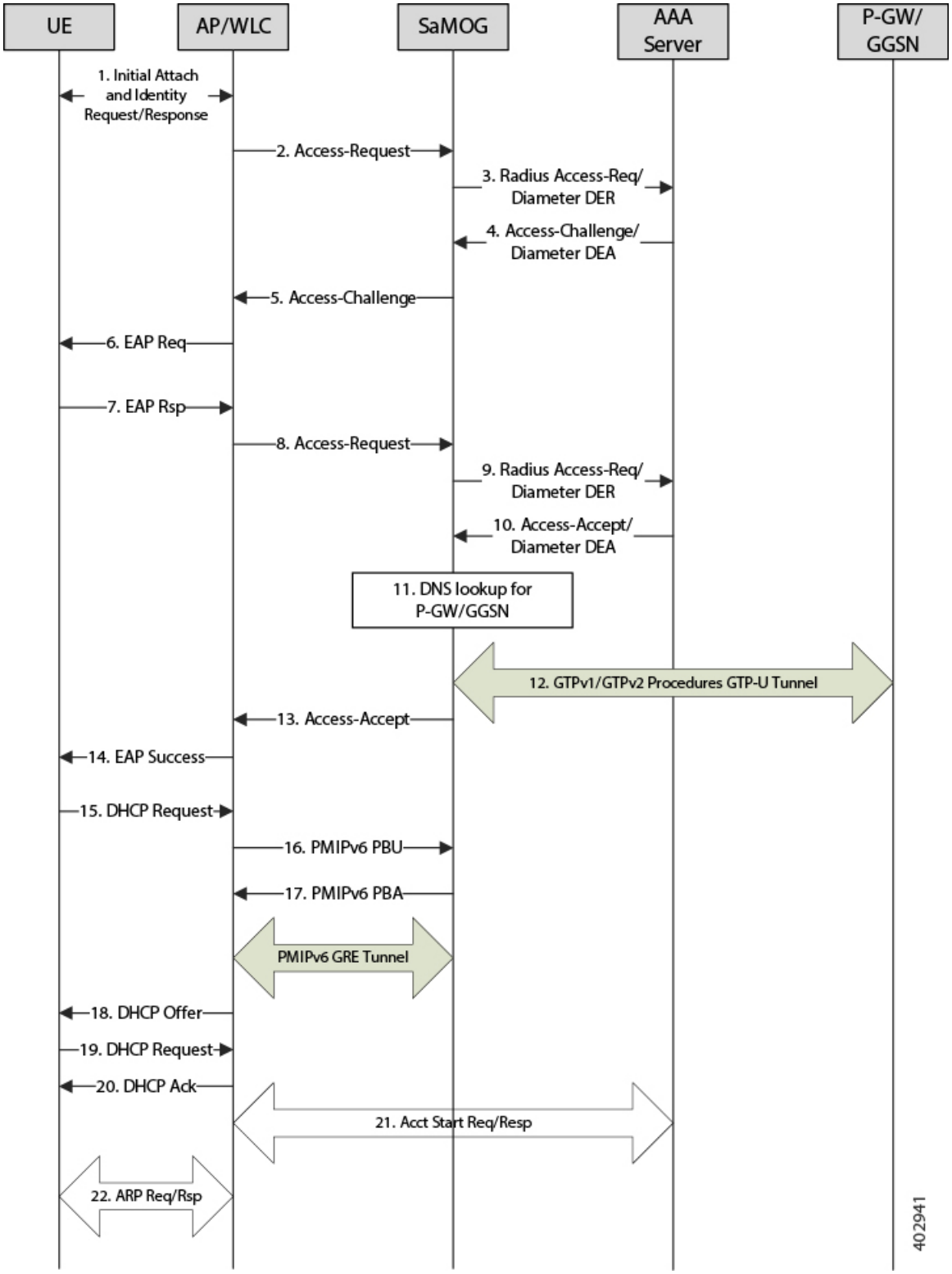


Table 6: SaMOG Gateway Session Establishment

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

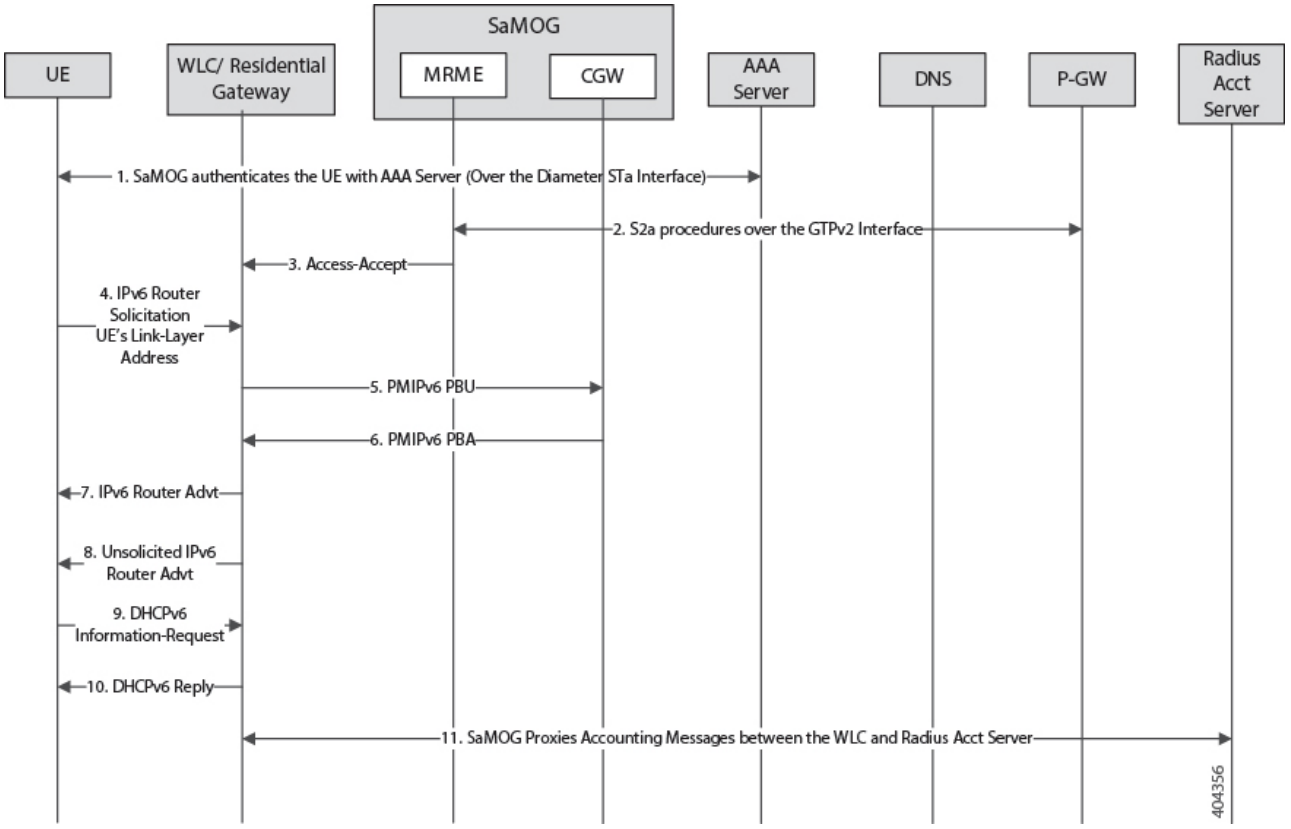


Table 7: SaMOG Gateway IPv6 prefix Over PMIPv6 Using SLAAC

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

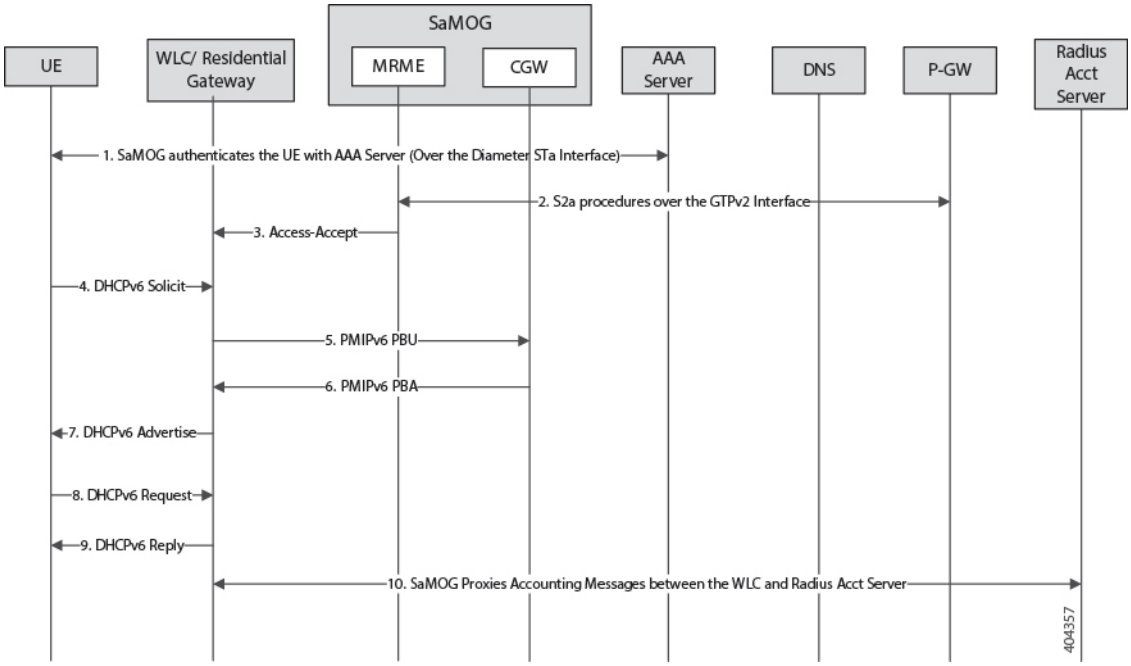


Table 8: SaMOG Gateway IPv6 prefix Over PMIPv6 Using Stateful DHCPv6

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

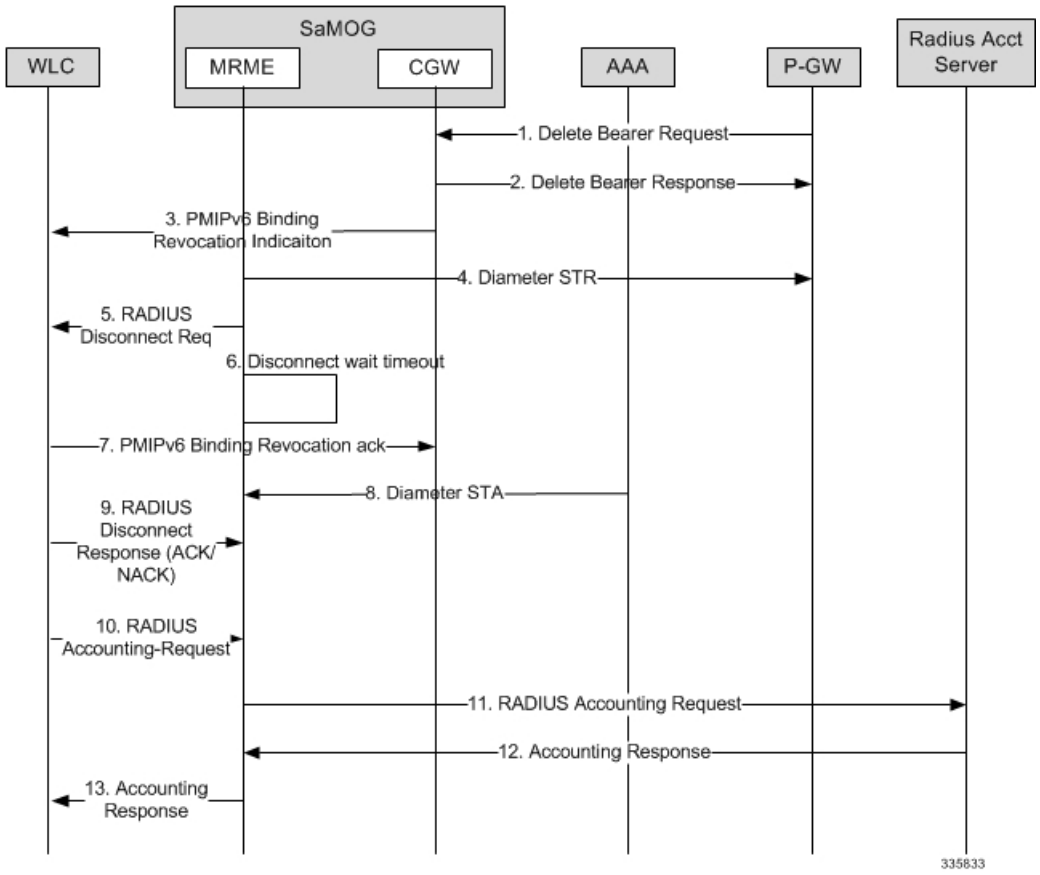


Table 10: P-GW Initiated Session Disconnection

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

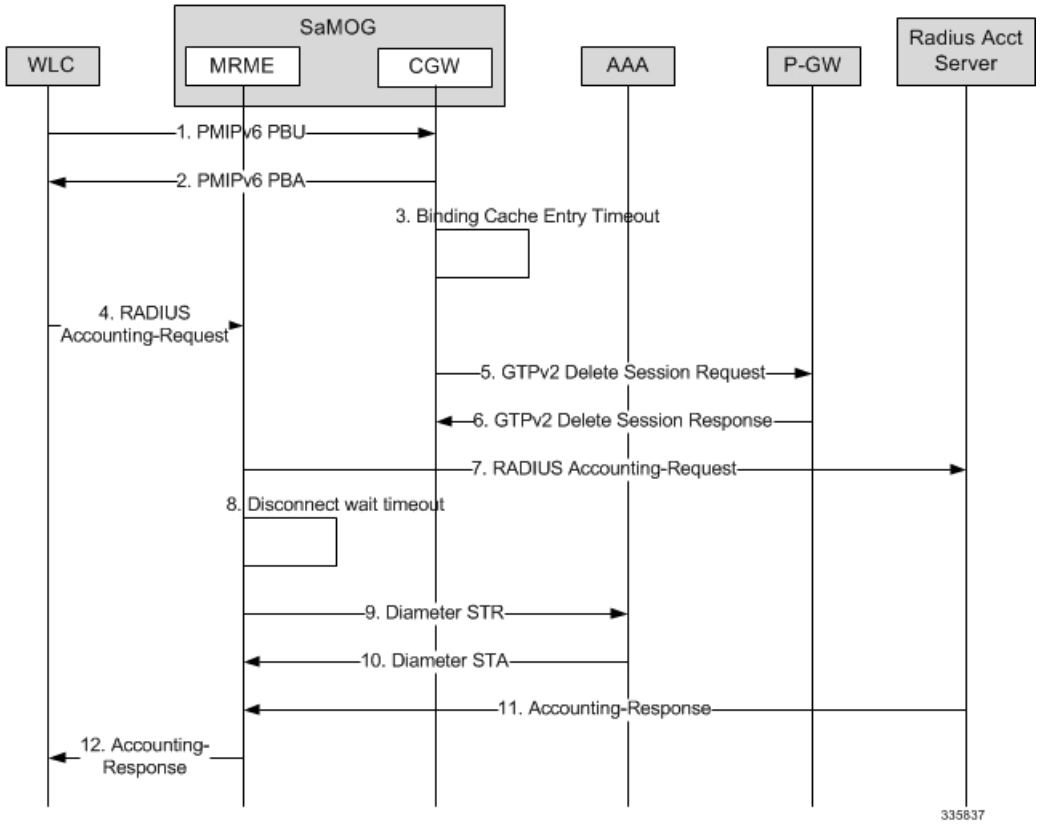


Table 11: WLC Initiated Session Disconnection

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

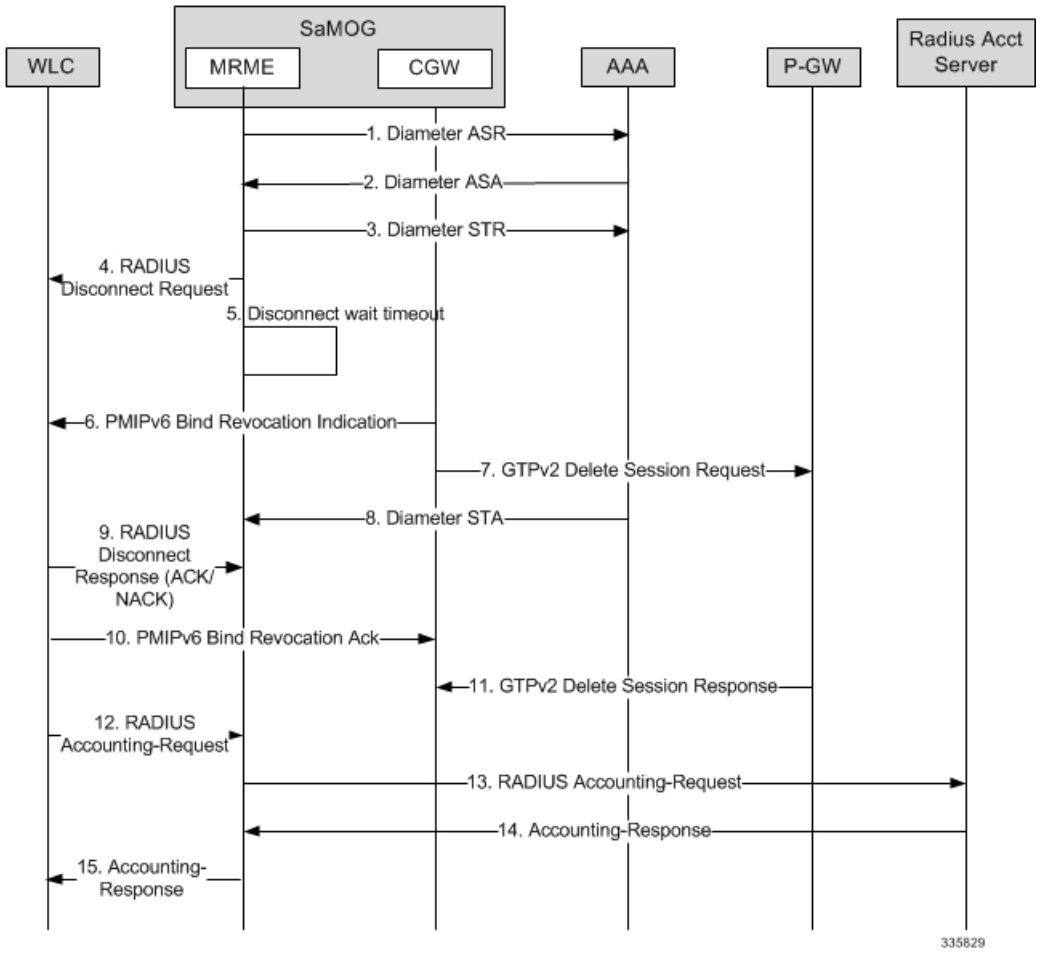


Table 12: AAA Server Initiated Session Disconnection

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

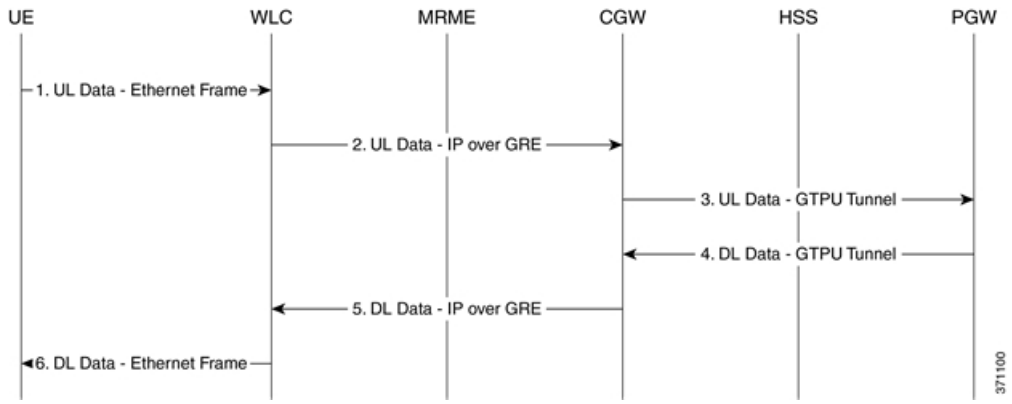


Table 13: SaMOG Gateway Data Flow

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.

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

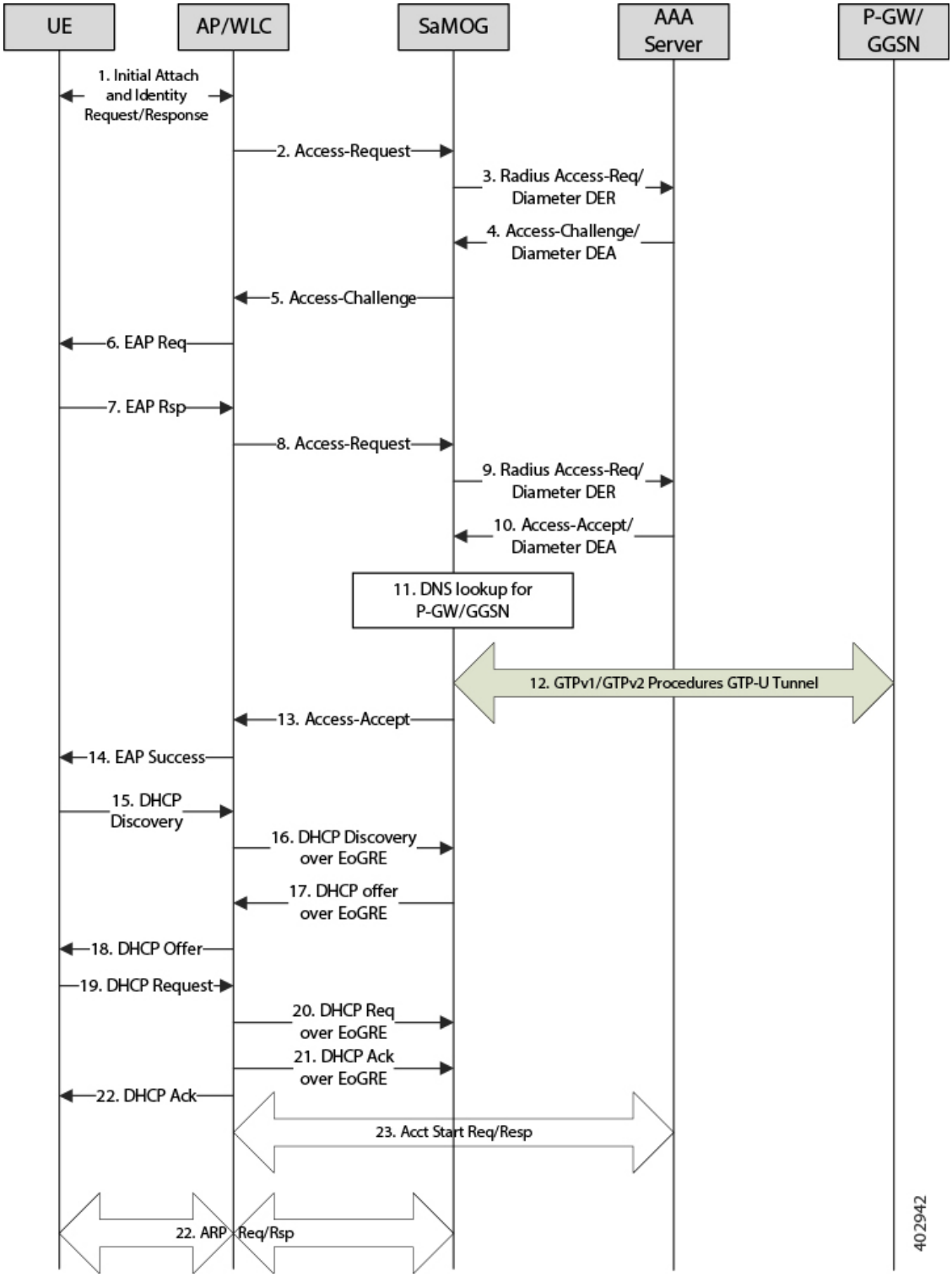


Table 14: SaMOG Gateway Session Establishment

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

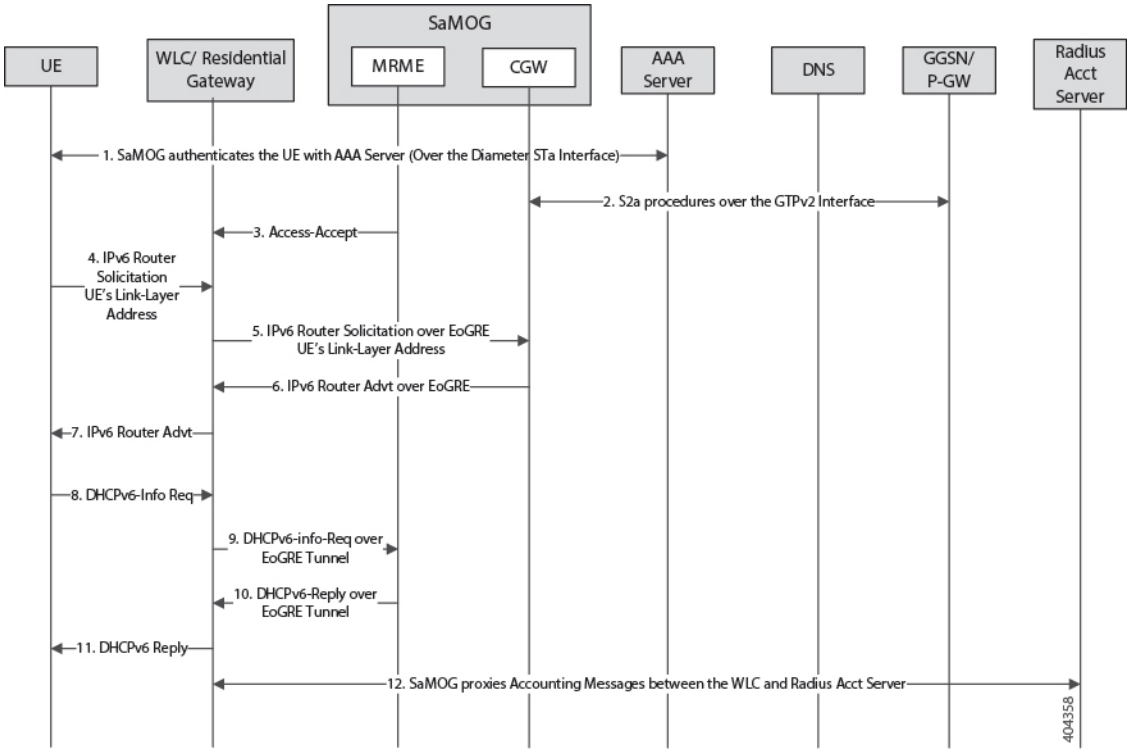


Table 15: SaMOG Gateway IPv6 prefix Over EoGRE Using SLAAC

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.

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.

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

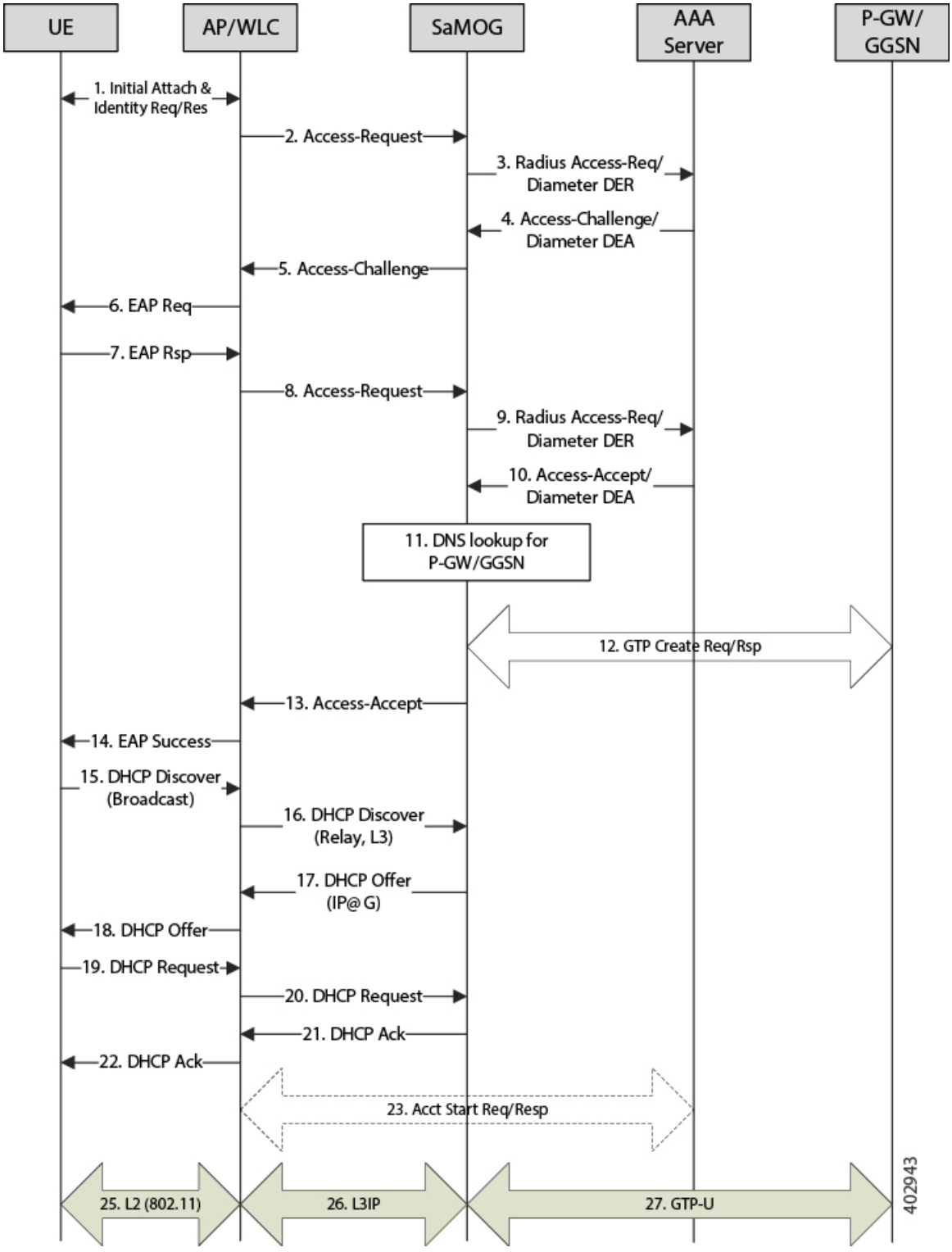


Table 17: Session Establishment for Layer 3 IP with DHCP Server

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

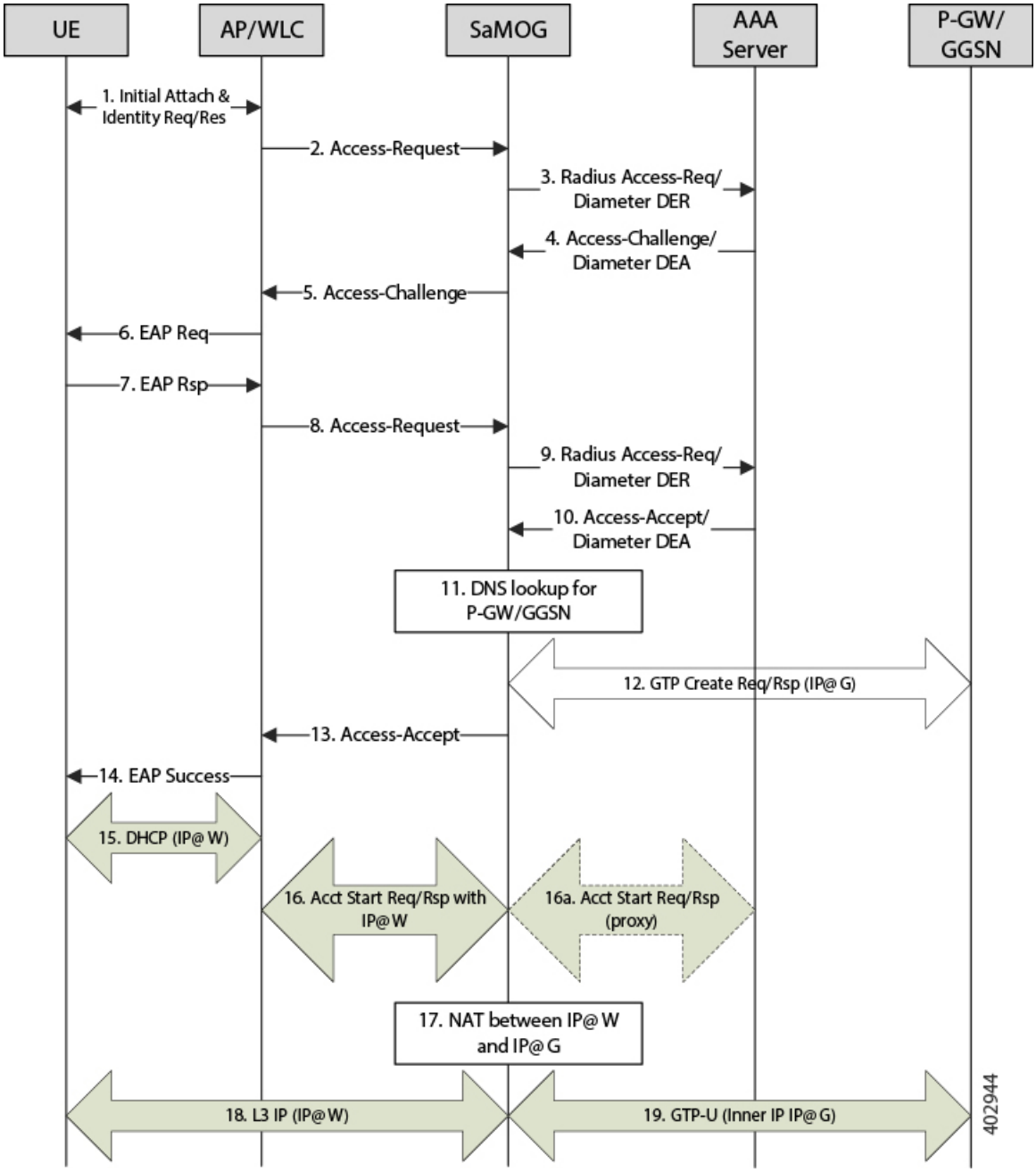


Table 18: Session Establishment for Layer 3 IP with IP@W

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)".