SaMOG Local Break Out

The SaMOG Local Breakout (LBO) feature enables subscribers to access the Internet without connecting to the EPC or 3G core. SaMOG currently supports the following LBO models:

Local Breakout - Enhanced

The Local Breakout (LBO) - Enhanced model is implemented by configuring a local P-GW or a local GGSN. All subscribers of a particular APN will be locally broken out without connecting to the P-GW or GGSN over the S2a interface. SaMOG performs IP allocation locally. This capability helps APNs whose data traffic can connect to the Internet immediately after authentication, instead of being sent to the 3GPP backbone.

License Requirements

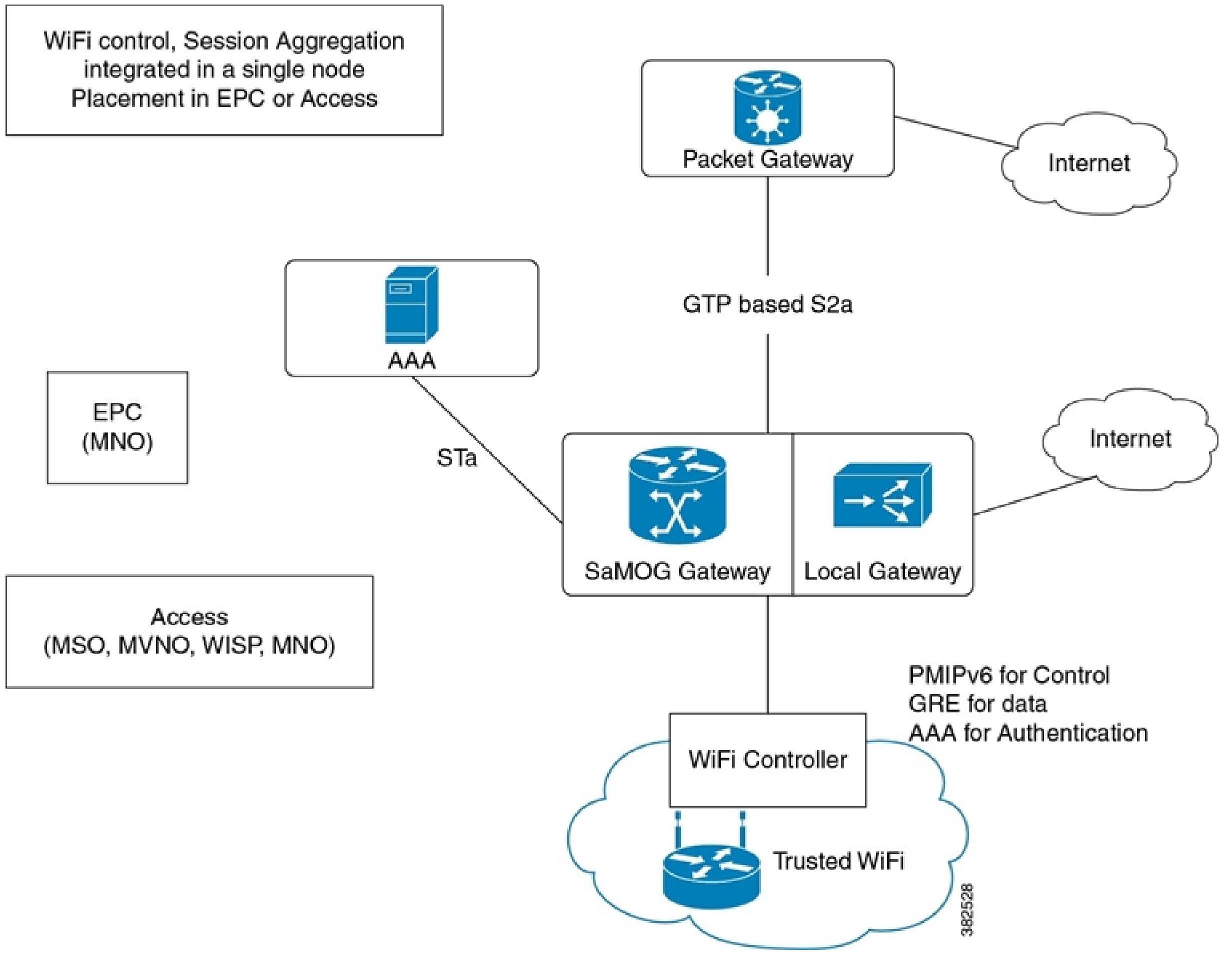
The Local Breakout - Enhanced model requires a separate LBO - Enhanced feature license. This license is mutually exclusive with the LBO - Basic and Flow-based LBO licenses.

SaMOG 3G license: Only a GGSN service can be configured and associated with the CGW service.

SaMOG general license: Either a GGSN service or a P-GW service can be configured and associated with the CGW service.

Overview

The following figure provides a high level architecture of the Local Breakout feature:



The APN provided by the AAA server is mapped to the locally configured P-GW or GGSN service IP. This eliminates the need for a DNS. The local P-GW or local GGSN assigns the IP using a locally configured IP pool after receiving the subscriber information from the AAA server. The subscriber information is received from the SaMOG service to the local P-GW service or local GGSN service through a GTP tunnel. This tunnel is set up within the same chassis.

The SaMOG Gateway decides whether an APN should be locally broken out based on the following parameters:

- A configuration in the APN profile indicating if LBO is enabled for the APN.
- Whether a "DEA-Flags" is received in the DEA messages on the STa interface. If DEA-Flags are received, SaMOG will verify if the "NSWO-Authorization" flag is set.

If the APN profile is configured for LBO, and either no "DEA-Flags" are received in the DEA messages, or "DEA-Flags" is received with the "NSWO-Authorization" flag set, SaMOG performs LBO for that APN.

LBO Decision based on AAA Policy and Local Policy

The decision on whether LBO can be done for a call is based on the following factors:

- A DIAMETER-based server can provide the following information:

  - The MIP6_FEATURE_VECTOR AVP in DEA message can have the GTPV2_SUPPORTED flag set to indicate that the AAA server authorizes the GTP call through the EPC core (GGSN/PGW).
  - The Bit 0 of the DEA_FLAG AVP (NSWO Authorization) is set to indicate that LBO is authorized for a session by the AAA server.

- The DIAMETER AAA server sends the APN information in the APN-Configuration AVP in DEA. This AVP may however be absent in case the AAA server authorizes only LBO, to indicate that any APN can be used for LBO for the subscriber.
- The operator can configure "local-offload" for each APN supporting LBO under the APN profile. However, the authorization from the AAA server will always be given preference over the local configuration. Local configuration will be used to take a decision when AAA server authorizes GTP as well as LBO for a call.

The following table indicates different scenarios where the occurance of LBO is determined:

AAA Indication	APN Received	Matching APN with LBO in the Local Configuration	LBO/GTP Call Decision
Both GTP and LBO NOT supported	—	—	Always an error condition
Only GTP Supported	No	—	Error Condition
	Yes	—	GTP Call setup with GGSN/P-GW
Only LBO Supported	No	Yes	LBO session established with the first APN with "local-offload" configured in local policy.
	No	No APN configured in local policy	Error Condition
	Yes	No	Error Condition
	Yes	Yes	LBO session established with received APN.
Both GTP and LBO Supported	No	—	Error Condition
	Yes	No	GTP session established with received APN.
	Yes	Yes	LBO session established with received APN.

Prepaid LBO Support

The SaMOG Gateway also supports Local Breakout (LBO) that enables time- and quota-based control to support prepaid subscribers. SaMOG interfaces with the Enhanced Charging Services (ECS) using the Gy interface for prepaid subscribers, and AAA for voucher-based subscribers. LBO for prepaid subscribers is supported on both PMIPv6 and EoGRE access types.

When a GTP session with the local P-GW or GGSN is set up, the local P-GW or GGSN service communicates with ECS to obtain the time and quota limits of the subscriber to establish connection. The time and quota limits are obtained with the Gy interface forwarding the CCR-I message to the Diameter Credit Control Application (DCCA) server. Until the time or volume quota is reached, the local P-GW or GGSN forwards the CCR-U message to DCCA in order to refresh the permitted time or volume quota allowed. When the UE terminates the session, the internal P-GW forwards the final service usage to ECS, and SaMOG completes the session.

Call Flows with Local Breakout - Enhanced

Attach Procedure

Figure 1: Attach Procedure Call Flow

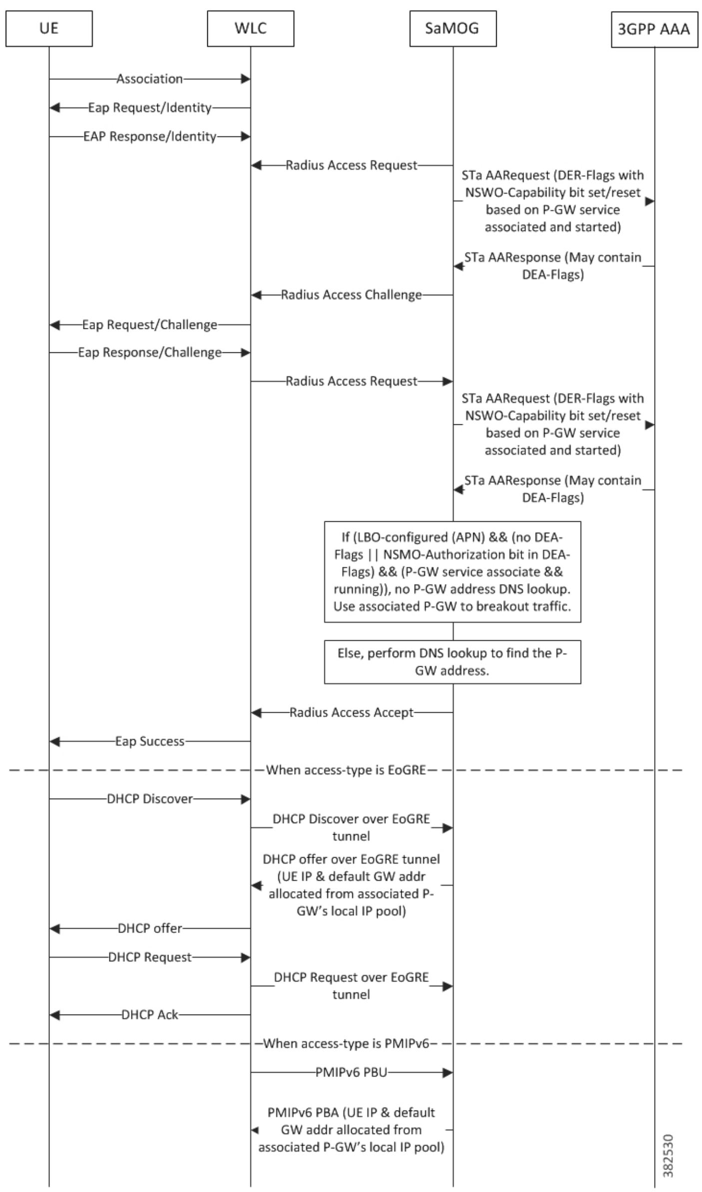


Table 1: Attach Procedure Call Flow Descriptions

Step	Description
1	UE associates with AP and WLC.
2	WLC starts EAP based authentication with UE and requests for the permanent identity of the user.
3	UE responds with the permanent identity (IMSI) stored on the SIM.
4	WLC requests SaMOG for authentication using Radius Access Request message.
5	SaMOG uses the STa interface towards 3GPP HSS to fetch subscriber authentication challenge. If LBO is enabled, SaMOG forwards DER-Flags (in the DER msg) with "NSWO-Capability" bit set to '1' to indicate to AAA that it supports LBO. Else, it sends the DER-Flags with "NSWO-Capability" bit set to '0'.
6	HSS returns the authentication parameters to SaMOG for the subscriber. The DEA message may contain DEA-Flags.
7	SaMOG sends Radius-Access-Challenge message to the WLC.
8	WLC in turn sends authentication challenge to UE.
9	UE responds with challenge response.
10	WLC initiates Radius Access Requests towards SaMOG with challenge response.
11	SaMOG originates STa AARequest towards HSS. If LBO is enabled, SaMOG sends DER-Flags (in the DER msg) with "NSWO-Capability" bit set to '1' to indicate to AAA that it supports LBO. Else, it sends the DER-Flags with "NSWO-Capability" bit set to '0'.
12	HSS authenticates the subscriber and also returns the subscriber profile information to MRME. The profile information will contain the Default QoS profile, Default APN, APN-AMBR, and Charging Characteristics.

Step	Description
13	If the APN profile requires LBO for the APN, either of the following conditions is met: • DEA-Flags not received • DEA-Flags received with the "NSWO-Authorization" bit set to 1. The P-GW service is then associated with the SaMOG service, and the associated P-GW IP address is used for LBO. Or, if a static IP address is provided by AAA, the address is used for allocation. If neither of the conditions above is met, DNS resolution is performed to determine the P-GW address.
14	SaMOG sends Radius-Access-Accept message towards WLC with some of the information mentioned in Step12 (APN Name, PDN-GW/LGW address).
15	EAP Success is sent to the UE.
16	For access-type EoGRE, UE sends DHCP Discover to SaMOG via. WLC. For access-type PIMP, WLC originates the PMIPv6 Proxy-Binding-Update message to SaMOG with the information from Step 13. Additionally, WLC allocates a GRE tunnel ID for downlink data transfer and includes it in PBU message.
17	For access-type EoGRE, the IP address allocated in Step 13 via. the associated P-GW is sent in the DHCP Offer msg. For access-type PIMPv6, the IP address allocated in Step 13 via. the associated P-GW is sent in the PBA message. The SaMOG service will setup the GRE tunnel and include the GRE tunnel ID for uplink data transfer.
18	For access-type EoGRE, the DHCP Request and DHCP Ack messages are forwarded to complete the IP address allocation. For access-type PMIPv6, WLC acts as DHCP server to the UE, and assigns the IP address received in PBA.

UE Initiated Detach

Figure 2: UE Initiated Detach Call Flow

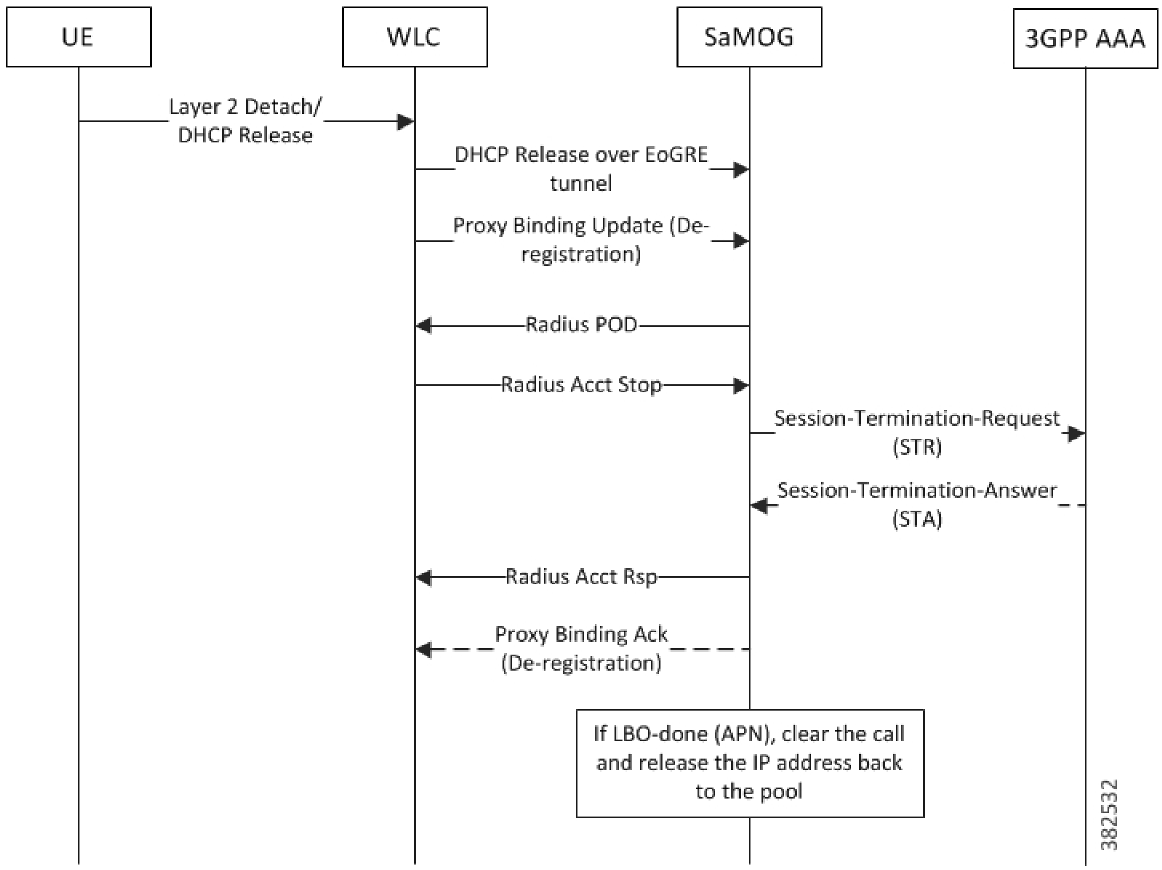


Table 2: UE Initiated Detach Call Flow Descriptions

Step	Description
1	UE initiates DHCP Release or L2 layer detach towards wireless network.
2	If access-type is EoGRE, UE sends a "DHCP Release" message to SaMOG. If the access-type is PMIPv6, WLC sends a PBU (De-registration) to SaMOG.
3	SaMOG sends a "Radius POD" to WLC.
4	WLC initiates Radius-Accounting-Stop message to SaMOG.
5-6	SaMOG in turn initiates STa Termination request to HSS, and receives a STa Termination response back from HSS.

Step	Description
7	SaMOG sends Radius-Accounting-Stop Response message to WLC.
8	For access-type PMIPv6, SaMOG sends back PMIPv6 Proxy Binding .
9	If the APN has been locally broken out, the allocated IP address is returned back to the P-GW IP pool. The session and associated IP-GRE/EoGRE tunnel is cleared.

AAA Initiated Detach

Figure 3: AAA Initiated Detach Call Flow

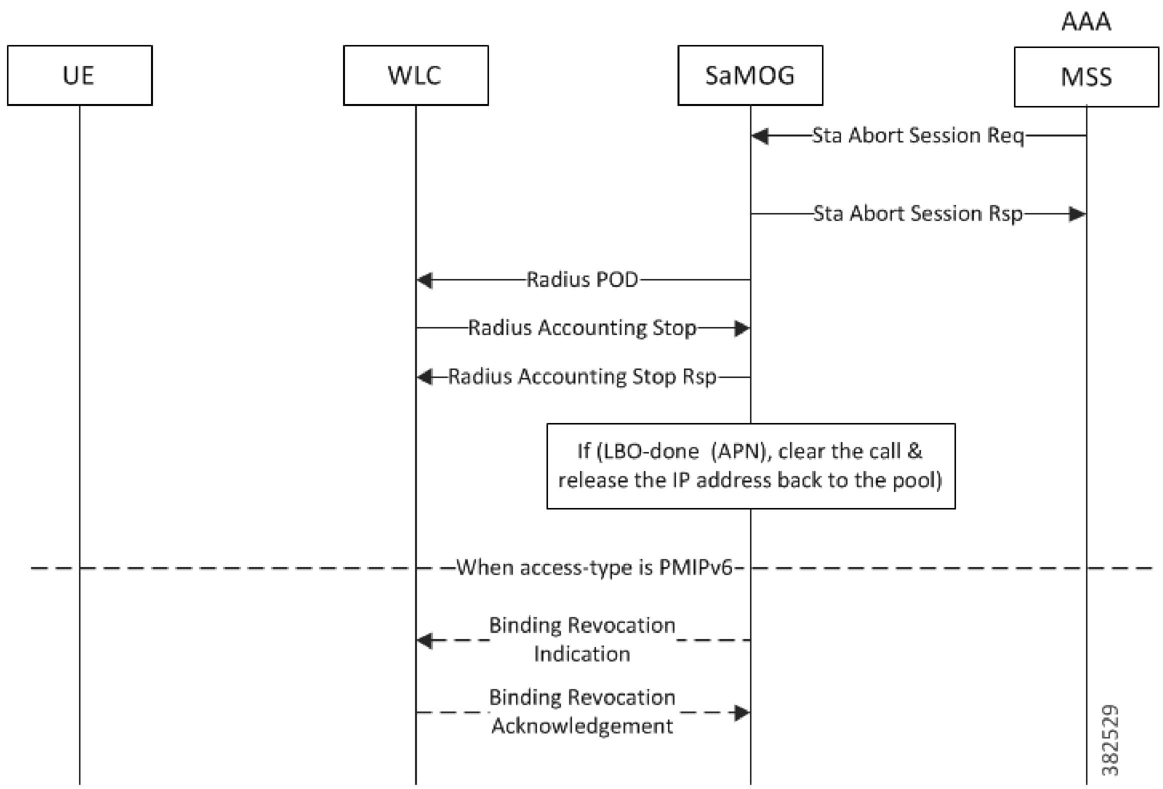


Table 3: AAA Initiated Detach Call Flow Descriptions

Step	Description
1	AAA sends STa Abort Session Req message to SaMOG.

Step	Description
2-3	SaMOG responds with an STa Abort Session Rsp message to AAA, and "Radius POD" message to WLC.
4	WLC initiates a Radius-Accounting-Stop Request message to SaMOG.
5	SaMOG sends Radius-Accounting-Stop Response message to WLC.
6	If the APN has been locally broken out, the allocated IP address is returned back to the P-GW IP pool. The session and associated IP-GRE/EoGRE tunnel is cleared.
7-8	If access-type is PMIPv6, SaMOG initiates a BRI message to WLC, and receives a BRA message back.

Limitations, Restrictions, and Dependancies

The following limitations, restrictions, and dependancies apply for the Local Breakout - Enhanced model:

- When an LBO session or GTP session is setup to an EPC/3G core, the mobility protocol or local breakout cannot be changed dynamically during reattach, even if the new authentication indicates the scope for such change. If the AAA server withdraws permission for the current mobility protocol/LBO, the session will be closed.
- In release 16.0, the Local Breakout feature supports 4G (GTPv2) sessions only.
- Prepaid support for Local Breakout feature using the AAA interface is limited to session-timeout AVP to control the session duration for voucher-based users. No additional support will be available on the AAA interface.
- For the LBO prepaid support, the SaMOG Gateway generates S-GW CDRs. Any packet drops on the interface P-GW service due to online credit control will still be counted in SGW-CDRs. However, operators can consider enabling P-GW CDRs in the internal P-GW as required.

Local Breakout - Basic

The Local Breakout (LBO) - Basic model enables SaMOG to connect the subscriber's User Equipment (UE) directly to the Internet without employing a local or external P-GW or GGSN service. The UE's IP address is allocated using an IP pool configured locally (or provided by the AAA server). The LBO basic model can be used with or without a Network Address Translation (NAT) service. If dynamic NAT is enabled for a subscriber, SaMOG allocates a global IP address from a pool, and replaces the source IP address of the data packet with this address.

License Requirements

The LBO - Basic model requires a separate feature license. This license is mutually exclusive with the LBO - Enhanced license, and can co-exist with the Flow-based LBO license.

Call Flows with Local Breakout - Basic

Local Breakout - Basic Session Setup

Figure 4: Local Breakout - Basic Session Setup Call Flow

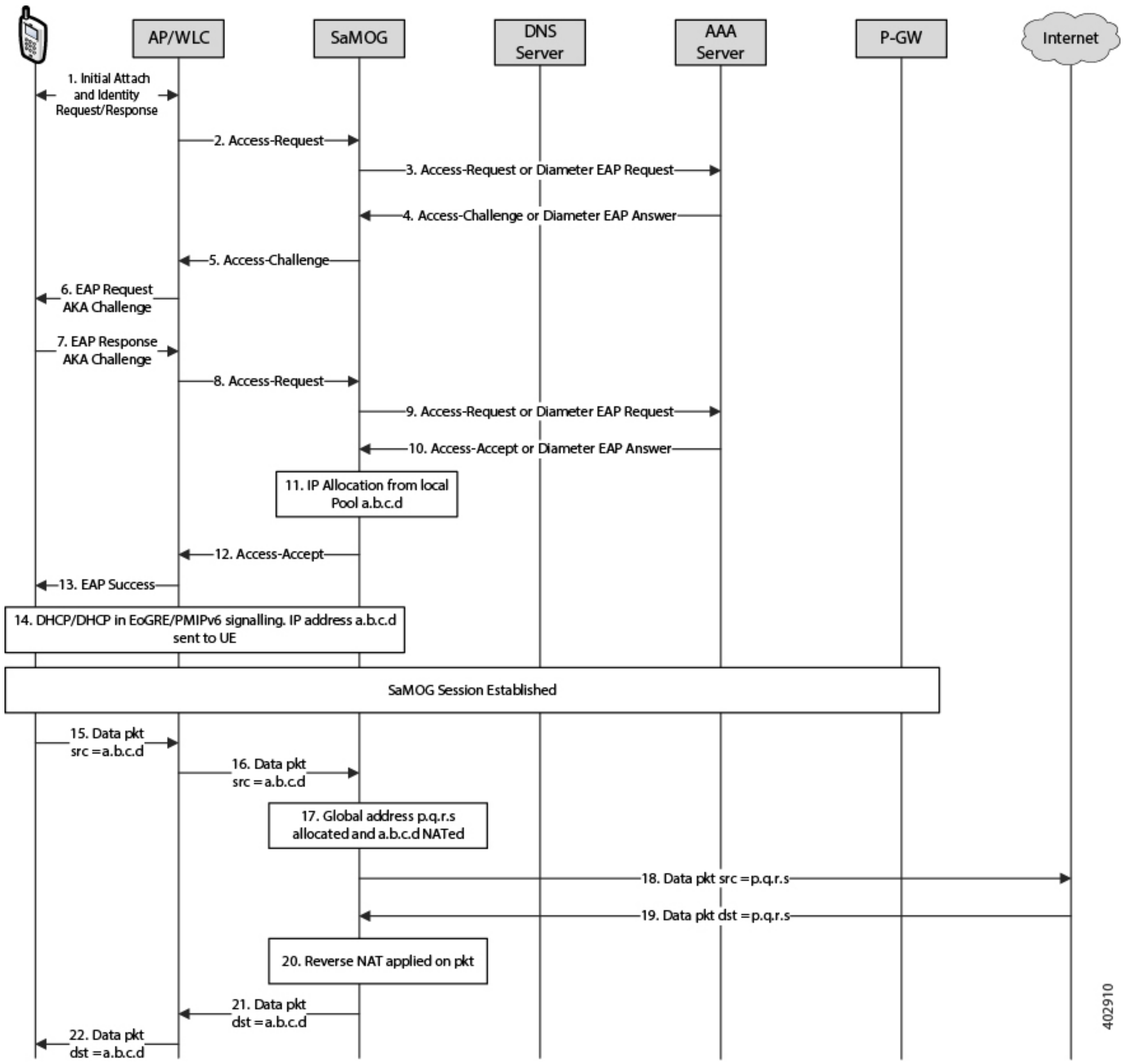


Table 4: Local Breakout - Basic Session Setup Call Flow Descriptions

Step	Description
1	UE initiates an initial attach procedure towards WLC.
2	WLC forms an Access-Request message with EAP-Identity payload, User-Name and Acct-Session-Id, and forwards the same to SaMOG.

Step	Description
3	SaMOG forms an Access-Request towards the RADIUS AAA server, or a Diameter EAP Request towards the STa AAA server using the attributes received from WLC.
4	AAA server performs EAP authentication and forwards the Access-Challenge/Diameter EAP Answer to SaMOG with the EAP payload.
5	SaMOG copies the EAP payload to the Access-Challenge towards WLC.
6	WLC forwards EAP Request with SIM Challenge towards UE.
7	UE sends EAP response with SIM Challenge response.
8	WLC sends Access-Request to SaMOG with EAP payload received from UE.
9	SaMOG sends Access-Request/Diameter EAP Request to AAA server with the EAP payload.
10	AAA server fetches the subscriber profile from HLR/HSS and validates the EAP Challenge response sent from UE. Access-Accept/Diameter EAP Answer is sent to SaMOG with user profile and EAP Success payload. SaMOG saves the user profile information. The AAA server authorizes local offload for the subscriber and the APN provided by AAA server has local-offload enabled.
11	SaMOG marks the session as an LBO - Basic candidate and allocates an IP address (a.b.c.d) from the local pool corresponding to the pool name received from AAA or configured under APN if the AAA server has not supplied any pool name.
12	SaMOG sends Access-Accept to the WLC with EAP-Success payload.
13	WLC forwards the EAP-Success to the UE.

Step	Description
14	DHCP or PMIPv6 messaging is then initiated to setup the data path. The UE IP address (a.b.c.d), DNS server address and default router address is supplied to the WLC/UE in DHCP or PMIPv6 (PBA) message. Once the WLC learns the UE IP address, it sends an Accounting-Start message containing the Framed-IP-Address attribute to SaMOG. SaMOG forwards it to the AAA accounting server, and the response from the accounting server is forwarded back to WLC.
15	Uplink data packet with the source IP address (a.b.c.d) is sent to WLC through the CAPWAP tunnel by UE.
16	WLC encapsulates the same packet into GRE/EoGRE tunnel or as L3IP, and sends it to SaMOG.
17	SaMOG performs dynamic NAT on this packet, allocates a global IP address from a pool (p.q.r.s), and replaces the source IP address of data packet with this address.
18	SaMOG routes the modified packet to the Internet.
19	The downlink packet contains the destination address set to p.q.r.s from the Internet to SaMOG.
20	SaMOG performs a reverse NAT, and replaces the address (a.b.c.d) as the destination address of the packet.
21	The modified packet is forwarded through the GRE/EoGRE tunnel or as L3IP to WLC.
22	WLC forwards the packet to the UE.

Important If NAT policy is not applied for the session (i.e. if ACLs are not provided, or if Rulebase is not provided, or if Rulebase doesn't contain NAT policy), the uplink data packets are directly offloaded to the Internet without NATting. and consequently reverse NAT is not applied for downlink packets from Internet, as NAT is not mandatory for LBO Basic.

Flow-based Local Breakout

The Flow-based Local Breakout (LBO) model enables SaMOG to selectively offload certain user data directly to the Internet without employing an external or internal P-GW or GGSN service, and forward the remaining traffic to an external P-GW or GGSN (via. the S2a tunnel) depending on configured Layer 4 rules. The User

Equipment's (UE) IP address is allocated by the external P-GW or GGSN service. SaMOG applies NAT addressing to all traffic that are offloaded directly to the Internet to differentiate between packets intended for local offload, and packets intended to be forwarded to P-GW or GGSN.

License Requirements

The Flow-based LBO model requires a separate feature license. This license is mutually exclusive with the LBO - Enhanced license, and can co-exist with the LBO - Basic license.

Flow-based LBO models

SaMOG applies Layer 4 rules to the data traffic using Access Control Lists (ACLs) to determine the part of traffic to be offloaded directly or sent to the P-GW or GGSN service. This decision can be based off an ACL whitelist or an ACL blacklist. While the ACL whitelist identifies the data to be forwarded to the P-GW or GGSN service, the ACL blacklist identifies the data to be locally offloaded.

Flow-based LBO using a Whitelist

A flow-based LBO using a whitelist is ideal in situations when a subscriber signs up for some premium content, and this content must be charged differently. SaMOG uses the ACL to route all traffic intended for the premium content server to be forwarded to P-GW or GGSN where special charging is applied using the Gx/Gy interface. SaMOG offloads the rest of the traffic that does not match the ACL directly to the Internet.

Flow-based LBO using a Blacklist

A flow-based LBO using blacklist is ideal in situations when SaMOG is deployed in a vicinity where a large number of subscribers access the same content (for example, a streaming video of an event in a stadium where the server is locally hosted). SaMOG offloads this content directly from the local server, and all other data traffic is routed to the P-GW or GGSN service.

Call Flows with Flow-based Local Breakout

Flow-based Local Breakout - Whitelist

Figure 5: Flow-based Local Breakout - Whitelist Call Flow

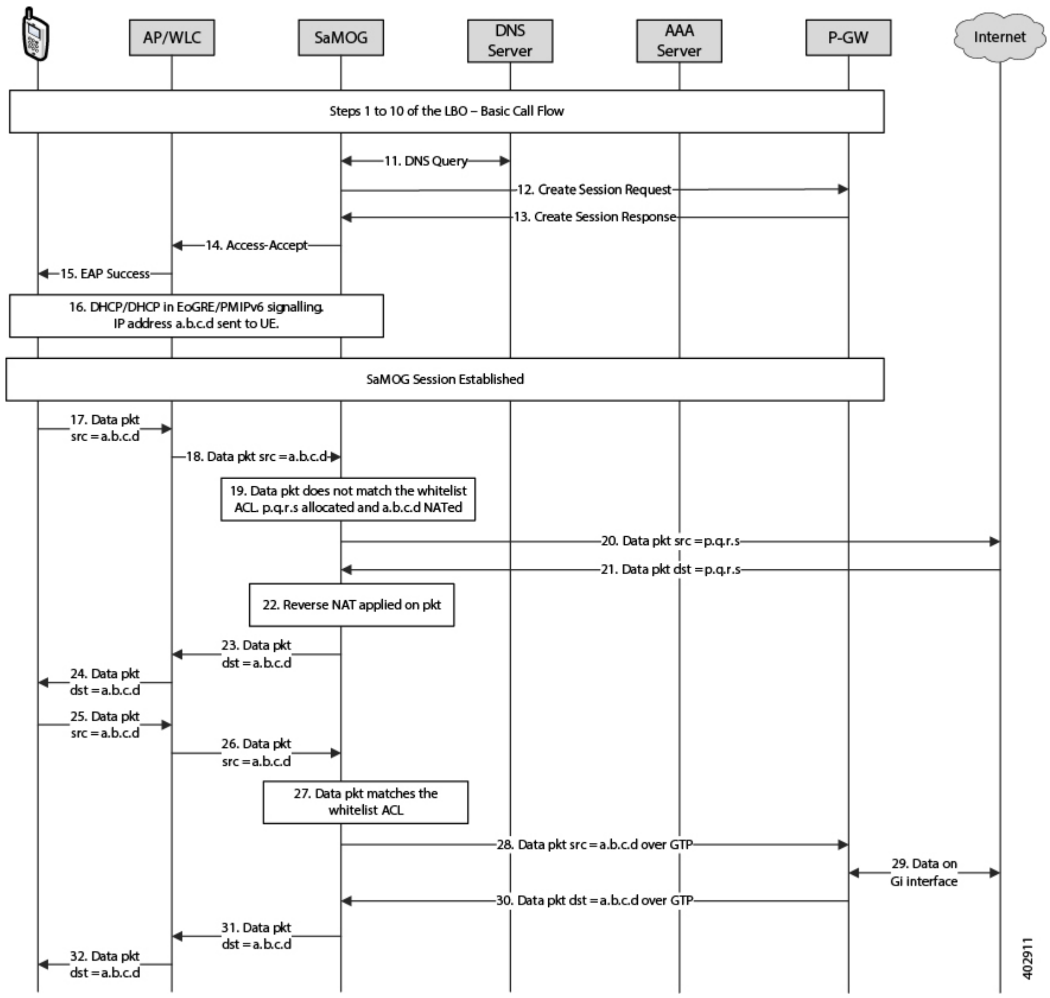


Table 5: Flow-based LBO - Whitelist Call Flow Descriptions

Step	Description
1	UE initiates an initial attach procedure towards WLC.
2	WLC forms an Access-Request message with EAP-Identity payload, User-Name and Acct-Session-Id, and forwards the same to SaMOG.
3	SaMOG forms an Access-Request towards the RADIUS AAA server, or a Diameter EAP Request towards the STa AAA server using the attributes received from WLC.

Step	Description
4	AAA server performs EAP authentication and forwards the Access-Challenge/Diameter EAP Answer to SaMOG with the EAP payload.
5	SaMOG copies the EAP payload to the Access-Challenge towards WLC.
6	WLC forwards EAP Request with SIM Challenge towards UE.
7	UE sends EAP response with SIM Challenge response.
8	WLC sends Access-Request to SaMOG with EAP payload received from UE.
9	SaMOG sends Access-Request/Diameter EAP Request to AAA server with the EAP payload.
10	AAA server fetches the subscriber profile from HLR/HSS and validates the EAP Challenge response sent from UE. Access-Accept/Diameter EAP Answer is sent to SaMOG with user profile and EAP Success payload. SaMOG saves the user profile information. The AAA server authorizes local offload for the subscriber and the APN provided by AAA server has flow-based LBO enabled. The AAA server may also provide a rulebase name that is configured in SaMOG and has the forwarding and NAT policy. The forwarding and NAT policy in turn has an ACL configured to identify the packets to be forwarded to the EPC core.
11	SaMOG performs DNS query with the DNS server and obtains the P-GW IP address.
12	SaMOG sets up the GTP session with PGW by sending a Create Session Request message to PGW.
13	PGW responds with a Create Session Response message and responds with the allocated UE IP address (a.b.c.d).
14	SaMOG sends Access-Accept to the WLC with EAP-Success payload.
15	WLC forwards the EAP-Success to the UE.

Step	Description
16	DHCP or PMIPv6 messaging is then initiated to setup the data path. The UE IP address (a.b.c.d), DNS server address and default router address is supplied to the WLC/UE in DHCP or PMIPv6 (PBA) message. Once the WLC learns the UE IP address, it sends an Accounting-Start message containing the Framed-IP-Address attribute to SaMOG. SaMOG forwards it to the AAA accounting server, and the response from accounting server is forwarded back to WLC.
17	The uplink data packet with the source IP address (a.b.c.d) is sent to WLC through the CAPWAP tunnel by UE
18	WLC encapsulates the same packet into GRE/EoGRE tunnel and forwards it to SaMOG.
19	SaMOG matches this packet with the ACL configured in the forward and NAT policy. Here, the packet does not match the ACL. SaMOG performs dynamic NAT on this packet. It allocates a global IP address from a pool (p.q.r.s) and replaces the source IP address of the data packet with this address.
20	SaMOG routes the modified packet to the Internet.
21	The downlink packet contains the destination address set to p.q.r.s from the Internet to SaMOG.
22	SaMOG performs a reverse NAT and replaces the address (a.b.c.d) as the destination address of the packet.
23	The modified packet is forwarded to the WLC over GRE/EoGRE tunnel.
24	The WLC forwards the packet to UE.
25	Another uplink data packet with the source IP address (a.b.c.d) is sent to WLC through the CAPWAP tunnel by UE.
26	WLC encapsulates the same packet into GRE/EoGRE tunnel and sends it to SaMOG
27	SaMOG matches this packet with the ACL configured in the forward and NAT policy. Here, the packet does match the ACL.

Step	Description
28	SaMOG then routes the packet to PGW over the GTP tunnel.
29	PGW processes the packet and sends it to the Internet over the Gi interface, and receives a downlink packet from the Internet.
30	The downlink packet comes with the destination address set to a.b.c.d from PGW to SaMOG over the GTP tunnel.
31	The packet is forwarded to the WLC through the GRE/EoGRE tunnel.
32	WLC forwards the packet to UE.

Flow-based Local Breakout - Blacklist

Figure 6: Flow-based Local Breakout - Blacklist Call Flow

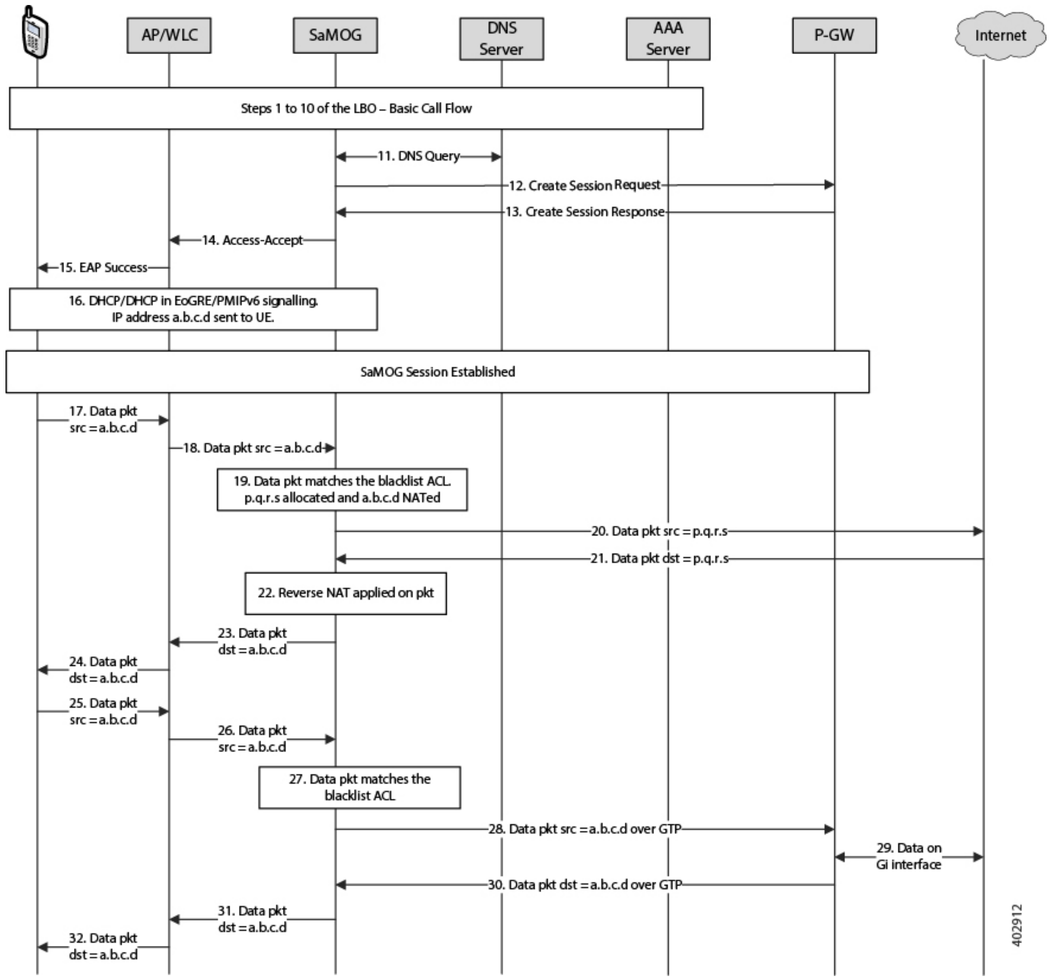


Table 6: Flow-based LBO - Blacklist Call Flow Descriptions

Step	Description
1	UE initiates an initial attach procedure towards WLC.
2	WLC forms an Access-Request message with EAP-Identity payload, User-Name and Acct-Session-Id, and forwards the same to SaMOG.
3	SaMOG forms an Access-Request towards the RADIUS AAA server, or a Diameter EAP Request towards the STa AAA server using the attributes received from WLC.

Step	Description
4	AAA server performs EAP authentication and forwards the Access-Challenge/Diameter EAP Answer to SaMOG with the EAP payload.
5	SaMOG copies the EAP payload to the Access-Challenge towards WLC.
6	WLC forwards EAP Request with SIM Challenge towards UE.
7	UE sends EAP response with SIM Challenge response.
8	WLC sends Access-Request to SaMOG with EAP payload received from UE.
9	SaMOG sends Access-Request/Diameter EAP Request to AAA server with the EAP payload.
10	AAA server fetches the subscriber profile from HLR/HSS and validates the EAP Challenge response sent from UE. Access-Accept/Diameter EAP Answer is sent to SaMOG with user profile and EAP Success payload. SaMOG saves the user profile information. The AAA server authorizes local offload for the subscriber and the APN provided by AAA server has flow-based LBO enabled. The AAA server may also provide a rulebase name that is configured in SaMOG and has the forwarding and NAT policy. The forwarding and NAT policy in turn has an ACL configured to identify the packets to be forwarded to the Internet directly.
11	SaMOG performs DNS query with the DNS server and obtains the P-GW IP address.
12	SaMOG sets up the GTP session with PGW by sending a Create Session Request message to PGW.
13	PGW responds with a Create Session Response message and responds with the allocated UE IP address (a.b.c.d).
14	SaMOG sends Access-Accept to the WLC with EAP-Success payload.
15	WLC forwards the EAP-Success to the UE.

Step	Description
16	DHCP or PMIPv6 messaging is then initiated to setup the data path. The UE IP address (a.b.c.d), DNS server address and default router address is supplied to the WLC/UE in DHCP or PMIPv6 (PBA) message. Once the WLC learns the UE IP address, it sends Accounting-Start message containing the Framed-IP-Address attribute to SaMOG. SaMOG forwards it to the AAA accounting server, and the response from accounting server is forwarded back to WLC.
17	The uplink data packet with the source IP address (a.b.c.d) is sent to WLC through the CAPWAP tunnel by UE.
18	WLC encapsulates the same packet into GRE/EoGRE tunnel and forwards it to SaMOG.
19	SaMOG matches this packet with the ACL configured in the forward and NAT policy. Here, the packet matches the ACL. SaMOG performs dynamic NAT on this packet. It allocates a global IP address from a pool (p.q.r.s) and replaces the source IP address of the data packet with this address.
20	SaMOG routes the modified packet to the Internet.
21	The downlink packet contains the destination address set to p.q.r.s from the Internet to SaMOG.
22	SaMOG performs a reverse NAT and replaces the address (a.b.c.d) as the destination address of the packet.
23	The modified packet is forwarded to the WLC over GRE/EoGRE tunnel.
24	The WLC forwards the packet to UE.
25	Another uplink data packet with the source IP address (a.b.c.d) is sent to WLC through the CAPWAP tunnel by UE.
26	WLC encapsulates the same packet into GRE/EoGRE tunnel and sends it to SaMOG
27	SaMOG matches this packet with the ACL configured in the forward and NAT policy. Here, the packet does not match the ACL.

Step	Description
28	SaMOG then routes the packet to PGW over the GTP tunnel.
29	PGW processes the packet and sends it to the Internet over the Gi interface, and receives a downlink packet from the Internet.
30	The downlink packet comes with the destination address set to a.b.c.d from PGW to SaMOG over the GTP tunnel.
31	The packet is forwarded to the WLC through the GRE/EoGRE tunnel.
32	WLC forwards the packet to UE.

Limitations, Restrictions, and Dependancies

The following limitations, restrictions, and dependancies apply for the Local Breakout - Basic model:

- For an L3IP access type, the IP address assigned by the P-GW or GGSN must be routable on the WLAN. SaMOG does not assign a separate IP address for the UE.
- The Flow-based LBO model will always require NAT to route the UE packets on the Internet directly.