RADIUS Accounting-based Session Creation

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

The following sections provide more detailed information:

Feature Description

Overview

The SaMOG Gateway can create sessions based on either of the following messages as a trigger:

RADIUS Access-Request messages: The Access Points (AP) or WLCs are configured with the SaMOG Gateway acting as the AAA Server. When the subscriber's user equipment (UE) performs an 802.11 association, these APs or WLCs trigger a RADIUS Access-Request message towards the SaMOG Gateway.

DHCP messages: The AP or WLC forwards DHCP messages (DHCP discover or DHCP Request) from the UE to the SaMOG Gateway over the EoGRE tunnel. The SaMOG Gateway uses this DHCP message as a trigger to initiate a session. This method of session creation is suited in networks where the AP or WLC is not capable of forwarding RADIUS messages.

RADIUS Accounting-based Session Creation

With the RADIUS Accounting-based Session Creation feature, sessions can be created when the APs forward a RADIUS Accounting-Start message with the allocated UE's IP address towards the accounting server. This method of session creation is suited in networks where the APs do not have EoGRE capabilities. These APs are configured with DHCP servers and the UE's IP address is allocated locally by the AP.

The SaMOG Gateway performs RADIUS-based authentication towards 3GPP AAA server by mapping parameters received in RADIUS Accounting request from the AP to a RADIUS Access-Request message towards the AAA server. The SaMOG Gateway perform APN-based local offload, using a Local P-GW for all accounting triggered sessions. The local P-GW allocates an IP address for the session. SaMOG performs

a static NAT between the UE's IP address (shared by the AP in the Framed-IP-Address attribute of the accounting message) and the IP address assigned by the local P-GW.

Relationship to Other Features

DHCP Triggered and RADIUS (Authentication)-based Session Creation

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

Session Recovery

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

Web Authorization

The SaMOG Gateway supports RADIUS Accounting-based session creation on the TAL phase of both Web Authorization and Optimized Web Authorization features. Session redirection is performed using the local P-GW.

How RADIUS Accounting-based Session Creation Works

Architecture

The following figure provides the deployment architecture for RADIUS Accounting-based session creation:

Figure 1: RADIUS Accounting-based Session Creation
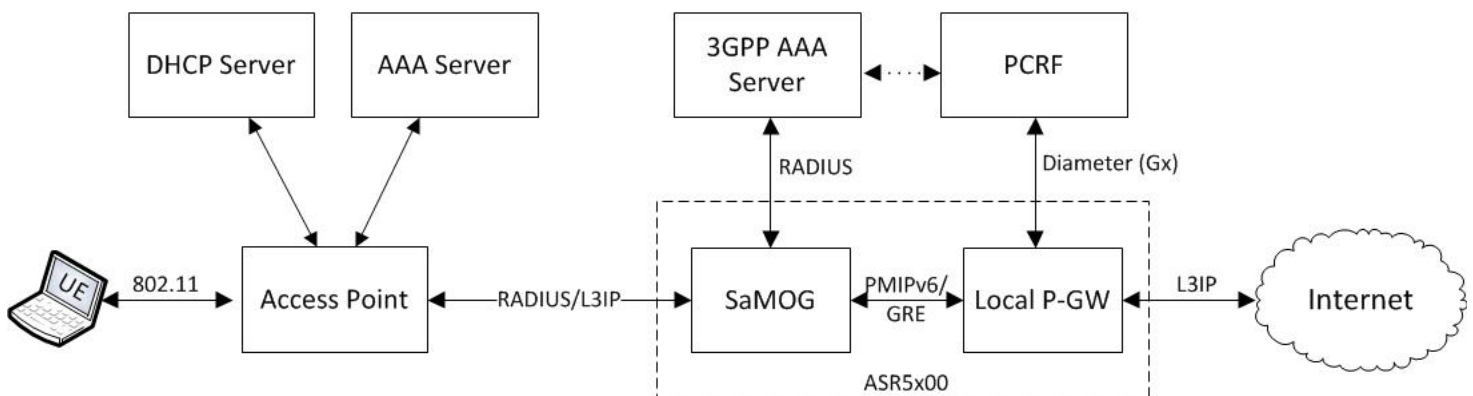
The following are the sequence of events for a RADIUS Accounting-based session creation deployment model:

1. The AP allocates an IP address from a local DHCP server. SaMOG acts as an Accounting server for the AP.

2. Once the IP address is allocated, the AP sends an Accounting Start message to SaMOG with the allocated IP address in the Framed-IP-Address attribute.

3. SaMOG accepts the Radius Accounting Start message as a session trigger and performs authentication with a 3GPP AAA server.

4. The AAA server sends the UE details (received in the Accounting message) to the PCRF, and also forwards the NAI information to SaMOG based on the UE location.

5. On successful authentication, SaMOG establishes a connection with the local P-GW using PMIPv6 control protocol and obtains the IP address.

6. SaMOG uses the NAI information received from the AAA server in the PMIPv6 PBU message. This information is used by the local P-GW in the Gx messaging towards PCRF during session creation.

7. The local P-GW sends the redirection rules and other policies to the local P-GW based on the NAI information.

8. Once the session with the local P-GW is successfully established, SaMOG installs a static NAT between the UE's IP address and the IP address provided by the local P-GW.

9. SaMOG can now respond to Accounting Start messages, and the UE starts sending data over L3IP access towards SaMOG.

10. This data then NATTed towards the local P-GW and routed to the internet or redirected by the local P-GW as per the installed policy.

11. The downlink data is sent to SaMOG by the local P-GW and a reverse NAT is performed before forwarding the packets to the AP.

Flows

Session Establishment

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

Figure 2: RADIUS Accounting-based Session Establishment Call Flow
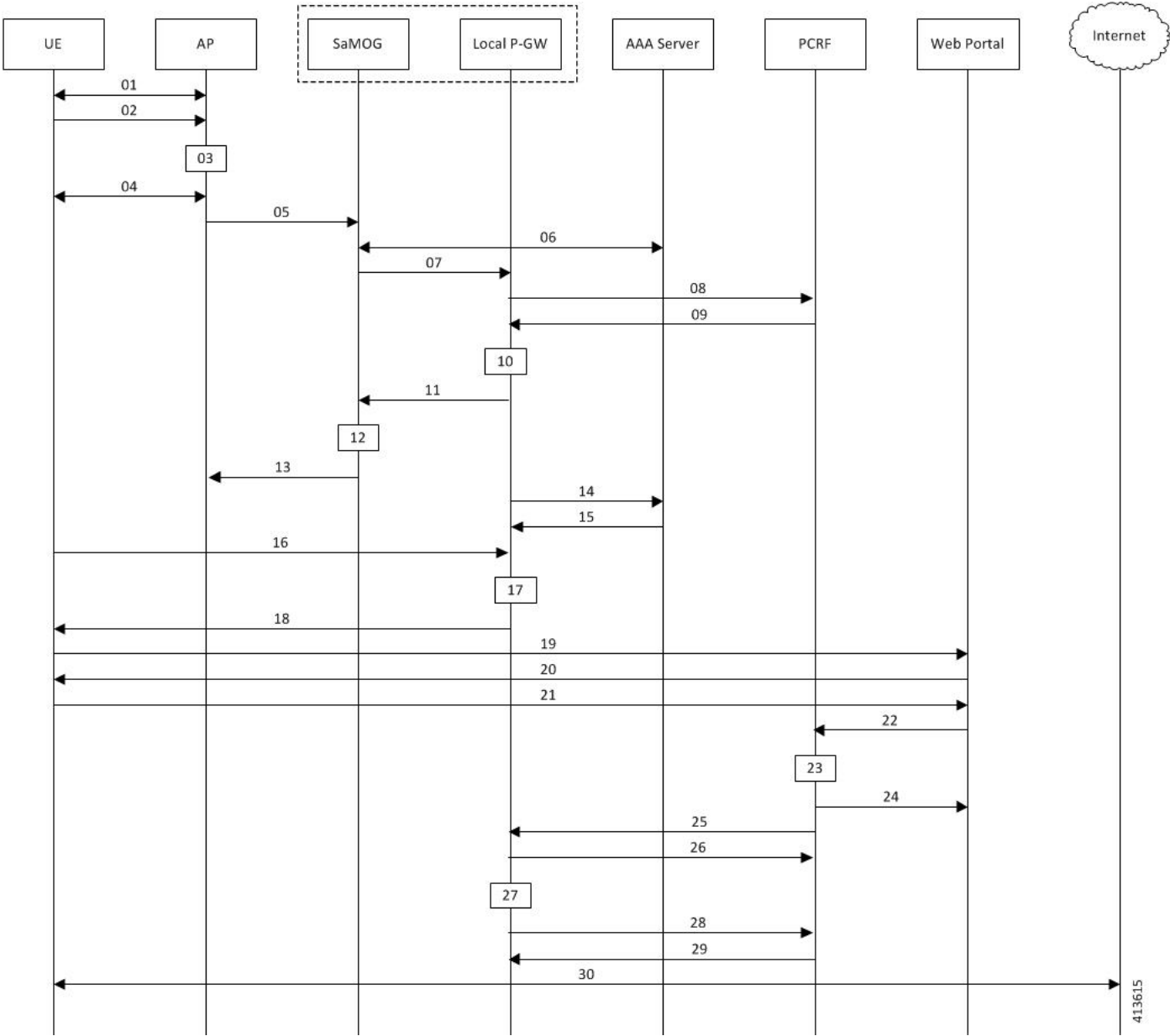
Table 1: RADIUS Accounting-based Session Establishment

Step	Description
01	UE performs 802.11 association with the AP and attaches to the open SSID.
02	UE sends DHCP Discover message to AP to get an IP address.
03	AP gets an IP address (For example, IP1) from a local DHCP server.

Step	Description
04	AP completes the DHCP transaction with the UE, and sends the IP (IP1) address to the UE in the DHCP offer/DHCP Reply message.
05	AP sends a Radius Accounting Start message to SaMOG with the following parameters: • UE MAC address in the Username and Calling Station-Id attribute. • Optional: VLAN ID in the NAS-Identifier attribute. • IP address (allocated by local DHCP server: IP1) in the Framed-IP-Address attribute. • AP-MAC and SSID in the Called-Station-Id attribute.
06	SaMOG caches the Accounting Start message and maps its contents to the Radius Access-Request message towards a AAA server. The Framed-IP-Address received in Accounting Start message is not sent towards the AAA server and the AP IP address (Radius endpoint address/source address of the Accounting Start message) is included in NAS-Port-Id attribute of the Access-Request. The AAA server determines that the UE MAC is not authenticated and sends Access-Accept message with an access point name (APN) and NAI in the MAC@realm format. These values are received using CS-AVPair attributes similar to DHCP triggered sessions.
07	SaMOG initiates a PMIPv6 Proxy Binding Update (PBU) message towards the local P-GW to setup the network side of the call. The MNID of the PBU is the NAI received from the AAA server.
08	The local P-GW sends CCR-I towards the PCRF, and includes the NAI/MNID received from SaMOG in the PBU message.
09	PCRF determines that the subscriber is not authenticated and sends a CCA-I with the L7 redirection rulebase name.
10	The local P-GW installs the L7 redirection rule and proceeds with session creation.
11	The local P-GW allocates an IP address (For example, IP2) for the UE and sends the IP address in the Proxy Binding Answer (PBA) message towards SaMOG.
12	SaMOG maps the static NAT between the IP address (IP1) received in the Accounting Start message from AP, and the IP address (IP2) sent by the local P-GW to the NAT table.
13	SaMOG completes session creation by sending the Accounting Response message to the AP.
14	The local P-GW sends an Accounting Start message towards the AAA server with the UE MAC and the Framed-IP-Address (with IP2).
15	The AAA server sends an Accounting Start response to the local P-GW.
16	The UE attempts to access the HTTP page, and the HTTP packet reaches the local P-GW through SaMOG. SaMOG performs static NAT to change the source IP address of the packet from IP1 to IP2 and forwards it to the local P-GW over the GRE tunnel.
17	As the L7 redirection rule on the local P-GW is active, HTTP packet is intercepted.

Step	Description
18	The local P-GW responds with a HTTP 302 response, and provides the URL of the authentication portal to the UE. SaMOG performs reverse NAT on this packet before forwarding it to the UE.
19	UE sends the HTTP GET request to the portal through SaMOG and the local P-GW.
20	The portal presents the login page to the UE to enter the username and password.
21	The subscriber enters the username and password to perform web authentication.
22	The portal shares the username, password and the source IP address (IP2) of the packet to the PCRF.
23	The PCRF validates the user credentials and marks the UE MAC corresponding to IP2 as authenticated.
24	The PCRF indicates authentication success to the portal. The portal then sends an HTTP 302 response to the UE with a redirect to the originally accessed web page.
25	The PCRF sends an RAR message on the Gx interface to indicate removal of redirection rule.
26	The local P-GW acknowledges the RAR message with an RAA message.
27	The local P-GW removes the L7 redirection rule for the UE session.
28	The local P-GW sends a CCR-U message to PCRF to get the quota information for the authenticated session.
29	The PCRF responds with a CCA-U message with the requested information.
30	UE now attempts to connect to the originally accessed web page again. As the L7 rule is not present at the local P-GW, the packets are sent to the Internet.

Standards Compliance

This feature complies with the following standard(s):

- RFC 2866 (RADIUS Accounting)

Configuring RADIUS Accounting-based Session Creation

Enabling RADIUS Accounting-based Session Creation Trigger

Use the following configuration to enable RADIUS Accounting-based session creation:

```
config
    context context_name
        twan-profile profile_name
```

```
                        session-trigger radius acct
                        end
```

Notes:

- Use the **default session-trigger** command to reset the configuration to its default value.

- **Default**: RADIUS (authentication)-based session trigger

Configuring Access Type and UE Address

Use the following configuration to configure the access type and UE address for RADIUS accounting-based session creation:

```
config
    context context_name
        twan-profile profile_name
            ue-address twan
            access-type ip
            end
```

Notes:

- Use the **ue-address twan** command to enable SaMOG to receive the TWAN UE address through the Accounting Start Framed-IP-Address message.

- • Use the **access-type ip** command to specify that all RADIUS clients under the TWAN profile will use the Layer 3 IP (L3IP) access type.

Monitoring and Troubleshooting RADIUS Accounting-based Session Creation

RADIUS Accounting-based Session Creation Show Command(s) and/or Outputs

show samog-service statistics

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

```
MRME Service Stats:
Radius Accounting Trigger Session Stats:
Total Attempted:     0
Total Setup:         0
Total Current:       0
Total Released:      0
Total Aborted:       0
Total Disconnected:  0
```

Table 2: **show samog-service statistics** *Command Output Descriptions*

Field	Description
Radius Accounting Trigger Session Stats:	
Total Attempted	Total number of Accounting-triggered MRME calls attempted.
Total Setup	Total number of Accounting-triggered MRME calls that were successfully made.
Total Current	Total number of Accounting-triggered MRME calls that are currently present in the system.
Total Released	Total number of Accounting-triggered MRME calls disconnected/released.
Total Aborted	Total number of Accounting-triggered MRME sessions aborted.
Total Disconnected	Total number of Accounting-triggered MRME session disconnects.

show subscribers samog-only full

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

```
MRME Subscriber Info:
    Session Trigger Type:  Radius Acct
```

Table 3: **show subscribers samog-only full** *Command Output Descriptions*

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

show twan-profile

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

```
TWAN Profile Name        : prof1
    Access-Type Client List
        Default Access Type       : IP
        Default Radius Dictionary  : custom71 | custom 70
        UE-address Type           : TWAN
        Session Trigger Type      : Radius Acct
```

Table 4: **show twan-profile** *Command Output Descriptions*

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

RADIUS Accounting-based Session Creation Bulk Statistics

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

Variable	Description	Data Type
mrme-acct-trigger-total-attempted	**Description**: Total number of Accounting-triggered MRME calls attempted. **Triggers**: Increments when there is an attempt to make an MRME call through accounting-trigger. **Availability**: Per SaMOG Service **Type**: Counter	Int32

Variable	Description	Data Type
mrme-acct-trigger-total-setup	**Description**: Total number of Accounting-triggered MRME calls that were successfully made. **Triggers**: Increments upon successful MRME call setup through accounting-trigger. This counter does not decrement when the call is disconnected. **Availability**: Per SaMOG Service **Type**: Counter	Int32
mrme-acct-trigger-total-current	**Description**: Total number of Accounting-triggered MRME calls that are currently present in the system. **Triggers**: Increments upon successful Accounting-triggered MRME call set up. Decrements upon successful disconnection of Accounting-Triggered MRME call. **Availability**: Per SaMOG Service **Type**: Gauge	Int32
mrme-acct-trigger-total-released	**Description**: Total number of Accounting-triggered MRME calls disconnected/released. **Triggers**: Increments when the Accounting-triggered MRME call is successfully disconnected. **Availability**: Per SaMOG Service **Type**: Counter	Int32
mrme-acct-trigger-total-aborted	**Description**: Total number of Accounting-triggered MRME sessions aborted. **Triggers**: Increments whenever Accounting-triggered MRME subscriber session is aborted by SaMOG due to various call setup failures such as authentication failure, P-GW selection failure, and Session Setup Timeout. **Availability**: Per SaMOG Service **Type**: Counter	Int32
mrme-acct-trigger-total-disconnected	**Description**: Total number of Accounting-triggered MRME session disconnects. **Triggers**: Increments when Accounting-triggered MRME session gets disconnected. **Availability**: Per SaMOG Service **Type**: Counter	Int32