



DHCP Trigger-based Session Creation

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

The following sections provide more detailed information:

- [Feature Description, on page 1](#)
- [How DHCP Trigger-based Session Creation Works, on page 2](#)
- [Configuring DHCP Trigger-based Session Creation, on page 5](#)
- [Monitoring and Troubleshooting DHCP Trigger-based Session Creation, on page 6](#)

Feature Description

Overview

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

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

DHCP Relay Agent Information Option

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

License Requirements

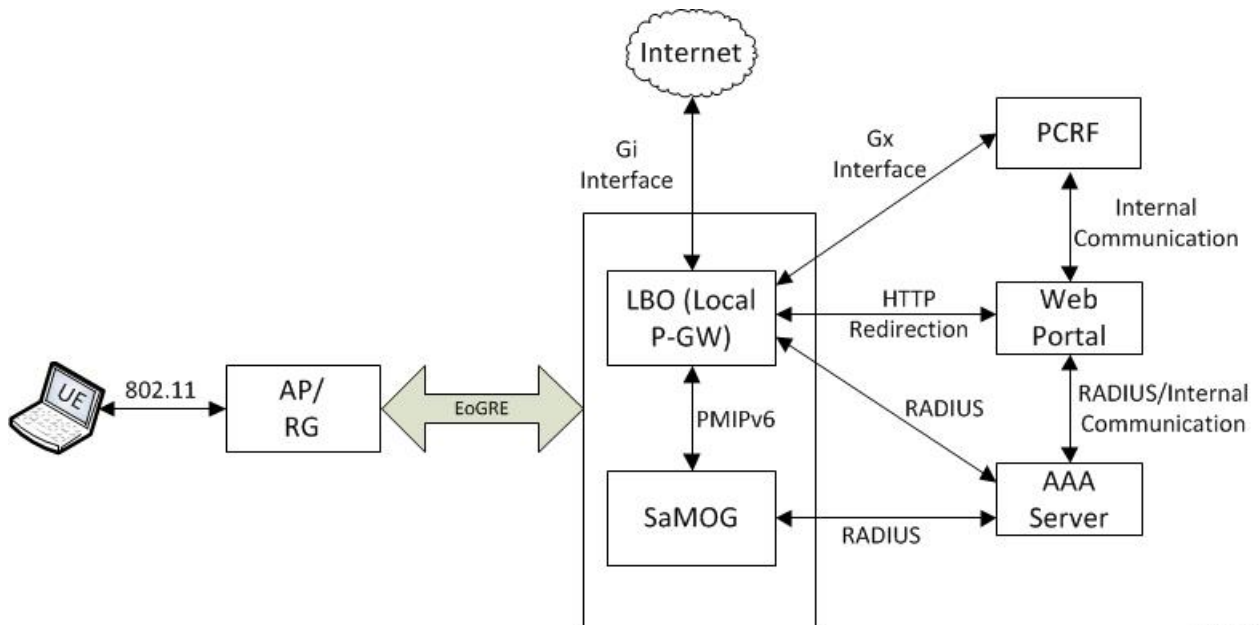
The DHCP trigger-based session creation feature does not require a separate license. However, a Local Breakout - Enhanced license is required to configure a local P-GW.

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

How DHCP Trigger-based Session Creation Works

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

Figure 1: DHCP Trigger-based Session Creation Architecture



411298

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

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

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

DHCP Relay Agent Information Option (option 82)

The SaMOG Gateway receives the location information in the AP-MAC or AP-MAC:SSID format in either the Circuit-ID (1) or Remote-ID (2) sub-option in the DHCP Relay Agent Information Option (option 82). Currently, the maximum supported length for DHCP option 82 is 64 bytes, and the maximum SSID value supported is 32 bytes. Formats other than AP-MAC or AP-MAC:SSID is considered as an opaque value. The SaMOG Gateway validates the Circuit-ID or Remote-ID sub-options based on the CLI configured under the TWAN Profile Configuration mode. For more configuration information, refer [Configuring DHCP Trigger-based Session Creation, on page 5](#).

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

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

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

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

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

Other AP-MAC formats are not parsed.

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

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

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

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

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

The SaMOG Gateway can be configured to send the mapped RADIUS attributes to the AAA server using the **radius attribute authentication nas-identifier** and **radius attribute authentication nas-port-id** commands under the Global Context Configuration or AAA Server Group Configuration Modes. For more information, refer [Configuring DHCP-based Session Location \(AP Without DHCP Relay Agent Information Option \(option 82\) Support\)](#), on page 5.

Limitations

Architectural Limitations

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

Configuration Limitations

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

Standards Compliance

This feature complies with the following standards:

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

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

Configuring DHCP Trigger-based Session Creation

Configuring TWAN Profile for DHCP Triggered Session Creation

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

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

Notes:

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

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

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

For Default AAA Server Group:

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

For Specific AAA Server Group:

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

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

Notes:

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

Verifying Configuration for DHCP Trigger-based Session Creation

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

```
show subscribers samog-only full
```

```
Session Trigger Type: DHCP
```

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

```
show twan-profile name twan_profile_name
```

```
Session Trigger Type: DHCP
```

Monitoring and Troubleshooting DHCP Trigger-based Session Creation

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

show samog-service statistics

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

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

```

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

```

Table 1: show samog-service statistics Command Output Descriptions

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

show subscribers samog-only full

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

show subscribers samog-only full

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

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

Table 2: show subscribers samog-only full Command Output Descriptions

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

show twan-profile name

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

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

Table 3: show twan-profile name Command Output Descriptions

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

show aaa group name

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

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


Table 4: show aaa group name Command Output Descriptions

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

DHCP Trigger-based Session Creation Bulk Statistics

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

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

