RADIUS Authentication-based non-UICC Sessions on PMIPv6 over S2a Interface

The following topics are discussed:

Feature Description

Overview

In Release 21.0 and earlier, for non-UICC devices, SaMOG supported the PMIPv6 protocol over the S2a interface for DHCP and RADIUS Accounting-based sessions.

In Release 21.1 and later, SaMOG supports the PMIPv6 protocol over the S2a interface for RADIUS Authentication triggered sessions also. This ensures that SaMOG can seamlessly handover non-UICC UE sessions that move from access points (AP) of one access type to another.

SaMOG forwards the MN-NAI value received from the AAA Server towards the Cisco WLC in the Access-Accept message. The Cisco WLC can use the same message in the PBU message towards SaMOG. For non-Cisco WLCs, the WLC may initiate a PBU message with the UE's MAC address (in any MAC format separated by '-', '.', ':') in the NAI attribute. SaMOG can then perform session lookup.

Web Authorization - Pre-Authentication Phase

In release 21.0 and earlier, during RADIUS authentication-based session creation, when the AAA server does not send the IMSI information in the Access-Accept message to SaMOG, SaMOG treats the call type as pre-authentication phase.

In release 21.1 and later, SaMOG applies the following logic to determine the call type as pre-authentication or Transparent Auto Logon (TAL) phase:

- If the IMSI information is included in the Access-Accept message from the AAA server, the call type will be considered as TAL phase (MN-NAI information can be included or excluded).
- If the IMSI information is not present and the MN-NAI information is present in the Acess-Accept message from the AAA server:

- SaMOG considers the call type to be TAL phase if the S2a protocol is PMIPv6.
- SaMOG considers the call type to be TAL phase, if the session trigger is DHCP or Accounting.
- SaMOG considers the call type to be pre-authentication phase if PMIPv6 is not the S2a protocol.

- If both IMSI and MN-NAI information is not present in the Access-Accept message from the AAA server, the call type will be considered as pre-authentication phase.

License Requirements

The following licenses are required for this feature:

- SaMOG General license (3G and 4G)
- SaMOG Local Breakout - Enhanced license to configure a local P-GW
- SaMOG Web Authorization license

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

How RADIUS Authentication-based Sessions on PMIPv6 over S2a Interface Work

Flows

RADIUS PMIPv6-based Session Establishment with S2a-PMIPv6 LBO

The figure below shows the detailed session establishment flow for a RADIUS PMIPv6-based WLC with S2a-PMIPv6 Local Breakout session. The table that follows the figure describes each step in the flow.

Figure 1: RADIUS PMIPv6-based Session Establishment with S2a-PMIPv6 LBO Call Flow

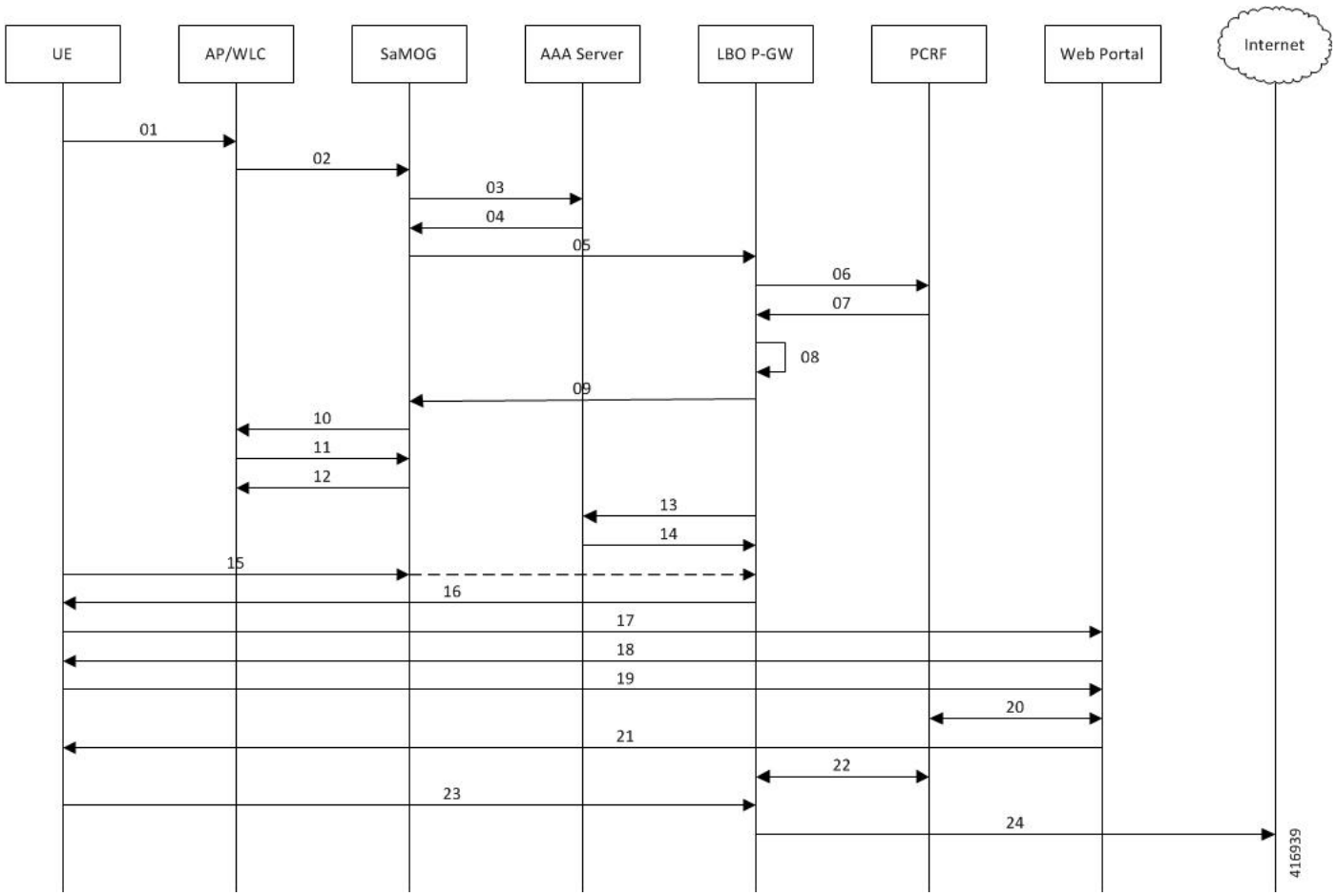

Table 1: RADIUS PMIPv6-based Session Establishment with S2a-PMIPv6 LBO

Step	Description
01	UE performs 802.11 association with the AP, and attaches to the open SSID.
02	AP forms a Radius Access Request (RAR) message and sends it to SaMOG. The RAR message has the following parameter: • UE MAC address in the Username and Calling-Station-Id attribute • (Optional) VLAN ID in the NAS-Identifier attribute • AP-MAC and SSID in the Called-Station-Id attribute
03	SaMOG caches the Access Request message from the AP/WLC and maps its contents to the Radius Access-Request message towards the AAA Server. The AP's IP address (Radius endpoint address/source address of the Access-Request message) is included in NAS-Port-Id attribute of the Access-Request message.

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

Step	Description
22	PCRF sends an RAR message on the Gx Interface to remove the redirection rule. LGW acknowledges the RAR with an RAA message. LGW removes the L7 redirection rule for the UE session. LGW sends a CCR-U message to the PCRF to get the quota information for the authenticated session. PCRF sends back a CCA-U message with the requested information.
23	UE attempts to reach the originally accessed web page again.
24	As the L7 rule is no longer present at the LGW, and the packets are sent to the Internet.

Limitations

Architectural Limitations

- This feature currently supports RADIUS-based AAA Server only.
- Only IPv4 address allocation is supported for the UE. IPv6 and IPv4v6 PDN types are currently not supported.
- All interfaces towards all external nodes will be IPv4 address only. IPv6 transport on any interface with external nodes is currently not supported.

Standards Compliance

This feature complies with the following standards:

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