



CHAPTER 24

SCE-Sniffer RADIUS Login Event Generator Functionality

Published: December 21, 2012

Introduction

This chapter describes the SCE-Sniffer RADIUS Login Event Generator (LEG) transactions for login and logout operations.

The Service Control Engine (SCE) devices analyze the RADIUS transactions and send the information to the SCE-Sniffer RADIUS LEG that resides on the Subscriber Manager (SM). The LEG performs login or logout operations to the SM using the information sent from the SCE devices.

- [SCE-Sniffer RADIUS Functionality, page 24-1](#)
- [Information About RADIUS Attributes, page 24-2](#)
- [Information About RADIUS Packets, page 24-4](#)



Note

[Chapter 22, “Domain Association Algorithm”](#) describes the algorithm used for deciding the subscriber domain to which a subscriber should be logged on.

SCE-Sniffer RADIUS Functionality

The LEG supports the following integrations with the RADIUS transactions:

- Integrating with the RADIUS accounting transactions

In this mode, the Accounting-Start and (optionally) Accounting-Interim-Update packets are used for login operations, and (optionally) the Accounting-Stop packets are used for logout operations. This integration mode is the simplest; therefore, if accounting transactions are used in your network it is advisable to use this integration mode.

- Integrating with the RADIUS authentication transactions

In this mode, the Access-Request and Access-Accept packets are used for login operations. This mode does not support logout operations. Use this integration mode if RADIUS accounting is not used in your network.

- Integrating with the RADIUS accounting and authentication transactions

This mode combines the previous two modes. Login operations use Authentication transactions, and logout operations use Accounting transactions.

Information About RADIUS Attributes

This section describes how subscriber properties are extracted from the RADIUS attributes.

- [Subscriber ID Association, page 24-2](#)
- [Domain Association, page 24-2](#)
- [Policy Association, page 24-3](#)
- [Subscriber IP Association, page 24-3](#)

Subscriber ID Association

By default, the attribute used for the subscriber ID association is the User-Name attribute (no. 1), but it can be configured to any other attribute including the Vendor-Specific attribute (no. 26).

The only requirement is that the configured attribute must be of type *string*.

This attribute must exist in the RADIUS traffic for successful login operations, because a subscriber cannot be introduced to the SM without its ID.

For logout operations, which are triggered by Accounting-Stop packets only, this attribute is not mandatory, because logouts can be performed using the mapping information.

Domain Association

**Note**

Domain association is only relevant for login operations and is optional.

Domain association is based on the Network Access System (NAS) that initiated the RADIUS transaction. The RADIUS attributes that identify the NAS are NAS-Identifier (no. 32), and NAS-IP-Address (no. 4). If none of the attributes exist, the LEG tries to identify the NAS using the IP address of the NAS taken from the UDP packet.

Before a login operation occurs, the NAS properties, NAS-Identifier and NAS-IP-Address, are matched against the configured domains or domain aliases of the SM. The login operation uses the matched domain or domain alias as the subscriber domain.

The domain association is performed in stages, as follows:

1. If the NAS-Identifier attribute exists, and a domain name or alias is configured in the SM for the same NAS-Identifier, the domain name or alias is used as the subscriber domain.
2. If the previous step fails, the same test is performed on the NAS-IP-Address attribute.
3. If the NAS-IP-Address does not exist as well, the same test is performed on the IP address of the NAS.
4. If the NAS-Identifier and the NAS-IP-Address attributes are missing or do not match to an existing SM domain or alias, the default subscriber domain is used.

Policy Association

**Note**

Policy association is only relevant for login operations and is optional.

The user can configure policy association. You can use any RADIUS attribute for policy association, including the Vendor-Specific attribute.

The term policy association refers to the act of setting a subscriber property according to information extracted from the RADIUS packets. An example of policy association is setting the `packageId` property of the Cisco SCA BB solution to control the network service level for which the subscriber is entitled.

To associate policy from a RADIUS attribute, the configured attribute must be of type **string** or **integer**. The subscriber property values are always integers. However, if the association is based on a string RADIUS attribute, it is mandatory to configure a mapping table. If the association is based on an integer RADIUS attribute, a mapping table is not needed, but can be used. See [Configuring the Policy Settings](#) for more information on configuring a mapping table.

You can define a default value for the policy if the configured RADIUS attribute is missing from the packet. The default value is valid only if the policy has not been set before (for example by other LEGs, or the Subscriber Manager).

The [Configuring the Policy Settings](#) section describes how to configure the policies.

Subscriber IP Association

The Subscriber IP Address is normally based on the Framed-IP-Address attribute, but can also be based on the RADIUS attribute. In different topologies, the subscriber IP address specification might be sent as a RADIUS attribute other than the Framed-IP-Address attribute.

The following algorithm extracts the IP addresses in this LEG:

1. If the user configured an attribute from which to extract the IP, the LEG looks for that attribute in the RDR. If the attribute exists, the LEG uses the attribute as the subscriber IP address.
2. If the attribute does not exist or is not configured, the LEG looks for the Framed-Route attributes; several Framed-Route attributes may exist. If any Framed-Route attributes exist, the LEG uses these attributes as the subscriber IP addresses.
3. If there are no Framed-Route attributes, the LEG looks for a Framed-IP-Address attribute and a Framed-IP-Netmask attribute. If a Framed-IP-Address attribute exists, the LEG uses this attribute as the subscriber IP address. If both the Framed-IP-Address and the Framed-IP-Netmask attributes exist, the operation is performed with the IP range represented by the IP address and the IP netmask.
4. Otherwise, the LEG performs a login without the IP address.

**Note**

The configured attribute can be a regular RADIUS attribute or a VSA. It is possible to encode the attribute as an integer in which case it is a single IP address. It can also be encoded as a string and is therefore an IP-Address/IP-Range value, which must be formatted as A.B.C.D/E or A.B.C.D.

**Note**

The supported format of the Framed-Route attribute is as described in RFC2865. It must start with a string that starts with the route itself in the format A.B.C.D/E followed by a space. Other values follow the space, but the LEG ignores these other values.

Information About RADIUS Packets

This section describes the RADIUS packets supported by the SCE-Sniffer RADIUS LEG and their impact on the SM.

- [Accounting-Start Packet, page 24-4](#)
- [Accounting-Interim-Update Packet, page 24-4](#)
- [Accounting-Stop Packet, page 24-4](#)
- [Access-Accept Packet, page 24-5](#)

Accounting-Start Packet

An Accounting-Start packet initiates a login operation with the following subscriber properties:

- Subscriber ID—See the [“Subscriber ID Association” section on page 24-2](#)
- Subscriber IP—See the [“Subscriber IP Association” section on page 24-3](#)
- Domain—See the [“Domain Association” section on page 24-2](#)
- Policy—See the [“Policy Association” section on page 24-3](#)

If the Accounting-Start packet does not hold the subscriber ID, the login operation is not performed and an error message is written to the user log. All other properties (subscriber IP, domain, and policy) are optional.

**Note**

The Accounting-Start and Accounting-Interim-Update packets are the only packets that hold all the subscriber properties. Use these packets whenever possible.

Accounting-Interim-Update Packet

An Accounting-Interim-Update packet initiates a login operation with exactly the same properties as the Accounting-Start packet.

If the Accounting-Interim-Update packet does not hold the subscriber ID, the login operation is not performed and an error message is written to the user log. All other properties (subscriber IP, domain, and policy) are optional.

**Note**

Use this packet when the subscribers are connected to the network for a long time in a single session.

Accounting-Stop Packet

An Accounting-Stop packet initiates a logout operation with the following subscriber properties:

- Subscriber ID—See [Subscriber ID Association, page 24-2](#)
- Subscriber IP—See [Subscriber IP Association, page 24-3](#)

Unlike the Accounting-Start packet, the subscriber ID is not mandatory in the Accounting-Stop packet. If it does not exist, the logout is based only on the mappings information. If the Accounting-Stop packet has a subscriber ID but does not have the mappings, all mappings of the subscriber are logged out. If both properties are missing, the logout operation is not performed and an error message is written to the user log.

**Note**

The Accounting-Stop packet is the only packet that initiates a logout operation. If you need to perform logouts, you must use this packet for integration.

Access-Accept Packet

An Access-Accept packet initiates a login operation with the following subscriber properties:

- Subscriber ID—See [Subscriber ID Association, page 24-2](#)
- Subscriber IP—See [Subscriber IP Association, page 24-3](#)
- Policy—See [Policy Association, page 24-3](#)

The subscriber ID is mandatory, subscriber IP and policy are not. If the subscriber ID is missing, the login operation is not performed and an error message is written to the user log.

**Note**

The Access-Accept packet does not hold any information needed for domain association. If you are using domains, consider using the accounting packets for domain integration.
