Alcatel-Lucent

Service Router | Release 12.0 R1

7750 SR-OS RADIUS Attributes Reference Guide

93-0472-02-01

Table of Contents

Table of Contents

RADIUS Attributes Reference 11

RADIUS Authentication Attributes

RADIUS Accounting Attributes

RADIUS CoA Message Attributes

Preface

About This Guide

This document provides an overview of all supported RADIUS Authentication, Authorization and Accounting attributes in 7750 SR-OS for SR-OS Release 12.0.

The authentication attributes are organized per application. The accounting attributes are organized per accounting application. For each application, three tables provide the attribute details:

- Description — A detailed description per attribute
- Limits — Value limits and format description per attribute. Note that the SR-OS RADIUS Python interface enables flexible formatting of the attributes received from and send to the RADIUS AAA servers.
- Applicability: — RADIUS messages where the attribute can be present.

The following displays conventions used in this RADIUS attribute document.

Attribute	Description
0	This attribute MUST NOT be present in packet.
0+	Zero or more instances of this attribute MAY be present in packet.
0-1	Zero or one instance of this attribute MAY be present in packet.
1	Exactly one instance of this attribute MUST be present in packet.

Notes:

- Unless explicitly stated differently, the term PPPoE is used in this document to indicate PPPoE, PPPoEoA or PPPoA.
- An unsupported attribute that is present in a CoA message is silently ignored, unless explicitly stated differently in the attribute description.

All Alcatel-Lucent Vendor Specific Attributes (VSAs) are available in a freeradius dictionary format. The dictionary is delivered together with the software package:
<cflash>\support\dictionary-freeradius.txt

Audience

This manual is intended for network administrators who are responsible for configuring and operating the 7750-SR routers using RADIUS AAA. It is assumed that the network administrators have an understanding of networking principles and configurations, routing processes, protocols and standards.

List of Technical Publications

The documentation set is composed of the following books:

- SR OS Basic System Configuration Guide
  This guide describes basic system configurations and operations.
- SR OS System Management Guide
  This guide describes system security and access configurations as well as event logging and accounting logs.
- SR OS Interface Configuration Guide
  This guide describes card, Media Dependent Adapter (MDA), and port provisioning.
- SR OS Router Configuration Guide
  This guide describes logical IP routing interfaces and associated attributes such as an IP address, port, link aggregation group (LAG) as well as IP and MAC-based filtering.
- SR OS Routing Protocols Guide
  This guide provides an overview of routing concepts and provides configuration examples for RIP, OSPF, IS-IS, BGP, and route policies.
- SR OS MPLS Guide
  This guide describes how to configure Multiprotocol Label Switching (MPLS) and Label Distribution Protocol (LDP).
- SR OS Services Guide
  This guide describes how to configure service parameters such as service distribution points (SDPs), customer information, and user services.
- SR OS OAM and Diagnostic Guide
  This guide describes how to configure features such as service mirroring and Operations, Administration and Management (OAM) tools.
- SR OS Quality of Service Guide
  This guide describes how to configure Quality of Service (QoS) policy management.
- SR OS Triple Play Guide
  This guide describes Triple Play services and support provided by the 7750 SR and presents examples to configure and implement various protocols and services.
- OS Multi-Service ISA Guide
  This guide describes services provided by integrated service adapters such as Application Assurance, IPSec, ad insertion (ADI) and Network Address Translation (NAT).
- 7750 SR OS RADIUS Attributes Reference Guide
  This guide describes all supported RADIUS Authentication, Authorization and Accounting attributes.

Feedback

authorized reseller, contact the technical support staff for that distributor or reseller for assistance. If you purchased an Alcatel-Lucent service agreement, contact your Alcatel-Lucent sales representative.

http://support.alcatel-lucent.com

Product manuals and documentation updates are available at alcatel-lucent.com. If you are a new user and require access to this service, contact your Alcatel-Lucent sales representative.

http://www.alcatel-lucent.com/myaccess

Report documentation errors, omissions and comments to:

ipd_online_feedback@alcatel-lucent.com

Include document name, version, part number and page(s) affected.

RADIUS Attributes Reference

In This Section

This document provides an overview of all supported RADIUS Authentication, Authorization and Accounting attributes in Alcatel-Lucent's 7750 SR-OS R12.0.

Topics include:

RADIUS Authentication Attributes

Subscriber Host Identification

Attributes related to subscriber-host configuration included in RADIUS authentication request and response.

Table 1: Subscriber Host Identification (description)

Attribute ID	Attribute Name	Description
1	User-Name	Refers to the user to be authenticated in the Access-Request. The format for IPoE/PPPoE hosts depends on configuration parameters pppoe-access-method, ppp-user-name or user-name-format in the CLI context **configure subscriber-mgmt authentication-policy** <*name*>. The format for ARP-hosts is not configurable and always the host IPv4-address.The RADIUS User-Name specified in an Access-Accept or CoA is reflected in the corresponding accounting messages. The attribute is omitted in authentication/accounting via **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute no user-name**.
2	User-Password	The password of the user to be authenticated, or the user's input following an Access-Challenge. For PPPoE users it indirectly maps to the password provided by a PPPoE PAP user in response to the PAP Authenticate-Request. For IPoE/ ARP hosts it indirectly maps to a pre-configured password (**configure subscriber-mgmt authentication-policy** <*name*> **password** <*password*> or **configure aaa isa-radius-policy** <*name*> **password** <*password*>).
3	CHAP-Password	Provided by a PPPoE CHAP user in response to the CHAP challenge. The CHAP challenge sent by the NAS to a PPPoE CHAP user is part of the CHAP authentication sequence RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*, (Challenge, Response, Success, Failure). The user generated CHAP password length is equal to the defined Limits and contains a one byte CHAP-Identifier from the user's CHAP Response followed by the CHAP Response from the user.

Table 1: Subscriber Host Identification (description) (Continued)

Attribute ID	Attribute Name	Description
4	NAS-IP-Address	The identifying IP Address of the NAS requesting the Authentication or Accounting. Included when the RADIUS server is reachable via IPv4. The address is determined by the routing instance through which the RADIUS server can be reached: “Management” — The active ipv4 address in the Boot Options File (**bof address** <*ipv4-address*>) “Base” or “VPRN” — the ipv4 address of the system interface (**configure router interface system address** <*address*>). The address can be overwritten with the configured source-address (**configure aaa radius-server-policy** <*policy-name*> **servers source-address** <*ip-address*>)
5	NAS-Port	The physical access-circuit on the NAS which is used for the Authentication or Accounting of the user. The format of this attribute is configurable on the NAS as a fixed 32 bit value or a parameterized 32 bit value. The parameters can be a combination of outer-vlan-id(o), inner-vlan-id(i), slot number(s), MDA number(m), port number or lag-id(p), ATM VPI(v) and ATM VCI(c), fixed bit values zero (0) or one (1) but cannot exceed 32 bit. The format can be configured for following applications: **configure aaa l2tp-accounting-policy** <*name*> **include-radius-attribute nas-port**, **configure router l2tp cisco-nas-port**, **configure service vprn** <*service-id*> **l2tp cisco-nas-port**, **configure subscriber-mgmt authentication-policy** <*name*> **include-radius-attribute nas-port**, **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute nas-port**.
6	Service-Type	The type of service the PPPoE user has requested, or the type of service to be provided for the PPPoE user. Optional in RADIUS-Accept and CoA. Treated as a session setup failure if different from Framed-User.
7	Framed-Protocol	the framing to be used for framed access in case of PPPoE users. Optional in RADIUS-Accept and CoA. Treated as a session setup failure if different from PPP.
8	Framed-IP-Address	The IPv4 address to be configured for the host via DHCPv4 (radius proxy) or IPCP (PPPoE). Simultaneous returned attributes [88] Framed-Pool and [8] Framed-IP-Address (RADIUS Access-Accept) are handled as host setup failures. Attribute is also used in CoA and Disconnect Message (part of the ESM or AA user identification-key). Attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute no framed-ip-addr.**

Table 1: Subscriber Host Identification (description) (Continued)

Attribute ID	Attribute Name	Description
9	Framed-IP-Netmask	The IP netmask to be configured for the user when the user is a router to a network. For DHCPv4 users, the attribute maps to DHCPv4 option [1] Subnet mask and is mandatory if [8] Framed-IP-Address is also returned. For PPPoE residential access, the attribute should be set to 255.255.255.255 (also the default value if the attribute is omitted). For PPPoE business access, the attribute maps to PPPoE IPCP option [144] Subnet-Mask only when the user requests this option and if the node parameter **configure subscriber-mgmt ppp-policy** <*ppp-policy-name*> **ipcp-subnet-negotiation** is set. Attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute no framed-ip-netmask**
18	Reply-Message	Text that may be displayed to the user by a PPPoE client as a success, failure or dialogue message. It is mapped to the message field from the PAP/CHAP authentication replies to the user. Omitting this attribute results in standard reply messages: login ok and login incorrect for PAP, CHAP authentication success and CHAP authentication failure for CHAP. String length greater than the defined Limits are accepted but truncated at this boundary.

Table 1: Subscriber Host Identification (description) (Continued)

Attribute ID	Attribute Name	Description
22	Framed-Route	Routing information (IPv4 managed route) to be configured on the NAS for a host (dhcp, pppoe, arp) that operates as a router without NAT (so called routed subscriber host). The route included in the Framed-Route attribute is accepted as a managed route only if it's next-hop points to the hosts ip-address or if the next-hop address equals 0.0.0.0 or if the included route is a valid classful network in case the subnet-mask is omitted. If neither is applicable, this specific framed-route attribute is ignored and the host is instantiated without this specific managed route installed. A Framed-Route attribute is also ignored if the SAP does not have anti-spoof configured to nh-mac (the host will be installed as a standalone host without managed route). Number of routes above Limits are silently ignored. Optionally, a metric, tag and/or protocol preference can be specified for the managed route. If the metrics are not specified or specified in a wrong format or specified with out of range values then default values are used for all metrics: metric=0, no tag and preference=0. If an identical managed route is associated with different routed subscriber hosts in the context of the same IES/VPRN service up to <*max-ecmp-routes*> managed routes are installed in the routing table (configured as **ecmp** <*max-ecmp-routes*> in the routing instance). Candidate ECMP Framed-Routes have identical prefix, equal lowest preference and equal lowest metric. The “lowest ip next-hop” is the tie breaker if more candidate ECMP Framed-Routes are available than the configured <*max-ecmp-routes*>. Other identical managed routes are shadowed (not installed in the routing table) and an event is logged. An alternative to RADIUS managed routes are managed routes via host dynamic BGP peering. Valid RADIUS learned managed routes can be included in RADIUS accounting messages with following configuration: **configure subscriber-mgmt radius-accounting-policy <***name***> include-radius-attribute framed-route**. Associated managed routes for an instantiated routed subscriber host are included in RADIUS accounting messages independent of the state of the managed route (Installed, Shadowed or HostInactive
25	Class	Attribute sent by the RADIUS server to the NAS in an Access-Accept or CoA and is sent unmodified by the NAS to the Accounting server as part of the Accounting-Request packet. Strings with a length longer than the defined Limits are accepted but truncated to this boundary. Only first 64B are stored in the CF persistency file.

Table 1: Subscriber Host Identification (description) (Continued)

Attribute ID	Attribute Name	Description
27	Session-Timeout	Sets the maximum number of seconds of service to be provided to the user (IPoEv4/PPPoE) before termination of the session. Attribute equals to [26-6527-160] Alc-Relative-Session-Timeout when received in Access-Accept since current session time portion is than zero. Value zero sets the session-timeout to infinite (no session-timeout). The attribute is CoA Nack'd if its value is smaller than the current-session time. Simultaneous received [27] Session-Timeout and [26-6527-160] Alc-Relative-Session-Timeout are treated as a error condition (setup failure if received via Access-Accept and Nack'd if received via CoA). For IPoEv4 radius proxy and CoA create-host scenarios, [27] Session-Timeout is interpreted as lease-time in stead of session-time if [26-6527-174] Alc-Lease-Time is omitted.
28	Idle-Timeout	Sets the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session (IPoE/PPPoE) or a connectivity check is triggered (IPoE). Values outside the allowed Limits are accepted but rounded to these boundaries. A value of zero is treated as an infinite idle-timeout. The idle-timeout handling on the node is implemented via category-maps (**configure subscriber-mgmt category-map** <*category-map-name*> and **configure subscriber-mgmt sla-profile** <*sla-profile-name*> **category-map** <*category-map-name*>).
30	Called-Station-Id	Allows the NAS to send in an Access Request and/or Accounting Request information with respect to the user called. Attribute is omitted in authentication/accounting via: **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute no called-station-id**. Supported applications: • LNS: the content is the string passed in the [21] Called Number AVP of the L2TP ICRQ message. • EAP authentication on WLAN Gateway: transparently forwarded as received in EAP authentication or accounting messages from the AP
31	Calling-Station-Id	Allows the NAS to send unique information identifying the user who requested the service. This format is driven by configuration (**configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute calling-station-id** <**llid**|**mac**|**remote-id**|**sap-id**|**sap-string**>). The LLID (logical link identifier) is the mapping from a physical to logical identification of a subscriber line and supplied by a RADIUS llid-server. The sap-string maps to **configure service** <*service-id*> **subscriber-interface** <*ip-int-name*> **group-interface** <*ip-int-name*> **sap** <*sap-id*> **calling-station-id** <*sap-string*>. A [31] Calling-Station-Id attribute value longer than the allowed maximum is treated as a setup failure. The attribute is omitted in authentication/accounting via **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute no calling-station-id**.

Table 1: Subscriber Host Identification (description) (Continued)

Attribute ID	Attribute Name	Description
32	NAS-Identifier	A string (**configure system name** <*system-name*>) identifying the NAS originating the Authentication or Accounting requests and sent when nas-identifier is included for the corresponding application: **configure subscriber-mgmt authentication-policy** (ESM authentication), **configure subscriber-mgmt radius-accounting-policy** (ESM accounting), **configure aaa isa-radius-policy** (LSN accounting, WLAN-GW soft-gre) and **configure aaa l2tp-accounting-policy** (L2TP accounting).
44	Acct-Session-Id	A unique identifier that represents the subscriber host or session that is authenticated. This attribute can be used as CoA or Disconnect Message key to target the host or session and is reflected in the accounting messages for this host or session.The attribute is included/excluded based on **configure subscriber-mgmt authentication-policy** <*name*> **include-radius-attribute acct-session-id** [**host**|**session**]. For PPPoE, either the **host** *acct-session-id* (default) or the **session** *acct-session-id* is included.
55	Event-Timestamp	Record the time that this event occurred on the NAS, in seconds since January 1, 1970 00:00 UTC
60	CHAP-Challenge	The CHAP challenge sent by the NAS to a PPPoE CHAP user as part of the chap authentication sequence RFC 1994 (Challenge, Response, Success, Failure). The generated challenge length for each new pppoe session is by default a random value between [32..64] bytes unless configured different under **configure subscriber-mgmt ppp-policy** <*ppp-policy-name*> **ppp-chap-challenge-length** [8..64] or **configure router l2tp group** <*tunnel-group-name*> **ppp chap-challenge-length** [8..64] for LNS. The CHAP challenge value is copied into the request-authenticator field of the RADIUS Access-Request message if the minimum and maximum value is configured at exact 16 (RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*, section 2.2, *Interoperation with PAP and CHAP*). Attribute CHAP-Password is provided by a PPPoE CHAP user in response to the [60] CHAP-challenge.
61	NAS-Port-Type	The type of the physical port of the NAS which is authenticating the user and value automatically determined from subscriber SAP encapsulation. It can be overruled by configuration. Included only if include-radius-attribute nas-port-type is added per application: **configure subscriber-mgmt authentication-policy** (ESM authentication), **configure subscriber-mgmt radius-accounting-policy** (ESM accounting), **configure aaa isa-radius-policy** (LSN accounting, WLAN-GW soft-gre) and **configure aaa l2tp-accounting-policy** (L2TP accounting). Checked for correctness if returned in CoA.
85	Acct-Interim-Interval	Indicates the number of seconds between each interim update for this specific session. Attribute values outside the allowed Limits are accepted but are rounded to the minimum or maximum Limit.

Table 1: Subscriber Host Identification (description) (Continued)

Attribute ID	Attribute Name	Description
87	NAS-Port-Id	A text string which identifies the physical/logical port of the NAS which is authenticating the user and/or reported for accounting. Attribute is also used in CoA and Disconnect Message (part of the user identification-key). The nas-port-id for physical ports usually contains <slot>/<mda>/<port>/<vlan|vpi>.<vlan|vci>. The physical port can have an optional prefix-string (max 8 chars) and suffix-string (max 64 chars) added for Authorization and Accounting (**configure subscriber-mgmt radius-accounting-policy | authentication-policy** <*name*> include-radius-attribute **nas-port-id** [**prefix-string** <*string*>] [**suffix** <**circuit-id**|**remote-id**>]). For logical access circuits (LNS) the nas-port-id is a fixed concatenation (delimiter #) of routing instance, tunnel-server-endpoint, tunnel-client-endpoint, local-tunnel-id, remote-tunnel-id, local-session-id, remote-session-id and call sequence number.
88	Framed-Pool	The name of one address pool or the name of a primary and secondary address pool separated with a 1 character configurable delimiter (**configure router/service vprn** <*service-id*> **dhcp local-dhcp-server** <*server-name*> **use-pool-from-client delimiter** <*delimiter*>) that should be used to assign an address for the user and maps to either 1) dhcpv4 option [82] vendor-specific-option [9] sub-option [13] dhcpPool if option is enabled on the node (**configure service ies/vprn** <*service-id*> **subscriber-interface** <*ip-int-name*> **group-interface** <*ip-int-name*> **dhcp option vendor-specific-option pool-name**) or 2) used directly as pool-name in the local configured dhcp server when local-address-assignment is used and client-application is ppp-v4 (**configure service ies/vprn** <*service-id*> **subscriber-interface** *ip-int-name* **group-interface** *ip-int-name* **local-address-assignment**). Alternative to [26-2352-36] Ip-Address-Pool-Name and [26-4874-2] ERX-Address-Pool-Name. Framed-Pool names longer than the allowed maximum are treated as host setup failures. Simultaneous returned attributes [88] Framed-Pool and [8] Framed-IP-Address are also handled as host setup failures.
95	NAS-IPv6-Address	The identifying IP Address of the NAS requesting the Authentication or Accounting. Included when the RADIUS server is reachable via IPv6. The address is determined by the routing instance through which the RADIUS server can be reached: “Management” — The active ipv6 address in the Boot Options File (**bof address** <*ipv6-address*>) “Base” or “VPRN” — The ipv6 address of the system interface (**configure router interface system ipv6 address** <*ipv6-address*>). The address can be overwritten with the configured ipv6-source-address (**configure aaa radius-server-policy** <*policy-name*> **servers ipv6-source-address** <*ipv6-address*>).

Table 1: Subscriber Host Identification (description) (Continued)

Attribute ID	Attribute Name	Description
97	Framed-IPv6-Prefix	ipv6-prefix/prefix-length to be configured via SLAAC (Router Advertisement) to the WAN side of the user. Any non /64 prefix-length for SLAAC host creation is treated as a session setup failure for this host. This attribute is an alternative to [100] Framed-IPv6-Pool and [26-6527-99] Alc-IPv6-Address, which assigns IPv6 addressing to the wan-side of a host via DHCPv6 IA-NA. Attribute is also used in CoA and Disconnect Message (part of the ESM or AA user identification-key). Attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute no framed-ipv6-prefix**
99	Framed-IPv6-Route	Routing information (ipv6 managed route) to be configured on the NAS for a v6 wan host (IPoE or PPPoE) that operates as a router. The functionality is comparable with offering multiple PD prefixes for a single host. The route included in the Framed-IPv6-Route attribute is accepted as a managed route only if it's next-hop is a wan-host (DHCPv6 IA-NA or SLAAC) or if the next-hop address equals ::. As a consequence, Framed-IPv6-Routes with explicit configured gateway prefix of a pd-host (DHCPv6 IA-PD) will not be installed. A Framed-Route attribute is also ignored if the SAP does not have anti-spoof configured to nh-mac (the host will be installed as a standalone host without managed route). Number of Routes above Limits are silently ignored. Optionally, a metric, tag and/or protocol preference can be specified for the managed route. If the metrics are not specified or specified in a wrong format or specified with out of range values then default values are used for all metrics: metric=0, no tag and preference=0. If an identical managed route is associated with different routed subscriber hosts in the context of the same IES/VPRN service up to <*max-ecmp-routes*> managed routes are installed in the routing table (configured as **ecmp** <*max-ecmp-routes*> in the routing instance). Candidate ECMP Framed-IPv6-Routes have identical prefix, equal lowest preference and equal lowest metric. “lowest ip next-hop” is the tie breaker if more candidate ECMP Framed-IPv6-Routes are available than the configured <*max-ecmp-routes*>. Other identical managed routes are shadowed (not installed in the routing table) and an event is logged. Valid RADIUS learned managed routes can be included in RADIUS accounting messages with following configuration: **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute framed-ipv6-route**. Associated managed routes for an instantiated routed subscriber host are included in RADIUS accounting messages independent of the state of the managed route (Installed, Shadowed or HostInactive).

Table 1: Subscriber Host Identification (description) (Continued)

Attribute ID	Attribute Name	Description
100	Framed-IPv6-Pool	The name of an assigned pool that should be used to assign an IPv6 address via DHCPv6 (IA-NA) to the WAN side of the user (IPoE, PPPoE). Maps to DHCPv6 vendor-option [17], sub-option [1] wan-pool. Framed-IPv6-Pool names longer than the allowed maximum are treated as host setup failures. This attribute is an alternative to [97] Framed-IPv6-Prefix and [26-6527-99] Alc-IPv6-Address, that also assign IPv6 addressing to the wan-side of a host via SLAAC or DHCPv6 IA-NA.
101	Error-Cause	The Error-Cause Attribute provides more detail on the cause of the problem if the NAS cannot honor Disconnect-Request or CoA-Request messages for some reason. It may be included within Disconnect-ACK, Disconnect-NAK and CoA-NAK messages. The Error-Causes are divided in 5 blocks. Range [400-499] is used for fatal errors committed by the RADIUS server. Range [500-599] is used for fatal errors occurring on a NAS or RADIUS proxy. Ranges [000-199 reserved], [300-399 reserved] and [200-299 used for successful completion in disconnect-ack/coa-ack] are not implemented.
123	Delegated-IPv6-Prefix	Attribute that carries the Prefix (ipv6-prefix/prefix-length) to be delegated via DHCPv6 (IA-PD) for the LAN side of the user (IPoE, PPPoE). Maps to DHCPv6 option IA-PD [25] sub-option IA-Prefix [26] Prefix. An exact Delegated-prefix-Length [DPL] match with **configure service** <*service-id*> **subscriber-interface** <*ip-int-name*> **ipv6 delegated-prefix-length** [48..64] is required with the received attribute prefix-length unless a variable DPL is configured (**configure service** <*service-id*> **subscriber-interface** <*ip-int-name*> **ipv6 delegated-prefix-length** *variable*). In the latter case multiple hosts for the same group-interface having different prefix-length [48..64] per host are supported. Simultaneous returned attributes [123] Delegated-IPv6-Prefix and [26-6527-131] Alc-Delegated-IPv6-Pool are handled as host setup failures. Attribute is also used in CoA and Disconnect Message (part of the ESM or AA user identification-key). Attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute no delegated-ipv6-prefix**.
26-2352-1	Client-DNS-Pri	The IPv4 address of the primary DNS server for this subscribers connection and maps to PPPoE IPCP option 129 Primary DNS Server address or DHCPv4 option 6 Domain Server. Is an alternative for 26-4874-4 ERX-Primary-Dns or 26-6527-9 Alc-Primary-Dns.
26-2352-2	Client-DNS-Sec	A IPv4 address of the secondary DNS server for this subscribers connection and maps to 'PPPoE IPCP option 131 Secondary DNS Server address or DHCPv4 option 6 Domain Server. Is an alternative for 26-4874-5 ERX-Secondary-Dns or 26-6527-10 Alc-Secondary-Dns.

Table 1: Subscriber Host Identification (description) (Continued)

Attribute ID	Attribute Name	Description
26-2352-36	Ip-Address-Pool-Name	The name of an assigned address pool that should be used to assign an address for the user and maps to dhcpv4 option[82] vendor-specific-option [9] sub-option [13] dhcpPool if option is enabled on the node (**configure service** <*service-id*> **subscriber-interface** <*ip-int-name*> **group-interface** <*ip-int-name*> **dhcp option vendor-specific-option pool-name**). Alternative to [88] Pool-Name and [26-4874-2] ERX-Address-Pool-Name. Framed-Pool names longer than the allowed maximum are treated as host setup failures. Simultaneous returned attributes Pool-Names [8] and Framed-IP-Address are also handled as host setup failures.
26-2352-99	RB-Client-NBNS-Pri	The IPv4 address of the primary NetBios Name Server (NBNS) for this subscribers connection and maps to 'PPPoE IPCP option 130 Primary DNS Server address or DHCPv4 option44 NETBIOS name server. Is an alternative for 26-4874-6 ERX-Primary-Wins or 26-6527-29 Alc-Primary-Nbns
26-2352-100	RB-Client-NBNS-Sec	The IPv4 address of the secondary NetBios Name Server (NBNS) for this subscribers connection and maps to 'PPPoE IPCP option 132 Primary DNS Server address or DHCPv4 option44 NETBIOS name server. Is an alternative for 26-4874-7 ERX-Secondary-Wins or 26-6527-30 Alc-Secondary-Nbns
26-3561-1	Agent-Circuit-Id	Information describing the subscriber agent circuit identifier corresponding to the logical access loop port of the Access Node/DSLAM from which a subscriber's requests are initiated. Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute circuit-id**.
26-3561-2	Agent-Remote-Id	An operator-specific, statically configured string that uniquely identifies the subscriber on the associated access loop of the Access Node/DSLAM. Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute remote-id**.
26-3561-129	Actual-Data-Rate-Upstream	The actual upstream train rate (coded in bits per second) of a subscriber's synchronized DSL link and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-3561-130	Actual-Data-Rate-Downstream	Actual downstream train rate (coded in bits per second) of a subscriber's synchronized DSL link and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.

Table 1: Subscriber Host Identification (description) (Continued)

Attribute ID	Attribute Name	Description
26-3561-131	Minimum-Data-Rate-Upstream	The subscriber's operator-configured minimum upstream data rate (coded in bits per second) and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** 7x50_PRD_Multicast_MVPN_sender_receiver_only_v0.2.doc **include-radius-attribute access-loop-options.**
26-3561-132	Minimum-Data-Rate-Downstream	The subscriber's operator-configured minimum downstream data rate (coded in bits per second) and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-3561-133	Attainable-Data-Rate-Upstream	The subscriber's attainable upstream data rate (coded in bits per second) and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-3561-134	Attainable-Data-Rate-Downstream	The subscriber's attainable downstream data rate (coded in bits per second) and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-3561-135	Maximum-Data-Rate-Upstream	The subscriber's maximum upstream data rate (coded in bits per second), as configured by the operator and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-3561-136	Maximum-Data-Rate-Downstream	The subscriber's maximum downstream data rate (coded in bits per second), as configured by the operator and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-3561-137	Minimum-Data-Rate-Upstream-Low-Power	The subscriber's minimum upstream data rate (coded in bits per second) in low power state, as configured by the operator and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.

Table 1: Subscriber Host Identification (description) (Continued)

Attribute ID	Attribute Name	Description
26-3561-138	Minimum-Data-Rate-Downstream-Low-Power	The subscriber's minimum downstream data rate (coded in bits per second) in low power state, as configured by the operator and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/ excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-3561-139	Maximum-Interleaving-Delay-Upstream	The subscriber's maximum one-way upstream interleaving delay in milliseconds, as configured by the operator and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/ excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-3561-140	Actual-Interleaving-Delay-Upstream	The subscriber's actual one-way upstream interleaving delay in milliseconds and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-3561-141	Maximum-Interleaving-Delay-Downstream	The subscriber's maximum one-way downstream interleaving delay in milliseconds, as configured by the operator and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/ excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-3561-142	Actual-Interleaving-Delay-Downstream	The subscriber's actual one-way downstream interleaving delay in milliseconds and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-3561-144	Access-Loop-Encapsulation	The last mile encapsulation used by the subscriber on the DSL access loop and maps to values received during PPPoE discovery Tags (tag 0x0105) or DHCP Tags (opt-82). Attribute is included/excluded in RADIUS/Accounting-Request based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**. Last mile encapsulation information can be used to adjust automatically the egress aggregate rate for this subscriber. Pre-configured encapsulation types are used if PPP/IPoE access loop information (tags) is not available (**configure subscriber-mgmt sub-profile** <*subscriber-profile-name*> **egress encap-offset** <*type*> or **configure subscriber-mgmt local-user-db** <*local-user-db-name*> **ppp host access-loop encap-offset** <*type*>). [26-6527-133] Alc-Access-Loop-Encap-Offset when returned in Access-Accept is taken into account (overrules received tags and pre-configured encapsulation types) for ALE adjust (last mile aware shaping) but is not reflected in access-loop-options send to RADIUS. Alc-Access-Loop-Encap from ANCP are currently not taken into account for ALE adjust.

Table 1: Subscriber Host Identification (description) (Continued)

Attribute ID	Attribute Name	Description
26-3561-254	IWF-Session	The presence of this Attribute indicates that the IWF has been performed with respect to the subscriber's session. IWF is utilized to enable the carriage of PPP over ATM (PPPoA) traffic over PPPoE. The Access Node inserts the PPPoE Tag 0x0105, vendor-id 0x0de9 with sub-option code 0xFE, length field is set to 0x00 into the PPPoE Discovery packets when it is performing an IWF functionality. Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-4874-2	ERX-Address-Pool-Name	The name of an assigned address pool that should be used to assign an address for the user and maps to dhcpv4 option[82] vendor-specific-option [9] sub-option [13] dhcpPool if option is enabled on the node (**configure service** <*service-id*> **subscriber-interface** <*ip-int-name*> **group-interface** <*ip-int-name*> **dhcp option vendor-specific-option pool-name**). Alternative to [88] Pool-Name and [26-2352-36] Ip-Address-Pool-Name. Framed-Pool names longer than the allowed maximum are treated as host setup failures. Simultaneous returned attributes Pool-Names [8] and Framed-IP-Address are also handled as host setup failures.
26-4874-4	ERX-Primary-Dns	The IPv4 address of the primary DNS server for this subscribers connection and maps to PPPoE IPCP option 129 Primary DNS Server address or DHCPv4 option 6 Domain Server. Is an alternative for 26-2352-1 Client-DNS-Pri or 26-6527-9 Alc-Primary-Dns
26-4874-5	ERX-Secondary-Dns	The IPv4 address of the secondary DNS server for this subscribers connection and maps to PPPoE IPCP option 131 Secondary DNS Server address or DHCPv4 option 6 Domain Server. Is an alternative for 26-2352-2 Client-DNS-Sec or 26-6527-10 Alc-Secondary-Dns
26-4874-6	ERX-Primary-Wins	The IPv4 address of the primary NetBios Name Server (NBNS) for this subscribers connection and maps to PPPoE IPCP option 130 Primary DNS Server address or DHCPv4 option44 NETBIOS name server. Is an alternative for 26-2352-99 RB-Client-NBNS-Pri or 26-6527-29 Alc-Primary-Nbns
26-4874-7	ERX-Secondary-Wins	The IPv4 address of the secondary NetBios Name Server (NBNS) for this subscribers connection and maps to PPPoE IPCP option 132 Primary DNS Server address or DHCPv4 option44 NETBIOS name server. Is an alternative for 26-2352-100 RB-Client-NBNS-Sec or 26-6527-30 Alc-Secondary-Nbns
26-4874-47	ERX-Ipv6-Primary-Dns	The IPv6 address of the primary DNSv6 server for this subscribers connection and maps to DNS Recursive Name Server option 23 (RFC 3646) in DHCPv6.Is an alternative for 26-6527-105 Alc-Ipv6-Primary-Dns
26-4874-48	ERX-Ipv6-Secondary-Dns	The IPv6 address of the secondary DNSv6 server for this subscribers connection and maps to DNS Recursive Name Server option 23 (RFC 3646) in DHCPv6.Is an alternative for 26-6527-106 Alc-Ipv6-Secondary-Dns

Table 1: Subscriber Host Identification (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-9	Alc-Primary-Dns	The IPv4 address of the primary DNS server for this subscribers connection and maps to PPPoE IPCP option 129 Primary DNS Server address or DHCPv4 option 6 Domain Server. Is an alternative for 26-2352-1 Client-DNS-Pri or 26-4874-4 ERX-Primary-Dns.
26-6527-10	Alc-Secondary-Dns	The IPv4 address of the secondary DNS server for this subscribers connection and maps to PPPoE IPCP option 131 Secondary DNS Server address or DHCPv4 option 6 Domain Server. Is an alternative for 26-2352-2 Client-DNS-Sec or 26-4874-5 ERX-Secondary-Dns.
26-6527-11	Alc-Subsc-ID-Str	A subscriber is a collection of subscriber-hosts (typically represented by IP-MAC combination) and is uniquely identified by a subscriber string. Subscriber-hosts queues/policers belonging to the same subscriber (residing on the same forwarding complex) can be treated under one aggregate scheduling QoS mechanism. Fallback to pre-configured values if attribute is omitted. Attribute values longer than the allowed string value are treated as setup failures. Can be used as key in CoA and Disconnect Message. Attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute no subscriber-id**.
26-6527-12	Alc-Subsc-Prof-Str	The subscriber profile is a template which contains settings (accounting, igmp, HQoS,...) which are applicable to all hosts belonging to the same subscriber were [26-6527-12] Alc-Subsc-Prof-Str is the string that maps (**configure subscriber-mgmt sub-ident-policy sub-profile-map**) to such an subscriber profile (**configure subscriber-mgmt sub-profile** <*subscriber-profile-name*>). Strings longer than the allowed maximum are treated as setup failures. Unreferenced strings (string does not map to a policy) are silently ignored and a fallback to pre-configured defaults is done. Attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute no sub-profile**.
26-6527-13	Alc-SLA-Prof-Str	The SLA profile is a template which contains settings (filter, QoS, host-limit...) which are applicable to individual hosts were [26-6527-13] Alc-SLA-Prof-Str is the string that maps (**configure subscriber-mgmt sub-ident-policy** <*sub-ident-policy-name*> **sla-profile-map**) to such a sla profile (**configure subscriber-mgmt sla-profile** <*sla-profile-name*>). Strings longer than the allowed maximum are treated as setup failures. Unreferenced strings (string does not map to a policy) are silently ignored and a fallback to pre-configured defaults is done. Attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute no sla-profile**.

Table 1: Subscriber Host Identification (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-16	Alc-ANCP-Str	Information describing the subscriber agent circuit identifier corresponding to the logical access loop port of the Access Node/DSLAM from which a subscriber's requests are initiated and used to associate the ANCP Circuit-Id (info received via ANCP Port Up and Port Down) with the PPPoE/IPoE Circuit-Id (info received via [26-6527-16] Alc-ANCP-Str and [26-3561-1] Agent-Circuit-Id). An subscriber is ANCP associated when both strings are equal and for associated subscribers the ingress/egress ANCP QoS rules apply (**configure subscriber-mgmt ancp ancp-policy** <*policy-name*> and **configure subscriber-mgmt sub-profile ancp ancp-policy** <*policy-name*>.
26-6527-18	Alc-Default-Router	Maps to dhcp offer/ack message option [3] default-router for a dhcpv4 radius proxy scenario and defines the default gateway for the user. This attribute is silently ignored if the NAS is doing dhcpv4 relay. In the latter case the default-router is part of the dhcpv4 server configuration.
26-6527-27	Alc-Client-Hardware-Addr	MAC address from a user that requests a service and included in CoA, Authentication or Accounting (**configure subscriber-mgmt authentication-policy/radius-accounting-policy include-radius-attribute mac-address**).
26-6527-28	Alc-Int-Dest-Id-Str	A string representing an aggregation point (for example, Access Node) and interpreted as the intermediate destination id. Subscribers connected to the same aggregation point should get the same int-dest-id string assigned. The int-dest-id is used in mc-ring access redundancy to identify subscribers behind a ring node (**configure redundancy multi-chassis peer** <*ip-address*> **mc-ring ring/ l3-ring** <*name*> **ring-node** <*ring-node-name*>). The *int-dest-id* can be used in QoS to shape the egress traffic of a group of subscribers to an aggregate rate using vports (**configure port** <*port-id*> **ethernet access egress vport** <*name*> **host-match dest** <*destination-string*>) or secondary shapers on HS-MDAv2 (**configure port** <*port-id*> ethernet egress exp-secondary-shaper <secondary-shaper-name>). For egress policed subscriber traffic, the *inter-dest-id* can be used to select the egress queue-group for forwarding (**configure port** <*port-id*> **ethernet access egress queue-group** <*name*> **host-match dest** <*destination-string*>). Strings longer than the allowed maximum are treated as setup failures.
26-6527-29	Alc-Primary-Nbns	The IPv4 address of the primary NetBios Name Server (NBNS) for this subscribers connection and maps to PPPoE IPCP option 130 Primary DNS Server address or DHCPv4 option44 NETBIOS name server. Is an alternative for 26-2352-99 RB-Client-NBNS-Pri or 26-4874-6 ERX-Primary-Wins.
26-6527-30	Alc-Secondary-Nbns	The IPv4 address of the secondary NetBios Name Server (NBNS) for this subscribers connection and maps to PPPoE IPCP option 132 Primary DNS Server address or DHCPv4 option44 NETBIOS name server. Is an alternative for 26-2352-100 RB-Client-NBNS-Sec or 26-4874-7 ERX-Secondary-Wins.

Table 1: Subscriber Host Identification (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-34	Alc-PPPoE-PADO-Delay	Specifies the number in deci-seconds that the PPPoE protocol stack on the NAS waits before sending a PADO packet in response to a PADI request. In dual homed topologies, you may want to designate a primary NAS and a backup NAS for handling a particular service request. In such a scenario, you can configure a delay for the backup NAS to allow sufficient time for the primary NAS to respond to the client with a PADO packet. If the primary NAS does not send the PADO packet within this delay period, then the backup NAS sends the PADO packet after the delay period expires. This attribute is only applicable if RADIUS PADI authentication is used (**configure subscriber-mgmt authentication-policy** <*ppp-policy-name*> pppoe-access-method padi). Values above the allowed Limits are truncated at the Limits boundary. There is no PADO delay if the attribute is omitted or if the attribute is received with a value of zero.
26-6527-35	Alc-PPPoE-Service-Name	Maps to PADI field PPPoE tags [0x0101] service-name and is sent in the Access-Request if enabled under **configure subscriber-mgmt authentication-policy** <*name*> **include-radius-attribute pppoe-service-name**. A PPPoE-Service-Name above the allowed maximum length is handled as a pppoe session setup failure.
26-6527-36	Alc-DHCP-Vendor-Class-Id	Initiated by DHCP clients via option 60 [Class-id] and reflected in Authentication/Accounting. (**configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute dhcp-vendor-class-id configure aaa isa-radius-policy** <*name*> **auth-include-attributes dhcp-vendor-class-id**). DHCP option [60] Class-id can also be used as User-name in RADIUS requests. (**configure subscriber-mgmt authentication-policy** <*name*> **user-name-format dhcp-client-vendor-opts**).
26-6527-45	Alc-App-Prof-Str	Application Assurance for residential, business or transit-AA subscribers is enabled through the assignment of an application profile as part of either enhanced subscriber management or static configuration. [26-6527-45] Alc-App-Prof-is is a string that maps (**configure subscriber-mgmt sub-ident-policy** <sub-*ident-policy-name*> **app-profile-map**) to such an application profile (**configure application-assurance group** <*aa-group-id:partition-id*> **policy app-profile** <*app-profile-name*>). This attribute is used in access-accept (to assign an application profile during esm host creation) and CoA (to change the application profile of a AA-subscriber or to create transit AA-subscriber). Strings longer than the allowed maximum are treated as setup failures. Unreferenced strings (strings not mapping to an application profile) will silently trigger a fallback to pre-configured default values if allowed. If no default value is pre-configured, the subscriber's application profile is silently disabled for esm AA-subscriber; in case of a transit AA-subscriber creation the CoA will be rejected. The change of an application profile to one configured under a different group/partition or the modification of the application profile of a static AA-subscriber is not allowed and will be treated as setup failures.

Table 1: Subscriber Host Identification (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-99	Alc-Ipv6-Address	The ipv6 address to be configured to the WAN side of the user (IPoE,PPPoE) via DHCPv6 (IA-NA). Maps to DHCPv6 option IA-NA[3] sub-option IA-Address[5] address. This attribute is an alternative to [97] Framed-IPv6-Prefix and [100] Framed-IPv6-Pool, which also assigns IPv6 addressing to the wan-side of a host via SLAAC or DHCPv6 IA-NA. Attribute is also used in CoA and Disconnect Message (part of the ESM or AA user identification-key). Attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute no ipv6-address**.
26-6527-102	Alc-ToServer-Dhcp-Options	Send to RADIUS all dhcpv4 options received in a DHCPv4 message triggering authentication. The dhcpv4 options are concatenated in the attribute up to maximum length per attribute (see limits). If more space is needed, an additional attribute is included. If the total dhcp options space requires more than the total maximum length (see limits), then no attributes are included. (**configure subscriber-mgmt authentication-policy** <*name*> **include-radius-attribute dhcp-options**, **configure aaa isa-radius-policy** <*name*> **auth-include-attributes dhcp-options**).
26-6527-103	Alc-ToClient-Dhcp-Options	Copy the content of the attribute value in dhcpv4 options for dhcpv4 messages towards the client. It is not required to send each option in a different VSA; concatenation is allowed. Only the attributes within the defined limits (see limits) are parsed and stored; the remaining attributes are silently ignored.
26-6527-105	Alc-Ipv6-Primary-Dns	The IPv6 address of the primary DNSv6 server for this subscribers connection and maps to DNS Recursive Name Server option 23 (RFC 3646) in DHCPv6. This attribute is an alternative for [26-4874-47] ERX-Ipv6-Primary-Dns
26-6527-106	Alc-Ipv6-Secondary-Dns	The IPv6 address of the secondary DNSv6 server for this subscribers connection and maps to DNS Recursive Name Server option 23' (RFC 3646) in DHCPv6. This attribute is an alternative for [26-4874-48] ERX-Ipv6-Secondary-Dns
26-6527-126	Alc-Subscriber-QoS-Override	Used to override queue/policer parameters (CIR, PIR, CBS, MBS) and HQoS parameters (aggregate rate or root arbiter rate) configured at sla-profile and sub-profile level. Enables per subscriber/host customization. Each set of Alc-Subscriber-QoS-Override attributes in a RADIUS message replaces the set of Alc-Subscriber-QoS-Override attributes from a previous message. Hence the sla-profile and sub-profile QoS configuration is always used as the base config. To undo a previously enabled RADIUS QoS-override and return to the base config, send a CoA with at least one Alc-Subscriber-QoS-Override attribute. The value part of each Alc-Subscriber-QoS-Override attribute must be empty (For example, Alc-Subscriber-QoS-Override += i:q:2:). Wrong formatted attributes or too many attributes (see limits) are treated as a setup failure or result in a CoA NAK.

Table 1: Subscriber Host Identification (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-128	Alc-ATM-Ingress-TD-Profile	The ATM Traffic Descriptor override for a PPPoA or PPPoEoA host and refers to the pre-configured traffic description QoS profile applied on the ingress ATM Virtual Circuit (**configure qos atm-td-profile** <*traffic-desc-profile-id*>). All subscriber hosts on a given ATM VC must have same ATM traffic descriptors and this attribute is ignored if it specifies an ATM Traffic Descriptor override while it has already specified another one for another host on the same ATM Virtual Circuit. A pre-configured description profile per ATM Virtual Circuit is used when this attribute is omitted. (**configure subscriber-mgmt msap-policy** <*msap-policy-name*> **atm egress/ingress traffic-desc or configure service vprn** <*service-id*> **subscriber-interface** <*ip-int-name*> **group-interface** <*ip-int-name*> **sap** <*sap-id*> **atm egress/ingress traffic-desc**). A Traffic Descriptor profile above the Limit is treated as a setup failure. Unreferenced Traffic Descriptor profiles within the Limit, or a Traffic Descriptor profile for a non ATM host are silently ignored.
26-6527-129	Alc-ATM-Egress-TD-Profile	The ATM Traffic Descriptor override for a PPPoA or PPPoEoA host and refers to the pre-configured traffic description QoS profile applied on the egress ATM Virtual Circuit (**configure qos atm-td-profile** <*traffic-desc-profile-id*>). All subscriber hosts on a given ATM VC must have same ATM traffic descriptors and this attribute is ignored if it specifies an ATM Traffic Descriptor override while it has already specified another one for another host on the same ATM Virtual Circuit. A pre-configured description profile per ATM Virtual Circuit is used when this attribute is omitted (**configure subscriber-mgmt msap-policy atm egress/ingress traffic-desc or configure service vprn** <*service-id*> **subscriber-interface** <*ip-int-name*> **group-interface** <*ip-int-name*> **sap** <*sap-id*> **atm egress/ingress traffic-desc**). A Traffic Descriptor profile above the Limits is treated as a setup failure. Unreferenced Traffic Descriptor profiles within the Limits, or a Traffic Descriptor profile for a non ATM host are silently ignored.
26-6527-131	Alc-Delegated-IPv6-Pool	The name of an assigned pool that should be used to assign an IPv6 prefix via DHCPv6(IA-PD) to the LAN side of the user (IPoE, PPPoE). Maps to DHCPv6 vendor-option[17],sub-option[2] pfx-pool. Alc-Delegated-ipv6-pool names longer than the allowed maximum are treated as host setup failures. Alternative method for [123] Delegated-IPv6-Prefix so simultaneous returned attributes [123] Delegated-IPv6-Prefix and [26-6527-131] Alc-Delegated-IPv6-Pool are handled as host setup failures. The length information [DPL] can be supplied via [26-6527-161] Alc-Delegated-IPv6-Prefix-Length along with the pool name. The [26-6527-161] Alc-Delegated-IPv6-Prefix-Length has priority over other possible sources of DPL. (As a fixed or variable DPL under **configure service ies/vprn subscriber-interface ipv6 delegated-prefix-length** or on the dhcpv6 server **configure router dhcp6 local-dhcp-server** <*server-name*> **pool** <*pool-name*> **delegated-prefix-length**).

Table 1: Subscriber Host Identification (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-132	Alc-Access-Loop-Rate-Down	The actual downstream rate (coded in kbits per second) of a PPPoE subscriber's synchronized DSL link and competes with the value received from alternative sources (dsl-forum tags, ludb, ancp). Values outside the Limits are treated as setup failures. Attribute is silently ignored for None-MLPPP sessions or IPoE sessions.
26-6527-133	Alc-Access-Loop-Encap-Offset	The last mile encapsulation representing the subscribers DSL access loop encapsulation and when returned in RADIUS-Accept (PTA or LAC) is taken into account for ALE adjust (last mile aware shaping) but not reflected in [26-3561-144] Access-Loop-Encapsulation (access-loop-options) send to Accounting. For LAC this attributes maps to LTP AVP [3561-144] Access-Loop-Encapsulation.
26-6527-135	Alc-PPP-Force-IPv6CP	Forces IPv6CP negotiation in conditions were the Access-Accept does not return any ipv6 related attributes (v6 pool, v6 prefix, v6 address, dnsv6).Without these ipv6 related attributes the NAS has no way to detect that this is a dual-stack pppoe user and therefore it will not start IPv6CP unless this attribute is returned in the Access-Accept. Values 1 triggers ipv6cp and value 0 is treated the same as not sending the attribute. Values different than the Limits are treated as setup failures.
26-6527-136	Alc-Onetime-Http-Redirection-Filter-Id	The pre-configured ipv4 filter with http-redirection rules. Via this host specific filter only the first HTTP request from the host will be redirected to a configured URL with specified parameters. There is no HTTP redirection for subsequent HTTP requests. Useful in cases where service providers need to push a web page of advertisement/announcements to broadband users.
26-6527-160	Alc-Relative-Session-Timeout	Sets or resets the IPoE/PPPoE session timeout to a relative value (current session time + newly received Alc-Relative-Session-Timeout). Attribute equals to [27] Session-Timeout if received in Access-Accept since current session time portion is than zero. Value zero sets/resets the session-timeout to infinite (no session-timeout). Simultaneous received [27] Session-Timeout and [26-6527-160] Alc-Relative-Session-Timeout are treated as a setup failure (setup failure if received in Access-Accept and ignored if received in CoA).
26-6527-161	Alc-Delegated-IPv6-Prefix-Length	Defines the IA-PD length information [DPL] and only applicable together with [26-6527-131] Alc-Delegated-IPv6-Pool (silently ignored if received in RADIUS Accept without Alc-Delegated-IPv6-Pool). Maps to DHCPv6 vendor-option[17] ,sub-option[3] pfx-len. The [26-6527-161] Alc-Delegated-IPv6-Prefix-Length has priority over other possible sources of DPL. (As a fixed or variable DPL under **configure service ies/vprn** <*service-id*> **subscriber-interface** <*ip-int-name*> **ipv6 delegated-prefix-length** or on the dhcpv6 server **configure router dhcp6 local-dhcp-server** <*server-name* **pool** <*pool-name*> **delegated-prefix-length**). DPL values outside the limits are treated as setup failures.

Table 1: Subscriber Host Identification (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-174	Alc-Lease-Time	Defines the lease-time in seconds for RADIUS proxy and create-host-CoA scenarios only. The [27] Session-Timeout is interpreted and used as IPoE lease-time if [26-6527-174] Alc-lease-Time is omitted. The maximum value 4294967295 corresponds with a lease-time > 9999 days (24855d 03h). Value zero triggers to fallback to the default lease-time of 7 days. Returning attribute [26-6527-174] Alc-Lease-Time in other scenarios then radius-proxy and create-host-CoA are treated as setup failures.
26-6527-175	Alc-DSL-Line-State	Status of the DSL line obtained via ANCP can be one of three value: SHOWTIME (the modem is ready to transfer data), IDLE (line is idle) or SILENT (line is silent). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options.**
26-6527-176	Alc-DSL-Type	Type of the DSL line (ADSL1, ADSL2, ADSL2PLUS, VDSL1, VDSL2, SDSL, other) obtained via ANCP. Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-6527-177	Alc-Portal-Url	The URL to which traffic matching the host's IPv4 filter entry with http-redirect action is redirected to. The URL overrides the configured URL in the redirect filter. Radius overrides must explicitly be enabled: **configure filter ip-filter** <*filter-id*> **entry** <*entry-id*> **action http-redirect** <*rdr-url-string*> **allow-radius-override**.
26-6527-178	Alc-Ipv6-Portal-Url	The URL to which traffic matching the host's IPv6 filter entry with http-redirect action is redirected to. The URL overrides the configured URL in the redirect filter. RADIUS overrides must explicitly be enabled: **configure filter ipv6-filter** <*filter-id*> **entry** <*entry-id*> **action http-redirect** <*rdr-url-string*> **allow-radius-override**.
26-6527-180	Alc-SAP-Session-Index	Per SAP unique PPPoE session index that can be included in RADIUS Access Request messages. The lowest free index is assigned to a new PPPoE session. Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy** <*name*> **include-radius-attribute sap-session-index**.
26-6527-181	Alc-SLAAC-IPv6-Pool	A pool name that can be used in local address assignment to assign an IPv6 SLAAC prefix via a Router Advertisement to the WAN side of the IPoE/PPPoE user. Alc-SLAAC-IPv6-Pool names longer than the allowed maximum are treated as host setup failures. If local-address-assignment is not enabled on the group-interface for ipv6 client-application ppp-slaac, then the PPP session will be terminated. If local-address-assignment is not enabled on the group-interface for ipv6 client-application ipoe-slaac, then the IPoE host will not be instantiated.

Table 1: Subscriber Host Identification (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-183	Alc-WPP-Error-Code	This attribute specifies the value of the ErrCode that the system should use in a WPP ACK_AUTH packet. This attribute can only be included in a Radius Access-Reject packet.
26-6527-185	Alc-Onetime-Http-Redirect-Reactivate	An indication to reactivate a onetime http redirect filter for the host. When received in a Radius CoA message, • the filter with the value indicated by [26-6527-136] Alc-Onetime-Http-Redirection-Filter-Id is activated. • If [26-6527-136] Alc-Onetime-Http-Redirection-Filter-Id contains the value 0, then the existing onetime http redirect filter id associated with the host is removed. • if no [26-6527-136] Alc-Onetime-Http-Redirection-Filter-Id VSA is provided in the RADIUS CoA message, then the existing onetime http redirect filter id associated with the host is applied. The value of the [26-6527-185] Alc-Onetime-Http-Redirect-Reactivate VSA is opaque. It is the presence of the VSA in a RADIUS CoA that triggers the action.

Table 2: Subscriber Host Identification (limits)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
1	User-Name	string	253 chars	Form depends on authentication method and configuration. For example: User-Name user1@domain1.com
2	User-Password	string	64 Bytes	Encrypted password For example: User-Password 4ec1b7bea6f2892fa466b461c6accc00
3	CHAP-Password	octets	16+1 Bytes	Users CHAP identifier 1 followed by the Encrypted password For example: CHAP-Password 01ef8ddc7237f4adcd991ac4c277d312e9
4	NAS-IP-Address	ipaddr	4 Bytes	# ipv4 address For example: NAS-IP-Address=192.0.2.1
5	NAS-Port	integer	4 Bytes	nas-port <binary-spec> <binary-spec> = <bit-specification> <binary-spec> <bit-specification> = 0 | 1 | <bit-origin> <bit-origin> = *<number-of-bits><origin> <number-of-bits> = [1..32] <origin> = o (outer VLAN ID), i (inner VLAN ID), s (slot number), m (MDA number), p (port number or lag-id), v (ATM VPI), c (ATM VCI) For example: # configured nas-port *12o*10i*3s*2m*5p for SAP 2/2/4:221.7 corresponds to 000011011101 0000000111 010 10 00100 NAS-Port = 231742788
6	Service-Type	integer	2 (mandatory value)	PPPoE and PPPoL2TP hosts only For example: Service-Type = Framed-User
7	Framed-Protocol	integer	1 (fixed value)	PPPoE and PPPoL2TP hosts only For example: Service-Type = PPP
8	Framed-IP-Address	ipaddr	4 Bytes	For example: # ip-address 10.11.12.13 Framed-IP-Address 0a0b0c0d

9	Framed-IP-Netmask	ipaddr	4 Bytes	For example: Framed-IP-Netmask = 255.255.255.255 #PPPoE residential
				Framed-IP-Netmask = 255.255.255.0 #PPPoE Business with IPCP option 144 support
				Framed-IP-Netmask = 255.255.255.0 # IPoE

18	Reply-Message	string	253 chars	For example: Reply-Message MyCustomizedReplyMessage

Table 2: Subscriber Host Identification (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
22	Framed-Route	string	max 16 Framed-Routes attributes	""<ip-prefix>[/<prefix-length>] <space> <gateway-address> [<space> <metric>] [<space> tag <space> <tag-value>] [<space> pref <space> <preference-value>]" where: <space> is a white space or blank character <ip-prefix>[/prefix-length] is the managed route to be associated with the routed subscriber host. The prefix-length is optional and if not specified, a class-full class A,B or C subnet is assumed. <gateway-address> must be the routed subscriber host IP address. "0.0.0.0" is automatically interpreted as the host IPv4 address. [<metric>] (Optional) Installed in the routing table as the metric of the managed route. If not specified, metric zero is used. Value = [0.. 65535] [tag <tag-value>] (Optional) The managed route will be tagged for use in routing policies. If not specified or tag-value=0, then the route is not tagged. Value = [0..4294967295] [pref <preference-value>] (Optional) Installed in the routing table as protocol preference for this managed route. If not specified, preference zero is used. Value = [0..255] For example: Framed-Route = "192.168.1.0/24 0.0.0.0" where 0.0.0.0 is replaced by host address. Default metrics are used (metric=0, preference=0 and no tag) Framed-Route = "192.168.1.0 0.0.0.0" where 192.168.1.0 is a class-C network /24 and 0.0.0.0 is replaced host address. Default metrics are used. Framed-Route = "192.168.1.0/24 192.168.1.1" where 192.168.1.1 is the host address. Default metrics are used. Framed-Route = "192.168.1.0 0.0.0.0 10 tag 3 pref 100" installs a managed route with metric=10, protocol preference = 100 and tagged with tag=3 Framed-Route = "192.168.1.0 0.0.0.0 tag 5" installs a managed route with metric=0 (default), protocol preference = 0 (default) and tagged with tag=5"
25	Class	octets	253 chars	For example: Class = My Class

Table 2: Subscriber Host Identification (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
27	Session-Timeout	integer	[0..2147483647] seconds	# 0 = infinite (no session-timeout) # [0..2147483647] in seconds For example: Session-Timeout = 3600
28	Idle-Timeout	integer	[60..15552000] seconds	# 0 = infinite (no idle-timeout) # [60..15552000] in seconds For example: Idle-Timeout = 3600
30	Called-Station-Id	string	64 chars	# LNS: L2TP Called Number AVP21 from LAC For example: Called-Station-Id = 4441212
31	Calling-Station-Id	string	64 chars	# llid|mac|remote-id|sap-id|sap-string (64 char. string configured at sap-level) For example: include-radius-attribute calling-station-id sap-id Calling-Station-Id = 1/1/2:1.1
32	NAS-Identifier	string	32 chars	For example: NAS-Identifier = PE1-Antwerp
44	Acct-Session-Id	string	22 bytes	No useful information can be extracted from the string. For example: # internal generated asid 22 Bytes/chars: 0x32343141464630303030303033323530423546373530 Acct-Session-Id = 241AFF0000003250B5F750
55	Event-Timestamp	date	4 Bytes	For example: # Jul 6 2012 17:28:23 CEST is reported as 4FF70417 Event-Timestamp = 4FF70417
60	CHAP-Challenge	octets	[8..64] Bytes	random length For example: 20 bytes CHAP-Challenge 0xa9710d2386c3e1771b8a3ea3d4e53f2a1c7024fb
61	NAS-Port-Type	integer	4 Bytes Values [0..255]	Values as defined in rfc-2865 and rfc-4603 For LNS, the value is set to virtual (5) For example: NAS-Port-Type = PPPoEoQinQ (34)
85	Acct-Interim-Interval	integer	4 Bytes	[300..15552000] seconds For example: # 1 hour interval for interim updates Acct-Interim-Interval = 3600

Table 2: Subscriber Host Identification (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
87	NAS-Port-Id	string	253 Bytes in Access-Request and Accounting Request messages. 128 Bytes in CoA	<prefix> : optional string 8 chars max <suffix> : optional string remote-id (max 64 chars) | circuit-id (max 64 chars) # NON-ATM and NON-LNS : <prefix><space><slot>/<mda>/<port>/<vlan>.<vlan><space><suffix> # ATM : <prefix><space><slot>/<mda>/<port>/<vpi>.<vci><space><suffix> # LNS : LNS rt-<routing instance>#lip-<tunnel-server-endpoint>#rip-<tunnel-client-endpoint>#ltid-<local-tunnel-id>#rtid-<remote-tunnel-id>#lsid-<local-session-id>#rsid-<remote-session-id>#<call sequence number> For example: NAS-Port-Id = 1/1/4:501.1001 NAS-Port-Id = LNS rtr-2#lip-3.3.3.3#rip-1.1.1.1#ltid-11381#rtid-1285#lsid-30067#rsid-19151#347
88	Framed-Pool	string	32 chars. per pool name. 65 chars. in total (primary pool, delimiter, secondary pool)	For example: Framed-Pool = MyPoolname
95	NAS-IPv6-Address	ipv6addr	16 Bytes	# ipv6 address For example: NAS-IPv6-Address = 2001:db8::1
97	Framed-IPv6-Prefix	ipv6prefix	max. 16 Bytes for prefix + 1 byte for length	PPPoE SLAAC wan-host <ipv6-prefix/prefix-length> with prefix-length 64 For example: Framed-IPv6-Prefix 2021:1:FFF3:1::/64

Table 2: Subscriber Host Identification (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
99	Framed-IPv6-Route	string	max. 16 Framed-IPv6-Route attributes	"<ip-prefix>/<prefix-length> <space> <gateway-address> [<space> <metric>] [<space> tag <space> <tag-value>] [<space> pref <space> <preference-value>]” where: <space> is a white space or blank character <ip-prefix>/<prefix-length> is the managed route to be associated with the routed subscriber host. <gateway-address> must be the routed subscriber host IP address. “::” and “0:0:0:0:0:0:0:0” are automatically interpreted as the wan-host IPv6 address. [<metric>] (Optional) Installed in the routing table as the metric of the managed route. If not specified, metric zero is used. Value = [0.. 65535] [tag <tag-value>] (Optional) The managed route will be tagged for use in routing policies. If not specified or tag-value=0, then the route is not tagged. Value = [0..4294967295] [pref <preference-value>] (Optional) Installed in the routing table as protocol preference for this managed route. If not specified, preference zero is used. Value = [0..255] For example: Framed-IPv6-Route = "5000:0:1::/48 ::" where :: resolves in the wan-host. Default metrics are used (metric=0, preference=0 and no tag) Framed-IPv6-Route = "5000:0:2::/48 0:0:0:0:0:0:0:0" where 0:0:0:0:0:0:0:0 resolves in the wan-host. Default metrics are used. Framed-IPv6-Route = "5000:0:3::/48 0::0" where 0::0 resolves in the wan-host. Default metrics are used. Framed-IPv6-Route = "5000:0:3::/48 2021:1::1" where 2021:1::1 is the wan-host. Default metrics are used. Framed-IPv6-Route = "5000:0:1::/48 :: 10 tag 3 pref 100" installs a managed route with metric = 10, protocol preference = 100 and tagged with tag = 3 Framed-IPv6-Route = "5000:0:1::/48 :: tag 5" installs a managed route with metric = 0 (default), protocol preference = 0 (default) and tagged with tag = 5
100	Framed-IPv6-Pool	string	32 chars	For example: Framed-IPv6-Pool MyWanPoolnameIANA

Table 2: Subscriber Host Identification (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
101	Error-Cause	octets	4 Bytes	Current supported causes are: Missing Attribute[402], NAS Identification Mismatch[403], Invalid Request[404], Unsupported Service[405], Invalid Attribute Value[407], Administratively Prohibited [501], Session Context Not Found [503], Resources Unavailable[506] For example: Error-Cause = Invalid Request
123	Delegated-IPv6-Prefix	ipv6prefix	max. 16 Bytes for prefix + 1 Byte for length	<ipv6-prefix/prefix-length> with prefix-length [48..64] For example: Delegated-IPv6-Prefix 2001:DB8:173A:100::/56
26-2352-1	Client-DNS-Pri	ipaddr	4 Bytes	For example: Client-DNS-Pri = 9.1.1.1
26-2352-2	Client-DNS-Sec	ipaddr	4 Bytes	For example: Client-DNS-Sec = 9.1.1.2
26-2352-36	Ip-Address-Pool-Name	string	65 chars	For example: Ip-Address-Pool-Name = Address_Pool_1
26-2352-99	RB-Client-NBNS-Pri	ipaddr	4 Bytes	For example: RB-Client-NBNS-Pri = 9.1.1.1
26-2352-100	RB-Client-NBNS-Sec	ipaddr	4 Bytes	For example: RB-Client-NBNS-Sec = 9.1.1.2
26-3561-1	Agent-Circuit-Id	string	247 chars	format see also RFC4679 # ATM/DSL <Access-Node-Identifier><atm slot/port:vpi.vci> # Ethernet/DSL <Access-Node-Identifier><eth slot/port[:vlan-id]> For example: ethernet dslam1 slot 2 port 1 vlan 100 Agent-Circuit-Id = dslam1 eth 2/1:100
26-3561-2	Agent-Remote-Id	string	247 chars	Format see also RFC4679 For example: Agent-Remote-Id = MyRemoteId
26-3561-129	Actual-Data-Rate-Upstream	integer	4294967295 bps	For example: # 1Mbps Actual-Data-Rate-Upstream = 1000000
26-3561-130	Actual-Data-Rate-Downstream	integer	4294967295 bps	For example: # 5Mbps Actual-Data-Rate-Downstream = 5000000

Table 2: Subscriber Host Identification (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-3561-131	Minimum-Data-Rate-Upstream	integer	4294967295 bps	For example: Minimum-Data-Rate-Upstream = 1000
26-3561-132	Minimum-Data-Rate-Downstream	integer	4294967295 bps	For example: Minimum-Data-Rate-Downstream = 1000
26-3561-133	Attainable-Data-Rate-Upstream	integer	4294967295 bps	For example: Attainable-Data-Rate-Downstream = 1000
26-3561-134	Attainable-Data-Rate-Downstream	integer	4294967295 bps	For example: Minimum-Data-Rate-Upstream = 1000
26-3561-135	Maximum-Data-Rate-Upstream	integer	4294967295 bps	For example: Maximum-Data-Rate-Upstream = 1000
26-3561-136	Maximum-Data-Rate-Downstream	integer	4294967295 bps	For example: Maximum-Data-Rate-Downstream = 1000
26-3561-137	Minimum-Data-Rate-Upstream-Low-Power	integer	4294967295 bps	For example: Minimum-Data-Rate-Upstream-Low-Power = 1000
26-3561-138	Minimum-Data-Rate-Downstream-Low-Power	integer	4294967295 bps	For example: Minimum-Data-Rate-Downstream-Low-Power = 1000
26-3561-139	Maximum-Interleaving-Delay-Upstream	integer	4294967295 milliseconds	For example: Maximum-Interleaving-Delay-Upstream = 10
26-3561-140	Actual-Interleaving-Delay-Upstream	integer	4294967295 milliseconds	For example: Actual-Interleaving-Delay-Upstream = 10

Table 2: Subscriber Host Identification (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-3561-141	Maximum-Interleaving-Delay-Downstream	integer	4294967295 milliseconds	For example: Maximum-Interleaving-Delay-Downstream = 10
26-3561-142	Actual-Interleaving-Delay-Downstream	integer	4294967295 milliseconds	For example: Actual-Interleaving-Delay-Downstream = 10
26-3561-144	Access-Loop-Encapsulation	octets	3 Bytes	<Data Link><Encaps-1><Encaps-2> <Data Link>: AAL5(1), Ethernet(2) <Encaps 1>: NotAvailable(0), Untagged Ethernet(1), Single-Tagged Ethernet(2) <Encaps 2>: Not Available(0), PPPoA LLC(1), PPPoA Null(2), IPoA LLC(3), IPoA Null(4), Ethernet over AAL5 LLC w FCS(5), Ethernet over AAL5 LLC w/o FCS(6), Ethernet over AAL5 Null w FCS(7), Ethernet over AAL5 Null w/o FCS(8) For example: Ethernet, Single-Tagged Ethernet , Ethernet over AAL5 LLC w FCS Access-Loop-Encapsulation = 020205
26-3561-254	IWF-Session	octets	len 0	For example: IWF-Session
26-4874-2	ERX-Address-Pool-Name	string	65 chars	For example: ERX-Address-Pool-Name = MyPoolname
26-4874-4	ERX-Primary-Dns	ipadress	4 Bytes	For example: ERX-Primary-Dns = 9.1.1.1
26-4874-5	ERX-Secondary-Dns	ipadress	4 Bytes	For example: ERX-Secondary-Dns = 9.1.1.2
26-4874-6	ERX-Primary-Wins	ipadress	4 Bytes	For example: ERX-Primary-Wins = 9.1.1.1
26-4874-7	ERX-Secondary-Wins	ipadress	4 Bytes	For example: ERX-Ipv6-Primary-Dns = 9.1.1.2
26-4874-47	ERX-Ipv6-Primary-Dns	ipv6addr	16 Bytes	For example: ERX-Secondary-Wins = 4000::1:1:1:1

Table 2: Subscriber Host Identification (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-4874-48	ERX-Ipv6-Secondary-Dns	ipv6addr	16 Bytes	For example: ERX-Ipv6-Secondary-Dns = 4000::1:1:1:2
26-6527-9	Alc-Primary-Dns	ipaddr	4 Bytes	For example: Alc-Primary-Dns = 9.1.1.1
26-6527-10	Alc-Secondary-Dns	ipaddr	4 Bytes	For example: Alc-Secondary-Dns = 9.1.1.2
26-6527-11	Alc-Subsc-ID-Str	string	32 chars	For example: Alc-Subsc-ID-Str = MySubscriberId
26-6527-12	Alc-Subsc-Prof-Str	string	16 chars	For example: Alc-Subsc-Prof-Str = MySubProfile
26-6527-13	Alc-SLA-Prof-Str	string	16 chars	For example: Alc-SLA-Prof-Str = MySlaProfile
26-6527-16	Alc-ANCP-Str	string	63 chars	format see also RFC4679 # ATM/DSL <Access-Node-Identifier><atm slot/port:vpi.vci> # Ethernet/DSL <Access-Node-Identifier><eth slot/port[:vlan-id]> For example: If [26-3561-1] Agent-Circuit-Id = dslam1 eth 2/1:100 then put Alc-ANCP-Str = dslam1 eth 2/1:100
26-6527-18	Alc-Default-Router	ipaddr	4 Bytes	For example: Alc-Default-Router = 185.2.255.254
26-6527-27	Alc-Client-Hardware-Addr	string	6 Bytes	For example: Alc-Client-Hardware-Addr = 00:00:00:00:00:01
26-6527-28	Alc-Int-Dest-Id-Str	string	32 chars	For example: Alc-Int-Dest-Id-Str= AccessNode1
26-6527-29	Alc-Primary-Nbns	ipaddr	4 Bytes	For example: Alc-Primary-Nbns = 9.1.1.1
26-6527-30	Alc-Secondary-Nbns	ipaddr	4 Bytes	For example: Alc-Secondary-Nbns = 9.1.1.2
26-6527-34	Alc-PPPoE-PADO-Delay	integer	[0..30] deci-seconds	For example: 3 seconds pado-delay Alc-PPPoE-PADO-Delay = 30

Table 2: Subscriber Host Identification (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-35	Alc-PPPoE-Service-Name	string	247 chars	For example: Alc-PPPoE-Service-Name = MyServiceName
26-6527-36	Alc-DHCP-Vendor-Class-Id	string	no limits	For example: Alc-DHCP-Vendor-Class-Id = My-DHCP-VendorClassId
26-6527-45	Alc-App-Prof-Str	string	16 bytes	# For example: Alc-App-Prof-Str = MyAppProfile
26-6527-99	Alc-Ipv6-Address	ipv6addr	16 Bytes	For example: Alc-Ipv6-Address 2021:1:FFF5::1
26-6527-102	Alc-ToServer-Dhcp-Options	octets	2 attributes 247 Bytes/ attribute 494 Bytes total	For example: DHCPv4 Discover , option-60 [Class-identifier-option] = DHCP-VendorClassId ; Agent-Circuit-Id = circuit10;Agent-Remote-Id = remote10 Alc-ToServer-Dhcp-Options = 66313501013c12444843502d56656e646f72436c617373496452150109636972637569743130020872656d6f74653130
26-6527-103	Alc-ToClient-Dhcp-Options	octets	8 attributes 247 Bytes/ attribute 494 Bytes total	For example: Insert DHCP Option 121, length=7, 16.192.168 10.1.255.254 # Classless Static Route: 192.168.0.0/16 10.1.255.254 Alc-ToClient-Dhcp-Options = 0x790710C0A80A01FFFE
26-6527-105	Alc-Ipv6-Primary-Dns	ipv6addr	16 Bytes	For example: Alc-Ipv6-Primary-Dns = 4000::1:1:1:2
26-6527-106	Alc-Ipv6-Secondary-Dns	ipv6addr	16 Bytes	For example: Alc-Ipv6-Secondary-Dns = 4000::1:1:1:2
26-6527-126	Alc-Subscriber-QoS-Override	string	18 attributes	ingress(i|I) ; egress(e|E) [iIeE]:[qQ]:queue-id:(pir|cir|mbs|cbs|wrr_weight) [iIeE]:[pP]:policer-id:(pir|cir|mbs|cbs) [iIeE]:[rR]:rate [iIeE]:[aA]:root:rate Remark: wrr_weight is egress queues [1..4] hsmdsv2 only For example: ingress queue 1 pir,cir,mbs,cbs and egress aggregate rate 800000 Alc-Subscriber-QoS-Override +=i:q:1:pir=40000,cir=20000,mbs=32000,cbs=16000 Alc-Subscriber-QoS-Override +=e:r:rate=800000,

Table 2: Subscriber Host Identification (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-128	Alc-ATM-Ingress-TD-Profile	integer	[1..1000] id	For example: Alc-ATM-Ingress-TD-Profile = 10
26-6527-129	Alc-ATM-Egress-TD-Profile	integer	[1..1000] id	For example: Alc-ATM-Egress-TD-Profile = 10
26-6527-131	Alc-Delegated-IPv6-Pool	string	32 chars	For example: Alc-Delegated-IPv6-Pool = MyLanPoolnameIAPD
26-6527-132	Alc-Access-Loop-Rate-Down	integer	[1..100000] kbps	For example: rate 4Mbps Alc-Access-Loop-Rate-Down = 4000
26-6527-133	Alc-Access-Loop-Encap-Offset	octets	3 bytes	<Data Link><Encaps-1><Encaps-2> <Data Link>: AAL5(0), Ethernet(1) <Encaps 1>: NotAvailable(0), Untagged Ethernet(1), Single-Tagged Ethernet(2) <Encaps 2>: Not Available(0), PPPoA LLC(1), PPPoA Null(2), IPoA LLC(3), IPoA Null(4), Ethernet over AAL5 LLC w FCS(5), Ethernet over AAL5 LLC w/o FCS(6), Ethernet over AAL5 Null w FCS(7), Ethernet over AAL5 Null w/o FCS(8) For example: # pppoe-tagged -> 01,02,00 Alc-Access-Loop-Encap-Offset = 0x010200 # pppoeoa-llc -> 00,01,06 Alc-Access-Loop-Encap-Offset = 0x000106 # pppoa-llc -> 00 00 01 Alc-Access-Loop-Encap-Offset = 0x000001
26-6527-135	Alc-PPP-Force-IPv6CP	integer	[0..1] false|true	For example: Alc-PPP-Force-IPv6CP = 1
26-6527-136	Alc-Onetime-Http-Redirection-Filter-Id	string	249 Bytes	“Ingr-v4:<number>” [1..65535] = apply this filter-id as one-time-http-redirect-filter 0 = Remove the current redirection filter and replace it with sla-profile ingress filter For example: Alc-Onetime-Http-Redirection-Filter-Id = Ingr-v4:1000
26-6527-160	Alc-Relative-Session-Timeout	integer	[0..2147483647] seconds	0 = infinite (no session-timeout) [0..2147483647] in seconds For example: Alc-Relative-Session-Timeout = 3600

Table 2: Subscriber Host Identification (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-161	Alc-Delegated-IPv6-Prefix-Length	integer	[48..64] DPL length	For example: Alc-Delegated-IPv6-Prefix-Length = 48
26-6527-174	Alc-Lease-Time	integer	[0..4294967295] seconds	0 : fallback to the default lease-time of 7 days. [1..4294967295] lease-time is seconds For example: Alc-Lease-Time = 3600
26-6527-175	Alc-DSL-Line-State	integer	4 Bytes	1=showtime, 2-idle, 3=silent For example: Alc-DSL-Line-State = SHOWTIME
26-6527-176	Alc-DSL-Type	integer	4 Bytes	0=other, 1=ADSL1, 2=ADSL2, 3=ADSL2PLUS, 4=VDSL1, 5=VDSL2, 6=SDSL For example: Alc-DSL-Type = VDSL2
26-6527-177	Alc-Portal-Url	string	247 chars	For example: Alc-Portal-Url = “http://portal.com/welcome?sub=$SUB”
26-6527-178	Alc-Ipv6-Portal-Url	string	247 chars	For example: Alc-IPv6-Portal-Url = “http://portal.com/welcome?sub=$SUB”
26-6527-180	Alc-SAP-Session-Index	integer	4 Bytes	For example: Alc-SAP-Session-Index = 5
26-6527-181	Alc-SLAAC-IPv6-Pool	string	32 chars	# For example Alc-SLAAC-IPv6-Pool = "MySlaacPoolname"
26-6527-183	Alc-WPP-Error-Code	integer	4 Bytes	A non-zero unsigned integer. Valid values are 1, 2 or 4
26-6527-185	Alc-Onetime-Http-Redirect-Reactivate	string	247 chars	The value of the attribute is opaque. Its presence in a RADIUS CoA triggers the action.

Table 3: Subscriber Host Identification (applicability)

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request
1	User-Name	1	0-1	0-1
2	User-Password	0-1	0	0
3	CHAP-Password	0-1	0	0
4	NAS-IP-Address	0-1	0	0
5	NAS-Port	0-1	0	0
6	Service-Type	0-1	0-1	0-1
7	Framed-Protocol	0-1	0-1	0-1
8	Framed-IP-Address	0	0-1	0-1
9	Framed-IP-Netmask	0	0-1	0
18	Reply-Message	0	0-1	0
22	Framed-Route	0	0+	0
25	Class	0	0-1	0-1
27	Session-Timeout	0	0-1	0-1
28	Idle-Timeout	0	0-1	0-1
30	Called-Station-Id	0-1	0	0-1
31	Calling-Station-Id	0-1	0-1	0-1
32	NAS-Identifier	0-1	0	0
44	Acct-Session-Id	0-1	0	0-1
55	Event-Timestamp	0	0	0
60	CHAP-Challenge	0-1	0	0
61	NAS-Port-Type	0-1	0	0-1
85	Acct-Interim-Interval	0	0-1	0-1
87	NAS-Port-Id	0-1	0	0-1
88	Framed-Pool	0	0-1	0
95	NAS-IPv6-Address	0-1	0	0
97	Framed-IPv6-Prefix	0	0-1	0-1

Table 3: Subscriber Host Identification (applicability) (Continued)

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request
99	Framed-IPv6-Route	0	0+	0
100	Framed-IPv6-Pool	0	0-1	0
101	Error-Cause	0	0	0-1
123	Delegated-IPv6-Prefix	0	0-1	0-1
26-2352-1	Client-DNS-Pri	0	0-1	0
26-2352-2	Client-DNS-Sec	0	0-1	0
26-2352-36	Ip-Address-Pool-Name	0	0-1	0
26-2352-99	RB-Client-NBNS-Pri	0	0-1	0
26-2352-100	RB-Client-NBNS-Sec	0	0-1	0
26-3561-1	Agent-Circuit-Id	0-1	0	0
26-3561-2	Agent-Remote-Id	0-1	0	0
26-3561-129	Actual-Data-Rate-Upstream	0-1	0	0
26-3561-130	Actual-Data-Rate-Downstream	0-1	0	0
26-3561-131	Minimum-Data-Rate-Upstream	0-1	0	0
26-3561-132	Minimum-Data-Rate-Downstream	0-1	0	0
26-3561-133	Attainable-Data-Rate-Upstream	0-1	0	0
26-3561-134	Attainable-Data-Rate-Downstream	0-1	0	0
26-3561-135	Maximum-Data-Rate-Upstream	0-1	0	0
26-3561-136	Maximum-Data-Rate-Downstream	0-1	0	0
26-3561-137	Minimum-Data-Rate-Upstream-Low-Power	0-1	0	0
26-3561-138	Minimum-Data-Rate-Downstream-Low-Power	0-1	0	0
26-3561-139	Maximum-Interleaving-Delay-Upstream	0-1	0	0
26-3561-140	Actual-Interleaving-Delay-Upstream	0-1	0	0
26-3561-141	Maximum-Interleaving-Delay-Downstream	0-1	0	0

Table 3: Subscriber Host Identification (applicability) (Continued)

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request
26-3561-142	Actual-Interleaving-Delay-Downstream	0-1	0	0
26-3561-144	Access-Loop-Encapsulation	0-1	0	0
26-3561-254	IWF-Session	0-1	0-1	0
26-4874-2	ERX-Address-Pool-Name	0	0-1	0
26-4874-4	ERX-Primary-Dns	0	0-1	0
26-4874-5	ERX-Secondary-Dns	0	0-1	0
26-4874-6	ERX-Primary-Wins	0	0-1	0
26-4874-7	ERX-Secondary-Wins	0	0-1	0
26-4874-47	ERX-Ipv6-Primary-Dns	0	0-1	0
26-4874-48	ERX-Ipv6-Secondary-Dns	0	0-1	0
26-6527-9	Alc-Primary-Dns	0	0-1	0
26-6527-10	Alc-Secondary-Dns	0	0-1	0
26-6527-11	Alc-Subsc-ID-Str	0	0-1	0-1
26-6527-12	Alc-Subsc-Prof-Str	0	0-1	0-1
26-6527-13	Alc-SLA-Prof-Str	0	0-1	0-1
26-6527-16	Alc-ANCP-Str	0	0-1	0-1
26-6527-18	Alc-Default-Router	0	0-1	0
26-6527-27	Alc-Client-Hardware-Addr	0-1	0-1	0
26-6527-28	Alc-Int-Dest-Id-Str	0	0-1	0-1
26-6527-29	Alc-Primary-Nbns	0	0-1	0
26-6527-30	Alc-Secondary-Nbns	0	0-1	0
26-6527-34	Alc-PPPoE-PADO-Delay	0	0-1	0
26-6527-35	Alc-PPPoE-Service-Name	0-1	0	0
26-6527-36	Alc-DHCP-Vendor-Class-Id	0-1	0	0
26-6527-45	Alc-App-Prof-Str	0	0-1	0-1
26-6527-99	Alc-Ipv6-Address	0	0-1	0-1

Table 3: Subscriber Host Identification (applicability) (Continued)

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request
26-6527-102	Alc-ToServer-Dhcp-Options	0+	0	0
26-6527-103	Alc-ToClient-Dhcp-Options	0	0+	0
26-6527-105	Alc-Ipv6-Primary-Dns	0	0-1	0
26-6527-106	Alc-Ipv6-Secondary-Dns	0	0-1	0
26-6527-126	Alc-Subscriber-QoS-Override	0	0-1	0-1
26-6527-128	Alc-ATM-Ingress-TD-Profile	0	0-1	0
26-6527-129	Alc-ATM-Egress-TD-Profile	0	0-1	0
26-6527-131	Alc-Delegated-IPv6-Pool	0	0-1	0
26-6527-132	Alc-Access-Loop-Rate-Down	0	0-1	0-1
26-6527-133	Alc-Access-Loop-Encap-Offset	0	0-1	0
26-6527-135	Alc-PPP-Force-IPv6CP	0	0-1	0
26-6527-136	Alc-Onetime-Http-Redirection-Filter-Id	0	0-1	0-1
26-6527-160	Alc-Relative-Session-Timeout	0	0-1	0-1
26-6527-161	Alc-Delegated-IPv6-Prefix-Length	0	0-1	0
26-6527-174	Alc-Lease-Time	0	0-1	0
26-6527-175	Alc-DSL-Line-State	0-1	0	0
26-6527-176	Alc-DSL-Type	0-1	0	0
26-6527-177	Alc-Portal-Url	0	0-1	0-1
26-6527-178	Alc-Ipv6-Portal-Url	0	0-1	0-1
26-6527-180	Alc-SAP-Session-Index	0-1	0	0
26-6527-181	Alc-SLAAC-IPv6-Pool	0	0-1	0
26-6527-183	Alc-WPP-Error-Code	0	0 (Access-Reject only)	0
26-6527-185	Alc-Onetime-Http-Redirect-Reactivate	0	0	0-1

Wholesale-Retail — Local Access Mode

Table 4: Wholesale-Retail: Local Access Mode (description)

Attribute ID	Attribute Name	Description
26-6527-17	Alc-Retail-Serv-Id	The service-id of the retailer to which this subscriber host belongs. Both ies/ vprn are supported for ppp hosts and VPRN for dhcpv4 hosts. (**configure service ies/vprn** <*retail-service-id*> **subscriber-interface retail-interface-id fwd-service** <*wholesale-service-id*> fwd-**subscriber-interface** *wholesale-interface-name*>). Returning an ies service-id for a dhcpv4 host is treated as a session setup failure.Not supported for dhcpv6 hosts.
26-6527-31	Alc-MSAP-Serv-Id	The service-id (IES/VPRN) where Managed SAP's are created.(**configure service ies/vprn** <*service-id*>). If this attribute is omitted, use msap defaults created under ludb or capture VPLS.(**configure subscriber-mgmt local-user-db** <*local-user-db-name*> **ppp/dhcp host msap-defaults service** <*service-id*> or **configure service vpls** <*service-id* **sap** <*sap-id*> **msap-defaults service** <*service-id*>). This omitted attribute without explicit created msap-defaults is treated as a setup failure.
26-6527-32	Alc-MSAP-Policy	Managed sap policy-name used to create Managed SAPs and refers to the CLI context **configure subscriber-mgmt msap-policy** <*msap-policy-name*>). The policy contains similar parameters that you would configure for a regular subscriber SAP. If this attribute is omitted we have to option to will fall back to msap defaults created under ludb or capture VPLS. (**configure subscriber-mgmt local-user-db ppp/dhcp host msap-defaults policy** <*msap-policy-name*> or **configure service vpls sap msap-defaults policy** <*msap-policy-name*>).This omitted attribute without explicit created msap-defaults is treated as a setup failure.
26-6527-33	Alc-MSAP-Interface	The group-interface-name where Managed SAPs are created and refers to CLI context **configure service ies/vprn subscriber-interface** <*ip-int-name*> **group-interface** <*ip-int-name*> **policy** <*msap-policy-name*>. If this attribute is omitted we have to option to will fall back to msap defaults created under ludb or capture VPLS. (**configure subscriber-mgmt local-user-db** <*local-user-db-name*> **ppp/dhcp host msap-defaults group-interface** <*ip-int-name*> or **configure service** <*service-id*> **vpls sap** <*sap-id*> **msap-defaults group-interface** <*ip-int-name*>). Strings above the Limits and an omitted attribute without explicit created msap-defaults are treated as setup failures.

Table 5: Wholesale-Retail: local access mode (limits)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-17	Alc-Retail-Serv-Id	integer	2147483647 id	For example: Alc-Retail-Serv-Id = 10
26-6527-31	Alc-MSAP-Serv-Id	integer	2147483647 id	For example: Alc-MSAP-Serv-Id = 20
26-6527-32	Alc-MSAP-Policy	string	32 chars	Policy may start with a letter or number For example: Alc-MSAP-Policy = 1-Policy-business
26-6527-33	Alc-MSAP-Interface	string	32 chars	Interface-name must start with a letter For example: Alc-MSAP-Interface = group-1

Table 6: Wholesale-Retail: Local Access Mode (applicability)

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request
26-6527-17	Alc-Retail-Serv-Id	0	0-1	0
26-6527-31	Alc-MSAP-Serv-Id	0	0-1	0
26-6527-32	Alc-MSAP-Policy	0	0-1	0
26-6527-33	Alc-MSAP-Interface	0	0-1	0

Wholesale-Retail — L2TP Tunneled Access Mode

Table 7: Wholesale-Retail: L2TP Tunneled Access Mode (description)

Attribute ID	Attribute Name	Description
64	Tunnel-Type	The tunneling protocol(s) to be used (in the case of a tunnel initiator) or the tunneling protocol in use (in the case of a tunnel terminator). This attribute is mandatory on LAC Access-Accept and needs to be L2TP. The same attribute is included on LNS in the Access-Request and Acct-Request if the CLI RADIUS policy include-radius-attribute tunnel-server-attrs is enabled on 7x50 LNS. For L2TP Tunnel/Link Accounting this attribute is always included on LAC and LNS.
65	Tunnel-Medium-Type	The transport medium to use when creating a tunnel for those protocols (such as L2TP) that can operate over multiple transports. This attribute is mandatory on LAC Access-Accept and needs to be IP or 'IPv4.The same attribute is included on LNS in the Access-Request and Acct-Request if the CLI RADIUS policy include-radius-attribute tunnel-server-attrs is enabled on 7x50 LNS. For L2TP Tunnel/Link Accounting this attribute is always included on LAC and LNS.
66	Tunnel-Client-Endpoint	The dotted-decimal IP address of the initiator end of the tunnel. Pre-configured values are used when attribute is omitted (**configure router/service vprn** <*service-id*> **l2tp local-address**). If omitted in Access Accept on LAC and no local-address configured, then the address is taken from the interface with name system. This attribute is included on LNS in the Access-Request and Acct-Request only if the CLI RADIUS policy include-radius-attribute tunnel-server-attrs is enabled on 7x50 LNS. For L2TP Tunnel/Link Accounting this attribute is always included on LAC and LNS as untagged.
67	Tunnel-Server-Endpoint	The dotted-decimal IP address of the server end of the tunnel and is on the LAC the dest-ip for all L2TP packets for that tunnel.
69	Tunnel-Password	A shared, salt encrypted, secret used for tunnel authentication and AVP-hiding. The usage of tunnel-authentication is indicated by attribute [26-6527-97] Alc-Tunnel-Challenge and the usage of AVP-hiding is indicated by attribute [26-6527-54] Alc-Tunnel-AVP-Hiding. The value with tag 0 is used as default for the tunnels where the value is not specified. Pre-configured values are used when attribute is omitted (**configure router/service vprn** <*service-id*> **l2tp password**). There is no default password. Received passwords longer than the maximum chars limit are truncated at maximum chars limit.

Table 7: Wholesale-Retail: L2TP Tunneled Access Mode (description) (Continued)

Attribute ID	Attribute Name	Description
81	Tunnel-Private-Group-ID	The group ID for a particular tunnelled session. This RADIUS attribute is copied by a 7750 LAC in AVP 37 - Private Group ID (ICCN) and is used by the LAC to indicate that this call is to be associated with a particular customer group. The 7750 LNS ignores AVP 37 when received from LAC. The value with tag 0 is used as default for the tunnels where the value is not specified. String lengths above the maximum value are treated as setup failures.
82	Tunnel-Assignment-ID	Indicates to the tunnel initiator the particular tunnel to which a session is to be assigned. Some tunnelling protocols, such as PPTP and L2TP, allow for sessions between the same two tunnel endpoints to be multiplexed over the same tunnel and also for a given session to utilize its own dedicated tunnel. Tag-0 Tunnel-Assignment-ID:0 string, has a special meaning and the string becomes the Tunnel-group name that can hold up to maximum 31 tunnels with the name Tunnel-Assignment-ID-[1..31] string. A Tunnel-group with the name default_radius_group is created on the LAC when this attribute with tag-0 is omitted. This attribute is not the same as attribute 26-4874-64 ERX-Tunnel-Group or 26-6527-46 Alc-Tunnel-Group since these attributes both refer to a tunnel-group name created in CLI context. When not specified, the default value for Tunnel-Assignment-ID-[1..31] string is unnamed. String lengths above the limits are treated as a setup failure.
83	Tunnel-Preference	Indicates the relative preference assigned to each tunnel if more than one set of tunnelling attributes is returned by the RADIUS server to the tunnel initiator. 0x0 (zero) being the lowest and 0x0FFFFFF(16777215) being the highest numerical value. The tunnel having the numerically lowest value in the Value field of this Attribute is given the highest preference. Other tunnel selection criteria are used if preference values from different tunnels are equal. Preference 50 is used when attribute is omitted. Values above the Limits wrap around by Freeradius before send to the NAS (start again from zero until the Limits).
90	Tunnel-Client-Auth-ID	Used during the authentication phase of tunnel establishment and copied by the LAC in L2TP SCCRQ AVP 7 Host Name. Reported in L2TP Tunnel/Link accounting when length is different from zero. The value with tag 0 is used as default for the tunnels where the value is not specified. Pre-configured values are used when the attribute is omitted (**configure router/service vprn** <*service-id*> **l2tp local-name**). The Node system-name is copied in AVP Host Name if this attribute is omitted and no local-name is configured.

Table 7: Wholesale-Retail: L2TP Tunneled Access Mode (description) (Continued)

Attribute ID	Attribute Name	Description
91	Tunnel-Server-Auth-ID	Used during the authentication phase of tunnel establishment and reported in L2TP Tunnel/Link accounting when length is different from zero. For authentication the value of this attribute is compared with the value of AVP 7 Host Name from the received LNS SCCRP. Authentication from LAC point of view passes if both attributes are the same. This authentication check is not performed if the RADIUS attribute is omitted.
26-2352-21	Tunnel-Max-sessions	The maximum number of sessions allowed per Tunnel-Group (untagged attribute only). This attribute has the same function as attribute 26-6527-48 Alc-Tunnel-Max-Sessions:0. No sessions are setup above the Limits. Pre-configured values (**configure router/ service vprn** <*service-id*> **l2tp session-limit**) are used when attribute is omitted.
26-4874-33	ERX-Tunnel-Maximum-Sessions	The maximum number of sessions allowed per Tunnel-Group (untagged attribute only).This attribute has the same meaning as attribute 26-6527-48 Alc-Tunnel-Max-Sessions:0. No sessions are setup above the Limits. Pre-configured values (**configure router/ service vprn** <*service-id*> **l2tp session-limit**) are used when attribute is omitted.
26-4874-64	ERX-Tunnel-Group	The name of the tunnel group that refers to the CLI created tunnel-group-name context.(**configure router** <*router-name*> **l2tp group** <*tunnel-group-name*>. Any other RADIUS returned L2TP parameter is ignored and other required info to setup the tunnel will have to come from the CLI created context. Strings above the Limits are treated as a setup failure.
26-6527-46	Alc-Tunnel-Group	The tunnel-group-name that refers to the CLI created tunnel-group-name context.(**configure router** <*router-name*> **l2tp group** <*tunnel-group-name*>. Any other RADIUS returned L2TP parameter is ignored and other required info to setup the tunnel will have to come from the CLI created context. Strings above the Limits are treated as a setup failure.

Table 7: Wholesale-Retail: L2TP Tunneled Access Mode (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-47	Alc-Tunnel-Algorithm	Describes how new sessions are assigned (weighted-access or existing-first) to one of the set of suitable tunnels that are available or could be made available. A pre-configured algorithm (**configure router/service vprn** <*service-id*> **l2tp session-assign-method**) is used when this attribute is omitted. The value existing-first specifies that the first suitable tunnel is used or set up for the first session and re-used for all subsequent sessions. The value weighted-access specifies that the sessions are shared between the available tunnels; if necessary, new tunnels are set up until the maximum number is reached; the distribution aims at an equal ratio of the actual number of sessions to the maximum number of sessions. The maximum number of sessions per tunnel is retrieved via attribute 26-6527-48 Alc-Tunnel-Max-Sessions or set to a pre-configured value if Alc-Tunnel-Max-Sessions is omitted. Values outside the Limits are treated as a setup failure.
26-6527-48	Alc-Tunnel-Max-Sessions	The maximum number of sessions allowed per Tunnel (if tag is 1..31) or per Tunnel-Group (if tag is 0).This attribute has the same meaning as attribute 26-2352-21 Tunnel-Max-sessions and 26-4874-33 ERX-Tunnel-Maximum-Sessions with the only difference that these latter attributes refers to the Tunnel-Group only (untagged attributed). No sessions are setup above the Limits. Pre-configured values (**configure router/service vprn** <*service-id*> **l2tp session-limit**) are used when attribute is omitted.
26-6527-49	Alc-Tunnel-Idle-Timeout	The period of time in seconds, that an established tunnel with no active sessions (Established-Idle) persists before being disconnected. The value with tag 0 is used as default for the tunnels where the value is not specified. Pre-configured values are used when attribute is omitted (**configure router/service vprn** <*service-id*> **l2tp idle-timeout**). The tunnel is not disconnected (infinite) without local configured idle-timeout or if the attribute has value -1 (16777215). Values above Limits are treated as setup failures.
26-6527-50	Alc-Tunnel-Hello-Interval	The time interval in seconds between two consecutive tunnel Hello messages. A value of '-1' specifies that the keepalive function is disabled. The value with tag 0 is used as default for the tunnels where the value is not specified. Pre-configured values are used when attribute is omitted (**configure router/service vprn** <*service-id*> **l2tp hello-interval**). Values outside Limits are treated as a setup failure.

Table 7: Wholesale-Retail: L2TP Tunneled Access Mode (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-51	Alc-Tunnel-Destruct-Timeout	The time in seconds that operational data of a disconnected tunnel will persist on the node before being removed. Availability of the data after tunnel disconnection allows better troubleshooting. The value with tag 0 is used as default for the tunnels where the value is not specified. Pre-configured values are used when attribute is omitted (**configure router/service vprn** <*service-id*> **l2tp destruct-timeout**). Values outside Limits are treated as a setup failure.
26-6527-52	Alc-Tunnel-Max-Retries-Estab	The number of retries allowed for established tunnels before their control connection goes down. An exponential backoff mechanism is used for the retransmission interval: the first retransmission occurs after 1 second, the next after 2 seconds, then 4 seconds up to a maximum interval of 8 seconds (1,2,4,8,8,8,8). The value with tag 0 is used as default for the tunnels where the value is not specified. Pre-configured values are used when attribute is omitted (**configure router/service vprn** <*service-id*> **l2tp max-retries-estab**). Values outside Limits are treated as a setup failure.
26-6527-53	Alc-Tunnel-Max-Retries-Not-Estab	The number of retries allowed for unestablished tunnels before their control connection goes down. An exponential backoff mechanism is used for the retransmission interval: the first retransmission occurs after 1 second, the next after 2 seconds, then 4 seconds up to a maximum interval of 8 seconds (1,2,4,8,8,8,8). The value with tag 0 is used as default for the tunnels where the value is not specified. Pre-configured values are used when attribute is omitted (**configure router/service vprn** <*service-id*> **l2tp max-retries-not-estab**). Values outside Limits are treated as a setup failure.
26-6527-54	Alc-Tunnel-AVP-Hiding	Identifies the hiding of data in the Attribute Value field of an L2TP AVP. The H bit in the header of each L2TP AVP provides a mechanism to indicate to the receiving peer whether the contents of the AVP are hidden or present in cleartext. This feature can be used to hide sensitive control message data such as user passwords or user IDs. All L2TP AVP's will be passed in cleartext if attribute is omitted and corresponds with the value 'nothing'. The value 'sensitive-only' specifies that the H bit is only set for AVP's containing sensitive information. The value 'all' specifies that the H bit is set for all AVP's where it is allowed. The value with tag 0 is used as default for the tunnels where the value is not specified. Pre-configured values are used when attribute is omitted (**configure router/service vprn** <*service-id*> **l2tp avp-hiding**). AVP hiding uses the shared LAC-LNS secret defined in attribute [69] Tunnel-Password or in configuration. If no password is specified, the tunnel setup will fail for values 'sensitive-only' and 'all'. Values outside the Limits are treated as a setup failure.

Table 7: Wholesale-Retail: L2TP Tunneled Access Mode (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-97	Alc-Tunnel-Challenge	Defines if tunnel authentication (challenge-response) is to be used or not. L2TP tunnel-authentication is based on RFC1994 CHAP authentication and requires the shared-secret defined in attribute [69] Tunnel-Password. The value with tag 0 is used as default for the tunnels where the value is not specified. When the attribute is omitted and no [69] Tunnel-Password attribute is specified, a pre-configured value is used (**configure router/service vprn** <*service-id*> **l2tp challenge**). When the attribute is omitted and a [69] Tunnel-Password attribute is specified, then the value '**always**' is used. When the attribute has the value 'always', no [69] Tunnel-Password attribute is specified and no pre-configured value exists for the password, then the tunnel setup fails. Values outside the Limits are treated as a setup failure.
26-6527-100	Alc-Serv-Id	The **ies/vprn** <*service-id*> on LNS node where the PPP sessions are established (**configure service ies/vprn** <*service-id*> **subscriber-interface** <*name*> **group-interface** <*name*>. Pre-configured values are used if attribute is omitted (**configure subscriber-mgmt local-user-db ppp host interface** <*ip-int-name*> **service-id** <*service-id*> or **configure router/service vprn** <*service-id*> **l2tp group ppp default-group-interface** <*ip-int-name*> **service-id** <*service-id*>). Values above the Limits or unreferenced are treated as a setup failure.
26-6527-101	Alc-Interface	Refers to the group interface <*name*> on LNS node only where the PPP sessions are established (**configure service ies/vprn** <*service-id*> **subscriber-interface** <*ip-int-name*> **group-interface** <*ip-int-name*>). Pre-configured values are used if the attribute is omitted (**configure subscriber-mgmt local-user-db** <local-user-db-name> **ppp host interface** <*ip-int-name*> **service-id** <*service-id*> or **configure router/service vprn** <*service-id*> **l2tp group ppp default-group-interface** <*ip-int-name*> **service-id** <*service-id*>). Alc-interface names longer than the maximum allowed value are treated as session setup failures.
26-6527-104	Alc-Tunnel-Serv-Id	The service-id from which the tunnel should be established, enables the tunnel origin to be in a VPRN (VRF). The default value = Base. Values above the Limits or unreferenced are treated as a setup failure.

Table 7: Wholesale-Retail: L2TP Tunneled Access Mode (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-120	Alc-Tunnel-Rx-Window-Size	Initial receive window size being offered to the remote peer. This attribute is copied in AVP 10 L2TP Receive Window Size. The remote peer may send the specified number of control messages before it must wait for an acknowledgment. The value with tag 0 is used as default for the tunnels where the value is not specified. A pre-configured value is used when attribute is omitted (**configure router/service vprn** <*service-id*> **l2tp receive-window-size**). Values outside the allowed Limits are treated as a setup failure.
26-6527-144	Alc-Tunnel-Acct-Policy	Refers to a pre-configured L2TP tunnel accounting policy-name (**configure aaa l2tp-accounting-policy** <*policy-name*>). L2TP tunnel accounting (RFC 2867) can collect usage data based either on L2TP tunnel and/or L2TP session and send these accounting data to a RADIUS server. Different RADIUS attributes like [66] Tunnel-Client-Endpoint, [67] Tunnel-Server-Endpoint, [68] Acct-Tunnel-Connection, [82] Tunnel-Assignment-ID could be used to identify the tunnel or session. The value with tag 0 is used as default for the tunnels where the value is not specified. Pre-configured values are used when attribute is omitted (**configure router/service vprn** <*service-id*> **l2tp radius-accounting-policy**). Unreferenced policy-names or policy-names longer than the allowed maximum are treated as host setup failures.

Table 8: Wholesale-Retail: L2TP Tunneled Access Mode (limits)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
64	Tunnel-Type	integer	3 (mandatory value)	Mandatory 3=L2TP For example: Tunnel-Type = L2TP
65	Tunnel-Medium-Type	integer	1 (mandatory value)	Mandatory 1=IP or IPv4 For example: Tunnel-Medium-Type = IP
66	Tunnel-Client-Endpoint	string	19 or 20 bytes (untagged/ tagged)	<Tag field><dotted-decimal IP address used on LAC as L2TP src-ip> If Tag field is greater than 0x1F, it is interpreted as the first byte of the following string field For example: # untagged Tunnel-Client-Endpoint = 312e312e312e31 Tunnel-Client-Endpoint = 1.1.1.1 # tagged 0 Tunnel-Client-Endpoint = 00312e312e312e31 Tunnel-Client-Endpoint:0 = 1.1.1.1 # tagged 1 Tunnel-Client-Endpoint = 01312e312e312e31 Tunnel-Client-Endpoint:1 = 1.1.1.1
67	Tunnel-Server-Endpoint	string	19 or 20 bytes (untagged/ tagged)	<Tag field><dotted-decimal IP address used on LAC as L2TP dst-ip> If Tag field is greater than 0x1F, it is interpreted as the first byte of the following string field For example: # tagged 1 Tunnel-Server-Endpoint = 01332e332e332e31 Tunnel-Server-Endpoint:1 = 3.3.3.3
69	Tunnel-Password	string	64 chars	For example: Tunnel-Password:1 = password
81	Tunnel-Private-Group-ID	string	32 chars	For example: Tunnel-Private-Group-ID:1 = MyPrivateTunnelGroup
82	Tunnel-Assignment-ID	string	32 chars	Tag 0x00 tunnel-group Tag 0x01-0x01f individual tunnels within this tunnel-group For example: Tunnel-Assignment-ID:0 += LNS-ALU Tunnel-Assignment-ID:1 += Tunnel-1 Tunnel-Assignment-ID:2 += Tunnel-2

Table 8: Wholesale-Retail: L2TP Tunneled Access Mode (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
83	Tunnel-Preference	integer	16777215	Default preference 50 For example: Tunnel 1 and 2 same preference and first selected Tunnel-Preference:1 += 10 Tunnel-Preference:2 += 10 Tunnel-Preference:3 += 20
90	Tunnel-Client-Auth-ID	string	64 chars.	For example: Tunnel-Client-Auth-Id:0 = LAC-Antwerp-1
91	Tunnel-Server-Auth-ID	string	64 chars.	For example: Tunnel-Server-Auth-ID:0 = LNS-Antwerp-1
26-2352-21	Tunnel-Max-sessions	integer	131071	max sessions per group with default=131071 default=131071 For example: Tunnel-Max-sessions:0 = 1000
26-4874-33	ERX-Tunnel-Maximum-Sessions	integer	131071	max sessions per group with default=131071 For example: ERX-Tunnel-Maximum-Sessions:0 = 1000
26-4874-64	ERX-Tunnel-Group	string	32 chars	node pre-configured tunnel-group For example: ERX-Tunnel-Group:0 = MyCliTunnelGroupName
26-6527-46	Alc-Tunnel-Group	string	32 chars	node pre-configured tunnel-group For example: Alc-Tunnel-Group = MyCliTunnelGroupName
26-6527-47	Alc-Tunnel-Algorithm	integer	[1..2]	1=weighted-access,2=existing-first default=existing-first For example: Alc-Tunnel-Algorithm:0 = weighted-access
26-6527-48	Alc-Tunnel-Max-Sessions	integer	131071	max sessions per group and/or tunnel with default=131071 For example: # 10000 for the group and individual settings per tunnel Alc-Tunnel-Max-Sessions:0 += 10000 Alc-Tunnel-Max-Sessions:1 += 2000 Alc-Tunnel-Max-Sessions:2 += 1000

Table 8: Wholesale-Retail: L2TP Tunneled Access Mode (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-49	Alc-Tunnel-Idle-Timeout	integer	3600 seconds	infinite = -1 or [0..3600] seconds with default= infinite For example: # don't disconnect tunnel1 Alc-Tunnel-Idle-Timeout :1 += 16777215 # disconnect tunnel2 after 1 minute Alc-Tunnel-Idle-Timeout :2 += 60 # disconnect tunnel3 immediately Alc-Tunnel-Idle-Timeout :3 += 0
26-6527-50	Alc-Tunnel-Hello-Interval	integer	[60..3600] seconds	no keepalive = -1 or [60..3600] seconds with default= 300 seconds For example: # tunnel 1 keepalive 120 seconds Alc-Tunnel-Hello-Interval:1 += 120
26-6527-51	Alc-Tunnel-Destruct-Timeout	integer	[60..86400] seconds	[60..86400] seconds with default= 60 seconds For example: # tunnel 1 tunnel destruct timer 120 seconds Alc-Tunnel-Destruct-Timeout:1 += 120
26-6527-52	Alc-Tunnel-Max-Retries-Estab	integer	[2..7]	default 5 For example: # retry 2 times for all tunnels in tunnel group Alc-Tunnel-Max-Retries-Estab:0 = 2
26-6527-53	Alc-Tunnel-Max-Retries-Not-Estab	integer	[2..7]	default 5 For example: # retry 2 times for all tunnels in tunnel group Alc-Tunnel-Max-Retries-Not-Estab:0 = 2
26-6527-54	Alc-Tunnel-AVP-Hiding	integer	[1..3]	1=nothing,2=sensitive-only,3=all; default nothing 1=nothing: All L2TP AVP's in clear text 2=sensitive-only: AVP 11-Challenge, 13-Response,14-Assigned Session ID,21-Called-number,22-Calling-number,26-Initial Received LCP Confreq,27-Last Sent LCP Confreq,28-Last Received LCP Confreq,29-Proxy Authen Type,30-Proxy Authen Name,31-Proxy Authen Challenge,32-Proxy Authen ID,33-Proxy Authen Response 3=all: All AVPs that, according RFC 2661 can be hidden, are hidden. For example: # Best common practices Alc-Tunnel-AVP-Hiding:0 = sensitive-only

Table 8: Wholesale-Retail: L2TP Tunneled Access Mode (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-97	Alc-Tunnel-Challenge	integer	[1..2]	1=never, 2=always; default never For example: Alc-Tunnel-Max-Retries-Estab:0 = always
26-6527-100	Alc-Serv-Id	integer	2147483647 id	For example: Alc-Serv-Id = 100
26-6527-101	Alc-Interface	string	32 chars	For example: Alc-Interface = MyGroupInterface

26-6527-104	Alc-Tunnel-Serv-Id	integer	2147483647 id	default = 'Base' router
				For example: # vprn service 100
				Alc-Tunnel-Serv-Id = 100

26-6527-120	Alc-Tunnel-Rx-Window-Size	integer	[4..1024]	default 64 For example: Alc-Tunnel-Rx-Window-Size = 1000
26-6527-144	Alc-Tunnel-Acct-Policy	string	32 chars	For example: Alc-Tunnel-Acct-Policy = MyL2TPTunnelPolicy

Table 9: Wholesale-Retail: L2TP Tunneled Access Mode (applicability)

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request	Encrypted	Tag	Max. Tag
64	Tunnel-Type	0-1	1	0	N	Y	31
65	Tunnel-Medium-Type	0-1	1	0	N	Y	31
66	Tunnel-Client-Endpoint	0-1	0-1	0	N	Y	31
67	Tunnel-Server-Endpoint	0-1	1	0	N	Y	31
69	Tunnel-Password	0	0-1	0	Y	Y	31
81	Tunnel-Private-Group-ID	0-1	0-1	0	N	Y	31
82	Tunnel-Assignment-ID	0	0-1	0	N	Y	31
83	Tunnel-Preference	0	0-1	0	N	Y	31
90	Tunnel-Client-Auth-ID	0-1	0-1	0	N	Y	31
91	Tunnel-Server-Auth-ID	0-1	0-1	0	N	Y	31
26-2352-21	Tunnel-Max-sessions	0	0-1	0	N	N	N/A
26-4874-33	ERX-Tunnel-Maximum-Sessions	0	0-1	0	N	N	N/A
26-4874-64	ERX-Tunnel-Group	0	0-1	0	N	N	N/A
26-6527-46	Alc-Tunnel-Group	0	0-1	0	N	N	N/A
26-6527-47	Alc-Tunnel-Algorithm	0	0-1	0	N	N	N/A
26-6527-48	Alc-Tunnel-Max-Sessions	0	0-1	0	N	Y	31
26-6527-49	Alc-Tunnel-Idle-Timeout	0	0-1	0	N	Y	31
26-6527-50	Alc-Tunnel-Hello-Interval	0	0-1	0	N	Y	31
26-6527-51	Alc-Tunnel-Destruct-Timeout	0	0-1	0	N	Y	31
26-6527-52	Alc-Tunnel-Max-Retries-Estab	0	0-1	0	N	Y	31
26-6527-53	Alc-Tunnel-Max-Retries-Not-Estab	0	0-1	0	N	Y	31
26-6527-54	Alc-Tunnel-AVP-Hiding	0	0-1	0	N	Y	31

Table 9: Wholesale-Retail: L2TP Tunneled Access Mode (applicability) (Continued)

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request	Encrypted	Tag	Max. Tag
26-6527-97	Alc-Tunnel-Challenge	0	0-1	0	N	Y	31
26-6527-100	Alc-Serv-Id	0	0-1	0	N	N	N/A
26-6527-101	Alc-Interface	0	0-1	0	N	N	N/A
26-6527-104	Alc-Tunnel-Serv-Id	0	0-1	0	N	N	N/A
26-6527-120	Alc-Tunnel-Rx-Window-Size	0	0-1	0	N	Y	31
26-6527-144	Alc-Tunnel-Acct-Policy	0	0-1	0	N	Y	31 (untagged)

Business Service Access

Table 10: Business Access (description)

Attribute ID	Attribute Name	Description
22	Framed-Route	Routing information (IPv4 managed route) to be configured on the NAS for a host (dhcp, pppoe, arp) that operates as a router without NAT (so called routed subscriber host). The route included in the Framed-Route attribute is accepted as a managed route only if it's next-hop points to the hosts ip-address or if the next-hop address equals 0.0.0.0 or if the included route is a valid classful network in case the subnet-mask is omitted. If neither is applicable, this specific framed-route attribute is ignored and the host is instantiated without this specific managed route installed. A Framed-Route attribute is also ignored if the SAP does not have anti-spoof configured to nh-mac (the host will be installed as a standalone host without managed route). Number of routes above Limits are silently ignored. Optionally, a metric, tag and/or protocol preference can be specified for the managed route. If the metrics are not specified or specified in a wrong format or specified with out of range values then default values are used for all metrics: metric=0, no tag and preference=0. If an identical managed route is associated with different routed subscriber hosts in the context of the same IES/VPRN service up to <*max-ecmp-routes*> managed routes are installed in the routing table (configured as **ecmp** <*max-ecmp-routes*> in the routing instance). Candidate ECMP Framed-Routes have identical prefix, equal lowest preference and equal lowest metric. “lowest ip next-hop” is the tie breaker if more candidate ECMP Framed-Routes are available than the configured <*max-ecmp-routes*>. Other identical managed routes are shadowed (not installed in the routing table) and an event is logged. An alternative to RADIUS managed routes are managed routes via host dynamic BGP peering. Valid RADIUS learned managed routes can be included in RADIUS accounting messages with following configuration: **configure subscriber-mgmt radius-accounting-policy <***name***> include-radius-attribute framed-route.** Associated managed routes for an instantiated routed subscriber host are included in RADIUS accounting messages independent of the state of the managed route (Installed, Shadowed or HostInactive).

Table 10: Business Access (description) (Continued)

Attribute ID	Attribute Name	Description
99	Framed-IPv6-Route	Routing information (ipv6 managed route) to be configured on the NAS for a v6 wan host (IPoE or PPPoE) that operates as a router. The functionality is comparable with offering multiple PD prefixes for a single host. The route included in the Framed-IPv6-Route attribute is accepted as a managed route only if it's next-hop is a wan-host (DHCPv6 IA-NA or SLAAC) or if the next-hop address equals ::. As a consequence, Framed-IPv6-Routes with explicit configured gateway prefix of a pd-host (DHCPv6 IA-PD) will not be installed. A Framed-Route attribute is also ignored if the SAP does not have anti-spoof configured to nh-mac (the host will be installed as a standalone host without managed route). Number of Routes above Limits are silently ignored. Optionally, a metric, tag and/or protocol preference can be specified for the managed route. If the metrics are not specified or specified in a wrong format or specified with out of range values then default values are used for all metrics: metric=0, no tag and preference=0. If an identical managed route is associated with different routed subscriber hosts in the context of the same IES/VPRN service up to <*max-ecmp-routes*> managed routes are installed in the routing table (configured as **ecmp** <*max-ecmp-routes*> in the routing instance). Candidate ECMP Framed-IPv6-Routes have identical prefix, equal lowest preference and equal lowest metric. “lowest ip next-hop” is the tie breaker if more candidate ECMP Framed-IPv6-Routes are available than the configured <*max-ecmp-routes*>. Other identical managed routes are shadowed (not installed in the routing table) and an event is logged. Valid RADIUS learned managed routes can be included in RADIUS accounting messages with following configuration: **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute framed-ipv6-route**. Associated managed routes for an instantiated routed subscriber host are included in RADIUS accounting messages independent of the state of the managed route (Installed, Shadowed or HostInactive).
26-6527-55	Alc-BGP-Policy	Refers to the pre-configured policy under **configure subscriber-mgmt bgp-peering-policy** <*policy-name*>. Mandatory attribute if dynamic bgp peering is used. The referenced policy can hold all parameters to setup the dynamic BGP session or policy parameters Peer-AS, MD5 key, Authentication-Keychain and import/export policies can be overruled by optional RADIUS attributes. Dynamic BGP peering related attributes are ignored if session does not terminate in a VPRN. Host setup is successful, but without BGP peering if an unreferenced policy-name is received or if anti-spoof is different from nh-mac. Policy-names above the maximum length are treated as setup failures.
26-6527-56	Alc-BGP-Auth-Keychain	References to the keychain parameters (**configure system security keychain**) used to sign and/or authenticate the BGP protocol stream via the TCP enhanced authentication option (draft-bonica-tcp-auth). Session setup is successful (without BGP peering) if an unreferenced auth-keychain is received. Received keychain names above the maximum length are treated as setup failures. Alternative for [26-6527-57] Alc-BGP-Auth-Key.

Table 10: Business Access (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-57	Alc-BGP-Auth-Key	Indicates the authentication key used between BGP peers before establishing sessions. Authentication is done using the MD5 message based digest protocol. Authentication keys are truncated at 247 Bytes and are not encrypted.
26-6527-58	Alc-BGP-Export-Policy	Refers to the pre-configured BGP export policy (**configure router policy-options policy-statement** <*name*>). RADIUS Policy is appended to the peer (if pre-configured policies for peer are smaller than 5) or replaces the fifth policy (if pre-configured policies for peer are exact 5). Session setup is successful (without export policy applied) if an unreferenced policy-name is received. Policy-names above the maximum length are treated as setup failures.
26-6527-59	Alc-BGP-Import-Policy	Refers to the pre-configured BGP import policy (**configure router policy-options policy-statement** <*name*>). RADIUS Policy is appended to the peer (if pre-configured policies for peer are smaller than 5) or replaces the fifth policy (if pre-configured policies for peer are exact 5). Session setup is successful (without import policy applied) if an unreferenced policy-name is received. Policy-names above the maximum length are treated as setup failures.
26-6527-60	Alc-BGP-PeerAS	indicates the Autonomous System number for the remote peer

Table 11: Business Access (limits)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
22	Framed-Route	string	max. 16 Framed-Route attributes	"<ip-prefix>[/<prefix-length>] <space> <gateway-address> [<space> <metric>] [<space> tag <space> <tag-value>] [<space> pref <space> <preference-value>]” where: <space> is a white space or blank character <ip-prefix>[/prefix-length] is the managed route to be associated with the routed subscriber host. The prefix-length is optional and if not specified, a class-full class A,B or C subnet is assumed. <gateway-address> must be the routed subscriber host IP address. “0.0.0.0” is automatically interpreted as the host IPv4 address. [<metric>] (Optional) Installed in the routing table as the metric of the managed route. If not specified, metric zero is used. Value = [0.. 65535] [tag <tag-value>] (Optional) The managed route will be tagged for use in routing policies. If not specified or tag-value=0, then the route is not tagged. Value = [0..4294967295] [pref <preference-value>] (Optional) Installed in the routing table as protocol preference for this managed route. If not specified, preference zero is used. Value = [0..255] For example: Framed-Route = "192.168.1.0/24 0.0.0.0" where 0.0.0.0 is replaced by host address. Default metrics are used (metric=0, preference=0 and no tag) Framed-Route = "192.168.1.0 0.0.0.0" where 192.168.1.0 is a class-C network /24 and 0.0.0.0 is replaced host address. Default metrics are used. Framed-Route = "192.168.1.0/24 192.168.1.1" where 192.168.1.1 is the host address. Default metrics are used. Framed-Route = "192.168.1.0 0.0.0.0 10 tag 3 pref 100" installs a managed route with metric=10, protocol preference = 100 and tagged with tag=3 Framed-Route = "192.168.1.0 0.0.0.0 tag 5" installs a managed route with metric=0 (default), protocol preference = 0 (default) and tagged with tag=5"

Table 11: Business Access (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
99	Framed-IPv6-Route	string	max. 16 Framed-IPv6-Route attributes	<ip-prefix>/<prefix-length> <space> <gateway-address> [<space> <metric>] [<space> tag <space> <tag-value>] [<space> pref <space> <preference-value>]” where: <space> is a white space or blank character <ip-prefix>/<prefix-length> is the managed route to be associated with the routed subscriber host. <gateway-address> must be the routed subscriber host IP address. “::” and “0:0:0:0:0:0:0:0” are automatically interpreted as the wan-host IPv6 address. [<metric>] (Optional) Installed in the routing table as the metric of the managed route. If not specified, metric zero is used. Value = [0.. 65535] [tag <tag-value>] (Optional) The managed route will be tagged for use in routing policies. If not specified or tag-value=0, then the route is not tagged. Value = [0..4294967295] [pref <preference-value>] (Optional) Installed in the routing table as protocol preference for this managed route. If not specified, preference zero is used. Value = [0..255] For example: Framed-IPv6-Route = "5000:0:1::/48 ::" where :: resolves in the wan-host. Default metrics are used (metric=0, preference=0 and no tag) Framed-IPv6-Route = "5000:0:2::/48 0:0:0:0:0:0:0:0" where 0:0:0:0:0:0:0:0 resolves in the wan-host. Default metrics are used. Framed-IPv6-Route = "5000:0:3::/48 0::0" where 0::0 resolves in the wan-host. Default metrics are used. Framed-IPv6-Route = "5000:0:3::/48 2021:1::1" where 2021:1::1 is the wan-host. Default metrics are used. Framed-IPv6-Route = "5000:0:1::/48 :: 10 tag 3 pref 100" installs a managed route with metric = 10, protocol preference = 100 and tagged with tag = 3 Framed-IPv6-Route = "5000:0:1::/48 :: tag 5" installs a managed route with metric = 0 (default), protocol preference = 0 (default) and tagged with tag = 5
26-6527-55	Alc-BGP-Policy	string	32 chars	For example: Alc-BGP-Policy = MyBGPPolicy

Table 11: Business Access (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-56	Alc-BGP-Auth-Keychain	string	32 chars	For example: Alc-BGP-Auth-Keychain = MyKeychainPolicy
26-6527-57	Alc-BGP-Auth-Key	octets	247 Bytes	For example: Alc-BGP-Auth-Key = "SecuredBGP"
26-6527-58	Alc-BGP-Export-Policy	string	32 chars	For example: Alc-BGP-Export-Policy = to_dynamic_bgp_peer
26-6527-59	Alc-BGP-Import-Policy	string	32 chars	For example: Alc-BGP-Import-Policy = from_dynamic_bgp_peer
26-6527-60	Alc-BGP-PeerAS	integer	[1..4294967294]	For example: Alc-BGP-PeerAS = 65001

Table 12: Business Access (applicability)

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request
22	Framed-Route	0	0+	0
99	Framed-IPv6-Route	0	0+	0
26-6527-55	Alc-BGP-Policy	0	0-1	0
26-6527-56	Alc-BGP-Auth-Keychain	0	0-1	0
26-6527-57	Alc-BGP-Auth-Key	0	0-1	0
26-6527-58	Alc-BGP-Export-Policy	0	0-1	0
26-6527-59	Alc-BGP-Import-Policy	0	0-1	0
26-6527-60	Alc-BGP-PeerAS	0	0-1	0

Accounting On-Line Charging

Table 13: Accounting: On-Line Charging (description)

Attribute ID	Attribute Name	Description
26-6527-95	Alc-Credit-Control-CategoryMap	Refers to a pre-configured category-map (**configure subscriber-mgmt category-map** <*category-map-name*>) that holds the credit-type (volume or time) and information for maximum three pre-defined categories (for example: category-names data in and out, video+data, etc.), their mappings to individual forwarding queues/policers, out-of-credit-actions and alike. The category-map-name can also be assigned via the ludb, or credit-control-policy if the attribute is omitted. This attribute is ignored if the host has no credit-control-policy defined in its sla-profile instance. Strings with length above the Limits are treated as a setup failure.
26-6527-96	Alc-Credit-Control-Quota	Defines a volume and time quota per category in a pre-defined format. Either volume OR time monitoring is supported and the operational credit-type (volume or time) is taken from the category map if both volume and time-quota in this attribute are non-zero. The operational credit-type becomes time if the volume-quota is zero and volume if the time-quota is zero. The Credit Expired becomes true and the corresponding Out Of Credit Action is triggered if both time and volume-quota are zero in the initial Authentication-Accept or CoA. Value zero for both time and volume-quota in additional Authentication Accepts (triggered by credit refresh or re-authentication) are interpreted as no extra credit granted and does not influence the current available credit, were non-zero values reset the current available credit. For CoA requests both Alc-Credit-Control-CategoryMap and Alc-Credit-Control-Quota attributes needs to be included. For RADIUS-Access Accepts this is not mandatory and either both or one of the two attributes can come from pre-defined values from the node. Volume quota values outside the defined limits are treated as an error condition. Time quota values above the defined limits are accepted and capped at maximum value. If more attributes are present than allowed by the limits, it is treated as a setup failure.

Table 14: Accounting: On-line Charging (limits)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-95	Alc-Credit-Control-CategoryMap	string	32 chars	For example: Alc-Credit-Control-CategoryMap = MyCatMap
26-6527-96	Alc-Credit-Control-Quota	string	(2^64 - 1) volume value (2^32 - 1) time value 3 attributes	volume-value volume-units|time-value time-units|category-name <volume-value>: converted in bytes and stored in 64 bit counter - value '0' = no volume credit - value between 100 Megabyte minimum and maximum (2^64 - 1 / 18446744073709551615) Bytes <volume-time>: converted in seconds and stored in 32 bit counter - value '0' = no time credit - value between 15 minutes minimum and (2^32 - 1 / 4294967295) seconds <volume-units>: - in byte (B or units omitted), kilobyte (K or KB), megabyte (M or MB), gigabyte (G or GB) - a combination (10GB200MB20KB|) of different volume units is not allowed. <time-units>: - in seconds (s or units omitted), in minutes (m), in hours (h), in days (d) - a combination (with some restrictions) of different time units is allowed. (15m30s allowed but 15m60s is not allowed) For example: # For category cat1 offer a volume of 500 Mbyte and a time volume of 1day, 2hours, 3minutes, 4seconds Alc-Credit-Control-Quota += 500MB|1d2h3m4s|cat1

Table 15: Accounting: On-Line Charging (applicability)

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request
26-6527-95	Alc-Credit-Control-CategoryMap	0	0-1	0-1
26-6527-96	Alc-Credit-Control-Quota	0-1	0-1	0-1

IP and IPv6 Filters

Table 16: IP and IPv6 filters (description)

Attribute ID	Attribute Name	Description
92	NAS-Filter-Rule	Subscriber host specific filter entry. The match criteria are automatically extended with the subscriber host ip- or ipv6-address as source (ingress) or destination (egress) ip. They represent a per host customization of a generic filter policy: only traffic to/from the subscriber host will match against these entries. A range of entries must be reserved for subscriber host specific entries in a filter policy: **config>filter>ip-filter# sub-insert-radius** Subscriber host specific filter entries are moved if the subscriber host filter policy is changed (new SLA profile or ip filter policy override) and if the new filter policy contains enough free reserved entries. When the subscriber host session terminates or is disconnected, then the corresponding subscriber host specific filter entries are also deleted. The function of the attribute is identical to [26-6527-159] Alc-Ascend-Data-Filter-Host-Spec but it has a different format. The format used to specify host specific filter entries (NAS-Filter-Rule format or Alc-Ascend-Data-Filter-Host-Spec format) cannot change during the lifetime of the subscriber host. Mixing formats in a single RADIUS message results in a failure.
242	Ascend-Data-Filter	A local configured filter policy can be extended with shared dynamic filter entries. A dynamic copy of the base filter (filter associated to the host via sla-profile or host filter override) is made and extended with the set of filter rules per type (ipv4/ipv6) and direction (ingress/egress) in the RADIUS message. If a dynamic copy with the same set of rules already exists, no new copy is made but the existing copy is associated with the host/session. If after host/session disconnection, no hosts/sessions are associated with the dynamic filter copy, then the dynamic copy is removed. Shared filter entries are moved if the subscriber host filter policy is changed (new SLA profile or ip filter policy override) and if the new filter policy contains enough free reserved entries. A range of entries must be reserved for shared entries in a filter policy: **configure filter ip-filter** <*filter-id*> **sub-insert-shared-radius** The function of the attribute is identical to [26-6527-158] Alc-Nas-Filter-Rule-Shared but it has a different format. The format used to specify shared filter entries (Alc-Nas-Filter-Rule-Shared format or Ascend-Data-Filter format) cannot change during the lifetime of the subscriber host. Mixing formats in a single RADIUS message results in a failure. Important note: Shared filter entries should only be used if many hosts share the same set of filter rules that need to be controlled from RADIUS.

Table 16: IP and IPv6 filters (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-134	Alc-Subscriber-Filter	Subscriber host preconfigured ip/ipv6 ingress and egress filters to be used instead of the filters defined in the sla-profile. Not relevant fields will be ignored (for example, IPv4 filters for an IPv6 host). Note that the scope of the local preconfigured filter should be set to template for correct operation. This is not enforced. For a RADIUS CoA message, if the ingress or egress field is missing in the VSA, there will be no change for that direction. For a RADIUS Access-Accept message, if the ingress or egress field is missing in the VSA, then the IP-filters as specified in the sla-profile will be active for that direction Applicable to all dynamic host types, including L2TP LNS but excluding L2TP LAC.
26-6527-158	Alc-Nas-Filter-Rule-Shared	A local configured filter policy can be extended with shared dynamic filter entries. A dynamic copy of the base filter (filter associated to the host via sla-profile or host filter override) is made and extended with the set of filter rules per type (ipv4/ipv6) and direction (ingress/egress) in the RADIUS message. If a dynamic copy with the same set of rules already exists, no new copy is made but the existing copy is associated with the host/session. If after host/session disconnection, no hosts/sessions are associated with the dynamic filter copy, then the dynamic copy is removed. Shared filter entries are moved if the subscriber host filter policy is changed (new SLA profile or ip filter policy override) and if the new filter policy contains enough free reserved entries. A range of entries must be reserved for shared entries in a filter policy: **config filter ip-filter** <*filter-id*> **sub-insert-shared-radius** The function of the attribute is identical to [242] Ascend-Data-Filter but it has a different format. The format used to specify shared filter entries (Alc-Nas-Filter-Rule-Shared format or Ascend-Data-Filter format) cannot change during the lifetime of the subscriber host. Mixing formats in a single RADIUS message results in a failure. Important note: shared filter entries should only be used if many hosts share the same set of filter rules that need to be controlled from RADIUS.
26-6527-159	Alc-Ascend-Data-Filter-Host-Spec	Subscriber host specific filter entry. The match criteria is automatically extended with the subscriber host ip- or ipv6-address as source (ingress) or destination (egress) ip. They represent a per host customization of a generic filter policy: only traffic to/from the subscriber host will match against these entries. A range of entries must be reserved for subscriber host specific entries in a filter policy: **config>filter>ip-filter# sub-insert-radius**. Subscriber host specific filter entries are moved if the subscriber host filter policy is changed (new SLA profile or ip filter policy override) and if the new filter policy contains enough free reserved entries. When the subscriber host session terminates or is disconnected, then the corresponding subscriber host specific filter entries are also deleted. The function of the attribute is identical to [92] Nas-Filter-Rule but it has a different format. The format used to specify host-specific filter entries (NAS-Filer-Rule format or Alc-Ascend-Data-Filter-Host-Spec format) cannot change during the lifetime of the subscriber host. Mixing formats in a single RADIUS message results in a failure.

Table 17: IP and IPv6 Filters (limits)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
92	NAS-Filter-Rule	string	max. 10 attributes per message or max. 10 filter entries per message	The format of a NAS-Filter-Rule is defined in RFC 3588, *Diameter Base Protocol*, section-4.3, *Derived AVP Data Formats*. A single filter rule is a string of format <action> <direction> <protocol> from <source> to <destination> <options> Multiple rules should be separated by a NUL (0x00). A NAS-Filter-Rule attribute may contain a partial rule, one rule, or more than one rule. Filter rules may be continued across attribute boundaries. A RADIUS message with NAS-Filter-Rule attribute value equal to 0x00 or " " (a space) removes all host specific filter entries for that host. See also IP Filter Attribute Details on page 78 For example: Nas-Filter-Rule = permit in ip from any to 10.1.1.1/32
242	Ascend-Data-Filter	Octets	multiple attributes per RADIUS message allowed. min. length 22 bytes (IPv4), 46 bytes (IPv6) max. length: 110 bytes (IPv4), 140 bytes (IPv6)	A string of octets with fixed field length (type (ipv4/ipv6), direction (ingress/egress), src-ip, dst-ip, ...). Each attribute represents a single filter entry. See IP Filter Attribute Details on page 78 for a description of the format. For example:# permit in ip from any to 10.1.1.1/32 Ascend-Data-Filter = 0x01010100000000000a0101010020 0000000000000000

Table 17: IP and IPv6 Filters (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-134	Alc-Subscriber-Filter	string	Max. 1 VSA.	Comma separated list of strings: Ingr-v4:<number>, Ingr-v6:<number>,Egr-v4:<number>,Egr-v6:<number> where <number> can be one of: [1..65535] = ignore sla-profile filter; apply this filter-id 0 = ignore sla-profile filter; do not assign a new filter (only allowed if no dynamic subscriber host specific rules are present) -1 = No change in filter configuration -2 = Restore sla-profile filter For example:Alc-Subscriber-Filter = Ingr-v4:20,Egr-v4:101
26-6527-158	Alc-Nas-Filter-Rule-Shared	string	Multiple attributes per RADIUS message allowed.	The format is identical to [92] NAS-Filter-Rule and is defined in RFC 3588 section-4.3. A single filter rule is a string of format <action> <direction> <protocol> from <source> to <destination> <options> Multiple rules should be separated by a NUL (0x00). An Alc-Nas-Filter-Rule-Shared attribute may contain a partial rule, one rule, or more than one rule. Filter rules may be continued across attribute boundaries. A RADIUS message with Alc-Nas-Filter-Rule-Shared attribute value equal to 0x00 or “ “ (a space) removes the shared filter entries for that host. See also IP Filter Attribute Details on page 78 For example:Alc-Nas-Filter-Rule-Shared = permit in ip from any to 10.1.1.1/32

Table 17: IP and IPv6 Filters (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-159	Alc-Ascend-Data-Filter-Host-Spec	octets	max. 10 attributes per message or max. 10 filter entries per message. min. length 22 bytes (IPv4), 46 bytes (IPv6) max. length: 110 bytes (IPv4), 140 bytes (IPv6)	A string of octets with fixed field length (type (ipv4/ipv6), direction (ingress/egress), src-ip, dst-ip,...). Each attribute represents a single filter entry. See IP Filter Attribute Details on page 78 for a description of the format. For example:# permit in ip from any to 10.1.1.1/32 Alc-Ascend-Data-Filter-Host-Spec = 0x01010100000000000a0101010020 0000000000000000

Table 18: IP and IPv6 Filters (applicability)

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request
92	NAS-Filter-Rule	0	0+	0+
242	Ascend-Data-Filter	0	0+	0+
26-6527-134	Alc-Subscriber-Filter	0	0-1	0-1
26-6527-158	Alc-Nas-Filter-Rule-Shared	0	0+	0+
26-6527-159	Alc-Ascend-Data-Filter-Host-Spec	0	0+	0+

IP Filter Attribute Details

[92] Nas-Filter-Rule and [26-6527-158] Alc-Nas-Filter-Rule-Shared

The format for [92] Nas-Filter-Rule and [26-6527-158] Alc-Nas-Filter-Rule-Shared is a string formatted as: <action> <direction> <protocol> from <source> to <destination> <options>. Table 19 displays details on the respective fields.

Table 19: [92] Nas-Filter-Rule Attribute Format

Action or Classifier	Value		Corresponding SR-OS Filter Function
<action>	deny		action drop
	permit		action forward
<direction>	in		ingress
	out		egress
<protocol>	ip		protocol none
	any number [0..255]		protocol [0..255]
	ip		next-header none
	any number [1..42]		next-header [1..42]
	any number [45..49]		next-header [45..49]
	any number [52..59]		next-header [52..59]
	any number [61..255]		next-header [61..255]
	any number 43|44|50|51|60		not supported
from <source>	any	100	ingress: src-ip = host-ip-address; src-port eq 100 egress: src-ip = 0.0.0.0/0 | ::/0; src-port eq 100
		200-65535	ingress: src-ip = host-ip-address; src-port range 200 65535 egress: src-ip = 0.0.0.0/0 | ::/0; src-port range 200 65535
	ip-prefix/length	100	ingress: src-ip = host-ip-address; src-port eq 100 egress: src-ip = ip-prefix/length; src-port eq 100
		200-65535	ingress: src-ip = host-ip-address; src-port range 200 65535 egress: src-ip = ip-prefix/length; src-port range 200 65535

Table 19: [92] Nas-Filter-Rule Attribute Format (Continued)

Action or Classifier	Value		Corresponding SR-OS Filter Function
to <destination>	any	100	ingress: dst-ip = 0.0.0.0/0 | ::/0; dst-port eq 100 egress: dst-ip = host-ip-address; dst-port eq 100
		200-65535	ingress: dst-ip = 0.0.0.0/0 | ::/0; dst-port range 200 65535 egress: dst-ip = host-ip-address; dst-port range 200 65535
	ip-prefix/length	100	ingress: dst-ip = ip-prefix/length; dst-port eq 100 egress: dst-ip = host-ip-address; dst-port eq 100
		200-65535	ingress: dst-ip = ip-prefix/length; dst-port range 200 65535 egress: dst-ip = host-ip-address; dst-port range 200 65535
<options: frag>	frag		fragment true (ipv4 only)
<options: ipoptions>	ssrr		ip-option 9 / ip-mask 255
	lsrr		ip-option 3/ ip-mask 255
	rr		ip-option 7/ ip-mask 255
	ts		ip-option 4/ ip-mask 255
	!ssrr		not supported
	!lsrr		not supported
	!rr		not supported
	!ts		not supported
	ssrr,lsrr,rr,ts		not supported
<options: tcpoptions>	mss		not supported
	window		not supported
	sack		not supported
	ts		not supported
	!mss		not supported
	!window		not supported
	!sack		not supported
	!ts		not supported
	mss,window,sack,ts		not supported

Table 19: [92] Nas-Filter-Rule Attribute Format (Continued)

Action or Classifier	Value	Corresponding SR-OS Filter Function
<options: established>	established	not supported
		not supported
		not supported
<options: setup>	setup	tcp-syn true
		tcp-ack false
		protocol tcp
<options: tcpflags>	syn	tcp-syn true
	!syn	tcp-syn false
	ack	tcp-ack true
	!ack	tcp-ack false
	fin	not supported
	rst	not supported
	psh	not supported
	urg	not supported

Table 19: [92] Nas-Filter-Rule Attribute Format (Continued)

Action or Classifier	Value	Corresponding SR-OS Filter Function
<options: icmptypesv4>	echo reply	protocol 1 / icmp-type 0
	destination unreachable	protocol 1 / icmp-type 3
	source quench	protocol 1 / icmp-type 4
	redirect	protocol 1 / icmp-type 5
	echo request	protocol 1 / icmp-type 8
	router advertisement	protocol 1 / icmp-type 9
	router solicitation	protocol 1 / icmp-type 10
	time-to-live exceeded	protocol 1 / icmp-type 11
	IP header bad	protocol 1 / icmp-type 12
	timestamp request	protocol 1 / icmp-type 13
	timestamp reply	protocol 1 / icmp-type 14
	information request	protocol 1 / icmp-type 15
	information reply	protocol 1 / icmp-type 16
	address mask request	protocol 1 / icmp-type 17
	address mask reply	protocol 1 / icmp-type 18
	-	protocol 1 / icmp-type [0..255]
	3-9 (range)	not supported
	3,5,8,9 (comma separated)	not supported
<options: icmptypesv6>	destination unreachable	icmp-type 1
	time-to-live exceeded	icmp-type 3
	IP header bad	icmp-type 4
	echo request	icmp-type 128
	echo reply	icmp-type129
	router solicitation	icmp-type 133
	router advertisement	icmp-type 134
	redirect	icmp-type 137

[242] Ascend-Data-Filter and [26-6527-159] Alc-Ascend-Data-Filter-Host-Spec

The format for [242] Ascend-Data-Filter and [26-6527-159] Alc-Ascend-Data-Filter-Host-Spec is an octet string with fixed length fields. Table 20 displays details on the respective fields.

Table 20: [242] Ascend-Data-Filter Attribute Format

Field	Length	Value
Type	1 byte	1 = IPv4
		3 = IPv6
Filter or forward	1 byte	0 = drop
		1 = accept
Indirection	1 byte	0 = egress
		1 = ingress
Spare	1 byte	ignored
Source IP address	IPv4 = 4 bytes	IP address of the source interface
	IPv6 = 16 bytes	
Destination IP address	IPv4 = 4 bytes	IP address of the destination interface
	IPv6 = 16 bytes	
Source IP prefix	1 byte	Number of bits in the network portion
Destination IP prefix	1 byte	Number of bits in the network portion
Protocol	1 byte	Protocol number. Note: match the inner most header only for IPv6
Established	1 byte	ignored (not implemented)
Source port	2 bytes	Port number of the source port
Destination port	2 bytes	Port number of the destination port
Source port qualifier	1 byte	0 = no compare
		1 = less than
		2 = equal to
		3 = greater than
		4 = not equal to (not supported)

Table 20: [242] Ascend-Data-Filter Attribute Format (Continued)

Field	Length	Value
Destination port qualifier	1 byte	0 = no compare
		1 = less than
		2 = equal to
		3 = greater than
		4 = not equal to (not supported)
Reserved	2 bytes	ignored

Subscriber Host Creation

Table 21: Subscriber Host Creation (description)

Attribute ID	Attribute Name	Description
8	Framed-IP-Address	The IPv4 address to be configured for the host via DHCPv4 (radius proxy) or IPCP (PPPoE). Simultaneous returned attributes [88] Framed-Pool and [8] Framed-IP-Address (RADIUS Access-Accept) are handled as host setup failures. Attribute is also used in CoA and Disconnect Message (part of the ESM or AA user identification-key). Attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute no framed-ip-addr**.
87	NAS-Port-Id	A text string which identifies the physical/logical port of the NAS which is authenticating the user and/or reported for accounting. Attribute is also used in CoA and Disconnect Message (part of the user identification-key). The nas-port-id for physical ports usually contains <slot>/<mda>/<port>/<vlan|vpi>.<vlan|vci>. The physical port can have an optional prefix-string(max 8 chars) and suffix-string (max 64 chars) added for Accounting (**configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute nas-port-id** [**prefix-string** <*string*>] [**suffix** <**circuit-id**|**remote-id**>]). For logical access circuits (LNS) the nas-port-id is a fixed concatenation (delimiter #) of routing instance, tunnel-server-endpoint, tunnel-client-endpoint, local-tunnel-id, remote-tunnel-id, local-session-id, remote-session-id and call sequence number.
26-6527-14	Alc-Force-Renew	An individual DHCPv4 session is renewed with a CoA with attribute [26-6527-14] Alc-Force-Renew. The NAS initiates the ForceRenew procedure with re-authentication (triggers dhcp Force Renew to client and start re-authentication on dhcp Request received).
26-6527-15	Alc-Create-Host	Used to create an IPv4 host via CoA. Additional mandatory attributes to create such a host are [8] Framed-IP-Address, [87] NAS-Port-Id and [26-6527-27] Alc-Client-Hardware-Addr
26-6527-27	Alc-Client-Hardware-Addr	MAC address from a user that requests a service and included in CoA, Authentication or Accounting (**configure subscriber-mgmt authentication-policy/radius-accounting-policy include-radius-attribute mac-address**)
26-6527-98	Alc-Force-Nak	An individual DHCPv4 session is terminated with a CoA with attribute [26-6527-98] Alc-Force-Nak. The NAS initiates the ForceRenew procedure which will be blocked (reply on client DHCP Request with DHCP Nak and send DHCP Release to DHCP server).

Table 22: Subscriber Host Creation (limits)

Attribute ID	Attribute Name	Type	Limits	SR-OS format
8	Framed-IP-Address	ipaddr	4 Bytes	For example: # ip-address 10.11.12.13 Framed-IP-Address 0a0b0c0d
87	NAS-Port-Id	string	253 Bytes	<prefix> : optional string 8 chars max <suffix> : optional string remote-id (max 64 chars) | circuit-id (max 64 chars) # NON-ATM and NON-LNS: <prefix><space><slot>/<mda>/<port>/<vlan>.<vlan><space><suffix> # ATM: <prefix><space><slot>/<mda>/<port>/<vpi>.<vci><space><suffix> # LNS: LNS rt-<routing instance>#lip-<tunnel-server-endpoint>#rip-<tunnel-client-endpoint>#ltid-<local-tunnel-id>#rtid-<remote-tunnel-id>#lsid-<local-session-id>#rsid-<remote-session-id>#<call sequence number> For example: NAS-Port-Id = 1/1/4:501.1001 NAS-Port-Id = LNS rtr-2#lip-3.3.3.3#rip-1.1.1.1#ltid-11381#rtid-1285#lsid-30067#rsid-19151#347
26-6527-14	Alc-Force-Renew	string	no limits	The attribute value is ignored For example: Alc-Force-Renew = anything Alc-Force-Renew = 1
26-6527-15	Alc-Create-Host	string	no limits	The attribute value is ignored For example: Alc-Create-Host = anything Alc-Create-Host = 1
26-6527-27	Alc-Client-Hardware-Addr	string	6 Bytes	For example: Alc-Client-Hardware-Addr = 00:00:00:00:00:01
26-6527-98	Alc-Force-Nak	string	no limits	The attribute value is ignored For example: Alc-Force-Nak = anything Alc-Force-Nak = 1

Table 23: Subscriber host creation (applicability)

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request
8	Framed-IP-Address	0	0-1	0-1
87	NAS-Port-Id	0-1	0	0-1
26-6527-14	Alc-Force-Renew	0	0	0-1
26-6527-15	Alc-Create-Host	0	0	0-1
26-6527-27	Alc-Client-Hardware-Addr	0-1	0-1	0
26-6527-98	Alc-Force-Nak	0	0	0-1

Subscriber Services

Table 24: Subscriber Services (description)

Attribute ID	Attribute Name	Description
26-6527-151	Alc-Sub-Serv-Activate	Activate a subscriber service. The attribute typically contains parameters as input for the Python script that populates the subscriber service data structure (sub_svc). The attribute is ignored if not used in Python. The parameters can cross an attribute boundary. The concatenation of all Alc-Sub-Serv-Activate attributes with the same tag in a single message is typically used as a unique subscriber service instance identifier (key). In subscriber service RADIUS accounting messages, the attribute is sent untagged and contains the subscriber service data structure sub_svc.name value used at service activation. Multiple attributes may be present if the total length does not fit a single attribute.
26-6527-152	Alc-Sub-Serv-Deactivate	Deactivate a subscriber service. The attribute typically contains parameters as input for the Python script that populates the subscriber service data structure (sub_svc). The attribute is ignored if not used in Python. The parameters can cross an attribute boundary. The concatenation of all Alc-Sub-Serv-Deactivate attributes with the same tag in a single message is typically used as the unique subscriber service instance identifier (key).
26-6527-153	Alc-Sub-Serv-Acct-Stats-Type	Enable or disable subscriber service accounting and specify the stats type: volume and time or time only. The attribute is used as input for the Python script that populates the subscriber service data structure (sub_svc.acct_stats_type). The attribute is ignored if not used in Python. The subscriber service accounting statistics type cannot be changed for an active subscriber service.
26-6527-154	Alc-Sub-Serv-Acct-Interim-Ivl	The interim accounting interval in seconds at which Acct-Interim-Update messages should be generated for subscriber service accounting. The attribute is used as input for the Python script that populates the subscriber service data structure (sub_svc.acct_interval). The attribute is ignored if not used in Python. sub_svc.acct_interval overrides the local configured update-interval value in the subscriber profile policy. With value = 0, the interim accounting is switched off. The subscriber service accounting interim interval cannot be changed for an active subscriber service.
26-6527-155	Alc-Sub-Serv-Internal	For internal use only

Table 25: Subscriber Services (limits)

Attribute ID	Attribute Name	Type	Limits	SR-OS format
26-6527-151	Alc-Sub-Serv-Activate	string	multiple VSA's per tag per message	For example: Alc-Sub-Serv-Activate:1 = rate-limit;1000;8000
26-6527-152	Alc-Sub-Serv-Deactivate	string	multiple VSA's per tag per message	For example: Alc-Sub-Serv-Deactivate:1 = rate-limit;1000;8000
26-6527-153	Alc-Sub-Serv-Acct-Stats-Type	integer	1 VSA per tag per message	1=off, 2=volume-time, 3=time For example: Alc-Sub-Serv-Acct-Stats-Type:1 = 2
26-6527-154	Alc-Sub-Serv-Acct-Interim-Ivl	integer	1 VSA per tag per message [300.. 15552000]	A value of 0 (zero) corresponds with no interim update messages. A value [1..299] seconds is rounded to 300s (min. CLI value) and a value > 15552000 seconds (max. CLI value) is rounded to the max. CLI value. [300..15552000] = override local configured update-interval for this subscriber service For example: Alc-Sub-Serv-Acct-Interim-Ivl:1 = 3600

Table 26: Subscriber Services (applicability)

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request	Tag	Max. Tag
26-6527-151	Alc-Sub-Serv-Activate	0	0+	0+	Y	0-31 (untagged)
26-6527-152	Alc-Sub-Serv-Deactivate	0	0+	0+	Y	0-31
26-6527-153	Alc-Sub-Serv-Acct-Stats-Type	0	0+	0+	Y	0-31
26-6527-154	Alc-Sub-Serv-Acct-Interim-Ivl	0	0+	0+	Y	0-31

WLAN Gateway

In this section, WLAN gateway application specific attributes are detailed, including generic Enhanced Subscriber Management (ESM) attributes that have different semantics when used in WLAN gateway scenarios.

Table 27: WLAN Gateway (description)

Attribute ID	Attribute Name	Description
4	NAS-IP-Address	The identifying IP Address of the NAS requesting Authentication or Accounting. Authentication generated from ISA (for a UE in migrant state) can be configured to use local IP address of RADIUS client on the ISA or the system IP address (on CPM). **config aaa isa-radius-policy** *name* **nas-ip-address-origin** {**isa-ip** | **system-ip**} When an ESM host exists for the UE (UE is in authenticated state), then the NAS IP in authentication and accounting is the system IP address.
30	Called-Station-Id	If configured for inclusion in authentication and accounting policy, the called-station-id received from EAP authentication request is transparently forwarded in access-request. If it is contained in the accounting messages received from the APs, it is transparently forwarded in the accounting messages sent from the WLAN-GW. For open SSIDs, called-station-id is not included in authentication or accounting. Typically the string contains "<AP MAC> : <SSID-name>".
31	Calling-Station-Id	Calling-station-id contains the MAC address of the UE, if it is configured for inclusion in isa-radius-policy for authentication generated from the ISA (for a UE in migrant state), or in authentication and accounting policy for messages generated from the CPM. For CPM generated authentication or accounting, the inclusion of calling-station-id MUST explicitly specify the format of the calling-station-id as MAC: **configure subscriber-mgmt authentication-policy | radius-accounting-policy** *name* **include-radius-attribute calling-station-id mac**.
87	NAS-Port-Id	A text string which has a fixed format containing tunnel-type (GRE), transport-service, and local and remote tunnel end-point IP address, as shown in the example: GRE rtr-11#lip-50.1.1.1#rip-201.1.1.2
26-3561-1	Agent-Circuit-Id	Agent-circuit-id is transparently taken from the circuit-id in DHCP option-82. Most WIFI access-points insert information describing the AP and SSID that the UE is associated with. Recommended format is an ASCII string containing AP's MAC@, SSID name and SSID type (open or secure), with a delimiter between each, as shown in example: "00:00:00:00:00:01;xfinity-wifi;o"
26-6527-145	Alc-MGW-Interface-Type	This contains the interface type that will be used to determine the type of GTP-C connection, overrides local configuration.

Table 27: WLAN Gateway (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-146	Alc-Wlan-APN-Name	Specifies the Access Point Name (APN) for which a GTP-C session will be set up. This will be signaled in the GTP-C setup and may be used to determine the IP address of the GGSN/P-GW by performing a DNS query if the [26-10415-5] 3GPP-GGSN-Address attribute is not present. This overrides a locally configured APN.
26-6527-147	Alc-MsIsdn	Contains the MSISDN (telephone number) of the UE, and will be included in GTP-C signaling. When not present the corresponding GTP-C Information Element will not be sent.
26-6527-148	Alc-RSSI	Received Signal Strength Indication. Used in conjunction with the radius-proxy track-accounting feature. When the radius-proxy receives this attribute in an accounting message, it will be copied into the DHCP lease state and echoed by the SROS accounting.
26-6527-149	Alc-Num-Attached-Ues	Number of attached WIFI UEs. The attribute is forwarded by the RADIUS proxy when received in an Access-Request from the AP.
26-6527-172	Alc-Wlan-Portal-Redirect	Used when authenticating migrant hosts. When an access-accept contains this attribute, the host will stay in migrant phase, but will have limited forwarding capabilities. All filtered (not allowed) http-traffic will be redirected to a specified portal URL. This attribute must contain the name of a redirect policy configured under **subscriber-mgmt http-redirect-policy** <*policy-name*> which will specify a set of forwarding filters. It is also allowed to just send an empty Alc- Wlan-Portal-Redirect VSA to force a redirect with the configured policy and url.
26-6527-173	Alc-Wlan-Portal-Url	If a migrant host is redirected, specifies the URL it has to be redirected to, takes precedence over the URL configured in the redirect policy under **subscriber-mgmt http-redirect-policy** <*policy-name*>.
26-6527-179	Alc-GTP-Local-Breakout	Specifies if part of the UE traffic is allowed to be locally broken out (i.e., NAT'ed and routed), subject to matching a filter with "gtp-local-breakout" action, associated with the UE.
26-6527-190	Alc-Wlan-Handover-Ip-Address	IP address provided in RADIUS Access-Accept message to signal handover from LTE or UMTS to WIFI. If this VSA is present, handover indication is set in GTP session creation request to PGW/GGSN.
26-25053-2	Ruckus-Sta-RSSI	Received Signal Strength Indication. Used in conjunction with the radius-proxy track-accounting feature. When the radius-proxy receives this attribute in an accounting message, it will be copied into the DHCP lease state and echoed by the SROS accounting.
26-10415-1	3GPP-IMSI	This is used to identify the host in a GTP-C connection. If not present and a gtp-c connection is requested, the subscriber-id or username in the EAP-SIM message will be parsed as an IMSI. This should be provided for any GTP-C user.

Table 27: WLAN Gateway (description) (Continued)

Attribute ID	Attribute Name	Description
26-10415-5	3GPP-GPRS-Negotiated-QoS-Profile	Used to signal the QOS for default bearer or primary PDP context via GTP “QOS IE” in create-PDP-context and "Bearer QOS" in create-session-request
26-10415-7	3GPP-GGSN-Address	For 3G, it represents the GGSN IPv4 address that is used by the GTP control plane for the context establishment on the Gn interface. For 4G, it represents the P-GW IPv4 address that is used on the S2a or S2b interface for the GTP session establishment. If not present, the WLAN-GW will send a DNS query based on the APN name derived from [26-6527-146] Alc-Wlan-APN-Name or local configuration.
26-10415-13	3GPP-Charging-Characteristics	Used to signal charging-characteristic IE content.
26-10415-20	3GPP-IMEISV	International Mobile Equipment Id and its Software Version, this will be echoed in the GTP-C setup messages.

Table 28: WLAN Gateway (limits)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
4	NAS-IP-Address	ipaddr	4 Bytes	For example: NAS-IPAddress = 10.1.1.2
30	Called-Station-Id	string	64 chars.	For example: Called-Station-Id = “0a-0b-0c-00-00-01 : AirportWifi”
31	Calling-Station-Id	string	64 chars.	For example: Calling-station-id = 00:00:00:00:00:01
87	NAS-Port-Id	string	253 chars.	GRE rtr-<routing instance>#lip-<local-tunnel-endpoint>#rip-<remote-tunnel-endpoint> For example: NAS-Port-Id = “GRE rtr-11#lip-50.1.1.1#rip-201.1.1.2”
26-3561-1	Agent-Circuit-Id	string	247 chars.	String containing information about the AP and the SSID that the UE is associated with. Recommended format is <AP-MAC>;<SSID-Name>;<SSID-Type>. SSID-Type can be open (‘o’), or secure (‘s’) For example: Agent-Circuit-Id = “00:00:00:00:00:01;xfinity-wifi;o”
26-6527-145	Alc-MGW-Interface-Type	integer	values 1..3	Gn(GTPv1)=1; S2a(GTPv2)=2; S2b(GTPv2)=3 default = s2a For example: Alc-MGW-Interface-Type = 1
26-6527-146	Alc-Wlan-APN-Name	string	100 chars. if both <NI> and <OI> parts are present. 63 chars. if only the <NI> part is present.	The APN Name attribute must be formatted as <NI>[.mnc<MNC>.mcc<MCC>.gprs]. The Operator-ID (OI) part is optional and is automatically derived from the IMSI if it is not present. The APN FQDN generated for DNS resolution is composed of the Network-ID (<NI>) portion and the Operator-ID (OI) portion (<MCC> and <MNC>) as per 3GPP TS 29.303 and is reformatted as <NI>.apn.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org For example: Alc-Wlan-APN-Name = wlangw.mnc004.mcc204.gprs
26-6527-147	Alc-MsIsdn	string	9..15 digits	For example: Alc-MsIsdn = 13109976224
26-6527-148	Alc-RSSI	integer	32 bit value	For example: Alc-RSSI = 30
26-6527-149	Alc-Num-Attached-Ues	integer	32 bit value	For example: Alc-Num-Attached-Ues = 3

Table 28: WLAN Gateway (limits) (Continued)

Attri-bute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-172	Alc-Wlan-Portal-Redirect	string	32 chars.	For example: Alc-Wlan-Portal-Redirect = Redirect-policy-1
26-6527-173	Alc-Wlan-Portal-Url	string	253 chars.	For example: Alc-Wlan-Portal-Url = http://welcome.portal.com
26-6527-179	Alc-GTP-Local-Breakout	integer	4 bytes	# values: not-allowed = 0, allowed = 1 For example: Alc-GTP-Local-Breakout = allowed
26-6527-190	Alc-Wlan-Handover-Ip-Address	ipaddr	4 Bytes	For example: Alc-Wlan-Handover-Ip-Address = 10.1.1.1
26-25053-2	Ruckus-Sta-RSSI	integer	32 bit value	For example: Ruckus-Sta-RSSI = 28
26-10415-1	3GPP-IMSI	string	1..15 digits	3GPP vendor specific attribute as defined in 3GPP TS 29.061. For example: 3GPP-IMSI = 204047910000598
26-10415-5	3GPP-GPRS-Negotiated-QoS-Profile	string	length as defined in the 3GPP TS 29.061	Specified in TS 29.061 version 8.5.0 Release 8 section 16.4.7.2 For example: 3GPP-GPRS-Negotiated-QoS-Profile = 08-4D020000002710000000138800000001f40000000bb8
26-10415-7	3GPP-GGSN-Address	ipaddr	4 bytes	3GPP vendor specific attribute as defined in TS 29.061. For example: 3GPP-GGSN-Address = 10.43.129.23
26-10415-13	3GPP-Charging-Characteristics	string	4 chars	Specified in TS 29.061 version 8.5.0 Release 8 section 16.4.7.2 For example: 3GPP-Charging-Characteristics = 1A2B
26-10415-20	3GPP-IMEISV	string	14..16 digits	3GPP vendor specific attribute as defined in TS 29.061.

Table 29: WLAN Gateway (applicability)

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request	Acct. Messages
4	NAS-IP-Address	1	0	0	1
30	Called-Station-Id	0-1	0	0-1	0-1
31	Calling-Station-Id	0-1	0	0-1	0-1
87	NAS-Port-Id	0-1	0	0-1	0-1
26-3561-1	Agent-Circuit-Id	0-1	0	0	0-1
26-6527-145	Alc-MGW-Interface-Type	0	0-1	0	0
26-6527-146	Alc-Wlan-APN-Name	0	0-1	0	0
26-6527-147	Alc-MsIsdn	0	0-1	0	0
26-6527-148	Alc-RSSI	0	0	0	0-1
26-6527-149	Alc-Num-Attached-Ues	0-1	0	0	0
26-6527-172	Alc-Wlan-Portal-Redirect	0	0-1	0	0
26-6527-173	Alc-Wlan-Portal-Url	0	0-1	0	0
26-6527-179	Alc-GTP-Local-Breakout	0	0-1	0	0-1
26-6527-190	Alc-Wlan-Handover-Ip-Address	0	0-1	0	0
26-25053-2	Ruckus-Sta-RSSI	0	0	0	0-1
26-10415-1	3GPP-IMSI	0	0-1	0	0
26-10415-5	3GPP-GPRS-Negotiated-QoS-Profile	0	0-1	0	0
26-10415-7	3GPP-GGSN-Address	0	0-1	0	0
26-10415-13	3GPP-Charging-Characteristics	0	0-1	0	0
26-10415-20	3GPP-IMEISV	0	0-1	0	0

Dynamic Data Services

Table 30: Dynamic Data Services (description)

Attribute ID	Attribute Name	Description
26-6527-164	Alc-Dyn-Serv-SAP-Id	Identifies the dynamic data service SAP. Only Ethernet ports and LAGs are valid. The Dynamic Service SAP-ID uniquely identifies a Dynamic Data Service instance. It can be specified explicitly or relative to the control channel SAP-ID using wildcards. If explicitly specified, the Dynamic Data Service SAP-ID and Control Channel SAP-ID do not have to be on the same port. The setup of the Dynamic Data Service fails if the SAP specified in Alc-Dyn-Serv-SAP-Id is not created. The Dynamic Data Service SAP becomes orphaned if the SAP is not deleted with a teardown action.
26-6527-165	Alc-Dyn-Serv-Script-Params	Parameters as input to the Dynamic Data Service Python script. The parameters can cross an attribute boundary. The concatenation of all Alc-Dyn-Serv-Script-Params attributes with the same tag in a single message must be formatted as function-key <dictionary> where function-key specifies which Python functions will be called and <dictionary> contains the actual parameters in a Python dictionary structure format. In dynamic service RADIUS accounting messages, the attribute is sent untagged and contains the last received Alc-Dyn-Serv-Script-Params value in an Access-Accept or CoA message for this dynamic service. Multiple attributes may be present if the total length does not fit a single attribute.
26-6527-166	Alc-Dyn-Serv-Script-Action	The action specifies if a dynamic data service should be created (setup), changed (modify) or deleted (teardown). Together with the <function-key> in the Alc-Dyn-Serv-Script-Params, this attribute determines which Python function will be called.The attribute is mandatory in a CoA message. The attribute is optional in an Access-Accept message. If included in an Access-Accept and the specified action is different from setup, the dynamic data service action fails.
26-6527-167	Alc-Dyn-Serv-Policy	Specifies the local configured Dynamic Data Service Policy to use for provisioning of this dynamic service. If the attribute is not present, the dynamic services policy with the name default is used. If the default policy does not exist, then the dynamic data service action fails.The Alc-Dyn-Serv-Policy attribute is optional in case of modify or teardown actions; the policy specified for the dynamic data service setup is automatically used. If the Alc-Dyn-Serv-Policy is specified for modify or teardown actions, it must point to the same dynamic services policy as used during the dynamic data service setup. If a different policy is specified, the action fails.

Table 30: Dynamic Data Services (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-168	Alc-Dyn-Serv-Acct-Interim-Ivl-1	The number of seconds between each dynamic data service accounting interim update for the primary accounting server. Overrides local configured value in the Dynamic Services policy. With value = 0, the interim accounting to the primary accounting server is switched off.The dynamic data service accounting interim interval cannot be changed for an active service. The attribute is rejected if the script action is different from setup
26-6527-169	Alc-Dyn-Serv-Acct-Interim-Ivl-2	The number of seconds between each dynamic data service accounting interim update for the duplicate accounting server. Overrides local configured value in the Dynamic Services policy. With value = 0, the interim accounting to the duplicate accounting server is switched off.The dynamic data service accounting interim interval cannot be changed for an active service. The attribute is rejected if the script action is different from setup
26-6527-170	Alc-Dyn-Serv-Acct-Stats-Type-1	Enable or disable dynamic data service accounting to the primary accounting server and specify the stats type: volume and time or time only. Overrides the local configured value in the Dynamic Services Policy.The dynamic data service accounting statistics type cannot be changed for an active service. The attribute is rejected if the script action is different from setup
26-6527-171	Alc-Dyn-Serv-Acct-Stats-Type-2	Enable or disable dynamic data service accounting to the secondary accounting server and specify the stats type: volume and time or time only. Overrides the local configured value in the Dynamic Services Policy.The dynamic data service accounting statistics type cannot be changed for an active service. The attribute is rejected if the script action is different from setup

Table 31: Dynamic Data Services (limits)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-164	Alc-Dyn-Serv-SAP-Id	string	1 VSA per tag per message	Any valid Ethernet SAP format (null, dot1q or qinq encaps), including LAGs. A wildcard (#) can be specified for the port field and optionally for one of the tag fields of a qinq encap. To find the dynamic data service SAP-ID, the wildcard fields are replaced with the corresponding field from the Control Channel SAP-ID. For example: Alc-Dyn-Serv-SAP-Id:1 = 1/2/7:10.201 Alc-Dyn-Serv-SAP-Id:2 = #:#.100
26-6527-165	Alc-Dyn-Serv-Script-Params	string	multiple VSA's per tag per message. Max length of concatenated strings per tag = 1000 bytes	The script parameters may be continued across attribute boundaries. The concatenated string must have following format: function-key <dictionary> where function-key specifies which Python functions will be used and <dictionary> contains the actual parameters in a Python dictionary structure format. For example: Alc-Dyn-Serv-Script-Params:1 = data_svc_1 = { 'as_id' : '100', 'comm_id' : '200', 'if_name' : 'itf1', 'ipv4_address': '1.1.1.1', 'egr_ip_filter' : '100' , 'routes' : [{'to' : '200.1.1.0/24', 'next-hop' : '20.1.1.1'}, {'to' : '200.1.2.0/24', 'next-hop' : '20.1.1.1'}]}
26-6527-166	Alc-Dyn-Serv-Script-Action	integer	1 VSA per tag per message	1=setup, 2=modify, 3=teardown For example: Alc-Dyn-Serv-Script-Action:1 = 2
26-6527-167	Alc-Dyn-Serv-Policy	string	1 VSA per tag per message; max. length: 32 chars.	The name of the local configured Dynamic Service Policy For example: Alc-Dyn-Serv-Policy:1 = dynsvc-policy-1

Table 31: Dynamic Data Services (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-168	Alc-Dyn-Serv-Acct-Interim-Ivl-1	integer	1 VSA per tag per message [300.. 15552000]	A value of 0 (zero) corresponds with no interim update messages. A value [1..299] seconds is rounded to 300s (min. CLI value) and a value > 15552000 seconds (max. CLI value) is rounded to the max. CLI value. Range = 0 | [300.. 15552000] For example: Alc-Dyn-Serv-Acct-Interim-Ivl-1:1 = 3600
26-6527-169	Alc-Dyn-Serv-Acct-Interim-Ivl-2	integer	1 VSA per tag per message [300.. 15552000]	A value of 0 (zero) corresponds with no interim update messages. A value [1..299] seconds is rounded to 300s (min. CLI value) and a value > 15552000 seconds (max. CLI value) is rounded to the max. CLI value. Range = 0 | [300.. 15552000] For example: Alc-Dyn-Serv-Acct-Interim-Ivl-2:1 = 86400
26-6527-170	Alc-Dyn-Serv-Acct-Stats-Type-1	integer	1 VSA per tag per message	1=off, 2=volume-time, 3=time For example: Alc-Dyn-Serv-Acct-Stats-Type-1:1 = 1
26-6527-171	Alc-Dyn-Serv-Acct-Stats-Type-2	integer	1 VSA per tag per message	1=off, 2=volume-time, 3=time For example: Alc-Dyn-Serv-Acct-Stats-Type-2:1 = 2

Table 32: Dynamic Data Services (applicability)

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request	Tag	Max. Tag.
26-6527-164	Alc-Dyn-Serv-SAP-Id	0	0+	0+	Y	0-31
26-6527-165	Alc-Dyn-Serv-Script-Params	0	0+	0+	Y	0-31 (untagged)
26-6527-166	Alc-Dyn-Serv-Script-Action	0	0+	0+	Y	0-31
26-6527-167	Alc-Dyn-Serv-Policy	0	0+	0+	Y	0-31
26-6527-168	Alc-Dyn-Serv-Acct-Interim-Ivl-1	0	0+	0+	Y	0-31
26-6527-169	Alc-Dyn-Serv-Acct-Interim-Ivl-2	0	0+	0+	Y	0-31
26-6527-170	Alc-Dyn-Serv-Acct-Stats-Type-1	0	0+	0+	Y	0-31
26-6527-171	Alc-Dyn-Serv-Acct-Stats-Type-2	0	0+	0+	Y	0-31

Table 33 lists the mandatory/optional attributes in CoA messages to the control channel.

Table 33: Dynamic Data Services — Control Channel CoA Attributes

Attribute name	Setup	Modify	Tear Down	Comment
Acct-Session-Id	M	M	M	Acct-Session-Id of the Control Channel (or any other valid CoA key for ESM hosts/sessions)
Alc-Dyn-Serv-SAP-Id	M(*)	M(*)	M(*)	Identifies the dynamic data service
Alc-Dyn-Serv-Script-Params	M(*)	M(*)	N/A	For a Modify, the Script Parameters represent the new parameters required for the change.
Alc-Dyn-Serv-Script-Action	M(*)	M(*)	M(*)	
Alc-Dyn-Serv-Policy	O	O	O	Default policy used when not specified for create Must be same as used for setup if specified for Modify or Teardown.
Alc-Dyn-Serv-Acct-Interim-Ivl-1	O	X (**)	X (**)	Ignored in Modify
Alc-Dyn-Serv-Acct-Interim-Ivl-2	O	X (**)	X (**)	Ignored in Modify
Alc-Dyn-Serv-Acct-Stats-Type-1	O	X (**)	X (**)	Ignored in Modify
Alc-Dyn-Serv-Acct-Stats-Type-2	O	X (**)	X (**)	Ignored in Modify

M = Mandatory, O = Optional, X = May Not, N/A = Not Applicable (ignored)
(*) = CoA Nackd if not specified (Error Cause: 402 — Missing Attribute)
(**) = CoA Nackd if specified (Error Cause: 405 — Unsupported Service)

Lawful Intercept

Table 34: Lawful Intercept (description)

Attribute ID	Attribute Name	Description
26-6527-122	Alc-LI-Action	Defines the traffic mirroring action start-mirroring 'enable' or stop-mirroring 'disable'. The Alc-LI-Action 'no-action' specifies that the router does not perform any traffic mirroring-related action. This setting can provide additional security by confusing unauthorized users who attempt to access traffic mirroring communication between the router and the RADIUS server. The CoA-only 'clear-dest-service' Alc-LI-Action creates the ability to delete all li-source entries from the mirror service defined via the Alc-LI-Destination service-id. A 'clear-dest-service' action requires an additional [26-6527-137] Alc-Authentication-Policy-Name if the CoA server is configured in the authentication policy. Values outside the Limits are treated as a setup failure.
26-6527-123	Alc-LI-Destination	Specifies the <*service-id*> that holds the mirror details (**configure mirror mirror-dest** <*service-id*>). Values above the Limits or unreferenced are treated as a setup failure.
26-6527-124	Alc-LI-FC	Defines which Forwarding Class(es) (FC's) have to be mirrored (example: Alc-LI-FC=ef). Attribute needs to be repeated for each FC's that needs to be mirrored. Values above the Limits are treated as a setup failure and all FC's will be mirrored if attribute is omitted. Additional Attributes above the Limits are silently ignored.
26-6527-125	Alc-LI-Direction	Defines if ingress, egress or both traffic directions needs to be mirrored. Both directions are mirrored if Attribute is omitted. Values above the Limits are treated as a setup failure.
26-6527-137	Alc-Authentication-Policy-Name	Used when clearing all radius li triggered sources from a mirror destination via CoA ([26-6527-122 Alc-LI-Action = 'clear-dest-service'). The policy defined in this attribute is used to authenticate the CoA and refers to **configure subscriber-mgmt authentication-policy** <*name*>. The attribute is mandatory if the RADIUS CoA server is configured in the authentication policy (**config>subscr-mgmt>auth-plcy>radius-auth-server**). The attribute is ignored if the RADIUS CoA server is configured in the radius-server context of the routing instance (**config>router>radius-server** or **config>service>vprn>radius-server**). Values above the Limits or unreferenced policies are treated as a setup failure.
26-6527-138	Alc-LI-Intercept-Id	Specifies the intercept-id to be placed in the LI-Shim header and only applicable if the mirror-dest (as specified by the Alc-LI-Destination) is configured with routable encap that contains the LI-Shim. A zero can be returned in CoA or RADIUS Accept or the value of 0 is used if this VSA is not present at all. The length of the attribute changes if the CLI parameter direction-bit (dir-bit) under the mirror-dest layer-3-encap is enabled or not (see limits).

Table 34: Lawful Intercept (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-139	Alc-LI-Session-Id	Specifies the session-id to placed in the LI-Shim header and only applicable if the mirror-dest (as specified by the Alc-LI-Destination) is configured with routable encap that contains the LI-Shim. A zero can be returned in CoA or RADIUS Accept or the value of 0 is used if this VSA is not present at all.

Table 35: Lawful Intercept (limits)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-122	Alc-LI-Action	integer	[1..4]	1=no-action, 2=enable, 3=disable, 4=clear-dest-service Note: Alc-LI-Action=clear-dest-service together with Alc-Authentication-Policy-Name attribute are only applicable in CoA For example: Alc-LI-Action = enable
26-6527-123	Alc-LI-Destination	string	2147483647 id	For example: Alc-LI-Destination = 9999

26-6527-124	Alc-LI-FC	integer	[0..7] values
			8 attributes
				0=be, 1=l2, 2=af, 3=l1, 4=h2, 5=ef, 6=h1, 7=nc
				For example: # mirror forwarding class be, af and ef
				Alc-LI-FC += be
				Alc-LI-FC += af
				Alc-LI-FC += ef

26-6527-125	Alc-LI-Direction	integer	[1..2]	1=ingress, 2=egress For example: Alc-LI-Direction = ingress
26-6527-137	Alc-Authentication-Policy-Name	string	32 chars	For example: Alc-Authentication-Policy-Name = MyAuthenticationPolicy
26-6527-138	Alc-LI-Intercept-Id	integer	29b w dir-bit 30b w/o dir-bit	29b = [0..536870911] 30b = [0..1073741823] For example: Alc-LI-Intercept-Id = 1234
26-6527-139	Alc-LI-Session-Id	integer	[0..4294967295] id	For example: Alc-LI-Session-Id = 8888

Table 36: Lawful Intercept (applicability)

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request	Encrypted
26-6527-122	Alc-LI-Action	0	1	1	Y
26-6527-123	Alc-LI-Destination	0	1	1	Y
26-6527-124	Alc-LI-FC	0	0+	0-1	Y
26-6527-125	Alc-LI-Direction	0	0-1	0-1	Y
26-6527-137	Alc-Authentication-Policy-Name	0	0	0-1	N
26-6527-138	Alc-LI-Intercept-Id	0	0-1	0-1	Y
26-6527-139	Alc-LI-Session-Id	0	0-1	0-1	Y

IPSEC

Table 37: IPSEC (description)

Attribute ID	Attribute Name	Description
1	User-Name	For IKEv2 remote-access tunnel, this represents the identity of the peer; the value of User-Name is the received IDi in IKEv2 message. This attribute is included in Access-Request and Accounting-Request
2	User-Password	For IKEv2 remote-access tunnel with pskradius authentication method, this represents the pre-shared-key of the ipsec-gw or ipsec-tunnel: **configure service ies/vprn** <*svc-id*> **interface** <*interface-name*> **sap** <*sap-id*> **ipsec-gw** <*gw-name*> **pre-shared-key** or **configure service vprn** <*svc-id*> **interface** <*interface-name*> **sap** <*sap-id*> **ipsec-tunnel** <*tnl-name*> **dynamic-keying pre-shared-key** For IKEv2 remote-access tunnel with authentication method other than pskradius, this represents the password configured in IPsec radius-authentication-policy: **configure ipsec radius-authentication-policy** <*policy-name*> **password**
8	Framed-IP- Address	The IPv4 address to be assigned to IKEv2 remote-access tunnel client via IKEv2 configuration payload: INTERNAL_IP4_ADDRESS. This attribute is also reflected in RADIUS accounting request packet.
9	Framed-IP-Netmask	The IPv4 netmask to be assigned to IKEv2 remote-access tunnel client via IKEv2 configuration payload: INTERNAL_IP4_NETMASK.
30	Called-Station-Id	The local gateway address of IKEv2 remote-access tunnel. The attribute can be included/excluded with **configure ipsec radius-authentication-policy** <*policy-name*> **include-radius-attribute called-station-id** or **configure ipsec radius-accounting-policy** <*policy-name*> **include-radius-attribute called-station-id**.
31	Calling-Station-Id	The peer's address and port of IKEv2 remote-access tunnel. The format is "address:port", for example, "10.1.1.1:1546". he attribute can be included/excluded with **configure ipsec radius-authentication-policy** <*policy-name*> **include-radius-attribute calling-station-id** or **configure ipsec radius-accounting-policy** <*policy-name*> **include-radius-attribute caling-station-id**.
44	Acct-Session-Id	A unique identifier representing an IKEv2 remote-access tunnel session that is authenticated. Same Acct-Session-Id is included in both access-request and accounting-request. The format is local_gw_ip-remote_ip:remote_port-time_stamp.

Table 37: IPSEC (description) (Continued)

Attribute ID	Attribute Name	Description
79	EAP-Message	This attribute encapsulates the received IKEv2 EAP payload in access-request. A RADIUS server can include this attribute in an acccess-challenge or access-accept.
80	Message-Authenticator	This attribute is used in EAP authentication and provides message integrity verification.
87	Nas-Port-Id	The public SAP ID of IKEv2 remote-access tunnel. The attribute can be included/excluded with **configure ipsec radius-authentication-policy** <*policy-name*> **include-radius-attribute nas-port-id** or **configure ipsec radius-accounting-policy** <*policy-name*> in**clude-radius-attribute nas-port-id**.
26-311-16	MS-MPPE-Send-Key	This attribute along with [26-311-17] MS-MPPE-Recv-Key hold the Master Session Key (MSK) of the EAP authentication. It is expected in access-accept when EAP authentication succeed with certain EAP methods.
26-311-17	MS-MPPE-Recv-Key	This attribute along with [26-311-16] MS-MPPE-Send-Key hold the Master Session Key (MSK) of the EAP authentication. It is expected in access-accept when EAP authentication succeed with certain EAP methods.
26-6527-9	Alc-Primary-Dns	The primary IPv4 DNS server address to be assigned to IKEv2 remote-access tunnel client via IKEv2 configuration payload: INTERNAL_IP4_DNS.
26-6527-61	Alc-IPsec-Serv-Id	IPSec private service id, used by IKEv1 xauth tunnel, referring to the preconfigured VPRN where the IPSec tunnel terminates (**configure service vprn** <*service-id*>). A default private service is used when this attribute is omitted (**configure service vprn interface sap ipsec-gw default-secure-service**). If the returned service id doesn't exist/out-of limits or exists but not a VPRN service, the tunnel setup will fail.
26-6527-62	Alc-IPsec-Interface	Private IPSec interface name, used by IKEv1 xauth tunnel, refers to a preconfigured private ipsec interface the IPSec tunnel terminates (**config>service>vprn>interface** <*int-name*> **tunnel**). A default private interface is used when this attribute is omitted (**config>service>ies>if>sap>ipsec-gw>default-secure-service** <*service-id*> **interface** <*ip-int-name*>); the maximum length is 32 bytes; if the returned interface doesn't exist/exceed the maximum length or exists but is not a private ipsec interface, the tunnel setup will fail.
26-6527-63	Alc-IPsec-Tunnel-Template-Id	IPSec tunnel-template id, used by IKEv1 xauth tunnel, refers to a preconfigured ipsec tunnel-template (**configure ipsec tunnel-template** <*ipsec template identifier*>). A default tunnel-template is used when this attribute is omitted (**configure service vprn interface sap ipsec-gw default-tunnel-template** <*template-id*>). If the returned template does not exist or exceeds the limits, the tunnel setup will fail.

Table 37: IPSEC (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-64	Alc-IPsec-SA-Lifetime	IPSec phase2 SA lifetime in seconds, used by IKEv1 xauth tunnel. A pre-configured value is used when this attribute is omitted (**configure ipsec ike-policy ipsec-lifetime** <*ipsec-lifetime*>). Values outside the Limits are treated as a tunnel setup failure.
26-6527-65	Alc-IPsec-SA-PFS-Group	IPSec PFS group id, used by IKEv1 xauth tunnel. The PFS group in ike-policy is used when this attribute is omitted (**configure ipsec ike-policy** *1* **pfs dh-group** <*grp-id*>); if the returned value is not one of the allowed value, the tunnel setup will fail.
26-6527-66	Alc-IPsec-SA-Encr-Algorithm	IPSec phase2 SA Encryption Algorithm, used by IKEv1 xauth tunnel. The esp-encryption-algorithm in ipsec-transform is used when this attribute is omitted (**configure ipsec ipsec-transform esp-encryption-algorithm** <*algo*>). This attribute must be used along with Alc-IPsec-SA-Auth-Algorithm, otherwise tunnel setup will fail. Values different then the Limits are treated as a setup failure.
26-6527-67	Alc-IPsec-SA-Auth-Algorithm	IPSec phase2 SA Authentication Algorithm, used by IKEv1 xauth tunnel. The esp-auth-algorithm in ipsec-transform is used when this attribute is omitted (**configure ipsec ipsec-transform esp-auth-algorithm** <*algo*>). Values different than the Limits are treated as a tunnel setup failure. This attribute must be used along with Alc-IPsec-SA-Encr-Algorithm, otherwise tunnel setup will fail.
26-6527-68	Alc-IPsec-SA-Replay-Window	IPSec anti-replay window size, used by IKEv1 xauth tunnel. The replay-window size in tunnel-template is used when this attribute is omitted (**configure ipsec tunnel-template replay-window** <*size*>). Values different than the Limits are treated as a tunnel setup failure

Table 38: IPSEC (limits)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
1	User-Name	string	253 bytes	# Format depends on IDi format. For example: User-Name = “user1@domain1.com”
2	User-Password	string	64 bytes	
8	Framed-IP-Address	ipaddr	4 bytes	For example: Framed-IP-Address = 192.168.10.100
9	Framed-IP-Netmask	ipaddr	4 bytes	For example: Framed-IP-Netmask = 255.255.255.0
30	Called-Station-Id	string	253 bytes	# local gateway address of IKEv2 remote-access tunnel. For example: Called-Station-Id = “172.16.100.1”
31	Calling-Station-Id	string	253 bytes	# peer-address:port For example: Calling-Station-Id = “192.168.5.100:500”
44	Acct-Session-Id	string	147 bytes	# local_gw_ip-remote_ip:remote_port-time_stamp. For example: Acct-Session-Id = 172.16.100.1-192.168.5.100:500-1365016423
79	EAP-Message	string	253 bytes	Binary string
80	Message-Authenticator	string	16 bytes	Binary string
87	Nas-Port-Id	string	44 bytes	# SAP-ID For example: Nas-Port-Id = “tunnel-1.public:100”
26-311-16	MS-MPPE-Send-Key	string	254 bytes	Binary string
26-311-17	MS-MPPE-Recv-Key	string	254 bytes	Binary string
26-6527-9	Alc-Primary-Dns	ipaddr	4 bytes	For example: Alc-Primary-Dns = 192.168.1.1
26-6527-61	Alc-IPsec-Serv-Id	integer	2147483647 id	For example: Alc-IPsec-Serv-Id = 100
26-6527-62	Alc-IPsec-Interface	string	32 chars	For example: Alc-IPsec-Interface = IPsec-Priv
26-6527-63	Alc-IPsec-Tunnel-Template-Id	integer	2048 id	For example: Alc-IPsec-Tunnel-Template-Id = 200

Table 38: IPSEC (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-64	Alc-IPsec-SA-Lifetime	integer	[1200..172800] seconds	For example: Alc-IPsec-SA-Lifetime = 2400
26-6527-65	Alc-IPsec-SA-PFS-Group	integer	[1|2|5]	1=group1, 2=group2, 5=group5 For example: Alc-IPsec-SA-PFS-Group = 2
26-6527-66	Alc-IPsec-SA-Encr-Algorithm	integer	[1..6]	1=null, 2=des, 3=des3, 4=aes128, 5=aes192, 6=aes256 For example: Alc-IPsec-SA-Encr-Algorithm = 3
26-6527-67	Alc-IPsec-SA-Auth-Algorithm	integer	[1..3]	1=null, 2=md5, 3=sha1 For example: Alc-IPsec-SA-Auth-Algorithm = 3
26-6527-68	Alc-IPsec-SA-Replay-Window	integer	32|64|128|256|512	For example: Alc-IPsec-SA-Replay-Window = 128

Table 39: IPSEC (applicability)

Attribute ID	Attribute Name	Access Request	Access Accept	Access Challenge	Acct Request
1	User-Name	1	0-1	0	1
2	User-Password	1	0	0	0
8	Framed-IP- Address	0	1	0	0-1
9	Framed-IP-Netmask	0	0-1	0	0
30	Called-Station-Id	0-1	0	0	0-1
31	Calling-Station-Id	0-1	0	0	0-1
44	Acct-Session-Id	1	0	0	1
79	EAP-Message	0+	0+	0+	0
80	Message-Authenticator	0-1	0-1	0-1	0
87	Nas-Port-Id	0-1	0	0	0-1
26-311-16	MS-MPPE-Send-Key	0	0-1	0	0
26-311-17	MS-MPPE-Recv-Key	0	0-1	0	0
26-6527-9	Alc-Primary-Dns	0	0-1	0	0
26-6527-61	Alc-IPsec-Serv-Id	0	0-1	0	0
26-6527-62	Alc-IPsec-Interface	0	0-1	0	0
26-6527-63	Alc-IPsec-Tunnel-Template-Id	0	0-1	0	0
26-6527-64	Alc-IPsec-SA-Lifetime	0	0-1	0	0
26-6527-65	Alc-IPsec-SA-PFS-Group	0	0-1	0	0
26-6527-66	Alc-IPsec-SA-Encr-Algorithm	0	0-1	0	0
26-6527-67	Alc-IPsec-SA-Auth-Algorithm	0	0-1	0	0
26-6527-68	Alc-IPsec-SA-Replay-Window	0	0-1	0	0

Application Assurance

Table 40: Application Assurance (description)

Attribute ID	Attribute Name	Description
8	Framed-IP-Address	Mandatory ipv4 address attribute to create (CoA), delete (Delete) or audit (CoA) an ipv4 AA-transit subscriber. In case of a ipv4 host creation (CoA), if the host is already configured for another AA-transit subscriber with the same parent SAP, it will be removed for this AA-subscriber and added to AA-subscriber, referred by the [26-6527-11] Alc-Subsc-ID-Str, in the CoA message. If the parent SAP, referred by the [87] NAS-Port-Id), is different, the host creation will fail. An AA-transit subscriber can have up to 32 hosts (ipv4 or ipv6). A host cannot be added to a AA-transit subscriber if it is already configured for a static AA-transit subscriber with a different subscriber-ID. A Disconnect message sent with the last host of an AA-transit subscriber will delete the AA-transit subscriber.
87	NAS-Port-Id	A text string identifying the physical SAP or SDP serving the AA-transit subscriber (parent SAP or SDP). Mandatory attribute to create (CoA), delete (Disconnect) or audit (CoA) a transit-AA subscriber.
97	Framed-IPv6-Prefix	The ipv6 address for AA-Transit subscriber creation/removal (same use as [8] Framed-Ip-Address).
26-6527-11	Alc-Subsc-ID-Str	A mandatory attribute used in Access-Accept for AA subscriber creation (as in ESM host creation) or application-profile change (CoA) and for AA-transit subscriber creation (CoA), removal (Disconnect) or audit (CoA). Attribute values longer than the allowed string value are treated as setup failures.
26-6527-45	Alc-App-Prof-Str	Application Assurance for residential, business or transit-AA subscribers is enabled through the assignment of an application profile as part of either enhanced subscriber management or static configuration. [26-6527-45] Alc-App-Prof-is is a string that maps (**configure subscriber-mgmt sub-ident-policy** <*sub-ident-policy-name*> **app-profile-map**) to such an application profile (**configure application-assurance group** <*aa-group-id:partition-id*> **policy app-profile** <*app-profile-name*>). This attribute is used in access-accept (to assign an application profile during esm host creation) and CoA (to change the application profile of a AA-subscriber or to create transit AA-subscriber). Strings longer than the allowed maximum are treated as setup failures. Unreferenced strings (strings not mapping to an application profile) will silently trigger a fallback to pre-configured default values if allowed. If no default value is pre-configured, the subscriber's application profile is silently disabled for esm AA-subscriber; in case of a transit AA-subscriber creation the CoA will be rejected. The change of an application profile to one configured under a different group/partition or the modification of the application profile of a static AA-subscriber is not allowed and will be treated as setup failures.

Table 40: Application Assurance (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-130	Alc-AA-Transit-IP	Used to create (CoA), modify (CoA), delete (disconnect) or audit (CoA) an Application Assurance transit-ipv4/v6-subscriber for business AA deployments and allows reporting and policy enforcement at IP address or prefix level within the parent SAP or spoke-SDP. Mandatory attributes to create(c), modify(m), delete(d) or audit(a) an AA-transit-ip-subscriber are: [8] Framed-IP-Address (c/m/d/a) or [97] Framed-IPv6-Prefix(c/m/d/a), [87] NAS-Port-Id(c/m/d/a), [26-6527-11] Alc-Subsc-ID-Str(c/m/d/a), [26-6527-45] Alc-App-Prof-Str(c/m/a) and [26-6527-130] Alc-AA-Transit-IP(c/m/d/a). The value of [26-6527-130] Alc-AA-Transit-IP must be an Integer, the value 1 (host) is used for host creation, 2 (audit-start) and 3 (audit-end) are used for the audit.
26-6527-182	Alc-AA-Sub-Http-Url-Param	Optional text string used to customize the URL used for HTTP In-Browser Notification and automatically appended at the end of the notification script URL as an argument. This text string can also be configured in the http-redirect URL policy using maco substitution. The VSA string typically contains one or more argument names and values; there is no limit in the number of arguments besides the maximum length of the VSA. Each new argument must be preceded by “&” so as to be understood properly by a web server, the format for the Alc-AA-Sub-Http-Url-Param string must be for instance: "&<arg1>=<value1>" or "&<arg1>=<value1>&<arg2>=<value2>" This VSA string can be overwritten through CoA.

Table 40: Application Assurance (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-193	Alc-AA-App-Service-Options	Used to apply Application Service Option (ASO) overrides. These attributes can only be applied if an app-profile is also or has previously been associated with the AA-sub (explicitly or by default), or else the override is rejected. An access accept or COA message can send one or more of these VSAs, with each VSA containing a string with the characteristic name and the value name pair. To provide multiple ASO attributes, the message can include multiple ASO VSAs, in addition to an App-profile VSA. The VSA string contains the characteristic name and the value name. The format for the Alc-AA-App-Service-Options string must be "<char>=<value>". An equal sign is used as the delimiter between characteristic string and value string. Each name can have any character including spaces, except '='. Everything before the '=' will be interpreted as the character string and everything after the '=' will be interpreted as the value string. One ASO char=value pair is supported per VSA, If an ASO char=value pair is not found in a VSA, the message is rejected. If an ASO char=value does not match a provisioned ASO for the group/partition for that subscriber, the message is rejected. An app profile is a defined set of ASO values. App-profiles interact with ASO overrides in this way: a) The Alc-AA-App-Service-Options VSA is optional on sub create (with app-profile assignment) and may be used later to modify policy. b) On a COA if an app-prof VSA is not present all ASO VSAs will be applied on top of the current policy of the sub. c) On a COA if an app-prof VSA is present, even if it is the same app-profile as currently applied, ll previous ASO override policy is removed. Any ASO VSAs in the same COA message as the new app-profile will be applied on top of the app-profile policy. In this way, re-sending app-profile resets all ASO state history. On a COA, if the app-profile changes, and no ASO VSAs exist, all current ASO overrides are removed. d) If the app-profile changes, and ASO VSAs exist, all current ASO overrides are removed, and the new ASO overrides are applied to this new app-profile. e) A new aa-sub characteristic can be applied, or an existing characteristic modified, by an ASO VSA. f) When a ASO VSA is received any existing overrides will remain and the new overrides are cumulative. If there are multiple ASO VSAs for the same characteristic in the COA, the last one will take effect.

Table 41: Application Assurance (limits)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
8	Framed-IP-Address	ipaddr	4 Bytes	# For example: ipv4 transit-AA-subscriber 150.0.200.1 Framed-IP-Address = “150.0.200.1”
87	NAS-Port-Id	string	253 bytes	# Depends on the parent port type # For example for sap NAS-Port-Id = 1/1/4:501.1001 # For example for spoke-sdp NAS-Port-Id = 4:100
97	Framed-IPv6-Prefix	ipv6prefix	max. 16 Bytes for prefix + 1 byte for length	# For example: Framed-IPv6-Prefix = 2001:cafe:cefe:1::/64
26-6527-11	Alc-Subsc-ID-Str	string	32 chars	# For example: Alc-Subsc-ID-Str = transit-sub-radius1
26-6527-45	Alc-App-Prof-Str	string	16 bytes	# For example: Alc-App-Prof-Str = MyAppProfile

26-6527-130	Alc-AA-Transit-IP	integer	4 Bytes	1=host, 2=audit-start, 3=audit-end
				For example: # CoA create AA transit subscriber on SAP 4/1/1, IP address 150.0.200.1
				Alc-AA-Transit-IP = host
				NAS-Port-ID = 4/1/1
				framed-ip-address = 150.0.200.1
				Alc-Subsc-ID-Str = transit-sub-radius1
				Alc-App-Prof-Str = MyAppProfile

26-6527-182	Alc-AA-Sub-Http-Url-Param	string	32 chars	# For example Alc-AA-Sub-Http-Url-Param = "&Provider=ISPname&Location=Station21"
26-6527-193	Alc-AA-App-Service-Options	string	65 bytes per string (char. 32bytes + 1 byte + value 32bytes) 32 VSAs per message	Format *charteristic=value,* # For example: Alc-AA-App- Service-Options = “ServiceTier=Bronze”

Table 42: Application Assurance (applicability)

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request
8	Framed-IP-Address	0	0	0-1
87	NAS-Port-Id	0	0	0-1
97	Framed-IPv6-Prefix	0	0	0-1
26-6527-11	Alc-Subsc-ID-Str	0	0-1	0-1
26-6527-45	Alc-App-Prof-Str	0	0-1	0-1
26-6527-130	Alc-AA-Transit-IP	0	0	0-1
26-6527-182	Alc-AA-Sub-Http-Url-Param	0	0-1	0-1
26-6527-193	Alc-AA-App-Service-Options	0	0-1	0-1

CLI User Authentication and Authorization

Table 43: CLI User Authentication and Authorization (description)

Attribute ID	Attribute Name	Description
1	User-Name	The name of user requesting user-Authentication, Authorization, Accounting. User-names longer the allowed maximum Limit are treated as an authentication failure.
2	User-Password	The password of user requesting user-Authentication, Authorization, Accounting and always encrypted in a fixed length
4	NAS-IP-Address	The identifying IP Address of the NAS requesting the Authentication or Accounting. Included when the RADIUS server is reachable via IPv4. The address is determined by the routing instance through which the RADIUS server can be reached: "Management"— The active ipv4 address in the Boot Options File (**bof address** <*ipv4-address*>) "Base" — The ipv4 address of the system interface (**configure router interface system address** <*address*>). The address can be overwritten with the configured source-address (**configure system security source-address application radius** <*ip-int-name*|*ip-address*>)
31	Calling-Station-Id	The IP address (coded in hex) from the user that requests Authentication, Authorization, Accounting or "CONSOLE" when requesting access from the serial port (Console).
44	Acct-Session-Id	A unique, without meaning, generated number per authenticated user and reported in all accounting messages and used to correlate users CLI commands (accounting data) from the same user.
61	NAS-Port-Type	Mandatory included as type Virtual (5) for telnet/ssh or Async (0) for Console.
95	NAS-IPv6-Address	The identifying IP Address of the NAS requesting the Authentication or Accounting. Included when the RADIUS server is reachable via IPv6. The address is determined by the routing instance through which the RADIUS server can be reached: "Management" — The active IPv6 address in the Boot Options File (**bof address** <*ipv6-address*>) "Base" — The IPv6 address of the system interface (**configure router interface system ipv6 address** <*ipv6-address*>). The address can be overwritten with the configured ipv6-source-address (**configure system security source-address application6 radius** <*ipv6-address*>)
26-6527-1	Timetra-Access	Specifies the type of access (FTP, console access or both) the user is permitted.

Table 43: CLI User Authentication and Authorization (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-2	Timetra-Home-Directory	Specifies the local home directory for the user for console and FTP access and is enforced with attribute [26-6527-3]Timetra-Restrict-To-Home. The home directory is not enforced if [26-6527-3]Timetra-Restrict-To-Home is omitted. The local home directory is entered from the moment when the authenticated user enters the **file** CLI command.
26-6527-3	Timetra-Restrict-To-Home	When the value is true the user is not allowed to navigate to directories above his home directory for file access. The home-directory is specified in [26-6527-2] Timetra-Home-Directory and is root if [26-6527-2] Timetra-Home-Directory is omitted.
26-6527-4	Timetra-Profile	The user profile(s) that the user has access to and refers to pre-configured user-profile-name's (**configure system security profile** <*user-profile-name*>). These pre-configured profiles hold a default-action, a match command-string and a command-action. Unreferenced profiles names are silently ignored. If the maximum number of profile strings is violated, or if a string is too long, processing the input is stopped but authorization continues and too long profile string (and all strings followed by that) are ignored. Each user can have multiple profiles and the order is important. The first user profile has highest precedence, followed by the second and so on. Note: For each authenticated RADIUS user a temporary profile with name [1]User-Name is always created (show system security profile) and executed as last profile. This temporary profile is build from the mandatory attribute [26-6527-5]Timetra-Default-Action and optional attributes [26-6527-6] Timetra-Cmd, [26-6527-7] Timetra-Action.
26-6527-5	Timetra-Default-Action	Specifies the default action (permit-all, deny-all or none) when the user has entered a command and none of the commands-strings in [26-6527-6]Timetra-Cmd resulted in a match condition. The attribute is mandatory and required even if the [36-6527-6] Timetra-Cmd's are not used.
26-6527-6	Timetra-Cmd	Command string, subtree command-string or a list of command-strings as scope for the match condition for user authorization. Multiple command-strings in the same attribute are delimited with the; character. Additional command-strings are encoded in multiple attributes. If the maximum number of command strings is violated, or if a string is too long, processing the input is stopped but authorization continues, so if the radius server is configured to have 5 command strings of which the 3rd is too long, only the first 2 entries will be used and the rest will be ignored. Each [26-6527-6] Timetra-Cmd attribute is followed in sequence by a [26-6527-7] Timetra-Action. (A missing Timetra-Action results in a deny). Note: For each authenticated RADIUS user a temporary profile with name [1]User-Name is always created (show system security profile) and executed as last profile. This temporary profile is build from the mandatory attribute [26-6527-5]Timetra-Default-Action and optional attributes [26-6527-6] Timetra-Cmd, [26-6527-7] Timetra-Action.

Table 43: CLI User Authentication and Authorization (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-7	Timetra-Action	Action to be used in case a user's command matches the commands specified in [26-6527-6] Timetra-Cmd attribute. Action deny is used if attribute is omitted and the [26-6527-5] Timetra-Default-Action is used when no match is found. Note: [26-6527-6]Timetra-Cmd, [26-6527-7]Timetra-Cmd and [26-6527-8]Timetra-Cmd are an alternative for [26-6527-4]Timetra-Profile. Note: For each authenticated RADIUS user a temporary profile with name [1]User-Name is always created (show system security profile) and executed as last profile. This temporary profile is build from the mandatory attribute [26-6527-5]Timetra-Default-Action and optional attributes [26-6527-6] Timetra-Cmd, [26-6527-7] Timetra-Action.
26-6527-8	Timetra-Exec-File	Specifies the file that is executed whenever the user is successfully authenticated.

Table 44: CLI User Authentication and Authorization (limits)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
1	User-Name	string	32 chars	For example: User-Name = “admin”
2	User-Password	string	16 chars fixed	Encrypted password For example: User-Password 4ec1b7bea6f2892fa466b461c6accc00
4	NAS-IP-Address	ipaddr	4 Bytes	# ip-address For example: NAS-IP-Address = “192.0.2.1”
31	Calling-Station-Id	string	64 Bytes	# users ip address or “CONSOLE” For example: Calling-Station-Id = “192.0.2.2” or Calling-Station-Id = “2001:db8::2”
44	Acct-Session-Id	string	22 Bytes	For example: Acct-Session-Id = “2128463592102512113409”
61	NAS-Port-Type	integer	4 Bytes value 5 fixed	Fixed set to value Virtual (5) for ssh/telnet and Async (0) for console. For example: NAS-Port-Type 00000005
95	NAS-IPv6-Address	ipv6addr	16 Bytes	# ipv6 address For example: NAS-IPv6-Address = 2001:db8::1
26-6527-1	Timetra-Access	integer	1,2,3	1=ftp, 2=console (serial port, Telnet and SSH(SCP)), 3=both For example: Timetra-Access = console
26-6527-2	Timetra-Home-Directory	string	190 chars	For example: Timetra-Home-Directory = cf3:/7750/configs/
26-6527-3	Timetra-Restrict-To-Home	integer	1,2 (false, true)	1=true, 2=false For example: Timetra-Restrict-To-Home = true
26-6527-4	Timetra-Profile	string	16 attributes 32 chars/ attribute	For example: Timetra-Profile += administrative1 Timetra-Profile += administrative2
26-6527-5	Timetra-Default-Action	integer	1,2,3	1=permit-all, 2=deny-all, 3=none For example: Timetra-Default-Action = none
26-6527-6	Timetra-Cmd	string	25 attributes 247 chars/ attribute	For example: Timetra-Cmd += configure router isis;show subscriber-mgmt sub-profile Timetra-Cmd += show router

Table 44: CLI User Authentication and Authorization (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-7	Timetra-Action	integer	25 attributes	# 1=permit, 2=deny For example: Timetra-Cmd = permit
26-6527-8	Timetra-Exec-File	string	200 chars	Timetra-Exec-File = <local-url>|<remote-url> # local-url : <cflash-id>/][<file-path> # remote-url : {ftp://|tftp://}<login>:<pswd>@<remote-locn>/<file-path> For example: Timetra-Exec-File = cf3:/MyScript Timetra-Exec-File = ftp://root:root@192.168.0.10/home/configs/MyScript.cfg

Table 45: CLI User Authentication and Authorization (applicability)

Attribute ID	Attribute Name	Access Request	Access Accept	Encrypted
1	User-Name	1	0	1
2	User-Password	1	0	0
4	NAS-IP-Address	0-1	0	1
31	Calling-Station-Id	1	0	1
44	Acct-Session-Id	0	0	1
61	NAS-Port-Type	1	0	1
95	NAS-IPv6-Address	0-1	0	1
26-6527-1	Timetra-Access	0	1	0
26-6527-2	Timetra-Home-Directory	0	1	0
26-6527-3	Timetra-Restrict-To-Home	0	1	0
26-6527-4	Timetra-Profile	0	0+	0
26-6527-5	Timetra-Default-Action	0	1	0
26-6527-6	Timetra-Cmd	0	0+	1
26-6527-7	Timetra-Action	0	0-1	0
26-6527-8	Timetra-Exec-File	0	0-1	0

AAA Route Downloader

Table 46: AAA Route Downloader (description)

Attribute ID	Attribute Name	Description
1	User-Name	Maps to **configure aaa route-downloader** <*name*> **base-user-name** <*user-name*> were the base-user-name sets the prefix for the username that shall be used in access requests. The actual name used will be a concatenation of this string, a " -" (hyphen) character and a monotonically increasing integer. Consecutive Access-Requests with incrementing User-Name are repeated until the aaa route download application receives an Access-Reject. Default is system-name.
2	User-Password	Maps to **configure aaa route-downloader** <*name*> **password** <*password*> in the RADIUS-Access request. Default is empty string.
22	Framed-Route	The RADIUS route-download application periodically sends a RADIUS Access-Request message to the RADIUS server to request that ipv4/ipv6 routes be downloaded. The RADIUS server responds with an Access-Accept message and downloads the configured ipv4/ipv6 routes. When the download operation is complete, the route-download application installs the ipv4/ipv6 routes in the routing table as black-hole routes with protocol Periodic and with fixed preference 255. A default metric (**configure aaa route-downloader** <*name*> **default-metric** [0..254]) is installed when the metric value is omitted in the formatted attribute. A default tag (**configure aaa route-downloader** <*name*> **default-tag** [0..4294967295]) is installed when the tag value is omitted in the formatted attribute. The complete RADIUS Access Accept is ignored (failed to parse route) if at least one route has the wrong format. Only the individual route is silently ignored (not seen as a process download failure) if the formatted vprn service or service-name is invalid. Routes no longer present in the download will be removed from the routing table and new routes are added, same routes are not replaced. Routes with different tags or metrics are seen as new routes. If the AAA server responds with an Access-Reject for the first username, then all routes will be removed from the routing table (implicit empty route-download table). The route-download application accepts downloaded ipv4 routes in either [22] Framed-Route or [26-1] Cisco-AVpair attribute format.
99	Framed-IPv6-Route	See description [22] Framed-Route \The route-download application accepts downloaded ipv6 routes only in [99] Framed-IPv6-Route format.
26-9-1	cisco-av-pair	See description [22] Framed-Route

Table 47: AAA Route Downloader (limits)

Attri-bute ID	Attribute Name	Type	Limits	SR-OS Format
1	User-Name	string	32 chars base-user-name	For example: # base-user-name download-pool USER NAME [1] 16 download-pool-1
2	User-Password	string	max. 32 chars.	Encrypted password For example: User-Password 4ec1b7bea6f2892fa466b461c6accc00

22	Framed-Route	string	253 bytes
			200.000 attributes
				Format [vrf {vpn-name|vpn-serviceid}] {IP} prefix-mask {null0 | null 0 | black-hole} [metric] [tag tag-value]
				#The prefix-mask could be in any form as: prefix/length, prefix mask or prefix (the mask is derived from the IP class of the prefix).
				For example:
				# A base route 192.1.0.0/24 with different formats, metric and tags
				Framed-Route = 192.1.0.0/24 black-hole tag 1,
				Framed-Route = 192.1.0.0 255.255.255.0 null 0 20 tag 1,
				Framed-Route = 192.1.0.0 null0 22255 tag 33,
				For example: # A vrf route 192.1.1.0/24 with different formats, metric and tags
				Framed-Route = vrf 6000 192.1.1.0 null0 254 tag 4,
				Framed-Route = vrf ws/rt-custmomerx 192.1.1.0 null0 254 tag 5,

99	Framed-IPv6-Route	string	253 bytes 200.000 attributes	Format [vrf {vpn-name|vpn-serviceid}] {IP} prefix-mask {null0 | null 0 | black-hole} [metric] [tag tag-value] #The prefix-mask could be in any form as: prefix/length, prefix mask or prefix (the mask is derived from the IP class of the prefix). For example: Framed-IPv6-Route += 4001:0:0:1::/64 null0, Framed-IPv6-Route += vrf ws/rt-custmomerx 4002:0:0:0:1::/96 null 0 10 tag 4294967295, Framed-IPv6-Route += vrf 6000 4003:0:1::/48 black-hole 0 tag 4294967295,t

Table 47: AAA Route Downloader (limits) (Continued)

Attri-bute ID	Attribute Name	Type	Limits	SR-OS Format
26-9-1	cisco-av-pair	string	253 bytes 200.000 attributes	Format [vrf {vpn-name|vpn-serviceid}] {IP} prefix-mask {null0 | null 0 | black-hole} [metric] [tag tag-value] #The prefix-mask could be in any form as: prefix/length, prefix mask or prefix (the mask is derived from the IP class of the prefix). For example: # A base route 192.1.5.0/24 without metric and tags (use defaults) cisco-avpair += ip:route=192.1.0.0 255.255.255.0 null0, For example: # A vrf route 192.1.1.0/24 with different formats, metric and tags cisco-avpair += ip:route=vrf 6000 192.1.1.0/24 null 0 0 tag 62, cisco-avpair += ip:route=vrf ws/rt-custmomerx 192.1.1.0/24 null 0 200 tag 63

Table 48: AAA Route Downloader (applicability)

Attribute ID	Attribute Name	Access Request	Access Accept
1	User-Name	1	0
2	User-Password	1	0
22	Framed-Route	0	0+
99	Framed-IPv6-Route	0	0+
26-9-1	cisco-av-pair	0	0+

RADIUS Accounting Attributes

Enhanced Subscriber Management (ESM) Accounting

There are currently three accounting modes in Enhanced Subscriber Management accounting:

- Host accounting (H)
- PPPoE Session accounting (S)
- Queue instance accounting (Q)

A single host can have up to two simultaneously active accounting modes.

The Acct Reporting Level column in Table 52 shows in which accounting mode messages the attribute is reported:

- HSQ means the attribute is present in the accounting messages of all accounting modes
- H->S->Q means the attribute is present in the accounting messages of a single accounting mode:
  - → If Host accounting is enabled, then the attribute is present in the accounting messages that belong to this mode.
  - → Else if session accounting is enabled, then the attribute is present in the accounting messages that belong to this mode.
  - → Else if Queue instance accounting is enabled, then the attribute is present in the accounting messages that belong to this mode.

Each accounting mode has a dedicated accounting session id. The accounting session id (number format) has a fixed length format of 22 bytes and is unique.

- Host accounting (per subscriber host):

  ```
  show service id <svc-id> subscriber-hosts detail

  Acct-Session-Id       : 241AFF000000204FE9D801
  ```

- Session accounting (per PPPoE session):

  ```
  show service id <svc-id> ppp session detail

  Acct-Session-Id   : 241AFF000000214FE9D801
  ```

- Queue instance accounting (per queue instance):

  ```
  show service id <svc-id> subscriber-hosts detail

  Acct-Q-Inst-Session-Id: 241AFF000000224FE9D801
  ```

The Host or Session accounting session id can be included in a RADIUS Access Request:

```
configure
    subscriber-mgmt
        authentication-policy <policy-name>
            include-radius-attribute acct-session-id [host|session]
```

The accounting session ID format that appears in RADIUS accounting messages can be configured to a fixed 22 byte hexadecimal number format or a variable length description format:

```
configure
    subscriber-mgmt
        radius-accounting-policy <policy-name>
            session-id-format {description|number}
```

An Acct-Multi-Session-Id is included in all RADIUS accounting messages (start/stop/interim):

Table 49: Enhanced Subscriber Management Accounting [50] Acct-Multi-Session-Id values

queue-instance-accounting	host-accounting	session-accounting	[50] Acct-Multi-Session-Id
✓	x	x	Not present
x	✓	x	Queue Instance Acct-Session-Id
x	x	✓	Queue Instance Acct-Session-Id
✓	✓	x	Queue Instance Acct-Session-Id
✓	x	✓	Queue Instance Acct-Session-Id
x	✓	✓	Session Acct-Session-Id

Table 50: Enhanced Subscriber Management Accounting (description)

Attribute ID	Attribute Name	Description
1	User-Name	Refers to the user to be authenticated in the Access-Request. The format for IPoE/PPPoE hosts depends on configuration parameters pppoe-access-method, ppp-user-name or user-name-format in the CLI context **configure subscriber-mgmt authentication-policy** <*name*>. The format for ARP-hosts is not configurable and always the host IPv4-address. The RADIUS User-Name specified in an Access-Accept or CoA is reflected in the corresponding accounting messages. The attribute is omitted in authentication/accounting via **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute no user-name**.

Table 50: Enhanced Subscriber Management Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
4	NAS-IP-Address	The identifying IP Address of the NAS requesting the Authentication or Accounting. Included when the RADIUS server is reachable via IPv4. The address is determined by the routing instance through which the RADIUS server can be reached: “Management” — The active IPv4 address in the Boot Options File (**bof address** <*ipv4-address*>) “Base” or “VPRN”— The the IPv4 address of the system interface (**configure router interface system address** <*address*>). The address can be overwritten with the configured source-address (**configure aaa radius-server-policy** <*policy-name*> **servers source-address** <*ip-address*>)
5	NAS-Port	The physical access-circuit on the NAS which is used for the Authentication or Accounting of the user. The format of this attribute is configurable on the NAS as a fixed 32 bit value or a parameterized 32 bit value. The parameters can be a combination of outer-vlan-id(o), inner-vlan-id(i), slot number(s), MDA number(m), port number or lag-id(p), ATM VPI(v) and ATM VCI(c), fixed bit values zero (0) or one (1) but cannot exceed 32 bit. The format can be configured for following applications: **configure aaa l2tp-accounting-policy** <*name*> **include-radius-attribute nas-port**, **configure router l2tp cisco-nas-port**, **configure service vprn** <*service-id*> **l2tp cisco-nas-port**, **configure subscriber-mgmt authentication-policy** <*name*> **include-radius-attribute nas-port**, **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute nas-port**.
6	Service-Type	The type of service the PPPoE user has requested, or the type of service to be provided for the PPPoE user. Optional in RADIUS-Accept and CoA. Treated as a session setup failure if different from Framed-User.
7	Framed-Protocol	The framing to be used for framed access in case of PPPoE users. Optional in RADIUS-Accept and CoA. Treated as a session setup failure if different from PPP.
8	Framed-IP-Address	The IPv4 address to be configured for the host via DHCPv4 (radius proxy) or IPCP (PPPoE). Simultaneous returned attributes [88] Framed-Pool and [8] Framed-IP-Address (RADIUS Access-Accept) are handled as host setup failures. Attribute is also used in CoA and Disconnect Message (part of the ESM or AA user identification-key). Attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute no framed-ip-addr**.

Table 50: Enhanced Subscriber Management Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
9	Framed-IP-Netmask	The IP netmask to be configured for the user when the user is a router to a network. For DHCPv4 users, the attribute maps to DHCPv4 option [1] Subnet mask and is mandatory if [8] Framed-IP-Address is also returned. For PPPoE residential access, the attribute should be set to 255.255.255.255 (also the default value if the attribute is omitted). For PPPoE business access, the attribute maps to PPPoE IPCP option [144] Subnet-Mask only when the user requests this option and if the node parameter **configure subscriber-mgmt ppp-policy** <*ppp-policy-name*> **ipcp-subnet-negotiation** is set. Attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute no framed-ip-netmask**.
22	Framed-Route	The routing information (IPv4 managed route) to be configured on the NAS for a host (dhcp, pppoe, arp) that operates as a router without NAT (so called Routed subscriber host). Valid RADIUS learned managed routes can be included in RADIUS accounting messages with following configuration: **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute framed-route**. Associated managed routes for an instantiated routed subscriber host are included in RADIUS accounting messages independent of the state of the managed route (Installed, Shadowed or HostInactive). In case of a PPP session, when a Framed-Route is available while the corresponding routed subscriber host is not yet instantiated, the managed route is in the state “notYetInstalled” and will not be included in RADIUS accounting messages.
25	Class	The attribute sent by the RADIUS server to the NAS in an Access-Accept or CoA and is sent unmodified by the NAS to the Accounting server as part of the Accounting-Request packet. Strings with a length longer than the defined Limits are accepted but truncated to this boundary. Only first 64B are stored in the CF persistency file.
30	Called-Station-Id	Allows the NAS to send in an Access Request and/or Accounting Request information with respect to the user called. Attribute is omitted in authentication/accounting via: **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute no called-station-id**. Supported applications: • LNS: The content is the string passed in the [21] Called Number AVP of the L2TP ICRQ message. • EAP authentication on WLAN Gateway: transparently forwarded as received in EAP authentication or Accounting messages from the AP

Table 50: Enhanced Subscriber Management Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
31	Calling-Station-Id	Allows the NAS to send unique information identifying the user who requested the service. This format is driven by configuration (**configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute calling-station-id** <**llid**|**mac**|**remote-id**|**sap-id**|**sap-string**>). The LLID (logical link identifier) is the mapping from a physical to logical identification of a subscriber line and supplied by a RADIUS llid-server. The sap-string maps to **configure service** <*service-id*> **subscriber-interface** <*ip-int-name*> **group-interface** <*ip-int-name*> **sap** <*sap-id*> **calling-station-id** <sap-string>. A [31] Calling-Station-Id attribute value longer than the allowed maximum is treated as a setup failure. The attribute is omitted in authentication/accounting via **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute no calling-station-id**.
32	NAS-Identifier	A string (**configure system name** <*system-name*>) identifying the NAS originating the Authentication or Accounting requests and sent when nas-identifier is included for the corresponding application: **configure subscriber-mgmt authentication-policy** (ESM authentication), **configure subscriber-mgmt radius-accounting-policy** (ESM accounting), **configure aaa isa-radius-policy** (LSN accounting, WLAN-GW soft-gre) and **configure aaa l2tp-accounting-policy** (L2TP accounting).
40	Acct-Status-Type	Indicates whether this Accounting-Request marks the beginning of the user service (Start) or the end (Stop) or reports interim updates.
41	Acct-Delay-Time	Indicates how many seconds the client has been trying to send this accounting record for. This attribute is included with value 0 in all initial accounting messages. Attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute no acct-delay-time**.
42	Acct-Input-Octets	Indicates how many octets have been received from the user over the course of this service being provided and included when standard accounting attributes are configured. (**configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute std-acct-attributes**). [52] Acct-Input-Gigawords indicates how many times (if greater than zero) the [42] Acct-Input-Octets counter has wrapped around 2^32.
43	Acct-Output-Octets	Indicates how many octets have been send from the user over the course of this service being provided and included when standard accounting attributes are configured. (**configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute std-acct-attributes**). [53] Acct-Output-Gigawords indicates how many times (if greater than zero) the [43] Acct-Output-Octets counter has wrapped around 2^32.

Table 50: Enhanced Subscriber Management Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
44	Acct-Session-Id	A unique identifier that represents a subscriber host, a set of subscriber hosts that belong to the same queue-instance or a set of hosts that belong to a PPPoE session. The attribute can have a fixed 22 byte hexadecimal number format or a variable length description format (**configure subscriber-mgmt radius-accounting-policy** <*policy-name*> **session-id-format {number**|**description**}). This attribute (in number format) can be used as CoA or Disconnect Message key to target the hosts or session.
45	Acct-Authentic	Indicates how the user was authenticated. Attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute no acct-authentic**.
46	Acct-Session-Time	Reports the elapsed time in seconds over the course of this service being provided.
47	Acct-Input-Packets	Indicates how many packets have been received from the user over the course of this service being provided and included when standard accounting attributes are configured. (**configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute std-acct-attributes**). There is no overflow attribute when attribute wraps around 2^32.
48	Acct-Output-Packets	Indicates how many packets have been send to the user over the course of this service being provided and included when standard accounting attributes are configured. (**configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute std-acct-attributes**). There is no overflow attribute when attribute wraps around 2^32.
49	Acct-Terminate-Cause	Indicates how the subscriber host or queue-instance or PPPoE session was terminated
50	Acct-Multi-Session-Id	A unique Accounting ID that links together multiple related accounting sessions. Each linked accounting session has a unique [44] Acct-Session-Id and the same [50] Acct-Multi-Session-Id. This attribute is not sent if only queue-instance accounting mode is enabled. The attribute can have a fixed 22 byte hexadecimal number format or a variable length description format (**configure subscriber-mgmt radius-accounting-policy** <*policy-name*> **session-id-format** {**number**|**description**}).
52	Acct-Input-Gigawords	Indicates how many times (one or more) the [42] Acct-Input-Octets counter has wrapped around 2^32 in the course of delivering this service and send together with [42] Acct-Input-Octets, [43] Acct-Output-Octets and [53] Acct-Output-Gigawords when standard accounting attributes are configured. (**configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute std-acct-attributes**). The attribute is not sent when its value=0.

Table 50: Enhanced Subscriber Management Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
53	Acct-Output-Gigawords	Indicates how many times (one or more) the [43] Acct-Output-Octets counter has wrapped around 2^32 in the course of delivering this service and send together with [42] Acct-Input-Octets, [43] Acct-Output-Octets and [52] Acct-Input-Gigawords when standard accounting attributes are configured (**configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute std-acct-attributes**). The attribute is not sent when its value=0.
55	Event-Timestamp	Record the time that this event occurred on the NAS, in seconds since January 1, 1970 00:00 UTC
61	NAS-Port-Type	The type of the physical port of the NAS which is authenticating the user and value automatically determined from subscriber SAP encapsulation. It can be overruled by configuration. Included only if include-radius-attribute nas-port-type is added per application: **configure subscriber-mgmt authentication-policy** (ESM authentication), **configure subscriber-mgmt radius-accounting-policy** (ESM accounting), **configure aaa isa-radius-policy** (LSN accounting, WLAN-GW soft-gre) and **configure aaa l2tp-accounting-policy** (L2TP accounting). Checked for correctness if returned in CoA.
87	NAS-Port-Id	A text string which identifies the physical/logical port of the NAS which is authenticating the user and/or reported for accounting. Attribute is also used in CoA and Disconnect Message (part of the user identification-key). The nas-port-id for physical ports usually contains <slot>/<mda>/<port>/<vlan|vpi>.<vlan|vci>. The physical port can have an optional prefix-string (max 8 chars) and suffix-string (max 64 chars) added for Accounting (**configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute nas-port-id** [**prefix-string** <*string*>] [**suffix** <**circuit-id**|**remote-id**>]). For logical access circuits (LNS) the nas-port-id is a fixed concatenation (delimiter #) of routing instance, tunnel-server-endpoint, tunnel-client-endpoint, local-tunnel-id, remote-tunnel-id, local-session-id, remote-session-id and call sequence number.
95	NAS-IPv6-Address	The identifying IP Address of the NAS requesting the Authentication or Accounting. Included when the RADIUS server is reachable via IPv6. The address is determined by the routing instance through which the RADIUS server can be reached: “Management” — The active ipv6 address in the Boot Options File (bof address <ipv6-address>) “Base” or “VPRN” — The ipv6 address of the system interface (configure router interface system ipv6 address <ipv6-address>). The address can be overwritten with the configured ipv6-source-address (**configure aaa radius-server-policy** <*policy-name*> **servers ipv6-source-address** <*ipv6-address*>).

Table 50: Enhanced Subscriber Management Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
96	Framed-Interface-Id	Contains the IPv6 interface ID from the user. The attribute can optionally be included in Accounting messages (**configure subscriber-mgmt radius-accounting-policy include-radius-attribute framed-interface-id**). The Framed-Interface-Id attribute is not sent in RADIUS Authentication and silently ignored in RADIUS Accept.
97	Framed-IPv6-Prefix	ipv6-prefix/prefix-length to be configured via SLAAC (Router Advertisement) to the WAN side of the user. Any non /64 prefix-length for SLAAC host creation is treated as a session setup failure for this host. This attribute is an alternative to [100] Framed-IPv6-Pool and [26-6527-99] Alc-IPv6-Address, which assigns IPv6 addressing to the wan-side of a host via DHCPv6 IA-NA. Attribute is also used in CoA and Disconnect Message (part of the ESM or AA user identification-key). Attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute no framed-ipv6-prefix**.
99	Framed-IPv6-Route	The routing information (IPv6 managed route) to be configured on the NAS for a v6 wan-host (IPoE or PPPoE) that operates as a router. Valid RADIUS learned managed routes can be included in RADIUS accounting messages with following configuration: **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute framed-ipv6-route**. Associated managed routes for an instantiated routed subscriber host are included in RADIUS accounting messages independent of the state of the managed route (Installed, Shadowed or HostInactive). In case of a PPP session, when a Framed-IPv6-Route is available while the corresponding routed subscriber host is not yet instantiated, the managed route is in the state “notYetInstalled” and will not be included in RADIUS accounting messages.
123	Delegated-IPv6-Prefix	Attribute that carries the Prefix (ipv6-prefix/prefix-length) to be delegated via DHCPv6 (IA-PD) for the LAN side of the user (IPoE, PPPoE). Maps to DHCPv6 option IA-PD [25] sub-option IA-Prefix [26] Prefix. An exact Delegated-prefix-Length [DPL] match with **configure service** <*service-id*> **subscriber-interface** <*ip-int-name*> **ipv6 delegated-prefix-length** [48..64] is required with the received attribute prefix-length unless a variable DPL is configured (**configure service** <*service-id*> **subscriber-interface** <*ip-int-name*> **ipv6 delegated-prefix-length variable**).In the latter case we support multiple hosts for the same group-interface having different prefix-length [48..64] per host. Simultaneous returned attributes [123] Delegated-IPv6-Prefix and [26-6527-131] Alc-Delegated-IPv6-Pool are handled as host setup failures. Attribute is also used in CoA and Disconnect Message (part of the ESM or AA user identification-key). Attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute no delegated-ipv6-prefix**.

Table 50: Enhanced Subscriber Management Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
26-3561-1	Agent-Circuit-Id	Information describing the subscriber agent circuit identifier corresponding to the logical access loop port of the Access Node/DSLAM from which a subscriber's requests are initiated. Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute circuit-id**.
26-3561-2	Agent-Remote-Id	An operator-specific, statically configured string that uniquely identifies the subscriber on the associated access loop of the Access Node/DSLAM. Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute remote-id**.
26-3561-129	Actual-Data-Rate-Upstream	Actual upstream train rate rate (coded in bits per second) of a subscriber's synchronized DSL link and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-3561-130	Actual-Data-Rate-Downstream	Actual downstream train rate (coded in bits per second) of a subscriber's synchronized DSL link and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-3561-131	Minimum-Data-Rate-Upstream	The subscriber's operator-configured minimum upstream data rate (coded in bits per second) and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-3561-132	Minimum-Data-Rate-Downstream	The subscriber's operator-configured minimum downstream data rate (coded in bits per second) and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-3561-133	Attainable-Data-Rate-Upstream	The subscriber's attainable upstream data rate (coded in bits per second) and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-3561-134	Attainable-Data-Rate-Downstream	The subscriber's attainable downstream data rate (coded in bits per second) and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.

Table 50: Enhanced Subscriber Management Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
26-3561-135	Maximum-Data-Rate-Upstream	The subscriber's maximum upstream data rate (coded in bits per second), as configured by the operator and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy**/**radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-3561-136	Maximum-Data-Rate-Downstream	The subscriber's maximum downstream data rate (coded in bits per second), as configured by the operator and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy**/**radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-3561-137	Minimum-Data-Rate-Upstream-Low-Power	The subscriber's minimum upstream data rate (coded in bits per second) in low power state, as configured by the operator and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy**/**radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-3561-138	Minimum-Data-Rate-Downstream-Low-Power	The subscriber's minimum downstream data rate (coded in bits per second) in low power state, as configured by the operator and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy**/**radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options.**
26-3561-139	Maximum-Interleaving-Delay-Upstream	The subscriber's maximum one-way upstream interleaving delay in milliseconds, as configured by the operator and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy**/**radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-3561-140	Actual-Interleaving-Delay-Upstream	The subscriber's actual one-way upstream interleaving delay in milliseconds and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy**/**radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-3561-141	Maximum-Interleaving-Delay-Downstream	The subscriber's maximum one-way downstream interleaving delay in milliseconds, as configured by the operator and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy**/**radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.

Table 50: Enhanced Subscriber Management Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
26-3561-142	Actual-Interleaving-Delay-Downstream	The subscriber's actual one-way downstream interleaving delay in milliseconds and maps to values received during PPPoE discovery (tag 0x0105) or DHCP (opt-82). Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy**/**radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-3561-144	Access-Loop-Encapsulation	The last mile encapsulation used by the subscriber on the DSL access loop and maps to values received during PPPoE discovery Tags (tag 0x0105) or DHCP Tags (opt-82). Attribute is included/excluded in RADIUS/Accounting-Request based on **configure subscriber-mgmt authentication-policy**/ **radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**. Last mile encapsulation information can be used to adjust automatically the egress aggregate rate for this subscriber. Pre-configured encapsulation types are used if PPP/IPoE access loop information (tags) is not available (**configure subscriber-mgmt sub-profile** <*subscriber-profile-name*> **egress encap-offset** <*type*> or **configure subscriber-mgmt local-user-db** <*local-user-db-name*> **ppp host access-loop encap-offset** <*type*>). [26-6527-133] Alc-Access-Loop-Encap-Offset when returned in Access-Accept is taken into account (overrules received tags and pre-configured encapsulation types) for ALE adjust (last mile aware shaping) but is not reflected in access-loop-options send to RADIUS. Alc-Access-Loop-Encap from ANCP are currently not taken into account for ALE adjust.
26-3561-254	IWF-Session	The presence of this Attribute indicates that the IWF has been performed with respect to the subscriber's session. IWF is utilized to enable the carriage of PPP over ATM (PPPoA) traffic over PPPoE. The Access Node inserts the PPPoE Tag 0x0105, vendor-id 0x0de9 with sub-option code 0xFE, length field is set to 0x00 into the PPPoE Discovery packets when it is performing an IWF functionality. Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy**/**radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.
26-6527-11	Alc-Subsc-ID-Str	A subscriber is a collection of subscriber-hosts (typically represented by IP-MAC combination) and is uniquely identified by a subscriber string. Subscriber-hosts queues/policers belonging to the same subscriber (residing on the same forwarding complex) can be treated under one aggregate scheduling QoS mechanism. Fallback to pre-configured values if attribute is omitted. Attribute values longer than the allowed string value are treated as setup failures. Can be used as key in CoA and Disconnect Message. Attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute no subscriber-id**.

Table 50: Enhanced Subscriber Management Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-12	Alc-Subsc-Prof-Str	The subscriber profile is a template which contains settings (accounting, igmp, HQoS, etc.) which are applicable to all hosts belonging to the same subscriber were [26-6527-12] Alc-Subsc-Prof-Str is the string that maps (**configure subscriber-mgmt sub-ident-policy sub-profile-m**ap) to such an subscriber profile (**configure subscriber-mgmt sub-profile** <*subscriber-profile-name*>). Strings longer than the allowed maximum are treated as setup failures. Unreferenced strings (string does not map to a policy) are silently ignored and a fallback to pre-configured defaults is done. Attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute no sub-profile**.
26-6527-13	Alc-SLA-Prof-Str	The SLA profile is a template which contains settings (filter, QoS, host-limit...) which are applicable to individual hosts were [26-6527-13] Alc-SLA-Prof-Str is the string that maps (**configure subscriber-mgmt sub-ident-policy** <*sub-ident-policy-name*> **sla-profile-map**) to such a sla profile (**configure subscriber-mgmt sla-profile** <*sla-profile-name*>). Strings longer than the allowed maximum are treated as setup failures. Unreferenced strings (string does not map to a policy) are silently ignored and a fallback to pre-configured defaults is done. Attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute no sla-profile**.
26-6527-19	Alc-Acct-I-Inprof-Octets-64	Indicates how many queue|policer ingress forwarded bytes have been handled for this user over the course of this service being provided. • queue|policer stat-mode = *: Count in-profile bytes (IPv4 and IPv6) [26-6527-107] Alc-Acct-I-statmode VSA only included for policers • queue|policer stat-mode = v4-v6: Count IPv4 bytes (in- and out-of-profile) [26-6527-107] Alc-Acct-I-statmode VSA included for policers and queues with value v4-v6 The attribute is included when detailed queue/policer statistics VSAs are configured. (**configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute detailed-acct-attributes**).

Table 50: Enhanced Subscriber Management Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-20	Alc-Acct-I-Outprof-Octets-64	Indicates how many queue|policer ingress forwarded bytes have been handled for this user over the course of this service being provided. • queue|policer stat-mode = *: Count out-of-profile bytes (IPv4 and IPv6) [26-6527-107] Alc-Acct-I-statmode VSA only included for policers • queue|policer stat-mode = v4-v6: Count IPv6 bytes (in- and out-of-profile) [26-6527-107] Alc-Acct-I-statmode VSA included for policers and queues with value v4-v6 The attribute is included when detailed queue/policer statistics VSAs are configured. (**configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute detailed-acct-attributes**).
26-6527-21	Alc-Acct-O-Inprof-Octets-64	Indicates how many queue|policer egress forwarded bytes have been handled for this user over the course of this service being provided. • queue|policer stat-mode = *: Count in-profile bytes (IPv4 and IPv6) [26-6527-127] Alc-Acct-O-statmode VSA only included for policers • queue|policer stat-mode = v4-v6: Count IPv4 bytes (in- and out-of-profile) [26-6527-127] Alc-Acct-O-statmode VSA included for policers and queues with value v4-v6 The attribute is included when detailed queue/policer statistics VSAs are configured. (**configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute detailed-acct-attributes**).
26-6527-22	Alc-Acct-O-Outprof-Octets-64	Indicates how many queue|policer egress forwarded bytes have been handled for this user over the course of this service being provided. • queue|policer stat-mode = *: Count out-of-profile bytes (IPv4 and IPv6) [26-6527-127] Alc-Acct-O-statmode VSA only included for policers • queue|policer stat-mode = v4-v6: Count IPv6 bytes (in- and out-of-profile) [26-6527-127] Alc-Acct-O-statmode VSA included for policers and queues with value v4-v6 The attribute is included when detailed queue/policer statistics VSAs are configured. (**configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute detailed-acct-attributes**).

Table 50: Enhanced Subscriber Management Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-23	Alc-Acct-I-Inprof-Pkts-64	Indicates how many queue|policer ingress forwarded packets have been handled for this user over the course of this service being provided. • queue|policer stat-mode = *: Count in-profile packets (IPv4 and IPv6) [26-6527-107] Alc-Acct-I-statmode VSA only included for policers • queue|policer stat-mode = v4-v6: Count IPv4 packets (in- and out-of-profile) [26-6527-107] Alc-Acct-I-statmode VSA included for policers and queues with value v4-v6 The attribute is included when detailed queue/policer statistics VSAs are configured. (**configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute detailed-acct-attributes**).
26-6527-24	Alc-Acct-I-Outprof-Pkts-64	Indicates how many queue|policer ingress forwarded packets have been handled for this user over the course of this service being provided. • queue|policer stat-mode = *: Count out-of-profile packets (IPv4 and IPv6) [26-6527-107] Alc-Acct-I-statmode VSA only included for policers • queue|policer stat-mode = v4-v6: Count IPv6 packets (in- and out-of-profile) [26-6527-107] Alc-Acct-I-statmode VSA included for policers and queues with value v4-v6 The attribute is included when detailed queue/policer statistics VSAs are configured. (**configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute detailed-acct-attributes**).
26-6527-25	Alc-Acct-O-Inprof-Pkts-64	Indicates how many queue|policer egress forwarded packets have been handled for this user over the course of this service being provided. • queue|policer stat-mode = *: Count in-profile packets (IPv4 and IPv6) [26-6527-127] Alc-Acct-O-statmode VSA only included for policers • queue|policer stat-mode = v4-v6: Count IPv4 packets (in- and out-of-profile) [26-6527-127] Alc-Acct-O-statmode VSA included for policers and queues with value v4-v6 The attribute is included when detailed queue/policer statistics VSAs are configured. (**configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute detailed-acct-attributes**).

Table 50: Enhanced Subscriber Management Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-26	Alc-Acct-O-Outprof-Pkts-64	Indicates how many queue|policer egress forwarded packets have been handled for this user over the course of this service being provided. • queue|policer stat-mode = *: Count out-of-profile packets (IPv4 and IPv6) [26-6527-127] Alc-Acct-O-statmode VSA only included for policers • queue|policer stat-mode = v4-v6: Count IPv6 packets (in- and out-of-profile) [26-6527-127] Alc-Acct-O-statmode VSA included for policers and queues with value v4-v6 The attribute is included when detailed queue/policer statistics VSAs are configured. (**configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute detailed-acct-attributes**).
26-6527-27	Alc-Client-Hardware-Addr	The MAC address from a user that requests a service and included in CoA, Authentication or Accounting (**configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute mac-address**).
26-6527-39	Alc-Acct-OC-O-Inprof-Octets-64	HSMDA override counter: counts egress forwarded bytes: • no queue stat-mode: Count in-profile bytes (IPv4 and IPv6) [26-6527-127] Alc-Acct-O-statmode VSA not included • queue stat-mode = v4-v6: Count IPv4 bytes (in- and out-of-profile) [26-6527-127] Alc-Acct-O-statmode VSA included with value v4-v6 Up to eight hsmda- counter-override counters can be specified in CLI (**configure qos sap-egress** <*policy-id*> **prec**|**dscp**|**ip-criteria**|**ipv6-criteria**).
26-6527-40	Alc-Acct-OC-O-Outprof-Octets-64	HSMDA override counter: counts egress forwarded bytes: • no queue stat-mode: Count out-of-profile bytes (IPv4 and IPv6) [26-6527-127] Alc-Acct-O-statmode VSA not included • queue stat-mode = v4-v6: Count IPv6 bytes (in- and out-of-profile) [26-6527-127] Alc-Acct-O-statmode VSA included with value v4-v6 Up to eight hsmda- counter-override counters can be specified in CLI (**configure qos sap-egress** <*policy-id*> **prec**|**dscp**|**ip-criteria**|**ipv6-criteria**).

Table 50: Enhanced Subscriber Management Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-43	Alc-Acct-OC-O-Inprof-Pkts-64	HSMDA override counter: counts egress forwarded packets: • no queue stat-mode: Count in-profile packets (IPv4 and IPv6) [26-6527-127] Alc-Acct-O-statmode VSA not included • queue stat-mode = v4-v6: Count IPv4 packets (in- and out-of-profile) [26-6527-127] Alc-Acct-O-statmode VSA included with value v4-v6 Up to eight hsmda- counter-override counters can be specified in CLI (**configure qos sap-egress** <*policy-id*> **prec|dscp|ip-criteria|ipv6-criteria**).
26-6527-44	Alc-Acct-OC-O-Outprof-Pkts-64	HSMDA override counter: counts egress forwarded packets: • no queue stat-mode: Count out-of-profile packets (IPv4 and IPv6) [26-6527-127] Alc-Acct-O-statmode VSA not included • queue stat-mode = v4-v6: Count IPv6 packets (in- and out-of-profile) [26-6527-127] Alc-Acct-O-statmode VSA included with value v4-v6 Up to eight hsmda- counter-override counters can be specified in CLI (**configure qos sap-egress** <*policy-id*> **prec|dscp|ip-criteria|ipv6-criteria**).
26-6527-69	Alc-Acct-I-High-Octets-Drop_64	A customized record and provides the flexibility to reduce the volume of data generated, network operators can define the record that needs to be collected. This attribute is generated when **configure subscriber-mgmt radius-accounting-policy** <*name*> **custom-record queue** <*queue-id*> **i-counters high-octets-discarded-count** is enabled. Customized records are available for queues, not for policers. Counts ingress dropped bytes: • no queue stat-mode: Count high-priority bytes (IPv4 and IPv6) [26-6527-107] Alc-Acct-I-statmode VSA not included • queue stat-mode = v4-v6: Count IPv4 bytes (high- and low-priority) [26-6527-107] Alc-Acct-I-statmode VSA included with value v4-v6

Table 50: Enhanced Subscriber Management Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-70	Alc-Acct-I-Low-Octets-Drop_64	A customized record and provides the flexibility to reduce the volume of data generated, network operators can define the record that needs to be collected. This attribute is generated when **configure subscriber-mgmt radius-accounting-policy** <*name*> **custom-record queue** <*queue-id*> **i-counters low-octets-discarded-count** is enabled. Customized records are available for queues, not for policers. Counts ingress dropped bytes: • no queue stat-mode: Count low-priority bytes (IPv4 and IPv6) [26-6527-107] Alc-Acct-I-statmode VSA not included • queue stat-mode = v4-v6: Count IPv6 bytes (high- and low-priority) [26-6527-107] Alc-Acct-I-statmode VSA included with value v4-v6
26-6527-71	Alc-Acct-I-High-Pack-Drop_64	A customized record and provides the flexibility to reduce the volume of data generated, network operators can define the record that needs to be collected. This attribute is generated when **configure subscriber-mgmt radius-accounting-policy** <*name*> **custom-record queue** <*queue-id*> **i-counters high-packets-discarded-count** is enabled. Customized records are available for queues, not for policers. Counts ingress dropped packets: • no queue stat-mode: Count high-priority packets (IPv4 and IPv6) [26-6527-107] Alc-Acct-I-statmode VSA not included • queue stat-mode = v4-v6: Count IPv4 packets (high- and low-priority) [26-6527-107] Alc-Acct-I-statmode VSA included with value v4-v6
26-6527-72	Alc-Acct-I-Low-Pack-Drop_64	A customized record and provides the flexibility to reduce the volume of data generated, network operators can define the record that needs to be collected. This attribute is generated when **configure subscriber-mgmt radius-accounting-policy** <*name*> **custom-record queue** <*queue-id*> **i-counters low-packets-discarded-count** is enabled. Customized records are available for queues, not for policers. Counts ingress dropped packets: • no queue stat-mode: Count low-priority packets (IPv4 and IPv6) [26-6527-107] Alc-Acct-I-statmode VSA not included • queue stat-mode = v4-v6: Count IPv6 packets (high- and low-priority) [26-6527-107] Alc-Acct-I-statmode VSA included with value v4-v6

Table 50: Enhanced Subscriber Management Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-73	Alc-Acct-I-High-Octets-Offer_64	A customized record and provides the flexibility to reduce the volume of data generated, network operators can define the record that needs to be collected. This attribute is generated when **configure subscriber-mgmt radius-accounting-policy** <*name*> **custom-record queue** <*queue-id*> **i-counters high-octets-offered-count** is enabled. Customized records are available for queues, not for policers. Counts ingress high priority offered bytes (IPv4 and IPv6); also when queue stat-mode = v4-v6.
26-6527-74	Alc-Acct-I-Low-Octets-Offer_64	A customized record and provides the flexibility to reduce the volume of data generated, network operators can define the record that needs to be collected. This attribute is generated when **configure subscriber-mgmt radius-accounting-policy** <*name*> **custom-record queue** <*queue-id*> **i-counters low-octets-offered-count** is enabled. Customized records are available for queues, not for policers. Counts ingress low priority offered bytes (IPv4 and IPv6); also when queue stat-mode = v4-v6.
26-6527-75	Alc-Acct-I-High-Pack-Offer_64	A customized record and provides the flexibility to reduce the volume of data generated, network operators can define the record that needs to be collected. This attribute is generated when **configure subscriber-mgmt radius-accounting-policy** <*name*> **custom-record queue** <*queue-id*> **i-counters high-packets-offered-count** is enabled. Customized records are available for queues, not for policers. Counts ingress high priority offered packets (IPv4 and IPv6); also when queue stat-mode = v4-v6.
26-6527-76	Alc-Acct-I-Low-Pack-Offer_64	A customized record and provides the flexibility to reduce the volume of data generated, network operators can define the record that needs to be collected. This attribute is generated when **configure subscriber-mgmt radius-accounting-policy** <*name*> **custom-record queue** <*queue-id*> **i-counters low-packets-offered-count** is enabled. Customized records are available for queues, not for policers. Counts ingress low priority offered packets (IPv4 and IPv6); also when queue stat-mode = v4-v6.
26-6527-77	Alc-Acct-I-Unc-Octets-Offer_64	A customized record and provides the flexibility to reduce the volume of data generated, network operators can define the record that needs to be collected. This attribute is generated when **configure subscriber-mgmt radius-accounting-policy** <*name*> **custom-record queue** <*queue-id*> **i-counters uncolored-octets-offered-count** is enabled.Customized records are available for queues, not for policers. Counts ingress uncolored offered bytes (IPv4 and IPv6); also when queue stat-mode = v4-v6.

Table 50: Enhanced Subscriber Management Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-78	Alc-Acct-I-Unc-Pack-Offer_64	A customized record and provides the flexibility to reduce the volume of data generated, network operators can define the record that needs to be collected. This attribute is generated when **configure subscriber-mgmt radius-accounting-policy** <*name*> **custom-record queue** <*queue-id*> **i-counters uncolored-packets-offered-count** is enabled. Customized records are available for queues, not for policers. Counts ingress uncolored offered packets (IPv4 and IPv6); also when queue stat-mode = v4-v6
26-6527-81	Alc-Acct-O-Inprof-Pack-Drop_64	A customized record and provides the flexibility to reduce the volume of data generated, network operators can define the record that needs to be collected. This attribute is generated when **configure subscriber-mgmt radius-accounting-policy** <*name*> **custom-record queue** <*queue-id*> **e-counters in-profile-packets-discarded-count** is enabled. Customized records are available for queues, not for policers. Counts egress dropped packets: • no queue stat-mode: Count in-profile packets (IPv4 and IPv6) [26-6527-127] Alc-Acct-O-statmode VSA not included • queue stat-mode = v4-v6: Count IPv4 packets (in- and out-of-profile) [26-6527-127] Alc-Acct-O-statmode VSA included with value v4-v6.
26-6527-82	Alc-Acct-O-Outprof-Pack-Drop_64	A customized record and provides the flexibility to reduce the volume of data generated, network operators can define the record that needs to be collected. This attribute is generated when configure subscriber-mgmt radius-accounting-policy <*name*> custom-record queue <queue-id> e-counters out-profile-packets-discarded-count is enabled. Customized records are available for queues, not for policers. Counts egress dropped packets: • no queue stat-mode: Count out-of-profile packets (IPv4 and IPv6) [26-6527-127] Alc-Acct-O-statmode VSA not included • queue stat-mode = v4-v6: Count IPv6 packets (in- and out-of-profile) [26-6527-127] Alc-Acct-O-statmode VSA included with value v4-v6.

Table 50: Enhanced Subscriber Management Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-83	Alc-Acct-O-Inprof-Octs-Drop_64	A customized record and provides the flexibility to reduce the volume of data generated, network operators can define the record that needs to be collected. This attribute is generated when **configure subscriber-mgmt radius-accounting-policy** <*name*> **custom-record queue** <*queue-id*> **e-counters in-profile-octets-forwarded-count** is enabled. Customized records are available for queues, not for policers. Counts egress dropped bytes: • no queue stat-mode: Count in-profile bytes (IPv4 and IPv6) [26-6527-127] Alc-Acct-O-statmode VSA not included • queue stat-mode = v4-v6: Count IPv4 bytes (in- and out-of-profile) [26-6527-127] Alc-Acct-O-statmode VSA included with value v4-v6.
26-6527-84	Alc-Acct-O-Outprof-Octs-Drop_64	A customized record and provides the flexibility to reduce the volume of data generated, network operators can define the record that needs to be collected. This attribute is generated when **configure subscriber-mgmt radius-accounting-policy** <*name*> **custom-record queue <***queue-id***> e-counters out-profile-octets-discarded-count** is enabled. Customized records are available for queues, not for policers. Counts egress dropped bytes: • no queue stat-mode: Count out-of-profile bytes (IPv4 and IPv6) [26-6527-127] Alc-Acct-O-statmode VSA not included • queue stat-mode = v4-v6: Count IPv6 bytes (in- and out-of-profile) [26-6527-127] Alc-Acct-O-statmode VSA included with value v4-v6.
26-6527-91	Alc-Acct-OC-O-Inpr-Pack-Drop_64	HSMDA override counter: counts egress dropped packets • no queue stat-mode: Count in-profile packets (IPv4 and IPv6) [26-6527-127] Alc-Acct-O-statmode VSA not included • queue stat-mode = v4-v6: Count IPv4 packets (in- and out-of-profile) [26-6527-127] Alc-Acct-O-statmode VSA included with value v4-v6 Up to eight hsmda-counter-override counters can be specified in CLI (**configure qos sap- egress** <*policy-id*> **prec**|**dscp**|**ip-criteria**|**ipv6-criteria**).

Table 50: Enhanced Subscriber Management Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-92	Alc-Acct-OC-O-Outpr-Pack-Drop_64	HSMDA override counter: counts egress dropped packets • no queue stat-mode: Count out-of-profile packets (IPv4 and IPv6) [26-6527-127] Alc-Acct-O-statmode VSA not included • queue stat-mode = v4-v6: Count IPv6 packets (in- and out-of-profile) [26-6527-127] Alc-Acct-O-statmode VSA included with value v4-v6 Up to eight hsmda-counter-override counters can be specified in CLI (**configure qos sap- egress** <*policy-id*> **prec**|**dscp**|**ip-criteria**|**ipv6-criteria**).
26-6527-93	Alc-Acct-OC-O-Inpr-Octs-Drop_64	HSMDA override counter: counts egress dropped bytes • no queue stat-mode: Count in-profile bytes (IPv4 and IPv6) [26-6527-127] Alc-Acct-O-statmode VSA not included • queue stat-mode = v4-v6: Count IPv4 bytes (in- and out-of-profile) [26-6527-127] Alc-Acct-O-statmode VSA included with value v4-v6 Up to eight hsmda-counter-override counters can be specified in CLI (**configure qos sap- egress** <*policy-id*> **prec**|**dscp**|**ip-criteria**|**ipv6-criteria**).
26-6527-94	Alc-Acct-OC-O-Outpr-Octs-Drop_64	HSMDA override counter: counts egress dropped bytes • no queue stat-mode: Count out-of-profile bytes (IPv4 and IPv6) [26-6527-127] Alc-Acct-O-statmode VSA not included • queue stat-mode = v4-v6: Count IPv6 bytes (in- and out-of-profile) [26-6527-127] Alc-Acct-O-statmode VSA included with value v4-v6 Up to eight hsmda-counter-override counters can be specified in CLI (**configure qos sap- egress** <*policy-id*> **prec**|**dscp**|**ip-criteria**|**ipv6-criteria**).
26-6527-99	Alc-Ipv6-Address	The ipv6 address to be configured to the WAN side of the user (IPoE,PPPoE) via DHCPv6 (IA-NA). Maps to DHCPv6 option IA-NA[3] sub-option IA-Address[5] address. This attribute is an alternative to [97] Framed-IPv6-Prefix and [100] Framed-IPv6-Pool, which also assigns IPv6 addressing to the wan-side of a host via SLAAC or DHCPv6 IA-NA. Attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute no ipv6-address**.

Table 50: Enhanced Subscriber Management Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-107	Alc-Acct-I-statmode	Identifies what ingress counters the operator wishes to maintain for the policer and defined by **configure qos sap-ingress** <*policy-id*> **policer** <*policer-id*> **stat-mode** <*stat-mode*>. The default stat-mode is minimal and the current stats-modes are: no-stats, minimal, offered-profile-no-cir, offered-priority-no-cir, offered-profile-cir, offered-priority-cir, offered-total-cir, offered-limited-profile-cir, offered-profile-capped-cir and offered-limited-capped-cir. For both policers and queues, the ingress stat-mode can be configured to v4-v6 at the sla-profile or sub-profile (hsmda) CLI context. For example: **configure subscriber-mgmt sla-profile** <*sla-profile-name*> **ingress qos** <*policy-id*> **queue** <*queue-id*> **stat-mode v4-v6** With ingress stat-mode v4-v6: • Ingress forwarded/dropped counters are reporting IPv4 counters in the in-profile attributes and IPv6 counters in the out-of-profile attributes. • The Alc-Acct-I-statmode VSA is included with value v4-v6 for both queues and/or policers.
26-6527-108	Alc-Acct-I-Hiprio-Octets_64	Policer-specific counter. Indicates how many policer ingress-high-priority-forwarded-bytes have been handled for this user over the course of this service being provided. The attribute is included in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute detailed-acct-attributes** for specific policer stat-mode only.
26-6527-109	Alc-Acct-I-Lowprio-Octets_64	Policer-specific counter. Indicates how many policer ingress-low-priority-forwarded-bytes have been handled for this user over the course of this service being provided. The attribute is included in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute detailed-acct-attributes** for specific policer stat-mode only.
26-6527-110	Alc-Acct-O-Hiprio-Octets_64	Policer-specific counter. Indicates how many policer egress-high-priority-forwarded-bytes have been handled for this user over the course of this service being provided. The attribute is included in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute detailed-acct-attributes** for specific policer stat-mode only.
26-6527-111	Alc-Acct-O-Lowprio-Octets_64	Policer-specific counter. Indicates how many policer egress-low-priority-forwarded-bytes have been handled for this user over the course of this service being provided. The attribute is included in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute detailed-acct-attributes** for specific policer stat-mode only.
26-6527-112	Alc-Acct-I-Hiprio-Packets_64	Policer-specific counter. Indicates how many policer ingress-high-priority-forwarded-packets have been handled for this user over the course of this service being provided. The attribute is included in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute detailed-acct-attributes** for specific policer stat-mode only.

Table 50: Enhanced Subscriber Management Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-113	Alc-Acct-I-Lowprio-Packets_64	Policer-specific counter. Indicates how many policer ingress-low-priority-forwarded-packets have been handled for this user over the course of this service being provided. The attribute is included in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute detailed-acct-attributes** for specific policer stat-mode only.
26-6527-114	Alc-Acct-O-Hiprio-Packets_64	Policer-specific counter. Indicates how many policer egress-high-priority-forwarded-packets have been handled for this user over the course of this service being provided. The attribute is included in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute detailed-acct-attributes** for specific policer stat-mode only.
26-6527-115	Alc-Acct-O-Lowprio-Packets_64	Policer-specific counter. ndicates how many policer egress-low-priority-forwarded-packets have been handled for this user over the course of this service being provided. The attribute is included in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute detailed-acct-attributes** for specific policer stat-mode only.
26-6527-116	Alc-Acct-I-All-Octets_64	Policer-specific counter. Indicates how many policer ingress-forwarded-bytes have been handled for this user over the course of this service being provided. The attribute is included in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute detailed-acct-attributes** for specific policer stat-mode only.
26-6527-117	Alc-Acct-O-All-Octets_64	Policer-specific counter. Indicates how many policer egress-forwarded-bytes have been handled for this user over the course of this service being provided. The attribute is included in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute detailed-acct-attributes** for specific policer stat-mode only.
26-6527-118	Alc-Acct-I-All-Packets_64	Policer-specific counter. Indicates how many policer ingress-forwarded-packets have been handled for this user over the course of this service being provided. The attribute is included in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute detailed-acct-attributes** for specific policer stat-mode only.
26-6527-119	Alc-Acct-O-All-Packets_64	Policer-specific counter. Indicates how many policer egress-forwarded-packets have been handled for this user over the course of this service being provided. The attribute is included in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute detailed-acct-attributes** for specific policer stat-mode only.

Table 50: Enhanced Subscriber Management Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-121	Alc-Nat-Port-Range	Holds for the NAT user his public outside ipv4 address, his assigned outside public port range and the outside routing instance. For LSN accounting, the attribute is sent when port-range-block is included under **configure aaa isa-radius-policy**. The attribute is also sent for ESM subscriber accounting if NAT is enabled and if configured in **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute nat-port-range**.
26-6527-127	Alc-Acct-O-statmode	Identifies what egress counters the operator wishes to maintain for the policer and defined by **configure qos sap-egress** <*policy-id*> **policer** <*policer-id*> **stat-mode** <*stat-mode*>. The default stat-mode is minimal and the current stats-modes are: no-stats, minimal, offered-profile-no-cir, offered-profile-cir, offered-total-cir, offered-limited-capped-cir and offered-profile-capped-cir For both policers and queues, the egress stat-mode can be configured to v4-v6 at the sla-profile or sub-profile (hsmda queues only) CLI context. For example: **configure subscriber-mgmt sla-profile** <*sla-profile-name*> **egress qos** <*policy-id*> **queue** <*queue-id*> **stat-mode v4-v6** With egress stat-mode v4-v6: • Egress forwarded/dropped counters are reporting IPv4 counters in the in-profile attributes and IPv6 counters in the out-of-profile attributes. • The Alc-Acct-O-statmode VSA is included with value v4-v6 for both queues and/or policers.
26-6527-148	Alc-RSSI	Received Signal Strength Indication. Used in conjunction with the radius-proxy track-accounting feature. When the radius-proxy receives this attribute in an accounting message, it will be copied into the DHCP lease state and echoed by the SROS accounting.
26-6527-163	Alc-Acct-Triggered-Reason	A reason attribute included in Acct-Interim messages to specify the reason for the interim update. Attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute no alc-acct-triggered-reason**.
26-6527-175	Alc-DSL-Line-State	Status of the DSL line obtained via ANCP can be one of three value: SHOWTIME (the modem is ready to transfer data), IDLE (line is idle) or SILENT (line is silent). Attribute is included/excluded based on "configure subscriber-mgmt authentication-policy/radius-accounting-policy <name> include-radius-attribute access-loop-options".
26-6527-176	Alc-DSL-Type	Type of the DSL line (ADSL1, ADSL2, ADSL2PLUS, VDSL1, VDSL2, SDSL, other) obtained via ANCP. Attribute is included/excluded based on **configure subscriber-mgmt authentication-policy/radius-accounting-policy** <*name*> **include-radius-attribute access-loop-options**.

Table 50: Enhanced Subscriber Management Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-194	Alc-IPv6-Acct-Input-Packets	Aggregate of all ingress forwarded IPv6 packet counters for policers and queues that have stat-mode v4-v6 enabled (for example: **configure subscriber-mgmt sla-profile** <*sla-profile-name*> **ingress qos** <*policy-id*> **queue**|**policer** <*id*> **stat-mode v4-v6**). Included when IPv6 aggregated accounting attributes are configured. (**configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute v6-aggregate-stats**). There is no overflow attribute when counter wraps around 2^32.
26-6527-195	Alc-IPv6-Acct-Input-Octets	Aggregate of all ingress forwarded IPv6 octet counters for policers and queues that have stat-mode v4-v6 enabled (for example: **configure subscriber-mgmt sla-profile** <*sla-profile-name*> **ingress qos** <*policy-id*> **queue**|**policer** <*id*> **stat-mode v4-v6**). Included when IPv6 aggregated accounting attributes are configured. (**configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute v6-aggregate-stats**). [26-6527-196] Alc-IPv6-Acct-Input-Gigawords indicates how many times (if greater than zero) this counter has wrapped around 2^32.
26-6527-196	Alc-IPv6-Acct-Input-GigaWords	Indicates how many times (one or more) the [26-6527-195] Alc-IPv6-Acct-Input-Octets counter has wrapped around 2^32 in the course of delivering this service. The attribute is not sent when its value equals zero. Included when IPv6 aggregated accounting attributes are configured. (**configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute v6-aggregate-stats**).
26-6527-197	Alc-IPv6-Acct-Output-Packets	Aggregate of all egress forwarded IPv6 packet counters for policers and queues that have stat-mode v4-v6 enabled (for example: **configure subscriber-mgmt sla-profile** <*sla-profile-name*> **egress qos** <*policy-id*> **queue**|**policer** <*id*> **stat-mode v4-v6**). Included when IPv6 aggregated accounting attributes are configured. (**configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute v6-aggregate-stats**). There is no overflow attribute when counter wraps around 2^32.
26-6527-198	Alc-IPv6-Acct-Output-Octets	Aggregate of all egress forwarded IPv6 octet counters for policers and queues that have stat-mode v4-v6 enabled (for example: **configure subscriber-mgmt sla-profile** <*sla-profile-name*> **egress qos** <*policy-id*> **queue**|**policer** <*id*> **stat-mode v4-v6**). Included when IPv6 aggregated accounting attributes are configured. (**configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute v6-aggregate-stats**). [26-6527-199] Alc-IPv6-Acct-Output-Gigawords indicates how many times (if greater than zero) this counter has wrapped around 2^32.

Table 50: Enhanced Subscriber Management Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-199	Alc-IPv6-Acct-Output-Gigawords	Indicates how many times (one or more) the [26-6527-198] Alc-IPv6-Acct-Output-Octets counter has wrapped around 2^32 in the course of delivering this service. The attribute is not sent when its value equals zero. Included when IPv6 aggregated accounting attributes are configured. (**configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute v6-aggregate-stats**).
26-25053-2	Ruckus-Sta-RSSI	Received Signal Strength Indication. Used in conjunction with the radius-proxy track-accounting feature. When the radius-proxy receives this attribute in an accounting message, it will be copied into the DHCP lease state and echoed by the SROS accounting.

Table 51: Enhanced Subscriber Management Accounting (limits)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
1	User-Name	string	253 chars	The format depends on authentication method and configuration For example: User-Name user1@domain1.com
4	NAS-IP-Address	ipaddr	4 Bytes	# ip-address For example: NAS-IP-Address = 192.0.2.1
5	NAS-Port	integer	4 Bytes	nas-port <binary-spec> <binary-spec> = <bit-specification> <binary-spec> <bit-specification> = 0 | 1 | <bit-origin> <bit-origin> = *<number-of-bits><origin> <number-of-bits> = [1..32] <origin> = o (outer VLAN ID), i (inner VLAN ID), s (slot number), m (MDA number), p (port number or lag-id), v (ATM VPI), c (ATM VCI) For example: # configured nas-port *12o*10i*3s*2m*5p for SAP 2/2/4:221.7 corresponds to 000011011101 0000000111 010 10 00100 NAS-Port = 231742788
6	Service-Type	integer	2 (mandatory value)	PPPoE and PPPoL2TP hosts only For example: Service-Type = Framed-User
7	Framed-Protocol	integer	1 (fixed value)	PPPoE and PPPoL2TP hosts only For example: Service-Type = PPP
8	Framed-IP-Address	ipaddr	4 Bytes	For example: # ip-address 10.11.12.13 Framed-IP-Address 0a0b0c0d
9	Framed-IP-Netmask	ipaddr	4 Bytes	For example: Framed-IP-Netmask = 255.255.255.255 #PPPoE residential Framed-IP-Netmask = 255.255.255.0 #PPPoE Business with IPCP option 144 support Framed-IP-Netmask = 255.255.255.0 # IPoE

Table 51: Enhanced Subscriber Management Accounting (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
22	Framed-Route	string	max. 16 Framed-Routes	<ip-prefix>/<prefix-length> <space> 0.0.0.0 <space> <metric> [<space> tag <space> <tag-value>] <space> pref <space> <preference-value>” The gateway address is always reported as "0.0.0.0", representing the host ip. For example: Framed-Route = "192.168.1.0/24 0.0.0.0 0 pref 0" corresponds with a managed route with default metrics (metric=0, no tag, preference=0) Framed-Route = "192.168.1.0/24 0.0.0.0 10 tag 3 pref 100" corresponds with a managed route with metric=10, tag=3 and preference=100
25	Class	octets	253 chars	For example: Class = My Class
30	Called-Station-Id	string	64 chars	# LNS: L2TP Called Number AVP21 from LAC For example: Called-Station-Id = 4441212
31	Calling-Station-Id	string	64 chars	# llid|mac|remote-id|sap-id|sap-string (64 char. string configured at sap-level) For example: include-radius-attribute calling-station-id sap-id Calling-Station-Id = 1/1/2:1.1
32	NAS-Identifier	string	32 chars	For example: NAS-Identifier = PE1-Antwerp
40	Acct-Status-Type	integer	4	1=Start, 2=Stop, 3=Interim Update, 7=Accounting-On, 8=Accounting-Off, 9=Tunnel-Start, 10=Tunnel-Stop, 11=Tunnel-Reject, 12=Tunnel-Link-Start, 13=Tunnel-Link-Stop, 14=Tunnel-Link-Reject, 15=Failed
41	Acct-Delay-Time	integer	4294967295 seconds	For example: # initial accounting start Acct-Delay-Time = 0 # no ack and retry after 5 seconds Acct-Delay-Time = 5
42	Acct-Input-Octets	integer	32 bit counter	For example: Acct-Input-Octets = 5000
43	Acct-Output-Octets	integer	32 bit counter	For example: Acct-Output-Octets = 2000

Table 51: Enhanced Subscriber Management Accounting (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
44	Acct-Session-Id	string	22 bytes (number format) max. 253 bytes (description format)	No useful information can be extracted from the string. For example: # internal generated asid 22 Bytes/chars: 0x32343141464630303030303033323530423 546373530 Acct-Session-Id = 241AFF0000003250B5F750
45	Acct-Authentic	integer	4	# value = 2 (local) for local user database authentication 1=Radius, 2=Local For Example: AUTHENTIC [45] 4 Radius(1)
46	Acct-Session-Time	integer	4 Bytes 4294967295 seconds	For example: Acct-Session-Time = 870
47	Acct-Input-Packets	integer	32 bit counter 4294967295 packets	For example: Acct-Input-Packets = 15200
48	Acct-Output-Packets	integer	32 bit counter 4294967295 packets	For example: Acct-Output-Packets = 153537
49	Acct-Terminate-Cause	integer	4 Bytes	Supported causes: 1=User-Request, 2=Lost-Carrier, 3=Lost-Service, 4=Idle-Timeout, 5=Session-Timeout, 6=Admin-Reset, 8=Port-Error, 10=NAS-Request, 15=Service-Unavailable See also table Acct Terminate Cause for complete overview For example: Acct-Terminate-Cause = User-Request
50	Acct-Multi-Session-Id	string	22 bytes (number format) max. 253 bytes (description format)	No useful information can be extracted from the string. For example: # internal generated asid 22 Bytes/chars: 0x32343141464630303030303033323530423 546373530 Acct-Session-Id = 241AFF0000003250B5F750
52	Acct-Input-Gigawords	integer	32 bit counter	For example: Acct-Input-Gigawords = 1
53	Acct-Output-Gigawords	integer	32 bit counter	For example: Acct-Output-Gigawords = 3

Table 51: Enhanced Subscriber Management Accounting (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
55	Event-Timestamp	date	4 Bytes	For example: # Jul 6 2012 17:28:23 CEST is reported as 4FF70417 Event-Timestamp = 4FF70417
61	NAS-Port-Type	integer	4 Bytes Values [0..255]	Values as defined in rfc-2865 and rfc-4603 For LNS, the value is set to virtual (5) For example: NAS-Port-Type = PPPoEoQinQ (34)
87	NAS-Port-Id	string	253 Bytes	<prefix> : optional string 8 chars max <suffix> : optional string remote-id (max 64 chars) | circuit-id (max 64 chars) # NON-ATM and NON-LNS : <prefix><space><slot>/<mda>/<port>/<vlan>.<vlan><space><suffix> # ATM : <prefix><space><slot>/<mda>/<port>/<vpi>.<vci><space><suffix> # LNS : LNS rt-<routing instance>#lip-<tunnel-server-endpoint>#rip-<tunnel-client-endpoint>#ltid-<local-tunnel-id>#rtid-<remote-tunnel-id>#lsid-<local-session-id>#rsid-<remote-session-id>#<call sequence number> For example: NAS-Port-Id = 1/1/4:501.1001 NAS-Port-Id = LNS rtr-2#lip-3.3.3.3#rip-1.1.1.1#ltid-11381#rtid-1285#lsid-30067#rsid-19151#347
95	NAS-IPv6-Address	ipv6addr	16 Bytes	# ipv6-address For example: NAS-IPv6-Address = 2001:db8::1
96	Framed-Interface-Id	ifid	8 Bytes	For example: Framed-Interface-Id 02:00:00:ff:fe:00:00:01
97	Framed-IPv6-Prefix	ipv6prefix	max. 16 Bytes for prefix + 1 Byte for length	PPPoE SLAAC wan-host <ipv6-prefix/prefix-length> with prefix-length 64 For example: Framed-IPv6-Prefix 2021:1:FFF3:1::/64

Table 51: Enhanced Subscriber Management Accounting (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
99	Framed-IPv6-Route	string	max. 16 Framed-IPv6-Route attributes	<ip-prefix>/<prefix-length> <space> :: <space> <metric> [<space> tag <space> <tag-value>] <space> pref <space> <preference-value>” The gateway address is always reported as "::", representing the wan host ip. For example: Framed-IPv6-Route = "5000:0:1::/56 :: 0 pref 0" corresponds with a managed route with default metrics (metric=0, no tag, preference=0) Framed-IPv6-Route = "5000:0:1::/56 :: 10 tag 3 pref 100" corresponds with a managed route with metric=10, tag=3 and preference=100
123	Delegated-IPv6-Prefix	ipv6prefix	max. 16 Bytes for prefix + 1 Byte for length	<ipv6-prefix/prefix-length> with prefix-length [48..64] For example: Delegated-IPv6-Prefix 2001:DB8:173A:100::/56
26-3561-1	Agent-Circuit-Id	string	247 chars	format see also RFC4679 # ATM/DSL <Access-Node-Identifier><atm slot/port:vpi.vci> # Ethernet/DSL <Access-Node-Identifier><eth slot/port[:vlan-id]> For example: ethernet dslam1 slot 2 port 1 vlan 100 Agent-Circuit-Id = dslam1 eth 2/1:100
26-3561-2	Agent-Remote-Id	string	247 chars	format see also RFC4679 For example: Agent-Remote-Id = MyRemoteId
26-3561-129	Actual-Data-Rate-Upstream	integer	4294967295 bps	For example: # 1Mbps Actual-Data-Rate-Upstream = 1000000
26-3561-130	Actual-Data-Rate-Downstream	integer	4294967295 bps	For example: # 5Mbps Actual-Data-Rate-Downstream = 5000000
26-3561-131	Minimum-Data-Rate-Upstream	integer	4294967295 bps	For example: Minimum-Data-Rate-Upstream = 1000
26-3561-132	Minimum-Data-Rate-Downstream	integer	4294967295 bps	For example: Minimum-Data-Rate-Downstream = 1000
26-3561-133	Attainable-Data-Rate-Upstream	integer	4294967295 bps	For example: Attainable-Data-Rate-Downstream = 1000

Table 51: Enhanced Subscriber Management Accounting (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-3561-134	Attainable-Data-Rate-Downstream	integer	4294967295 bps	For example: Minimum-Data-Rate-Upstream = 1000
26-3561-135	Maximum-Data-Rate-Upstream	integer	4294967295 bps	For example: Maximum-Data-Rate-Upstream = 1000
26-3561-136	Maximum-Data-Rate-Downstream	integer	4294967295 bps	For example: Maximum-Data-Rate-Downstream = 1000
26-3561-137	Minimum-Data-Rate-Upstream-Low-Power	integer	4294967295 bps	For example: Minimum-Data-Rate-Upstream-Low-Power = 1000
26-3561-138	Minimum-Data-Rate-Downstream-Low-Power	integer	4294967295 bps	For example: Minimum-Data-Rate-Downstream-Low-Power = 1000
26-3561-139	Maximum-Interleaving-Delay-Upstream	integer	4294967295 milliseconds	For example: Maximum-Interleaving-Delay-Upstream = 10
26-3561-140	Actual-Interleaving-Delay-Upstream	integer	4294967295 milliseconds	For example: Actual-Interleaving-Delay-Upstream = 10
26-3561-141	Maximum-Interleaving-Delay-Downstream	integer	4294967295 milliseconds	For example: Maximum-Interleaving-Delay-Downstream = 10
26-3561-142	Actual-Interleaving-Delay-Downstream	integer	4294967295 milliseconds	For example: Actual-Interleaving-Delay-Downstream = 10
26-3561-144	Access-Loop-Encapsulation	octets	3 Bytes	<Data Link><Encaps-1><Encaps-2> <Data Link>: AAL5(1), Ethernet(2) <Encaps 1>: NotAvailable(0), Untagged Ethernet(1), Single-Tagged Ethernet(2) <Encaps 2>: Not Available(0), PPPoA LLC(1), PPPoA Null(2), IPoA LLC(3), IPoA Null(4), Ethernet over AAL5 LLC w FCS(5), Ethernet over AAL5 LLC w/o FCS(6), Ethernet over AAL5 Null w FCS(7), Ethernet over AAL5 Null w/o FCS(8) For example: Ethernet , Single-Tagged Ethernet , Ethernet over AAL5 LLC w FCS Access-Loop-Encapsulation = 020205
26-3561-254	IWF-Session	octets	len 0	For example: IWF-Session
26-6527-11	Alc-Subsc-ID-Str	string	32 chars	For example: Alc-Subsc-ID-Str = MySubscriberId

Table 51: Enhanced Subscriber Management Accounting (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-12	Alc-Subsc-Prof-Str	string	16 chars	For example: Alc-Subsc-Prof-Str = MySubProfile
26-6527-13	Alc-SLA-Prof-Str	string	16 chars	For example: Alc-SLA-Prof-Str = MySlaProfile
26-6527-19	Alc-Acct-I-Inprof-Octets-64	octets	10 bytes/ attribute w/ max 31 attributes	<Q/P-selection 1 Byte><Queue-id|Policer-id 1 Byte><8 Byte value> where Q/P-selection : 00 = Queue counters, 80= Policer counters where Queue-id|Policer-id range <1..32> For example: # 500 bytes in profile traffic for ingress queue 2 Alc-Acct-I-Inprof-Octets-64 = 0x000200000000000001f4 # 1000 bytes in profile traffic for ingress policer 3 Alc-Acct-I-Inprof-Octets-64 = 0x800300000000000003e8
26-6527-20	Alc-Acct-I-Outprof-Octets-64	octets	10 bytes/ attribute w/ max 31 attributes	<Q/P-selection 1 Byte><Queue-id|Policer-id 1 Byte><8 Byte value> where Q/P-selection : 00 = Queue counters, 80= Policer counters where Queue-id|Policer-id range <1..32> For example: # 500 bytes out of profile traffic for ingress queue 2 Alc-Acct-I-Outprof-Octets-64 = 0x000200000000000001f4 # 1000 bytes out of profile traffic for ingress policer 3 Alc-Acct-I-Outprof-Octets-64 = 0x800300000000000003e8
26-6527-21	Alc-Acct-O-Inprof-Octets-64	octets	10 bytes/ attribute w/ max 8 attributes	<Q/P-selection 1 Byte><Queue-id|Policer-id 1 Byte><8 Byte value> where Q/P-selection : 00 = Queue counters, 80= Policer counters where Queue-id|Policer-id range <1..8> For example: # 500 bytes in profile traffic for egress queue 2 Alc-Acct-O-Inprof-Octets-64 = 0x000200000000000001f4 # 1000 bytes in profile traffic for egress policer 3 Alc-Acct-O-Inprof-Octets-64 = 0x800300000000000003e8

Table 51: Enhanced Subscriber Management Accounting (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-22	Alc-Acct-O-Outprof-Octets-64	octets	10 bytes/ attribute w/ max 8 attributes	<Q/P-selection 1 Byte><Queue-id|Policer-id 1 Byte><8 Byte value> where Q/P-selection : 00 = Queue counters, 80= Policer counters where Queue-id|Policer-id range <1..8> For example: # 500 bytes out of profile traffic for egress queue 2 Alc-Acct-O-Inprof-Octets-64 = 0x00020000000000001f4 # 1000 bytes out of profile traffic for egress policer 3 Alc-Acct-O-Inprof-Octets-64 = 0x800300000000000003e8
26-6527-23	Alc-Acct-I-Inprof-Pkts-64	octets	10 bytes/ attribute w/ max 31 attributes	<Q/P-selection 1 Byte><Queue-id|Policer-id 1 Byte><8 Byte value> where Q/P-selection : 00 = Queue counters, 80= Policer counters where Queue-id|Policer-id range <1..32> For example: # 500 packets in profile traffic for ingress queue 2 Alc-Acct-I-Inprof-Pkts-64 = 0x00020000000000001f4 # 1000 packets in profile traffic for ingress policer 3 Alc-Acct-I-Inprof-Pkts-64 = 0x800300000000000003e8
26-6527-24	Alc-Acct-I-Outprof-Pkts-64	octets	10 bytes/ attribute w/ max 31 attributes	<Q/P-selection 1 Byte><Queue-id|Policer-id 1 Byte><8 Byte value> where Q/P-selection : 00 = Queue counters, 80= Policer counters where Queue-id|Policer-id range <1..32> For example: # 500 packets out profile traffic for ingress queue 2 Alc-Acct-I-Outprof-Pkts-64 = 0x00020000000000001f4 # 1000 packets out profile traffic for ingress policer 3 Alc-Acct-I-Outprof-Pkts-64 = 0x800300000000000003e8
26-6527-25	Alc-Acct-O-Inprof-Pkts-64	octets	10 bytes/ attribute w/ max 8 attributes	<Q/P-selection 1 Byte><Queue-id|Policer-id 1 Byte><8 Byte value> where Q/P-selection : 00 = Queue counters, 80= Policer counters where Queue-id|Policer-id range <1..8> For example: # 500 packets in profile traffic for egress queue 2 Alc-Acct-O-Inprof-Pkts-64 = 0x00020000000000001f4 # 1000 packets in profile traffic for egress policer 3 Alc-Acct-O-Inprof-Pkts-64 = 0x800300000000000003e8

Table 51: Enhanced Subscriber Management Accounting (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-26	Alc-Acct-O-Outprof-Pkts-64	octets	10 bytes/ attribute w/ max 8 attributes	<Q/P-selection 1 Byte><Queue-id|Policer-id 1 Byte><8 Byte value> where Q/P-selection : 00 = Queue counters, 80= Policer counters where Queue-id|Policer-id range <1..8> For example: # 500 packets out profile traffic for egress queue 2 Alc-Acct-O-Outprof-Pkts-64 = 0x000200000000000001f4 # 1000 packets out profile traffic for egress policer 3 Alc-Acct-O-Outprof-Pkts-64 = 0x800300000000000003e8
26-6527-27	Alc-Client-Hardware-Addr	string	6 Bytes	For example: Alc-Client-Hardware-Addr = 00:00:00:00:00:01
26-6527-39	Alc-Acct-OC-O-Inprof-Octets-64	octets	10 bytes	<Counter-id> <8 Byte value> For example: Alc-Acct-OC-O-Inprof-Octets-64 = 0x000200000000000001f4
26-6527-40	Alc-Acct-OC-O-Outprof-Octets-64	octets	10 bytes	<Counter-id> <8 Byte value> For example: Alc-Acct-OC-O-Outprof-Octets-64 = 0x000100000000000000d3
26-6527-43	Alc-Acct-OC-O-Inprof-Pkts-64	octets	10 bytes	<Counter-id> <8 Byte value> For example: Alc-Acct-OC-O-Inprof-Pkts-64 = 0x0005000000000001fda4
26-6527-44	Alc-Acct-OC-O-Outprof-Pkts-64	octets	10 bytes	<Counter-id> <8 Byte value> For example: Alc-Acct-OC-O-Outprof-Pkts-64 = 0x00010000000000000aea
26-6527-69	Alc-Acct-I-High-Octets-Drop_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1..32> For example: INPUT_HIGH_OCTETS_DROP_64 [69] 10 0x00010000000000000000
26-6527-70	Alc-Acct-I-Low-Octets-Drop_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1..32> For example: INPUT_LOW_OCTETS_DROP_64 [70] 10 0x00010000000000000000
26-6527-71	Alc-Acct-I-High-Pack-Drop_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1..32> For example: INPUT_HIGH_PACK_DROP_64 [71] 10 0x00010000000000000000

Table 51: Enhanced Subscriber Management Accounting (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-72	Alc-Acct-I-Low-Pack-Drop_64	octets	10 bytes	<Queue-id 2Bytes><8 Bytes value> where Queue-id range <1..32> For example: INPUT_LOW_PACK_DROP_64 [72] 10 0x00010000000000000000
26-6527-73	Alc-Acct-I-High-Octets-Offer_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1..32> For example: INPUT_HIGH_OCTETS_OFFER_64 [73] 10 0x00010000000000000000
26-6527-74	Alc-Acct-I-Low-Octets-Offer_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1..32> For example: INPUT_LOW_OCTETS_OFFER_64 [74] 10 0x00010000000000000000
26-6527-75	Alc-Acct-I-High-Pack-Offer_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1..32> For example: INPUT_HIGH_PACK_OFFER_64 [75] 10 0x00010000000000000000
26-6527-76	Alc-Acct-I-Low-Pack-Offer_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1..32> For example: INPUT_LOW_PACK_OFFER_64 [76] 10 0x00010000000000000000
26-6527-77	Alc-Acct-I-Unc-Octets-Offer_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1..32> For example: INPUT_UNC_OCTETS_OFFER_64 [77] 10 0x00010000000000000000
26-6527-78	Alc-Acct-I-Unc-Pack-Offer_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1..32> For example: INPUT_UNC_PACK_OFFER_64 [78] 10 0x00010000000000000000
26-6527-81	Alc-Acct-O-Inprof-Pack-Drop_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1..8> For example: OUTPUT_INPROF_PACK_DROP_64 [81] 10 0x00010000000000000000

Table 51: Enhanced Subscriber Management Accounting (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-82	Alc-Acct-O-Outprof-Pack-Drop_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1..8> For example: OUTPUT_OUTPROF_PACK_DROP_64 [82] 10 0x00010000000000000000
26-6527-83	Alc-Acct-O-Inprof-Octs-Drop_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1..8> For example: OUTPUT_INPROF_OCTS_DROP_64 [83] 10 0x00010000000000000000
26-6527-84	Alc-Acct-O-Outprof-Octs-Drop_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1..8> For example: OUTPUT_OUTPROF_OCTS_DROP_64 [84] 10 0x00010000000000000000
26-6527-91	Alc-Acct-OC-O-Inpr-Pack-Drop_64	octets	10 bytes	<Counter-id> <8 Byte value> For example: Alc-Acct-OC-O-Inpr-Pack-Drop_64 = 0x000100000000000129b1
26-6527-92	Alc-Acct-OC-O-Outpr-Pack-Drop_64	octets	10 bytes	<Counter-id> <8 Byte value> For example: Alc-Acct-OC-O-Outpr-Pack-Drop_64 = 0x000700000000000307b4
26-6527-93	Alc-Acct-OC-O-Inpr-Octs-Drop_64	octets	10 bytes	<Counter-id> <8 Byte value> For example: Alc-Acct-OC-O-Inpr-Octs-Drop_64 = 0x000100000000000143fa
26-6527-94	Alc-Acct-OC-O-Outpr-Octs-Drop_64	octets	10 bytes	<Counter-id> <8 Byte value> For example: Alc-Acct-OC-O-Outpr-Octs-Drop_64 = 0x0001000000000000ab65
26-6527-99	Alc-Ipv6-Address	ipv6addr	16 Bytes	For example: Alc-Ipv6-Address 2021:1:FFF5::1
26-6527-107	Alc-Acct-I-statmode	string	253 chars	<Q/P-selection 1 Byte><Queue-id|Policer-id 1 Byte><space><statmode-string> Q/P-selection: 0x00 = Queue statmode, 0x80 = Policer statmode Queue-id|Polcer-id range <1..32> stat-mode : configured stat-mode For example: # configure ingress policer 5 stat-mode offered-priority-no-cir INPUT_STATMODE [107] 30 0x8005 offered-priority-no-cir

Table 51: Enhanced Subscriber Management Accounting (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-108	Alc-Acct-I-Hiprio-Octets_64	octets	10 bytes	<0x80><policer-id><8 byte value> where policer-id <1..32> For example: # ingress policer 5 INPUT_HIPRIO_OCTETS_64 [108] 10 0x80050000000000000000
26-6527-109	Alc-Acct-I-Lowprio-Octets_64	octets	10 bytes	<0x80><policer-id><8 byte value> where policer-id <1..32> For example: # ingress policer 5 INPUT_LOWPRIO_OCTETS_64 [109] 10 0x80050000000000000000
26-6527-110	Alc-Acct-O-Hiprio-Octets_64	octets	10 bytes	<0x80><policer-id><8 byte value> where policer-id <1..32> For example: # ingress policer 5 OUTPUT_HIPRIO_OCTETS_64 [110] 10 0x80050000000000000000
26-6527-111	Alc-Acct-O-Lowprio-Octets_64	octets	10 bytes	<0x80><policer-id><8 byte value> where policer-id <1..32> For example: # ingress policer 5 OUTPUT_LOWPRIO_OCTETS_64 [111] 10 0x80050000000000000000
26-6527-112	Alc-Acct-I-Hiprio-Packets_64	octets	10 bytes	<0x80><policer-id><8 byte value> where policer-id <1..32> For example: # ingress policer 5 INPUT_HIPRIO_PACKETS_64 [112] 10 0x80050000000000000000
26-6527-113	Alc-Acct-I-Lowprio-Packets_64	octets	10 bytes	<0x80><policer-id><8 byte value> where policer-id <1..32> For example: # ingress policer 5 INPUT_LOWPRIO_PACKETS_64 [113] 10 0x80050000000000000000
26-6527-114	Alc-Acct-O-Hiprio-Packets_64	octets	10 bytes	<0x80><policer-id><8 byte value> where policer-id <1..8> For example: # egress policer 1 OUTPUT_HIPRIO_PACKETS_64 [114] 10 0x80010000000000000000
26-6527-115	Alc-Acct-O-Lowprio-Packets_64	octets	10 bytes	<0x80><policer-id><8 byte value> where policer-id <1..8> For example: # egress policer 1 OUTPUT_LOWPRIO_PACKETS_64 [115] 10 0x80010000000000000000

Table 51: Enhanced Subscriber Management Accounting (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-116	Alc-Acct-I-All-Octets_64	octets	10 bytes	<0x80><policer-id><8 byte value> where policer-id <1..8> For example: # egress policer 1 INPUT_ALL_OCTETS_64 [116] 10 0x80010000000000000000
26-6527-117	Alc-Acct-O-All-Octets_64	octets	10 bytes	<0x80><policer-id><8 byte value> where policer-id <1..8> For example: # egress policer 1 OUTPUT_ALL_OCTETS_64 [117] 10 0x80010000000000000000
26-6527-118	Alc-Acct-I-All-Packets_64	octets	10 bytes	<0x80><policer-id><8 byte value> where policer-id <1..32> For example: # ingress policer 3 INPUT_ALL_PACKETS_64 [118] 10 0x80030000000000000000
26-6527-119	Alc-Acct-O-All-Packets_64	octets	10 bytes	<0x80><policer-id><8 byte value> where policer-id <1..8> For example: # egress policer 1 OUTPUT_ALL_PACKETS_64 [119] 10 0x80010000000000000000
26-6527-121	Alc-Nat-Port-Range	string	no limits	<public-ip><space><port-range><space><outside-routing-instance> For example: # public pool address 180.0.1.248; port-range [37674..37723] in Base Alc-Nat-Port-Range = 180.0.1.248 37674-37723 router base
26-6527-127	Alc-Acct-O-statmode	string	253 chars	<Q/P-selection 1 Byte><Queue-id|Policer-id 1 Byte><space><statmode-string> Q/P-selection: 0x00 = Queue statmode, 0x80 = Policer statmode Queue-id|Policer-id range <1..32> stat-mode: configured stat-mode For example: # configure egress policer 5 stat-mode offered-limited-capped-cir OUTPUT_STATMODE [127] 33 0x8001 offered-limited-capped-cir
26-6527-148	Alc-RSSI	integer	32 bit value	For example: Alc-RSSI = 30

Table 51: Enhanced Subscriber Management Accounting (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-163	Alc-Acct-Triggered-Reason	integer	4 bytes	1=regular, 2=sla-start, 3=sla-stop, 4=Framed-IP-Address-up, 5=Framed-IP-Address-down, 6=Alc-IPv6-Address-up, 7=Alc-IPv6-Address-down, 8=Delegated-IPv6-Prefix-up, 9=Delegated-IPv6-Prefix-down, 10=Framed-IPv6-Prefix-up, 11=Framed-IPv6-Prefix-down, 12=Interval-Changed, 13=DSL-Line-Attributes-Changed, , 14=Wlan-Mobility-Event, 15=Persistence-Recover, 16=SRRP-Switchover For Example: ACCT TRIGGERED INTERIM REASON [163] 4 regular(1)
26-6527-175	Alc-DSL-Line-State	integer	4 bytes	1=showtime, 2-idle, 3=silent For example: Alc-DSL-Line-State = SHOWTIME
26-6527-176	Alc-DSL-Type	integer	4 bytes	0=other, 1=ADSL1, 2=ADSL2, 3=ADSL2PLUS, 4=VDSL1, 5=VDSL2, 6=SDSL For example: Alc-DSL-Type = VDSL2
26-6527-194	Alc-IPv6-Acct-Input-Packets	integer	4 bytes	For example: Alc-IPv6-Acct-Input-Packets = 14511
26-6527-195	Alc-IPv6-Acct-Input-Octets	integer	4 bytes	For example: Alc-IPv6-Acct-Input-Octets = 2932215
26-6527-196	Alc-IPv6-Acct-Input-GigaWords	integer	4 bytes	For example: Alc-IPv6-Acct-Input-GigaWords = 1
26-6527-197	Alc-IPv6-Acct-Output-Packets	integer	4 bytes	For example: Alc-IPv6-Acct-Output-Packets = 54122
26-6527-198	Alc-IPv6-Acct-Output-Octets	integer	4 bytes	For example: Alc-IPv6-Acct-Output-Octets = 8521943
26-6527-199	Alc-IPv6-Acct-Output-Gigawords	integer	4 bytes	For example: Alc-IPv6-Acct-Output-Gigawords = 2
26-25053-2	Ruckus-Sta-RSSI	integer	32 bits value	For example: Ruckus-Sta-RSSI = 28

Table 52: Enhanced Subscriber Management Accounting (applicability)

Attribute ID	Attribute Name	Acct Start	Acct Stop	Acct Interim-Update	Acct On (*)	Acct Off (*)	Acct Reporting Level
1	User-Name	0-1	0-1	0-1	0	0	H->S->Q
4	NAS-IP-Address	0-1	0-1	0-1	0-1	0-1	HSQ
5	NAS-Port	0-1	0-1	0-1	0	0	H->S->Q
6	Service-Type	1	1	1	0	0	H->S->Q
7	Framed-Protocol	1	1	1	0	0	H->S->Q
8	Framed-IP-Address	0-1	0-1	0-1	0	0	H->S->Q
9	Framed-IP-Netmask	0-1	0-1	0-1	0	0	H->S->Q
22	Framed-Route	0+	0+	0+	0	0	H->S->Q
25	Class	0-1	0-1	0-1	0	0	H->S->Q
30	Called-Station-Id	0-1	0-1	0-1	0	0	H->S->Q
31	Calling-Station-Id	0-1	0-1	0-1	0	0	H->S->Q
32	NAS-Identifier	0-1	0-1	0-1	1	1	HSQ
40	Acct-Status-Type	1	1	1	1	1	HSQ
41	Acct-Delay-Time	0-1	0-1	0-1	0-1	0-1	HSQ
42	Acct-Input-Octets	0	0-1	0-1	0	0	HSQ
43	Acct-Output-Octets	0	0-1	0-1	0	0	HSQ
44	Acct-Session-Id	1	1	1	1	1	HSQ
45	Acct-Authentic	0-1	0-1	0-1	1	1	H->S->Q
46	Acct-Session-Time	0	1	1	0	0	HSQ
47	Acct-Input-Packets	0	0-1	0-1	0	0	HSQ
48	Acct-Output-Packets	0	0-1	0-1	0	0	HSQ
49	Acct-Terminate-Cause	0	1	0	0	1	HSQ
50	Acct-Multi-Session-Id	0-1	0-1	0-1	0	0	HSQ

Table 52: Enhanced Subscriber Management Accounting (applicability) (Continued)

Attribute ID	Attribute Name	Acct Start	Acct Stop	Acct Interim-Update	Acct On (*)	Acct Off (*)	Acct Reporting Level
52	Acct-Input-Gigawords	0	0-1	0-1	0	0	HSQ
53	Acct-Output-Gigawords	0	0-1	0-1	0	0	HSQ
55	Event-Timestamp	1	1	1	1	1	HSQ
61	NAS-Port-Type	0-1	0-1	0-1	0	0	H->S->Q
87	NAS-Port-Id	0-1	0-1	0-1	0	0	H->S->Q
95	NAS-IPv6-Address	0-1	0-1	0-1	0-1	0-1	HSQ
96	Framed-Interface-Id	0-1	0-1	0-1	0	0	H->S->Q
97	Framed-IPv6-Prefix	0-1	0-1	0-1	0	0	H->S->Q
99	Framed-IPv6-Route	0+	0+	0+	0	0	H->S->Q
123	Delegated-IPv6-Prefix	0-1	0-1	0-1	0	0	H->S->Q
26-3561-1	Agent-Circuit-Id	0-1	0-1	0-1	0	0	H->S->Q
26-3561-2	Agent-Remote-Id	0-1	0-1	0-1	0	0	H->S->Q
26-3561-129	Actual-Data-Rate-Upstream	0-1	0-1	0-1	0	0	H->S->Q
26-3561-130	Actual-Data-Rate-Downstream	0-1	0-1	0-1	0	0	H->S->Q
26-3561-131	Minimum-Data-Rate-Upstream	0-1	0-1	0-1	0	0	H->S->Q
26-3561-132	Minimum-Data-Rate-Downstream	0-1	0-1	0-1	0	0	H->S->Q
26-3561-133	Attainable-Data-Rate-Upstream	0-1	0-1	0-1	0	0	H->S->Q
26-3561-134	Attainable-Data-Rate-Downstream	0-1	0-1	0-1	0	0	H->S->Q
26-3561-135	Maximum-Data-Rate-Upstream	0-1	0-1	0-1	0	0	H->S->Q
26-3561-136	Maximum-Data-Rate-Downstream	0-1	0-1	0-1	0	0	H->S->Q
26-3561-137	Minimum-Data-Rate-Upstream-Low-Power	0-1	0-1	0-1	0	0	H->S->Q
26-3561-138	Minimum-Data-Rate-Downstream-Low-Power	0-1	0-1	0-1	0	0	H->S->Q

Table 52: Enhanced Subscriber Management Accounting (applicability) (Continued)

Attribute ID	Attribute Name	Acct Start	Acct Stop	Acct Interim-Update	Acct On (*)	Acct Off (*)	Acct Reporting Level
26-3561-139	Maximum-Interleaving-Delay-Upstream	0-1	0-1	0-1	0	0	H->S->Q
26-3561-140	Actual-Interleaving-Delay-Upstream	0-1	0-1	0-1	0	0	H->S->Q
26-3561-141	Maximum-Interleaving-Delay-Downstream	0-1	0-1	0-1	0	0	H->S->Q
26-3561-142	Actual-Interleaving-Delay-Downstream	0-1	0-1	0-1	0	0	H->S->Q
26-3561-144	Access-Loop-Encapsulation	0-1	0-1	0-1	0	0	H->S->Q
26-3561-254	IWF-Session	0-1	0-1	0-1	0	0	H->S->Q
26-6527-11	Alc-Subsc-ID-Str	0-1	0-1	0-1	0	0	HSQ
26-6527-12	Alc-Subsc-Prof-Str	0-1	0-1	0-1	0	0	HSQ
26-6527-13	Alc-SLA-Prof-Str	0-1	0-1	0-1	0	0	HSQ
26-6527-19	Alc-Acct-I-Inprof-Octets-64	0	0+	0+	0	0	HSQ
26-6527-20	Alc-Acct-I-Outprof-Octets-64	0	0+	0+	0	0	HSQ
26-6527-21	Alc-Acct-O-Inprof-Octets-64	0	0+	0+	0	0	HSQ
26-6527-22	Alc-Acct-O-Outprof-Octets-64	0	0+	0+	0	0	HSQ
26-6527-23	Alc-Acct-I-Inprof-Pkts-64	0	0+	0+	0	0	HSQ
26-6527-24	Alc-Acct-I-Outprof-Pkts-64	0	0+	0+	0	0	HSQ
26-6527-25	Alc-Acct-O-Inprof-Pkts-64	0	0+	0+	0	0	HSQ
26-6527-26	Alc-Acct-O-Outprof-Pkts-64	0	0+	0+	0	0	HSQ
26-6527-27	Alc-Client-Hardware-Addr	0-1	0-1	0-1	0	0	H->S->Q
26-6527-39	Alc-Acct-OC-O-Inprof-Octets-64	0	0+	0+	0	0	HSQ
26-6527-40	Alc-Acct-OC-O-Outprof-Octets-64	0	0+	0+	0	0	HSQ
26-6527-43	Alc-Acct-OC-O-Inprof-Pkts-64	0	0+	0+	0	0	HSQ
26-6527-44	Alc-Acct-OC-O-Outprof-Pkts-64	0	0+	0+	0	0	HSQ

Table 52: Enhanced Subscriber Management Accounting (applicability) (Continued)

Attribute ID	Attribute Name	Acct Start	Acct Stop	Acct Interim-Update	Acct On (*)	Acct Off (*)	Acct Reporting Level
26-6527-69	Alc-Acct-I-High-Octets-Drop_64	0	0+	0+	0	0	HSQ
26-6527-70	Alc-Acct-I-Low-Octets-Drop_64	0	0+	0+	0	0	HSQ
26-6527-71	Alc-Acct-I-High-Pack-Drop_64	0	0+	0+	0	0	HSQ
26-6527-72	Alc-Acct-I-Low-Pack-Drop_64	0	0+	0+	0	0	HSQ
26-6527-73	Alc-Acct-I-High-Octets-Offer_64	0	0+	0+	0	0	HSQ
26-6527-74	Alc-Acct-I-Low-Octets-Offer_64	0	0+	0+	0	0	HSQ
26-6527-75	Alc-Acct-I-High-Pack-Offer_64	0	0+	0+	0	0	HSQ
26-6527-76	Alc-Acct-I-Low-Pack-Offer_64	0	0+	0+	0	0	HSQ
26-6527-77	Alc-Acct-I-Unc-Octets-Offer_64	0	0+	0+	0	0	HSQ
26-6527-78	Alc-Acct-I-Unc-Pack-Offer_64	0	0+	0+	0	0	HSQ
26-6527-81	Alc-Acct-O-Inprof-Pack-Drop_64	0	0+	0+	0	0	HSQ
26-6527-82	Alc-Acct-O-Outprof-Pack-Drop_64	0	0+	0+	0	0	HSQ
26-6527-83	Alc-Acct-O-Inprof-Octs-Drop_64	0	0+	0+	0	0	HSQ
26-6527-84	Alc-Acct-O-Outprof-Octs-Drop_64	0	0+	0+	0	0	HSQ
26-6527-91	Alc-Acct-OC-O-Inpr-Pack-Drop_64	0	0+	0+	0	0	HSQ
26-6527-92	Alc-Acct-OC-O-Outpr-Pack-Drop_64	0	0+	0+	0	0	HSQ
26-6527-93	Alc-Acct-OC-O-Inpr-Octs-Drop_64	0	0+	0+	0	0	HSQ
26-6527-94	Alc-Acct-OC-O-Outpr-Octs-Drop_64	0	0+	0+	0	0	HSQ
26-6527-99	Alc-Ipv6-Address	0-1	0-1	0-1	0	0	H->S->Q
26-6527-107	Alc-Acct-I-statmode	0	0+	0+	0	0	HSQ
26-6527-108	Alc-Acct-I-Hiprio-Octets_64	0	0+	0+	0	0	HSQ
26-6527-109	Alc-Acct-I-Lowprio-Octets_64	0	0+	0+	0	0	HSQ
26-6527-110	Alc-Acct-O-Hiprio-Octets_64	0	0+	0+	0	0	HSQ

Table 52: Enhanced Subscriber Management Accounting (applicability) (Continued)

Attribute ID	Attribute Name	Acct Start	Acct Stop	Acct Interim-Update	Acct On (*)	Acct Off (*)	Acct Reporting Level
26-6527-111	Alc-Acct-O-Lowprio-Octets_64	0	0+	0+	0	0	HSQ
26-6527-112	Alc-Acct-I-Hiprio-Packets_64	0	0+	0+	0	0	HSQ
26-6527-113	Alc-Acct-I-Lowprio-Packets_64	0	0+	0+	0	0	HSQ
26-6527-114	Alc-Acct-O-Hiprio-Packets_64	0	0+	0+	0	0	HSQ
26-6527-115	Alc-Acct-O-Lowprio-Packets_64	0	0+	0+	0	0	HSQ
26-6527-116	Alc-Acct-I-All-Octets_64	0	0+	0+	0	0	HSQ
26-6527-117	Alc-Acct-O-All-Octets_64	0	0+	0+	0	0	HSQ
26-6527-118	Alc-Acct-I-All-Packets_64	0	0+	0+	0	0	HSQ
26-6527-119	Alc-Acct-O-All-Packets_64	0	0+	0+	0	0	HSQ
26-6527-121	Alc-Nat-Port-Range	0-1	0-1	0-1	0	0	HSQ
26-6527-127	Alc-Acct-O-statmode	0	0+	0+	0	0	HSQ
26-6527-148	Alc-RSSI	0-1	0-1	0-1	0	0	HSQ
26-6527-163	Alc-Acct-Triggered-Reason	0	0	0-1	0	0	HSQ
26-6527-175	Alc-DSL-Line-State	0-1	0-1	0-1	0	0	H->S->Q
26-6527-176	Alc-DSL-Type	0-1	0-1	0-1	0	0	H->S->Q
26-6527-194	Alc-IPv6-Acct-Input-Packets	0	0-1	0-1	0	0	HSQ
26-6527-195	Alc-IPv6-Acct-Input-Octets	0	0-1	0-1	0	0	HSQ
26-6527-196	Alc-IPv6-Acct-Input-GigaWords	0	0-1	0-1	0	0	HSQ
26-6527-197	Alc-IPv6-Acct-Output-Packets	0	0-1	0-1	0	0	HSQ
26-6527-198	Alc-IPv6-Acct-Output-Octets	0	0-1	0-1	0	0	HSQ
26-6527-199	Alc-IPv6-Acct-Output-Gigawords	0	0-1	0-1	0	0	HSQ
26-25053-2	Ruckus-Sta-RSSI	0-1	0-1	0-1	0	0	HSQ

(*) Note on acct-on/off: The table represents the acct-on-off attributes for an accounting server configured via a radius-server-policy (**configure subscriber-mgmt radius-accounting-policy** <*name*> **radius-server-policy** <*radius-server-policy-name*> and with **acct-on-off** enabled. If the accounting server is configured direct under the radius-accounting-server (**configure subscriber-mgmt radius-accounting-policy** <*name*> **radius-accounting-server server** <*server-index*>, then the following attributes are not sent in acct-on/off messages: [44] Acct-Session-Id, [45] Acct-Authentic and [49] Acct-Terminate-Cause; and attribute [26-6527-12] Alc-Subsc-Prof-Str is sent.

Subscriber Service Accounting

This section specifies the attributes for RADIUS accounting on subscriber service instances. The attributes included in the subscriber service accounting messages are identical to the attributes that are included in the associated parent subscriber host accounting session (Host accounting mode for IPoE and Session accounting mode for PPPoE). Volume counters are always reported in standard attributes. Differences for attribute content and additional attributes are detailed in the tables below.

Table 53: Subscriber Service Accounting (description)

Attribute ID	Attribute Name	Description
42	Acct-Input-Octets	octets received for this subscriber service instance. Only included if stats-type is set to volume and time.
43	Acct-Output-Octets	octets send for this subscriber service instance. Only included if stats-type is set to volume and time.
44	Acct-Session-Id	Unique generated hexadecimal number that represents the accounting session for this Subscriber Service instance.
47	Acct-Input-Packets	packets received for this subscriber service instance. Only included if stats-type is set to volume and time.
48	Acct-Output-Packets	packets send for this subscriber service instance. Only included if stats-type is set to volume and time.
50	Acct-Multi-Session-Id	Accounting session id of the parent PPPoE session session acct-session-id or IPoE host (host acct-session-id). The format (variable length description or fixed 22B hexadecimal number) is identical to the parent PPPoE session or IPoE host and determined by session-id-format in the radius-accounting-policy (**configure subscriber-mgmt radius-accounting-policy** <*policy-name*> **session-id-format** {**number**|**description**}).

Table 53: Subscriber Service Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
52	Acct-Input-Gigawords	indicates how many times (one or more) the [42] Acct-Input-Octets counter has wrapped around 2^32 in the course of delivering this service. Only included if its value is different from zero and stats-type is set to volume and time.
53	Acct-Output-Gigawords	indicates how many times (one or more) the [42] Acct-Input-Octets counter has wrapped around 2^32 in the course of delivering this service. Only included if its value is different from zero and stats-type is set to volume and time.
26-6527-151	Alc-Sub-Serv-Activate	Activate a subscriber service. The attribute typically contains parameters as input for the Python script that populates the subscriber service data structure (sub_svc). The attribute is ignored if not used in Python. The parameters can cross an attribute boundary. The concatenation of all Alc-Sub-Serv-Activate attributes with the same tag in a single message is typically used as a unique subscriber service instance identifier (key). In subscriber service RADIUS accounting messages, the attribute is sent untagged and contains the subscriber service data structure sub_svc.name value used at service activation. Multiple attributes may be present if the total length does not fit a single attribute.

Table 54: Subscriber Service Accounting (limits)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
42	Acct-Input-Octets	integer	4 Bytes	For example: Acct-Input-Octets = 5000
43	Acct-Output-Octets	integer	4 Bytes	For example: Acct-Output-Octets = 2000
44	Acct-Session-Id	string	22 Bytes	For example: # Acct-Session-Id = 24ADFF0000000950C5F138 Acct-Session-Id 0x32313238343633353932313032353132313133343039
47	Acct-Input-Packets	integer	4 Bytes 4294967295 packets	For example: Acct-Input-Packets = 15200
48	Acct-Output-Packets	integer	4 Bytes 4294967295 packets	For example: Acct-Output-Packets = 153537

Table 54: Subscriber Service Accounting (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
50	Acct-Multi-Session-Id	string	22 bytes (number format) max. 253 bytes (description format)	For example: Acct-Multi-Session-Id = 24ADFF0000000750C8EB26
52	Acct-Input-Gigawords	integer	4 Bytes	For example: Acct-Input-Gigawords = 7
53	Acct-Output-Gigawords	integer	4 Bytes	For example: Acct-Output-Gigawords = 3
26-6527-151	Alc-Sub-Serv-Activate	string	multiple VSA's per tag per message	For example: Alc-Sub-Serv-Activate;1 = rate-limit;1000;8000

Table 55: Subscriber Service Accounting (applicability)

Attribute ID	Attribute Name	Acct Start	Acct Stop	Acct Interim-Update
42	Acct-Input-Octets	0	0-1	0-1
43	Acct-Output-Octets	0	0-1	0-1
44	Acct-Session-Id	1	1	1
47	Acct-Input-Packets	0	0-1	0-1
48	Acct-Output-Packets	0	0-1	0-1
50	Acct-Multi-Session-Id	1	1	1
52	Acct-Input-Gigawords	0	0-1	0-1
53	Acct-Output-Gigawords	0	0-1	0-1
26-6527-151	Alc-Sub-Serv-Activate	1	1	1

Large Scale NAT (LSN) Accounting

Table 56: LSN Accounting (description)

Attribute ID	Attribute Name	Description
1	User-Name	Refers to the user-name reported in Accounting for subscriber-aware or subscriber-unaware Large Scale NAT users. The reported format for subscriber-unaware users is LSN44@, DS-lite@ or NAT64@ followed by the users inside ipv4 or ipv6 address. The reported format and length for subscriber-aware users is configured and driven by **configure router nat inside subscriber-identification** and send when user-name is included under **configure aaa isa-radius-policy** <*name*>. This attribute has the same content as [26-6527-11] Alc-Subsc-ID-Str for subscriber-unaware Large Scale NAT users.
4	NAS-IP-Address	The identifying IP Address of the NAS requesting the Authentication or Accounting and maps to the ipv4 address from the system interface (**configure router interface system address** <*ip-address*>).
5	NAS-Port	Unique 32 bit encoded number [31..0] that holds the MS-ISA MDA used for LSN accounting. The following formatting is used [3 bits 31..29 value 000], [4 bits 28..25 value slot-ms-isa], [4 bits 24..21 value mda-nbr-ms-isa], [6 bits 20..15 000010], [15 bits 14..0 0000 0000 0000 0000].
8	Framed-IP-Address	Refers to the inside private IP address of the user (LSN44) and send when framed-ip-addr is included in **configure aaa isa-radius-policy** <*name*>.
30	Called-Station-Id	Holds information to which nat-group and nat-member the NAT user belongs. The format of this attribute is a string 00-00-00-00-<NatGroup>-<NatMember>. The command **show isa nat-group** holds the link between ms-isa mda, NatGroup and NatMember. Optionally sent when called-station-id is included under **configure aaa isa-radius-policy** <*name*>.
32	NAS-Identifier	A string (**configure system name** <*system-name*>) identifying the NAS originating the Authentication or Accounting requests and sent when nas-identifier is included for the corresponding application: configure subscriber-mgmt authentication-policy (ESM authentication), **configure subscriber-mgmt radius-accounting-policy** (ESM accounting), **configure aaa isa-radius-policy** (LSN accounting, WLAN-GW soft-gre) and **configure aaa l2tp-accounting-policy** (L2TP accounting).
42	Acct-Input-Octets	Indicates how many Layer 3 octets have been sent to this nat user over the course of this service being provided and send together with [43] Acct-Output-Octets, [52] Acct-Input-Gigawords and [53] Acct-Output-Gigawords when octet-counters is included under **configure aaa isa-radius-policy** <*name*>.

Table 56: LSN Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
43	Acct-Output-Octets	Indicates how many L3 octets have been received from this nat user over the course of this service being provided and send together with [42] Acct-Input-Octets, [52] Acct-Input-Gigawords and [53] Acct-Output-Gigawords when octet-counters is included under **configure aaa isa-radius-policy** <*name*>.
44	Acct-Session-Id	This unique 16 bytes attribute has two different behaviors. If multi-session-id is not included under **configure aaa isa-radius-policy** <*name*> then multiple port-ranges for the same user are all reported with a common 16 bytes [44] Acct-Session-id for the different port-ranges and reported via start, interim and stop accounting messages and without attribute [50] Acct-Multi-Session-Id. If multi-session-id is configured under **configure aaa isa-radius-policy** <*name*> then multiple port-ranges for the same user are reported with different 16 bytes [44] Acct-Session-id via start and stop accounting messages with an additional common 16 bytes attribute [50] Acct-Multi-Session-Id. For an accounting-on and accounting-off the first 8 bytes from the 16 bytes are put to zero.
46	Acct-Session-Time	Reports the elapsed time in seconds the user has allocated an unique port-range in accounting start, interim or stop. For accounting-off it reports the elapsed time in second since the last accounting-on.
47	Acct-Input-Packets	Indicates how many packets have been send for this nat user over the course of this service being provided and send together with [48] Acct-Output-Packets when frame-counters is included under **configure aaa isa-radius-policy** <*name*>.
48	Acct-Output-Packets	Indicates how many packets have been received for this nat user over the course of this service being provided and send together with [47] Acct-Input-Packets when frame-counters is included under **configure aaa isa-radius-policy** <*name*>.
49	Acct-Terminate-Cause	Indicates why a specific NAT port-range is released in Acct-Stop messages. Cause host-Request is used If the last port-range for this NAT user is freed and cause port-unneeded is used when we release a port-range which is not the last one (multiple port-ranges) for this NAT user. Cause [10]Nas-request is reported in Accounting-Off and cause [11]Nas-reboot is reported in Accounting-on. This attribute is only send when release-reason is included under **configure aaa isa-radius-policy** <*name*>.

Table 56: LSN Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
50	Acct-Multi-Session-Id	This unique 16 bytes attribute has two different behaviors. If multi-session-id is not included under **configure aaa isa-radius-policy** <*name*> then multiple port-ranges for the same user are all reported with a common 16 bytes [44] Acct-Session-id for the different port-ranges and reported via start, interim and stop accounting messages and without attribute [50] Acct-Multi-Session-Id. If multi-session-id is yes included under **configure aaa isa-radius-policy** <*name*> then multiple port-ranges for the same user are reported with different 16 bytes [44] Acct-Session-id via start and stop accounting messages with an additional common 16 bytes attribute [50] Acct-Multi-Session-Id.
52	Acct-Input-Gigawords	Indicates how many times (zero or more) the [42] Acct-Input-Octets counter has wrapped around 2^32 in the course of delivering this service and send together with [42] Acct-Input-Octets, [43] Acct-Output-Octets and [53] Acct-Output-Gigawords when octet-counters is included under **configure aaa isa-radius-policy** <name.
53	Acct-Output-Gigawords	Indicates how many times (zero or more) the [43] Acct-Output-Octets counter has wrapped around 2^32 in the course of delivering this service and send together with [42] Acct-Input-Octets, [43] Acct-Output-Octets and [52] Acct-Input-Gigawords when octet-counters is included under **configure aaa isa-radius-policy** <*name*>.
55	Event-Timestamp	Record the time that this event occurred on the NAS, in seconds since January 1, 1970 00:00 UTC and send when hardware-timestamp is included under **configure aaa isa-radius-policy** <*name*>.
97	Framed-IPv6-Prefix	Inside private ipv6address of the user (NAT64,DSLITE) and send when framed-ip-addr is included under **configure aaa isa-radius-policy** <*name*>.
26-6527-11	Alc-Subsc-ID-Str	The reported format is LSN44@, DS-lite@ and NAT64@ followed by the users inside ipv4 or ipv6 address and send when nat-subscriber-string is included under **configure aaa isa-radius-policy** <*name*>. This attribute has the same content as [1]User-Name for subscriber-unaware Large Scale NAT users.
26-6527-100	Alc-Serv-Id	Refers in the Accounting-Request to the inside VRF used for LSN subscribers using RADIUS LSN accounting (**configure aaa isa-radius-policy nat acct-include-attributes inside-service-id**). The outside VRF is reported via [26-6527-140] Alc-Nat-Outside-Serv-Id and both attributes are not included if instance's are Base.

Table 56: LSN Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
26-6527-121	Alc-Nat-Port-Range	Holds for the NAT user his public outside ipv4 address, his assigned outside public port range and the outside routing instance. For LSN accounting, the attribute is sent when port-range-block is included under **configure aaa isa-radius-policy**. The attribute is also sent for ESM subscriber accounting if NAT is enabled and if configured in **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute nat-port-range**.
26-6527-140	Alc-Nat-Outside-Serv-Id	Refers to the public outside service-id and send when outside-service-id is included under **configure aaa isa-radius-policy** and the *service-id* is different than the base instance.
26-6527-141	Alc-Nat-Outside-Ip-Addr	Holds for the NAT user his public outside ipv4 address and send when outside-ip is included under **configure aaa isa-radius-policy** <*name*>. The content of this attribute is identical to the outside ipv4 address in [26-6527-121] Alc-Nat-Port-Range.

Table 57: LNS Accounting (limits)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
1	User-Name	string	[32|64] chars	Subscriber unaware: LSN44@<ipaddr>, DS-lite@<ipv6addr> and NAT64@<ipv6addr>Subscriber aware: format and length depends on the subscriber-identification attribute configuration- attribute-type alc-sub-string max 32 chars- attribute-type user-name , class and station-id max 64 chars- attribute-type imsi and imei max 32 chars For example:# subscriber unaware: NAT64 host ipv6 address 2001::0001User-Name = NAT64@2001:0000:0000:0000:0000:0000:0000:0001# subscriber aware: NAS subscriber-id = private-user1 and subscriber-identification alc-sub-stringUser-Name = private-user1
4	NAS-IP-Address	ipaddr	4 Bytes	For example:# ip-address 10.1.1.1NAS-IP-Address 0a010101
5	NAS-Port	integer	4 Bytes	For example:# MS-ISA MDA 1/2 # 1/2/nat-out-ip corresponds to [000] [slot 0001] [mda 0010] [nat-outip 00010] [000 0000 0000 0000] : value 37814272# note : nat-out-ip is translated value 2 (00010) and it represents the logical port on the ms-isa (show port 1/2 returns all virtual ports)NAS-Port = 37814272
8	Framed-IP-Address	ipaddr	4 Bytes	For example:# private inside ipv4address LSN44 user192.168.0.1Framed-IP-Address = 192.168.0.1
30	Called-Station-Id	string	17 Bytes	00-00-00-00-<natgroup>-<natmember> For example:# nat group 1 and nat member 1# Called-Station-Id = 30302d30302d30302d30302d30312d30312dCalled-Station-Id = 00-00-00-00-01-01
32	NAS-Identifier	string	32 chars	For example:NAS-Identifier = PE1-Antwerp
42	Acct-Input-Octets	integer	4 Bytes	For example:Acct-Input-Octets = 5000
43	Acct-Output-Octets	integer	4 Bytes	For example:Acct-Output-Octets = 2000

Table 57: LNS Accounting (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
44	Acct-Session-Id	string	32 bytes	No useful information can be extracted from the string. For example:# internal generated asid 32 Bytes/16 chars: 0x3466666434383332306232313436393738363238346262323339326462636232Acct-Session-Id = 4ffd48320b21469786284bb2392dbcb2
46	Acct-Session-Time	integer	4 Bytes 4294967295 seconds	For example:Acct-Session-Time = 870
47	Acct-Input-Packets	integer	4 Bytes 4294967295 packets	For example:Acct-Input-Packets = 15200
48	Acct-Output-Packets	integer	4 Bytes 4294967295 packets	For example:Acct-Output-Packets = 153537
49	Acct-Terminate-Cause	integer	4 Bytes	See also table Acct Terminate Cause 10=Nas-Request, 11=Nas-Reboot, 14=Port-Suspended, 18=Host-Request For example:Acct-Terminate-Cause = Port-unneeded
50	Acct-Multi-Session-Id	string	32 bytes	No useful information can be extracted from the string. For example:# internal generated asid 32 Bytes/16 chars: 0x3566666434383332306232313436393738363238346262323339326462636232Acct-Multi-Session-Id = 5ffd48320b21469786284bb2392dbcb2
52	Acct-Input-Gigawords	integer	4 Bytes	For example:# no overflowAcct-Input-Gigawords = 0
53	Acct-Output-Gigawords	integer	4 Bytes	For example:# no overflowAcct-Output-Gigawords = 0
55	Event-Timestamp	date	4 Bytes	For example:# Jul 6 2012 17:28:23 CEST is reported as 4FF70417Event-Timestamp = 4FF70417
97	Framed-IPv6-Prefix	ipv6prefix	max. 16 Bytes for prefix + 1 byte for length	private inside ipv6address of nat64 or DSlite user For example: Framed-IPv6-Prefix = 2001::1/128

Table 57: LNS Accounting (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-11	Alc-Subsc-ID-Str	string	32 chars	LSN44@<ipaddr>, DS-lite@<ipv6addr> and NAT64@<ipv6addr> For example:Alc-Subsc-ID-Str = LSN44@192.168.0.1Alc-Subsc-ID-Str = DS-Lite@2001:0000:0000:0000:0000:0000:0000:0001Alc-Subsc-ID-Str = NAT64@2002:0000:0000:0000:0000:0000:0000:0001
26-6527-100	Alc-Serv-Id	integer	2147483647 id	For example:# inside vprn-id 100Alc-Serv-Id = 100
26-6527-121	Alc-Nat-Port-Range	string	no limits	<public-ip><space><port-range><space><outside-routing-instance> For example:# public pool address 180.0.1.248; port-range [37674..37723] in BaseAlc-Nat-Port-Range = 180.0.1.248 37674-37723 router base
26-6527-140	Alc-Nat-Outside-Serv-Id	integer	2147483647 id	For example:# outside vpn-id 200Alc-Nat-Outside-Serv-Id = 200
26-6527-141	Alc-Nat-Outside-Ip-Addr	ipaddr	4 bytes	For example: Alc-Nat-Outside-Ip-Addr = 180.0.1.248

Table 58: LSN Accounting (applicability)

Attribute ID	Attribute Name	Acct Start	Acct Stop	Acct Interim-Update	Acct On	Acct Off
1	User-Name	0-1	0-1	0-1	0	0
4	NAS-IP-Address	1	1	1	1	1
5	NAS-Port	1	1	1	1	1
8	Framed-IP-Address	0-1	0-1	0-1	0	0
30	Called-Station-Id	0-1	0-1	0-1	0-1	0-1
32	NAS-Identifier	0-1	0-1	0-1	0-1	0-1

Table 58: LSN Accounting (applicability) (Continued)

Attribute ID	Attribute Name	Acct Start	Acct Stop	Acct Interim-Update	Acct On	Acct Off
42	Acct-Input-Octets	0	0-1	0-1	0	0
43	Acct-Output-Octets	0	0-1	0-1	0	0
44	Acct-Session-Id	1	1	1	1	1
46	Acct-Session-Time	1	1	1	1	1
47	Acct-Input-Packets	0-1	0-1	0-1	0	0
48	Acct-Output-Packets	0-1	0-1	0-1	0	0
49	Acct-Terminate-Cause	0	0-1	0	0-1	0-1
50	Acct-Multi-Session-Id	0-1	0-1	0	0	0
52	Acct-Input-Gigawords	0	0-1	0-1	0	0
53	Acct-Output-Gigawords	0	0-1	0-1	0	0
55	Event-Timestamp	0-1	0-1	0-1	0-1	0-1
97	Framed-IPv6-Prefix	0-1	0-1	0-1	0	0
26-6527-11	Alc-Subsc-ID-Str	0-1	0-1	0-1	0	0
26-6527-100	Alc-Serv-Id	0-1	0-1	0-1	0	0
26-6527-121	Alc-Nat-Port-Range	0-1	0-1	0-1	0	0
26-6527-140	Alc-Nat-Outside-Serv-Id	0-1	0-1	0-1	0	0
26-6527-141	Alc-Nat-Outside-Ip-Addr	0-1	0-1	0-1	0	0

L2TP Tunnel Accounting

Table 59: L2TP Tunnel Accounting (description)

Attribute ID	Attribute Name	Description
1	User-Name	Refers to the PPPoE user-name
4	NAS-IP-Address	The identifying IP Address of the NAS requesting the Authentication or Accounting. Included when the RADIUS server is reachable via IPv4. The address is determined by the routing instance through which the RADIUS server can be reached: “Management” — The active ipv4 address in the Boot Options File (**bof address** <*ipv4-address*>) “Base” or “VPRN” — The ipv4 address of the system interface (**configure router interface system address** <*address*>). The address can be overwritten with the configured source-address (**configure aaa radius-server-policy** <*policy-name*> **servers source-address** <*ip-address*>).
5	NAS-Port	The physical access-circuit on the NAS which is used for the Authentication or Accounting of the user. The format of this attribute is configurable on the NAS as a fixed 32 bit value or a parameterized 32 bit value. The parameters can be a combination of outer-vlan-id(o), inner-vlan-id(i), slot number(s), MDA number(m), port number or lag-id(p), ATM VPI(v) and ATM VCI(c), fixed bit values zero (0) or one (1) but cannot exceed 32 bit. The format can be configured for following applications: **configure aaa l2tp-accounting-policy** <*name*> **include-radius-attribute nas-port**, **configure router l2tp cisco-nas-port**, **configure service vprn** <*service-id*> **l2tp cisco-nas-port**, **configure subscriber-mgmt authentication-policy** <*name*> **include-radius-attribute nas-port**, **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute nas-port**.
6	Service-Type	The type of service the PPPoE user has requested, or the type of service to be provided for the PPPoE user. Optional in RADIUS-Accept and CoA. Treated as a session setup failure if different from Framed-User.
32	NAS-Identifier	A string (**configure system name** <*system-name*>) identifying the NAS originating the Authentication or Accounting requests and sent when nas-identifier is included for the corresponding application: **configure subscriber-mgmt authentication-policy** (ESM authentication), **configure subscriber-mgmt radius-accounting-policy** (ESM accounting), **configure aaa isa-radius-policy** (LSN accounting, WLAN-GW soft-gre) and **configure aaa l2tp-accounting-policy** (L2TP accounting).

Table 59: L2TP Tunnel Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
41	Acct-Delay-Time	Indicates how many seconds the client has been trying to send this accounting record for. This attribute is included with value 0 in all initial accounting messages. Attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute no acct-delay-time.**
42	Acct-Input-Octets	Tunnel-link and Tunnel level accounting uses the ESM accounting statistics. For Tunnel Link Stop it reports the input bytes for this user over the course of this service being provided. For Tunnel Stop this attribute represent an aggregate of input bytes of all sessions that belong(ed) to this tunnel over the course of this service being provided. Attribute [52] Acct-Output-Gigawords indicates how many times (if greater than zero) the [42] Acct-Input-Octets counter has wrapped around 2^32 in the course of delivering this service.
43	Acct-Output-Octets	Tunnel-link and Tunnel level accounting uses the ESM accounting statistics. For Tunnel Link Stop it reports the output bytes for this user over the course of this service being provided. For Tunnel Stop this attribute represent an aggregate of output bytes of all sessions that belong(ed) to this tunnel over the course of this service being provided. Attribute [53] Acct-Output-Gigawords indicates how many times (if bigger than zero) the [43] Acct-Output-Octets counter has wrapped around 2^32 in the course of delivering this service.
44	Acct-Session-Id	Is a unique generated number and maps for the Tunnel-link stop to the accounting-session-id from the PPPoE session (show service id ppp session detail). For Tunnel-stop accounting it is longer and a concatenation of start-time and connection-id with delimiter .. The start-time equals to the node uptime reported in Timeticks (nd:hh:mm:ss:ts) and value/6000 gives the uptime in minutes. The connection-id equals {tunnel-id * 65536} and the tunnel-id maps to L2TP AVP 9 Assigned Tunnel Id.
46	Acct-Session-Time	Reports the elapsed time in seconds over the course of this service (L2TP session or L2TP tunnel) being provided.
47	Acct-Input-Packets	Tunnel-link and Tunnel level accounting uses the ESM accounting statistics. For Tunnel Link Stop it reports the input packets for this user over the course of this service being provided. For Tunnel Stop this attribute represent an aggregate of input packets of all sessions that belong/belonged to this tunnel over the course of this service being provided.
48	Acct-Output-Packets	Tunnel-link and Tunnel level accounting uses the ESM accounting statistics. For Tunnel Link Stop it reports the output packets for this user over the course of this service being provided. For Tunnel Stop this attribute represent an aggregate of output packets of all sessions that belong/belonged to this tunnel over the course of this service being provided.
49	Acct-Terminate-Cause	indicates how the L2TP session or L2TP tunnel was terminated

Table 59: L2TP Tunnel Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
52	Acct-Input-Gigawords	Indicates how many times (zero or more) the [42] Acct-Input-Octets counter has wrapped around 2^32 in the course of delivering this service.
53	Acct-Output-Gigawords	Indicates how many times (zero or more) the [43] Acct-Output-Octets counter has wrapped around 2^32 in the course of delivering this service.
55	Event-Timestamp	Record the time that this event occurred on the NAS, in seconds since January 1, 1970 00:00 UTC
61	NAS-Port-Type	The type of the physical port of the NAS which is authenticating the user and value automatically determined from subscriber SAP encapsulation. It can be overruled by configuration. Included only if include-radius-attribute nas-port-type is added per application: **configure subscriber-mgmt authentication-policy** (ESM authentication), **configure subscriber-mgmt radius-accounting-policy** (ESM accounting), **configure aaa isa-radius-policy** (LSN accounting, WLAN-GW soft-gre) and **configure aaa l2tp-accounting-policy** (L2TP accounting). Checked for correctness if returned in CoA.
64	Tunnel-Type	The tunneling protocol(s) to be used (in the case of a tunnel initiator) or the tunneling protocol in use (in the case of a tunnel terminator). This attribute is mandatory on LAC Access-Accept and needs to be L2TP. The same attribute is included on LNS in the Access-Request and Acct-Request if the CLI RADIUS policy include-radius-attribute tunnel-server-attrs is enabled on 7x50 LNS. For L2TP Tunnel/Link Accounting this attribute is always included on LAC and LNS.
65	Tunnel-Medium-Type	Which transport medium to use when creating a tunnel for those protocols (such as L2TP) that can operate over multiple transports. This attribute is mandatory on LAC Access-Accept and needs to be IP or 'IPv4.The same attribute is included on LNS in the Access-Request and Acct-Request if the CLI RADIUS policy include-radius-attribute tunnel-server-attrs is enabled on 7x50 LNS. For L2TP Tunnel/Link Accounting this attribute is always included on LAC and LNS.
66	Tunnel-Client-Endpoint	The dotted-decimal IP address of the initiator end of the tunnel. Pre-configured values are used when attribute is omitted (**configure router/ service vprn** <*service-id*> **l2tp local-address**). If omitted in Access Accept on LAC and no local-address configured, then the address is taken from the interface with name **system**. This attribute is included on LNS in the Access-Request and Acct-Request only if the CLI RADIUS policy include-radius-attribute tunnel-server-attrs is enabled on 7x50 LNS. For L2TP Tunnel/Link Accounting this attribute is always included on LAC and LNS as untagged.
67	Tunnel-Server-Endpoint	The dotted-decimal IP address of the server end of the tunnel and is on the LAC the dest-ip for all L2TP packets for that tunnel.

Table 59: L2TP Tunnel Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
68	Acct-Tunnel-Connection	Indicates the identifier assigned to the tunnel session. For Tunnel start/stop it is a concatenation, without delimiter, of LAC-tunnel-id (4bytes) and LNS-tunnel-id (4 bytes)" were the LAC-tunnel-id maps to the hex value of L2TP AVP 9 AssignedTunnelId from SCCRQ and LNS-tunnel-id maps to the hex value L2TP AVP 9 AssignedTunnelId in SCCRP. Unknown tunnel-id's (Tunnel Reject and Tunnel Link Reject) are reported as 0000 or ffff. For Tunnel Link Start/Stop it maps to the integer Call Serial Number from ICRQ L2TP AVP 15 Call Serial Number
82	Tunnel-Assignment-ID	Indicates to the tunnel initiator the particular tunnel to which a session is to be assigned. Some tunnelling protocols, such as PPTP and L2TP, allow for sessions between the same two tunnel endpoints to be multiplexed over the same tunnel and also for a given session to utilize its own dedicated tunnel.
86	Acct-Tunnel-Packets-Lost	Indicates the number of packets dropped and uses the ESM accounting statistics for this. For Tunnel Link Stop it reports an aggregate of the dropped input and output packets for this user over the course of this service being provided. For Tunnel Stop this attribute represent an aggregate of input and output dropped packets of all sessions that belong/belonged to this tunnel over the course of this service being provided.
87	NAS-Port-Id	LAC : a text string identifying the physical access circuit (slot/mda/port/outer-vlan.inner-vlan) of the user that requested the Authentication and/or Accounting. The physical port on LAC can have an optional prefix-string (max 8 chars) and suffix-string (max 64 chars) added (**configure aaa l2tp-accounting-policy** <*policy-name*> **include-radius-attribute nas-port-id prefix-string** <*string*> suffix(circuit-id|remote-id)). LNS: a text string identifying the logical access circuit of the user that requested the Authentication and/or Accounting. This logical access circuit is a fixed concatenation (delimiter #) of routing instance, tunnel-server-endpoint, tunnel-client-endpoint, local-tunnel-id, remote-tunnel-id, local-session-id, remote-session-id and call sequence number.
90	Tunnel-Client-Auth-ID	Used during the authentication phase of tunnel establishment and copied by the LAC in L2TP SCCRQ AVP 7 Host Name. Reported in L2TP Tunnel/Link accounting when length is different from zero. The value with tag 0 is used as default for the tunnels where the value is not specified. Pre-configured values are used when the attribute is omitted (**configure router/service vprn** <*service-id*> **l2tp local-name**). The Node system-name is copied in AVP Host Name if this attribute is omitted and no local-name is configured.
91	Tunnel-Server-Auth-ID	Used during the authentication phase of tunnel establishment and reported in L2TP Tunnel/Link accounting when length is different from zero. For authentication the value of this attribute is compared with the value of AVP 7 Host Name from the received LNS SCCRP. Authentication from LAC point of view passes if both attributes are the same. This authentication check is not performed if the RADIUS attribute is omitted.

Table 59: L2TP Tunnel Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
95	NAS-IPv6-Address	The identifying IP address of the NAS requesting the Authentication or Accounting. Included when the RADIUS server is reachable via IPv6. The address is determined by the routing instance through which the RADIUS server can be reached: “Management” — The active ipv6 address in the Boot Options File (**bof address** <*ipv6-address*>) “Base” or “VPRN” — The ipv6 address of the system interface (**configure router interface system ipv6 address** <*ipv6-address*>). The address can be overwritten with the configured ipv6-source-address (**configure aaa radius-server-policy** <*policy-name*> **servers ipv6-source-address** <*ipv6-address*>).

Table 60: L2TP Tunnel Accounting (limits)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
1	User-Name	string	253 Bytes	Format depends on authentication method and configuration. For example: User-Name user1@domain1.com
4	NAS-IP-Address	ipaddr	4 Bytes	# ip-address For example: NAS-IP-Address= 192.0.2.1
5	NAS-Port	integer	4 Bytes	nas-port <binary-spec> <binary-spec> = <bit-specification> <binary-spec> <bit-specification> = 0 | 1 | <bit-origin> <bit-origin> = *<number-of-bits><origin> <number-of-bits> = [1..32] <origin> = o (outer VLAN ID), i (inner VLAN ID), s (slot number), m (MDA number), p (port number or lag-id), v (ATM VPI), c (ATM VCI) For example : # configured nas-port *12o*10i*3s*2m*5p for SAP 2/2/4:221.7 corresponds to 000011011101 0000000111 010 10 00100 NAS-Port = 231742788
6	Service-Type	integer	2 (mandatory value)	PPPoE and PPPoL2TP hosts only For example: Service-Type = Framed-User
32	NAS-Identifier	string	32 chars	For example:NAS-Identifier = PE1-Antwerp
41	Acct-Delay-Time	integer	4294967295 seconds	For example:# initial accounting start Acct-Delay-Time = 0# no ack and retry after 5 seconds Acct-Delay-Time = 5
42	Acct-Input-Octets	integer	4 Bytes	For example:Acct-Input-Octets = 5000
43	Acct-Output-Octets	integer	4 Bytes	For example:Acct-Output-Octets = 2000
44	Acct-Session-Id	string	[17|22] Bytes	Tunnel number format : <uptime><.><connection-id>Tunnel-link number format : Corresponds to PPPoE session ASID (No useful information can be extracted from the string). For example:# for tunnel accountingAcct-Session-Id = 18120579.84213760# for tunnel-link accountingAcct-Session-Id = 241AFF0000029B4FD5C03E
46	Acct-Session-Time	integer	4 Bytes4294967295 seconds	For example:Acct-Session-Time = 870

Table 60: L2TP Tunnel Accounting (limits)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
47	Acct-Input-Packets	integer	4 Bytes4294967295 packets	For example:Acct-Input-Packets = 213
48	Acct-Output-Packets	integer	4 Bytes4294967295 packets	For example:Acct-Output-Packets = 214
49	Acct-Terminate-Cause	integer	4 Bytes	See also table Acct Terminate Cause 1=User-Request, 2=Lost-Carrier, 9=NAS-Error, 10=NAS-Request, 11=NAS-Reboot, 15=Service-Unavailable For example:Acct-Terminate-Cause = NAS-Request
52	Acct-Input-Gigawords	integer	4 Bytes	For example:# no overflowAcct-Input-Gigawords = 0
53	Acct-Output-Gigawords	integer	4 Bytes	For example:# no overflowAcct-Output-Gigawords = 0
55	Event-Timestamp	date	4 Bytes	For example:# Jul 6 2012 17:28:23 CEST is reported as 4FF70417Event-Timestamp = 4FF70417
61	NAS-Port-Type	integer	4 Bytes Values [0..255]	Values as defined in rfc-2865 and rfc-4603For LNS, the value is set to virtual (5) For example: NAS-Port-Type = PPPoEoQinQ (34)
64	Tunnel-Type	integer	3 (mandatory value)	Mandatory 3=L2TP For example:Tunnel-Type = L2TP
65	Tunnel-Medium-Type	integer	1 (mandatory value)	Mandatory 1=IP or IPv4 For example:Tunnel-Medium-Type = IP
66	Tunnel-Client-Endpoint	string	19 or 20 bytes (untagged/ tagged)	<Tag field><dotted-decimal IP address used on LAC as L2TP src-ip>If Tag field is greater than 0x1F, it is interpreted as the first byte of the following string field For example: # untagged Tunnel-Client-Endpoint = 312e312e312e31Tunnel-Client-Endpoint = 1.1.1.1# tagged 0 Tunnel-Client-Endpoint = 00312e312e312e31Tunnel-Client-Endpoint:0 = 1.1.1.1# tagged 1 Tunnel-Client-Endpoint = 01312e312e312e31Tunnel-Client-Endpoint:1 = 1.1.1.1

Table 60: L2TP Tunnel Accounting (limits)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
67	Tunnel-Server-Endpoint	string	19 or 20 bytes (untagged/ tagged)	<Tag field><dotted-decimal IP address used on LAC as L2TP dst-ip>If Tag field is greater than 0x1F, it is interpreted as the first byte of the following string field For example: # tagged 1 Tunnel-Server-Endpoint = 01332e332e332e31Tunnel-Server-Endpoint:1 = 3.3.3.3
68	Acct-Tunnel-Connection	string	[4|8] bytes	tunnel-start/stop : 8 Byte value representing the lac + lns tunnel-id converted in hexadecimallink-start/ stop : maps to the AVP 15 call Serial Number from ICRQ (32 bit)
82	Tunnel-Assignment-ID	string	32 chars	For example: Tunnel-Assignment-ID = Tunnel-1
86	Acct-Tunnel-Packets-Lost	integer	4 Bytes	Sum of all dropped packets on ingress and egress For example:Acct-Tunnel-Packets-Lost = 748
87	NAS-Port-Id	string	no limits	LAC : <prefix><space><slot/mda/ port:vlan|vpi.vlan|vci><space> <suffix> - prefix : configurable string 8 chars max - suffix : remote-id (max 64 chars) | circuit-id (max 64 chars)LNS : pre-defined format - LNS rtr-2#lip-3.3.3.3#rip-1.1.1.1#ltid-11381#rtid-1285#lsid-30067#rsid-19151#347
90	Tunnel-Client-Auth-ID	string	64 chars.	For example: Tunnel-Client-Auth-Id:0 = LAC-Antwerp-1
91	Tunnel-Server-Auth-ID	string	64 chars.	For example: Tunnel-Server-Auth-ID:0 = LNS-Antwerp-1
95	NAS-IPv6-Address	ipv6addr	16 Bytes	# ipv6-address For example: NAS-IPv6-Address = 2001:db8::1

Table 61: L2TP Tunnel Accounting (applicability)

Attibute ID	Attribute Name	Acct Tunnel-Start	Acct Tunnel-Stop	Acct Tunnel-Reject	Acct Tunnel-Link-Start	Acct Tunnel-Link-Stop	Acct Tunnel-Link-Reject
1	User-Name	0	0	0	1	1	1
4	NAS-IP-Address	0-1	0-1	0-1	0-1	0-1	0-1
5	NAS-Port	0	0	0	0-1	0-1	0-1
6	Service-Type	0	0	0	1	1	1
32	NAS-Identifier	0-1	0-1	0-1	0-1	0-1	0-1
41	Acct-Delay-Time	1	1	1	1	1	1
42	Acct-Input-Octets	0	1	0	0	1	0
43	Acct-Output-Octets	0	1	0	0	1	0
44	Acct-Session-Id	1	1	1	1	1	1
46	Acct-Session-Time	0	1	0	0	1	0
47	Acct-Input-Packets	0	1	0	0	1	0
48	Acct-Output-Packets	0	1	0	0	1	0
49	Acct-Terminate-Cause	0	1	1	0	1	1
52	Acct-Input-Gigawords	0	0-1	0	0	0-1	0
53	Acct-Output-Gigawords	0	0-1	0	0	0-1	0
55	Event-Timestamp	1	1	1	1	1	1
61	NAS-Port-Type	0	0	0	0-1	0-1	0-1
64	Tunnel-Type	1	1	1	1	1	1
65	Tunnel-Medium-Type	1	1	1	1	1	1
66	Tunnel-Client-Endpoint	1	1	1	1	1	1
67	Tunnel-Server-Endpoint	1	1	1	1	1	1
68	Acct-Tunnel-Connection	1	1	1	1	1	0

Table 61: L2TP Tunnel Accounting (applicability) (Continued)

Attibute ID	Attribute Name	Acct Tunnel-Start	Acct Tunnel-Stop	Acct Tunnel-Reject	Acct Tunnel-Link-Start	Acct Tunnel-Link-Stop	Acct Tunnel-Link-Reject
82	Tunnel-Assignment-ID	1	1	1	1	1	1
86	Acct-Tunnel-Packets-Lost	0	1	0	0	1	0
87	NAS-Port-Id	0	0	0	0-1	0-1	0-1
90	Tunnel-Client-Auth-ID	1	1	1	1	1	1
91	Tunnel-Server-Auth-ID	1	1	0	1	1	1
95	NAS-IPv6-Address	0-1	0-1	0-1	0-1	0-1	0-1

Application Assurance (AA) Accounting

Table 62: Application Assurance Accounting (description)

Attribute ID	Attribute Name	Description
1	User-Name	The AA-subscriber reported in AA Accounting statistics and included in Start, Interim and Stop Accounting messages. This attribute has the same content as [26-6527-11] Alc-Subsc-ID-Str for AA RADIUS Accounting.
4	NAS-IP-Address	The identifying IP Address of the NAS requesting the Accounting and maps to the ipv4 address from the system interface (**configure router interface system address** <*ip-address*>). Allows to monitor node redundancy activity switch.
32	NAS-Identifier	A string (**configure system name** <system-name>) identifying the NAS originating the AA Accounting requests. It is sent in all accounting messages. Allows to monitor node redundancy activity switch.
40	Acct-Status-Type	Indicates AA Acct request type. Acct On is sent each time a RADIUS accounting policy (**configure application-assurance radius-accounting-policy** <*rad-acct-plcy-name*>) is enabled under a partition (**configure application-assurance group** <aa-*group-id:partition-id*> **statistics aa-sub radius-accounting-policy** <*rad-acct-plcy-name*>) or after a node reboot. An Acct Start is sent for each new AA-subscriber created under a partition were radius accounting is enabled. An Acct Interim will be sent every configured interval time (**configure application-assurance radius-accounting-policy** <*rad-acct-plcy-name*> **interim-update-interval** <*minutes*>) for each AA-subscriber under a partition with the radius-accounting policy applied. An Acct Stop is sent at AA-subscriber removal. An application-profile change or an Application-Service-Options [ASO] override against a subscriber will not trigger Acct Start/Stop messages and do not affect the AA RADIUS Acct session.
44	Acct-Session-Id	Unique value per node used to identify the AA subscriber accounting session. Reported in accounting Start, Stop and Interim Updates messages. Its value is automatically derived from the subscriber ID string ([26-6527-11] Alc-Subsc-ID-Str) and the AA subscriber type, that guarantees to preserve the subscriber session ID after ISA card redundancy activity switch or after a node redundancy activity switch (in AARP context). An activity switch will not modify the session id, but can be detected if needed thanks to the [26-6527-156] Alc-AA-Group-Partition-Isa-Id or the [32] NAS-Identifier. The AA RADIUS Acct session is independent from the ESM RADIUS Acct session. An AA Acct Off is sent when accounting stats is disabled (removing of radius-acct policy)
49	Acct-Terminate-Cause	Indicates how the session was terminated.

Table 62: Application Assurance Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
55	Event-Timestamp	Record the time that this event occurred on the NAS, in seconds since January 1, 1970 00:00 UTC
26-6527-11	Alc-Subsc-ID-Str	AA-subscriber string name, used together with the AA-subscriber type to construct the [44] Acct-Session-Id. Sent in all Acct Start, Interim Updates and Stop messages. This attribute has the same content as [1] User-Name for AA RADIUS Accounting.
26-6527-19	Alc-Acct-I-Inprof-Octets-64	Identify a charging group and his corresponding total ingress in-profile bytes. Report cumulative volume of pre-configured AA-subscriber charging groups since start of the session (as described in RFC2689) in Acct Interim Update or Stop messages.
26-6527-21	Alc-Acct-O-Inprof-Octets-64	Identify a charging group and his corresponding total egress in-profile bytes. Report cumulative volume of pre-configured aa-subscriber charging groups since start of the session (as described in RFC2689) in Acct Interim Update or Acct Stop.
26-6527-23	Alc-Acct-I-Inprof-Pkts-64	Identify a charging group and his corresponding total ingress in-profile packets. Report cumulative volume of pre-configured aa-subscriber charging groups since start of the session (as described in RFC2689) in Acct Interim Update or Acct Stop.
26-6527-25	Alc-Acct-O-Inprof-Pkts-64	Identify a charging group and his corresponding total egress in-profile packets. Report cumulative volume of pre-configured aa-subscriber charging groups since start of the session (as described in RFC2689) in Acct Interim Update or Acct Stop.
26-6527-45	Alc-App-Prof-Str	Designate the AA-subscriber current application profile. Sent in all Acct Start, Interim Update and Stop messages.
26-6527-156	Alc-AA-Group-Partition-Isa-Id	Designate the AA Group/partition and the ISA card assigned to the AA-subscriber reported in the Accounting Statistics. Sent in all Acct requests. The ISA id allows to monitor ISA card switch over.
26-6527-157	Alc-AA-Peer-Identifier	Specifies Application-Assurance RADIUS Peer Information and used by the PCRF(DSC) to autodiscover redundant AA nodes.When AA Seen IP (Seen-IP transit subscriber notification provides RADIUS Accounting Start notification of the IP addresses and location of active subscribers within a parent AA service) is used together with AARP (asymmetry removal that is required to remove routing asymmetry when using redundant transit-aa-nodes), meaning you have 2 redundant transit 7750 node, we expect PCRF(DSC) to push a CoA create to both 7x50 nodes. This is achieved by adding the peer-identifier information in the original Accounting-start sent by the primary 7x50.

Table 63: Application Assurance Accounting (limits)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
1	User-Name	string	32 chars	# format varies with the aa-sub type For example:# sap formataa-sub : 1/1/6:61.2# spoke-sdp formataa-sub : 4:100# esm or transit formataa-sub : user1@domain1.com
4	NAS-IP-Address	ipaddr	4 Bytes	For example:# ip-address 10.1.1.1NAS-IP-Address 0a010101
32	NAS-Identifier	string	32 chars	For example:NAS-Identifier = PE1-Antwerp
40	Acct-Status-Type	integer	4	1=Start, 2=Stop, 3=Interim Update, 7=Accounting-On, 8=Accounting-Off
44	Acct-Session-Id	string	22 Bytes	<subscriber-type>|<Alc-Subsc-ID-str>where <subscriber-type> = esm or transit For example: Acct-Session-Id = esm|ipoe_sub_08
49	Acct-Terminate-Cause	integer	4 Bytes	# Supported causes: 1=User-Request, 2=Lost-Carrier, 3=Lost-Service, 4=Idle-Timeout, 5=Session-Timeout, 6=Admin-Reset, 8=Port-Error, 10=NAS-Request, 15=Service-Unavailable# See table Acct Terminate Cause for complete overview For example:Acct-Terminate-Cause = User-Request
55	Event-Timestamp	date	4 Bytes	For example:# Jul 6 2012 17:28:23 CEST is reported as 4FF70417Event-Timestamp = 4FF70417
26-6527-11	Alc-Subsc-ID-Str	string	16 char	<aa-subscriber text name> For example: Alc-Subsc-ID-Str = ipoe_sub_08
26-6527-19	Alc-Acct-I-Inprof-Octets-64	octets	10 Bytes	<Type of second byte 1 Byte ><Charging-Group export-id 1 Byte><10 Byte value> where <Type of second byte > = 40 indicates byte 2 is AA charging-group export-id where <Charging-Group export-id> = <1…31> For example:# 500 bytes reported in CG id 2Alc-Acct-I-Inprof-Octets-64 = 0x400200000000000001f4
26-6527-21	Alc-Acct-O-Inprof-Octets-64	octets	10 Bytes	<Type of second byte 1 Byte ><Charging-Group export-id 1 Byte><10 Byte value> where <Type of second byte > = 40 indicates byte 2 is AA charging-group export-id where <Charging-Group export-id> = <1…31> For example: Alc-Acct-O-Inprof-Octets-64 = 0x40020000000000651d26

Table 63: Application Assurance Accounting (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
26-6527-23	Alc-Acct-I-Inprof-Pkts-64	octets	10 Bytes	<Type of second byte 1 Byte ><Charging-Group export-id 1 Byte><10 Byte value> where <Type of second byte > = 40 indicates byte 2 is AA charging-group export-idwhere <Charging-Group export-id> = <1…31> For example:Alc-Acct-I-Inprof-Pkts-64 = 0x4002000000001acae3e7
26-6527-25	Alc-Acct-O-Inprof-Pkts-64	octets	10 Bytes	<Type of second byte 1 Byte ><Charging-Group export-id 1 Byte><10 Byte value> where <Type of second byte > = 40 indicates byte 2 is AA charging-group export-id where <Charging-Group export-id> = <1…31> For example:Alc-Acct-O-Inprof-Pkts-64 = 0x400200000000004368c4
26-6527-45	Alc-App-Prof-Str	string	16 char	For example:Alc-App-Prof-Str = MyAppProfile
26-6527-156	Alc-AA-Group-Partition-Isa-Id	string	no limits	<Group ID>:<Partition ID>:<ISA slot>/<ISA MDA> For example:Alc-AA-Group-Partition-Isa-Id = 2:4:3/2
26-6527-157	Alc-AA-Peer-Identifier	string	no limits	<AARP ID>@<Peer IP address>@<Peer Port-id> For example:# system-ip 10.1.1.2 remote redundant transit-aa-node Alc-AA-Peer-Identifier = 200@10.1.1.2@1/1/1/4:200

Table 64: Application Assurance Accounting (applicability)

Attribute ID	Attribute Name	Acct Start	Acct Stop	Acct Interim-Update	Acct On	Acct Off
1	User-Name	1	1	1	0	0
4	NAS-IP-Address	1	1	1	1	1
32	NAS-Identifier	1	1	1	1	1
40	Acct-Status-Type	1	1	1	1	1
44	Acct-Session-Id	1	1	1	0	0
49	Acct-Terminate-Cause	0	0-1	0	0	0
55	Event-Timestamp	1	1	1	1	1
26-6527-11	Alc-Subsc-ID-Str	1	1	1	0	0
26-6527-19	Alc-Acct-I-Inprof-Octets-64	0	0-1	0-1	0	0
26-6527-21	Alc-Acct-O-Inprof-Octets-64	0	0-1	0-1	0	0
26-6527-23	Alc-Acct-I-Inprof-Pkts-64	0	0-1	0-1	0	0
26-6527-25	Alc-Acct-O-Inprof-Pkts-64	0	0-1	0-1	0	0
26-6527-45	Alc-App-Prof-Str	1	1	1	0	0
26-6527-156	Alc-AA-Group-Partition-Isa-Id	1	1	1	1	1
26-6527-157	Alc-AA-Peer-Identifier	0-1	0	0	0	0

Dynamic Data Service accounting

This section specifies the attributes for RADIUS accounting on dynamic data service SAPs. The attributes for RADIUS accounting of the associated control channel is identical as the ESM accounting case (see section Enhanced Subscriber Management (ESM) accounting.

Table 65: Dynamic Data Service Accounting (description)

Attribute ID	Attribute Name	Description
1	User-Name	The RADIUS user-name from the Dynamic Data Service Control Channel associated with this Dynamic Data Service SAP accounting session
4	NAS-IP-Address	The identifying IP Address of the NAS requesting the Authentication or Accounting. Included when the RADIUS server is reachable via IPv4. The address is determined by the routing instance through which the RADIUS server can be reached: “Management” — The active ipv4 address in the Boot Options File (**bof address** <*ipv4-address*>) “Base” or “VPRN” — The ipv4 address of the system interface (**configure router interface system address** <*address*>). The address can be overwritten with the configured source-address (**configure aaa radius-server-policy** <*policy-name*> **servers source-address** <*ip-address*>)
25	Class	The Class attribute from the Dynamic Data Service Control Channel associated with this Dynamic Data Service SAP accounting session
32	NAS-Identifier	A string (**configure system name** <*system-name*>) identifying the NAS originating the Accounting requests.
40	Acct-Status-Type	Indicates whether this Accounting-Request marks the beginning of the user service (Start) or the end (Stop) or reports interim updates.
41	Acct-Delay-Time	Indicates how many seconds the client has been trying to send this accounting record for. This attribute is included with value 0 in all initial accounting messages. Attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** <*name*> **include-radius-attribute no acct-delay-time.**
44	Acct-Session-Id	Unique generated hexadecimal number that represents the accounting session for this Dynamic Data Service SAP.
46	Acct-Session-Time	The acct session time is started when the corresponding dynamic data service sap is created. The acct session time is stopped when the corresponding dynamic data service sap is deleted. When the SAP is orphaned (not deleted in the teardown function call), the session time stops after the teardown script is executed. In case an accounting stop is sent as a result of a failure scenario, the acct-session-time will be zero.

Table 65: Dynamic Data Service Accounting (description) (Continued)

Attribute ID	Attribute Name	Description
49	Acct-Terminate-Cause	Indicates how the accounting session was terminated
50	Acct-Multi-Session-Id	Accounting session id from the associated Control Channel (session acct-session-id for PPPoE sessions and cost acct-session-id for IPoE hosts)
55	Event-Timestamp	Record the time that this event occurred on the NAS, in seconds since January 1, 1970 00:00 UTC
87	NAS-Port-Id	The Dynamic Data Service SAP where this accounting session is started for
95	NAS-IPv6-Address	The identifying IP Address of the NAS requesting the Authentication or Accounting. Included when the RADIUS server is reachable via IPv6. The address is determined by the routing instance through which the RADIUS server can be reached: “Management” — The active ipv6 address in the Boot Options File (**bof address** <*ipv6-address*>) “Base” or “VPRN”— The ipv6 address of the system interface (**configure router interface system ipv6 address** <*ipv6-address*>). The address can be overwritten with the configured ipv6-source-address (**configure aaa radius-server-policy** <*policy-name*> **servers ipv6-source-address** <*ipv6-address*>)
26-3561-1	Agent-Circuit-Id	The Agent-Circuit-Id attribute from the Dynamic Data Service Control Channel associated with this Dynamic Data Service SAP accounting session
26-3561-2	Agent-Remote-Id	The Agent-Remote-Id attribute from the Dynamic Data Service Control Channel associated with this Dynamic Data Service SAP accounting session
26-6527-165	Alc-Dyn-Serv-Script-Params	Parameters as input to the Dynamic Data Service Python script. The parameters can cross an attribute boundary. The concatenation of all Alc-Dyn-Serv-Script-Params attributes with the same tag in a single message must be formatted as function-key <dictionary> where function-key specifies which Python functions will be called and <dictionary> contains the actual parameters in a Python dictionary structure format. In dynamic service RADIUS accounting messages, the attribute is sent untagged and contains the last received Alc-Dyn-Serv-Script-Params value in an Access-Accept or CoA message for this dynamic service. Multiple attributes may be present if the total length does not fit a single attribute.

Table 66: Dynamic Data Service Accounting (limits)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
1	User-Name	string	253 chars	The format depends on authentication method and configuration For example: User-Name user1@domain1.com
4	NAS-IP-Address	ipaddr	4 Bytes	# ip-address For example: NAS-IP-Address “192.0.2.1”
25	Class	octets	253 chars64 chars persistency	For example:Class = This is a Class attribute
32	NAS-Identifier	string	32 chars	For example:NAS-Identifier = PE1-Antwerp
40	Acct-Status-Type	integer	4	1=Start, 2=Stop, 3=Interim Update, 7=Accounting-On, 8=Accounting-Off, 9=Tunnel-Start, 10=Tunnel-Stop, 11=Tunnel-Reject, 12=Tunnel-Link-Start, 13=Tunnel-Link-Stop, 14=Tunnel-Link-Reject, 15=Failed
41	Acct-Delay-Time	integer	4294967295 seconds	For example:# initial accounting start Acct-Delay-Time = 0# no ack and retry after 5 secondsAcct-Delay-Time = 5
44	Acct-Session-Id	string	22 Bytes	For example: # Acct-Session-Id = 24ADFF0000000950C5F138 Acct-Session-Id 0x323132383436333539323130323531323131 33343039
46	Acct-Session-Time	integer	4 Bytes4294967295 seconds	For example:Acct-Session-Time = 870
49	Acct-Terminate-Cause	integer	4 Bytes	Supported causes: 1=User-Request, 2=Lost-Carrier, 3=Lost-Service, 4=Idle-Timeout, 5=Session-Timeout, 6=Admin-Reset, 8=Port-Error, 10=NAS-Request, 15=Service-Unavailable See also table Acct Terminate Cause for complete overview For example:Acct-Terminate-Cause = User-Request
50	Acct-Multi-Session-Id	string	22 bytes	For example:Acct-Multi-Session-Id = 24ADFF0000000250C8EA5E
55	Event-Timestamp	date	4 Bytes	For example:# Jul 6 2012 17:28:23 CEST is reported as 4FF70417Event-Timestamp = 4FF70417

Table 66: Dynamic Data Service Accounting (limits) (Continued)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
87	NAS-Port-Id	string	253 Bytes	Ethernet SAPs:<slot>/<mda>/<port>:<vlan>.<vlan> For example:NAS-Port-Id = 1/1/4:50:100
95	NAS-IPv6-Address	ipv6addr	16 Bytes	# ipv6-address For example: NAS-IPv6-Address = 2001:db8::1
26-3561-1	Agent-Circuit-Id	string	247 chars	Format, see also RFC 4679 # ATM/DSL <Access-Node-Identifier><atm slot/port:vpi.vci># Ethernet/DSL <Access-Node-Identifier><eth slot/port[:vlan-id]> For example: ethernet dslam1 slot 2 port 1 vlan 100Agent-Circuit-Id = dslam1 eth 2/1:100
26-3561-2	Agent-Remote-Id	string	247 chars	format see also RFC 4679 For example: Agent-Remote-Id = MyRemoteId
26-6527-165	Alc-Dyn-Serv-Script-Params	string	multiple VSA's per tag per message. Max length of concatenated strings per tag = 1000 bytes	The script parameters may be continued across attribute boundaries. The concatenated string must have following format: “function-key”=<dictionary> where “function-key” specifies which Python functions will be used and <dictionary> contains the actual parameters in a Python dictionary structure format. For example: Alc-Dyn-Serv-Script-Params:1 = “data_svc_1 = { 'as_id' : '100', 'comm_id' : '200', 'if_name' : 'itf1', 'ipv4_address' : '1.1.1.1', 'egr_ip_filter' : '100' , 'routes' : [{'to' : '200.1.1.0/24', 'next-hop' : '20.1.1.1'}, {'to' : '200.1.2.0/24', 'next-hop' : '20.1.1.1'}]}

Table 67: Dynamic Data Service Accounting (applicability)

Attribute ID	Attribute Name	Acct Start	Acct Stop	Acct Interim-Update
1	User-Name	0-1	0-1	0-1
4	NAS-IP-Address	0-1	0-1	0-1
25	Class	0-1	0-1	0-1
32	NAS-Identifier	1	1	1
40	Acct-Status-Type	1	1	1
41	Acct-Delay-Time	0-1	0-1	0-1
44	Acct-Session-Id	1	1	1
46	Acct-Session-Time	0	1	1
49	Acct-Terminate-Cause	0	0-1	0
50	Acct-Multi-Session-Id	1	1	1
55	Event-Timestamp	1	1	1
87	NAS-Port-Id	1	1	1
95	NAS-IPv6-Address	0-1	0-1	0-1
26-3561-1	Agent-Circuit-Id	0-1	0-1	0-1
26-3561-2	Agent-Remote-Id	0-1	0-1	0-1
26-6527-165	Alc-Dyn-Serv-Script-Params	1+	1+	1+

CLI User Access Accounting

Table 68: CLI User Access Accounting (description)

Attribute ID	Attribute Name	Description
1	User-Name	The name of user requesting user-Authentication, Authorization, Accounting. User-names longer the allowed maximum Limit are treated as an authentication failure.
4	NAS-IP-Address	The identifying IP Address of the NAS requesting the Authentication or Accounting. Included when the RADIUS server is reachable via IPv4. The address is determined by the routing instance through which the RADIUS server can be reached: “Management” — The active ipv4 address in the Boot Options File (**bof address** <*ipv4-address*>) “Base” — The ipv4 address of the system interface (con**figure router interface system address** <*address*>). The address can be overwritten with the configured source-address (**configure system security source-address application radius** <*ip-int-name*|*ip-address*>)
31	Calling-Station-Id	The IP address (coded in hex) from the user that requests Authentication, Authorization, Accounting.
44	Acct-Session-Id	A unique number generated per authenticated user and reported in all accounting messages. Used to correlate CLI commands (accounting data) from the same user.
61	NAS-Port-Type	Mandatory included as type Virtual(5).
95	NAS-IPv6-Address	The identifying IP Address of the NAS requesting the Authentication or Accounting. Included when the RADIUS server is reachable via IPv6. The address is determined by the routing instance through which the RADIUS server can be reached: “Management” — The active ipv6 address in the Boot Options File (**bof address** <*ipv6-address*>) “Base” — The ipv6 address of the system interface (**configure router interface system ipv6 address** <*ipv6-address*>). The address can be overwritten with the configured ipv6-source-address (**configure system security source-address application6 radius** <*ipv6-address*>)

Table 68: CLI User Access Accounting (description)

Attribute ID	Attribute Name	Description
26-6527-6	Timetra-Cmd	A command-string, subtree command-string or a list of command-strings as scope for the match condition for user authorization. Multiple command-strings in the same attribute are delimited with the; character. Additional command-strings are encoded in multiple attributes. If the maximum number of command strings is violated, or if a string is too long, processing the input is stopped but authorization continues, so if the radius server is configured to have 5 command strings of which the 3rd is too long, only the first 2 entries will be used and the rest will be ignored. Each [26-6527-6] Timetra-Cmd attribute is followed in sequence by a [26-6527-7] Timetra-Action. (A missing Timetra-Action results in a deny). Note: For each authenticated RADIUS user a temporary profile with name [1]User-Name is always created (show system security profile) and executed as last profile. This temporary profile is build from the mandatory attribute [26-6527-5]Timetra-Default-Action and optional attributes [26-6527-6] Timetra-Cmd, [26-6527-7] Timetra-Action.

Table 69: CLI User Access Accounting (limits)

Attribute ID	Attribute Name	Type	Limits	SR-OS Format
1	User-Name	string	16 chars	For example: User-Name=“admin”
4	NAS-IP-Address	ipaddr	4 Bytes	For example: NAS-IP-Address= “192.0.2.1”

31	Calling-Station-Id	string	64 Bytes	# users ip address
				For example:
				Calling-Station-Id= “192.0.2.2” or
				Calling-Station-Id= “2001:db8..2”

44	Acct-Session-Id	string	22 Bytes	For example: Acct-Session-Id = “2128463592102512113409”
61	NAS-Port-Type	integer	4 Bytes value 5 fixed	Fixed set to value virtual (5) For example NAS-Port-Type 00000005
95	NAS-IPv6-Address	ipv6addr	16 Bytes	For example: NAS-IPv6-Address = 2001:db8::1

26-6527-6	Timetra-Cmd	string	25 attributes 247 chars/ attribute	For example:
				Timetra-Cmd += configure router isis;show subscriber-mgmt sub-profile
				Timetra-Cmd += show router

Table 70: CLI User Access Accounting (applicability)

Attribute ID	Attribute Name	Acct Start	Acct Stop
1	User-Name	1	1
4	NAS-IP-Address	0-1	0-1
31	Calling-Station-Id	1	1
44	Acct-Session-Id	1	1
61	NAS-Port-Type	1	1
95	NAS-IPv6-Address	0-1	0-1
26-6527-6	Timetra-Cmd	1	1

Accounting Terminate Causes

Table 71 specifies the different Terminate Causes generated by SR-OS in [49] Acct-Terminate-Cause attribute.

Table 71: Accounting Terminate Causes

Code	Acct Terminate Cause	Description	SR-OS
1	User-Request	User requested termination of service, for example, with LCP Terminate or by logging out.	yes
2	Lost-Carrier	Data Carrier Detect (DCD) was dropped on the port	yes
3	Lost-Service	Service can no longer be provided; for example, user's connection to a host was interrupted.	yes
4	Idle-Timeout	Idle timer expired	yes
5	Session-Timeout	Maximum session length timer expired	yes
6	Admin-Reset	Administrator reset the port or session	yes
7	Admin-Reboot	Administrator is ending service on the NAS, for example, prior to rebooting the NAS.	no
8	Port-Error	NAS detected an error on the port which required ending the session	yes
9	NAS-Error	NAS detected some error (other than on the port) which required ending the session	yes
10	NAS-Request	NAS ended session for a non-error reason not otherwise listed here.	yes
11	NAS-Reboot	The NAS ended the session in order to reboot non-administratively (crash).	yes
12	Port-Unneeded	NAS ended session because resource usage fell below low-water mark (for example, if a bandwidth-on-demand algorithm decided that the port was no longer needed).	no
13	Port-Preempted	NAS ended session in order to allocate the port to a higher priority use	no
14	Port-Suspended	NAS ended session to suspend a virtual session	yes
15	Service-Unavailable	NAS was unable to provide requested service	yes
16	Callback	NAS is terminating current session in order to perform callback for a new session	no
17	User-Error	Input from user is in error, causing termination of session.	no

Table 71: Accounting Terminate Causes (Continued)

Code	Acct Terminate Cause	Description	SR-OS
18	Host-Request	Login Host terminated session normally	yes
19	Supplicant Restart	Indicates re-initialization of the Supplicant state machines (dot1x)	no
20	Reauthentication Failure	Indicates that a previously authenticated Supplicant has failed to re-authenticate successfully following expiry of the re-authentication timer or explicit re-authentication request by management action. (dot1x)	no
21	Port Reinitialized	Termination cause indicates that the Port's MAC has been reinitialized (dot1x)	no
22	Port Administratively Disabled	Indicates that the Port has been administratively disabled (dot1x)	no
23	Lost Power		no

RADIUS CoA Message Attributes

Subscriber Host Identification Attributes

Table 72 details the different attributes that can be used in a CoA and Disconnect Message to identify one or multiple subscriber host(s).

Table 72: CoA and Disconnect Message: Subscriber Host Identification Attributes

# (priority)	Attribute ID	Attribute Name		Identifies
1. NAS-Port-Id + single address/prefix attribute	87	NAS-Port-Id	+ IP address/prefix	Single host (*)
	8	Framed-IP-Address	+ [87] NAS-Port-Id	Single IPv4 host (*)
	26-6527-99	Alc-Ipv6-Address	+ [87] NAS-Port-Id	Single IPv6 host (IA_NA) (*)
	97	Framed-Ipv6-Prefix	+ [87] NAS-Port-Id	Single IPv6 host (SLAAC) (*)
	123	Delegated-Ipv6-Prefix	+ [87] NAS-Port-Id	Single IPv6 host (IA_PD) (*)
2.	44	Acct-Session-Id (number format)	Host acct-session-id	Single host (*)
			Queue instance acct-session-id	All hosts attached to this sla-profile instance (**) HSMDAv2: all hosts of the corresponding subscriber (**)
			Session acct-session-id	All hosts of the dual stack PPPoE session
3.	26-6527-11	Alc-Subsc-ID-Str		All hosts of the corresponding subscriber (**)

Notes: (*) Although a single host is identified, the CoA or Disconnect Message will apply to all hosts of a dual stack PPPoE session.

(**) Maximum 32 hosts can be targeted in a single CoA or Disconnect Message. When more than 32 hosts are identified, the CoA and Disconnect Message is rejected with error cause 501 (Administratively Prohibited)

Typically only a single (set of) attribute(s) is used to target a host or a number of hosts: “NAS-Port-Id + IP” or “Acct-Session-Id” or “Alc-Subsc-ID-Str”. In case that both “NAS-Port-Id + IP” and “Acct-Session-Id” attributes are specified to identify subscriber hosts, only the host identified by “NAS-Port-Id + IP” will be targeted. If the identified host is not part of the hosts that would be identified by the “Acct-Session-Id” attribute, then the CoA will be NAKed with [101] Error-Cause attribute value 503 Session Context Not Found.

For example:

```
Change of Authorization(43) id 224 len 81 from 192.168.1.1:32772 vrid 1
    SESSION ID [44] 22 24ADFF0000003D5107AB80   # priority 2
    NAS PORT ID [87] 12 lag-1:10.300            # priority 1
    FRAMED IP ADDRESS [8] 4 172.1.2.251         # priority 1
    VSA [26] 15 Alcatel(6527)
      SLA PROF STR [13] 13 sla-profile-1
```

The CoA targets the host identified with the combination of [87] NAS-Port-Id and [8] Framed-IP-Address (prio 1) only if the host is also identified by [44] Acct-Session-Id (prio 2), else the CoA is NAKed.

Following attributes are accepted only if the CoA is targeted to a single host:

- [26-6527-14] Alc-Force-Renew
- [26-6527-15] Alc-Create-Host
- [26-6527-98] Alc-Force-Nak
- [26-6527-130] Alc-AA-Transit-IP

Overview of CoA Attributes

Table 73 provides an overview of all attributes that are supported in a RADIUS Change of Authorization (CoA) message. For attribute details, refer to the other sections in this document.

Table 73: RADIUS CoA Message Supported Attributes

Attribute ID	Attribute Name
1	User-Name
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
25	Class
27	Session-Timeout
28	Idle-Timeout
30	Called-Station-Id
31	Calling-Station-Id
44	Acct-Session-Id
61	NAS-Port-Type
85	Acct-Interim-Interval
87	NAS-Port-Id
92	NAS-Filter-Rule
97	Framed-IPv6-Prefix
101	Error-Cause
123	Delegated-IPv6-Prefix
242	Ascend-Data-Filter
26-6527-11	Alc-Subsc-ID-Str
26-6527-12	Alc-Subsc-Prof-Str
26-6527-13	Alc-SLA-Prof-Str
26-6527-14	Alc-Force-Renew
26-6527-15	Alc-Create-Host

Table 73: RADIUS CoA Message Supported Attributes (Continued)

Attribute ID	Attribute Name
26-6527-16	Alc-ANCP-Str
26-6527-28	Alc-Int-Dest-Id-Str
26-6527-45	Alc-App-Prof-Str
26-6527-95	Alc-Credit-Control-CategoryMap
26-6527-96	Alc-Credit-Control-Quota
26-6527-98	Alc-Force-Nak
26-6527-99	Alc-Ipv6-Address
26-6527-122	Alc-LI-Action
26-6527-123	Alc-LI-Destination
26-6527-124	Alc-LI-FC
26-6527-125	Alc-LI-Direction
26-6527-126	Alc-Subscriber-QoS-Override
26-6527-130	Alc-AA-Transit-IP
26-6527-132	Alc-Access-Loop-Rate-Down
26-6527-134	Alc-Subscriber-Filter
26-6527-136	Alc-Onetime-Http-Redirection-Filter-Id
26-6527-137	Alc-Authentication-Policy-Name
26-6527-138	Alc-LI-Intercept-Id
26-6527-139	Alc-LI-Session-Id
26-6527-151	Alc-Sub-Serv-Activate
26-6527-152	Alc-Sub-Serv-Deactivate
26-6527-153	Alc-Sub-Serv-Acct-Stats-Type
26-6527-154	Alc-Sub-Serv-Acct-Interim-Ivl
26-6527-158	Alc-Nas-Filter-Rule-Shared
26-6527-159	Alc-Ascend-Data-Filter-Host-Spec
26-6527-160	Alc-Relative-Session-Timeout
26-6527-164	Alc-Dyn-Serv-SAP-Id

Table 73: RADIUS CoA Message Supported Attributes (Continued)

Attribute ID	Attribute Name
26-6527-165	Alc-Dyn-Serv-Script-Params
26-6527-166	Alc-Dyn-Serv-Script-Action
26-6527-167	Alc-Dyn-Serv-Policy
26-6527-168	Alc-Dyn-Serv-Acct-Interim-Ivl-1
26-6527-169	Alc-Dyn-Serv-Acct-Interim-Ivl-2
26-6527-170	Alc-Dyn-Serv-Acct-Stats-Type-1
26-6527-171	Alc-Dyn-Serv-Acct-Stats-Type-2
26-6527-177	Alc-Portal-Url
26-6527-178	Alc-Ipv6-Portal-Url
26-6527-179	Alc-GTP-Local-Breakout
26-6527-182	Alc-AA-Sub-Http-Url-Param
26-6527-185	Alc-Onetime-Http-Redirect-Reactivate
26-6527-193	Alc-AA-App-Service-Options

Table 74: RADIUS CoA message [101] Error-Cause values

Code	CoA Error Cause	Description	SR-OS
201	Residual Session Context Removed	Residual Session Context Removed is sent in response to a Disconnect-Request if one or more user sessions are no longer active, but residual session context was found and successfully removed. This value is only sent within a Disconnect-ACK and MUST NOT be sent within a CoA-ACK, Disconnect-NAK, or CoA-NAK.	No
202	Invalid EAP Packet (Ignored)	Invalid EAP Packet (Ignored) is a non-fatal error that MUST NOT be sent by implementations of this specification.	No
401	Unsupported Attribute	Unsupported Attribute is a fatal error sent if a Request contains an attribute (such as a Vendor-Specific or EAP-Message Attribute) that is not supported.	No
402	Missing Attribute	Missing Attribute is a fatal error sent if critical attributes (such as NAS or session identification attributes) are missing from a Request.	Yes
403	NAS Identification Mismatch	NAS Identification Mismatch is a fatal error sent if one or more NAS identification attributes (see Section 3) do not match the identity of the NAS receiving the Request.	Yes
404	Invalid Request	Invalid Request is a fatal error sent if some other aspect of the Request is invalid, such as if one or more attributes (such as EAP-Message Attribute(s)) are not formatted properly.	Yes
405	Unsupported Service	Unsupported Service is a fatal error sent if a Service-Type Attribute included with the Request is sent with an invalid or unsupported value. This error cannot be sent in response to a Disconnect-Request.	Yes
406	Unsupported Extension	Unsupported Extension is a fatal error sent due to lack of support for an extension such as Disconnect and/or CoA packets. This will typically be sent by a proxy receiving an ICMP port unreachable message after attempting to forward a CoA-Request or Disconnect-Request to the NAS.	No
407	Invalid Attribute Value	Invalid Attribute Value is a fatal error sent if a CoA-Request or Disconnect-Request contains an attribute with an unsupported value.	Yes
501	Administratively Prohibited	Administratively Prohibited is a fatal error sent if the NAS is configured to prohibit honoring of CoA-Request or Disconnect-Request packets for the specified session.	Yes
502	Request Not Routable (Proxy)	Request Not Routable is a fatal error that MAY be sent by a proxy and MUST NOT be sent by a NAS. It indicates that the proxy was unable to determine how to route a CoA-Request or Disconnect-Request to the NAS. For example, this can occur if the required entries are not present in the proxy's realm routing table.	No

Table 74: RADIUS CoA message [101] Error-Cause values (Continued)

Code	CoA Error Cause	Description	SR-OS
503	Session Context Not Found	Session Context Not Found is a fatal error sent if the session context identified in the CoA-Request or Disconnect-Request does not exist on the NAS.	Yes
504	Session Context Not Removable	Session Context Not Removable is a fatal error sent in response to a Disconnect-Request if the NAS was able to locate the session context, but could not remove it for some reason. It MUST NOT be sent within a CoA-ACK, CoA-NAK, or Disconnect-ACK, only within a Disconnect-NAK.	No
505	Other Proxy Processing Error	Other Proxy Processing Error is a fatal error sent in response to a CoA or Disconnect-Request that could not be processed by a proxy, for reasons other than routing.	No
506	Resources Unavailable	Resources Unavailable is a fatal error sent when a CoA or Disconnect-Request could not be honored due to lack of available NAS resources (memory, non-volatile storage, etc.).	Yes
507	Request Initiated	Request Initiated is a fatal error sent by a NAS in response to a CoA-Request including a Service-Type Attribute with a value of Authorize Only. It indicates that the CoA-Request has not been honored, but that the NAS is sending one or more RADIUS Access-Requests including a Service-Type Attribute with value Authorize Only to the RADIUS server.	No
508	Multiple Session Selection Unsupported	Multiple Session Selection Unsupported is a fatal error sent by a NAS in response to a CoA-Request or Disconnect-Request whose session identification attributes match multiple sessions, where the NAS does not support Requests applying to multiple sessions.	No