NOKIA

7750 SERVICE ROUTER
VIRTUALIZED SERVICE ROUTER

RADIUS ATTRIBUTES REFERENCE GUIDE
RELEASE 15.0.R5

3HE 11975 AAAC TQZZA 01

Issue: 01

September 2017

Table of Contents

List of tables

1 RADIUS Attributes Reference

1.1 About this Guide

This document provides an overview of all supported RADIUS Authentication, Authorization and Accounting attributes for the 7750 SR.

Topics include:

- RADIUS Authentication Attributes
- RADIUS Accounting Attributes
- RADIUS CoA and Disconnect Message Attributes

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

Table 1 lists and describes the attribute conventions used in this guide.

Table 1 **Attribute Conventions**

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.

Attribute Type Identifiers and VSA Type Identifiers used in this guide follow the dotted number notation as outlined in RFC 6929, *Remote Authentication Dial In User Service (RADIUS) Protocol Extensions*. For example:

- 1 (User-Name), a standard attribute type

- 26.6527.11 (Alc-Subsc-ID-Str), A Nokia Vendor Specific Attribute: Attribute type 26, Vendor Id 6527 and VendorType 11.
- 241.26.6527.16 (Alc-IPv6-Router-Adv-Policy), A Nokia Extended-Vendor-Specific-1 Attribute: Attribute Type 241, Extended Type 26, Vendor Id 6527 and Vendor Type 16.

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 Nokia 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.

1.2 RADIUS Authentication Attributes

1.2.1 Subscriber Host Identification

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

Table 2 **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 included in accounting via **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute 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 preconfigured 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 2 **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), IPCP (PPPoE), or data-triggered subscriber management. Simultaneously returned [88] Framed-Pool and [8] Framed-IP-Address (RADIUS Access-Accept) attributes are handled as host setup failures. Attribute is also used in CoA and Disconnect messages (part of the ESM or AA user identification key). Attribute can be omitted in accounting via the **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute no framed-ip-addr** command.

Table 2 **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 2 **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, or **data-triggered**) that operates as a router without NAT (routed subscriber host). The route included in the Framed-Route attribute is accepted as a managed route only if its next-hop points to the hosts ip-address, if the next-hop address equals 0.0.0.0, or if the included route is a valid classful network, in which 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 is installed as a standalone host without a managed route). Any routes above the configured Limits are silently ignored. Optionally, a metric, tag or protocol preference can be specified for the managed route. If the metrics are not specified, specified in a wrong format, or specified with out-of-range values, then the 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.

Table 2 **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 host, PPPoE or IPoE session) before termination of the session. The attribute equals [26.6527.160] Alc-Relative-Session-Timeout when received in Access-Accept since current session time portion is then equal to zero. Value zero sets the session-timeout to infinite (**no session-timeout**). The attribute is CoA NAK'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 an error condition (setup failure if received via Access-Accept and NAK'd if received via CoA). With IPoE session disabled for IPoEv4 radius proxy and CoA create-host scenarios, [27] Session-Timeout is interpreted as lease-time instead of session-time if [26.6527.174] Alc-Lease-Time is omitted. For WLAN-GW group interfaces, the interpretation of the Session-Timeout attribute is configured with: **configure service ies | vprn** *service-id* **subscriber-interface** *ip-int-name* **group-interface** *ip-int-name* **wlangw ipoe-session radius-session-timeout** {**backwards-compatible** | **ignore** | **absolute**}.
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

Table 2 **Subscriber Host Identification (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 ies | vprn** *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: **include-radius-attribute nas-identifier** in **configure subscriber-mgmt authentication-policy** (ESM authentication), **configure subscriber-mgmt radius-accounting-policy** (ESM accounting), **configure aaa isa-radius-policy** (LSN accounting, WLAN-GW) 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 or 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.

Table 2 **Subscriber Host Identification (Description) (Continued)**

Attribute ID	Attribute Name	Description
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 from 32 to 64 bytes unless configured different under **configure subscriber-mgmt ppp-policy** *ppp-policy-name* **ppp-chap-challenge-length** [8 to 64] or **configure service vprn** *service-id* | **router l2tp group** *tunnel-group-name* **ppp chap-challenge-length** [8 to 64] for LNS (the command can also be specified at the tunnel level). 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) and **configure aaa l2tp-accounting-policy** (L2TP accounting). Checked for correctness if returned in CoA. The **NAS-Port-Type** attribute is always included when the **Nas-Port-Id** is also included.
85	Acct-Interim-Interval	The interval, in seconds, at which Acct-Interim-Update messages should be generated for the first RADIUS Accounting Policy in the subscriber profile. Overrides the local configured update-interval value in the RADIUS accounting policy. This only takes effect if interim-updates are enabled for one of the accounting modes in the RADIUS Accounting Policy. An attribute value of 0 disables the generation of Acct-Interim-Update messages. Attribute [85] Acct-Interim-Interval takes precedence over [26.6527.232] Alc-Acct-Interim-Ivl with tag 1 when both are included. Attribute values outside the allowed limits are accepted but are rounded to the minimum or maximum limit.

Table 2 **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 Authentication 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. Included only if **include-radius-attribute nas-port-id** 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) and **configure aaa l2tp-accounting-policy** (L2TP accounting). For a **capture-sap**, the **nas-port-id** attribute is always included in authentication requests.
88	Framed-Pool	The name of one address pool or the name of a primary and secondary address pool separated with a one 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.

Table 2 **Subscriber Host Identification (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*).
97	Framed-IPv6-Prefix	The IPv6 prefix or 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**.

Table 2 **Subscriber Host Identification (Description) (Continued)**

Attribute ID	Attribute Name	Description
99	Framed-IPv6-Route	Routing information (IPv6 managed route) to be configured on the NAS for an IPv6 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 its next hop is a WAN host (DHCPv6 IA-NA, SLAAC, or /128 data-triggered). Therefore, Framed-IPv6-Routes with an explicitly 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 is installed as a standalone host without managed route). Any routes above the configured limits are silently ignored. Optionally, a metric, tag, or protocol preference can be specified for the managed route. If the metrics are not specified, specified in a wrong format, or specified with out-of-range values, then the following 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 or 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 an identical prefix, equal lowest preference, and equal lowest metric. The 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 the 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).
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 assigns IPv6 addressing to the WAN side of a host via SLAAC or DHCPv6 IA-NA.

Table 2 **Subscriber Host Identification (Description) (Continued)**

Attribute ID	Attribute Name	Description
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	The attribute that carries the prefix (IPv6 prefix or 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 ies | vprn** *service-id* **subscriber-interface** *ip-int-name* **ipv6 delegated-prefix-length** [48 to 64] is required with the received attribute prefix-length unless a variable DPL is configured (**configure service ies | vprn** *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 to 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). This attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute no delegated-ipv6-prefix**. For data-triggered subscriber host authentication, an Access-Accept message can include this attribute to specify the prefix to create an IPv6 prefix host.
26.2352.1	Client-DNS-Pri	The IPv4 address of the primary DNS server for this subscriber's 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 subscriber's 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 2 **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 ies | vprn** *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 subscriber's 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 subscriber's connection and maps to PPPoE IPCP option 132 Primary DNS Server address or DHCPv4 option44 NETBIOS name server. This attribute 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 or DSLAM from which a subscriber's requests are initiated. Attribute is included or excluded based on **configure subscriber-mgmt authentication-policy**/**radius-accounting-policy** *name* **include-radius-attribute circuit-id**. For data-triggered subscriber host authentication: • in Access-Request, the attribute contains the source IPv4 or IPv6 address of the data trigger packet • when included in Access-Accept, the attribute is used as circuit-id to build the IPoE session key when **configure subscriber-mgmt ipoe-session-policy** *policy-name* **circuit-id-from-auth** is configured. For data-triggered subscriber host authentication, this attribute in the Access-Request message contains the source IPv4 or IPv6 address of the data-trigger. The Access-Accept message can include this attribute to specify the circuit ID of the IPoE session if the **configure subscriber-management ipoe-session-policy** *name* **circuit-id-from-auth** command is configured.

Table 2 **Subscriber Host Identification (Description) (Continued)**

Attribute ID	Attribute Name	Description
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 or DSLAM. Attribute is included or 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 or 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 or 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 or 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 or 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 or 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 or excluded based on **configure subscriber-mgmt authentication-policy**/**radius-accounting-policy** *name* **include-radius-attribute access-loop-options**.

Table 2 **Subscriber Host Identification (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 or 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 or 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 or 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 or 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 or 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 or excluded based on **configure subscriber-mgmt authentication-policy**/**radius-accounting-policy** *name* **include-radius-attribute access-loop-options**.

Table 2 **Subscriber Host Identification (Description) (Continued)**

Attribute ID	Attribute Name	Description
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 or 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 or 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 or 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. Preconfigured encapsulation types are used if PPP or IPoE access loop information (tags) is not available (c**onfigure subscriber-mgmt sub-profile** *subscriber-profile-name* **egress encap-offset type** *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 preconfigured 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**.

Table 2 **Subscriber Host Identification (Description) (Continued)**

Attribute ID	Attribute Name	Description
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 ies | vprn** *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 subscriber's 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. Applicable in proxy scenarios only for IPoE.
26.4874.5	ERX-Secondary-Dns	The IPv4 address of the secondary DNS server for this subscriber's 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. Applicable in proxy scenarios only for IPoE.
26.4874.6	ERX-Primary-Wins	The IPv4 address of the primary NetBios Name Server (NBNS) for this subscriber's 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 subscriber's 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 subscriber's 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. Applicable in proxy scenarios only.
26.4874.48	ERX-Ipv6-Secondary-Dns	The IPv6 address of the secondary DNSv6 server for this subscriber's 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. Applicable in proxy scenarios only.

Table 2 **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 subscriber's 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. Applicable in proxy scenarios only for IPoE.
26.6527.10	Alc-Secondary-Dns	The IPv4 address of the secondary DNS server for this subscriber's 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. Applicable in proxy scenarios only for IPoE.
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 or policers belonging to the same subscriber (residing on the same forwarding complex) can be treated under one aggregate scheduling QoS mechanism. Fallback to preconfigured 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 that contains settings (accounting, IGMP, HQoS, and so on) that apply to all hosts belonging to the same subscriber where [26.6527.12] Alc-Subsc-Prof-Str is the string that maps (**configure subscriber-mgmt sub-ident-policy** *sub-ident-policy-name* **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 (where the string does not map to a policy) are silently ignored and a fallback to preconfigured defaults is done. This 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, and so on) 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 (where the string does not map to a policy) are silently ignored and a fallback to preconfigured defaults is done. This attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-polic**y *name* i**nclude-radius-attribute no sla-profile**.

Table 2 **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 or 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). A subscriber is associated with ANCP when both strings are equal. For associated subscribers, the ingress and 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 an DHCP offer or 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 using 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** *name* **include-radius-attribute mac-address**).
26.6527.28	Alc-Int-Dest-Id-Str	A string representing an aggregation point (example, Access Node) and interpreted as the intermediate destination ID. Subscribers connected to the same aggregation point receives 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 *int-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 subscriber’s 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.

Table 2 **Subscriber Host Identification (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.30	Alc-Secondary-Nbns	The IPv4 address of the secondary NetBios Name Server (NBNS) for this subscriber's 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.
26.6527.34	Alc-PPPoE-PADO-Delay	Specifies the number in deciseconds 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** *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] Vendor Class Identifier and reflected in Authentication. (**configure subscriber-mgmt authentication-policy** *name* **include-radius-attribute dhcp-vendor-class-id or configure aaa isa-radius-policy** *name* **auth-include-attributes dhcp-vendor-class-id**). DHCP option [60] Vendor Class Identifier can also be used as User-name in RADIUS requests. (**configure subscriber-mgmt authentication-policy** *name* **user-name-format dhcp-client-vendor-opts**).

Table 2 **Subscriber Host Identification (Description) (Continued)**

Attribute ID	Attribute Name	Description
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-Str 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 in 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) silently triggers a fallback to preconfigured default values if allowed. If no default value is preconfigured, the subscriber's application profile is silently disabled for esm AA-subscriber; in case of a transit AA-subscriber creation, the CoA is rejected. The change of an application profile to one configured under a different group or partition or the modification of the application profile of a static AA-subscriber is not allowed and is treated as setup failures.
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). For data-triggered subscriber host creation in the Enhanced Subscriber Management (ESM) context, the attribute can be included in an Access-Accept message to specify the IPv6 address to create a /128 IPv6 host. For data-triggered authentication of an IPv6 UE in Distributed Subscriber Management (DSM) context, this attribute contains the IPv6 address that triggered the request. Inclusion of this attribute is configured under **configure aaa isa-radius-policy** *policy-name* **auth-include-attributes ipv6-address**. For data-triggered subscriber host creation, an Access-Accept message can contain this attribute to specify the IPv6 address to create an IPv6 / 128 host.

Table 2 **Subscriber Host Identification (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.100	Alc-Serv-Id	Applies to GTP access hosts only. This VSA refers to a the service where the GTP sessions will be terminated (**configure service** {**vprn | ies**} *service-id*). This overrides a potential default configured under **configure subscriber-mgmt gtp apn-policy** *policy-name* **apn** *apn* **defaults group-interface** *interface-name* **svc-id** *service-id*. This VSA must be accompanied with a valid Alc-Interface VSA.
26.6527.101	Alc-Interface	Applies to GTP access hosts only. This VSA refers to a group-interface of type GTP where the GTP sessions will be terminated (**configure service** {**vprn** | **ies**} **subscriber-interface** *ip-int-name* **group-interface** *ip-int-name* **gtp**). This overrides a potential default configured under **configure subscriber-mgmt gtp apn-policy** *policy-name* **apn** *apn* **defaults group-interface** *interface-name* **svc-id** *service-id*. If neither a default or a radius-specified interface is provided, session setup will fail.
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. If more space is needed, an additional attribute is included. If the total dhcp options space requires more than the total maximum length, then no attributes are included. (**configure subscriber-mgmt authentication-policy** *name* **include-radius-attribute dhcp-options**, or **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. Attributes outside the defined limits result in a setup failure.
26.6527.105	Alc-Ipv6-Primary-Dns	The IPv6 address of the primary DNSv6 server for this subscriber's connection. Maps to DNS Recursive Name Server option 23 (RFC 3646) in DHCPv6 and Recursive DNS Server Option type 25 (RFC 6106) for SLAAC RA. This attribute is an alternative for [26.4874.47] ERX-Ipv6-Primary-Dns. Applicable in proxy scenarios only.
26.6527.106	Alc-Ipv6-Secondary-Dns	The IPv6 address of the secondary DNSv6 server for this subscriber's connection. Maps to DNS Recursive Name Server option 23 (RFC 3646) in DHCPv6 and Recursive DNS Server Option type 25 (RFC 6106) for SLAAC RA. This attribute is an alternative for [26.4874.48] ERX- Ipv6-Secondary-Dns. Applicable in proxy scenarios only.

Table 2 **Subscriber Host Identification (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.126	Alc-Subscriber-QoS-Override	Used to override queue or policer parameters (CIR, PIR, CBS, MBS) and HQoS parameters (aggregate rate, scheduler rate or root arbiter rate) configured at **sla-profile** and **sub-profile** context. Enables per subscriber or 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 or subscriber 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:). Incorrectly formatted attributes or too many attributes are treated as a setup failure or result in a CoA NAK.
26.6527.128	Alc-ATM-Ingress-TD-Profile	The ATM Traffic Descriptor override for a PPPoA or PPPoEoA host and refers to the preconfigured 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 preconfigured 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 preconfigured 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 preconfigured 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.

Table 2 **Subscriber Host Identification (Description) (Continued)**

Attribute ID	Attribute Name	Description
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 [48 to 64] DPL or variable DPL under **configure service ies | vprn** *service-id* **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**).
26.6527.132	Alc-Access-Loop-Rate-Down	The actual downstream rate (coded in kb/s) 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. This attribute is silently ignored for non-MLPPP sessions or IPoE sessions.
26.6527.133	Alc-Access-Loop-Encap-Offset	The last mile encapsulation representing the subscriber’s DSL access loop encapsulation. When returned in RADIUS-Accept (PTA or LAC), it 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 where no IPv6 related attributes (such as v6 pool, v6 prefix, v6 address, DNSv6) are obtained via authentication (Access Accept, local user database, and so on). Without these IPv6 related attributes, the NAS cannot detect that this is a dual-stack PPPoE user and therefore it will not start IPv6CP negotiation. An attribute value other than 0 (zero) forces IPv6CP negotiation to start when no IPv6 attributes are obtained in authentication. An attribute value of 0 (zero) is treated the same as not sending the attribute.
26.6527.136	Alc-Onetime-Http-Redirection-Filter-Id	The preconfigured IPv4 filter with HTTP redirection rules. Via this host-specific filter only the first HTTP request from the host is redirected to a configured URL with specified parameters. There is no HTTP redirection for subsequent HTTP requests which is useful in cases where service providers need to push a web page of advertisement or announcements to broadband users.

Table 2 **Subscriber Host Identification (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.146	Alc-Wlan-APN-Name	This VSA contains the Access Point Name string as signaled in the incoming GTP-C message for GTP Access hosts. Inclusion of this attribute can be configured via **configure subscriber-mgmt authentication-policy** *name* **include-radius-attribute apn**.
26.6527.147	Alc-MsIsdn	This VSA contains the MSISDN (telephone number) as signaled in the incoming GTP-C message for GTP Access hosts. If the corresponding GTP-C IE is not present the VSA will not be included. Inclusion of this attribute can be configured via **configure subscriber-mgmt authentication-policy** *name* **include-radius-attribute msisdn**.
26.6527.160	Alc-Relative-Session-Timeout	Sets or resets the IPoE or 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. A value of zero sets or 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 or CoA rejected (NAK) with error cause = Invalid Request).
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 [48 to 64] DPL 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.
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. Returning attribute [26.6527.174] Alc-Lease-Time in other scenarios than 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 or excluded based on **configure subscriber-mgmt authentication-policy**/**radius-accounting-policy** *name* **include-radius-attribute access-loop-options**.

Table 2 **Subscriber Host Identification (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.176	Alc-DSL-Type	Type of the DSL line (ADSL1, ADSL2, ADSL2PLUS, VDSL1, VDSL2, SDSL, other) obtained via ANCP. This attribute is included or 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. 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. 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, this is a unique PPPoE or IPoE session index that can be included in RADIUS Access Request messages. The lowest free index is assigned to a new PPPoE or IPoE session. Attribute is included or 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 or 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 is terminated. If **local-address-assignment** is not enabled on the group-interface for **ipv6 client-application ipoe-slaac**, then the IPoE host is not instantiated.
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.

Table 2 **Subscriber Host Identification (Description) (Continued)**

Attribute ID	Attribute Name	Description
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.
26.6527.191	Alc-ToServer-Dhcp6-Options	This attribute contains DHCPv6 client options present in a DHCPv6 Solicit or Request message to be passed to RADIUS in an Access-Request. Up to two attributes are included in the Access-Request message when the length of the DHCPv6 options exceeds the maximum length of a single attribute. No attributes are included if the total length of the DHCPv6 options exceeds 494 bytes. When the DHCPv6 solicit or request message is encapsulated in a Relay-Forward message, only the inner DHCPv6 client options are copied in the Alc-ToServer-Dhcp6-Options attribute. Options inserted by a Relay Agent are ignored. Attribute is included or excluded based on **configure subscriber-mgmt authentication-policy** *name* **include-radius-attribute dhcp6-options**. For DHCPv6 triggered authentication in a Distribute Subscriber Management (DSM) context, this attribute contains the DHCPv6 client options as sent to the WLAN-GW. Inclusion of this attribute is configured via **configure aaa isa-radius-policy** *policy-name* **auth-include-attributes dhcp6-options**.
26.6527.192	Alc-ToClient-Dhcp6-Options	The value of this attribute represents DHCPv6 options encoded in a hexadecimal format. DHCPv6 options originated by RADIUS are appended to the options already present in the DHCPv6 Advertise and Reply messages towards the client. Passing the RADIUS obtained DHCPv6 options to the client is supported for both DHCPv6 proxy and relay. Attributes outside the defined limits result in a setup failure.

Table 2 **Subscriber Host Identification (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.200	Alc-v6-Preferred-Lifetime	An IPv6 address or prefix preferred lifetime is the length of time that a valid address or prefix is preferred (for example, the time until deprecation). When the preferred lifetime expires, the address or prefix becomes deprecated (it can still be used in existing communications but should not be used as a source in new communications). This attribute is applicable only when an IPv6 address or prefix is assigned via RADIUS (DHCPv6 proxy). It overrides the **dhcp6 proxy-server preferred-lifetime** configuration on the group-interface. The attribute value is expressed in seconds. Values outside the allowed range result in a setup failure. If, for the final determined values from the different sources (LUDB, RADIUS, defaults), the following rule is violated: renew timer 7705 SAR-8 rebind timer <= preferred lifetime <= valid lifetime then the default timers are used: renew-timer = 30 min, rebind-timer = 48 min, preferred-lifetime = 1hr, valid-lifetime = 1 day. Note that only a single value can be specified that applies to both IA-NA address and IA-PD prefix.
26.6527.201	Alc-v6-Valid-Lifetime	The IPv6 address or prefix valid lifetime is the length of time an address or prefix remains in the valid state (for example, the time until invalidation). When the valid lifetime expires, the address or prefix becomes invalid and must no longer be used in communications. This attribute is used as the DHCPv6 lease time. This attribute is applicable only when an IPv6 address or prefix is assigned via RADIUS (DHCPv6 proxy). Overrides the **dhcp6 proxy-server valid-lifetime** configuration on the group-interface. The attribute value is expressed in seconds. Values outside the allowed range result in a setup failure. If, for the final determined values from the different sources (LUDB, RADIUS, defaults), the following rule is violated: renew timer <= rebind timer <= preferred lifetime <= valid lifetime then the default timers are used: renew-timer = 30 min, rebind-timer = 48 min, preferred-lifetime = 1hr, valid-lifetime = 1 day. Note that only a single value can be specified that applies to both IA-NA address and IA-PD prefix.

Table 2 **Subscriber Host Identification (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.202	Alc-Dhcp6-Renew-Time	The attribute value represents the DHCPv6 lease renew time (T1). T1 is the time at which the client contacts the addressing authority to extend the lifetimes of the DHCPv6 leases (addresses or prefixes). This attribute is applicable only when an IPv6 address or prefix is assigned via RADIUS (DHCPv6 proxy). Overrides the **dhcp6 proxy-server renew-timer** configuration on the group interface. The attribute value is expressed in seconds. Values outside the allowed range result in a setup failure. If, for the final determined values from the different sources (LUDB, RADIUS, defaults), the following rule is violated: renew timer <= rebind timer <= preferred lifetime <= valid lifetime then the default timers are used: renew-timer = 30 min, rebind-timer = 48 min, preferred-lifetime = 1hr, valid-lifetime = 1 day. Note that only a single value can be specified that applies to both IA-NA address and IA-PD prefix.
26.6527.203	Alc-Dhcp6-Rebind-Time	The attribute value represents the DHCPv6 lease rebind time (T2). T2 is the time at which the client contacts any available addressing authority to extend the lifetimes of DHCPv6 leases. This attribute is applicable only when an IPv6 address or prefix is assigned via RADIUS (DHCPv6 proxy). The attribute overrides the **dhcp6 proxy-server rebind-timer** configuration on the group interface The attribute value is expressed in seconds. Values outside the allowed range result in a setup failure. If, for the final determined values from the different sources (LUDB, RADIUS, defaults), the following rule is violated: renew timer <= rebind timer <= preferred lifetime <= valid lifetime then the default timers are used: renew-timer = 30 min, rebind-timer = 48 min, preferred-lifetime = 1hr, valid-lifetime = 1 day. Note that only a single value can be specified that applies to both IA-NA address and IA-PD prefix.

Table 2 **Subscriber Host Identification (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.217	Alc-UPnP-Sub-Override-Policy	Specifies the UPnP policy to use for this L2-Aware subscriber. The policy must be configured in **configure service upnp upnp-policy** *policy-name*. Overrides the configured policy in the sub-profile for the subscriber: **configure subscriber-mgmt sub-profile** *name* **upnp-policy** *policy-name*. The value "_tmnx_no_override" removes any existing override and installs the upnp-policy configured in the sub-profile instead. The value "_tmnx_disabled" creates a special override that disables UPnP for this subscriber. Specifying a non-existing policy results in a host or session setup failure or in a CoA Reject. All hosts belonging to the subscriber are affected by a UPnP policy override. Changing the UPnP policy clears all existing UPnP mappings.
26.6527.228	Alc-Trigger-Acct-Interim	When included in a CoA message an accounting interim update is generated for all accounting modes that have interim-updates enabled. The Alc-Trigger-Acct-Interim attribute with free formatted string value is echoed in the CoA triggered accounting interim update message. The [26.6527.163] Alc-Acct-Triggered- Reason attribute in the interim update is set to 18 (CoA-Triggered).
26.6527.232	Alc-Acct-Interim-Ivl	Tagged Attribute. The interval in seconds at which Acct-Interim-Update messages should be generated. Overrides the local configured update-interval value in the RADIUS accounting policy. Only takes effect if interim-updates are enabled for one of the accounting modes in the RADIUS accounting policy. With attribute value=0, the interim accounting is switched off. The tag value (1 to 5) indicates which RADIUS accounting policy in the subscriber profile is updated. To change the update interval of the first accounting policy, attribute [85] Acct-Interim-Interval takes precedence over [26.6527.232] Alc-Acct-Interim-Ivl with tag 1 when both are included.

Table 2 **Subscriber Host Identification (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.234	Alc-DNAT-Override	A composite RADIUS attribute used to modify DNAT function for L2-Aware NAT subscribers: • enable or disable DNAT functionality without affecting SNAPT • modify destination IP address in DNAT After the DNAT configuration is modified via CoA (by enabling or disabling DNAT or changing the DNAT IP address), the existing flows remain active for five more seconds while the new flows are being created in accordance with the new configuration. After a five-second timeout, the stale flows are cleared from the system. If multiple Alc-DNAT-Override attributes with conflicting actions are received in the same CoA or Access-Accept, the last one takes precedence.
26.6527.238	Alc-Remove-Override	This attribute, when included in a CoA, removes the override installed with or deactivates the action triggered by the referenced attribute ID.
26.6527.242	Alc-Radius-Py	A free format attribute reserved for use in combination with a RADIUS Python script. SR OS ignores the attribute when received in an access accept or CoA and will not generate the attribute. The primary purpose for this attribute is to interact with RADIUS servers that do not support RFC 6929 extended and long extended vendor specific attribute types. This attribute can be used between the RADIUS server and the Python script. The Python script should convert the attribute value in an RFC 6929 compliant attribute format.
26.6527.244	Alc-Force-DHCP-Relay	When this attribute is included in an Access Accept message at the authentication of a data triggered subscriber hosts IPoE session, then a DHCP relay is performed when the subscriber host in the session is promoted to a DHCP host at renew or rebind. The IP and/or IPv6 address/prefix origin is set to DHCP or DHCP6 for the data triggered subscriber host that is promoted to a DHCP host. The IP address/prefix for all IP stacks of the subscribers IPoE session must also be included in the Access Accept. Attributes with invalid value are ignored.
241.26.6527.16	Alc-IPv6-Router-Adv-Policy	This attribute specifies the Router Advertisement policy to be used for this subscriber host or session. The Router Advertisement policy is configured in **configure subscriber-mgmt router-advertisement-policy** *name*. The Router Advertisement policy overrides the default Router Advertisement parameters configured in the **ipv6 router-advertisements** CLI context at the group interface or subscriber interface (wholesale or retail). Referencing a non-existing policy results in a subscriber host or session setup failure or a CoA reject.

Table 2 **Subscriber Host Identification (Description) (Continued)**

Attribute ID	Attribute Name	Description
241.26.6527.17	Alc-Nat-Outside-IPs	This attribute allows to specify an outside NAT IP address from AAA instead of allocating an address from the local NAT pools. An IP address can be provided for each policy.
241.26.6527.18	Alc-Mld-Import-Policy	This attribute overrides the subscriber's current list of dynamic MLD import policies. The order in which the policies were added can be checked with **show router** [*router-instance*] **mld hosts host** *ipv6-address* **detail**. Note that the configured MLD import policy (**configure subscriber-mgmt mld-policy** *mld-policy-name* **import** *policy-name*) cannot be overridden and is always applied as the last policy in the MLD import policies list. As the import policies are evaluated in the applied order using a match and exit, it is good practice to only include a default-action in the configured MLD import policy. Access-Accept fails and CoA is rejected if more than 14 attributes are present.
241.26.6527.24	Alc-IPv6-DMZ-Enabled	This attribute applies to vRGW only. When present, this VSA determines if the corresponding session should be treated as part of a demilitarized zone in an IPv6 firewall or not. This attribute is ignored if the session is not part of a subscriber with firewall enabled.
241.26.6527.27	Alc-IPv6-Sub-If-Prefix	This attribute installs a subscriber interface IPv6 prefix of type **pd**, **wan-host** or both. This is similar to a statically configured IPv6 prefix on a subscriber interface. The prefix is part of the subscriber host or session state. The prefix is removed from the system when the subscriber host or session disconnects. An invalid prefix, such as when overlapping with a static provisioned prefix, results in a subscriber host or session setup failure.
241.26.6527.35	Alc-Mld-Import-Policy-Modif	This attribute modifies the subscriber's dynamic MLD import policy list. The command can either add or delete an MLD import policy to or from the list. The CoA is rejected if more than the allowed number of attributes are included or if the number of resulting dynamic MLD import policies is more than 14.
241.26.6527.37	Alc-VAS-IPv4-Filter	(l2-aware NAT subscriber only). This VSA enables IPv4 service chaining for an l2-aware NAT subscriber using the named Value Added Services (VAS) filter configured under **configure subscriber-mgmt isa-service-chaining vas-filter**.

Table 2 **Subscriber Host Identification (Description) (Continued)**

Attribute ID	Attribute Name	Description
241.26.6527.38	Alc-VAS-NSH-IPv4-Opaque-Meta-Data	(l2-aware NAT subscriber only). For Value Added Services (VAS) enabled sessions this VSA specifies the Network Services Header (NSH) context header data for MD type 1. This value will override **insert-subscriber-id** or **opaque-data** configured under **configure subscriber-mgmt isa-service-chaining vas-filter** *filter-name* **entry** *id* **action {downstream | upstream} insert-nsh meta-data**. An NSH header with this context data will only be inserted if **svc-path** is correctly configured under **configure subscriber-mgmt isa-service-chaining vas-filter** *filter-name* **entry** *id* **action {downstream | upstream} insert-nsh**.
241.26.6527.39	Alc-Static-Port-Forward	Static port forwards to be installed for layer-2 aware NAT subscribers using external address assignment.
241.26.6527.40	Alc-IPv6-Slaac-Replacement-Prefix	Override the current host SLAAC prefix with the one specified in the VSA. The host address origin is not changed. Three subsequent Router Advertisements are sent to the SLAAC host respecting the configured advertisement intervals. The Router Advertisements contain both the current and new SLAAC prefixes: the valid and preferred lifetime for the current prefix are set to zero and for the new prefix the values are either specified in the router advertisement policy or the group interface configuration. Because of the prefix change, all traffic send using the old SLAAC prefix as source address is dropped in the BNG when anti-spoof is set to IP + MAC. Note that the prefix change results in a SLAAC host delete and create.
26.10415.5	3GPP-GPRS-Negotiated-QoS-Profile	This VSA contains the QoS values signaled in the incoming GTP-C message for GTP Access hosts. Inclusion of this attribute can be configured via c**onfigure subscriber-mgmt authentication-policy** *name* **include-radius-attribute gprs-negotiated-qos-profile**.
26.10415.20	3GPP-IMEISV	This VSA contains the International Mobile Equipment Identity and its software version as signaled in the incoming GTP-C message for GTP Access hosts. If the corresponding GTP-C IE is not present the VSA will not be included. Inclusion of this attribute can be configured via **configure subscriber-mgmt authentication-policy** *name* **include-radius-attribute imei.**
26.10415.21	3GPP-RAT-Type	This VSA contains the Radio Access Type as signaled in the incoming GTP-C message for GTP Access hosts. Inclusion of this attribute can be configured via **configure subscriber-mgmt authentication-policy** *name* i**nclude-radius-attribute rat-type**.

Table 2 **Subscriber Host Identification (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.10415.22	3GPP-User-Location-Info	This VSA contains the User Location Information as signaled in the incoming GTP-C message for GTP Access hosts. Inclusion of this attribute can be configured via **configure subscriber-mgmt authentication-policy** *name* **include-radius-attribute uli**.

Table 3 **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 to 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

Table 3 **Subscriber Host Identification (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
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 3 **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 to 65535] [tag <tag-value>] (Optional) The managed route is tagged for use in routing policies. If not specified or tag-value=0, then the route is not tagged. Value = [0 to 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 to 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. (*Continued on next page*)

Table 3 **Subscriber Host Identification (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
22 (*cont.*)	Framed-Route (*cont.*)			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
25	Class	octets	Up to 6 attributes. Max. value length for each attribute is 253 chars	For example: Class += My Class1 Class += MyClass2
27	Session-Timeout	integer	[0 to 2147483647] seconds	# 0 = infinite (no session-timeout) # [0 to 2147483647] in seconds For example: Session-Timeout = 3600
28	Idle-Timeout	integer	[60 to 15552000] seconds	# 0 = infinite (no idle-timeout) # [60 to 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	Internally generated 22 bytes number. For example: Acct-Session-Id = 241AFF0000003250B5F750
60	CHAP-Challenge	octets	[8 to 64] bytes	random length For example: 20 bytes CHAP-Challenge 0xa9710d2386c3e1771b8a3ea3d4e53f2a1c7024fb

Table 3 **Subscriber Host Identification (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
61	NAS-Port-Type	integer	4 bytes Values [0 to 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	0, [300 to 15552000]	A value of 0 (zero) disables the generation of interim update messages. A value of 1 to 299 is rounded to 300s (minimum CLI value). A value of 300 to 15552000 specifies the Acct-Interim-Update message interval in seconds. A value greater than 15552000 is rounded to 15552000 (maximum CLI value). For example: 1 hour interval for interim updates Acct-Interim-Interval = 3600

Table 3 **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	Ethernet: "<prefix> <space> <slot>/<mda>/ <port>:<vlan>.<vlan> <space> <suffix>" LAG: "<prefix> <space> lag-<lag-id> : <outer vlan id> [.<inner vlan id>] <space> <suffix>" PseudoWire port (both attached to physical port or anchored): "<prefix> <space> pw-<pw-port-id> : <outer vlan id> [.<inner vlan id>] <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>" <prefix>: optional string: 8 chars max <suffix>: optional string: remote-id (max 64 chars) | circuit-id (max 64 chars) 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" Framed-Pool = "Pool-1#Pool-2"
95	NAS-IPv6-Address	ipv6addr	16 bytes	# ipv6 address For example: NAS-IPv6-Address = 2001:db8::1

Table 3 **Subscriber Host Identification (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
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
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 to 65535] [tag <tag-value>] (Optional) The managed route is tagged for use in routing policies. If not specified or tag-value=0, then the route is not tagged. Value = [0 to 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 to 255]

Table 3 **Subscriber Host Identification (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
99 (continued)	Framed-IPv6-Route	string	max. 16 Framed-IPv6-Route attributes	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
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 to 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

Table 3 **Subscriber Host Identification (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
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 RFC 4679 For example: Agent-Remote-Id = MyRemoteId
26.3561.129	Actual-Data-Rate-Upstream	integer	4294967295 b/s	For example: # 1Mb/s Actual-Data-Rate-Upstream = 1000000
26.3561.130	Actual-Data-Rate-Downstream	integer	4294967295 b/s	For example: # 5Mb/s Actual-Data-Rate-Downstream = 5000000
26.3561.131	Minimum-Data-Rate-Upstream	integer	4294967295 b/s	For example: Minimum-Data-Rate-Upstream = 1000
26.3561.132	Minimum-Data-Rate-Downstream	integer	4294967295 b/s	For example: Minimum-Data-Rate-Downstream = 1000
26.3561.133	Attainable-Data-Rate-Upstream	integer	4294967295 b/s	For example: Attainable-Data-Rate-Downstream = 1000
26.3561.134	Attainable-Data-Rate-Downstream	integer	4294967295 b/s	For example: Minimum-Data-Rate-Upstream = 1000

Table 3 **Subscriber Host Identification (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.3561.135	Maximum-Data-Rate-Upstream	integer	4294967295 b/s	For example: Maximum-Data-Rate-Upstream = 1000
26.3561.136	Maximum-Data-Rate-Downstream	integer	4294967295 b/s	For example: Maximum-Data-Rate-Downstream = 1000
26.3561.137	Minimum-Data-Rate-Upstream-Low-Power	integer	4294967295 b/s	For example: Minimum-Data-Rate-Upstream-Low-Power = 1000
26.3561.138	Minimum-Data-Rate-Downstream-Low-Power	integer	4294967295 b/s	For example: Minimum-Data-Rate-Downstream-Low-Power = 1000
26.3561.139	Maximum-Interleaving-Delay-Upstream	integer	4294967295 ms	For example: Maximum-Interleaving-Delay-Upstream = 10
26.3561.140	Actual-Interleaving-Delay-Upstream	integer	4294967295 ms	For example: Actual-Interleaving-Delay-Upstream = 10
26.3561.141	Maximum-Interleaving-Delay-Downstream	integer	4294967295 ms	For example: Maximum-Interleaving-Delay-Downstream = 10
26.3561.142	Actual-Interleaving-Delay-Downstream	integer	4294967295 ms	For example: Actual-Interleaving-Delay-Downstream = 10

Table 3 **Subscriber Host Identification (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
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 without FCS(6), Ethernet over AAL5 Null w FCS(7), Ethernet over AAL5 Null without 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	ipaddr	4 bytes	For example: ERX-Primary-Dns = 9.1.1.1
26.4874.5	ERX-Secondary-Dns	ipaddr	4 bytes	For example: ERX-Secondary-Dns = 9.1.1.2
26.4874.6	ERX-Primary-Wins	ipaddr	4 bytes	For example: ERX-Primary-Wins = 9.1.1.1
26.4874.7	ERX-Secondary-Wins	ipaddr	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
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

Table 3 **Subscriber Host Identification (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
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 to 30] deci-seconds	For example: 3 seconds pado-delay Alc-PPPoE-PADO-Delay = 30
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	247 chars	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

Table 3 **Subscriber Host Identification (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.99	Alc-Ipv6-Address	ipv6addr	16 bytes	For example: Alc-Ipv6-Address 2021:1:FFF5::1
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 = myGTPgroupinterface
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

Table 3 **Subscriber Host Identification (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.126	Alc-Subscriber-QoS-Override	string	18 attributes	<direction>:<QoS object>:[<id or name>:][<parameter>=value,...] [ileE]:[qQ]:<queue-id>:(pir|cir|mbs|cbs) [eE]:[qQ]:<queue-id>:(wrr_weight|class_weight) [ileE]:[pP]:<policer-id>:(pir|cir|mbs|cbs) [eE]:[rR]:(rate) [eE]:[lL]:(rate) [eE]:[gG]:<wrr-group-id>:(rate|class-weight) [ileE]:[aA]:root:(rate) [ileE]:[sS]:<scheduler-name>:(rate|cir) See [26.6527.126] Alc-Subscriber-QoS-Override Attribute Details for a detailed description of the attribute format. For example: ingress queue 1 pir, cir, mbs, cbs and egress aggregate rate overrides Alc-Subscriber-QoS-Override += i:q:1:pir=40000,cir=20000,mbs=32000,cbs=16000, Alc-Subscriber-QoS-Override += e:r:rate=800000
26.6527.128	Alc-ATM-Ingress-TD-Profile	integer	[1 to 1000] id	For example: Alc-ATM-Ingress-TD-Profile = 10
26.6527.129	Alc-ATM-Egress-TD-Profile	integer	[1 to 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 to 100000] kb/s	For example: rate 4M b/s Alc-Access-Loop-Rate-Down = 4000

Table 3 **Subscriber Host Identification (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
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 without FCS(6), Ethernet over AAL5 Null with FCS(7), Ethernet over AAL5 Null without 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 to 4294967295]	0 : False - start IPv6CP negotiation only when IPv6 attributes are obtained in authentication >0 : True - also start IPv6CP negotiation when no IPv6 attributes are obtained in authentication For example: Alc-PPP-Force-IPv6CP = 1
26.6527.136	Alc-Onetime-Http-Redirection-Filter-Id	string	249 bytes	“Ingr-v4:<number>” [1 to 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
26.6527.146	Alc-Wlan-APN- Name	string	247 bytes	The APN is directly reflected as present in the incoming GTP-C message. For example: Alc-Wlan-APN-Name = demo.mnc001.mcc001.gprs
26.6527.147	Alc-MsIsdn	string	9 to 15 digits	Textual representation of the MSISDN in decimal format. For example: Alc-MsIsdn = 13109976224

Table 3 **Subscriber Host Identification (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.160	Alc-Relative-Session-Timeout	integer	[0 to 2147483647] seconds	0 = infinite (no session-timeout) [0 to 2147483647] in seconds For example: Alc-Relative-Session-Timeout = 3600
26.6527.161	Alc-Delegated-IPv6-Prefix-Length	integer	[48 to 64] DPL length	For example: Alc-Delegated-IPv6-Prefix-Length = 48
26.6527.174	Alc-Lease-Time	integer	[0 to 4294967295] seconds	0 : fallback to the default lease-time of 7 days. The maximum value 4294967295 corresponds with a lease-time > 9999 days (24855d 03h). [1 to 4294967295] lease-time in 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	URL string. An empty string removes the override. For example: Alc-Portal-Url = “http://portal.com/welcome/sub=$SUB”
26.6527.178	Alc-Ipv6-Portal-Url	string	247 chars	URL string. An empty string removes the override. For example: Alc-IPv6-Portal-Url = “http://portal.com/welcome/sub=$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"

Table 3 **Subscriber Host Identification (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
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.
26.6527.191	Alc-ToServer-Dhcp6-Options	octets	2 attributes 247 bytes/ attribute 494 bytes total	For example, when the DHCPv6 solicit contains following options: Option : ELAPSED_TIME (8), Length : 2 Time : 0 seconds Option : CLIENTID (1), Length : 10 LL : HwTyp=0001,LL=005100000002 00030001005100000002 Option : ORO (6), Length : 4 Requested Option : IA_NA (3) Requested Option : IA_PD (25) Option : IA_NA (3), Length : 12 IAID : 0 Time1: 0 seconds Time2: 0 seconds Option : IA_PD (25), Length : 12 IAID : 1 Time1: 0 seconds Time2: 0 seconds Alc-ToServer-Dhcp6-Options = 0x00080002000000010000a000300010051000000020006000400030019000300 0c0000000000000000000000000019000c000000010000000000000000

Table 3 **Subscriber Host Identification (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.192	Alc-ToClient-Dhcp6-Options	octets	8 attributes 247 bytes/ attribute 494 bytes total	For example, to insert following option: Option: Simple Network Time Protocol Server (31) Length: 32 Value: SNTP servers address: 2001:db8:cafe:1::1 SNTP servers address: 2001:db8:cafe:2::1 Alc-ToClient-Dhcp6-Options = 0x001F002020010DB8CAFE0001000000000000000120010DB8CAFE0002000000000000000001
26.6527.200	Alc-v6-Preferred-Lifetime	integer	[300 to 315446399] seconds	For example: Alc-v6-Preferred-Lifetime = 3600
26.6527.201	Alc-v6-Valid-Lifetime	integer	[300 to 315446399] seconds	For example: Alc-v6-Valid-Lifetime = 86400
26.6527.202	Alc-Dhcp6-Renew-Time	integer	[0 to 604800] seconds	For example: Alc-Dhcp6-Renew-Time = 1800
26.6527.203	Alc-Dhcp6-Rebind-Time	integer	[0 to 1209600] seconds	For example: Alc-Dhcp6-Rebind-Time = 2880
26.6527.217	Alc-UPnP-Sub-Override-Policy	string	32 chars	UPnP policy name or special values “_tmnx_no_override” or “_tmnx_disabled”. For example: Alc-UPnP-Sub-Override-Policy = “my-UPnP-policy”
26.6527.228	Alc-Trigger-Acct-Interim	string	247 chars	Free formatted string that is echoed in the triggered interim update message. For example: Alc-Trigger-Acct-Interim = "CoA - Filter update"

Table 3 **Subscriber Host Identification (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.232	Alc-Acct-Interim-lvl	integer	1 VSA per tag per message Max. tag 1- 5 Value [300 to 15552000]	Tagged attribute A value of 0 (zero) disables the generation of interim update messages. A value [1 to 299] seconds is rounded to 300s (min. CLI value) and a value > 15552000 seconds (max. CLI value) is rounded to the max. CLI value. An untagged attribute or tag value of 0 (zero) and tag values greater than 5 are not supported and result in a host setup failure or CoA Reject. A tag value of [1 to 5] changes the update interval of the corresponding accounting policy specified in the subscriber profile. For example: Alc-Acct-Interim-lvl:1 += 300 Alc-Acct-Interim-lvl:2 += 600

Table 3 **Subscriber Host Identification (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.234	Alc-DNAT-Override	string	247 chars	{DNAT-state | DNAT-ip-addr}[,nat-policy-name] DNAT state = none | disable • none — Negates any previous DNAT related override in the referenced (*nat-policy-name*) or default **nat-policy**. Consequently, the DNAT functionality is set as originally defined in the **nat-policy**. • disable — Disables DNAT functionality in the referenced (*nat-policy-name*) or default **nat-policy**. DNAT-ip-addr = IPv4 address in dotted format (a.b.c.d) • implicit enable with specified destination IP DNAT-state and DNAT-ip-addr parameters are mutually exclusive nat-policy-name = name of the **nat-policy**. This is an optional parameter and if not specified then the default **nat-policy** is assumed. If two parameters are present simultaneously within the Alc-DNAT-Override attribute, then they are separated by a comma with no white spaces used as delimiter. For example: Alc-DNAT-Override=none This re-enables DNAT functionality in the default **nat-policy**, assuming that DNAT was previously disabled via the Alc-DNAT-Override=disable attribute submitted either in Access-Accept or in a previous CoA. If the **none** value was received at the time when the DNAT is already enabled, a CoA ACK is sent back to the originator. This negates any previous DNAT-related override in the default **nat-policy**. The DNAT functionality is set as originally defined in the default **nat-policy**. If the DNAT classifier is not present in the default nat-policy when this CoA is received, an error log message is raised.

Table 3 **Subscriber Host Identification (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.234				For example: Alc-DNAT-Override =1.1.1.1, nat-pol-1 This changes the default DNAT IP address to 1.1.1.1 in the specified **nat-policy** with name **nat-policy-1**. DNAT is implicitly enabled in case that it was disabled before this CoA was received. For example: Alc-DNAT-Override = none, 1.1.1.1 DNAT-state and DNAT-ip-addr parameters are mutually exclusive within the same Alc-DNAT-Override attribute. A CoA ACK is returned to the RADIUS server and an error event is logged.
26.6527.238	Alc-Remove-Override	string	Single attribute identifier per attribute Multiple attributes per message	[<action><space>]<attribute identifier> See [26.6527.238] Alc-Remove-Override Attribute Details for a detailed description of the attribute format and its possible values For example: To deactivate an ESM L2TP steering profile: Alc-Remove-Override = "deactivate 241.26.6527.25”
26.6527.242	Alc-Radius-Py	octets	247 bytes	Free formatted attribute value for use with a corresponding RADIUS Python script.
26.6527.244	Alc-Force-DHCP-Relay	string	max. 2 attributes fixed values	Fixed values: “relay-ipv4” – sets the lease origin to DHCP “relay-ipv6” – sets the lease origin to DHCP6 For example: Alc-Force-DHCP-Relay = “relay-ipv4”
241.26.6527.16	Alc-IPv6-Router-Adv-Policy	string	32 chars	The Router Advertisement policy name. For example: Alc-IPv6-Router-Adv-Policy = “RA-policy-01”
241.26.6527.17	Alc-Nat-Outside-IPs	string	max. 4 attributes	<outside IP address>;<NAT policy name> For example: Alc-Nat-Outside-IPs += 192.0.2.1;nat-policy-1 Alc-Nat-Outside-IPs += 198.51.100.1;nat-policy-2

Table 3 **Subscriber Host Identification (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
241.26.6527.18	Alc-Mld-Import-Policy	string	32 chars Up to 14 attributes	The MLD import policy name. A subscriber can have a list of up to 14 MLD import policies associated from Radius. Each MLD policy must be included in a separate attribute. For example: Alc-Mld-Import-Policy=”ch-lineup-01”
241.26.6527.24	Alc-IPv6-DMZ-Enabled	Integer	[0..1]	0: DMZ disabled 1: DMZ enabled For example: DMZ enabled Alc-IPv6-DMZ-Enabled = 1
241.26.6527.27	Alc-IPv6-Sub-If-Prefix	string	127 chars Max. 1 attribute	<IPv6 prefix>/<prefix length><space><type> Where <*type*> is either **pd**, **wan-host**, or **wan-host pd**. When not specified, **pd** is assumed. A maximum of one prefix per subscriber host or session can be specified and up to 24 prefixes per system or per subscriber interface. For example: Alc-IPv6-Sub-If-Prefix = “2000::/32 pd” Alc-IPv6-Sub-If-Prefix = “2000::/32 wan-host pd” Alc-IPv6-Sub-If-Prefix = “2000::/32”
241.26.6527.35	Alc-Mld-Import-Policy-Modif	string	34 chars Max. 5 attribute	<action>:<MLD policy name> where <action> is a — Adds the MLD policy to the list of import policies. s – Subtracts (removes) the MLD policy from the list of import policies. For example: Alc-Mld-Import-Policy-Modif=”a:ch-lineup-01” Alc-Mld-Import-Policy-Modif=”s:ch-lineup-02”
241.26.6527.37	Alc-VAS-IPv4-Filter	string	1..32 characters	Name of a VAS filter as defined under **configure subscriber-mgmt isa-service-chaining vas-filter** For example: Alc-VAS-IPv4-Filter="vas_filter_1"

Table 3 **Subscriber Host Identification (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
241.26.6527.38	Alc-VAS-NSH-IPv4-Opaque-Meta-Data	octets	16 bytes	Opaque data in network order to send in NSH. This will only be applicable if insert-nsh is correctly configured and will override insert-subscriber-id or opaque data configured under **configure subscriber-mgmt isa-service-chaining vas-filter** *filter-name* **entry** *id* **action {downstream|upstream} insert-nsh meta-data**.
241.26.6527.39	Alc-Static-Port-Forward	string	64 SPFs	See [241.26.6527.39] Alc-Static-Port-Forward Attribute Details for a detailed description of the attribute format and its possible values For example: Add an l2-aware NAT SPF to open up TCP port 80 (HTTP) on the outside and forward it to port 8080 on ip 1.1.1.1 on the inside: Alc-Static-Port-Forward = "c tcp 1.1.1.1 8080->80"
241.26.6527.40	Alc-IPv6-Slaac-Replacement-Prefix	ipv6prefix	Max. 16 Bytes for prefix + 1 Byte for length	<ipv6-prefix/prefix-length> with prefix-length 64 For example: Alc-IPv6-Slaac-Replacement-Prefix = 2021:1:FFF3:1::/64
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
26.10415.20	3GPP-IMEISV	string	14 to 16 digits	3GPP vendor specific attribute as defined in TS 29.061
26.10415.21	3GPP-RAT-Type	octets	1 octet [0..255]	Specifies the Radio Access Technology type, see 3GPP 29.061 section 16.4.7.2. for more details For example (E-UTRAN RAT Type): 3GPP-RAT-Type = 0x06
26.10415.22	3GPP-User-Location-Info	octets	247 bytes	3GPP vendor specific attribute as defined in TS 29.061

Table 4 **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 [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+	0+
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 [1]
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 [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 [1]
99	Framed-IPv6-Route	0	0+	0

Table 4 **Subscriber Host Identification (Applicability) (Continued)**

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request
100	Framed-IPv6-Pool	0	0-1	0
101	Error-Cause	0	0	0-1
123	Delegated-IPv6-Prefix	0	0-1	0-1 [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	0-1	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
26.3561.142	Actual-Interleaving-Delay-Downstream	0-1	0	0

Table 4 **Subscriber Host Identification (Applicability) (Continued)**

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request
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	0-1
26.4874.48	ERX-Ipv6-Secondary-Dns	0	0-1	0-1
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 [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	0-1
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 [1]
26.6527.100	Alc-Serv-Id	0	0-1	0

Table 4 **Subscriber Host Identification (Applicability) (Continued)**

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request
26.6527.101	Alc-Interface	0	0-1	0
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	0-1
26.6527.106	Alc-Ipv6-Secondary-Dns	0	0-1	0-1
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
26.6527.146	Alc-Wlan-APN-Name	0-1	0	0
26.6527.147	Alc-MsIsdn	0-1	0	0
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

Table 4 **Subscriber Host Identification (Applicability) (Continued)**

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request
26.6527.185	Alc-Onetime-Http-Redirect-Reactivate	0	0	0-1
26.6527.191	Alc-ToServer-Dhcp6-Options	0+	0	0
26.6527.192	Alc-ToClient-Dhcp6-Options	0	0+	0
26.6527.200	Alc-v6-Preferred-Lifetime	0	0-1	0
26.6527.201	Alc-v6-Valid-Lifetime	0	0-1	0
26.6527.202	Alc-Dhcp6-Renew-Time	0	0-1	0
26.6527.203	Alc-Dhcp6-Rebind-Time	0	0-1	0
26.6527.217	Alc-UPnP-Sub-Override-Policy	0	0-1	0-1
26.6527.228	Alc-Trigger-Acct-Interim	0	0	0-1
26.6527.232	Alc-Acct-Interim-Ivl	0	0+	0+
26.6527.234	Alc-DNAT-Override	0	0+	0+
26.6527.238	Alc-Remove-Override	0	0	0+
26.6527.242	Alc-Radius-Py	0+	0+	0+
26.6527.244	Alc-Force-DHCP-Relay	0	0+	0
241.26.6527.16	Alc-IPv6-Router-Adv-Policy	0	0-1	0-1
241.26.6527.17	Alc-Nat-Outside-IPs	0	0+	0+
241.26.6527.18	Alc-Mld-Import-Policy	0	0+	0+
241.26.6527.19	Alc-Bonding-Id [2]	0	0-1	0
241.26.6527.22	Alc-Bonding-Reference-Rate	0	0-1	0-1
241.26.6527.27	Alc-IPv6-Sub-If-Prefix	0	0-1	0
241.26.6527.35	Alc-Mld-Import-Policy-Modif	0	0	0+
241.26.6527.37	Alc-VAS-IPv4-Filter	0	0-1	0-1
241.26.6527.38	Alc-VAS-NSH-IPv4-Opaque-Meta-Data	0	0-1	0-1
241.26.6527.39	Alc-Static-Port-Forward	0	0+	0+
241.26.6527.40	Alc-IPv6-Slaac-Replacement-Prefix	0	0	0-1
26.10415.5	3GPP-GPRS-Negotiated-QoS-Profile	0-1	0-1	0

Table 4 **Subscriber Host Identification (Applicability) (Continued)**

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request
26.10415.20	3GPP-IMEISV	0-1	0	0
26.10415.21	3GPP-RAT-Type	0-1	0	0
26.10415.22	3GPP-User-Location-Info	0-1	0	0

Notes:

1. Can be included as (part of) CoA key to identify one or multiple subscriber host(s) or session(s). See Subscriber Host Identification section for details.
2. Attribute description and limits are defined in the Bonding section.

1.2.1.1 [26.6527.126] Alc-Subscriber-QoS-Override Attribute Details

The format for [26.6527.126] Alc-Subscriber-QoS-Override is a string formatted as:

<direction>:<QoS object>:[<id or name>:][<parameter>=value,...]

Table 5 provides details on the respective fields.

Multiple parameters can be combined in a comma separated list.

The direction must be specified as:

- i or I for ingress
- e or E for egress

For example:

Alc-Subscriber-QoS-Override = "E:Q:1:pir=2000,cir=1000"

Overrides are always stored as part of the subscriber host or session but are only applied when the override is valid in the active QoS configuration. For example:

- An egress queue 5 PIR rate override is stored with the subscriber session but not applied when the sap-egress QoS policy has no queue 5 defined
- An HSQ egress queue wrr-weight override is stored with the subscriber session but not applied when the queue is not attached to a WRR group.

Table 5 **Alc-Subscriber-QoS-Override Attribute Details**

Direction	QoS object	Id or Name	Parameter=value	Description
i, I, e or E	q or Q	queue id [1..32] ingress [1..8] egress	pir=<pir-rate>	Queue PIR value in kilobits per second -1 or "max" : maximum value -2 : no override
			cir=<cir-rate>	Queue CIR value in kilobits per second -1 or "max" : maximum value -2 : no override
			mbs=<mbs-size>	Queue MBS size in bytes -1 or "max" : maximum value -2 : no override
			cbs=<cbs-size>	Queue CBS size in bytes -1 or "max" : maximum value -2 : no override
e or E	q or Q	queue id [1..8]	class_weight=<weight>	Class weight [1, 2, 4 or 8] -2 : no override Applies to HSQ hs-class-weight
e or E	q or Q	queue id [1..4] HSMDA [1..8] HSQ	wrr_weight=<weight>	WRR weight [1..4] for HSMDAv2 [1..127] for HSQ -2 : no override Applies to HSMDAv2 wrr_weight or HSQ hs-wrr-weight

Table 5 **Alc-Subscriber-QoS-Override Attribute Details (Continued)**

Direction	QoS object	Id or Name	Parameter=value	Description
i, I, e or E	p or P	policer id [1..63]	pir=<pir-rate>	Policer PIR value in kilobits per second -1 or "max" : maximum value -2 : no override
			cir=<cir-rate>	Policer CIR value in kilobits per second -1 or "max" : maximum value -2 : no override
			mbs=<mbs-size>	Policer MBS size in bytes -1 or "max" : maximum value -2 : no override
			cbs=<cbs-size>	Policer CBS size in bytes -1 or "max" : maximum value -2 : no override
e or E	r or R	not applicable	rate=<rate>	Egress aggregate rate in kilobits per second -1 or "max" : maximum value -2 : no override applies to sub-profile agg-rate-limit or HSQ sub-profile hs-agg-rate-limit For HSQ hs-sla-mode single, the applied rate is the minimum between the sla-profile and sub-profile hs-agg-rate-limit
e or E	l or L	not applicable	rate=<rate>	Egress aggregate rate in kilobits per second -1 or "max" : maximum value -2 : no override applies to HSQ sla-profile hs-agg-rate-limit For HSQ hs-sla-mode single, the applied rate is the minimum between the sla-profile and sub-profile hs-agg-rate-limit

Table 5 **Alc-Subscriber-QoS-Override Attribute Details (Continued)**

Direction	QoS object	Id or Name	Parameter=value	Description
e or E	g or G	wrr group id [1..2]	rate=<rate>	WRR group PIR value in kilobits per second -1 or "max" : maximum value -2 : no override applies to HSQ hs-wrr-group <group-id> rate
			class-weight=<weight>	WRR groups class weight [1, 2, 4 or 8] -2 : no override applies to HSQ hs-wrr-group <group-id> hs-class-weight
i, I, e or E	a or A	fixed name: root	rate=<rate>	Root arbiter rate in kilobits per second -1 or "max" : maximum value -2 : no override
i, I, e or E	s or S	scheduler-name	rate=<pir-rate>	Scheduler PIR rate in kilobits per second -1 or "max" : maximum value -2 : no override
			cir=<cir-rate>	Scheduler CIR rate in kilobits per second -1 or "max" : maximum value -2 : no override "sum" : sum of the queue or policer CIRs parented to the scheduler

1.2.1.2 [26.6527.238] Alc-Remove-Override Attribute Details

The format for [26.6527.238] Alc-Remove-Override is a string formatted as:

[<action><space>]<attribute identifier>

where <action> is:

- **deactivate** - Deactivates the function that was activated with the specified VSA.
- no <action> specified - Remove the override that was installed with the specified VSA.

  If the CoA target is:

– an ESM subscriber host/session or a vRGW session -> BRG level, then the application falls back to the system default for that attribute
– a vRGW session -> session level, then the application falls back to the BRG level value for that attribute. If there is no BRG level attribute specified, then the application falls back to the system default for that attribute. For some attributes, a BRG level value must be present: fallback to the system default is not possible

where <attribute identifier> is a single attribute identifier specified in dotted number notation or alternatively using a "-" (hyphen) as the delimiter.

Table 6 lists the attribute identifiers that can be specified as value in the Alc-Remove-Override VSA to remove the override from or to deactivate the action triggered by the references attributes.

Table 6 **Alc-Remove-Override Attribute - Applicable Attribute Identifiers**

Attribute ID	Attribute Name	Action		Applicability		
				ESM Session/ Host	vRGW session	
		Unspecified -remove override	Deactivate		BRG level	Session level
92	NAS-Filter-Rule	✓	X	X	n/a	✓ [1]
26.6527.13	Alc-SLA-Prof-Str	✓	X	X	n/a	✓ [1]
26.6527.45	Alc-App-Prof-Str	✓	X	X	n/a	✓ [1]
26.6527.126	Alc-Subscriber-QoS-Override	✓	X	X	n/a	✓
26.6527.134	Alc-Subscriber-Filter	✓	X	X	n/a	✓ [1]
26.6527.158	Alc-Nas-Filter-Rule-Shared	✓	X	X	n/a	✓ [1]
26.6527.182	Alc-AA-Sub-Http-Url-Param	✓	X	X	n/a	✓ [1]
26.6527.193	Alc-AA-App-Service-Option	X	✓	X	✓	✓
241.26.6527.17	Alc-Nat-Outside-IP	X	✓	X	✓	n/a
241.26.6527.25	Alc-Steering-Profile	X	✓	✓	X	X
241.26.6527.37	Alc-VAS-IPv4-Filter	X	✓	✓	✓	✓
241.26.6527.39	Alc-Static-Port-Forward	X	✓	X	✓	n/a

Note:

1. A BRG level value must be present when removing: it is not possible to fall back to system default.

1.2.2 Wholesale-Retail — Local Access Mode

Table 7 **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. (**configure service ies | vprn** *retail-service-id* **subscriber-interface** *retail-interface-name* **fwd-service** *wholesale-service-id* **fwd-subscriber-interface** *wholesale-interface-name*). Returning an IES service ID for an IPoEv4 host is treated as a session setup failure. This attribute must be included together with NAS-Port-Id and an IP-address or prefix attribute in a CoA targeting a subscriber host in a retail service.
26.6527.31	Alc-MSAP-Serv-Id	The service ID where Managed SAPs 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/ipoe host msap-defaults service** *service-id* or **configure service vpls** *service-id* **sap** *sap-id* **msap-defaults service** *service-id*). This omitted attribute without explicitly 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 would be configured for a regular subscriber SAP. If this attribute is omitted, then the MSAP default configured in **ludb** or **capture-sap** is used (**configure subscriber-mgmt local-user-db ppp/ipoe host** *host-name* **msap-defaults policy** *msap-policy-name* or **configure service vpls** *service-id* **sap** *sap-id* **msap-defaults policy** *msap-policy-name*).This omitted attribute without explicitly 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** *service -id* **subscriber-interface** *ip-int-name* **group-interface** *ip-int-name*. If this attribute is omitted, the MSAP defaults configured in the **ludb** or **capture-sap** are used. (**configure subscriber-mgmt local-user-db** *local-user-db-name* **ppp/ipoe host** *host-name* **msap-defaults group-interface** *ip-int-name* or **configure service vpls** *service-id* **sap** *sap-id* **msap-defaults group-interface** *ip-int-name*). Strings above the limits and an omitted attribute without explicitly created MSAP defaults are treated as setup failures.

Table 8 **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 9 **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	0-1
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

1.2.3 Wholesale-Retail — L2TP Tunneled Access Mode

Table 10 **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 a 7750 SR LNS. For L2TP Tunnel or Link Accounting, this attribute is always included on LAC and LNS.

Table 10 **Wholesale-Retail: L2TP Tunneled Access Mode (Description) (Continued)**

Attribute ID	Attribute Name	Description
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 a 7750 SR LNS. For L2TP Tunnel or 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. Preconfigured 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 a 7750 SR LNS. For L2TP Tunnel or 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 is also on the LAC the destination IP for all L2TP packets for that tunnel. To support more than 31 tunnels in a single RADIUS Access-Accept message, multiple Tunnel-Server-Endpoint attributes with the same tag can be inserted. All tunnels specified by Tunnel-Sever-Endpoint attributes with a given tag uses the tunnel parameters specified by the other Tunnel attributes having the same tag value.
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. Preconfigured 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 character limit are truncated at that limit.

Table 10 **Wholesale-Retail: L2TP Tunneled Access Mode (Description) (Continued)**

Attribute ID	Attribute Name	Description
81	Tunnel-Private-Group-ID	The group ID for a particular tunneled session. This RADIUS attribute is copied by a 7750 SR 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 SR 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 tunneling 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 to 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 to 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 tunneling 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).

Table 10 **Wholesale-Retail: L2TP Tunneled Access Mode (Description) (Continued)**

Attribute ID	Attribute Name	Description
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 or 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. Preconfigured 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 or 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. Preconfigured 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. Preconfigured 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/service vprn** *service-id* **l2tp group** *tunnel-group-name*. Any other RADIUS returned L2TP parameter is ignored and other required info to setup the tunnel should 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/service vprn** *service-id* **l2tp group** *tunnel-group-name*. Any other RADIUS returned L2TP parameter is ignored and other required info to setup the tunnel should come from the CLI-created context. Strings above the limits are treated as a setup failure.

Table 10 **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, weighted-random or existing-first) to one of the set of suitable tunnels that are available or could be made available. A preconfigured algorithm (**configure router/service vprn** *service-id* **l2tp session-assign-method**) is used when this attribute is omitted. Attribute 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 weighted-access attribute value (**session-assign-method weighted**) specifies that the sessions are equally distributed over the available tunnels; 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. When there are multiple tunnels with an equal number of sessions (equal weight), LAC selects the first tunnel from the candidate list. The weighted-random attribute value enhances the weighted-access algorithm such that when there are multiple tunnels with an equal number of sessions (equal weight), LAC randomly selects a tunnel. The maximum number of sessions per tunnel is retrieved via attribute 26.6527.48 Alc-Tunnel-Max-Sessions or set to a preconfigured 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 to 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. Preconfigured 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 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. Preconfigured 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 the Limits are treated as setup failures.

Table 10 **Wholesale-Retail: L2TP Tunneled Access Mode (Description) (Continued)**

Attribute ID	Attribute Name	Description
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. Preconfigured values are used when attribute is omitted (**configure router/ service vprn** *service-id* **l2tp hello-interval**). Values outside the limits are treated as a setup failure.
26.6527.51	Alc-Tunnel-Destruct-Timeout	The time in seconds that operational data of a disconnected tunnel persists 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. Preconfigured values are used when attribute is omitted (**configure router/service vprn** *service-id* **l2tp destruct-timeout**). Values outside the 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 back-off 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. Preconfigured values are used when attribute is omitted (**configure router/service vprn** *service-id* **l2tp max-retries-estab**). Values outside the 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 back-off 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. Preconfigured values are used when attribute is omitted (**configure router/service vprn** *service-id* **l2tp max-retries-not-estab**). Values outside the limits are treated as a setup failure.

Table 10 **Wholesale-Retail: L2TP Tunneled Access Mode (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.54	Alc-Tunnel-AVP-Hiding	Indicates if data is hidden 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 AVPs are passed in cleartext if the attribute is omitted and corresponds with the **nothing** value. The **sensitive-only** value specifies that the H bit is only set for AVPs containing sensitive information. The **all** value specifies that the H bit is set for all AVPs where it is allowed. The value with tag 0 is used as default for the tunnels where the value is not specified. Preconfigured values are used when the 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 fails for **sensitive-only** and **all** values. Values outside the Limits are treated as a setup failure.
26.6527.97	Alc-Tunnel-Challenge	Indicates whether the tunnel authentication (challenge-response) is to be used. L2TP tunnel-authentication is based on RFC 1994 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 preconfigured 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 **always** value is used. When the attribute has the **always** value, no [69] Tunnel-Password attribute is specified and no preconfigured 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 service ID on the LNS node where the PPP sessions are established (**configure service ies/vprn** *service-id* **subscriber-interface** *name* **group-interface** *name*). Preconfigured values are used if attribute is omitted (**configure subscriber-mgmt local-user-db** *local-user-db-name* **ppp host** *host-name* **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.

Table 10 **Wholesale-Retail: L2TP Tunneled Access Mode (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.101	Alc-Interface	Refers to the group interface *ip-int-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* **lns**). Preconfigured values are used if the attribute is omitted (**configure subscriber-mgmt local-user-db** *local-user-db-name* **ppp host** *host-name* **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 equals Base. Values above the limits or unreferenced are treated as a setup failure.
26.6527.120	Alc-Tunnel-Rx-Window-Size	The initial receive window size being offered to the remote peer. This attribute is copied in the 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 preconfigured value is used when the 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 preconfigured 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 L2TP sessions and send these accounting data to a RADIUS server. Different RADIUS attributes such as [66] Tunnel-Client-Endpoint, [67] Tunnel-Server-Endpoint, [68] Acct-Tunnel-Connection, [82] Tunnel-Assignment-ID can 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. Preconfigured values are used when the 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 10 **Wholesale-Retail: L2TP Tunneled Access Mode (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.204	Alc-Tunnel-DF-bit	This attribute is used on an L2TP LAC only. By default, a LAC does not allow L2TP packet fragmentation by sending L2TP towards the LNS with the Do not Fragment (DF) bit set to 1. This DF bit can be set to 0 to allow downstream routers to fragment the L2TP packets. The LAC itself will not fragment L2TP packets. Packets sent with MTU bigger than the allowed size on the LAC egress port are dropped. This attribute is silently ignored if RADIUS returns an Alc-Tunnel-Group attribute. In that case, the tunnel level, group level, or as last resort, the root level configuration is used instead.
26.6527.214	Alc-Tunnel-Recovery-Method	Sets the L2TP LAC failover recovery method to be used for this tunnel: MCS or recovery tunnel (RFC 4951). Preconfigured values are used when the attribute is omitted (**configure router/service vprn** *service-id* **l2tp failover recovery-method**). When the tunnel recovery method is set to **recovery-tunnel** but LNS does not support this capability, then the system automatically falls back to **mcs**. Values outside the limits are treated as a setup failure.
26.6527.215	Alc-Tunnel-Recovery-Time	Only applicable when the L2TP LAC failover recovery-method is set to recovery-tunnel. Sets the L2TP LAC failover recovery-time to be negotiated with LNS via L2TP failover extensions (RFC 4951). It indicates to the LNS how long it needs to extend its protocol retry timeout before declaring the control channel down. Preconfigured values are used when attribute is omitted (**configure router/service vprn** *service-id* **l2tp failover recovery-time**). Values outside the limits are treated as a setup failure.
241.26.6527.25	Alc-Steering-Profile	The steering profile that should be applied to perform traffic steering on L2TP LAC. The steering profile is configured in the following CLI context: **configure subscriber-mgmt steering-profile** *name*. An L2TP LAC session is successfully set up when a non-existent steering profile name is referenced in an Access-Accept. A CoA containing a non-existent steering profile is rejected. In both cases, the non-existent steering profile is stored in the L2TP LAC session information and becomes active when the profile is configured at a later stage. To deactivate traffic steering on L2TP LAC, the [26.6527.238] Alc-Remove-Override attribute must be used.

Table 11 **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	Max. length = 15 bytes (untagged) or 16 bytes (tagged)	<tag field><dotted-decimal IP address used on LAC as L2TP src-ip> If the 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	Max. length = 15 bytes (untagged) or 16 bytes (tagged) Max. 451 attributes or limited by RADIUS message size	<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 = 01332e332e332e33 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

Table 11 **Wholesale-Retail: L2TP Tunneled Access Mode (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
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
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 preconfigured tunnel-group For example: ERX-Tunnel-Group:0 = MyCliTunnelGroupName
26.6527.46	Alc-Tunnel-Group	string	32 chars	node preconfigured tunnel-group For example: Alc-Tunnel-Group = MyCliTunnelGroupName
26.6527.47	Alc-Tunnel-Algorithm	integer	values [1 to 3]	1=weighted-access, 2=existing-first, 3=weighted-random default=existing-first For example: Alc-Tunnel-Algorithm:0 = weighted-access

Table 11 **Wholesale-Retail: L2TP Tunneled Access Mode (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.48	Alc-Tunnel-Max-Sessions	integer	131071	max sessions per group 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
26.6527.49	Alc-Tunnel-Idle-Timeout	integer	3600 seconds	infinite = -1 or [0 to 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 to 3600] seconds	no keepalive = -1 or [60 to 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 to 86400] seconds	[60 to 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 to 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 to 7]	default 5 For example: # retry 2 times for all tunnels in tunnel group Alc-Tunnel-Max-Retries-Not-Estab:0 = 2

Table 11 **Wholesale-Retail: L2TP Tunneled Access Mode (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.54	Alc-Tunnel-AVP-Hiding	integer	values [1 to 3]	1=nothing,2=sensitive-only,3=all; default nothing 1=nothing: All L2TP AVPs 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
26.6527.97	Alc-Tunnel-Challenge	integer	values [1 to 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 to 1024]	Tag 0 = default when not specified (all tunnels) Tag 1 to 31 = specific tunnel 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
26.6527.204	Alc-Tunnel-DF-bit	integer	values [0 to 1]	0=clr-lac-data, 1=set-lac-data; default = 1 For example: Alc-Tunnel-DF-bit:0 = clr-lac-data

Table 11 **Wholesale-Retail: L2TP Tunneled Access Mode (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.214	Alc-Tunnel-Recovery-Method	integer	values [0 to 1]	0=recovery-tunnel, 1=mcs; default = 0 For example: Alc-Tunnel-Recovery-Method:1 = recovery-tunnel
26.6527.215	Alc-Tunnel-Recovery-Time	integer	[0 to 900] seconds	[0 to 900] in seconds; default = 0 For example: Alc-Tunnel-Recovery-Time = 180
241.26.6527.25	Alc-Steering-Profile	string	32 chars	Steering profile name For example: Alc-Steering-Profile = “steering-profile-1”

Table 12 **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

Table 12 **Wholesale-Retail: L2TP Tunneled Access Mode (Applicability) (Continued)**

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request	Encrypted	Tag	Max. Tag
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
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 (untag-ged)
26.6527.204	Alc-Tunnel-DF-bit	0	0-1	0	N	Y	31
26.6527.214	Alc-Tunnel-Recovery-Method	0	0-1	0	N	Y	31
26.6527.215	Alc-Tunnel-Recovery-Time	0	0-1	0	N	Y	31
241.26.6527.25	Alc-Steering-Profile	0	0-1	0-1	N	N	N/A

1.2.4 Business Service Access

Table 13 **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 the next-hop points to the host's IP address 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 is installed as a standalone host without managed route). The number of routes above limits are silently ignored. Optionally, a metric, tag, and protocol preference can be specified for the managed route. If the metrics are not specified, are 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 the **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute framed-route** configuration. 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 13 **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 its 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 is installed as a standalone host without a managed route). The number of routes above limits are silently ignored. Optionally, a metric, tag, or protocol preference can be specified for the managed route. If the metrics are not specified, 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 or 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. The 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 13 **Business Access (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.55	Alc-BGP-Policy	Refers to a preconfigured policy under **configure subscriber-mgmt bgp- peering-policy** *policy-name*. Mandatory attribute for dynamic BGPv4 peering. The referenced policy contains all required parameters to setup the dynamic BGPv4 peer. Peer-AS, MD5 key, Authentication-Keychain and import and export policies can be overridden by optional RADIUS attributes. Dynamic BGPv4 peering related attributes are ignored if the session or host does not terminate in a VPRN. Host setup is successful, but without BGPv4 peering if a non-existing policy-name is received or if the SAP anti-spoof type is different from nh-mac. Policy names above the maximum length result in a host setup failure.
26.6527.56	Alc-BGP-Auth-Keychain	Optional attribute for dynamic BGPv4 peering. Refers to the keychain parameters (**configure system security keychain** *keychain-name*) used to sign or authenticate the BGP protocol stream via the TCP enhanced authentication option (draft-bonica-tcp-auth). Host setup is successful, but without BGPv4 peering if a non-existing keychain name is received. Keychain names above the maximum length result in a host setup failure. Alternative for [26.6527.57] Alc-BGP-Auth-Key.
26.6527.57	Alc-BGP-Auth-Key	Optional attribute for dynamic BGPv4 peering. Indicates the authentication key used between BGPv4 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	Optional attribute for dynamic BGPv4 peering. This refers to a preconfigured BGP export policy (**configure router policy-options policy-statement** *name*). The RADIUS received policy is appended to the list of export policies configured in the peering policy (**configure subscriber-mgmt bgp-peering-policy** *policy-name* **export** *policy-name*) if there are fewer than 15 preconfigured policies or replaces the fifteenth policy. Host setup is successful, but without export policy applied if a non-existing policy-name is received. Policy names above the maximum length result in a host setup failure.
26.6527.59	Alc-BGP-Import-Policy	Optional attribute for dynamic BGPv4 peering. Refers to a preconfigured BGP import policy (**configure router policy-options policy-statement** *name*). The RADIUS received policy is appended to the peer (if preconfigured policies for peer are smaller than 15) or replaces the fifteenth policy (if preconfigured policies for peer are exact 15). Host setup is successful but without import policy applied if a non-existing policy-name is received. Policy names above the maximum length result in a host setup failure.
26.6527.60	Alc-BGP-PeerAS	Optional attribute for dynamic BGPv4 peering. Specifies the Autonomous System number for the remote BGPv4 peer.

Table 13 **Business Access (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.207	Alc-RIP-Policy	Refers to the preconfigured policy under **configure subscriber-mgmt rip-policy** *policy-name* and enables the BNG to listen to RIPv1 or RIPv2 messages from the host (master SRRP node only in case of a dual-homed BNG). The referenced policy contains the authentication type and authentication key used to establish a RIP neighbor with this host. Host setup is successful, but the RIP message from the host are ignored if a non-existing policy name is received or if the SAP anti-spoof type is different from NH-MAC. Policy names exceeding the maximum length result in a host setup failure.
26.6527.208	Alc-BGP-IPv6-Policy	Refers to a preconfigured policy under **configure subscriber-mgmt bgp- peering-policy** *policy-name*. Mandatory attribute for dynamic BGPv6 peering. The referenced policy contains all required parameters to setup the dynamic BGPv6 peer. Peer-AS, MD5 key, Authentication-Keychain and import or export policies can be overridden by optional RADIUS attributes. Dynamic BGPv6 peering related attributes are ignored if the session or host does not terminate in a VPRN. Host setup is successful, but without BGPv6 peering if a non-existing policy name is received or if the SAP anti-spoof type is different from nh-mac. Policy names above the maximum length result in a host setup failure. Note that unlike the ESMv4 case, there is no IPv6 interface address associated with a subscriber interface. The peering address for CPE devices can be any routable IPv6 interface address in the same routing instance as the host (example a loopback interface). This requires multi-hop BGPv6 capability on the CPE.
26.6527.209	Alc-BGP-IPv6-Auth-Keychain	Optional attribute for dynamic BGPv6 peering. Refers to the keychain parameters (**configure system security keychain** *keychain-name*) used to sign or authenticate the BGPv6 protocol stream via the TCP enhanced authentication option (draft-bonica-tcp-auth). Host setup is successful, but without BGPv6 peering if a non-existing keychain name is received. Keychain names above the maximum length result in a host setup failure. Alternative for [26.6527.201] Alc-BGP-IPv6-Auth-Key.
26.6527.210	Alc-BGP-IPv6-Auth-Key	Optional attribute for dynamic BGPv6 peering. Indicates the authentication key used between BGPv6 peers before establishing sessions. Authentication is performed using the MD5 message based digest protocol. Authentication keys are truncated at 247 bytes and are not encrypted.

Table 13 **Business Access (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.211	Alc-BGP-IPv6-Export-Policy	Optional attribute for dynamic BGPv6 peering. Refers to a preconfigured BGP export policy (**configure router policy-options policy-statement** *name*). The RADIUS received policy is appended to the peer (if there are fewer than 15) or replaces the fifteenth policy. Host setup is successful, but without export policy applied if a non-existing policy name is received. Policy names above the maximum length result in a host setup failure.
26.6527.212	Alc-BGP-IPv6-Import-Policy	Optional attribute for dynamic BGPv6 peering. Refers to a preconfigured BGP import policy (**configure router policy-options policy-statement** *name*). The RADIUS received policy is appended to the peer (if there are fewer than 15) or if the received policy replaces the fifteenth policy. Host setup is successful, but without import policy applied if a non-existing policy name is received. Policy names above the maximum length result in a host setup failure.
26.6527.213	Alc-BGP-IPv6-PeerAS	Optional attribute for dynamic BGPv6 peering. Specifies the Autonomous System number for the remote BGPv6 peer.

Table 14 **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 to 65535] [tag <tag-value>] (Optional) The managed route is tagged for use in routing policies. If not specified or tag-value=0, then the route is not tagged. Value = [0 to 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 to 255]

Table 14 **Business Access (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
22 (continued)	Framed-Route	string	max. 16 Framed-Route attributes	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"
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 to 65535] [tag <tag-value>] (Optional) The managed route is tagged for use in routing policies. If not specified or tag-value=0, then the route is not tagged. Value = [0 to 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 to 255]

Table 14 **Business Access (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
99 (continued)	Framed-IPv6-Route	string	max. 16 Framed-IPv6-Route attributes	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
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 to 4294967294]	For example: Alc-BGP-PeerAS = 64500
26.6527.207	Alc-RIP-Policy	string	32 chars	For example: Alc-RIP-Policy = MyRIPPolicy
26.6527.208	Alc-BGP-IPv6-Policy	string	32 chars	For example: Alc-BGP-IPv6-Policy = MyBGPPolicy

Table 14 **Business Access (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.209	Alc-BGP-IPv6-Auth-Keychain	string	32 chars	For example: Alc-BGP-IPv6-Auth-Keychain = MyKeychain
26.6527.210	Alc-BGP-IPv6-Auth-Key	octets	247 bytes	For example: Alc-BGP-IPv6-Auth-Key = “SecuredBGPv6”
26.6527.211	Alc-BGP-IPv6-Export-Policy	string	32 chars	For example: Alc-BGP-IPv6-Export-Policy = to_dynamic_bgpv6_peer
26.6527.212	Alc-BGP-IPv6-Import-Policy	string	32 chars	For example: Alc-BGP-IPv6-Import-Policy = from_dynamic_bgpv6_peer
26.6527.213	Alc-BGP-IPv6-PeerAS	integer	[1 to 4294967294]	For example: Alc-BGP-IPv6-PeerAS = 64500

Table 15 **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
26.6527.207	Alc-RIP-Policy	0	0-1	0
26.6527.208	Alc-BGP-IPv6-Policy	0	0-1	0
26.6527.209	Alc-BGP-IPv6-Auth-Keychain	0	0-1	0
26.6527.210	Alc-BGP-IPv6-Auth-Key	0	0-1	0
26.6527.211	Alc-BGP-IPv6-Export-Policy	0	0-1	0

Table 15 **Business Access (Applicability) (Continued)**

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request
26.6527.212	Alc-BGP-IPv6-Import-Policy	0	0-1	0
26.6527.213	Alc-BGP-IPv6-PeerAS	0	0-1	0

1.2.5 Accounting On-Line Charging

Table 16 **Accounting: On-Line Charging (Description)**

Attribute ID	Attribute Name	Description
26.6527.95	Alc-Credit-Control-CategoryMap	Refers to a preconfigured category-map (**configure subscriber-mgmt category-map** *category-map-name*) that contains credit control information for up to 16 predefined categories 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 lengths above the limits are treated as a setup failure.
26.6527.96	Alc-Credit-Control-Quota	Defines a volume and time quota per category. 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 17 **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 16 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 1 Byte and (2^64 - 1 / 18446744073709551615) Bytes <time-value>: converted in seconds and stored in 32 bit counter - value '0' = no time credit - value between 1 second 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 of different time units is allowed with some restrictions: 15m30s is accepted while 15m60s is not. For example: 500 Mbytes volume credit for category cat1 and 1 day, 2 hours, 3 minutes and 4 seconds time credit for category cat2 Alc-Credit-Control-Quota += 500MB|0|cat1, Alc-Credit-Control-Quota += 0|1d2h3m4s|cat2

Table 18 **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+	0+	0+

1.2.6 IP and IPv6 Filters

Table 19 **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 or from the subscriber host matches against these entries. A range of entries must be reserved for subscriber host specific entries in a filter policy: **configure filter ip-filter/ipv6-filter** *filter-id* **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.

Table 19 **IP and IPv6 Filters (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.529.242	Ascend-Data-Filter	A local configured filter policy can be extended with shared dynamic filter entries. A dynamic copy of the base filter (the 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 or IPv6) and direction (ingress or 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 or session. If after host or session disconnection, no hosts or 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**/**ipv6 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. Shared filter entries should only be used if many hosts share the same set of filter rules that need to be controlled from RADIUS.
26.6527.134	Alc-Subscriber-Filter	Subscriber host preconfigured IP or IPv6 ingress and egress filters to be used instead of the filters defined in the SLA profile. Non-relevant fields are ignored (for example, IPv4 filters for an IPv6 host). The scope of the local preconfigured filter should be set to template for correct operation (**configure filter ip-filter/ipv6-filter** *filter-id* **scope template**). This is not enforced. For a RADIUS CoA message, if the ingress or egress field is missing in the VSA, there is 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 is active for that direction Applicable to all dynamic host types, including L2TP LNS but excluding L2TP LAC.

Table 19 **IP and IPv6 Filters (Description) (Continued)**

Attribute ID	Attribute Name	Description
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 (the 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 or IPv6) and direction (ingress or 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 or session. If after host or session disconnection, no hosts or 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|ipv6-filter** *filter-id* **sub-insert-shared-radius** The function of the attribute is identical to [26.529.242] 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. 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 address or IPv6 address as source (ingress) or destination (egress) IP. They represent a per host customization of a generic filter policy: only traffic to or from the subscriber host matches against these entries. A range of entries must be reserved for subscriber host specific entries in a filter policy: **configure filter ip-filter/ipv6-filter** *filter-id* **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 20 **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. For example: Nas-Filter-Rule = permit in ip from any to 10.1.1.1/32
26.529.242	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 lengths (type (**ipv4**/**ipv6**), direction (ingress or egress), src-ip, dst-ip, and so on. Each attribute represents a single filter entry. See IP Filter Attribute Details for a description of the format. For example: # permit in ip from any to 10.1.1.1/32 Ascend-Data-Filter = 0x01010100000000000a0101010020000000000000000

Table 20 **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 to 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. For example: Alc-Nas-Filter-Rule-Shared = permit in ip from any to 10.1.1.1/32

Table 20 **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** or **ipv6**), direction (**ingress** or **egress**), **src-ip**, **dst-ip**, and so on). Each attribute represents a single filter entry. See IP Filter Attribute Details 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 = 0x01010100000000000a0101010020000000000000000

Table 21 **IP and IPv6 Filters (Applicability)**

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request
92	NAS-Filter-Rule	0	0+	0+
26.529.242	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+

1.2.6.1 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 22 provides details on the respective fields.

Table 22 **[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 to 255]		protocol [0 to 255]
	ip		next-header none
	any number [1 to 42]		next-header [1 to 42]
	any number [45 to 49]		next-header [45 to 49]
	any number [52 to 59]		next-header [52 to 59]
	any number [61 to 255]		next-header [61 to 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 to 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 to 65535	ingress: src-ip = host-ip-address; src-port range 200 65535 egress: src-ip = ip-prefix/length; src-port range 200 65535

Table 22 **[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 to 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 to 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

Table 22 **[92] Nas-Filter-Rule Attribute Format (Continued)**

Action or Classifier	Value	Corresponding SR OS Filter Function
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
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 22 **[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 to 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

[26.529.242] Ascend-Data-Filter and [26.6527.159] Alc-Ascend-Data-Filter-Host-Spec

The format for [26.529.242] Ascend-Data-Filter and [26.6527.159] Alc-Ascend-Data-Filter-Host-Spec is an octet string with fixed length fields. Table 23 displays details on the respective fields.

Table 23 **[26.529.242] 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 23 **[26.529.242] Ascend-Data-Filter Attribute Format (Continued)**

Field	Length	Value
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

1.2.7 Subscriber Host Creation

Table 24 **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), IPCP (PPPoE) or data-triggered subscriber management. Simultaneous returned attributes [88] Framed-Pool and [8] Framed-IP-Address (RADIUS Access-Accept) are handled as host setup failures. This attribute is also used in CoA and Disconnect Message (part of the ESM or AA user identification-key). This 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 port of the NAS (SAP id) where the host is created.
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** *policy-name* **include-radius-attribute mac-address**)

Table 24 **Subscriber Host Creation (Description) (Continued)**

Attribute ID	Attribute Name	Description
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 and then answers the clients DHCP request with a DHCP NAK to force the client in a rebind state. The NAS also sends a DHCP release to the DHCP server.

Table 25 **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	<slot> / <mda> / <port> [: <qtag1> [. <qtag2>]] For example: NAS-Port-Id = 1/1/4:501.1001
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 26 **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

Table 26 **Subscriber Host Creation (Applicability) (Continued)**

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request
26.6527.27	Alc-Client-Hardware-Addr	0-1	0-1	0
26.6527.98	Alc-Force-Nak	0	0	0-1

1.2.8 Subscriber Services

Table 27 **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.

Table 27 **Subscriber Services (Description) (Continued)**

Attribute ID	Attribute Name	Description
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 28 **Subscriber Services (Limits)**

Attribute ID	Attribute Name	Type	Limits	SR OS format
26.6527.151	Alc-Sub-Serv-Activate	string	multiple VSAs per tag per message	For example: Alc-Sub-Serv-Activate:1 = rate-limit;1000;8000
26.6527.152	Alc-Sub-Serv-Deactivate	string	multiple VSAs 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 to 15552000]	A value of 0 (zero) corresponds with no interim update messages. A value [1 to 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 to 15552000] = override local configured update-interval for this subscriber service For example: Alc-Sub-Serv-Acct-Interim-Ivl:1 = 3600

Table 29 **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

1.2.9 GTP Uplink

In this section, GTP uplink application specific attributes are detailed. These attributes are applicable to WLAN Gateway as well as ESM scenarios such as Hybrid Access.

Table 30 **GTP Uplink (Description)**

Attribute ID	Attribute Name	Description
26.6527.145	Alc-MGW-Interface-Type	This contains the interface type that is used to determine the type of GTP-C connection, overrides local configuration.
26.6527.146	Alc-Wlan-APN-Name	Specifies the Access Point Name (APN) for which a GTP-C session is set up. This is 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-Mslsdn	Contains the MSISDN (telephone number) of the UE, and is included in GTP-C signaling. When not present the corresponding GTP-C Information Element is not sent.
26.6527.179	Alc-GTP-Local-Breakout	Specifies if part of the UE traffic can be locally broken out (such as, NATed and routed), subject to matching an IPv4 filter entry with action **gtp-local-breakout**, associated with the UE.
26.6527.205	Alc-GTP-Default-Bearer-Id	When establishing a GTP connection for a UE, this specifies the bearer ID (GTPv2) or NSAPI (GTPv1) that is used for the data path connection. If not provided, a default value of 5 is used.

Table 30 **GTP Uplink (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.219	Alc-Egress-Report-Rate-Subtract	This value is subtracted from the base downlink AMBR value calculated via the report-rate mechanism. This attribute will only be interpreted if report-rate is enabled in the applicable SLA profile: **configure subscriber-mgmt sla-profile** *sla-profile-name* **egress report-rate.**
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 is parsed as an IMSI. This should be provided for any GTP-C user.
26.10415.3	3GPP-PDP-Type	Specifies which address type should be requested from the P-GW: **ipv4**, **ipv6** or **ipv4v6**. If this attribute is not present, the value under **configure router | service vprn** *service-id* **wlan-gw pdn-type** is used.
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 is echoed in the GTP-C setup messages.
26.10415.21	3GPP-RAT-Type	Specifies the value that is signaled in the RAT Type IE during GTPv1/GTPv2 setup. If this attribute is not present, the value under **configure subscriber-mgmt wlan-gw mgw-profile** *profile-name* **rat-type** *type* is used.
26.10415.22	3GPP-User-Location-Info	This attribute specifies the location information for a given UE that is echoed in the ULI IE in GTP-C setup messages. The format and radius-to-GTP mapping is specified in 3GPP specification 29.061. If not present, no user location is reflected in GTP. RADIUS servers can use the information from for example, attributes [30] Called-Station-Id, [26.6527.206] Alc-Wlan-SSID-VLAN or [87] NAS-Port-Id to create a corresponding ULI value.

Table 31 **GTP Uplink (Limits)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.145	Alc-MGW-interface-Type	integer	values [1 to 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 to 15 digits	For example: Alc-MsIsdn = 13109976224
26.6527.179	Alc-GTP-Local-Breakout	integer	values [0 to 1]	values: not-allowed = 0, allowed = 1 For example: Alc-GTP-Local-Breakout = allowed
26.6527.205	Alc-GTP-Default-Bearer-Id	integer	[5 to 15]	If outside of the specified range, 5 is used.
26.6527.219	Alc-Egress-Report-Rate-Subtract	integer	[0 to 2147483647] kb/s	Example (subtract 500 kb/s): Alc-Egress-Report-Rate-Subtract=500
26.10415.1	3GPP-PDP-Type	string	1 to 15 digits	3GPP vendor specific attribute as defined in 3GPP TS 29.061. For example: 3GPP-IMSI = 204047910000598
26.10415.3	3GPP-PDP-Type	integer	[0,2,3]	0=ipv4, 2 =ipv6, 3 = ipv4v6 Example (Request a dual stack session): 3GPP-PDP-Type=3

Table 31 **GTP Uplink (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
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 to 16 digits	3GPP vendor specific attribute as defined in TS 29.061.
26.10415.21	3GPP-RAT-Type	octets	1 octet, [0..255]	Specifies the Radio Access Technology type, see 3GPP 29.061 section 16.4.7.2. for more details. For example (E-UTRAN RAT Type): 3GPP-RAT-Type = 0x06
26.10415.22	3GPP-User-Location-Info	octets	247 bytes	Specified in TS 29.061

Table 32 **GTP Uplink (Applicability)**

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request	Acct. Messages
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-Mslsdn	0	0-1	0	0
26.6527.179	Alc-GTP-Local-Breakout	0	0-1	0	0-1
26.6527.205	Alc-GTP-Default-Bearer-Id	0	0-1	0	0
26.6527.219	Alc-Egress-Report-Rate-Subtract	0	0-1	0	0
26.10415.1	3GPP-IMSI	0	0-1	0	0

Table 32 **GTP Uplink (Applicability) (Continued)**

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request	Acct. Messages
26.10415.3	3GPP-PDP-Type	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
26.10415.21	3GPP-RAT-Type	0	0-1	0	0
26.10415.22	3GPP-User-Location-Info	0	0-1	0	0

1.2.10 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. Relevant attributes for GTP uplink are documented in a separate GTP Uplink section.

Table 33 **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 (**configure aaa isa-radius-policy** *policy-name* **auth-include-attributes/acct-include-attributes called-station-id**), 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. Typically the string contains "*AP MAC* : *SSID-name*".

Table 33 **WLAN Gateway (Description) (Continued)**

Attribute ID	Attribute Name	Description
31	Calling-Station-Id	Calling-station-id contains the MAC address of the UE, if it is configured for inclusion in isa-radius-policy (**configure aaa isa-radius-policy** *policy-name* **auth-include-attributes calling-station-id**) 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 with format defined by the aggregation type: GRE or L2TPv3: "*tunnel-type* rtr-*virtual router id*#lip-*local ip address*#rip-*remote ip address*" where *tunnel-type* = GRE | L2TP, rtr-*virtual router id* is the transport service lip-*local ip address* is the local tunnel end-point rip-*remote ip address* is the remote tunnel end-point For example: NAS-Port-Id = "GRE rtr-11#lip-50.1.1.1#rip-201.1.1.2" VLAN: "VLAN svc-*svc-id*[:*vlan*[.*vlan*]]" where svc-*svc-id* is the relative identifier of the internal _tmnx_WlanGwL2ApService Epipe service connecting the WLAN-GW group interface SAP to the MS-ISA. [:*vlan*[.*vlan*]] is the optional dot1q or qinq encapsulation identifying the AP For example: NAS-Port-Id = "VLAN svc-1:10"
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 APs 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"
26.6527.148	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 is copied into the DHCP lease state and echoed by SR OS accounting.

Table 33 **WLAN Gateway (Description) (Continued)**

Attribute ID	Attribute Name	Description
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. For authentication originated by the WLAN GW, this attribute contains the total number of UEs that are currently attached to this UE's tunnel. This can be used to detect if this is the first UE on a tunnel (value 1). For non wlan-gw/vRGW UEs this value is 0. Inclusion can be configured by adding the option **wifi-num-attached-ues** in **configure subscriber-mgmt authentication-policy** *name* **include-radius-attribute** for ESM, and in **configure aaa isa-radius-policy** *name* **auth-include-attributes** for DSM.
26.6527.172	Alc-Wlan-Portal-Redirect	Used when authenticating migrant hosts. When an access-accept contains this attribute, the host stays in the migrant phase, but has limited forwarding capabilities. All filtered (not allowed) http-traffic is redirected to a specified portal URL. This attribute must contain the name of a redirect policy configured under **configure subscriber-mgmt http-redirect-policy** *policy-name* which specifies a set of forwarding filters. To force a redirect with the configured policy and URL, send an empty Alc- Wlan-Portal-Redirect VSA.
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 **configure subscriber-mgmt http-redirect-policy** *policy-name*.
26.6527.184	Alc-Wlan-Ue-Creation-Type	When promoting a migrant user, this indicates if the UE should be created on CPM/IOM (as an ESM host) or on ISA (as a DSM host). When this attribute is not present during promote, creation-type CPM/IOM is assumed. The attribute can be included in an Access-Accept message for a UE that is auto-signed-in (it does not need web redirect to portal), or in a CoA message triggered to remove web redirect for a UE after successful portal authentication. If Alc-Wlan-Ue-Creation-Type indicates a DSM UE then any IPv6 or GTP related parameters in an Access-Accept or CoA message is ignored, and the UE is created as a DSM host. Alc-Wlan-Ue-Creation-Type cannot be changed mid-session via CoA. A CoA containing Alc-Wlan-Ue-Creation-Type for an existing UE does not result in any change of state, and is NAK'd.

Table 33 **WLAN Gateway (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.186	Alc-Wlan-Dsm-Ot-Http-Redirect-Url	If a one-time redirect is enabled for a distributed subscriber management host, then this attribute specifies the redirect URL. This URL overrides the configured URL under **configure service ies/vprn** *service-id* **subscriber-interface** *subscriber-interface-name* **group-interface** *group-interface-name* **wlan-gw vlan-tag-ranges range start** *starting-vlan* **end** *ending-vlan* **distributed-sub-mgmt one-time-redirect**.
26.6527.187	Alc-Wlan-Dsm-Ip-Filter	Specifies the name of a distributed subscriber management (DSM) ip filter configured under **configure subscriber-mgmt wlan-gw distributed-sub-mgmt dsm-ip-filter** *ip-filter-name*. This filter is applied to the DSM UE. This overrides the value configured under **configure service ies/vprn** *service-id* **subscriber-interface** *subscriber-interface-name* **group-interface** *group-interface-name* **wlan-gw vlan-tag-ranges range start** *starting-vlan* **end** *ending-vlan* **distributed-sub-mgmt dsm-ip-filter** *dsm-ip-filter-name*.
26.6527.188	Alc-Wlan-Dsm-Ingress-Policer	Specifies the name of a distributed subscriber management (DSM) ingress policer configured under **configure subscriber-mgmt wlan-gw distributed-sub-mgmt dsm-policer** *policer-name*. This policer is applied to the DSM UE. This overrides the value configured under **configure service ies/vprn** *service-id* **subscriber-interface** *subscriber-interface-name* **group-interface** *group-interface-name* **wlan-gw vlan-tag-ranges range start** *starting-vlan* **end** *ending-vlan* **distributed-sub-mgmt ingress-policer** *policer-name*.
26.6527.189	Alc-Wlan-Dsm-Egress-Policer	Specifies the name of a distributed subscriber management (DSM) egress policer configured under **configure subscriber-mgmt wlan-gw distributed-sub-mgmt dsm-policer** *policer-name*. This policer is applied to the DSM UE. This overrides the value configured under **configure service ies/vprn** *service-id* **subscriber-interface** *subscriber-interface-name* **group-interface** *group-interface-name* **wlan-gw vlan-tag-ranges range start** *starting-vlan* **end** *ending-vlan* **distributed-sub-mgmt egress-policer** *policer-name*.
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.

Table 33 **WLAN Gateway (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.206	Alc-Wlan-SSID-VLAN	The VLAN is transparently taken from the UEs Ethernet layer and can be reflected in both authentication and accounting. This is typically added by the Access Point and uniquely identifies an SSID. This is useful when the SSID is not available in the [30] Called-Station-Id (for example, datatrigger scenarios). When this attribute is configured for inclusion but no VLAN is present in the UE payload, the attribute will not be reflected in RADIUS. When this attribute is sent in an Access-Accept message for a RADIUS proxy, the VLAN is used to perform SSID validation. If there is already an active UE and there is a mismatch between both VLANs, the UE is removed. If there is no UE present yet, the VLAN is stored and any subsequent data-plane packets (such as, DHCP Discover) is dropped unless the stored VLAN is matched.
26.6527.216	Alc-Datatrig-Lease-Time	Defines the initial lease-time used for data-triggered DHCP relay hosts. If this attribute is not provided or equal to zero, the used lease-time is 7 days. This lease time is overridden upon the first renew after data-triggered host-creation.
26.6527.218	Alc-Wlan-Handover-Ipv6-Address	Specifies the current IPv6 address of the UE in a 3GPP-to-WLAN handover scenario. In GTPv2 this sets the HI bit and signals the IP in the PDN Address Allocation IE. In GTPv1 this is not supported.
26.6527.233	Alc-Tunnel-QoS-Override	Used to override WLAN gateway tunnel HQoS parameters (aggregate rate and scheduler PIR/CIR), and enables per-tunnel customization. This attribute is included in a per-UE RADIUS message, and the value is applied to the tunnel with which the tunnel is currently associated. To remove an override, an empty value should be signaled. When removing an override, the tunnel QoS will revert to the configured values. It is not possible to revert to a previously applied override. It is also not possible to enable QoS via overrides. Tunnel QoS must be enabled on the WLAN gateway for overrides to function.
241.26.6527.6	Alc-Xconnect-Tunnel-Service	Specifies the service in which the control and data traffic for a x-connect UE is tunneled between visited WLAN-GW and home WLAN-GW. X-connect UE is a roaming UE that requires to be anchored on its home WLAN-GW.
241.26.6527.7	Alc-Xconnect-Tunnel-Remote-Ipv6	Specifies the IPv6 destination endpoint of the tunnel between visited WLAN-GW and home WLAN-GW for a x-connect UE.
241.26.6527.8	Alc-Xconnect-Tunnel-Type	Specifies the type of tunnel between visited WLAN-GW and home WLAN-GW for a x-connect UE. Supported tunnel types are L2oGRE and L2TPv3 with IPv6 transport.

Table 33 **WLAN Gateway (Description) (Continued)**

Attribute ID	Attribute Name	Description
241.26.6527.49	Alc-Xconnect-Tunnel-Local-Ipv6	Specifies the IPv6 source used for the tunnel between visited WLAN-GW and home WLAN-GW for a x-connect UE.
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 is copied into the DHCP lease state and echoed by the SR OS accounting.

Table 34 **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	L2TP | GRE: “<tunnel-type> rtr-<virtual router id>#lip-<local ip address>#rip-<remote ip address>” VLAN: “VLAN svc-<svc-id>[:<vlan>[.<vlan>]]” 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”
26.6527.148	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 34 **WLAN Gateway (Limits) (Continued)**

Attribute 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	247 chars	For example: Alc-Wlan-Portal-Url = http://welcome.portal.com
26.6527.184	Alc-Wlan-Ue-Creation-Type	integer	values [0 to 1]	values: iom = 0, isa = 1 Any other value is invalid and the corresponding RADIUS message is dropped. For example: Alc-Wlan-Ue-Creation-Type = iom
26.6527.186	Alc-Wlan-Dsm-Ot-Http-Redirect-Url	string	247 chars	For example: Alc-Wlan-Dsm-Ot-Http-Redirect-Url = “http://www.mydomain.com/advertisement?mac=$MAC”
26.6527.187	Alc-Wlan-Dsm-Ip-Filter	string	32 chars	If the filter cannot be found, the RADIUS Access-Accept message is dropped or the CoA NAK’d. For example: Alc-Wlan-Dsm-Ip-Filter = drop_non_http
26.6527.188	Alc-Wlan-Dsm-Ingress-Policer	string	32 chars	If the policer cannot be found, the RADIUS Access-Accept message is dropped or the CoA NAK’d. For example: Alc-Wlan-Dsm-Ingress-Policer = 1 Mb/s
26.6527.189	Alc-Wlan-Dsm-Egress-Policer	string	32 chars	If the policer cannot be found, the RADIUS Access-Accept message is dropped or the CoA NAK’d. For example: Alc-Wlan-Dsm-Egress-Policer = 10 Mb/s-limit
26.6527.190	Alc-Wlan-Handover-Ip-Address	ipaddr	4 bytes	For example: Alc-Wlan-Handover-Ip-Address = 10.1.1.1
26.6527.206	Alc-Wlan-SSID-VLAN	string	247 chars	Textual representation of the vlan. If no vlan-tag was present this attribute will not be included. For example: Alc-Wlan-SSID-VLAN = “2173”

Table 34 **WLAN Gateway (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.216	Alc-Datatrig-Lease-Time	integer	[0 to 2147483647] seconds	0: fallback to the default lease-time of 7 days. [1 to 2147483647] lease-time in seconds For example: Alc- Datatrig-Lease-Time = 3600
26.6527.218	Alc-Wlan-Handover-Ipv6-Address	ipv6addr	16 bytes	# IPv6 address For example: Alc-Wlan-Handover-Ipv6-Address = 2001:db8::1
26.6527.233	Alc-Tunnel-QoS-Override	string	Up to 4 attributes	<direction>:<QoS object>:[<id or name>:][<parameter>=value,...] <direction> = e or E for egress <QoS object> = r or R for egress aggregate-rate overrides <QoS object> = s or S for scheduler overrides <id or name> = identifies the QoS object, for example scheduler-name <parameter>=value,... = a comma-separated list of parameters to override with the corresponding value. All rates and CIRs are in kb/s. [eE]:[rR]:(rate) [eE]:[sS]:<scheduler-name>:(rate|cir) For example: aggregate rate override to 8 Mb/s Alc-Tunnel-QoS-Override += e:r:rate=8000
241.26.6527.6	Alc-Xconnect-Tunnel-Service	integer	2147483647 id	A valid VPRN or IES service ID For example: Alc-Xconnect-Tunnel-Service = 20
241.26.6527.7	Alc-Xconnect-Tunnel-Remote-Ipv6	ipv6addr	16 bytes	IPv6 address For example: Alc-Xconnect-Tunnel-IPv6 = 2001:db8::1
241.26.6527.8	Alc-Xconnect-Tunnel-Type	integer	Values [0,1]	0 = l2tpv3 1 = gre For example: Alc-Xconnect-Tunnel-Type = 0

Table 34 **WLAN Gateway (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
241.26.6527.49	Alc-Xconnect-Tunnel-Local-Ipv6	ipv6addr	16 bytes	IPv6 address For example: Alc-Xconnect-Tunnel-IPv6 = 2001:db8::1
26.25053.2	Ruckus-Sta-RSSI	integer	32 bit value	For example: Ruckus-Sta-RSSI = 28

Table 35 **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
26.6527.148	Alc-RSSI	0	0	0	0-1
26.6527.149	Alc-Num-Attached-Ues	0-1	0	0	0-1
26.6527.172	Alc-Wlan-Portal-Redirect	0	0-1	0	0
26.6527.173	Alc-Wlan-Portal-Url	0	0-1	0	0
26.6527.184	Alc-Wlan-Ue-Creation-Type	0	0-1	0-1	0-1
26.6527.186	Alc-Wlan-Dsm-Ot-Http-Redirect-Url	0	0-1	0-1	0
26.6527.187	Alc-Wlan-Dsm-Ip-Filter	0	0-1	0-1	0
26.6527.188	Alc-Wlan-Dsm-Ingress-Policer	0	0-1	0-1	0
26.6527.189	Alc-Wlan-Dsm-Egress-Policer	0	0-1	0-1	0
26.6527.190	Alc-Wlan-Handover-Ip-Address	0	0-1	0	0
26.6527.206	Alc-Wlan-SSID-VLAN	0-1	0-1	0	0-1

Table 35 **WLAN Gateway (Applicability) (Continued)**

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request	Acct. Messages
26.6527.216	Alc-Datatrig-Lease-Time	0	0-1	0	0
26.6527.218	Alc-Wlan-Handover-Ipv6-Address	0	0-1	0	0
26.6527.233	Alc-Tunnel-QoS-Override	0	0-1	0-1	0
241.26.6527.6	Alc-Xconnect-Tunnel-Service	0	0-1	0	0-1
241.26.6527.7	Alc-Xconnect-Tunnel-Remote-Ipv6	0	0-1	0	0-1
241.26.6527.8	Alc-Xconnect-Tunnel-Type	0	0-1	0	0-1
241.26.6527.49	Alc-Xconnect-Tunnel-Local-Ipv6	0	0	0	0-1
26.25053.2	Ruckus-Sta-RSSI	0	0	0	0-1

Table 36 lists the applicability of ISA authentication attributes on WLAN-GW. The following messages are distinguished:

- Access Request: Applicable to any Access Request generated by the ISA. Not applicable to proxied requests.
- Portal Access Accept: Applicable to a UE that must perform portal authentication after RADIUS authentication.
- DSM Access Accept: Applicable to a UE that bypasses portal authentication.
- CoA: Applicable to a CoA received in DSM state or a CoA moving a UE from portal to DSM state.

Table 36 **WLAN Gateway ISA Authentication (Applicability)**

Attribute ID	Attribute Name	Access Request	Portal Access Accept	DSM Accept	CoA
1	User-Name	1	0	0	0-1 [1]
2	User-Password	1	0	0	0
4	NAS-IP-Address	0-1	0	0	0
5	NAS-Port	0-1	0	0	0

Table 36 **WLAN Gateway ISA Authentication (Applicability) (Continued)**

Attribute ID	Attribute Name	Access Request	Portal Access Accept	DSM Accept	CoA
8	Framed-IP-Address	0-1	0	0	0
25	Class	0	0+	0+	0+
27	Session-Timeout	0	0-1	0-1	0-1
28	Idle-Timeout	0	0-1	0-1	0-1
30	Called-Station-Id	0-1	0	0	0
31	Calling-Station-Id	0-1	0	0	0
32	NAS-Identifier	0-1	0	0	0
44	Acct-Session-Id	0	0	0	0-1 [1]
61	NAS-Port-Type	0-1	0	0	0
85	Acct-Interim-Interval	0	0	0-1	0-1
87	NAS-Port-Id	0-1	0	0	0
26.3561.1	Agent-Circuit-id	0-1	0	0	0
26.3561.2	Agent-Remote-id	0-1	0	0	0
26.6527.17	Alc-Retail-Serv-id	0	0-1	0-1	0
26.6527.27	Alc-Client-Hardware-Addr	0-1	0	0	0
26.6527.36	Alc-Dhcp-Vendor-Class-id	0-1	0	0	0
26.6527.45	Alc-App-Prof-Str	0	0	0-1	0-1
26.6527.99	Alc-Ipv6-Address	0-1	0	0	0
26.6527.102	Alc-ToServer-Dhcp-Options	0+	0	0	0
26.6527.105	Alc-Ipv6-Primary-Dns	0	0-1	0-1	0-1
26.6527.106	Alc-Ipv6-Secondary-Dns	0	0-1	0-1	0-1
26.6527.122	Alc-LI-Action	0	0	0-1	0-1
26.6527.123	Alc-LI-Destination	0	0	0-1	0-1
26.6527.138	Alc-LI-Intercept-Id	0	0	0-1	0-1
26.6527.139	Alc-LI-Session-id	0	0	0-1	0-1
26.6527.172	Alc-Wlan-Portal-Redirect	0	1	0	0

Table 36 **WLAN Gateway ISA Authentication (Applicability) (Continued)**

Attribute ID	Attribute Name	Access Request	Portal Access Accept	DSM Accept	CoA
26.6527.173	Alc-Wlan-Portal-Url	0	0-1	0	0
26.6527.182	Alc-AA-Sub-Http-Url-Param	0	0	0-1	0-1
26.6527.184	Alc-Wlan-Ue-Creation-Type	0	0	1	0-1
26.6527.186	Alc-Wlan-Dsm-Ot-Http-Redirect-Url	0	0	0-1	0-1
26.6527.187	Alc-Wlan-Dsm-Ip-Filter	0	0	0-1	0-1
26.6527.188	Alc-Wlan-Dsm-Ingress-Policer	0	0	0-1	0-1
26.6527.189	Alc-Wlan-Dsm-Egress-Policer	0	0	0-1	0-1
26.6527.191	Alc-ToServer-Dhcp6-Options	0+	0	0	0
26.6527.206	Alc-Wlan-SSID-VLAN	0-1	0	0-1 [2]	0

Notes:

1. CoA key only to identify one or multiple subscriber host(s) or session(s)
2. Only supported for Distributed RADIUS Proxy

1.2.11 Virtual Residential Gateway

This section describes the attributes that are used in Virtual Residential Gateway (vRGW) authentication. This includes both authentication at the home/BRG (Bridged Residential Gateway) level and authentication at the per device/session level. The terminology used is as follows:

- vRGW refers to the virtual residential gateway functionality in the SR OS
- BRG refers to the physical device in the home. In the context of the vRGW it refers to a single residence.
- HLE refers to Home LAN Extension functionality in SR OS.

Table 37 and Table 38 list the description and limits for vRGW authentication attributes that are specific to vRGW applications only or that are different from the ESM or WLAN-GW authentication scenarios.

Table 39 lists the applicability for BRG level authentication Access Request attributes. This table is only applicable when the vRGW performs authentication on behalf of the BRG.

Table 40 lists the applicability for BRG level and session level authentication Access-Accept/CoA attributes of sessions in a vRGW context. Access-Accept and CoA attributes that are not listed or explicitly listed as 0 are not supported.

Table 37 **vRGW (Description)**

Attribute ID	Attribute Name	Description
1	User-Name	In BRG authentication this is fixed to the Bridged Residential Gateway Identifier (BRG-Id)
2	User-Password	In BRG authentication this maps to a pre-configured password: **configure subscriber-mgmt vrgw brg brg-profile** *profile-name* **radius-authentication password** *password* The attribute is not included when no password is configured.
26.6527.35	Alc-PPPoE-Service-Name	This VSA indicates the value of the service-name attribute that will be included in a PADI sent by the PPPoE client.

Table 37 **vRGW (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.220	Alc-Home-Aware-Pool	This specifies a basic small-scale IP pool that can be used to allocate addresses to multiple hosts of the same subscriber. This IP allocation mechanism has priority over other mechanisms (IP from RADIUS, IP from LUDB, IP from DHCP server). It is not necessary for a pool to be configured on the NAT inside, but if there is one, this will override those values. This attribute updates following four parameters: 1. The default-gateway IP address of the subnet. 2. The prefix length of the subnet. 3. The subnet itself (derived from default-gateway and prefix length). 4. The range of IP addresses suitable for allocation. These must fall inside the subnet. The start and end addresses are included for allocation. The attribute can also be used to change the pool for an existing subscriber, resulting in: 1. No existing hosts are deleted. 2. Hosts whose IP also falls in the new range will have their lease moved to the new pool and will keep running as before. 3. Hosts whose IP no longer falls in the new range will keep on running but the first renew is NAK'd. An IP from the new range is then assigned through a regular DORA sequence. If the pool is incorrect formatted, host setup will fail or the CoA will not be applied and NAK'd.
26.6527.221	Alc-DMZ-Address	In a vRGW context with home-aware pool management this attribute identifies the IP address to be used for DMZ. This attribute does not trigger the creation of a host with this IP, but if the host specified by this IP is installed, DMZ is enabled in NAT. All incoming traffic that does not match an existing NAT flow is forwarded to this host with ports unchanged.

Table 37 **vRGW (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.222	Alc-Standby-Ips	After a stateless redundancy event this attribute can be used to inform the home aware pool of addresses that were in use before failure. The pool will set these addresses aside and not use them for dynamic allocation. Only devices explicitly requiring this IP, for example via data trigger or DHCP renew, will get this IP address assigned. After a configurable time (**configure subscriber-mgmt vrgw brg brg-profile** *profile-name* **dhcp-pool standby-ip-lifetime**) all addresses that are still in standby is returned to the pool and made available for dynamic allocation. This VSA only applies when the pool is initially created any further changes are ignored.

Table 37 **vRGW (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.223	Alc-Reserved-Addresses	For a subscriber with home-aware pool management this attribute lists a set of MAC-IP combinations that are reserved. IP addresses listed here will only be allocated to the host with that specific MAC address. There are three types of reserved addresses: • Sticky private IP: the IP address falls in the pool subnet and in the dynamic range. This IP address will only be allocated using DHCP to the host with the specified MAC address. • Static private IP: The IP address falls in the pool subnet. This host is automatically created as soon as the subscriber access parameters are known (SAP or tunnel). This host uses L2-Aware NAT for forwarding to the network. • Static public IP: The IP address falls outside the pool subnet and any L2-Aware subnets. This host is created just as a static private IP, but the resulting host does not use L2-Aware NAT for forwarding. This is mainly used to simplify configuration of always-on devices in home networks. For example a network printer might have a sticky or private static IP, a light webserver might use private static IP + DMZ or a public static IP. A keyword is used to differentiate between sticky and static addresses. This attribute can be repeated multiple times to specify multiple reserved hosts. The list of reserved addresses can be changed via a CoA as follows: • Adding an address to the list creates the static host or makes an IP sticky. This is rejected if another host already uses the specified IP. • Removing an address from the list deletes the static host or removes stickiness. • Removing the last/all sticky addresses can be done by listing the sticky mapping of 00:00:00:00:00:00 to 0.0.0.0, no other sticky mappings may be present at that point.
26.6527.224	Alc-BRG-Profile	Specifies that this Bridged Residential Gateway (BRG) should use the values configured under **configure subscriber-mgmt vrgw brg brg-profile** *profile-name*.

Table 37 **vRGW (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.225	Alc-BRG-Id	In session authentication, reflects the BRG identifier of the associated BRG (if known) in Access-Request. In BRG authentication, reflects the BRG identifier (if known), in the Access Request. Can also be used as key to target a specific BRG with a CoA/Disconnect message.
26.6527.235	Alc-BRG-DHCP-Streaming-Dest	When specified in authentication, DHCPv4 messages (UDP layer) from all sessions for that BRG is mirrored to this destination. If a valid non 0.0.0.0 value is provided for the destination address, then streaming is enabled for the BRG (for example, for all sessions associated with the BRG). Streaming can be disabled at the BRG level by including this VSA with value 0.0.0.0.
26.6527.236	Alc-Host-DHCP-Streaming-Disabled	(Applies to session level authentication of a session associated with a BRG or CoA targeted to a session in a vRGW context.) This attribute controls the DHCPv4 streaming per session. A value of 1 disables DHCPv4 streaming for the session, and value of 0 enables it.
26.6527.238	Alc-Remove-Override	This VSA refers to another VSA that will be removed or explicitly disabled. When the referred VSA is removed, SR OS will fall back to behavior as if the VSA was never specified. When removed on session level the BRG level will be used (if present). When removed on BRG level the default behavior will be used.
26.6527.241	Alc-Per-Host-Port-Range	This attribute is used to enable or disable per-host outside port-range allocation for vRGW. When present, this attribute indicates how many ports should be available in each per host range. A value of zero disables per-host port range allocation. This attribute can only be used if a single block per nat outside IP is provisioned via **configure router | service vprn** *service-id* **nat outside pool** *nat-pool-name* **port-reservation blocks 1**.
241.26.6527.1	Alc-PPPoE-Client-Service	This VSA indicates in which L2 service PPPoE traffic will be forwarded.
241.26.6527.2	Alc-PPPoE-Client-MAC	This VSA indicates the MAC address used by the PPPoE Client. If this VSA is omitted, then the BRG-ID formatted as MAC address is used instead. The PPPoE session setup will fail when the VSA is not included and the BRG-ID is not formatted as a MAC address.
241.26.6527.3	Alc-PPPoE-Client-Policy	This VSA indicates that a BRG PPPoE client needs to be started and which pre-configured policy should be used as input parameters. If this attribute is omitted, all other PPPoE-Client related VSAs will be ignored.

Table 37 **vRGW (Description) (Continued)**

Attribute ID	Attribute Name	Description
241.26.6527.4	Alc-PPPoE-Client-Username	This VSA specifies which username must be used in the PAP authentication phase of the PPPoE Client setup. If it is not provisioned, the BRG-ID is used.
241.26.6527.5	Alc-PPPoE-Client-Password	This VSA specifies which password (PAP) or secret (CHAP) must be used in the authentication phase of the PPPoE Client setup.
241.26.6527.9	Alc-Bridge-Id	This VSA enables a Home LAN Extension (HLE) service for the subscriber: the system creates an HLE service and bridge domain using the attribute value as the bridge domain id. Not specifying a bridge id when HLE is enabled on the wlangw group interface for session and BRG level authentication results in a session setup failure.
241.26.6527.10	Alc-Vxlan-VNI	This VSA specifies the VXLAN Network Identifier (VNI) to be used for an egress VXLAN packet of the HLE service. When the VSA is not included, then the system automatically assigns a VNI.
241.26.6527.14	Alc-RT	This VSA specifies the Route Target of the HLE BGP EVPN service. When the VSA is not included, then the system derives the route target as "target:<configured_lanext_as>:<Alc-Bridge-Id>". Where <configured_lanext_as> is the value configured with **configure subscriber-mgmt vrgw lanext router-target-as-number** *as-number*.
241.26.6527.15	Alc-RD	This VSA specifies the Route Distinguisher of the HLE BGP EVPN service. When the VSA is not included, then the system derives the route distinguisher as "<configured_lanext_as>:<Alc-Bridge-Id>". Where <configured_lanext_as> is the value configured with **configure subscriber-mgmt vrgw lanext router-target-as-number** *as-number.*
241.26.6527.39	Alc-Static-Port-Forward	This VSA includes any static port forwards for L2-aware NAT and/or IPv6 firewall.

Table 38 **vRGW (Limits)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
1	User-Name	string	32 chars	For example: User-Name = “00:01:02:03:04:05”
2	User-Password	string	64 bytes encrypted password	For example: User-Password = “4ec1b7bea6f2892fa466b461c6accc00”
26.6527.35	Alc-PPPoE-Service-Name	string	247 chars	For example: Alc-PPPoE-Service-Name = MyServiceName

Table 38 **vRGW (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.220	Alc-Home-Aware-Pool	string	Max. 2048 IP addresses in range	<gateway-ip>/<prefix-length> <space> <start-address> <dash> <end-address> For example: Alc-Home-Aware-Pool = “192.168.1.2/24 192.168.1.50-192.168.1.100”
26.6527.221	Alc-DMZ-Address	ipaddr	4 bytes	Must be within the subnet of the home aware pool. 0.0.0.0 disables DMZ. For example: Enable Alc-DMZ-Address = 192.168.1.90 For example: Disable Alc-DMZ-Address = 0.0.0.0
26.6527.222	Alc-Standby-Ips	ipaddr	4 bytes Up to 128 VSA’s	This attribute can occur multiple times. For example: Alc-Standby-Ips += 192.168.1.100 Alc-Standby-Ips += 192.168.1.111 Alc-Standby-Ips += 192.168.1.115

Table 38 **vRGW (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.223	Alc-Reserved-Addresses	string	Max. 40 chars Max. 64 attributes	<static|sticky> <space> <mac-address> <space> <ip-address> Per attribute, a single MAC and IP to specify the reservation and a keyword to specify the type of reservation (sticky or static). To delete all/last host of a certain reservation type, specify the type keyword and a mapping of MAC 00:00:00:00:00:00 to IP 0.0.0.0 For example: • static private host 00:00:01:00:00:01 = 192.168.1.90, sticky host 00:00:0A:00:00:0A = 192.168.1.70 and static public host 00:00:0B:00:00:0B = 100.0.0.1 Alc-Reserved-Addresses = “static 00:00:01:00:00:01 192.168.1.90” Alc-Reserved-Addresses = “sticky 00:00:0A:00:00:0A 192.168.1.70” Alc-Reserved-Addresses = “sticky 00:00:0B:00:00:0B 100.0.0.1” • to remove all or last sticky IPs Alc-Reserved-Addresses = “sticky 00:00:00:00:00:00 0.0.0.0”.
26.6527.224	Alc-BRG-Profile	string	16 chars	For example: Alc-BRG-Profile = “default_brg”
26.6527.225	Alc-BRG-Id	string	32 chars	For example: Alc-BRG-Id = “00:01:02:03:04:05”

Table 38 **vRGW (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.235	Alc-BRG-DHCP-Streaming-Dest	ipaddr	4 bytes	The destination IPv4 address for streaming DHCPv4 messages. IPv4 = 0.0.0.0 disables DHCPv4 streaming at BRG level For example: Alc-BRG-DHCP-Streaming-Dest = 140.1.1.1. Alc-BRG-DHCP-Streaming-Dest = 0.0.0.0
26.6527.236	Alc-Host-DHCP-Streaming-Disabled	integer	4 bytes [0 to 1]	0 = enable DHCPv4 streaming for this session 1 = disable DHCPv4 streaming for this session Controls DHCPv4 streaming on per session level. For example: Alc-Host-DHCP-Streaming-Disabled = 1
26.6527.238	Alc-Remove-Override	string	Single attribute identifier per attribute. Multiple attributes per message.	[<action><space>]<attribute identifier> See [26.6527.238] Alc-Remove-Override Attribute Details for a detailed description of the attribute format and its possible values. For example: remove overrides for SLA-Profile And NAS-Filter-Rule: Alc-Remove-Override += “26.6527.13” Alc-Remove-Override += “92”
26.6527.241	Alc-Per-Host-Port-Range	integer	0-64512	A value of 0 disables per-host port range allocation. Ports are allocated from the available dynamic ports per IP address. A value of 1 to 64512 specifies the number of ports per host range. This is additionally limited by the number of available dynamic ports per IP address. For example: 1000 ports per host, max. 64 hosts Alc-Per-Host-Port-Range = 1000
241.26.6527.1	Alc-PPPoE-Client-Service	integer	2147483647	For example: Alc-PPPoE-Client-Service = 2

Table 38 **vRGW (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
241.26.6527.2	Alc-PPPoE-Client-MAC	string	17 chars	MAC address in aa: or AA: format. For example: Alc-PPPoE-Client-MAC = "00:00:5E:00:53:01"
241.26.6527.3	Alc-PPPoE-Client-Policy	string	32 chars	String referring to a policy configured under **configure subscriber-mgmt pppoe-client-policy** For example: Alc-PPPoE-Client-Policy = Policy-1
241.26.6527.4	Alc-PPPoE-Client-Username	string	247 chars	For example: Alc-PPPoE-Client-Username = user-1
241.26.6527.5	Alc-PPPoE-Client-Password	string	247 chars	Encrypted Password For example: Alc-PPPoE-Client-Password = password-1
241.26.6527.9	Alc-Bridge-Id	integer	1 - 4294967294	For example: Alc-Bridge-Id = 200.
241.26.6527.10	Alc-Vxlan-VNI	integer	1 - 16777214	For example: Alc-Vxlan-VNI =250
241.26.6527.14	Alc-RT	string	SR OS supported format	One of the following formats: • target:<ip-addr:comm-val> • target:<2byte-asnumber:ext-comm-val> • target:<4byte-asnumber:comm-val> For example: Alc-RT = "target: 64496:200"
241.26.6527.15	Alc-RD	string	SR OS supported format	One of the following formats: • <ip-addr:comm-val> • <2byte-asnumber:ext-comm-val> • <4byte-asnumber:comm-val> For example: Alc-RD = "64496:510"

Table 38 **vRGW (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
241.26.6527.39	Alc-Static-Port-Forward	string	64 SPFs	See [241.26.6527.39] Alc-Static-Port-Forward Attribute Details for details on this format. For example: • Add an IPv6 firewall SPF to open up TCP port 80 (HTTP) Alc-Static-Port-Forward = "c tcp 1::1 80" • Add an IPv6 SPF to open up UDP port 5 but only for traffic coming from IP 2::2 and port 80 Alc-Static-Port-Forward = "c udp 1::1 5 foreign 2::2 80" • Add an l2-aware NAT SPF to open up TCP port 80 (HTTP) on the outside and forward it to port 8080 on ip 1.1.1.1 on the inside Alc-Static-Port-Forward = "c tcp 1.1.1.1 8080->80"

Table 39 **vRGW- BRG Level Authentication -- Access Request (Applicability)**

Attribute ID	Attribute Name	Access Request
1	User-Name	1
2	User-Password	0-1
26.6527.225	Alc-BRG-Id	1

Table 40 **vRGW - BRG and Session Level Authentication (Applicability)**

Attribute ID	Attribute Name	BRG Level		Session Level	
		Access Accept	CoA	Access Accept	CoA
1	User-Name	n/a	n/a	0-1	0-1
8	Framed-IP-Address	n/a	n/a	0-1	0-1

Table 40 **vRGW - BRG and Session Level Authentication (Applicability) (Continued)**

Attribute ID	Attribute Name	BRG Level		Session Level	
		Access Accept	CoA	Access Accept	CoA
9	Framed-IP-Netmask	n/a	n/a	0-1	0
22	Framed-Route	n/a	n/a	0+	0
25	Class	0+	0+	0+	0+
27	Session-Timeout	0-1	0-1	0-1	0-1
28	Idle-Timeout	0-1	0-1	0-1	0-1
44	Acct-Session-Id	n/a	n/a	0-1	0-1
61	NAS-Port-Type	n/a	n/a	0-1	0-1
85	Acct-Interim-Interval	0-1	0-1	0-1	0-1
87	NAS-Port-Id	n/a	n/a	0	0-1
92	NAS-Filter-Rule	0+	0+	0+	0+
97	Framed-IPv6-Prefix	0-1	0-1	0	0-1
99	Framed-IPv6-Route	n/a	n/a	0+	0
100	Framed-IPv6-Pool	0-1 [1]	0-1 [1]	n/a	n/a
101	Error-Cause	0	0-1	0	0-1
26.529.242	Ascend-Data-Filter	0+	0+	0+	0+
26.2352.1	Client-DNS-Pri	0-1 [2]	0-1 [2]	0-1	0
26.2352.2	Client-DNS-Sec	0-1 [2]	0-1 [2]	0-1	0
26.2352.99	RB-Client-NBNS-Pri	0-1 [2]	0-1 [2]	0-1	0
26.2352.100	RB-Client-NBNS-Sec	0-1 [2]	0-1 [2]	0-1	0
26.4874.4	ERX-Primary-Dns	0-1 [2]	0-1 [2]	0-1	0
26.4874.5	ERX-Secondary-Dns	0-1 [2]	0-1 [2]	0-1	0
26.4874.6	ERX-Primary-Wins	0-1 [2]	0-1 [2]	0-1	0
26.4874.7	ERX-Secondary-Wins	0-1 [2]	0-1 [2]	0-1	0
26.4874.47	ERX-Ipv6-Primary-Dns	0-1 [2]	0-1 [2]	0-1	0-1
26.4874.48	ERX-Ipv6-Secondary-Dns	0-1 [2]	0-1 [2]	0-1	0-1
26.6527.9	Alc-Primary-Dns	0-1 [2]	0-1 [2]	0-1	0

Table 40 **vRGW - BRG and Session Level Authentication (Applicability) (Continued)**

Attribute ID	Attribute Name	BRG Level		Session Level	
		Access Accept	CoA	Access Accept	CoA
26.6527.10	Alc-Secondary-Dns	0-1 [2]	0-1 [2]	0-1	0
26.6527.11	Alc-Subsc-ID-Str	0-1 [3]	0	0-1	0-1
26.6527.12	Alc-Subsc-Prof-Str	0-1	0-1	n/a	n/a
26.6527.13	Alc-SLA-Prof-Str	0-1	0-1	0-1	0-1
26.6527.18	Alc-Default-Router	0-1 [2]	0-1 [2]	0-1	0
26.6527.27	Alc-Client-Hardware-Addr	n/a	n/a	0-1	0-1
26.6527.28	Alc-Int-Dest-Id-Str	0-1	0-1	n/a	n/a
26.6527.29	Alc-Primary-Nbns	0-1 [2]	0-1 [2]	0-1	0
26.6527.30	Alc-Secondary-Nbns	0-1 [2]	0-1 [2]	0-1	0
26.6527.31	Alc-MSAP-Serv-Id	n/a	n/a	0-1	0
26.6527.32	Alc-MSAP-Policy	n/a	n/a	0-1	0
26.6527.33	Alc-MSAP-Interface	n/a	n/a	0-1	0
26.6527.35	Alc-PPPoE-Service-Name	0-1 [5]	0-1 [5]	n/a	n/a
26.6527.45	Alc-App-Prof-Str	0-1	0-1	0-1	0-1
26.6527.95	Alc-Credit-Control-CategoryMap	n/a	n/a	0-1	0-1
26.6527.96	Alc-Credit-Control-Quota	n/a	n/a	0+	0+
26.6527.99	Alc-Ipv6-Address	n/a	n/a	0-1	0-1
26.6527.103	Alc-ToClient-Dhcp-Options	0+	0+	0+	0
26.6527.105	Alc-Ipv6-Primary-Dns	0-1 [2]	0-1 [2]	0-1	0-1
26.6527.106	Alc-Ipv6-Secondary-Dns	0-1 [2]	0-1 [2]	0-1	0-1
26.6527.122	Alc-LI-Action (enable/disable)	0-1	0-1	0-1	0-1
26.6527.123	Alc-LI-Destination	0-1	0-1	0-1	0-1
26.6527.124	Alc-LI-FC	0+	0+	0+	0+
26.6527.125	Alc-LI-Direction	0-1	0-1	0-1	0-1
26.6527.126	Alc-Subscriber-QoS-Override	0-1	0-1	0-1	0-1
26.6527.134	Alc-Subscriber-Filter	0-1	0-1	0-1	0-1

Table 40 **vRGW - BRG and Session Level Authentication (Applicability) (Continued)**

Attribute ID	Attribute Name	BRG Level		Session Level	
		Access Accept	CoA	Access Accept	CoA
26.6527.138	Alc-LI-Intercept-Id	0-1	0-1	0-1	0-1
26.6527.139	Alc-LI-Session-Id	0-1	0-1	0-1	0-1
26.6527.151	Alc-Sub-Serv-Activate	n/a	n/a	0+	0+
26.6527.152	Alc-Sub-Serv-Deactivate	n/a	n/a	0+	0+
26.6527.153	Alc-Sub-Serv-Acct-Stats-Type	n/a	n/a	0+	0+
26.6527.154	Alc-Sub-Serv-Acct-Interim-Ivl	n/a	n/a	0+	0+
26.6527.158	Alc-Nas-Filter-Rule-Shared	0+	0+	0+	0+
26.6527.159	Alc-Ascend-Data-Filter-Host-Spec	0+	0+	0+	0+
26.6527.160	Alc-Relative-Session-Timeout	0-1	0-1	0-1	0-1
26.6527.174	Alc-Lease-Time	0-1 [2]	0-1 [2]	0-1	0
26.6527.177	Alc-Portal-Url	0-1	0-1	0-1	0-1
26.6527.178	Alc-Ipv6-Portal-Url	0-1	0-1	0-1	0-1
26.6527.181	Alc-SLAAC-IPv6-Pool	0-1 [1]	0-1 [1]	n/a	n/a
26.6527.182	Alc-AA-Sub-Http-Url-Param	0-1	0-1	0-1	0-1
26.6527.192	Alc-ToClient-Dhcp6-Options	0+	0+	0+	0
26.6527.193	Alc-AA-App-Service-Options	0-1	0-1	0-1	0-1
26.6527.200	Alc-v6-Preferred-Lifetime	0-1 [2]	0-1 [2]	0-1	0
26.6527.201	Alc-v6-Valid-Lifetime	0-1 [2]	0-1 [2]	0-1	0
26.6527.202	Alc-Dhcp6-Renew-Time	0-1 [2]	0-1 [2]	0-1	0
26.6527.203	Alc-Dhcp6-Rebind-Time	0-1 [2]	0-1 [2]	0-1	0
26.6527.217	Alc-UPnP-Sub-Override-Policy	0-1	0-1	n/a	n/a
26.6527.220	Alc-Home-Aware-Pool	0-1	0-1	n/a	n/a
26.6527.221	Alc-DMZ-Address	0-1	0-1	n/a	n/a
26.6527.222	Alc-Standby-Ips	0-1 [3]	0	n/a	n/a
26.6527.223	Alc-Reserved-Addresses	0+	0+	n/a	n/a
26.6527.224	Alc-BRG-Profile	0-1	0-1	n/a	n/a

Table 40 **vRGW - BRG and Session Level Authentication (Applicability) (Continued)**

Attribute ID	Attribute Name	BRG Level		Session Level	
		Access Accept	CoA	Access Accept	CoA
26.6527.225	Alc-BRG-Id	0-1 [4]	0-1 [4]	0-1	0
26.6527.228	Alc-Trigger-Acct-Interim	n/a	n/a	0	0-1
26.6527.234	Alc-DNAT-Override	0+	0+	n/a	n/a
26.6527.235	Alc-BRG-DHCP-Streaming-Dest	0-1	0-1	n/a	n/a
26.6527.236	Alc-Host-DHCP-Streaming-Disabled	n/a	n/a	0-1	0-1
26.6527.238	Alc-Remove-Override	0	0+	0	0+
26.6527.241	Alc-Per-Host-Port-Range	0-1	0-1	n/a	n/a
241.26.6527.1	Alc-PPPoE-Client-Service	0-1 [3]	0	n/a	n/a
241.26.6527.2	Alc-PPPoE-Client-MAC	0-1 [3]	0	n/a	n/a
241.26.6527.3	Alc-PPPoE-Client-Policy	0-1 [5]	0-1 [5]	n/a	n/a
241.26.6527.4	Alc-PPPoE-Client-Username	0-1 [5]	0-1 [5]	n/a	n/a
241.26.6527.5	Alc-PPPoE-Client-Password	0-1 [5]	0-1 [5]	n/a	n/a
241.26.6527.9	Alc-Bridge-Id	0-1	0	0-1	0
241.26.6527.10	Alc-Vxlan-VNI	0-1	0	n/a	n/a
241.26.6527.14	Alc-RT	0-1	0	n/a	n/a
241.26.6527.15	Alc-RD	0-1	0	n/a	n/a
241.26.6527.16	Alc-IPv6-Router-Adv-Policy	0-1	0-1	0-1	0-1
241.26.6527.17	Alc-Nat-Outside-IPs	0+	0+	0	0
241.26.6527.24	Alc-IPv6-DMZ-Enabled	n/a	n/a	0-1	0-1
241.26.6527.26	Alc-Aa-Sub-Scope	0-1 [3]	0	n/a	n/a
241.26.6527.37	Alc-VAS-IPv4-Filter	0-1	0-1	0-1	0-1
241.26.6527.38	Alc-VAS-NSH-IPv4-Opaque-Meta-Data	n/a	n/a	0-1	0-1
241.26.6527.39	Alc-Static-Port-Forward	0+	0+	0	0

Notes:

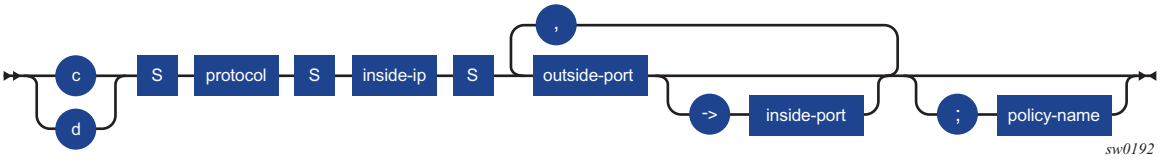
1. Only for new sessions. Ignored for existing sessions.

2. The update is applied to an existing session at the next DHCP/DHCPv6 Renew or Router Advertisement (RA).
3. May be present in re-auth but cannot change for an existing BRG.
4. Mandatory in CoA (used as key to identify the BRG).
5. Any change can lead to a restart of the PPPoE Client.

1.2.11.1 [241.26.6527.39] Alc-Static-Port-Forward Attribute Details

Static port forwards (SPF) for NAT and firewall can be installed using the Alc-Static-Port-Forward Extended VSA. This section describes the format used for each application. Figure 1 illustrates a diagram showing an overview of this syntax.

Figure 1 **Alc-Static-Port-Forward: Format for l2-Aware NAT Static Port Forwards**



For l2-aware, the format looks as follows:

{c|d}<space>protocol<space>inside-ip<space>outside-port[->insideport][,outside-port[->insideport]]*[;policy-name]

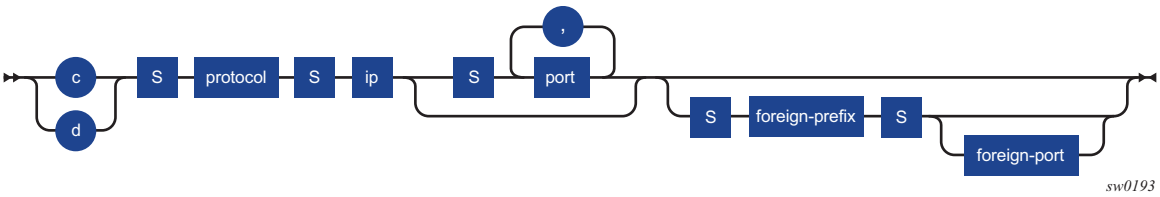
Table 41 describes the l2-aware format.

Table 41 **l2-aware Field Descriptions**

Field Name	Description
c/d	This field specifies whether the specified SPF needs to be created or deleted.
protocol	This field specifies the protocol to which this SPF applies. This can be either the literals 'udp' or 'tcp' or the protocol numbers 6 or 17.
inside-ip	This field specifies the inside IP to which the SPF traffic is forwarded.
outside-port, inside-port	This field is a list of ports that is opened. If inside-port is not specified, it is chosen the same as outside-port. Each specified (inside,outside) port pair results in a separate installed SPF.
policy-name	This field is the policy to which this SPF applies. If not provided, the default policy of the subscriber (sub-profile changes) is used.

Figure 2 illustrates a diagram showing an overview of the residential firewall format.

Figure 2 **Alc-Static-Port-Forward: Format for Residential Firewall Static Port Forwards**



For residential firewall, the format looks as follows:

{c|d}<space>protocol<space>ip[<space>port[,]]*[<space>foreign-prefix[<space>foreign-port]]

Table 42 describes the Residential Firewall format.

Table 42 **Residential Firewall Field Descriptions**

Field Name	Description
c/d	This field specifies whether the specified SPF needs to be created or deleted.
protocol	This field specifies the protocol to which this SPF applies. For tcp or udp, the literal tcp or udp can be used. Only SPFs for TCP, UDP and supported unknown protocols can be used. SPFs for other protocols (for example, ICMPv6) are not supported. Note: If ICMPv6 is configured as an unknown protocol, a warning is issued.
ip	This field specifies the IP to which the SPF applies.
port	This field is a list of ports that will be opened. No port may be specified for unknown protocols and at least one port needs to be specified for TCP/UDP.
foreign-prefix	This field limits the SPF to only allow traffic received from this prefix.
foreign-port	This field further limits traffic to this specific port.

Any Static Port Forwards that are syntactically correct, but do not apply (for example, unused NAT policy or nonexistent IP) also count towards the maximum supported port forwards.

1.2.12 Bonding

This section describes attributes applicable to bonding. Table 43 and Table 44 give an overview of all authentication attributes specific to bonding. Table 45 subsequently gives an overview of the attributes that are applicable for the authentication of a Bonding context.

Table 43 **Bonding (Description)**

Attribute ID	Attribute Name	Description
241.26.6527.19	Alc-Bonding-Id	When present in authentication of an access session, indicates that the IPoE or PPPoE session being authenticated is part of a bonding context with the given ID. The bonding-ID will also be used as the subscriber-id for the associated bonding subscriber.
241.26.6527.20	Alc-Bonding-Serv-Id	Indicates the service in which a bonding subscriber will be created and must be specified during authentication of the access session together with the attribute [241.26.6527.21] Alc-Bonding-Interface.
241.26.6527.21	Alc-Bonding-Interface	Defines the group-interface where the bonding subscriber will be created and must be passed during authentication of the access session. The specified group interface must be of the type bonding.
241.26.6527.22	Alc-Bonding-Reference-Rate	For the preferred access connection in a bonding context this defines which rate is considered to determine if that connection is completely filled. The attribute either specifies an absolute rate or a QoS object from which rate will be used. When a QoS object is specified, dynamic overrides are taken into account. The bonding load-balancing mechanism sends traffic over this connection first until the specified rate is reached; then it starts to send traffic over the alternate link too. This mechanism is configured under **configure subscriber-mgmt sla-profile** *sla-profile-name* **egress bonding-selection**. If the attribute is not present, then the bonding selection will use the subscriber aggregate-rate. If there is no aggregate-rate defined then the maximum absolute value will be used.

Table 44 **Bonding (Limits)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
241.26.6527.19	Alc-Bonding-Id	string	1-32 chars	A valid human-readable string, must not start with an underscore (_). For example: Alc-Bonding-Id = home1

Table 44 **Bonding (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
241.26.6527.20	Alc-Bonding-Serv-Id	integer	2147483647 id	A valid VPRN or IES service ID For example: Alc-Bonding-Serv-Id = 5
241.26.6527.21	Alc-Bonding-Interface	string	1-32 chars	The name of a group-interface of type bonding within the service defined by Alc-Bonding-Serv-Id For example: Alc-Bonding-Interface = bonding-group-interface
241.26.6527.22	Alc-Bonding-Reference-Rate	string	1..4294967295 kbps or a valid QoS object	Format must be one of the following (quotes not included): '<value>': Absolute rate in kbps 'r|R': Aggregate rate 'a|A:<name>': Rate of named arbiter 's|S:<name>': rate of named scheduler For example: Alc-Bonding-Reference-Rate = s:scheduler-1

Table 45 **Bonding Context (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
4	NAS-IP-Address	0-1	0	0
8	Framed-IP-Address	0	0-1	0-1
9	Framed-IP-Netmask	0	0-1	0
25	Class	0	0-1	0-1
27	Session-Timeout	0	0-1	0-1
32	NAS-Identifier	0-1	0	0
44	Acct-Session-Id	0-1	0	0-1
61	NAS-Port-Type	0-1	0	0-1

Table 45 **Bonding Context (Applicability) (Continued)**

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request
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
92	NAS-Filter-Rule	0	0+	0+
95	NAS-IPv6-Address	0-1	0	0
97	Framed-IPv6-Prefix	0	0-1	0-1
101	Error-Cause	0	0	0-1
26.529.242	Ascend-Data-Filter	0	0+	0+
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	Client-NBNS-Pri	0	0-1	0
26.2352.100	Client-NBNS-Sec	0	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	0-1
26.4874.48	ERX-Ipv6-Secondary-Dns	0	0-1	0-1
26.6527.9	Alc-Primary-Dns	0	0-1	0
26.6527.10	Alc-Secondary-Dns	0	0-1	0
226.6527.11	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
26.6527.18	Alc-Default-Router	0	0-1	0
26.6527.28	Alc-Int-Dest-Id-Str	0	0-1	0-1

Table 45 **Bonding Context (Applicability) (Continued)**

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request
26.6527.29	Alc-Primary-Nbns	0	0-1	0
26.6527.30	Alc-Secondary-Nbns	0	0-1	0
26.6527.45	Alc-App-Prof-Str	0	0-1	0-1
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
26.6527.105	Alc-Ipv6-Primary-Dns	0	0-1	0-1
26.6527.106	Alc-Ipv6-Secondary-Dns	0	0-1	0-1
26.6527.122	Alc-LI-Action	0	1	1
26.6527.123	Alc-LI-Destination	0	1	1
26.6527.124	Alc-LI-FC	0	0+	0-1
26.6527.125	Alc-LI-Direction	0	0-1	0-1
26.6527.126	Alc-Subscriber-QoS-Override	0	0-1	0-1
26.6527.134	Alc-Subscriber-Filter	0	0-1	0-1
26.6527.136	Alc-Onetime-Http-Redirection-Filter-Id	0	0-1	0-1
26.6527.137	Alc-Authentication-Policy-Name	0	0	0-1
26.6527.138	Alc-LI-Intercept-Id	0	0-1	0-1
26.6527.139	Alc-LI-Session-Id	0	0-1	0-1
26.6527.151	Alc-Sub-Serv-Activate	0	0+	0+
26.6527.152	Alc-Sub-Serv-Deactivate	0	0+	0+
26.6527.153	Alc-Sub-Serv-Acct-Stats-Type	0	0+	0+
26.6527.154	Alc-Sub-Serv-Acct-Interim-Ivl	0	0+	0+
26.6527.158	Alc-Nas-Filter-Rule-Shared	0	0+	0+
26.6527.159	Alc-Ascend-Data-Filter-Host-Spec	0	0+	0+
26.6527.160	Alc-Relative-Session-Timeout	0	0-1	0-1
26.6527.174	Alc-Lease-Time	0	0-1	0
26.6527.177	Alc-Portal-Url	0	0-1	0-1

Table 45 **Bonding Context (Applicability) (Continued)**

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request
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
26.6527.182	Alc-AA-Sub-Http-Url-Param	0	0-1	0-1
26.6527.185	Alc-Onetime-Http-Redirect-Reactivate	0	0	0-1
26.6527.193	Alc-AA-App-Service-Options	0	0-1	0-1
26.6527.200	Alc-v6-Preferred-Lifetime	0	0-1	0
26.6527.201	Alc-v6-Valid-Lifetime	0	0-1	0
26.6527.217	Alc-UPnP-Sub-Override-Policy	0	0-1	0-1
26.6527.228	Alc-Trigger-Acct-Interim	0	0	0-1
26.6527.232	Alc-Acct-Interim-Ivl	0	0+	0+
26.6527.234	Alc-DNAT-Override	0	0-1	0-1
26.6527.238	Alc-Remove-Override	0	0	0+
26.6527.242	Alc-Radius-Py	0+	0+	0+
241.26.6527.20	Alc-Bonding-Serv-Id	0	0-1	0
241.26.6527.21	Alc-Bonding-Interface	0	0-1	0

1.2.13 Dynamic Data Services

Table 46 **Dynamic Data Services (Description)**

Attribute ID	Attribute Name	Description
1	User-Name	This attribute is for RADIUS authentication of data triggered Dynamic Data Services only. The user to be authenticated in the Access-Request. The attribute value is the dynamic service data trigger sap-id.

Table 46 **Dynamic Data Services (Description) (Continued)**

Attribute ID	Attribute Name	Description
2	User-Password	This attribute is for RADIUS authentication of data triggered Dynamic Data Services only. The password of the user to be authenticated. The attribute value is preconfigured: **configure service dynamic-services dynamic-services-policy** *dynsvc-policy-name* **authentication password** *password*
4	NAS-IP-Address	This attribute is for RADIUS authentication of data triggered Dynamic Data Services only. The identifying IP Address of the NAS requesting the Authentication. 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** i*p- address*).
8	Framed-IP-Address	This attribute is for RADIUS authentication of data triggered Dynamic Data Services only. The IPv4 source address of an IPv4 data trigger frame that resulted in the authentication. Not included if the data trigger frame is not an IPv4 packet.
32	NAS-Identifier	(RADIUS authentication of data triggered Dynamic Data Services only) A string identifying the NAS originating the Authentication request. The attribute value is the system name of the router: **configure system name** *system-name*
44	Acct-Session-Id	(RADIUS authentication of data triggered Dynamic Data Services only) A unique identifier that represents the dynamic service data trigger that is authenticated. This attribute can be used as CoA or Disconnect Message key to target the dynamic service data trigger and is reflected in the accounting messages as attribute [50] Acct-Multi-Session-Id.
87	NAS-Port-Id	(RADIUS authentication of data triggered Dynamic Data Services only) A text string which identifies the physical or logical port of the NAS which is authenticating the user. Attribute is also used in CoA and Disconnect Message as identification key. The attribute value is the dynamic service data trigger sap-id.

Table 46 **Dynamic Data Services (Description) (Continued)**

Attribute ID	Attribute Name	Description
95	NAS-IPv6-Address	(RADIUS authentication of data triggered Dynamic Data Services only) 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*).
26.6527.27	Alc-Client-Hardware-Addr	(RADIUS authentication of data triggered Dynamic Data Services only) The MAC address of the dynamic service data trigger frame that resulted in the authentication. The format is fixed: xx:xx:xx:xx:xx:xx
26.6527.99	Alc-Ipv6-Address	(RADIUS authentication of data triggered Dynamic Data Services only) The IPv6 source address of an IPv6 data trigger frame that resulted in the authentication. Not included if the data trigger frame is not an IPv6 packet.
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 [26.6527.164] 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 [26.6527.165] 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 is 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 [26.6527.165] 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 46 **Dynamic Data Services (Description) (Continued)**

Attribute ID	Attribute Name	Description
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 [26.6527.165] Alc-Dyn-Serv-Script-Params, this attribute determines which Python function is 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 which 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 [26.6527.167] 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 [26.6527.167] 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.
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.

Table 46 **Dynamic Data Services (Description) (Continued)**

Attribute ID	Attribute Name	Description
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 47 **Dynamic Data Services (Limits)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
1	User-Name	string	253 chars	Fixed to the sap-id of the dynamic service data trigger packet For example: User-Name = "1/1/1:10.2"
2	User-Password	string	64 bytes	Encrypted password For example: User-Password = "6/TcjoaomHgakafcDrpCDk"
4	NAS-IP-Address	ipaddr	4 bytes	IPv4 address. For example: NAS-IP-Address = 192.0.2.1
8	Framed-IP-Address	ipaddr	4 bytes	IPv4 address. For example: Framed-IP-Address = 10.1.0.1
32	NAS-Identifier	string	32 chars	For example:NAS-Identifier = "router-1"
44	Acct-Session-Id	string	22 bytes	Internal generated 22 byte number. For example: Acct-Session-Id = "144DFF000000CB56A79EC4"
87	NAS-Port-Id	string	253 chars	Fixed to the sap-id of the dynamic service data trigger packet For example: User-Name = "1/1/1:10.2"
95	NAS-IPv6-Address	ipv6addr	16 bytes	IPv6 address. For example: NAS-IPv6-Address = 2001:db8::1
26.6527.27	Alc-Client-Hardware-Addr	string	6 bytes	Format fixed to xx:xx:xx:xx:xx:xx For example: Alc-Client-Hardware-Addr = 00:51:00:dd:01:01

Table 47 **Dynamic Data Services (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.99	Alc-Ipv6-Address	ipv6addr	16 bytes	IPv6 address. For example: Alc-Ipv6-Address = 2001:db8:100::1
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 VSAs 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 are 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 47 **Dynamic Data Services (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.168	Alc-Dyn-Serv-Acct-Interim-lvl-1	integer	1 VSA per tag per message [300 to 15552000]	A value of 0 (zero) corresponds with no interim update messages. A value [1 to 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 to 15552000] For example: Alc-Dyn-Serv-Acct-Interim-lvl-1:1 = 3600
26.6527.169	Alc-Dyn-Serv-Acct-Interim-lvl-2	integer	1 VSA per tag per message [300 to 15552000]	A value of 0 (zero) corresponds with no interim update messages. A value [1 to 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 to 15552000] For example: Alc-Dyn-Serv-Acct-Interim-lvl-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 48 **Dynamic Data Services (Applicability)**

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request	Tag	Max. Tag.
1	User-Name	1	0	0	N	n/a
2	User-Password	1	0	0	N	n/a
4	NAS-IP-Address	0-1	0	0	N	n/a

Table 48 **Dynamic Data Services (Applicability) (Continued)**

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request	Tag	Max. Tag.
8	Framed-IP-Address	0-1	0	0	N	n/a
32	NAS-Identifier	1	0	0	N	n/a
44	Acct-Session-Id	1	0	0-1	N	n/a
87	NAS-Port-Id	1	0	0-1	N	n/a
95	NAS-IPv6-Address	0-1	0	0	N	n/a
26.6527.27	Alc-Client-Hardware-Addr	1	0	0	N	n/a
26.6527.99	Alc-Ipv6-Address	0-1	0	0	N	n/a
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 49 lists the mandatory/optional attributes in CoA messages to the control channel.

Table 49 **Dynamic Data Services — Control Channel CoA Attributes**

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

Notes:

1. CoA rejected (NAK) if not specified (Error Cause: 402 — Missing Attribute)
2. CoA rejected (NAK) if specified (Error Cause: 405 — Unsupported Service)

Table 50 lists the mandatory/optional attributes in CoA messages sent to a dynamic data service associated with a dynamic services data trigger using Nas-Port-Id or Acct-Session-Id of a dynamic data service sap as CoA key.

Table 50 **Data Triggered Dynamic Services (CoA Key = Nas-Port-Id or Acct-Session-Id of Dynamic Data Service SAP) - CoA Attributes**

Attribute Name	Setup	Modify	Teardown	Comment
Nas-Port-Id	N/S	M [1]	M [1]	(CoA key) Nas-Port-Id of a Dynamic Data Service sap

Table 50 **Data Triggered Dynamic Services (CoA Key = Nas-Port-Id or Acct-Session-Id of Dynamic Data Service SAP) - CoA Attributes (Continued)**

Attribute Name	Setup	Modify	Teardown	Comment
Alc-Dyn-Serv-SAP-Id	N/S	O	O	If specified, the sap-id must be the same as the Nas-Port-Id or correspond with the dynamic service sap identified with the Acct-Session-Id.
Alc-Dyn-Serv-Script-Params	N/S	M [2]	N/A	For a Modify, the Script Parameters represent the new parameters required for the change.
Alc-Dyn-Serv-Script-Action	N/S	M [2]	M [2]	
Alc-Dyn-Serv-Policy	N/S	O	O	Must be same as used for setup if specified for Modify or Teardown.
Alc-Dyn-Serv-Acct-Interim-Ivl-1	N/S	X [3]	X [3]	
Alc-Dyn-Serv-Acct-Interim-Ivl-2	N/S	X [3]	X [3]	
Alc-Dyn-Serv-Acct-Stats-Type-1	N/S	X [3]	X [3]	
Alc-Dyn-Serv-Acct-Stats-Type-2	N/S	X [3]	X [3]	
M = Mandatory, O = Optional, X = May Not, N/A = Not Applicable (ignored), N/S = Not Supported				

Notes:

1. Only one of Acct-Session-Id or Nas-Port-Id is mandatory as key in a CoA message to identify the dynamic data service sap
2. CoA rejected (NAK) if not specified (Error Cause: 402 - Missing Attribute)
3. CoA rejected (NAK) if specified (Error Cause: 405 - Unsupported Service)

Table 51 lists the mandatory/optional attributes in CoA messages sent to a dynamic services data trigger using the Acct-Session-Id of the data trigger as CoA key.

Table 51 **Data Triggered Dynamic Services (CoA Key = Acct-Session-Id of Dynamic Service Data Trigger) - CoA Attributes**

Attribute Name	Setup	Modify	Teardown	Comment
Acct-Session-Id	M	M	M	(CoA key) Acct-Session-Id of a dynamic service data trigger.
Alc-Dyn-Serv-SAP-Id	M [1]	M [1]	M [1]	Identifies the dynamic data service associated with the dynamic service data trigger.

Table 51 **Data Triggered Dynamic Services (CoA Key = Acct-Session-Id of Dynamic Service Data Trigger) - CoA Attributes (Continued)**

Attribute Name	Setup	Modify	Teardown	Comment
Alc-Dyn-Serv-Script-Params	M [1]	M [1]	N/A	For a Modify, the Script Parameters represent the new parameters required for the change.
Alc-Dyn-Serv-Script-Action	M [1]	M [1]	M [1]	
Alc-Dyn-Serv-Policy	O	O	O	Default policy used when not specified for Setup action. Must be same as used for setup if specified for Modify or Teardown.
Alc-Dyn-Serv-Acct-Interim-Ivl-1	O	X [2]	X [2]	
Alc-Dyn-Serv-Acct-Interim-Ivl-2	O	X [2]	X [2]	
Alc-Dyn-Serv-Acct-Stats-Type-1	O	X [2]	X [2]	
Alc-Dyn-Serv-Acct-Stats-Type-2	O	X [2]	X [2]	
M = Mandatory, O = Optional, X = May Not, N/A = Not Applicable (ignored)				

Notes:

1. CoA rejected (NAK) if not specified (Error Cause: 402 - Missing Attribute)
2. CoA rejected (NAK) if specified (Error Cause: 405 - Unsupported Service)

1.2.14 Lawful Intercept

Table 52 **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	Defines the LI destination which could be either the mirror destination service ID or the IP destination. • Service ID This 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. • IP destination This configures the IP address, port and router instance of the RADIUS LI mirror destination template. Note: The VSA Alc-LI-Action = 4 (clear-dest-service) can be used to delete the auto-generated mirror destination service identified by three parameters: ip-dst, udp-dst and routing instance. These parameters can be specified in the Alc-LI-Destination VSA. Missing parameters are obtained from the active radius mirror destination template (**configure li radius mirror-dest-template** *name*). All mirror destination services with any ip-src, udp-src, and direction-bit are deleted. A LI admin user can also clear the mirror destination service created from Radius with following CLI command: **clear li radius mirror-dest** *svc-id*.
26.6527.124	Alc-LI-FC	Defines which Forwarding Classes (FCs) should be mirrored (for example: Alc-LI-FC=ef). Attribute needs to be repeated for each FC that needs to be mirrored. Values above the Limits are treated as a setup failure and all FCs are 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.

Table 52 **Lawful Intercept (Description) (Continued)**

Attribute ID	Attribute Name	Description
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 (**configure subscriber-mgmt authentication-policy** *policy-name* **radius-authentication-server**). The attribute is ignored if the RADIUS CoA server is configured in the **radius-server** context of the routing instance (**configure router | service vprn** *service-id* **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 [26.6527.123] Alc-LI-Destination attribute) is configured with routable encap that contains the LI-Shim (**configure mirror mirror-dest** *service-id* **encap layer-3-encap ip-udp-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.
26.6527.139	Alc-LI-Session-Id	Specifies the session-id to be placed in the LI-Shim header and only applicable if the mirror-dest (as specified by the [26.6527.123] Alc-LI-Destination attribute) is configured with routable encap that contains the LI-Shim (**configure mirror mirror-dest** *service-id* **encap layer-3-encap ip-udp-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.
26.6527.243	Alc-LI-Use-Outside-Ip	Defines if Lawful Intercept should be performed before or after NAT on a l2-aware NAT subscriber. If set to true (1), the lawful intercepted traffic contains the subscriber outside public IP address. If set to false (2), the lawful intercepted traffic contains the subscriber inside private IP address.

Table 53 **Lawful Intercept (Limits)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.122	Alc-LI-Action	integer	[1 to 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

Table 53 **Lawful Intercept (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.123	Alc-LI-Destination	string	32 chars	• Service ID destination The service ID For example: Alc-LI-Destination = 9999 • IP destination IP-address[:<port>][router <instance>] where :<port> and router <instance> are optional. When not specified, the system uses the port and router instance configured on the LI mirror destination template (**configure li radius mirror-dest-template** *name*). For example: Alc-LI-Destination = "192.168.0.10:101 router Base"
26.6527.124	Alc-LI-FC	integer	[0 to 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 to 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 with dir-bit 30b without dir-bit	29b = [0 to 536870911] 30b = [0 to 1073741823] For example: Alc-LI-Intercept-Id = 1234
26.6527.139	Alc-LI-Session-Id	integer	[0 to 4294967295] id	For example: Alc-LI-Session-Id = 8888

Table 53 **Lawful Intercept (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.243	Alc-LI-Use-Outside-Ip	integer	[1 to 2]	1=true, 2=false For example: Alc-LI-User-Outside-IP = 1

Table 54 **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+	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
26.6527.243	Alc-LI-Use-Outside-Ip	0	0-1	0-1	Y

1.2.15 IPSec

Table 55 **IPSec (Description)**

Attribute ID	Attribute Name	Description
1	User-Name	For IKEv1 remote-access tunnel, this represents the xauth username. 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.

Table 55 **IPSec (Description) (Continued)**

Attribute ID	Attribute Name	Description
2	User-Password	For IKEv1 remote-access tunnel, this represents the xauth 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** *service-id* **interface** *interface-name* **sap** *sap-id* **ipsec-gw** *gw-name* **pre-shared-key** or **configure service vprn** *service-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 IKEv1/v2 remote-access tunnel client via configuration payload: INTERNAL_IP4_ADDRESS. This attribute is also reflected in RADIUS accounting request packet for IKEv2 tunnel.
9	Framed-IP-Netmask	The IPv4 netmask to be assigned to IKEv1/v2 remote-access tunnel client via 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", example, "10.1.1.1:1546". The 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 calling-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.
46	Acct-Session-Time	This attribute represents the tunnel's lifetime in seconds. It is included in an Accounting-Stop packet.
79	EAP-Message	This attribute encapsulates the received IKEv2 EAP payload in access-request. A RADIUS server can include this attribute in an access-challenge or access-accept.

Table 55 **IPSec (Description) (Continued)**

Attribute ID	Attribute Name	Description
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* **include-radius-attribute nas-port-id**.
88	Framed-Pool	The name of one IPv4 address pool or the name of a primary and secondary IPv4 address pool separated with a one 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 for local address assignment during IKEv2 remote-access tunnel setup. A RADIUS server can include the attribute in an Access-Accept. The value of this attribute overrides the local configured value in the …>**ipec-gw>local-address-assignment>ipv4** CLI context.
97	Framed-IPv6-Prefix	The IPv6 address to be assigned to IKEv2 remote-access tunnel client via IKEv2 configuration payload: INTERNAL_IP6_ADDRESS. The prefix and prefix-length of Framed-IPv6-Prefix are conveyed in the corresponding part of INTERNAL_IP6_ADDRESS. The attribute is included in RADIUS accounting request packet.
100	Framed-IPv6-Pool	The name of the IPv6 address pool used for local address assignment during IKEv2 remote-access tunnel setup. A RADIUS server can include the attribute in an Access-Accept. The value of this attribute overrides the local configured value in the **ipec-gw>local-address-assignment>ipv6** CLI context.
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 IPv4 DNS server address to be assigned to an IKEv1/v2 remote-access tunnel client via configuration payload: INTERNAL_IP4_DNS. In case of IKEv2, up to four DNS server addresses can be returned to a client, including Alc-Primary-Dns, Alc-Secondary-Dns, Alc-Ipv6-Primary-Dns and Alc-Ipv6-Secondary-Dns.

Table 55 **IPSec (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.10	Alc-Secondary-Dns	The IPv4 DNS server address to be assigned to an IKEv2 remote-access tunnel client via IKEv2 configuration payload: INTERNAL_IP4_DNS. Up to four DNS server addresses can be returned to a client, including Alc-Primary-Dns, Alc-Secondary-Dns, Alc-Ipv6-Primary-Dns and Alc-Ipv6-Secondary-Dns.
26.6527.61	Alc-IPsec-Serv-Id	IPSec private service id, used by IKEv1/v2 remote-access 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/v2 remote-access 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/v2 remote-access 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.
26.6527.64	Alc-IPsec-SA-Lifetime	IPSec phase2 SA lifetime in seconds, used by IKEv1/v2 remote-access tunnel. A preconfigured value is used when this attribute is omitted (**configure ipsec ike-policy** *policy-id* **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/v2 remote-access tunnel. The PFS group in ike-policy is used when this attribute is omitted (**configure ipsec ike-policy** *policy-id* **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/v2 remote-access 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.

Table 55 **IPSec (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.67	Alc-IPsec-SA-Auth-Algorithm	IPSec phase2 SA Authentication Algorithm, used by IKEv1/v2 remote-access 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/v2 remote-access 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.
26.6527.105	Alc-Ipv6- Primary-Dns	The IPv6 DNS server address to be assigned to an IKEv2 remote-access tunnel client via IKEv2 configuration payload: INTERNAL_IP6_DNS. Up to four DNS server addresses can be returned to a client, which could be any combination of Alc-Primary-Dns, Alc-Secondary-Dns, Alc-Ipv6-Primary-Dns and Alc-Ipv6-Secondary-Dns.
26.6527.106	Alc-Ipv6-Secondary-Dns	The IPv6 DNS server address to be assigned to an IKEv2 remote-access tunnel client via IKEv2 configuration payload: INTERNAL_IP6_DNS. Up to four DNS server addresses can be returned to a client, which could be any combination of Alc-Primary-Dns, Alc-Secondary-Dns, Alc-Ipv6-Primary-Dns and Alc-Ipv6-Secondary-Dns.
26.6527.229	Alc-IPsec-Ts-Override	The name of the ts-list to be used during IKEv2 tunnel setup. It overrides the CLI configured value via the CLI command **ts-negotiation**.
26.6527.237	Alc-Subject-Key-Identifier	The binary value of Subject Key Id in peer's certificate.
241.26.6527.41	Alc-Acct-IPsec-Bidir-Kibibytes	(IKEv2 RA tunnel only) The number of kilobytes of bi-directional (encryption + decryption) traffic passed over the IPsec tunnel.
241.26.6527.42	Alc-Acct-IPsec-Encrypted-Kibibytes	(IKEv2 RA tunnel only) The number of kilobytes of encrypted traffic passed over the IPsec tunnel.
241.26.6527.43	Alc-Acct-IPsec-Decrypted-Kibibytes	(IKEv2 RA tunnel only) The number of kilobytes of decrypted traffic passed over the IPsec tunnel.
241.26.6527.44	Alc-Acct-IPsec-Bidir-Packets	(IKEv2 RA tunnel only) The number of packets of bi-directional (encryption + decryption) passed over the IPsec tunnel.
241.26.6527.45	Alc-Acct-IPsec-Encrypted-Packets	(IKEv2 RA tunnel only) The number of encrypted packets passed over the IPsec tunnel.

Table 55 **IPSec (Description) (Continued)**

Attribute ID	Attribute Name	Description
241.26.6527.46	Alc-Acct-IPsec-Decrypted-Packets	(IKEv2 RA tunnel only) The number of decrypted packets passed over the IPsec tunnel.

Table 56 **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
46	Acct-Session-Time	integer	4 bytes 4294967295 seconds	For example: Acct-Session-Time = 870
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”

Table 56 **IPSec (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
88	Framed-Pool	string	32 chars per pool name	For example: Framed-Pool = "MyPoolname"
97	Framed-IPv6-Prefix	ipv6prefix	max. 16 bytes for prefix + 1 byte for length	For example: Framed-IPv6-Prefix = 2001:DB8:CAFE:1::100/128
100	Framed-IPv6-Pool	string	32 chars	For example: Framed-IPv6-Pool = "MyV6Poolname"
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	Up to 4 attributes (4B per attribute)	For example: Alc-Primary-Dns = 192.168.1.1
26.6527.10	Alc-Secondary-Dns	ipaddr	Up to 4 attributes (4B per attribute)	For example: Alc-Secondary-Dns = 192.168.2.1
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	1 to 2048	For example: Alc-IPsec-Tunnel-Template-Id = 200
26.6527.64	Alc-IPsec-SA-Lifetime	integer	[1200 to 172800] seconds	For example: Alc-IPsec-SA-Lifetime = 2400
26.6527.65	Alc-IPsec-SA-PFS-Group	integer	[1|2|5|14|15]	1=group1, 2=group2, 5=group5, 14=group14, 15=group15 For example: Alc-IPsec-SA-PFS-Group = 2
26.6527.66	Alc-IPsec-SA-Encr-Algorithm	integer	[1 to 6]	1=null, 2=des, 3=3des, 4=aes128, 5=aes192, 6=aes256 For example: Alc-IPsec-SA-Encr-Algorithm = 3

Table 56 **IPSec (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.67	Alc-IPsec-SA-Auth-Algorithm	integer	[1 to 7]	1=null, 2=md5, 3=sha1, 4=sha256, 5=sha384, 6=sha512, 7=aesXcbc 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
26.6527.105	Alc-Ipv6- Primary-Dns	ipv6addr	Up to 4 attributes (16B per attribute)	For example: Alc-Ipv6-Primary-Dns = 2001:DB8:1::1
26.6527.106	Alc-Ipv6- Secondary-Dns	ipv6addr	Up to 4 attributes (16B per attribute)	For example: Alc-Ipv6-Secondary-Dns = 2001:DB8:2::1
26.6527.229	Alc-IPsec-Ts-Override	string	32 bytes	For example:Alc-IPsec-Ts-Override="ikev2-ts-list-1"
26.6527.237	Alc-Subject-Key-Identifier	integer64	8 bytes	The least significant 247 bytes of the Subject Key Id in peer's certificate.
241.26.6527.41	Alc-Acct-IPsec-Bidir-Kibibytes	integer64	8 bytes	For example: Alc-Acct-IPsec-Bidir-Kibibytes = 2000
241.26.6527.42	Alc-Acct-IPsec-Encrypted-Kibibytes	integer64	8 bytes	For example: Alc-Acct-IPsec-Encrypted-Kibibytes = 1000
241.26.6527.43	Alc-Acct-IPsec-Decrypted-Kibibytes	integer64	8 bytes	For example: Alc-Acct-IPsec-Decrypted-Kibibytes = 1000
241.26.6527.44	Alc-Acct-IPsec-Bidir-Packets	integer64	8 bytes	For example: Alc-Acct-IPsec-Bidir-Packets = 1000
241.26.6527.45	Alc-Acct-IPsec-Encrypted-Packets	integer64	8 bytes	For example: Alc-Acct-IPsec-Encrypted-Packets = 500
241.26.6527.46	Alc-Acct-IPsec-Decrypted-Packets	integer64	8 bytes	For example: Alc-Acct-IPsec-Decrypted-Packets = 500

Table 57 **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
46	Acct-Session-Time	0	0	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
88	Framed-Pool	0	0-1	0	0
97	Framed-IPv6-Prefix	0	0-1	0	0-1
100	Framed-IPv6-Pool	0	0-1	0	0
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+	0	0
26.6527.10	Alc-Secondary-Dns	0	0+	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

Table 57 **IPSec (Applicability) (Continued)**

Attribute ID	Attribute Name	Access Request	Access Accept	Access Challenge	Acct Request
26.6527.68	Alc-IPsec-SA-Replay-Window	0	0-1	0	0
26.6527.105	Alc-Ipv6- Primary-Dns	0	0+	0	0
26.6527.106	Alc-Ipv6- Secondary-Dns	0	0+	0	0
26.6527.229	Alc-IPsec-Ts-Override	0	0-1	0	0
26.6527.237	Alc-Subject-Key-Identifier	0-1	0	0	0
241.26.6527.41	Alc-Acct-IPsec-Bidir-Kibibytes	0	0	0	0-1
241.26.6527.42	Alc-Acct-IPsec-Encrypted-Kibibytes	0	0	0	0-1
241.26.6527.43	Alc-Acct-IPsec-Decrypted-Kibibytes	0	0	0	0-1
241.26.6527.44	Alc-Acct-IPsec-Bidir-Packets	0	0	0	0-1
241.26.6527.45	Alc-Acct-IPsec-Encrypted-Packets	0	0	0	0-1
241.26.6527.46	Alc-Acct-IPsec-Decrypted-Packets	0	0	0	0-1

1.2.16 Application Assurance

Table 58 **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 an IPv4 host creation (CoA), if the host is already configured for another AA-transit subscriber with the same parent SAP, it is 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 or 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.

Table 58 **Application Assurance (Description) (Continued)**

Attribute ID	Attribute Name	Description
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-Str 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 preconfigured default values if allowed. If no default value is preconfigured, the subscriber's application profile is silently disabled for the ESM AA-subscriber; in case of a transit AA-subscriber creation the CoA is 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 is treated as setup failures.
26.6527.130	Alc-AA-Transit-IP	Used to create (CoA), modify (CoA), delete (disconnect) or audit (CoA) an Application Assurance **transit-ipv4** or **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 macro 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 58 **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 '=' is interpreted as the character string and everything after the '=' is 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: • The Alc-AA-App-Service-Options VSA is optional on sub create (with app-profile assignment) and may be used later to modify policy. • On a CoA, if an app-profile VSA is not present, all ASO VSAs are applied on top of the current policy of the sub. • On a CoA, if an app-profile VSA is present, even if it is the same app-profile as currently applied, all previous ASO override policy is removed. Any ASO VSAs in the same CoA message as the new app-profile are 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. • 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. (*Continued on next page*)

Table 58 **Application Assurance (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.193 (*cont.*)	Alc-AA-App-Service-Options (*cont.*)	• A new aa-sub characteristic can be applied, or an existing characteristic modified, by an ASO VSA. • When an ASO VSA is received any existing overrides remain and the new overrides are cumulative. If there are multiple ASO VSAs for the same characteristic in the CoA, the last one takes effect.
241.26.6527.26	Alc-Aa-Sub-Scope	This attribute is used to define the scope of the [26.6527.45] Alc-App-Prof-Str attribute and the related [26.6527.193] Alc-AA-App-Service-Options attributes to affect either the subscriber (all hosts) or to affect only the specific host IP addresses used by a unique MAC address. The absence of this attribute defaults to using subscriber scope.

Table 59 **Application Assurance (Limits)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
8	Framed-IP-Address	ipaddr	4 bytes	# 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 # Example for sap NAS-Port-Id = 1/1/4:501.1001 # Example for spoke-sdp NAS-Port-Id = 4:100
97	Framed-IPv6-Prefix	ipv6prefix	max. 16 bytes for prefix + 1 byte for length	# Example: Framed-IPv6-Prefix = 2001:cafe:cefe:1::/64
26.6527.11	Alc-Subsc-ID-Str	string	32 chars	# Example: Alc-Subsc-ID-Str = transit-sub-radius1
26.6527.45	Alc-App-Prof-Str	string	16 bytes	# Example: Alc-App-Prof-Str = MyAppProfile

Table 59 **Application Assurance (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
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	247 chars (DSM) 32 chars (ESM)	# For example: Alc-AA-Sub-Http-Url-Param = "&Provider=ISPname&Location=Station 21"
26.6527.193	Alc-AA-App-Service-Options	string	65 bytes per string (char. 32bytes + 1 byte + value 32bytes) 32 VSAs per message	Format characteristic=value, # For example: Alc-AA-App- Service-Options = “ServiceTier=Bronze”
241.26.6527.26	Alc-Aa-Sub-Scope	integer	4 bytes	1=subscriber, 2=mac For example: To set the scope of the application profile to subscriber hosts with the same MAC address: Alc-Aa-Sub-Scope = 2 To set the scope of the application profile to all subscriber hosts belonging to the same ESM subscriber: Alc-Aa-Sub-Scope = 1

Table 60 **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

Table 60 **Application Assurance (Applicability) (Continued)**

Attribute ID	Attribute Name	Access Request	Access Accept	CoA Request
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
241.26.6527.26	Alc-Aa-Sub-Scope	0	0-1	0-1

1.2.17 CLI User Authentication and Authorization

Table 61 **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*)
18	Reply-Message	The attribute received in the Access-Challenge message for challenge-response interactive authentication. The content of the Reply-Message attribute is displayed to the user. The user is prompted for a response.
24	State	The attribute received in the Access-Challenge message for challenge-response interactive authentication and sent unmodified in the new Access-Request

Table 61 **CLI User Authentication and Authorization (Description) (Continued)**

Attribute ID	Attribute Name	Description
27	Session-Timeout	The attribute received in the Access-Challenge message for challenge-response interactive authentication. The maximum number of seconds in which the user should provide the response. After this time, the prompt is terminated.
28	Idle-Timeout	The attribute received in the Access-Challenge message for challenge-response interactive authentication. The number of seconds after which the prompt is terminated when no user activity is detected.
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.
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.

Table 61 **CLI User Authentication and Authorization (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.4	Timetra-Profile	The user profile(s) that the user has access to and refers to preconfigured user-profile-name's (**configure system security profile** *user-profile-name*). These preconfigured profiles hold a **default-action**, a **match** *command-string* and an **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 that 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 built 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, thus, if the RADIUS server is configured to have five command strings of which the third is too long, only the first two entries are used and the rest are 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 that 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 built from the mandatory attribute [26.6527.5]Timetra-Default-Action and optional attributes [26.6527.6] Timetra-Cmd, [26.6527.7] Timetra-Action.

Table 61 **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. **Notes:** • [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. • 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 built 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 62 **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”
18	Reply-Message	string	—	For example: Reply-Message = “Please enter your response for challenge: 4598 2441 ?”
24	State	string	—	For example: State = “Challenge-Response”
27	Session-Timeout	integer	—	For example: Session-Timeout = 180
28	Idle-Timeout	integer	—	For example: Idle-Timeout = 90
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”

Table 62 **CLI User Authentication and Authorization (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
44	Acct-Session-Id	string	22 bytes	For example: Acct-Session-Id = “212846359210251211 3409”
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
26.6527.7	Timetra-Action	integer	25 attributes	# 1=permit, 2=deny For example: Timetra-Cmd = permit

Table 62 **CLI User Authentication and Authorization (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
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 63 **CLI User Authentication and Authorization (Applicability)**

Attribute ID	Attribute Name	Access Request 1	Access-Challenge 1	Access Request 2	Access-Accept 1 or 2
1	User-Name	1	0	1	0
2	User-Password	1	0	1	0
4	NAS-IP-Address	0-1	0	0-1	0
18	Reply-Message	0	1+	0	0
24	State	0	0-1	0-1	0
27	Session-Timeout	0	0-1	0	0
28	Idle-Timeout	0	0-1	0	0
31	Calling-Station-Id	1	0	1	0
44	Acct-Session-Id	0	0	0	0
61	NAS-Port-Type	1	0	1	0
95	NAS-IPv6-Address	0-1	0	0-1	0
26.6527.1	Timetra-Access	0	0	0	1
26.6527.2	Timetra-Home-Directory	0	0	0	1
26.6527.3	Timetra-Restrict-To-Home	0	0	0	1
26.6527.4	Timetra-Profile	0	0	0	0+
26.6527.5	Timetra-Default-Action	0	0	0	1

Table 63 **CLI User Authentication and Authorization (Applicability) (Continued)**

Attribute ID	Attribute Name	Access Request 1	Access-Challenge 1	Access Request 2	Access-Accept 1 or 2
26.6527.6	Timetra-Cmd	0	0	0	0+
26.6527.7	Timetra-Action	0	0	0	0-1
26.6527.8	Timetra-Exec-File	0	0	0	0-1

1.2.18 AAA Route Downloader

Table 64 **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 is 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.

Table 64 **AAA Route Downloader (Description) (Continued)**

Attribute ID	Attribute Name	Description
22	Framed-Route	The RADIUS route-download application periodically sends a RADIUS Access-Request message to the RADIUS server to request that IPv4 or 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 or 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 to 254*]) is installed when the metric value is omitted in the formatted attribute. A default tag (**configure aaa route-downloader** *name* **default-tag** [*0 to 4294967295*]) is installed when the tag value is omitted in the formatted attribute. The complete RADIUS Access Accept is ignored (fails to parse the 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 are removed from the routing table and new routes are added. The 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 are removed from the routing table (implicit empty route-download table). The route-download application accepts downloaded IPv4 routes in either [22] Framed-Route or [26.9.1] 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 65 **AAA Route Downloader (Limits)**

Attribute 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

Table 65 **AAA Route Downloader (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
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 vpn-name should not contain blank spaces as this would result in a parsing error and a drop of the corresponding prefix. #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 vpn-name should not contain blank spaces as this would result in a parsing error and a drop of the corresponding prefix. #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 65 **AAA Route Downloader (Limits) (Continued)**

Attribute 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 vpn-name should not contain blank spaces as this would result in a parsing error and a drop of the corresponding prefix. #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 66 **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+

1.3 RADIUS Accounting Attributes

1.3.1 Enhanced Subscriber Management (ESM) Accounting

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

- Host accounting (H)
- 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 71 shows the accounting mode messages that report the attribute:

- 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 or IPoE session):

```
show service id <svc-id> ppp session detail
show service id <svc-id> ipoe 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 67 **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

The reporting of volume counters in accounting is coupled to the sending of periodic or host triggered Accounting Interim Updates messages. Volume based accounting is therefore enabled via the **interim-update** CLI parameter for all accounting modes and/or by the **host-update** CLI parameter in session accounting mode as shown in Table 68.

Table 68 **Accounting Statistics Type**

Accounting Mode	Statistics Type
host-accounting interim-update session-accounting interim-update [host-update] session-accounting host-update queue-instance-accounting interim-update	Time and volume based accounting
host-accounting session-accounting queue-instance-accounting	Time based accounting

The different sets of volume accounting attributes that can be included in the Accounting Interim and Stop messages are controlled via **include-radius-attribute** CLI commands. Multiple volume reporting types can be enabled simultaneously:

```
configure
  subscriber-mgmt
    radius-accounting-policy <name>
      include-radius-attribute
        [no] detailed-acct-attributes  # 64 bit per queue/policer counters
        [no] std-acct-attributes       # 32 bit aggregate counters (v4+v6)
        [no] v6-aggregate-stats        # 32 bit aggregate counters (v6 only)
```

Table 69 **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 accounting via **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute no user-name**.

Table 69 **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 IPv4 address of the system interface (**configure router interface system address** *address*). The default NAS-IP-Address value can be overwritten: ESM: **configure aaa radius-server-policy** *policy-name* **servers source-address** *ip- address* DSM: **configure aaa isa-radius-policy** *name* **nas-ip-address-origin** {**isa-ip** | **system-ip**}
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 bits. 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.

Table 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

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**.
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.

Table 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
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. WLAN Gateway: Reflects the currently learned AP-MAC and SSID. These can be learned via EAP, DHCP (opt82), DHCPv6 LDRA (interface-id) or arp-over-GRE.
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 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 ies | vprn** *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 accounting via **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute no calling-station-id**. For DSM the Calling-Station-Id is always equal to the remote-id if present and the UE MAC address otherwise.
32	NAS-Identifier	A string (**configure system name** *system-name*) identifying the NAS originating the Accounting requests and sent when **nas-identifier** is included for the corresponding application: **configure subscriber-mgmt radius-accounting-policy** (ESM accounting), **configure aaa isa-radius-policy** (LSN accounting, WLAN-GW) 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. In initial accounting messages this attribute is included with value 0 for ESM and omitted for DSM. Attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute no acct-delay-time**.

Table 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
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 sent 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**). [53] Acct-Output-Gigawords indicates how many times (if greater than zero) the [43] Acct-Output-Octets counter has wrapped around 2^32.
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 or IPoE 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**}). For DSM, the attribute has a fixed 10-byte hexadecimal number format with each byte separated by a hyphen. 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. When the accounting session time equals zero (example when the accounting start is followed immediately by an accounting interim update or by an accounting stop within the same second), then the attribute is not included.
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.

Table 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
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/IPoE session was terminated. An overview of the mapping between [26.6527.226] Alc-Error-Code / [26.6527.227] Alc-Error-Message and the corresponding [49] Acct-Terminate-Cause attribute value can be displayed with the command: **tools dump aaa radius-acct-terminate-cause**.
50	Acct-Multi-Session-Id	A unique Accounting ID that links together multiple related accounting sessions. (see Enhanced Subscriber Management Accounting [50] Acct-Multi-Session-Id Values) 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**}). For DSM the attribute has a fixed 10 byte hexadecimal number format with each byte separated by a hyphen. There are no DSM hosts linked together through this attribute.
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.
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.

Table 69 **Enhanced Subscriber Management 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
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 radius-accounting-policy** (ESM accounting), **configure aaa isa-radius-policy** (LSN accounting, WLAN-GW) and **configure aaa l2tp-accounting-policy** (L2TP accounting). Checked for correctness if returned in CoA.
64	Tunnel-Type	(L2TP LAC and LNS only) 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 in LAC Access-Accept and its value must be L2TP. The attribute is included in Acct-Request messages if the **tunnel-server-attrs** (LNS) or **tunnel-client-attrs** (LAC) option is configured in the **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute** CLI context.
65	Tunnel-Medium-Type	(L2TP LAC and LNS only) The transport medium to use when creating a tunnel for protocols (such as L2TP) that can operate over multiple transports. This attribute is mandatory in LAC Access-Accept and its value must be IP or IPv4. The attribute is included in Acct-Request messages if the **tunnel-server-attrs** (LNS) or **tunnel-client-attrs** (LAC) option is configured in the **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute** CLI context.
66	Tunnel-Client-Endpoint	(L2TP LAC and LNS only) The dotted-decimal IP address of the initiator end of the tunnel. Preconfigured 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. The attribute is included in Acct-Request messages if the t **tunnel-server-attrs** (LNS) or **tunnel-client-attrs** (LAC) option is configured in the **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute** CLI context.

Table 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
67	Tunnel-Server-Endpoint	(L2TP LAC and LNS only) The dotted-decimal IP address of the server end of the tunnel is also on the LAC the dest-ip for all L2TP packets for that tunnel. The attribute is included in Acct-Request messages if the **tunnel-server-attrs** (LNS) or **tunnel-client-attrs** (LAC) option is configured in the **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute** CLI context.
68	Acct-Tunnel-Connection	(L2TP LAC and LNS only) The format of the attribute in Acct-Request messages can be configured with **configure subscriber-mgmt radius-accounting-policy** *name* **acct-tunnel-connection-fmt** *ascii-spec*. By default, the Call Serial Number is inserted. The attribute is included in Acct-Request messages if the **tunnel-server-attrs** (LNS) or **tunnel-client-attrs** (LAC) option is configured in the **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute** CLI context.
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. For WLAN-GW, the Nas-Port-Id is a text string with format defined by the aggregation type (see WLAN Gateway for details): GRE or L2TPv3: “*tunnel-type* rtr-*virtual router id*#lip-*local ip address*#rip-*remote ip address*” VLAN: “VLAN svc-*svc-id*[:*vlan*[.*vlan*]]”

Table 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
90	Tunnel-Client-Auth-ID	(L2TP LAC and LNS only) Used during the authentication phase of tunnel establishment and copied by the LAC in L2TP SCCRQ AVP 7 Host Name. 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** s*ervice-id* **l2tp local-name** *host-name*). The system name (**configure system name** *system-name*) is copied in AVP Host Name if this attribute is omitted and no local-name is configured. The attribute is included in Acct-Request messages if the **tunnel-server-attrs** (LNS) or **tunnel-client-attrs** (LAC) option is configured in the **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute** CLI context.
91	Tunnel-Server-Auth-ID	(L2TP LAC and LNS only) Used during the authentication phase of tunnel establishment. 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. The attribute is included in Acct-Request messages if the **tunnel-server-attrs** (LNS) or **tunnel-client-attrs** (LAC) option is configured in the **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute** CLI context.
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*).
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** *name* **include-radius-attribute framed-interface-id**). The Framed-Interface-Id attribute is not sent in RADIUS Authentication and silently ignored in RADIUS Accept.

Table 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
97	Framed-IPv6-Prefix	The IPv6 prefix or 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**. For Distributed Subscriber Management (DSM), if SLAAC is active for a UE, the attribute contains the prefix assigned to this UE. Inclusion of this attribute is enabled via **configure aaa isa-radius-policy** *policy-name* **acct-include-attributes 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 and/or a DHCPv6 IA-PD host modeled as a managed route. Valid RADIUS learned managed routes and DHCPv6 IA-PD hosts modeled as a managed route 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.

Table 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
123	Delegated-IPv6-Prefix	Attribute that carries the Prefix (IPv6 prefix or 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 ies | vprn** *service-id* **subscriber-interface** *ip-int-name* **ipv6 delegated-prefix-length** [*48 to 64*] is required with the received attribute prefix-length unless a variable DPL is configured (**configure service** ies | vprn *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 to 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**.
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 (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 69 **Enhanced Subscriber Management Accounting (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** *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**.
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**.

Table 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
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**.
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**.

Table 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
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. Preconfigured 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** *type* or **configure subscriber-mgmt local-user-db** *local-user-db-name* **ppp host** *host-name* **access-loop-encapsulation encap-offset** type *type*). [26.6527.133] Alc-Access-Loop-Encap-Offset when returned in Access-Accept is taken into account (overrules received tags and preconfigured 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 preconfigured 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**. For DSM accounting sessions the Alc-Subsc-ID-Str reflects the UE MAC address.

Table 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.12	Alc-Subsc-Prof-Str	The subscriber profile is a template that contains settings (accounting, IGMP, HQoS, and so on) 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-ident-policy-name* **sub-profile-map**) to such a 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 preconfigured defaults are used. 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 that contains settings (filter, QoS, host-limit, and so on) 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 an SLA profile (**configure subscriber-mgmt sla-profile** *sla-profile-name*). Strings longer than the allowed maximum are treated as setup failures. Unreferenced strings (a string that does not map to a policy) are silently ignored and preconfigured defaults are used. The attribute is omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute no sla-profile**.

Table 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
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 stat-mode = v4-v6: Count IPv4 bytes (in- and out-of-profile) [26.6527.107] Alc-Acct-I-statmode VSA included for queues with value v4-v6 • policer stat-mode = v4-v6: This attribute is not used. For policers, ingress forwarded IPv4 bytes (in- and out-of-profile) are reported with attribute [26.6527.108] Alc-Acct-I-Hiprio-Octets_64. 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**).
26.6527.20	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 stat-mode = v4-v6: Count IPv6 bytes (in- and out-of-profile) [26.6527.107] Alc-Acct-I-statmode VSA included for queues with value v4-v6 • policer stat-mode = v4-v6: This attribute is not used. For policers, ingress forwarded IPv6 bytes (in- and out-of-profile) are reported with attribute [26.6527.109] Alc-Acct-I-Lowprio-Octets_64. 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 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
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 stat-mode = v4-v6: Count IPv4 bytes (in- and out-of-profile) [26.6527.127] Alc-Acct-O-statmode VSA included for queues with value v4-v6 • policer stat-mode = v4-v6: This attribute is not used. For policers, egress forwarded IPv4 bytes (in- and out-of-profile) are reported with attribute [26.6527.110] Alc-Acct-O-Hiprio-Octets_64. 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 stat-mode = v4-v6: Count IPv6 bytes (in- and out-of-profile) [26.6527.127] Alc-Acct-O-statmode VSA included for queues with value v4-v6 • policer stat-mode = v4-v6: This attribute is not used. For policers, egress forwarded IPv6 bytes (in- and out-of-profile) are reported with attribute [26.6527.111] Alc-Acct-O-Lowprio-Octets_64. 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 69 **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 out-of-profile bytes (IPv4 and IPv6) [26.6527.107] Alc-Acct-I-statmode VSA only included for policers • queue stat-mode = v4-v6: Count IPv4 packets (in- and out-of-profile) [26.6527.107] Alc-Acct-I-statmode VSA included for queues with value v4-v6 • policer stat-mode = v4-v6: This attribute is not used. For policers, ingress forwarded IPv4 packets (in- and out-of-profile) are reported with attribute [26.6527.112] Alc-Acct-I-Hiprio-Packets_64. 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 stat-mode = v4-v6: Count IPv6 packets (in- and out-of-profile) [26.6527.107] Alc-Acct-I-statmode VSA included for queues with value v4-v6 • policer stat-mode = v4-v6: This attribute is not used. For policers, ingress forwarded IPv6 packets (in- and out-of-profile) are reported with attribute [26.6527.113] Alc-Acct-I-Lowprio-Packets_64. 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 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
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 stat-mode = v4-v6: Count IPv4 packets (in- and out-of-profile) [26.6527.127] Alc-Acct-O-statmode VSA included for queues with value v4-v6 • policer stat-mode = v4-v6: This attribute is not used. For policers, egress forwarded IPv4 packets (in- and out-of-profile) are reported with attribute [26.6527.114] Alc-Acct-O-Hiprio-Packets_64. 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**).
26.6527.26	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 stat-mode = v4-v6: Count IPv6 packets (in- and out-of-profile) [26.6527.127] Alc-Acct-O-statmode VSA included for queues with value v4-v6 • policer stat-mode = v4-v6: This attribute is not used. For policers, egress forwarded IPv6 packets (in- and out-of-profile) are reported with attribute [26.6527.115] Alc-Acct-O-Lowprio-Packets_64. 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 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
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**).
26.6527.36	Alc-DHCP-Vendor-Class-Id	Initiated by DHCP clients via option 60 [Class-id] and reflected in Accounting. (**configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute dhcp-vendor-class-id**).
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 69 **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**).

Table 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
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
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

Table 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
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 69 **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.

Table 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
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.
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.

Table 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
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.
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-discarded-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.

Table 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
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 69 **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**).

Table 69 **Enhanced Subscriber Management Accounting (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 omitted in accounting via **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute no ipv6-address**. For Distributed Subscriber Management (DSM), if IA-NA is active for a UE, the attribute contains the address assigned to this UE. Inclusion of this attribute is enabled via **configure aaa isa-radius-policy** *policy-name* **acct-include-attributes ipv6-address**.
26.6527.100	Alc-Serv-Id	DSM only. The attribute contains the service ID where the Layer 3 tunnel is terminated. The attribute is omitted in case of a Layer 2 tunnel or if the service ID is not known.
26.6527.102	Alc-ToServer-Dhcp-Options	DSM only. The attribute contains all dhcpv4 options received in the last DHCPv4 message. Each dhcpv4 option is stored in a separate attribute.
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 full list of stat-modes can be found in the *Quality of Service Guide*. 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.

Table 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.108	Alc-Acct-I-Hiprio-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. • stat-mode = *(specific stat-mode only): ingress forwarded high-priority bytes • stat-mode = v4-v6: ingress forwarded IPv4 bytes (in- and out-of-profile) 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-forwarded-bytes have been handled for this user over the course of this service being provided. • stat-mode = *(specific stat-mode only): ingress forwarded low-priority bytes • stat-mode = v4-v6: ingress forwarded IPv6 bytes (in- and out-of-profile) 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-forwarded-bytes have been handled for this user over the course of this service being provided. • stat-mode = *(specific stat-mode only): egress forwarded high-priority bytes • stat-mode = v4-v6: egress forwarded IPv4 bytes (in- and out-of-profile) 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 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.111	Alc-Acct-O-Lowprio-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. • stat-mode = *(specific stat-mode only): egress forwarded low-priority bytes • stat-mode = v4-v6: egress forwarded IPv6 bytes (in- and out-of-profile) 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-forwarded-packets have been handled for this user over the course of this service being provided. • stat-mode = *(specific stat-mode only): ingress forwarded high-priority packets • stat-mode = v4-v6: ingress forwarded IPv4 packets (in- and out-of-profile) 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.
26.6527.113	Alc-Acct-I-Lowprio-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. • stat-mode = *(specific stat-mode only): ingress forwarded low-priority packets • stat-mode = v4-v6: ingress forwarded IPv6 packets (in- and out-of-profile) 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 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.114	Alc-Acct-O-Hiprio-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. • stat-mode = *(specific stat-mode only): egress forwarded high-priority packets • stat-mode = v4-v6: egress forwarded IPv4 packets (in- and out-of-profile) 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. Indicates how many policer egress forwarded packets have been handled for this user over the course of this service being provided. • stat-mode = *(specific stat-mode only): egress forwarded low-priority packets • stat-mode = v4-v6: egress forwarded IPv6 packets (in- and out-of-profile) 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.

Table 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
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.
26.6527.121	Alc-Nat-Port-Range	This attribute is used to report allocated or released NAT resources for an L2-Aware NAT subscriber. The reported NAT resources include a public IPv4 address, a public port range, an outside routing instance and a NAT policy name. This attribute is included in accounting by configuring the **nat-port-range** option under the **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attributes** CLI hierarchy.
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 full list of stat-modes can be found in the *Quality of Service Guide*. For both policers and queues, the egress stat-mode can be configured to IPv4-IPv6 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 or 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.
26.6527.140	Alc-Nat-Outside-Serv-Id	DSM only. For a DSM UE, this attribute includes the service ID of the outside VRF where IPv4 traffic is forwarded after NAT.
26.6527.141	Alc-Nat-Outside-Ip-Addr	DSM only. For a DSM UE, this attribute contains the IPv4 address of the UE after NAT.
26.6527.146	Alc-Wlan-APN-Name	This VSA contains the Access Point Name string as signaled in incoming GTP-C messages for a GTP access host. Inclusion of this attribute can be configured via **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute apn**.

Table 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.147	Alc-MsIsdn	This VSA includes the MSISDN (telephone number) as signaled in incoming GTP-C messages for a GTP access host. Inclusion of this attribute can be configured via **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute msisdn**.
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 is copied into the DHCP lease state and echoed by SR OS accounting.
26.6527.149	Alc-Num-Attached-UEs	Indicates the total number of UEs that are currently attached to the tunnel of the UE for which the accounting message is generated. In an accounting stop message this counter includes the UE for which the accounting stop is generated, even if the UE is being removed. Therefore the reported counter can only be zero for non-wlan-gw/ vRGW UEs. Inclusion can be configured with the option wifi-num-attached-ues. For ESM in **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute**, and for DSM in **configure aaa isa-radius-policy** *name* **acct-include-attributes**.
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 (the line is idle) or SILENT (the line is silent). Attribute is included/excluded based on **configure subscriber-mgmt 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**.
26.6527.184	Alc-Wlan-Ue-Creation-Type	DSM only. Indicates if the UE is either an ESM host (IOM) or DSM host (ISA). Fixed to ISA in case of DSM.
26.6527.191	Alc-ToServer-Dhcp6-Options	DSM only. If IA-NA is active, the attribute contains the options sent by the client in the last DHCPv6 transaction. Inclusion of this attribute is enabled via **configure aaa isa-radius-policy** *policy-name* **acct-include-attributes dhcp6-options**.

Table 69 **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 (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 (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 (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 (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 69 **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**).
26.6527.206	Alc-Wlan-SSID-VLAN	On a WLAN-GW group interface this attribute indicates the UE VLAN tag inside of the tunnel. This VLAN is usually used to differentiate between SSIDs. If no VLAN is present or the host is not active on a wlan-gw-group interface this attribute is not sent. (**configure subscriber-mgmt radius-accounting-policy** *name* **include- radius-attribute wifi-ssid-vlan**).
26.6527.226	Alc-Error-Code	The [26.6527.226] Alc-Error-Code and [26.6527.227] Alc-Error-Message attributes specify the reason why a subscriber session has ended. Each numeric Alc-Error-Code corresponds with a human readable Alc-Error-Message string. An overview of the Error Codes and their mapping to Termination Causes can be displayed with: **tools dump aaa radius-acct-terminate-cause** Included with following CLI: **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute alc-error-code**.
26.6527.227	Alc-Error-Message	The [26.6527.226] Alc-Error-Code and [26.6527.227] Alc-Error-Message attributes specify the reason why a subscriber session has ended. Each numeric Alc-Error-Code corresponds with a human readable Alc-Error-Message string. An overview of the Error Codes and their mapping to Termination Causes can be displayed with: **tools dump aaa radius-acct-terminate-cause** Included with following CLI: **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute alc-error-code**.
26.6527.228	Alc-Trigger-Acct-Interim	This attribute, when received in a CoA message, triggers an accounting interim update message for accounting modes that have interim-updates enabled. The Alc-Trigger-Acct-Interim attribute with free formatted string value is echoed in the CoA triggered accounting interim update message. The [26.6527.163] Alc-Acct-Triggered-Reason attribute in the interim update is set to 18 (CoA-Triggered).

Table 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.230	Alc-Acct-O-Exprof-Octets_64	Policer-specific counter. Indicates how many policer egress-exceed-profile-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.
26.6527.231	Alc-Acct-O-Exprof-Packets_64	Policer-specific counter. Indicates how many policer egress-exceed-profile-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.
26.6527.239	Alc-BRG-Num-Active-Sessions	This attribute applies to vRGW only. Indicates the total number of device sessions that are active (such as, DHCP completed) and linked to the related BRG instance. In accounting stop messages, this counter includes the session related to this accounting stop, even if the session is being removed. Inclusion for ESM can be configured with **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute brg-num-active-sessions**.
26.6527.240	Alc-Nat-Port-Range-Freed	This attribute contains information about the released NAT resources after a NAT policy change triggered via CoA in L2-Aware NAT.
241.26.6527.9	Alc-Bridge-Id	This attribute applies to vRGW only. The attribute contains the bridge domain id for the subscribers Home LAN Extension (HLE) service.
241.26.6527.10	Alc-Vxlan-VNI	This attribute applies to vRGW only. The attribute contains the VXLAN Network Identifier (VNI) used for egress VXLAN packets of the Home LAN Extension (HLE) service.
241.26.6527.14	Alc-RT	This attribute applies to vRGW only. The attribute contains the Route Target of the Home LAN Extension (HLE) BGP EVPN service.
241.26.6527.15	Alc-RD	This attribute applies to vRGW only. The attribute contains the Route Distinguisher of the Home LAN Extension (HLE) BGP EVPN service.
241.26.6527.19	Alc-Bonding-Id	This attribute indicates the connection is part of a bonding context. If the bonding-id is equal to the subscriber-id this indicates the bonding subscriber, else it is one of the access connections. Inclusion of this attribute can be configured via **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute bonding-id**.

Table 69 **Enhanced Subscriber Management Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
241.26.6527.23	Alc-Bonding-Active-Connection	This attribute indicates which connections are active in a bonding subscriber. Inclusion of this attribute can be configured via **configure subscriber-mgmt radius-accounting-policy** name **include-radius-attribute active-connections**.
241.26.6527.25	Alc-Steering-Profile	This attribute contains the name of the steering profile that is attached to the L2TP LAC session. The attribute is included in Start, Interim-Update and Stop messages when a steering profile is attached and when enabled in configuration with **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute steering-profile**.
241.26.6527.28	Alc-HLE-Device-Type	Indicate the type of Home LAN Extension host. Value is fixed to "Device in the home".
241.26.6527.36	Alc-Bonding-Load-Balance-Stats	This attribute indicates how many subscriber egress packets/octets have been sent towards each access connection due to load balancing. Note that the access connection can still drop packets as a result of its own QoS enforcement and therefore have a lower forwarded count. Inclusion of this attribute is subject to **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute detailed-acct-attributes**.
241.26.6527.48	Alc-Firewall-Info	Provides the firewall policy and associated outside service used by the subscriber to which this VSA relates. Inclusion of this attribute can be configured via **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute firewall-info**.
26.10415.20	3GPP-IMEISV	This VSA includes the International Mobile Equipment Identity and Software Version as signaled in incoming GTP-C messages. Inclusion of this attribute can be configured via **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute imei**.
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 is copied into the DHCP lease state and echoed by the SR OS accounting.

Table 70 **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 to 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 70 **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	Up to 6 attributes. Max. value length for each attribute is 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 WLAN-GW: AP-MAC and SSID, separated by a colon For example: Called-Station-Id = 00:00:01:00:00:01:my_ssid
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

Table 70 **Enhanced Subscriber Management Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
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
44	Acct-Session-Id	string	22 bytes (number format) max. 253 bytes (description format) 29 bytes (DSM format)	Internal generated 22 byte string (number format): Acct-Session-Id = 241AFF0000003250B5F750 DSM: Acct-Session-Id = 01-02-00-00-00-19-00-00-00-01
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 (DSM) 42949672 seconds (ESM)	The attribute value wraps after approximately 497 days (ESM): 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

Table 70 **Enhanced Subscriber Management Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
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) 253 bytes (description format) 29 bytes (DSM format)	Internal generated 22 byte string (number format): Acct-Multi-Session-Id = 241AFF0000003250B5F750 DSM: Acct-Multi-Session-Id = 01-02-00-00-00-19-00-00-5b-d9
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
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 to 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)
64	Tunnel-Type	integer	3 (mandatory value)	3 = L2TP For example: Tunnel-Type = 3
65	Tunnel-Medium-Type	integer	1 (mandatory value)	1 = IP or IPv4 For example: Tunnel-Medium-Type = 1
66	Tunnel-Client-Endpoint	string	Max. 19 bytes (untagged)	<dotted-decimal IP address used on LAC as L2TP src-ip> For example: Tunnel-Client-Endpoint = "1.1.1.1"

Table 70 **Enhanced Subscriber Management Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
67	Tunnel-Server-Endpoint	string	Max. 19 bytes (untagged)	<dotted-decimal IP address used on LAC as L2TP dst-ip> For example: Tunnel-Server-Endpoint = "2.2.2.2"
68	Acct-Tunnel-Connection	string	253 chars	By default, the Call Serial Number is inserted. Configured format: (if the resulting string is longer than 253 characters, it is truncated) **acct-tunnel-connection-fmt** *ascii-spec* <ascii-spec> : <char-specification> <ascii-spec> <char-specification> : <ascii-char> | <char-origin> <ascii-char> : a printable ASCII character <char-origin> : %<origin> <origin> : n | s | S | t | T | c | C n - Call Serial Number s | S - Local (s) or Remote (S) Session Id t | T - Local (t) or Remote (T) Tunnel Id c | C - Local (c) or Remote (C) Connection Id

Table 70 **Enhanced Subscriber Management Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
87	NAS-Port-Id	string	253 bytes	<prefix> : optional string 8 chars max <suffix> : optional string containing remote-id (max 64 chars) or circuit-id (max 64 chars) # IPoE/PPPoE: "<prefix><space><slot>/<mda>/<port>/ <vlan>.<vlan><space><suffix> # ATM : <prefix><space><slot>/<mda>/<port>/ <vpi>.<vci><space><suffix>" For example: NAS-Port-Id = "1/1/4:501.1001" # 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 = "LNS rtr-2#lip-3.3.3.3#rip-1.1.1.1#ltid-11381#rtid-1285#lsid-30067#rsid-19151#347" # WLAN-GW: GRE or L2TPv3: "<tunnel-type> rtr-<virtual router id>#lip-<local ip address>#rip-<remote ip address>" VLAN: "VLAN svc-<svc-id>[:<vlan>[.<vlan>]]" For example: NAS-Port-Id = "GRE rtr-11#lip-50.1.1.1#rip-201.1.1.2"
90	Tunnel-Client-Auth-ID	string	64 chars	For example: Tunnel-Client-Auth-Id:0 = "LAC-1"
91	Tunnel-Server-Auth-ID	string	64 chars	For example: Tunnel-Server-Auth-Id:0 = "LNS-1"
95	NAS-IPv6-Address	ipv6addr	16 bytes	# ipv6-address For example: NAS-IPv6-Address = 2001:db8::1

Table 70 **Enhanced Subscriber Management Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
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
99	Framed-IPv6-Route	string	max. 17 Framed-IPv6-Route attributes (16 managed routes and 1 DHCPv6 IA-PD host as managed route)	<ip-prefix>/<prefix-length> <space> :: <space> <metric> [<space> tag <space> <tag-value>] <space> pref <space> <preference-value> [<space>type pd-host] The gateway address is always reported as "::", representing the wan host ip. For DHCPv6 IA-PD hosts modeled as a managed route, the key word "**type pd-host**" is appended to the Framed-IPv6-Route attribute. For example: Framed-IPv6-Route = "2001:db8:1::/56 :: 0 pref 0" corresponds with a managed route with default metrics (metric=0, no tag, preference=0) Framed-IPv6-Route = "2001:db8:1::/56 :: 10 tag 3 pref 100" corresponds with a managed route with metric=10, tag=3 and preference=100 Framed-IPv6-Route = "2001:db8:d2:10::/56 :: 0 pref 0 type pd-host" corresponds with a PD host modeled as managed route
123	Delegated-IPv6-Prefix	ipv6prefix	max. 16 bytes for prefix + 1 byte for length	<ipv6-prefix/prefix-length> with prefix-length [48 to 64] For example: Delegated-IPv6-Prefix 2001:DB8:173A:100::/56

Table 70 **Enhanced Subscriber Management Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
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 b/s	For example: # 1Mb/s Actual-Data-Rate-Upstream = 1000000
26.3561.130	Actual-Data-Rate-Downstream	integer	4294967295 b/s	For example: # 5Mb/s Actual-Data-Rate-Downstream = 5000000
26.3561.131	Minimum-Data-Rate-Upstream	integer	4294967295 b/s	For example: Minimum-Data-Rate-Upstream = 1000
26.3561.132	Minimum-Data-Rate-Downstream	integer	4294967295 b/s	For example: Minimum-Data-Rate-Downstream = 1000
26.3561.133	Attainable-Data-Rate-Upstream	integer	4294967295 b/s	For example: Attainable-Data-Rate-Downstream = 1000
26.3561.134	Attainable-Data-Rate-Downstream	integer	4294967295 b/s	For example: Minimum-Data-Rate-Upstream = 1000
26.3561.135	Maximum-Data-Rate-Upstream	integer	4294967295 b/s	For example: Maximum-Data-Rate-Upstream = 1000
26.3561.136	Maximum-Data-Rate-Downstream	integer	4294967295 b/s	For example: Maximum-Data-Rate-Downstream = 1000
26.3561.137	Minimum-Data-Rate-Upstream-Low-Power	integer	4294967295 b/s	For example: Minimum-Data-Rate-Upstream-Low-Power = 1000
26.3561.138	Minimum-Data-Rate-Downstream-Low-Power	integer	4294967295 b/s	For example: Minimum-Data-Rate-Downstream-Low-Power = 1000

Table 70 **Enhanced Subscriber Management Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
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 without FCS(6), Ethernet over AAL5 Null w FCS(7), Ethernet over AAL5 Null without 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
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

Table 70 **Enhanced Subscriber Management Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.19	Alc-Acct-I-Inprof-Octets-64	octets	10 bytes/ attribute with 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 to 32> For example: # 500 bytes in profile traffic for ingress queue 2 Alc-Acct-I-Inprof-Octets-64 = 0x0002000000000000001f4 # 1000 bytes in profile traffic for ingress policer 3 Alc-Acct-I-Inprof-Octets-64 = 0x80030000000000003e8
26.6527.20	Alc-Acct-I-Outprof-Octets-64	octets	10 bytes/ attribute with 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 to 32> For example: # 500 bytes out of profile traffic for ingress queue 2 Alc-Acct-I-Outprof-Octets-64 = 0x0002000000000000001f4 # 1000 bytes out of profile traffic for ingress policer 3 Alc-Acct-I-Outprof-Octets-64 = 0x80030000000000003e8
26.6527.21	Alc-Acct-O-Inprof-Octets-64	octets	10 bytes/ attribute with 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 range <1 to 8> or Policer-id range <1 to 63> For example: # 500 bytes in profile traffic for egress queue 2 Alc-Acct-O-Inprof-Octets-64 = 0x0002000000000000001f4 # 1000 bytes in profile traffic for egress policer 3 Alc-Acct-O-Inprof-Octets-64 = 0x80030000000000003e8

Table 70 **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 with 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 range <1 to 8> or Policer-id range <1 to 63> For example: # 500 bytes out of profile traffic for egress queue 2 Alc-Acct-O-Outprof-Octets-64 = 0x00020000000000001f4 # 1000 bytes out of profile traffic for egress policer 3 Alc-Acct-O-Outprof-Octets-64 = 0x800300000000000003e8
26.6527.23	Alc-Acct-I-Inprof-Pkts-64	octets	10 bytes/ attribute with 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 to 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 with 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 to 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

Table 70 **Enhanced Subscriber Management Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.25	Alc-Acct-O-Inprof-Pkts-64	octets	10 bytes/ attribute with 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 range <1 to 8> or Policer-id range <1 to 63> 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
26.6527.26	Alc-Acct-O-Outprof-Pkts-64	octets	10 bytes/ attribute with 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 range <1 to 8> or Policer-id range <1 to 63> For example: # 500 packets out profile traffic for egress queue 2 Alc-Acct-O-Outprof-Pkts-64 = 0x00020000000000001f4 # 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
26.6527.36	Alc-DHCP-Vendor-Class-Id	string	247 chars	For example: Alc-DHCP-Vendor-Class-Id = My-DHCP-VendorClassId
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 = 0x00020000000000001f4
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 = 0x000100000000000000aea

Table 70 **Enhanced Subscriber Management Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.69	Alc-Acct-I-High-Octets-Drop_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1 to 32> For example: INPUT_HIGH_OCTETS_DROP_64 [69] 10 0x0001000000000000000
26.6527.70	Alc-Acct-I-Low-Octets-Drop_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1 to 32> For example: INPUT_LOW_OCTETS_DROP_64 [70] 10 0x0001000000000000000
26.6527.71	Alc-Acct-I-High-Pack-Drop_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1 to 32> For example: INPUT_HIGH_PACK_DROP_64 [71] 10 0x0001000000000000000
26.6527.72	Alc-Acct-I-Low-Pack-Drop_64	octets	10 bytes	<Queue-id 2Bytes><8 Bytes value> where Queue-id range <1 to 32> For example: INPUT_LOW_PACK_DROP_64 [72] 10 0x0001000000000000000
26.6527.73	Alc-Acct-I-High-Octets-Offer_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1 to 32> For example: INPUT_HIGH_OCTETS_OFFER_64 [73] 10 0x0001000000000000000
26.6527.74	Alc-Acct-I-Low-Octets-Offer_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1 to 32> For example: INPUT_LOW_OCTETS_OFFER_64 [74] 10 0x0001000000000000000
26.6527.75	Alc-Acct-I-High-Pack-Offer_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1 to 32> For example: INPUT_HIGH_PACK_OFFER_64 [75] 10 0x0001000000000000000

Table 70 **Enhanced Subscriber Management Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.76	Alc-Acct-I-Low-Pack-Offer_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1 to 32> For example: INPUT_LOW_PACK_OFFER_64 [76] 10 0x0001000000000000000
26.6527.77	Alc-Acct-I-Unc-Octets-Offer_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1 to 32> For example: INPUT_UNC_OCTETS_OFFER_64 [77] 10 0x0001000000000000000
26.6527.78	Alc-Acct-I-Unc-Pack-Offer_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1 to 32> For example: INPUT_UNC_PACK_OFFER_64 [78] 10 0x0001000000000000000
26.6527.81	Alc-Acct-O-Inprof-Pack-Drop_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1 to 8> For example: OUTPUT_INPROF_PACK_DROP_64 [81] 10 0x0001000000000000000
26.6527.82	Alc-Acct-O-Outprof-Pack-Drop_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1 to 8> For example: OUTPUT_OUTPROF_PACK_DROP_64 [82] 10 0x0001000000000000000
26.6527.83	Alc-Acct-O-Inprof-Octs-Drop_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1 to 8> For example: OUTPUT_INPROF_OCTS_DROP_64 [83] 10 0x0001000000000000000
26.6527.84	Alc-Acct-O-Outprof-Octs-Drop_64	octets	10 bytes	<Queue-id 2Bytes><8 Byte value> where Queue-id range <1 to 8> For example: OUTPUT_OUTPROF_OCTS_DROP_64 [84] 10 0x0001000000000000000
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

Table 70 **Enhanced Subscriber Management Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
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 = 0x00070000000000307b4
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 = 0x00010000000000143fa
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
26.6527.100	Alc-Serv-Id	integer	2147483647 id	DSM only. For example: Alc-Serv-Id = 100
26.6527.102	Alc-ToServer-Dhcp-Options	octets	multiple attributes 247 bytes / attribute	DSM only. For example: DHCPv4 Discover with three options: Class-identifier-option (60) = DHCP-VendorClassId, Agent-Circuit-Id (82-1) = circuit10 Agent-Remote-Id (82-2) = remote10 Alc-ToServer-Dhcp-Options = 350101 Alc-ToServer-Dhcp-Options = 3c12444843502d56656e646f72436c6173734964 Alc-ToServer-Dhcp-Options = 52150109636972637569743130020872656d6f74653130
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 | Policer-id range <1 to 63> 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 70 **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 to 63> 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 to 63> 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 to 63> 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 to 63> 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 to 63> 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 to 63> 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 to 63> For example: # egress policer 1 OUTPUT_HIPRIO_PACKETS_64 [114] 10 0x80010000000000000000

Table 70 **Enhanced Subscriber Management Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.115	Alc-Acct-O-Lowprio-Packets_64	octets	10 bytes	<0x80><policer-id><8 byte value> where policer-id <1 to 63> For example: # egress policer 1 OUTPUT_LOWPRIO_PACKETS_64 [115] 10 0x80010000000000000000
26.6527.116	Alc-Acct-I-All-Octets_64	octets	10 bytes	<0x80><policer-id><8 byte value> where policer-id <1 to 63> 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 to 63> 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 to 63> 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 to 63> 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> <space> <nat-policy-name> For example: a public pool address 180.0.1.248; port-range [37674..37723] in Base with nat-policy-name = nat-pol-1 Alc-Nat-Port-Range = "180.0.1.248 37674-37723 router base nat-pol-1"

Table 70 **Enhanced Subscriber Management Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
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 range <1 to 8> or Policer-id range <1 to 63> 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
26.6527.140	Alc-Nat-Outside-Serv-Id	integer	2147483647 id	DSM only. For example: Alc-Nat-Outside-Serv-Id = 300
26.6527.141	Alc-Nat-Outside-Ip-Addr	ipaddr	4 bytes	DSM only. For example: Alc-Nat-Outside-Ip-Addr = 21.0.0.113
26.6527.146	Alc-Wlan-APN-Name	string	247 chars	The APN is directly reflected as present in the incoming GTP-C message. For example: Alc-Wlan-APN-Name = demo.mnc001.mcc001.gprs
26.6527.147	Alc-MsIsdn	string	9 to 15 digits	Textual representation of the MSISDN in decimal format. 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	A number indicating how many UEs are active. For example: Alc-Num-Attached-Ues = 1
26.6527.163	Alc-Acct-Triggered-Reason	integer	4 bytes	See Table 92 for a description of Accounting Triggered Reason values. 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

Table 70 **Enhanced Subscriber Management Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
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
26.6527.184	Alc-Wlan-Ue-Creation-Type	integer	values [0 to 1]	DSM only. Value in case of DSM is fixed to isa (1) For example: Alc-Wlan-Ue-Creation-Type = isa
26.6527.191	Alc-ToServer-Dhcp6-Options	octets	Multiple attributes 247 bytes / attribute (truncated if DHCPv6 option is longer)	DSM only. One DHCPv6 option per RADIUS attribute. In case of DHCPv6 relay or LDRA this reflects the options as they appear in the outer packet. For example: an LDRA message with following options: • Interface-Id = 00:00:00:00:00:05;1;0 • Remote Identifier = alu00:02:00:00:00:19 • Relay-Message containing: – Client Identifier – Server Identifier – IA_NA (4ffd:100:2::1) – Elapsed Time – Option Request Options Results in three attributes: Alc-ToServer-Dhcp6-Options= 0012001530303a30303a30303a30303a30303a30353b313b6f Alc-ToServer-Dhcp6-Options= 002500180000197f616c7530303a30323a30303a30303a30303a3139 Alc-ToServer-Dhcp6-Options= 0009006003e115820001000a000300010002000000190002000a000300010812ff0000000003002c0000000100000708000000b40000500184ffd010000020000000000000000000100000e1000000e10000000000080002000000060006000100020003

Table 70 **Enhanced Subscriber Management Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
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
26.6527.206	Alc-Wlan-SSID-VLAN	string	247 chars	Textual representation of the VLAN. If no vlan-tag was present this attribute will not be included. For example: Alc-Wlan-SSID-VLAN = “2173”
26.6527.226	Alc-Error-Code	integer	4 bytes	For example: Alc-Error-Code = 202
26.6527.227	Alc-Error-Message	string	247 chars	For example: Alc-Error-Message = "Service cleared by operator"
26.6527.228	Alc-Trigger-Acct-Interim	string	247 chars	Free formatted string that is echoed in the triggered interim update message. For example: Alc-Trigger-Acct-Interim = "CoA - Filter update"
26.6527.230	Alc-Acct-O-Exprof-Octets_64	octets	10 bytes	<0x80><policer-id><8 byte value> where policer-id <1..63> For example: # egress policer 1 OUTPUT EXCEEDPROF OCTETS 64 [230] 10 0x80010000000000000000

Table 70 **Enhanced Subscriber Management Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.231	Alc-Acct-O-Exprof-Packets_64	octets	10 bytes	<0x80><policer-id><8 byte value> where policer-id <1..63> For example: # egress policer 1 OUTPUT EXCEEDPROF PACKETS 64 [231] 10 0x80010000000000000000
26.6527.239	Alc-BRG-Num-Active-Sessions	integer	32 bits value	A counter indicating how many sessions are connected. For example: Alc-Brg-Num-Active-Sessions = 3
26.6527.240	Alc-Nat-Port-Range-Freed	string	No limits	<public-ip> <space> <port- range> <space> <outside-routing-instance> <space> <nat-policy-name> For example: a public pool with address 180.0.1.248; port-range [37674..37723] in Base, nat-policy name nat-pol-1 Alc-Nat-Port-Range = "180.0.1.248 37674-37723 router base nat-pol-1"
241.26.6527.9	Alc-Bridge-Id	integer	1 - 4294967294	For example: Alc-Bridge-Id = 200
241.26.6527.10	Alc-Vxlan-VNI	integer	1 - 16777214	For example: Alc-Vxlan-VNI =250
241.26.6527.14	Alc-RT	string	SROS supported format	• target:<ip-addr:comm-val> • target:<2byte-asnumber:ext-comm-val> • target:<4byte-asnumber:comm-val> For example: Alc-Steering-Profile = “steering-profile-1”
241.26.6527.15	Alc-RD	string	SROS supported format	One of the following formats: • <ip-addr:comm-val> • <2byte-asnumber:ext-comm-val> • <4byte-asnumber:comm-val> For example: Alc-RD = “64496:510”
241.26.6527.19	Alc-Bonding-Id	string	1..32 chars	ID used to identify the bonding context. For example: Alc-Bonding-Id=home1

Table 70 **Enhanced Subscriber Management Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
241.26.6527.23	Alc-Bonding-Active-Connection	integer	[1..2]	ID used to identify the connection. Included for each connection active. For example: Connection 1 and 2 active Alc-Active-Connection+=1 Alc-Active-Connection+=2
241.26.6527.25	Alc-Steering-Profile	string	32 chars	Steering profile name. For example: Alc-Steering-Profile = “steering-profile-1”
241.26.6527.28	Alc-HLE-Device-Type	integer	1	Value: 1 = Device in the home For example: Alc-HLE-Device-Type = 1
241.26.6527.36	Alc-Bonding-Load-Balance-Stats	octets	10 bytes per attribute	First byte indicates which data is reported: 0x01 = egress packets 0x02 = egress octets Second byte indicates the connection ID. Remaining 8 bytes indicate the value as a 64-bit integer. For example: 100 packets totaling 40000B over connection 1, 50 packets totaling 30000B over connection 2 Alc-Bonding-Load-Balance-Stats += 0x0101000000000000064 Alc-Bonding-Load-Balance-Stats += 0x0102000000000000032 Alc-Bonding-Load-Balance-Stats += 0x02010000000000009c40 Alc-Bonding-Load-Balance-Stats += 0x02020000000000007530
241.26.6527.48	Alc-Firewall-Info	string	247 char	<service> <space> <firewall-policy-name> For example: a firewall-policy fw-pol-1 active in the base router: Alc-Firewall-Info = "router base fw-pol-1" For example: A firewall-policy fw-pppoe active in epipe 20: Alc-Firewall-Info = "pppoe-service-id 20 fw-pppoe"
26.10415.20	3GPP-IMEISV	string	14 to 16 digits	3GPP vendor specific attribute as defined in TS 29.061

Table 70 **Enhanced Subscriber Management Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.25053.2	Ruckus-Sta-RSSI	integer	32 bits value	For example: Ruckus-Sta-RSSI = 28

Table 71 **Enhanced Subscriber Management Accounting (Applicability)**

Attribute ID	Attribute Name	Acct Start	Acct Stop	Acct Interim-Update	Acct On [1]	Acct Off [1]	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+	0+	0+	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

Table 71 **Enhanced Subscriber Management Accounting (Applicability) (Continued)**

Attribute ID	Attribute Name	Acct Start	Acct Stop	Acct Interim-Update	Acct On [1]	Acct Off [1]	Acct Reporting Level
46	Acct-Session-Time	0	0-1	0-1	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
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
64	Tunnel-Type	0-1 [2]	0-1	0-1	0	0	HSQ
65	Tunnel-Medium-Type	0-1 [2]	0-1	0-1	0	0	HSQ
66	Tunnel-Client-Endpoint	0-1 [2]	0-1	0-1	0	0	HSQ
67	Tunnel-Server-Endpoint	0-1 [2]	0-1	0-1	0	0	HSQ
68	Acct-Tunnel-Connection	0-1 [2]	0-1	0-1	0	0	HSQ
87	NAS-Port-Id	0-1	0-1	0-1	0	0	H->S->Q
90	Tunnel-Client-Auth-ID	0-1 [2]	0-1	0-1	0	0	HSQ
91	Tunnel-Server-Auth-ID	0-1 [2]	0-1	0-1	0	0	HSQ
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

Table 71 **Enhanced Subscriber Management Accounting (Applicability) (Continued)**

Attribute ID	Attribute Name	Acct Start	Acct Stop	Acct Interim-Update	Acct On [1]	Acct Off [1]	Acct Reporting Level
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
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

Table 71 **Enhanced Subscriber Management Accounting (Applicability) (Continued)**

Attribute ID	Attribute Name	Acct Start	Acct Stop	Acct Interim-Update	Acct On [1]	Acct Off [1]	Acct Reporting Level
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
26.6527.36	Alc-DHCP-Vendor-Class-Id	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
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

Table 71 **Enhanced Subscriber Management Accounting (Applicability) (Continued)**

Attribute ID	Attribute Name	Acct Start	Acct Stop	Acct Interim-Update	Acct On [1]	Acct Off [1]	Acct Reporting Level
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
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

Table 71 **Enhanced Subscriber Management Accounting (Applicability) (Continued)**

Attribute ID	Attribute Name	Acct Start	Acct Stop	Acct Interim-Update	Acct On [1]	Acct Off [1]	Acct Reporting Level
26.6527.119	Alc-Acct-O-All-Packets_64	0	0+	0+	0	0	HSQ
26.6527.121	Alc-Nat-Port-Range	0+	0+	0+	0	0	HSQ
26.6527.127	Alc-Acct-O-statmode	0	0+	0+	0	0	HSQ
26.6527.146	Alc-Wlan-APN-Name	0-1	0-1	0-1	0	0	SQ
26.6527.147	Alc-MsIsdn	0-1	0-1	0-1	0	0	SQ
26.6527.148	Alc-RSSI	0-1	0-1	0-1	0	0	HSQ
26.6527.149	Alc-Num-Attached-UEs	0-1	0-1	0-1	0	0	H->S->Q
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
26.6527.206	Alc-Wlan-SSID-VLAN	0-1	0-1	0-1	0	0	H->S->Q
26.6527.226	Alc-Error-Code	0	0-1	0	0	0	HSQ
26.6527.227	Alc-Error-Message	0	0-1	0	0	0	HSQ
26.6527.228	Alc-Trigger-Acct-Interim	0	0	0-1	0	0	HSQ
26.6527.230	Alc-Acct-O-Exprof-Octets_64	0	0+	0+	0	0	HSQ
26.6527.231	Alc-Acct-O-Exprof-Packets_64	0	0+	0+	0	0	HSQ
26.6527.239	Alc-BRG-Num-Active-Sessions	0-1	0-1	0-1	0	0	H->S->Q

Table 71 **Enhanced Subscriber Management Accounting (Applicability) (Continued)**

Attribute ID	Attribute Name	Acct Start	Acct Stop	Acct Interim-Update	Acct On [1]	Acct Off [1]	Acct Reporting Level
26.6527.240	Alc-Nat-Port-Range-Freed	0	0+	0+	0	0	HSQ
241.26.6527.9	Alc-Bridge-Id	0-1	0-1	0-1	0	0	H->S->Q
241.26.6527.10	Alc-Vxlan-VNI	0-1	0-1	0-1	0	0	H->S->Q
241.26.6527.14	Alc-RT	0-1	0-1	0-1	0	0	H->S->Q
241.26.6527.15	Alc-RD	0-1	0-1	0-1	0	0	H->S->Q
241.26.6527.19	Alc-Bonding-Id	0-1	0-1	0-1	0	0	H->S->Q
241.26.6527.23	Alc-Bonding-Active-Connection	0+	0	0+	0	0	H->S->Q
241.26.6527.25	Alc-Steering-Profile	0-1	0-1	0-1	0	0	HS
241.26.6527.28	Alc-HLE-Device-Type	0-1	0-1	0-1	0	0	H->S->Q
241.26.6527.36	Alc-Bonding-Load-Balance-Stats	0	0+	0+	0	0	H->S->Q
241.26.6527.48	Alc-Firewall-Info	0-1	0-1	0-1	0	0	HSQ
26.10415.20	3GPP-IMEISV	0-1	0-1	0-1	0	0	SQ
26.25053.2	Ruckus.Sta-RSSI	0-1	0-1	0-1	0	0	HSQ

Notes:

1. 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.
2. For L2TP LAC PPPoE sessions, when the Tunnel Client Attributes are included (**configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute tunnel-client-attrs**), the Accounting Start message for Session and Host accounting modes is delayed until all L2TP tunnel information is available. For Queue-Instance accounting mode, the Accounting Start is not delayed and the Tunnel Client Attributes will only be included in the next Accounting Interim Update or Accounting Stop message.

1.3.2 Distributed Subscriber Management (DSM) Accounting

In Distributed Subscriber Management (DSM), a single accounting session per UE is started. A unique Accounting-Session-ID per UE is generated. An Acct-Multi-Session-Id is also generated but currently not used to link any accounting sessions.

Acct-Status-Type and Acct-Session-Id are always included by default. The presence of all other attributes is dictated by configuration (**config>aaa>isa-radius-policy** *name* **acct-include-attributes**). Unless otherwise stated in a note, the attribute description and limits are the same as for Enhanced Subscriber Management (ESM) Accounting (Table 69 and Table 70), Table 72 provides an overview of the applicability of the attributes in DSM accounting messages.

Accounting On and Accounting Off messages are generated when a server is enabled or disabled in an **isa-radius-policy** (**config>aaa>isa-radius-policy** *name* **servers** *id*>[**no**] **shutdown**). An accounting-On will also be generated every 5 minutes for a RADIUS server that is unresponsive.

Table 72 **Distributed Subscriber Management 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
5	NAS-Port	0-1	0-1	0-1	1	1
8	Framed-IP-Address	0-1	0-1	0-1	0	0
9	Framed-IP-Netmask	0-1	0-1	0-1	0	0
25	Class	0+	0+	0+	0	0
30	Called-Station-Id	0-1	0-1	0-1	0-1	0-1
31	Calling-Station-Id	0-1	0-1	0-1	0	0
32	NAS-Identifier	0-1	0-1	0-1	0-1	0-1
40	Acct-Status-Type	1	1	1	1	1
41	Acct-Delay-Time	0-1	0-1	0-1	0	0
42	Acct-Input-Octets	0-1	0-1	0-1	0	0
43	Acct-Output-Octets	0-1	0-1	0-1	0	0
44	Acct-Session-Id	1	1	1	1	1

Table 72 **Distributed Subscriber Management Accounting (Applicability) (Continued)**

Attribute ID	Attribute Name	Acct Start	Acct Stop	Acct Interim-Update	Acct On (*)	Acct Off (*)
46	Acct-Session-Time	0-1	0-1	0-1	0-1	0-1
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	0-1	0	0
52	Acct-Input-Gigawords	0-1	0-1	0-1	0	0
53	Acct-Output-Gigawords	0-1	0-1	0-1	0	0
55	Event-Timestamp	0-1	0-1	0-1	0-1	0-1
61	NAS-Port-Type	0-1	0-1	0-1	0	0
87	NAS-Port-Id	0-1	0-1	0-1	0	0
97	Framed-IPv6-Prefix	0-1	0-1	0-1	0	0
26.3561.1	Agent-Circuit-Id	0-1	0-1	0-1	0	0
26.3561.2	Agent-Remote-Id	0-1	0-1	0-1	0	0
26.6527.11	Alc-Subsc-ID-Str	0-1	0-1	0-1	0	0
26.6527.19	Alc-Acct-I-Inprof-Octets-64 [1]	0	0-1	0-1	0	0
26.6527.21	Alc-Acct-O-Inprof-Octets-64 [1]	0	0-1	0-1	0	0
26.6527.23	Alc-Acct-I-Inprof-Pkts-64 [1]	0	0-1	0-1	0	0
26.6527.25	Alc-Acct-O-Inprof-Pkts-64 [1]	0	0-1	0-1	0	0
26.6527.27	Alc-Client-Hardware-Addr	0-1	0-1	0-1	0	0
26.6527.36	Alc-DHCP-Vendor-Class-Id	0-1	0-1	0-1	0	0
26.6527.99	Alc-Ipv6-Address	0-1	0-1	0-1	0	0
26.6527.100	Alc-Serv-Id	0-1	0-1	0-1	0	0
26.6527.102	Alc-ToServer-Dhcp-Options	0+	0+	0+	0	0
26.6527.121	Alc-Nat-Port-Range	0+	0+	0+	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

Table 72 **Distributed Subscriber Management Accounting (Applicability) (Continued)**

Attribute ID	Attribute Name	Acct Start	Acct Stop	Acct Interim-Update	Acct On (*)	Acct Off (*)
26.6527.148	Alc-RSSI	0-1	0-1	0-1	0	0
26.6527.163	Alc-Acct-Triggered-Reason	0	0	0-1	0	0
26.6527.184	Alc-Wlan-Ue-Creation-Type	0-1	0-1	0-1	0	0
26.6527.191	Alc-ToServer-Dhcp6-Options	0-1	0-1	0-1	0	0
26.6527.206	Alc-Wlan-SSID-VLAN	0-1	0-1	0-1	0	0

Note:

1. The attributes are included for AA-sub stats when enabled via "**configure service vprn|ies** *service-id* **subscriber-interface** *ip-int-name* **group-interface** *ip-int-name* **wlan-gw vlan-tag-ranges range start** [*0..4096*] **end** [*0..4096*] **distributed-sub-mgmt collect-aa-acct-stats**" and explicitly included as "**configure aaa isa-radius-policy** *name* **acct-include-attributes**" with "**octet-counters**" for octet counter and "**frame-counters**" for packet counters. The description and limits are detailed in Table 82 and Table 83 in the Application Assurance (AA) Accounting section.

1.3.3 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 session accounting (Host accounting mode for IPoE host and Session accounting mode for PPPoE and IPoE sessions). Volume counters are always reported in standard attributes. Differences for attribute content and additional attributes are detailed in Table 73.

Table 73 **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.

Table 73 **Subscriber Service Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
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/IPoE 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/IPoE 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**}).
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 74 **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

Table 74 **Subscriber Service Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
44	Acct-Session-Id	string	22 bytes	For example: # Acct-Session-Id = 24ADFF0000000950C5F138 Acct-Session-Id 0x3231323834363335393231303235313231 3133343039
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
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 75 **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

Table 75 **Subscriber Service Accounting (Applicability) (Continued)**

Attribute ID	Attribute Name	Acct Start	Acct Stop	Acct Interim-Update
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

1.3.4 Large Scale NAT (LSN) Accounting

Table 76 **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 user's 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** *policy-name* **acct-include-attributes**. 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 to 0] that holds the MS-ISA MDA used for LSN accounting. The following formatting is used [3 bits 31 to 29 value 000], [4 bits 28 to 25 value slot-ms-isa], [4 bits 24 to 21 value mda-nbr-ms-isa], [6 bits 20 to 15 000010], [15 bits 14 to 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** *policy-name* **acct-include-attributes**.

Table 76 **LSN Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
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** *policy-name* **acct-include-attributes**.
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 radius-accounting-policy** (ESM accounting), **configure aaa isa-radius-policy** (LSN accounting, WLAN-GW) and **configure aaa l2tp-accounting-policy** (L2TP accounting).
42	Acct-Input-Octets	Indicates how many Layer 3 octets were sent to this NAT user over the course of this service being provided and sent 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** *policy-name* **acct-include-attributes**.
43	Acct-Output-Octets	Indicates how many Layer 3 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** *policy-name* **acct-include-attributes**.
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** *policy-name* **acct-include-attributes** 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** *policy-name* **acct-include-attributes** 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 a 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** *policy-name* **acct-include-attributes**.

Table 76 **LSN Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
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** *policy-name* **acct-include-attributes.**
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** *policy-name* **acct-include-attributes**.
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** *policy-name* **acct-include-attributes** 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 included under **configure aaa isa-radius-policy** *policy-name* **acct-include-attributes** 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** *policy-name* **acct-include-attributes**.
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** *policy-name* **acct-include-attributes**.
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** *policy-name* **acct-include-attributes**.

Table 76 **LSN Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
97	Framed-IPv6-Prefix	Inside private IPv6 address of the user (NAT64,DSLITE) and send when **framed-ipv6-prefix** is included under **configure aaa isa-radius-policy** *policy-name* **acct-include-attributes**.
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** *policy-name* **acct-include-attributes.** 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** *policy-name* **nat acct-include-attributes inside-service-id**). The outside VRF is reported via [26.6527.140] Alc-Nat-Outside-Serv-Id.
26.6527.121	Alc-Nat-Port-Range	This attribute is used to report allocated or released NAT resources in LSN. The reported NAT resources include a public IPv4 address, public port range(s), and outside routing instance. This attribute is included in accounting by configuring the **port-range-block** option under the **configure aaa isa-radius-policy** *policy-name* **acct-include-attributes** CLI hierarchy.
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** *policy-name* **acct-include-attributes**.
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** *policy-name* **acct-include-attributes**. The content of this attribute is identical to the outside IPv4 address in [26.6527.121] Alc-Nat-Port-Range.
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 included in LSN accounting only when **acct-include-attribute acct-trigger-reason** is enabled in the **isa-radius-policy**.

Table 77 **LSN 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 = 30302d30302d30302d30302d30312d30312d Called-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 77 **LSN 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

Table 77 **LSN Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
97	Framed-IPv6-Prefix	ipv6prefix	max. 16 bytes for prefix + 1 byte for length	private inside IPv6 address of NAT64 or DSlite user For example: Framed-IPv6-Prefix = 2001::1/128
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	VPRN service ID or 0 (zero) when inside service is the Base routing instance. For example: inside VPRN service 100: Alc-Serv-Id = 100
26.6527.121	Alc-Nat-Port-Range	string	no limits	<public-ip><space><port-range><space><outside-routing-instance> For example: a public pool address 180.0.1.248; port-range [37674 to 37723] in Base: Alc-Nat-Port-Range = “180.0.1.248 37674-37723 router base”
26.6527.140	Alc-Nat-Outside-Serv-Id	integer	2147483647 id	VPRN service ID or 0 (zero) when outside service is the Base routing instance. For example: outside VPRN service 200: Alc-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
26.6527.163	Alc-Acct-Triggered-Reason	integer	4 bytes	See Table 92 for a description of Accounting Triggered Reason values. For example: ACCT TRIGGERED INTERIM REASON [163] 4 Nat-Free (19)

Table 78 **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
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

Table 78 **LSN Accounting (Applicability) (Continued)**

Attribute ID	Attribute Name	Acct Start	Acct Stop	Acct Interim-Update	Acct On	Acct Off
26.6527.163	Alc-Acct-Triggered-Reason	0	0	0-1	0	0

1.3.5 L2TP Tunnel Accounting

Table 79 **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**.

Table 79 **L2TP Tunnel Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
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.
31	Calling-Station-Id	Includes the hostname and sap-id. Send when calling-station-id is included in **configure aaa l2tp-accounting-policy** *policy-name* **include-radius-attribute 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 aaa l2tp-accounting-policy** (L2TP accounting).
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 of the PPPoE session (**show service id** *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.

Table 79 **L2TP Tunnel Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
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.
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 i**nclude-radius-attribute nas-port-type** is added per application: **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 **configure subscriber-mgmt authentication-policy|radius-accounting-policy** *policy name* **include-radius-attribute tunnel-server-attrs** is enabled on LNS. For L2TP Tunnel/Link Accounting this attribute is always included on LAC and LNS.

Table 79 **L2TP Tunnel Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
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 **configure subscriber-mgmt authentication-policy|radius-accounting-policy** *policy name* **include-radius-attribute tunnel-server-attrs** is enabled on 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. Preconfigured 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 **configure subscriber-mgmt authentication-policy|radius-accounting-policy** *policy name* **include-radius-attribute tunnel-server-attrs** is enabled on 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.
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 (4 bytes) 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-ids (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. The default format of the attribute can be changed with **configure aaa l2tp-accounting-policy** *policy-name* **acct-tunnel-connection-fmt** *ascii-spec*.
82	Tunnel-Assignment-ID	Indicates to the tunnel initiator the particular tunnel to which a session is to be assigned. Some tunneling 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.

Table 79 **L2TP Tunnel Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
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 (8 characters maximum) and suffix-string (64 characters maximum) 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 or Accounting. This logical access circuit is a fixed concatenation (delimiter number) 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. Preconfigured 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 79 **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 80 **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 to 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) 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
31	Calling-Station-Id	string	253 chars	For example: Calling-Station-Id = "router-1 1/1/4:1200.10"
32	NAS-Identifier	string	32 chars	For example: NAS-Identifier = PE1-Antwerp

Table 80 **L2TP Tunnel Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
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 bytes 42949672 seconds	The attribute value wraps after approximately 497 days For example: Acct-Session-Time = 870
47	Acct-Input-Packets	integer	4 bytes 4294967295 packets	For example: Acct-Input-Packets = 213
48	Acct-Output-Packets	integer	4 bytes 4294967295 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

Table 80 **L2TP Tunnel Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
61	NAS-Port-Type	integer	4 bytes Values [0 to 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
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

Table 80 **L2TP Tunnel Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
68	Acct-Tunnel-Connection	string	[4|8] bytes	Default format: 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) Configured format: (if the resulting string is longer than 253 characters, it is truncated) **acct-tunnel-connection-fmt** *ascii-spec* <ascii-spec> : <char-specification> <ascii-spec> <char-specification> : <ascii-char>|<char-origin> <ascii-char> : a printable ASCII character <char-origin> : %<origin> <origin> : n | s | S | t | T | c | C n - Call Serial Number s | S - Local (s) or Remote (S) Session Id t | T - Local (t) or Remote (T) Tunnel Id c | C - Local (c) or Remote (C) Connection Id
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 81 **L2TP Tunnel Accounting (Applicability)**

Attribute 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
31	Calling-Station-Id	0-1	0-1	0-1	0-1	0-1	0-1
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

Table 81 **L2TP Tunnel Accounting (Applicability) (Continued)**

Attribute ID	Attribute Name	Acct Tunnel-Start	Acct Tunnel-Stop	Acct Tunnel-Reject	Acct Tunnel-Link-Start	Acct Tunnel-Link-Stop	Acct Tunnel-Link-Reject
68	Acct-Tunnel-Connection	1	1	1	1	1	0
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

1.3.6 Application Assurance (AA) Accounting

Table 82 **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.
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.

Table 82 **Application Assurance Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
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 is 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	The 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 due 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 the RADIUS accounting policy).
49	Acct-Terminate-Cause	Indicates how the session was terminated.
55	Event-Timestamp	Records 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. If Application Assurance per subscriber MAC is enabled, then the MAC address is appended, with a '-' as a separator between sub id and MAC. If the sub id is more than 19 characters, it's truncated to 19 characters and '+' is used as a separator between the sub id and MAC to indicate truncation.

Table 82 **Application Assurance Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
26.6527.19	Alc-Acct-I-Inprof-Octets-64	Identifies a charging group, app-group, application or sub-aggregate and its corresponding total from-sub admitted bytes. Reports cumulative volume of preconfigured AA-subscriber charging group, app-group or application since the start of the session (as described in RFC 2689) in Acct Interim Update or Stop messages.
26.6527.21	Alc-Acct-O-Inprof-Octets-64	Identifies a charging group, app-group, application or sub-aggregate and its corresponding total to-sub admitted bytes. Reports cumulative volume of preconfigured AA-subscriber charging group, app-group or application since the start of the session (as described in RFC 2689) in Acct Interim Update or Acct Stop messages.
26.6527.23	Alc-Acct-I-Inprof-Pkts-64	Identifies a charging group, app-group or application and its corresponding total from-sub admitted packets. Reports cumulative volume of preconfigured AA-subscriber charging group, app-group or application since the start of the session (as described in RFC 2689) in Acct Interim Update or Acct Stop messages.
26.6527.25	Alc-Acct-O-Inprof-Pkts-64	Identifies a charging group, app-group or application and its corresponding total to-sub admitted packets. Reports cumulative volume of preconfigured AA-subscriber charging group, app-group or application since the start of the session (as described in RFC 2689) in Acct Interim Update or Acct Stop messages.
26.6527.45	Alc-App-Prof-Str	Designates 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	Designates 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 (removal of routing asymmetry when using redundant transit-aa-nodes), for example, having two redundant transit 7750 SR nodes, PCRF(DSC) pushes a CoA create message to both 7750 SR nodes. This is achieved by adding the peer-identifier information in the original Accounting-start sent by the primary 7750 SR.

Table 83 **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, esm-mac 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	32 char	<aa-subscriber text name> For example: Scope = subscriber: Alc-Subsc-ID-Str = ipoe_sub_08 Scope = mac Alc-Subsc-ID-Str = ipoe_sub_08-000102030405 Scope = mac, with subId = "ipoe_sub_012345678901234" truncated to 19 chars: Alc-Subsc-ID-Str = ipoe_sub_0123456789+000102030405

Table 83 **Application Assurance Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.19	Alc-Acct-I-Inprof-Octets-64	octets	10 bytes	<Type of second byte 1 Byte><export-id 1 Byte><8 Byte value> Where: <Type of second byte> = 0x40 indicates byte 2 is AA charging-group export-id <Type of second byte> = 0x50 indicates byte 2 is AA app-group export-id <Type of second byte> = 0x60 indicates byte 2 is AA application export-id <Type of second byte> = 0x70 indicates byte 2 is sub-aggregate export-id (=1) <export-id> =<1 to 255> For example: 500 bytes reported in CG id 2 Alc-Acct- I-Inprof-Octets-64 = 0x400200000000000001f4
26.6527.21	Alc-Acct-O-Inprof-Octets-64	octets	10 bytes	<Type of second byte 1 Byte><export-id 1 Byte><8 Byte value> Where: <Type of second byte> = 0x40 indicates byte 2 is AA charging-group export-id <Type of second byte> = 0x50 indicates byte 2 is AA app-group export-id <Type of second byte> = 0x60 indicates byte 2 is AA application export-id <Type of second byte> = 0x70 indicates byte 2 is sub-aggregate export-id (=1) <export-id> = <1 to 255> For example: Alc-Acct-O-Inprof-Octets-64 = 0x40020000000000651d26

Table 83 **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 ><export-id 1 Byte><8 Byte value> Where <Type of second byte> = 0x40 indicates byte 2 is AA charging-group export-id <Type of second byte> = 0x50 indicates byte 2 is AA app-group export-id <Type of second byte> = 0x60 indicates byte 2 is AA application export-id <export-id> = <1…255> 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 ><export-id 1 Byte><8 Byte value> Where <Type of second byte > =0x40 indicates byte 2 is AA charging-group export-id <Type of second byte> = 0x50 indicates byte 2 is AA app-group export-id <Type of second byte> = 0x60 indicates byte 2 is AA application export-id < export-id> = <1 to 255> 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 84 **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

1.3.7 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 Enhanced Subscriber Management (ESM) Accounting.

Table 85 **Dynamic Data Service Accounting (Description)**

Attribute ID	Attribute Name	Description
1	User-Name	Dynamic data services associated with an ESM control channel: • The RADIUS user-name from the Dynamic Data Service Control Channel associated with this Dynamic Data Service SAP accounting session Dynamic data services associated with a dynamic service data trigger: • The dynamic data services sap-id
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	(Dynamic Data Services associated with an ESM control channel only) The Class attributes 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.
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 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. If an accounting stop is sent as a result of a failure scenario, the Acct-Session-Time is zero.

Table 85 **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	Dynamic data services associated with and ESM control channel: • Accounting session ID of the associated Control Channel (session acct-session-id for PPPoE or IPoE sessions and host acct-session-id for IPoE hosts) Dynamic data services associated with a dynamic service data trigger: • Accounting session id of the associated dynamic services data trigger (send in Access-Request in case of RADIUS authentication)
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	(Dynamic Data Services associated with an ESM control channel only) 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	(Dynamic Data Services associated with an ESM control channel only) The Agent-Remote-Id attribute from the Dynamic Data Service Control Channel associated with this Dynamic Data Service SAP accounting session

Table 85 **Dynamic Data Service Accounting (Description) (Continued)**

Attribute ID	Attribute Name	Description
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 the function-key specifies which Python functions are 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 86 **Dynamic Data Service Accounting (Limits)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
1	User-Name	string	253 chars	For dynamic data services associated with an ESM control channel, the format depends on authentication method and configuration. For dynamic data services associated with a dynamic service data trigger, the format is fixed to the dynamic services sap-id. 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	Up to 6 attributes. Max. value length for each attribute is 253 chars	For example: Class = “This is a Class attribute”
32	NAS-Identifier	string	32 chars	For example: NAS-Identifier = router-1
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

Table 86 **Dynamic Data Service Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
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 0x3231323834363335393231303235313231 3133343039
46	Acct-Session-Time	integer	42949672 seconds	The attribute value wraps after approximately 497 days 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
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

Table 86 **Dynamic Data Service Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
26.6527.165	Alc-Dyn-Serv-Script-Params	string	multiple VSAs 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 are 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 87 **Dynamic Data Service Accounting (Applicability)**

Attribute ID	Attribute Name	Acct Start	Acct Stop	Acct Interim-Update
1	User-Name	1	1	1
4	NAS-IP-Address	0-1	0-1	0-1
25	Class	0+	0+	0+
32	NAS-Identifier	1	1	1
40	Acct-Status-Type	1	1	1
41	Acct-Delay-Time	1	1	1
44	Acct-Session-Id	1	1	1
46	Acct-Session-Time	0	1	1
49	Acct-Terminate-Cause	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+

1.3.8 CLI User Access Accounting

Table 88 **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 (**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.
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 88 **CLI User Access Accounting (Description) (Continued)**

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 five command strings of which the third is too long, only the first two entries are used and the rest are 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 built from the mandatory attribute [26.6527.5]Timetra-Default-Action and optional attributes [26.6527.6] Timetra-Cmd, [26.6527.7] Timetra-Action.

Table 89 **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 to 2”
44	Acct-Session-Id	string	22 bytes	For example: Acct-Session-Id = “212846359210251211 3409”
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

Table 89 **CLI User Access Accounting (Limits) (Continued)**

Attribute ID	Attribute Name	Type	Limits	SR OS Format
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 90 **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

1.3.9 Accounting Terminate Causes

Table 91 specifies the different Terminate Causes generated by the SR OS in [49] Acct-Terminate-Cause attribute. An overview of different Enhanced Subscriber Management (ESM) Error Codes and their mapping to the Accounting Terminate Cause can be shown with the CLI command: **tools dump aaa radius-acct-terminate-cause**.

Table 91 **Accounting Terminate Causes**

Code	Acct Terminate Cause	Description	SR OS
1	User-Request	User requested termination of service, 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; example, user's connection to a host was interrupted.	yes

Table 91 **Accounting Terminate Causes (Continued)**

Code	Acct Terminate Cause	Description	SR OS
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, 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 (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
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

Table 91 **Accounting Terminate Causes (Continued)**

Code	Acct Terminate Cause	Description	SR OS
22	Port Administratively Disabled	Indicates that the Port has been administratively disabled (dot1x)	no
23	Lost Power	—	no

1.3.10 Accounting Triggered Reason VSA Values

Enhanced Subscriber Management (ESM) and Distributed Subscriber Management (DSM) accounting generate Accounting Interim Update messages periodically or triggered by an event. The reason for the Accounting Interim Update message is included in the [26.6527.163] Alc-Acct-Triggered-Reason attribute.

For ESM, sending of Accounting Interim Updates and inclusion of the [26.6527.163] Alc-Acct-Triggered-Reason attribute must be enabled explicitly via following configuration:

```
subscriber-mgmt
        radius-accounting-policy "acct-policy-1" create
            host-accounting interim-update              # maximum two accounting
            queue-instance-accounting interim-update    # modes can be enabled
            session-accounting interim-update           # simultaneously
            include-radius-attribute
                alc-acct-triggered-reason
            exit
        exit
```

Table 92 specifies the different Accounting Triggered Reason values generated by the SR OS in [26.6527.163] Alc-Acct-Triggered-Reason attribute.

Table 92 **Accounting Triggered Reason**

Value	Reason	Description	Accounting Mode				
			CPM Based			ISA Based	
			ESM			DSM	LSN
			Host	Session	Queue		
1	regular	Periodic Accounting Interim Update. The interval can be returned from RADIUS or configured ESM: **configure subscriber-mgmt radius-accounting-policy** *name* **update-interval**. DSM: **configure service vprn | ies** *service-id* **subscriber-interface** *sub-itf* **group-interface** *grp-itf* **wlan-gw vlan-tag-ranges range** *start* **start** *end* **end distributed-sub-mgmt accounting-update-interval**	X	X	X	X	—
2	sla-start	An sla-stop followed by an sla-start is generated when a CoA with new sla-profile is received.	X	X	—	—	—
3	sla-stop	An sla-stop followed by an sla-start is generated when a CoA with new sla-profile is received.	X	X	—	—	—
4	Framed-IP-Address-up	IP address or prefix tracking [1] Generated for a session when an IPv4 host is added.	—	X [2]	—	X	—
5	Framed-IP-Address-down	IP address or prefix tracking [1] Generated for a session when an IPv4 host is deleted.	—	X [2]	—	X	—
6	Alc-Ipv6-Address-up	IP address or prefix tracking [1] Generated for a session when a DHCPv6 IA-NA host is added.	—	X [2]	—	X	—
7	Alc-Ipv6-Address-down	IP address or prefix tracking [1] Generated for a session when a DHCPv6 IA-NA host is deleted.	—	X [2]	—	X	—

Table 92 **Accounting Triggered Reason (Continued)**

Value	Reason	Description	Accounting Mode				
			CPM Based			ISA Based	
			ESM			DSM	LSN
			Host	Session	Queue		
8	Delegated-IPv6-Prefix-up	IP address or prefix tracking [1] Generated for a session when a DHCPv6 IA-PD host or DHCPv6 IA-PD as managed route is added.	—	X [2]	—	—	—
9	Delegated-IPv6-Prefix-down	IP address or prefix tracking [1] Generated for a session when a DHCPv6 IA-PD host or DHCPv6 IA-PD as managed route is deleted.	—	X [2]	—	—	—
10	Framed-IPv6-Prefix-up	IP address or prefix tracking [1] Generated for a session when a SLAAC host is added.	—	X [2]	—	X	—
11	Framed-IPv6-Prefix-down	IP address or prefix tracking [1] Generated for a session when a SLAAC host is deleted.	—	X [2]	—	X	—
12	Interval-Changed	Generated when the interval, at which Accounting Interim Updates are send, is changed. (RADIUS Access-Accept or CoA with attribute [85] Acct-Interim-Interval received). Notifies the Accounting server that this host uses a different Accounting Interim Update interval than the configured update-interval in the radius-accounting-policy.	X	X	X	X	—
13	DSL-Line-Attributes-Changed	Generated when DSL-Line-Attributes values (example: Actual-Data-Rate-Upstream) are received via ANCP after the PPPoE session or IPoE binding was already established.	X	X	X	—	—

Table 92 **Accounting Triggered Reason (Continued)**

Value	Reason	Description	Accounting Mode				
			CPM Based			ISA Based	
			ESM			DSM	LSN
			Host	Session	Queue		
14	Wlan-Mobility-Event	Generated when mobility triggered accounting is enabled (**configure router** | **service vprn** *id* **wlan-gw mobility-triggered-acct interim-update**) and when a mobility event is detected (re-authentication, accounting start, accounting interim-update, data or Inter Access Point Protocol (IAPP)). For DSM, counters are always included in the triggered interim update message. For ESM counters can be included with **configure router | service vprn** *id* **wlan-gw mobility-triggered-acct interim-update include-counters**.	X	—	X	X	—
15	Persistence-Recover	IPoE subscriber hosts can be made persistent across node reboots: state is restored from a persistency file located on the compact flash file system. A triggered Accounting Interim Update message is generated for each subscriber host that is successfully restored.	X	—	X	—	—
16	SRRP-Switchover	Generated in dual homing scenarios by the node switching from srrp-non-master to srrp-master state.	X	X	X	—	—
17	Nat-Port-Range-Event	Generated when L2-Aware NAT port ranges are created and removed. This will only be triggered if any of the attributes outside-ip, outside-service or port-range-block is configured as an accounting include attribute.	—	—	—	X	—

Table 92 **Accounting Triggered Reason (Continued)**

Value	Reason	Description	Accounting Mode				
			CPM Based			ISA Based	
			ESM			DSM	LSN
			Host	Session	Queue		
18	CoA-Triggered	Generated when a CoA message is received containing the [26.6527.228] Alc-Trigger-Acct-Interim attribute. The Alc-Trigger-Acct-Interim attribute is also echoed in the CoA triggered accounting interim update message.	X	X	X	—	—
19	Nat-Free	Generated for Large Scale NAT per port-block accounting when an existing port-block is released.	—	—	—	—	X
20	Nat-Map	Generated for Large Scale NAT per port-block accounting when a new port-block is allocated.	—	—	—	—	X
21	Nat-Update	Generated for a periodically scheduled Large Scale NAT interim accounting update in both per port-block and per subscriber logging mode.	—	—	—	—	X
22	Stateless-SRRP-Switchover	Generated when a host is deleted because of stateless SRRP switchover.	—	X2	—	—	—
23	Data-Triggered-Host-Promotion	Generated when a data-triggered host is promoted to a DHCP host when the host sends a DHCP packet.	X	X	X	—	—
24	Lac-Traffic-Steering-Enabled	Generated when a steering profile is attached to a PPPoE L2TP LAC session The steering profile name is included in attribute [241.26.6527.25] Alc-Steering-Profile when configured with **configure subscriber-mgmt radius-accounting-policy** *name* **include-radius-attribute steering-profile**.	X	X	—	—	—

Table 92 **Accounting Triggered Reason (Continued)**

Value	Reason	Description	Accounting Mode				
			CPM Based			ISA Based	
			ESM			DSM	LSN
			Host	Session	Queue		
25	Lac-Traffic-Steering-Disabled	Generated when a steering profile is removed from a PPPoE L2TP LAC session The [241.26.6527.25] Alc-Steering-Profile attribute is not included in the triggered interim update message.	X	X	—	—	—

Notes:

1. IP address or prefix tracking: a triggered Accounting Interim Update message notifies the RADIUS accounting server of the acquisition or release of an IP address or prefix during the lifetime of a session.
2. Requires host-update to be configured for session-accounting mode (**configure subscriber-mgmt radius-accounting-policy** *name* **session-accounting interim-update host-update**).

1.4 RADIUS CoA and Disconnect Message Attributes

1.4.1 Subscriber Host Identification Attributes

Table 93 details the different attributes that can be used in a CoA and Disconnect Message to identify one or multiple subscriber host(s).

Table 93 **CoA and Disconnect Message: Subscriber Host Identification Attributes**

# (priority)	Attribute ID	Attribute Name	Notes	Identifies
1 NAS-Port-Id + single address/ prefix attribute [1, 4]	87	NAS-Port-Id	+ IP address or prefix	Single host [2]
	8	Framed-IP-Address	+ [87] NAS-Port-Id	Single IPv4 host [2]
	26.6527.99	Alc-Ipv6-Address	+ [87] NAS-Port-Id	Single IPv6 host (IA_NA) [2]
	97	Framed-Ipv6-Prefix	+ [87] NAS-Port-Id	Single IPv6 host (SLAAC) [2]
	123	Delegated-Ipv6-Prefix	+ [87] NAS-Port-Id	Single IPv6 host (IA_PD) [2]
2	44	Acct-Session-Id (number format)	Host acct-session-id	Single host [2]
			Queue instance acct-session-id	All hosts attached to this SLA profile instance [3] HSMDAv2: all hosts of the corresponding subscriber [3]
			Session acct-session-id	All hosts of the dual stack PPPoE or IPoE session
3	26.6527.225	Alc-BRG-Id	—	Updates the BRG and all sessions attached to this BRG.
4	26.6527.11	Alc-Subsc-ID-Str	—	All hosts of the corresponding subscriber [3]

Table 93 **CoA and Disconnect Message: Subscriber Host Identification Attributes**

# (priority)	Attribute ID	Attribute Name	Notes	Identifies
5	26.6527.100	Alc-Serv-Id	+ [8] Framed-IP-Address	Single IPv4 host [5]
	8	Framed-IP-Address	+ [26.6527.100] Alc-Serv-Id	Single IPv4 host [5]

Notes:

1. To target a subscriber host in a retail service it is mandatory to include the [26.6527.17] Alc-Retail-Serv-Id attribute. Omitting this attribute results in a CoA NAK with [101] Error-Cause attribute value 503 (Session Context Not Found).
2. Although a single host is identified, the CoA or Disconnect Message will apply to all hosts of a dual stack PPPoE session or IPoE session (if enabled).
3. A maximum of 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 [101] Error-Cause attribute value 501 (Administratively Prohibited).
4. If multiple hosts share the same IP on a single SAP (such as in a L2-Aware NAT scenario), then only a single host is identified. To make the selection of the host deterministic, the MAC address of one of the hosts can be included with the [26.6527.27] Alc-Client-Hardware-Addr to target that single host.
5. If multiple hosts share the same IP in the specified service, then the CoA is rejected (NAK).

Typically, only a single attribute or set of attributes is used to target a host or a number of hosts: “NAS-Port-Id + IP” or “Acct-Session-Id” or “Alc-Subsc-ID-Str”. If 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” is targeted. If the identified host is not part of the hosts that would be identified by the “Acct-Session-Id” attribute, then the CoA is NAK’d with [101] Error-Cause attribute value 503 Session Context Not Found.

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 NAK’d.

Following attributes are accepted only if the CoA is targeted to a single host as shown in Table 93:

- [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

1.4.2 WLAN-GW migrant users Identification Attributes

Table 94 details the attribute that can be used in a CoA and Disconnect Message to target migrant users. A Disconnect Message removes any existing migrant state for the specified UE. A CoA can only be sent for a UE in portal state to trigger the creation of an ESM or DSM user. In contrast to most CoAs this update is not incremental: the CoA must include all required authentication attributes to create the user. The applicability of attributes is the same as for an Access-Accept message in an authentication procedure.

Table 94 **CoA and Disconnect Message: WLAN-GW Migrant Users Identification Attributes**

Attribute ID	Attribute Name	Notes
1	User-Name	Must be MAC format

1.4.3 Distributed Subscriber Management (DSM) UE Identification Attributes

Table 95 details the different attributes that can be used in a CoA and Disconnect Message to identify a single DSM UE.

Table 95 **CoA and Disconnect Message: DSM UE Identification Attributes**

# (priority)	Attribute ID	Attribute Name	Notes
1	44	Acct-Session-Id	—
2	1	User-Name	Must be MAC format

1.4.4 IPSec Tunnel Identification Attributes

Table 96 details the different attributes that can be used in a Disconnect Message to identify one or multiple IKEv2 remote-access tunnel(s).

Table 96 **Disconnect Message: IPSec Tunnel Identification Attributes**

ID method [1]	Attribute ID	Attribute Name	Notes	Identifies
1	87	NAS-Port-Id	NAS-Port-Id+ Alc-IPsec-Serv-Id + a single IP Address or IPv6 Prefix attribute	Single IPSec Tunnel
	26.6527.61	Alc-IPSec-Serv-Id		
	8 97	Framed-IP-Address Framed-IPv6-Prefix		
2	44	Acct-Session-Id	—	Single IPSec Tunnel for a given public service
3	1	User-Name	—	All IPSec Tunnels with the User-Name as the IDi [2]

Notes:

1. Only one of the three identification methods should be used in a Disconnect Request, otherwise the system will reject it by sending a Disconnect-NAK with [101] Error-Cause value set to 404 (Invalid Request).
2. If there are multiple tunnels having the specified IDi, then all these tunnels are terminated.

1.4.5 Dynamic Data Services Identification Attributes

This section details the attributes that can be used in a CoA and Disconnect Message to identify Dynamic Data Services associated with a dynamic service data trigger.

To identify Dynamic Data Services associated with an Enhanced Subscriber Management (ESM) control channel, the CoA and Disconnect Messages must be send to the control channel. See section "Subscriber Host Identification Attributes" for attributes that can be used as key.

Table 97 lists the attributes that can be used in a CoA and Disconnect Message to identify one or multiple Dynamic Data Services associated with a dynamic service data trigger.

Table 97 **CoA and Disconnect Message: Data Triggered Dynamic Services Identification Attributes**

Attribute ID	Attribute Name	Identifies
44	Acct-Session-Id	Accounting session id of a dynamic services data trigger (can be displayed with "**show service dynamic-services data-triggers** [**sap** *sap-id*]"): • Identifies a single dynamic service. • Modify and Teardown actions are supported in CoA. • Only a single dynamic service is deleted with a Disconnect Message. Accounting session id of a dynamic services sap associated with a dynamic services data trigger (can be displayed with "**show service dynamic-services saps summary** [**sap** *sap-id*]"): • Identifies a single dynamic service. • Modify and Teardown actions are supported in CoA. • The identified dynamic service is deleted with a Disconnect Message.
87	NAS-Port-Id	Targets a dynamic services sap-id: • Identifies a single dynamic service. • Modify and Teardown actions are supported in CoA. • The identified dynamic service is deleted with a Disconnect Message. **Note:** If the *sap-id* corresponds with the *sap-id* of a dynamic services data trigger, then all dynamic data services associated with that data trigger are deleted in case of a Teardown action in CoA or a Disconnect Message.

1.4.6 Overview of CoA Attributes

Table 98 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 98 **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
100	Framed-IPv6-Pool
101	Error-Cause
123	Delegated-IPv6-Prefix
26.529.242	Ascend-Data-Filter
26.2352.1	Client-DNS-Pri
26.2352.2	Client-DNS-Sec
26.2352.99	RB-Client-NBNS-Pri
26.2352.100	RB-Client-NBNS-Sec

Table 98 **RADIUS CoA Message Supported Attributes (Continued)**

Attribute ID	Attribute Name
26.4874.4	ERX-Primary-Dns
26.4874.5	ERX-Secondary-Dns
26.4874.6	ERX-Primary-Wins
26.4874.7	ERX-Secondary-Wins
26.4874.47	ERX-Ipv6-Primary-Dns
26.4874.48	ERX-Ipv6-Secondary-Dns
26.6527.9	Alc-Primary-Dns
26.6527.10	Alc-Secondary-Dns
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
26.6527.16	Alc-ANCP-Str
26.6527.17	Alc-Retail-Serv-Id
26.6527.18	Alc-Default-Router
26.6527.27	Alc-Client-Hardware-Addr
26.6527.28	Alc-Int-Dest-Id-Str
26.6527.29	Alc-Primary-Nbns
26.6527.30	Alc-Secondary-Nbns
26.6527.35	Alc-PPPoE-Service-Name
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
26.6527.103	Alc-ToClient-Dhcp-Options

Table 98 **RADIUS CoA Message Supported Attributes (Continued)**

Attribute ID	Attribute Name
26.6527.105	Alc-Ipv6-Primary-Dns
26.6527.106	Alc-Ipv6-Secondary-Dns
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
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

Table 98 **RADIUS CoA Message Supported Attributes (Continued)**

Attribute ID	Attribute Name
26.6527.170	Alc-Dyn-Serv-Acct-Stats-Type-1
26.6527.171	Alc-Dyn-Serv-Acct-Stats-Type-2
26.6527.174	Alc-Lease-Time
26.6527.177	Alc-Portal-Url
26.6527.178	Alc-Ipv6-Portal-Url
26.6527.179	Alc-GTP-Local-Breakout
26.6527.181	Alc-SLAAC-IPv6-Pool
26.6527.182	Alc-AA-Sub-Http-Url-Param
26.6527.185	Alc-Onetime-Http-Redirect-Reactivate
26.6527.186	Alc-Wlan-Dsm-Ot-Http-Redirect-Url
26.6527.187	Alc-Wlan-Dsm-Ip-Filter
26.6527.188	Alc-Wlan-Dsm-Ingress-Policer
26.6527.189	Alc-Wlan-Dsm-Egress-Policer
26.6527.192	Alc-ToClient-Dhcp6-Options
26.6527.193	Alc-AA-App-Service-Options
26.6527.200	Alc-v6-Preferred-Lifetime
26.6527.201	Alc-v6-Valid-Lifetime
26.6527.202	Alc-Dhcp6-Renew-Time
26.6527.203	Alc-Dhcp6-Rebind-Time
26.6527.217	Alc-UPnP-Sub-Override-Policy
26.6527.220	Alc-Home-Aware-Pool
26.6527.221	Alc-DMZ-Address
26.6527.223	Alc-Reserved-Addresses
26.6527.224	Alc-BRG-Profile
26.6527.225	Alc-BRG-Id
26.6527.228	Alc-Trigger-Acct-Interim
26.6527.232	Alc-Acct-Interim-lvl

Table 98 **RADIUS CoA Message Supported Attributes (Continued)**

Attribute ID	Attribute Name
26.6527.233	Alc-Tunnel-Qos-Override
26.6527.234	Alc-DNAT-Override
26.6527.235	Alc-BRG-DHCP-Streaming-Dest
26.6527.236	Alc-Host-DHCP-Streaming-Disabled
26.6527.238	Alc-Remove-Override
26.6527.241	Alc-Per-Host-Port-Range
26.6527.242	Alc-Radius-Py
26.6527.243	Alc-LI-Use-Outside-Ip
241.26.6527.3	Alc-PPPoE-Client-Policy
241.26.6527.4	Alc-PPPoE-Client-Username
241.26.6527.5	Alc-PPPoE-Client-Password
241.26.6527.16	Alc-IPv6-Router-Adv-Policy
241.26.6527.17	Alc-Nat-Outside-IPs
241.26.6527.18	Alc-Mld-Import-Policy
241.26.6527.22	Alc-Bonding-Reference-Rate
241.26.6527.24	Alc-IPv6-DMZ-Enabled
241.26.6527.25	Alc-Steering-Profile
241.26.6527.26	Alc-Aa-Sub-Scope
241.26.6527.35	Alc-Mld-Import-Policy-Modif
241.26.6527.37	Alc-VAS-IPv4-Filter
241.26.6527.38	Alc-VAS-NSH-IPv4-Opaque-Meta-Data
241.26.6527.39	Alc-Static-Port-Forward
241.26.6527.40	Alc-IPv6-Slaac-Replacement-Prefix

1.4.7 [101] Error-Cause Attribute Values

Table 99 provides an overview of the [101] Error-Cause attribute values as defined in RFC 5176 and lists if they are generated in SR OS.

Table 99 **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 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

Table 99 **RADIUS CoA Message [101] Error-Cause Values (Continued)**

Code	CoA Error Cause	Description	SR OS
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. Example, this can occur if the required entries are not present in the proxy's realm routing table.	No
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, and so on).	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

Table 100 lists the possible [101] Error-Cause attribute values generated in the SR OS in response to a Disconnect Message targeting an IPsec tunnel.

Table 100 **RADIUS Disconnect Message [101] Error-Cause Values for IPSec Tunnel**

Code	CoA Error Cause	Description
404	Invalid Request	A fatal error sent if some other aspect of the Disconnect-Request is invalid, such as multiple tunnel identifications present in the request.
503	Session Context Not Found	A fatal error sent if the tunnel identified in the Disconnect-Request does not exist.
504	Session Context Not Removable	A fatal error sent if all identified tunnels belong to a tunnel group in MC-IPsec standby status.

2 Standards and Protocol Support

Note: The information presented is subject to change without notice.

Nokia assumes no responsibility for inaccuracies contained herein.

Access Node Control Protocol (ANCP)

draft-ietf-ancp-protocol-02, *Protocol for Access Node Control Mechanism in Broadband Networks*

RFC 5851, *Framework and Requirements for an Access Node Control Mechanism in Broadband Multi-Service Networks*

Application Assurance (AA)

3GPP Release 12 (ADC rules over Gx interfaces)

RFC 3507, *Internet Content Adaptation Protocol (ICAP)*

Asynchronous Transfer Mode (ATM)

AF-ILMI-0065.000, *Integrated Local Management Interface (ILMI) Version 4.0*

AF-PHY-0086.001, *Inverse Multiplexing for ATM (IMA) Specification Version 1.1*

AF-TM-0121.000, *Traffic Management Specification Version 4.1*

AF-TM-0150.00, *Addendum to Traffic Management v4.1 optional minimum desired cell rate indication for UBR*

GR-1113-CORE, *Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1*

GR-1248-CORE, *Generic Requirements for Operations of ATM Network Elements (NEs), Issue 3*

ITU-T I.432.1, *B-ISDN user-network interface - Physical layer specification: General characteristics (02/99)*

ITU-T I.610, *B-ISDN operation and maintenance principles and functions (11/95)*

RFC 1626, *Default IP MTU for use over ATM AAL5*

RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*

Bidirectional Forwarding Detection (BFD)

RFC 5880, *Bidirectional Forwarding Detection (BFD)*

RFC 5881, *Bidirectional Forwarding Detection (BFD) IPv4 and IPv6 (Single Hop)*

RFC 5883, *Bidirectional Forwarding Detection (BFD) for Multihop Paths*

RFC 7130, *Bidirectional Forwarding Detection (BFD) on Link Aggregation Group (LAG) Interfaces*

Border Gateway Protocol (BGP)

draft-hares-idr-update-attrib-low-bits-fix-01, *Update Attribute Flag Low Bits Clarification*

draft-ietf-idr-add-paths-guidelines-08, *Best Practices for Advertisement of Multiple Paths in IBGP*

draft-ietf-idr-best-external-03, *Advertisement of the best external route in BGP*

draft-ietf-idr-bgp-flowspec-oid-03, *Revised Validation Procedure for BGP Flow Specifications*

draft-ietf-idr-bgp-gr-notification-01, *Notification Message support for BGP Graceful Restart*

draft-ietf-idr-bgp-optimal-route-reflection-10, *BGP Optimal Route Reflection (BGP-ORR)*

draft-ietf-idr-error-handling-03, *Revised Error Handling for BGP UPDATE Messages*

draft-ietf-idr-flowspec-interfaceset-03, *Applying BGP flowspec rules on a specific interface set*

draft-ietf-idr-link-bandwidth-03, *BGP Link Bandwidth Extended Community*

draft-ietf-sidr-origin-validation-signaling-04, *BGP Prefix Origin Validation State Extended Community*

draft-uttaro-idr-bgp-persistence-03, *Support for Long-lived BGP Graceful Restart*

RFC 1772, *Application of the Border Gateway Protocol in the Internet*

RFC 1997, *BGP Communities Attribute*

RFC 2385, *Protection of BGP Sessions via the TCP MD5 Signature Option*

RFC 2439, *BGP Route Flap Damping*

RFC 2545, *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*

RFC 2858, *Multiprotocol Extensions for BGP-4*

RFC 2918, *Route Refresh Capability for BGP-4*

RFC 3107, *Carrying Label Information in BGP-4*

RFC 3392, *Capabilities Advertisement with BGP-4*

RFC 4271, *A Border Gateway Protocol 4 (BGP-4)*

RFC 4360, *BGP Extended Communities Attribute*

RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*

RFC 4456, *BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)*

RFC 4486, *Subcodes for BGP Cease Notification Message*

RFC 4659, *BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*

RFC 4684, *Constrained Route Distribution for Border Gateway Protocol/ MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)*

RFC 4724, *Graceful Restart Mechanism for BGP* (helper mode)

RFC 4760, *Multiprotocol Extensions for BGP-4*

RFC 4798, *Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)*

RFC 4893, *BGP Support for Four-octet AS Number Space*

RFC 5004, *Avoid BGP Best Path Transitions from One External to Another*

RFC 5065, *Autonomous System Confederations for BGP*

RFC 5291, *Outbound Route Filtering Capability for BGP-4*

RFC 5396, *Textual Representation of Autonomous System (AS) Numbers* (asplain)

RFC 5575, *Dissemination of Flow Specification Rules*

RFC 5668, *4-Octet AS Specific BGP Extended Community*

RFC 6810, *The Resource Public Key Infrastructure (RPKI) to Router Protocol*

RFC 6811, *Prefix Origin Validation*

RFC 6996, *Autonomous System (AS) Reservation for Private Use*

RFC 7311, *The Accumulated IGP Metric Attribute for BGP*

RFC 7607, *Codification of AS 0 Processing*

RFC 7674, *Clarification of the Flowspec Redirect Extended Community*

RFC 7752, *North-Bound Distribution of Link-State and Traffic Engineering (TE) Information Using BGP*

RFC 7911, *Advertisement of Multiple Paths in BGP*

Circuit Emulation

RFC 4553, *Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)*

RFC 5086, *Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)*

RFC 5287, *Control Protocol Extensions for the Setup of Time-Division Multiplexing (TDM) Pseudowires in MPLS Networks*

Ethernet

IEEE 802.1AB, *Station and Media Access Control Connectivity Discovery*

IEEE 802.1ad, *Provider Bridges*

IEEE 802.1ag, *Connectivity Fault Management*

IEEE 802.1ah, *Provider Backbone Bridges*

IEEE 802.1ak, *Multiple Registration Protocol*
IEEE 802.1aq, *Shortest Path Bridging*
IEEE 802.1ax, *Link Aggregation*
IEEE 802.1D, *MAC Bridges*
IEEE 802.1p, *Traffic Class Expediting*
IEEE 802.1Q, *Virtual LANs*
IEEE 802.1s, *Multiple Spanning Trees*
IEEE 802.1w, *Rapid Reconfiguration of Spanning Tree*
IEEE 802.1X, *Port Based Network Access Control*
IEEE 802.3ab, *1000BASE-T*
IEEE 802.3ac, *VLAN Tag*
IEEE 802.3ad, *Link Aggregation*
IEEE 802.3ae, *10 Gb/s Ethernet*
IEEE 802.3ah, *Ethernet in the First Mile*
IEEE 802.3ba, *40 Gb/s and 100 Gb/s Ethernet*
IEEE 802.3i, *Ethernet*
IEEE 802.3u, *Fast Ethernet*
IEEE 802.3x, *Ethernet Flow Control*
IEEE 802.3z, *Gigabit Ethernet*
ITU-T G.8031/Y.1342, *Ethernet Linear Protection Switching*
ITU-T G.8032/Y.1344, *Ethernet Ring Protection Switching*
ITU-T Y.1731, *OAM functions and mechanisms for Ethernet based networks*

Ethernet VPN (EVPN)

draft-ietf-bess-evpn-ac-df-01, *AC-Influenced Designated Forwarder Election for EVPN*
draft-ietf-bess-evpn-etree-11, *E-TREE Support in EVPN & PBB-EVPN*
draft-ietf-bess-evpn-overlay-04, *A Network Virtualization Overlay Solution using EVPN*
draft-ietf-bess-evpn-prefix-advertisement-02, *IP Prefix Advertisement in EVPN*
draft-ietf-bess-evpn-proxy-arp-nd-02, *Operational Aspects of Proxy-ARP/ND in EVPN Networks*
draft-ietf-bess-evpn-vpls-seamless-integ-00, *(PBB-)EVPN Seamless Integration with (PBB-)VPLS*
draft-ietf-bess-evpn-vpws-14, *Virtual Private Wire Service support in Ethernet VPN*
draft-rabadan-bess-evpn-pref-df-02, *Preference-based EVPN DF Election*
draft-snr-bess-pbb-evpn-isid-cmacflush-01, *PBB-EVPN ISID-based CMAC-Flush*

RFC 7432, *BGP MPLS-Based Ethernet VPN*

RFC 7623, *Provider Backbone Bridging Combined with Ethernet VPN (PBB-EVPN)*

Frame Relay

ANSI T1.617 Annex D, *DSS1 - Signalling Specification For Frame Relay Bearer Service*

FRF.1.2, *PVC User-to-Network Interface (UNI) Implementation Agreement*

FRF.12, *Frame Relay Fragmentation Implementation Agreement*

FRF.16.1, *Multilink Frame Relay UNI/NNI Implementation Agreement*

FRF.5, *Frame Relay/ATM PVC Network Interworking Implementation*

FRF2.2, *PVC Network-to-Network Interface (NNI) Implementation Agreement*

ITU-T Q.933 Annex A, *Additional procedures for Permanent Virtual Connection (PVC) status management*

Generalized Multiprotocol Label Switching (GMPLS)

draft-ietf-ccamp-rsvp-te-srlg-collect-04, *RSVP-TE Extensions for Collecting SRLG Information*

RFC 3471, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description*

RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions*

RFC 4204, *Link Management Protocol (LMP)*

RFC 4208, *Generalized Multiprotocol Label Switching (GMPLS) User-Network Interface (UNI): Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Support for the Overlay Model*

RFC 4872, *RSVP-TE Extensions in Support of End-to-End Generalized Multi-Protocol Label Switching (GMPLS) Recovery*

RFC 5063, *Extensions to GMPLS Resource Reservation Protocol (RSVP) Graceful Restart* (helper mode)

Intermediate System to Intermediate System (IS-IS)

draft-ginsberg-isis-mi-bis-01, *IS-IS Multi-Instance* (single topology)

draft-ietf-isis-mi-02, *IS-IS Multi-Instance*

draft-kaplan-isis-ext-eth-02, *Extended Ethernet Frame Size Support*

ISO/IEC 10589:2002, Second Edition, Nov. 2002, *Intermediate system to Intermediate system intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode Network Service (ISO 8473)*

RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*

RFC 2973, *IS-IS Mesh Groups*

RFC 3359, *Reserved Type, Length and Value (TLV) Codepoints in Intermediate System to Intermediate System*

RFC 3719, *Recommendations for Interoperable Networks using Intermediate System to Intermediate System (IS-IS)*

RFC 3787, *Recommendations for Interoperable IP Networks using Intermediate System to Intermediate System (IS-IS)*

RFC 4971, *Intermediate System to Intermediate System (IS-IS) Extensions for Advertising Router Information*

RFC 5120, *M-ISIS: Multi Topology (MT) Routing in IS-IS*

RFC 5130, *A Policy Control Mechanism in IS-IS Using Administrative Tags*

RFC 5301, *Dynamic Hostname Exchange Mechanism for IS-IS*

RFC 5302, *Domain-wide Prefix Distribution with Two-Level IS-IS*

RFC 5303, *Three-Way Handshake for IS-IS Point-to-Point Adjacencies*

RFC 5304, *IS-IS Cryptographic Authentication*

RFC 5305, *IS-IS Extensions for Traffic Engineering TE*

RFC 5306, *Restart Signaling for IS-IS* (helper mode)

RFC 5307, *IS-IS Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*

RFC 5308, *Routing IPv6 with IS-IS*

RFC 5309, *Point-to-Point Operation over LAN in Link State Routing Protocols*

RFC 5310, *IS-IS Generic Cryptographic Authentication*

RFC 6213, *IS-IS BFD-Enabled TLV*

RFC 6232, *Purge Originator Identification TLV for IS-IS*

RFC 6233, *IS-IS Registry Extension for Purges*

RFC 6329, *IS-IS Extensions Supporting IEEE 802.1aq Shortest Path Bridging*

RFC 7775, *IS-IS Route Preference for Extended IP and IPv6 Reachability*

RFC 7794, *IS-IS Prefix Attributes for Extended IPv4 and IPv6 Reachability*

Internet Protocol (IP) — Fast Reroute

draft-ietf-rtgwg-lfa-manageability-08, *Operational management of Loop Free Alternates*

RFC 5286, *Basic Specification for IP Fast Reroute: Loop-Free Alternates*

RFC 7431, *Multicast-Only Fast Reroute*

RFC 7490, *Remote Loop-Free Alternate (LFA) Fast Reroute (FRR)*

Internet Protocol (IP) — General

draft-grant-tacacs-02, *The TACACS+ Protocol*

RFC 768, *User Datagram Protocol*

RFC 793, *Transmission Control Protocol*

RFC 854, *Telnet Protocol Specifications*

RFC 1350, *The TFTP Protocol (revision 2)*

RFC 2347, *TFTP Option Extension*

RFC 2348, *TFTP Blocksize Option*

RFC 2349, *TFTP Timeout Interval and Transfer Size Options*

RFC 2428, *FTP Extensions for IPv6 and NATs*

RFC 2784, *Generic Routing Encapsulation (GRE)*

RFC 4250, *The Secure Shell (SSH) Protocol Assigned Numbers*

RFC 4251, *The Secure Shell (SSH) Protocol Architecture*

RFC 4252, *The Secure Shell (SSH) Authentication Protocol* (publickey, password)

RFC 4253, *The Secure Shell (SSH) Transport Layer Protocol*

RFC 4254, *The Secure Shell (SSH) Connection Protocol*

RFC 4632, *Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan*

RFC 5082, *The Generalized TTL Security Mechanism (GTSM)*

RFC 5656, *Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer* (ECDSA)

RFC 6398, *IP Router Alert Considerations and Usage* (MLD)

RFC 6528, *Defending against Sequence Number Attacks*

Internet Protocol (IP) — Multicast

cisco-ipmulticast/pim-autorp-spec01, *Auto-RP: Automatic discovery of Group-to-RP mappings for IP multicast* (version 1)

draft-dolganow-bess-mvpn-expl-track-01, *Explicit Tracking with Wild Card Routes in Multicast VPN*

draft-ietf-idmr-traceroute-ipm-07, *A "traceroute" facility for IP Multicast*

draft-ietf-l2vpn-vpls-pim-snooping-07, *Protocol Independent Multicast (PIM) over Virtual Private LAN Service (VPLS)*

RFC 1112, *Host Extensions for IP Multicasting*

RFC 2236, *Internet Group Management Protocol, Version 2*

RFC 2365, *Administratively Scoped IP Multicast*

RFC 2375, *IPv6 Multicast Address Assignments*

RFC 2710, *Multicast Listener Discovery (MLD) for IPv6*

RFC 3306, *Unicast-Prefix-based IPv6 Multicast Addresses*

RFC 3376, *Internet Group Management Protocol, Version 3*

RFC 3446, *Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)*

RFC 3590, *Source Address Selection for the Multicast Listener Discovery (MLD) Protocol*

RFC 3618, *Multicast Source Discovery Protocol (MSDP)*

RFC 3810, *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*

RFC 3956, *Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*

RFC 3973, *Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)* (auto-RP groups)

RFC 4541, *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*

RFC 4601, *Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*

RFC 4604, *Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast*

RFC 4607, *Source-Specific Multicast for IP*

RFC 4608, *Source-Specific Protocol Independent Multicast in 232/8*

RFC 4610, *Anycast-RP Using Protocol Independent Multicast (PIM)*

RFC 4611, *Multicast Source Discovery Protocol (MSDP) Deployment Scenarios*

RFC 5059, *Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)*

RFC 5186, *Internet Group Management Protocol Version 3 (IGMPv3) / Multicast Listener Discovery Version 2 (MLDv2) and Multicast Routing Protocol Interaction*

RFC 5384, *The Protocol Independent Multicast (PIM) Join Attribute Format*

RFC 5496, *The Reverse Path Forwarding (RPF) Vector TLV*

RFC 6037, *Cisco Systems' Solution for Multicast in MPLS/BGP IP VPNs*

RFC 6512, *Using Multipoint LDP When the Backbone Has No Route to the Root*

RFC 6513, *Multicast in MPLS/BGP IP VPNs*

RFC 6514, *BGP Encodings and Procedures for Multicast in MPLS/IP VPNs*

RFC 6515, *IPv4 and IPv6 Infrastructure Addresses in BGP Updates for Multicast VPNs*

RFC 6516, *IPv6 Multicast VPN (MVPN) Support Using PIM Control Plane and Selective Provider Multicast Service Interface (S-PMSI) Join Messages*

RFC 6625, *Wildcards in Multicast VPN Auto-Discover Routes*

RFC 6826, *Multipoint LDP In-Band Signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Path*

RFC 7246, *Multipoint Label Distribution Protocol In-Band Signaling in a Virtual Routing and Forwarding (VRF) Table Context*

RFC 7385, *IANA Registry for P-Multicast Service Interface (PMSI) Tunnel Type Code Points*

RFC 7716, *Global Table Multicast with BGP Multicast VPN (BGP-MVPN) Procedures*

Internet Protocol (IP) — Version 4

RFC 791, *Internet Protocol*

RFC 792, *Internet Control Message Protocol*

RFC 826, *An Ethernet Address Resolution Protocol*

RFC 951, *Bootstrap Protocol (BOOTP)*

RFC 1034, *Domain Names - Concepts and Facilities*

RFC 1035, *Domain Names - Implementation and Specification*

RFC 1519, *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*

RFC 1534, *Interoperation between DHCP and BOOTP*

RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol*

RFC 1812, *Requirements for IPv4 Routers*

RFC 1918, *Address Allocation for Private Internets*

RFC 2003, *IP Encapsulation within IP*

RFC 2131, *Dynamic Host Configuration Protocol*

RFC 2132, *DHCP Options and BOOTP Vendor Extensions*

RFC 2401, *Security Architecture for Internet Protocol*

RFC 3021, *Using 31-Bit Prefixes on IPv4 Point-to-Point Links*

RFC 3046, *DHCP Relay Agent Information Option (Option 82)*

RFC 3768, *Virtual Router Redundancy Protocol (VRRP)*

RFC 4884, *Extended ICMP to Support Multi-Part Messages* (ICMPv4 and ICMPv6 Time Exceeded)

Internet Protocol (IP) — Version 6

RFC 1981, *Path MTU Discovery for IP version 6*

RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*

RFC 2464, *Transmission of IPv6 Packets over Ethernet Networks*

RFC 2473, *Generic Packet Tunneling in IPv6 Specification*

RFC 2529, *Transmission of IPv6 over IPv4 Domains without Explicit Tunnels*

RFC 3122, *Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification*

RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*

RFC 3587, *IPv6 Global Unicast Address Format*

RFC 3596, *DNS Extensions to Support IP version 6*

RFC 3633, *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*

RFC 3646, *DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*

RFC 3736, *Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6*

RFC 3971, *SEcure Neighbor Discovery (SEND)*

RFC 3972, *Cryptographically Generated Addresses (CGA)*

RFC 4007, *IPv6 Scoped Address Architecture*

RFC 4193, *Unique Local IPv6 Unicast Addresses*

RFC 4291, *Internet Protocol Version 6 (IPv6) Addressing Architecture*

RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*

RFC 4861, *Neighbor Discovery for IP version 6 (IPv6)*

RFC 4862, *IPv6 Stateless Address Autoconfiguration* (router functions)

RFC 4890, *Recommendations for Filtering ICMPv6 Messages in Firewalls*

RFC 4941, *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*

RFC 5007, *DHCPv6 Leasequery*

RFC 5095, *Deprecation of Type 0 Routing Headers in IPv6*

RFC 5798, *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6* (IPv6)

RFC 5952, *A Recommendation for IPv6 Address Text Representation*

RFC 6092 *Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service* (Internet Control and Management, Upper-Layer Transport Protocols, UDP Filters, IPsec and Internet Key Exchange (IKE), TCP Filters)

RFC 6106, *IPv6 Router Advertisement Options for DNS Configuration*

RFC 6164, *Using 127-Bit IPv6 Prefixes on Inter-Router Links*

RFC 8021, *Generation of IPv6 Atomic Fragments Considered Harmful*

Internet Protocol Security (IPsec)

draft-ietf-ipsec-isakmp-mode-cfg-05, *The ISAKMP Configuration Method*

draft-ietf-ipsec-isakmp-xauth-06, *Extended Authentication within ISAKMP/Oakley (XAUTH)*

RFC 2401, *Security Architecture for the Internet Protocol*

RFC 2403, *The Use of HMAC-MD5-96 within ESP and AH*

RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*

RFC 2405, *The ESP DES-CBC Cipher Algorithm With Explicit IV*

RFC 2406, *IP Encapsulating Security Payload (ESP)*

RFC 2407, *IPsec Domain of Interpretation for ISAKMP (IPsec DoI)*

RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*

RFC 2409, *The Internet Key Exchange (IKE)*

RFC 2410, *The NULL Encryption Algorithm and Its Use With IPsec*

RFC 3526, *More Modular Exponential (MODP) Diffie-Hellman group for Internet Key Exchange (IKE)*

RFC 3566, *The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec*

RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec*

RFC 3706, *A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers*

RFC 3947, *Negotiation of NAT-Traversal in the IKE*

RFC 3948, *UDP Encapsulation of IPsec ESP Packets*

RFC 4210, *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*

RFC 4211, *Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)*

RFC 4301, *Security Architecture for the Internet Protocol*

RFC 4303, *IP Encapsulating Security Payload*

RFC 4307, *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*

RFC 4308, *Cryptographic Suites for IPsec*

RFC 4434, *The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)*

RFC 4868, *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPSec*

RFC 4945, *The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2 and PKIX*

RFC 5019, *The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments*

RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

RFC 5998, *An Extension for EAP-Only Authentication in IKEv2*

RFC 6712, *Internet X.509 Public Key Infrastructure -- HTTP Transfer for the Certificate Management Protocol (CMP)*

RFC 6960, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*

RFC 7296, *Internet Key Exchange Protocol Version 2 (IKEv2)*

RFC 7321, *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)*

RFC 7383, *Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation*

RFC 7383, *Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation*

RFC 7468, *Textual Encodings of PKIX, PKCS, and CMS Structures*

Label Distribution Protocol (LDP)

draft-ietf-mpls-ldp-ip-pw-capability-09, *Controlling State Advertisements Of Non-negotiated LDP Applications*

draft-pdutta-mpls-ldp-adj-capability-00, *LDP Adjacency Capabilities*

draft-pdutta-mpls-ldp-v2-00, *LDP Version 2*

draft-pdutta-mpls-mldp-up-redundancy-00, *Upstream LSR Redundancy for Multi-point LDP Tunnels*

draft-pdutta-mpls-multi-ldp-instance-00, *Multiple LDP Instances*

draft-pdutta-mpls-tldp-hello-reduce-04, *Targeted LDP Hello Reduction*

RFC 3037, *LDP Applicability*

RFC 3478, *Graceful Restart Mechanism for Label Distribution Protocol* (helper mode)

RFC 5036, *LDP Specification*

RFC 5283, *LDP Extension for Inter-Area Label Switched Paths (LSPs)*

RFC 5443, *LDP IGP Synchronization*

RFC 5561, *LDP Capabilities*

RFC 5919, *Signaling LDP Label Advertisement Completion*

RFC 6388, *Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths*

RFC 6512, *Using Multipoint LDP When the Backbone Has No Route to the Root*

RFC 6826, *Multipoint LDP in-band signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths*

RFC 7032, *LDP Downstream-on-Demand in Seamless MPLS*

RFC 7552, *Updates to LDP for IPv6*

Layer Two Tunneling Protocol (L2TP) Network Server (LNS)

draft-mammoliti-l2tp-accessline-avp-04, *Layer 2 Tunneling Protocol (L2TP) Access Line Information Attribute Value Pair (AVP) Extensions*

RFC 2661, *Layer Two Tunneling Protocol "L2TP"*

RFC 2809, *Implementation of L2TP Compulsory Tunneling via RADIUS*

RFC 3438, *Layer Two Tunneling Protocol (L2TP) Internet Assigned Numbers: Internet Assigned Numbers Authority (IANA) Considerations Update*

RFC 3931, *Layer Two Tunneling Protocol - Version 3 (L2TPv3)*

RFC 4719, *Transport of Ethernet Frames over Layer 2 Tunneling Protocol Version 3 (L2TPv3)*

RFC 4951, *Fail Over Extensions for Layer 2 Tunneling Protocol (L2TP) "failover"*

Management

draft-ieft-snmpv3-update-mib-05, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*

draft-ietf-isis-wg-mib-06, *Management Information Base for Intermediate System to Intermediate System (IS-IS)*

draft-ietf-mboned-msdp-mib-01, *Multicast Source Discovery protocol MIB*

draft-ietf-mpls-ldp-mib-07, *Definitions of Managed Objects for the Multiprotocol Label Switching, Label Distribution Protocol (LDP)*

draft-ietf-mpls-lsr-mib-06, *Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base Using SMIv2*

draft-ietf-mpls-te-mib-04, *Multiprotocol Label Switching (MPLS) Traffic Engineering Management Information Base*

draft-ietf-ospf-mib-update-08, *OSPF Version 2 Management Information Base*

draft-ietf-vrrp-unified-mib-06, *Definitions of Managed Objects for the VRRP over IPv4 and IPv6* (IPv6)

ianaaddressfamilynumbers-mib, *IANA-ADDRESS-FAMILY-NUMBERS-MIB*

ianagmplstc-mib, *IANA-GMPLS-TC-MIB*

ianaiftype-mib, *IANAifType-MIB*

ianaiprouteprotocol-mib, *IANA-RTPROTO-MIB*

IEEE8021-CFM-MIB, *IEEE P802.1ag(TM) CFM MIB*

IEEE8021-PAE-MIB, *IEEE 802.1X MIB*

IEEE8023-LAG-MIB, *IEEE 802.3ad MIB*

LLDP-MIB, *IEEE P802.1AB(TM) LLDP MIB*

RFC 1157, *A Simple Network Management Protocol (SNMP)*

RFC 1212, *Concise MIB Definitions*

RFC 1213, *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*

RFC 1215, *A Convention for Defining Traps for use with the SNMP*

RFC 1724, *RIP Version 2 MIB Extension*

RFC 1901, *Introduction to Community-based SNMPv2*

RFC 2021, *Remote Network Monitoring Management Information Base Version 2 using SMIv2*

RFC 2115, *Management Information Base for Frame Relay DTEs Using SMIv2*

RFC 2206, *RSVP Management Information Base using SMIv2*

RFC 2213, *Integrated Services Management Information Base using SMIv2*

RFC 2494, *Definitions of Managed Objects for the DS0 and DS0 Bundle Interface Type*

RFC 2514, *Definitions of Textual Conventions and OBJECT-IDENTITIES for ATM Management*

RFC 2515, *Definitions of Managed Objects for ATM Management*

RFC 2570, *SNMP Version 3 Framework*

RFC 2571, *An Architecture for Describing SNMP Management Frameworks*

RFC 2572, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*

RFC 2573, *SNMP Applications*

RFC 2574, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*

RFC 2575, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*

RFC 2578, *Structure of Management Information Version 2 (SMIv2)*

RFC 2579, *Textual Conventions for SMIv2*

RFC 2580, *Conformance Statements for SMIv2*

RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol*

RFC 2819, *Remote Network Monitoring Management Information Base*

RFC 2856, *Textual Conventions for Additional High Capacity Data Types*

RFC 2863, *The Interfaces Group MIB*

RFC 2864, *The Inverted Stack Table Extension to the Interfaces Group MIB*

RFC 2933, *Internet Group Management Protocol MIB*

RFC 3014, *Notification Log MIB*

RFC 3164, *The BSD syslog Protocol*

RFC 3165, *Definitions of Managed Objects for the Delegation of Management Scripts*

RFC 3231, *Definitions of Managed Objects for Scheduling Management Operations*

RFC 3273, *Remote Network Monitoring Management Information Base for High Capacity Networks*

RFC 3416. *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*

RFC 3417, *Transport Mappings for the Simple Network Management Protocol (SNMP)* (SNMP over UDP over IPv4)

RFC 3419, *Textual Conventions for Transport Addresses*

RFC 3498, *Definitions of Managed Objects for Synchronous Optical Network (SONET) Linear Automatic Protection Switching (APS) Architectures*

RFC 3584, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*

RFC 3592, *Definitions of Managed Objects for the Synchronous Optical Network/ Synchronous Digital Hierarchy (SONET/SDH) Interface Type*

RFC 3593, *Textual Conventions for MIB Modules Using Performance History Based on 15 Minute Intervals*

RFC 3635, *Definitions of Managed Objects for the Ethernet-like Interface Types*

RFC 3637, *Definitions of Managed Objects for the Ethernet WAN Interface Sublayer*

RFC 3826, *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*

RFC 3877, *Alarm Management Information Base (MIB)*

RFC 3895, *Definitions of Managed Objects for the DS1, E1, DS2, and E2 Interface Types*

RFC 3896, *Definitions of Managed Objects for the DS3/E3 Interface Type*

RFC 4001, *Textual Conventions for Internet Network Addresses*

RFC 4022, *Management Information Base for the Transmission Control Protocol (TCP)*

RFC 4113, *Management Information Base for the User Datagram Protocol (UDP)*

RFC 4220, *Traffic Engineering Link Management Information Base*

RFC 4273, *Definitions of Managed Objects for BGP-4*

RFC 4292, *IP Forwarding Table MIB*

RFC 4293, *Management Information Base for the Internet Protocol (IP)*

RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*

RFC 4511, *Lightweight Directory Access Protocol (LDAP): The Protocol*

RFC 4513, *Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms* (TLS)

RFC 4631, *Link Management Protocol (LMP) Management Information Base (MIB)*

RFC 4878, *Definitions and Managed Objects for Operations, Administration, and Maintenance (OAM) Functions on Ethernet-Like Interfaces*

RFC 5101, *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information*

RFC 5102, *Information Model for IP Flow Information Export*

RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2* (TLS client, RSA public key)

RFC 6424, *Mechanism for Performing Label Switched Path Ping (LSP Ping) over MPLS Tunnels*

RFC 6425, *Detecting Data Plane Failures in Point-to-Multipoint Multiprotocol Label Switching (MPLS) - Extensions to LSP Ping*

RFC 7420, *Path Computation Element Communication Protocol (PCEP) Management Information Base (MIB) Module*

SFLOW-MIB, *sFlow MIB Version 1.3 (Draft 5)*

Multiprotocol Label Switching — Transport Profile (MPLS-TP)

RFC 5586, *MPLS Generic Associated Channel*

RFC 5921, *A Framework for MPLS in Transport Networks*

RFC 5960, *MPLS Transport Profile Data Plane Architecture*

RFC 6370, *MPLS Transport Profile (MPLS-TP) Identifiers*

RFC 6378, *MPLS Transport Profile (MPLS-TP) Linear Protection*

RFC 6426, *MPLS On-Demand Connectivity and Route Tracing*

RFC 6427, *MPLS Fault Management Operations, Administration, and Maintenance (OAM)*

RFC 6428, *Proactive Connectivity Verification, Continuity Check and Remote Defect indication for MPLS Transport Profile*

RFC 6478, *Pseudowire Status for Static Pseudowires*

RFC 7213, *MPLS Transport Profile (MPLS-TP) Next-Hop Ethernet Addressing*

Multiprotocol Label Switching (MPLS)

RFC 3031, *Multiprotocol Label Switching Architecture*

RFC 3032, *MPLS Label Stack Encoding*

RFC 3443, *Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks*

RFC 4023, *Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)*

RFC 4182, *Removing a Restriction on the use of MPLS Explicit NULL*

RFC 5332, *MPLS Multicast Encapsulations*

RFC 5884, *Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs)*

RFC 6790, *The Use of Entropy Labels in MPLS Forwarding*

RFC 7510, *Encapsulating MPLS in UDP*

Network Address Translation (NAT)

draft-ietf-behave-address-format-10, *IPv6 Addressing of IPv4/IPv6 Translators*

draft-ietf-behave-v6v4-xlate-23, *IP/ICMP Translation Algorithm*

draft-miles-behave-l2nat-00, *Layer2-Aware NAT*

draft-nishitani-cgn-02, *Common Functions of Large Scale NAT (LSN)*

RFC 4787, *Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*

RFC 5382, *NAT Behavioral Requirements for TCP*

RFC 5508, *NAT Behavioral Requirements for ICMP*

RFC 6146, *Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*

RFC 6333, *Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion*

RFC 6334, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite*

RFC 6887, *Port Control Protocol (PCP)*

RFC 6888, *Common Requirements For Carrier-Grade NATs (CGNs)*

RFC 7915, *IP/ICMP Translation Algorithm*

Network Configuration Protocol (NETCONF)

RFC 6020, *YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)*

RFC 6241, *Network Configuration Protocol (NETCONF)*

RFC 6242, *Using the NETCONF Protocol over Secure Shell (SSH)*

RFC 6243, *With-defaults Capability for NETCONF*

Open Shortest Path First (OSPF)

draft-ietf-ospf-ospfv3-lsa-extend-13, *OSPFv3 LSA Extendibility*

RFC 1586, *Guidelines for Running OSPF Over Frame Relay Networks*

RFC 1765, *OSPF Database Overflow*

RFC 2328, *OSPF Version 2*

RFC 3101, *The OSPF Not-So-Stubby Area (NSSA) Option*

RFC 3509, *Alternative Implementations of OSPF Area Border Routers*

RFC 3623, *Graceful OSPF Restart Graceful OSPF Restart* (helper mode)

RFC 3630, *Traffic Engineering (TE) Extensions to OSPF Version 2*

RFC 4203, *OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*

RFC 4222, *Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance*

RFC 4552, *Authentication/Confidentiality for OSPFv3*

RFC 4576, *Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)*

RFC 4577, *OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)*

RFC 5185, *OSPF Multi-Area Adjacency*

RFC 5187, *OSPFv3 Graceful Restart* (helper mode)

RFC 5243, *OSPF Database Exchange Summary List Optimization*

RFC 5250, *The OSPF Opaque LSA Option*

RFC 5309, *Point-to-Point Operation over LAN in Link State Routing Protocols*

RFC 5340, *OSPF for IPv6*

RFC 5709, *OSPFv2 HMAC-SHA Cryptographic Authentication*

RFC 5838, *Support of Address Families in OSPFv3*

RFC 6987, *OSPF Stub Router Advertisement*

RFC 7684, *OSPFv2 Prefix/Link Attribute Advertisement*

RFC 7770, *Extensions to OSPF for Advertising Optional Router Capabilities*

OpenConfig

gnmi.proto, *gRPC Network Management Interface (gNMI), version 0.3.1* (Subscribe RPC)

OpenFlow

ONF *OpenFlow Switch Specification Version 1.3.1* (OpenFlow-hybrid switches)

Path Computation Element Protocol (PCEP)

draft-alvarez-pce-path-profiles-04, *PCE Path Profiles*

draft-ietf-pce-segment-routing-08, *PCEP Extensions for Segment Routing*

draft-ietf-pce-stateful-pce-14, *PCEP Extensions for Stateful PCE*

RFC 5440, *Path Computation Element (PCE) Communication Protocol (PCEP)*

Point-to-Point Protocol (PPP)

RFC 1332, *The PPP Internet Protocol Control Protocol (IPCP)*

RFC 1377, *The PPP OSI Network Layer Control Protocol (OSINLCP)*

RFC 1661, *The Point-to-Point Protocol (PPP)*

RFC 1662, *PPP in HDLC-like Framing*

RFC 1877, *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*

RFC 1989, *PPP Link Quality Monitoring*

RFC 1990, *The PPP Multilink Protocol (MP)*

RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*

RFC 2153, *PPP Vendor Extensions*

RFC 2516, *A Method for Transmitting PPP Over Ethernet (PPPoE)*

RFC 2615, *PPP over SONET/SDH*

RFC 2686, *The Multi-Class Extension to Multi-Link PPP*

RFC 2878, *PPP Bridging Control Protocol (BCP)*

RFC 4638, *Accommodating a Maximum Transit Unit/Maximum Receive Unit (MTU/MRU) Greater Than 1492 in the Point-to-Point Protocol over Ethernet (PPPoE)*

RFC 5072, *IP Version 6 over PPP*

Policy Management and Credit Control

3GPP TS 29.212 Release 11, *Policy and Charging Control (PCC); Reference points* (Gx support as it applies to wireline environment (BNG))

RFC 3588, *Diameter Base Protocol*

RFC 4006, *Diameter Credit-Control Application*

Pseudowire

draft-ietf-l2vpn-vpws-iw-oam-04, *OAM Procedures for VPWS Interworking*

MFA Forum 12.0.0, *Multiservice Interworking - Ethernet over MPLS*

MFA Forum 13.0.0, *Fault Management for Multiservice Interworking v1.0*

MFA Forum 16.0.0, *Multiservice Interworking - IP over MPLS*

MFA Forum 9.0.0, *The Use of Virtual trunks for ATM/MPLS Control Plane Interworking*

RFC 3916, *Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)*

RFC 3985, *Pseudo Wire Emulation Edge-to-Edge (PWE3)*

RFC 4385, *Pseudo Wire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN*

RFC 4446, *IANA Allocations for Pseudowire Edge to Edge Emulation (PWE3)*

RFC 4447, *Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*

RFC 4448, *Encapsulation Methods for Transport of Ethernet over MPLS Networks*

RFC 4619, *Encapsulation Methods for Transport of Frame Relay over Multiprotocol Label Switching (MPLS) Networks*

RFC 4717, *Encapsulation Methods for Transport Asynchronous Transfer Mode (ATM) over MPLS Networks*

RFC 4816, *Pseudowire Emulation Edge-to-Edge (PWE3) Asynchronous Transfer Mode (ATM) Transparent Cell Transport Service*

RFC 5085, *Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires*

RFC 5659, *An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge*

RFC 5885, *Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)*

RFC 6073, *Segmented Pseudowire*

RFC 6310, *Pseudowire (PW) Operations, Administration, and Maintenance (OAM) Message Mapping*

RFC 6391, *Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network*

RFC 6575, *Address Resolution Protocol (ARP) Mediation for IP Interworking of Layer 2 VPNs*

RFC 6718, *Pseudowire Redundancy*

RFC 6829, *Label Switched Path (LSP) Ping for Pseudowire Forwarding Equivalence Classes (FECs) Advertised over IPv6*

RFC 6870, *Pseudowire Preferential Forwarding Status bit*

RFC 7023, *MPLS and Ethernet Operations, Administration, and Maintenance (OAM) Interworking*

RFC 7267, *Dynamic Placement of Multi-Segment Pseudowires*

Quality of Service (QoS)

RFC 2430, *A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE)*

RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*

RFC 2598, *An Expedited Forwarding PHB*

RFC 3140, *Per Hop Behavior Identification Codes*

RFC 3260, *New Terminology and Clarifications for Diffserv*

Remote Authentication Dial In User Service (RADIUS)

RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*

RFC 2866, *RADIUS Accounting*

RFC 2867, *RADIUS Accounting Modifications for Tunnel Protocol Support*

RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*

RFC 2869, *RADIUS Extensions*

RFC 3162, *RADIUS and IPv6*

RFC 4818, *RADIUS Delegated-IPv6-Prefix Attribute*

RFC 5176, *Dynamic Authorization Extensions to RADIUS*

RFC 6911, *RADIUS attributes for IPv6 Access Networks*

RFC 6929, *Remote Authentication Dial-In User Service (RADIUS) Protocol Extensions*

Resource Reservation Protocol — Traffic Engineering (RSVP-TE)

draft-newton-mpls-te-dynamic-overbooking-00, *A Diffserv-TE Implementation Model to dynamically change booking factors during failure events*

RFC 2702, *Requirements for Traffic Engineering over MPLS*

RFC 2747, *RSVP Cryptographic Authentication*

RFC 2961, *RSVP Refresh Overhead Reduction Extensions*

RFC 3097, *RSVP Cryptographic Authentication -- Updated Message Type Value*

RFC 3209, *RSVP-TE: Extensions to RSVP for LSP Tunnels*

RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions* (IF_ID RSVP_HOP object with unnumbered interfaces and RSVP-TE graceful restart helper procedures)

RFC 3477, *Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)*

RFC 3564, *Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering*

RFC 3906, *Calculating Interior Gateway Protocol (IGP) Routes Over Traffic Engineering Tunnels*

RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*

RFC 4124, *Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering*

RFC 4125, *Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*

RFC 4127, *Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*

RFC 4561, *Definition of a Record Route Object (RRO) Node-Id Sub-Object*

RFC 4875, *Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs)*

RFC 4950, *ICMP Extensions for Multiprotocol Label Switching*

RFC 5151, *Inter-Domain MPLS and GMPLS Traffic Engineering -- Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions*

RFC 5712, *MPLS Traffic Engineering Soft Preemption*

RFC 5817, *Graceful Shutdown in MPLS and Generalized MPLS Traffic Engineering Networks*

Routing Information Protocol (RIP)

RFC 1058, *Routing Information Protocol*

RFC 2080, *RIPng for IPv6*

RFC 2082, *RIP-2 MD5 Authentication*

RFC 2453, *RIP Version 2*

Segment Routing (SR)

draft-francois-rtgwg-segment-routing-ti-lfa-04, *Topology Independent Fast Reroute using Segment Routing*

draft-gredler-idr-bgp-ls-segment-routing-ext-03, *BGP Link-State extensions for Segment Routing*

draft-ietf-isis-segment-routing-extensions-04, *IS-IS Extensions for Segment Routing*

draft-ietf-mpls-spring-lsp-ping-02, *Label Switched Path (LSP) Ping/Trace for Segment Routing Networks Using MPLS Dataplane*

draft-ietf-ospf-segment-routing-extensions-04, *OSPF Extensions for Segment Routing*

Synchronous Optical Networking (SONET)/Synchronous Digital Hierarchy (SDH)

ANSI T1.105.03, *Jitter Network Interfaces*

ANSI T1.105.06, *Physical Layer Specifications*

ANSI T1.105.09, *Network Timing and Synchronization*

ITU-T G.703, *Physical/electrical characteristics of hierarchical digital interfaces*

ITU-T G.707, *Network node interface for the synchronous digital hierarchy (SDH)*

ITU-T G.813, *Timing characteristics of SDH equipment slave clocks (SEC)*

ITU-T G.823, *The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy*

ITU-T G.824, *The control of jitter and wander within digital networks which are based on the 1544 kbit/s hierarchy*

ITU-T G.825, *The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)*

ITU-T G.841, *Types and Characteristics of SDH Networks Protection Architecture, issued in October 1998 and as augmented by Corrigendum 1, issued in July 2002*

ITU-T G.957, *Optical interfaces for equipments and systems relating to the synchronous digital hierarchy*

Time Division Multiplexing (TDM)

ANSI T1.403, *DS1 Metallic Interface Specification*

ANSI T1.404, *DS3 Metallic Interface Specification*

Timing

GR-1244-CORE, *Clocks for the Synchronized Network: Common Generic Criteria, Issue 3, May 2005*

GR-253-CORE, *SONET Transport Systems: Common Generic Criteria. Issue 3, September 2000*

IEEE 1588-2008, *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*

ITU-T G.781, *Synchronization layer functions, issued 09/2008*

ITU-T G.813, *Timing characteristics of SDH equipment slave clocks (SEC), issued 03/2003*

ITU-T G.8261, *Timing and synchronization aspects in packet networks, issued 04/2008*

ITU-T G.8262, *Timing characteristics of synchronous Ethernet equipment slave clock (EEC), issued 08/2007*

ITU-T G.8264, *Distribution of timing information through packet networks, issued 10/2008*

ITU-T G.8265.1, *Precision time protocol telecom profile for frequency synchronization, issued 10/2010*

ITU-T G.8275.1, *Precision time protocol telecom profile for phase/time synchronization with full timing support from the network, issued 07/2014*

RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification*

Two-Way Active Measurement Protocol (TWAMP)

RFC 5357, *A Two-Way Active Measurement Protocol (TWAMP)* (server, unauthenticated mode)

RFC 5938, *Individual Session Control Feature for the Two-Way Active Measurement Protocol (TWAMP)*

RFC 6038, *Two-Way Active Measurement Protocol (TWAMP) Reflect Octets and Symmetrical Size Features*

Virtual Private LAN Service (VPLS)

RFC 4761, *Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*

RFC 4762, *Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling*

RFC 5501, *Requirements for Multicast Support in Virtual Private LAN Services*

RFC 6074, *Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)*

RFC 7041, *Extensions to the Virtual Private LAN Service (VPLS) Provider Edge (PE) Model for Provider Backbone Bridging*

RFC 7117, *Multicast in Virtual Private LAN Service (VPLS)*

Voice and Video

DVB BlueBook A86, *Transport of MPEG-2 TS Based DVB Services over IP Based Networks*

ETSI TS 101 329-5 Annex E, *QoS Measurement for VoIP - Method for determining an Equipment Impairment Factor using Passive Monitoring*

ITU-T G.1020 Appendix I, *Performance Parameter Definitions for Quality of Speech and other Voiceband Applications Utilizing IP Networks - Mean Absolute Packet Delay Variation & Markov Models*

ITU-T G.107, *The E Model - A computational model for use in planning*

ITU-T P.564, *Conformance testing for voice over IP transmission quality assessment models*

RFC 3550 Appendix A.8, *RTP: A Transport Protocol for Real-Time Applications* (estimating the interarrival jitter)

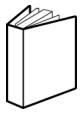
RFC 4585, *Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)*

RFC 4588, *RTP Retransmission Payload Format*

Wireless Local Area Network (WLAN) Gateway

3GPP TS 23.402, *Architecture enhancements for non-3GPP accesses* (S2a roaming based on GPRS)

Customer Document and Product Support



Customer Documentation

Customer Documentation Welcome Page

Technical Support

Product Support Portal

Documentation Feedback

Customer Documentation Feedback

3HE 11975 AAAC TQZZA 01