RADIUS Attributes

SYSTEM ADMINISTRATOR GUIDE

Contents

1 Overview

This document describes standard Remote Authentication Dial-In User Service (RADIUS) and vendor-specific attributes (VSAs) supported by the SmartEdge router and SM family chassis.

This document applies to both the Ericsson SmartEdge® and SM family routers. However, the software that applies to the SM family of systems is a subset of the SmartEdge OS; some of the functionality described in this document may not apply to SM family routers.

For information specific to the SM family chassis, including line cards, refer to the SM family chassis documentation.

For specific information about the differences between the SmartEdge and SM family routers, refer to the Technical Product Description *SM Family of Systems* (part number 5/221 02-CRA 119 1170/1) in the **Product Overview** folder of this Customer Product Information library.

For more information about RADIUS attributes, see the following documents:

- 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 3576, *Dynamic Authorization Extensions to Remote Authentication Dial-In User Service (RADIUS)*

- RFC 4818, *RADIUS Delegated-IPv6-Prefix-Attribute*

Internet Engineering Task Force (IETF) RADIUS attributes are the original set of 255 standard attributes used to communicate authentication, authorization, and accounting (AAA) information between a client and a server. Because IETF attributes are standard, the attribute data is predefined and well known so that all clients and servers can exchange AAA information. RADIUS VSAs are derived from one IETF RADIUS attribute 26, Vendor-Specific, which enables a vendor, in this case, Ericsson, to create an additional 255 attributes.

The maximum Radius TLV length is 255 (one byte). However, for the IETF attribute, the maximum string length for the attribute itself is 255-1 (for type) -1 (for length) = 253; for VSA, the maximum string length for the VSA attribute

itself is 255-1 (for type) -1 (for length) -4 (for vendor ID) -1 (for VSA type) -1 (for VSA length) = 247.

RADIUS packets and files are described further in the following sections.

1.1   RADIUS Packet Format

Figure 1 illustrates the format of a RADIUS packet.
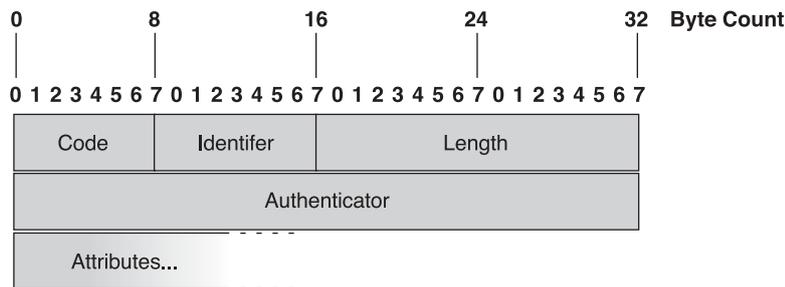
Figure 1   RADIUS Packet Format (797)

Table 1 describes the fields contained in a RADIUS packet.

Table 1   RADIUS Packet Fields

Field	Description	Platform
Code	Identifies the RADIUS packet type. The type can be one of the following: • Access-Request (1) • Access-Accept (2) • Access-Reject (3) • Accounting-Request (4) • Accounting-Response (5) • Disconnect-Request (40) • Disconnect-ACK (41) • Disconnect-NAK (42) • CoA-Request (43) • CoA-ACK (44) • CoA-NAK (45)	SmartEdge SM-Family
Identifier	Helps the RADIUS server match request and responses and detect duplicate requests.	SmartEdge SM-Family

Table 1   RADIUS Packet Fields

Field	Description	Platform
Length	Specifies the length of the entire packet.	SmartEdge
		SM-Family
Authenticator	Authenticates the reply from the RADIUS server. There are two types of authenticators: • Request-Authentication (available in Access-Request and Accounting-Request packets) • Response-Authentication (available in Access-Accept, Access Reject, Access-Challenge, and Accounting-Response packets)	SmartEdge SM-Family

1.2   Packet Types

Table 2 describes RADIUS packet types.

Table 2   RADIUS Packet Types

Type	Description	Platform
Access-Request	Sent from a client to a RADIUS server. The RADIUS server uses the packet to determine whether to allow access to a specific network access server (NAS), which permits subscriber access. Subscribers performing authentication must submit an Access-Request packet. When an Access-Request packet is received, the RADIUS server must forward a reply.	SM-Family
Access-Accept	Upon receiving an Access-Request packet, the RADIUS server sends an Access-Accept packet if all attribute values in the Access-Request packet are acceptable.	SmartEdge SM-Family
Access-Reject	Upon receiving an Access-Request packet, the RADIUS server sends an Access-Reject packet if any of the attribute values are not acceptable.	SmartEdge SM-Family
Access-Challenge	Upon receiving an Access-Request packet, the RADIUS server can send the client an Access-Challenge packet, which requires a response. If the client does not know how to respond, or if the packets are invalid, the RADIUS server discards the packets. If the client responds to the packet, a new Access-Request packet is sent with the original Access-Request packet.	SmartEdge SM-Family
Accounting-Request	Sent from a client to a RADIUS accounting server. If the RADIUS accounting server successfully records the Accounting-Request packet, it must submit an Accounting-Response packet.	SmartEdge SM-Family
Accounting-Response	Sent by the RADIUS accounting server to the client to acknowledge that the Accounting-Request has been received and recorded successfully.	SmartEdge SM-Family
CoA-Request	Sent by the RADIUS server to the NAS to dynamically change session authorizations.	SmartEdge SM-Family
CoA-Response	Sent by the NAS to the RADIUS server to acknowledge (ACK) a CoA request if the session authorizations were successfully changed. A negative-acknowledge character (NAK/NACK) is sent if the CoA request is unsuccessful.	SmartEdge SM-Family

Table 2   RADIUS Packet Types

Type	Description	Platform
Disconnect-Request	Sent by the RADIUS server to the NAS to terminate a session and discard all session context.	SmartEdge SM-Family
Disconnect-Response	Sent by the NAS to the RADIUS server to acknowledge (ACK) a disconnect request if the session is successfully terminated and the context discarded. A NAK is sent if the disconnect request is unsuccessful.	SmartEdge SM-Family

1.3   RADIUS Files

RADIUS files communicate AAA information between a client and server. These files are described in the following sections.

1.3.1   RADIUS Dictionary File

Table 3 describes the information contained in a RADIUS dictionary file.

Table 3   RADIUS Dictionary File

Name	ID	Value Type	Platform
ASCII string name of the attribute; for example, UserName.	Numerical identification of the attribute; for example, the User-Name attribute is 1.	Each attribute can be specified through one of the following value types: • binary—0 to 254 octets. • date—32-bit value in big endian order; for example, seconds since 00:00:00 GMT, JAN. 1, 1970. • ipadd—4 octets in network byte order. • integer—32-bit value in big endian order (high byte first). • string—0 to 253 octets.	SmartEdge SM-Family

An integer can be expanded to represent a string. The following example is an integer-based attribute and its corresponding string values. In this example, the values for VSA 144, Acct_Reason, describe the reason for sending subscriber accounting packets to the RADIUS server. Each value is represented by an integer:

```
#

ATTRIBUTE      Acct_Reason    144               Integer

VALUE          AAA_LOAD_ACCT_SESSION_UP          1

VALUE          AAA_LOAD_ACCT_SESSION_DOWN        2

VALUE          AAA_LOAD_ACCT_PERIODIC            3

.

.
```

1.3.2   RADIUS Clients Files

A clients file contains a list of RADIUS clients allowed to send authentication and accounting requests to the RADIUS server. To receive authentication, the client name and authentication key sent to the RADIUS server must be an exact match with the data contained in the clients file; see the following example:

```
#

Client Name       Key

10.1.1.1           test

nas-1              secret
```

1.3.3   Subscriber Files

A subscriber file contains an entry for each subscriber that the RADIUS server authenticates. The first line in any subscriber file is a "user access" line; the server must check the attributes on the first line before it can grant access to the user.

The following example allows the subscriber to access five tunnel attributes:

```
#

redback.com Password="redback" Service-Type Outbound

        Tunnel-Type = :1:L2TP

        Tunnel-Medium-Type = :1:IP

        Tunnel-Server-Endpoint = :1:10.0.0.1

        Tunnel-Password =:1:"welcome"

        Tunnel-Assignment-ID = :1:"nas"
```

2 Supported Standard RADIUS Attributes

Standard RADIUS attributes appear in the various types of RADIUS messages as described in the following sections.

2.1 Standard Attributes in Access-Accept and Accounting Messages

Table 4 describes the standard RADIUS attributes that can appear in Access-Request, Account-Request, and Access-Response messages.

Table 4   Supported Standard RADIUS Attributes

#	Attribute Name	Sent in Access-Request	Sent in Acct-Request	Receivable in Access-Response	Description	Platform
1	User-Name	Yes	Yes	No	String. Name of the user to be authenticated; only used in Access-Request packets. The `radius attribute username` command provides options to change the format of the User-Name attribute.	SmartEdge SM-Family
2	User-Password	Yes	No	No	String. Sent unless using the CHAP-Password attribute.	SmartEdge SM-Family
3	CHAP-Password	Yes	No	No	String. Sent in Access-Request packet unless using the User-Password attribute.	SmartEdge SM-Family
4	NAS-IP-Address	Yes	Yes	No	IP address. Specifies an IPv4 source IP address for RADIUS packets sent by the router. This attribute is not sent unless explicitly enabled through the `radius attribute nas-ip-address` command (in context configuration mode).	SmartEdge SM-Family
5	NAS-Port	Yes	Yes	No	Integer. This attribute is sent using the *slot-port* format. For details on this format or to modify the format in which this attribute is sent, see the `radius attribute nas-port` command.	SmartEdge SM-Family
6	Service-Type	Yes	Yes	Yes	Integer. Type of service requested or provided. Values are: • 2=Framed • 5=Outbound • 6=Administrative • 7=NAS Prompt	SmartEdge SM-Family

Table 4   Supported Standard RADIUS Attributes

#	Attribute Name	Sent in Access-Request	Sent in Acct-Request	Receivable in Access-Response	Description	Platform
7	Framed-Protocol	Yes	Yes	Yes	Integer. The value indicates the framing to be used for framed access. This attribute must not be used in a user profile designed for RFC 1483 and RFC 1490 bridged or routed circuits, or for telnet sessions. This value is sent only for Point-to-Point Protocol (PPP) service types. The value for PPP is 1.	SmartEdge SM-Family
8	Framed-IP-Address	Yes	Yes	Yes	IP address. In Accounting-Request packets, returns the IP address assigned to the subscriber either dynamically or statically. In Access-Accept packets, a return value of 255.255.255.254 or 0.0.0.0 causes the router to assign the subscriber an address from an IP address pool. This attribute is received in Access-Response messages and is sent in Access-Request messages conditioned by the **aaa hint ip address** command (in context configuration mode).	SmartEdge
9	Framed-IP-Netmask	No	Yes	Yes	IP address. Assigns a range of addresses to a subscriber circuit—it is not a netmask in the conventional sense of determining which address bits are host versus. prefix, and so on.	SmartEdge
11	Filter-Id	No	Yes	Yes	String. Specifies that inbound or outbound traffic be filtered. Use the ***in:<acl name>*** format for v4 in acl and ***out:<acl name>*** format for v4 out acl. ***ipv6:in:<acl name>*** format for v6 in acl and ***ipv6:out:<acl name>*** format for v6 out acl.	SmartEdge
12	Framed-MTU	No	No	Yes	Integer. Maximum transmission unit (MTU) to be configured for the user when it is not negotiated by some other means (such as Point-to-Point Protocol [PPP]). It is only used in Access-Accept packets.	SmartEdge SM-Family
18	Reply-Message	No	No	Yes	String. Text that can be displayed to the user. Multiple Reply-Message attributes can be included. If any are displayed, they must be displayed in the same order as they appear in the packet.	SmartEdge SM-Family

Table 4   Supported Standard RADIUS Attributes

#	Attribute Name	Sent in Access-Request	Sent in Acct-Request	Receivable in Access-Response	Description	Platform
22	Framed-Route	No	Yes	Yes	IP address. The format is `h.h.h.h/nn g.g.g.g n` where: • `h.h.h.h`=IP address of destination host or network. • `nn`=optional netmask size in bits (if not present, defaults to 32). • `g.g.g.g`=IP address of gateway. • `n`=Number of hops for this route.	SmartEdge SM-Family
24	State	No	No	Yes	Binary String.	SmartEdge SM-Family
25	Class	No	Yes	Yes	String. If received, this information must be sent on, without interpretation, in all subsequent packets sent to the RADIUS accounting server for that subscriber session.	SmartEdge
26	Vendor-Specific	Yes	Yes	No	String. Allows Ericsson to support its own VSAs, embedded with the Vendor-Id attribute set to 2352. For the VSAs supported by the router, see Table 7.	SmartEdge SM-Family
27	Session-Timeout	No	Yes	Yes	Integer. Sets the maximum number of seconds of service allowed the subscriber before termination of the session. Corresponds to the `timeout` command (in subscriber configuration mode) with the `absolute` keyword, except that the attribute requires seconds instead of minutes. The value 0 indicates that the timeout is disabled.	SmartEdge
28	Idle-Timeout	No	Yes	Yes	Integer. Sets the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session. Corresponds to the SmartEdge router `timeout idle` command (in subscriber configuration mode), except that the attribute calls for seconds instead of minutes.	SmartEdge SM-Family
30	Called-Station-Id	Yes	No	No	String. The telephone number that the call came from.	SmartEdge SM-Family

Table 4   Supported Standard RADIUS Attributes

#	Attribute Name	Sent in Access-Request	Sent in Acct-Request	Receivable in Access-Response	Description	Platform
31	Calling-Station-Id	Yes	Yes	No	Dependent on the type of subscriber terminated in the router: This attribute is not sent unless explicitly enabled through the `radius attribute calling-station-id` command (in context configuration mode).	SmartEdge
32	NAS-Identifier	Yes	Yes	No	String. Value for the system hostname.	SmartEdge SM-Family
33	Proxy_State	No	Yes	No	Binary String. Specifies the state sent by the proxy server.	SmartEdge SM-Family
40	Acct-Status-Type	No	Yes	No	Integer. Values can be: • 1=Start • 2 =Stop • 3=Interim-Updated • 7=Accounting-On • 8=Accounting-Off • 9=Tunnel Start • 10=Tunnel Stop • 12=Link Start • 13=Link Stop • 15=Reserved for failed • 101=Service-Start • 102=Service-Stop • 103=Service-Interim-Update	SmartEdge SM-Family
41	Acct-Delay-Time	No	Yes	No	Integer. Time, in seconds, for which the client has been trying to send the record.	SmartEdge SM-Family
42	Acct-Input-Octets	No	Yes	No	Integer. Number of octets that have been received from the port over the course of providing this service. Can only be present in Accounting-Request records where the Acct-Status-Type attribute is set to Stop or Update.	SmartEdge SM-Family
43	Acct-Output-Octets	No	Yes	No	Integer. Number of octets that have been sent to the port in the course of delivering this service. Can only be present in Accounting-Request records where the Acct-Status-Type attribute is set to Stop or Update.	SmartEdge SM-Family

Table 4   Supported Standard RADIUS Attributes

#	Attribute Name	Sent in Access-Request	Sent in Acct-Request	Receivable in Access-Response	Description	Platform
44	Acct-Session-Id	Yes	Yes	No	String. Unique session accounting ID to match start and stop records for in a log file. The start and stop records for a given subscriber session have the same Acct-Session-Id attribute value. The format is `cct-handle timestamp`. If service accounting is enabled with VSA 191, this attribute also includes the service accounting identifier, which is the `service-name` that is defined in VSA 190. The session accounting and service accounting identifiers are separated by a hyphen (-). By default, this attribute is sent in Accounting-Request packets. To send this attribute in Access-Request packets, you must use the `radius attribute acct-session-id` command (in context configuration mode).	SmartEdge
45	Acct-Authentic	No	Yes	No	String. Values are RADIUS and local.	SmartEdge SM-Family
46	Acct-Session-Time	No	Yes	No	Integer. Number of seconds for which the user has received service. Can only be present in Accounting-Request records where the Acct-Status-Type attribute is set to Stop or Update.	SmartEdge SM-Family
47	Acct-Input-Packets	No	Yes	No	Integer. Number of packets that have been received from the port over the course of providing this service to a framed user. Can only be present in Accounting-Request records where the Acct-Status-Type attribute is set to Stop or Update.	SmartEdge SM-Family
48	Acct-Output-Packets	No	Yes	No	Integer. Number of packets that have been sent to the port in the course of delivering this service to a Framed User. Can only be present in Accounting-Request records where the Acct-Status-Type attribute is set to Stop or Update.	SmartEdge SM-Family

Table 4   Supported Standard RADIUS Attributes

#	Attribute Name	Sent in Access-Request	Sent in Acct-Request	Receivable in Access-Response	Description	Platform
49	Acct-Terminate-Cause	No	Yes	No	Integer. Value represents the cause of session termination. Values are: • 1=User request • 2=Lost carrier • 3=Lost service • 4=Idle timeout • 5=Session timeout • 6=Admin reset • 8=Port error • 9=NAS error • 10=NAS request • 15=Service unavailable • 17=User error	SmartEdge SM-Family
50	Acct-Multi-Session-Id	No	Yes	No	String. Links multiple related sessions with a unique accounting ID.	SmartEdge SM-Family
52	Acct-Input-Gigawords	No	Yes	No	Integer. Value represents the number of times the Acct-Input-Octets counter has wrapped around 2^32 in the course of providing this service. This attribute can only be present in Accounting-Request records where the Acct-Status-Type attribute is set to Stop or Interim-Update.	SmartEdge SM-Family
53	Acct-Output-Gigawords	No	Yes	No	Integer. Value represents the number of times the Acct-Output-Octets counter has wrapped around 2^32 in the course of delivering this service. This attribute can only be present in Accounting-Request records where the Acct-Status-Type attribute is set to Stop or Interim-Update.	SmartEdge SM-Family
55	Event-Timestamp	No	Yes	No	Integer. Value represents the time this event occurred on the NAS, in seconds, since January 1, 1970 00:00 UTC.	SmartEdge SM-Family
61	NAS-Port-Type	Yes	Yes	No	Integer. The default value is either 0 or 5, indicating an asynchronous connection through a console port or a connection through a transport protocol, respectively, depending on how the subscriber is connected to its authenticating NAS. The range of values is 0 to 255.	SmartEdge

Table 4   Supported Standard RADIUS Attributes

#	Attribute Name	Sent in Access-Request	Sent in Acct-Request	Receivable in Access-Response	Description	Platform
					Values 0 to 19 are as follows: • 0—async • 1—sync • 2—ISDN (sync) • 3—ISDN (async V120) • 4—ISDN (async V110) • 5—Virtual • 6—PIAFS (wireless ISDN used in Japan) • 7—HDLC (clear-channel) • 8—X.25 • 9—X.75 • 10—G3_Fax (G.3 Fax) • 11—SDSL (symmetric DSL) • 12—ADSL_CAP (asymmetric DSL, Carrierless Amplitude Phase Modulation) • 13—ADSL_DMT (asymmetric DSL, discrete multi-tone) • 14—IDSL (ISDN digital subscriber line) • 15—Ethernet • 16—xDSL (digital subscriber line of unknown type) • 17—Cable • 18—Wireless (wireless—Other) • 19—Wireless_802_11 (wireless—IEEE 802.11) You can modify the value of this attribute through the `radius attribute nas-port-type` command (in ATM profile, dot1q profile, link-group, or port configuration mode).	SmartEdge
62	Port-Limit	No	Yes	Yes	Integer. Maximum number of sessions a particular subscriber can have active at one time.	SmartEdge SM-Family
64	Tunnel-Type	No	Yes	Yes	Integer. Value indicates the tunneling protocol to be used. The supported value is 3, which indicates the Layer 2 Tunneling Protocol (L2TP).	SmartEdge SM-Family
65	Tunnel-Medium-Type	No	Yes	Yes	Integer. Value represents the transport medium to use when creating an L2TP tunnel for protocols that can operate over multiple transports. The supported value is 1, which indicates IPv4.	SmartEdge SM-Family
66	Tunnel-Client-Endpoint	No	Yes	Yes	String. Fully qualified domain name or IP address of the initiator end of an L2TP tunnel.	SmartEdge SM-Family
67	Tunnel-Server-Endpoint	No	Yes	Yes	String. Fully qualified domain name or IP address of the server end of an L2TP tunnel.	SmartEdge SM-Family

Table 4   Supported Standard RADIUS Attributes

#	Attribute Name	Sent in Access-Request	Sent in Acct-Request	Receivable in Access-Response	Description	Platform
68	Acct-Tunnel-Connection	No	Yes	No	String. Unique accounting ID to easily match start and stop records in a log file for L2TP sessions. The start and stop records for a given session will have the same Acct-Tunnel-Connection attribute value.	SmartEdge SM-Family
69	Tunnel-Password	No	No	Yes	String. Password. Only used in Access-Accept packets.	SmartEdge SM-Family
77	Connect-Info	Yes	Yes	No	String containing either: • An ATM, 802.1Q, or Frame Relay profile name sent to the RADIUS server. • The values from L2TP attribute-value pairs (AVPs) 24 and 38 in the Tx/Rx format. Speeds are in bits-per-second.	SmartEdge SM-Family
80	Message-Authenticator	Yes	No	Yes	String. Signs access requests to prevent spoofing.	SmartEdge SM-Family
81	Tunnel-Pvt-Grp-ID	Yes	Yes	Yes	String. Indicates the group ID for a particular tunneled session. If the tunnel initiator can pre-determine the group resulting from a particular connection, the Tunnel-Private-Group-ID Attribute may be included in the Access-Request packet and should be included in the Access-Accept packet (if this tunnel session is to be treated as belonging to a particular private group). Private groups may be used to associate a tunneled session with a particular group of users.	SmartEdge
82	Tunnel-Assignment-ID	No	Yes	Yes	String. Used to distinguish between different peers with configurations that use the same IP address. If no Tunnel-Client-Endpoint or Tunnel-Server-Endpoint attribute is supplied with this tag, and if the Tunnel-Assignment-ID matches the name of a locally configured peer, the session will be tunneled to that peer.	SmartEdge SM-Family
83	Tunnel-Preference	No	No	Yes	String. If more than one set of tunneling attributes is returned by the RADIUS server to the tunnel initiator, this attribute should be included in all sets to indicate the preference assigned to each set; the lower the value for a set, the more preferable it is.	SmartEdge SM-Family

Table 4   Supported Standard RADIUS Attributes

#	Attribute Name	Sent in Access-Request	Sent in Acct-Request	Receivable in Access-Response	Description	Platform
85	Acct-Interim-Interval	No	No	Yes	Integer. The Value field indicates the number of seconds between each interim update sent from the NAS for this specific session. The value must be between 600 and 604,800 seconds (7 days). Any value outside this range logs a message to the system and the value resets to the corresponding minimum or maximum allowed value. Before you set this value, consider the possible impact to network traffic.	SmartEdge SM-Family
87	NAS-Port-ID	Yes	Yes	No	String. By default, this attribute is sent in RADIUS packets. The default format is: `slot/port` `[vpi-vci vpi vci`|`vlan-id` `[tunl-vlan-id:]pvc-vlan-id]` `[pppoe sess-id` | `clips sess-id]`. where `slot` and `port` are each 4 bits and `tunl-vlan-id` and `pvc-vlan-id` are each 12 bits. The `tunl-vlan-id` field is 0 if it does not exist. For example, 4/1 vpi-vci 207 138 pppoe 5. Use the `radius attribute nas-port-id` command (in context configuration mode) to specify another format for this attribute.	SmartEdge SM-Family
88	Framed-Pool	No	Yes	Yes	String. Name of the interface or IP pool used to assign an IP pool address to the subscriber. The behavior is identical to vendor VSA 36, IP-Address-Pool-Name. If both the Framed-Pool and IP-Address-Pool-Name attributes are both received in a RADIUS Access-Accept packet, Framed-Pool takes precedence and is applied.	SmartEdge
89	CUI	Yes	Yes	Yes	String. Optional. Chargeable User Identify (CUI). Identifies users when they roam outside their home network.	SmartEdge SM-Family
90	Tunnel-Client-Auth-ID	No	Yes	Yes	String. Defines the local hostname provided to remote tunnel peer (used during tunnel setup). The behavior is identical to vendor VSA 16, Tunnel-Local-Name.	SmartEdge SM-Family

Table 4   Supported Standard RADIUS Attributes

#	Attribute Name	Sent in Access-Request	Sent in Acct-Request	Receivable in Access-Response	Description	Platform
91	Tunnel-Server-Auth-ID	No	Yes	Yes	String. Defines an alias for the remote peer name. The value of this attribute must match the value of the hostname AVP that the peer sends in the SCCRQ or SCCRP message (depending on the tunnel initiator).	SmartEdge SM-Family
95	NAS-IPv6-Address	Yes	Yes	No	IP address. Specifies an IPv6 source IP address of the Network Access Server (NAS) in RADIUS Access-Request and Access-Accounting request packets configured using the CLI. These RADIUS packets are sent by the router. This attribute is not sent unless explicitly enabled through the `radius attribute nas-ipv6 address interface <name>` command (in context configuration mode). For more information about NAS and RADIUS, see *Configuring RADIUS*.	SmartEdge
96	Framed-Interface-ID	No	Yes	Yes	64-bit integer. Provides an interface ID for PPP clients that cannot generate their own interface ID. This value is sent in the Access-Response (Access-Accept) message for an IPv6 subscriber. When this value is in the authentication request, the AAA client receives this attribute from the authentication response.	SmartEdge
97	Framed-IPv6-Prefix	No	Yes	Yes	Binary. Used for stateless address autoconfiguration. Indicates the Framed-IPv6-Prefix to be assigned to the user. The Framed-IPv6-Prefix is also sent if the prefixes are applied in the a subscriber record.	SmartEdge
99	Framed-IPv6-Route	No	Yes	Yes	String. Provides routing information to be configured for the user on the NAS.	SmartEdge
100	Framed-IPv6-Pool	No	Yes	Yes	String. Name of a shared IPv6 prefix pool that is configured under the same context as the subscriber. The subscriber obtains its IPv6 prefixes from the specified IPv6 pool.	SmartEdge

Table 4   Supported Standard RADIUS Attributes

#	Attribute Name	Sent in Access-Request	Sent in Acct-Request	Receivable in Access-Response	Description	Platform
123	Delegated-IPv6-Prefix	No	Yes	Yes	Binary. Indicates the IPv6 prefix to be delegated to the subscriber using DHCPv6. This value is sent in Access-Accept and Accounting-Request messages. Multiple instances of this attribute can be present in one RADIUS packet. The Delegated-IPv6-Prefix is also sent if the prefixes are applied in the subscriber record.	SmartEdge
242	Ascend_Data_Filter	No	Yes	Yes	Binary String.	SmartEdge SM-Family

2.2   Standard RADIUS Attributes in CoA and Disconnect Messages

Table 5 lists the standard RADIUS attributes that can appear in CoA-Request, CoA-Response, Disconnect-Request, and Disconnect-Response messages. For details about these standard attributes, see Table 5.

Table 5   Standard RADIUS Attributes in CoA and Disconnect Messages

#	Attribute Name	Sent in CoA Request	Sent in CoA Response	Sent in Disconnect Request	Sent in Disconnect Response	
1	User-Name	Yes	No	Yes	No	SmartEdge SM-Family
4	NAS-IP-Address[1]	No	No	No	No	SmartEdge SM-Family
5	NAS-Port	Yes	No	Yes	No	SmartEdge SM-Family
6	Service-Type	Yes	Yes[2]	Yes	Yes[3]	SmartEdge SM-Family
7	Framed-Protocol	Yes	No	No	No	SmartEdge SM-Family
8	Framed-IP-Address	Yes	No	Yes	No	SmartEdge SM-Family
9	Framed-IP-Netmask	Yes	No	No	No	SmartEdge SM-Family
11	Filter-Id	Yes	No	No	No	SmartEdge SM-Family

Table 5   Standard RADIUS Attributes in CoA and Disconnect Messages

#	Attribute Name	Sent in CoA Request	Sent in CoA Response	Sent in Disconnect Request	Sent in Disconnect Response	
12	Framed-MTU	Yes	No	No	No	SmartEdge SM-Family
18	Reply-Message	Yes	No	Yes	No	SmartEdge SM-Family
22	Framed-Route	Yes	No	No	No	SmartEdge SM-Family
24	State	Yes	Yes	Yes	Yes	SmartEdge SM-Family
25	Class	Yes	No	Yes	No	SmartEdge SM-Family
26	Vendor-Specific	Yes	No	Yes	No	SmartEdge SM-Family
27	Session-Timeout	Yes	No	No	No	SmartEdge SM-Family
28	Idle-Timeout	Yes	No	No	No	SmartEdge SM-Family
30	Called-Station-Id	Yes	No	Yes	No	SmartEdge SM-Family
31	Calling-Station-Id	Yes	No	Yes	No	SmartEdge SM-Family
32	NAS-Identifier	Yes	No	Yes	No	SmartEdge SM-Family
33	Proxy_State	Yes	Yes	Yes	Yes	SmartEdge SM-Family
44	Acct-Session-Id	Yes	No	Yes	No	SmartEdge SM-Family
50	Acct-Multi-Session-Id	Yes	No	Yes	No	SmartEdge SM-Family
55	Event-Timestamp	Yes	Yes	Yes	Yes	SmartEdge SM-Family
61	NAS-Port-Type	Yes	No	Yes	No	SmartEdge SM-Family
62	Port-Limit	Yes	No	No	No	SmartEdge SM-Family
64	Tunnel-Type	Yes	No	No	No	SmartEdge SM-Family

Table 5   Standard RADIUS Attributes in CoA and Disconnect Messages

#	Attribute Name	Sent in CoA Request	Sent in CoA Response	Sent in Disconnect Request	Sent in Disconnect Response	
65	Tunnel-Medium-Type	Yes	No	No	No	SmartEdge SM-Family
66	Tunnel-Client-Endpoint	Yes	No	No	No	SmartEdge SM-Family
67	Tunnel-Server-Endpoint	Yes	No	No	No	SmartEdge SM-Family
69	Tunnel-Password	Yes	No	No	No	SmartEdge SM-Family
81	Tunnel_Pvt_Grp_ID	Yes	Yes	Yes		SmartEdge SM-Family
82	Tunnel-Assignment-ID	Yes	No	No	No	SmartEdge SM-Family
83	Tunnel-Preference	Yes	No	No	No	SmartEdge SM-Family
85	Acct_Interim_Interval	Yes	No	No	No	SmartEdge SM-Family
87	NAS-Port-Id	Yes	No	Yes	No	SmartEdge SM-Family
90	Tunnel-Client-Auth-ID	Yes	No	No	No	SmartEdge SM-Family
91	Tunnel-Server-Auth-ID	Yes	No	No	No	SmartEdge SM-Family
95	NAS-IPv6-Address	No	No	No	No	SmartEdge
96	Framed-Interface-Id	No	No	No	No	SmartEdge SM-Family
97	Framed-IPv6-Prefix	No	No	No	No	SmartEdge
99	Framed-IPv6-Route	No	No	No	No	SmartEdge
101	Error-Cause	No	Yes[1]	No	Yes	SmartEdge SM-Family
123	Delegated-IPv6-Prefix	No	No	No	No	SmartEdge
242	Ascend_Data_Filter	Yes	No	No	No	SmartEdge SM-Family

(1) Ignored if received.
(2) Sent in NAK message only.
(3) Sent in NAK message only.

2.3 Standard RADIUS Attributes That Can Be Reauthorized

Table 6 lists the standard RADIUS attributes that are reauthorized when you enter the **reauthorize** command (in exec mode).

Table 6   Standard RADIUS Attributes Supported by Reauthorization

#	Attribute Name	Description	Platform
11	Filter-Id	Filters inbound or outbound traffic through an access control list (ACL).	SmartEdge SM-Family
25	Class	Forwards the information sent by the RADIUS server to the router, without interpretation, in subsequent accounting messages to the RADIUS accounting server for that subscriber session.	SmartEdge
26	Vendor_Specific	Allows Ericsson to support its own VSAs.	SmartEdge SM-Family
27	Session-Timeout	Sets the in-service time allowed before the session terminates.	SmartEdge SM-Family
28	Idle-Timeout	Sets the idle time allowed before the session terminates.	SmartEdge SM-Family
85	Acct_Interim_Interval	Sets the value to an integer.	SmartEdge SM-Family
242	Ascend_Data_Filter	Allows multiple values.	SmartEdge SM-Family

3 Vendor VSAs Provided by Ericsson AB

Vendor VSAs appear in the various types of RADIUS messages as described in the following sections.

Note: The VSA names in this document may not agree with the names for Vendor VSAs in your RADIUS system, because your RADIUS administrators may have customized the VSA names. Use the RADIUS dictionary file to map the VSA numbers to names; see Section 1.3.1 on page 4.

3.1 Vendor VSAs in Access-Accept and Accounting Messages

Table 7 lists the supported vendor VSAs that can appear in Access-Request, Account-Request, and Access-Response messages.

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform
1	Client-DNS-Pri	No	Yes	Yes	IP address of the primary DNS server for this subscriber's connection.	SmartEdge
2	Client-DNS-Sec	No	Yes	Yes	IP address of the secondary DNS server for this subscriber's connection.	SmartEdge
3	DHCP-Max-Leases	No	Yes	Yes	Integer. Maximum number of DHCP addresses this subscriber can allocate to hosts. The range of values is 1 to 255.	SmartEdge
4	Context-Name	No	Yes	Yes	Binds the subscriber session to specified context, overriding the structured username. This information is only interpreted when global AAA is enabled.	SmartEdge
5	Bridge-Group	No	No	Yes	String. Bridge group name; attaches subscriber to the named bridge group.	SmartEdge
6	BG-Aging-Time	No	No	Yes	String. bg-name:val; configures bridge aging time for subscriber attaching to the named bridge group.	SmartEdge
7	BG-Path-Cost	No	No	Yes	String. bg-name:val; configures bridge path cost for subscriber attaching to the named bridge group.	SM-Family

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform
8	BG-Span-Dis	No	No	Yes	String. bg-name:val; disables spanning tree for subscriber attaching to the named bridge group. The val argument can have the following values: • 1 = TRUE • 2 = FALSE	SmartEdge
9	BG-Trans-BPDU	No	No	Yes	String. bg-name:val; sends transparent spanning tree bridge protocol data units (BPDUs) for a subscriber attaching to the named bridge group. The val argument can have the following values: • 1 = TRUE • 2 = FALSE	SmartEdge
14	Source-Validation	No	Yes	Yes	Integer. Enables source validation for subscriber, according to one of the following values: • 1=TRUE • 0=FALSE	SmartEdge
15	Tunnel-Domain	No	No	Yes	Integer. Binds the subscriber to a tunnel based on the domain name portion of the username, according to one of the following values: • 1=TRUE • 0=FALSE	SmartEdge
16	Tunnel-Local-Name	No	No	Yes	String. Defines the local hostname provided to the remote peer during tunnel setup.	SmartEdge SM-Family
17	Tunnel-Remote-Name	No	No	Yes	String. Defines an alias for the remote peer name.	SmartEdge SM-Family
18	Tunnel-Function	No	Yes	Yes	Integer. Determines this tunnel configuration as a LAC-only endpoint or an LNS endpoint, according to one of the following values: • 1=LAC only • 2=LNS only	SmartEdge SM-Family
19	Tunnel_Flow_Control	Yes	Yes	No	Integer. Specifies using data message sequencing for the L2TP peer (LAC or LNS) in the L2TP data channel.	SmartEdge SM-Family

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Recei ved in Access-Respons	Notes	Platform
20	Tunnel_Static	Yes	Yes	No	Integer. Specifies the static routes configured for a given tunnel.	SmartEdge SM-Family
21	Tunnel-Max-Sessions	No	Yes	Yes	Integer. Limits the number of sessions per tunnel using this tunnel configuration.	SmartEdge SM-Family
22	Tunnel-Max-Tunnels	No	Yes	Yes	Integer. Limits the number of tunnels that can be initiated using this tunnel configuration.	SmartEdge SM-Family
23	Tunnel-Session-Auth	No	No	Yes	Integer. Specifies the authentication method to use during PPP authentication, according to one of the following values: • 1=CHAP • 2=PAP • 3=CHAP-PAP	SmartEdge SM-Family
24	Tunnel-Window	No	No	Yes	Integer. Configures the receive window size for incoming L2TP messages.	SmartEdge SM-Family
25	Tunnel-Retransmit	No	No	Yes	Integer. Specifies the number of times the router retransmits a control message.	SmartEdge SM-Family
26	Tunnel-Cmd-Timeout	No	No	Yes	Integer. Specifies the number of seconds for the timeout interval between control message retransmissions.	SmartEdge SM-Family
27	PPPOE-URL	No	Yes	Yes	String in PPPoE URL format. Defines the PPPoE URL that is sent to the remote PPPoE client in the PADM packet.	SmartEdge SM-Family
28	PPPOE-MOTM	No	Yes	Yes	String. Defines the PPPoE MOTM message that is sent to the remote PPPoE client in the PADM packet.	SmartEdge SM-Family
29	Tunnel-Group	No	Yes	Yes	Integer. Indicates whether this record is a tunnel group with a list of member peers: • 1 = TRUE • 0 = FALSE	SmartEdge SM-Family
30	Tunnel-Context	No	Yes	Yes	String. Context name. Used in a DNIS peer record, this attribute specifies the context where the named peer should be found.	SmartEdge SM-Family

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform
31	Tunnel-Algorithm	No	No	Yes	Integer. Specifies the session distribution algorithm used to choose between the peer configurations in the RADIUS response. This VSA instructs the router on how to interpret standard RADIUS attribute 83, Tunnel-Preference, according to one of the following values: • 1=Priority • 2=Load-Balance • 3=Weighted round-robin	SmartEdge SM-Family
32	Tunnel-Deadtime	No	No	Yes	Integer. Specifies the number of minutes during which no sessions are attempted to an L2TP peer when the peer is down.	SmartEdge SM-Family
33	Mcast-Send	No	Yes	Yes	Integer. Defines whether the subscriber can send multicast packets, according to one of the following values: • 1=NO SEND • 2=SEND • 3=UNSOLICITED SEND	SmartEdge
34	Mcast-Receive	No	Yes	Yes	Integer. Defines whether the subscriber can receive multicast packets, according to one of the following values: • 1=NO RECEIVE • 2=RECEIVE	SmartEdge
35	Mcast-MaxGroups	No	Yes	Yes	Integer. Specifies the maximum number of multicast groups of which the subscriber can be a member.	SmartEdge
36	Ip-Address-Pool-Name	No	Yes	Yes	String. Name of the interface or IP pool used to assign an IP pool address to the subscriber.	SmartEdge
37	Tunnel-DNIS	No	Yes	Yes	Integer. L2TP peer parameter specifying if incoming sessions from this peer are to be switched based on the incoming DNIS AVP if present or on the incoming DNIS AVP only (terminated if no DNIS AVP is present): • 1 = DNIS • 2 = DNIS ONLY	SmartEdge SM-Family
38	Medium-Type	Yes	Yes	No	Integer. Contains the medium type of the circuit. The system sets this value to DSL for CLIPS and PPP subscribers.	SmartEdge

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform
39	PVC-Encapsulation-Type	No	No	Yes	Integer. Encapsulation type to be applied to the circuit: • 2 = Routed 1483 • 4 = ATM multi • 5 = Bridged 1483 • 6 = ATM PPP • 7 = ATM PPP serial • 8 = ATM PPP NLPID • 9 = ATM PPP auto • 10 = ATM PPPoE • 12 = ATM PPP LLC • 22 = Ethernet IPoE • 23 = Ethernet PPPoE • 24 = Ethernet dot1q • 26 = Ethernet dot1q pppoe • 31 = Ethernet dot1q tunnel pppoe • 32 = Ethernet dot1q multi • 33 = Ethernet dot1q tunnel multi	SmartEdge SM-Family
40	PVC-Profile-Name	No	No	Yes	String. Name of the ATM profile that is assigned to the subscriber record, a named profile, or the default profile, using the **shaping profile** command (in subscriber configuration mode), to use for this circuit.	SmartEdge
42	Bind-Type	No	No	Yes	Integer. Binding type to be applied to this circuit: • 1 = authentication • 3 = interface • 4 = subscriber • 14 = autosubscriber • CCOD (circuit creation on demand) circuits support only subscriber bind types.	SmartEdge SM-Family

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform
43	Bind-Auth-Protocol	No	No	Yes	Integer. Authentication protocol to use for this circuit: • 1 = PAP • 2 = CHAP • 4 = CHAP PAP • 5 = AAA-PPP-CHAP-WAIT-PAP • 7 = PAP CHAP	SmartEdge SM-Family
44	Bind-Auth-Max-Sessions	No	No	Yes	Integer. Maximum number of PPPoE sessions allowed to be created for this circuit. Also specifies the same for PPPoE sessions tunneled with Ethernet encapsulation over L2TP on the LNS.	SmartEdge SM-Family
45	Bind-Bypass-Bypass	No	No	Yes	String. Name of the bypass being bound.	SmartEdge SM-Family
46	Bind-Auth-Context	No	No	Yes	String. Bind authentication context name. Also specifies the same for PPPoE sessions tunneled with Ethernet encapsulation over L2TP on the LNS.	SmartEdge SM-Family
47	Bind-Auth-Service-Grp	No	No	Yes	String. Bind authentication service group name. Also specifies the same for PPPoE sessions tunneled with Ethernet encapsulation over L2TP on the LNS.	SmartEdge SM-Family
48	Bind-Bypass-Context	No	No	Yes	String. Bind bypass context name.	SmartEdge SM-Family
49	Bind-Int-Context	No	No	Yes	String. Bind interface context name. Also specifies the same for IP bridging sessions tunneled with Ethernet encapsulation over L2TP on the LNS.	SmartEdge SM-Family
50	Bind-Tun-Context	No	No	Yes	String. Bind tunnel context name.	SmartEdge SM-Family
51	Bind-Ses-Context	No	No	Yes	String. Bind session context name.	SmartEdge SM-Family
52	Bind-Dot1q-Slot	No	No	Yes	Integer. Bind 802.1Q slot number.	SmartEdge SM-Family
53	Bind-Dot1q-Port	No	No	Yes	Integer. Bind 802.1Q port number.	SmartEdge SM-Family
54	Bind-Dot1q-Vlan-Tag-Id	No	No	Yes	Integer. Bind 802.1Q VLAN tag ID.	SmartEdge SM-Family

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform
55	Bind-Int-Interface-Name	No	No	Yes	String. Bind interface name. Also specifies the same for IP bridging sessions tunneled with Ethernet encapsulation over L2TP on the LNS.	SmartEdge SM-Family
56	Bind-L2TP-Tunnel-Name	No	No	Yes	String. Bind L2TP tunnel name.	SmartEdge SM-Family
57	Bind-L2TP-Flow-Control	No	No	Yes	Integer. Bind L2TP flow control.	SmartEdge SM-Family
58	Bind-Sub-User-At-Context	No	No	Yes	String. Bind subscriber context name.	SmartEdge
59	Bind-Sub-Password	No	No	Yes	String. Bind subscriber password.	SmartEdge
60	Ip-Host-Addr	No	No	Yes	String in the form $A.B.C.D$ $hh:hh:hh:hh:hh:hh$. IP host address and MAC address. A space must separate the IP address from the MAC address.	SmartEdge SM-Family

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Recei ved in Access-Respons	Notes	Platform
61	Ip_Tos_Field	No	No	Yes	Integer. Specifies the value of the IP ToS field. Used for soft QoS: • 0 = normal • 1 = min-cost only • 2 = max-reliability only • 3 = max-reliability plus min-cost • 4 = max-throughput only • 5 = max-throughput plus min-cost • 6 = max-throughput plus max-reliability • 7 = max-throughput plus max-reliability plus min-cost • 8 = min-delay only • 9 = min-delay plus min-cost • 10 = min-delay plus max-reliability • 11 = min-delay plus max-reliability plus min-cost • 12 = min-delay plus max-throughput • 13 = min-delay plus max-throughput plus min-cost • 14 = min-delay plus max-throughput plus max-reliability • 15 = min-delay plus max-throughput plus max-reliability plus min-cost	SmartEdge SM-Family
62	NAS-Real-Port	Yes	Yes	No	Integer. Indicates the port number of the physical circuit on which the session was received. The format (in bits) is: SSSSPPPPCCCCCCCCCCCCC CCCCCCCCCCCC where: • S = Slot • P = Port • C = Circuit (for ATM, 8-bits of VPI, and 16-bits of VCI)	SmartEdge SM-Family
63	Tunnel-Session-Auth -Ctx	No	Yes	Yes	String. L2TP peer parameter that specifies the name of the context in which all incoming PPP over L2TP sessions should be authenticated, regardless of the domain specified in the username.	SmartEdge SM-Family

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform
64	Tunnel-Session-Auth-Service-Grp	No	Yes	Yes	String. L2TP peer parameter specifying the service group (service access control list [ACL]) to be used for all incoming PPP over L2TP sessions.	SmartEdge SM-Family
67	Tunnel-Police-Rate	No	Yes	Yes	4-byte integer. L2TP or GRE peer parameter specifying the policing rate for a tunnel in kbps. Valid range of values is 10 to 1,250,000 kbps. If this parameter is configured, the Tunnel-Police-Burst must also be configured.	SmartEdge SM-Family
68	Tunnel-Police-Burst	No	Yes	Yes	4-byte integer. L2TP or GRE peer parameter specifying the policing burst for a tunnel in bytes. Valid range of values is 0 to 1,562,500,000 bytes. If this parameter is configured, the Tunnel-Police-Rate must also be configured.	SmartEdge SM-Family
69	Tunnel-L2F-Second-Password	No	Yes	Yes	String. L2F peer parameter specifying the password string used to authenticate the L2F remote peer. [1]	SmartEdge SM-Family
70	ACL-Definition	No	Yes	Yes	String. Used to define ACL definitions in the RADIUS database. The ACL-Name attribute is the username and the Service-Type attribute must be set to Access-Control-List. The data content of this attribute contains ACL definitions similar to the command-line interface (CLI).	SmartEdge SM-Family
71	PPPoE-IP-Route-Add	No	Yes	Yes	String. Allows the PPPoE subscriber routing table to be populated in terms of what routes to be installed if multiple PPPoE sessions exist. A more granular set of routes can be achieved when multiple sessions are active to the client. The format is $h.h.h.h\ nn\ g.g.g.g\ m$ where: • $h.h.h.h$=IP address of destination host or network. • nn=optional netmask size in bits (if not present, defaults to 32). • $g.g.g.g$=IP address of gateway. • m=Number of hops for this route. If the first byte of VSA 71 is 121 (classless static route), then this VSA is used to handle the DHCP option 121.	SmartEdge

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform
72	TTY-Level-Start	No	No	Yes	Integer. Indicates the starting privilege level for the administrator. The range of values is 0 to 15 and the value must be less than or equal to the value of TTY-Level-Max.	SmartEdge SM-Family
73	TTY-Level-Max	No	No	Yes	Integer. Indicates the maximum privilege level for the administrator. The range of values is 0 to 15, and the value must be greater than or equal to the value of TTY-Level-Start.	SmartEdge SM-Family
74	Tunnel-Checksum	No	Yes	Yes	Integer. Enables GRE checksums. When enabled, a checksum is computed for each outgoing GRE packet. This allows the remote system to verify the integrity of each packet. Incoming packets that fail the checksum are discarded. A value of 1 equals enabled. Any other value for this attribute equals disabled.	SmartEdge SM-Family
75	Tunnel-Profile	No	No	Yes	String. Attaches a profile to the tunnel. Used when configuring a tunnel from a RADIUS server. A Tunnel-Profile attribute in a subscriber record is ignored.	SmartEdge SM-Family
78	Tunnel-Client-VPN	No	Yes	Yes	String. Name of the target context (a virtual private network [VPN]) on the client side of the tunnel. Required for GRE. If omitted, the system automatically sets the value equal to the value set for the Tunnel-Server-VPN attribute.	SmartEdge SM-Family
79	Tunnel-Server-VPN	No	Yes	Yes	String. Name of the target context (VPN) on the server side of the tunnel.	SmartEdge SM-Family
85	Tunnel-Hello-Timer	No	No	Yes	Integer. Hello timer (in seconds) representing the time the tunnel is silent before it transmits a hello message. It is configured using the `hello-timer` command (in L2TP peer configuration mode).	SmartEdge SM-Family
86	Redback-Reason	No	Yes	No	Integer. If the NetOp Policy Manager (PM) sends the router (through SNMP) a non-zero clear reason while trying to clear (bounce) the subscriber session, this clear reason value is sent to the RADIUS server in the RADIUS accounting Stop packet in this VSA.	SmartEdge
87	Qos_Policing	No	Yes	Yes	String. Attaches a QoS policing policy to the subscriber session.	SmartEdge
88	Qos_Metering	No	Yes	Yes	String. Attaches a QoS metering policy to the subscriber session.	SmartEdge

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform
89	Qos_Queuing	No	Yes	Yes	String. Attaches a QoS queuing policy of any type supported by the circuit to the subscriber session.	SmartEdge
90	Igmp_Svc_Prof_Id	No	Yes	Yes	String. Name of the IGMP service profile that is applied to the subscriber session.	SmartEdge
91	Sub_Profile_Name	No	Yes	Yes	Name of the subscriber profile that is applied to the subscriber session.	SmartEdge
92	Forward-Policy	No	Yes	Yes	String. Attaches an in or out forward policy to the subscriber session. The forward policy is in the following format `in:`*`forward-policy-name`* `out:`*`forward-policy-name`*	SmartEdge
94	Reauth-String	No	No	Yes	String. The format is: `ID-type;subID;attr-num;attr-value;attr-num;attr-value...` When the `ID-type` is 1, the `subID` is read as a RADIUS accounting session ID. When the `ID-type` is 2, the `subID` is read as a name. The semicolon (`;`) acts as a delimiter. `Attr-num` is an integer that identifies a RADIUS attribute. For example, standard RADIUS attribute 11 (Filter-Id) for an access control list (ACL) or vendor VSA 87 (Qos_Policing) for a QoS policing policy. (vendor VSAs include the Ericsson prefix, 2352.) `Attr-value` is the value of the RADIUS attribute specified by `attr-num`.	SmartEdge
95	Reauth-More	No	No	Yes	Integer. 0 or 1 (False or True).	SmartEdge SM-Family
96	Agent-Remote-Id	Yes	Yes	No	String. Used for two types of subscriber sessions: • Incoming CLIPS sessions to the router from a DHCP relay network. This is suboption 2 in a DHCP option 82 packet. • PPPoE sessions. Sent by the PPP client in the PADR. This attribute can also be set through the **`radius attribute calling-station-id`** and **`radius attribute nas-port-id`** commands in context configuration mode.	SmartEdge

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform
97	Agent-Circuit-Id	Yes	Yes	No	String. Used for two types of subscriber sessions: • CLIPS sessions coming into the router by way of a DHCP relay network. This is suboption 1 in a DHCP option 82 packet. • PPPoE sessions. Sent by the PPP client in the PADR. This attribute can also be set through the `radius attribute calling-station-id` and `radius attribute nas-port-id` commands in context configuration mode.	SmartEdge
98	Platform-Type	Yes	Yes	No	Integer. Indicates the Ericsson product family from which the RADIUS access request is sent. The supported values are: • 2=PLATFORM_TYPE_SE800 • 3=PLATFORM_TYPE_SE400	SmartEdge SM-Family
99	Client_NBNS_Pri	No	Yes	Yes	IP address. Configures the IP address of a primary NetBios Name Server (NBNS) that the subscriber must use.	SmartEdge
100	Client_NBNS_Sec	No	Yes	Yes	IP address. Configures the IP address of a secondary NBNS that the subscriber must use.	SmartEdge
101	Shaping-Profile-Name	No	Yes	Yes	String. Name of the ATM shaping profile.	SmartEdge SM-Family
104	IP-Interface-Name	No	Yes	Yes	String. Interface name. Binds a subscriber to the specified interface. This VSA is used in conjunction with VSA 3, DHCP-Max-Leases. This attribute can also be set through the `ip interface name` command (in subscriber configuration mode).	SmartEdge
105	NAT-Policy-Name	No	Yes	Yes	String. NAT policy name. Attaches the specified NAT policy to a subscriber.	SmartEdge
107	HTTP-Redirect-Profile-Name	No	Yes (alive/ and stop records only)	Yes	String of up to 32 characters. HTTP redirect profile name.	SmartEdge

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform
108	Bind-Auto-Sub-User	No	No	Yes	String. Subscriber name prefix as specified by the `bind auto-subscriber` command (in ATM PVC, CLIPS PVC, or dot1q PVC configuration mode). The prefix is included in the automatically generated subscriber name. For more information about this command and the format for the automatically generated subscriber name, see *Configuring Bindings*.	SmartEdge
109	Bind-Auto-Sub-Context	No	No	Yes	String. Name of context in which the subscriber is bound with the `bind auto-subscriber` command (in ATM PVC, CLIPS PVC, or dot1q PVC configuration mode). For more information about this command, see *Configuring Bindings*.	SmartEdge
110	Bind-Auto-Sub-Password	No	No	Yes	String. Password prefix as specified by the `bind auto-subscriber` command (in ATM PVC, CLIPS PVC, or dot1q PVC configuration mode). The prefix is included in the automatically generated subscriber password. For more information about this command and the format for the automatically generated subscriber password, see *Configuring Bindings*.	SmartEdge
111	Circuit-Protocol-Encap	No	Yes	Yes	Integer. Circuit encapsulation for CCOD child circuit. The following are the supported values: • 27 = PPPoE encapsulation • 34 = PPPoE multiencapsulation • 35 = PPPoE tunnel multiencapsulation	SmartEdge SM-Family
112	OS-Version	Yes	Yes	No	String. Software version number.	SmartEdge SM-Family

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform
113	Session-Traffic-Limit	No	Yes	Yes	String. Specifies that inbound or outbound traffic be limited. Use the in: limit and out: limit format where limits are independent and in Kbytes. Specifies that inbound, outbound, or aggregated traffic be limited. Use the in: limit, out: limit or aggregate: limit format, where limits are in Kilobytes (KB). The limit values set for inbound and outbound traffic are independent of each other. The limit value set for aggregate traffic is the total sum of both inbound and outbound traffic. When configuring Session-Traffic-Limit, you can configure the limit for either of these options: • Inbound traffic, outbound traffic, or both • Aggregate traffic You cannot configure the limit for aggregate traffic and for inbound or outbound traffic.	SmartEdge SM-Family
114	QoS-Reference	No	Yes	Yes	String. Specifies the node name, the node-name index, the group name, and the group-name index. A colon (:) separates the node-name index from the group name.	SmartEdge SM-Family
125	DHCP-Vendor-Class-Id	Yes	Yes	No	String. DHCP option 60 value.	SmartEdge SM-Family
127	DHCP-Vendor-Encap-Options	No	Yes	Yes	String. DHCP option 43 values. The format is: *code:value:code:value* where: • *code* = DHCP vendor-encapsulation option number • *value* = option data in one of the following formats: IP address type = dot notation Number = decimal integer ASCII string = ASCII characters without quotation marks Binary string = Hex values of bytes separated by commas (",") For descriptions of the vendor-encapsulated options found in RFC 2132, `DHCP Options and BOOTP Vendor Extension`, see the tables in the *option* command.	SmartEdge SM-Family

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform
128	Acct-Input-Octets-64	No	Yes	No	Integer. 64-bit value for the Acct-Input-Octets standard attribute per RFC 2139.	SmartEdge SM-Family
129	Acct-Output-Octets-64	No	Yes	No	Integer. 64-bit value for the Acct-Output-Octets standard attribute per RFC 2139.	SmartEdge SM-Family
130	Acct-Input-Packets-64	No	Yes	No	Integer. 64-bit value for the Acct-Input-Packets standard attribute per RFC 2139.	SmartEdge SM-Family
131	Acct-Output-Packets-64	No	Yes	No	Integer. 64-bit value for Acct-Output-Packets attribute per RFC 2139.	SmartEdge SM-Family
						SM-Family
133	Acct-Mcast-In-Octets-64	No	Yes	No	Integer. 64-bit value for the Acct-Mcast-In-Octets attribute.	SmartEdge SM-Family
134	Acct-Mcast-Out-Octets-64	No	Yes	No	Integer. 64-bit value for the Acct-Mcast-Out-Octets attribute.	SmartEdge SM-Family
135	Acct-Mcast-In-Packets-64	No	Yes	No	Integer. 64-bit value for the Acct-Mcast-In-Packets attribute.	SmartEdge SM-Family
136	Acct-Mcast-Out-Packets-64	No	Yes	No	Integer. 64-bit value for the Acct-Mcast-Out-Packets attribute.	SmartEdge SM-Family
137	LAC-Port	Yes	Yes	No	Integer. Contains the circuit handle for the incoming session on an L2TP LAC. This attribute should be present for a subscriber on an L2TP tunnel switch or LNS only. The circuit can be virtual for a PPPoE session.	SmartEdge
138	LAC-Real-Port	Yes	Yes	No	Integer. Contains the circuit handle for the real circuit of an incoming PPPoE session on an L2TP LAC. This attribute should be present for a subscriber on an L2TP tunnel switch or LNS only.	SmartEdge

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform
139	LAC-Port-Type	Yes	Yes	No	Integer. Contains the port type for the incoming session on an L2TP LAC. This attribute should be present for a subscriber on an L2TP tunnel switch or LNS only. The port can be virtual for a PPPoE session. Values for port types are: • 40 = NAS_PORT_TYPE_10BT • 41 = NAS_PORT_TYPE_100 BT • 42 = NAS_PORT_TYPE_DS 3_FR • 43 = NAS_PORT_TYPE_DS 3_ATM • 44 = NAS_PORT_TYPE_OC3 • 45 = NAS_PORT_TYPE_HSSI • 46 = NAS_PORT_TYPE_EIA 530 • 47 = NAS_PORT_TYPE_T1 • 48 = NAS_PORT_TYPE_CH AN_T3 • 49 = NAS_PORT_TYPE_DS 1_FR • 50 = NAS_PORT_TYPE_E3_ ATM • 51 = NAS_PORT_TYPE_IMA_ ATM • 52 = NAS_PORT_TYPE_DS3 _ATM_2 • 53 = NAS_PORT_TYPE_OC3 _ATM_2 • 54 = NAS_PORT_TYPE_1000 BSX • 55 = NAS_PORT_TYPE_E1_ FR • 56 = NAS_PORT_TYPE_E1_ ATM • 57 = NAS_PORT_TYPE_E3_ FR • 58 = NAS_PORT_TYPE_OC 3_POS • 59 = NAS_PORT_TYPE_OC 12_POS • 60 = NAS_PORT_TYPE_PPP OE	SmartEdge

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform
140	LAC-Real-Port-Type	Yes	Yes	No	Integer. Contains the port type for the real circuit of an incoming PPPoE session on an L2TP LAC. This attribute should be present for a subscriber on an L2TP tunnel switch or LNS only. See VSA 139 for port-type values.	SmartEdge
142	Session-Error-Code	No	Yes	No	Integer. 32 bits. Stop record only. Communicates specific error code information between Ericsson devices.	SmartEdge SM-Family
143	Session-Error-Msg	No	Yes	No	String. Stop record only. Describes how the session terminated.	SmartEdge SM-Family
144	Acct_Reason	No	Yes	No	Integer. Reason code describing why the router generated an accounting packet for a particular subscriber to RADIUS. Reason code values are: • 1 = AAA_LOAD_ACCT_SESSION_UP • 2 = AAA_LOAD_ACCT_SESSION_DOWN • 3 = AAA_LOAD_ACCT_PERIODIC • 7 = AAA_ACCT_RC_SUBSCRIBER_REAUTHOR • 16 = AAA_LOAD_ACCT_VOLUME_INGRESS_ EXCEEDED • 17 = AAA_LOAD_ACCT_VOLUME_EGRESS_ EXCEEDED • 18 = AAA_LOAD_ACCT_IDLE_TIMEOUT • 19 = AAA_LOAD_ACCT_TIME_EXCEEDED • 28 = AAA_LOAD_ACCT_VOLUME_AGGR_LIMIT_EXCEEDED • 34 = AAA_ACCT_RC_V6_UP • 35 = AAA_ACCT_RC_V6_DOWN • 36 = AAA_ACCT_RC_V4_UP • 37 = AAA_ACCT_RC_V4_DOWN • 38 = AAA_ACCT_RC_DHCPV6_PD_PREFIX_GRANTED • 39 = AAA_ACCT_RC_DHCPV6_PD_PREFIX_RELEASED	SmartEdge

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform
145	Mac-Addr	Yes	Yes	No	String. MAC address. The format is 17 octets in hex. The MAC address is sent for all subscriber PPPoE sessions. Supported media includes ATM PVCs, 802.1Q PVCs (tagged or untagged VLANs), and Ethernet ports.	SmartEdge
147	Acct-Mcast-In-Octets	No	Yes	No	Integer. Number of inbound multicast octets.	SmartEdge SM-Family
148	Acct-Mcast-Out-Octets	No	Yes	No	Integer. Number of outbound multicast octets.	SmartEdge SM-Family
149	Acct-Mcast-In-Packets	No	Yes	No	Integer. Number of inbound multicast packets.	SmartEdge SM-Family
150	Acct-Mcast-Out-Packets	No	Yes	No	Integer. Number of outbound multicast packets.	SmartEdge SM-Family
151	Reauth-Session-Id	No	No	Yes	String. Identifies the reauthorize session request. The value in this attribute is a string of attributes and values for the identified subscriber.	SmartEdge SM-Family
156	Qos-Rate-Inbound	No	Yes	Yes	String. Changes the inbound QoS rate. The format is rate:*burst*:*excess-burst*; changing the *burst* and *excess-burst* values is optional.	SmartEdge SM-Family
157	Qos-Rate-Outbound	No	Yes	Yes	String. Changes the outbound QoS rate. The format is rate:*burst*:*excess-burst*; changing the *burst* and *excess-burst* values is optional.	SmartEdge SM-Family
158	Route-Tag	No	Yes	Yes	Integer. Assigns a route tag to the subscriber's IP address (Framed-IP-Route), as well as the subscriber's route statements (Framed-IP-Route).	SmartEdge SM-Family
164	Dynamic-Policy-Filter	No	Yes	Yes	String. The string consists of a set of ASCII tokens separated by one or more spaces. No other characters are allowed. The tokens are shown in a syntax statement in Section 3.5 on page 52 section along with descriptions of the keywords and arguments in the syntax table.	SmartEdge SM-Family
165	HTTP-Redirect-URL	No	Yes	Yes	String. URL to which the router redirects HTTP requests.	SmartEdge SM-Family
166	DSL-Actual-Rate-Up	Yes	Yes	No	Integer 32-bit value. The actual DSL rate in the upstream direction.	SmartEdge SM-Family

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform
167	DSL-Actual-Rate-Down	Yes	Yes	No	Integer 32-bit value. The actual DSL rate in the downstream direction.	SmartEdge SM-Family
168	DSL-Min-Rate-Up	Yes	Yes	No	Integer 32-bit value. The minimum DSL rate in the upstream direction.	SmartEdge SM-Family
169	DSL-Min-Rate-Down	Yes	Yes	No	Integer 32-bit value. The minimum DSL rate in the downstream direction.	SmartEdge SM-Family
170	DSL-Attainable-Rate-Up	Yes	Yes	No	Integer 32-bit value. The attainable DSL rate in the upstream direction.	SmartEdge SM-Family
171	DSL-Attainable-Rate-Down	Yes	Yes	No	Integer 32-bit value. The attainable DSL rate in the downstream direction.	SmartEdge SM-Family
172	DSL-Max-Rate-Up	Yes	Yes	No	Integer 32-bit value. The maximum DSL rate in the upstream direction.	SmartEdge SM-Family
173	DSL-Max-Rate-Down	Yes	Yes	No	Integer 32-bit value. The maximum DSL rate in the downstream direction.	SmartEdge SM-Family
174	DSL-Min-Low-Power-Rate-Up	Yes	Yes	No	Integer 32-bit value. The DSL minimum low power rate in the upstream direction.	SmartEdge SM-Family
175	DSL-Min-Low-Power-Rate-Down	Yes	Yes	No	Integer 32-bit value. The DSL minimum low power rate in the downstream direction.	SmartEdge SM-Family
176	DSL-Max-Inter-Delay-Up	Yes	Yes	No	Integer 32-bit value. The maximum DSL interleaving delay in the upstream direction.	SmartEdge SM-Family
177	DSL-Actual-Inter-Delay-Up	Yes	Yes	No	Integer 32-bit value. The actual DSL interleaving delay in the upstream direction.	SmartEdge SM-Family
178	DSL-Max-Inter-Delay-Down	Yes	Yes	No	Integer 32-bit value. The maximum DSL interleaving delay in the downstream direction.	SmartEdge SM-Family
179	DSL-Actual-Inter-Delay-Down	Yes	Yes	No	Integer 32-bit value. The actual DSL interleaving delay in the downstream direction.	SmartEdge SM-Family
180	DSL-Line-State	Yes	Yes	No	Integer 32-bit value. The DSL port state: • 1 = SHOWTIME • 2 = IDLE • 3 = SILENT	SmartEdge SM-Family

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform
181	DSL-L2-Encapsulation	Yes	Yes	No	Integer 32-bit value. The DSL data link protocol and data link encapsulation: Data link byte: • 0 = ATM AAL5 • 1 = ETHERNET Encapsulation byte 1: • 1 = Untagged • 2 = Ethernet Encapsulation byte 2: • 0 = NA • 1 = PPPoA LLC • 2 = PPPoA NULL • 3 = IPoA LLC • 4 = IPoA NULL • 5 = Ethernet over AAL5 LLC with FCS • 6 = Ethernet over AAL5 LLC without FCS • 7 = Ethernet over AAL5 NULL with FCS • 8 = Ethernet over AAL5 NULL without FCS	SmartEdge SM-Family
182	DSL-Transmission-System	Yes	Yes	No	Integer 32-bit value. The DSL access-loop type of transmission system: • 1 = ADSL1 • 2 = ADSL2 • 3 = ADSL2+ • 4 = VDSL1 • 5 = VDSL2 • 6 = SDSL • 7 = UNKNOWN	SmartEdge SM-Family
183	DSL-PPPOA-PPPOE-Inter-Work-Flag	Yes	Yes	No	Integer. PPPoA-to-PPPoE interworking flag.	SmartEdge SM-Family
184	DSL-combined-Line-Info	Yes	Yes	No	String. The value of the TLV described in *GSMP Extensions for Layer 2 Control (L2C) Topology Discovery and Line Configuration*, section 5.4.1 ,"Topology Discovery."	SmartEdge SM-Family

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform
185	DSL-Actual-Rate-Down-Factor	Yes	Yes	No	Integer. The rate that can be learned from the DSLAM or from a PPPoE or DHCP tag, depending on the configuration of the **access-line rate** command (in subscriber configuration mode).	SmartEdge SM-Family
189	Flow_FAC_Profile	No	Yes	No	String. Specifies the name of a Flow Admission-Control profile. This attribute is used to apply flow on the circuit of the configured subscriber. The Flow_FAC_Profile attribute can only be configured under subscriber profile.	SmartEdge SM-Family
190	Service-Name	No	Yes	Yes	String. The name of the service to be activated, together with the following optional fields: • *:service id*—Used when there is more than one instance of the same service. • *service-parameter*—Zero or more parameters formatted as name-value pairs. Names and values are separated by an equals sign (=) with no spaces around it. Pairs are separated by spaces. You can also specify service parameters in VSA 192. See VSA 192 for formatting details.	SmartEdge SM-Family
191	Service-Options	No	No	Yes	Integer. Specifies whether accounting is enabled for service management: • ACCT-DISABLED = 0x00 • ACCT-ENABLED = 0x01	SmartEdge SM-Family
192	Service-Parameter	No	Yes	Yes	String. Service parameters for a service that is specified in VSA 190, formatted as name-value pairs. Names and values are separated by an equal sign (=) with no spaces around it. Pairs are separated by spaces. If a parameter needs an array, the values in the array are separated by commas (,) with no space between the value and the comma. If the value is a string that includes either spaces or commas, enclose the string in double quotes (").	SmartEdge SM-Family

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform
193	Service-Error-Cause	No	Yes	No	Integer. Specifies a service management error according to one of the following values: • 0 = Service success • 401 = Unsupported attribute • 402 = Missing attribute • 404 = Invalid request • 506 = Resource unavailable • 550 = Generic service error • 551 = Service not found • 552 = Service already active • 553 = Service accounting disabled • 554 = Service duplicate parameter If the RADIUS server does not support this VSA, the 550, 551, and 552, 553, and 554 error codes can be mapped to the standard Error-Cause attribute 550 (other proxy processing error).	SmartEdge SM-Family
194	Deactivate-Service-Name	No	No	No	String. The service profile name of the service to be deactivated together with the following optional fields: • *:service id*—Used when there is more than one instance of the same service. • *service-parameter*—Zero or more parameters formatted as name-value pairs. Names and values are separated by an equals sign (=) with no spaces around it. Pairs are separated by spaces.	SmartEdge SM-Family
195	QoS-Overhead	No	Yes	Yes	String. Attaches a QoS overhead profile to the subscriber session. If the overhead profile is defined in the RADIUS record of the subscriber, the subscriber has the specified overhead profile when the subscriber session comes up.	SmartEdge SM-Family
196	Dynamic-QoS-Param	No	No	Yes	String. The format varies by QoS parameter. For more information, see Section 3.6 on page 58. Zero or more Dynamic-QoS-Param VSAs can be sent in an Access-Accept or CoA-Request packet to the router.	SmartEdge SM-Family

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform
199	Double_Authentication	No	No	Yes	Integer. The integer value is 1. Indicates that the session needs one more authentication. It is valid only if it is received from a global access response.	SmartEdge SM-Family
201	DHCP-Field	Yes	Yes	No	Binary. Identifies a standard DHCP client field. This generic VSA is used to identify standard DHCP client fields that must be sent in RADIUS authentication or accounting requests. To distinguish each supported DHCP client field, a unique `dhcp-sub-field` field is used within this VSA to indicate a specific value that corresponds to a specific DHCP client field. Currently, this VSA supports only `dhcp-sub-field` field of type 1, the `giaddr` or gateway address field. A RADIUS server uses the gateway address field to provide static routes to clients based on this address.	SmartEdge SM-Family
202	DHCP-Option	Yes	Yes	No	Binary. Identifies a DHCP client option. This VSA is a generic VSA, which is used to identify various supported DHCP client options that must be sent in RADIUS authentication or accounting requests. To distinguish each supported DHCP client option, a unique `dhcp-sub-type` field is used within this VSA to indicate a specific value that corresponds to a specific DHCP option. Currently, this VSA supports DHCP options 12 (hostname), 61 (client identifier), and 77 (user class).	SmartEdge SM-Family

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform
203	Security-Service	No	Yes	Yes	String configured in RADIUS. Specifies an ASE security profile. Optionally specifies a preshared key using the following format: Security-Service="ike preshared-key hex hex-value | ASCII-value". The IKE preshared key is only received in an Acct-Response message; it is never sent in an Access-Request or Acct-Request message. The ASE DPI traffic management policy name is received in the Access-Request and sent in the Acct-Request in the format Security-Service="dpi traffic-management policy *policy-name*". To enable DPI security service for a subscriber either through COA or reauthorization at a later point, configure RADIUS to send the Access-Accept message at initial subscriber logon with the following format: Security-Service="dpi traffic-management enable-coa".	SmartEdge SM-Family

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform

204	Reauth-Service-Name	No	No	No	String. The name of the service to be reauthorized, together with the optional field of ***service-parameter***. Parameters are formatted as name-value pairs. Names and values are separated by an equals sign (=) with no spaces around it. Pairs are separated by spaces. The service name and service parameters are separated by spaces. For example: Reauth-Service-Name: = "voip_service inLimit=1000 timeout=10"
					
					This VSA is used to provide dynamic reauthorization of the RADIUS service attributes of an RSE service without bringing the associated service down. The following are the supported RADIUS service attributes:
					
					• Service-Interim-Accounting
					
					• Service-Timeout
					
					• Service-Volume-Limit
					
					For more information about these attributes, see Section 7 on page 69.
					
					If not all reauthorizable service parameters fit in VSA 204 due to the limitations of number of characters you can use in this VSA, you can use vendor VSA 192, Service-Parameters, to carry these additional service parameters. You can also configure VSA 204 to carry only the service name and VSA 192 carry all the service parameters. See VSA 192 for formatting details.
					
					If you are using VSA 192 with VSA 204, use a RADIUS attribute tag to correlate this VSA with VSA 204. The tag is an arbitrary number you assign to both VSAs.
					
					For example:
					`Reauth-Service-Name:2`
					`= "voip_service"`
					`Service-Parameters:2 =`
					`"timeout=1`
					`inLimit=777 outLimit=1000"`
					
					In the above example, `2` is the RADIUS attribute tag assigned to both VSAs.
					
					If a CoA-Request message is to include more than one set of associated VSAs that are tagged with RADIUS attribute tags, and there exists among these sets at least one common VSA, ensure that the RADIUS attribute tag you assign to each set is unique. Ensuring the uniqueness of each tag allows the router to successfully process the CoA-Request message.
						SmartEdge
						
						SM-Family

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform
207	RB-IPV6-DNS	No	Yes	Yes	String. This attribute is a Ericsson VSA to configure the IPv6 Primary and Secondary DNS of a subscriber. An example is shown below: `IPv6-DNS = "1=2000::106 :a00:20ff:fe99:a998,2=2 000::106:a00:20ff:fe99: a995` 1= **value** indicates the primary ipv6 dns for the subscriber. 2=**value** indicates the secondary ipv6-dns for the subscriber. Note that the primary and secondary ipv6 dns can be configured using the same VSA. This attribute cannot be modified through CoA. For more information on these commands, refer to *dns6* primary and secondary CLI commands.	SmartEdge

208	RB-IPv6 Option	No	Yes	Yes	String. This VSA is used to configure multiple ipv6 attributes for a single subscriber. The nd-profile, ipv6-source-validation, and ipv6-route-tag can be configured using the IPv6-Option Ericsson VSA. IPv6 Source validation or reverse-path-forwarding for the subscriber can be configured using the following syntax:
					
					`IPv6-Option ="source-va lidation=1"`
					
					The example below shows how a route-tag can be configured for the subscriber:
					
					`IPv6-Option ="route-tag =22"`
					
					The ND profile for the subscriber can be configured as shown below.
					
					`IPv6-Option += "nd=nd1"`
					
					This attribute, IPv6-Option cannot be modified through CoA.
						SmartEdge

209	Cluster-Partition-ID	Yes	Yes	No	String (up to 243 characters) sent in Access-Request and Accounting-Request messages to provide the VRRP Partition ID. After a VRRP state transition, this VSA contains a new value for the VRRP Partition ID (in the Access-Request and Accounting-Request messages). The subscriber sessions initiated before the VRRP transition should be cleaned up.	SmartEdge

Table 7   Vendor VSAs Supported

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Respons	Notes	Platform
210	Circuit_Group_Member	No	Yes	Yes	String. Name of a configured circuit group, which is an alphanumeric string comprising up to 39 characters. This VSA is used to specify that the subscriber is a member of the specified circuit group. This VSA is the equivalent of the `circuit-group-member` command configured in the local subscriber record. Subscriber circuit-group-membership cannot be dynamically modified, added, or removed. To make circuit-group-membership changes, terminate the subscriber session, reassign circuit group membership, and then reestablish the subscriber session. For information about circuit groups including VPCGs, see *Circuit Groups*.	SmartEdge SM-Family
212	Delegated-Max-Prefix	No	Yes	Yes	Integer. Number of IPv6-Delegated-Prefixes that must be assigned to the subscriber. Range is from 1 to 5; default is 1.	SmartEdge
213	IPv4-Address-Release-Control	Yes	Yes	No	String (up to 63 characters) sent in Access-Request and Interim Accounting-Request messages to identify IPv4 address save mode for the session.	SmartEdge

(1) The Tunnel-Password attribute is used for authentication in the other direction.

3.2   Vendor VSAs in CoA and Disconnect Messages

Table 8 lists the Vendor VSAs that can appear in CoA-Request, CoA-Response, Disconnect-Request, and Disconnect-Response messages. For details about these attributes, see Table 7.

Table 8   Vendor VSAs in CoA and Disconnect Messages

#	VSA Name	Sent in CoA Request	Sent in CoA Response	Sent in Disconnect Request	Sent in Disconnect Response	Platform
4	Context_Name	Yes	No	Yes	No	SmartEdge SM-Family
33	Mcast_Send	Yes	No	No	No	SmartEdge SM-Family

Table 8   Vendor VSAs in CoA and Disconnect Messages

#	VSA Name	Sent in CoA Request	Sent in CoA Response	Sent in Disconnect Request	Sent in Disconnect Response	Platform
34	Mcast_Receive	Yes	No	No	No	SmartEdge SM-Family
35	Mcast_MaxGroups	Yes	No	No	No	SmartEdge SM-Family
87	Qos_Policing	Yes		Yes		SmartEdge SM-Family
88	Qos_Metering	Yes		Yes		SmartEdge SM-Family
89	Qos_Queuing	Yes		Yes		SmartEdge SM-Family
90	Igmp_Svc_Prof_Id	Yes	No	No	No	SmartEdge SM-Family
92	Forward-Policy	Yes	No	No	No	SmartEdge SM-Family
94	Reauth_String	Yes	No	No	No	SmartEdge SM-Family
95	Reauth_More	Yes	No	No	No	SmartEdge SM-Family
96	RBN_Agent_Remote_ID	Yes	No	Yes	No	SmartEdge SM-Family
97	RBN_Agent_Circuit_ID	Yes	No	Yes	No	SmartEdge SM-Family
101	Shaping_Profile_Name	Yes	No	No	No	SmartEdge SM-Family
102	Bridge_Profile	Yes	No	No	No	SmartEdge SM-Family
105	Nat_Policy_Name	Yes	No	No	No	SmartEdge SM-Family
107	HTTP_Redirect_Profile_Name	Yes	No	No	No	SmartEdge SM-Family
112	OS_Version	Yes	No	No	No	SmartEdge SM-Family
113	Session_Traffic_Limit	Yes	No	No	No	SmartEdge SM-Family
114	Qos_Reference	Yes	No	No	No	SmartEdge SM-Family

Table 8   Vendor VSAs in CoA and Disconnect Messages

#	VSA Name	Sent in CoA Request	Sent in CoA Response	Sent in Disconnect Request	Sent in Disconnect Response	Platform
156	Qos_Rate_Inbound	Yes	No	No	No	SmartEdge SM-Family
157	Qos_Rate_Outbound	Yes	No	No	No	SmartEdge SM-Family
164	Dynamic-Policy-Filter	Yes	No	No	No	SmartEdge SM-Family
165	HTTP-Redirect-URL	Yes	No	No	No	SmartEdge SM-Family
189	Flow_FAC_Profile	Yes	No	No	No	SmartEdge SM-Family
190	Service-Name	Yes	Yes	No	No	SmartEdge SM-Family
191	Service-Options	No	No	No	No	SmartEdge SM-Family
192	Service-Parameter	Yes	No	No	No	SmartEdge SM-Family
193	Service-Error-Cause	No	Yes	No	No	SmartEdge SM-Family
194	Deactivate-Service-Name	Yes	Yes	No	No	SmartEdge SM-Family
196	Dynamic-QoS-Param	Yes	No	No	No	SmartEdge SM-Family
203	Security-Service	Yes	No	No	No	SmartEdge SM-Family
204	Reauth-Service-Name	Yes	Yes	No	No	SmartEdge SM-Family

3.3   Vendor VSAs That Can Be Reauthorized

Table 9 lists the vendor VSAs that are reauthorized when you enter the `reauthorize` command (in exec mode). For details about these VSAs, see Table 7.

Table 9   Vendor VSAs Supported by Reauthorization

#	VSA Name	Description	Platform
33	Mcast-Send	Defines whether the subscriber can send multicast packets.	SmartEdge SM-Family

Table 9   Vendor VSAs Supported by Reauthorization

#	VSA Name	Description	Platform
34	Mcast-Receive	Defines whether the subscriber can receive multicast packets.	SmartEdge SM-Family
35	Mcast-MaxGroups	Specifies the maximum number of multicast groups of which the subscriber can be a member.	SmartEdge SM-Family
87	Qos_Policing	Attaches a QoS policing policy to the subscriber session.	SmartEdge SM-Family
88	Qos_Metering	Attaches a QoS metering policy to the subscriber session.	SmartEdge SM-Family
89	Qos_Queuing	Attaches a QoS queuing service profile to the subscriber session.	SmartEdge SM-Family
90	Igmp_Svc_Prof_Id	Applies an IGMP service profile to the subscriber session.	SmartEdge SM-Family
92	Forward-Policy	Attaches an in or out forward policy to the subscriber session.	SmartEdge SM-Family
101	Shaping-Profile-Name	Indicates the name of the ATM shaping profile.	SmartEdge SM-Family
102	Bridge-Profile-Name	Indicates the name of the bridge profile.	SmartEdge SM-Family
107	HTTP-Redirect-Profile-Name	Indicates the name of the HTTP redirect profile.	SmartEdge SM-Family
113	Session-Traffic-Limit	Specifies that inbound or outbound traffic be limited. Specifies that inbound, outbound, or aggregated traffic be limited.	SmartEdge SM-Family
114	Qos_Reference	Specifies the node name, node-name index, group name, and group-name index. A colon (:) separates the node-name index from the group name.	SmartEdge SM-Family
156	Qos_Rate_Inbound	Changes the inbound QoS rate; changing the excess burst rate is optional.	SmartEdge SM-Family
157	Qos_Rate_Outbound	Changes the outbound QoS rate; changing the excess burst rate is optional.	SmartEdge SM-Family
164	Dynamic_Policy_Filter	Specifies a class rule for a dynamic policy ACL.	SmartEdge SM-Family
165	HTTP_Redirect_URL	Specifies the URL to which the router redirects HTTP requests.	SmartEdge SM-Family
189	Flow_FAC_Profile	Specifies flow.	SmartEdge SM-Family
190	Service_Name	Carries the service name and parameters required to activate the service.	SmartEdge SM-Family

Table 9   Vendor VSAs Supported by Reauthorization

#	VSA Name	Description	Platform
191	Service_Options	Carries the service action, which indicates the action the router should perform. The enumerated types for this attribute are shown below: a) ACTIVATE-ENABLED = 0x01 b) ACTIVATE-DISABLED = 0x00	SmartEdge SM-Family
192	Service_Parameter	Carries the parameters required to activate the service.	SmartEdge SM-Family
194	Deactivate_Service_Name	Deactivates the specified service name and the parameters associated with the service.	SmartEdge SM-Family
195	Qos_Overhead	Attaches a QoS overhead profile to the subscriber session	SmartEdge SM-Family
196	Dynamic_QoS_Param	Parameterizes QoS policies	SmartEdge SM-Family
203	Security-Service	Specifies an ASE security profile.	SmartEdge SM-Family
204	Reauth-Service-Name	Carries the service name and parameters required to reauthorize the named service.	SmartEdge SM-Family

3.4   VSA for RSE Reauthorization

The router supports the following VSAs:

- Reauth-Service-Name ()Ericsson VSA# 204)—Triggers service reauthorization from the RADIUS server while the service is active without affecting the data traffic for the service—that is, without restarting the service. The format of the VSA is `<service name> service_parameter1`. This attribute is accepted only in RADIUS COA-Request message and sent back in COA-Response to the RADIUS server. If this attribute is sent in Access-Accept, it is silently ignored. This attribute optionally also includes service parameters that need to reauthorized.

  Unlike Service-Name, not all mandatory attributes are required in Reauth-Service-Name VSA. The received parameters, along with service profile configuration, are used to generate the internal service attributes. The generated attribute is then checked to determine if it can be reauthorized. If not, the reauthorization request is rejected, and a COA-Response (NAK/NACK) and error cause are sent to RADIUS server. If the attribute is reauthorizable, and if the value remains unchanged, then the reauthorization procedure for that attribute is ignored. The "Reauth" attributes are then provisioned.

- Service-Parameters (Ericsson VSA# 192)—All reauthorizable service parameters may not fit in the Reauth-Service-Name VSA. Ericsson VSA# 192 (Service-Parameters) is used to carry the additional service parameters. Reauth-Service-Name may carry just the service name, and Service-Parameters may carry all the service parameters. The RADIUS attribute tag is used to correlate the Service-Parameters VSA with the Reauth-Service-Name VSA. A COA-Request can zero or more instances of this attribute. There can be more than one instance of this attribute with an identical RADIUS attribute tag.

- Service-Error-Cause (Ericsson VSA# 193)—Indicates the error cause associated with a specific service. The COA-Error-Cause is a global attribute, which indicates the error cause for the one complete COA-Request. The Service-Error-Cause VSA indicates the error cause associated with each service action in a COA-Request. This attribute is tagged, and a COA-Response can have more than one instance of this attribute. The tags of this attribute must be unique.

- Service-Option (Ericsson VSA# 191)--Not required for service reauthorization and is silently discarded if sent by the RADIUS server.

3.5   VSA 164 Format

VSA 164 has the following format:

ip *dir action* [**dstip** *n.n.n.n*[*/nn*]] [**srcip** *n.n.n.n*[*/nn*]] [{**dscp** *dscp-value* | **tos** *tos-value tos-mask*}] [*protocol* [**dstport** *dst-op dst-port*] [**srcport** *src-op src-port*] [**est**]] **class** *class-name service*

Table 10 describes keywords and arguments for VSA 164.

Table 10   VSA 164 Keywords and Arguments

`ip`	Specifies that the filter applies to IP packets.	Platform
`ipv6`	Specifies that the Dynamic-Policy-Filter applies to IPv6 packets.	SmartEdge
`dir`	Specifies the direction of the traffic with one of the following keywords: • `in`—Traffic is inbound to the router. • `out`—Traffic is outbound from the router.	SmartEdge SM-Family
`forward`	Specifies the filter action.	SmartEdge SM-Family
`dstip n.n.n.n[/nn`	Optional. IP address and netmask for the destination port. The range of values for the netmask is 0 to 32.	SmartEdge SM-Family
`srcip n.n.n.n[/nn`	Optional. IP address and netmask for the source port. The range of values for the netmask is 0 to 32.	SmartEdge SM-Family

Table 10   VSA 164 Keywords and Arguments

`dscp dscp-value`	Optional. Differentiated Services Code Point (DSCP) value that the packet must have to be considered a match. The range of values is decimal 0 to 63, a hexadecimal value listed in Table 13, or one of the keywords listed in Table 13.	SmartEdge SM-Family
`tos tos-value tos-mask`	Optional. Type of service (ToS) that the packet must have to be considered a match. The range of values for the `tos-value` argument is decimal 0 to 255 or the hexadecimal equivalent, but only certain values are allowed. The `tos-mask` argument identifies the group of bits in the IP ToS byte; see Table 14.	SmartEdge SM-Family
`protocol`	Optional. Protocol, according to one of the following keywords: • `icmp`—Internet Control Message Protocol (ICMP) • `tcp`—Transmission Control Protocol (TCP) • `udp`—User Datagram Protocol (UDP) • `ospf`—Open Shortest Path First (OSPF) protocol	SmartEdge SM-Family
`dstport dst-op dst-port`	Optional. Comparison operation and port name or number for the destination port. Table 11 lists the keywords for the comparison operation (the `dst-op` argument). For the `dst-port` argument, you can specify either a port name or a port number. Table 12 lists the keywords for the port name. The range of values for port number is 1 to 1,023.	SmartEdge SM-Family
`srcport src-op src-port`	Optional. Comparison operation and port name or number for the source port. Table 11 lists the keywords for the comparison operation (the `src-op` argument). For the `src-port` argument, you can specify either a port name or a port number. Table 12 lists the keywords for the port name. The range of values for port number is 1 to 1,023.	SmartEdge SM-Family
`est`	Optional. TCP established. This keyword is valid only if you specify the `tcp` keyword for the protocol.	SmartEdge SM-Family
`class class-name`	Class name. The format is a string of 1 to 39 case-sensitive printable characters.	SmartEdge SM-Family
`service`	Type of service policy, according to one of the following keywords: • `fwd`—Forward policy • `nat`—Network Address Translation (NAT) policy • `qos`—Quality of service (QoS) policy (either metering or policing)	SmartEdge SM-Family

Table 11 lists the keyword operators for the `dst-op` and `src-op` arguments.

Table 11   Keyword Operators for Comparison Operations

Operator	Description	Platform
`<`	Port number is less than the specified port number.	SmartEdge SM-Family
`=`	Port name or number matches the specified port name or number.	SmartEdge SM-Family
`>`	Port number is greater than the specified port number.	SmartEdge SM-Family
`!=`	Port name or number does not match the specified port name or number.	SmartEdge SM-Family

Table 12 lists the keywords for the *dst-port* and *src-port* arguments in alphabetical order.

Table 12   Keywords for Destination and Source Port Numbers and Names

Port Name	Description	Platform
cmd	514/udp; shell command	SmartEdge SM-Family
domain	53/udp, 53/tcp; Domain Name Server	SmartEdge SM-Family
exec	512/tcp; remote process execution	SmartEdge SM-Family
finger	79/udp, 79/tcp; Finger	SmartEdge SM-Family
ftp	21/udp, 21/tcp; FTP	SmartEdge SM-Family
ftp-data	20/udp, 20/tcp; FTP default data	SmartEdge SM-Family
gopher	70/udp, 70/tcp; Gopher	SmartEdge SM-Family
hostname	101/udp, 101/tcp; NIC Host Name Server	SmartEdge SM-Family
kerberos	88/udp, 88/tcp; Kerberos	SmartEdge SM-Family
login	513/tcp; remote login, such as Telnet	SmartEdge SM-Family
nameserver	42/udp, 42/tcp; Host Name Server	SmartEdge SM-Family
nntp	119/udp, 119/tcp; NNTP	SmartEdge SM-Family
ntp	123/tcp, 123/udp; NTP	SmartEdge SM-Family
smtp	25/udp; SMTP	SmartEdge SM-Family
talk	517/udp; similar to a tenex link, but across machine; does not use link protocol; a rendezvous port from which a tcp connection is established	SmartEdge SM-Family
telnet	23/udp; Telnet	SmartEdge SM-Family

Table 12   Keywords for Destination and Source Port Numbers and Names

Port Name	Description	Platform
`tftp`	69/udp; TFTP	SmartEdge SM-Family
`www`	80/udp, 80/tcp; World Wide Web HTTP	SmartEdge SM-Family

Table 13 lists the keyword and hexadecimal value substitutions for the `dscp-value` argument.

Table 13   Keyword and Hexadecimal Substitutions for the dscp-value Argument

Keyword	Hexadecimal Value	Definition	Platform
`af11`	0x0a	Assured Forwarding—Class 1/Drop precedence 1	SmartEdge SM-Family
`af12`	0x0c	Assured Forwarding—Class 1/Drop precedence 2	SmartEdge SM-Family
`af13`	0x0e	Assured Forwarding—Class 1/Drop precedence 3	SmartEdge SM-Family
`af21`	0x12	Assured Forwarding—Class 2/Drop precedence 1	SmartEdge SM-Family
`af22`	0x14	Assured Forwarding—Class 2/Drop precedence 2	SmartEdge SM-Family
`af23`	0x16	Assured Forwarding—Class 2/Drop precedence 3	SmartEdge SM-Family
`af31`	0x1a	Assured Forwarding—Class 3/Drop precedence 1	SmartEdge SM-Family
`af32`	0x1c	Assured Forwarding—Class 3/Drop precedence 2	SmartEdge SM-Family
`af33`	0x1e	Assured Forwarding—Class 3/Drop precedence 3	SmartEdge SM-Family
`af41`	0x22	Assured Forwarding—Class 4/Drop precedence 1	SmartEdge SM-Family

Table 13   Keyword and Hexadecimal Substitutions for the dscp-value Argument

Keyword	Hexadecimal Value	Definition	Platform
`af42`	0x24	Assured Forwarding—Class 4/Drop precedence 2	SmartEdge SM-Family
`af43`	0x26	Assured Forwarding—Class 4/Drop precedence 3	SmartEdge SM-Family
`cs0`	0x00	Class selector 0	SmartEdge SM-Family
`cs1`	0x08	Class selector 1	SmartEdge SM-Family
`cs2`	0x10	Class selector 2	SmartEdge SM-Family
`cs3`	0x18	Class selector 3	SmartEdge SM-Family
`cs4`	0x20	Class selector 4	SmartEdge SM-Family
`cs5`	0x28	Class selector 5	SmartEdge SM-Family
`cs6`	0x30	Class selector 6	SmartEdge SM-Family
`cs7`	0x38	Class selector 7	SmartEdge SM-Family
`df`	0x00	Default Forwarding (alternative to `cs0`)	SmartEdge SM-Family
`ef`	0x2e	Expedited Forwarding	SmartEdge SM-Family
`prec1`	0x08	Precedence selector 1 (alternative to `cs1`)	SmartEdge SM-Family
`prec2`	0x10	Precedence selector 2 (alternative to `cs2`)	SmartEdge SM-Family

Table 13   Keyword and Hexadecimal Substitutions for the dscp-value Argument

Keyword	Hexadecimal Value	Definition	Platform
`prec3`	0x18	Precedence selector 3 (alternative to `cs3`)	SmartEdge SM-Family
`prec4`	0x20	Precedence selector 4 (alternative to `cs4`)	SmartEdge SM-Family
`prec5`	0x28	Precedence selector 5 (alternative to `cs5`)	SmartEdge SM-Family
`prec6`	0x30	Precedence selector 6 (alternative to `cs6`)	SmartEdge SM-Family
`prec7`	0x38	Precedence selector 7 (alternative to `cs7`)	SmartEdge SM-Family

Table 14 lists the definitions for the groups of bits in the IP ToS byte and the value for the *tos-mask* argument for each group. ToS values must correspond to the ToS mask so that the value does not have any bits outside the range of the mask.

Table 14   ToS Mask Group Definitions

ToS Group	Bit Range	Decimal Value	Hexadecimal Value	Platform
Flags	1 to 4	30	0x1E	SmartEdge SM-Family
Precedence	5 to 7	224	0xE0	SmartEdge SM-Family
Combined	1 to 7	254	0xFE	SmartEdge SM-Family
DSCP	2 to 7	252	0xFC	SmartEdge SM-Family

If you specify either the **dscp** *dscp-value* or the **tos** *tos-value* construct in the VSA, you must specify the construct before you specify any protocol-related options (*protocol* argument, **class** keyword).

To display the definition of this VSA, use the **show subscribers** command with the **active** keyword (in any mode) or the **show access-group**

command (in any mode). For more information about these commands, see *Command List*.

Matching criteria consist of Layer 3 and Layer 4 parameters. All parameters are optional; if you omit a parameter, the parameter has the value "any," which means that any packet matches that parameter.

You can specify Layer 4 parameters only if you specify either TCP or UDP as the protocol.

If you do not specify the `netmask` argument, the system uses a default netmask, which is based on the IP network class corresponding to the IP address.

You cannot specify `0.0.0.0` as an IP address.

3.6 VSA 196 Format

VSA 196 has the following format:

attribute [**parent**] [**remove**]

Table 15   VSA 196 Format

attribute	Specifies one of the following dynamic quality of service (QoS) parameters:	Platform
Forwarding Policy Attributes	• `ipv6-fwd-in-access-group <acl-name1>:<acl-name2>:<acl-name3>:...:<acl-name10>`[1] • `fwd-in-access-group <acl-name1>:<acl-name2>:<acl-name3>:...:<acl-name10>`[2]	SmartEdge SM-Family

Table 15   VSA 196 Format

Metering Policy Attributes	• `meter-circuit-burst` *`bytes`*	SmartEdge
	• `meter-circuit-exceed` {`mark-dscp` *`dscp-value`* | `mark-precedence` *`precedence-value`* | `mark-priority` *`priority-value`*} | {`drop-qos-priority` *`priority-value`* | `drop-all` | `no-action`}	SM-Family
	• `meter-circuit-excess-burst` *`bytes`*	
	• `meter-circuit-conform` {`mark-dscp` *`dscp-value`* | `mark-precedence` *`precedence-value`* | `mark-priority` *`priority-value`*} | `no-action`}	
	• `meter-circuit-mark` {`mark-dscp` *`dscp-value`* | `mark-precedence` *`precedence-value`* | `mark-priority` *`priority-value`*}	
	• `meter-circuit-rate rate-absolute` *`rate-value`*	
	• `meter-circuit-violate` {`mark-dscp` *`dscp-value`* | `mark-precedence` *`precedence-value`* | `mark-priority` *`priority-value`*} | `drop-all` | `no-action`}	
	• `meter-class-burst`*`class-name`**`burst-bytes`*	
	• `meter-class-conform` *`class-name`* {`mark-dscp` / `mark-precedence` / `mark-priority` / `no-action`}	
	• `meter-class-exceed`*`class-name`* {`mark-dscp` | `mark-prec edence` / `mark-priority` | `drop-qos-priority-group` | `drop-all` | `no-action`}	
	• `meter-class-excess-burst`*`class-name`**`excess-burst-bytes`*	
	• `meter-class-mark`*`class-name`* {`mark-dscp` | `mark-precedence` / `mark-priority`}	
	• `meter-class-rate`*`class-name`* {`rate-absolute` *`kbps`* | `rate-percentage` *`percentage`*}	
	• `meter-class-violate`*`class-name`* {`mark-dscp` | `mark-precedence` / `mark-priority` | `drop-all` | `no-action`}	

Table 15   VSA 196 Format

Policing Policy Attributes	• `police-circuit-burst` *`bytes`* • `police-circuit-conform` {`mark-dscp` *`dscp-value`* | `mark-precedence` *`precedence-value`* | `mark-priority` *`priority-value`*} | `no-action`} • `police-circuit-exceed` {`mark-dscp` *`dscp-value`* | `mark-precedence` *`precedence-value`* | `mark-priority` *`priority-value`*} | {`drop-qos-priority` *`priority-value`*} | `drop-all` | `no-action`} • `police-circuit-excess-burst` *`bytes`* • `police-circuit-mark` {`mark-dscp` *`dscp-value`* | `mark-precedence` *`precedence-value`* | `mark-priority` *`priority-value`*} • `police-circuit-rate rate-absolute` *`rate-value`* • `police-circuit-violate` {`mark-dscp` *`dscp-value`* | `mark-precedence` *`precedence-value`* | `mark-priority` *`priority-value`*} | `drop-all` | `no-action`} • `police-class-burst`*`class-name`*`burst-bytes` • `police-class-conform`*`class-name`* {`mark-dscp` | `mark-precedence` | `mark-priority` | `no-action`} • `police-class-exceed`*`class-name`* {`mark-dscp` | `mark-precedence` | `mark-priority` | `drop-qos-priority-group` | `drop-all` | `no-action`} • `police-class-excess-burst`*`class-name`**`excess-burst-bytes`* • `police-class-mark`*`class-name`* {`mark-dscp` | `mark-precedence` | `mark-priority`} • `police-class-rate` *`class-name`* {`rate-absolute`*`kbps`* | `rate-percentage` *`percentage`*} • `police-class-violate`*`class-name`* {`mark-dscp` | `mark-precedence` / `mark-priority` / `drop-all` / `no-action`}	SmartEdge SM-Family
PWFQ Policy Attributes	• `pwfq-priority-group-rate` *`group-num`* {`rate-absolute`*`kbps`* / `rate-percentage` *`percentage`*} • `pwfq-queue-priority` *`queue-num`* {*`priority-group`* / *`weight-value`*} • `pwfq-queue-weight` *`queue-num`**`weight-value`* • `pwfq-circuit-rate-min` *`rate-value`* • `pwfq-circuit-rate-max` *`rate-value`* • `pwfq-circuit-weight` *`weight`*	SmartEdge SM-Family
`parent`	Optional. Enter the `parent` keyword to apply the modification of a `dynamic-qos-param` attribute to the parent circuit of the subscriber session instead of the subscriber session. The parent circuit of a subscriber session is considered to be the 802.1q VLAN or ATM PVC which encapsulates its traffic and under which the `bind authentication` or `bind subscriber` CLI configuration entry of the subscriber was specified. You can also use the `remove` keyword with the `parent` keyword to remove applied dynamic parameter on parent circuit.	SmartEdge SM-Family
`remove`	Optional. Enter the `remove` keyword to remove a dynamic parameter and revert the QoS parameter to the default value.	SmartEdge SM-Family

(1) The ipv6-fwd-in-access-group does not support the parent keyword.

(2) The fwd-in-access-group does not support the parent keyword.

Note: VSA 196 offers a superset of the functionality of VSA 156 (Qos-Rate-Inbound) and 157 (Qos-Rate-Outbound). Use either VSA 196, or VSA 156 or 157 or both, to modify the circuit-level rate and associated parameters (burst and excess-burst) on a single circuit. When VSA 196 is applied with VSA 156 or 157 to the same property of a single circuit, VSA 196 takes precedence. Any property (rate, burst, or excess-burst) specified through VSA 156 or 157 is ignored when the corresponding VSA 196 attribute is in place. If the VSA 196 attribute is removed (for example, by the COA attribute removal) and either VSA 156 or 157 is still applied to the subscriber session, the previously overridden VSA takes effect.

When the same QoS rate of a circuit is subject to modification from both the DSL line rate (received through ANCP or through TR-101 PPPoE or DHCP tags) and a rate applied through VSA 156, 157, or 196 (set through RADIUS or the `policy-refresh` exec command), the lower of the last line rate received or the relevant VSA rate (determined by the preceding precedence rule) is applied.

The description of `policy-refresh` command (in exec mode) provides more information on this VSA; for details, see *Commands: o through po*.

4 Vendor VSA Support for CCOD Multiencapsulated PVCs in 802.1Q Tunnels

RADIUS supports circuit creation on demand (CCOD) multiencapsulated permanent virtual circuits (PVCs) in 802.1Q tunnels. Multiencapsulated CCOD is typically used in a scenario in which some subscribers have high-speed Internet service only, and others have voice over IP (VoIP) or Video-on-Demand (VoD) and optionally high-speed Internet. When the router receives a subscriber request for service, it queries the RADIUS server. The RADIUS server returns an authorization that informs the router about which type of C-VLAN (customer VLAN) encapsulation to provision:

- For customers subscribed to high-speed Internet services only, RADIUS authorizes the creation of a PPPoE-encapsulated 802.1Q PVC only.

- For customers subscribed to high-speed Internet services and that have VoIP, VoD, or both, RADIUS authorizes an on-demand multiencapsulated 802.1Q PVC and a static PPPoE-encapsulated 802.1Q PVC.

Table 16 and Table 17 lists the vendor VSAs that provide support for multiencapsulated CCOD 802.1Q PVCs. For details about these VSAs, see Table 7.

If the C-VLAN encapsulation type is PPPoE, the supported RADIUS Ericsson VSAs in the Access-Accept Accept message are listed in the following table:

Table 16   Vendor VSAs Supported in PPPoE-Encapsulated 802.1Q PVCs

#	VSA Name	Platform
39	PVC-Encapsulation-Type	SmartEdge SM-Family
40	PVC-Profile-Name	SmartEdge SM-Family
42	Bind-Type	SmartEdge SM-Family
43	Bind-Auth-Protocol	SmartEdge SM-Family
44	Bind-Auth-Max-Sessions	SmartEdge SM-Family
46	Bind-Auth-Context	SmartEdge SM-Family
89	Qos_Queuing	SmartEdge SM-Family

Table 16   Vendor VSAs Supported in PPPoE-Encapsulated 802.1Q PVCs

#	VSA Name	Platform
97	Agent-Circuit-Id	SmartEdge SM-Family
195	QoS-Overhead	SmartEdge SM-Family

If the C-VLAN encapsulation type is multi, the supported RADIUS vendor VSAs in the Access Accept message are listed in the following table:

Table 17   Vendor VSAs Supported in Multiencapsulated PVCs in 802.1Q Tunnels

#	VSA Name	Platform
39	PVC-Encapsulation-Type	SmartEdge SM-Family
40	PVC-Profile-Name	SmartEdge SM-Family
42	Bind-Type	SmartEdge SM-Family
43	Bind-Auth-Protocol	SmartEdge SM-Family
44	Bind-Auth-Max-Sessions	SmartEdge SM-Family
46	Bind-Auth-Context	SmartEdge SM-Family
89	Qos_Queuing	SmartEdge SM-Family
97	Agent-Circuit-Id	SmartEdge SM-Family
108	Bind-Auto-Sub-User	SmartEdge SM-Family
109	Bind-Auto-Sub-Context	SmartEdge SM-Family
110	Bind-Auto-Sub-Password	SmartEdge SM-Family
111	Circuit-Protocol-Encap	SmartEdge SM-Family
195	QoS-Overhead	SmartEdge SM-Family

5 Other Supported VSAs

Table 18 lists other supported VSAs. These VSAs require a vendor ID of 529.

Table 18   Other Supported VSAs

#	Attribute Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Response	Notes	Platform
242	Ascend-Data-Filter	No	Yes	Yes	Multivalue attribute. An Access-Accept packet contains multiple binary strings each representing a rule in an IP access control list (ACL). The rules are interpreted in the order they are received from the RADIUS server. If the RADIUS server returns both the router Filter-Id and Ascend-Data-Filter attributes for the same subscriber in the same direction, the Ascend-Data-Filter attribute is ignored, the router Filter-Id attribute is applied in that direction, and an event message to that effect is logged.ipv6 in forward dstip 10::1/64.	SmartEdge SM-Family

6 RADIUS Attributes Supported by RFlow

The following lists the RADIUS attributes supported by RFlow on the router. The format of the RADIUS attribute for RFlow profile is:

```
Flow-IP-Profile = "[{in|out|both}:<profile-name>]"
Attribute Type: STRING
Attribute Length: <Maximum length of flow ip profile name supported by CLI>
Attribute Id: 205
Note: only the following forms of the attribute are valid:
Flow-IP-Profile = "in:<profile-name>"
Flow-IP-Profile = "out:<profile-name>"
Flow-IP-Profile = "both:<profile-name>"
Flow-IP-Profile = ""
```

The type string of the VSA includes the Flow-IP-Profile attribute. The attribute value is defined as *dir:name*, where **dir** is **in**, **out**, or **both**, and **name** is a string that corresponds to the RFlow profile name configured on the router.

The following lists the standard RFlow RADIUS attributes that are supported by the router and that can appear in Access-Request and Access-Response messages:

- If you specify an invalid direction string a COA-Reject results.

- If you provision multiple Flow-IP-Profile attributes for the same subscriber, only the last instance takes effect. For example, if you specify **Flow-IP-Profile="in:p1"** on the RADIUS server and also specify **Flow-IP-Profile="out:p1"**, only **"out:p1"** is applied to the subscriber circuit.

- If you provision a subscriber with a CoA, the direction or profile can be changed dynamically during the life of the subscriber session.

- You can remove the actual RFlow profile configured under the subscriber profile, subscriber name, or subscriber default at any time. Removing the profile does not affect the RFlow profile applied to existing subscribers.

- If you do not provision the Flow-IP-Profile attribute, it does not bring down the subscriber session.

- You can remove an RFlow profile (unprovisioned) by sending a NULL attribute from the COA server—that is, you specify **Flow-IP-Profile=** for the subscriber.

66/1543-CRA 119 1170/1-V1 Uen K | 2011-10-29

7 Supported Service Attributes

Table 19 lists the service attributes that the SmartEdge router supports. These attributes appear in service profiles that a RADIUS server uses to specify the conditions for a subscriber session.

Table 19   Service Attributes Supported

Attribute Name	Description	Platform
Service-Interim-Accounting	Integer. Number of seconds after which the service accounting counters are updated. The range of values is 900 to 2,147,483,647. Before this attribute is sent to the SmartEdge PPA for processing, the value for the Service-Interim-Accounting attribute is rounded to the nearest integer that divides by 60 evenly. For example, if 925 is the value for the Service-Interim-Accounting attribute, the SmartEdge router rounds this integer to 900.	SmartEdge
Service-Timeout	Integer. Number of seconds after which a session times out. The range of values is 60 to 2,147,483,647.	SmartEdge
Service-Volume-Limit	Integer. Volume of traffic (in KB) in either the upstream or downstream direction after which a service for a subscriber session has exceeded its volume limit. The range of values is 0 through 2,147,483,647.	SmartEdge

8 RADIUS Attributes Supported by Mobile IP Services

For Mobile IP services, RADIUS attributes appear in various types of RADIUS messages, as described in the following sections.

8.1 Standard RADIUS Attributes and Mobile IP Services

The following list includes the standard Mobile IP service RADIUS attributes that are supported by the SmartEdge router and that can appear in Access-Request, Account-Request, and Access-Response messages:

- CUI

- Class

- Calling-Station-ID

- User-Name

- User-Password

- NAS-IP-Address

- NAS-Port

- Framed-IP-Address

- Idle-Timeout

- Message-Authenticator

- NAS-Identifier

- Ip-Address-Pool-Name

- Acct-Status-Type

- Acct-Input-Octets

- Acct-Multi-Session-ID—Set to the value of the AAA-Session-ID attribute, which is generated by the AAA server after the mobile node (MN) is successfully authenticated. This identifier is sent by the Access-Accept message, which is unique for each connectivity service network (CSN), and is used to match all accounting records in a session.

- Acct-Output-Octets

- Acct-Session-Id

- Acct-Session-Time

- Acct-Input-Packets

- Acct-Output-Packets

For more information about these attributes, see Section 2.1 on page 7 and Section 2.3 on page 20.

Note: For Mobile IP, the username is the mobile node (MN) Network Access Identifier (NAI).

8.2 3GPP2 RADIUS VSAs

Table 20 describes the Third Generation Partnership Project 2 (3GPP2) RADIUS VSAs used by Mobile IP services that are supported by the SmartEdge router and that can appear in Access-Request, Account-Request, and Access-Response messages. Mobile IP services complies with 3GPP2 standard X.S0011-001-C v3.0, `cdma2000 Wireless IP Network Standard: Introduction.`

Table 20   3GPP2 RADIUS VSAs Supported

#	Attribute Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Response	Description	Platform
7	Home Agent IP Address	Yes	Yes	No	IP address of the HA.	SmartEdge
57	MN-HA SPI	Yes	No	No	Integer. Security Parameter Index (SPI). Sent when the SPI is changing for the mode node (MN) along with the HA and MN shared secret key.	SmartEdge
58	MN-HA shared secret key	No	No	Yes	Octet string. Shared secret key used for MN and HA authentication.	SmartEdge
79	Foreign Agent Address	No	Yes	No	IP address of the foreign agent (FA).	SmartEdge

8.3 3GPP2 RADIUS VSAs That Can Be Reauthorized

Table 21 lists the 3GPP2 RADIUS VSAs used by Mobile IP services that are reauthorized when you enter the **`reauthorize`** command.

Table 21   3GPP2 RADIUS VSAs Supported by Reauthorization

#	Attribute Name	Description	Platform
57	MN-HA SPI	Integer. SPI. Sent when the SPI is changing for the MN, along with the HA and MN shared secret key.	SmartEdge
58	MN-HA shared secret key	Octet string. Shared secret key used for MN and HA authentication.	SmartEdge

8.4   WiMax Forum RADIUS VSAs

Table 22 lists the WiMax Forum RADIUS VSAs supported for Mobile IP and that can appear in Access-Request, Account-Request, and Access-Response messages.

Table 22   WiMax Forum RADIUS VSAs for Mobile IP Supported

#	Attribute Name	Sent in Access - Request	Sent in Acct-Request	Received in Access-Response	Description	Platform
1	WiMax-Capability	Yes	No	Yes	Type-length values (TLVs). Indicates the capabilities that the home agent (HA) supports, such as accounting and hotlining: • TLV ID 1: WiMAX release • TLV ID 2: Accounting capabilities • TLV ID 3: Hotlining capabilities • TLV ID 4: Idle Mode notification capabilities The WiMax-Capability attribute is optionally received in the access response message.	SmartEdge
3	GMT-Time-Zone-Off set	No	Yes	No	Integer. The difference in seconds between the HA and RADIUS server, in Greenwich Mean Time (GMT). This information is used to calculate local time. The GMT-Time-Zone-Offset attribute is optionally sent in the Acct-Request message.	SmartEdge
4	WIMAX-Session-ID	Yes[(1)]	No	Yes	Binary string. Unique identifier in the home network for the session set in the home network AAA server. The Received in Access-Response is also received in the CoA.	SmartEdge
6	hHA-IP-MIP4	Yes	No	No	IP address. IP address of the home agent (HA).	SmartEdge

Table 22   WiMax Forum RADIUS VSAs for Mobile IP Supported

#	Attribute Name	Sent in Access - Request	Sent in Acct- Request	Received in Access- Response	Description	Platform
10	MN-HA-MIP4-Key	No	No	Yes	Binary string. The shared secret key used for authentication between the mobile node (MN) and HA.	SmartEdge
11	MN-HA-MIP4-SPI	Yes	No	Yes	Integer. Security Parameter Index (SPI) that corresponds to the shared secret key used for mobile node (MN) and HA authentication. The HA includes this attribute in the Access-Request message to request the corresponding shared key from the RADIUS server. The RADIUS server includes this attribute in the Access-Response message and when it sends the CoA message to the HA to indicate that a new key will be used for subsequent MN and HA authentication or reauthentication for an existing mobile subscriber session.	SmartEdge
15	HA-RK-Key	No	No	Yes	Octet. Key used to generate FA-HA keys.	SmartEdge
16	HA-RK-SPI	Yes (Optional)	No	Yes	Integer. SPI associated with HA-RK-Key.	SmartEdge
17	HA-RK-Lifetime	No	No	Yes	Integer. Lifetime of the HA-RK-Key.	SmartEdge
18	RRQ-HA-IP	Yes	No	No	IP address. The IP address identified in the HA IP address file in the RRQ.	SmartEdge
19	RRQ-MN-HA-Key	No	No	Yes (Option al)	Encrypted string. MN-HA key bound to the HA IP address.	SmartEdge
24	Hotline-Indicator	No	Yes	Yes	String. Enables hotlining. Sent by RADIUS or COA server that is reported in the session and hotlining accounting records. The Hotline-Profile-ID and Hotline-Indicator enable hotlining.	SmartEdge
48	Acct-Input-Packets-Gigawords	No	Yes	No	Integer. Incremented when the standard RADIUS attribute 47, Acct-Input-Packets, overflows. The Sent in Acct-Request is optional.	SmartEdge
49	Acct-Output-Packets-Gigawords	No	Yes	No	Integer. Incremented when the standard RADIUS attribute 48, Acct-Output-Packets, overflows. The Sent in Acct-Request is optional.	SmartEdge
53	Hotline-Profile-ID	No	Yes	Yes	String. Hotlining profile identifier sent by RADIUS or CoA server. The Hotline-Profile-ID and Hotline-Indicator attributes enable hotlining.	SmartEdge

Table 22   WiMax Forum RADIUS VSAs for Mobile IP Supported

#	Attribute Name	Sent in Access - Request	Sent in Acct-Request	Received in Access-Response	Description	Platform
58	HA-RK-Key-Requested	Yes (if dynamic keys are required)	No	No	Integer. Flag indicating that the HA requires an HA-RK-Key.	SmartEdge
64	vHA-IP-MIP4	No	Yes	Yes	IP address. IP address of the visited HA from the AAA server.	SmartEdge

(1) Yes, if the Access-Request is sent for reauthentication.

8.5   WiMax Forum RADIUS VSAs in the CoA

Table 23 lists the WiMax Forum RADIUS VSAs supported for Mobile IP and that can appear in CoA-Request and CoA-Response messages. For details about these VSAs, see Table 22.

Table 23   WiMax Forum RADIUS VSAs for Mobile IP Supported

#	Attribute Name	Sent in CoA Request	Sent in CoA Response	Notes	Platform
4	WiMAX-Session-ID	Yes	No	Binary string. Unique identifier in the home network for the session set in the home network AAA server. The Received in Access-Response is also received in the CoA.	SmartEdge
24	Hotline-Indicator	Yes	No	String. Sent by RADIUS or CoA server that is reported in the session and hotlining accounting records. A CoA containing a Hotline-Profile-ID without an accompanying Hotline-Indicator deactivates hotlining for that profile	SmartEdge
53	Hotline-Profile-ID	Yes	No	String. Hotlining profile identifier sent by RADIUS or CoA. A CoA containing a Hotline-Profile-ID without an accompanying Hotline-Indicator deactivates hotlining for that profile.	SmartEdge

8.6   Motorola VSAs

Table 24 lists the Motorola VSAs supported for Mobile IP and that can appear in Access-Request, Account-Request, and Access-Response messages.

Table 24   Motorola VSAs for Mobile IP Supported

#	Attribute Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Response	Description	Platform
66	Coa_IPv4	Yes	No	No	IP Address. Care of Address in MIP RRQ. An FA can have multiple CoA addresses, and the HA IP address must be derived based on the CoA peer.	SmartEdge

Table 24   Motorola VSAs for Mobile IP Supported

#	Attribute Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Response	Description	Platform
67	FA-hHA-Key	No	No	Yes	Encrypted string. The FA-HA-key is used by the FA to create an FA-HA authentication extension. This field is protected with an encryption algorithm defined in RFC 2868, `RADIUS Attributes for Tunnel Protocol Support`, for Tunnel-Password.	SmartEdge
68	FA-hHA-Lifetime	No.	No	Yes	Integer. The amount of time in seconds that this FA-hHA-key can be used after it is fetched.	SmartEdge
69	FA-hHA-SPI	Yes (Optional)	No	Yes	Integer. The SPI for the FA-hHA-key. The FA-hHA-SPI can be sent in the Access Request to the AAA server if the foreign agent (FA) does not have a matching key corresponding to the key used by the home agent (HA) in a registration revocation message.	SmartEdge
70	EP-Request-Type	Yes	No	No	Integer. Sent to the CAPC/AAA server for each RRQ coming to the FA. Values are: • 0 - Reserved • 1 - MIP Context Request. The value of this attribute is 1 for Mobile FA subscribers. • 2 - Non-MIP context request. The value of this attribute is 2 for Fixed CLIPs subscribers.	SmartEdge
71	MN-FA-Key	No	No	Yes	Encrypted string. The MN-FA key used for MN-FA authentication.	SmartEdge
72	MN-FA-Lifetime	Nos	No	Yes	Integer. The amount of time in seconds that the MN-FA key can be used after the FA obtains it.	SmartEdge
73	MN-FA-SPI	Yes	No	Yes	Integer. The SPI associated with the MN-FA Key.	SmartEdge
74	FA-IP-MIP4	Yes	No	No	IP address. The IP address of the FA that received the MIP request and used to generate the MN-FA key for authentication.	SmartEdge
75	FA-vHA-key	No	No	Yes	Encrypted string. The FA-HA key used by the FA to create FA-HA authentication extension.	SmartEdge
76	FA-vHA-Lifetime	No.	No	Yes	Integer. The amount of time in seconds that this FA-hHA-Key can be used after the FA obtains it from the Authenticator within ASN-GW.	SmartEdge

Table 24   Motorola VSAs for Mobile IP Supported

#	Attribute Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Response	Description	Platform
77	FA-vHA-SPI	Yes (Optional)	No	Yes	Integer. The SPI for the FA-hHA-Key. This is the same value as the hHA-RK SPI.	SmartEdge
78	Accounting-Mode	No	No	Yes	Binary bit mask value. Received from the CAPC/AAA server in response to the AR. The Accounting-Mode is a bitmap with the following bit values: • 0x00 - No accounting. This value is assumed if the Accounting-Mode VSA is not included in the Access-Accept over R7. • 0x01 - IP-Session-based accounting. • 0x02 - Flow-based accounting. • 0x10 - Wait for RADIUS attributes parsing and applying result before sending accounting messages. • 0x11 - used by ASN-GW DP in Wimax 4.0	SmartEdge

9 RADIUS Attribute 49 Error Codes

This section lists the Ericsson terminate error codes and the Remote Authentication Dial-In User Service (RADIUS) attribute 49 (Acct-Terminate-Cause) error codes, which are included in Accounting-Stop messages, in the following tables:

- Table 25—Account termination error codes 0 to 99

- Table 26—Account termination error codes 100 to 220

RADIUS attribute 49 error codes and their definitions are included in RFC 2866, *RADIUS Accounting*.

Table 25   RADIUS Attribute 49 Termination Error Codes 0 to 99

Ericsson Terminate Error Code and Code Description	Attribute 49 Error Code and Code Description (VSA 142 Values)	Session Error Message (VSA 143 Values)	Platform
0 No Error	18 Host_Request	No error was recorded	SmartEdge SM-Family
1 Unknown Error	9 NAS_Error	No error was recorded	SmartEdge SM-Family
2 Error Not Specified	9 NAS_Error	No termination cause code was given by peer	SmartEdge SM-Family
3 Vendor Specific Error	9 NAS_Error	Vendor Specific Error	SmartEdge SM-Family
4-19 Not Used	0 INVALID		SmartEdge SM-Family
20 Session Timeout	5 Session_Timeout	Session Timeout	SmartEdge SM-Family
21 Setup_Timeout	15 Service_Unavailable	Couldn't establish a session within session timeout period	SmartEdge SM-Family
22 Bad_Session_ID	9 NAS_Error	Received packet with bad session ID	SmartEdge SM-Family
23 Unknown_Remote_Session_Error	9 NAS_Error	Remote peer sent general/unknown error for this session	SmartEdge SM-Family
24 Authentication_Failed	17 User_Error	Authentication Failure	SmartEdge SM-Family
25 Bind_Failed	15 Service_Unavailable	Failed to bind subscriber	SmartEdge SM-Family
26 Provision_Failed	15 Service_Unavailable	Subscriber provisioning failed	SmartEdge SM-Family

Table 25   RADIUS Attribute 49 Termination Error Codes 0 to 99

Ericsson Terminate Error Code and Code Description	Attribute 49 Error Code and Code Description (VSA 142 Values)	Session Error Message (VSA 143 Values)	Platform
27 No_Session	15 Service_Unavailable	Cannot find AAA_SESSION	SmartEdge SM-Family
28 Stale_Session	15 Service_Unavailable	Clearing stale AAA SESSION	SmartEdge SM-Family
29 Aging_Session	15 Service_Unavailable	Clearing unstable session due to XC Switchover	SmartEdge SM-Family
30 FSM_Timeout	9 NAS_Error	State Machine Timeout	SmartEdge SM-Family
31 FSM_Error	9 NAS_Error	State Machine Error	SmartEdge SM-Family
32-39 Not Used	0 INVALID		SmartEdge SM-Family
40 Session_Cleared	6 Admin_Reset	Session cleared by administrator	SmartEdge SM-Family
41 CCT_Cleared	6 Admin_Reset	Circuit cleared by administrator	SmartEdge SM-Family
42 Port_Admin_Down	6 Admin_Reset	Port shutdown by administrator	SmartEdge SM-Family
43 Port_Admin_Deleted	6 Admin_Reset	Port removed from configuration	SmartEdge SM-Family
44 CCT_Admin_Down	6 Admin_Reset	Circuit disabled by administrator	SmartEdge SM-Family
45 Peer_Admin_Down	6 Admin_Reset	Peer disabled by administrator	SmartEdge SM-Family
46 Admin_RAD_Test	23 Admin_Test	Radius test by administrator	SmartEdge SM-Family
47 Admin_RAD_Test	24 Auto_Test	Auto radius connectivity test	SmartEdge SM-Family
48 Admin_Logout	25 Admin_Logout	Administrator logout	SmartEdge SM-Family
49 SVC_Cleared	6 Admin_Reset	Service cleared by administrator	SmartEdge SM-Family
50-59 Not Used	0 INVALID		SmartEdge SM-Family
60 CCT_Unbound	6 Admin_Reset	The `no bind` command was entered on this circuit by the administrator	SmartEdge SM-Family

Table 25   RADIUS Attribute 49 Termination Error Codes 0 to 99

Ericsson Terminate Error Code and Code Description	Attribute 49 Error Code and Code Description (VSA 142 Values)	Session Error Message (VSA 143 Values)	Platform
61 CCT_Deleted	6 Admin_Reset	Circuit removed from configuration	SmartEdge SM-Family
62 Encaps_Changed	6 Admin_Reset	Circuit reset because of encapsulation change	SmartEdge SM-Family
63 Context_Deleted	3 Lost_Service	Context removed from configuration	SmartEdge SM-Family
64 Intf_Deleted	3 Lost_Service	Interface removed from configuration	SmartEdge SM-Family
65 Intf_Changed	3 Lost_Service	Interface configuration changed	SmartEdge SM-Family
66 Profile_Deleted	3 Lost_Service	Dynamic shaping profile was deleted	SmartEdge SM-Family
67 Port_Shutdown	6 Admin_Reset	Shutdown configured on port.	SmartEdge SM-Family
68 CCT_Shutdown	6 Admin_Reset	Shutdown configured on circuit.	SmartEdge SM-Family
69-79 Not Used	0 INVALID		SmartEdge SM-Family
80 NAS_Error	? INVALID		SmartEdge SM-Family
81 CCT_Mismatch	? INVALID		SmartEdge SM-Family
82-99 Not Used	0 INVALID		SmartEdge SM-Family

Table 26   RADIUS Attribute 49 Termination Error Codes 100 to 220

Ericsson Terminate Error Code and Code Description	Attribute 49 Error Code and Code Description (VSA 142 Values)	Session Error Message (VSA 143 Values)	Platform
100 Lost_Carrier	2 Lost_Carrier	Lost carrier	SmartEdge SM-Family
101 EC_Busy	9 NAS_Error	Busy signal, try again later	SmartEdge SM-Family
102 Bad_Framing	8 Port_Error	Incorrect or missing framing	SmartEdge SM-Family
103 No_Dialtone	9 NAS_Error	No dialtone detected	SmartEdge SM-Family

Table 26   RADIUS Attribute 49 Termination Error Codes 100 to 220

Ericsson Terminate Error Code and Code Description	Attribute 49 Error Code and Code Description (VSA 142 Values)	Session Error Message (VSA 143 Values)	Platform
104 No_Carrier	9 NAS_Error	No carrier detected	SmartEdge SM-Family
105 LMI_Down	2 Lost_Carrier	LMI declared PVC down or LMI control channel lost	SmartEdge SM-Family
106 Port_Down	2 Lost_Carrier	Port down	SmartEdge SM-Family
107 HDLC_Down	2 Lost_Carrier	HDLC down on circuit	SmartEdge SM-Family
108 CCT_Down	2 Lost_Carrier	Circuit down	SmartEdge SM-Family
109-129 Not Used	0 INVALID		SmartEdge SM-Family
130 Bad_Peer_Config	17 User_Error	Bad peer configuration, negotiation failed	SmartEdge SM-Family
131 Confrej_By_Peer	17 User_Error	Peer rejected required option(s)	SmartEdge SM-Family
132 Rej_IPCP	17 User_Error	Peer refused to negotiate IPCP	SmartEdge SM-Family
133 Peer_Req_Auth	17 User_Error	Peer required outbound authentication	SmartEdge SM-Family
134 No_Auth_Protocol	17 User_Error	Peer refused to negotiate an authentication protocol	SmartEdge SM-Family
135 LCP_Rej_Callback	17 User_Error	Peer refused to negotiate a callback	SmartEdge SM-Family
136 LCP_Fsm_Timeout	17 User_Error	LCP state machine timeout	SmartEdge SM-Family
137 Auth_Fsm_Timeout	17 User_Error	Authentication state machine timeout	SmartEdge SM-Family
138 No_LCP_Packets	2 Lost_Carrier	No LCP packets received from peer	SmartEdge SM-Family
139 LCP_Looped	2 Lost_Carrier	Link loopback detected	SmartEdge SM-Family
140 Recv_Term_Req	1 User_Request	Received PPP Terminate Request	SmartEdge SM-Family
141 Echo_Timeout	2 Lost_Carrier	No response to PPP keepalive from peer	SmartEdge SM-Family

Table 26   RADIUS Attribute 49 Termination Error Codes 100 to 220

Ericsson Terminate Error Code and Code Description	Attribute 49 Error Code and Code Description (VSA 142 Values)	Session Error Message (VSA 143 Values)	Platform
142 Idle_Timeout	4 Idle_Timeout	No traffic within idle timeout period	SmartEdge SM-Family
143 ABS_Timeout	5 Session_Timeout	Session absolute timeout expired	SmartEdge SM-Family
144 Layer_Down	9 NAS_Error	A PPP layer went down (LCP/IPCP/CHAP/PAP)	SmartEdge SM-Family
145 Rec_PADT	1 User_Request	Received PPPoE Active-Discovery Terminate from client	SmartEdge SM-Family
146 PPPOE_Real_CCT_Unbound	6 Admin_Reset	The circuit transporting the PPPoE session was unbound	SmartEdge SM-Family
147 IPCP_No_Addr	9 NAS_Error	No IP address was configured or pool was out of usable addresses	SmartEdge SM-Family
148 No_Confreq_Resp	17 User_Error	No response to PPP Confreq from peer	SmartEdge SM-Family
149 Rej_Crypto	1 User_Request	Peer rejected encryption, which is required by local policy	SmartEdge SM-Family
150 No_MP_Bundle	9 NAS_Error	Cannot find MP bundle	SmartEdge SM-Family
151 Traffic_Limit_Exceeded	10 NAS_Request	Traffic limit exceeded	SmartEdge SM-Family
152 Peer_LCP_Restart	1 User_Request	Received LCP confreq from remote peer after LCP was up	SmartEdge SM-Family
153 Term_ACK	1 User_Request	Received PPP Terminate Ack	SmartEdge SM-Family
154 Idle_Timeout_IN	4 Idle_Timeout	No traffic received within idle timeout period	SmartEdge SM-Family
155 Idle_Timeout_OUT	4 Idle_Timeout	No traffic transmitted within idle timeout period	SmartEdge SM-Family
156 MP_Master_Not_Up	9 NAS_Error	MP Master link did not come up	SmartEdge SM-Family
157 PPP_PPPoE_Sync_Timeout	15 Service_Unavailable	PPPoEd initiated cleanup, stuck pppoe session	SmartEdge SM-Family
158 PPPoE_Magic_Timeout	15 Service_Unavailable	PPPoEd initiated cleanup, no PPP magic received	SmartEdge SM-Family
159 PPPoE_Bind_Timeout	15 Service_Unavailable	PPPoEd Initiated cleanup, no subscriber binding received	SmartEdge SM-Family

Table 26   RADIUS Attribute 49 Termination Error Codes 100 to 220

Ericsson Terminate Error Code and Code Description	Attribute 49 Error Code and Code Description (VSA 142 Values)	Session Error Message (VSA 143 Values)	Platform
160 Tun_Cleared	6 Admin_Reset	Tunnel was cleared	SmartEdge SM-Family
161 Recv_Stopccn	3 Lost_Service	Received a StopCCN from peer	SmartEdge SM-Family
162 Rexmit_Timeout	3 Lost_Service	Control channel timeout - Remote peer dead	SmartEdge SM-Family
163 No_Ctrl_Conn	15 Service_Unavailable	Control packet received but no control channel exists	SmartEdge SM-Family
164 Bad_Len	9 NAS_Error	Length field did not match packet size or packet size invalid	SmartEdge SM-Family
165 Bad_Field	9 NAS_Error	A header field had an invalid value	SmartEdge SM-Family
166 Temp_Res_Fail	15 Service_Unavailable	Temporarily out of resource. Try later	SmartEdge SM-Family
167 Perm_Res_Fail	15 Service_Unavailable	Remote peer permanently lacks sufficient resources for session	SmartEdge SM-Family
168 Try_Another	10 NAS_Request	Remote peer was too busy to accept session. Try another peer	SmartEdge SM-Family
169 Unk_M_Avp	9 NAS_Error	Unknown Mandatory AVP	SmartEdge SM-Family
170 Bad_Dest	9 NAS_Error	Destination Invalid	SmartEdge SM-Family
171 Not Used	0 INVALID		SmartEdge SM-Family
172 Max_Tunnels	15 Service_Unavailable	Reached configured max-tunnels limit	SmartEdge SM-Family
173 Max_Sessions	15 Service_Unavailable	Reached configured max-sessions limit	SmartEdge SM-Family
174 Tunnel_Not_LNS	15 Service_Unavailable	Can't create session; Configured for LAC-only	SmartEdge SM-Family
175 No_Avail_Card	15 Service_Unavailable	Can't create LNS or LTS session: no available card	SmartEdge SM-Family
176 Wrong_Endpoints	9 NAS_Error	Wrong remote or local address received from peer	SmartEdge SM-Family
177-179 Not Used	0 INVALID		SmartEdge SM-Family

Table 26   RADIUS Attribute 49 Termination Error Codes 100 to 220

Ericsson Terminate Error Code and Code Description	Attribute 49 Error Code and Code Description (VSA 142 Values)	Session Error Message (VSA 143 Values)	Platform
180 Clips_Bounce	10 NAS_Request	CLIPS circuit was reset due to a 'clips-bounce' request	SmartEdge SM-Family
181-189 Not Used	0 INVALID		SmartEdge SM-Family
190 DHCP_Lease_Released	1 User_Request	Client released DHCP lease	SmartEdge SM-Family
191 DHCP_Lease_Expired	5 Session_Timeout	DHCP lease expired	SmartEdge SM-Family
192 DHCP_Server_Unavailable	15 Service_Unavailable	DHCP server is unavailable	SmartEdge SM-Family
193 DHCP_IPhost_Cleared	6 Admin_Reset	DHCP IP-host cleared	SmartEdge SM-Family
194 SESS_SBXC_SYNC_FAIL	15 Service_Unavailable	Standby sync failed	SmartEdge SM-Family
195 SESS_PROTECTION_SWITCH	13 Port_Preempted	Port protection switch	SmartEdge SM-Family
196 DHCP_IPHOST_Mismatch	17 User_Error	DHCP IP-host mismatch	SmartEdge SM-Family
197 DHCP_Lease_NACK	15 Service_Unavailable	DHCP lease nack'ed	SmartEdge SM-Family
198-199 Not Used	0 INVALID		SmartEdge SM-Family
200 CCOD_Idle_Down	6 Admin_Reset	CCOD Idle down timer expired for circuit	SmartEdge SM-Family
201-209 Not Used	0 INVALID		SmartEdge SM-Family
210 LI_Fail_Start	15 Service_Unavailable	Couldn't establish a session, Security Fail	SmartEdge SM-Family
211-219 Not Used	0 INVALID		SmartEdge SM-Family
220 MEM_ALLOC_ERROR	9 NAS_Error	Memory allocation failed	SmartEdge SM-Family