ERICSSON

Configuring L2TP

SYSTEM ADMINISTRATOR GUIDE

68/1543-CRA 119 1170/1-V1 Uen J

Contents

1 Overview

This document describes how to configure, monitor, and administer Layer 2 Tunneling Protocol (L2TP) peers and groups. This document also contains a list of the standard L2TP attribute-value pairs (AVPs) supported by the SmartEdge OS as well as a list vendor-specific AVPs.

The SmartEdge router functions as an L2TP access concentrator (LAC) or as an L2TP network server (LNS). In each context configured on the system, the SmartEdge router can function as a LAC to one or more LNSs, as an LNS to one or more LACs, or as both a LAC and an LNS.

LNSs and LACs are collectively referred to as L2TP peers.

The SmartEdge OS implementation of L2TP conforms to:

- RFC 2661, *Layer Two Tunneling Protocol "L2TP"*
- RFC 2809, *Implementation of L2TP Compulsory Tunneling via RADIUS*
- RFC 2867, *RADIUS Tunnel Accounting Support*
- RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*
- RFC 3145, *L2TP Disconnect Cause Information*
- RFC 3931*Layer Two Tunneling Protocol - Version 3 (L2TPv3)*

  The data plane specifications recommended in RFC 3931 are supported. The signal plan specifications are not supported

1.1 L2TP Features

The SmartEdge OS implementation of L2TP supports the following features:

- Context-specific L2TP peers and groups of peers
- User Datagram Protocol/Internet Protocol (UDP/IP) encapsulation
- LAC support for connections over any circuit that supports subscriber-based Point-to-Point Protocol (PPP)
- LAC and LNS support for IPv4, IPv6, and dual-stack subscriber services. See *Configuring IPV6 Subscriber Services* for information about configuring IPv6 and dual-stack subscriber services on the SmartEdge router
- Access link group support between the LAC and subscribers
- Ethernet and dotq link group support between the LAC and the LNS

- Multilink PPP (MLPPP) for L2TP subscribers
- LNS support for connections over any circuit that supports IP packets
- Configurable distribution of incoming LAC sessions
- Configuration of L2TP peers locally, in a SmartEdge OS configuration file, or remotely, on a RADIUS server
- Dynamic or static peer selection for subscriber circuits
- Configurable default settings for L2TP peers
- Anonymous (unnamed) peers to allow connections from peers that are not defined locally
- Support for combined LAC and LNS functions (tunnel switching) for a given subscriber
- Slot redundancy to allow incoming subscriber sessions to be distributed across multiple cards

  Note: Priority weighted-fair queuing (PWFQ) is not supported on cards configured for LNS slot redundancy.

1.2 L2TPv3 Features

RFC 3931 defines version 3 of L2TP (L2TPv3). When it is necessary to distinguish between L2TPv2 and L2TPv3 in this document, L2TP as defined in RFC 2661 is referred to as *L2TPv2*, and L2TP as defined in RFC 3391 is referred to as *L2TPv3*.

The SmartEdge OS implementation of L2TPv3 supports the following:

- QoS propagation for all packet payload types
  - 802.1p bits propagate from inner packet payload (VLAN) to the DSCP bits of the L2TPv3 tunnel outer IP header
  - IP DSCP bits propagate from inner packet payload (IP) to the DSCP bits of the L2Tpv3 tunnel outer IP header
- Termination of Ethernet and Ethernet VLAN PW transported through L2TPv3 into VPLS instances.
- Statically configurable inbound and outbound 32-bit cookies on a peer-by-peer basis
- Multiple sessions per peer. Each session can correspond to a different PW type, and the PWs can terminate at a VPLS bridge instance (as the current implementation assumes)

1.3 L2TP AVPs

For information about all standard and vendor-specific attribute-value pairs (AVPs) supported by the SmartEdge OS, see the section L2TP Attribute-Value Pairs. The vendor-specific AVPs are embedded according to the procedure recommended in RFC 2661, *Layer 2 Tunneling Protocol L2TP*.

When an LNS subscriber uses and L2TP tunnel, authentication is performed using RADIUS.

For information about configuring RADIUS and all standard and vendor-specific RADIUS attributes supported by the SmartEdge OS, see the document, *Configuring RADIUS*.

1.4 Requirements and Restrictions

- To configure L2TP functions and features, the software license for L2TP must be enabled; see *Enabling Licensed Features*.
- Unless otherwise noted, the SmartEdge 100 router supports all commands described in this document.
- When QoS propagation is enabled for static L2TPv3 encapsulation, the MPLS EXP values are updated as well. This can cause remote peers that validate the cookie to drop packets. As a workaround, configure class maps to set the EXP bits to 0. The workaround is described in detail in *Configuring L2TPv3 Tunnels on VPLS Pseudowires* in *Configuring VPLS*.
- LAC and LNS IPv6 and LAC and LNS dual-stack (IPv4 and IPv6) traffic is supported on IPv4 L2TP tunnels only. IPv6 L2TP tunnels are not supported on the SmartEdge router. When PPP sessions are terminated on a SmartEdge LNS, IPv6 packets are not fragmented on the LNS. The IPV6 packet is encapsulated in the IPv4 tunnel and the IPv4 tunnel packets are fragmented.

1.5 L2TP Tunnels and Peers

L2TP tunnels are UDP/IP-encapsulated circuits that carry subscriber-based PPP sessions to another router. The router is designated as an LNS or a LAC, depending on its tunnel function:

- When functioning as an LNS, the SmartEdge router accepts sessions from LACs in the network and can either terminate them or switch them to another LNS. The role of the LNS is terminating sessions.
- When functioning as a LAC, the SmartEdge router tunnels subscriber PPP sessions to a number of LNSs. The role of the LAC is aggregating subscriber sessions onto a tunnel.

Figure 1 shows a SmartEdge router, acting as a LAC, with connections to a pair of LNS peers.

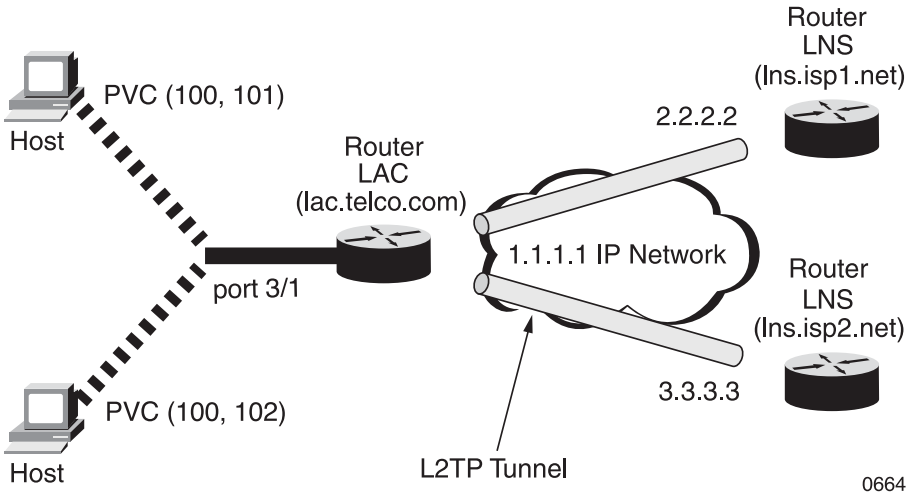

Figure 1 L2TP Tunnels over UDP/IP (664)

1.6 Tunnel Switching

The SmartEdge OS can also act as an L2TP tunnel switch (LTS), accepting PPP sessions over one tunnel and relaying them to other LNSs over another tunnel. A tunnel switch has aspects of both LAC and LNS operation.

Figure 2 shows two LACs (**lac1.com** and **lac2.com**) feeding into a tunnel switch (**switch.com**), which provides upstream connectivity to each indicated LNS (**lns1.net** and **lns2.net**). In this figure the following configurations have been made:

- The two LACs are configured to tunnel appropriate PPP sessions (perhaps all of them) to **switch.com**
- Each LNS is configured to accept an L2TP tunnel from **switch.com**.

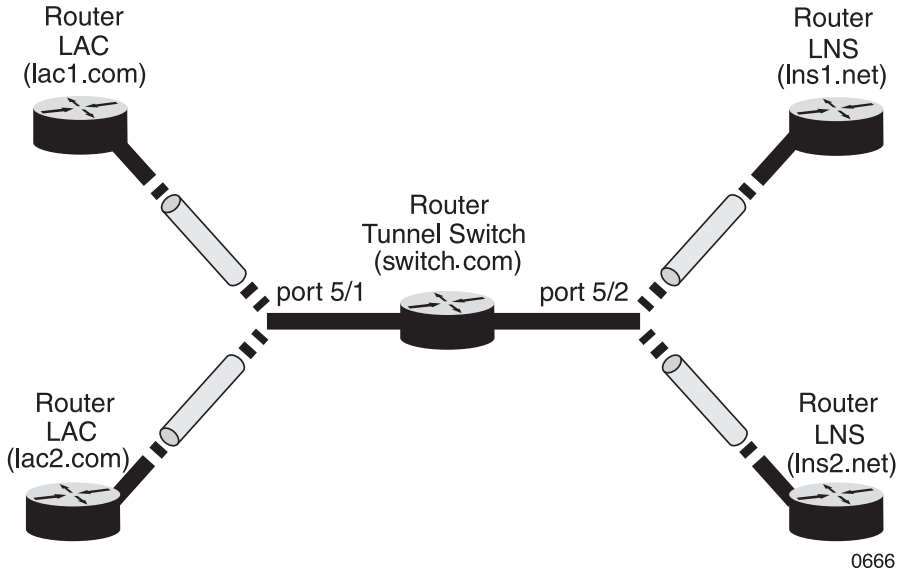

Figure 2 L2TP Tunnel Switching (666)

1.7 L2TP Peer Groups

An L2TP peer group is a group of LNS peers among which PPP sessions are distributed by the SmartEdge router when functioning as a LAC. The group members, the group itself, and the LAC are all configured in the same context. Peers must be defined prior to inclusion in a group.

1.7.1 Session Distribution

PPP sessions are distributed among the peers in a group according to the algorithm specified in the **`algorithm`** command in L2TP group configuration mode. The algorithm options are:

- Strict priority

  Each peer is assigned a priority that corresponds to the order in which the peers are created; the highest priority peer is the one that is created first. With strict priority distribution, sessions are directed to the highest priority peer, unless connectivity to that peer is lost (the peer is labeled “dead”) or the maximum number of tunnels and sessions to the peer has been reached. After that, sessions are directed to the peer with the next highest priority. If two or more peers have the same priority, sessions are load balanced among them.

- Load balancing

  Each session is directed to the peer that has the fewest sessions at the moment so that sessions are distributed across peers in the group equally. If peers have assigned priorities, they are ignored.

- Weighted-round-robin

  Each session is directed to a peer that is chosen using a weighted-round-robin algorithm to calculate the priority (weight). The peer with the lowest weight receives the most sessions.

Each algorithm is subject to the maximum number of tunnels and the maximum number of sessions configured for the peers that are members of the group. For example, if the strict priority algorithm is specified and the maximum sessions limit is reached on the highest-priority peer, additional sessions are sent to the next highest-priority peer.

When an LNS peer is not reachable (regardless of the algorithm being used), it is labeled “dead” for a period of time. There is no further attempt to reach a “dead” peer until the dead-time has expired, unless one of the following conditions is true:

- If a peer is not a member of a group or is the only member of a group, the deadtimer is not enforced unless it is configured to be enforced, using the **`l2tp strict-deadtime`** command in context configuration mode.
- If all peers in a group are “dead”, there is an immediate attempt to re-establish a connection with at least one of them.

When a session is being brought up, the system attempts to establish a tunnel to any “dead” peer in the group. A peer is not marked as “alive” until the system can successfully establish a tunnel to it.

1.7.2 RADIUS and Accounting Considerations

The RADIUS Tunnel-Preference attribute determines which peer has the highest priority when using the strict priority algorithm. Lower preference numbers have higher priority.

When some peers have a tunnel preference and some do not, the ones without a tunnel preference are considered of lower priority than those with a tunnel preference.

A new L2TP tunnel is created by a RADIUS server when one of the three following conditions occurs:

- All existing tunnels have the maximum number of sessions active.
- A new peer is created and a session is assigned to it.
- The **`l2tp admin test`** command (in exec mode) is issued by an administrator to create a tunnel.

An L2TP peer is created when one of the following standard RADIUS attributes is received and its value does not match that for any existing peer:

- Tunnel-Server-Endpoint (RADIUS attribute 66)

- Tunnel-Client-Endpoint (RADIUS attribute 67)
- Tunnel-Assignment-Id (RADIUS attribute 82)

Only attribute 66 is required, but the others, if provided, are also used to search for an exact match. These attributes are found in the *RADIUS Attributes* document.

L2TP peers that are configured by a RADIUS server can be automatically removed from memory should they be marked as “inactive”, using the **`l2tp clear-radius-peer`** command in context configuration mode. An inactive peer is one for which the session count has been zero (0) for a configurable period of time.

If L2TP tunnel or session accounting is enabled, accounting messages are sent to a RADIUS server. Types of messages include Tunnel-Start, Tunnel-Stop, Link Start, Link Stop. For more information about configuring L2TP accounting, see the document, *Configuring Mobile IP for a Foreign Agent*.

If a LAC sends AVPs 24 (Tx Connect Speed) and 38 (Rx Connect Speed) or just AVP 24 to the SmartEdge router, the SmartEdge OS inserts the speeds in RADIUS attribute 77 (Connect-Info) and includes it in RADIUS Access-Accept and Accounting-Request messages. The format of attribute 77 in this case is Tx/Rx with the / character separating the two speeds. Speeds are provided in bits per second. If only AVP 24 is present, the format is Tx. The inclusion of only the Rx speed is not supported.

1.8 Mapping Subscribers to Peers

In addition to mapping a subscriber to a specific peer (static selection), the SmartEdge OS supports three types of dynamic selection:

- Dynamic context selection—***`sub-name@ctx-name`***
- Dynamic peer selection—***`sub-name@l2tp-peer-name`***
- Dynamic peer group selection—***`sub-name@l2tp-group-name`***

To specify dynamic selection for a subscriber, each peer or peer group must have a name (or domain alias) identical to a SmartEdge OS context name or to an alias name for the context.

The SmartEdge OS maps the subscriber’s PPP session to a peer or peer group with the same name or domain alias as the ***`@domain`*** portion of the structured subscriber name used by that subscriber.

Note: The separator character between the subscriber name and the context, L2TP peer, or L2TP group name argument is configurable and can be any of %, -, @, _, \\, #, and /. For information about configuring the separator character, see the document, *Configuring Mobile IP for a Foreign Agent*. The default value is @, which is used throughout this document.

1.9 Slot Redundancy

Slot redundancy allows you to configure alternate cards for L2TP sessions when the SmartEdge router is acting as an LNS or LTS. With slot redundancy, subscriber sessions from a LAC are automatically switched to another card if the card on which the sessions are running is shut down for any reason (such as a card reload). Slot redundancy also allows sessions from a given LAC peer to be distributed among multiple cards. Various types of redundancy are possible; some choices are:

- Load balance all sessions between multiple cards
- Give preference to the card with the route to the LAC and load balance across alternate cards after the first card has exceeded the maximum number of sessions allowed on it
- Establish 1+1 redundancy with one card having preference over a second card
- Assign sessions to one or more cards based on preference

Figure 3 shows the slot redundancy configured in the SmartEdge router **lns.com**. The card in slot **3** is the card with the route to the LAC; two slots, **4** and **5**, are configured to accept the subscriber sessions from the LAC when the card in slot **3** is running at full capacity. All three cards pass the traffic to the Internet using the card in slot **12**. The commands to implement this slot redundancy configuration are provided in the example in the L2TP Slot Redundancy for a LAC Peer section.

Slot redundancy is fully configurable, and online changes do not affect current sessions. For example, if card **5** is removed from the configuration for slot redundancy, the sessions on that card are not disrupted; however, no new sessions are assigned to it.

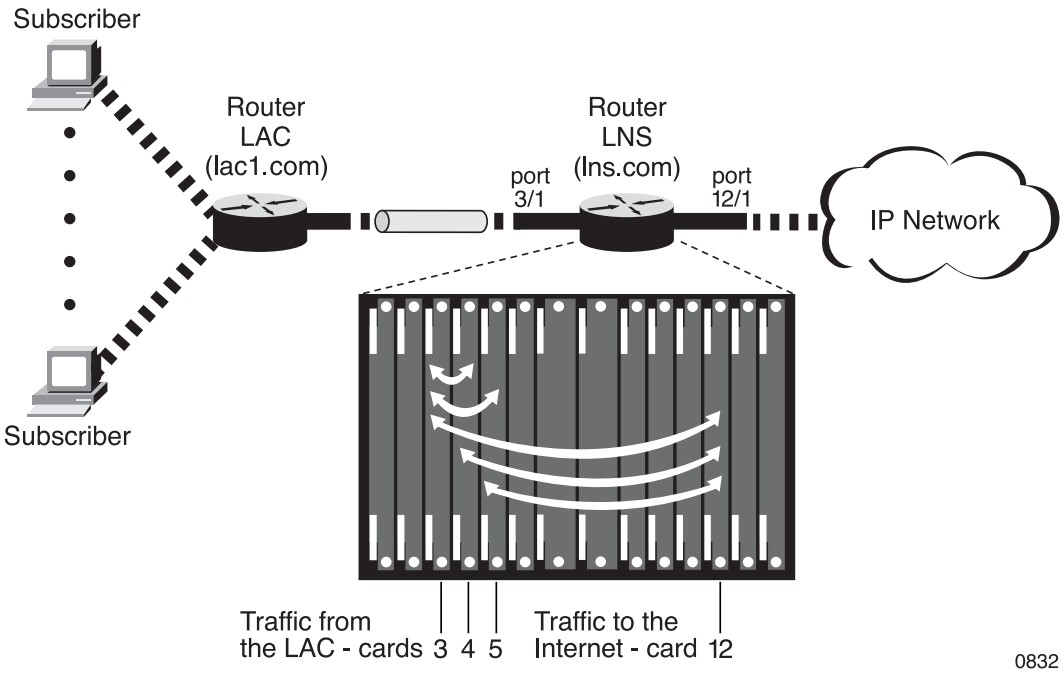

Figure 3 L2TP Slot Redundancy (832)

1.10 QoS Considerations

The SmartEdge OS supports the attachment of quality of service (QoS) metering, policing, and queuing policies to LNS subscriber sessions; queuing policies are restricted to priority weighted fair queuing (PWFQ) policies which are supported only on Gigabit Ethernet 3 (GE3) and Gigabit Ethernet 1020 (GE1020) traffic cards. However, slot redundancy is not supported for queuing policies; if an LNS subscriber session moves to a port on a different slot, it is no longer governed by the PWFQ policy attached to the LNS subscriber session. For more information about QoS policies and attaching them to LNS subscriber sessions, see the document, *Configuring Circuits for QoS*.

1.11 Avoiding Unwanted Fragmentation and Reassembly

In IP networks, it is generally preferable to avoid fragmentation when possible, because it can exacerbate packet loss and the reassembly of fragments consumes resources on host computers. By its nature, the L2TP protocol makes packets larger because it must add headers to encapsulate the packet, thus making fragmentation situations more likely to occur than with normal Internet traffic.

The L2TP software on the SmartEdge router offers administrator the choice of several solutions to manage fragmentation. The options available depend on the role of the SmartEdge router:

- Increase the minimum transmission unit (MTU) setting (the SmartEdge OS role is a LAC or LNS)

  You can increase the MTU setting between the SmartEdge router and the L2TP peer so that neither tunnel endpoint is required to fragment packets toward the other. We recommend increasing the MTU value to 1,700 bytes. Use the **`ip mtu`** command in the interface configuration mode to change the MTU setting.

  Note: For this solution to work, the entire path between the LAC and LNS must support an MTU of 1,700 bytes.

- Require a smaller maximum receive unit (MRU) in the initial Link Control Protocol (LCP) negotiation (the SmartEdge OS role is a LAC)

  Use the **`ppp peer-options`** command in global configuration mode to attempt to negotiate a smaller MRU between the PPP clients and the SmartEdge router. This can be done at either the LAC or LNS end of the tunnel. For complete documentation of this command, see the document, *Configuring PPP and PPPoE*.

- Force LCP renegotiation on MRU mismatch (the SmartEdge OS role is an LNS)

  This option causes the SmartEdge router to examine the proxy LCP information sent by the LAC, if available. The SmartEdge router determines if the client and LAC negotiated MRU values would lead to fragmentation, and if so, restarts LCP negotiation to configure lower MRU values. If the MRU values negotiated between client and LAC are acceptable, no renegotiation is forced.

  Use the **`l2tp renegotiate lcp`** command in context configuration mode to specify the conditions under which the SmartEdge router renegotiates the LCP options.

If fragmentation cannot be avoided, the SmartEdge router, when acting as an LNS, gives the administrator a choice between forcing fragmentation of the user packet (the inner packet) or the encapsulating L2TP packet (the outer packet). If the L2TP packet is fragmented, the LAC performs the reassembly. If the user packet is fragmented, the subscriber's computer performs the reassembly. To enable fragmentation of the user packet or L2TP packet, use the **`l2tp-fragment`** command in context configuration mode.

1.12 MLPPP for L2TP Subscribers

Multilink PPP (MLPPP) is an extension to PPP that allows a peer to use a more than one physical link for communication. When using more than one physical

link to connect two peers, you need a mechanism to do load balancing for the connection across the two (or more) links in the MLPPP bundle. MLPP fragments the datagrams and sends them across the multiple links in the bundle in a way that optimizes use of the media.

MLPP can be configured for L2TP subscribers. Using this form of MLPP, you do not create the MLPPP bundles; instead, the SmartEdge OS creates them dynamically, using the endpoint discriminator sent by the peer during the LCP negotiation and the subscriber name to determine whether to create a new MLPPP bundle or add the session to a current MLPPP bundle.

To use this form of MLPP, you must use ports configured on a GE traffic card that has a packet processing ASIC (PPA) version 2 (PPA2) on both the LNS and L2TP access concentrator (LAC). This form of MLPP is not supported when the L2TP Tunnel Switch (LTS) is enabled. For more information about MLPP and configuring MLPP for L2TP subscribers, see the document, *Configuring PPP and PPPoE*.

1.13 Link Aggregation for L2TP

Link aggregation allows a peer to use more than one FE or GE port for communication to load balance traffic and optimize the use of the physical links.

There are three types of link groups:

- Ethernet —Ethernet groups are network-facing (or trunk) link groups and bundle IPoE encapsulated circuits. They can be configured between a LAC and an LNS.
- dot1q—dot1q groups are network-facing (or trunk) link groups and bundle 802.1Q PVCs. They can be configured between a LAC and an LNS.
- Access—Access link groups are subscriber-facing and bundle either PPPoE or 802.1Q single- or double-encapsulated (Q-in-Q) circuits. They can be configured between a LAC and a subscriber.

To use link groups, you must use FE or GE ports configured on a GE traffic card on the LAC or LNS.

For more information about link aggregation and configuring Ethernet, dot1q, and access link groups, see *Configuring Link Aggregation*.

1.14 Terminology

Note: When IP Version 6 (IPv6) addresses are not referenced or explicitly specified, the term IP address can refer generally to IP Version 4 (IPv4) addresses, IPv6 addresses, or IP addressing. In instances where IPv6 addresses are referenced or explicitly specified, the term IP address refers only to IPv4 addresses.

2 L2TP Configuration and Operations Tasks

For information about troubleshooting L2TP, see the troubleshooting L2TP section in the *BRAS Troubleshooting Guide*.

2.1 L2TP Configuration Guidelines

Consider the following guidelines when configuring an L2TP peer or group:

- The following guidelines apply to L2TP names:
  - L2TP peer and group names must be unique within a context.
  - An L2TP group name can be used in commands where an L2TP peer name can be used.
  - To enable the use of a shorter service name for an L2TP peer, it is common to specify the fully qualified domain name for the peer or peer group in the **`l2tp-peer`** or **`l2tp-group`** command, and create the service name as a domain alias, using the **`domain`** command in L2TP peer or L2TP group configuration mode.
- The following guidelines apply to L2TP domain aliases:
  - Because a hostname for a peer or a group can be unwieldy—often in the form of a fully qualified domain name—the SmartEdge OS allows you to create a domain alias for the context for each peer and peer group. For example, a peer can have a fully qualified domain name of hssi_3_0.chi.core.isp.net, but you can refer to this peer as isp.net. You use these aliases for assigning tunnels to subscribers only.
  - You can create multiple domain aliases for a context to allow unique domain aliases for the peers and groups configured in the context.
  - You can assign multiple domain aliases to a peer or group.
  - You can specify a domain alias for an L2TP peer or group wherever the fully qualified L2TP peer or group name appears; for example, in the **`tunnel name`** command in subscriber configuration mode.
- The following guidelines apply to L2TP groups:
  - You must create the group in the same context as the LNS peers that include its members; a group cannot include any LNS peer that is not created in the same context as the group.
  - You must create an LNS peer before you can assign it to a group of peers.

- The following guidelines apply to subscriber sessions that are tunneled:
  - To allow subscriber sessions to be tunneled, you must have configured PPP for the subscriber circuit.
  - A subscriber session is directed towards one peer in a group of peers if that group has a domain alias that matches the domain of the session. Similarly, a subscriber session is directed towards an individual peer if that peer has a domain alias that matches the domain of the session.
- The following guidelines apply to slot redundancy:
  - Sessions are load balanced across traffic cards that are assigned equal preference.
  - Each traffic card can support up to 16,000 active subscriber sessions; to support more sessions from a single LAC, you can specify additional cards using the either **`priority`** or **`route`** keyword.
  - You must explicitly configure the traffic cards using the **`card`** command (in global configuration mode) prior to configuring slot redundancy for them. Sessions are not assigned to unconfigured traffic cards.

2.2 Configuring a Context for L2TP Peers and Groups

Configuring L2TP peers and groups is context-specific. You configure certain attributes that apply to all L2TP peers and groups configured in a context, unless otherwise noted; to configure these attributes, perform the tasks described in Table 1.

Note: The commands listed in task 3 are all optional and are meant only to help solve an operational problem; do not use these commands unless the L2TP is not functioning correctly and the Technical Assistance Center (TAC) directs you to include them in the L2TP configuration.

Table 1 Configure a Context for L2TP Peers and Groups

Step	Task	Root Command	Notes
1.	Create or select the context for the named, default, or unnamed peer or peer group, and access context configuration mode.	*context*	Enter this command in global configuration mode.
2.	Create a domain alias for the context.	*domain (L2TP peer)*	Optional. You can enter this command multiple times.
3.	Specify optional attributes for L2TP:		

Table 1 Configure a Context for L2TP Peers and Groups

Step	Task	Root Command	Notes
	Specify the Tunnel-Server-Auth-ID RADIUS attribute as its peer name if Tunnel-Assignment-ID RADIUS attribute is not present.	*l2tp radius-peer*	Enter this command in context configuration mode.
	Enable any inactive L2TP peer configured by a RADIUS server in this context to be automatically removed from memory.	*l2tp clear-radius-peer*	
	Specify the conditions under which the SmartEdge router, when acting as an LNS, renegotiates with a LAC.	*l2tp renegotiate lcp*	
	Select the type of fragmentation.	*l2tp fragment*	
	Enable proxy authentication for LAC peers.	*l2tp proxy-auth*	Enabled by default.
	Populate the L2TP Receive (Rx) Connect Speed or Transmit (Tx) Connect Speed attribute-value pair (AVP) from a custom source.	*l2tp avp*	
	Pass subscriber calling information to an L2TP network server (LNS) in a Dialed Number Identification Service (DNIS) AVP.	*l2tp avp calling-number*	
	Enable the L2TP process to transmit the Calling-Number AVP # 22 in the Incoming-Call-Request (ICRQ).	*dnis generate*	

Table 1 Configure a Context for L2TP Peers and Groups

Step	Task	Root Command	Notes
	Enable the SmartEdge router configured as an LNS to propagate physical port information that is compatible with an SMS router configured as an LAC.	*l2tp avp nas-port-id format all*	The default behavior for the SmartEdge router configured as the LNS is to send the fixed string, `256/17`, to the RADIUS server.
	Enable the SmartEdge router configured as an LAC to propagate physical port information that is compatible with an SMS router configured as an LNS.	*l2tp avp nas-port-id format all*	The default behavior for the SmartEdge router configured as the LAC is that AVP #49 is not sent to the LNS.
	Specify the conditions under which the SmartEdge router, when acting as a Layer 2 Tunneling Protocol (L2TP) network server (LNS) renegotiates the Link Control Protocol (LCP) options with an L2TP access concentrator (LAC).	*l2tp renegotiate lcp*	
	Specify the maximum receive unit (MRU) size used during renegotiation.	*l2tp renegotiate mru*	
4.	Specify optional timers:		
	Set the minimum amount of time for which a peer not within an L2TP group is marked as “dead”.	*l2tp deadtime*	

2.3 Configuring an LNS Peer

The SmartEdge router can provide LAC functions for a number of subscriber circuits, with each subscriber circuit configured to use either dynamic peer selection or a static connection to a specific LNS peer.

You can configure either a named or default LNS peer when the SmartEdge router acts as a LAC; a default peer allows you to create a set of defaults for the peer configuration attributes. Then when creating a named peer, all the settings of the default peer apply to the configuration of the named peer except for those that you choose to redefine.

To configure a named LNS peer, you must know the hostname that it uses during the establishment of the tunnel to it. To configure either a named or default LNS peer, perform the tasks described in Table 2.

Table 2 Configure an LNS Peer

Step	Task	Root Command	Notes
1.	Configure the context attributes for this peer.		For a complete list of commands, see Table 1.
2.	Create the named or default peer and access L2TP peer configuration mode.	*l2tp-peer*	Enter this command in context configuration mode.
3.	Associate a description with this LNS peer.	*description (L2TP peer)*	
4.	Specify the role of the SmartEdge router as a LAC for this LNS peer.	*function*	Specify the **`lac-only`** keyword; this is the default value.
5.	Assign a domain alias for this LNS peer.	*domain (L2TP peer)*	Assign at least one of the domain aliases created for the context in step 2 in Table 4.
6.	Create a local name for the SmartEdge router to use in packets sent to the LNS peer.	*local-name*	The default value is system hostname.
7.	Configure the L2TP tunnel time-out value.	*cleanup-timer*	If no subscriber sessions have been connected over the L2TP tunnel for a time greater than or equal to the specified time, the tunnel is disconnected. In the default state, tunnels with named peers do not time out. For tunnels with unnamed peers, the default time-out is 60 seconds. Supported on all traffic cards.
8.	Specify one or more operational attributes (all attributes are optional):		
	Limit the number of tunnels allowed for this LNS peer.	*max-tunnels*	

Table 2 Configure an LNS Peer

Step	Task	Root Command	Notes
	Limit the number of sessions allowed for this LNS peer.	*max-sessions*	
	Queue incoming out-of-order L2TP packets until the expected next sequence packet is received.	*message-reordering*	ECMP can cause L2TP packets to be received out of- order You can monitor out-of-order packets using the following command: **`show l2tp counter peer`** ***`peer-name`*** **`tunnel`**
	Specify an authorization key used by the LNS peer to encrypt and decrypt information sent on the control channel.	*tunnel-auth key*	
	Specify the number of unacknowledged control messages that can be sent by this LNS peer (the value to send in the Receive-Window-Size AVP).	*tunnel-window*	
9.	Specify one or more timing attributes (all attributes are optional):		
	Specify the interval before sending an L2TP Hello packet to this LNS peer if there has been no control message activity between this peer and the SmartEdge router.	*hello-timer*	
	Specify the timeout value for an acknowledgment message before a control message is retransmitted to this LNS peer.	*timeout (L2TP Peers)*	
	Specify the number of retries that an unacknowledged control message is retransmitted to this LNS peer before the tunnel is brought down.	*retry*	

2.4 Configuring an LNS Peer Group

When the SmartEdge router is acting as a LAC, you can configure a group of LNS peers. To configure an LNS peer group, perform the tasks described in Table 3.

Table 3 Configure an LNS Peer Group

Step	Task	Root Command	Notes
1.	Configure the context attributes for this peer group.		For a complete list of commands, see Table 1.
2.	Configure the LNS peers to be included in this group.		For a complete list of commands, see Table 1.
3.	Create the L2TP peer group and access L2TP group configuration mode.	*l2tp-group*	Enter this command in context configuration mode.
4.	Specify attributes for the peer group:		
	Assign a domain alias for this L2TP peer group.	*domain (L2TP peer)*	Assign at least one of the domain aliases created for the context in step 2 in Table 1.
	Specify the algorithm by which sessions are assigned to the LNS peers in the group.	*algorithm*	
	Set the minimum amount of time for which a peer within an L2TP group is marked as “dead”.	*deadtime*	
5.	Add an existing LNS peer to the L2TP group.	*peer*	

2.5 Configuring a LAC Peer

The SmartEdge router can provide LNS functions for a number of LACs. You can configure either a named, default, or unnamed (anonymous) peer when the SmartEdge router acts as an LNS; a default peer allows you to create a set of defaults for the peer attributes. Then when creating a named peer, all the settings of the default peer apply to the configuration of the named peer, except for those that you choose to redefine.

Slot redundancy allows you to configure multiple cards to carry L2TP subscriber sessions to a LAC. With slot redundancy, sessions are automatically switched to another card if the card on which the subscriber sessions are running, is shut down for any reason.

To configure a named peer, you must know the hostname that the LAC peer uses during the establishment of the tunnel to the SmartEdge router.

To configure a named, default, or unnamed (anonymous) LAC peer, perform the tasks described in Table 4.

Table 4 Configuring a LAC Peer

Step	Task	Root Command	Notes
1.	Configure the context attributes for this peer.		For a complete list of commands, see Table 1.
2.	Create the named, default, or unnamed peer, and access L2TP peer configuration mode.	*l2tp-peer*	Enter this command in context configuration mode.
3.	Associate a description with this peer.	*description (L2TP peer)*	
4.	Specify the role of the SmartEdge router as an LNS for this LAC peer.	*function*	Specify the **`lns-only`** keyword.
5.	Specify a domain alias for this LAC peer.	*domain (L2TP peer)*	Specify one of the domain aliases created for the context in step 2 in Table 1.
6.	Create a local name for the SmartEdge router to use in packets sent to the LAC peer.	*local-name*	The system hostname is the default.
7.	Configure slot redundancy for this LAC peer with both of the following tasks:		
	Select the algorithm for slot redundancy.	*lns card*	Specify the **`selection`** keyword.
	Specify a card and its preference.	*lns card*	Specify the **`preference`** keyword. Enter this command for each card that carries L2TP subscriber sessions to the LAC.
8.	Configure the L2TP tunnel time-out value.	*cleanup-timer*	If no subscriber sessions have been the connected over the L2TP tunnel for a time greater than or equal to the specified time, the tunnel is disconnected. In the default state, tunnels with named peers do not time out. For tunnels with unnamed peers, the default time-out is 60 seconds. Supported on all traffic cards.

Table 4 Configuring a LAC Peer

Step	Task	Root Command	Notes
9.	Specify operational attributes (all attributes are optional):		
	Limit the number of tunnels allowed for this peer.	*max-tunnels*	Specify at least two tunnels for quick recovery if problems occur.
	Limit the number of sessions allowed for this peer.	*max-sessions*	
	Queue incoming out-of-order L2TP packets until the expected next sequence packet is received.	*message-reordering*	ECMP can cause L2TP packets to be received out of order. You can monitor out-of-order packets using the following command: **`show l2tp counter peer`** ***`peer-name`*** **`tunnel`**
	Specify an authorization key used by the L2TP peer to encrypt and decrypt information sent on the control channel.	*tunnel-auth key*	
	Specify the number of unacknowledged control messages that can be sent by this L2TP peer.	*tunnel-window*	
	Specify the method used by the SmartEdge router when acting as an L2TP LNS to authenticate subscriber sessions that arrive from this peer.	*session-auth*	
10.	Specify timing attributes (all attributes are optional):		
	Specify the interval before sending an L2TP Hello packet to an L2TP peer if there has been no control message activity between the peer and the SmartEdge router.	*hello-timer*	

Table 4 Configuring a LAC Peer

Step	Task	Root Command	Notes
	Specify the time-out value for an acknowledgment message before a control message is retransmitted to an L2TP peer.	*timeout (L2TP Peers)*	
	Specify the number of retries that an unacknowledged control message is retransmitted to an L2TP peer before the tunnel is brought down.	*retry*	

2.6 Configuring a Subscriber for L2TP Peer Selection

When the SmartEdge router is acting as a LAC, you must specify either dynamic or static peer selection for the subscriber sessions. To specify peer selection, perform the task described in Table 5; enter all commands in subscriber configuration mode.

Table 5 Configuring a Subscriber for L2TP Peer Selection

Task	Root Command	Notes
Select the peer or peer group for a subscriber with one of the following tasks:		
Enable dynamic peer selection.	*tunnel domain*	Uses the domain portion of the subscriber name to match a configured peer or group.
Enable static peer selection.	*tunnel name*	

2.7 Configuring an L2TP Tunnel Switch

When the SmartEdge router acts as a tunnel switch, it acts as an LNS to incoming subscriber circuits and as a LAC to the LNS peers to which it switches those subscriber circuits. To configure the SmartEdge router as an L2TP tunnel switch, perform the tasks described in Table 6. To allow the subscriber sessions to be switched, each subscriber must have a domain name that matches the domain alias for the LNS to which the subscriber's sessions are switched.

Table 6 Configure an L2TP Tunnel Switch

Step	Task	Root Command	Notes
1.	Configure the context for the L2TP tunnel switch.		For a complete list of commands, see Table 1.

Table 6 Configure an L2TP Tunnel Switch

Step	Task	Root Command	Notes
2.	Create an LNS peer for each upstream peer.		For a complete list of commands, see Table 2. Perform this step for each LNS peer to which the subscriber sessions are switched.
3.	Create a LAC peer for each downstream peer.		For a complete list of commands, see Table 4. Perform this step for each LAC peer from which subscriber sessions are switched.
4.	Configure a subscriber record for each subscriber to be switched.		For a complete list of commands, see Table 5. The domain name for each subscriber must match the domain alias for the LNS to which the subscriber session will be switched.

2.8 L2TPv3 Configuration

See *Configuring L2TPv3 Tunnels on VPLS Pseudowires* in *Configuring VPLS* for L2TPv3 configuration guidelines.

2.9 L2TP Peer and Group Operations

To monitor and administer Layer 2 Tunneling Protocol (L2TP) peers and groups, perform the appropriate task listed in Table 7. Enter the **`clear`** and **`l2tp`** commands in exec mode; enter the **`show`** commands in any mode.

For information about troubleshooting L2TP, see the troubleshooting L2TP section in the *BRAS Troubleshooting Guide*.

Table 7 L2TP Peer and Group Operations

Task	Root Command
Shut down one or more tunnels or sessions with an L2TP peer or group.	*show flow admission-control profile*
Display tunnels information of an L2TP peer or group.	*debug l2tp*
Gracefully enable or disable the connection to a L2TP peer.	*l2tp admin*
Perform L2TP tunnel and session testing.	*l2tp admin test*

Table 7 L2TP Peer and Group Operations

Task	**Root Command**
Display configuration commands for L2TP groups and peers.	*show configuration (circuits)*
Display global L2TP information.	*show l2tp global*
Display L2TP group information.	*show l2tp group*
Display L2TP peer information.	*show l2tp peer*
Display L2TP tunnel counter information.	*show l2tp counters peer*

3 Configuration Examples

This section provides functional examples that configure the SmartEdge router to act as a connected LAC and as a connected LNS.

For information about troubleshooting L2TP, see the troubleshooting L2TP section in the *BRAS Troubleshooting Guide*

3.1 SmartEdge Router as a LAC

In the examples in this section, the SmartEdge router, with system hostname, **telco.com**, acts as a LAC to two LNSs of an ISP. With these examples, if a subscriber specifies ***sub-name*@isp1.net**, the SmartEdge OS connects the subscriber's PPP session to the LNS peer **lns1.isp.net**; if a subscriber specifies ***sub-name*@isp2.net**, the SmartEdge OS connects the subscriber's PPP session to either of the LNS peers in the group.

The following L2TP tasks show the basic configuration:

- Context Aliases
- LNS Peers
- Group of LNS Peers
- Subscribers

3.1.1 Context Aliases

The following example shows how to enter the **local** context and configure domain aliases for the context for use with two LNS peers:

```
[local]telco.com(config)#context local
[local]telco.com(config-ctx)#domain isp1.net
[local]telco.com(config-ctx)#domain isp2.net
[local]telco.com(config-ctx)#end
```

3.1.2 LNS Peers

This example shows how to create a tunnel to each LNS peer and specify a domain alias for the peer, the local name for the SmartEdge router, and the key to be used by the peer to authenticate the establishment of the tunnel:

```
[local]telco.com(config)#context local
[local]telco.com(config-ctx)#l2tp-peer name lns1.isp.net media udp-ip remote ip 2.2.2.1 local 1.1.1.1
[local]telco.com(config-l2tp)#function lac-only
[local]telco.com(config-l2tp)#domain isp1.net
[local]telco.com(config-l2tp)#local-name lac1.isp.net
[local]telco.com(config-l2tp)#tunnel-auth key SeCrEt1
[local]telco.com(config-l2tp)#end
```

A second LNS peer is configured in a similar fashion as follows:

```
[local]telco.com(config)#context local
[local]telco.com(config-ctx)#l2tp-peer name lns2.isp.net media udp-ip remote ip 2.2.3.1 local 1.1.1.1
[local]telco.com(config-l2tp)#function lac-only
[local]telco.com(config-l2tp)#local-name lac2.isp.net
[local]telco.com(config-l2tp)#tunnel-auth key SeCrEt2
[local]telco.com(config-l2tp)#end
```

3.1.3 Group of LNS Peers

The following example shows how to create an L2TP group, **group1**, assign a domain alias, **ips2.net**, set the session algorithm to **load balance**, set the deadtime to **15** minutes, and add two existing LNS peers to the group:

```
[local]telco.com(config-ctx)#l2tp-group name group1
[local]telco.com(config-l2tp-group)#domain isp2.net
[local]telco.com(config-l2tp-group)#algorithm load-balance
[local]telco.com(config-l2tp-group)#deadtime 15
[local]telco.com(config-l2tp-group)#peer name lns1.isp.net
[local]telco.com(config-l2tp-group)#peer name lns2.isp.net
[local]telco.com(config-l2tp-group)#end
```

3.1.4 Subscribers

The following examples show how to configure subscribers for the LAC.

3.1.4.1 Dynamic Peer Selection

The following example shows how to enable dynamic peer selection for all subscribers in the **local** context:

```
[local]telco.com(config)#context local
[local]telco.com(config-ctx)#subscriber default
[local]telco.com(config-sub)#tunnel domain
[local]telco.com(config-sub)#end
```

3.1.4.2 Static Peer Selection

The following example shows how to specify that a PPP session for subscriber **fred** is always tunneled to the LNS peer, **lns1.isp.net**:

```
[local]telco.com(config)#context local
[local]telco.com(config-ctx)#subscriber name fred
[local]telco.com(config-sub)#tunnel name lns1.isp.net
[local]telco.com(config-sub)#end
```

3.2 SmartEdge Router as an LNS

In the examples in this section, the SmartEdge router, with system hostname, **isp.net**, acts as an LNS for an ISP. The following L2TP tasks show the basic configuration:

3.2.1 Context Alias

The following example shows how to enter the **local** context and configure a domain alias for the context for use with a LAC peer:

```
[local]isp.net(config)#context local
[local]isp.net(config-ctx)#domain isp1.net
[local]isp.net(config-ctx)#end
```

3.2.2 LAC Peer

The following example shows how to configure a SmartEdge router to act as an LNS for a LAC peer. It is assumed that subscriber records exist either locally or on a RADIUS server for configuring and authenticating subscriber sessions.

```
[local]isp.net(config)#context local
[local]isp.net(config-ctx)#l2tp-peer name lac1.isp.net media udp-ip remote ip 10.1.1.1
[local]isp.net(config-l2tp)#function lns-only
[local]isp.net(config-l2tp)#domain isp1.net
[local]isp.net(config-l2tp)#local-name lns1.isp.net
[local]isp.net(config-l2tp)#tunnel-auth key SeCrEt1
[local]isp.net(config-l2tp)#session-auth chap pap
[local]isp.net(config-l2tp)end
```

3.3 SmartEdge Router as a Tunnel Switch

The following example shows how to set up tunnel switching in which all PPP sessions that arrive at the tunnel switch (the SmartEdge router, **switch.com)**, over the downstream tunnels **lac1.com** and **lac2.com** are mapped into an upstream tunnel selected according to the structured subscriber name. For example, if a subscriber specifies **joe@lns2.net**, the SmartEdge OS places the session into the tunnel to **lns2.net**; a subscriber, **fred**, is tunneled to the **lns1.net** LNS.

The following example shows how to set up the tunnel switch, **switch.com**,. in the **local** context, with the domain alias names, **lnscom1** and **lnscom2**; the LAC peer, **lac.com**; and the LNS peers, **lns1.net** and **lns2.net**. It also shows

how to create two subscribers, **joe** and **fred**, and specify the LNS for each, using the domain alias for each LNS.

```
!Configure the context for the switch
[local]switch.com(config)#context local
[local]switch.com(config-ctx)#aaa authentication subscriber none
[local]switch.com(config-ctx)#domain lnscom1
[local]switch.com(config-ctx)#domain lnscom2
[local]switch.com(config-if)#exit

!Configure the LAC peer (LNS side of the switch)
[local]switch.com(config-ctx)#l2tp-peer name lac.com media udp-ip remote-ip 10.1.1.1
[local]switch.com(config-l2tp)#function lns-only
[local]switch.com(config-l2tp)#exit

!Configure the LNS peers (LAC side of the switch)
[local]switch.com(config-ctx)#l2tp-peer name lns1.net media udp-ip remote-ip 10.3.1.1
[local]switch.com(config-l2tp)#function lac-only
[local]switch.com(config-ctx)#domain lnscom1
[local]switch.com(config-l2tp)#exit
[local]switch.com(config-ctx)#l2tp-peer name lns2.net media udp-ip remote-ip 10.4.1.1
[local]switch.com(config-l2tp)#function lac-only
[local]switch.com(config-ctx)#domain lnscom2
[local]switch.com(config-l2tp)#exit

!Configure a named subscriber for lns1.net
[local]switch.com(config-ctx)#subscriber name joe
[local]switch.com(config-sub)#tunnel name lnscom1
[local]switch.com(config-sub)#exit

!Configure a named subscriber for lns2.net
[local]switch.com(config-ctx)#subscriber name fred
[local]switch.com(config-sub)#tunnel name lnscom2
[local]switch.com(config-sub)#exit
```

3.4 L2TP Slot Redundancy for a LAC Peer

The following example shows how to configure slot redundancy for a LAC peer, as shown in Figure 3. Because slot **3** has the route to the LAC, it is preferred for subscriber sessions up to the maximum allowed for the card; the configuration establishes that additional sessions are to be load balanced between cards **4** and **5**.

```
!Configure the LAC peer
[local]switch.com(config-ctx)#l2tp-peer name lac.com media udp-ip remote-ip 10.1.1.1
[local]switch.com(config-l2tp)#function lns-only

!Configure the alternate traffic cards for slot redundancy
[local]Redback(config)#card gigaether-4-port 3
[local]Redback(config)#card gigaether-4-port 4
[local]Redback(config)#card gigaether-4-port 5

!Select the algorithm and specify the card preferences
[local]Redback(config-l2tp)#lns card selection route
[local]Redback(config-l2tp)#lns card 4 preference 20
[local]Redback(config-l2tp)#lns card 5 preference 20
```

4 L2TP Attribute-Value Pairs

Table 8 lists the standard L2TP AVPs supported by the SmartEdge OS, in order by AVP number.

Table 8 Standard L2TP AVPs Supported by the SmartEdge OS

Num	AVP Name	Mandatory	May be Hidden	Message Types Used In	Notes
0	Message Type	Yes (see Notes)	Yes	All	2-octet unsigned integer. Must be the first AVP in a message. When Mandatory (M)-bit=1, tunnel must be cleared if message type is unknown to the implementation. If M-bit=0, unknown message type can be ignored.
1	Result Code	Yes	No	CDN StopCCN	2-octet unsigned integer plus an optional error code and optional error message.
2	Protocol Version	Yes	No	SCCRP SCCRQ	1-octet unsigned integer for the version and 1-octet unsigned integer for the revision.
3	Framing Capabilities	Yes	Yes	SCCRP SCCRQ	32-bit mask with 2 bits defined. The A-bit indicates whether asynchronous framing is supported. The S-bit indicates whether synchronous framing is supported.
4	Bearer Capabilities	Yes	Yes	SCCRP SCCRQ	32-bit mask with 2 bits defined. The A-bit indicates whether analog access is supported. The D-bit indicates whether digital access is supported.
5	Tie Breaker	No	No	SCCRQ	8-octet value used to select a single tunnel when both LAC and LNS simultaneously request a tunnel. Lower value equals higher priority.
6	Firmware Revision	No	Yes	SCCRP SCCRQ	2-octet unsigned integer encoded in a vendor-specific format.
7	Host Name	Yes	No	SCCRP SCCRQ	String. Arbitrary number of octets, with a minimum length of 1 octet.

Table 8 Standard L2TP AVPs Supported by the SmartEdge OS

Num	AVP Name	Mandatory	May be Hidden	Message Types Used In	Notes
8	Vendor Name	No	Yes	SCCRP SCCRQ	Vendor-specific string.
9	Assigned Tunnel ID (L2TPv2) Assigned Connection ID (L2TPv3)	Yes	Yes	SCCRP SCCRQ StopCCN	L2TPv2 Assigned Tunnel ID is a 2-octet, non-zero unsigned integer. L2TPv3 Assigned Connection ID is a 4-octet, non-zero unsigned integer.
10	Receive Window Size	Yes	No	SCCRP SCCRQ	2-octet unsigned integer.
11	Challenge	Yes	Yes	SCCRP SCCRQ	1 or more octets of random data.
12	Q.931 Cause Code	Yes	No	CDN	Returned Q.931 cause code and returned Q.931 message code in their native ITU encodings. Optional ASCII text advisory message can also be included.
13	Challenge Response	Yes	Yes	SCCCN SCCRP	16-octet value.
14	Assigned Session ID	Yes	Yes	CDN ICRP ICRQ OCRP OCRQ	2-octet, non-zero unsigned integer. For L2TPv3 tunnels, the Session ID is a 4-octet, nonzero unsigned integer.
15	Call Serial Number	Yes	Yes	ICRQ OCRQ	32-bit value.
16	Minimum BPS	Yes	Yes	OCRQ	32-bit value indicating minimum speed in bits per second.
17	Maximum BPS	Yes	Yes	OCRQ	32-bit value indicating maximum speed in bits per second.
18	Bearer Type	Yes	Yes	ICRQ OCRQ	32-bit mask with 2 bits defined. The A-bit indicates if the call refers to an analog channel. The D-bit indicates if the call refers to a digital channel. Both bits can be set. For ICRQ messages, it is also valid to set neither.

Table 8 Standard L2TP AVPs Supported by the SmartEdge OS

Num	AVP Name	Mandatory	May be Hidden	Message Types Used In	Notes
19	Framing Type	Yes	Yes	ICCN OCCN OCRQ	32-bit mask with 2 bits defined. The A-bit indicates asynchronous framing. The S-bit indicates synchronous framing.
21	Called Number	Yes	Yes	ICRQ OCRQ	ASCII string.
22	Calling-Number	Yes	Yes	ICRQ	ASCII string used to encode the originating number for the incoming call.
23	Sub-Address	Yes	Yes	ICRQ OCRQ	ASCII string.
24	Tx Connect Speed	Yes	Yes	ICCN OCCN	4-octet value indicating the speed in bits per second. Used to inform the LNS of rate-limited speed, as required by carriers supporting PPPoE, PPPoA, and PPPoEoA. The Tx Connect Speed get populated with the upstream and downstream rates received through ANCP from the DSLAM when the SmartEdge router is used as an LAC.
25	Physical Channel ID	No	Yes	ICRQ OCRP	4-octet value for logging purposes only. Sent to RADIUS from the LNS side. Encodes the vendor specific physical channel number used for a call.
26	Initial Received LCP CONFREQ	No	Yes	ICCN	Arbitrary number of octets. A copy of the body of the initial CONFREQ received, starting at the first option within the body of the LCP message.
27	Last Sent LCP CONFREQ	No	Yes	ICCN	Arbitrary number of octets. A copy of the body of the final CONFREQ sent to the client to complete LCP negotiation, starting at the first option within the body of the LCP message.

Table 8 Standard L2TP AVPs Supported by the SmartEdge OS

Num	AVP Name	Mandatory	May be Hidden	Message Types Used In	Notes
28	Last Received LCP CONFREQ	No	Yes	ICCN	Arbitrary number of octets. A copy of the body of the final CONFREQ received from the client to complete LCP negotiation, starting at the first option within the body of the LCP message.
29	Proxy Authen Type	No	Yes	ICCN	2-octet unsigned integer.
30	Proxy Authen Name	No	Yes	ICCN	String. Arbitrary number of octets.
31	Proxy Authen Challenge	No	Yes	ICCN	String. 1 or more octets.
32	Proxy Authen ID	No	Yes	ICCN	2-octet unsigned integer.
33	Proxy Authen Response	No	Yes	ICCN	String. Arbitrary number of octets.
34	Call Errors	Yes	Yes	WEN	Includes the following fields: Reserved, CRC Errors, Framing Errors, Hardware Overruns, Buffer Overruns, Time-out Errors, and Alignment Errors.
35	ACCM	Yes	Yes	SLI	Send and Receive ACCM are each 4-octet values preceded by a 2-octet reserved quantity.
36	Random Vector	Yes	No	All	String of arbitrary length. Must precede the first AVP with the Hidden (H) bit set. More than one can be used per message. Hidden AVP uses the Random Vector AVP most closely preceding it.
37	Private Group	No	Yes	ICCN	Arbitrary number of octets.

Table 8 Standard L2TP AVPs Supported by the SmartEdge OS

Num	AVP Name	Mandatory	May be Hidden	Message Types Used In	Notes
38	Rx Connect Speed	No	Yes	ICCN OCCN	4-octet value indicating the speed in bits per second. The Rx Connect Speed get populated with the upstream and downstream rates received through ANCP from the DSLAM when the SmartEdge router is used as an LAC.
39	Sequencing Required	Yes	No	ICCN OCCN	This AVP has no value field. Indicates that sequence numbers must be present on the data channel. The Ericsson implementation of L2TP prefers not to require sequencing. Therefore, if the SmartEdge router is functioning as a LAC, it never requests this attribute. However, if the LNS uses it, the LAC honors it. If the SmartEdge router is functioning as an LNS, it honors an LAC's request for this attribute, but never volunteers it.
46	PPP Disconnect Cause	No	Yes	CDN	2-octet value in network byte order and a string of arbitrary length.

Redback vendor-specific AVPs are embedded according to the procedure recommended in RFC 2661, *Layer 2 Tunneling Protocol L2TP*. Table 9 lists the vendor-specific L2TP AVPs supported by the SmartEdge OS, in order by AVP number.

Table 9 Redback Vendor-Specific L2TP AVPs Supported by the SmartEdge OS

Num	AVP Name	Mandatory	May be Hidden	Message Types Used In	Notes
1	Rbak HURL	No	No	L2TP-HURL	String containing the URL from the **`pppoe url`** command in the subscriber record.
2	Rbak MOTM	No	No	L2TP-HURL	String containing the MOTM defined on the LNS side of the tunnel.

Glossary

DNIS
Dialed Number Identification Service

GE1020
Gigabit Ethernet 1020

GE3
Gigabit Ethernet 3

ICRQ
Incoming-Call-Request

IPv4
IP Version 4

IPv6
IP Version 6

L2TP
Layer 2 Tunneling Protocol

L2TPv3
Layer Two Tunneling Protocol - Version 3

LAC
L2TP access concentrator

LCP
Link Control Protocol

LNS
(L2TP) network server

LNS
L2TP network server

LTS
L2TP Tunnel Switch

LTS
L2TP tunnel switch

MLPPP
Multilink PPP

MP
Multilink PPP

PPP
Point-to-Point Protocol

TAC
Technical Assistance Center

UDP/IP
User Datagram Protocol/Internet Protocol