L2TP for Subscriber Access — LAC

In This Chapter

This section provides information about L2TP for subscriber access.

Topics in this section include:

Applicability

This example is applicable to the 7750 SR-c4/c12, SR-7/12 with IOM3/IMMs (LNS facing port) and describes L2TP Access Concentrator (LAC) support for the L2TP Aggregation Architecture (LAA) model and was tested on SROS-11.0.R4. PPP hosts are supported in a Routed CO model (with IES or VPRN services) using ATM, Ethernet or Ethernet over Pseudo wire SAPs. A description of the L2TP Tunnel Switch (LTS) and L2TP Network Server (LNS) functions are out of the scope of this example.

Overview

PPP Access Architectures (PTA versus LAA)

The Broadband Forum proposes two architectures for Point-to-Point Protocol (PPP) access.

- The PPP Termination Aggregation Architecture (PTA)
- The L2TP Aggregation Architecture (LAA)

The PTA architecture (local-access model) uses the Broadband Network Gateway (BNG) to terminate user PPP sessions (see scenario PPPoE-5 in Figure 375).

The LAA architecture (which is a tunneled-access model) uses a LAC to transport PPP sessions from the LAC to an LNS which performs tunnel termination (see scenario PPPoE-1 and PPPoE -2 in Figure 375).

Optionally an LTS can be used in the transport network to perform the grooming of traffic between tunnels (see scenarios PPPoE-3 and PPPoE-4 in Figure 375).

The LNS is the logical termination point of the PPP sessions originated by the remote clients and tunneled by the LAC/LTS.

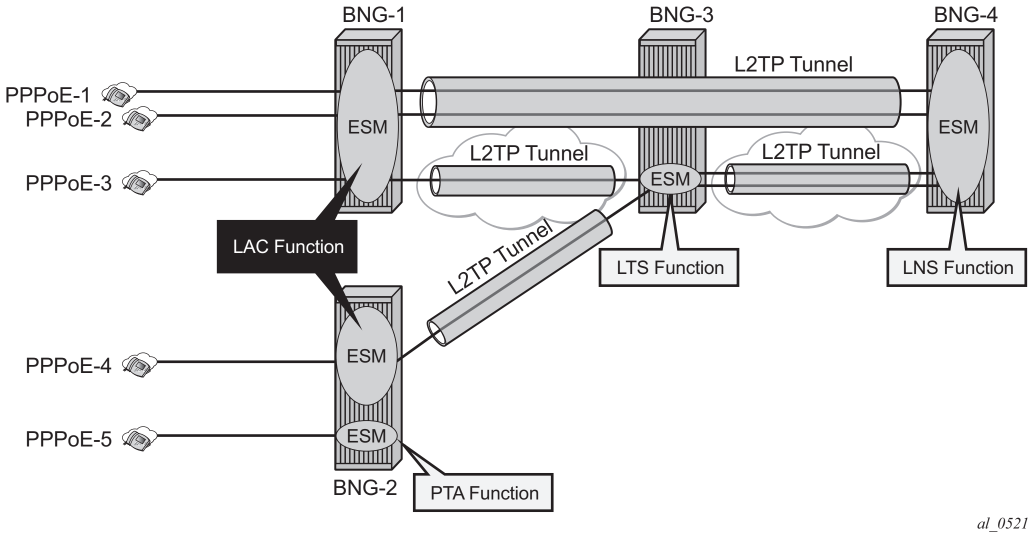


Figure 375: Network Topology

Supported L2TP Encapsulations

The router instance where the L2TP tunnel starts and where ESM is handled can be one and the same but does not need to be the same. The LNS peer address can be reachable via IP, BGP/IGP shortcuts, over a spoke SDP (GRE/MPLS), RFC 4364 VPRNs (*BGP/MPLS IP Virtual Private Networks*), but cannot be an address belonging to a directly connected interface. See Figure 376.

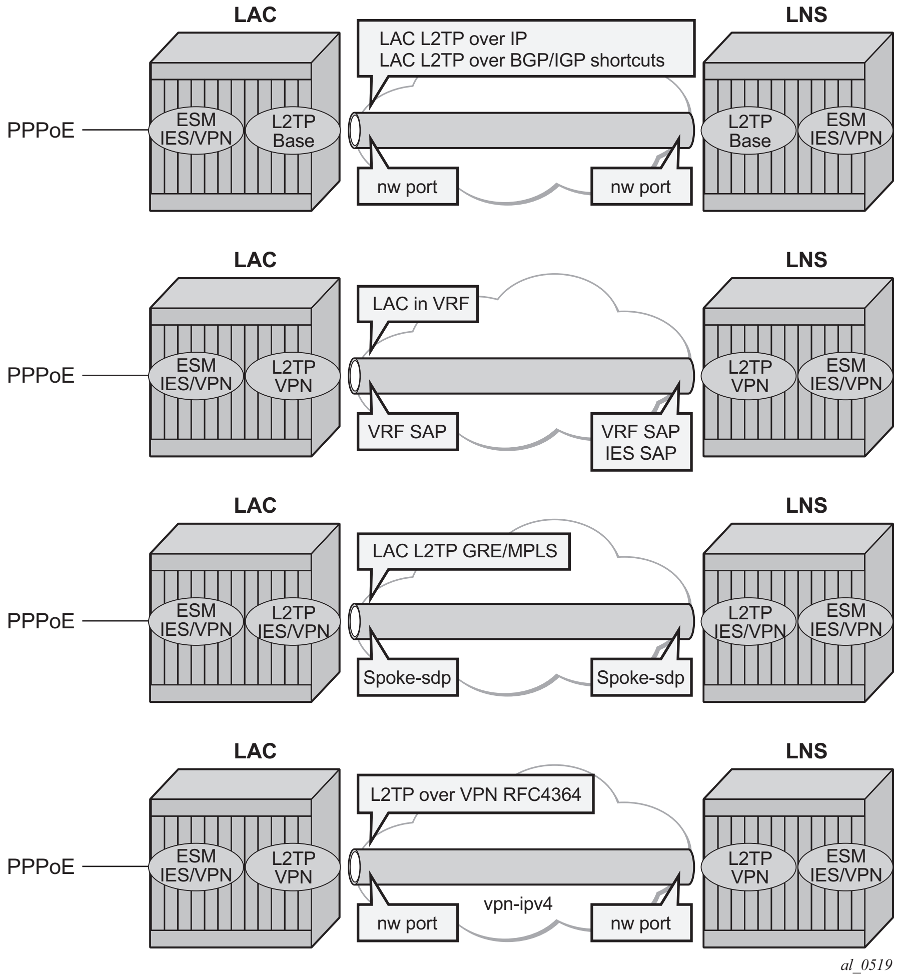


Figure 376: Supported LT2P Encapsulations

Recap of the L2TPv2 Protocol

L2TPv2 is a client-server protocol that encapsulates Layer 2 packets such as PPP, for transmission across a network and uses two different UDP message types:

- Control messages—L2TP passes control and data messages over separate control and data channels. The in-band control channel passes sequenced control connection management, call management, error reporting and session control messages. Optionally a shared-secret challenge authentication method can be used between the tunnel endpoints. The following messages are used for L2TP tunnel session setup, teardown and keepalive.
  - ç Tunnel setup (Control Connection Management)
    - Start-Control-Connection-Request (SCCRQ)
    - Start-Control-Connection-Reply (SCCRP)
    - Start-Control-Connection-Connected (SCCCN)
    - Stop-Control-Connection-Notification (StopCCN)
  - ç Tunnel keepalive
    - Hello (HELLO)
  - ç Session setup (Call management) over an existing tunnel
    - Incoming-Call-Request (ICRQ)
    - Incoming-Call-Reply (ICRP)
    - Incoming-Call-Connected (ICCN)
    - Call-Disconnect-Notify (CDN)

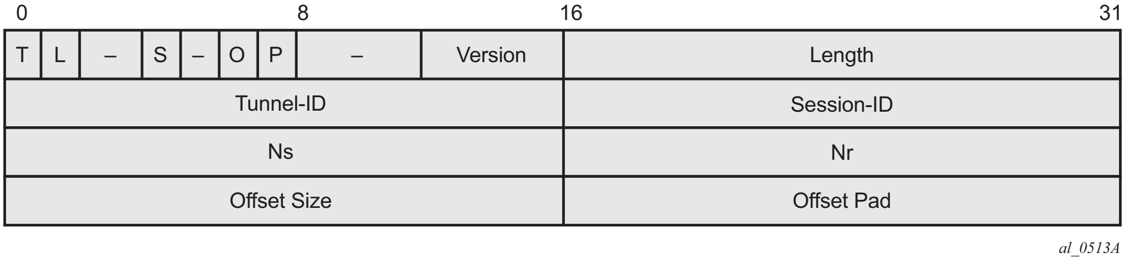
  The Zero-Length Body (ZLB) message is a control packet with only an L2TP header. ZLB messages are used for explicitly acknowledging packets on the reliable control channel.

  To maximize extensibility while still permitting interoperability, a uniform method for encoding message types and bodies is used throughout L2TP via Attribute Value Pairs (AVP).
- Data messages — Data messages are used to encapsulate PPP frames that are sent into the L2TP tunnel.

L2TPv2 sessions run over an L2TP tunnel and are referenced by an L2TP session-id. An L2TP tunnel can carry none, one or multiple L2TP sessions. An L2TP session corresponds to a PPPoE session. L2TPv3 for LAC-LNS dynamic tunnel setup is not supported.

L2TP Header and AVP Layout

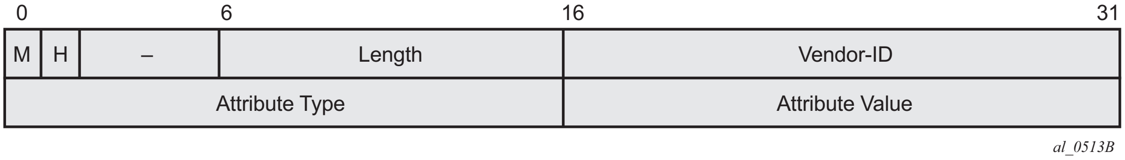
The L2TPv2 header consists of following fields (RFC 2611, *URN Namespace Definition Mechanisms*):



Field	Description
T	Type of L2TP message (1 bit): 0—data message 1—control message
L	Indicates if the optional Length field is present in the message (1 bit): 0—the field is left out of the message entirely 1—the field is included (must be included in control messages)
-	Reserved for future use, must be set to zero.
S	Indicates if the Ns and Nr fields are present (1 bit): 0—the fields are left out of the message entirely 1—the fields are included (must be included in control messages)
O	Indicates if the Offset field is present (1 bit): 0—the field is left out of the message entirely (must be left out of control messages) 1—the field is included
P	Used with data messages only. Indicates priority of the data message (1 bit): 0—no (this value is used for all control messages) 1—yes
Version	The version of the message (4 bits): 2—this is the latest version of the L2TP data message header 1—indicates an L2F packet as described in RFC 2341 Packets with an unknown version number are discarded.
Length	The total length (in bytes) of the L2TP message (16 bits).

Field	Description
Tunnel-ID	Identifies the L2TP tunnel (that is, the control connection).This number has local significance — each end gives the same tunnel different tunnel IDs. The ID refers to the receiver, not the sender, and is assigned during tunnel creation (16 bits).
Session-ID	Identifies the PPP session within a tunnel. This number has local significance—each end gives the same session different session IDs. The ID refers to the receiver, not the sender, and is assigned during session creation (16 bits).
Ns	The sequence number of the message. This is mandatory for control messages (to enable re-transmission of lost messages) but optional for data messages (to re-order data messages that were mis-sequenced during forwarding). The number, which starts at 0 and increments by 1, is assigned by an L2TP peer for each session in a tunnel (16 bits).
Nr	The sequence number of the next control message expected to be received. This is equal to the sequence number of last received control message plus 1. Used by the receiving peer to ensure that control messages are sent in order without duplication. In data messages, the field (if present as indicated by the S bit) is ignored (16 bits).
Offset Size	The location of the L2TP payload, expressed as the number of octets from the start of the message header (16 bits).
Offset pad	User-defined bytes used to pad the message header so that the payload starts at the location indicated by the Offset Size field (16 bits).

The AVP header consists of following fields (RFC2611):



Field	Description
M	Mandatory bit — If the M bit is set on an unrecognized AVP within a message associated with a particular session, the session associated with this message MUST be terminated (1 bit).
H	Hidden bit — Identifies the hiding of data in the Attribute-Value field of an AVP. This capability can be used to avoid the passing of sensitive data, such as user passwords, as clear text in an AVP. The H-bit MUST only be set if a shared secret exists between the LAC and LNS. The shared secret is the same secret that is used for tunnel authentication. If the H-bit is set in any AVP(s) in a given control message, a Random Vector AVP must also be present in the message and MUST precede the first AVP having an H bit of 1 (1 bit).
-	Reserved for future use, must be set to zero (4 bits).
Length	Indicates the total number of bytes (including the overall length and bitmask fields) contained in this AVP (10 bits).
Vendor-id	Any vendor wishing to implement their own L2TP extensions can use their own Vendor ID along with private Attribute values. Vendor-ID=0 means that the standard AVP's are used (2 bytes).
Attribute Type	A value with a unique interpretation across all AVPs defined under a given Vendor (2 bytes).
Attribute Value	This is the actual value as indicated by the Vendor ID and Attribute Type (2 bytes).

RADIUS-Triggered Tunnel/Session Setup without LNS Renegotiation

Figure 377 depicts the complete PPP session setup, using RADIUS authentication on both LAC and LNS. After the discovery phase (PADI/PADO/PADR/PADS) and LCP negotiation phase (LCP config_request/Ack), the LAC initiates the L2TP tunnel setup based on Radius authentication information (Radius Request/Accept) and includes the negotiated PPP user-LAC information (called LCP proxy information). The LNS replies directly with a successful CHAP authentication if it agrees with the received proxy information. IP negotiation (IPCP config_request/Ack) is further handled between the user and the LNS and therefore the LAC has no IP knowledge of this PPP session.

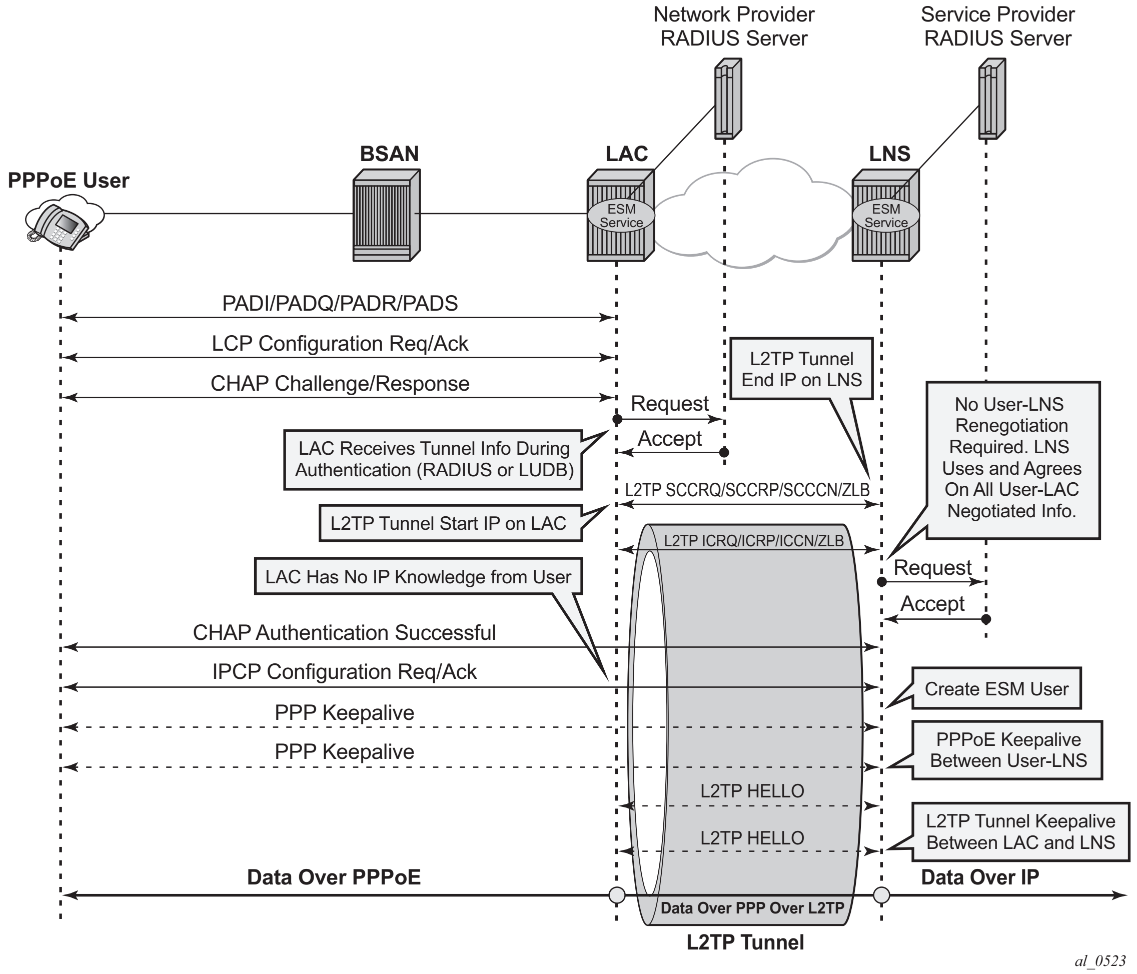

Network Provider RADIUS Server
Service Provider RADIUS Server
PPPoE User
BSAN
LAC
LNS
ESM Service
ESM Service
PADI/PADQ/PADR/PADS
LCP Configuration Req/Ack
CHAP Challenge/Response
Request
Accept
L2TP Tunnel End IP on LNS
No User-LNS Renegotiation Required. LNS Uses and Agrees On All User-LAC Negotiated Info.
LAC Receives Tunnel Info During Authentication (RADIUS or LUDB)
L2TP SCCRQ/SCCRP/SCCCN/ZLB
L2TP Tunnel Start IP on LAC
L2TP ICRQ/ICRP/ICCN/ZLB
LAC Has No IP Knowledge from User
Request
Accept
CHAP Authentication Successful
IPCP Configuration Req/Ack
Create ESM User
PPP Keepalive
PPPoE Keepalive Between User-LNS
PPP Keepalive
L2TP HELLO
L2TP Tunnel Keepalive Between LAC and LNS
L2TP HELLO
Data Over PPPoE
Data Over IP
Data Over PPP Over L2TP
L2TP Tunnel
al_0523

Figure 377: RADIUS Triggered Tunnel/Session Setup without LNS Renegotiation

RADIUS-Triggered Tunnel/Session Setup with LNS Renegotiation

Figure 378 shows the scenario were the LNS does not agree with the received LCP proxy information and (re)starts the LCP phase (LCP config_request/Ack) directly with the PPP user. The rest of this scenario is the same as shown in Figure 377.

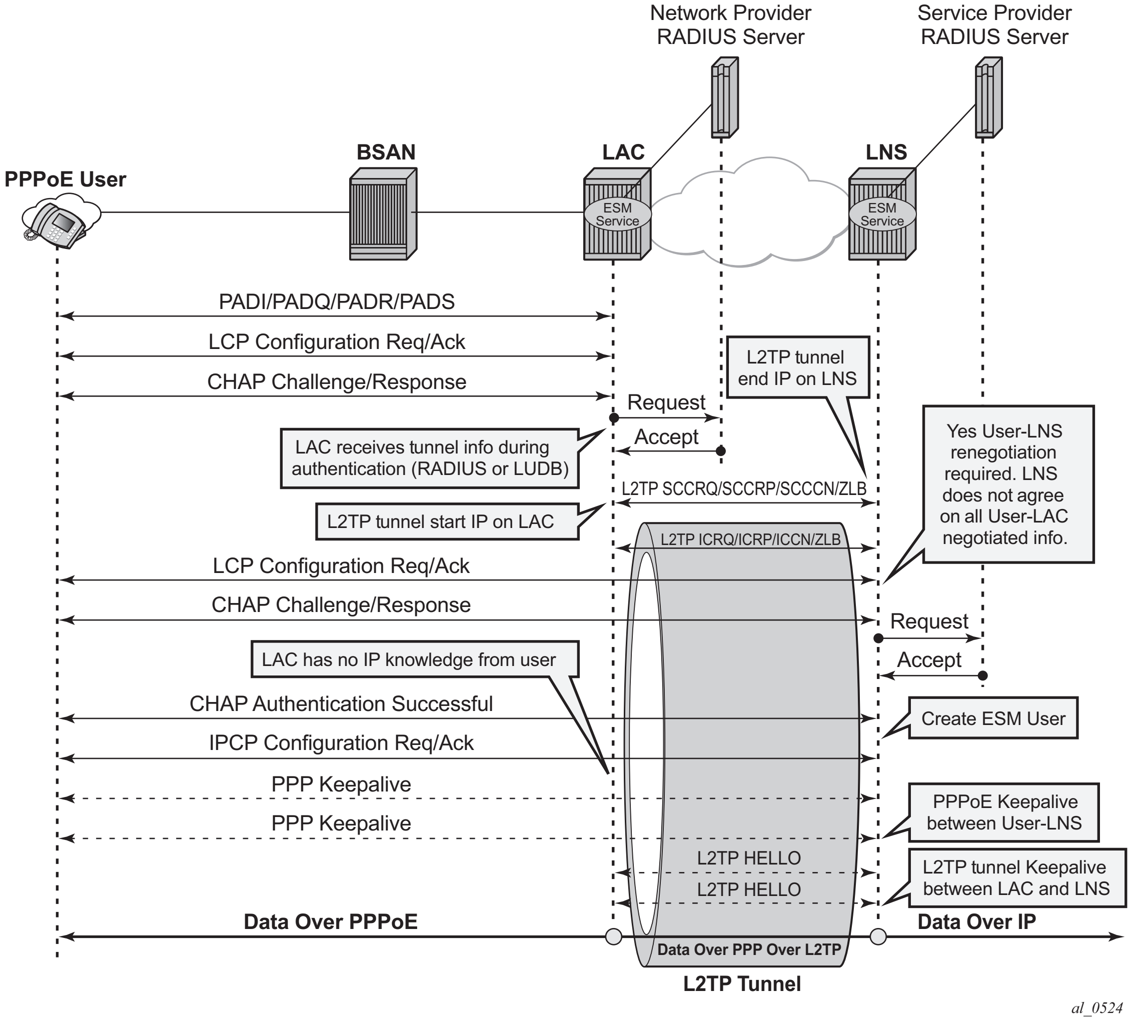

Network Provider RADIUS Server
Service Provider RADIUS Server
BSAN
LAC
LNS
PPPoE User
ESM Service
ESM Service
PADI/PADQ/PADR/PADS
LCP Configuration Req/Ack
CHAP Challenge/Response
L2TP tunnel end IP on LNS
Request
Accept
LAC receives tunnel info during authentication (RADIUS or LUDB)
L2TP SCCRQ/SCCRP/SCCCN/ZLB
L2TP tunnel start IP on LAC
L2TP ICRQ/ICRP/ICCN/ZLB
Yes User-LNS renegotiation required. LNS does not agree on all User-LAC negotiated info.
LCP Configuration Req/Ack
CHAP Challenge/Response
Request
Accept
LAC has no IP knowledge from user
CHAP Authentication Successful
Create ESM User
IPCP Configuration Req/Ack
PPP Keepalive
PPP Keepalive
PPPoE Keepalive between User-LNS
L2TP HELLO
L2TP HELLO
L2TP tunnel Keepalive between LAC and LNS
Data Over PPPoE
Data Over IP
Data Over PPP Over L2TP
L2TP Tunnel
al_0524

Figure 378: RADIUS Triggered Tunnel/Session Setup with LNS Renegotiation

Running Multiple PPP Sessions Over a Single L2TP Tunnel

Figure 379 shows multiple PPP sessions tunneled over a single L2TP Tunnel. The LAC encapsulates each PPP session with a different L2TP session-id (SID) but with the same L2TP Tunnel-id (TID).

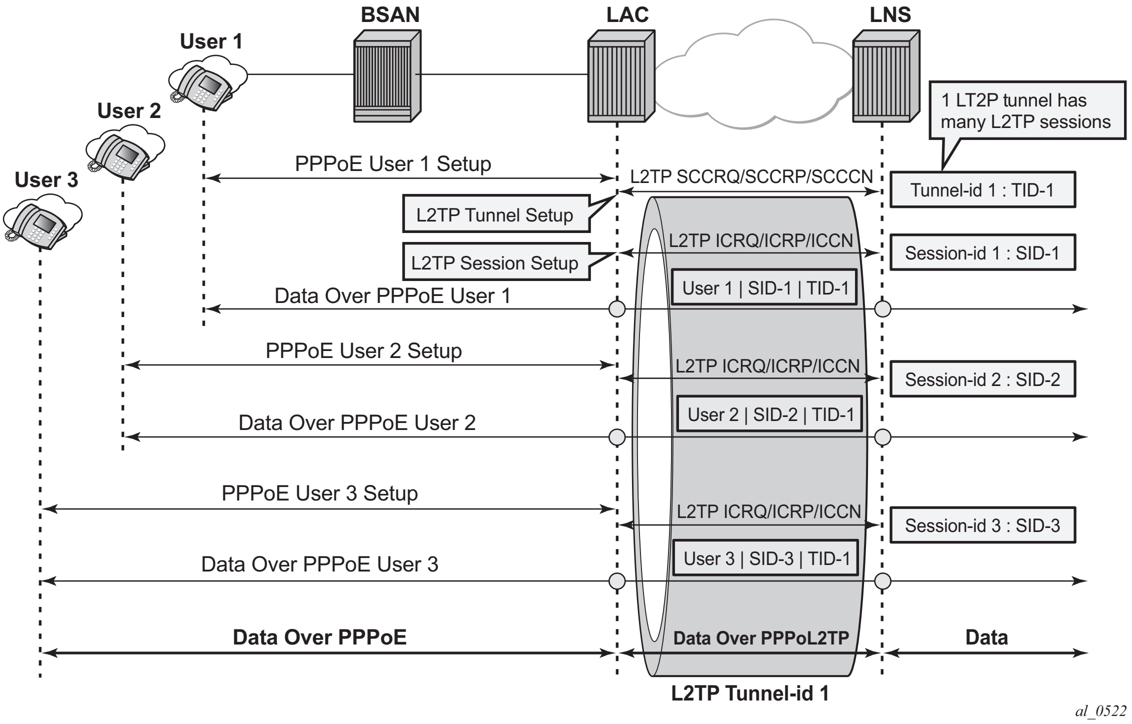


Figure 379: Running Multiple PPP Sessions Over a Single L2TP Tunnel

PPP User-Initiated Release/Terminate

Figure 380 shows the user initiated terminate_request tunneled by the LAC followed by the user initiated PADT terminated on the LAC. The LAC informs the LNS about the termination of the session via the L2TP CDN message. The L2TP tunnel can be optionally (idle-timeout) terminated via the L2TP StopCCN message.

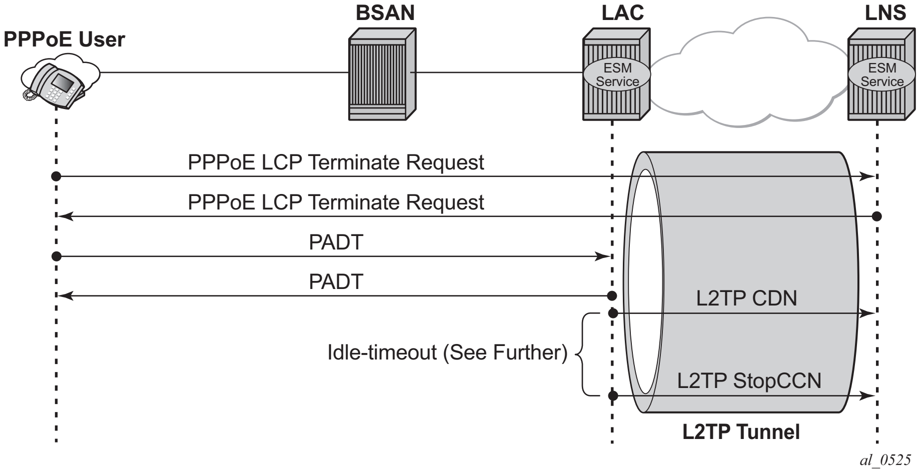


Figure 380: PPP User Initiated Release/Terminate

L2TP Tunnel/Session State Diagram

Figure 381 gives an overview of the main L2TP tunnel and session states. An L2TP tunnel in the establishedIdle state is a tunnel without sessions. A **tools** command (see Advanced Topics on page 2490) can put an L2TP tunnel in a draining state (this prevents adding new sessions on tunnel but the leaves the current sessions intact) or in a drained state (moved from draining to drained when all sessions terminated). The draining and drained state are not shown in the state diagram.

The L2TP tunnel setup occurs first with the triggers being: session activation, auto-establish and a **tools start** command (see the advanced section). An L2TP session setup trigger is always session based.

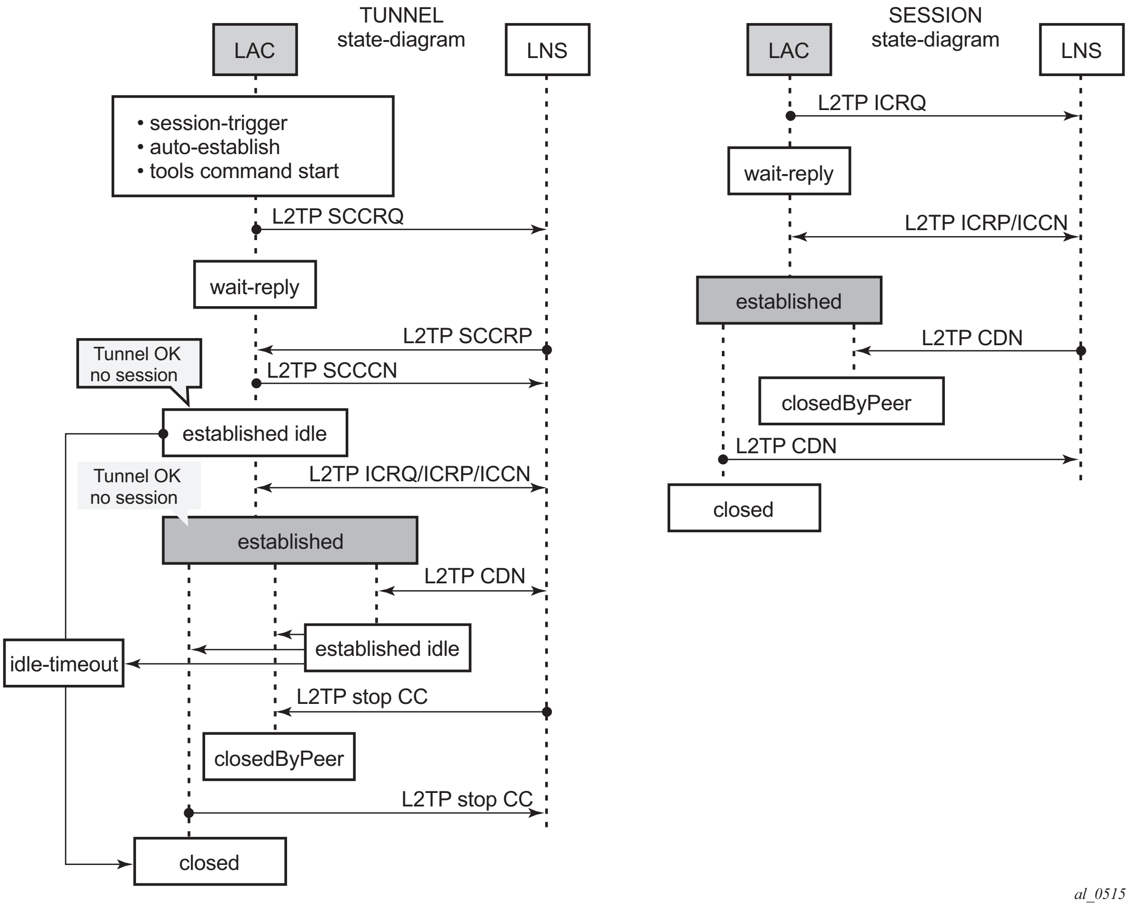


Figure 381: L2TP Tunnel and Session State Diagram

Configuration

Scenario 1: RADIUS-Derived L2TP Parameters

ç LAC in the Base Routing Context (base) with Single Endpoint/Single Tunnel on page 2465

ç LAC in the Base Routing Context with Multiple Endpoints on page 2467

ç LAC in a VRF on page 2469

In this example the LAC receives an incoming connection and contacts the LAC RADIUS server. The RADIUS server retrieves the attributes for the user's domain (for example @wholesale.com) and passes the tunnel attributes to the LAC. Based on these RADIUS provided tunnel attributes, the LAC selects or initiates a new tunnel to the LTS or directly to the LNS. Once the tunnel is established, the LNS authenticates the end user using its own RADIUS server. Configuring the LNS and the LTS are out of the scope of this example.

In a RADIUS driven L2TP setup either all or some of the required L2TP attributes are returned via RADIUS. If the RADIUS server returns only the L2TP [67] Tunnel-Server-Endpoint attributes then the L2TP tunnel/session is established using the ‘node parameter values’ for the other required L2TP parameters. The ‘l2tp node parameters’ are defined under the configure router/service l2tp hierarchy. If the RADIUS server does not return all of the L2TP attributes and the node values are not configured, then the system falls back to default settings for these L2TP parameters.

The standard and vendor specific [26-6572] L2TP RADIUS attributes are listed in the tables below, together with the corresponding l2tp node parameters and defaults.

Attribute ID	Attribute Name	Mandatory	CLI Node Parameter	Corresponding Defaults	
64	Tunnel-Type	Y	-	-	-
65	Tunnel-Medium-Type	Y	-	-	-
66	Tunnel-Client-Endpoint:[0-31]	N	local-address	no local-address	system-ip
67	Tunnel-Server-Endpoint	N	-	-	-
69	Tunnel-Password	N	password	no password	-
82	Tunnel-Assignment-ID:0	N	-	-	default_radius_group

Attribute ID	Attribute Name	Mandatory	CLI Node Parameter	Corresponding Defaults	
82	Tunnel-Assignment-ID:[1..31]	N	-	-	Unnamed
83	Tunnel-Preference	N	preference	no preference	50
90	Tunnel-Client-Auth-ID	N	local-name	no local-name	system-name
91	Tunnel-Server-Auth-ID	N	-	-	-

26-6527	Attribute Name	Mandatory	CLI Node Parameter	Corresponding Defaults	
-46	Alc-Tunnel-Group	N	-	-	-
-47	Alc-Tunnel-Algorithm	N	session-assign-method	no session-assign-method	existingFirst
-48	Alc-Tunnel-Max-Sessions:0	N	-	group-session-limit	131071
-48	Alc-Tunnel-Max-Sessions:[1..31]	N	-	tunnel-session-limit	32767
-49	Alc-Tunnel-Idle-Timeout	N	idle-timeout	no idle-timeout	Infinite
-50	Alc-Tunnel-Hello-Interval	N	hello-interval	no hello-interval	300 sec
-51	Alc-Tunnel-Destruct-Timeout	N	destruct-timeout	no destruct-timeout	60 sec
-52	Alc-Tunnel-Max-Retries-Estab	N	max-retries-estab	no max-retries-estab	5
-53	Alc-Tunnel-Max-Retries-Not-Estab	N	max-retries-not-estab	no max-retries-not-estab	5
-54	Alc-Tunnel-AVP-Hiding	N	avp-hiding	no avp-hiding	Never
-97	Alc-Tunnel-Challenge	N	challenge	no challenge	Never
-104	Alc-Tunnel-Serv-Id	N	-	-	Base
-120	Alc-Tunnel-Rx-Window-Size	N	receive-window-size	no receive-window-size	64

26-6527	Attribute Name	Mandatory	CLI Node Parameter	Corresponding Defaults	
-144	Alc-Tunnel-Acct-Policy	N	radius-accounting-policy	no radius-accounting-policy	-

LAC in the Base Routing Context (base) with Single Endpoint/Single Tunnel

Using the mandatory L2TP RADIUS attributes (see the RADIUS user file below) the LAC establishes an L2TP tunnel. The tunnel endpoint IP addresses used are the Base router system interface IPv4 address (LAC tunnel endpoint) and the address indicated by the Tunnel-Server-Endpoint RADIUS attribute [67], which serves as the peer tunnel LNS endpoint address.

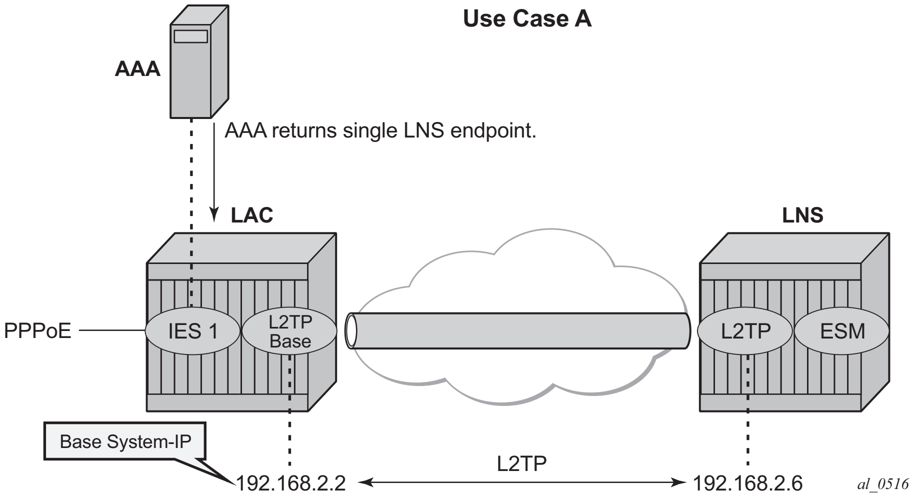


Figure 382: LAC in Base Routing with Single Endpoint/Single Tunnel

The PPPoE user terminates on IES service 1, sap 1/1/2:100.1, and is authenticated via RADIUS **authentication-policy** *authentication-1* which provides wholesale/retail (L2TP) information.

```
configure service ies 1
      subscriber-interface "sub-lt2p"
          unnumbered "system"
          group-interface "grp-l2tp"
              authentication-policy "authentication-1"  #Radius authentication
              sap 1/1/2:100.1
                  sub-sla-mgmt
                      sub-ident-policy "sub-ident-1"
                      no shutdown
                  exit
              exit
              pppoe
                  no shutdown
              exit
          exit
      exit
      service-name "L2TP"
      no shutdown
```

The excerpt from the FreeRADIUS users file below shows the attributes to be returned.

```
user1@wholesale.com  Cleartext-Password := "ALU" ,NAS-Identifier == "pe1"
      Alc-Subsc-ID-Str = "%{User-name}",
      Alc-Subsc-Prof-Str = "sub-func1",
      Alc-SLA-Prof-Str = "sla-func1",
# Tunnel 1 related (tag 1)                              #Tunnel 1
       Tunnel-Type:1 += L2TP,                           #
       Tunnel-Medium-Type:1 += IP,                      #
       Tunnel-Server-Endpoint:1 += 192.168.2.6,         #LNS peer address
```

L2TP is enabled (no shutdown) in the related service instance.

- The L2TP tunnel is setup in the base instance and not in a VRF because the attribute Alc-Tunnel-Serv-Id is not returned from RADIUS.
- Missing L2TP parameters are taken from defaults from router l2tp.

```
configure router l2tp
       calling-number-format "%S %s"  # L2TP AVP 22 format
                                      # Default format ‘system-name sap-id’
       <snip>
       no local-name                  # default name equals system-name
       no max-retries-estab           # default value equals 5
       <snip>
       no shutdown                    # enable L2TP
```

This scenario shows the PPPoE session termination (base IES service 1) and the L2TP tunnel setup in the same base router instance.

LAC in the Base Routing Context with Multiple Endpoints

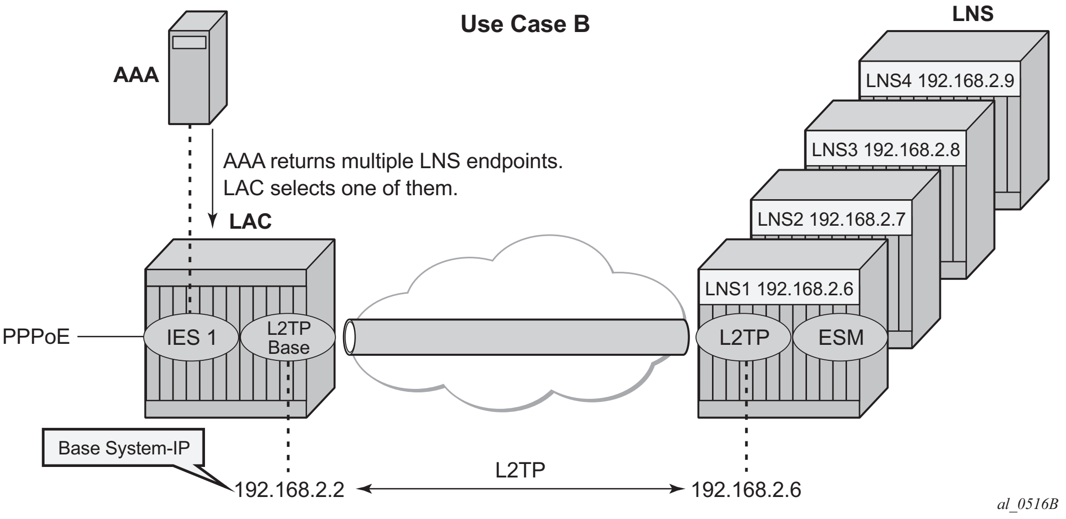


Figure 383: LAC in the Base Routing with Multiple Endpoints

The excerpt from the FreeRADIUS users file below shows that user1@wholesale.com has 4 possible endpoints (LNS), each with its own tunnel preference. The LAC selects one L2TP endpoint out of these 4 tunnel specifications according the configured L2TP selection process. This example uses weighted load balancing between LNS-T1 and LNS-T2 (tunnels LNS1-T1 and LNS2-T2 have best (lowest) and equal preference).

Note: The L2TP tunnel selection process is out of the scope of this example.

```
user1@wholesale.com  Cleartext-Password := "ALU" ,NAS-Identifier == "pe1"
       Alc-Subsc-ID-Str = "%{User-name}",
       Alc-Subsc-Prof-Str = "sub-func1",
       Alc-SLA-Prof-Str = "sla-func1",
# group related (tag 0)parameters applicable for all tunnels
       Tunnel-Client-Endpoint:0 = 192.168.2.2,            #LAC L2TP source IP
       Alc-Tunnel-Algorithm:0 = weighted-access,          #tunnel selection
       Tunnel-Assignment-Id:0 = "l2tp-functional-radius", #L2TP group name
       Tunnel-Client-Auth-Id:0 = "lac-pe1",               #LAC name
       Alc-Tunnel-Max-Retries-Estab:0 = 2,
       #
# Tunnel 1 related (tag 1)                               #Tunnel 1
       Tunnel-Type:1 += L2TP,                            #
       Tunnel-Medium-Type:1 += IP,                       #
       Tunnel-Server-Endpoint:1 += 192.168.2.6,          # LNS peer address
       Tunnel-Assignment-Id:1 += "LNS1-T1",              # tunnel name
       Tunnel-Preference:1 += 100,                       # preference 100
       #
# Tunnel 2 related (tag 2)                               #Tunnel 2
       Tunnel-Type:2 += L2TP,
       Tunnel-Medium-Type:2 += IP,
       Tunnel-Server-Endpoint:2 += 192.168.2.7,
       Tunnel-Assignment-Id:2 += "LNS2-T2",
       Tunnel-Preference:2 += 100,
       #
# Tunnel 3 related (tag 3)                                #Tunnel 3
       Tunnel-Type:3 += L2TP,
       Tunnel-Medium-Type:3 += IP,
       Tunnel-Server-Endpoint:3 += 192.168.2.8,
       Tunnel-Assignment-Id:3 += "LNS3-T3",
       Tunnel-Preference:3 += 120,
       #
# Tunnel 4 related (tag 4)                                #Tunnel 4
       Tunnel-Type:4 += L2TP,
       Tunnel-Medium-Type:4 += IP,
       Tunnel-Server-Endpoint:4 += 192.168.2.9,
       Tunnel-Assignment-Id:4 += "LNS4-T4",
       Tunnel-Preference:4 += 140,
```

This scenario also shows the PPPoE session termination (base IES service 1) and the L2TP tunnel setup in the same base router instance.

LAC in a VRF

Figure 384 shows the PPPoE session termination (base IES service 1) and the L2TP tunnel setup in a different router instance (VPRN 65536).

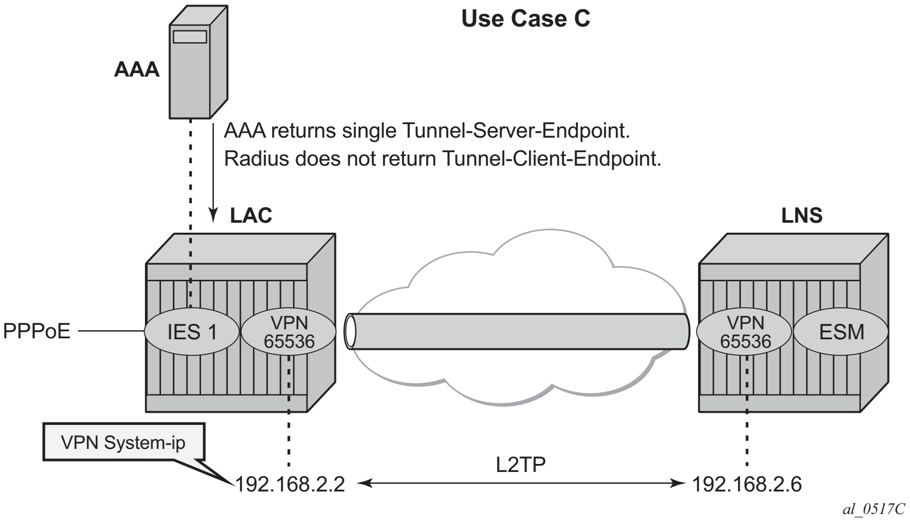


Figure 384: LAC in a VRF

Using the L2TP RADIUS attributes indicated below, the LAC initiates an L2TP tunnel in VPRN 65536. The PPPoE session is still terminated in base IES service 1, which proves that both router instances can be different. (See use-case A for configuration details IES service 1).

```
user1@wholesale.com  Cleartext-Password := "ALU" ,NAS-Identifier == "pe1"
      Alc-Subsc-ID-Str = "%{User-name}",
      Alc-Subsc-Prof-Str = "sub-func1",
      Alc-SLA-Prof-Str = "sla-func1",
      Alc-Tunnel-Serv-Id = 65536,                    #L2TP starts in VRF 65536
      Tunnel-Assignment-Id:0 = "l2tp-functional-radius",
      Tunnel-Client-Auth-Id:0 = "lac-pe1",
      Tunnel-Type:1 += L2TP,
      Tunnel-Medium-Type:1 += IP,
      Tunnel-Server-Endpoint:1 += 192.168.2.6,
      Tunnel-Assignment-Id:1 += "LNS1-T1",
```

If RADIUS does not return the L2TP source IP address (Tunnel-Client-Endpoint) then the IP address from the VPRN 65536 interface named ‘system’ is taken as the L2TP source address. The tunnel-setup fails if this system interface is not created.

```
configure service vprn 65536
  <snip>
  interface "system"                          #source IP for tunnel
      address 192.168.2.2/32
```

```
        loopback
    exit
    l2tp
        no shutdown
    exit
```

Scenario 2: Node-Derived L2TP Parameters

ç RADIUS Returns L2TP Group on page 2470

ç RADIUS-Less Setup (LUDB Returns L2TP Group) on page 2472

In this example, the LAC receives the incoming connection and an ‘L2TP tunnel-group-name’ is assigned during LUDB or RADIUS authentication. This tunnel-group-name refers to the CLI preconfigured tunnel-group name context (**configure router** <*router-name*> **l2tp group** <*tunnel-group-name*>), which provides the context for all relevant tunnel attributes.

Based on these attributes, the LAC selects and initiates a tunnel to the LTS or directly to the LNS as in Scenario 2: Node-Derived L2TP Parameters on page 2470.

RADIUS Returns L2TP Group

In this example, the L2TP tunnel-group-name is assigned during RADIUS authentication.

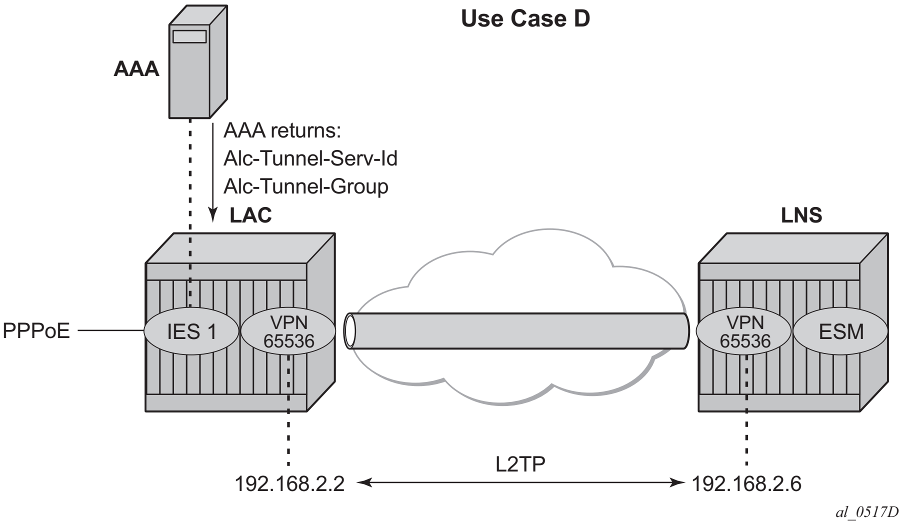


Figure 385: RADIUS Returns L2TP Group

```
user1@wholesale.com  Cleartext-Password := "ALU" ,NAS-Identifier == "pe1"
      Alc-Subsc-ID-Str = "%{User-name}",
      Alc-Subsc-Prof-Str = "sub-func1",
      Alc-SLA-Prof-Str = "sla-func1",
      Alc-Tunnel-Serv-Id = 65536,             #LAC in VRF
      Alc-Tunnel-Group = wholesale.com,       #points to L2TP node group name
```

The L2TP tunnel is setup in VPRN 65536 (Alc-Tunnel-Serv-Id) and all L2TP tunnel information is taken from the l2tp group wholesale.com hierarchy (Alc-Tunnel-Group) as defined on the node.

```
configure service vprn 65536
   <snip>
   interface "system"                #interface with name system is
       address 192.168.2.2/32        #used as LAC L2TP source ip-address
       loopback
   exit
   l2tp
       group "wholesale.com"         #corresponds with Alc-Tunnel-Group
          tunnel "wholesale.com"
              local-address 192.168.2.2  #optional since system itf exists
              local-name "lac-pe1"
              peer 192.168.2.6
              no auto-establish      #use session-trigger iso auto-establish
              no shutdown
          exit
          no shutdown
      exit
      no shutdown
   exit
```

An L2TP tunnel is set up by either a PPP session-trigger, a **tools** command or by the l2tp group tunnel auto-establish parameter configuration. See the advanced section below for the non-session-triggered tunnel setup.

RADIUS-Less Setup (LUDB Returns L2TP Group)

In this example, the L2TP tunnel-group-name is assigned during LUDB authentication.

The PPPoE user enters on an IES service 1, sap 1/1/2:100.1, and is authenticated via the LUDB which provides L2TP wholesale/retail and ESM information. No RADIUS authentication is required in this example, as the PPPoE context refers to a local-user database **l2tp** to provide the subscriber authentication and the tunnel set-up parameters.

```
configure service ies 1
      subscriber-interface "sub-lt2p"
          unnumbered "system"
          group-interface "grp-l2tp"
              sap 1/1/2:100.1
                  sub-sla-mgmt
                      sub-ident-policy "sub-ident-1"
                      no shutdown
                  exit
              exit
              pppoe
                  no shutdown
                  user-db "l2tp"
              exit
          exit
      exit
      service-name "L2TP"
      no shutdown
```

The referenced local user database **l2tp** configuration provides all of the required L2TP and ESM information.

```
configure subscriber-mgmt local-user-db "l2tp"
    ppp
       match-list username
       host "wholesale.com" create
         host-identification
              username "wholesale.com" domain-only
         exit
         password ignore
                    identification-strings 254 create
                        subscriber-id "user1@wholesale.com"
                        sla-profile-string "sla-func1"
                        sub-profile-string "sub-func1"
                    exit
         l2tp
              group "wholesale.com" service-id 65536         #points to L2TP group
         exit                                                #name and LAC in VRF
         no shutdown
        exit
    exit
```

Operation and Troubleshooting

This chapter explains how the use cases A to E described in the configuration section are verified using show, debug and tools commands.

The standard router debugging tools can be used to monitor and troubleshoot the L2TP tunnel and session setup.

Overview of Debug and Show Commands

```
# useful show commands
show service id <service-id> ppp session [detail]
show router l2tp tunnel [detail]
show router l2tp session [detail]
show router l2tp peer [ip-address]

# debug to show PPPoE packet interaction
debug service id <service-id> ppp packet mode egr-ingr-and-dropped
debug service id <service-id> ppp packet detail-level medium

# debug to show RADIUS authentication interaction
debug router radius packet-type authentication

#debug to show LUDB authentication interaction
debug subscriber-mgmt local-user-db <local-user-db-name> detail all

# debug to show LAC Tunnel selection process and L2TP state-machine
debug router l2tp event lac-session-setup
debug router l2tp event finite-state-machine

# debug to show L2TP Tunnel and session setup
debug router l2tp packet direction both
debug router l2tp packet detail-level high
```

Understanding the Debug l2tp Command Output

The L2TP ICRQ message extract shown below (**debug router l2tp packet**) is used to explain how the displayed debug output should be interpreted. See Recap of the L2TPv2 Protocol on page 2453 -L2TP Header and AVP Layout on page 2454 for more details.

```
<date> <time> CEST MINOR: DEBUG #2001 Base L2TP(v2, ctrl, egress)
"L2TP(v2, ctrl, egress): UDP 192.0.2.2:1701 -> 192.168.2.6:1701
tunnel 1240 session 0, ns 2 nr 1, flags:, reserved=0
    AVP MessageType(0,0), flags: mandatory, reserved=0
        IncomingCallRequest(10)
<snip>
    AVP CallingNumber(0,22), flags: mandatory, reserved=0
        "pe1 1/1/2:100.1"
    AVP AgentCircuitId(3561,1), flags:, reserved=0
        "circuit0"
<snip>
```

- L2TP(v2, ctrl, egress): UDP 192.0.2.2:1701 -> 192.168.2.6:1701
  - ç version: v2
  - ç type field (T-bit): control message (ctrl)
  - ç 192.0.2.2:1701 -> 192.168.2.6:1701
    - 192.0.2.2:1701 - source tunnel-end-point:source udp port
    - 192.168.2.6:1701 - destination tunnel-end-point:destination udp port
- tunnel 1240 session 0, ns 2 nr 1, flags:, reserved=0
  - ç tunnel-id:1240
  - ç session-id:0
  - ç ns:2
  - ç nr:1
  - ç flags: 0 (refers to T/L/S/O/P bits L2TP header)
  - ç reserved field:0
- AVP CallingNumber(0,22), flags: mandatory, reserved=0
  - ç AVP MessageType(0,22): "pe1 1/1/2:100.1"
    - Vendor-id: 0 - Standard Attribute
    - Attribute Type: 22 – Calling Number AVP
    - Attribute Value: "pe1 1/1/2:100.1

Scenario 1: RADIUS-Derived L2TP Parameters

- LAC in Base Routing Context (base) with Single Endpoint/Single Tunnel on page 2475

LAC in Base Routing Context (base) with Single Endpoint/Single Tunnel

The '**debug service id <service-id> ppp packet mode egr-ingr-and-dropped** command shows PPPoE packet interaction. Below is a snapshot from the PADI packet showing the service, SAP and received PPPoE Tags. The received PPPoE DSL forum tags are by default copied during the LAC L2TP tunnel setup into the Incoming Call Request (ICRQ) DSL Forum AVP's (RFC 5515).

```
<date> <time> CEST MINOR: DEBUG #2001 Base PPPoE
"PPPoE: RX Packet
   IES 1, SAP 1/1/2:100.1

   DMAC: ff:ff:ff:ff:ff:ff
   SMAC: 00:00:00:01:01:01
   Ether Type: 0x8863 (Discovery)

   PPPoE Header:
   Version: 1                 Type      : 1
   Code   : 0x09 (PADI)       Session-Id: 0x0000 (0)
   Length : 58

   PPPoE Tags:
   [0x0101] Service-Name: "AGILENT"
   [0x0103] Host-Uniq: len = 4, value = 00 0f 00 00
   [0x0105] Vendor-Specific: vendor-id = 0x0de9 (ADSL Forum)
      [0x01] Agent-Circuit-Id: "circuit0" #copied in ICRQ DSL forum AVP's
      [0x02] Agent-Remote-Id: "remote0"   #copied in ICRQ DSL forum AVP's
      [0x81] Actual-Upstream: 2000        #copied in ICRQ DSL forum AVP's
      [0x82] Actual-Downstream: 4000"     #copied in ICRQ DSL forum AVP's
```

The **debug router radius packet-type authentication** command shows the actual authentication parameters returned by RADIUS. This example returns the minimum set of L2TP related RADIUS attributes.

```
<date> <time> CEST MINOR: DEBUG #2001 Base RADIUS
"RADIUS: Receive
  Access-Accept(2) id 165 len 103 from 172.16.1.1:1812 vrid 1 pol subscr-mgmt
    VSA [26] 21 Alcatel(6527)
      SUBSC ID STR [11] 19 user1@wholesale.com
    VSA [26] 11 Alcatel(6527)
      SUBSC PROF STR [12] 9 sub-func1
    VSA [26] 11 Alcatel(6527)
      SLA PROF STR [13] 9 sla-func1
    TUNNEL TYPE [64] 4 1 L2TP(3)               # L2TP
    TUNNEL MEDIUM TYPE [65] 4 1 IPv4(1)        # IPv4
    TUNNEL SERVER ENDPOINT [67] 8 1 192.168.2.6    # L2TP peer LNS address
"
```

The **debug router l2tp event lac-session-setup** command shows the LAC tunnel selection for this example. An L2TP group-name ‘default_radius_group’ with tunnel-name ‘unnamed’ is created in this case.

```
<date> <time> CEST MINOR: DEBUG #2001 Base PPPoE 29->L2TP
"PPPoE 29->L2TP: UDP 0.0.0.0:1701 -> 192.168.2.6:1701
pref 50 tunnel default_radius_group:unnamed  #group-name=default_radius_group
    request to open new tunnel 3288"         #tunnel-name=unnamed

<date> <time> CEST MINOR: DEBUG #2001 Base PPPoE 29->L2TP
"PPPoE 29->L2TP: UDP 0.0.0.0:1701 -> 192.168.2.6:1701
pref 50 tunnel default_radius_group:unnamed
    create session 215482368"
```

The ‘**debug router l2tp packet detail-level**’ command shows the L2TP tunnel and session setup for this example.

Tunnel setup: The LAC sends a Start-Control-Connection-Request (SCCRQ) containing the assigned tunnel-id (no tunnel authentication in the example). The tunnel is now in a wait-reply state.

```
<date> <time> CEST MINOR: DEBUG #2001 Base L2TP(v2, ctrl, egress)
"L2TP(v2, ctrl, egress): UDP 192.0.2.2:1701 -> 192.168.2.6:1701
tunnel 0 session 0, ns 0 nr 0, flags:, reserved=0
    AVP MessageType(0,0), flags: mandatory, reserved=0
        StartControlConnectionRequest(1)                #SCCRQ
    AVP ProtocolVersion(0,2), flags: mandatory, reserved=0
        version=1, revision=0
    AVP HostName(0,7), flags: mandatory, reserved=0     #default=system-name
        "pe1"
    AVP WindowSize(0,10), flags: mandatory, reserved=0
        64                                              #default=64
    AVP FramingCapabilities(0,3), flags: mandatory, reserved=0
        sync=no, async=no
    AVP BearerCapabilities(0,4), flags: mandatory, reserved=0
        digital=yes, analogue=no
    AVP FirmwareRevision(0,6), flags:, reserved=0
        2816
    AVP VendorName(0,8), flags:, reserved=0
        "Alcatel-Lucent"
    AVP AssignedTunnelId(0,9), flags: mandatory, reserved=0 #LAC Tunnel-id
        3288"
```

Tunnel setup: The LNS can bring up the tunnel, so the LNS replies with a Start-Control-Connection-Reply (SCCRP) including the assigned tunnel-id.

```
<date> <time> CEST MINOR: DEBUG #2001 Base L2TP(v2, ctrl, ingress)
"L2TP(v2,ctrl,ingress): UDP 192.168.2.6:1701 -> 192.0.2.2:1701 #LNS TO LAC
tunnel 3288 session 0, ns 0 nr 1, flags:, reserved=0
    AVP MessageType(0,0), flags: mandatory, reserved=0
        StartControlConnectionReply(2)                         #SCCRP
    AVP ProtocolVersion(0,2), flags: mandatory, reserved=0
        version=1, revision=0
    AVP HostName(0,7), flags: mandatory, reserved=0
```

```
        "pe3"
    AVP WindowSize(0,10), flags: mandatory, reserved=0
        64
    AVP FramingCapabilities(0,3), flags: mandatory, reserved=0
        sync=no, async=no
    AVP BearerCapabilities(0,4), flags: mandatory, reserved=0
        digital=yes, analogue=no
    AVP FirmwareRevision(0,6), flags:, reserved=0
        2816
    AVP VendorName(0,8), flags:, reserved=0
        "Alcatel-Lucent"
    AVP AssignedTunnelId(0,9), flags: mandatory, reserved=0 #LNS Tunnel-id
        1240"
```

Tunnel setup: The LAC responds with a Start-Control-Connection-Connected (SCCCN) message. After an LNS ZLB acknowledgment, the tunnel is in the establishedIdle state.

```
<date> <time> CEST MINOR: DEBUG #2001 Base L2TP(v2, ctrl, egress)
"L2TP(v2, ctrl, egress): UDP 192.0.2.2:1701 -> 192.168.2.6:1701 #LAC TO LNS
tunnel 1240 session 0, ns 1 nr 1, flags:, reserved=0
    AVP MessageType(0,0), flags: mandatory, reserved=0
        StartControlConnectionConnected(3)"                 #SCCN
```

Session setup: Now the tunnel exists, a three-way exchange for session establishment within the tunnel is performed. The LAC sends an Incoming-Call-Request (ICRQ) with the parameter information for the session. The session is now in the wait-reply state.

```
<date> <time> CEST MINOR: DEBUG #2001 Base L2TP(v2, ctrl, egress)
"L2TP(v2, ctrl, egress): UDP 192.0.2.2:1701 -> 192.168.2.6:1701 #LAC TO LNS
tunnel 1240 session 0, ns 2 nr 1, flags:, reserved=0
    AVP MessageType(0,0), flags: mandatory, reserved=0
        IncomingCallRequest(10)                             #ICRQ
    AVP AssignedSessionId(0,14), flags: mandatory, reserved=0
        256
    AVP CallSerialNumber(0,15), flags: mandatory, reserved=0
        31
    AVP CallingNumber(0,22), flags: mandatory, reserved=0
        "pe1 1/1/2:100.1"                     #calling-number-format '%S %s'
    AVP AgentCircuitId(3561,1), flags:, reserved=0
        "circuit0"                            #copy from PADI by default
    AVP AgentRemoteId(3561,2), flags:, reserved=0
        "remote0"                             #copy from PADI by default
    AVP ActDataRateUp(3561,129), flags:, reserved=0
        2000000                               #copy from PADI by default
    AVP ActDataRateDown(3561,130), flags:, reserved=0
        4000000"                              #copy from PADI by default
```

Session setup: The LNS sends an Incoming-Call-Reply (ICRP) that contains the assigned session-id. The session is now in the connect state.

```
<date> <time> CEST MINOR: DEBUG #2001 Base L2TP(v2, ctrl, ingress)
"L2TP(v2,ctrl,ingress): UDP 192.168.2.6:1701 -> 192.0.2.2:1701 #LNS TO LAC
tunnel 3288 session 256, ns 1 nr 3, flags:, reserved=0
```

```
    AVP MessageType(0,0), flags: mandatory, reserved=0
        IncomingCallReply(11)                              #ICRP
    AVP AssignedSessionId(0,14), flags: mandatory, reserved=0
        31234"
```

Session setup: The LAC sends an Incoming Call Connected (ICCN) and provides the LNS with additional information from the user initiated session. This information includes the LCP information from the negotiation that the LAC and remote user performed. This information is used by the LNS to decide whether to start LCP re-negotiation and/or Authentication re-negotiation with the PPP user or not. After an LNS ZLB acknowledgment the session is in the established state.

```
<date> <time> CEST MINOR: DEBUG #2001 Base L2TP(v2, ctrl, egress)
"L2TP(v2, ctrl, egress): UDP 192.0.2.2:1701 -> 192.168.2.6:1701 #LAC TO LNS
tunnel 1240 session 31234, ns 3 nr 2, flags:, reserved=0
    AVP MessageType(0,0), flags: mandatory, reserved=0
        IncomingCallConnected(12)                        #ICCN
    AVP FramingType(0,19), flags: mandatory, reserved=0
        sync=no, async=no
    AVP TxConnectSpeed(0,24), flags: mandatory, reserved=0
        4000000        #report-rate: More on this in the Advanced section
    AVP InitialRxLcpConfReq(0,26), flags:, reserved=0 #copy from the PPP users
         05 06 19 cc 71 18 01 04 ff fb                #first LCP-conf-request
         [5] Magic-Number: 0x19cc7118
         [1] MRU: 1500
    AVP LastTxLcpConfReq(0,27), flags:, reserved=0
         01 04 05 d4 03 05 c2 23 05 05 06 0f 4d f8 18
         [1] MRU: 1492
         [3] Authentication-Protocol: 0xc223 (CHAP), Algorithm = 5 (MD5)
         [5] Magic-Number: 0x0f4df818
    AVP LastRxLcpConfReq(0,28), flags:, reserved=0    #copy from the PPP users
         05 06 19 cc 71 18 01 04 ff fb                #last LCP-conf-request
         [5] Magic-Number: 0x19cc7118
         [1] MRU: 1500
    AVP ProxyAuthenType(0,29), flags:, reserved=0     #user-LAC negotiated
        chap(2)                                       #authentication type
    AVP ProxyAuthenName(0,30), flags:, reserved=0
         "user1@wholesale.com"
    AVP ProxyAuthenChallenge(0,31), flags:, reserved=0
         92 59 c2 53 04 72 06 8f a8 87 cc c6 7d 09 8e d0
         95 43 16 33 70 7e 65 86 d3 c4 16 94 1e 54 e5 30
         2e 28 04 b1 9b 0a c1 c3 12 8e 8b 8f 18 99 e0 ad
         5d
    AVP ProxyAuthenId(0,32), flags:, reserved=0
        id=1, reserved=0
    AVP ProxyAuthenResponse(0,33), flags:, reserved=0
         50 cb bd 10 3c 7c ec 47 0b 04 0d 7d 49 c2 7f bd
    AVP RxConnectSpeed(0,38), flags:, reserved=0
        2000000"                                    #report-rate. More on this
                                                    #in the Advanced section
```

The PPPoE session operational information for IES 1/base instance is shown below.

```
show service id 1 ppp session
==============================================================================
PPP sessions for service 1
==============================================================================
User-Name
  Descr.
           Up Time       Type  Termination     IP/L2TP-Id/Interface-Id
------------------------------------------------------------------------------
user1@wholesale.com
  svc:1 sap:1/1/2:100.1 mac:00:00:00:01:01:01 sid:1
           0d 00:00:14    oE   lac             215482624  #L2TP session-id
------------------------------------------------------------------------------
No. of PPP sessions: 1
```

The tunnel operational information in base instance shows that the tunnel is established.

```
show router l2tp tunnel
==============================================================================
Conn ID    Loc-Tu-ID Rem-Tu-ID State              Blacklist-state   Ses Active
  Group                                                             Ses Total
    Assignment
------------------------------------------------------------------------------
215482368  3288      1240      established        not-blacklisted   1
  default_radius_group                                              1
    unnamed
------------------------------------------------------------------------------
No. of tunnels: 1
```

Detailed tunnel operational information is obtained using following command.

```
show router l2tp tunnel detail
==============================================================================
L2TP Tunnel Status
==============================================================================

Connection ID: 215482368
State        : established
IP           : 192.0.2.2
UDP          : 1701
Peer IP      : 192.168.2.6
Peer UDP     : 1701
Tx dst-IP    : 192.168.2.6
Tx dst-UDP   : 1701
Rx src-IP    : 192.168.2.6
Rx src-UDP   : 1701
Name         : pe1
Remote Name  : pe3
Assignment ID: unnamed
Group Name   : default_radius_group
Acct. Policy : N/A
Error Message: N/A

                                        Remote Conn ID    : 81264640
Tunnel ID         : 3288              Remote Tunnel ID  : 1240
```

```
Preference        : 50                Receive Window    : 64
Hello Interval (s): 300
Idle TO (s)       : infinite          Destruct TO (s)   : 60
Max Retr Estab    : 5                 Max Retr Not Estab: 5
Session Limit     : 32767             AVP Hiding        : never
Transport Type    : udpIp             Challenge         : never
Time Started      : 10/04/2013 15:37:10 Time Idle         : N/A
Time Established  : 10/04/2013 15:37:10 Time Closed       : N/A
Stop CCN Result   : noError           General Error     : noError
Blacklist-state   : not-blacklisted
```

The session operational information shows the session is established.

```
show router l2tp session
==============================================================================
L2TP Session Summary
==============================================================================
ID                  Control Conn ID     Tunnel-ID   Session-ID  State
------------------------------------------------------------------------------
215482624           215482368           3288        256         established
------------------------------------------------------------------------------
No. of sessions: 1
```

For detailed operational session information use the following command.

```
show router l2tp session detail
==============================================================================
L2TP Session 215482624
==============================================================================

Connection ID: 215482624
State        : established
Tunnel Group : default_radius_group
Assignment ID: unnamed
Error Message: N/A

Control Conn ID   : 215482368           Remote Conn ID    : 81295874
Tunnel ID         : 3288                Remote Tunnel ID  : 1240
Session ID        : 256                 Remote Session ID : 31234
Time Started      : 10/04/2013 15:37:10
Time Established  : 10/04/2013 15:37:10 Time Closed       : N/A
CDN Result        : noError             General Error     : noError
------------------------------------------------------------------------------
No. of sessions:
```

LAC in Base Routing Context with Multiple Endpoints (Tunnel Selection Process)

The **debug router radius packet-type authentication** command shows the actual RADIUS authentication parameters returned. This example returns multiple tunnel endpoints from which the LAC selects one. This example uses weighted load balancing. (The L2TP tunnel selection process is out of the scope of this example).

```
<date> <time> CEST MINOR: DEBUG #2001 Base RADIUS
"RADIUS: Receive
  Access-Accept(2) id 190 len 299 from 172.16.1.1:1812 vrid 1 pol subscr-mgmt
    VSA [26] 21 Alcatel(6527)
      SUBSC ID STR [11] 19 user1@wholesale.com
    VSA [26] 11 Alcatel(6527)
      SUBSC PROF STR [12] 9 sub-func1
    VSA [26] 11 Alcatel(6527)
      SLA PROF STR [13] 9 sla-func1
#
    TUNNEL CLIENT ENDPOINT [66] 7 192.168.2.2
    VSA [26] 6 Alcatel(6527)
      TUNNEL ALGORITHM [47] 4 weighted access(1)   #input for tunnel selection
    TUNNEL ASSIGNMENT ID [82] 22 l2tp-functional-radius
    TUNNEL CLIENT AUTH ID [90] 7 lac-pe1
    VSA [26] 6 Alcatel(6527)
      TUNNEL MAX RETRIES ESTAB [52] 4 0 2
#
    TUNNEL TYPE [64] 4 1 L2TP(3)                   #Tunnel 1
    TUNNEL MEDIUM TYPE [65] 4 1 IPv4(1)
    TUNNEL SERVER ENDPOINT [67] 8 1 192.168.2.6
    TUNNEL ASSIGNMENT ID [82] 8 1 LNS1-T1
    TUNNEL PREFERENCE [83] 4 1 100                 #input for tunnel selection
#
    TUNNEL TYPE [64] 4 2 L2TP(3)                   #Tunnel 2
    TUNNEL MEDIUM TYPE [65] 4 2 IPv4(1)
    TUNNEL SERVER ENDPOINT [67] 8 2 192.168.2.7
    TUNNEL ASSIGNMENT ID [82] 8 2 LNS2-T2
    TUNNEL PREFERENCE [83] 4 2 100                #input for tunnel selection
#
    TUNNEL TYPE [64] 4 3 L2TP(3)                  #Tunnel 3
    TUNNEL MEDIUM TYPE [65] 4 3 IPv4(1)
    TUNNEL SERVER ENDPOINT [67] 8 3 192.168.2.8
    TUNNEL ASSIGNMENT ID [82] 8 3 LNS3-T3
    TUNNEL PREFERENCE [83] 4 3 120                #input for tunnel selection
#
    TUNNEL TYPE [64] 4 4 L2TP(3)                  #Tunnel 4
    TUNNEL MEDIUM TYPE [65] 4 4 IPv4(1)
    TUNNEL SERVER ENDPOINT [67] 8 4 192.168.2.9
    TUNNEL ASSIGNMENT ID [82] 8 4 LNS4-T4
    TUNNEL PREFERENCE [83] 4 4 140
```

The **debug router l2tp event lac-session-setup** command shows the LAC tunnel LNS1-T1 is selected for this example.

```
<date> <time> CEST MINOR: DEBUG #2001 Base PPPoE 15->L2TP
"PPPoE 15->L2TP: UDP 192.168.2.2:1701 -> 192.168.2.6:1701 #end 192.168.2.6
preference 100 tunnel l2tp-functional-radius:LNS1-T1      #preference 100
```

```
    request to open new tunnel 11212"

<date> <time> CEST MINOR: DEBUG #2001 Base PPPoE 15->L2TP
"PPPoE 15->L2TP: UDP 192.168.2.2:1701 -> 192.168.2.7:1701 #end 192.168.2.7
preference 100 tunnel l2tp-functional-radius:LNS2-T2      #preference 100
    skipped as another tunnel was selected"

<date> <time> CEST MINOR: DEBUG #2001 Base PPPoE 15->L2TP
"PPPoE 15->L2TP: UDP 192.168.2.2:1701 -> 192.168.2.6:1701
preference 100 tunnel l2tp-functional-radius:LNS1-T1      #selects 192.168.2.6
    create session 734820645"
```

The operational PPPoE session information in IES 1/base instance is shown as follows.

```
show service id 1 ppp session
===============================================================================
PPP sessions for service 1
===============================================================================
User-Name
  Descr.
           Up Time       Type  Termination     IP/L2TP-Id/Interface-Id
-------------------------------------------------------------------------------
user1@wholesale.com
  svc:1 sap:1/1/2:100.1 mac:00:00:00:01:01:01 sid:1
           0d 00:00:20   oE    lac             734820645
-------------------------------------------------------------------------------
No. of PPP sessions: 1
```

The operational tunnel information (base instance) is shown below.

```
show router l2tp tunnel
===============================================================================
Conn ID    Loc-Tu-ID Rem-Tu-ID State             Blacklist-state   Ses Active
  Group                                                            Ses Total
    Assignment
-------------------------------------------------------------------------------
734789632  11212     13723     established       not-blacklisted   1
  l2tp-functional-radius                                           1
    LNS1-T1
-------------------------------------------------------------------------------
No. of tunnels: 1
```

Operational session information (base instance) shows the session is in the established state.

```
show router l2tp session
===============================================================================
L2TP Session Summary
===============================================================================
ID                  Control Conn ID     Tunnel-ID   Session-ID  State
-------------------------------------------------------------------------------
734820645           734789632           11212       31013       established
-------------------------------------------------------------------------------
No. of sessions: 1
```

The L2TP endpoint/peer information shows there is one single tunnel for tunnel endpoint 192.168.2.6.

```
show router l2tp peer
======================================================
L2TP Peers
======================================================
Peer IP                    Port  Tun Active Ses Active
              Drain Reachability Tun Total  Ses Total
------------------------------------------------------
192.168.2.6                    1701  1          1   #LNS endpoint 192.168.2.6
                                 1          1
192.168.2.7                    1701  0          0
                                 0          0
192.168.2.8                    1701  0          0
                                 0          0
192.168.2.9                    1701  0          0
                                 0          0
------------------------------------------------------
No. of peers: 4
```

The following command gives a system overview of subscriber session related data. This system overview shows the current and peak values per session type (local PTA, LAC, LTS, LNS) and an overview of the number of originated or terminated L2TP tunnels. Peak values can be cleared via the **clear subscriber-mgmt peakvalue-stats** command.

```
show subscriber-mgmt statistics session system
=======================================================================
Subscriber Management Statistics for System
=======================================================================
          Type                      Current    Peak      Peak Timestamp
-----------------------------------------------------------------------
Session Statistics
-----------------------------------------------------------------------
Local     PPP Sessions - PPPoE            0       1 11/13/2013 17:04:23
          PPP Sessions - PPPoEoA          0       0
          PPP Sessions - PPPoA            0       0
          PPP Sessions - L2TP (LNS)       0       0
-----------------------------------------------------------------------
LAC       PPP Sessions - PPPoE            1       1 11/19/2013 15:46:40
          PPP Sessions - PPPoEoA          0       0
          PPP Sessions - PPPoA            0       0
          PPP Sessions - L2TP (LTS)       0       0
-----------------------------------------------------------------------
Total     PPP Sessions - established      1       2 11/19/2013 15:46:40
          PPP Sessions - in setup         0       1 11/19/2013 15:46:39
          PPP Sessions - local            0       1 11/13/2013 17:04:23
          PPP Sessions - LAC              1       1 11/19/2013 15:46:40
-----------------------------------------------------------------------
-----------------------------------------------------------------------
L2TP      L2TP Tunnels - originator       1       2 11/19/2013 15:40:13
          L2TP Tunnels - receiver         0       0
          Total L2TP Tunnels              1       2 11/19/2013 15:40:13
-----------------------------------------------------------------------
=======================================================================
Peak values last reset at : n/a
```

LAC in a VRF

This example returns VPRN 65536 as the L2TP service instance [26-6527-104 Alc-Tunnel-Serv-Id]. The VPRN 65536 interface system address is used as the L2TP source address since the attribute Tunnel-Client-Endpoint is not returned.

The ip-address 192.168.2.6 (Tunnel-Server-Endpoint) needs to be routable in VRF 65536 over a SAP or to a remote PE. This example uses BGP/MPLS IP Virtual Private Networks (VPNs) (RFC4364) to access the remote PE.

```
show router 65536 route-table
==============================================================================
Route Table (Service: 65536)
==============================================================================
Dest Prefix[Flags]                          Type    Proto     Age        Pref
      Next Hop[Interface Name]                                    Metric
------------------------------------------------------------------------------
<snip>
192.168.2.2/32                              Local   Local     11h10m45s  0
       system                                                       0
192.168.2.6/32                              Remote  BGP VPN   11h10m12s  170
       192.0.2.6 (tunneled)                                         0
```

Operational PPPoE session information for IES 1 (base instance) is shown using following command.

```
show service id 1 ppp session
==============================================================================
PPP sessions for service 1
==============================================================================
User-Name
  Descr.
           Up Time       Type  Termination     IP/L2TP-Id/Interface-Id
------------------------------------------------------------------------------
user1@wholesale.com
  svc:1 sap:1/1/2:100.1 mac:00:00:00:01:01:01 sid:1
           0d 00:00:12   oE    lac             718372593
------------------------------------------------------------------------------
No. of PPP sessions: 1
```

Operational tunnel information for VPRN 65536 is displayed as follows.

```
show router 65536 l2tp tunnel
==============================================================================
Conn ID    Loc-Tu-ID Rem-Tu-ID State              Blacklist-state   Ses Active
  Group                                                             Ses Total
    Assignment
------------------------------------------------------------------------------
718340096  10961     15559     established        not-blacklisted   1
  l2tp-functional-radius                                            1
    LNS1-T1
------------------------------------------------------------------------------
No. of tunnels: 1
```

Operational session information for VPRN 65536 is displayed using following command, and shows that the session is established.

```
show router 65536 l2tp session
==============================================================================
L2TP Session Summary
==============================================================================
ID                  Control Conn ID     Tunnel-ID   Session-ID  State
------------------------------------------------------------------------------
718372593           718340096           10961       32497       established
------------------------------------------------------------------------------
No. of sessions: 1
```

Scenario 2: Node-Derived L2TP Parameters

RADIUS Returns L2TP Group

This example returns VPRN 65536 as the L2TP service instance [26-6527-104] Alc-Tunnel-Serv-Id and an l2tp group-name wholesale.com [26-6527-46] Alc-Tunnel-Group.

```
<date> <time> CET MINOR: DEBUG #2001 Base RADIUS
"RADIUS: Receive
  Access-Accept(2) id 73 len 114 from 172.16.1.1:1812 vrid 1 pol subscr-mgmt
    VSA [26] 21 Alcatel(6527)
      SUBSC ID STR [11] 19 user1@wholesale.com
    VSA [26] 11 Alcatel(6527)
      SUBSC PROF STR [12] 9 sub-func1
    VSA [26] 11 Alcatel(6527)
      SLA PROF STR [13] 9 sla-func1
    VSA [26] 6 Alcatel(6527)
      TUNNEL SERVICE ID [104] 4 65536         #LAC in VRF
    VSA [26] 15 Alcatel(6527)
      TUNNEL GROUP [46] 13 wholesale.com      #points to L2TP node group name
```

For operational PPPoE session information in IES 1/base instance, use following command.

```
*A:pe1# show service id 1 ppp session
==============================================================================
PPP sessions for service 1
==============================================================================
User-Name
  Descr.
           Up Time       Type  Termination     IP/L2TP-Id/Interface-Id
------------------------------------------------------------------------------
user1@wholesale.com
  svc:1 sap:1/1/2:100.1 mac:00:00:00:01:01:01 sid:1
           0d 00:00:11    oE    lac             768347764
------------------------------------------------------------------------------
No. of PPP sessions: 1
```

Operational tunnel information for VPRN 65536 shows the tunnel is in the established state.

```
show router 65536 l2tp tunnel
==============================================================================
Conn ID    Loc-Tu-ID Rem-Tu-ID State              Blacklist-state   Ses Active
  Group                                                             Ses Total
    Assignment
------------------------------------------------------------------------------
768344064  11724     14445     established        not-blacklisted   1
  wholesale.com                                                     1
```

```
    wholesale.com
-------------------------------------------------------------------------------
No. of tunnels: 1
```

The operational session information for VPRN 65536 shows the session is in the established state.

```
show router 65536 l2tp session
===============================================================================
L2TP Session Summary
===============================================================================
ID                  Control Conn ID     Tunnel-ID   Session-ID  State
-------------------------------------------------------------------------------
768347764           768344064           11724       3700        established
-------------------------------------------------------------------------------
No. of sessions: 1
```

LUDB Returns L2TP Group

This example returns VPRN 65536 as the L2TP service instance and l2tp group-name wholesale.com (LUDB **l2tp** group "wholesale.com" service-id 65536).

The **debug subscriber-mgmt local-user-db "l2tp" detail all** command shows the LUDB authentication access (The returned parameter details are not shown).

```
<date> <time> CET MINOR: DEBUG #2001 Base LUDB
"LUDB: User lookup success - host found
  user-name:
    original:  user1@wholesale.com
    masked:    user1@wholesale.com

  Host wholesale.com found in user data base l2tp     #host found
```

To show the operational data from LUDB **l2tp**, use the following command.

```
show subscriber-mgmt local-user-db "l2tp" ppp-host "wholesale.com" | match N/A invert-
match | match none invert-match
===============================================================================
PPP Host "wholesale.com"
===============================================================================
Admin State          : Up
Last Mgmt Change     : 11/22/2013 17:35:28

Host Identification
 User Name           : wholesale.com (domain only)

Matched Objects      : userName

Password Type        : ignore
PADO Delay           : 0msec
Force IPv6 CP        : Disabled

Identification Strings (option 254)
 Subscriber Id       : user1@wholesale.com
 SLA Profile String  : sla-func1
 Sub Profile String  : sub-func1

L2TP
 Service             : 65536                      #LAC in VRF
 Tunnel Group        : wholesale.com              #points to L2TP group name
```

The **debug router l2tp event lac-session-setup** command shows the LAC tunnel selected for this example.

```
<date> <time> CET MINOR: DEBUG #2001 vprn65536 PPPoE 28->L2TP
"PPPoE 28->L2TP: UDP 192.168.2.2:1701 -> 192.168.2.6:1701
preference 50 tunnel wholesale.com:wholesale.com       #group and tunnel name
    request to open new tunnel 15501"

462 2013/11/22 17:39:13.21 CET MINOR: DEBUG #2001 vprn65536 PPPoE 28->L2TP
"PPPoE 28->L2TP: UDP 192.168.2.2:1701 -> 192.168.2.6:1701
```

```
preference 50 tunnel wholesale.com:wholesale.com
    create session 1015877546"
```

For the operational PPPoE session information in IES 1/base instance, use the following command.

```
show service id 1 ppp session
==============================================================================
PPP sessions for service 1
==============================================================================
User-Name
  Descr.
           Up Time       Type  Termination     IP/L2TP-Id/Interface-Id
------------------------------------------------------------------------------
user1@wholesale.com
  svc:1 sap:1/1/2:100.1 mac:00:00:00:01:01:01 sid:1
           0d 00:00:10   oE    lac             1015877546
------------------------------------------------------------------------------
No. of PPP sessions: 1
```

Operational tunnel information for VPRN 65536 can be obtained using following command.

```
show router 65536 l2tp tunnel
==============================================================================
Conn ID    Loc-Tu-ID Rem-Tu-ID State              Blacklist-state   Ses Active
  Group                                                             Ses Total
    Assignment
------------------------------------------------------------------------------
1015873536 15501     11826     established        not-blacklisted   1
  wholesale.com                                                     1
    wholesale.com
------------------------------------------------------------------------------
No. of tunnels: 1
```

The operational session information for VPRN 65536 shows the session is in the established state.

```
show router 65536 l2tp session
==============================================================================
L2TP Session Summary
==============================================================================
ID                  Control Conn ID     Tunnel-ID   Session-ID  State
------------------------------------------------------------------------------
1015877546          1015873536          15501       4010        established
------------------------------------------------------------------------------
No. of sessions: 1
```

Advanced Topics

Non-Session-Triggered L2TP Tunnel Setup

In addition to the ppp-session-triggered setup, an L2TP tunnel can also be setup via a tools command or an auto-establish command. These non-session-triggers are useful, for example, during the initial configuration phase where the LAC-LNS tunnel setup can be tested without any other user interaction. The PPP user still triggers the L2TP session-setup over this L2TP tunnel and RADIUS needs to return an l2tp group-name with the relevant name during authentication.

Auto-Establish

Every one minute a check is performed to determine if tunnels need to be established (a process referred to as scan auto-establish). The tunnel state is establishedIdle when the tunnel is setup, and becomes established when user triggered sessions are setup over this tunnel.

```
configure service vprn 65536
   <snip>
   l2tp
       group "wholesale.com"
          tunnel "wholesale.com"
              local-address 192.168.2.2
              local-name "lac-pe1"
              peer 192.168.2.6
              auto-establish        #triggers tunnel setup
              no shutdown
          exit
          no shutdown
      exit
      no shutdown
   exit
```

There is no difference in operational behavior for a tunnel setup via a session-trigger or an auto-establish command. Removing the auto-establish parameter has no impact on active tunnels (establishedIdle or established).

```
show router 65536 l2tp tunnel
==============================================================================
Conn ID    Loc-Tu-ID Rem-Tu-ID State              Blacklist-state   Ses Active
  Group                                                             Ses Total
    Assignment
------------------------------------------------------------------------------
960495616  14656     721       establishedIdle    not-blacklisted   0
  wholesale.com                                                     0
    wholesale.com
------------------------------------------------------------------------------
No. of tunnels: 1
```

Tools Tunnel Start

An alternative for auto-establish is the tools start command.

```
configure service vprn 65536
   <snip>
   l2tp
       group "wholesale.com"
          tunnel "wholesale.com"
              local-address 192.168.2.2
              local-name "lac-pe1"
              peer 192.168.2.6
              no auto-establish        #no triggers tunnel setup
              no shutdown
          exit
          no shutdown
      exit
      no shutdown
   exit


tools perform router 65536 l2tp group wholesale.com tunnel wholesale.com start
```

How Long Does a Tunnel Remain Idle Before Being Torn Down?

A persistent tunnel is a tunnel that remains available after the last session over that tunnel is closed. To create a persistent tunnel, the idle-timeout parameter must be set to infinite.

A non-persistent tunnel is torn down immediately (idle-timeout zero) after the last session over that tunnel is closed or after a configurable delay. The idle-timeout parameter is set via the RADIUS [26-6527-49] Alc-Tunnel-Idle-Timeout attribute or the corresponding node parameter. The default value for this parameter is infinite (persistent).

Idle-Timeout

```
configure router l2tp | configure service vprn l2tp
       idle-timeout [0..3600]seconds
       <snip>
       group <tunnel-group-name>
           idle-timeout [0..3600]secondzs | infinite
           <snip>
           tunnel  <tunnel-name>
              idle-timeout [0..3600]seconds | infinite
              <snip>
```

The following shows an example of a persistent tunnel (idle-timeout infinite).

```
show router l2tp tunnel detail       # Example persistent tunnel
==============================================================================
Connection ID: 111804416
State        : establishedIdle       # moves from established to establishedI-
dle
                                     # after last session is closed
<snip>
Assignment ID: unnamed
Group Name   : default_radius_group
Error Message: N/A
                                      Remote Conn ID    : 586874880
Tunnel ID        : 1706               Remote Tunnel ID  : 8955
Preference       : 50                 Receive Window    : 64
Hello Interval(s): 300
Idle TO (s)      : infinite           Destruct TO (s)   : 60
<snip>
```

The following shows an example of a non-persistent tunnel (idle-timeout 10 seconds).

```
show router l2tp tunnel  detail   # Example non-persistent tunnel
==============================================================================
Connection ID: 1039335424
State        : closed            # moves from established to establishedIdle
                                 # after last session is terminated. Ten
                                 # seconds later state becomes closed(tunnel
                                 # destroyed). Operational tunnel data
                                 # stays available (trouble shooting
                                  # purposes)for a short period of time.(see
                                  # further destruct-timeout).
<snip>
Assignment ID: unnamed
Group Name   : default_radius_group
Error Message: idle timeout (10 seconds) expired
                                       Remote Conn ID    : 218169344
Tunnel ID        : 15859               Remote Tunnel ID  : 3329
Preference       : 50                  Receive Window    : 64
Hello Interval(s): 300
Idle TO (s)      : 10                  Destruct TO (s)   : 60
<snip>
```

Tools Tunnel Stop

In addition to the idle-timeout used for tunnel termination, a tools stop command is also available that can be used to terminate persistent and non-persistent tunnels at any moment in time. Be aware that this command is very destructive and destroys all sessions carried over the closed tunnel.

Following command shows the tunnel is in the establishedIdle state.

```
show router 65536 l2tp tunnel
===============================================================================
Conn ID    Loc-Tu-ID Rem-Tu-ID State             Blacklist-state   Ses Active
  Group                                                            Ses Total
    Assignment
-------------------------------------------------------------------------------
462749696  7061      9070      establishedIdle    not-blacklisted   0
  wholesale.com                                                    0
    wholesale.com
-------------------------------------------------------------------------------
No. of tunnels: 1
```

The command below terminates the l2tp tunnel. The tunnel is aborted (the LAC sends StopCCN) using the <connection-id> or <tunnel-group-name>+<tunnel-name> as input. This StopCCN indicates "operator request" as the error reason.

```
tools perform router 65536 l2tp group wholesale.com tunnel wholesale.com stop
#
tools perform router 65536 l2tp tunnel 462749696 stop
```

The trace and debug output below shows the tunnel being aborted.

```
<date> <time> CET MINOR: DEBUG #2001 vprn65536 L2TP(v2, ctrl, egress)
"L2TP(v2, ctrl, egress): UDP 192.168.2.2:1701 -> 192.168.2.6:1701
tunnel 9070 session 0, ns 2 nr 1, flags:, reserved=0
    AVP MessageType(0,0), flags: mandatory, reserved=0
        StopControlConnectionNotification(4)
    AVP ResultCode(0,1), flags: mandatory, reserved=0
        result-code: "generalRequestToClearControlConnection"(1), error-code:
```

```
        "noGeneralError"(0)
        error-msg: "operator request"
    AVP AssignedTunnelId(0,9), flags: mandatory, reserved=0
        7061"
```

Keepalive (hello)

A keepalive mechanism is employed by L2TP in order to differentiate tunnel outages from extended periods of no control or data activity on a tunnel. This is accomplished by injecting Hello control messages after a specified period of time has elapsed since the last data or control message (ZLB not included) was received on a tunnel. As for any other L2TP control message, if the Hello message is not reliably delivered then the tunnel is declared down and reset, as defined in RFC 2661, *Layer Two Tunneling Protocol "L2TP"*. This means that the 7x50 does not initiate hello packets if session control traffic is handled over this tunnel. The 7x50 resets the hello timer if the system transmits any control packet over this tunnel (ZLB packets and data traffic are not taken into account).

The keepalive function is disabled (not recommended) using RADIUS [26-6527-50] Alc-Tunnel-Hello-Interval -1 or hello-interval infinite. The number of retries for unsuccessful Hello packet delivery equals RADIUS [26-6527-52] Alc-Tunnel-Max-Retries-Estab or node parameter max-retries-estab (default 5). The retry interval is initially set to 1 second and doubles on each retry with a maximum interval of 8 seconds. Using a max-retries-estab 7 results in a retry of [1,2,4,8,8,8,8 seconds].

```
configure router l2tp | configure service vprn l2tp
       hello-interval [60..3600]seconds | infinite  #default 300s
       max-retries-estab [2..7]                     #default 5
       <snip>
       group <tunnel-group-name>
           hello-interval [60..3600]seconds | infinite
           max-retries-estab [2..7]
           <snip>
           tunnel  <tunnel-name>
              hello-interval [60..3600]seconds | infinite
              max-retries-estab [2..7]
              <snip>
```

For example, the LAC can be configured with an hello-timer of 1 minute and the LNS with an hello-timer of 2 minutes. The hello-timer interval for LAC and LNS do not have to be same as the keepalive mechanism works asynchronous. See L2TP Keepalive Mechanism on page 2496.

```
LAC > show router l2tp tunnel
==============================================================================
Conn ID    Loc-Tu-ID Rem-Tu-ID State              Blacklist-state   Ses Active
  Group                                                             Ses Total
    Assignment
------------------------------------------------------------------------------
148635648  2268      13918     established        not-blacklisted   1
  l2tp-functional-radius                                            1
    LNS1-T1
```

Keepalive (hello)

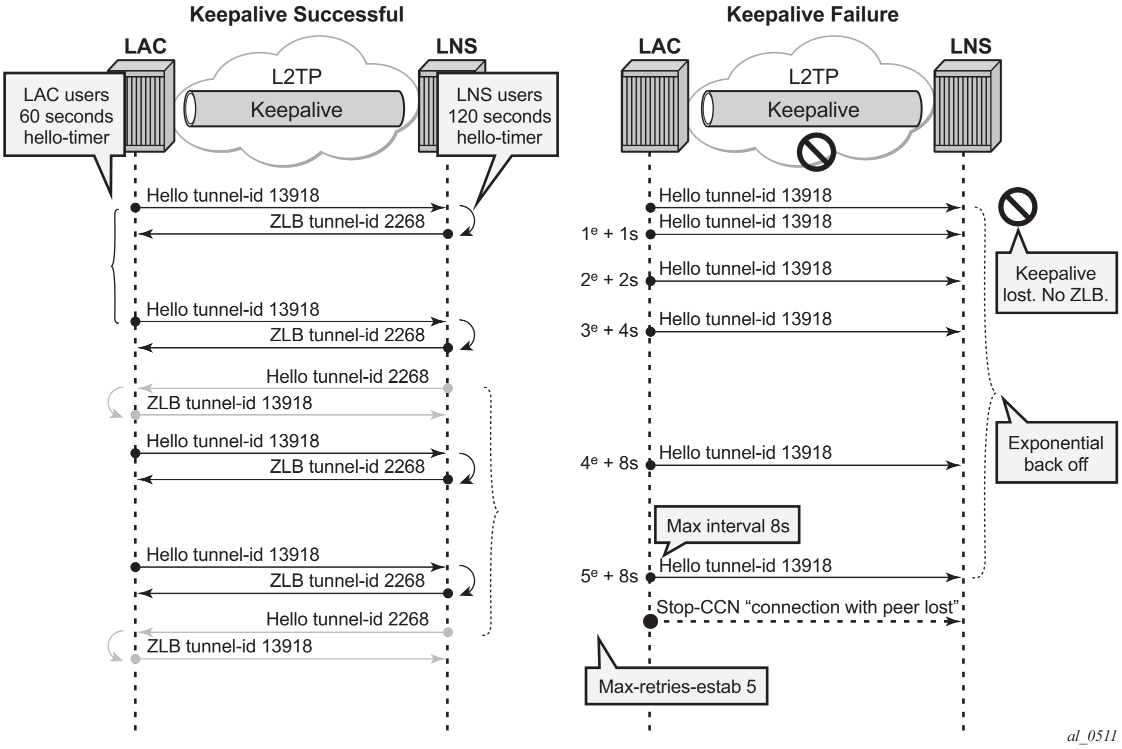


Figure 386: L2TP Keepalive Mechanism

Figure 386 shows the tunnel being closed after 5 unsuccessful Hello deliveries with error-message **connection with peer lost**.

```
LAC > show router l2tp tunnel detail
===============================================================================
L2TP Tunnel Status
===============================================================================
Connection ID: 148635648
State        : closed
<snip>
Error Message: connection with peer lost
                                          Remote Conn ID    : 912130048
Tunnel ID        : 2268                   Remote Tunnel ID  : 13918
Preference       : 100                    Receive Window    : 64
Hello Interval(s): 60
<snip>
```

Does L2TP Keeps Info About Closed Tunnels, Sessions?

The destruct-timeout parameter (expressed in seconds) controls the period of time that the tunnel, or session data related to a closed (disconnected) tunnel, or session persists before being removed. The destruct_timeout is a debugging aid by saving underlying memory structures after the tunnel, or session is terminated. It is configured via the RADIUS [26-6527-51] Alc-Tunnel-Destruct-Timeout attribute or the corresponding node parameter. Default value for this parameter is 60 seconds.

```
configure router l2tp | configure service vprn l2tp
       destruct-timeout [60..86400]
       <snip>
       group <tunnel-group-name>
           destruct-timeout [60..86400]
           <snip>
           tunnel  <tunnel-name>
              destruct-timeout [60..86400]
```

The following output shows a session that is closed and the reason for it being terminated.

```
show router l2tp session detail
==============================================================================
L2TP Session 228095933
==============================================================================

Connection ID: 228095933
State        : closed       #session destroyed but data still available
Tunnel Group : default_radius_group
Assignment ID: unnamed
Error Message: Terminated by PPPoE: RX PADT

Control Conn ID   : 228065280           Remote Conn ID    : 609491118
Tunnel ID         : 3480                Remote Tunnel ID  : 9300
Session ID        : 30653               Remote Session ID : 6318
Time Started      : 10/08/2013 17:14:36
Time Established  : 10/08/2013 17:14:36 Time Closed       : 10/08/2013 17:14:43
CDN Result        : generalError        General Error     : vendorSpecific
```

The following output shows a tunnel that is closed and the reason for it being closed.

```
show router l2tp tunnel detail
==============================================================================
L2TP Tunnel Status
==============================================================================
Connection ID: 228065280
State        : closed              #tunnel destroyed but data still available
<snip>
Assignment ID: unnamed
Group Name   : default_radius_group
Error Message: idle timeout (0 seconds) expired
                                        Remote Conn ID    : 609484800
Tunnel ID        : 3480                Remote Tunnel ID  : 9300
```

```
Preference       : 50                  Receive Window    : 64
Hello Interval(s): 300
Idle TO (s)      : 0                   Destruct TO (s)   : 60
Max Retr Estab   : 5                   Max Retr Not Estab: 5
Session Limit    : 32767               AVP Hiding        : never
Transport Type   : udpIp               Challenge         : never
Time Started     : 10/08/2013 17:14:36 Time Idle         : 10/08/2013 17:14:43
Time Established : 10/08/2013 17:14:36 Time Closed       : 10/08/2013 17:14:43
Stop CCN Result  : generalReq          General Error     : noError
Blacklist-state  : not-blacklisted
```

Floating Peers

A floating peer exists if the peer LNS address indicated in the source address of the SCCRP is different from the peer address known on the LAC. Floating peer allowance is configuration driven and is rejected by default.

The parameter peer-address-change-policy specifies whether the LAC accepts, ignores or rejects requests from a peer to change the destination IP address or UDP port.

```
configure router l2tp | configure service vprn l2tp
       peer-address-change-policy accept | ignore | reject   #default reject
```

- accept — Specifies that this system accepts any source IP address change for received L2TP control messages related to a locally originated tunnel in the state wait-reply and rejects any peer address change for other tunnels. In case the new peer IP address is accepted, it is learned and used as destination address in subsequent L2TP messages.

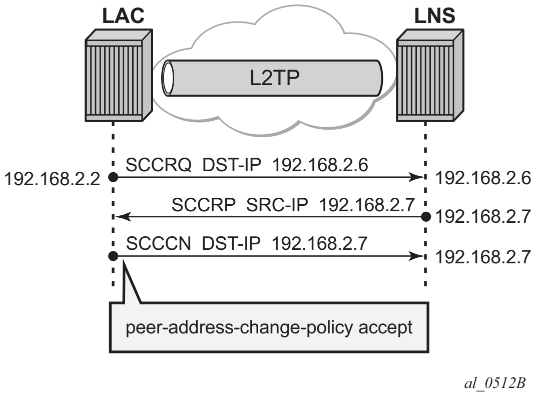


Figure 387: Floating Peers Accept

- Ignore — Specifies that this system ignores any source IP address change for received L2TP control messages, does not learn any new peer IP address and does not change the destination address in subsequent L2TP messages.

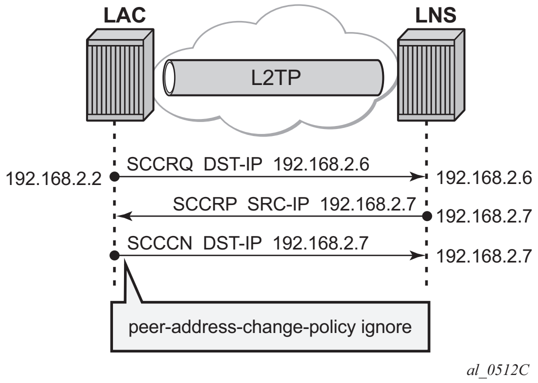


Figure 388: Floating Peers Ignore

- Reject — Specifies that this system rejects any source IP address change for received L2TP control messages and drops those messages.

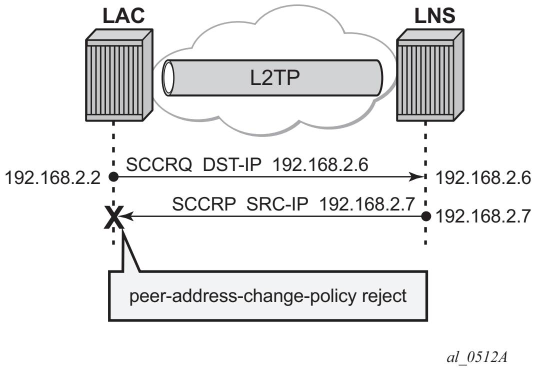


Figure 389: Floating Peers Reject

The values Peer IP, Tx dst-IP and Rx src-IP in the **show router l2tp tunnel detail** command indicates if floating peers are used or not.

An example of a floating peer (peer-address-change-policy accept) is shown below.

```
show router l2tp tunnel detail
=======================================
L2TP Tunnel Status
=======================================
Connection ID: 897122304
State         : established
IP            : 192.0.2.2
UDP           : 1701
Peer IP       : 192.168.2.6     # (1) peer address used in SCCRQ
Peer UDP      : 1701
Tx dst-IP     : 192.168.2.7     # (3) peer address used in SCCCN
Tx dst-UDP   : 1701
Rx src-IP    : 192.168.2.7     # (2) SCCRP different IP received
Rx src-UDP   : 1701
<snip>
```

Tx Connect Speed AVP 24 and Rx Connect Speed AVP 38

The Connect Speed (TX AVP 24 and RX AVP 38) is passed in the ICCN messages sent from the LAC to the LNS. The L2TP AVP 24 defines the (Tx) connect speed in bps from the perspective of traffic flowing from the LAC towards the subscriber (BNG downstream rate).The L2TP AVP 38 defines the (Rx) connect speed in bps from the perspective of traffic flowing from the subscriber towards the LAC (BNG upstream rate).

The report-rate configuration option indicates what rate is reported to the LNS when creating an L2TP session.

```
configure subscriber-mgmt
 sla-profile <sla-profile-name>
  ingress
   report-rate agg-rate-limit|scheduler|pppoe-actual-rate|rfc5515-actual-rate
  egress
   report-rate agg-rate-limit|scheduler|pppoe-actual-rate|rfc5515-actual-rate
```

- agg-rate-limit — Take the aggregate rate as received from the RADIUS Access-Accept message in VSA Alc-Subscriber-QoS-Override. When this RADIUS VSA is not present in the Access-Accept, or when RADIUS is not used, then take the configured aggregate rate limit. In the case where this is not configured then take the port rate.
- scheduler <scheduler-name> — Take the rate of the specified scheduler. In case the scheduler is not linked with the scheduler-policy from the subscriber-profile then take the port rate.
- pppoe-actual-rate — Take the rate from the DSL-Forum Vendor-Specific PPPoE Tag when available, otherwise take the port rate.
- rfc5515-actual-rate — Put the same value as the transmitted Actual-Data-Rate-Upstream AVP in the Rx-Connect-Speed AVP, and the same value as the transmitted Actual-Data-Rate-Downstream AVP in the Tx-Connect-Speed AVP.

Calling Number AVP 22 Format

The format of AVP 22 Calling Number in the ICRQ message is configurable via the parameter calling-number-format. The default format is "%S<space>%s" and corresponds to the concatenation of system-name<space>sap-id. Available parameters are %S (system-name), %c (Agent Circuit Id), %r Agent Remote Id, %s (sap-id), %l (Logical Line ID) and fixed strings. A combination can be configured from any of these parameters, but the total configured format cannot exceed 255 characters.

Example 1: Default configuration.

```
configure router l2tp
   calling-number-format "%S %s”     #default configuration
   <snip>

<date> <time> CEST MINOR: DEBUG #2001 Base L2TP(v2, ctrl, egress)
"L2TP(v2, ctrl, egress): UDP 192.0.2.2:1701 -> 192.168.2.6:1701
tunnel 1240 session 0, ns 2 nr 1, flags:, reserved=0
    AVP MessageType(0,0), flags: mandatory, reserved=0
        IncomingCallRequest(10)
    <snip>
    AVP CallingNumber(0,22), flags: mandatory, reserved=0
        "pe1 1/1/2:100.1"
```

Example 2: Customized configuration and all parameters (%S %s %c) are available to construct the requested AVP 22.

```
configure router l2tp
   calling-number-format "start-%S###%s###%c-end"
   <snip>

<date> <time> CEST MINOR: DEBUG #2001 Base L2TP(v2, ctrl, egress)
"L2TP(v2, ctrl, egress): UDP 192.0.2.2:1701 -> 192.168.2.6:1701
tunnel 12758 session 0, ns 2 nr 1, flags:, reserved=0
    AVP MessageType(0,0), flags: mandatory, reserved=0
        IncomingCallRequest(10)
    <snip>
    AVP CallingNumber(0,22), flags: mandatory, reserved=0
        "start-pe1###1/1/2:100.1###circuit0-end"
```

Example 3: Customized configuration and not all parameters are available to construct the requested AVP 22. Option-82 circuit-id (%c) and LLID (%l) information are missing and therefore missing (skipped) in the formatted attribute.

```
configure router l2tp
   calling-number-format "%S#%c#%r#%l#%s"
   <snip>

<date> <time> CEST MINOR: DEBUG #2001 Base L2TP(v2, ctrl, egress)
"L2TP(v2, ctrl, egress): UDP 192.0.2.2:1701 -> 192.168.2.6:1701
tunnel 8847 session 0, ns 2 nr 1, flags:, reserved=0
    AVP MessageType(0,0), flags: mandatory, reserved=0
```

Calling Number AVP 22 Format

```
    IncomingCallRequest(10)
<snip>
AVP CallingNumber(0,22), flags: mandatory, reserved=0
    "pe1##remote0##1/1/2:100.1"
```

Prevent LAC from transmitting Calling Number AVP 22 to LNS

By default, the LAC includes the Calling Number AVP 22 in the L2TP incoming-call-request (ICRQ) packets transmitted to LNS. This AVP identifies the interface that is connected to the customer in the access network. Network access interface information can be hidden by configuring the LAC not to send the Calling Number AVP to the LNS.

Use the command below to disable the sending of L2TP Calling Number AVP 22.

```
configure router l2tp
        exclude-avps calling-number
```

cisco-nas-port AVP 100

Interoperation with a Cisco LNS requires that the LAC communicates a NAS port type to the LNS via the L2TP ICRQ ‘Cisco Nas Port Info AVP (100)’. This AVP (100) includes information that identifies the NAS port and indicates whether the port type is Ethernet or ATM and is configured via the cisco-nas-port parameter.

Cisco AVP 100 format

- First 5 bytes are NAS-Port-Type:

    ç 0f10090203 (Ethernet)

    ç 0f10090201 (ATM)

- Remaining 4 bytes corresponds with the configured cisco-nas-port value

Example:

- Ethernet 12b s-vlan-id; 10b c-vlan-id; 3b slot number; 2b MDA nbr; 5b port
- ATM 12b VPI; 10b VCI; 3b slot number; 2b MDA nbr; 5b port

```
configure router l2tp
        cisco-nas-port ethernet "*12o*10i*3s*2m*5p" atm "*12v*10c*3s*2m*5p"
```

nas-port 1/1/2:100.1 corresponds to 1100100 0000000001 001 01 00010 = 104858786

```
<date> <time> CEST MINOR: DEBUG #2001 Base L2TP(v2, ctrl, egress)
"L2TP(v2, ctrl, egress): UDP 192.0.2.2:1701 -> 192.168.2.6:1701
tunnel 10948 session 0, ns 2 nr 1, flags:, reserved=0
    AVP MessageType(0,0), flags: mandatory, reserved=0
        IncomingCallRequest(10)
    AVP CiscoNasPort(9,100), flags:, reserved=0
        104858786 type=ethernet(0f:10:09:02:03)     # 104858786 = 1/1/2:100.1
    AVP AssignedSessionId(0,14), flags: mandatory, reserved=0
        7556
```

cisco-nas-port AVP 100

```
AVP CallSerialNumber(0,15), flags: mandatory, reserved=0
    41
AVP CallingNumber(0,22), flags: mandatory, reserved=0
    "pe1 1/1/2:100.1"
<snip>
```

L2TP Group/Peer/Tunnel Draining

When the LAC has established sessions, the LAC can avoid the creation of new sessions for a specific group, peer, or tunnel, via the **drain** command.

No new sessions are created for a group, peer or tunnel that is being drained (draining state) but the current sessions are left intact.

After the **drain** command is issued, the group, peer, or tunnel moves from a draining to drained state when the last session is closed. A drained group, peer, or tunnel can then be managed (reconfigured, deleted) without any user impact.

Be aware that a group, peer, or tunnel in a draining or drained state is skipped in the tunnel selection process. The next example shows a tunnel draining; group and peer draining works according in the same way.

A tunnel has 1 session and is in established state.

```
show router 65536 l2tp tunnel
==============================================================================
Conn ID    Loc-Tu-ID Rem-Tu-ID State              Blacklist-state   Ses Active
  Group                                                              Ses Total
    Assignment
------------------------------------------------------------------------------
270073856  4121      3238      established        not-blacklisted   1
  wholesale.com                                                     1
    wholesale.com
------------------------------------------------------------------------------
No. of tunnels: 1
```

The following tools **drain** command puts the tunnel in a draining state and leaves the sessions intact.

```
tools perform router 65536 l2tp tunnel 270073856 drain
```

Initially the tunnel is in the draining state.

```
show router 65536 l2tp tunnel
==============================================================================
Conn ID    Loc-Tu-ID Rem-Tu-ID State              Blacklist-state   Ses Active
  Group                                                              Ses Total
    Assignment
------------------------------------------------------------------------------
270073856  4121      3238      draining           not-blacklisted   1
  wholesale.com                                                     1
    wholesale.com
------------------------------------------------------------------------------
No. of tunnels: 1
```

The tunnel moves to the drained state at the moment the last session is closed. Debugging shows that a drained tunnel is also not used as last resort and is skipped during the tunnel selection process.

```
show router 65536 l2tp tunnel
===============================================================================
Conn ID    Loc-Tu-ID Rem-Tu-ID State            Blacklist-state   Ses Active
  Group                                                           Ses Total
    Assignment
-------------------------------------------------------------------------------
270073856  4121      3238      drained          not-blacklisted   1
  wholesale.com                                                   1
    wholesale.com
-------------------------------------------------------------------------------
No. of tunnels: 1
```

The output below shows new sessions cannot select a drained tunnel.

```
<date> <time> CET MINOR: DEBUG #2001 vprn65536 PPPoE 30->L2TP
"PPPoE 30->L2TP: UDP 192.168.2.2:1701 -> 192.168.2.6:1701
preference 50 tunnel wholesale.com:wholesale.com        #tunnelis drained
    no additional session can be created in tunnel 4121"

785 2013/11/24 16:11:39.05 CET MINOR: DEBUG #2001 vprn65536 PPPoE 30->L2TP
"PPPoE 30->L2TP:
    stop: no more tunnels can be tried"
```

The drained tunnel can then be closed without user impact.

```
tools perform router 65536 l2tp tunnel 270073856 stop
```

Conclusion

This example provides the LAC L2TP access server configuration and troubleshooting commands for the LAA architecture (tunneled-access) model.