Technical Guide

L2TPv2 Tunneling of PPP

Feature Overview and Configuration Guide

This document describes the overall process of tunneling PPPoE connections through L2TP tunnels. There are two main sections to this description:

- an overview of L2TPv2 tunnels
- an explanation of how the LAC end of the L2TP tunnel employs PPPoE AC functionality to transition multiple PPPoE connections onto an L2TPv2 tunnel.

Configuration examples show how to configure an AlliedWare Plus device to terminate multiple incoming PPPoE client connections and tunnel their PPP sessions via the L2TP LAC to one or more remote L2TP LNS devices. They illustrate how to use DNS or RADIUS lookups or static configuration to determine tunnel destinations.

C613-22085-00 REVB

Contents

Products and software version that apply to this guide

This guide applies to AlliedWare Plus™ products that support PPP tunneling via L2TPv2 (LAC), running version **5.4.6** or later.

To see whether your product supports PPP tunneling via L2TPv2 (LAC), see the following documents:

- The product's Datasheet
- The AlliedWare Plus Datasheet
- The product's Command Reference

These documents are available from the above links on our website at alliedtelesis.com.

Feature support may change in later software versions. For the latest information, see the above documents.

Related documents

The following documents give more information about related features on AlliedWare Plus products:

- the Point-to-Point Protocol (PPP) Feature Overview and Configuration Guide
- the RADIUS Feature Overview and Configuration Guide
- the DNS section in the Internet Protocol (IP) Addressing and Protocols Feature Overview and Configuration Guide

These documents are available from the links above or on our website at alliedtelesis.com

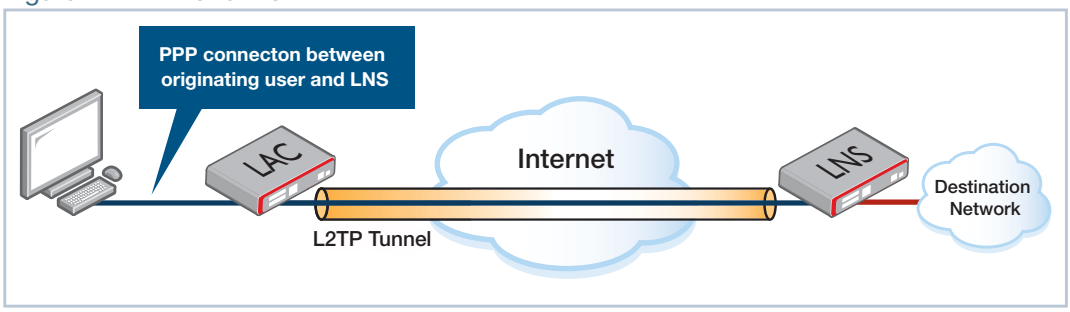
L2TPv2 Tunnels Overview

The L2TPv2 components implemented on AlliedWare Plus devices supporting L2TPv2 tunnels are based on the functionality described in RFC 2661.

L2TPv2 tunnels Layer 2 connections through a separate or intermediate Layer 3 network such as the Internet.

L2TPv2 creates tunnels between a local endpoint (an L2TP Access Concentrator or LAC) and a remote endpoint (an L2TP Network Server or LNS). The LAC typically acts as a client and initiates the tunnels, while the LNS typically acts as a server that listens for incoming tunnel requests. Network traffic is bi-directional between the LAC and the LNS once an L2TP tunnel is established through the intermediate network. See Figure 1 below.

Figure 1: L2TP to tunnel PPP



The LAC creates an L2TPv2 tunnel to the defined LNS. The connection request from the LAC may include the information required to allow the LNS to authenticate the user at the originating end of the Layer 2 connection and accept or decline the connection. Once the L2TPv2 tunnel is established, an L2TP session is created over the tunnel. Encapsulated PPP frames associated with the session can then pass through the tunnel. The LNS accepts the frames, strips off the L2TP encapsulation and processes them as normal incoming PPP frames. These PPP frames are processed as if they had come directly from the link layer. For an L2TP and PPP encapsulation diagram for data over an IP network see Figure 2 on page 6.

L2TPv2 Terminology

This section describes some key L2TPv2 terms.

- **L2TPv2 (Layer 2 Tunneling Protocol)**

  L2TPv2 enables encapsulated Layer 2 frames to be carried across the network. For L2TPv2 these L2 frames are Point-to-Point Protocol (PPP) Layer 2 frames. L2TPv2 enables Point-to-Point (PPP) frames to be totally encapsulated within network packets, so that they can then be tunnelled through a Layer 3 network such as the Internet. PPP defines an encapsulation mechanism for transporting multiprotocol packets, such as IP packets, across point-to-point links. L2TPv2 extends the PPP model by tunneling the point-to-point link across an intermediate Layer 3 network.

- **LAC (L2TP Access Concentrator)**

  An LAC resides at one end of an L2TPv2 tunnel. The LAC sits between an LNS and a client and forwards PPP packets to and from each. Packets sent from the LAC to the LNS are encapsulated and sent into the L2TP tunnel. The packets sent from the LNS arrive via the tunnel, are decapsulated, and sent to the client. The LAC and LNS have no awareness of what data is contained within the PPP packets.

- **LNS (L2TP Network Server)**

  An LNS resides at one end of an L2TPv2 tunnel and acts as a peer to the LAC. An LNS is an L2TPv2 server that terminates the incoming tunnel from the L2TP LAC. An LNS is the logical termination point of the PPP session that is being tunneled from the client by the LAC.

- **L2TPv2 Tunnel**

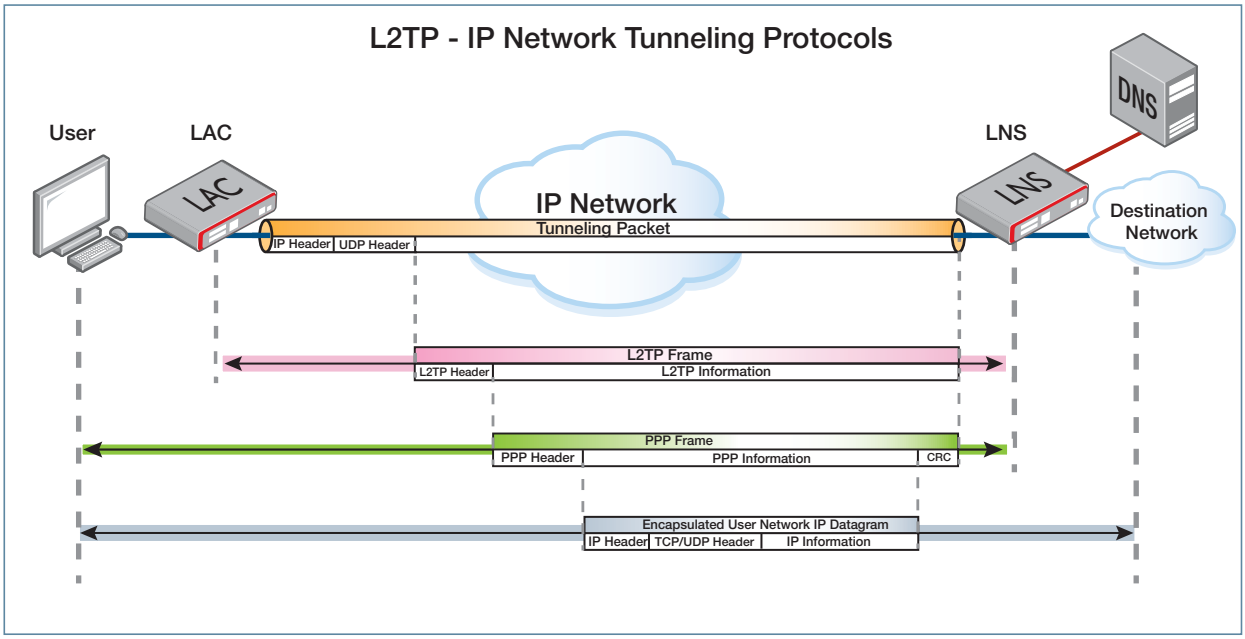
  A tunnel is a logical connection between the LAC and the LNS that can carry one or more PPP sessions. The tunnel consists of a control connection and zero or more sessions, each of which carries an encapsulated PPP connection. With AlliedWare Plus L2TPv2, each tunnel has two tunnel identifiers, one for the local end and one for the peer. Outgoing frames have the destination tunnel identifier.

- **L2TPv2 Session**

  An L2TPv2 session is created between the LAC and LNS when an end-to-end PPP connection is to be established between a client and the LNS. There is a one-to-one relationship between established L2TPv2 sessions and their associated L2TPv2 calls, where a single tunnelled PPP session is referred to as an L2TPv2 call. An L2TPv2 session must be created before the PPP session can be established since L2TPv2 is connection-oriented. L2TPv2 is a connection oriented protocol in that both the LAC and its associated LNS each manage and maintain the state of their L2TPv2 connection.

L2TPv2 Encapsulation

Figure 2: L2TPv2 encapsulation: PPP frame encapsulated within L2TP frame within tunneling packet



Managed L2TPv2 Tunnels Messaging

L2TP has two types of messages; control messages and data messages. Control messages are used for tunnel establishment, tunnel maintenance and session management. Data messages are used to encapsulate PPP frames.

- Control messages constitute communication between the LAC and LNS. The control messages are ‘in-band’ in that they use the same packet transport that is used for data packets. The data within the control messages is carried as a series of AVPs.
- An AVP (Attribute Value Pair) is a variable length concatenation of an attribute ID and an associated value for the attribute. Multiple AVPs make up control messages that are used in the establishment, maintenance and teardown of L2TP tunnels.
- Some control messages contain no AVPs. These ‘empty’ messages are called ZLB (Zero Length Body) messages, so these are L2TP control packet with only an L2TP header. ZLB messages are used for acknowledging other control messages.

Control message types

There are two sets of LAC-LNS Control messages:

- The messages that control L2TP tunnels (Table 1)
- The messages that control L2TP calls (sessions) within a tunnel (Table 2)

Table 1: LAC-LNS tunnel (control channel) connection management messages that are used to establish, clear, and maintain L2TP tunnels

MESSAGE TYPE	MESSAGE NAME
1 (SCCRQ)	Start-Control-Connection-Request
2 (SCCRP)	Start-Control-Connection-Reply
3 (SCCRN)	Start-Control-Connection-Connected
4 (StopCCN)	Stop-Control-Connection-Notification.

Table 2: LAC-LNS session or call management messages that are used to establish, clear, and maintain L2TP calls (sessions) within the tunnels

MESSAGE TYPE	MESSAGE NAME
10 (ICRQ)	Incoming-Call-Request
11 (ICRP)	Incoming-Call-Reply
12 (ICCN)	Incoming-Call-Connected
14 (CDN)	Call-Disconnect-Notify.

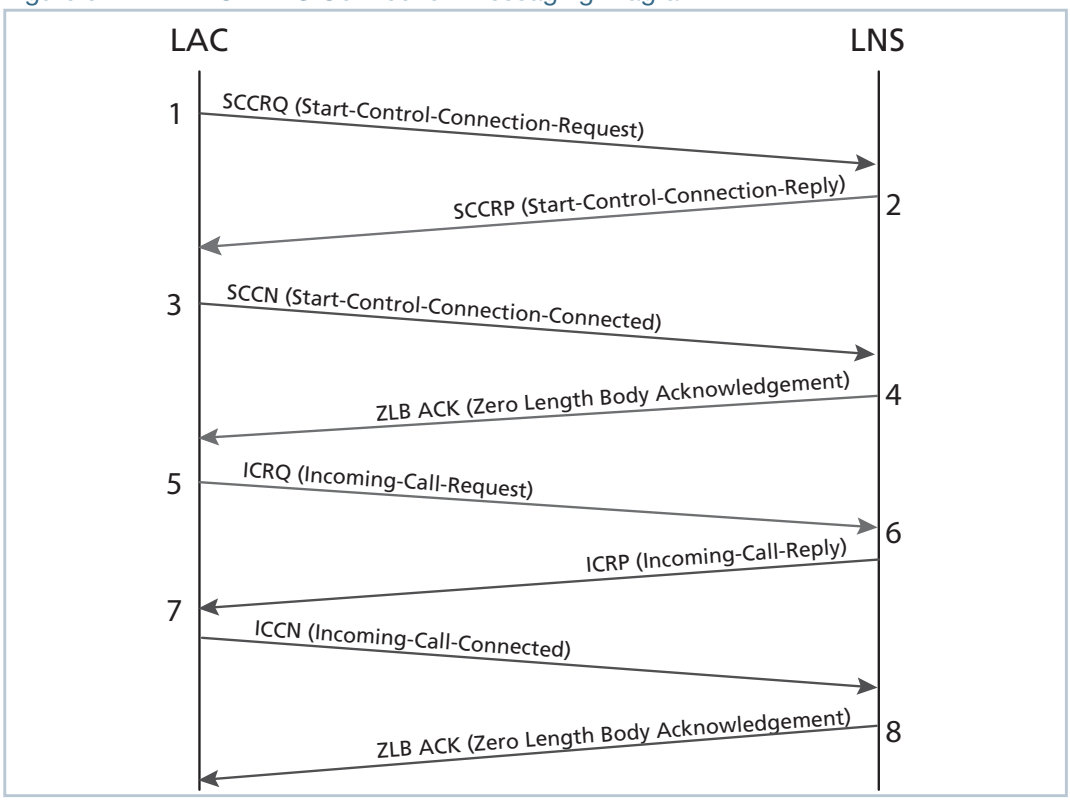
For LAC-LNS messaging sequence when establishing an L2TP connection, see Figure 3 on page 8.

L2TPv2 Connection Sequence

The sequence for a typical successful L2TP connection between the LAC and the LNS is listed below. See "Managed L2TPv2 Tunnels Messaging" on page 6 for a description of the message types.

1. The LAC sends an SCCRQ (Start-Control-Connection-Request) message to the LNS. AVPs (Attribute Value Pairs) are included in this message.
2. The LNS responds to the LAC with an SCCRP (Start-Control-Connection-Reply) message. The response to the LAC challenge and AVPs are included with this message.
3. The LAC sends an SCCN (Start-Control-Connection-Connected) message to the LNS.
4. The LNS responds to the LAC with a ZLB ACK (Zero Length Body Acknowledgement) message. The ZLB ACK message may be in another message. The L2TP tunnel is now up.
5. The LAC sends an ICRQ (Incoming-Call-Request) message to the LNS.
6. The LNS responds to the LAC with an ICRP (Incoming-Call-Reply) message.
7. The LAC send an ICCN (Incoming-Call-Connected) message to the LNS.
8. The LNS responds to the LAC with a ZLB ACK (Zero Length Body Acknowledgement) message. The ZLB ACK message may be in another message. The L2TP session is now up.
9. PPP negotiation can now begin after both the L2TP tunnel and the L2TP session are up.

Figure 3: L2TP LAC - LNS Connection Messaging Diagram



Operation of the L2TP LAC

As previously discussed, the LAC can transport one or more PPP client sessions inside an L2TP tunnel to an LNS device. In fact, a given LAC can connect to multiple LNSs. So different PPP connections being tunneled by the LAC can be tunneled to different LNSs.

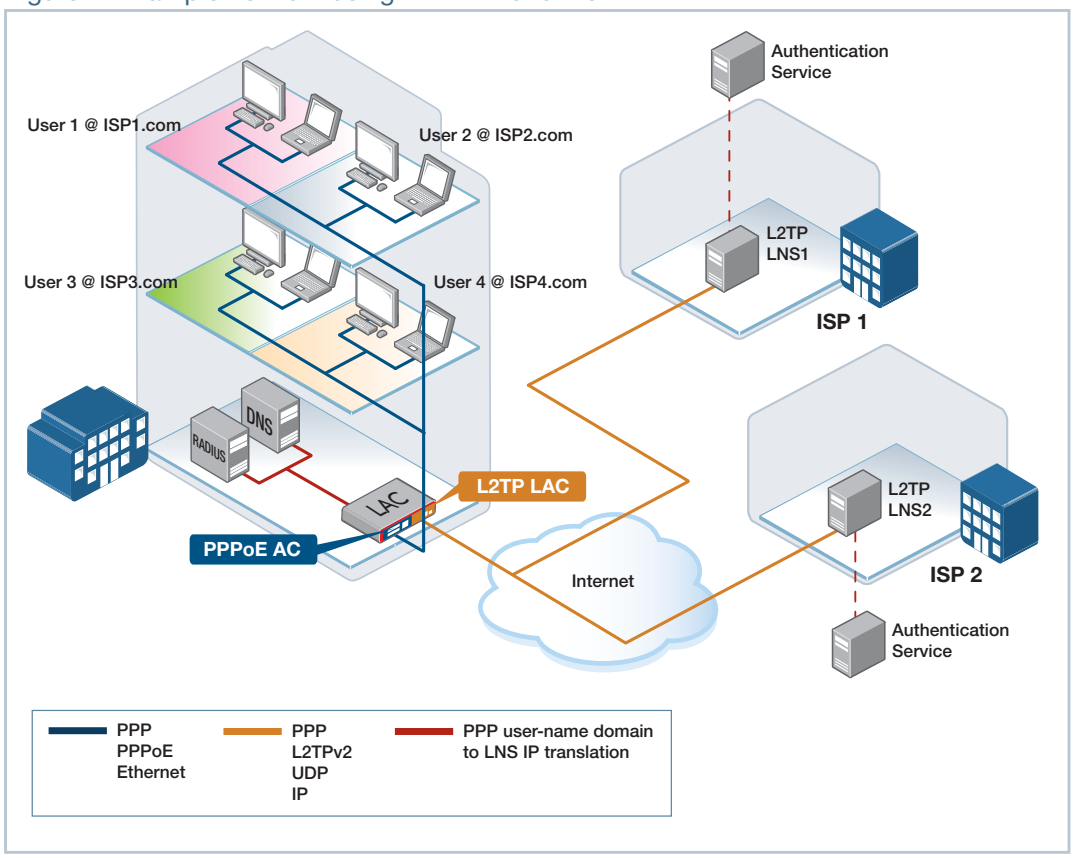
The LAC determines the target IP address of the LNS for each PPP's tunnel via one of several methods:

- By statically configuring the IP address of the LNS.
- By using the domain information extracted from each PPP client session and performing DNS lookup.
- By using the domain information extracted from each PPP client session and performing RADIUS lookup.

When a client PPP session arrives at the LNS device, the LNS extracts it from the L2TP tunnel and fully terminates and authenticates it. The ISP managing the LNS typically allocates an Internet IP address to the client PPP interface from its own database.

In the diagram below, multiple clients who wish to connect to different ISPs create PPPoE connections to the same LAC. By extracting the domain credentials from the users' sessions, the LAC determines the LNS to which to tunnel each user's PPP connection.

Figure 4: Example network using L2TPv2 to tunnel PPP

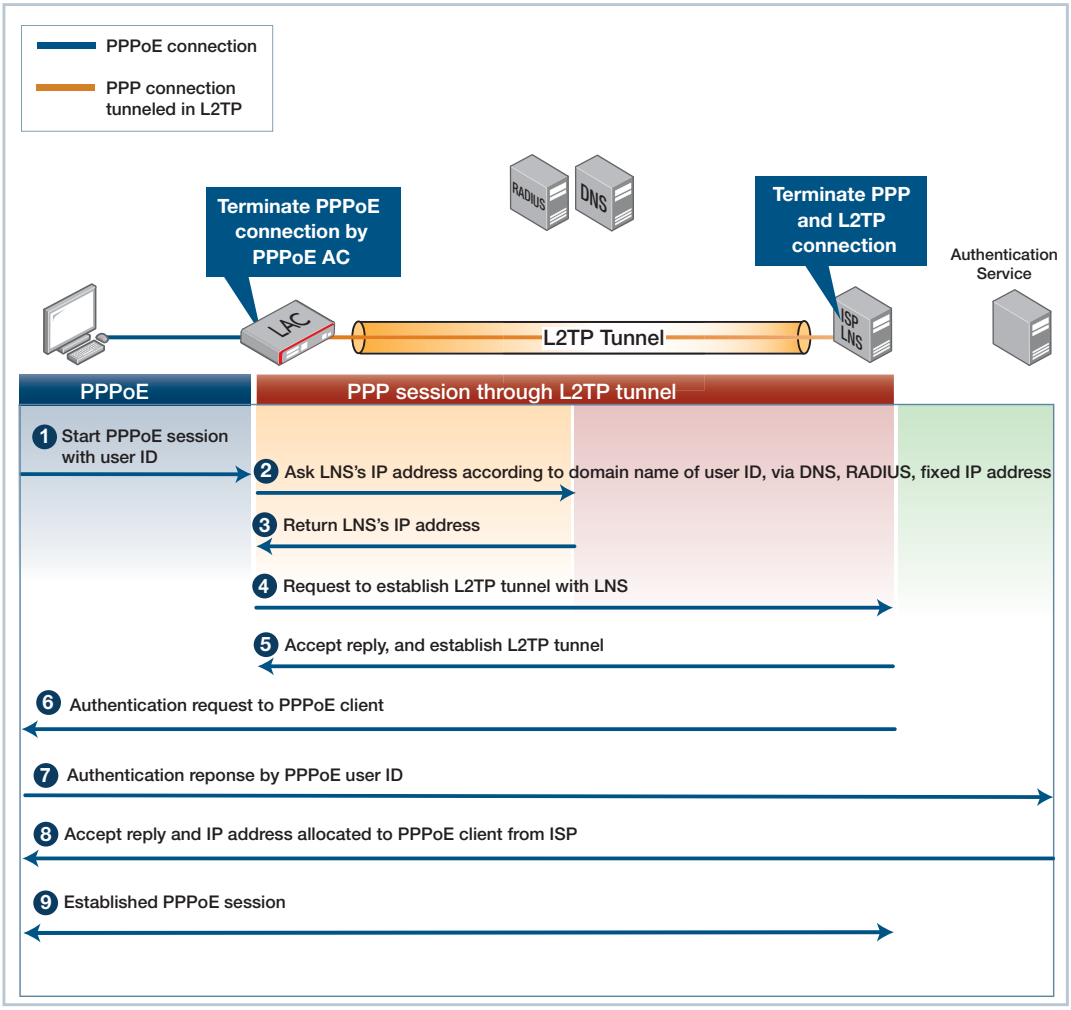


Process of Establishing an L2TP Tunnel for PPP

The purpose of L2TP tunneling is to form an end-to-end PPP connection that is terminated at one end by a client and at the other end by an LNS. A common scenario is for home-user clients connecting via PPP to an LNS at an ISP's premises. The AR-series Firewall can provide the PPPoE Access Concentrator and the L2TP LAC that work together to take the client's PPPoE connection, and tunnel it through to an LNS.

The sequence of events involved in establishing the connection from the home user through to the LNS are illustrated in Figure 5 below.

Figure 5: Establishing an L2TPv2 tunnel for PPP



Note that the PPP connection is established between the client and the LNS.

The process of establishing such a connection using L2TP tunneling of PPPoE is transparent to the PPP client, and is as follows:

1. The client initiates a PPP connection over PPPoE to the LAC—the AR-series firewall that is acting as the PPPoE Access Concentrator and L2TP LAC.
2. The LAC requests the IP address of the ISP's L2TP Network Server (LNS) from static configuration or by RADIUS or DNS lookup. This is the address of the LNS that will terminate the PPP session.

3. The DNS or RADIUS server returns the IP address of the LNS.
4. Once the LAC gets the IP address to the LNS, it acts as an L2TP LAC, and sends a request to the LNS to establish an L2TP tunnel. The authentication for the tunnel will depend on the setting of the ‘shared-secret’. When shared-secret is given, authentication mode is set to challenge; when shared-secret is not given, authentication mode is set to none.

   If the LAC issues an EAP or CHAP challenge, the name field for the challenge will be populated with a dummy name (see more explanation of this in "Details of the L2TPv2 Implementation on the AR-Series Firewall" on page 12).

   The L2TPv2 Vendor name AVP will be populated with text identifying the vendor (this is described some more in "Details of the L2TPv2 Implementation on the AR-Series Firewall" on page 12).

   If the LNS address was determined by RADIUS or DNS query, the LAC packages up the PPP information it learned from PPPoE initiation packets via the partial termination. It passes this information to the LNS as a 'proxy auth’ pair via the ICCN message.
5. The LNS replies and establishes the L2TP tunnel to the LAC.
6. In establishing the L2TPv2 tunnel (after DNS or RADIUS lookup) the L2TPv2 ICCN message will be populated with PPP Proxy Auth AVPs [Attribute-Value Pairs] filled with information from the already partially terminated client PPP sessions (for instance challenge and response for CHAP). The LNS should be configured to use those AVPs to take over the PPP link establishment itself and in doing so authenticate (by which ever means it chooses) the PPP client. This will be on by default and will support CHAP, PAP and EAP.
7. The LNS requests PPP authentication from it’s authentication service.
8. The authentication service authenticates the PPP client and allocates an IP address to the PPP client.
9. The PPP client, the LAC and the LNS have now formed an end-to-end PPP connection. The client packages data into PPP frames that it sends over PPPoE to the LAC, which then strips the PPPoE layer and forwards the contained PPP packets through the L2TP tunnel to the ISP’s LNS.

Details of the L2TPv2 Implementation on the AR-Series Firewall

The functionality of L2TPv2 that is supported on your device is implemented as defined in RFC 2661, ‘Layer Two Tunneling Protocol (L2TPv2)’. Your device can act as an L2TPv2 LAC, but not as an LNS.

- By default, connections are established via the control channel using UDP destination port 1701.
- Up to 256 concurrent PPP sessions are supported across L2TPv2 tunnels.
- Up to 6 concurrent L2TPv2 LAC to LNS tunnels are supported.
- If the method for determining the LNS IP address uses either DNS or RADIUS lookups, the PPP user-name must be in the format ‘user@domain.com’.
- If the LAC issues an EAP or CHAP challenge, the name field for the challenge will be populated with the text 'Allied Telesis'.
- The L2TPv2 Vendor name AVP will be populated with the text ‘Allied Telesis Inc’.

PPPoE Access Concentrator (AC)

As described above, the AR-series Firewall acts as a PPPoE access concentrator, to enable clients to establish a PPPoE session that is ultimately tunneled through to the LNS.

It is common for clients to access the Internet via a PPPoE connection. You can think of a PPPoE Access Concentrator (AC) as a possible termination point of one or more PPPoE client sessions.

The AR-series firewall PPPoE Access Concentrator (AC) can terminate multiple incoming PPPoE client connections and tunnel their PPP sessions via the L2TP LAC to one or more remote L2TP LNS devices.

The user typically configures each PPPoE client with both:

- a PPPoE service-name to connect to a PPPoE Access Concentrator
- a PPP user ID in the format of username@domain, e.g. john@ISP1.com, to allow authentication.

The PPPoE AC needs to be configured with a matching service name. The PPPoE AC on the AR-series Firewall can temporarily terminate and extract the domain portion information from each client PPP session. It uses the domain information to determine which ISP each client wishes to connect to via an L2TP tunnel.

The AR-series Firewall only supports operating as a PPPoE AC for the purposes of tunneling PPP client sessions to a remote ISP via L2TP; it cannot operate as a fully functional PPPoE access concentrator.

DNS and RADIUS

The LAC can be configured to use DNS or RADIUS lookup to get the IP address of the LNS.

DNS

If DNS lookup is configured, the LAC partially terminates the PPP session from the client to retrieve the user-name of the session. For a PPP user-name of, for instance, user@domain.com, the LAC extracts the 'domain.com' portion and prefixes it with a configurable string, such as ‘lns’. This string can be can be configured by the command **l2tp peer-address dns-lookup prefix <*string*>**. It sends this in a DNS request to the DNS server, which sends back the IP address of the LNS.

RADIUS

If RADIUS lookup is configured, the LAC again partially terminates the PPP session from the client to retrieve the user-name of the session. For a PPP user-name of, for instance, user@domain.com, the LAC extracts the 'domain.com' portion. It then sends an Access-Request packet to the RADIUS server with parameters: User-Name=domain.com,User-Password=’password’.

The RADIUS server responds by sending an Access-Accept packet back to the LAC with the IPv4 address of the LNS contained in Framed-IP-Address format (e.g. 192.168.11.2). Note that the RADIUS server is doing no authentication in this process.

Configuration

This section describes what needs to be configured for L2TPv2 tunneling of PPPoE, followed by configuration procedures for:

- "Example 1: Tunneling PPPoE connections with a static L2TP LNS address" on page 15
- "Example 2: Tunneling PPPoE Connections with L2TP LNS address found by RADIUS lookup" on page 16
- "Example 3: Tunneling PPPoE connections with L2TP LNS address found by DNS lookup" on page 18

To configure the device as a PPPoE client, see the ‘Configuring PPPoE’ section in the Point-to-Point Protocol (PPP) Feature Overview and Configuration Guide.

L2TPv2 Connections

To configure L2TPv2, the following must be configured:

Create and configure an L2TP profile (**l2tp-profile** command), give it a name and specify for the profile:

- the shared secret used to authenticate the LNS (**shared-secret** command)
- the RADIUS group to use if an LNS address is to be found by RADIUS (**server** command)
- the DNS server to query if an LNS address is to be found be DNS (**ip name-server** command)

PPPoE Access Concentrator

To configure the PPPoE AC, create a PPPoE AC instance (**pppoe-ac** command), give it a name, and specify:

- the service name for the clients to use in order to connect to this instance, if desired (the service name can be left unspecified as **any**), and whether it is to advertise the service-name (**service-name** command)
- that the PPP packets from the client will be sent to L2TP (**destination** command)
- the name of the L2TP profile to which it will send PPP packets from this client (**l2tp profile** command)
- how the LNS address is to be determined—
  DNS (**l2tp peer-address dns-lookup prefix** command)
  RADIUS (**l2tp peer-address radius-lookup group** command)
  or static (**l2tp peer-address static** command)

Example 1: Tunneling PPPoE connections with a static L2TP LNS address

Table 3: Configuration example 1: Tunneling PPPoE connections with a static L2TP LNS address

Step 1. Configure the PPPoE service.	
`awplus#` `configure terminal`	Enter Configuration mode.
`awplus(config)#` `pppoe-ac mylittleac`	Create and name the PPPoE AC instance and enter PPPoE AC Configuration mode.

`awplus(config-pppoe-ac)#` `service-name any`
or
`awplus(config-pppoe-ac)#` `service-name remote-office`
	Set the service name for the PPPoE client to connect to. Either:
	■ To set the service to allow the client to connect without checking the service-name tag from the client, use **service-name any**; or
	■ To set the PPPoE AC service to only accept connections when the service-tag in the client packets match the a particular service name, specify the **service-name**.

`awplus(config-pppoe-ac)#` `service-name remote-office advertised`	Specify **advertised** if the service name is to be advertised, or omit if it is not to be advertised.
`awplus(config-pppoe-ac)#` `destination l2tp`	Configure the PPPoE service to use L2TP for its destination.
`awplus(config-pppoe-ac)#` `l2tp peer-address static 192.168.11.2`	Assign a static IP address for the L2TP peer. This is the address of the LNS that will terminate the L2TP tunnel and the PPP session.
`awplus(config-pppoe-ac)#` `l2tp profile my-l2tp-profile1`	Specify the L2TP profile used to tunnel this PPPoE service. This is the L2TP profile created by the **l2tp-profile** command.
`awplus#` `exit`	Leave PPPoE AC Configuration mode.
Step 2. Configure the L2TP tunnel.	
`awplus(config)#` `l2tp-profile my-l2tp-profile1`	Create the L2TP profile and enter L2TP Profile Configuration mode.
`awplusawplus(config-l2tp-profile)#` `shared-secret oursecret`	Configure the shared secret for this L2TP tunnel. The ISP must configure the same shared secret on the LNS for this tunnel.
`awplus#` `exit`	Leave L2TP Profile Configuration mode.
Step 3. Configure the interface.	
`awplus(config)#` `int eth1`	Enter Interface Configuration mode for the interface.

Table 3: Configuration example 1: Tunneling PPPoE connections with a static L2TP LNS address

`awplus(config-if)#` `pppoe-ac-service mylittleac`	Configure the interface to use the PPPoE AC service, so that PPPoE packets arriving on this interface will be processed by this PPPoE AC instance.

Example 2: Tunneling PPPoE Connections with L2TP LNS address found by RADIUS lookup

Table 4: Configuration example 2: Tunneling PPPoE Connections with L2TP LNS address found by RADIUS lookup

Step 1. **Configure the PPPoE service.**	
`awplus#` `configure terminal`	Enter Configuration mode.
`awplus(config)#` `pppoe-ac mylittleac`	Create and name the PPPoE AC instance and enter PPPoE AC configuration mode.

`awplus(config-pppoe-ac)#`
`service-name any`
or
`awplus(config-pppoe-ac)#`
`service-name remote-office`
	Set the service name for the PPPoE client to connect to. Either:
	■ To set the service to allow the client to connect without checking the service-name tag from the client, use **service-name any**; or
	■ To set the PPPoE AC service to only accept connections when the service-tag in the client packets match the a particular service name, specify the **service-name**.

`awplus(config-pppoe-ac)#` `service-name remote-office advertised`	Specify **advertised** if the service name is to be advertised, or omit if it is not to be advertised.
`awplus(config-pppoe-ac)#` `destination l2tp`	Configure the PPPoE service to use L2TP for its destination.
`awplus(config-pppoe-ac)#` `l2tp peer-address radius-lookup group my_group`	Set the PPPoE AC service to use RADIUS lookup to get the address of the LNS. Specify the name of the RADIUS group. With this setting, when the PPPoE AC service uses RADIUS lookup a PPP user-name of, for instance, user@domain.com will first have the 'domain.com' portion extracted. An Access-Request packet is sent to the RADIUS server with User-Name=domain.com,User-Password='password'. An Access-Accept packet is expected back with the IPv4 address of the LNS contained in Framed-IP-Address format (e.g. 192.168.11.2). This is the address of the LNS that will terminate the L2TP tunnel and the PPP session.

Table 4: Configuration example 2: Tunneling PPPoE Connections with L2TP LNS address found by RADIUS lookup (continued)

`awplus(config-pppoe-ac)#` `l2tp profile my-l2tp-profile1`	Specify the L2TP profile used to tunnel this PPPoE AC service.
`awplus#` `exit`	Leave PPPoE AC configuration mode.
Step 2. Configure the L2TP tunnel.	
`awplus(config)#` `l2tp-profile my-l2tp-profile1`	Create an L2TP profile for the tunnel and enter the configuration mode.
`awplusawplus(config-l2tp-profile)#` `shared-secret oursecret`	Configure the shared secret for this L2TP tunnel. The ISP must configure the same shared secret on the LNS for this tunnel.
`awplus#` `exit`	Leave L2TP Profile Configuration mode.
Step 3. Configure the LAC to use RADIUS.	
`awplus(config)#` `radius-server host 192.168.1.200 key testing123-1`	Specify the address and key for the RADIUS server.
`awplus(config)#` `aaa group server radius my_group`	Create a RADIUS group. This is the group referred to in the **l2tp peer-address radius-lookup group** command above.
`awplus(config-sg)#` `server 192.168.1.200`	Add the address of the RADIUS server group.
`awplus#` `exit`	Leave RADIUS Server Group Configuration mode.
Step 4. Configure the Ethernet interface.	
`awplus(config)#` `int eth1`	Enter Interface Configuration mode for the interface.
`awplus(config-if)#` `pppoe-ac-service mylittleac`	Configure the interface to use the PPPoE AC service, so that PPPoE packets arriving on this interface will be processed by this PPPoE AC instance.

Example 3: Tunneling PPPoE connections with L2TP LNS address found by DNS lookup

Table 5: Configuration example 3: Tunneling PPPoE connections with L2TP LNS address found by DNS lookup

Step 1. Configure the PPPoE service.	
`awplus#` `configure terminal`	Enter Configuration mode.
`awplus(config)#` `pppoe-ac mylittleac`	Create and name the PPPoE AC instance and enter PPPoE AC configuration mode.

`awplus(config-pppoe-ac)#`
`service-name any`
or
`awplus(config-pppoe-ac)#`
`service-name remote-office`
	Set the service name for the PPPoE client to connect to. Either:
	■ To set the service to allow the client to connect without checking the service-name tag from the client, use **service-name any**; or
	■ To set the PPPoE AC service to only accept connections when the service-tag in the client packets match the a particular service name, specify the **service-name**.

`awplus(config-pppoe-ac)#` `service-name remote-office advertised`	Specify **advertised** if the service name is to be advertised, or omit if it is not to be advertised.
`awplus(config-pppoe-ac)#` `destination l2tp`	Configure the PPPoE service to use L2TP for its destination.
`awplus(config-pppoe-ac)#` `l2tp peer-address dns-lookup prefix lns`	Set the PPPoE AC to use DNS lookup to get the IP address of the destination LNS. For a PPP user-name of, for instance, user@domain.com, the 'domain.com' portion will first be extracted, prefixed with 'lns.' to become 'lns.domain.com'. This is sent to the DNS server, which sends back the LNS address to use. This is the address of the LNS that will terminate the PPP session.
`awplus(config-pppoe-ac)#` `l2tp profile my-l2tp-profile1`	Specify the L2TP profile used to tunnel this PPPoE service.
`awplus#` `exit`	Leave PPPoE AC Configuration mode.
Step 2. Configure the L2TP tunnel.	
`awplus(config)#` `l2tp-profile my-l2tp-profile1`	Create and name the L2TP profile.
`awplusawplus(config-l2tp-profile)#` `shared-secret oursecret`	Configure the shared secret for this L2TP tunnel. The ISP must configure the same shared secret on the LNS for this tunnel.

Table 5: Configuration example 3: Tunneling PPPoE connections with L2TP LNS address found by DNS lookup (continued)

`awplus#` `exit`	Leave L2TP Profile Configuration mode.
Step 3. Configure the LAC to use DNS.	
`awplus(config)#` `ip name-server 10.1.1.1`	Specify the address of the DNS server from which to look up the LNS address.
Step 4. Configure the Ethernet interface.	
`awplus(config)#` `int eth1`	Enter Interface Configuration mode for the interface.
`awplus(config-if)#` `pppoe-ac-service mylittleac`	Configure the interface to use the PPPoE AC service, so that PPPoE packets arriving on this interface will be processed by this PPPoE AC instance.

Monitoring and Debugging

Show commands

show pppoe-ac connections

To display all PPPoE Access Concentrator (AC) connections for all routes, use the command:

```
awplus# show pppoe-ac connections
```

This will show the connections from clients and the tunnels into which these connections are being sent.

To display connected PPPoE routes for a particular PPPoE service instance named ‘pppoeservice1’, use the command:

```
awplus# show pppoe-ac pppoeservice1 connections
```

Table 6: Example output from **show pppoe-ac connections**

```
awplus# show pppoe-ac connections

PPPoE Access Concentrator Connection Status

------------------------------------------------------------------------
Route Name:                     pppoeservice-eth1
Route ID:                       29785
Source Information
  Interface:                    eth1
  Session ID:                   14204
  Service Name:                 test
  State:                        Open
  Peer MAC:                     00:00:cd:38:01:4f
Destination Information
  Type:                         L2TP
  Tunnel ID:                    11223
  Session ID:                   57309

Route Name:                     ac1-eth2
Route ID:                       34409
Source Information
  Interface:                    eth2
  Session ID:                   14108
  Service Name:                 my_isp
  State:                        Open
  Peer MAC:                     00:00:cd:38:01:4d
Destination Information
  Type                          L2TP
  Tunnel ID                     47432
  Session ID                    10056
```

show pppoe-ac statistics

To display statistics for the PPPoE access concentrator, use the command:

```
awplus# show pppoe-ac statistics
```

```
awplus# show pppoe-ac statistics

PPPoE Access Concentrator Statistics
Name                                                    Value
-------------------------------------------------------------
lnsLookupSuccessfulRequests                             0
lnsLookupFailedRequests                                 0
lnsLookupDnsFailures                                    0
lnsLookupRadiusFailures                                 0
l2tpTunnelsOpened                                       2
l2tpSessionsOpened                                      2
l2tpSessionsClosed                                      0
l2tpDnsFailures                                         0
pppoePadiReceived                                       2
pppoeInvalidPadi                                        0
pppoePadoSent                                           2
pppoePadsSent                                           2
pppoePadrReceived                                       2
pppoeInvalidPadr                                        0
pppoeResentPadr                                         0
pppoePadtReceived                                       0
pppoeInvalidPadt                                        0
pppoePadtSent                                           0
routesCreated                                           2
routesCreateFail                                        0
routesDeleted                                           0
routesDeleteFail                                        0
routesDstOpenFail                                       0
routesDestCloseFail                                     0
routesSourceCloseFail                                   0
routesClosedByDest                                      0
routesClosedBySource                                    0
```

show pppoe-ac config-check

To display a configuration check for all PPPoE AC service instances, use the command:

```
awplus#show pppoe-ac config-check
```

To display a configuration check for a particular PPPoE AC service instance named ‘ac1’, use the command:

```
awplus#show pppoe-ac ac1 config-check
```

This output indicates whether you have a full and valid configuration for a PPPoE instance, or which configuration still needs to be completed.

```
awplus# show pppoe-ac config-check

PPPoE Access Concentrator ac:
  Incomplete Configuration
  Required: add pppoe-ac-service to one or more interfaces
  Required: destination
  Required: service-name
  Required: l2tp peer-address
  Required: l2tp profile


PPPoE Access Concentrator ac1:
  Incomplete Configuration
  Required: add pppoe-ac-service to one or more interfaces


PPPoE Access Concentrator pppoeservice1:
  Complete Configuration
```

show running-config pppoe-ac

To display the running configuration of PPPoE Access Concentrator, use the command:

```
awplus#show running-config pppoe-ac
```

```
awplus# show running-config pppoe-ac

 pppoe-ac-service ISP-service
  service-name remote-office advertised
  ppp-auth-protocols pap
  destination l2tp
  l2tp peer-address static 192.168.11.2
  l2tp profile PUBLIC
```

show running-config l2tp-profile

To display the running configuration of L2TPv2 tunnel profiles, use the command:

```
awplus#show running-config l2tp-profile
```

```
awplus# show running-config l2tp-profile
l2tp-profile public
 version 2
 secret "my_password"
```

Debugging PPPoE Access Concentrators and L2TPv2 tunnels

To enable debugging for the PPPoE Access Concentrator, use the command:

```
awplus#debug pppoe-ac
```

To disable debugging for the PPPoE Access Concentrator, use the command:

```
awplus#no debug pppoe-ac
```

To see whether debugging of PPPoE AC is enabled or disabled, use the command:

```
awplus#show debugging pppoe ac
```

To enable debugging for dynamic L2TPv2 tunnels, use the command:

```
awplus#debug l2tp dynamic
```

To disable debugging for dynamic L2TPv2 tunnels, use the command:

```
awplus#no debug l2tp dynamic
```

To see whether debugging of dynamic L2TPv2 tunnels is enabled or disabled, use the command:

```
awplus#show debugging l2tp dynamic
```

C613-22085-00 REVB

Allied Telesis™ NETWORK SMARTER

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com