

L2TP Overview..... 1
 Benefits..... 2
 Prerequisites..... 2
 Incoming Call Sequence..... 2

L2TP Overview

With the "Private / Intranet Access" serviced mode, the terminal equipment user's PPP link is relayed through the IWF (PDSN) Server over an L2TP tunnel to a remote L2TP Network Server (LNS), which terminates the PPP link behind a private Intranet firewall (see Figure C on page 10). This allows the user wireless access to services within their private corporate network, or access to a secondary ISP (given that these private networks support L2TP tunnel access).

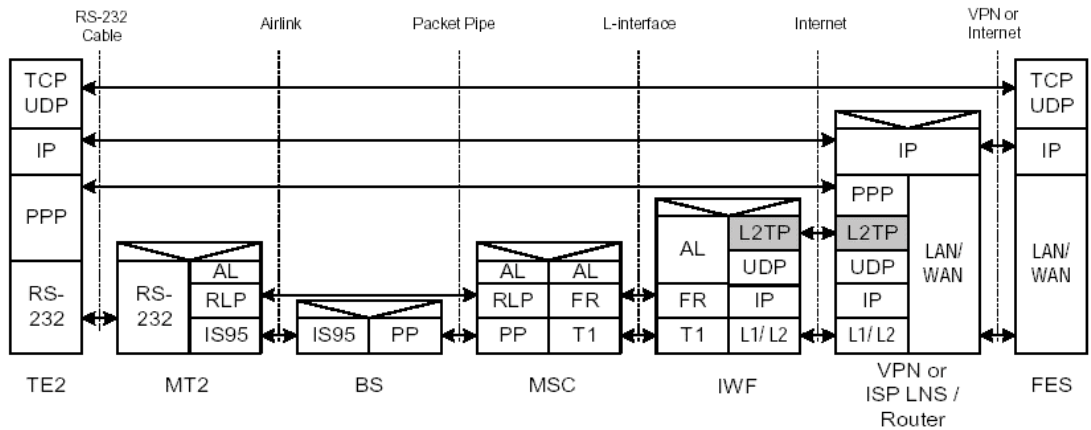
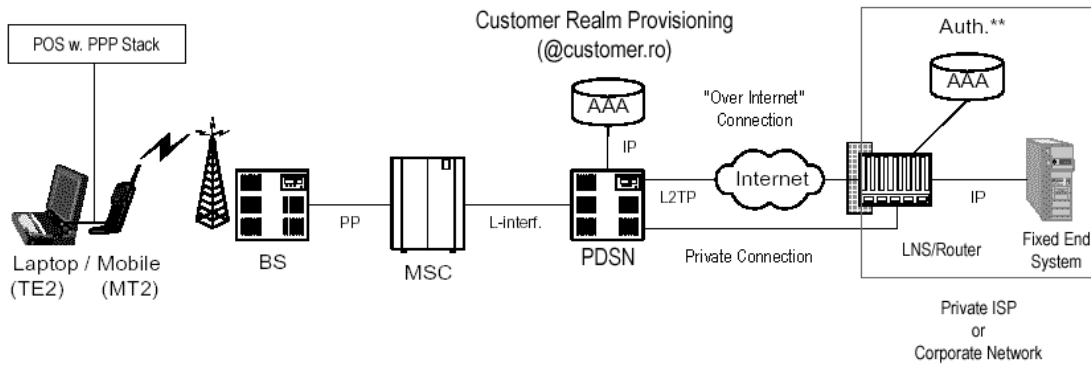


Figure 1

Mobile User shall create a Zapp Connection with username@realm.ro
 IWF verifies the "realm" and redirects the call to the assigned LNS
 "Username" is verified by LNS Router (using its AAA)
 The IP address is assigned by LNS

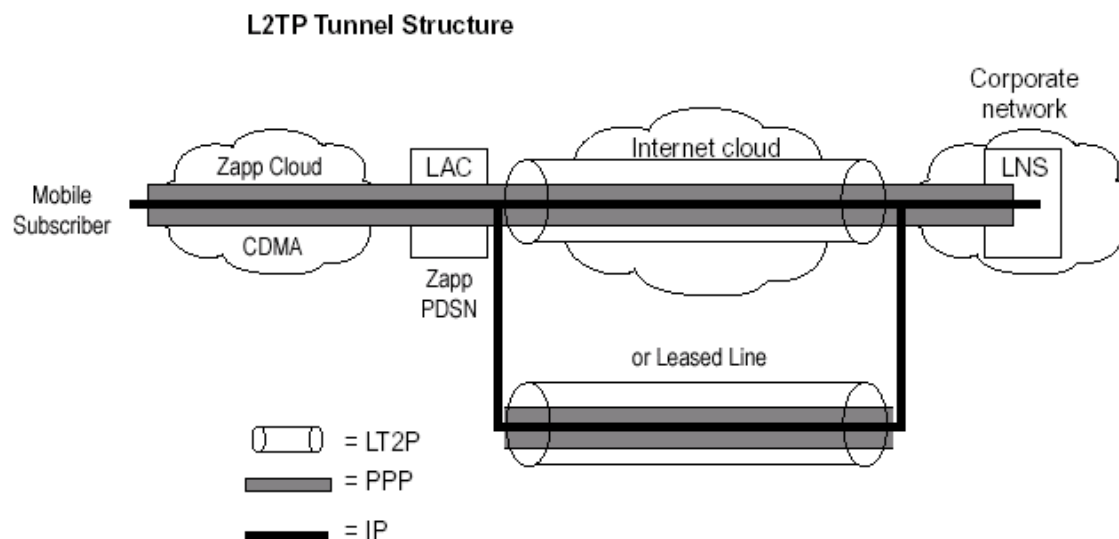


Figure 2

Benefits

L2TP offers the following benefits:

- Vendor interoperability.
- Can be used as part of the wholesale access solution, which allows ISPs to the telco or service providers offer VPNs to Internet Service Providers (ISPs) and other service providers.
- Can be operated as a client initiated VPN solution, where enterprise customers using a PC, can use the client initiated L2TP from a third party.
- Supports Multihop, which enables Multichassis Multilink PPP in multiple home gateways. This allows you to stack home gateways so that they appear as a single entity.

Prerequisites

A router or access server must be using a software image that supports L2TP/VPDN and the hardware platform you are using.

Incoming Call Sequence

A VPDN connection between a remote user, a LAC (in Zapp Network), and the LNS at the home LAN using an L2TP tunnel is accomplished as follows:

- 1 The remote user initiates a PPP connection using a Zapp Device and forwards it to customer LNS.
- 2 The LAC (Zapp PDSN) accepts the connection and the PPP link is established.
- 3 After the end user and LNS negotiate LCP, the LAC partially authenticates the end user with CHAP or PAP. The username, domain name, or DNIS is used to determine whether the user is a VPDN client. If the user is not a VPDN client, authentication continues, and the client will access the Internet or other contacted service. If the username is a VPDN client, the mapping will name a specific endpoint (the LNS).

Technical Support - Data Services

TELEMOBIL SA,
data.services@zapp.ro



4 The tunnel end points, the LAC and the LNS, authenticate each other before any sessions are attempted within a tunnel. Alternatively, the LNS can accept tunnel creation without any tunnel authentication of the LAC.

5 Once the tunnel exists, an L2TP session is created for the end user.

6 The LAC will propagate the LCP negotiated options and the partially authenticated CHAP/PAP information to the LNS. The LNS will funnel the negotiated options and authentication information directly to the virtual access interface. If the options configured on the virtual template interface does not match the negotiated options with the LAC, the connection will fail, and a disconnect is sent to the LAC.

The end result is that the exchange process appears to be between the dial-up client and the remote LNS exclusively, as if no intermediary device (the LAC) is involved. Figure 3 offers a pictorial account of the L2TP incoming call sequence with its own corresponding sequence numbers. the sequence numbers in figure 3 are not related to the sequence numbers described above.

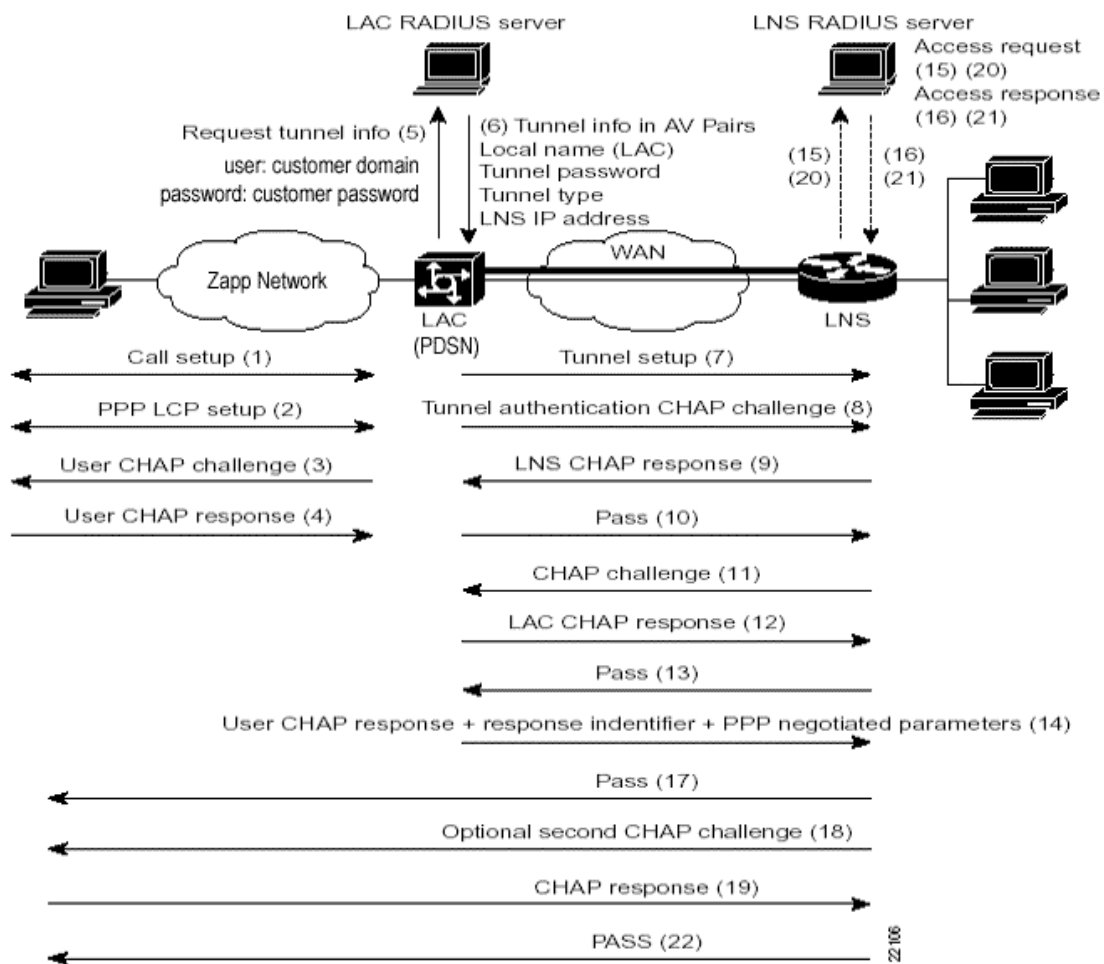


Figure 3