Lw4o6

Overview

Lw4o6 is an extension to the DS-Lite architecture which moves the NAPT44 function to the IPv4/IPv6 client tunnel located in the CPE. It is standardized in RFC7596 (2015)

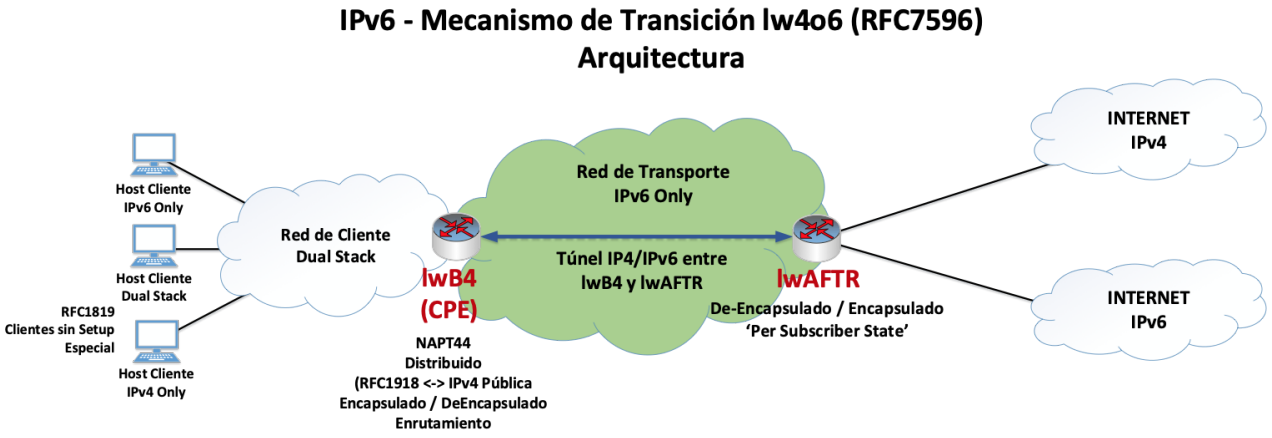
There are two components in the Lw4o6 architecture:

a) **lw4o6:** Lightweight Basic Bridging BroadBand
b) **lwAFTR:** Lightweight Address Family Transition Router

In DS-Lite, NAPT44 (RFC3022) focuses on the AFTR. This function is fully based on maintaining state (per-flow state). NAPT44 can also perform logging functions for the ISP's outgoing connections (in some countries connection logging is a legal requirement).

Lw4o6 provides a solution to the problem of DS-Lite (large processing capacity required for CGNAT and logging) by distributing NAPT44 to the CPEs. Thus, the amount of state information in the lwAFTR is significantly reduced, as this is no longer based on a per-flow model but a rather on a per-subscriber model (significant reduction of lwAFTR use of memory and CPU). In other words, lwAFTR no longer requires CGNAT.

Also, with lw4o6, by delegating and distributing the NAPT44 process to lwB4s, CPEs can share the use of public IPv4 addresses. This is done by allocating port-restricted IPv4 addresses to lwB4 CPEs for TCP and UDP connections. In lw4o6, this is known as address sharing. ICMPv4 traffic from the lwB4 to the Internet is limited. All other technical aspects of lw4o6 operation are the same as in DS-Lite, the mechanism from which it derives.



Technical Characteristics

The main motivation of lw4o6 is to serve as an extension of DS-Lite to improve the NAPT44 process, functionally modifying this process so that it will be distributed at the lwB4 CPE level and optionally allowing different CPEs/lwB4s to use shared public IPv4 addresses, using restricted port set and maintaining the same use of IPv4/IPv6 tunnels over an IPv6-only operator's transport network. lw4o6 eliminates the need for the lwAFTR to perform CGNAT.

- **lwB4 provisioning.** The lwB4 can use different options to obtain its provisioning parameters, such as DHCPv6 Options, manual configuration,
  - IPv4 addressing for the tunnel, taken from the well-known range 192.0.0.0/29
  - IPv6 address after the lwAFTR
  - Public IPv4 for use in NAPT44
  - 'Port Set' restriction for use in NAPT44
  - IPv6 prefix (IPv6 binding prefix) for use in the IPv4/IPv6 tunnel, as origin IPv6. The lwB4 builds the origin IPv6 of the IPv4/IPv6 tunnel based on the assigned IPv6 prefix (/64), the public IPv4 and the assigned 'Port Set ID' (PSID).

- **lwAFTR per-subscriber state.** The lwAFTR must maintain an lwB4 binding table containing the following 3-tuples:
  - IPv6 address for the lwB4
  - Reserved public IPv4 address
  - Restricted port set

This table is used by the lwAFTR for the IPv4-in-IPv6 encapsulation of inbound packets received from each lwB4 and outbound packets to the IPv4 Internet, as well as for the encapsulation of inbound traffic from the IPv4 Internet. The lwAFTR does not perform any kind of NAPT process.

- **Lw4o6 works over an IPv6-only transport network (*details).** DS-Lite uses IPv6-only between the B4 and the AFTR. The use of IPv6-only in the transport network suggests greater efficiency and performance in the core network and L3 switching of the operator (ISP).

Advantages:

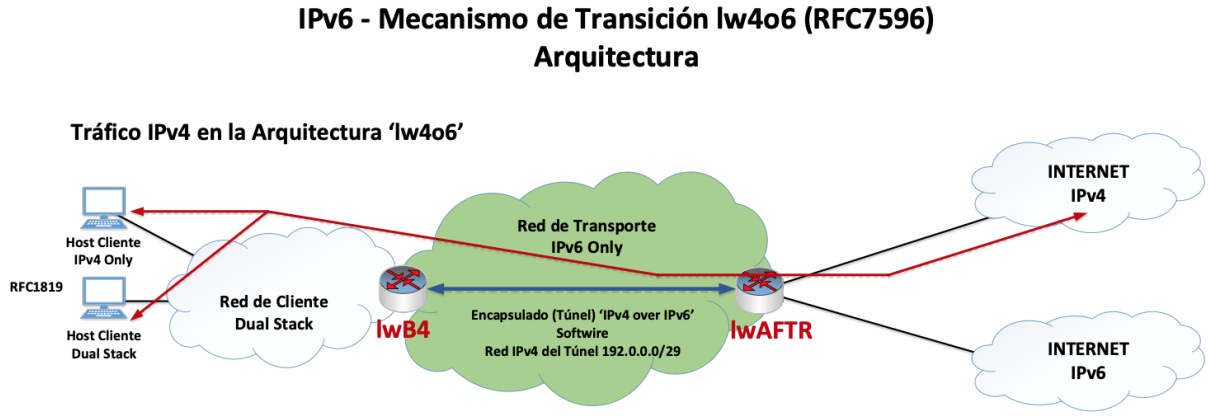
- Does not require adaptations or modifications in dual-stack or IPv4-only customers
- IPv6-only transport network: high efficiency and performance, single protocol stack and management
- Promotes IPv6-only deployment in the ISP's transport network
- Because the transport network is IPv6-only, there are no limitations or need to overlap the addressing of thousands of CPEs/B4s

- Native IPv6 traffic is neither translated nor encapsulated
- Support for all protocol types using unicast traffic
- Automatic provisioning of lwB4 with DHCPv6 options
- Adaptations have no impact on the operator's IPv6 addressing
- Does not require CGNAT in the lwAFTR
- Better performance than DS-Lite, as NAPT is distributed

Disadvantages:

- Overhead in the transport network due to the IPv4/IPv6 tunnel encapsulation between lwB4 and lwAFTR
- Does not support multicast traffic
- May require CPE update to support lwB4
- Does not solve the problem of IPv4 exhaustion
- Does not support IPv4 mesh networks layered over the ISP's transport network
- Not designed for mobile cellular networks
- IPv4/IPv6 encapsulation in the IPv6-only transport network adds some complexity to DPI in the operator's network

IPv4 Traffic in the lw4o6 Architecture

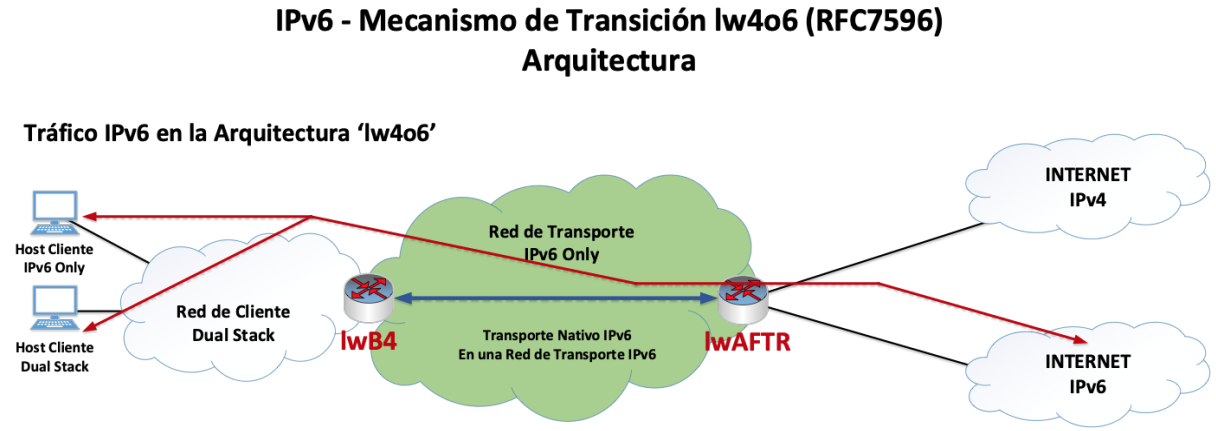


Details:

- IPv4-only or dual-stack clients direct and forward IPv4 traffic to the lwB4, which can be directly connected or routed to the client's network. Clients use either static addressing or DHCPv4. Clients can use the lwB4 as DNS.
- The lwB4 then activates NAPT44, using the public IPv4 address and the restricted port set. It then encapsulates (tunnels) IPv4 packets in IPv6.
- The lwB4 routes and sends the IPv6 packets towards the lwAFTR, which can be either directly connected or routed.
- The lwAFTR extracts the IPv4 packets from the IPv6 packets according to the Per-Subscriber Table and proceeds to route the packets to the IPv4 Internet.

- Inbound traffic to the IPv4 Internet is processed similarly, reversing the order of the steps:
  IPv4 Internet >> lwAFTR >> IPv6-only network >> lwB4 >> IPv4 end client

IPv6 Traffic in the lw4o6 Architecture



Details:

- IPv6-only or dual-stack clients' IPv6-only traffic is directly and natively routed through the lwB4 CPE, the operator's IPv6-only transport network, and the lwAFTR, without undergoing any type of encapsulation or translation process other than routing.