Содержание

PPPoL2TP configuration and commands

L2TP (Layer 2 Tunneling Protocol) is a protocol for tunneling level 2 traffic through a level 3 network. L2TP is used to provide tunneling of the PPP (Point-to-Point Protocol) in your network.

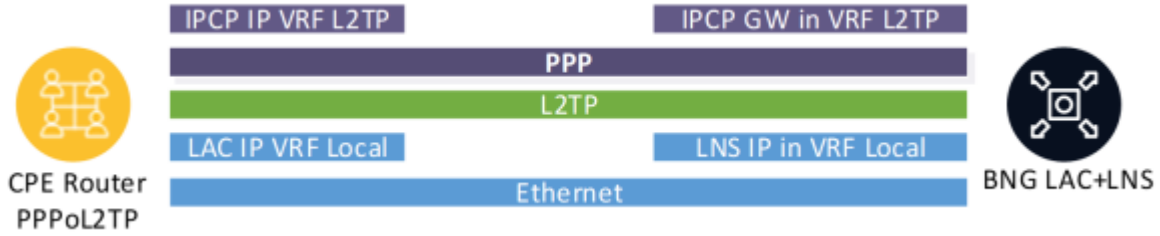
L2TP operation requires a LAC (L2TP access concentrator) and a LNS (L2TP network server). The LNS is one of the endpoints of the L2TP tunnel. The LAC, configured on the access device, receives packets from the remote client and forwards them to the LNS in the remote network. The LAC and LNS are peers.

Implementation features:

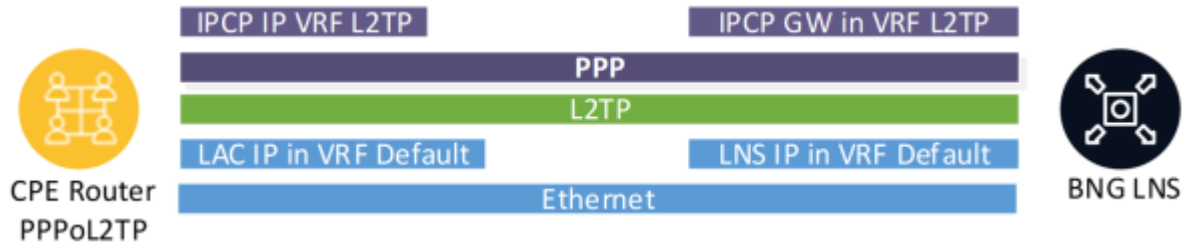
1. L2TPv2 is supported
2. Since the subscriber acts as the concentrator (LAC), one tunnel is established between the subscriber and the LNS (SSG L2TP server), containing exactly one PPP session.
3. Transport for L2TP is IPv4 only (IPv6 is not planned)
4. No authorization is required when establishing an L2TP connection (tunnel): the BRAS LNS establishes an L2TP tunnel with any initiator; to establish an L2TP tunnel, the initiator (acting as LAC) does not use a password, BRAS does not check the initiator's name and does not require a password for the L2TP tunnel.

From the BRAS perspective, there are two types of L2TP subscribers. Subscribers are assigned a local BRAS IP for L2TP establishment:

1. A PPPoL2TP subscriber obtains an IP address via DHCP on the current BRAS and initiates L2TP with the current BRAS.



2. A PPPoL2TP subscriber obtains an IP address via DHCP on a remote BRAS and initiates L2TP with the current BRAS.



Parameters:

Parameter	Description	Default Value and Possible Values
`bras_l2tp_enable`	Enabling BRAS L2TP (PPPoL2TP) functionality. Note: the `bras_enable` option must be enabled. Requires restart	

Parameter	Description	Default Value and Possible Values
`bras_l2tp_max_retransmit`	Maximum number of CTL message retransmits (RFC 2661 p.5.8). If no acknowledgment is received for any retransmit — the tunnel is closed (as inactive). Does not require restart	Default value — 5
`bras_l2tp_mru`	Maximum size of a PPP packet encapsulated in L2TP. If an MTU is not explicitly set for the L2TP server — the value of the `bras_l2tp_mru` option is used. ℹ Parameter can be configured at the LNS server level via CLI	Default value — 1460
`bras_l2tp_ratelimit`	Control of the number of requests from a subscriber to open an L2TP tunnel/session per second (L2TP spam prevention). Does not require restart	0 — control disabled (default value)
`bras_l2tp_ratelimit_ban`	Ban time for a subscriber when `bras_l2tp_ratelimit` is exceeded, in seconds. Does not require restart	When control mode bras_l2tp_ratelimit is enabled (bras_l2tp_ratelimit != 0), this parameter must be set to a value other than 0
`bras_l2tp_min_lifetime`	Minimum tunnel lifetime, seconds. A subscriber can create new tunnels no more frequently than once every `bras_l2tp_min_lifetime` seconds (spam protection). Does not require restart	Default value: 2 0 — no restrictions
`bras_l2tp_default_vrf`	Default VRF name in which L2TP servers are announced. VRF can be set individually for each L2TP server. If a VRF is not explicitly set for a server — the VRF specified in this option is used. Does not require restart. ℹ Parameter can be configured at the LNS server level via CLI	
`ajb_save_ip`	Recording L2TP packets in pcap is set by the ajb_save_ip parameter. It can specify: - The subscriber's IP address for the L2TP tunnel, all traffic for this subscriber will be recorded; - The L2TP server's IP address: in this case, all data exchange with this server will be recorded in pcap. More details about the parameter in the section Трассировка fastDPI BRAS L2 ℹ Parameter can be configured at the LNS server level via CLI	

Parameter	Description	Default Value and Possible Values
`allowed-mark`	Added the ability to specify for which subnets L2TP tunnels can be created. As usual, subnets are specified via AS (files `aslocal.bin` and `asnum.dscp`); among AS flags, only `mark3` is allowed. In the L2TP server properties, using the `allowed-mark` parameter, the flag number (1, 2, or 3) is specified, which will be the sign allowing the establishment of L2TP tunnels for this AS. Example of setting AS flag `mark2`: l2tp server modify 78.107.11.103 allowed-mark=2 By default, an LNS does not have the allowed-mark property, meaning tunnels are allowed to be created for all IPs. To remove the allowed-mark property from an LNS, specify allowed-mark=0: `l2tp server modify 78.107.11.103 allowed-mark=0` After this, this L2TP server will create tunnels for any subscriber. That is, the general algorithm for specifying ACL for an LNS server is as follows: 1. Choose the `mark3` flag that we will use as the ACL label. Only the `mark3` flag is used to avoid collision with marking for other purposes 2. Mark in `asnum.dscp` the autonomous systems for allowed subnets with this flag (see Общая настройка BRAS для L2/L3 режимов) 3. Using the CLI command, set the LNS server property `allowed-mark` equal to the flag number ⓘ Parameter can be configured at the LNS server level via CLI	

CLI Commands:

Command	Description
`l2tp server add IP <props>`	Adding a new L2TP server
`l2tp server modify IP <props>`	Modifying properties of an already set L2TP server
`l2tp server delete IP`	Deleting an L2TP server
`l2tp show [all|IP]`	Viewing L2TP server properties
`l2tp stat [all|IP]`	Viewing L2TP server statistics
`l2tp term`	Termination of all L2TP sessions. It is possible to specify parameters `ip`, `mac`, `subs_id`, `login` or `all`: `l2tp term [hard] [ip=X | mac=X | subs_id=X | login=X | all]`

LNS Statistics

Display statistics:

```
fdpi_cli l2tp server stat <IP>
```

Example output:

```
        invalid session type: 0
           session not found: 13
            bad L2TP version: 0
        malformed ctl packet: 0
          too complex packet: 0
     unknown mandatory attr: 0
    unsupported ctl message: 0
     unexpected ctl message: 2
               out of order: 0
        window size exceeded: 0
   too many unconfirmed msg: 0
   subs IP/tid/sid mismatch: 0
      malformed data packet: 0
         too frequent SCCRQ: 0
             rate-limit ban: 0
           AS access denied: 0
              MTU exhausted: 0
   ctl retransmit exhausted: 0
              FSM violation: 0
                      TOTAL: 15
```

Output parameter descriptions:

1. `invalid session type` — Session found in PPP DB by l2subs_id is not an L2TP session
2. `session not found` — Session not found in PPP DB by l2subs_id
3. `bad L2TP version` — Unsupported L2TP version
4. `malformed ctl packet` — Erroneous ctl packet (does not comply with RFC)
5. `too complex packet` — Too complex packet - too many attributes
6. `unknown mandatory attr` — Unknown mandatory attribute
7. `unsupported ctl message` — Unsupported ctl packet
8. `unexpected ctl message` — Ctl packet not supported in current state
9. `out of order` — Ctl packet order violation
10. `window size exceeded` — Violation of our window size
11. `too many unconfirmed msg` — Too many unconfirmed ctl messages for the session
12. `subs IP/tid/sid mismatch` — Error: subscriber IP, or L2TP tunnel/session id does not match those remembered in the session
13. `malformed data packet` — Erroneous data packet
14. `too frequent SCCRQ` — Too frequent L2TP tunnel recreation
15. `rate-limit ban` — Ratelimit exceeded
16. `AS access denied` — Denial of L2TP session creation for the subnet (⇒ for AS)
17. `MTU exhausted` — MTU (snaplen) exceeded when processing an incoming packet
18. `ctl retransmit exhausted` — Number of sessions closed due to exhaustion of ctl message

retransmits

19. `FSM violation` — State machine violation