Содержание

Настройка PPPoL2TP и команды

L2TP (Layer 2 Tunneling Protocol) — протокол для туннелирования трафика уровня 2 через сеть уровня 3. L2TP используется для обеспечения туннелирования протокола PPP (Point-to-Point Protocol, «точка-точка») в вашей сети.

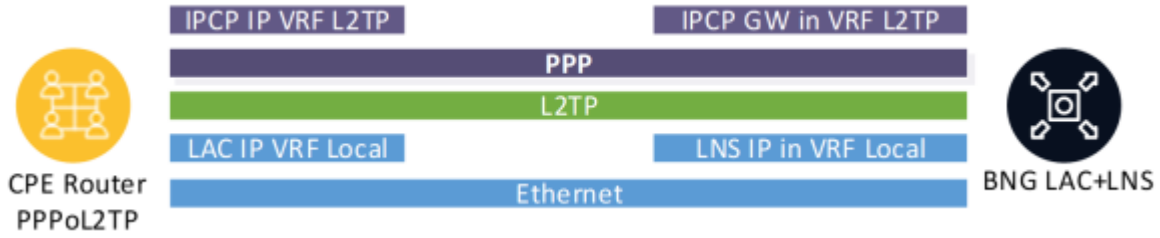
Для работы L2TP требуется LAC (L2TP access concentrator, концентратор доступа L2TP) и LNS (L2TP network server, сетевой сервер L2TP). LNS является одной из конечных точек туннеля L2TP. LAC, настроенный на устройстве доступа, получает пакеты от удаленного клиента и пересылает их на LNS в удаленной сети. LAC и LNS являются одноранговыми.

Особенности реализации:

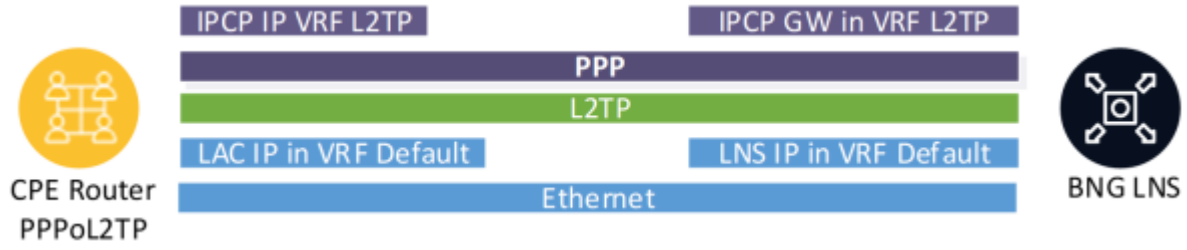
1. Поддерживается L2TPv2
2. Так как абонент выступает в роли концентратора (LAC), то между абонентом и LNS (L2TP-сервером СКАТ) устанавливается один туннель, в нем ровно одна PPP сессия.
3. Транспорт для L2TP - только IPv4 (IPv6 не планируется)
4. При первоначальной установке L2TP-соединения (туннеля) аутентификация на уровне L2TP не требуется: BRAS LNS устанавливает L2TP-туннель с любым инициатором (LAC), не проверяет имя инициатора и не запрашивает пароль для самого L2TP-туннеля. При этом логин и пароль абонента передаются далее в RADIUS в рамках PPP-сессии. Таким образом, для установления туннеля логин и пароль не нужны, но для дальнейшей работы L2TP и авторизации абонента передача логина и пароля обязательна и они должны быть заданы в настройках абонента.

С точки зрения BRAS, есть два типа L2TP абонентов. Абонентам выдан IP локального BRAS для установки L2TP:

1. Абонент PPPoL2TP получает IP-адрес по DHCP на текущем BRAS и поднимает L2TP с текущим BRAS.



2. Абонент PPPoL2TP получает IP-адрес по DHCP на удаленном BRAS и поднимает L2TP с текущим BRAS.



Параметры:

Параметр	**Описание**	**Значение по умолчанию и возможные значения**
`bras_l2tp_enable`	Включение функциональности BRAS L2TP (PPPoL2TP). Примечание: опция `bras_enable` должна быть включена. Требует перезапуска	
`bras_l2tp_max_retransmit`	Максимальное число ретрансмитов CTL-сообщений (RFC 2661 p.5.8). Если не получили подтверждения приема ни на один ретрансмит — туннель закрывается (как неактивный). Не требует перезапуска	Значение по умолчанию — 5
`bras_l2tp_mru`	Максимальный размер PPP-пакета, инкапсулированного в L2TP. Если для L2TP-сервера явно не задан MTU — используется значение опции `bras_l2tp_mru`. ⓘ Параметр может настраиваться на уровне LNS сервера через CLI	Значение по умолчанию — 1462
`bras_l2tp_ratelimit`	Контроль количества запросов от абонента на открытие L2TP-туннеля/сессии в секунду (предотвращение L2TP-спама). Не требует перезапуска	0 — контроль отключен (значение по умолчанию)
`bras_l2tp_ratelimit_ban`	Время бана абонента при превышении `bras_l2tp_ratelimit`, в секундах. Не требует перезапуска	При включенном режиме контроля bras_l2tp_ratelimit (bras_l2tp_ratelimit != 0) этот параметр должен быть задан отличным от 0
`bras_l2tp_min_lifetime`	Минимальное время жизни туннеля, секунд. Абонент может создавать новые туннели не чаще, чем раз в `bras_l2tp_min_lifetime` секунд (защита от спама). Не требует перезапуска	Значение по умолчанию: 2 0 — без ограничений
`bras_l2tp_default_vrf`	Имя VRF по умолчанию, в котором анонсируются L2TP-сервера. VRF может быть задана индивидуально для каждого L2TP-сервера. Если для сервера явно не задан VRF — используется VRF, заданный в этой опции. Не требует перезапуска. ⓘ Параметр может настраиваться на уровне LNS сервера через CLI	

Параметр	Описание	Значение по умолчанию и возможные значения
ajb_save_ip	Запись L2TP-пакетов в pcap задается параметром ajb_save_ip. В нем можно указать: - IP-адрес абонента для L2TP-туннеля, будет записываться весь трафик для данного абонента; - IP-адрес L2TP-сервера: в этом случае в pcap будет записываться весь обмен данными с этим сервером. Подробнее про параметр в разделе Трассировка fastDPI BRAS L2 ℹ Параметр может настраиваться на уровне LNS сервера через CLI	

Параметр	Описание	Значение по умолчанию и возможные значения
`allowed-mark`	Добавлена возможность указывать, для каких подсетей можно создавать L2TP-туннели. Как обычно, подсети указываются через AS (файлы `aslocal.bin` и `asnum.dscp`); среди флагов AS разрешено только `mark3`. В свойствах L2TP-сервера с помощью параметра `allowed-mark` указывается номер флага (1, 2 или 3), который будет признаком разрешения устанавливать L2TP-туннели для этой AS. Пример задания флага AS `mark2`: l2tp server modify 78.107.11.103 allowed-mark=2 По умолчанию, у LNS нет свойства allowed-mark, то есть разрешено создавать туннели для всех IP. Чтобы удалить у LNS свойство allowed-mark, нужно указать allowed-mark=0: `l2tp server modify 78.107.11.103 allowed-mark=0` После этого данный L2TP-сервер будет создавать туннели для любого абонента. То есть общий алгоритм указания ACL для LNS-сервера таков: 1. Выбираем флаг `mark3`, который мы будем использовать как метку ACL. Используется только флаг `mark3` во избежание коллизии с маркировкой для других целей 2. Помечаем в `asnum.dscp` автономные системы для разрешенных подсетей этим флагом (см. Общая настройка BRAS для L2/L3 режимов) 3. CLI-командой задаем LNS-серверу свойство `allowed-mark`, равное номеру флага ℹ Параметр может настраиваться на уровне LNS сервера через CLI	

CLI-команды:

Команда	Описание
`l2tp server add IP <props>`	Добавление нового L2TP-сервера
`l2tp server modify IP <props>`	Изменение свойств уже заданного L2TP-сервера
`l2tp server delete IP`	Удаление L2TP-сервера
`l2tp server show [all|IP]`	Просмотр свойств L2TP-серверов
`l2tp server stat [all|IP]`	Просмотр статистики L2TP-серверов

Команда	Описание
`l2tp term`	Закрытие всех L2TP-сессий. Есть возможность указать параметры `ip`, `mac`, `subs_id`, `login` или `all`: `l2tp term [hard] [ip=X | mac=X | subs_id=X | login=X | all]`

Статистика LNS

Вывести статистику:

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

Пример вывода:

```
        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
```

Описание параметров вывода:

1. `invalid session type` — Найденная в PPP DB по l2subs_id сессия не является L2TP-сессией
2. `session not found` — Сессия не найдена в PPP DB по l2subs_id
3. `bad L2TP version` — Неподдерживаемая версия L2TP
4. `malformed ctl packet` — Ошибочный ctl-пакет (не соответствует RFC)
5. `too complex packet` — Слишком сложный пакет - слишком много атрибутов
6. `unknown mandatory attr` — Неизвестный обязательный атрибут
7. `unsupported ctl message` — Неподдерживаемый ctl-пакет
8. `unexpected ctl message` — В текущем состоянии ctl-пакет не поддерживается
9. `out of order` — Нарушен порядок ctl-пакетов
10. `window size exceeded` — Нарушение размера нашего окна
11. `too many unconfirmed msg` — Слишком много неподтвержденных ctl msg у сессии
12. `subs IP/tid/sid mismatch` — Ошибка: IP абонента, или L2TP tunnel/session is не

совпадает с теми, что запомнены в сессии
13. `malformed data packet` — Ошибочный data-пакет
14. `too frequent SCCRQ` — Слишком частое пересоздание L2TP-туннеля
15. `rate-limit ban` — Превышение ratelimit
16. `AS access denied` — Запрет создания L2TP-сессий для подсети (⇒ для AS)
17. `MTU exhausted` — Превышение MTU (snaplen) при поступлении пакета на обработку
18. `ctl retransmit exhausted` — Число закрытых сессий из-за исчерпания ретрансмитов ctl-сообщений
19. `FSM violation` — Нарушение state machine