



зелёная точка
смотри. слушай. говори

РЕЗЕРВИРОВАНИЕ L3 И L2 КАНАЛОВ ЧЕРЕЗ СТОРОННИЙ ИНТЕРНЕТ

с помощью

MikroTik

Владимир Кузнецов

MUM Moscow 2019





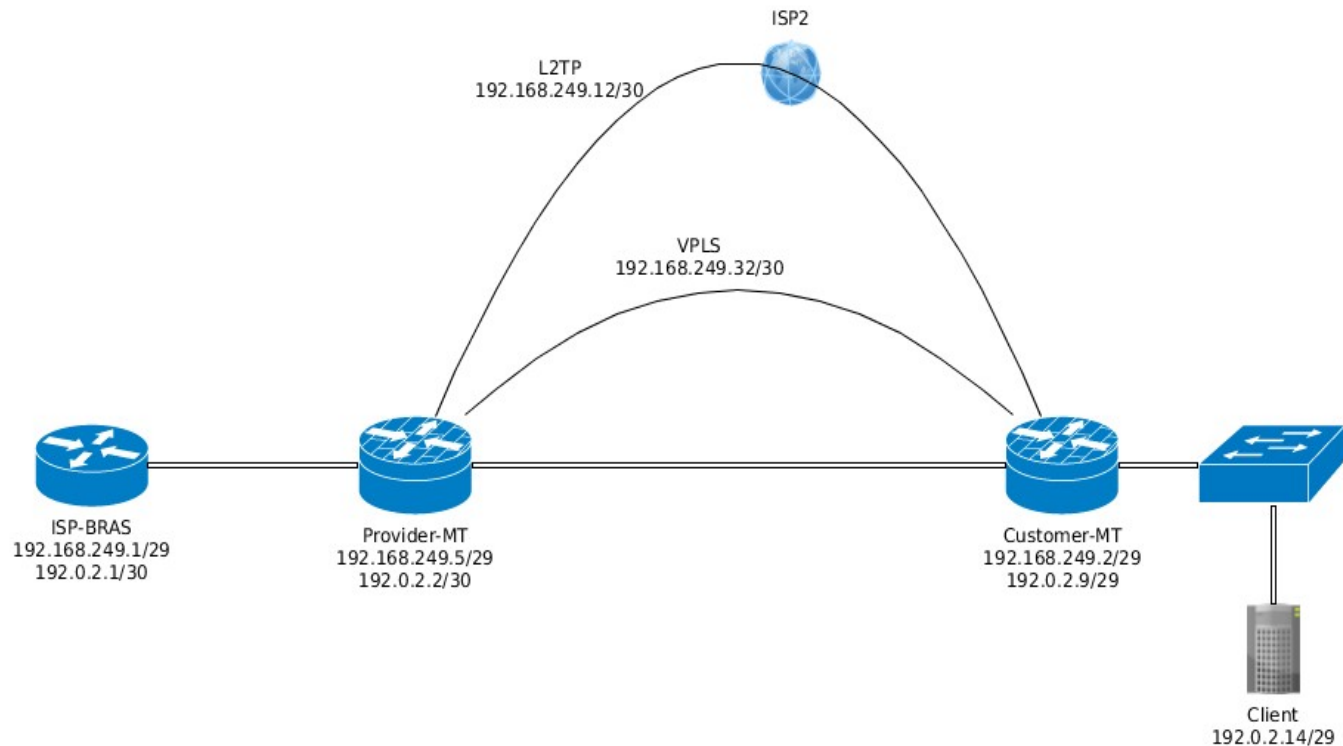
Обо мне

- Владимир Кузнецов smithy1208@gmail.com
- Россия, Липецк
- Ведущий инженер службы сети передачи данных
- ООО “Зеленая точка Липецк” <https://lipetsk.zelenaya.net>
- MTCNA 1905NA3454
- 10 лет опыта сетевого администрирования в ISP
- Канал в телеграмм <https://t.me/miktrain> (MikroTik-Training.ru)

О чём презентация

- Cisco ip sla
- L2TP
- OSPF
- VPLS (MPLS, LDP)

Схема





Описание

Клиент получает от провайдера сети с публичными IP (L3) и несколько vlan (L2) и хочет иметь резерв через “чужой” интернет.

Сети небольшие ($< /24$), поэтому без BGP.



Решение:

Разместить у провайдера MikroTik.

- Между роутером провайдера (Cisco ISP-BRAS), Provider-MT и Customer-MT есть канал L2 (192.168.249.0/29). Настраиваем ip sla таким образом, что если доступен канал L2, сети клиента маршрутизируем в него (на Customer-MT). Если L2 канал недоступен, то сети клиента маршрутизируем на Provider-MT.
- На Provider-MT должны быть маршруты в сторону сетей клиента.
- На Customer-MT должен быть **default gateway** в сторону ISP1

Таким образом L3 сети клиента зарезервированы.



Резервирование L2VPN

- Через резервного провайдера построен L2TP (накручиваем MRRU=1508).
- Настроен OSPF для автоматического резервирования через L2 канал и L2TP. Приоритет на канал L2. OSPF бонусом анонсирует нам нужные сети (и **default**).
- Поверх этого включаем MPLS и поднимаем VPLS, таким образом с помощью **bridge** мы обеспечим резервирование L2VPN (vlans).



Configuration 1-1. Links. Provider-MT

```
/interface bridge
```

```
add name=br-lo0
```

```
/ip address
```

```
add address=192.168.249.9/32 interface=br-lo0
```

```
add address=192.168.249.5/29 interface=vlan3029
```

```
/interface l2tp-server server set enabled=yes mrru=1508
```

```
/interface l2tp-server add name=l2tp-ppp2 user=ppp2
```

```
/ppp secret add local-address=192.168.249.13 name=ppp2 password=123 remote-address=192.168.249.14
```



Configuration 1-1. Links. Customer-MT

```
/interface bridge
```

```
add name=br-lo0
```

```
/ip address
```

```
add address=192.0.2.9/29 interface=ether4
```

```
add address=192.168.249.2/29 interface=vlan3029
```

```
add address=192.168.249.10/32 interface=br-lo0
```

```
/interface l2tp-client
```

```
add connect-to=10.7.2.1 disabled=no mrru=1508 name=l2tp-ppp2 password=123 user=ppp2
```



Configuration 1-2. OSPF. Provider-MT

```
/routing ospf instance
```

```
set [ find default=yes ] distribute-default=if-installed-as-type-1 router-id=192.168.249.9
```

```
/routing ospf interface
```

```
add cost=10 interface=vlan3029 network-type=broadcast
```

```
add cost=20 interface=l2tp-ppp2 network-type=point-to-point
```

```
/routing ospf network
```

```
add area=backbone network=192.168.249.0/28
```



Configuration 1-2. OSPF. Customer-MT

```
/routing ospf instance
```

```
set [ find default=yes ] router-id=192.168.249.10
```

```
/routing ospf interface
```

```
add cost=10 interface=vlan3029 network-type=broadcast
```

```
add cost=20 interface=l2tp-ppp2 network-type=point-to-point
```

```
/routing ospf network
```

```
add area=backbone network=192.168.249.0/28
```

```
add area=backbone network=192.0.2.8/29
```



Configuration 1-3. MPLS. Provider-MT

```
/mpls ldp
```

```
set enabled=yes lsr-id=192.168.249.9 transport-address=192.168.249.9
```

```
/mpls ldp interface
```

```
add interface=vlan3029
```

```
add interface=l2tp-ppp2
```

```
/interface vpls
```

```
add disabled=no name=vpls1 remote-peer=192.168.249.10 vpls-id=0:0
```



Configuration 1-3. MPLS. Customer-MT

```
/mpls ldp
```

```
set enabled=yes lsr-id=192.168.249.10 transport-address=192.168.249.10
```

```
/mpls ldp interface
```

```
add interface=ether1
```

```
add interface=l2tp-ppp2
```

```
/interface vpls
```

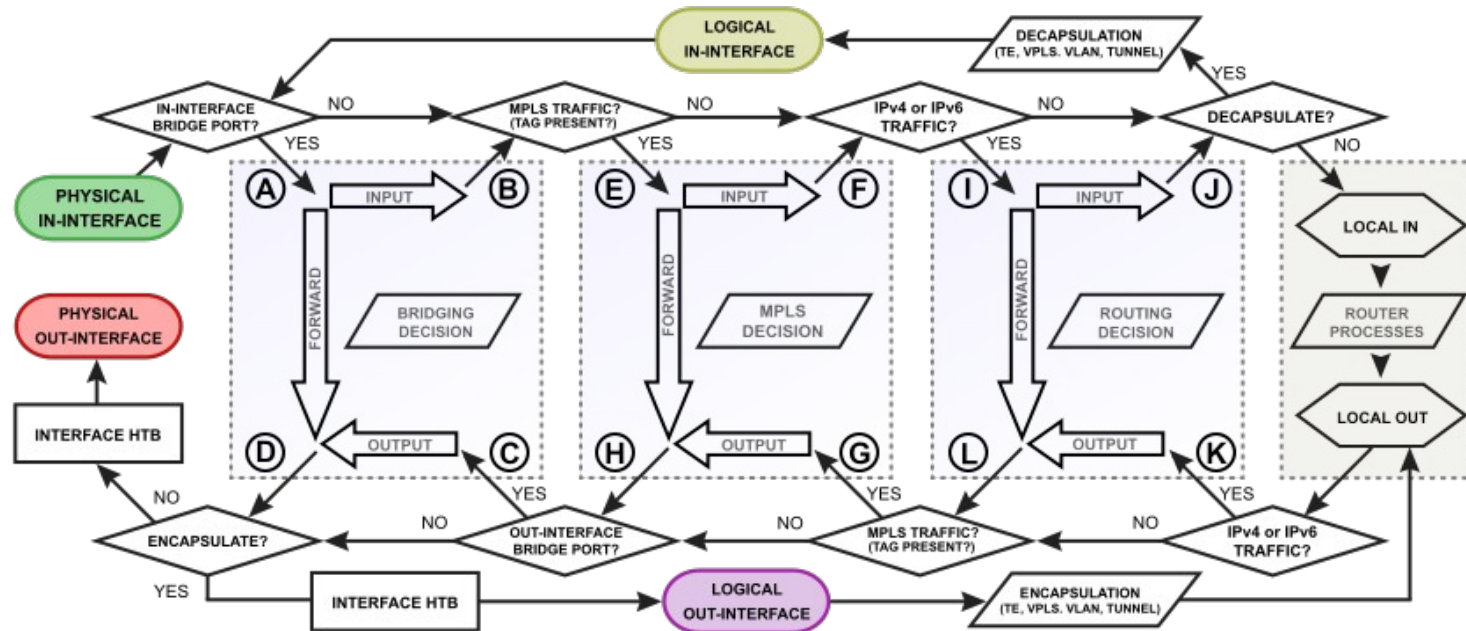
```
add disabled=no name=vpls1 remote-peer=192.168.249.9 vpls-id=0:0
```



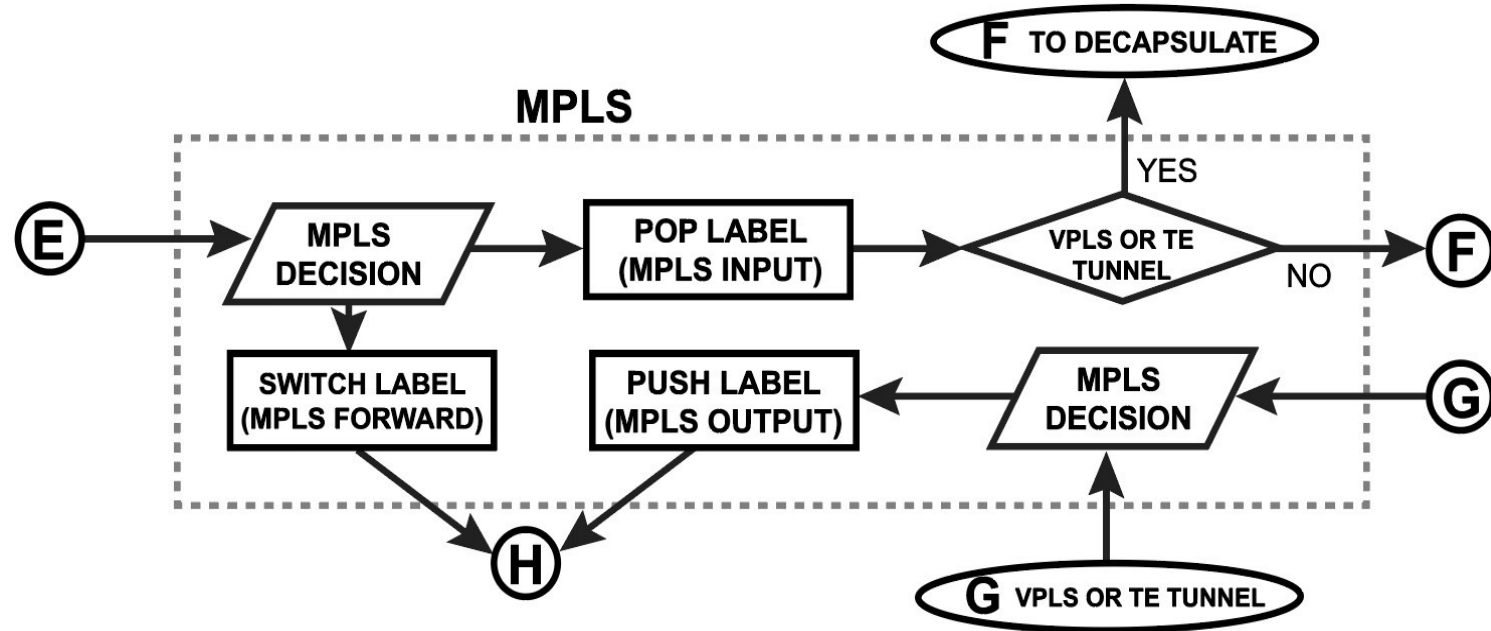
Почему VPLS, а не EoIP?

- Потому что в MPLS действий с пакетом меньше (ставим/снимаем/меняем метку), что выглядит рациональным.

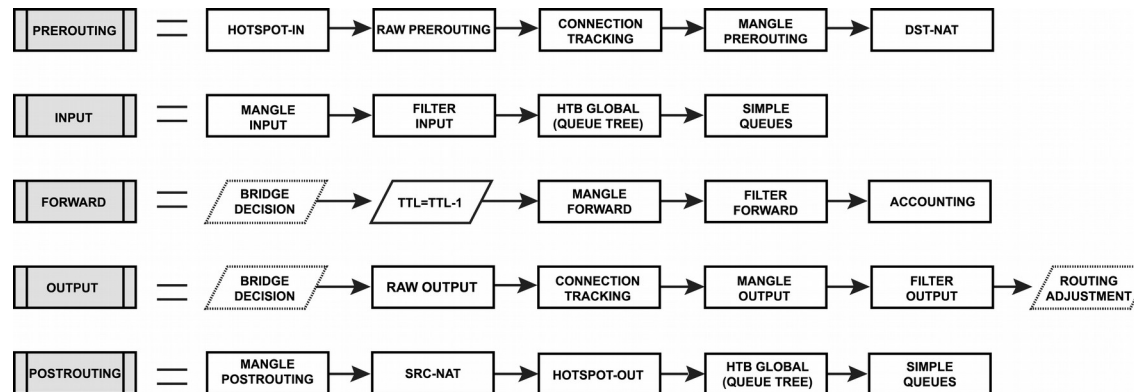
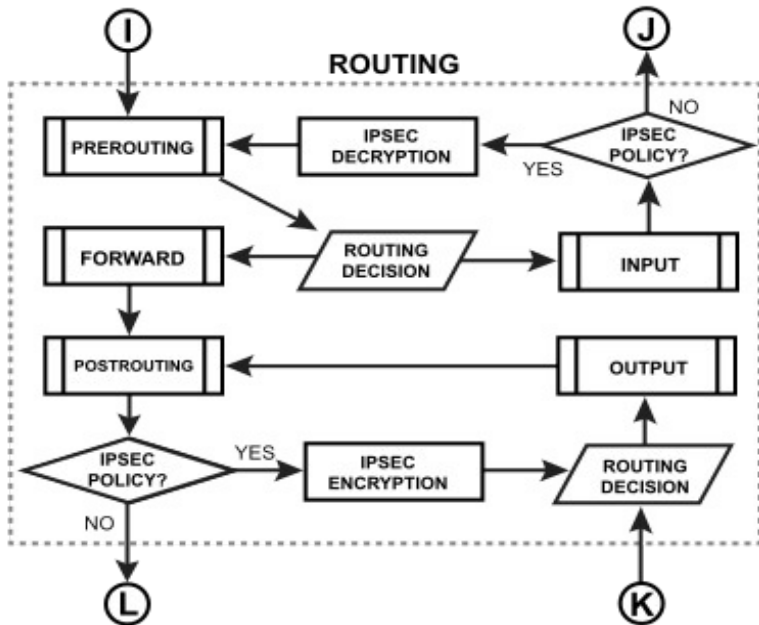
Packet Flow Diagram v6



MPLS DECISION



ROUTING DECISION





Configuration 1-4. Vlans. Provider-MT

```
/interface bridge
```

```
add name=br-MAIN protocol-mode=none vlan-filtering=yes admin-mac=50:00:00:03:00:01 auto-mac=no
```

```
/interface bridge port
```

```
add bridge=br-MAIN interface=ether1
```

```
add bridge=br-MAIN interface=ether2
```

```
add bridge=br-MAIN interface=vpls1
```

```
/interface bridge vlan
```

```
add bridge=br-MAIN tagged=br-MAIN,ether1,ether2 vlan-ids=3029
```

```
add bridge=br-MAIN tagged=br-MAIN,ether1 vlan-ids=3030
```

```
add bridge=br-MAIN tagged=ether1,vpls1 vlan-ids=691,2019
```

v.kuznetsov@lipetsk.zelenaya.net MUM Moscow 2019



Configuration 1-4. Vlans. Customer-MT

```
/interface bridge
```

```
add name=br-VPN protocol-mode=none vlan-filtering=yes admin-mac=50:00:00:04:00:04 auto-mac=no
```

```
/interface bridge port
```

```
add bridge=br-VPN interface=vpls1
```

```
add bridge=br-VPN interface=ether5
```

```
/interface bridge vlan
```

```
add bridge=br-VPN tagged=vpls1,ether5 vlan-ids=691
```

```
add bridge=br-VPN tagged=vpls1,ether5 vlan-ids=2019
```



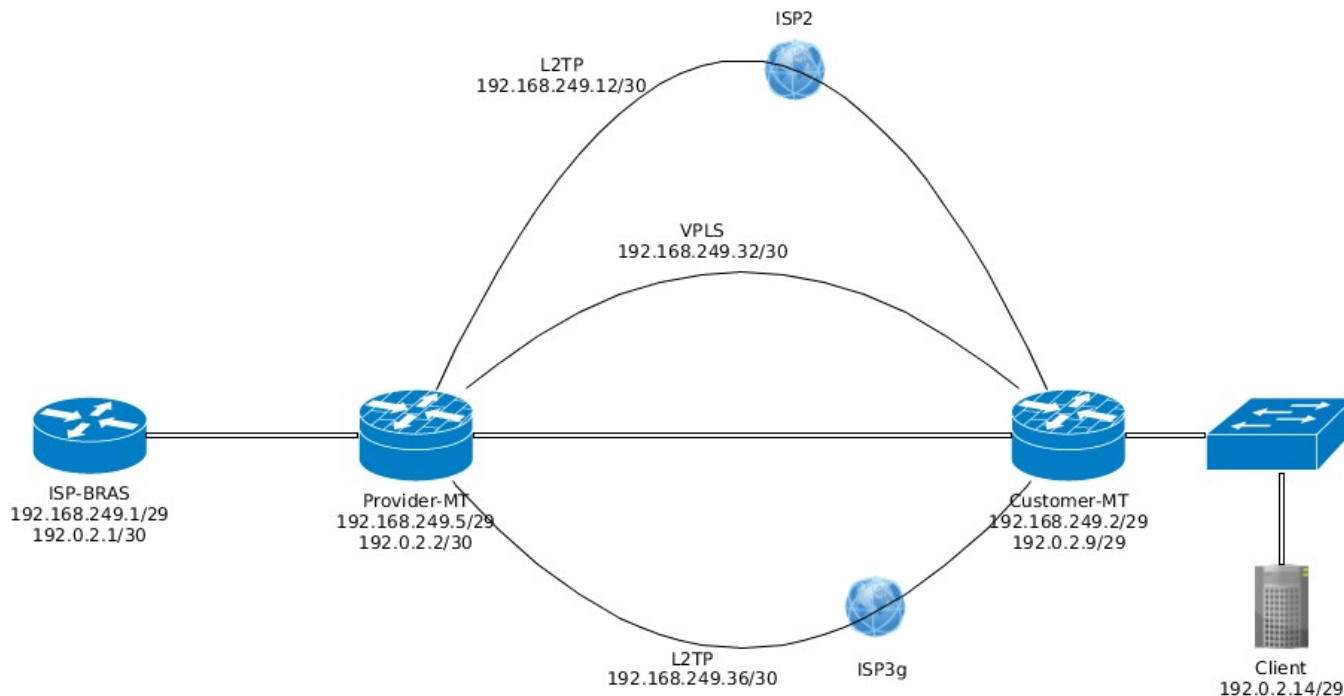
И всё? Почти да. Cisco ip sla:

```
#cisco ISP-BRAS
```

```
interface FastEthernet0/0.3029
  encapsulation dot1Q 3029
  ip address 192.168.249.1 255.255.255.248
!
ip sla monitor 1
  type echo protocol ipIcmpEcho 192.168.249.2 source-interface FastEthernet0/0.3029
ip sla monitor schedule 1 life forever start-time now
!
track 1 rtr 1 reachability
!
ip route 192.0.2.8 255.255.255.248 192.168.249.2 track 1
ip route 192.0.2.8 255.255.255.248 192.0.2.2 100
!
write memory
```

А давайте добавим резерв по 3G...

Но при этом по 3G не нужно резервировать L2, только L3.





Решение.

Можно абстрагироваться и представить, что у нас снова два канала:

1. Наш VPLS
2. L2TP через 3G

Создадим новый ospf instance для этих интерфейсов и перенесем анонсы клиентской сети в этот instance (area).



Configuration 2-1. Link. Provider-MT

```
/interface l2tp-server
```

```
add name=l2tp-ppp3 user=ppp3
```

```
/ppp secret
```

```
add local-address=192.168.249.37 name=ppp3 password=123 remote-address=192.168.249.38
```

```
/ip address
```

```
add address=192.168.249.33/30 interface=br-MAIN
```



Configuration 2-1. Link. Customer-MT

```
/interface l2tp-client
```

```
add connect-to=192.0.2.2 disabled=no mrru=1508 name=l2tp-ppp3 password=123 user=ppp3
```

```
/ip address
```

```
add address=192.168.249.34/30 interface=br-VPN
```



Configuration 2-2. OSPF. Provider-MT

```
/ip address add address=192.168.249.33/30 interface=br-MAIN
```

```
/routing ospf instance
```

```
set [ find default=yes ] distribute-default=never
```

```
add distribute-default=if-installed-as-type-1 name=ospf1 router-id=192.168.249.33
```

```
/routing ospf area add instance=ospf1 name=area1
```

```
/routing ospf interface
```

```
add cost=10 interface=br-MAIN network-type=broadcast
```

```
add cost=20 interface=l2tp-ppp3 network-type=point-to-point
```

```
/routing ospf network
```

```
add area=area1 network=192.168.249.32/28
```



Configuration 2-2. OSPF. Customer-MT

```
/ip address add address=192.168.249.34/30 interface=br-VPN
/routing ospf instance

    add name=ospf1 router-id=192.168.249.34

/routing ospf area add instance=ospf1 name=area1

/routing ospf interface

    add cost=10 interface=br-VPN network-type=broadcast

    add cost=20 interface=l2tp-ppp3 network-type=point-to-point

/routing ospf network

    add area=area1 network=192.168.249.32/28

    add area=area1 network=192.0.2.8/29
```

OSPF

admin@192.168.1.231 (Customer-MT) via 192.168.1.231 - WinBox v6.44.5 on CHR (x86_64)

Date: Aug/22/2019 Uptime: 2d 05:37:5

OSPF

Interfaces Instances Networks Areas Area Ranges Virtual Links Neighbors NBMA Neighbors Sham Links LSA Routes ...

+ - [check] [x] [info] [filter] Find

	Interface	Cost	Priority	Authenti...	Authenticatio...	Network Type	Instance	Area	Neig...	State
P	all	10	1	none	*****	broadcast	default		0	down
	br-MAIN	10	1	none	*****	broadcast	ospf1	area1	1	backup
	l2tp-ppp3	20	1	none	*****	point to point	ospf1	area1	1	point to point
DP	br-lo0	10	1	none	*****	broadcast	default	backbone	0	passive
	l2tp-ppp2	20	1	none	*****	point to point	default	backbone	1	point to point
	vlan3029	10	1	none	*****	broadcast	default	backbone	1	designated r...

admin@192.168.1.231 (Customer-MT) - WinBox v6.44.5 on CHR (x86_64)

Date: Aug/22/2019 Uptime: 2d 05:37

OSPF

Interfaces Instances Networks Areas Area Ranges Virtual Links Neighbors NBMA Neighbors Sham Links LSA Routes ...

+ - [check] [x] [info] [filter] Find

	Interface	Cost	Priority	Authenti...	Authenticatio...	Network Type	Instance	Area	Neig...	State
P	all	10	1	none	*****	broadcast	default		0	down
	br-VPN	10	1	none	*****	broadcast	ospf1	area1	1	designated r...
DP	ether4	10	1	none	*****	broadcast	ospf1	area1	0	passive
	l2tp-ppp3	20	1	none	*****	point to point	ospf1	area1	1	point to point
DP	br-lo0	10	1	none	*****	broadcast	default	backbone	0	passive
	l2tp-ppp2	20	1	none	*****	point to point	default	backbone	1	point to point
	vlan3029	10	1	none	*****	broadcast	default	backbone	1	backup



Route1

Route List

Routes

Nexthops

Rules

VRF



OSPF



is



yes

	Dst. Address	Gateway	Distance	Ro
DAo	192.0.2.8/29	192.168.249.34 reachable br-MAIN	110	
DAo	192.168.249.10	192.168.249.2 reachable vlan3029	110	
DAo	192.168.249.13	192.168.249.2 reachable vlan3029	110	
DAo	192.168.249.37	192.168.249.34 reachable br-MAIN	110	

admin@192.168.1.231 (Customer-MT) - WinBox v6.44.5 on CHR (x86_64)

Route List

Routes

Nexthops

Rules

VRF



OSPF



is



yes

	Dst. Address	Gateway	Distance	Ro
DAo	0.0.0.0/0	192.168.249.33 reachable br-VPN	110	
DAo	192.168.249.9	192.168.249.5 reachable vlan3029	110	
DAo	192.168.249.14	192.168.249.5 reachable vlan3029	110	
DAo	192.168.249.38	192.168.249.33 reachable br-VPN	110	



Route2

Route List

Routes

Nexthops

Rules

VRF



OSPF



is



yes

	Dst. Address	Gateway	Distance	Ro
DAo	192.0.2.8/29	192.168.249.34 reachable br-MAIN	110	
DAo	192.168.249.10	192.168.249.14 reachable l2tp-ppp2	110	
DAo	192.168.249.13	192.168.249.14 reachable l2tp-ppp2	110	
DAo	192.168.249.37	192.168.249.34 reachable br-MAIN	110	

admin@192.168.1.231 (Customer-MT) - WinBox v6.44.5 on CHR (x86_64)

Route List

Routes

Nexthops

Rules

VRF



OSPF



is



yes

	Dst. Address	Gateway	Distance	Ro
DAo	0.0.0.0/0	192.168.249.33 reachable br-VPN	110	
DAo	192.168.249.0/29	192.168.249.13 reachable l2tp-ppp2	110	
DAo	192.168.249.9	192.168.249.13 reachable l2tp-ppp2	110	
DAo	192.168.249.14	192.168.249.13 reachable l2tp-ppp2	110	
DAo	192.168.249.38	192.168.249.33 reachable br-VPN	110	



Route3

Route List

Routes

Nexthops

Rules

VRF



OSPF



is



yes

	Dst. Address	Gateway	Distance	Ro
DAo	192.0.2.8/29	192.168.249.38 reachable l2tp-ppp3	110	
DAo	192.168.249.37	192.168.249.38 reachable l2tp-ppp3	110	

admin@192.168.1.231 (Customer-MT) - WinBox v6.44.5 on CHR (x86_64)

Route List

Routes

Nexthops

Rules

VRF



OSPF



is



yes

	Dst. Address	Gateway	Distance	Ro
DAo	0.0.0.0/0	192.168.249.37 reachable l2tp-ppp3	110	
DAo	192.168.249.38	192.168.249.37 reachable l2tp-ppp3	110	

Demo. EVE-NG



Заключение.

Решено согласно техническому заданию.

- Если «жива» ВОЛС основного провайдера, то трафик пойдёт через неё, т. к. у неё будет основной приоритет. (routing and VPLS)
- Иначе, будет использоваться l2tp-ppp2 через проводного резервного провайдера. (routing and VPLS)
- Если же «отвалятся» проводные провайдера, то VPLS _не_ построится, т. к. в area1 нет анонсов до loopbacks (br-lo0), отработает только маршрутизация через l2tp-ppp3. (routing).

СПАСИБО ЗА ВНИМАНИЕ!



зелёнаяточка
смотри. слушай. говори

- Владимир Кузнецов smithy1208@gmail.com
- Россия, Липецк
- Ведущий инженер службы сети передачи данных
- ООО “Зеленая точка Липецк”
- <https://lipetsk.zelenaya.net>
- Канал в телеграмм <https://t.me/miktrain>
(MikroTik-Training.ru)
- Routing, OSPF, BGP, MPLS, LDP, VPLS, VRF, VPN, ...
- Ссылка на презентацию <http://bit.ly/2z1RnwV>

