

Использование L2TP + OSPF для резервирования канала связи с филиалами

Юрий Шевчик
Минск 2014

КТО Я?

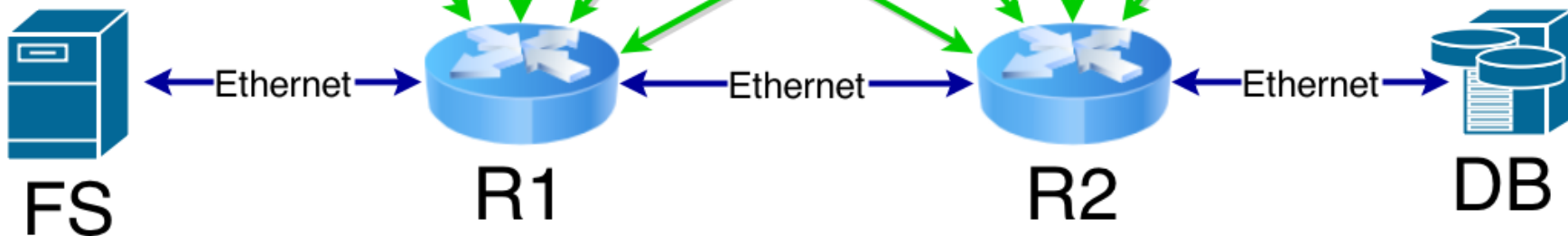
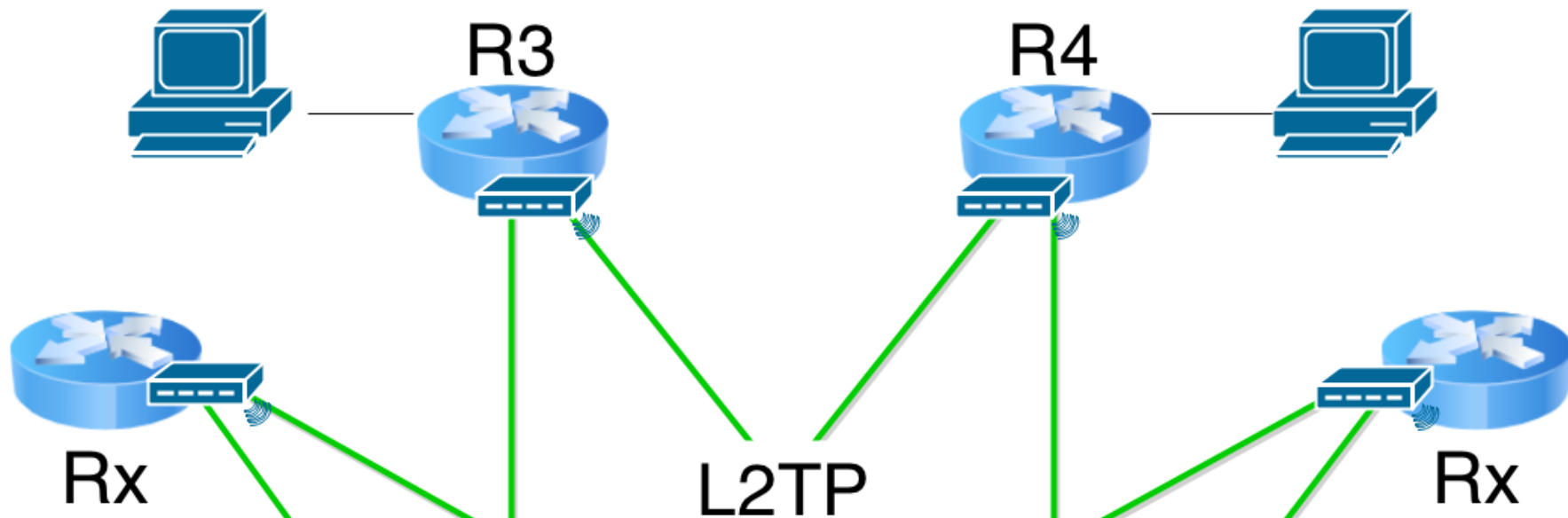
- Системный администратор в компании по продаже офисных принадлежностей
- Опыт построения сетей более 10 лет
- Получил сертификат МТСНА
- Познакомился с MikroTik пару лет назад

Зачем это нужно?

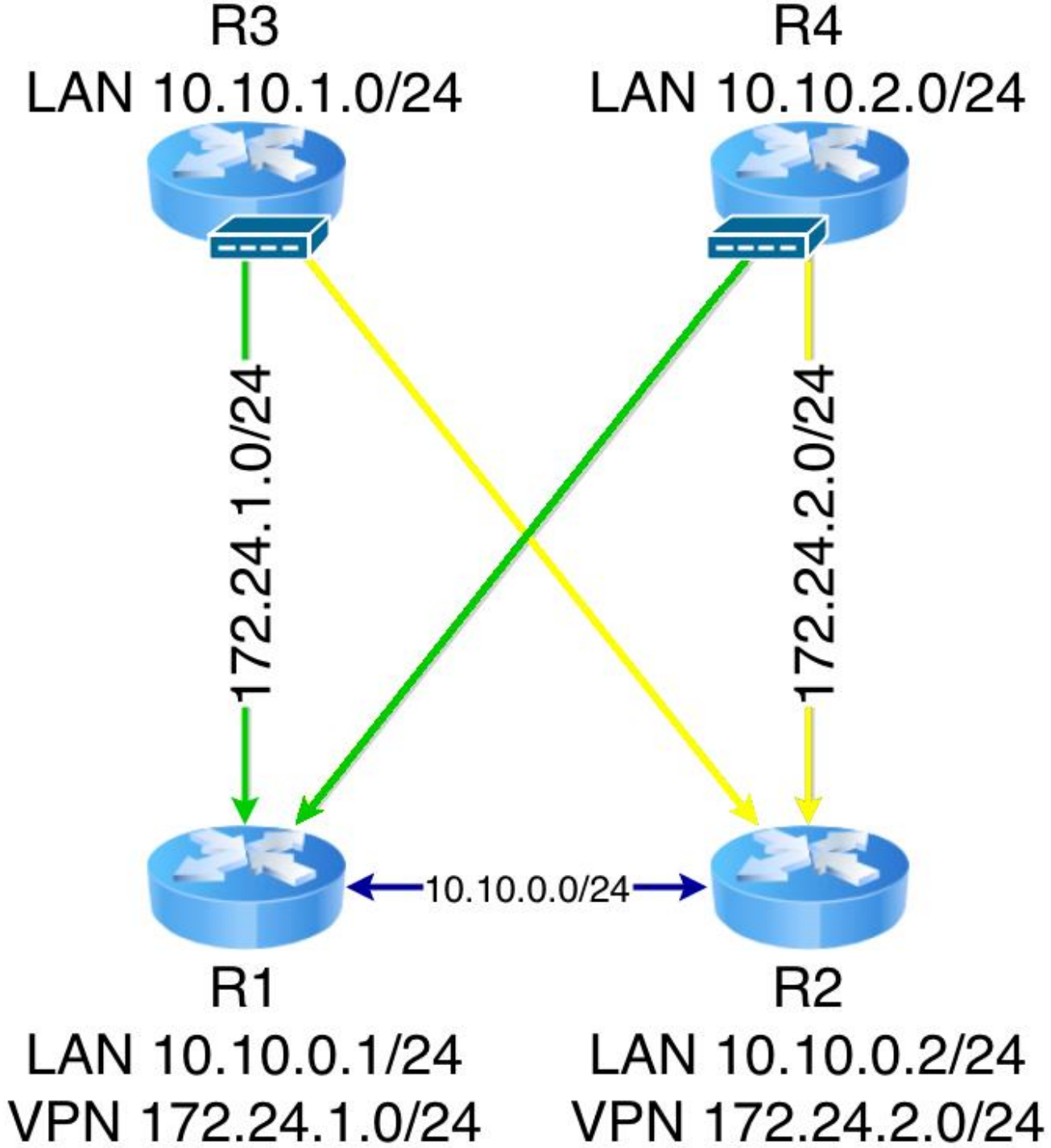
- ✓ Получить устойчивый доступ к удаленному офису, складу, квартире, видеонаблюдению, передвижной лаборатории и т.п.
- ✓ Не зависеть от выхода из строя одного из провайдеров интернета и оборудования на центральном офисе
- ✓ Использовать 3G модем для подключения
- ✓ Не покупать «белый» ip адрес

Пример ТОПОЛОГИИ СЕТИ

Представительства компании



Центральный офис



**Конфигурация
ОСНОВНЫХ
маршрутизаторов
в главном офисе
(R1 и R2)**

Настраиваем R1

#Указываем имена портов ethernet подключений:

```
/interface ethernet
```

```
set [ find default-name=ether1 ] name=eth1-wan
```

```
set [ find default-name=ether2 ] name=eth2-lan
```

#Добавляем ip адреса интерфейсам:

```
/ip address
```

```
add address=87.252.252.215/27 interface=eth1-wan network=87.252.252.192
```

```
add address=10.10.0.1/24 interface=eth2-lan network=10.10.0.0
```

#Добавляем маршрут по умолчанию (WAN):

```
/ip route
```

```
add distance=1 gateway=eth1-wan
```

#Указываем диапазон виртуальных адресов для L2TP:

```
/ip pool
```

```
add name=l2tp ranges=172.24.1.100-172.24.1.200
```


Настраиваем R1

#Включаем L2TP сервер:

```
/interface l2tp-server server
```

```
set authentication=mschap2 default-profile=l2tp enabled=yes
```

#Создаем учетные данные для L2TP подключений:

```
/ppp secret
```

```
add name=region3 password=1qazxsw23edc service=l2tp
```

```
add name=region4 password=1qazxsw23edc service=l2tp
```

#Настраиваем L2TP профиль:

```
/ppp profile
```

```
add change-tcp-mss=yes local-address=172.24.1.1 name=l2tp remote-address=l2tp
```

#Переименовываем роутер:

```
/system identity
```

```
set name=R1
```

Настраиваем R1

#Добавляем область OSPF:

```
/routing ospf area
```

```
add area-id=0.0.0.1 default-cost=10 inject-summary-lsas=no name=vpn type=stub
```

#Добавляем подсети OSPF:

```
/routing ospf network
```

```
add area=vpn network=10.10.0.0/24
```

```
add area=vpn network=172.24.1.0/24
```

Настраиваем R2

#Указываем имена портов ethernet подключений:

```
/interface ethernet
```

```
set [ find default-name=ether1 ] name=eth1-wan
```

```
set [ find default-name=ether2 ] name=eth2-lan
```

#Добавляем ip адреса интерфейсам:

```
/ip address
```

```
add address=87.252.252.216/27 interface=eth1-wan network=87.252.252.192
```

```
add address=10.10.0.2/24 interface=eth2-lan network=10.10.0.0
```

#Добавляем маршрут по умолчанию (WAN):

```
/ip route
```

```
add distance=1 gateway=eth1-wan
```

#Указываем диапазон виртуальных адресов для L2TP:

```
/ip pool
```

```
add name=l2tp ranges=172.24.2.100-172.24.2.200
```

Настраиваем R2

#Включаем L2TP сервер:

```
/interface l2tp-server server
```

```
set authentication=mschap2 default-profile=l2tp enabled=yes
```

#Создаем учетные данные для L2TP подключений:

```
/ppp secret
```

```
add name=region3 password=1qazxsw23edc service=l2tp
```

```
add name=region4 password=1qazxsw23edc service=l2tp
```

#Настраиваем L2TP профиль:

```
/ppp profile
```

```
add change-tcp-mss=yes local-address=172.24.2.1 name=l2tp remote-address=l2tp
```

#Переименовываем роутер:

```
/system identity
```

```
set name=R2
```

Настраиваем R2

#Добавляем область OSPF:

```
/routing ospf area
```

```
add area-id=0.0.0.1 default-cost=10 inject-summary-lsas=no name=vpn type=stub
```

#Добавляем подсети OSPF:

```
/routing ospf network
```

```
add area=vpn network=10.10.0.0/24
```

```
add area=vpn network=172.24.2.0/24
```

R1 и R2

**ГОТОВЫ ПРИНИМАТЬ
ВХОДЯЩИЕ L2TP
ПОДКЛЮЧЕНИЯ**

**Приступим к
настройке
удаленных роутеров
(R3 и R4)**

Настраиваем R3

#Указываем имя роутера:

```
/system identity
```

```
set name=R3
```

#Создаем клиентские L2TP подключения к R1 и R2:

```
/interface l2tp-client
```

```
add add-default-route=no allow=mschap2 connect-to=87.252.252.215 \  
    dial-on-demand=no disabled=no keepalive-timeout=60 max-mru=1450 max-mtu=\  
    1450 mrru=1600 name=L2TP-R1 password=1qazxsw23edc profile=default user=\  
    region3
```

```
add add-default-route=no allow=mschap2 connect-to=87.252.252.216 \  
    dial-on-demand=no disabled=no keepalive-timeout=60 max-mru=1450 max-mtu=\  
    1450 mrru=1600 name=L2TP-R2 password=1qazxsw23edc profile=default user=\  
    region3
```


Настраиваем R3

#Задаем локальный ip адрес роутера:

```
/ip address
```

```
add address=10.10.1.1/24 interface=lan network=10.10.1.0
```

#Добавляем DHCP клиента для аренды ip адреса от провайдера интернета:

```
/ip dhcp-client
```

```
add default-route-distance=0 dhcp-options=hostname,clientid disabled=no \  
    interface=wan
```

Настраиваем R3

#Добавляем область OSPF:

```
/routing ospf area
```

```
add area-id=0.0.0.1 default-cost=10 inject-summary-lsas=no name=vpn type=stub
```

#Добавляем подсети OSPF:

```
/routing ospf network
```

```
add area=vpn network=10.10.1.0/24
```

```
add area=vpn network=172.24.1.1/32
```

```
add area=vpn network=172.24.2.1/32
```

Настраиваем R4

#Указываем имя роутера:

```
/system identity
```

```
set name=R4
```

#Создаем клиентские L2TP подключения к R1 и R2:

```
/interface l2tp-client
```

```
add add-default-route=no allow=mschap2 connect-to=87.252.252.215 \  
    dial-on-demand=no disabled=no keepalive-timeout=60 max-mru=1450 max-mtu=\  
    1450 mrru=1600 name=L2TP-R1 password=1qazxsw23edc profile=default user=\  
    region3
```

```
add add-default-route=no allow=mschap2 connect-to=87.252.252.216 \  
    dial-on-demand=no disabled=no keepalive-timeout=60 max-mru=1450 max-mtu=\  
    1450 mrru=1600 name=L2TP-R2 password=1qazxsw23edc profile=default user=\  
    region3
```

Настраиваем R4

#Задаем локальный ip адрес роутера:

```
/ip address
```

```
add address=10.10.2.1/24 interface=lan network=10.10.2.0
```

#Добавляем DHCP клиента для аренды ip адреса от провайдера интернета:

```
/ip dhcp-client
```

```
add default-route-distance=0 dhcp-options=hostname,clientid disabled=no \  
    interface=wan
```

Настраиваем R4

#Добавляем область OSPF:

```
/routing ospf area
```

```
add area-id=0.0.0.1 default-cost=10 inject-summary-lsas=no name=vpn type=stub
```

#Добавляем подсети OSPF:

```
/routing ospf network
```

```
add area=vpn network=10.10.2.0/24
```

```
add area=vpn network=172.24.1.1/32
```

```
add area=vpn network=172.24.2.1/32
```

**Все роутеры
настроены на обмен
маршрутами
по 2-м L2TP тоннелям**

**Проверим, что
все работает
как нужно**

PPP R3 10.10.1.1

Interface	PPPoE Servers	Secrets	Profiles	Active Connections		
<div style="display: flex; justify-content: space-between;"> PPP Scanner PPTP Server SSTP Server L2TP Server OVPN Server PPPoE Scan </div>						
Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
R ↔ L2TP-R1	L2TP Client		0 bps	0 bps	0	0
R ↔ L2TP-R2	L2TP Client		0 bps	0 bps	0	0

Route List

Routes	Next hops	Rules	VRF
<div style="display: flex; justify-content: space-between;"> + - ✓ ✗ 📄 🔍 Find </div>			
Dst. Address	Gateway	Distance	Routing Mark
DAS ▶ 0.0.0.0/0	192.168.1.1 reachable mts	0	
DAo ▶ 10.10.0.0/24	172.24.2.1 reachable L2TP-R2, 172.24.1.1 reachable L2TP-R1	110	
DAC ▶ 10.10.1.0/24	localnet reachable	0	10.10.1.1
DAo ▶ 10.10.2.0/24	172.24.2.1 reachable L2TP-R2, 172.24.1.1 reachable L2TP-R1	110	
DAC ▶ 172.24.1.1	L2TP-R1 reachable	0	172.24.1.196
DAo ▶ 172.24.1.196	172.24.1.1 reachable L2TP-R1	110	
DAo ▶ 172.24.1.197	172.24.1.1 reachable L2TP-R1	110	
DAC ▶ 172.24.2.1	L2TP-R2 reachable	0	172.24.2.196
DAo ▶ 172.24.2.196	172.24.2.1 reachable L2TP-R2	110	
DAo ▶ 172.24.2.197	172.24.2.1 reachable L2TP-R2	110	
DAC ▶ 192.168.1.0/24	mts reachable	0	192.168.1.100

OSPF

Networks	Areas	Area Ranges	Virtual Links	Neighbors	NBMA Neighbors	Sham Links	LSA	Routes	AS Border Routers	Area Border Routers
<div style="display: flex; justify-content: space-between;"> + - ✓ ✗ 📄 🔍 </div>										
Instance	Router ID	Address	Interface	State Changes	Adjacency	State				
default	10.10.0.1	172.24.1.1	L2TP-R1	4	02:22:40	Full				
default	10.10.0.2	172.24.2.1	L2TP-R2	4	02:22:14	Full				

Terminal

```
[admin@R3] > tool traceroute R1 count=100
# ADDRESS          LOSS SENT  LAST    AVG    BEST  WORST  STD-DEV STATUS
1 172.24.2.1        0% 100 49.3ms 51.4   34.7  109.4   9.1
2 10.10.0.1         0% 100 60ms   61.2   46.6   100     8.4

[admin@R3] > tool traceroute R2 count=100
# ADDRESS          LOSS SENT  LAST    AVG    BEST  WORST  STD-DEV STATUS
1 10.10.0.2         0% 100 48.3ms 51.4   44.5   89.2   6.3

[admin@R3] > tool traceroute R4 count=100
# ADDRESS          LOSS SENT  LAST    AVG    BEST  WORST  STD-DEV STATUS
1 172.24.2.1        0% 100 45.5ms 52.5   44.4  105.7   9.3
2 10.10.2.1         0% 100 139.9ms 118.8  86.4  229.8  115.8
```

PPP R4 10.10.2.1

Interface	PPPoE Servers	Secrets	Profiles	Active Connections		
<div style="display: flex; justify-content: space-between;"> PPP Scanner PPTP Server SSTP Server L2TP Server OVPN Server PPPoE Scan </div>						
Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
R ↔ L2TP-R1	L2TP Client		0 bps	0 bps	0	0
R ↔ L2TP-R2	L2TP Client		544 bps	0 bps	1	1
R ↔ ppp-out	PPP Client	1500	5.6 kbps	7.8 kbps	8	8

Route List

Routes	Next hops	Rules	VRF
<div style="display: flex; justify-content: space-between;"> + - ✓ ✗ 📄 🔍 Find </div>			
Dst. Address	Gateway	Distance	Routing Mark
DAS ▶ 0.0.0.0/0	10.112.112.130 reachable ppp-out	1	
DAo ▶ 10.10.0.0/24	172.24.1.1 reachable L2TP-R1, 172.24.2.1 reachable L2TP-R2	110	
DAo ▶ 10.10.1.0/24	172.24.1.1 reachable L2TP-R1, 172.24.2.1 reachable L2TP-R2	110	
DAC ▶ 10.10.2.0/24	localnet reachable	0	10.10.2.1
DAC ▶ 10.112.112.130	ppp-out reachable	0	10.104.239.238
DAC ▶ 172.24.1.1	L2TP-R1 reachable	0	172.24.1.197
DAo ▶ 172.24.1.196	172.24.1.1 reachable L2TP-R1	110	
DAo ▶ 172.24.1.197	172.24.1.1 reachable L2TP-R1	110	
DAC ▶ 172.24.2.1	L2TP-R2 reachable	0	172.24.2.197
DAo ▶ 172.24.2.196	172.24.2.1 reachable L2TP-R2	110	
DAo ▶ 172.24.2.197	172.24.2.1 reachable L2TP-R2	110	

OSPF

Networks	Areas	Area Ranges	Virtual Links	Neighbors	NBMA Neighbors	Sham Links	LSA	Routes	AS Border Routers	Area Border Routers
<div style="display: flex; justify-content: space-between;"> + - ✓ ✗ 📄 🔍 </div>										
Instance	Router ID	Address	Interface	State Changes	Adjacency	State				
default	10.10.0.1	172.24.1.1	L2TP-R1	4	02:17:44	Full				
default	10.10.0.2	172.24.2.1	L2TP-R2	4	02:17:22	Full				

Terminal

```
[admin@R4] > tool traceroute R1 count=100
# ADDRESS          LOSS SENT  LAST    AVG    BEST  WORST  STD-DEV STATUS
1 172.24.2.1        0% 100 37.8ms 42.1   32.3   89.1   7
2 10.10.0.1         0% 100 37.8ms 42.6   35.6  119.8  12

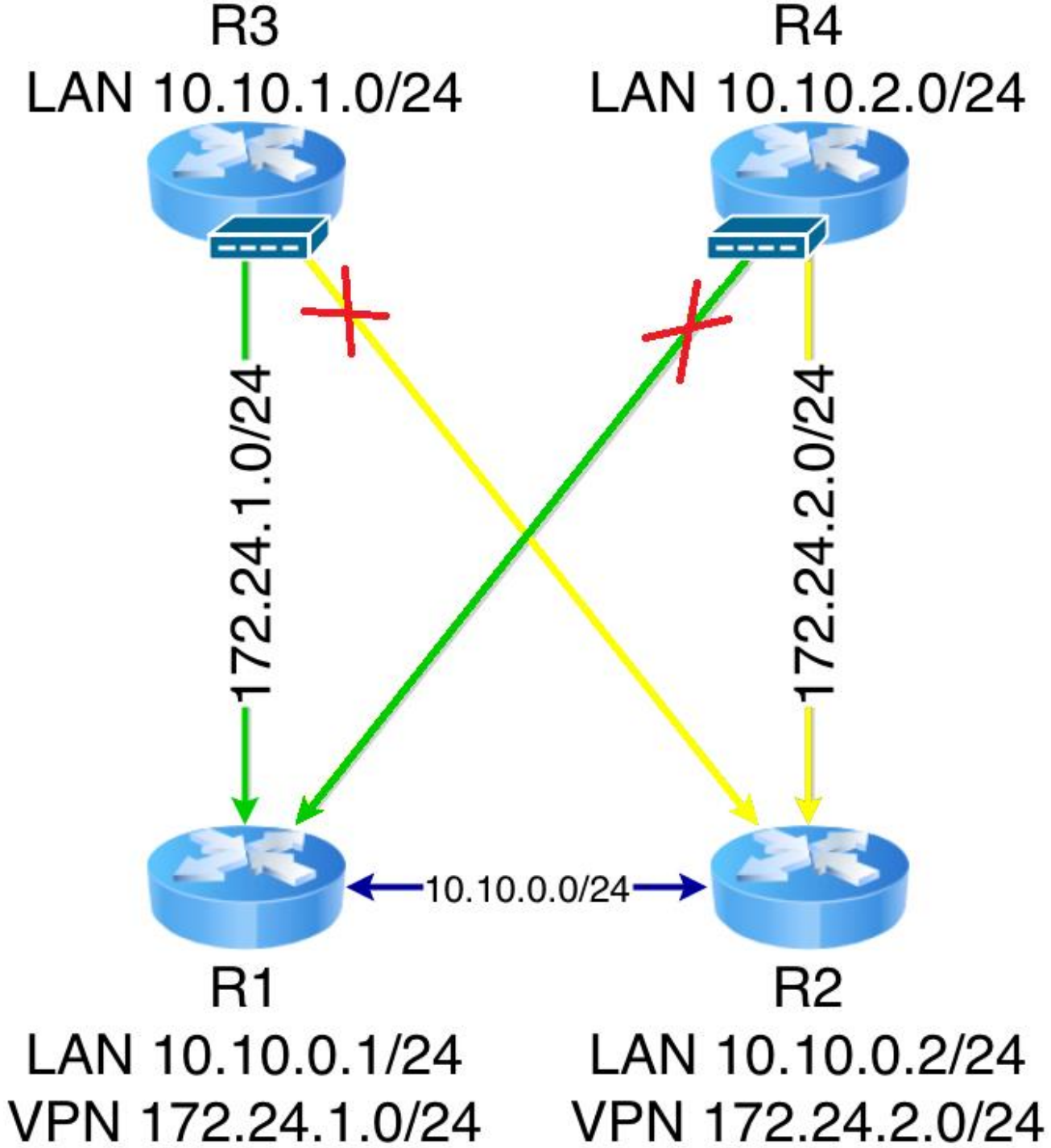
[admin@R4] > tool traceroute R2 count=100
# ADDRESS          LOSS SENT  LAST    AVG    BEST  WORST  STD-DEV STATUS
1 172.24.1.1        0% 100 42.7ms 48.8   34.5   307   27.7
2 10.10.0.2         0% 100 35.8ms 50     35.8  119.8  17

[admin@R4] > tool traceroute R3 count=100
# ADDRESS          LOSS SENT  LAST    AVG    BEST  WORST  STD-DEV STATUS
1 172.24.1.1        0% 100 83.1ms 53.1   30.3  127.4  20.1
2 10.10.1.1         0% 100 423.9ms 121.7  91.8  423.9  119.3
```


R3 и R4 получили
маршруты от R1 и R2

Трассировка
проходит ко всем
соседним роутерам

Отключим
по 1-му
подключению
R3 и R4
для проверки
резервирования



PPP R3 10.10.1.1

Interface	PPPoE Servers	Secrets	Profiles	Active Connections		
<div style="display: flex; justify-content: space-between;"> PPP Scanner PPTP Server SSTP Server L2TP Server OVPN Server PPPoE Scan </div>						
Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
X L2TP-R1	L2TP Client			0 bps	0 bps	0
R L2TP-R2	L2TP Client			0 bps	0 bps	0

Route List

Routes	Nexthops	Rules	VRF	
<div style="display: flex; justify-content: space-between;"> + - ✓ ✗ 📄 🔍 Find </div>				
Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAS 0.0.0.0/0	192.168.1.1 reachable mts	0		
DAo 10.10.0.0/24	172.24.2.1 reachable L2TP-R2	110		
DAC 10.10.1.0/24	localnet reachable	0		10.10.1.1
DAo 10.10.2.0/24	172.24.2.1 reachable L2TP-R2	110		
DAo 172.24.1.1	172.24.2.1 reachable L2TP-R2	110		
DAo 172.24.1.197	172.24.2.1 reachable L2TP-R2	110		
DAC 172.24.2.1	L2TP-R2 reachable	0		172.24.2.196
DAo 172.24.2.196	172.24.2.1 reachable L2TP-R2	110		
DAC 192.168.1.0/24	mts reachable	0		192.168.1.100

OSPF

Networks	Areas	Area Ranges	Virtual Links	Neighbors	NBMA Neighbors	Sham Links	LSA	Routes	AS Border Routers	Area Border Routers
<div style="display: flex; justify-content: space-between;"> + - ✓ ✗ 📄 🔍 Find </div>										
Instance	Router ID	Address	Interface	State Changes	Adjacency	State				
default	10.10.0.2	172.24.2.1	L2TP-R2	4	02:39:48	Full				

Terminal

```

[admin@R3] > tool traceroute R1 count=100
# ADDRESS          LOSS SENT  LAST    AVG    BEST  WORST  STD-DEV STATUS
1 172.24.2.1        0% 100 45.6ms 52.5   44.4   88.6   7.6
2 10.10.0.1         0% 100 59.8ms 61.2   54.8   100    6.2

[admin@R3] > tool traceroute R2 count=100
# ADDRESS          LOSS SENT  LAST    AVG    BEST  WORST  STD-DEV STATUS
1 10.10.0.2         0% 100 46.8ms 51.5   44.2   82.6   7

[admin@R3] > tool traceroute R4 count=100
# ADDRESS          LOSS SENT  LAST    AVG    BEST  WORST  STD-DEV STATUS
1 172.24.2.1        0% 100 53.6ms 51.9   44.4   89.7   7.9
2 10.10.0.1         0% 100 60.3ms 61.9   48.8   90     6.6
3 10.10.2.1         0% 100 119.4ms 112.7  89.4   180   94.2
    
```

PPP R4 10.10.2.1

Interface	PPPoE Servers	Secrets	Profiles	Active Connections		
<div style="display: flex; justify-content: space-between;"> PPP Scanner PPTP Server SSTP Server L2TP Server OVPN Server PPPoE Scan </div>						
Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
R L2TP-R1	L2TP Client			0 bps	0 bps	0
X L2TP-R2	L2TP Client			0 bps	0 bps	0
R ppp-out	PPP Client	1500	98.9 kbps	30.0 kbps		23

Route List

Routes	Nexthops	Rules	VRF	
<div style="display: flex; justify-content: space-between;"> + - ✓ ✗ 📄 🔍 Find </div>				
Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAS 0.0.0.0/0	10.112.112.130 reachable ppp-out	1		
DAo 10.10.0.0/24	172.24.1.1 reachable L2TP-R1	110		
DAo 10.10.1.0/24	172.24.1.1 reachable L2TP-R1	110		
DAC 10.10.2.0/24	localnet reachable	0		10.10.2.1
DAC 10.112.112.130	ppp-out reachable	0		10.104.239.238
DAC 172.24.1.1	L2TP-R1 reachable	0		172.24.1.197
DAo 172.24.1.197	172.24.1.1 reachable L2TP-R1	110		
DAo 172.24.2.1	172.24.1.1 reachable L2TP-R1	110		
DAo 172.24.2.196	172.24.1.1 reachable L2TP-R1	110		

OSPF

Networks	Areas	Area Ranges	Virtual Links	Neighbors	NBMA Neighbors	Sham Links	LSA	Routes	AS Border Routers	Area Border Routers
<div style="display: flex; justify-content: space-between;"> + - ✓ ✗ 📄 🔍 Find </div>										
Instance	Router ID	Address	Interface	State Changes	Adjacency	State				
default	10.10.0.1	172.24.1.1	L2TP-R1	4	02:35:19	Full				

Terminal

```

[admin@R4] > tool traceroute R1 count=100
# ADDRESS          LOSS SENT  LAST    AVG    BEST  WORST  STD-DEV STATUS
1 10.10.0.1         0% 100 78.3ms 51.7   35.3  207.8  26

[admin@R4] > tool traceroute R2 count=100
# ADDRESS          LOSS SENT  LAST    AVG    BEST  WORST  STD-DEV STATUS
1 172.24.1.1        0% 100 43.2ms 47.2   32.1  119.1  15.7
2 10.10.0.2         0% 100 41.8ms 50     33.7  199.8  24.9

[admin@R4] > tool traceroute R3 count=100
# ADDRESS          LOSS SENT  LAST    AVG    BEST  WORST  STD-DEV STATUS
1 172.24.1.1        0% 100 84.3ms 48.6   33.5  124.5  14.3
2 10.10.0.2         0% 100 59.9ms 49.4   36    129.9  17.6
3 10.10.1.1         0% 100 123.9ms 116.4  89.8  205.5  116
    
```

Все еще
работает



Вопросы?

Спасибо
за
внимание!

Знаете как улучшить
или упростить?

routeros@icloud.com