MikroTik MUM 2015 Молдова, Кишинев

Построение корпоративной VPN сети на основе EoIP туннелей с отказоустойчивостью на базе протокола RSTP и безопасностью на основе IPsec tunnel mode

by Marcov Andrei

VPN L2 network

О себе:

* Андрей Марков, инженер магистральных транспортных сетей IP/MPLS SA “Moldtelecom”
* С MikroTik’ом работаю с 2010 года
* Сертификаты MTCNA, MTCRE (“Aitec CA”)

  Cisco CCNA (SA Moldtelecom)
* MUM 2013 Кишинев, MUM 2015 Москва

Цель презентации

Показать на практическом примере один из способов организации отказоустойчивой L2 VPN сети используя маршрутизаторы MikroTik:

* **CCR1036-12G-4S**

* **RB2011UiAS-2HnD-IN**

* **RB751U-2HnD**

Техническое задание (ТЗ):

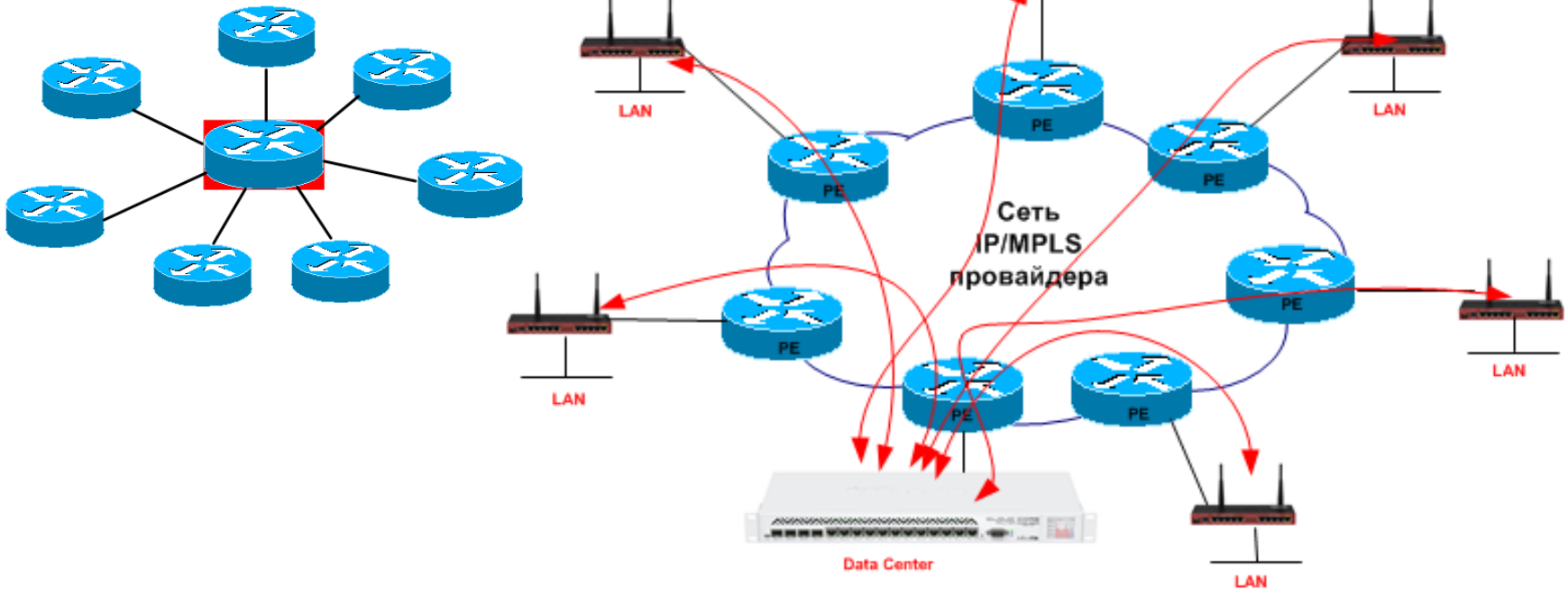
1. Топология сети «Звезда», все филиалы соединяются с головным офисом

2. Централизованное управление трафиком

3. Отказоустойчивость (link redundancy и минимальное время сходимости сети)

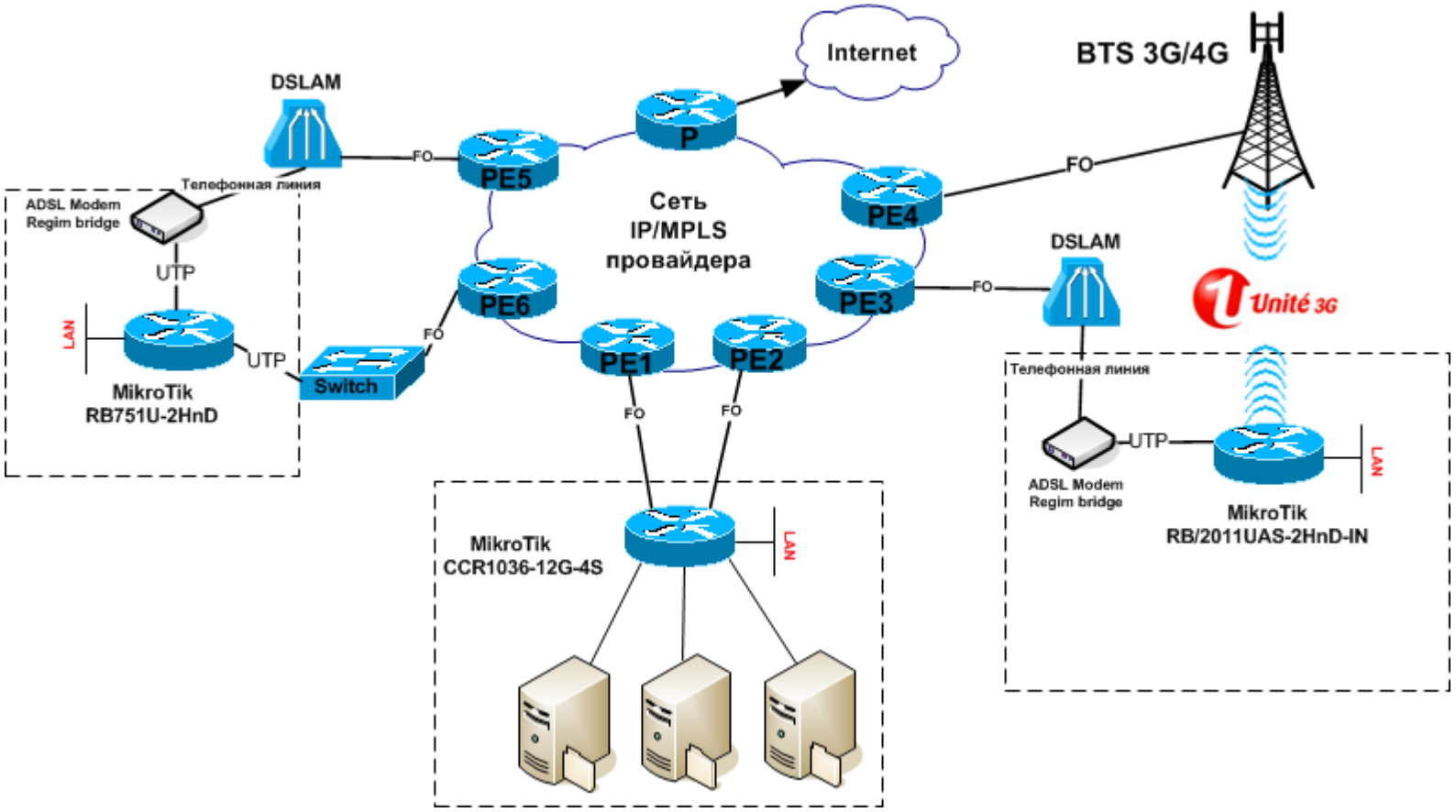
4. Безопасная передача данных

Топология сети «Звезда», все филиалы соединяются с центральным офисом.



Избыточность линков (link redundancy)

Рассмотрим на примере двух точек и дата центра:



Как видно из схемы, каждый узел имеет дублирующий линк.

Ethernet over IP (EoIP)

a) Строим EoIP туннели от филиалов в головной офис (Data Center) согласно топологии «Звезда».

Для этого необходимо прописать статические маршруты:

Router B:

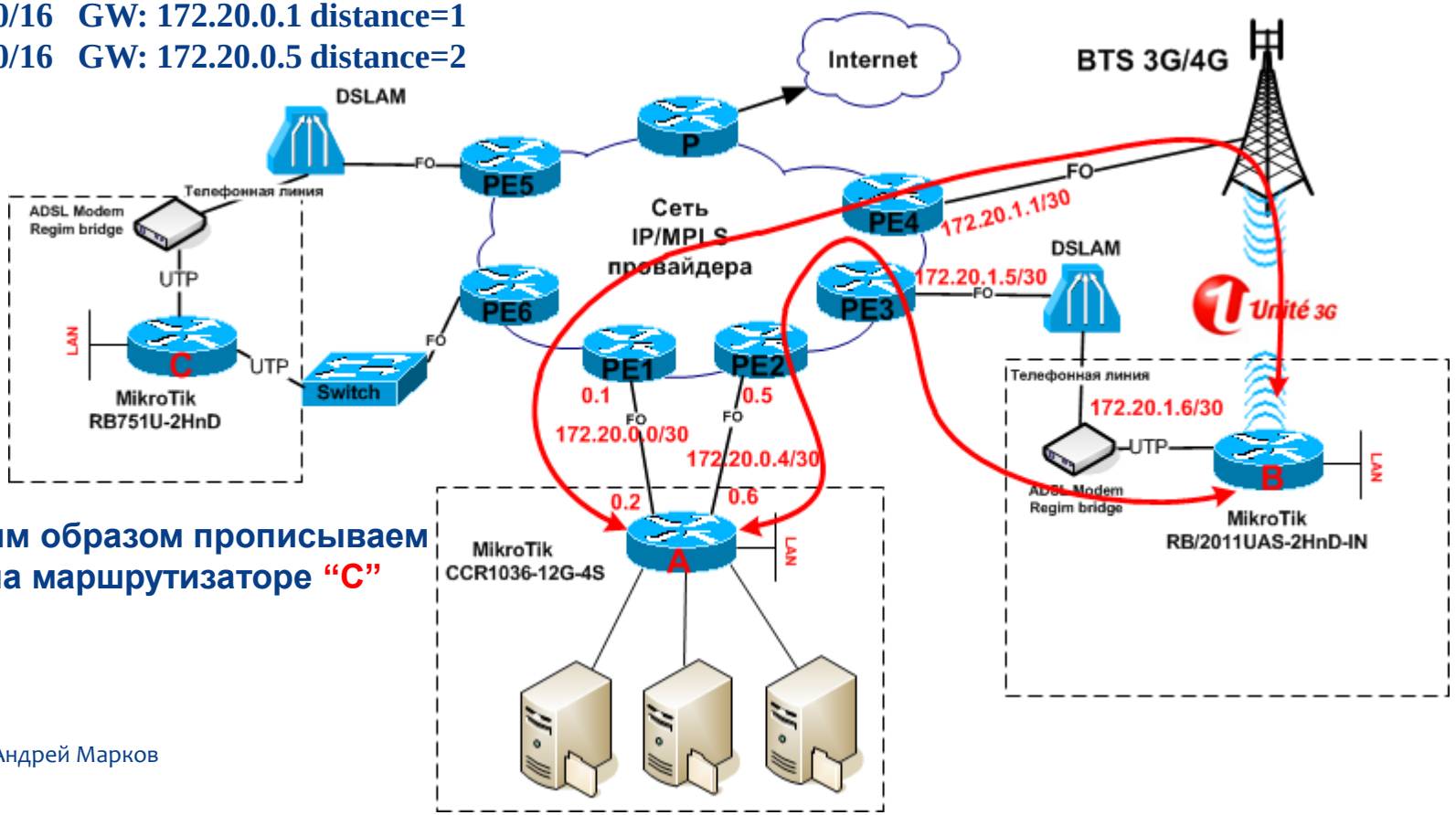
Dst: 172.20.0.0/30 GW: 172.20.1.1

Dst: 172.20.0.4/30 GW: 172.20.1.5

Router A:

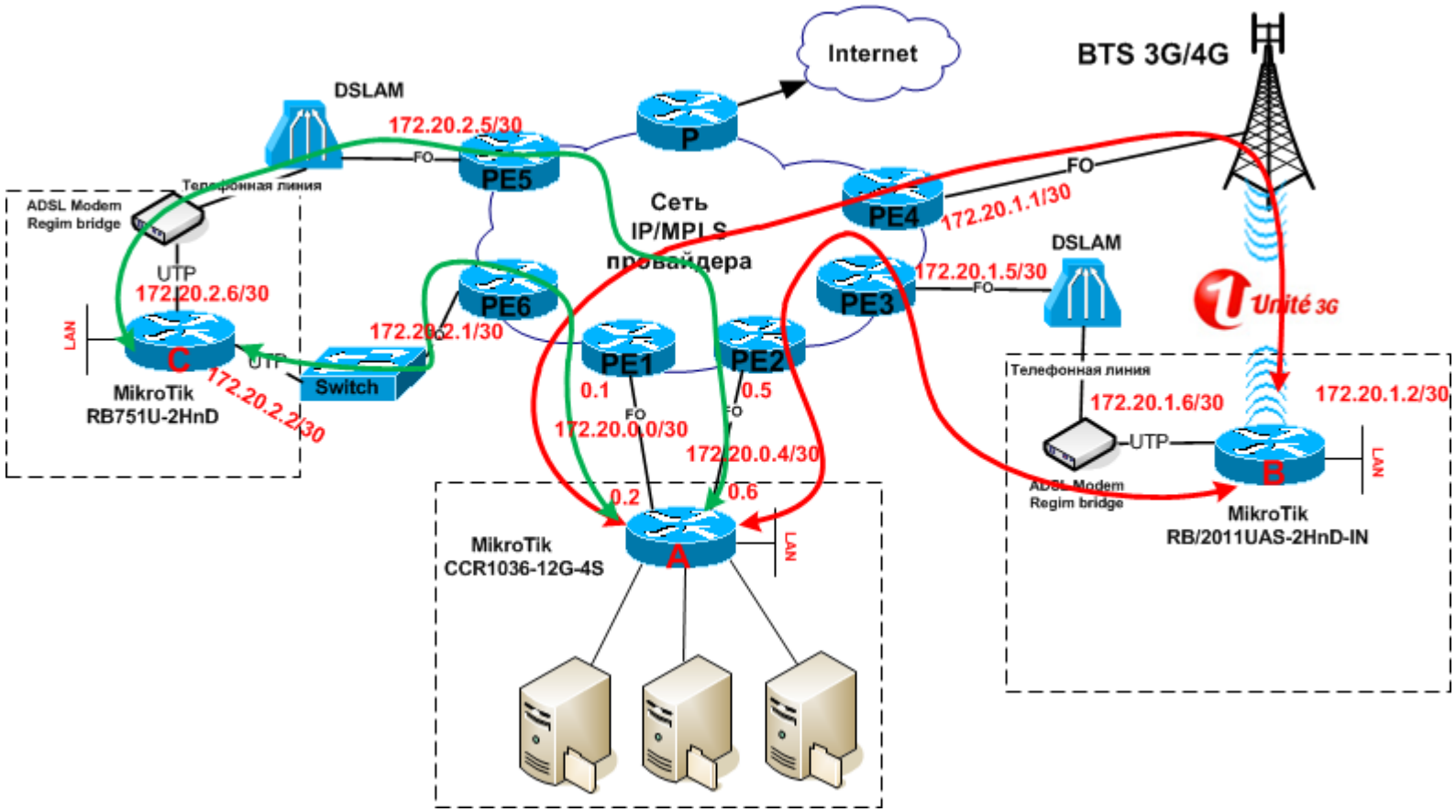
Dst: 172.20.0.0/16 GW: 172.20.0.1 distance=1

Dst: 172.20.0.0/16 GW: 172.20.0.5 distance=2



Аналогичным образом прописываем маршруты на маршрутизаторе “C”

b) Получается по 2 EoIP туннеля на филиал. Необходимо, чтоб каждый из линков шел по разным путям до конечной точки



Базовый конфиг EoIP будет выглядеть так:

Router A:

```
0   name="eoip_A-to-B_1"  local-address=172.20.0.2 remote-address=172.20.1.2 tunnel-id=1
1   name="eoip_A-to-B_2"  local-address=172.20.0.6 remote-address=172.20.1.6 tunnel-id=2
2   name="eoip_A-to-C_1"  local-address=172.20.0.2 remote-address=172.20.2.2 tunnel-id=3
3   name="eoip_A-to-C_2"  local-address=172.20.0.6 remote-address=172.20.2.6 tunnel-id=4
```

Router B:

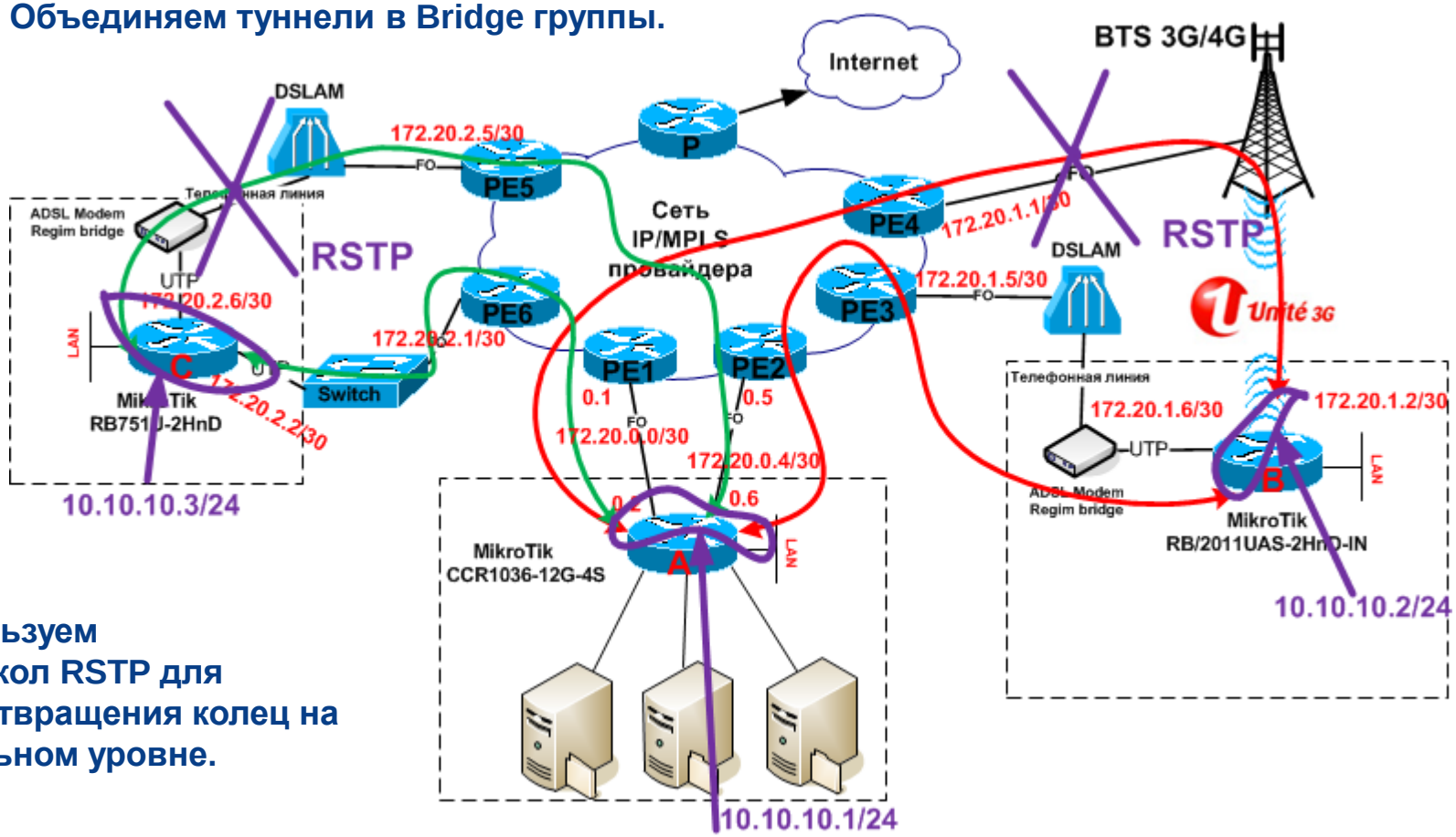
```
0   name="eoip_B-to-A_1" local-address=172.20.1.2 remote-address=172.20.0.2 tunnel-id=1
1   name="eoip_B-to-A_2" local-address=172.20.1.6 remote-address=172.20.0.6 tunnel-id=2
```

Router C:

```
0   name="eoip_C-to-A_1" local-address=172.20.2.2 remote-address=172.20.0.2 tunnel-id=3
1   name="eoip_C-to-A_2" local-address=172.20.2.6 remote-address=172.20.0.6 tunnel-id=4
```

Отказоустойчивость

c) Объединяем туннели в Bridge группы.



Используем протокол RSTP для предотвращения колец на канальном уровне.

RSTP *(Rapid spanning tree protocol)*

- Протокол работает на канальном уровне. RSTP позволяет делать топологию избыточной на физическом уровне, но при этом логически блокировать петли.

Время сходимости составляет 3 x Hello interval (2 second)=6 seconds

Как указать какой Link будет избыточным?

1) **Необходимо четко указать Root Bridge* (изменив Priority)**
2) **Меняя значения Cost (стоимость пути) можем изменять статус линка.**

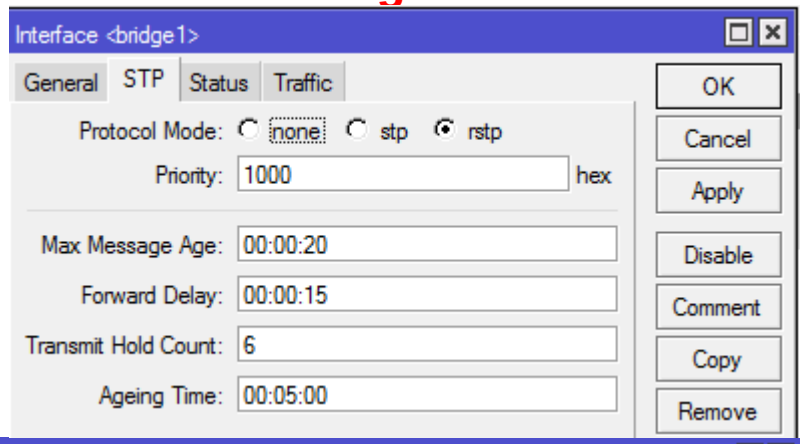
*** Только один коммутатор может быть корневым. Для того чтобы выбрать корневой коммутатор, все коммутаторы отправляют сообщения BPDU, указывая себя в качестве корневого коммутатора. Если коммутатор получает BPDU от коммутатора с меньшим Bridge ID, то он перестает анонсировать информацию о том, что он корневой и начинает передавать BPDU коммутатора с меньшим Bridge ID.**

Создаем Bridge интерфейсы и присваиваем им IP с одной подсети:

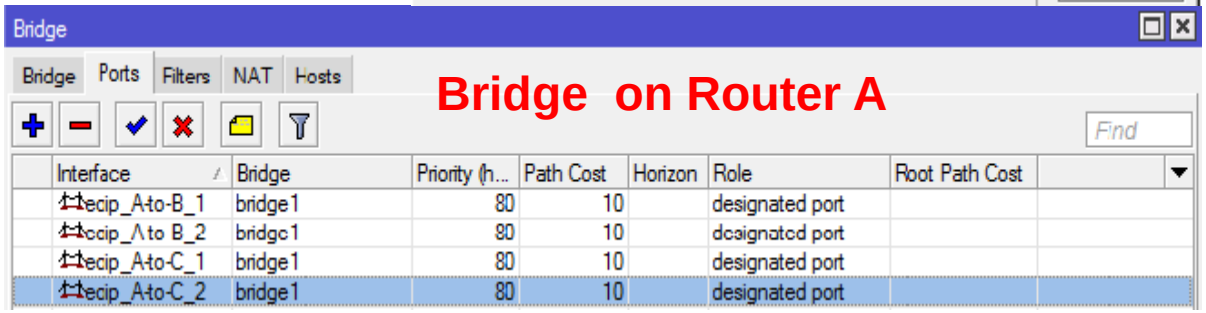
Router A:
IP address=10.10.10.1/24 interface=bridge1
Router B:
IP address=10.10.10.2/24 interface=bridge1
Router C:
IP address=10.10.10.3/24 interface=bridge1

Эти IP будут впоследствии использоваться как Peer для настройки IPSec

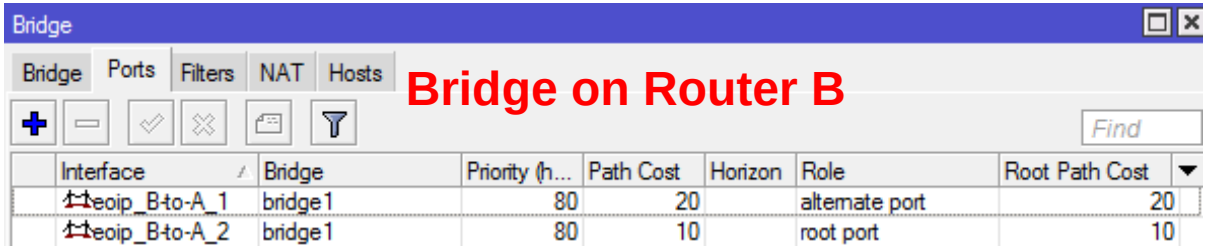
Root Bridge on Router A



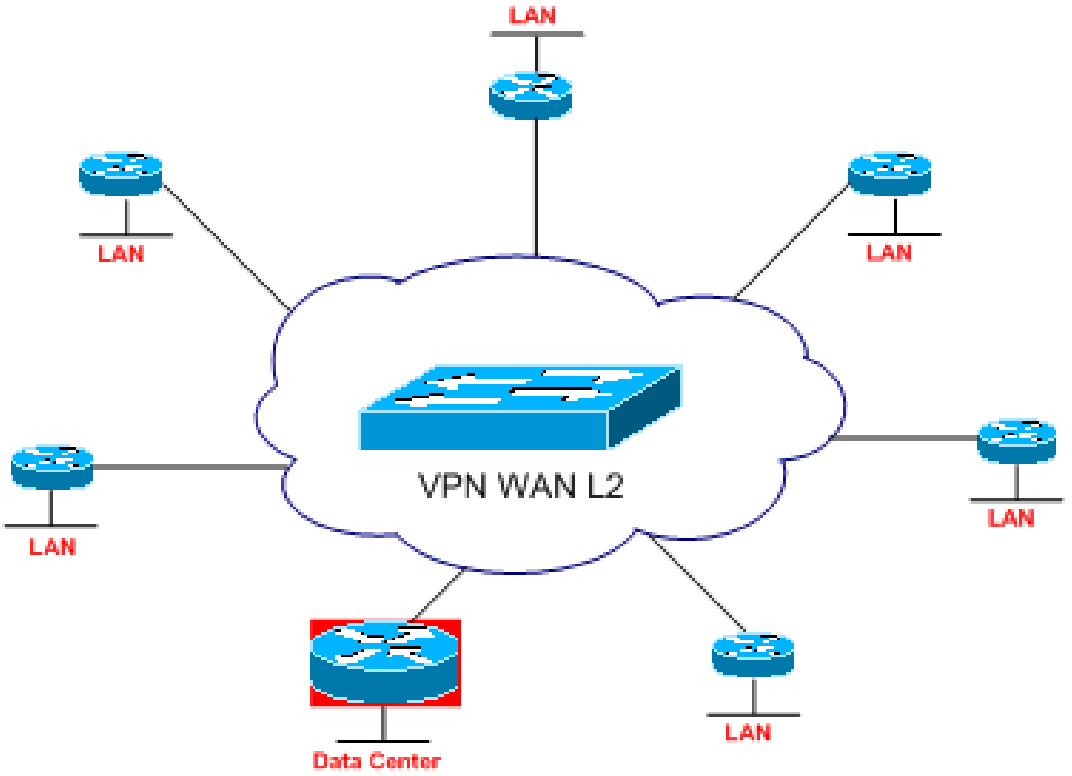
Bridge on Router A



Bridge on Router B

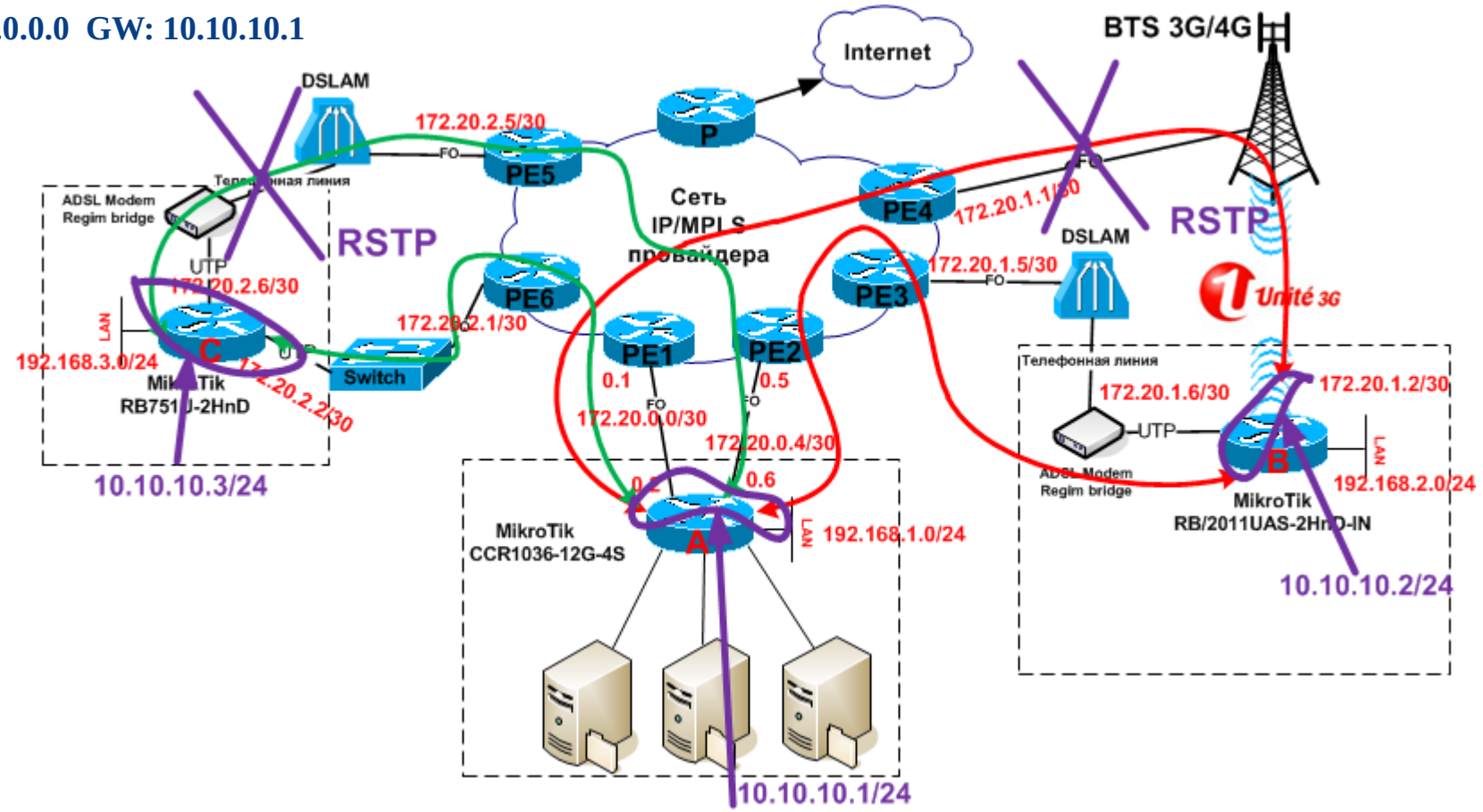


Логически у нас получится единый WAN-овский Layer 2 broadcast домен за счет того, что все туннели на центральном маршрутизаторе добавляются в одну bridge группу.



.

Чтоб локальные сети виделись между собой настраиваем статическую маршрутизацию:
Router A:
Dst: 192.168.2.0/24 GW: 10.10.10.2 // В сторону филиала “B”
Dst: 192.168.3.0/24 GW: 10.10.10.3 // В сторону филиала “C”
Router B и C:
Dst: 0.0.0.0 GW: 10.10.10.1



Безопасная передача данных

Трафик шифруем средствами IPSec.
В качестве Peer указываем IP адреса на Bridge интерфейсах!

Router A

```
/ip ipsec proposal
add auth-algorithms=md5 name=proposal1 pfs-group=modp768
/ip ipsec peer
add address=10.10.10.2/32 dh-group=modp768 enc-algorithm=aes-128 \
    hash-algorithm=md5 nat-traversal=no secret=12345678
/ip ipsec policy
add dst-address=192.168.2.0/24 proposal=proposal1 sa-dst-address=10.10.10.2 \
    sa-src-address=10.10.10.1 src-address=0.0.0.0/0 tunnel=yes
```

Router B

```
/ip ipsec proposal
add auth-algorithms=md5 name=proposal1 pfs-group=modp768
/ip ipsec peer
add address=10.10.10.1/32 dh-group=modp768 enc-algorithm=aes-128 \
    hash-algorithm=md5 nat-traversal=no secret=12345678
/ip ipsec policy
add dst-address=0.0.0.0/0 proposal=proposal1 sa-dst-address=10.10.10.1 \
    sa-src-address=10.10.10.2 src-address=192.168.2.0/24 tunnel=yes
```

Туннельный режим обязывает шифровать пакет полностью и инкапсулировать его в другой UDP пакет, чем обеспечивается его беспроблемная маршрутизация.

Спасибо за внимание,

Ваши вопросы?

Email:
andrei.marcov@moldtelecom.md
marcov.andrei@yandex.ru