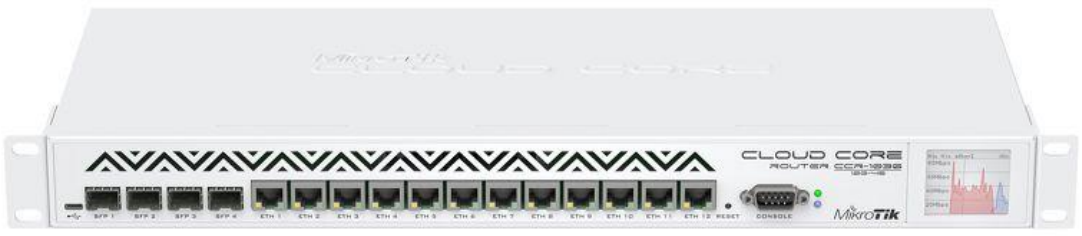
Построение отказоустойчивой транспортной сети VPN – L3, с использованием туннелей GRE over Ipsec, протоколов L2 RSTP, LACP , L3 VRRP, OSPF .

Сеть построена на базе маршрутизаторов MikroTik CCR-1036-12G-4S, RB-951Ui-2HnD. Оборудование установлено в Дата-Центре Национального Оператора АО“Молдтелеком” и на автотрассах Республики Молдова.



CCR-1036-12G-4S

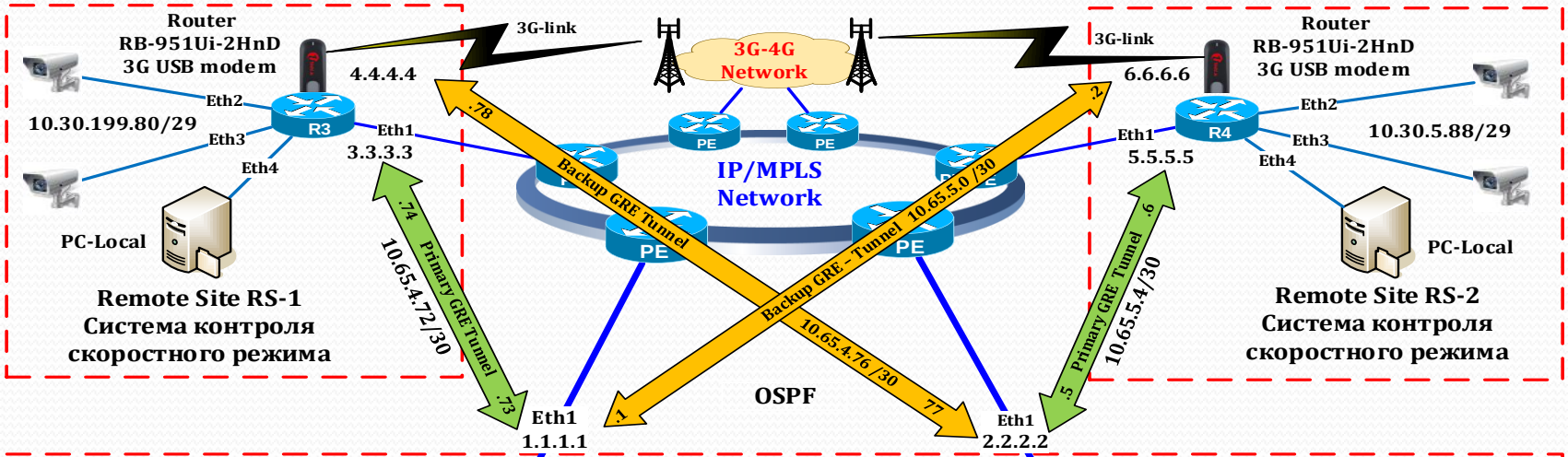
RB-951Ui-2HnD

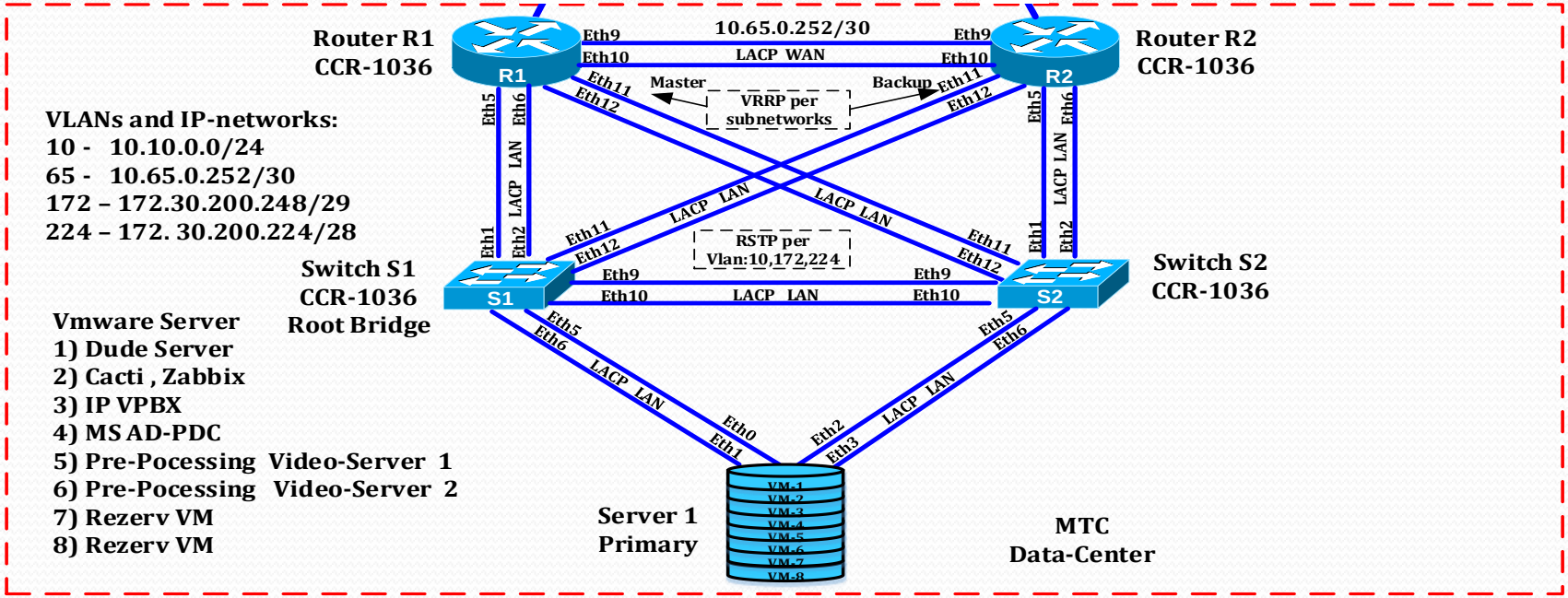
Об авторе

- Лелюхин Олег . Кишинёв, Республика Молдова
- Более 15 лет работаю в Национальном Операторе SA”Moldtelecom” .
- Проектирование корпоративных сетей и разработка новых сервисов.
- С MikroTik-ом работаю с 2009 года
- В компании насчитывается более 4000 MikroTik-ов
- Cisco CCNA, CCNP - Ассоциация DNT
- Cisco CCNA инструктор - SA “Moldtelecom”
- MTCNA - Aitec
- MTCRE - Aitec
- MTCWE - MikroTik-Trainings.com
- MUM-2013-Kishinev, MUM-2015-Moscow

Топология сети VPN – L3

Схема организации транспортной сети передачи данных для видеонаблюдения на автотрассах Республики Молдова.





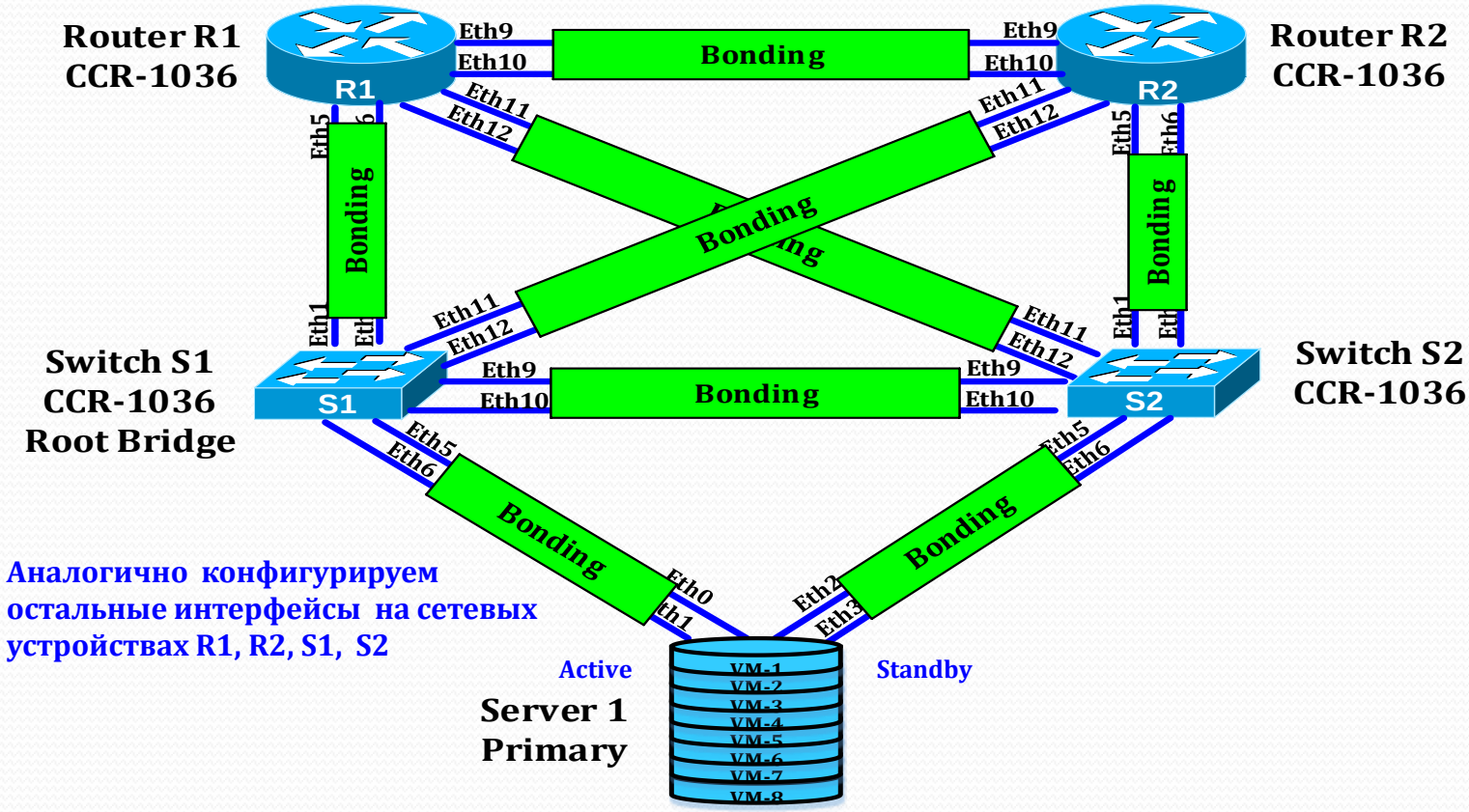
VLANs and IP-networks:
10 - 10.10.0.0/24
65 - 10.65.0.252/30
172 – 172.30.200.248/29
224 – 172. 30.200.224/28

Vmware Server
1) Dude Server
2) Cacti , Zabbix
3) IP VPBX
4) MS AD-PDC
5) Pre-Pocessing Video-Server 1
6) Pre-Pocessing Video-Server 2
7) Rezerv VM
8) Rezerv VM

Step-1. Bonding

Объединение двух физических Ethernet интерфейсов в один логический

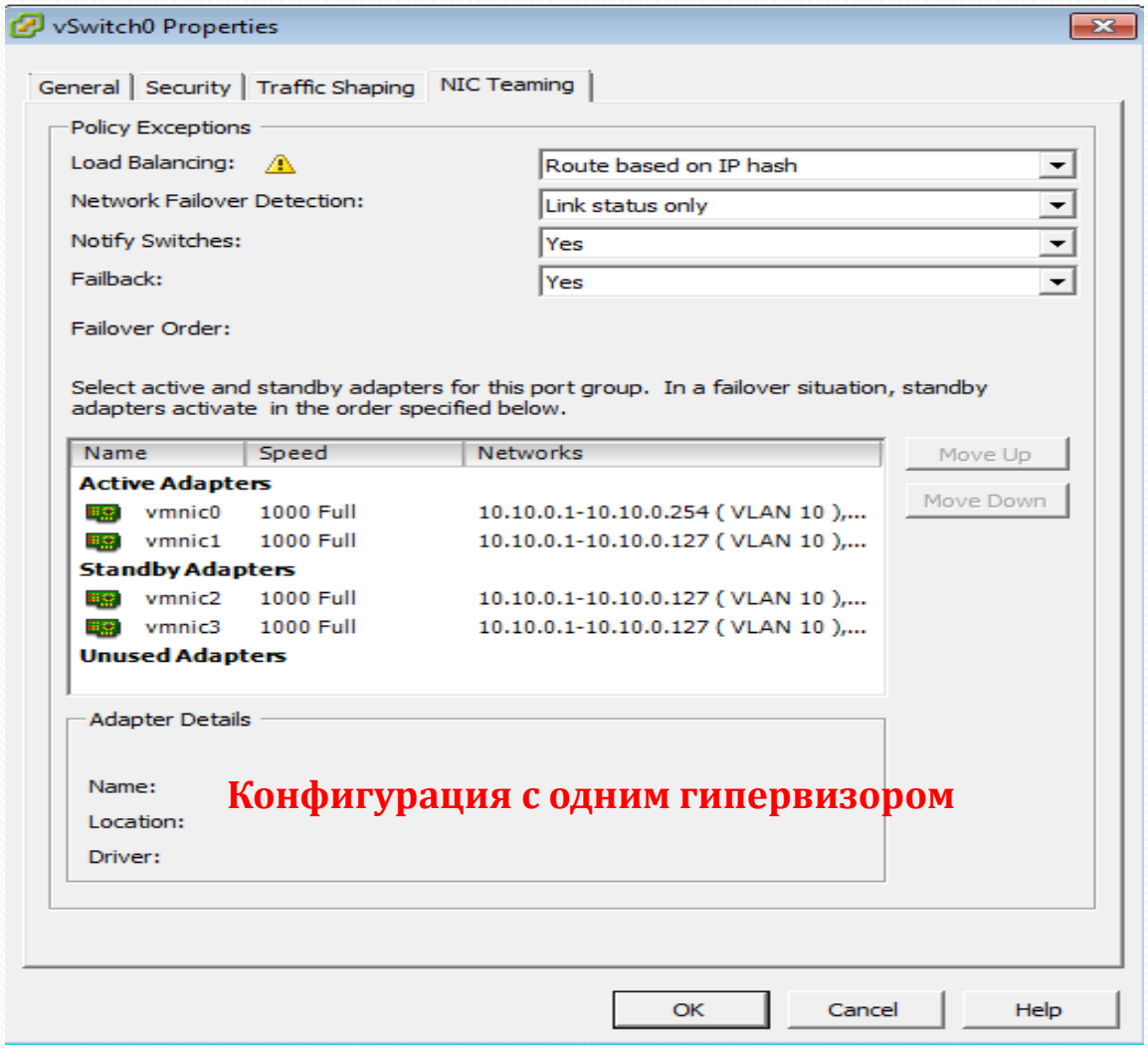
```
[admin@R1] /interface bonding> add mode=802.3ad name=Bonding_R1-R2 \
                slaves=ether9_R1-R2,ether10_R1-R2 transmit-hash-policy=layer-2-and-3
```




```
[admin@R2] /interface bonding> add mode=802.3ad name=bonding_R2-R1 \
                slaves=ether9_R2-R1,ether10_R2-R1 transmit-hash-policy=layer-2-and-3
```

Step-2. LACP

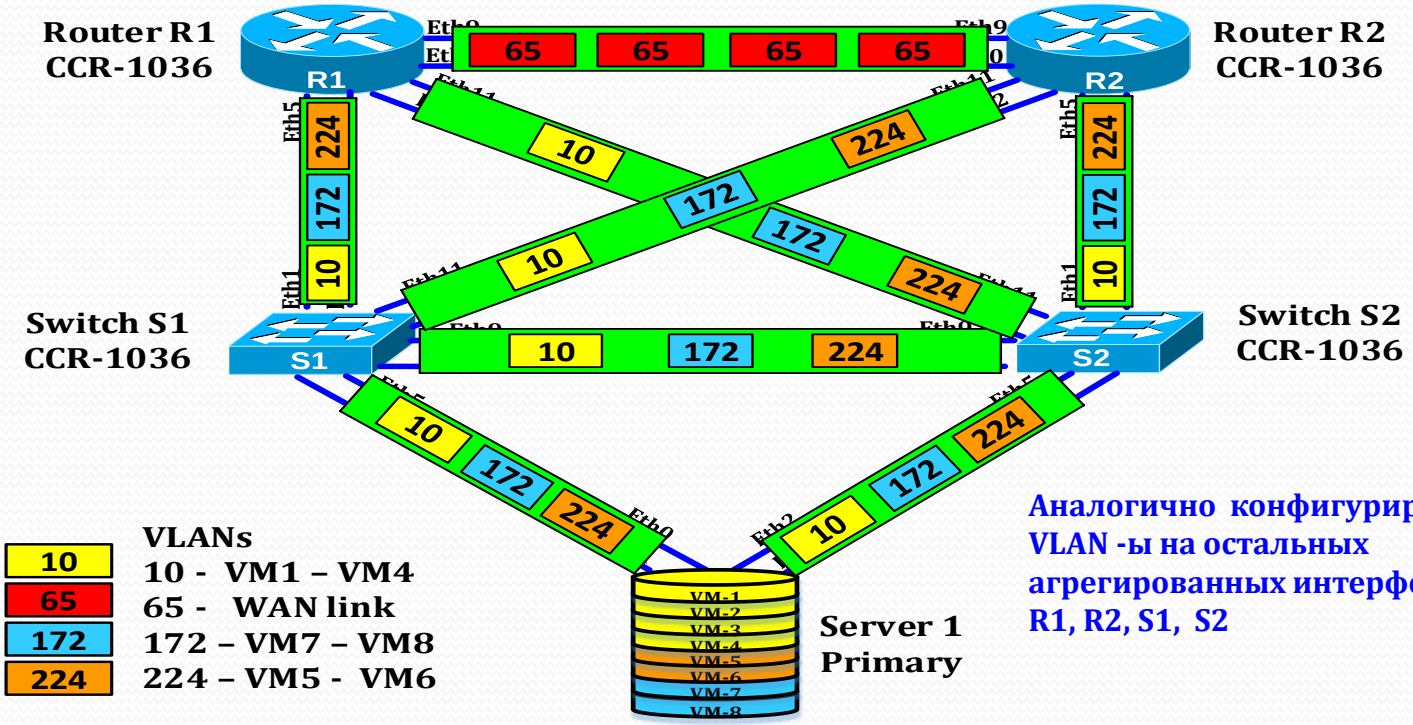
Объединение двух физических Ethernet интерфейсов в один логический на сервере виртуальных машин под управлением VMware vSphere ESXi



Step-3. VLANs

Конфигурирование VLAN-ов на Bonding интерфейсах для разделения сетевого трафика на L2. Tagged frames

```
[admin@R1] /interface vlan> add interface=Bonding_R1-S1 name=vlan10_bond_R1-S1 vlan-id=10
[admin@R1] /interface vlan> add interface=Bonding_R1_S2 name=vlan10_bond_R1-S2 vlan-id=10
```



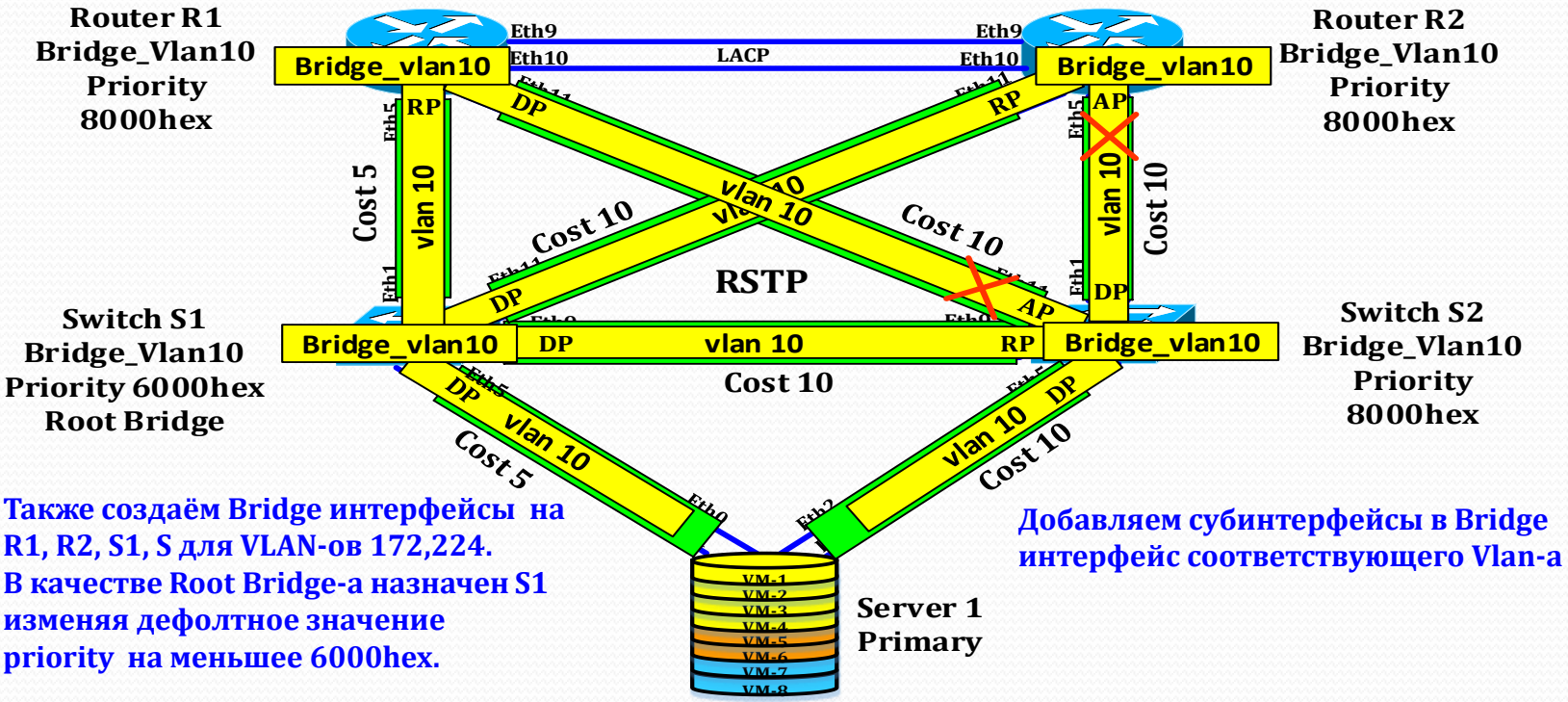
Аналогично конфигурируем VLAN -ы на остальных агрегированных интерфейсах R1, R2, S1, S2

```
[admin@R2] /interface vlan> add interface=bonding_R2-S1 name=vlan10_bond_R2-S1 vlan-id=10
[admin@R2] /interface vlan> add interface=bonding_R2-S2 name=vlan10_bond_R2-S2 vlan-id=10
```

Step-4. Bridge and RSTP

Конфигурирование Bridge-интерфейсов и добавление субинтерфейсов для создания щироковещательных доменов в соответсвующих VLAN-ах. Настройка протокола RSTP и назначение “Root Bridge”-а.

```
[admin@S1] /interface bridge>  add admin-mac=4C:5E:0C:6A:11:D6 auto-mac=no mtu=1500 \
        name=bridge_Vlan10  priority=0x6000
[admin@S2] /interface bridge>  add admin-mac=4C:5E:0C:63:88:EE auto-mac=no mtu=1500 name=bridge_Vlan10
```



Также создаём Bridge интерфейсы на R1, R2, S1, S для VLAN-ов 172,224. В качестве Root Bridge-а назначен S1 изменяя дефолтное значение priority на меньшее 6000hex.

Добавляем субинтерфейсы в Bridge интерфейс соответствующего Vlan-а

```
admin@S1] /interface bridge port>
add bridge=bridge_Vlan10 interface=vlan10_bond-S1-S2
add bridge=bridge_Vlan10 interface=vlan10_bond-S1-R1 path-cost=5
add bridge=bridge_Vlan10 interface=vlan10_bond-S1-R2
add bridge=bridge_Vlan10 interface=vlan10_bond-S1-Server1
```

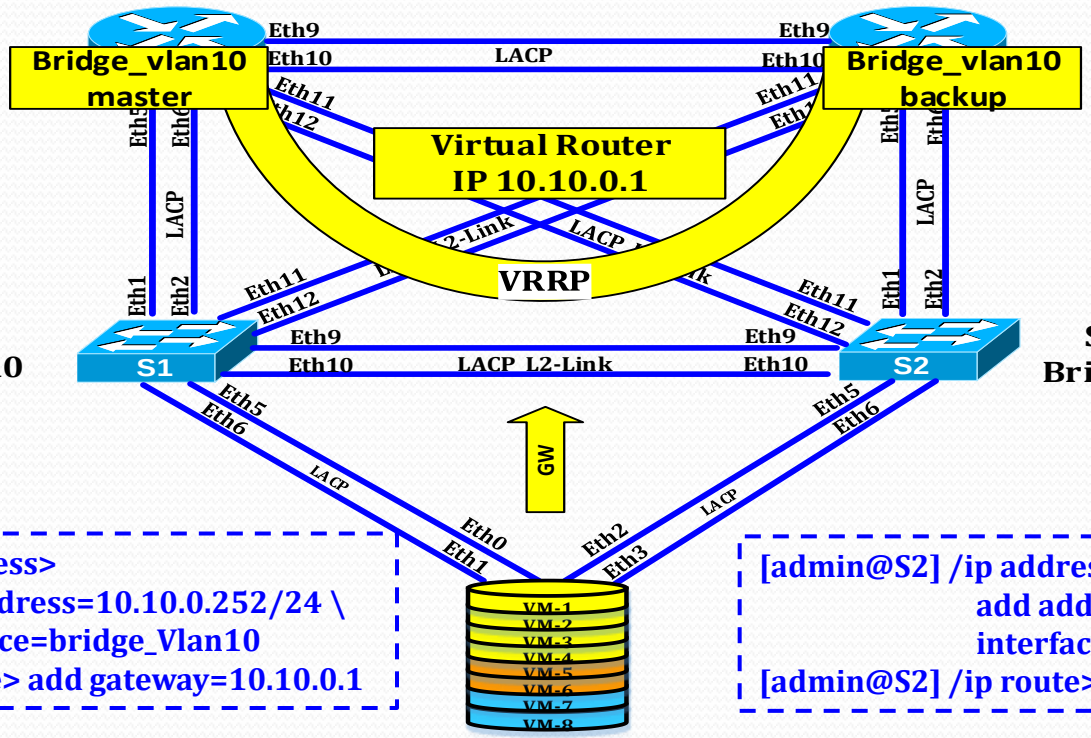
```
admin@S2] /interface bridge port>
add bridge=bridge_Vlan10 interface=vlan10_bond-S2-S1
add bridge=bridge_Vlan10 interface=vlan10_bond-S2-R1
add bridge=bridge_Vlan10 interface=vlan10_bond-S2-R2
add bridge=bridge_Vlan10 interface=vlan10_bond-S2-Server1
```

Step-5. LAN IP addressing. VRRP

Присваивание IP-адресов Bridge-интерфейсам и активация протокола VRRP. Назначение основного "Master" и резервного "Backup" шлюза.

```
[admin@R1] /ip address> add address=10.10.0.2/24 interface=Bridge_Vlan10
[admin@R2] /ip address> add address=10.10.0.3/24 interface=Bridge_Vlan10
```

Router R1
Bridge_Vlan10
IP address
10.10.0.2/24



Router R2
Bridge_Vlan10
IP address
10.10.0.3/24

Switch S1
Bridge_Vlan10

Switch S2
Bridge_Vlan10

```
[admin@S1] /ip address>
                add address=10.10.0.252/24 \
                interface=bridge_Vlan10
[admin@S1] /ip route> add gateway=10.10.0.1
```

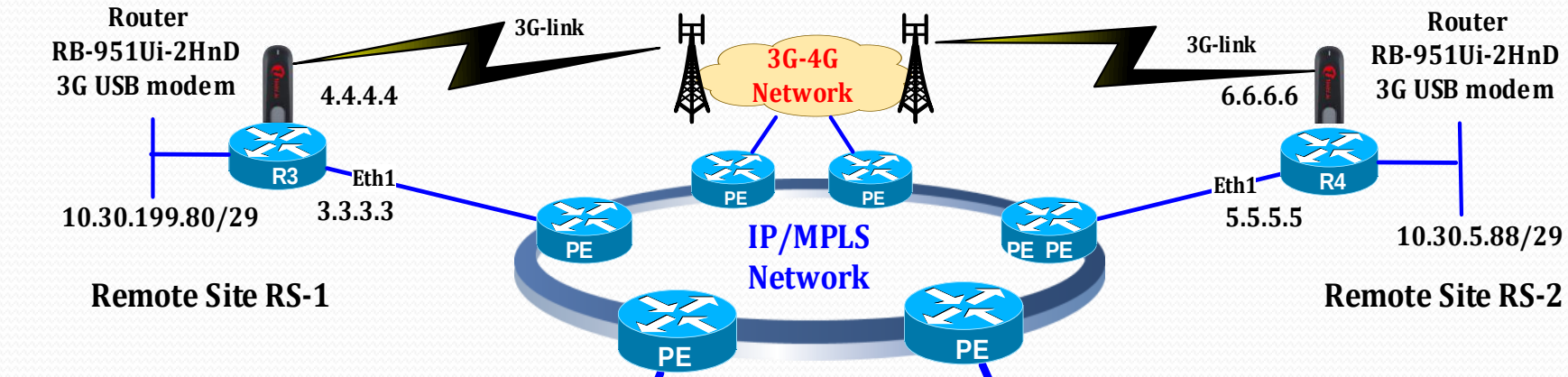
```
[admin@S2] /ip address>
                add address=10.10.0.253/24 \
                interface=bridge_Vlan10
[admin@S2] /ip route> add gateway=10.10.0.1
```

```
[admin@R1] /interface vrrp> add interface=Bridge_Vlan10  \
                name=VRRP_10 priority=254 version=2 vrid=10
[admin]@R1 /ip address> add address=10.10.0.1/32  \
                interface=VRRP_10
```

```
[admin@R2] /interface vrrp> add interface=bridge_Vlan10  \
                name=vrrp-10 version=2 vrid=10
[admin]@R2 /ip address> add address=10.10.0.1/32  \
                interface=VRRP_10
```

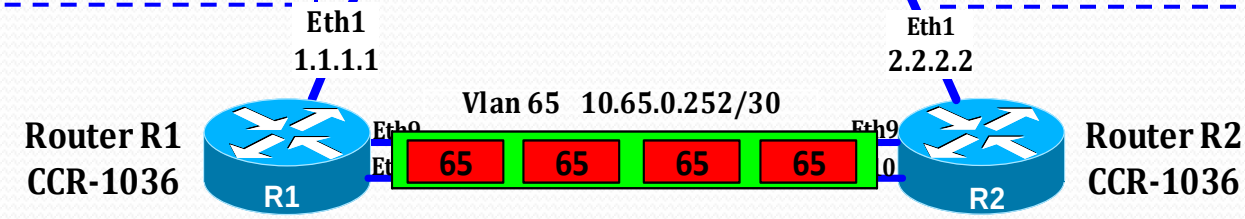
Step-6. WAN IP addressing.

```
[admin@R3] /ip address> add address=10.30.199.81 /29 interface=Bridge_LAN
[admin@R3] /ip dhcp-client> add default-route-distance=0 dhcp-options=hostname,clientid disabled=no \
                interface=Ether1
[admin@R3] /interface ppp-client>add add-default-route=yes allow=pap,chap,mschap1,mschap2 apn=internet.unite.md \
data-channel=0 default-route-distance=2 dial-command=ATDT dial-on-demand=no disabled=no info-channel=0 \
keepalive-timeout=30  max-mru=1500 max-mtu=1500 modem-init="" mrru=disabled name=ppp-out1 \
   null-modem=no password="" phone="" pin="" port=usb1 profile=default  use-peer-dns=yes user=""
[admin@R3] / ip route> add distance=1 dst-address=2.2.2.2/32 gateway=ppp-out1
```




```
[admin@R1] /ip dhcp-client>
        add default-route-distance=0 \
        dhcp-options=hostname,clientid \
        disabled=no   interface=Ether1
/ip address> add address=10.65.0.254/30 \
                interface=vlan65_bond_R1-R2
```

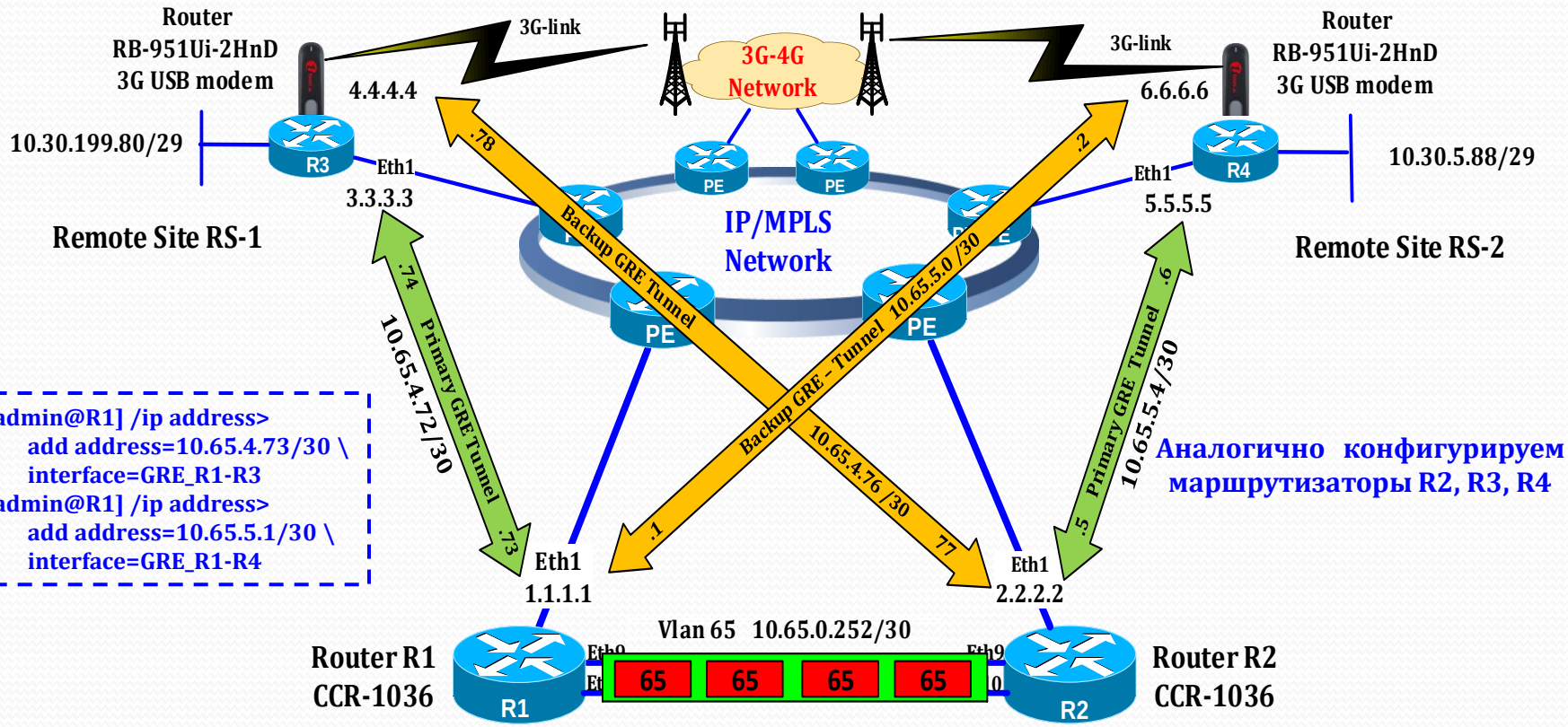
```
[admin@R2] /ip dhcp-client>
        add default-route-distance=0 \
        dhcp-options=hostname,clientid \
        disabled=no   interface=Ether1
/ip address> add address=10.65.0.253/30 \
                interface=vlan65_bond_R2-R1
```



Step-7. GRE-Tunnels.

Подключение к операторской транспортной сети .
Организация сети VPN-L3 типа “Site-to-Site ”

```
[admin@R1] /interface gre> add clamp-tcp-mss=no dscp=0 keepalive=10,3 local-address=1.1.1.1 mtu=1476 \
   name=GRE_R1-R3 remote-address=4.4.4.4
[admin@R1] /interface gre> add clamp-tcp-mss=no dscp=0 keepalive=10,3 local-address=1.1.1.1 mtu=1476 \
   name=GRE_R1-R4 remote-address=6.6.6.6
```



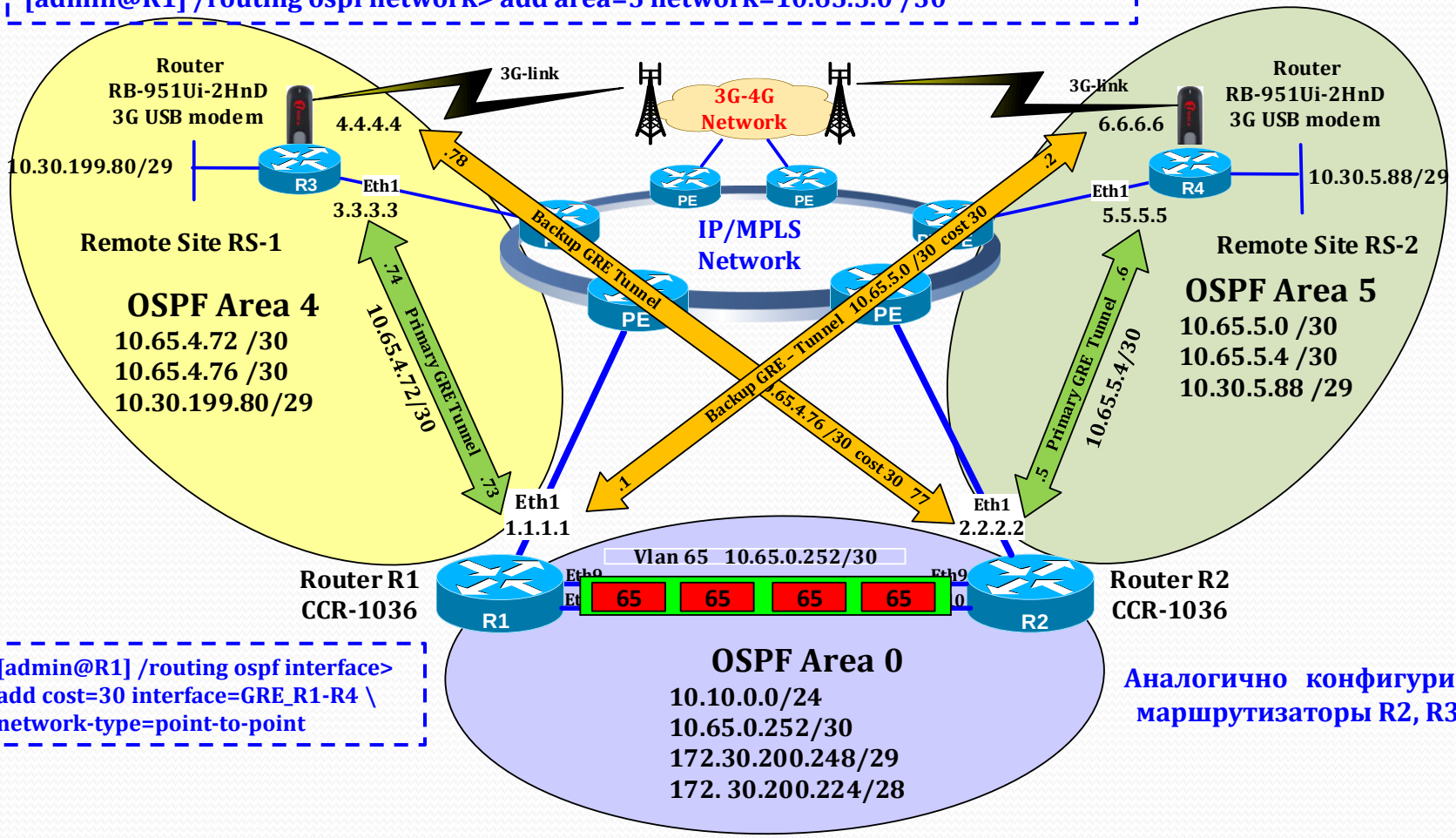

```
[admin@R1] /ip address>
     add address=10.65.4.73/30 \
     interface=GRE_R1-R3
[admin@R1] /ip address>
     add address=10.65.5.1/30 \
     interface=GRE_R1-R4
```

Аналогично конфигурируем маршрутизаторы R2, R3, R4

Step-8. Multiarea OSPF.

Динмическая маршрутизация
на базе протокола OSPF

```
[admin@R1] /routing ospf area> add area-id=0.0.0.4 name=area4
[admin@R1] /routing ospf area> add area-id=0.0.0.5 name=area5
[admin@R1] /routing ospf network> add area=backbone network=10.10.0.0/24
[admin@R1] /routing ospf network> add area=4 network=10.65.4.72 /30
[admin@R1] /routing ospf network> add area=5 network=10.65.5.0 /30
```



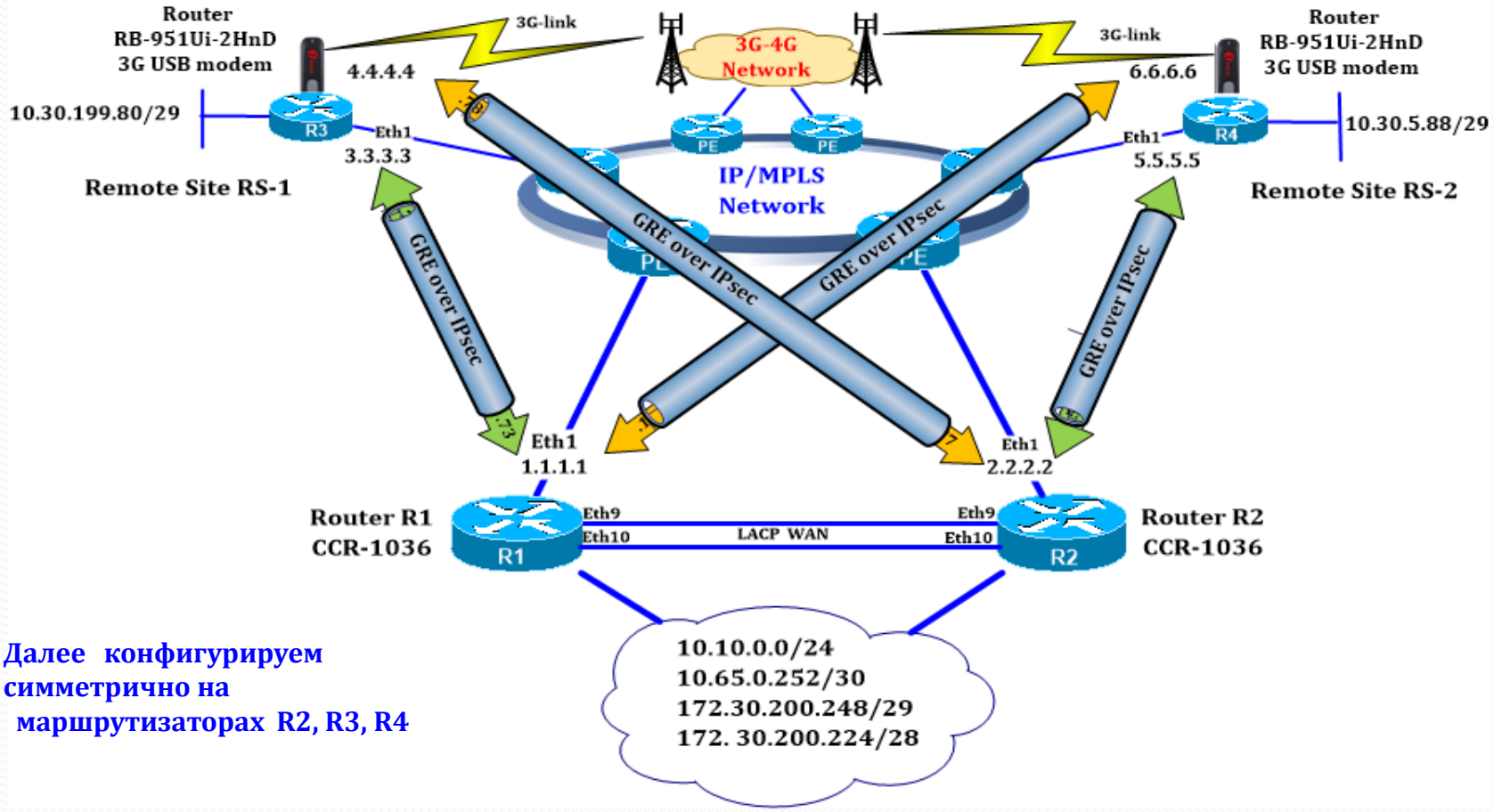

```
[admin@R1] /routing ospf interface>
add cost=30 interface=GRE_R1-R4 \
network-type=point-to-point
```

Аналогично конфигурируем маршрутизаторы R2, R3, R4

Step-9. Ipsec tunnels.

Шифрование передаваемых данных при помощи Ipsec туннелей (Transport mode).

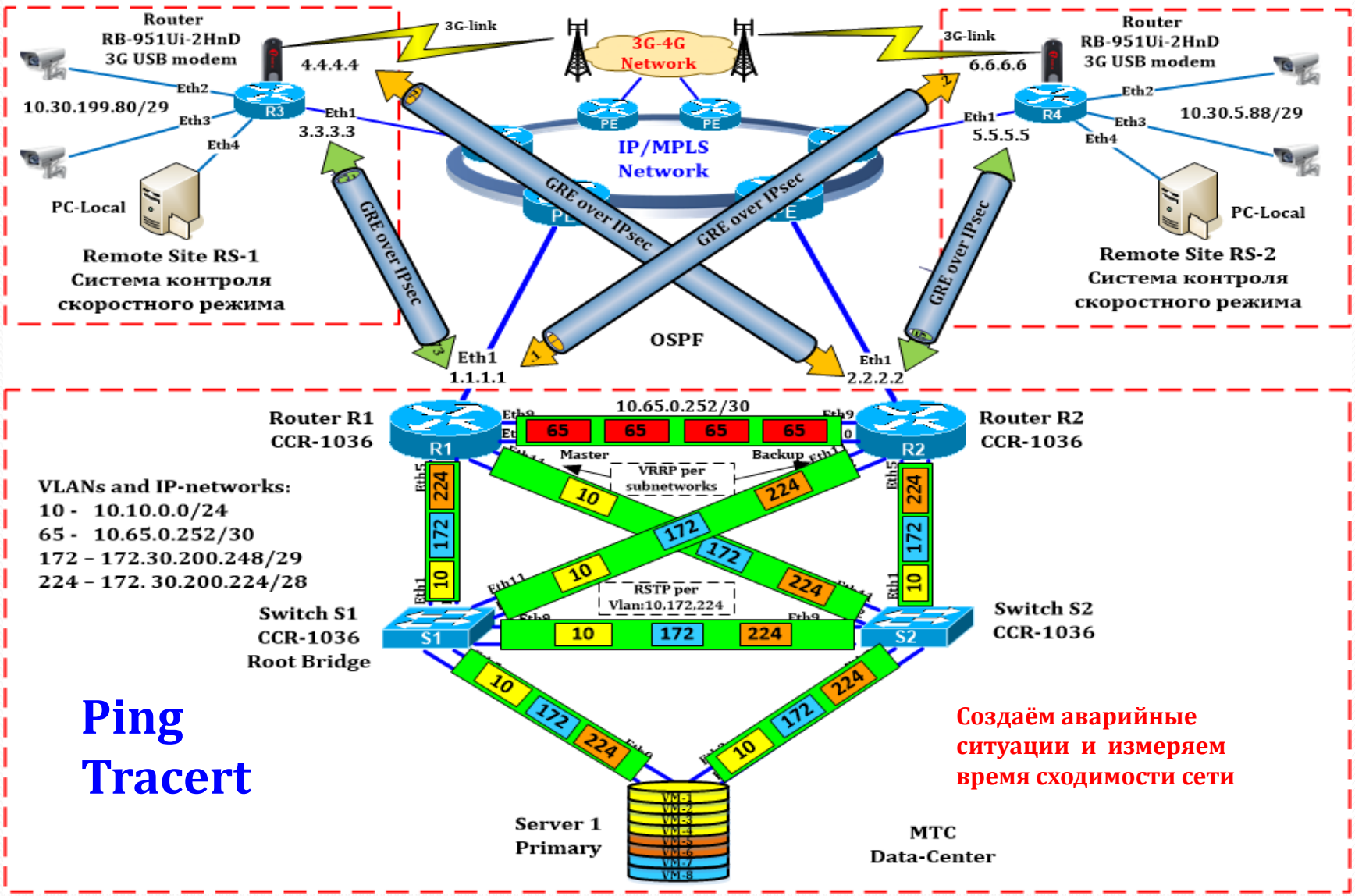
```
[admin@R1] /ip ipsec proposal>add enc-algorithms=3des lifetime=1h name=MUM2015
[admin@R1] /ip ipsec peer> add address=3.3.3.3/32 dpd-interval=disable-dpd  dpd-maximum-failures=3\
           enc-algorithm=3des lifetime=1h policy-group=default  secret=MikroTik
[admin@R1] /ip ipsec policy>add  dst-address=3.3.3.3/32   proposal=MUM2015  sa-dst-address=3.3.3.3 \
           sa-src-address=1.1.1.1   src-address=1.1.1.1/32
```



Далее конфигурируем симметрично на маршрутизаторах R2, R3, R4

Step-10. Verifying

Проверка отказоустойчивости сети.
Устранение неисправностей.



Спасибо за внимание

Задавайте вопросы
или
пишите на E-Mail
leliuhin@moldtelecom.md

oleliuhin@gmail.com

I will be back !