MikroTik

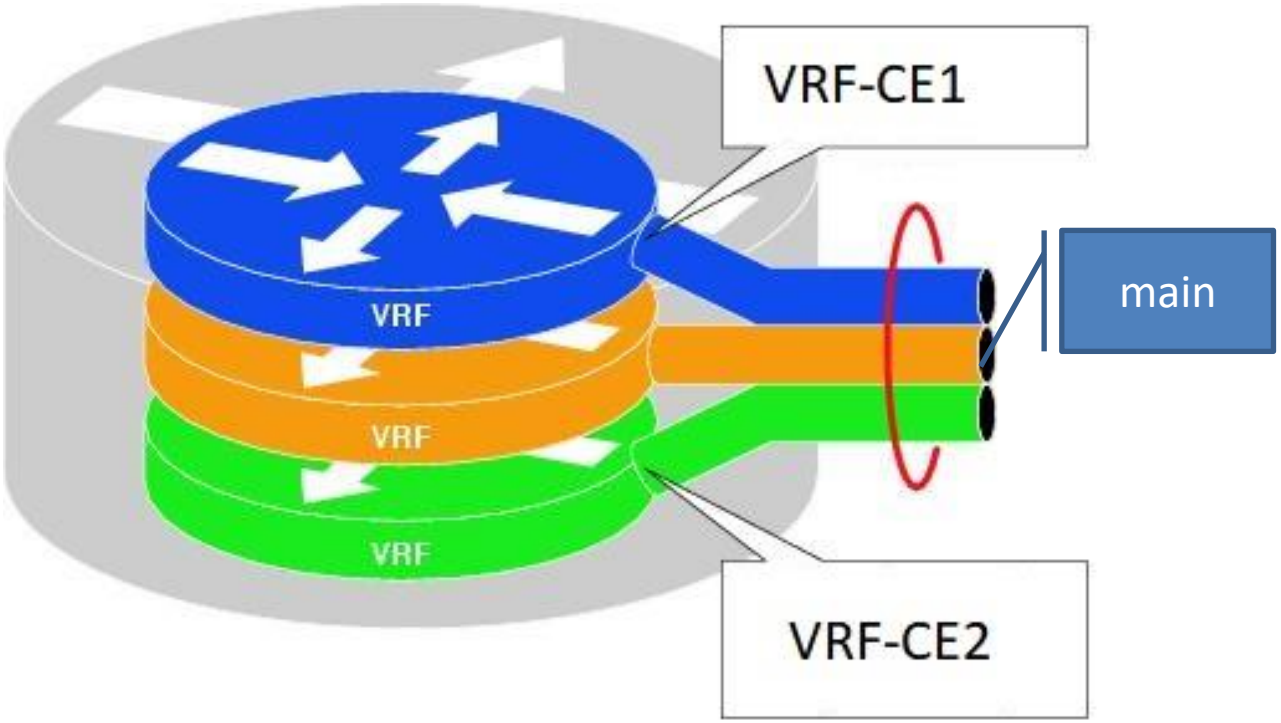
VRF Lite

Теория и практика

Брыксин Анатолий
anatoly.bryksin@gmail.com

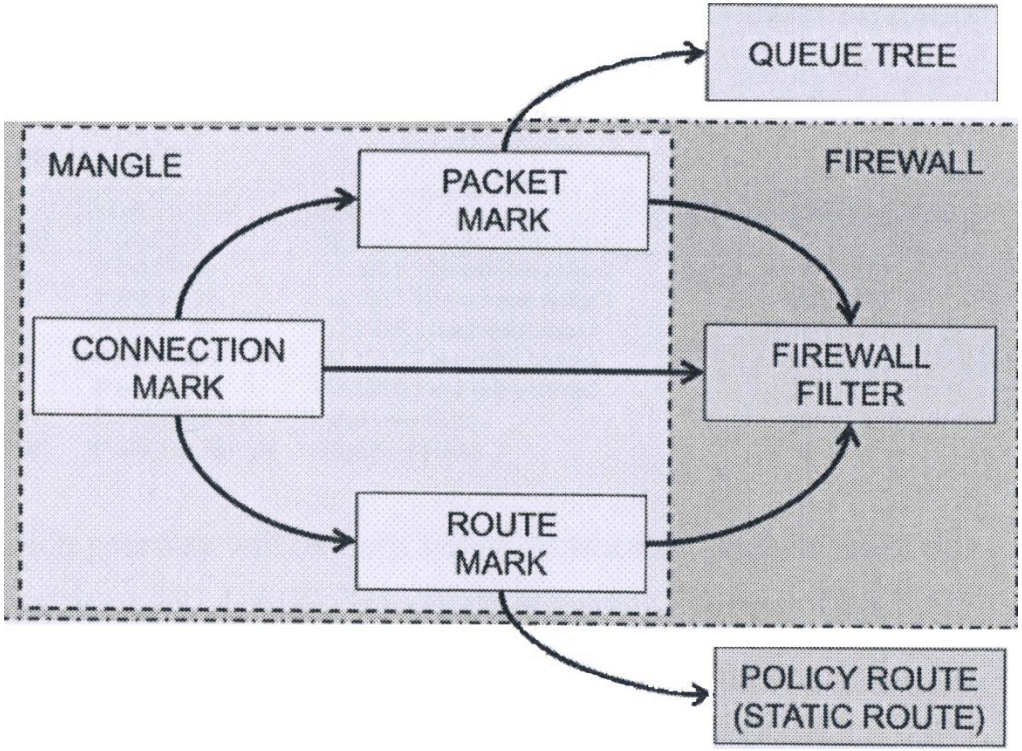
MTCRE: 1703RE117
MTCINE:1703INE7137

Понятие VRF



Интерфейсы
Маршруты
ARP-Таблицы

Маркировка трафика



Маркировки действуют только в пределах маршрутизатора

Конфигурирование VRF

Создание VRF

- /ip route vrf add routing-mark=<VRF-NAME> interface=<list-interfaces>
  - <interfaces> - перечень интерфейсов входящих в VRF
  - <VRF-NAME> - метка, для маркировки маршрутов из VRF

Просмотр таблицы маршрутизации VRF

- /ip route print where routing-mark=”<VRF-NAME>”

  Пример:

  /ip route print where routing-mark~”<pattern>”

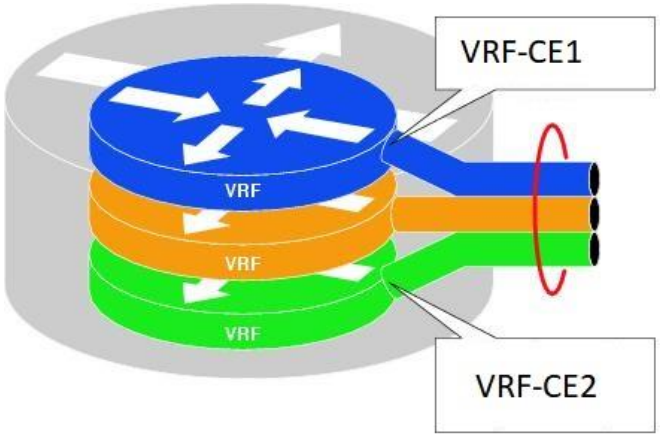
Static Route(Теория)

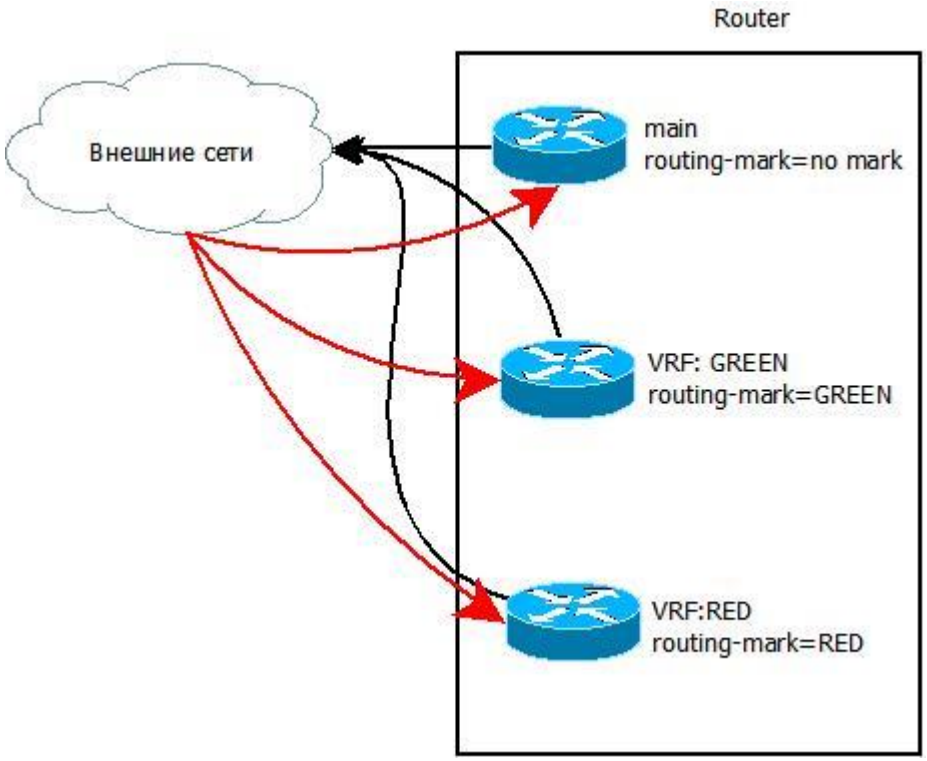
- /ip route add dst-address=<network>/<netmask> gateway=<gateway> distance=<distance> check-gateway=ping/arp routing-mark=<VRF-Name>

Пример

- /ip route add dst-address=192.168.0.0/16 gateway=1.1.1.1 routing-mark=<VRF-Name>
- /ip route add gateway=1.1.1.1 routing-mark=<VRF-Name>

Организация доступа в Интернет





Route Leaking

- В качестве шлюза для маршрутизации можно использовать:
  - <ip-address>@main – адрес из таблицы main
  - <ip-address>%interface – адрес и интерфейс
  - <interface> - если сеть подключена к данному маршрутизатору.

Route Leaking (Примеры)

Маршрутизация через таблицу main

- /ip route add dst-address=0.0.0.0/0 gateway=1.1.1.1@main routing-mark=<VRF-Name>

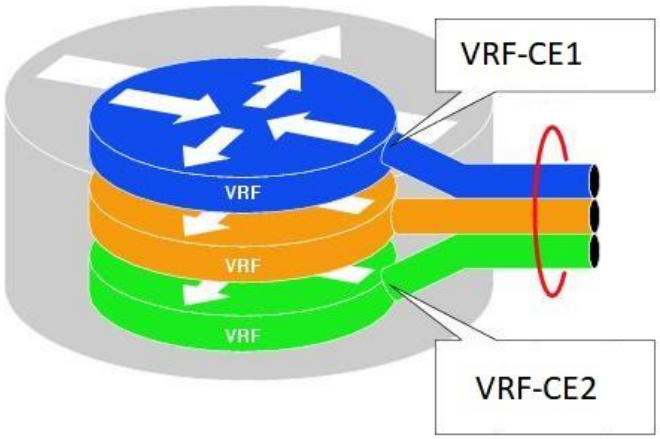
Маршрутизация через связку шлюз и интерфейс

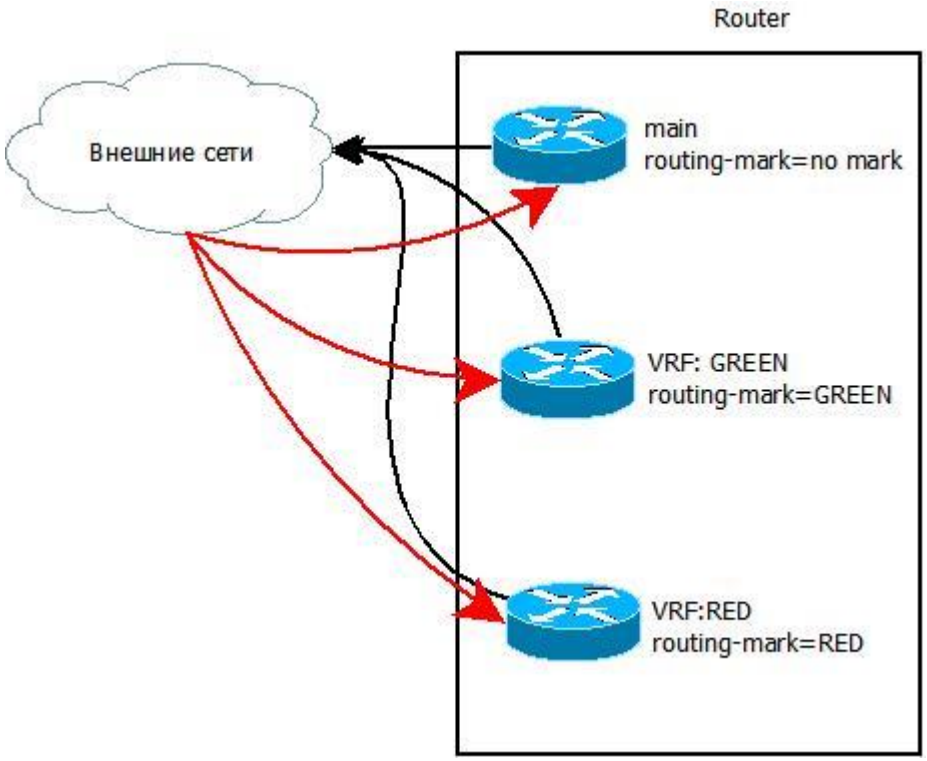
- /ip route add dst-address=0.0.0.0/0 gateway=2.2.2.2%MTS routing-mark=<VRF-Name>

Маршрутизация через интерфейс (direct connect)

- /ip route add dst-address=192.168.1.100 gateway=ether2 routing-mark=<VRF-Name>

Организация доступа в Интернет

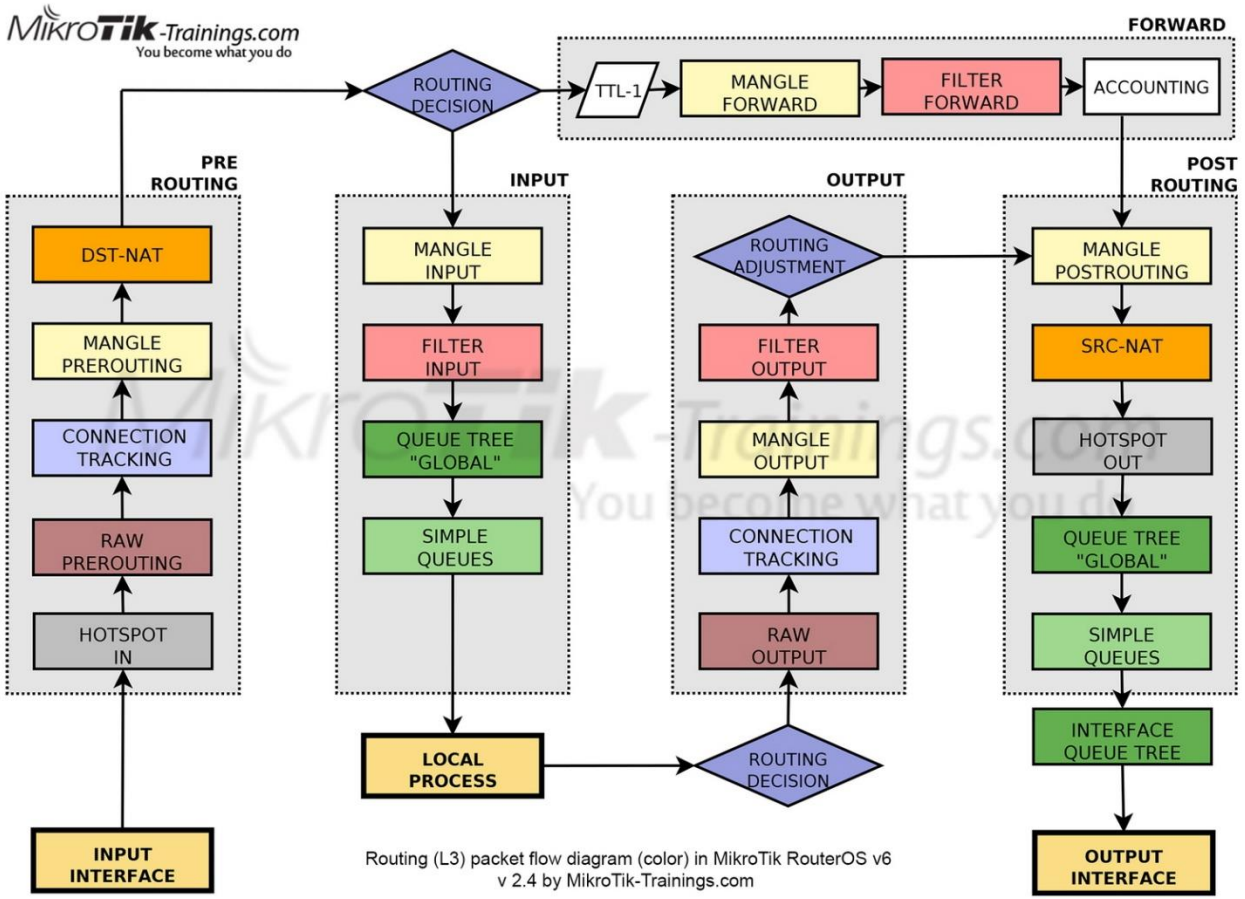




Критерий для возврата в VRF

1) ip,address,порт
2) Connection mark

Mikrotik Data Flow Diagram



Критерии для возврата в VRF

1) ip адрес , порт назначения, протокол tcp/ip, который использует публикуемый сервис
2) Маркировка соединения(connection mark)

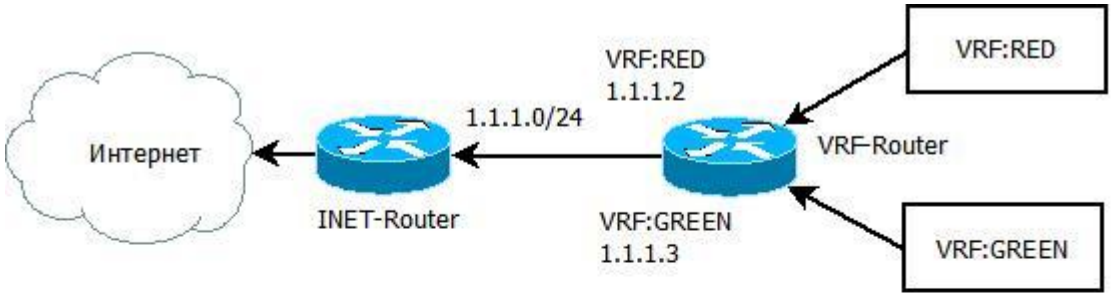
Route Leaking (возврат в VRF)

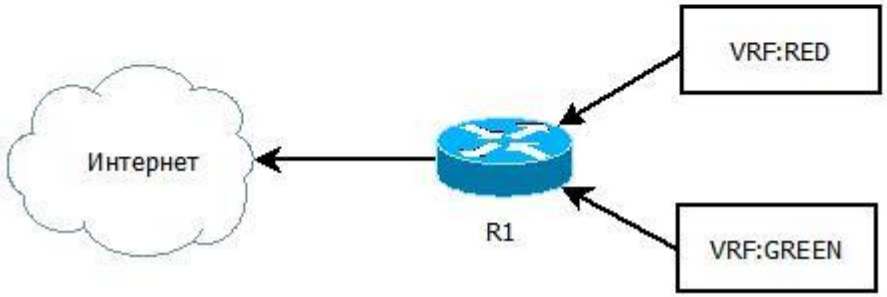
- /ip firewall mangle add chain=prerouting in-interface-list=WAN

  [….список критериев….]

  action=routing-mark new-routing-mark=<VRF-Name>

Организация доступа в интернет из VRF





Организация доступа к сервисам VRF из сети интернет

- Входящий трафик в VRF должен приобрести маркировку <VRF-Name>
  /ip firewall mangle add action=prerouting

  […. Критерии….] **ip(внешний)/порт(**

  action=routing-mark **new-routing-mark=<VRF-Name>**
- Правило DST-NAT
  /ip firewall nat add chain=dst-nat

  […. Критерии….] ip/port(внешний) -> ip/port(внутренний)

  action=dst-nat to-addresses=<ip(внутренний)> to-ports=<port(внутренний)>

- NAT для исходящего трафика
  /ip firewall nat add chain-src-nat **routing-mark=<VRF-Name>** out-interface-list=WAN action=masquerade

Организация доступа в интернет из VRF

- Промаркировать исходящие соединения из VRF
  /ip firewall mangle
  add action=mark-connection chain=postrouting
  new-connection-mark=VRF-Name-CONN routing-table=VRF-CE1

- Правило NAT для исходящих соединений из VRF
  /ip firewall nat
  add action=masquerade chain=srcnat out-interface=WAN routing-mark=VRF-CE1

- Правило для возврата пакетов для промаркированных соединений в VRF
  /ip firewall mangle
  add action=mark-routing chain=prerouting
  connection-mark=VRF-Name-CONN new-routing-mark=VRF-Name

VRF QOS

/ip firewall mangle add action=mark-packet chain=prerouting comment=SHAPE:VRF-NAME **routing-mark=VRF-NAME** **new-packet-mark=VRF-NAME** passthrough=yes

/queue simple

add dst=WAN1 max-limit=2M/2M name=VRF-NAME-WAN1 **packet-marks=VRF-NAME** target=""

add dst=WAN2 max-limit=2M/2M name=VRF-NAME-WAN2 **packet-marks=VRF-NAME** target=""

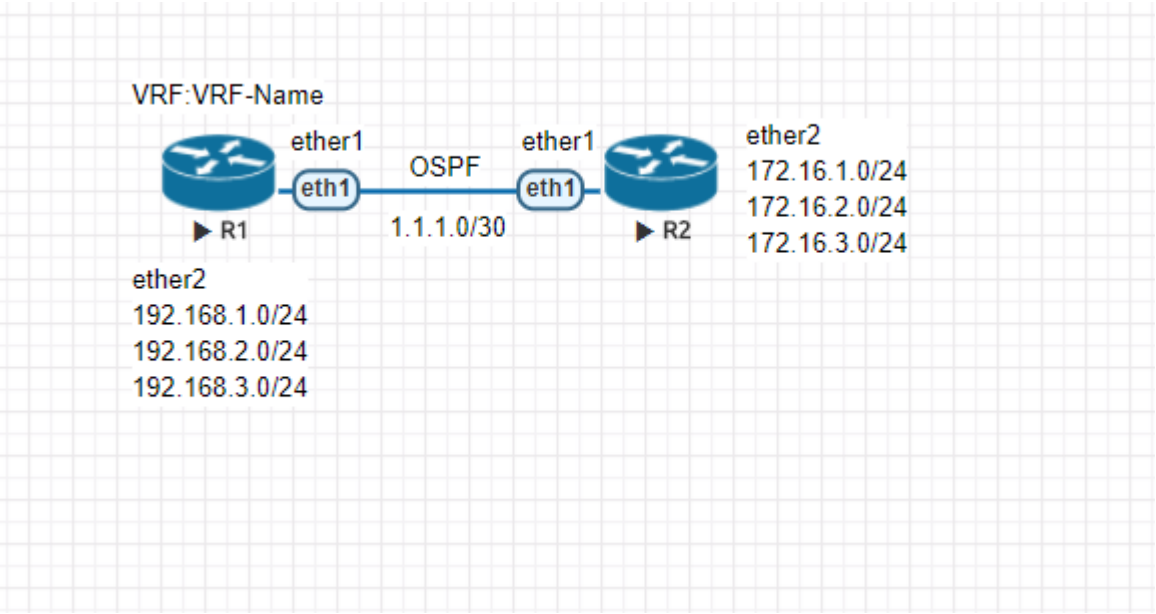
Добавление динамических маршрутов (CPE PE)(OSPF, BGP)

В ROS имеется возможность интеграции с протоколами динамической маршрутизации OSPF,BGP

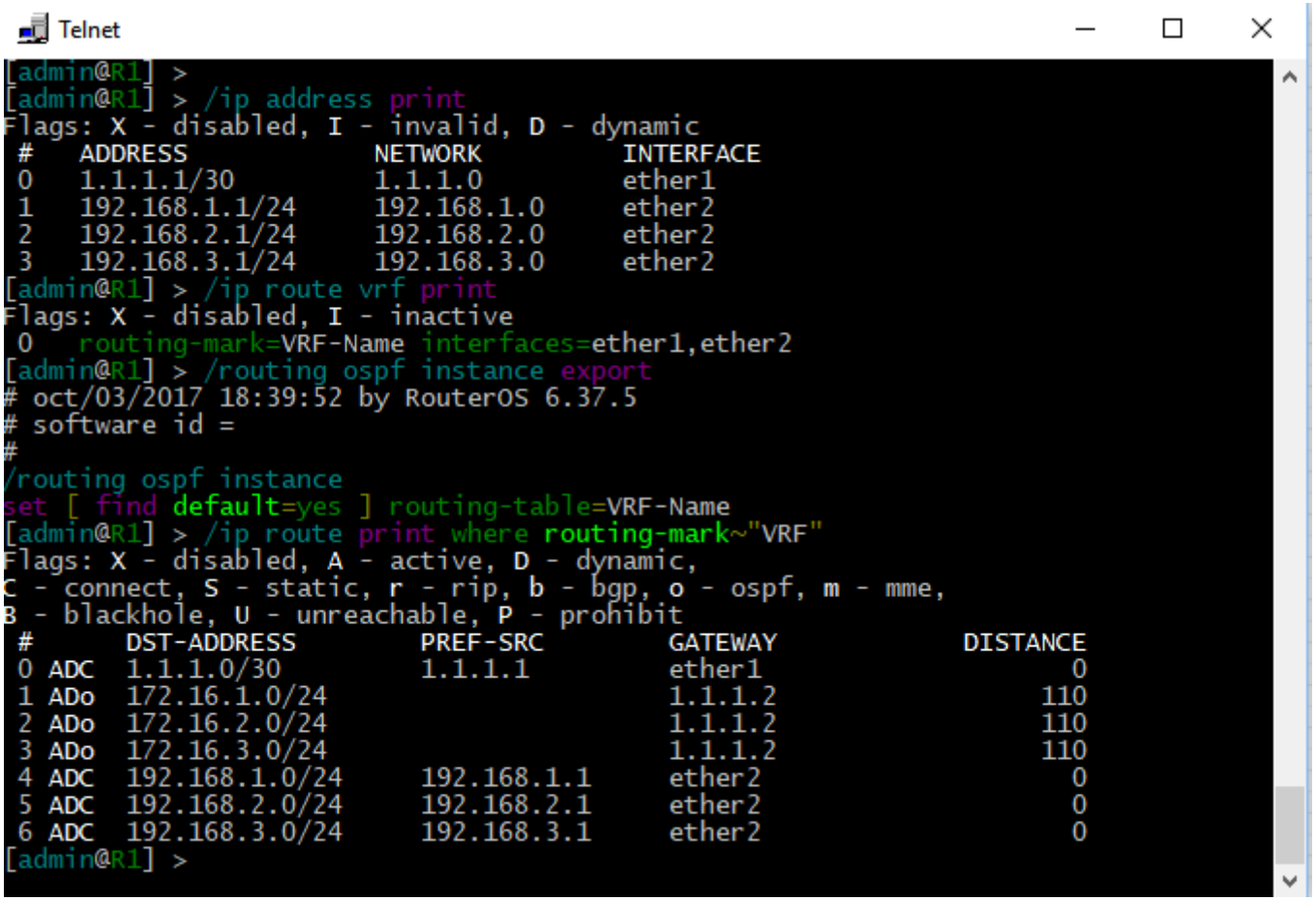
- /routing ospf instance set 0 routing-mark=”<VRF-Name>”
- /routing bgp instance set 0 routing-mark=”<VRF-Name>”

Пример взаимодействия – соединение с оборудованием с поддержкой OSPF (Switch L3, Quagga, …..)

VRF:OSPF (Пример)



VRF:OSPF (Example)



Troubleshooting

VRF Troubleshutting

- /ping <address> routing-mark=”<NAME>”
- /ip route check dst address=<address> routing-mark=”<NAME>”
- /tool traceroute address=<ip> routing-mark=”<NAME>”

Безопасность

Gateway через VRF недоступны по L3, но доступны по L2

Если отдаете VRF во враждебную среду отключаем

/tool mac-server на vrf интерфейсах
/ip neighbor discovery interface/