MULTIWAN НА ROUTEROS
РЕАЛИЗАЦИЯ, ПРОБЛЕМЫ, РЕШЕНИЯ

Solution.
Production.
Warranty.

MikroTik

официальный дистрибьютор

www.spw.ru

Об авторе

- Илья Князев. Санкт-Петербург, Россия.
- Mikrotik Certified Trainer [TR0309]
- Другие сертификаты Mikrotik
  - MTCNA
  - MTCTCE
  - MTCWE
  - MTCUME
  - MTCRE
  - MTCINE

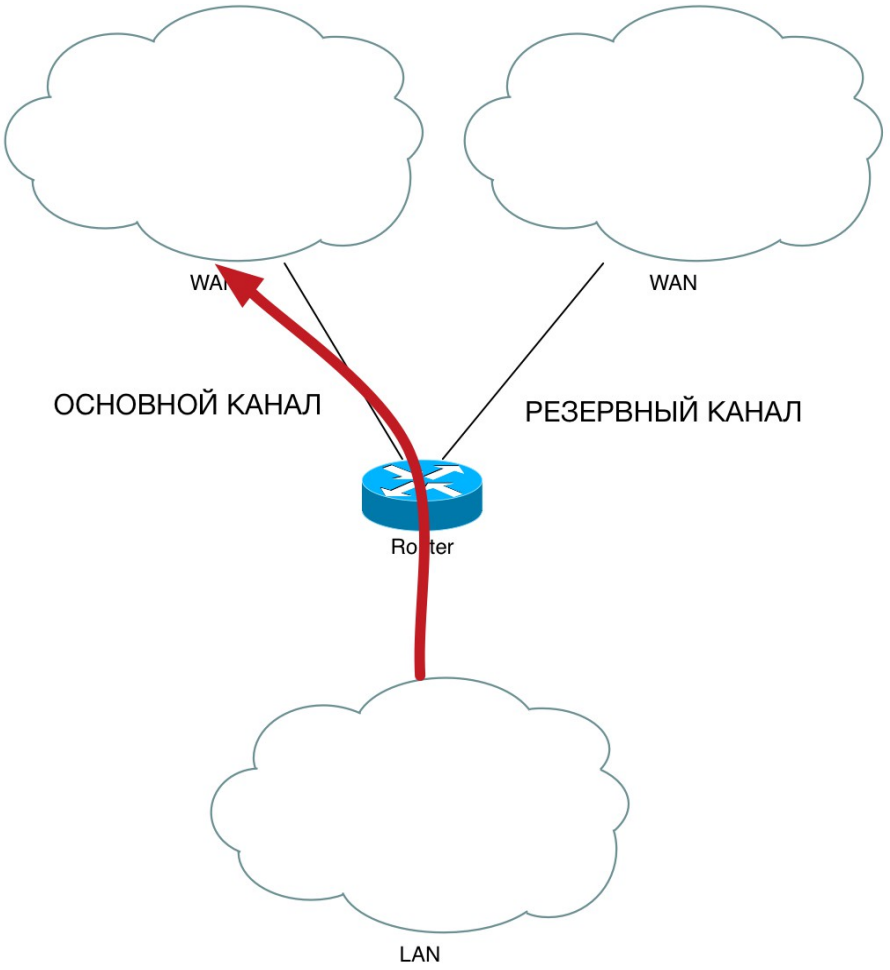
Зачем нужен MultiWAN?

- Для резервирования каналов.
- Для распределения нагрузки между несколькими каналами передачи данных

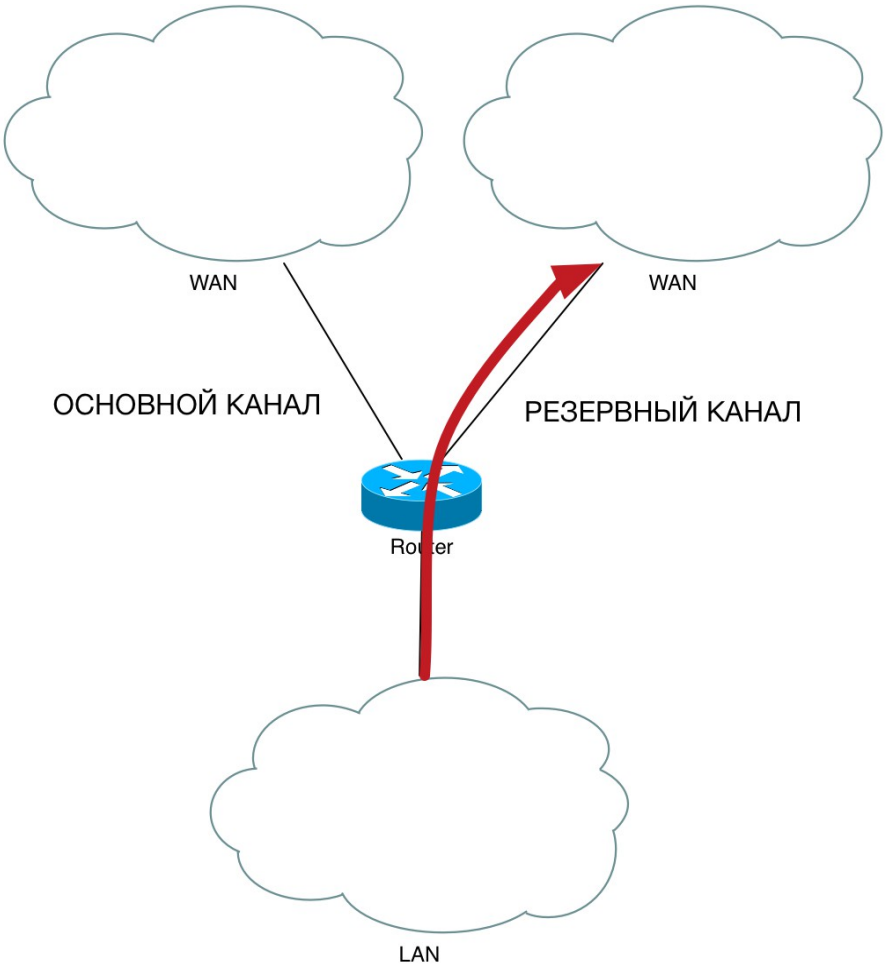
Вариант реализации MultiWAN Active/backup

- В этом случае трафик всегда направляется в основной канал, если он исправен.
- Если основной канал становится недоступным — трафик направляется в резервный канал, пока не будет восстановлен основной.

Резервирование канала



ОСНОВНОЙ КАНАЛ ИСПРАВЕН



ОСНОВНОЙ КАНАЛ НЕДОСТУПЕН

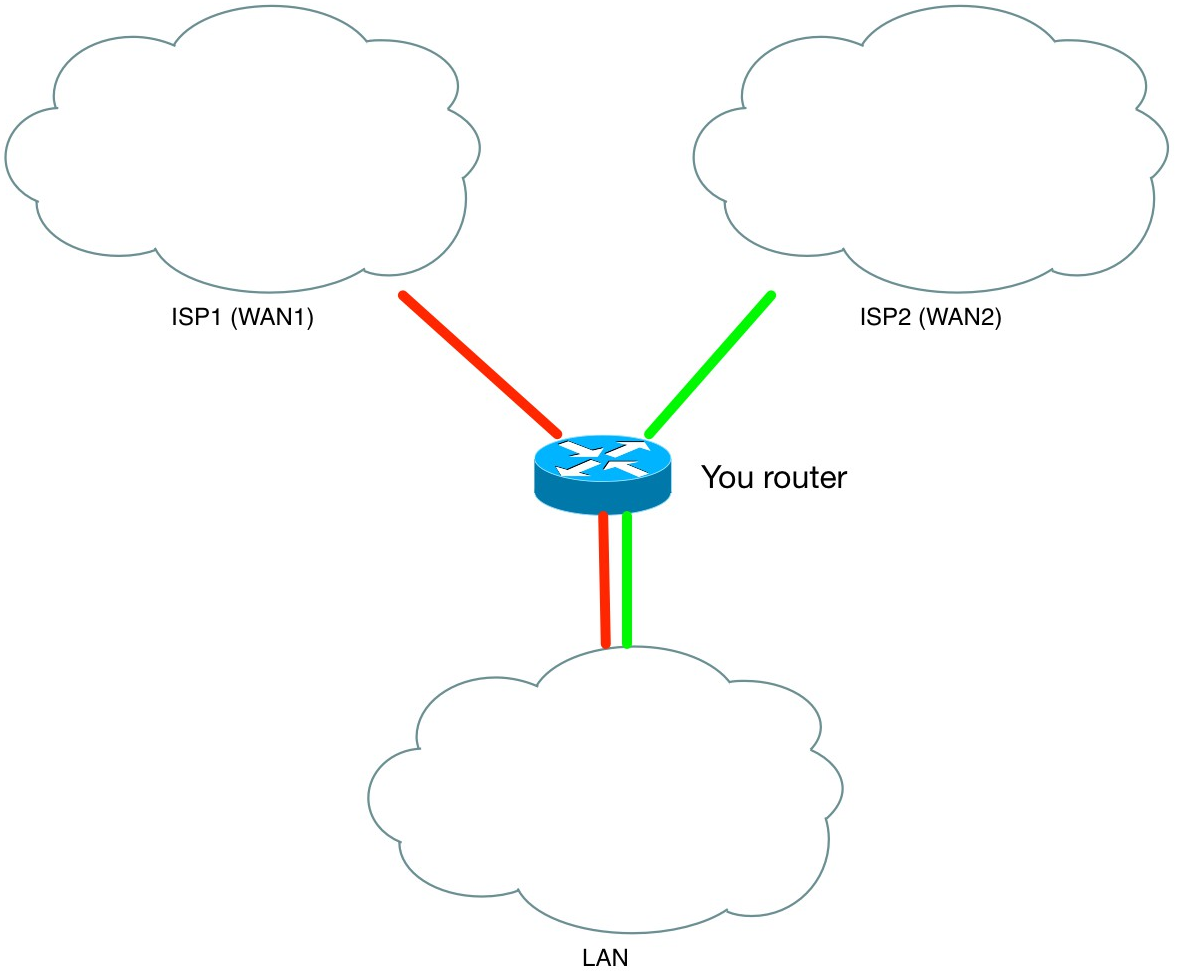
Резервирование канала

- Для работы резервирования достаточно указать разную дистанцию на маршрутах и включить проверку доступности gateway.
- Если вы хотите проверять доступность не шлюза провайдера, а какого-то другого адреса (например шлюза центрального офиса), используйте recurcive-routing или используйте скрипты.

Вариант реализации MultiWAN WAN Load Balancing (WLB)

- Другие названия технологии Dual WAN, MultivWAN, Multihoming. Позволяет распределять трафик между двумя и более каналами, без использования дополнительных протоколов маршрутизации, например BGP
- WLB распределяет трафик между несколькими каналами основываясь на заданных соотношениях нагрузки или правилах.
- WLB обеспечивает при этом резервирование подключений.

WAN Load Balancing (WLB)

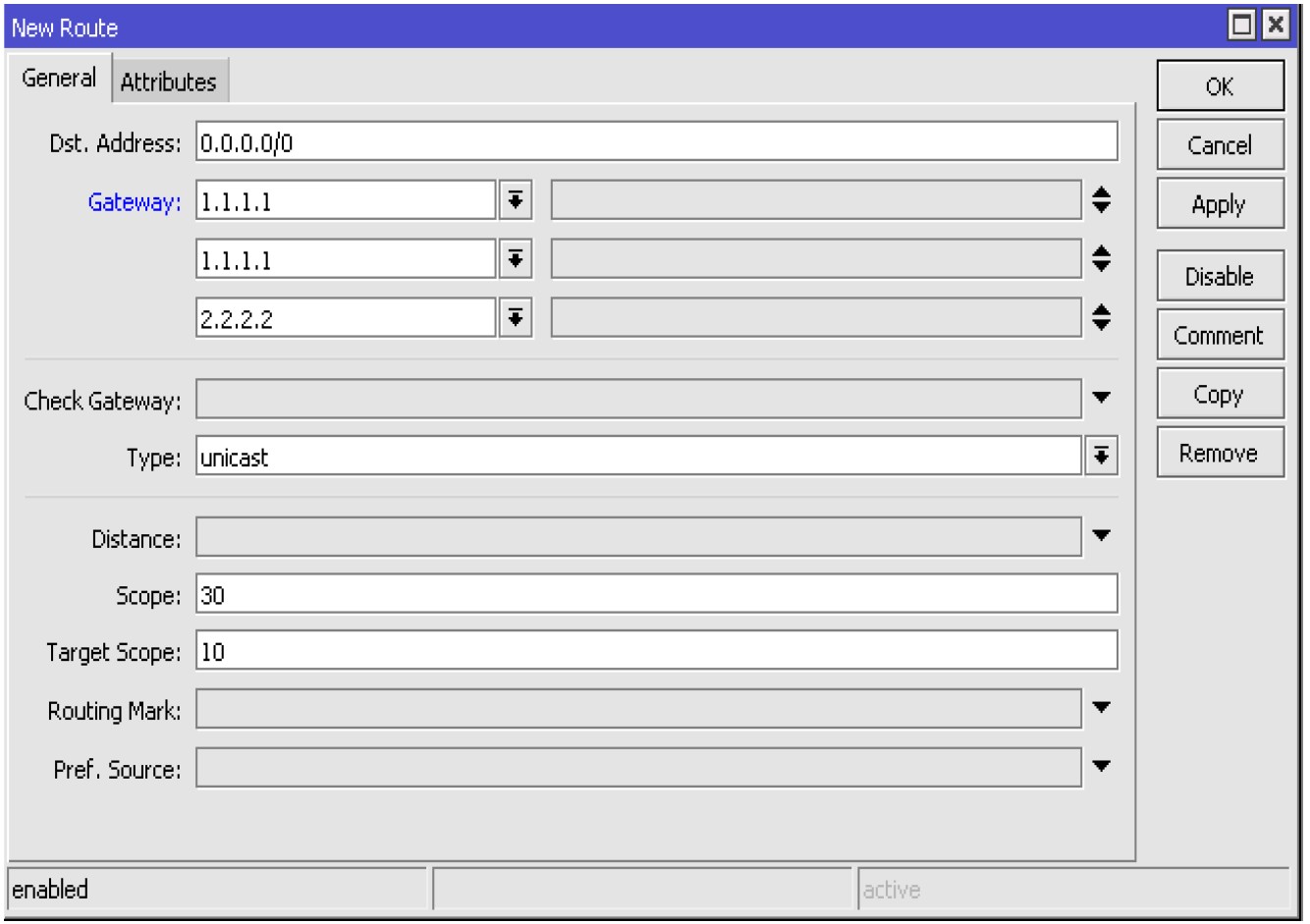


ECMP Routing
Equal cost multi-path routing

- Очень простой в реализации способ балансировки нагрузки.
- Для его реализации достаточно в маршруте указать несколько шлюзов. После чего маршрутизатор начинает распределять нагрузку между ними.
- Можно пропорционально распределить каналы, указав один шлюз несколько раз

ECMP Routing
Equal cost multi-path routing

- На этом примере мы делим каналы 2/3 к 1/3



Policy Based Routing (PBR)

- По умолчанию маршрутизатор принимает решений об пересылке пакета, основываясь на адресе назначений, указанного в заголовке пакета.
- PBR позволяет определять куда будет отправлен пакет, основываясь на других параметрах. Таких как протокол, порт, адрес источника, маркировки соединения и других.
- Например, используя эту технологию, вы можете отправить VoIP трафик в один канал, а весь остальной трафик в другой.

Policy Based Routing (PBR)

- Для использования PBR в RouterOS вы должны создать правило в IP Firewall Mange, которое будет маркировать интересующие вас пакеты (Action=mark routing) и создать в таблице маршрутизации маршрут с этой маркировкой.
- Например если вы хотите отправить весь WWW трафик на шлюз 1.1.1.1 вам надо набрать 2 команды:

```
/ip firewall mangle
add action=mark-routing chain=prerouting dst-port=80 new-routing-mark=rm-www protocol=tcp

/ip route
add distance=1 gateway=1.1.1.1 routing-mark=rm-www
```

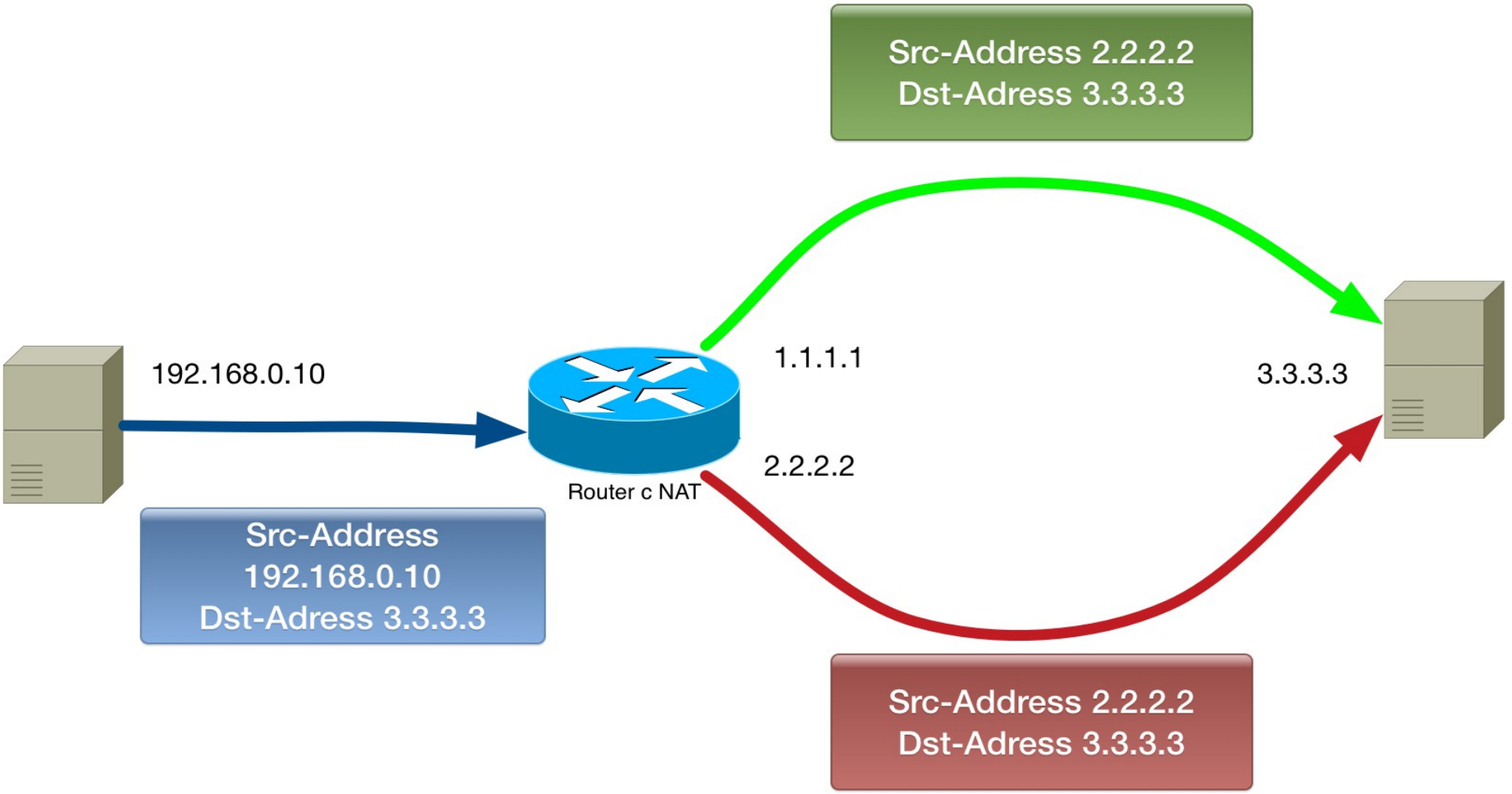
Policy Based Routing (PBR)

- Таким образом для использования этой технологии надо определиться каким образом вы будете распределять трафик. Вариантами могут быть
  - Распределение по службам и протоколам.
  - Распределение по ip-адресам
  - Распределение по соединениям (Per Connection Classifier).
  - Распределение по времени суток.
  - Любые другие варианты, которые вы сможете описать в правиле mangle.

NAT (Network Address Translation)

- Применяется в том числе при необходимости преобразования внутренних адресов к внешним.
- Часто вступает в конфликт с MultiWAN, так как внешний адрес пакета может неожиданно для получателя меняться на другой.
- К сожалению в большинстве случаев невозможно обойтись без этой технологии.

NAT (Network Address Translation)



NAT и MultiWAN

- Для корректной работы маршрутизации, необходимо, чтобы пакеты, которые пришли снаружи на конкретный интерфейс, были отправлены назад с того же интерфейса.
- Маркируйте пакеты в цепочках prerouting и output
- Не забывайте про цепочку output.
- Если вы используете VPN с указанием Source-address, не забудьте создать соответствующее правило в mangle output

Типовые правила mangle при NAT для каждого WAN-интерфейса

- Маркируйте входящее подключение connection-mark в цепочке prerouting
- На основании connection-mark маркируйте маршрут в цепочках prerouting и output

```
/ip firewall mangle
add action=mark-connection chain=prerouting in-interface=WAN1 \
    new-connection-mark=con-WAN1
add action=mark-routing chain=prerouting connection-mark=con-WAN1 \
    new-routing-mark=route-WAN1
add action=mark-routing chain=output connection-mark=con-WAN1 \
    new-routing-mark=route-WAN1
```

Общая стратегия настройки

- Определитесь с режимом работы (Active/Backup) или WLB
- Определитесь с алгоритмом распределения нагрузки на каналы.
- Создайте соответсвующие маршруты и правила в IP Firewall Mangle
- Используйте открытые DNS или явно пропишите маршруты к DNS оператора.

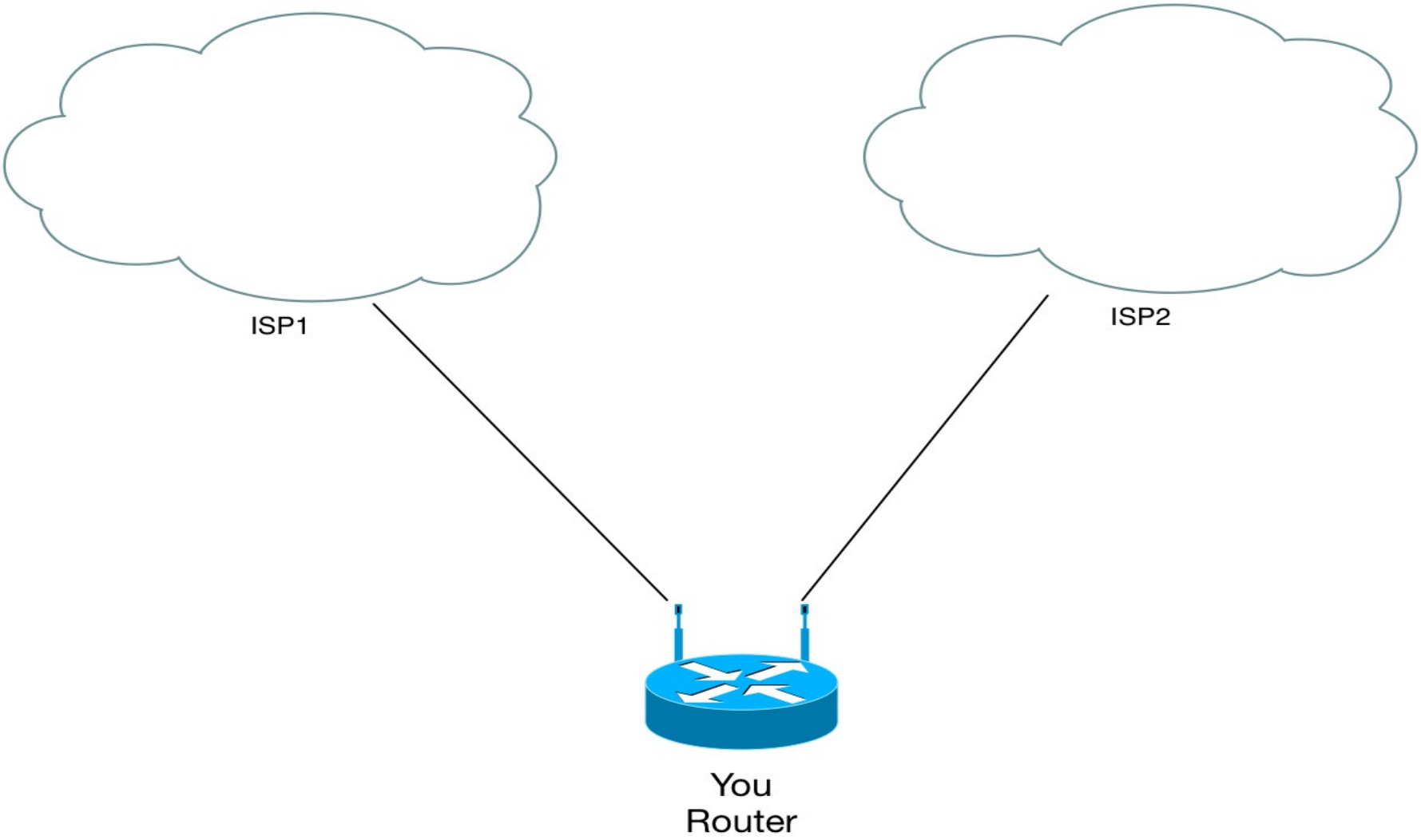
На что еще обратить внимание

- Если маршрут в именованной таблице маршрутизации недоступен, пакет будет отправлен через основную таблицу маршрутизации.
- Если у вас возникает проблема с одним из каналов, то маршрутизатор будет пытаться отправить пакет через другой канал.
- Если у вас на обоих WAN-интерфейсах одна и та же подсеть и один и тот же шлюз, можно указать в шлюзе имя интерфейса через знак %. Например 1.1.1.1%WAN1

WLB и динамические адреса

- Представьте себе, что ваш маршрутизатор подключен к двум провайдерам.
- Оба провайдера назначают вам адреса по протоколу DHCP.
- Вы хотите настроить Wan Load Balancing

Схема сети

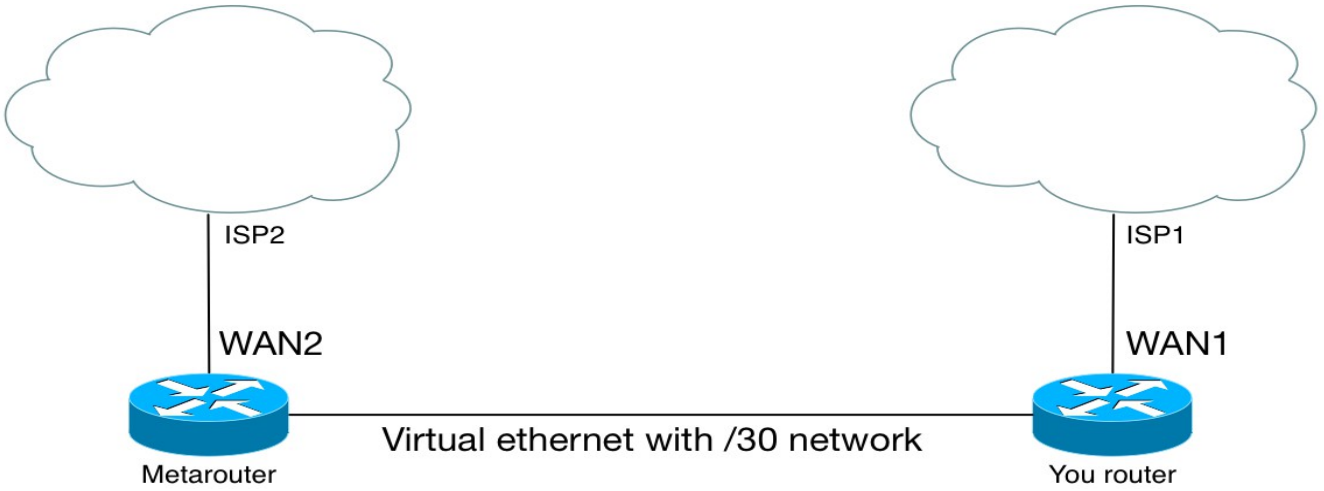


Проблемы конфигурации:

- Мы не можем создать маршрут, в том числе маршрут с маркировкой, потому что мы не знаем адрес шлюза, который назначается динамически.
- В свойствах DHCP-клиента можно указать только дистанцию для маршрута по умолчанию.
- Возможна ситуация когда оба провайдера отдадут вам один и тот же адрес и один и тот же шлюз.

Простое решение

- Использовать второй маршрутизатор. Если ваш маршрутизатор поддерживает metarouter, то можно использовать его. Тогда вы можете создать статический маршрут между ними и использовать маркировку для пакетов идущих на него.



В чем преимущества и недостатки?

- Достаточно простое в настройке решение.
- Имеет следующие недостатки:
  - Не все оборудование поддерживает Metarouter
  - Если вы используете metarouter — он тоже потребляет ресурсы маршрутизатора
  - Если вы покупаете второй маршрутизатор — вы тратите деньги.
  - Чем больше маршрутизаторов, тем сложнее их обслуживать.

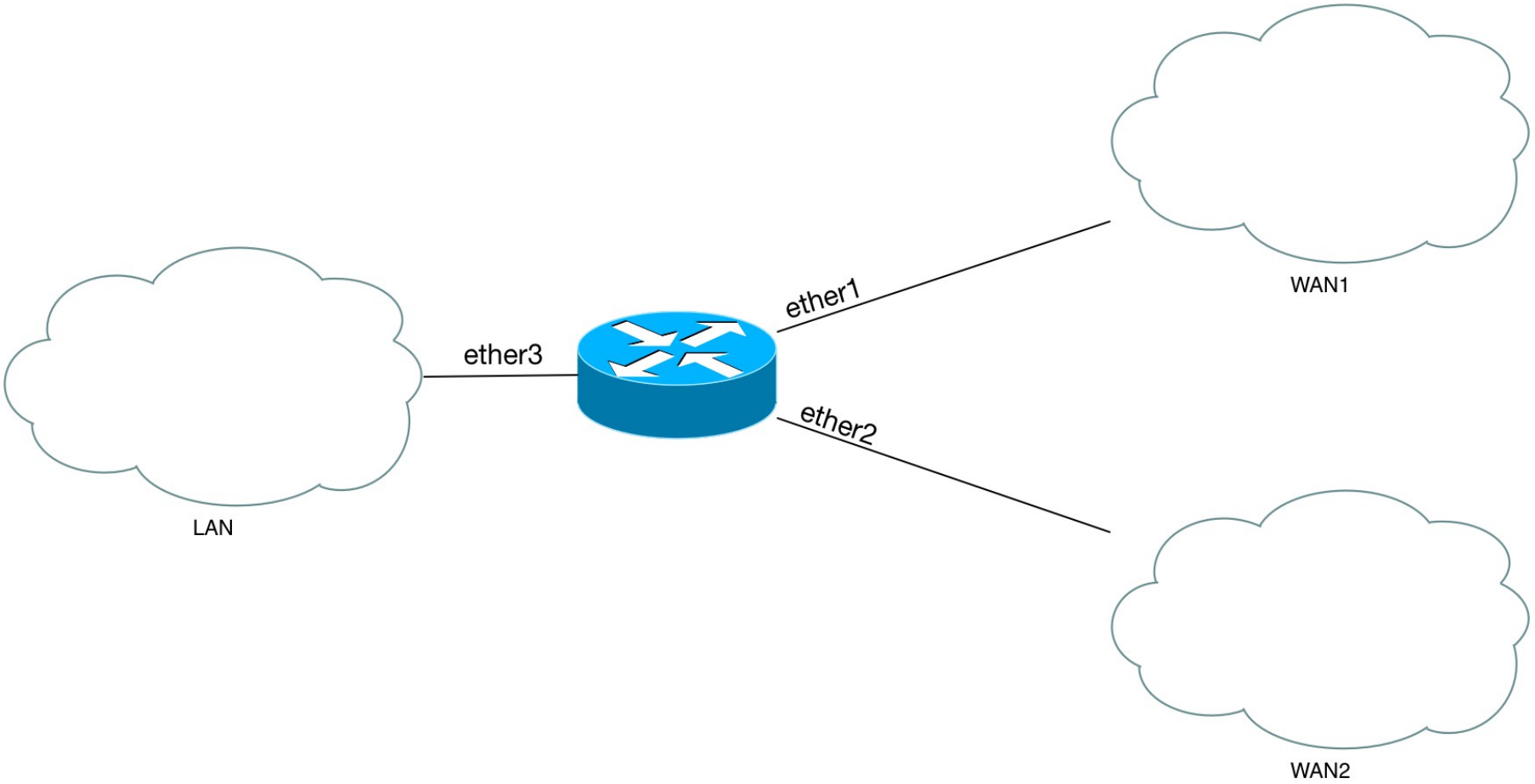
Более сложное решение

- Использовать Virtual Routing and Forwarding (VRF)
- VRF использует PBR (Policy Based Routing)
- Можно создать несколько независимых именованных таблиц маршрутизации на одном и том же роутере..
- VRF решает проблему одинаковых подсетей, так как таблицы маршрутизации независимы.

Пример такого решения

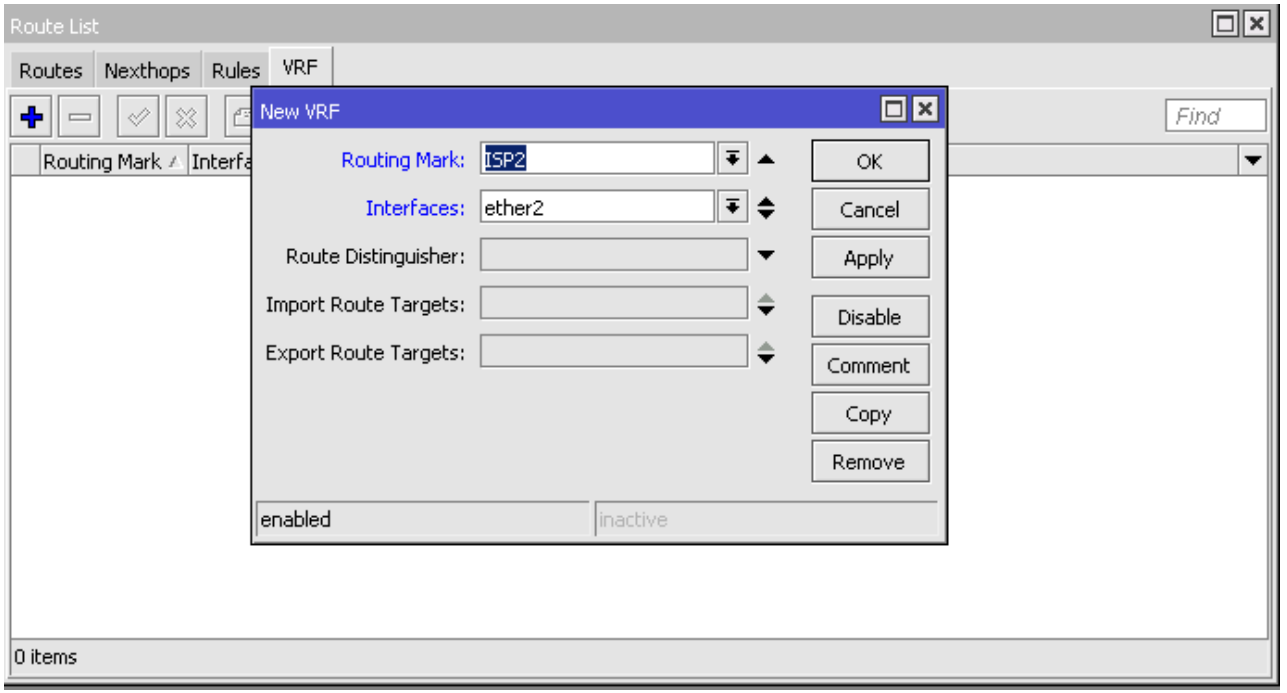
- Есть два провайдера, предоставляющих динамические адреса.
- Мы хотим направить трафик на хост 8.8.8.8 через одного провайдера, а весь остальной трафик через другого.

Схема сети



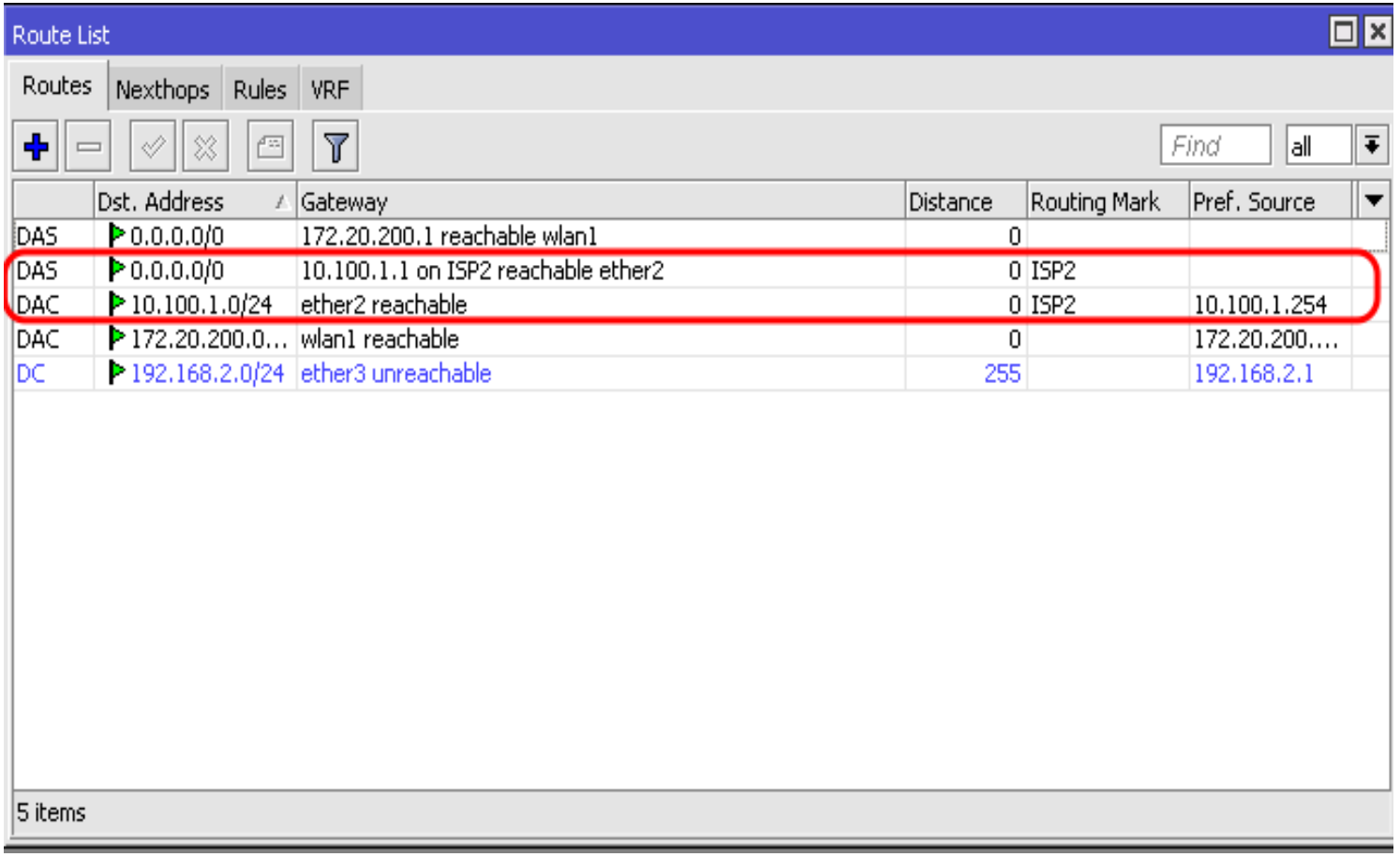
Шаг 1

- Открываем меню /ip routes и создаем VRF, указав в качестве названия (routing mark) ISP2 и добавляем интерфейс на который подключен к этому провайдеру.



Шаг 1

- В таблице маршрутизации автоматически появились маршруты с маркировкой ISP2



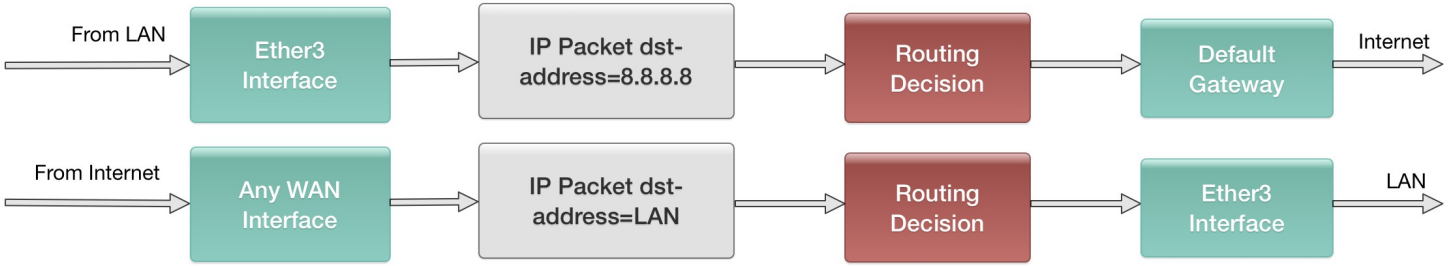
Шаг 2

- Добавляем в Firewall правила mangle, которые будут маркировать маршрут mark-routing action
  - Первое правило маркирует пакеты, которые должны быть отправлены через ISP2
  - Второе правило «размаркировывает» входящие пакеты, чтобы они могли быть обработаны основной таблицей маршрутизации.

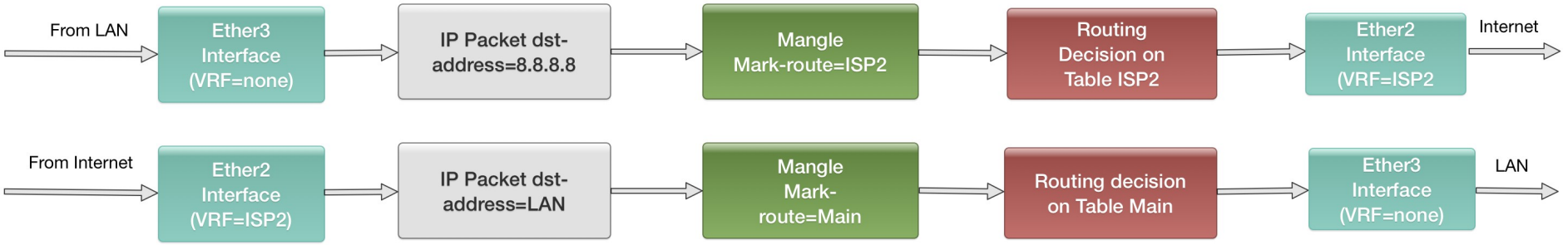
```
/ip firewall mangle
add action=mark-routing chain=prerouting dst-address=8.8.8.8 in-interface=ether3 \
    new-routing-mark=ISP2
add action=mark-routing chain=prerouting in-interface=ether2 new-routing-mark=\
    main
```

Как это работает ?

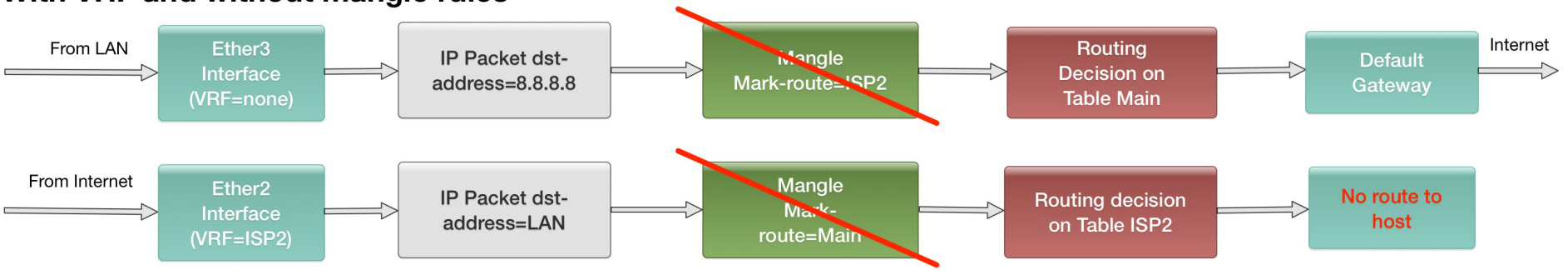
Without VRF



With VRF



With VRF and without mangle rules



Резервирование канала без смены адресов

- Может потребоваться для доступа к вашим службам из Интернет.
- Требует неизменности вашего адреса.
- У вас есть два варианта решения этой задачи
  - Покупка AS (Autonomus System) и настройка BGP
  - Установка дополнительного маршрутизатора в датацентре с высоким уровнем доступности, построением VPN до него и балансировки нагрузки между VPN-соединениями

Спасибо за внимание

- Я всегда готов ответить на ваши вопросы.
- Вы можете связаться со мной:
  - Web: http://spw.ru
  - E-mai:l ikn@spw.ru
  - Skype: Ilya.Knyazev