Простой метод создания отказоустойчивого VPN между роутером MikroTik и оборудованием другого производителя

Алексей Чудин
Россия, Москва
28 марта 2014

Обо мне

Меня зовут Алексей Чудин

Опыт работы с сетями около 10 лет

Сертифицированный тренер MikroTik, а также инженер по направлениям: MTCWE, MTCRE, MTCTCE

Цель презентации

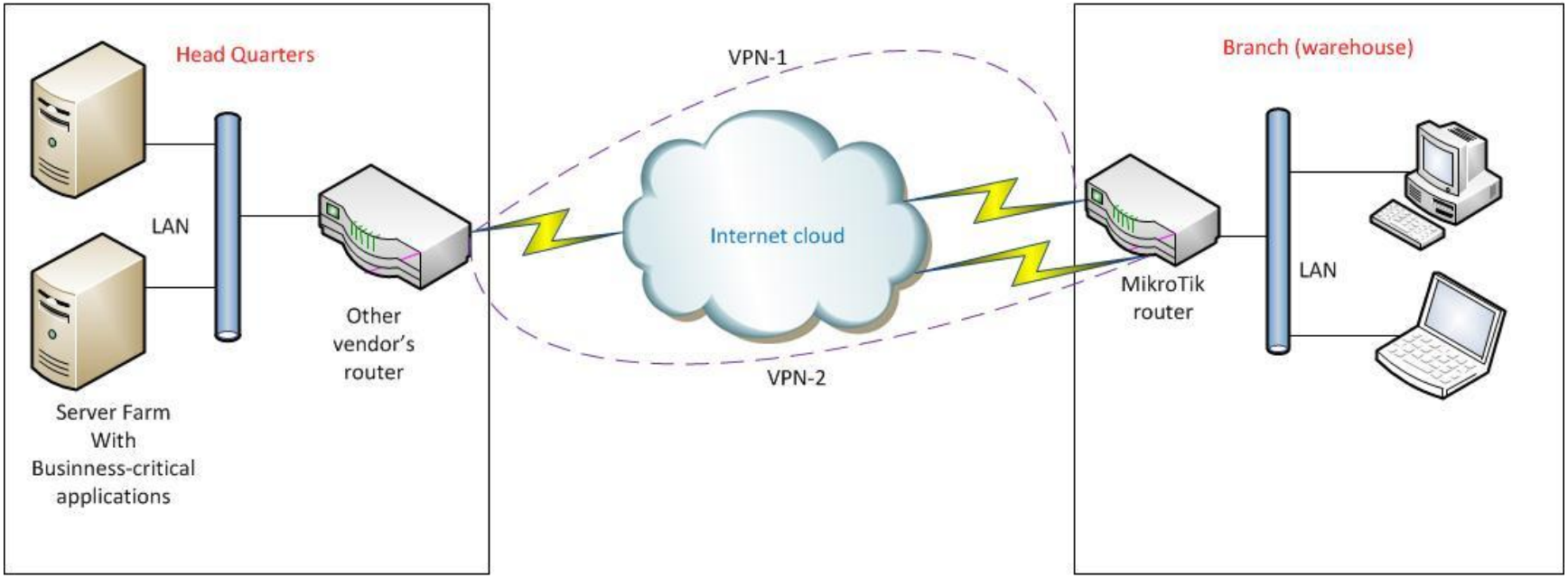
Показать на практическом примере:

- создание отказоустойчивых VPN используя GRE-туннели,
- конфигурирование Policy Based Routing при использовании нескольких провайдеров,
- изменение приоритетов маршрутов
- уменьшение времени переключения каналов

Постановка задачи

- Для упрощения нашего примера допустим, что у нас есть 1 стабильный и надежный провайдер в главном офисе и 2 не очень стабильных – на удаленном складе (например, 2 АДСЛ-провайдера). В главном офисе у нас роутер другого производителя, на складе - MikroTik
- Наша задача: обеспечить отказоустойчивое соединение к ИТ-ресурсам главного офиса со склада

Постановка задачи



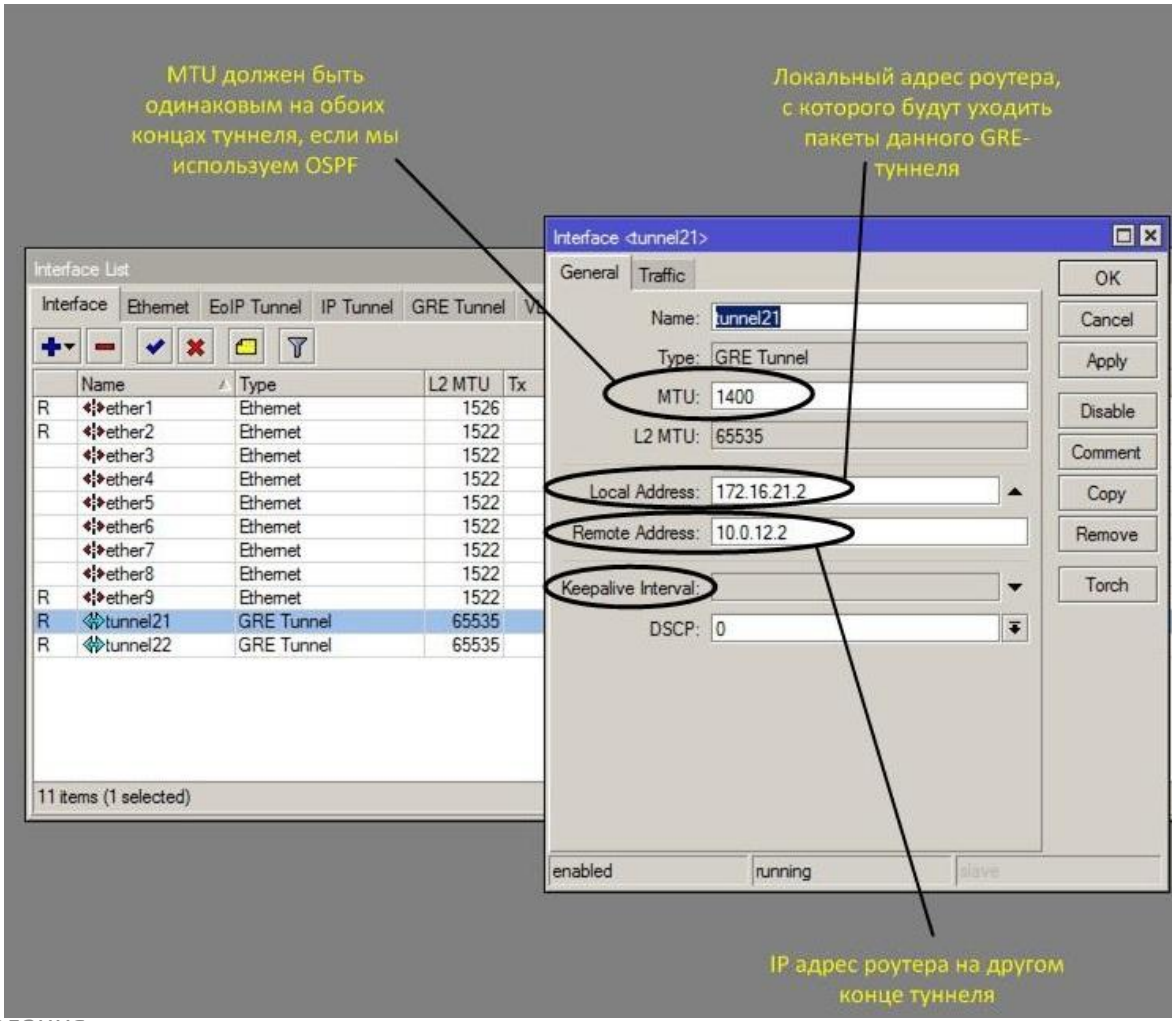
☺

Использование GRE-туннелей

Если мы используем MikroTik с одной стороны и оборудование другого производителя с другой, то наиболее простой способ организации VPN между ними – использование GRE-туннелей, потому что:

- Многие производители поддерживают GRE-туннели
- GRE-туннели поддерживают multicast, поэтому можно использовать OSPF

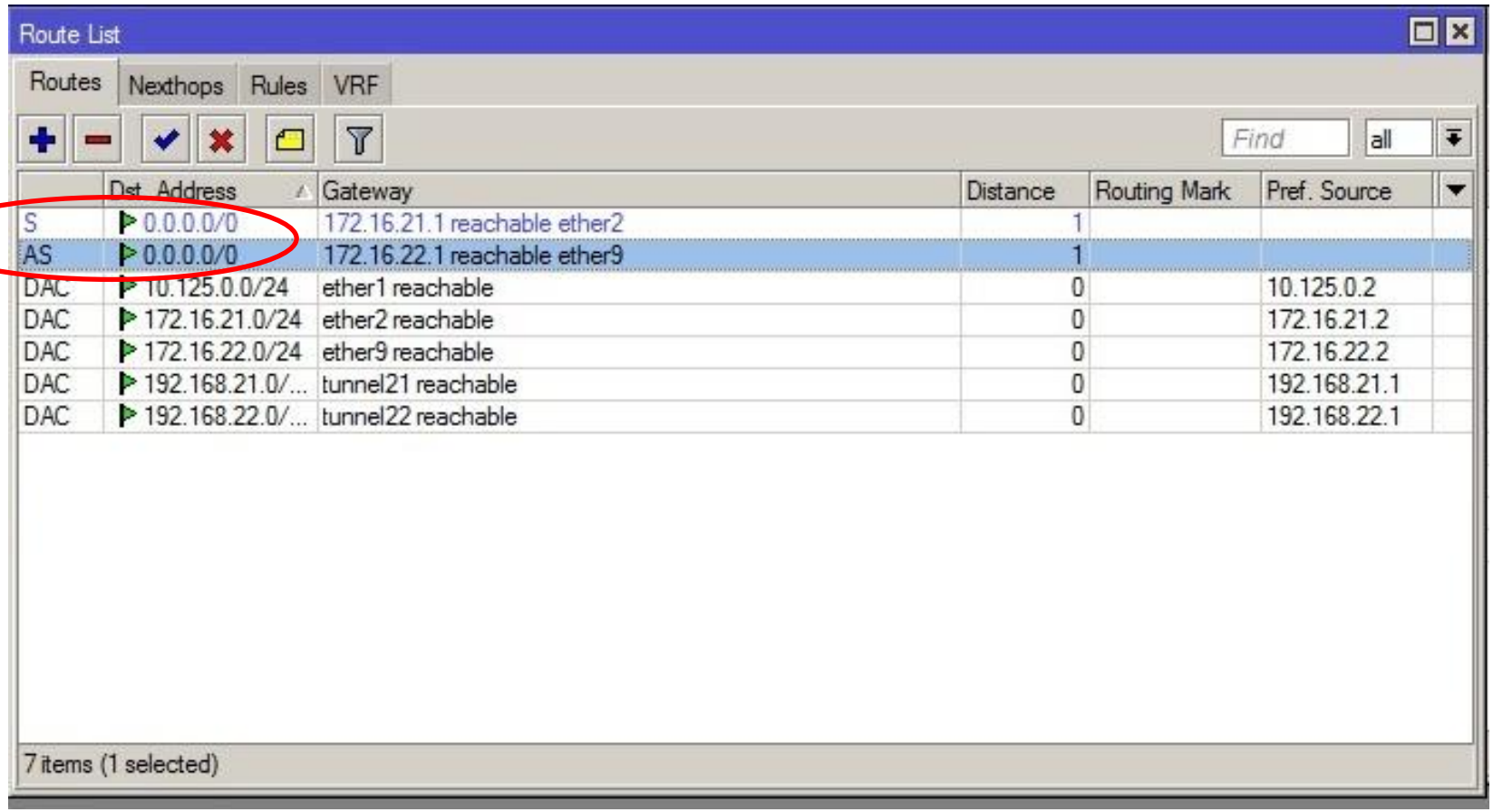
Создание GRE-туннеля



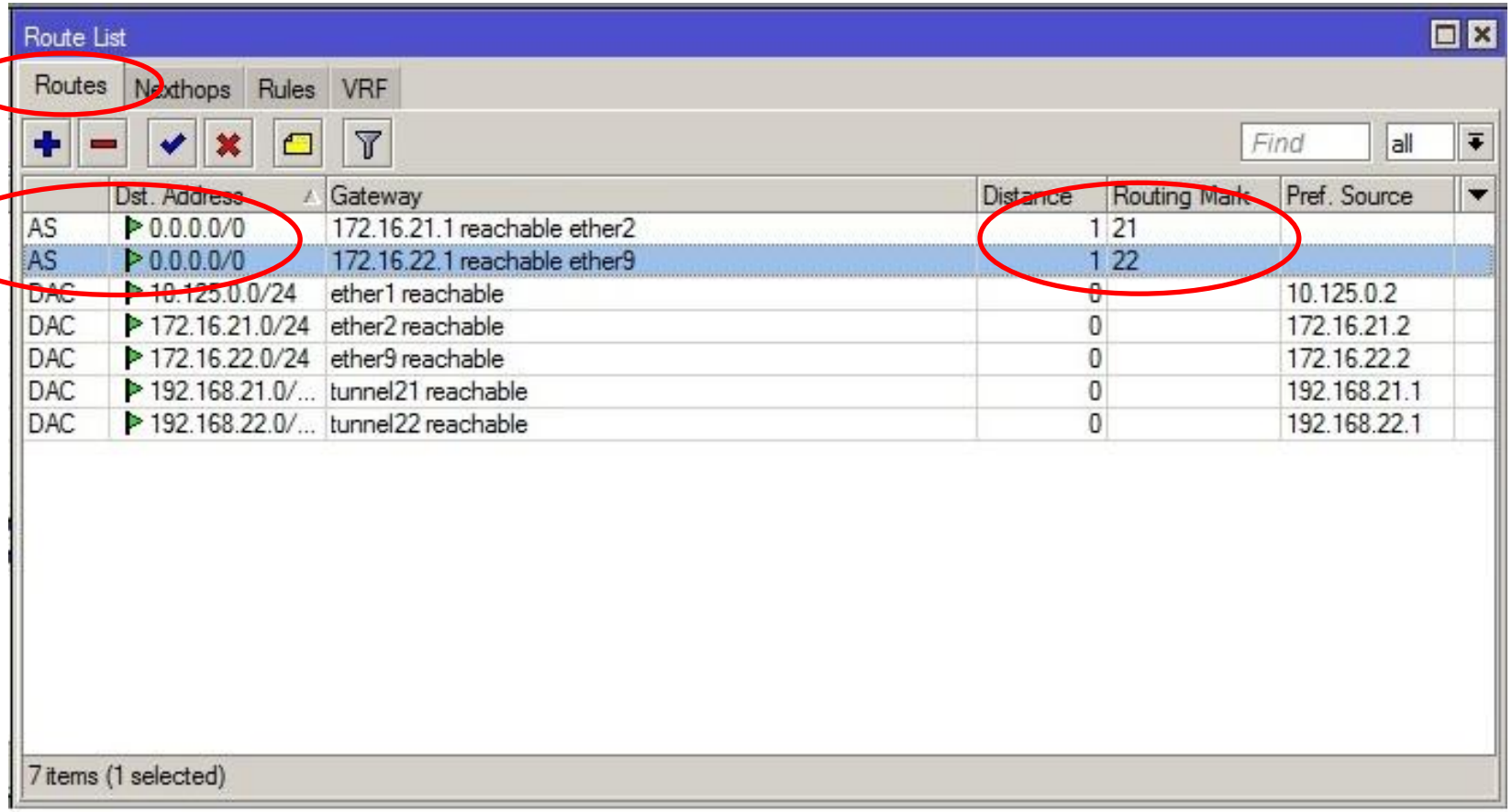
Добавление 2-х маршрутов по умолчанию

- Когда мы добавляем 2 и более маршрутов по умолчанию, только один из них будет в активном состоянии
- Это означает, что роутер будет отвечать на пакеты (например, пинги), используя этот активный дефолтный маршрут, даже если пакеты пришли на другие интерфейсы
- Нам же надо, чтобы роутер отвечал на наши запросы с того же интерфейса, на который эти запросы пришли
- Иными словами, нам нужно принимать решение о пересылке пакета используя его source-адрес, тогда как роутинг оперирует destination-адресами пакетов

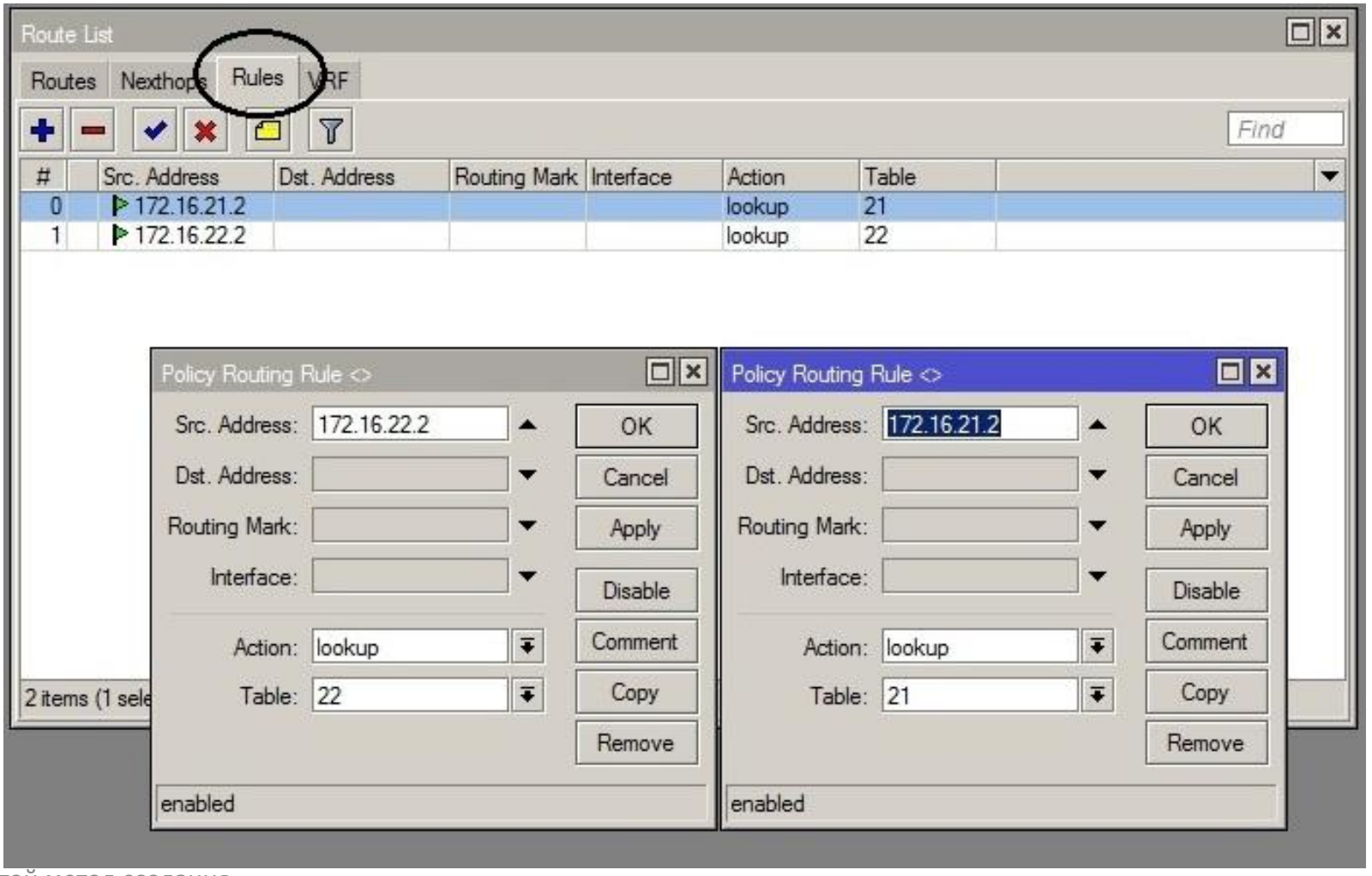
Добавление 2-х маршрутов по умолчанию



Решение: использование Policy Based Routing (PBR)

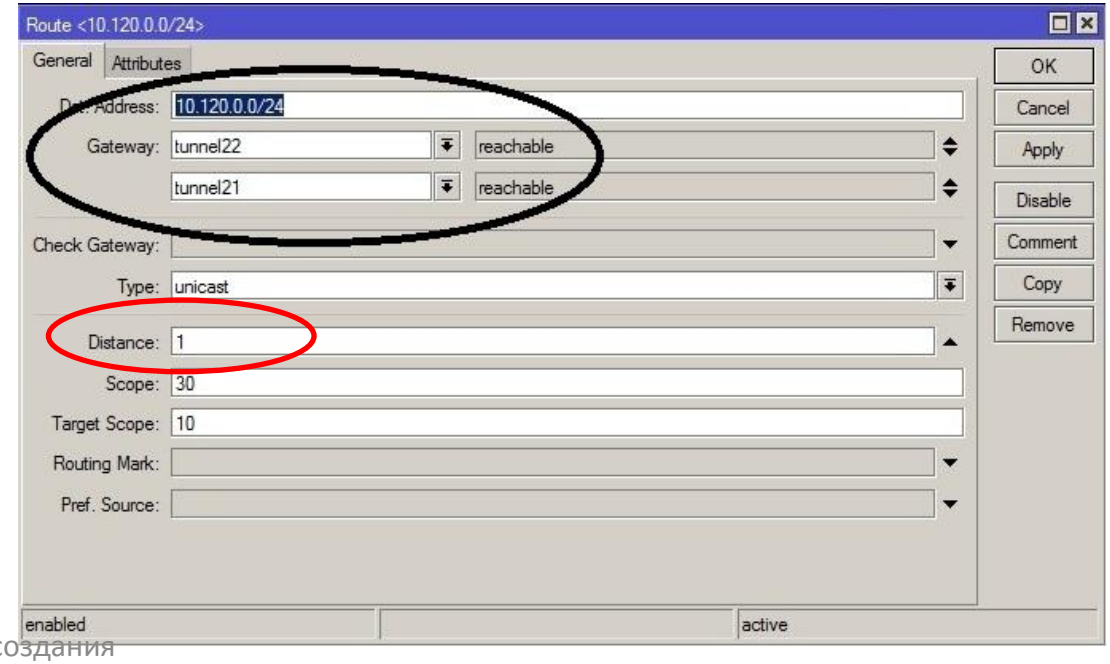


PBR: Route Rules



Балансировка нагрузки

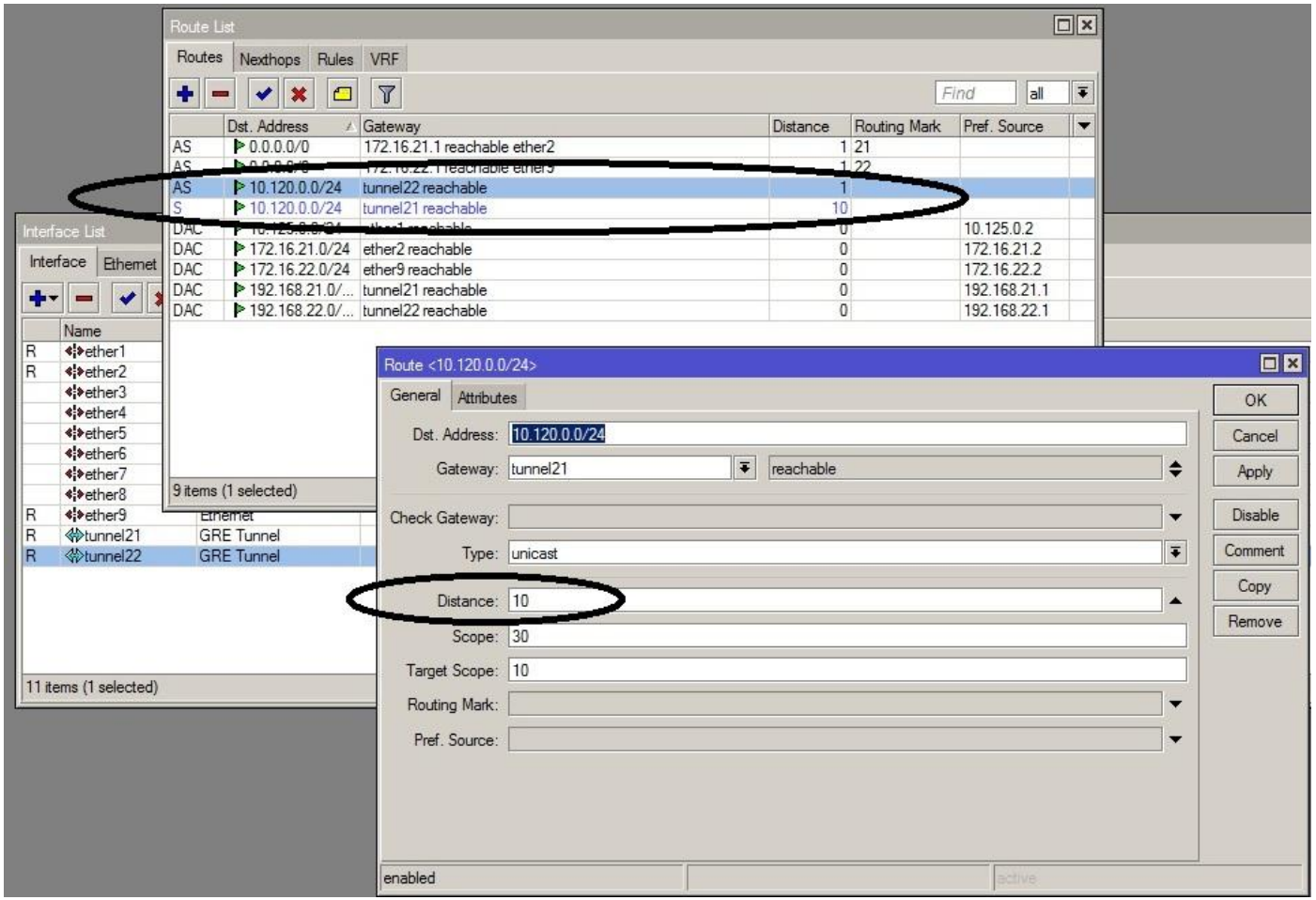
- Балансировка нагрузки будет работать по умолчанию, потому что маршруты через GRE-туннели имеют одинаковое значение distance независимо от реального качества канала



Приоритет маршрутов

- Однако балансировка трафика по двум каналам не всегда нужна. Например, если у нас второй канал – GPRS-модем с ограничением по трафику или вообще спутниковый интернет
- В этом случае схема работы такая: один канал основной, в случае его падения трафик пойдет через резервный канал
- Для этого используем опцию route distance; маршрут с меньшим значением distance будет в активном состоянии. Если этот канал падает, то активным становится маршрут с большим значением distance

Приоритет маршрутов

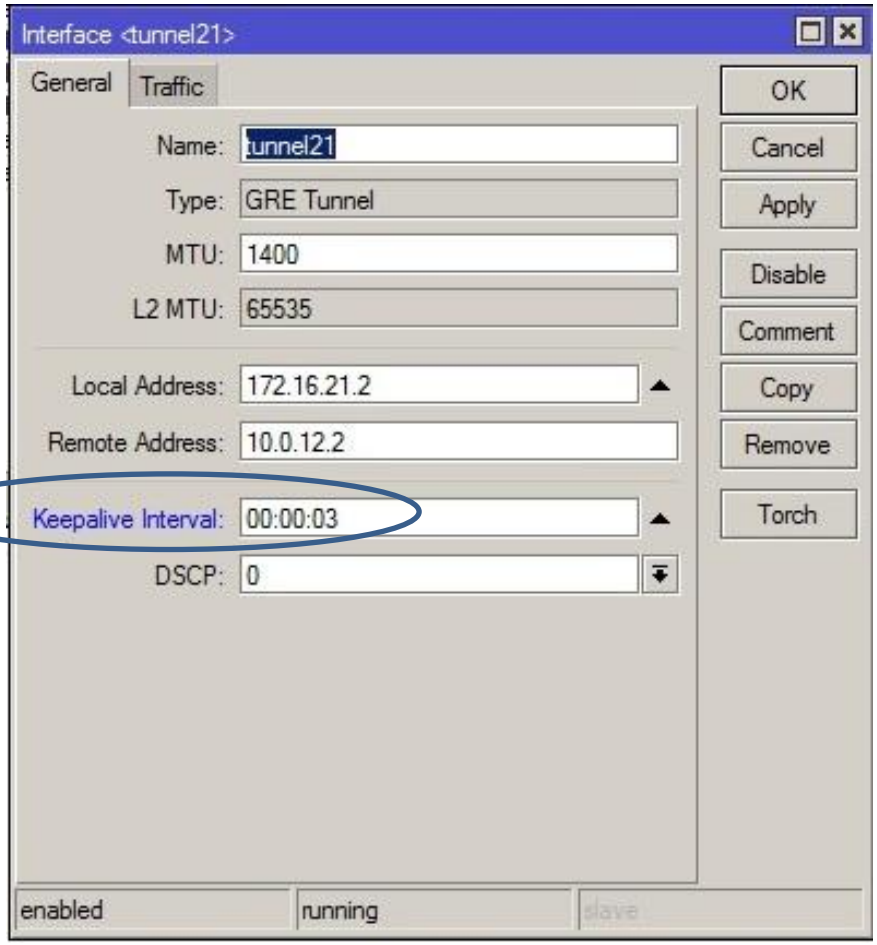


Простой метод создания отказоустойчивого VPN между роутером MikroTik и оборудованием другого производителя

Опция Keepalive

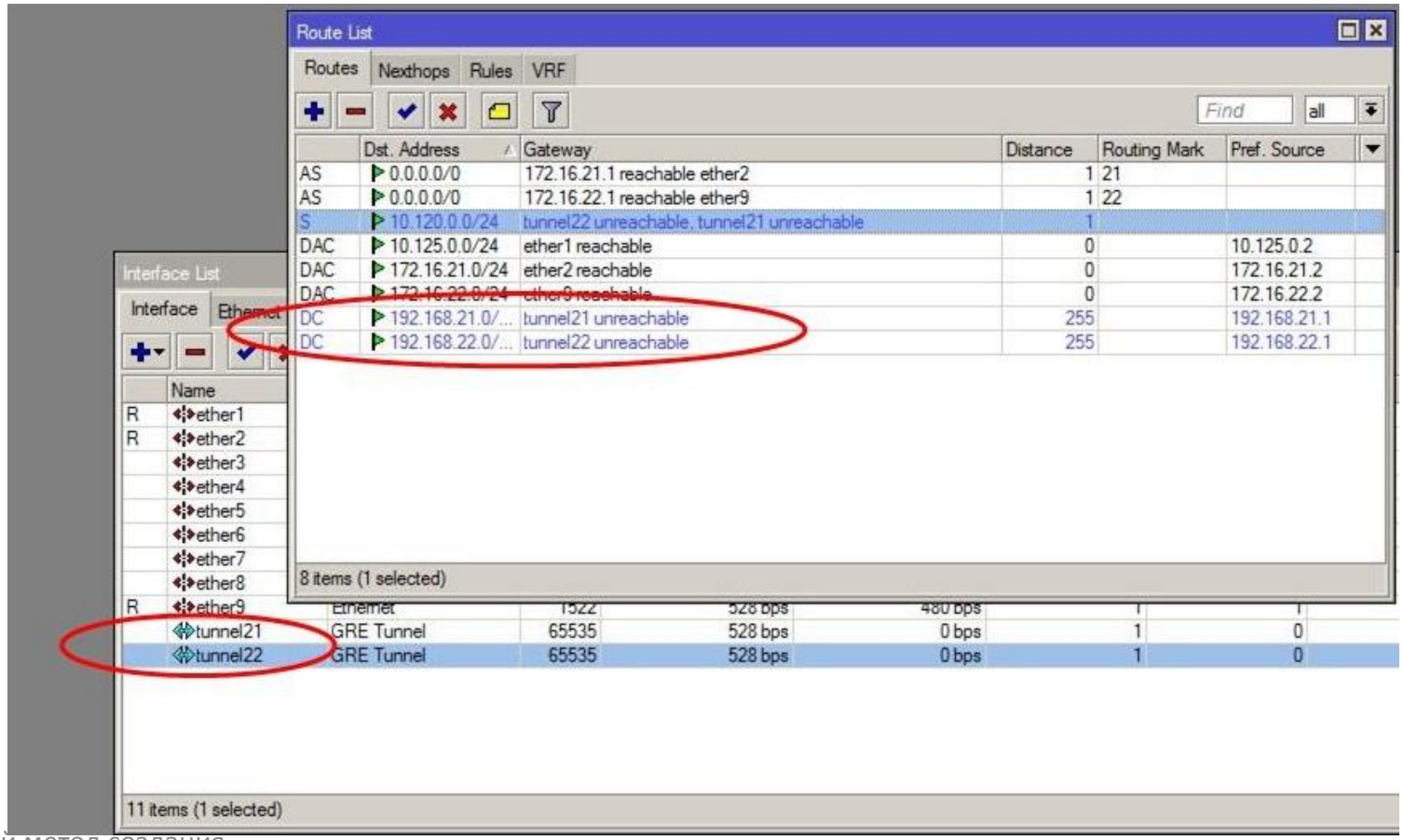
- Когда же маршрут станет неактивным? Когда интерфейс GRE уйдет в down. Но GRE-туннели разработаны как stateless, поэтому они всегда в up-статусе (Running), они не проверяют статус друг друга. Это означает, что и маршрут через GRE-туннель останется активным.
- К счастью, есть решение этой проблемы – активирование и использование опции **keepalive**

Опция Keepalive



Опция Keepalive

- Опция Keepalive должна быть включена на обоих концах GRE-туннеля!



Опция Keepalive

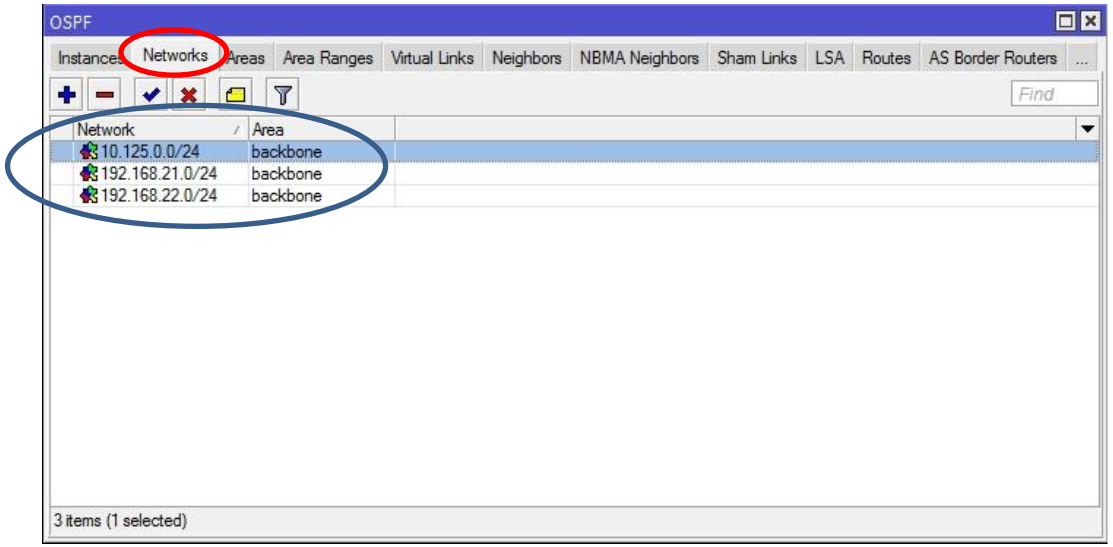
- Но что делать, если роутер другого производителя не поддерживает опцию keepalive в GRE-туннеле?

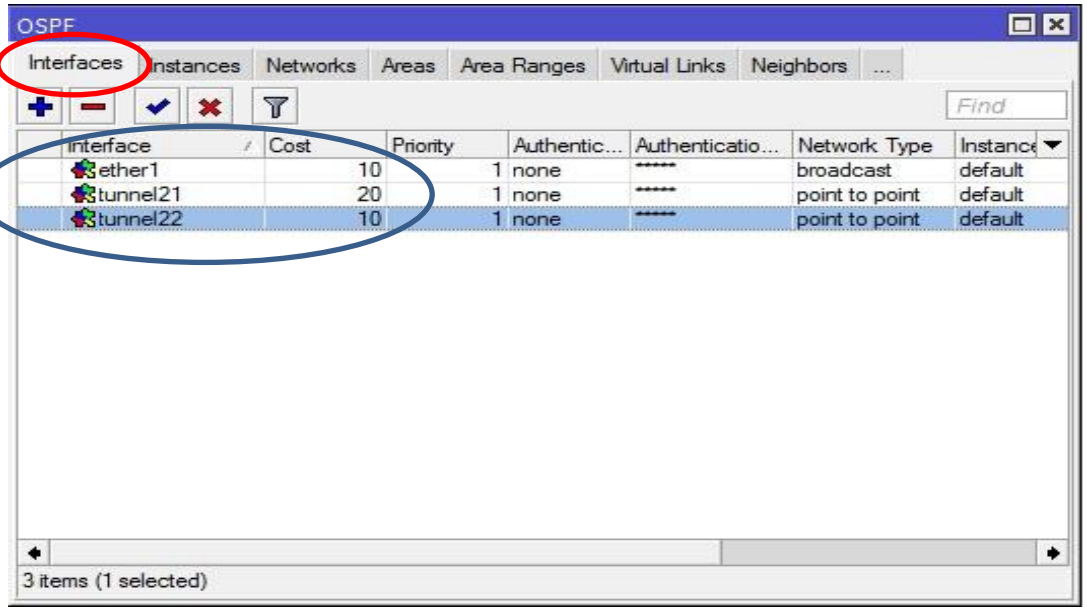
- Мы можем использовать протокол OSPF, который проверяет статус интерфейсов используя собственный механизм Hello-пакетов.

Базовая настройка OSPF

- Для запуска процесса OSPF достаточно добавить сети, которые будут в нем участвовать

- Стоимость (cost) OSPF-интерфейсов GRE будет одинаковая по умолчанию, поэтому включится балансировка нагрузки по двум каналам. Чтобы избежать балансировки и выставить приоритеты маршрутов, можно вручную поменять значение cost на интерфейсе



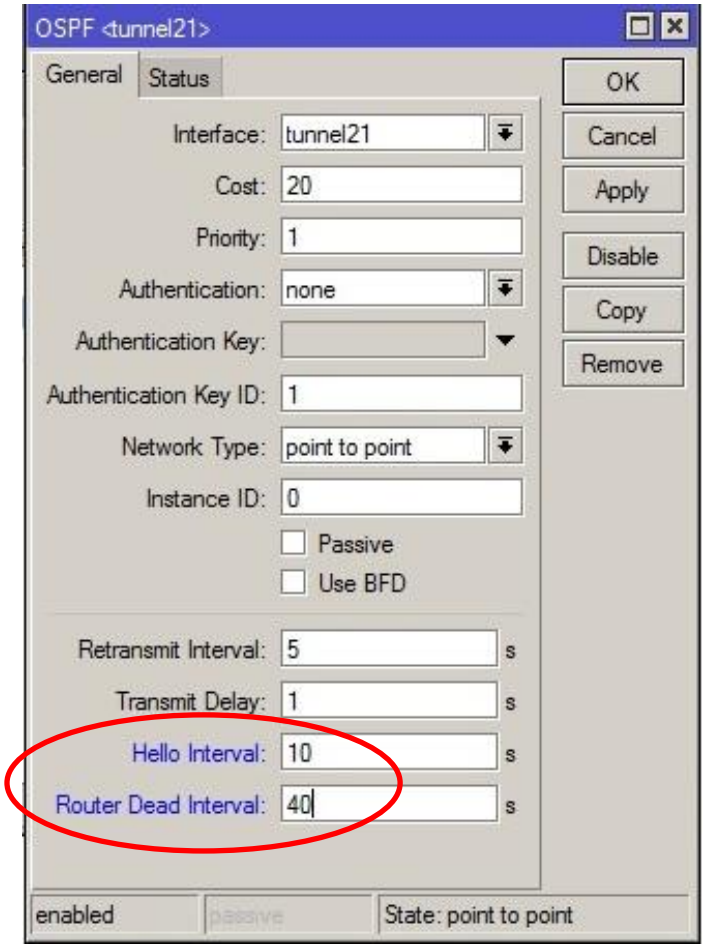


?

Сколько времени потребуется OSPF с дефолтными настройками для переключения маршрута?

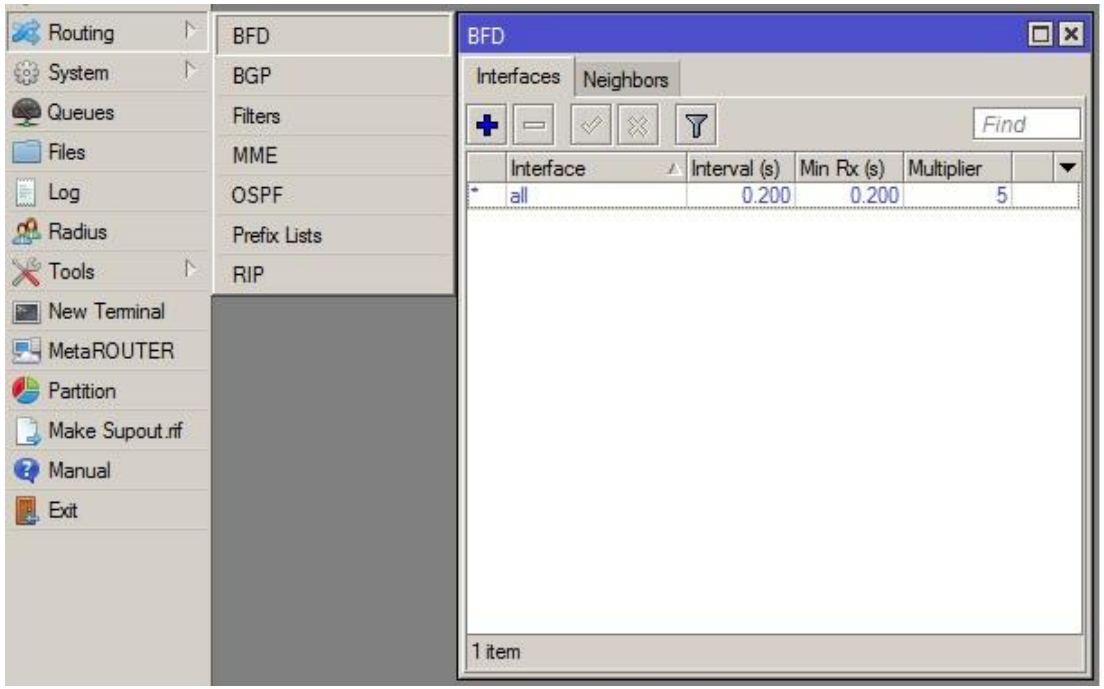
Простейший тюнинг OSPF

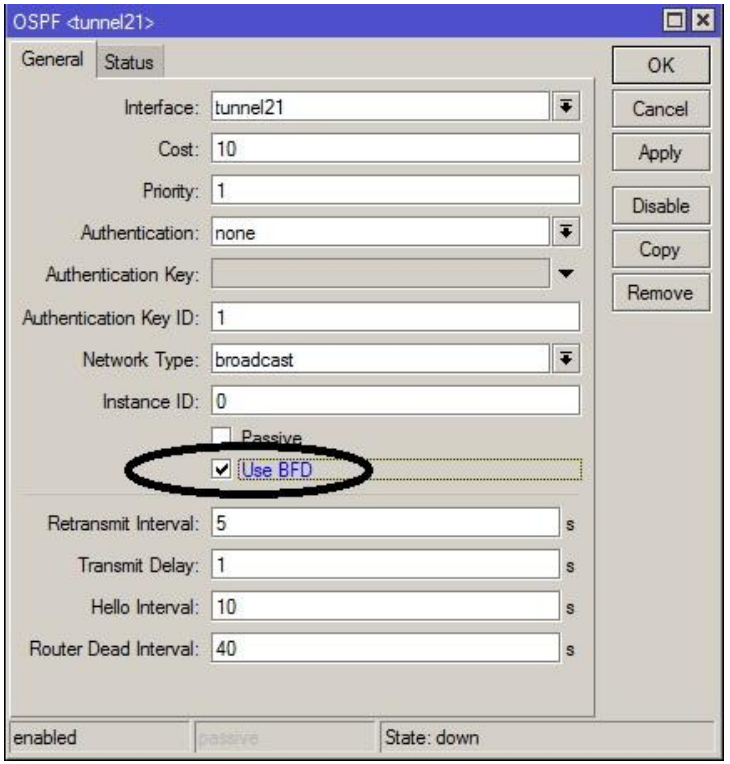
- Важно! Hello и Dead интервалы туннельных интерфейсов должны совпадать!



Продвинутый тюнинг OSPF

- Средствами OSPF в MikroTik можно сократить время переключения до 2 секунд. А если нужно переключать еще быстрее?
- Выход есть! Используем BFD!





Простой метод создания отказоустойчивого VPN между роутером MikroTik и оборудованием другого производителя

Заключение

Мы рассмотрели простой метод создания отказоустойчивого VPN с использованием двух интернет-провайдеров.

Наиболее важные выводы:

- GRE-туннели полезны для организации VPN через WAN
- Чтобы направить трафик каждого туннеля через канал соответствующего провайдера, используем PBR
- Чтобы знать статус GRE-интерфейса на другом конце туннеля, используем полезнейшую опцию keepalive. Если оборудование на другом конце не поддерживает keepalive в GRE, используем протокол OSPF
- Можно балансировать нагрузку через оба туннеля, либо активно использовать только основной туннель, а другой держать в резерве. Все это можно организовать с помощью как статической, так и динамической маршрутизации
- Если мы используем OSPF поверх GRE-туннелей, нужно помнить, что MTU туннелей, а также Hello и Dead интервалы должны совпадать на обоих концах VPN-а
- Для сокращения времени переключения каналов в OSPF можно уменьшить дефолтные значения Hello и Dead интервалов, а можно включить поддержку BFD, убедившись, что оборудование на другом конце нашего VPN-а поддерживает BFD поверх GRE-интерфейсов

Знаете способ проще? ☺

Пишите:
extremail@inbox.ru

Спасибо за ваше внимание!