

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: МТСWE, МТСRE, МТСТСЕ

Цель презентации

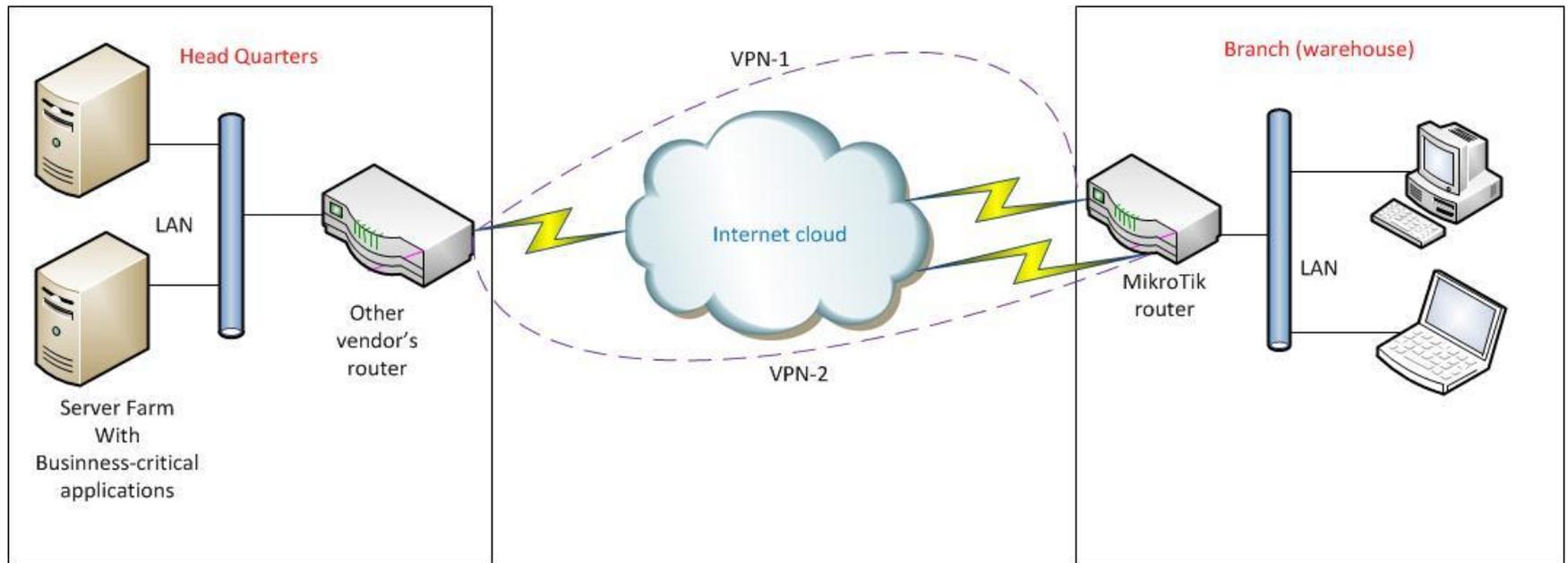
Показать на практическом примере:

- 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



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



Простой метод создания
отказоустойчивого VPN
между роутером MikroTik и
оборудованием другого

Алексей Чудин

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

MTU должен быть одинаковым на обоих концах туннеля, если мы используем OSPF

Локальный адрес роутера, с которого будут уходить пакеты данного GRE-туннеля

Name	Type	L2 MTU	Tx
R ether1	Ethernet	1526	
R ether2	Ethernet	1522	
R ether3	Ethernet	1522	
R ether4	Ethernet	1522	
R ether5	Ethernet	1522	
R ether6	Ethernet	1522	
R ether7	Ethernet	1522	
R ether8	Ethernet	1522	
R ether9	Ethernet	1522	
R tunnel21	GRE Tunnel	65535	
R tunnel22	GRE Tunnel	65535	

Interface <tunnel21>

General Traffic

Name: tunnel21

Type: GRE Tunnel

MTU: 1400

L2 MTU: 65535

Local Address: 172.16.21.2

Remote Address: 10.0.12.2

Keepalive Interval:

DSCP: 0

enabled running slave

IP адрес роутера на другом конце туннеля

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

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

	Dest. Address	Gateway	Distance	Routing Mark	Pref. Source
S	▶ 0.0.0.0/0	172.16.21.1 reachable ether2	1		
AS	▶ 0.0.0.0/0	172.16.22.1 reachable ether9	1		
DAC	▶ 10.125.0.0/24	ether1 reachable	0		10.125.0.2
DAC	▶ 172.16.21.0/24	ether2 reachable	0		172.16.21.2
DAC	▶ 172.16.22.0/24	ether9 reachable	0		172.16.22.2
DAC	▶ 192.168.21.0/...	tunnel21 reachable	0		192.168.21.1
DAC	▶ 192.168.22.0/...	tunnel22 reachable	0		192.168.22.1

7 items (1 selected)

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

Решение: использование Policy Based Routing (PBR)

The screenshot shows the 'Route List' window in Mikrotik WinBox. The 'Routes' tab is selected. The table below shows the routing table with columns: Dst. Address, Gateway, Distance, Routing Mark, and Pref. Source. The first two rows are selected, and their 'Routing Mark' values are circled in red.

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	172.16.21.1 reachable ether2	1	21	
AS	0.0.0.0/0	172.16.22.1 reachable ether9	1	22	
DAC	10.125.0.0/24	ether1 reachable	0		10.125.0.2
DAC	172.16.21.0/24	ether2 reachable	0		172.16.21.2
DAC	172.16.22.0/24	ether9 reachable	0		172.16.22.2
DAC	192.168.21.0/...	tunnel21 reachable	0		192.168.21.1
DAC	192.168.22.0/...	tunnel22 reachable	0		192.168.22.1

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

PBR: Route Rules

The screenshot displays the Mikrotik WinBox interface. At the top, the 'Route List' window is open, with the 'Rules' tab selected and circled. Below the tabs is a toolbar with icons for adding, deleting, and filtering rules. A table lists two route rules:

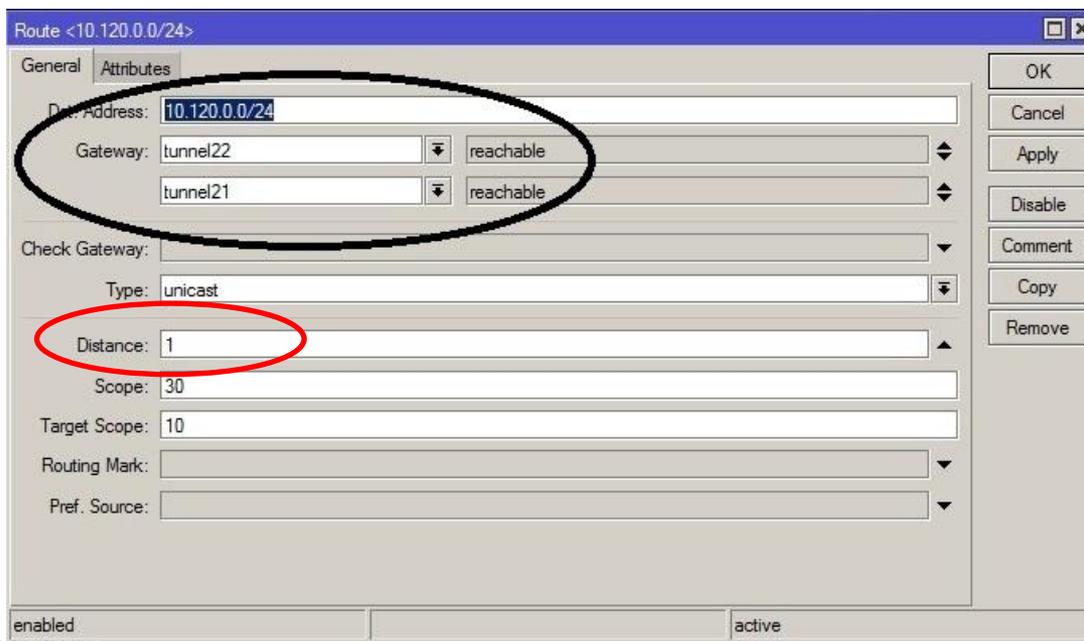
#	Src. Address	Dst. Address	Routing Mark	Interface	Action	Table
0	▶ 172.16.21.2				lookup	21
1	▶ 172.16.22.2				lookup	22

Below the table, two 'Policy Routing Rule' configuration windows are shown. The left window is for rule #1, with 'Src. Address' set to 172.16.22.2 and 'Table' set to 22. The right window is for rule #0, with 'Src. Address' set to 172.16.21.2 and 'Table' set to 21. Both windows have 'Action' set to 'lookup' and 'Interface' set to an empty dropdown. The status at the bottom of each window is 'enabled'.

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

Балансировка нагрузки

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



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

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

The screenshot displays the Mikrotik WinBox interface. The 'Route List' window is open, showing a table of routes. The route for 10.120.0.0/24 via tunnel21 is highlighted, and its 'Distance' is set to 10. A dialog box for editing this route is also open, showing the 'Distance' field set to 10. The 'Interface List' window shows the configuration of interfaces, including tunnel21 and tunnel22.

Src	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	172.16.21.1 reachable ether2	1	21	
AS	0.0.0.0/0	172.16.22.1 reachable ether9	1	22	
AS	10.120.0.0/24	tunnel22 reachable	1		
S	10.120.0.0/24	tunnel21 reachable	10		
DAC	10.125.0.0/24	tunnel1 reachable	0		10.125.0.2
DAC	172.16.21.0/24	ether2 reachable	0		172.16.21.2
DAC	172.16.22.0/24	ether9 reachable	0		172.16.22.2
DAC	192.168.21.0/...	tunnel21 reachable	0		192.168.21.1
DAC	192.168.22.0/...	tunnel22 reachable	0		192.168.22.1

Route <10.120.0.0/24> configuration:

- General: Dst. Address: 10.120.0.0/24, Gateway: tunnel21, reachable
- Attributes: Type: unicast, Distance: 10, Scope: 30, Target Scope: 10, Routing Mark: , Pref. Source:

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

The screenshot shows the configuration window for an interface named 'tunnel21'. The window has two tabs: 'General' and 'Traffic'. The 'General' tab is active. The configuration fields are as follows:

- Name: tunnel21
- Type: GRE Tunnel
- MTU: 1400
- L2 MTU: 65535
- Local Address: 172.16.21.2
- Remote Address: 10.0.12.2
- Keepalive Interval: 00:00:03 (highlighted with a blue oval)
- DSCP: 0

On the right side of the window, there are several buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, and Torch. At the bottom of the window, there are three status indicators: 'enabled', 'running', and 'slave'.

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

Опция Keepalive

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

The screenshot shows the Mikrotik WinBox interface. The 'Route List' window is open, displaying the 'Routes' tab. The table below shows the current routing table:

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	172.16.21.1 reachable ether2	1	21	
AS	0.0.0.0/0	172.16.22.1 reachable ether9	1	22	
S	10.120.0.0/24	tunnel22 unreachable, tunnel21 unreachable	1		
DAC	10.125.0.0/24	ether1 reachable	0		10.125.0.2
DAC	172.16.21.0/24	ether2 reachable	0		172.16.21.2
DAC	172.16.22.0/24	ether9 reachable	0		172.16.22.2
DC	192.168.21.0/24	tunnel21 unreachable	255		192.168.21.1
DC	192.168.22.0/24	tunnel22 unreachable	255		192.168.22.1

The 'Interface List' window on the left shows the following interfaces:

Interface	Name
R	ether1
R	ether2
	ether3
	ether4
	ether5
	ether6
	ether7
	ether8
R	ether9
	tunnel21
	tunnel22

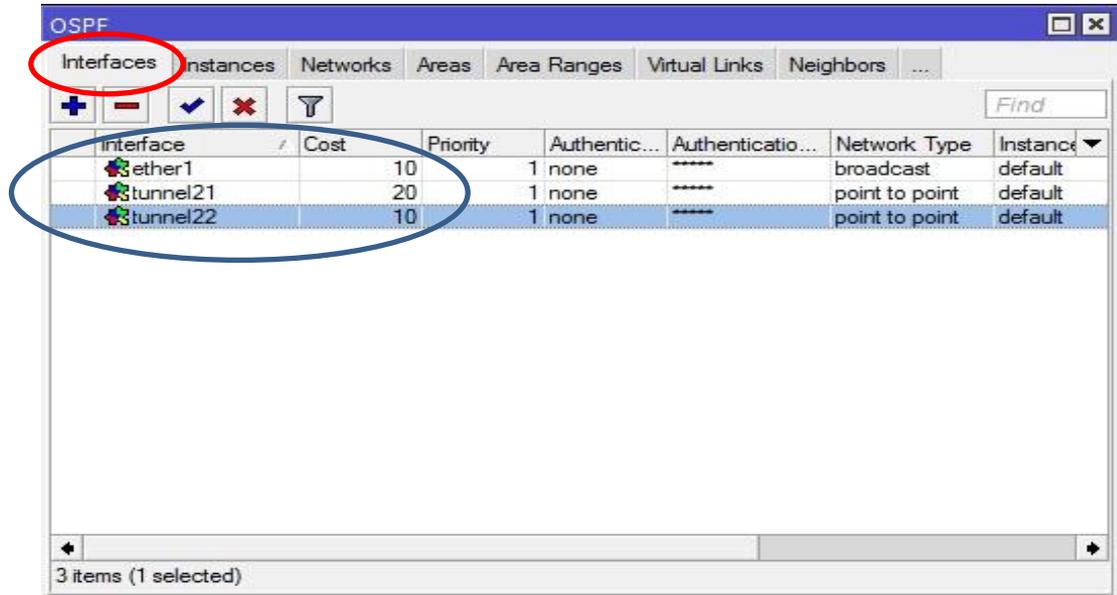
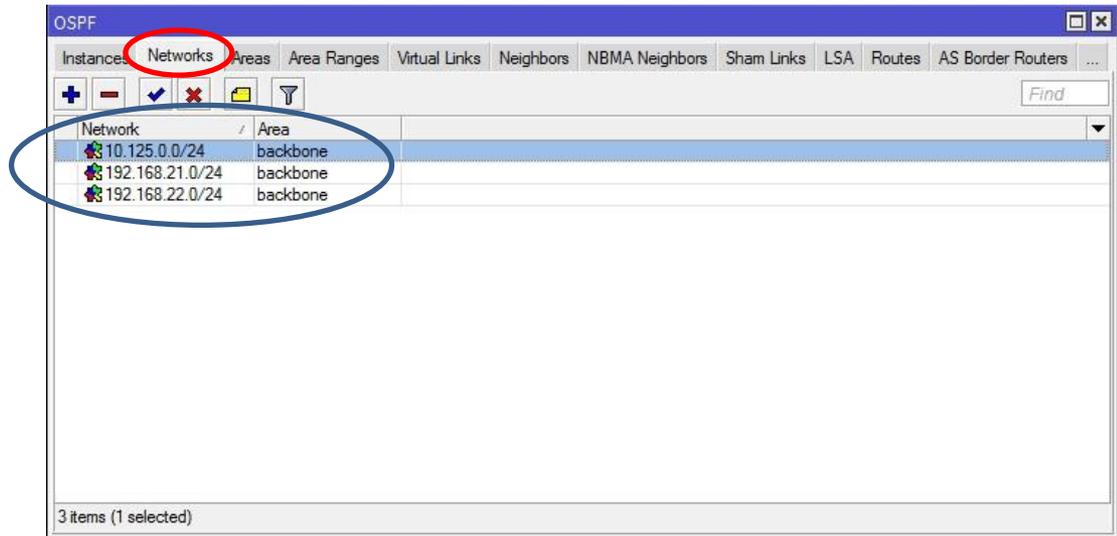
Простой метод создания отказоустойчивого VPN между роутером Mikrotik и оборудованием другого производителя

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 одинаковой по умолчанию, поэтому включится балансировка нагрузки по двум каналам. Чтобы избежать балансировки и выставить приоритеты маршрутов, можно вручную поменять значение cost на интерфейсе



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

?

Сколько времени потребуется OSPF с дефолтными настройками для переключения маршрута?

Простейший тюнинг OSPF

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

The screenshot shows the OSPF configuration window for interface tunnel21. The 'General' tab is active. The configuration includes:

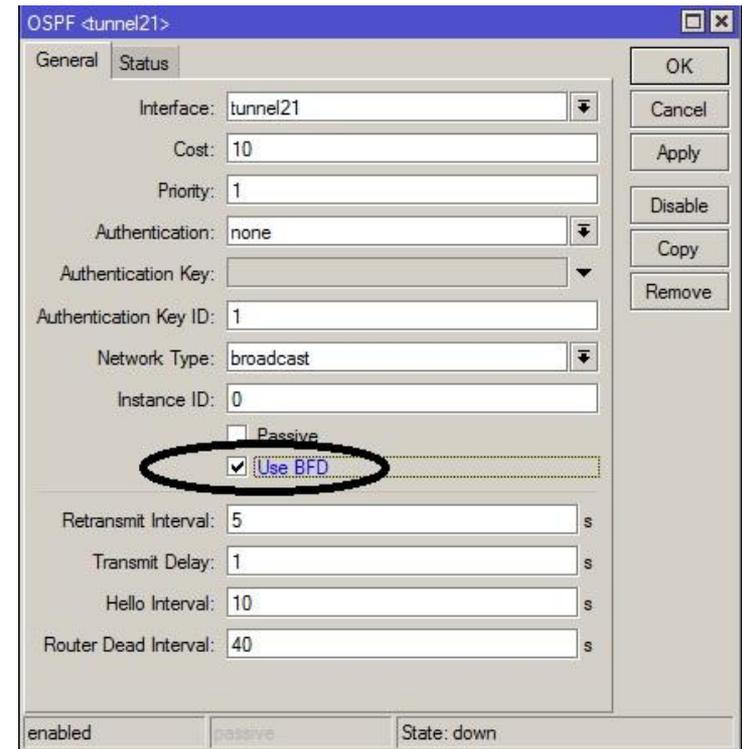
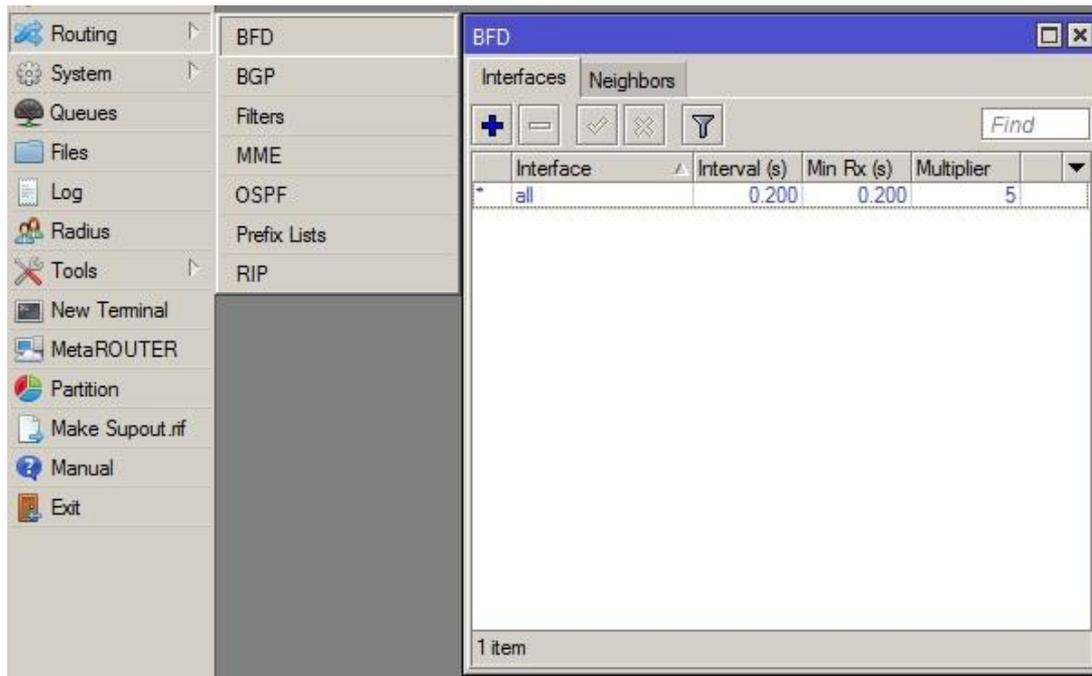
- Interface: tunnel21
- Cost: 20
- Priority: 1
- Authentication: none
- Authentication Key: (empty)
- Authentication Key ID: 1
- Network Type: point to point
- Instance ID: 0
- Passive:
- Use BFD:
- Retransmit Interval: 5 s
- Transmit Delay: 1 s
- Hello Interval: 10 s
- Router Dead Interval: 40 s

The 'Hello Interval' and 'Router Dead Interval' fields are circled in red, indicating they must be equal for tunnel interfaces. The status bar at the bottom shows 'enabled', 'passive', and 'State: point to point'.

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

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!