

# **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, MTCTSE

# Цель презентации

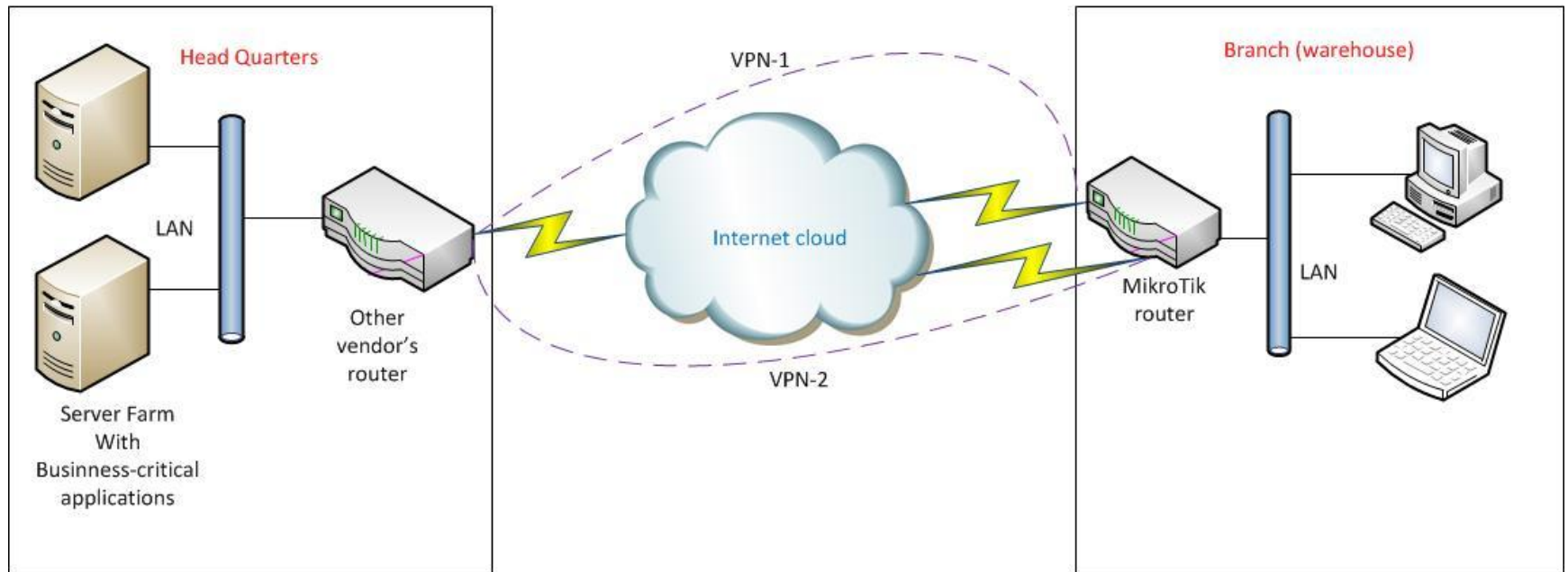
Показать на практическом примере:

- 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

Interface	Name	Type	L2 MTU	Tx
R	ether1	Ethernet	1526	
R	ether2	Ethernet	1522	
	ether3	Ethernet	1522	
	ether4	Ethernet	1522	
	ether5	Ethernet	1522	
	ether6	Ethernet	1522	
	ether7	Ethernet	1522	
	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

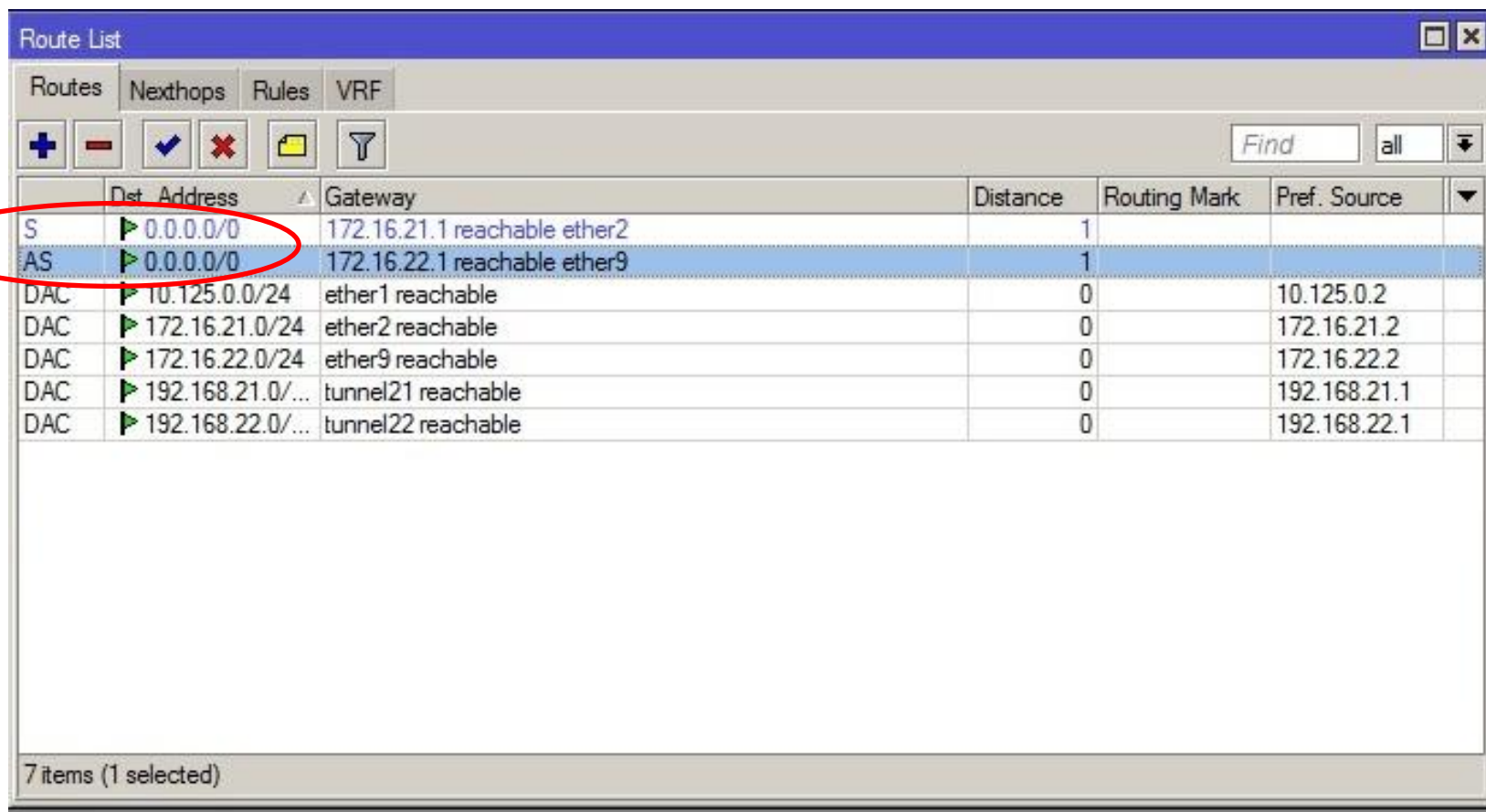
Простой метод создания отказоустойчивого VPN между роутером MikroTik и оборудованием другого производителя



# 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

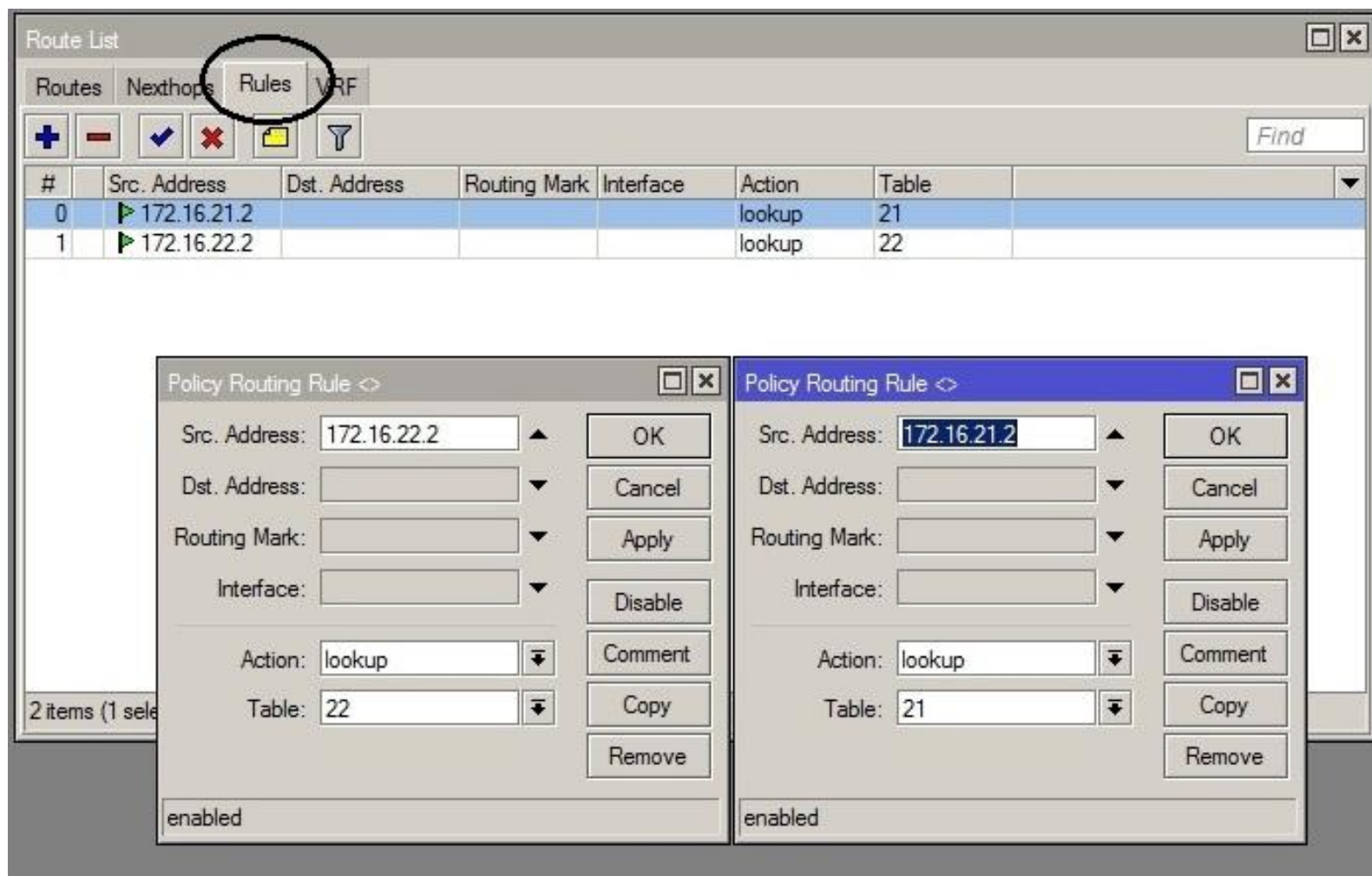
# Решение: использование Policy Based Routing (PBR)

	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

7 items (1 selected)

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

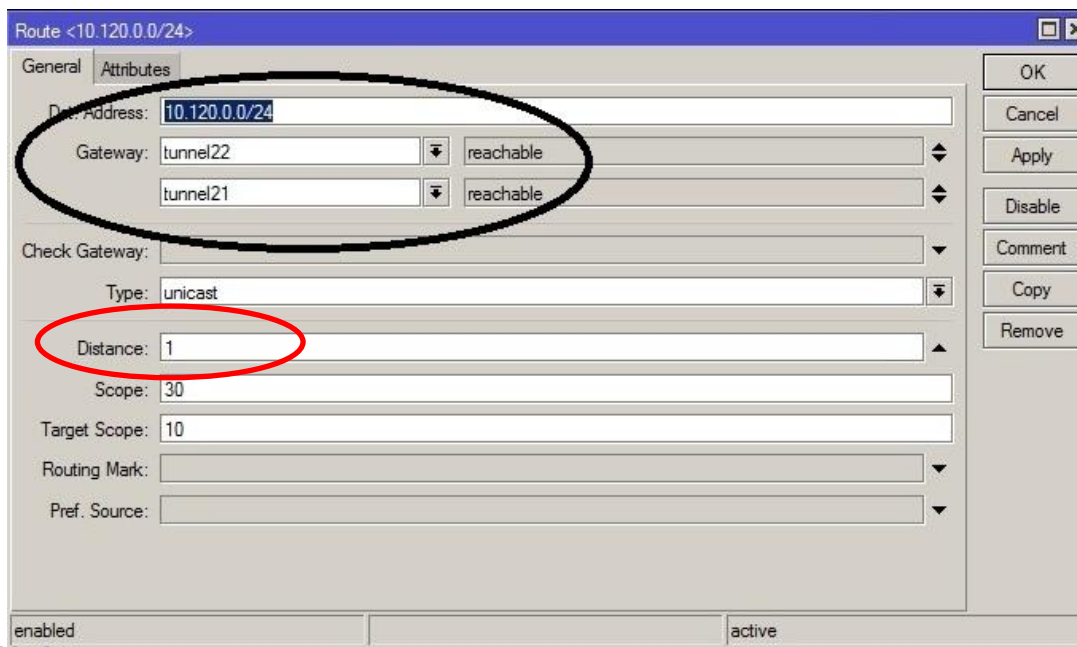
# PBR: Route Rules



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. On the left, the 'Interface List' shows 'tunnel21' and 'tunnel22' selected. The main 'Route List' window shows a table of routes. A red oval highlights the route for '10.120.0.0/24' via 'tunnel21' with a distance of 10. Below this, the 'Route <10.120.0.0/24>' configuration window is open, showing the 'General' tab. A red oval highlights the 'Distance' field, which is set to 10. The 'Gateway' is set to 'tunnel21' and 'reachable'. The 'Type' is 'unicast'. The 'Scope' is 30 and 'Target Scope' is 10. The 'Routing Mark' and 'Pref. Source' fields are empty. The 'enabled' checkbox is checked.

Routes	Nexthops	Rules	VRF
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
DAC	172.16.21.0/24	ether2 reachable	0
DAC	172.16.22.0/24	ether9 reachable	0
DAC	192.168.21.0/24	tunnel21 reachable	0
DAC	192.168.22.0/24	tunnel22 reachable	0

Route <10.120.0.0/24>

General Attributes

Dst. Address: 10.120.0.0/24

Gateway: tunnel21 reachable

Check Gateway:

Type: unicast

Distance: 10

Scope: 30

Target Scope: 10

Routing Mark:

Pref. Source:

enabled active

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

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: 00:00:03

DSCP: 0

OK Cancel Apply Disable Comment Copy Remove Torch

enabled running 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 a table of routes. The 'Routes' tab is selected. The table has columns: Dst. Address, Gateway, Distance, Routing Mark, Pref., and Source. The following routes are listed:

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 is also visible on the left, showing a list of interfaces. The 'tunnel21' and 'tunnel22' entries are highlighted with red circles, indicating they are unreachable.

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

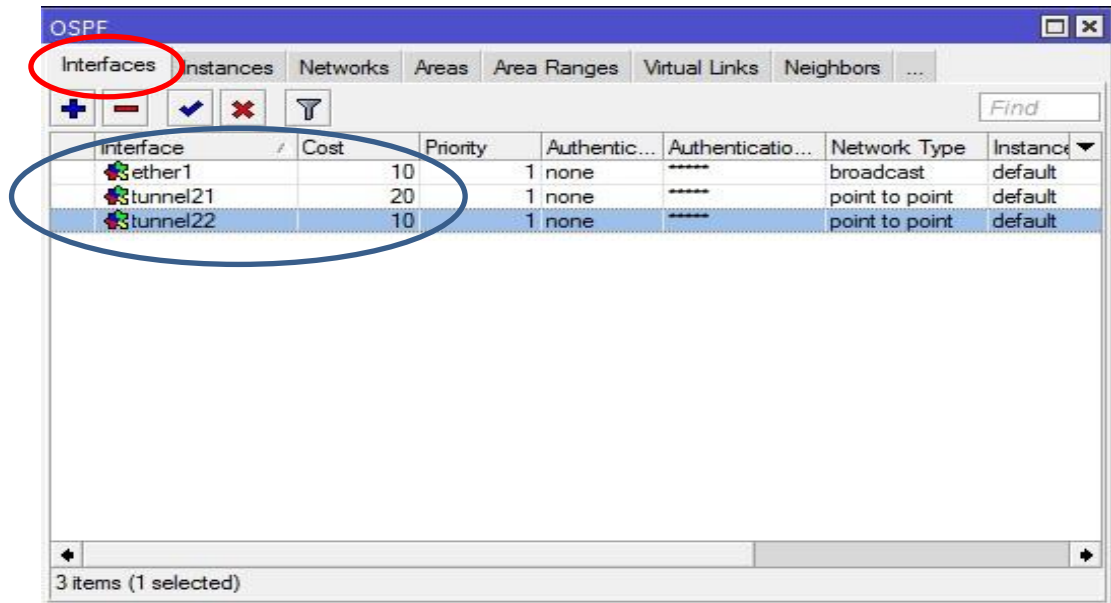
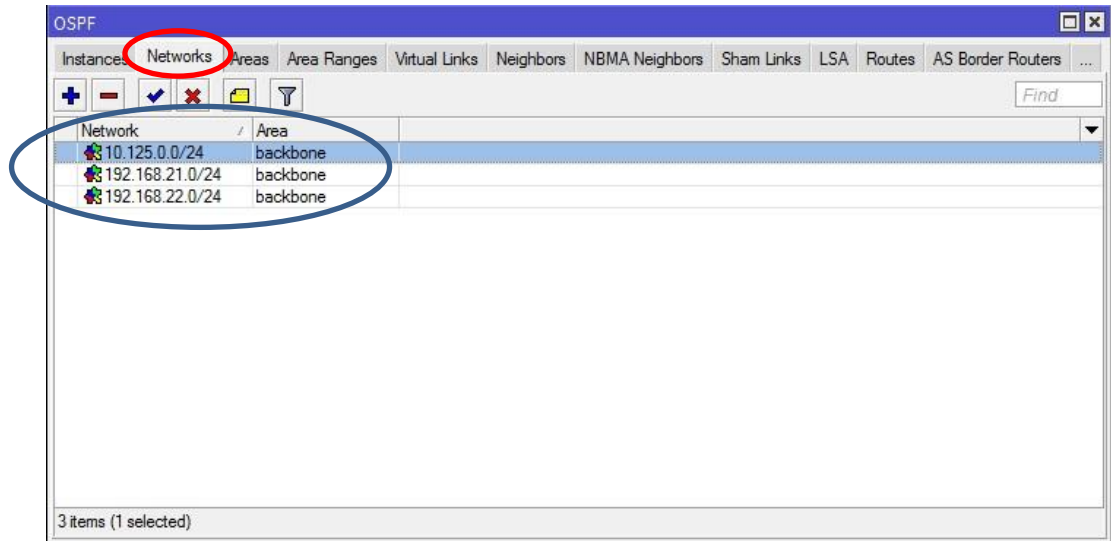
# Опция Keeralive

- Но что делать, если роутер другого производителя не поддерживает опцию keeralive 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!

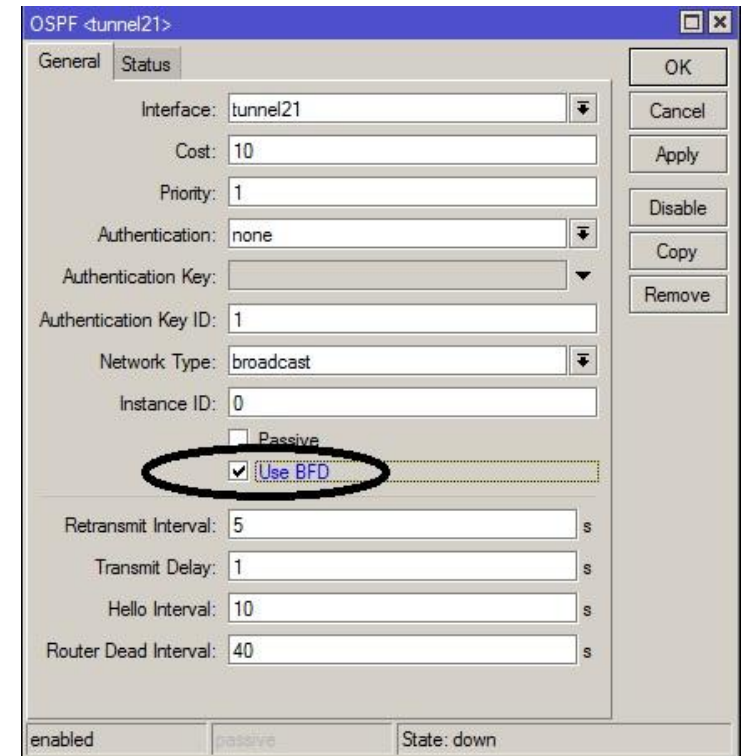
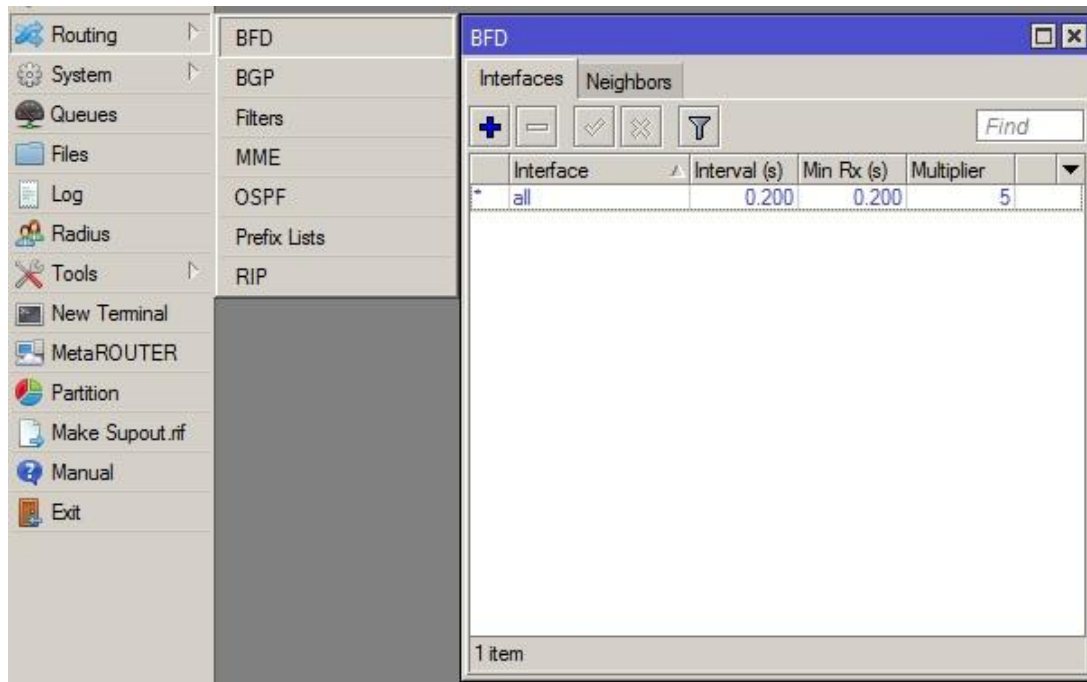
The screenshot shows the 'OSPF <tunnel21>' configuration window. The 'General' tab is active. The 'Interface' is 'tunnel21', 'Cost' is 20, 'Priority' is 1, 'Authentication' is 'none', 'Authentication Key' is empty, 'Authentication Key ID' is 1, 'Network Type' is 'point to point', and 'Instance ID' is 0. The 'Retransmit Interval' is 5s, 'Transmit Delay' is 1s, 'Hello Interval' is 10s, and 'Router Dead Interval' is 40s. The 'Hello Interval' and 'Router Dead Interval' are circled in red. The 'Passive' and 'Use BFD' checkboxes are unchecked. The 'Status' tab is also visible. At the bottom, the state is 'enabled', 'passive', and 'State: point to point'.

Field	Value
Interface	tunnel21
Cost	20
Priority	1
Authentication	none
Authentication Key	
Authentication Key ID	1
Network Type	point to point
Instance ID	0
Retransmit Interval	5 s
Transmit Delay	1 s
Hello Interval	10 s
Router Dead Interval	40 s

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!