

Отказоустойчивый VPN 2-го и 3-го уровня между роутером MikroTik и оборудованием других производителей.

Алексей Чудин
MUM
2014

Обо мне

Меня зовут Алексей Чудин

Опыт работы с сетями почти 10 лет

Сертифицированный тренер MikroTik

Сертификаты: MTCNA, MTCRE, MTCWE,
MTCTSE, MTCUME, MTCINE

Microsoft: MCP, MCSA

Cisco: CCNA, CCNP (R&S)

Цель презентации

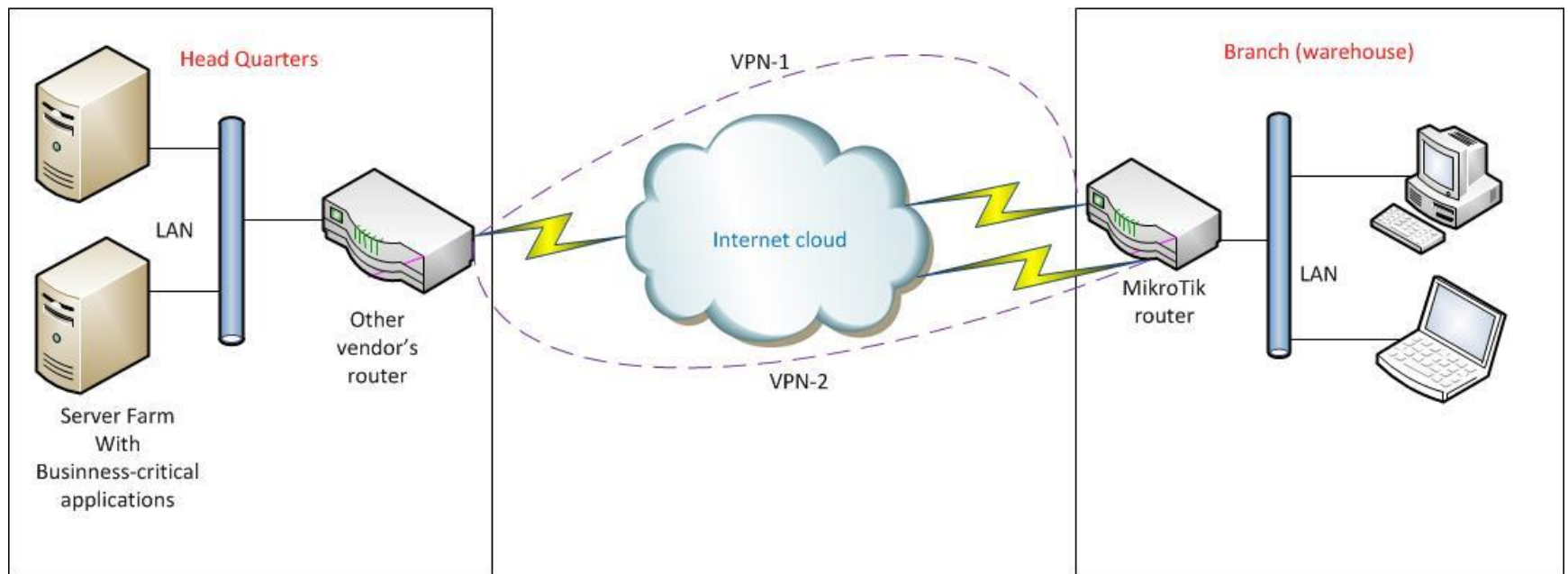
Показать на практическом примере:

- создание отказоустойчивых VPN используя GRE-туннели,
- конфигурирование Policy Based Routing при использовании нескольких провайдеров,
- изменение приоритетов маршрутов
- уменьшение времени переключения каналов
- создание отказоустойчивых туннелей на 2-м уровне (EoIP)

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 ADSL-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



Simple Method to Organize
Branch-VPN Failover between
MikroTik and Other Vendor's
Router Over WAN



Simple Method to Organize
Branch-VPN Failover between
MikroTik and Other Vendor's
Router Over WAN

Aleksei Chudin

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

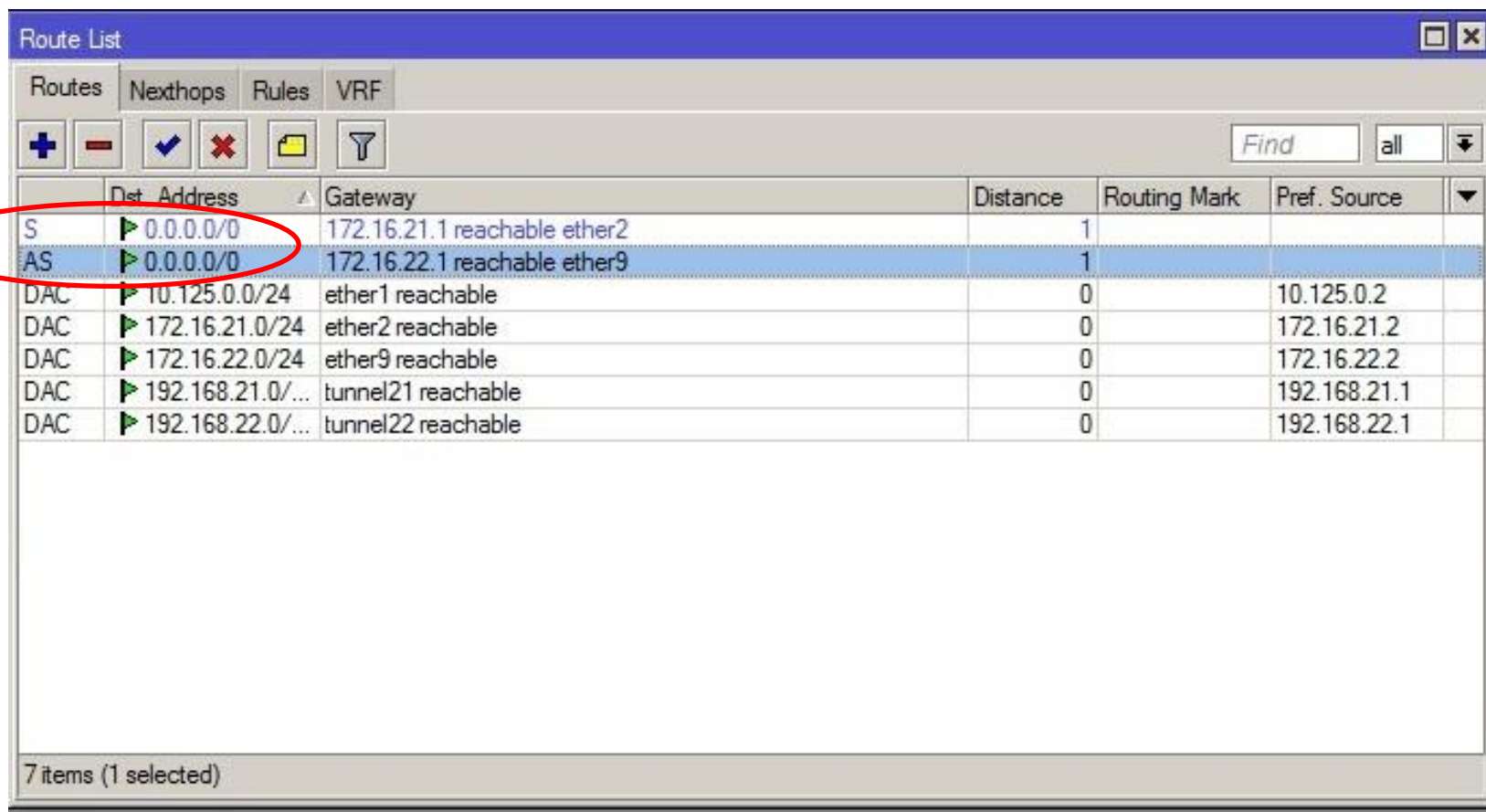
enabled running slave

IP адрес роутера на другом конце туннеля

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)

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)

PBR: Route Rules

The screenshot shows the Mikrotik WinBox interface. The 'Route List' window is open, with the 'Rules' tab selected. The 'Rules' tab contains a table with the following data:

#	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' dialog boxes are open. The left dialog box shows the configuration for rule 22, and the right dialog box shows the configuration for rule 21.

Policy Routing Rule <> (Left Dialog)

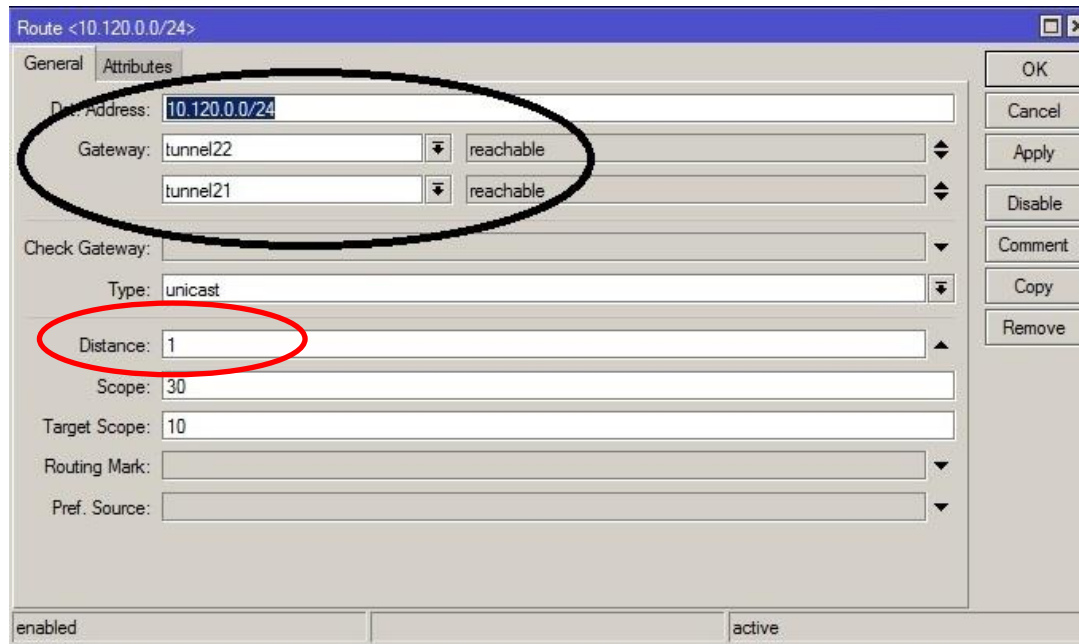
- Src. Address: 172.16.22.2
- Dst. Address: (empty)
- Routing Mark: (empty)
- Interface: (empty)
- Action: lookup
- Table: 22
- Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove
- Status: enabled

Policy Routing Rule <> (Right Dialog)

- Src. Address: 172.16.21.2
- Dst. Address: (empty)
- Routing Mark: (empty)
- Interface: (empty)
- Action: lookup
- Table: 21
- Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove
- Status: enabled

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

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 is highlighted, showing two gateways: tunnel21 (Distance 1) and tunnel22 (Distance 10). A black oval highlights these two entries in the table. Below the table, the 'Interface List' shows tunnel21 and tunnel22 as GRE Tunnels. A second window, 'Route <10.120.0.0/24>', is open, showing the configuration for this specific route. The 'Distance' field is set to 10, and a black oval highlights this field. The 'Gateway' is set to tunnel21, and the 'Type' is set to unicast.

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: [v]

Type: unicast

Distance: 10

Scope: 30

Target Scope: 10

Routing Mark: [v]

Pref. Source: [v]

enabled active

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

Simple Method to Organize
Branch-VPN Failover between
MikroTik and Other Vendor's
Router Over WAN

Опция Keepalive

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

The screenshot displays the Mikrotik WinBox interface. On the left, the 'Interface List' shows a list of interfaces including ether1 through ether9, and tunnel21 and tunnel22, which are highlighted with a red circle. On the right, the 'Route List' window is open, showing a table of routes. The table has columns for Dst. Address, Gateway, Distance, Routing Mark, Pref., and Source. The routes for tunnel21 and tunnel22 are highlighted with a red circle, showing 'unreachable' status. The bottom status bar indicates '11 items (1 selected)'.

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/...	tunnel21 unreachable	255		192.168.21.1	
DC 192.168.22.0/...	tunnel22 unreachable	255		192.168.22.1	

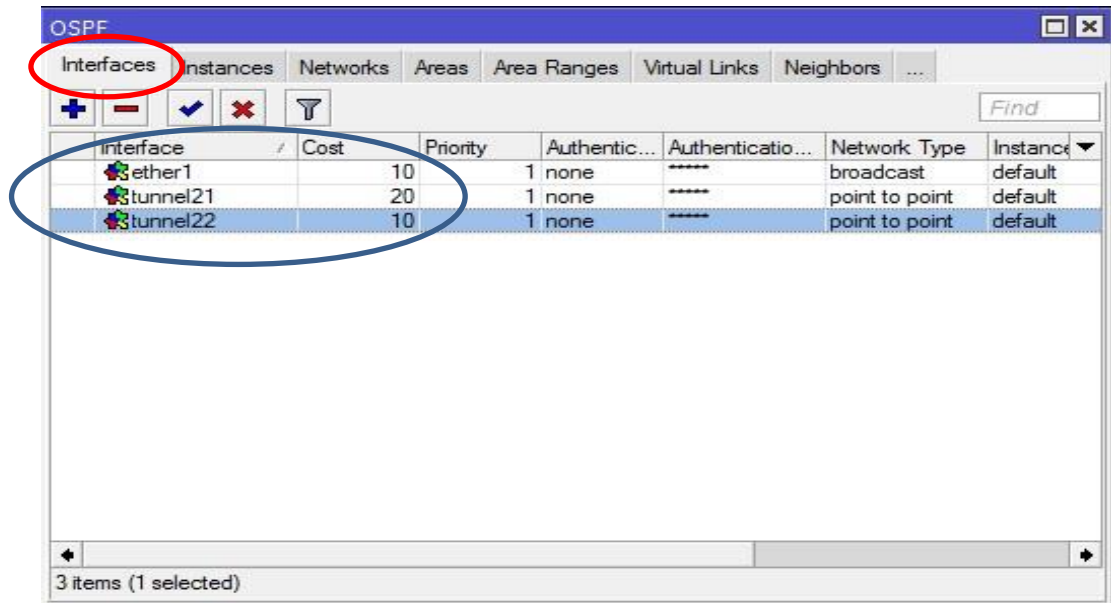
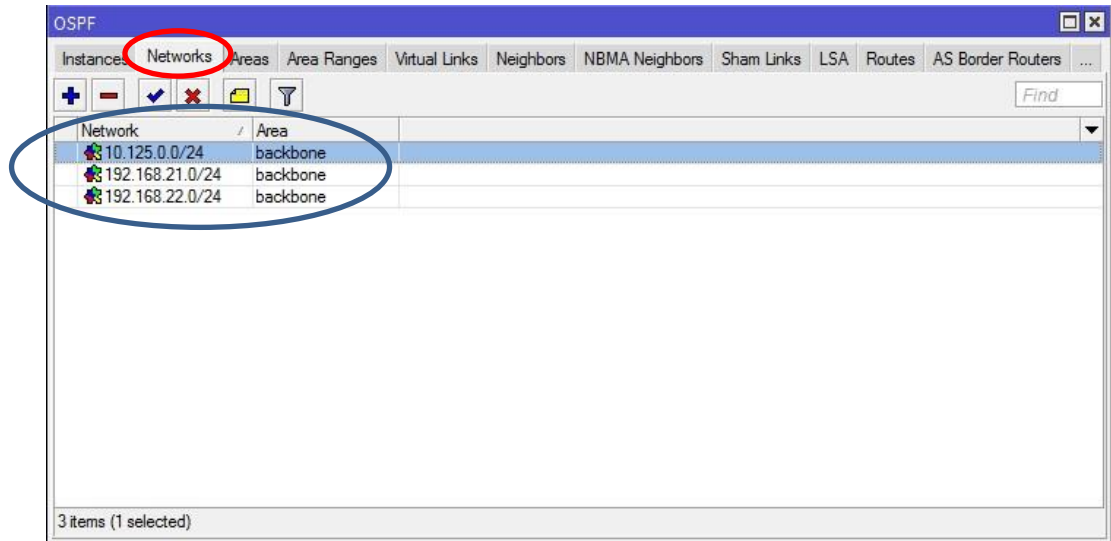
Name	Type	MTU	Speed	Mode	Admin Dist	Oper Dist
ether1	Ethernet	1522	528 bps	480 bps	1	0
ether2	Ethernet	1522	528 bps	480 bps	1	0
ether3	Ethernet	1522	528 bps	480 bps	1	0
ether4	Ethernet	1522	528 bps	480 bps	1	0
ether5	Ethernet	1522	528 bps	480 bps	1	0
ether6	Ethernet	1522	528 bps	480 bps	1	0
ether7	Ethernet	1522	528 bps	480 bps	1	0
ether8	Ethernet	1522	528 bps	480 bps	1	0
ether9	Ethernet	1522	528 bps	480 bps	1	0
tunnel21	GRE Tunnel	65535	528 bps	0 bps	1	0
tunnel22	GRE Tunnel	65535	528 bps	0 bps	1	0

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



?

Сколько времени потребуется OSPF с
дефолтными настройками для переключения
маршрута (broadcast network)?

Простейший тюнинг OSPF

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

OSPF <tunnel21>

General Status

Interface: tunnel21

Cost: 20

Priority: 1

Authentication: none

Authentication Key:

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

OK

Cancel

Apply

Disable

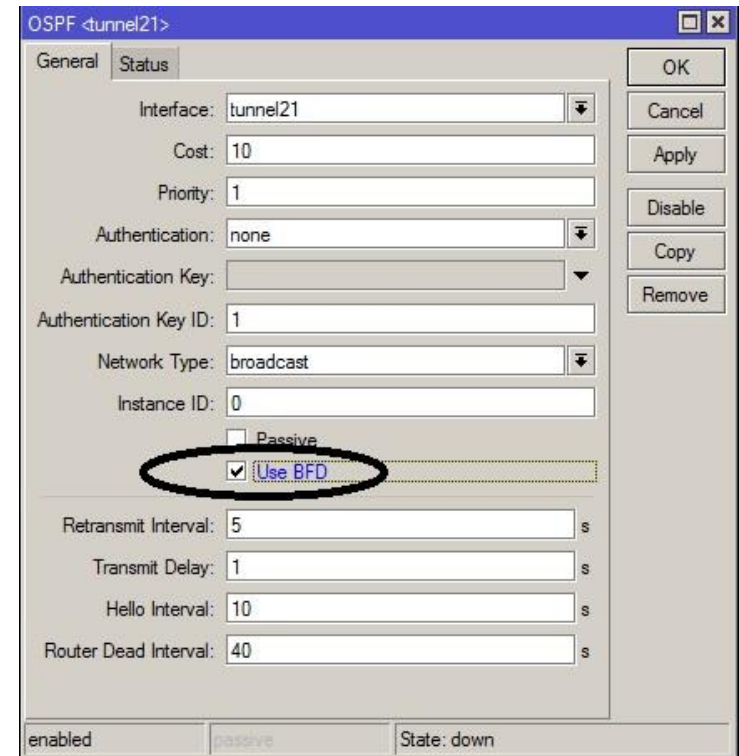
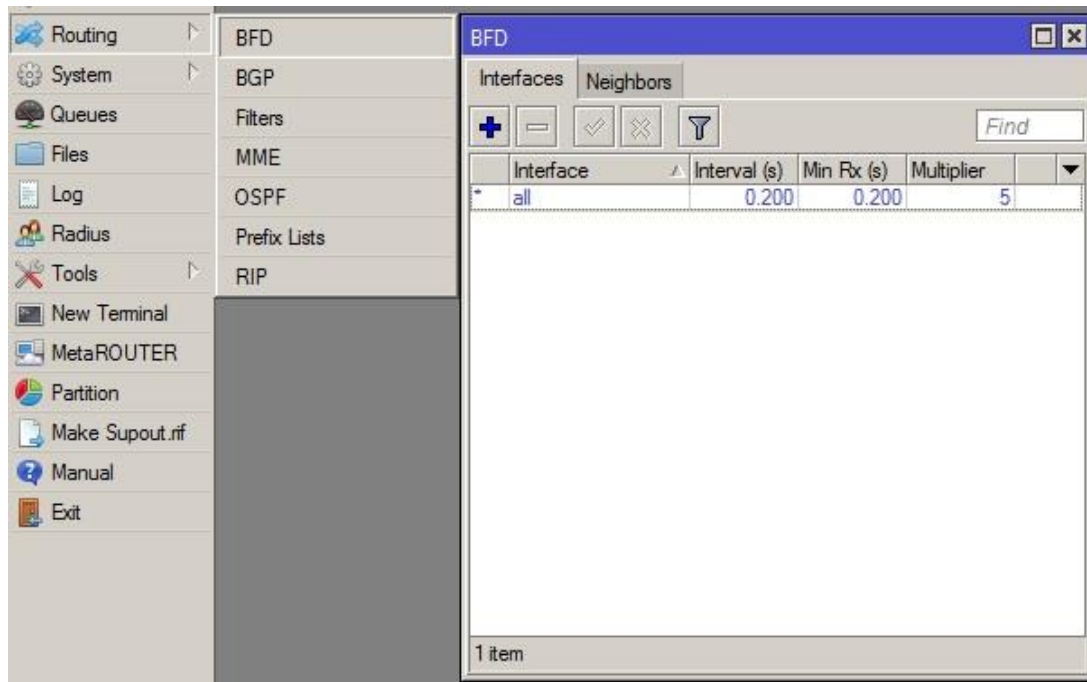
Copy

Remove

enabled passive State: point to point

Продвинутый тюнинг OSPF

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



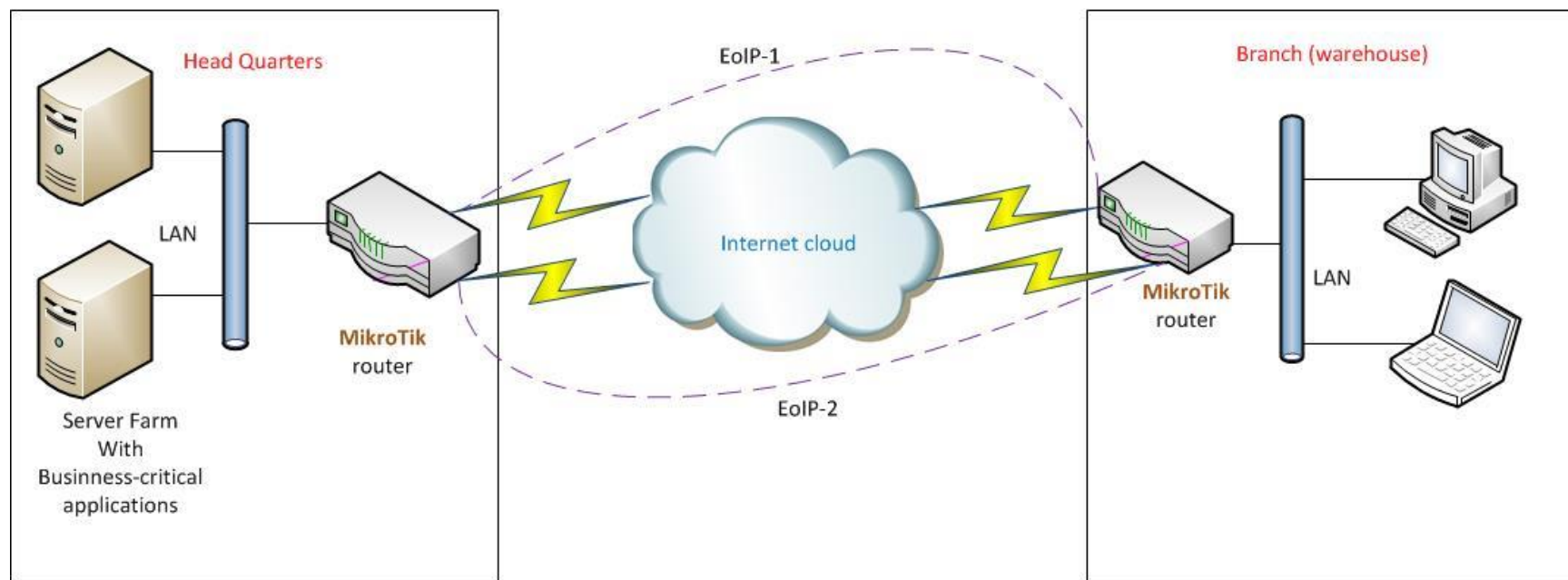
Выводы

Итак, мы рассмотрели простые методы организации отказоустойчивых VPN между MikroTik и оборудованием других производителей через WAN.

Наиболее важные заключения:

- GRE туннели очень полезны для данной задачи
- Мы можем использовать PBR для того, чтобы направить трафик каждого туннеля через соответствующего провайдера
- Мы можем проверять статус GRE-туннеля на противоположном конце с помощью опции keepalive (она должна быть активирована на обоих концах туннеля)
- Можно использовать балансировку нагрузки между туннелями, то есть суммировать пропускную способность каналов провайдеров. Либо можно использовать один туннель как основной, а другой как резервный. Делаем это при помощи distance (static routing), либо изменив cost на интерфейсе (OSPF)
- При использовании OSPF мы можем изменить Hello и Dead интервалы для уменьшения времени переключения каналов
- При этом важно не забыть, что MTU, Hello и Dead интервалы должны быть одинаковыми на обоих концах туннеля

Отказоустойчивый VPN 2-го уровня на основе EoIP-туннелей



Настраиваем EoIP-туннели

The image displays two side-by-side configuration windows for EoIP tunnels in MikroTik WinBox. Both windows are titled 'Interface <eoip-tunnel1>' and 'Interface <eoip-tunnel2>' respectively. Each window has a 'General' tab and a 'Traffic' tab. The 'General' tab is active in both.

Interface <eoip-tunnel1> Configuration:

- Name: eoip-tunnel1
- Type: EoIP Tunnel
- MTU: 1500
- Actual MTU: 1500
- L2 MTU: 65535
- MAC Address: 02:8E:19:83:EE:E2
- ARP: enabled
- Local Address: 10.0.11.1 (highlighted with a red circle)
- Remote Address: 10.0.14.2 (highlighted with a red circle)
- Tunnel ID: 1
- Keepalive Interval: 00:00:01 (highlighted with a red circle)
- DSCP: inherit
- Dont Fragment: no
- ☒ Clamp TCP MSS

Interface <eoip-tunnel2> Configuration:

- Name: eoip-tunnel2
- Type: EoIP Tunnel
- MTU: 1500
- Actual MTU: 1500
- L2 MTU: 65535
- MAC Address: 02:59:A0:61:0B:BF
- ARP: enabled
- Local Address: 10.0.21.1 (highlighted with a red circle)
- Remote Address: 10.0.23.2 (highlighted with a red circle)
- Tunnel ID: 2
- Keepalive Interval: 00:00:01 (highlighted with a red circle)
- DSCP: inherit
- Dont Fragment: no
- ☒ Clamp TCP MSS

At the bottom of each window, there are three status indicators: 'enabled', 'running', and 'slave'.

Добавляем маршруты по умолчанию

	Det	Address	Gateway	Distance	Routing Mark	Pref	Source
AS	▶	0.0.0.0/0	10.0.21.2 reachable ether3	1	2		
AS	▶	0.0.0.0/0	10.0.11.2 reachable ether1	1	1		
DAC	▶	10.0.11.0/24	ether1 reachable	0			10.0.11.1
DAC	▶	10.0.13.0/24	bridge1 reachable	0			10.0.13.100
DAC	▶	10.0.21.0/24	ether3 reachable	0			10.0.21.1

5 items

Добавляем Route Rules

The screenshot displays the Mikrotik WinBox interface. At the top, the 'Route List' window is open, showing a table of routes. Below it, two 'Policy Routing Rule' configuration windows are shown side-by-side, illustrating how to add rules for different source addresses.

Route List Table:

#	Src. Address	Dst. Address	Routing Mark	Interface	Action	Table
0	10.0.11.1				lookup	1
1	10.0.21.1				lookup	2

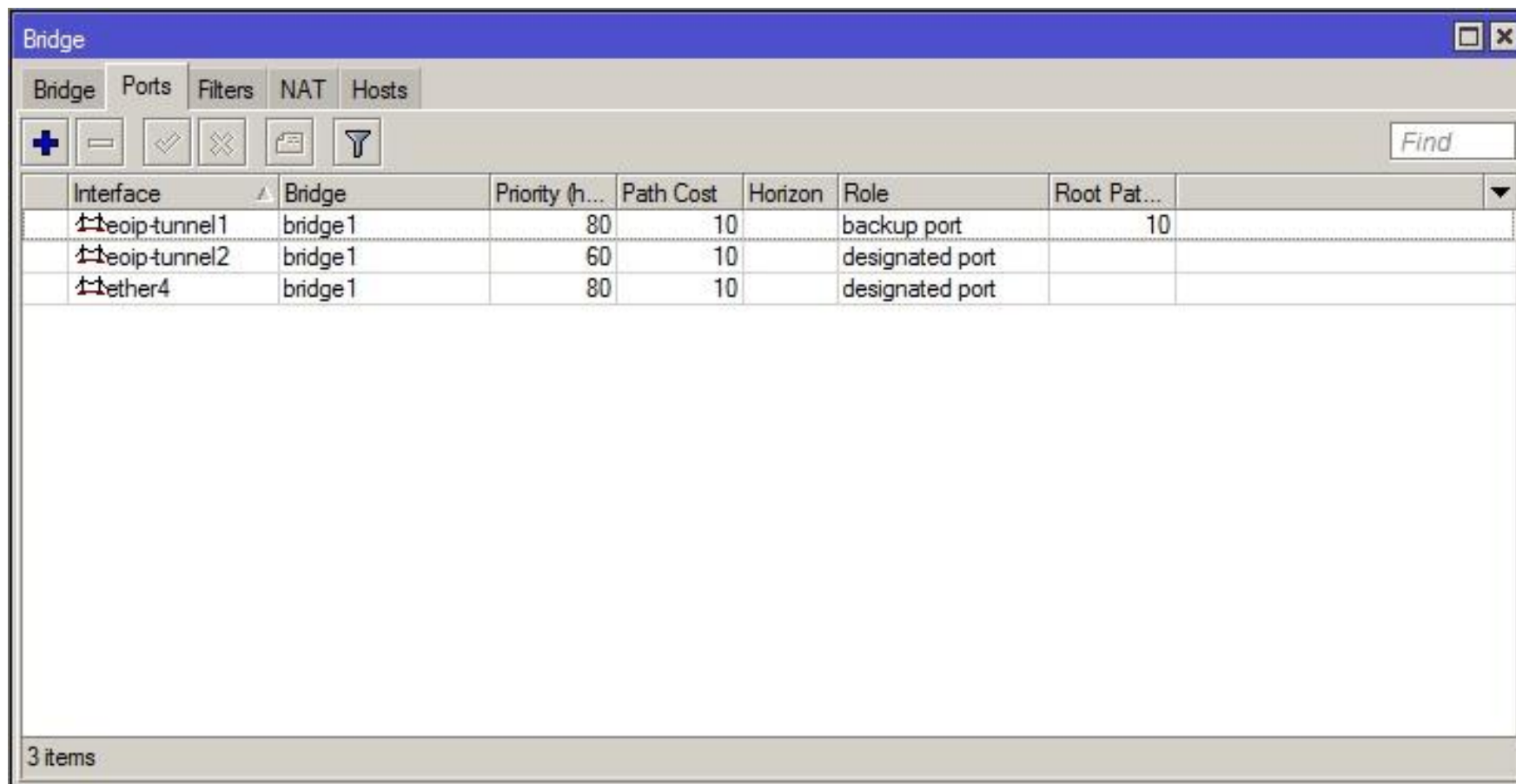
Policy Routing Rule Configuration (Left Window):

- Src. Address: 10.0.11.1
- Dst. Address: (empty)
- Routing Mark: (empty)
- Interface: (empty)
- Action: lookup
- Table: 1
- Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove
- Status: enabled

Policy Routing Rule Configuration (Right Window):

- Src. Address: 10.0.21.1
- Dst. Address: (empty)
- Routing Mark: (empty)
- Interface: (empty)
- Action: lookup
- Table: 2
- Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove
- Status: enabled

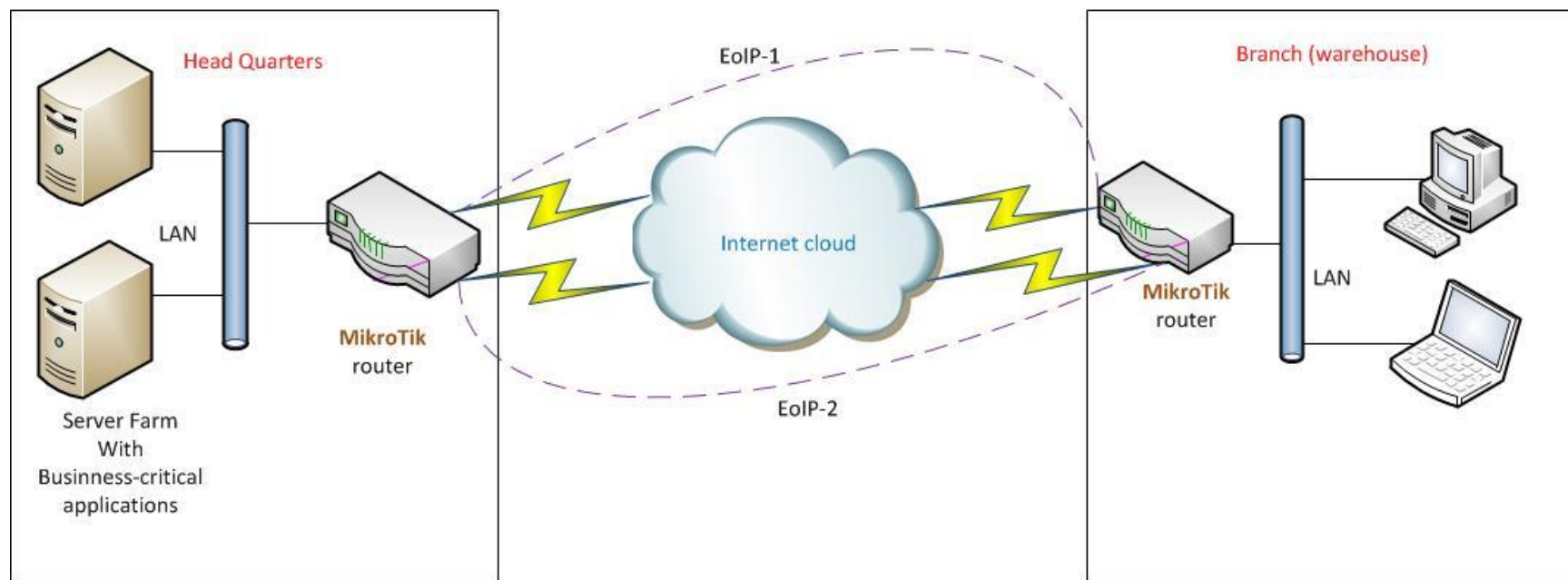
Добавляем интерфейсы в bridge



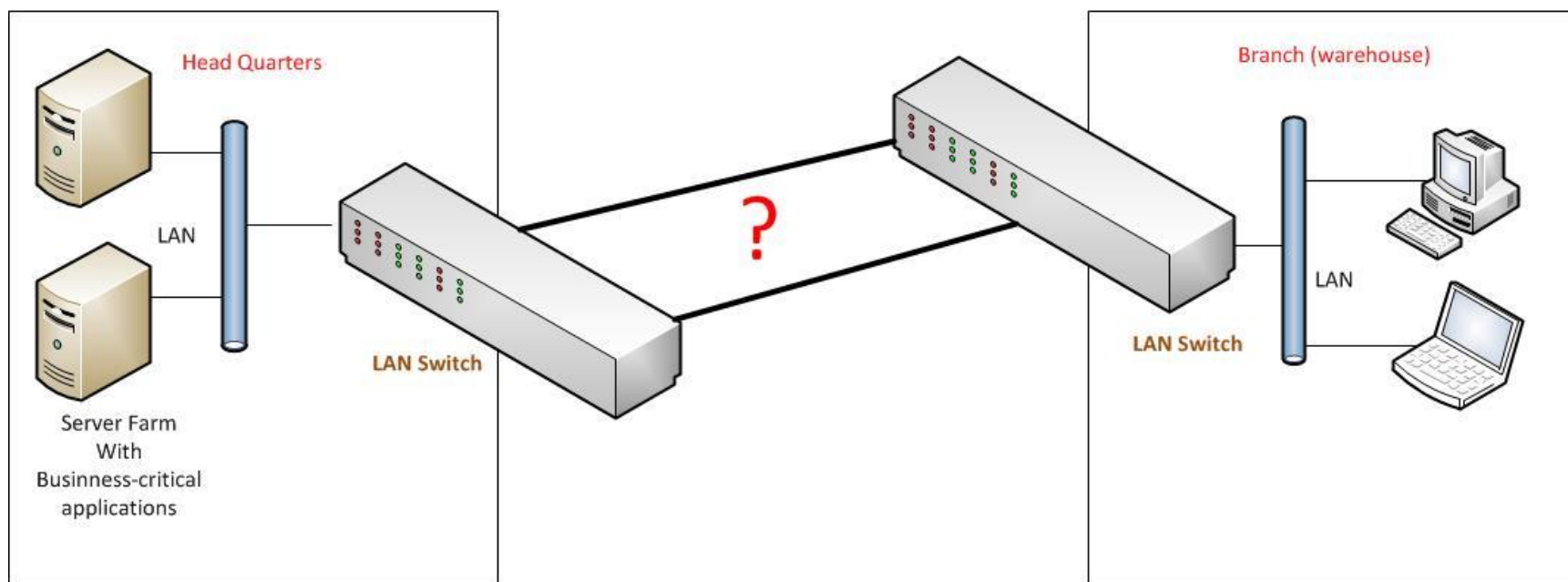
Interface	Bridge	Priority (h...	Path Cost	Horizon	Role	Root Pat...
eoip-tunnel1	bridge 1	80	10		backup port	10
eoip-tunnel2	bridge 1	60	10		designated port	
ether4	bridge 1	80	10		designated port	

3 items

Схема туннелей



Та же схема на 2-м уровне



Свойства бриджа

Interface <bridge1>

General STP Status Traffic

Protocol Mode: ☐ none ☐ stp ☒ rstp

Priority: 8000 hex

Max Message Age: 00:00:06

Forward Delay: 00:00:15

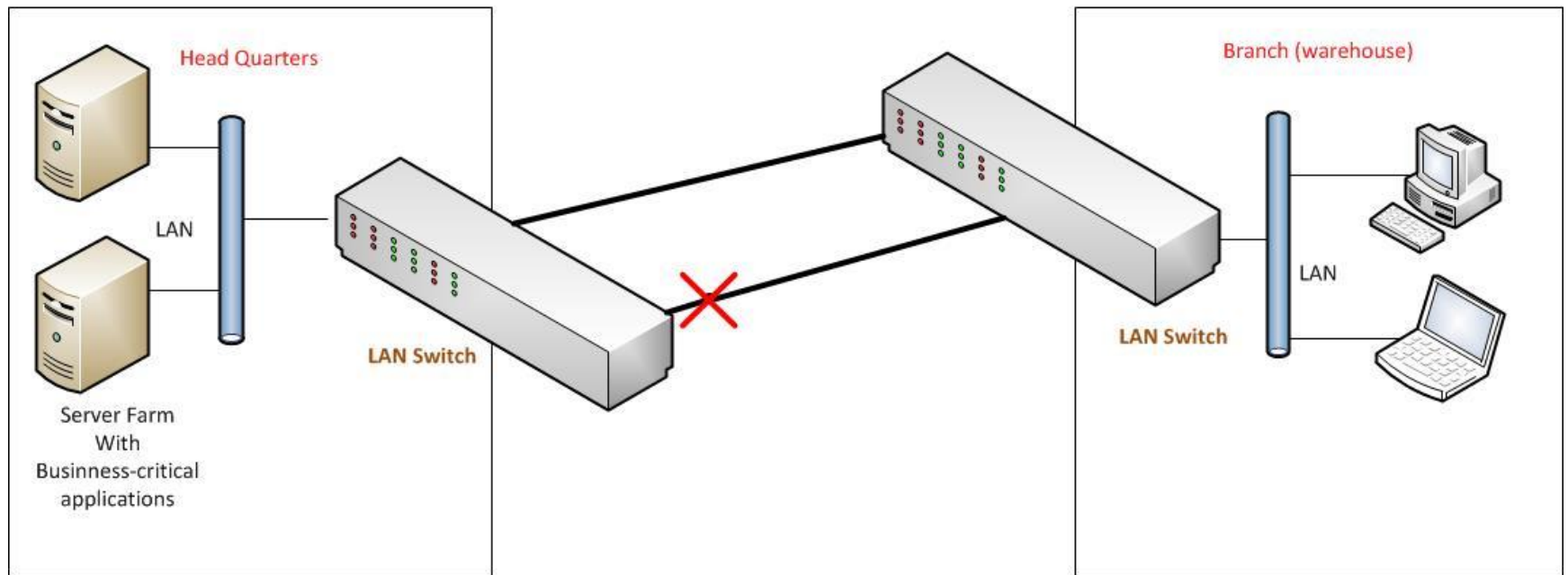
Transmit Hold Count: 6

Ageing Time: 00:05:00

OK Cancel Apply Disable Comment Copy Remove Torch

enabled running slave

RSTP, Backup port



RSTP, backup port, port priority

Bridge

Bridge Ports Filters NAT Hosts

+ - ✓ ✕ [icon] [icon] Find

Interface	Bridge	Priority (h...	Path Cost	Horizon	Role	Root Pat...
eoip-tunnel1	bridge1	80	10		backup port	10
eoip-tunnel2	bridge1	60	10		designated port	
ether4	bridge1	80	10		designated port	

3 items

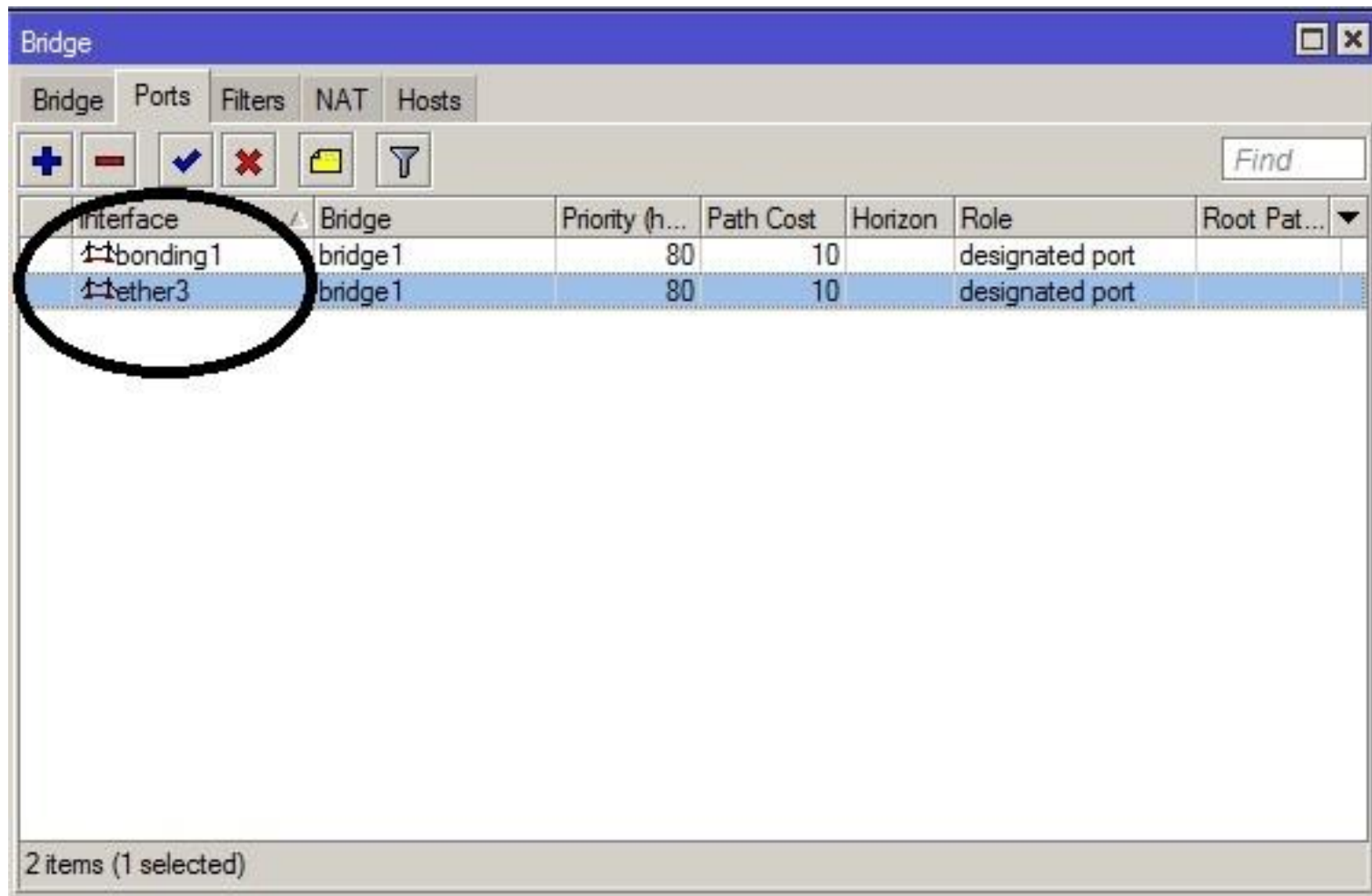
Bonding

The screenshot shows the 'New Interface' window with the 'Bonding' tab selected. The configuration is as follows:

- Slaves:** A list containing 'eoip-tunnel1' and 'eoip-tunnel2'. 'eoip-tunnel2' is currently selected.
- Mode:** 'balance rr' (selected)
- Primary:** 'none' (selected)
- Link Monitoring:** 'none' (selected)
- Transmit Hash Policy:** 'layer 2' (selected)
- Down Delay:** '0' ms
- Up Delay:** '0' ms
- LACP Rate:** '30 s' (selected)

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

Bonding+bridge



Interface	Bridge	Priority (h...	Path Cost	Horizon	Role	Root Pat...
bonding1	bridge1	80	10		designated port	
ether3	bridge1	80	10		designated port	

2 items (1 selected)

Вопросы?

Пишите на training@mikrotik-courses.ru

Спасибо за ваше
внимание!