DUAL-WAN

redundancja łącza danych

Ihor Hreskiv — MBUM #8 — Warszawa 09.2023

Ihor Hreskiv

MIKROTIK
CERTIFIED TRAINER

Jestem miłośnikiem urządzeń MikroTik od kilku lat

Lubię BSD/Linux

eve-ng fan

Najczęściej używam CHR

MTC(all)E

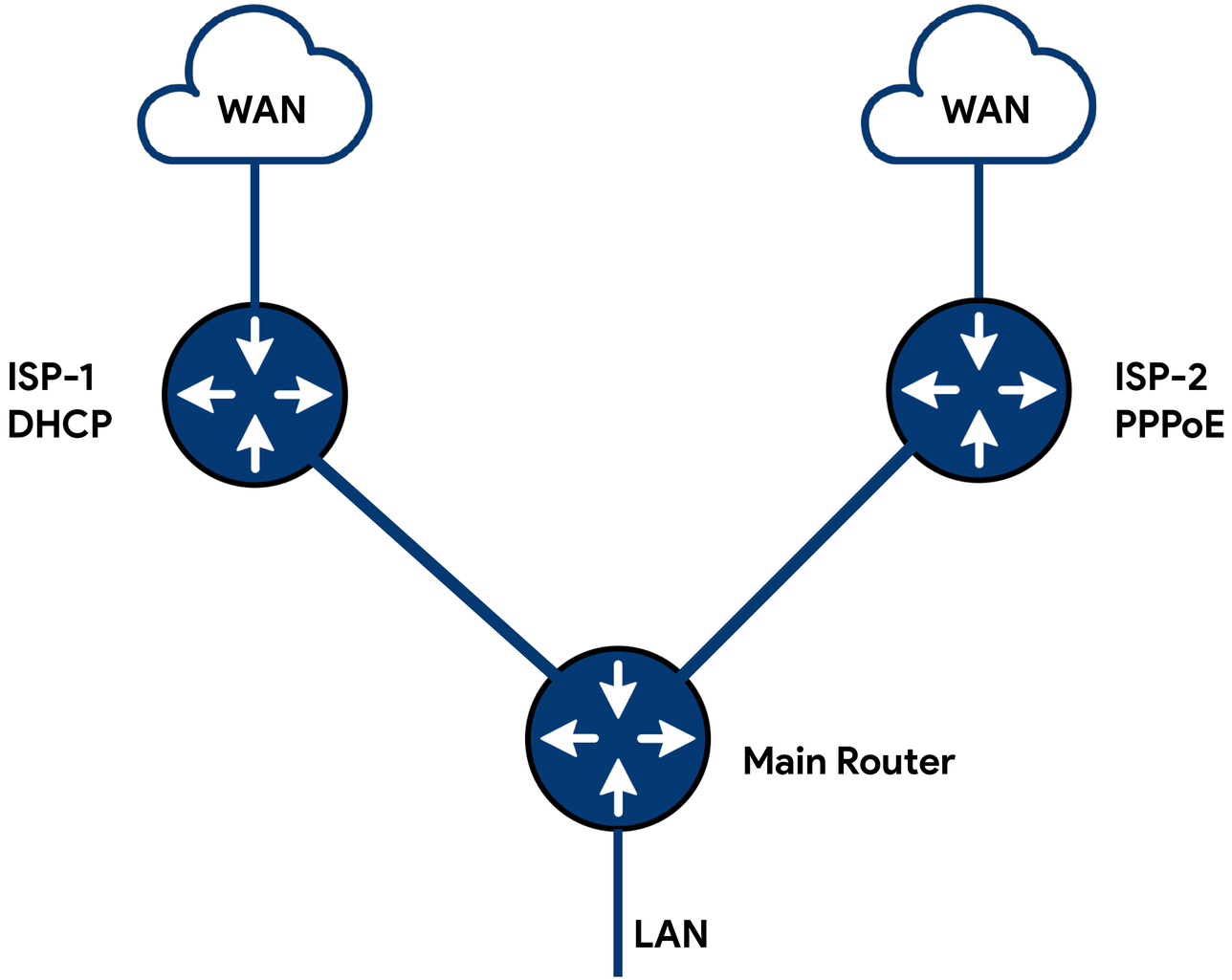
O co tu chodzi?

Active-Passive

Active-Active

Kombinacja Active-Passive oraz Active-Active

Schemat sieci



Dostawca usług ISP-1 przydziela adresacje za pomocą DHCP z puli adresowej 100.64.29.0/29

Dostawca usług ISP-2 ma uruchomiony PPPoE koncentrator i przydziela adres po stronie klienta 172.31.255.2

Sieć lokalna po stronie routera Main ma adresację 192.168.255.0/24

Active-Passive

Zadania do wykonania

Dodanie DHCP klienta od strony ISP-1

Dodanie PPPoE klienta od strony ISP-2

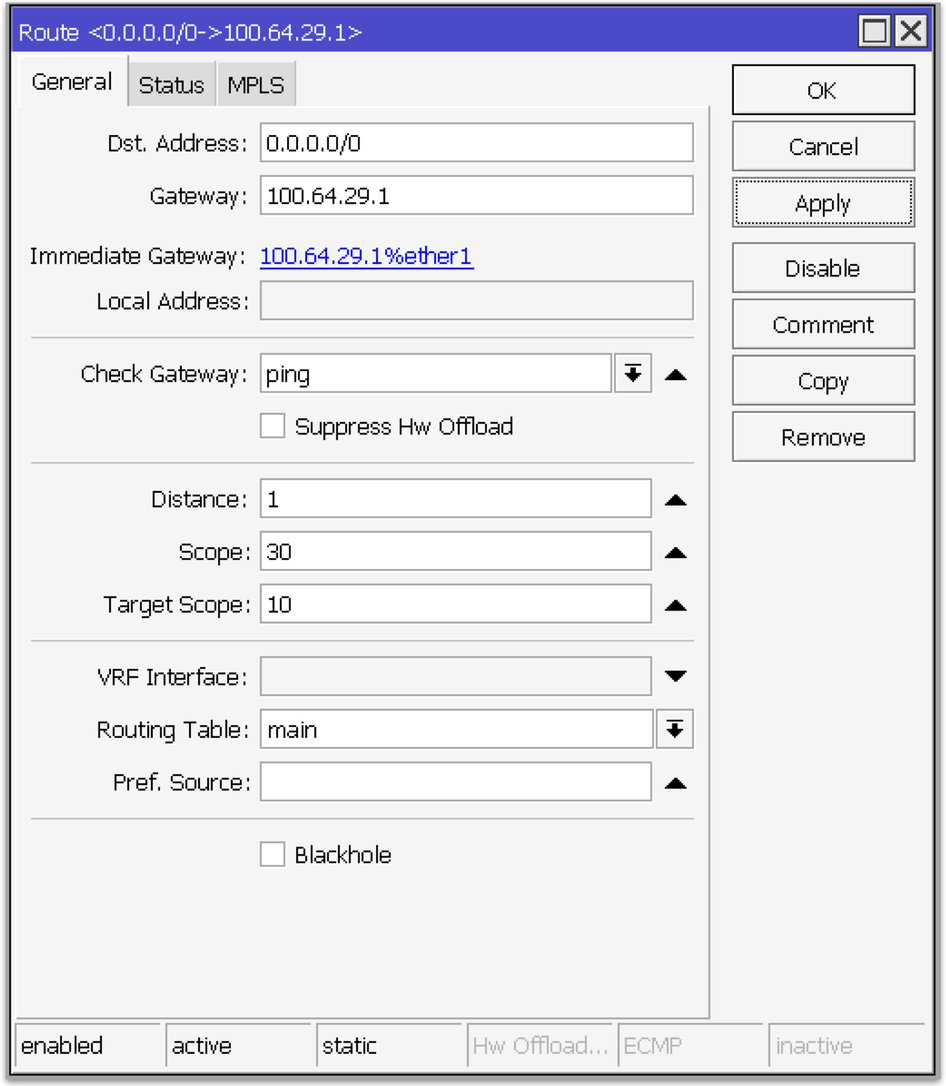
Dodanie odpowiednich reguł w tablice Firewall/NAT

check-gateway

Mechanizm pozwala sprawdzenie dostępności bramy za pomocą protokołu ICMP lub ARR

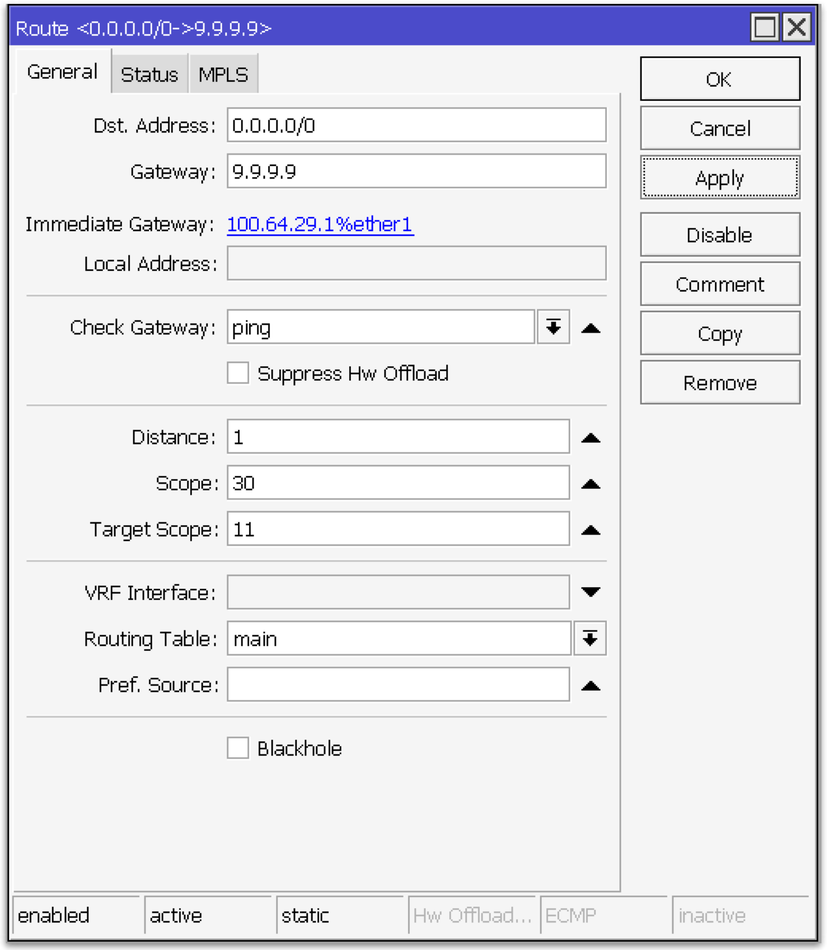
Przy ustawieniu ***check-gateway=ping*** router wysyła zapytania *Echo request* co 10 sekund i przy nie dostarczeniu dwóch odpowiedzi *Echo Reply* brama zostanie uznana za nieaktywną.

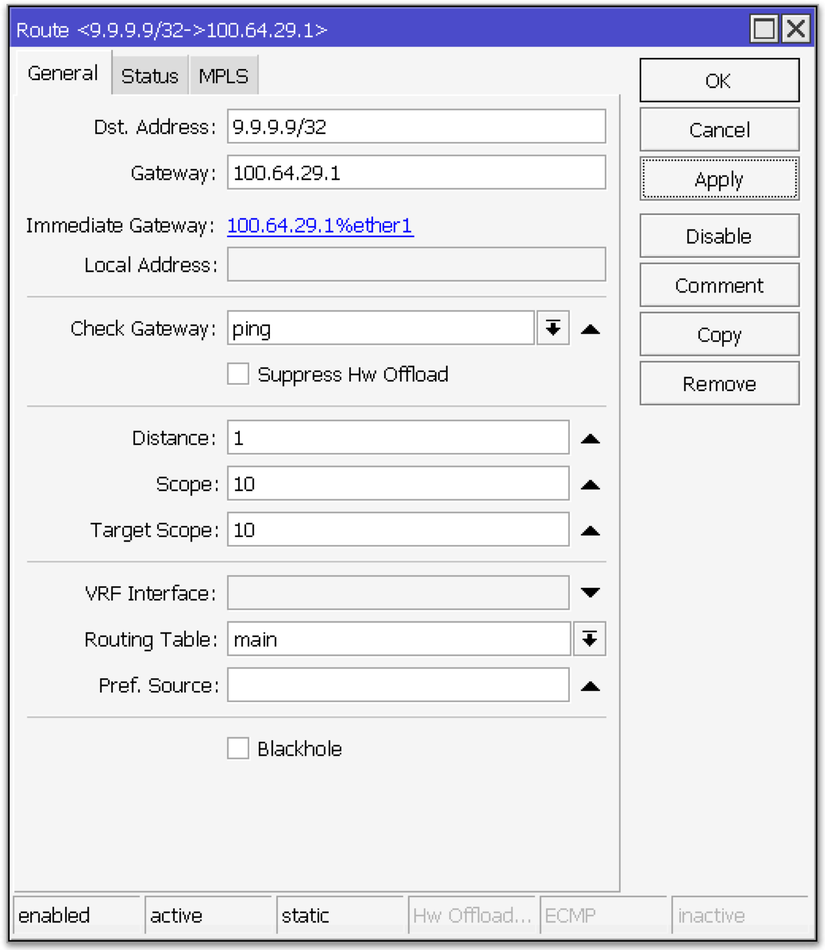
Ważne: w ROS 6, w przypadku uznania bramy za nieaktywną, wszystkie wpisy, które wskazują na ten sam adres bramy, też będą nieaktywne.
W ROS7 - nie.



Recursive routing

Rekursywny routing jest mechanizmem, który pozwala dostać się do bramy, która nie jest bezpośrednio podłączona do hosta.



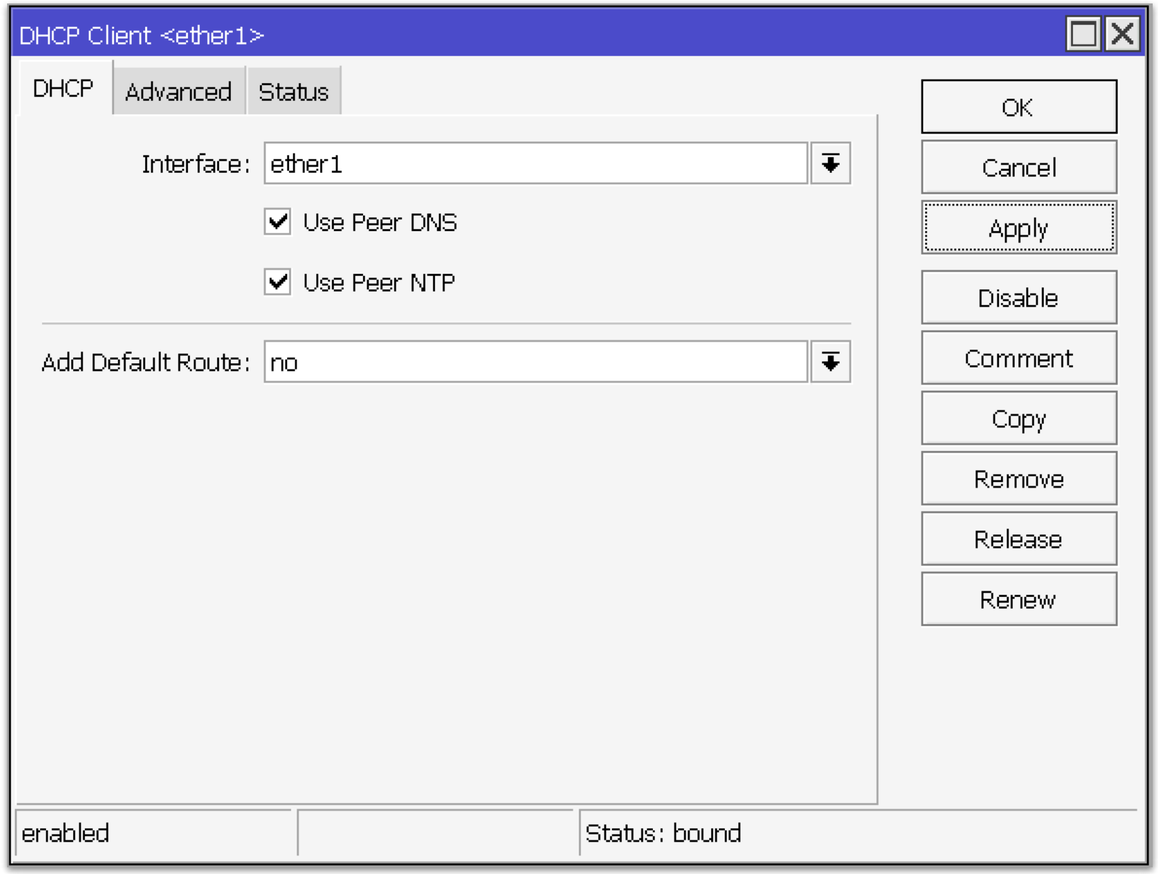


Recursive routing

IP adresy który używamy dla rekursywnego routingu najlepiej wybierać ze swoich VPS lub serwerów, ale też można spotkać użycie adres publicznych DNS serwerów, takich jak:

```
8.8.8.8  (Google DNS)
9.9.9.9  (Oracle DNS)
1.1.1.1  (Cloudflare DNS)
4.2.2.1  (Level3 DNS)
4.2.2.2  (Level3 DNS)
4.2.2.3  (Level3 DNS)
4.2.2.4  (Level3 DNS)
```

DHCP client



Dodajemy DHCP klient bez dodawania wpisu trasy domyślnej!!!

Wpis trasy domyślnej powstanie z wyniku działania skryptu, który jest podany w zakładce Advanced

Przy wykonaniu skryptu będą utworzone wpisy w firewall/nat oraz tablice routingu.

DHCP client script

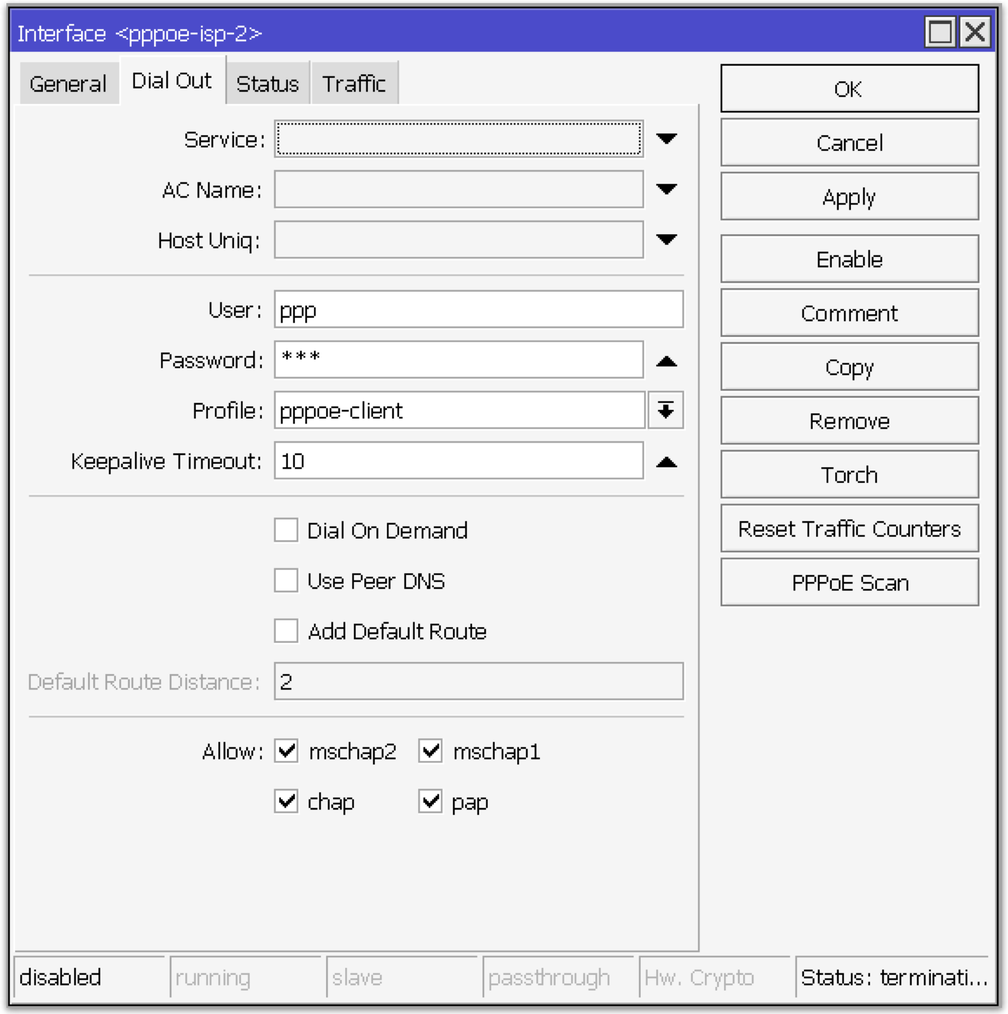
```
:if ($bound=1) do={
   /ip route remove [ find gateway="9.9.9.9" ]; /ip route remove \
[ find where dst-address ~"9.9.9.9" ]
   /ip route add check-gateway=ping comment="Recursive route via ISP-1" distance=1 \
dst-address=9.9.9.9/32 gateway=$"gateway-address" scope=10
   /ip route add check-gateway=ping comment="Route via ISP-1" distance=1 \
gateway=9.9.9.9 target-scope=11
   :if [:tobool ([/ip firewall/nat/ find comment="src-nat via ISP-1"])] do={
    /ip firewall nat set [find comment="src-nat via ISP-1"] action=src-nat chain=srcnat \
ipsec-policy=out,none out-interface=$"interface" to-addresses=$"lease-address"
    } else={ /ip firewall nat add action=src-nat chain=srcnat ipsec-policy=out,none \
out-interface=$"interface" to-addresses=$"lease-address" comment="src-nat via ISP-1" }
} else={
   /ip route remove [ find gateway="9.9.9.9" ]; /ip route remove [ find where \
dst-address ~"9.9.9.9" ]
   /ip firewall nat remove  [find comment="src-nat via ISP-1"]
   /routing/rule/remove [find comment="From ISP-1 IP to Inet"]
}
```

PPPoE client

W PPPoE kliencie odznaczamy checkbox “Add Default Route”

Wpis trasy domyślnej powstanie z wyniku działania skryptu, który jest podany w profilu pod nazwą “pppoe-client”

Przy wykonaniu skryptu będą utworzone wpisy w firewall/nat oraz tablice routingu.



PPP profile

On up

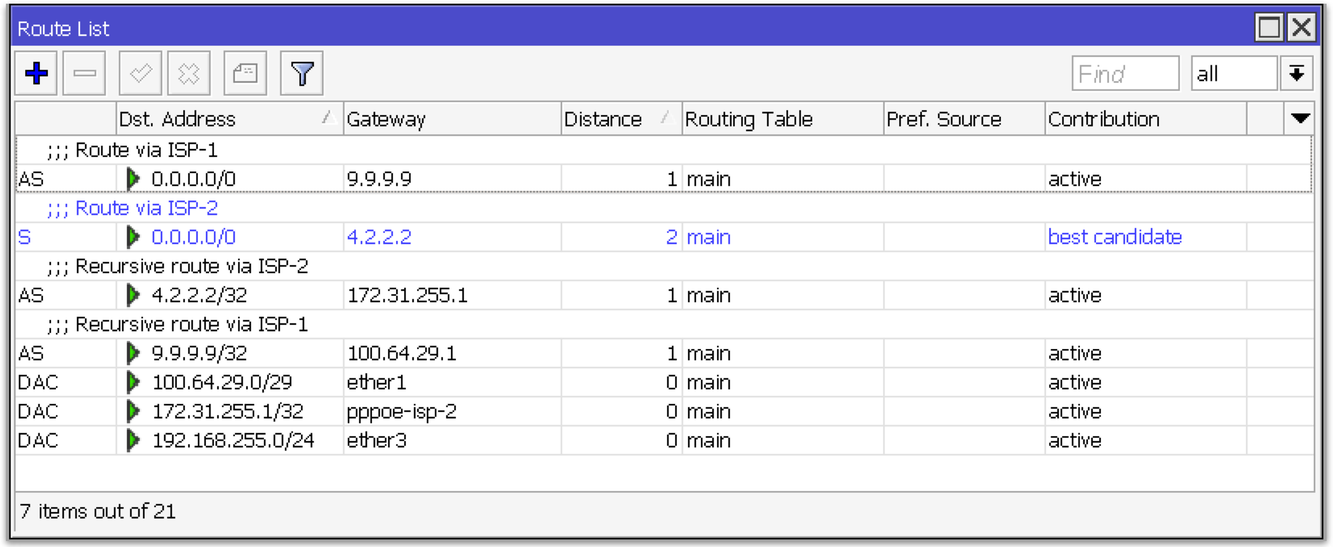
```
/ip route remove [find gateway="4.2.2.2"];
/ip route remove [find where dst-address ~"4.2.2.2"]

/ip route add check-gateway=ping comment="Recursive route via ISP-2" distance=1 \
dst-address=4.2.2.2/32 gateway=$"remote-address" scope=10
/ip route add check-gateway=ping comment="Route via ISP-2" distance=3 \
gateway=4.2.2.2 target-scope=11
   :if [:tobool ([/ip firewall/nat/ find comment="src-nat via ISP-2"])] do={
     /ip firewall nat set [find comment="src-nat via ISP-2"] action=src-nat chain=srcnat \
      ipsec-policy=out,none out-interface=$interface to-addresses=$"local-address";
    } else={/ip firewall nat add action=src-nat chain=srcnat ipsec-policy=out,none \
out-interface=$interface to-addresses=$"local-address" comment="src-nat via ISP-2" ; }
```

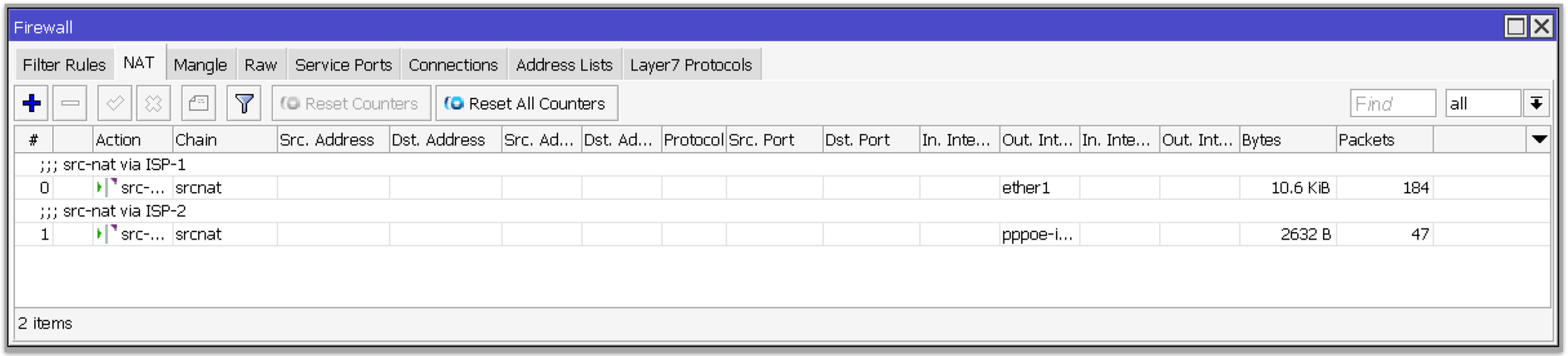
On down

```
/ip route remove [find gateway="4.2.2.2"]
/ip route remove [find where dst-address ~”4.2.2.2"]
/ip firewall nat remove  [find comment="src-nat via ISP-2"]
```

Wynik działania



Tablica routingu oraz Firewall/NAT wypełniona za pomocą skryptów, z zastosowaniem rekursywnego routingu oraz sprawdzania dostępności bramy.



Active-Active

Zadania

Oznakowanie wchodzącego ruchu od każdego z operatorów

Oznakowanie ruchu wychodzącego z routera

Oznakowanie routingu

Dodanie zapasowych tras, w przypadku awarii jednego z operatorów

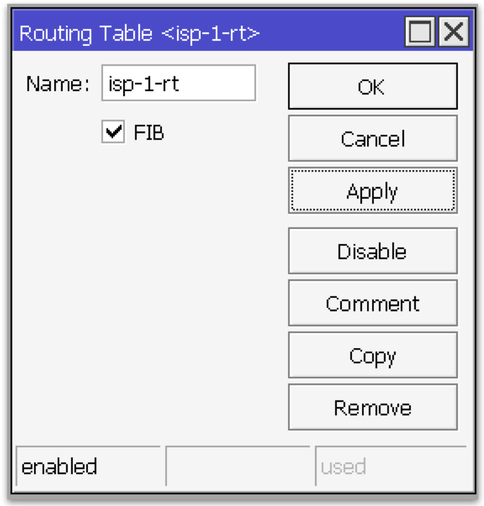
Dodanie list interfejsów

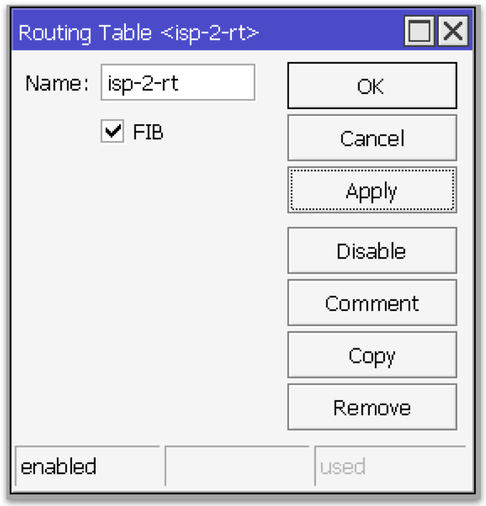
Dodajemy listy interfejsów oraz dodajemy interfejsy do odpowiednich list

```
/interface list add name=WAN
/interface list add name=LAN
```

```
/interface/list/member/add list=WAN interface=ether1
/interface/list/member/add list=WAN interface=pppoe-isp-2
/interface/list/member/add list=LAN interface=ether3
```

Dodanie tablic routingu






```
/routing table add disabled=no fib name=isp-1-rt
/routing table add disabled=no fib name=isp-2-rt
```

W ROS7 mechanizm route-mark działa w taki sposób jak i w systemie operacyjnym linux *iproute2*, czyli jest konieczność dodania najpierw tablic routingu a potem wykorzystanie ich w odpowiednich regułach Firewall/Mangle

Oznakowanie połączeń od ISP

```
/ip firewall mangle add action=mark-connection chain=prerouting \
comment="Mark connections from ISP1" connection-mark=no-mark \
in-interface=ether1 new-connection-mark=isp-1-conn passthrough=no

/ip firewall mangle add action=mark-connection chain=prerouting \
comment="Mark connections from ISP2" connection-mark=no-mark \
in-interface=pppoe-isp-2 new-connection-mark=isp-2-conn passthrough=no
```

Za pomocą danych reguł markujemy wszystkie połączenia przychodzące od operatorów.

Oznakowanie ruchu na forward

```
/ip firewall mangle add action=mark-routing chain=prerouting \
comment="Mark route on forward via ISP1" connection-mark=isp-1-conn \
dst-address-type=!local in-interface-list=!WAN \
new-routing-mark=isp-1-rt passthrough=no

/ip firewall mangle add action=mark-routing chain=prerouting \
comment="Mark route on forward via ISP2" connection-mark=isp-2-conn \
dst-address-type=!local in-interface-list=!WAN \
new-routing-mark=isp-2-rt passthrough=no
```

W tym miejscu oznakujemy ruch dotyczący łańcucha *forward*, oraz który nie dotyczy lokalnego ruchu i nie przychodzi z zewnątrz.

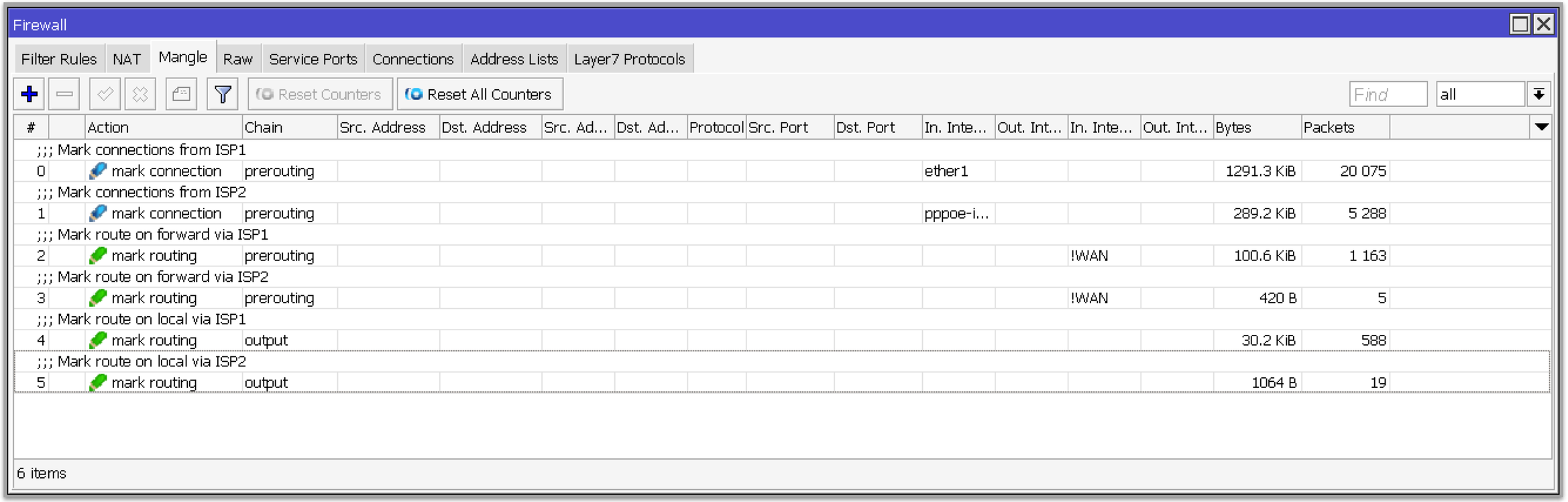
Oznakowanie ruchu na output

```
/ip firewall mangle add action=mark-routing chain=output \
comment="Mark route on local via ISP1" connection-mark=isp-1-conn \
dst-address-type=!local new-routing-mark=isp-1-rt passthrough=no

/ip firewall mangle add action=mark-routing chain=output \
comment="Mark route on local via ISP2" connection-mark=isp-2-conn \
dst-address-type=!local new-routing-mark=isp-2-rt passthrough=no
```

Oznakowanie ruchu wychodzącego z routera na łańcuchu output, który powinien wychodzić poprzez właściwego operatora

Wszystkie wpisy z Firewall/Mangle

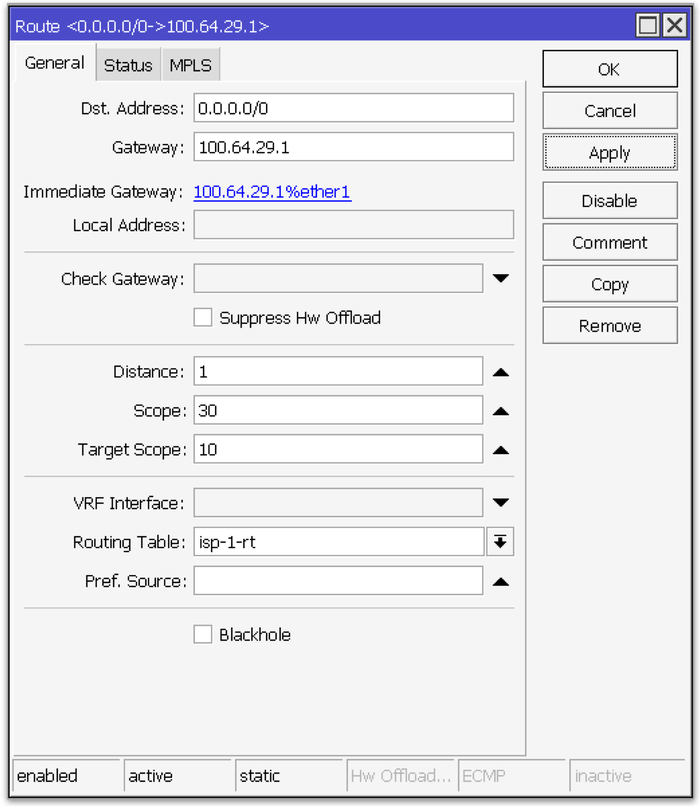


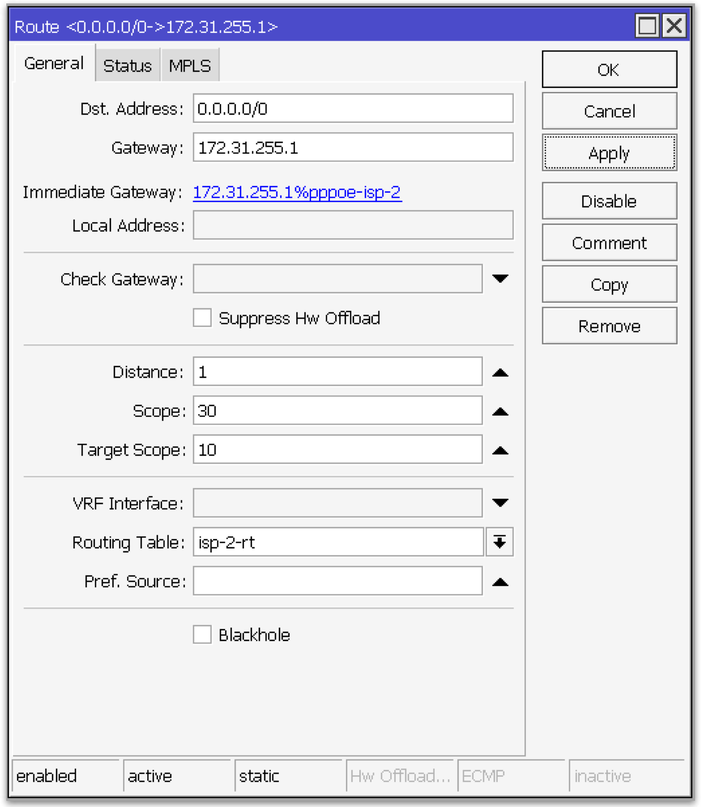
#	Action	Chain	Src. Address	Dst. Address	Src. Ad...	Dst. Ad...	Protocol	Src. Port	Dst. Port	In. Inte...	Out. Int...	In. Inte...	Out. Int...	Bytes	Packets
;;; Mark connections from ISP1															
0	mark connection	prerouting								ether1				1291.3 KiB	20 075
;;; Mark connections from ISP2															
1	mark connection	prerouting								pppoe-i...				289.2 KiB	5 288
;;; Mark route on forward via ISP1															
2	mark routing	prerouting										!WAN		100.6 KiB	1 163
;;; Mark route on forward via ISP2															
3	mark routing	prerouting										!WAN		420 B	5
;;; Mark route on local via ISP1															
4	mark routing	output												30.2 KiB	588
;;; Mark route on local via ISP2															
5	mark routing	output												1064 B	19

Minimalny zestaw reguł z tablicy firewall/mangle, który może być dopełniony dodatkowymi regułami

Dodanie wpisów w tablicach routingu

Dodanie domyślnych tras w odpowiednich tablicach routingu, co pozwoli wysyłanie ruchu poprzez poprawnego operatora.





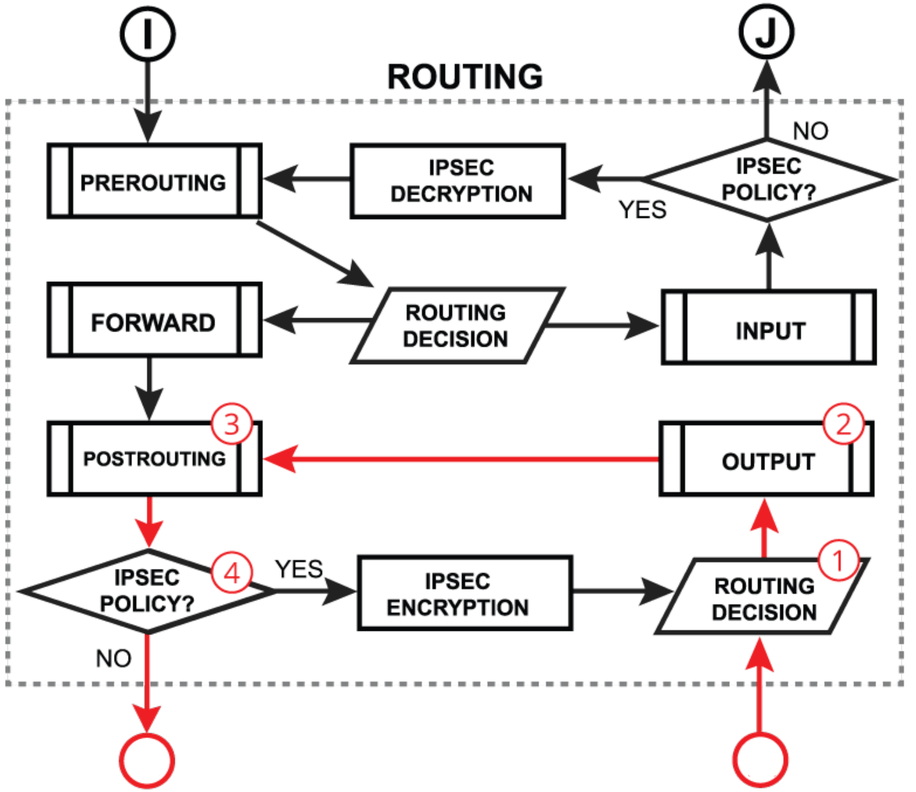

```
/ip/route/add gateway=100.64.29.1 routing-table=isp-1-rt
/ip/route/add gateway=172.31.255.1 routing-table=isp-2-rt
```

“Awaryjna” trasa

```
/interface bridge add name=lo-em comment="Emergency loopback"
/ip route add distance=254 gateway=lo-em comment="Emergency route"
```

Dany wpis pozwala przejść do decyzji Route decision od lokalnych procesów niezależnie od stanu połączenia z dowolnym z ISP.

Szczegół wychodzącego lokalnego ruchu polega na tym, że pakiet, dla opuszczenia routera powinien przejść Route Decision, a bez aktywnej domyślnej trasy on zostanie odrzucony.



Połączenie dwóch metod

Route List

Find | all

	Dst. Address	Gateway	Distance	Routing Table	Pref. Source	Contribution
	;;; Route via ISP-1					
AS	0.0.0.0/0	9.9.9.9	1	main		active
AS	0.0.0.0/0	100.64.29.1	1	isp-1-rt		active
AS	0.0.0.0/0	172.31.255.1	1	isp-2-rt		active
	;;; Route via ISP-2					
S	0.0.0.0/0	4.2.2.2	2	main		best candidate
	;;; Emergency route					
S	0.0.0.0/0	lo-em	254	main		best candidate
	;;; Recursive route via ISP-2					
AS	4.2.2.2/32	172.31.255.1	1	main		active
	;;; Recursive route via ISP-1					
AS	9.9.9.9/32	100.64.29.1	1	main		active
DAC	100.64.29.0/29	ether1	0	main		active
DAC	172.31.255.1/32	pppoe-isp-2	0	main		active
DAC	192.168.255.0/24	ether3	0	main		active

10 items out of 24

Dziękuję

e-mail: *ihor@hreskiv.pl*

Szkolenia: *https://mwtc.pl*

Artykuły: *https://mikrotikacademy.pl*