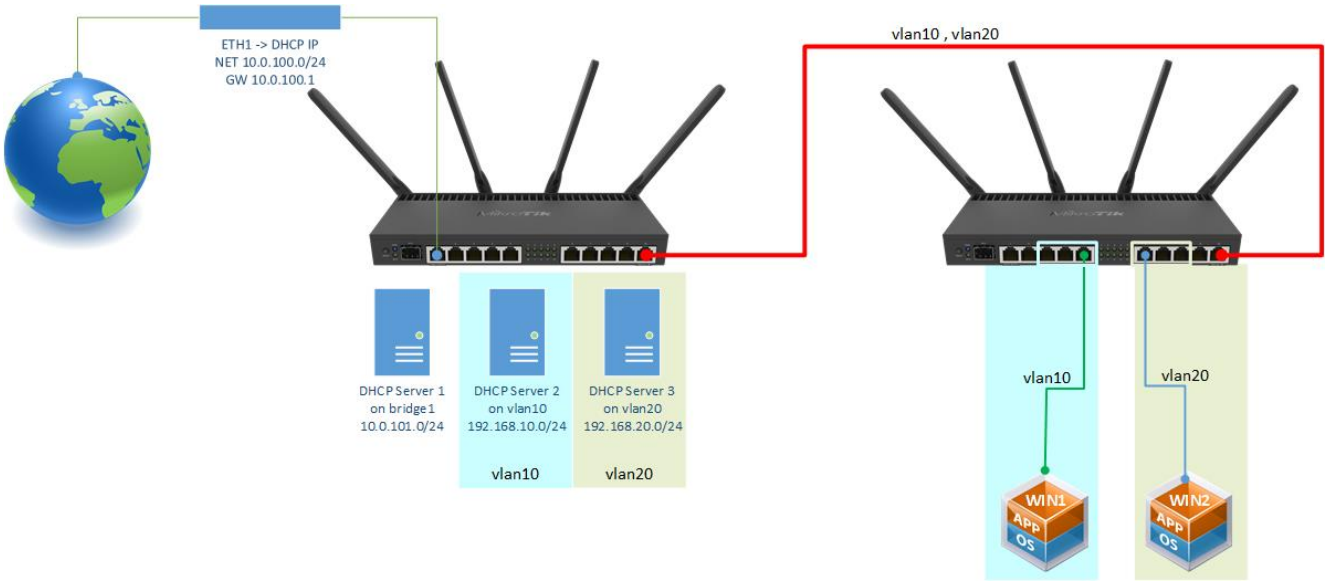
Mikrotik 7

written by archi | 3 grudnia 2022

Mikrotik – wykorzystanie technologii VLAN bez switch chip

Celem laboratorium jest wykonanie podziału sieci komputerowej (fizycznej) na odrębne podsieci z separacją ruchu pomiędzy nimi. Wykorzystamy funkcjonalność 802.11Q (VLAN), które gwarantują możliwości komunikacji pomiędzy elementami sieci z jednoczesną separacją ruchu. Technologia VLAN pozwala na przekazywanie pakietów pomiędzy odbiorcami z wykorzystaniem przełączników sieciowych na portach klasy untagged (access port'y). Komunikacja pomiędzy przełącznikami (głównie na łączach uplink) odbywa się na portach tagged (trunk). VLAN często wykorzystywane są do zmniejszenia ruchu klasy broadcast w segmentach sieci.

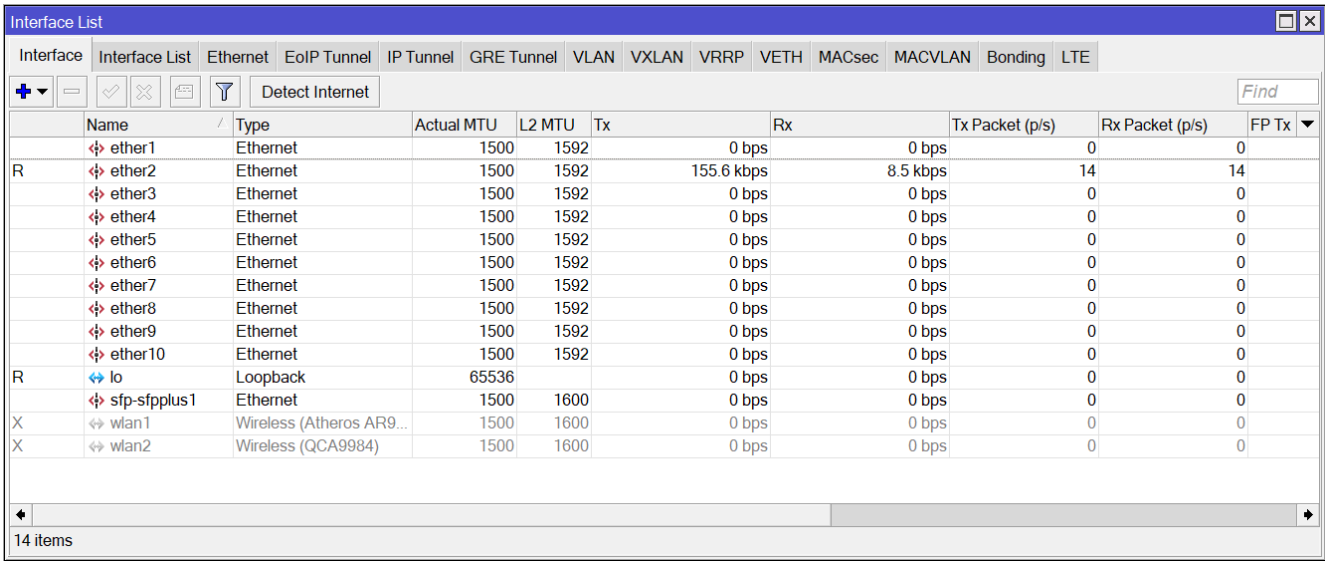


---

1. Połącz z krosownicy (Karta-port1) do twojego switcha prywatnego.

2. Połącz port switcha do routera R1 na port ETHER2.

3. Przejdź do okna Interface



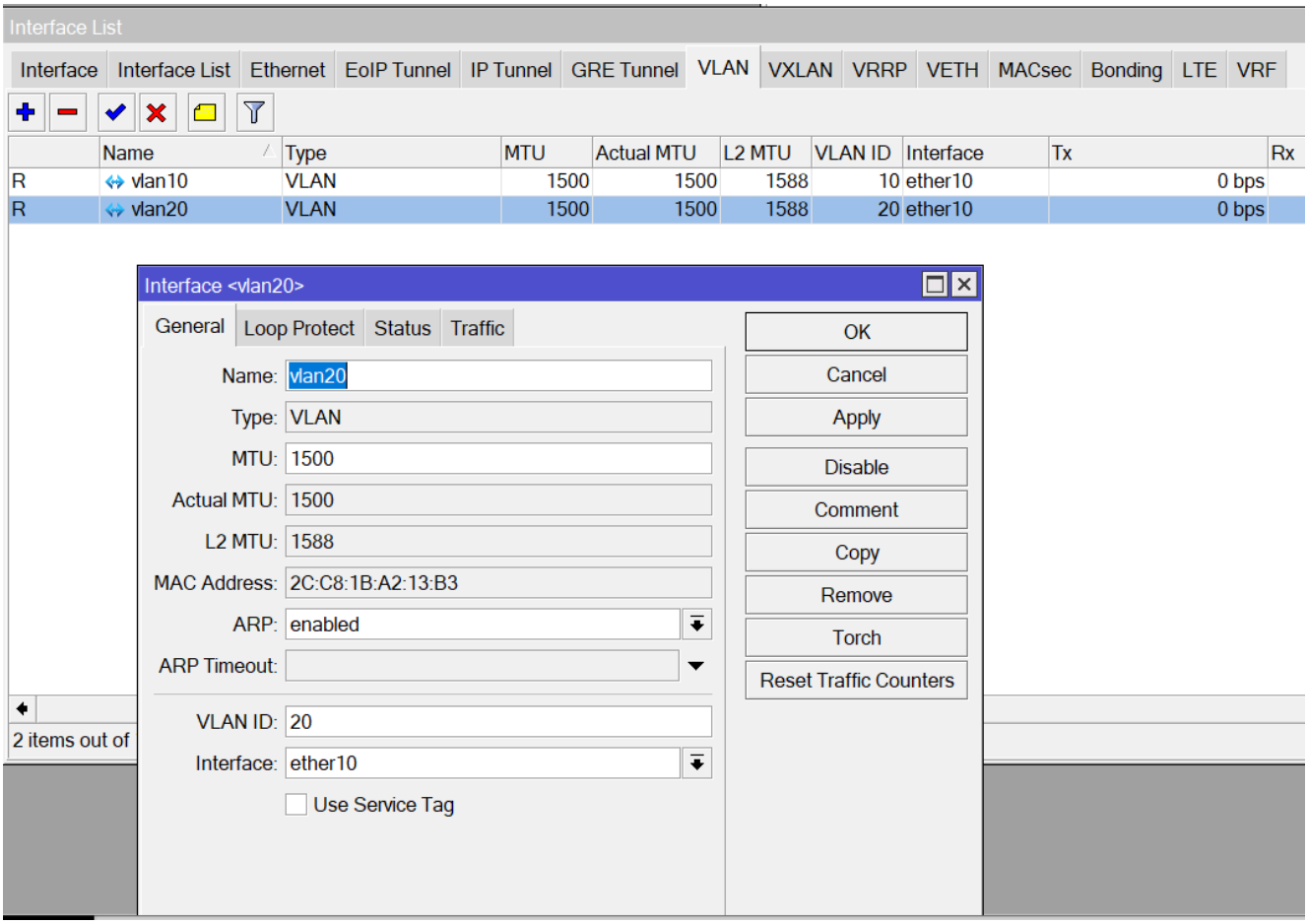
4. W zakładce VLAN:

– utwórz vlan o nazwie VLAN10 z identyfikatorem „vlan ID” ustawionym na 10

– utwórz vlan o nazwie VLAN20 z identyfikatorem „vlan ID” ustawionym na 20

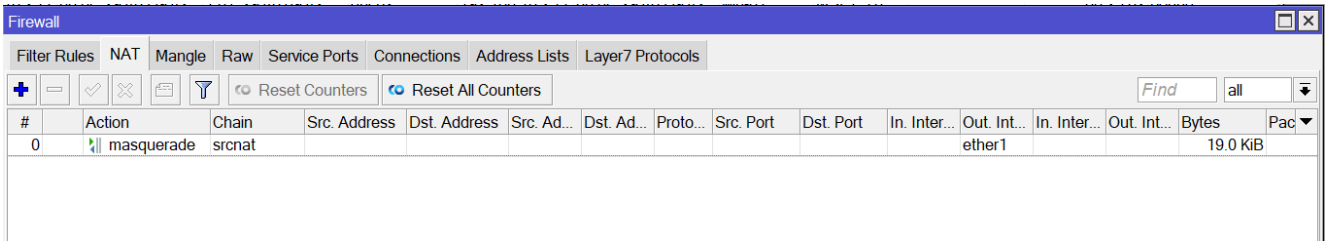
– przypnij oba vlan’y do interfejsu ETHER10.

Zobacz przykład dla VLAN20 poniżej.

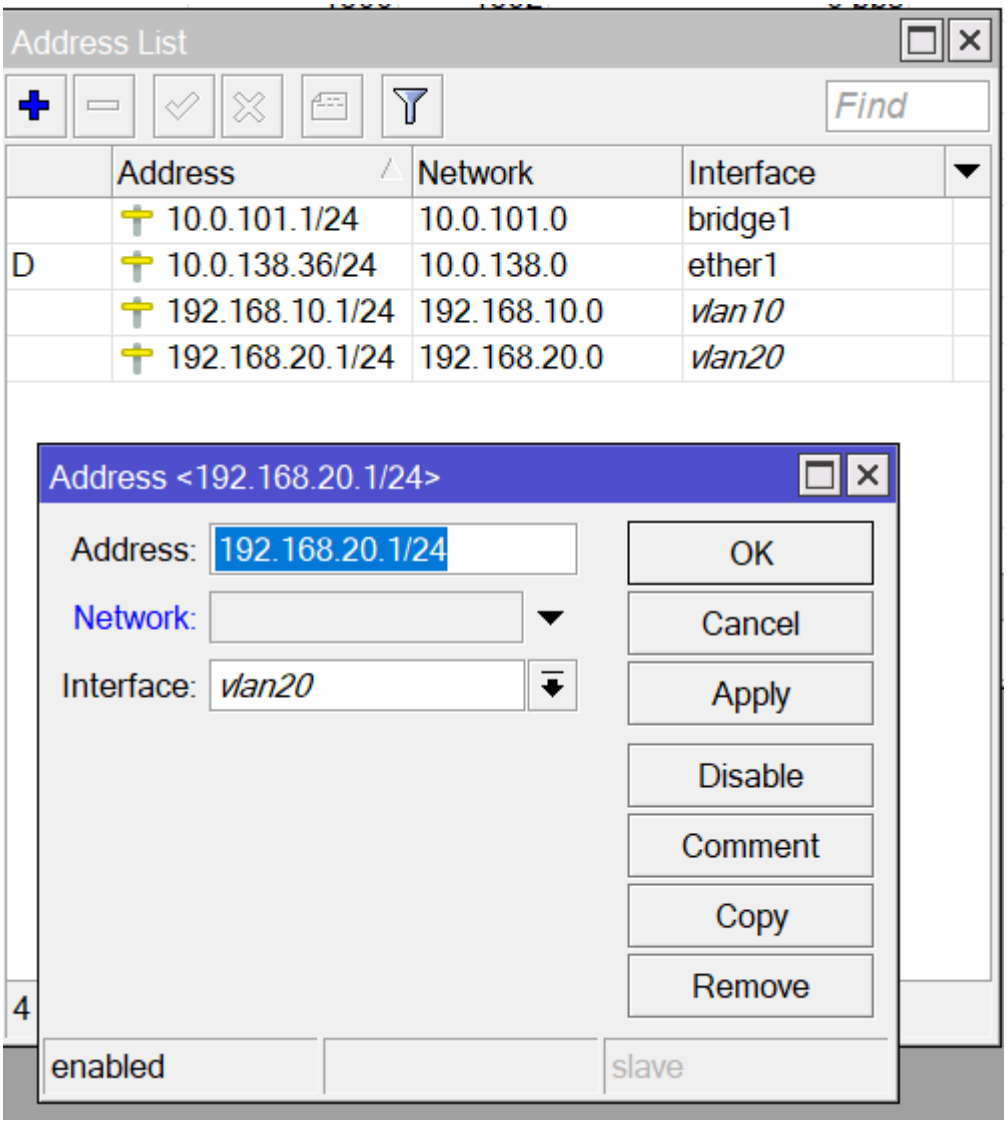


5. Utwórz bridge o nazwie „bridge1”.

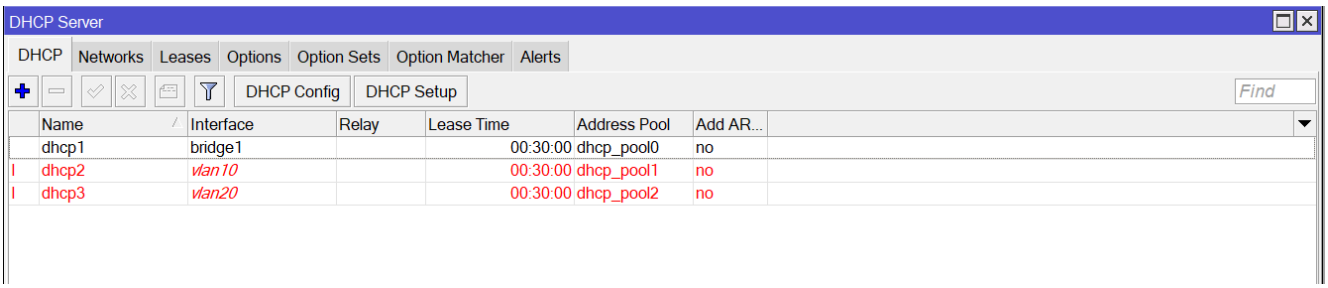
6. Utwórz dhcp-client na porcie Ether1 i podłącz router R1 do Internetu (48-portowy switch) oraz utwórz regułę w firewall dla maskowania adresów IP.



7. Nadaj adresy IP dla nowych interfejsów vlan10, vlan20 oraz bridge1 odpowiednio dla vlan10 adres 192.168.10.1/24, dla vlan20 adres 192.168.20.1/24, dla bridge1 adres 10.0.101.1/24. Przykład poniżej dla vlan20.



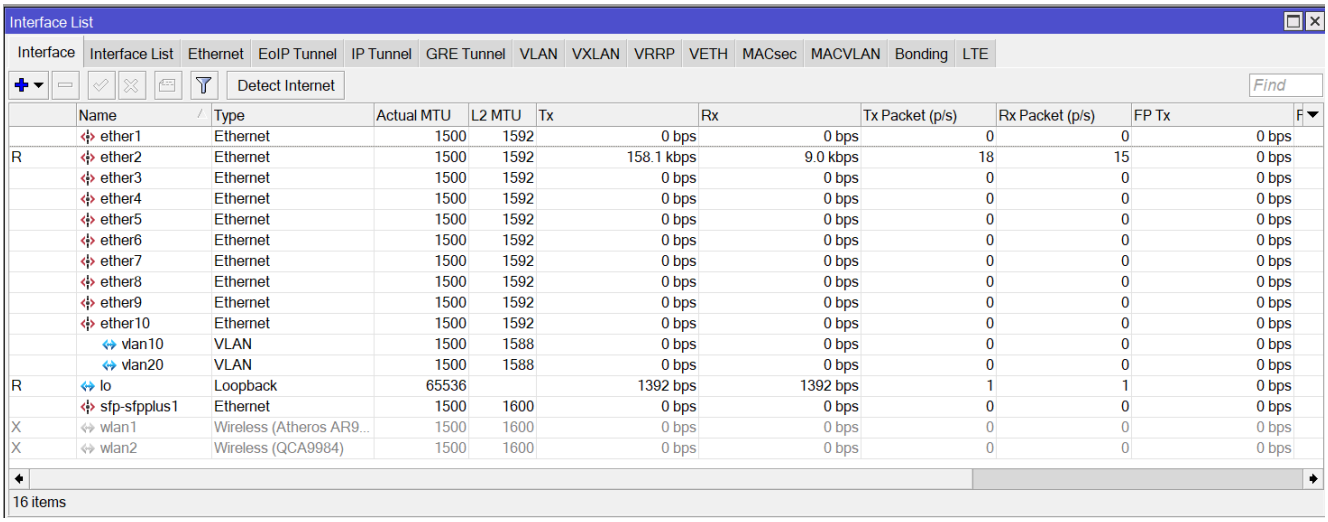
8. Ustaw serwery DHCP dla interfejsów bridge1, vlan10, vlan20. Użyj „DHCP Setup” dla odpowiedniego interfejsu i pozostaw wszystkie parametry na proponowanych wartościach. Pamiętaj o nadaniu adresu DNS w opjach serwera DHCP np. na 8.8.8.8



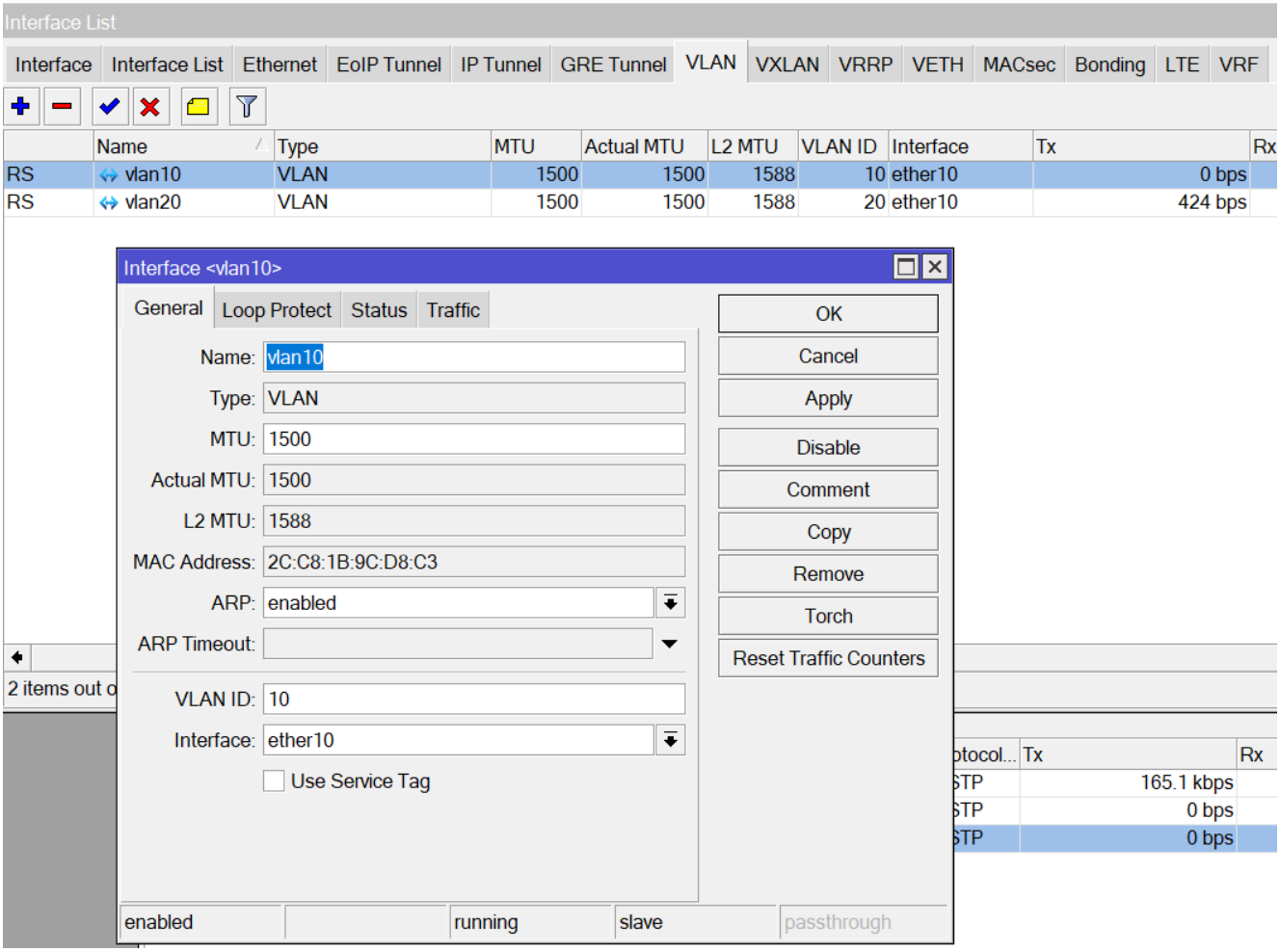
---

9. Połącz się do routera R2 kolejnym portem switcha na port ETHER2 routera. Będziemy teraz konfigurować R2.

10. Otwórz interfejsy i przejdź do zakładki VLAN

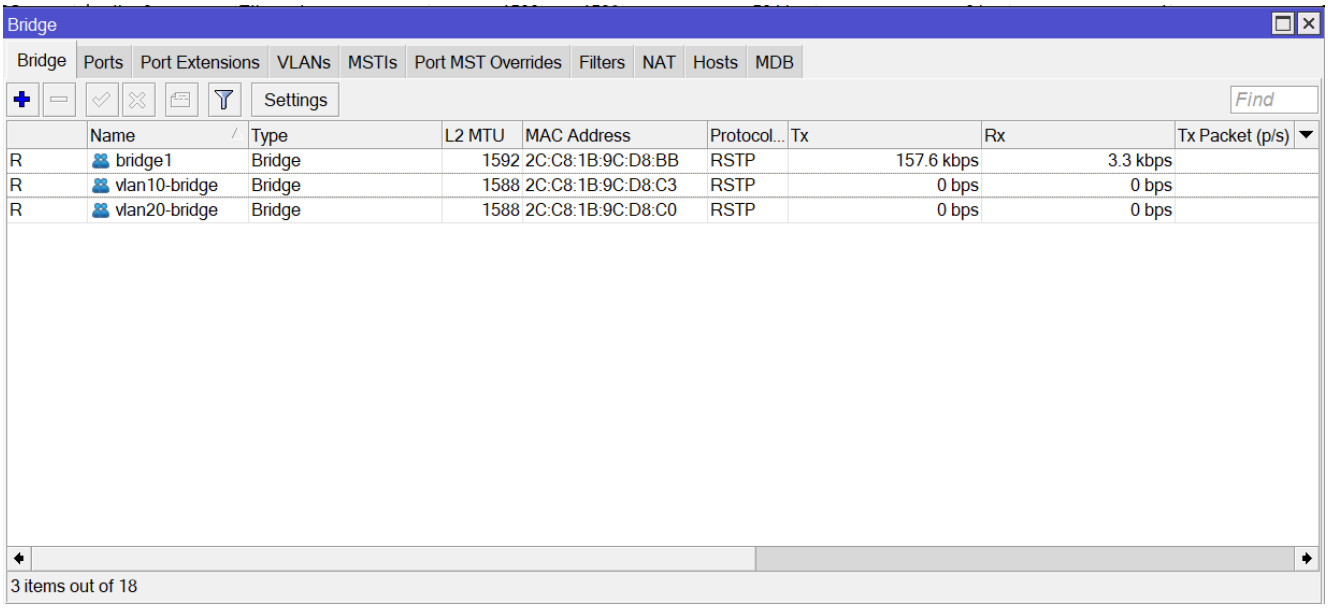


11. Podobnie jak dla routera R1 ustaw vlan10 i vlan20 przypisane do interfejsu Ether10.



12. W ramach definicji Bridge dodaj dwa nowe switch mostki o nazwach bridge1, vlan10-bridge, vlan20-bridge. Będą one służyć za porty urządzenia

switch, do którego będzie można podłączyć komputery w trybie „untagged” lub w terminologii Cisco „Access Port”.



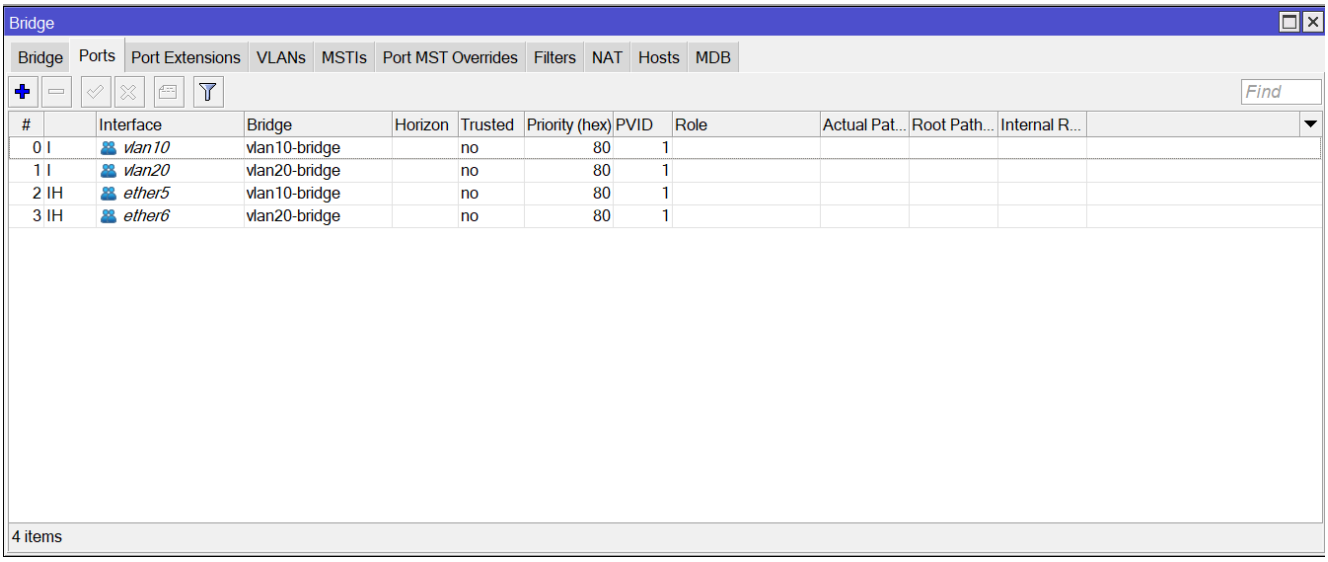
13. Dodaj i zmień odpowiednie porty do definicji bridge:

– przypisz interface vlan10 do bridge vlan10-bridge,

– przypisz interface vlan20 do bridge vlan20-bridge,

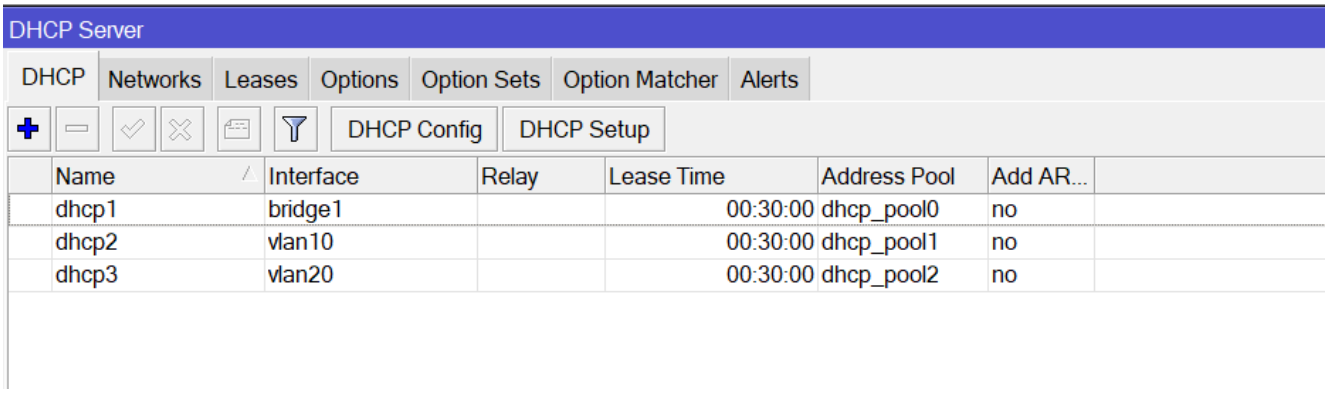
– przypisz interface ether5 do bridge vlan10-bridge,

– przypisz interface ether6 do bridge vlan20-bridge.



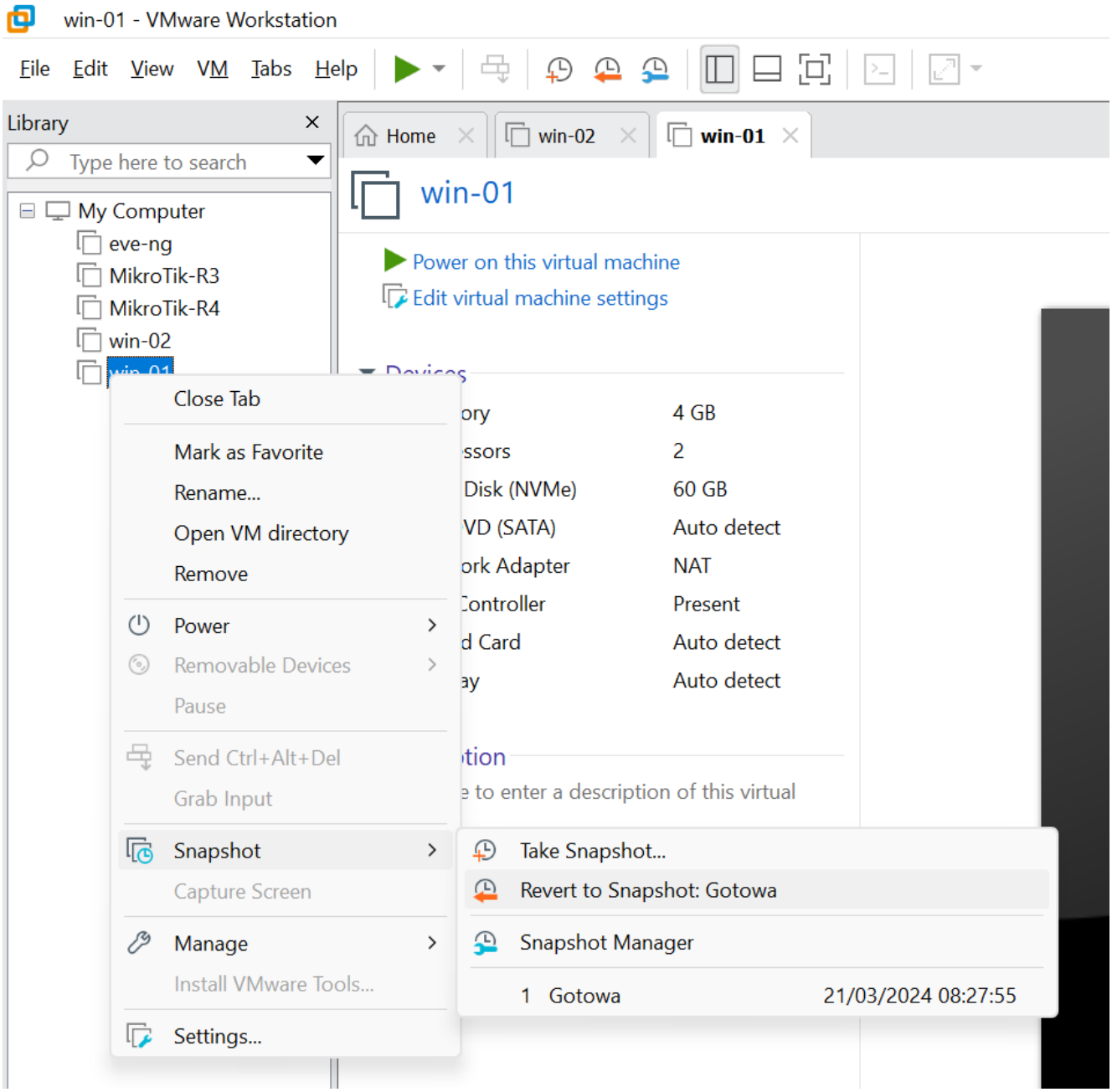
15. **Połącz port Ether10 Mikrotika R1 z portem Ether10 Mikrotika R2** (*przy pomocy krótkiego przewodu RJ45 – zielony 0,5m*)

16. Sprawdź na routerze R1, czy zmienił się kolor (czerwony na czarny) serwerów dhcp2 i dhcp3.



---

17. Uruchom VMware Workstation i wykonaj REVERT do stanu „Gotowa” na obu maszynach (Win1 i Win2).



18. Przypisz maszyna wirtualną interfejsy sieciowe:

– maszynie wirtualnej win-01 interfejs Karta-Port2,

– maszynie wirtualnej win-02 interfejs Karta-Port3.

18a. Połącz w Mikrotiku R2:

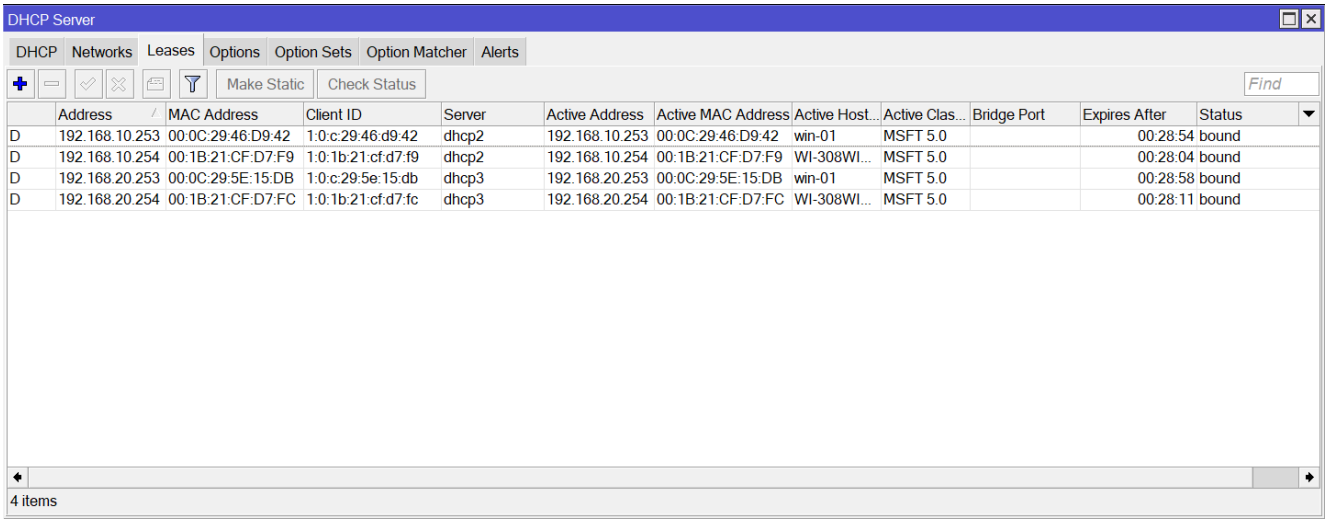
– port ether5 do Karta-Port2,

– port ether6 do Karta-Port3.

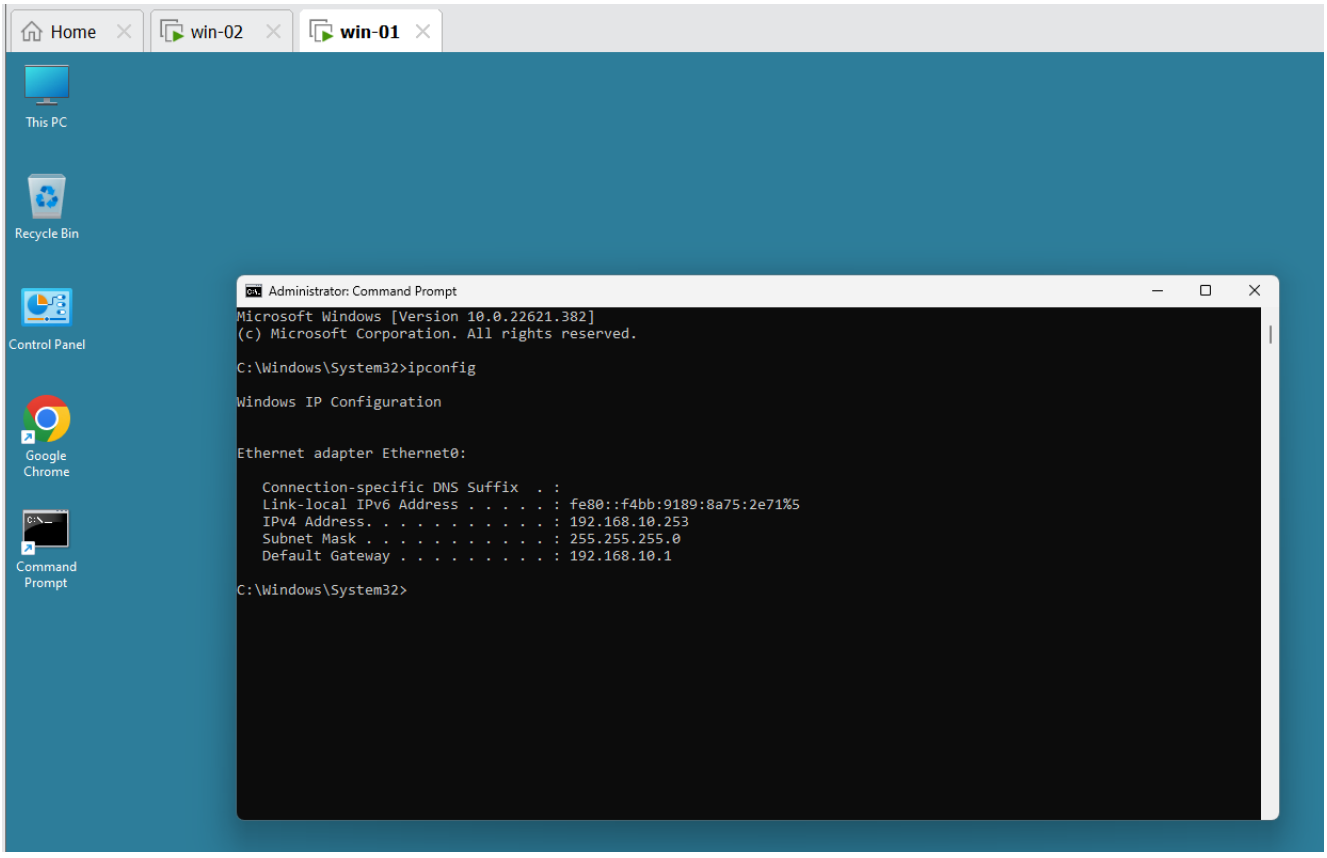
18b. Włącz maszyny wirtualne Win1 i Win2.

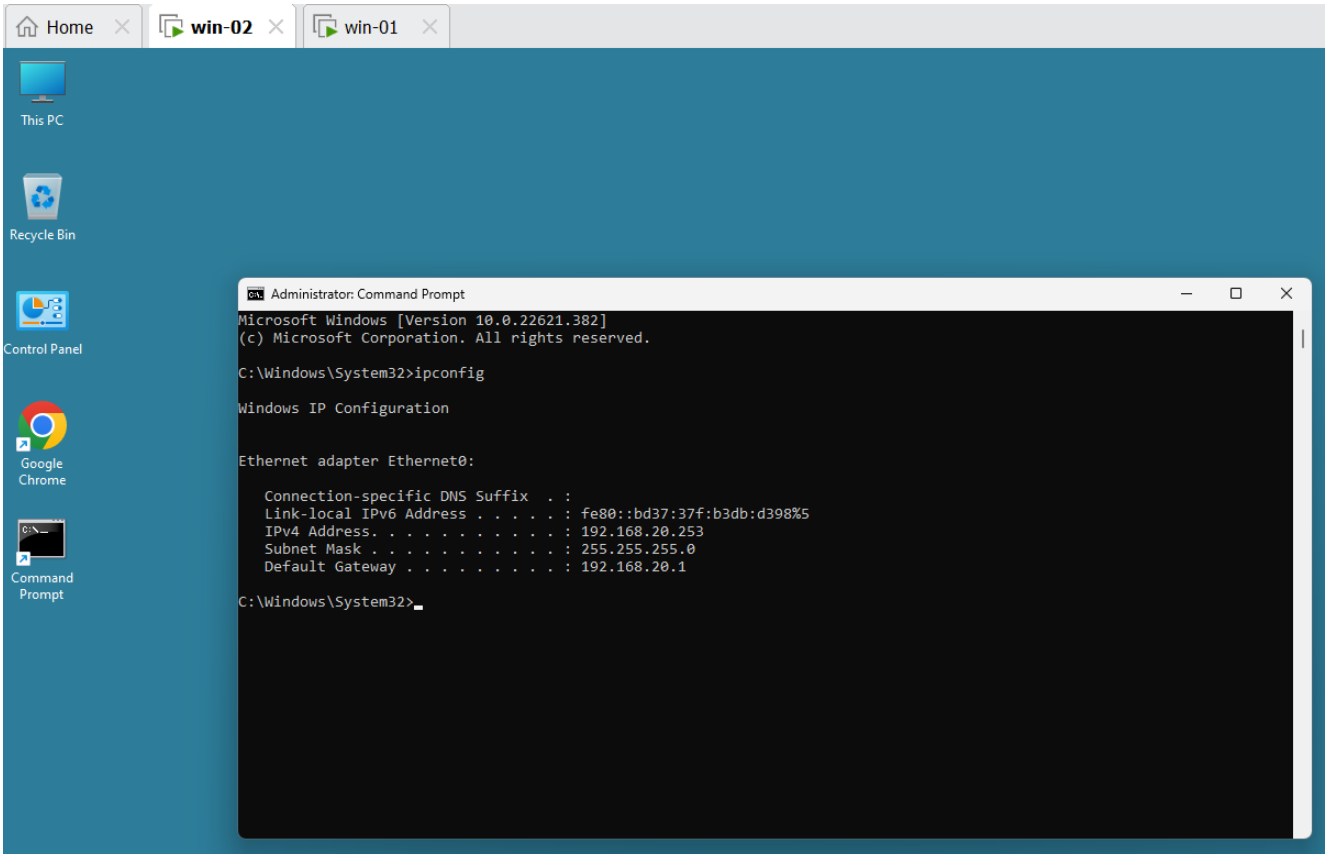
19. Maszyny wirtualne powinny otrzymać od routera R1 adresy IP w swoich

klasach IP zgodnie z podłączonymi vlan. Maszyna Win1 powinna dostać adres IP z klasy 192.168.10.0/24, a maszyna Win2 z klasy 192.168.20.0/24.



20. Sprawdź na każdej z maszyn czy ma właściwą konfigurację IP.





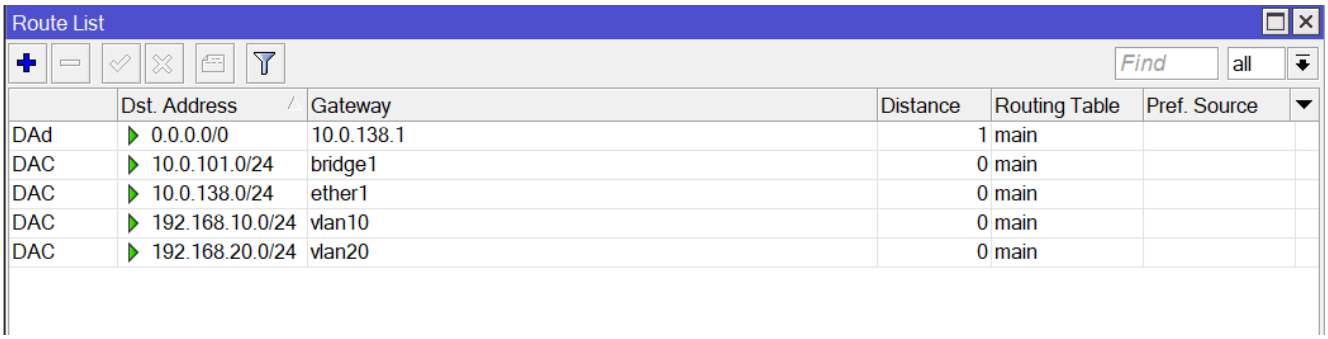
21. Wykonaj komendę ping z każdej z maszyn do adresu 8.8.8.8 a następnie do np. onet.pl. Jeśli adresy są osiągalne to konfiguracja jest poprawna.

```
C:\Windows\System32>ping onet.pl

Pinging onet.pl [65.9.95.42] with 32 bytes of data:
Reply from 65.9.95.42: bytes=32 time=11ms TTL=239
Reply from 65.9.95.42: bytes=32 time=11ms TTL=239
Reply from 65.9.95.42: bytes=32 time=11ms TTL=239
Reply from 65.9.95.42: bytes=32 time=11ms TTL=239

Ping statistics for 65.9.95.42:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 11ms, Average = 11ms

C:\Windows\System32>
```

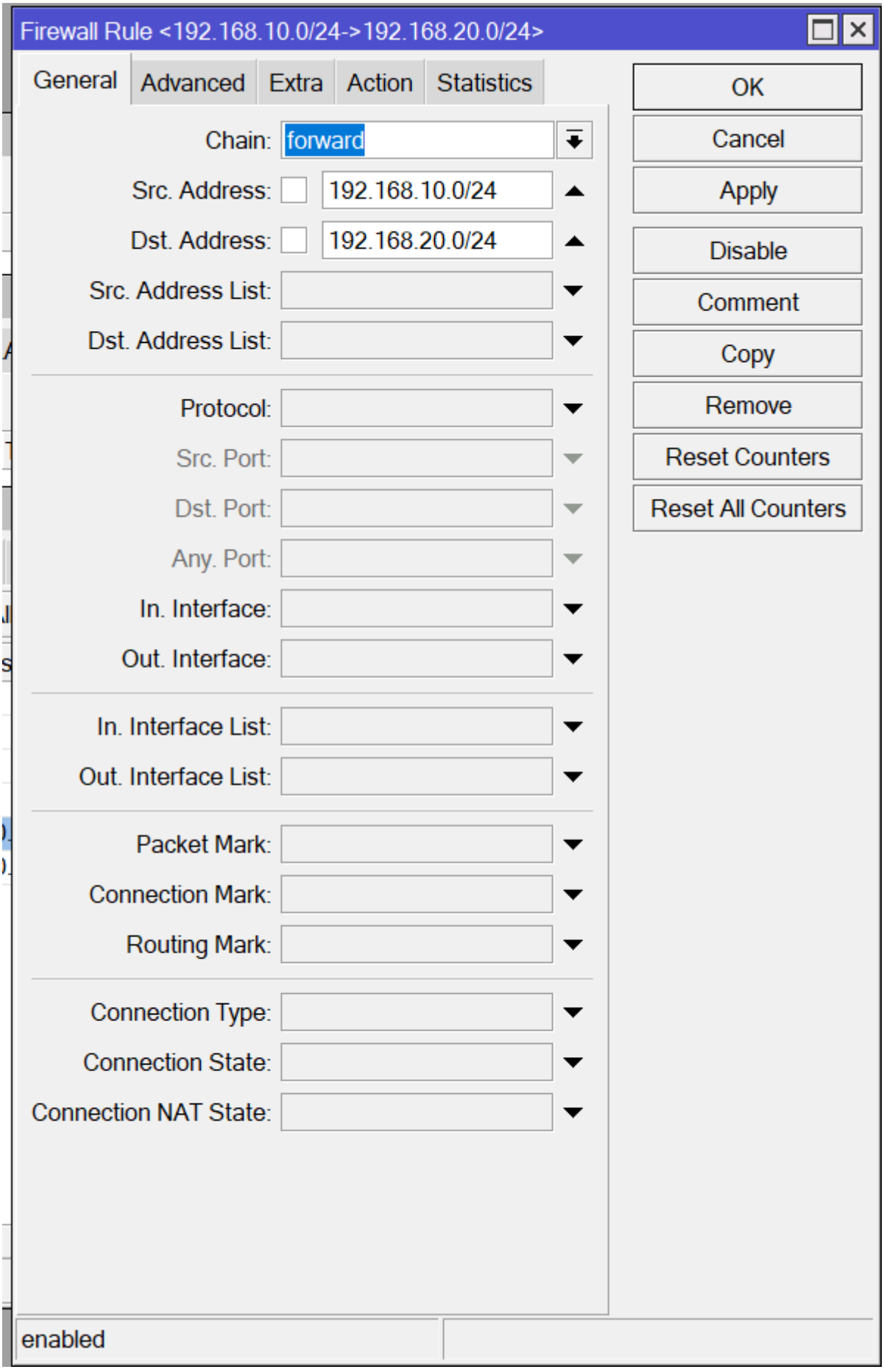
22. W obydwu maszynach wirtualnych wyłącz zaporę sieciową „Windows Defender Firewall with Advanced Security” i sprawdź czy maszyny win-01 i win-02 mogą się pingować nawzajem.

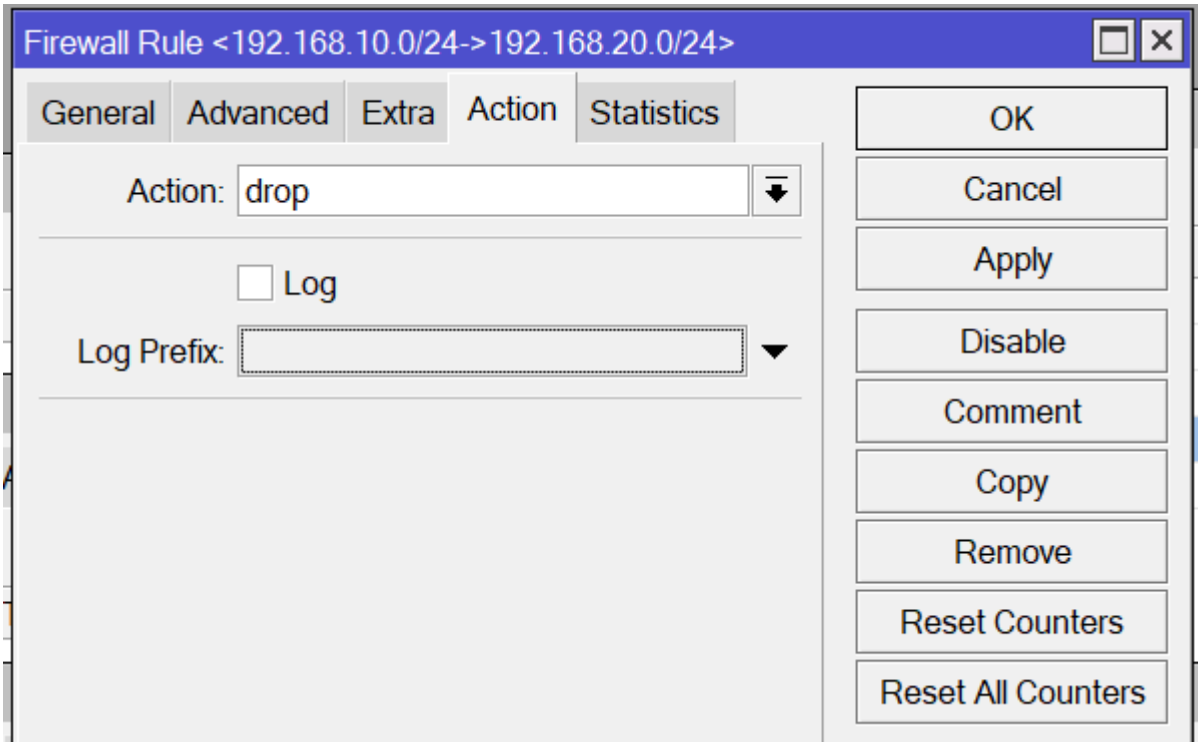
23. Czy maszyny win-01 i win-02 powinny móc komunikować się ze sobą? Maszyny znajdują się w 2 różnych VLAN-ach, więc nie powinny się

komunikować (tak domyślnie działają VLAN-y na switchach, natomiast my korzystamy z routerów). Domyślnie Mikrotik R1 dodał routing do obu podsieci podczas definiowania adresów IP.

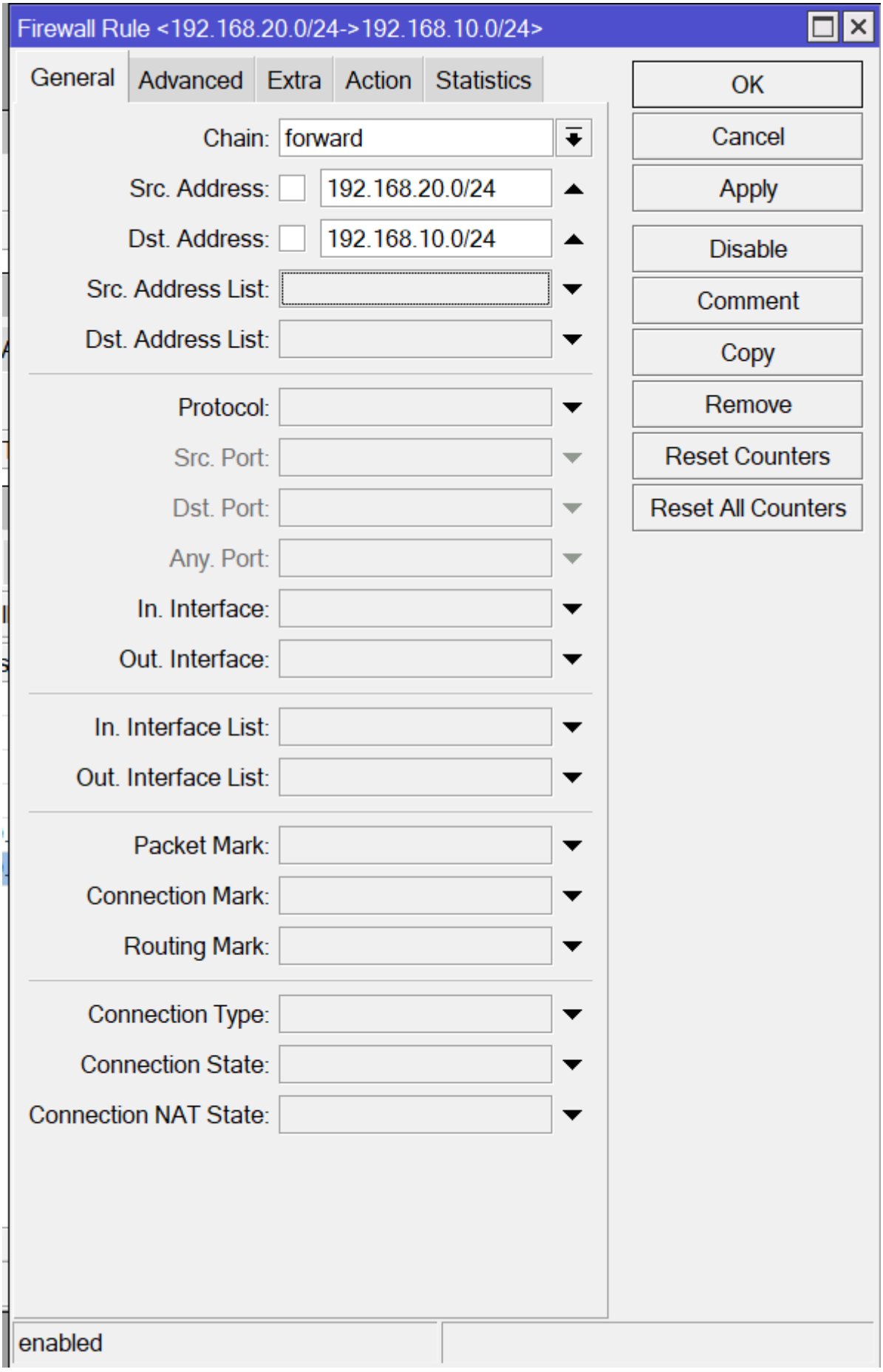


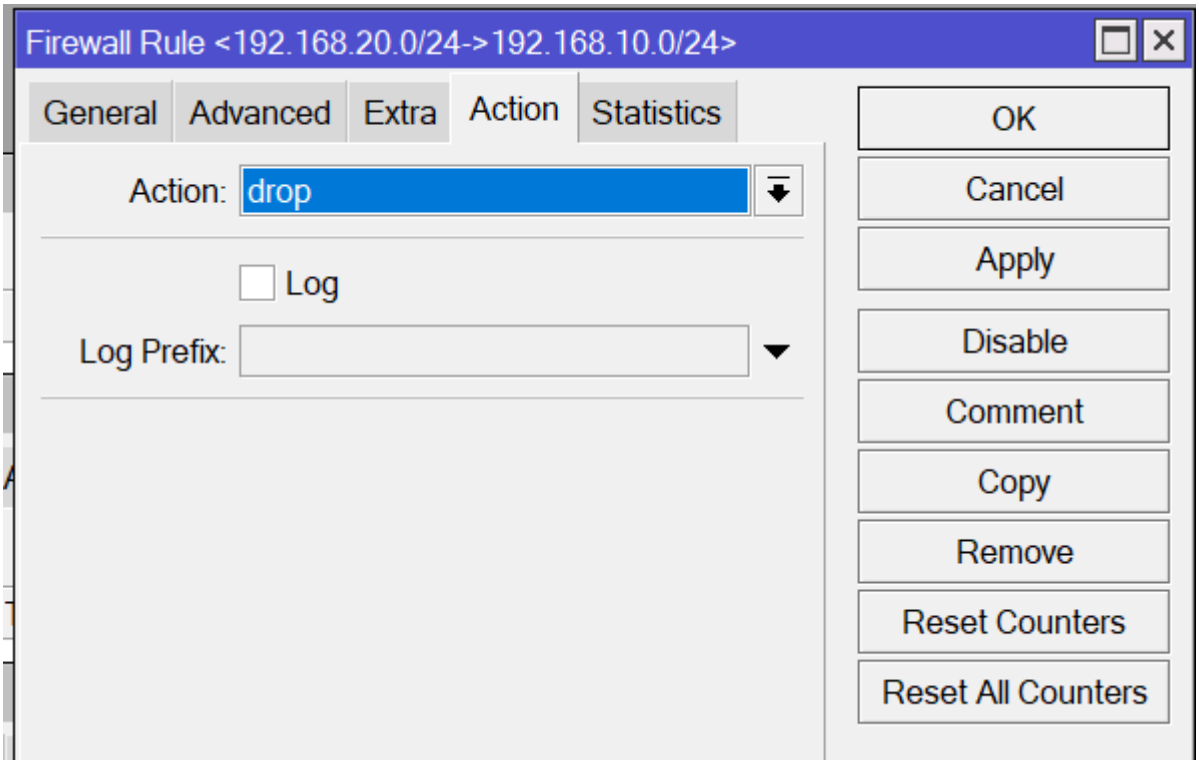
24. Musimy zablokować routing w Mikrotiku R1 wykorzystując do tego firewall na Mikrotiku R1. Dodaj dwie reguły blokujące routing pomiędzy klasami IP 192.168.10.0/24 i 192.168.20.0/24 w **Mikrotiku R1**.

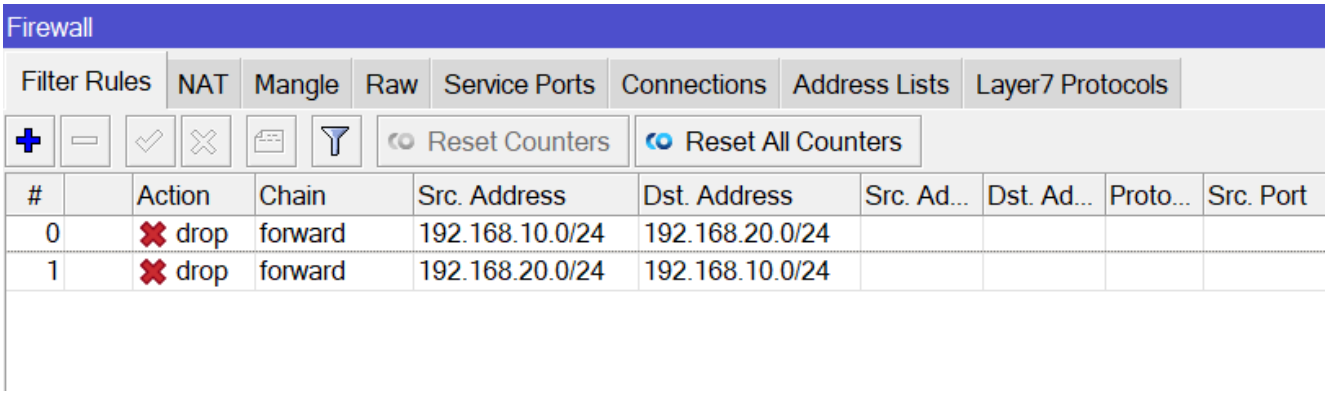

Firewall Rule <192.168.10.0/24->192.168.20.0/24>
General
Advanced
Extra
Action
Statistics
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Chain: forward
Src. Address: 192.168.10.0/24
Dst. Address: 192.168.20.0/24
Src. Address List:
Dst. Address List:
Protocol:
Src. Port:
Dst. Port:
Any. Port:
In. Interface:
Out. Interface:
In. Interface List:
Out. Interface List:
Packet Mark:
Connection Mark:
Routing Mark:
Connection Type:
Connection State:
Connection NAT State:
enabled



i ruch w drugą stronę


Firewall Rule <192.168.20.0/24->192.168.10.0/24>
General
Advanced
Extra
Action
Statistics
Chain: forward
Src. Address: 192.168.20.0/24
Dst. Address: 192.168.10.0/24
Src. Address List:
Dst. Address List:
Protocol:
Src. Port:
Dst. Port:
Any. Port:
In. Interface:
Out. Interface:
In. Interface List:
Out. Interface List:
Packet Mark:
Connection Mark:
Routing Mark:
Connection Type:
Connection State:
Connection NAT State:
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
enabled





25. Sprawdź czy pingowanie pomiędzy Win1 i Win2 przestało działać, a Internet działa dalej.

Zadanie samodzielne

26. Na mikrotiku R2 powiększ oba vlan’y o dodatkowe 2 porty dla każdego z nich podobnie jak dodane zostały porty do których podłączone są maszyny wirtualne Win1 i Win2

27. Na mikrotiku R1 uruchom narzędzie Tools / Torch. Wybierz interface vlan10, powiększ timeout do 10 sekund i wystartuj narzędzie. Ruch który zobaczysz jest generowany przez wbudowane mechanizmy Windows 11 (np.

telemetrię). W maszynie która jest w vlan10 uruchom polecenie:

ping 1.1.1.1 -t

Sprawdź czy w narzędziu torch pojawi się wpis dotyczący protokołu icmp skierowany do adresu ip 1.1.1.1.

Następnie wewnątrz tej samej maszyny uruchom w przeglądarce youtube.com, a w nim jakiś filmik i sprawdź czy jesteś w stanie znaleźć ten ruch w spisie połączeń.