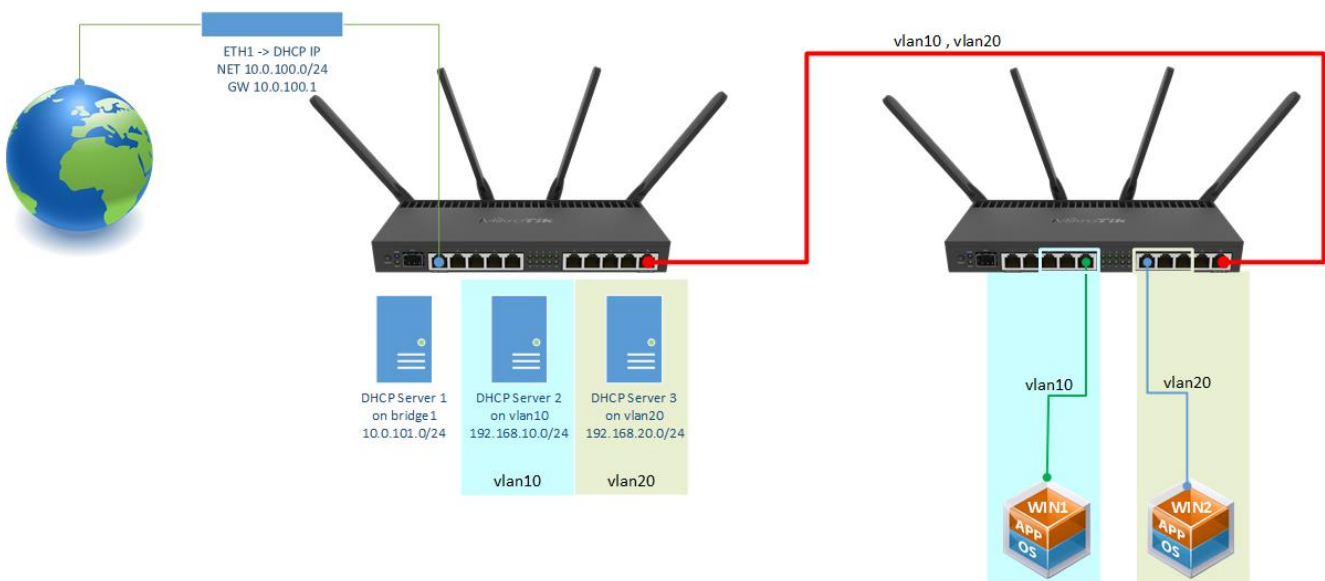


# Mikrotik 7

written by archi | 3 grudnia 2022

## Mikrotik - wykorzystanie technologii VLAN bez switch chip

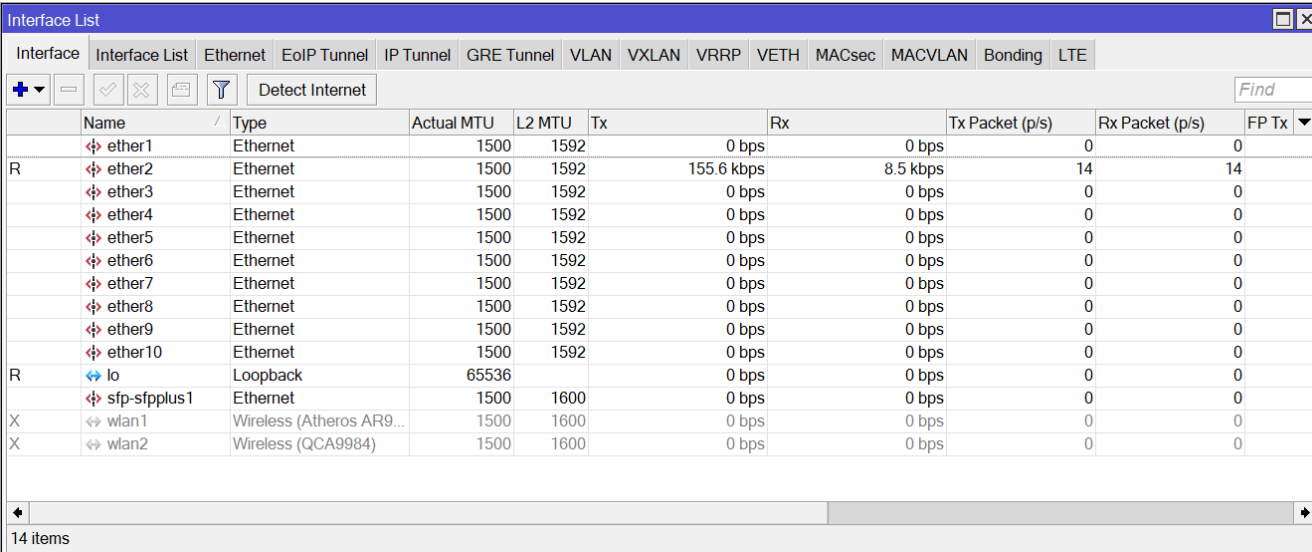
Celem laboratorium jest wykonanie podziału sieci komputerowej (fizycznej) na odrębne podsieci z separacją ruchu pomiędzy nimi. Wykorzystamy funkcjonalność [802.11Q](#) (VLAN), które gwarantują możliwości komunikacji pomiędzy elementami sieci z jednoczesną separacją ruchu. [Technologia VLAN](#) pozwala 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

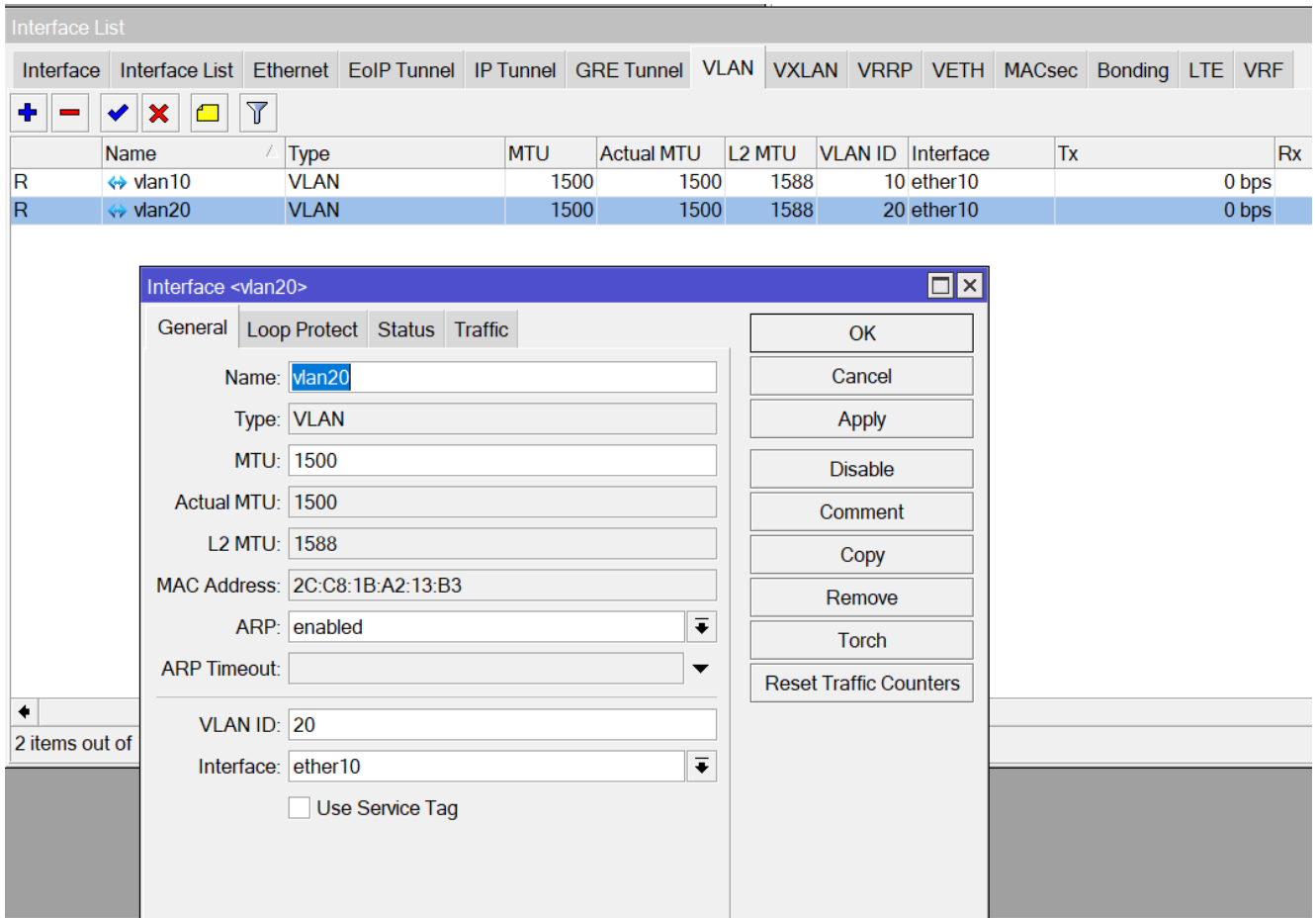


Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx
ether1	Ethernet	1500	1592	0 bps	0 bps	0	0	0
ether2	Ethernet	1500	1592	155.6 kbps	8.5 kbps	14	14	14
ether3	Ethernet	1500	1592	0 bps	0 bps	0	0	0
ether4	Ethernet	1500	1592	0 bps	0 bps	0	0	0
ether5	Ethernet	1500	1592	0 bps	0 bps	0	0	0
ether6	Ethernet	1500	1592	0 bps	0 bps	0	0	0
ether7	Ethernet	1500	1592	0 bps	0 bps	0	0	0
ether8	Ethernet	1500	1592	0 bps	0 bps	0	0	0
ether9	Ethernet	1500	1592	0 bps	0 bps	0	0	0
ether10	Ethernet	1500	1592	0 bps	0 bps	0	0	0
lo	Loopback	65536		0 bps	0 bps	0	0	0
sfp-sfpplus1	Ethernet	1500	1600	0 bps	0 bps	0	0	0
wlan1	Wireless (Atheros AR9...	1500	1600	0 bps	0 bps	0	0	0
wlan2	Wireless (QCA9984)	1500	1600	0 bps	0 bps	0	0	0

### 4. W zakładce VLAN:

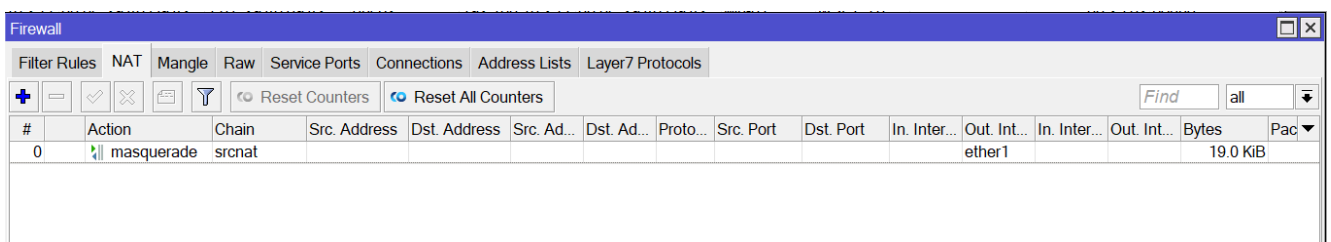
- utwórz vlan o nazwie VLAN10 z identyfikatorem „vlan ID” ustawionym na 10
- utwórz vlan o nazwie VLAN20 z identyfikatorem „vlan ID” ustawionym na 20
- przypnij oba vlan’y do interfejsu ETHER10.

Zobacz przykład dla VLAN20 poniżej.

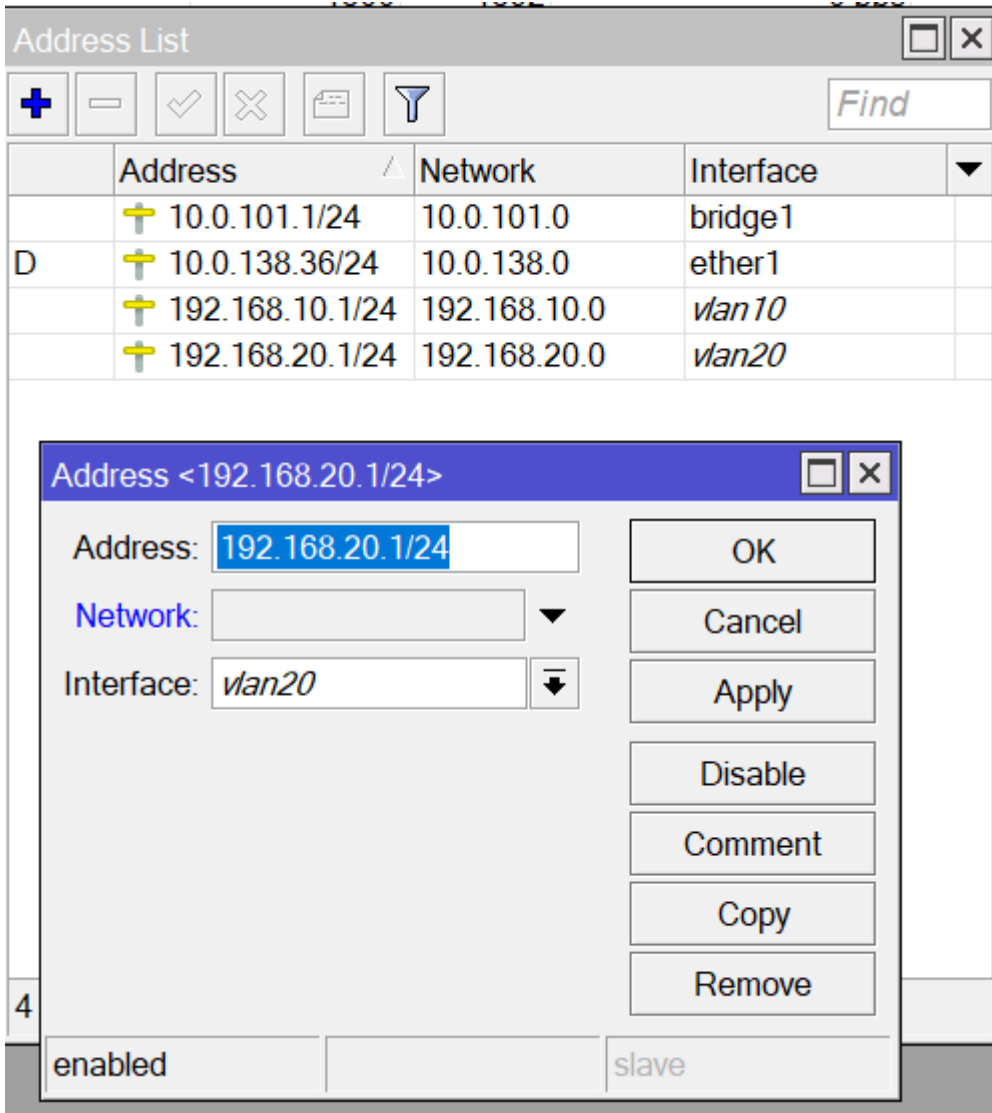


5. Utwórz bridge o nazwie „bridge1”.

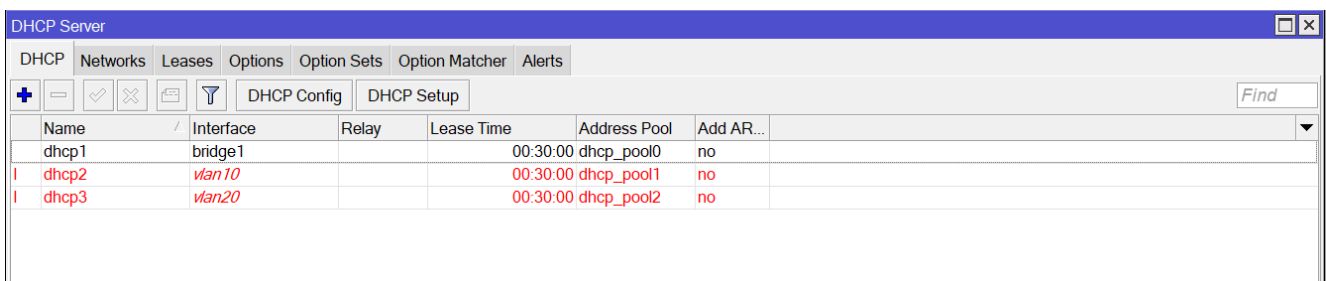
6. Utwórz dhcp-client na porcie Ether1 i podłącz router R1 do Internetu (48-portowy switch) oraz utwórz regułę w firewall dla maskowania adresów IP.



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

Interface	Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	F
R	ether1	Ethernet	1500	1592	0 bps	0 bps	0	0	0	0 bps
R	ether2	Ethernet	1500	1592	158.1 kbps	9.0 kbps	18	15	0	0 bps
	ether3	Ethernet	1500	1592	0 bps	0 bps	0	0	0	0 bps
	ether4	Ethernet	1500	1592	0 bps	0 bps	0	0	0	0 bps
	ether5	Ethernet	1500	1592	0 bps	0 bps	0	0	0	0 bps
	ether6	Ethernet	1500	1592	0 bps	0 bps	0	0	0	0 bps
	ether7	Ethernet	1500	1592	0 bps	0 bps	0	0	0	0 bps
	ether8	Ethernet	1500	1592	0 bps	0 bps	0	0	0	0 bps
	ether9	Ethernet	1500	1592	0 bps	0 bps	0	0	0	0 bps
	ether10	Ethernet	1500	1592	0 bps	0 bps	0	0	0	0 bps
	vlan10	VLAN	1500	1588	0 bps	0 bps	0	0	0	0 bps
	vlan20	VLAN	1500	1588	0 bps	0 bps	0	0	0	0 bps
R	lo	Loopback	65536		1392 bps	1392 bps	1	1	0	0 bps
	sfp-sfpplus1	Ethernet	1500	1600	0 bps	0 bps	0	0	0	0 bps
X	wlan1	Wireless (Atheros AR9...	1500	1600	0 bps	0 bps	0	0	0	0 bps
X	wlan2	Wireless (QCA9884)	1500	1600	0 bps	0 bps	0	0	0	0 bps

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

Name	Type	MTU	Actual MTU	L2 MTU	VLAN ID	Interface	Tx	Rx
RS	vlan10	VLAN	1500	1500	1588	10 ether10	0 bps	
RS	vlan20	VLAN	1500	1500	1588	20 ether10	424 bps	

**Interface <vlan10>**

General | Loop Protect | Status | Traffic

Name:

Type:

MTU:

Actual MTU:

L2 MTU:

MAC Address:

ARP:

ARP Timeout:

VLAN ID:

Interface:

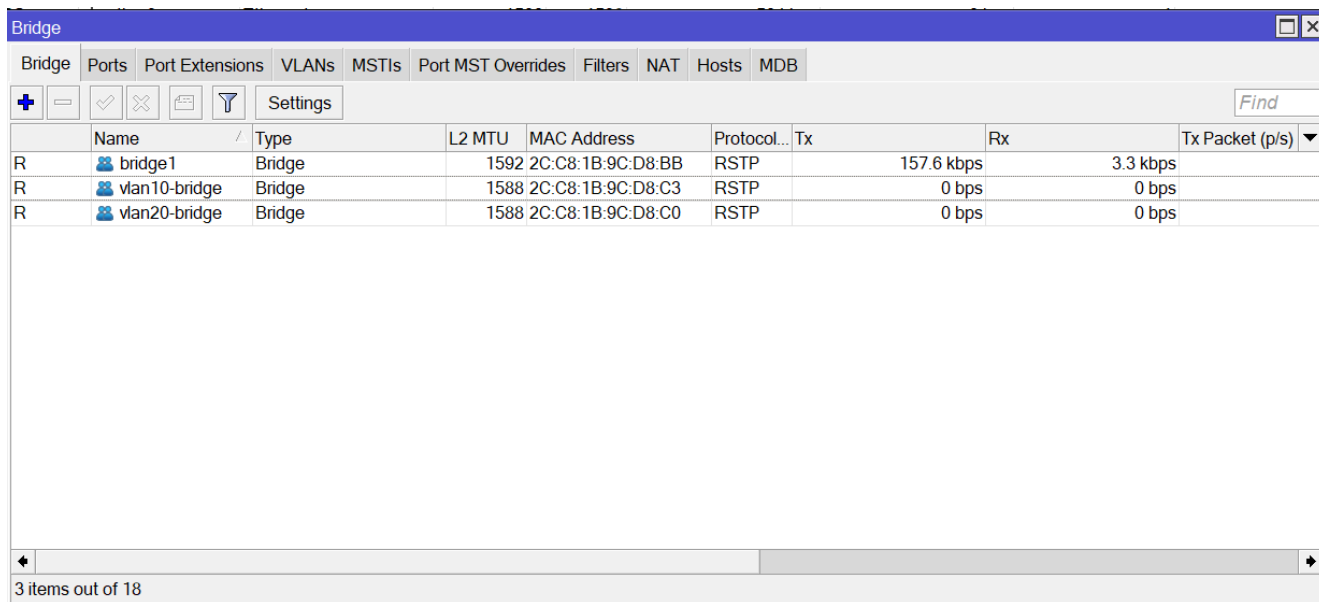
Use Service Tag

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Torch, Reset Traffic Counters

enabled | running | slave | passthrough

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”.

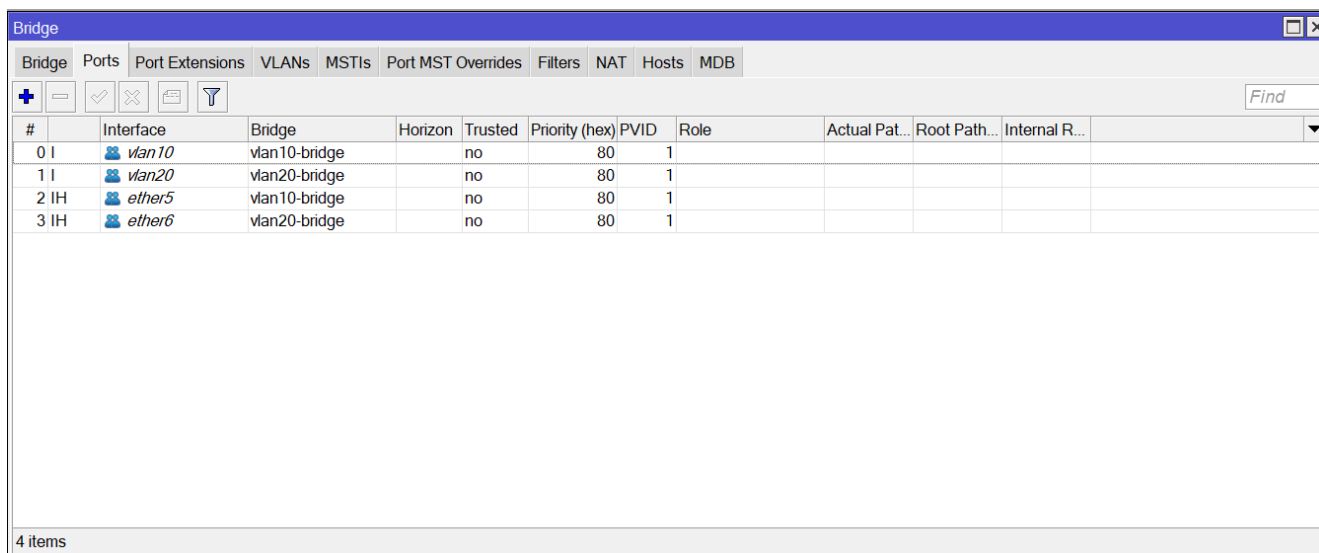


The screenshot shows the Mikrotik WinBox Bridge configuration window. The 'Settings' tab is active, displaying a table of bridge configurations. The table has columns for Name, Type, L2 MTU, MAC Address, Protocol, Tx, Rx, and Tx Packet (p/s). Three bridges are listed: bridge1, vlan10-bridge, and vlan20-bridge.

	Name	Type	L2 MTU	MAC Address	Protocol...	Tx	Rx	Tx Packet (p/s)
R	bridge1	Bridge	1592	2C:C8:1B:9C:D8:BB	RSTP	157.6 kbps	3.3 kbps	
R	vlan10-bridge	Bridge	1588	2C:C8:1B:9C:D8:C3	RSTP	0 bps	0 bps	
R	vlan20-bridge	Bridge	1588	2C:C8:1B:9C:D8:C0	RSTP	0 bps	0 bps	

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.

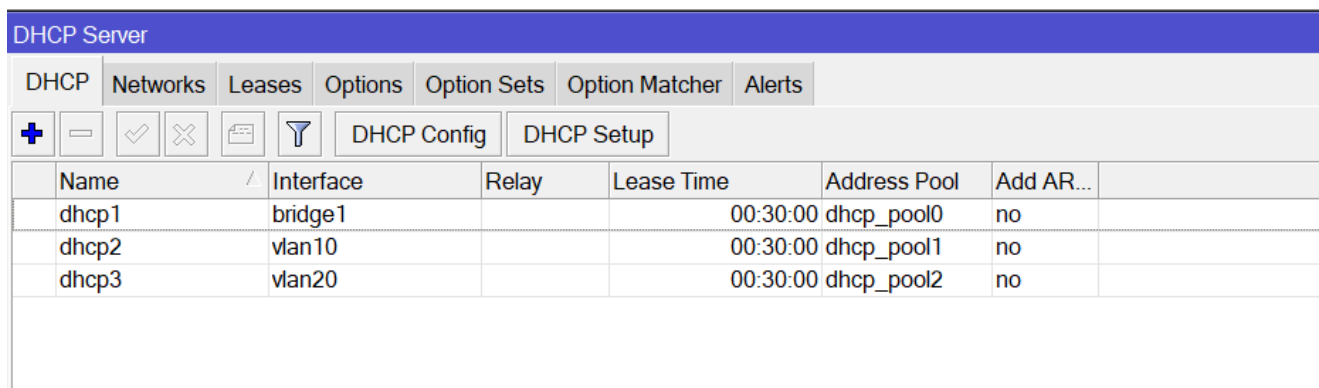


The screenshot shows the Mikrotik WinBox Bridge configuration window with the 'Ports' tab selected. It displays a table of port assignments for the bridges. The table has columns for #, Interface, Bridge, Horizon, Trusted, Priority (hex), PVID, Role, Actual Pat..., Root Path..., and Internal R... Four items are listed.

#	Interface	Bridge	Horizon	Trusted	Priority (hex)	PVID	Role	Actual Pat...	Root Path...	Internal R...
0 I	vlan10	vlan10-bridge		no	80	1				
1 I	vlan20	vlan20-bridge		no	80	1				
2 IH	ether5	vlan10-bridge		no	80	1				
3 IH	ether6	vlan20-bridge		no	80	1				

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

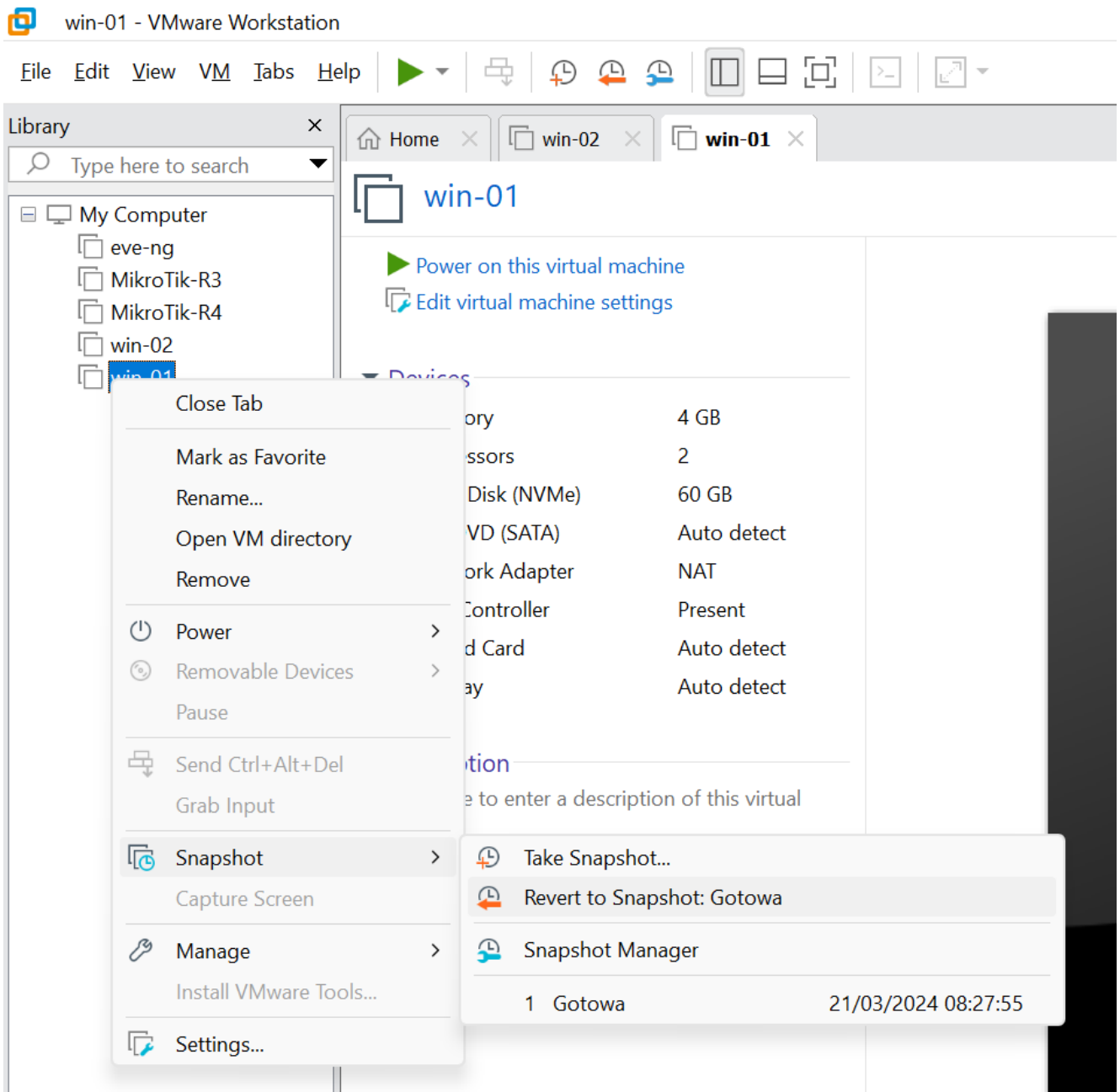
16. Sprawdź na routerze R1, czy zmienił się kolor (czerwony na czarny) serwerów dhcp2 i dhcp3.



The screenshot shows the DHCP Server configuration page. At the top, there are tabs for DHCP, Networks, Leases, Options, Option Sets, Option Matcher, and Alerts. Below the tabs are several icons (plus, minus, checkmark, cross, document, funnel) and two buttons: DHCP Config and DHCP Setup. The main content is a table with the following data:

Name	Interface	Relay	Lease Time	Address Pool	Add AR...
dhcp1	bridge1		00:30:00	dhcp_pool0	no
dhcp2	vlan10		00:30:00	dhcp_pool1	no
dhcp3	vlan20		00:30:00	dhcp_pool2	no

**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:

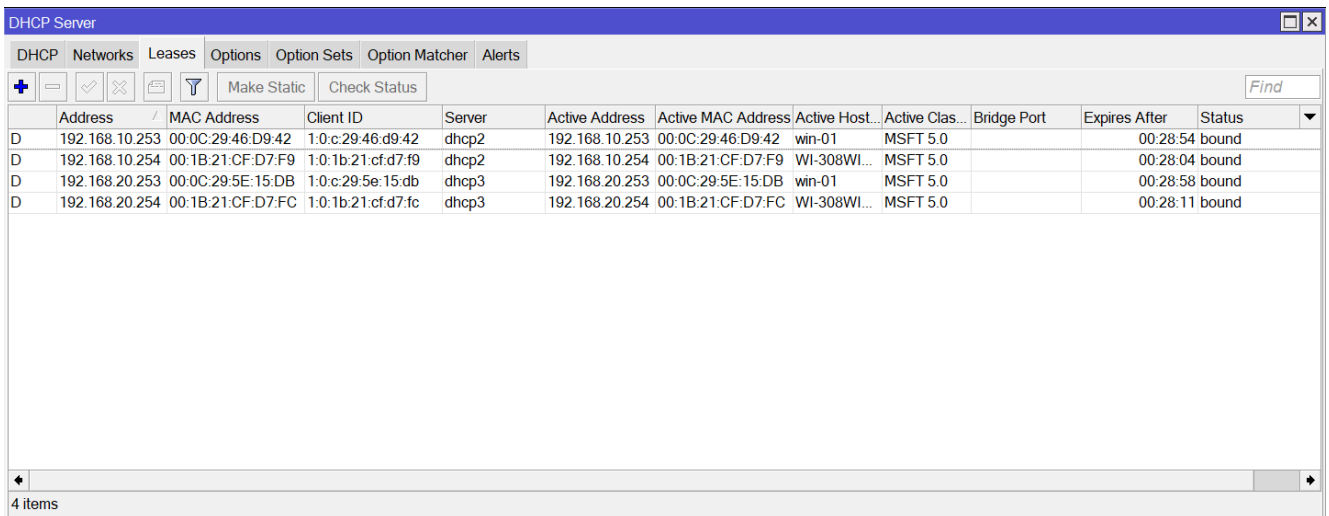
- port ether5 do Karta-Port2,
- port ether6 do Karta-Port3.

18b. Włącz maszyny wirtualne Win1 i Win2.

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

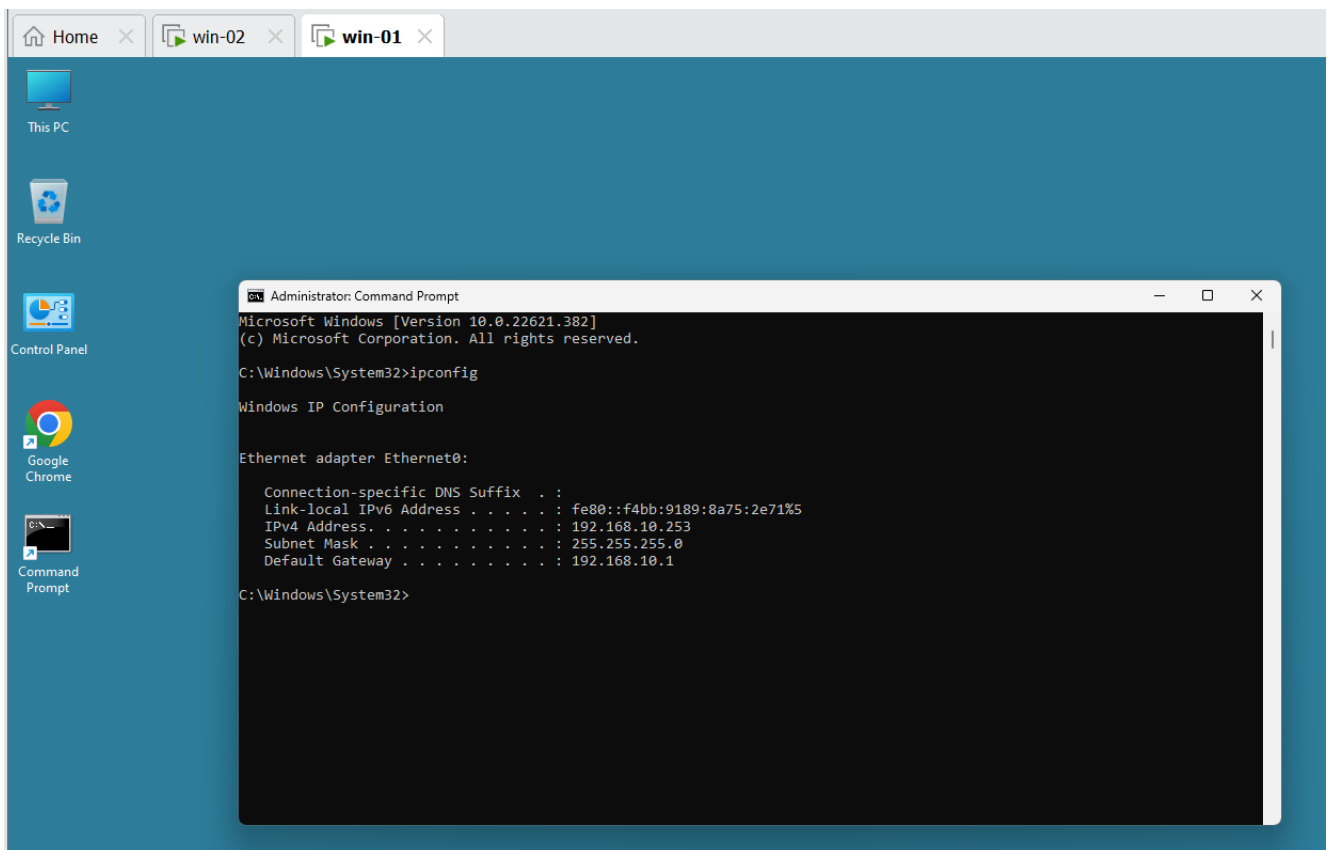


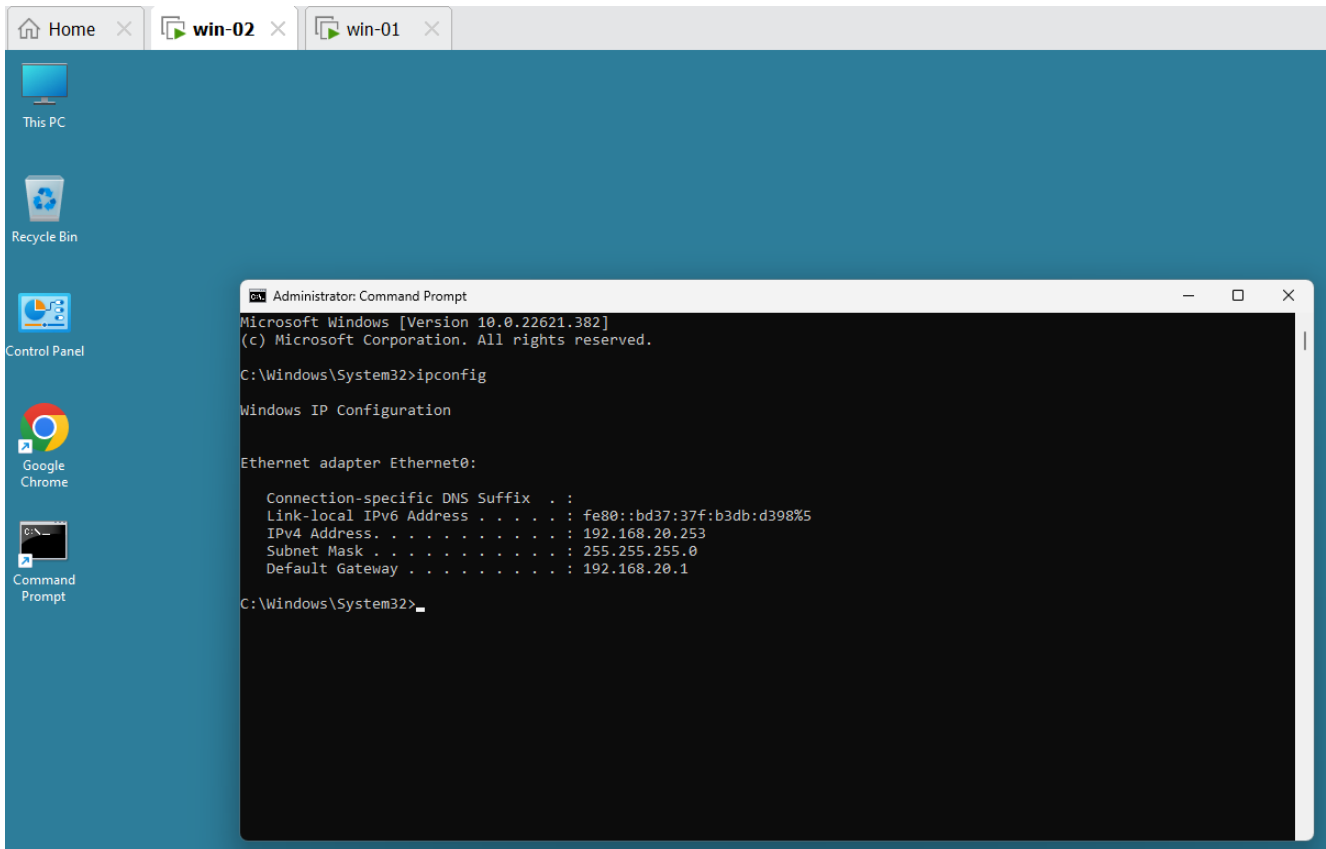
klasach IP zgodnie z podłączonymi vlan. Maszyna Win1 powinna dostać adres IP z klasy 192.168.10.0/24, a maszyna Win2 z klasy 192.168.20.0/24.



	Address	MAC Address	Client ID	Server	Active Address	Active MAC Address	Active Host...	Active Clas...	Bridge Port	Expires After	Status
D	192.168.10.253	00:0C:29:46:D9:42	1:0:c:29:46:d9:42	dhcp2	192.168.10.253	00:0C:29:46:D9:42	win-01	MSFT 5.0		00:28:54	bound
D	192.168.10.254	00:1B:21:CF:D7:F9	1:0:1b:21:cf:d7:f9	dhcp2	192.168.10.254	00:1B:21:CF:D7:F9	WI-308WI...	MSFT 5.0		00:28:04	bound
D	192.168.20.253	00:0C:29:5E:15:DB	1:0:c:29:5e:15:db	dhcp3	192.168.20.253	00:0C:29:5E:15:DB	win-01	MSFT 5.0		00:28:58	bound
D	192.168.20.254	00:1B:21:CF:D7:FC	1:0:1b:21:cf:d7:fc	dhcp3	192.168.20.254	00:1B:21:CF:D7:FC	WI-308WI...	MSFT 5.0		00:28:11	bound

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

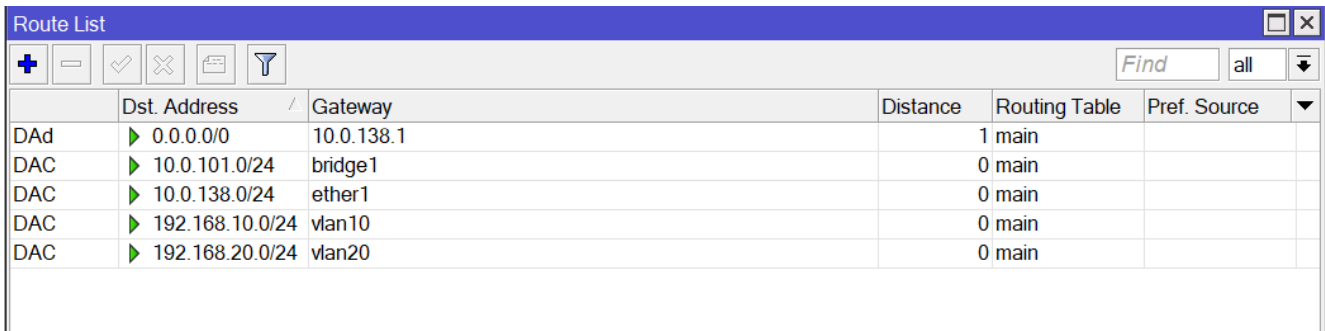
Ping statistics for 65.9.95.42:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 11ms, Average = 11ms

C:\Windows\System32>
```

22. W obydwu maszynach wirtualnych wyłącz zapórę 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.



The screenshot shows the 'Route List' window in Mikrotik WinBox. The window title is 'Route List'. It contains a toolbar with icons for adding, deleting, and filtering routes, and a search field labeled 'Find' with a dropdown menu set to 'all'. Below the toolbar is a table with the following columns: 'Dst. Address', 'Gateway', 'Distance', 'Routing Table', and 'Pref. Source'. The table contains five entries:

	Dst. Address	Gateway	Distance	Routing Table	Pref. Source
DAd	0.0.0.0/0	10.0.138.1	1	main	
DAC	10.0.101.0/24	bridge1	0	main	
DAC	10.0.138.0/24	ether1	0	main	
DAC	192.168.10.0/24	vlan10	0	main	
DAC	192.168.20.0/24	vlan20	0	main	

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

Chain:  ▼

Src. Address:   ▲

Dst. Address:   ▲

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

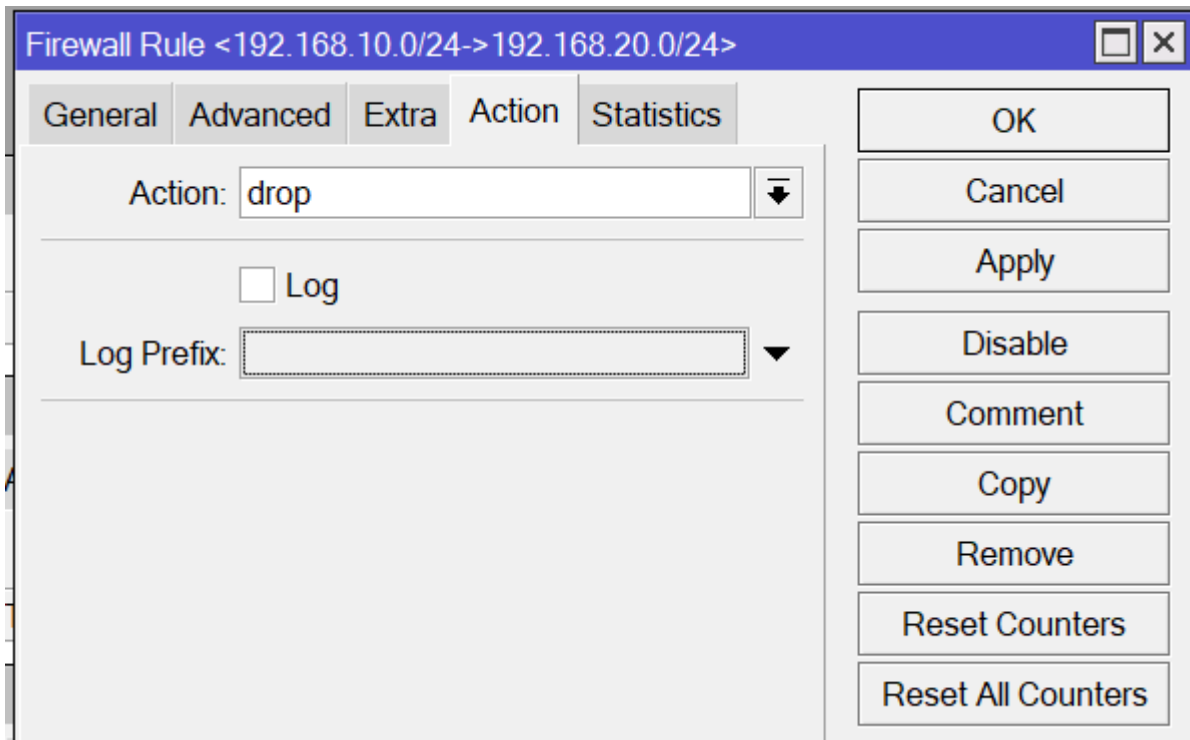
Copy

Remove

Reset Counters

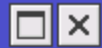
Reset All Counters

enabled



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

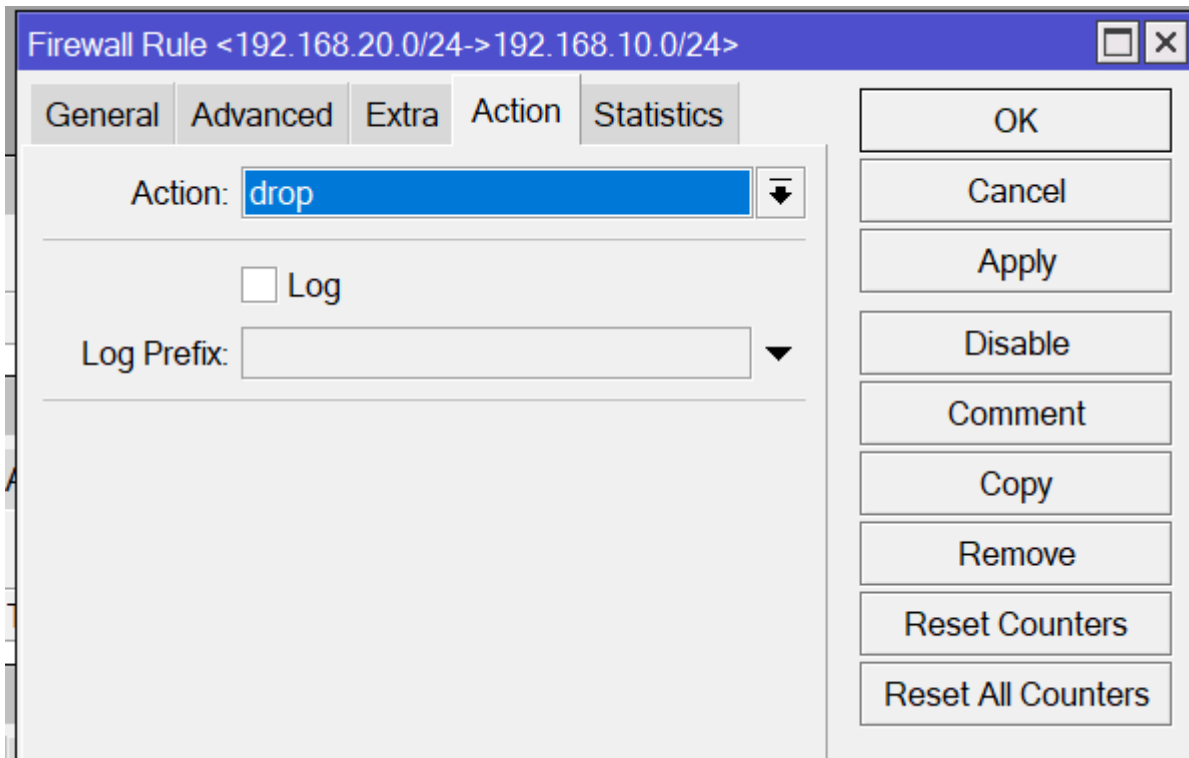
Copy

Remove

Reset Counters

Reset All Counters

enabled



Firewall									
Filter Rules									
NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols									
+ - ✓ ✗ [Filter Icon] [Reset Counters] [Reset All Counters]									
#	Action	Chain	Src. Address	Dst. Address	Src. Ad...	Dst. Ad...	Proto...	Src. Port	
0	✗ drop	forward	192.168.10.0/24	192.168.20.0/24					
1	✗ drop	forward	192.168.20.0/24	192.168.10.0/24					

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.

The screenshot shows the WinBox interface for a Mikrotik router. The 'Torch (Running)' window is open, displaying configuration and a traffic log. The 'Basic' tab is selected, showing the interface set to 'vlan10' and an entry timeout of '00:00:10'. The 'Filters' section is also visible, with various protocol and address filters set to 'any'. The traffic log table below shows the following data:

Eth. Prot...	Protocol	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
4 (802.2)						0 bps	448 bps	0	1
800 (ip)	17 (udp)	192.168.10.201:52446	212.191.227.44:443 (https)			7.9 Mbps	137.5 kbps	772	158
800 (ip)	6 (tcp)	192.168.10.201:50798	10.0.137.25:7680			0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.10.201:50799	10.0.101.142:7680			0 bps	0 bps	0	0
800 (ip)	1 (icmp)	192.168.10.201	192.168.10.1		48	0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.10.201:50795	88.221.255.169:80 (http)			0 bps	0 bps	0	0
800 (ip)	2 (igmp)	192.168.10.200	224.0.0.22			0 bps	2.4 kbps	0	5
800 (ip)	17 (udp)	192.168.10.200:5353	224.0.0.251:5353			0 bps	4.6 kbps	0	6
800 (ip)	17 (udp)	192.168.10.200:63886	224.0.0.252:5355			0 bps	576 bps	0	1
806 (arp)						336 bps	480 bps	1	1
86dd (ipv6)	58	fe80::e0a2:59e:d141:8bdb	ff02::16			0 bps	3.6 kbps	0	5
86dd (ipv6)	17 (udp)	fe80::e0a2:59e:d141:8bdb:5353	ff02::fb:5353			0 bps	5.6 kbps	0	6
86dd (ipv6)	17 (udp)	fe80::e0a2:59e:d141:8bdb:63...	ff02::1:3:5355			0 bps	736 bps	0	1

Summary statistics at the bottom of the log:

- 13 items
- Total Tx: 7.9 Mbps
- Total Rx: 156.0 kbps
- Total Tx Packet: 773
- Total Rx Packet: 184