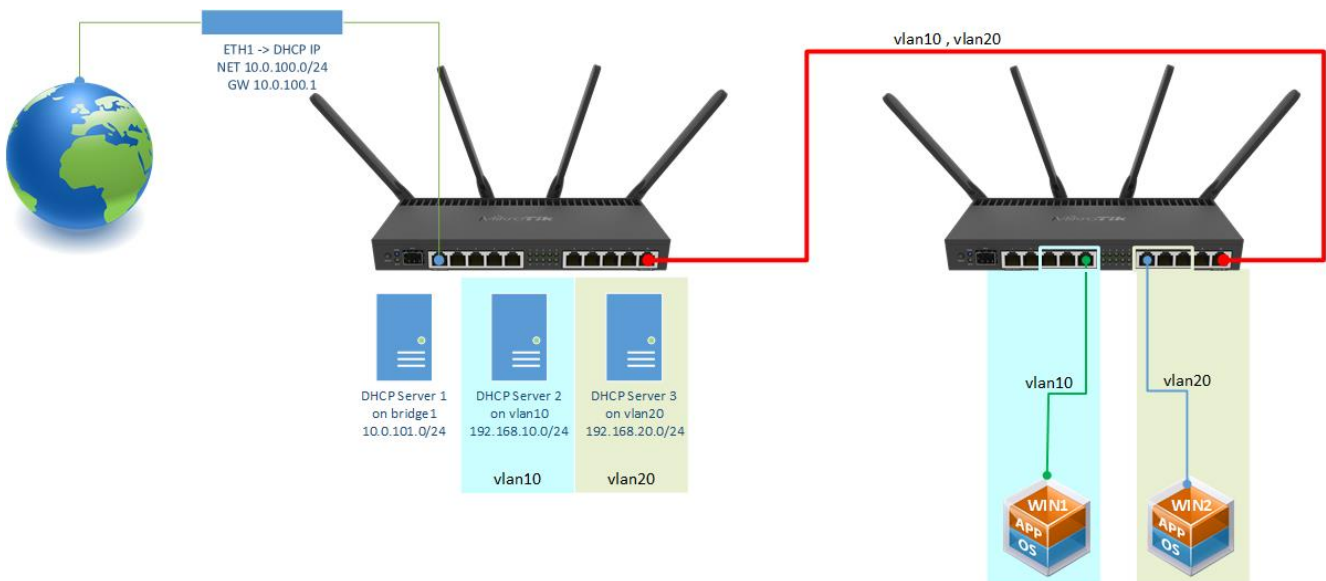


# Mikrotik 7

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 się do routera R1 portem komputera 4 na port ETHER2

# routera

## 2. Przejdź do okna Interface

Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (...)	FP Tx	FP Rx	FP T...	FP Rx Packet (p/s)
XS	WiFi2.4GHz	Wireless (Atheros AR9...	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0
XS	WiFi5GHz	Wireless (QCA9984)	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0
R	bridge1	Bridge	1500	1592	159.9 kbps	7.1 kbps	16	16	0 bps	0 bps	0
R	ether1	Ethernet	1500	1592	0 bps	0 bps	0	0	0 bps	0 bps	0
RS	ether2	Ethernet	1500	1592	160.4 kbps	9.4 kbps	16	16	0 bps	8.9 kbps	0
S	ether3	Ethernet	1500	1592	0 bps	0 bps	0	0	0 bps	0 bps	0
S	ether4	Ethernet	1500	1592	0 bps	0 bps	0	0	0 bps	0 bps	0
S	ether5	Ethernet	1500	1592	0 bps	0 bps	0	0	0 bps	0 bps	0
S	ether6	Ethernet	1500	1592	0 bps	0 bps	0	0	0 bps	0 bps	0
S	ether7	Ethernet	1500	1592	0 bps	0 bps	0	0	0 bps	0 bps	0
S	ether8	Ethernet	1500	1592	0 bps	0 bps	0	0	0 bps	0 bps	0
S	ether9	Ethernet	1500	1592	0 bps	0 bps	0	0	0 bps	0 bps	0
R	ether10	Ethernet	1500	1592	0 bps	1016 bps	0	2	0 bps	952 bps	0
R	vlan10	VLAN	1500	1588	0 bps	440 bps	0	1	0 bps	440 bps	0
R	vlan20	VLAN	1500	1588	0 bps	440 bps	0	1	0 bps	440 bps	0
S	sfp-sfpplus1	Ethernet	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0

## 3. W zakładce VLAN:

- utwórz VLAN10 z vlan ID 10
- utwórz VLAN20 z vlan ID 20
- przypnij oba vlan'y do interfejsu ETHER10.

Zobacz przykład dla VLAN20 poniżej.

Interface List

Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VXLAN	VRRP	VETH	MACsec	Bonding	LTE	VRF
R	↔ vlan10												
R	↔ vlan20												

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

Interface <vlan20>

General | Loop Protect | Status | Traffic

Name:

Type:

MTU:

Actual MTU:

L2 MTU:

MAC Address:

ARP:

ARP Timeout:

VLAN ID:

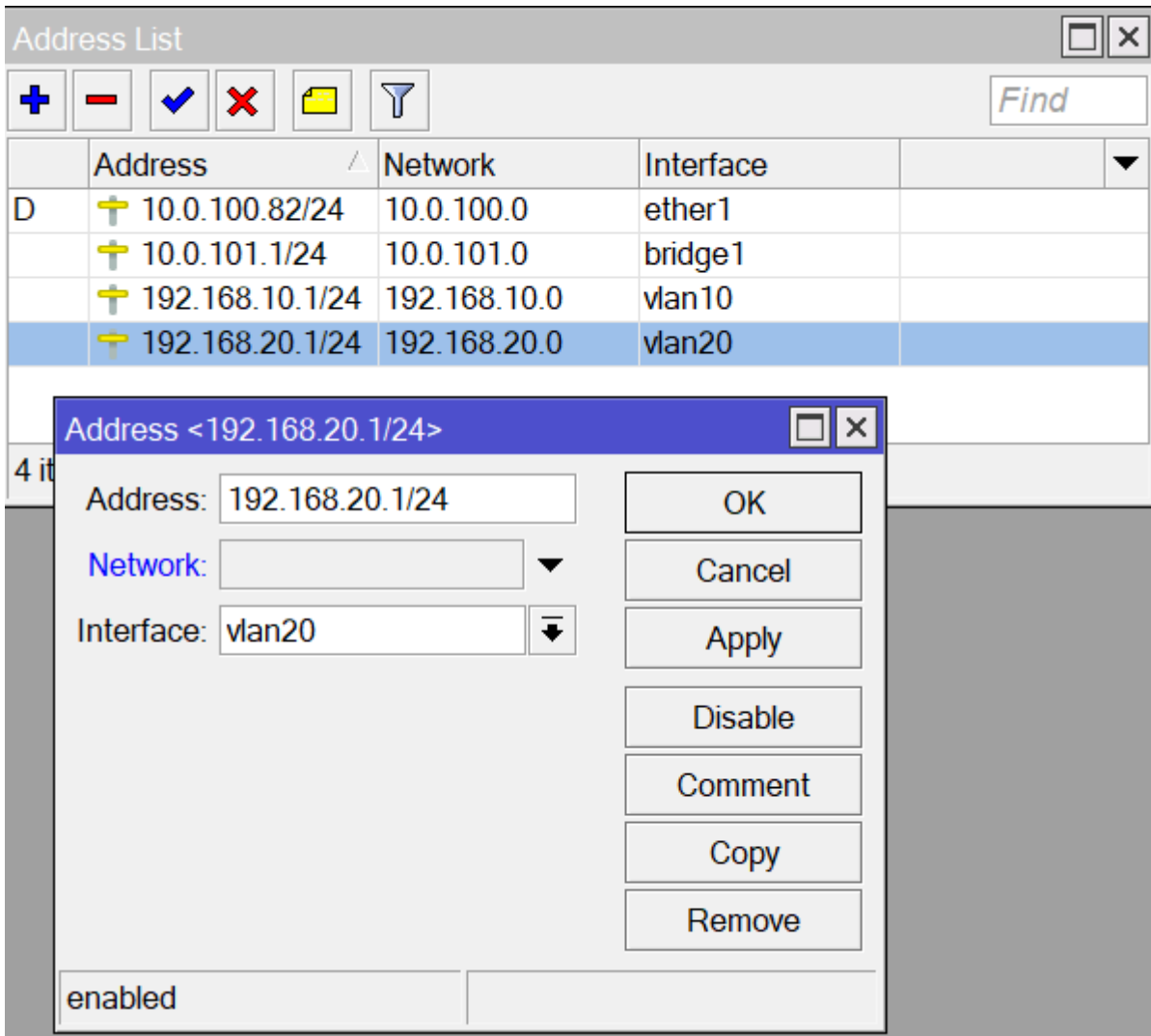
Interface:

Use Service Tag

OK  
Cancel  
Apply  
Disable  
Comment  
Copy  
Remove  
Torch  
Reset Traffic Counters

2 items out of

4. Nadaj adresy IP dla nowych interfejsów vlan10 i vlan20 odpowiednio dla vlan10 adres 192.168.10.1/24, a dla vlan20 adres 192.168.20.1/24. Przykład poniżej dla vlan20.



5. Ustaw serwery DHCP dla obu interfejsów. Użyj „DHCP Setup” dla odpowiedniego interfejsu i pozostaw wszystkie parametry na proponowanych wartościach. Sprawdź jedynie czy adres DNS będzie zaproponowany jako 8.8.8.8. Jeżeli nie pamiętasz jak tworzyć serwer DHCP, zajrzyj do laborki z [DHCP](#).

DHCP Server

DHCP Networks Leases Options Option Sets Option Matcher Alerts

+ - ✓ ✗ 📄 🔍 DHCP Config DHCP Setup Find

Name	Interface	Relay	Lease Time	Address Pool	Add ARP For Leases
dhcp1	bridge1		00:10:00	dhcp	no
dhcp2	vlan10		00:10:00	dhcp_pool8	no
dhcp3	vlan20		00:10:00	dhcp_pool9	no

3 items (1 selected)

**6. Połącz się do routera R2 portem komputera 3 na port ETHER2 routera. Będziemy teraz konfigurować R2.**

7. Otwórz interfejsy i przejdź do zakładki VLAN

Interface List

Interface Interface List Ethernet EoIP Tunnel IP Tunnel GRE Tunnel VLAN VXLAN VRRP VETH MACsec Bonding LTE VRF

+ - ✓ ✗ 📄 🔍 Detect Internet Find

Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx
XS WiFi5GHz	Wireless (QCA9984)	1500	1600	0 bps	0 bps	0	0	0	0 bps
R bridge1	Bridge	1500	1592	159.9 kbps	3.8 kbps	3	4	0	0 bps
ether1	Ethernet	1500	1592	0 bps	0 bps	0	0	0	0 bps
RS ether2	Ethernet	1500	1592	165.6 kbps	4.0 kbps	15	4	0	0 bps
S ether3	Ethernet	1500	1592	0 bps	0 bps	0	0	0	0 bps
S ether4	Ethernet	1500	1592	0 bps	0 bps	0	0	0	0 bps
S ether5	Ethernet	1500	1592	0 bps	0 bps	0	0	0	0 bps
S ether6	Ethernet	1500	1592	0 bps	0 bps	0	0	0	0 bps
RS ether7	Ethernet	1500	1592	520 bps	2.3 kbps	1	2	456	0 bps
S ether8	Ethernet	1500	1592	0 bps	0 bps	0	0	0	0 bps
RS ether9	Ethernet	1500	1592	520 bps	1784 bps	1	1	0	0 bps
R ether10	Ethernet	1500	1592	5.2 kbps	520 bps	5	1	520	0 bps
RS vlan10	VLAN	1500	1588	2.1 kbps	0 bps	2	0	0	0 bps
RS vlan20	VLAN	1500	1588	2.6 kbps	456 bps	3	1	488	0 bps
S sfp-sfpplus1	Ethernet	1500	1600	0 bps	0 bps	0	0	0	0 bps
R vlan10-bridge	Bridge	1500	1588	0 bps	1640 bps	0	1	0	0 bps
R vlan20-bridge	Bridge	1500	1588	0 bps	1640 bps	0	1	0	0 bps

18 items (1 selected)

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

Interface List

Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VXLAN	VRRP	VETH	MACsec	Bonding	LTE	VRF	
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

OK  
Cancel  
Apply  
Disable  
Comment  
Copy  
Remove  
Torch  
Reset Traffic Counters

enabled | running | slave | passthrough

9. W ramach definicji Bridge dodaj dwa nowe switch mostki o nazwach vlan10-bridge i vlan20-bridge. Będą one służyć za porty urządzenia switch, do którego będzie można podłączyć komputery w trybie „untagged” lub w terminologii Cisco „Access Port”.

Bridge

Bridge | Ports | Port Extensions | VLANs | MSTIs | Port MST Overrides | Filters | NAT | Hosts | MDB

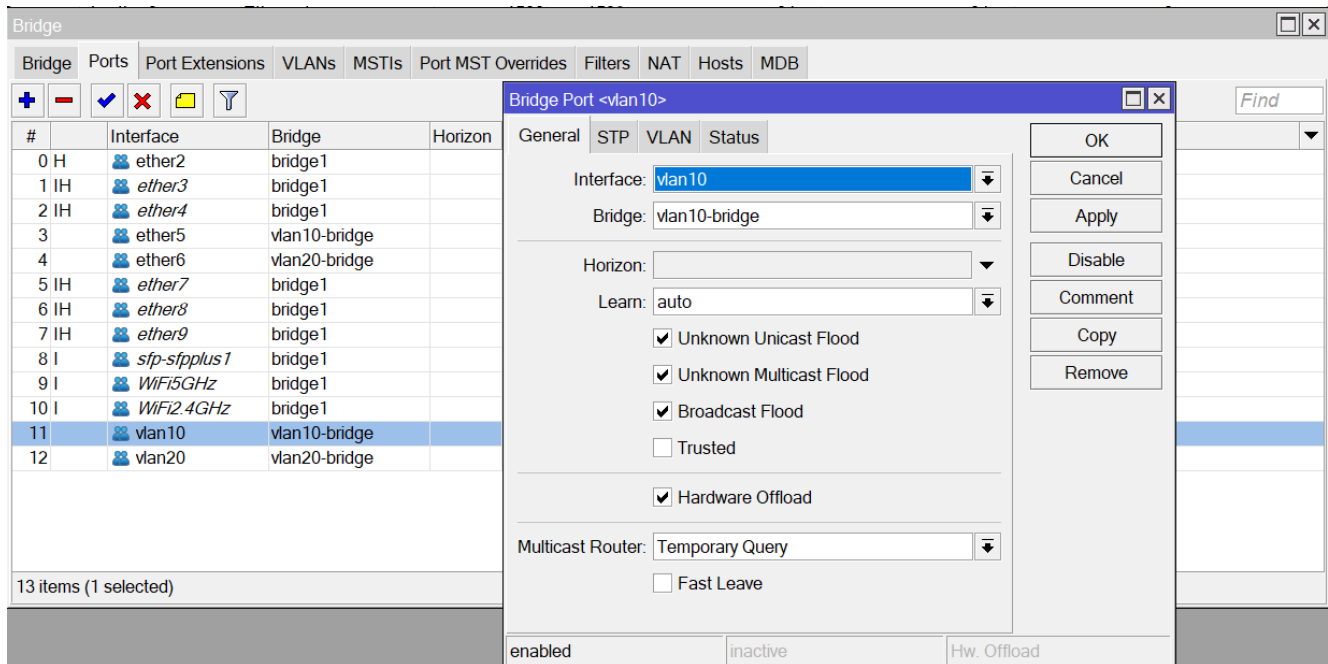
Settings

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

3 items out of 18

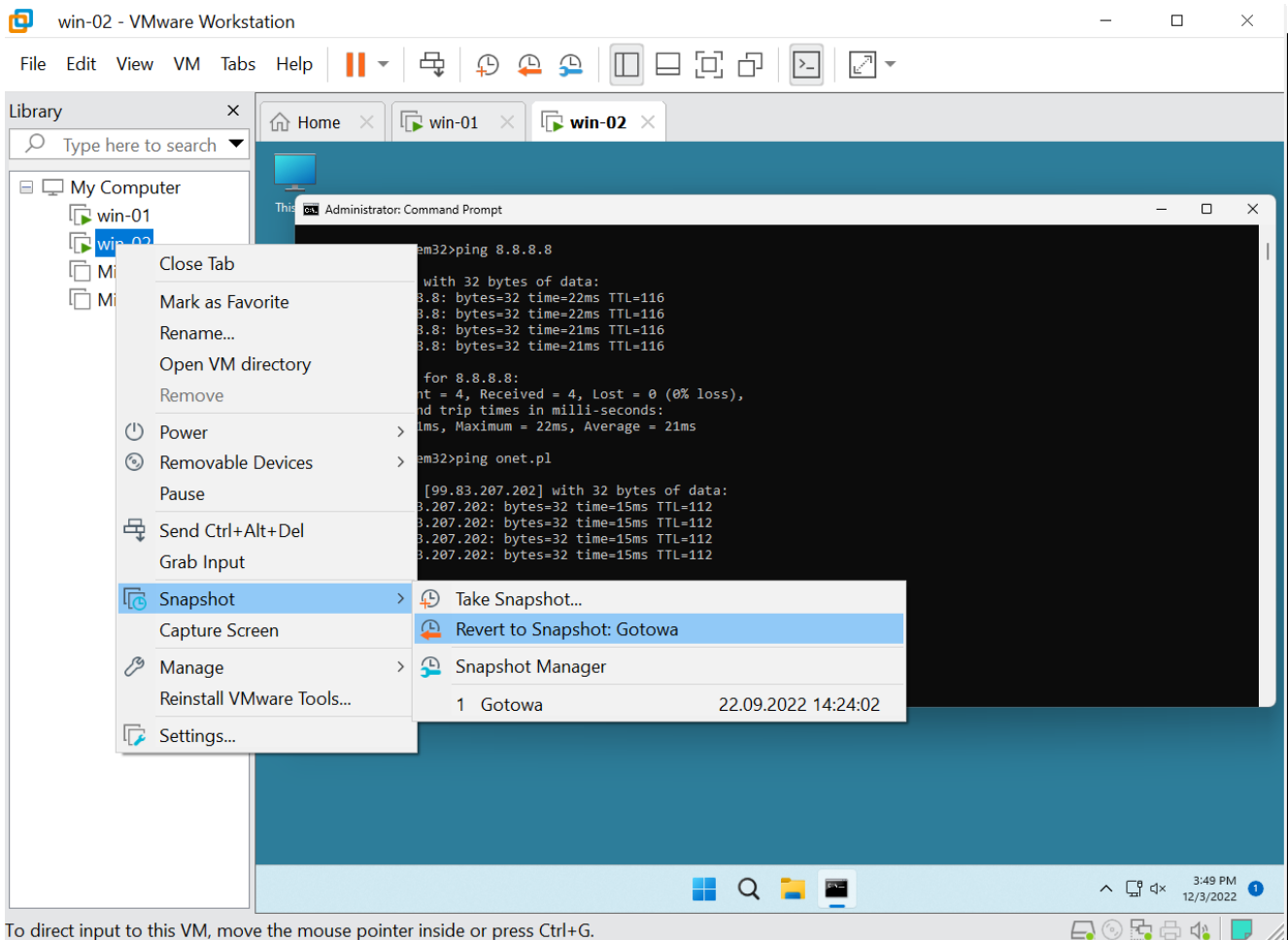
10. Dodaj i zmień odpowiednie porty do definicji bridge:

- przypisz interface vlan10 do bridge vlan10-bridge,
- przypisz interface vlan20 do bridge vlan20-bridge,
- zmień przypisanie interfejsu ether5 do bridge vlan10-bridge,
- zmień przypisanie interfejsu ether6 do bridge vlan20-bridge.



11. Połącz **R1** -> Ether10 z **R2** -> Ether10 (przy pomocy krótkiego przewodu RJ45 - zielony 0,5m)

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



13. Podłącz Win1 do Karta-Port1 a następnie do routera R2 do portu ether5, natomiast Win2 do Karta-Port2 i następnie do routera R2 do portu ether6.

14. 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.

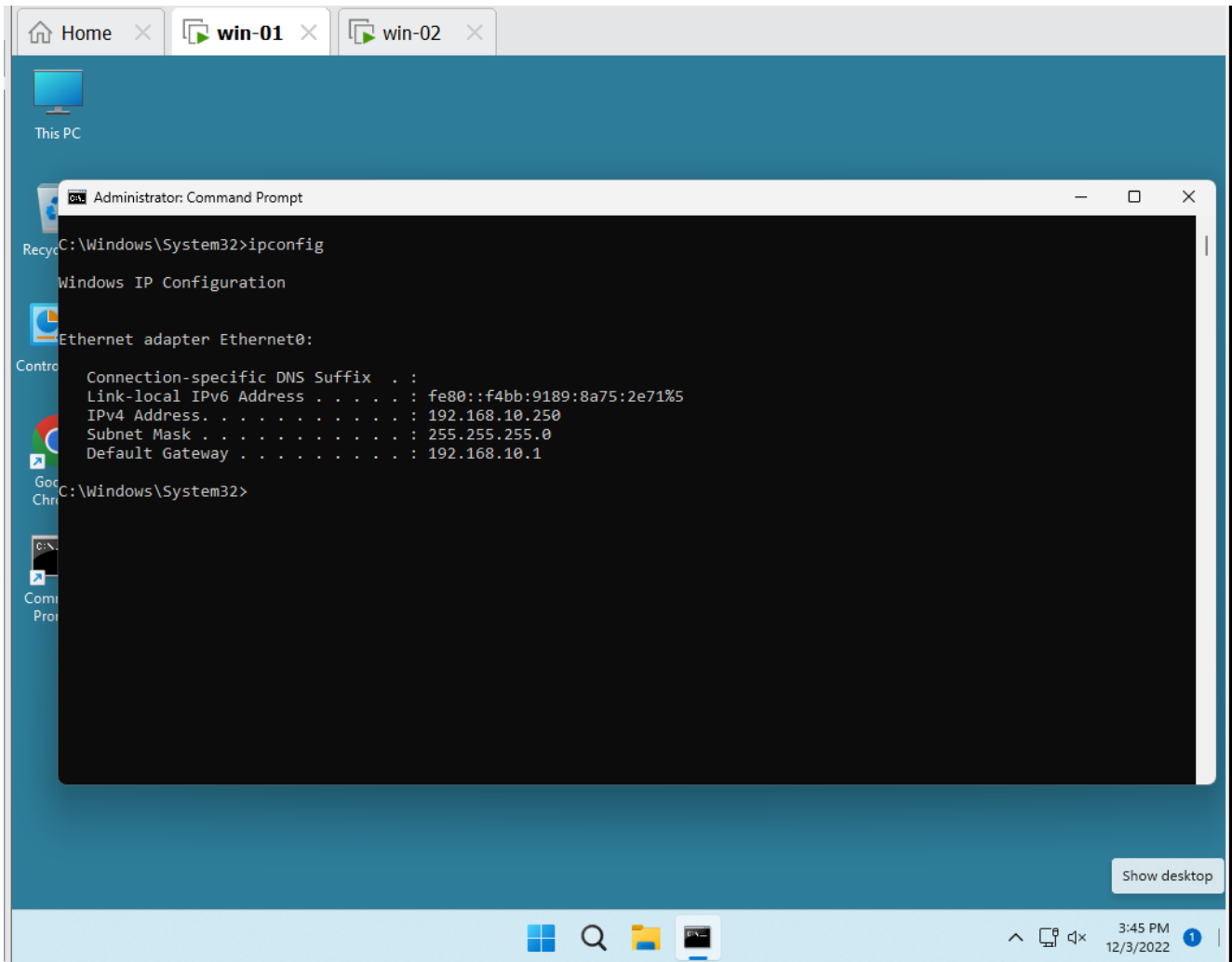
The screenshot shows the DHCP Server console with the 'Leases' tab selected. The table below represents the data shown in the console:

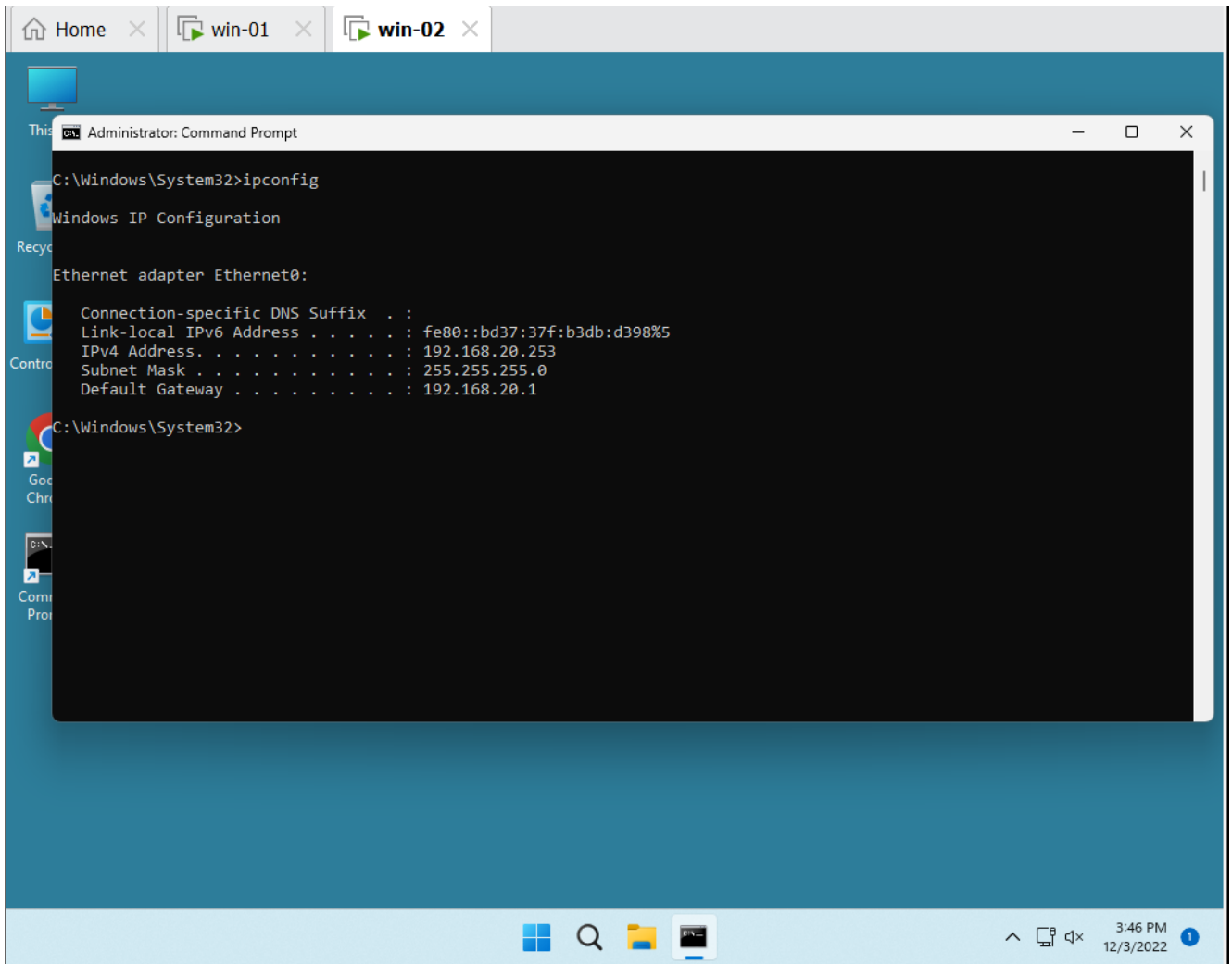
	Address	MAC Address	Client ID	Server	Active Address	Active MAC Address	Active Ho...	Bridge Port	Expires After
D	192.168.10.249	00:1B:21:CF:D7:F8	1:0:1b:21:cf:d7:f8	dhcp2	192.168.10.249	00:1B:21:CF:D7:F8	LAB308-11		00:09:45 bc
D	192.168.20.250	00:1B:21:CF:D7:F9	1:0:1b:21:cf:d7:f9	dhcp3	192.168.20.250	00:1B:21:CF:D7:F9	LAB308-11		00:09:46 bc
D	10.0.101.146	00:1B:21:CF:D7:FC	1:0:1b:21:cf:d7:fc	dhcp1	10.0.101.146	00:1B:21:CF:D7:FC	LAB308-11	ether2	00:06:47 bc
D	192.168.10.250	00:0C:29:46:D9:42	1:0:c:29:46:d9:42	dhcp2	192.168.10.250	00:0C:29:46:D9:42	win-01		00:06:53 bc
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-02		00:07:45 bc

At the bottom of the console, it indicates "5 items".

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







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

```
Administrator: Command Prompt

C:\Windows\System32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::bd37:37f:b3db:d398%5
    IPv4 Address. . . . . : 192.168.20.253
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.20.1

C:\Windows\System32>ping 8.8.8.8

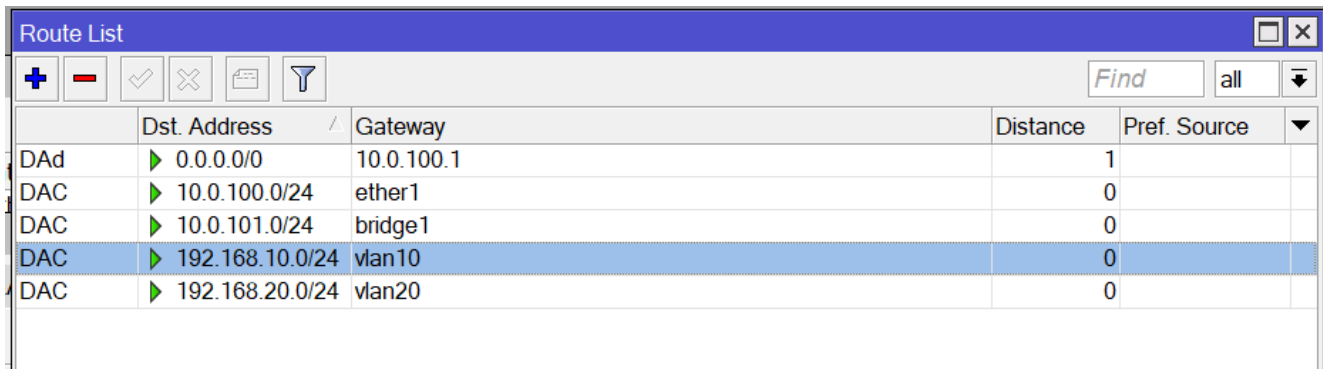
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=22ms TTL=116
Reply from 8.8.8.8: bytes=32 time=22ms TTL=116
Reply from 8.8.8.8: bytes=32 time=21ms TTL=116
Reply from 8.8.8.8: bytes=32 time=21ms TTL=116

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 21ms, Maximum = 22ms, Average = 21ms

C:\Windows\System32>
```

17. Wyłącz na obu windowsach Firewall i sprawdź nawzajem czy z maszyny win-01 można spingować maszynę win-02 oraz czy z win-02 można spingować win-01.

17a. Czy maszyny Win1 i Win2 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'. Below the title bar is a toolbar with icons for adding (+), deleting (-), checking (✓), unchecking (✗), refreshing (refresh icon), and filtering (funnel icon). To the right of the toolbar is a search field labeled 'Find' with a dropdown menu currently set to 'all'. Below the toolbar is a table with the following columns: 'Type', 'Dst. Address', 'Gateway', 'Distance', and 'Pref. Source'. The table contains five rows of route information.

Type	Dst. Address	Gateway	Distance	Pref. Source
DAd	0.0.0.0/0	10.0.100.1	1	
DAC	10.0.100.0/24	ether1	0	
DAC	10.0.101.0/24	bridge1	0	
DAC	192.168.10.0/24	vlan10	0	
DAC	192.168.20.0/24	vlan20	0	

18. 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

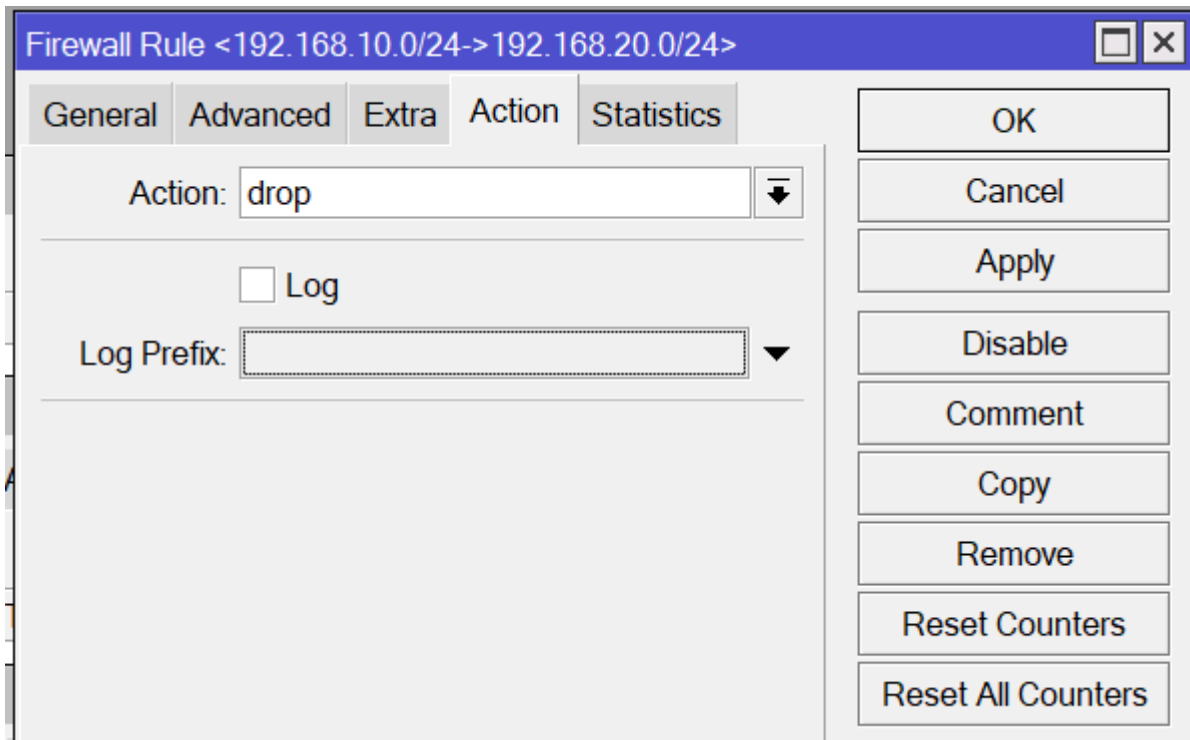
Copy

Remove

Reset Counters

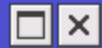
Reset All Counters

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

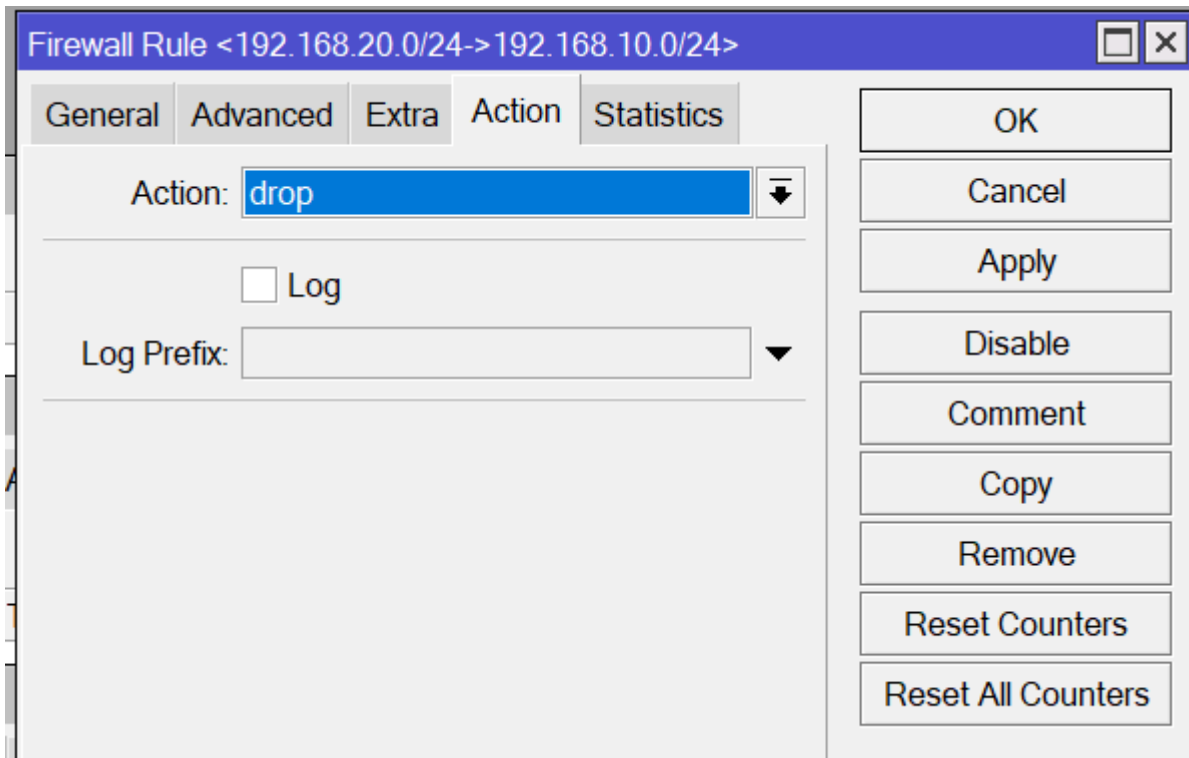
Copy

Remove

Reset Counters

Reset All Counters

enabled



19. 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

20. 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 youtube.com, a w nim jakiś filmik i sprawdź czy jesteś w stanie znaleźć ten ruch w spisie połączeń.



admin@10.0.101.1 (R1) - WinBox (64bit) v7.6 on RB4011iGS+5HacQ2HnD (arm)

Session Settings Dashboard

Safe Mode Session: 10.0.101.1

- Quick Set
- CAPsMAN
- User Manager
- Interfaces
- Wireless
- WireGuard
- Zero Tier
- Bridge
- PPP
- Switch
- Mesh
- IP
- IPv6
- MPLS
- Routing
- System
- Queues
- Files
- Log
- RADIUS
- Tools
- New Terminal
- TR069
- LoRa
- IoT
- Dot1X
- Dude
- Container
- Partition
- Make Supout.rf
- New WinBox
- Exit
- Windows

**Torch (Running)**

**- Basic**

Interface: vlan10

Entry Timeout: 00:00:10 s

**- Filters**

Src. Address:

Dst. Address:

Src. Address6:

Dst. Address6:

MAC Protocol:

Protocol:

Port:

VLAN Id:

DSCP:

Start

Stop

Close

New Window

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 (pv6)	58	fe80::e0a2:59e:d141:8bdb	ff02::16			0 bps	3.6 kbps	0	5
86dd (pv6)	17 (udp)	fe80::e0a2:59e:d141:8bdb:5353	ff02::fb:5353			0 bps	5.6 kbps	0	6
86dd (pv6)	17 (udp)	fe80::e0a2:59e:d141:8bdb:63...	ff02::1:3:5355			0 bps	736 bps	0	1

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