



MikroTik Certified Network Associate



MikroTik Warsaw
Training Center

MikroTik



Mikrotiks Ltd. (po łotewsku *mikro tīkls* znaczy «mikro-sieci»)

- Łotewska firma, produkująca sprzęt sieciowy, oraz twórca systemu operacyjnego RouterOS, który pracuje na jądrze Linux
- Założona w 1996 roku
- Początkowo specjalizowała się w rozwiązaniach bezprzewodowych

Product categories

All products

Ethernet routers

Switches

Wireless systems

Wireless for home and office

LTE products

Data over Powerlines

IoT products

60 GHz products

RouterBOARD

Enclosures

Interfaces

Accessories

Antennas



<https://mikrotik.com/products>

Podstawy

RouterOS

- System operacyjny firmy MikroTik (oparty na Linux-a)
- System jest licencjonowany
- Może pracować na platformie RouterBoard (m.in. *ARM*, *ARM64*, *SMIPS*, *MIPSBE*, *Tile*), sprzęcie kompatybilnym z *x86*, również jako maszyna wirtualna

Licencjonowanie

- Każde urządzenie RouterBoard posiada zainstalowany system operacyjny RouterOS wraz z odpowiednią licencją
- Licencja może być dokupiona osobno (na przykład - RouterOS dla platformy x86)
- Licencja powiązana z dyskiem twardym (UUID dysku)/pamięcią flash, na którym zainstalowano RouterOS

Typ licencji

| Level number | 0 (Trial mode) | 1 (Free Demo) | 3 (WISP CPE) | 4 (WISP) | 5 (WISP) | 6 (Controller) |
|------------------------------|----------------|------------------------------|---------------------|-----------|-----------|----------------|
| Price | <i>no key</i> | <i>registration required</i> | <i>not for sale</i> | \$45 | \$95 | \$250 |
| Wireless AP mode (PtM) | 24h trial | - | no | yes | yes | yes |
| PPPoE tunnels | 24h trial | 1 | 200 | 200 | 500 | unlimited |
| PPTP tunnels | 24h trial | 1 | 200 | 200 | 500 | unlimited |
| L2TP tunnels | 24h trial | 1 | 200 | 200 | 500 | unlimited |
| OVPN tunnels | 24h trial | 1 | 200 | 200 | 500 | unlimited |
| EoIP tunnels | 24h trial | 1 | unlimited | unlimited | unlimited | unlimited |
| VLAN interfaces | 24h trial | 1 | unlimited | unlimited | unlimited | unlimited |
| Queue rules | 24h trial | 1 | unlimited | unlimited | unlimited | unlimited |
| HotSpot active users | 24h trial | 1 | 1 | 200 | 500 | unlimited |
| User manager active sessions | 24h trial | 1 | 10 | 20 | 50 | unlimited |



Licencjonowanie

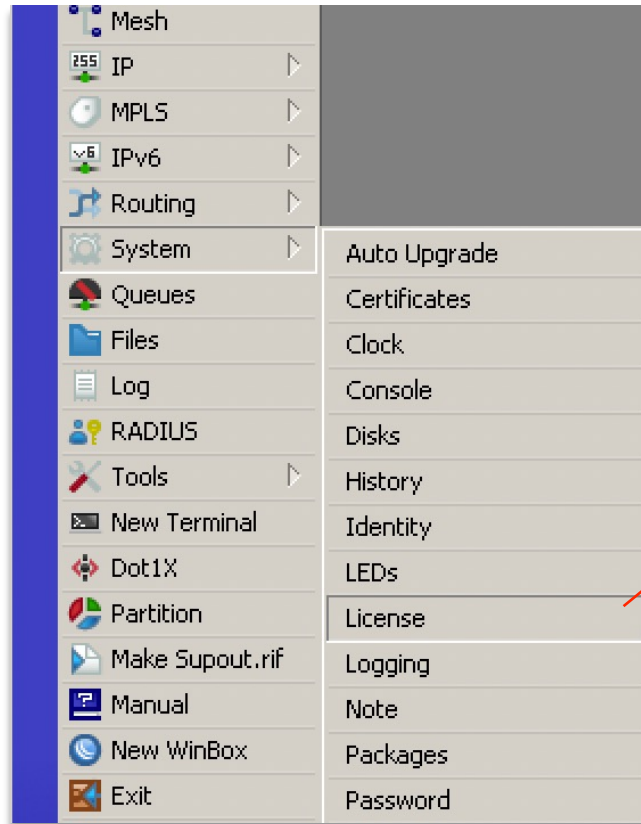
CHR - Cloud Hosted Router

- CHR - system RouterOS, który jest dostosowany dla pracy w środowiskach wirtualnych
- Dostępne obrazy: VHDX, VMDK, VDI, RAW oraz OVA template
- Poziom licencji wskazują na prędkość interfejsów
- Licencja łatwo przenoszona pomiędzy instancjami maszyn wirtualnych, powiązana z kontem użytkownika w serwisie MikroTik
- Istnieje możliwość uzyskania licencji DEMO na czas 60 dni na dowolnym poziomie

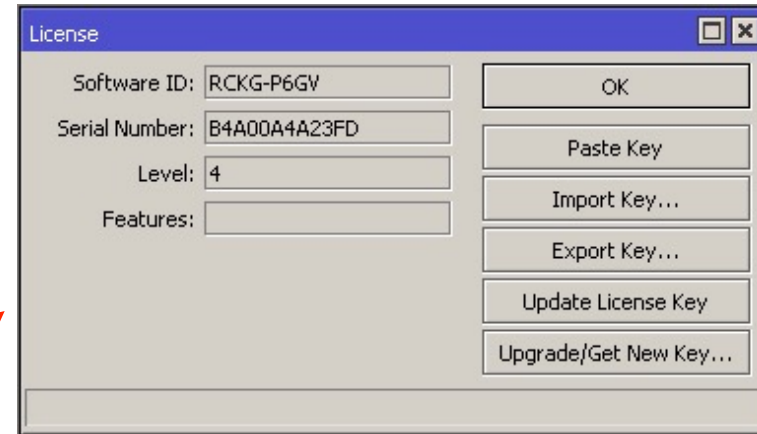
| Typ licencji | Ograniczenia | Cena, \$ |
|--------------|----------------|----------|
| Free | 1Mbit/s | darmowa |
| P1 | 1 Gbit/s | 45 |
| P10 | 10 Gbit/s | 95 |
| P-Unlimited | bez ograniczeń | 250 |

Licencja

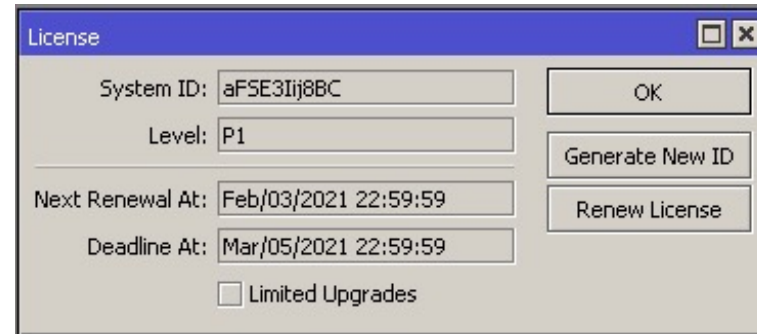
Sprawdzanie poziomu zainstalowanej licencji
w WinBox



Licencja L4 dla RouterBord-a



Licencja P1 dla CHR



/system license print

Hardware / Architektury

- **MIPSBE** (CRS1xx, CRS2xx, CRS312-4C+8XG, CRS326-24S+2Q+, CRS354, Cube Lite60, DISC, FiberBox, hAP, hAP ac, hAP ac lite, LDF, LHG, LHG Lite60, ItAP mini, mANTBox, mANTBox 2, mAP, NetBox, NetMetal, PowerBox, PWR-Line, QRT, RB9xx, SXTsq, cAP, hEX Lite, RB4xx, wAP, BaseBox, DynaDish, RB2011, SXT, OmniTik, Groove, Metal, Sextant, RB7xx, hEX PoE)
- **ARM64** (nRAY, CCR2004)
- **SMIPS** (hAP mini, hAP lite)
- **TILE** (CCR1xxx)
- **PPC** (RB3xx, RB600, RB8xx, RB1100AHx2, RB1100AH, RB1100, RB1200)
- **ARM** (cAP ac, CRS305-1G-4S+, CRS309-1G-8S+, CRS317-1G-16S+, CRS318, CRS326-24G-2S+, CRS328-24P-4S+, CRS328-4C-20S-4S+, Cube 60G ac, DISC AC, hAP ac², hAP ac³, LDF ac, LHG 60G, LHG ac, mANTBox 52, NetMetal ac², RB4011, SXTsq (ac series), wAP 60G series, Chateau, RB3011, RB1100AHx4, Audience, RB450Gx4)
- **X86** (RB230, X86)
- **MMIPS** (hEX (RB750Gr3), hEX S, RBMxx)

SwitchOS

- System operacyjny firmy MikroTik przeznaczony dla przełączników sieciowych
- Modele, który wspierają:
 - 260GS
 - 260GSP
 - 250GS
 - CSS326
 - CRS317
 - CSS106
- System znacząco różni się od RouterOS
- Zarządzanie przez stronę www, brak konsoli

Zarządzanie MikroTik

- **Telnet** – nieszyfrowane połączenie
- **SSH** – szyfrowane połączenie
- **WWW (WebFig)** – dowolna przeglądarka
- **WinBox (IP/MAC-WinBox)** - szyfrowane połączenie, klient MikroTik
- **Null Modem** – kabel konsolowy (port szeregowy)
- **MacTelnet** – z jednego MikroTik do innego
- **SNMP** – monitoring/zarządzanie
- **API** – biblioteki dla języków programowania (PHP, Python oraz inne)

CLI / Wiersz poleceń

```
beep --
caps-man --
certificate -- Certificate management
console --
delay -- does nothing for a while
disk --
do -- executes command
dude --
environment -- list of all variables
error -- make error value
execute -- run script as separate console job
file -- Local router file storage.
find -- Find items by value
for -- executes command for a range of integer values
foreach -- executes command for every element in a list
global -- set value global variable
if -- executes command if condition is true
import --
interface -- Interface configuration
ip -- IP options
ipv6 --
len -- return number of elements in value
local -- set value of local variable
log -- System logs
mpls --
nothing -- do nothing and return nothing
parse -- build command from text
password -- Change password
```

Dostępny w (WinBox, telnet, ssh, null modem)

- <tab> – podpowiada dostępne komendy
- <up> – przeszukiwanie historii komend
- <?> – wyświetla komendy z krótkim opisem

Telnet / SSH

```
1. Mikrotik (telnet)

MMM      MMM      KKK      TTTTTTTTTTTT      KKK
MMMM     MMMM     KKK      TTTTTTTTTTTT      KKK
MMM MMMM MMM III KKK KKK RRRRRR 000000 TTT III KKK KKK
MMM MM  MMM III KKKKK RRR RRR 000 000 TTT III KKKKK
MMM     MMM III KKK KKK RRRRRR 000 000 TTT III KKK KKK
MMM     MMM III KKK KKK RRR RRR 000000 TTT III KKK KKK

MikroTik RouterOS 6.45.1 (c) 1999-2019      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]       Completes the command/word. If the input is ambiguous,
            a second [Tab] gives possible options

/           Move up to base level
..         Move up one level
/command   Use command at the base level

[admin@MikroTik] > |
```

```
2. ssh

MMM      MMM      KKK      TTTTTTTTTTTT      KKK
MMMM     MMMM     KKK      TTTTTTTTTTTT      KKK
MMM MMMM MMM III KKK KKK RRRRRR 000000 TTT III KKK KKK
MMM MM  MMM III KKKKK RRR RRR 000 000 TTT III KKKKK
MMM     MMM III KKK KKK RRRRRR 000 000 TTT III KKK KKK
MMM     MMM III KKK KKK RRR RRR 000000 TTT III KKK KKK

MikroTik RouterOS 6.45.1 (c) 1999-2019      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]       Completes the command/word. If the input is ambiguous,
            a second [Tab] gives possible options

/           Move up to base level
..         Move up one level
/command   Use command at the base level

[admin@MikroTik] > |
```

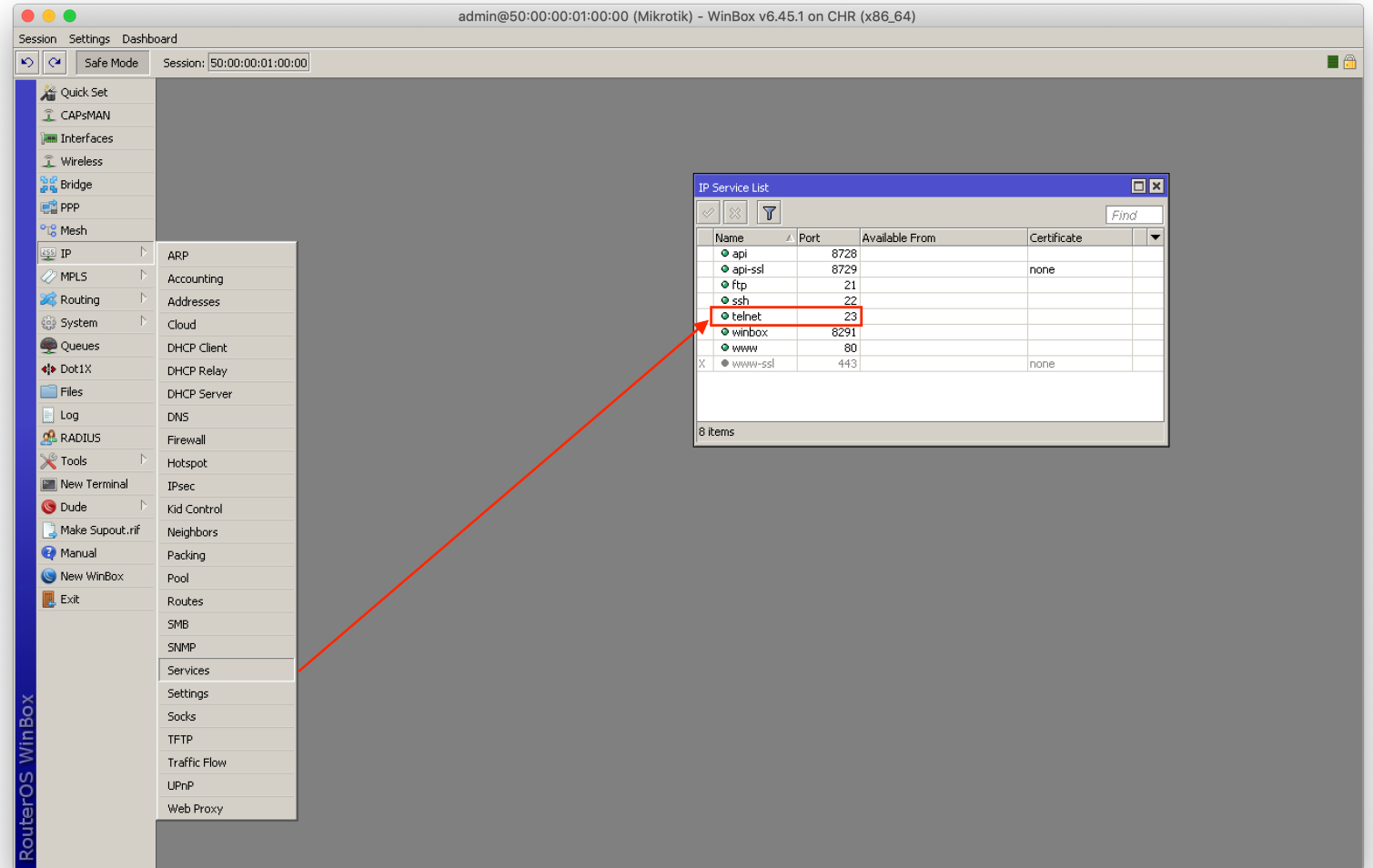
Telnet

włączenie/wyłączenie dostępu

Telnet (ang. *TELEtype NETwork*)— standard protokołu komunikacyjnego używanego w sieciach komputerowych do obsługi odległego terminala.

Protokół nie przewiduje stosowania szyfrowania ani sprawdzania poprawności danych. Dlatego jest podatny na wszelkiego rodzaju ataki, na które narażony jest protokół TCP.

Alternatywą dla telnet do zdalnego dostępu do systemu jest protokół sieciowy SSH. Główną przewagą SSH nad Telnet jest szyfrowane połączenie.



WWW

http://[adres.urzqdzienia]/webfig

RouterOS v6.45.1 (stable) Quick Set WebFig Terminal ? 📄

Interface Interface List Ethernet EoIP Tunnel IP Tunnel GRE Tunnel VLAN VRRP Bonding LTE Interface List

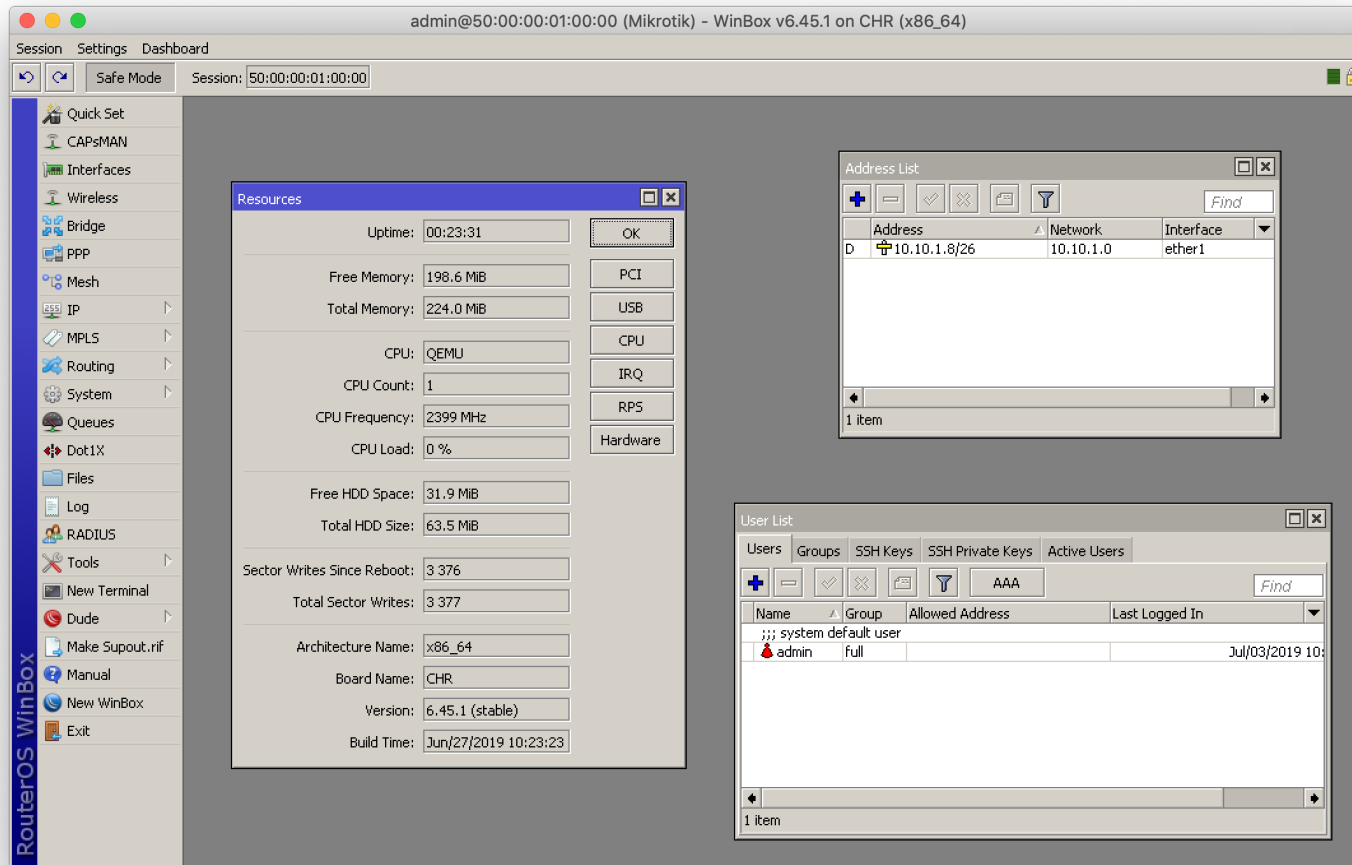
Add New Detect Internet

8 items

| | | Name | Type | Actual MTU | L2 MTU | Tx | Rx | Tx Packet (p/s) | Rx Packet (p/s) | FP Tx | FP Rx | FP Tx Packet (p/s) | FP Rx Packet (p/s) | | |
|---|----|-------------|-----------------------|-------------|--------|------------|-----------|-----------------|-----------------|------------|-----------|--------------------|--------------------|---|--|
| - | D | R | ↕ bridge-local | Bridge | 1500 | 1598 | 0 bps | 0 bps | 0 | 0 | 0 bps | 0 bps | 0 | 0 | |
| D | R | ⚡ ether1 | Ethernet | 1500 | 1598 | 125.8 kbps | 31.1 kbps | 25 | 26 | 121.2 kbps | 28.9 kbps | 24 | 25 | | |
| D | RS | ⚡ ether2 | Ethernet | 1500 | 1598 | 0 bps | 0 bps | 0 | 0 | 0 bps | 0 bps | 0 | 0 | | |
| D | S | ⚡ ether3 | Ethernet | 1500 | 1598 | 0 bps | 0 bps | 0 | 0 | 0 bps | 0 bps | 0 | 0 | | |
| D | | ⚡ pwr-line1 | PWR | 1500 | 1598 | 0 bps | 0 bps | 0 | 0 | 0 bps | 0 bps | 0 | 0 | | |
| - | D | R | ↔ sstp-cowo | SSTP Client | 1500 | | 14.1 kbps | 2.9 kbps | 3 | 4 | 0 bps | 0 bps | 0 | 0 | |
| - | D | R | ↔ sstp-frankfurt | SSTP Client | 1500 | | 0 bps | 0 bps | 0 | 0 | 0 bps | 0 bps | 0 | 0 | |
| D | S | 📶 wlan1 | Wireless (Atheros AR9 | 1500 | 1600 | 0 bps | 0 bps | 0 | 0 | 0 bps | 0 bps | 0 | 0 | | |

Tools Tools IPV6 Make Supout.rif Undo Redo Safe Mode WinBox Graphs End-User License

WinBox



WinBox- Najpopularniejsze narzędzie wykorzystywane do konfigurowania systemu RouterOS. Umożliwia m.in podgląd parametrów pracy urządzenia oraz dokonywanie modyfikacji konfiguracji. Pozwala na połączenie z routerem za pomocą adresu IP/DNS jak również adresu MAC (nie jest wymagane wcześniejsze skonfigurowanie adresu IP) Domyślnie wykorzystuje **protokół TCP, port 8291**. Połączenie jest szyfrowane.

The screenshot shows the 'IP Service List' window. It contains a table with the following data:

| Name | Port | Available From | Certificate |
|-----------|------|----------------|-------------|
| api | 8728 | | |
| api-ssl | 8729 | | none |
| ftp | 21 | | |
| ssh | 22 | | |
| telnet | 23 | | |
| winbox | 8291 | | |
| www | 80 | | |
| X www-ssl | 443 | | none |

8 items

Aplikację można pobrać ze strony
<https://mikrotik.com/download>

WinBox

połączenie

IP adres

MAC adres

WinBox v3.19 (Addresses)

Connect To: 10.10.1.8

Login: admin

Session: <own>

Note: Mikrotik

Group: [dropdown]

RoMON Agent: [dropdown]

Buttons: Add/Set, Connect To RoMON, Connect

Managed Neighbors

Refresh

| MAC Address | IP Address | Identity | Version | Board | Uptime |
|-------------------|------------|----------|-----------------|-------|--------------|
| 50:00:00:01:00:00 | 10.10.1.8 | Mikrotik | 6.45.1 (stable) | CHR | 13d 18:13:48 |

1 item

Automatyczne wykrywanie urządzeń MikroTik, znajdujących się w tym samym segmencie sieci co nasz komputer (MNDP)

WinBox v3.19 (Addresses)

Connect To: 50:00:00:01:00:00

Login: admin

Session: <own>

Note: Mikrotik

Group: [dropdown]

RoMON Agent: [dropdown]

Buttons: Add/Set, Connect To RoMON, Connect

Managed Neighbors

Refresh

| MAC Address | IP Address | Identity | Version | Board | Uptime |
|-------------------|------------|----------|-----------------|-------|--------------|
| 50:00:00:01:00:00 | 10.10.1.8 | Mikrotik | 6.45.1 (stable) | CHR | 13d 18:14:22 |

1 item

Aby podłączyć się do urządzenia z systemem RouterOS za pomocą aplikacji WinBox należy:

- podać adres IP (opcjonalnie numer portu po znaku ":" jeśli został zmieniony) urządzenia do którego chcemy się podłączyć lub gdy znajdujemy się w tym samym segmencie sieci (L2), możemy połączyć się bez podawania adresu IP dzięki protokołowi MAC-WinBox wskazując adres MAC
- podać poprawną nazwę użytkownika oraz hasło (domyślnie użytkownik: admin, hasło: nie jest ustawione)

Null Modem

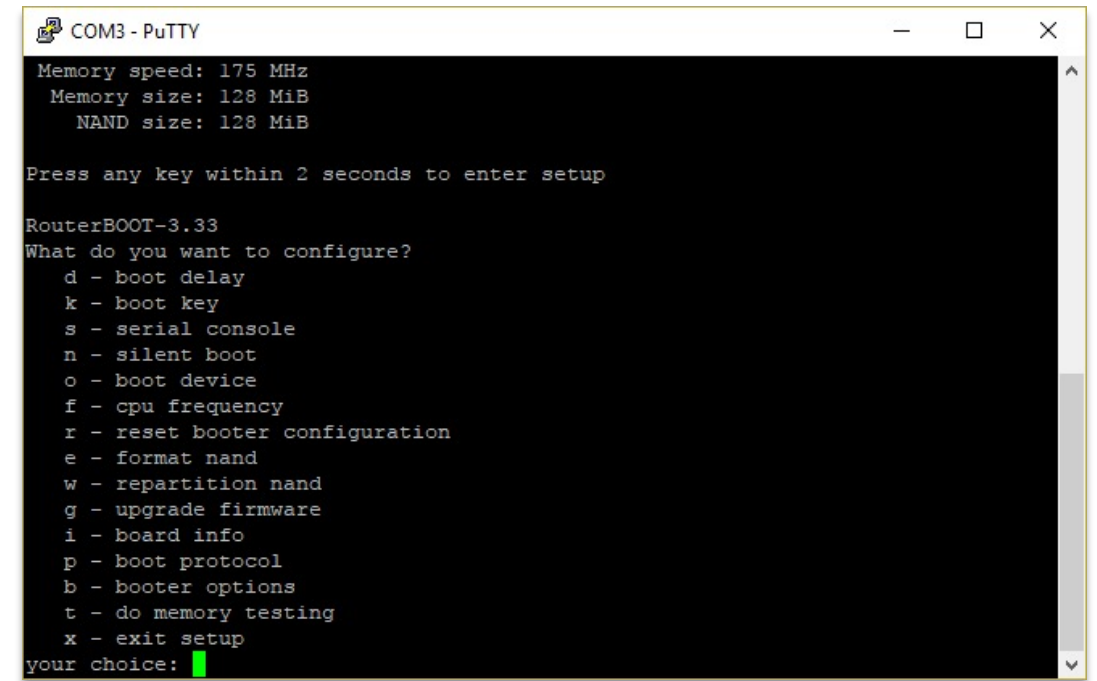
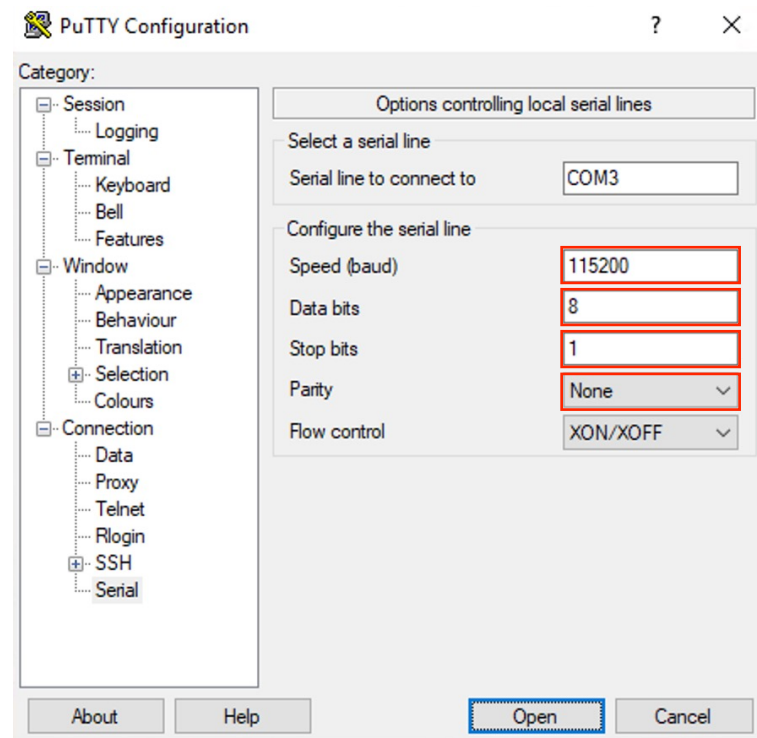
Parametry połączenia:

Baud rate: *115200 bit/s*

Data bits: *8*

Stop bits: *1*

Parity: *none*



Domyślna konfiguracja

- Każde zakupione urządzenie posiada konfigurację domyślną
Konfigurację domyślną można nadpisać
Konfigurację domyślną można usunąć
- Aby przywrócić konfigurację domyślną wydajemy polecenie:
/system reset-configuration

lub

za pomocą **przycisku reset**, znajdującego się na obudowie urządzenia
(*przycisk należy wcisnąć przed włączeniem urządzenia do zasilania,
włączyć zasilanie, po upływie 5 sekund należy zwolnić przycisk*)

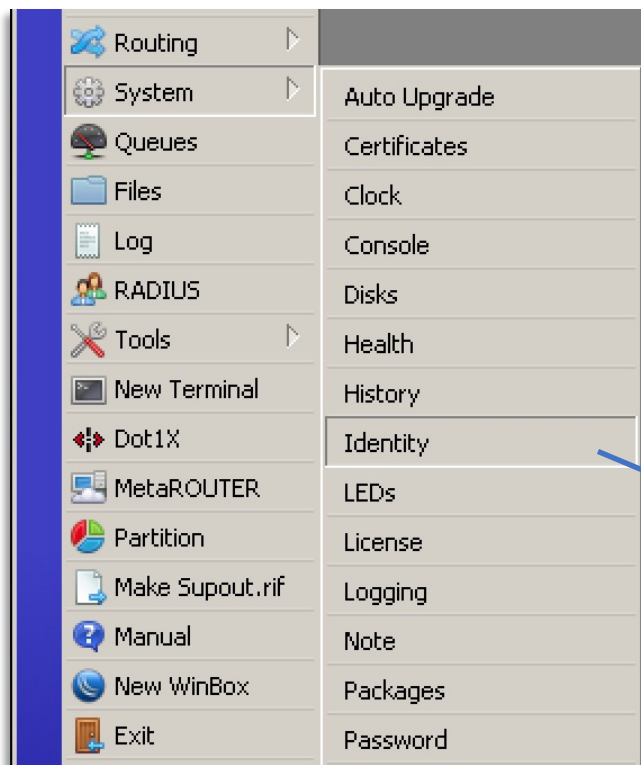


```
[devuser@Audience-dom] > system default-configuration print
script: # | Welcome to RouterOS!
# | 1) Set a strong router password in the System > Users menu
# | 2) Upgrade the software in the System > Packages menu
# | 3) Enable firewall on untrusted networks
# | 4) Set your country name to observe wireless regulations
# | -----
# | RouterMode:
# | * WAN port is protected by firewall and enabled DHCP client
# | * Wireless and Ethernet interfaces (except WAN port/s)
# |   are part of LAN bridge
# | WPS Sync:
# | mode:          ap-bridge;
# | wpa2:          yes;
# | channel width: 20/40mhz-XX;
```

Podstawowe ustawienia

identity

Warto ustawić go w sposób przemyślany, np. określając lokalizację urządzenia, jego funkcję, model.

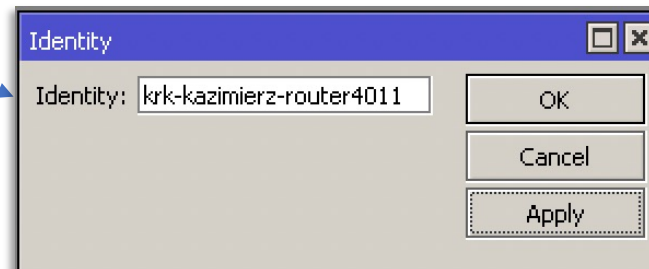


Przykłady nazw:

krk-kazimierz-router4011

waw-ogrodowa-sw1

dc1-switch-sw2-crs



Lub z linii poleceń: ***/system identity set name=krk-kazimierz-router4011***

Podstawowe ustawienia

Nadanie adresu IP

The image illustrates the process of assigning an IP address in Mikrotik WinBox. It shows three windows:

- Left Pane:** A tree view of the configuration menu. The 'Addresses' option under the 'Routing' category is highlighted with a red arrow.
- Address List Window:** A table showing the current IP address assignments. It has columns for 'Address', 'Network', and 'Interface'. One entry is visible: '192.168.176.4/24' assigned to 'ether1'. A red arrow points from the 'Addresses' menu item to this window.
- Address Configuration Dialog:** A dialog box for editing an IP address. The title is 'Address <172.16.5.254/24>'. It contains fields for 'Address' (172.16.5.254/24), 'Network' (a dropdown menu), and 'Interface' (ether2). There are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove'. A status bar at the bottom indicates 'enabled'. A red arrow points from the 'Address List' window to this dialog.

Adres IP nadajemy razem z **maską sieci**. Adres IP możemy nadawać zarówno jak na interfejsach fizycznych:

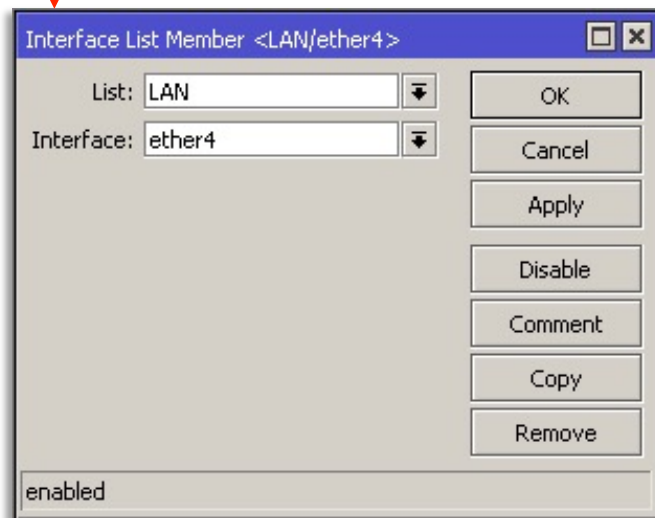
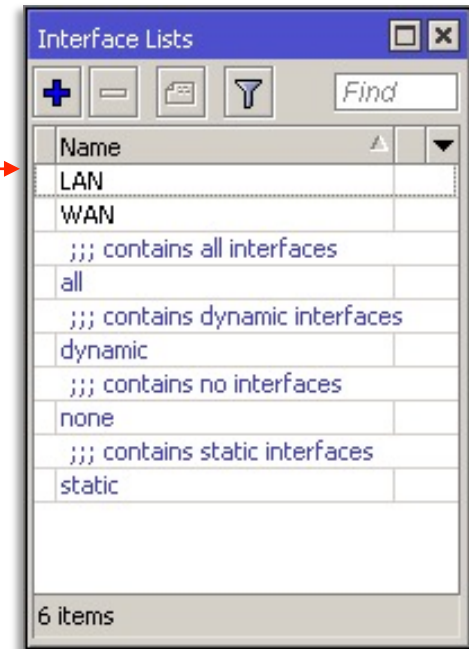
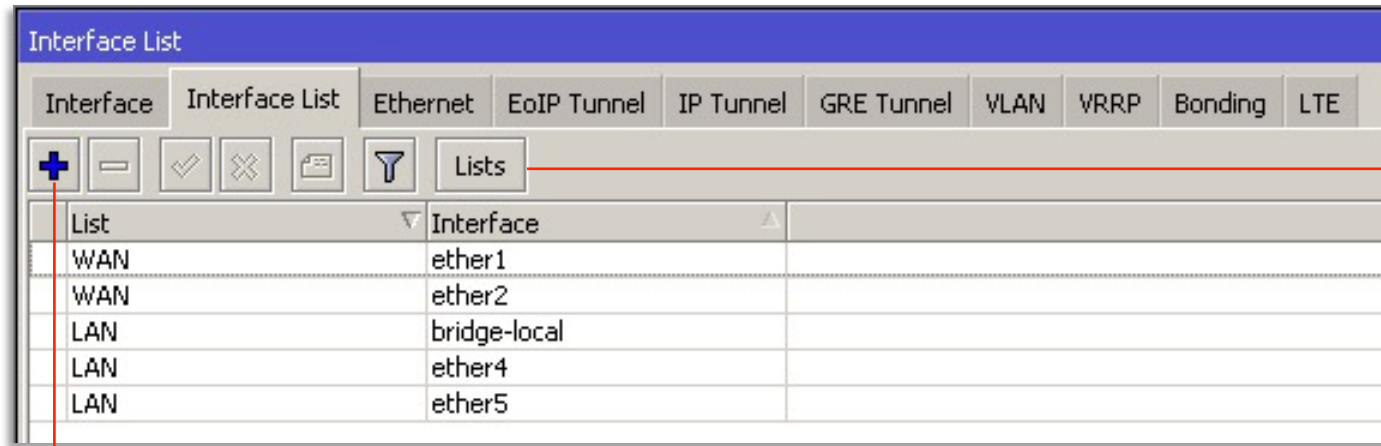
- ether1, ether2, wlan1, wlan2

tak i na logicznych:

- ipip, vlan, bridge

Podstawowe ustawienia

Interface list

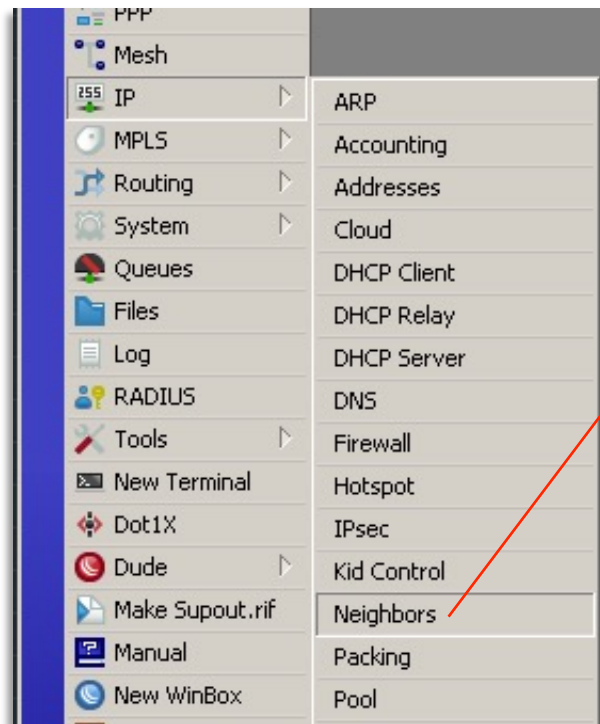


- Lista interfejsów umożliwia łatwe grupowanie interfejsów
- Listę interfejsów możemy wykorzystać m.in.: tworząc reguły firewalla, konfigurując MAC-Winbox, zakres działania protokołu MNDP

Podstawowe ustawienia

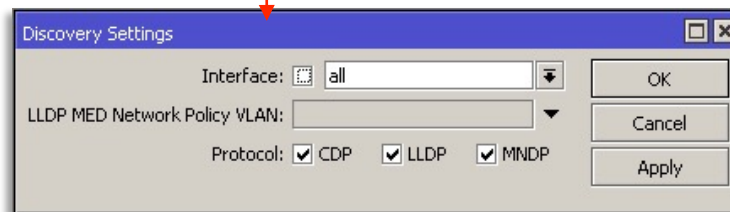
MikroTik Neighbor Discovery protocol

Protokół umożliwia wykrywanie urządzeń znajdujących się w tej samej domenie rozgłoszeniowej (broadcast domain)



Znalezione urządzenia

| Interface | IP Address | MAC Address | Identity | Platform | Version | Board Name | IPv6 | Age (s) | Uptime |
|---------------|--------------|-------------------|-------------|----------|-----------------|-------------------|------|---------|---------------|
| ether1 | | C4:AD:34:B8:B3:7D | MikroTik | MikroTik | 6.47.8 (stable) | RB2011UIAS-2HnD | no | 25 | 39d 19:48:29 |
| ether3 | | 74:4D:28:B4:D6:F3 | AP-osp | MikroTik | 6.48 (stable) | RBD52G-5HacD2HnD | no | 44 | 12d 20:34:33 |
| ether4 | | C4:AD:34:08:E2:2F | AP-conf | MikroTik | 6.48 (stable) | RBD52G-5HacD2HnD | no | 33 | 12d 20:34:29 |
| ether5 | | C4:AD:34:6E:49:24 | WAP-AC-LTE6 | MikroTik | 6.48 (stable) | RBwAPGR-5HacD2HnD | no | 33 | 12d 20:19:32 |
| ether5 | | CC:2D:ED:1C:78:B9 | SW-1 | MikroTik | 6.48 (stable) | RB960PGS | no | 11 | 12d 20:35:20 |
| ether5 | | 48:8F:5A:9B:09:38 | hAP-AC2 | MikroTik | 6.48 (stable) | RBD52G-5HacD2HnD | no | 28 | 5d 02:10:28 |
| ether5 | | C4:AD:34:78:D6:5C | MikroTik | MikroTik | 6.48 (stable) | RBmAPL-2nD | no | 34 | 23:14:15 |
| sloneczko | 10.10.87.250 | 00:00:00:00:00:00 | rtr-ng | MikroTik | 6.42.1 (stable) | CCR1036-8G-25+ | no | 25 | 381d 03:59:17 |
| vlan-150-mgmt | 172.16.254.2 | CC:2D:ED:1C:78:B9 | SW-1 | MikroTik | 6.48 (stable) | RB960PGS | no | 11 | 12d 20:35:20 |
| vlan-150-mgmt | 172.16.254.3 | 74:4D:28:B4:D6:F3 | AP-osp | MikroTik | 6.48 (stable) | RBD52G-5HacD2HnD | no | 44 | 12d 20:34:33 |
| vlan-150-mgmt | 172.16.254.4 | C4:AD:34:08:E2:2F | AP-conf | MikroTik | 6.48 (stable) | RBD52G-5HacD2HnD | no | 33 | 12d 20:34:29 |
| vlan-150-mgmt | 172.16.254.6 | C4:AD:34:6E:49:24 | WAP-AC-LTE6 | MikroTik | 6.48 (stable) | RBwAPGR-5HacD2HnD | no | 33 | 12d 20:19:32 |
| vlan-199-crew | 10.10.1.10 | 90:9C:4A:BA:F1:C7 | | | | | no | 60 | 00:00:00 |
| vlan-1000-lte | 10.200.200.2 | C4:AD:34:6E:49:24 | WAP-AC-LTE6 | MikroTik | 6.48 (stable) | RBwAPGR-5HacD2HnD | no | 33 | 12d 20:19:32 |



Interface-y na których działa mechanizm wykrywania (MNDP). W tym miejscu podajemy listę interface-ów, a nie pojedyncze interface-y. Aby włączyć wykrywanie na pojedynczym interfejsie musimy go uprzednio dodać do odpowiedniej listy.

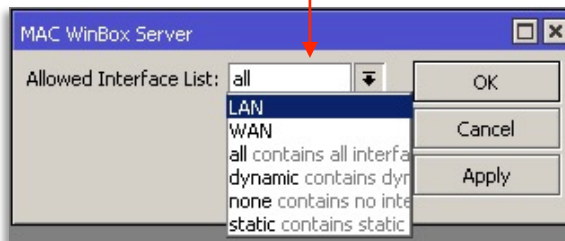
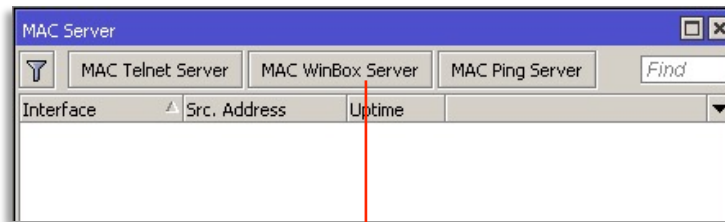
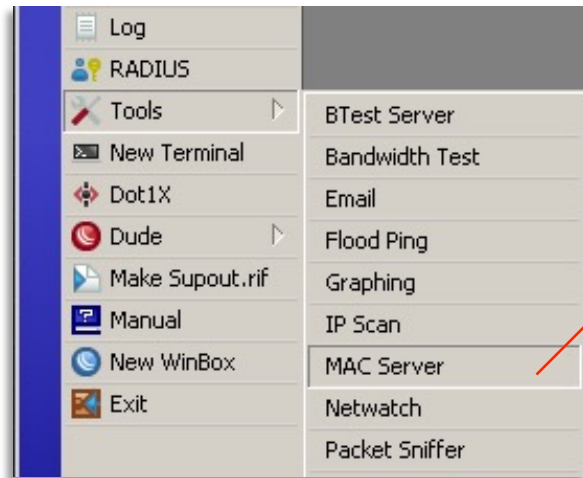
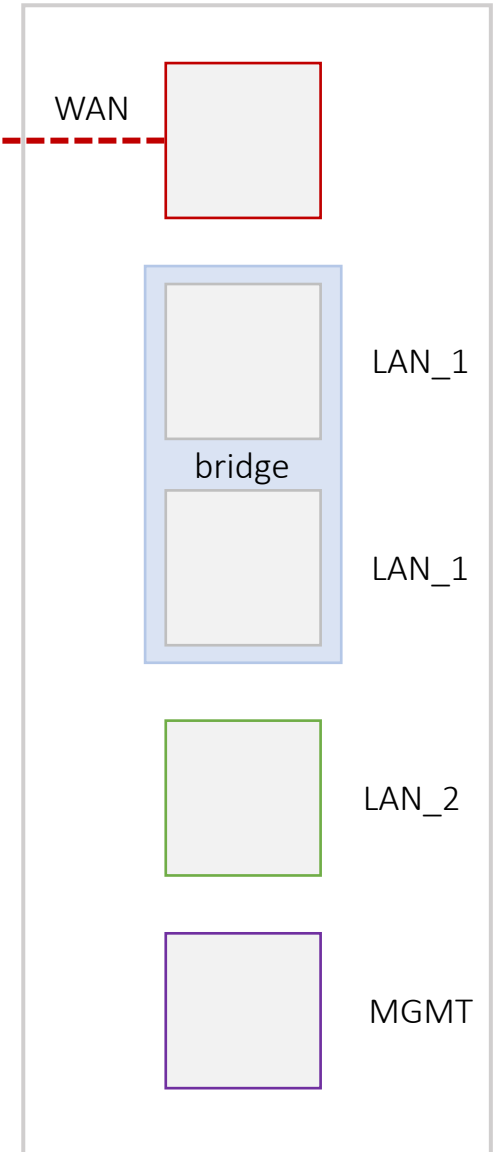
Aktywowanie działania protokołu na danym interfejsie nie umożliwia nam znalezienie innych urządzeń ale również sprawia, iż my sami jesteśmy wykrywani !!!

Podstawowe ustawienia

MAC-WinBox, MAC-Telnet



Dostęp do urządzenia z wykorzystaniem jego adresu **MAC**, nie potrzebujemy posiadać adresu IP, dostęp możliwy jedynie w ramach tej samej domeny rozgłoszeniowej, dalej konieczne jest podanie prawidłowego loginu i hasła. Dla schematu powyżej ustawimy dostęp do urządzenia, z wykorzystaniem **MAC WinBox Server** tylko dla połączeń z interfejsu ether należącego do grupy **MGMT**.



Podstawowe ustawienia

Konta użytkowników systemu

The image shows the Mikrotik WinBox configuration interface. On the left is a sidebar menu with categories like System, Queues, Files, Log, Radius, Tools, and Ext. The main area displays a list of system settings, with 'Users' selected. A red arrow points from 'Users' in the sidebar to the 'Users' tab in the 'User List' window. Another red arrow points from the 'admin' user entry in the 'User List' to the 'New User' dialog box.

The 'New User' dialog box contains the following fields:

- Name:
- Group:
- Allowed Address:
-
- Last Logged In:
- Password:
- Confirm Password:
- enabled:

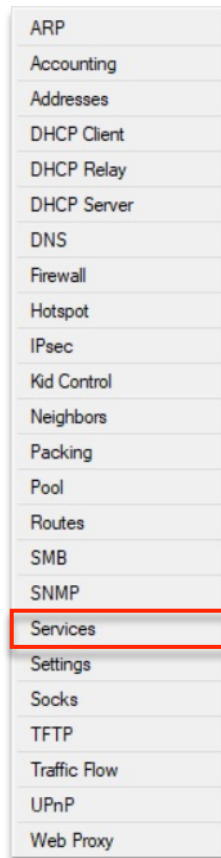
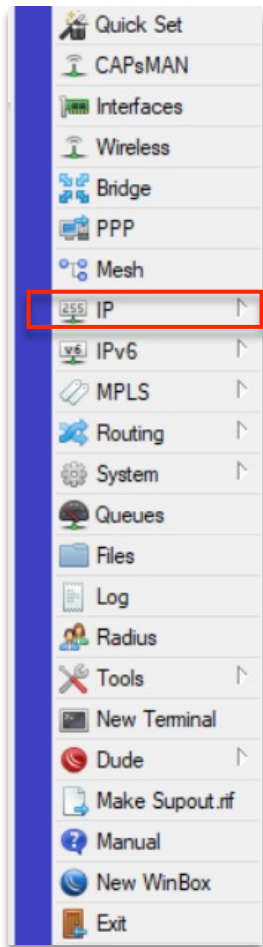
The 'User List' window shows a table with the following data:

| Name | Group | Allowed Address | Last Logged In |
|---------------------|-------|-----------------|----------------------|
| system default user | | | |
| admin | full | | Sep/20/2017 12:44:01 |

Można ograniczyć możliwość logowania się użytkownika z adresów innych niż wskazane **Allowed Address**

Podstawowe ustawienia

ograniczenie dostępu do urządzenia



A screenshot of the IP Service List window. The window title is 'IP Service List'. It contains a table with columns: Name, Port, Available From, and Certificate. The table lists several services, with the ports for 'ssh' and 'winbox' highlighted in red boxes.

| | Name | Port | Available From | Certificate |
|---|---------|------|----------------|-------------|
| X | api | 8728 | | |
| X | api-ssl | 8729 | | none |
| X | ftp | 21 | | |
| | ssh | 3089 | | |
| X | telnet | 23 | | |
| | winbox | 1043 | | |
| X | www | 80 | | |
| X | www-ssl | 443 | | none |

8 items

Możemy rozważyć zmianę portów na jakich pracują usługi:

- SSH zamiast 22 na 3089 (dla przykładu)
- WinBox zamiast 8291 na 1043

Ewentualnie wskazanie z jakich adresów IP usługa będzie dostępna (Available From)

Dostęp z zewnątrz do routera (internet)

z konkretnych adresów IP

próba
logowania
→

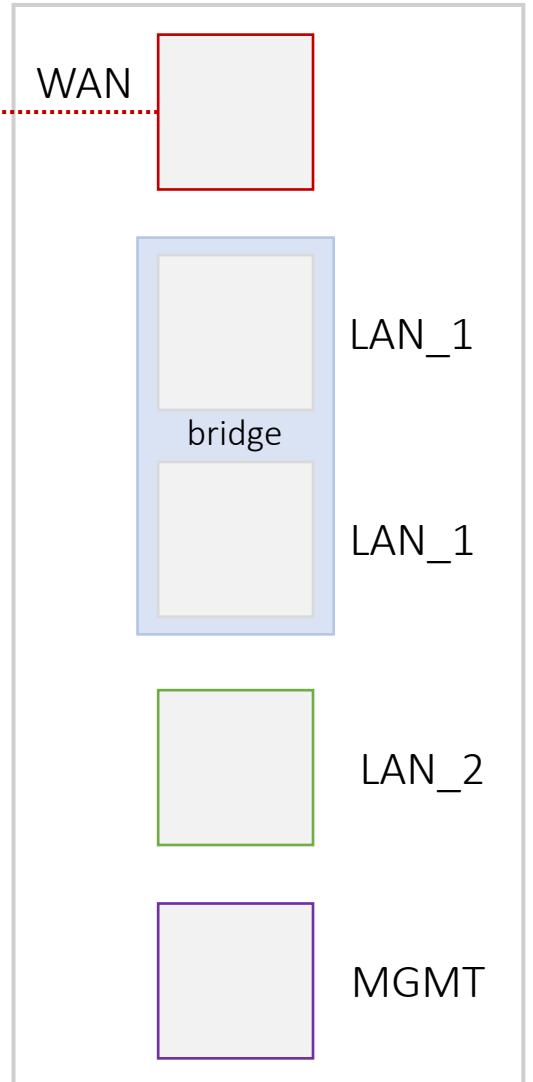
/ip firewall filter

/ip services

/users

| Name | Port | Available From | Certificate |
|-----------|------|------------------------------|-------------|
| X api | 8728 | | |
| X api-ssl | 8729 | | none |
| X ftp | 21 | | |
| X ssh | 22 | | |
| X telnet | 23 | | |
| winbox | 8291 | 45.32.154.212, 45.32.154.100 | |
| X www | 80 | | |
| X www-ssl | 443 | | none |

| Name | Group | Allowed Address | Last Logged In |
|-------------------------|-------|------------------------------|----------------|
| ... system default user | | | |
| admin | full | 45.32.154.212, 45.32.154.100 | |
| michal | full | 45.32.154.212, 45.32.154.100 | |



```
/ip firewall filter add chain=input comment="Accept Established, Related"  
connection-state=established,related action=accept  
/ip firewall filter add chain=input src-address=45.32.154.212 action=accept  
/ip firewall filter add chain=input src-address=45.32.154.100 action=accept  
/ip firewall filter add chain=input action=drop
```

Podstawowe ustawienia

ograniczenie dostępu do urządzenia

```
/tool bandwidth-server set enabled=no
```

```
/ip dns set allow-remote-requests=no
```

```
/ip socks set enabled=no
```

```
/ip upnp set enable=no
```

```
/ip cloud set ddns-enable=no update-time=no
```

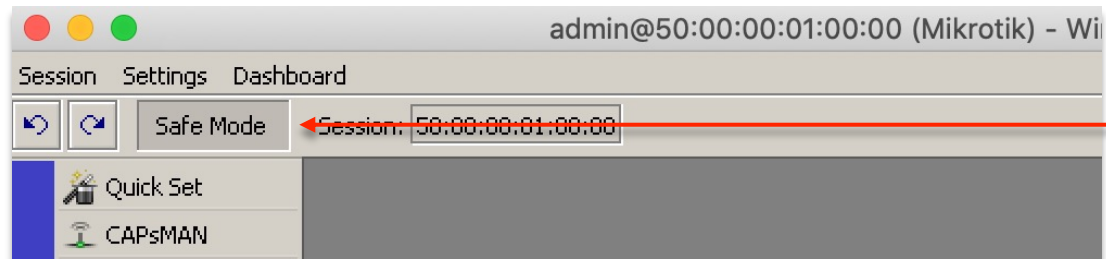
```
/lcd set enabled=no
```

```
/ip proxy set enabled=no
```

Podstawowe ustawienia

Safe Mode

Domyślnie każda wprowadzona przez nas zmiana konfiguracji zostaje zapisana w nieulotnej pamięci NAND naszego urządzenia. W przypadku popełnienia błędu w konfiguracji reguł firewall-a, routingu, itp., możemy utracić dostęp do naszego urządzenia i konieczna będzie wizyta na miejscu, a w ostateczności przywrócenie ustawień domyślnych. Aby ustrzec się przed utratą dostępu do urządzenia zalecane jest stosowanie trybu **Safe Mode**.



Przed przystąpieniem do pracy z konfiguracją urządzenia należy wcisnąć przycisk **Safe Mode**. W tym momencie w przypadku gdy nasza sesja z WinBox-em zostanie zerwana, wszystkie zmiany wprowadzone przez nas zostaną odwrócone. Należy pamiętać, aby po skończonej pracy, ponownie odznaczyć przycisk **Safe Mode** aby nasze zmiany zostały zapisane na stałe.

```
[admin@Mikrotik] >  
[Safe Mode taken] ←  
[admin@Mikrotik] <SAFE> system identity set name=Mikrotik  
[Safe Mode released]  
[admin@Mikrotik] >
```

Aby aktywować tryb **Safe Mode** w trybie CLI wciskamy *CTRL-x*, aby opuścić tryb **Safe Mode** ponownie wciskamy *CTRL-x*

UPGRADE

Software / Firmware

Software- oprogramowanie RouterOS wydawane jest stosunkowo często, zawiera poprawki dotyczące wydajności, nowych funkcjonalności oraz ewentualnych błędów wykrytych we wcześniejszych wersjach oprogramowania. Istnieją trzy gałęzie oprogramowania:

- **Long-term** – najbardziej stabilna wersja oprogramowania, pozbawiona nowych funkcjonalności
- **Stable** – zawiera poprawki z gałęzi **Long-term**, oraz dodatkowo nowe funkcjonalności
- **Testing** – wersja testowa, posiadająca najnowszy kod, uznawana za mało stabilną

Firmware zawiera poprawki dla sterowników, np. dodano obsługę nowych wkładek SFP, poprawiono sterownik do modułu radiowego.

UPGRADE oprogramowania

Software

The image shows two overlapping Mikrotik WinBox windows. The background window is WinBox v3.18 (Addresses), and the foreground window is WinBox v6.45.1 on CHR (x86_64). The foreground window displays a table with the following data:

| MAC Address | IP Address | Identity | Version | Board | Uptime |
|-------------------|------------|----------|-----------------|-------|--------|
| 50:00:00:01:00:00 | 10.10.1.8 | Mikrotik | 6.45.1 (stable) | CHR | 0 |

Two red arrows point from the text below to the 'Version' column of the table in the foreground window.

Informacja o aktualnie zainstalowanej wersji oprogramowania

UPGRADE oprogramowania

Software

Proces upgrade-u możemy wykonać na kilka sposobów:

- Wgranie pliku (drag & drop WinBox lub ftp, a następnie ponowne uruchomienie urządzenia)
- NetInstall
- Auto Upgrade
- CAPsMAN
- The DUDE
- Packages -> Check for Updates -> Download & Install

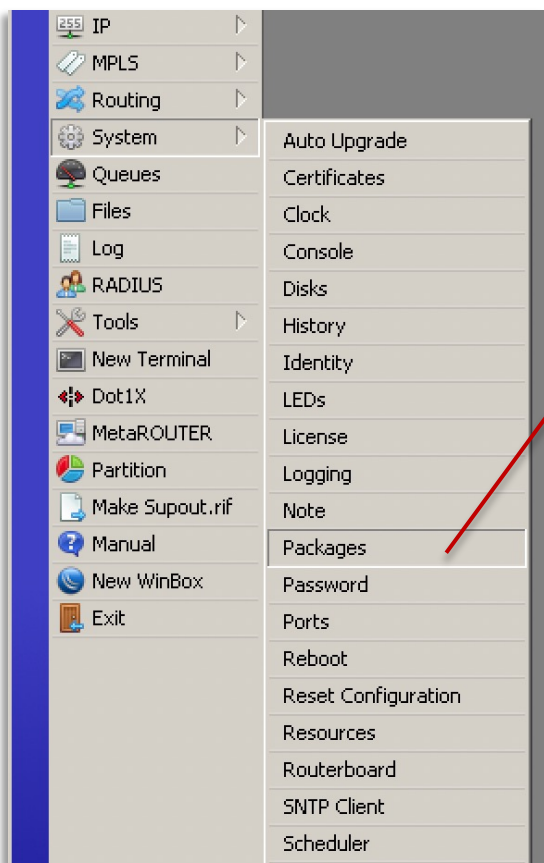
Uwaga: w przypadku ręcznego upgrade-u należy pobrać ze strony <https://mikrotik.com/download> paczkę z rozszerzeniem npk dla architektury zgodnej z posiadanyim urządzeniem

UPGRADE oprogramowania

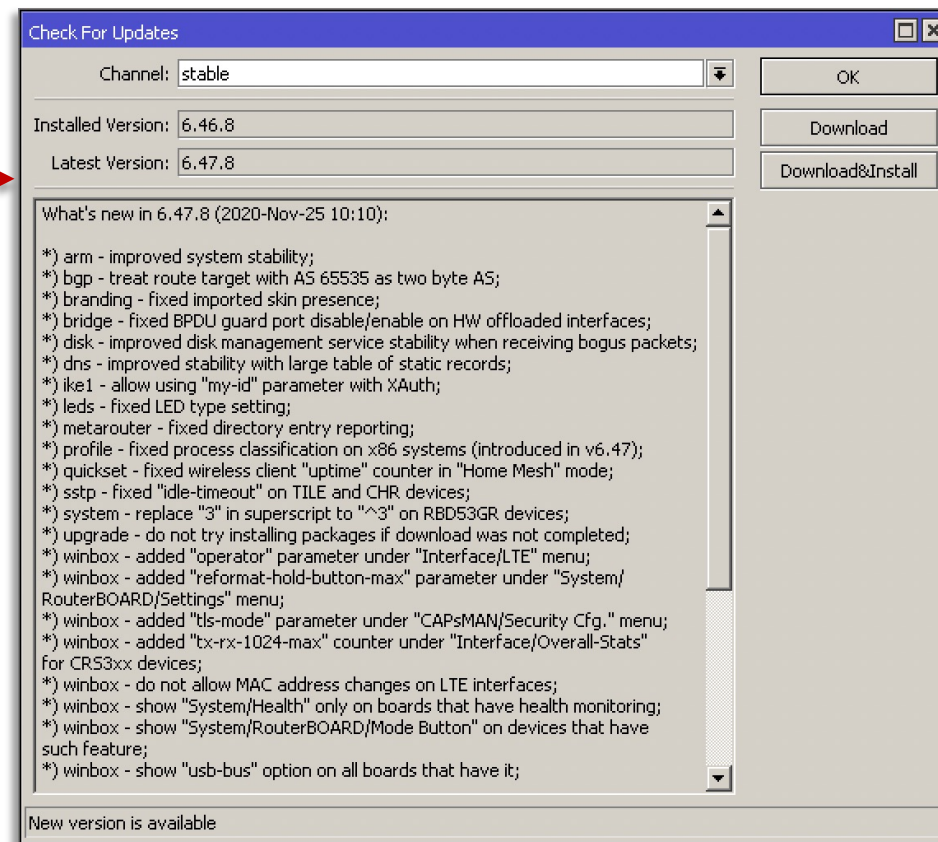
Software

Metoda 1

Packages -> Check for Updates -> Download & Install



| Name | Version | Build Time | Scheduled |
|-----------------|---------|----------------------|-----------|
| routeros-mipsbe | 6.46.8 | Oct/29/2020 08:29:55 | |
| advanced-tools | 6.46.8 | Oct/29/2020 08:29:55 | |
| dhcp | 6.46.8 | Oct/29/2020 08:29:55 | |
| hotspot | 6.46.8 | Oct/29/2020 08:29:55 | |
| ipv6 | 6.46.8 | Oct/29/2020 08:29:55 | |
| mpls | 6.46.8 | Oct/29/2020 08:29:55 | |
| ppp | 6.46.8 | Oct/29/2020 08:29:55 | |
| routing | 6.46.8 | Oct/29/2020 08:29:55 | |
| security | 6.46.8 | Oct/29/2020 08:29:55 | |
| system | 6.46.8 | Oct/29/2020 08:29:55 | |
| wireless | 6.46.8 | Oct/29/2020 08:29:55 | |











UPGRADE oprogramowania

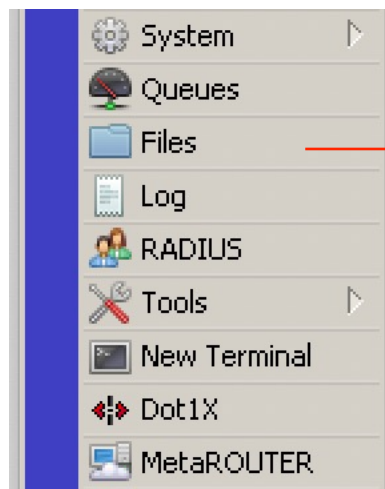
Software

Metoda 2

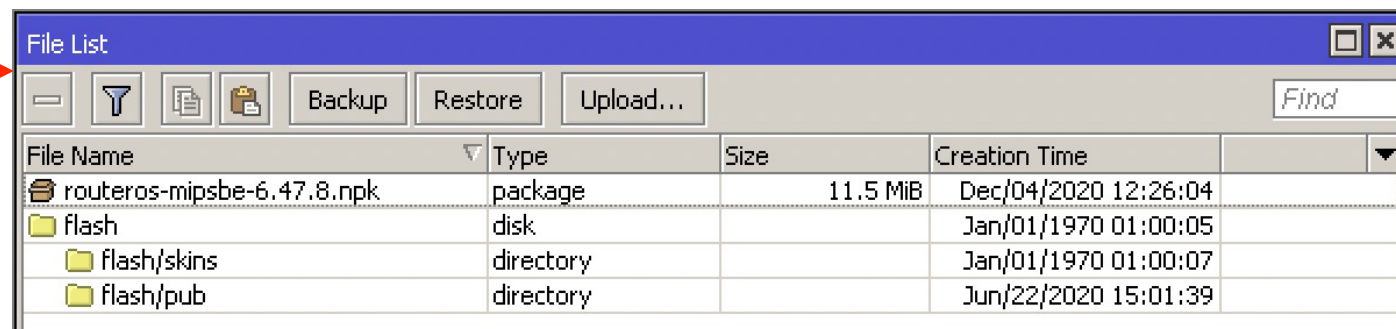
Pobieramy software ze strony <https://mikrotik.com/download> plik .npk

Koniecznienie zgodny z naszą architekturą sprzętową !!!

| | 6.46.8 (Long-term) | 6.47.8 (Stable) | 6.48beta58 (Testing) | 7.1beta3 (Development) |
|-----------------------|---|---|---|---|
| MIPSBE | CRS1xx, CRS2xx, CRS312-4C+8XG, CRS326-24S+2Q+, CRS354, Cube Lite60, DISC, FiberBox, hAP, hAP ac, hAP ac lite, LDF, LHG, LHG Lite60, ItAP mini, mANTBox, mANTBox 2, mAP, NetBox, NetMetal, PowerBox, PWR-Line, QRT, RB9xx, SXTsq, cAP, hEX Lite, RB4xx, wAP, BaseBox, DynaDish, RB2011, SXT, OmniTik, Groove, Metal, Sextant, RB7xx, hEX PoE | | | |
| Main package |  |  |  |  |
| Extra packages |  |  |  |  |



Plik zapisujemy do głównego katalogu



The 'File List' window displays a table of files and directories. The file 'routeros-mipsbe-6.47.8.npk' is listed as a package file, 11.5 MiB in size, created on Dec/04/2020 at 12:26:04. Below it are three directories: 'flash', 'flash/skins', and 'flash/pub'.

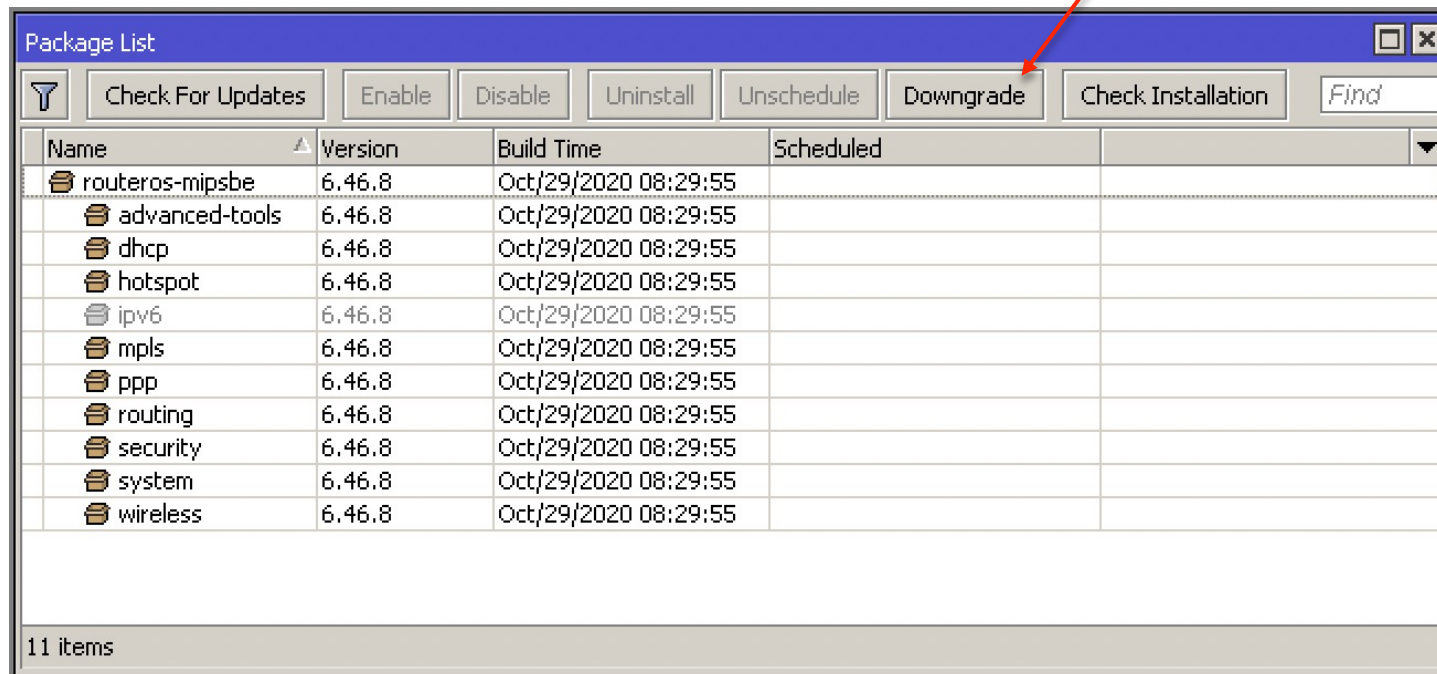
| File Name | Type | Size | Creation Time |
|----------------------------|-----------|----------|----------------------|
| routeros-mipsbe-6.47.8.npk | package | 11.5 MiB | Dec/04/2020 12:26:04 |
| flash | disk | | Jan/01/1970 01:00:05 |
| flash/skins | directory | | Jan/01/1970 01:00:07 |
| flash/pub | directory | | Jun/22/2020 15:01:39 |

DOWNGRADE oprogramowania

Software

Aby powrócić do starszej wersji oprogramowania RouterOS :

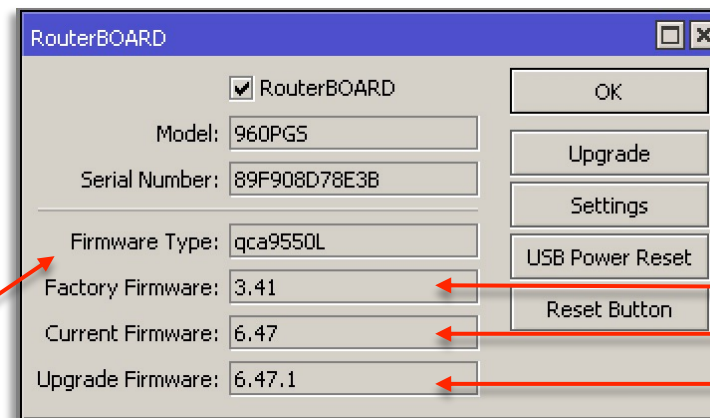
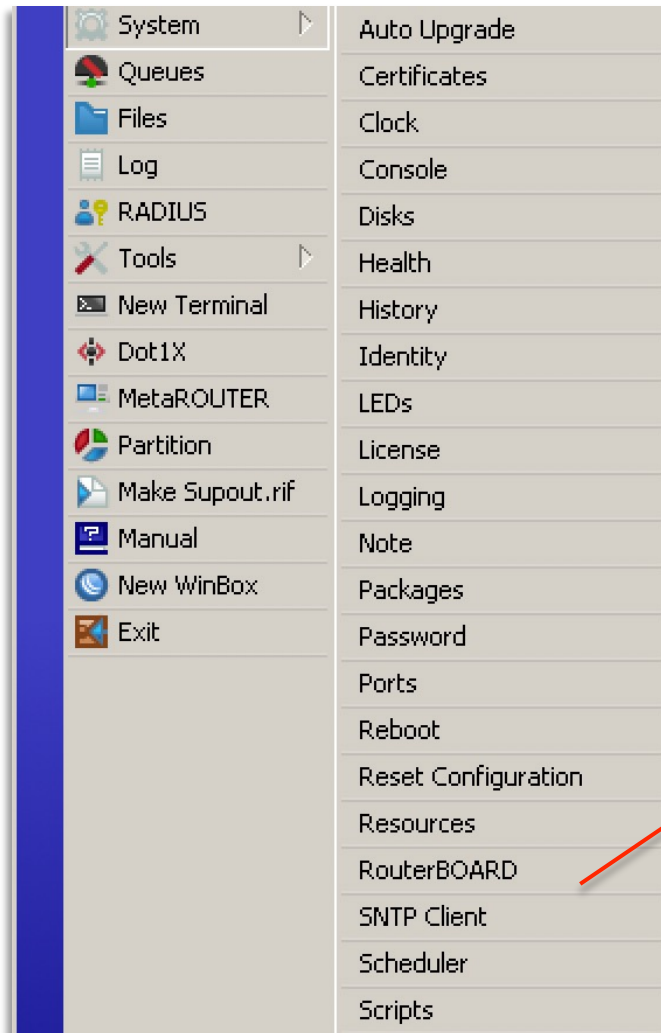
- należy pobrać software ze strony: <https://mikrotik.com/download/archive>
- umieścić plik w głównym katalogu **Files**
- następnie w zakładce */system package* wybrać opcję **Downgrade**



UPGRADE oprogramowania

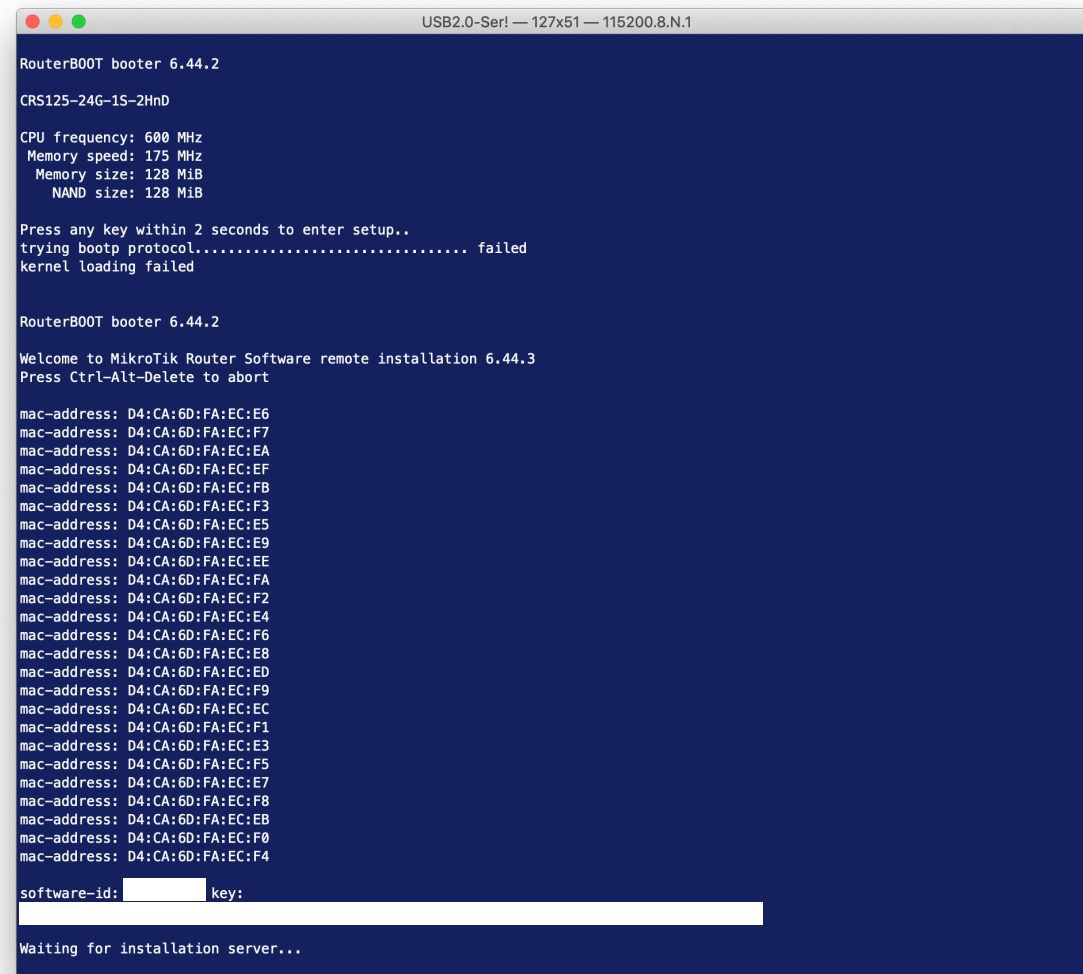
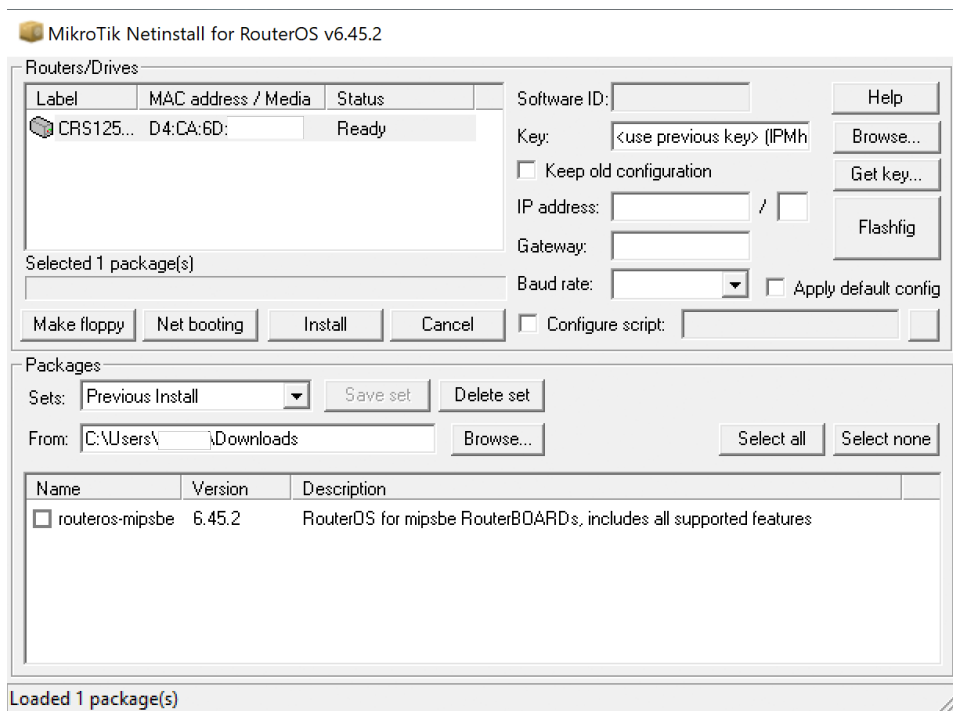
Firmware

Sprawdzamy jaką wersję Firmware aktualnie posiadamy



fabryczne
aktualne
najnowsze

NetInstall

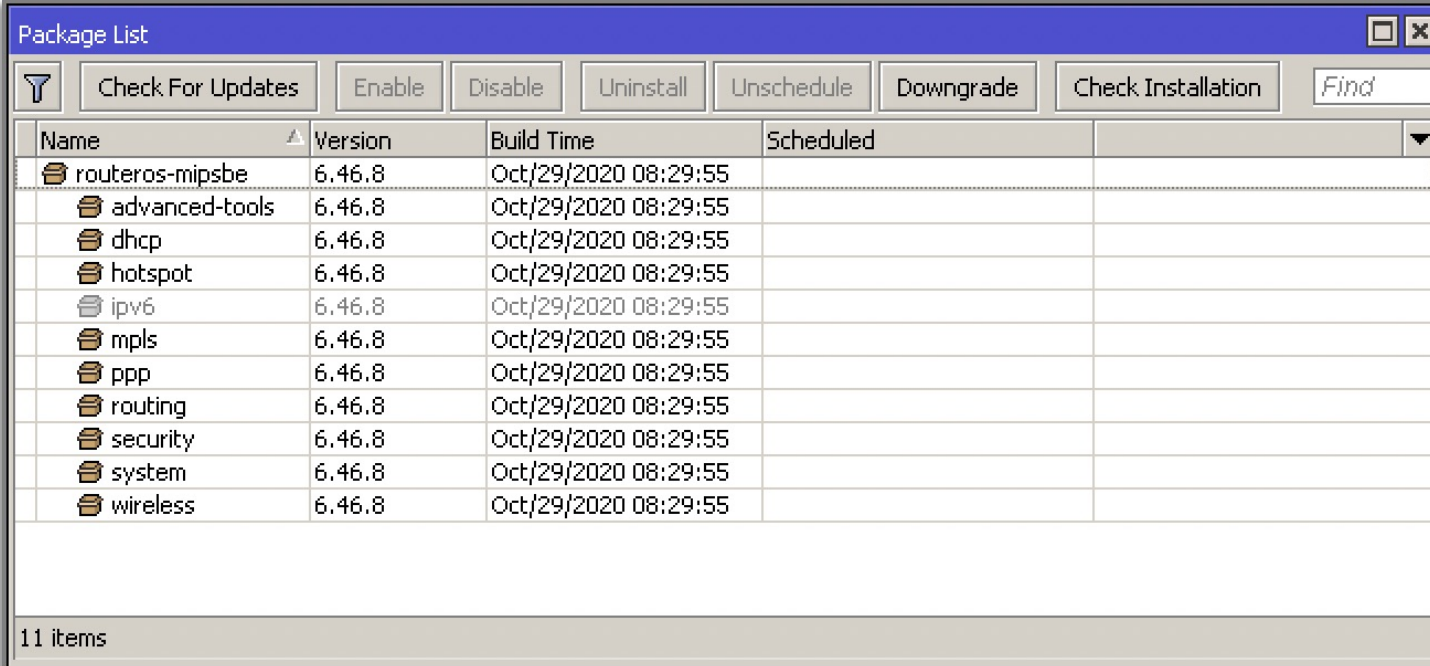


- Narzędzie NetInstall pozwala na instalację oprogramowania RouterOS, gdy to uległo uszkodzeniu.
- Wykorzystuje **BOOTP**
- Należy połączyć PC z MikroTik do **ether1**
- **NIE JEST MOŻLIWY** reset hasła użytkownika RouterOS za pomocą NetInstall bez utraty konfiguracji

Software

Paczki (moduły)

Funkcjonalności systemu RouterOS zostały podzielone na paczki (moduły), część z nich dostarczana jest z podstawową wersją systemu **Main Package**, pozostałe można zainstalować dodatkowo ze zbioru **Extra packages**



The screenshot shows a window titled "Package List" with a toolbar containing buttons for "Check For Updates", "Enable", "Disable", "Uninstall", "Unschedule", "Downgrade", "Check Installation", and a "Find" search box. Below the toolbar is a table with the following data:

| Name | Version | Build Time | Scheduled |
|-----------------|---------|----------------------|-----------|
| routeros-mipsbe | 6.46.8 | Oct/29/2020 08:29:55 | |
| advanced-tools | 6.46.8 | Oct/29/2020 08:29:55 | |
| dhcp | 6.46.8 | Oct/29/2020 08:29:55 | |
| hotspot | 6.46.8 | Oct/29/2020 08:29:55 | |
| ipv6 | 6.46.8 | Oct/29/2020 08:29:55 | |
| mpls | 6.46.8 | Oct/29/2020 08:29:55 | |
| ppp | 6.46.8 | Oct/29/2020 08:29:55 | |
| routing | 6.46.8 | Oct/29/2020 08:29:55 | |
| security | 6.46.8 | Oct/29/2020 08:29:55 | |
| system | 6.46.8 | Oct/29/2020 08:29:55 | |
| wireless | 6.46.8 | Oct/29/2020 08:29:55 | |

At the bottom of the window, it indicates "11 items".

Zestaw modułów podstawowych **Main package**

Software

Paczki (moduły)

Funkcjonalności dostarczone przez paczki:

- **advanced-tools** – narzędzie ping (flood-ping, ping-speed), Netwatch, ip-scan, SMS tool, Wake-on-LAN
- **calea** – narzędzie do gromadzenia danych do specjalnego użytku zgodnie z "Communications Assistance for Law Enforcement Act" w USA
- **dhcp** – Dynamic Host Control Protocol klient oraz serwer
- **hotspot** – umożliwia skonfigurowanie strony powitalnej, na której użytkownicy muszą podać hasło, aby uzyskać dostęp do sieci
- **ipv6** – wsparcie dla adresacji ipv6
- **mpls** – wsparcie dla protokołu Multi Protocol Labels Switching
- **multicast** – wsparcie dla IGMP (Internet Group Management Protocol)
- **ntp** – Network Time Protocol, serwer dokładnego czasu NTP (**uwaga**: klient ntp znajduje się w paczce **system**)
- **openflow** – wsparcie OpenFlow
- **ppp** – MIPPP client, PPP, PPTP, L2TP, PPPoE, ISDN PPP klienci oraz serwer
- **routerboard** – dostęp do ustawień bootloader-a RouterBOOT
- **routing** – wsparcie dynamicznych protokołów routingu RIP, BGP, OSPF oraz filtry
- **security** – IPSEC, SSH
- **system** – **routing statyczny!!!**, ip addresses, klient sNTP, telnet, API, kolejki (QoS), firewall, web proxy, DNS cache, TFTP, IP pool, SNMP, packet sniffer, e-mail wysyłanie poczty, graphing, bandwidth-test, torch, EoIP, IPIP, bridging, VLAN, VRRP.

Software

Paczki (moduły)

Funkcjonalności paczek:









- **ups** – zarządzanie systemami zasilania awaryjnego APC
- **user-manager** – MikroTik User Manager serwer (Radius) dla zarządzania Hotspot oraz innymi serwisami, powiązanymi z autoryzacją Radius-a
- **wireless** – kontroler CAPsMAN, repeater
- **arlan** – wsparcie dla kart radiowych Aironet Arlan
- **isdn** – wsparcie dla modemów ISDN
- **lcd** – wsparcie dla wyświetlaczy LCD podłączanych za pomocą COM/LPT
- **radiolan** – wsparcie dla kart Radiolan
- **gps** – obsługa wbudowanych lub dołączonych na USB modułów GPS

Szczegóły na stronie: <https://wiki.mikrotik.com/wiki/Manual:System/Packages>

Software

Przykład: Instalacja dodatkowej paczki

Zainstalujemy paczkę **user-manager** (serwer Radius). Ponieważ paczka nie znajduje się w podstawowym zestawie **Main package**, nie jest ona dostępna na naszym urządzeniu. Musimy pobrać paczkę z **Extra packages** dla naszej architektury.

| | 6.46.8 (Long-term) | 6.47.8 (Stable) | 6.48beta58 (Testing) | 7.1beta3 (Development) |
|----------------|---|---|---|---|
| MIPSBE | CRS1xx, CRS2xx, CRS312-4C+8XG, CRS326-24S+2Q+, CRS354, Cube Lite60, DISC, FiberBox, hAP, hAP ac, hAP ac lite, LDF, LHG, LHG Lite60, ItAP mini, mANTBox, mANTBox 2, mAP, NetBox, NetMetal, PowerBox, PWR-Line, QRT, RB9xx, SXTsq, cAP, hEX Lite, RB4xx, wAP, BaseBox, DynaDish, RB2011, SXT, OmniTik, Groove, Metal, Sextant, RB7xx, hEX PoE | | | |
| Main package |  |  |  |  |
| Extra packages |  |  |  |  |

```
100K Nov 26 08:10 advanced-tools-6.47.8-mipsbe.npk
20K Nov 26 08:10 calea-6.47.8-mipsbe.npk
188K Nov 26 08:10 dhcp-6.47.8-mipsbe.npk
52K Nov 26 08:10 gps-6.47.8-mipsbe.npk
180K Nov 26 08:10 hotspot-6.47.8-mipsbe.npk
232K Nov 26 08:10 ipv6-6.47.8-mipsbe.npk
56K Nov 26 08:10 lcd-6.47.8-mipsbe.npk
176K Nov 26 08:10 lora-6.47.8-mipsbe.npk
1.9M Nov 26 08:10 lte-6.47.8-mipsbe.npk
96K Nov 26 08:10 mpls-6.47.8-mipsbe.npk
72K Nov 26 08:10 multicast-6.47.8-mipsbe.npk
260K Nov 26 08:10 ntp-6.47.8-mipsbe.npk
76K Nov 26 08:10 openflow-6.47.8-mipsbe.npk
304K Nov 26 08:10 ppp-6.47.8-mipsbe.npk
120K Nov 26 08:10 routing-6.47.8-mipsbe.npk
344K Nov 26 08:10 security-6.47.8-mipsbe.npk
7.5M Nov 26 08:10 system-6.47.8-mipsbe.npk
140K Nov 26 08:10 tr069-client-6.47.8-mipsbe.npk
64K Nov 26 08:10 ups-6.47.8-mipsbe.npk
888K Nov 26 08:10 user-manager-6.47.8-mipsbe.npk
2.6M Nov 26 08:10 wireless-6.47.8-mipsbe.npk
```

- Kopiujemy paczkę do katalogu głównego (**root folder**)
- Wykonujemy reboot urządzenia:
/system reboot

Kopia bezpieczeństwa

Backup/Export

Każdy administrator, zgodnie z przyjętą polityką wykonywania kopii bezpieczeństwa, powinien przeprowadzać cyklicznie backup konfiguracji urządzeń pracujących w jego sieci.

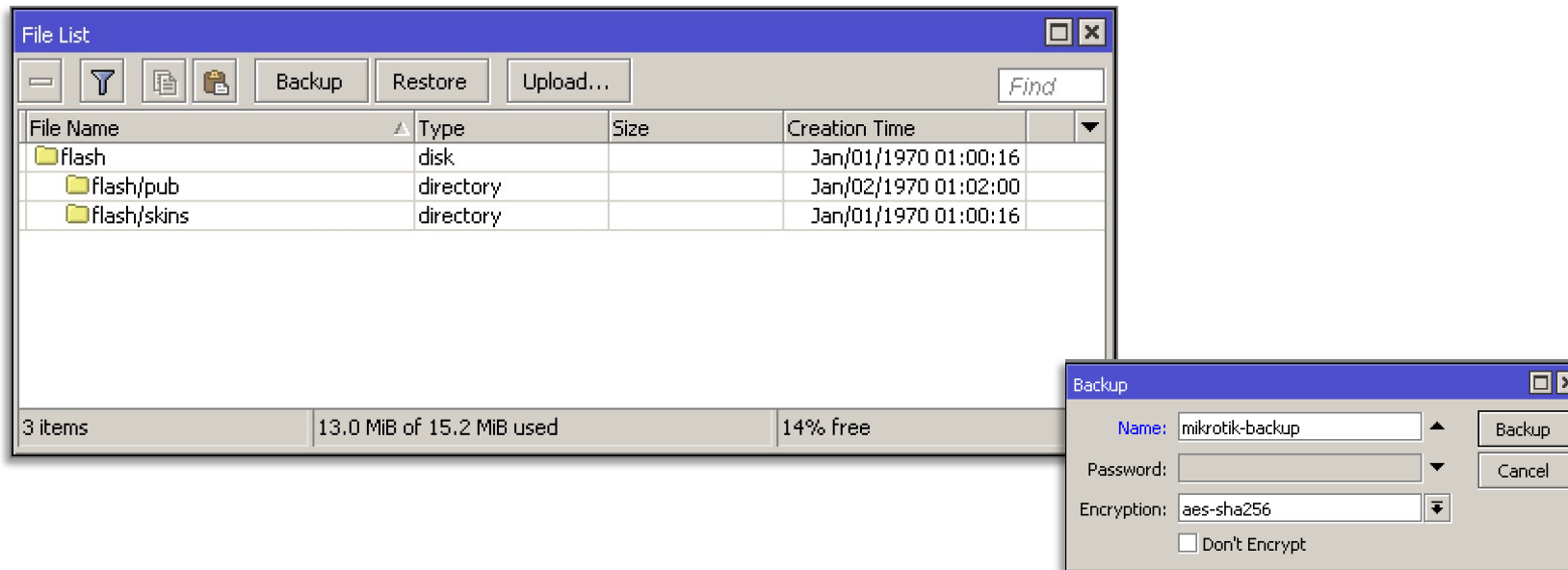
W systemie RouterOS wykonanie kopii bezpieczeństwa możliwe jest na dwa sposoby:

- **Backup**
- **Export**

Kopia bezpieczeństwa

Backup

Mechanizm tworzy plik binarny będący zapisem konfiguracji urządzenia



- Plik zostanie utworzony w katalogu **Files** z nazwą *mikrotik-backup.backup*
- Aby przywrócić backup używamy opcji **Restore**
- Parametr **Password** pozwala na zabezpieczenie backup-u hasłem. W przypadku gdy nie podamy hasła będzie wymagane hasło użytkownika, który wykonał backup

Kopia bezpieczeństwa

Export

```
1. Mikrotik (telnet)

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]       Completes the command/word. If the input is ambiguous,
            a second [Tab] gives possible options

/           Move up to base level
..         Move up one level
/command    Use command at the base level

[admin@Mikrotik] > export
# jul/03/2019 15:19:02 by RouterOS 6.45.1
# software id =
#
#
#
/interface ethernet
set [ find default-name=ether1 ] disable-running-check=no
set [ find default-name=ether2 ] disable-running-check=no
set [ find default-name=ether3 ] disable-running-check=no
set [ find default-name=ether4 ] disable-running-check=no
set [ find default-name=ether5 ] disable-running-check=no
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip dhcp-client
add disabled=no interface=ether1
/system identity
set name=Mikrotik
[admin@Mikrotik] > |
```

Kopia bezpieczeństwa

Export

- Pozwala na zapisanie konfiguracji do pliku w formacie .rsc:
`/export file=export-2019-07-03` (utworzy plik `export-2019-07-03.rsc`)
- Pozwala na wyświetlenie tylko fragmentu konfiguracji

```
[admin@Mikrotik] > ip export
# jul/03/2019 15:27:39 by RouterOS 6.45.1
# software id =
#
#
#
/ip dhcp-client
add disabled=no interface=ether1
[admin@Mikrotik] > |
```

- Plik z rozszerzeniem .rsc możemy otworzyć w notatniku, a następnie po edycji wgrać go ponownie
- Fragmenty konfiguracji możemy wkleić bezpośrednio w okno terminala

UWAGA:

Opcja `export` nie zapisze haseł użytkowników systemowych !!!

Wszystkie inne hasła (IPsec, vpn, wireless) zostaną zapisane do pliku

Aby zrezygnować z zapisywania haseł vpn, wireless należy użyć przełącznika:

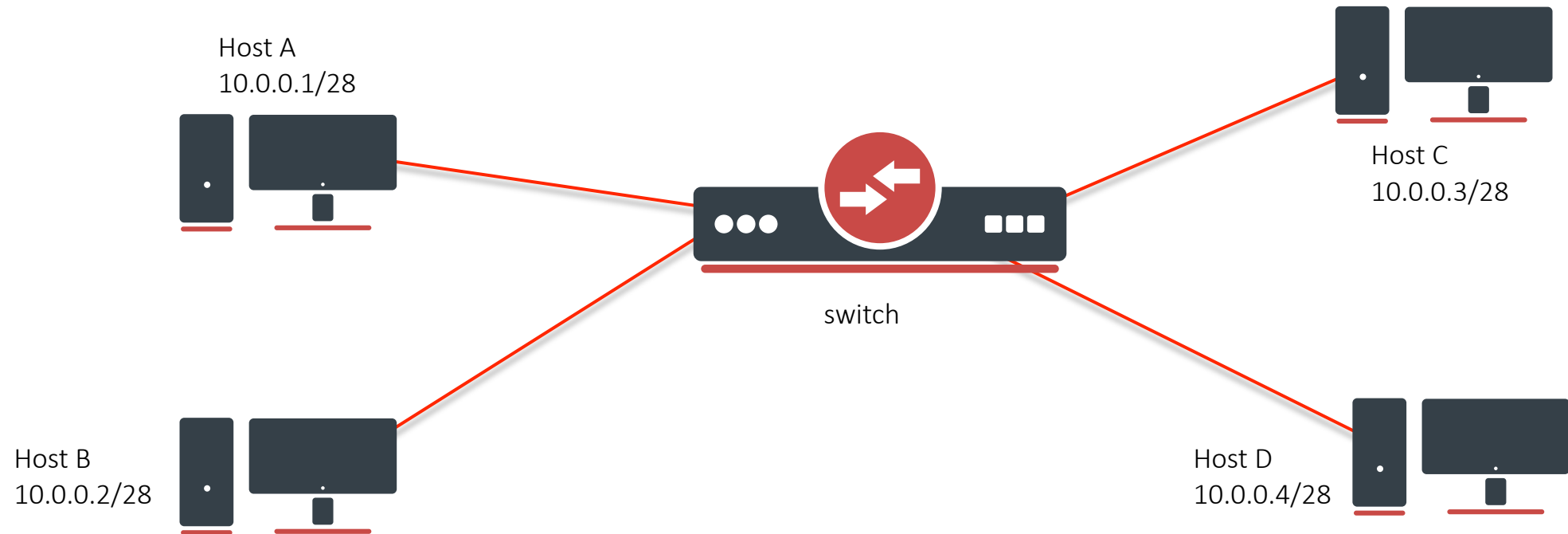
```
/export file=filename hide-sensitive
```

ARP / DHCP

ARP

Address Resolution Protocol

Urządzenia sieciowe: hosty, routery znajdujące się w tej samej domenie rozgłoszeniowej komunikują się ze sobą za pomocą adresów MAC



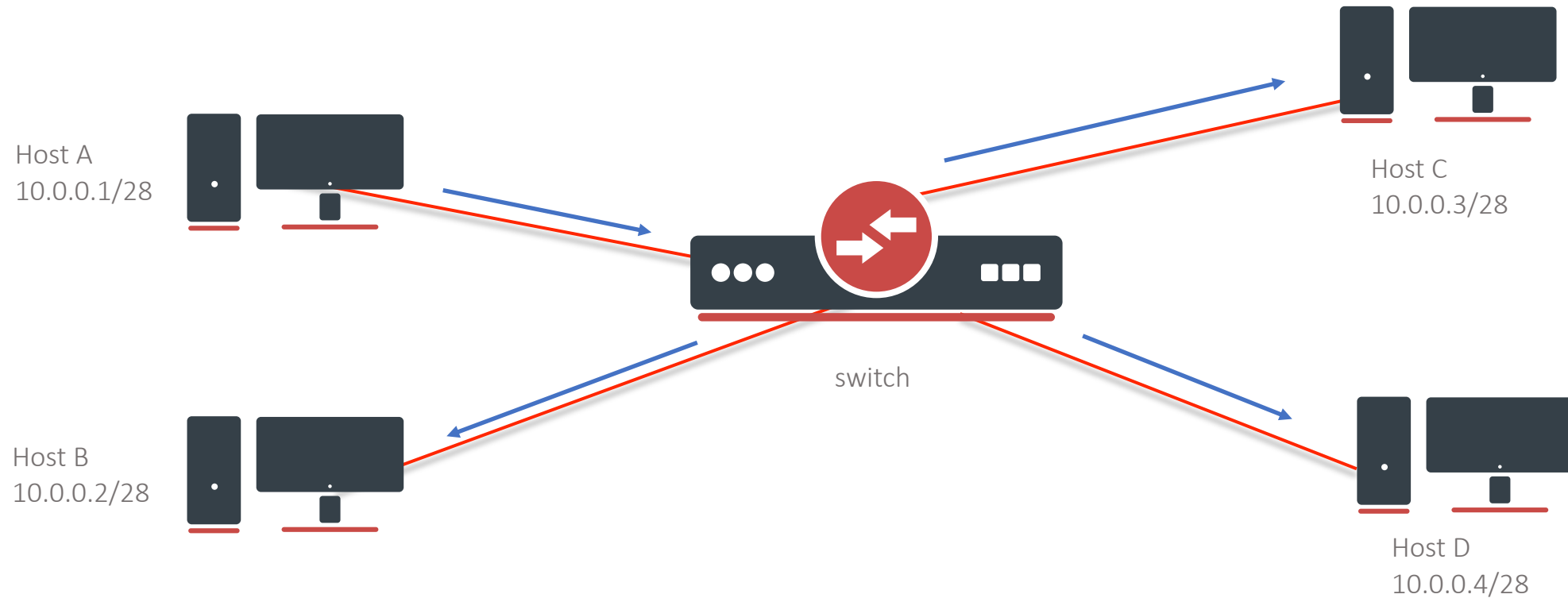
Aby **Host A** mógł komunikować się z **Host D** nie wystarczy znajomość jego adresu IP, potrzebny jest także MAC adres.

Protokół ARP umożliwia stronie nadającej uzyskanie informacji o adresie MAC hosta docelowego.

ARP

Address Resolution Protocol/Request

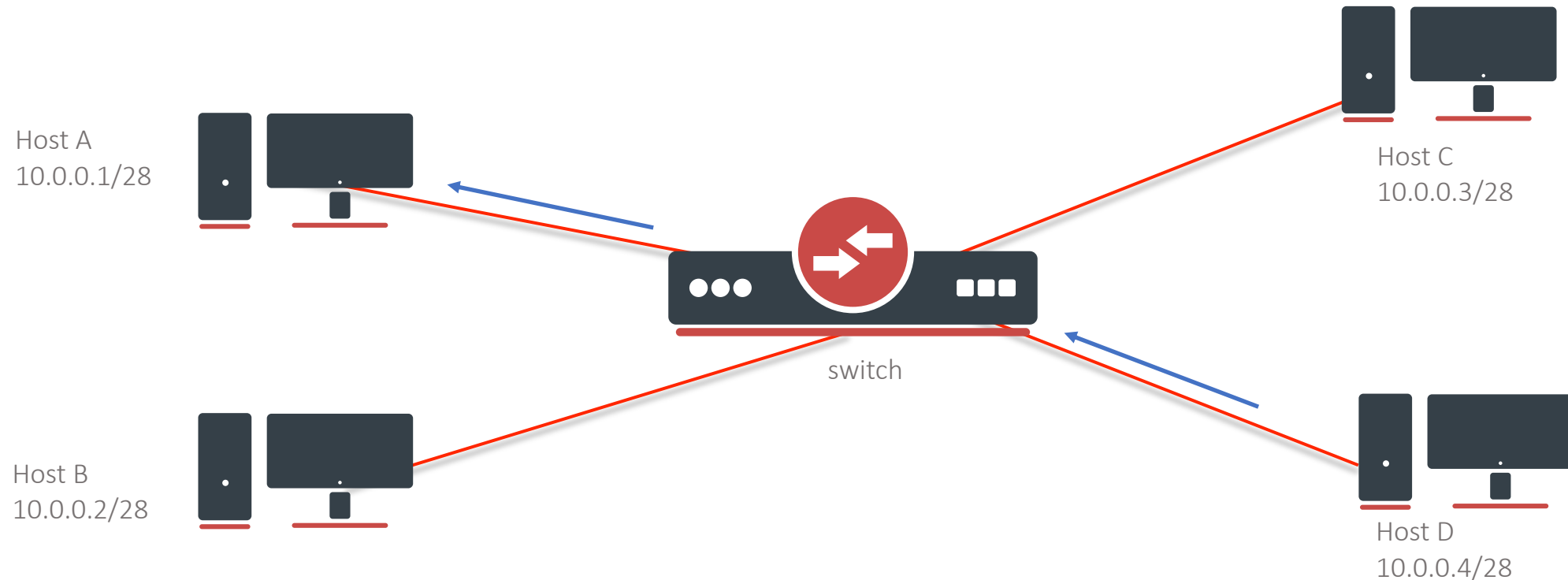
1. Host A wysyła zapytanie ARP Request o treści: proszę o MAC adres hosta o IP adresie 10.0.0.4
2. Przełącznik wysyła zapytanie dalej do wszystkich podłączonych do niego hostów.



ARP

Address Resolution Protocol/Reply

3. Na zapytanie o MAC adres odpowie jedynie **Host D**, którego adresu IP dotyczy zapytanie
4. Przełącznik prześle odpowiedź, ale tym razem już tylko do **Host A**



Host A dodaje u siebie wpis w tablicy ARP utrzymywanej lokalnie

W tym momencie **Host A** zna już MAC adres **Host-a D** i może rozpocząć właściwą komunikację.

ARP

Address Resolution Protocol



REQUEST

| | | | |
|--|------------------------------------|--|------------------------------------|
| MAC adres HOST A <i>00-A0-24-70-FE-BD</i> | IP adres HOST A <i>10.0.0.1</i> | MAC adres HOST D <i>00-00-00-00-00-00</i> | IP adres HOST D <i>10.0.0.4</i> |
|--|------------------------------------|--|------------------------------------|

REPLY

| | | | |
|--|------------------------------------|--|------------------------------------|
| MAC adres HOST D <i>00-02-67-79-0F-4C</i> | IP adres HOST D <i>10.0.0.4</i> | MAC adres HOST A <i>00-A0-24-70-FE-BD</i> | IP adres HOST A <i>10.0.0.1</i> |
|--|------------------------------------|--|------------------------------------|

ARP

Address Resolution Protocol

Tablica ARP na naszym urządzeniu

The screenshot shows the Mikrotik WinBox interface. On the left, the configuration tree is visible with 'IP' > 'ARP' selected. A red arrow points from this selection to the 'ARP List' window on the right. The 'ARP List' window displays a table with the following data:

| | IP Address | MAC Address | Interface |
|---|--------------|-------------------|--------------|
| D | 10.250.1.100 | 48:45:20:58:F7:87 | bridge-trunk |
| | 192.168.1.1 | F0:84:C9:5C:E5:C2 | ether1 |

Below the table, it indicates '2 items'. A red arrow points from the 'D' in the first row to the explanatory text below.

Litera **D** oznacza, iż wpis w naszej tablicy ARP został dodany dynamicznie, w wyniku działania protokołu ARP

ARP

Address Resolution Protocol

The screenshot displays the Mikrotik WinBox interface. On the left is a sidebar with navigation options: Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, and MPLS. The main window shows the 'Interface List' dialog with a table of interfaces. The 'ether1' interface is selected, and its configuration window is open, showing the 'ARP' setting set to 'enabled'.

| Name | Type | Actual MTU | L2 MTU | Tx |
|--------------|--------------------------|------------|--------|----|
| bridge-local | Bridge | 1500 | 1598 | |
| ether1 | Ethernet | 1500 | 1598 | |
| ether2 | Ethernet | 1500 | 1598 | |
| ether3 | Ethernet | 1500 | 1598 | |
| ether4 | Ethernet | 1500 | 1598 | |
| ether5 | Ethernet | 1500 | 1598 | |
| wlan1 | Wireless (Atheros AR...) | 1500 | 1600 | |
| wlan2 | Wireless (Atheros AR...) | 1500 | 1600 | |

Interface <ether1> configuration:

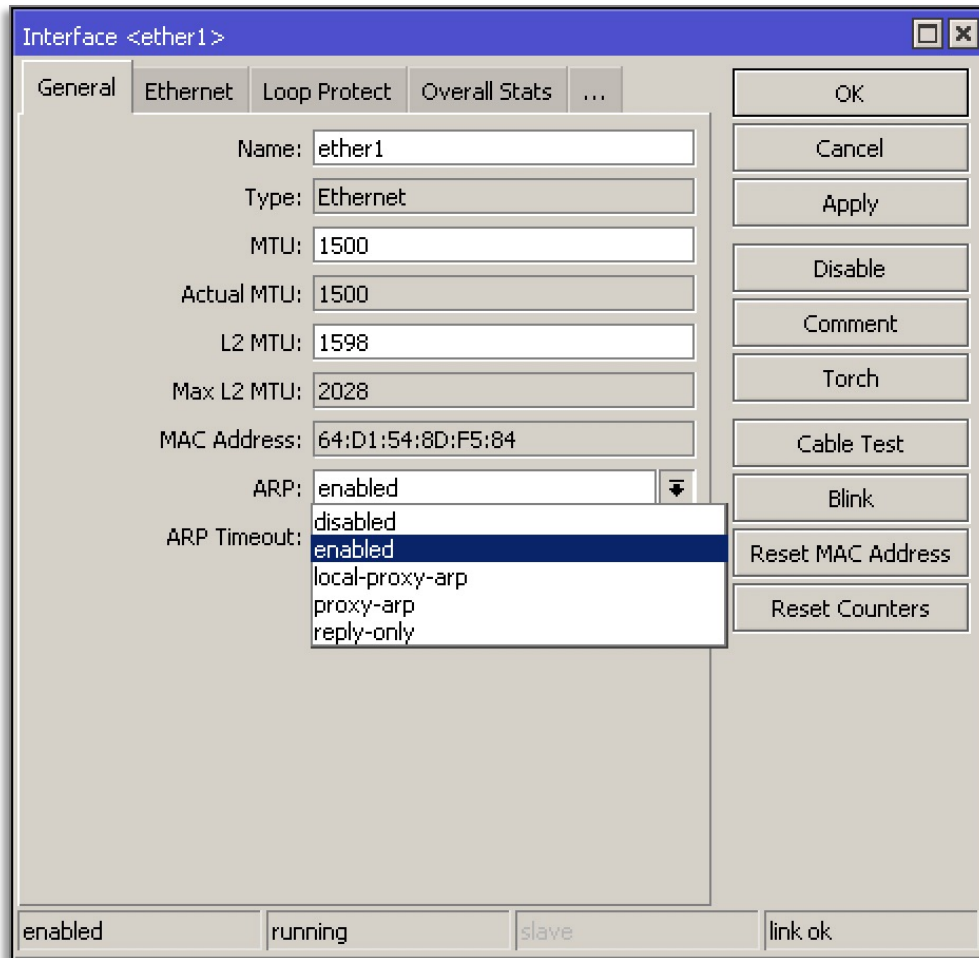
- Name: ether1
- Type: Ethernet
- MTU: 1500
- Actual MTU: 1500
- L2 MTU: 1598
- Max L2 MTU: 2028
- MAC Address: 64:D1:54:8D:F5:84
- ARP: enabled
- ARP Timeout: [empty]

Interface status: enabled, running, slave, link ok

Domyślnie wszystkie interface-y mają włączoną obsługę protokołu ARP

ARP

Możliwe ustawienia ARP



Możliwe ustawienia:

- **disabled** — wyłączona obsługa protokołu ARP
- **enabled** — włączona obsługa protokołu **ARP** (domyślnie)
- **local-proxy-arp** — funkcja działa w ramach jednego interface-u router pośredniczy w komunikacji pomiędzy wszystkimi hostami pomimo faktu, iż znajdują się w tej samej domenie rozgłoszeniowej
- **proxy-arp** — router na zapytanie arp z innej sieci odpowie swoim adresem MAC i w późniejszej fazie będzie pośredniczył w przesyłaniu pakietów
- **reply-only** — urządzenie nigdy nie będzie wysyłało arp request, istnieje konieczność ręcznego wprowadzania wpisów do tablicy arp, urządzenie odpowie na zapytanie arp request jeżeli takie się pojawi

ARP

Ręczne dodawanie wpisów ARP

W przypadku gdy wyłączyliśmy działanie protokołu ARP na interface-ie, musimy ręcznie dodać wpisy aby umożliwić komunikację IP z innymi urządzeniami

The image illustrates the process of manually adding ARP entries in a network configuration environment. It consists of three main components:

- Configuration Menu:** A tree view on the left shows the navigation path: IP > ARP. A red arrow points from the 'ARP' menu item to the ARP List window.
- ARP List Window:** A table window titled 'ARP List' showing existing entries. A red arrow points from the '+' icon in the toolbar to the ARP configuration dialog.
- ARP Configuration Dialog:** A dialog box titled 'ARP <10.10.10.20>' with the following fields and options:
 - IP Address: 10.10.10.20
 - MAC Address: 6C:3B:6B:82:F3:BE
 - Interface: bridge1
 - Published
 - Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Make Static, Ping, MAC Ping, Telnet, MAC Telnet, Torch.
 - Status indicators: enabled, published, complete, DHCP.

DHCP

Dynamic Host Configuration Protocol

Protokół służy do automatycznego konfigurowania ustawień sieciowych klientów łączących się do sieci. Serwer DHCP wysyła do klientów niezbędne informacje takie jak:

- adres IP wraz maską sieci
- brama domyślna (default gateway)
- serwery DNS

DHCP umożliwia również przesłanie innych parametrów, z których klient może skorzystać:

- NTP - serwer dokładnego czasu
- WINS – serwer Windows Internet Name Service
- Next Server (option 66)
- Boot Filename (option 67)
- inne

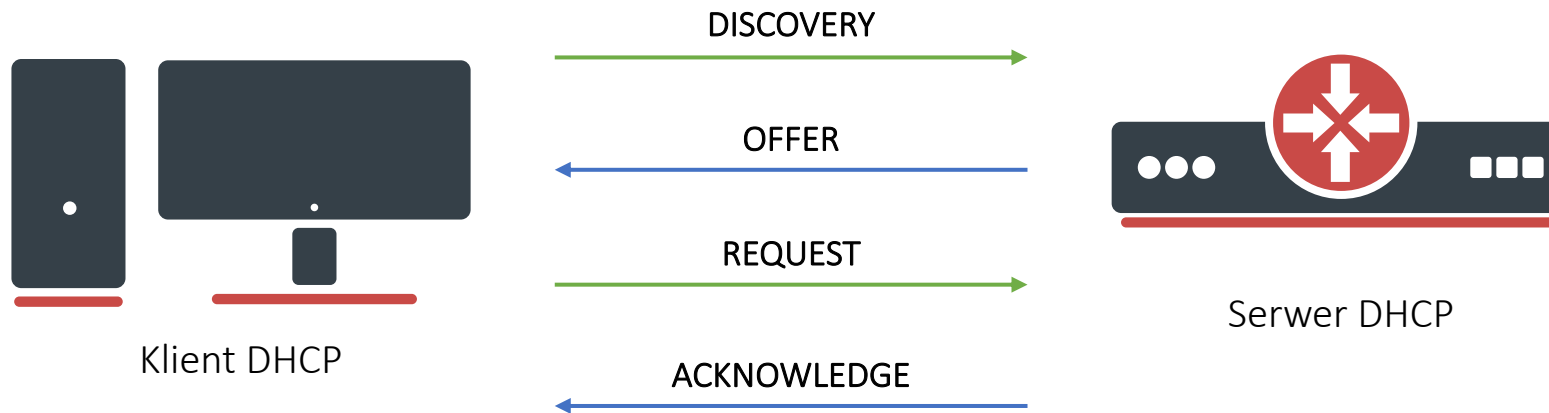
DHCP

Komunikaty RFC2131

- **DHCPDISCOVER** - Klient wysyła komunikat rozgłoszeniowy, aby znaleźć dostępne serwery
- **DHCPOFFER** - Serwer wysyła do klienta w odpowiedzi na DHCPDISCOVER propozycję parametrów konfiguracyjnych
- **DHCPREQUEST** - Powiadomienie klienta do serwerów lub (a) żądanie proponowanych parametrów z jednego serwera i niejawne odrzucenie ofert od wszystkich innych, (b) potwierdzenie poprawności wcześniej przydzielonego adresu po, na przykład, ponownym uruchomieniu systemu, lub (c) przedłużenie dzierżawy na określony adres sieciowy
- **DHCPACK** - Serwer wysyła do klienta ustawienia konfiguracyjne, w tym podany adres sieciowy
- **DHCPNAK** - Serwer wysyła do klienta informację, że propozycja adresu sieciowego klienta jest nieprawidłowa (na przykład klient przeniósł się do nowej podsieci) lub upłynął czas dzierżawy klienta
- **DHCPDECLINE** - Klient wysyła do serwera powiadomienie, że adres sieciowy jest już używany
- **DHCPRELEASE** - Klient do serwera, aby anulować dzierżawę
- **DHCPINFORM** - Klient do serwera z żądaniem tylko o parametry konfiguracyjne; klient ma już skonfigurowany adres

DHCP

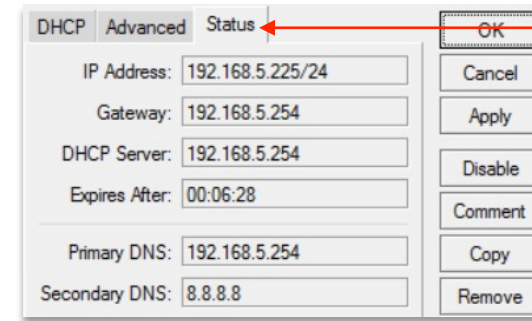
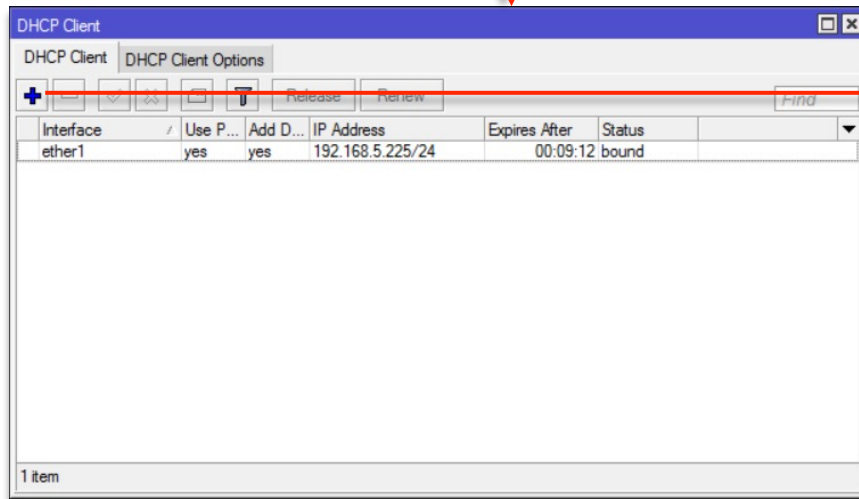
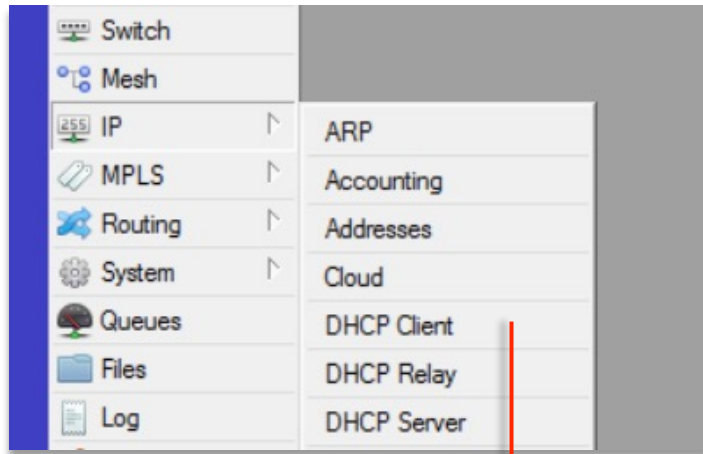
Wymiana komunikatów



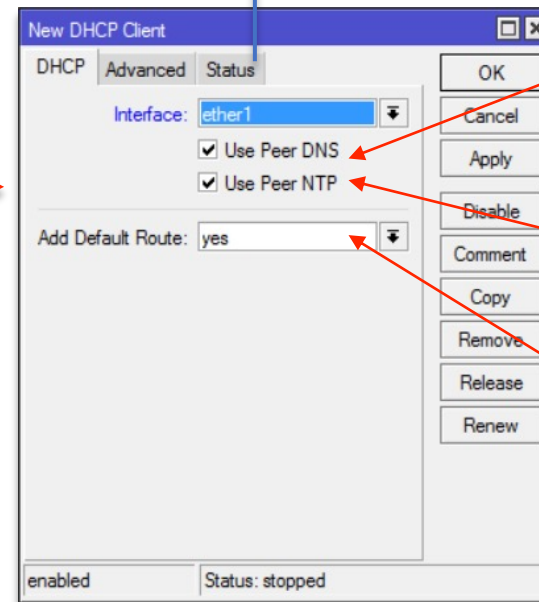
- **DHCPDISCOVER message**
IP: source=0.0.0.0; destination=255.255.255.255; UDP: source port=68; destination port=67
- **DHCPOFFER message**
IP: source= 192.168.1.1; destination=255.255.255.255; UDP: source port=67; destination port=68
- **DHCPREQUEST**
IP: source=0.0.0.0; destination=255.255.255.255; UDP: source port=68; destination port=67
- **DHCPACK**
IP: source= 192.168.1.1; destination=255.255.255.255; UDP: source port=67; destination port=68

DHCP

Konfiguracja klienta



Weryfikacja czy nasz klient uzyskał adres z serwera DHCP



Jeżeli serwer poda adresy serwerów DNS, to czy mamy z nich skorzystać

Jeżeli serwer poda adres serwera NTP to mamy go użyć

Czy mamy użyć bramy domyślnej (default gateway), podanego przez serwer DHCP

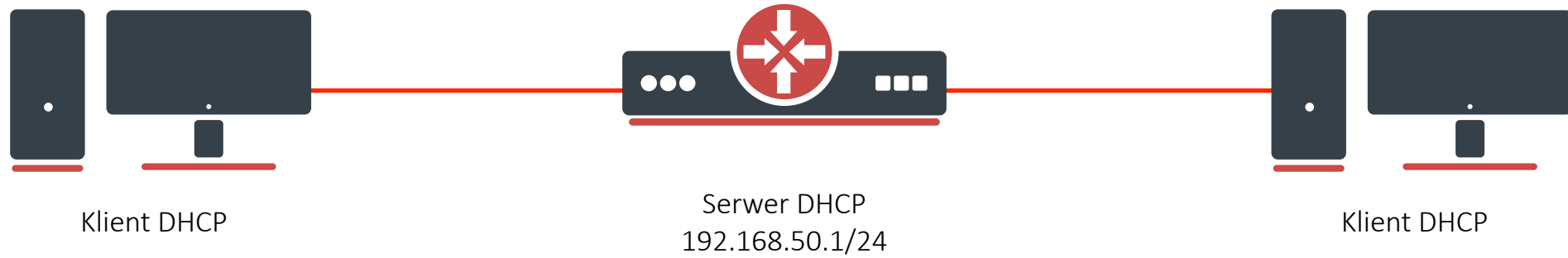
DHCP

Konfiguracja DHCP serwera

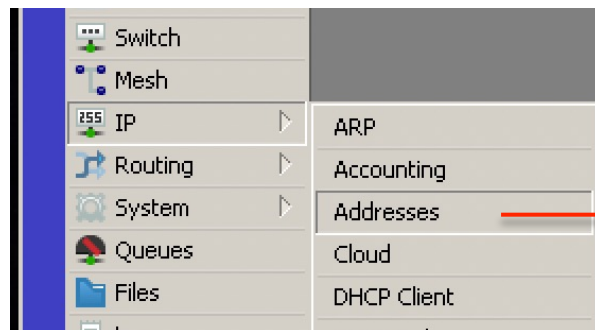
- konieczne jest wskazanie interface-u, na którym będzie pracował serwer (***na jednym interface-ie może pracować tylko jeden serwer DHCP !!!***)
- należy zaadresować interfejs, na którym będzie pracować DHCP serwer!!!
- należy wskazać **address pool** (zakres adresów, z którego serwer będzie przydzielał adresy)
- **lease time** - czas dzierżawy adresu IP
- **Relay** - czy pozwalać za zapytania typu unicast DHCP Relay serwerów (0.0.0.0 – nie zezwalaj, 10.10.2.1 – zezwalaj tylko z wskazanej adresy)

DHCP

Konfiguracja DHCP serwera



1. Nadanie adresu IP na interfejsie



The "Address List" window displays a table with three entries. A red arrow points from the "+" icon in the toolbar to the "Address" column of the second row.

| | Address | Network | Interface |
|---|-----------------|--------------|---------------|
| D | 10.10.1.20/26 | 10.10.1.0 | wlan1 |
| | 192.168.50.1/24 | 192.168.50.0 | vlan-50-main |
| | 192.168.60.1/24 | 192.168.60.0 | vlan-60-guest |

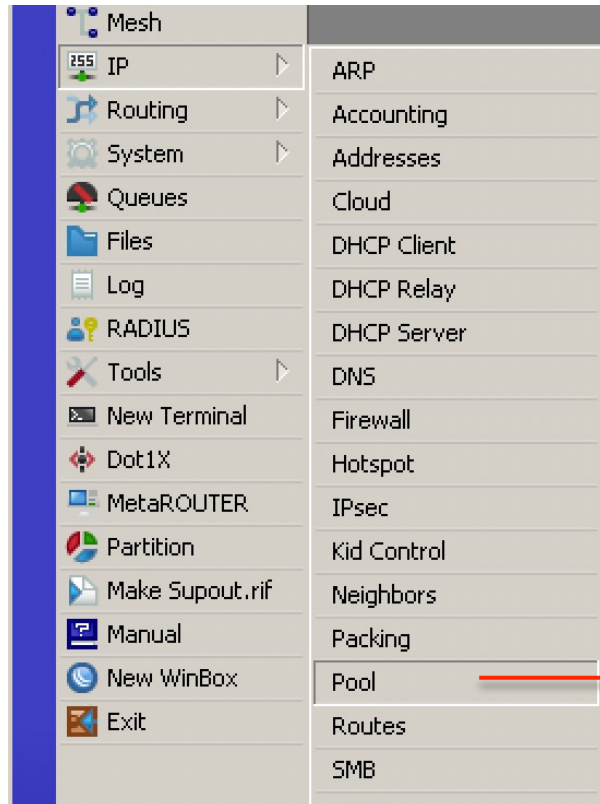
3 items

The "Address <192.168.50.1/24>" dialog box shows configuration fields: Address (192.168.50.1/24), Network (192.168.50.0), and Interface (vlan-50-main). Buttons for OK, Cancel, Apply, Disable, Comment, Copy, and Remove are visible. The status "enabled" is shown at the bottom.

DHCP

Konfiguracja DHCP serwera

2. Skonfigurowanie ip-pool – zakresu adresów, które będzie przydzielać serwer naszym klientom.



The screenshot shows the 'IP Pool <pool-dhcp-vlan-50>' configuration dialog box. It has a title bar with a close button. The fields are: Name: pool-dhcp-vlan-50, Addresses: 192.168.50.2-192.168.50.254, and Next Pool: none. On the right side, there are buttons for OK, Cancel, Apply, Comment, Copy, and Remove. A red arrow points from the 'OK' button to the text 'Nazwa puli adres' (Name of the address pool). Another red arrow points from the 'Addresses' field to the text 'Zakres adresów' (Address range).

Nazwa puli adres

Zakres adresów

The screenshot shows the 'IP Pool' main window with two tabs: 'Pools' and 'Used Addresses'. The 'Pools' tab is active, showing a table with the following data:

| Name | Addresses | Next Pool |
|-------------------|-----------------------------|-----------|
| pool-dhcp-vlan-50 | 192.168.50.2-192.168.50.254 | none |
| pool-dhcp-vlan-60 | 192.168.60.2-192.168.60.254 | none |

At the bottom of the window, it says '2 items'. A red arrow points from the 'Pool' option in the WinBox menu to the 'Pools' tab.

DHCP

Konfiguracja DHCP serwera

3. Dodanie serwera

The screenshot shows the Mikrotik WinBox interface. On the left, a sidebar contains various system menus. The main window displays the 'DHCP Server' configuration menu. A table below the menu lists existing DHCP servers:

| Name | Interface | Relay | Lease Time |
|--------------------|---------------|-------|------------|
| dhcp-vlan-50-main | vlan-50-main | | 00: |
| dhcp-vlan-60-guest | vlan-60-guest | | 00: |

The screenshot shows the 'DHCP Server <dhcp-vlan-50-main>' configuration dialog box. The 'Generic' tab is active. The configuration includes:

- Name: dhcp-vlan-50-main
- Interface: vlan-50-main
- Relay: (empty)
- Lease Time: 00:10:00
- Bootp Lease Time: forever
- Address Pool: pool-dhcp-vlan-50
- DHCP Option Set: (empty)
- Src. Address: (empty)
- Delay Threshold: (empty)
- Authoritative: yes
- Bootp Support: static
- Client MAC Limit: (empty)
- Use RADIUS: no
- Always Broadcast
- Add ARP For Leases
- Use Framed As Classless
- Conflict Detection

The status at the bottom is 'enabled'.

Interfejs, na którym pracuje serwer DHCP

Poprzednio stworzona pula adresów

Gdy na interfejsie mamy skonfigurowaną opcję **ARP disabled** lub **reply-only**, możemy użyć tego ustawienia do wpisania klienta do tablicy ARP naszego routera

DHCP

Konfiguracja DHCP serwera

4. Ustawienie, jakie parametry, poza adresem IP, będą wysyłane do klienta

The screenshot shows the DHCP Server configuration interface. The main window has tabs for DHCP, Networks, Leases, Options, Option Sets, Vendor Classes, and Alerts. A table lists the configured networks:

| Address | Gateway | DNS Servers | Domain | WINS Servers | Next |
|-----------------|--------------|-------------|--------|--------------|------|
| 192.168.50.0/24 | 192.168.50.1 | 8.8.8.8 | | | |
| 192.168.60.0/24 | 192.168.60.1 | 8.8.8.8 | | | |

A red arrow points from the '+' icon in the DHCP tab to the 'DHCP Network <192.168.50.0/24>' dialog box. The dialog box contains the following configuration options:

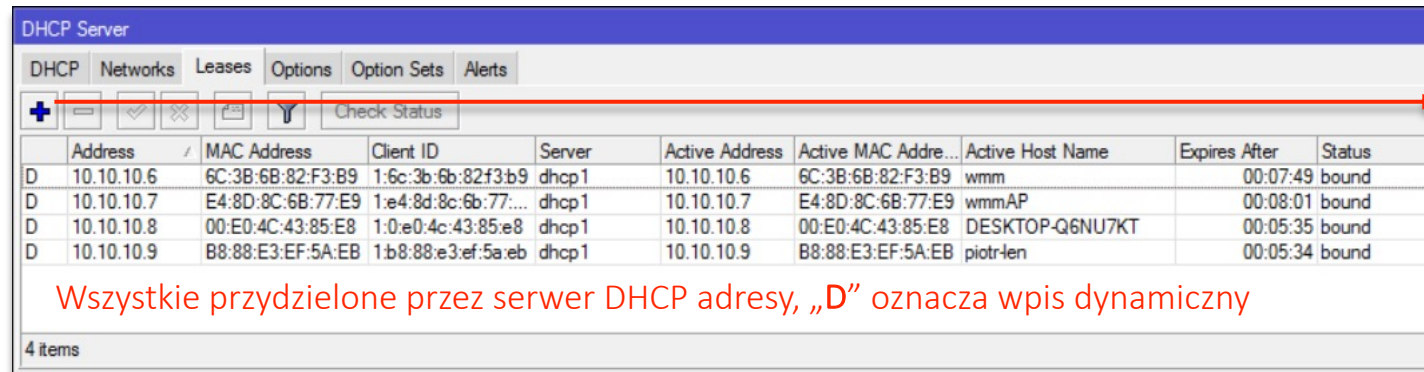
- Address: 192.168.50.0/24
- Gateway: 192.168.50.1
- Netmask: (empty)
- No DNS
- DNS Servers: 8.8.8.8
- Domain: (empty)
- WINS Servers: (empty)
- NTP Servers: 192.168.50.1
- CAPS Managers: (empty)
- Next Server: (empty)
- Boot File Name: (empty)
- DHCP Options: (empty)
- DHCP Option Set: (empty)

Buttons on the right side of the dialog include OK, Cancel, Apply, Comment, Copy, and Remove.

DHCP

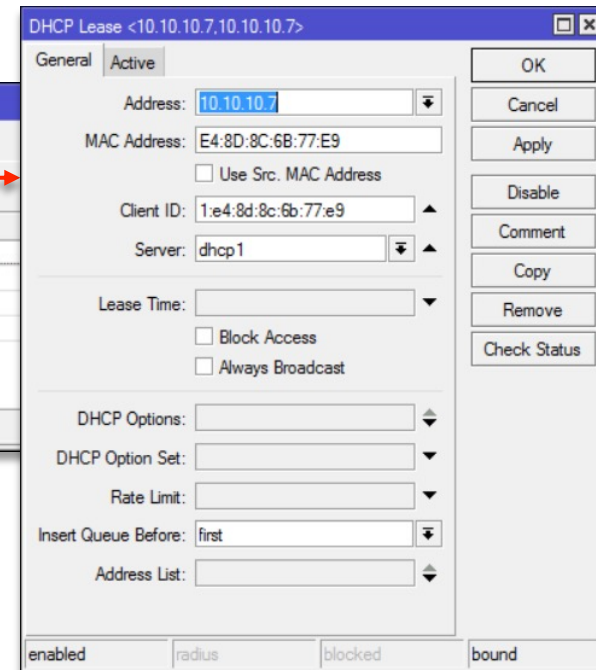
Konfiguracja DHCP serwera

Dzierżawa adresów IP



| | Address | MAC Address | Client ID | Server | Active Address | Active MAC Address | Active Host Name | Expires After | Status |
|---|------------|-------------------|----------------------|--------|----------------|--------------------|------------------|---------------|--------|
| D | 10.10.10.6 | 6C:3B:6B:82:F3:B9 | 1:6c:3b:6b:82f3b9 | dhcp1 | 10.10.10.6 | 6C:3B:6B:82:F3:B9 | wmm | 00:07:49 | bound |
| D | 10.10.10.7 | E4:8D:8C:6B:77:E9 | 1:e4:8d:8c:6b:77:... | dhcp1 | 10.10.10.7 | E4:8D:8C:6B:77:E9 | wmmAP | 00:08:01 | bound |
| D | 10.10.10.8 | 00:E0:4C:43:85:E8 | 1:0:e0:4c:43:85:e8 | dhcp1 | 10.10.10.8 | 00:E0:4C:43:85:E8 | DESKTOP-Q6NU7KT | 00:05:35 | bound |
| D | 10.10.10.9 | B8:88:E3:EF:5A:EB | 1:b8:88:e3:ef:5a:eb | dhcp1 | 10.10.10.9 | B8:88:E3:EF:5A:EB | piotr-len | 00:05:34 | bound |

Wszystkie przydzielone przez serwer DHCP adresy, „D” oznacza wpis dynamiczny



DHCP Lease <10.10.10.7,10.10.10.7>

General Active

Address: 10.10.10.7

MAC Address: E4:8D:8C:6B:77:E9

Use Src. MAC Address

Client ID: 1:e4:8d:8c:6b:77:e9

Server: dhcp1

Lease Time: [dropdown]

Block Access

Always Broadcast

DHCP Options: [dropdown]

DHCP Option Set: [dropdown]

Rate Limit: [dropdown]

Insert Queue Before: first

Address List: [dropdown]

enabled radius blocked bound

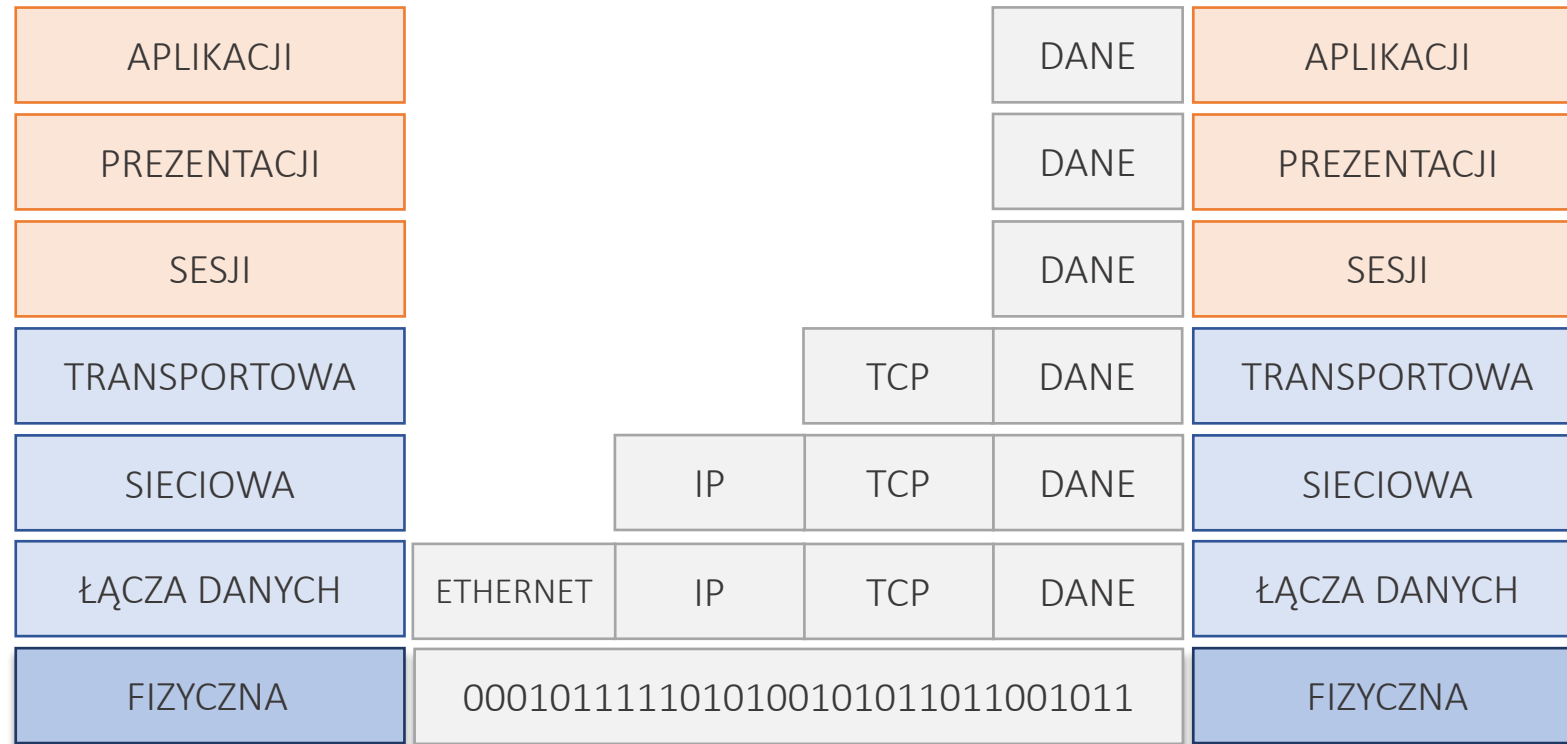
OK Cancel Apply Disable Comment Copy Remove Check Status

Możemy stworzyć ręcznie wpis (rezerwację) dla konkretnego host-a w tablicy **lease**, dzięki temu będziemy mieć pewność, że za każdym razem host dostanie ten sam adres IP. Szczególnie przydatne gdy mamy np. drukarkę i chcemy aby była zawsze osiągalna pod tym samym adresem IP

MODEL OSI

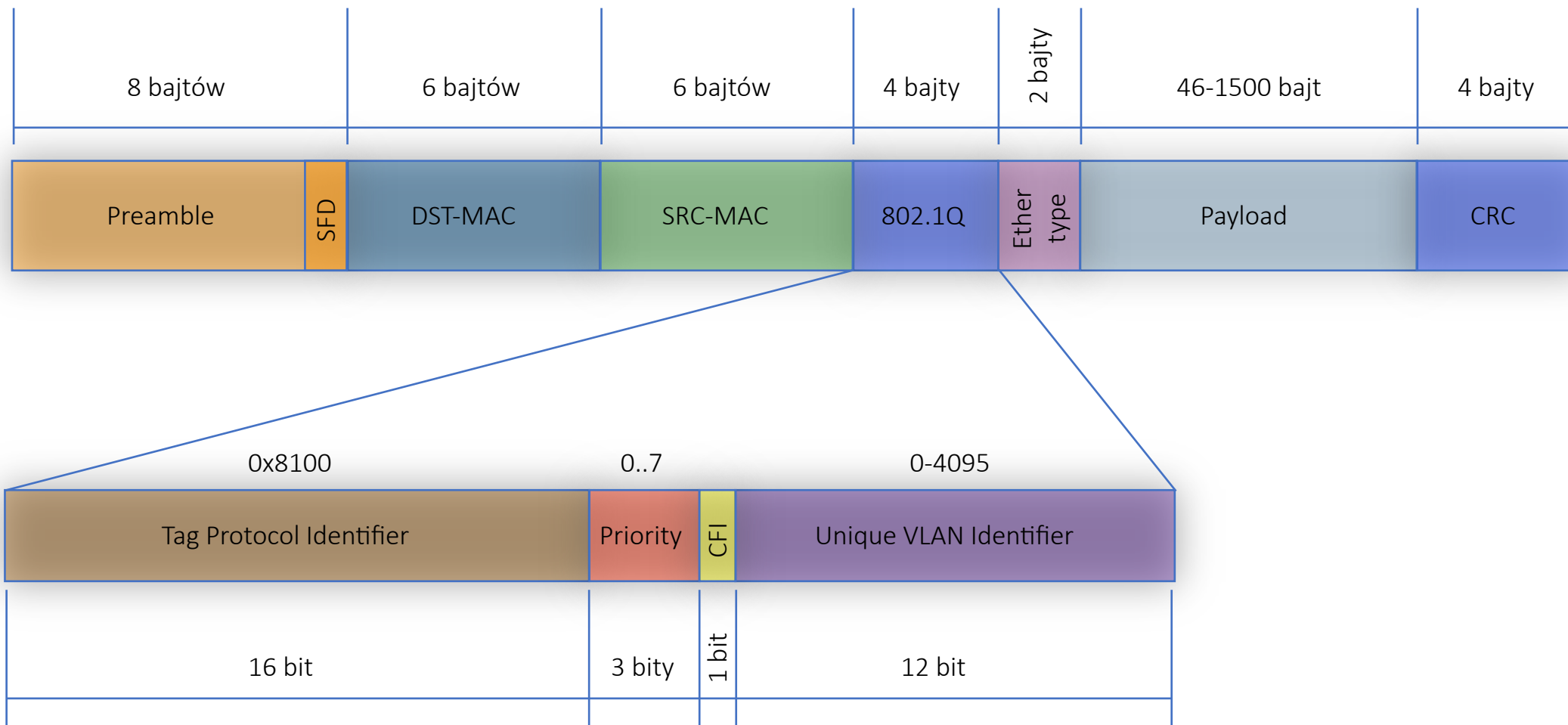
Model OSI

Warstwy / Layers



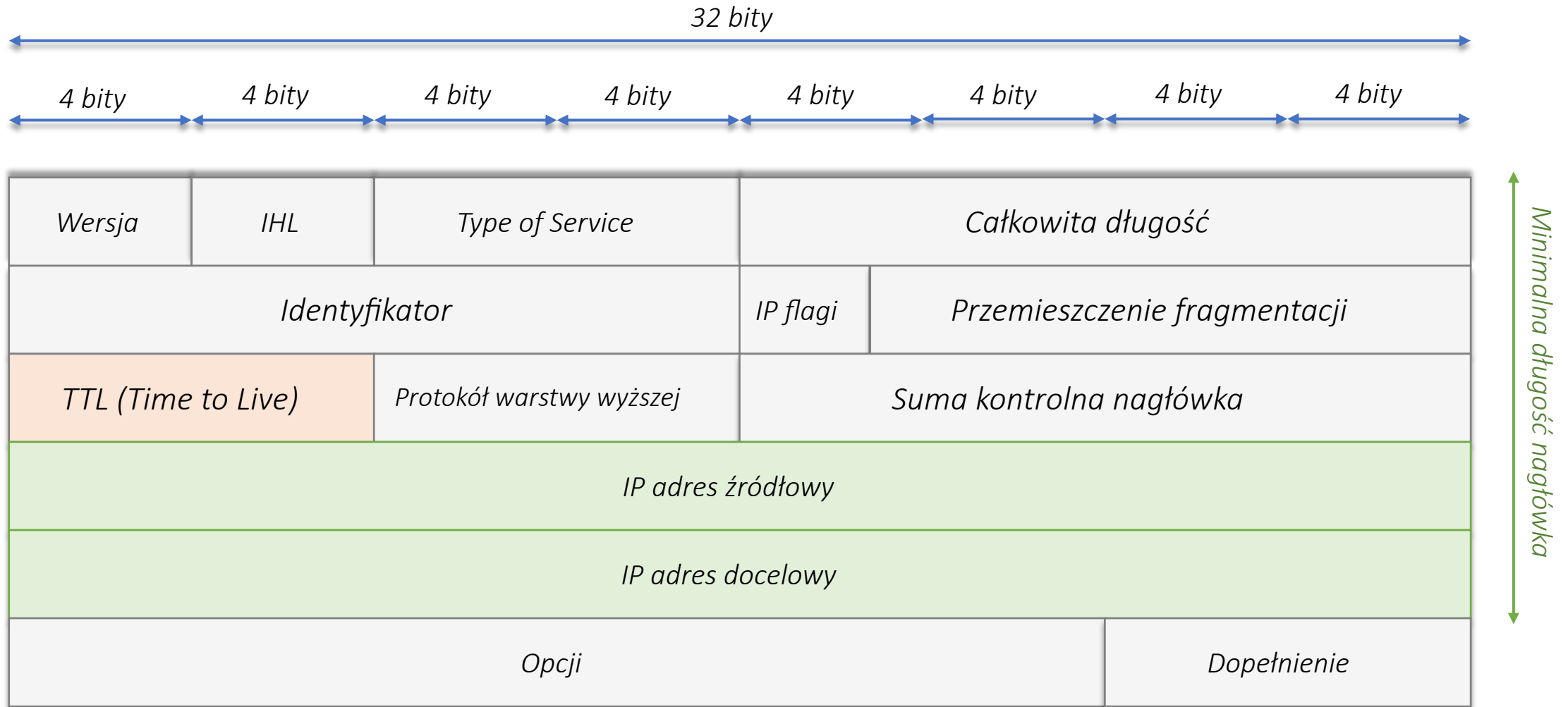
Model OSI

Layer 2 / Ethernet / łącza danych



Model OSI

Layer 3 / Nagłówek IPv4



Model OSI

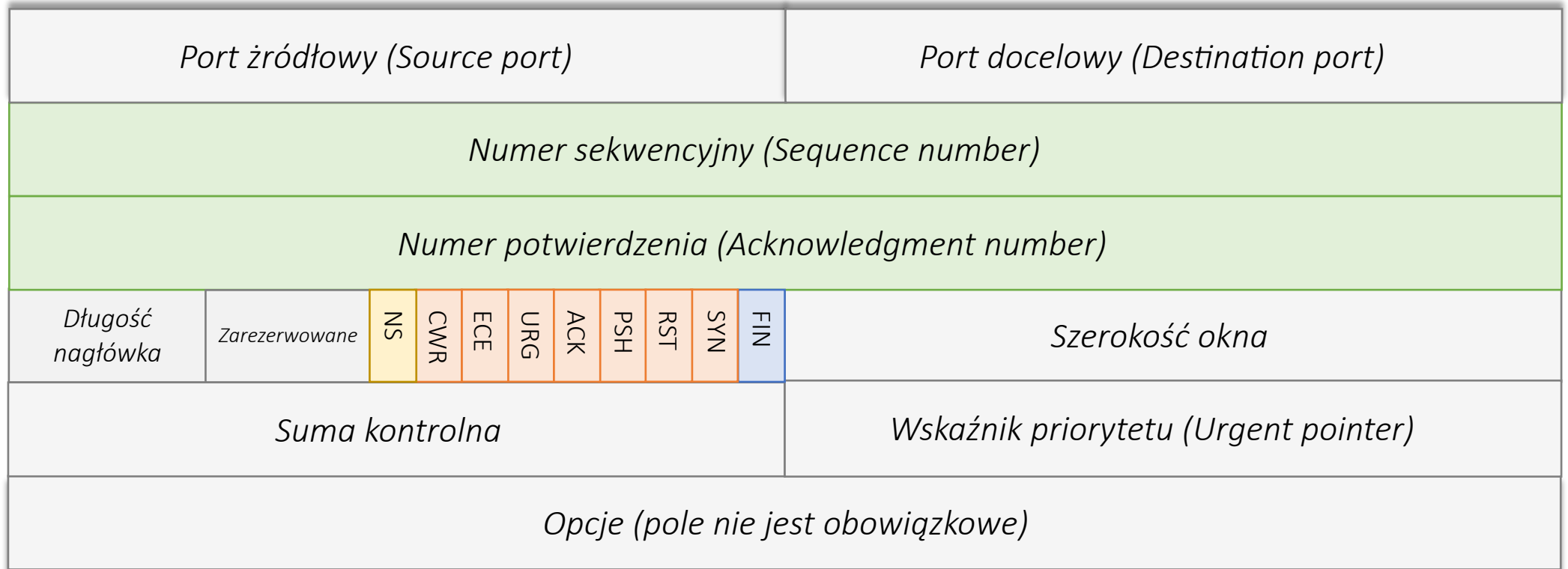
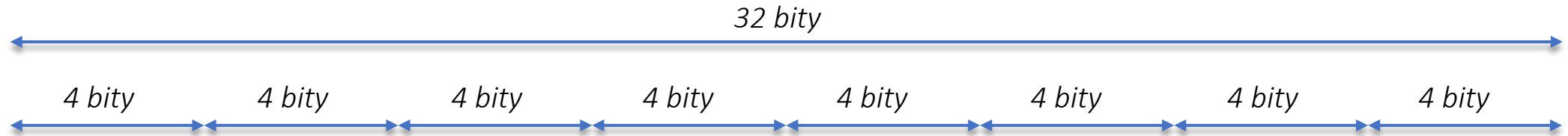
Layer 3 / Nagłówek IPv4

- **Wersja** — 4-bitowe pole, IPv4 lub IPv6 (w naszym przypadku **IPv4**)
- **IHL** – Internal Header Length (długość nagłówka IP). Ta wartość — to pełna długość nagłówka z uwzględnieniem dwóch pól o zmiennej długości.
- **Całkowita długość** – 16-bitowe pole, opisujący długość pakietu w bajtach, łącznie z nagłówkiem i danymi.
- **TTL** – wartość 0-255, licznik, który przechowuje stale malejącą wartość liczby węzłów mijanych (routerów, czasami nazywanych hop-ami) w drodze do celu. Każdy kolejny router IP na trasie danego pakietu zmniejsza wartość jego pola TTL o jeden. Czas życia pakietu pomaga unikać przeciążenia sieci w przypadku źle skonfigurowanych tras routingu w routerach, np. występowania pętli w sieci.
- **IP Flags** – DF (don't fragment), można zakazać fragmentacji pakietu
- **Protokół warstwy wyższej** – TCP, UDP lub inne
- **Adres źródłowy** – adres IP nadawcy
- **Adres docelowy** – adres IP odbiorcy

Minimalny rozmiar nagłówka IP- 160 bitów lub 20 bajtów

Model OSI

Layer 4 / Nagłówek TCP



Minimalna długość nagłówka

Model OSI

Layer 4 / Nagłówek TCP / Flags

Flags / Flagi — 9-bitowa informacja/polecenie dotyczące bieżącego pakietu. Opisane w *RFC 793*.
Poszczególne flagi oznaczają:



URG — *Urgent*, informuje o istotności pola "Priorytet"

ACK — *Acknowledge*, informuje o istotności pola "Numer potwierdzenia"

PSH — *Push*, wymusza przesłanie pakietu

RST — *Reset*, resetuje połączenie (wymagane ponowne uzgodnienie sekwencji)

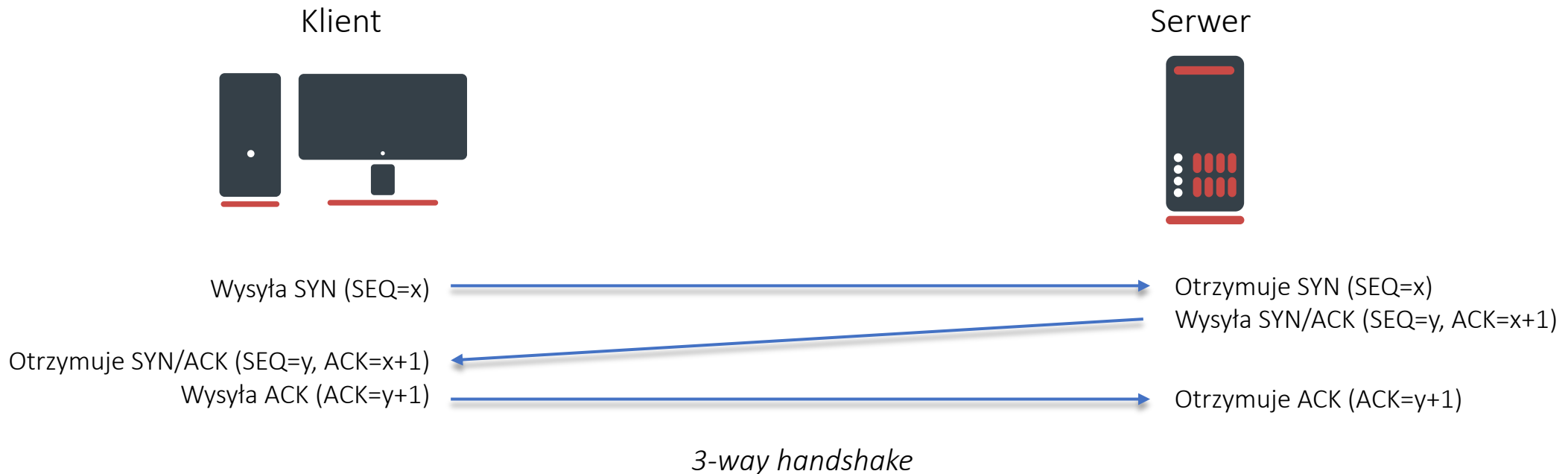
SYN — *Synchronize*, synchronizuje kolejne numery sekwencyjne

FIN — *Finish*, oznacza zakończenie przekazu danych

Model OSI

Layer 4 / TCP

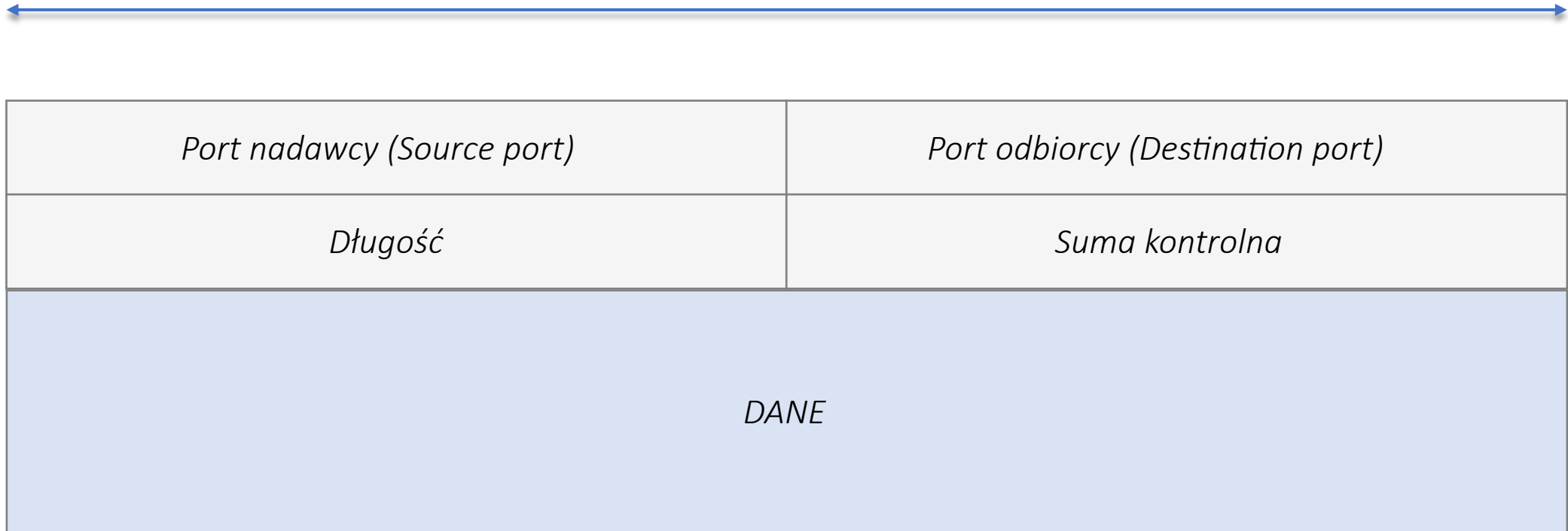
TCP- Transmission Control Protocol (Protokół sterowania transmisją), połączeniowy, strumieniowy, niezawodny. Połączeniowy charakter protokołu wynika z jasno zdefiniowanego cyklu życia danego połączenia, gdzie na początku mamy fazę inicjującą następnie established i w przypadku zakończenia połączenia strony informują się o zakończeniu transmisji. Niezawodność protokołu polega na potwierdzaniu przez stronę odbierającą czy otrzymała przesłane dane. Jest to protokół typu klient-serwer, gdzie jedna strona cały czas nasłuchuje na połączenie. Aby możliwa była wymiana danych pomiędzy klientem i serwerem konieczna jest wstępna procedura zwana potrójnym uściśnięciem ręki (**3-way handshake**).



Model OSI

Layer 4 / UDP

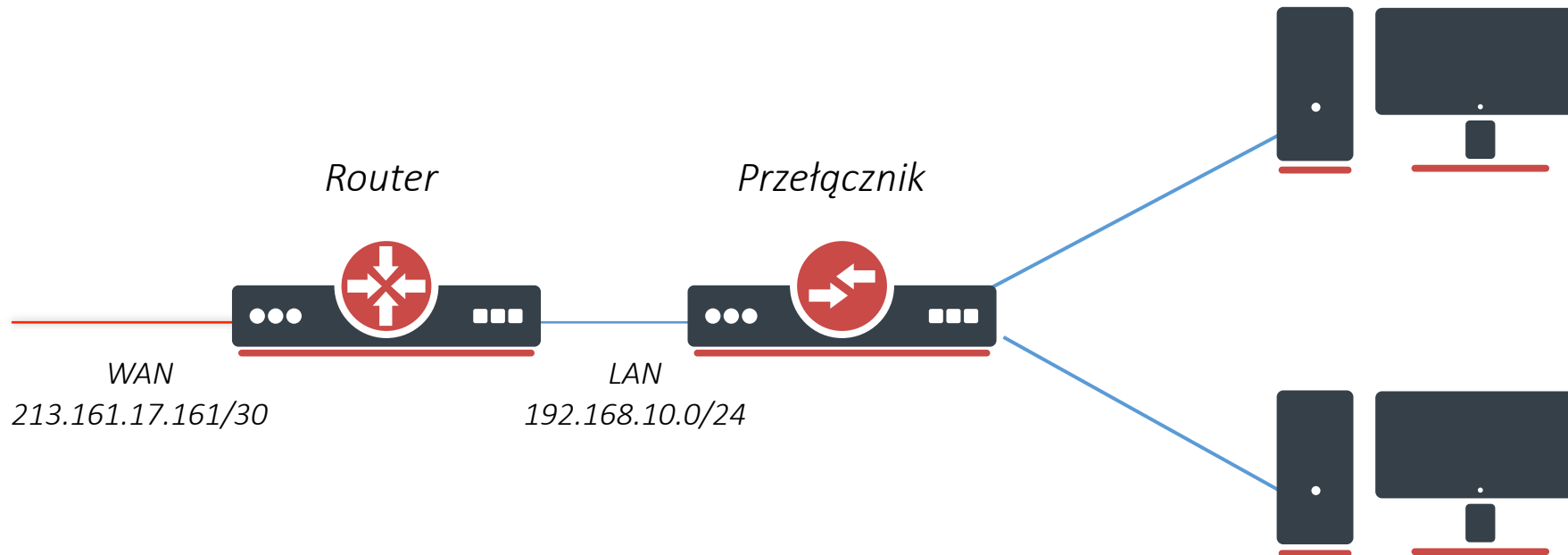
32 bity



Nie ma gwarancji dostarczenia datagramu, brak potwierżeń.
Nie posiada mechanizmu kontroli przepływu.

BRIDGE

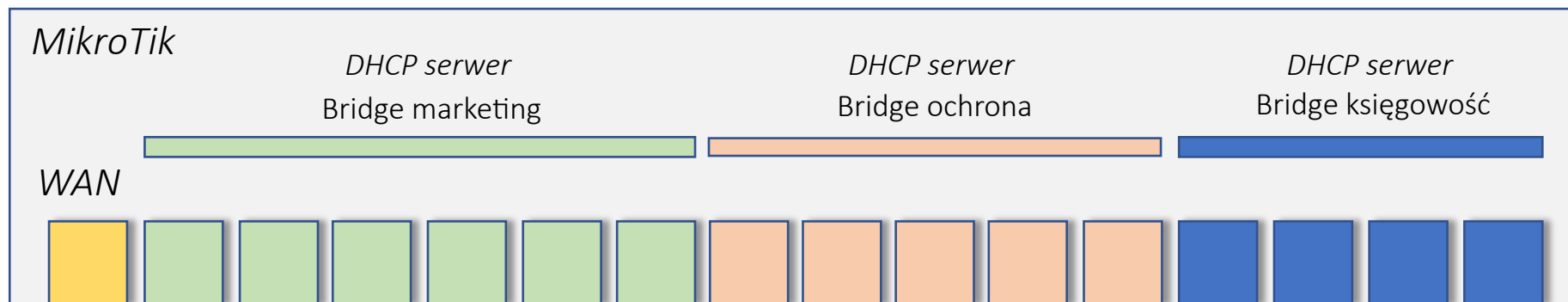
Bridge



Router – łączy więcej niż jedną domenę rozgłoszeniową (segment sieci)

Switch/przetłacznik – działa w ramach jednej domeny rozgłoszeniowej (segmentu sieci)

Bridge



- W rozwiązaniach MikroTik mamy możliwość połączenia funkcjonalności routera i switcha w ramach jednego urządzenia
- Bridge w systemie RouterOS jest programowym odpowiednikiem fizycznego przełącznika
- Jeżeli którykolwiek z portów należy do **bridge-a**, to nie powinien on posiadać adresacji IP oraz usług typu klient, serwer DHCP.

*Jeżeli w danej sieci pracuje **bridge**, to serwer DHCP zawsze uruchamiamy na interfejsie typu **bridge** !!!*

Bridge

Bridge

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

Settings

| | Name | Type | L2 MTU | Tx | Rx |
|---|-----------------|--------|--------|------------|-----------|
| R | bridge-local | Bridge | 1598 | 531.7 kbps | 54.6 kbps |
| R | bridge-loopback | Bridge | 65535 | 0 bps | 0 bps |

2 items out of 14

Interface <bridge-local>

General STP VLAN Status Traffic

Name: bridge-local
Type: Bridge
MTU: [dropdown]
Actual MTU: 1500
L2 MTU: 1598
MAC Address: 74:4D:28:B4:A4:F5
ARP: enabled
ARP Timeout: [dropdown]
Admin. MAC Address: [dropdown]
Ageing Time: 00:05:00

IGMP Snooping
 DHCP Snooping
 Fast Forward

enabled running slave

| | FP Tx Packet (p/s) | FP Rx Packet (p/s) | MAC Address | Protoc... |
|-------|--------------------|--------------------|-------------------|-----------|
| 0 bps | 0 | 0 | 74:4D:28:B4:A4:F5 | none |
| 0 bps | 0 | 0 | A2:F9:D6:24:26:A5 | none |

Do bridge możemy dodać porty:

- fizyczne: ether1, ether2, wlan1 ...
- logiczne: eoip, vlan, ...

- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- Bridge**
- PPP
- Switch
- Mesh
- IP
- MPLS

Bridge

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

| # | Interface | Bridge | Horizon | Trusted | Priority (...) | Path Cost | Role | Root Pat... |
|---|-------------------|--------------|---------|---------|----------------|-----------|-----------------|-------------|
| 0 | H ether2 | bridge-local | | no | 80 | 10 | designated port | |
| 1 | IH ether3 | bridge-local | | no | 80 | 10 | disabled port | |
| 2 | I wlan1 | bridge-local | | no | 80 | 10 | disabled port | |
| 3 | I wlan2 | bridge-local | | no | 80 | 10 | disabled port | |
| 4 | IH ether4 | bridge-local | | no | 80 | 10 | disabled port | |
| 5 | IH ether5 | bridge-local | | no | 80 | 10 | disabled port | |
| 6 | D 5GHz-home-1 | bridge-local | | no | 80 | 10 | designated port | |
| 7 | DI 2GHz-home-1 | bridge-local | | no | 80 | 10 | disabled port | |
| 8 | D 2GHz-PWR-DOWN-1 | bridge-local | | no | 80 | 10 | designated port | |

9 items

Bridge Port <ether2>

General STP VLAN Status

Interface: ether2
Bridge: bridge-local
Horizon: [dropdown]
Learn: auto

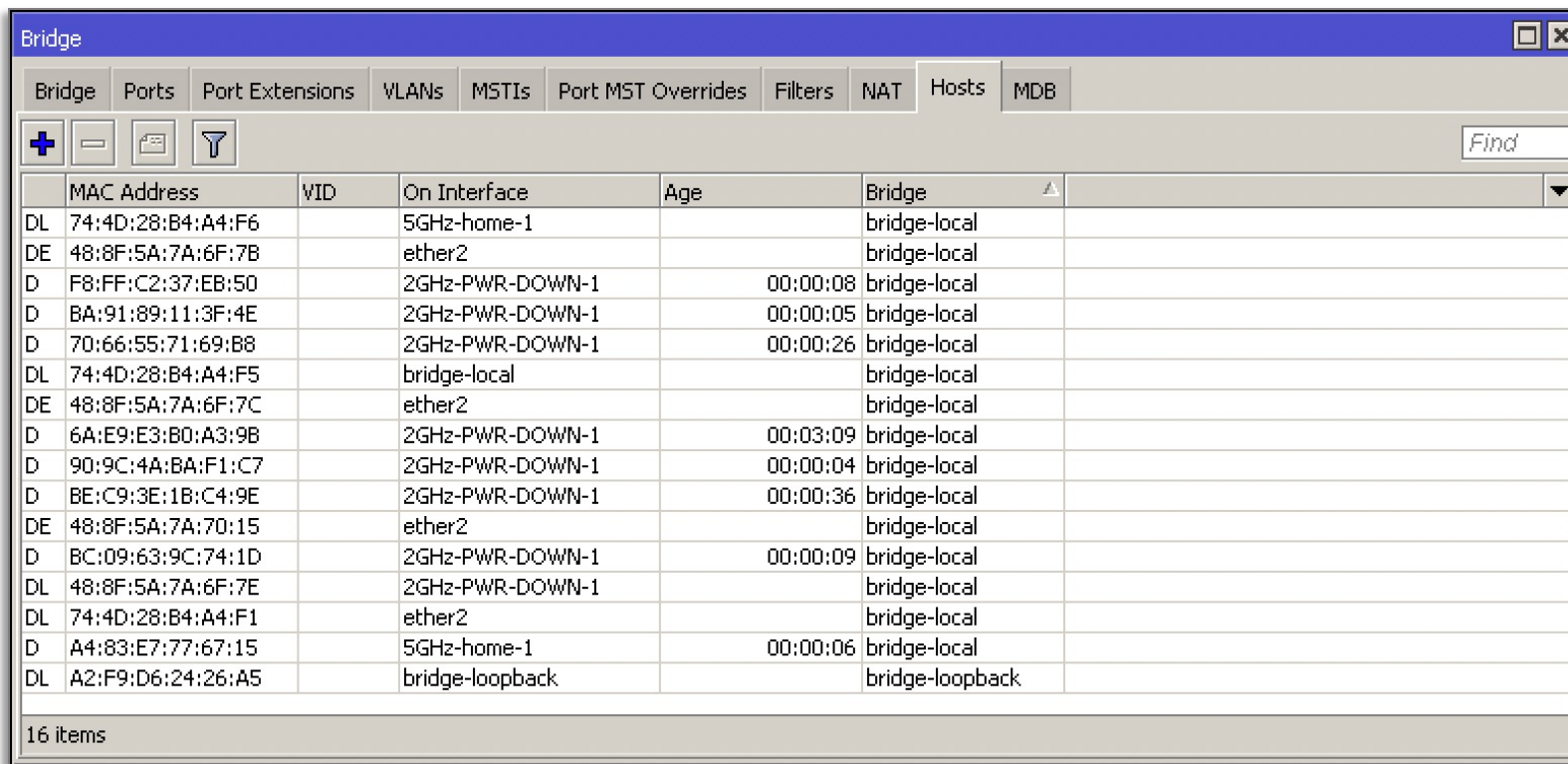
Unknown Unicast Flood
 Unknown Multicast Flood
 Broadcast Flood
 Trusted
 Hardware Offload
 Trusted

Multicast Router: Temporary Query
 Fast Leave

enabled inactive Hw. Offload

Bridge

Tablica MAC adresów bridge



The screenshot shows a window titled "Bridge" with a menu bar containing "Bridge", "Ports", "Port Extensions", "VLANs", "MSTIs", "Port MST Overrides", "Filters", "NAT", "Hosts", and "MDB". Below the menu bar are several icons: a plus sign, a minus sign, a document icon, and a funnel icon. To the right of these icons is a search box labeled "Find". The main area contains a table with the following columns: "MAC Address", "VID", "On Interface", "Age", and "Bridge". The table lists 16 items, each with a type (DL or D), a MAC address, a VID, an interface name, an age, and a bridge name.

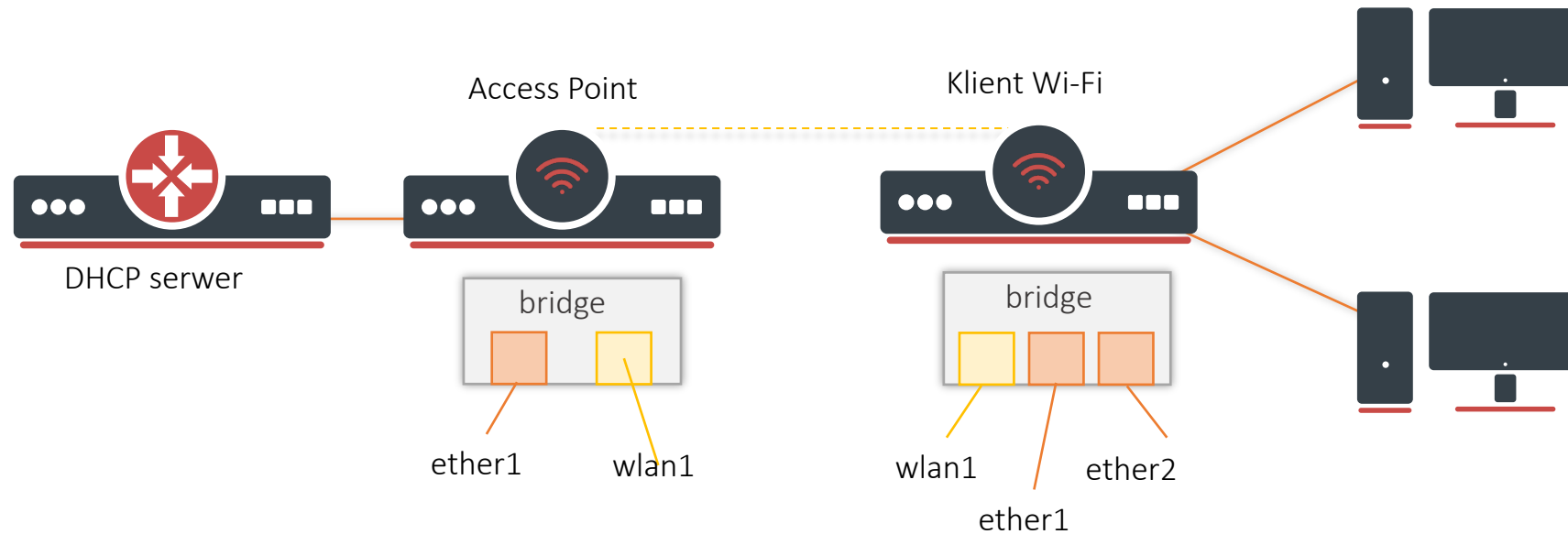
| | MAC Address | VID | On Interface | Age | Bridge |
|----|-------------------|-----|-----------------|----------|-----------------|
| DL | 74:4D:28:B4:A4:F6 | | 5GHz-home-1 | | bridge-local |
| DE | 48:8F:5A:7A:6F:7B | | ether2 | | bridge-local |
| D | F8:FF:C2:37:EB:50 | | 2GHz-PWR-DOWN-1 | 00:00:08 | bridge-local |
| D | BA:91:89:11:3F:4E | | 2GHz-PWR-DOWN-1 | 00:00:05 | bridge-local |
| D | 70:66:55:71:69:B8 | | 2GHz-PWR-DOWN-1 | 00:00:26 | bridge-local |
| DL | 74:4D:28:B4:A4:F5 | | bridge-local | | bridge-local |
| DE | 48:8F:5A:7A:6F:7C | | ether2 | | bridge-local |
| D | 6A:E9:E3:B0:A3:9B | | 2GHz-PWR-DOWN-1 | 00:03:09 | bridge-local |
| D | 90:9C:4A:BA:F1:C7 | | 2GHz-PWR-DOWN-1 | 00:00:04 | bridge-local |
| D | BE:C9:3E:1B:C4:9E | | 2GHz-PWR-DOWN-1 | 00:00:36 | bridge-local |
| DE | 48:8F:5A:7A:70:15 | | ether2 | | bridge-local |
| D | BC:09:63:9C:74:1D | | 2GHz-PWR-DOWN-1 | 00:00:09 | bridge-local |
| DL | 48:8F:5A:7A:6F:7E | | 2GHz-PWR-DOWN-1 | | bridge-local |
| DL | 74:4D:28:B4:A4:F1 | | ether2 | | bridge-local |
| D | A4:83:E7:77:67:15 | | 5GHz-home-1 | 00:00:06 | bridge-local |
| DL | A2:F9:D6:24:26:A5 | | bridge-loopback | | bridge-loopback |

16 items

Możemy ustalić do którego portu jest podłączone urządzenie klienta, pod warunkiem, że znamy MAC adres klienta.

Bridge

Dodawanie do bridge-a bezprzewodowych interfejsów



Aby móc połączyć dwie sieci w warstwie drugiej za pomocą mostu radiowego należy dodać interfejsy fizyczne przewodowe (ether1, ether2, ...) oraz wireless (wlan1) do bridge-a. Dodatkowo istotne jest ustawienie prawidłowego trybu pracy dla interfejsa wlan1 po stronie klienta sieci Wi-Fi.

| | | |
|-------------------|----------------------|---|
| | | |
| bridge, ap bridge | station | Brak komunikacji w L2 |
| bridge, ap bridge | station bridge | L2 działa, gdy AP i klient używają RouterOS |
| bridge, ap bridge | station pseudobridge | L2 działa z dowolnym AP |

Bridge

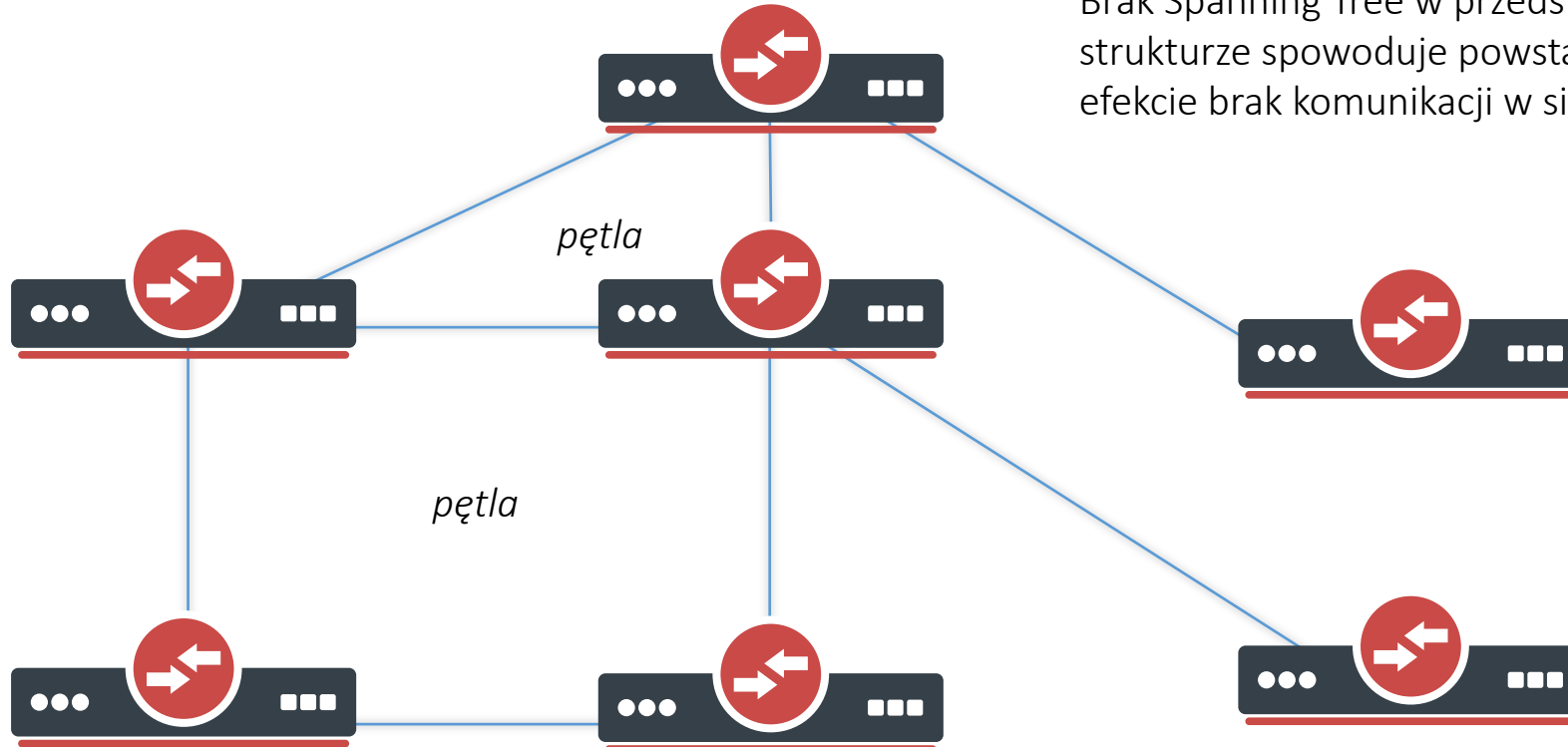
Spanning Tree Protocol

Protokoły z grupy Spanning Tree (Protokół drzewa rozpinającego) umożliwiają tworzenie redundantnej struktury między przełącznikami. Głównym zadaniem protokołu STP jest doprowadzenie sieci Ethernet z wieloma połączeniami do topologii drzewiastej (drzewo szkieletowe), co eliminuje powstawanie pętli. Odbywa się to poprzez automatyczne blokowanie obecnie nadmiarowych połączeń w celu zapewnienia pełnej łączności z portami.

- **Spanning Tree Protocol** — pierwsza wersja protokołu, potrzebuje na wykrywanie problemów lub rekonfiguracji topologii od 30 do 60 sekund
- **Rapid Spanning Tree Protocol** — zapewnia krótszy czas przywracania sprawności połączeń po awarii
- **MSTP** – wsparcie dla vlan, umożliwia równoważenie obciążenia i zwiększa odporność sieci na błędy dzięki zapewnieniu wielu ścieżek przekazywania ruchu danych
- **PVSTP** – wsparcie dla vlan, zamknięte rozwiązanie Cisco (nie jest wspierane MikroTik)

Bridge

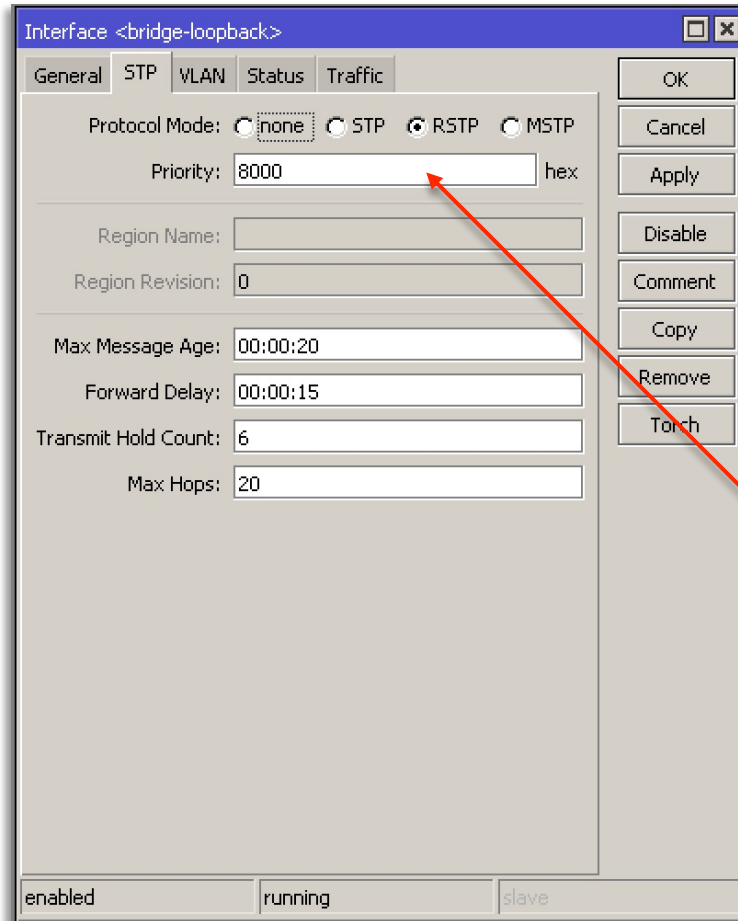
Spanning Tree Protocol



Brak Spanning Tree w przedstawionej strukturze spowoduje powstanie pętli i w efekcie brak komunikacji w sieci.

Bridge

Spanning Tree Protocol



The screenshot shows the configuration window for a bridge interface, titled "Interface <bridge-loopback>". The "STP" tab is selected. The "Protocol Mode" is set to "RSTP" (checked). The "Priority" is set to "8000" in a text box, with a red arrow pointing to it. Other fields include "Region Name", "Region Revision" (0), "Max Message Age" (00:00:20), "Forward Delay" (00:00:15), "Transmit Hold Count" (6), and "Max Hops" (20). The status bar at the bottom shows "enabled", "running", and "slave".

Elekcja Root Bridge

Najważniejszym przełącznikiem w strukturze STP jest Root Bridge, to on będzie obsługiwał największą część ruchu w sieci, należy w sposób przemyślany zaplanować, który z przełączników w naszej sieci powinien pełnić tę funkcję.

Root Bridge zostanie przełącznik posiadający najniższy numer **Bridge ID**.

Bridge ID to 8 bajtowe pole składające się z:

- Priorytetu (domyślnie 0x8000) hex
- MAC adres

Domyślnie każdy interface typu bridge ma włączoną obsługę protokołu **Rapid Spanning Tree**

ROUTING

Routing

Adres IPv4

- Adres IP zapisany jest w postaci dziesiętnej rozdzielonej kropkami 192.168.20.5
- Z punktu widzenia urządzeń sieciowych adres IP — to 32 bity *11000000
10101000 00010100 00000101*
- Adresując urządzenie należy pamiętać aby zawsze podać maskę sieci, w której urządzenie pracuje. Jest to niezbędne, aby urządzenie wiedziało, czy dany ruch powinno wysłać do routera czy też lokalnie za pomocą protokołu ARP
- Ze względu na rodzaj przeznaczenia adresy dzielimy na **zewnętrzne** lub **publiczne**, **wewnętrzne (prywatne)**, stosowane w ramach naszej organizacji oraz **adresy specjalnego przeznaczenia** np. **loopback**
- Każda sieć zawsze posiada dodatkowo dwa zarezerwowane adresy: **adres sieci (network address)**, oraz **adres rozgłoszeniowy (broadcast address)**

Routing

Adres IPv4

1. Prywatna adresacja – opisana w dokumencie *RFC 1918*

- 10.0.0.0 – 10.255.255.255 lub 10.0.0.0/8 (255.0.0.0)
- 172.16.0.0 – 172.31.255.255 lub 172.16.0.0/12 (255.240.0.0)
- 192.168.0.0 – 192.168.255.255 lub 192.168.0.0/16 (255.255.0.0)

2. Adresy specjalnego przeznaczenia

- 127.0.0.0/8 loopback, zdefiniowano w *RFC 1122*
- 169.254.0.0/16 link local adresacja, *RFC 3927*

Więcej adresów specjalnego przeznaczenia opublikowano na stronie:

<https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml>

Przykład:

Adres sieci: 192.168.10.0

Maska sieci: 255.255.255.240 lub w notacji CIDR /28

Adres rozgłoszeniowy: 192.168.10.15

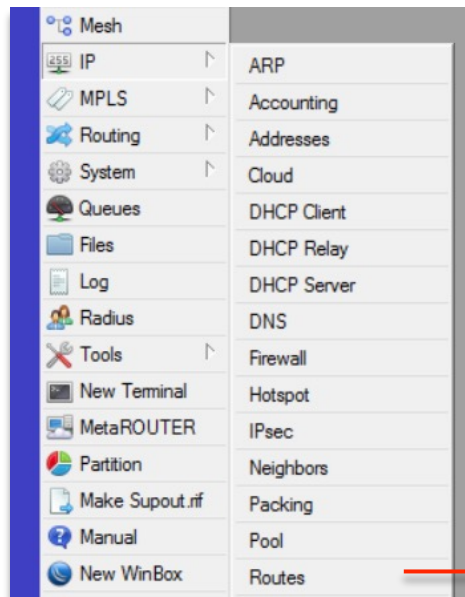
Adresy, które możemy użyć do zaadresowania hostów (usable addresses): 192.168.10.1-192.168.10.14

Routing

Tablica routing'u

Każde urządzenie posiadające adres IP, posiada również tablicę routing'u

- Windows - ***route print***
- Linux - ***ip route show***
- RouterOS - ***/ip route print***
- MacOS - ***netstat -nr***



The 'Route List' window displays a table of routing entries. The table has the following columns: Dst. Address, Gateway, Distance, Routing Mark, and Pref. Source. The entries are as follows:

| Dst. Address | Gateway | Distance | Routing Mark | Pref. Source |
|-----------------------|---|----------|--------------|----------------|
| AS ▶ 0.0.0.0/0 | 192.168.23.254 reachable wlan3-WAN | 1 | | |
| DAC ▶ 2.2.2.0/24 | bridge-sstp reachable | 0 | | 2.2.2.2 |
| DAo ▶ 10.8.0.1 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAo ▶ 10.250.1.0/24 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAo ▶ 127.1.1.250 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAC ▶ 157.25.99.64/29 | bridge1-lan reachable | 0 | | 157.25.99.65 |
| DAC ▶ 172.16.10.100 | ssstp-out-vult-chr-frankfurt reachable | 0 | | 172.16.10.101 |
| DAo ▶ 172.16.10.101 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAo ▶ 172.16.100.1 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAo ▶ 172.16.100.2 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAC ▶ 172.20.20.1 | korkowa-dom reachable | 0 | | 172.20.20.2 |
| DAo ▶ 192.168.1.0/24 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAC ▶ 192.168.5.0/24 | bridge1-lan reachable | 0 | | 192.168.5.254 |
| DAC ▶ 192.168.23.0/24 | wlan3-WAN reachable | 0 | | 192.168.23.100 |
| AS ▶ 192.168.50.0/24 | 172.20.20.1 reachable korkowa-dom | 1 | | |

16 items

Routing

Sieci bezpośrednio podłączone do router'a / host'a

Address <192.168.230.5/24>

Address: 192.168.230.5/24

Network:

Interface: bridge1-lan

OK
Cancel
Apply
Disable
Comment
Copy
Remove

enabled

Address List

| Address | Network | Interface |
|-------------------|---------------|-----------------------------|
| BRIDGE_SSTP | | |
| 2.2.2.2/24 | 2.2.2.0 | bridge-sstp |
| BIURO | | |
| X 10.10.10.1/24 | 10.10.10.0 | vlan10 |
| GOSCIE | | |
| X 10.10.20.1/24 | 10.10.20.0 | vlan20 |
| TMOBILE | | |
| 157.25.99.65/29 | 157.25.99.64 | ether2 |
| D 172.16.10.101 | 172.16.10.100 | sstp-out-vult-chr-frankfurt |
| D 172.20.20.2 | 172.20.20.1 | korkowa-dom |
| LAN | | |
| 192.168.5.254/24 | 192.168.5.0 | bridge1-lan |
| WAN | | |
| 192.168.23.100/24 | 192.168.23.0 | wlan3-WAN |
| 192.168.230.5/24 | 192.168.230.0 | bridge1-lan |

9 items (1 selected)

Route List

| Dist. Address | Gateway | Distance | Routing Mark | Pref. Source |
|----------------------|---|----------|--------------|----------------|
| AS 0.0.0.0/0 | 192.168.23.254 reachable wlan3-WAN | 1 | | |
| DAC 2.2.2.0/24 | bridge-sstp reachable | 0 | | 2.2.2.2 |
| DAo 10.8.0.1 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAo 10.250.1.0/24 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAo 127.1.1.250 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAC 157.25.99.64/29 | bridge1-lan reachable | 0 | | 157.25.99.65 |
| DAC 172.16.10.100 | sstp-out-vult-chr-frankfurt reachable | 0 | | 172.16.10.101 |
| DAo 172.16.10.101 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAo 172.16.100.1 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAo 172.16.100.2 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAC 172.20.20.1 | korkowa-dom reachable | 0 | | 172.20.20.2 |
| DAo 192.168.1.0/24 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAC 192.168.5.0/24 | bridge1-lan reachable | 0 | | 192.168.5.254 |
| DAC 192.168.23.0/24 | wlan3-WAN reachable | 0 | | 192.168.23.100 |
| AS 192.168.50.0/24 | 172.20.20.1 reachable korkowa-dom | 1 | | |
| DAC 192.168.230.0/24 | bridge1-lan reachable | 0 | | 192.168.230.5 |
| AS 213.52.130.173 | 172.20.20.1 reachable korkowa-dom | 1 | | |

17 items

Po dodaniu adresy IP urządzenie automatycznie, na podstawie adresu i maski sieci, doda wpis do tablicy routing'u, który wskaże, iż pakiety do sieci 192.168.230.0/24 powinny być skierowane na interfejs bridge1-lan.

Routing

Tablica routing'u: flagi, parametr distance

- *X* – Trasa wyłączona administracyjnie
- *A* – Trasa aktywna
- *D* – Wpis dodano w sposób dynamiczny, na przykład otrzymany za pomocą DHCP
- *C* – Trasa bezpośrednio podłączona do naszego routera, powiązana z adresem IP jaki nadaliśmy na interfejs
- *S* – Trasa statyczna
- *r* – Wpis dodany za pomocą RIP
- *b* – Wpis dodany za pomocą BGP
- *o* – Wpis dodany za pomocą OSPF
- *m* – Wpis dodany za pomocą MME
- *B* – Blackhole, dostęp zablokowany
- *U* – Niedostępny
- *P* – Zabroniony

| | Dist. Address | Gateway | Distance | Routing Mark | Pref. Source |
|-----|-----------------|---|----------|--------------|----------------|
| AS | 0.0.0.0/0 | 192.168.23.254 reachable wlan3-WAN | 1 | | |
| DAC | 2.2.2.0/24 | bridge-sstp reachable | 0 | | 2.2.2.2 |
| DAo | 10.8.0.1 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAo | 10.250.1.0/24 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAo | 127.1.1.250 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAC | 157.25.99.64/29 | bridge1-lan reachable | 0 | | 157.25.99.65 |
| DAC | 172.16.10.100 | sstp-out-vult-chr-frankfurt reachable | 0 | | 172.16.10.101 |
| DAo | 172.16.10.101 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAo | 172.16.100.1 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAo | 172.16.100.2 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAC | 172.20.20.1 | korkowa-dom reachable | 0 | | 172.20.20.2 |
| DAo | 192.168.1.0/24 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAC | 192.168.5.0/24 | bridge1-lan reachable | 0 | | 192.168.5.254 |
| DAC | 192.168.23.0/24 | wlan3-WAN reachable | 0 | | 192.168.23.100 |
| AS | 192.168.50.0/24 | 172.20.20.1 reachable korkowa-dom | 1 | | |

Im niższa jest wartość parametru **distance**, tym wyższy priorytet ma trasa
Domyślne wartości:

- Połączony bezpośrednio – distance 0
- Dodany dynamicznie (DHCP, PPP) – distance 1
- Statyczny, dodany ręcznie – distance 1
- OSPF – distance 110
- BGP – distance 20
- IGRP – distance 100

Routing

Tablica routing'u: kolejność przetwarzania wpisów

| | Dst. Address | Gateway | Distance | Routing Mark | Pref. Source |
|-----|------------------|---|----------|--------------|----------------|
| AS | 0.0.0.0/0 | 192.168.23.254 reachable wlan3-WAN | 1 | | |
| S | 0.0.0.0/0 | 192.168.230.1 reachable bridge1-lan | 5 | | |
| DAC | 2.2.2.0/24 | bridge-sstp reachable | 0 | | 2.2.2.2 |
| DAo | 10.8.0.1 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| AS | 10.20.100.0/23 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 10 | | |
| AS | 10.20.100.0/24 | 192.168.23.254 reachable wlan3-WAN | 1 | | |
| DAo | 10.250.1.0/24 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAo | 127.1.1.250 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAC | 157.25.99.64/29 | bridge1-lan reachable | 0 | | 157.25.99.65 |
| DAC | 172.16.10.100 | sstp-out-vult-chr-frankfurt reachable | 0 | | 172.16.10.101 |
| DAo | 172.16.10.101 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAo | 172.16.100.1 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAo | 172.16.100.2 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAC | 172.20.20.1 | korkowa-dom reachable | 0 | | 172.20.20.2 |
| DAo | 192.168.1.0/24 | 172.16.10.100 reachable sstp-out-vult-chr-frankfurt | 110 | | |
| DAC | 192.168.5.0/24 | bridge1-lan reachable | 0 | | 192.168.5.254 |
| DAC | 192.168.23.0/24 | wlan3-WAN reachable | 0 | | 192.168.23.100 |
| AS | 192.168.50.0/24 | 172.20.20.1 reachable korkowa-dom | 1 | | |
| DAC | 192.168.230.0/24 | bridge1-lan reachable | 0 | | 192.168.230.5 |

Przykład 1

Do routera trafia pakiet IP z adresem docelowym 8.8.8.8, pakiet zostanie skierowany zgodnie z tablicą routing'u na router o adresie: 192.168.23.254

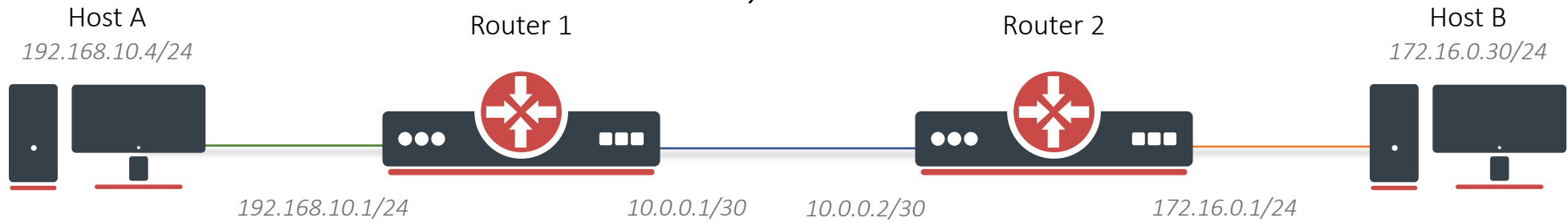
Przykład 2

Router chce się dostać do adresu 192.168.5.113, z tablic routing'u wynika, iż najlepszym wpisem do edycji tego ruchu będzie sieć własna 192.168.5.0/24, dlatego router wykorzystuje protokół ARP dla dostarczenia pakietu.

Najpierw pod uwagę bierze się szczegółowość wpisu (czyli dla adresu 10.20.100.10 najlepszym wariantem będzie 10.20.100.0/24 niż 10.20.100.0/23), jedynie dla wpisów z taką samą szczegółowością będzie sprawdzać się parametr (w tym przykładzie 0.0.0.0/0) **distance**

Routing

Przykład



Router 1

Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit

| # | DST-ADDRESS | PREF-SRC | GATEWAY | DISTANCE |
|-------|-----------------|--------------|----------|----------|
| 0 A S | 0.0.0.0/0 | | 10.0.0.2 | 1 |
| 1 ADC | 10.0.0.0/30 | 10.0.0.1 | ether2 | 0 |
| 2 ADC | 192.168.10.0/24 | 192.168.10.1 | ether1 | 0 |

Router 2

Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit

| # | DST-ADDRESS | PREF-SRC | GATEWAY | DISTANCE |
|-------|---------------|------------|----------|----------|
| 0 A S | 0.0.0.0/0 | | 10.0.0.1 | 1 |
| 1 ADC | 10.0.0.0/30 | 10.0.0.2 | ether2 | 0 |
| 2 ADC | 172.16.0.0/24 | 172.16.0.1 | ether1 | 0 |

Wpisy w tablicach routingu każdego z routerów

Routing

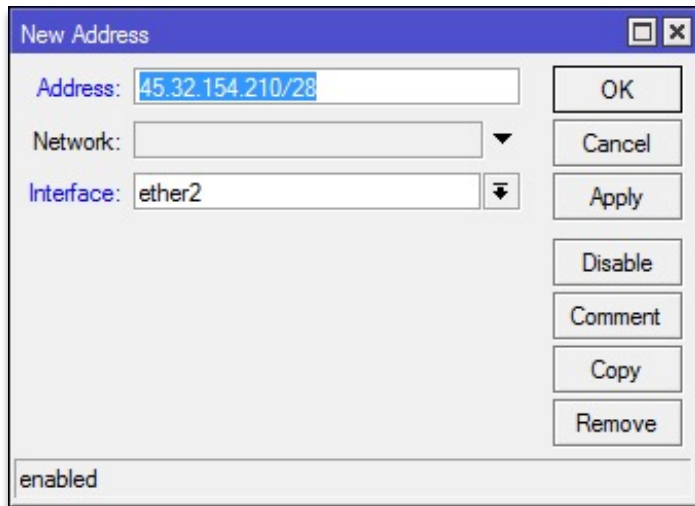
Dodawanie tras routing'u / brama domyślna / default gateway

Dostawca Internetu:

Network: 45.32.154.208/28

Gateway: 45.32.154.209

DNS: 8.8.8.8

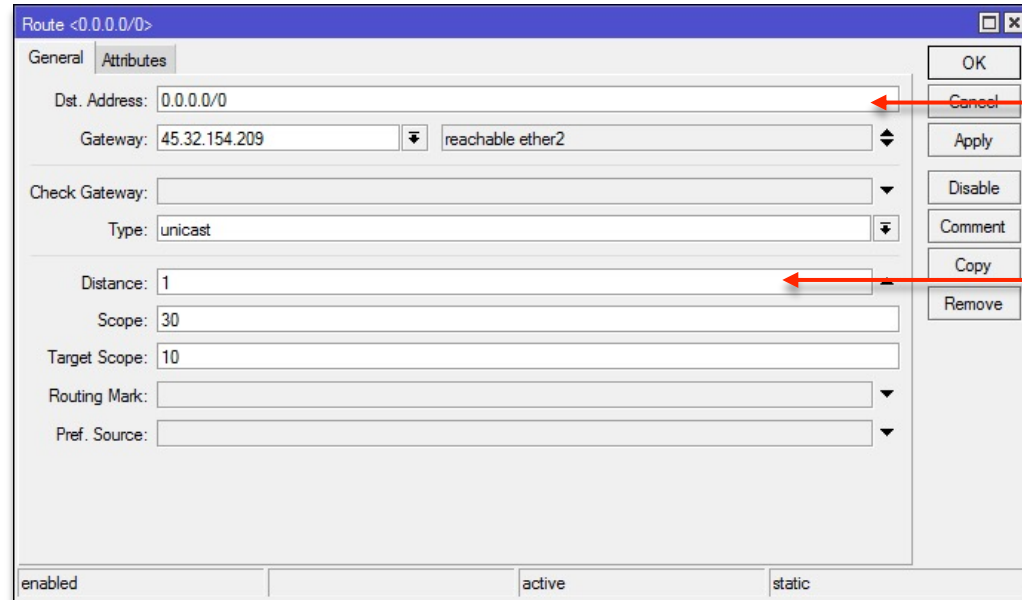


New Address dialog box with the following fields and values:

- Address: 45.32.154.210/28
- Network: (empty)
- Interface: ether2

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove. Status: enabled

Konfigurujemy adres IP na naszym routerze



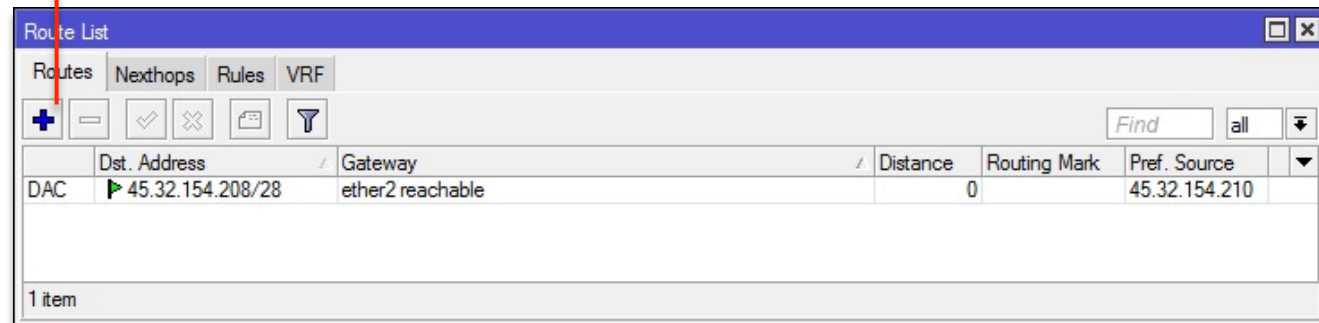
Route <0.0.0.0/0> dialog box with the following fields and values:

- General tab selected
- Dst. Address: 0.0.0.0/0
- Gateway: 45.32.154.209 reachable ether2
- Type: unicast
- Distance: 1
- Scope: 30
- Target Scope: 10
- Routing Mark: (empty)
- Pref. Source: (empty)

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove. Status: enabled, active, static

0.0.0.0/0 default gateway

Trasa dodana ręcznie, parametr **distance** domyślnie ustawiony na 1



Route List window showing a table of routes:

| | Dst. Address | Gateway | Distance | Routing Mark | Pref. Source |
|-----|------------------|------------------|----------|--------------|---------------|
| DAC | 45.32.154.208/28 | ether2 reachable | 0 | | 45.32.154.210 |

1 item

Routing

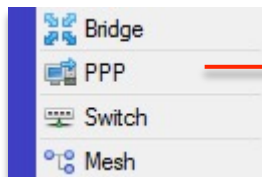
Dodawanie tras routing'u / Dual WAN

| | Dst. Address | Gateway | Distance | Routing Mark | Pref. Source |
|-----|------------------|--------------------------------|----------|--------------|---------------|
| S | 0.0.0.0/0 | 45.32.154.209 reachable ether2 | 1 | | |
| DAS | 0.0.0.0/0 | ppp-out2 reachable | 1 | | |
| DAC | 10.112.112.128 | ppp-out2 reachable | 0 | | 10.187.170.92 |
| DAC | 45.32.154.208/28 | ether2 reachable | 0 | | 45.32.154.210 |

Trasa dodana ręcznie z **distance 1**

Trasa dodana automatycznie, w tym wypadku modem LTE *ppp*. Trasy dodane dynamicznie (dhcp client, ppp) domyślnie mają parametr **distance** ustawiony w 1

W danym przykładzie głównym kanałem sieci może być modem LTE (trasy mają taki sam **distance**). Żeby wybrać główny link za pomocą połączenia kablowego musimy zmienić **distance** dla połączenia LTE, na wartość większą niż 1



| | Name | Type | Actual MTU | L2 MTU | Tx |
|---|----------|------------|------------|--------|----|
| X | ppp-out1 | PPP Client | | | |
| R | ppp-out2 | PPP Client | 1500 | | |

Interface <ppp-out2>

General | PPP | Status | Traffic

User:

Password:

Remote Address:

Keepalive Timeout:

Dial On Demand

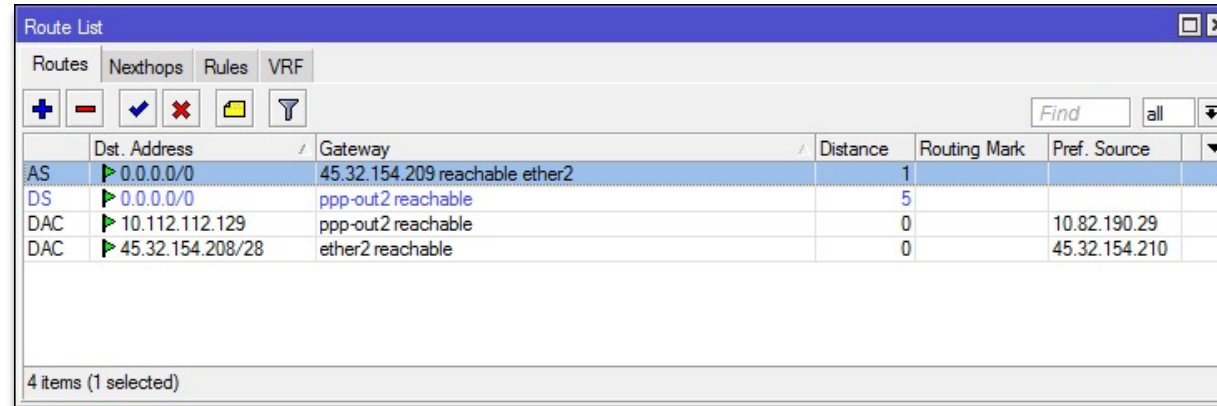
Use Peer DNS

Add Default Route

Default Route Distance:

Routing

Dodawanie tras routing'u / Check gateway / Sprawdzanie bramy

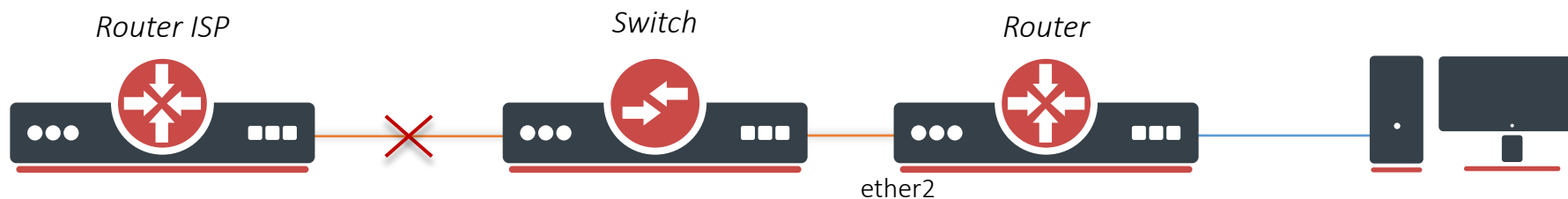


The screenshot shows a 'Route List' window with a table of routing entries. The table has columns for 'Dist. Address', 'Gateway', 'Distance', 'Routing Mark', and 'Pref. Source'. The first row is selected and highlighted in blue.

| | Dist. Address | Gateway | Distance | Routing Mark | Pref. Source |
|-----|------------------|--------------------------------|----------|--------------|---------------|
| AS | 0.0.0.0/0 | 45.32.154.209 reachable ether2 | 1 | | |
| DS | 0.0.0.0/0 | ppp-out2 reachable | 5 | | |
| DAC | 10.112.112.129 | ppp-out2 reachable | 0 | | 10.82.190.29 |
| DAC | 45.32.154.208/28 | ether2 reachable | 0 | | 45.32.154.210 |

4 items (1 selected)

Podstawowy Default Gateway przełączy się na modem LTE jedynie w przypadku, gdy łącze podstawowe zostanie wyłączone elektrycznie (nie połączony lub uszkodzony kabel)



W wypadku awarii routera naszego ISP, modem LTE nie zostanie głównym łączem, gdyż interfejs **ether2** z punktu widzenia routera jest w stanie aktywnym.

Aby rozwiązać ten problem, możemy skorzystać z mechanizmu **Check Gateway**

Routing

Dodawanie tras routing'u / Check gateway / Sprawdzenie bramy

Route <0.0.0.0/0>

General Attributes

Dst. Address: 0.0.0.0/0

Gateway: 45.32.154.209 reachable ether2

Check Gateway: ping
arp
ping

Type: ping

Distance: 1

Scope: 30

Target Scope: 10

Routing Mark:

Pref. Source:

OK
Cancel
Apply
Disable
Comment
Copy
Remove

enabled active static

Check Gateway ping:

- Co 10 sekund router wysyła komunikat Echo Request (ping) do gateway'a!
- Brak odpowiedzi na 2 komunikaty Echo Request pod rząd jest przyczyną uznania gateway'a za niedostępny !

WIRELESS

WIRELESS

Standardy

| | | | | |
|----------|--------------|--------------|------------------|------|
| | | | | |
| 802.11a | 5GHz | 54 Mbps | 20 MHz | 1999 |
| 802.11b | 2GHz | 11 Mbps | 22 MHz | 1999 |
| 802.11g | 2GHz | 54 Mbps | 20 MHz | 2003 |
| 802.11n | 2 oraz 5 GHz | do 450 Mbps | 20/40 MHz | 2006 |
| 802.11ac | 5GHz | do 1300 Mbps | 20/40/80/160 MHz | 2012 |

Nstream – standard MikroTik

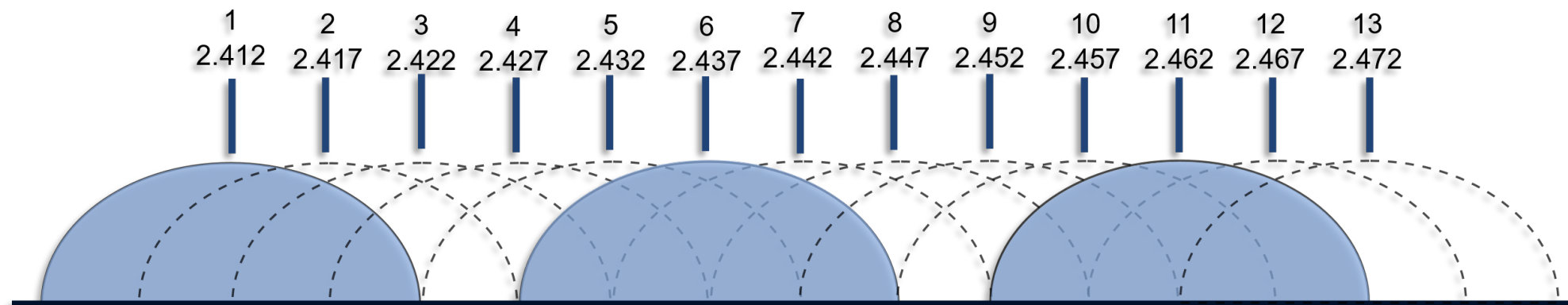
Nstream Dual – standard MikroTik

NV2 – standard MikroTik, oparty na TDMA (podział na szczeliny czasowe), eliminuje problemy spotykane w 802.11, a mianowicie **CSMA/CA***

**CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance*

WIRELESS

Kanały 2,4 GHz

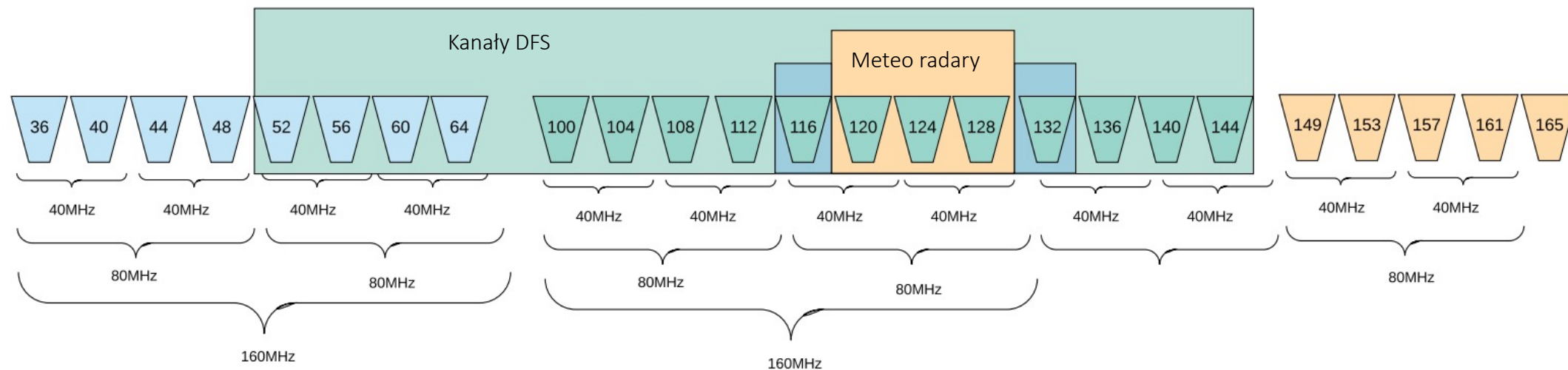


Tylko 3 nie pokrywające się kanały !!!

US- tylko 11 kanałów, Japonia- 14 kanałów

WIRELESS

Канали 5 GHz



25 nie pokrywające się kanałów
Uwaga na DFS (dynamic frequency selection) !!!

WIRELESS

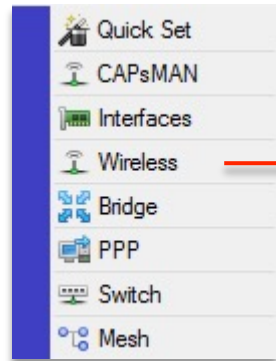
Ustawienia

Gdzie możemy się podłączyć, a gdzie nie (jako klient WiFi)

- MAC adres
- SSID
- ...

Hasła PSK, Radius

- WPA, WPA2
- AES, TKIP
- ...



A screenshot of the 'Wireless Tables' window in Mikrotik WinBox. The window has several tabs: 'Interfaces', 'Nstreme Dual', 'Access List', 'Registration', 'Connect List', 'Security Profiles', and 'Channels'. Below the tabs are several sub-tabs: 'CAP', 'WPS Client', 'Setup Repeater', 'Scanner', 'Freq. Usage', 'Alignment', 'Wireless Sniffer', and 'Wireless Snooper'. A table is displayed with columns: Name, Type, Actual MTU, Tx, Rx, Tx Packet (p/s), Rx Packet (p/s), FP Tx, and FP Rx. Two rows are visible, both for 'wlan1' and 'wlan2' interfaces.

| Name | Type | Actual MTU | Tx | Rx | Tx Packet (p/s) | Rx Packet (p/s) | FP Tx | FP Rx |
|-------|--------------------------|------------|-------|-------|-----------------|-----------------|-------|-------|
| wlan1 | Wireless (Atheros AR9... | 1500 | 0 bps | 0 bps | 0 | 0 | 0 bps | 0 bps |
| wlan2 | Wireless (Atheros AR9... | 1500 | 0 bps | 0 bps | 0 | 0 | 0 bps | 0 bps |

Ustawienia modułu radiowego

- SSID
- Moc nadawania
- Częstotliwość
- Kanał
- Tryb pracy
- ...

Kto może podłączyć się do Access Point'a (AP)

- WPA, WPA2
- MAC adres
- Dodatkowe ograniczenia
- Blokowanie dostępu
- ...

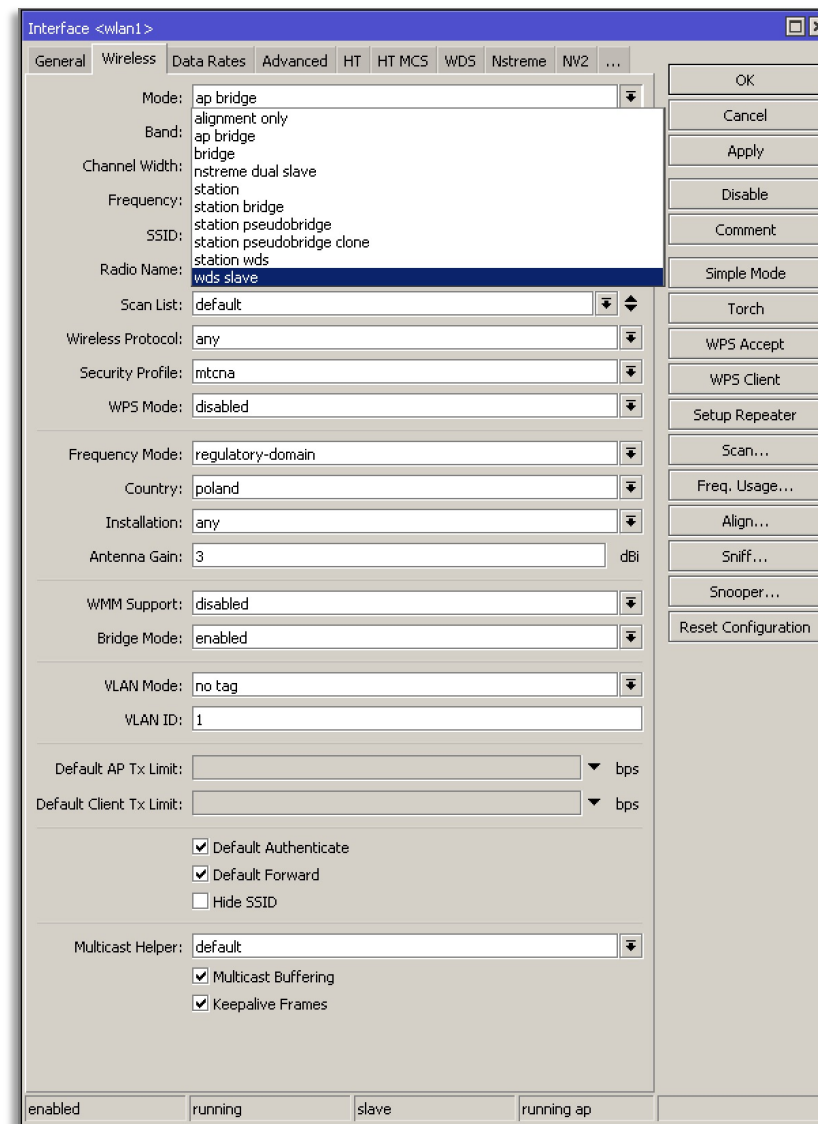
Informacja o podłączonych klientach oraz do kogo my podłączeni jako klient

- Moc sygnału
- Modulacja
- Jakość połączenia
- ...

WIRELESS

Tryby pracy

- **station** – klient sieci WiFi, możemy podłączyć się do innego AP (Access Point - AP)
- **station bridge** – klient sieci WiFi, interfejs możemy dodać do bridge'a (tylko kiedy się łączymy do innego MikroTik'a)
- **station pseudobridge** – klient sieci WiFi, interfejs możemy dodać do bridge'a
- **station wds**
- **wds slave**
- **bridge** – rodzaj AP, służy dla połączeń typu Punkt-Punkt, w takim trybie istnieje możliwość podłączenia **tylko jednego klienta!**
- **ap bridge** – AP, maksymalna liczba klientów, który mogą się podłączyć - 2007 !
- **alignment only** – wizowanie anten



WIRELESS

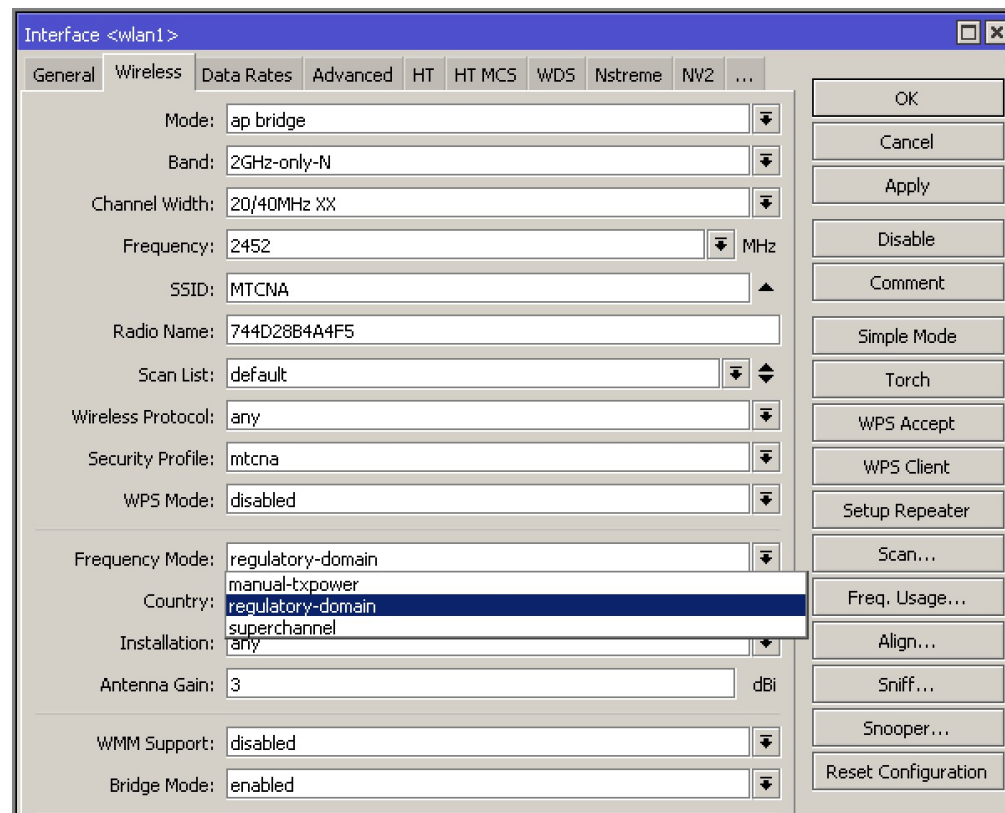
Częstotliwości wspierane przez kartę

Pełny zakres częstotliwości wspierany przez kartę:

- dla 2,4 GHz: 2192 MHz – 2539 MHz
- dla 5 GHz: 4920 MHz – 6100 MHz

Tryb częstotliwości:

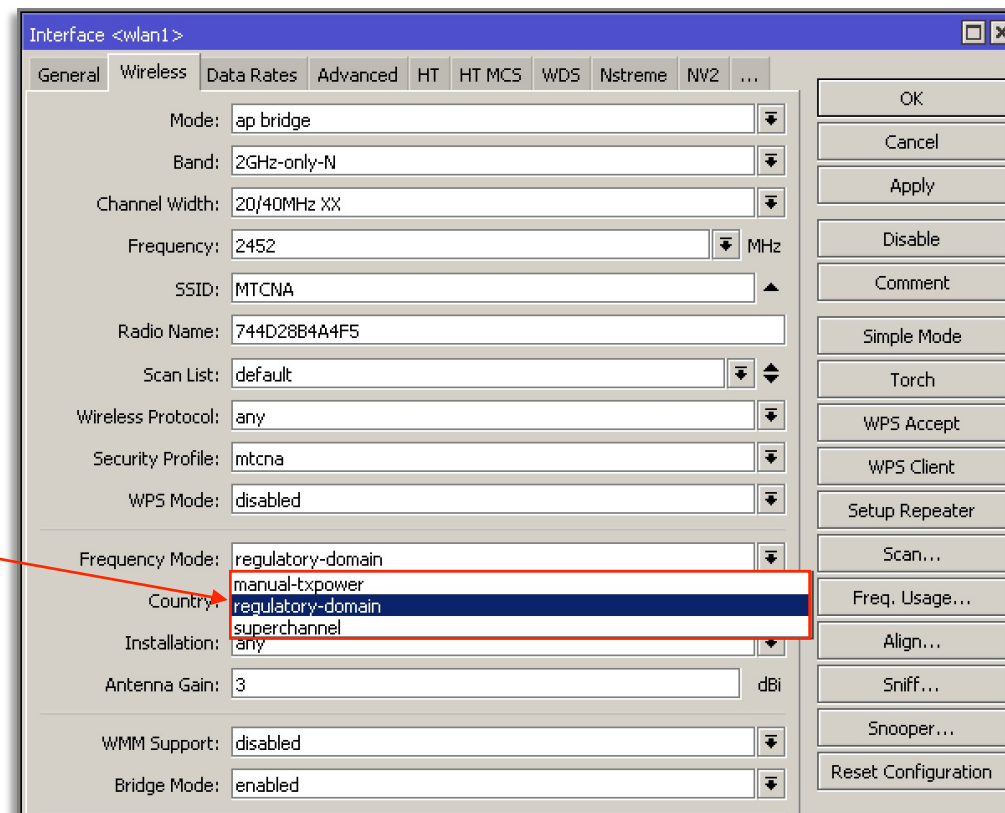
- **superchannel** – brak żadnych ograniczeń
- **regulatory-domain** – ogranicza częstotliwości i moce jakie są dozwolone, trzeba wskazać **Country**
- **manual-txpower** – ogranicza zakres częstotliwości ale pozwala na ustawienie mocy nadawania



WIRELESS

Moc nadawania / ręczne ustawienie

Aby móc ręcznie dobrać moc modułu radiowego należy zmienić parametr *Frequency Mode* na *superchannel* lub *manual-txpower*

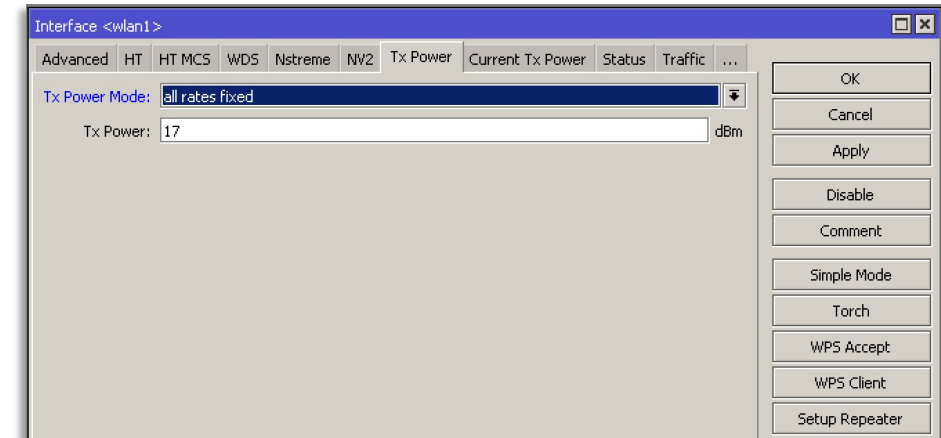
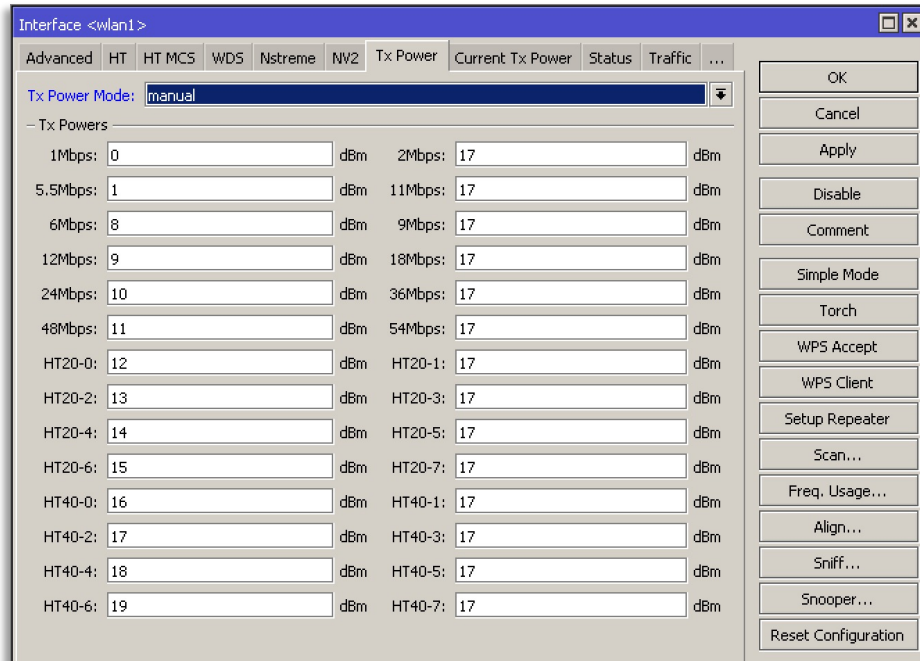
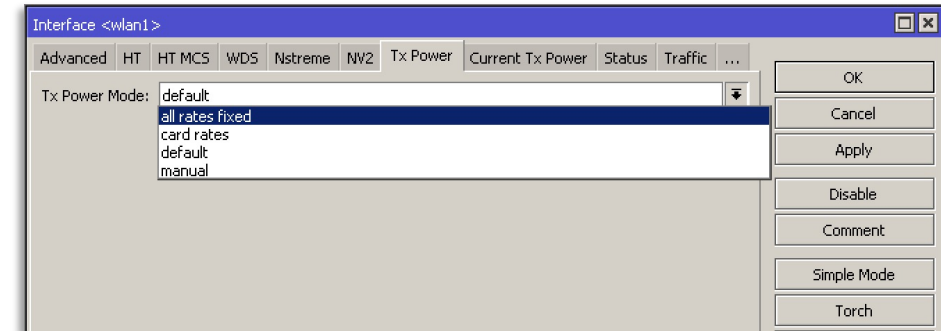


WIRELESS

Moc nadawania / ręczne ustawienie

Na zakładce **Tx Power** możemy wybrać następujące tryby:

- **all rates fixed** - moc nadawania będzie jednakowa dla wszystkich modulacji
- **manual** - można ustawić moc nadawania dla każdej modulacji osobno (można uszkodzić moduł, jeżeli wpisać większą wartość niż wspiera karta)



WIRELESS

Moc nadawania / reguła «3» oraz «10»

Z każdym wzrostem mocy o 3 dB, moc w mW podwaja się

Gdy moc jest zmniejszona o 3 dB, moc w mW zmniejsza się o połowę

Z każdym wzrostem mocy o 10 dB moc w mW jest mnożona przez 10

Gdy moc jest zmniejszona o 10 dB, moc w mW jest dzielona przez 10

Przykład: mamy AP, który wysyła sygnał z mocą 100 mW.

Podłączamy antenę ze wzmocnieniem 3 dB.

Całkowita moc nadawania będzie: $100 \text{ mW} + 3 \text{ dB} = 100 \times 2 = 200 \text{ mW}$

WIRELESS

Radio Name

Radio Name - nazwa bezprzewodowego interfejsu, używana **wyłącznie w RouterOS**

Channel Width: 20MHz
Frequency: 2452 MHz
SSID: home2
Radio Name: B869F4C95B5E
Scan List: default

Apply
Disable
Comment
Simple Mode
Torch

Można podejrzeć w *Registration Table*

| Radio Name | MAC Address | Interface | Uptime | AP | ... | Last Activity (s) | Tx/Rx Signal ... | Tx Rate | Rx Rate |
|--------------|-------------------|-----------|----------|----|-----|-------------------|------------------|------------------------|------------------|
| B869F4C95B5E | B8:69:F4:C9:5B:5E | wlan1 | 00:02:06 | no | no | 1.050 | -42/-38 | 1Mbps | 6Mbps |
| | 6C:72:E7:92:B0:36 | wlan2 | 00:00:11 | no | no | 2.600 | -46 | 6Mbps | 6.5Mbps-20MHz/15 |
| | 6C:40:08:96:E4:F4 | wlan2 | 00:19:57 | no | no | 0.000 | -45 | 866.6Mbps-80MHz/25/SGI | 585Mbps-80MHz/25 |

3 items

WIRELESS

Zarządzanie podłączaniem się klientów / Access List/Connect List

Access List – lista przetwarzana jako pierwsza, ~~sekwencyjnie~~ →

Default Authenticate – gdy klient nie jest zdefiniowany w Access List, sprawdzany jest Security Profile, odznaczenie tej opcji spowoduje, iż klienci, którzy nie znaleźli się w Access List nie będą mogli się podłączyć

Connect List – lista sieci/AP do których MikroTik może podłączyć się jako klient

Default Forward - określa czy możliwa jest komunikacja pomiędzy klientami AP →

New AP Access Rule

MAC Address:

Interface: all

Signal Strength Range: -120..120

AP Tx Limit:

Client Tx Limit:

Authentication

Forwarding

VLAN Mode: no tag

VLAN ID: 1

Private Key: none

Private Pre Shared Key:

Management Protection Key:

Time:

enabled

New Station Connect Rule

Interface: wlan1

MAC Address:

Connect

SSID:

Area Prefix:

Signal Strength Range: -120..120

Wireless Protocol: any

Security Profile: default

enabled

Interface <wlan1>

General Wireless Data Rates Advanced HT HT MCS WDS Nstream

Mode: ap bridge

Band: 2GHz-G/N

Default Authenticate

Default Forward

Hide SSID

WIRELESS

Ustawienia

Wspierany standardy

auto- urządzenie
dobrze częstotliwość,
która jest najmniej zajęta

Ograniczenie prędkości Upload
podłączonego klienta

The screenshot shows the 'Interface <wlan2>' configuration window with the 'Wireless' tab selected. The 'Mode' is set to 'ap bridge'. The 'Band' is '5GHz-A/N/AC', 'Channel Width' is '20MHz', and 'Frequency' is 'auto'. The 'SSID' is 'mtcna'. The 'Wireless Protocol' is '802.11'. The 'Security Profile' is 'default'. The 'WPS Mode' is 'push button'. The 'Frequency Mode' is 'regulatory-domain' and 'Country' is 'poland'. The 'Antenna Gain' is '0'. 'WMM Support' is 'disabled' and 'Bridge Mode' is 'enabled'. 'VLAN Mode' is 'no tag' and 'VLAN ID' is '1'. The 'Default AP Tx Rate' and 'Default Client Tx Rate' are both set to '0' bps. There are checkboxes for 'Default Authenticate', 'Default Forward', 'Hide SSID', 'Multicast Buffering', and 'Keepalive Frames'. The 'Multicast Helper' is set to 'default'. At the bottom, there are status indicators: 'disabled', 'running', 'slave', and 'disabled'.

Tryb pracy Access Point

Szerokość kanału, w 802.11 n/ac
możemy agregować kanały

SSID rozgłaszanej sieci

Ograniczenie prędkości
Download podłączonego
klienta

The screenshot shows the 'Wireless Tables' configuration window with the 'Security Profiles' tab selected. The 'Security Profile <default>' is selected. The 'Name' is 'default' and the 'Mode' is 'dynamic keys'. Under 'Authentication Types', 'WPA2 PSK' is checked. Under 'Unicast Ciphers', 'aes ccm' is checked. Under 'Group Ciphers', 'aes ccm' is checked. The 'WPA Pre-Shared Key' is empty, and the 'WPA2 Pre-Shared Key' is '*****'. The 'Supplicant Identity' is 'MikroTik' and the 'Group Key Update' is '00:05:00'. 'Management Protection' is 'disabled'. The 'Management Protection Key' is empty.

WIRELESS

Konfiguracja / AP / Ograniczenie liczby klientów

Interface <wlan2>

Data Rates Advanced HT HT MCS WDS Nstreme Tx Power ...

Area:

Max Station Count: 2007

Distance: dynamic km

Burst Time: us

Hw. Retries: 7

Hw. Fragmentation Threshold:

Hw. Protection Mode: none

Hw. Protection Threshold: 0

Frame Lifetime: 0.00 s

Adaptive Noise Immunity: none

Preamble Mode: long short both

Allow Shared Key

Disconnect Timeout: 00:00:03

On Fail Retry Time: 0.10 s

Update Stats Interval: s

OK

Cancel

Apply

Enable

Comment

Simple Mode

Torch

WPS Accept

WPS Client

Setup Repeater

Scan...

Freq. Usage...

Align...

Sniff...

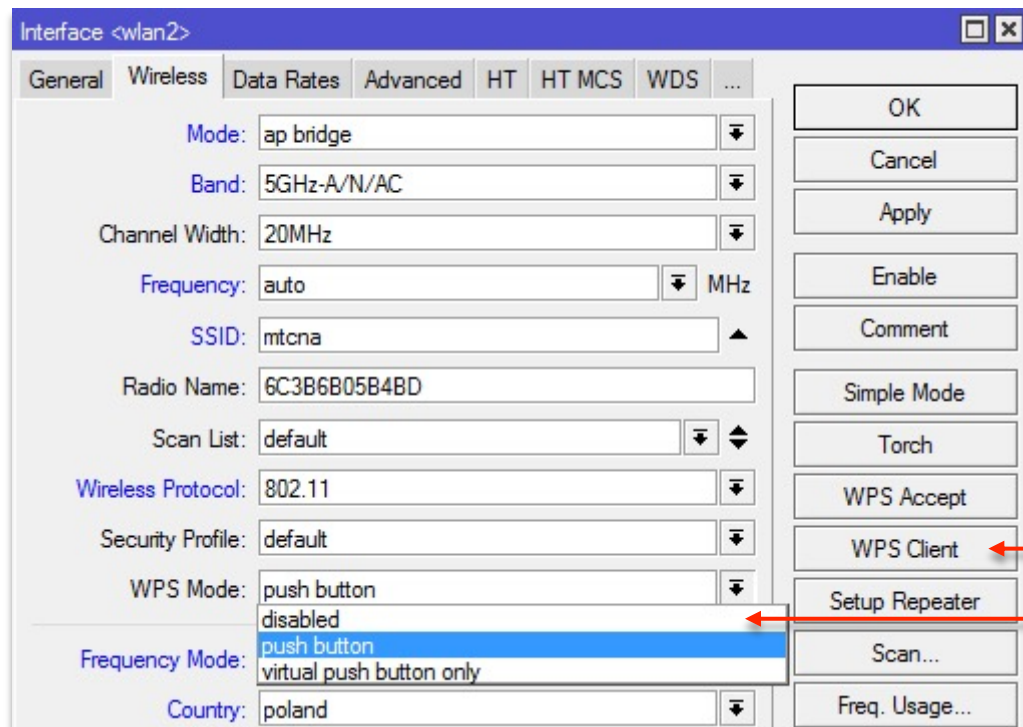
Snooper...

Reset Configuration

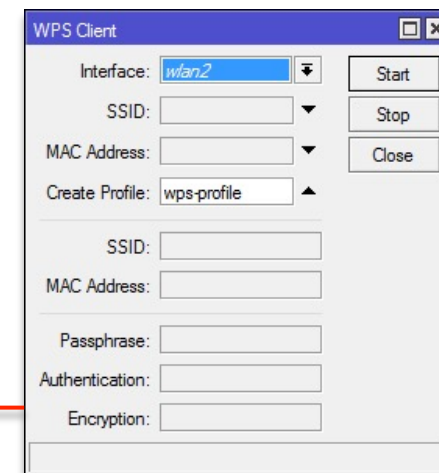
Ograniczenie liczby klientów
mogących podłączyć się do
naszego Access Point'a

WIRELESS

Konfiguracja / WPS



Jeżeli mamy ustawiony dostęp do naszego Access Point'a za pomocą hasła WPA PSK możemy umożliwić zalogowanie się klientów wspierających WPS bez konieczności podawania hasła **WPS Accept**, możemy też skorzystać z funkcjonalność WPS oferowanych przez inne Access Point'y (gdy jesteśmy klientem sieci WiFi) **WPS Client**



- **disabled** – funkcja nieaktywna
- **push button** – w momencie gdy włączymy przycisk, klienci przez dwie minuty mogą podłączyć się bez podawania hasła
- **virtual push button only** – gdy nie posiadamy na obudowie przycisku możemy wcisnąć **WPS Accept**

WIRELESS

Registration table / Informacje o połączeniach

Informacja o podłączonych:

- klientach
- AP do których podłączyliśmy się jako klient

| Radio Name | MAC Address | Interface | Uptime | AP | W... | Last Activ... | Tx/Rx Signal ... | Tx Rate | Rx Rate |
|------------|-------------------|-----------|-------------|-----|------|---------------|------------------|-------------|-------------|
| | 82:2A:A8:0B:DE:71 | wlan3-WAN | 3d 02:22:38 | yes | no | 0.030 | -41 | 144.4Mbp... | 144.4Mbp... |
| | 48:5A:3F:87:4B:A4 | wlan4-LAN | 00:37:46 | no | no | 0.030 | -37 | 54Mbps | 54Mbps |
| | 48:45:20:58:F7:87 | wlan4-LAN | 00:03:56 | no | no | 0.000 | -46 | 54Mbps | 54Mbps |

| General | 802.1x | Signal | Nstreme | NV2 | Statistics |
|------------------------|---------------|--------|---------|-----|------------|
| Tx Rate: | 6Mbps | | | | |
| Rx Rate: | 1Mbps | | | | |
| Tx/Rx Packets: | 3/13 | | | | |
| Tx/Rx Bytes: | 300 B/2408 B | | | | |
| Tx/Rx Frames: | 3/16 | | | | |
| Tx/Rx Frame Bytes: | 308 B/2657 B | | | | |
| Tx/Rx Hw. Frames: | 8/31 | | | | |
| Tx/Rx Hw. Frame Bytes: | 1145 B/3609 B | | | | |

| General | 802.1x | Signal | Nstreme | NV2 | Statistics |
|----------------------------|-----------|--------|---------|-----|------------|
| Last Activity: | 0.190 s | | | | |
| Tx/Rx Signal Strength: | -46 dBm | | | | |
| Tx/Rx Signal Strength Ch0: | -50 dBm | | | | |
| Tx/Rx Signal Strength Ch1: | -47 dBm | | | | |
| Tx/Rx Signal Strength Ch2: | | | | | |
| Signal To Noise: | 70 dB | | | | |
| Tx/Rx CCQ: | 17 % | | | | |
| P Throughput: | 5166 kbps | | | | |

| Rate | Strength | Last Measured |
|--------|----------|---------------|
| 1Mbps | -46 | 00:00:00.19 |
| HT20-6 | -38 | 00:00:30.73 |

Po wybraniu klienta znajdującego się na liście podłączonych mamy dostęp do dodatkowych informacji dotyczących połączenia

WIRELESS

Narzędzia / Snooper

Wireless Snooper (Running)

Interface: wlan1

Start

Stop

Close

Settings

New Window

all

| Channel | Address | SSID | Signal | Of Freq. (%) | Of Traf. (%) | Bandwidth | Net... | Sta... |
|-------------------|-------------------|--------------|--------|--------------|--------------|------------|--------|--------|
| 2412/20/gn(13dBm) | 3C:17:10:64:87:68 | Orange_S... | -86 | 0.0 | 0.0 | 0 bps | | |
| 2412/20/gn(13dBm) | F0:EF:86:76:FD:FD | | -86 | 0.0 | 0.0 | 0 bps | | |
| 2412/20/gn(13dBm) | 34:2C:C4:6B:66:BC | UPC0552... | -84 | 0.0 | 0.0 | 0 bps | | |
| 2412/20/gn(13dBm) | FA:8F:CA:70:79:21 | | -85 | 0.0 | 0.0 | 0 bps | | |
| 2412/20/gn(13dBm) | 54:67:51:E4:65:AF | Luke, I a... | -81 | 0.0 | 0.0 | 0 bps | | |
| 2412/20/gn(13dBm) | 38:43:7D:F1:29:43 | UPC3119... | -86 | 0.0 | 0.0 | 0 bps | | |
| 2412/20/gn(13dBm) | 8C:5B:F0:F4:C1:7B | UPC2471... | -89 | 0.0 | 0.0 | 0 bps | | |
| 2412/20/gn(13dBm) | AC:22:05:60:3C:D2 | UPC7C65... | -84 | 0.3 | 2.5 | 12.5 kbps | | |
| 2412/20/gn(13dBm) | | | | 12.9 | | 399.6 kbps | 29 | 37 |
| 2417/20/gn(13dBm) | 04:95:E6:C8:0D:89 | UPC1210... | | 0.5 | 16.3 | 17.2 kbps | | 1 |
| 2417/20/gn(13dBm) | 50:64:2B:5D:46:51 | Rybacka | | 0.0 | 0.0 | 0 bps | | 1 |
| 2417/20/gn(13dBm) | A0:9D:C1:CF:34:F2 | | -82 | 0.8 | 27.5 | 20.0 kbps | | |
| 2417/20/gn(13dBm) | 04:95:E6:C8:0D:89 | UPC1210... | -73 | 0.5 | 16.3 | 17.2 kbps | | |
| 2417/20/gn(13dBm) | 50:64:2B:5D:46:51 | Rybacka | -84 | 0.0 | 0.0 | 0 bps | | |
| 2417/20/gn(13dBm) | | | | 3.1 | | 50.1 kbps | 2 | 3 |
| 2422/20/gn(13dBm) | | | | 0.8 | | 20.0 kbps | 0 | 0 |
| 2427/20/gn(13dBm) | E0:91:F5:66:7B:BA | OLA | | 0.5 | 66.5 | 20.8 kbps | | 1 |

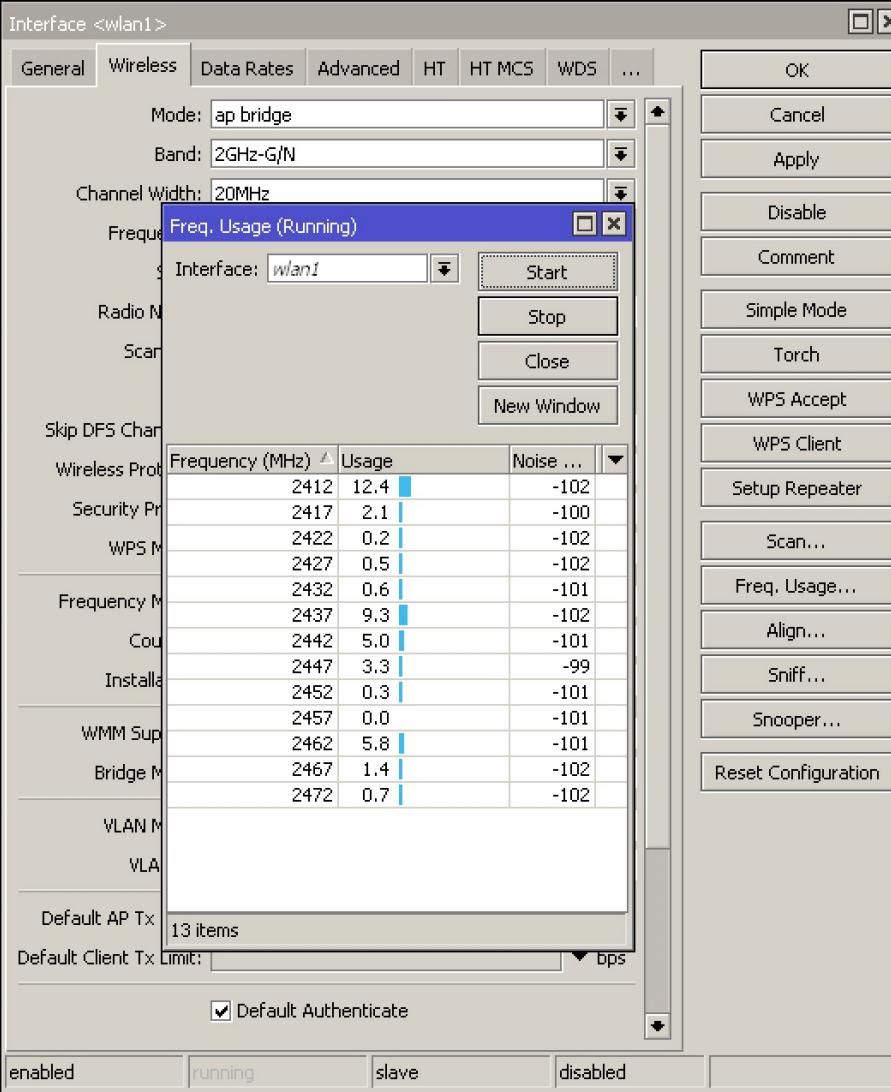
195 items

Pokazuje nie tylko Access Point'y ale i klientów którzy są do nich podłączeni

WIRELESS

Narzędzia / Frequency usage

Określamy które częstotliwości są najbardziej wykorzystywane, pokazuje jedynie Access Point'y w standardzie 802.11



The screenshot shows the Mikrotik WinBox interface for configuring the wireless interface 'wlan1'. The 'Wireless' tab is active, and the 'Freq. Usage (Running)' dialog box is open, displaying a table of frequency usage for the wlan1 interface.

| Frequency (MHz) | Usage | Noise ... |
|-----------------|-------|-----------|
| 2412 | 12.4 | -102 |
| 2417 | 2.1 | -100 |
| 2422 | 0.2 | -102 |
| 2427 | 0.5 | -102 |
| 2432 | 0.6 | -101 |
| 2437 | 9.3 | -102 |
| 2442 | 5.0 | -101 |
| 2447 | 3.3 | -99 |
| 2452 | 0.3 | -101 |
| 2457 | 0.0 | -101 |
| 2462 | 5.8 | -101 |
| 2467 | 1.4 | -102 |
| 2472 | 0.7 | -102 |

FIREWALL

FIREWALL

Zadania

- Filtrowanie ruchu przychodzącego do routera
- Filtrowanie ruchu wychodzącego z routera
- Filtrowanie ruchu przechodzącego przez router (np. z sieci LAN do Internetu)
- Translacja portów/adresów (NAT)
- Logowanie informacji o połączeniach
- Zbieranie statystyk (np. ile ruchu http wyszło z sieci LAN)
- Oznaczanie ruchu na potrzeby innych usług (kolejkowanie QoS, routing)
- Zmiana pól nagłówka IP (DSCP, TTL, ...)

Domyślnie firewall pracuje w warstwie 3 i 4 modelu OSI. W systemie RouterOS funkcjonalność firewall'a został rozszerzona między innymi o możliwość pracy w warstwie 7 (znacząco zwiększa zużycie CPU).

FIREWALL

Blokowanie / zezwalanie na ruch

- z router'a
- do router'a
- z sieci LAN
- do sieci LAN
- ...

NAT

- przekierowanie portów
- masquerade
- NAT 1:1
- source NAT
- ...

Mangle

- zmiana TTL
- zmiana DSCP
- oznaczanie ruchu
- ...

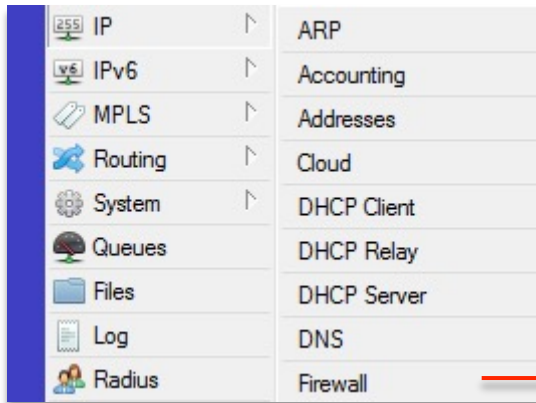
Informacje o stanie połączeń

- tryb stateful
- tryb stateless
- ...

Listy adresów

- dynamiczna
- można użyć w tablicach mangle, nat, filter

Filtry warstwy 7

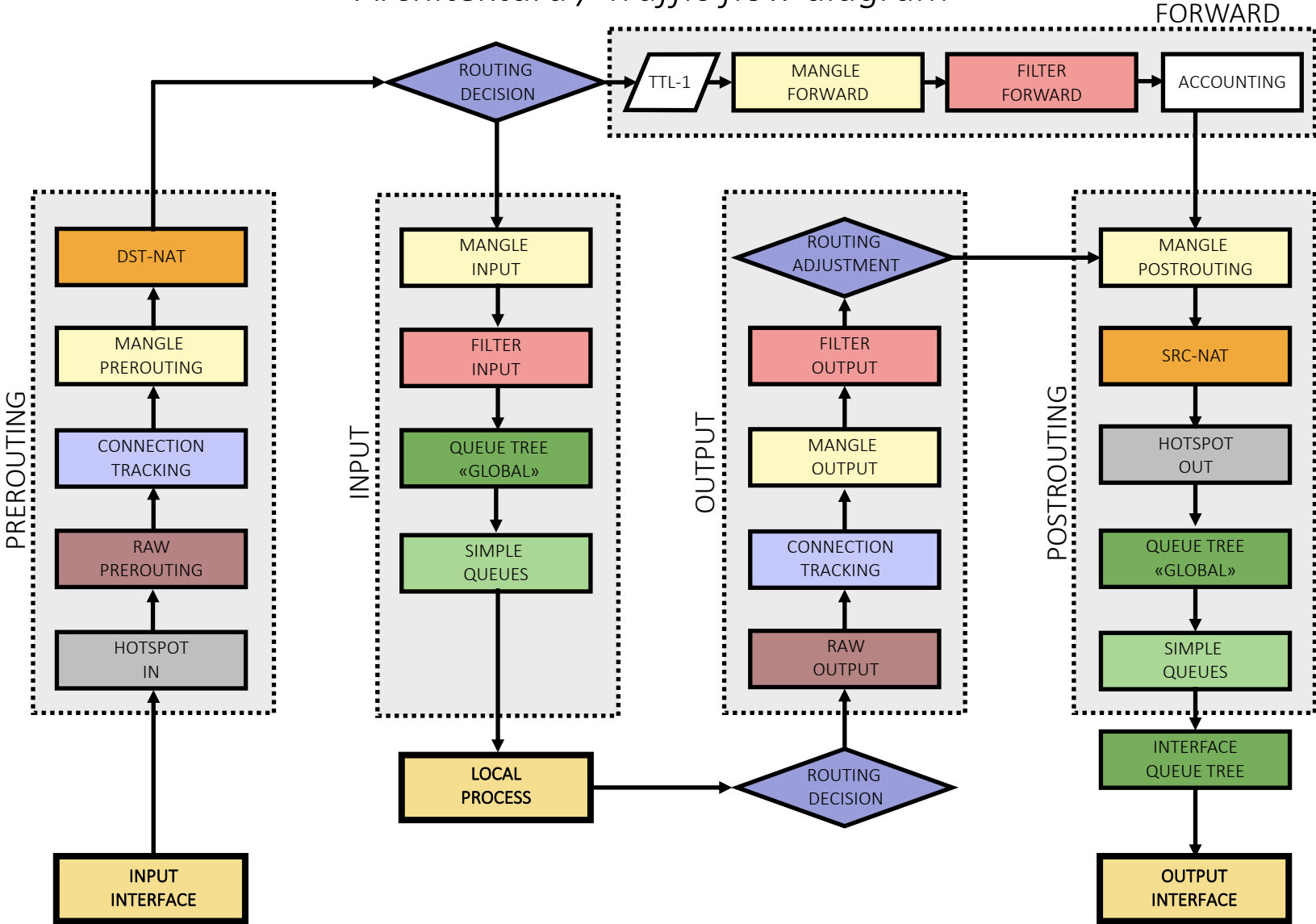


A screenshot of the Mikrotik WinBox Firewall Connections tab. The window title is 'Firewall'. The tabs at the top are Filter Rules, NAT, Mangle, Raw, Service Ports, Connections (selected), Address Lists, and Layer7 Protocols. Below the tabs is a 'Tracking' button and a 'Find' search box. The main area contains a table of active connections. The table has columns for Src. Address, Dst. Address, Proto..., Connecti..., Timeout, TCP State, Orig./Repl. Rate, and Orig./Repl. Bytes. The table shows 47 items, with a maximum of 218008 entries. Red arrows from the text blocks above point to the 'Filter Rules', 'NAT', 'Mangle', 'Connections', 'Address Lists', and 'Layer7 Protocols' tabs.

| | Src. Address | Dst. Address | Proto... | Connecti... | Timeout | TCP State | Orig./Repl. Rate | Orig./Repl. Bytes |
|------|--------------------|---------------------|----------|-------------|----------|-------------|-------------------|---------------------|
| SACs | 10.250.1.100:6298 | 40.77.229.15:443 | 6 (tcp) | | 23:59:58 | established | 1576 bps/1384 bps | 5.4 KiB/7.3 KiB |
| SACs | 10.250.1.100:6302 | 74.125.71.108:993 | 6 (tcp) | | 23:53:01 | established | 0 bps/0 bps | 20.9 KiB/29.6 KiB |
| SACs | 10.250.1.100:6343 | 52.59.65.107:443 | 6 (tcp) | | 23:59:38 | established | 0 bps/0 bps | 103.0 KiB/65.6 KiB |
| SACs | 10.250.1.100:6402 | 77.234.45.60:80 | 6 (tcp) | | 23:57:51 | established | 0 bps/0 bps | 40.1 KiB/197.4 KiB |
| SACs | 10.250.1.100:8745 | 173.194.76.188:5228 | 6 (tcp) | | 19:14:47 | established | 0 bps/0 bps | 1240 B/726 B |
| SACs | 10.250.1.100:8756 | 169.44.82.101:443 | 6 (tcp) | | 23:59:54 | established | 0 bps/0 bps | 143.2 KiB/116.0 ... |
| SACs | 10.250.1.100:8806 | 40.77.229.17:443 | 6 (tcp) | | 23:59:35 | established | 0 bps/0 bps | 51.3 KiB/71.1 KiB |
| SACs | 10.250.1.100:8974 | 66.102.1.188:5228 | 6 (tcp) | | 23:59:26 | established | 0 bps/0 bps | 16.8 KiB/20.6 KiB |
| SACs | 10.250.1.100:10224 | 188.128.193.60:143 | 6 (tcp) | | 23:52:30 | established | 0 bps/0 bps | 8.9 KiB/58.0 KiB |
| SACs | 10.250.1.100:10561 | 79.96.150.178:143 | 6 (tcp) | | 23:53:00 | established | 0 bps/0 bps | 5.2 KiB/9.1 KiB |
| SACs | 10.250.1.100:10820 | 162.125.18.133:443 | 6 (tcp) | | 23:59:37 | established | 0 bps/0 bps | 65.7 KiB/34.3 KiB |
| SACs | 10.250.1.100:11044 | 79.96.150.178:143 | 6 (tcp) | | 23:52:30 | established | 0 bps/0 bps | 4545 B/17.1 KiB |
| SACs | 10.250.1.100:11049 | 79.96.150.178:143 | 6 (tcp) | | 23:53:00 | established | 0 bps/0 bps | 50.7 KiB/2526.5 ... |
| SACs | 10.250.1.100:11160 | 79.96.150.178:143 | 6 (tcp) | | 23:52:00 | established | 0 bps/0 bps | 4105 B/11.8 KiB |
| SACs | 10.250.1.100:11170 | 79.96.150.178:143 | 6 (tcp) | | 23:53:00 | established | 0 bps/0 bps | 2485 B/31.7 KiB |
| SACs | 10.250.1.100:11459 | 162.125.18.133:443 | 6 (tcp) | | 23:59:53 | established | 0 bps/0 bps | 30.0 KiB/13.8 KiB |
| SACs | 10.250.1.100:12369 | 40.77.229.7:443 | 6 (tcp) | | 23:55:55 | established | 0 bps/0 bps | 2833 B/4887 B |

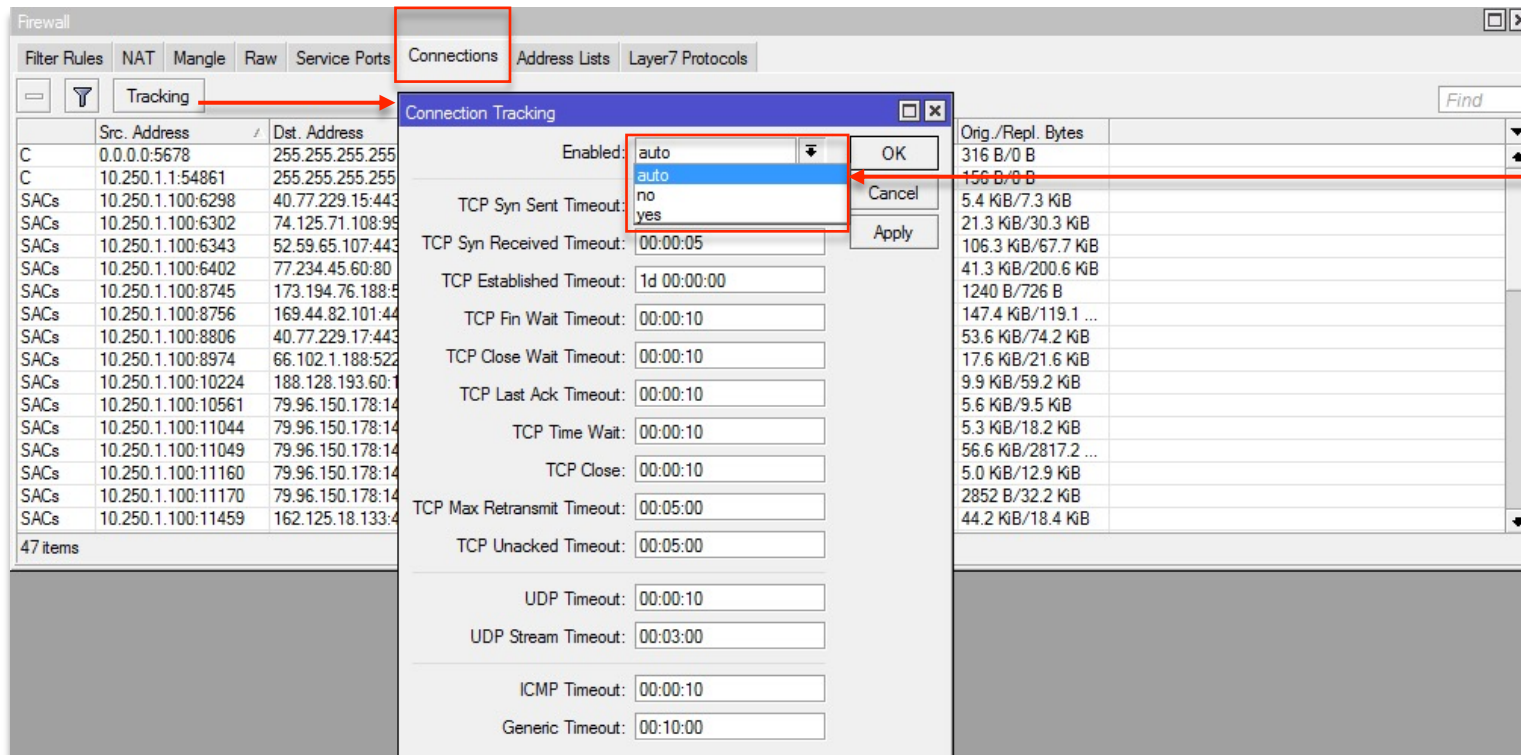
FIREWALL

Architektura / Traffic flow diagram



FIREWALL

Statefull/Stateless



- **auto** – pojawienie się choćby jednej reguły NAT przełączy firewall'a w tryb stanowy
- **enable** – bez względu czy są reguły NAT czy nie, firewall zawsze pracuje stanowo
- **disable** – tryb *stateless*, NAT nie będzie działał

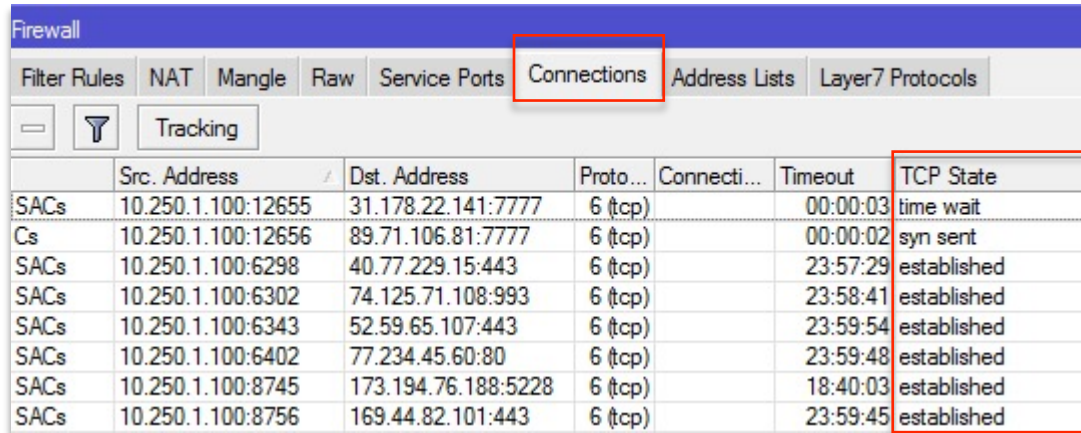
W przypadku filtrowania ruchu możemy zdecydować, czy chcemy aby firewall był stanowy czy bezstanowy. W przypadku funkcjonalności NAT nie mamy takiego wyboru, firewall musi pracować w trybie stanowym!!! Tryb stanowy zwiększa zużycie zasobów.

Firewall może pracować w dwóch trybach:

- **Statefull (śledzenie stanu połączeń)** – urządzenie jest świadome czy przychodzące, wychodzące pakiety są częścią już istniejącego połączenia, czy stanowią dopiero jego początek
- **Stateless (brak śledzenia stanu połączeń)** – router nie ma wiedzy, czy dany pakiet jest częścią już istniejącego połączenia, czy dopiero pierwszym, inicjującym połączenie, pakietem

FIREWALL

Statefull/Stateless

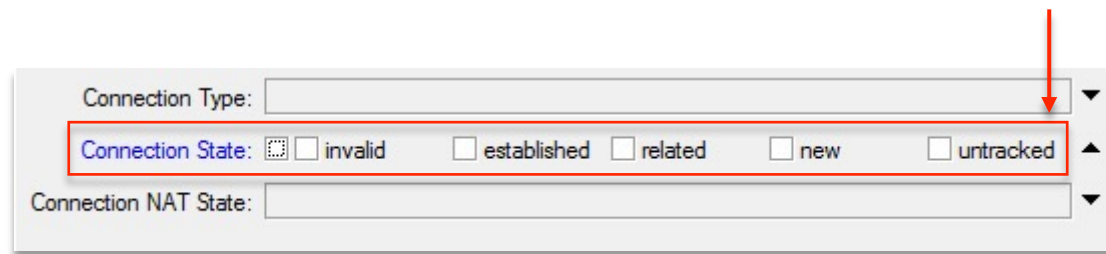


| | Src. Address | Dst. Address | Proto... | Connecti... | Timeout | TCP State |
|------|--------------------|---------------------|----------|-------------|----------|-------------|
| SACs | 10.250.1.100:12655 | 31.178.22.141:7777 | 6 (tcp) | | 00:00:03 | time wait |
| Cs | 10.250.1.100:12656 | 89.71.106.81:7777 | 6 (tcp) | | 00:00:02 | syn sent |
| SACs | 10.250.1.100:6298 | 40.77.229.15:443 | 6 (tcp) | | 23:57:29 | established |
| SACs | 10.250.1.100:6302 | 74.125.71.108:993 | 6 (tcp) | | 23:58:41 | established |
| SACs | 10.250.1.100:6343 | 52.59.65.107:443 | 6 (tcp) | | 23:59:54 | established |
| SACs | 10.250.1.100:6402 | 77.234.45.60:80 | 6 (tcp) | | 23:59:48 | established |
| SACs | 10.250.1.100:8745 | 173.194.76.188:5228 | 6 (tcp) | | 18:40:03 | established |
| SACs | 10.250.1.100:8756 | 169.44.82.101:443 | 6 (tcp) | | 23:59:45 | established |

TCP State

- **established** – każdy pakiet po zakończonej procedurze 3-way handshake, przed wystaniem prośby o rozłączenie
- **time-wait** – klient wysyła flagę FIN, serwer odpowiada ACK oraz FIN, klient odpowiada ACK
- **close** – procedura zakończenia połączenia
- **syn-sent** – pierwszy pakiet TCP z flagą SYN
- **syn-received** – odpowiedź na SYN, SYN/ACK wysłana przez serwer

TCP jest protokołem stanowym, wiemy kiedy połączenie się rozpoczyna i kiedy kończy. W przypadku innych protokołów np. UDP nie mamy tej informacji przekazanej wprost. Jednakże firewall także jest w stanie określić który z pakietów jest pierwszy i czy kolejne należą do już istniejącego połączenia. Firewall określa to na podstawie **IP źródłowe, IP docelowe, port źródłowy, port docelowy**. Z informacji o stanie połączenia możemy korzystać bezpośrednio, budując reguły w **filter, nat, mangle**.



Connection Type:

Connection State: invalid established related new untracked

Connection NAT State:

- **established** – pakiety należą do istniejącego połączenia
- **related** – pakiety należą do istniejącego połączenia
- **new** – pierwszy pakiet, inicjujący połączenie
- **invalid** – pakiet bez flagi SYN, jednocześnie nie należy do żadnego istniejącego połączenia

Connection State dotyczy połączeń TCP, UDP oraz ICMP

FIREWALL

Reguły / Tablica Filter

| # | Action | Chain | Src. Address | Dst. Address | Proto... | Src. Port | Dst. Port | In. Interface | Out. Interface | Bytes | Packets |
|--------------------------------|----------|-------|--------------|--------------|-----------|-----------|-----------|---------------|----------------|-----------|---------|
| ::: Allow ESTABLISHED, RELATED | | | | | | | | | | | |
| 0 | ✓ accept | input | | | | | | | | 25.4 MiB | 235 679 |
| ::: WAN allow WinBox | | | | | | | | | | | |
| 1 | ✓ accept | input | | | 6 (tcp) | | 8291 | | | 0 B | 0 |
| ::: WAN allow SSH | | | | | | | | | | | |
| 2 | ✓ accept | input | | | 6 (tcp) | | 22 | | | 0 B | 0 |
| ::: VPN allow WinBox | | | | | | | | | | | |
| 3 | ✓ accept | input | | | 6 (tcp) | | 8291 | | | 0 B | 0 |
| ::: VPN allow SSH | | | | | | | | | | | |
| 4 | ✓ accept | input | | | 6 (tcp) | | 22 | | | 0 B | 0 |
| ::: DNS allow from LAN | | | | | | | | | | | |
| 5 | ✓ accept | input | | | 17 (u...) | | 53 | | | 868.6 KiB | 13 630 |
| ::: Block ALL on INPUT | | | | | | | | | | | |
| 6 | ✗ drop | input | | | | | | | | 16.1 KiB | 274 |

Ile pakietów zostało obsłużonych przez daną regułę

Ile ruchu przewinęło się przez daną regułę

Powyższy zestaw reguł zablokuje cały ruch na łańcuchu INPUT do routera, za wyjątkiem: połączeń wcześniej nawiązanych, połączeń do WinBox, połączeń SSH, zapytań DNS z sieci lokalnej

- Reguły filtrujące decydują czy dany ruch ma zostać zablokowany czy jest dozwolony
- Reguły są przetwarzane sekwencyjnie
- Pierwsza pasująca reguła kończy przetwarzanie pozostałych (wyjątek stanowią akcji: passthrough, log)

FIREWALL

Reguły / Chains / Łańcuchy

Łańcuchy (*Chains*) w tablicy Filter

- **input** – ruch skierowany bezpośrednio do routera (vpn, winbox, web-proxy, ssh, telnet, ping, ...)
- **output** – ruch wychodzący z routera
- **forward** – ruch przechodzący przez router (wchodzi jednym interface'em, wychodzi drugim) np. z jednej sieci do drugiej, z sieci LAN do Internetu

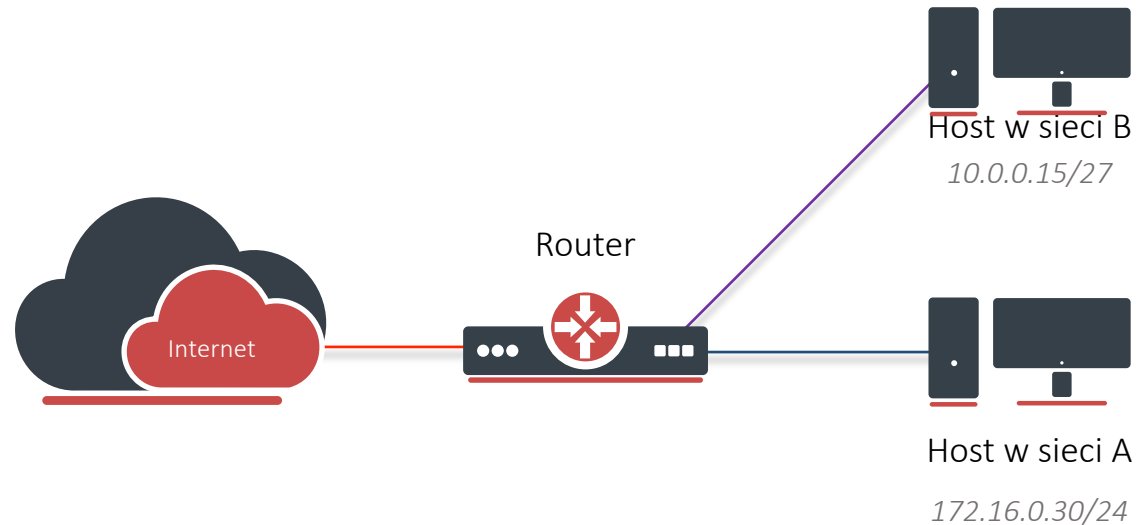
Przykład:

Ruch z Sieci A do sieci B przechodzi przez łańcuch **FORWARD**

Ruch od hosta w sieci B do routera, na usługę WinBox, filtrujemy na łańcuchu **INPUT**

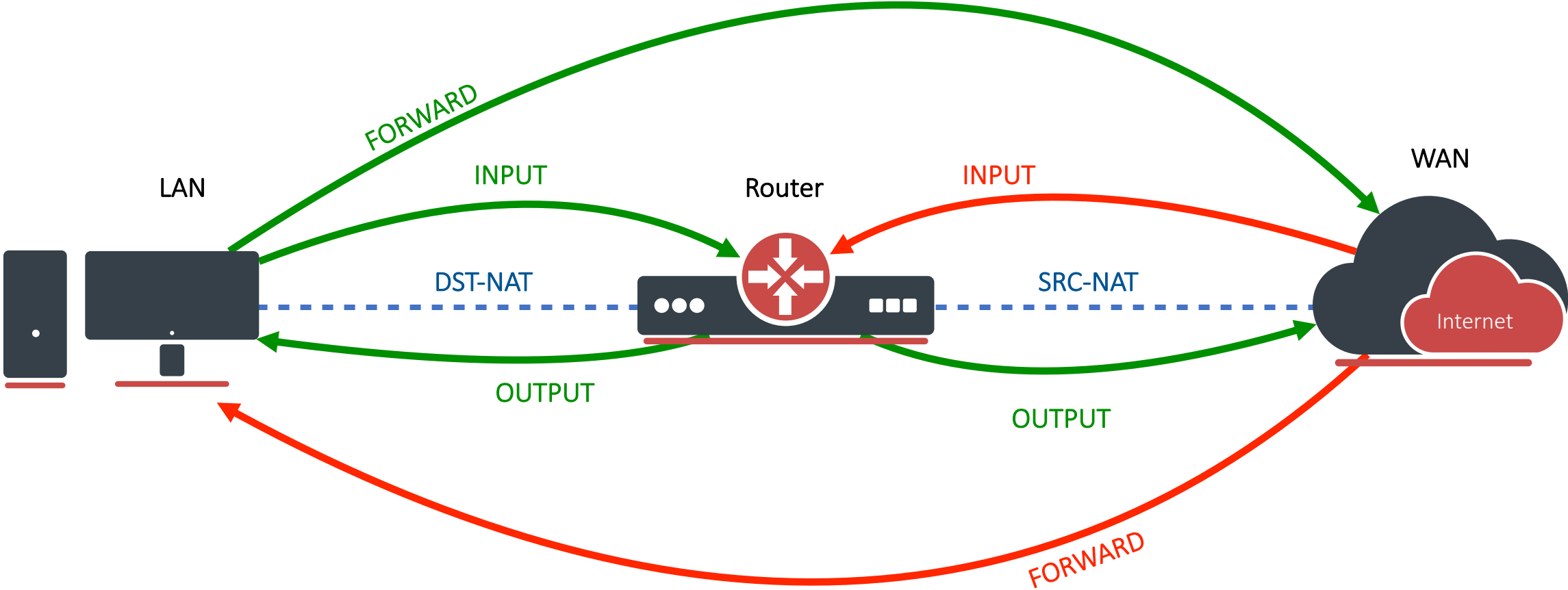
Ruch z sieci A do Internetu filtrujemy na łańcuchu **FORWARD**

Ruch z Internetu do naszego router'a, na port SSH, filtrujemy na łańcuchu **INPUT**



FIREWALL

Ogólne zasady



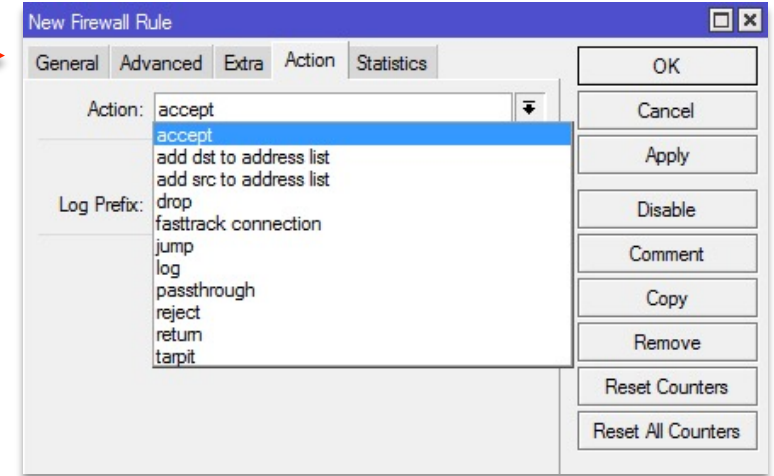
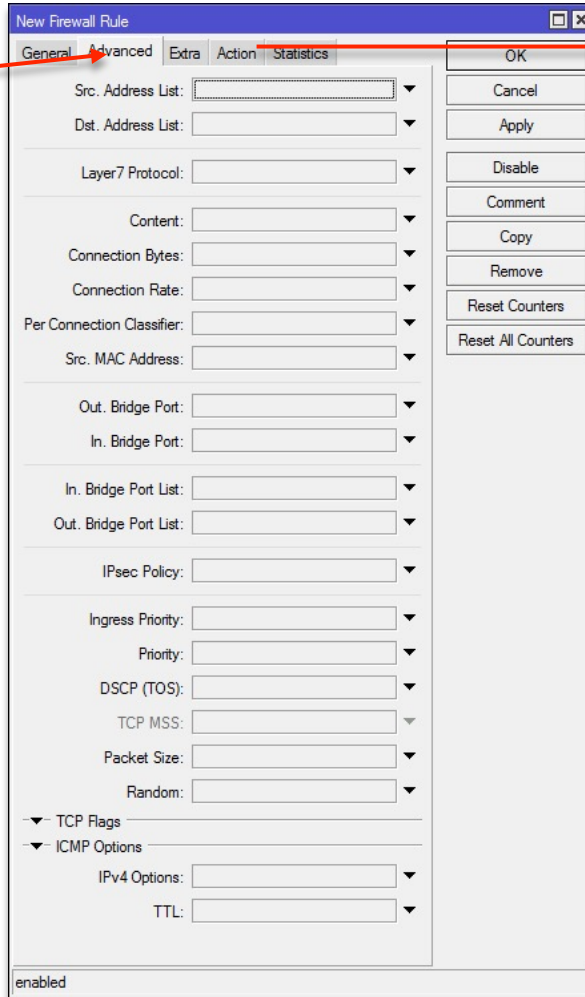
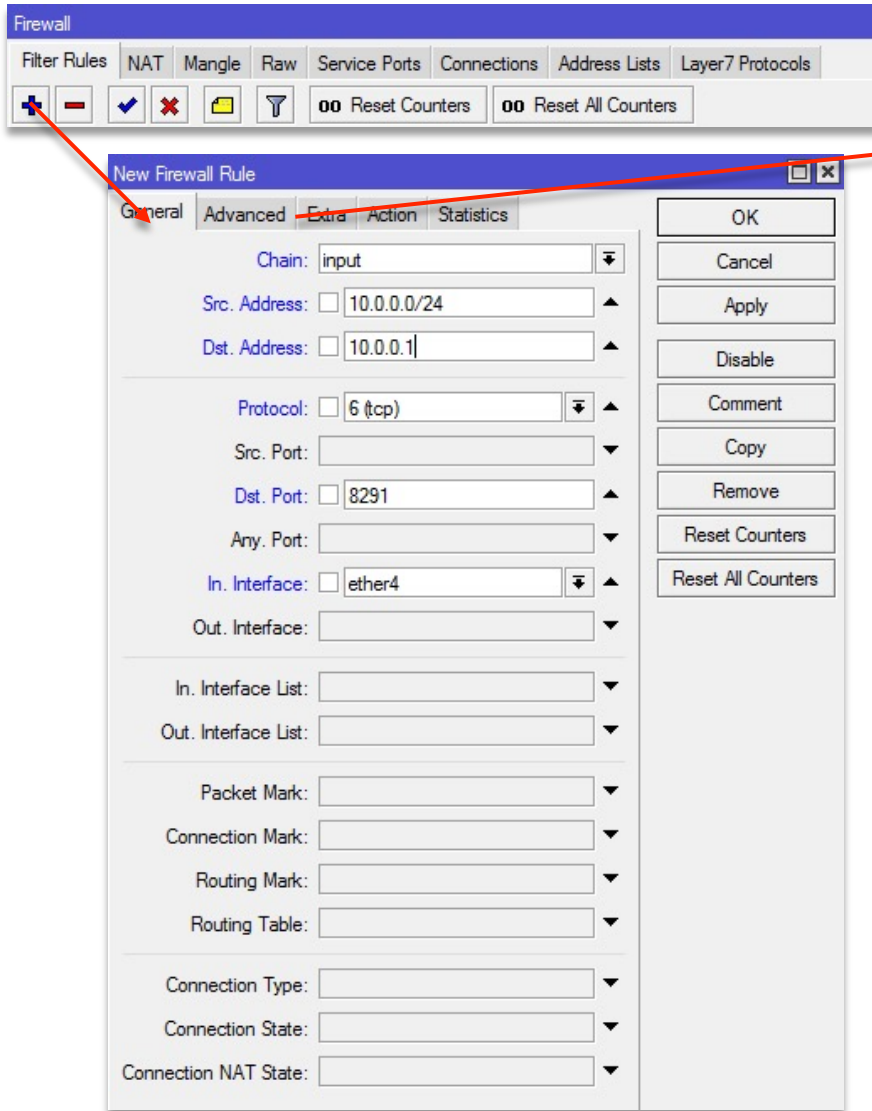
Dozwolony ruch (warunkowo bezpieczny)

Ruch zabroniony (warunkowo niebezpieczny)

* Dany schemat jest przykładowym

FIREWALL

Reguły filter / dodanie reguły



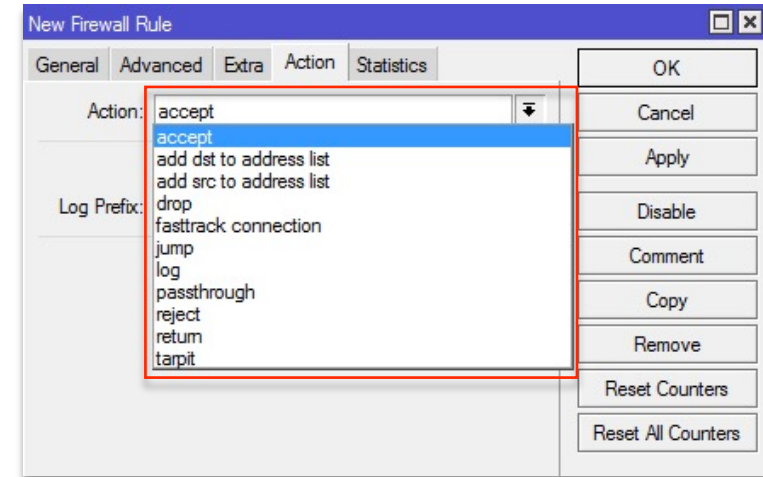
W zakładkach **General**, **Advanced**, **Extra** definiujemy jaki ruch pasuje do naszej reguły. Aby pakiet pasował do danej reguły muszą być spełnione wszystkie warunki. W powyższym przykładzie dla połączeń z sieci **10.0.0.0/24** do naszego routera na adres **10.0.0.1**, przychodzących na interfejs **ether4**, na port **8291/TCP** zdefiniowaliśmy akcję **accept**

W zakładce **Action** konfigurujemy co z danym pakietem należy zrobić.

FIREWALL

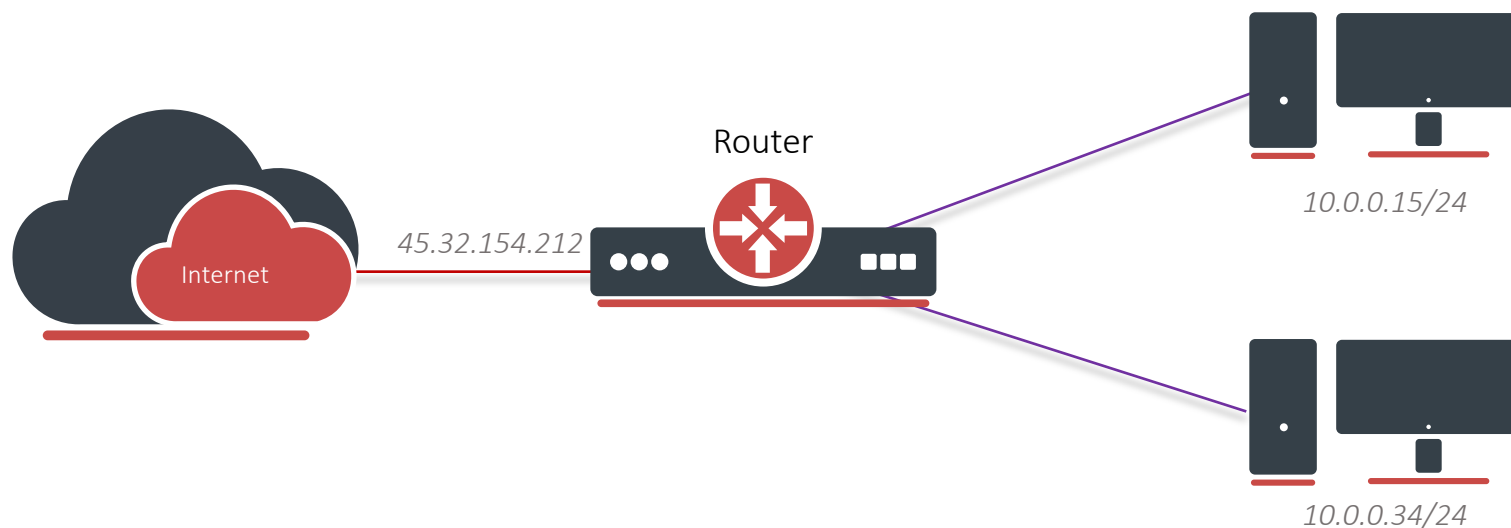
Reguły filter / Akcji

- **accept** – akceptuj pakiet
- **add dst to address list** – dodaj adres docelowy do address list
- **add src to address list** – dodaj adres źródłowy do address list
- **drop** – zablokuj pakiet, nie informuj strony która go wysłała
- **jump** – przejdź do innego zdefiniowanego przez użytkownika łańcucha
- **log** – loguje informacje o pakiecie (in-interface, out-interface, src-mac, protocol, src-ip:port, dst-ip:port, długość pakietu), nie kończy przetwarzania dalszych reguł
- **passthrough** – wykorzystywane do zebrania statystyk, nie kończy przetwarzania innych reguł
- **reject** – zablokuj pakiet, wyślij komunikat ICMP z przyczyną odrzucenia
- **return** – w przypadku gdy przetwarzamy reguły znajdujące się w przez nas utworzonym łańcuchu, opcja nakazuje powrót do łańcucha źródłowego
- **tarpit** – pośredniczy w TCP procedurze 3-way handshake dzięki czemu spowalnia ataki na serwery usług TCP (odpowiada na pakiet SYN pakietem SYN/ACK i dopiero po zakończeniu procedury 3-way przekaze połączenie dalej)



FIREWALL

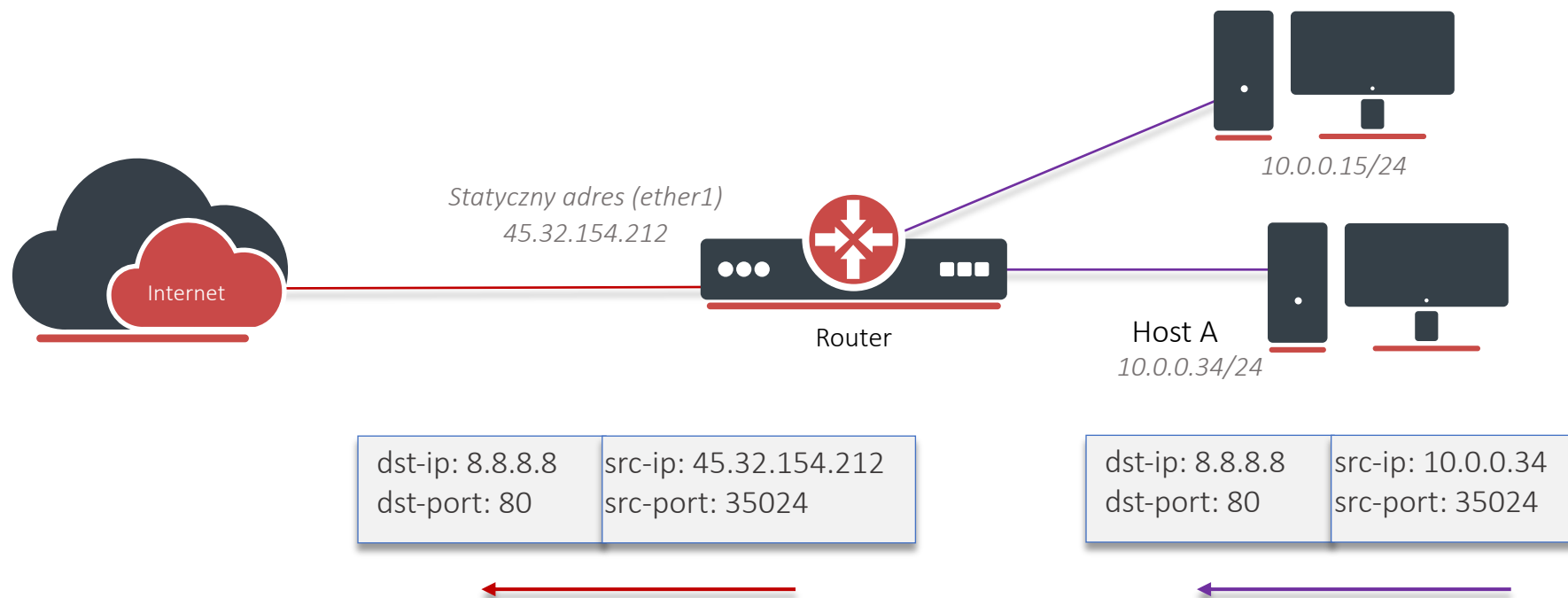
NAT - Network Address Translation



Nasz router posiada jeden adres zewnętrzny, w sieci lokalnej mamy kilka komputerów. Aby wszystkie urządzenia mogły komunikować się ze światem muszą zaprezentować się na zewnątrz naszej sieci zewnętrznym adresem IP. W tym celu stosuje się technologię NAT. Router będzie odpowiedzialny za podmianę adresów źródłowych naszych komputerów (10.0.0.34, 10.0.0.15, ...) na adres 45.32.154.212 za każdym razem gdy komputer będzie łączył się do zasobów sieci Internet. Tablica NAT posiada dwa łańcuchy `srcnat` i `dstnat`.

FIREWALL

NAT / srcnat



Host A chciał nawiązać połączenie z adresem 8.8.8.8 na port 80-http, pakiet trafił do routera i router, aby móc przesać go dalej, podmienił adres źródłowy pakietu. Jednocześnie umieszcza informację o tej podmianie w tablicy Connection Tracking. Jeżeli przyjdzie odpowiedź z serwera 8.8.8.8 router na podstawie wpisu w Connection Tracking podmieni adres docelowy i skieruje pakiet do Host A.

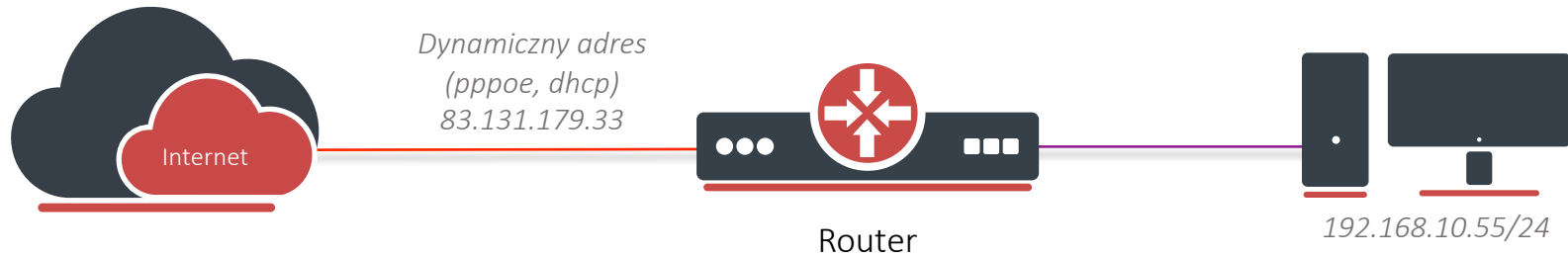
FIREWALL

NAT / srcnat

The image displays the Mikrotik WinBox interface for configuring a NAT rule. The main window is titled "Firewall" and shows a list of rules. A red arrow points to the "+" button in the top toolbar, which opens the "New NAT Rule" dialog. The dialog has several tabs: "General", "Advanced", "Extra", "Action", and "Statistics". The "Action" tab is selected, showing the "Action" dropdown set to "src-nat". Other fields in the "Action" tab include "Log" (unchecked), "Log Prefix", "To Addresses" (45.32.154.212), and "To Ports". The "General" tab is also visible, showing "Chain" set to "srcnat" and "Out. Interface" set to "ether1". A second red arrow points from the "Action" tab to the "src-nat" dropdown.

FIREWALL

NAT / masquerade



New NAT Rule

General Advanced Extra Action Statistics

Chain: srcnat

Src. Address: 192.168.10.0/24

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface: ether1

Akcja **masquerade** działa podobnie do src-nat, z tą różnicą, iż w przypadku **masquerade** zewnętrzny adres IP jest określany przez router na podstawie interfejsu (**out-interface**) na jakim działa ta reguła.

New NAT Rule

General Advanced Extra Action Statistics

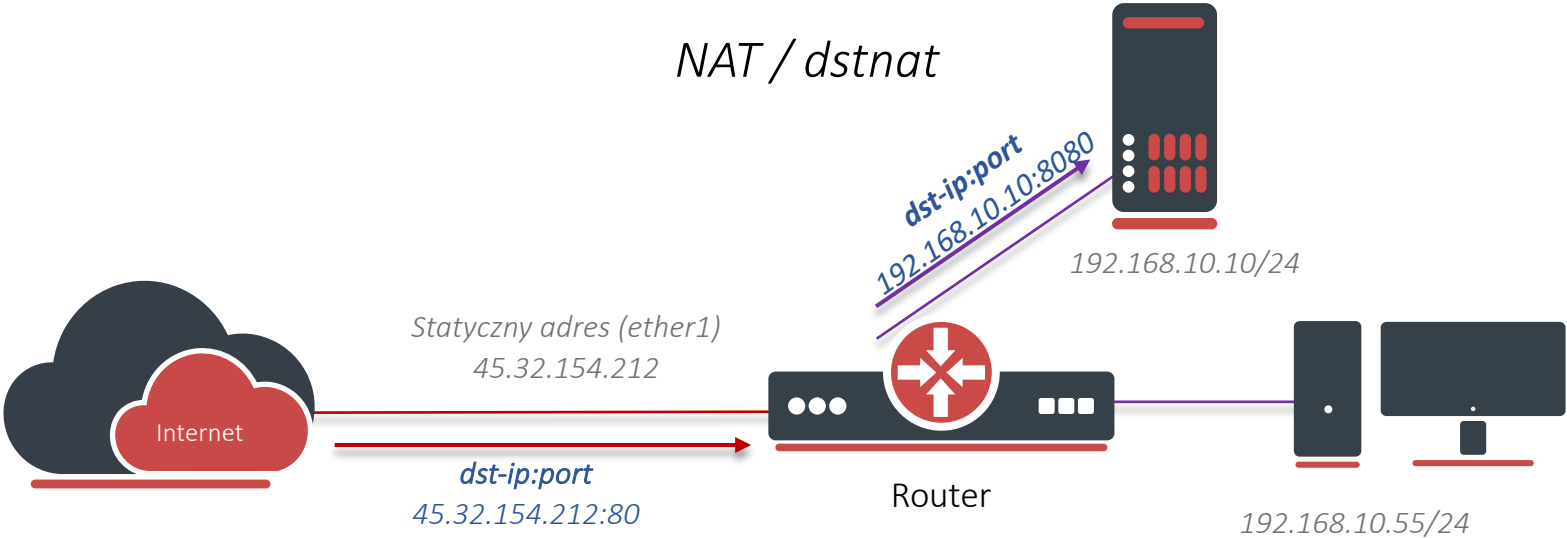
Action: masquerade

Log

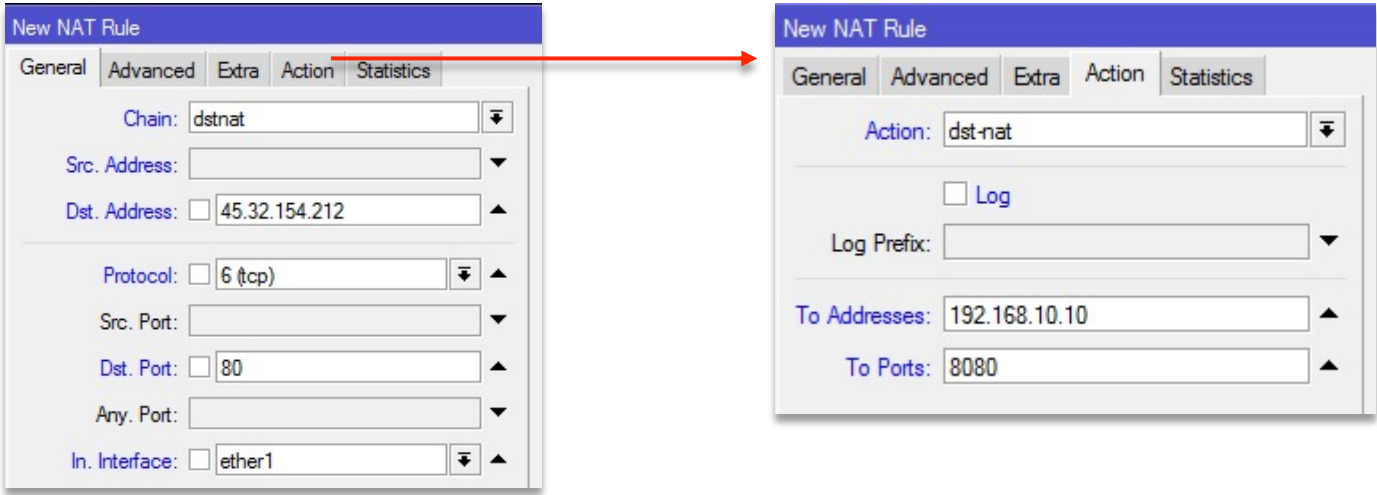
Log Prefix:

FIREWALL

NAT / dstnat



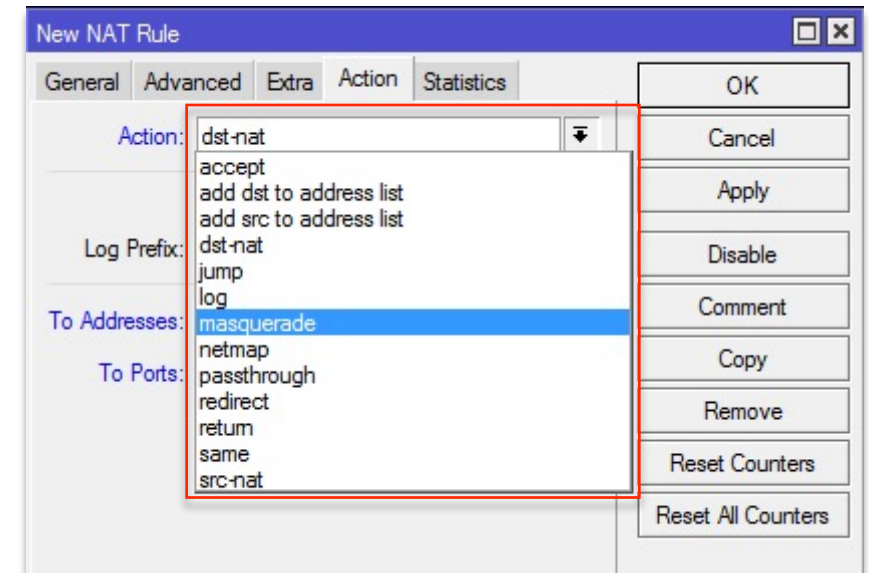
W sieci lokalnej posiadamy serwer www, chcemy aby był on dostępny z zewnątrz.
W tym celu musimy stworzyć regułę na łańcuchu *dstnat*



FIREWALL

NAT / Akcji

- **accept** – akceptuj pakiet, nie stosuj mechanizmu NAT
- **add dst to address list** – dodaj adres docelowy do address list
- **add src to address list** – dodaj adres źródłowy do address list
- **drop** – zablokuj pakiet, nie informuj strony która go wysłała
- **jump** – przejdź do innego zdefiniowanego przez użytkownika łańcucha
- **log** – loguje informacje o pakiecie (in-interface, out-interface, src-mac, protocol, src-ip:port, dst-ip:port, długość pakietu), nie kończy przetwarzania dalszych reguł
- **passthrough** – wykorzystywane do zebrania statystyk, nie kończy przetwarzania innych reguł
- **redirect** – przekieruj połączenie do **router'a** (chain: dstnat), przydatne gdy wdrażamy na MikroTik'u transparentny web-proxy lub cache DNS
- **return** – w przypadku gdy przetwarzamy reguły znajdujące się w przez nas utworzonym łańcuchu, opcja nakazuje powrót do łańcucha źródłowego
- **same** – w przypadku, gdy mamy wiele zewnętrznych adresów IP i chcemy aby użytkownik lokalny zawsze wychodził tym samym adresem
- **netmap** – nat 1:1, przydatne gdy mamy tyle samo adresów w sieci lokalnej co zewnętrznych, wpis trzeba uruchomić zarówno na łańcuchu srcnat jak i dstnat
- **src-nat** – podmienia adres źródłowy pakietu z sieci lan na zewnętrzny adres routera, podobnie jak **masquerade**, z tą różnicą że musimy podać zewnętrzny IP adres
- **dst-nat** – pozwala na przekierowanie portów do hostów znajdujących się w sieci wewnętrznej
- **masquerade** – podmienia adres źródłowy pakietu z sieci lan na zewnętrzny adres routera, najbardziej powszechny typ NAT



FIREWALL

FastTrack

Ze względu na złożoną architekturę firewall'a (dużo tablic oraz łańcuchów) w środowiskach zorientowanych na dużą wydajność można skorzystać z okrojonej wersji firewall'a, zwanej FastTrack.

Odbywa się to z kosztem mniejszej funkcjonalności:

- wspiera jedynie TCP, UDP
- jest wsparcie dla srcnat, dstnat
- nie działają kolejki SIMPLE QUEUE oraz QUEUE TREE
- nie działa IPSEC
- nie działa Hotspot

Aby uruchomić mechanizm dla ruchu z naszej sieci LAN wystarczy dodać dwie reguły:

```
/ip firewall filter add chain=forward action=fasttrack-connection connection-state=established,related  
/ip firewall filter add chain=forward action=accept connection-state=established,related
```

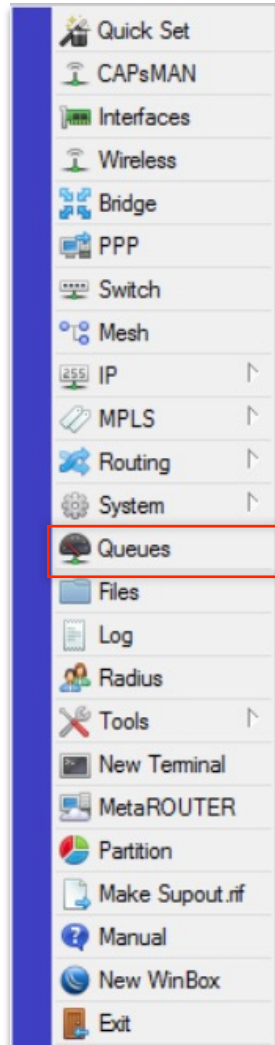
Mechanizm FastTrack działa jedynie na wybranych architekturach:

- **RB6XX** porty: ether1,2
- **RB7XX** porty: wszystkie
- **RB800** porty: ether1,2
- **RB9XX** porty: wszystkie
- **RB1000** porty: wszystkie
- **RB1100** porty: ether1-11
- **RB2011** porty: wszystkie
- **RB3011** porty: wszystkie
- **CRS** porty: wszystkie
- **CCR** porty: wszystkie
- Dla pozostałych architektur wsparcie jest jedynie dla interfejsów wireless

QoS

QoS

Quality of Service



Zastosowanie:

- Ograniczenie zużycia pasma
- Priorytetyzacja ważnego ruchu
- Może być zastosowana dla:
 - konkretnych hostów
 - konkretnych usług (http, VoIP)
 - konkretnych sieci
 - rozmiaru pakietów

W jaki sposób określić i oznaczyć ruch, który powinien mieć pierwszeństwo w naszej sieci?

- na poziomie samego routera możemy skorzystać z mechanizmu **Queues** i oznaczyć ruch za pomocą reguł **mangle** (oznaczone w ten sposób pakiety będą mogły być wykorzystane jedynie w ramach danego routera, znacznik **mangle** nie przechodzi pomiędzy urządzeniami !!!)
- w przypadku gdy w naszej sieci używamy również sprzętu innych dostawców możemy oprzeć się na polu **TOS** (nagłówek IP). Uwaga aby w naszej sieci operować na atrybucie **TOS** musimy mieć zaufanie do wszystkich urządzeń jakie w niej pracują.

QoS

Quality of Service

Teoretyczne pojęcia:

- **CIR (Committed Information Rate)** – w systemie RouterOS oznaczone jako **Limit At**, minimalne zagwarantowane pasmo jakie otrzyma dany użytkownik lub usługa
- **MIR (Maximum Information Rate)** – w systemie RouterOS oznaczone jako **Max Limit**, jeżeli użytkownik lub usługa wykorzystał swój CIR ale mamy zapas, jego transfer zostaje zwiększony do podanej tu wartości

Simple Queue <queue-lan>

General Advanced Statistics Traffic Total Total Statistics

Total Limit At: [] bits/s

Total Max Limit: [] bits/s

Total Priority: []

Total Burst Limit: [] bits/s

Total Burst Threshold: [] bits/s

Total Burst Time: [] s

Total Queue Type: default-small

Total = download + upload

Simple Queue <queue-lan>

General Advanced Statistics Traffic Total Total Statistics

Name: queue-lan

Target: 192.168.10.0/24

Dst.: []

MIR

Max Limit: 10M Target Upload: 20M Target Download: [] bits/s

Burst Limit: unlimited bits/s

Burst Threshold: unlimited bits/s

Burst Time: 0 s

Time: []

enabled

W przypadku, gdy mamy równorzędne kolejki, parametr **Priority** będzie bramy pod uwagę przy podjęciu decyzji, która kolejka może wykorzystać MIR. **Priority** nie ma wpływu na CIR.

Simple Queue <queue-lan>

General Advanced Statistics Traffic Total Total Statistics

Packet Marks: []

CIR

Limit At: 8M Target Upload: 16M Target Download: [] bits/s

Priority: 8

Bucket Size: 0.100 ratio

Queue Type: default-small

Parent: none

enabled

QoS

Burst

Opcja **Burst** pozwala, na pewien okres czasu, zwiększyć transfer powyżej limitu MIR (max-limit), przydatne gdy chcemy pozwolić użytkownikom na komfortowe korzystanie np. z serwisów www, gdzie po załadowaniu się strony użytkownik nie pobiera dużych ilości danych, możemy więc «nagrodzić go» za to, iż nie obciąża łącza, w postaci «gratisowej przepustowości» na krótki czas

Max-limit – Maksymalna prędkość, gdy nie działa Burst

Burst-treshhold – wartość decydująca o przyznaniu lub odebraniu dodatkowej przepustowości

The screenshot shows the 'New Simple Queue' configuration window. The 'General' tab is selected. The 'Name' field contains 'queue-burst'. The 'Target' dropdown is set to 'bridge1-lan'. The 'Dst.' field is empty. Under the 'Target Upload' and 'Target Download' sections, the 'Max Limit' is set to '2M'. In the 'Burst' section, 'Burst Limit' is '4M', 'Burst Threshold' is '1500K', and 'Burst Time' is '16'. The 'Time' section is collapsed. The 'enabled' checkbox at the bottom is checked. On the right side, there are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Reset Counters', 'Reset All Counters', and 'Torch'.

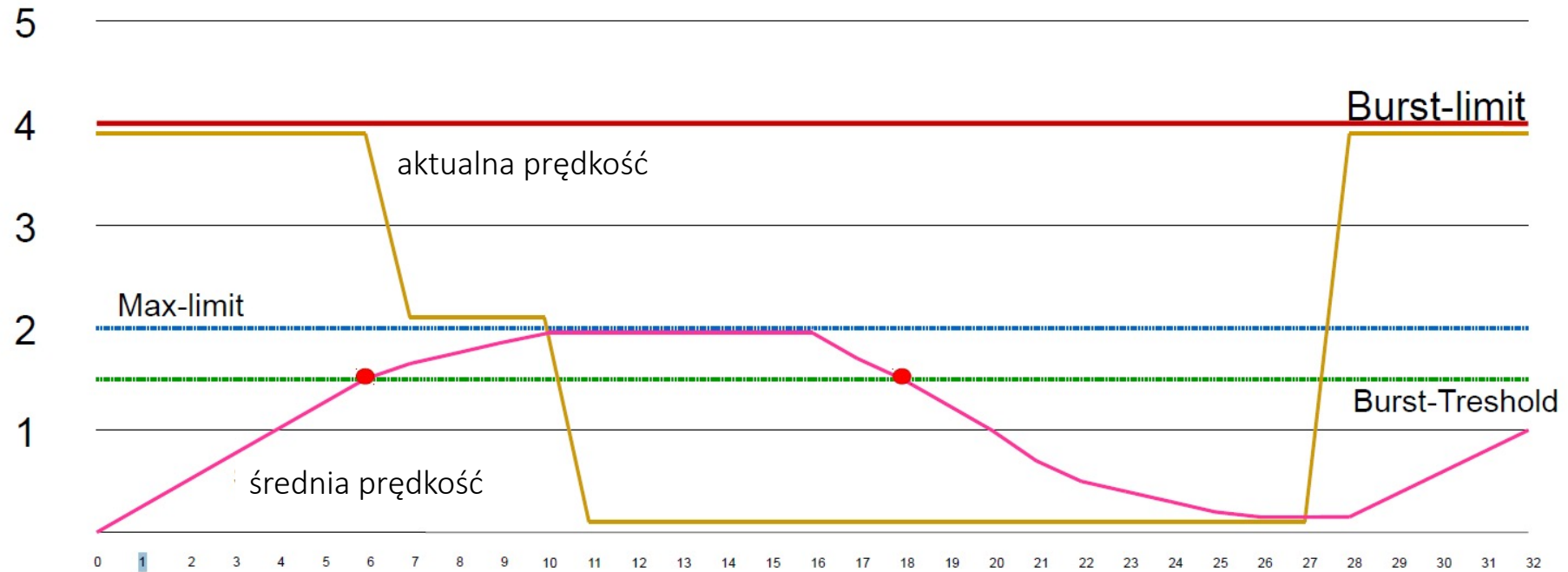
Burst-limit maksymalna wartość transferu w momencie gdy **Burst** jest przyznany

Burst-time – okres czasu (w sekundach) z jakiego obliczana jest średnia wartość transferu

QoS

Burst

burst-time=16, max-limit=2M, burst-treshold=1500K, burst-limit=4M



- **Burst-limit** maksymalna wartość transferu w momencie gdy burst jest dozwolony
- **Burst-time** – okres czasu (w sekundach) z jakiego obliczana jest średnia wartość transferu
- **Average-rate** – średnia wartość obliczana dla **Burst-time**
- **Actual-rate** – aktualna wartość transferu
- **Burst-treshhold** – wartość poniżej, której użytkownik pracuje na swoją nagrodę

QoS

Burst / Obliczenia

Średnia z ostatnich 16 sekund (Burst-time=16)



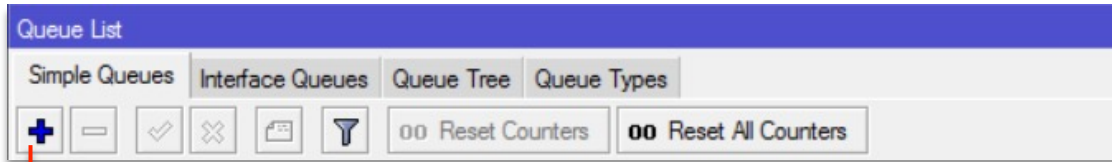
| | | | | |
|------------------|---|--|----------------------------|--------------|
| <i>Sekunda 0</i> | $(0+0+0+0+0+0+0+0+0+0+0+0+0+0+0+0)/16=0\text{Kbps}$ | <i>average-rate < burst-threshold</i> | <i># Burst is allowed</i> | 4Mbps |
| <i>Sekunda 1</i> | $(0+0+0+0+0+0+0+0+0+0+0+0+0+0+0+4)/16=250\text{Kbps}$ | <i>average-rate < burst-threshold</i> | <i># Burst is allowed</i> | 4Mbps |
| <i>Sekunda 2</i> | $(0+0+0+0+0+0+0+0+0+0+0+0+0+0+4+4)/16=500\text{Kbps}$ | <i>average-rate < burst-threshold</i> | <i># Burst is allowed</i> | 4Mbps |
| <i>Sekunda 3</i> | $(0+0+0+0+0+0+0+0+0+0+0+0+0+4+4+4)/16=750\text{Kbps}$ | <i>average-rate < burst-threshold</i> | <i># Burst is allowed</i> | 4Mbps |
| <i>Sekunda 4</i> | $(0+0+0+0+0+0+0+0+0+0+0+4+4+4+4)/16=1000\text{Kbps}$ | <i>average-rate < burst-threshold</i> | <i># Burst is allowed</i> | 4Mbps |
| <i>Sekunda 5</i> | $(0+0+0+0+0+0+0+0+0+0+4+4+4+4+4)/16=1250\text{Kbps}$ | <i>average-rate < burst-threshold</i> | <i># Burst is allowed</i> | 4Mbps |
| <i>Sekunda 6</i> | $(0+0+0+0+0+0+0+0+4+4+4+4+4+4+4)/16=1500\text{Kbps}$ | <i>average-rate > burst-threshold</i> | <i># Burst not allowed</i> | 2Mbps |



Aktualnie dozwolona prędkość

QoS

Simple Queue



| # | Name | Target | Upload Max Limit | Download Max Limit | Packet Marks | Total Max Limit (bits/s) |
|---|------------|-------------|------------------|--------------------|--------------|--------------------------|
| 0 | queue-lan | bridge1-lan | 5M | 5M | | |
| 1 | queue-lan2 | bridge1-lan | 14M | 20M | | |

General | Advanced | Statistics | Traffic | Total | Total Statistics

Name: queue-lan

Target: bridge1-lan

Dst.: [dropdown]

Target Upload: Max Limit: 5M

Target Download: Max Limit: 5M bits/s

Burst Limit: unlimited bits/s

Burst Threshold: unlimited bits/s

Burst Time: 0 s

enabled

Możemy określić:

- interfejs
- adres IP hosta 192.168.10.56
- adres sieci 192.168.10.0/24

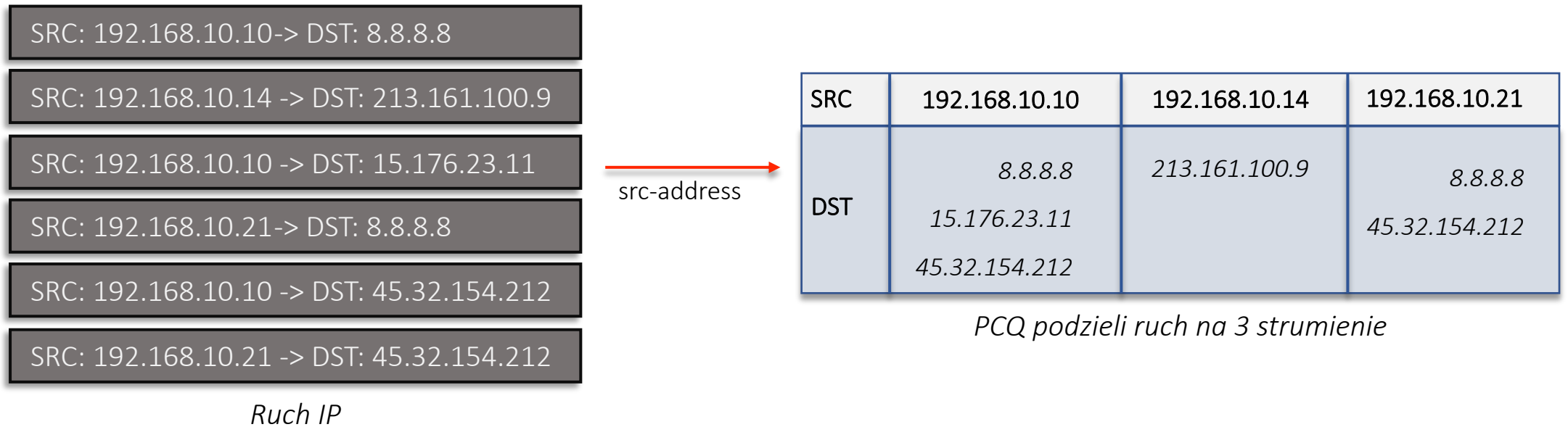
Max-limit – maksymalna prędkość upload/download dla użytkowników podłączonych do interface bridge1-lan wyniesie 5M/5M

Simple Queue przetwarzane są sekwencyjnie. Widzimy, iż mamy dwie kolejki dla tego samego interfejsu. Tylko pierwsza zadziała

QoS

PCQ / Przykład

Per Connection Queue (PCQ) rodzaj kolejki wykorzystywany do sprawiedliwego wykorzystania pasma, w przypadku, gdy mamy zmieniającą się liczbę użytkowników. PCQ stworzy strumienie na podstawie klasyfikatora (dst-address, src-address, dst-port, src-port)

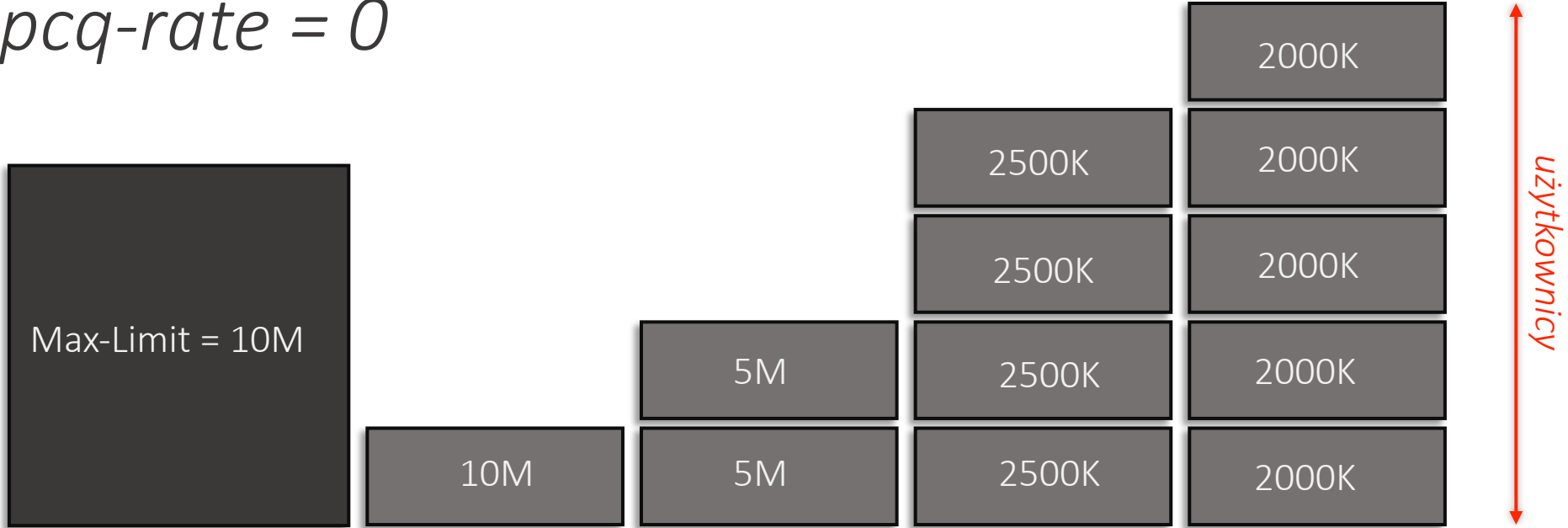


Powyżej mechanizm **pcq** dla klasyfikatora src-address
Każdy ze strumieni otrzyma takie samo pasmo do wykorzystania

QoS

pcq-rate

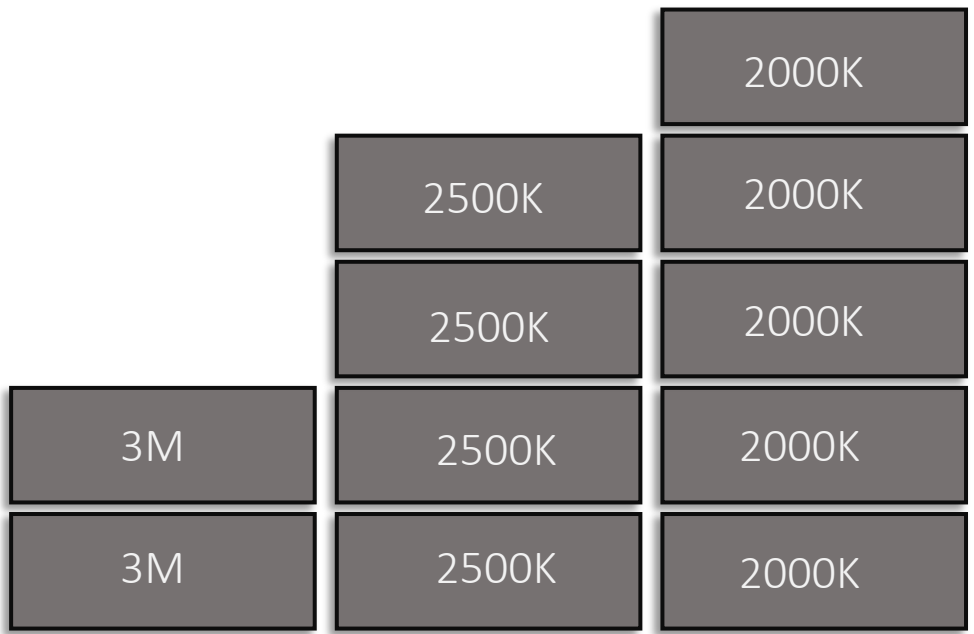
pcq-rate = 0



QoS

pcq-rate

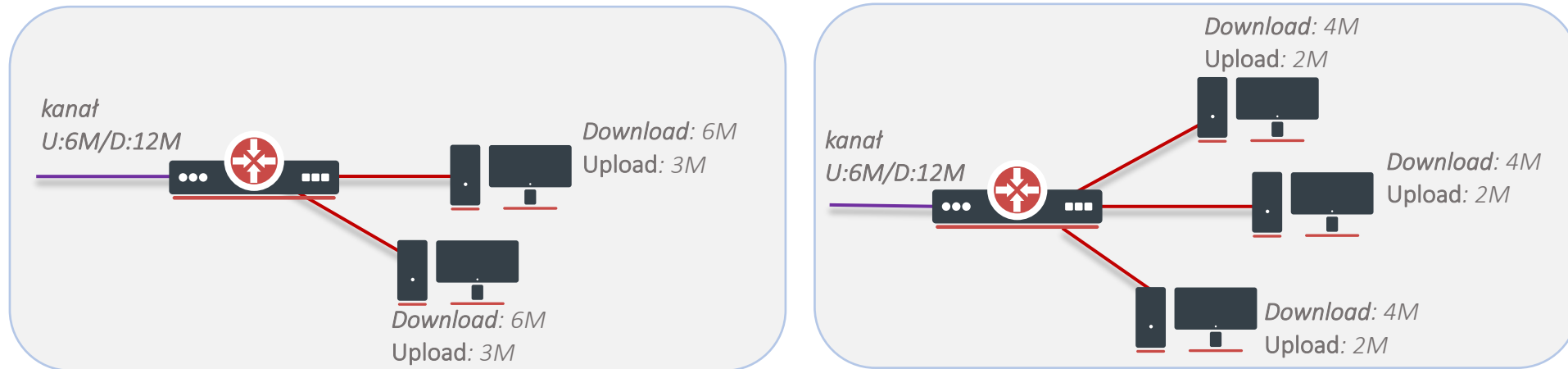
pcq-rate = 3M



QoS

PCQ / Przykład

W biurze dysponujemy łączem upload 6M, download 12M chcemy aby każdy z użytkowników dostał taką samą przepustowość. Problem polega na tym, że nasi użytkownicy czasami pracują z domu, a czasami z biura. Nie jesteśmy w stanie zdefiniować ilu użytkowników w danym dniu będzie w biurze. Kolejowanie powinno automatycznie dostosować się do liczby użytkowników i w zależności od ich liczby przydzielić im pasmo na łączu.



```
/queue type add name="PCQ_download", kind=pcq pcq-rate=0 pcq-classifier=dstaddress  
/queue type add name="PCQ_upload" kind=pcq pcq-rate=0 pcq-classifier=src-address  
/queue simple add target-addresses=192.168.0.0/24 queue=PCQ_upload/PCQ_download max-limit=6M/12M
```

PPP / VPN / TUNELE

Tunele

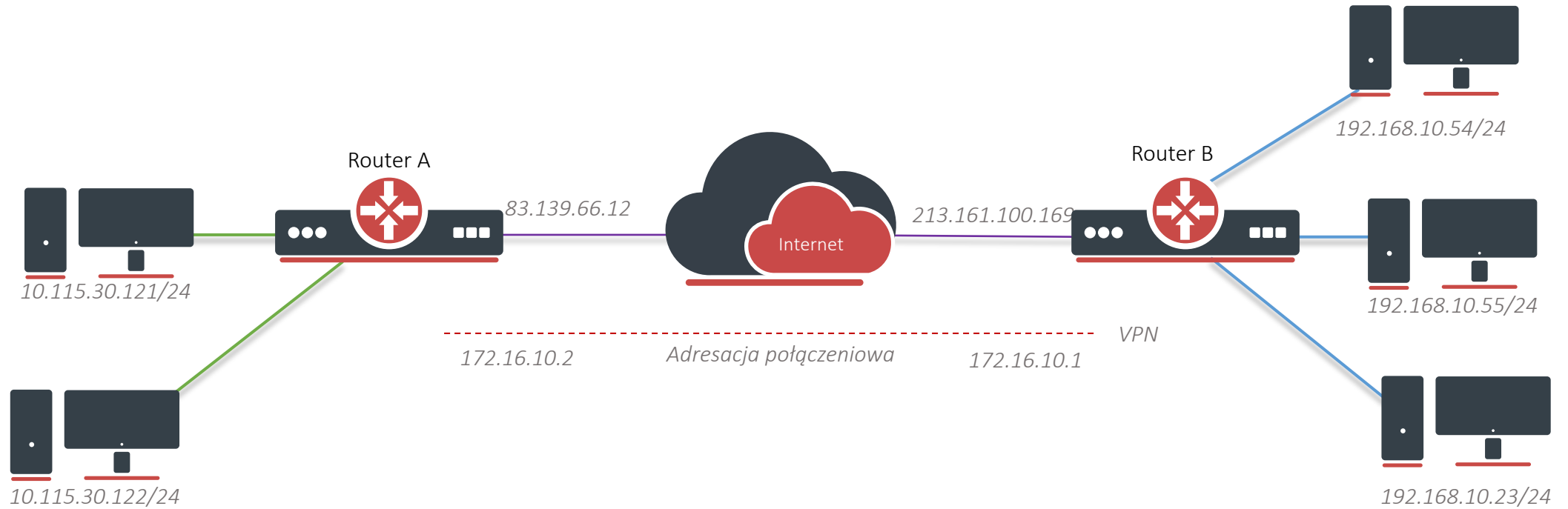
- Pozwala na szyfrowanie komunikacji
- Możliwość połączenia się z zewnątrz do sieci korporacyjnej
- Można wyeliminować problemy z NAT'em (usługi, które słabo przechodzą przez NAT np. VoIP)
- Ułatwia zarządzanie polityką bezpieczeństwa
- Adresacja Punkt-Punkt, wygodny sposób przydzielania klientom adresów IP (np. PPPoE)

Cechy dobrych tuneli:

- Wspiera silne algorytmy kryptograficzne
- Łatwy do implementacji, konfiguracji
- Dostępny dla różnych systemów operacyjnych bez konieczności instalowania dodatkowego oprogramowania
- Sprzętowe wsparcie po stronie routera, koncentratora

Tunele

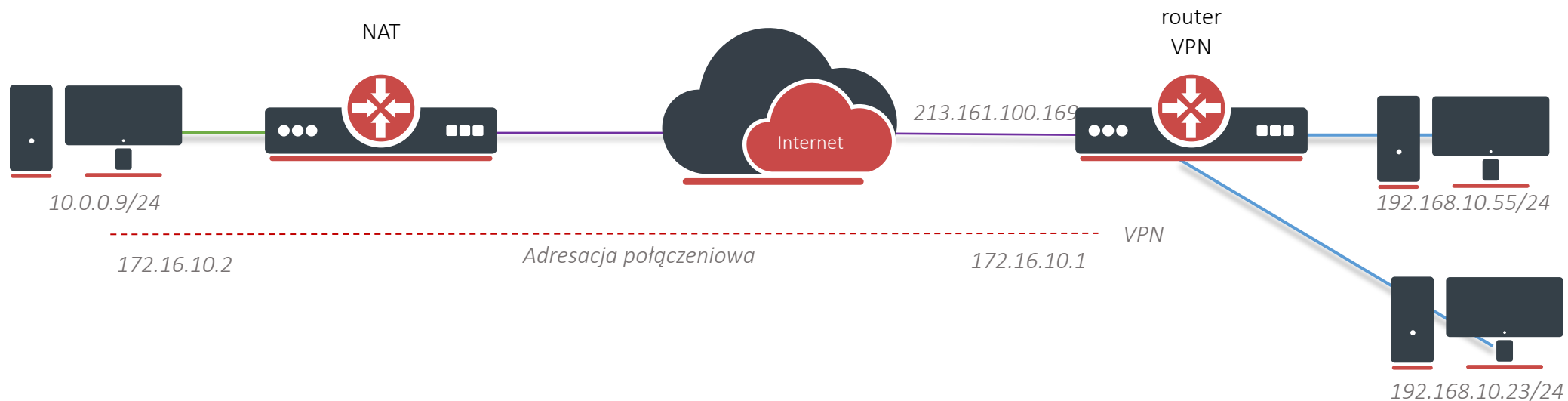
Site to site



Dwa oddziały firmy połączone tunelem typu VPN
Komunikacja pomiędzy sieciami **10.115.30.0/24** a **192.168.10.0/24** odbywa się poprzez kanał VPN.
Oba oddziały posiadają zewnętrzne adresy IP.

Tunele

Dostęp zdalny / Road-Warrior

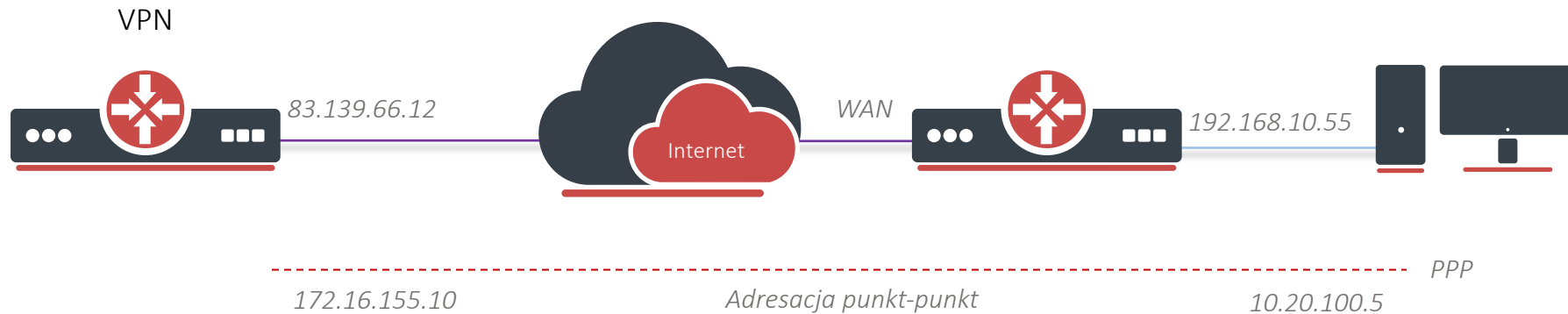


Użytkownik mobilny łączy się z oddziałem firmy z dowolnego miejsca (kawiarnia, dom, hotel), może znajdować się za NAT'em. Po poprawnym zalogowaniu się (login, hasło), Router VPN przydzieli mu specjalny adres połączeniowy (172.16.10.2). Użytkownik za pomocą tej adresacji będzie miał dostęp do sieci 192.168.10.0/24. Dodatkowo użytkownik może mieć ustawioną opcję **Add Default Route**, dzięki czemu cały jego ruch będzie teraz obsługiwany za pomocą połączenia VPN

Tunele

Adresacja punkt-punkt

- Specjalny typ adresacji wspierany przez protokoły z grupy PPP
- Adresacja nie wymaga istnienia adresu sieci i adresu rozgłoszeniowego
- Zakończenia tunelu mają adresy z maską /32



Tunele

Konfiguracja użytkowników (ppp)

Interface

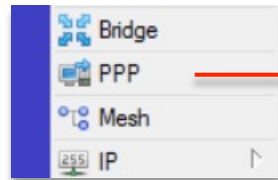
- podłączeni klienci
- my, jako klienci sieci VPN
- uruchomienie serwerów (PPTP, SSTP, L2TP, OVPN)
- ...

Użytkownicy

- login
- hasło
- adresacja ppp
- profil z dodatkowymi ustawieniami
- ...

Profiles (dodatkowe ustawienia)

- adresacja ppp
- kompresja
- czy dane powinny być szyfrowane
- ...



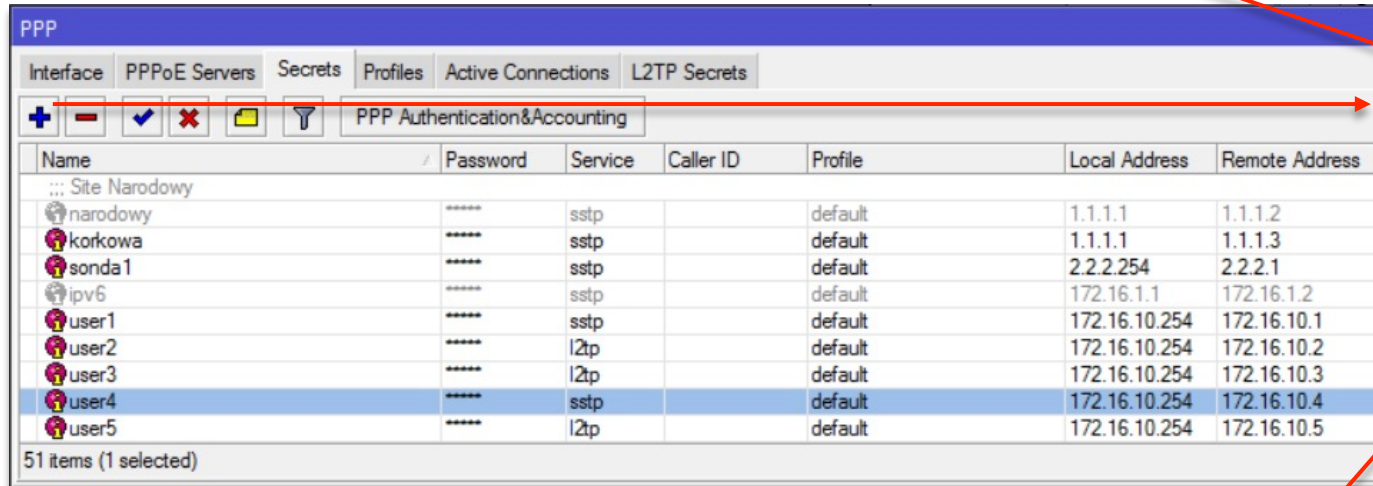
Konieczna jest aktywna paczka ppp

| Name | Password | Service | Caller ID | Profile | Local Address | Remote Address | Last Logged Out |
|--------------------|----------|---------|---------------|---------|---------------|----------------|----------------------|
| user3 | **** | l2tp | | default | 172.16.10.254 | 172.16.10.3 | Aug/24/2017 11:31:12 |
| user4 | **** | sstp | | default | 172.16.10.254 | 172.16.10.4 | Aug/25/2017 10:59:47 |
| user5 | **** | l2tp | | default | 172.16.10.254 | 172.16.10.5 | Aug/24/2017 13:44:42 |
| user6 | **** | l2tp | | default | 172.16.10.254 | 172.16.10.6 | Aug/24/2017 14:31:26 |
| user7 | **** | pptp | | default | 172.16.10.254 | 172.16.10.7 | Aug/20/2017 09:57:28 |
| user8 | **** | pptp | | default | 172.16.10.254 | 172.16.10.8 | Aug/20/2017 09:57:28 |
| user9 | **** | any | | default | 172.16.10.254 | 172.16.10.9 | Aug/20/2017 09:57:28 |
| user10 | **** | any | | default | 172.16.10.254 | 172.16.10.10 | Aug/20/2017 09:57:28 |
| user11 | **** | any | | default | 172.16.10.254 | 172.16.10.11 | Aug/20/2017 09:57:28 |
| user12 | **** | any | | default | 172.16.10.254 | 172.16.10.12 | Aug/20/2017 09:57:28 |
| user13 | **** | any | | default | 172.16.10.254 | 172.16.10.13 | Aug/20/2017 09:57:28 |
| user14 | **** | any | | default | 172.16.10.254 | 172.16.10.14 | Aug/20/2017 09:57:28 |
| user15 | **** | any | | default | 172.16.10.254 | 172.16.10.15 | Mar/18/2017 11:13:39 |
| user16 | **** | any | | default | 172.16.10.254 | 172.16.10.16 | Mar/18/2017 11:12:38 |
| user17 | **** | any | | default | 172.16.10.254 | 172.16.10.17 | |
| p1 | **** | any | | default | 172.16.10.254 | 172.16.10.55 | |
| ... BIURO OGRODOWA | | | | | | | |
| ogrodowa | **** | sstp | | default | 172.16.10.100 | 172.16.10.101 | Sep/20/2017 02:58:52 |
| piotr | **** | pptp | 82.134.33.215 | unknown | 172.16.10.254 | 172.16.10.222 | |
| hap1 | **** | l2tp | | default | 172.16.22.1 | 172.16.22.2 | Aug/25/2017 09:57:56 |
| hap2 | **** | l2tp | | default | 172.16.22.1 | 172.16.22.3 | Aug/24/2017 20:22:56 |
| ppp1 | **** | pppoe | | default | 172.16.65.254 | 172.16.65.1 | May/20/2017 14:16:01 |
| ppp2 | **** | pppoe | | default | 172.16.65.254 | 172.16.65.2 | May/21/2017 09:16:50 |
| ppp3 | **** | pppoe | | default | 172.16.65.254 | 172.16.65.3 | May/21/2017 09:16:29 |
| ppp4 | **** | pppoe | | default | 172.16.65.254 | 172.16.65.4 | |

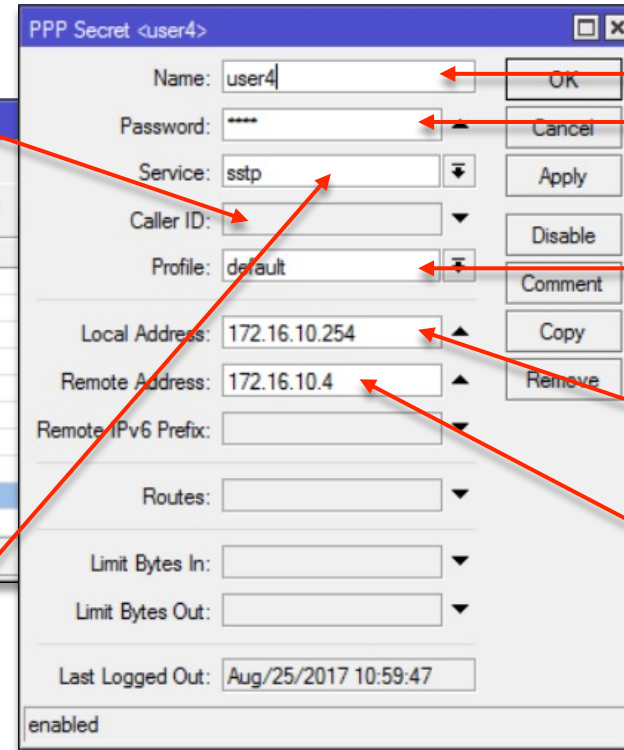
Tunele

Konfiguracja użytkowników (ppp)

ograniczenie adresu IP, z którego klient może się podłączyć



| Name | Password | Service | Caller ID | Profile | Local Address | Remote Address |
|---------------|----------|---------|-----------|---------|---------------|----------------|
| Site Narodowy | | | | | | |
| narodowy | ***** | sstp | | default | 1.1.1.1 | 1.1.1.2 |
| korkowa | ***** | sstp | | default | 1.1.1.1 | 1.1.1.3 |
| sonda 1 | ***** | sstp | | default | 2.2.2.254 | 2.2.2.1 |
| ipv6 | ***** | sstp | | default | 172.16.1.1 | 172.16.1.2 |
| user1 | ***** | sstp | | default | 172.16.10.254 | 172.16.10.1 |
| user2 | ***** | l2tp | | default | 172.16.10.254 | 172.16.10.2 |
| user3 | ***** | l2tp | | default | 172.16.10.254 | 172.16.10.3 |
| user4 | ***** | sstp | | default | 172.16.10.254 | 172.16.10.4 |
| user5 | ***** | l2tp | | default | 172.16.10.254 | 172.16.10.5 |



PPP Secret <user4>

Name: user4
Password: ****
Service: sstp
Caller ID:
Profile: default
Local Address: 172.16.10.254
Remote Address: 172.16.10.4
Remote IPv6 Prefix:
Routes:
Limit Bytes In:
Limit Bytes Out:
Last Logged Out: Aug/25/2017 10:59:47
enabled

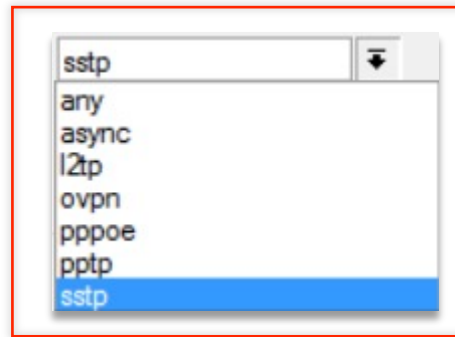
login

hasło

dodatkowe
ustawienia

adresacja ppp
strona router'a

adresacja ppp
strona klienta

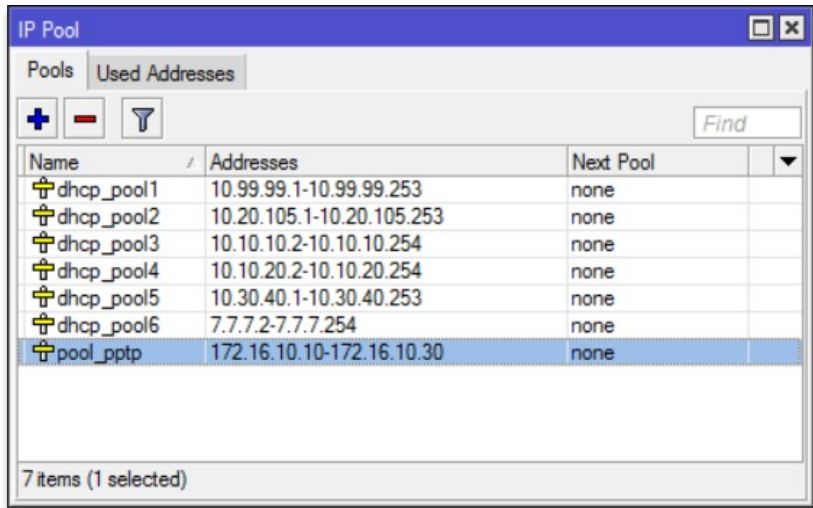


sstp
any
async
l2tp
ovpn
pppoe
pptp
sstp

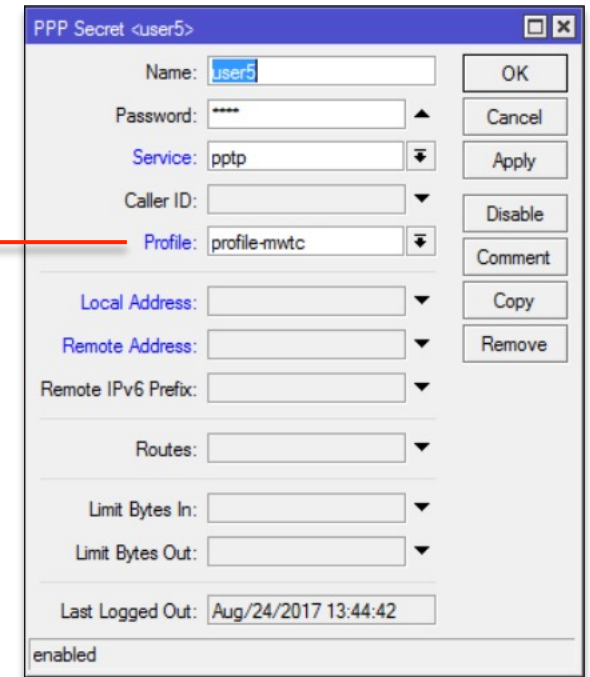
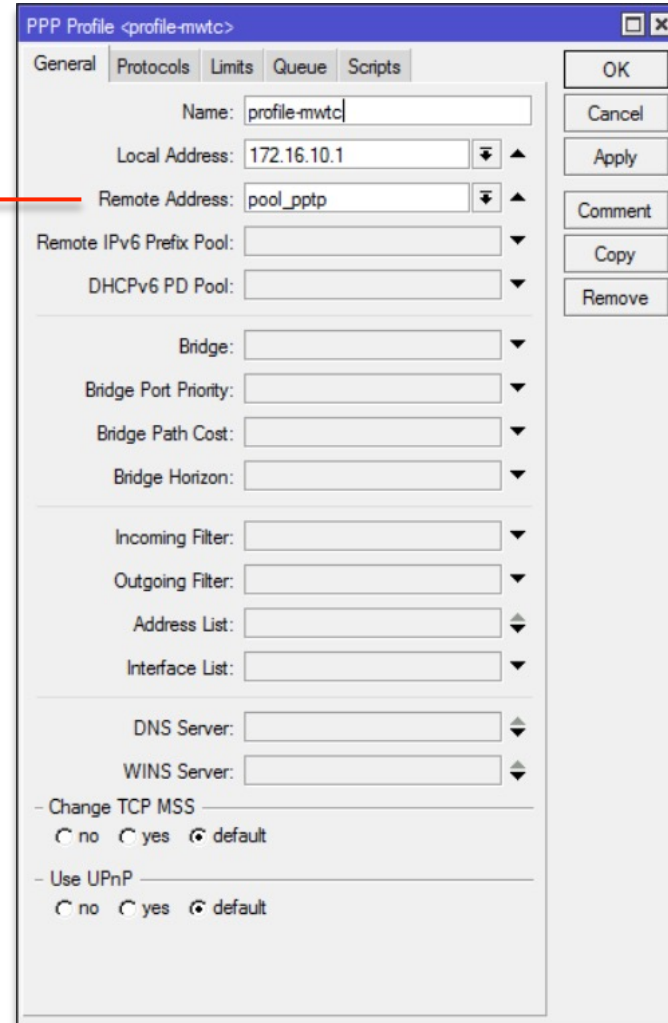
Usługi do jakich klient będzie mógł się podłączyć

Tunele

ppp / profile



Gdy mamy wielu użytkowników usług PPP możemy zdefiniować zakres (IP pool) adresów (podobnie jak dla DHCP), który będzie przydzielany.

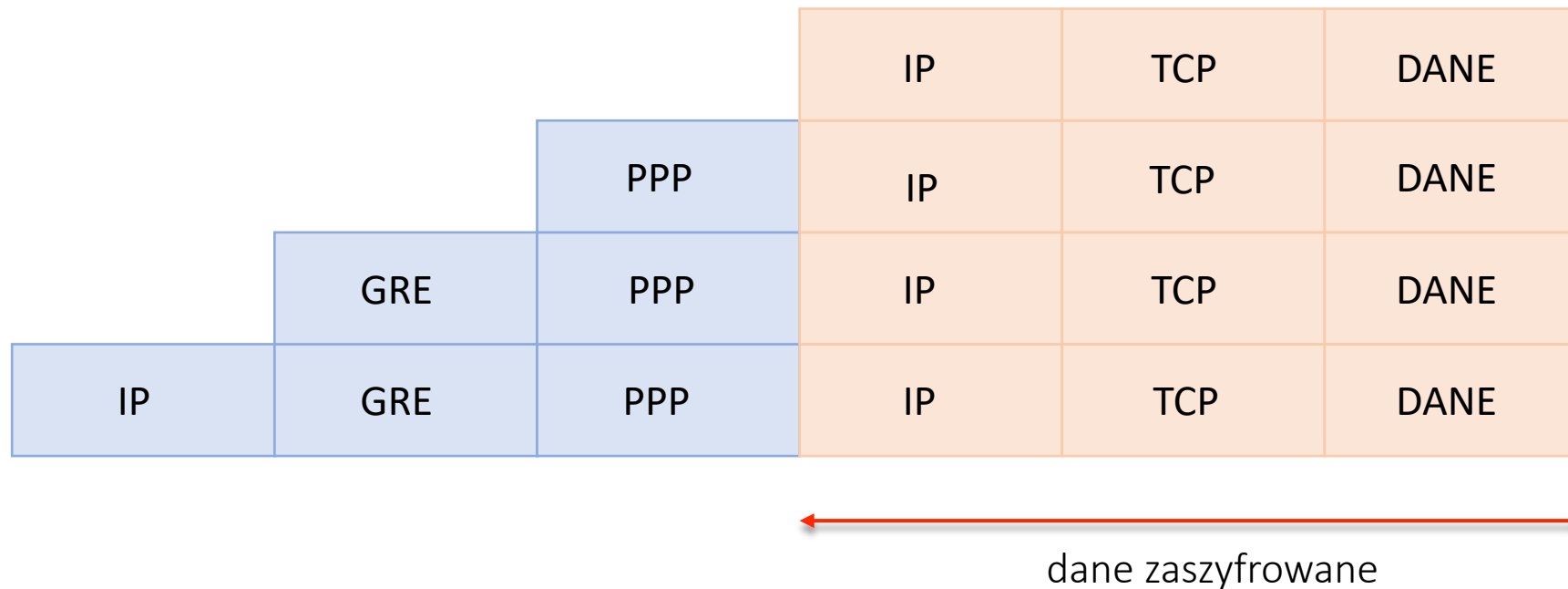


W tym wypadku nie podajemy **Local Address**, **Remote Address**. Dane zostaną pobrane z konfiguracji profilu **profile-mwtc**

Tunele

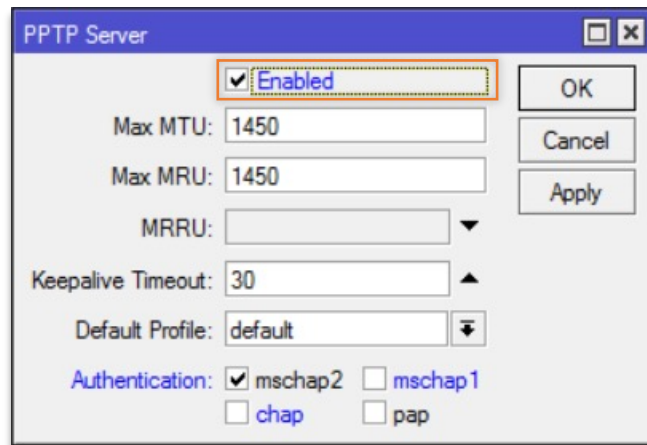
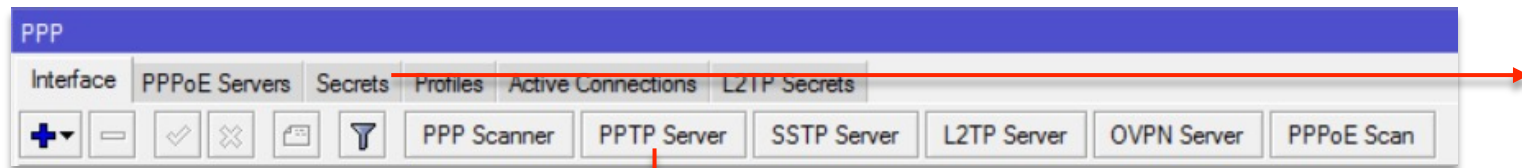
PPTP

- Używa protokołu **1723/TCP** oraz protokołu **GRE (numer 47)**
- Łatwy w konfiguracji
- Dostępny w wielu systemach operacyjnych
- Mało bezpieczny



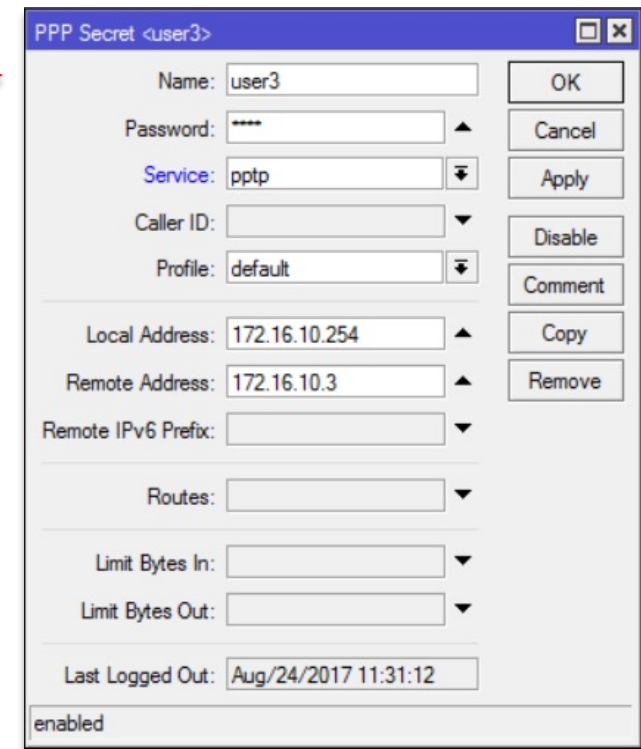
Tunele

PPTP serwer



Uruchomienie serwera

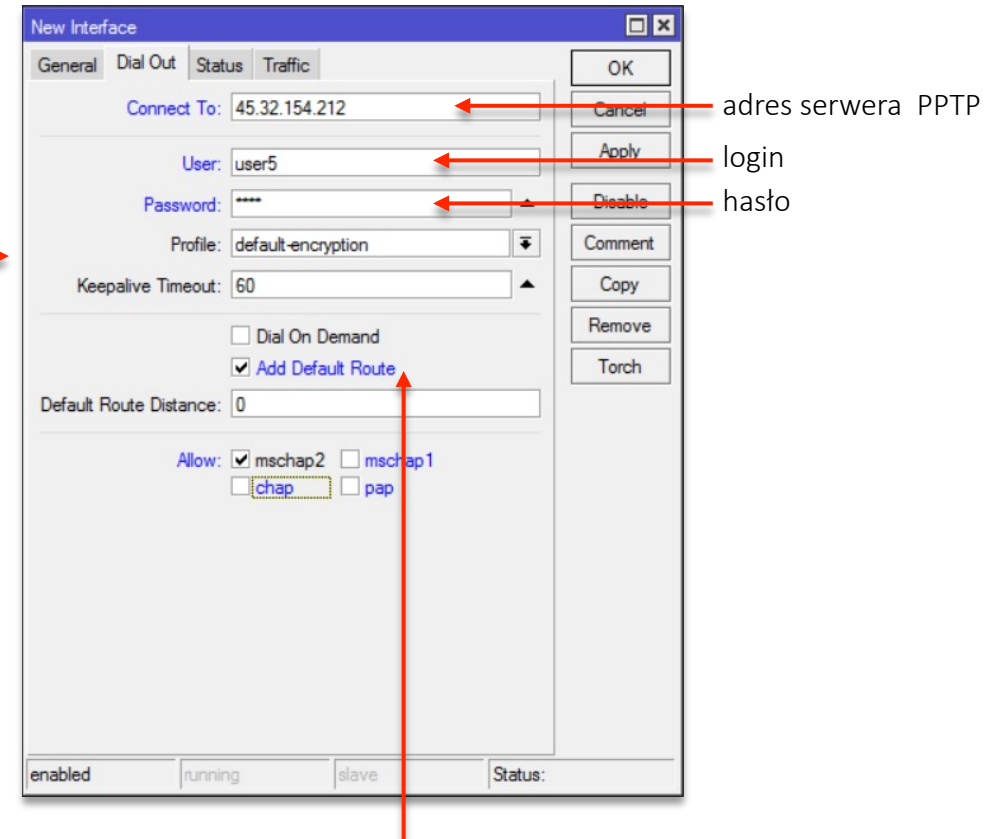
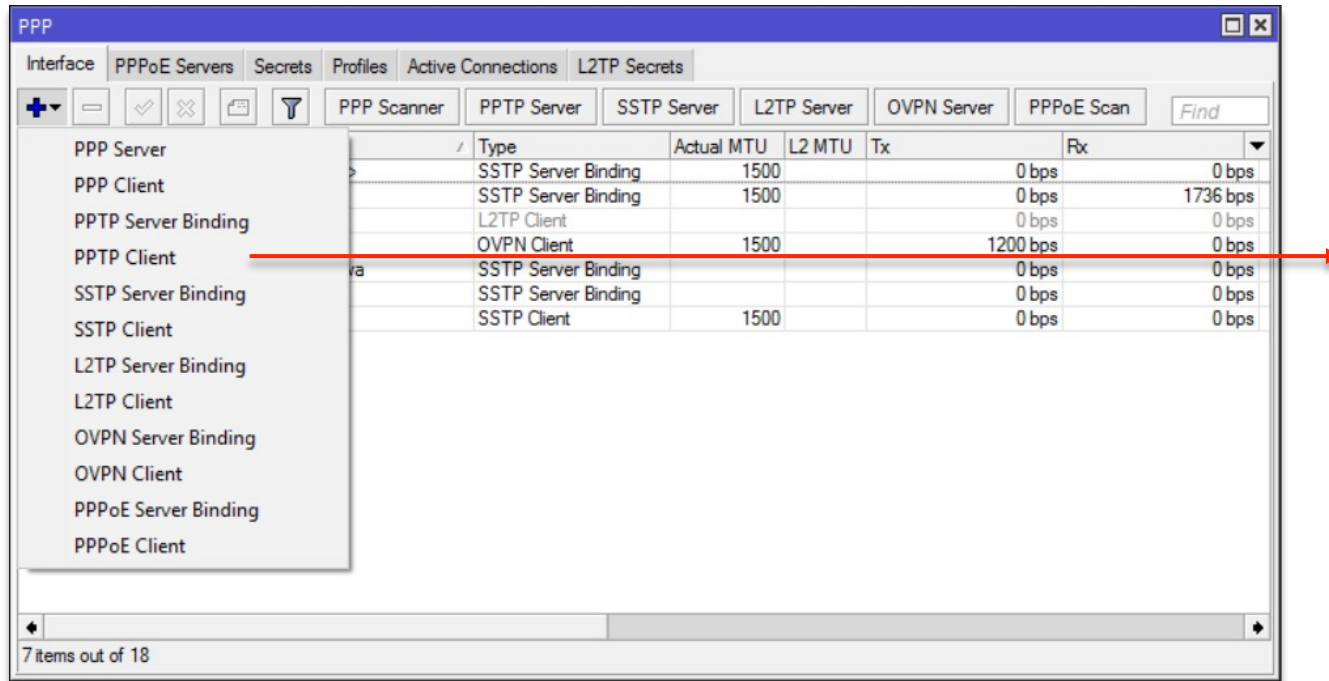
Serwer PPTP nasłuchuje na wszystkich interfejsach naszego routera. Należy zabezpieczyć do niego dostęp, stosując reguły firewall'a. Należy odblokować dostęp dla protokołu **TCP port 1723**, oraz protokół **GRE**, dla interfejsów i adresów, na których zezwalamy na połączenie.



Dodanie użytkownika

Tunele

PPTP klient



Po nawiązaniu połączenia z serwerem PPTP w tablicy routing'u pojawi się wpis 0.0.0.0/0 wskazujący jako gateway serwer VPN. Przydatne, gdy chcemy aby cały ruch od klienta przechodził przez nasz router.

Tunele

SSTP

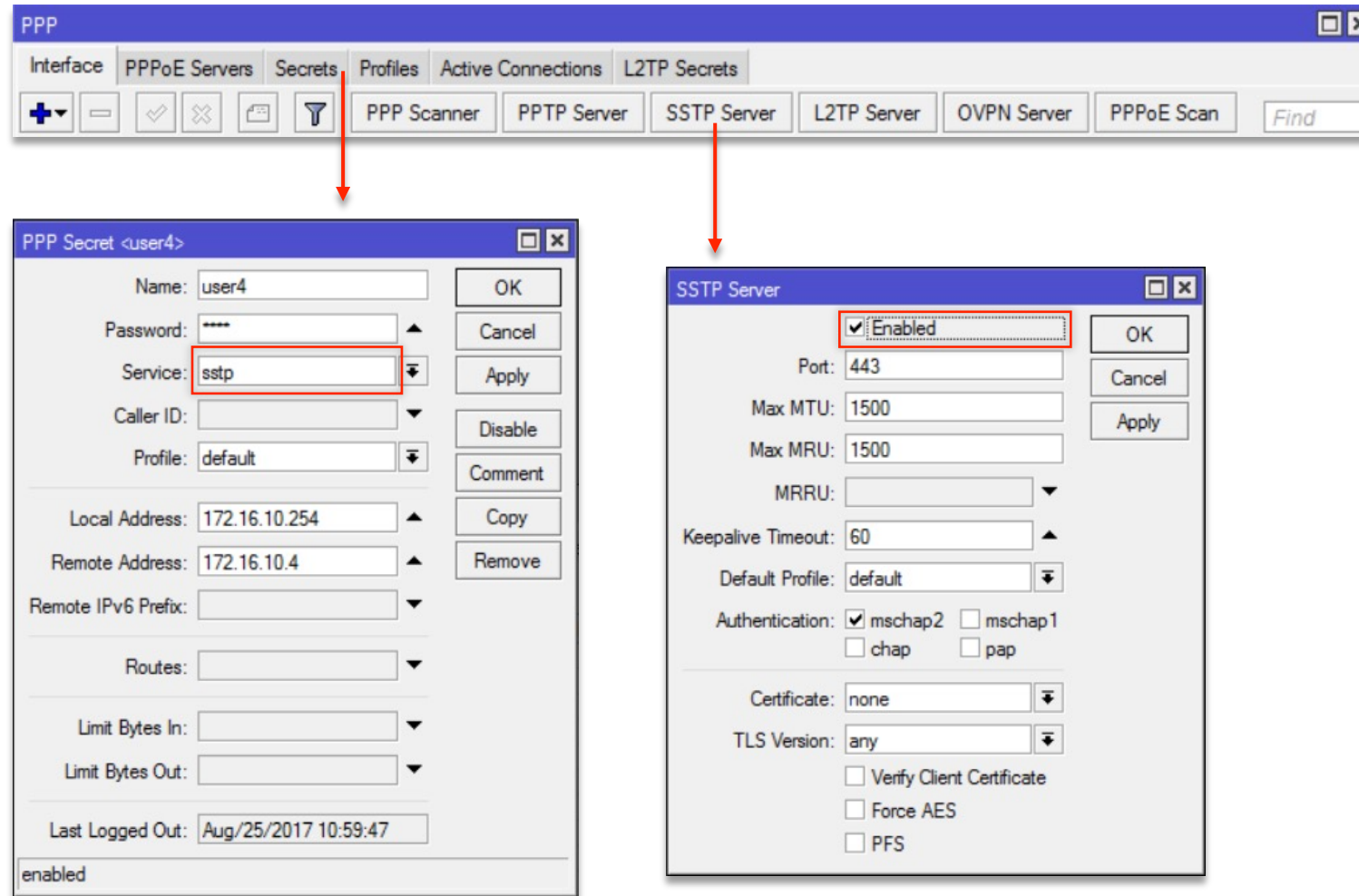
- Następca protokołu PPTP
- Autorem rozwiązania jest Microsoft
- Silny algorytm szyfrujący AES
- Słabe wsparcie dla systemów innych niż Windows
- Uwierzytelnienie można oprzeć o hasła lub certyfikaty
- Domyślnie korzysta z 443/TCP, łatwo przechodzi przez firewall

Dwa routery MikroTik można ze sobą połączyć, stosując uwierzytelnienie oparte o hasło (certyfikaty nie są wymagane).

Aby podłączyć się za pomocą klienta wbudowanego w system Windows konieczne jest skonfigurowanie certyfikatu na routerze

Tunele

SSTP serwer



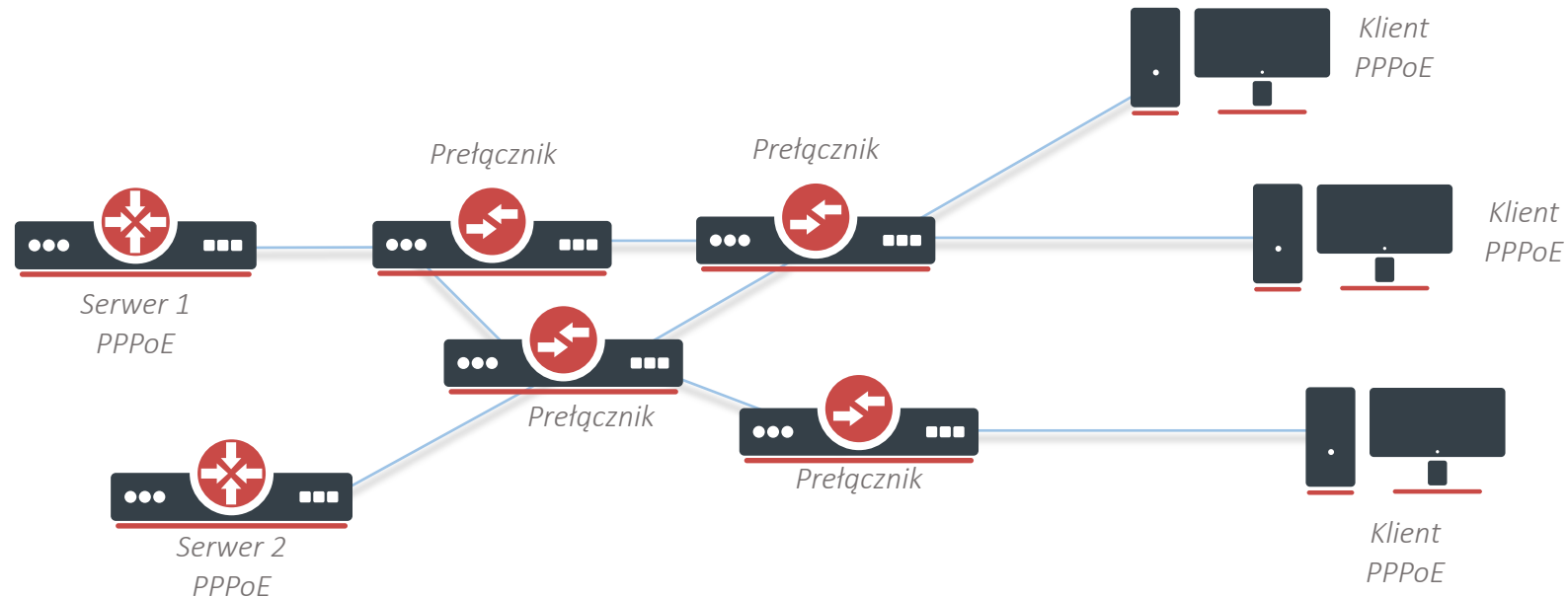
Dodanie użytkownika

Uruchomienie serwera

Tunele

PPPoE

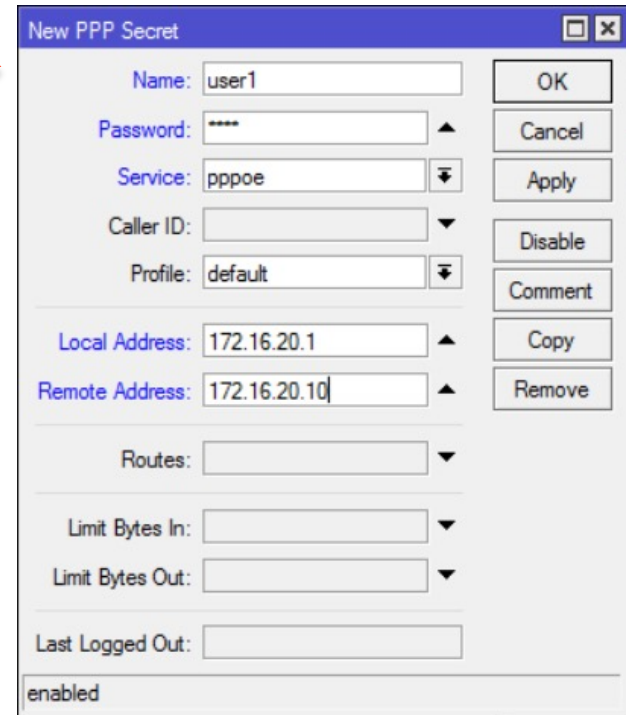
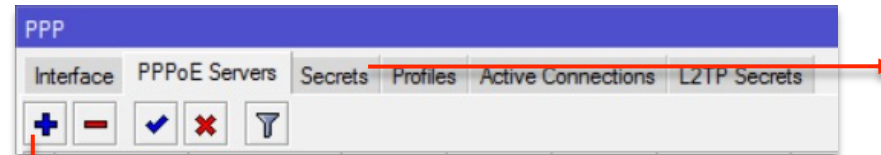
Aby zabezpieczyć sieć lokalną możemy wykorzystać protokół PPPoE. Mając w sieci dużo punktów dostępu (gniazdek) na otwartej przestrzeni możemy uzależnić dostęp użytkownika do sieci od loginów/hasła, bez których użytkownik nie będzie mógł korzystać z sieci pomimo, iż podłączył się do przełącznika.



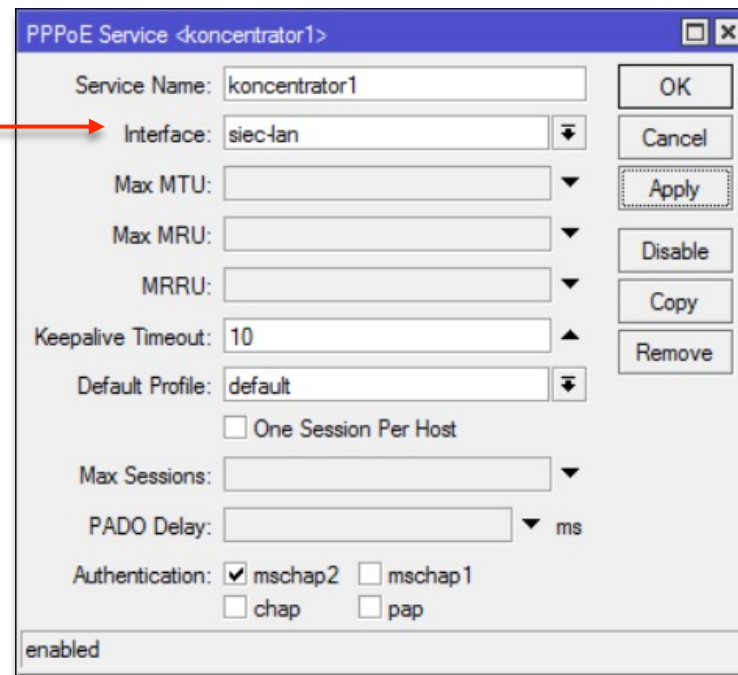
W danym segmencie sieci może znajdować się więcej niż jeden serwer (koncentrator) PPPoE

Tunele

PPPoE serwer

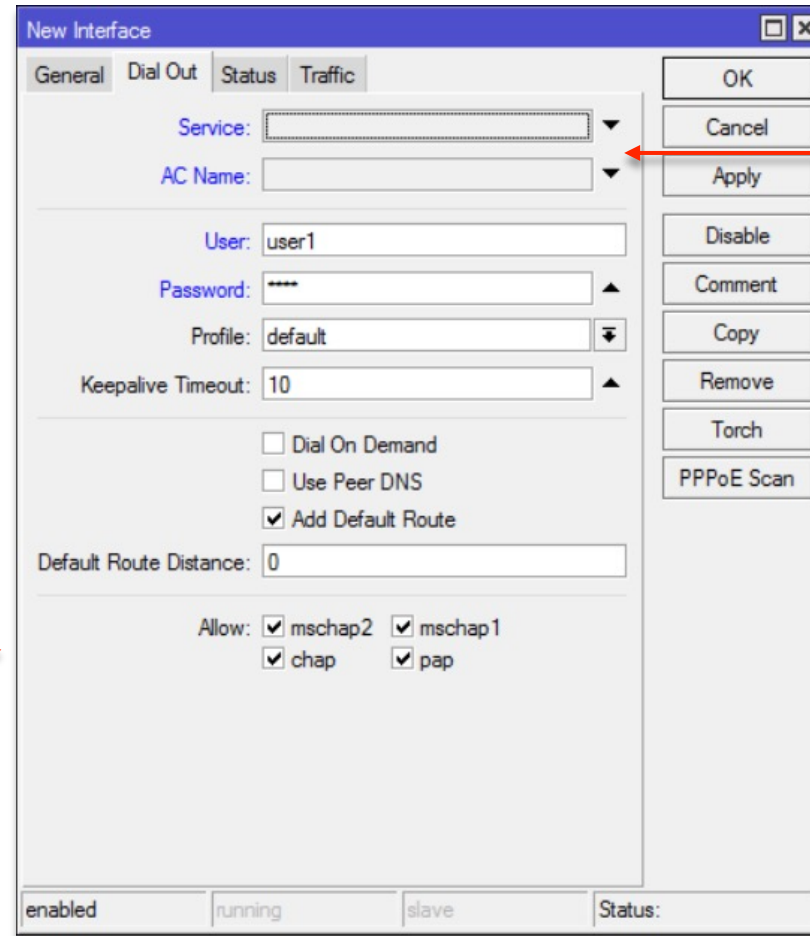
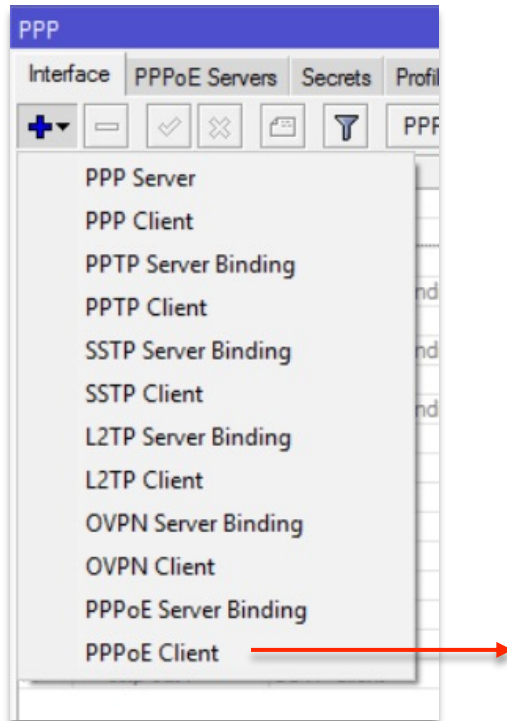


Serwer PPPoE musi być uruchomiony na interface warstwy drugiej (np. ether1, bridge, wlan1, EoIP)

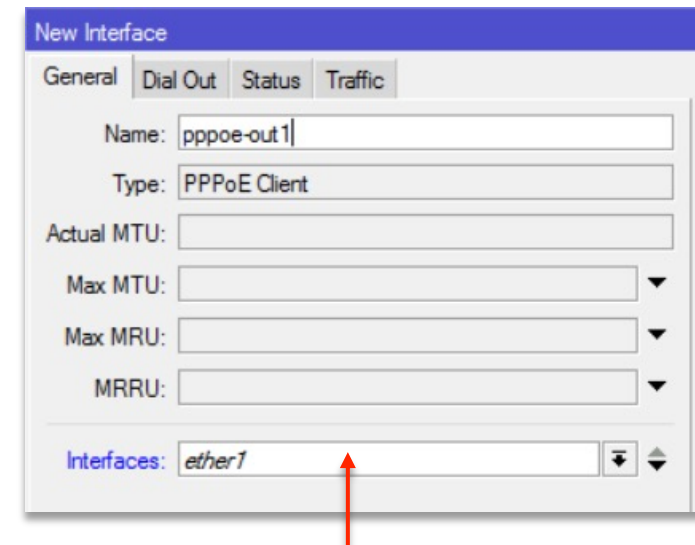


Tunele

PPPoE klient



W przypadku braku **Service** i **AC Name** klient podłączy się do pierwszego koncentratora, który mu odpowie. W przypadku środowisk, w których występuje kilka koncentratorów, klient ma możliwość określenia, do którego chciałby się połączyć.



W konfiguracji klienta konieczne musimy określić interface (warstwy drugiej), na którym zamierzamy uruchomić PPPoE klienta!

NARZĘDZIA

Narzędzia

e-mail

MikroTik umożliwia wysyłkę wiadomości email za pomocą zewnętrznego serwera SMTP.
W oknie Tools -> Email należy podać dane dostępowe do konta pocztowego.

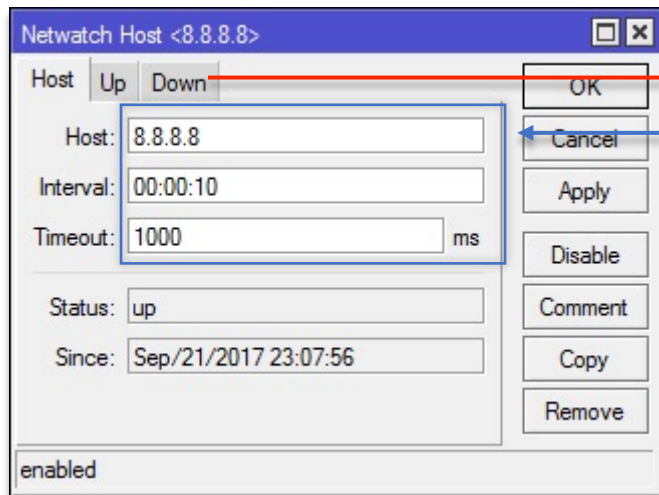
The image shows a screenshot of the MikroTik Tools menu on the left, with the 'Email' option highlighted. A red arrow points from 'Email' to the 'Email Settings' dialog box in the center. Another red arrow points from the 'Send Email' button in the 'Email Settings' dialog to the 'Send Email' dialog box on the right. The 'Email Settings' dialog contains the following fields: Server (serwer1775955.home.pl), Port (587), Start TLS (yes), From (<michal@mwtc.pl>), User (michal@mwtc.pl), and Password (masked). The 'Send Email' dialog contains: Address (serwer1775955.home.pl), Port (587), User (michal@mwtc.pl), Password (masked), a checkbox for TLS (unchecked), To (michal@ngt.com.pl), CC (empty), From (<michal@mwtc.pl>), Subject (Wiadomość testowa), and a text area for the body containing 'Mail wysłany z mikrotika'.

Mail może być również wysłany z linii komend, skryptu

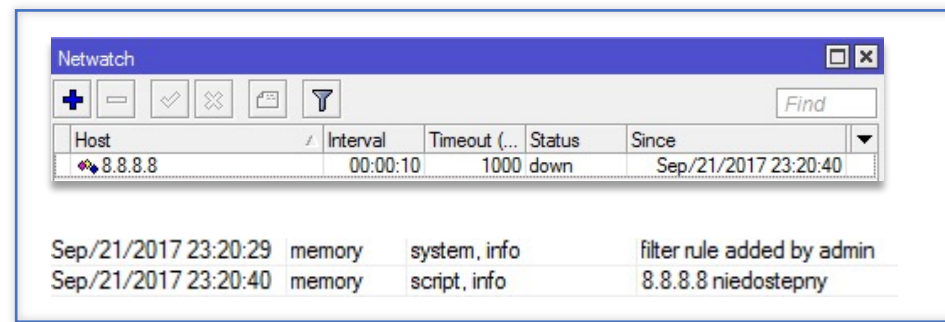
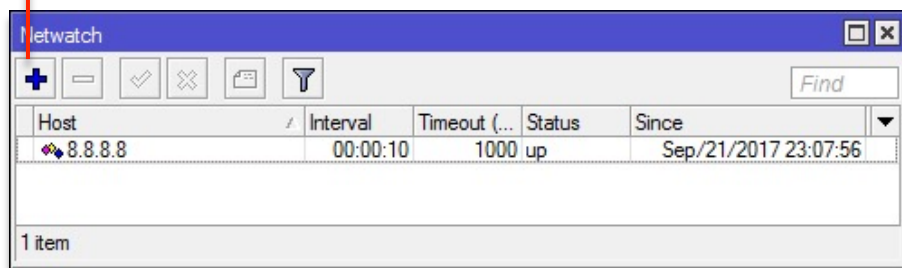
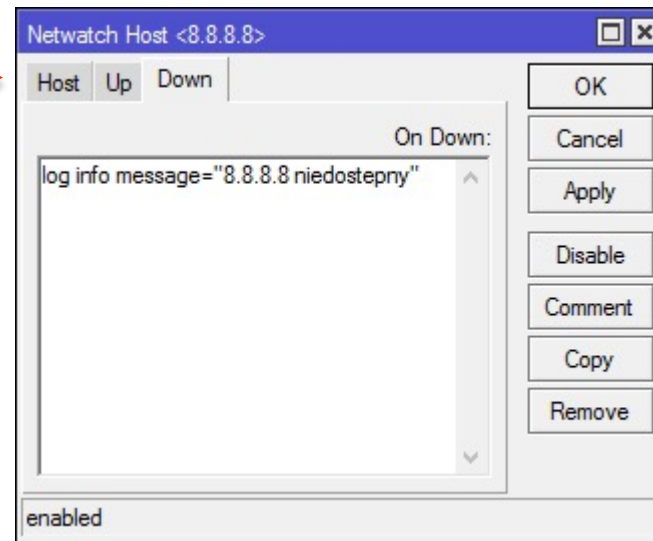
Narzędzia

Netwatch

Możemy sprawdzać, czy dany host jest osiągalny, a w momencie gdy przestanie odpowiadać na Echo Request (ping) wykonać skrypt.



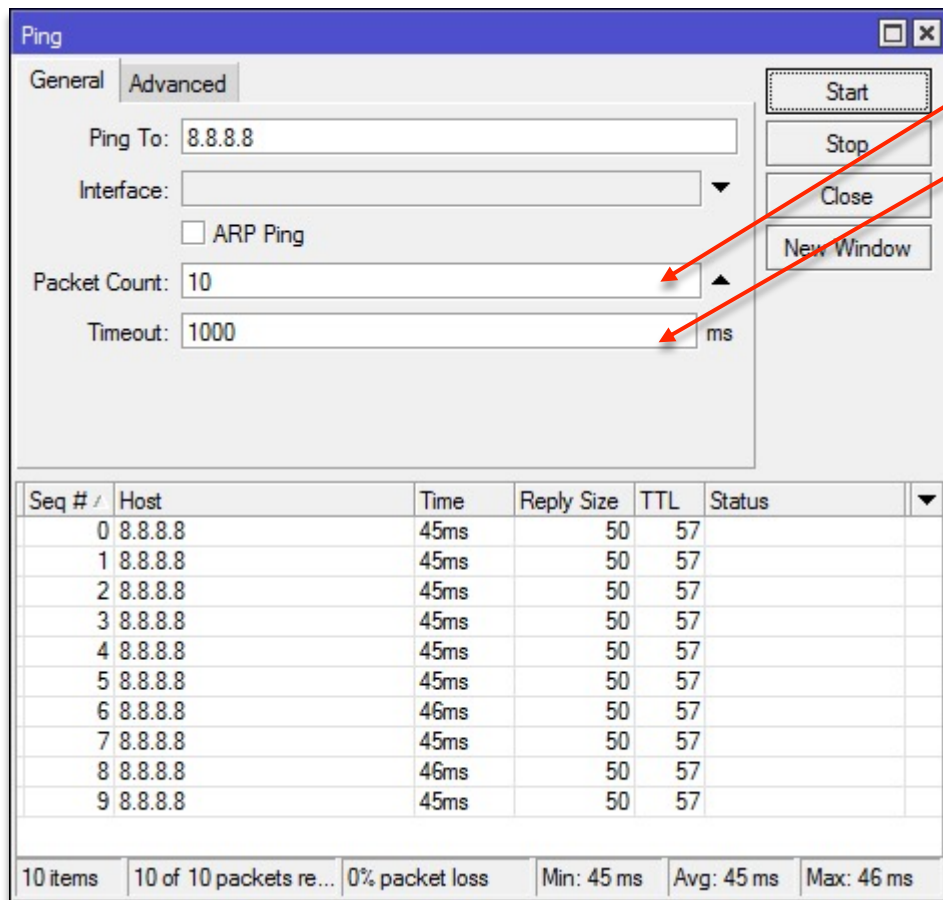
- Sprawdzamy, czy 8.8.8.8 odpowiada na ping
- Sprawdzamy co 10 sekund
- Na odpowiedź czekamy 1 sekunde



W przypadku niedostępności 8.8.8.8 pojawi się wpis w logu

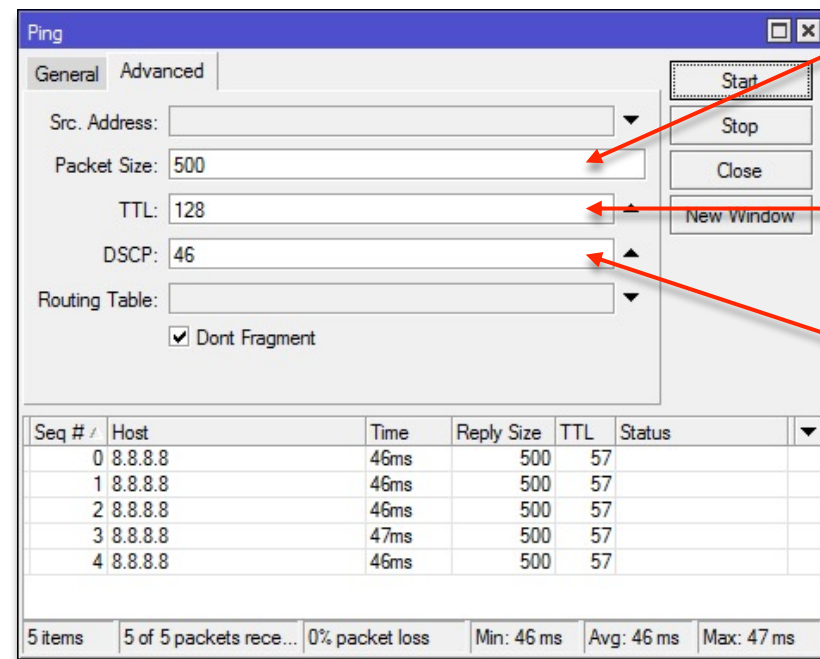
Narzędzia

ping



Ilość zapytań

Maksymalny czas oczekiwania na odpowiedź



Rozmiar pakietu w połączeniu z flagą **don't fragment** pozwala stwierdzić, jaki maksymalny pakiet można przesać bez fragmentacji

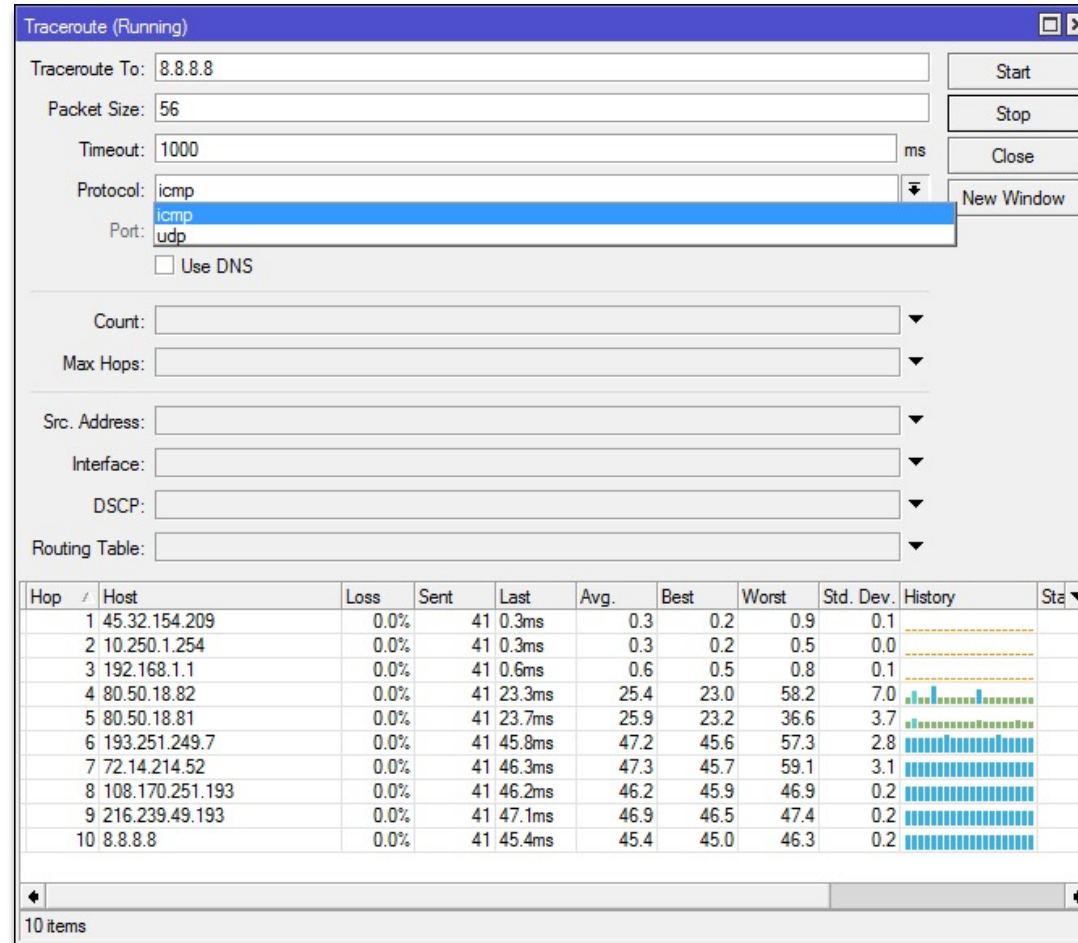
Time to Live

Sprawdzenie, czy w sieci używane są priorytety

Ustawienia zaawansowane

Narzędzia

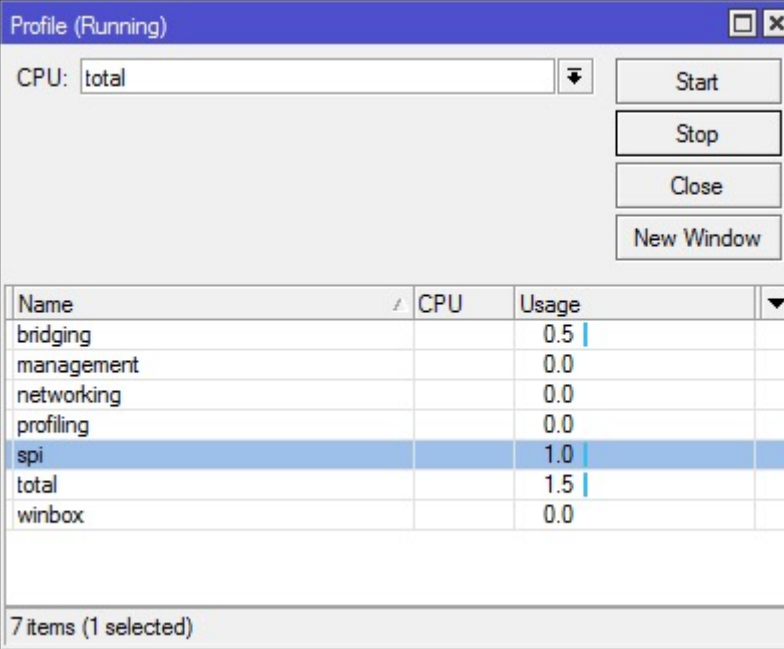
Traceroute



Pozwala zbadać ile routerów (hopów) pośredniczy w dostarczeniu pakietu do celu

Narzędzia

Profiler



The screenshot shows a window titled "Profile (Running)". At the top, there is a dropdown menu for "CPU:" set to "total". To the right of this menu are four buttons: "Start", "Stop", "Close", and "New Window". Below these controls is a table with the following data:

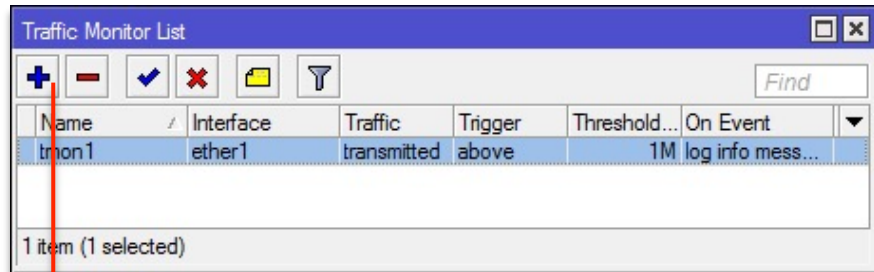
| Name | CPU | Usage |
|------------|-----|-------|
| bridging | | 0.5 |
| management | | 0.0 |
| networking | | 0.0 |
| profiling | | 0.0 |
| spi | | 1.0 |
| total | | 1.5 |
| winbox | | 0.0 |

At the bottom of the window, it says "7 items (1 selected)".

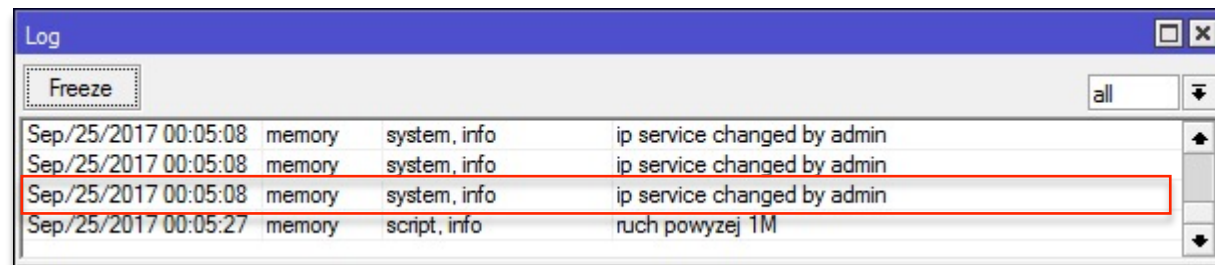
Narzędzie pozwala określić, który z elementów systemu generuje jakie obciążenie.

Narzędzia

Interface Traffic Monitor



Możemy ustawić alarm dotyczący ilości przesyłanego ruchu na danym interfejsie



Narzędzia

Torch

Torch (Running)

Basic

Interface: ether1

Entry Timeout: 00:00:03 s

Collect

- Src. Address
- Dst. Address
- MAC Protocol
- Protocol
- DSCP
- Src. Address6
- Dst. Address6
- Port
- VLAN Id

Filters

Src. Address: 0.0.0.0/0

Dst. Address: 0.0.0.0/0

Src. Address6: ::/0

Dst. Address6: ::/0

MAC Protocol: all

Protocol: any

Port: any

VLAN Id: any

DSCP: any

| Et... | Prot... | Src. | Dst. | VLAN Id | DSCP | Tx Rate | Rx Rate | Tx Pack |
|----------|-----------|---------------------------|---------------------|---------|------|----------|---------|---------|
| 800 (ip) | 6 (tcp) | 130.211.103.172:80 (http) | 192.168.1.200:16079 | | | 0 bps | 0 bps | 0 |
| 800 (ip) | 6 (tcp) | 130.211.103.172:80 (http) | 192.168.1.200:16080 | | | 0 bps | 0 bps | 0 |
| 800 (ip) | 6 (tcp) | 31.13.81.34:443 (https) | 192.168.1.200:35024 | | | 0 bps | 0 bps | 0 |
| 800 (ip) | 6 (tcp) | 31.13.81.5:443 (https) | 192.168.1.200:52077 | | | 0 bps | 0 bps | 0 |
| 800 (ip) | 6 (tcp) | 54.75.226.24:80 (http) | 192.168.1.200:16099 | | | 0 bps | 0 bps | 0 |
| 800 (ip) | 6 (tcp) | 54.75.226.24:80 (http) | 192.168.1.200:16098 | | | 0 bps | 0 bps | 0 |
| 800 (ip) | 6 (tcp) | 54.75.226.24:80 (http) | 192.168.1.200:16100 | | | 0 bps | 0 bps | 0 |
| 800 (ip) | 6 (tcp) | 45.32.154.212:443 (https) | 192.168.1.200:48938 | | | 1464 bps | 528 bps | 1 |
| 800 (ip) | 6 (tcp) | 204.2.197.204:80 (http) | 192.168.1.200:16177 | | | 0 bps | 0 bps | 0 |
| 800 (ip) | 6 (tcp) | 204.2.197.204:80 (http) | 192.168.1.200:16178 | | | 0 bps | 0 bps | 0 |
| 800 (ip) | 1 (ic...) | 8.8.8.8 | 192.168.1.200 | | | 0 bps | 0 bps | 0 |
| 800 (ip) | 6 (tcp) | 54.84.18.204:80 (http) | 192.168.1.200:16148 | | | 0 bps | 0 bps | 0 |
| 800 (ip) | 6 (tcp) | 54.84.18.204:80 (http) | 192.168.1.200:16146 | | | 0 bps | 0 bps | 0 |
| 800 (ip) | 6 (tcp) | 54.84.18.204:80 (http) | 192.168.1.200:16147 | | | 440 bps | 480 bps | 1 |

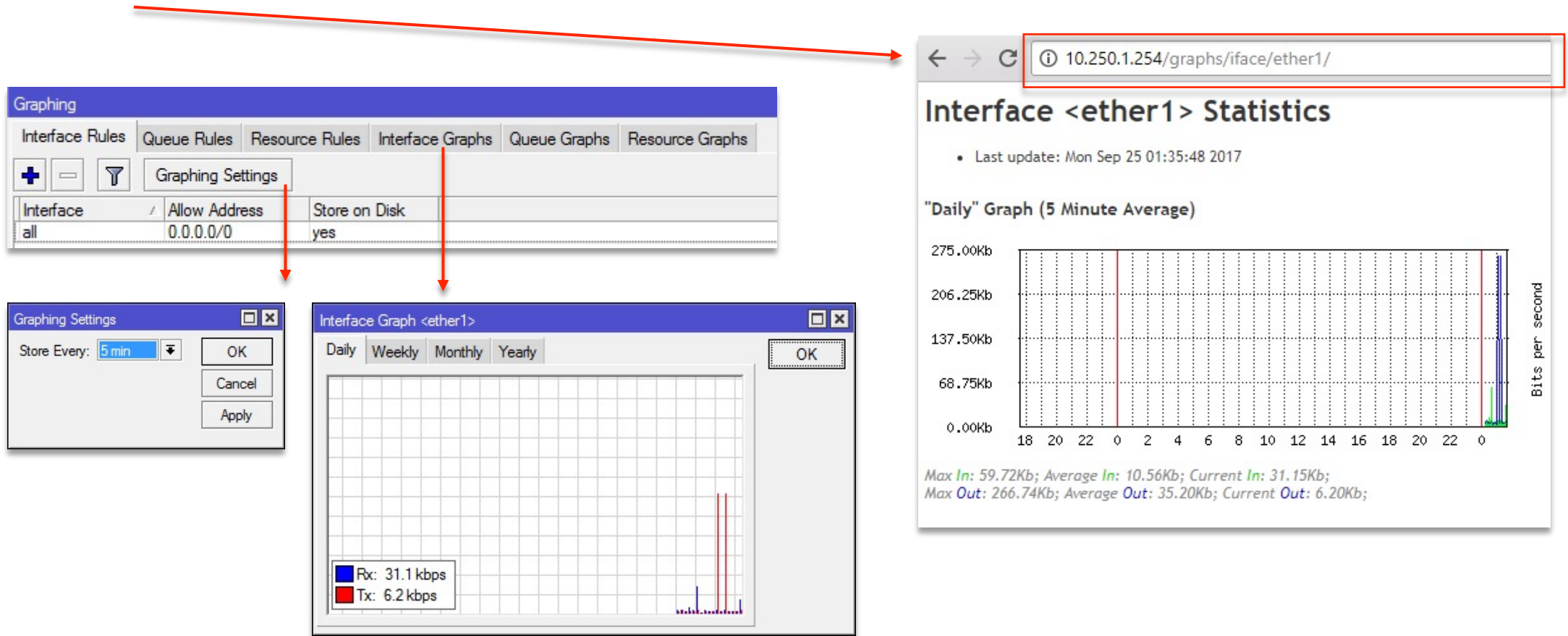
8 items | Total Tx: 624 bps | Total Rx: 0 bps | Total Tx Packet: 1 | Total Rx Packet: 0

Narzędzie pozwala na sprawdzenie jaki ruch jest przesyłany w czasie rzeczywistym

Narzędzia

Graphing

Narzędzie pozwala na zapisywanie statyk z obciążenia urządzenia, interfejsów, kolejek do **pamięci nieulotnej** urządzenia i późniejszą analizę. Mechanizm zapisuje **dane uśrednione** za dany okres. Statystyki możemy przeglądać przez stronę www.



Narzędzia

SNMP

```
MMM      MMM      KKK      TTTTTTTTTT      KKK
MMMM     MMMM     KKK      TTTTTTTTTT      KKK
MMM MMMM MMM III KKK KKK RRRRRR 000000 TTT III KKK KKK
MMM MM  MMM III KKKKK  RRR RRR 000 000 TTT III KKKKK
MMM     MMM III KKK KKK RRRRRR 000 000 TTT III KKK KKK
MMM     MMM III KKK KKK RRR RRR 000000 TTT III KKK KKK

MikroTik RouterOS 6.40.1 (c) 1999-2017      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]       Completes the command/word. If the input is ambiguous,
            a second [Tab] gives possible options

/           Move up to base level
..         Move up one level
/command    Use command at the base level
[admin@wap-ac-finlandzka] > interface print oid
Flags: D - dynamic, X - disabled, R - running, S - slave
0 RS name=.1.3.6.1.2.1.2.2.1.2.3 actual-mtu=.1.3.6.1.2.1.2.2.1.4.3
   mac-address=.1.3.6.1.2.1.2.2.1.6.3 admin-status=.1.3.6.1.2.1.2.2.1.7.3
   oper-status=.1.3.6.1.2.1.2.2.1.8.3 bytes-in=.1.3.6.1.2.1.31.1.1.1.6.3
   packets-in=.1.3.6.1.2.1.31.1.1.1.7.3
   discards-in=.1.3.6.1.2.1.2.2.1.13.3 errors-in=.1.3.6.1.2.1.2.2.1.14.3
   bytes-out=.1.3.6.1.2.1.31.1.1.1.10.3
   packets-out=.1.3.6.1.2.1.31.1.1.1.11.3
   discards-out=.1.3.6.1.2.1.2.2.1.19.3
   errors-out=.1.3.6.1.2.1.2.2.1.20.3

1 XS name=.1.3.6.1.2.1.2.2.1.2.1 actual-mtu=.1.3.6.1.2.1.2.2.1.4.1
   mac-address=.1.3.6.1.2.1.2.2.1.6.1 admin-status=.1.3.6.1.2.1.2.2.1.7.1
   oper-status=.1.3.6.1.2.1.2.2.1.8.1 bytes-in=.1.3.6.1.2.1.31.1.1.1.6.1
   packets-in=.1.3.6.1.2.1.31.1.1.1.7.1
   discards-in=.1.3.6.1.2.1.2.2.1.13.1 errors-in=.1.3.6.1.2.1.2.2.1.14.1
   bytes-out=.1.3.6.1.2.1.31.1.1.1.10.1
   packets-out=.1.3.6.1.2.1.31.1.1.1.11.1
   discards-out=.1.3.6.1.2.1.2.2.1.19.1
   errors-out=.1.3.6.1.2.1.2.2.1.20.1

2 RS name=.1.3.6.1.2.1.2.2.1.2.2 actual-mtu=.1.3.6.1.2.1.2.2.1.4.2
   mac-address=.1.3.6.1.2.1.2.2.1.6.2 admin-status=.1.3.6.1.2.1.2.2.1.7.2
|- [Q quit|D dump|down]
```

Simple Network Management Protocol (SNMP) Simple Network Management Protocol (SNMP) służy do zebrania statystyk z interface'ów, obciążenia systemu, a także innych parametrów. Z protokołu SNMP korzystają systemy monitorujące (Nagios, Zabbix, CACTI, MRTG, The DUDE, ...), które cyklicznie odpytują monitorowane urządzenia. W każdym zapytaniu wskazane są OID'y, których stan ma zostać przesłany w odpowiedzi. System monitoringu używa portu **161/UDP** do wysyłania zapytań. System monitorowany, np. router, też może sam zainicjować komunikację do systemu monitorującego, w sytuacji, gdy ma coś pilnego do przekazania, tzw mechanizm TRAP. Trap do komunikacji korzysta z portu **162/UDP**. W RouterOS dostępne są wersje protokołu: v1, v2c, v3. Protokół poza zapytaniami o OID może też wysyłać komendy do routera (w ograniczonym zakresie).

wyświetla listę OID

Przykładowe zapytanie (o MAC adres interfejsu) snmp

```
root@DESKTOP-Q6NU7KT# snmpget -v2c -c public 10.250.1.1 .1.3.6.1.2.1.2.2.1.6.3
```

Zwraca:

```
iso.3.6.1.2.1.2.2.1.6.3 = Hex-STRING: 6C 3B 6B C9 EF 43
```

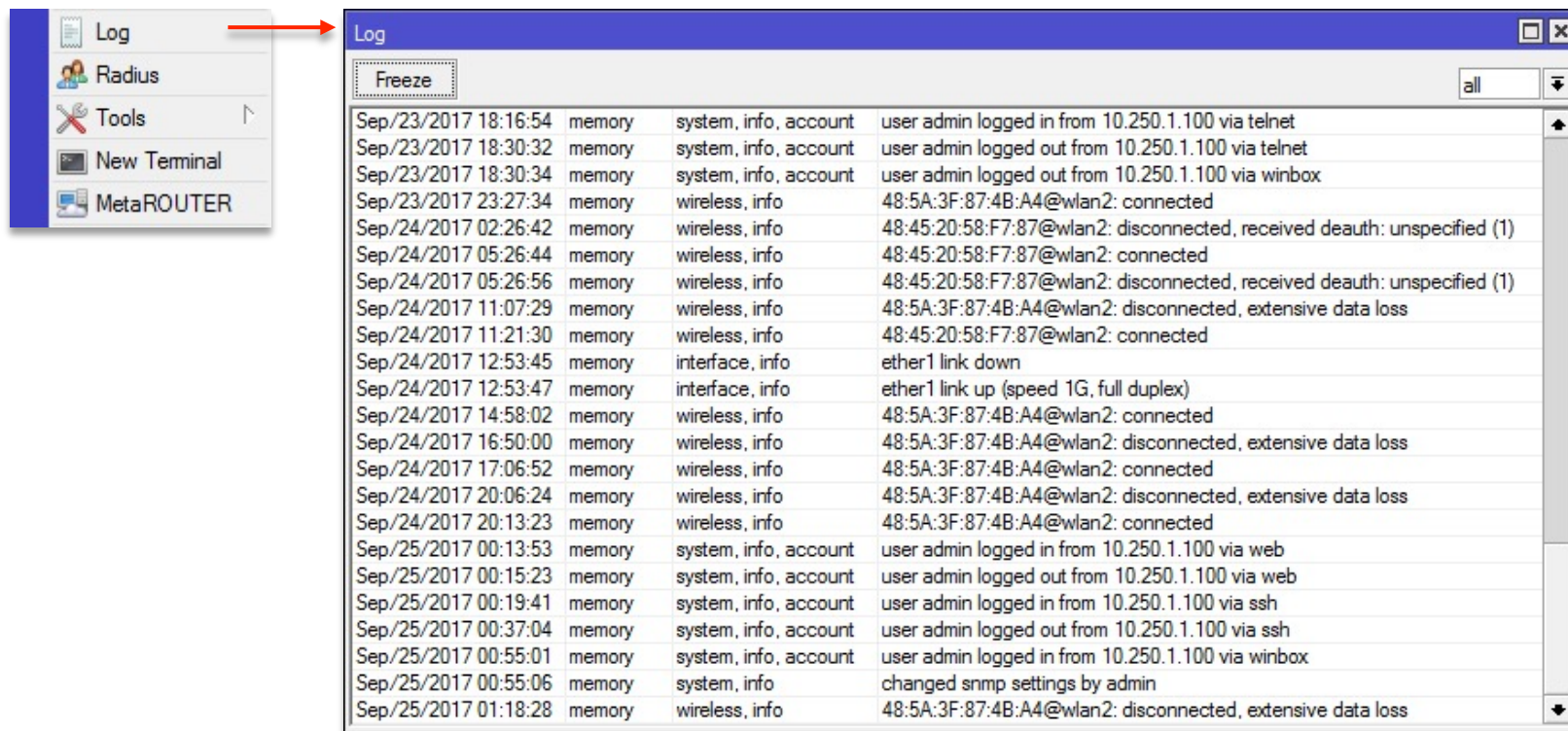
Management Information Base (MIB) dla systemu RouterOS, można pobrać ze strony:

<http://download2.mikrotik.com/Mikrotik.mib>

Narzędzia

Logowanie

Domyślnie RouterOS loguje zdarzenia w pamięci RAM. Po restarcie urządzenia logi są tracone. Istnieje możliwość zapisywania logów na nieulotną pamięć NAND naszego urządzenia, jednakże nie jest to wskazane. Rodzaj użytych pamięci nie jest przystosowany do dużej liczby zapisów. Jednym z rozwiązań jest dołączenie do naszego urządzenia pamięci na USB i odkładanie na niej logów. Zdecydowanie lepszym sposobem jest wysyłanie logów do zdalnego serwera **syslog**.



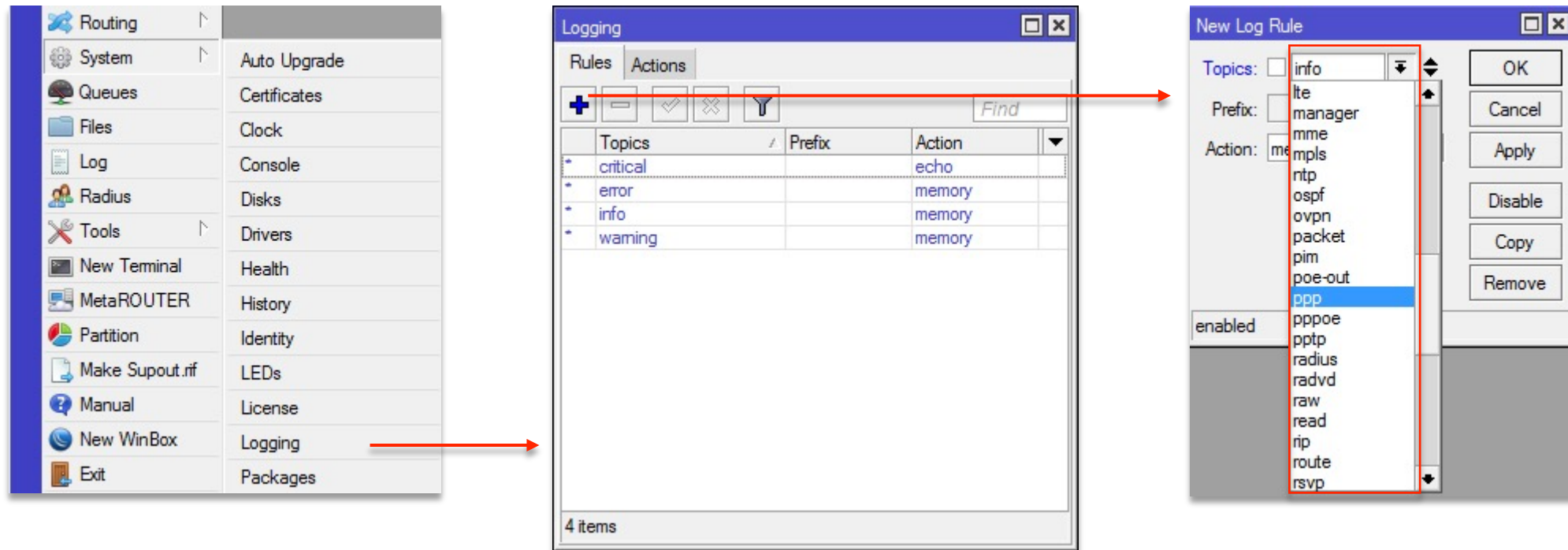
The image shows a RouterOS interface. On the left is a vertical menu with icons and labels: Log, Radius, Tools, New Terminal, and MetaROUTER. A red arrow points from the 'Log' menu item to a window titled 'Log'. The window has a 'Freeze' button and a dropdown menu set to 'all'. The main area of the window displays a list of log entries with columns for date/time, memory usage, system type, info, and account details.

| Date/Time | Memory | System | Info | Account | Details |
|----------------------|--------|-----------|------|---------|---|
| Sep/23/2017 18:16:54 | memory | system | info | account | user admin logged in from 10.250.1.100 via telnet |
| Sep/23/2017 18:30:32 | memory | system | info | account | user admin logged out from 10.250.1.100 via telnet |
| Sep/23/2017 18:30:34 | memory | system | info | account | user admin logged out from 10.250.1.100 via winbox |
| Sep/23/2017 23:27:34 | memory | wireless | info | | 48-5A:3F:87:4B:A4@wlan2: connected |
| Sep/24/2017 02:26:42 | memory | wireless | info | | 48:45:20:58:F7:87@wlan2: disconnected, received deauth: unspecified (1) |
| Sep/24/2017 05:26:44 | memory | wireless | info | | 48:45:20:58:F7:87@wlan2: connected |
| Sep/24/2017 05:26:56 | memory | wireless | info | | 48:45:20:58:F7:87@wlan2: disconnected, received deauth: unspecified (1) |
| Sep/24/2017 11:07:29 | memory | wireless | info | | 48-5A:3F:87:4B:A4@wlan2: disconnected, extensive data loss |
| Sep/24/2017 11:21:30 | memory | wireless | info | | 48:45:20:58:F7:87@wlan2: connected |
| Sep/24/2017 12:53:45 | memory | interface | info | | ether1 link down |
| Sep/24/2017 12:53:47 | memory | interface | info | | ether1 link up (speed 1G, full duplex) |
| Sep/24/2017 14:58:02 | memory | wireless | info | | 48-5A:3F:87:4B:A4@wlan2: connected |
| Sep/24/2017 16:50:00 | memory | wireless | info | | 48-5A:3F:87:4B:A4@wlan2: disconnected, extensive data loss |
| Sep/24/2017 17:06:52 | memory | wireless | info | | 48-5A:3F:87:4B:A4@wlan2: connected |
| Sep/24/2017 20:06:24 | memory | wireless | info | | 48-5A:3F:87:4B:A4@wlan2: disconnected, extensive data loss |
| Sep/24/2017 20:13:23 | memory | wireless | info | | 48-5A:3F:87:4B:A4@wlan2: connected |
| Sep/25/2017 00:13:53 | memory | system | info | account | user admin logged in from 10.250.1.100 via web |
| Sep/25/2017 00:15:23 | memory | system | info | account | user admin logged out from 10.250.1.100 via web |
| Sep/25/2017 00:19:41 | memory | system | info | account | user admin logged in from 10.250.1.100 via ssh |
| Sep/25/2017 00:37:04 | memory | system | info | account | user admin logged out from 10.250.1.100 via ssh |
| Sep/25/2017 00:55:01 | memory | system | info | account | user admin logged in from 10.250.1.100 via winbox |
| Sep/25/2017 00:55:06 | memory | system | info | | changed snmp settings by admin |
| Sep/25/2017 01:18:28 | memory | wireless | info | | 48-5A:3F:87:4B:A4@wlan2: disconnected, extensive data loss |

Narzędzia

Logowanie

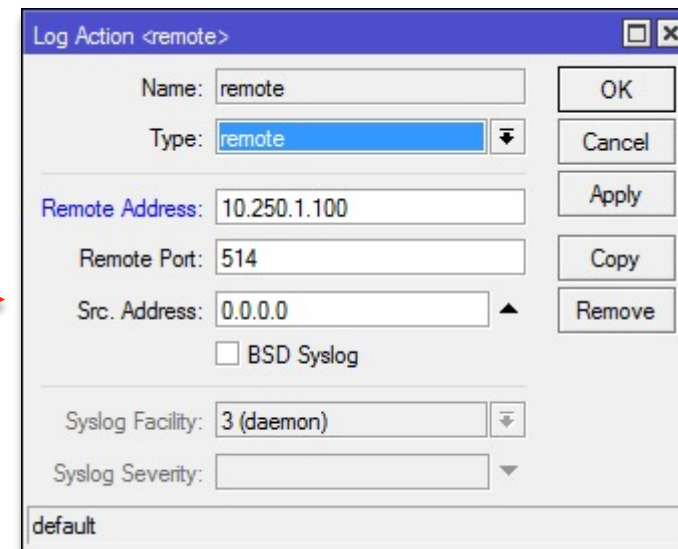
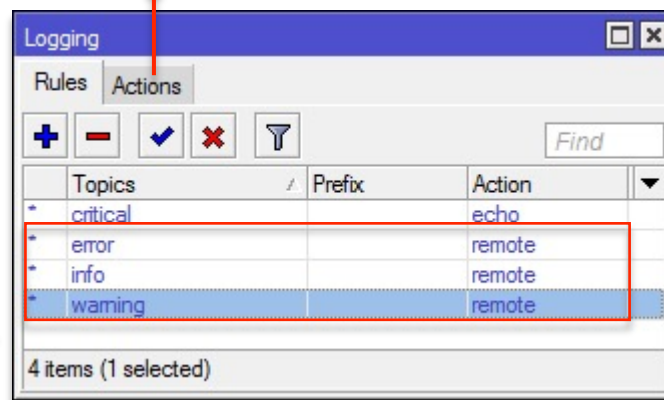
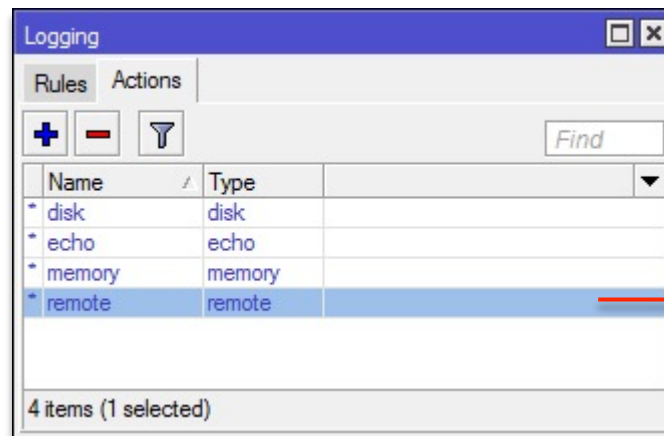
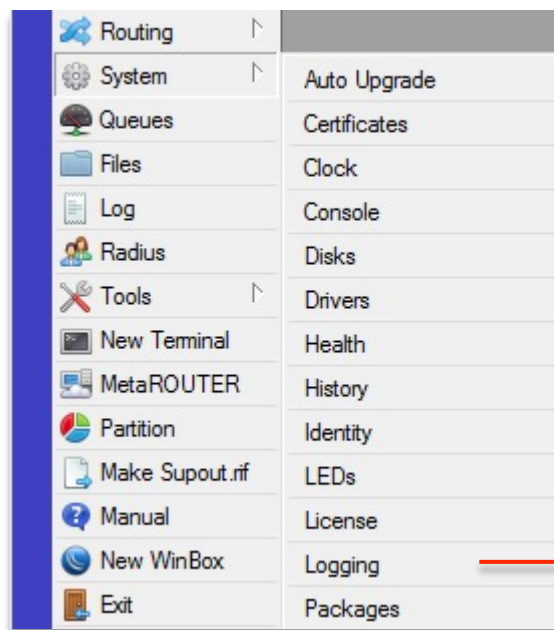
W przypadku gdy potrzebujemy rozszerzone informacje, tzw debug, możemy ustawić bardziej szczegółowe logowanie.



Narzędzia

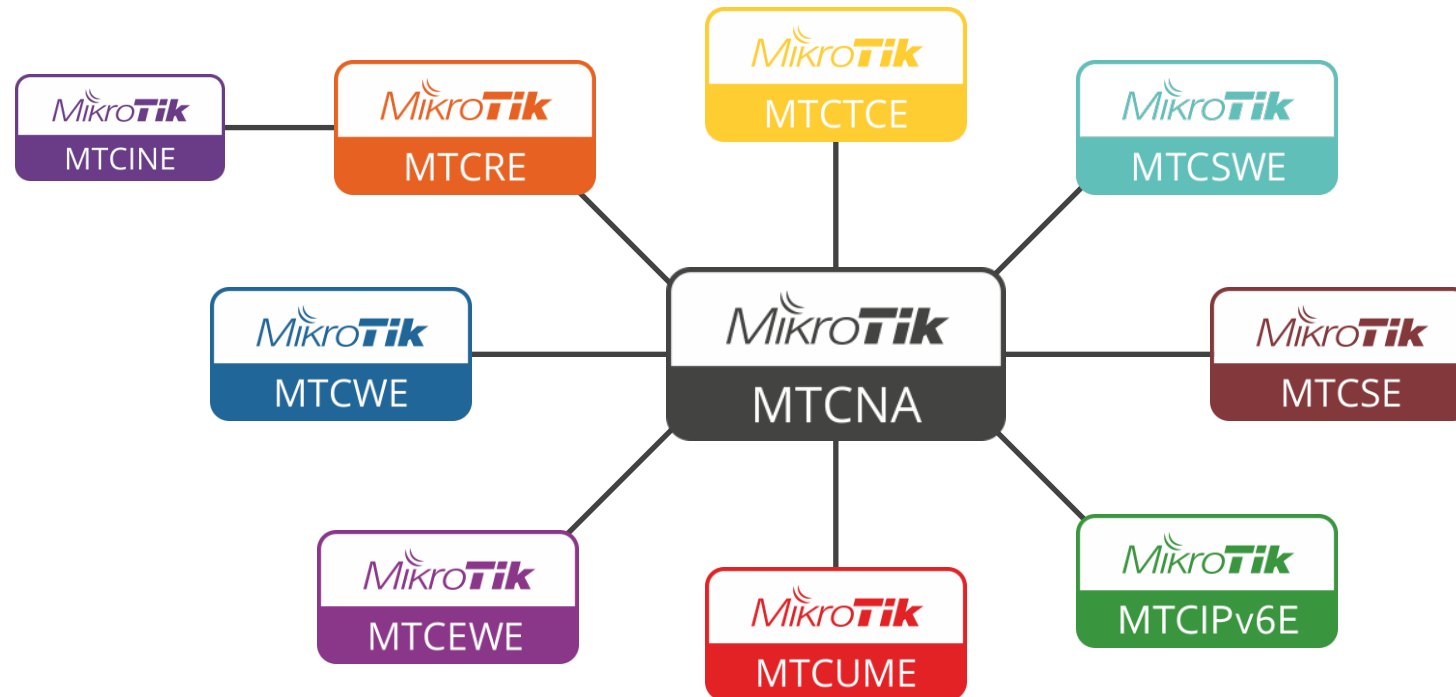
Logowanie

Ustawienie logowania do zewnętrznego serwera *syslog*



Dziękujemy za uwagę!

Certyfikowane szkolenia MikroTik



Autorskie warsztaty

Więcej informacji, harmonogram i zapisy na stronie <https://mwtc.pl>