Mikrotik hAP Lite RB941-2ND-TC

Specyfikacja

- Procesor: QCA9531 650MHz (1 rdzeń);
- Pamięć: 32MB DDR;
- Pamięć wbudowana: 16MB (typu Flash);
- Porty: 4x Fast Ethernet (100 Mbit/s);
- Licencja: RouterOS Level 4 (AP support);
- Funkcje: Access Point (w standardzie 802.11b/g/n, 2x2 MIMO 2.4GHz, szybkość 300Mb/s), WPS, Auto MDI/X;
- Tryby pracy: AP/CPE/P2P/Repeater;
- Pobór mocy: maksymalnie 3W;

Domyślne ustawienia

- domyślne IP: 192.168.88.1;
- domyślna maska: 255.255.255.0;
- serwer DHCP: domyślnie włączony na wewnętrznym LAN;
- domyślny SSID: *MikroTik*;
- domyślny użytkownik: admin;
- domyślne hasło: brak;
- WAN: port1 (włączony klient DHCP, wyłączony domyślnie dostęp do routera);
- LAN: port 2-4;

Licencja systemu RouterOS

System oparty na Linux, przypisany do routera (~OEM). Istnieje 6 poziomów licencji.

Level number	0 (Free)	1 (Demo)	3 (CPE)	4 (WISP)	5 (WISP AP)	6 (Controller)
Upgradable	-	-	RouterOS v4.x (1 rok)	RouterOS v4.x (1 rok)	RouterOS v5.x (3 lata)	RouterOS v5.x (3 lata)
Initial Config support	-	-	-	15 days	30 days	30 days
Wireless AP	24h	-	-	yes	yes	yes
Wireless client, bridge	24h	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	24h	-	yes	yes	yes	yes
EoIP tunnels	24h	1	1	bez limitu	bez limitu	bez limitu
PPPoE tunnels	24h	1	1	200	500	bez limitu
PPTP tunnels	24h	1	1	200	bez limitu	bez limitu
L2TP tunnels	24h	1	1	200	bez limitu	bez limitu
OVPN tunnels	24h	1	1	200	bez limitu	bez limitu
VLAN interfaces	24h	1	1	bez limitu	bez limitu	bez limitu
P2P firewall rules	24h	1	1	bez limitu	bez limitu	bez limitu
NAT rules	24h	1	bez limitu	bez limitu	bez limitu	bez limitu
HotSpot active users	24h	1	1	200	500	bez limitu
RADIUS client	24h	-	yes	yes	yes	yes
Queues	24h	1	bez limitu	bez limitu	bez limitu	bez limitu
Web Proxy	24h	-	yes	yes	yes	yes
User Manager active sessions	24h	1	10	20	50	bez limitu

Uwaga: W wersji 0 (free) prędkość połączenia ograniczona jest do 10Mb/s. Wyłączenie systemu zatrzymuje zegar (czas aktywności systemu). Do wygenerowania nowej licencji potrzebny jest „software-id”:

[admin@MikrTik] > **system license print**

Klikamy następnie w „*Renew License*”, wprowadzamy dane naszego konta *Mikrotik*, *level P Unlimited (Trial)*. Przedłuża to ważność o dwa miesiące, co możemy sprawdzić na naszym koncie Mikrotik w dziale „*All CHR keys*”.

Oprogramowanie umożliwia teoretycznie zamianę zwykłego komputera w router (przeszkodą jest jedynie licencja). Układy, z których robione są Mikrotik’i zwane są RouterBOARD.

Inne oprogramowanie:

- **The Dude Network Manager** - monitorowanie sieci;
- **Netinstall** - upgrade systemu za pomocą połączenia sieciowego (np. w przypadku awarii); połączenie możemy zrealizować np. za pomocą szeregowego kabla null-modem i oprogramowania *HyperTerminal* lub *PuTTy*: wejście w tryb *Setup* / **o** (*boot device*) / **e** (*boot over Ethernet*). Na serwerze Netinstall wprowadzamy właśnie „software-id”, „keep old configuration” i wskazujemy plik z aktualizacją systemu. Po zakończonej aktualizacji ponownie włączamy domyślną opcję „*boot from NAND, if fail then Ethernet*”.

Logowanie do routera

Przez przeglądarkę

Do urządzenia można zalogować się na adres http://192.168.88.1 zarówno przez porty LAN 2-4, jak i przez Wi-Fi (nie przez protokół *https*!). Na obu typach interfejsów jest włączony serwer DHCP.

Przez Winbox

Jeśli router był resetowany do trybu „*bez domyślnej konfiguracji*” (*System / Reset Configuration*), nie będzie posiadał domyślnego IP (będzie wykrywany z IP: 0.0.0.0). W tej sytuacji jedynym sposobem, aby dostać się do jego konfiguracji, będzie program *WinBox* / *Neighbors*. Aplikacja oferuje wykrycie za pomocą protokołu MNDP (*MikroTik Neighbor Discovery Protocol*) podłączonego do naszego portu routera (zakładka „*Neighbors*”) i połączenie się z nim za pomocą jego adresu MAC (przydatne, gdy nie znamy IP routera lub wynosi ono 0.0.0.0). Należy pamiętać, że port 1 ma wyłączone przez firewall skanowanie adresów MAC.

Aby zobaczyć dalszych sąsiadów (spoza naszej sieci), a nawet nimi zarządzać, łączymy się sami ze sobą: *Connect to RoMON*. Zarządzanie:

Tools / RoMON (*RoMON* identyfikuje sąsiada przez MAC portu 1 nawet jeśli jesteśmy połączeni przez port 4).

Przez port konsolowy

Logowanie przez port konsolowy: router musi mieć taki fizyczny port, używamy kabla RS-232 (może być z przełączką na USB).

Przez telnet

Logowanie przez klienta telnet (trzeba go włączyć w *Panelu Sterowania*) przy podłączeniu z routerem za pomocą RJ-45.

C:\> **telnet 192.168.88.1**

Wyjście z telnetu, gdy jesteśmy w jakimś dziale: **/**

Wyjście w ogóle: **quit**

Przez SSH

C:\> **ssh 192.168.88.1**

Przez FTP

C:\> **ftp 192.168.88.1**

Uwaga 1: Należy zdefiniować przez jakie serwisy można logować się:
IP / Services (protokoły i adresy)

Uwaga 2: Należy rozważyć wyłączenie „*MAC Server*” (czyli łączenie się przez MAC):
Tools / MAC Server: *none*;

Uwaga 3: W sieci domowej należy raczej wyłączyć „*Mikrotik Neighbor Discovery protocol*” (port UDP 5678):
IP / Neighbors*: none*;

Uwaga 4: Można monitorować, kto jest obecnie połączony z routerem:
System / Users / Active Users

Predefiniowane tryby pracy

- **CPE** (*Customer Premises Equipment*) - czyli „wireless station”, nie tworzy jednak własnej sieci;
- **Home AP** - prosty Access Point z SSID;
- **PTP Bridge** (*Point to Point*) - ;
- **WISP AP** (*Wireless Internet Service Provider*) - umożliwia emisję kilku SSID, VLANs, *Isolated Network*;

Uwaga: Tryby pracy, a także poszczególne opcje, zależą od rodzaju licencji (patrz: *System / License*).

Tryb tekstowy

Powrót o poziom wyżej w linii poleceń odbywa się za pomocą „**..**”, a powrót na najwyższy poziom to „**/**” (to jest Linux!). Pomoc można uzyskać za pomocą „**?**”.

W czasie konfiguracji można włączyć tryb „safe mode”. Powoduje on, że cała wprowadzana przez sam konfiguracja zostanie zapisana dopiero przy opuszczaniu tego trybu (nie wcześniej). Opcja sensowna, gdy np. zabraknie nagle zasilania.

[admin@MikroTik]> **Ctrl+x**
[admin@MikroTik]><SAFE>

Nazwa routera

System / Identity

Adresacja IP

Wyświetlenie IP w trybie tekstowym:
[admin@MikroTik]> **ip address print**

Nadanie adresu w trybie graficznym (wpisać adres ze skróconą maską):

IP / Addresses

Interfejsy

Interface / Bonding - dwa fizyczne porty możemy połączyć w jeden logiczny; wysyłane pakiety będą równo obciążać te porty; jest to też zabezpieczeniem przez awarią jednego z nich. *Mode: Balance-rr*.

Interface / PPPoE - jest to połączenie Point-to-Point z maską sieci 32. Tworząc na routerze klienta (*Type: PPPoE Client*), należy podać login i hasło, które wcześniej utworzyliśmy na serwerze PPP (*PPP \ Secrets*); *Remote Address* to adres klienta;

Interface / PPTP Client (*Point to Point Tunnel Protocol*) - używany do łączenia dwóch LAN-ów ze sobą (*Dial Out: nazwa.servera*); w tej samej sekcji można również uruchomić serwer PPTP;

VRRP (*Virtual Router Redundancy Protocol*)

Z kilku routerów fizycznych możemy stworzyć jeden router wirtualny, aby zapewnić większą ich niezawodność. Jeden z routerów jest routerem głównym (*Master*) na podstawie nadanego priorytetu (elekcja), pozostałe są zapasowe (*Backup*). Wszystkie posiadają ten sam identyfikator wirtualny (VRID) oraz ten sam wirtualny numer IP (IP VR), który nadajemy wirtualnemu interfejsowi, a nie fizycznemu. Adres MAC wirtualnego interfejsu to: 00:00:5e:00:01:xx. Gdy router główny nie odpowiada na zapytania ARP, następuje nowa elekcja wśród routerów zapasowych.

Opcje:

- **Preemption Mode** - zapobiega ponownej elekcji po aktywacji Mastera;
- **Interval** - co jaki czas ma następować elekcja;
- **Authentication** - wybrać *„AH - IP Authentication Header”*;

Firewall i bezpieczeństwo

Connection tracking - w sporym stopniu obciąża system, można go wyłączyć, chyba że korzystamy z NAT (wtedy jest potrzebny);

Filter Chain:

Input - to, co wchodzi do routera;

Output - to, co wychodzi z routera;

Forward - to, co przechodzi przez router;

Maskarada:

IP / Firewall / NAT / + / General: srcnat, Action / Action: masquerade (bez żadnych opcji; potrzebne, aby komputery z LAN miały dostęp do Internetu).

NAT:

Src-nat - zmiana adresu portu źródłowego (jeśli chcemy występować w Internecie pod publicznym IP); *Chain: Src-nat*; *Action: Masquerade*;

Dst-nat - zmiana adresu portu docelowego i ewentualnie jego portu, np. przekierowanie ruchu zewnętrznego do wewnętrznego serwera poczty lub www: *Chain: Dst-nat (zewnętrzne IP) / Action: Dst-nat (wewnętrzne IP)*;

Firewall Mangle - *IP / Firewall / Mangle*; służy do oznaczania połączeń i pakietów według zadanych kryteriów (ale tylko w obrębie samego routera, nie są przesyłane na zewnątrz); *Chain: Prerouting* (wybór protokołu lub portu docelowego); *Action: mark_routing* (priorytet);

Filtracja MAC - aby połączyć się mogły tylko wybrane MAC-i, należy wyłączyć opcję „*Default Authentication*”.

Przekierowanie portów

Przekierowanie adresów:

IP / Firewall / NAT / + / Chain: dstnat, Dst. Address (zewnętrzny adres routera na WAN)

Action: Action: dst-nat

To Addresses: *IP serwera WWW* (na LAN, w sieci wewnętrznej, bez portu)

Wtedy, z drugiego komputera, wpisujemy IP routera, który przekierowuje do wewnętrznego serwera www.

Przekierowanie portu:

General: Protocol: 6(TCP)

Dst. Port: 80

Action: To Ports: 80

Uwaga: Jeśli port będzie inny (np. 8081) należy wyłączyć / skonfigurować zaporę.

Port Mapping

Można za jego pomocą przekierować porty (jak w NAT). Jeśli funkcja „*Port Mapping*” nie jest obecna, należy zrobić update systemu.

Wi-Fi

[admin@MikroTik]> **interface wireless print** (jakie są interfejsy Wi-Fi)

Utworzenie Wi-Fi w trybie graficznym:

- *Interface / Wireless / Mode: ap bridge*
- *Security Profile: default* (hasło)
- *Wireless / Wireless Tables / Security Profiles: dynamic keys* (hasło)
- *IP / DHCP Server / DHCP Setup*

WEP - szyfrowanie (104-bitowe), które może zostać złamane w czasie krótszym niż minuta;

WPA/WPA2 Personal (PSK) - wszystkie stacje wykorzystują jedną hasło;

WPA/WPA2 Enterprise (EAP) - każdy użytkownik ma osobne hasło przydzielane przez serwer RADIUS;

Kto jest podpięty pod Wi-Fi (graficznie):

- *Wi-Fi: Wireless / Registration*

Separacja klientów Wi-Fi (na *Access Point*, tryb graficzny):

- *Interface / Wireless / Default Forward* (odznaczamy);
- Filtracja WiFi (MAC): Registration / dodajemy MAC do Access Listy;

- Autentication: nie łączy się z Wi-Fi
- Forward: separacja klientów Wi-Fi.

Wirtualne interfejsy Wi-Fi:
Wireless / WiFi Interface / + / Virtual (osobna sieć dla uczniów i osobna dla nauczycieli).

Tablica routingu

Jeśli router nie wie, gdzie wysłać dany pakiet, kieruje go do bramy domyślnej (docelowa sieć wtedy to z reguły [*Destination: 0.0.0.0/0*] / [*Type: Unicast]*). Brama domyślna nie jest koniecznym elementem routingu.
Brama domyślna:
IP / Routes / Route List / + / General / Dst. Address: *0.0.0.0/0*, **Gateway:** *IP Bramy*

Domyślną metryką w systemie RouterOS jest 10.

Protokoły routingu:
- *Routing / RIP - Interface: all; Network: 0.0.0.0/0; Neighbours: 0.0.0.0/0; Distribute Default: Never*;
- *Routing / OSPF - Instances: Router ID: 0.0.0.0* (nie może się powtarzać wewnątrz sieci OSPF); Network / Area: backbone; Interface: all; Network Type: broadcast; w ramach protokołu OSPF, routing może odbywać się także przez tunel nieszyfrowany **IPIP**, czyli pakiet IP wewnątrz pakietu IP (tworzy wspólny dla obu sieci adres IP inny niż ich lokalne adresy; tworzymy także interface IPIP2, Type: IP Tunnel). OSPF może także wysyłać dane przez szyfrowany tunel IPSec;

Monitorowanie działania protokołu: *System / Logging: rip*;
Adresy multicastowe:
- **FF02::1** - wszystkie urządzenia na linku;
- **FF02::2** - wszystkie routery;
- **FF02::5** / **FF02::6** - komunikaty OSPFv3;
- **FF02::9** - komunikaty RIPng;
- **FF02::1:2** - DHCP Relay Servers;

Adresy Link Local:
- **FE80::/10** (FE8, FE9, FEA, FEB);

Router jako most

Router pracując w trybie mostka (*Quick Set* → **WISP AP**) staje się „przeźroczystym” punktem dostępu do nadrzędnego routera (urządzenia w takiej sieci pobierają od nadrzędnego routera numer IP [DHCP]). Przekazuje on klientom połączenie zarówno przez Wi-Fi, jak i przez swoje porty ethernet (2-3). Mostek pracuje w warstwie 2 modelu OSI, czyli opiera się na numerach MAC i ma wspólną domenę rozgłoszeniową. Innymi słowy, mostek należy wyobrażać sobie jako wirtualny switch, składający się z wybranych portów fizycznych.
Most pozwala na komunikację pomiędzy hostami należącymi do różnych sieci tak, jakby były w tej samej sieci (jest programowym switchem). Ponieważ mosty są przeźroczyste, nie jest możliwe wykrycie ich obecności.

(R)STP (*Rapid Spaning Tree Protocol*) - eliminuje ryzyko wystąpienia pętli w mostach (bez tego ramki w warstwie 2 OSI mogłyby krążyć w nieskończoność).

Ustawienia *Quick Set*:

Info: Na początku należy zresetować konfigurację (*Reset Configuration / No Default Configuration*). Po konfiguracji router pobierze dla siebie IP od nadrzędnego routera przez które będzie można się zalogować.

Mode: *Bridge*

Frequency: *auto*

Security: *WPA2*

Encryption: *AES CCM*

Address acquisition: *Automatic* (czyli DHCP)

Address source: *Any*

Gateway: *IP_Nadrzędnego_Routera*

Router_Identity: *MikroTik_Blue*

Ustawienia *WebFig* (koniecznie przez *WinBox*):

1. *Sytem / Reset Configuration / [x] No default configuration → Reset Configuration*.
2. *Brigde / Bridge / +* / (tworzymy wirtualny interfejs, który będzie zawierał fizyczne interfejsy)
   - Name: *Most*;
   - Type: *Bridge*;
   - ARP: *enabled*;
   - [x] *Fast Forward*;
   - *OK*.
3. *Bridge / Ports / + / General /*
   - Interface: *wlan1* (opcje: *Bridge: Most; Learn: auto;* [x] **Flood;* zatwierdzamy OK);
   - Interface: *ether** (dodajemy wszystkie interfejsy ethernetowe; opcje: *Bridge: Most; Learn: auto;* [x] **Flood;* [x] *Hardware Offload*[1]).
4. *Wireless / Security Profiles /* edit: *default / General /*
   - Mode: *dynamic keys*;
   - Authentication Types: *WPA2 PSK*;
   - Unicast Cipher: [x] *aes ccm*;
   - Group Cipher: [x] *aes ccm*;
   - WPA2 Pre-Shared Key: *hasło do połączenia*;
   - Management Protection: *allowed*;
   - Management Protection Key: *hasło*;
   - [x] *Disable PMKID* (zapobiega atakowi na WPA-PSK);
   - *OK*.
5. *Wireless / WiFi Interfaces /* edit: *wlan1 / Wireless / Advanced mode*:
   - Mode: *AP bridge*;
   - Security Profile: *default*;
   - SSID: nazwa sieci Wi-Fi;
   - WPS Mode: *disabled*;
   - Installation: *indoor*;
   - Country: *poland*;
   - *OK*.
6. *Wireless / WiFi Interfaces /* PPM: *wlan1 → enable*.
7. *IP / DHCP client / DHCP Client / + / New DHCP Client / DHCP*:
   - Interface: *Most* (nazwa mostka);

[1] Odciąża procesor i przerzuca część pracy na „switch chip”. Tylko jeden bridge może korzystać z tej opcji.

- [x] *Use Peer DNS*;
- [x] *Use Peer NTP*;
- Add Default Route: *yes*.

Uwaga: DHCP stosujemy, jeśli chcemy mieć przenośny most, który zamierzamy stosować w różnych obcych sieciach. Router będzie za każdym razem pobierał inne IP (możemy je ustalić poprzez ARP lub przez WinBox). Jeśli zamierzamy stosować most w naszej stałej sieci, można mu nadać stałe IP (lub zdefiniować na routerze nadrzędnym przyznawanie ciągle tego samego IP na podstawie MAC Binding).

8. *System / Users / Users / + / New User* (tworzymy nowego admina):
   - Name: *nazwaUżytkownika*;
   - Group: *full*;
   - Password: *hasło*.

Uwaga: Po stworzeniu nowego administratora, usuwamy „admina”.

Serwer DHCP

Serwer DHCP musi mieć stałe IP:
IP / DHCP Server / DHCP Setup (nie klikać w +) / **DHCP Address Space** (to adres sieci)

Używa portów UDP 67 (w stronę klienta) i UDP 68 (w stronę serwera).
Najpierw definiujemy pulę adresów (początkowy zakres adresów [adresy statyczne] rezerwujemy sobie na drukarki i serwery):
IP / Pool / + /
Next Pool: *none*.

Następnie dodajemy utworzoną pulę adresów do serwera DHCP:
IP / DHCP Server / DHCP / + /
IP / DHCP Server / Networks / + / Address: adres naszej sieci LAN.
Uwaga: Konfigurując serwer na moście, należy dodać do interfejsu *Bridge*.

Bonding MAC / IP:
DHCP Server / Leases / Make Static

Klient DHCP

IP / DHCP Client

Aby wyłączyć pobieranie IP z serwera DHCP (przez telnet):
[admin@MikroTik]> **ip dhcp-client disable 0**

Aby port WAN dostał IP z DHCP:
IP / DHCP Client: ether1

Serwer DNS

IP / DNS

Uwaga: Należy wyłączyć „*Allow Remote Requests*” (jeśli router ma IP publiczne), bo inaczej maszyny z LAN mogą korzystać z naszego DNS. Opcja powinna być jednak ustawiona, gdy router jest w sieci wewnętrznej.

Klient DNS

IP / DNS / DNS Settings:

- Dynamic Servers: 1.1.1.1, 1.0.0.1;
- [x] *Allow Remote Requests*.

Uwaga: Na komputerach dobrze jest wskazać jako serwer DNS adres routera, wtedy zapytania będą cachowane w routerze, co skraca czas odpowiedzi i zmniejsza ruch w sieci.

VPN

W trybie graficznym na routerze:

PPP / Interface / PPTP Server: Enabled;

- Secret / Name: *ppp;*
- Password: *ppp;*
- Service: *any*;
- Profile: *any*;
- Local Address: *jakiś*;
- Remote Address: *jakiś* (wymyślone lokalne adresy).

W Windows:

- *Centrum sieci / Skonfiguruj nowe połączenie / Połącz z miejscem pracy / Użyj mojego połączenia VPN / IP Mikrotika / Połączenia sieciowe: nazwaKarty / Połącz /* ikonka sieci obok zegara: *Połącz: ppp ppp*.

Przycisk MODE

Domyślnie, przycisk „*Mode*” nie inicjuje żadnego działania. Można przypisać mu dowolne działanie, np. wykonanie skryptu. Przykładowo:

/system script add name=test-script source={:log info message=("1234567890");}

/system routerboard mode-button set on-event=test-script

/system routerboard mode-button set enabled=yes

Uwaga: Jeśli mimo to, przycisk nie działa, należy uaktualnić wersję firmware’u.

Backup

W wersji graficznej:

Files / Backup

W wersji tekstowej:

Binarny zrzut konfiguracji (razem z hasłami):

[admin@MikroTik]> **system backup save name=***kopia-2023-05-15.bin*

[admin@MikroTik]> **system backup load name=***kopia-2023-05-15.bin*

Tekstowy zapis konfiguracji (bez haseł) lub części konfiguracji (gdy chcemy ją powielać na wielu urządzeniach):

[admin@MikroTik]> **export file=***ustawienia* (system doda rozszerzenie *.rsc)

[admin@MikroTik]> **interface wireless export file=***ustawienia-wifi.txt*

Reset

Reset do ustawień fabrycznych za pomocą przycisku:

1. Przy wyłączonym routerze, wcisnąć przycisk *Reset*, włączyć zasilanie, zwolnić przycisk, gdy zacznie migać dioda USR (np. po drugim mrugnięciu). Ta opcja wczytuje kopię zapasową boot loadera, a następnie resetuje ustawienia, ale zachowuje IP 192.168.88.1.
2. Przytrzymanie przycisku *Reset* dłużej, do momentu aż przestanie migać dioda USR (zacznie świecić jednolitym światłem), spowoduje wejście routera w tryb *Netinstall* (router szuka serwerów instalacji *RouterOS*).

Uwaga: W przypadku, gdy router pracuje w trybie mostka, reset przyciskiem spowoduje zresetowanie go do trybu mostka. Aby uzyskać całkowity reset do ustawień fabrycznych, należy zresetować go programowo za pomocą *Winbox* (w innych modelach, można do tego celu użyć ekranu dotykowego na obudowie routera).

Reset do ustawień fabrycznych za pomocą Winbox / przeglądarka internetowa:

Reset / *„No default Configuration”* (IP resetowane jest do 0.0.0.0)

Upgrade

Wyższa wersja systemu (*Upgrade*):

System / Packages / Check for update (aktualizacja) **/ Download & Install**

Mesh

Topologia siatki - każdy węzeł łączy się bezpośrednio i dynamicznie z jak największą ilością innych węzłów. Taka sieć pozwala na samoorganizowanie się i samokonfigurowanie.

Zakładka „*Mesh*”: adresacja może być oparta o IP lub o ARP. Testowanie to przycisk „*Mesh Traceroute*”(możemy tutaj określić limit przeskoków).

Separacja portów

Domyślnie porty 2-4 mogą się ze sobą komunikować. Możemy skonfigurować router w ten sposób, aby komunikowały się ze sobą tylko wybrane porty, a reszta była od nich odseparowana (komunikacja między nimi nie będzie działać):

***Switch** / **Port Isolation** /* wybrać port (np. *ether2*) */ **Forwarding Override** [x] / **Forward To**: ether** (wybrać porty, z którymi będzie możliwa komunikacja)

Info: Komunikacja przez port 1 jest zawsze możliwa bez względu na to, czy będzie tu ujęty czy nie. Jest on *de facto* portem zewnętrznym (WAN) służącym do komunikacji z Internetem.

Inne

Wirtualne Mikrotiki: *http://mikrotik.com/download* (wersja *.ova na *Virtualbox*). Logujemy się do niego przez przeglądarkę (trzeba ustalić IP).

Próbne egzaminy: *http://artbud.edu.pl*.

Ostatnia aktualizacja: 28 sierpnia 2022.