

# Programming the **MikroTik hAP** series for 44net VPN use



This document covers the following devices (\*may cover other RouterOS devices)

[MikroTik hAP lite RB941-2nD](#)

[Mikrotik hAP mini RB931-2nD](#)

[MikroTik hAP ac lite RB952Ui-5ac2nD-TC](#)

**Mark Phillips, NI2O 20240722 V1.70**  
**Copyright © 2024 All Rights Reserved**

## Table of Contents

<b>1 Assumptions</b>	<b>2</b>
<b>2 Power up and connect the hAP lite</b>	<b>2</b>
<b>3 Log into the hAP lite</b>	<b>3</b>
<b>4 Create a new password</b>	<b>3</b>
<b>5 Confirm the “WAN” connection</b>	<b>3</b>
5.1 Quickset	3
<b>6 Update your firmware</b>	<b>3</b>
<b>7 Configure the 44net IP settings</b>	<b>3</b>
7.1 Laptop testing	4
<b>8 VPN configuration</b>	<b>4</b>
8.1 Add additional routes	6
<b>9 Testing</b>	<b>6</b>
<b>10 Configure WiFi and other router services</b>	<b>8</b>
<b>11 Force a reboot</b>	<b>8</b>

## Version Control

Author	Notes	Date
Mark Phillips, NI2O	Initial creation	04/12/2022
Mark Phillips, NI2O	Firmware update added	12/29/2022
Mark Phillips, NI2O	Document updated	01/17/2023
Mark Phillips, NI2O	Document updated	03/17/2023
Mark Phillips, NI2O	Test PING address updated	07/22/2024

## Credits

Charles Hargrove, N2NOV  
Damon Liebert, N1LJK

# 1 Assumptions

- The device is not configured and is in a factory default state.
- RouterOS (firmware) version at least 7.2 (these instructions will NOT work with V6 firmware).
- Familiarity with RouterOS.

## 2 Power up and connect the *hAP lite*

Connect the *hAP lite* RJ45 Internet port to your LAN. Connect your laptop to any of the 3 remaining RJ45 ports (note: the *hAP lite* only supports ethernet connections up to 100mbps). Connect the supplied power supply to the power port.

## 3 Log into the *hAP lite*

From your laptop connect to the *hAP lite* by entering <http://192.168.88.1> into your browser's address bar.

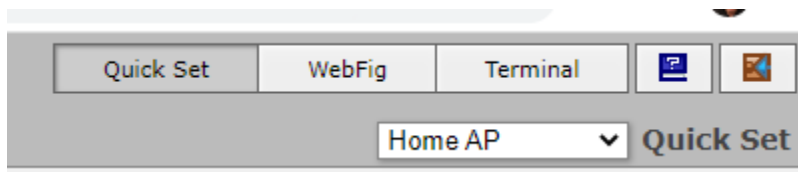
## 4 Create a new password

This will become the permanent password required to access the web gui interface of the *hAP lite*.

## 5 Confirm the “WAN” connection

### 5.1 Quickset

Ensure the page you are looking at is the “Quick Set” page. This is found in the top right corner of the Mikrotik GUI.



Look for a part of the displayed page that says “Internet”. Confirm that the *hAP lite* has indeed connected to the network attached to its “Internet” port and has acquired an IP address. If a manual address is required click the “Static” button and populate the relevant details.

Internet	
Address Acquisition	<input type="radio"/> Static <input checked="" type="radio"/> Automatic <input type="radio"/> PPPoE
IP Address	192.168.210.162 <span>Renew Release</span>
Netmask	255.255.255.0 (/24)
Gateway	192.168.210.1
MAC Address	DC:2C:6E:4A:59:A2
Firewall Router	<input checked="" type="checkbox"/>

## 6 Update your firmware

The Wireguard VPN only works on RouterOS V7.2 and upwards. To ensure that your router is running on the latest firmware, perform a firmware update by following this link

[https://wiki.mikrotik.com/wiki/Manual:Upgrading\\_RouterOS](https://wiki.mikrotik.com/wiki/Manual:Upgrading_RouterOS)

## 7 Configure the 44net IP settings

In the area of the page labeled “Local Network” configure the network information as issued by your local sysop. This is NOT the same as your VPN details.

Local Network	
IP Address	44.56.72.17
Netmask	255.255.255.240 (/28) ▼
DHCP Server	<input checked="" type="checkbox"/>
DHCP Server Range	▲ 44.56.72.18-44.56.72.30
NAT	<input type="checkbox"/>
UPnP	<input type="checkbox"/>

If you wish to use DHCP to dynamically assign addresses to your 44net devices, ensure that you enter the correct range of addresses in the “DHCP Server Range” field. A discussion on how to correctly identify usable IP addresses is without the scope of this document. If you are in any doubt please consult your allocation notice from your local sysop as in the below example.

*44net IP subnet details for NI2O’s test lab.....*

*IP range 44.56.72.16/28*

*Netmask 255.255.255.240*

*Gateway 44.56.72.17*

*Broadcast 44.56.72.31*

*Usable IP’s 13 (not including the gateway)*

Uncheck the “NAT” setting? Leaving this checked will force the *hAP lite* to perform Network Address Translation on all your outgoing Internet bound data giving the illusion that you are using a single network device rather than multiple devices. This could be desired if Internet access is also required.

Finally, click the “Apply Configuration” button at the bottom of the page.

## 7.1 Laptop testing

Perform the following steps to force your laptop to accept the new settings from the *hAP lite*;

- *Unplug the network cable from your computer*
- *Count to 20 then plug the cable back in again*
- *Open another tab in your browser and type in the ip address of the router you set above*
- *With luck you should be presented with the router's login prompt*
- *Hit the reload button until you get the prompt*
- *Log in to the router using the password you set earlier*

## 8 VPN configuration

Click the “Webfig” button at the top right corner of the displayed webpage.

From the left menu that now appears, click “Wireguard”. A new page will appear on the right. Click “Add New”. In the “Name” field enter “44net\_access”. In the “Listen Port” field enter “51844”. Click “Apply”

Notice that some more information is now populated in the displayed page.

Actual MTU	1420
Listen Port	51844
Private Key	.....
Public Key	ft7S3pyvr91GmWR5YelisWAKiNghiScXOR+SZ+BrXiM=

Delete the contents of the “Private Key” field and paste the private key from the config file supplied by your local sysop (example below).

```
[Interface]
Address = 44.56.0.221/26
ListenPort = 51844
PrivateKey = 6lPQsJNzh6OounB795/zGmAe6+O/FM535PISqr/UqUk=

[Peer]
PublicKey = nW9HaYfZeM5opuqiBdPM0CkW0Eo42+CKH6SxWvKmLWM=
PresharedKey = E1hkV6oH9+dmlyFFKCh3kFqgwZNNTWZeChV1ptTyzkA=
```

*AllowedIPs = 44.0.0.0/9, 44.128.0.0/10*  
*Endpoint = hamgatepa.ampr.org:51844*

Click “Apply”. Note that the “Public Key” field may change.

From the left menu, select “Wireguard”. From the right page select the “Peers” tab. Click “Add New”. Populate the “Public Key”, “Endpoint Port” and “Preshared Key” fields extracting the information from the file supplied by your local sysop (example above).

The “Endpoint” field will only accept an IP address. If your sysop supplied you with an endpoint IP address (the address of the AMPR server) enter that, but if you have only a hostname point your browser here to convert it to an IP address <https://dnschecker.org/all-dns-records-of-domain.php>

Now we have to enter the “Allowed Address” information. This information tells the VPN which networks it is allowed to carry. This is the same information as the “AllowedIPs” that your local sysop gave you (example above).

Enter one subnet per line. Another line can be obtained by pressing the down arrow next to the words “Allowed Address”. Set the “Persistent Keepalive” to 00:00:25 for 25 seconds (not like the picture). This optional field is required if you are behind a NAT type firewall. Finally, press the “Apply” button.

CAPsMAN

Wireless

Interfaces

WireGuard

PPP

Bridge

Switch

Mesh

IP

MPLS

IPv6

Routing

System

Queues

Files

Log

RADIUS

Tools

Make Supout.rif

Undo

Redo

Hide Passwords

Safe Mode

Design Skin

WinBox

Graphs

End-User License

RouterOS v7.2 (stable)

OK

Cancel

Apply

Remove

Enabled

☒

Interface

44net\_access

Public Key

nW9HaYfZeM5opuqiBdPM9

Endpoint

161.35.142.19

Endpoint Port

51844

Allowed Address

44.0.0.0/9

44.128.0.0/10

Preshared Key

Persistent Keepalive

00:25:00

Rx

92 B

Tx

180 B

Last Handshake

00:00:39

Comment

You should see some RX and TX counters increase indicating that you have a successful connection.

## 8.1 Add additional routes

Additional routes will be required to tell the router to use the VPN instead of the default Internet route. Select IP then Routes from the left menu. Create a route for both 44.0.0.0/9 and 44.128.0.0/10 that points to the VPN tunnel %44net\_access (you may need to type this in as it will not appear as a gateway - do not skip the %)

If you have a larger subnet allocation make sure to also add a route for that. Your additional subnet may NOT travel over the VPN so make sure to specify the relevant IP address or port name

Route List

Add New

all ▾

6 items

		▲ Dst. Address	Gateway	Distance	Pref. Source	
-	DAd	0.0.0.0/0	192.168.1.1	1		
- D	AS	44.0.0.0/9	%44net_access	1		
-	DAC	44.118.0.192/26	%44net_access			
-	DAC	44.118.57.0/28	%bridge			
- D	AS	44.128.0.0/10	%44net_access	1		
-	DAC	192.168.1.0/24	%ether1			

## 9 Testing

To test connectivity from your *hAP lite* to the greater 44net network, from the left menu select Tools > Ping. On the right page enter 44.4.50.2 in the “Ping to” field and ensure the “44net\_access” interface is selected. Click “Start”. Observe the table at the top of the page populate with statistics



RouterOS v7.2 (stable)

Start Stop Close

5 of 5 packets received 0 % packet loss Min: 85.716 ms Avg: 93.610 ms Max: 113.886 ms

Ping To 44.4.50.2

Interface 44net\_access

ARP Ping ☐

Packet Count

Timeout 1000 ms

Src. Address

Packet Size 50

TTL

DSCP

Dont Fragment ☐

	#	Seq #	Host	Time (ms)	Reply Size	TTL	Status
	0	0	44.4.50.2	113.886	50	252	
	1	1	44.4.50.2	88.188	50	252	
	2	2	44.4.50.2	91.960	50	252	
	3	3	44.4.50.2	88.303	50	252	
	4	4	44.4.50.2	85.716	50	252	

To test connectivity from your devices, issue a PING to 44.1.1.17 (portal.ampr.org). If this is successful, also do a traceroute or MTR to the same address. Your traceroute should reveal a handful of other 44net devices that your route passes along before arriving at the destination IP address. If you see public (non 44.x.x.x) addresses in the path then you may not be connected to the VPN. Check with your local sysop to confirm your connection status.

To ensure you are not tracing your test target via the public internet, issue a traceroute from your console. In the below example we make 1 hop across the 44Net via the Hamgate. If this table produced a non-44Net address as the first hop then you are not configured correctly.

```
root@AMPRVPN:~# traceroute 44.1.1.17
traceroute to 44.1.1.17 (44.1.1.17), 30 hops max, 60 byte packets
1  vpnhost.hamgatepa.ampr.org (44.56.0.192) 13.186 ms 13.131 ms 13.119 ms
2  * * *
3  169.228.34.82 (169.228.34.82) 80.406 ms 80.788 ms 81.213 ms
4  nodem-core-6807-vlan2995-gw.ucsd.edu (132.239.255.49) 80.292 ms 80.287 ms 80.269 ms
5  mx0-vlan2761-gw.ucsd.edu (132.239.254.162) 88.606 ms 80.236 ms 80.226 ms
Etc ....
```

Some users have reported that they are getting a row of stars where they expect the Mikrotik to be. If this is happening to you (usually on inbound tests) don't worry about it. Your end of the VPN is refusing to identify itself. This is considered a security measure.

```
root@hamgatepa:~# traceroute -n 44.56.132.3
traceroute to 44.56.132.3 (44.56.132.3), 30 hops max, 60 byte packets
1 * * *
2 44.56.132.2 13.786 ms 13.772 ms 13.740 ms
3 44.56.132.3 13.714 ms 13.685 ms 21.629 ms
root@hamgatepa:~#
```

## 10 Configure WiFi and other router services

Your *hAP lite* has WiFi abilities. This is an optional step and is not covered in this document. The WiFi works out of the box as you would expect it to. If you have enabled DHCP with 44net address space you'll be able to connect to the access point via WiFi. Your WiFi connected device will also be connected as a node on the 44Net.

## 11 Force a reboot

Force the *hAP lite* to reboot by selecting System > Reboot from the left menu. This will check that your router retains the configuration you have just created.