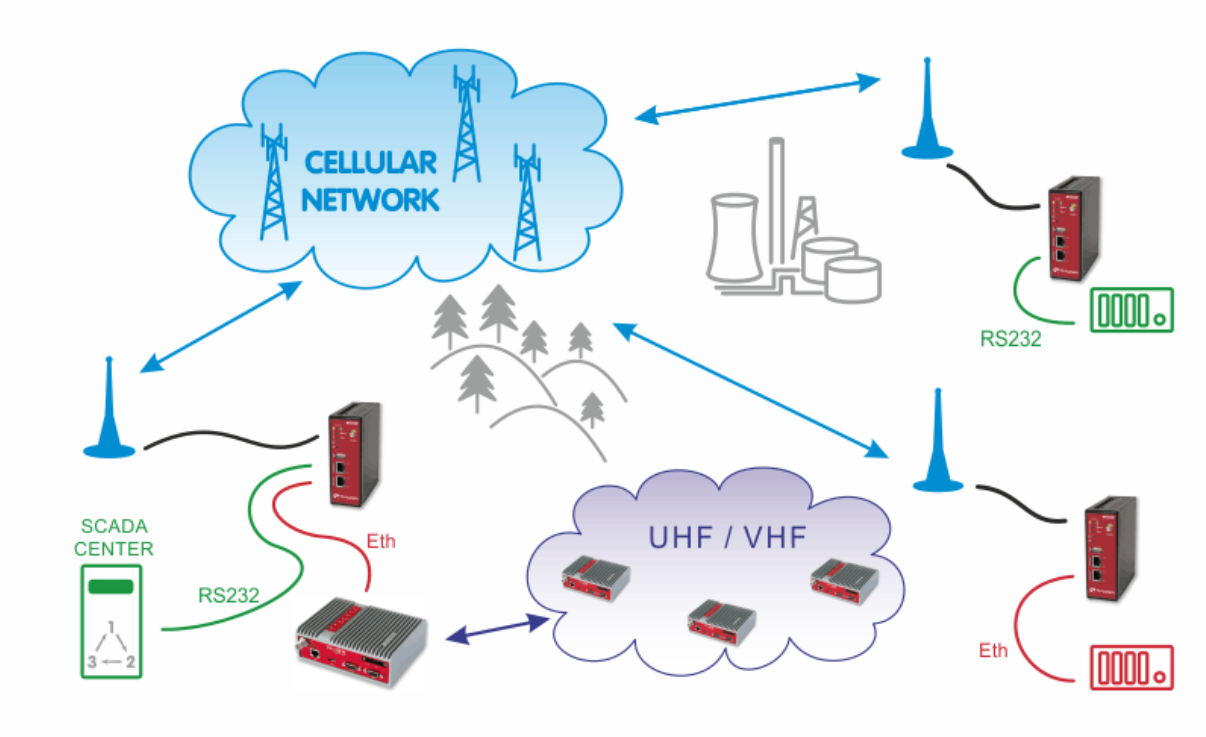
RACOM
RADIO DATA NETWORKS

Application notes



M!DGE/MG102i - WAN Backup

version 1.1
3/2/2018

RACOM s.r.o. • Mirova 1283 • 592 31 Nove Mesto na Morave • Czech Republic
Tel.: +420 565 659 511 • Fax: +420 565 659 512 • E-mail: racom@racom.eu

www.racom.eu

Table of Contents

Introduction

Under typical circumstances, VPN tunnels between central M!DGE and other routers are established over the WAN network. When the WAN fails, traffic to/from the respective remote router is automatically redirected to the cellular network.

1. Basic Backup Example

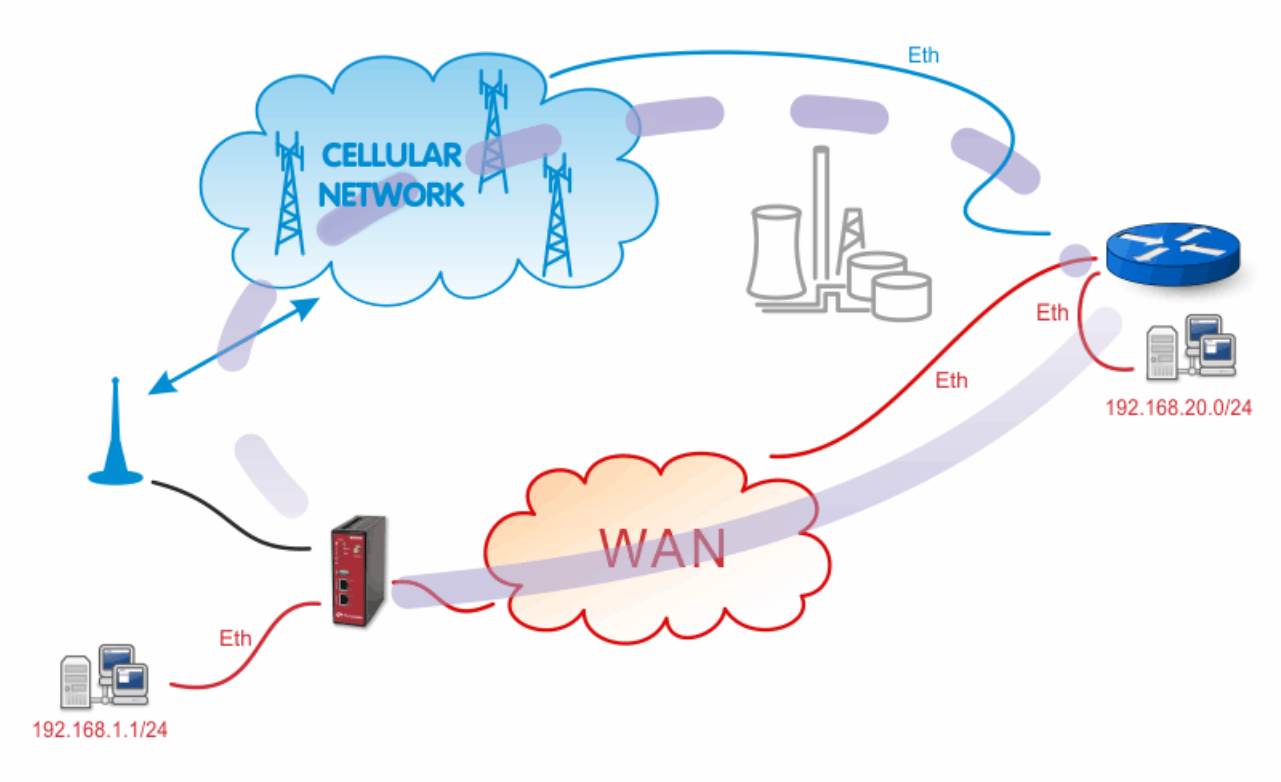


Fig. 1.1: Basic Backup Example

1.1. M!DGE Configuration

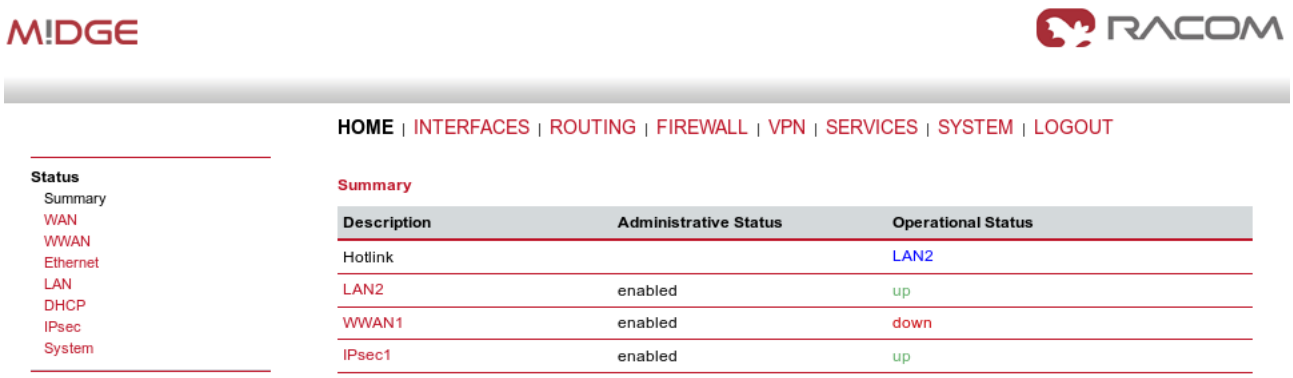


Fig. 1.2: Central M!DGE HOME menu

M!DGE is connected via the WAN network using its LAN2 interface. The WWAN1 link (cellular network) is down and the IPsec VPN connection is already established. To achieve this, several steps must be performed.

1.1.1. Ethernet Ports

In the example, the first port (LAN1) is used for the local subnet 192.168.1.0/24 and the WAN port (LAN2) is configured with an IP address 192.168.131.239/24. See the following pictures for the details.

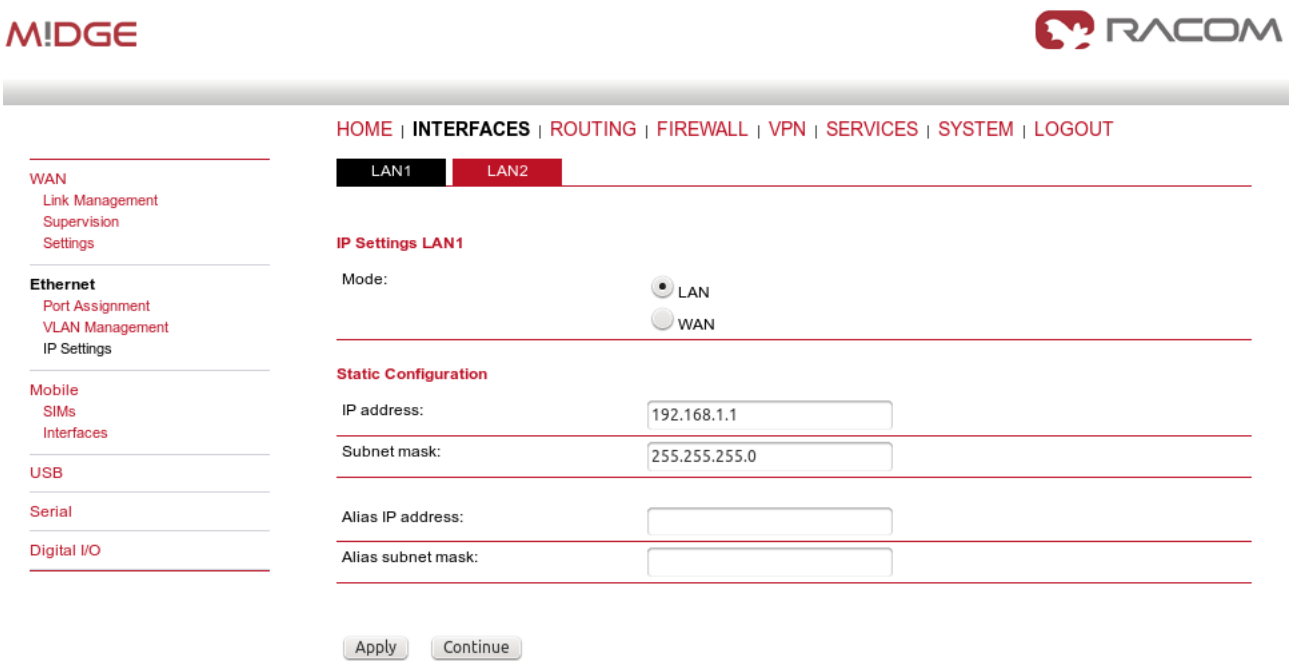


Fig. 1.3: Central M!DGE LAN1 configuration

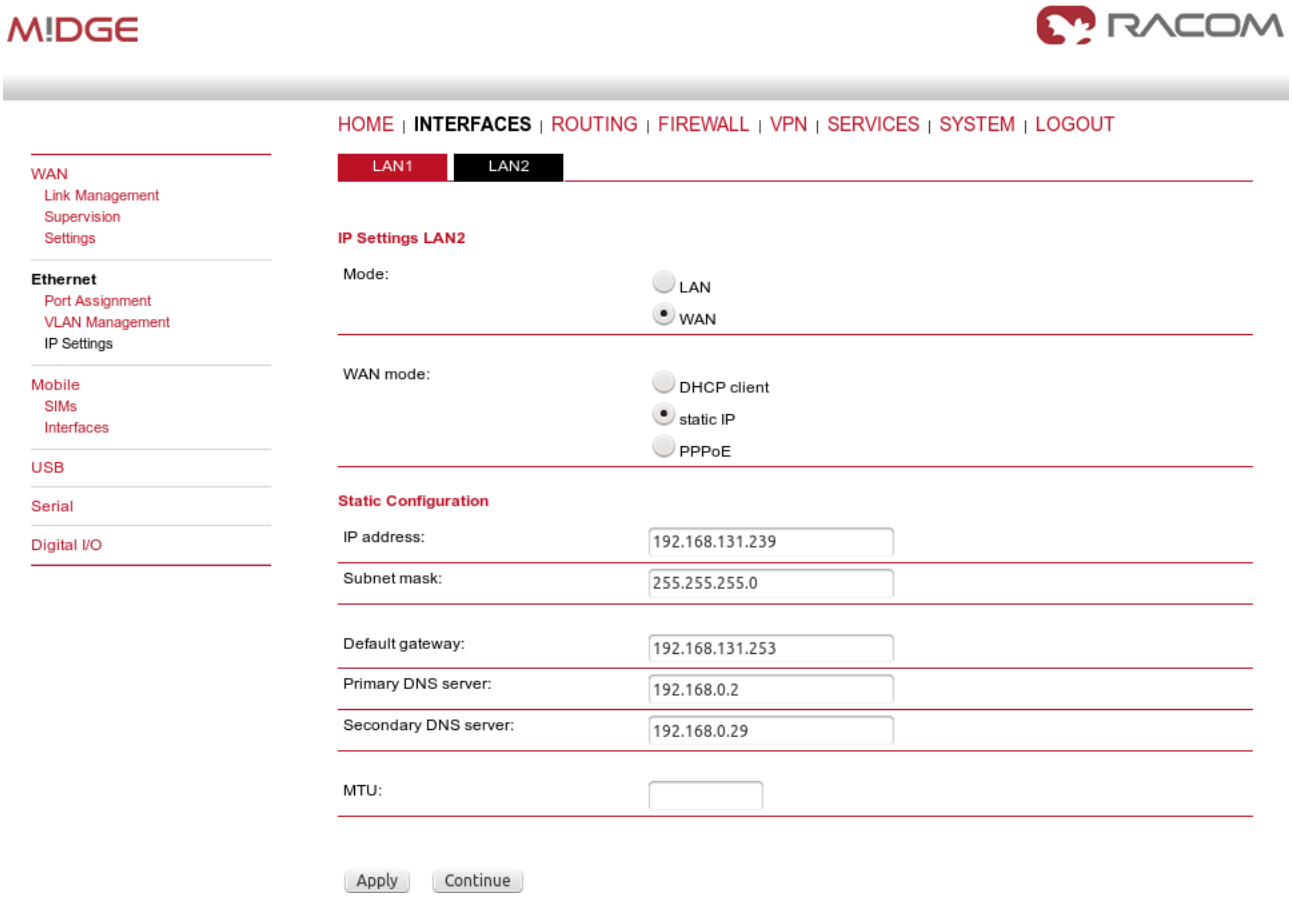


Fig. 1.4: Central M!DGE WAN configuration

1.1.2. Cellular Network

For the backup link, you need to configure your SIM card and APN accordingly. The configuration is made in the INTERFACES – Mobile menu. Configure it to meet your APN configuration.

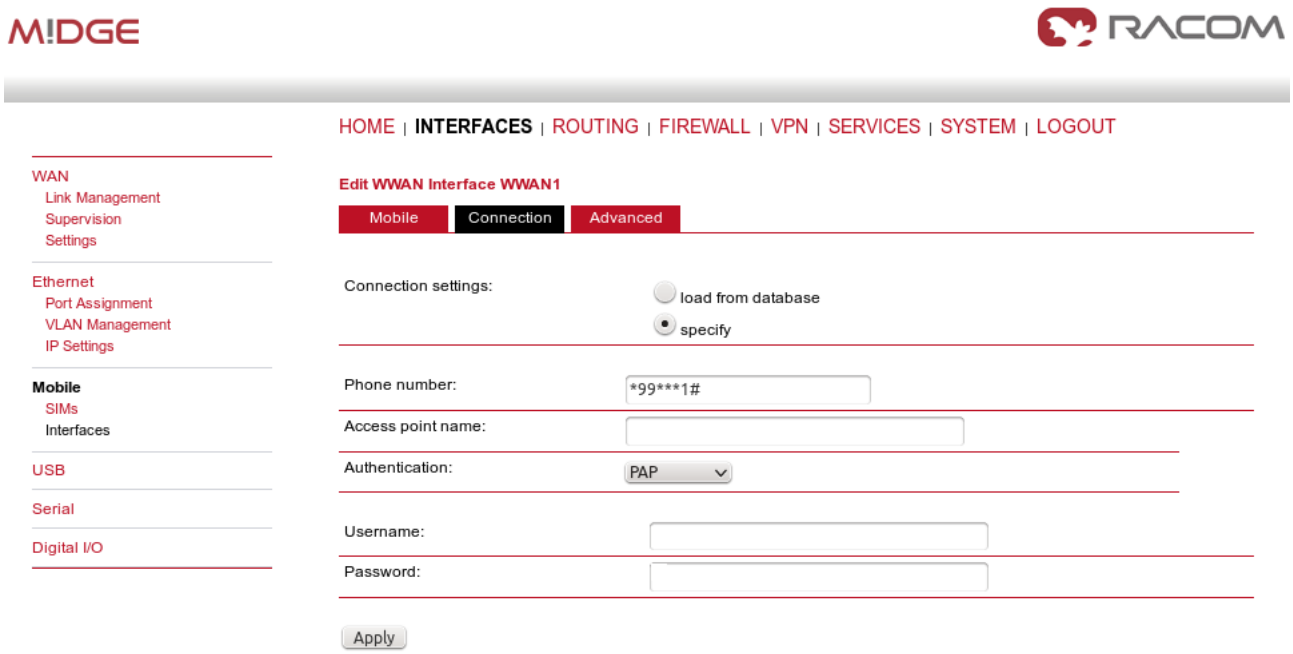


Fig. 1.5: Mobile interface configuration

Use manual for more details about the mobile interface configuration[1].

1.1.3. VPN Tunnel

Configure and enable the IPsec (or OpenVPN) tunnel to the remote peer. In the example, the local network is 192.168.1.0/24 and remote network is 192.168.20.0/24.

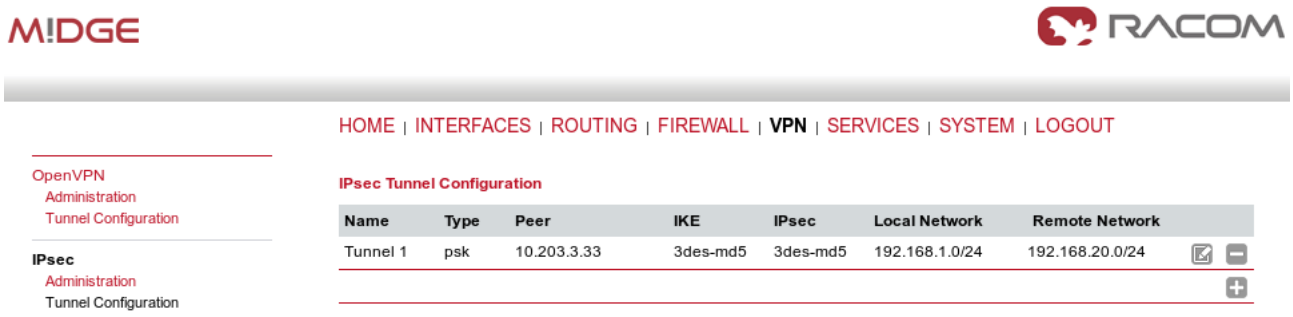


Fig. 1.6: IPsec configuration

Keep in mind that you need to configure Peer IP address to be reachable via both connections (WAN and WWAN) so it may establish IPsec connection.

[1] http://www.racom.eu/eng/products/m/midge1/web_conf.html#interfaces

See the VPN examples in *VPN Configuration*[2] application note or the *manual*[3] for more details.

1.1.4. WAN Link Management

In the Link Management menu, configure the LAN2 interface as the permanent and primary option. Set the WWAN interface as its backup. The Establishment mode can be either set to „on switchover“ (to be connected only when the permanent link is not active) or „permanent“ (to be connected all the time – it is used for the faster link switching).

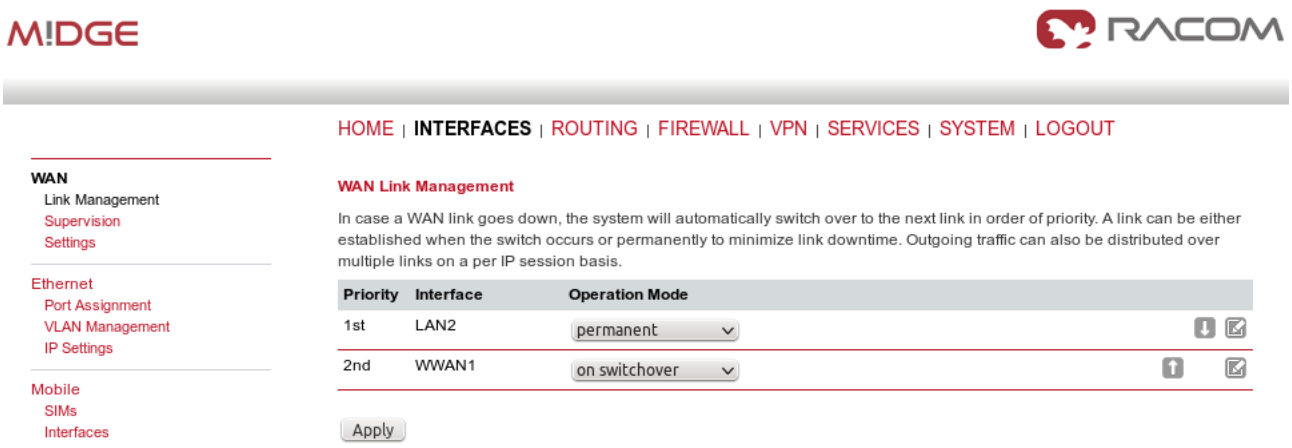


Fig. 1.7: WAN Link Management

Another step is configuring the Supervision feature.

[2] http://www.racom.eu/eng/products/m/midge/app/vpn/index.html
[3] http://www.racom.eu/eng/products/m/midge1/web_conf.html#VPN

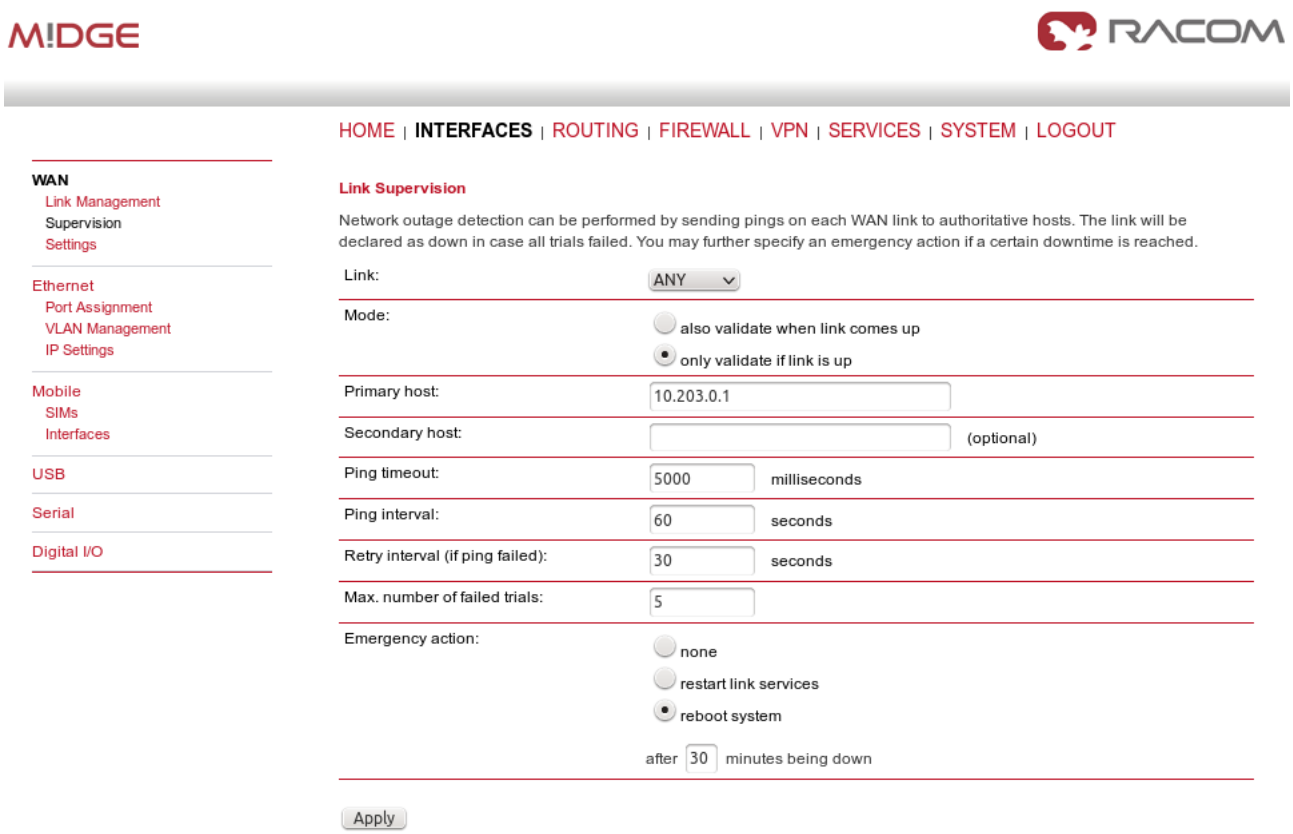


Fig. 1.8: Supervision

The Supervision enables M!DGE to control the link switching procedure. In our example, M!DGE checks the connection by executing the ping packets to the host on the IP address 10.203.0.1. If five consecutive ping packets are unsuccessful, the link is considered down and is switched. If there is no connectivity for 30 minutes, the unit is rebooted as a result of the Emergency action.

Both links are checked when they are up (Link – ANY), otherwise you could choose just one link to be checked or create two different Supervision for each link (e.g. lower timeouts and more frequent checks on the WAN link).

1.2. Practical Test

Now you should be connected via the primary WAN link (LAN2). The easiest way to test the switching is to unplug the ETH cable from the LAN2 interface. M!DGE almost immediately recognizes the unplugged cable and it switches to the cellular network. The VPN tunnel should also be reestablished.

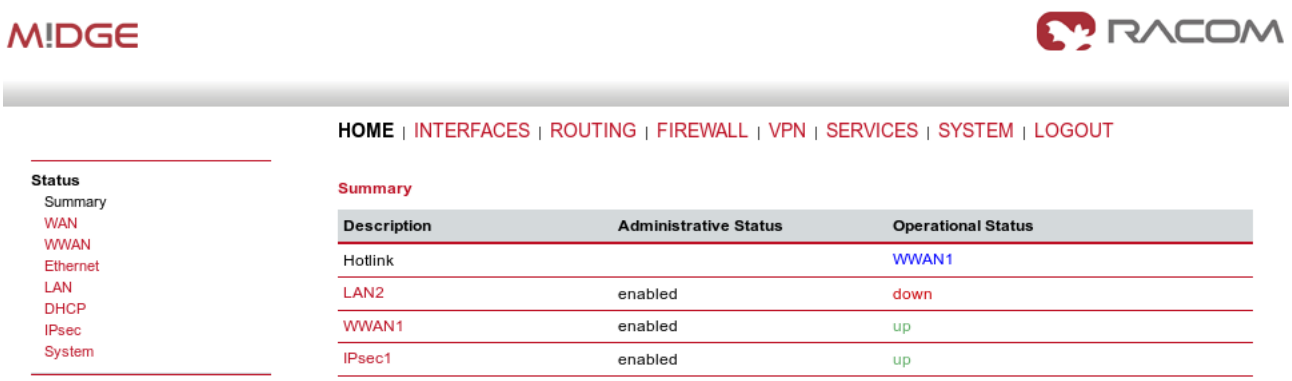


Fig. 1.9: WWAN link is UP

Note

You can test the connectivity by issuing a ping to any desired IP address (e.g. behind the VPN tunnel) in the SYSTEM – Troubleshooting – Network debugging menu.

Plug the cable back into the LAN2 interface and wait a moment for the M!DGE to reestablish the primary connection again.

You can also check the correct functioning of the Supervision feature.

Fill in both host IP addresses in the Supervision menu. One needs to be reachable only via the cellular network and the other one only via the WAN network. Turn off the server with an IP address reachable via the WAN network. The active connection should be changed to the cellular network. Turn on the server again and see the link switch back to the primary one.

2. Mobile IP together with VPN tunnels

If the primary link fails in the previous example, our M!DGE has to dial up the mobile connection and reestablish the VPN tunnel which can take more time than your application can handle. With Mobile IP and permanent backup link availability, we can shorten this time to several seconds...

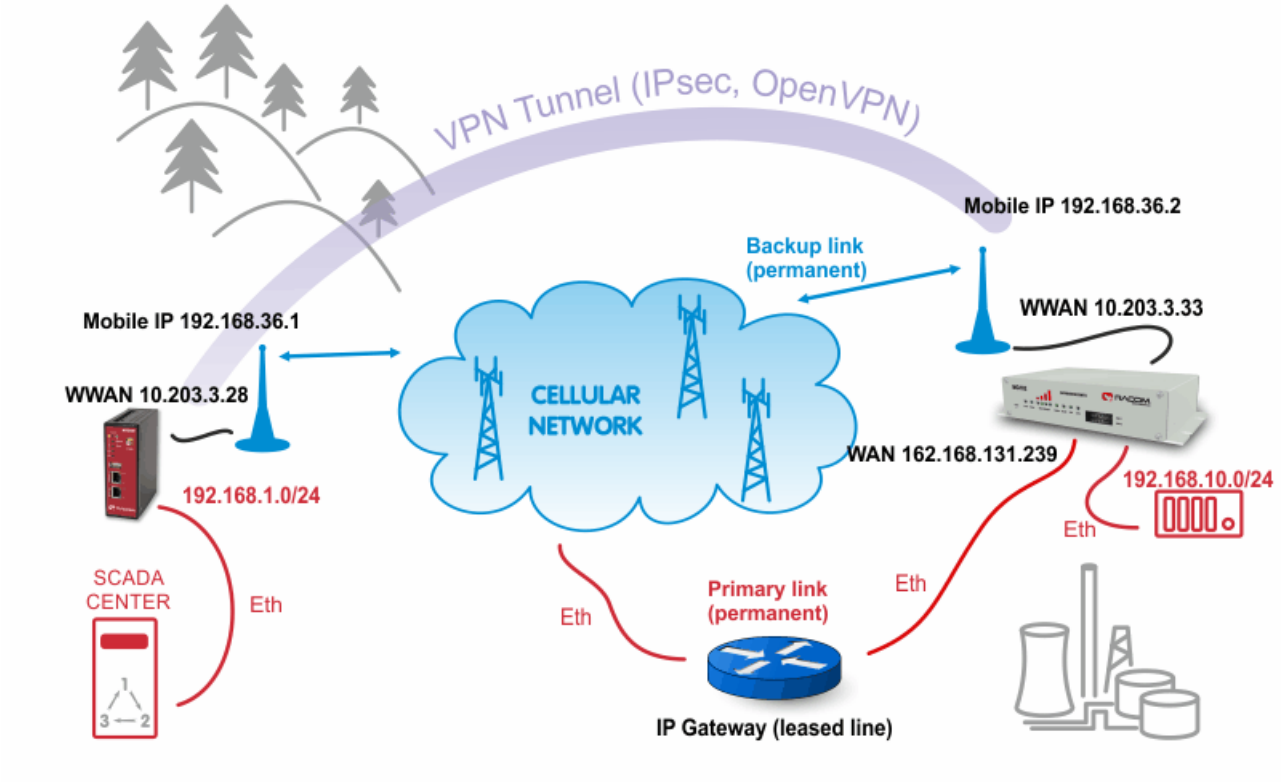


Fig. 2.1: MobileIP with VPN tunnel example topology

The diagram depicts an example in which the M!DGE unit is the VPN and MobileIP server. The server has just one connection option and it needs to communicate with the device behind the remote MG102i unit.

The remote MG102i unit has two possible connection types. The primary link is via faster leased line to the provider's network and the cellular connection is the backup option. Both will be “up” permanently.

Note

The remote connection types can be various, e.g. using WLAN or dualSIM unit with two cellular providers.

On both units, we configure the Mobile IP feature so the VPN tunnel can resist switching the links.

2.1. M!DGE Configuration

On the central M!DGE unit, we need to configure Ethernet IP addresses, mobile connection, VPN tunnel, correct time and of course Mobile IP.

2.1.1. Ethernet

The Ethernet IP address of the server is 192.168.1.1 with 255.255.255.0 mask.

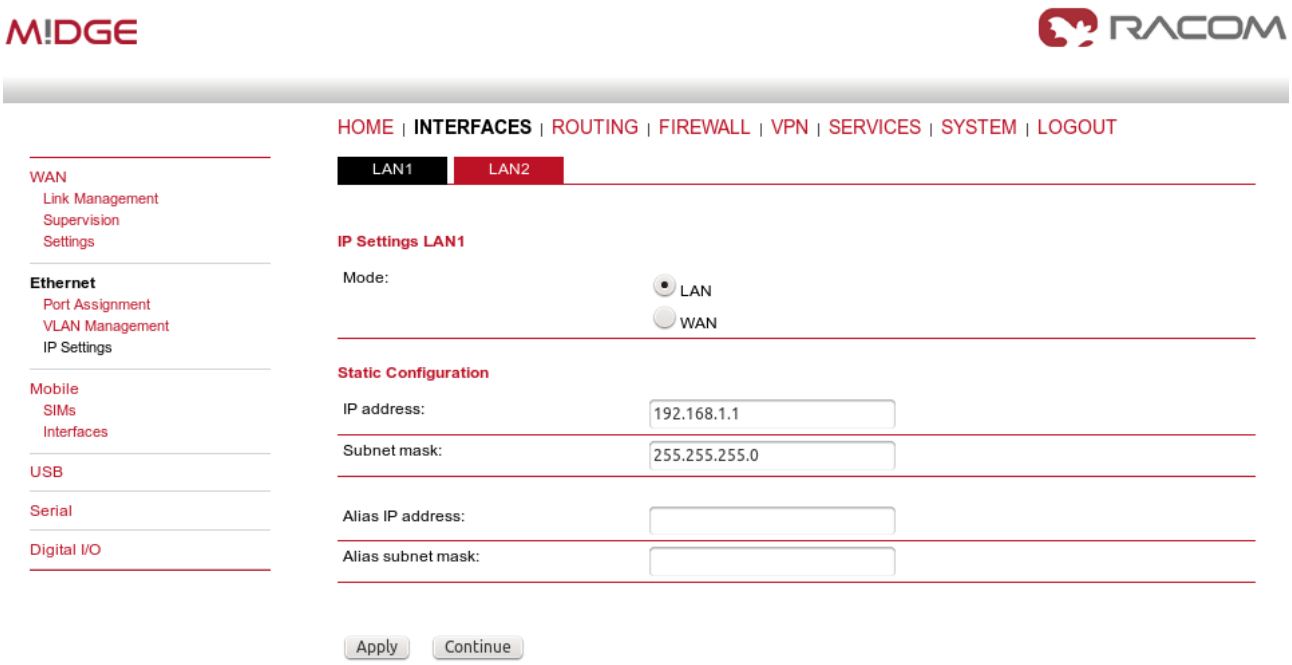


Fig. 2.2: Server's Ethernet configuration

The server is utilizing only the first port so you do not need change the LAN2 IP address. Another step is to define the mobile connection. Configure the SIM card, APN and username/password in the INTERFACES - Mobile menu and check whether it is enabled afterwards.

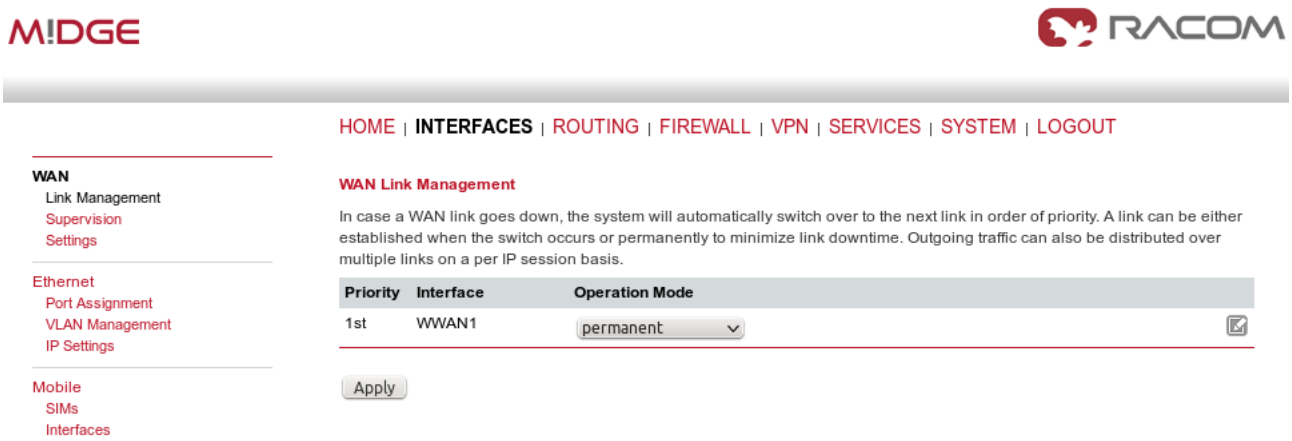


Fig. 2.3: Server mobile connection is activated

In case you will use OpenVPN tunnel, it's necessary to have a correct time in the unit. This can be achieved by setting the NTP server to synchronize the internal time. Go to the SYSTEM – Time & Region menu and fill in the reachable NTP server of your choice. Also set the correct time zone and Daylight saving option.

Note

If using IPsec tunnel, it is not necessary to have a correct time our routers, but it is still useful for troubleshooting.

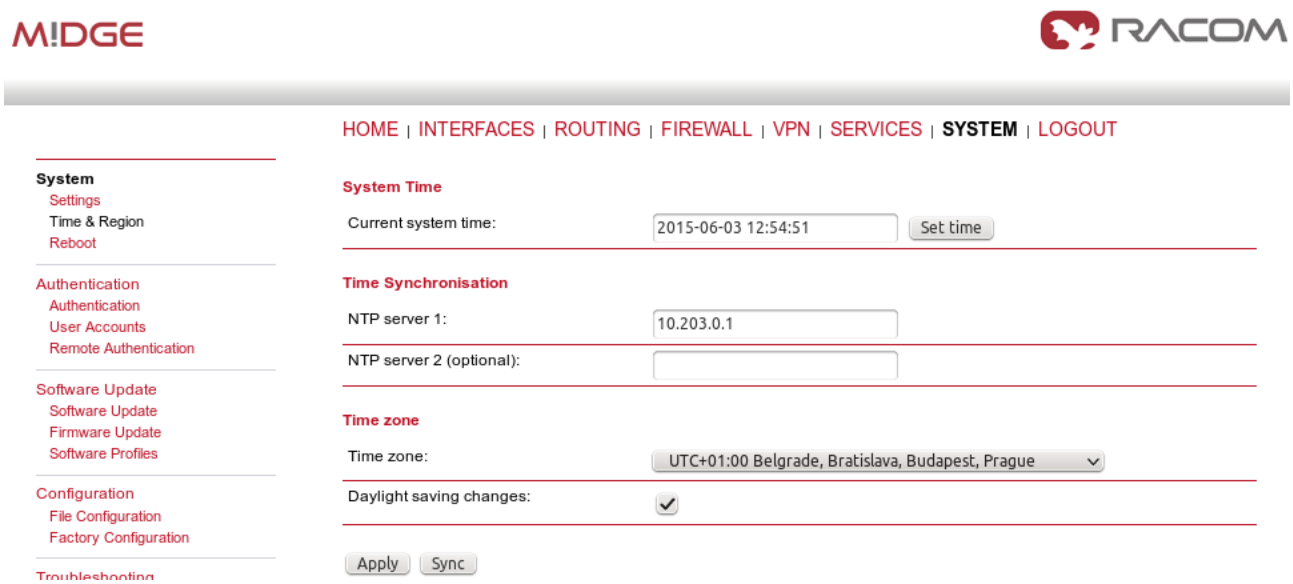


Fig. 2.4: NTP Configuration

2.1.2. Mobile IP

Now we need to configure the MobileIP functionality. With Mobile IP, the client (mobile node) can be connected to the network anywhere and if the server's (home agent) cellular IP address is reachable from the client, you can always communicate via new pair of IP addresses. See the details in the example.

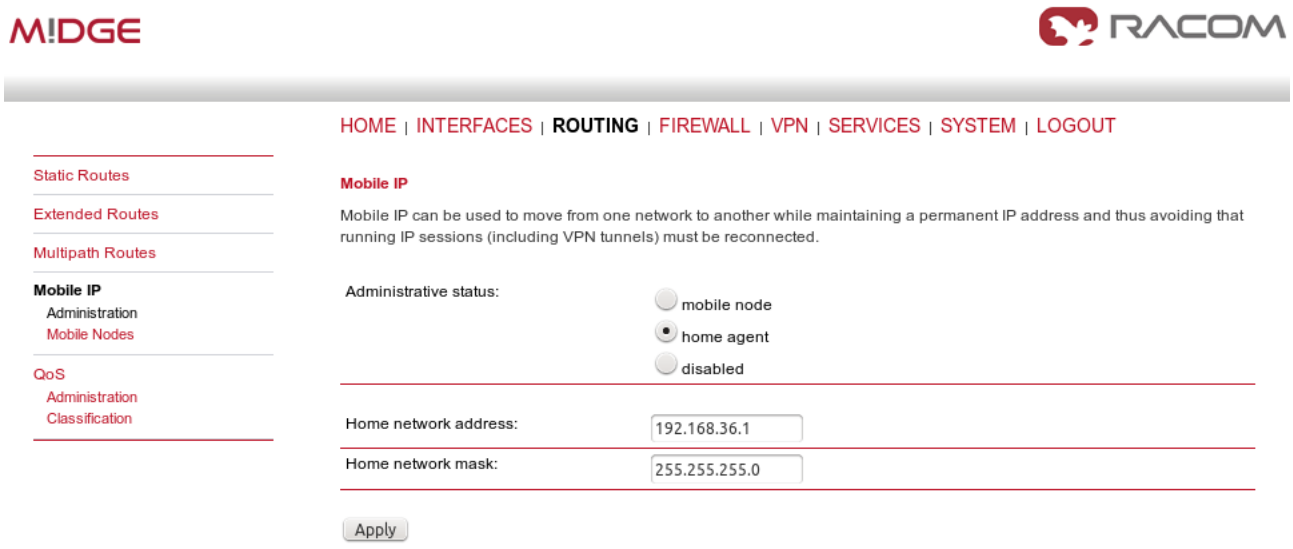


Fig. 2.5: Mobile IP Home agent configuration

The configuration itself is very easy. Just choose the “home agent” status and fill in the agent's IP address and mask – in our example it is 192.168.36.1/24.

The Mobile IP is automatically enabled afterwards.

Another step is to configure the clients (mobile nodes). For each client, define a specific SPI (36 in our example), authentication type (prefix-suffix-md5) and shared secret (ASCII password).

Fig. 2.6: Mobile nodes

The last step is to configure the VPN tunnel. It can either be OpenVPN or IPsec, the functionality is the same in this example.

2.1.3. OpenVPN

Configure the OpenVPN server in routed mode.

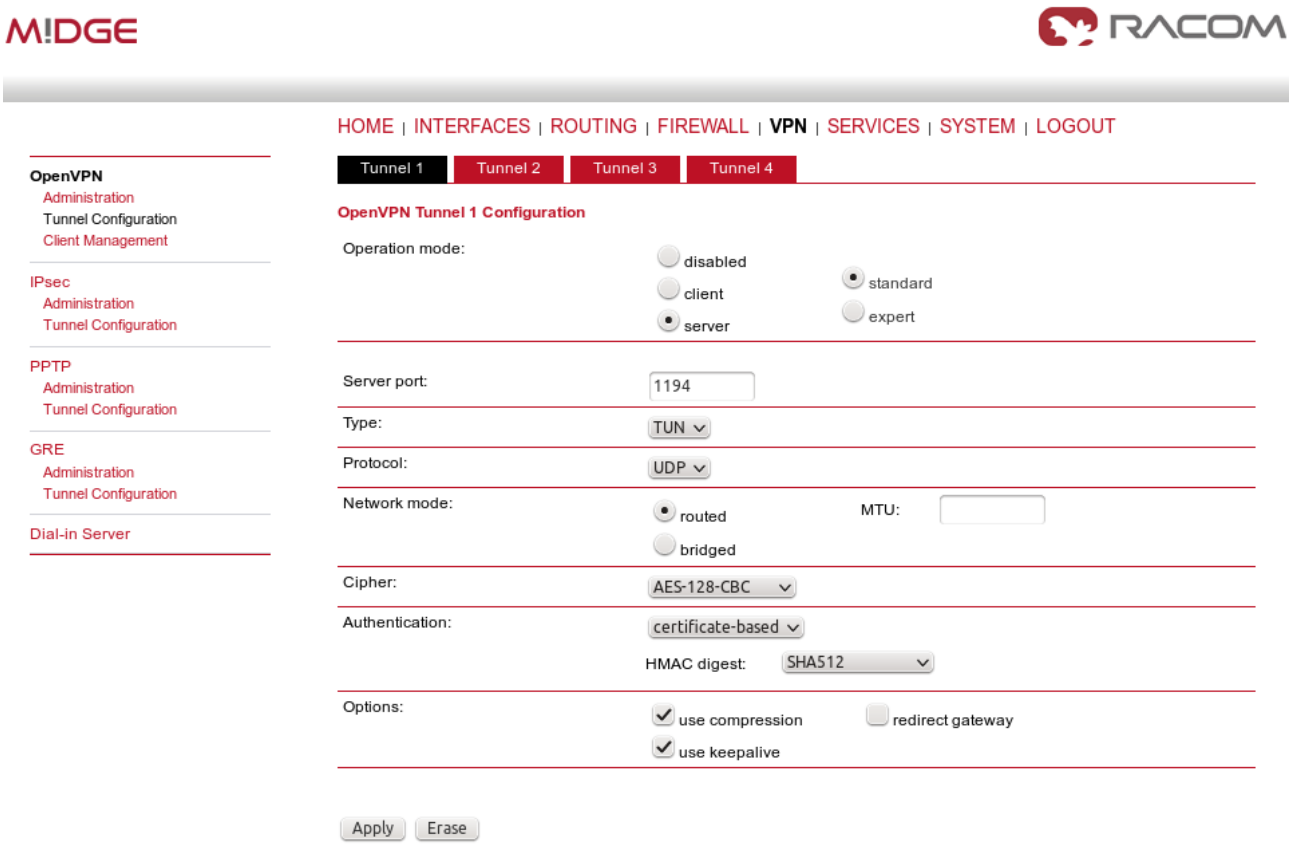


Fig. 2.7: OpenVPN server, Mobile IP

Configure one client (MG102i). Configure the correct IP subnets.

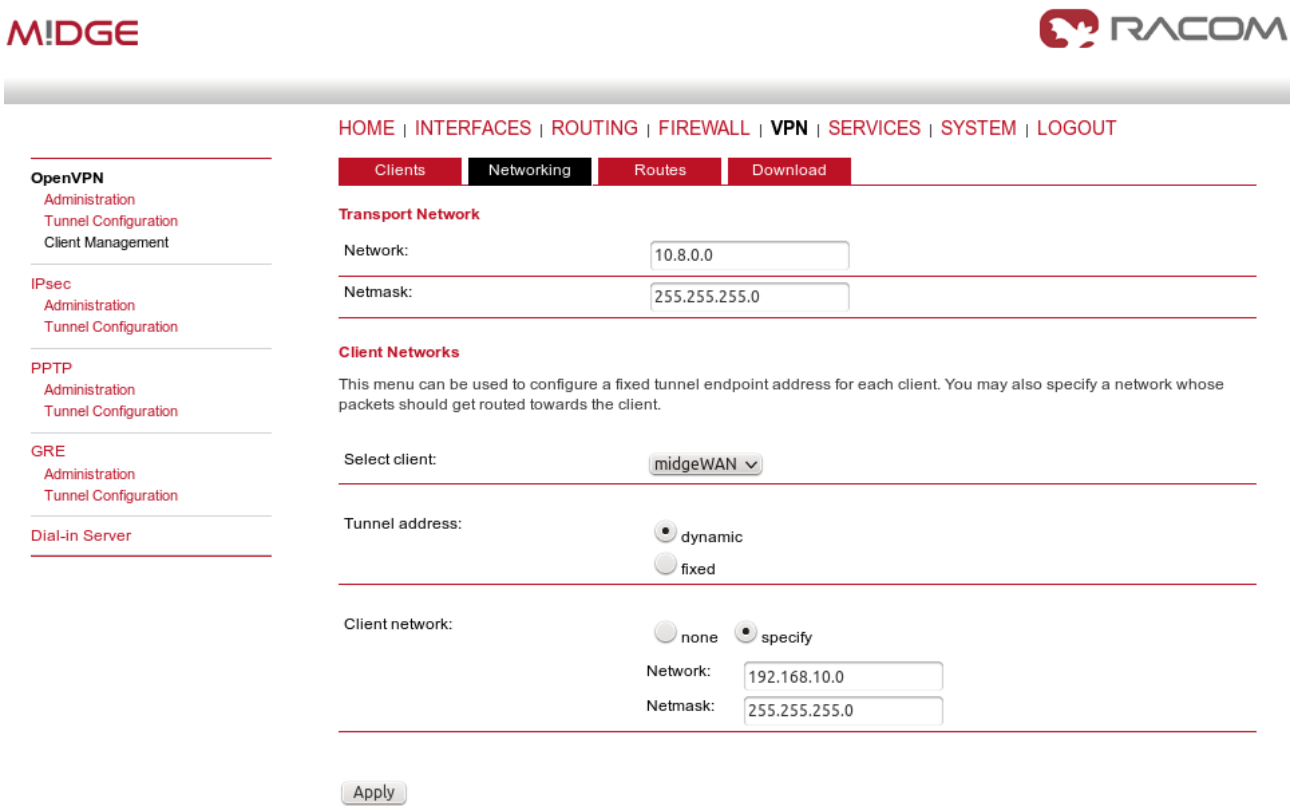


Fig. 2.8: OpenVPN server – Networking

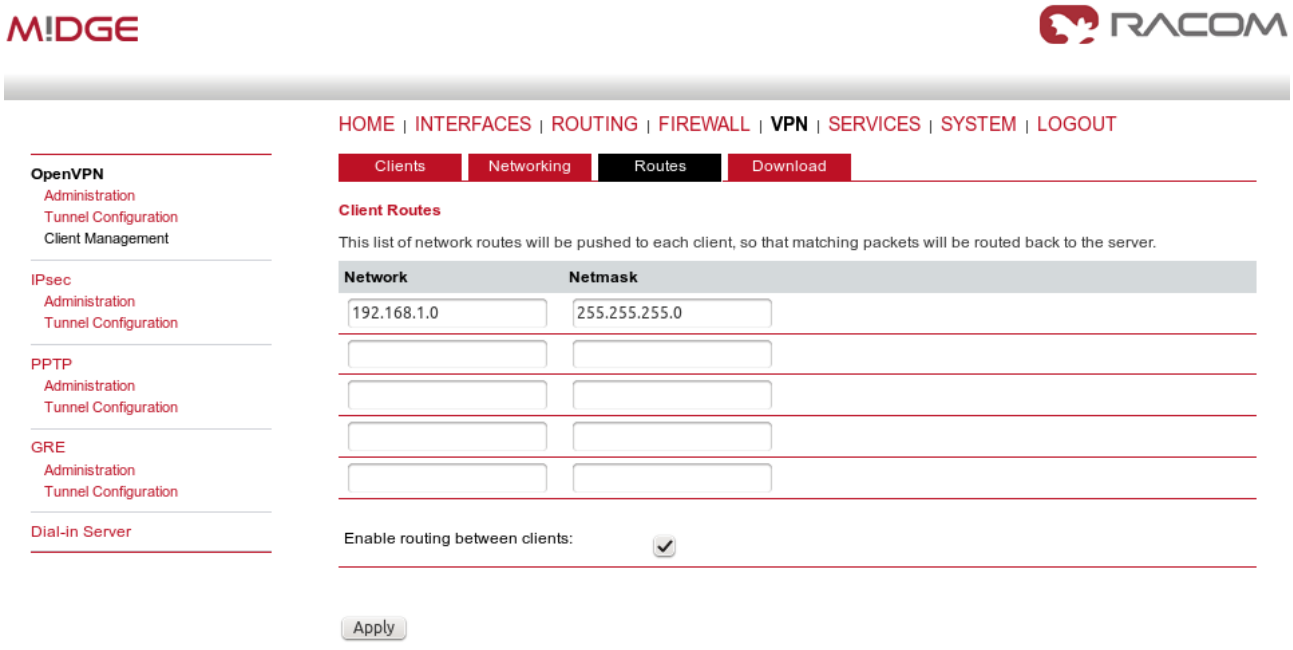


Fig. 2.9: OpenVPN server – Routes

The only difference to the basic VPN configuration is when downloading the Expert file for the client. You must configure the Mobile IP address (192.168.36.1 in our example) so the remote unit connects via Mobile IP network.

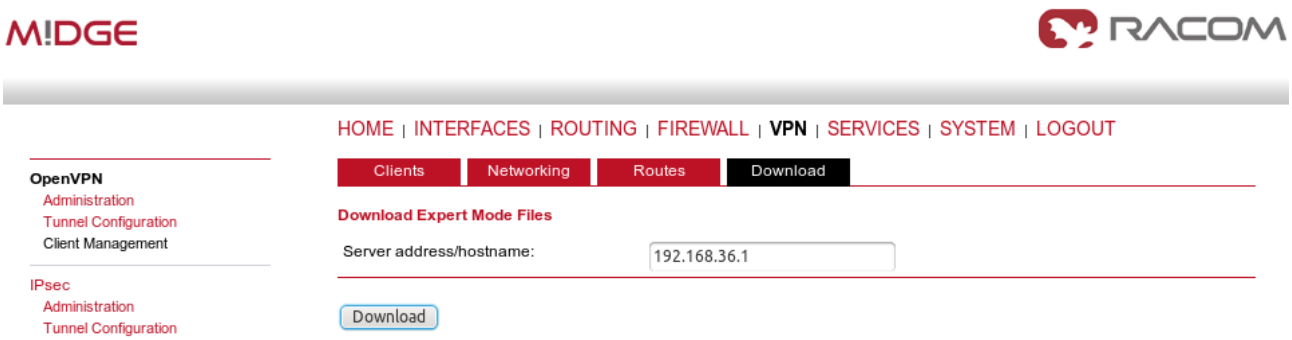


Fig. 2.10: OpenVPN server – Downloading expert file

Enable OpenVPN server and **uncheck** the box for **"Restart on link change"**. This is very important step, do not forget to uncheck this box. If the box is checked, everytime any link changes the status, the tunnel is restarted and we do not want this. This is mainly important on the client's side.

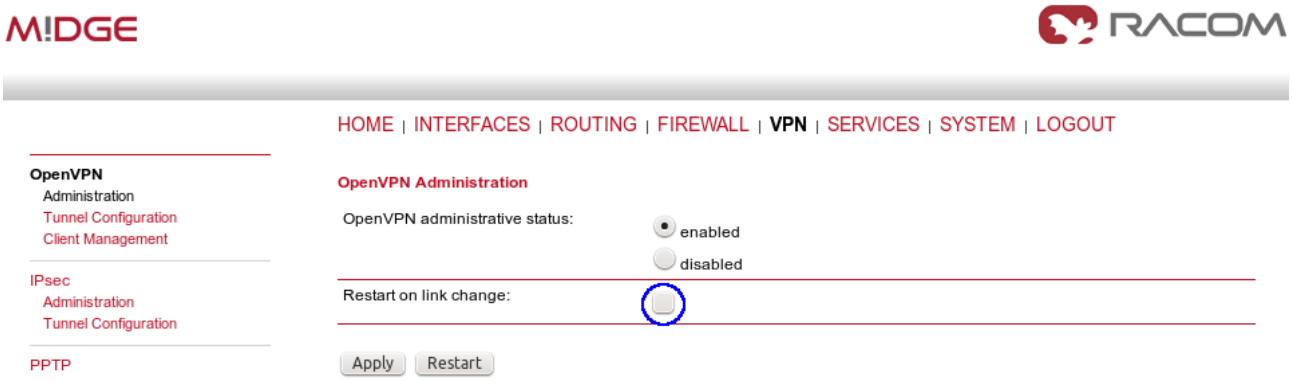


Fig. 2.11: Enabling OpenVPN server

When we finish all configuration steps, we should see the following state in the HOME menu.

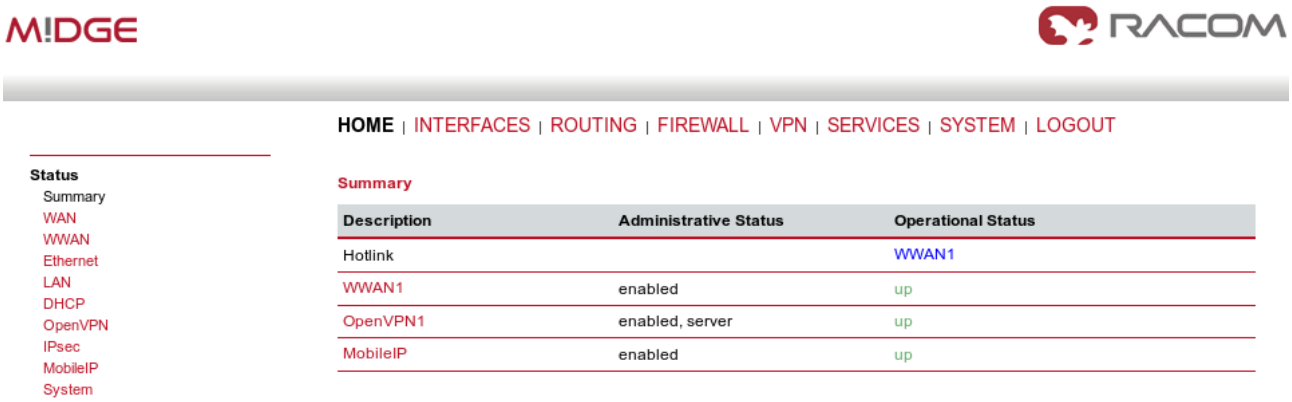


Fig. 2.12: OpenVPN server and Mobile IP are running

2.1.4. IPsec

If you want to use IPsec, the situation is very similar. Just configure the correct IP subnets, set Peer IP address to the Mobile IP address (192.168.36.2) and uncheck the "Restart on link change" box as with OpenVPN.

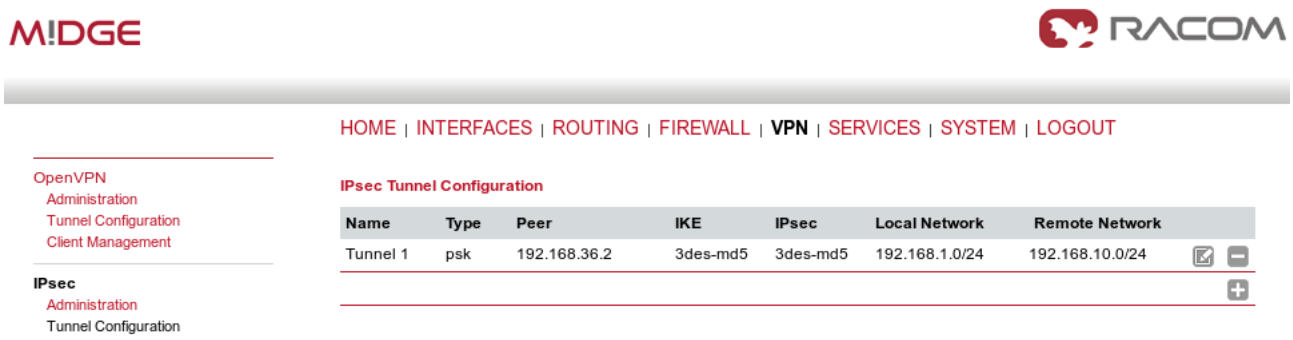


Fig. 2.13: IPsec – M!DGE configuration

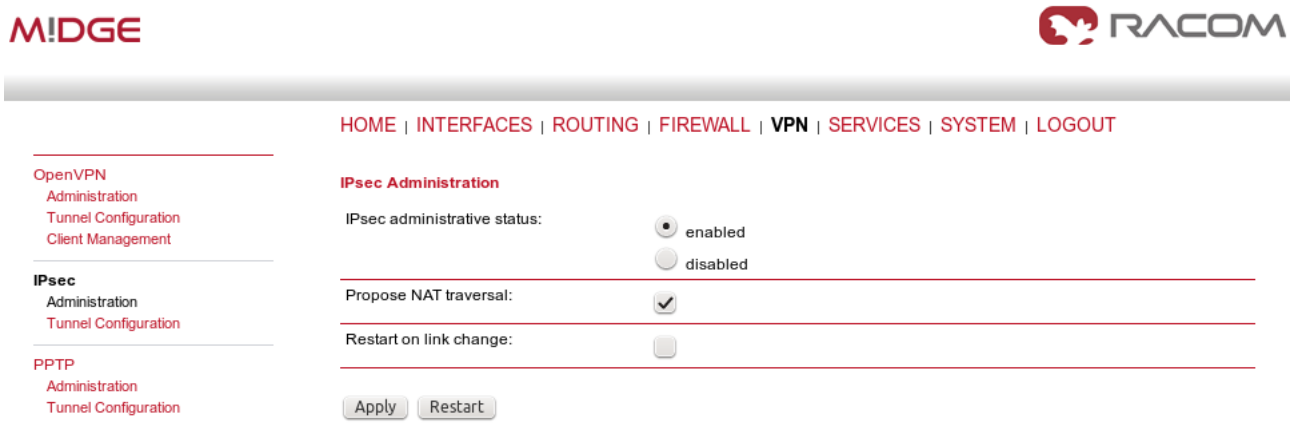


Fig. 2.14: Enabling IPsec – M!DGE

2.2. MG102i Configuration

The client's configuration is more complex due to two connectivity options. The unit needs to be connected to both options simultaneously (permanently).

2.2.1. WAN Configuration

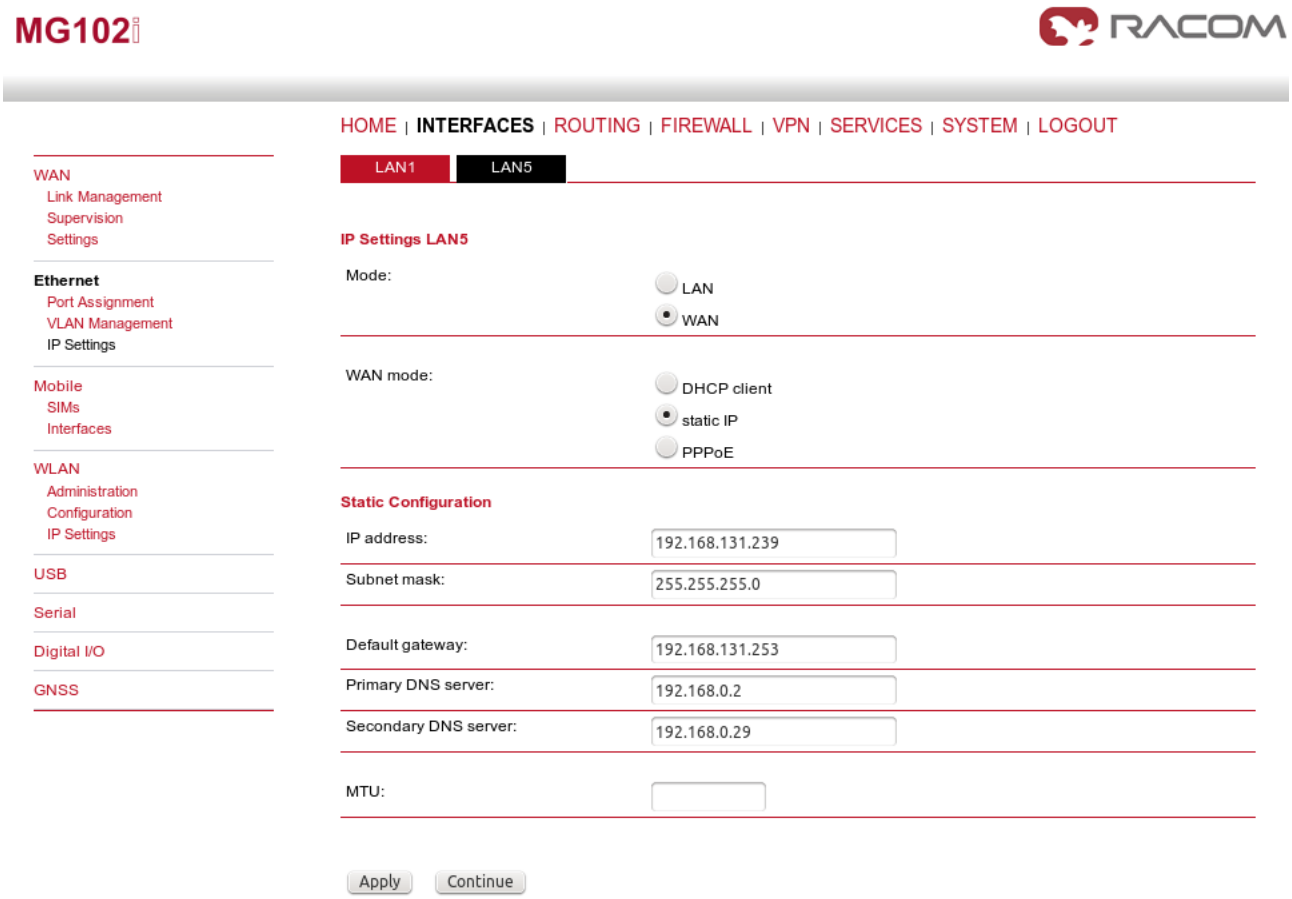


Fig. 2.15: MG102i WAN configuration

The LAN5 interface is configured as the primary WAN link. LAN1 subnet should be set to 192.168.10.1/24.

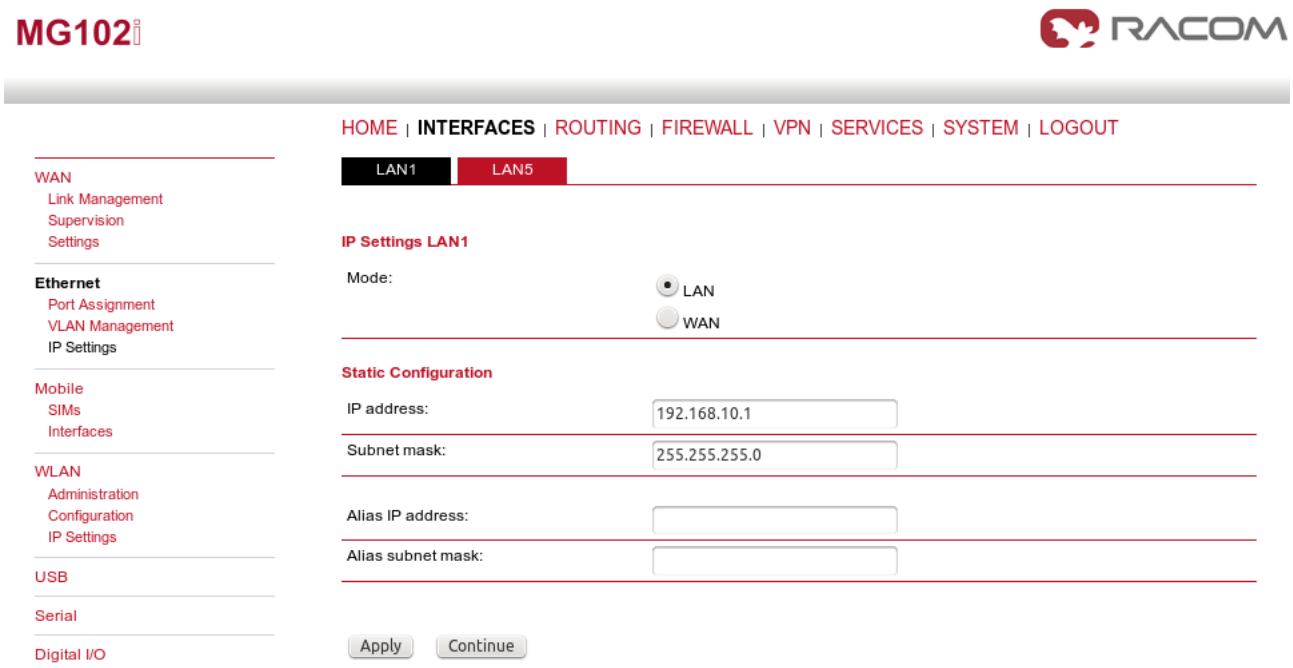


Fig. 2.16: MG102i LAN configuration

Configure the mobile connection and set both links to be permanently “up”.

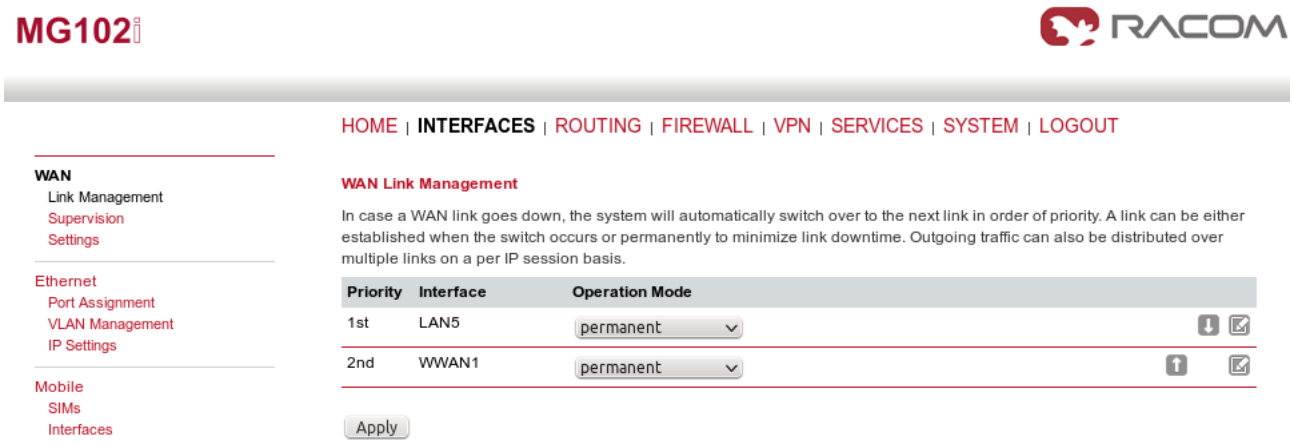


Fig. 2.17: MG102i Link Management

We need to recognize that LAN5 is not available for us and switch to WWAN interface. This is recognized if the Ethernet cable is disconnected, but with Supervision feature, we can check the IP host reachability with ping probes and if this host is not reachable, switch to the backup profile.

In our example, we configure this for each link separately.

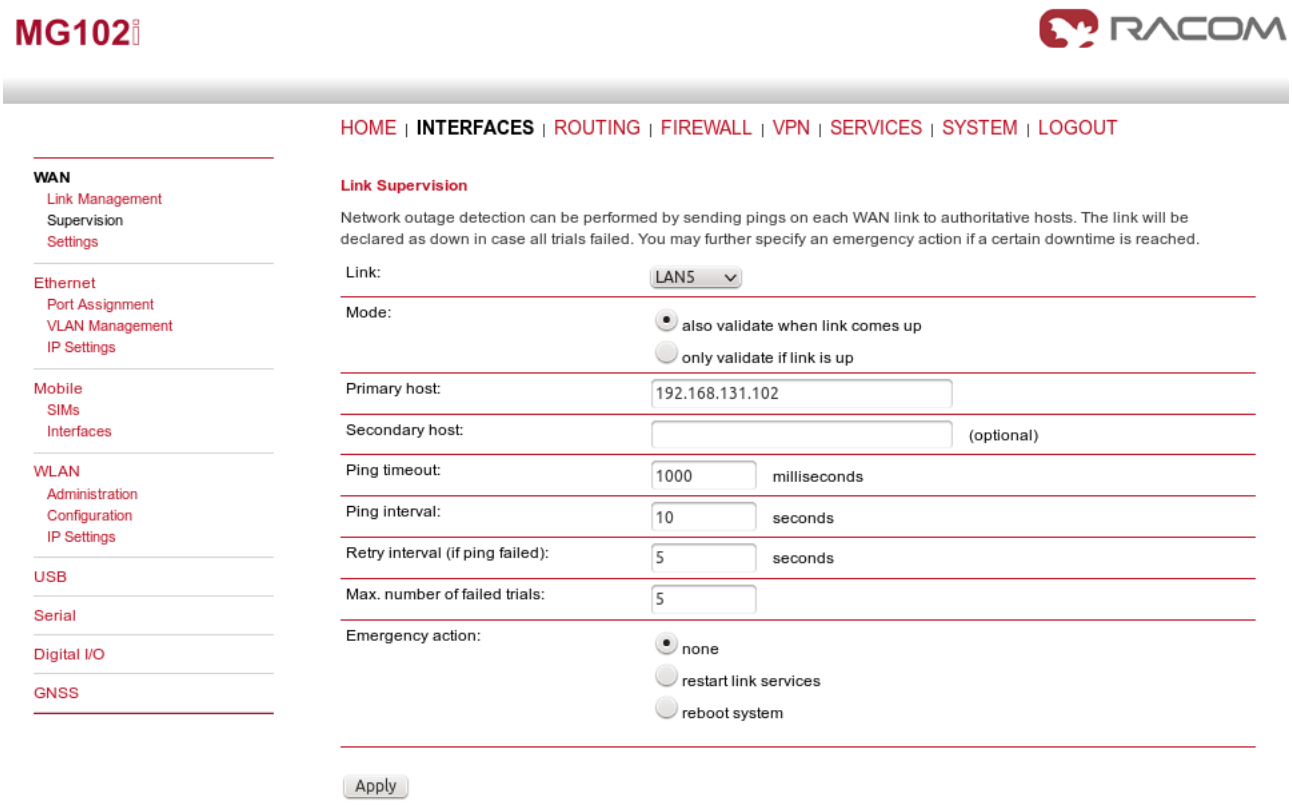


Fig. 2.18: LAN5 Supervision

The primary link is checked every 10 seconds by pinging the 192.168.131.102 host. If the ping is lost 5 times, the link is considered down and the mechanism switches to the WWAN option.

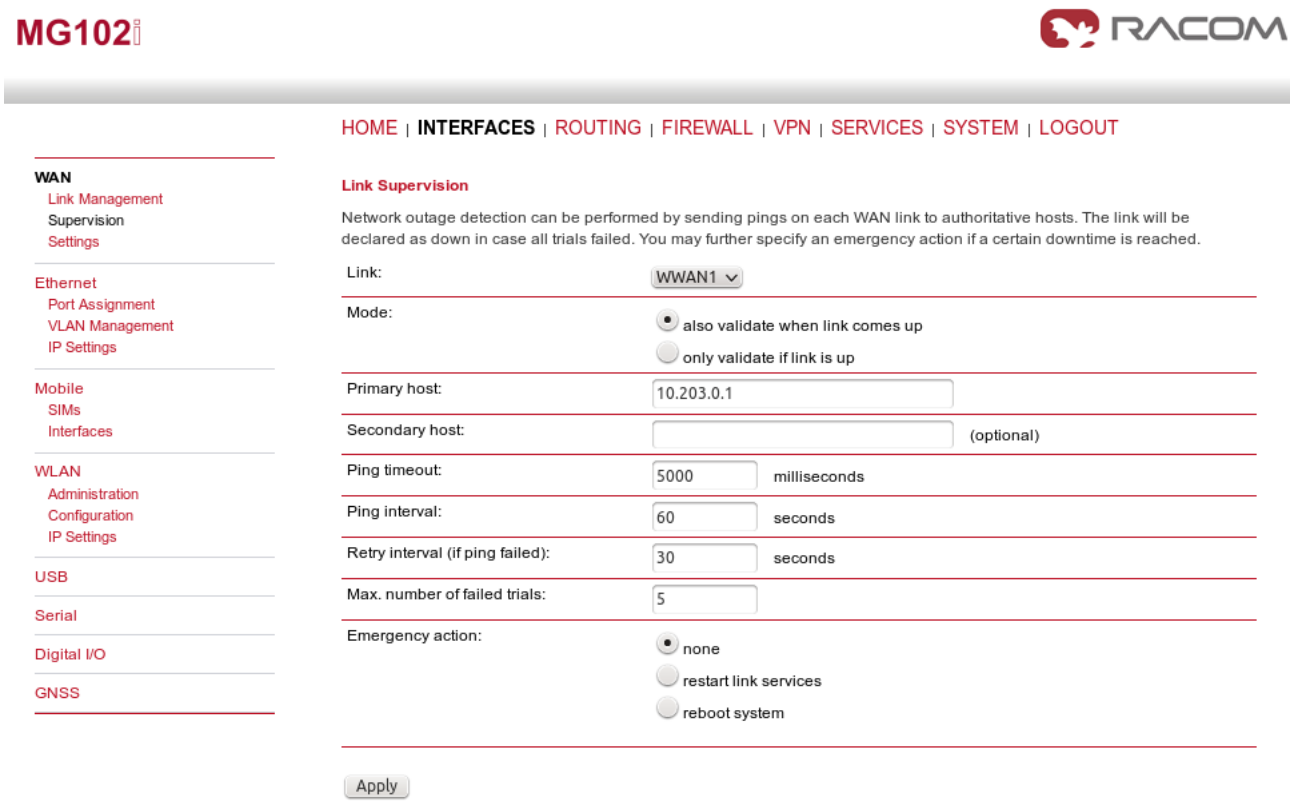


Fig. 2.19: WWAN1 Supervision

The WWAN1 interface is also checked, but we increased the ping timeout (mobile latency can be high) and we check the reachability (of IP 10.203.0.1) less frequently.

Note

In this example, if we switch off the host 192.168.131.102, the Supervision feature will switch the active link to WWAN. It is good to have a similar option for your own testing.

Configure the NTP server in the SYSTEM – Time & Region menu so we have the correct time.

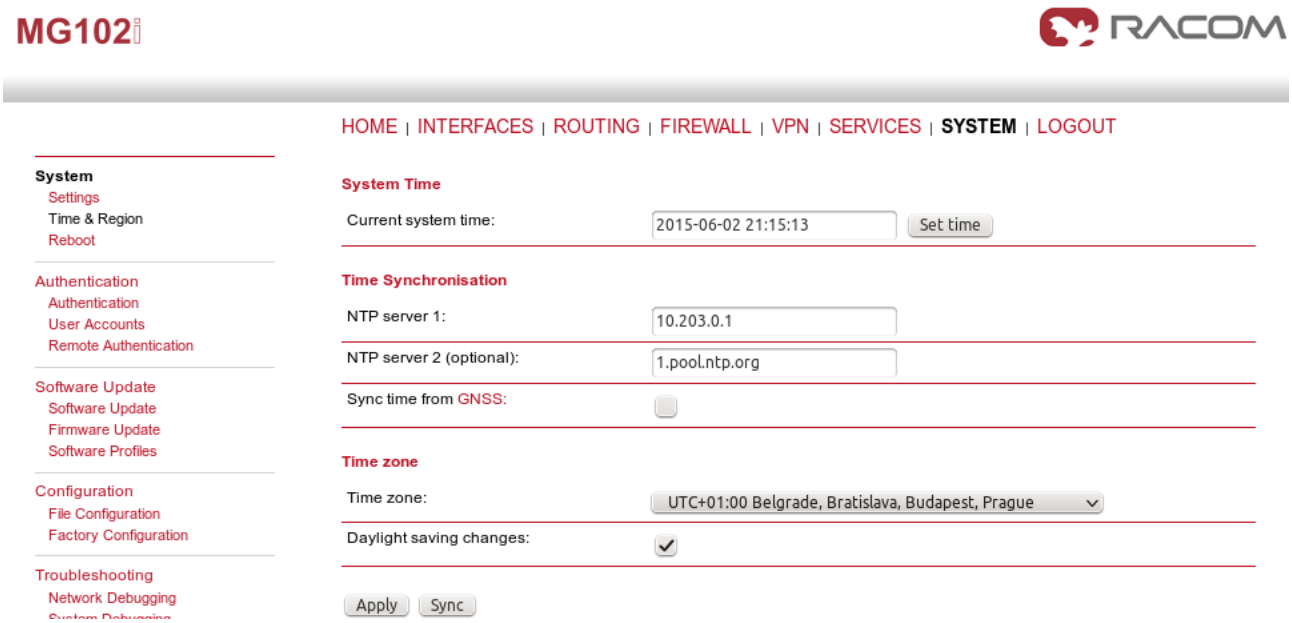


Fig. 2.20: MG102i NTP configuration

2.2.2. Mobile IP

Our MG102i unit needs to be configured as a mobile node for the Mobile IP functionality. Go to the Routing – Mobile IP menu.

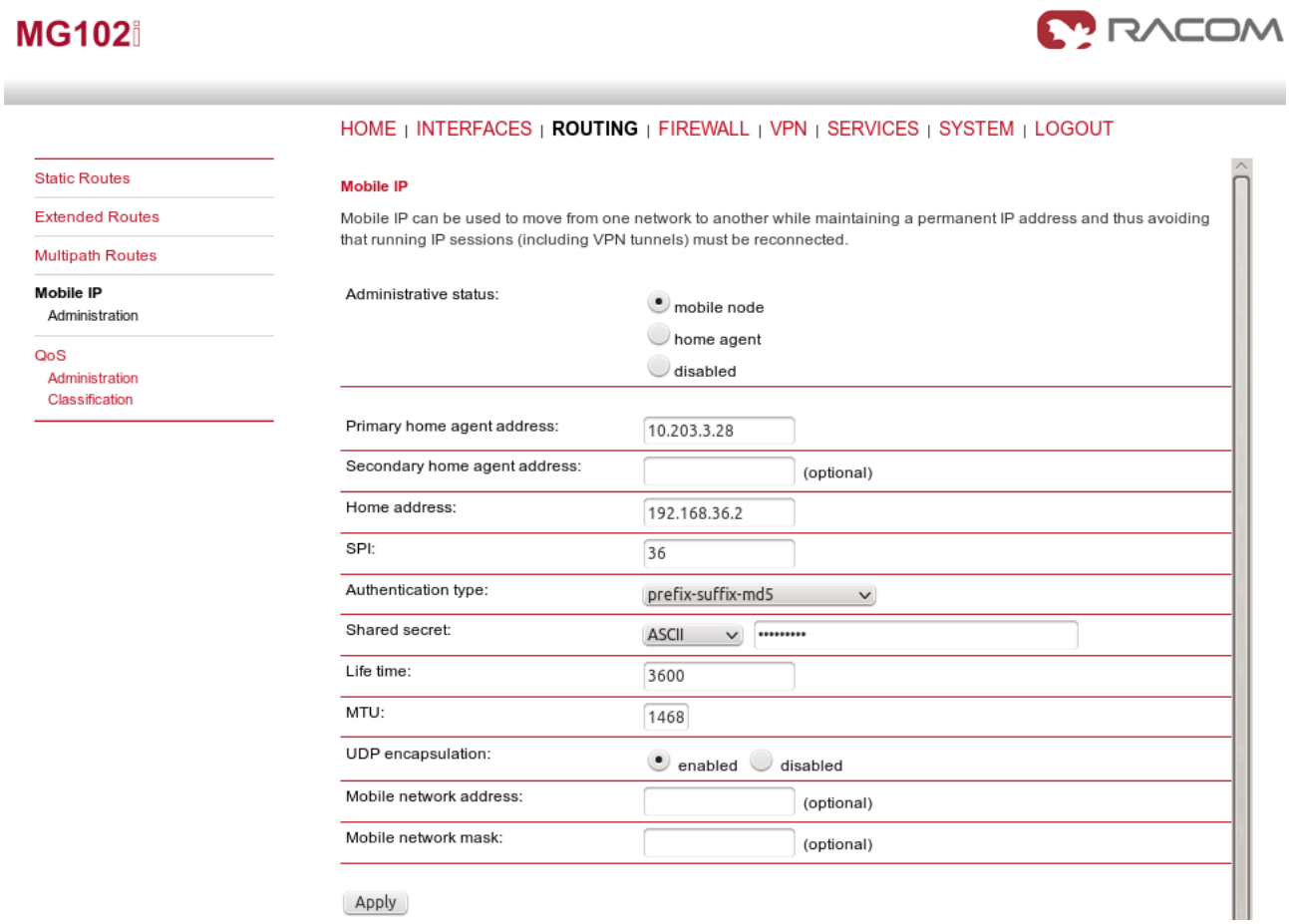


Fig. 2.21: MG102i Mobile IP – Mobile node

Set the Primary home agent address to the cellular IP address of the M!DGE (server) unit, 10.203.3.28 in our example. The home address must fall into the 192.168.36.0/24 subnet. Set the correct SPI which was configured on the server and fill in the correct secret. Keep the rest in the defaults.

Another step is to define the server's Mobile IP address (192.168.36.1/32 via MobileIP1 interface) in the Routing menu.

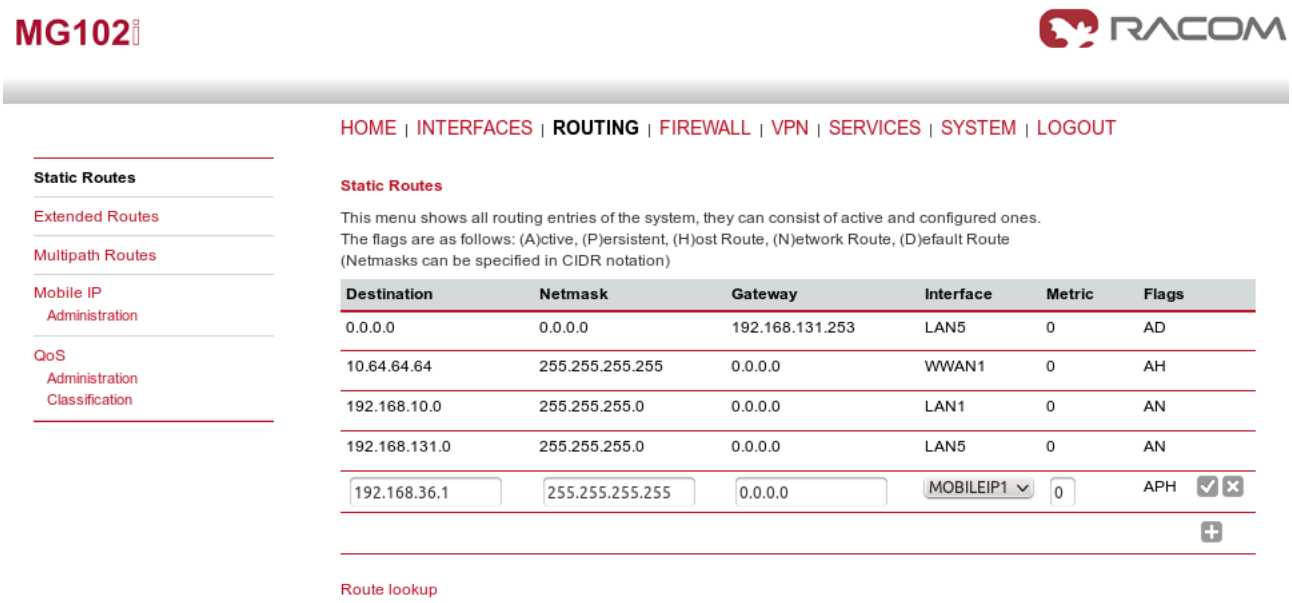


Fig. 2.22: MG102i Routing menu

Without this option, MG102i unit would not know the server's Mobile IP address which is essential for the proper functionality of Mobile IP.

2.2.3. OpenVPN

MG102i is a client in the OpenVPN configuration so just upload the Expert file and set the mode to “Routed”.

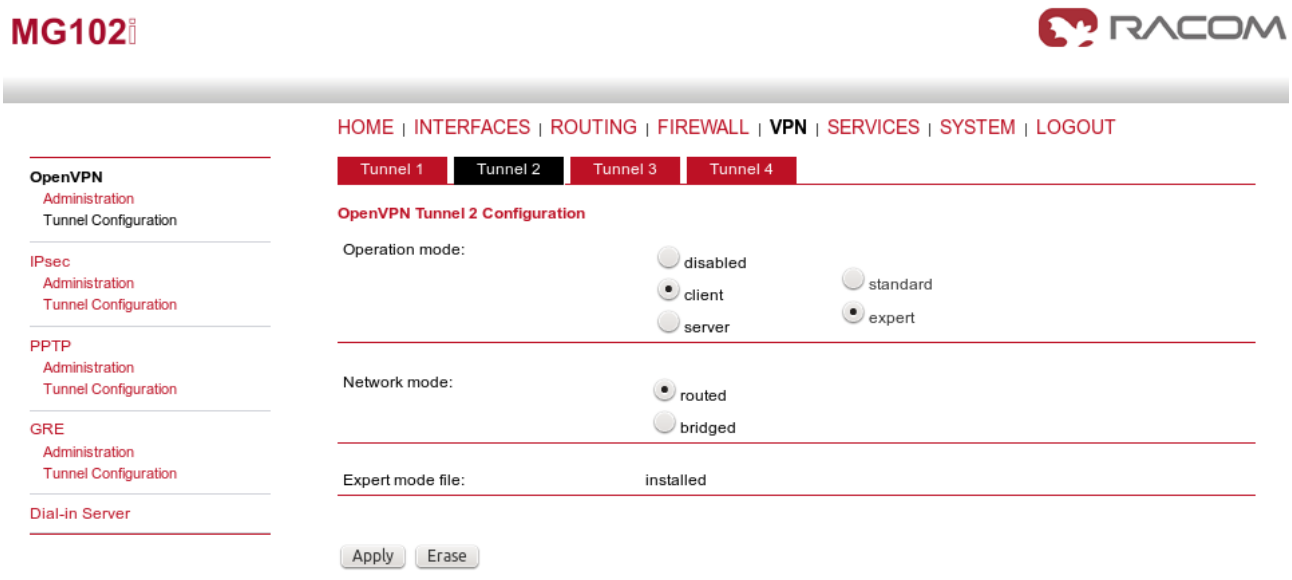


Fig. 2.23: MG102i OpenVPN – Expert file

Enable the tunnel and **uncheck** the **“Restart on link change”**. This is essential for fast switching of active link, do not forget to uncheck this option.

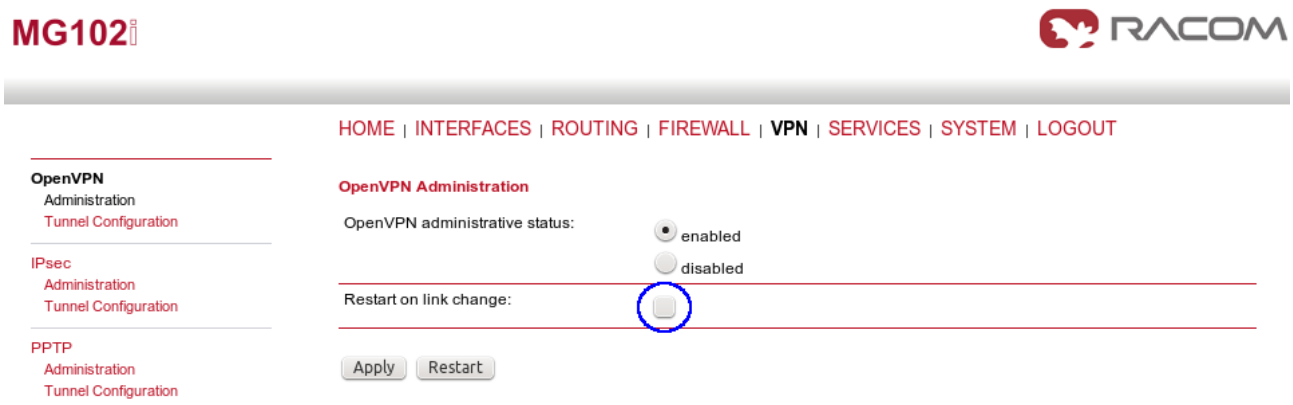


Fig. 2.24: Enabling OpenVPN – MG102i

The tunnel should be established quickly and the HOME menu should be similar to the following example.

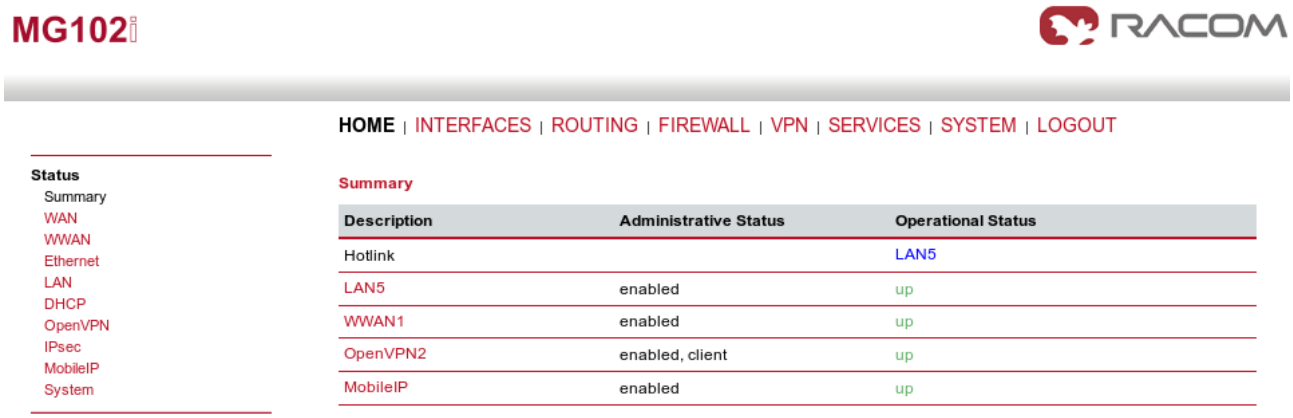


Fig. 2.25: OpenVPN and Mobile IP running – MG102i

2.2.4. IPsec

If you choose IPsec, configure the tunnel as on the server (credentials, IDs switched, networks switched, …) and set the Peer IP to 192.168.36.1 (Mobile IP address of M!DGE unit).

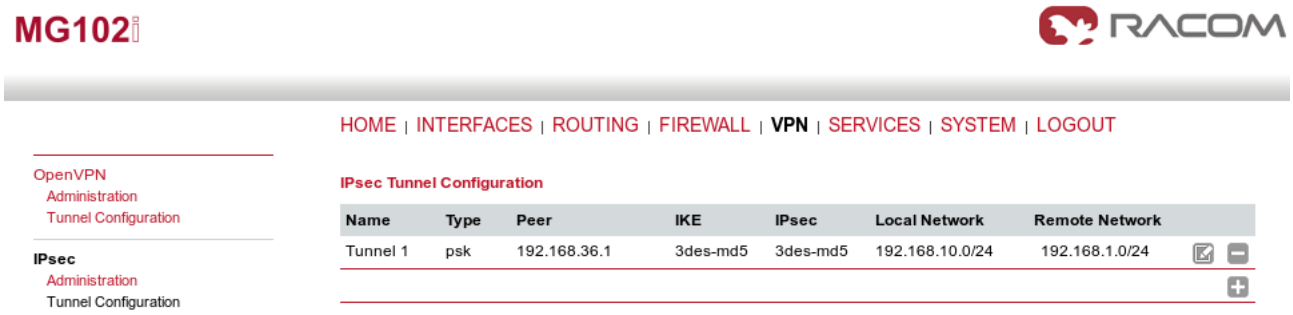


Fig. 2.26: IPsec configuration – MG102i

Enable the tunnel and uncheck the **“Restart on link change”** box again.

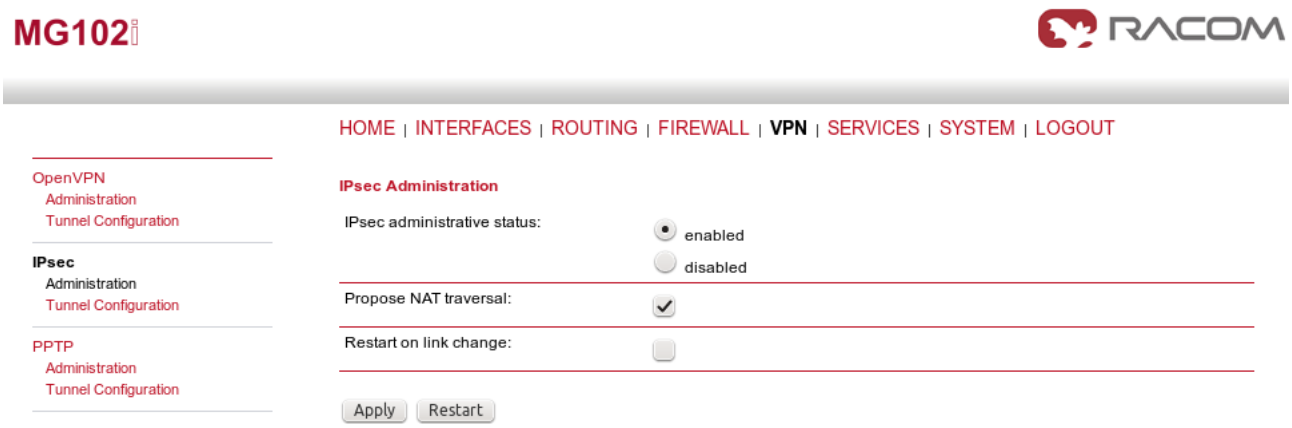


Fig. 2.27: Enabling IPsec – MG102i

If configured correctly, check the HOME menu.

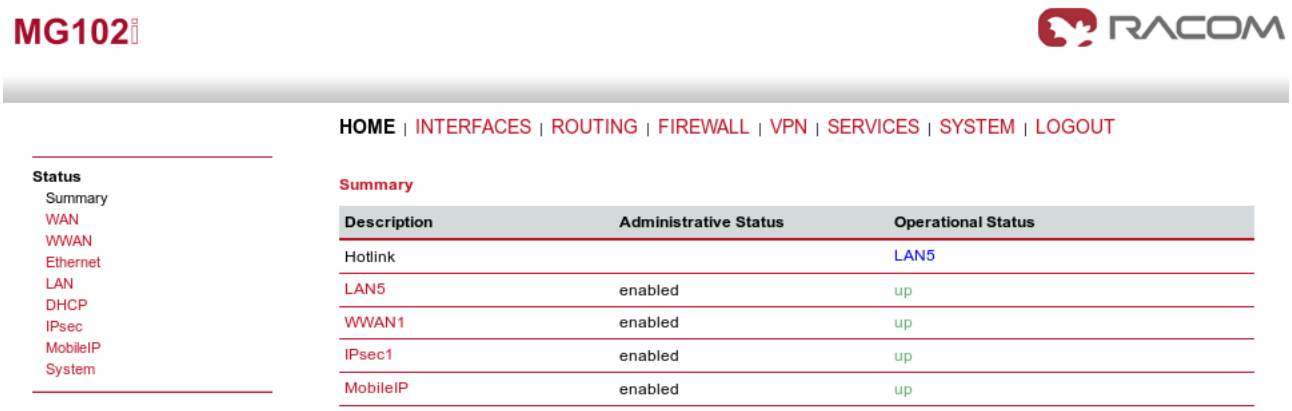


Fig. 2.28: Ipsec and Mobile IP running – MG102i

2.3. Practical Test

After all required configuration steps are done, the reachability of devices in the M!DGE and MG102i subnets should be achieved. The encrypted data should pass through the LAN5 (WAN) interface on MG102i unit. If you do not have any attached devices, you can check the reachability from the CLI menu of either M!DGE or MG102i.

```
~ $ ping -I 192.168.10.1 192.168.1.1
PING 192.168.1.1 (192.168.1.1) from 192.168.10.1: 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=519.988 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=571.220 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=537.150 ms
64 bytes from 192.168.1.1: seq=3 ttl=64 time=523.829 ms
^C
--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 519.988/538.046/571.220 ms
```

Fig. 2.29: Ping probe from MG102i to M!DGE

If you are using Windows to access the unit, run Putty for accessing the unit via SSH. Set the user to “root” and use the same password as for the admin account for the web interface. Running the command “ping” must be defined with “-I” parameter so the source address would fall into the VPN routed subnet.

To force the link of MG102i to switch to backup option, you can either unplug the Ethernet cable or switch off the host set in the Supervision menu. The result will be that the WWAN interface will be used.

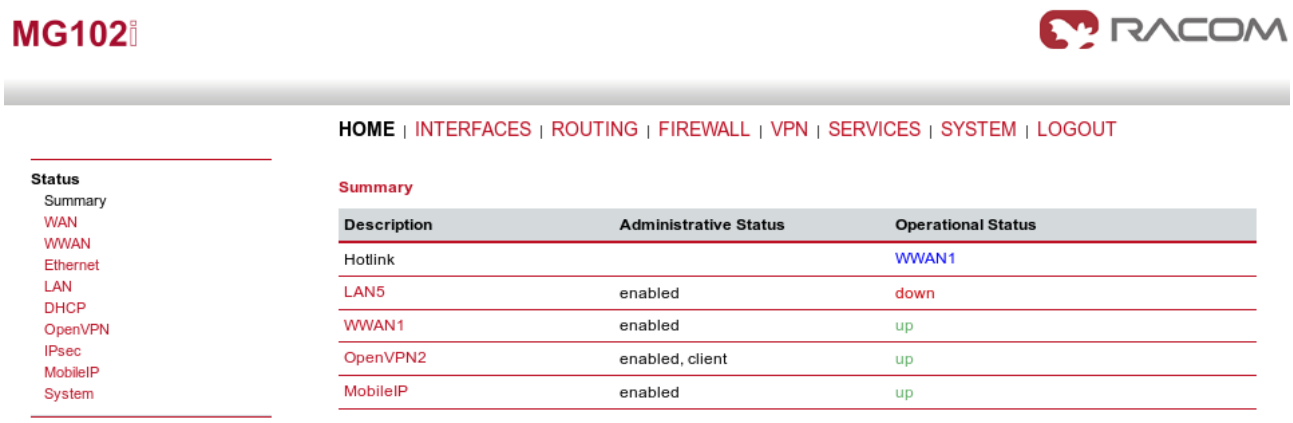


Fig. 2.30: Using the backup interface

During the switchover, run the ping command continuously from the Server to the Client (pinging 192.168.10.1 IP address with a source address within 192.168.1.0/24 subnet). You will see that several packets are lost, but the time needed for the switchover is within seconds. You can compare it without using Mobile IP functionality.

You can also run your target application and see what happens during switching the links.

Note

Using the web interface's Network debugging tool would not work, because the source IP address/interface cannot be set and the reply would not be forwarded to the VPN tunnel.

See the *manual*[1] for more details.

[1] http://www.racom.eu/eng/products/m/midge1/index.html

Appendix A. Revision History

Revision 1.0 2017-12-07
First issue

Revision 1.1 2018-02-28
Termination of M!DGE UMTS routers manufacturing