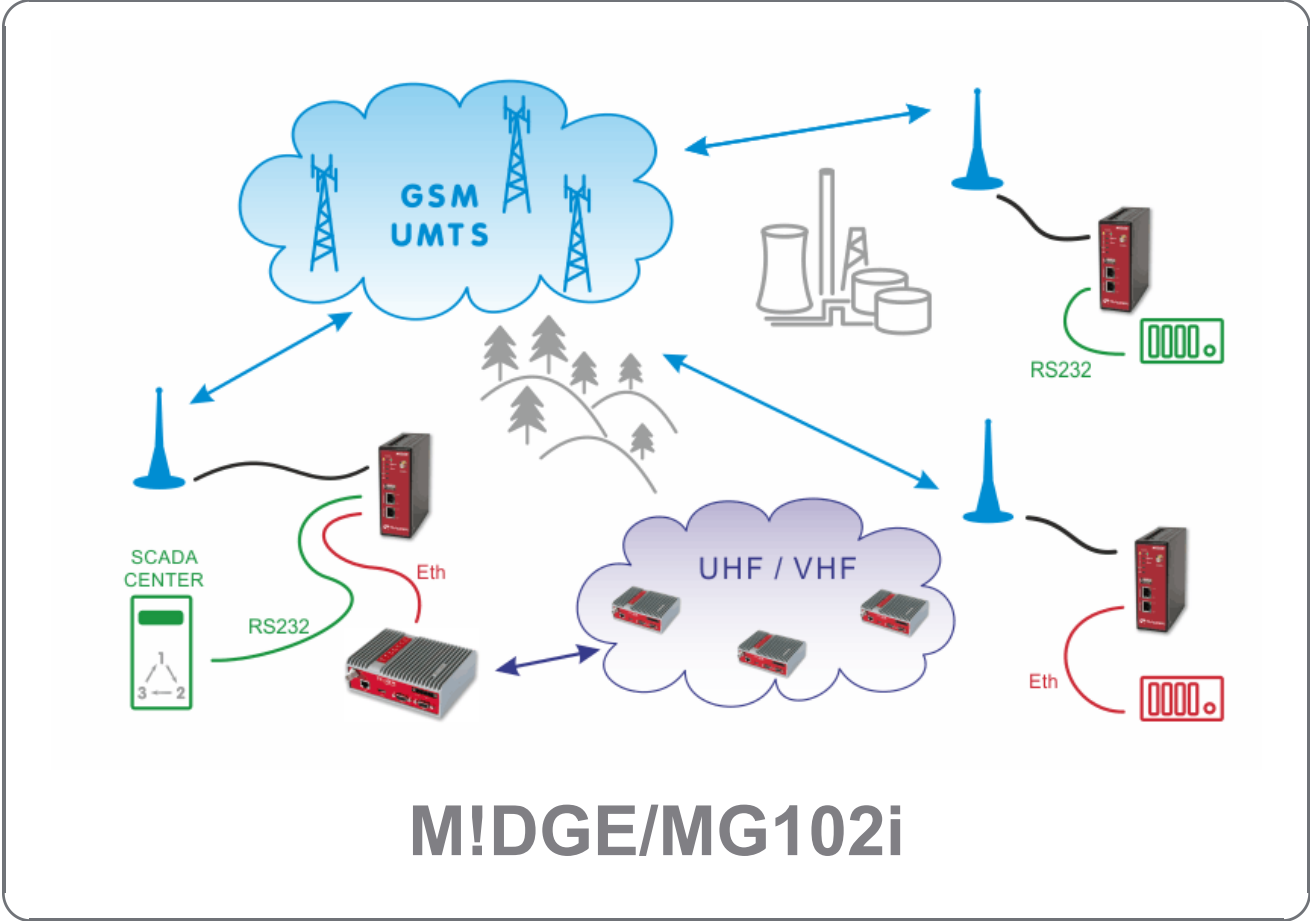




Application notes



version 4.0
7/21/2015

Table of Contents

Introduction	5
1. Overview of Typical MIDGE/MG102i Applications	7
1.1. A Standalone MIDGE/MG102i in the Center	7
1.2. A leased line to the Cellular Network Center	10
1.3. Backup of WAN by GSM Network	14
1.4. Serial Port SCADA Protocols in GSM Network	14
1.5. GSM and UHF/VHF Radio Data Network Combination	16
2. VPN Configuration Options	17
2.1. OpenVPN	17
2.2. IPsec	32
2.3. GRE	38
2.4. PPTP	39
3. Backup of WAN by the GSM Network	40
3.1. Basic Backup Example	40
3.2. Mobile IP together with VPN tunnels	45
4. SCADA Serial Protocols over GSM Network	63
4.1. SCADA Protocols – private APN	64
4.2. SCADA Protocols – public APN	70
5. UHF/VHF and GPRS/UMTS Combination	74
5.1. Practical Example	75
A. Revision History	82

Introduction

Thank you for your interest in our GPRS routers. This application note will help you get up and running with our solution, to serve your business. It will provide you with various applications where these routers come in handy and how to configure them properly.



Note

This document is not intended to explain all configuration options – see the Manual¹ for details.

SIM cards for mobile connectivity are required, as with using any cellular router. All SIM cards must have **data transmission enabled** and you need to know the **Access Point Name (APN)**, which is the name of a gateway between the mobile network and another computer network, most often the public Internet.



Note

If not specified otherwise, all features are supported within all cellular systems based on GSM such as GPRS, UMTS, HSPA+, LTE and others.

Choosing the most suitable APN for your application is important. As well as considering the number of units within your application. If you have about 5 – 25 units, you can work just with our M!DGE/MG102i routers, but if hundreds of units are required, a special leased line to service providers or VPN concentrators can be required. See the differences in Section 1.1, “A Standalone M!DGE/MG102i in the Center” and Section 1.2, “A leased line to the Cellular Network Center”.

Basically, you can have **five options for choosing APN**:

1. The public “**internet**” APN via which you obtain a **private and dynamic mobile IP address**. Typically, our unit needs to initiate the connection to the Internet – i.e. the client cannot send data to this unit without establishing some kind of connection from our unit first (TCP, VPN tunnel, ...). Also keep in mind that the obtained IP address is always different. This APN can be suitable if you have one central location (e.g. with public and static IP address) and the clients connect via VPN tunnel.
2. The second solution is almost the same, but with a **static IP address**. This IP address is still within the **private IP range** and is not reachable from outside directly, because this direction is blocked by the provider's network firewalls. However the benefit can be that the VPN concentrator accepts incoming VPN tunnels only from predefined IP addresses and the rest are rejected.
3. Another option is to obtain a **dynamic public IP address**. With these IP addresses, you can have the communication among the units without VPN tunnels (but they can be used) and in both directions. The only issue is that you need to configure **Dynamic DNS** services for each unit so the connections will be made via hostnames (always the same for a given unit) and not via IP addresses (which are different). Keep in mind that Dynamic DNS functionality can be chargeable and is not under RACOM control.
4. The last general solution is to have both **public and static IP addresses**. This is typically required only for the central unit and is usually the most expensive solution. The benefit is that you do not need to use Dynamic DNS nor rely on third party functionality. Together with the third option, do not forget to configure firewall rules to limit the access to your units, because the connection is open from the Internet side.
5. The last, but very important option is to use **private APN**. The IP addresses are given to you within a **private range**, they are usually **static** and they **cannot access the Internet**, but they can

¹ <http://www.racom.eu/eng/products/m/midge1/index.html>

reach each other directly. The benefit is that you have full control of your network and each unit is reachable from any other. You don't need to configure any VPN tunnels unless required by security reasons. Nobody can access the network without the knowledge of APN credentials.

M!DGE/MG102i units can also be used **jointly with our UHF/VHF** routers RipEX. The network made up of RipEX radios works within a private frequency range and is very secure and robust. The RipEX network can be used in places where 99.9% reliability is required. On the other hand, you can add some M!DGE/MG102i units to your existing RipEX network here and there where it wouldn't be essential to have RipEX radio coverage, e.g. one very remote location, but with a good cellular signal.

M!DGE/MG102i can be a good option as a **backup to your existing WAN** connectivity. If this connectivity fails, our router can serve as a backup internet access via the cellular network and as soon as the primary connection is fixed, it's activated again. With MG102i, you can use two different SIM cards and if one connection fails, the second can serve as a backup solution.

Our routers are equipped with the serial interface RS232 and two Ethernet ports (MG102i has five Ethernet ports) so your application can use both of them simultaneously. Within the RS232 interface, we support recognizing individual protocols (**Protocol server**) such as IEC101, Modbus and others so you can route the packets based on their serial protocol's addresses.

Both routers also support **redundancy** solutions so you are safe in unlikely case of any HW failure. We can check the connectivity status and switch between connections very fast. Both routers are fully compatible with each other.

1. Overview of Typical MIDGE/MG102i Applications

This chapter is intended to be a brief overview of typical GSM applications. If noted, a detailed example with all configuration steps is given. If there is anything missing or is unclear, do not hesitate to contact technical department for details via the support@racom.eu e-mail address.



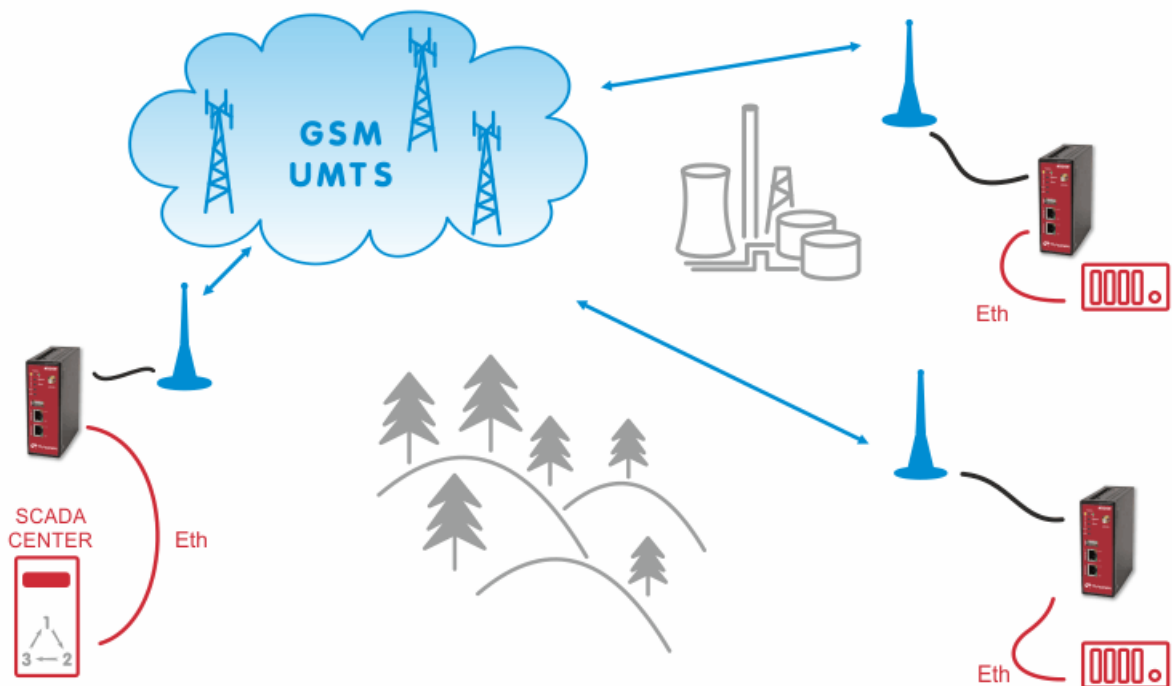
Note

While the terms “SCADA center” and “RTU” are used in the following pictures, any other device (ATMs, lottery terminals, surveillance cameras, etc.) with the same interface type (RS232, ETH) can be used.

1.1. A Standalone MIDGE/MG102i in the Center

This simple and easy solution is feasible for small networks with up to about 20 MIDGE/MG102i units. Note that the center reliability in this arrangement is limited by the reliability of the GPRS/UMTS/HSPA service in the central location.

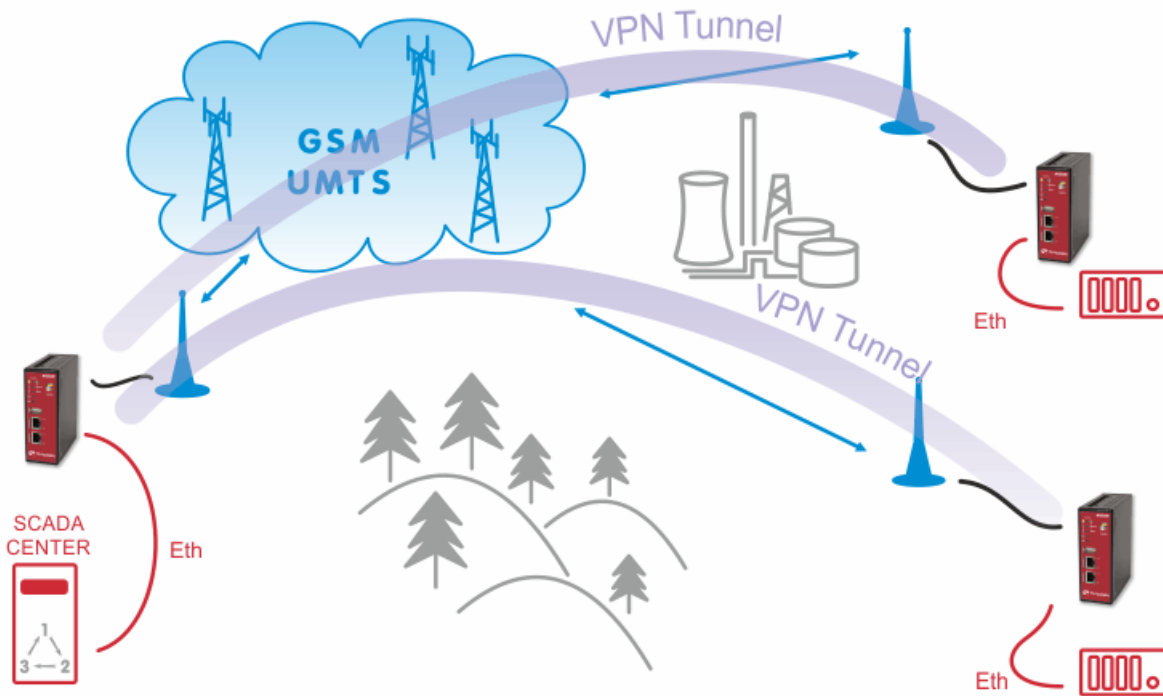
1.1.1. Central MIDGE/MG102i – without VPN tunnels



This solution is possible if

1. you have your own APN within the defined private IP subnet.
2. all the units within the general “internet” APN have public IP addresses which are given statically or dynamically (usage of Dynamic DNS is a must in this case).

1.1.2. Central MIDGE/MG102i – with VPN tunnels



The central unit must be reachable from all clients. The central unit must have the public IP address which can either be static or dynamic. In case of dynamic IP address, the dynamic DNS functionality has to be configured and enabled.

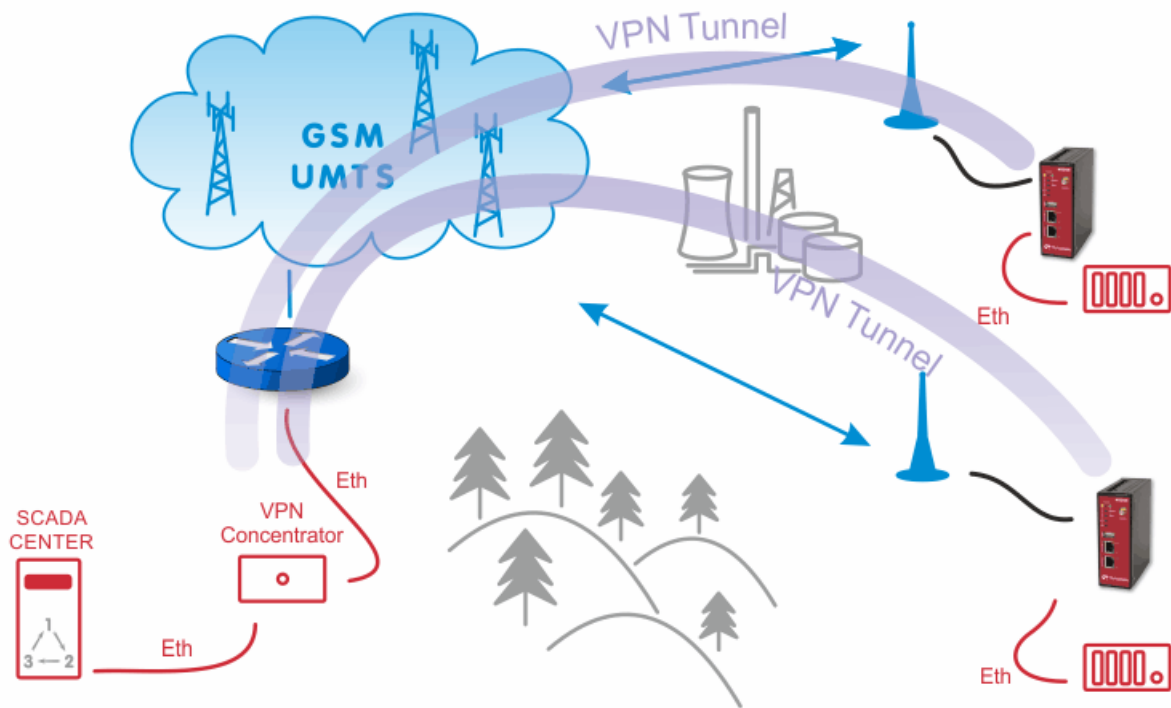
The clients can have static or dynamic IP address even within the private range, thus not reachable from “Internet”. After establishing the VPN tunnel with the server, the subnets between the server and clients are reachable as required.

VPN Tunnels have to be initialized from remotes to the center. The MIDGE/MG102i in the center is capable to simultaneously handle up to 10 OpenVPN tunnels (or up to 25 with Server feature key) and 4 IPsec tunnels. This means that up to 25 remote units are possible for the first application and other four units for the second application.



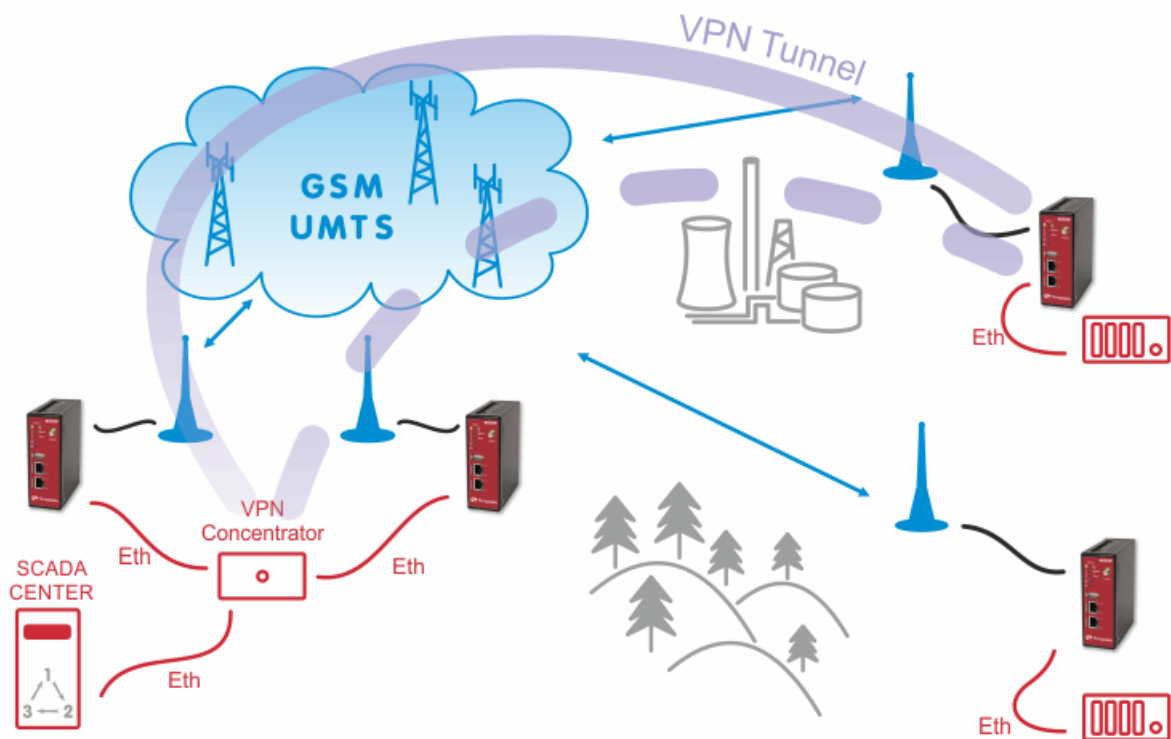
Note

VPN tunnels bring some additional overhead which causes higher data volume. Keep this in mind if paying to the service provider per data volume and not a fixed sum of money.



When a higher number of tunnels (i.e. a higher number of remote units) is required, VPN concentrator has to be used – a special router (e.g. CISCO) for IPsec tunnels or an ordinary PC (Linux/Windows) for OpenVPN tunnels.

1.1.3. Redundant MIDGE/MG102i – VPN tunnels only



Two MIDGE/MG102i units with Virtual Router Redundancy Protocol (VRRP) functionality can be used. The VRRP creates one virtual IP address for both units and this IP address is active for the local LAN. Two independent SIM cards (one in each unit) are used for obtaining public mobile IP addresses. The OpenVPN tunnel is the recommended tunnel type.

In the picture above, there is an additional VPN concentrator as a VPN server. We can also use MIDGE units to be the OpenVPN servers and configure clients to connect to one of them primarily and use the second one as a backup solution.

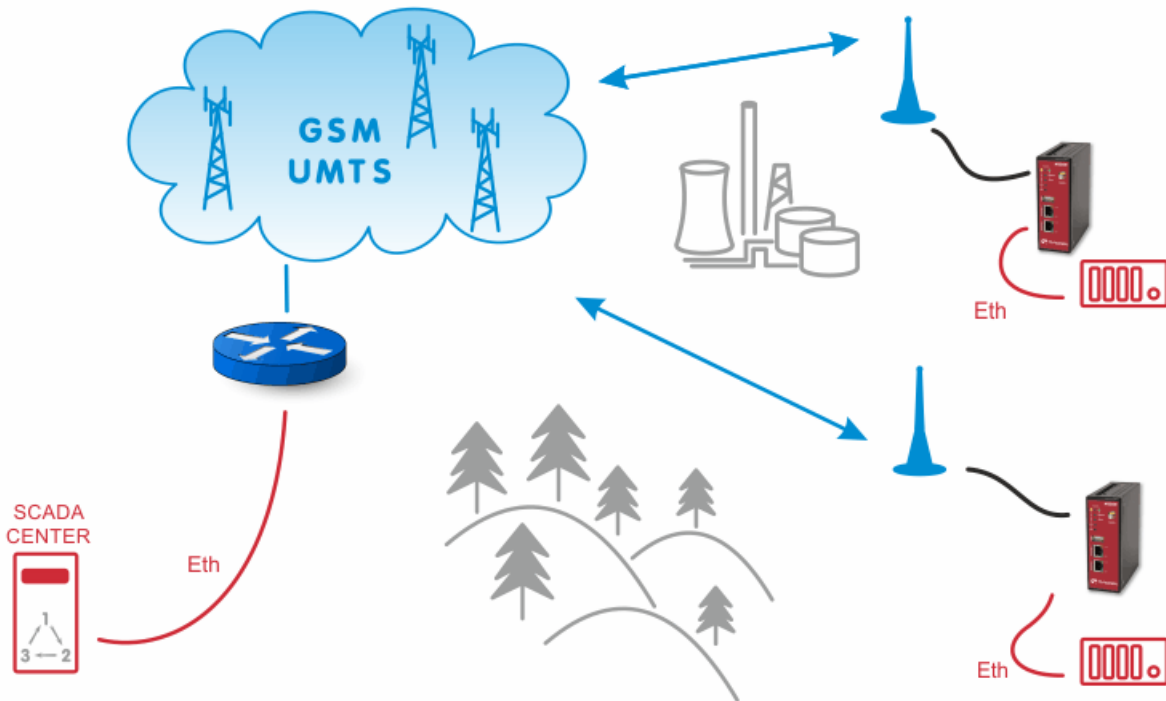
[nový obrázek, kde nebude VPN concentrator – tam bude místo toho switch. A u MIDGE jednotek bude VPN server (primary, backup).

This solution increases the hardware reliability of the center. A redundant VPN concentrator (cluster) solution may be used to further improve the reliability. However a leased line to the GSM operator center is more reliable solution and it is recommended whenever the reliability of the network really matters.

1.2. A leased line to the Cellular Network Center

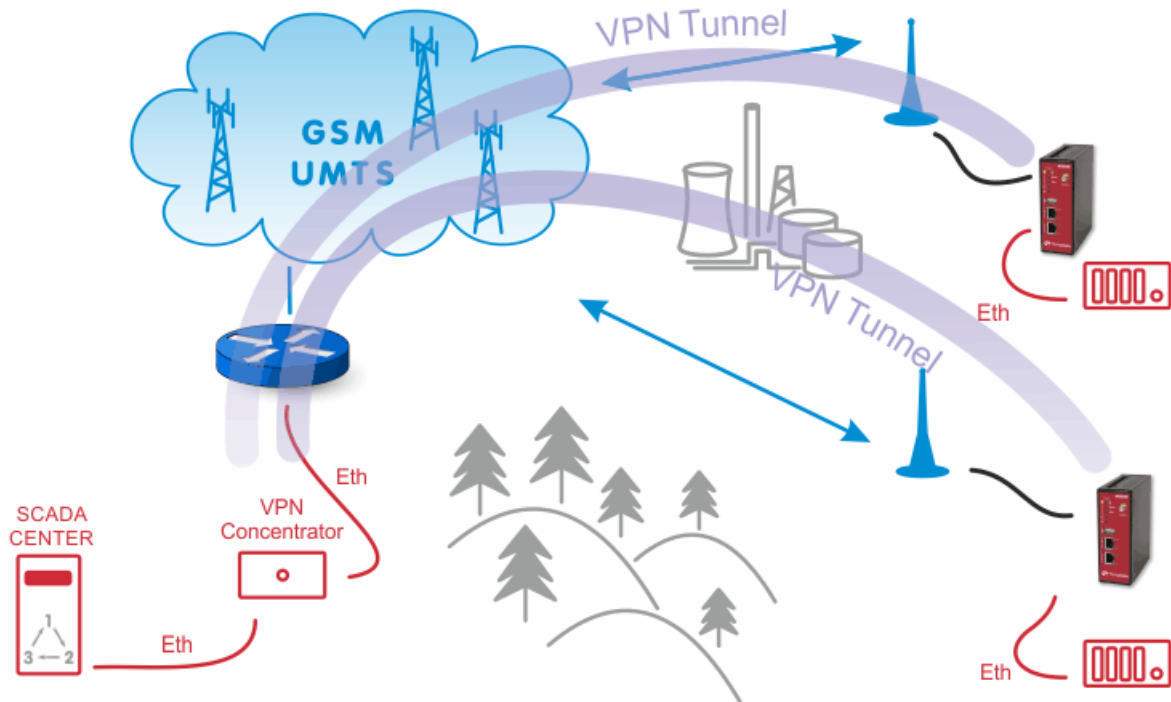
This scenario is feasible for networks with any number of remote sites. A leased line generally provides a better reliability than a wireless cellular connection and its capacity is not limited by the GSM technology available at the center location. The leased line connects the SCADA center directly to the operator's CORE WAN. Sometimes it can be substituted by an Internet connection between the SCADA center and the operator's center.

1.2.1. Leased Line Connection – without VPN tunnels



The solution is the same as in Section 1.1.1, "Central MIDGE/MG102i – without VPN tunnels". The only difference is that we do not have MIDGE/MG102i in the center.

1.2.2. Leased Line Connection – with VPN tunnels

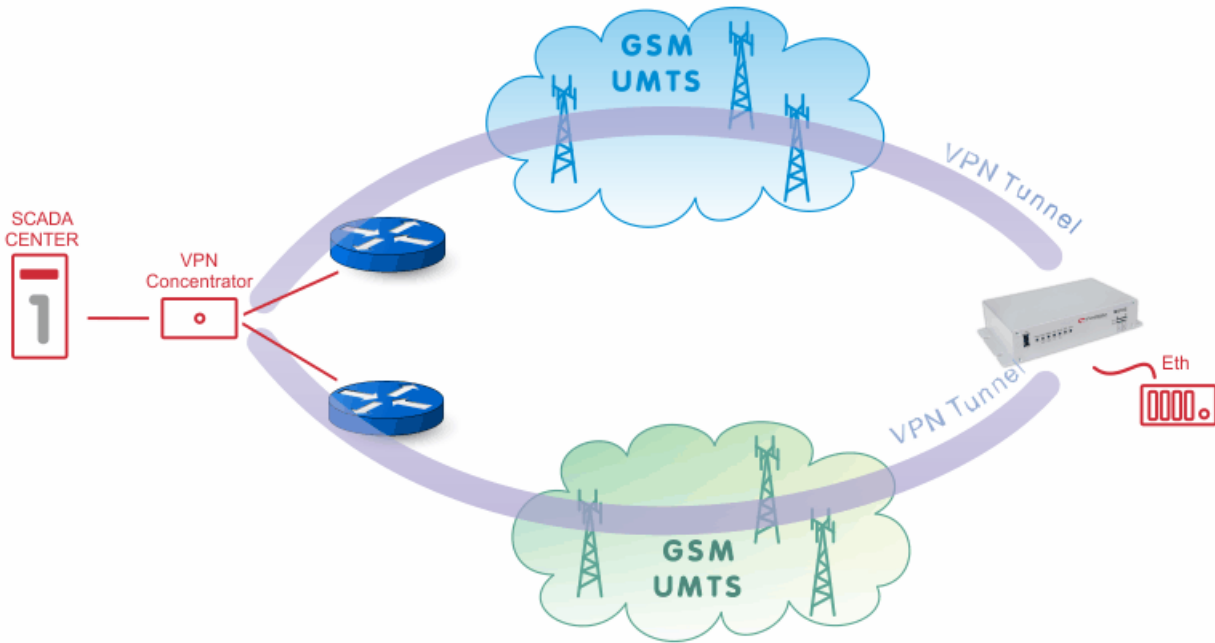


The solution is the same as in Section 1.1.2, “Central M!DGE/MG102i – with VPN tunnels”. The only difference is that we do not have M!DGE/MG102i in the center, but there is a dedicated VPN concentrator which can handle more than 25 clients simultaneously (e.g. CISCO). The redundant VPN concentrator (cluster) may be used for higher reliability.

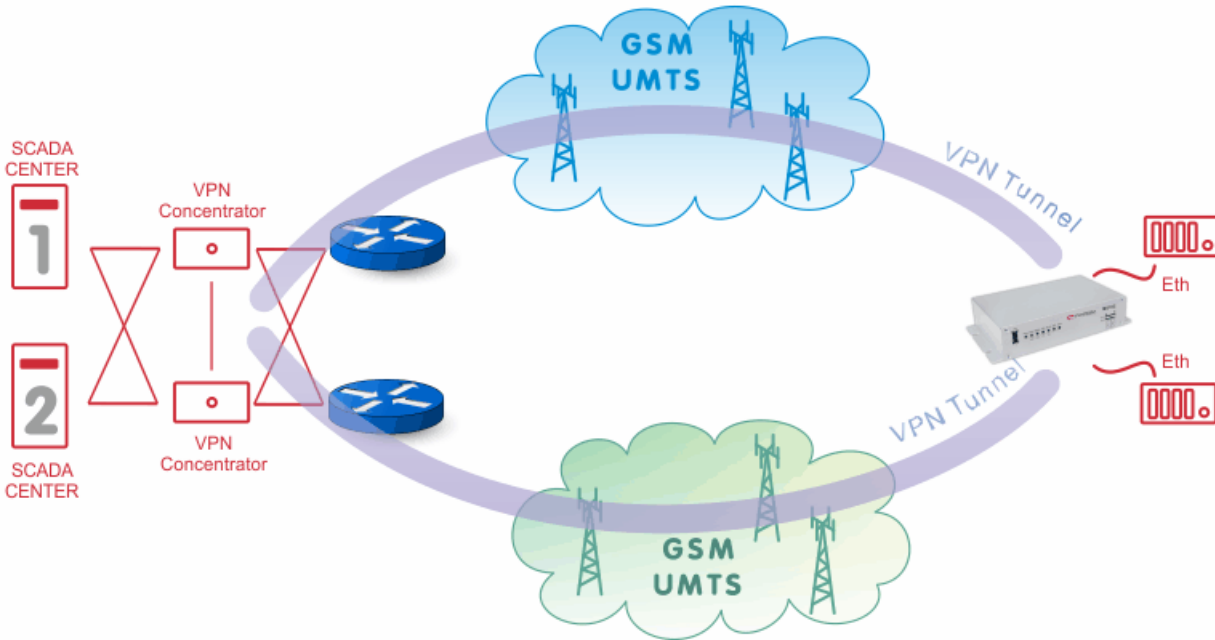
1.2.3. Redundant Connection of Remote Units using two different GSM providers

With a MG102i dual-SIM cellular router, we can use two SIM cards. If the primary provider network fails, the traffic is automatically switched to the second provider.

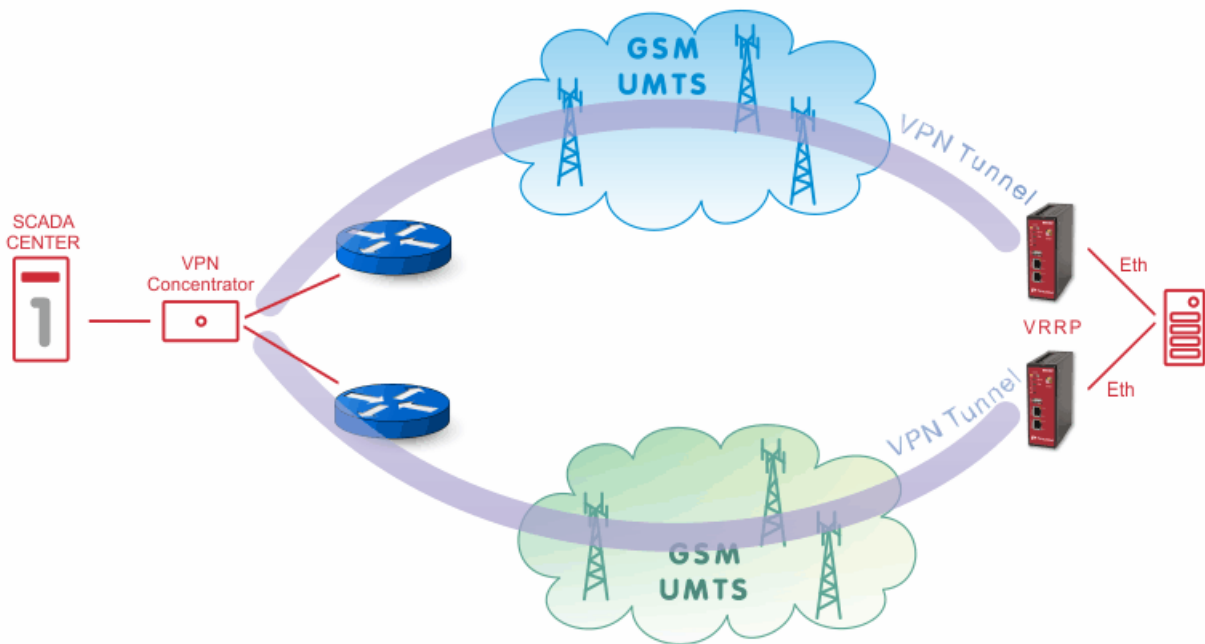
Even with a single provider, two independent Access Point Names (APN) can be used to improve overall reliability.



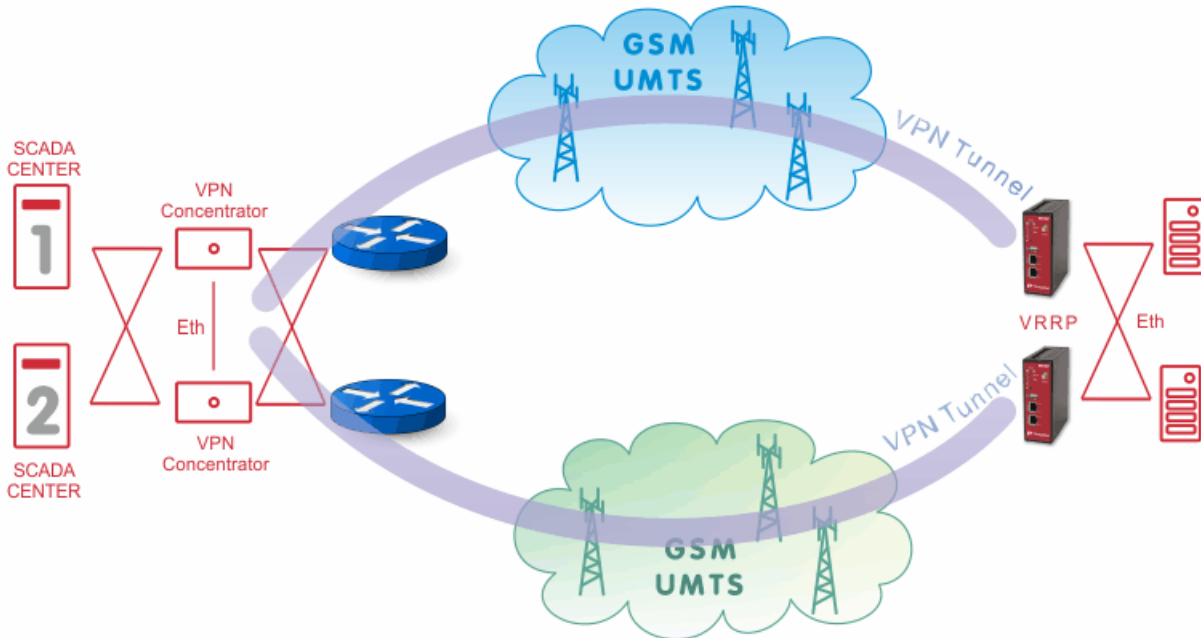
The fully redundant solution of the center is possible as follows:



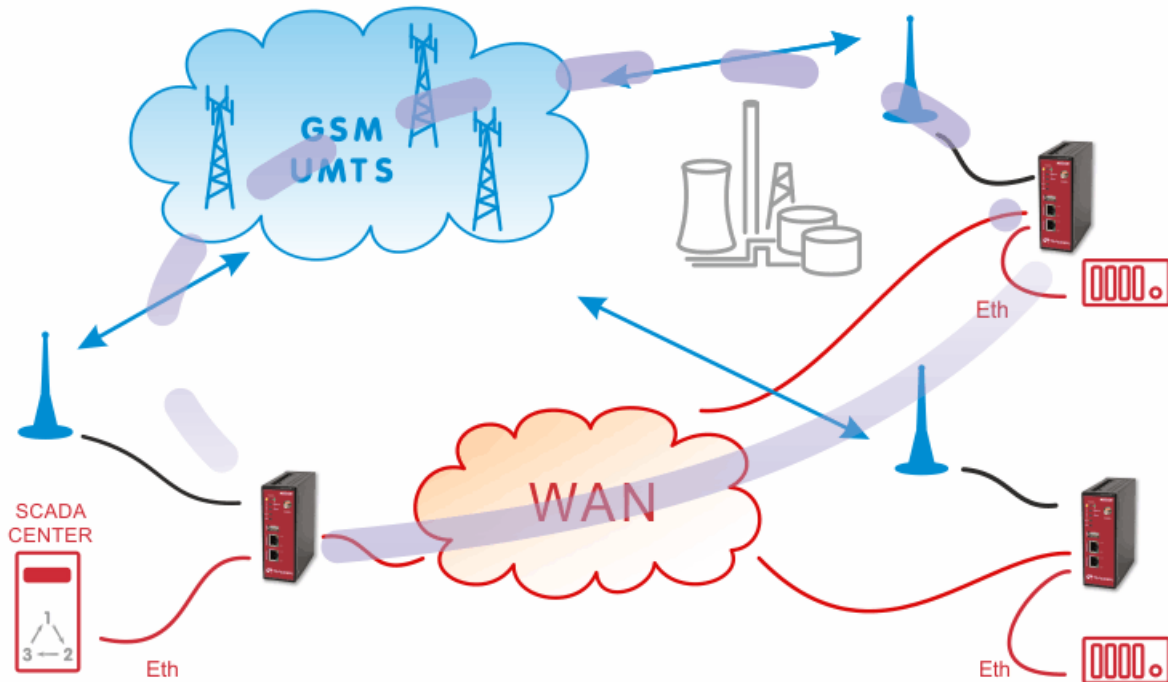
Remote redundancy with two M!DGE/MG102i units with VRRP activated – this solution can handle both the network service failure and the M!DGE/MG102i router (+ antenna installation) HW fault:



A fully redundant solution for both the center and remote locations is certainly possible:



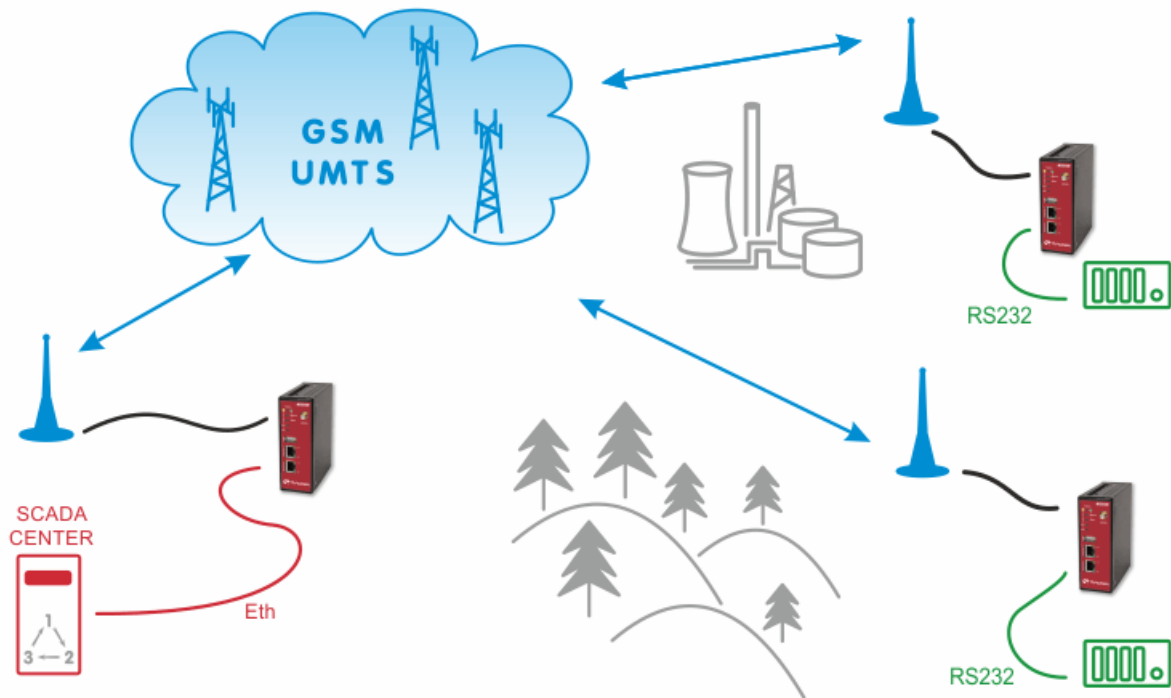
1.3. Backup of WAN by GSM Network



Under usual circumstances, VPN tunnels between remote and central M!DGE/MG102i units are established over the WAN network. When the WAN fails, the traffic from/to the respective remote M!DGE/MG102i is automatically redirected to the cellular network.

1.4. Serial Port SCADA Protocols in GSM Network

SCADA protocols (IEC101, Modbus, ...) on the serial interface (RS232) use proprietary addressing. Since IP addresses have to be used in the cellular network, a translation between the SCADA addresses and IP addresses is required.



MIDGE/MG102i has several ways how to handle the serial traffic. The preferred one is using the **Protocol Server** functionality. This feature is the same as in RipEX modems and it is a proprietary implementation of SCADA addresses to/from IP addresses translation. Thanks to this feature, point-to-multipoint, multi-master or basic point-to-point SCADA applications are possible to handle within GSM network without the need of any additional device. Details in Chapter 4, *SCADA Serial Protocols over GSM Network*.

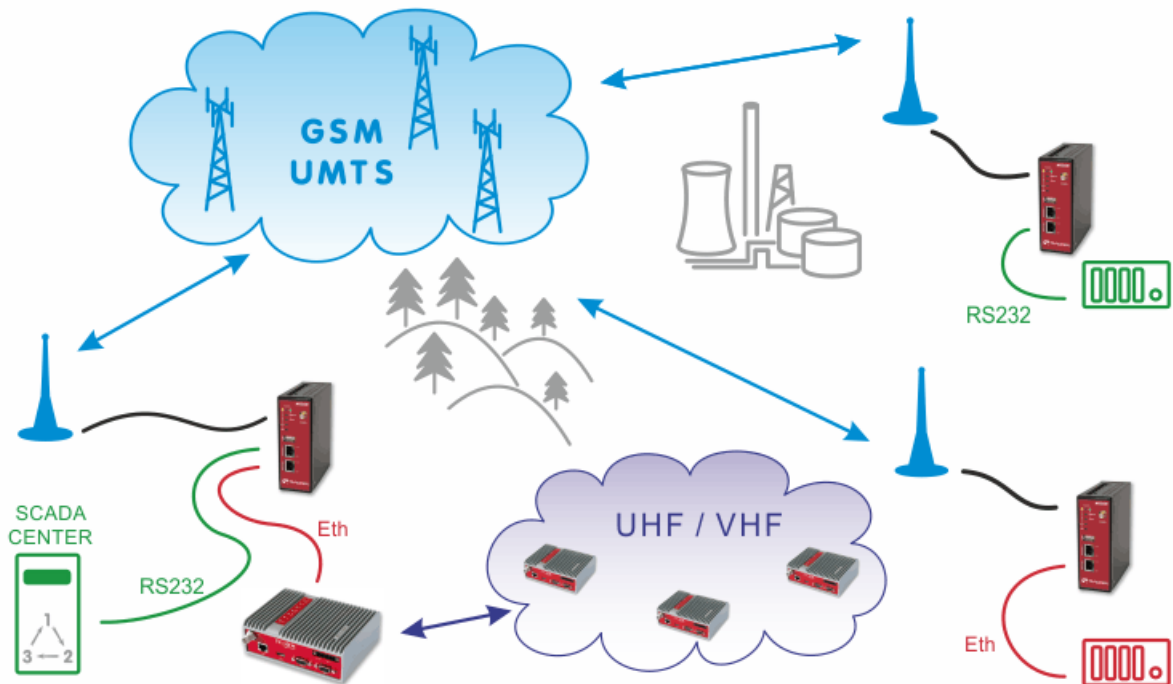
Another possible way is to configure **TCP or UDP server** which does not recognize individual serial protocols, but is capable to handle simple applications. Both implementations can be modified by the end-user to suit individual needs. This can be done via SDK programming which resembles very basic C programming. Using hostnames instead of IP addresses is possible in both options.



Note

The arrangements described in Section 1.1, “A Standalone MIDGE/MG102i in the Center” and Section 1.2, “A leased line to the Cellular Network Center” also apply to the serial SCADA protocols, but the DNS hostnames cannot be used with the Protocol Server feature, only with TCP/UDP Server.

1.5. GSM and UHF/VHF Radio Data Network Combination



The picture above describes an arrangement, where part of the remote sites is connected over a private UHF/VHF radio network (e.g. sites requiring 99.9% availability) and the remaining sites are connected over the cellular public network (e.g. distant, isolated locations where it would be uneconomical to extend the radio coverage to).

2. VPN Configuration Options

M!DGE/MG102i units support several VPN types. Based on your application, number of clients, topology and other factors, the most suitable option should be selected.

RACOM recommends using either **OpenVPN** or **IPsec**. Both are very secure and robust solutions. IPsec is very common for point-to-point tunneling or it's typically used with some bigger VPN concentrator such as CISCO. OpenVPN is very common for interconnecting large environments and M!DGE/MG102i can serve as the VPN server for up to 25 clients. If higher number of clients is required, a special VPN concentrator needs to be installed.



Note

A special software feature key (Server extension) must be ordered to provide the support for 25 OpenVPN clients. Our routers support up to 10 OpenVPN clients without this key.

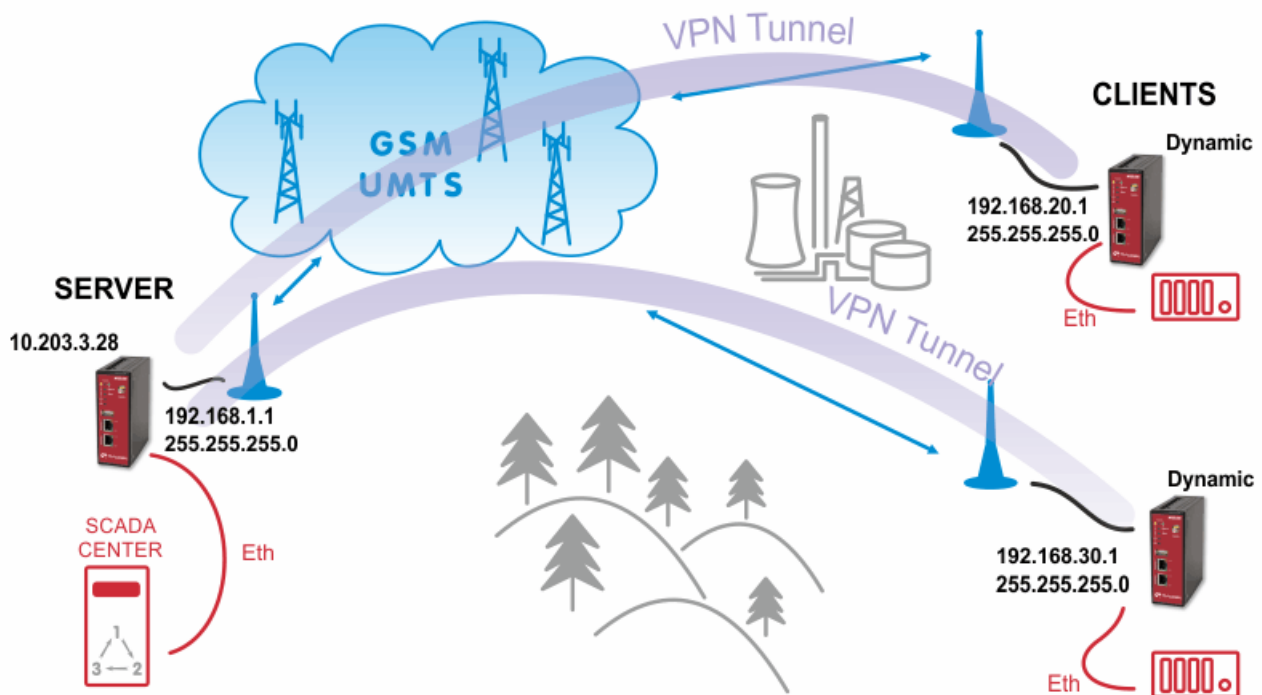
PPTP is a very common solution, usually for connecting Windows PC to the M!DGE/MG102i, but should be used only if other options are not possible. The PPTP security algorithms have already been broken and it's not as secure as IPsec or OpenVPN. **GRE** tunnel is useful for routing subnets among the units, because it also creates a special "greX" interface and it's possible to define as many routes as needed. Keep in mind that GRE is not encrypted, the packets are just wrapped into the GRE header and they can be easily eavesdropped. These notes are not issues of RACOM, but they come from general implementation of those protocols.

See the following examples for details.

2.1. OpenVPN

The OpenVPN tunnel can be operated in two modes – either in the Routed mode or in the Bridged mode. If the VPN network consists of one subnet only, the bridged mode should be used. The whole network seems to be just bridged within the local switches. If you need to interconnect several networks/subnets, you need to utilize the Routed mode. See the detailed examples below.

2.1.1. OpenVPN – Routed mode



Static IP addresses are required for all SIM cards.

OpenVPN Server Configuration

The first step is configuring the Server. Make sure you are connected to the GSM network and so you have the WAN interface active.



Note

You can also use the Ethernet interface as a WAN interface.

M!DGE **RACOM**

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

WWAN1

Description	Value
Administrative state	enabled
Operational state	up
Link is up since	2015-05-04 10:47:35
Modem	Mobile1
SIM	SIM1 (ready)
Signal strength	-91 dBm (medium)
Registration status	registeredInHomeNetwork
Service type	HSPA
Network	O2 - CZ (Cell E751860)
IP address	10.203.3.28
Gateway	10.64.64.64
Transfer rate down / up	1.48 Kbit/s / 12.21 Kbit/s
Data downloaded / uploaded	513.71 KB / 4.74 MB Reset

Fig. 2.1: Server WAN status

With OpenVPN, it is required to have a correct time. One possibility is to set the NTP server synchronization. Go to the **SYSTEM – Time & Region** menu and configure the unit with a reachable NTP server.

M!DGE **RACOM**

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

System Time

Current system time: Set time

Time Synchronisation

NTP server 1: (circled in blue)

NTP server 2 (optional):

Time zone

Time zone: v

Daylight saving changes:

Apply Sync

Fig. 2.2: NTP synchronization

When you are successfully connected and the time is correct, start configuring the OpenVPN server. The default values can be used or read the manual for parameter descriptions.

HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT

Tunnel 1 | Tunnel 2 | Tunnel 3 | Tunnel 4

OpenVPN Tunnel 1 Configuration

Operation mode: disabled **server** **standard** client expert

Server port:

Type: **TUN** GRE

Protocol:

Network mode: **routed** bridged MTU:

Cipher:

Authentication:

HMAC digest:

Options: use compression redirect gateway use keepalive

Fig. 2.3: OpenVPN Server Configuration

After applying the configuration, the certificates need to be created. Click on the given link or go to the **SYSTEM – Keys & Certificates** menu.

Authentication:

HMAC digest:

root certificate, server certificate and server key are missing
[Manage keys and certificates](#)

Fig. 2.4: Missing certificates

In this menu, create the certificates. By default, the Action is set to “generate locally”, but you can also upload the certificates or enroll them via SCEP.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

System
Settings
Time & Region
Reboot

Authentication
Authentication
User Accounts
Remote Authentication

Software Update
Software Update
Firmware Update
Software Profiles

Configuration
File Configuration

OpenVPN1

The certificates used for authenticating OpenVPN Tunnel 1 running in server mode

CA certificate	missing
Server certificate	missing
Server key	missing

Action:

X.509 attributes: C=CZ, ST=Czech Republic, L=Czech Republic, O=RACOM, OU=Networking, CN=MIDGE/emailAddress=support@racom.eu

Fig. 2.5: Creating certificates

**Note**

If needed, the Certificates can be configured to contain specific Organization, Country, e-mail, etc. in the **SYSTEM – Keys & Certificates – Configuration** menu.

See the following example where the certificates are created.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

System
Settings
Time & Region
Reboot

Authentication
Authentication
User Accounts
Remote Authentication

Software Update
Software Update
Firmware Update
Software Profiles

Configuration
File Configuration
Factory Configuration

Troubleshooting
Network Debugging
System Debugging
Tech Support

Keys & Certificates

Licensing











Legal Notice

OpenVPN1

The certificates used for authenticating OpenVPN Tunnel 1 running in server mode

CA certificate	installed	view
Server certificate	installed	view
Server key	installed	view

Client Certificates

Name	Status	
OpenVPN1 Client1	missing	
OpenVPN1 Client2	missing	
OpenVPN1 Client3	missing	
OpenVPN1 Client4	missing	
OpenVPN1 Client5	missing	
OpenVPN1 Client6	missing	
OpenVPN1 Client7	missing	
OpenVPN1 Client8	missing	
OpenVPN1 Client9	missing	
OpenVPN1 Client10	missing	

Action:

X.509 attributes: C=CZ, ST=Czech Republic, L=Czech Republic, O=RACOM, OU=Networking, CN=MIDGE/emailAddress=support@racom.eu

Fig. 2.6: Created OpenVPN certificates

In the same menu, you can generate or upload certificates for individual clients or go back to the OpenVPN – Client Management menu, configure required hosts and the certificates will be locally created automatically after downloading the Expert mode file.



HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT

Clients | Networking | Routes | Download

Client Management

Enabled	Client	Connection info
<input checked="" type="checkbox"/>	midge1	not connected
<input checked="" type="checkbox"/>	midge2	not connected
<input type="checkbox"/>	Client3	
<input type="checkbox"/>	Client4	
<input type="checkbox"/>	Client5	
<input type="checkbox"/>	Client6	
<input type="checkbox"/>	Client7	
<input type="checkbox"/>	Client8	
<input type="checkbox"/>	Client9	
<input type="checkbox"/>	Client10	

Apply Refresh

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

Fig. 2.7: OpenVPN Clients

In the Networking menu, you can define the clients' networks or leave it empty. Each client can have its own network/mask. In our example, configure the network 192.168.20.0/24 for midge1 and 192.168.30.0/24 for midge2. The tunnel address can be dynamic.

HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT

Clients Networking **Routes** Download

Transport Network

Network:

Netmask:

Client Networks

This menu can be used to configure a fixed tunnel endpoint address for each client. You may also specify a network whose packets should get routed towards the client.

Select client:

Tunnel address:

dynamic

fixed

Client network:

none specify

Network:

Netmask:

Fig. 2.8: OpenVPN Networking (Client1 example)

In the Routes menu, you can add networks which will be pushed into all clients' Routing menu so that matching packets will be routed back to the server. Routing between the clients can be enabled too. Fill in the Server's IP subnet 192.168.1.0/24.

HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT

Clients Networking **Routes** Download

Client Routes

This list of network routes will be pushed to each client, so that matching packets will be routed back to the server.

Network	Netmask
<input type="text" value="192.168.1.0"/>	<input type="text" value="255.255.255.0"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

Enable routing between clients:

Fig. 2.9: OpenVPN Routes (Server's subnet)

Another step is to download the Expert file for all the configured clients. Fill in the server's IP address which can be different in your case (the IP address depends on your APN configuration).

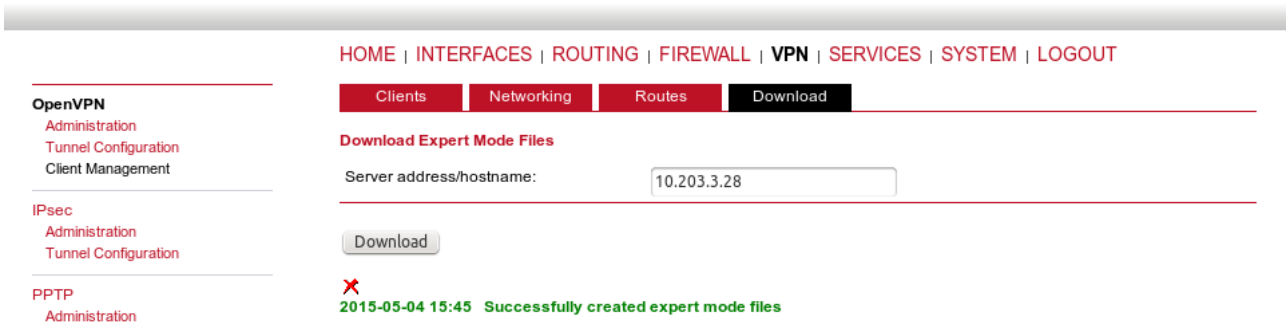


Fig. 2.10: OpenVPN downloading Expert file

The last step is Enabling the OpenVPN server.

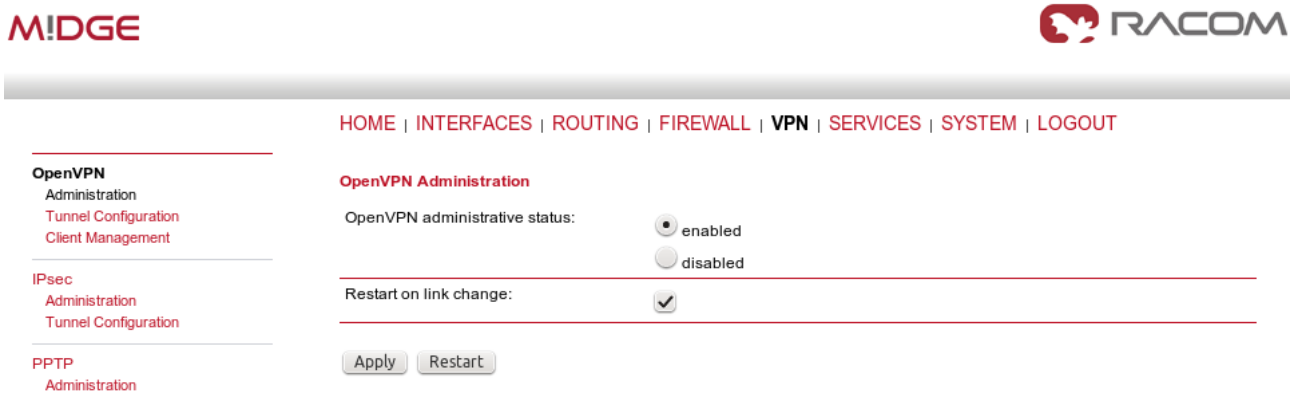


Fig. 2.11: Enabling OpenVPN server

The OpenVPN server configuration is now complete. The server is running and listening for all VPN clients.

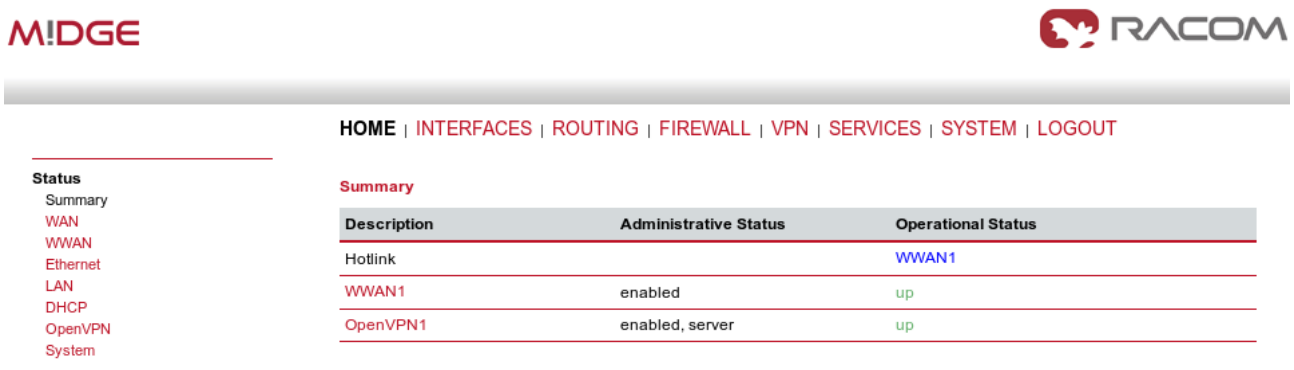


Fig. 2.12: OpenVPN server is running

OpenVPN Client Configuration

The easiest way how to configure the client is to upload the Expert file downloaded from the server. Unzip the file to obtain Expert files for individual clients.

Configure the APN on both clients and set the correct NTP server for time synchronization. Afterwards, go to the OpenVPN menu and upload the expert file.

HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT

Tunnel 1 | Tunnel 2 | Tunnel 3 | Tunnel 4

OpenVPN Tunnel 1 Configuration

Operation mode: disabled client server standard expert

Network mode: routed bridged

Expert mode file: midge1.zip

Fig. 2.13: OpenVPN client configuration (midge1)

The Expert mode file should be installed. Now, enable the OpenVPN client and check the VPN status.

HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT

OpenVPN Status

Administrative status: enabled

Name	Type	Peer	Address	Status
Tunnel1	client	10.203.3.28	10.8.0.6	up

Fig. 2.14: OpenVPN client – connected successfully

Testing OpenVPN tunnel

On both the client and the server, you should see the updated Routing menu. There is a new TUN interface. See the Server's Routing menu.

- Static Routes
- Extended Routes
- Multipath Routes
- Mobile IP Administration
- QoS Administration
- QoS Classification

Static Routes

This menu shows all routing entries of the system, they can consist of active and configured ones. The flags are as follows: (A)ctive, (P)ersistent, (H)ost Route, (N)etwork Route, (D)efault Route (Netmasks can be specified in CIDR notation)

Destination	Netmask	Gateway	Interface	Metric	Flags
0.0.0.0	0.0.0.0	10.64.64.64	WWAN1	0	AD
10.8.0.0	255.255.255.0	10.8.0.2	TUN1	0	AN <input checked="" type="checkbox"/>
10.8.0.2	255.255.255.255	0.0.0.0	TUN1	0	AH <input checked="" type="checkbox"/>
10.64.64.64	255.255.255.255	0.0.0.0	WWAN1	0	AH
192.168.1.0	255.255.255.0	0.0.0.0	LAN1	0	AN
192.168.2.0	255.255.255.0	0.0.0.0	LAN2	0	AN
192.168.20.0	255.255.255.0	10.8.0.2	TUN1	0	AN <input checked="" type="checkbox"/>
192.168.30.0	255.255.255.0	10.8.0.2	TUN1	0	AN <input checked="" type="checkbox"/>

Route lookup

Fig. 2.15: OpenVPN Routing

You can define new routes in the Routing menu manually, just choose the correct TUN interface. Note that adding routes this way is not possible with the Bridged tunnel type or with IPsec.

Check the reachability of remote network by issuing the PING command from the SYSTEM – Troubleshooting – Network Debugging menu. Ping the remote M!DGE Ethernet IP address or you can even try to ping a device behind the remote M!DGE. In the example below, a ping from the server to the client is displayed.

- System
 - Settings
 - Time & Region
 - Reboot
- Authentication
 - Authentication
 - User Accounts
 - Remote Authentication
- Software Update
 - Software Update
 - Firmware Update
 - Software Profiles
- Configuration
 - File Configuration
 - Factory Configuration
- Troubleshooting
 - Network Debugging
 - System Debugging
 - Tech Support

Network Debugging

- ping
- tracert
- tcpdump
- darkstat

```
PING 192.168.20.1 (192.168.20.1): 40 data bytes
48 bytes from 192.168.20.1: seq=0 ttl=64 time=1479.866 ms
48 bytes from 192.168.20.1: seq=1 ttl=64 time=738.485 ms
48 bytes from 192.168.20.1: seq=2 ttl=64 time=498.122 ms
48 bytes from 192.168.20.1: seq=3 ttl=64 time=497.766 ms
48 bytes from 192.168.20.1: seq=4 ttl=64 time=497.361 ms

--- 192.168.20.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 497.361/742.320/1479.866 ms
```

Run again

Fig. 2.16: Checking OpenVPN tunnel via ping

2.1.2. OpenVPN – Bridged mode

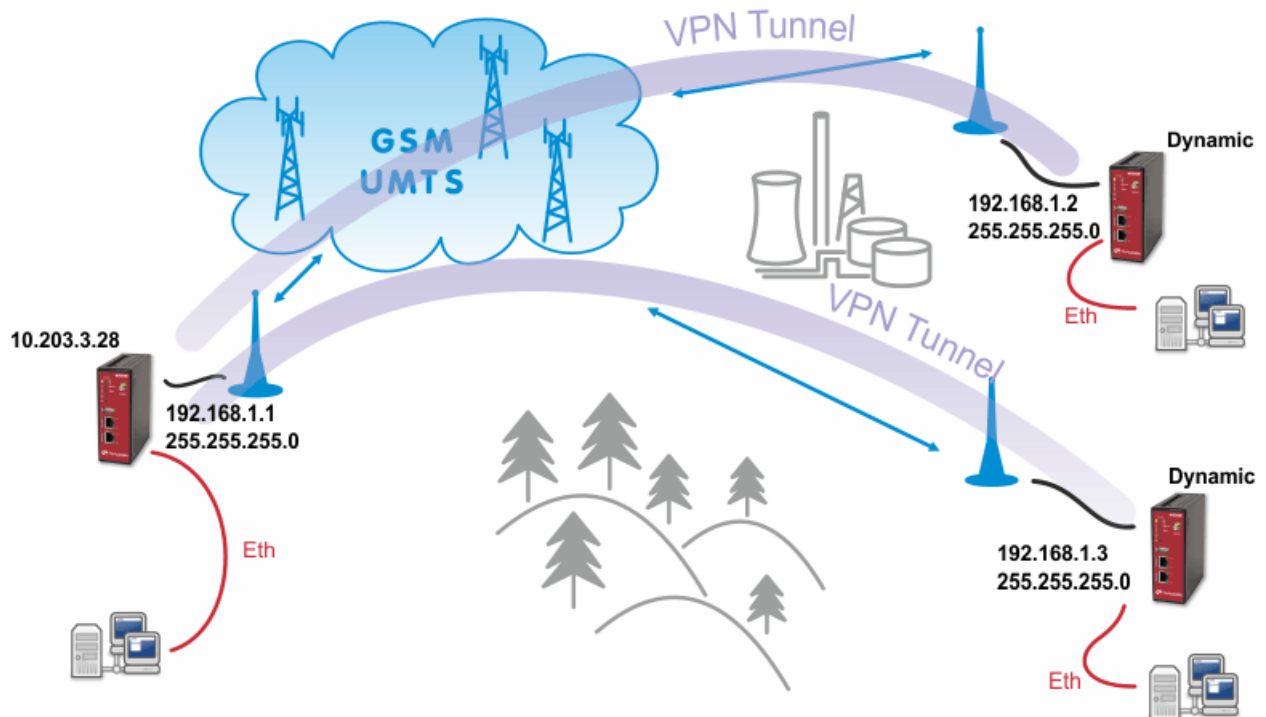


Fig. 2.17: OpenVPN Bridged mode

The Bridge type of the OpenVPN tunnel used when you need to interconnect the devices within one IP subnet so we create “transparent” network. In our example, we will use the 192.168.1.0/24 subnet. The center has the IP address 192.168.1.1. The clients have 192.168.1.2 and .1.3. You can attach any device (e.g. notebook) to any M!DGE so you can test the reachability of not just M!DGE units, but even the connected devices.



Note

Make sure you have the correct IP addresses on all M!DGE units (INTERFACES – Ethernet – IP settings).

OpenVPN Server Configuration

The configuration is very similar to the previous example. In the Tunnel configuration, set the Type to “TAP”, Network mode to “bridged” and select the correct LAN interface.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Tunnel 1 | Tunnel 2 | Tunnel 3 | Tunnel 4

OpenVPN Tunnel 1 Configuration

Operation mode: disabled standard client expert server

Server port:

Type:

Protocol:

Network mode: routed bridged Interface:

Cipher:

Authentication:

HMAC digest:

Options: use compression redirect gateway use keepalive

Fig. 2.18: OpenVPN Server – bridged mode

Create the required certificates and enable two clients in the Management menu. See the details in Section 2.1.1, “OpenVPN – Routed mode”.

The Networking and Routes menus do not require anything to change. We are NOT defining any routes in this mode.

HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT

Clients | **Networking** | Routes | Download

OpenVPN
Administration
Tunnel Configuration
Client Management

IPsec
Administration
Tunnel Configuration

PPTP
Administration
Tunnel Configuration

GRE
Administration
Tunnel Configuration

Dial-in Server

Transport Network

Network:

Netmask:

Client Networks

This menu can be used to configure a fixed tunnel endpoint address for each client. You may also specify a network whose packets should get routed towards the client.

Select client:

Tunnel address:
 dynamic
 fixed

Client network:
 none specify

Fig. 2.19: OpenVPN Networking – bridged mode

HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT

Clients | **Networking** | **Routes** | Download

OpenVPN
Administration
Tunnel Configuration
Client Management

IPsec
Administration
Tunnel Configuration

PPTP
Administration
Tunnel Configuration

GRE
Administration
Tunnel Configuration

Dial-in Server

Client Routes

This list of network routes will be pushed to each client, so that matching packets will be routed back to the server.

Network	Netmask
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

Enable routing between clients:

Fig. 2.20: OpenVPN Routes – bridged mode

Download the Expert file and Enable the tunnel.

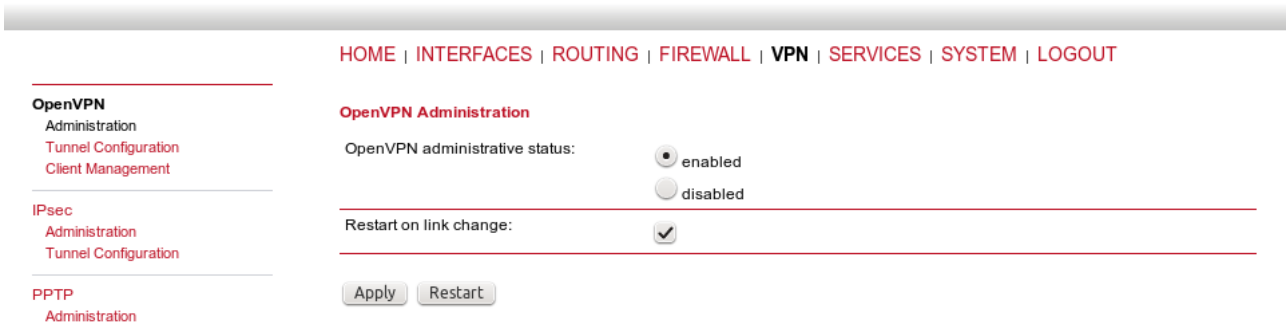


Fig. 2.21: Enabling OpenVPN server

Finally, you check the OpenVPN status in the HOME menu.

OpenVPN Client Configuration

The client's configuration is very simple, just upload the Expert file.



Note

You could, of course, use the Standard Operation mode, but using Expert file is simpler.

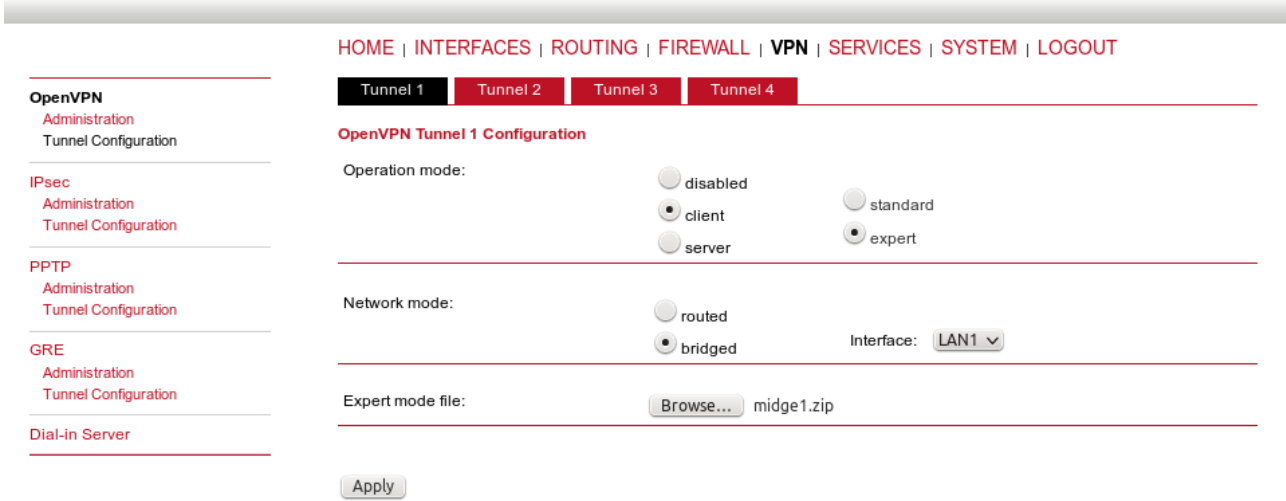


Fig. 2.22: OpenVPN client configuration – bridged mode

Enable the tunnel and check the VPN status.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Status

- Summary
- WAN
- WWAN
- Ethernet
- LAN
- DHCP
- OpenVPN
- Firewall
- System

Summary

Description	Administrative Status	Operational Status
Hotlink		WWAN1
WWAN1	enabled	up
OpenVPN1	enabled, client	up

Fig. 2.23: OpenVPN client HOME menu

Testing OpenVPN tunnel

Test the tunnel using the Ping functionality.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

System

- Settings
- Time & Region
- Reboot

Authentication

- Authentication
- User Accounts
- Remote Authentication

Software Update

- Software Update
- Firmware Update
- Software Profiles

Configuration

- File Configuration
- Factory Configuration

Troubleshooting

- Network Debugging
- System Debugging
- Tech Support

Network Debugging

ping | traceroute | tcpdump | darkstat

```

PING 192.168.1.1 (192.168.1.1): 40 data bytes
48 bytes from 192.168.1.1: seq=0 ttl=64 time=1232.972 ms
48 bytes from 192.168.1.1: seq=1 ttl=64 time=573.181 ms
48 bytes from 192.168.1.1: seq=2 ttl=64 time=481.849 ms
48 bytes from 192.168.1.1: seq=3 ttl=64 time=461.501 ms
48 bytes from 192.168.1.1: seq=4 ttl=64 time=470.749 ms

--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 461.501/644.050/1232.972 ms

```

Run again

Fig. 2.24: Testing OpenVPN (ping from the client to the server)

Remember that there is no route in the Routing menu, because we are using TAP interface instead of TUN.

HOME | INTERFACES | **ROUTING** | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Static Routes

Extended Routes

Multipath Routes

Mobile IP

Administration

QoS

Administration

Classification

Static Routes

This menu shows all routing entries of the system, they can consist of active and configured ones.

The flags are as follows: (A)ctive, (P)ersistent, (H)ost Route, (N)etwork Route, (D)efault Route (Netmasks can be specified in CIDR notation)

Destination	Netmask	Gateway	Interface	Metric	Flags
0.0.0.0	0.0.0.0	10.64.64.64	WWAN1	0	AD
10.64.64.64	255.255.255.255	0.0.0.0	WWAN1	0	AH
192.168.1.0	255.255.255.0	0.0.0.0	LAN1	0	AN
192.168.2.0	255.255.255.0	0.0.0.0	LAN2	0	AN



Route lookup

Fig. 2.25: Routing menu – bridged mode



Note

You can ping among the devices connected via M!DGE units. The link should be transparent and no extra routes are needed on the devices.

```
$ ping -c 5 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=1636 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=1327 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=1477 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=1207 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=1097 ms

--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 1097.632/1349.279/1636.959/191.392 ms, pipe 2
```

OpenVPN is a very powerful tool. If you need to know more about the possible options, use the M!DGE/MG102i manual for more details.

2.2. IPsec

IPsec can be used in a network of any size. A dedicated router (or several routers) serve(s) as the VPN concentrator. The choice of vendor and type depends on the SLA requirements and the size of the network - RACOM has positive experience with Cisco routers (IOS or ASA based), however routers from other vendors (e.g. Juniper, Netgear, WatchGuard or others) can certainly be used.

The following routers were used as IPsec VPN concentrators:

- M!DGE/MG102i – up to 4 tunnels
- Cisco 1700 – up to 100
- Cisco ASA 5510 – up to 250
- Cisco 871-K9 – up to 10 tunnels
- Cisco 1841-HSEC/ K9 – up to 800 tunnels

Please follow the instruction in the user manual of the specific router for IPsec tunnel settings. RACOM support team can assist you with basic settings for Cisco routers. A short description of the IPsec tunnel configuration in M!DGE/MG102i follows.

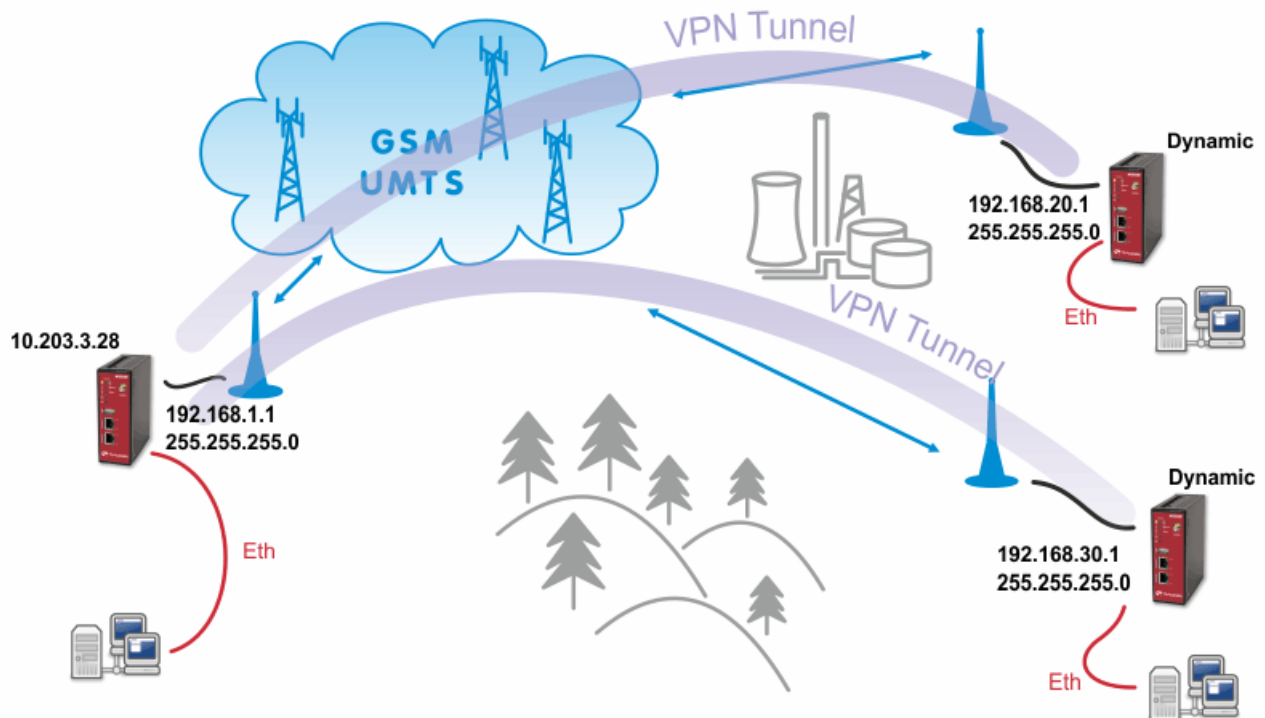


Fig. 2.26: IPsec

The topology is the same as with the routed OpenVPN example. Remember that it is not possible to have a bridged mode of IPsec as it was possible with OpenVPN.

Both remote M!DGE/MG102i units in the example have dynamic mobile IP addresses. We will set the center's peer IP to 0.0.0.0 so it will accept the connections from any IP address.

With IPsec, the most common way to authenticate each other is via a pre-shared key. Due to this, it is not essential to have a correct time using the NTP server.

2.2.1. IPsec Configuration

Server's configuration

Go to the **VPN – IPsec – Tunnel Configuration** menu and create a new tunnel by pressing the “+” sign.

The screenshot shows the M!DGE web interface with the RACOM logo. The breadcrumb navigation is HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT. On the left, there are navigation menus for OpenVPN, IPsec, PPTP, GRE, and Dial-in Server. The main content area is titled 'IPsec Tunnel Configuration' and contains a table with the following columns: Name, Type, Peer, IKE, IPsec, Local Network, and Remote Network. A blue circle with a plus sign is overlaid on the right side of the table, indicating a 'create' button.

Fig. 2.27: Creating IPsec tunnel

In the General tab, fill in 0.0.0.0 into the IP address field. Due to this address, any remote unit can establish the connection with the central unit if the credentials are correct. The remote unit's IP address is not an issue.



Note

From our experience, change the Action to “restart”.

The screenshot shows the M!DGE web interface with the RACOM logo. The breadcrumb navigation is HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT. On the left, there are navigation menus for OpenVPN, IPsec, PPTP, GRE, and Dial-in Server. The main content area is titled 'IPsec Tunnel 1 Configuration' and has four tabs: General, IKE Proposal, IPsec, and Networks. The 'General' tab is active. Under 'Remote Peer', the 'IP address' field contains '0.0.0.0'. Under 'Dead Peer Detection (DPD)', the 'Administrative status' is checked, 'Detection cycle' is 30 seconds, and 'Failure threshold' is 3. The 'Action' dropdown menu is set to 'restart'. An 'Apply' button is at the bottom.

Fig. 2.28: IPsec server's General configuration

Apply the changes and go to the next tab, IKE Proposal. Define any pre-shared key, which must be the same on the center and the remote sites. Fill in the Local and Peer IDs. In our example, FQDNs are used. The central ID is “midge-central” and the ID for the first client is “midge-client1”.



Note

You need to add a second tunnel if you need to connect M!DGE “client2”.

Other parameters can stay in defaults or you can enable PFS for higher security.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

OpenVPN
Administration
Tunnel Configuration

IPsec
Administration
Tunnel Configuration

PPTP
Administration
Tunnel Configuration

GRE
Administration
Tunnel Configuration

Dial-in Server

IPsec Tunnel 1 Configuration

General | **IKE Proposal** | IPsec | Networks

IKE Authentication

Authentication type: pre-shared key

PSK:

Local ID type: Fully Qualified Domain Name (FQDN)

Local ID: midge-central

Peer ID type: Fully Qualified Domain Name (FQDN)

Peer ID: midge-client1

IKE Proposal (Phase 1)

Negotiation mode: main

Encryption algorithm: 3DES

Authentication algorithm: MD5

IKE Diffie-Hellman group: 2 (1024)

SA life time: 86400 (seconds)

Perfect forward secrecy (PFS):

Apply

Fig. 2.29: IPsec central's IKE Proposal tab

After applying the changes, you can leave everything in defaults within the IPsec Proposal tab.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

OpenVPN
Administration
Tunnel Configuration

IPsec
Administration
Tunnel Configuration

PPTP
Administration
Tunnel Configuration

GRE
Administration
Tunnel Configuration

Dial-in Server

IPsec Tunnel 1 Configuration

General | IKE Proposal | **IPsec** | Networks

IPsec Proposal (IKE Phase 2)

Encapsulation mode: Tunnel

IPsec protocol: ESP

Encryption algorithm: 3DES

Authentication algorithm: MD5

SA life time: 28800 (seconds)

Force encapsulation:

Apply

Fig. 2.30: IPsec central's IPsec Proposal tab

In the last tab, define the required routable networks. In our example, we interconnect server's 192.168.1.0/24 subnet with client's 192.168.20.0/24 subnet. Leave the "NAT address" blank.

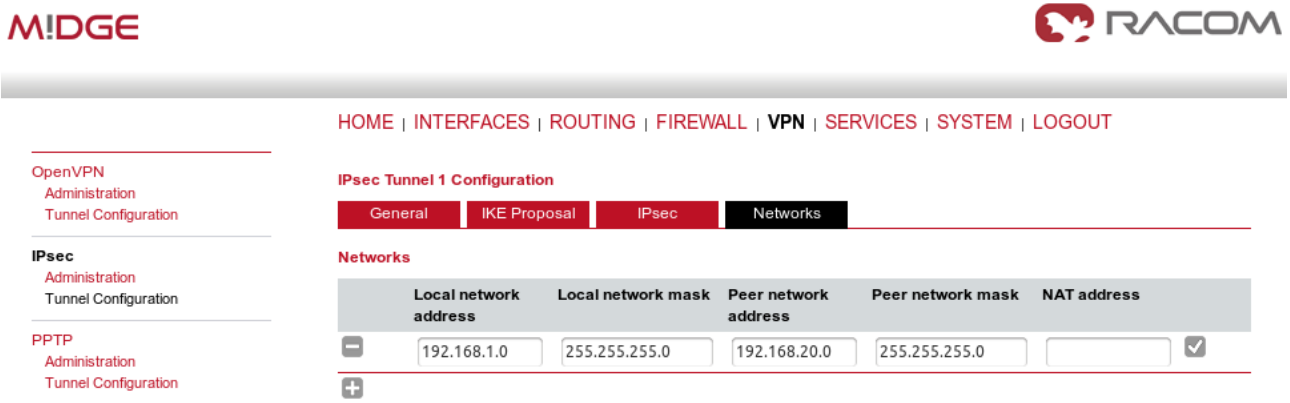


Fig. 2.31: IPsec central's Networks tab

Return back to the Administration menu and enable the tunnel. Check both parameters – Propose NAT traversal and Restart on link change.

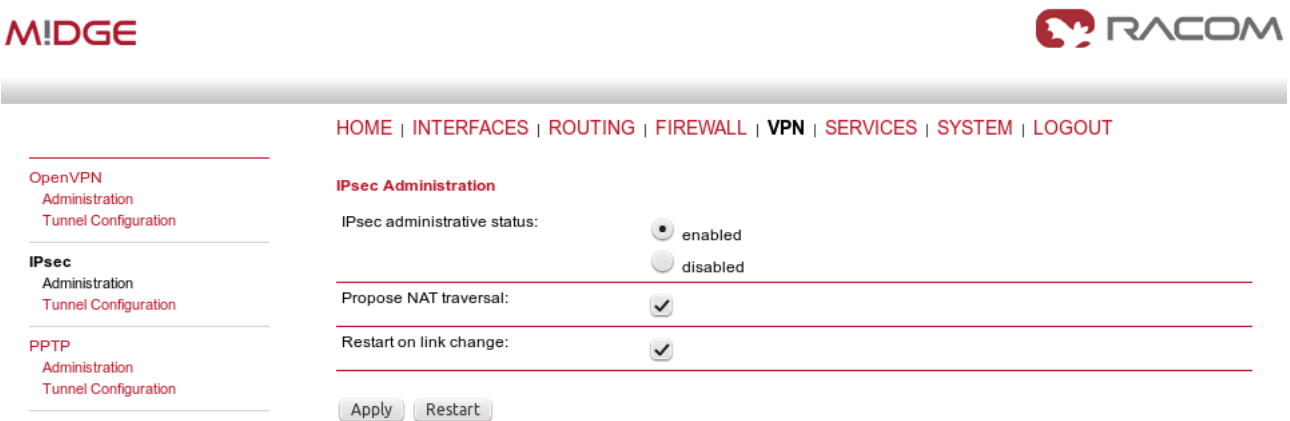


Fig. 2.32: Enabling IPsec tunnel

The pop-up window will appear asking you to confirm the MSS to be decreased due to IPsec overhead. Confirm this change.

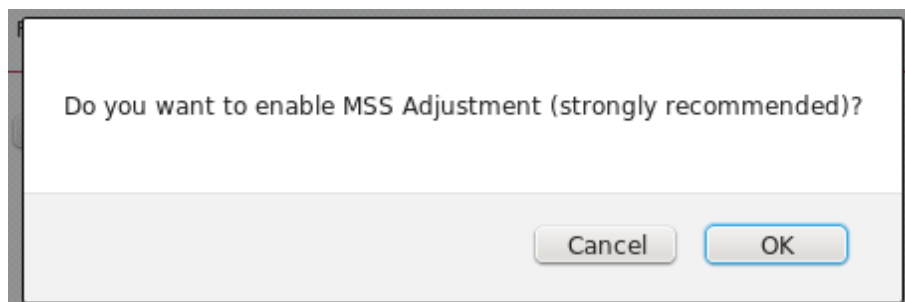


Fig. 2.33: MSS Adjustment

If you now check the tunnel status, it will be “down”, because the client's configuration is not yet finished.

Client's configuration

The client's configuration must follow the server's one. The Peer IP address must be the server's IP address.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

OpenVPN
Administration
Tunnel Configuration

IPsec
Administration
Tunnel Configuration

PPTP
Administration
Tunnel Configuration

GRE
Administration
Tunnel Configuration

Dial-in Server

IPsec Tunnel 1 Configuration

General | **IKE Proposal** | IPsec | Networks

Remote Peer

IP address:

Dead Peer Detection (DPD)

Administrative status:

Detection cycle: (seconds)

Failure threshold:

Action:

Fig. 2.34: Client's IPsec General tab

In the IKE Proposal tab, the PSK must be the same as on the server's side and switch the IDs. Do not forget to enable PFS if checked on the server.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

OpenVPN
Administration
Tunnel Configuration

IPsec
Administration
Tunnel Configuration

PPTP
Administration
Tunnel Configuration

GRE
Administration
Tunnel Configuration

Dial-in Server

IPsec Tunnel 1 Configuration

General | **IKE Proposal** | IPsec | Networks

IKE Authentication

Authentication type:

PSK:

Local ID type:

Local ID:

Peer ID type:

Peer ID:

IKE Proposal (Phase 1)

Negotiation mode:

Encryption algorithm:

Authentication algorithm:

IKE Diffie-Hellman group:

SA life time: (seconds)

Perfect forward secrecy (PFS):

Fig. 2.35: Client's IPsec IKE Proposal

Leave IPsec proposal in defaults and configure the Networks. Just switch the subnets (compared to the central's configuration).

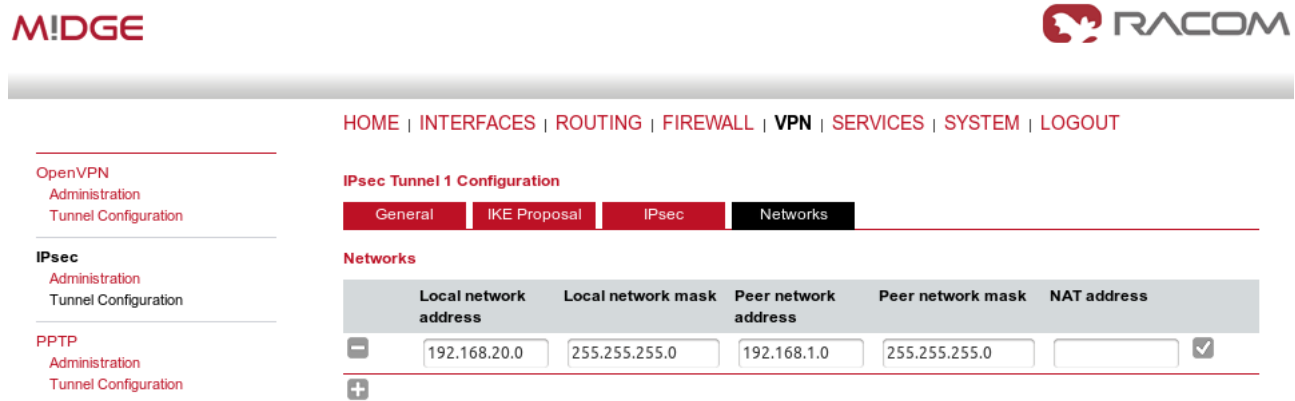


Fig. 2.36: Client's IPsec Networks tab

We can now Enable the tunnel and confirm the MSS adjustment.

After the algorithm completes the tunnel establishment, the tunnel should be marked “up” on both units. Check the HOME menu.

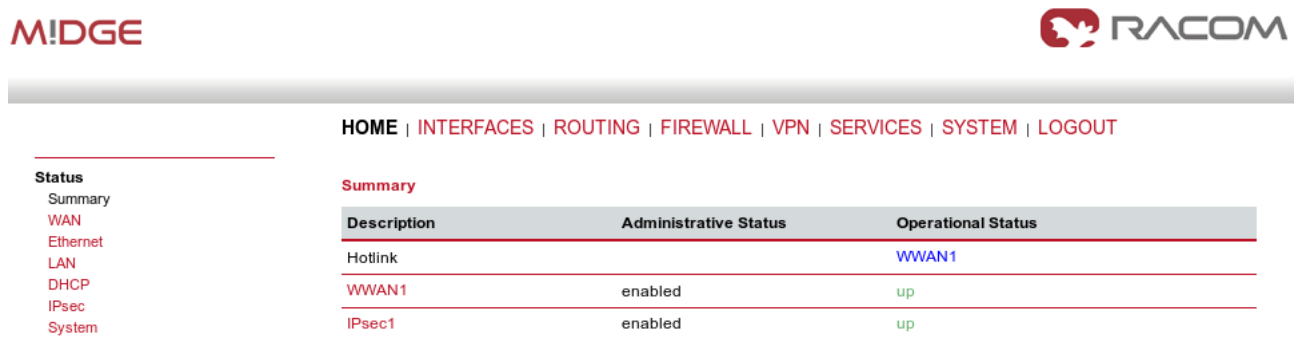


Fig. 2.37: IPsec is established successfully

Once the tunnel is UP, you can check the functionality via the ping, e.g. from the command shell:

```
~ $ ping -I 192.168.1.1 192.168.20.1
PING 192.168.20.1 (192.168.20.1) from 192.168.1.1: 56 data bytes
64 bytes from 192.168.20.1: seq=0 ttl=64 time=849.734 ms
64 bytes from 192.168.20.1: seq=1 ttl=64 time=1058.866 ms
64 bytes from 192.168.20.1: seq=2 ttl=64 time=918.134 ms
```

You need to set the source IP address so the IPsec routing would work. Otherwise, there could be no route back from the remote M!DGE.

Use M!DGE/MG102i manual for more details.

2.3. GRE

The description is being prepared.

2.4. PPTP

The description is being prepared.

3. Backup of WAN by the GSM Network

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.

3.1. Basic Backup Example

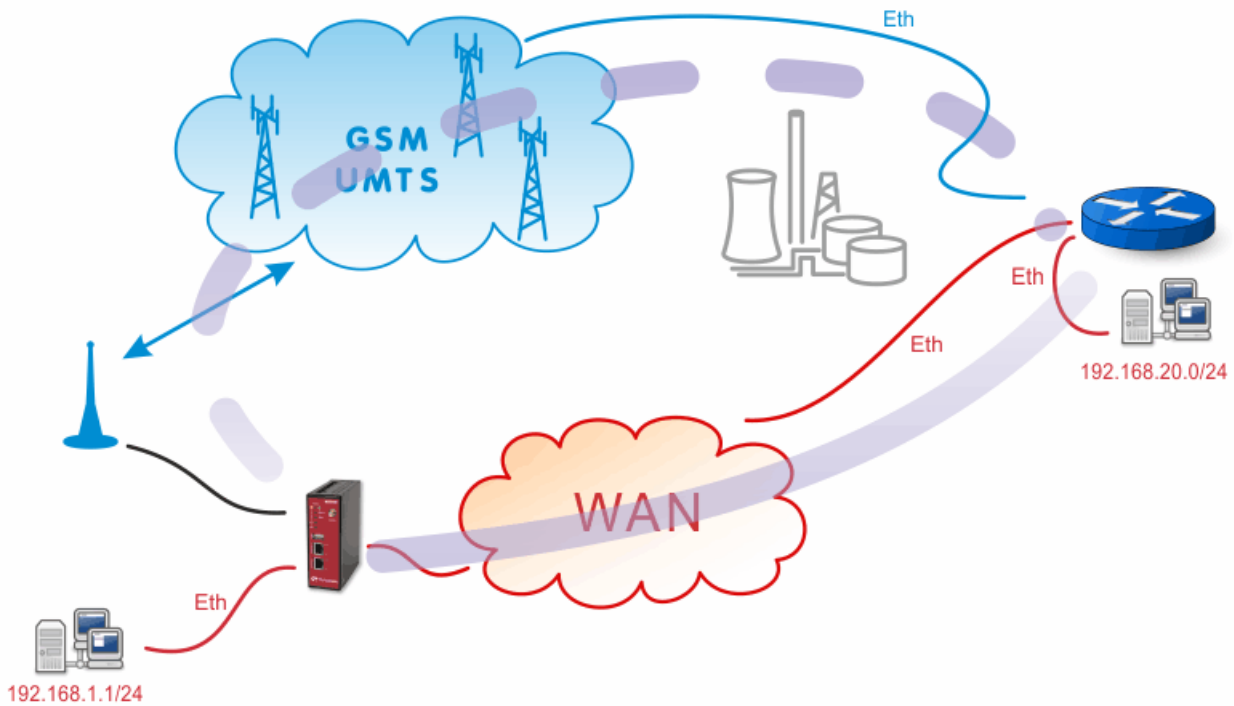


Fig. 3.1: Basic Backup Example

3.1.1. M!DGE Configuration

M!DGE

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Status

- Summary
- WAN
- WWAN
- Ethernet
- LAN
- DHCP
- IPsec
- System

Summary

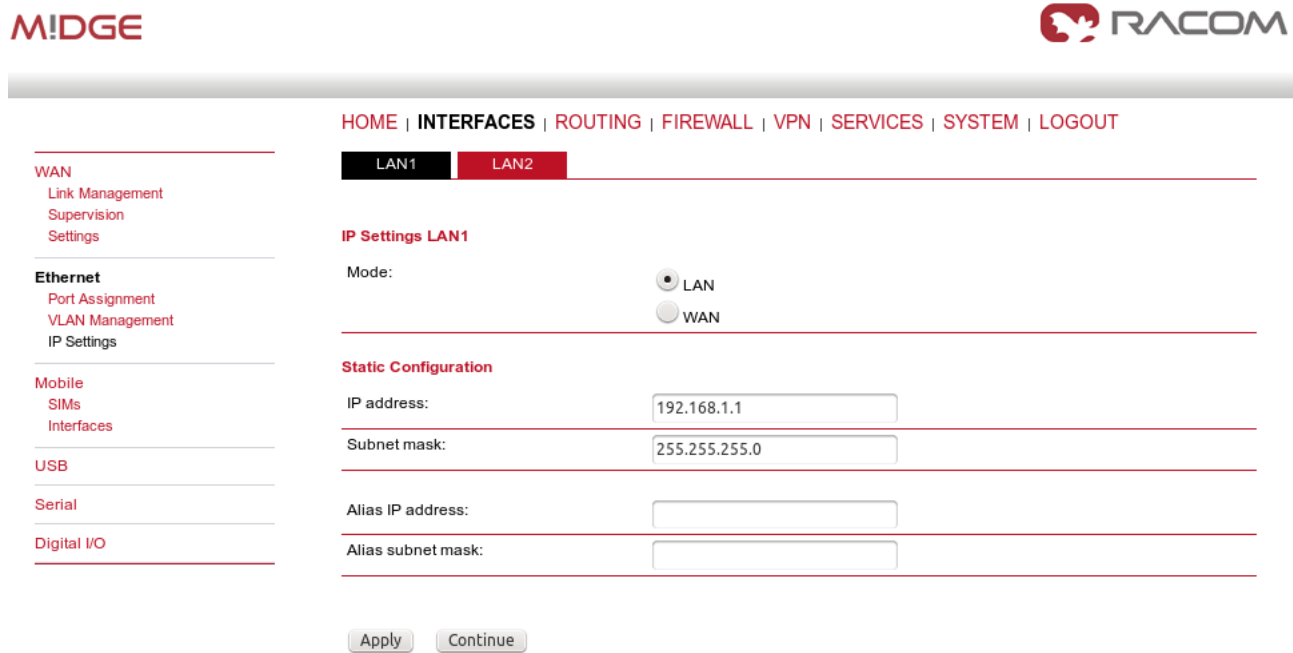
Description	Administrative Status	Operational Status
Hotlink		LAN2
LAN2	enabled	up
WWAN1	enabled	down
IPsec1	enabled	up

Fig. 3.2: 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.

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.



M!DGE **RACOM**

HOME | **INTERFACES** | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

LAN1 | LAN2

IP Settings LAN1

Mode: LAN WAN

Static Configuration

IP address:

Subnet mask:

Alias IP address:

Alias subnet mask:

Navigation Menu:

- WAN
 - Link Management
 - Supervision
 - Settings
- Ethernet**
 - Port Assignment
 - VLAN Management
 - IP Settings
- Mobile
 - SIMs
 - Interfaces
- USB
- Serial
- Digital I/O

Fig. 3.3: Central M!DGE LAN1 configuration

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

LAN1 | LAN2

IP Settings LAN2

Mode: LAN WAN

WAN mode: DHCP client static IP PPPoE

Static Configuration

IP address:

Subnet mask:

Default gateway:

Primary DNS server:

Secondary DNS server:

MTU:

WAN
Link Management
Supervision
Settings

Ethernet
Port Assignment
VLAN Management
IP Settings

Mobile
SIMs
Interfaces

USB

Serial

Digital I/O

Fig. 3.4: Central M!DGE WAN configuration

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.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

WAN
Link Management
Supervision
Settings

Ethernet
Port Assignment
VLAN Management
IP Settings

Mobile
SIMs
Interfaces

USB

Serial

Digital I/O

Edit WWAN Interface WWAN1

Mobile | **Connection** | Advanced

Connection settings: load from database
 specify

Phone number:

Access point name:

Authentication:

Username:

Password:

Apply

Fig. 3.5: Mobile interface configuration

Use manual for more details about the mobile interface configuration¹.

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.

HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT

OpenVPN
Administration
Tunnel Configuration

IPsec
Administration
Tunnel Configuration

IPsec Tunnel Configuration

Name	Type	Peer	IKE	IPsec	Local Network	Remote Network	
Tunnel 1	psk	10.203.3.33	3des-md5	3des-md5	192.168.1.0/24	192.168.20.0/24	

Fig. 3.6: 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.

See the VPN examples in Chapter 2, *VPN Configuration Options* or the manual² for more details.

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“

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

² http://www.racom.eu/eng/products/m/midge1/web_conf.html#VPN

(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).

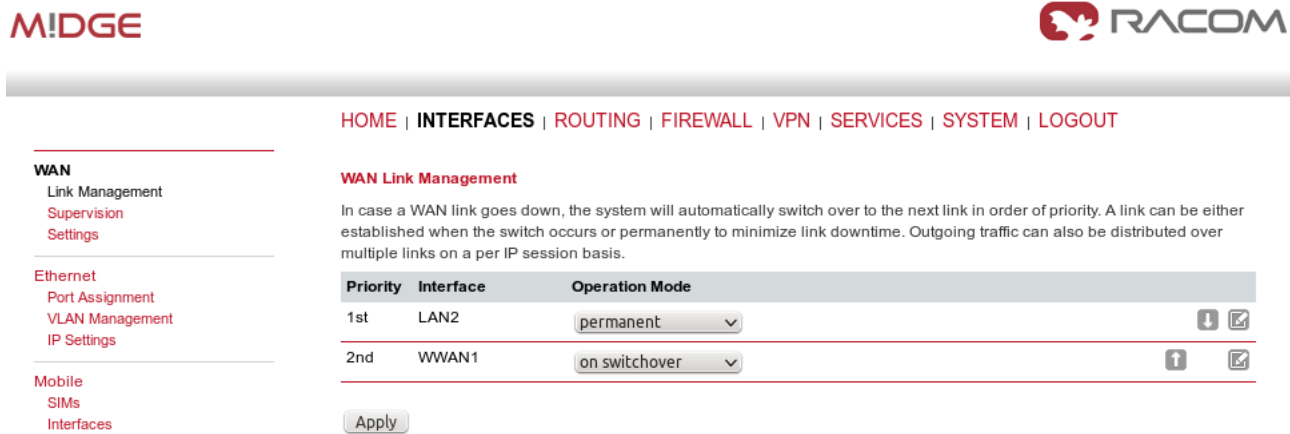


Fig. 3.7: WAN Link Management

Another step is configuring the Supervision feature.

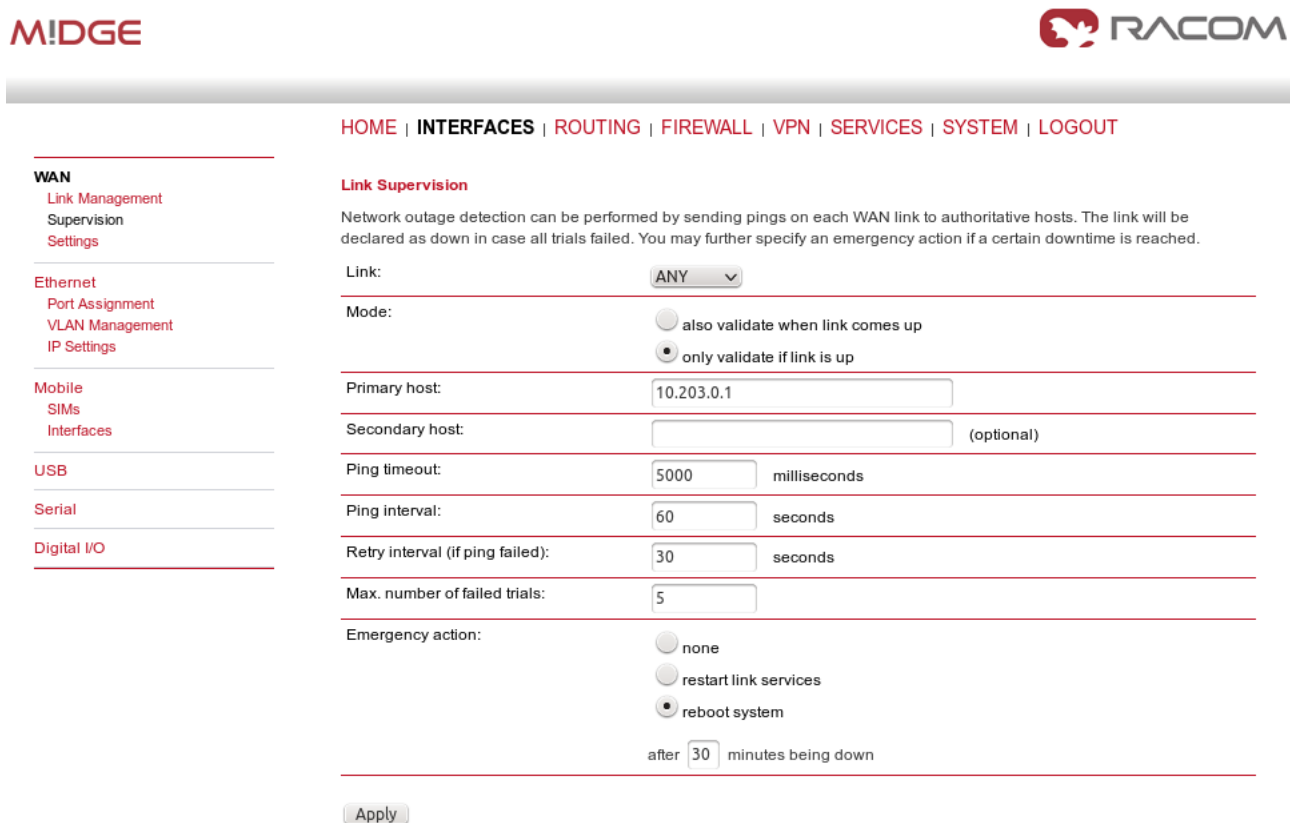


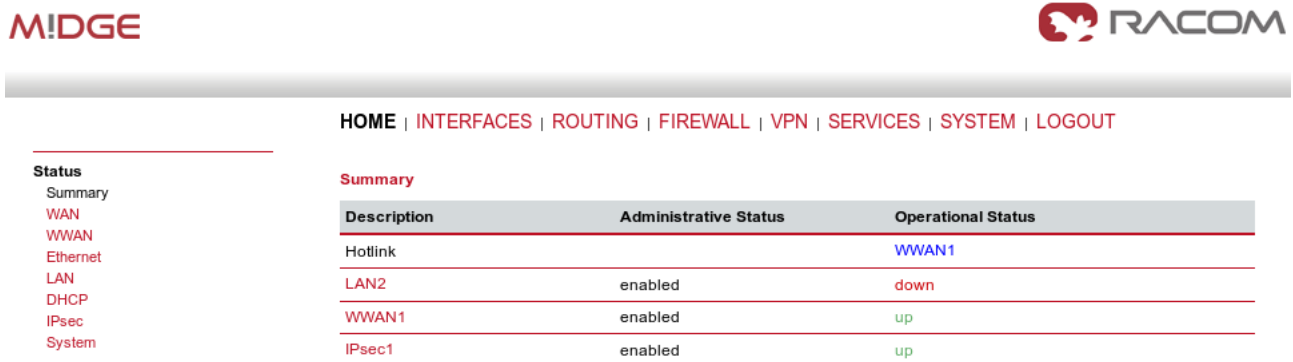
Fig. 3.8: Supervision

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).

3.1.2. 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.



The screenshot shows the M!DGE web interface with the RACOM logo in the top right. The navigation menu includes HOME, INTERFACES, ROUTING, FIREWALL, VPN, SERVICES, SYSTEM, and LOGOUT. On the left, a 'Status' sidebar lists WAN, WWAN, Ethernet, LAN, DHCP, IPsec, and System. The main content area shows a 'Summary' table with the following data:

Description	Administrative Status	Operational Status
Holink		WWAN1
LAN2	enabled	down
WWAN1	enabled	up
IPsec1	enabled	up

Fig. 3.9: 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.

3.2. 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...

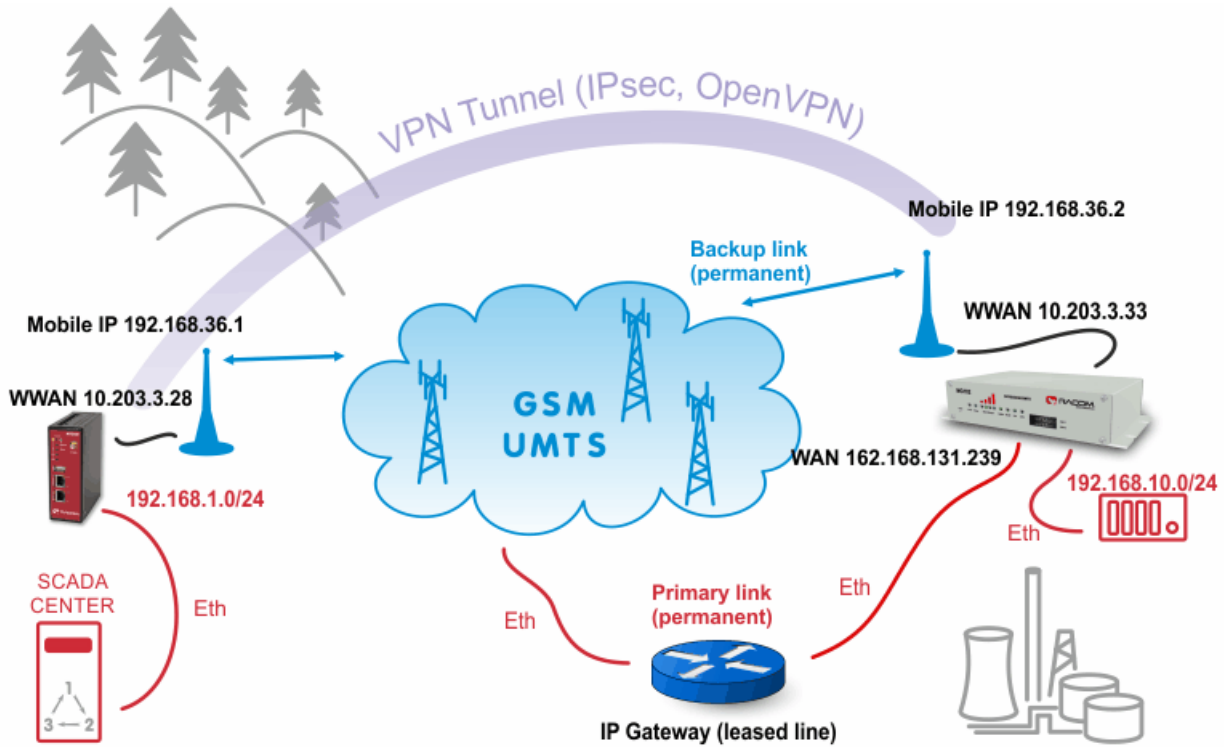


Fig. 3.10: MobileIP with VPN tunnel example topology

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.

3.2.1. 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.

Ethernet

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

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

LAN1 | LAN2

IP Settings LAN1

Mode: LAN WAN

Static Configuration

IP address:

Subnet mask:

Alias IP address:

Alias subnet mask:

Apply Continue

Fig. 3.11: 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.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

WAN Link Management

In case a WAN link goes down, the system will automatically switch over to the next link in order of priority. A link can be either established when the switch occurs or permanently to minimize link downtime. Outgoing traffic can also be distributed over multiple links on a per IP session basis.

Priority	Interface	Operation Mode
1st	WWAN1	<input type="text" value="permanent"/>

Apply

Fig. 3.12: 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.

- System
 - Settings
 - Time & Region
 - Reboot
- Authentication
 - Authentication
 - User Accounts
 - Remote Authentication
- Software Update
 - Software Update
 - Firmware Update
 - Software Profiles
- Configuration
 - File Configuration
 - Factory Configuration
- Troubleshooting

System Time

Current system time:

Time Synchronisation

NTP server 1:

NTP server 2 (optional):

Time zone

Time zone:

Daylight saving changes:

Fig. 3.13: NTP Configuration

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.

- Static Routes
- Extended Routes
- Multipath Routes
- Mobile IP**
 - Administration
 - Mobile Nodes
- QoS
 - Administration
 - Classification

Mobile IP

Mobile IP can be used to move from one network to another while maintaining a permanent IP address and thus avoiding that running IP sessions (including VPN tunnels) must be reconnected.

Administrative status: mobile node home agent disabled

Home network address:

Home network mask:

Fig. 3.14: 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).

HOME | INTERFACES | **ROUTING** | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Static Routes

Extended Routes

Multipath Routes

Mobile IP

Administration

Mobile Nodes

SPI:

Authentication type:

Shared secret:

Fig. 3.15: 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.

OpenVPN

Configure the OpenVPN server in routed mode.

HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT

Tunnel 1 | Tunnel 2 | Tunnel 3 | Tunnel 4

OpenVPN Tunnel 1 Configuration

Operation mode: disabled client standard expert

Server port:

Type:

Protocol:

Network mode: routed bridged MTU:

Cipher:

Authentication:

HMAC digest:

Options: use compression redirect gateway use keepalive

Fig. 3.16: OpenVPN server, Mobile IP

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

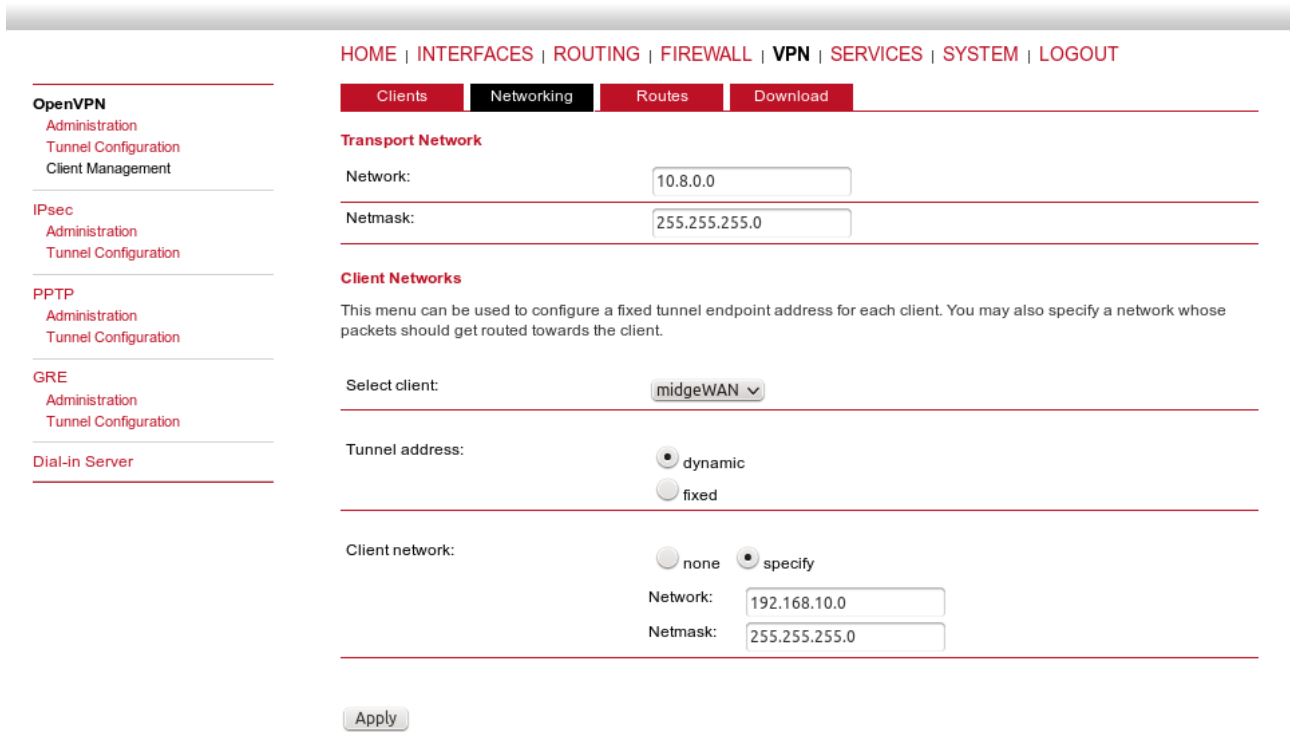


Fig. 3.17: OpenVPN server – Networking

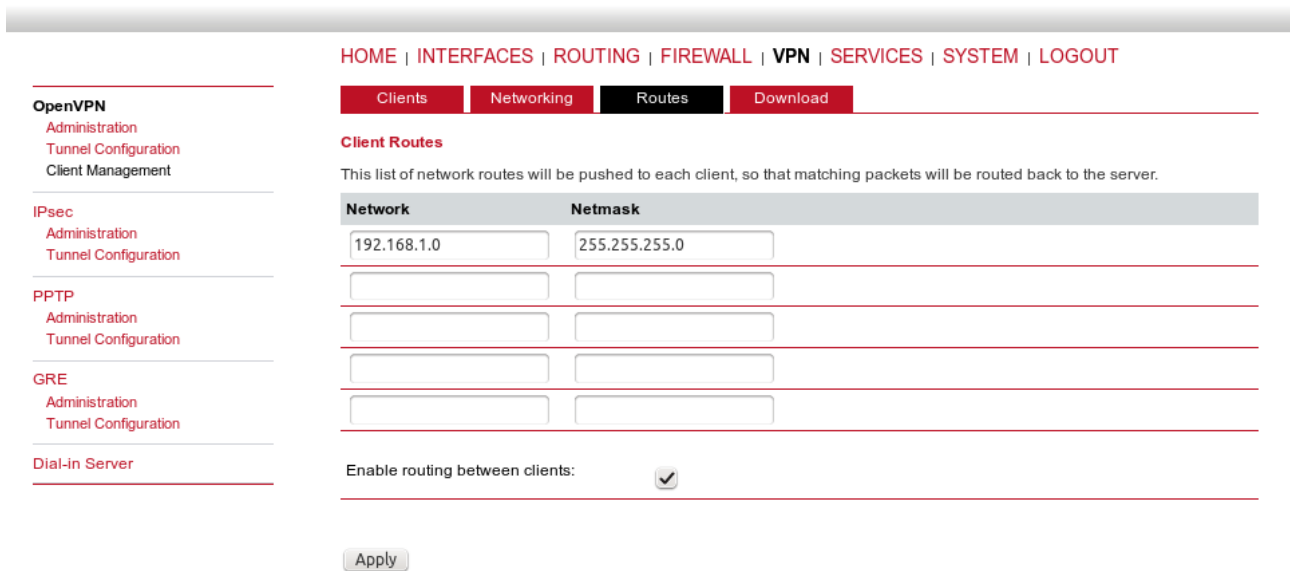


Fig. 3.18: OpenVPN server – Routes

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.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Clients | Networking | Routes | Download

OpenVPN
Administration
Tunnel Configuration
Client Management

Download Expert Mode Files

Server address/hostname:

IPsec
Administration
Tunnel Configuration

Fig. 3.19: 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.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

OpenVPN Administration

OpenVPN administrative status: enabled disabled

Restart on link change:

OpenVPN
Administration
Tunnel Configuration
Client Management

IPsec
Administration
Tunnel Configuration

PPTP

Fig. 3.20: Enabling OpenVPN server

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

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Status
Summary
WAN
WWAN
Ethernet
LAN
DHCP
OpenVPN
IPsec
MobileIP
System

Summary

Description	Administrative Status	Operational Status
Hotlink		WWAN1
WWAN1	enabled	up
OpenVPN1	enabled, server	up
MobileIP	enabled	up

Fig. 3.21: OpenVPN server and Mobile IP are running



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.

HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT

OpenVPN
Administration
Tunnel Configuration
Client Management

IPsec Tunnel Configuration

Name	Type	Peer	IKE	IPsec	Local Network	Remote Network	
Tunnel 1	psk	192.168.36.2	3des-md5	3des-md5	192.168.1.0/24	192.168.10.0/24	 
							

IPsec
Administration
Tunnel Configuration

Fig. 3.22: IPsec – M!DGE configuration

HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT

OpenVPN
Administration
Tunnel Configuration
Client Management

IPsec Administration

IPsec administrative status: enabled
 disabled

Propose NAT traversal:

Restart on link change:

IPsec
Administration
Tunnel Configuration

PPTP
Administration
Tunnel Configuration

Fig. 3.23: Enabling IPsec – M!DGE

3.2.2. 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).

WAN Configuration

MG102i



HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

LAN1 | LAN5

IP Settings LAN5

Mode: LAN WAN

WAN mode: DHCP client static IP PPPoE

Static Configuration

IP address:

Subnet mask:

Default gateway:

Primary DNS server:

Secondary DNS server:

MTU:

Fig. 3.24: MG102i WAN configuration

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

MG102i

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

LAN1 | LAN5

IP Settings LAN1

Mode: LAN WAN

Static Configuration

IP address:

Subnet mask:

Alias IP address:

Alias subnet mask:

Apply Continue

Fig. 3.25: MG102i LAN configuration

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

MG102i

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

WAN Link Management

In case a WAN link goes down, the system will automatically switch over to the next link in order of priority. A link can be either established when the switch occurs or permanently to minimize link downtime. Outgoing traffic can also be distributed over multiple links on a per IP session basis.

Priority	Interface	Operation Mode
1st	LAN5	permanent
2nd	WWAN1	permanent

Apply

Fig. 3.26: 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.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

WAN

Link Management

Supervision

Settings

Ethernet

Port Assignment

VLAN Management

IP Settings

Mobile

SIMs

Interfaces

WLAN

Administration

Configuration

IP Settings

USB

Serial

Digital I/O

GNSS

Link Supervision

Network outage detection can be performed by sending pings on each WAN link to authoritative hosts. The link will be declared as down in case all trials failed. You may further specify an emergency action if a certain downtime is reached.

Link: LAN5 v

Mode: also validate when link comes up
 only validate if link is up

Primary host: 192.168.131.102

Secondary host: (optional)

Ping timeout: 1000 milliseconds

Ping interval: 10 seconds

Retry interval (if ping failed): 5 seconds

Max. number of failed trials: 5

Emergency action: none
 restart link services
 reboot system

Apply

Fig. 3.27: 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.

- WAN
 - Link Management
 - Supervision
 - Settings
- Ethernet
 - Port Assignment
 - VLAN Management
 - IP Settings
- Mobile
 - SIMs
 - Interfaces
- WLAN
 - Administration
 - Configuration
 - IP Settings
- USB
- Serial
- Digital I/O
- GNSS

Link Supervision

Network outage detection can be performed by sending pings on each WAN link to authoritative hosts. The link will be declared as down in case all trials failed. You may further specify an emergency action if a certain downtime is reached.

Link:

Mode:
 also validate when link comes up
 only validate if link is up

Primary host:

Secondary host: (optional)

Ping timeout: milliseconds

Ping interval: seconds

Retry interval (if ping failed): seconds

Max. number of failed trials:

Emergency action:
 none
 restart link services
 reboot system

Apply

Fig. 3.28: 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.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

System

- Settings
- Time & Region
- Reboot

Authentication

- Authentication
- User Accounts
- Remote Authentication

Software Update

- Software Update
- Firmware Update
- Software Profiles

Configuration

- File Configuration
- Factory Configuration

Troubleshooting

- Network Debugging
- System Debugging

System Time

Current system time:

Time Synchronisation

NTP server 1:

NTP server 2 (optional):

Sync time from GNSS:

Time zone

Time zone:

Daylight saving changes:

Fig. 3.29: MG102i NTP configuration

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.

[Static Routes](#)
[Extended Routes](#)
[Multipath Routes](#)
Mobile IP
[Administration](#)
[QoS](#)
[Administration](#)
[Classification](#)
Mobile IP

Mobile IP can be used to move from one network to another while maintaining a permanent IP address and thus avoiding that running IP sessions (including VPN tunnels) must be reconnected.

Administrative status:

- mobile node
 home agent
 disabled

 Primary home agent address:

 Secondary home agent address: (optional)

 Home address:

 SPI:

 Authentication type:

 Shared secret:

 Life time:

 MTU:

 UDP encapsulation: enabled disabled

 Mobile network address: (optional)

 Mobile network mask: (optional)

Fig. 3.30: MG102i Mobile IP – Mobile node

Set the Primary home agent address to the cellular IP address of the MIDGE (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.

HOME | INTERFACES | **ROUTING** | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Static Routes

This menu shows all routing entries of the system, they can consist of active and configured ones. The flags are as follows: (A)ctive, (P)ersistent, (H)ost Route, (N)etwork Route, (D)efault Route (Netmasks can be specified in CIDR notation)

Destination	Netmask	Gateway	Interface	Metric	Flags
0.0.0.0	0.0.0.0	192.168.131.253	LAN5	0	AD
10.64.64.64	255.255.255.255	0.0.0.0	WWAN1	0	AH
192.168.10.0	255.255.255.0	0.0.0.0	LAN1	0	AN
192.168.131.0	255.255.255.0	0.0.0.0	LAN5	0	AN
<input type="text" value="192.168.36.1"/>	<input type="text" value="255.255.255.255"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="MOBILEIP1"/>	<input type="text" value="0"/>	APH <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>

Route lookup

Fig. 3.31: 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.

OpenVPN

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

HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT

Tunnel 1 | **Tunnel 2** | Tunnel 3 | Tunnel 4

OpenVPN Tunnel 2 Configuration

Operation mode:

disabled
 client
 standard
 expert

Network mode:

routed
 bridged

Expert mode file: installed

Fig. 3.32: 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.

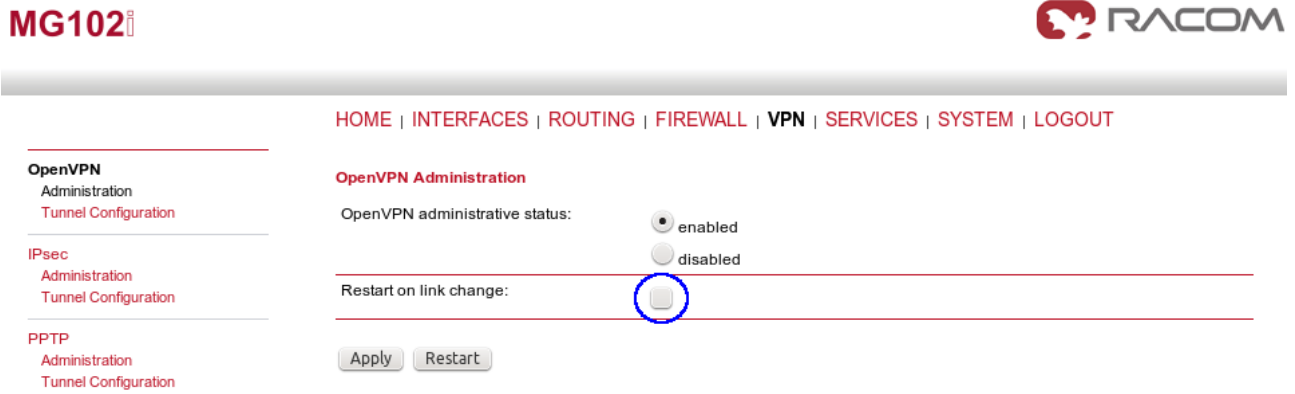


Fig. 3.33: Enabling OpenVPN – MG102i

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

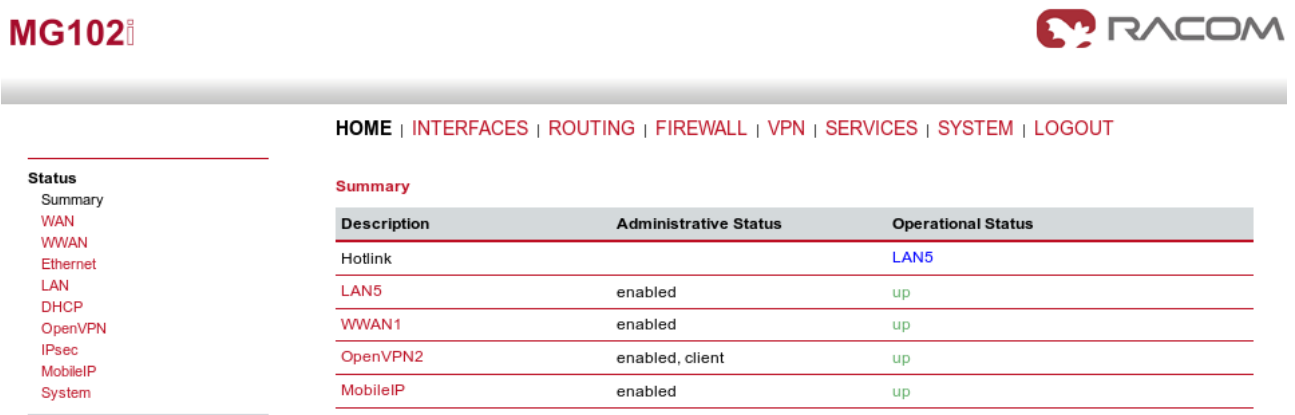


Fig. 3.34: OpenVPN and Mobile IP running – MG102i

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 MIDGE unit).

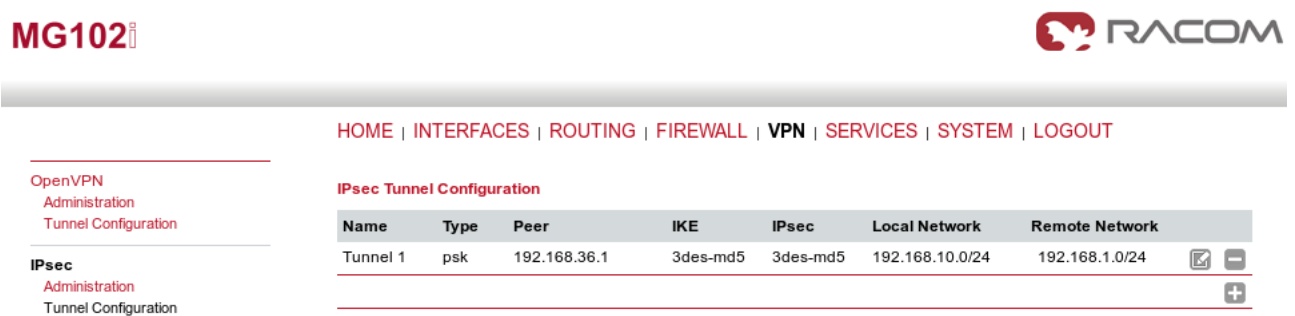


Fig. 3.35: IPsec configuration – MG102i

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

MG102i



HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

OpenVPN
Administration
Tunnel Configuration

IPsec
Administration
Tunnel Configuration

PPTP
Administration
Tunnel Configuration

IPsec Administration

IPsec administrative status: enabled
 disabled

Propose NAT traversal:

Restart on link change:

Apply Restart

Fig. 3.36: Enabling IPsec – MG102i

If configured correctly, check the HOME menu.

MG102i



HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Status
Summary
WAN
WWAN
Ethernet
LAN
DHCP
IPsec
MobileIP
System

Summary

Description	Administrative Status	Operational Status
Hotlink		LAN5
LAN5	enabled	up
WWAN1	enabled	up
IPsec1	enabled	up
MobileIP	enabled	up

Fig. 3.37: Ipsec and Mobile IP running – MG102i

3.2.3. 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. 3.38: 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.

MG102i



HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Status

Summary
WAN
WWAN
Ethernet
LAN
DHCP
OpenVPN
IPsec
MobileIP
System

Summary

Description	Administrative Status	Operational Status
Hotlink		WWAN1
LAN5	enabled	down
WWAN1	enabled	up
OpenVPN2	enabled, client	up
MobileIP	enabled	up

Fig. 3.39: 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 manual³ for more details.

³ <http://www.racom.eu/eng/products/m/midge1/index.html>

4. SCADA Serial Protocols over GSM Network

In recent years, world of communication is ruled by the Internet Protocol stack and RS232-based interfaces are generally considered obsolete. Typical SCADA device life cycle is nevertheless long enough to guarantee demand for good old serial interfaces for several years from now. Common RS232 to TCP (UDP) converters can help in some cases by creating the required number of transparent peer-to-peer connections from all remote serial ports to the corresponding (physical or virtual) ports in the data center. However such solution requires a special routing arrangement in the center, hence it is not always feasible. A typical SCADA Front End Processor (the central interface of the application to the communication network) uses a proprietary protocol over a single RS232 interface. Each message coming out from the FEP is addressed and should be delivered to the designated remote serial port. Certainly a transparent broadcasting to all remotes could do the job, making the service provider happy (assuming the resulting bills are paid). Obviously the proper solution is to transmit the message to the destination address only.

A SCADA serial protocol typically uses simple 8 or 16 bit addressing. The mobile network address scheme is an IP network, where the range is defined by the service provider (sometimes including individual addresses, even in the case of a private APN). Consequently a mechanism of translation between the SCADA and the IP addresses is required. To make things worse, IP addresses may be assigned to GPRS (EDGE, UMTS, etc.) devices dynamically upon each connection.

This chapter describes how to efficiently solve this problem using RACOM made routers.

Two basic situations are described:

- a. The MIDGE/MG102i IP addresses are reachable from each other in both directions. This can either mean that you have the private APN with the own IP subnet for your application. Or it can mean that all routers have static public IP addresses. The example in Section 4.1, "SCADA Protocols – private APN" shows the routers' configuration using the private APN with static addresses.
- b. The MIDGE/MG102i IP addresses are NOT reachable in both directions – only the center is reachable from the remote side. The center must have a static public IP address. The remote units (slaves in the Master-Slave configuration) can have private and dynamic IP addresses. Utilization of VPN tunnels is required. See the example Section 4.2, "SCADA Protocols – public APN" for more details.

4.1. SCADA Protocols – private APN

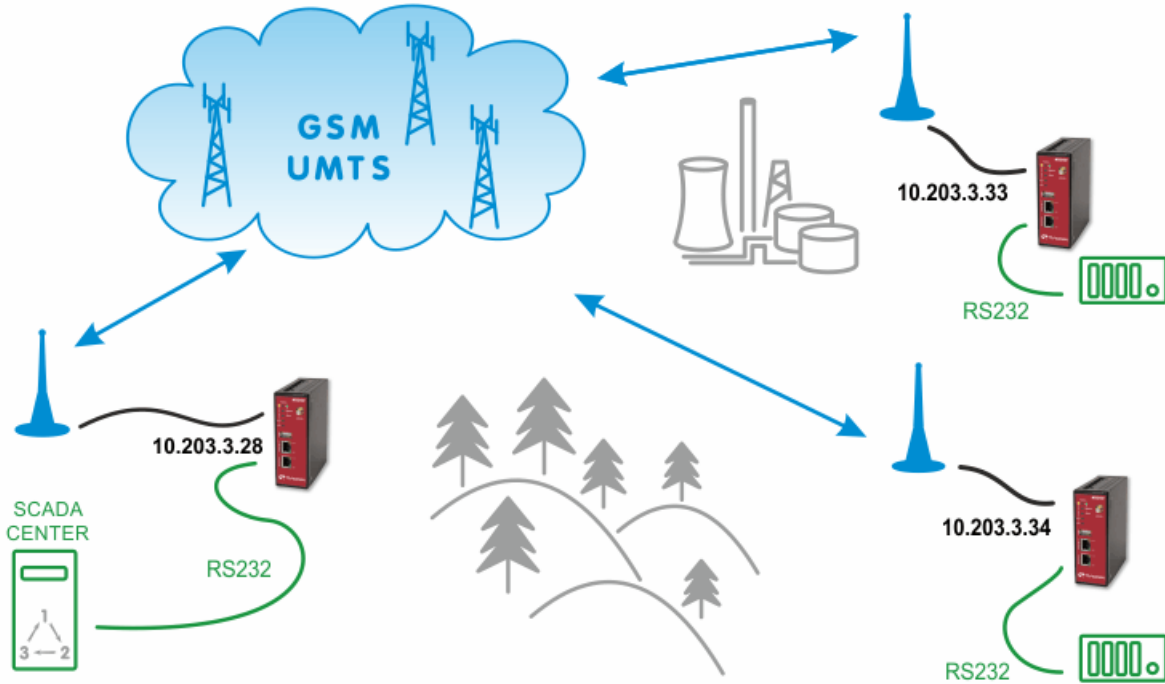


Fig. 4.1: SCADA Solution within Private APN

4.1.1. APN Configuration

In the INTERFACES – Mobile – Interfaces menu, configure the private APN as defined by your service provider.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

WAN
Link Management
Supervision
Settings

Ethernet
Port Assignment
VLAN Management
IP Settings

Mobile
SIMs
Interfaces

USB

Serial

Digital I/O

Edit WWAN Interface WWAN1

Mobile Connection **Advanced**

Connection settings: load from database specify

Phone number:

Access point name:

Authentication:

Username:

Password:

Apply

Fig. 4.2: Private APN configuration

Once established, you can check the connection status in the HOME menu.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

WWAN1

Description	Value
Administrative state	enabled
Operational state	up
Link is up since	2015-05-22 13:46:15
Modem	Mobile1
SIM	SIM1 (ready)
Signal strength	-93 dBm (medium)
Registration status	registeredInHomeNetwork
Service type	HSPA
Network	O2-CZ (Cell E751860)
IP address	10.203.3.28
Gateway	10.64.64.64
Transfer rate down / up	0 bit/s / 0 bit/s
Data downloaded / uploaded	101.67 MB / 61.04 MB <input type="button" value="Reset"/>

Status
Summary
WAN
WWAN
Ethernet
LAN
DHCP
IPsec
System

Fig. 4.3: Private APN connection is established

Configure other units with the appropriate credentials. In our example the Master M!DGE obtained the IP address 10.203.3.28 and the remote M!DGE units have 10.203.3.33 and 10.203.3.34.

4.1.2. SCADA Master Configuration

Our example will explain the Modbus Master-slave configuration with two slave units. On the Master station, select the INTERFACES – Serial menu and set the Protocol server option.

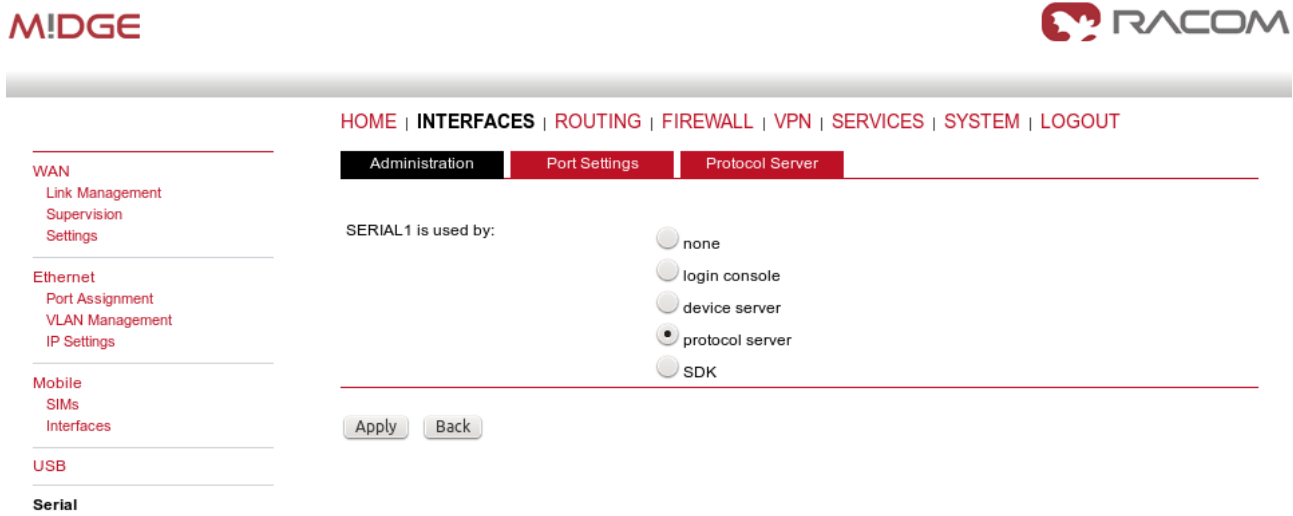


Fig. 4.4: Master Protocol server configuration

Configure the correct RS232 parameters such as baud rate, stop bits, ...

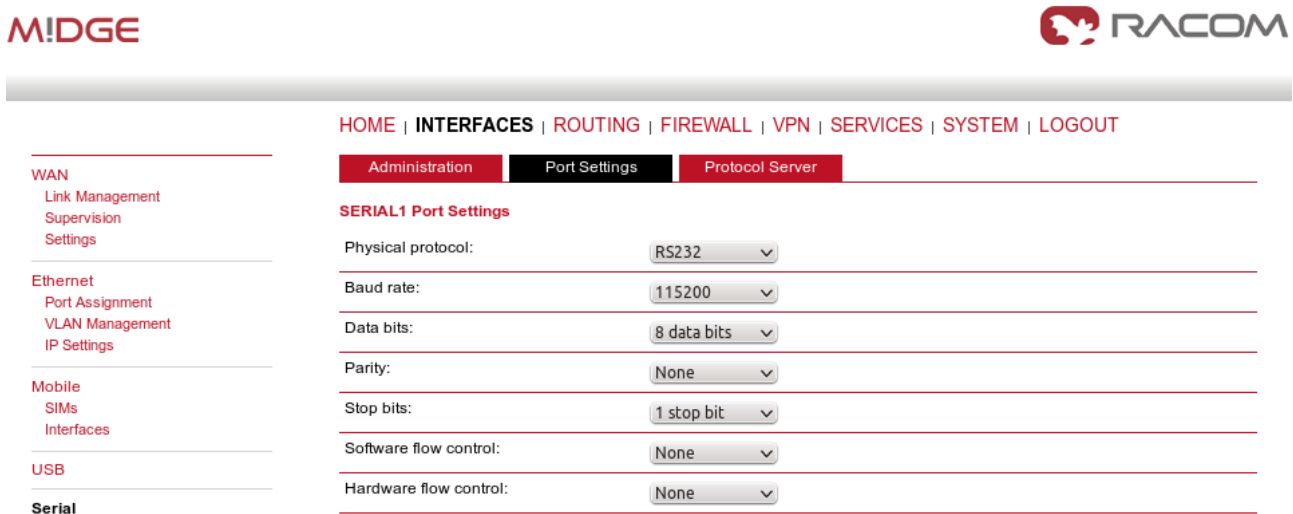


Fig. 4.5: Port Settings



Note

Configuration within the Port Settings – Server configuration is only usable with Device server option, but we configure Protocol server. You can ignore the settings here.

Go to the Protocol server menu and configure the Master parameters. Focus on the correct Address translation. You can either use mask or table for this purpose. If in doubts, open the Help window via the button located on top right corner. This Help explains the whole Protocol server functionality.

In the example below, the Master translates addresses A and B (hex) into IP addresses (and vice versa) 10.203.3.33, resp. 10.203.3.34. Using the port 8882 is mandatory if the remote device is connected via MIDGE RS232 interface.

HOME | **INTERFACES** | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Administration | Port Settings | **Protocol Server** | Help

Protocol Server

Protocol: Modbus

Parameters

Mode of Connected device: Master

Broadcast: Off

Address translation

Address translation: Table

Address format: Hex

Address (8b)	IP	Interface (UDP port)	Note	Act.	Modify
a	10.203.3.33	COM(8882)	Remote MIDGE A	<input checked="" type="checkbox"/>	↓ - +
b	10.203.3.34	COM(8882)	Remote MIDGE B	<input checked="" type="checkbox"/>	↑ - +

Apply

Fig. 4.6: Modbus Master configuration

4.1.3. SCADA Slave Configuration

The Slave configuration is very straightforward. You just set the Modbus Mode to “slave” and the rest is solved by the Protocol server.

HOME | **INTERFACES** | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Administration | Port Settings | **Protocol Server** | Help

Protocol Server

Protocol: Modbus

Parameters

Mode of Connected device: Slave

Broadcast: Off

Address translation: Table

Address format: Hex

Apply

Fig. 4.7: Modbus Slave configuration

4.1.4. Troubleshooting

In case that you encounter any issue, you can read the **Protocol Server Help** which is reachable from the right top corner of the page. Sending the issue description to our technical support at support@racom.eu is possible. Please try to include the following information:

- The **issue description** (together with topology, required technology, ...)
- Please increase the **debug level of rrsp2 daemon** first (SYSTEM – Troubleshooting – System Debugging – Debug Levels – set rrsp2 to “4”). When applied, try to run your application and then download the Tech Support package (can be downloaded from the SYSTEM – Troubleshooting – Tech Support menu).

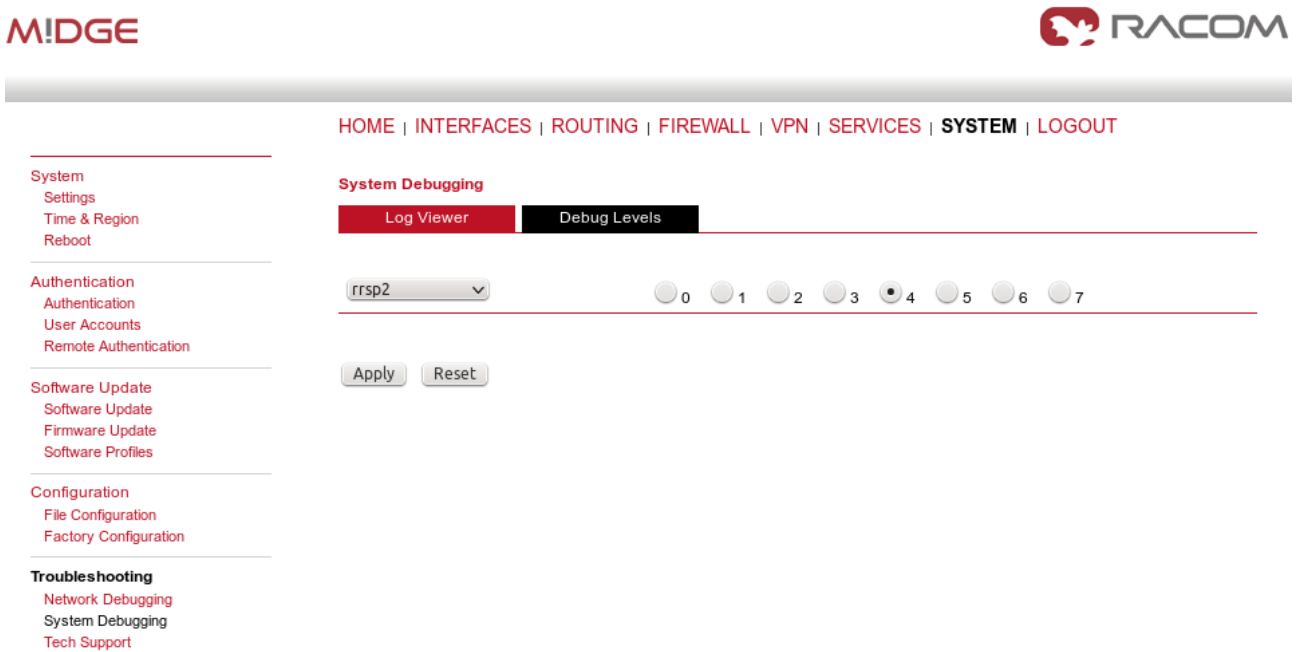


Fig. 4.8: Debug level of rrsp2 daemon

- You can also include the **WWAN interface monitoring** output: SYSTEM – Troubleshooting – Network debugging - tcpdump – Set interface to “wwan1” and check all the “Exclude” boxes. Click start, run your application and after a while, stop the tcpdump again and download the file.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

System
Settings
Time & Region
Reboot

Authentication
Authentication
User Accounts
Remote Authentication

Software Update
Software Update
Firmware Update
Software Profiles

Configuration
File Configuration
Factory Configuration

Troubleshooting
Network Debugging
System Debugging
Tech Support

Network Debugging

ping | traceroute | **tcpdump** | darkstat

The tcpdump utility generates a network capture (PCAP) of an interface which can be later analyzed with [Wireshark](#).

Interface:

Maximum number of packets:

Exclude:

- http
- https
- telnet
- ssh

Fig. 4.9: Tcpdump via Web interface



Note

It is not possible to monitor the serial interface in M!DGE/MG102i.

4.2. SCADA Protocols – public APN

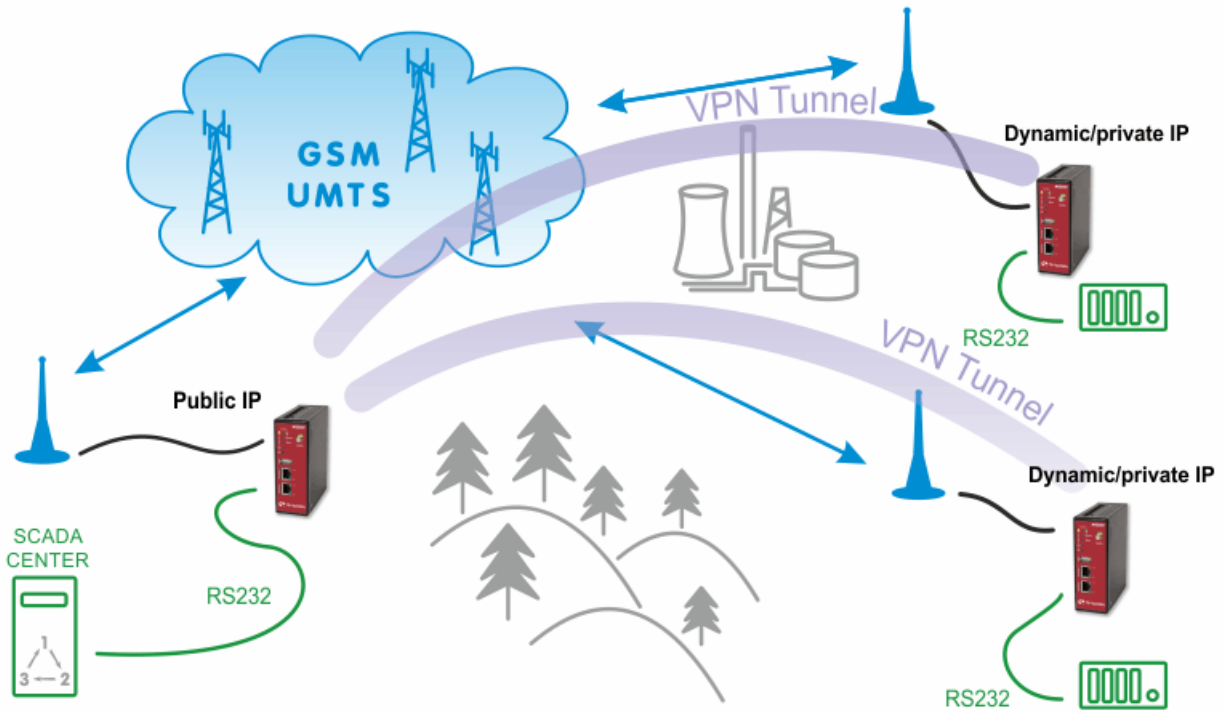


Fig. 4.10: Public APN SCADA configuration

4.2.1. APN Configuration

With the public APN, you need to have a public and static IP address in the center. In our example, we configure the APN to be “internet.open.s” so we obtain the required IP address.

M!DGE
RACOM

WAN

- Link Management
- Supervision
- Settings

Ethernet

- Port Assignment
- VLAN Management
- IP Settings

Mobile

- SIMs
- Interfaces

USB

Serial

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Edit WWAN Interface WWAN1

Mobile
Connection
Advanced

Connection settings: load from database specify

Phone number:

Access point name:

Authentication:

Fig. 4.11: Public APN configuration (static, public IP address)

The remote stations can be configured with the most basic APN, e.g. “internet” to obtain the private and dynamic IP address. In the next section, we will configure the VPN tunnel which is necessary for this kind of connection. Without the tunnel, the serial communication will be blocked within the mobile network.

In this example, we configure the OpenVPN tunnel in the routed mode. See Section 2.1.1, “OpenVPN – Routed mode” for configuration details. The only difference is that we do not need to configure any VPN connected networks on any M!DGE unit, we just use the fixed tunnel addresses for serial data communication.

The screenshot shows the M!DGE web interface for configuring a VPN tunnel. The navigation menu includes HOME, INTERFACES, ROUTING, FIREWALL, VPN, SERVICES, SYSTEM, and LOGOUT. The current page is under the 'Networking' tab, specifically the 'Client Networks' section for 'Client1'. The 'Transport Network' section shows a Network of 10.8.0.0 and a Netmask of 255.255.255.0. The 'Client Networks' section has a description: 'This menu can be used to configure a fixed tunnel endpoint address for each client. You may also specify a network whose packets should get routed towards the client.' The 'Select client' dropdown is set to 'Client1'. Under 'Tunnel address', the 'dynamic' radio button is unselected and the 'fixed' radio button is selected. The 'fixed' radio button and its associated text input field containing '10.8.0.6' are circled in blue. The 'Client network' section has 'none' selected. An 'Apply' button is at the bottom.

Fig. 4.12: Fixed OpenVPN tunnel address for clients

The clients can be then configured just via the Expert files downloaded from the Master M!DGE. The first client will obtain 10.8.0.6 tunnel address and the second client 10.8.0.10.

4.2.2. SCADA Master Configuration

The configuration is the same as explained with the Private APN , but replace the IP addresses.

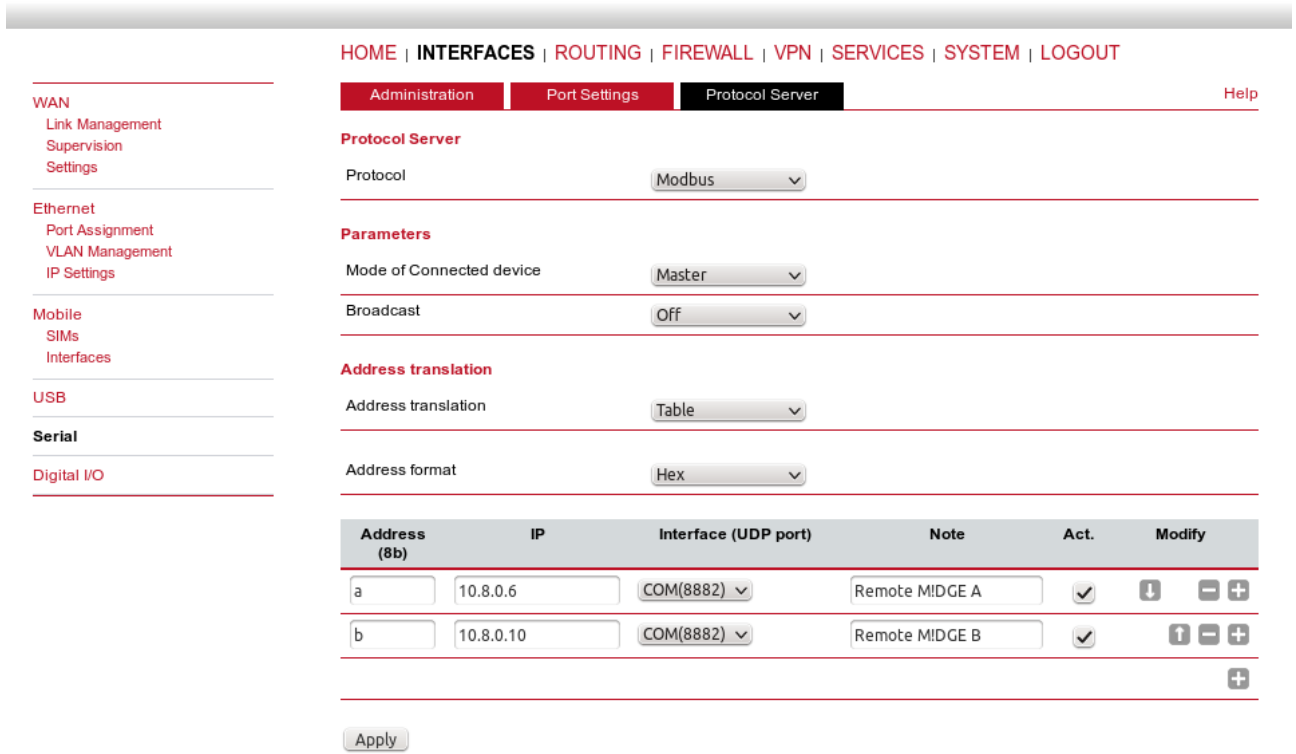


Fig. 4.13: Master Protocol server configuration (public APN)

Now we are finished, but due to Protocol server configuration, we need to disable source IP control mechanism, because IP addresses are changed due to using VPN tunnel. This needs to be done via SSH access to the M!DGE unit. Login as root using the same password as for the web administrator access and run the following command:

```
$ vi /etc/config/factory-config.cfg
```

The configuration file will be opened. Find the line with

```
rrsp.2.ComTtMasking.0.COM_PROT_CHECK_SRCIP=1
```

and change the last digit to “0” (press the button “i” to enter editor)

```
rrsp.2.ComTtMasking.0.COM_PROT_CHECK_SRCIP=0
```

Press “ESC” button and close the file by typing “:x”. Then run the command

```
$ rm /etc/rrconf/rrsp2.cfg
```

and reboot the unit via the command

```
$ reboot
```

After the unit boots up, you have finished the Master configuration.

4.2.3. SCADA Slave Configuration

The Slave must be connected via the OpenVPN tunnel to the Master and its Protocol server must be configured to the Modbus – Slave mode.

4.2.4. Troubleshooting

The troubleshooting is the same as explained in the Section 4.1.4, “Troubleshooting”.

**Note**

If your server is using TCP connection, configure the Device server instead of Protocol server and set the Mode to “TCP Raw” with the appropriate TCP port.

5. UHF/VHF and GPRS/UMTS Combination

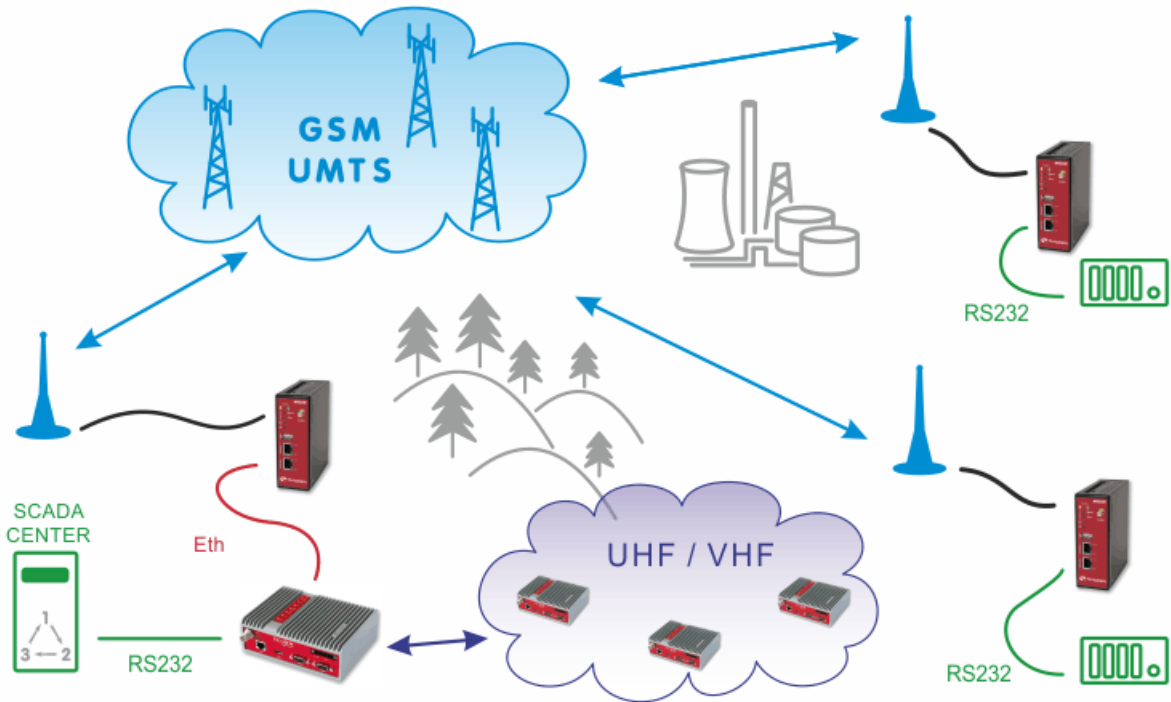


Fig. 5.1: UHF/VHF and GPRS/UMTS Combination

The picture above describes an arrangement, where part of the remote sites is connected over a private UHF/VHF radio network (e.g. sites requiring 99.9% availability) and the remaining sites are connected over a cellular public network (very remote location, but with a good cellular signal).

The SCADA Center can be connected either to central RipEX or even to MIDGE, both can serve as the Master unit. Please see the following example of one possible settings. MIDGE units use the private APN with static IP addresses.

5.1. Practical Example

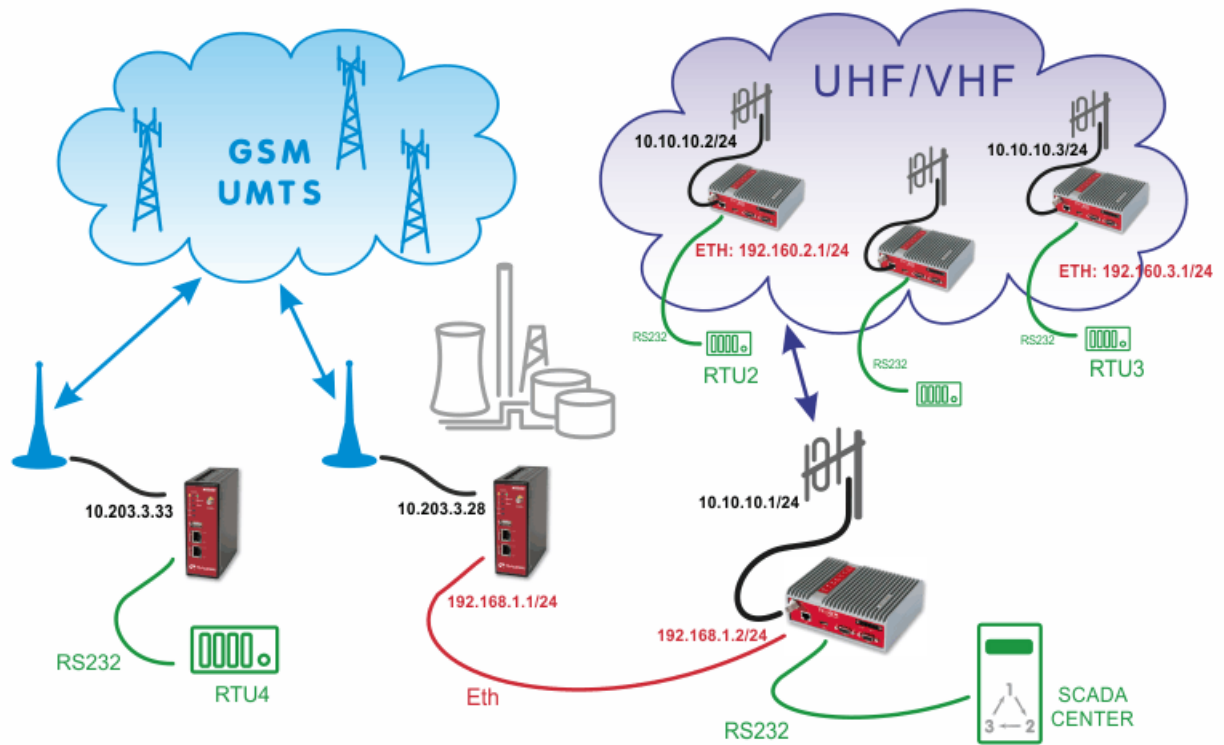


Fig. 5.2: UHF/VHF and GPRS/UMTS/HSPA combination example

In the example, the SCADA Center is connected via RS232 interface to RipEX1 (COM1). The Center is utilized with Modbus RTU Master configuration and polls two RTUs connected via RipEX network. There is one distant RTU4 location which is reachable over the cellular network.

5.1.1. RipEX Center Configuration

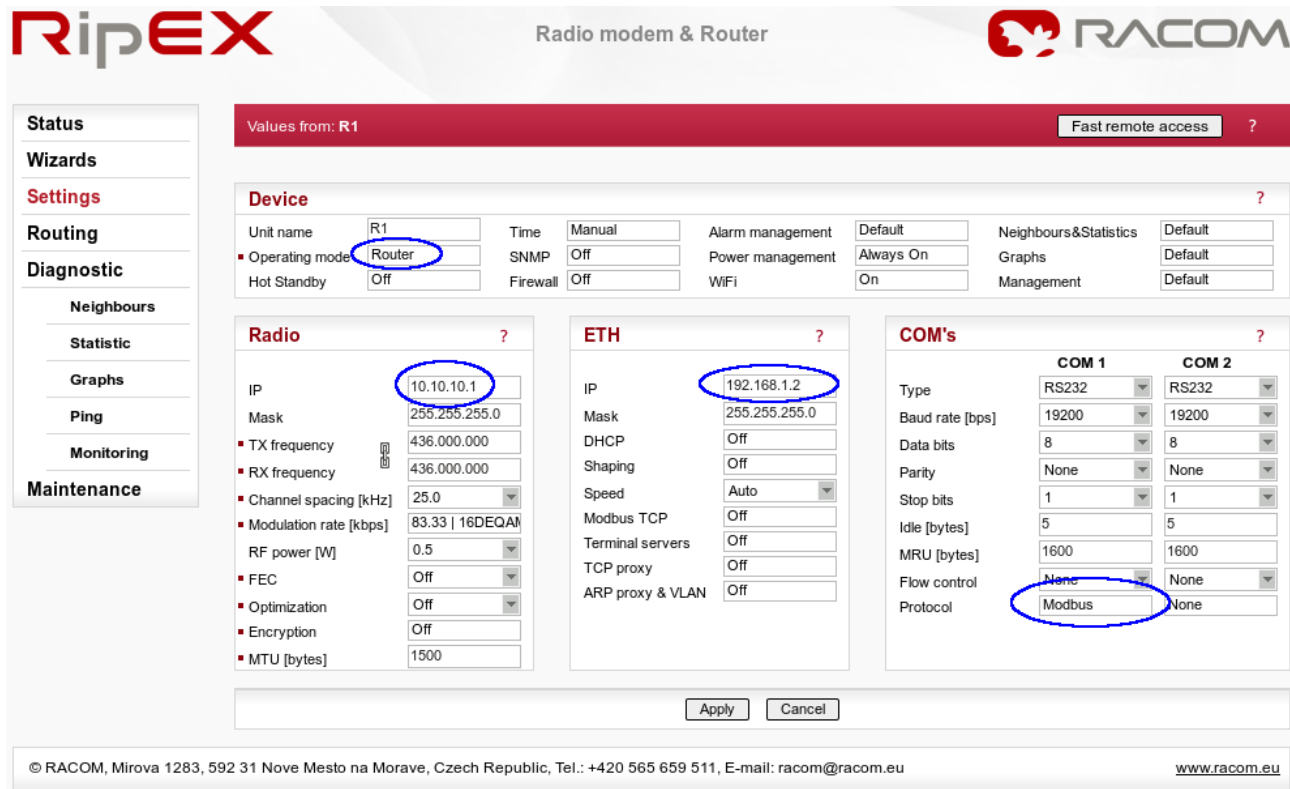


Fig. 5.3: RipEX Center Settings

Apply the correct IP addresses within the Router mode and set the COM1 protocol.

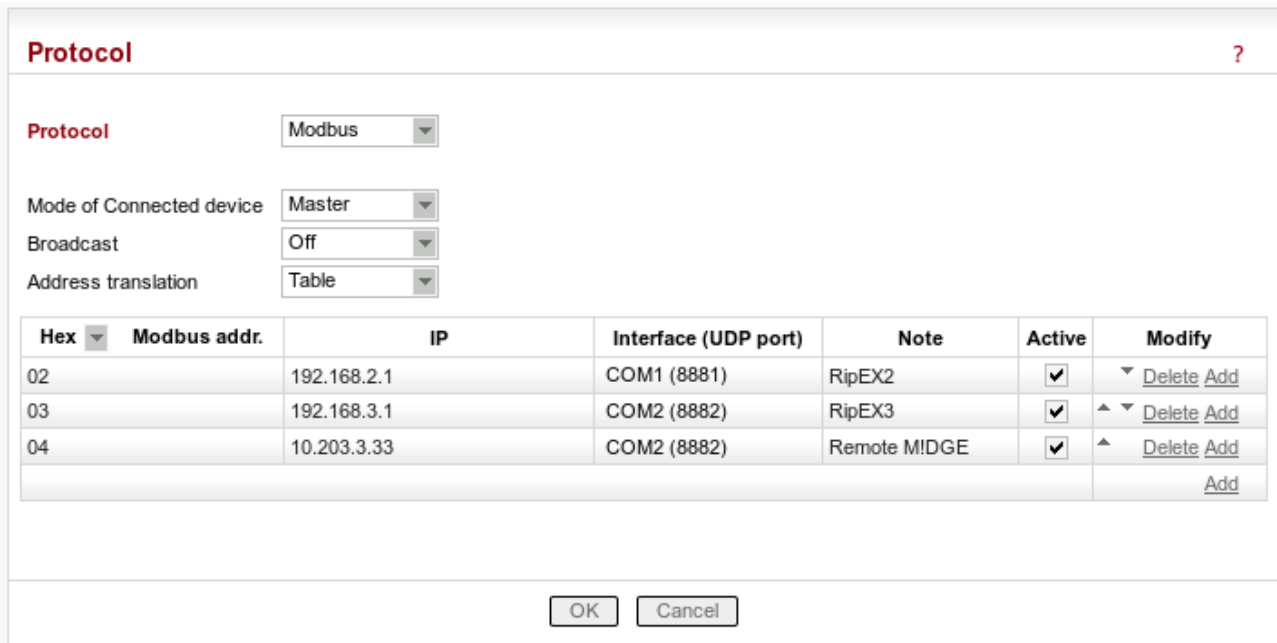


Fig. 5.4: Modbus Master configuration

In the example, hexadecimal Modbus addresses 02 and 03 are transferred to the RipEX network on the Ethernet IP addresses. The Slave 04 is transferred via the cellular network and the destination IP

address is the mobile IP address of the remote MIDGE unit. The COM port must be COM2 with UDP port 8882, otherwise the remote MIDGE would not handle the traffic correctly.

RipEX Radio modem & Router **RACOM**

Values from: R1 Fast remote access ?

Interfaces ?

Radio	MAC	00:02:A9:BA:73:6B	IP	10.10.10.1	Mask	255.255.255.0
ETH	MAC	00:02:A9:BA:6F:83	IP	192.168.1.2	Mask	255.255.255.0

Routes ?

Destination	Mask	Gateway	Backup	Note	Active	Modify
192.168.2.0/24	255.255.255.0	10.10.10.2	Off	RipEX2	<input checked="" type="checkbox"/>	▼ Delete Add
192.168.3.0/24	255.255.255.0	10.10.10.3	Off	RipEX3	<input checked="" type="checkbox"/>	▲▼ Delete Add
10.203.3.0/24	255.255.255.0	192.168.1.1	Off	MIDGE	<input checked="" type="checkbox"/>	▲ Delete Add
Default		0.0.0.0	Off		<input type="checkbox"/>	Add

Backup ?

Name	Peer IP	Hysteresis [s]	SNMP Trap	Alternative paths			Note	Modify
				Gateway	Policy	Active		
								Add

Legend Up Down Unknown Currently used

Route for IP:

© RACOM, Mirova 1283, 592 31 Nove Mesto na Morave, Czech Republic, Tel.: +420 565 659 511, E-mail: racom@racom.eu www.racom.eu

Fig. 5.5: Central RipEX routing menu

In the Routing menu, three routes have to be added. First two are the LAN subnets of RipEX units and the third line defines the APN subnet (the gateway is the local MIDGE Ethernet IP address).

5.1.2. Remote RipEX Configuration

Both remote RipEX units have almost the same configuration so only R2 unit is described. Configure the correct IP addresses (together with RF frequency, ...) and set the COM1 port as the Modbus Slave as in the following screenshot.

Protocol ?

Protocol:

Mode of Connected device:

Broadcast accept:

Fig. 5.6: Remote RipEX Modbus Slave configuration

The only missing configuration is the Routing rule to the central RipEX subnet (192.168.1.1/24).

RipEX Radio modem & Router **RACOM**

Remote Connection Active

Values from: R2 Remote IP: 10.10.10.2 [Connect] [Disconnect] ?

Interfaces

Radio	MAC	00:02:A9:BA:54:2B	IP	10.10.10.2	Mask	255.255.255.0
ETH	MAC	00:02:A9:BA:50:43	IP	192.168.2.1	Mask	255.255.255.0

Routes

Destination	Mask	Gateway	Backup	Note	Active	Modify
192.168.1.1/24	255.255.255.0	10.10.10.1	Off		<input checked="" type="checkbox"/>	Delete Add
Default		0.0.0.0	Off		<input type="checkbox"/>	Add

Backup

Name	Peer IP	Hysteresis [s]	SNMP Trap	Alternative paths			Note	Modify
				Gateway	Policy	Active		
								Add

Legend: Up Down Unknown Currently used

[Apply] [Cancel] Route for IP: [] [Find] [Check routing] [Backup status]

© RACOM, Mirova 1283, 592 31 Nove Mesto na Morave, Czech Republic, Tel.: +420 565 659 511, E-mail: racom@racom.eu www.racom.eu

Fig. 5.7: Remote RipEX Routing menu

5.1.3. Central MIDGE Configuration

MIDGE **RACOM**

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

WWAN1

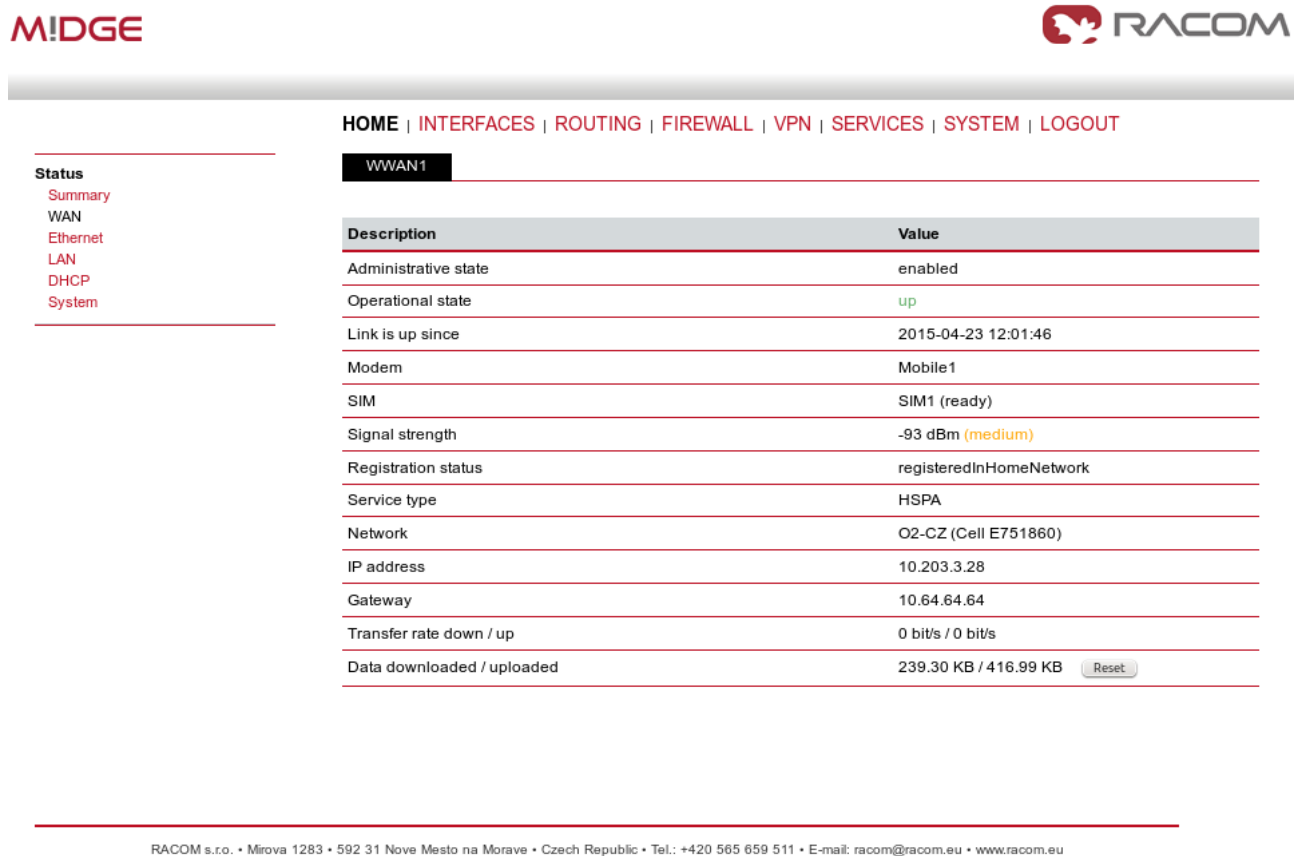
Description	Value
Administrative state	enabled
Operational state	up
Link is up since	2015-04-23 12:01:46
Modem	Mobile1
SIM	SIM1 (ready)
Signal strength	-93 dBm (medium)
Registration status	registeredInHomeNetwork
Service type	HSPA
Network	O2-CZ (Cell E751860)
IP address	10.203.3.28
Gateway	10.64.64.64
Transfer rate down / up	0 bit/s / 0 bit/s
Data downloaded / uploaded	239.30 KB / 416.99 KB [Reset]

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

Fig. 5.8: Central MIDGE Status menu

The central M!DGE just needs to be configured so it is connected via the private APN, no other special configuration is needed.

5.1.4. Remote M!DGE Configuration



The screenshot displays the M!DGE web interface. At the top left is the M!DGE logo, and at the top right is the RACOM logo. Below the logos is a navigation bar with the following links: HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT. The main content area is titled 'WWAN1' and contains a table with the following data:

Description	Value
Administrative state	enabled
Operational state	up
Link is up since	2015-04-23 12:01:46
Modem	Mobile1
SIM	SIM1 (ready)
Signal strength	-93 dBm (medium)
Registration status	registeredInHomeNetwork
Service type	HSPA
Network	O2-CZ (Cell E751860)
IP address	10.203.3.28
Gateway	10.64.64.64
Transfer rate down / up	0 bit/s / 0 bit/s
Data downloaded / uploaded	239.30 KB / 416.99 KB <input type="button" value="Reset"/>

At the bottom of the page, there is a footer with the following text: RACOM s.r.o. • Mirova 1283 • 592 31 Nove Mesto na Morave • Czech Republic • Tel.: +420 565 659 511 • E-mail: racom@racom.eu • www.racom.eu

Fig. 5.9: The remote M!DGE Status menu

After connecting to the private APN, only the Protocol server needs to be configured. In the INTERFACES – Serial Port, choose the Protocol server.

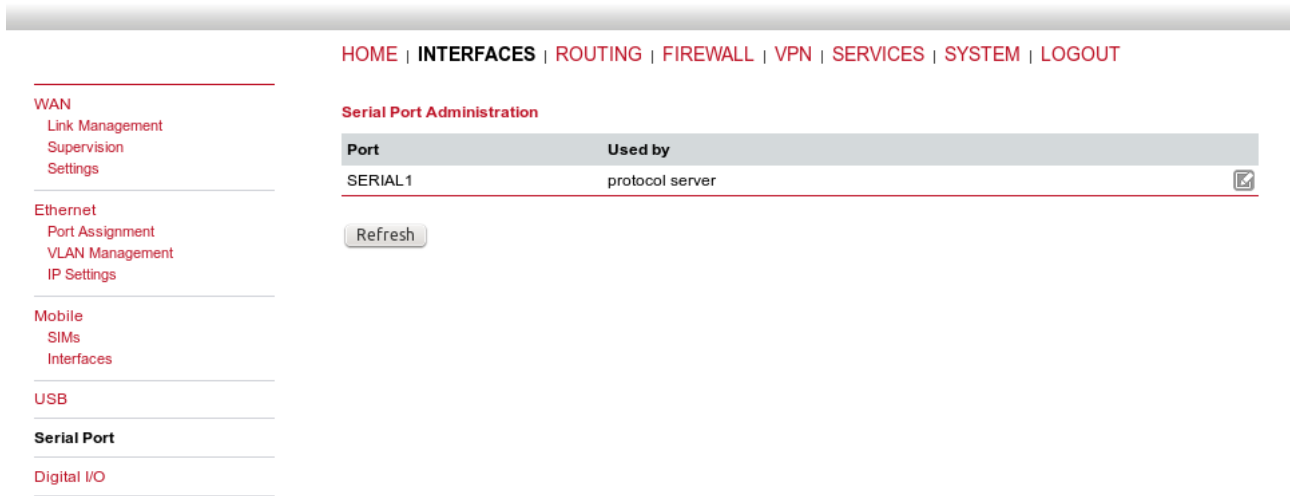


Fig. 5.10: Serial Port configuration

Set the desired port settings.

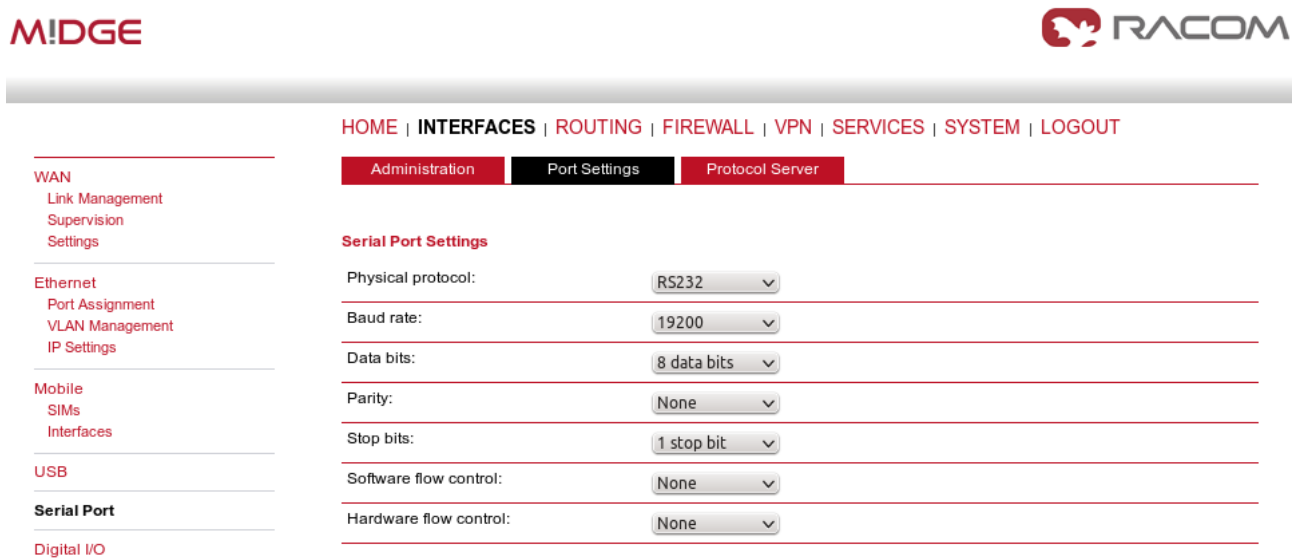


Fig. 5.11: Port settings

And as the last step, configure the Protocol server as the Modbus slave.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Administration | Port Settings | Protocol Server Help

Protocol Server

Protocol

Parameters

Mode of Connected device

Broadcast

WAN
Link Management
Supervision
Settings

Ethernet
Port Assignment
VLAN Management
IP Settings

Mobile
SIMs
Interfaces

USB

Serial Port

Digital I/O

Fig. 5.12: Modbus Slave M!DGE configuration

Now you should be able to poll the required information from all RTUs within the UHF/VHF or cellular network.



Note

If you do not use the private APN, you need to configure the VPN tunnels. See Chapter 2, *VPN Configuration Options* and Section 4.2, “SCADA Protocols – public APN”.

Appendix A. Revision History

Revision 1.0	2011-12-15
First issue	
Revision 2.0	2013-05-21
Added chapter M!DGE/MG102i CENTRE	
Revision 3.0	2013-07-18
Added Chapter 3, <i>Backup of WAN by the GSM Network</i>	
Revision 3.1	2013-06-04
Updated according to M!DGE/MG102i FW	
Revision 4.0	2015-07-20
Complete revision	