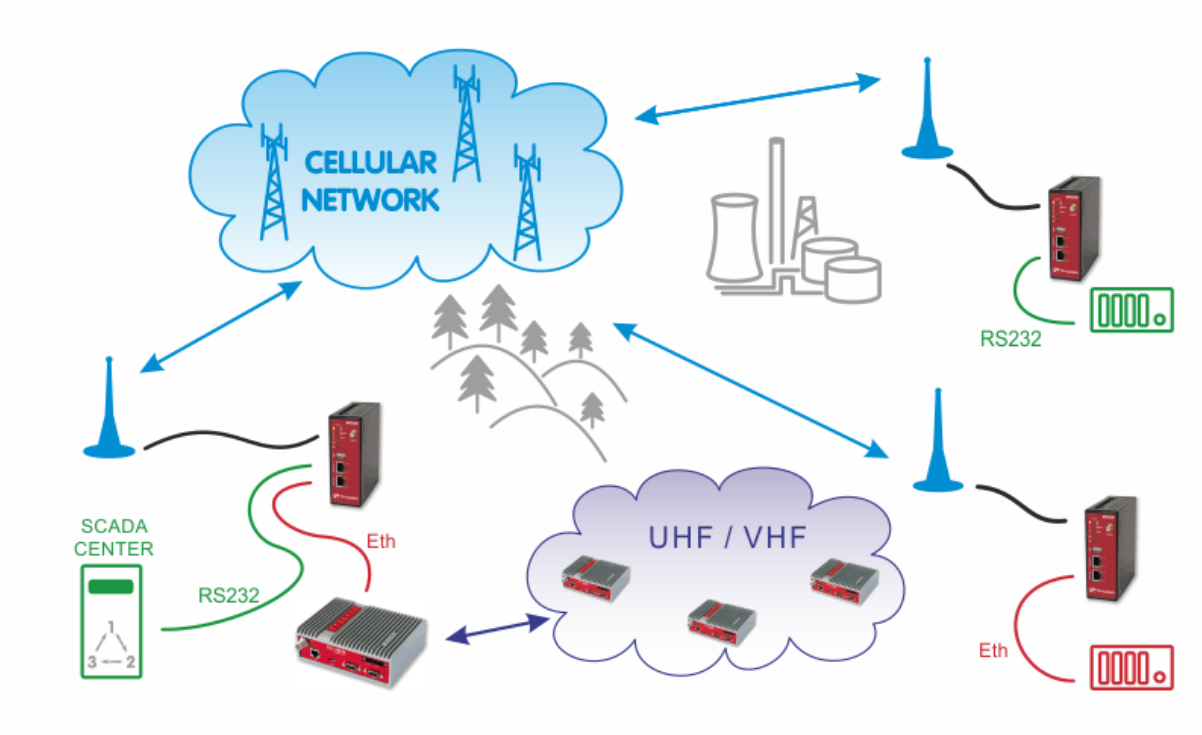
RACOM
RADIO DATA NETWORKS

Application notes



M!DGE/MG102i - Introduction

version 1.1
3/2/2018

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

www.racom.eu

Table of Contents

Introduction

Thank you for your interest in our cellular 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 *Manual*[1] 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 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 "*A Standalone M!DGE/MG102i in the Center*[2]" and Section "*A leased line to the Cellular Network Center*[3]" in the *Typical Usage*[4] application note.

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

[1] http://www.racom.eu/eng/products/m/midge1/index.html
[2] http://www.racom.eu/eng/products/m/midge/app/typuse/in_centre.html
[3] http://www.racom.eu/eng/products/m/midge/app/typuse/leased_line.html
[4] http://www.racom.eu/eng/products/m/midge/app/typuse/index.html

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 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.

Appendix A. Revision History

Revision 1.0 2018-01-18
First issue

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