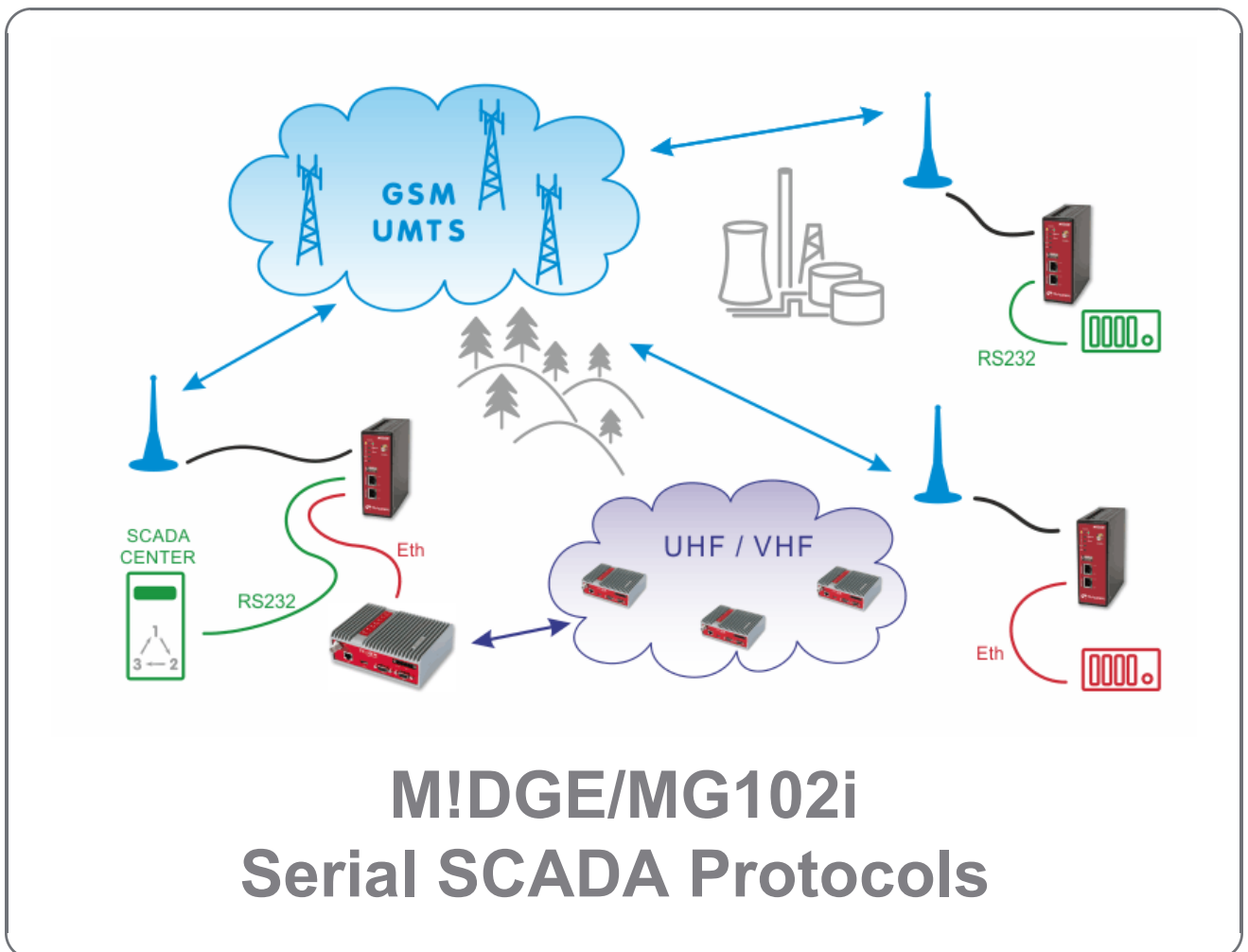


Application notes



version 1.0
12/7/2017

Table of Contents

Introduction	5
1. SCADA Protocols – private APN	6
1.1. APN Configuration	6
1.2. SCADA Master Configuration	8
1.3. SCADA Slave Configuration	9
1.4. Troubleshooting	10
2. SCADA Protocols – public APN	12
2.1. APN Configuration	12
2.2. SCADA Master Configuration	13
2.3. SCADA Slave Configuration	15
2.4. Troubleshooting	15
A. Revision History	16

Introduction

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 Chapter 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 Chapter 2, *SCADA Protocols – public APN* for more details.

1. SCADA Protocols – private APN

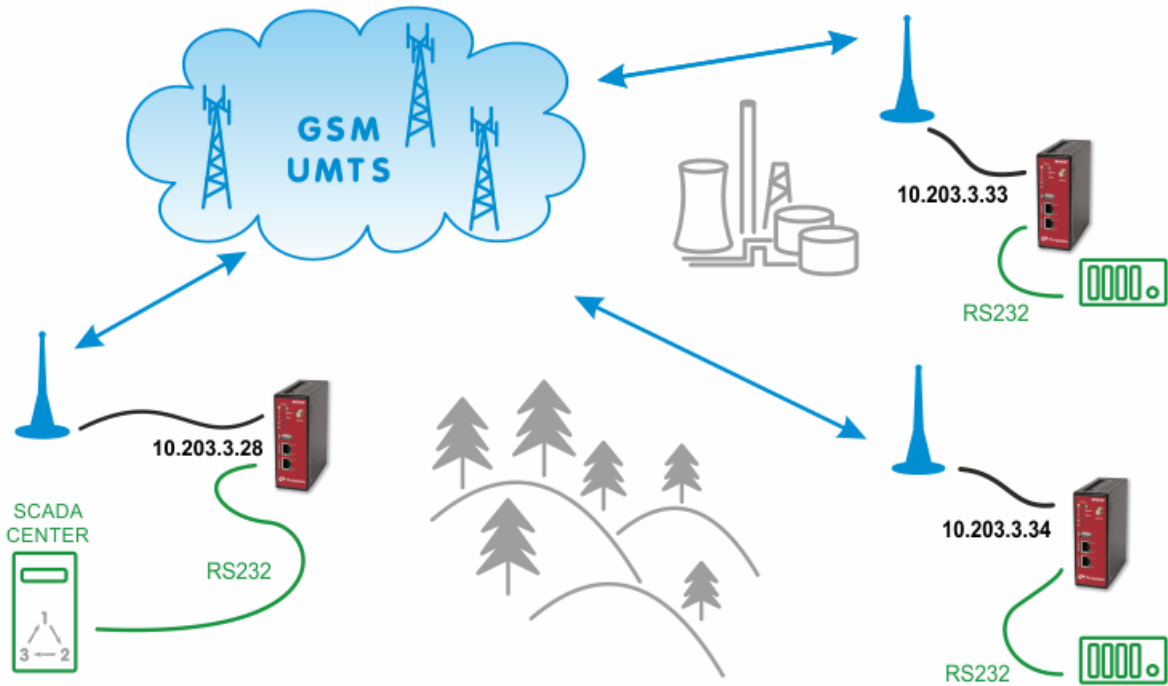


Fig. 1.1: SCADA Solution within Private APN

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. 1.2: 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"/>

Fig. 1.3: 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.

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.

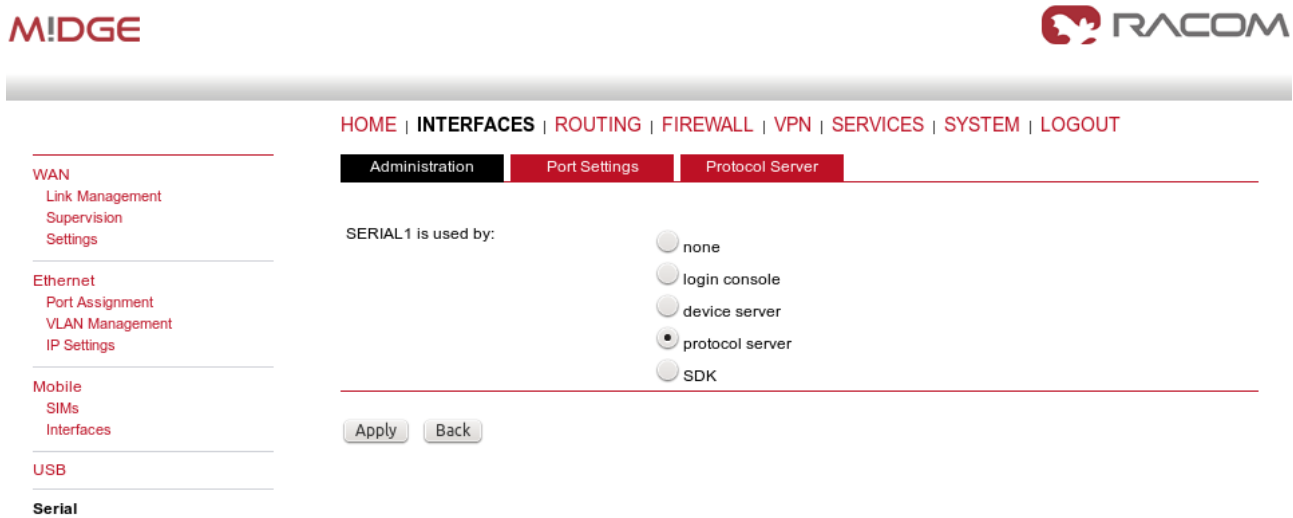


Fig. 1.4: Master Protocol server configuration

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

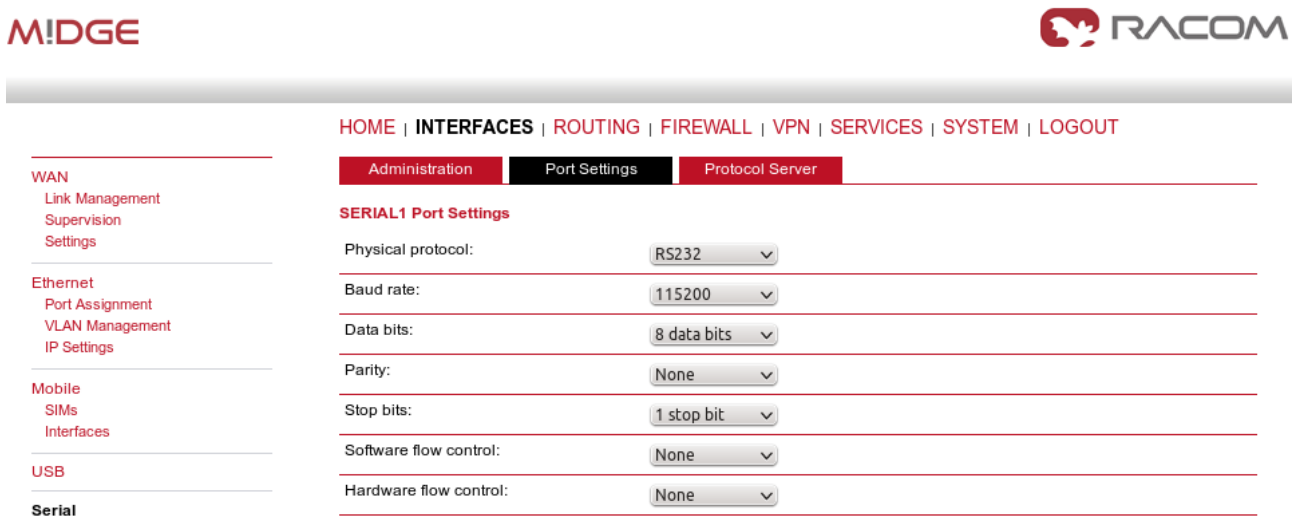


Fig. 1.5: Port Settings



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. 1.6: Modbus Master configuration

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

Apply

Fig. 1.7: Modbus Slave configuration

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).

MIDGE

RACOM

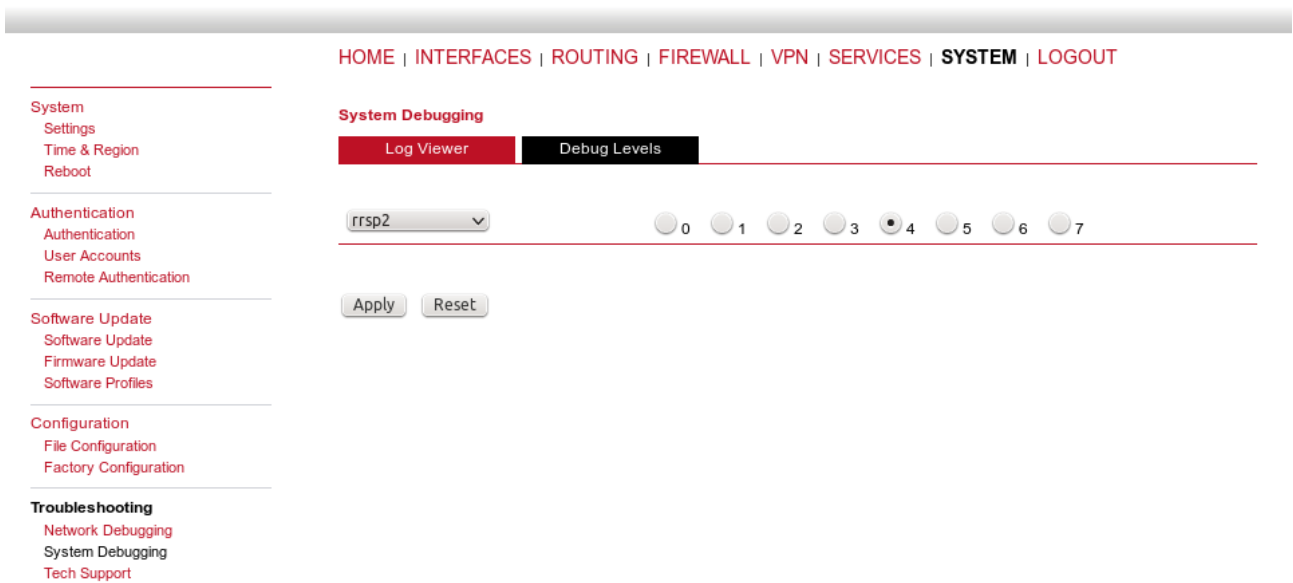


Fig. 1.8: Debug level of rrsp2 daemon

- 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. 1.9: Tcpdump via Web interface

**Note**

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

2. SCADA Protocols – public APN

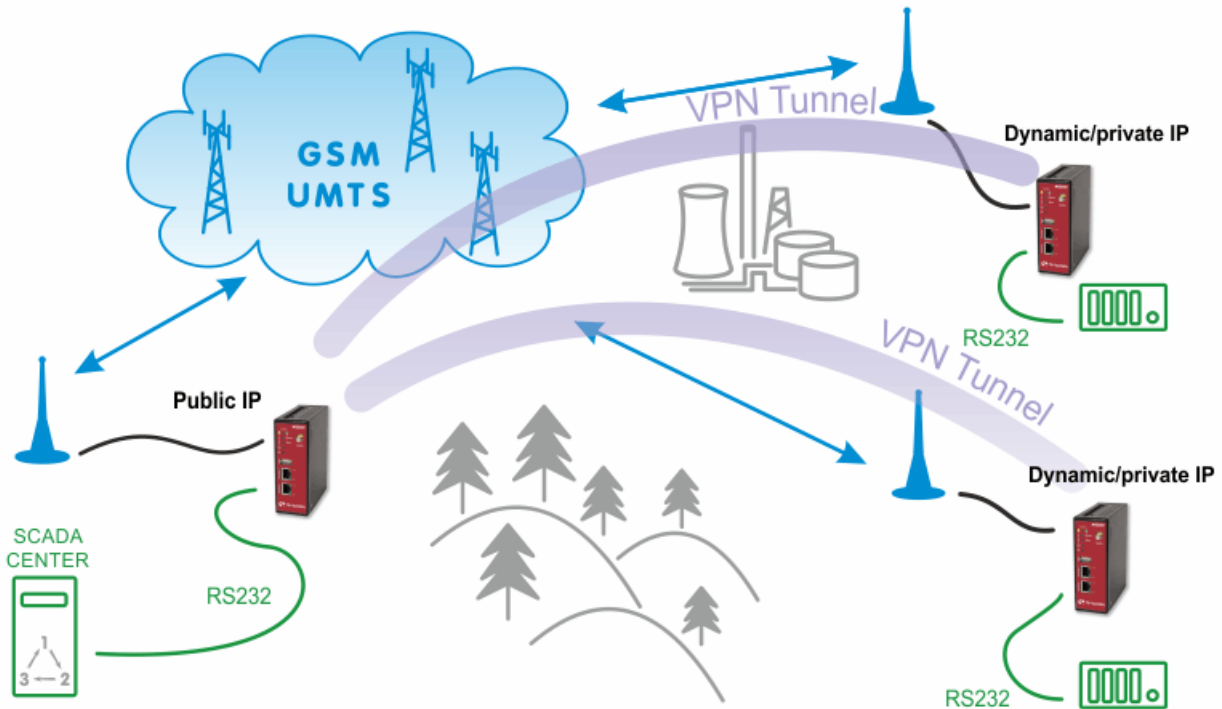


Fig. 2.1: Public APN SCADA configuration

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

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. 2.2: 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 ??? 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 configuration fields are as follows:

- Transport Network:** Network: 10.8.0.0, Netmask: 255.255.255.0
- Client Networks:** Select client: Client1
- Tunnel address:** Radio buttons for 'dynamic' and 'fixed'. The 'fixed' option is selected and highlighted with a blue circle. The input field next to it contains '10.8.0.6'.
- Client network:** Radio buttons for 'none' and 'specify'.

An 'Apply' button is located at the bottom of the configuration area.

Fig. 2.3: 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.

2.2. SCADA Master Configuration

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

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	10.8.0.6	COM(8882)	Remote MIDGE A	<input checked="" type="checkbox"/>	↓ - +
b	10.8.0.10	COM(8882)	Remote MIDGE B	<input checked="" type="checkbox"/>	↑ - +

Apply

Fig. 2.4: 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 MIDGE 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.

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.

2.4. Troubleshooting

The troubleshooting is the same as explained in the Section 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.

Appendix A. Revision History

Revision 1.0	2017-12-07
First issue	