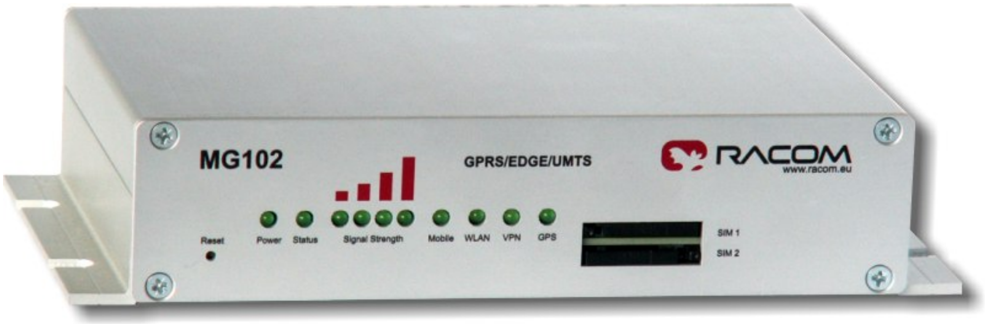
RADIO DATA NETWORKS

Operating manual



GPRS/EDGE/UMTS routers M!DGE, MG102

1.1
11/24/2011

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

List of Figures

List of Tables

Introduction

Thank you for purchasing M!DGE/MG102 Wireless Router from Racom. This chapter gives you an introduction to M!DGE/MG102 Wireless Router. The following chapters describe the installation and the configuration.

In next description is used the notation **router** instead of **GPRS/EDGE/UMTS router**.

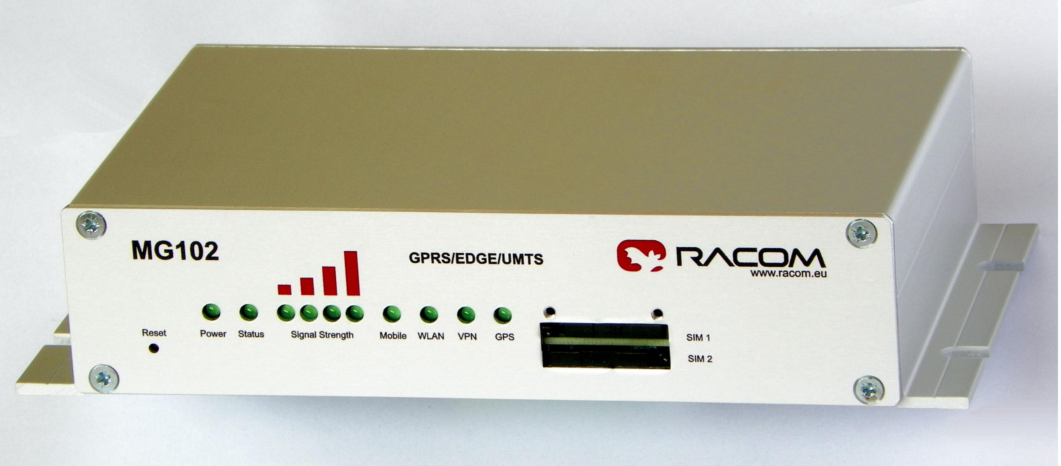


Fig. 1: Router MG102

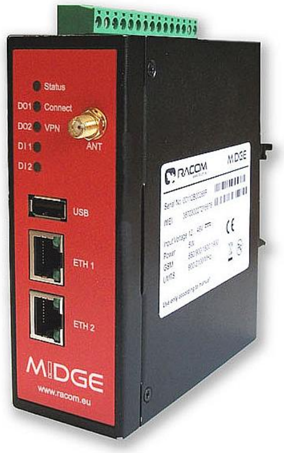


Fig. 2: Router M!DGE

1. Product description

1.1. The M!DGE – MG102 Family

The handling of the different MG models is very similar. All models run MG Software which adapts itself to the MG Hardware. The software will not allow you to configure options the hardware does not offer (e.g. GPS or Digital I/O). The below table shows the hardware varieties:

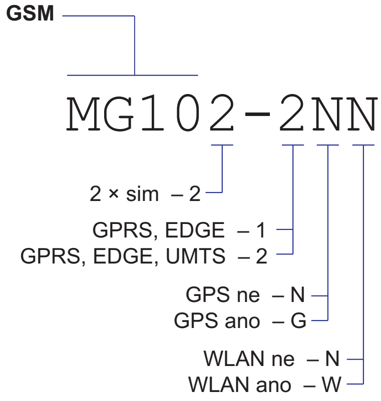
Tab. 1.1: MG Model Overview

	M!DGE	**MG102-1NN**	**MG102-1GN**	**MG102-2NN**	**MG102-2GN**	**MG102-2NW**	**MG102-2GW**
GSM, GPRS, EDGE	yes	yes	yes	yes	yes	yes	yes
UMTS, HSDPA, HSUPA	yes	–	–	yes	yes	yes	yes
WLAN	–	–	–	–	–	yes	yes
SIM card sockets	1	2	2	2	2	2	2
Ethernet ports	2	4	4	4	4	4	4
Serial ports	1	1	1	1	1	1	1
Integrated GPS receiver	–	–	yes	–	yes	–	yes
Digital inputs / outputs	2/2	–	–	–	–	–	–

Following models are in standard production:

- M!DGE
- MG102-1NN and MG102-1GN
- MG102-2NN and MG102-2GN

Other models are available on demand.



Example:

MG102-2GN

= GPRS router MG102,
includes two SIM card – works in two networks,
works in 850/900/1800/1900/2100 MHz bands,
modem has an integrated GPS receiver

Fig. 1.1: Production code MG102

1.2. Product Description M!DGE

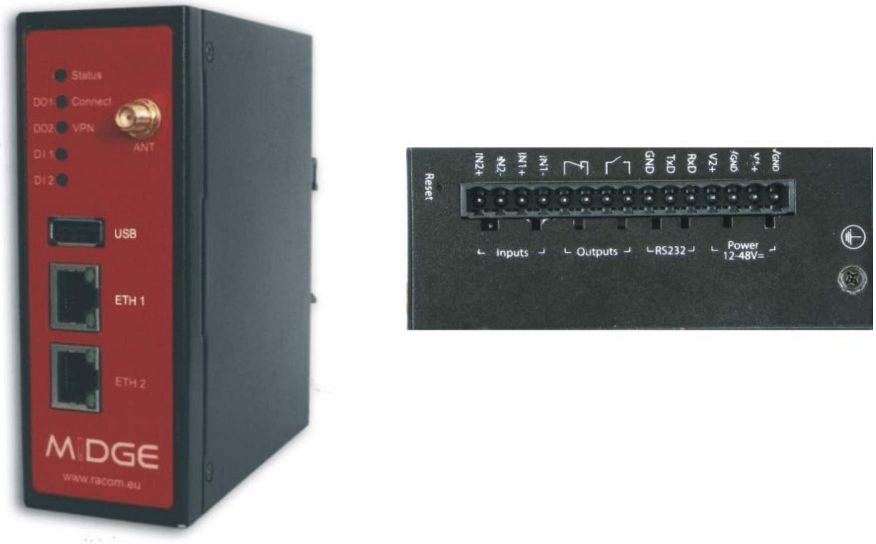


Fig. 1.2: Front panel and terminal panel of M!DGE

The following table describes the meaning of the status indicators:

Tab. 1.2: M!DGEs interfaces and status indicators

Label	Color	State	Function
Status	green	solid	The caption on the green side apply start up, maintenance
		blinking slowly	The caption on the yellow side apply start up, maintenance
Mob	green yellow red	green on	Very good GSM signal
		yellow on	Good GSM signal
		red on	Bad GSM signal
VPN	green	on	VPN connection is up
		off	VPN connection is down
In1	yellow	on	Input set
		off	Input not set
In2	yellow	on	Input set
		off	Input not set
Out1	yellow	on	Closed
		off	Opened
Out2	yellow	on	Closed
		off	Opened
USB	—	—	USB Host Port. Support for memory sticks for configuration and software update.
Ethernet 1	—	—	First Ethernet Port. Can be used as LAN or WAN Port
Ethernet 2	—	—	First Ethernet Port. Can be used as LAN or WAN Port
Mobile	—	—	SMA female connector for GSM/UMTS antenna 50 Ω

Please find the description of each interface in the following table:

1.2.1. Pin Assignments

Screw terminal

Tab. 1.3: Pin assignment of screw terminal

pin	signal
1	V_{GND}
2	V1+ (12–48 V=)
3	V_{GND}
4	V2+ (12–48 V=)
5	RxD
6	TxD
7	GND
8	Out1: Dry contact relay Normally open with M!DGE without powering
9	
10	Out2: Dry contact relay Normally open with M!DGE without powering
11	
12	DI1−
13	DI1+
14	DI2−
15	DI2+

1.3. Product Description MG102

1.3.1. The Front Panel

The front panel has 10 status indicators. In addition there are two SIM card slots and a reset button at the front panel.

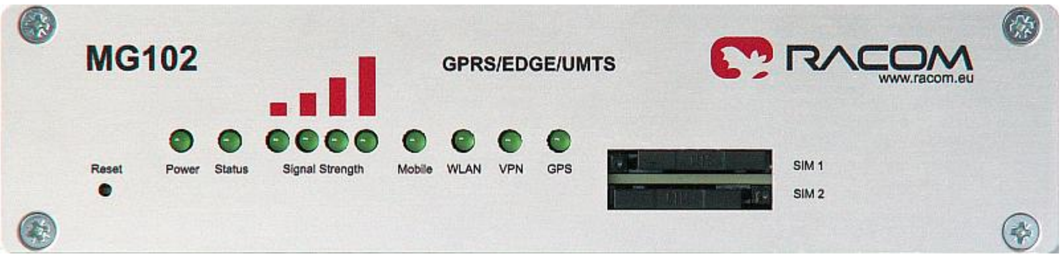


Fig. 1.3: The Front Panel

The following table describes the components on the front panel:

Tab. 1.4: Components on the front panel

Panel	Label	Color	State	Function
Front	Power	green	on	The device is powered
			off	Power is missing
Front	Status	green	blinking slowly	This indicates one of the following conditions: - the device is starting up - loading a new configuration - factory reset initiated by Web Manager
			on	The device is ready
			blinking fastly	Restart triggered by watchdog
			off	The device does not start up
Front	Signal Strength	green	on	1 LED on: weak signal 2 LEDs on: medium signal 3 LEDs on: strong signal 4 LEDs on: very strong signal
			off	No or insufficient signal
			running	Software update
Front	UMTS/GSM	green	blinking slowly	Mobile connection is being established
			on	Mobile connection is up
			off	Mobile connection is down
Front	WLAN	green	blinking slowly	WLAN connection is being established
			on	WLAN connection is up
			off	WLAN connection is down
Front	VPN	green	on	VPN connection is up
			off	VPN connection is down
Front	GPS (MG102 -xGx only)	green	on	Service is enabled and valid GPS data is received and transmitted
			off	No GPS data transmitted (not available or service disabled)
Front	Reset	–	–	Restart: press this button when the status LED is on Factory reset: press and hold this button for at least 5 seconds
Front	SIM1	–	–	SIM socket 1
Front	SIM2	–	–	SIM socket 2

1.3.2. The Back Panel

The back panel has the interfaces described in the table below:

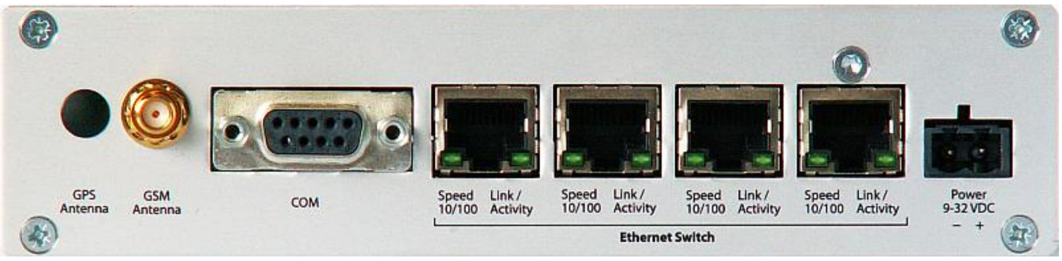


Fig. 1.4: The Back Panel of 2009 model

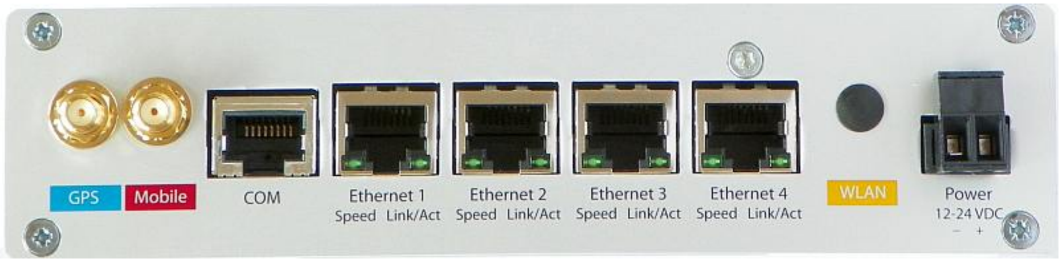

GPS
Mobile
COM
Ethernet 1 Speed Link/Act
Ethernet 2 Speed Link/Act
Ethernet 3 Speed Link/Act
Ethernet 4 Speed Link/Act
WLAN
Power 12-24 VDC
– +

Fig. 1.5: The Back Panel of 2010 model

Tab. 1.5: Components on the back panel

Panel	Label	Color	State	Function
Back	GPS Antenna (MG102-xGx only)	–	–	GPS antenna connector Impedance: 50 Ω Connector: SMA female MG102-xGx support passive GPS antennas only
Back	UMTS / GSM Antenna	–	–	UMTS / GSM antenna connector Impedance: 50 Ω Connector: SMA female
Back	COM	–	–	Sub-D 9 (model 2009) or RJ45 port (model 2010) RS232 (default) or RS485 (configurable)
Back	Ethernet Ports	–	–	4 Ethernet ports – 4port Eth switch / 4 LANs/1WAN+3LANs according to setting The default IP address is set to `192.168.1.1.`
Back	Power	–	–	Voltage feed connector (9–32 VDC)
Back	Link/Activity (Ethernet Ports)	green	on	Physical link
			off	No physical link
			flashing	Data transmission
Back	Speed 10/100 (Ethernet Ports)	green	on	Data rate 100 MBit/s
			off	Data rate 10 MBit/s

1.4. M!DGE/MG102 Software

All M!DGE/MG102 Wireless Routers run M!DGE/MG102 Software. Software offers the following key features:

- Interfaces and Connection Management (section Section 3.1.4, “Interfaces”)
  - Dial-out (on demand, permanent)
  - Connection Monitoring
  - Fallback to backup profile or SIM
  - SIM and PIN management
  - Automatic or manual network selection
- Routing (section Section 3.1.5, “Routing”)
  - Static Routing
  - NAPT / Port Forwarding
- Security / Firewall (section Section 3.1.6, “Firewall”)
  - NAPT / Port Forwarding
  - Access Control Lists
  - Stateful Inspection Firewall
- Virtual Private Networking (VPN) (section Section 1.5.3, “Virtual Private Networks (VPN)”)
  - OpenVPN Client
  - PPTP Server
  - IPsec Peer
  - Dial-in Server
- Services (section Section 3.1.8, “Services”)
  - COM Server (Tunneling of the serial line over IP)
  - Modbus-RTU to Modbus-TCP Gateway
  - DHCP Server
  - DNS Proxy Server
  - Dynamic DNS Client
  - E-mail Client
  - Notification via E-mail and SMS
  - SMS Client
  - SSH Server
  - SNMP Agent
  - Telnet Server
  - Unstructured Supplementary Service Data (USSD)
  - Web Server
  - GPS Daemon (MG102-xGx only)
- System Administration (section Section 3.1.9, “System”)
  - Configuration via Web Manager
  - Configuration via Command Line Interface (CLI) accessible via Secure Shell (SSH) and telnet
  - Batch configuration with text files
  - User admnistration
  - Troubleshooting tools
  - Over the air software update

1.5. Application Overview

M!DGE/MG102 is an access router for mobile telecom networks. Router can hook up a whole local area network to the mobile telecom network. Certainly M!DGE/MG102 can also be used to attach a single device.

1.5.1. Mobile Internet Access

M!DGE/MG102 can be used for mobile Internet access. Supported services include:

- Universal Mobile Telecommunications System (UMTS), High Speed Packet Access (HSPA) including HSDPA and HSUPA
- General Packet Radio Service (GPRS), Enhanced Data rates for GSM Evolution (EDGE)
- Circuit Switched Data (CSD)

1.5.2. Access to a Remote Network

M!DGE/MG102 can be used to access a remote network. Possible setups are:

- Access via public IP address
- Access via M!DGE/MG102 initiated VPN
- Access via CSD Dial-in

1.5.3. Virtual Private Networks (VPN)

M!DGE/MG102 supports various types of VPN technologies. The following components are included:

- OpenVPN client
- IPsec initiator
- PPTP server
- Dial-in server

2. Installation

2.1. Environmental Conditions

The following precaution must be taken before installing M!DGE/MG102:

- Avoid direct solar radiation
- Protect the device from humidity, steam and aggressive fluids
- Grant sufficient circulation of air around M!DGE/MG102
- For indoor use only
- Temperature range MG102: −25 °C to +70 °C
- Temperature range M!DGE: −25 °C to +70 °C
- Humidity: 0 to 95 % (non condensing)
- Altitude up to 4000 m (MG102)
- Mains Voltage Ripple less than ±10 % of the nominal voltage
- Overvoltage Category: II
- Pollution Degree: 2

2.2. Installation of the Router

MG102 is designed for mounting to a panel using through holes or to be put on a worktop for installing to DIN rails use DIN rail bracket. M!DGE is designed for mounting to a DIN rail. M!DGE is designed for mounting to a DIN rail. Please consider the safety instructions and the environmental conditions.

2.2.1. Installation of the SIM Card(s)

The MG102 router incorporates two separate SIM card sockets so that if your application demands it, you may install SIM cards for two different networks of two different mobile network operators. If you only use one SIM card insert it in SIM socket 1.

M!DGE has only one SIM card socked. For instalation of SIM card the cover has to be removed. Make sure the SIM is suitable for data transmission.

2.2.2. Installation of the UMTS/GSM Antenna

MG102 Wireless Routers will only operate reliably over the GSM network if there is a good signal. For many applications the flexible stub antenna provided will be suitable but in some circumstances it may be necessary to use a remote antenna with an extended cable to allow the antenna itself to be positioned to provide the best possible signal reception. MG102 can supply a range of suitable antennas. Consider the effects caused by Faraday cages such as large metal surfaces (elevators, machine housings, etc.), close meshed iron constructions. Fit the antenna or connect the antenna cable to the GSM antenna connector.

Note

Be sure that the antenna was installed according to the recommendation of antenna producer and all parts of antenna and antenna holder was properly fasten.

2.2.3. Installation of the GPS Antenna

MG102 require passive GPS antennas. The router needs to put the antenna with a good view of satellites.

2.2.4. Installation of the Local Area Network

Up to four Ethernet devices can directly be connected to the MG102, maximal two to M!DGE.

2.2.5. Installation of the Power Supply

MG102 can be powered with the included power supply or another external source supplying between 9 and 32 Volts DC (10–55 Volts DC M!DGE). M!DGE/MG102 is for use with certified (CSA or equivalent) power supply, which must have a limited and SELV circuit output.

2.3. GPRS/EDGE/UMTS router assembly

Routers M!DGE/MG102 are special devices which require skilled assembly. For subsequent maintenance RACOM specially trains the user’s skilled staff and as an additional aid provides them with Operating regulations for radio data networks and Firmware – Documentation. Only the manufacturer, RACOM s.r.o. Mírová 1283, 592 31 Nové Město na Moravě, Czech Republic, Tel.: +420 565659511, is entitled to repair any devices.

⚠ **Important**

CAUTION! Danger of explosion upon replacing the incorrect type of battery. Follow the manufacturers instructions for handling used batteries.

3. Configuration

M!DGE/MG102 holds different configurations, such as the factory configuration and the user configuration. The user configuration can be modified by the user as follows:

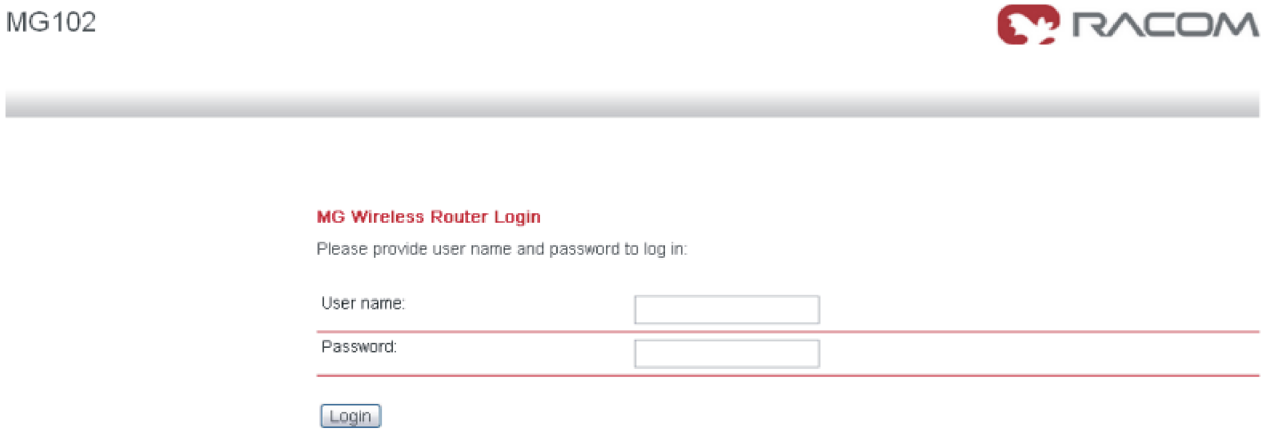
- Using the forms on the web pages of Web Manager (chapter Section 3.1, “Configuration via the M!DGE/MG102 Web Manager”)
- Upload a new configuration file using the Web Manager (chapter Chapter 3, *Configuration*)
- Using the M!DGE/MG102 Command Line Interface (chapter Section 3.3, “Configuration via Command Line Interface (CLI)”)
- M!DGE can be configured via a USB stick with a prepared configuration file.

If you are new to M!DGE/MG102 we recommend configuring it using the M!DGE/MG102 Web Manager.

3.1. Configuration via the M!DGE/MG102 Web Manager

The M!DGE/MG102 Web Manager can always be reached via the Ethernet interface. After the successful setup the Web Manager can also be accessed via the mobile interface. Any up to date web browser may be used. Any web browser supporting JavaScript may be used. By default the IP address of the Ethernet interface is 192.168.1.1, the web server runs on port 80.

3.1.1. Initial Access to the Web Manager and Password Definition



MG Wireless Router Login

Please provide user name and password to log in:

User name:

Password:

The minimum configuration steps usually include:

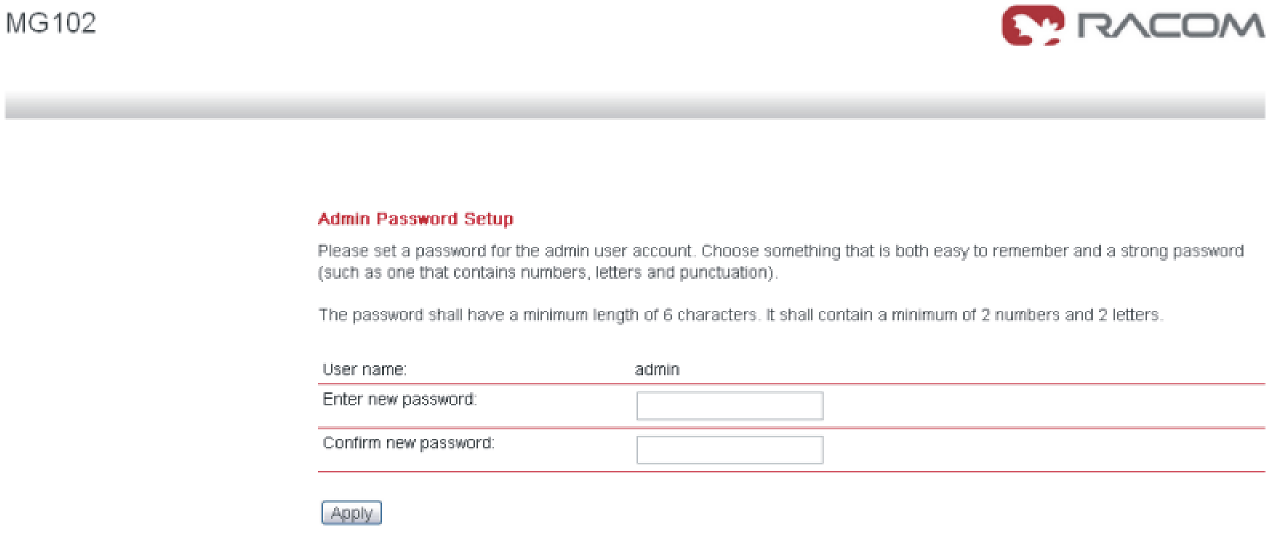
1. defining the admin password
2. entering the PIN code for the SIM card
3. configuring the Access Point Name (APN)
4. start the mobile connection

Step	Description
1.	Please connect the Ethernet interfaces of your computer and the M!DGE/MG102.
2.	If not yet enabled, please enable the Dynamic Host Configuration Protocol (DHCP) so that your computer can lease an IP address from M!DGE/MG102. Wait a moment until your PC has received the parameters (IP address, subnet mask, default gateway, DNS server). How to do using Windows XP: Start > Connect To > Show all connections > Local Area Connection > Right Click > Properties > Internet Protocol (TCP/IP) > Properties > Obtain an IP address automatically. Alternative: Instead of using the DHCP, configure a static IP address on your PC (e.g. `192.168.1.10` mask 255.255.255.0) so that it is operating in the same subnet as the M!DGE/MG102. The factory default IP address is `192.168.1.1` The default subnet mask is `255.255.255.0.`
3.	Start a Web Browser on your PC. Type the M!DGE/MG102 IP address in the address bar: `http://192.168.1.1`
4.	Follow the instructions of the Web Manager to configure the device.

3.1.2. Initial Access for the admin user account

Please set a password for the admin user account. Choose something that is both easy to remember and a strong password (such as one that contains numbers, letters and punctuation).

The password shall have a minimum length of 6 characters. It shall contain a minimum of 2 numbers and 2 letters.



Admin Password Setup

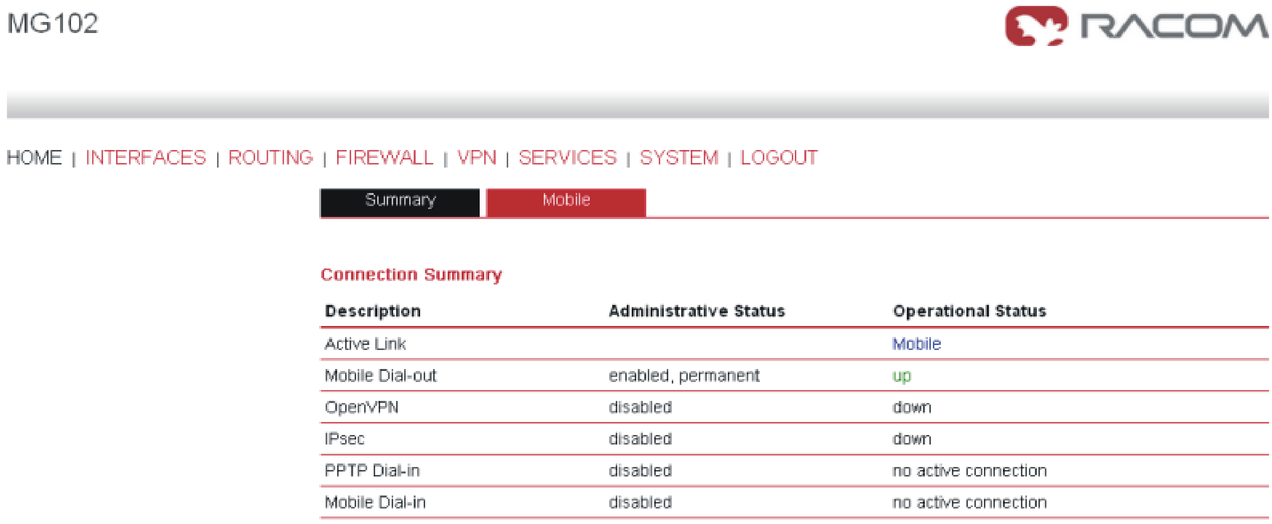
Please set a password for the admin user account. Choose something that is both easy to remember and a strong password (such as one that contains numbers, letters and punctuation).

The password shall have a minimum length of 6 characters. It shall contain a minimum of 2 numbers and 2 letters.

User name:	admin
Enter new password:	
Confirm new password:	

3.1.3. Home

This page gives you a system overview. It helps you when initially setting up device but also functions as dashboard during normal operation.


MG102
RACOM
HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT
Summary
Mobile

Connection Summary

Description	Administrative Status	Operational Status
Active Link		Mobile
Mobile Dial-out	enabled, permanent	up
OpenVPN	disabled	down
IPsec	disabled	down
PPTP Dial-in	disabled	no active connection
Mobile Dial-in	disabled	no active connection

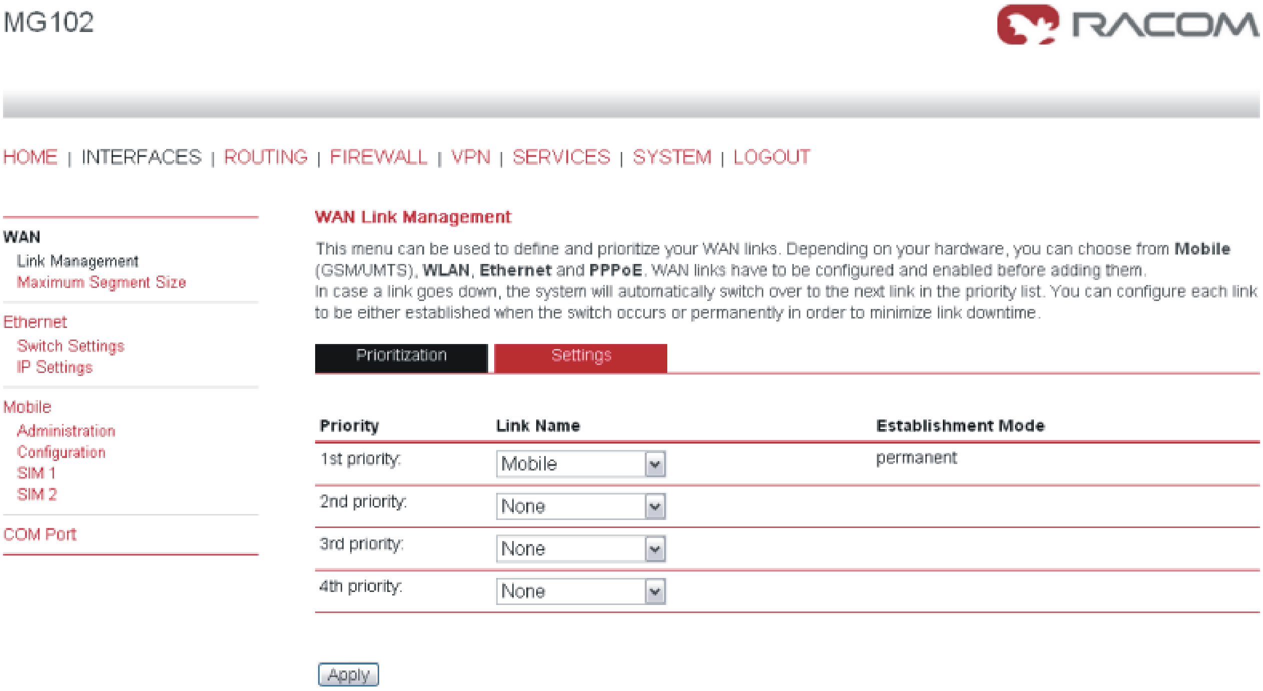
3.1.4. Interfaces

In the section the physical Interfaces of M!DGE/MG102 are configured. Details for all enabled connections are displayed on its own section Appendix A, *Connectors and Cables*

WAN

- **Link Management**

  FW 3.4 introduces a WAN link manager. Depending on your hardware, you can choose from Mobile (GSM/UMTS), WLAN, Ethernet and PPPoE. WAN links have to be configured and enabled before adding them. In case a link goes down, the system will automatically switch over to the next link in the priority list. You can configure each link to be either established when the switch occurs or permanently in order to minimize link downtime.



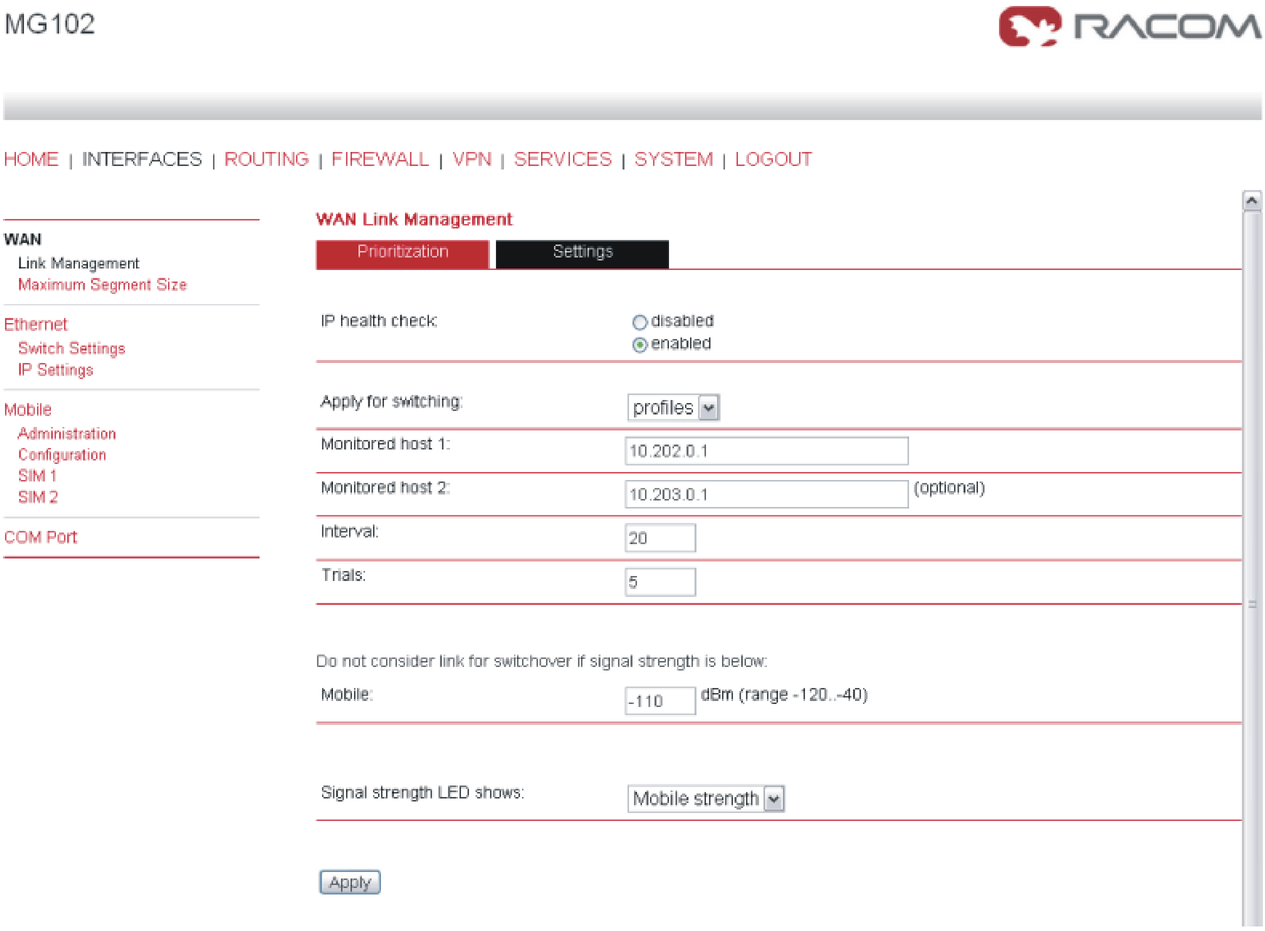
WAN Link Management

This menu can be used to define and prioritize your WAN links. Depending on your hardware, you can choose from **Mobile** (GSM/UMTS), **WLAN**, **Ethernet** and **PPPoE**. WAN links have to be configured and enabled before adding them.
In case a link goes down, the system will automatically switch over to the next link in the priority list. You can configure each link to be either established when the switch occurs or permanently in order to minimize link downtime.

Priority	Link Name	Establishment Mode
1st priority:	Mobile	permanent
2nd priority:	None	
3rd priority:	None	
4th priority:	None	

Step	Description
1st priority:	This link will be used if ever possible.
2nd priority:	The first fallback technology. You can hold it ready (faster) or establish it only when the fallback actually occurs.
3rd priority:	The second fallback technology. You can hold it ready (faster) or establish it only when the fallback actually occurs.
4th priority:	The third fallback technology. You can hold it ready (faster) or establish it only when the fallback actually occurs.

- **Link Management – Setings**



WAN Link Management

IP health check: ○ disabled ● enabled

Apply for switching: profiles

Monitored host 1: 10.202.0.1

Monitored host 2: 10.203.0.1 (optional)

Interval: 20

Trials: 5

Do not consider link for switchover if signal strength is below:

Mobile: -110 dBm (range -120..-40)

Signal strength LED shows: Mobile strength

IP health check – this feature is prepared for switching between profiles or lines. MG102 is checking availability of Monitored host 1 (optionaly 2). If the host (hosts) is (are) not reachable the second profile (link) will be switched to.

Note

This functionality has a close relationship with Connection Supervisor.

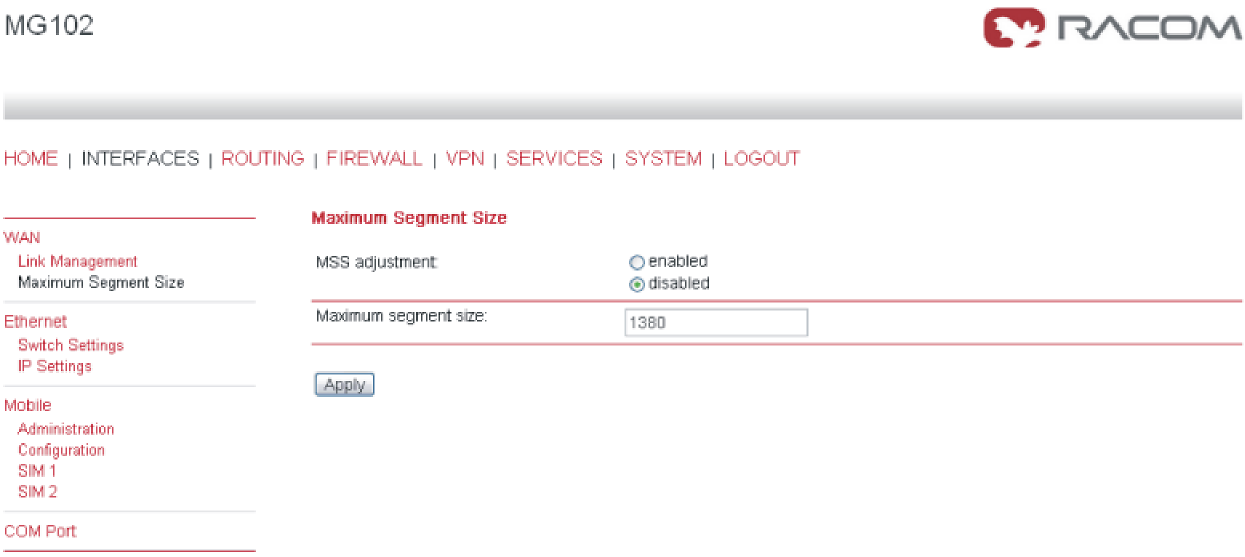
Parameter	Description
Mobile:	The required signal strength for GSM/UMTS in order to qualify the link as a fallback alternative.
WLAN:*	The required signal strength for WLAN in order to qualify the link as a fallback alternative.
Signal strength LED shows:	Specify whether the Signal strength LEDs on the NB2500/NB2600/NB2600R front panel shall indicate the WLAN or mobile signal strength.

Note

WLAN is available only with relevant HW.
IP health check option is not used at M!DGE.

- **Maximum Segment Size**

  The maximum segment size (MSS) is the largest amount of data, specified in bytes, that a computer or communications device can handle in a single, unfragmented piece. For optimum communications, the number of bytes in the data segment and the headers must not add up to more than the number of bytes in the maximum transmission unit (MTU).



Maximum Segment Size

MSS adjustment ○ enabled ● disabled

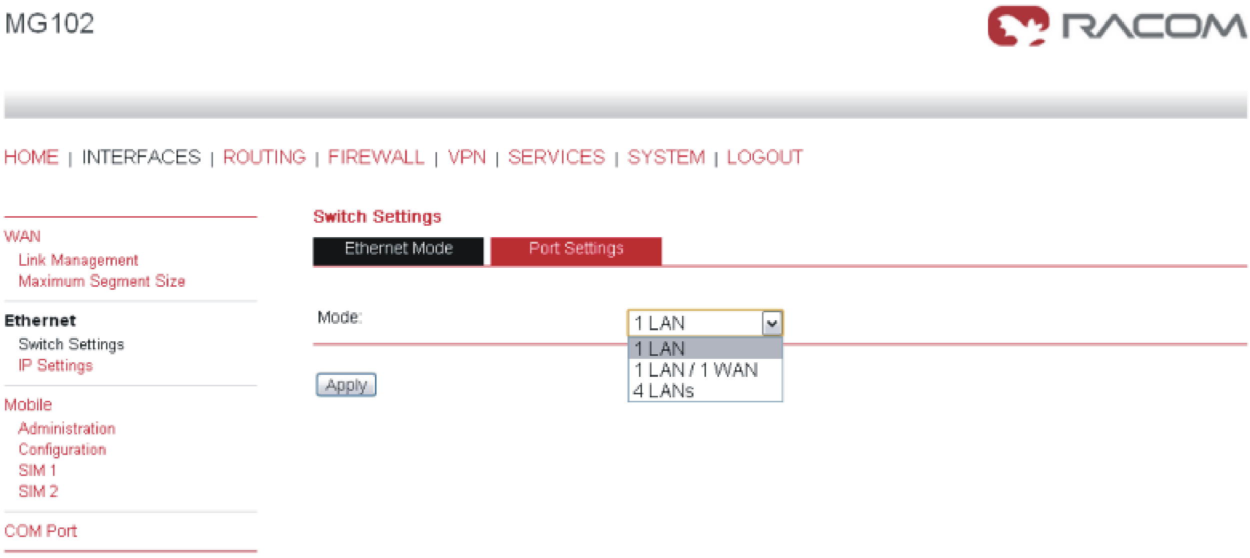
Maximum segment size: 1380

Parameter	Description
MSS adjustment:	The maximum segment size (MSS) for the mobile interface

Ethernet Interface

- **Switch Settings**

  Choose whether you want to have all Ethernet ports in one LAN (default) or apply a subnet for every Ethernet port or have a WAN port separated.



Switch Settings

Mode: 1 LAN

Combined mode (LAN)

Ports	Network	MG102 IP Address
Port 1, 2, 3, 4	192.168.1.0/24	192.168.1.1

Mixed mode (LAN / WAN)

Ports	Network	MG102 IP Address
Port 1–3 (MG102)	192.168.1.0/24	192.168.1.1
Port 4 (MG102)	192.168.2.0/24	192.168.2.1

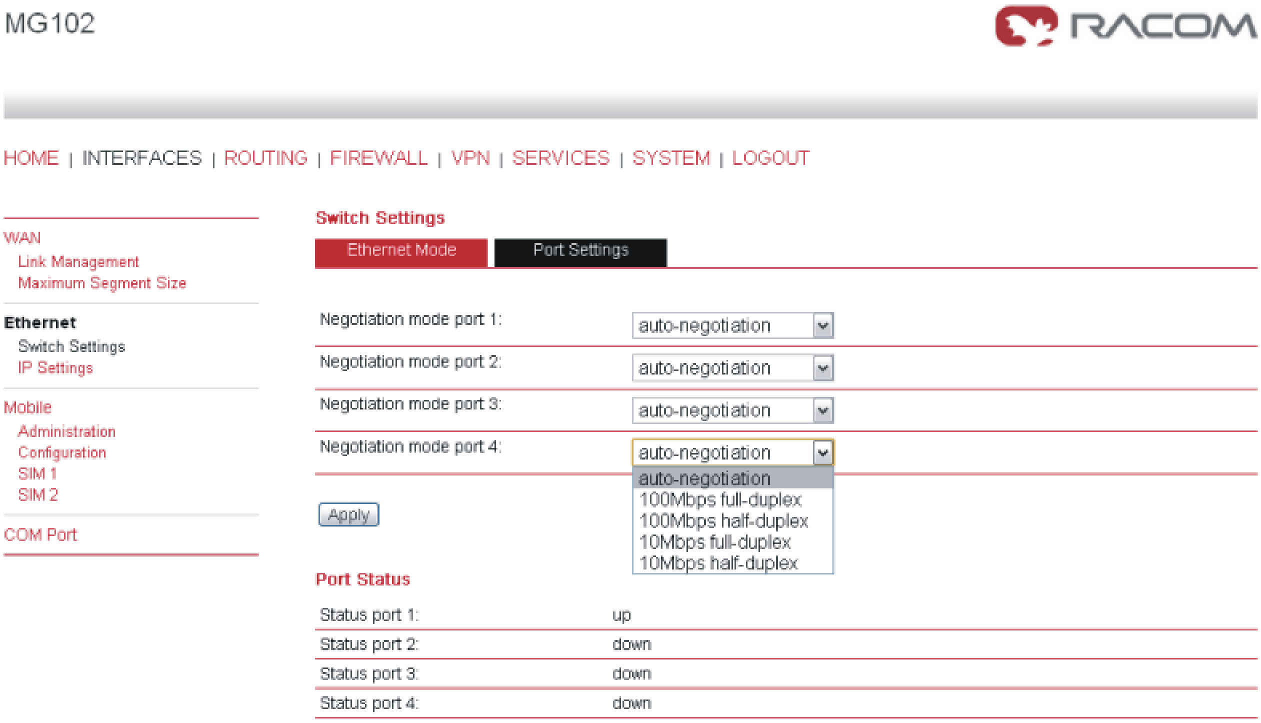
M!DGE uses two Ethernet interfaces. It is possible set the same LAN for both or LAN1 and LAN2 or LAN and WAN combination.

Separated mode (LANs)

Ports	Network	MG102 IP Address
Port 1	192.168.1.0/24	192.168.1.1
Port 2	192.168.2.0/24	192.168.2.1
Port 3	192.168.3.0/24	192.168.3.1
Port 4	192.168.4.0/24	192.168.4.1

- **Port Settings**

For every Ethernet port the link negotiation can be set. In most cases auto negotiation will work.



Switch Settings

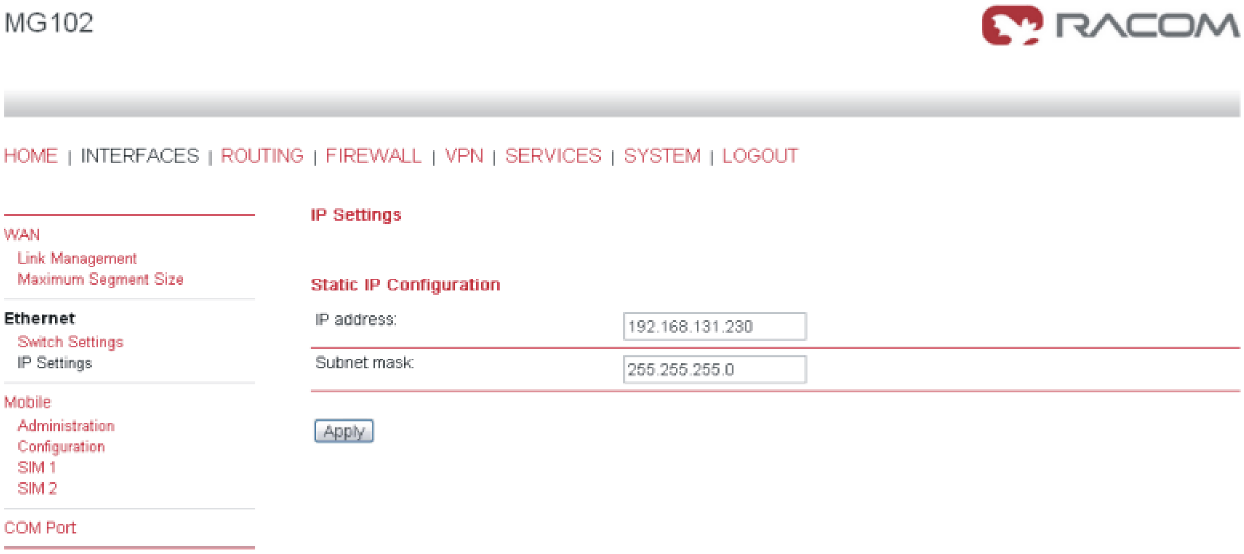
Negotiation mode port 1:	auto-negotiation
Negotiation mode port 2:	auto-negotiation
Negotiation mode port 3:	auto-negotiation
Negotiation mode port 4:	auto-negotiation

Port Status

Status port 1:	up
Status port 2:	down
Status port 3:	down
Status port 4:	down

- **IP Settings**

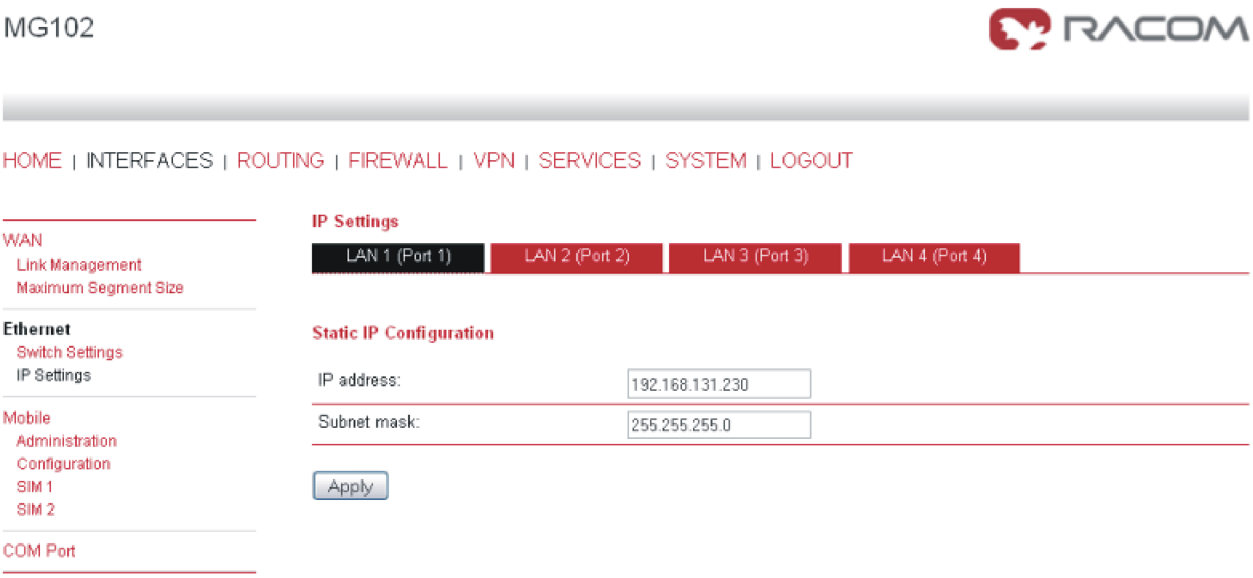
Define the M!DGE/MG102 LAN. Usually the first address within that LAN is assigned to the router. Provide that IP address and net mask in dot-decimal notation or use the defaults.



IP Settings

Static IP Configuration

IP address:	192.168.131.230
Subnet mask:	255.255.255.0

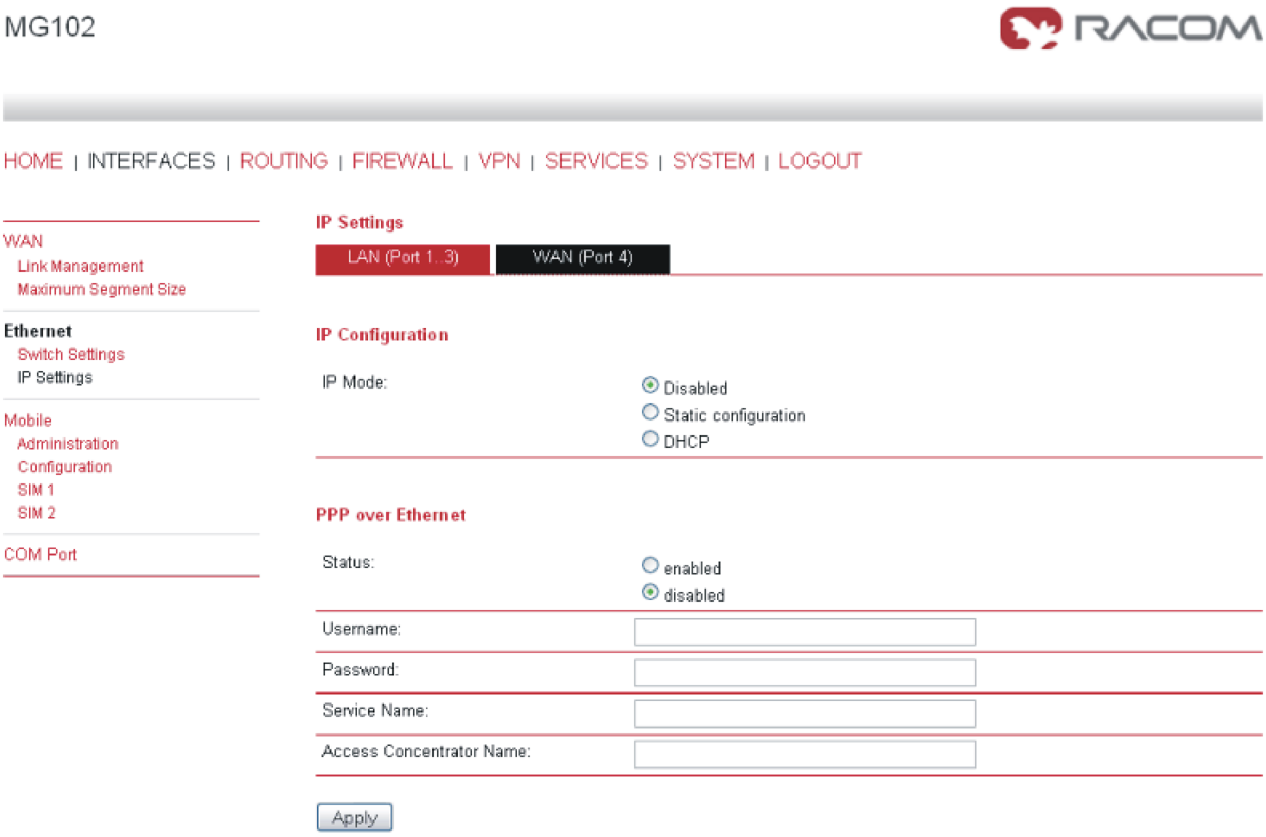


IP Settings

Static IP Configuration

IP address:	192.168.131.230
Subnet mask:	255.255.255.0

- ○ **WAN**



IP Settings

IP Configuration

IP Mode: ● Disabled ○ Static configuration ○ DHCP

PPP over Ethernet

Status: ○ enabled ● disabled

Username:

Password:

Service Name:

Access Concentrator Name:

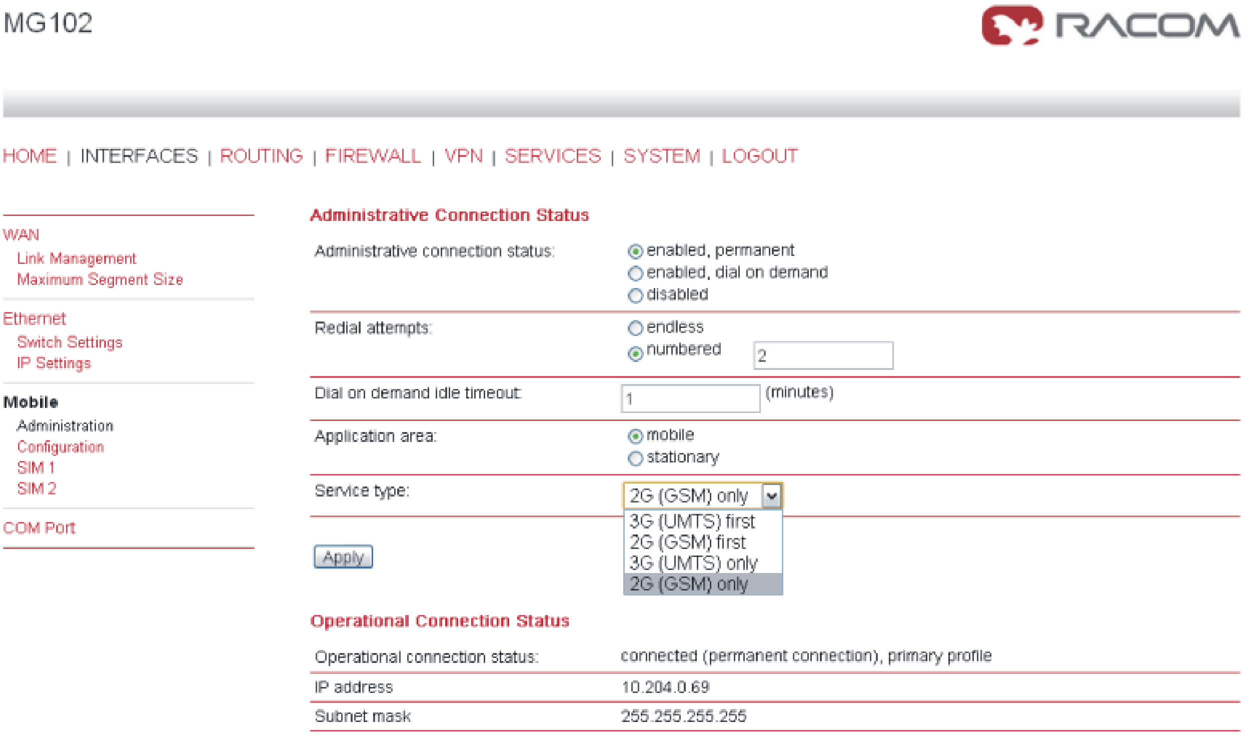
Parameter	Description
IP mode:	Disabled means that the IP interface will be left unconfigured. Static configuration allows you to set the IP parameters. DHCP means that the IP configuration will be retrieved automatically from an external DHCP server.
Status:	Enable or disable the PPPoE connection

Parameter	Description
Password:	PPPoE password
Service name:	Specifies the service name set on the access concentrator. Leave it blank unless you have many services and need to specify the one you need to connect to.
Access concentrator name:	This may be left blank and the client will connect to any access concentrator.

Mobile

- **Administration**

After the configuration (e.g. setting the APN), the mobile connection is enabled here. We recommend using the ´pernament´ option. The UMTS/GSM LED is blinking during the connection establishment and goes on as soon as the connection is up. See the troubleshooting section and log files if the connection does not come up.



Administrative Connection Status

Administrative connection status: ● enabled, permanent ○ enabled, dial on demand ○ disabled

Redial attempts: ○ endless ● numbered 2

Dial on demand idle timeout: 1 (minutes)

Application area: ● mobile ○ stationary

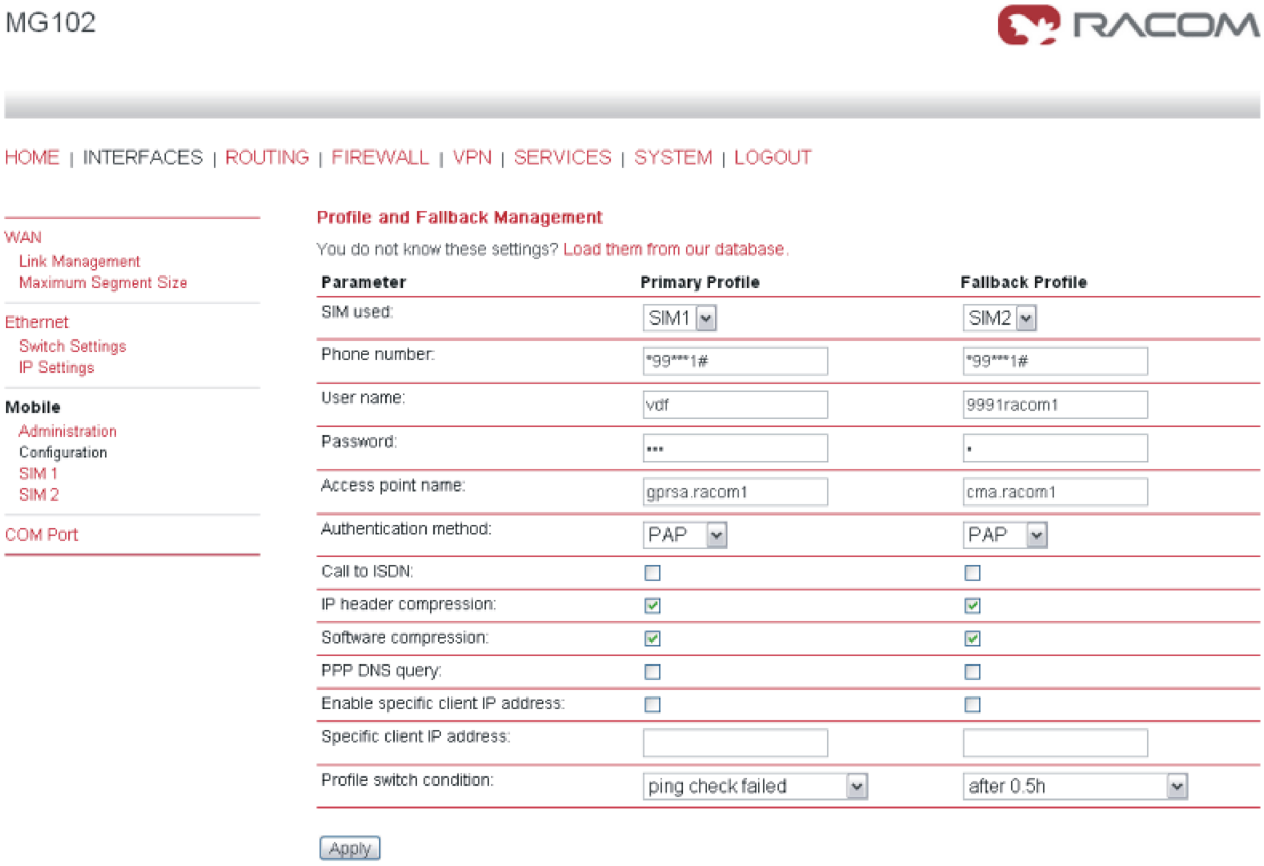
Service type: 2G (GSM) only (3G (UMTS) first, 2G (GSM) first, 3G (UMTS) only, 2G (GSM) only)

Operational Connection Status

Operational connection status:	connected (permanent connection), primary profile
IP address	10.204.0.69
Subnet mask	255.255.255.255

Parameter	Description
Administrative connection status:	This can be permanent, dial on demand or disabled. The on demand method waits for traffic coming from the LAN going to the WAN. The permanent method keeps up the mobile interface. In case of link loss the connection is reestablished.
Redial attempts:	Number of redialing attempts before switching to the next profile.
Dial on demand idle timeout:	Time in minutes after that an idle connection will be disconnected when working with ‘dial on demand’
Operational connection status:	Shows whether a connection is up or not.
Application area:	Choose mobile if M!DGE/MG102 is driving around. For stationary installation choose ‘stationary’
Service type:	The preferred service type can be set here.
IP address:	IP address on mobile interface (ppp0) assigned by PPP server
Subnet mask:	Subnet mask on mobile interface (ppp0) assigned by PPP server

- **Configuration**



MG102

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

WAN
Link Management
Maximum Segment Size

Ethernet
Switch Settings
IP Settings

Mobile
Administration
Configuration
SIM 1
SIM 2

COM Port

Profile and Fallback Management

You do not know these settings? Load them from our database.

Parameter	Primary Profile	Fallback Profile
SIM used:	SIM1	SIM2
Phone number:	*99***1#	*99***1#
User name:	vdf	9991racom1
Password:	•••	•
Access point name:	gprsa.racom1	cma.racom1
Authentication method:	PAP	PAP
Call to ISDN:	□	□
IP header compression:	☑	☑
Software compression:	☑	☑
PPP DNS query:	□	□
Enable specific client IP address:	□	□
Specific client IP address:		
Profile switch condition:	ping check failed	after 0.5h

Parameter	Description
SIM used:	Specify the SIM card that shall be used for this profile.
Phone number:	Set the phone number that is to dial. This should be *99***1# for packet services (GPRS/UMTS). For ISDN and CSD connections use the phone number to dial.
User Name:	User name (get this information from mobile operator, can be void)
Password:	Password (get this information from mobile operator, can be void)
Access point name:	Access Point Name (get this information from mobile operator or from our APN database)
Authentication method:	Use Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP)
Call to ISDN:	Ckeck this, if the connection is made to an ISDN modem.
IP Header Compression:	Enable or disable Van Jacobson TCP/IP Header Compression for PPP. In order to benefit of this features the mobile operator must support it.
Software Compression:	Enable or disable PPP data compression. In order to benefit of this features the mobile operator must support it.
PPP DNS query:	Specifies whether a DNS request to the provider is made or not.

Parameter	Description
Enable Specific Client IP Address:	Enable or disable fixed IP address on the mobile interface.
Specific Client IP Address:	Specify a fixed client IP address on the mobile interface.
Profile switch condition:	Specifies the condition for a profile switch to the other profile. Primary profile ○ never the Fallback profile will not be used ○ redial attemps reached Fallback Profile will be needed after the number of redial attemp will be exceeded. (Interfaces → Mobile → Administrators) ○ ping check failed Fallback Profile will be used in case that number of trials set in Interfaces → WAN → Link Managenet → Settings will be excceded.

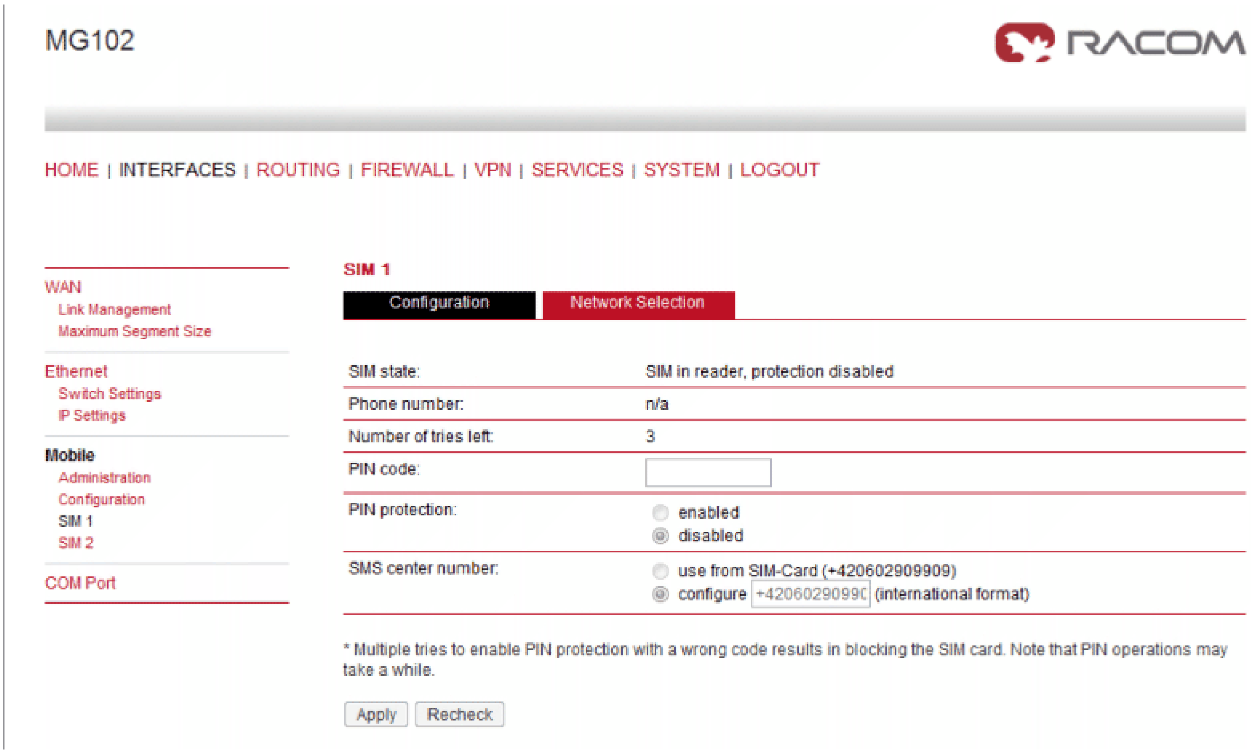
Note

If the time set in Services → Connection Supervisor → Ping Monitor Configuration is shorter then time set. In the above mentioned menus – Fallback Profile NEVER be used.

- **Maximum Segment Size (MSS)**

  described above Maximum Segment Size

- **SIM**



SIM 1

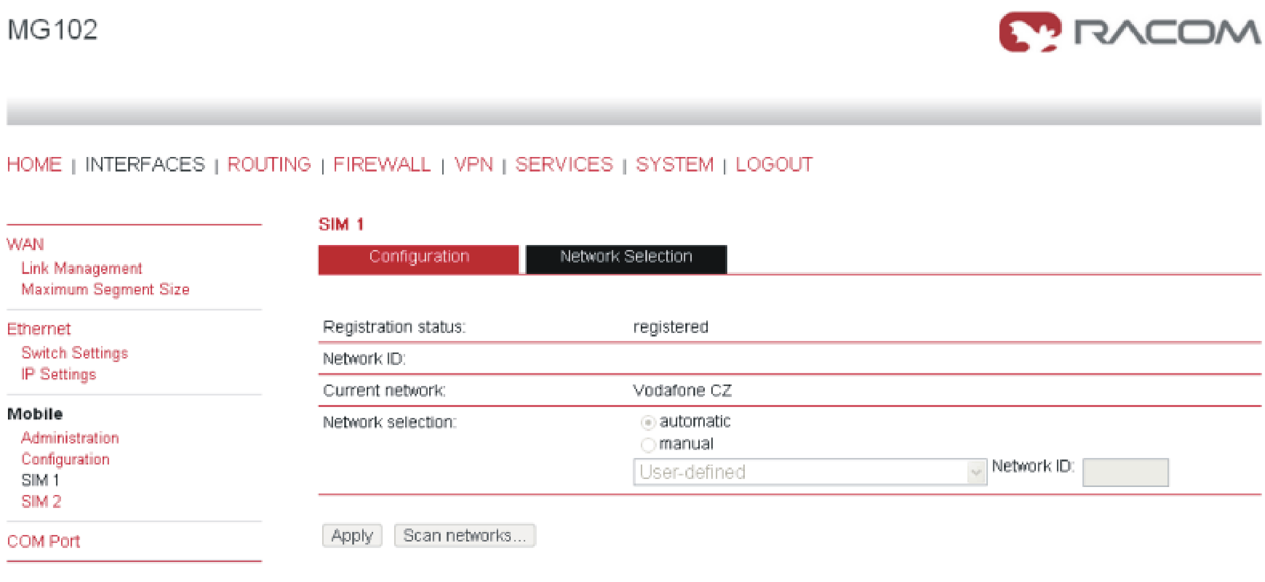
SIM state:	SIM in reader, protection disabled
Phone number:	n/a
Number of tries left:	3
PIN code:	
PIN protection:	○ enabled ● disabled
SMS center number:	○ use from SIM-Card (+420602909909) ● configure +4206029099((international format)

* Multiple tries to enable PIN protection with a wrong code results in blocking the SIM card. Note that PIN operations may take a while.

This section lets you store the PIN code. With the correct PIN code deposited you will be able to enable or disable PIN protection.

M!DGE/MG102 can only read SIM cards if the correct PIN code is provided or if PIN protection is disabled. It is not recommended to disable PIN protection since a SIM card thief could misuse an unprotected SIM.

Parameter	Description
PIN code:	The PIN code for the SIM card.
PIN protection:	Enable or disable PIN protection
SMS center number:	Number of Short Message Service Centers (SMSCs) for sending Mobile Originating (MO) SMS messages. Contact your mobile operator.



SIM 1

Registration status: registered

Network ID:

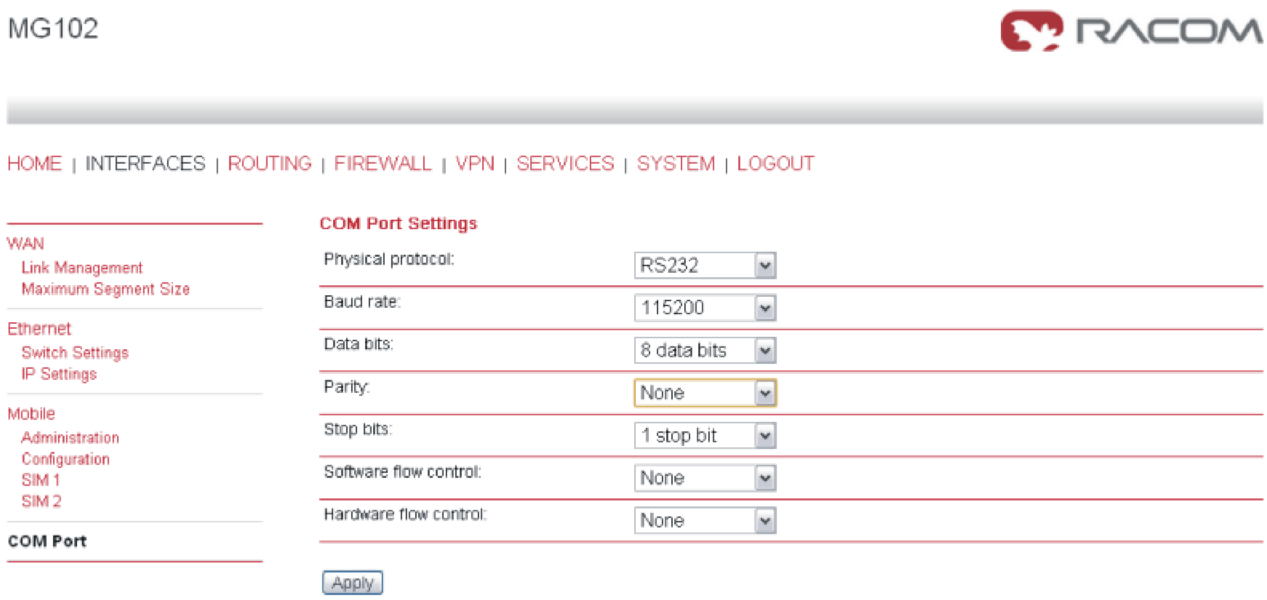
Current network: Vodafone CZ

Network selection: ● automatic ○ manual

User-defined Network ID:

Parameter	Description
Network selection:	Choose automatic or manual provider network selection. For manual selection, please specify the provider.

COM Port



COM Port Settings

Physical protocol: RS232

Baud rate: 115200

Data bits: 8 data bits

Parity: None

Stop bits: 1 stop bit

Software flow control: None

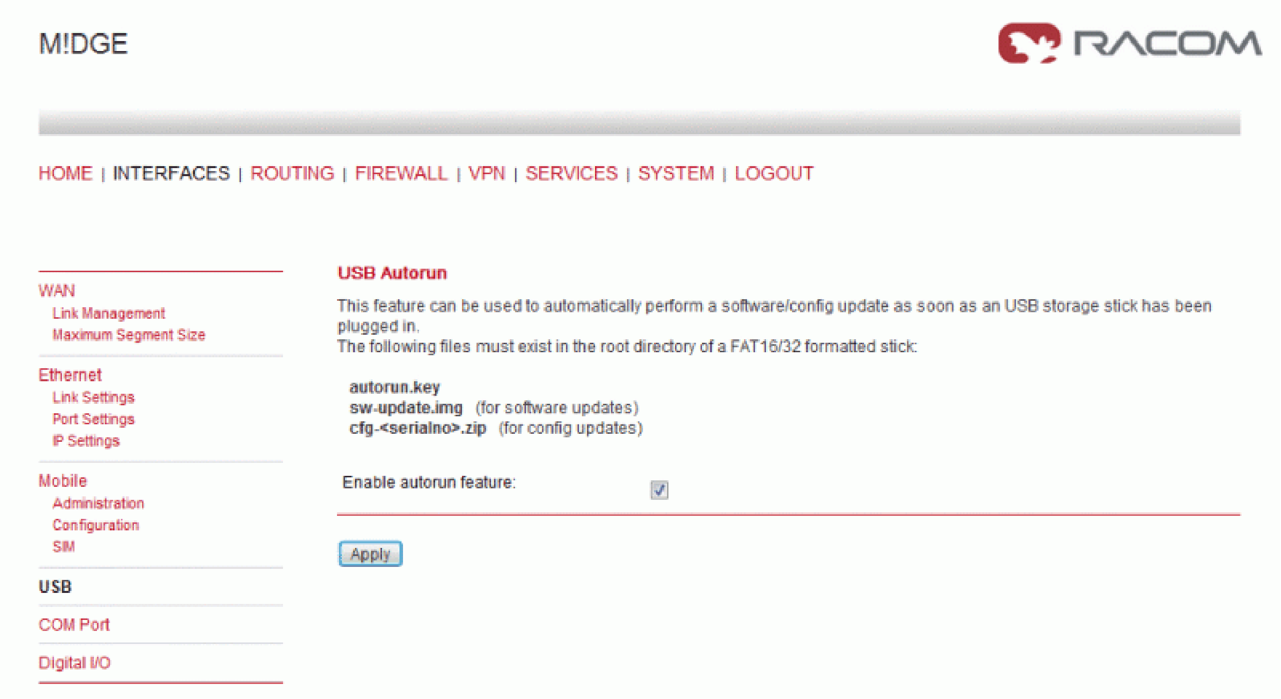
Hardware flow control: None

Parameter	Description
Physical protocol:	RS232 or RS485. Consider the pin assignments on chapter Appendix A, *Connectors and Cables*
Baud rate:	This property specifies the baud rate of the COM port
Parity:	This property specifies the parity used with every frame that is transmitted or received.
Stop bits:	This property specifies the number of stop bits used to indicate the end of a frame.

Parameter	Description
Data bits:	This property specifies the number of data bits contained in each frame.
Software flow control:	In XON/XOFF software flow control, either end can send a stop (XOFF) or start (XON) character to the other end to control the rate of incoming data.
Hardware flow control:	In RTS/CTS hardware flow control, the computer and the modem use the RTS and CTS lines respectively to control the flow of data

USB Port

valid only for M!DGE



USB Autorun

This feature can be used to automatically perform a software/config update as soon as an USB storage stick has been plugged in.
The following files must exist in the root directory of a FAT16/32 formatted stick:

autorun.key
sw-update.img (for software updates)
cfg-<serialno>.zip (for config updates)

Enable autorun feature: ☑

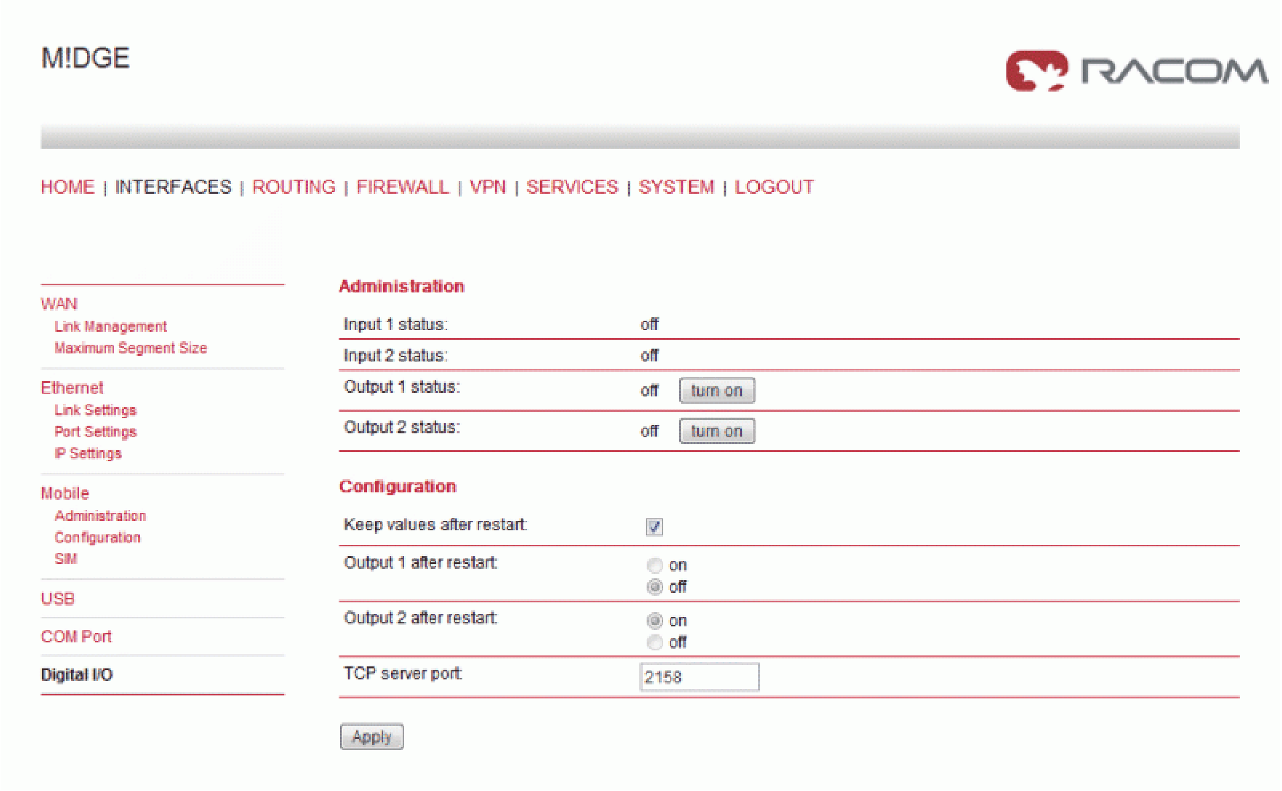
Apply

Parameter	Description
✓	Enable USB autorun feature.

Digital I/O Server (M!DGE only)

- **Digital I/O Management via Web Manager**

  The digital inputs and outputs can be monitored and controlled via the Web Manager or by software.



M!DGE

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

WAN
Link Management
Maximum Segment Size
Ethernet
Link Settings
Port Settings
IP Settings
Mobile
Administration
Configuration
SIM
USB
COM Port
Digital I/O

Administration

Input 1 status:	off	
Input 2 status:	off	
Output 1 status:	off	turn on
Output 2 status:	off	turn on

Configuration

Keep values after restart:	☑
Output 1 after restart:	○ on ● off
Output 2 after restart:	● on ○ off
TCP server port:	2158

Apply

Parameter	Description
Digital inputs levels:	
logical level 0	0 to 5.6 VDC
logical level 1	7.2 to 40 VDC
	Note Negative input voltage is not recognised.
Digital outputs parametres:	
Maximal continuous current	1 A
Maximal switching voltage	60 VDC, 42 VAC (Vrms)
Maximal switching capacity	60 W

- **Digital I/O Management**

To manage digital inputs and outputs via TCP software is required that handles the TCP connection. For test purposes e.g. telnet can be used. The payload contains the states of the four inputs/outputs:

The value 0 represents the state “off”, the value 1 the state “on”.

7							0
0	0	0	0	IN1	IN2	OUT1	OUT2

- **Monitor the digital inputs and outputs**

  Every change of digital inputs triggers a message of the above format to be sent. It also contains the valid states of the outputs.
- **Set digital outputs**

  To set the states of the digital I/O send the following pattern as ASCII characters

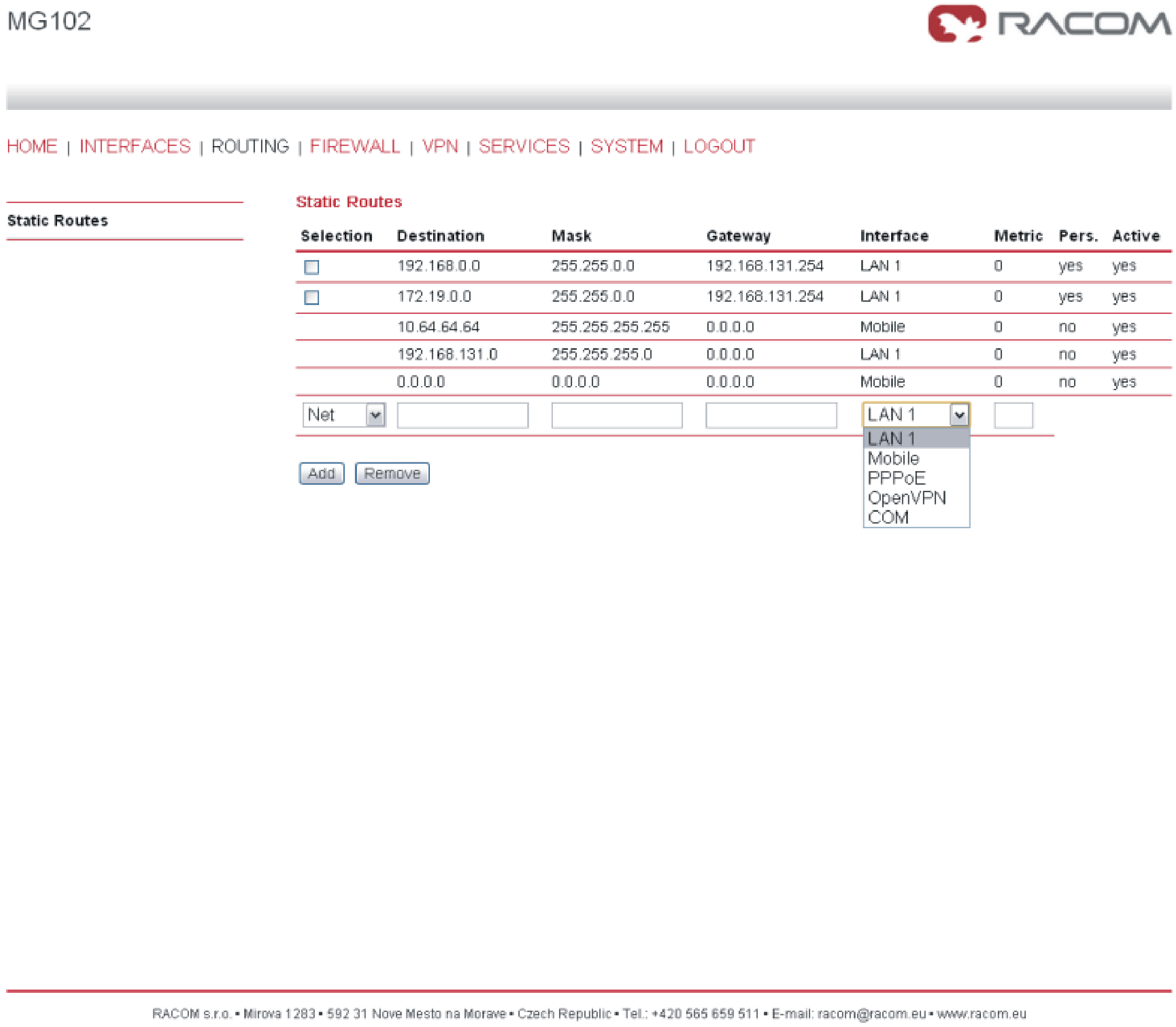
Pattern	Description
00000000	Turn all digital outputs off
00000001	Turn output 2 on, turn output 1 off
00000010	Turn output 1 on, turn output 2 off
00000011	Turn output 1 on, turn output 2 on

- **Get status of digital inputs and output**

  To get the states of the digital I/O send the following pattern as ASCII characters

Pattern	Description
00010000	Request a message with all states

3.1.5. Routing



MG102

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

Static Routes

Selection	Destination	Mask	Gateway	Interface	Metric	Pers.	Active
☐	192.168.0.0	255.255.0.0	192.168.131.254	LAN 1	0	yes	yes
☐	172.19.0.0	255.255.0.0	192.168.131.254	LAN 1	0	yes	yes
	10.64.64.64	255.255.255.255	0.0.0.0	Mobile	0	no	yes
	192.168.131.0	255.255.255.0	0.0.0.0	LAN 1	0	no	yes
	0.0.0.0	0.0.0.0	0.0.0.0	Mobile	0	no	yes
Net				LAN 1			

LAN 1
Mobile
PPPoE
OpenVPN
COM
Add
Remove

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

Static routing is the term used to refer to a manual method that is used to set up routing between networks. Static routing has the advantage of being predictable and simple to set up.

This section lists the routing table and lets the user add and delete routes.

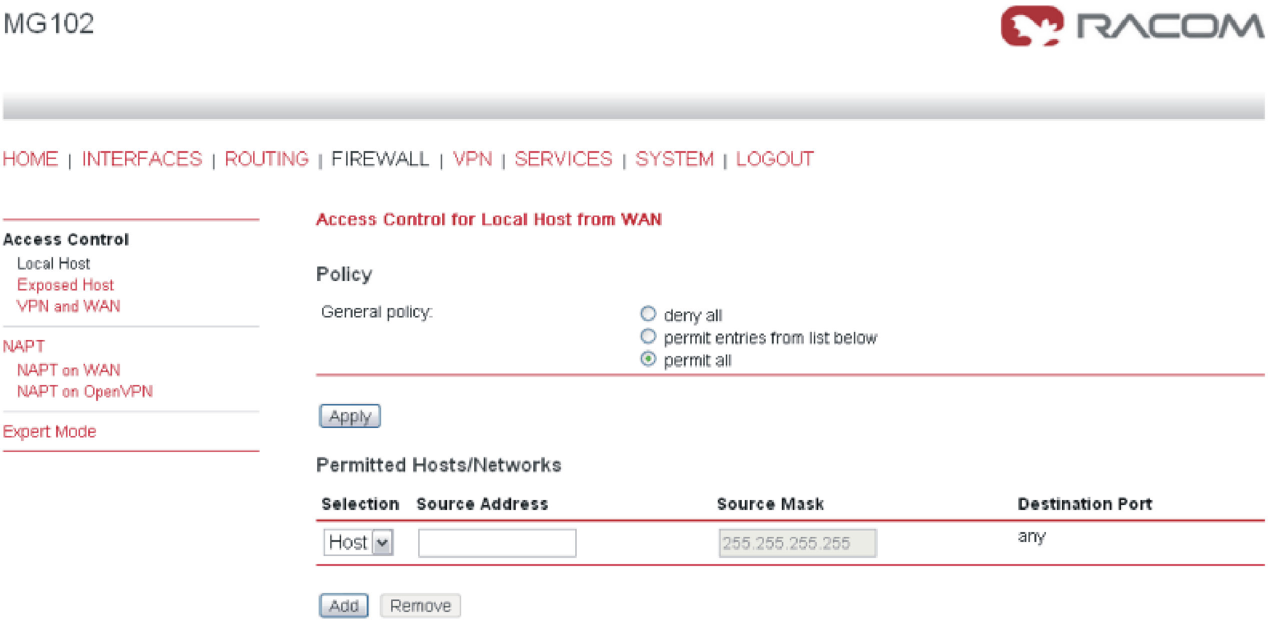
Parameter	Description
Select	To enter network route select “Net”. To enter a route to a host select “Host”.
Destination	The destination network or host. You can provide IP addresses in dotted decimal or host/network names.
Mask	The network's IP address together with its address mask defines a range of IP addresses. For IP subnets, the address mask is referred to as the subnet mask. For host routes, the mask is "all ones" (in dotted decimal 255.255.255.255).
Gateway	Next hop (gateway); the next router which knows how to reach the destination
Interface	Identity of network interface through which a packet will be sent to reach the gateway.
Metric	The 'distance' to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.

Parameter	Description
Persistent	Displays whether a particular route is persistent or not.
Active	Displays whether a particular route is active or not.

3.1.6. Firewall

Access Control Lists

- **Access Control for Local Host** – The access from the WAN interface to M!DGE/MG102 itself and its local applications can be managed using this filter.



Access Control for Local Host from WAN

Policy

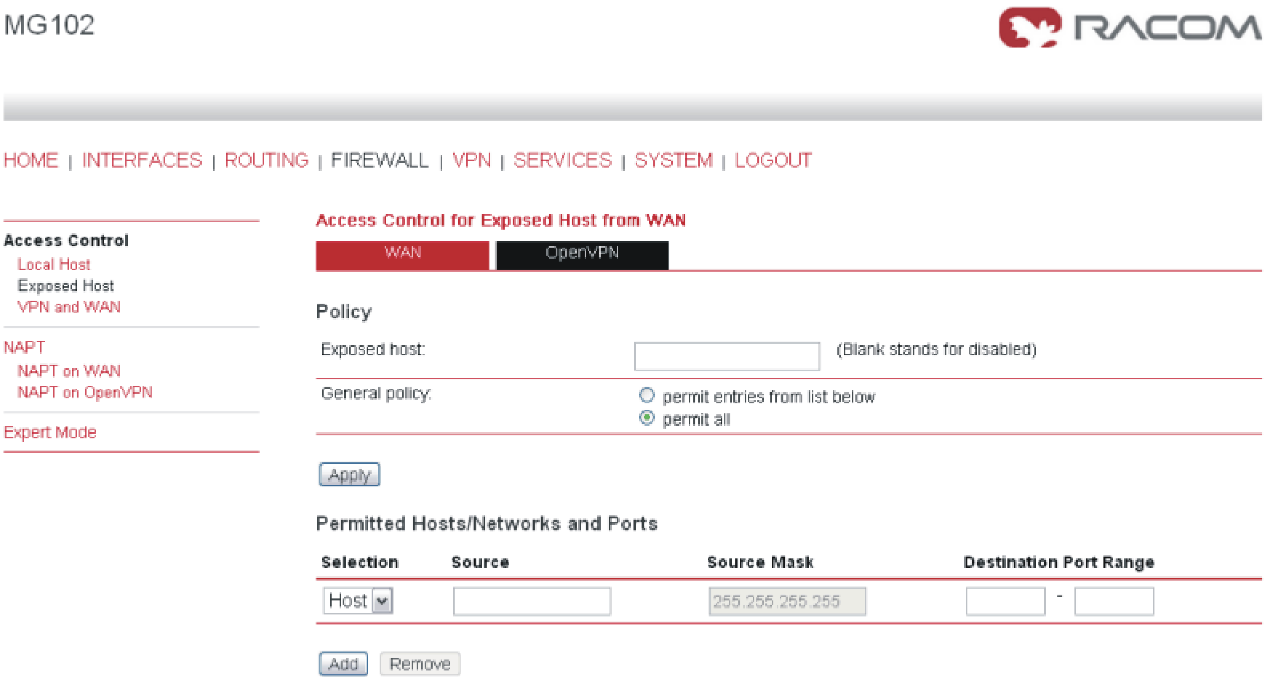
General policy: ○ deny all ○ permit entries from list below ● permit all

Permitted Hosts/Networks

Selection	Source Address	Source Mask	Destination Port
Host		255.255.255.255	any

- **Access Control for Exposed Host from WAN and OpenVPN** – The access from the WAN interface to a defined Exposed Host can be managed using this filter. The same can be done on the second tab for the OpenVPN interface.

You can set both WAN and Open VPN rules.


MG102

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

Access Control
Local Host
Exposed Host
VPN and WAN

NAPT
NAPT on WAN
NAPT on OpenVPN

Expert Mode

Access Control for Exposed Host from WAN

WAN | OpenVPN

Policy

Exposed host: (Blank stands for disabled)

General policy: ○ permit entries from list below
● permit all

Apply

Permitted Hosts/Networks and Ports

Selection	Source	Source Mask	Destination Port Range
Host		255.255.255.255	-

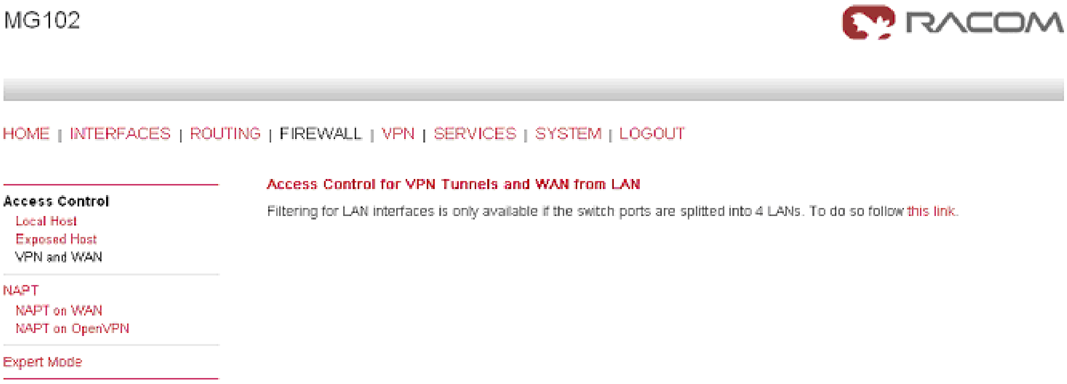
Add Remove

Parameter	Description
Exposed host:	Enter the IP Address of the device that is to expose. Leave this field blank to disable the feature.

- **Access Control for VPN Tunnels and WAN from LAN** – Having the Ethernet ports split into multiple LANs this filter manages the access from any LAN port to any VPN Tunnel. Use the option “specify permitted networks“ to permit access to certain networks. Those networks might be any peer networks of a VPN tunnel or the WAN interface to get direct Internet access.

Note

Filtering for LAN interfaces is available only if 4LANs are set in Interfaces → Switch setings → Ethernet Mode.


MG102

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

Access Control
Local Host
Exposed Host
VPN and WAN

NAPT
NAPT on WAN
NAPT on OpenVPN

Expert Mode

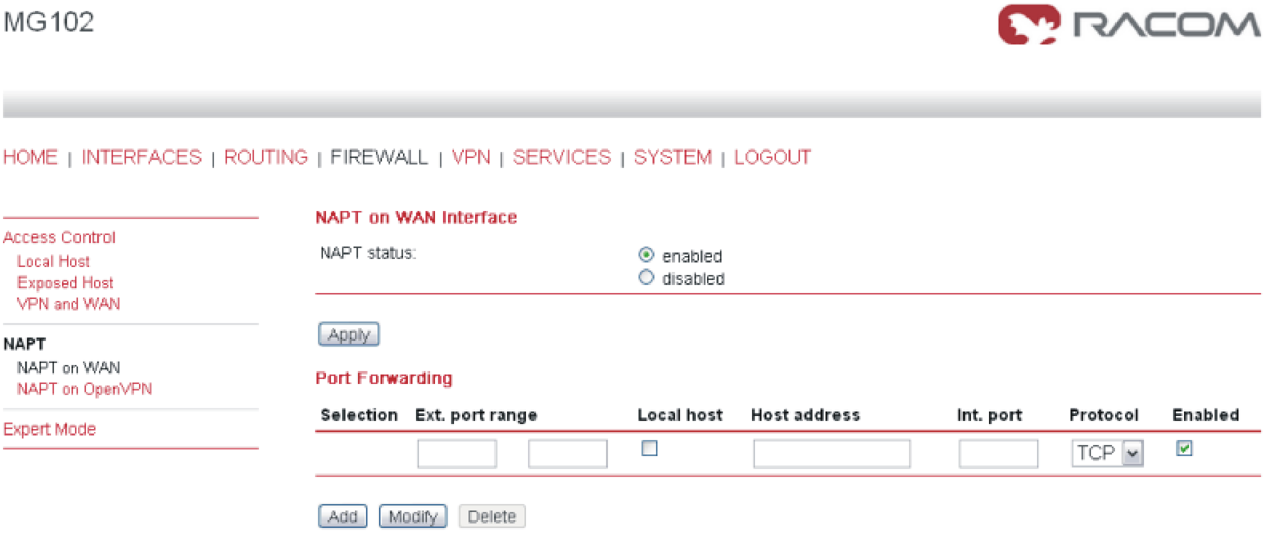
Access Control for VPN Tunnels and WAN from LAN

Filtering for LAN interfaces is only available if the switch ports are splitted into 4 LANs. To do so follow this link.

NAPT

This page lets you set the options for Network Address and Port Translation (NAPT). NAPT is a feature that translates TCP or UDP communications made between hosts on a private network and hosts on a public network. It allows a single public IP address to be used by many hosts on the private network, which is usually called a Local Area Network or LAN.

- **NAPT on Mobile Interface**



NAPT on WAN Interface

NAPT status: ● enabled ○ disabled

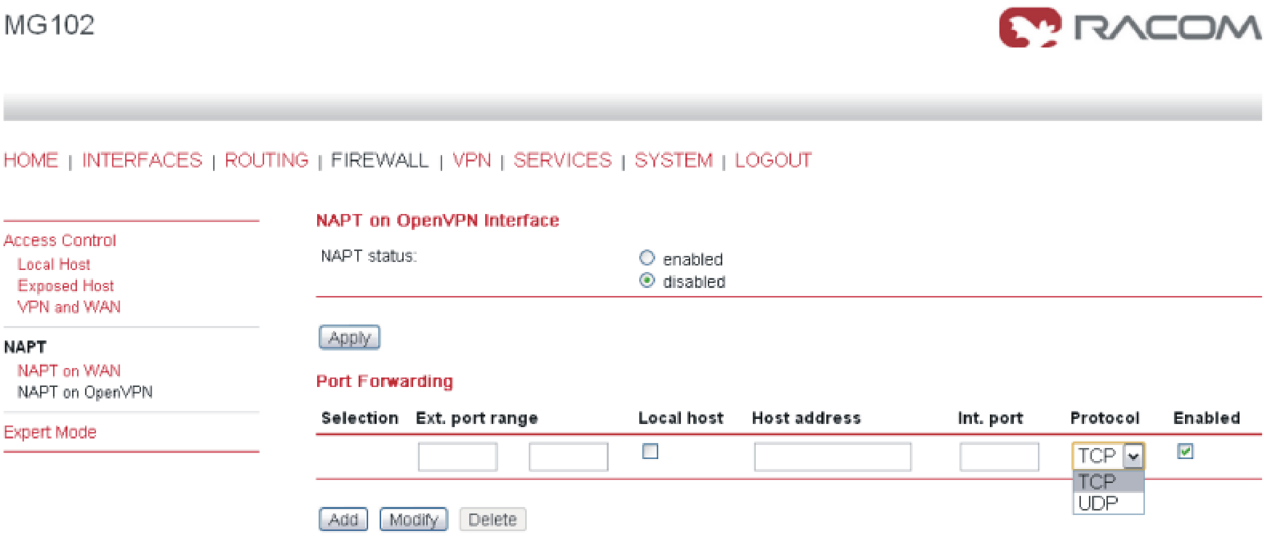
Port Forwarding

Selection	Ext. port range		Local host	Host address	Int. port	Protocol	Enabled
			□			TCP	☑

Port forwarding is the act of forwarding a network port from one network node to another. This technique can allow an external user to reach a port on a private IP address (inside the LAN) from the outside (Internet).

Parameter	Description
NAPT status	Enable or disable NAPT. NAPT needs to be enabled normally (i.e. when using Internet Access). Internet Service Providers will not route your private LAN Addresses.
Service name:	User-defined Name for the NAPT entry.
External port:	External IP port (mobile interface).
Local host:	Check this box to forward traffic to local host service (Webserver, SSH, Telnet). To forward traffic to an external host in the LAN provide the host address below.
Host address:	Host to which the traffic will be forwarded.
Internal port:	Port to which the traffic will be forwarded.
Protocol:	Protocol (UDP or TCP) to which this entry applies.
Enabled:	Enable (Yes) or disable (No) the entry.

- **NAPT on OpenVPN Interface**



NAPT on OpenVPN Interface

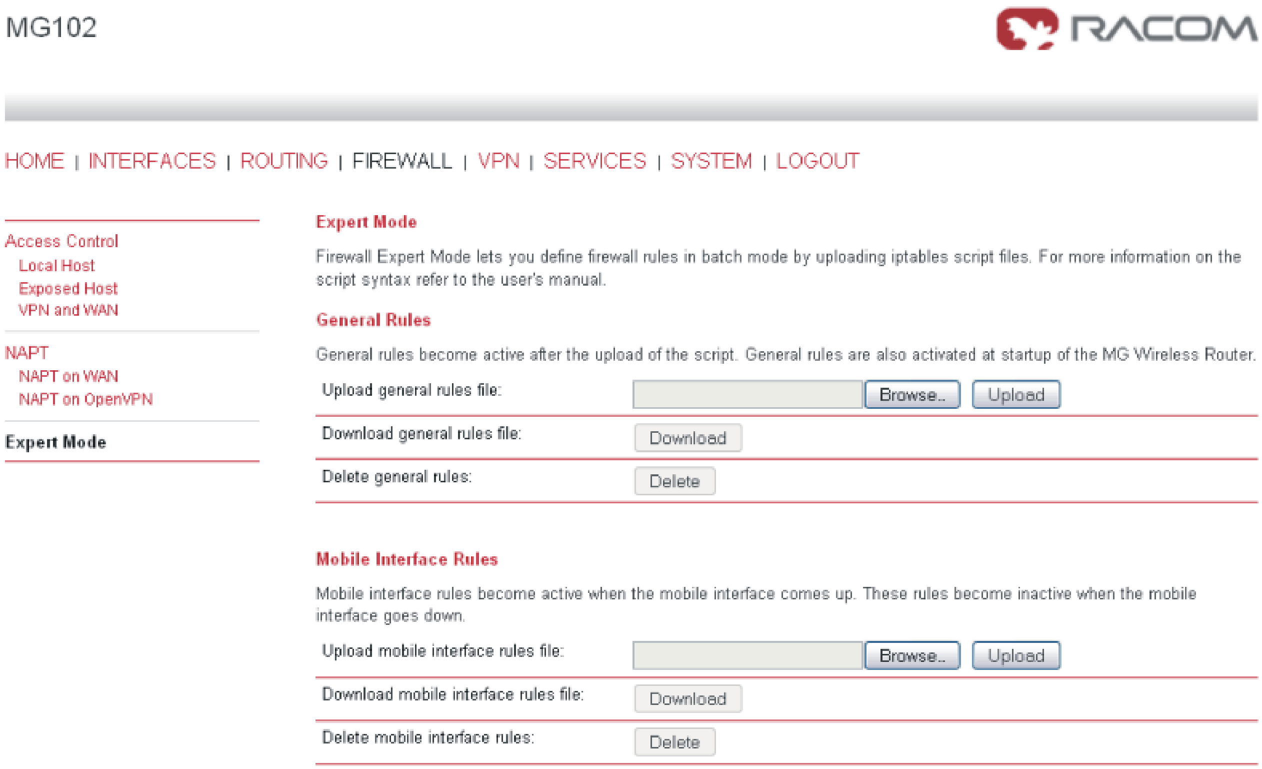
NAPT status: ○ enabled ● disabled

Port Forwarding

Selection	Ext. port range		Local host	Host address	Int. port	Protocol	Enabled
			□			TCP TCP UDP	☑

The same settings as above, but for other interface

Expert Mode



Expert Mode

Firewall Expert Mode lets you define firewall rules in batch mode by uploading iptables script files. For more information on the script syntax refer to the user's manual.

General Rules

General rules become active after the upload of the script. General rules are also activated at startup of the MG Wireless Router.

Upload general rules file:

Download general rules file:

Delete general rules:

Mobile Interface Rules

Mobile interface rules become active when the mobile interface comes up. These rules become inactive when the mobile interface goes down.

Upload mobile interface rules file:

Download mobile interface rules file:

Delete mobile interface rules:

Upload text files with firewall rules.

3.1.7. VPN

OpenVPN

Install an OpenVPN Server or subscribe to the appropriate service.

If you have your own OpenVPN server the first step in building an OpenVPN 2.0 configuration is to establish a PKI (public key infrastructure). The PKI consists of:

- a separate certificate (also known as a public key) and private key for the server and each client, and
- a master Certificate Authority (CA) certificate and key which is used to sign each of the server and client certificates.

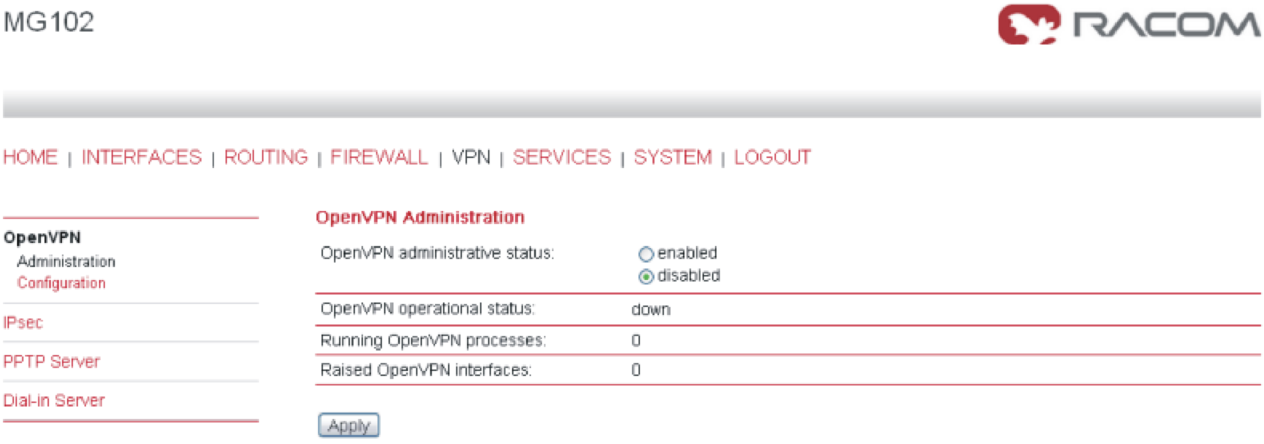
Prepare the OpenVPN certificate files. Use the tools and documentation that come with the OpenVPN software. A Guide to basic RSA Key Management is found under http://openvpn.net/easyrsa.html

For alternative authentication methods see http://openvpn.net/index.php/documentation/howto.html#auth

For more information also see http://openvpn.net/howto.html

Please make sure that the M!DGE/MG102 system time is correct when working with OpenVPN. Otherwise authentication issues may arise.

- **OpenVPN Administration**

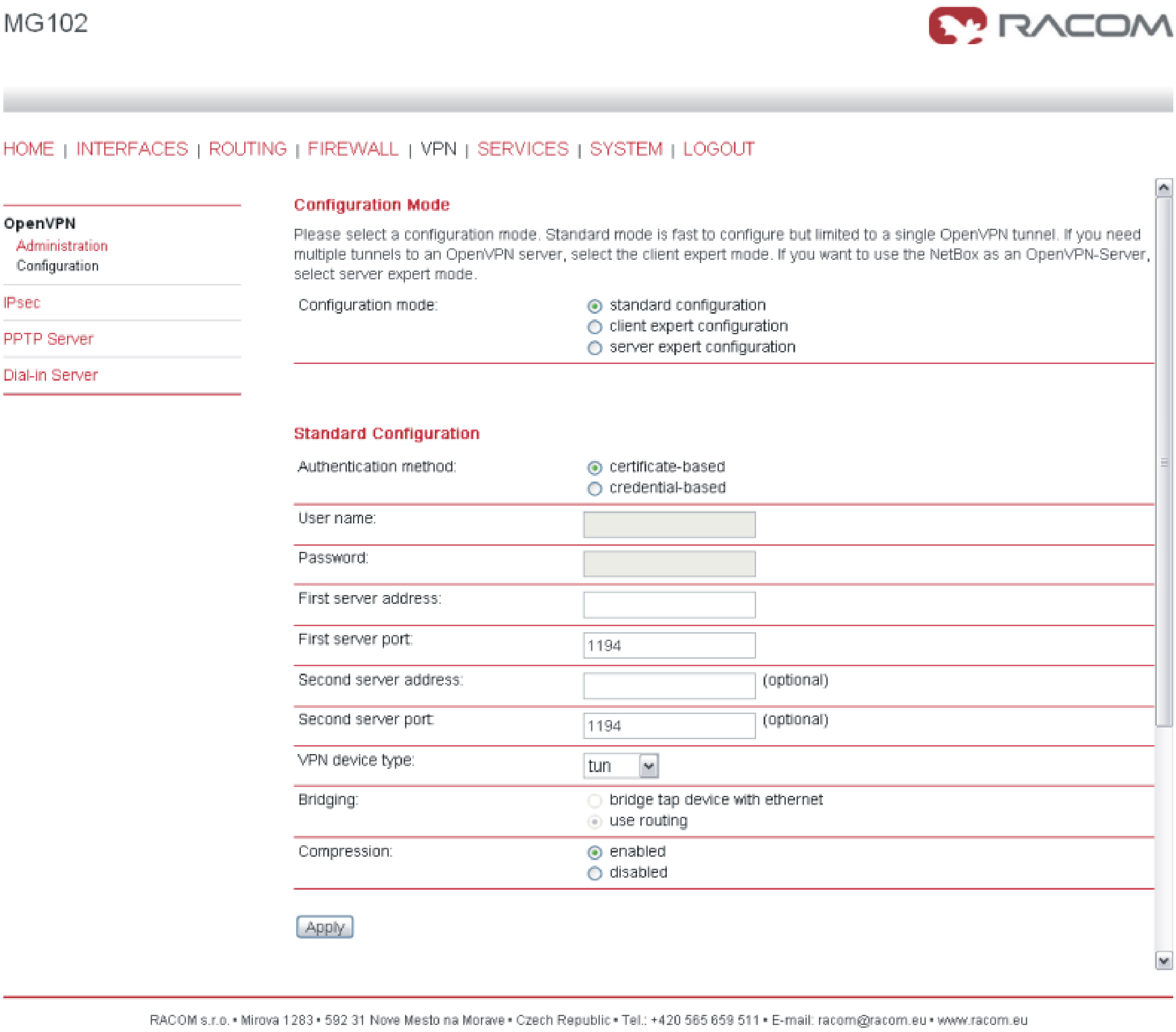


OpenVPN Administration

OpenVPN administrative status:	○ enabled ● disabled
OpenVPN operational status:	down
Running OpenVPN processes:	0
Raised OpenVPN interfaces:	0

Parameter	Description
OpenVPN administrative status:	Enable or disable OpenVPN. If enabled, OpenVPN client configurations will be started after mobile connection establishment. Server configurations will be started immediately after M!DGE/MG102 startup.

- **OpenVPN Configuration (Standard Client Configuration)**



MG102

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

Configuration Mode

Please select a configuration mode. Standard mode is fast to configure but limited to a single OpenVPN tunnel. If you need multiple tunnels to an OpenVPN server, select the client expert mode. If you want to use the NetBox as an OpenVPN-Server, select server expert mode.

Configuration mode: ● standard configuration ○ client expert configuration ○ server expert configuration

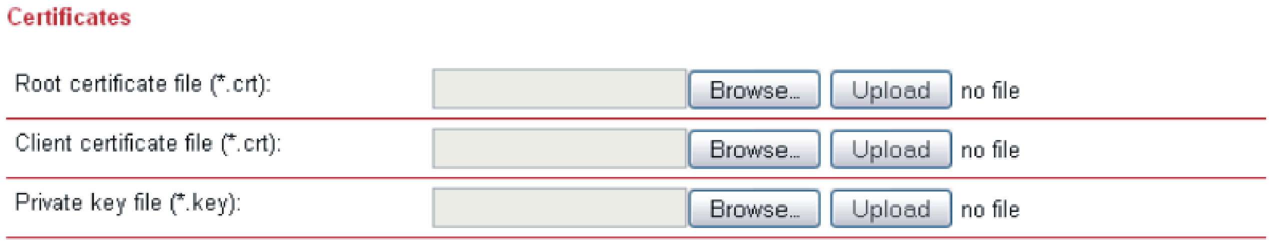
Standard Configuration

Authentication method:	● certificate-based ○ credential-based
User name:	
Password:	
First server address:	
First server port:	1194
Second server address:	(optional)
Second server port:	1194 (optional)
VPN device type:	tun
Bridging:	○ bridge tap device with ethernet ● use routing
Compression:	● enabled ○ disabled

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

Parameter	Description
Configuration mode:	Set the active configuration
Authentication method:	Use certificates or user name / password
First server address	First OpenVPN server address
First server port	First OpenVPN server port, default 1194
Second server address	Second OpenVPN server address (optional)
Second server port	Second OpenVPN server port (optional)
VPN device type	tun or tap
Bridging	With tap: bridge tap device with ethernet, or use routing
Compression	Enable or disable OpenVPN compression

- **OpenVPN Client Certificates**



Certificates

Root certificate file (*.crt): no file

Client certificate file (*.crt): no file

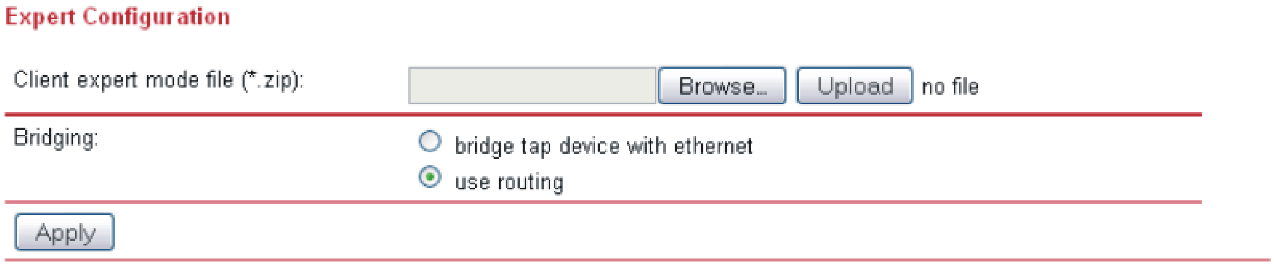
Private key file (*.key): no file

Certificate File	File Type	Description
Root certificate file	*.crt	Master Certificate Authority (CA) certificate and key which is used to sign each of the server and client certificates.
Client certificate file	*.crt	Separate certificate (also known as a public key)
First server address	*.key	Private key for the server and each client

Tip

Use the dial-out connection method “permanent“ in context with OpenVPN.

OpenVPN Configuration (Client Expert Configuration)



Expert Configuration

Client expert mode file (*.zip): no file

Bridging:
○ bridge tap device with ethernet
● use routing

This configuration mode gives you more flexibility. The configuration upload takes a zip file which may include one or more OpenVPN client configurations.

Typically such a zip file includes files such as:

- client.conf (The client configuration file, referring to …)
- ca.crt (OpenVPN root certificate file)
- client.crt (OpenVPN client certificate file)
- client.key (OpenVPN private key file)

The name of the configuration file (here client.conf) can be chosen freely but the extension must be .conf. To configure multiple tunnels (i.e. multiple *.conf files each referring to its certificates) you should place all files belonging to a single tunnel/process into a subfolder or make sure that there are no naming conflicts.

If OpenVPN is enabled and the configuration mode is set to “client expert configuration” all configurations (*.conf) will be started *after mobile connection establishment.*

OpenVPN Configuration (Server Expert Configuration)

This configuration mode lets you run an OpenVPN server on M!DGE/MG102. The configuration upload takes a zip file which may include one or more OpenVPN server configurations.

Typically such a zip file includes files such as:

- server.conf (The client configuration file, referring to)
- ca.crt (OpenVPN root certificate file)
- server.crt (OpenVPN client certificate file)
- server.key (OpenVPN private key file)
- dh1024.pem (Diffie hellman parameters)
- A directory (with default name “ccd”) containing client-specific configuration files

To configure multiple server processes (i.e. multiple *.conf files each referring to its certificates) you should place all files belonging to a single tunnel/process into a subfolder or make sure that there are no naming conflicts.

If OpenVPN is enabled and the configuration mode is set to “server expert configuration” all configurations (*.conf) will be started after M!DGE/MG102 startup.

Consider the following points when running OpenVPN without having established a mobile connection:

- Configure a Default Route to the Ethernet Interface / LAN.
- Configure a time server (NTP) and make sure that it is available via the LAN.
- Manually configure a DNS server (on DHCP Server web page!) and make sure that it is available via the LAN.

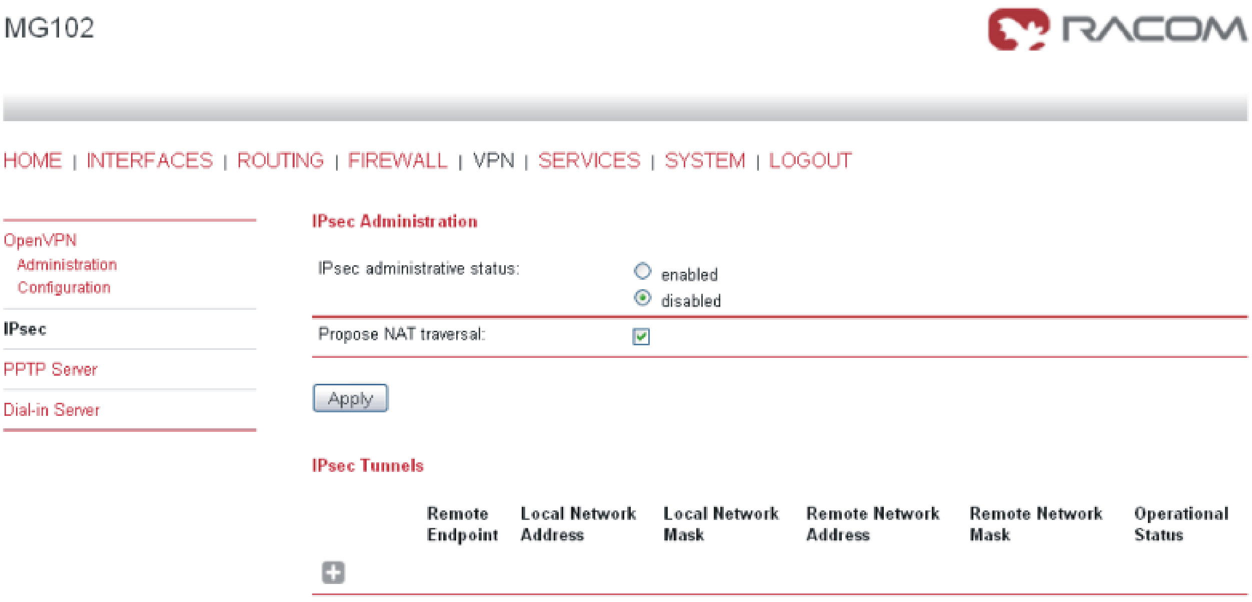
For further information and external OpenVPN documentation please see chapter the section called “OpenVPN”.

IPsec

IPsec (IP security) is a suite of protocols for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet in a data stream. IPsec also includes protocols for cryptographic key establishment.

IPsec can be used to create Virtual Private Networks (VPN) and this is the dominant use.

- **IPsec Administration**



IPsec Administration

IPsec administrative status: ○ enabled ● disabled

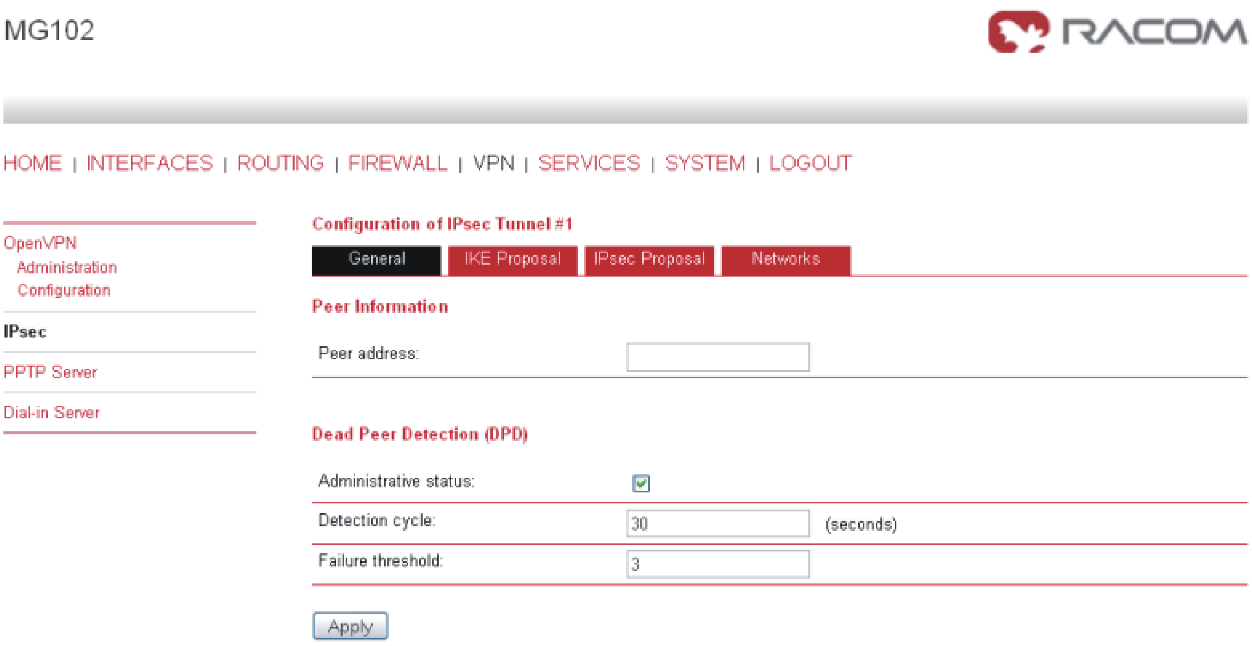
Propose NAT traversal: ☑

IPsec Tunnels

Remote Endpoint	Local Network Address	Local Network Mask	Remote Network Address	Remote Network Mask	Operational Status

Parameter	Description
IPsec administrative status:	Enable or disable IPsec.

- **IPsec Configuration**



Configuration of IPsec Tunnel #1

Peer Information

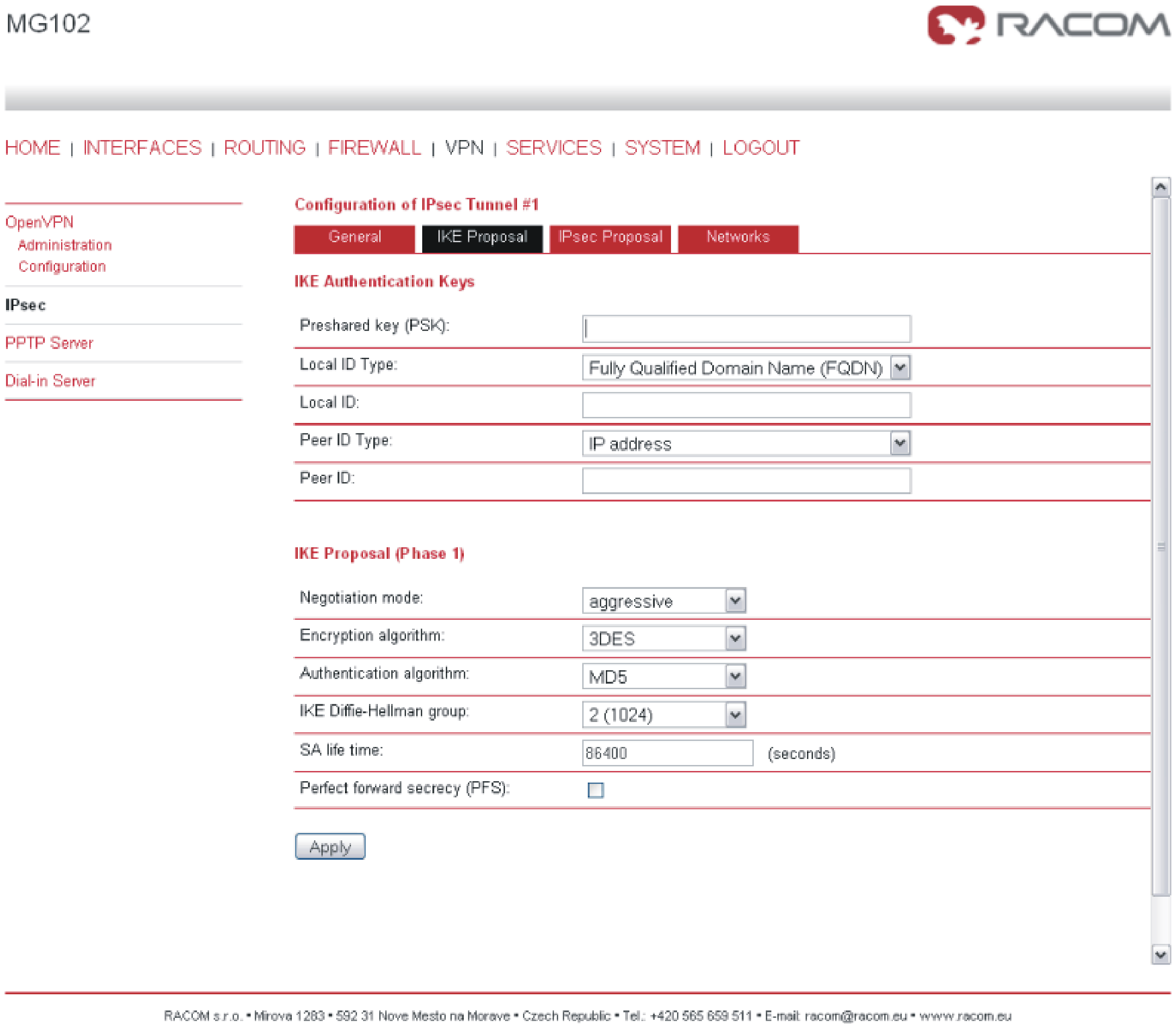
Peer address:

Dead Peer Detection (DPD)

Administrative status: ☑

Detection cycle: 30 (seconds)

Failure threshold: 3


MG102
RACOM
HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT
OpenVPN
Administration
Configuration
IPsec
PPTP Server
Dial-in Server
General
IKE Proposal
IPsec Proposal
Networks
Apply
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

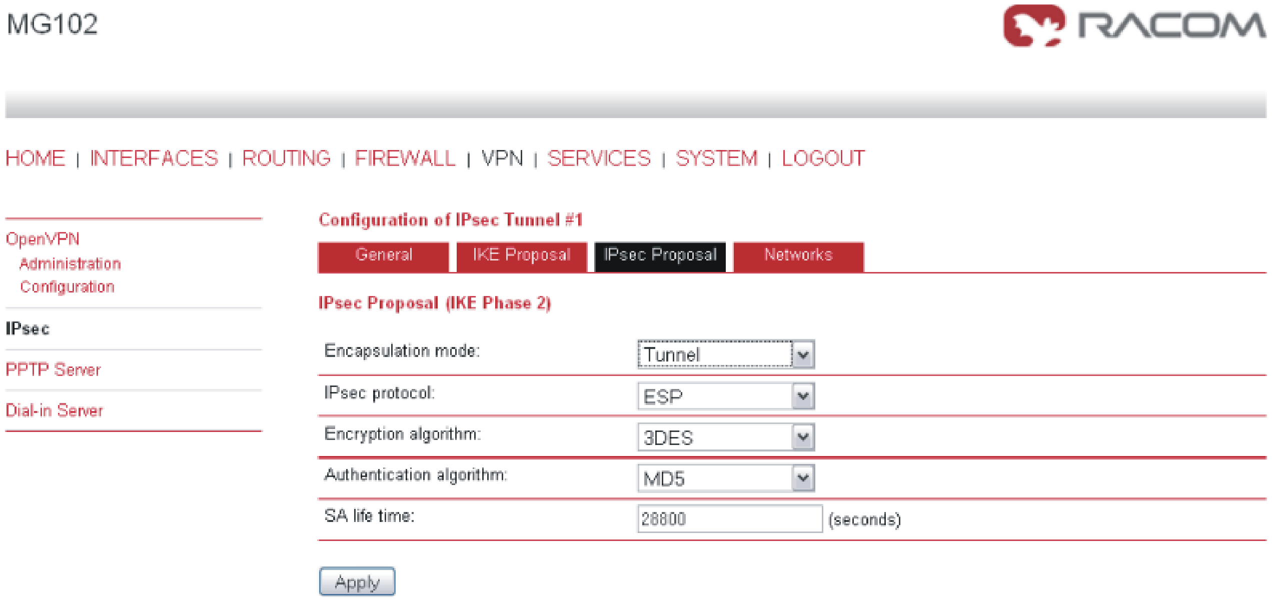
Configuration of IPsec Tunnel #1

IKE Authentication Keys

Preshared key (PSK):	
Local ID Type:	Fully Qualified Domain Name (FQDN)
Local ID:	
Peer ID Type:	IP address
Peer ID:	

IKE Proposal (Phase 1)

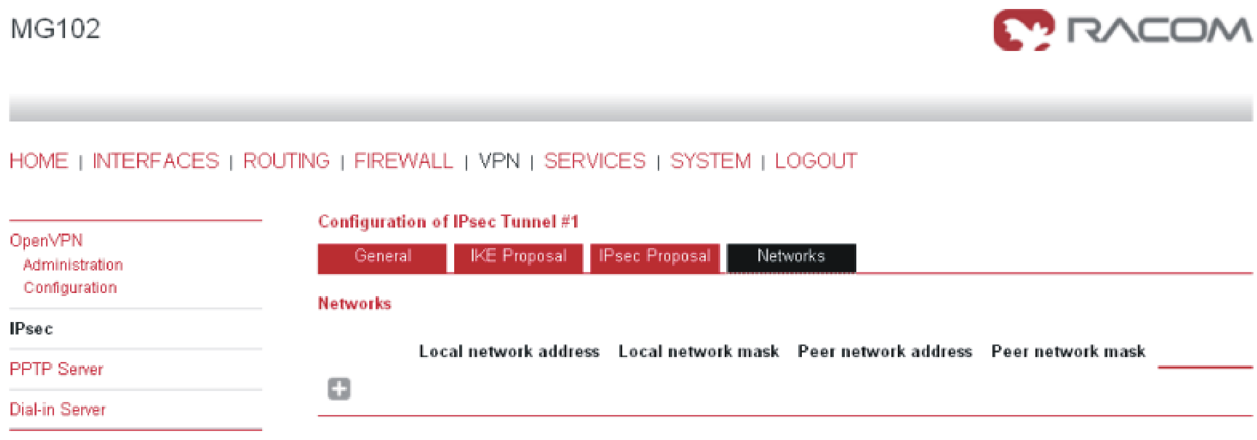
Negotiation mode:	aggressive
Encryption algorithm:	3DES
Authentication algorithm:	MD5
IKE Diffie-Hellman group:	2 (1024)
SA life time:	86400 (seconds)
Perfect forward secrecy (PFS):	□



Configuration of IPsec Tunnel #1

IPsec Proposal (IKE Phase 2)

Encapsulation mode:	Tunnel
IPsec protocol:	ESP
Encryption algorithm:	3DES
Authentication algorithm:	MD5
SA life time:	28800 (seconds)



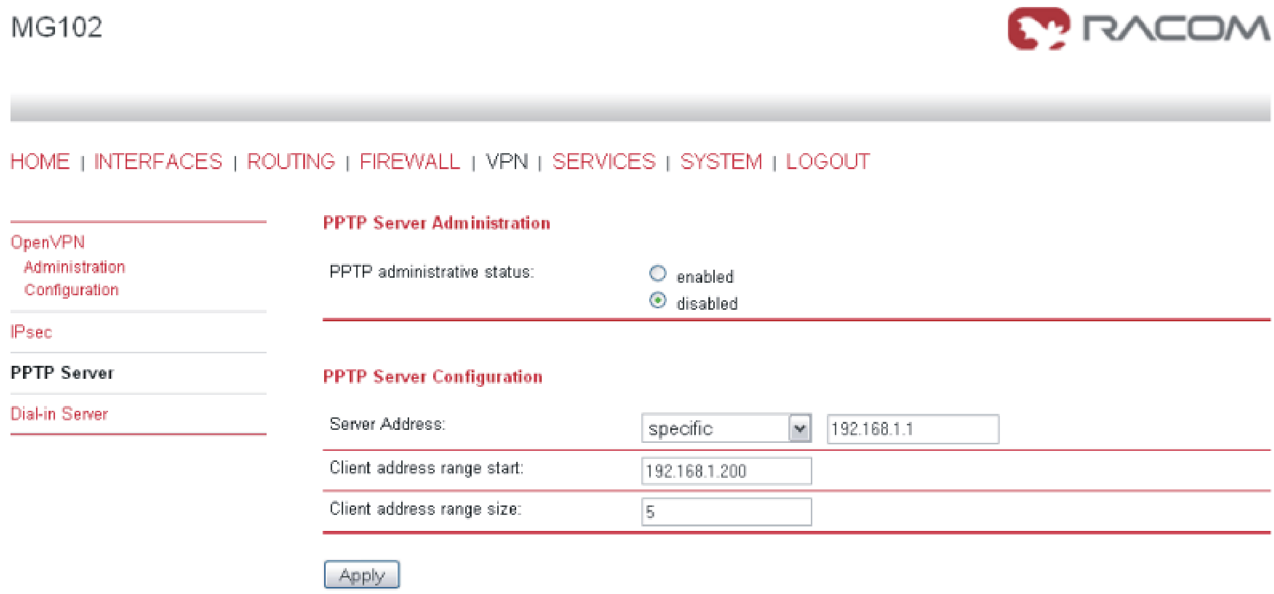
Configuration of IPsec Tunnel #1

Networks

Local network address	Local network mask	Peer network address	Peer network mask

Parameter	Description
Remote server address:	IP address or host name of IPsec peer / responder / server.
Remote LAN address:	The remote private network. Provide an IP address in dotted decimal notation.
Remote LAN subnet mask:	The remote private network. Provide a subnet mask in dotted decimal notation.
NAT Traversal	Enable or disable NAT-Traversal.
Preshared Key (PSK):	The pre-shared key (PSK)
IKE mode:	Choose a negotiation mode. The default is main mode (identity-protection). Aggressive mode is less secure than main mode as it reveals your identity to an eavesdropper. However, with *pre-shared key authentication and dynamic IP addresses aggressive mode is the only choice*.
IKE encryption:	IKE encryption method
IKE hash:	IKE hash method
IKE Diffie-Hellman Group:	IKE Diffie-Hellman Group
Perfect Forward Secrecy (PFS):	Use Perfect Forward Secrecy. This feature increases security as with PFS, penetration of the key-exchange protocol does not compromise keys negotiated earlier.
Local ID:	Local ID
Remote ID:	Remote ID
ESP encryption:	ESP encryption method
ESP hash:	ESP hash method
Status:	Enable or disable Dead Peer Detection.
Detection cycle [sec]:	Set the delay (in seconds) between Dead Peer Dectection (RFC 3706) keepalives (R_U_THERE, R_U_THERE_ACK) that are sent for this connection (default 30 seconds).
Failure count:	The number of unanswered DPD R_U_THERE requests until the IPsec peer is considered dead (M!DGE/MG102 will try to reestablish a dead connection automatically)

PPTP Server



PPTP Server Administration

PPTP administrative status: ○ enabled ● disabled

PPTP Server Configuration

Server Address: specific 192.168.1.1

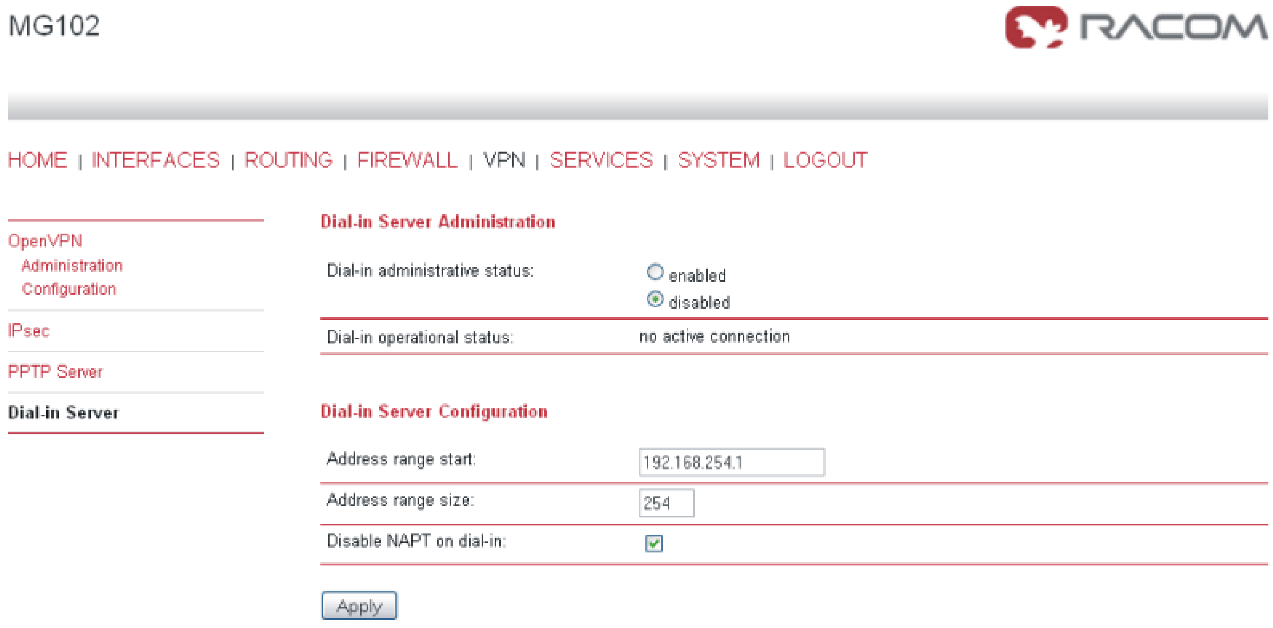
Client address range start: 192.168.1.200

Client address range size: 5

The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP is popular because it is easy to configure and it was the first VPN protocol that was supported by Microsoft Dial-up Networking. Users that are allowed to connect to the PPTP server are defined under the section “User Accounts”.

Parameter	Description
PPTP state	Enable/disable PPTP server
PPTP address range start:	Address range start for PPTP server
PPTP address range size:	Address range size for PPTP server

Dial-in Server



Dial-in Server Administration

Dial-in administrative status: ○ enabled ● disabled

Dial-in operational status: no active connection

Dial-in Server Configuration

Address range start: 192.168.254.1

Address range size: 254

Disable NAPT on dial-in: ☑

On this page the Dial-in server of M!DGE/MG102 can be administrated and configured. Users that are allowed to dial-in are defined under the section “User Accounts”.

- **Dial-in Server Administration**

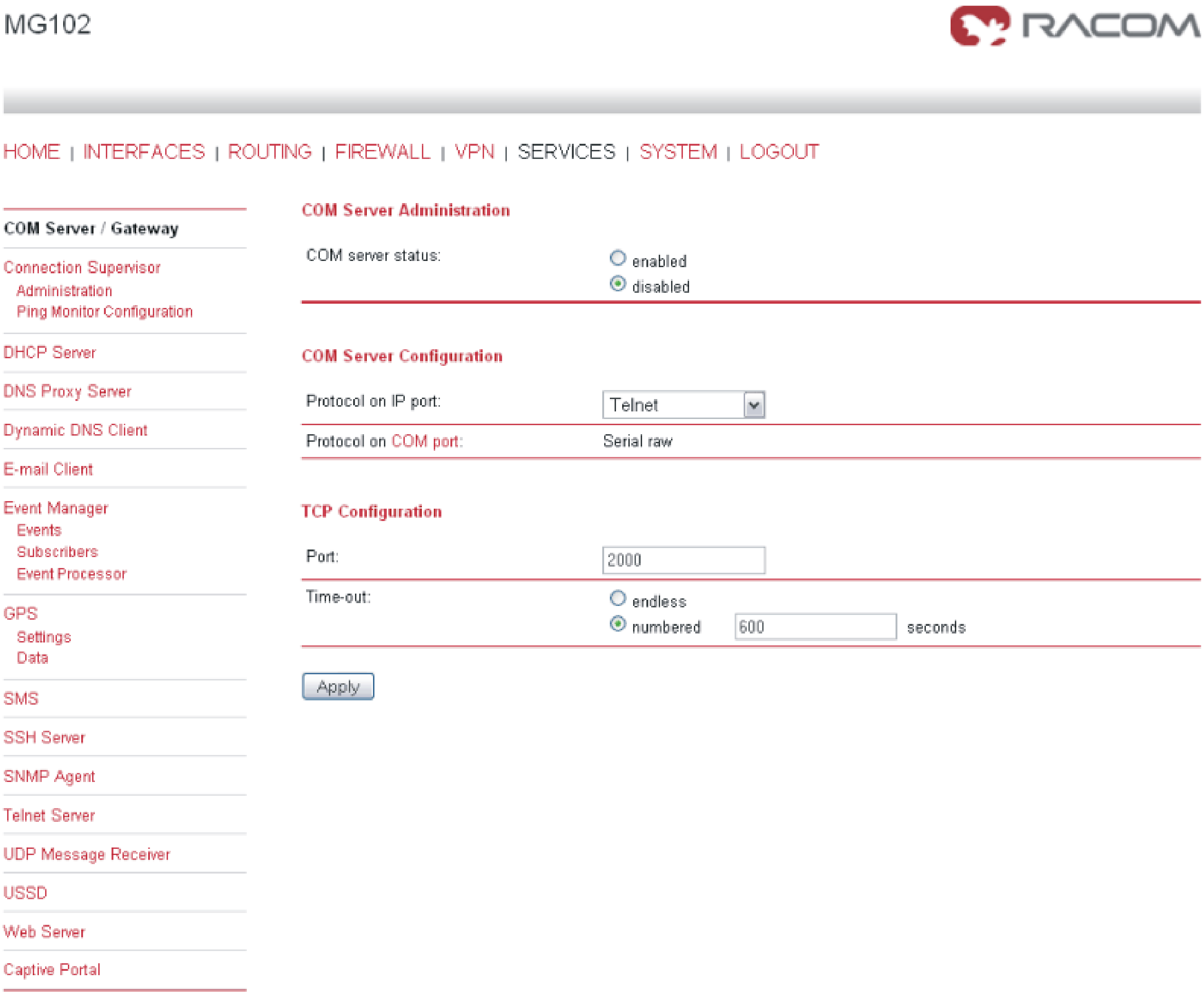
Parameter	Description
Dial-in administrative status:	The Dial-in server can be enabled or disabled. Consequently the device will allow incoming calls or not.
Dial-in operational status:	Shows whether a connection is active or not.

- **Dial-in Server Configuration**

Parameter	Description
Address range start:	Start address of the range for the dial-in server.
Address range size:	Number of addresses that the dial-in server can assign.

3.1.8. Services

COM Server / Gateway



COM Server Administration

COM server status: ○ enabled ● disabled

COM Server Configuration

Protocol on IP port: Telnet

Protocol on COM port: Serial raw

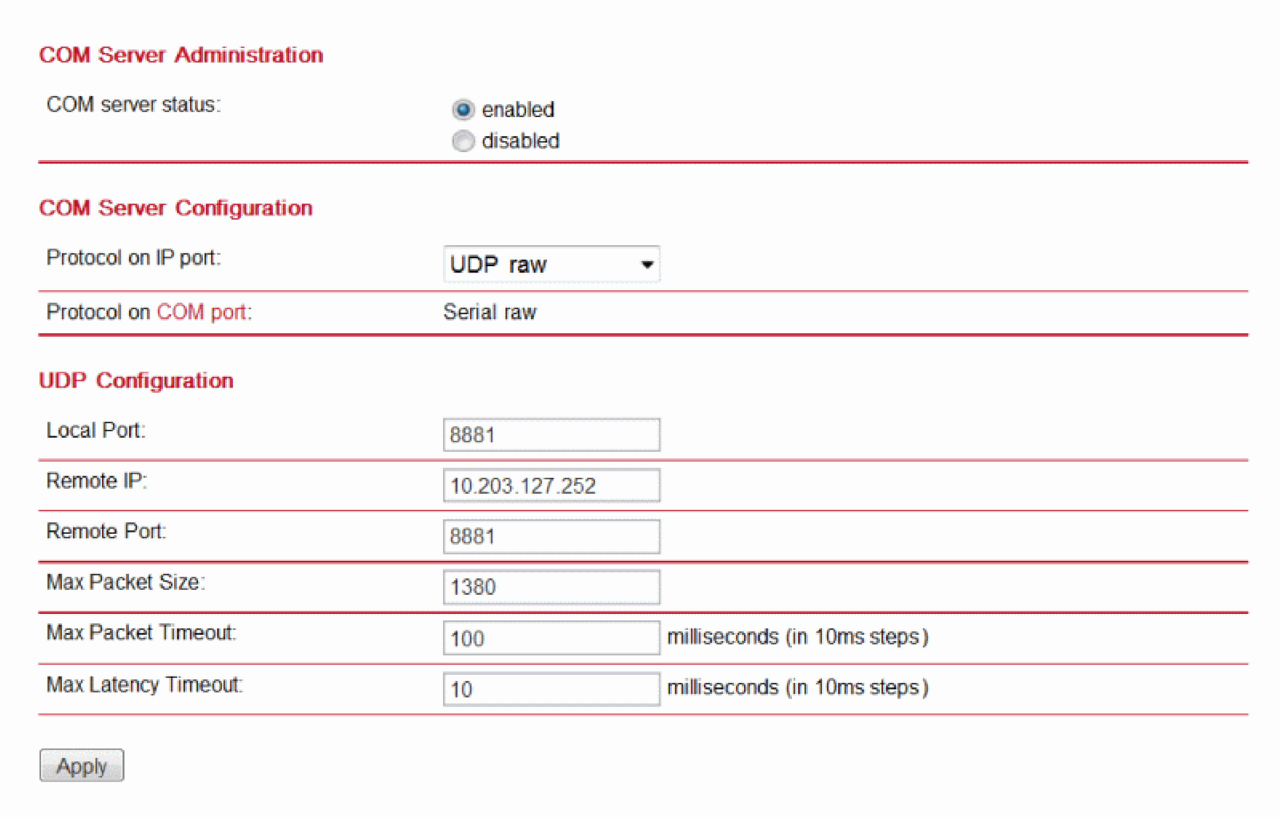
TCP Configuration

Port: 2000

Time-out: ○ endless ● numbered 600 seconds

Max Packet Size: Limits the package size to the configured value

- Max Packet Timeout: If data is received on serial line, waits for more data for the configured time to avoid to much segmentation which would lead on inefficiency
- Max Latency Timeout: Limits the maximum latency if the above criteria are not fulfilled



COM Server Administration

COM server status: ● enabled ○ disabled

COM Server Configuration

Protocol on IP port: UDP raw

Protocol on COM port: Serial raw

UDP Configuration

Local Port:	8881
Remote IP:	10.203.127.252
Remote Port:	8881
Max Packet Size:	1380
Max Packet Timeout:	100 milliseconds (in 10ms steps)
Max Latency Timeout:	10 milliseconds (in 10ms steps)

- **COM Server Administration**

Parameter	Description
COM server status:	The COM server / modbus gateway can be enabled or disabled.

- **COM Server Configuration**

Parameter	Description
Protocol on TCP/IP:	“Telnet” or “TCP raw” for COM server applications, “Modbus TCP” for modbus gateway
Protocol on COM port:	The protocol implicitely defined on the COM port.

- **TCP Configuration**

Parameter	Description
Protocol on COM port:	The protocol implicitely defined on the COM port.
Time-out	TCP – timeout in seconds or endless

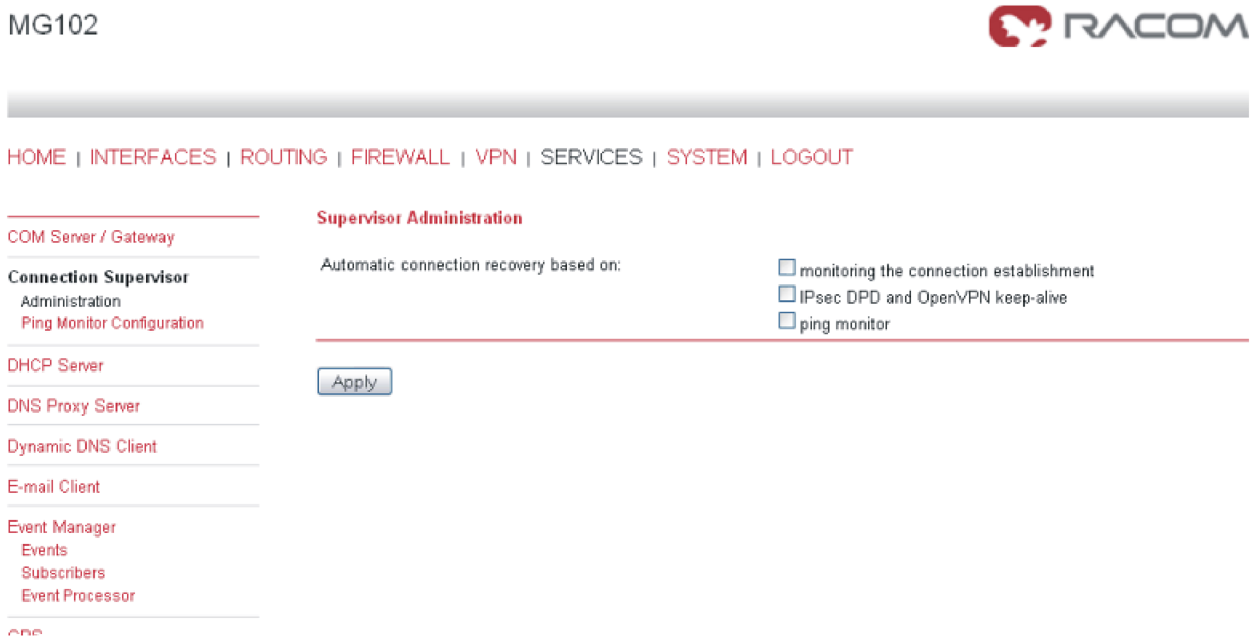
- **UDP Configuration**

Parameter	Description
Local Port	Local UDP port
Remote IP	IP address of remote

Parameter	Description
Remote Port	UDP port of remote
Max. Packet Size	Max. lenght of packet
Max. Packet Timeout	If data is received on serial line, waits for more data for the configured time to avoid to much segmentation which would lead on inefficiency
Max. Latency Timeout	Limits the maximum latency if the above criteria are not fulfilled

Connection Supervisor

The connection supervisor monitors connectivity and automatically recovers the connections in case of link loss.



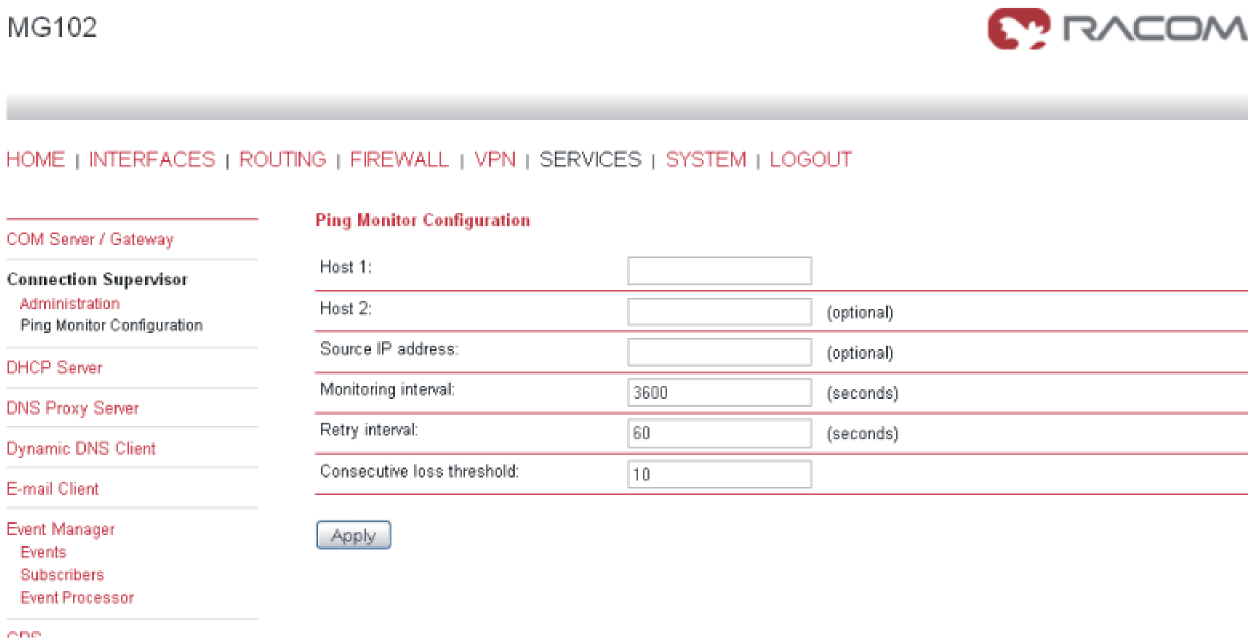
Supervisor Administration

Automatic connection recovery based on:

□ monitoring the connection establishment
□ IPsec DPD and OpenVPN keep-alive
□ ping monitor

First you should check the option “monitor connection establishment“ to make sure that problems during connections establishment are detected and recovered.

Second the active connection should be monitored. If you are running an IPsec or OpenVPN based VPN we recommend to use the protocol integrated monitoring service (IPsec DPD or OpenVPN keep-alive). Else you should configure and enable the ping monitor application.



Ping Monitor Configuration

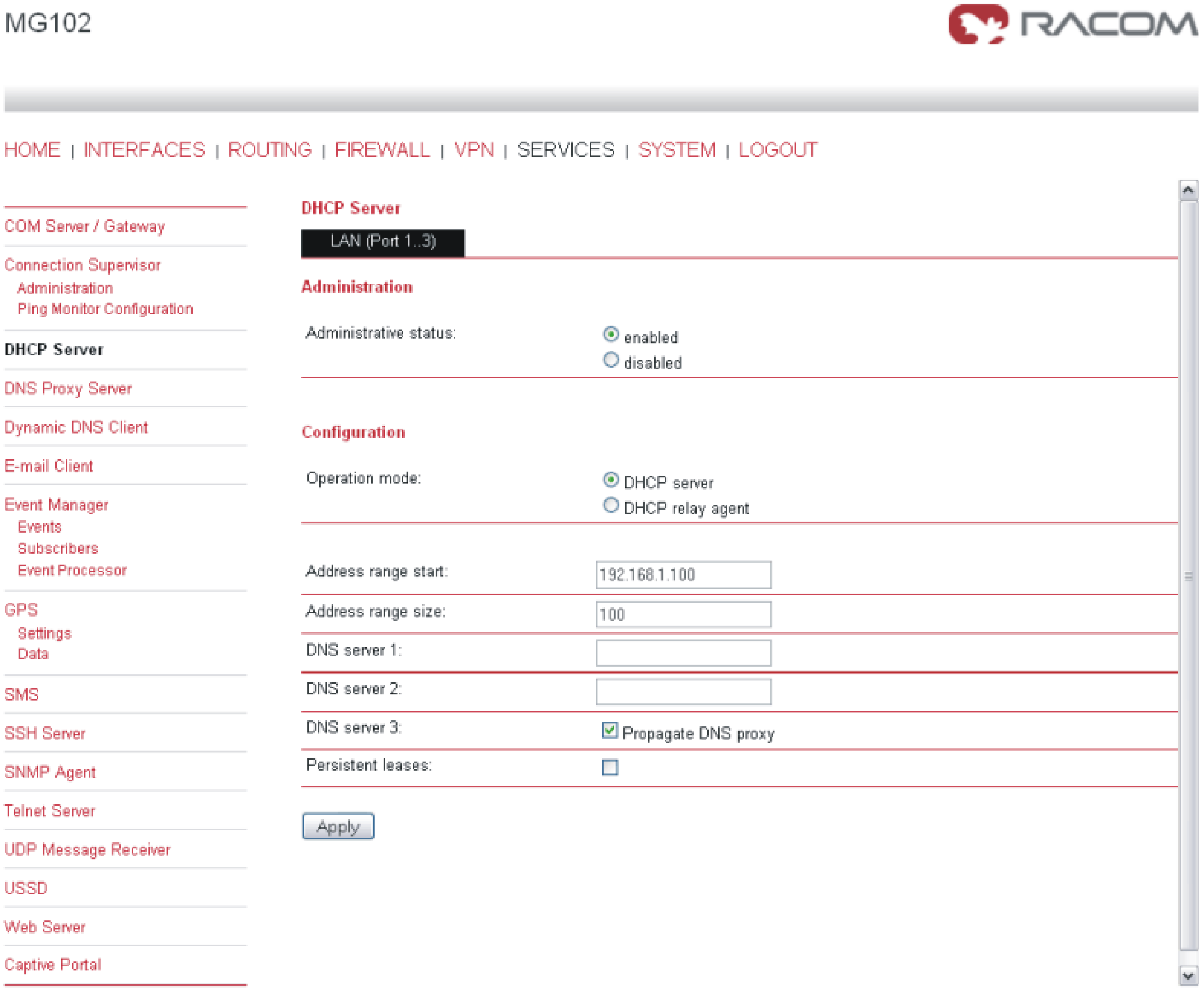
Host 1:		
Host 2:		(optional)
Source IP address:		(optional)
Monitoring interval:	3600	(seconds)
Retry interval:	60	(seconds)
Consecutive loss threshold:	10	

Parameter	Description
Host 1:	Reference host 1 to which IP connectivity is checked by sending probes.
Host 2:	Reference host 2 to which IP connectivity is checked by sending probes (optional). The test is considered successful if host 1 or 2 answers.
Source IP address:	Source IP address to be used as source of the ping probes.
Monitoring interval:	The time to wait before sending the next probe in case the last probe was successful.
Retry interval:	The time to wait until sending the next probe in case the last probe was unsuccessful.
Consecutive loss threshold:	Number of consecutive unsuccessful probes that are required until the next recovery action is initiated.
The recovery actions are:	1. Trying to reestablish a broken connection 2. Restart the internal modem 3. Restart the M!DGE/MG102

Note

If both Host1 and Host2 are not available the restarting with primary profile will follow. In case that IP health check is set for longer period that Ping monitor for internal switch to the fallback profile will NEVER be proceded.

DHCP Server



Administration

Administrative status:	● enabled ○ disabled

Configuration

Operation mode:	● DHCP server ○ DHCP relay agent
Address range start:	192.168.1.100
Address range size:	100
DNS server 1:	
DNS server 2:	
DNS server 3:	☑ Propagate DNS proxy
Persistent leases:	□

The DHCP server assigns the following information:

1. Any IP address out of the configured range
2. As default gateway the IP address of M!DGE/MG102 is assigned
3. As DNS server the IP address of M!DGE/MG102 is assigned or manually configured DNS servers

- **DHCP Server Administration**

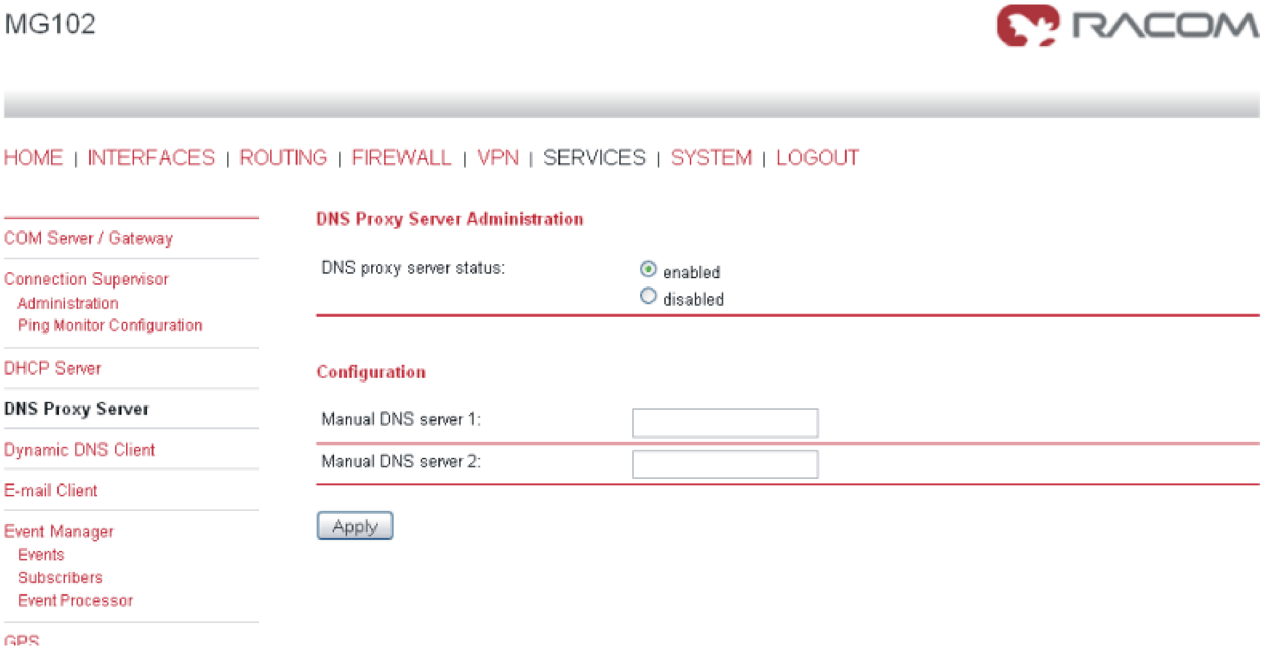
Parameter	Description
DHCP server status:	The Dynamic Host Configuration Protocol (DHCP) server can be enabled or disabled. If it is enabled it will answer to DHCP requests of devices in the LAN.

- **DHCP Server Configuration**

Parameter	Description
Address range start:	Address range start for DHCP server

Parameter	Description
Address range size:	Address range size for DHCP server
DNS server 1:	Manually configured first DNS server
DNS server 2:	Manually configured second DNS server
DNS server 3:	Propagate DNS proxy server as third DNS server

DNS Proxy Server



DNS Proxy Server Administration

DNS proxy server status: ● enabled ○ disabled

Configuration

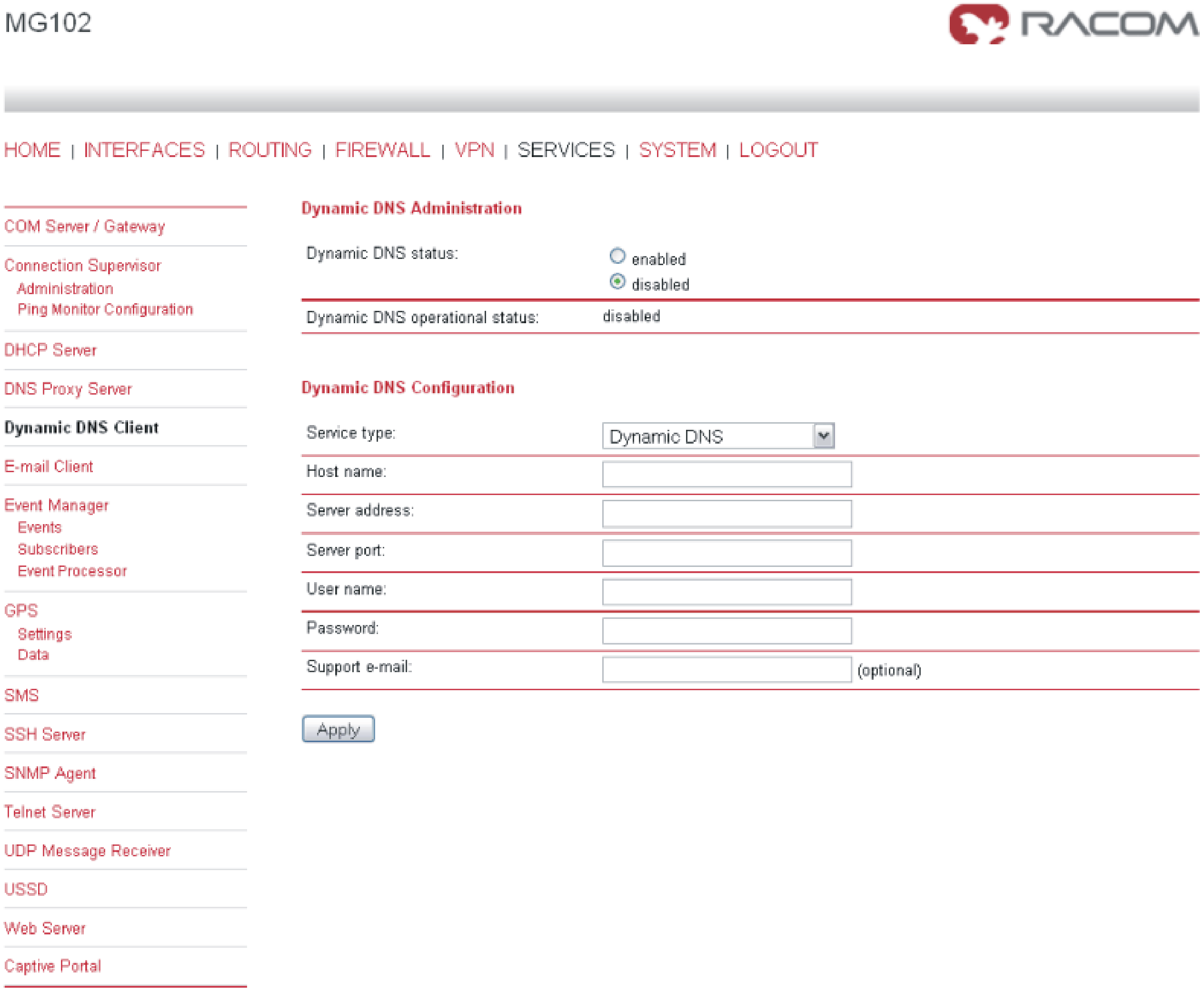
Manual DNS server 1:

Manual DNS server 2:

The DNS Proxy enabled M!DGE/MG102 forwards DNS requests to the DNS server provided by the mobile operator. Devices within the M!DGE/MG102 LAN may be configured to use M!DGE/MG102 as DNS server.

Parameter	Description
DNS proxy server status:	Enabled or disabled

Dynamic DNS



Dynamic DNS Administration

Dynamic DNS status:	○ enabled ● disabled
Dynamic DNS operational status:	disabled

Dynamic DNS Configuration

Service type:	Dynamic DNS
Host name:	
Server address:	
Server port:	
User name:	
Password:	
Support e-mail:	(optional)

The Dynamic DNS Client of M!DGE/MG102 is completely compatible to the Dynamic Network Services provided by the organization DynDNS (www.dyndns.com).

- **Dynamic DNS Administration**

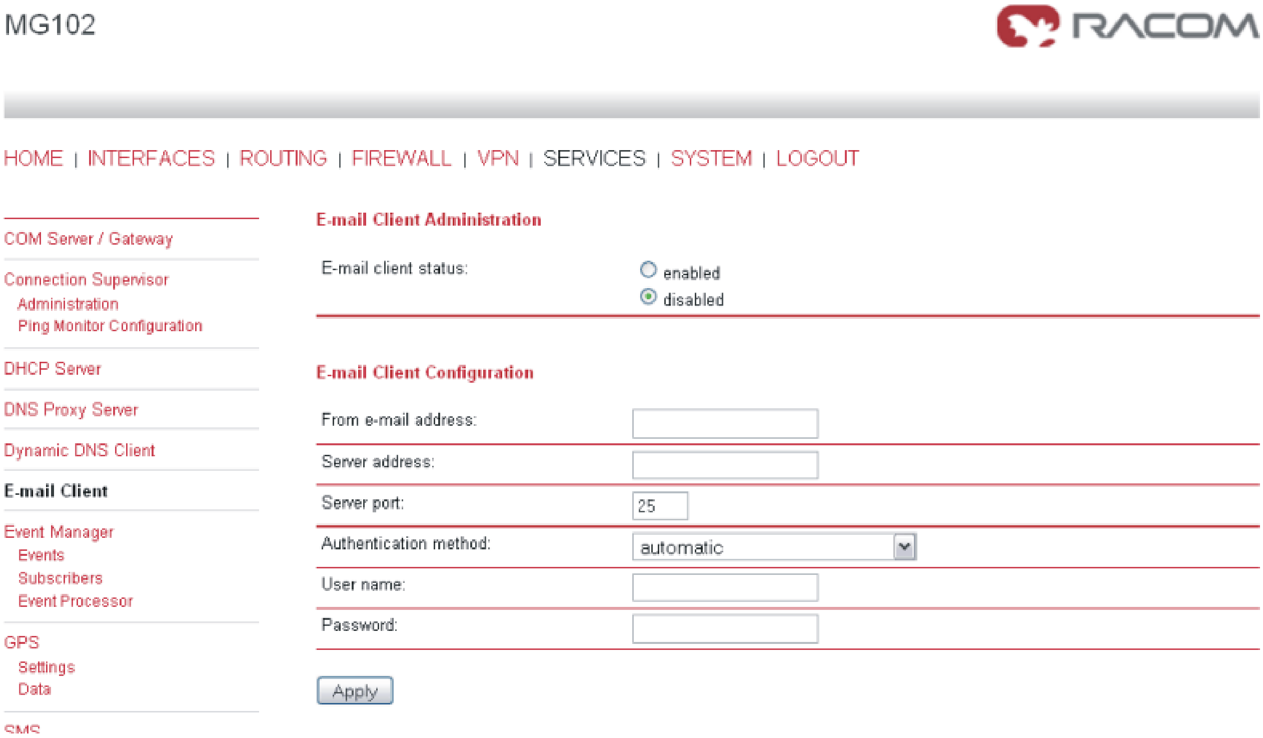
Parameter	Description
Dynamic DNS status:	Enable or disable the Dynamic DNS Client

- **Dynamic DNS Configuration**

Parameter	Description
Service type:	DynDNS Service according Dynamic Network Services, Inc. (www.dyndns.com). Please consult www.dyndns.com for more details.
Host name:	URL under which M!DGE/MG102 will be available, e.g. my M!DGE/MG102.dyndns.org
Server address:	Server IP Address or URL, normally members.dyndns.org
Server port:	TCP Port of the Dynamic DNS Server, e.g. 80 or 8245

Parameter	Description
User name:	Username
Password:	Password
Support e-mail:	Optional support e-mail address

E-mail Client



E-mail Client Administration

E-mail client status: ○ enabled ● disabled

E-mail Client Configuration

From e-mail address:	
Server address:	
Server port:	25
Authentication method:	automatic
User name:	
Password:	

- **E-Mail Client Administration**

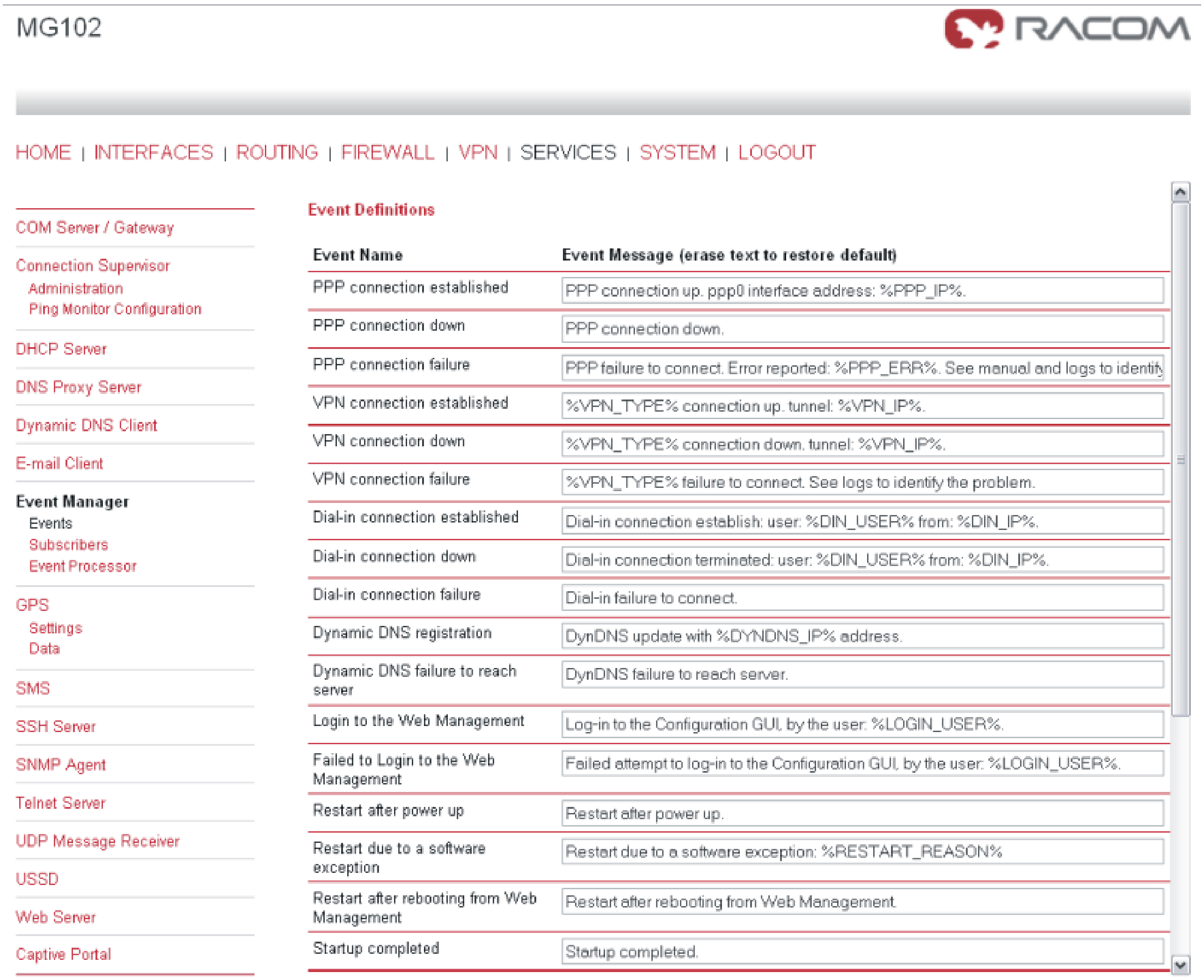
Parameter	Description
E-mail client status:	Sending e-mail can be enabled or disabled. Disabling the e-mail client means that no notification via e-mail will be performed.

- **E-mail Client Configuration**

Parameter	Description
From e-mail address:	Sender’s e-mail address
Server address:	SMTP server address
Server port:	Default port for SMTP is 25
Authentication required:	If enabled M!DGE/MG102 will logon to SMTP server before sending e-mails
User name:	Username
Password:	Password

Event Manager

- **Events**



MG102

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

- COM Server / Gateway
- Connection Supervisor
  - Administration
  - Ping Monitor Configuration
- DHCP Server
- DNS Proxy Server
- Dynamic DNS Client
- E-mail Client
- Event Manager
  - Events
  - Subscribers
  - Event Processor
- GPS
  - Settings
  - Data
- SMS
- SSH Server
- SNMP Agent
- Telnet Server
- UDP Message Receiver
- USSD
- Web Server
- Captive Portal

Event Definitions

Event Name	Event Message (erase text to restore default)
PPP connection established	PPP connection up. ppp0 interface address: %PPP_IP%.
PPP connection down	PPP connection down.
PPP connection failure	PPP failure to connect. Error reported: %PPP_ERR%. See manual and logs to identify
VPN connection established	%VPN_TYPE% connection up. tunnel: %VPN_IP%.
VPN connection down	%VPN_TYPE% connection down. tunnel: %VPN_IP%.
VPN connection failure	%VPN_TYPE% failure to connect. See logs to identify the problem.
Dial-in connection established	Dial-in connection establish: user: %DIN_USER% from: %DIN_IP%.
Dial-in connection down	Dial-in connection terminated: user: %DIN_USER% from: %DIN_IP%.
Dial-in connection failure	Dial-in failure to connect.
Dynamic DNS registration	DynDNS update with %DYNDNS_IP% address.
Dynamic DNS failure to reach server	DynDNS failure to reach server.
Login to the Web Management	Log-in to the Configuration GUI, by the user: %LOGIN_USER%.
Failed to Login to the Web Management	Failed attempt to log-in to the Configuration GUI, by the user: %LOGIN_USER%.
Restart after power up	Restart after power up.
Restart due to a software exception	Restart due to a software exception: %RESTART_REASON%
Restart after rebooting from Web Management	Restart after rebooting from Web Management.
Startup completed	Startup completed.

There are several predefined system events. If such an event occurs a notification message to SMS or e-mail recipients if such an events

Parameter	Description
PPP connection established	PPP connection up. ppp0 interface address: %PPP_IP%.
PPP connection down	PPP connection down.
PPP connection failure	PPP failure to connect. Error reported: %PPP_ERR%. See manual and logs to identify the problem.
VPN connection established	VPN connection up. tun0/tap0 interface address: %VPN_IP%.
VPN connection down	VPN connection down.
VPN connection failure	VPN failure to connect. See logs to identify the problem.
Dial-in connection established	Dial-in connection establish: user: %DIN_USER% from: %DIN_IP%.
Dial-in connection down	Dial-in connection terminated: user: %DIN_USER% from: %DIN_IP%.

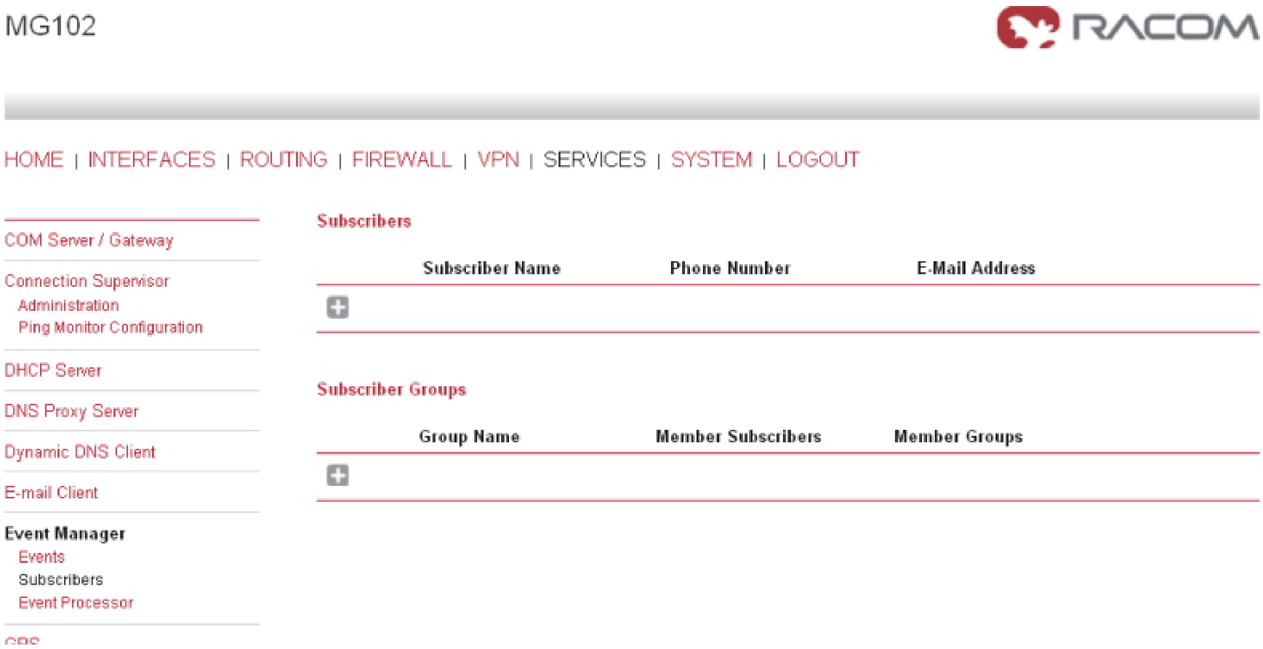
Parameter	Description
Dial-in connection failure	Dial-in failure to connect.
Dynamic DNS registration	DYNDNS update with %DYNDNS_IP% address.
Dynamic DNS failure to reach server	DynDNS failure to reach server.
Login to the Web Manager	Log-in to the Configuration GUI, by the user: %LOGIN_USER%.
Failed to Login to the Web Manager	Failed attempt to log-in to the Configuration GUI, by the user: %LOGIN_USER%.
Restart after power up	Restart after power up.
Restart due to a software exception	Restart due to a software exception.
Restart after rebooting from Web Management	Restart after rebooting from Web Management.
Restart due to Web Manager	Restart due to Web Manager.
Startup completed	Startup completed
Arriving UDP Message	%UDP_MESSAGE%
Test Event	This is a test.
GPS reception on	GPS position is available.
GPS reception off	GPS position is not available.
Digital Input 1 on	Input change: IN1 is On.
Digital Input 1 off	Input change: IN1 is Off.
Digital Input 2 on	Input change: IN2 is On.
Digital Input 2 off	Input change: IN2 is Off.
Digital Output 1 on	Output change: OUT1 is On, changed from %DIO_SOURCE%.
Digital Output 1 off	Output change: OUT1 is Off, changed from %DIO_SOURCE%.
Digital Output 2 on	Output change: OUT2 is On, changed from %DIO_SOURCE%.
Digital Output 2 off	Output change: OUT2 is Off, changed from %DIO_SOURCE%.

The following event variables will be replaced within event texts as follows:

Parameter	Description
%PPP_IP%	The current IP address on the mobile interface (ppp0)
%PPP_ERR%	Error message in case of mobile connection failure
%VPN_IP%	The current address of the OpenVPN interdface
%VPN_TYPE%	IPsec or OpenVPN
%DYNDNS_IP%	The IP address which has been sent to the DNS server
%DIN_USER%	User name which the dial-in connection has been authenticated against
%DIN_IP%	The IP address of the dial-in peer
%LOGIN_USER%	Name of the user who tried to log on to the Web Manager
%DIO_SOURCE%	Source that triggered an output change
%UDP_MESSAGE%	Text message that has been received by the message receiver

Parameter	Description
%RESTART_REASON%	Reason why a restart happened
%DST_IN1%	Status of digital input 1, possible values include [on, off]
%DST_IN2%	Status of digital input 2, possible values include [on, off]
%DST_OUT1%	Status of digital output 1, possible values include [on, off]
%DST_OUT2%	Status of digital output 2, possible values include [on, off]

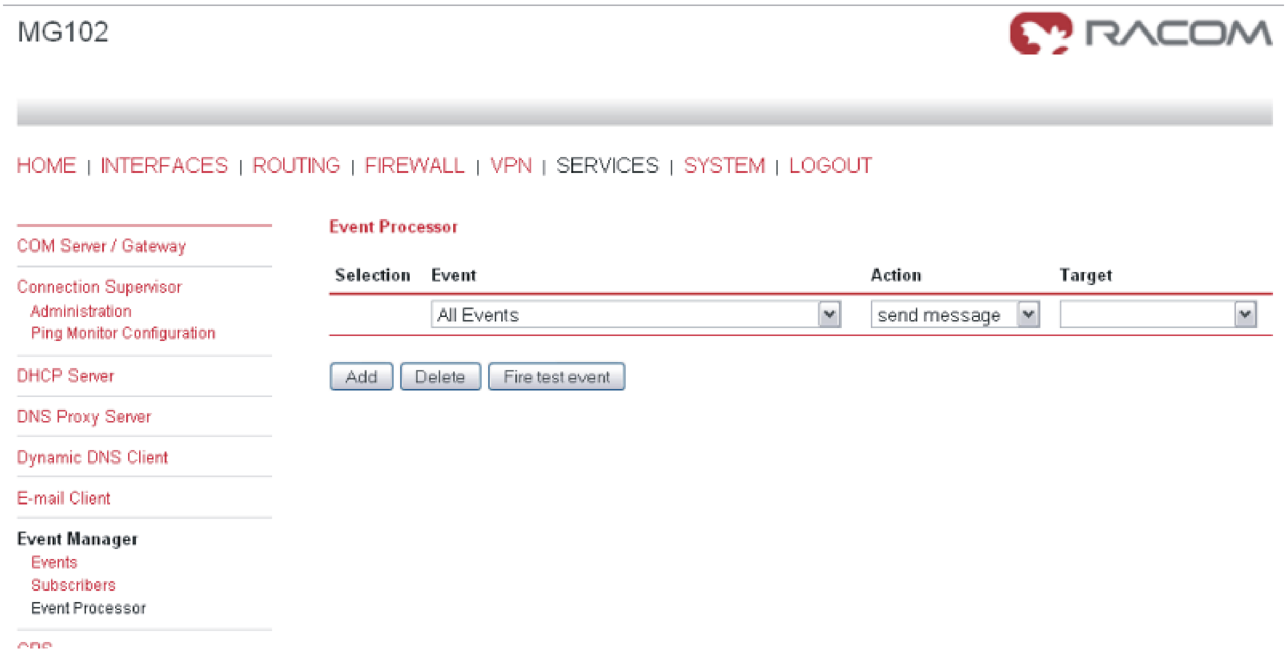
- **Subscribers**



Subscribers are recepients of SMS or e-mail event notifications.

It is possible to create groups and fill them with users and other groups. This mechanism let you send event notifications to multiple destinations/users.

- **Event Processor**

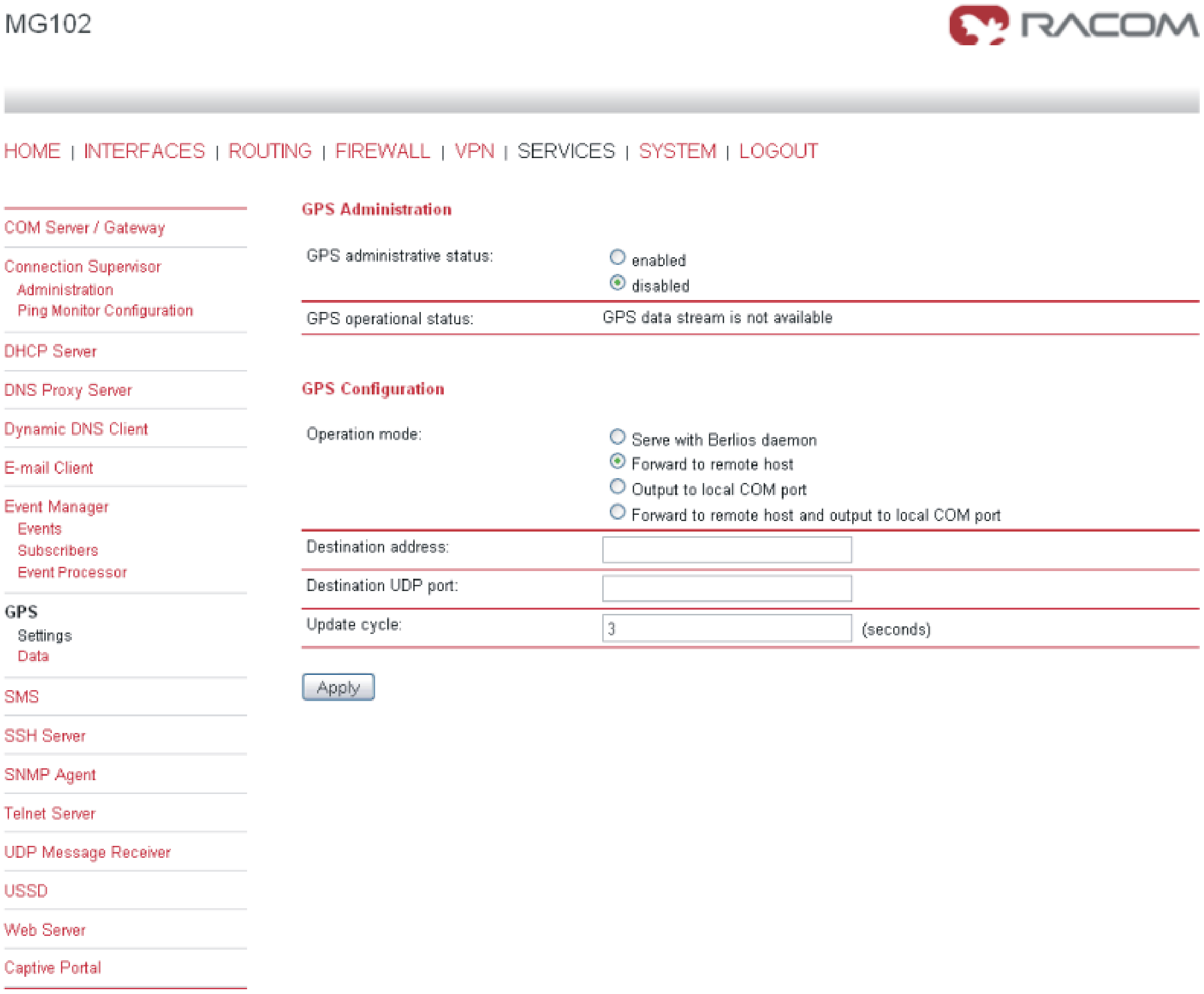


Event Processor

Selection	Event	Action	Target
	All Events	send message	

Notifications can be generated or digital outputs can be set based on the occurrence of several events.

GPS



GPS Administration

GPS administrative status:	○ enabled ● disabled
GPS operational status:	GPS data stream is not available

GPS Configuration

Operation mode:	○ Serve with Berlios daemon ● Forward to remote host ○ Output to local COM port ○ Forward to remote host and output to local COM port
Destination address:	
Destination UDP port:	
Update cycle:	3 (seconds)

This feature is available on MG102xGx.

If valid GPS data is available (at least 3 satellites available) it will be sent as UDP payload to the configured host. The content of such a data package is separated into two lines. The first line contains GPS data in the GPGGA format; the second line contains GPRMC data.

For more information on the GPS data stream see chapter Section 4.1, “GPS Server”

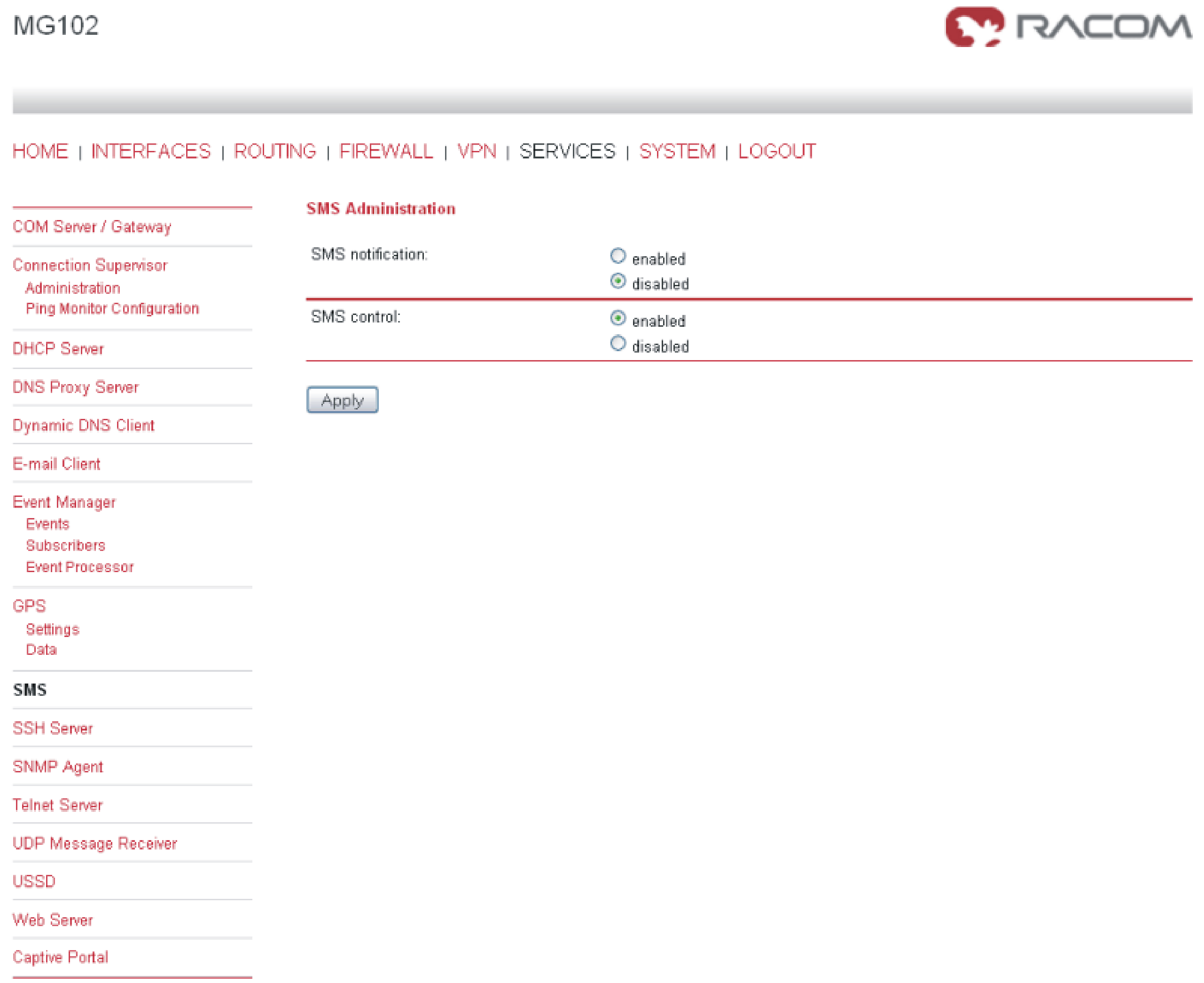
Parameter	Description
GPS status:	Enable or disable GPS data stream
Destination address:	Destination address of application where the GPS data will be sent to
Destination UDP port:	Destination UDP port of application where the GPS data will be sent to
GPS update cycle:	The refresh cycle / frequency of sending data

- **GPS Data**

  GPS Data is only supported with activated Berlios GPS daemon. Go to GPS Settings to configure.

SMS

SMS can be used to control M!DGE/MG102 and for event notification.



SMS Administration

SMS notification: ○ enabled ● disabled

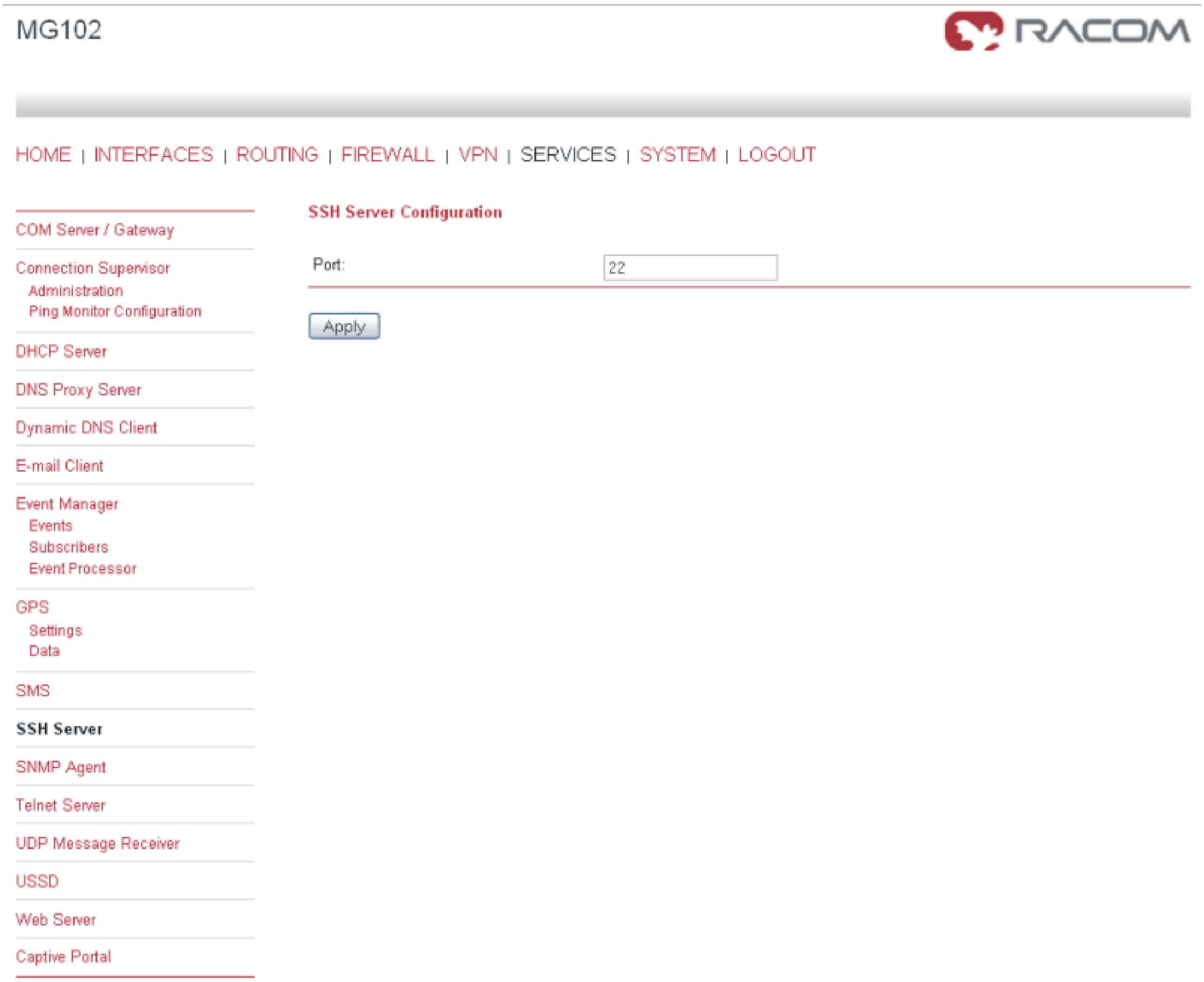
SMS control: ● enabled ○ disabled

Parameter	Description
SMS notification:	Sending SMS can be enabled or disabled. Disabling sending SMS means that no notification via SMS will be performed.
SMS control:	Receiving SMS can be enabled or disabled. Disabling receiving SMS means that controlling M!DGE/MG102 via SMS will not be possible.

Command	Parameters	Description
status	—	A SMS with the following information will be returned • Signal strength • Mobile connection state (up/down) • current IP address of the mobile (ppp) interface • current IP address of the VPN interface (if enabled)

Command	Parameters	Description
connect	—	This will initiate a Dial-out connection over GSM and the VPN connection (if enabled) and trigger sending an SMS with the following information: • current IP address of the PPP interface • current IP address of the VPN interface (if enabled) The profile name is an optional parameter.
disconnect	—	terminates all connections on the mobile interface (Dial-out and VPN)
reboot	—	M!DGE/MG102 will be restarted
method	manual	Set administrative status of the mobile connection to disabled
	permanent	Set administrative status of the mobile connection to enabled, permanent.
	dialondemand	Set administrative status of the mobile connection to enabled, dial on demand.
output	1 on	Switch output 1 on
	1 off	Switch output 1 off
	2 on	Switch output 1 on
	2 off	Switch output 2 off

SSH Server



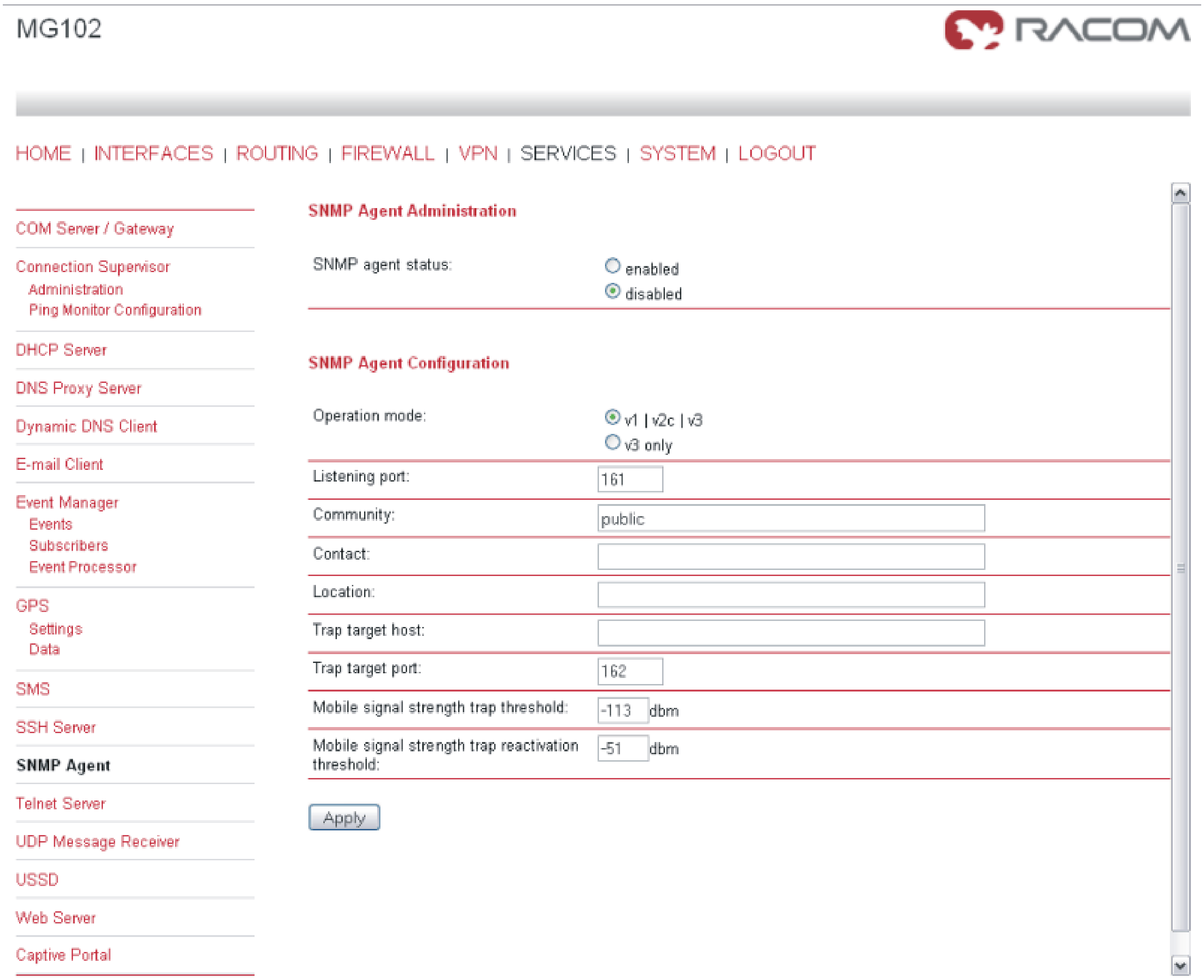
SSH Server Configuration

Port: 22

Parameter	Description
Port:	SSH server port

The standard port 22 is used. For higher security change it to different number. This number shall be used as parametr in SSH command.

SNMP Agent



SNMP Agent Administration

SNMP agent status: ○ enabled ● disabled

SNMP Agent Configuration

Operation mode: ● v1 | v2c | v3 ○ v3 only

Listening port: 161

Community: public

Contact:

Location:

Trap target host:

Trap target port: 162

Mobile signal strength trap threshold: -113 dbm

Mobile signal strength trap reactivation threshold: -51 dbm

Parameter	Description
SNMP agent status:	Enable or disable the SNMP agent.
Listening Port:	SNMP agent port.
Community:	An SNMP community is the group that devices and management stations running SNMP belong to.
Contact:	System maintainer.
Location:	Location of the device.
Trap target host:	The host where the traps will be sent to.
Trap target port:	The port where the traps will be sent to.
Signal strength trap threshold dBm:	A trap will be sent, if signal strength goes lower than this.
Signal strength trap reactivation threshold dBm:	No further traps will be sent as long signal strengt his not higher than this.
Operation mode	SNMP version.

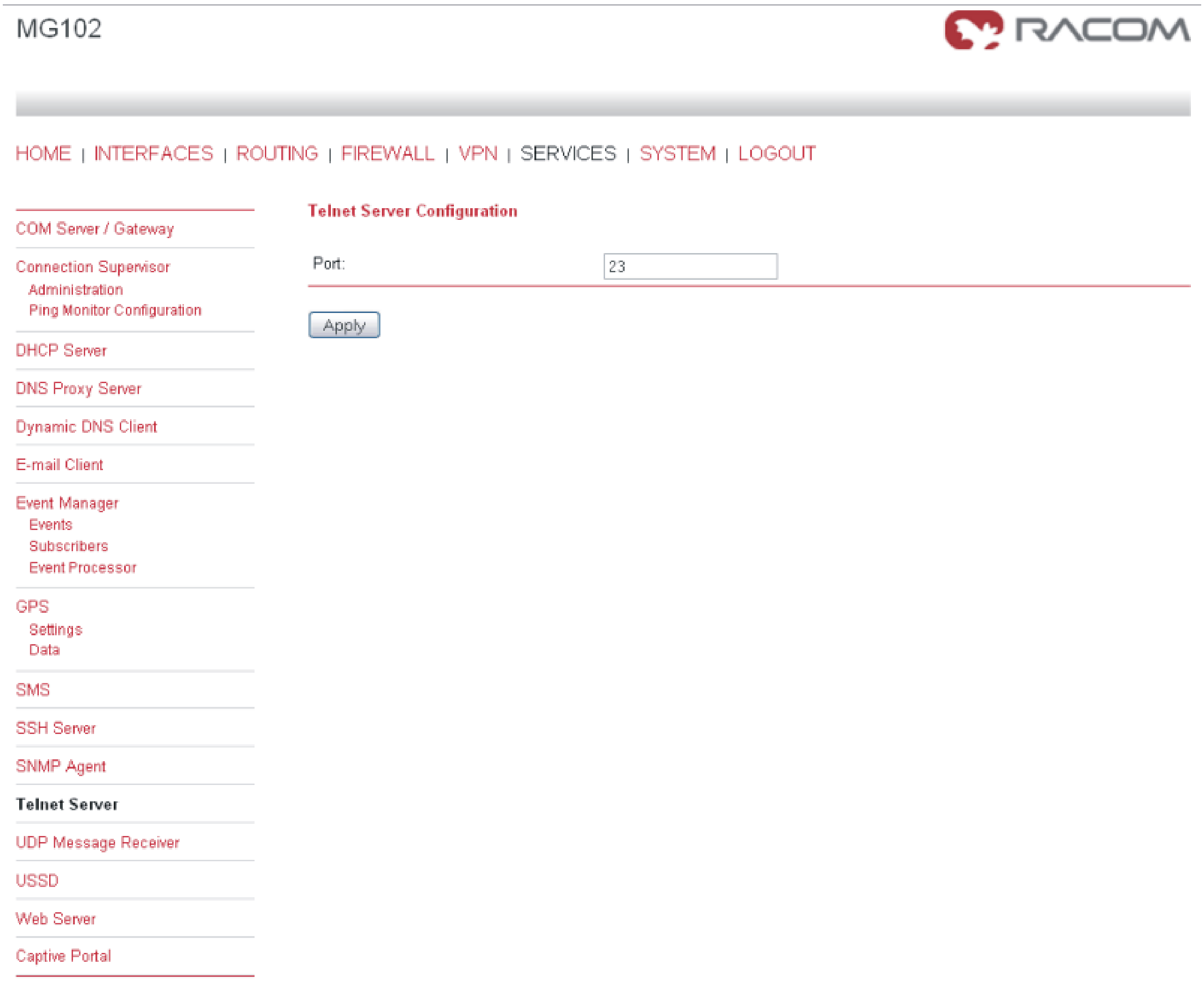
SNMP traps are generated in the following situations, if the SNMP agent is enabled:

- Startup of the M!DGE/MG102
- Shutdown of the M!DGE/MG102
- VPN connected
- VPN disconnected
- Signal Strength below „Signal strength trap threshold“

The startup trap is implemented using the standard coldStart & warmStart traps.

The system-shutdown trap is sent, when the system is rebooted via the reboot function of the web interface or when the watchdog reboots the system.

Telnet Server

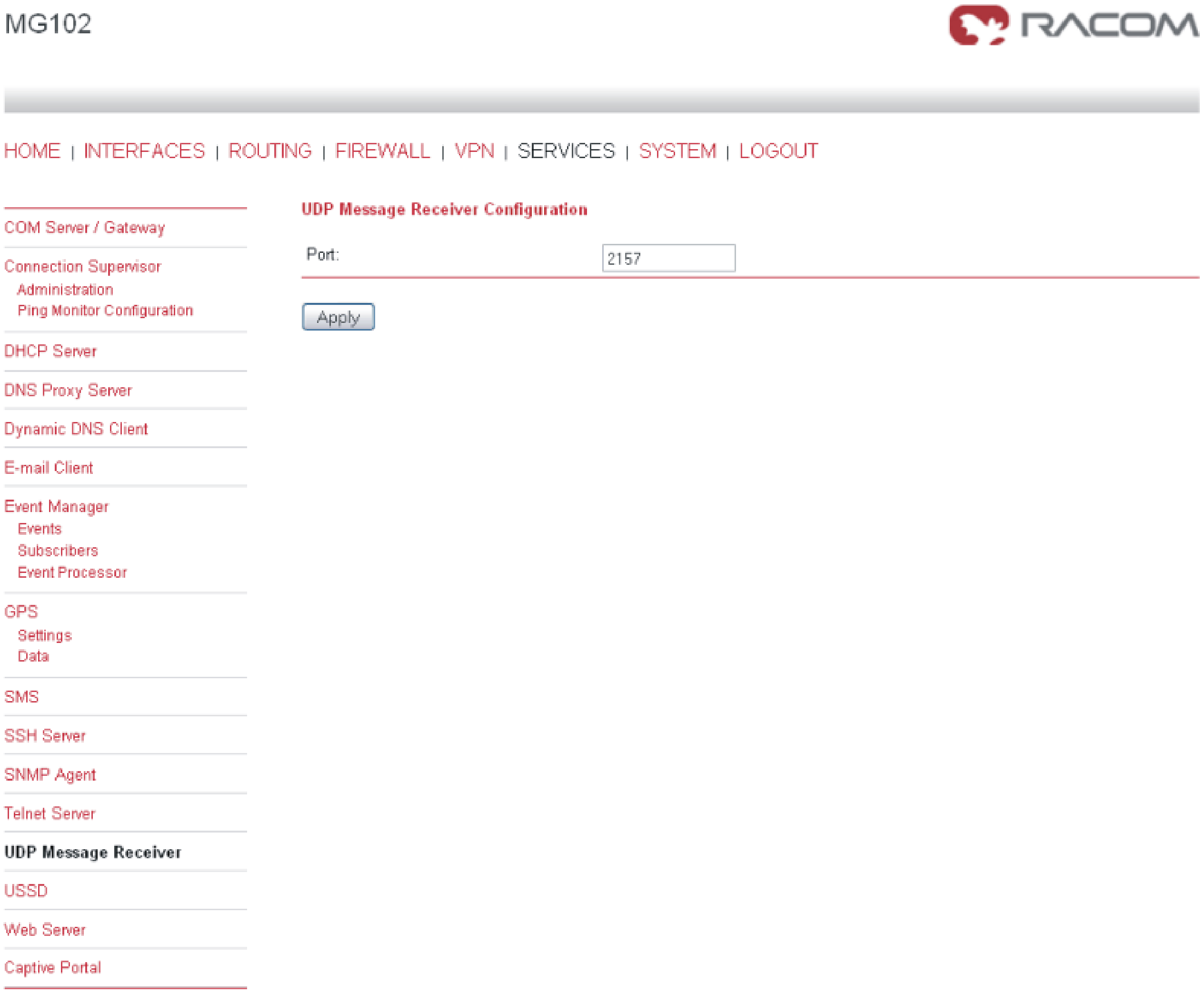


Telnet Server Configuration

Port: 23

Parameter	Description
Port:	Telnet server port

UDP Message Receiver



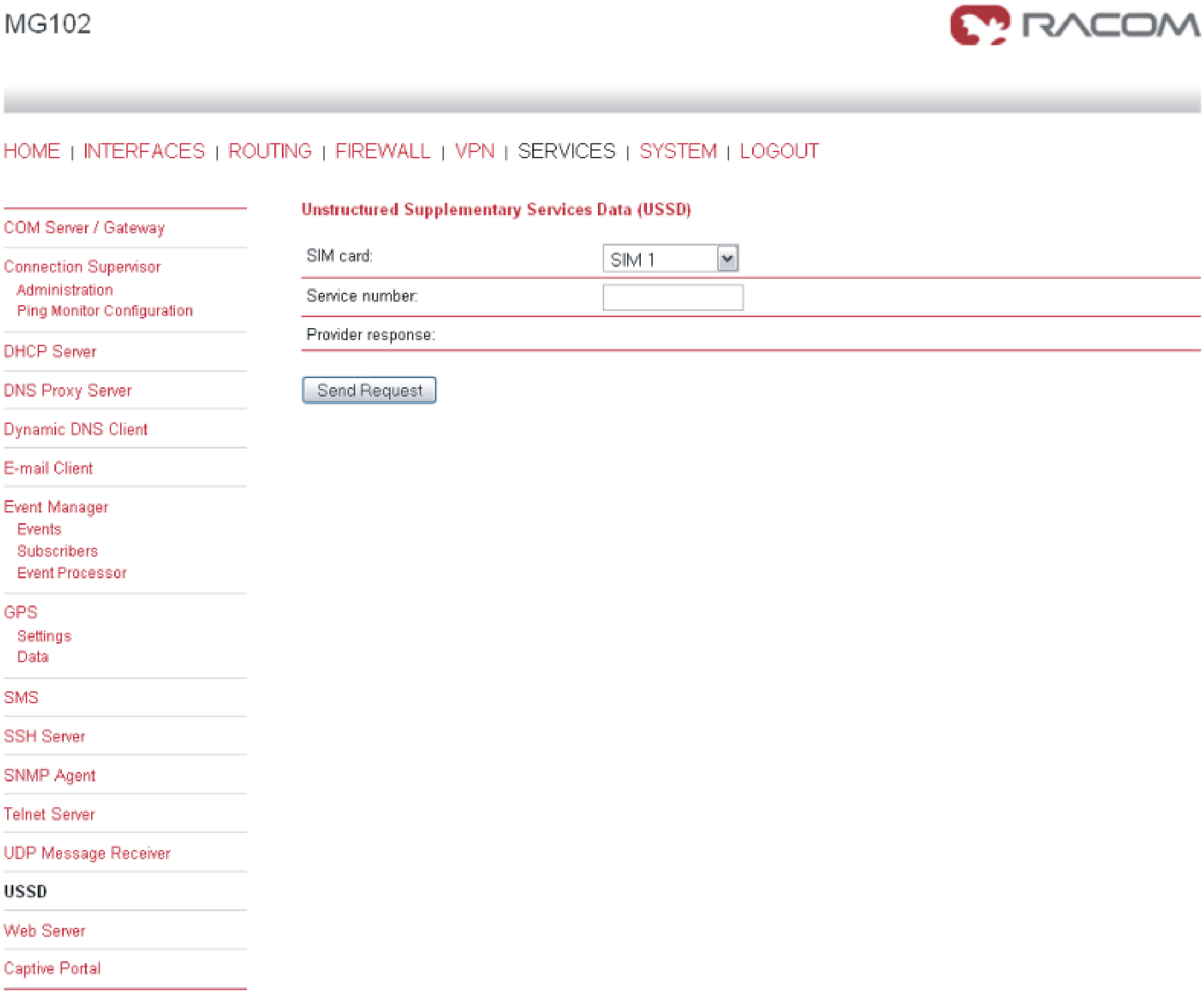
UDP Message Receiver Configuration

Port: 2157

Parameter	Description
Port:	UDP message receiver port

The UPD Message Receiver is a service that listens on the configured port (default 2157) for arriving UDP packets with a string in the payload. If an UPD package is arriving, the event “Arriving UDP Message” is fired (see chapter ???). Use the Event Manager (the section called “Event Manager”) to forward the message (UDP payload) to a SMS or E-mail destination.

Unstructured Supplementary Services Data (USSD)

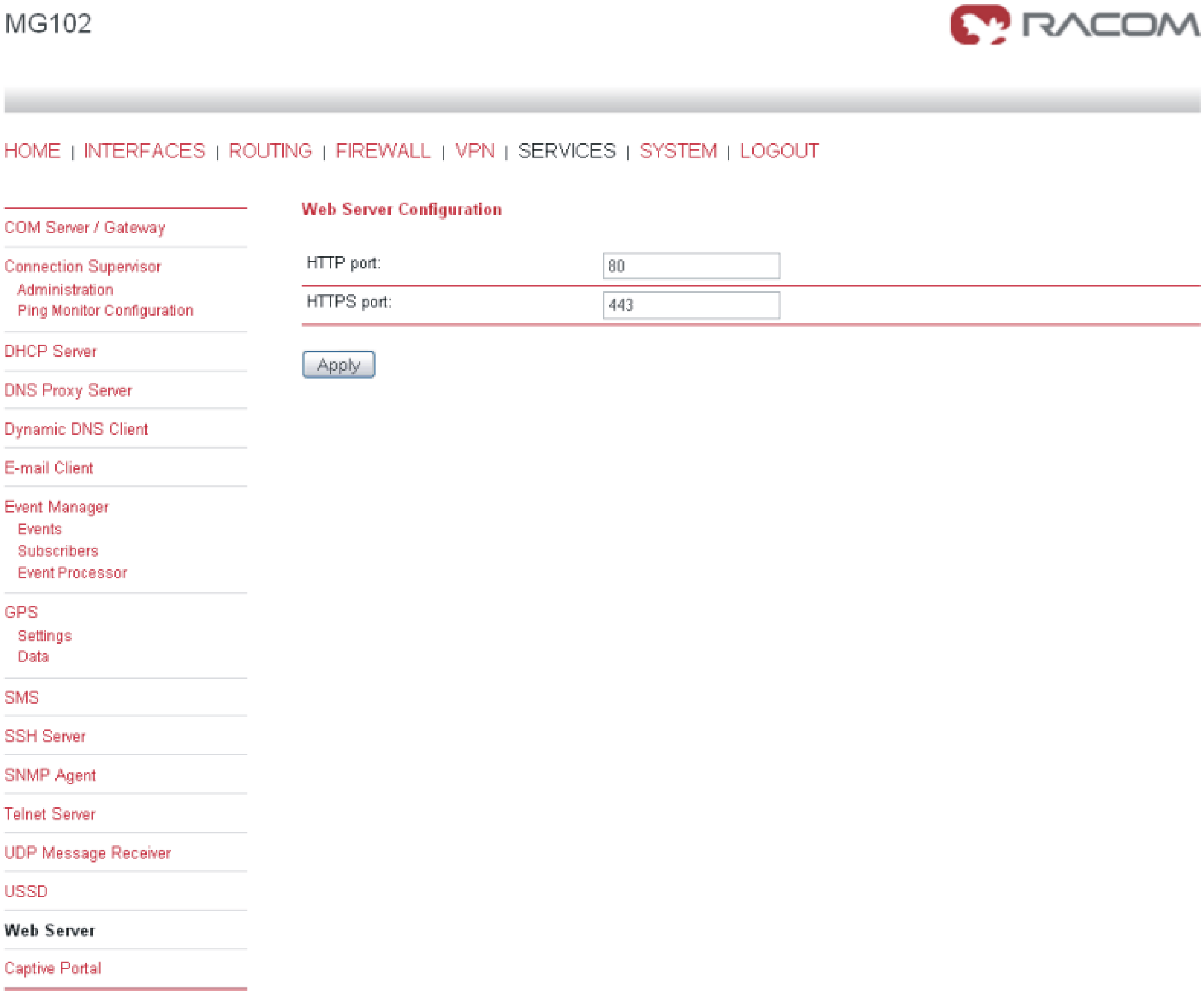


Unstructured Supplementary Services Data (USSD)

SIM card:	SIM 1
Service number:	
Provider response:	

Unstructured Supplementary Services Data (USSD) is a GSM service that allows high speed interactive communication between the subscribers and applications across a GSM Network. A sample USSD service is the bill status service accessed by dialing *141# or similar numbers in between * and # according to mobile network. Contact your mobile operator for further information.

Web Server



Web Server Configuration

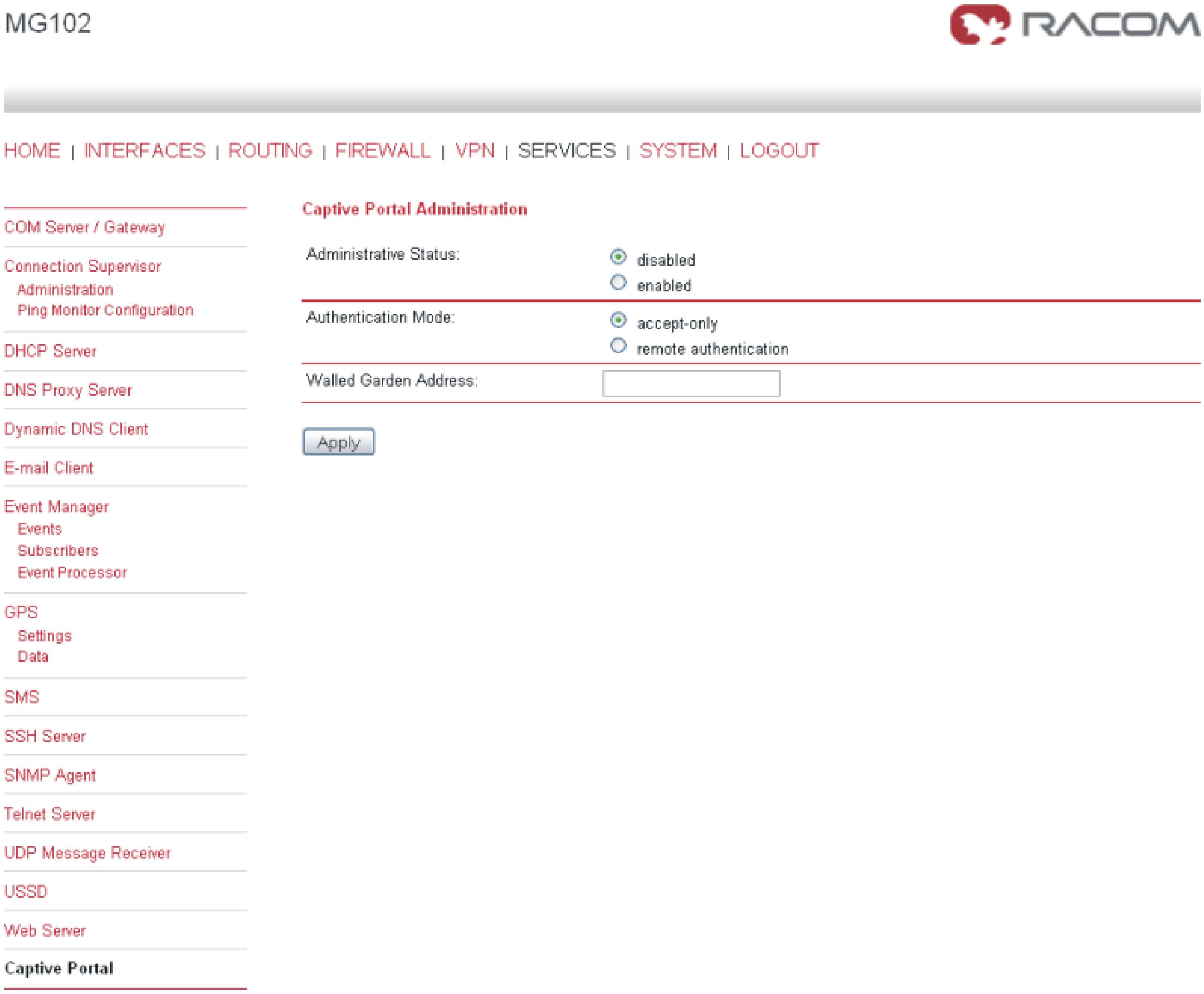
HTTP port: 80

HTTPS port: 443

Parameter	Description
HTTP port:	Web server port for http connections
HTTPS port:	Web server port for https connections

Captive Portal

The captive portal is used to redirect unauthorized WLAN/LAN clients to a login page where they have to authenticate against locally configured users or remotely over RADIUS.



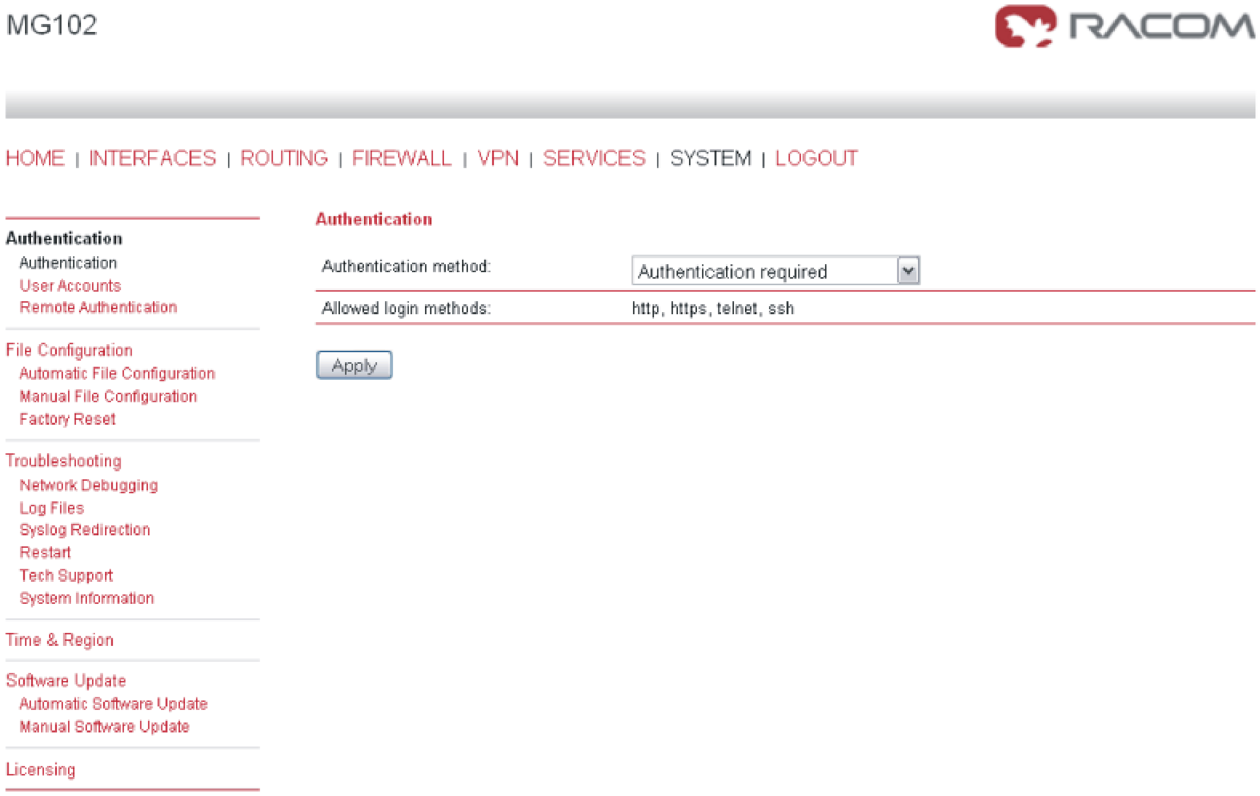
Captive Portal Administration

Administrative Status:	● disabled ○ enabled
Authentication Mode:	● accept-only ○ remote authentication
Walled Garden Address:	

Parameter	Description
Administrative Status:	Enable or disable the captive portal.
Authentication Mode:	Define whether user must accept by pressing a button or they have to authenticate to a RADUIS server.
Walled Garden Address:	Requests to this address are not being checked.

3.1.9. System

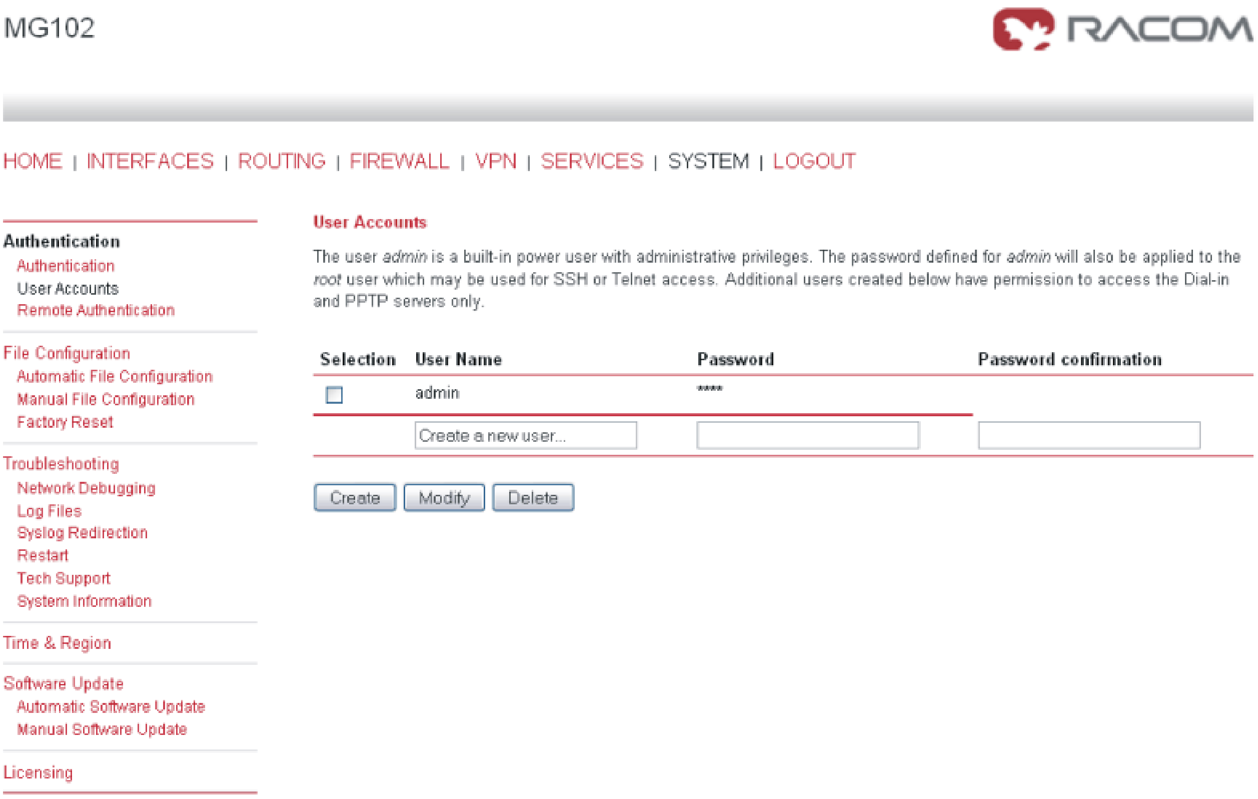
Authentication



Authentication

Authentication method:	Authentication required
Allowed login methods:	http, https, telnet, ssh

User Accounts



User Accounts

The user *admin* is a built-in power user with administrative privileges. The password defined for *admin* will also be applied to the *root* user which may be used for SSH or Telnet access. Additional users created below have permission to access the Dial-in and PPTP servers only.

Selection	User Name	Password	Password confirmation
□	admin	****	
	Create a new user...		

This page lets you manage the user accounts on the device.

The user **admin** is a built-in power user that has permission to access both the Web Manager and the Dial-in server. Any other user-defined user only has permission for dial-in connections.

Parameter	Description
User name	Define a user name
Enter password:	Define a password
Re-enter password:	Confirm the password

File Configuration

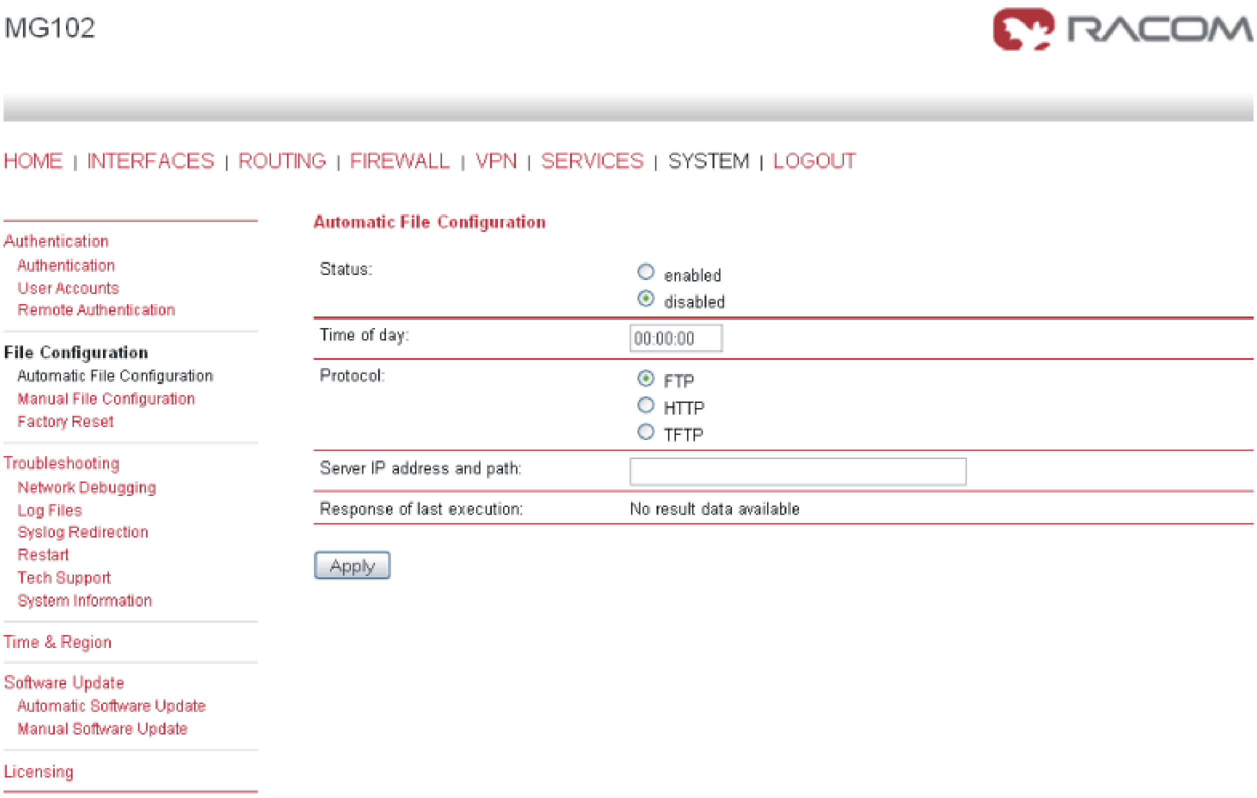
Configuration via the Web Manager becomes tedious for large volumes of devices. M!DGE/MG102 offers automatic and manual file-based configuration.

A single text file (*.cfg) or a zip archive (*.zip) containing one or more of the following files can be uploaded.

When uploading a zip file, the files included must be named as follows:

- user-config.cfg (the user configuration file)
- ca.crt.credential_mode (OpenVPN root certificate file for credential based authentication)
- ca.crt.certificate_mode (OpenVPN root certificate file for certificate based authentication)
- client.crt.certificate_mode (OpenVPN client certificate file)
- client.key.certificate_mode (OpenVPN private key file)
- templateProfiles (updating provider database)

- **Automatic File Configurration**



Automatic File Configuration

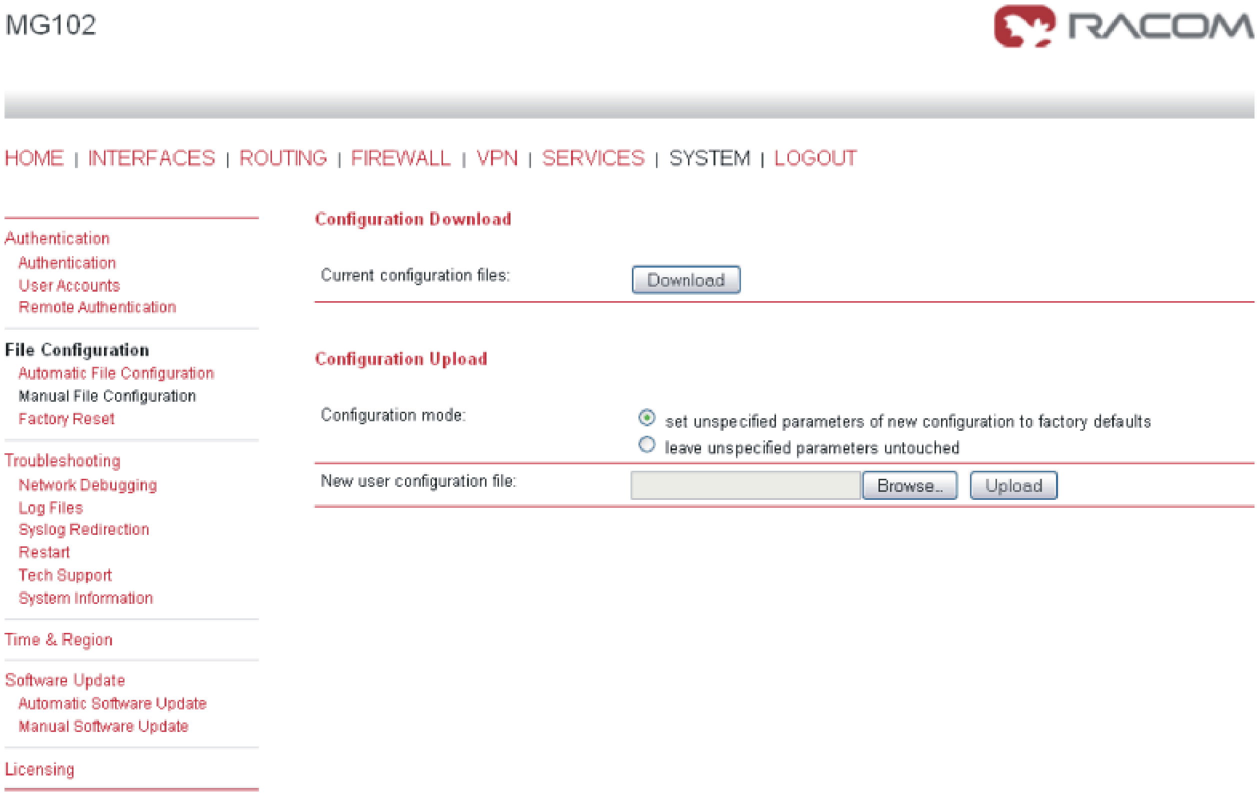
Status:	○ enabled ● disabled
Time of day:	00:00:00
Protocol:	● FTP ○ HTTP ○ TFTP
Server IP address and path:	
Response of last execution:	No result data available

Parameter	Description
Status:	Enable/disable automatic configuration update
Time of day:	Every day at this time M!DGE/MG102 will do a check for updates
Mode:	Update over mobile or Ethernet Interface?
Protocol:	Specify the protocol used to transfer the new user configuration file to M!DGE/MG102. You will need an appropriate server
Server IP address and path:	The server and directory where the new s configuration file can be downloaded
Last software update:	The result of the last try will be displayed here.

M!DGE/MG102 will only try to download the following files:

- <serialNumber>.cfg
- <serialNumber>.zip

- **Manual File Configuration**



Configuration Download

Current configuration files: Download

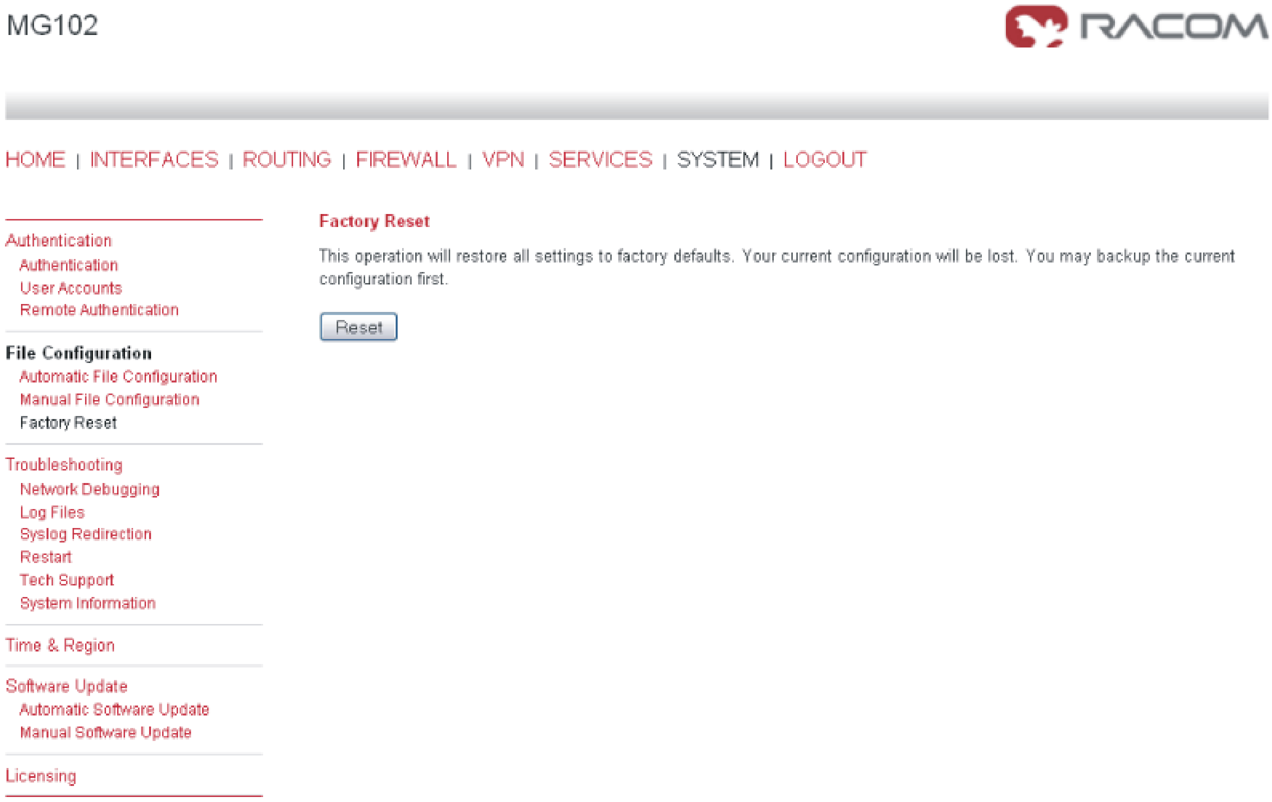
Configuration Upload

Configuration mode: ● set unspecified parameters of new configuration to factory defaults
○ leave unspecified parameters untouched

New user configuration file: Browse... Upload

Parameter	Description
Current configuration files:	Press [Download] will download a zip file name user-config.zip containing • user-config.cfg • ca.crt.credential_mode • ca.crt.certificate_mode • client.crt.certificate_mode • client.key.certificate_mode • templateProfiles if available.
New configuration files:	The following files are acceppted for upload: • *.cfg (max size 100KB) • *.zip (max size 100KB) The zip file may include • user-config.cfg • ca.crt.credential_mode • ca.crt.certificate_mode • client.crt.certificate_mode • client.key.certificate_mode • templateProfiles

- **Factory reset**



Factory Reset

This operation will restore all settings to factory defaults. Your current configuration will be lost. You may backup the current configuration first.

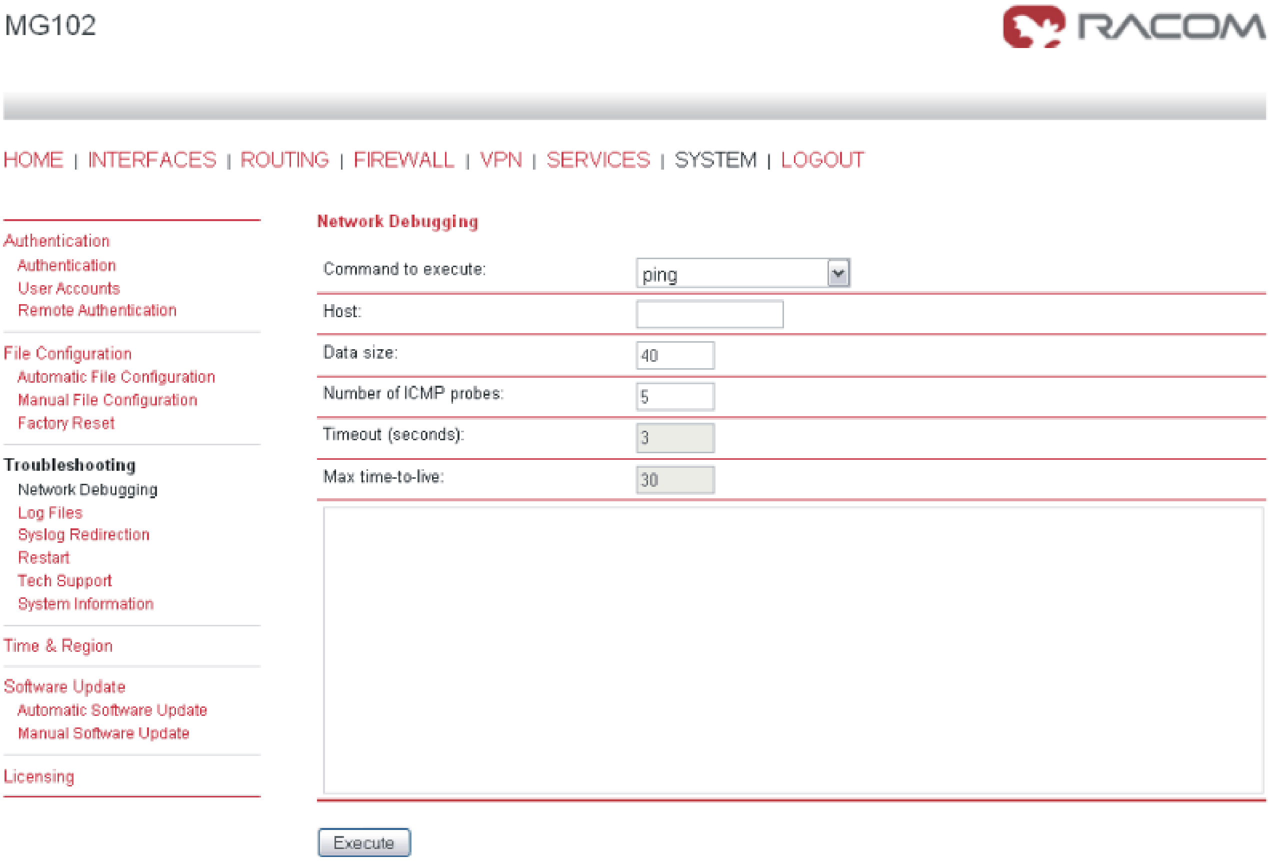
Press [Reset] to set the device to factory default. Your current configuration will be lost.

This action can also be initiated by pressing and holding the Reset button for at least five seconds.

The factory reset will also set the IP address of the Ethernet interface to 192.168.1.1. You will be able to communicate again with the device using the default network parameters.

Troubleshooting

- **Network Debugging**

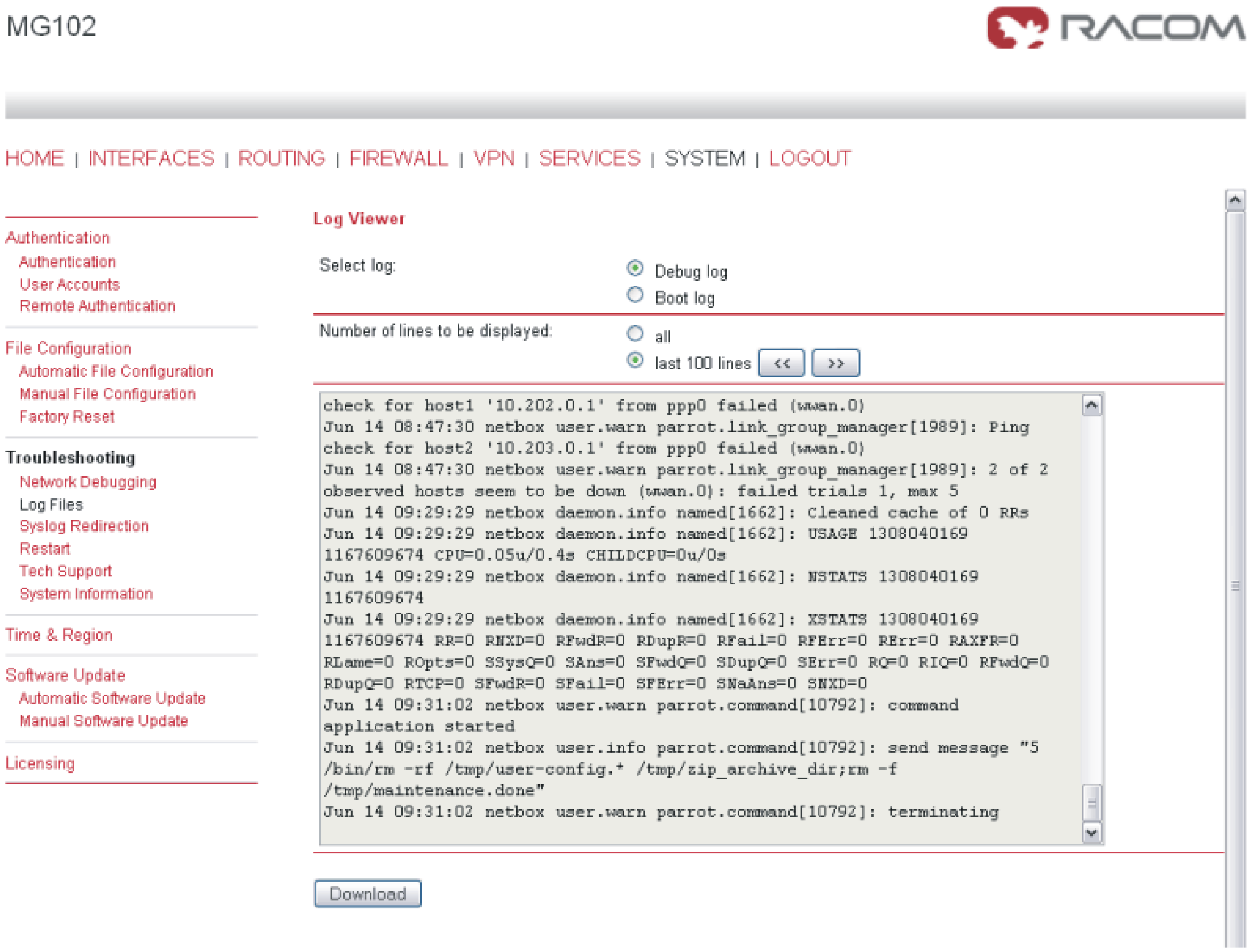


MG102

Network Debugging

Command to execute:	ping
Host:	
Data size:	40
Number of ICMP probes:	5
Timeout (seconds):	3
Max time-to-live:	30

- **Log Files**



Log Viewer

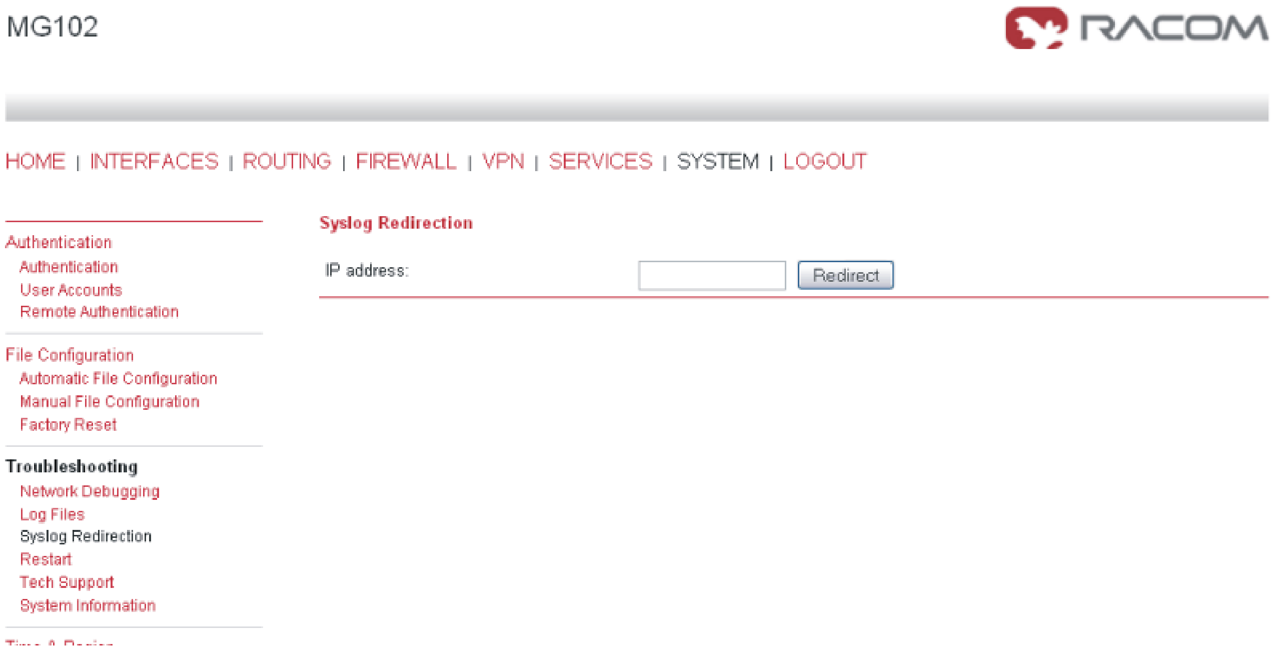
Select log: ● Debug log ○ Boot log

Number of lines to be displayed: ○ all ● last 100 lines << >>

```
check for host1 '10.202.0.1' from ppp0 failed (wwan.0)
Jun 14 08:47:30 netbox user.warn parrot.link_group_manager[1989]: Ping
check for host2 '10.203.0.1' from ppp0 failed (wwan.0)
Jun 14 08:47:30 netbox user.warn parrot.link_group_manager[1989]: 2 of 2
observed hosts seem to be down (wwan.0): failed trials 1, max 5
Jun 14 09:29:29 netbox daemon.info named[1662]: Cleaned cache of 0 RRs
Jun 14 09:29:29 netbox daemon.info named[1662]: USAGE 1308040169
1167609674 CPU=0.05u/0.4s CHILDCPU=0u/0s
Jun 14 09:29:29 netbox daemon.info named[1662]: NSTATS 1308040169
1167609674
Jun 14 09:29:29 netbox daemon.info named[1662]: XSTATS 1308040169
1167609674 RR=0 RNXD=0 RFwdR=0 RDupR=0 RFail=0 RFErr=0 RErr=0 RAXFR=0
RLame=0 ROpts=0 SSysQ=0 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0
RDupQ=0 RTCP=0 SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Jun 14 09:31:02 netbox user.warn parrot.command[10792]: command
application started
Jun 14 09:31:02 netbox user.info parrot.command[10792]: send message "5
/bin/rm -rf /tmp/user-config.* /tmp/zip_archive_dir;rm -f
/tmp/maintenance.done"
Jun 14 09:31:02 netbox user.warn parrot.command[10792]: terminating
```

Log files can be viewed a downloaded here. Please provide these files when placing a support request.

- **System Log Redirection**

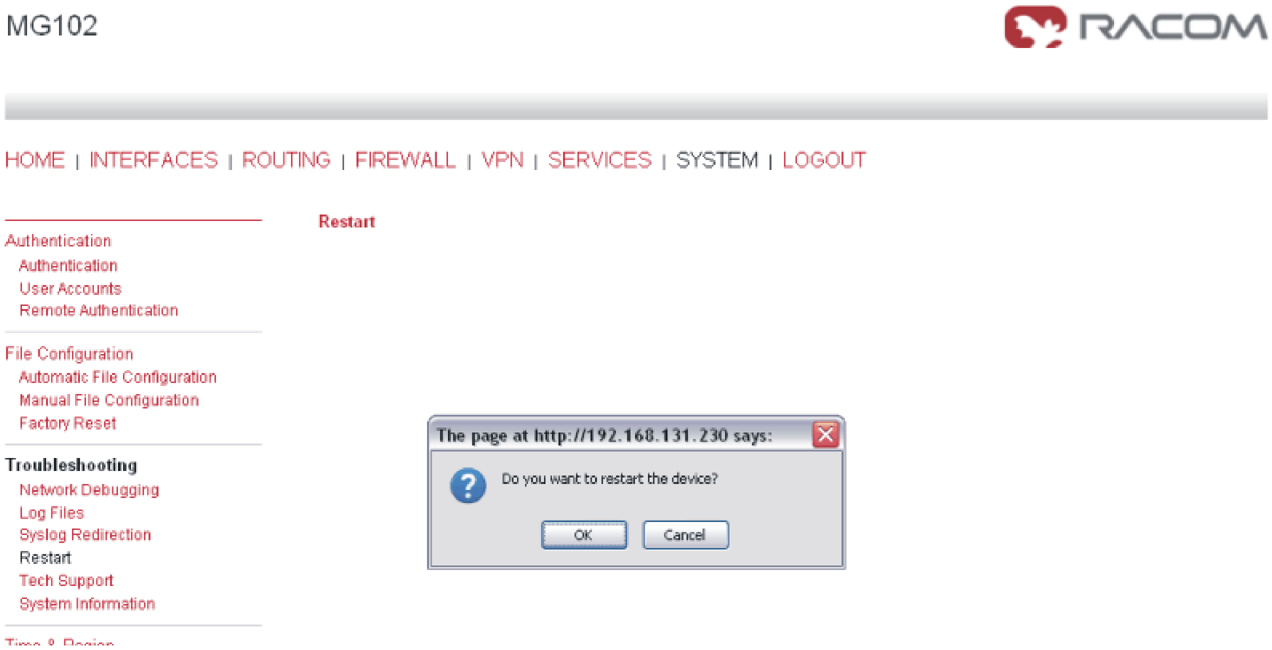


Syslog Redirection

IP address:

Parameter	Description
IP address:	The host where the syslog messages will be forwarded to. A Syslog server has to be running on this IP address. You can use free TFTP server TFTPD32 for example.

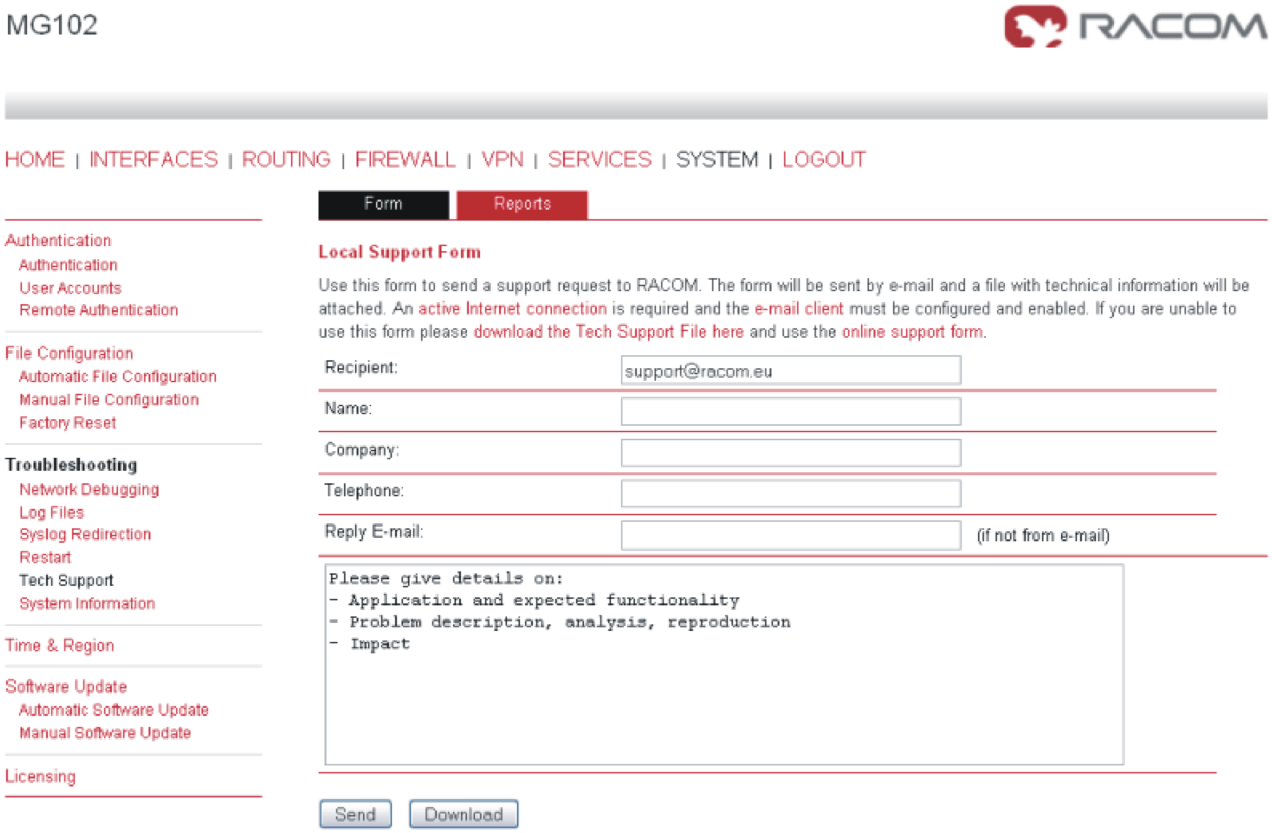
- **Restart**



The page at http://192.168.131.230 says:

Do you want to restart the device?

- **Tech Support**



Local Support Form

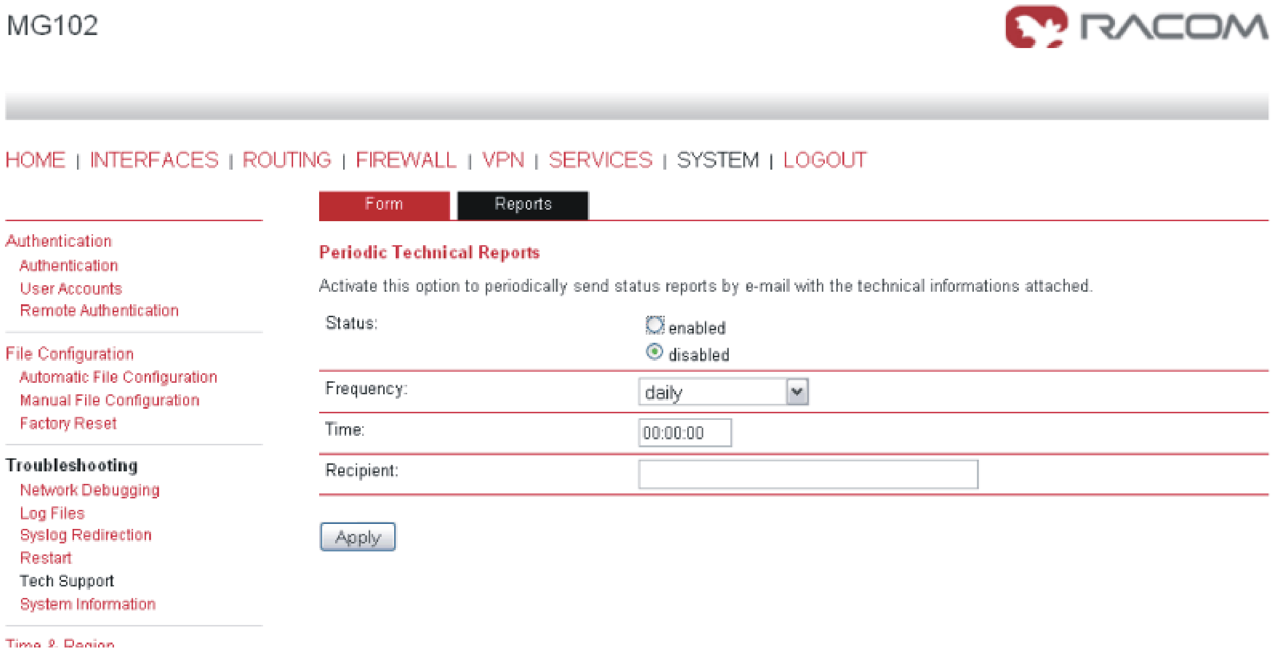
Use this form to send a support request to RACOM. The form will be sent by e-mail and a file with technical information will be attached. An active Internet connection is required and the e-mail client must be configured and enabled. If you are unable to use this form please download the Tech Support File here and use the online support form.

Recipient:	support@racom.eu
Name:	
Company:	
Telephone:	
Reply E-mail:	(if not from e-mail)

```
Please give details on:
- Application and expected functionality
- Problem description, analysis, reproduction
- Impact
```

Note

For using of this feature a connection to Internet is required.

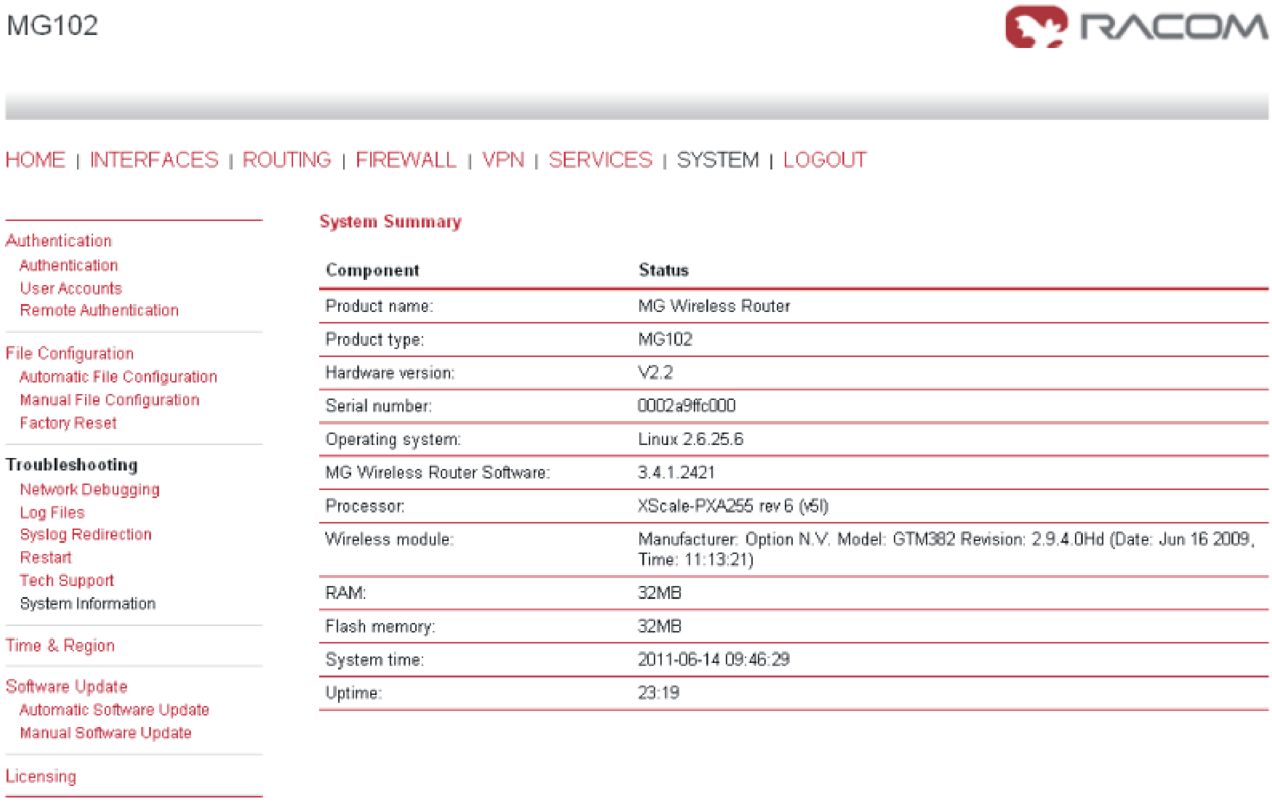


Periodic Technical Reports

Activate this option to periodically send status reports by e-mail with the technical informations attached.

Status:	○ enabled ● disabled
Frequency:	daily
Time:	00:00:00
Recipient:	

- **System Information:**

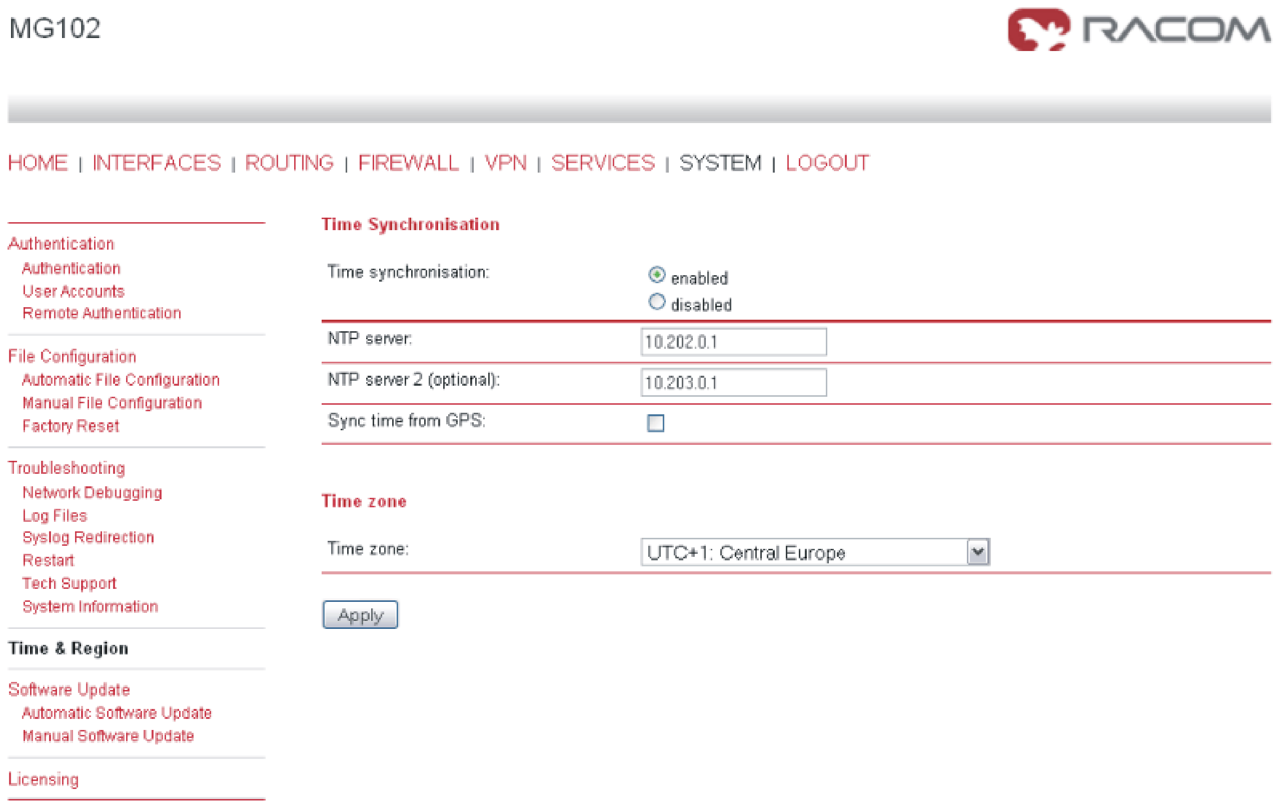


System Summary

Component	Status
Product name:	MG Wireless Router
Product type:	MG102
Hardware version:	V2.2
Serial number:	0002a9ffc000
Operating system:	Linux 2.6.25.6
MG Wireless Router Software:	3.4.1.2421
Processor:	XScale-PXA255 rev 6 (v5l)
Wireless module:	Manufacturer: Option N.V. Model: GTM382 Revision: 2.9.4.0Hd (Date: Jun 16 2009, Time: 11:13:21)
RAM:	32MB
Flash memory:	32MB
System time:	2011-06-14 09:46:29
Uptime:	23:19

Provide this information when placing a support request.

Time and Region



Time Synchronisation

Time synchronisation: ● enabled ○ disabled

NTP server: 10.202.0.1

NTP server 2 (optional): 10.203.0.1

Sync time from GPS: □

Time zone

Time zone: UTC+1: Central Europe

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. M!DGE/MG102 can synchronize its system time with a NTP server.

If enabled, time synchronisation is done after the mobile interface is up but before starting any VPN connections. Later on time synchronisation is performed every 60 minutes.

For Time synchronization from GPS use a non existing address of NTP server e. g. 1.1.1.1.

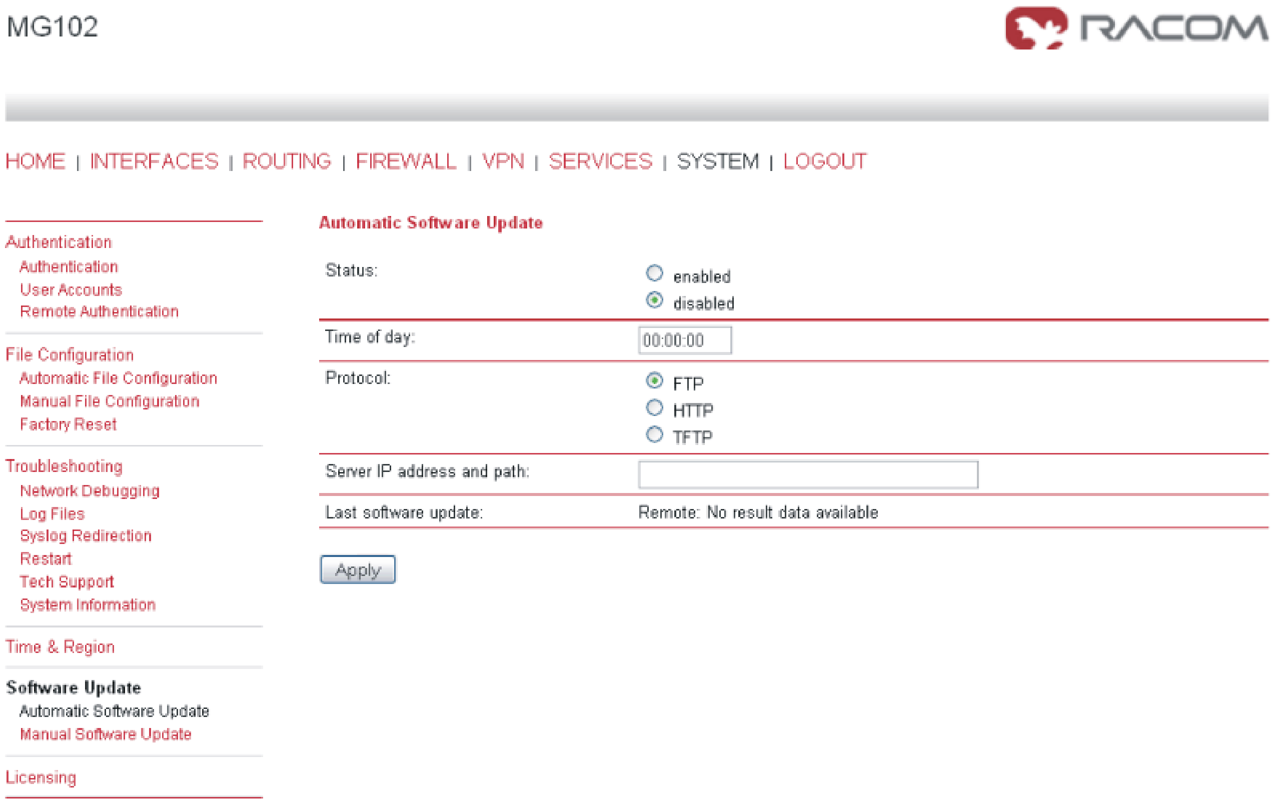
Parameter	Description
NTP state:	Enable/disable time synchronisation
NTP server:	Host name of NTP server
NTP server 2 (optional):	Host name of optional second NTP server
Time zone:	Time zone

Software Update

Software upgrade from the last official software release to the current release published on www.racom.eu is supported. For further details please consult the release note.

Software downgrade is not supported. Software downgrade may lead to loss of configuration and inaccessibility of the device.

- **Automatic Software Update**



Automatic Software Update

Status:	○ enabled ● disabled
Time of day:	00:00:00
Protocol:	● FTP ○ HTTP ○ TFTP
Server IP address and path:	
Last software update:	Remote: No result data available

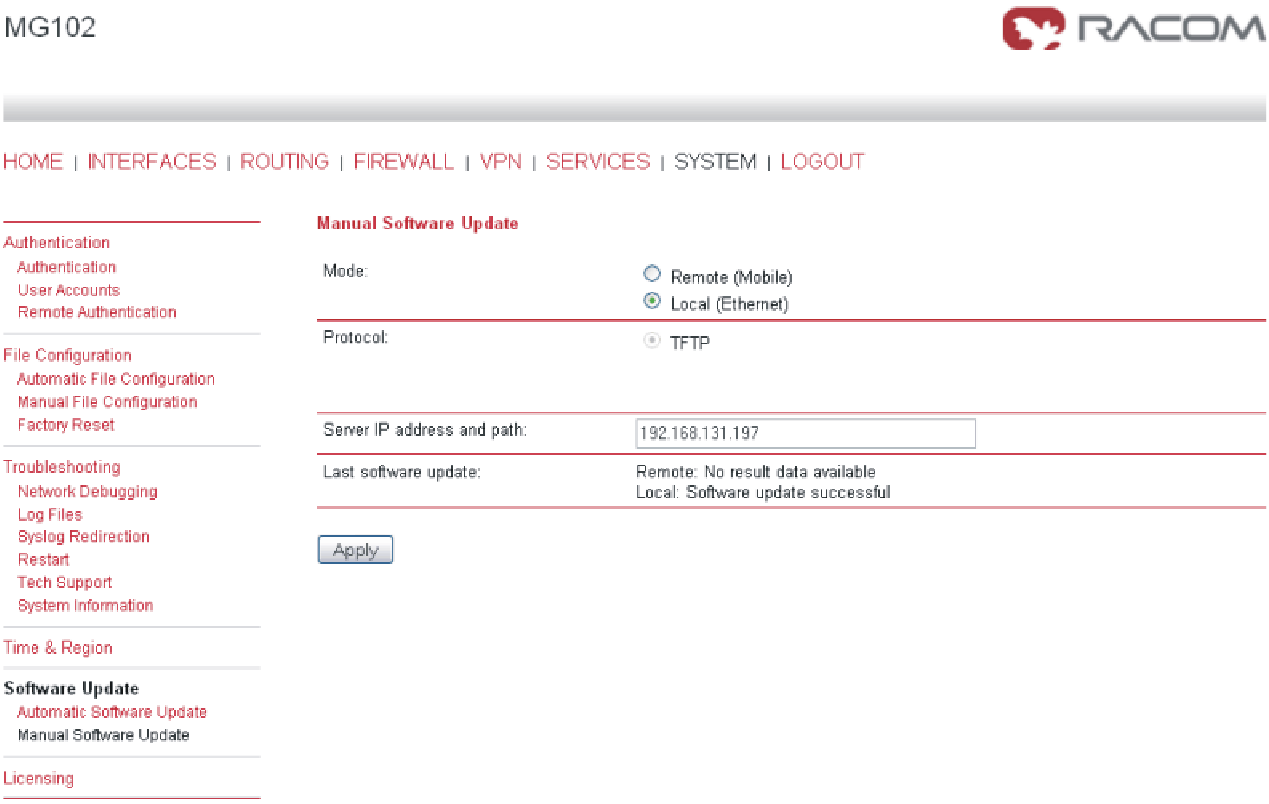
Parameter	Description
Status:	Enable/disable automatic software update
Time of day:	Every day at this time M!DGE/MG102 will do a check for updates
Mode;	Update over mobile or Ethernet Interface?
Protocol:	Specify the protocol used to transfer the new software to M!DGE/MG102. You will need an appropriate server
Server IP address and path:	The directory where the new software can be downloaded
Last software update:	The result of the last try will be displayed here.

- **Manual Software Update**

The easiest way to update the M!DGE/MG102 Software is to connect M!DGE/MG102 to network with a TFTP server. If you only have a Notebook or a PC available the update process involves the preparation of a TFTP Server.

Tip

Be aware of any firewall on your PC that may hinder you doing the update! We recommend disabling the firewall on your PC during the update.



Manual Software Update

Mode: ○ Remote (Mobile) ● Local (Ethernet)

Protocol: ● TFTP

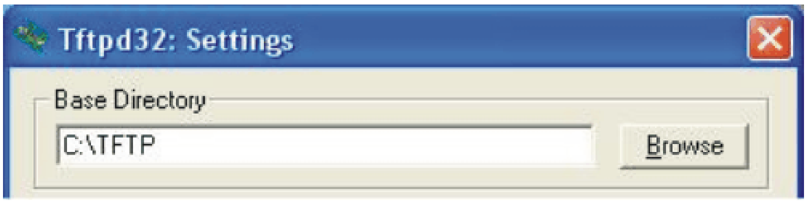
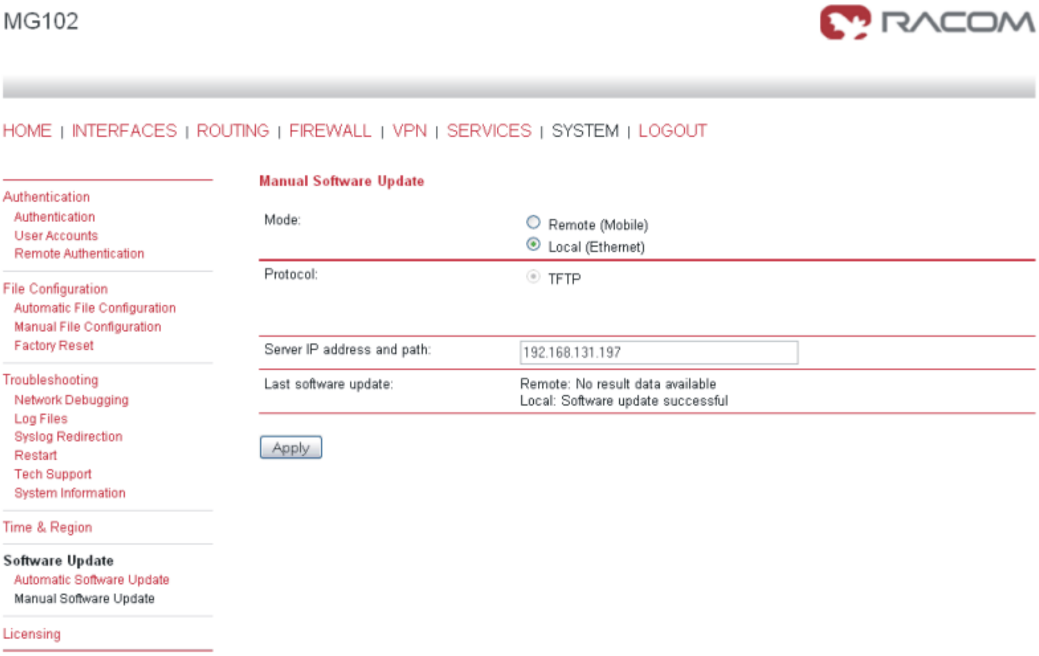
Server IP address and path: 192.168.131.197

Last software update: Remote: No result data available
Local: Software update successful

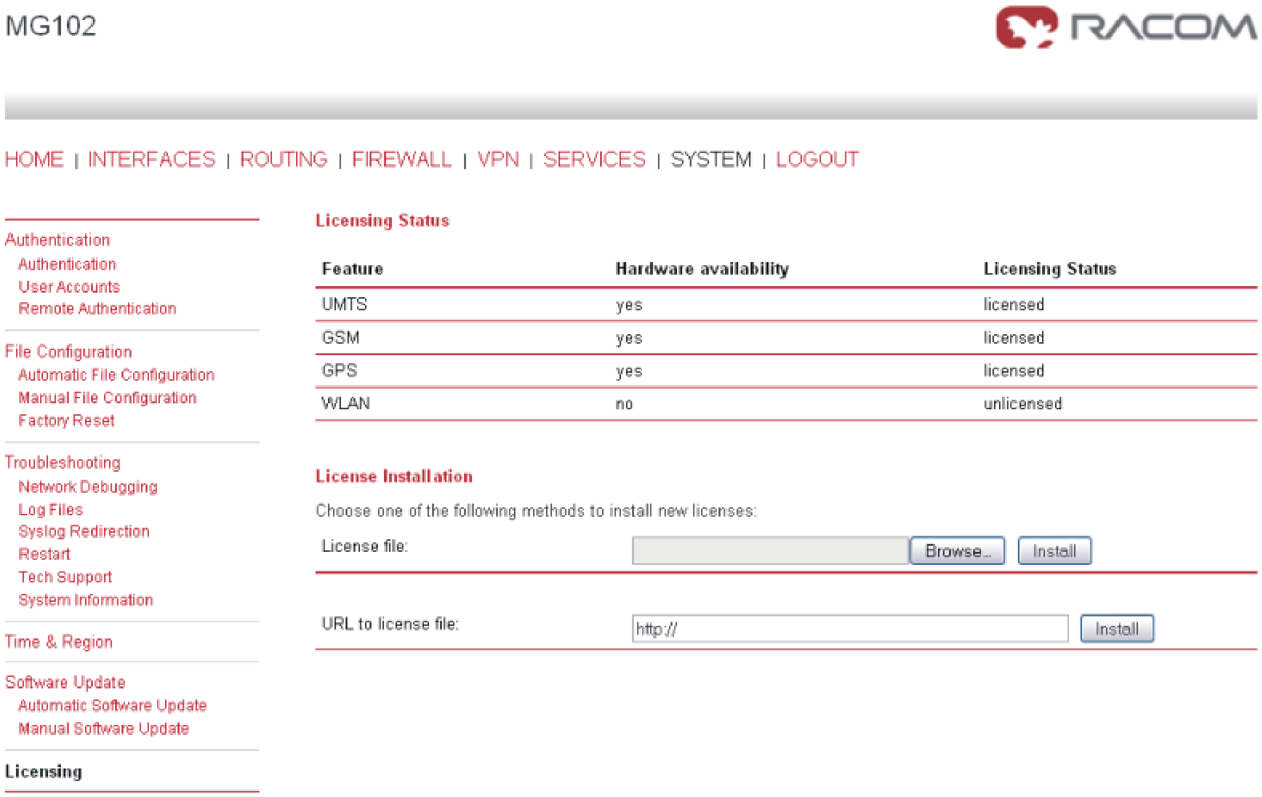
Parameter	Description
Mode:	Update over mobile or Ethernet Interface?
Protocol:	Specify the protocol used to transfer the new software to M!DGE/MG102. You will need an appropriate server.
Server IP address and path:	Provide a host name and a path to a server which hosts the new software. For local updates (TFTP) this value is limited to 26 characters.
Last software update:	The result of the last try will be displayed here.

Step by Step:

Para-meter	Description
1.	Connect your PC with MG102 using a network cable.
2.	If the IP address has been modified set it back to 192.168.1.1 and the subnet mask to `255.255.255.0` (see also chapter 3.1.3.1). Your PC must operate in the same subnet as MG102.
3.	Set the IP address of your PC to `192.168.1.2` and the subnet mask to 255.255.255.0

Para-meter	Description
4.	Download the recommended TFTP server “TFTPD32” from our website, install it on your PC and start it. Configure the TFTP server as follows: -In the dialog „Tftpd32: Settings“ choose the base directory (e.g. „C:\TFTP“). Create a new directory if there is none.  Tftpd32: Settings Base Directory C:\TFTP - Unpack the new software to this directory into a subfolder such as 3.3.1.2135
5.	On the web page “SYSTEM→Manual Software Update” enter the IP address and path of the TFTP server (192.168.1.2) as follows:  MG102 RACOM HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT Authentication Authentication User Accounts Remote Authentication File Configuration Automatic File Configuration Manual File Configuration Factory Reset Troubleshooting Network Debugging Log Files Syslog Redirection Restart Tech Support System Information Time & Region Software Update Automatic Software Update Manual Software Update Licensing Manual Software Update Mode: ○ Remote (Mobile) ● Local (Ethernet) Protocol: ● TFTP Server IP address and path: 192.168.131.197 Last software update: Remote: No result data available Local: Software update successful
6.	Press [Apply] and confirm by pressing [OK]. Wait until the update is complete. See the progress bar Do not unplug the power connector during the update!
7.	Check the results of the update. Refreshing the page or even reopening the browser windows may avoid cache problem. In case of success, “software update successfull” will be displayed, otherwise an error message.

Licensing



Licensing Status

Feature	Hardware availability	Licensing Status
UMTS	yes	licensed
GSM	yes	licensed
GPS	yes	licensed
WLAN	no	unlicensed

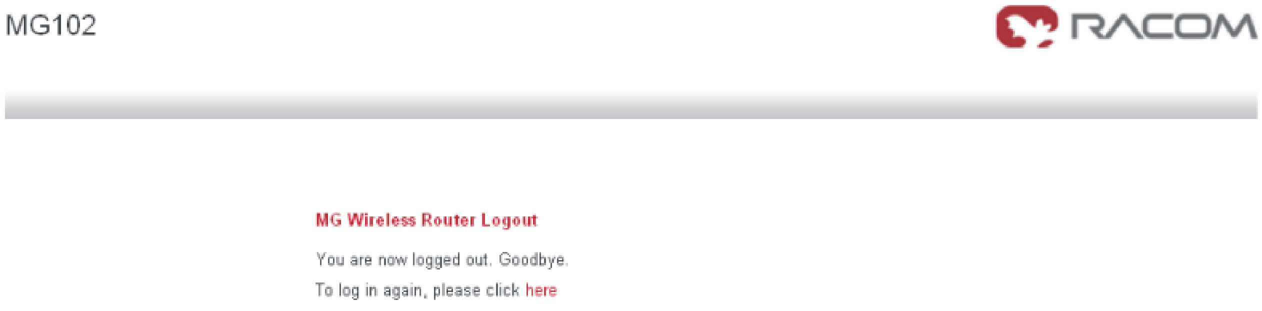
License Installation

Choose one of the following methods to install new licenses:

License file:

URL to license file: http://

3.1.10. Logout



MG Wireless Router Logout

You are now logged out. Goodbye.

To log in again, please click here

Log out from Web Manager

3.2. Configuration Parameters of the M!DGE/MG102

The information in this chapter is needed to configure M!DGE/MG102 via the Command Line Interface or File Configuration. If you are using the Web Manager and its forms to configure M!DGE/MG102, you may skip this chapter.

A configuration parameter consists of two main parts, its name (latter called key) and its value. The user configuration file contains all parameters. Download this file (user-config.cfg) using the Web Manager to get all parameters listed.

Racom has defined some types of parameters that are often used. The table below shows the defined parameter types. In addition other types of parameters may exist.

Parameter Type	Allowed characters	Format	Description
email	a–z A–Z 0–9 _-. @ (mandatory)	user@hostname	String must include “@” Second part must be a valid hostname
hostname	a–z A–Z 0–9 _-.		Fully-Qualified Host Name (FQHN) or host name
ipaddress	Numbers and dots	xxx.xxx.xxx.xxx	Decimal dotted notation
netmask	Numbers and dots	xxx.xxx.xxx.xxx	Decimal dotted notation
username	a–z A–Z 0–9 _-. @		
password	All but &, \", \'		
phone number	+ 0–9 * #		
time	0–9, and :	hh:mm:ss	Time, e.g. for automatic software or configuration update

3.2.1. Interfaces related Parameters

Ethernet

Parameter	Default Value	Range	Description
network.PrivateInterface.IpAddress	192.168.1.1	ipaddress	IP address Ethernet
network.PrivateInterface.NetMask	255.255.255.0	netmask	Netmask Ethernet

Mobile Interface and SIM Cards

Parameter	Default Value	Range	Description
simcard.check.pincode	void	4 digit numeric value	PIN code, e.g. 1234
simcard.pinStatus	0	[0,1]	0 = PIN protection disabled 1 = PIN protection enabled
simcard.sim2.check.pincode	void	4 digit numeric value	PIN code, e.g. 1234

Parameter	Default Value	Range	Description
simcard.sim2.pinStatus	0	[0,1]	0 = PIN protection disabled 1 = PIN protection enabled
networkselection.mode	automatic	[automatic,manual]	
networkselection.network_lai	void	numeric value (LAI)	Select the network provider defined by the supplied Local Area Identity (LAI)
dialout.connectionMethod	0	[0..2]	0 = manual only 1 = dial on demand 2 = permanent
dialout.connSetup.redialAttempt	2	[1..4294967296]	Redial attempts
dialout.connSetup.idleTimeout	1	[1..35791394]	Idle timeout in minutes (in case of dial on demand)
dialout.profiles.0.name	void	username	Profile name
dialout.profiles.0.username	void	username	Username
dialout.profiles.0.password	void	password	Password
dialout.profiles.0.phoneNumber	void	phone number	Phone number

dialout.profiles.0.authMethod	void	[chap, pap]	Chap = CHAP
			Pap = PAP

dialout.profiles.0.apn	void	hostname	Acess Point Name
dialout.profiles.0.IPHC	void	[0,1]	0 = off 1 = enable IP header compression
dialout.profiles.0.IPSC	void	[0,1]	0 = off 1 = enable software compression
dialout.profiles.0.queryDNS=1	void	[0,1]	0 = do not query DNS server 1 = query DNS server
dialout.profiles.0.ESCIP	void	[0,1]	0 = off 1 = enable specific client IP address
dialout.profiles.0.SCAddress	void	ipaddress	Specific client address
dialout.profiles.0.SIM	SIM1	[SIM1,SIM2]	SIM used for primary profile
dialout.profiles.0.ISDN	void	[0,1]	0 = normal call 1 = is ISDN call
dialout.profiles.0.switchCondition	never	[never, redialAttemptsReached]	Condition for profile switch
dialout.profiles.1.name	void	username	Profile name
dialout.profiles.1.username	void	username	Username
dialout.profiles.1.password	void	password	Password
dialout.profiles.1.phoneNumber	void	phone number	Phone number

dialout.profiles.1.authMethod	void	[chap, pap]	Chap = CHAP
			Pap = PAP

Parameter	Default Value	Range	Description
dialout.profiles.1.apn	void	hostname	Acess Point Name
dialout.profiles.1.IPHC	void	[0,1]	0 = off 1 = enable IP header compression
dialout.profiles.1.IPSC	void	[0,1]	0 = off 1 = enable software compression
dialout.profiles.1.queryDNS=1	void	[0,1]	0 = do not query DNS server 1 = query DNS server
dialout.profiles.1.ESCIP	void	[0,1]	0 = off 1 = enable specific client IP address
dialout.profiles.1.SCAddress	void	ipaddress	Specific client address
dialout.profiles.1.SIM	SIM2	[SIM1,SIM2]	SIM used for fallback profile
dialout.profiles.1.ISDN	void	[0,1]	0 = normal call 1 = is ISDN call
dialout.profiles.1.switchCondition	never	[never, elpas8h, elaps16h, elaps24h, redialAttemptsReached]	Condition for profile switch
network.MSS.status	0	[0,1]	0 = disabled 1= enabled
network.MSS.adjustment	1400	[100,1500]	Maximum Segment Size

Digital I/O

Parameter	Default Value	Range	Description
digitalIO.receiving.tcpPort	2158	[1 .. 65535]	TCP Port for monitoring
digitalIO.controlOutPut.output1	off	[on,off]	State of output 1
digitalIO.controlOutPut.output2	off	[on,off]	State of output 2
digitalIO.keepOnReboot	1	[0,1]	0 = set values after reboot to digitalIO.afterReboot.output1 digitalIO.afterReboot.output2 1 = restore values after reboot
digitalIO.afterReboot.output1	off	[on,off]	State of output 1 after reboot
digitalIO.afterReboot.output2	off	[on,off]	State of output 2 after reboot

3.2.2. Routing related Parameters

Parameter		Default Value	Range	Description
static_routes.<I>.interface	with I = [0..20]	void	hostname	
static_routes.<I>.target		void	hostname	
static_routes.<I>.mask		void	netmask	
static_routes.<I>.gateway		void	hostname	
static_routes.<I>.metric		void	[0..32766]	Default is 0.

3.2.3. Firewall related Parameters

NAPT on mobile Interface

Parameter		Default Value	Range	Description
napt_mobile.status	with j = [0..49]	1	[0,1]	0 = NAPT off 1 = NAPT on
napt_mobile..<j>.extPort.start		void	[1 .. 65535]	External port range start
napt_mobile..<j>.extPort.end		void	[1 .. 65535]	External por range end
napt_mobile..<j>.intHost		void	ipaddress	
napt_mobile.<j>.intPort		void	[1 .. 65535]	Internal port
napt_mobile.<j>.protocol		TCP	[TCP, UDP]	TCP or UDP
napt_mobile.<j>.status		1	[0,1]	0 = disabled 1= enabled
napt_mobile.<j>.isRedirect		0	[0,1]	0 = redirect to other host 1 = redirect to localhost

NAPT on OpenVPN Interface

Parameter		Default Value	Range	Description
napt_openvpn.status	with j = [0..49]	1	[0,1]	0 = NAPT off 1 = NAPT on
napt_openvpn.<j>.extPort		void	[1 .. 65535]	External port range start
napt_openvpn.<j>.intPort		void	[1 .. 65535]	External por range end
napt_openvpn.<j>.intHost		void	ipaddress	
napt_openvpn.<j>.intPort		void	[1 .. 65535]	Internal port
napt_openvpn.<j>.protocol		TCP	[TCP, UDP]	TCP or UDP
napt_openvpn.<j>.status		1	[0,1]	0 = disabled 1= enabled
napt_openvpn.<j>.isRedirect		0	[0,1]	0 = redirect to other host 1 = redirect to localhost

Access Control List Local Host

Parameter		Default Value	Range	Description
firewall_local_host.policy		2	[0,1,2]	0 = deny all 1 = permit entries 0 = permit all
firewall_local_host.<j>. target	with j = [0..19]	void	hostname	Source host / net
firewall_local_host.<j>.mask		void	netmask	

Access Control List for Exposed Host on Mobile Interface

Parameter		Default Value	Range	Description
firewall_exposed_host_mobile.policy		1	[0,1,2]	0 = deny all 1 = permit entries 0 = permit all
firewall_exposed_host_mobile.host		void	hostname	The exposed host
firewall_exposed_host_mobile.<j>.target	with j = [0..19]	void	hostname	Source host / net
firewall_exposed_host_mobile.<j>.mask		void	netmask	

Access Control List for Exposed Host on OpenVPN Interface

Parameter		Default Value	Range	Description
firewall_exposed_host_openvpn.policy		1	[0,1,2]	0 = deny all 1 = permit entries 0 = permit all
firewall_exposed_host_openvpn.host		void	hostname	The exposed host
firewall_exposed_host_openvpn.<j>.target	with j = [0..19]	void	hostname	Source host / net
firewall_exposed_host_openvpn.<j>.mask		void	netmask	

3.2.4. VPN related Parameters

OpenVPN

Parameter	Default Value	Range	Description
vpn.status	0	[0,1]	0 = disabled 1= enabled
vpn.mode	0	[0,1]	0 = Standard mode 1= Expert mode
vpn.auth	0	[0,1]	0 = crertificate-based authentication 1= credential-based authentication
vpn.configuration.serverAddress	void	hostname	OpenVPN server FQHN
vpn.configuration.serverPort	void	[1 .. 65535]	OpenVPN server port
vpn.configuration.serverAddress2	void	hostname	2nd OpenVPN server FQHN
vpn.configuration.serverPort2	1194	[1 .. 65535]	2nd OpenVPN server port

vpn.configuration.devType	tun	[tun, tap]	tun = tun device
			tap = tap device

vpn.configuration.compressionStatus	1	[0,1]	0 = disabled 1= enabled
vpn.configuration.username	void	username	For credential-based authentication
vpn.configuration.password	void	password	For credential-based authentication

IPsec Parameters

Parameter	Default Value	Range	Description
ipsec.status	0	[0,1]	0 = disabled 1= enabled
ipsec.remote.serverIp	void	ipaddress	
ipsec.remote.lanAddress	void	Ipaddress	0 = crertificate-based authentication 1= credential-based authentication

Parameter	Default Value	Range	Description
ipsec.remote.lanMask	255.255.0.0	netmask	OpenVPN server FQHN
ipsec.ike.psk	void	password	OpenVPN server port
ipsec.ike.mode	identity-protection	[identity-protection, aggressive]	
ipsec.ike.encryption	3des	3des	
ec.ike.hash	md5	[sha1, md5]	
ipsec.ike.dh	modp1024	[modp1024, modp1536]	
ipsec.ike.localId	void	username	
ipsec.ike.remoteId	void	username	
ipsec.esp.encryption	3des	3des	
ipsec.esp.hash	md5	[sha1, md5]	
ipsec.pfs	0	[0,1]	For credential-based authentication
ipsec.dpd.state	1	[0,1]	For credential-based authentication
ipsec.dpd.cycle	30	[5.. 120]	For credential-based authentication
ipsec.dpd.failureCount	3	[1.. 10]	

PPTP Server

Parameter	Default Value	Range	Description
network.PPTP.status	1	[0,1]	0 = disabled 1= enabled
network.PPTP.AddressRangeStart	192.168.1.200	ipaddress	Address range start
network.PPTP.AddressRangeSize	5	[2,254]	Address range size

Dial-in Server

Parameter	Default Value	Range	Description
dialin.status	0	[0,1]	0 = Dial-in disabled 1= Dial-in enabled
dialin.configuration.addressRangeStart	192.168.254.1	ipaddress	Address range start
dialin.configuration.addressRangeSize	254	[2..254]	Address range size
dialin.disableNapt	0	[0,1]	0 = off 1= Disable NAPT on Dial-on

3.2.5. Services related Parameters

COM Server

Parameter	Default Value	Range	Description
serial_srv.status	void	[0,1]	0 = disabled 1= enabled
serial_srv.opt.protocol	telnet	[raw, telnet, modbus]	
serial_srv.opt.port	2000	[1 .. 65535]	
serial_srv.opt.baud_rate	115200	[300, 1200, 2400, 4800, 9600, 19200, 38400, 115200]	
serial_srv.opt.parity=	void	NONE, ODD, EVEN]	
serial_srv.opt.stopbits=	void	1DATABITS, 2DATABITS]	
serial_srv.opt.databits	8DATABITS	[8DATABITS, 7DATABITS]	
serial_srv.opt.xonxoff	void	[0,1]	0 = disabled 1= enabled
serial_srv.opt.rtscts	void	[0,1]	0 = disabled 1= enabled
serial_srv.opt.phys_proto	RS232	[RS232, RS485]	

DNS Proxy Server

Parameter	Default Value	Range	Description
network.DNS.status	1	[0,1]	0 = DNS Proxy off 1= DNS Proxy on

DHCP Server

Parameter	Default Value	Range	Description
network.DHCP.status	1	[0,1]	0 = DHCP server off 1= DHCP server on
network.DHCPSettings.AddressRangeStart	192.168.1.100	ipaddress	DHCP range start
network.DHCPSettings.AddressRangeSize	100	[1..255]	DHCP range size
network.DHCPSettings.DNSServer	Proxy	hostname	DNS Server 1
network.DHCPSettings.DNSServer0	void	hostname	DNS Server 2
network.DHCPSettings.DNSServer1	void	hostname	DNS Server 3

Dynamic DNS

Parameter	Default Value	Range	Description

dyndns.serviceType	dyndns	[dyndns, dyndns-static, dyndns-custom]	dyndns = Dynamic DNS
			dyndns-static = Static DNS
			dyndns-custom = Custom DNS

dyndns.hostname	void	hostname	
dyndns.username	void	username	
dyndns.password	void	password	
dyndns.supportEmail	void	e-mail	
dyndns.serverAddress	void	hostname	
dyndns.port	void	[1 .. 65535]	Dynamic DNS Listening Port
dyndns.status	0	[0,1]	0 = disabled 1= enabled

SMS Parameters

Parameter	Default Value	Range	Description
sms.receiving.status	1	[0,1]	0 = disabled 1= enabled
sms.sending.status	0	[0,1]	0 = disabled 1= enabled
sms.sending.gateway	void	phone number	SMSC number
sms.sending.sim2.gateway	void	phone number	SMSC number

E-Mail Parameters

Parameter	Default Value	Range	Description
email.sending.status	0	[0,1]	0 = disabled 1= enabled
email.sending.smtp.host	void	hostname	
email.sending.smtp.port	void	[1 .. 65535]	
email.sending.smtp.from	void	email	From E-mail Address
email.sending.smtp.authentication	void	[0,1]	0 = disabled 1= enabled
email.sending.smtp.username	void	username	
email.sending.smtp.password	void	password	

GPS Parameters

Parameter	Default Value	Range	Description
gps.status	0	[0,1]	0 = Dial-in disabled 1= Dial-in enabled
gps.destination.hostname	void	hostname	
gps.destination.port	void	[1 .. 65535]	
gps.updateCycle	3	[3..∞]	

Event Manager

- **Events**

Parameter	Default Value	Range	Description
events.pppUp.message	void	password	Event Message
events.pppDown.message	void	password	Event Message
events.pppFailure.message	void	password	Event Message
events.vpnUp.message	void	password	Event Message
events.vpnDown.message	void	password	Event Message
events.vpnFailure.message	void	password	Event Message
events.dialInUp.message	void	password	Event Message
events.dialInDown.message	void	password	Event Message
events.dialInFailure.message	void	password	Event Message
events.dyndnsReg.message=	void	password	Event Message
events.dyndnsFailure.message=	void	password	Event Message
events.logInGUI.message=	void	password	Event Message
events.logFailedGUI.message=	void	password	Event Message
events.restartCrash.message=	void	password	Event Message
events.restartWebManagement.message	void	password	Event Message
events.powerUp.message	void	password	Event Message
events.startUpComplete.message	void	password	Event Message
events.digitalInput1_On.message	void	password	Event Message
events.digitalInput2_On.message	void	password	Event Message
events.digitalInput1_Off.message	void	password	Event Message
events.digitalInput2_Off.message	void	password	Event Message
events.digitalOutput1_On.message	void	password	Event Message
events.digitalOutput2_On.message	void	password	Event Message
events.digitalOutput1_Off.message	void	password	Event Message
events.digitalOutput2_Off.message	void	password	Event Message
events.udpMessage.message	void	password	Event Message
events.gpsUp.message	void	password	Event Message
events.gpsDown.message	void	password	Event Message

Parameter	Default Value	Range	Description
events.testEvent.message	void	password	Event Message

- **Subscribers**

Parameter		Default Value	Range	Description
subscriber.<k>.name	with k = [0..19]	void	hostname	Name of subscriber
subscriber.<k>.sms.destination		void	phone number	Phone number for SMS
subscriber.<k>.email.destination		void	email	E-mail address
subscr_grp.<l>.name	with l = [0..9]	void	hostname	Name of group
subscr_grp.<l>.members.users		void	0:1:2:…19	Indices of users in this group
subscr_grp.<l>.members.groups		void	0:1:2:…9	Indices of groups in this group

- **Event Processor**

Parameter		Default Value	Range	Description
evtProc.sequence		void	0:1:2:…9	
evtProc.<l>. eventName	with l = [0..9]	void	hostname	

evtProc.<l>.action		void	[send, switchOn, switchOff]	Send = send message
				Switch = switch digital I/O

evtProc.<l>.target		void	u:0…9 g:0…9 o:0…2	Index of subscriber or group or input or output

SNMP Agent

Parameter	Default Value	Range	Description
snmp.status	0	[0,1]	0 = Dial-in disabled 1= Dial-in enabled
snmp.port	161	[1 .. 65535]	
snmp.community	public		
snmp.contact	void		
snmp.location	void		
snmp.traphost	void	hostname	
snmp.trapport	162	[1 .. 65535]	
snmp.siglow	-113	[-113 to -51]	Signal strength trap threshold dBm
snmp.sighigh	-51	[-113 to -51]	Signal strength trap reactivation threshold dBm:

SSH Server

Parameter	Default Value	Range	Description
sshServer.port	22	[1 .. 65535]	

Telnet Server

Parameter	Default Value	Range	Description
telnetServer.port	23	[1 .. 65535]	

Web Server

Parameter	Default Value	Range	Description
webServer.http.port	80	[1 .. 65535]	
webServer.https.port	80	[1 .. 65535]	

UDP Message Receiver

Parameter	Default Value	Range	Description
udpMessage.receiving.udpPort	2157	[1 .. 65535]	

3.2.6. System related Parameters

User Accounts

Parameter		Default Value	Range	Description
user.admin.password		void	password	"not set" = reset admin password
administrator.deviceAccess		1	[0,1]	0 = disabled 1= enabled
user.<k>.name	with k = [0..20]	void	hostname	
user.<k>.password		void	password	

Troubleshooting

Parameter	Default Value	Range	Description
redirectSyslogIp	void	ipaddress	
webMgrDbg.status	1	[0,1]	0 = disabled 1= enabled

Time Synchronisation

Parameter	Default Value	Range	Description
network.NTP.status	1	[0,1]	0 = disabled 1= enabled
network.NTP.server	swisstime.ethz.ch ???	hostname	NTP server
network.NTP.server2	void	hostname	Backup NTP server
network.timezone	UTC+2	[UTC-12 … UTC+12]	Time zone

Software Update

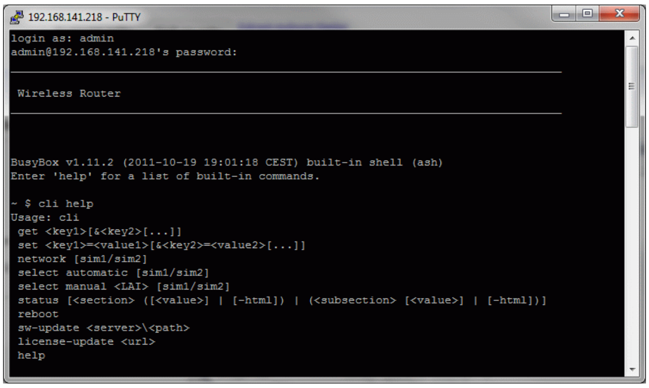
Parameter	Default Value	Range	Description
swu_man.url		ipaddress	
swu_auto.status	1	[0,1]	0 = disabled 1= enabled
swu_auto.time		time	hh:mm:ss
swu_auto.url		hostname	

Configuration Update

Parameter	Default Value	Range	Description
cfg_auto.status	1	[0,1]	0 = disabled 1= enabled
cfg_auto.time	void	time	hh:mm:ss
cfg_auto.url	void	hostname	

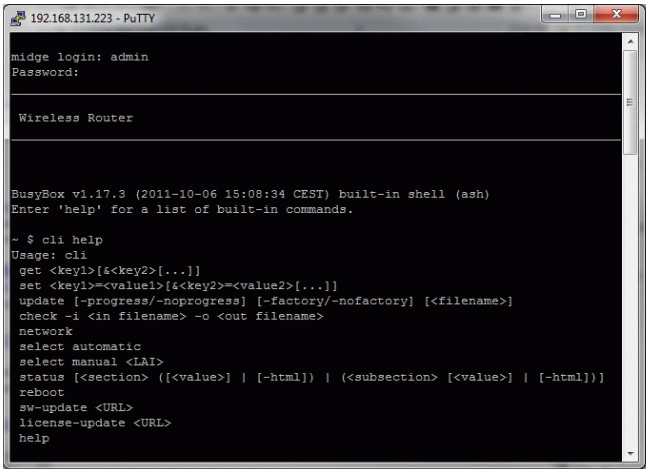
3.3. Configuration via Command Line Interface (CLI)

The command line interface is accessible after successful login to M!DGE/MG102 via telnet or Secure Shell (SSH). By default the telnet server answers on port 23, the SSH server on port 22.



192.168.141.218 - PuTTY

```
login as: admin
admin@192.168.141.218's password:
──────────────────────────────────────────────────────────────────

 Wireless Router

──────────────────────────────────────────────────────────────────



BusyBox v1.11.2 (2011-10-19 19:01:18 CEST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

~ $ cli help
Usage: cli
 get <key1>[&<key2>[...]]
 set <key1>=<value1>[&<key2>=<value2>[...]]
 network [sim1/sim2]
 select automatic [sim1/sim2]
 select manual <LAI> [sim1/sim2]
 status [<section> ([<value>] | [-html]) | (<subsection> [<value>] | [-html])]
 reboot
 sw-update <server>\<path>
 license-update <url>
 help
```



192.168.131.223 - PuTTY

```
midge login: admin
Password:
──────────────────────────────────────────────────────────────────────────

 Wireless Router

──────────────────────────────────────────────────────────────────────────



BusyBox v1.17.3 (2011-10-06 15:08:34 CEST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

~ $ cli help
Usage: cli
 get <key1>[&<key2>[...]]
 set <key1>=<value1>[&<key2>=<value2>[...]]
 update [-progress/-noprogress] [-factory/-nofactory] [<filename>]
 check -i <in filename> -o <out filename>
 network
 select automatic
 select manual <LAI>
 status [<section> ([<value>] | [-html]) | (<subsection> [<value>] | [-html])]
 reboot
 sw-update <URL>
 license-update <URL>
 help
```

Logon via SSH with PuTTY

Logon via Telnet via Windows Telnet Client

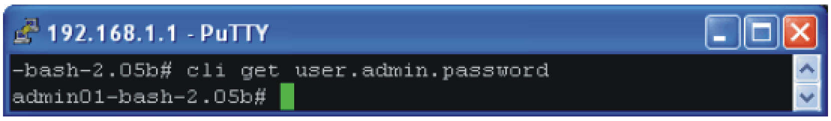
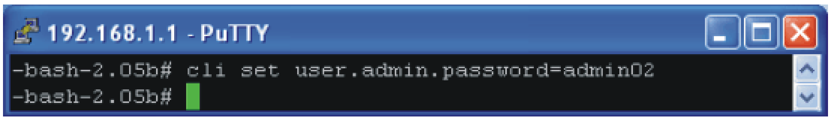
After authentication, type “cli help” into the Shell to learn about the usage of the command line interface. CLI will stop after every call. You have to include ‘cli’ for every new call.

3.3.1. CLI Overview

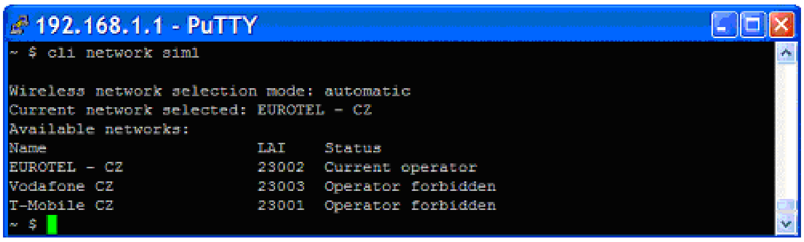
The Command Line Interface mainly provides functions to read and write values of the M!DGE/MG102 configuration parameters. In addition, the CLI provides functions to query status information.

Command	Return	Description
cli get	string	Read values of one or more specified configuration parameters.
cli set	void	Write values of one or more specified configuration parameters.
cli network	string	Show available networks including Location Area Identities (LAIs)
cli select	void	Select the network provider defined by the supplied Local Area Identity (LAI) or set the network selection method to automatic
cli status	string	Show a status overview of M!DGE/MG102
cli help	string	Print the cli help message (usage)
Ctrl+C	void	Abort a command. Exit from CLI

3.3.2. CLI Usage

Command	Usage and Return Value
cli get	‘cli get’ is used to read values from configuration parameters. Arguments include all configuration keys as described in chapter 3.2 Usage: cli get <key1>[&<key2>[...]] Example: cli get user.admin.password The return value is the value of the queried parameter.  -bash-2.05b# cli get user.admin.password admin01-bash-2.05b# **Note** cli get <invalidKey> returns no error message
cli set	‘cli set’ is used to assign values to configuration parameters. Arguments include all configuration keys as described in chapter 3.2 Usage: set <key1>=<value1>[&<key2>=<value2>[...]] Example: cli set user.admin.password=admin02  -bash-2.05b# cli set user.admin.password=admin02 -bash-2.05b# ‘cli set’ produces no return value and no error message. To check if the modification took place, use ‘cli get’

Command	Usage and Return Value
	Note cli set <invalidKey>=<correctValue> returns no error message cli set <validKey>=< inCorrectValue> returns no error message, no range check is performed
cli configure	Not for end user use! Root rights are required.
cli configureAll	Not for end user use! Root rights are required.

cli network	‘cli network’ provides mobile network information on the optionally specified SIM card. If no SIM card is specified, the command is applied to SIM1. The information returned includes the Local Area Identity (LAI)
	Usage: network [sim1/sim2]
	Example: cli network sim1
	
	192.168.1.1 - PuTTY
	`~ $ cli network sim1`
	`Wireless network selection mode: automatic`
	`Current network selected: EUROTEL - CZ`
	`Available networks:`
	`Name                      LAI    Status`
	`EUROTEL - CZ              23002  Current operator`
	`Vodafone CZ               23003  Operator forbidden`
	`T-Mobile CZ               23001  Operator forbidden`
	`~ $`
	‘cli set’ produces no return value and no error message. To check if the modification took place, use ‘cli get’
	Note
	The following commands are identical:
	‘cli network’ and ‘cli network sim1’

cli select automatic	‘cli select automatic’ sets the network selection mode for the specified SIM card to automatic. Usage: select automatic [sim1/sim2] **Note** The following commands are identical: ‘cli select automatic’ and ‘cli select automatic sim1’ The following commands have the same effect: ‘cli select automatic sim1’ and ‘cli set networkselection.mode=automatic’ ‘cli select automatic sim2’ and ‘cli set networkselection.sim2.mode=automatic’

Command	Usage and Return Value
cli select manual	‘cli select manual’ selects the network provider defined by the supplied Local Area Identity (LAI) for the specified SIM card Usage: select manual <LAI> [sim1/sim2] **Note** The following commands are identical: ‘cli select manual <lai>’ and ‘cli select manual sim1 <lai>’ The following commands have the same effect: ‘cli select manual <lai> sim1’ and ‘cli set networkselection.network_lai=<lai> ‘cli select manual <lai> sim2’ and ‘cli set networkselection.sim2.network_lai=<lai>
cli status	‘cli status’ returns both, ‘cli status overview’ and ‘cli status system’ concatenated. The option -html is used to query a HTML version of the status information.
cli status overview	show the status of all interfaces, networks and services.
cli status overview interfaces	show the status of all interfaces
cli status overview interfaces sim_state	show the state of the SIM-Card
cli status overview interfaces pin_state	show the state of the PIN
cli status overview interfaces signal_strength	show the actual signal strength
cli status overview interfaces con_state	show the state of the wireless connection
cli status overview interfaces con_type	show the type of the wireless connection
cli status overview interfaces net_sel_mode	show the mode of the network selection
cli status overview interfaces net_sel_prov	show the current network provider
cli status overview interfaces data_rxtx	show the amount of received and transmitted data
cli status overview interfaces stream_updown	show the actual down- and upstream rates
cli status overview interfaces last_reset	show the last reset date of data counter
cli status overview networks	show the status of all networks
cli status overview networks napt_state_mob	show the state of the NAPT service on the mobile if

Command	Usage and Return Value
cli status overview networks napt_state_ovpn	show the state of the NAPT service on the vpn if
cli status overview networks openvpn_state	show the state of the OpenVPN connection
cli status overview networks ipsec_state	show the state of the IPsec connection
cli status overview networks pptp_state	show the state of the PPTP server
cli status overview services	show the status of all services
cli status overview services dyndns_state	show the state of the Dynamic DNS client
cli status overview services dialin_state	show the state of the Dial-in service
cli status overview services dhcp_state	show the state of the DHCP server
cli status overview services dns_state	show the state of the DNS Proxy server
cli status overview services gps_state	show the state of the GPS signal
cli status overview services keepalive_state	show the state of the Keep-alive service
cli status overview services sms_rec_state	show the state of the SMS receiving service
cli status overview services sms_send_state	show the state of the SMS sending service
cli status overview services email_state	show the state of the E-Mail service
cli status overview services dig_in	show the state of the digital inputs
cli status overview services dig_out	show the state of the digital outputs
cli status system	show M!DGE/MG102 systems information including hardware and software versions
cli status system prod_name	show the M!DGE/MG102 product name
cli status system prod_type	show the M!DGE/MG102 product type
cli status system hw_ver	show the M!DGE/MG102 hardware version
cli status system serial	show the M!DGE/MG102 serial number
cli status system os	show the M!DGE/MG102 operating system
cli status system nbsw	show the M!DGE/MG102 software version
cli status system cpu	show the M!DGE/MG102 CPU
cli status system wireless_module	show the M!DGE/MG102 wireless module
cli status system ram	show the amount of RAM installed in the M!DGE/MG102
cli status system flash	show the amount of flash installed in the M!DGE/MG102
Help	Print the cli help message (usage)

Command	Usage and Return Value
Exit	Not for end user use! Root rights are required.

4. Software Interfaces

4.1. GPS Server

4.1.1. Berlios GPS Server

This is a TCP server which provides GPS data in various formats. Find more information under http://gpsd.berlios.de

4.1.2. MG102 GPS Server

If valid GPS data is available it will be sent as UDP Payload to the configured host. The content is separated into two lines. The first line contains data in the GPGGA format; the second line contains GPRMC data.

$GPGGA – Global Positioning System Fix Data

Format: $GPGGA,<time>,<latitude>,<longitude>,<quality>,<satellites>,0,<sealevel>,,*<CS><CR><LF>

Sample Data: $GPGGA,154250,4749.8678,N,00871.8469,E,1,06,0.0,498,M,0.0,M,,*6A <CR><LF>

No.	Name	Data	Description
1	Sentence Identifier	$GPGGA	Global Positioning System Fix Data
2	Time	<time>	UTC of position fix
3	Latitude	<latitude,N/S>	Latitude of fix
4	Longitude	<longitude,E/W>	Longitude of fix
5	Fix Quality	<quality>	0 = Invalid 1 = GPS fix 6 = estimated
6	Number of Satellites	<satellites>	Number of satellites in view
7	Horizontal Dilution of Precision (HDOP)	0.0	Not available (Value = 0)
8	Altitude	<sealevel,M>	Meters above mean sea level
9	Height of geoid above WGS84 ellipsoid	0.0,M	Not available (Value = 0)
10	Time since last DGPS update	blank	No last update
11	DGPS reference station id	blank	No station id
12	Checksum	*<CS>	Used by program to check for transmission errors
13	White spaces	<CR><LF>	Carriage return and line feed

$GPRMC – Recommended minimum specific GPS/Transit data

Format: $GPRMC,<time>,<state>,<latitude>,<longitude>,<speed>,<course>,<date>,0.0,E,<mode>*<CS><CR><LF>

Sample Data: $GPRMC,154250,A,4749.8678,N,00871.8469,E,0.0,0.0,230707,0.0,E,A*1F<CR><LF>

No.	Name	Data	Description
1	Sentence Identifier	$GPGGA	Recommended minimum specific GPS/Transit data
2	Time	<time>	UTC of position fix

3	Data status	<state>	A = Data OK
			V = navigation receiver warning

4	Latitude	<latitude,N/S>	Latitude of fix
6	Longitude	<longitude,E/W>	Longitude of fix
8	Speed	<speed>	Speed over ground in knots
9	Course	<course>	Track made good in degrees True
10	Date	<date>	UT date
11	Magnetic variation	0.0,E	Not available (Value = 0.0,E)

12	Mode	White spaces	A = autonomic = valid
			E = estimated
			N = not valid

13	Checksum	*<CS>	Used by program to check for transmission errors
14	White spaces	<CR><LF>	Carriage return and line feed

$PNMID – Racom Proprietary Sentence

Format: $PNMID,serialnumber*<CS><CR><LF>

Sample Data: $PNMID,0112BFFF2B0*1F<CR><LF>

No.	Name	Data	Description
1	Sentence Identifier	$GPGGA	Racom Proprietary Sentence
2	Serial number	<serial number>	M!DGE/MG102 serial number / MAC Address
13	Checksum	*<CS>	Used by program to check for transmission errors
14	White spaces	<CR><LF>	Carriage return and line feed

5. Troubleshooting

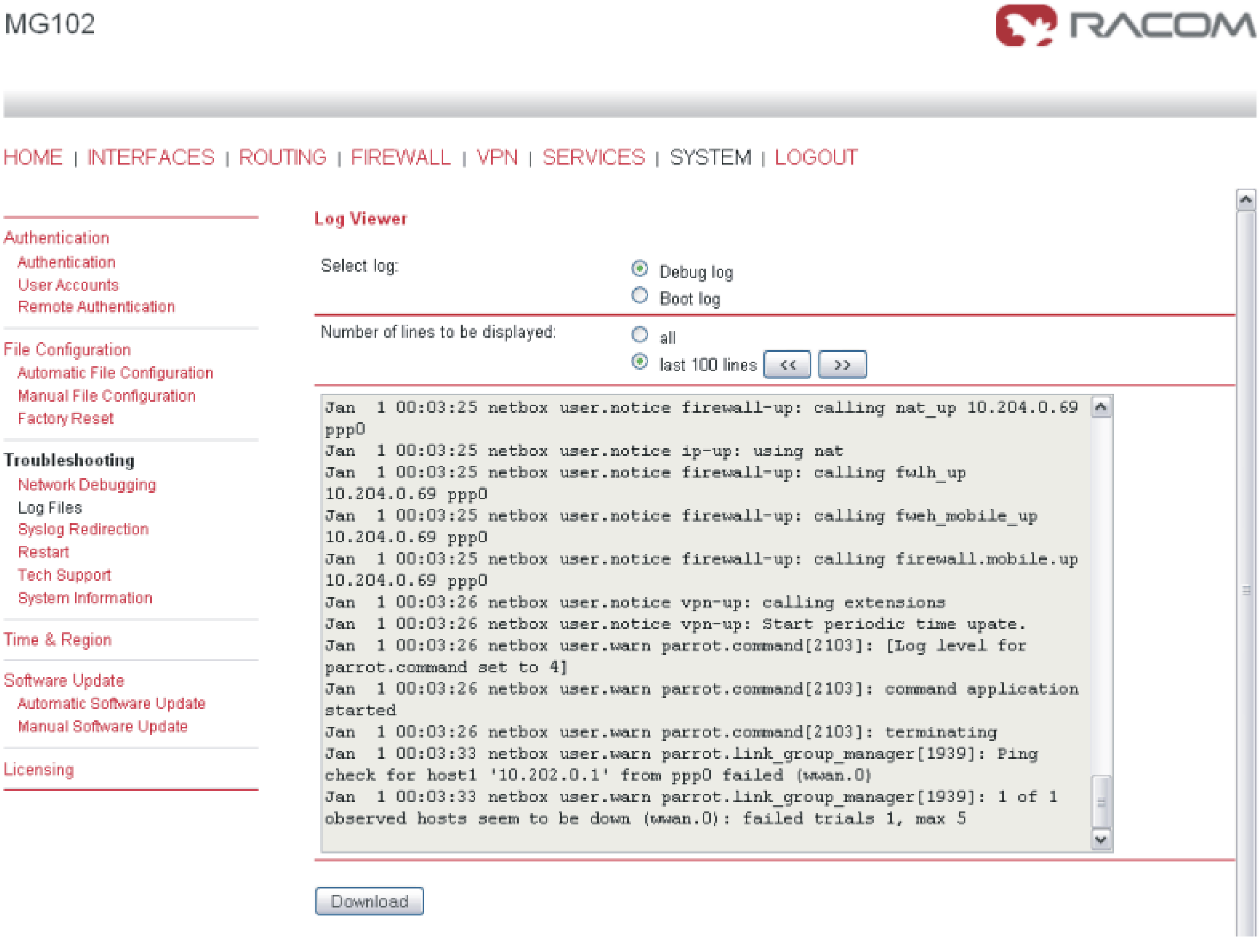
5.1. Error Messages

The Web Manager show error messages in the status bar in the footer of a certain web page.

Common error messages are:

Error Message	Problem Solving
SIM missing	Insert a SIM card
PIN code required	Insert the PIN code on the “SIM” page
Connection failed	See the “Debug Log” under Check APN, phone number, username, password

5.2. System Log and Log Files



Log Viewer

Select log: ● Debug log ○ Boot log

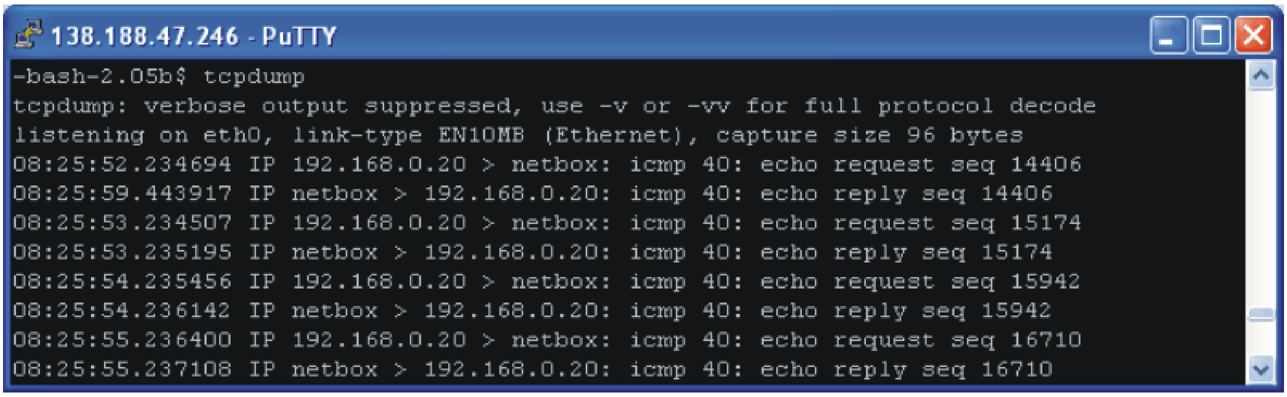
Number of lines to be displayed: ○ all ● last 100 lines

```
Jan  1 00:03:25 netbox user.notice firewall-up: calling nat_up 10.204.0.69
ppp0
Jan  1 00:03:25 netbox user.notice ip-up: using nat
Jan  1 00:03:25 netbox user.notice firewall-up: calling fwlh_up
10.204.0.69 ppp0
Jan  1 00:03:25 netbox user.notice firewall-up: calling fweh_mobile_up
10.204.0.69 ppp0
Jan  1 00:03:25 netbox user.notice firewall-up: calling firewall.mobile.up
10.204.0.69 ppp0
Jan  1 00:03:26 netbox user.notice vpn-up: calling extensions
Jan  1 00:03:26 netbox user.notice vpn-up: Start periodic time upate.
Jan  1 00:03:26 netbox user.warn parrot.command[2103]: [Log level for
parrot.command set to 4]
Jan  1 00:03:26 netbox user.warn parrot.command[2103]: command application
started
Jan  1 00:03:26 netbox user.warn parrot.command[2103]: terminating
Jan  1 00:03:33 netbox user.warn parrot.link_group_manager[1939]: Ping
check for host1 '10.202.0.1' from ppp0 failed (wwan.0)
Jan  1 00:03:33 netbox user.warn parrot.link_group_manager[1939]: 1 of 1
observed hosts seem to be down (wwan.0): failed trials 1, max 5
```

Find more information about troubleshooting tools. The Web Manager provides varions debugging tools under SYSTEM/Troubleshooting:

5.3. Network Protocol Analyzer

Via the Linux Shell (bash), the protocol analyzer “tcpdump” is available:



```
-bash-2.05b$ tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
08:25:52.234694 IP 192.168.0.20 > netbox: icmp 40: echo request seq 14406
08:25:59.443917 IP netbox > 192.168.0.20: icmp 40: echo reply seq 14406
08:25:53.234507 IP 192.168.0.20 > netbox: icmp 40: echo request seq 15174
08:25:53.235195 IP netbox > 192.168.0.20: icmp 40: echo reply seq 15174
08:25:54.235456 IP 192.168.0.20 > netbox: icmp 40: echo request seq 15942
08:25:54.236142 IP netbox > 192.168.0.20: icmp 40: echo reply seq 15942
08:25:55.236400 IP 192.168.0.20 > netbox: icmp 40: echo request seq 16710
08:25:55.237108 IP netbox > 192.168.0.20: icmp 40: echo reply seq 16710
```

6. Customer Service

6.1. Support

Please send questions or comments about M!DGE/MG102 to:

support@racom.eu

Appendix A. Connectors and Cables

A.1. Pin Assignments for the Communication Interfaces

Tab. A.1: Pin assignment COM interface RS232

DSUB9F	COM – RS232	
pin	**signal**	**In/ Out**
1	CD	O
2	RxD	O
3	TxD	I
4	DTR	I
5	GND	
6	DSR	O
7	RTS	I
8	CTS	O
9	RI	—

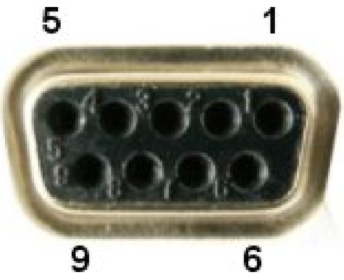


Fig. A.1: Serial connector Sub-D 9pol plug female (DSUB9F)

Tab. A.2: Pin assignment COM interface RS485

DSUB9F	COM – RS485	
pin	**signal**	**In/ Out**
1	—	—
2	—	—
3 (M!DGE)	RxD/TxD+	I/O
4	—	—
5	GND	
6	—	—
7	—	—
8	RxD/TxD−	I/O
9(MG102)	RxD/TxD+	I/O

Note

Do not use pins that are not listed here!

A.2. Ethernet Plug (ETH; RJ-45)

Tab. A.3: Pin assignment Ethernet Interface

RJ-45 Socket	ETH (Ethernet 10BaseT and 100BaseT)
pin	**signal**
1	TX+
2	TX−
3	RX+
6	RX−

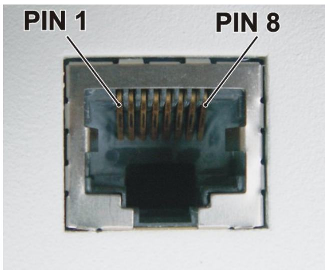


Fig. A.2: RJ-45 Plug

A.3. Power Plug MG102

Tab. A.4: Pin assignment power plug

MSTB 2,5/ 2-ST-5,08 (Phoenix Contact)	Power
pin	**signal**
1	**−**
2	**+**

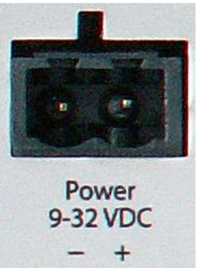


Fig. A.3: Power connector

A.4. Cable ETH/RS232

Tab. A.5: Pin assignment Ethernet Interface

	ETH RJ-45	RS232 D-SUB-9	
signal	**pin**	**pin**	**In/ Out**
RxD	3	2	O
TxD	6	3	I
DTR	7	4	I
GND	5	5	
GND	4	5	
DSR	2	6	O
RTS	8	7	I
CTS	1	8	O

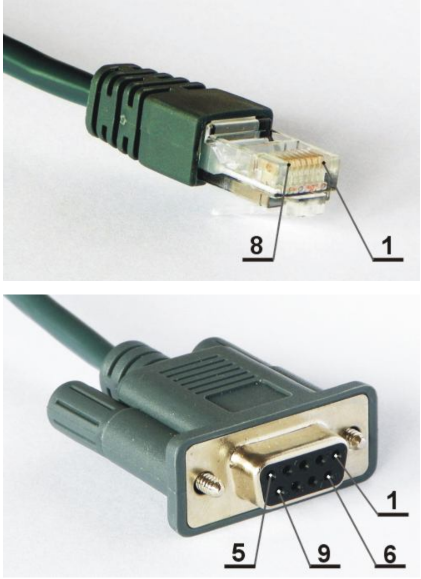


Fig. A.4: RJ-45 and RS232 D-SUB-9

Appendix B. Safety Instructions

The M!DGE/MG102 Wireless Router must be used in compliance with any and all applicable international and national laws and in compliance with any special restrictions regulating the utilization of the communication module in prescribed applications and environments.

To prevent possible injury to health and damage to appliances and to ensure that all the relevant provisions have been complied with, use only the original accessories. Unauthorized modifications or utilization of accessories that have not been approved may result in the termination of the validity of the guarantee.

The M!DGE/MG102 Wireless Routers must not be opened. Only the replacement of the SIM card is permitted.

Voltage at all connectors of the communication module is limited to SELV (Safety Extra Low Voltage) and must not be exceeded.

For use with certified (CSA or equivalent) power supply, which must have a limited and SELV circuit output. The M!DGE/MG102 is designed for indoor use only. Do not expose the communication module to extreme ambient conditions. Protect the communication module against dust, moisture and high temperature.

We remind the users of the duty to observe the restrictions concerning the utilization of radio devices at petrol stations, in chemical plants or in the course of blasting works in which explosives are used. Switch off the communication module when traveling by plane.

When using the communication module in close proximity of personal medical devices, such as cardiac pacemakers or hearing aids, you must proceed with heightened caution.

If it is in the proximity of TV sets, radio receivers and personal computers, M!DGE/MG102 Wireless Router may cause interference.

It is recommended that you should create an approximate copy or backup of all the important settings that are stored in the memory of the device.

You must not work at the antenna installation during a lightning.

Always keep a distance bigger than 40cm from the antenna in order to reduce your exposure to electromagnetic fields below the legal limits. This distance applies to Lambda/4 and Lambda/2 antennas. Bigger distances apply for antennas with higher gain.

Adhere to the instructions documented in this user's manual.

B.1. Declaration of Conformity

Racom declares that under our own responsability the products M!DGE/MG102 Wireless Routers comply with the relevant standards following the provisions of the Council Directive 1999/5/EC.

B.2. RoHS and WEEE compliance

The RAy is fully compliant with the European Commission‟s RoHS (Restriction of Certain Hazardous Substances in Electrical and Electronic Equipment) and WEEE (Waste Electrical and Electronic Equipment) environmental directives).

RoHS Restriction of hazardous substances (RoHS)

The RoHS Directive prohibits the sale in the European Union of electronic equipment containing these hazardous substances: lead, cadmium, mercury, hexavalent chromium, polybrominated biphenyls (PBBs), and polybrominated diphenyl ethers (PBDEs).

End-of-life recycling programme (WEEE)

In accordance with the requirements of the counsil directive 2002/96/EC on Waste Electronical and Electronic Equipment (WEEE), ensure that at end-of-life you separate this product from other waste and scrap and deliver it to the WEEE collection system in your country for recycling.

Appendix C. Glossary

APN	Access Point Name / Access Point Node
CE	Consumer Electronic Label by Consumer Electronic Association CEA (www.ce.org[1])
CS	Coding Scheme
CSD	Circuit Switched Data
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
EDGE	Enhanced Data Service for GSM Evolution
EMC	Electromagnetic compatibility
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GSM	Global Packet Radio Service
GUI	Graphical User Interface
HSCSD	High Speed Circuit Switched Data
HSDPA	High-Speed Downlink Packet Access
HSUPA	High-Speed Uplink Packet Access
HTML	Hypertext Markup Language
HW	Hardware
IP	Internet Protocol
IPSec	Internet Protocol Security
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
LAN	Local Area Network
NAPT	Network Address Port Translation
NAT	Network Address Translation
POP	Point of Presence
POP, POP3	Post Office Protocol, Version 3

[1] http://www.ce.org

PPP	Point to Point Protocol
RAS	Remote Access Service (Dial-in Networking PPP)
RoHS	Restriction of hazardous substances
SIM	Subscriber Identity Module
SW	Software
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
URL	Universal Resource Locator
VPN	Virtual Private Network
WEEE	Waste Electrical and Electronic Equipment) environmental directives

Appendix D. Revision History

Revision 1.1	2011-11-01
1. XML version	