RACOM
RADIO DATA NETWORKS

Operating manual

M!DGE
GPRS/UMTS/HSPA/LTE router

1.3
6/25/2013

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

Important Notice ... 5
Getting started ... 6
1. M!DGE router ... 7
1.1. Introduction ... 7
1.2. Key Features ... 7
1.3. Standards ... 8
2. M!DGE in detail ... 9
3. Implementation Notes ... 11
3.1. Ethernet SCADA protocols ... 11
3.2. Serial SCADA protocols ... 11
3.3. Centre of the network ... 11
3.4. VPN tunnels ... 11
4. Product ... 12
4.1. Dimensions ... 12
4.2. Connectors ... 12
4.3. Indication LEDs ... 15
4.4. Technical specifications ... 17
4.5. Model offerings ... 19
4.6. Accessories ... 19
5. Bench test / Step by Step Guide ... 21
5.1. Connecting the hardware ... 21
5.2. Powering up your M!DGE ... 21
5.3. Connecting M!DGE to a programming PC ... 21
5.4. Basic Setup ... 22
6. Installation ... 23
6.1. Mounting ... 23
6.2. Antenna mounting ... 23
6.3. Grounding ... 23
6.4. Power Supply ... 23
7. Web Configuration ... 24
7.1. HOME ... 24
7.2. INTERFACES ... 25
7.3. ROUTING ... 38
7.4. FIREWALL ... 42
7.5. VPN ... 46
7.6. SERVICES ... 54
7.7. SYSTEM ... 77
7.8. LOGOUT ... 93
8. Command Line Interface ... 94
8.1. General Usage ... 94
8.2. Print Help ... 95
8.3. Getting Config Parameters ... 96
8.4. Setting Config Parameters ... 96
8.5. Getting Status Information ... 96
8.6. Sending E-Mail or SMS ... 97
8.7. Updating System Facilities ... 98
8.8. Restarting Services ... 98
8.9. Resetting System ... 99
8.10. Rebooting System ... 99
8.11. Running Shell Commands ... 99
8.12. CLI–PHP ... 99

9. Troubleshooting ... 103
9.1. Common Errors ... 103
9.2. Messages ... 103
9.3. Troubleshooting tools ... 104
10. Safety, environment, licensing ... 105
10.1. Safety Instructions ... 105
10.2. Warranty ... 106
A. Glossary ... 107
Index ... 109
B. Revision History ... 111

List of Figures

1. Router M!DGE UMTS and M!DGE LTE ... 6
2.1. Front panel and terminal panel of M!DGE ... 9
4.1. Dimensions in milimetres ... 12
4.2. Antenna connectors SMA ... 12
4.3. 2× Eth RJ45 Plug - pin numbering ... 13
4.4. USB connector ... 13
4.5. Screw terminal ... 14
4.6. Indication LEDs ... 15
4.7. Flat bracket ... 19
4.8. Demo case ... 20
6.1. Grounding ... 23

List of Tables

4.1. Pin assignment Ethernet Interface ... 13
4.2. USB pin description ... 13
4.3. Pin assignment of screw terminal ... 14
4.4. Digital inputs levels ... 14
4.5. Digital outputs parametres ... 14
4.6. M!DGEs interfaces and status indicators ... 16
4.7. Technical specifications ... 18

Important Notice

Copyright

Disclaimer

Although every precaution has been taken in preparing this information, RACOM assumes no liability for errors and omissions, or any damages resulting from the use of this information. This document or the equipment may be modified without notice, in the interests of improving the product.

Trademark

All trademarks and product names are the property of their respective owners.

Important Notice

- Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors), or be totally lost. Significant delays or losses of data are rare when wireless devices such as the M!DGE are used in an appropriate manner within a well-constructed network. M!DGE should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. RACOM accepts no liability for damages of any kind resulting from delays or errors in data transmitted or received using M!DGE, or for the failure of M!DGE to transmit or receive such data.
- Under no circumstances is RACOM or any other company or person responsible for incidental, accidental or related damage arising as a result of the use of this product. RACOM does not provide the user with any form of guarantee containing assurance of the suitability and applicability for its application.
- RACOM products are not developed, designed or tested for use in applications which may directly affect health and/or life functions of humans or animals, nor to be a component of similarly important systems, and RACOM does not provide any guarantee when company products are used in such applications.

Getting started

M!DGE Wireless Routers will only operate reliably over the cellular network if there is a strong signal. For many applications a flexible stub antenna would be suitable but in some circumstances it may be necessary to use a remote antenna with an extension cable to allow the antenna itself to be positioned so as to provide the best possible signal reception. RACOM can supply a range of suitable antennas.

1. **Install the SIM card**
   Insert a SIM card into the SIM socket. Make sure the SIM is suitable for data transmission.
2. **Connect the GSM/UMTS antenna**
   Fit a GSM/UMTS antenna. 1. If needed, contact RACOM for suitable antennas and other details.
3. **Connect the LAN cable**
   Connect one M!DGE Ethernet port to your computer using an Eth cat.5 cable
4. **Connect the power supply**
   Connect the power supply wires to the M!DGE screw terminals. Enable the power supply.
5. **Setting of IP address of the connected computer**
   By default the DHCP server is enabled, thus you can allow the Dynamic Host Configuration Protocol (DHCP) on your computer to lease an IP address from the M!DGE. Wait aproximatelly 20 seconds until your computer has received the parameters (IP address, subnet mask, default gateway, DNS server).
   As an alternative. you can configure a static IP address on your PC (e.g. 192.168.1.2/24) so that it is operating in the same subnet as the M!DGE. The M!DGE default IP address for first Eth interface is 192.168.1.1, the subnet mask is 255.255.255.0.
6. **Start setting up using web browser**
   Open a web browser such as Internet Explorer or Firefox. In the address field of the web browser, enter default IP address of M!DGE (i.e. http://192.168.1.1); initial screen will appear. Follow the instructions and use the M!DGE/MG102 Web Manager to configure the device. For more datails see chap. 7. Web Configuration

Fig. 1: Router M!DGE UMTS and M!DGE LTE

1. M!DGE router

1.1. Introduction

Although M!DGE wireless routers have been specifically designed for SCADA and telemetry, they are well suited to variety of wireless applications. M!DGE HW and SW are ready to maintain reliable and secure connections from an unlimited number of remote locations to a central server. Both standard Ethernet/IP and serial interfaces are available. Moreover, two digital inputs and two digital outputs can be used for direct monitoring and control of application devices.

M!DGE versatility is further enhanced by two independent Ethernet ports. These can be configured to either support two independent LANs (e.g. LAN and WAN settings), or simply connect two devices within one LAN (effectively replacing an Eth switch). M!DGE software is based on proven components, including an Embedded Linux operating system and standard TCP/IP communication protocols.

Combining M!DGE with an MG102 two-SIM router in one network is quite straightforward because of fully compatible interface settings and behaviour on all HW interfaces. Thanks to the compact size and versatility of M!DGE, wireless routers prove indispensable in many SCADA and telemetry, as well as POS, ATM, lottery and security/surveillance applications.

M!DGE together with RACOM RipEX radio router offers an unrivalled solution for combining GPRS and UHF/VHF licensed radio in a single network. Even a single RipEX in the centre of a M!DGE network allows for efficient use of addressed serial SCADA protocols.

1.2. Key Features

Mobile Interface Parameters

- Mobile Connection HSDPA, HSUPA, UMTS, EDGE, GPRS, GSM and LTE
- Global connectivity
- Transparent hand-over between 2G and 3G (M!DGE UMTS) or 2G, 3G and 4G (M!DGE LTE)

Power supply

- Redundant dual power input pins
- Input voltage: 10.2 – 57.6 VDC
- Max. power consumption: 5 W

Services /Networking

- Fallback Management
- Connection supervision
- Automatic connection recovery
- OpenVPN, IPsec, PPTP, NAPT
- VRRP
- DHCP server, DNS proxy server, DNS update agent
- Telnet server, SSH server, Web server
- NTP
- COM server, Modbus gateway
- Port Forwarding
- Firewall, Access Control Lists

Interfaces

- 2 Ethernet ports: LAN, WAN/LAN
- RS232
- 2× DI, 2× DO
- USB host

Diagnostic and Management

- Web interface, CLI available
- File configuration
- OTA SW update
- Advanced troubleshooting
- SMS remote control, SMS and E-mail notification
- SNMP

1.3. Standards

EMC	EN 301 489-1 V1.7.1
	EN 301 489-7 V1.3.1
	EN 61 000-6:2005
	EN 50 121-3-2:2006
	EN 50 121-4:2006
Electrical Safety	EN 60950-1:2006
IP rating	IP40
ETH	IEEE 802.3i
	IEEE 802.3u
	IEEE 802.3af

2. M!DGE in detail

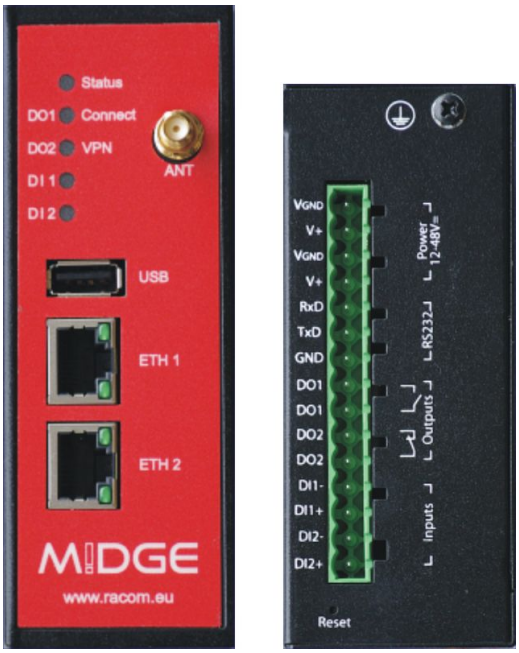


Fig. 2.1: Front panel and terminal panel of M!DGE

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

- Interfaces and Connection Management (section Section 7.2, “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 7.3, “ROUTING”)
  - Static Routing
  - NAPT / Port Forwarding
- Security / Firewall (section Section 7.4, “FIREWALL”)
  - NAPT / Port Forwarding
  - Access Control Lists
  - Stateful Inspection Firewall
- Virtual Private Networking (VPN) (section Section 7.5, “VPN”)
  - OpenVPN Client
  - PPTP Server
  - IPsec Peer
  - Dial-in Server
- Services (section Section 7.6, “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 7.7, “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

3. Implementation Notes

3.1. Ethernet SCADA protocols

SCADA equipment with an Ethernet protocol behave as standard Ethernet equipment from a communications perspective . Thus the communication goes transparently through the GPRS//UMTS/LTE network. The implementation requires a heightened caution to IP addressing and routing. NAPT functionality should be used frequently.

3.2. Serial SCADA protocols

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

Please read the application note SCADA applications and M!DGE/MG102[1] which describes how to efficiently solve this problem using RACOM routers.

3.3. Centre of the network

In every network, the centre plays a key role and has to be designed according to customer's requirements. Several possible solutions are described in the application note M!DGE/MG102 CENTRE – Application note[2].

3.4. VPN tunnels

security of customer's data arriving through the mobile network is often very important. Private APN is the basic security requirement, but not safe enough for such applications.

VPN tunnels solution is closely connected with the centre. The solution is mentioned in application note M!DGE/MG102 CENTRE – Application note[3], details for the elemental solution are described in the application note SCADA applications and M!DGE/MG102[4].

[1] http://hnilux.racom.cz:3004/download/hw/midge/free/cz/midge-app-en.pdf
[2] http://hnilux.racom.cz:3004/download/hw/midge/free/cz/midge-app-en1.pdf
[3] http://hnilux.racom.cz:3004/download/hw/midge/free/cz/midge-app-en1.pdf
[4] http://hnilux.racom.cz:3004/download/hw/midge/free/cz/midge-app-en.pdf

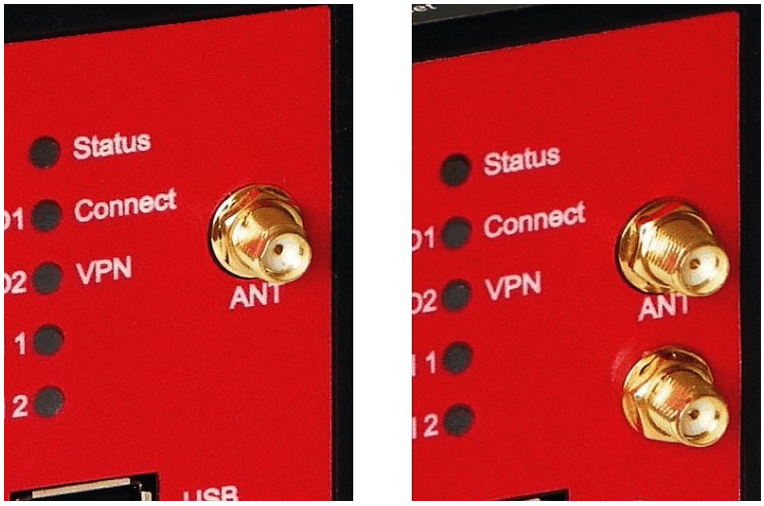
4. Product

4.1. Dimensions

Fig. 4.1: Dimensions in milimetres

4.2. Connectors

4.2.1. Antenna SMA



The UMTS model has one SMA antenna connector.

The LTE model is equipped with two antenna connectors. The ANT connector (above) serves as a main antenna connection, the second connector is auxiliary and serves for better communication with BTS (diversity).

Fig. 4.2: Antenna connectors SMA

4.2.2. 2× Eth RJ45

Tab. 4.1: Pin assignment Ethernet Interface

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

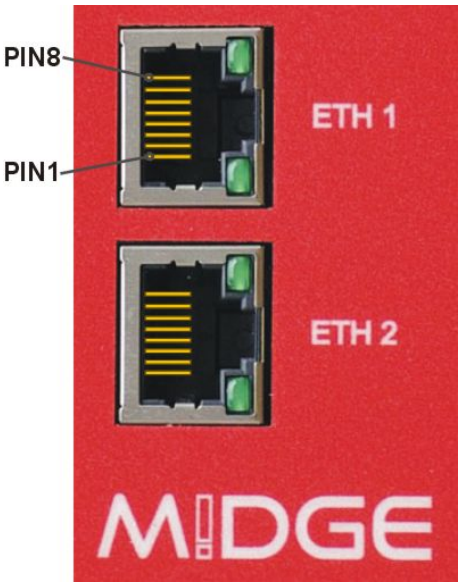


Fig. 4.3: 2× Eth RJ45 Plug - pin numbering

4.2.3. USB

M!dge uses USB 1.1, Host A interface. USB interface is wired as standard:

Tab. 4.2: USB pin description

USB pin	signal	wire
1	+5 V	red
2	Data(−)	white
3	Data (+)	green
4	GND	black

Fig. 4.4: USB connector

4.2.4. Screw terminal

Screw terminal plug type Stelvio Kontek CPF5/15 or MRT3P/15V01 can be used.

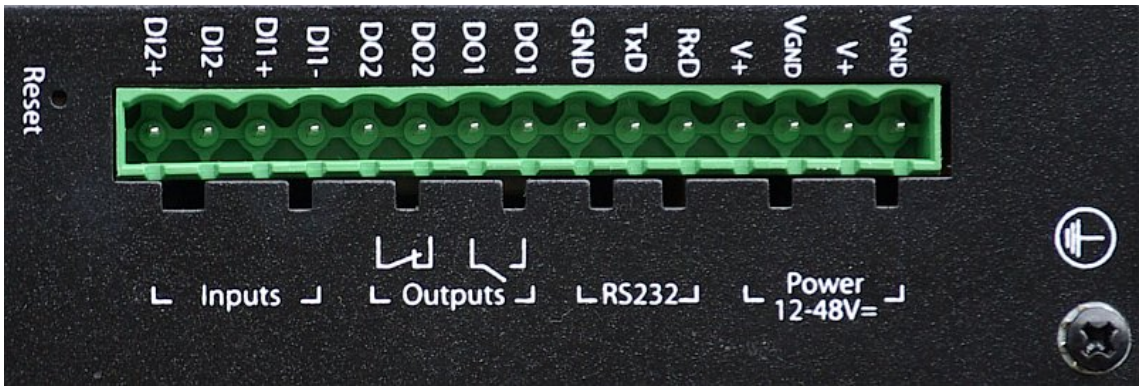


Fig. 4.5: Screw terminal

Tab. 4.3: Pin assignment of screw terminal

pin	pin description	signal
1	V_{GND}	Ground internally connected with casing ground
2	V+ (12–48 V=)	Dual power input - not connected with pin 4: 12–48 VDC (–15% +20%) = 10.2–57.6 VDC
3	V_{GND}	Ground internally connected with casing ground
4	V+ (12–48 V=)	Dual power input– not connected with pin 2: 12–48 VDC (–15 % +20 %) = 10.2–57.6 VDC.
5	RxD	RS232 – RxD
6	TxD	RS232 – RxD
7	GND	RS232 – RxD
8	DO1:	Digital output. Dry contact relay. Normally open with M!DGE without powering
9		
10	DO2:	Digital output. Dry contact relay. Normally open with M!DGE without powering. See section Section 7.2.6, “Digital I/O” for detailes.
11		
12	DI1−	Digital input 1 See section Section 7.2.6, “Digital I/O”
13	DI1+	Digital input 1
14	DI2−	Digital input 2
15	DI2+	Digital input 2

Tab. 4.4: 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.	

Tab. 4.5: Digital outputs parametres

Maximal continuous current	1 A
Maximal switching voltage	60 VDC, 42 VAC (Vrms)
Maximal switching capacity	60 W

4.2.5. Reset button

The Reset button is placed close to the screw terminal and it is labelled "Reset". Use a blunt tool with 1 mm in diameter (e.g. paper clip) to press the button.

Keep it pressed for at least 3 seconds for reboot and at least 10 seconds for a factory reset. The start of the factory reset is confirmed by all LEDs lighting up for one second. The button can be released afterwards.

4.3. Indication LEDs

Fig. 4.6: Indication LEDs

Tab. 4.6: M!DGEs interfaces and status indicators

Label	State	Function
Status	blinking slowly	Start up, maintenance
	solid	Ready
	green color	Right side description
	yellow color	Left side description
Connect	green on	Excellent GSM signal
	yellow on	Medium GSM signal
	red on	Weak GSM signal
	red blinking	Mobile interface enabled but not connected
	red continually	Connected
VPN	green on	VPN connection is up
	green blinking	VPN connection is enabled and not connected
DO1	yellow on	Closed
	yellow off	Opened
DO2	yellow on	Closed
	yellow off	Opened
DI1	yellow on	Input set
	yellow off	Input not set
DI2	yellow on	Input set
	yellow off	Input not set

4.4. Technical specifications

Tab. 4.7: Technical specifications

Mobile Interface UMTS	Multimode HSDPA, HSUPA, UMTS, EDGE, GPRS and GSM 3G–UMTS, HSDPA, HSUPA, UMTS: 850/900/1900/2100 MHz 2G–EDGE, GPRS, GSM: 850/900/1800/1900 MHz Data rates: max. 7.2 Mbps downlink / 5.76 Mbps uplink	
Mobile Interface LTE	Multimode LTE, HSPA+, UMTS, EDGE, GPRS, GSM 4G–LTE: 800/900/1800/2100/2600 MHz 3G–UMTS/HSPA+: 900/2100 MHz 2G–GSM/GPRS/EDGE: 900/1800/1900 MHz Data rates up to 100 Mbps downlink / 50 Mbps uplink	
Ethernet	2× Ethernet 10/100 Base-T, Auto MDX, 2× RJ45, bridged or routed	
Serial Interface	1× 3-wire RS232 on 15-pin screw terminal block	
Digital I/O	2 digital inputs	0–5.6 VDC level 0 7.2–40 VDC level 1, maximum voltage 40 VDC
	2 digital outputs	Relay outputs 1st NO, 2nd NC Limiting continuous current 1 A Max. switching voltage 60 VDC, 42 VAC (Vrms) Maximum switching capacity 60 W on 15-pin terminal block
USB service interface	USB host interface supporting memory devices USB type A connector	
Antenna Interface	Impedance:	50 Ω
	Connector:	SMA female
Power Supply	Input voltage:	10.2–57.6 VDC (12–48 VDC –15 % / +20 %)
	Power consumption:	Rx max. 3.2 W Tx max. 5 W
Environmental Conditions	For indoor use only, IP40 Metal casing, DIN rail mounting kit included Temperature range: –25 to +70 °C (–13 to +158 °F) Humidity: 0 to 95 % (non condensing) Overvoltage Category: II Pollution Degree: 2	
Mounting	DIN rail mounting	
Dimensions / Weight	125 × 45 × 110 mm, 450 g (1 lbs)	
Type Approval	CE, R&TTE (see EC Declaration of Conformity)	
Options		
Antennas	Various antennas suitable for your application are available	
Mounting kit	Flat bracket mounting kit	

4.5. Model offerings

M!DGE-UMTS GPRS/EDGE/UMTS/HSPA router, 2Eth, RS232, 2DI, 2DO
DIN rail holder included

M!DGE-LTE GPRS/EDGE/UMTS/HSPA+/LTE router, 2Eth, RS232, 2DI, 2DO
DIN rail holder included

SW feature keys

The SW feature key should be added to a new or running system via adding a licence: menu SYSTEM - Licensing (see Section 7.7.7, “Licensing”).

Mobile IP This key allows building a MobileIP VPN tunnel. See http://en.wikipedia.org/wiki/Mobile_IP for short explanation.

Server Ext. OpenVPN server extension - without this key the maximum number of connected clients shall reach 10. This key extends the number to 25.

4.6. Accessories

4.6.1. F bracket

Fig. 4.7: Flat bracket

Flat-bracket

Installation bracket for flat mounting. For details on use see chapter Mounting and chapter Dimensions.

4.6.2. Demo case

A rugged plastic case for carrying up to three RipEX's and one M!DGE 3G SCADA router. It also contains all the accessories needed to perform an on-site signal measurement, complete application bench-test or a functional demostration of both radiomodems and the 3G router. During a field test, units can be powered from the backup battery and external antenna can be connected to one of the RipEX units through the „N“ connector on the case.

Fig. 4.8: Demo case

Contents:

- Brackets and cabling for installation of three RipEXes and one M!DGE (units are not part of the delivery)
- 1× power supply Mean Well AD-155A (100-240 V AC 50-60 Hz/13.8 V DC)
- 1× Backup battery (12V/5Ah, FASTON.250), e.g. Fiamm 12FGH23
- 1× Power cable (European Schuko CEE 7/7 to IEC 320 C13)
- 1× Ethernet patch cable (3 m, UTP CAT 5E, 2× RJ-45)
- Quick start guide

RipEX accessories:

- 3× Dummy load antennas
- 1× L-bracket, 1x Flat-bracket samples
- 1× Fan kit
- 1× X5 – ETH/USB adapter

M!DGE accessories:

- Whip antenna (900–2100 MHz, 2.2 dBi, vertical)
- Externel dimensions: 455 × 365 × 185 mm
- Weight approx. 4 kg (excluding RipEXes and M!DGE)

5. Bench test / Step by Step Guide

Before starting to work with the HW please be sure that you have a SIM card enabled for data and you have all the necessary information from the mobile operator (PIN, APN, login, passwd)

5.1. Connecting the hardware

5.1.1. Install the SIM card

Insert a SIM card into the SIM socket. If the router has two SIM card sockets, use the first one. Make sure the SIM is suitable for data transmission.

There are two reasons for installing the SIM card as the first task: a) the SIM card may be damaged when inserted into the powered equipment, b) the information from SIM card are read only after a power cycle.

5.1.2. Connect the GSM/UMTS antenna

Fit a GSM/UMTS antenna. For details see section Section 4.6, “Accessories” or contact RACOM for suitable antennas.

5.1.3. Connect the LAN cable

Connect one M!DGE Ethernet port to your computer using an Eth cat.5 cable.

5.1.4. Connect the power supply

Connect the power supply wires to the M!DGE screw terminals. Enable of the power supply.

5.2. Powering up your M!DGE

Switch on your power supply. Status LED flashes for a few seconds and after 8 seconds it starts blinking to a green light. After approximately 30 seconds your M!DGE will have booted and will be ready; the Status LED remains shining on.

When the Mobile Connection is enabled the Connect LED starts blinking while connecting to the GPRS/UMTS network – the color (green/yellow/red) represents the signal strength (excellent, medium, weak).

You’ll find the description of the individual LED states in Section Section 4.3, “Indication LEDs”.

5.3. Connecting M!DGE to a programming PC

a. Please connect the Ethernet interfaces of your computer and M!DGE.
b. If not yet enabled, please enable the Dynamic Host Configuration Protocol (DHCP) so that your computer can lease an IP address from M!DGE. Wait a moment until your PC has received the parameters (IP address, subnet mask, default gateway, DNS server). How to do using Windows XP:

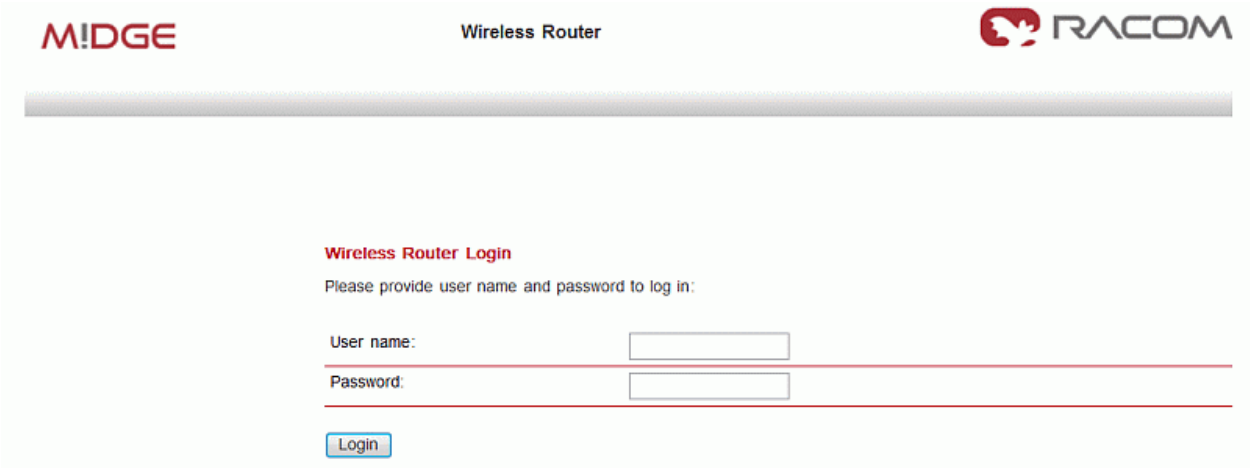
   Start > Connect To > Show all connections > Local Area Connection > Right Click > Properties > Internet Protocol (TCP/IP) > Properties > Obtain an IP address automatically.

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.

The factory default IP address is `192.168.1.1` The default subnet mask is `255.255.255.0`.

c. Start a Web Browser on your PC. Type the M!DGE/MG102 IP address in the address bar: `http://192.168.1.1`

d. 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.



5.4. Basic Setup

The M!DGE/MG102 Web Manager can always be reached via the Ethernet interface. After successful setup, 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, IP address of the Ethernet interface is 192.168.1.1, the web server runs on port 80.

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. Starting the mobile connection

6. Installation

6.1. Mounting

M!DGE Wireless Router is designed for a DIN rail mounting or on a panel using flat bracket. Please consider the safety instructions in Chapter 10, *Safety, environment, licensing*.

6.2. Antenna mounting

M!DGE Wireless Routers will only operate reliably over the GSM network if there is a strong signal. For many applications the flexible stub antenna provided would 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 so as to provide the best possible signal reception. RACOM can supply a range of suitable antennas.

Beware of the eflective effects caused by large metal surfaces (elevators, machine housings, etc.), close meshed iron constructions and choose the antenna location accordingly. Fit the antenna or connect the antenna cable to the GSM antenna connector.

In external antennas the surge protection of coaxial connection would be required.

Note

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

6.3. Grounding

Grounding screw has to be properly connected with cabinet grounding using a copper wire with minimal cross section of 4 mm^2.

Fig. 6.1: Grounding

6.4. Power Supply

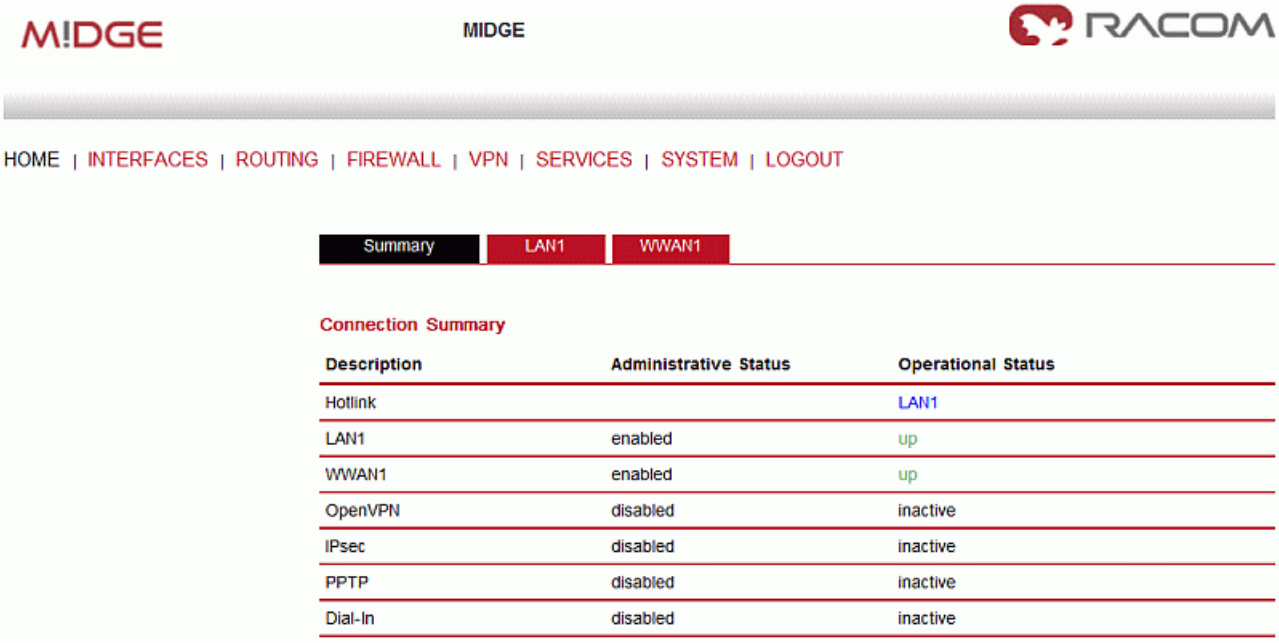
M!DGE can be powered with an external power source capable of voltages from 10 to 55 Volts DC. M!DGE should be powered using a certified (CSA or equivalent) power supply, which must have a limited and SELV circuit output.

M!DGE is equipped with dual power supply connector - it is possible to use two independent power supplies (even with different voltage). The ground terminals are connected together and they are connected with the box grounding as well.

7. Web Configuration

7.1. HOME

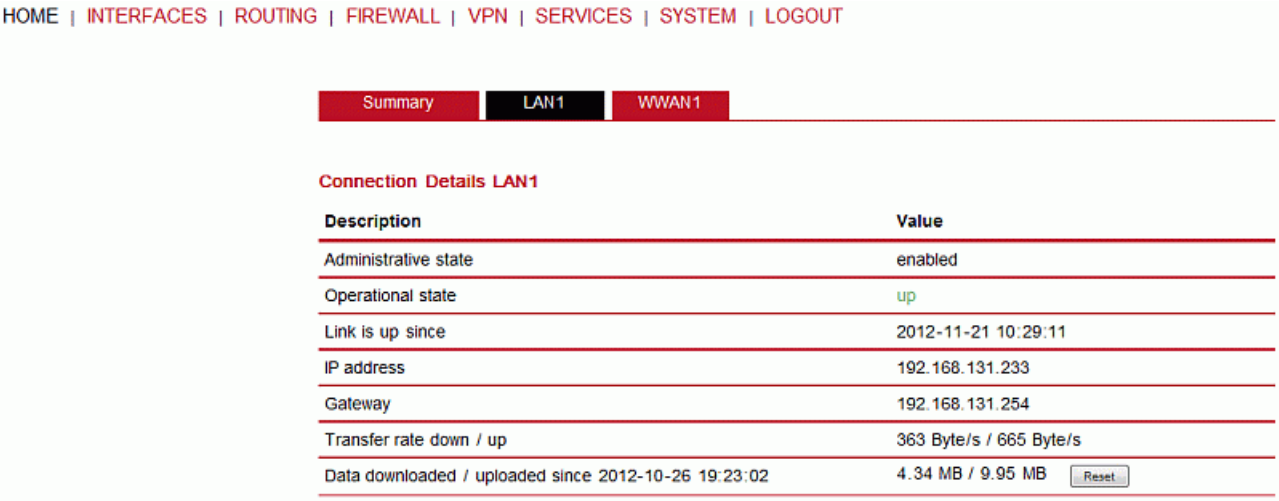
This page gives you a system overview. It helps you when initially setting up the device and also functions as a dashboard during normal operation.



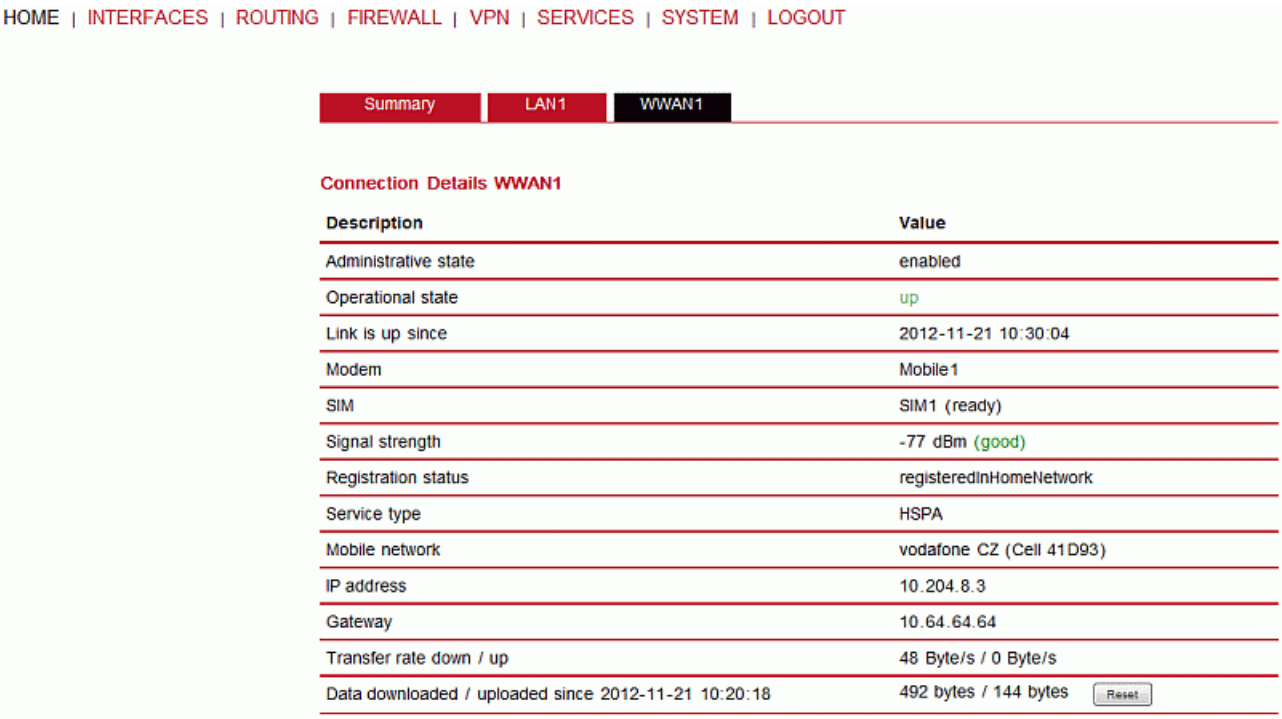
Description	Administrative Status	Operational Status
Hotlink		LAN1
LAN1	enabled	up
WWAN1	enabled	up
OpenVPN	disabled	inactive
IPsec	disabled	inactive
PPTP	disabled	inactive
Dial-In	disabled	inactive

The highest priority link which has been established successfully will become the so-called **hotlink** which holds the default route for outgoing packets.

Detailed information about status of each WAN interface is available in a separate window.



Description	Value
Administrative state	enabled
Operational state	up
Link is up since	2012-11-21 10:29:11
IP address	192.168.131.233
Gateway	192.168.131.254
Transfer rate down / up	363 Byte/s / 665 Byte/s
Data downloaded / uploaded since 2012-10-26 19:23:02	4.34 MB / 9.95 MB



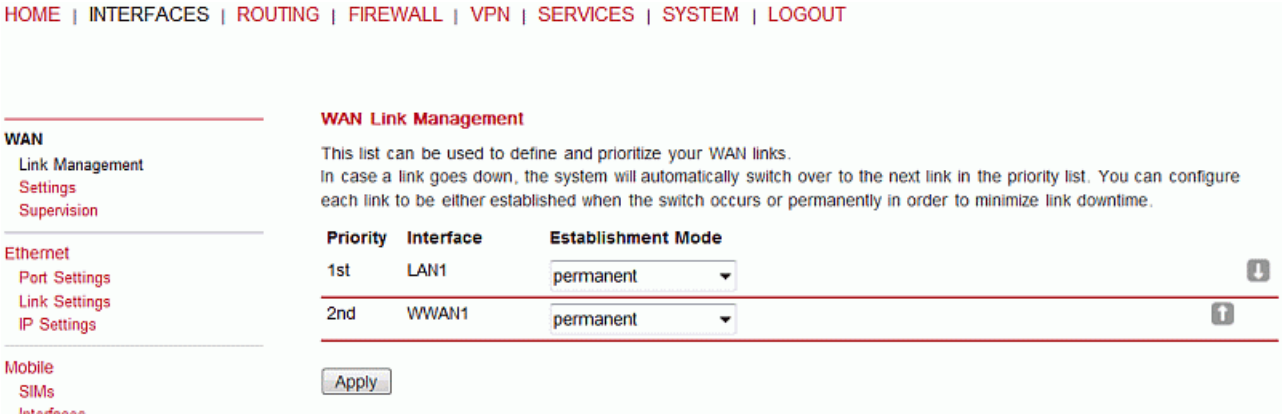
7.2. INTERFACES

Details for all physical connections are given in section Section 4.2, “Connectors”.

7.2.1. WAN

Link Management

The item available in WAN Link Manager matches with enabled WAN interfaces - for edding an item you have to set respective WAN interface (e.g. Ethernet, Mobile). The priority you can change using arrows on the right side of the window.



1st priority: This link will be used whenever possible.

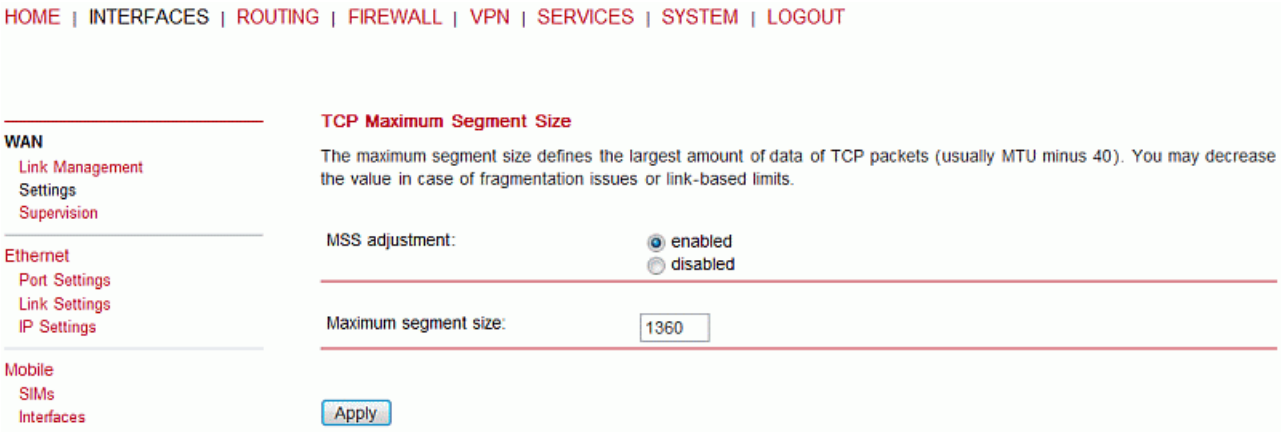
2nd priority: The first fallback technology. You can keep it ready (faster) or establish it only when the fallback actually occurs.

Up to four priorities shall be used.

Links are being triggered every 5 seconds and put to sleep for 30 seconds in case it was not possible to establish them within 30 seconds. Hence it might happen that permanent links will be dialed in background and, as soon as they got established, replace lower priority links again.

We recommend to generally use the **permanent** option for WAN links. However, in case of time-limited mobile tariffs, the **switchover** option should be used.

Settings



The maximum segment size defines the largest amount of data of TCP packets (usually MTU minus 40). You may decrease the value in case of fragmentation issues or link-based limits.

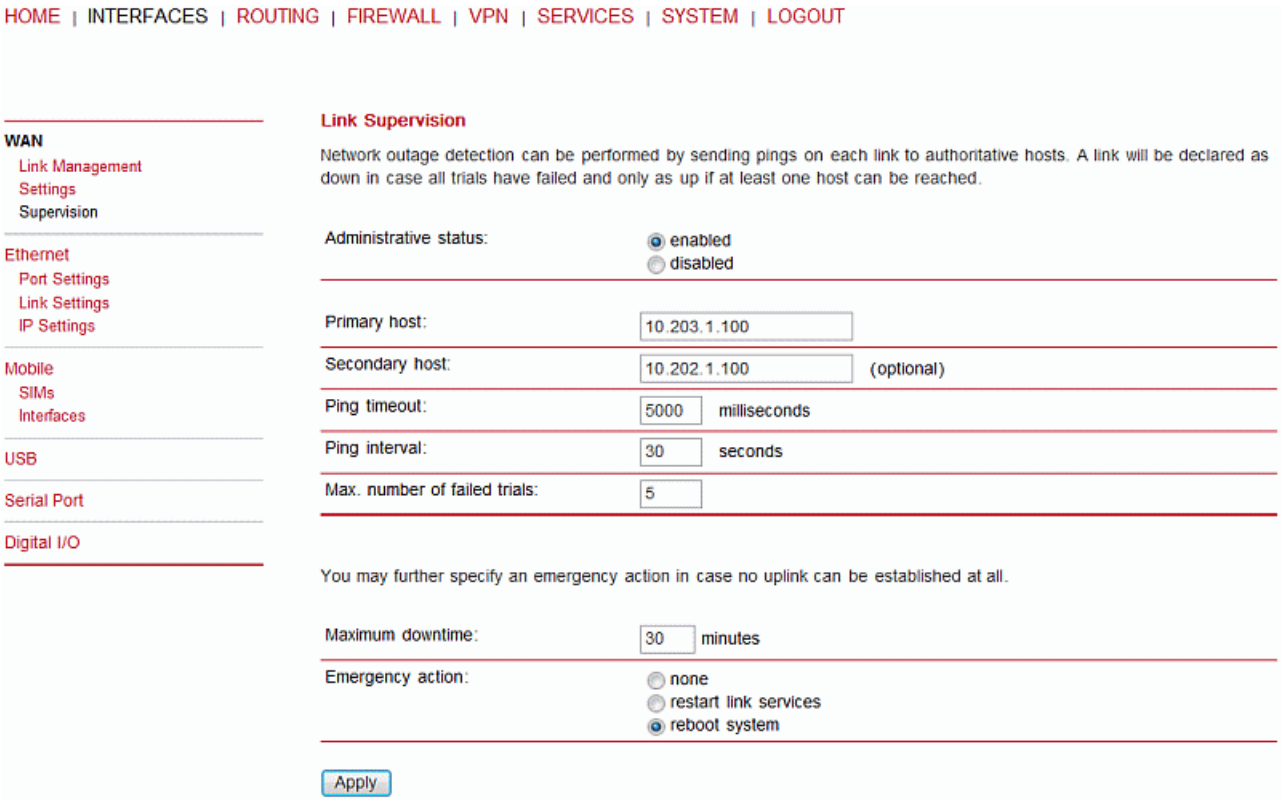
MSS adjustment	Enable or disable MSS adjustment on WAN interfaces.
Maximum segment size	Maximum number of bytes in a TCP data segment.

Connection Supervision

The connection supervision is used for switching between several connections if available. In addition it is possible set an emergency action for case that no connection is available with maximal down time.

Actions are:

- None
- Restart link services
- Reboot system



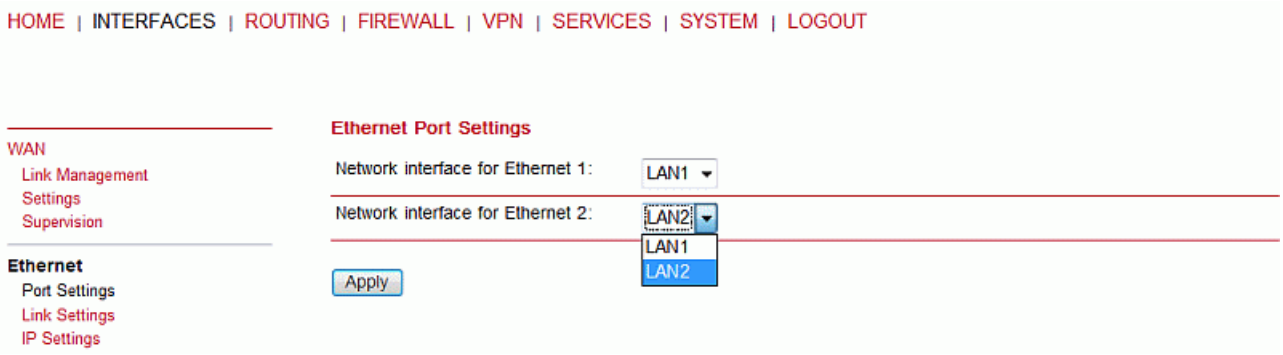
Supervision status:	Enable or disable connection supervision.
Primary host:	Reference host 1 which will be used for checking IP connectivity (done via ICMP pings).
Secondary host:	Reference host which will be used for checking IP connectivity (done via ICMP pings). The test is considered successful if either host 1 or 2 answers.
Ping Timeout:	Time for which the system is waiting for ping response. With mobile networks the response should last even several seconds in some cases. You can check the typical response using SYSTEM-Troubleshooting-Network Debugging-Ping. The first response is typically longer in GPRS/UMTS networks, the timeout should be longer than this time.
Ping interval:	Time to wait before sending the next probe.
Max. number of failed trials:	The maximum number of failed ping trials until the ping check will be declared as failed.

7.2.2. Ethernet

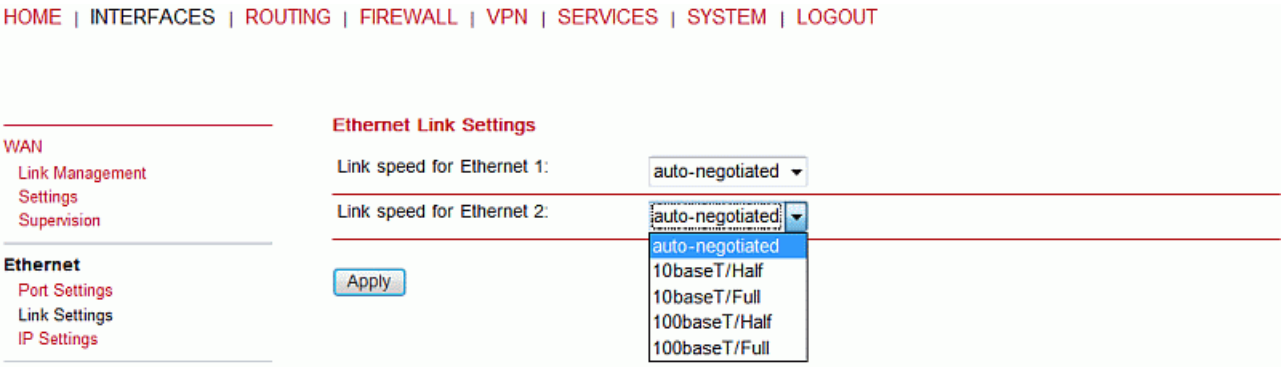
Port Settings

This menu can be used to individual assigning of each Ethernet port to a LAN interface in case you want to have different subnets per port or use one port as WAN interface.

If it is desired to have both ports in the same LAN you may assign them to the same interface. Please note that the ports will be bridged by software and operated by running the Spanning Tree Protocol.



Link Settings



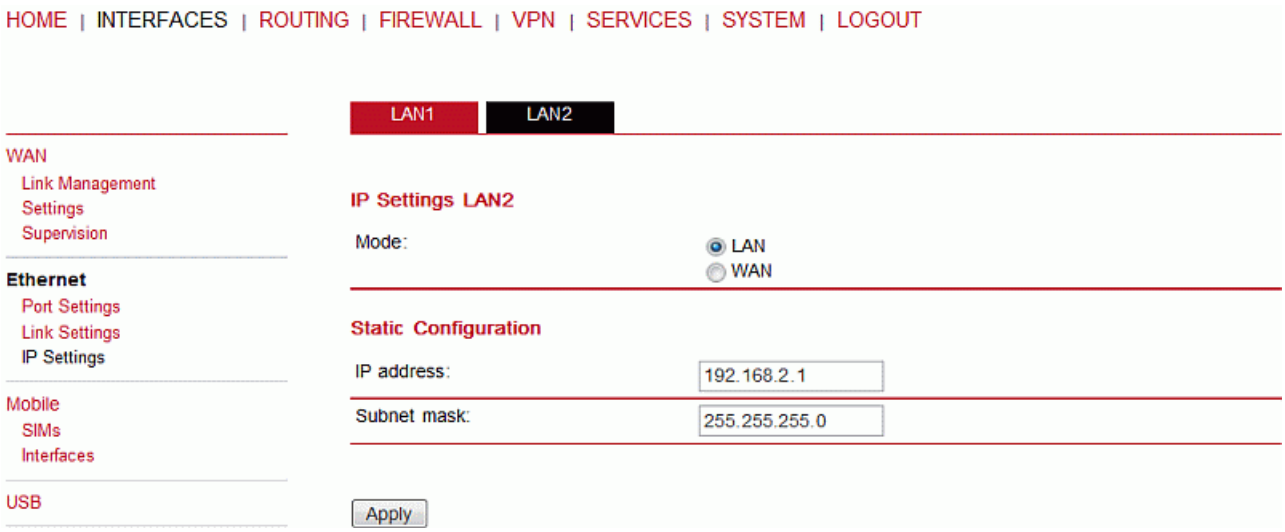
Link negotiation can be set for each Ethernet port individually. Most devices support autonegotiation which will configure the link speed automatically according to the existing devices in the network, however manual setting of 10 basetT or 100 baseT and Half or Full duplex shall be set as well.

IP Settings

Two individual windows will be used when different LAN is set in Port settings menu. For each of them you can define whether LAN or WAN interface has to be used.

Note

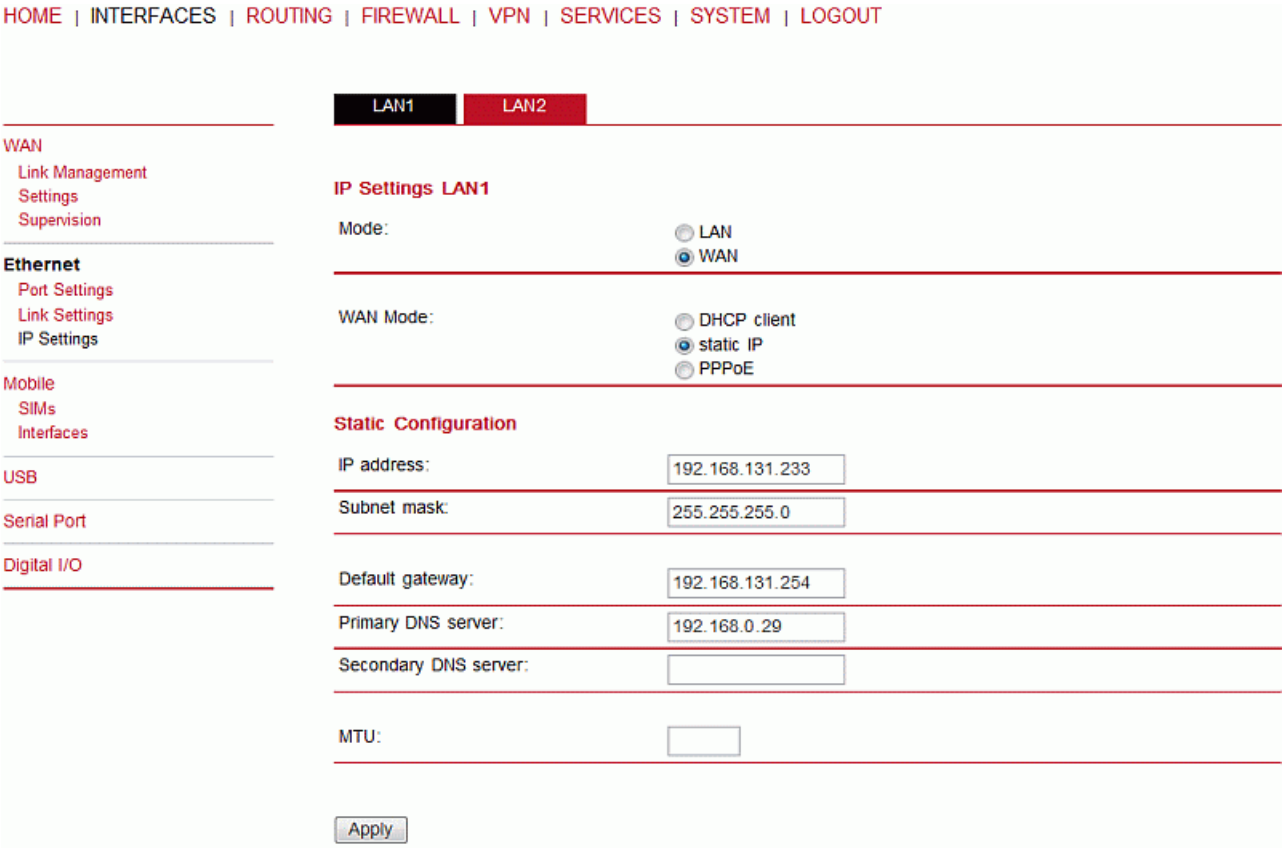
The default IP address for LAN 1 interface is 192.168.1.1/24, for LAN2 192.168.2.1/24



Static configuration of M!DGE's own IP address and Subnet mask is available for LAN mode.

Note

Setting of the IP address is conected with the DHCP Server (if enabled) - menu SERVICES-DHCP Server.



WAN mode enables the following possibilities:

DHCP client — means that the IP configuration will be retrieved from a DHCP server in the network. Thus, no further configuration is required.

Static configuration	allows you to set the IP parameters manually. Not only IP address and Subnet mask, but Default gateway and at least the Primary DNS server has to be set.	
PPPoE	is the preferred protocol when communicating with another WAN access device (like a DSL modem).	
	User name:	PPPoE user name to be used for authentication at the access device.
	Password:	PPPoE password to be used for authentication at the access device.
	Service name:	Specifies the service name set of 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.

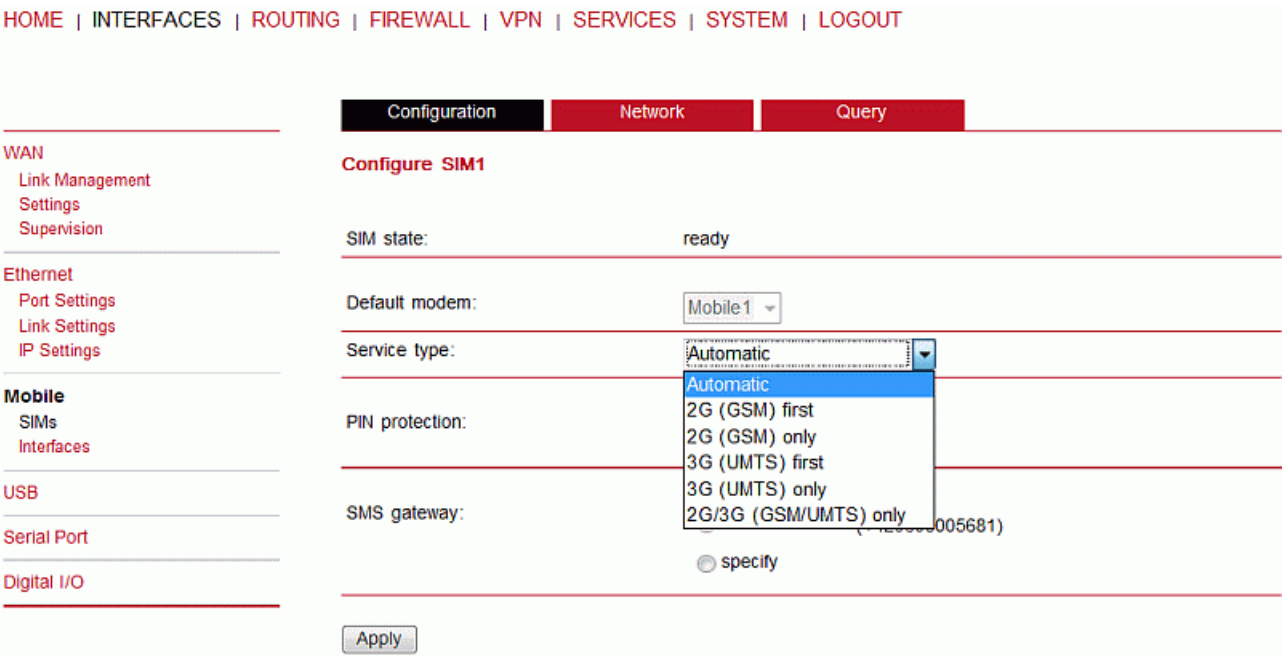
7.2.3. Mobile

SIMs

The SIM page gives an overview about the available SIM cards, their assigned modems and the current state. Once a SIM card has been inserted, assigned to a modem and successfully unlocked the card should remain in state `ready` and the network registration status should have turned to registered. You may update the state in order to restart PIN unlocking and trigger another network registration attempt.

Configuration

A SIM card is generally assigned to a default modem but this may switch, for instance if you set up two WWAN interfaces with one modem but different SIM cards. Close attention has to be paid when other services (such as SMS or Voice) are operating on that modem as a SIM switch will affect their operation.



You can configure the following settings:

Default modem	The default modem assigned to this SIM card.
Service type	The default service type to be used with this SIM card. Remember that the link manager might change this in case of different settings. The default is to use automatic, in areas with interfering base stations you can force a specific type (e.g. 3G-only) in order to prevent any flapping between the stations around.
PIN protection	Depending on the used card, it can be necessary to unlock the SIM with a PIN code. Please check the account details associated with your SIM whether PIN protection is enabled.
PIN code	The PIN code for unlocking the SIM card
SMS gateway	The service center number for sending short messages. It is generally retrieved automatically from your SIM card but you may define a fix number here.

Network

This page provides information about the current network status, signal strength and the Local Area Identifier (LAI) to which the modem has been registered. An LAI is a globally unique number that identifies the country, network provider and LAC of any given location area. It can be used to force the modem to register to a particular mobile cell in case of competing stations.

You may further initate mobile network scan for getting networks in range and assign a LAI manually.

Query

This page allows you to send a Hayes AT command to the modem. Besides the 3GPP-conforming AT command set further modem-specific commands can be applied which can be provided on demand. Some modems also support to run Unstructured Supplementary Service Data (USSD) requests, e.g. for querying the available balance of a pre-paid account.

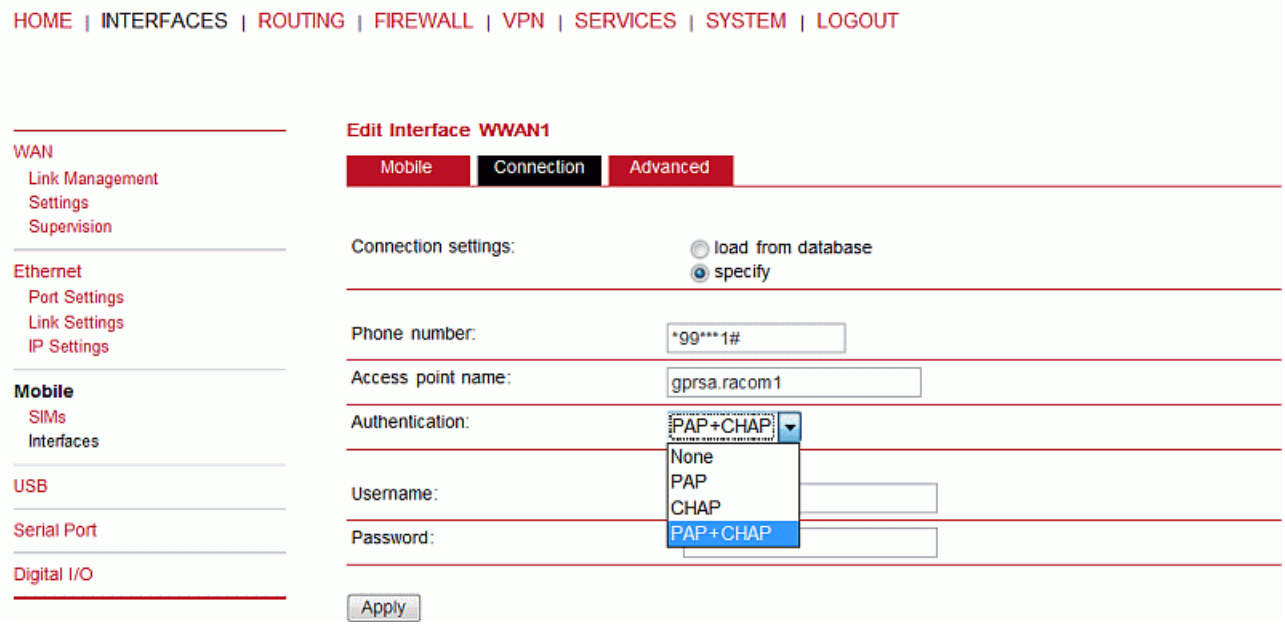
WWAN Interfaces

This page can be used to manage your WWAN interfaces. The resulting link will pop up automatically on the WAN Link Management page once an interface has been added. The Mobile LED will be blinking during the connection establishment process and goes on as soon as the connection is up. Refer to the troubleshooting section or log files in case the connection did not come up.

The following mobile settings are required:

Modem	The modem to be used for this WWAN interface
SIM	The SIM card to be used for this WWAN interface
Service type	The required service type

Please note that these settings supersede the general SIM based settings as soon as the link is being dialed.



Generally, the connection settings are derived automatically as soon as the modem has registered and the network provider has been found in our database. Otherwise, it will be required to configure the following settings:

Phone number	The phone number to be dialed, for 3G+ connections this commonly refers to be *99***1#. For circuit switched 2G connections you can enter the fixed phone number to be dialed in international format (e.g. +420xx).
Access point name	The access point name (APN) being used
Authentication	The authentication scheme being used, if required this can be PAP or/and CHAP
Username	The username used for authentication
Password	The password used for authentication

Furtheron, you may configure the following advanced settings:

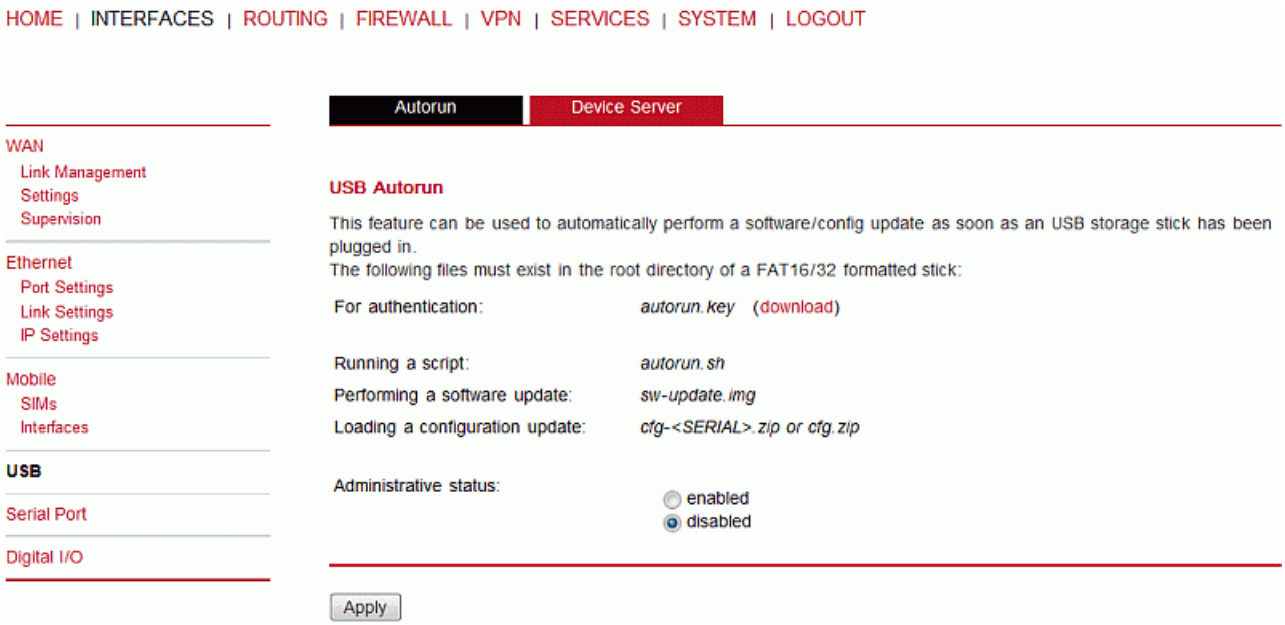
Required signal strength	The mimimum required signal strength before the connection
IP header compression	Enable or disable Van Jacobson TCP/IP Header Compression for PPP-based connections. This feature will improve TCP/IP performance over slow serial links. Has to be supported by your provider.
Software compression	Enable or disable data compression for PPP-based connections. Software compression reduces the size of packets to improve throughput. Has to be supported by your provider.
Client address	Specify a fixed client IP address on the mobile interface.
MTU	The Maximum Transmission Unit represents the largest amount of data that can be transmitted within one IP packet and can be defined for any WAN interface.

7.2.4. 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. Following files must exist in the root directory of a FAT16/32 formatted stick:

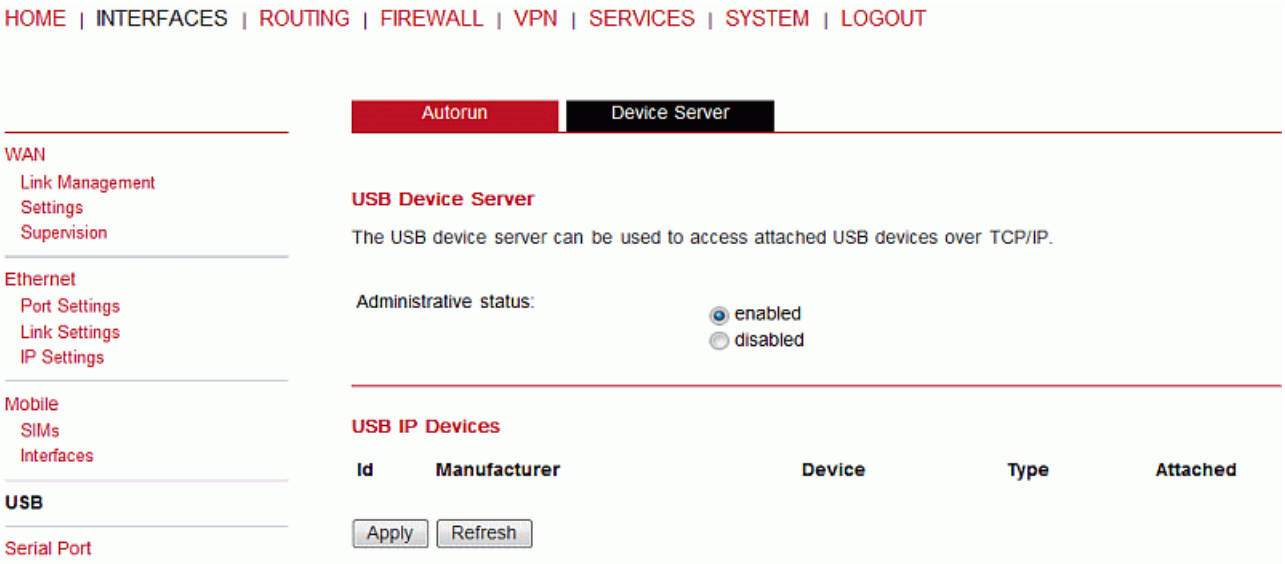
- For authentication: `autorun.key`
- For a software update: `sw-update.img`
- For a configuration update: `cfg-<SERIALNO>.zip` or `cfg.zip`



Enable auto run feature:	Enable or disable auto run feature.

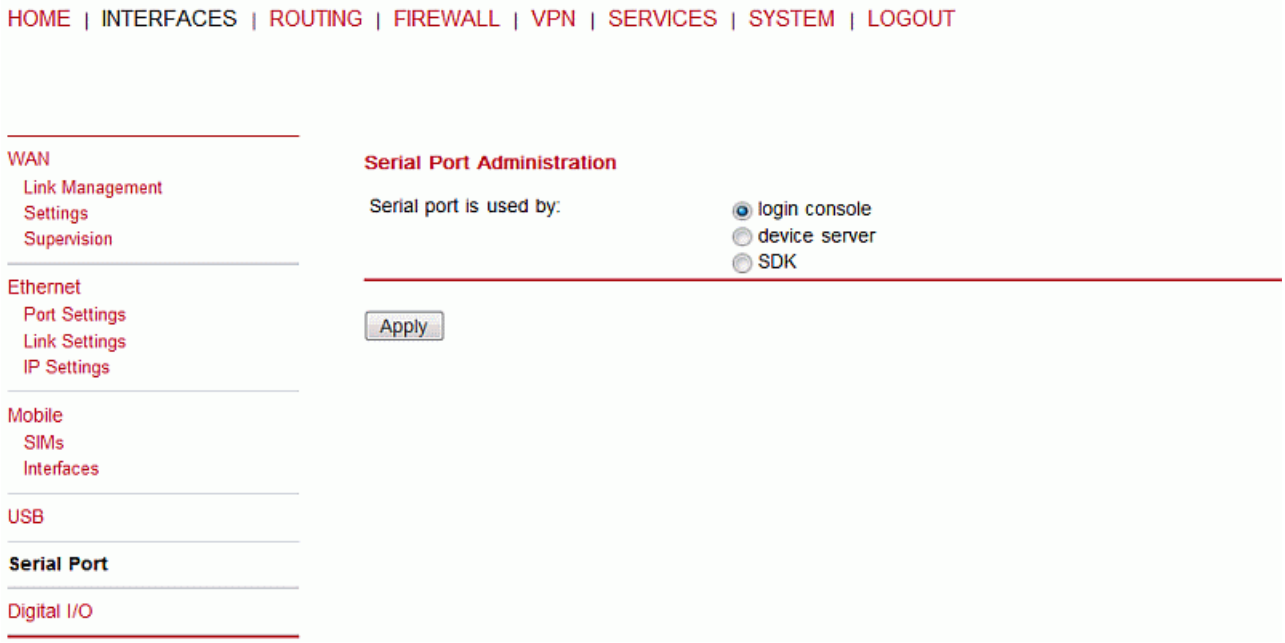
The `autorun.key` file must hold valid access keys to perform any actions when the storage device is plugged in. The keys are made up of your admin password. They can be generated and downloaded. You may also define multiple keys in this file (line-after-line) in case your admin password differs if applied to multiple M!DGE routers.

Device Server



As soon as the USB device server has been enabled you can refresh the discovered USB devices plugged in and attach them to the USB/IP server. Enabled device can now be exported to a remote host. You will need an additional driver on the remote site and further installation instructions which we can provide on demand.

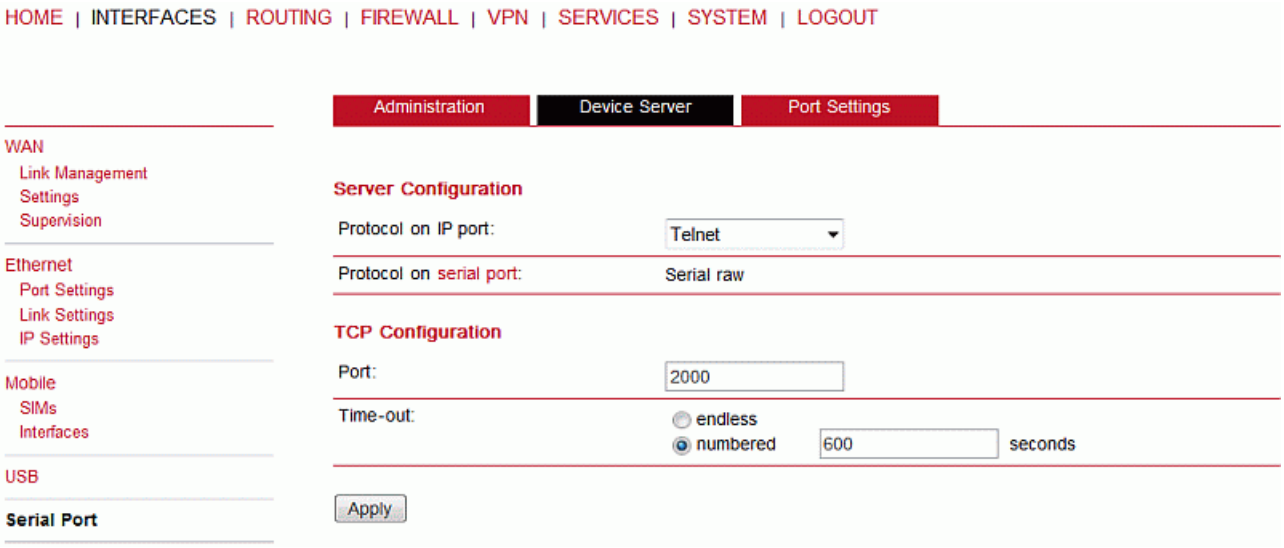
7.2.5. Serial Port



Three possibilities are availble:

- login console for enabling serial console (serial console is mentioned especially for maintenance reasons in case that the web interface should not be used from any reason)
- device server or
- SDK (for more about this possibility see chapter SDK)

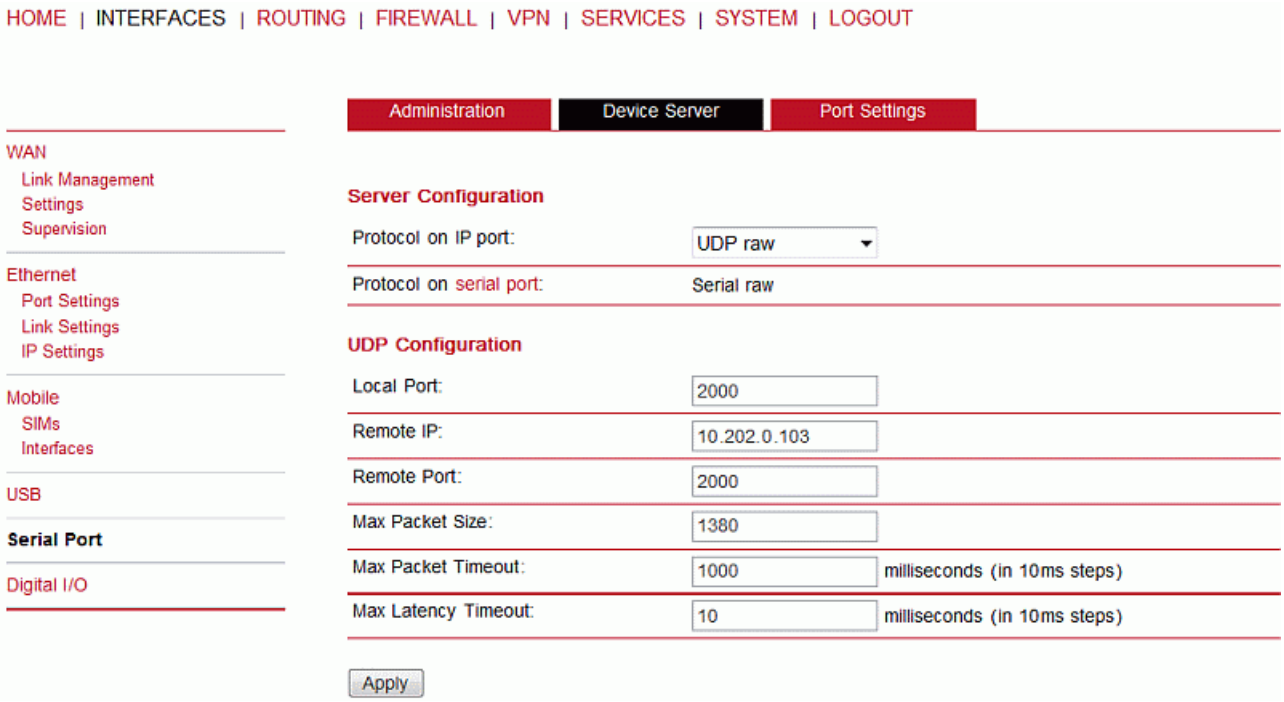
Device Server



Server status:	Enable or disable serial device server.
Protocol on IP port:	“Telnet”, “UDP raw” or “TCP raw”
Protocol on serial port:	The protocol implicitly defined on the serial port.

TCP or Telnet Configuration

Port:	The TCP port that is used by this application.
Time-out:	Time-out:



UDP Configuration

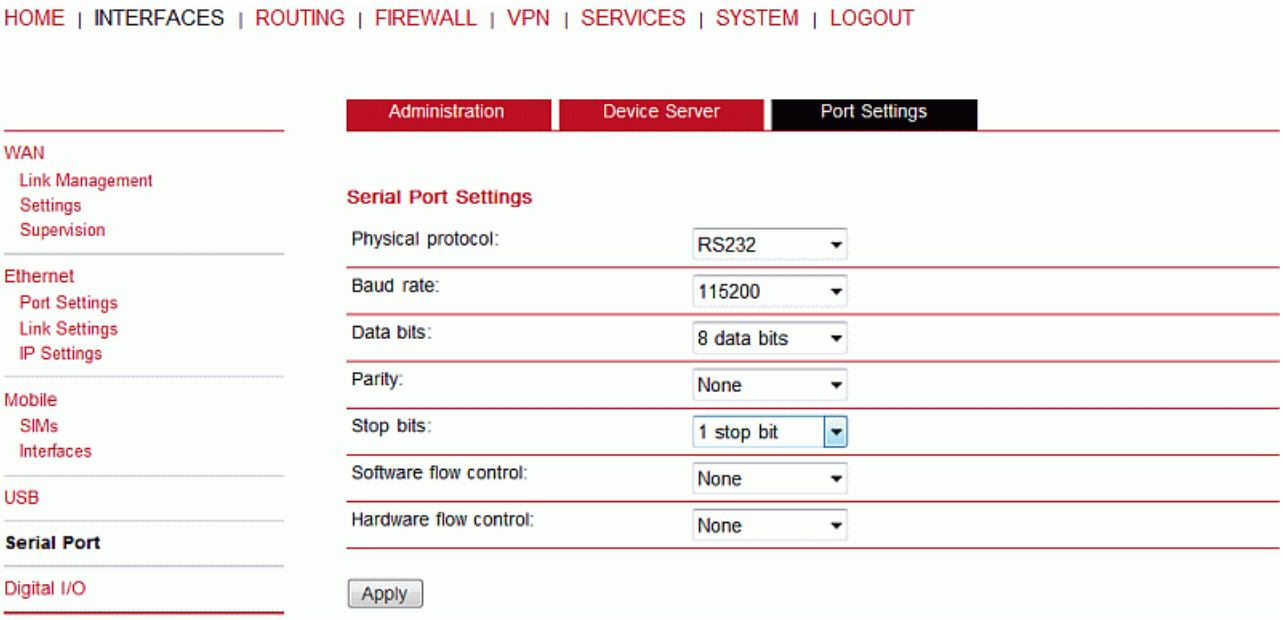
Local Port:	Local UDP port

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

Conditions of sending a UDP packet to the Remote IP address Remote port:

- The serial data are comming with longer inter packet deley than Max Latency Timeout packet will be closed and send out to specified Remote IP address.
- When the inter packet delay is shorter than Max Latency Timeout all packets will be collected to a buffer for Max Packet Timeout. After that time the buffer will be send out to the the Remote IP address fragmented according the Max Packet Size (a burst of several packets in case that the content of the buffer is biggre than Max Packet Size.

Serial Port Setting



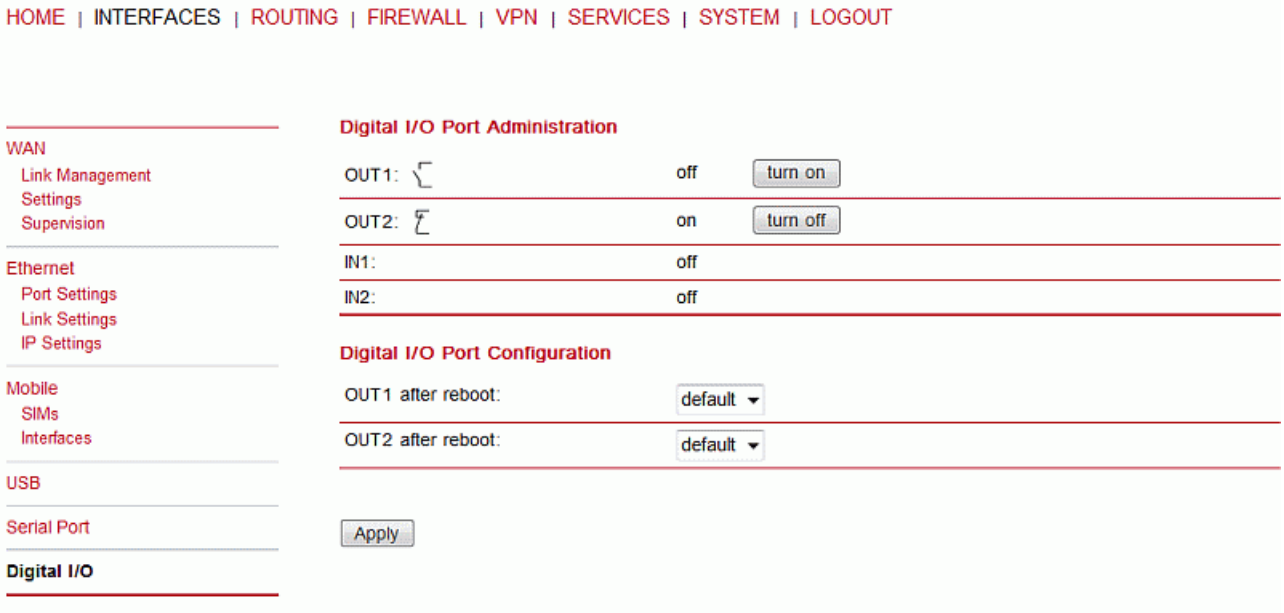
Physical protocol:	Only RS232 is supported.
Baud rate:	Specifies the baud rate of the COM port.
Data bits:	Specifies the number of data bits contained in each frame.
Parity:	Specifies the parity used with every frame that is transmitted or received.
Stop bits:	Specifies the number of stop bits used to indicate the end of a 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: While 3 wired conection is used with M!DGE hardware flow control is not available.

7.2.6. Digital I/O

The Digital I/O page displays the current status of the I/O ports and can be used to turn output ports on or off.

You can apply the following settings:



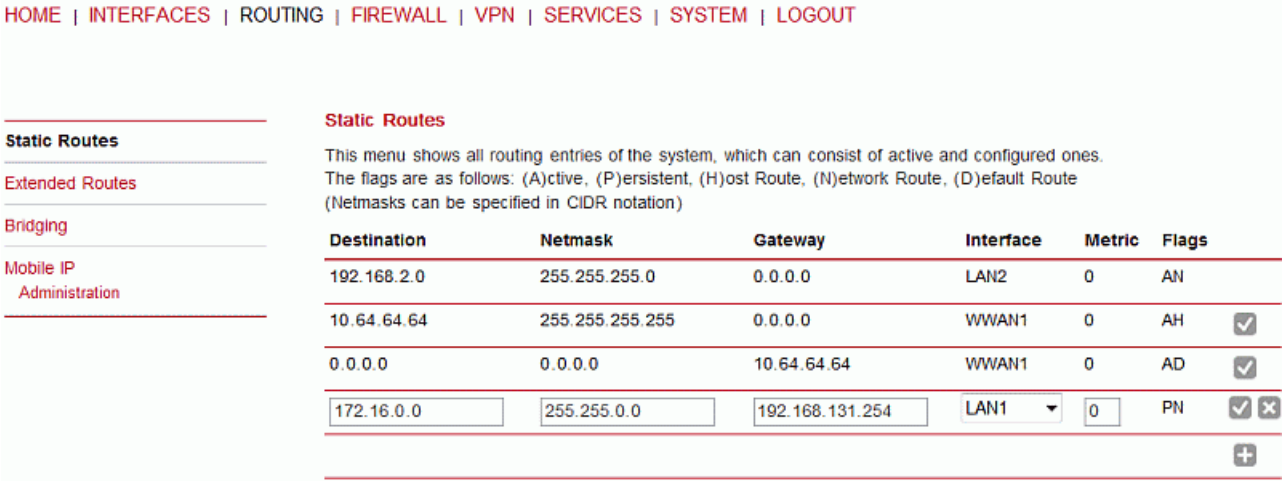
Besides on and off you may keep the status after reboot at default which corresponds to the default state as the hardware will be initialised at power-up.

The digital inputs and outputs can also be monitored and controlled by SDK scripts.

7.3. ROUTING

7.3.1. Static Routes

This menu shows all routing entries of the system, which can consist of active and configured ones. (Netmasks can be specified in CIDR notation, i.e. **24** expands to `255.255.255.0`).



Destination: Destination network or host provided by IP addresses in dotted decimal.

Netmask: Subnet mask which forms, in combination with the destination, the network to be addressed. A single host can be specified by a netmask of `255.255.255.255`, a default route corresponds to `0.0.0.0`.

Gateway: The next hop which operates as gateway for this network (can be omitted on peer-to-peer links).

Interface: Network interface on which a packet will be transmitted in order to reach the gateway or network behind.

Metric: The routing metric of the interface (default 0). The routing metric is used by routing protocols, higher metrics have the effect of making a route less favourable; metrics are counted as additional costs to the destination network.

Flags: (A)ctive, (P)ersistent, (H)ost Route, (N)etwork Route, (D)efault Route

The flags obtain the following meanings:

Active: The route is considered active, it might be inactive if the interface for this route is not yet up

Persistent: The route is persistent, which means it is a configured route, otherwise it corresponds to an interface route

Host: The route is a host route, typically the netmask is set to 255.255.255.255.

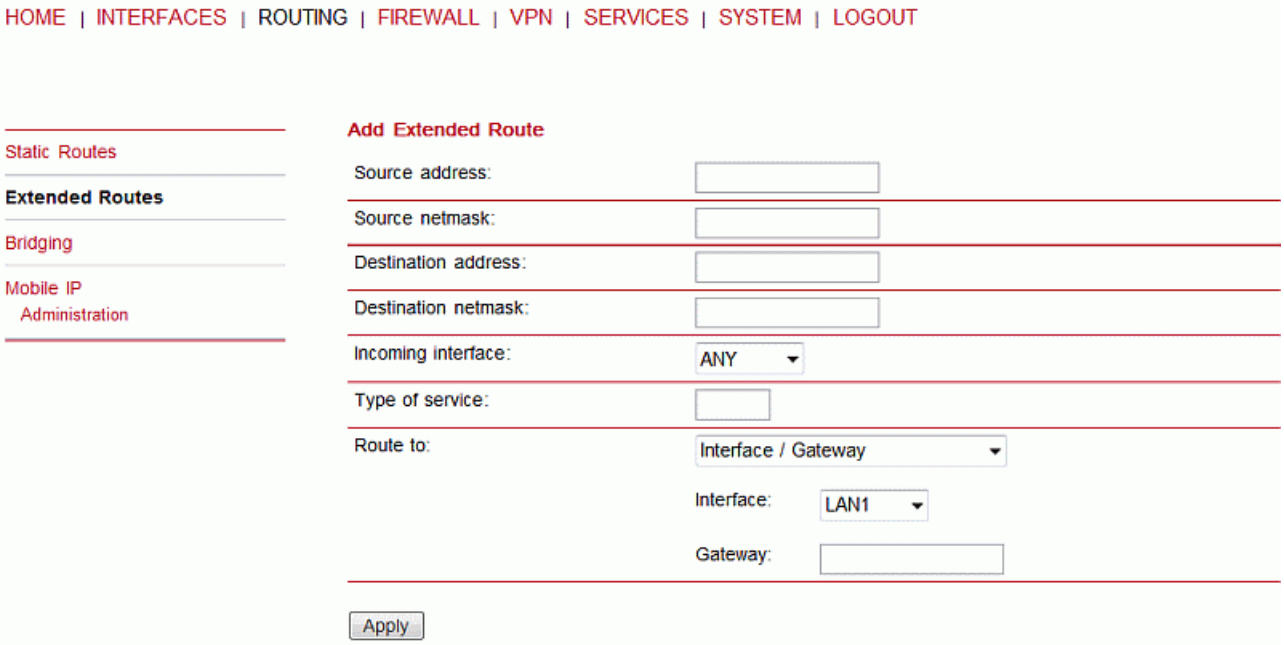
Network: The route is a network route, consisting of an address and net-mask which forms the subnet to be addressed

Default Route	The route is a default route, address and netmask are set to 0.0.0.0, thus matching any packet

7.3.2. Extended Routing

Extended routes can be used to perform policy-based routing, they generally precede static routes.

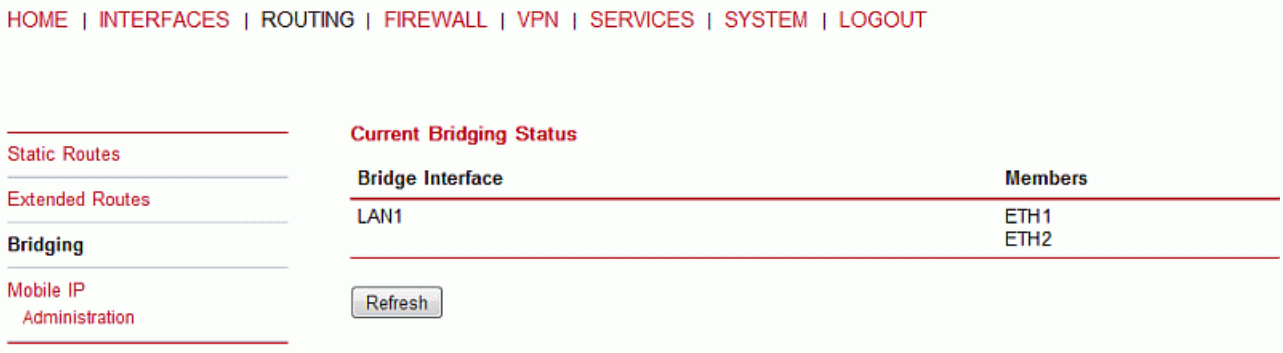
Extended routes can be made up not only of a destination address/netmask but also a source address/netmask, incoming interface and the type of service (TOS) of packets.



Source address	The source address of a packet
Source netmask	The source address of a packet
Destination address	The destination address of a packet
Destination netmask	The destination address of a packet
Incoming interface	The interface on which the packet enters the system
Type of service	The TOS value within the header of the packet
Route to	Specifies the target interface or gateway to where the packet should get routed to.

7.3.3. Bridging

Information about bridge status.



7.3.4. Mobile IP

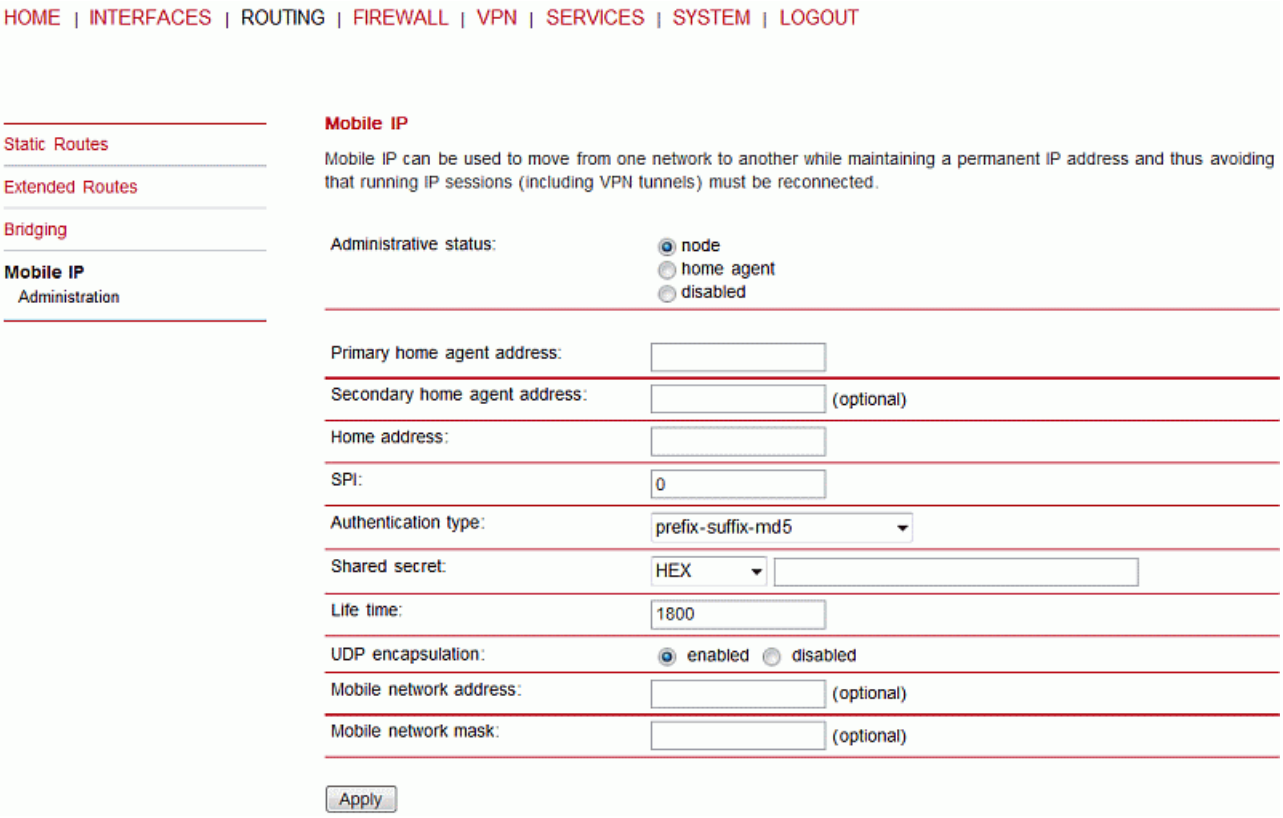
Mobile IP (MIP) can be used to enable a seamless switch between different WAN technologies.

Note

A valid license key is required for running Mobile IP.

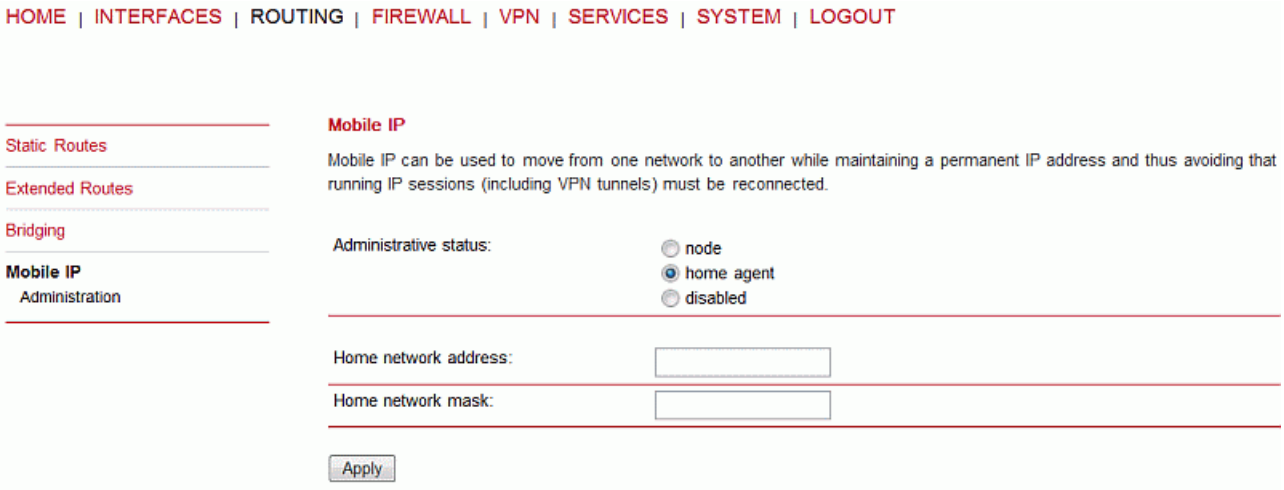
It boasts with very small outages during switchover while keeping all IP sessions alive which is being accomplished by communicating with the static public IP address of a home agent which will encapsulate the packets and send them further to the router. Switching works by telling the home agent that the hotlink address has changed, the agent will then re-route (that means encapsulate the packets with the new target address) the packets transparently down to the box.

Our implementation supports RFC 3344, 5177, 3024 and 3519 and interoperability with Cisco has been verified. However, M!DGE routers can run as node and home agent which makes them able to replace expensive kits in the backbone for smaller scenarios.



If MIP is run as node, the following settings can be configured:

Primary home agent address:	The address of the primary home agent
Secondary home agent address:	The address of the secondary (fallback) home agent
Home address:	The permanent home address of the node which can be used to address the box
SPI:	The Security Parameter Index (SPI) identifying the security context between a pair of nodes (represented in 8 chars hex)
Authentication type:	The used authentication, can be prefix-suffix-md5 or hmacmd5
Shared secret:	The shared secret used for authentication, can be a 128-bit hex or ASCII string
Life time:	The lifetime of security associations
UDP encapsulation:	Specifies whether UDP encapsulation shall be used
Mobile network address:	Optionally specifies a subnet which should be routed to the box
Mobile network mask:	The netmask for the optional routed network



If MIP is run as home agent, you will have to set up a home address and netmask first and configure various nodes afterwards which are made up of the following settings:

Home network address:	The home address of the network
Home network mask:	The mask for the home network.

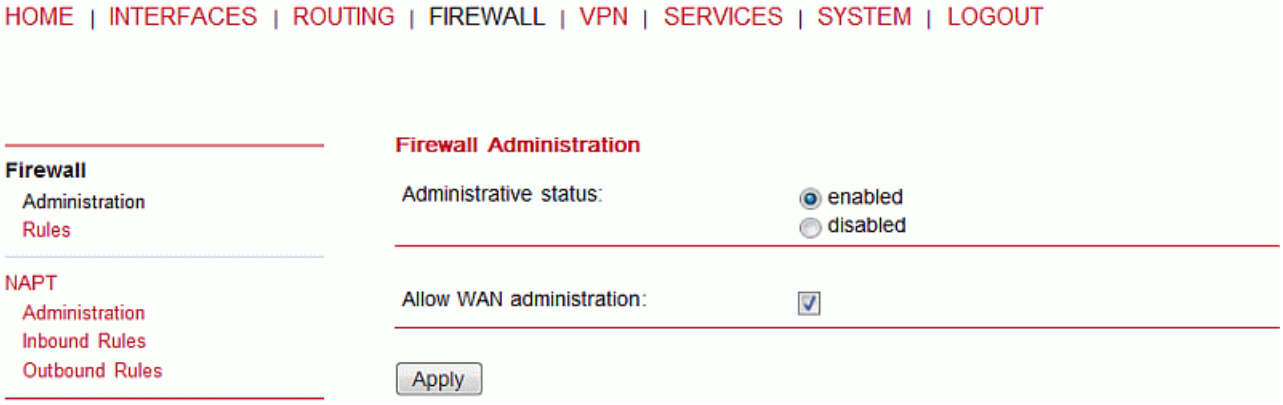
7.4. FIREWALL

This router uses Linux's netfilter/iptables firewall framework (see http://www.netfilter.org for more information). It is set up of a range of rules which control each packet's permission to pass the router. Packets, not matching any of the rules, are allowed by default.

7.4.1. Firewall

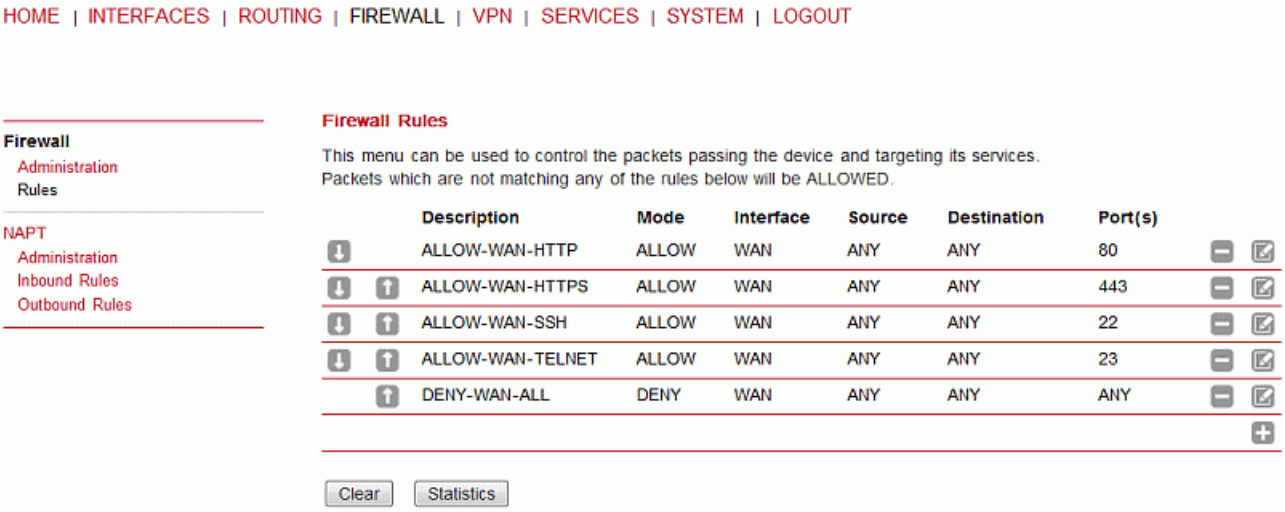
Administration

The adminstration page can be used to enable and disable firewalling. When turning it on, a shortcut can be used to generate a predefined set of rules which allow administration (over HTTP, HTTPS, SSH or TELNET) by default but block any other packets coming from the WAN interface.



Administrative status: Enable or disable packet filtering.

Allow WAN administration: This option will predefine the rules for services on the WAN link as follows:



Statistics

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

Firewall
Administration
Rules

NAPT
Administration
Inbound Rules
Outbound Rules

Firewall Matching Statistics

Packets	Description	Mode	Interface	Source	Destination	Port(s)
0	ALLOW-WAN-HTTP	ALLOW	WAN	ANY	ANY	80
6	ALLOW-WAN-HTTPS	ALLOW	WAN	ANY	ANY	443
3	ALLOW-WAN-SSH	ALLOW	WAN	ANY	ANY	22
0	ALLOW-WAN-TELNET	ALLOW	WAN	ANY	ANY	23
28	DENY-WAN-ALL	DENY	WAN	ANY	ANY	ANY
1767	ALL OTHER	ALLOW				

Back Refresh

Statistics presents numbers of packets for the individual rules.

Add Firewall Rule

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

Firewall
Administration
Rules

NAPT
Administration
Inbound Rules
Outbound Rules

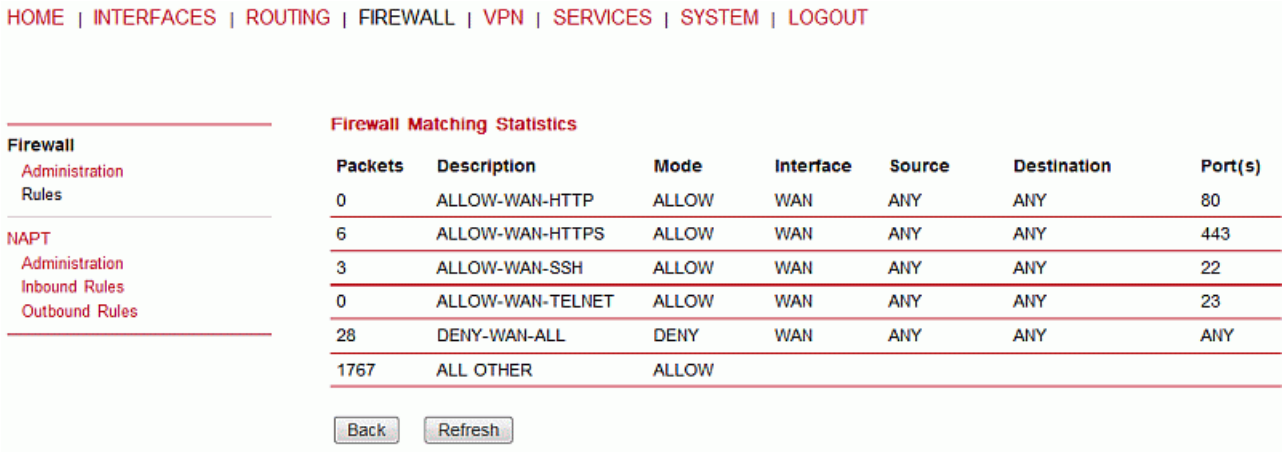
Add Firewall Rule

Description: SCADA address
Mode: ALLOW
Incoming interface: LAN1
Source: ANY specify
Address: 192.168.141.222
Netmask: 255.255.255.255
Destination: ANY LOCAL specify
Protocol: Any

Add rule Cancel

Description:	A meaningful description about the purpose of this rule.
Mode:	Whether the packets of this rule should be allowed or denied.
Incoming interface:	Interface on which matching packets are received.
Source:	Source address of matching packets, can be any or a source network/host.
Destination:	The destination address of matching packets, can be any, local (addressed to the system itself) or specified by an address/network.
Protocol:	Used IP protocol of matching packets.
Destination port(s):	Destination port of matching packets. You can specify a single port or a range of ports here. Note that protocol must be set to UDP/TCP when using port filters.

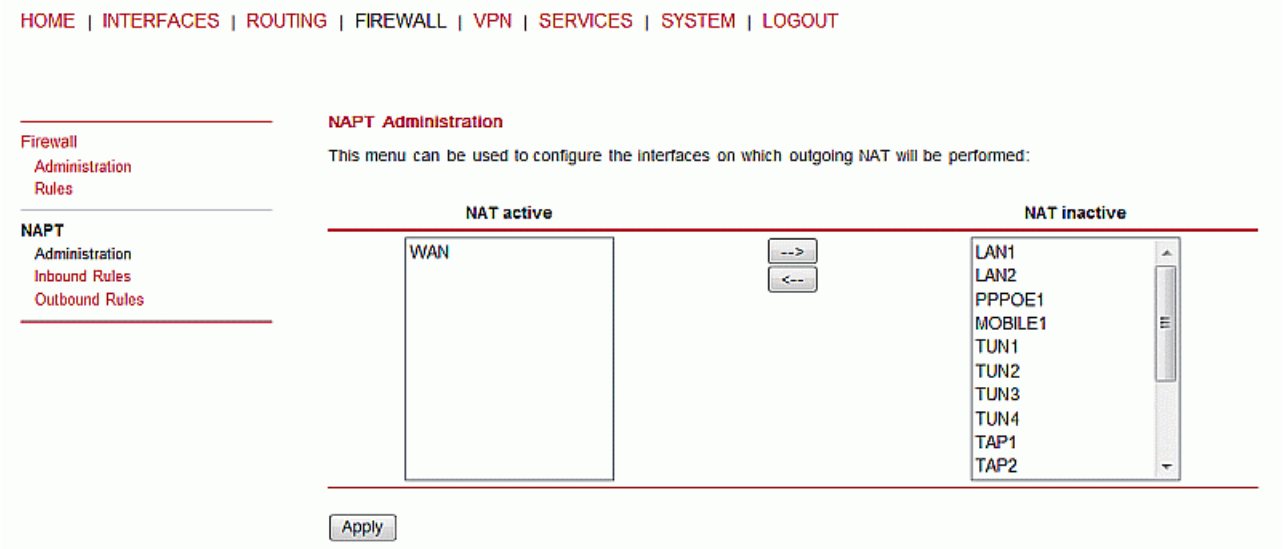
7.4.2. NAPT



This page allows setting of the options for Network Address and Port Translation (NAPT). NAPT translates IP addresses or TCP/UDP ports and enables communication between hosts on a private network and hosts on a public network. It generally allows a single public IP address to be used by many hosts from the private LAN network.

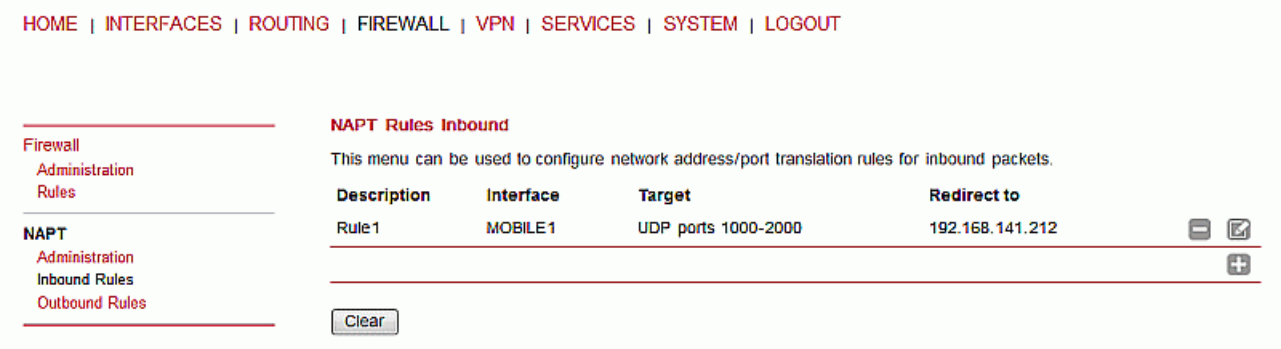
Administration

This menu can be used to configure the interfaces on which outgoing NAT will be performed.



Inbound Rules

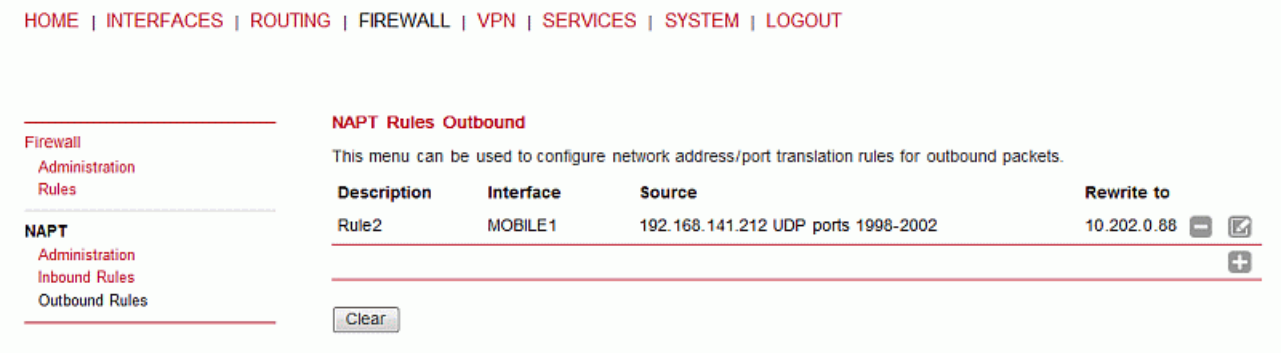
Inbound rules can be used to modify the target section of IP packets and, for instance, forward a service or port to an internal host. By doing so, they will expose the service and make it reachable e.g. from the Internet. You may also establish 1:1 NAT to a complete host.



Description:	A meaningful description of this rule
Incoming interface:	Interface from which matching packets are received
Target address:	Destination address of matching packets (optional)
Protocol:	Used protocol of matching packets
Ports:	Used UDP/TCP port of matching packets
Redirect to:	Address to which matching packets shall be redirected
Redirect port:	Port to which matching packets will be targeted

Outbound Rules

Outbound rules will modify the source section of IP packets and can be for instance used for 1:1 NAT.



Description:	A meaningful description of this rule
Incoming interface:	Outgoing interface on which matching packets are leaving the router
Source address:	Source address of matching packets (optional)
Protocol:	Used protocol of matching packets
Ports:	Used UDP/TCP port of matching packets
Rewrite source address:	Address to which the source address of matching packets shall be rewritten
Rewrite source port:	Port to which the source port of matching packets shall be rewritten

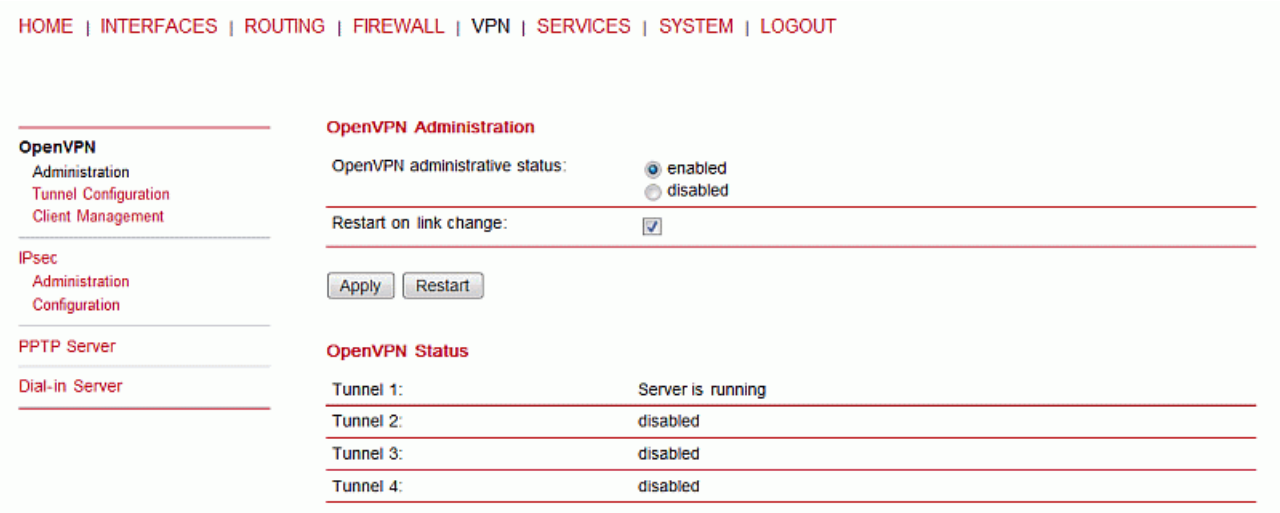
7.5. VPN

7.5.1. OpenVPN

Administration

OpenVPN administrative status: Enable or disable OpenVPN.

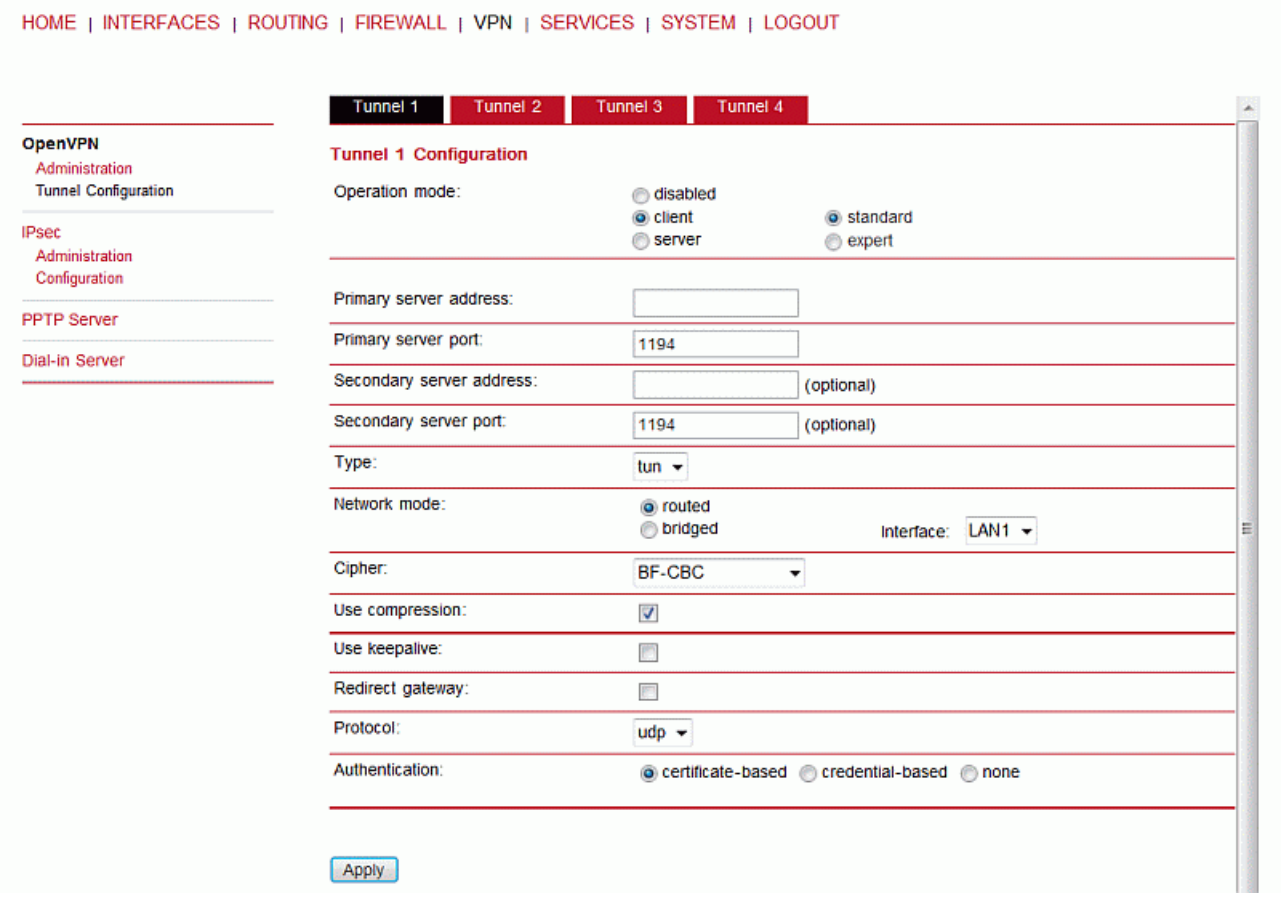
If enabled, OpenVPN client configurations will be started whenever a WAN link has been established. Server configurations will be started immediately after boot up.



Tunnel Configuration

The router supports a single server tunnel and up to 4 client tunnels. You can specify tunnel parameters in standard configuration or upload an expert mode file which has been created in advance. Refer to section ‘OpenVPN Client Management’ to learn more about how to manage clients and generate the files.

Operation mode: Choose client or server mode for this tunnel



Client Mode

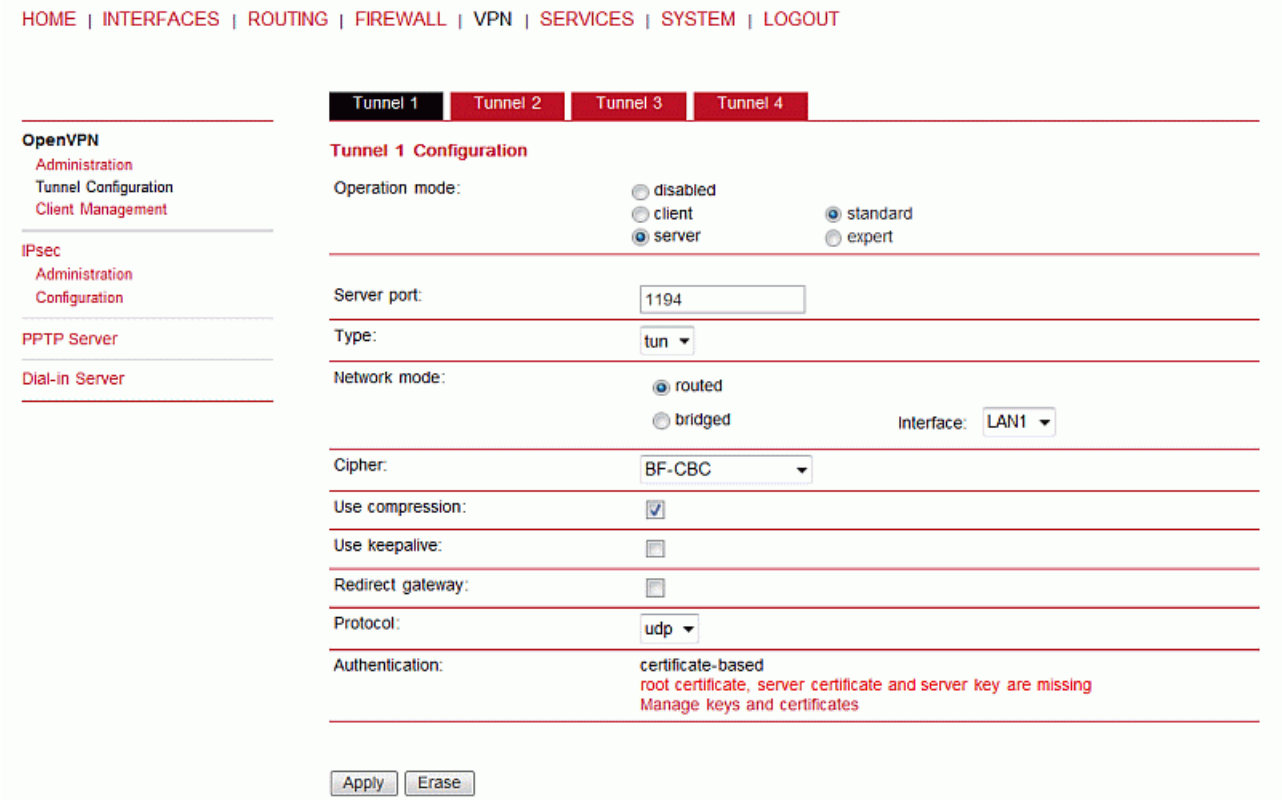
Primary server address:	Primary OpenVPN server address (for clients)
Primary server port:	OpenVPN server port (1194 by default)
Secondary server address:	Secondary OpenVPN server address (optional, for clients) to switch over in case the primary address cannot be reached
Secondary server port:	Secondary OpenVPN server port (optional, for clients)
Type:	The VPN device type which can be either TUN (typically used for routed connections) or TAP (used for bridged networks)
Network mode:	Defines how the packets should be forwarded, can be routed or bridged from or to a particular interface.
Cipher:	Required cipher mechanism used for encryption
Use compression:	Enable or disable OpenVPN compression
Use keep alive:	Can be used to send a periodic keep alive packet in order to keep the tunnel up despite inactivity
Redirect gateway:	By redirecting the gateway, all packets will be directed to the VPN tunnel. Please ensure that essential services (such as DNS or NTP

servers) can be reached at the network behind the tunnel. If in doubt, create an extra static route pointing to the correct interface.

Protocol: The OpenVPN tunnel protocol to be used

Authentication: You can choose between no authentication, credential-based (where you have to specify a username and password) and based on keys and certificates. Note that keys/certificates have to be created under SYSTEM -> Keys/Certificates. You may also upload files which you have generated on your host system.

Server Mode



A server tunnel typically requires the following files:

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

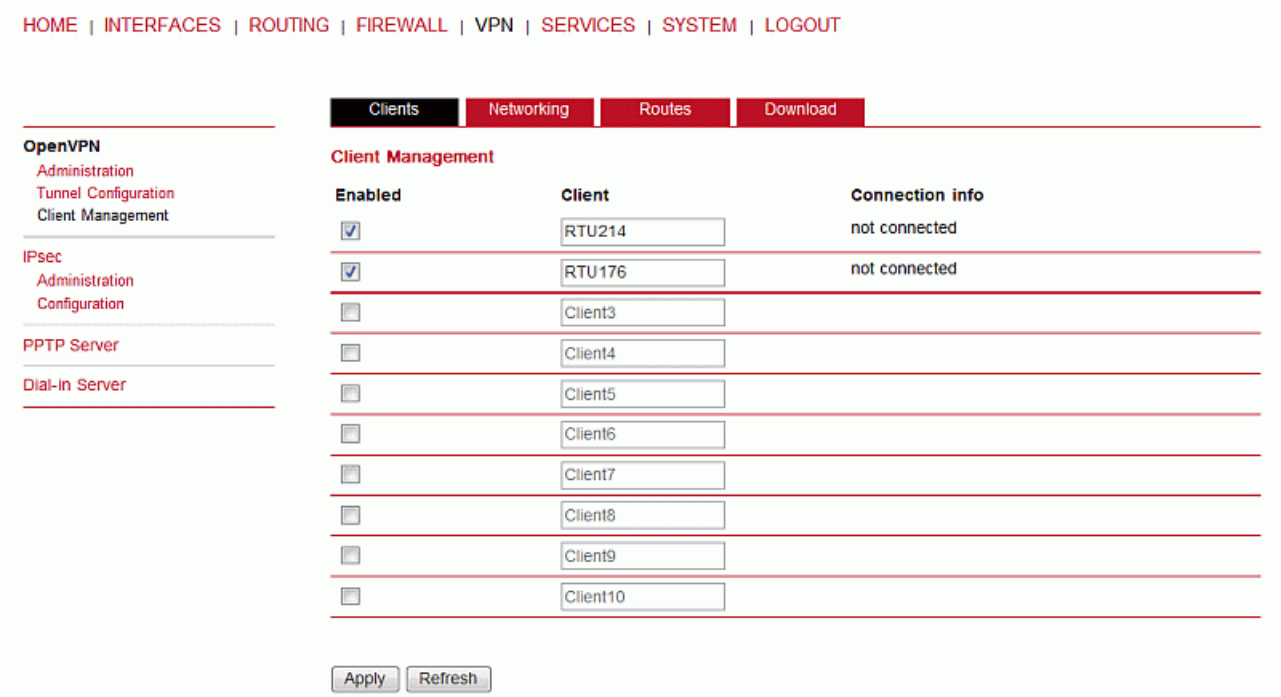
Note

OpenVPN tunnels require a correct system time. Please ensure that all NTP servers are reachable. When using host names a working DNS server is required as well.

Client Management

Once you have successfully set up an OpenVPN server tunnel you can manage and enable clients which can connect to your service, the client's page also informs you about currently connected clients. Further, you can specify a fixed tunnel endpoint address of each client and its network behind. You can also define routes to be pushed to each client if you want to redirect traffic for particular networks towards the server.

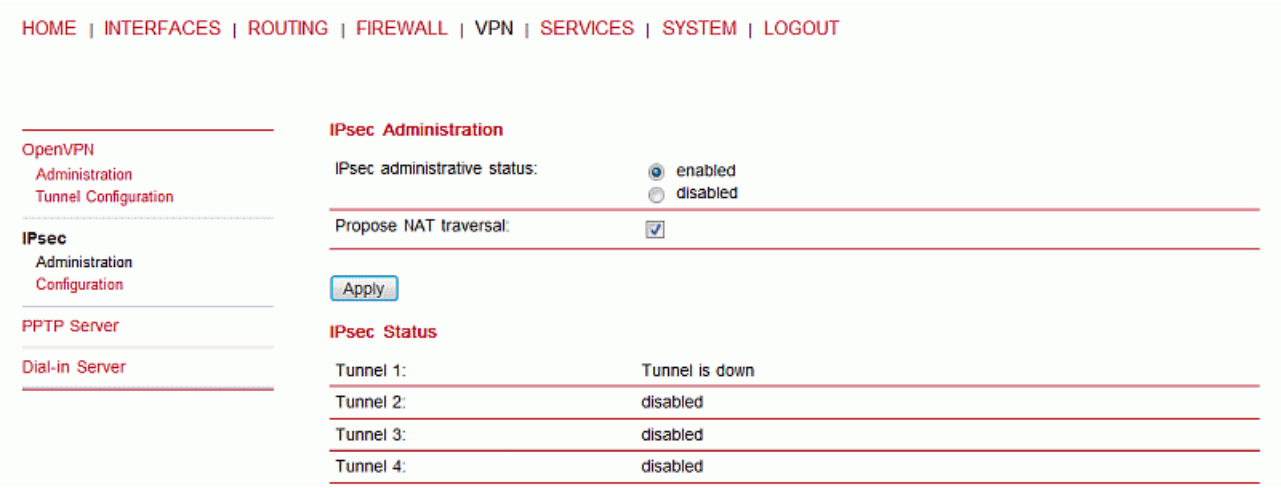
Finally, you can generate and download all expert mode files to easily populate each client.



7.5.2. IPsec

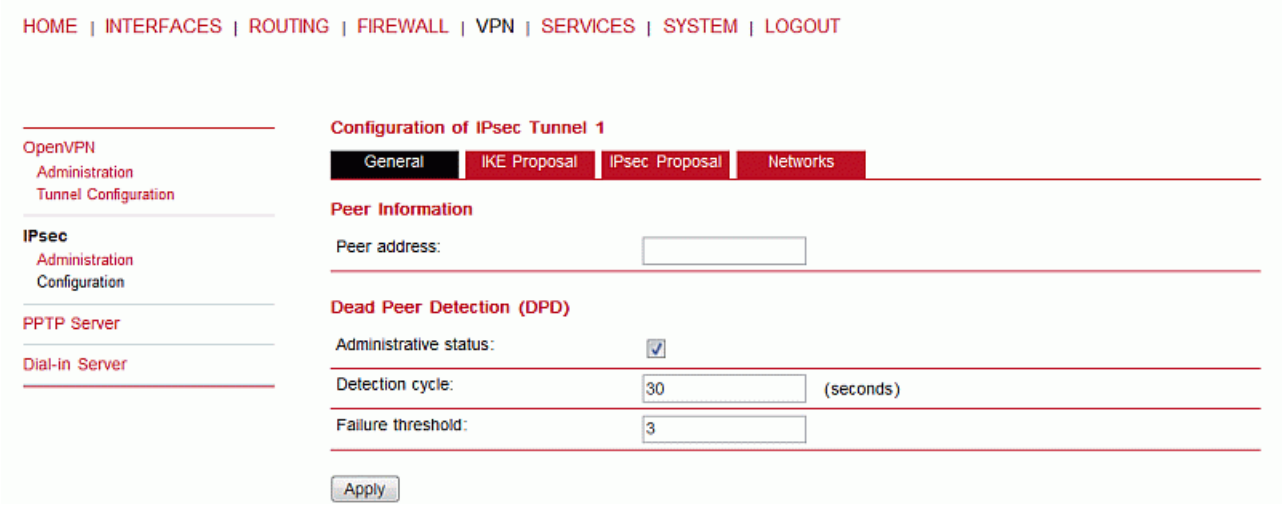
IPsec is primarily used for securing Internet communications by authenticating and/or encrypting IP packets within a data stream. IPsec includes various cryptographic protocols and ciphers for key exchange and data encryption and can be seen as one of the strongest VPN technologies in terms of security.

Administration



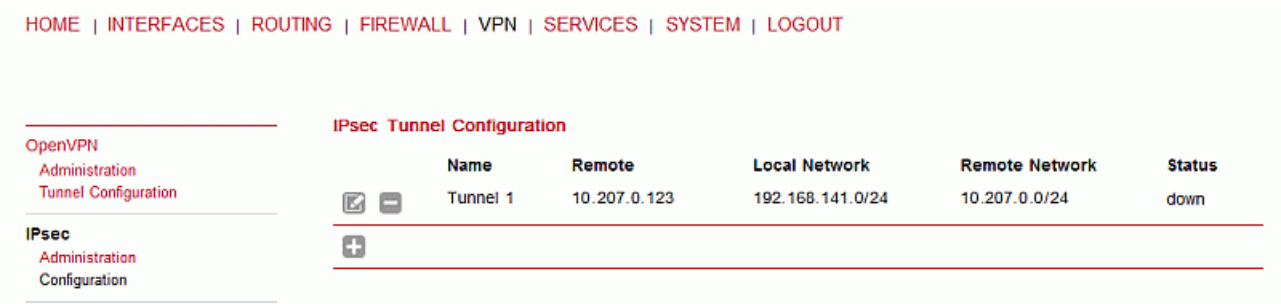
IPsec administrative status:	Enable or disable IPsec
Propose NAT Traversal:	NAT-Traversal is mainly used for connections which traverse a path where a router modifies the IP address/port of packets

Configuration



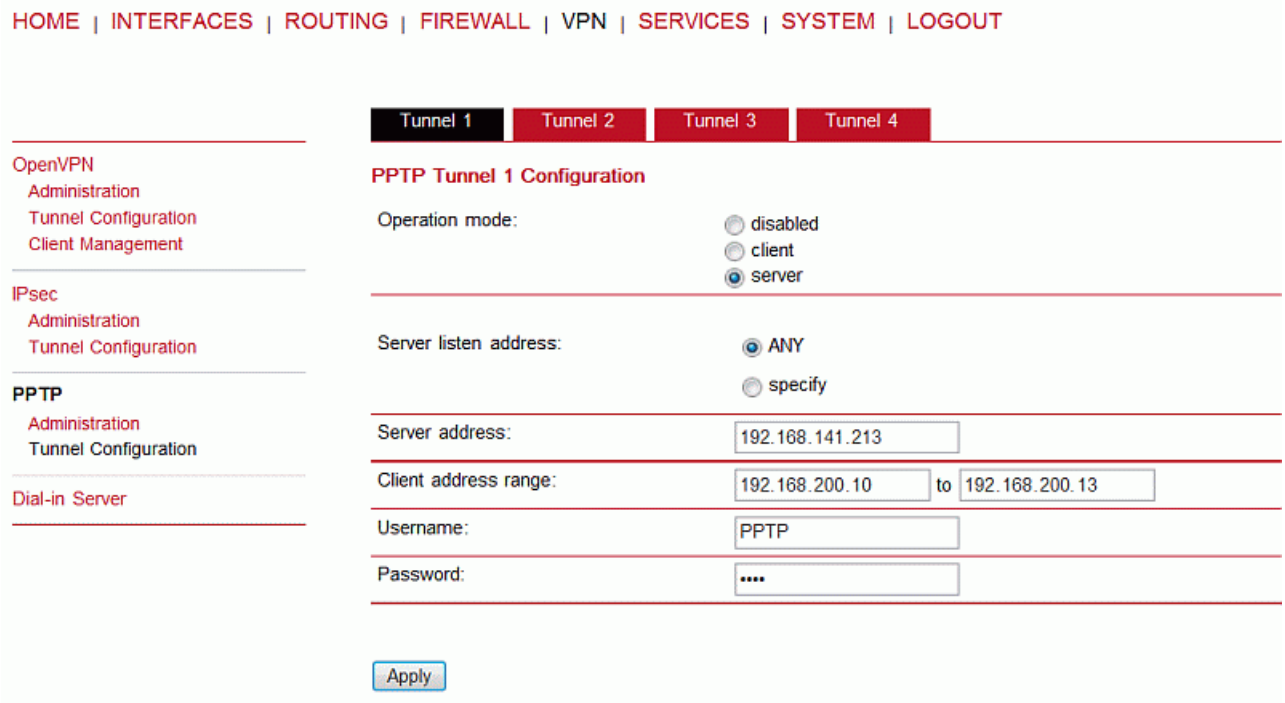
Remote server address:	IP address or host name of IPsec peer / responder / server
Remote LAN address:	The remote private network, provided by an IP address in dotted decimal notation
Remote LAN subnet mask:	The remote private network, provided by a subnet mask in dotted decimal notation
NAT Traversal:	Enable or disable NAT-Traversal. NAT-Traversal is mainly used for connections which traverse a path where a router modifies the IP address/port of packets. It encapsulates packets in UDP and therefore requires a slight overhead which has to be taken into account when running over small sized MTU interfaces
Preshared Key (PSK):	The pre-shared key (PSK)
IKE mode:	Choose a negotiation mode. The default is main mode (identity-protection). Aggressive mode has to be used when dealing with dynamic endpoint addresses. It is however referred to be less secure compared to main mode as it reveals your identity to an eavesdropper.
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 heavily increases security as PFS avoids penetration of the key-exchange protocol and prevents compromising the 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. DPD will detect any broken IPSec connections, in particular the ISAKMP tunnel, and refresh the corresponding SAs (Security Associations) and SPIs (Security Payload Identifier) for a faster re-establishment of the tunnel
Detection cycle [sec]:	Set the delay (in seconds) between Dead Peer Detection (RFC 3706) keep alives (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 (The router will then try to re-establish a dead connection automatically)



7.5.3. PPTP

Point-to-Point Tunnelling Protocol (PPTP) is a method for implementing virtual private networks between two hosts. PPTP is easy to configure and widely deployed amongst Microsoft Dial-up networking servers. However, it is nowadays considered insecure. When setting up a PPTP tunnel, you would need to choose between server or client.



A client tunnel requires the following paramters to be set:

Server address: The address of the remote server

Username: The username used for authentication

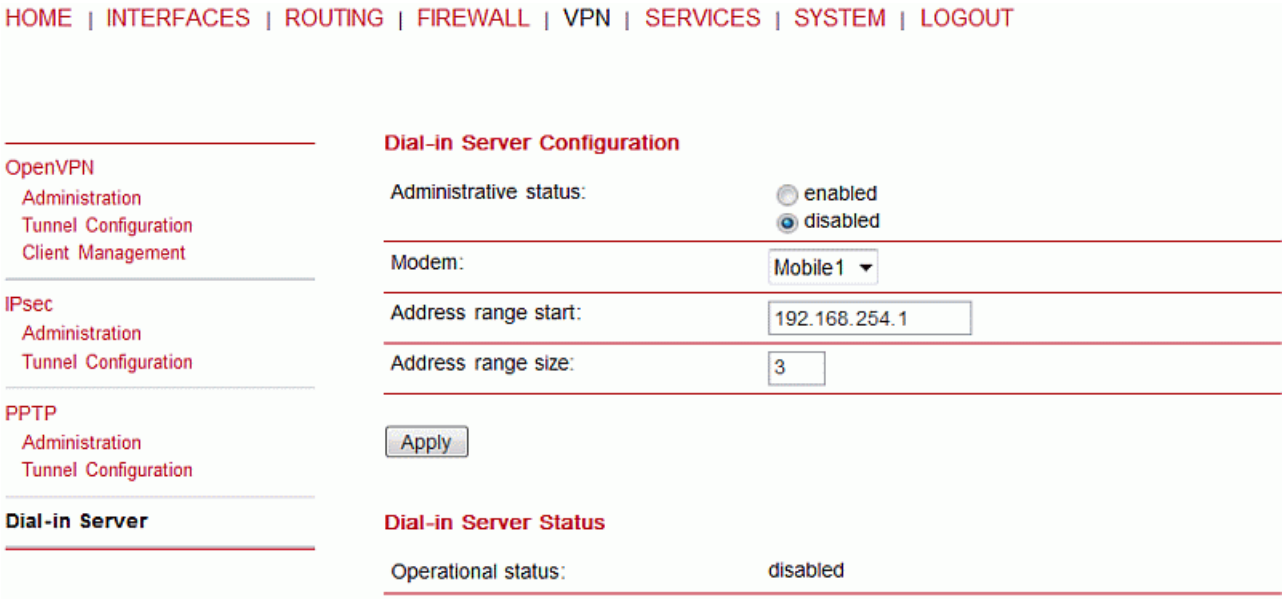
Password: The password used for authentication

7.5.4. Dial-in Server

On this page you can configure the Dial-in server in order to establish a data connection over GSM calls. Thus, one would generally apply a required service type of 2G-only, so that the modem registers to GSM only. Naturally, a concurrent use of mobile Dial-Out and Dial-In connection is not possible.

Note

The Dial-in Server is not supported by the M!DGE/MG102i LTE hardware.



Administrative status	Enabled/disabled - incoming call shall be /shall not be answered
Modem	Specifies the modem on which calls can come in
Address range start:	Start address of range of clients connecting to the dial-in server
Address range size:	Number of client addresses connecting to the server
Dial-in operational status:	Shows the actual status of the connection

Besides the admin account you can configure further users in the user accounts section. which shall be allowed to dial-in. Please note that Dial-In connections are generally discouraged. As they are implemented as GSM voice calls, they suffer from unreliability and poor bandwidth.

7.6. SERVICES

7.6.1. SDK

Racom routers are shipping with a Software Development Kit (SDK) which offers a simple and fast way to implement customer-specific functions and applications. It consists of:

1. An SDK host which defines the runtime environment (a so-called sandbox), that is, controlling access to system resources (such as memory, storage and CPU) and, by doing so, catering for the right scalability.
2. An interpreter language called arena, a light-weight scripting language optimized for embedded systems, which uses a syntax similar to ANSI-C but adds support for exceptions, automatic memory management and runtime polymorphism on top of that.
3. A RACOM-specific Application Programming Interface (API), which ships with a comprehensive set of functions for accessing hardware interfaces (e.g. digital IO ports, GPS, external storage media, serial ports) but also for retrieving system status parameters, sending E-Mail or SMS messages or simply just to configure the router.

Anyone, reasonably experienced in the C language, will find an environment that is easy to dig in. However, feel free to contact us via suport@racom.eu and we will happily support you in finding a programming solution to your specific problem.

The Language

The arena scripting language offers a broad range of POSIX functions (like printf or open) and provides, together with tailor-made API functions, a simple platform for implementing any sort of applications to interconnect your favourite device or service with the router.

Here comes a short example:

```
/* This script prints short status and if the SMS section is setted properly, the status ▶
will be send even to your mobile phone :-)
 */

printf("------------------------------");
printf("\n\n");
printf(nb_status_summary(all));
printf("\n\n");
printf("------------------------------");

/* Please change the following number to your mobile phone number
 */
nb_sms_send("+420123456789", nb_status_summary(all));
```

A set of example scripts can be downloaded directly from the router, you can find a list of them in the appendix. The manual at menu SERVICES-Administration-Troubleshootings-SDK API gives a detailed introduction of the language, including a description of all available functions.

SDK API Functions

The current range of API functions can be used to implement the following features:

1. Send/Retrieve SMS
2. Send E-mail
3. Read/Write from/to serial device
4. Control digital input/output ports
5. Run TCP/UDP servers
6. Run IP/TCP/UDP clients
7. Access files of mounted media (e.g. an USB stick)
8. Retrieve status information from the system
9. Get or set configuration parameters
10. Write to syslog
11. Transfer files over HTTP/FTP
12. Get system events / Reboot system
13. Control the LEDs

The SDK API manual at menu SERVICES-Administration-Troubleshootings-SDK API provides an overview but also explains all functions in detail.

Please note that some functions require the corresponding services (e.g. E-Mail, SMS) to be properly configured prior to utilizing them in the SDK.

Let's now pay some attention to the very powerful API function nb_status. It can be used to query the router's status values in the same manner as they can be shown with the CLI. It returns a structure of variables for a specific section (a list of available sections can be obtained by running cli status -h).

By using the dump function you can figure out the content of the returned structure:

```
/* Dump current WAN status */

dump ( nb_status ("wan") );
```

The script will then generate lines like maybe these:

```
struct(17): {
  .WANLINK1_GATEWAY = string[11]: "10.64.64.64"
  .WANLINK1_STATE = string[2]: "up"
  .WANLINK1_STATE_UP_SINCE = string[19]: "2013-01-22 09:00:47"
  .WANLINK1_DIAL_ATTEMPTS = string[1]: "1"
  .WANLINK5_STATE = string[8]: "disabled"
  .WANLINK1_DIAL_SUCCESS = string[1]: "1"
  .WANLINK1_ADDRESS = string[10]: "10.204.8.0"
  .WANLINK1_SERVICE_TYPE = string[4]: "hspa"
  .WANLINK1_TYPE = string[4]: "wwan"
  .WANLINK1_DIAL_FAILURES = string[1]: "0"
  .WANLINK1_REGISTRATION_STATE = string[23]: "registeredInHomeNetwork"
  .WANLINK1_SIM = string[4]: "SIM1"
  .WANLINK1_INTERFACE = string[5]: "wwan0"
  .WANLINK3_STATE = string[8]: "disabled"
  .WANLINK1_SIGNAL_STRENGTH = string[3]: "-73"
  .WANLINK4_STATE = string[8]: "disabled"
  .WANLINK2_STATE = string[8]: "disabled"
}
```

In combination with the nb_config_set function, it is possible to start a re-configuration of any parts of the system upon status changes. You may query possible sections and parameters again with the CLI:

```
~ $ cli get -c network
Showing configuration sections (matching 'network'):

network.link
network.hostname
network.lanInterface
network.wlanInterface
network.wanInterface
network.DNS
network.DHCP
network.NTP
network.timezone
network.MSS

~ $ cli get -c network.NTP
Showing configuration sections (matching 'network.NTP'):

network.NTP.status
network.NTP.server
network.NTP.server2
network.NTP.gpstime
```

Running the CLI in interactive mode, you will be also able to step through possible configuration parameters by the help of the TAB key.

Here is an example how one might adopt those functions:

```
/* Check the current NTP server and set it to the IP address 192.168.0.2
   and enable the NTP synchronization
*/

printf ("The NTP server was previously using IP address: ");
printf (nb_config_get("network.NTP.server"));
printf("\n\n");
nb_config_set("network.NTP.server=192.168.0.2");

if (nb_config_get ("network.NTP.status") == "0"){

   printf ("and was not running.");
   printf("\n\n");
   nb_config_set ("network.NTP.status=1");
   }
   else {
   printf ("and was running.");
   printf("\n\n");
   }

printf ("The NTP server is now running with IP address: ");
printf (nb_config_get("network.NTP.server"));
```

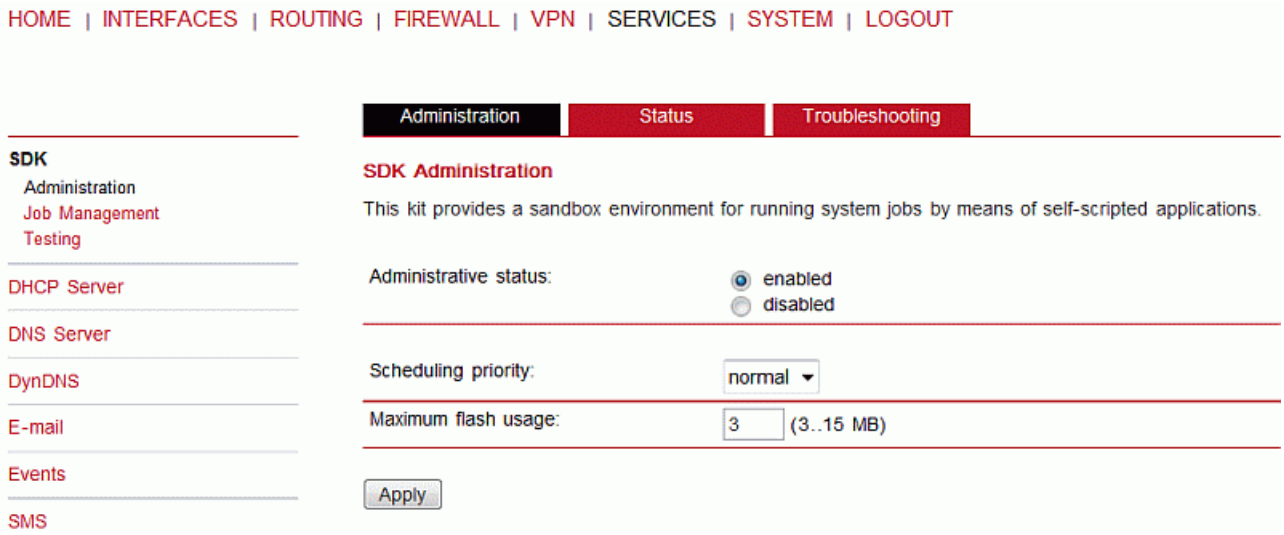
Running SDK

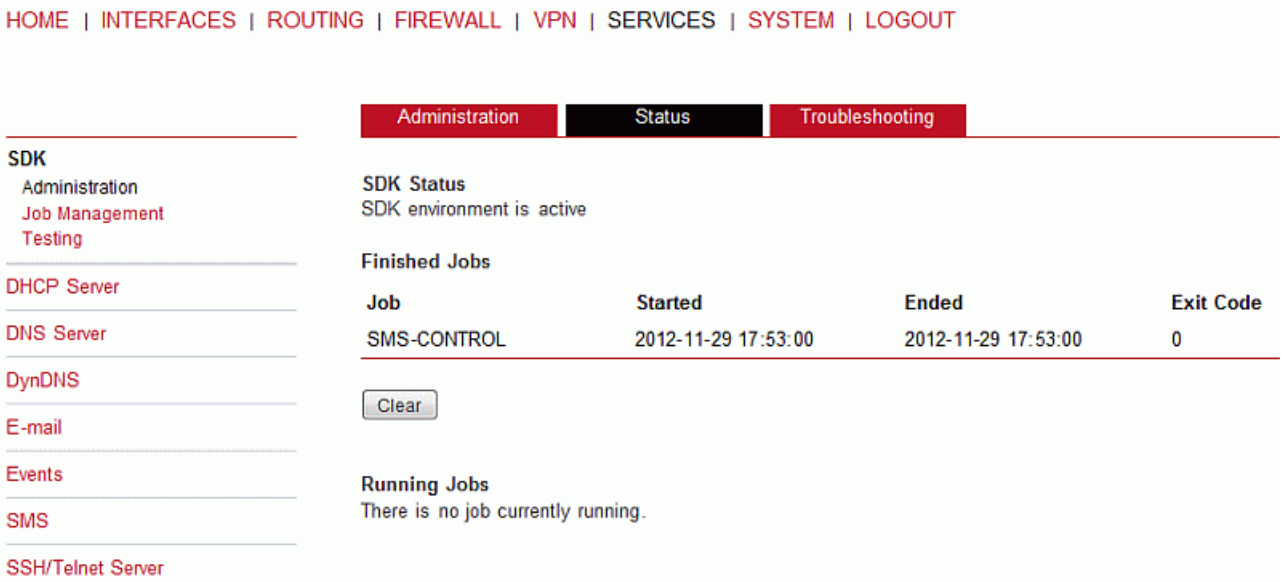
In the SDK, we are speaking of `scripts` and `triggers` which form `jobs`. Any `arena` script can be uploaded to the router or imported by using dedicated user configuration packages. You may also edit the script directly at the Web Manager or select one of our examples. You will further have a testing section on the router which can be used to check your syntax or doing test runs.

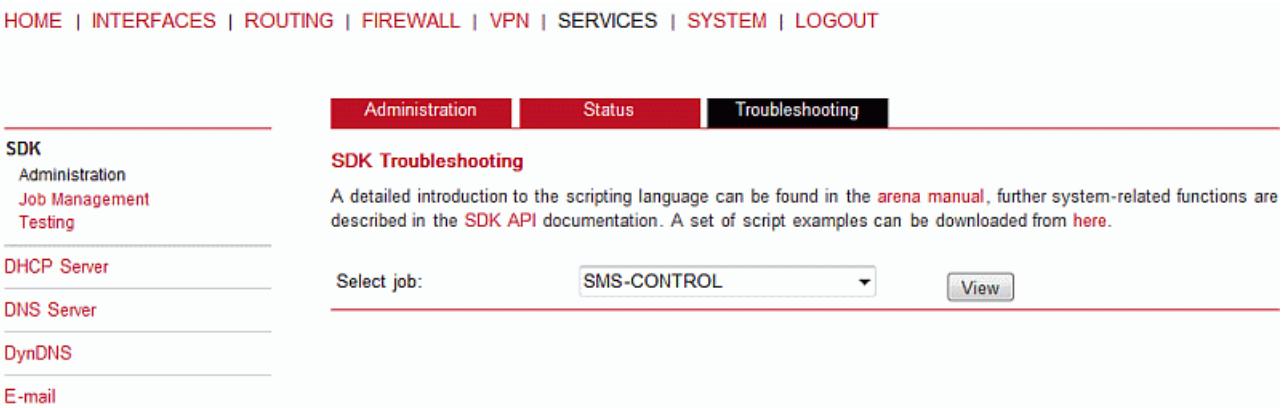
Once uploaded, you will have to specify a trigger, that is, telling the router when the script is to be executed. This can be either time-based (e.g. each Monday) or triggered by one of the pre-defined system events (e.g. wan-up) as described in Section 7.6.6, “Events” chapter. With both, a script and a trigger, you can finally set up an SDK job now. The test event usually serves as a good facility to check whether your job is doing well. The admin section also offers facilities to troubleshoot any issues and control running jobs. The SDK host (sdkhost) corresponds to the daemon managing the scripts and their operations and thus avoiding any harm to the system. In terms of resources, it will limit CPU and memory for running scripts and also provide a pre-defined portion of the available flash storage. You may, however, extend it by external USB storage or (depending on your model) SD cards.

Files written to `/tmp` will be hold in memory and will be cleared upon a restart of the script. As your scripts operate in the sandbox, you will have no access to tools on the system (such as `ifconfig`).

Administration





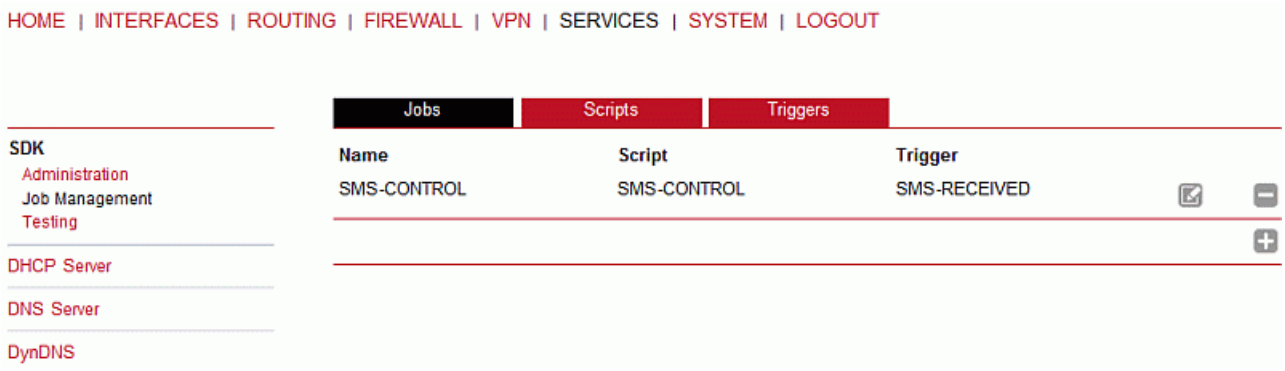


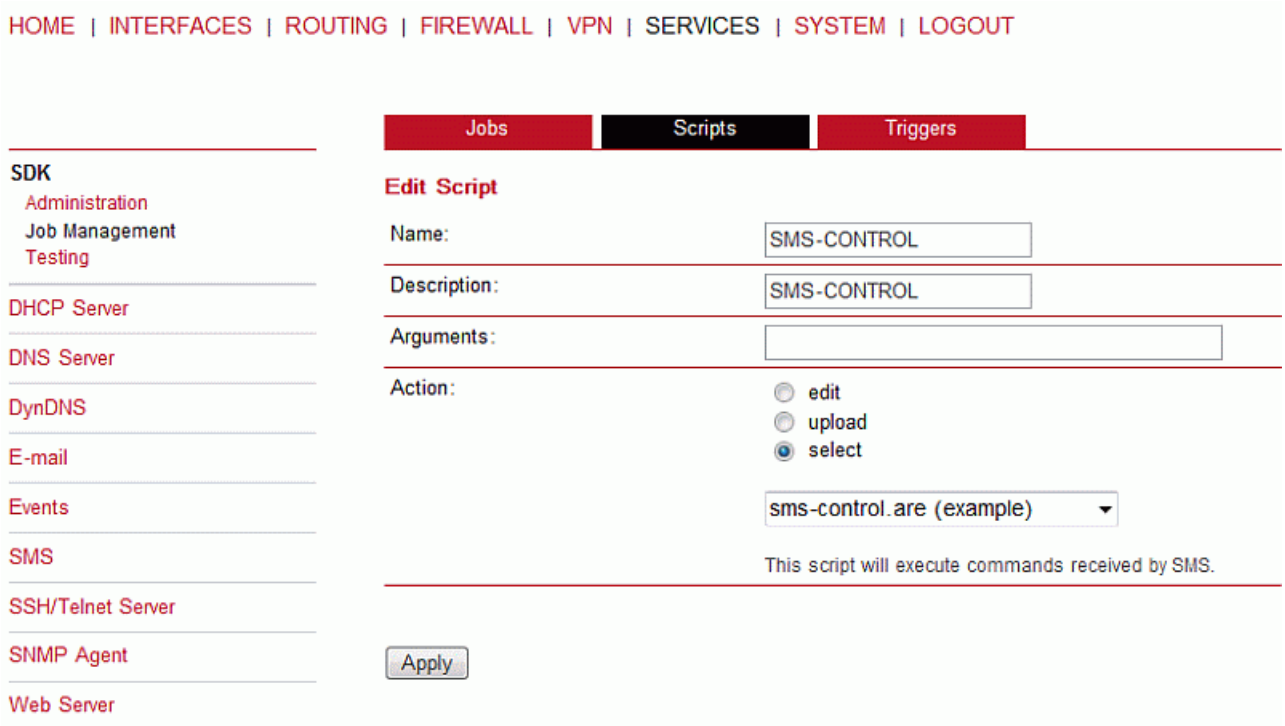
This page can be used to control the SDK host and apply the following settings:

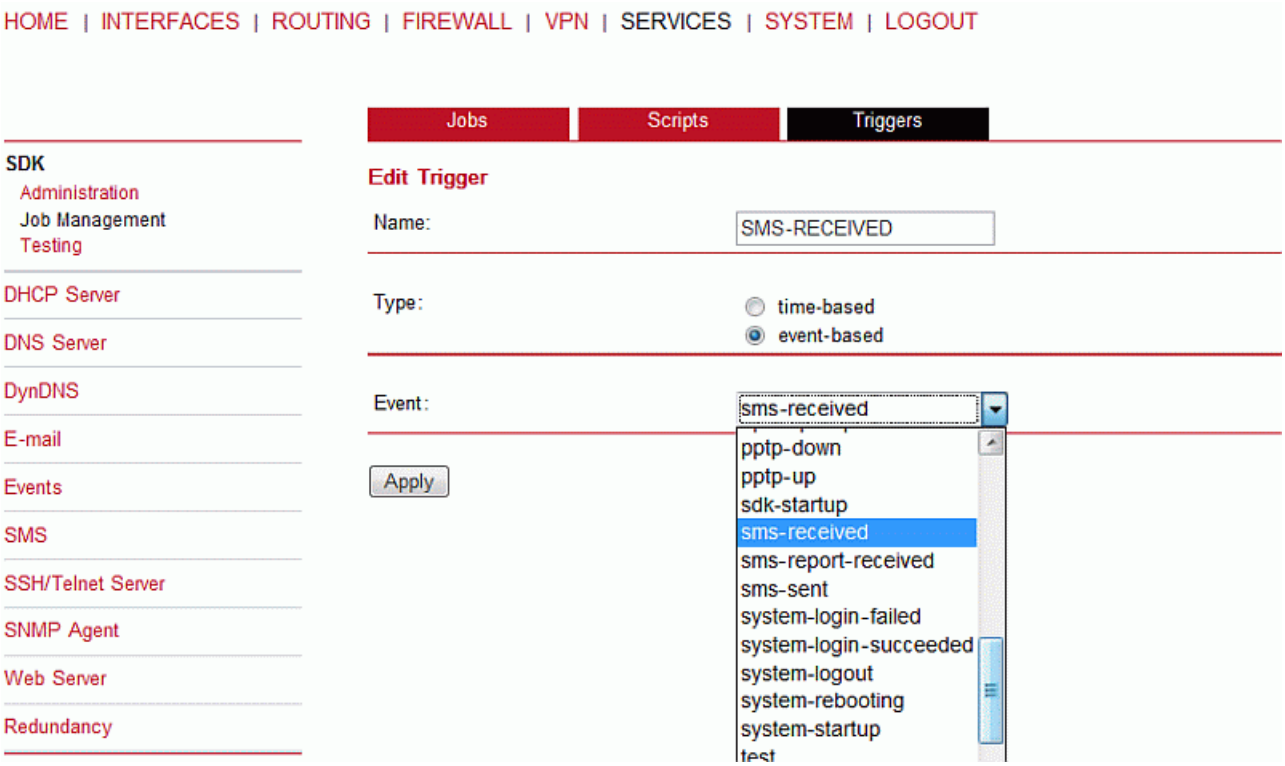
Parameter:	Description
Administrative status:	Specifies whether SDK scripts should run or not
Scheduling priority:	Specifies the process priority of the sdkhost, higher priorities will speed up scheduling your scripts, lower ones will have less impact to the host system
Maximum flash usage:	The maximum amount of MBytes your scripts can write to the internal flash

The status page informs you about the current status of the SDK. It provides an overview about any finished jobs, you can also stop a running job there and view the script output in the troubleshooting section where you will also find links for downloading the manuals and examples.

Job Management







This page can be used to set up scripts, triggers and jobs. It is usually a good idea to create a trigger first which is made up by the following parameters:

Name: A meaningful name to identify the trigger

Type: The type of the trigger, either time-based or event-based

Condition: Specifies the time condition for time-based triggers (e.g. hourly)

Timespec: The time specification which, together with the condition, specifies the `time(s)` when the trigger should be pulled

Event: The system event upon which the trigger should be pulled

You can now add your personal script to the system by applying the following parameters:

Name: A meaningful name to identify the script

Description: An optional description of the script

Arguments: An optional set of arguments passed to the script (supports quoting)

Action: You may either edit a script, upload it to the system or select one of the example scripts or an already uploaded script

You are ready to set up a job afterwards, it can be created by using the following parameters:

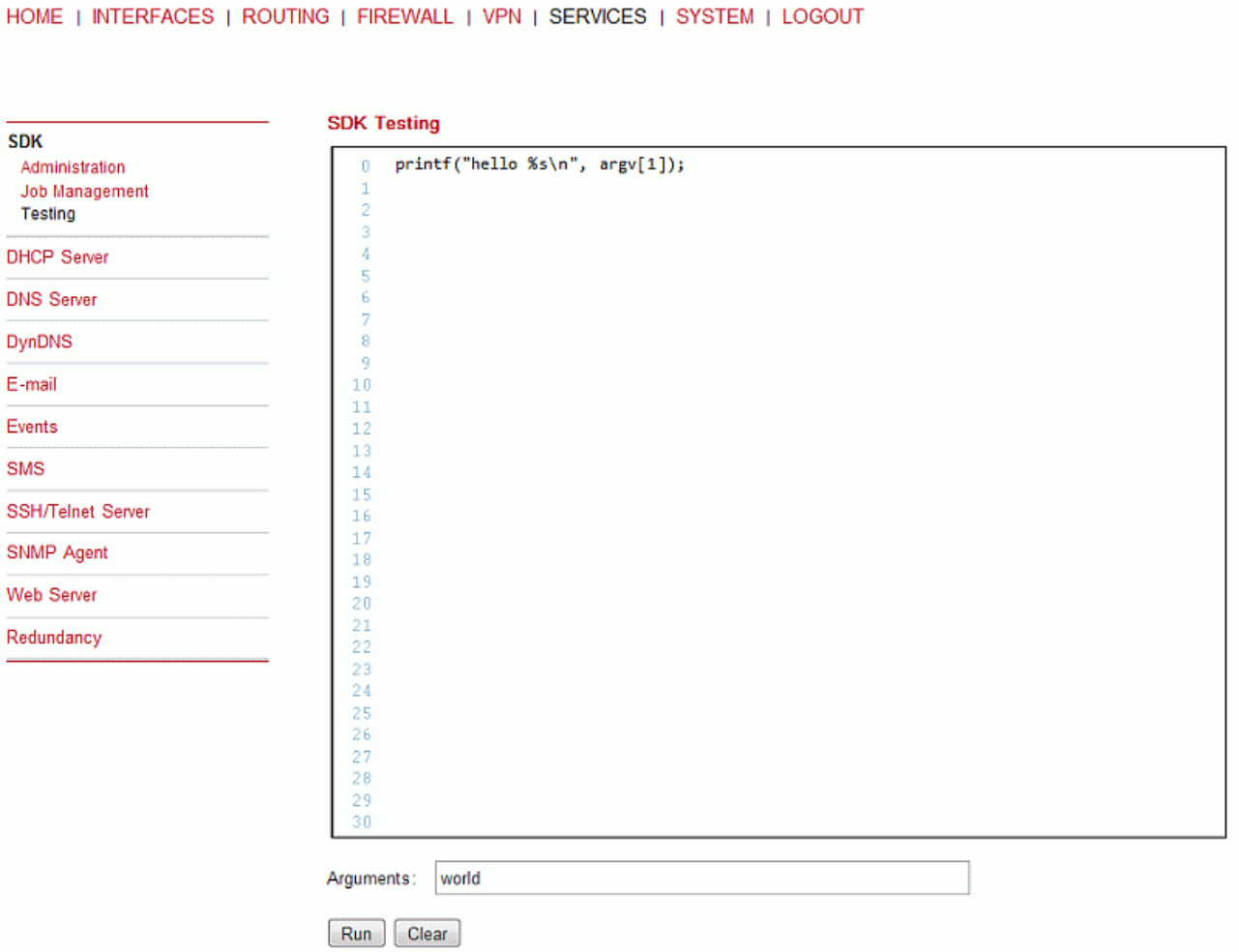
Name: A meaningful name to identify the job

Trigger: Specifies the trigger that should launch the job

Script: Specifies the script to be executed

Arguments: Defines arguments which can be passed to the script (supports quoting), they will precede the arguments you formerly may have assigned to the script itself

Testing



The testing page offers an editor and an input field for optional arguments which can be used to perform test runs of your script or test dedicated portions of it. Please note that you might need to quote arguments as they will otherwise be separated by white-spaces.

```
/* arguments :  schnick schnack "s c h n u c k"

for (i = 0; i < argc ; i++) {
    printf (" argv %d: %s\n", argv [i]);
}

/* generates :
 *      argv0 :  scriptname
 *      argv1 :  schnick
 *      argv2 :  schnack
 *      argv3 :  s c h n u c k
 */
```

In case of syntax errors, arena will usually print error messages as follows (indicating the line and position where the parsing error occurred):

```
/scripts/testrun:2:10:FATAL: parse error, unexpected $, expecting ';'
```

SDK Sample Application

As an introduction, you can step through a sample application, namely the SMS control script, which implements remote control over short messages and can be used to send a status of the system back to the sender. The source code is listed in the appendix.

Once enabled, you can send a message to the phone number associated with a SIM / modem. It generally requires a password to be given on the first line and a command on the second, such as:

```
admin01
status
```

We strongly recommend to use authentication in order to avoid any unintended access, however you may pass noauth as argument to disable it. You can then skip the first line containing the password. Having a closer look to the script, you will see that you will also be able to restrict the list of permitted senders. Please inspect the system log for troubleshooting any issues.

The following commands are supported:

status — A SMS with the following information will be returned

- Signal strength
- Mobile connection state (up/down)
- current IP address of the mobile interface
- current IP address of the VPN interface (if enabled)

connect — This will initiate a Dial-out connection over GSM/UMTS 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)

disconnect — terminates all WAN connections (including VPN)

reboot — Initiates a system reboot

output 1 on — Switch digital output 1 on

output 1 off — Switch digital output 1 off

output 2 on — Switch digital output 2 on

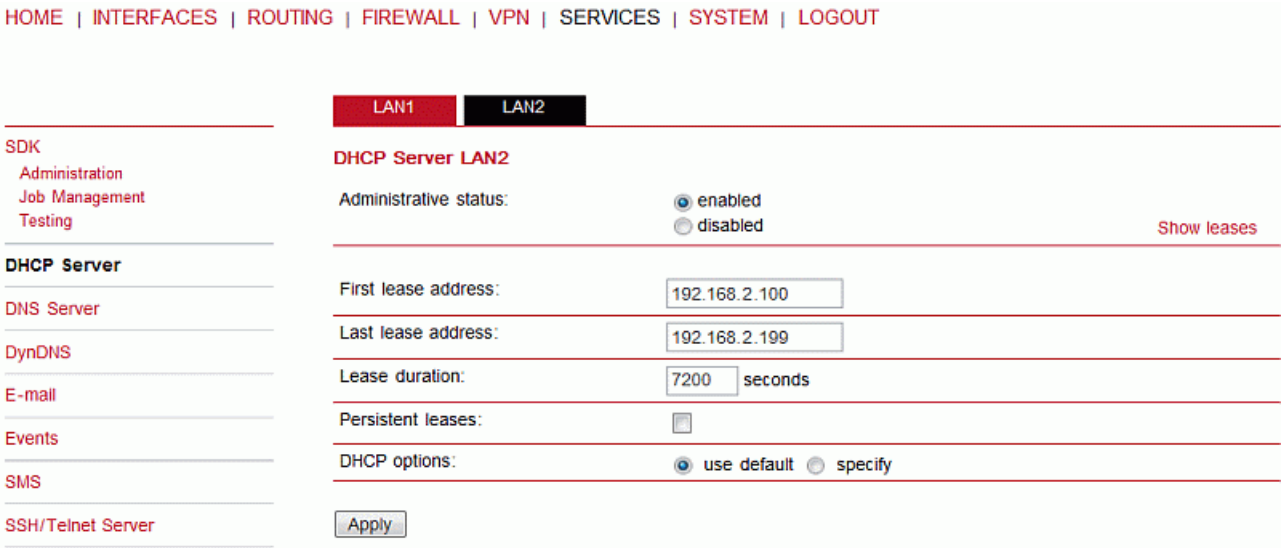
output 2 off — Switch digital output 2 off

A response to the status command typically looks like:

```
System: MIDGE midge (0002A9FFC32E)
WAN1: WWAN1 is up (10.204.8.3, Mobile1,
HSPA, -65 dBm, LAI 23003)
DIO: IN1=off, IN2=off, OUT1=off, OUT2=on
```

7.6.2. DHCP Server

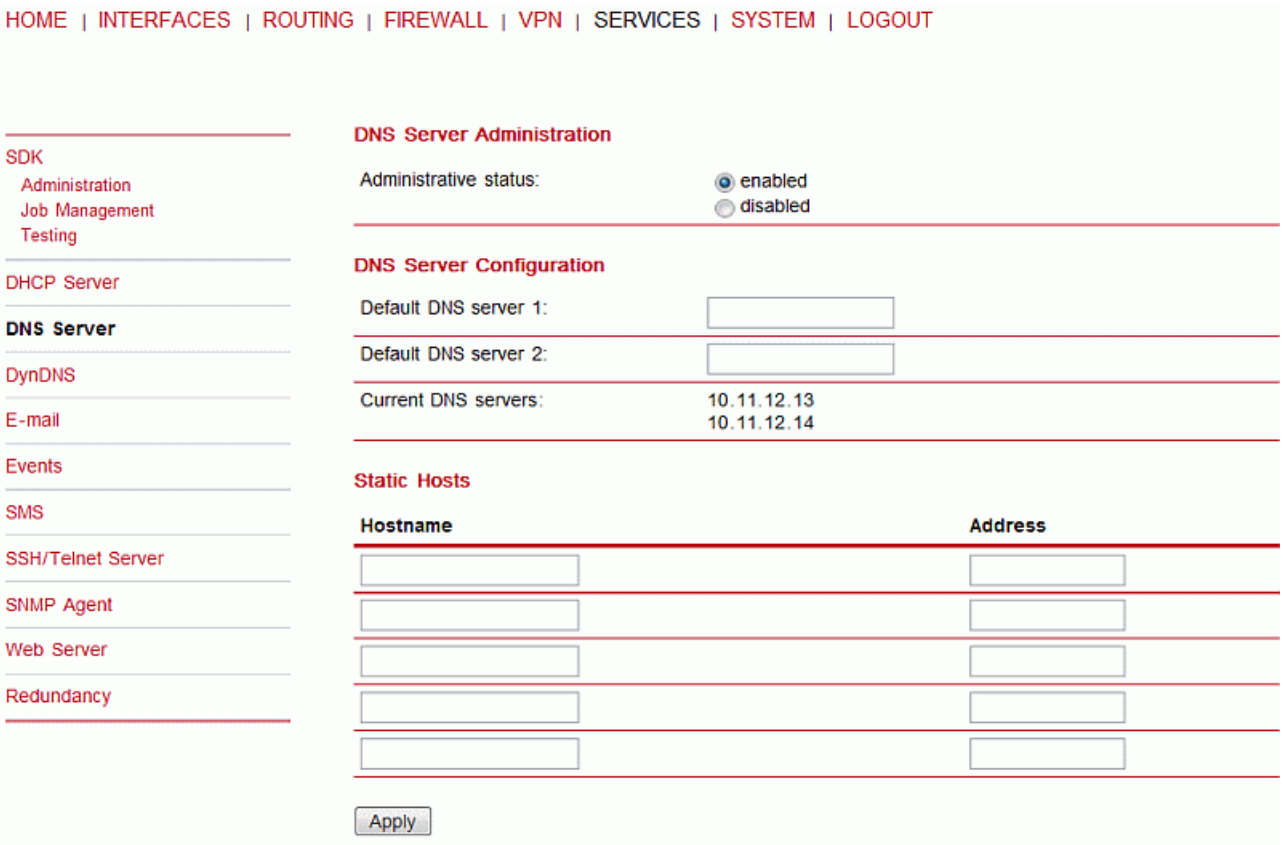
This section can be used to individually configure a DHCP service for each LAN interface.



Administrative status:	The Dynamic Host Configuration Protocol (DHCP) server can be enabled or disabled. If enabled it will answer to DHCP requests from hosts in the LAN
First lease address:	First address for DHCP clients
Last lease address:	Last address for DHCP clients
Persistent leases:	By turning this option on, router will remember to give leases even after a reboot. It can be used to ensure the same IP addresses are assigned to a particular host.
DHCP options:	By default DHCP will hand out the interface address as default gateway and DNS server address if not configured elsewhere. It is possible to specify different addresses here.

7.6.3. DNS Server

The DNS server can be used to proxy DNS requests towards servers on the net which have for instance been negotiated during WAN link negotiation. By pointing DNS requests to the router, one can reduce outbound DNS traffic as it is caching already resolved names but it can be also used for serving fixed addresses for particular host names.

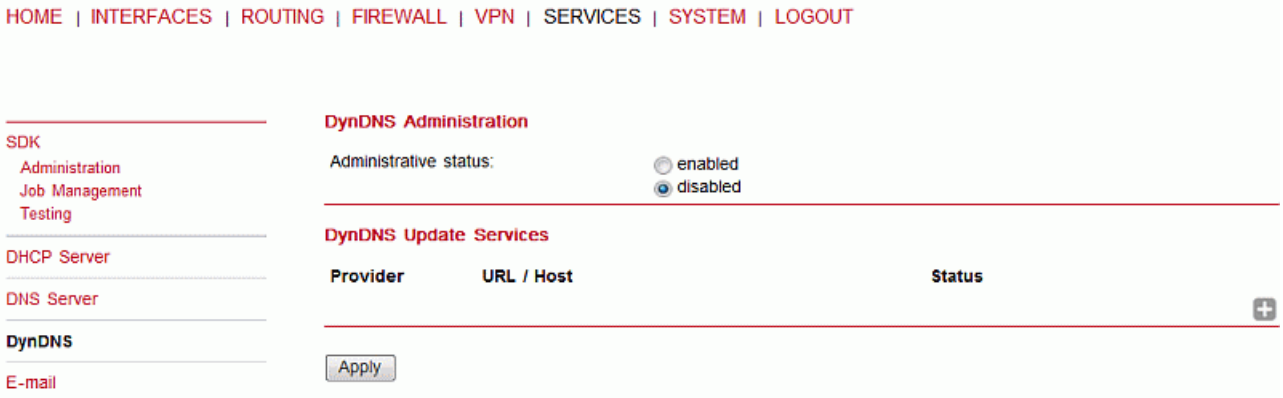


Administrative status:	Enabled or disabled
Default DNS server 1:	The primary DNS server to be queried
Default DNS server 2:	The secondary server which will be used in case the primary server is not available.

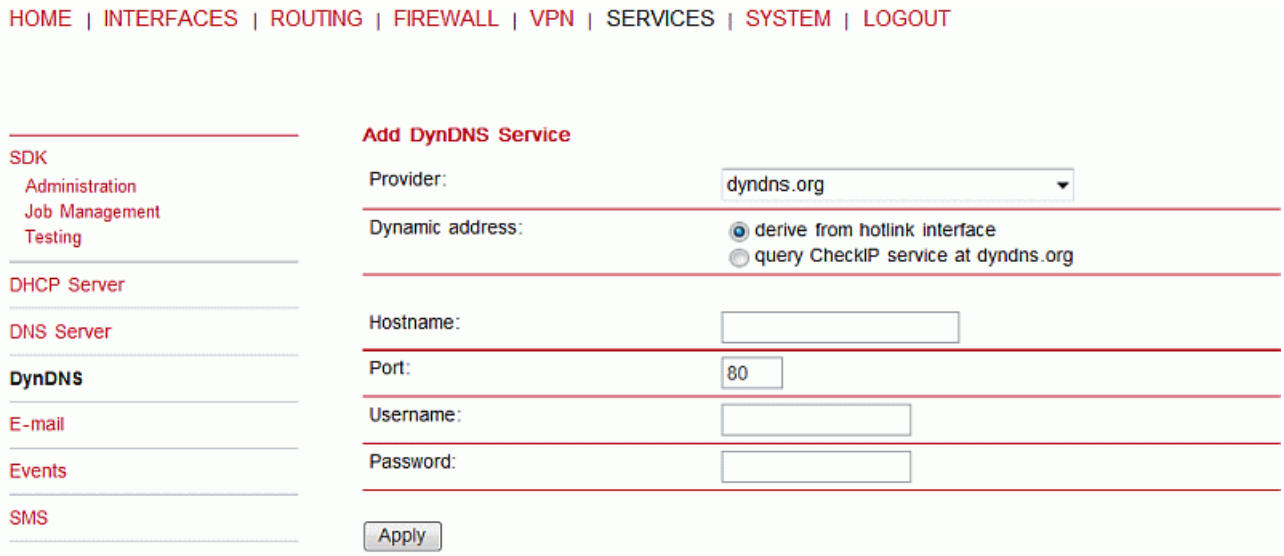
You may further configure static hosts for serving fixed IP addresses for various hostnames. Please remember to point local hosts to the router's address for resolving them.

7.6.4. Dynamic DNS

Dynamic DNS client on this box is generally compatible with various DynDNS services on the Internet running by means of definitions by the DynDNS organization (see www.dyndns.com for server implementations).



Administrative status: Enabled or disabled



Dynamic address: Specifies whether the address is derived from the hot-link or via an external service

Hostname: The host-name provided by your DynDNS service (e.g. mybox.dyndns.org)

Port: The HTTP port of the service (typically 80)

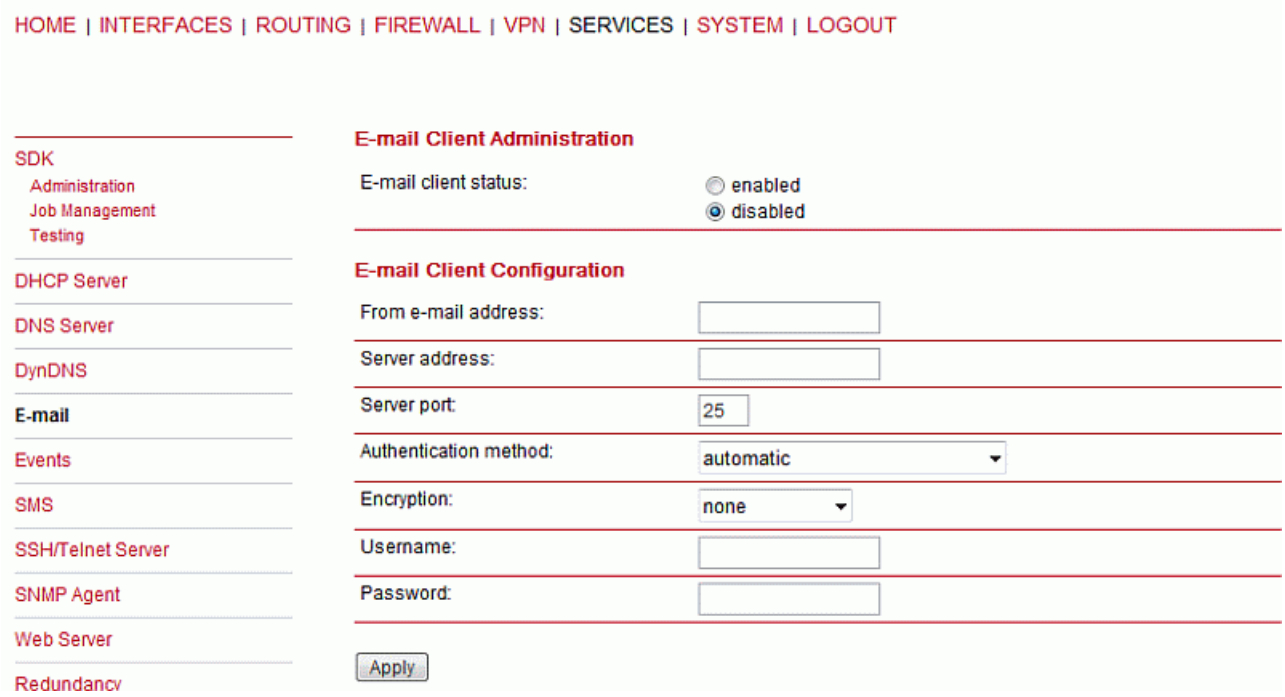
Username: The user-name used for authenticating at the service

Password: The password used for authentication

Please note that your RACOM router can operate as DynDNS service as well, provided that you hold a valid SERVER license and have your hosts pointed to the DNS service of the router.

7.6.5. E-mail client

The E-Mail client can be used to send notifications to a particular E-Mail address upon certain events or by SDK scripts.

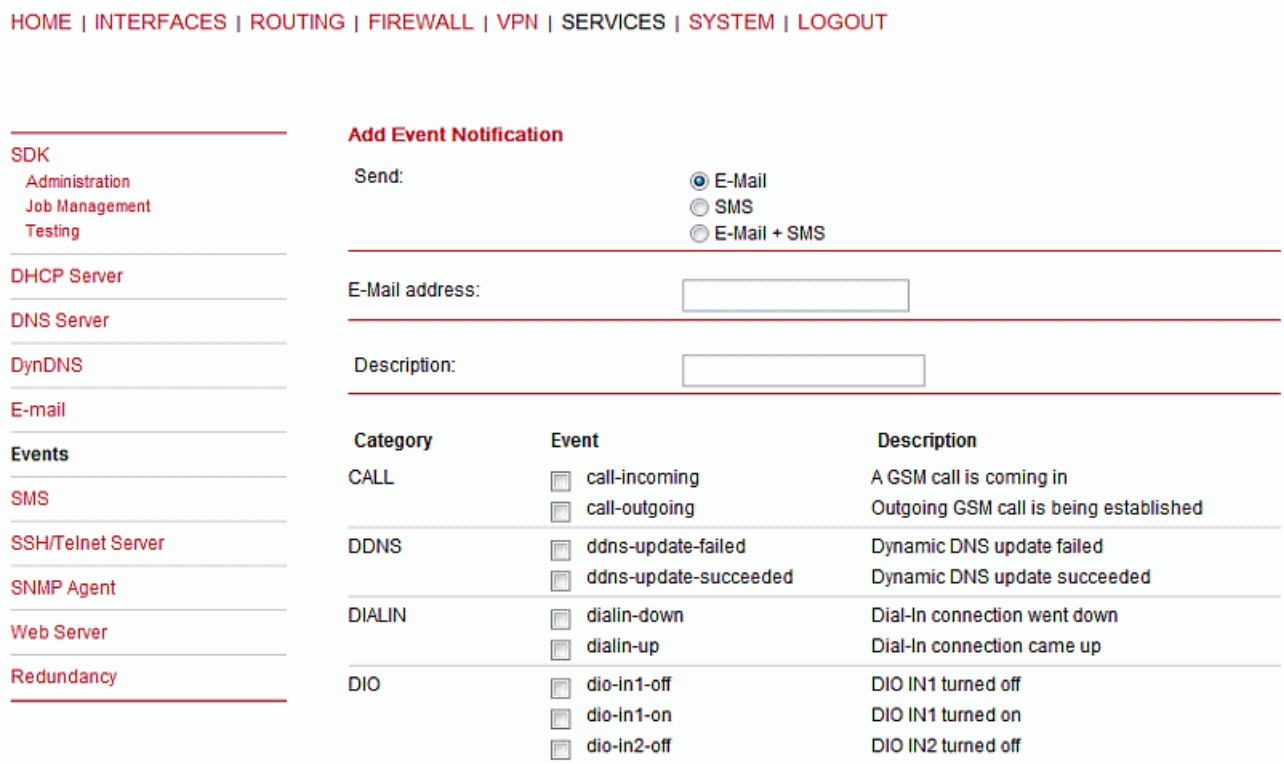


E-mail client status:	Administrative status of the E-Mail client - Enabled or disabled
From e-mail address:	E-Mail address of the sender
Server address:	SMTP server address
Server port:	SMTP server port (typically 25)
Authentication method:	Choose the required authentication method to authenticate against the SMTP server
User name:	User name for authentication
Password:	Password for authentication

7.6.6. Events

By using the event manager you can notify one or more recipients by SMS or E-Mail upon certain system events. The messages will contain a description provided by you and a short system info.

Events



The default texts for a specific Event are as folows:

wan-up	WAN link came up
wan-down	WAN link went down
dio-in1-on	DIO IN1 turned on
dio-in2-on	DIO IN2 turned on
dio-in1-off	DIO IN1 turned off
dio-in2-off	DIO IN2 turned off
dio-out1-on	DIO OUT1 turned on
dio-out2-on	DIO OUT2 turned on
dio-out1-off	DIO OUT1 turned off
dio-out2-off	DIO OUT2 turned off
gps-up	GPS signal is available
gps-down	GPS signal is not available
openvpn-up	OpenVPN connection came up
openvpn-down	OpenVPN connection went down
ipsec-up	IPsec connection came up

ipsec-down	IPsec connection went down
pptp-up	PPTP connection came up
pptp-down	PPTP connection went down
dialin-up	Dial-In connection came up
dialin-down	Dial-In connection went down
mobileip-up	Mobile IP connection came up
mobileip-down	Mobile IP connection went down
system-login-failed	User login failed
system-login-succeeded	User login succeeded
system-logout	User logged out
system-rebooting	System reboot has been triggered
system-startup	System has been started
sdk-startup	SDK has been started
sms-sent	SMS has been sent
sms-received	SMS has been received
sms-report-received	SMS report has been received
call-incoming	A GSM call is coming in
call-outgoing	Outgoing GSM call is being established
ddns-update-succeeded	Dynamic DNS update succeeded
ddns-update-failed	Dynamic DNS update failed
usb-storage-added	USB storage device has been added
usb-storage-removed	USB storage device has been removed
system-time-updated	System time has been updated
test	test event

7.6.7. SMS

This page lets you turn the SMS event notification service on and enable remote control via SMS.

Administration

On RACOM routers it is possible to receive or send short messages (SMS) over each mounted modem (depending on the assembly options). Messages are received by querying the SIM card over a modem,

so prior to that, the required assignment of a SIM card to a modem needs to be specified on the SIMs page.

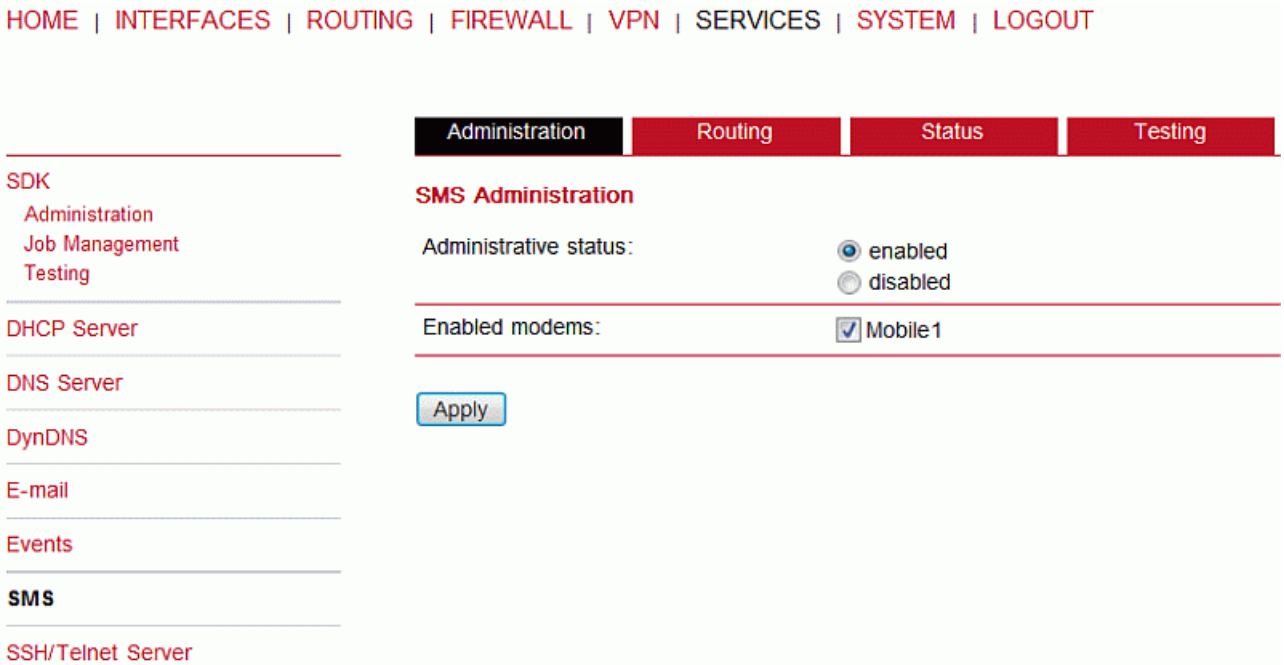
Please bear in mind, in case you are running multiple WWAN interfaces sharing the same SIM, that the system may switch SIMs during operation which will also result in different settings for SMS communication.

Received messages are pulled from the SIMs and temporarily stored on the router but get cleared after a system reboot. Please consider to consult an SDK script in case you want to process or copy them.

Sending messages heavily depends on the registration state of the modem and whether the provided SMS Center service works and may fail. You may use the sms-report-received event to figure out whether a message has been successfully sent.

Please do not forget that modems might register roaming to foreign networks where other fees may apply. You can manually assign a fixed network (by LAI) in the SIMs section.

The relevant page can be used to enable the SMS service and specify on which it should operate.

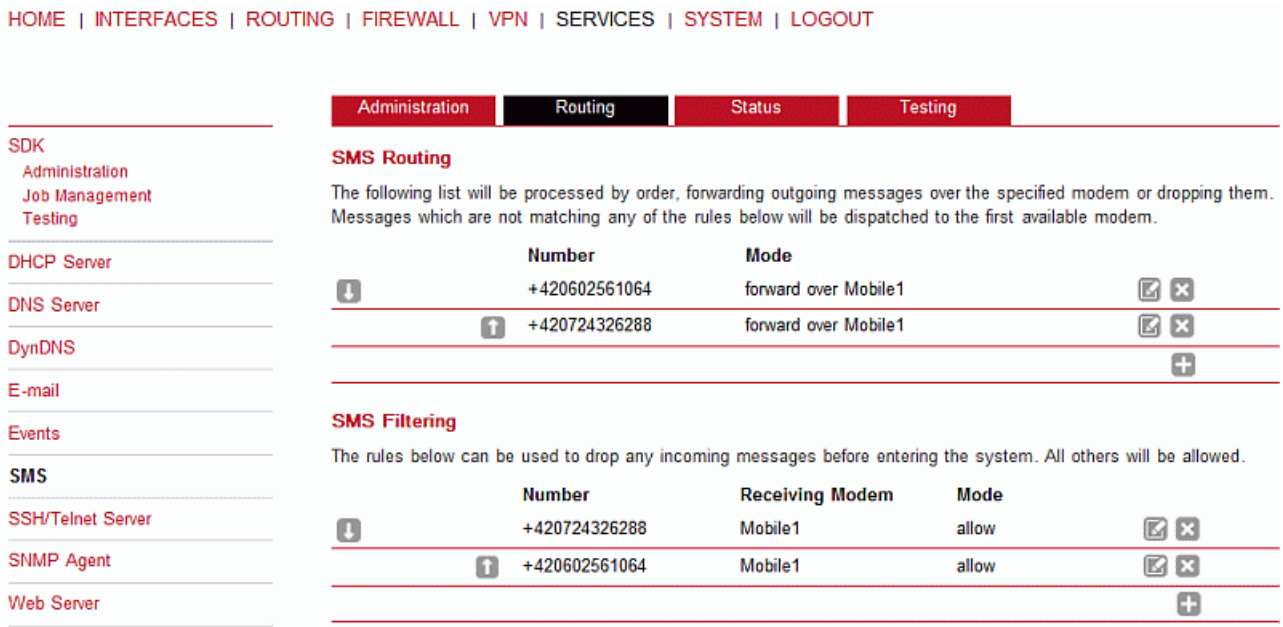


SMS notification: Sending SMS can be enabled or disabled. Disabling sending SMS means that no notification via SMS will be performed.

SMS control: Receiving SMS can be enabled or disabled. Disabling receiving SMS means that controlling M!DGE via SMS will not be possible

Routing & Filtering

By using SMS routing you can specify outbound rules which will be applied whenever message are sent. On the one hand, you can forward them to an enabled modem. For a particular number, you can for instance enforce messages being sent over a dedicated SIM.



Phone numbers can also be specified by regular expressions, here are some examples:

```
+12345678   Specifies a fixed number
+1*         Specifies any numbers starting with +1
+1*9        Specifies any numbers starting with +1 and ending with 9
+[12]*      Specifies any numbers starting with either +1 or 2
```

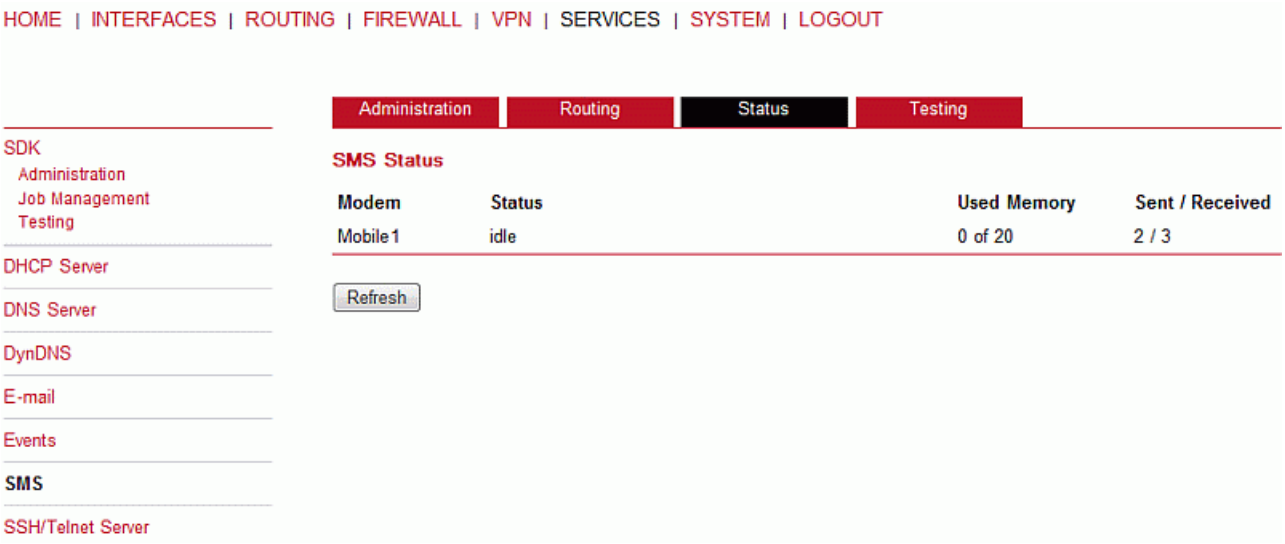
Please note that numbers have to be entered in international format including a valid prefix. On the other hand, you can also define rules to drop outgoing messages, for instance, when you want to avoid using any expensive service or international numbers.

Both types of rules form a list will be processed by order, forwarding outgoing messages over the specified modem or dropping them. Messages which are not matching any of the rules below will be dispatched to the first available modem.

Filtering serves a concept of firewalling incoming messages, thus either dropping or allowing them on a per-modem basis. The created rules are processed by order and in case of matches will either drop or forward the incoming message before entering the system. All non-matching messages will be allowed.

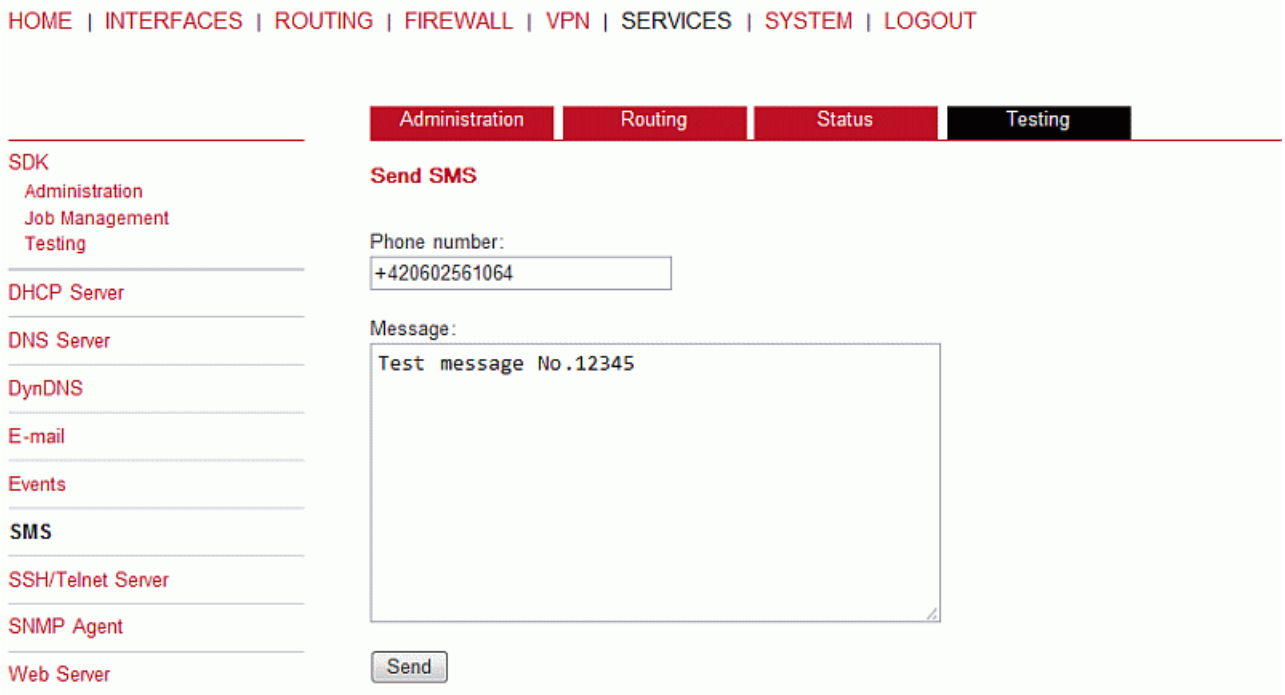
Status

The status page can be used to the current modem status and get information about any sent or received messages. There is a small SMS inbox reader which can be used to view or delete the messages. Please note that the inbox will be cleared each midnight in case it exceeds 512 kBytes of flash usage.



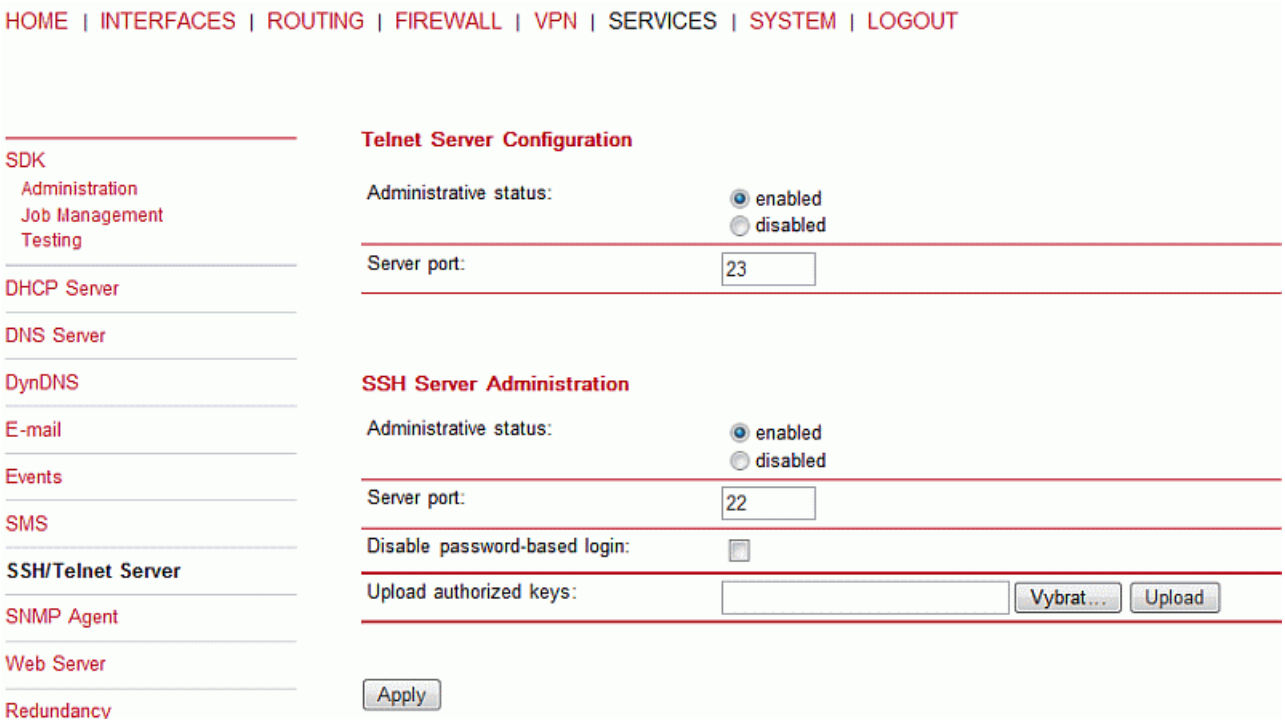
Testing

This page can be used to test whether SMS sending in general or filtering/routing rules works. The maximum length per message part is limited to 160 characters, we also suggest to exclusively use characters which are supported by the GSM 7-bit alphabet.



7.6.8. SSH/Telnet Server

Apart from the Web Manager, the SSH and Telnet services can be used to log into the system. Valid users include root and admin as well as additional users as they can be created in the User Accounts section. Please note, that a regular system shell will only be provided for the root user, the CLI will be launched for any other user whereas normal users will only be able to view status values, the admin user will obtain privileges to modify the system.



Please note that these services will be accessible from the WAN interface also. In doubt, please consider to disable or restrict access to them by applying applicable firewall rules.

The following parameters can be applied to the Telnet service:

Administrative status: Whether the Telnet service is enabled or disabled

Server port: The TCP port of the service (usually 23)

The following parameters can be applied to the SSH service:

Administrative status: Whether the SSH service is enabled or disabled

Server port: The TCP port of the service (usually 22)

Disable password-based login: By turning on this option, all users will have to authenticate by SSH keys which can be uploaded to the router.

7.6.9. SNMP Agent

M!DGE is equipped with a SNMP daemon, supporting basic MIB tables (such as ifTable), plus additional enterprise MIBs to manage multiple systems. M!DGE OID starts with 1.3.6.1.4.1.33555.10 prefix. The corresponding VENDOR MIB can be downloaded from the router.

Once the SNMP agent is enabled, SNMP traps are generated for the following conditions:

- Start-up of the M!DGE
- Shutdown of the M!DGE
- VPN connected
- VPN disconnected
- Signal strength fell below "Signal strength trap threshold"

Start-up trap is implemented using the standard cold Start & warm Start traps. System-shutdown trap is sent, when the system is rebooted via the web interface reboot function or when the watchdog reboots the system.

M!DGE extensions contain support for:

- Rebooting the device
- Updating to a new system software via FTP/TFTP/HTTP
- Updating to a new system configuration via FTP/TFTP/HTTP
- Getting WWAN/GNSS/WLAN/DIO information

Setting MIB values is limited to SNMPv3 and only the 'admin' user is entitled to trigger the extensions.

Note

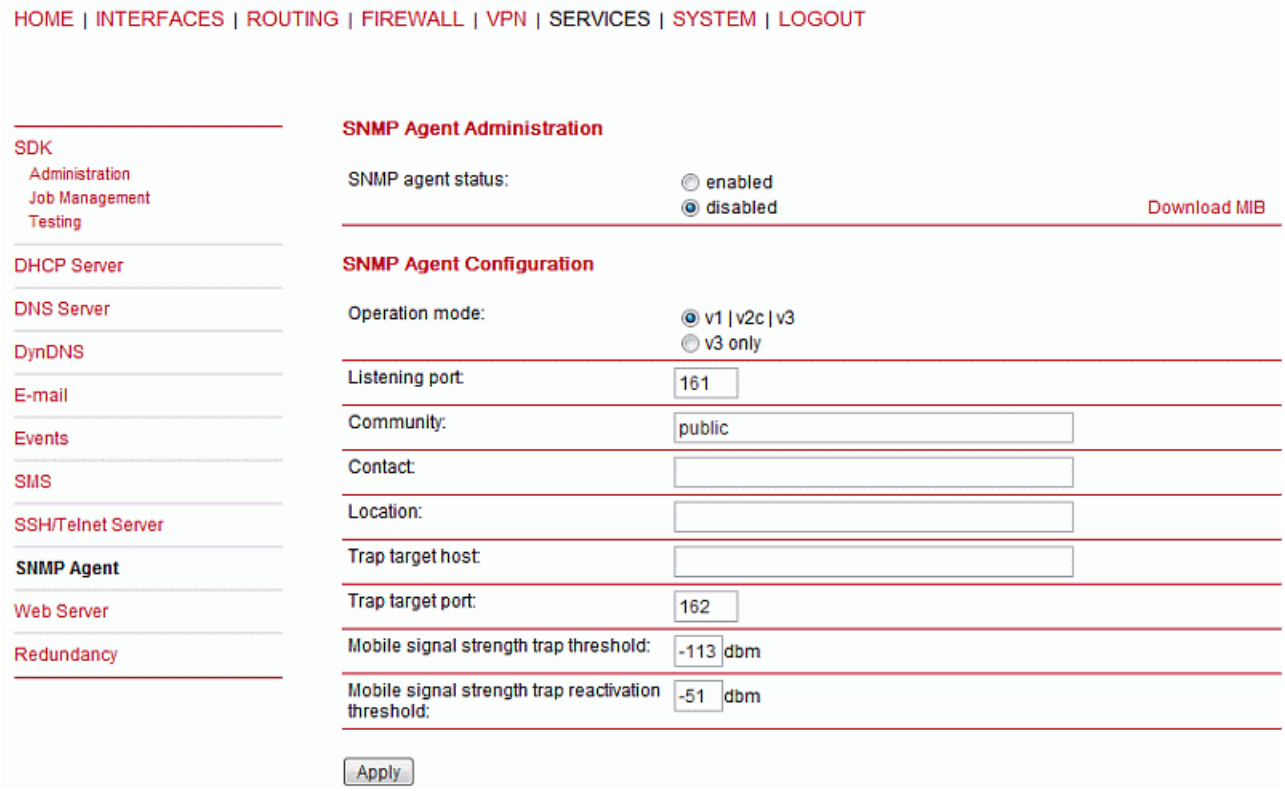
Attention must be paid to the fact that SNMP passwords have to be more than 8 characters long. Shorter passwords will be doubled for SNMP, e.g. 'admin01' becomes 'admin01admin01'.

SNMP extensions can be read and triggered as follows:

- To get system software version:
  snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.33555.10.40.1.0
- To get a kernel version:
  snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.33555.10.40.2.0
- To get a serial number:
  snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.33555.10.40.3.0
- To restart the device:
  snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.33555.10.40.10.0 i 1
- To run a configuration update:
  snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.33555.10.40.11.0 s "http://server/directory"

REMARK: config Update expects a zip-file named <serial-number>.zip in the specified directory which contains at least a "user-config.zip"
Supported protocols are TFTP, HTTP(s) and FTP.
Specifying a username/password or port is not yet supported.

- get configuration update status:
  snmpget -v 3 -u snmpadmin -n "" -l authNoPriv -a MD5 -x DES -A snmpadmin 192.168.1.1 1.3.6.1.4.1.31496.10.40.12.0
  The return value can be one of: (1) succeeded, (2) failed, (3) inprogress, (4) notstarted.
- run software update:
  snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.31496.10.40.13.0 s "http://server/directory"
- get software update status:
  snmpget -v 3 -u snmpadmin -n "" -l authNoPriv -a MD5 -x DES -A snmpadmin 192.168.1.1 1.3.6.1.4.1.31496.10.40.14.0
  Return value can be either of: (1) succeeded, (2) failed, (3) inprogress, (4) notstarted.

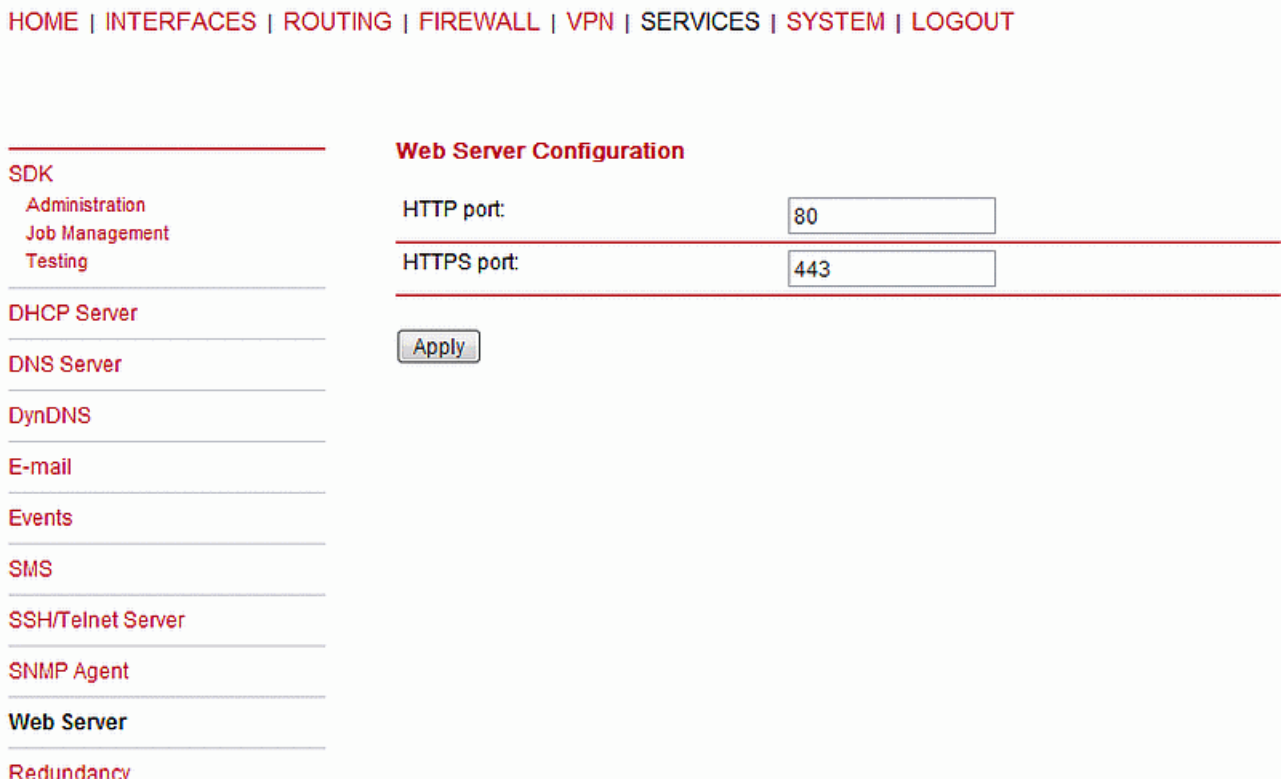


SNMP agent status:	Enable or disable the SNMP agent
Listening Port:	SNMP agent port
Community:	A SNMP community string corresponding to the group that devices and management stations running SNMP belong to
Contact:	System maintainer/contact information
Location:	Location of the device
Trap target host:	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:	A trap will be sent, if signal strength falls below this threshold
Signal strength trap reactivation threshold:	No further traps will be sent as long as signal strength is not higher than this value

7.6.10. Web Server

This page can be used to configure different ports for accessing the Web Manager via HTTP/HTTPS. We strongly recommend to use HTTPS when accessing the web service via a WAN interface as the communication will be encrypted and thus avoids any misuse of the system.

In order to enable HTTPS you would need to generate or upload a server certificate in the section SYSTEM-Keys and Certificates.



HTTP port: Web server port for HTTP connections

HTTPS port: Web server port for HTTPS connections

7.6.11. Redundancy

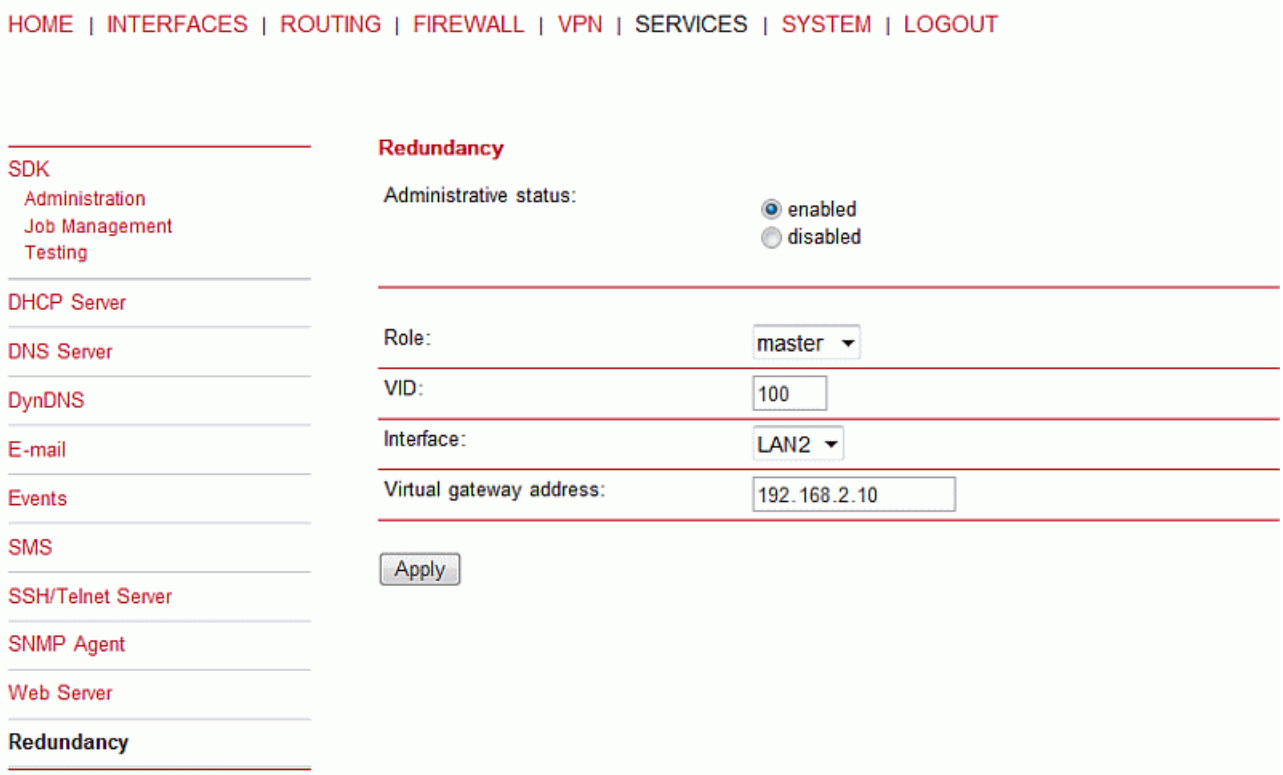
This section can be used to set up a redundant pair of M!DGEs (or other systems) by running the Virtual Router Redundancy Protocol (VRRP) among them. A typical VRRP scenario defines a first host playing the master and another the backup device, they both define a virtual gateway IP address which will be distributed by gratuitous ARP messages for updating the ARP cache of all LAN hosts and thus redirecting the packets accordingly.

A takeover will happen within approximately 3 seconds as soon as the partner is no longer reachable (checked via multicast packets). This may happen when one device is rebooting or the Ethernet link went down. Same applies when the WAN link goes down.

In case DHCP has been activated, please keep in mind that you will need to reconfigure the DHCP gateway address offered by the server and let them point to the virtual gateway address. In order to avoid conflicts you may turn off DHCP on the backup device or even better, split the DHCP lease range in order to prevent any lease duplication.

Note

M!DGE assigns a priority of 100 to the master and 1 to the backup router. Please adapt the priority of your third-party device appropriately.

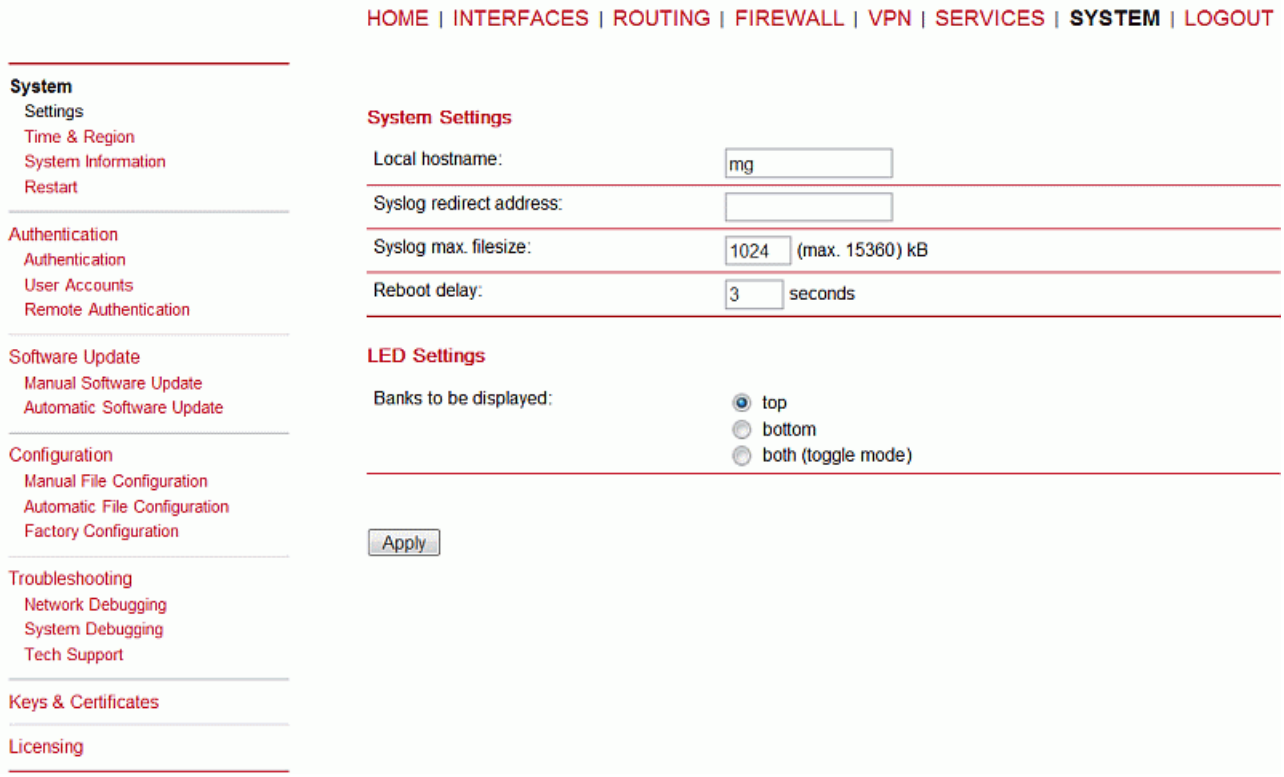


Administrative status:	Administrative status
Role:	Role of this system (either master or backup)
VID:	The Virtual Router ID (you can theoretically run multiple instances)
Interface:	Interface on which VRRP should be performed
Virtual gateway address:	Virtual gateway address formed by the participating hosts

7.7. SYSTEM

7.7.1. System

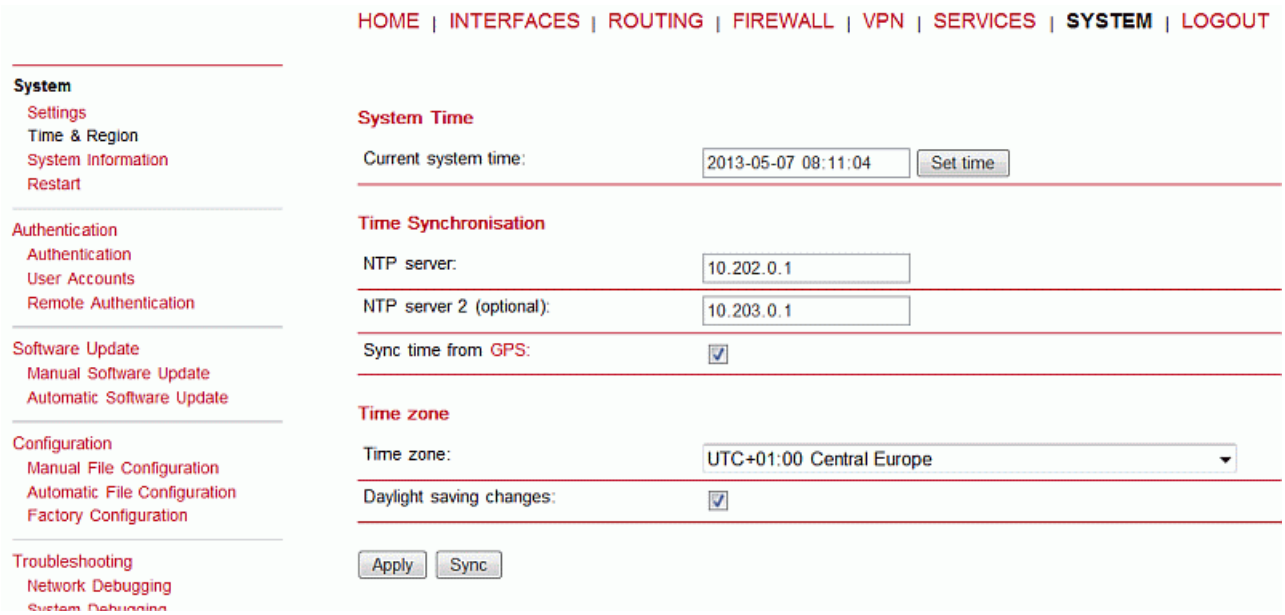
Settings



Local host name:	The local host name of the system
Syslog redirect address:	The host where system log messages should be forwarded to. You can use for example a tiny system log server for Windows included in TFTP32.
LED Settings:	You can configure the behaviour of the status LEDs on the front panel of your device. They are usually divided into two banks - left for he digital IO port status or right for indication of the connection status. You may configure toggle mode, so that the LEDs periodically show both bank states. See description of LEDs in section Section 4.3, “Indication LEDs” .

Time & Region

Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. M!DGE can synchronize its system time with a NTP server. If enabled, time synchronization is usually triggered after a WAN link has come up but before starting any VPN connections. Further time synchronizations are scheduled in the background every 60 minutes.

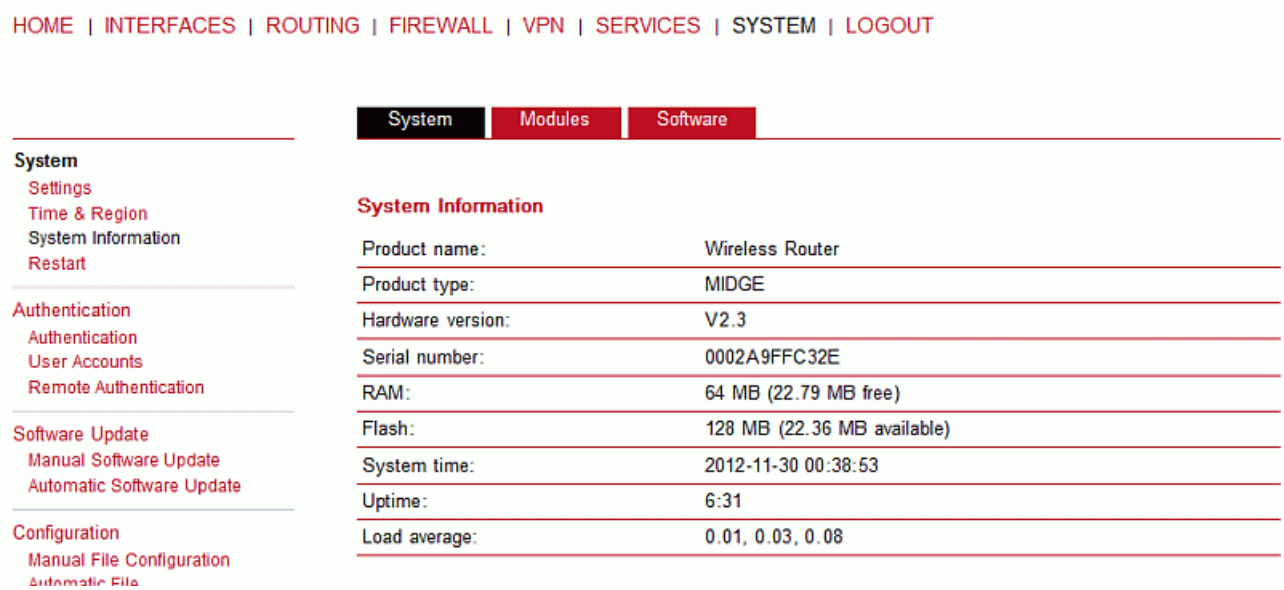


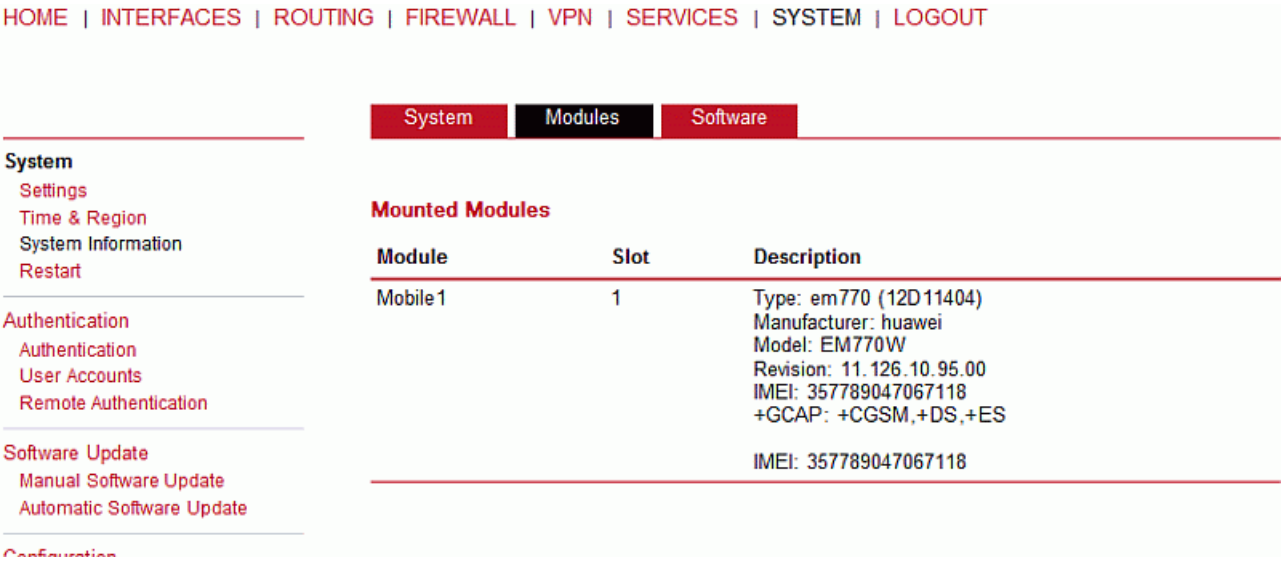
System Time:	It is possible set time manually - the time shall be lost after a restart.
Time synchronisation	...
NTP server:	Host name of NTP server
NTP server 2 (optional):	Host name of an optional second NTP server
Time zone:	Time zone
Daylight saving changes:	This option can be used to reflect daylight saving changes (e.g. switching from summer to winter time) depending on the selected time zone.

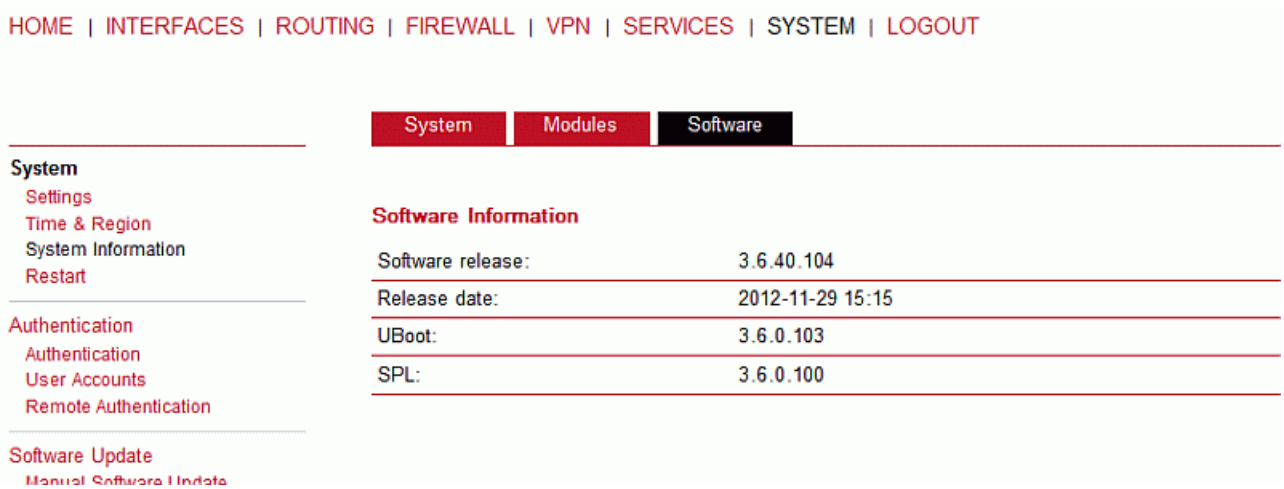
Sync will perform the time synchronisation immediatelly.

System Information

System information page displays various details of your M!DGE. Update of the page takes several seconds.





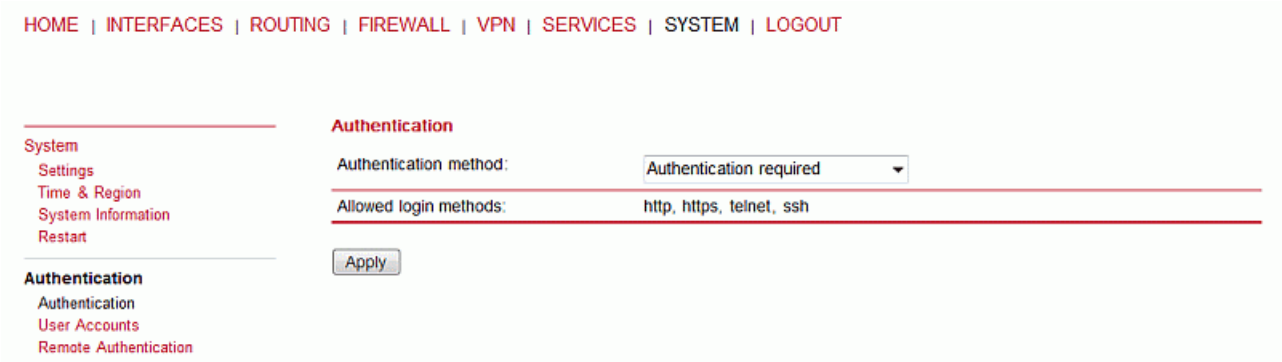


Restart

This menu can be used to restart the system. Any WAN links will be dropped.

7.7.2. Authentication

Authentication

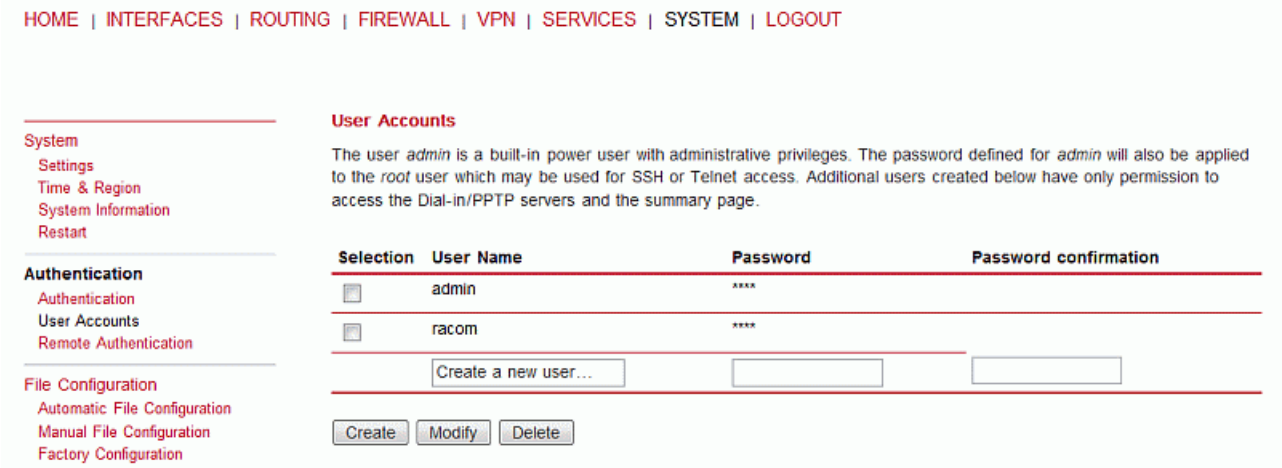


This page offers a simple shortcut to only allow secure connections (SSH, HTTPS) for managing the router.

User Accounts

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

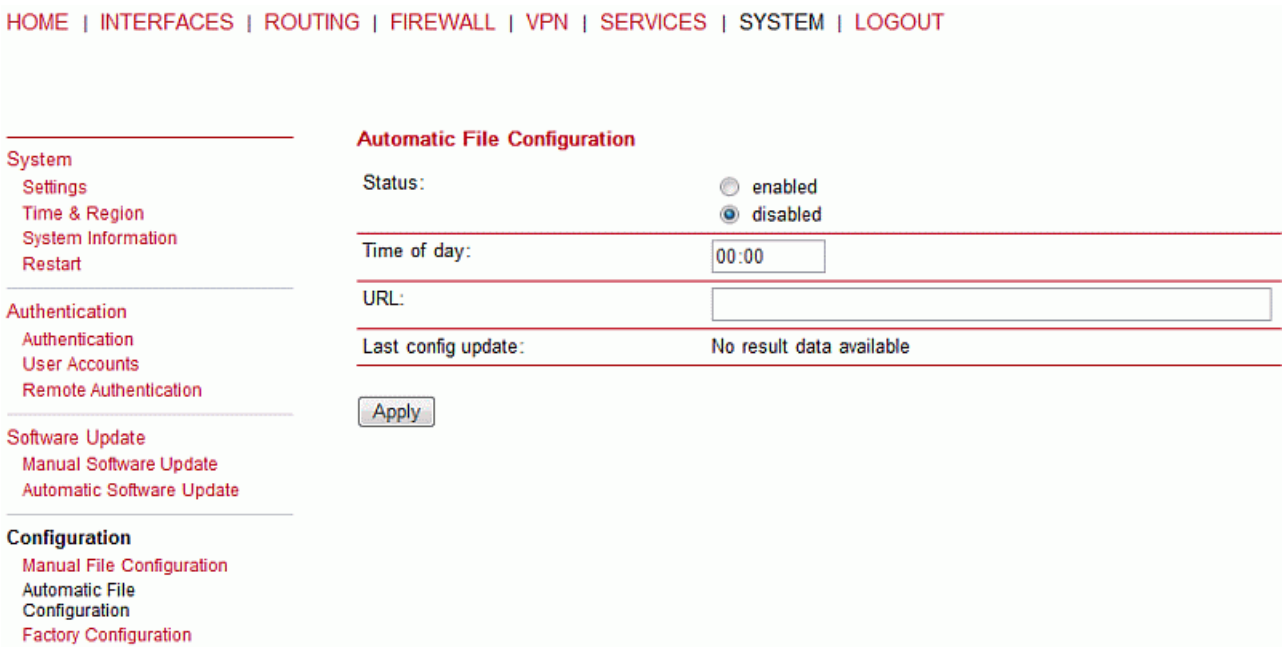
By using this page you can manage the user accounts on the system. The standard admin user is a built-in power user that has permission to access the Web Manager and other administrative services and is used by several services as default user. Keep in mind that the admin password will be also applied to the root user which is able to enter a system shell. Any other user represents a user with lower privileges, for instance it has only permission to view the status page or retrieve status values when using the CLI.



User name:	Define a user name
Enter password:	Define a password
Password confirmation:	Confirm the password

Remote Authentication

A remote RADIUS server can be used to authenticate users. This applies for the Web Manager and other services supporting and incorporating remote authentication.



Administrative status:	Defines whether remote authentication should be used
RADIUS server:	RADIUS server address
RADIUS secret:	Secret used to authenticate against the RADIUS server
Authentication port:	Port used for authentication
Accounting port:	Port used for accounting messages
Use for login:	This option enables remotely-defined users to access the Web Manager

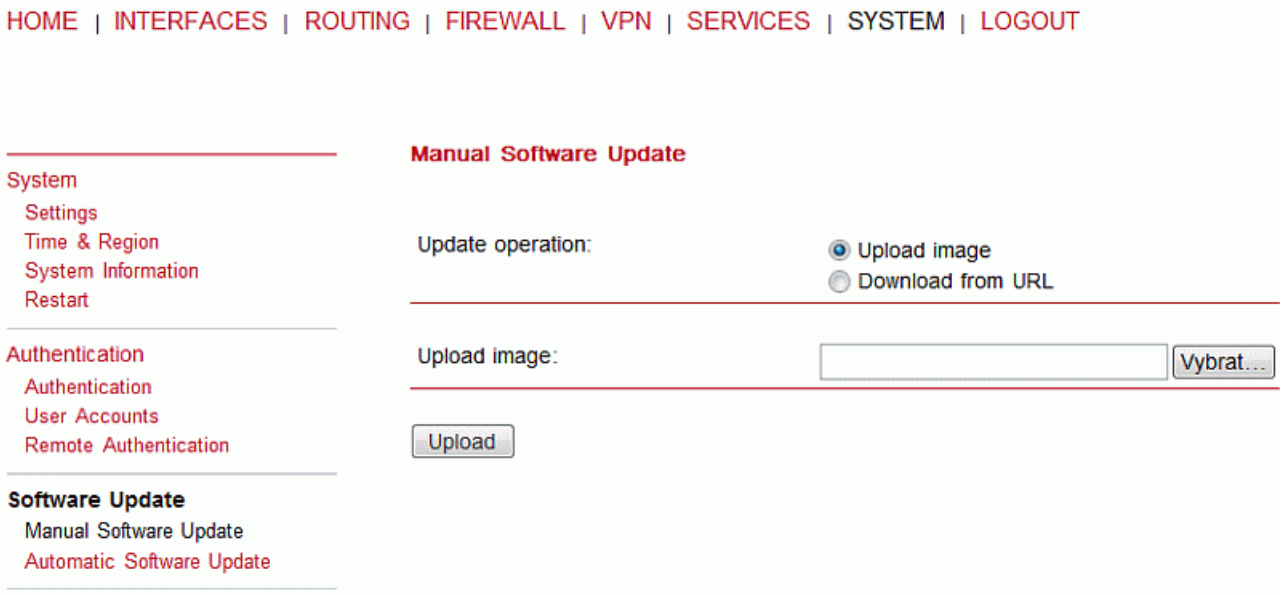
7.7.3. Software Update

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.

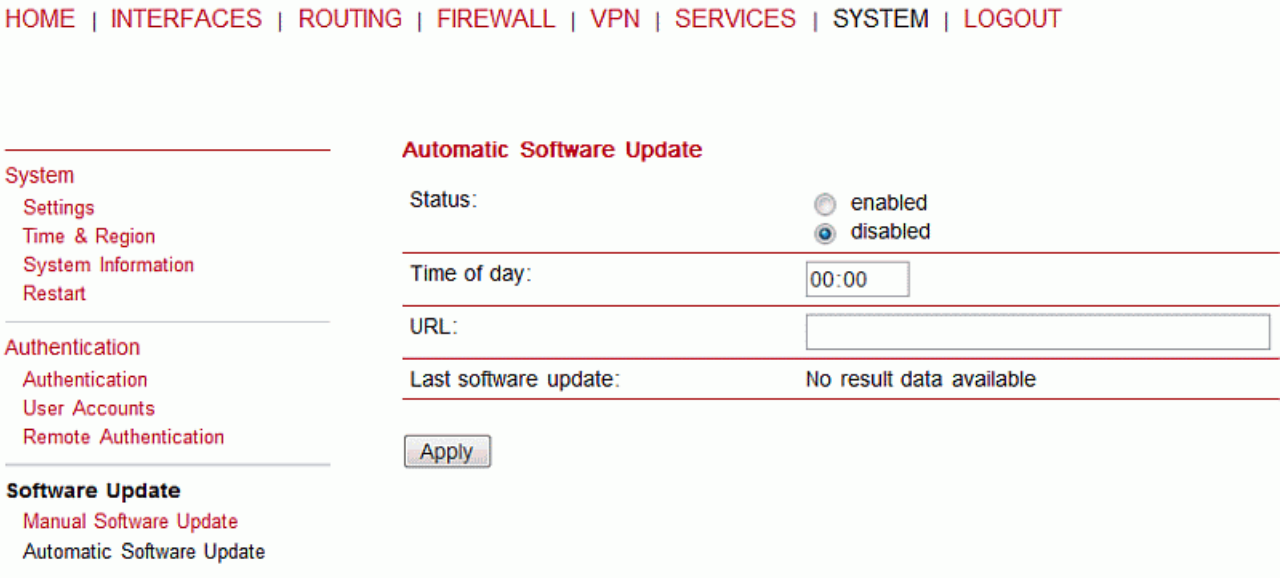
Manual Software Update

This menu can be used to run a manual software update of the system



Update operation	Update operation method being used. You can upload the image, download it from an URL or use the latest version from our server
URL	Server URL where the software update image should be downloaded from. Supported protocols are TFTP, HTTP(s), and FTP

Automatic Software Update



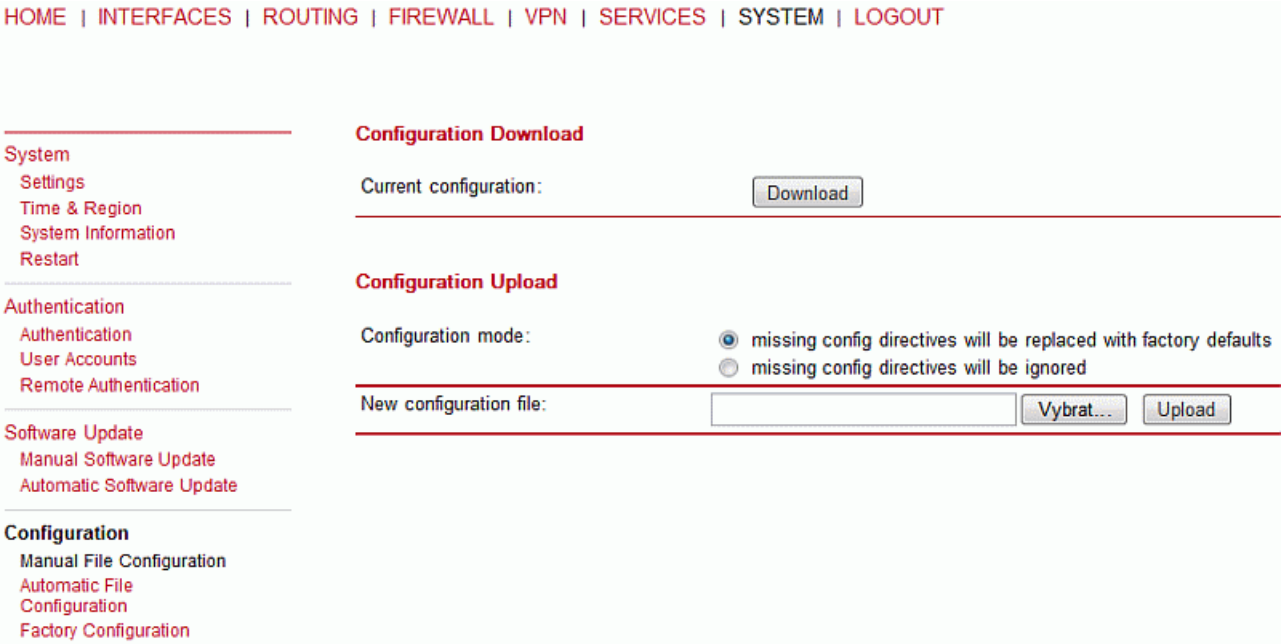
Status:	Enable/disable automatic software update
Time of day:	Every day at this time M!DGE will do a check for updates
URL:	The server URL where the software update package should be downloaded from. Supported protocols are TFTP, HTTP(s), and FTP
Last software update:	Result of the last software update attempt

7.7.4. Configuration

Configuration via the Web Manager becomes tedious for large volumes of devices. M!DGE therefore offers automatic and manual file-based configuration to automate things. Once you have successfully set up the system you can back up the configuration and restore the system with it afterwards. You can either upload a single configuration file (.cfg) or a complete package (.zip) containing the configuration file and a packed version of other essential files (such as certificates).

Manual File Configuration

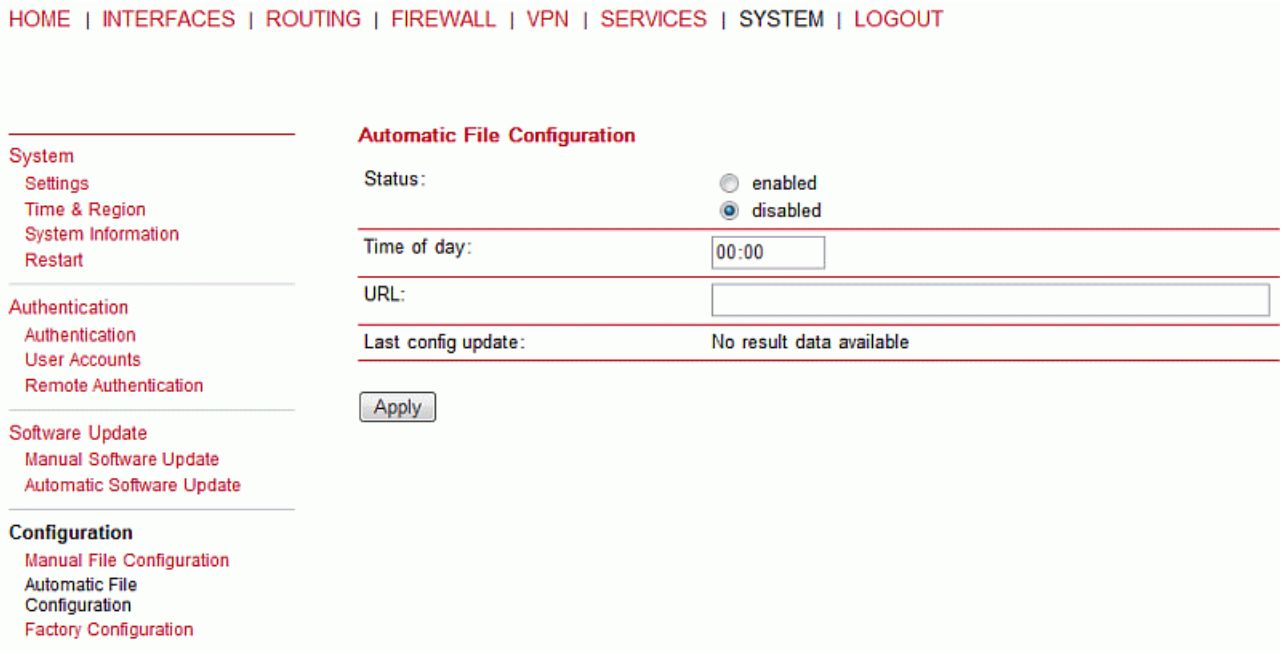
This section can be used to download the currently running system configuration (including essential files such as certificates).



In order to restore a particular configuration you can upload a configuration previously downloaded.

You can choose between missing configuration directives set to factory defaults or getting ignored, that means, potentially existing configuration directives will be kept at the system.

Automatic File Configuration



Status:	Enable/disable automatic configuration update
Time of day:	Time of day when the system will check for updates
URL:	The server URL where the configuration file should be retrieved from (supported protocols are HTTP(s), TFTP, FTP)
Last config update:	Result of the last configuration update attempt

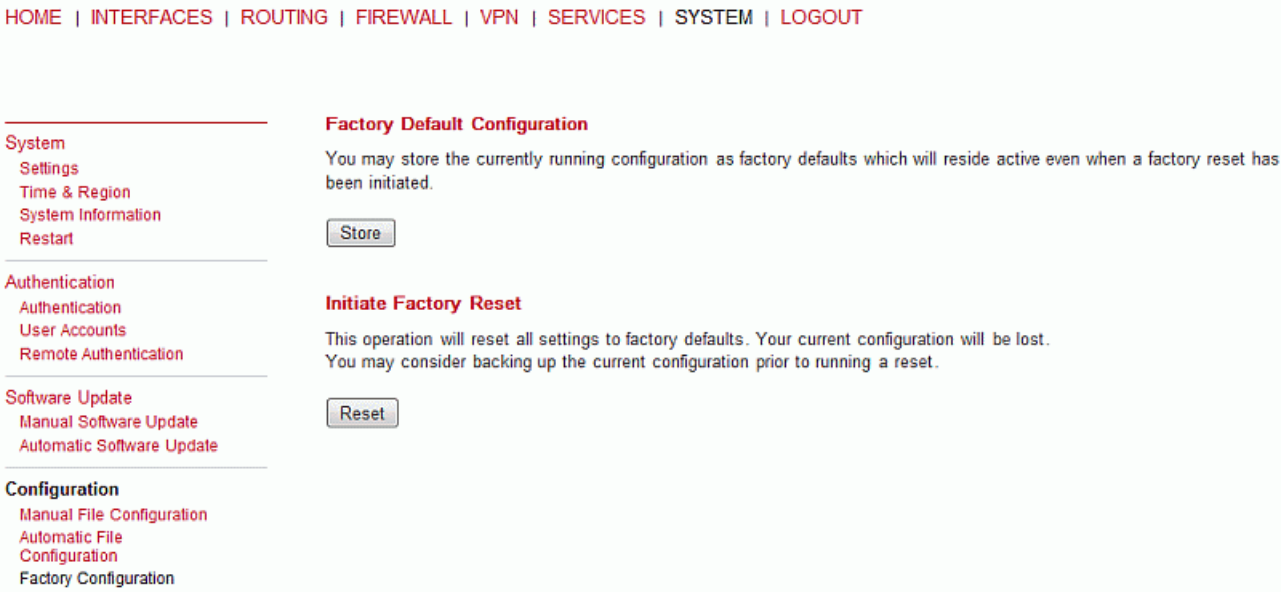
Factory Configuration

This menu can be used to reset the device to factory defaults. Your current configuration will be lost.

This procedure can also be initiated by pressing and holding the Reset button for at least five seconds. A successfully initiated factory reset can be noticed by all LEDs being turned on.

Factory reset will set the IP address of the first Ethernet interface back to 192.168.1.1. You will be able to communicate again with the device using the default network parameters.

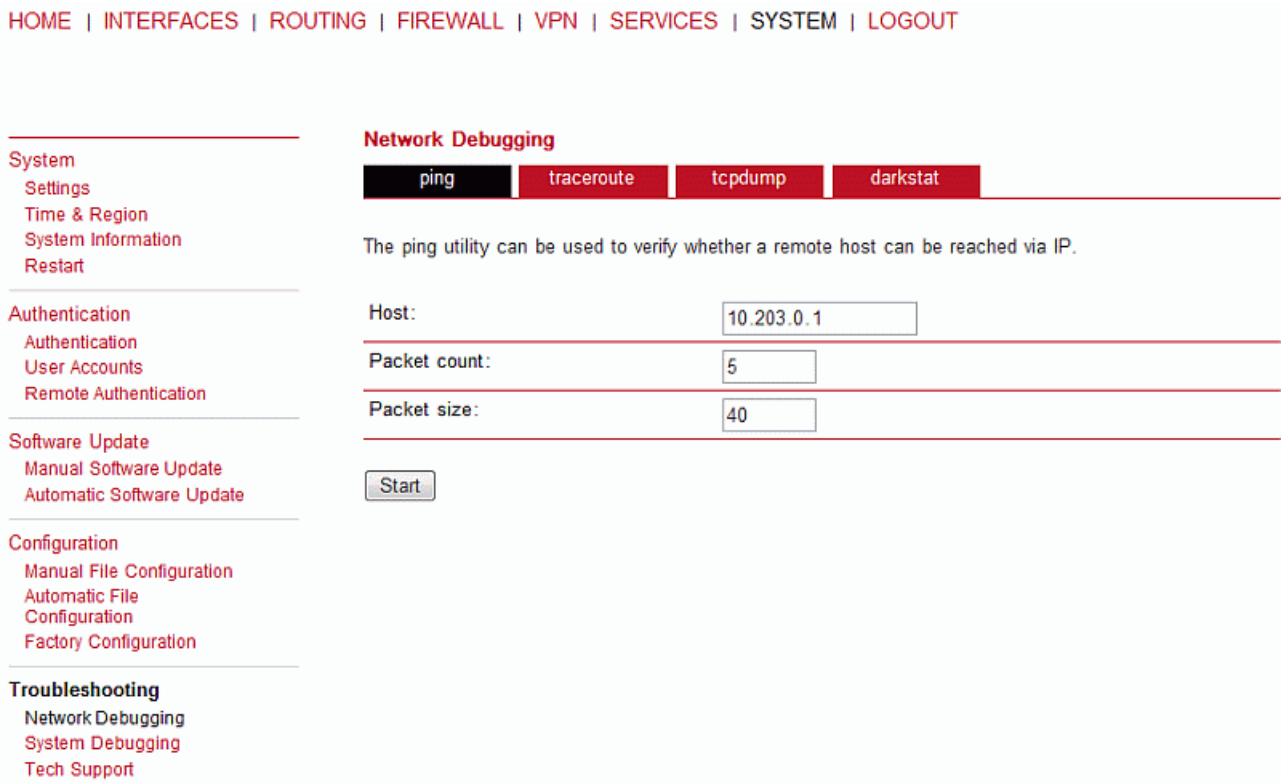
You may store the currently running configuration as factory defaults which will reside active even when a factory reset has been initiated (e.g. by your service staff). Please ensure that this corresponds to a working configuration. A real factory reset to the default settings can be achieved by restoring the original factory configuration and initiating the factory reset again.



7.7.5. Troubleshooting

Network Debugging

Various tools reside on this page for further analysis of potential configuration issues.



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

System
- Settings
- Time & Region
- System Information
- Restart

Authentication
- Authentication
- User Accounts
- Remote Authentication

Software Update
- Manual Software Update
- Automatic Software Update

Configuration
- Manual File Configuration
- Automatic File Configuration
- Factory Configuration

Troubleshooting
- Network Debugging
- System Debugging
- Tech Support

Network Debugging

ping | traceroute | tcpdump | darkstat

The traceroute utility can be used to print the route packets trace to a remote host.

Target host:	192.168.0.2
Time-To-Live:	3
Timeout:	30

Start

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

System
- Settings
- Time & Region
- System Information
- Restart

Authentication
- Authentication
- User Accounts
- Remote Authentication

Software Update
- Manual Software Update
- Automatic Software Update

Configuration
- Manual File Configuration
- Automatic File Configuration
- Factory Configuration

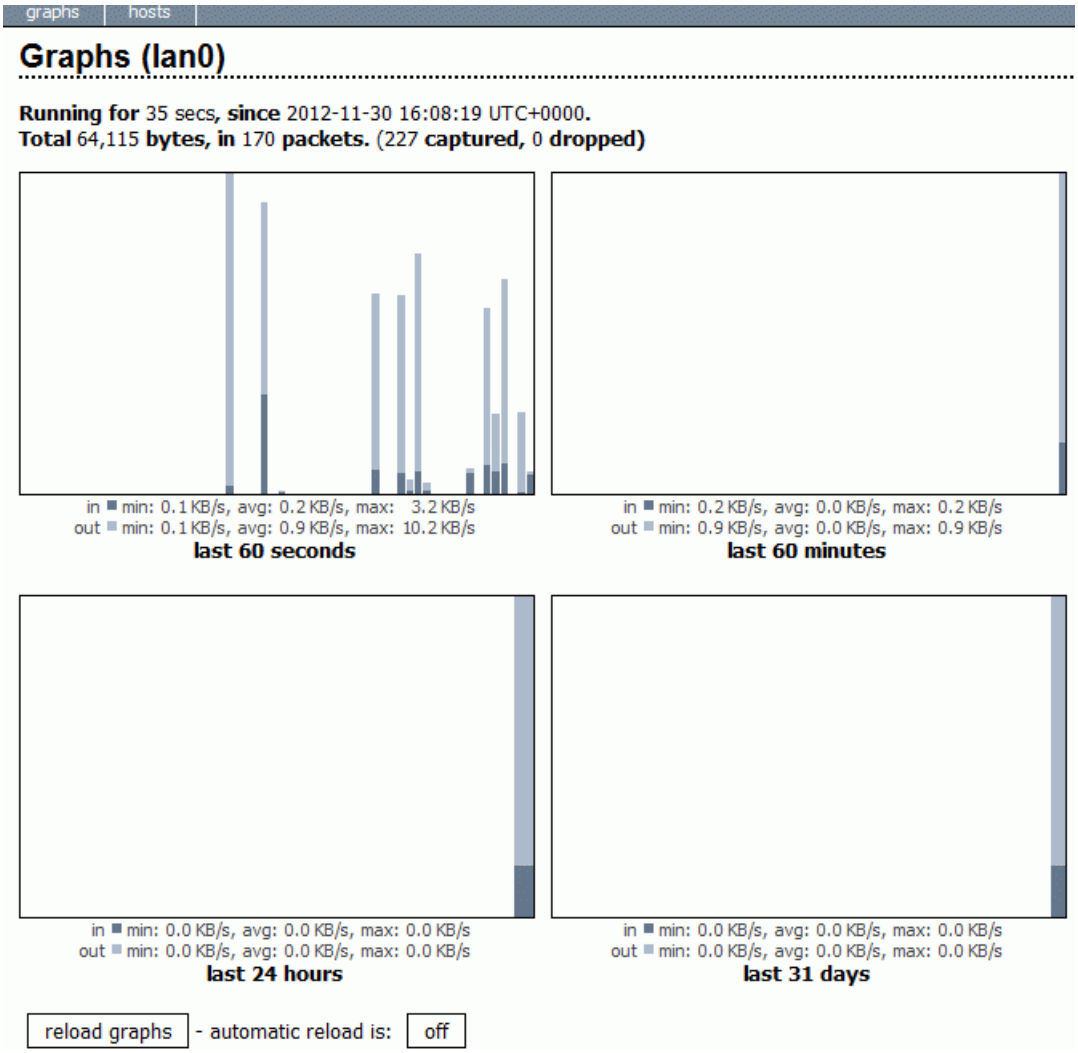
Troubleshooting
- Network Debugging
- System Debugging
- Tech Support

Network Debugging

ping | traceroute | tcpdump | darkstat

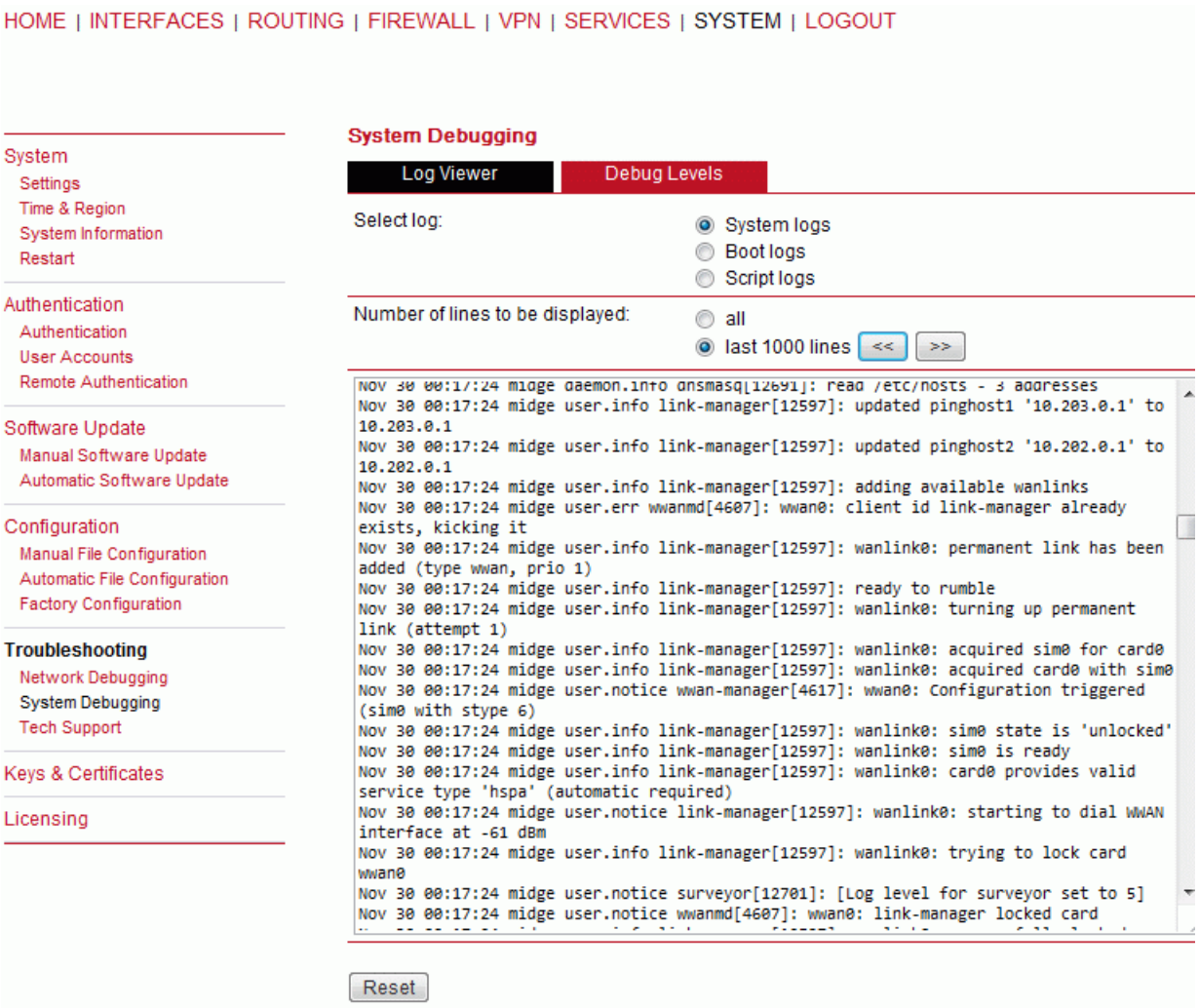
```
tcpdump: listening on wwan0, link-type LINUX_SLL (Linux cooked), capture size 1500 bytes
14 packets received by filter
0 packets dropped by kernel


Captured 14 packets
```

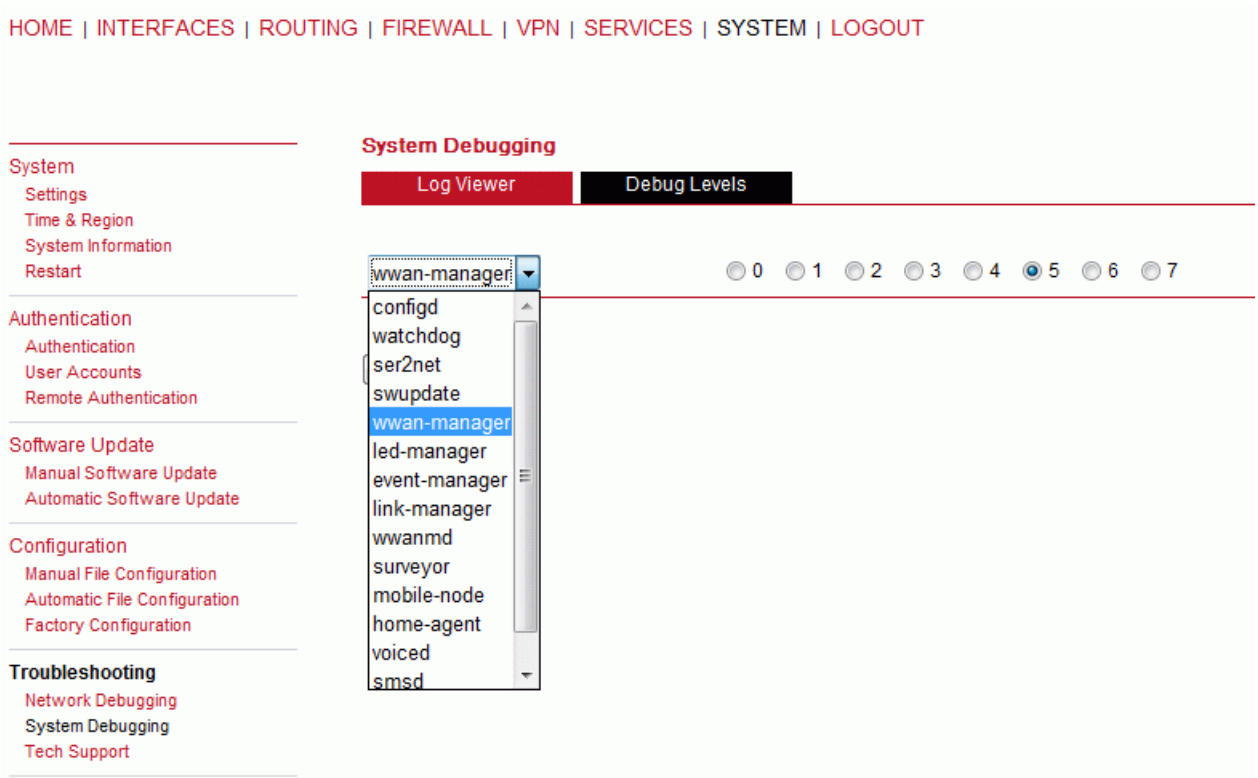
Run again Download



System Debugging

Log files can be viewed, downloaded and reset here. Please study them carefully in case of any issues.


HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT
System
Settings
Time & Region
System Information
Restart
Authentication
Authentication
User Accounts
Remote Authentication
Software Update
Manual Software Update
Automatic Software Update
Configuration
Manual File Configuration
Automatic File Configuration
Factory Configuration
Troubleshooting
Network Debugging
System Debugging
Tech Support
Keys & Certificates
Licensing
System Debugging
Log Viewer
Debug Levels
Select log:
System logs
Boot logs
Script logs
Number of lines to be displayed:
all
last 1000 lines
<<
>>
Nov 30 00:17:24 midge daemon.info dnsmasq[12691]: read /etc/hosts - 3 addresses
Nov 30 00:17:24 midge user.info link-manager[12597]: updated pinghost1 '10.203.0.1' to 10.203.0.1
Nov 30 00:17:24 midge user.info link-manager[12597]: updated pinghost2 '10.202.0.1' to 10.202.0.1
Nov 30 00:17:24 midge user.info link-manager[12597]: adding available wanlinks
Nov 30 00:17:24 midge user.err wwanmd[4607]: wwan0: client id link-manager already exists, kicking it
Nov 30 00:17:24 midge user.info link-manager[12597]: wanlink0: permanent link has been added (type wwan, prio 1)
Nov 30 00:17:24 midge user.info link-manager[12597]: ready to rumble
Nov 30 00:17:24 midge user.info link-manager[12597]: wanlink0: turning up permanent link (attempt 1)
Nov 30 00:17:24 midge user.info link-manager[12597]: wanlink0: acquired sim0 for card0
Nov 30 00:17:24 midge user.info link-manager[12597]: wanlink0: acquired card0 with sim0
Nov 30 00:17:24 midge user.notice wwan-manager[4617]: wwan0: Configuration triggered (sim0 with stype 6)
Nov 30 00:17:24 midge user.info link-manager[12597]: wanlink0: sim0 state is 'unlocked'
Nov 30 00:17:24 midge user.info link-manager[12597]: wanlink0: sim0 is ready
Nov 30 00:17:24 midge user.info link-manager[12597]: wanlink0: card0 provides valid service type 'hspa' (automatic required)
Nov 30 00:17:24 midge user.notice link-manager[12597]: wanlink0: starting to dial WWAN interface at -61 dBm
Nov 30 00:17:24 midge user.info link-manager[12597]: wanlink0: trying to lock card wwan0
Nov 30 00:17:24 midge user.notice surveyor[12701]: [Log level for surveyor set to 5]
Nov 30 00:17:24 midge user.notice wwanmd[4607]: wwan0: link-manager locked card
Reset


HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT
System
Settings
Time & Region
System Information
Restart
Authentication
Authentication
User Accounts
Remote Authentication
Software Update
Manual Software Update
Automatic Software Update
Configuration
Manual File Configuration
Automatic File Configuration
Factory Configuration
Troubleshooting
Network Debugging
System Debugging
Tech Support
System Debugging
Log Viewer
Debug Levels
wwan-manager
0 1 2 3 4 5 6 7
configd
watchdog
ser2net
swupdate
wwan-manager
led-manager
event-manager
link-manager
wwanmd
surveyor
mobile-node
home-agent
voiced
smsd

Default debugging levels for individual daemons are as follows:

- configd – 0
- watchdog – 4
- ser2net – 4
- swupdate – 5
- led-manager – 5
- event-manager – 5
- link-manager – 6
- wwanmd – 5
- surveyor – 5
- mobile-node – 4
- home-agent – 4
- voiced – 4
- smsd – 5
- sdkhost – 5

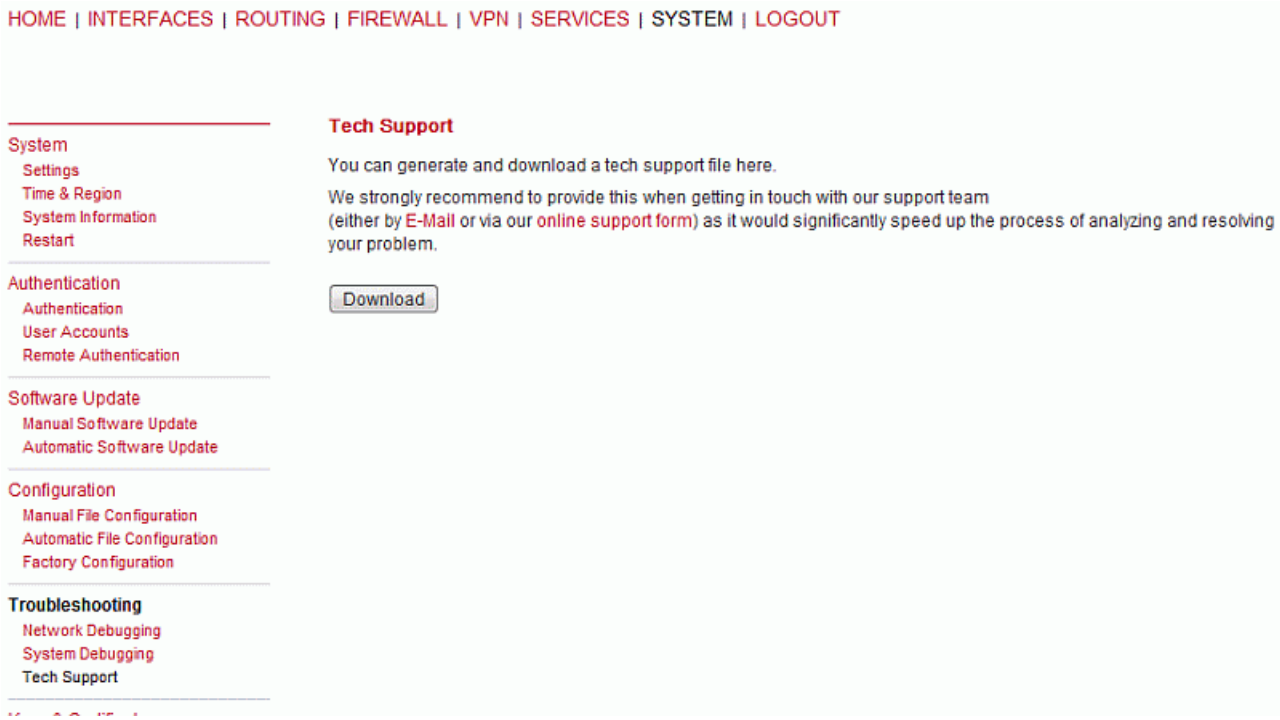
Tech Support

You can generate and download a tech support file here.

We strongly recommend providing this file when getting in touch with our support team, either by e-mail or via our online support form, as it would significantly speed up the process of analyzing and resolving your problem.

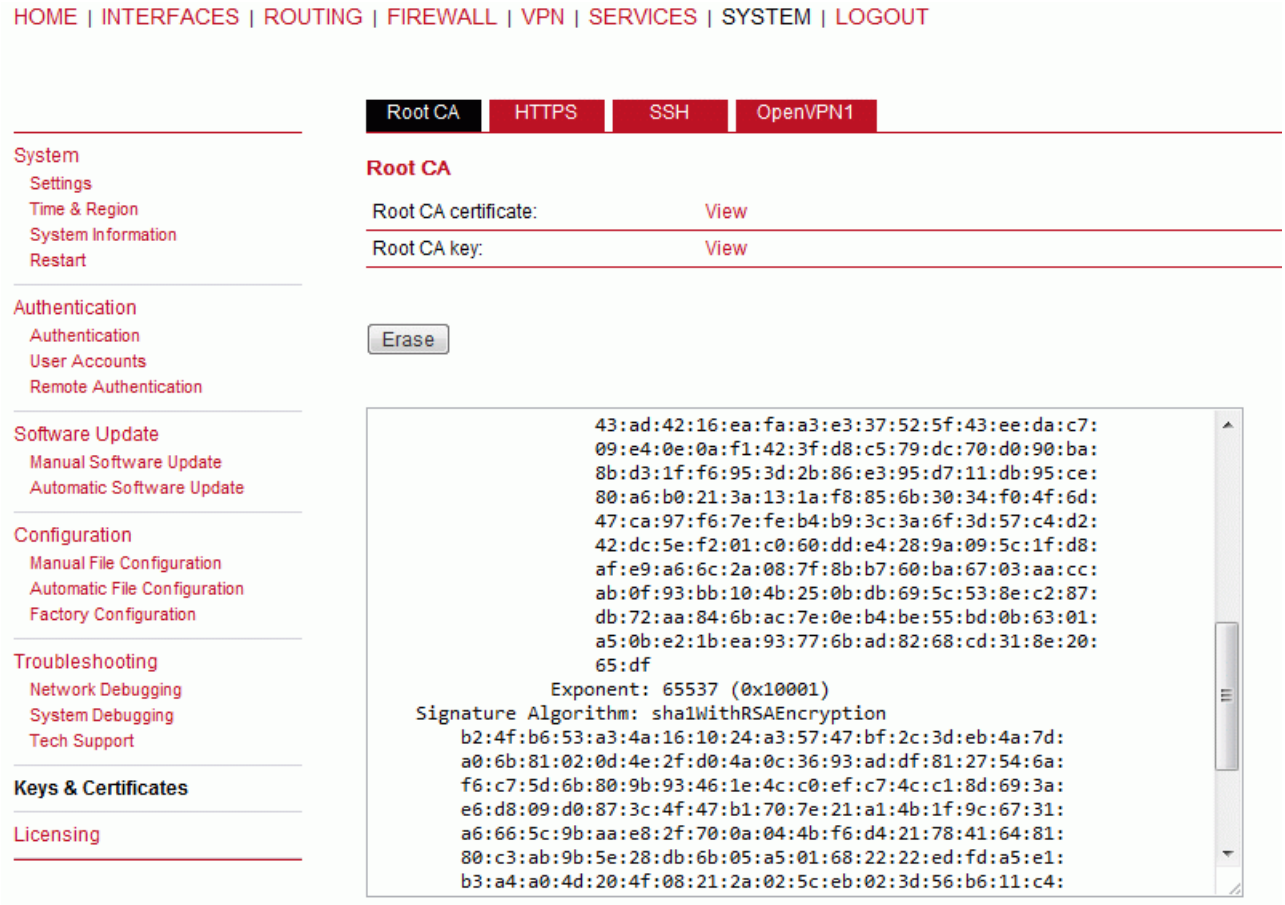
Note

For both direct E-mail and Online support form a connection to the Internet has to be available.



7.7.6. Keys & Certificates

The key and certificate page lets you generate required files for securing your services (such as the HTTP and SSH server). Keep in mind that you will need to create keys and certificates for OpenVPN in case of certificate based authentication. You can also revoke and invalidate certificates again (for instance if they have been compromised or lost).



The following terms are used:

Root CA	The root Certificate Authority (CA) which issues certificates, its key can be used to certify it at trusted third party on other systems
Certificate	Corresponds to a digital certificate which uses a signature to bind a public key with an identity
Key	Corresponds to an either public or private key
CSR	Certificate Signing Request, which can be used to sign a certificate by a third party authority
P12	PKCS12 container format which can include certificates and keys protected by password
RSAThe certificate owner's location	An encryption algorithm based on the fact that factorization of large integers is difficult
DSS/DSA	An encryption algorithm based on the discrete logarithm problem

Phrase	A password used for protecting keys

A single certificate can obtain the following ASN.1 attributes:

CN The certificate owner's common name, mainly used to identify a host

C The certificate owner's country (usually a TLD abbreviation)

ST The certificate owner's state

L The certificate owner's location

C The certificate owner's country

O The certificate owner's organization

OU The name of the organizational unit to which the certificate issuer belongs

E The certificate owner's email address

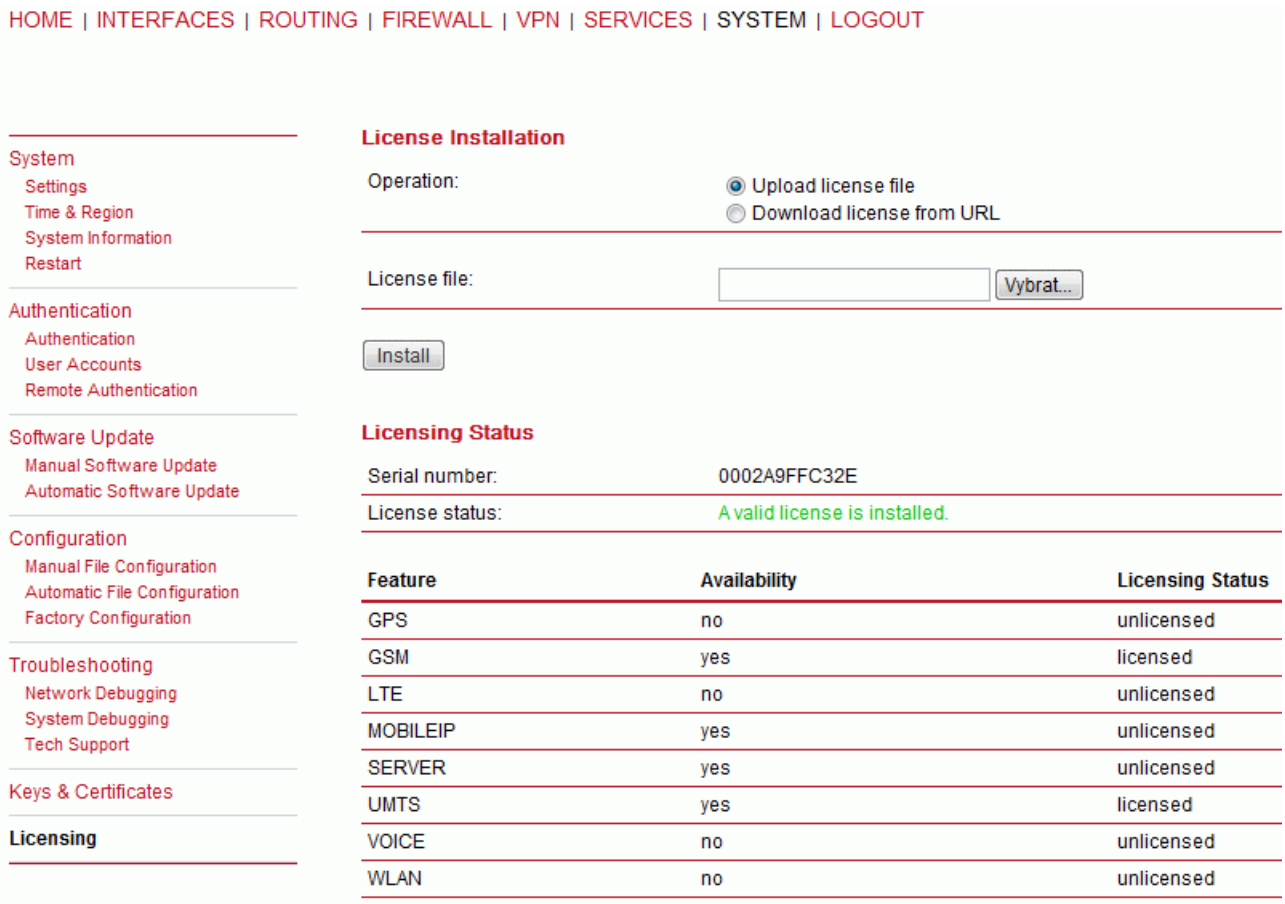
Those attributes form a so-called subject name, mainly used for matching a certificate or when signing certificate requests:

```
Subject: C=CZ, ST=Czech Republic, L=Czech Republic, O=RACOM, OU=Networking,
CN=midge/emailAddress=support@racom.eu
```

Depending on your configuration, keys and certificates may be used for particular services, for instance if OpenVPN uses a certificate-based authentication or if you want to access the Web Manager over HTTPS. Please note that an accurate system time is needed prior to creating certificates as it influences the lifetime of a certificate. The validity period is usually set to 10 years. You can further revoke and invalidate client certificates again (for instance if they have been compromised or lost).

7.7.7. Licensing

This menu allows you to view and update the license status of your system. Note that some features are disabled if no valid license is provided.



Availability means that the license should be able to aloow this funcionality for the actual HW.

7.8. LOGOUT

Log out from Web Manager.

8. Command Line Interface

The Command Line Interface (CLI) offers a unified control interface to the router and can be used to get/set configuration parameters, apply updates, restart services or perform other system tasks.

The CLI should be started using **cli -i** command from system shell or when logging as root user. A list of available commands can be displayed by running **cli -l**. It will be started automatically in interactive mode when logging in as *admin* user.

```
~ $ cli
Name:
          cli (Command Line Utility)

Usage:
          [-ilh] <command>
```

```
~ $ cli -i
MIDGE Command Line Interface (version 0.1)
(C) Copyright RACOM s.r.o, Czech Republic

Enter 'help' for a list of available commands
or hit the TAB key for auto-completion.

Ready to serve.

>
```

The CLI supports TAB completion, that is expanding entered words or fragments by hitting the TAB key at any time. This applies to commands but also to arguments and generally offers a convenient way for working on the shell.

Please note that each CLI session will perform an automatic logout as soon as a certain time of inactivity (10 minutes by default) have been reached. It can be turned off by the command `no-autologout`.

The CLI can be exited by running `exit`.

8.1. General Usage

When operating the `CLI` in interactive mode, each entered command will be executed by the `RETURN` key. You can use the `Left` and `Right` keys to move the current point between entered characters or use the `Up` and `Down` keys to search the history of entered commands. Pressing `CTRL-c` twice or `CTRL-d` on an empty command line will exit the `CLI`.

List of supported key sequences:

Key Sequence	Action
CTRL-a	Move to the start of the current line.
CTRL-e	Move to the end of the line.
CTRL-f	Move forward a character.

Key Sequence	Action
CTRL-b	Move back a character.
ALT-f	Move forward to the end of the next word.
ALT-b	Move back to the start of the current or previous word.
CTRL-l	Clear the screen leaving the current line at the top of the screen, with an argument given refresh the current line without clearing the screen.
CTRL-p	Fetch the previous command from the history list, moving back in the list.
CTRL-n	Fetch the next command from the history list, moving forward in the list.
ALT-<	Move to the first line in the history.
ALT->	Move to the end of the input history.
CTRL-r	Search backward starting at the current line and moving up through the history.
CTRL-s	Session will be frozen.
CTRL-q	Reactivate frozen session.
CTRL-d	Delete character at point or exit CLI if at the beginning of the line.
CTRL-t	Drag the character before point forward moving point forward as well. If point is at the end of the line, then this transposes the two characters before point.
ALT-t	Drag the word before point past the word after point, moving point over that word as well. If point is at the end of the line, this transposes the last two words on the line.
CTRL-k	Delete the text from point to the end of the line.
CTRL-y	Yank the top of the deleted text into the buffer at point.

Please note, that it can be required to apply quotes (") when entering commands with arguments containing whitespaces.

The following sections are trying to explain the available commands.

8.2. Print Help

The `help` command can be used to get the list of available commands when called without arguments, otherwise it will print the usage of the specified command.

```
> help
Usage:
          help [<command>]

Available commands:

          get                  Get config parameters
          set                  Set config parameters
          status               Get status information
          send                 Send message or mail
          update               Update system facilities
          restart              Restart service
          reset                Reset system to factory defaults
          reboot               Reboot system
```

```
          shell                Run shell command
          help                 Print help for command
          no-autologout       Turn off auto-logout
          exit                 Exit
```

8.3. Getting Config Parameters

The **`get`** command can be used to get configuration values (not the current values).

```
> get -h
Usage:
          get [-hsvlc] <parameter> [<parameter>..]

Options:
          -s      generate sourceable output
          -v      validate config parameter
          -l      use legacy syntax with '&' separator
          -c      show configuration sections (can match a pattern)
```

See the following example for reading configuration DIO values:

```
> get dio.out1
dio.out1=on
> get dio.out2
dio.out2=on
```

8.4. Setting Config Parameters

The **`set`** command can be used to set configuration values.

```
> set -h
Usage:
          set [-hvl] <parameter>=<value> [<parameter>=<value>..]

Options:
          -v      validate config parameter
          -l      use legacy syntax with '&' separator
```

See the following example for setting configuration digital output values. Both values will be "off" and both values will be also "off" after the next start-up procedure.

```
> set dio.out1=off
> set dio.out2=off
```

8.5. Getting Status Information

The **status** command can be used to get various status information of the system.

```
> status -h
Usage:
          status [-hs] <section>

Options:
          -s      generate sourceable output

Available sections:

          config              Current configuration
          summary             Short status summary
          system              System information
          license             License information
          wwan                WWAN module status
          wlan                WLAN module status
          gnss                GNSS (GPS) module status
          lan                 LAN interface status
          wan                 WAN interface status
          openvpn             OpenVPN connection status
          ipsec               IPsec connection status
          pptp                PPTP connection status
          dialin              Dial-In connection status
          dio                 Digital IO status
          neigh               Neighborhood status
          location            Current Location
```

In the following example, we read the current DIO values. Remember that the current states do not correspond to the configuration values set with "set dio.out" commands.

```
> status dio
=== DIGITAL IO INFORMATION ===
IN1:                            off
IN2:                            on
OUT1:                           on
OUT2:                           off
```

8.6. Sending E-Mail or SMS

The **send** command can be used to send a message via E-Mail/SMS to the specified address or phone number.

```
> send -h
Name:
          cli-send (Send message or mail)

Usage:
          send [-h] <type> <dest> <msg>

Options:
          <type>      type of message to be sent (mail or sms)
```

```
          <dest>      destination of message (mail-address or phone-number)
          <msg>       message to be sent
```

8.7. Updating System Facilities

The **update** command can be used to perform various system updates.

```
> update -h
Usage:
          update [-hr] <software|config|license|sshkeys> <URL>

Options:
          -r       reboot after update

Available actions:
          software           Perform software update
          config             Update configuration
          license            Update licenses
          sshkeys            Install SSH authorized keys

You may run 'update software latest' to install the latest version.
```

8.8. Restarting Services

The **restart** command can be used to restart system services.

```
> restart -h
Usage:
          restart [-h] <service>

Available services:

          link-manager           WAN links
          wwan-manager           WWAN manager
          wlan WLAN              interfaces
          network                Networking
          dnsmasq                DNS/DHCP server
          configd                Configuration daemon
          firewall               Firewall and NAPT
          lighttpd               HTTP server
          openvpn                OpenVPN connections
          ipsec                  IPsec connections
          pptp                   PPTP connections
          snmpd                  SNMP daemon
          syslog                 Syslog daemon
          telnet                 Telnet server
          dropbear               SSH server
          vrrpd                  VRRP daemon
          usbipd                 USB/IP daemon
          surveyor               Supervision daemon
```

```
          voiced                  Voice daemon
          gpsd                    GPS daemon
          smsd                    SMS daemon
```

8.9. Resetting System

The **reset** command can be used to reset the router back to factory defaults.

```
> reset -h
Usage:

          reset [-h ]
```

8.10. Rebooting System

The **reboot** command can be used to reboot the router.

```
> reboot -h
Usage:

          reboot [-h]
```

8.11. Running Shell Commands

The **shell** command can be used to execute a system shell and run any arbitrary application.

```
> shell -h
Usage:

          shell [-h] [<cmd>]
```

8.12. CLI–PHP

CLI-PHP, an HTTP frontend to the CLI application, can be used to configure and control the router remotely. It is enabled in factory configuration, thus can be used for deployment purposes, but disabled as soon as the admin account has been set up. The service can later be turned on/off by setting the cliphp.status configuration parameter:

```
> get cliphp.status
cliphp.status=0

>set cli.php.status=1
> get cliphp.status
cliphp.status=1
```

```
          cliphp.status=0           Service is disabled
          cliphp.status=1           Service is enabled
```

This section describes the CLI-PHP interface for Version 2, the general usage is defined as follows:

```
Usage:
    http (s):://cli.php?<key1>=<value1>&<key2>=<value2>..<keyN>=<
    valueN>
Available keys:
output             Output format ( html, plain )
usr                Username to be used for authentication
pwd                Password to be used for authentication
commandV           Command to be executed
arg0..arg31        Arguments passed to commands
Notes:
    The commands correspond to CLI commands as seen by 'cli -l', the
    arguments
   (arg0..arg31) will be directly passed to the cli application

    Thus, an URL containing the following sequence:

      command=get&arg0=admin.password&arg1=admin.debug&arg2=admin.access

   will lead to cli being called as:

    $ cli get "admin.password" "admin.debug" "admin.access"

    It supports whitespaces but please be aware that any special
    characters in the URL
    must be specified according to RFC1738 (which usually done by
    common clients such
    as wget, lynx, curl).

Response:
    The returned response will always contain a status line in the
    format:

    <return>: <msg>

    with return values of OK if succeeded and ERROR if failed. Any
    output
    from the commands will be appended

Examples:

    OK: status command successful
    ERROR: authentication failed
```

status – Display status information

```
Key usage:
        command=status[&arg0=<section>]
Notes:
        Available sections can be retrieved by running command=
        status&arg0=-h.
        System status can be displayed without authentication.
```

```
Examples:

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=status&arg0=-h
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=status&arg0=summary
http://192.168.1.1/cli.php?version=2&output=html&command=status
```

get – Get configuration parameter

```
Key usage:

        command=get&arg0=<config-key>[&arg1=<config-key>..]

Examples:

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=get&arg0=config.version

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=get&arg0=openvpn.status&arg1=snmp.status&arg2=ipsec.status
```

set – Set configuration parameter

```
Key usage:
     command=set&arg0=<config-key>&arg1=<config-value>[&arg2=<config
     -key>&arg3=<config-value>..]
Notes :
     In contrast to the other commands, this command requires a set
     of tuples because of the reserved '=' char, i.e.
     [arg0=key0, arg1=val0], [arg2=key1, arg3=val1], [arg4=key2, arg5=val2], etc

Examples:


http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=set&arg0=snmp.status&arg1=1

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=set&arg0=snmp.status&arg1=0&arg2=openvpn.status&arg3=1
```

restart – Restart a system service

```
Key usage:
     command=restart&arg0=<service>
Notes:
     Available services can be retrieved by running 'command=restart&arg0=-h'

Examples:
```

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=restart&arg0=-h

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=restart&arg0=link-manager
```

reboot - Trigger system reboot

```
Key usage :
     command=reboot

Examples :


http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=reboo
```

reset - Run factory reset

```
Key usage :
     command=reset

Examples :


http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=reset
```

update - Update system facilities

```
Key usage :
     command=update&arg0=<facility>&arg1=<URL>
Notes :
     Available facilities can be retrieved by running 'command=update
&arg0=-h'

Examples:

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=127
admin01&command=update&arg0=software&arg1=tftp://192.168.1.254/latest

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=update&arg0=config&arg1=tftp://192.168.1.254/user-
config.zip

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=update&arg0=license&arg1=http://192.168.1.254/xxx.lic
```

9. Troubleshooting

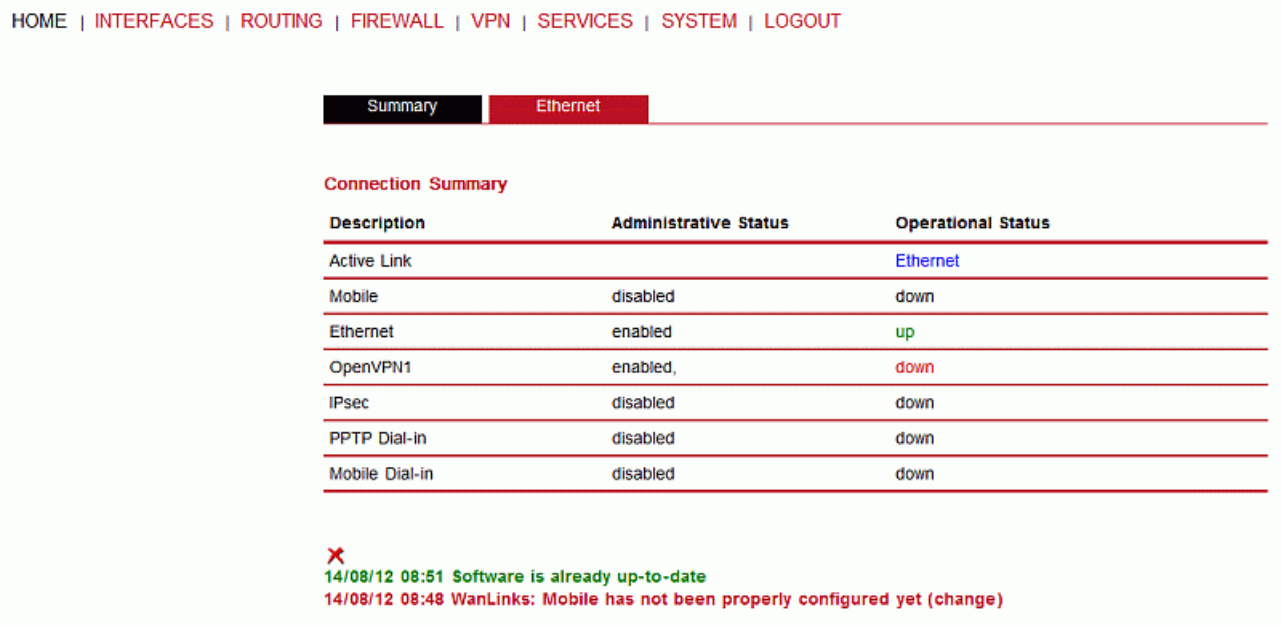
9.1. Common Errors

With GPRS/UMTS connection (even if GSM signal good enough) folowing Errors are common:

SIM missing	Check status of SIM card on menu INTERFACES-SIM- Configuration and Insert/re-insert a SIM card and perform a power cycle
PIN code required	Insert the PIN code on menu INTERFACES-SIM- Configuration
Connection not established or failed	Insert the PIN code on menu INTERFACES-SIM- Configuration
Connection not established or failed	See the SYSTEM-Troubleshooting-Log Files-Debug Log under Check APN, phone number, username, password

9.2. Messages

The Web Manager displays messages in the status bar in the footer of a web page.



There are three levels:

Green	Action was succesful – an informative message with several important actions informing about positive result.
Yellow	Warning – please consider the information.
Red	Error – command was not performed, typically with recommended action which is required before the possible succesful action.

9.3. Troubleshooting tools

9.3.1. Pinger

Connection from the M!DGE router you can check using a build in pinger available in **SYSTEM-Troubleshooting - Network Debugging**.

Traceroute command is availablein the same menu for tracing the packets from the M!DGE router to the Host.

9.3.2. Log Files

Information about boot up process and about running proceses you can find in Linux like Logfiles **- menu SYSTEM -Troubleshooting - Log Files**.

10. Safety, environment, licensing

10.1. 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 utilisation 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 keep your exposure to electromagnetic fields below the legal limits. This distance applies to Lambda/4 and Lambda/2 antennas. Larger distances apply for antennas with higher gain.

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

10.1.1. Declaration of Conformity

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

10.1.2. RoHS and WEEE compliance

The M!DGE 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).

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 council 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.

10.2. Warranty

RACOM-supplied parts or equipment ("equipment") is covered by warranty for inherently faulty parts and workmanship for a warranty period as stated in the delivery documentation from the date of dispatch to the customer. The warranty does not cover custom modifications to software. During the warranty period RACOM shall, on its option, fit, repair or replace ("service") faulty equipment, always provided that malfunction has occurred during normal use, not due to improper use, whether deliberate or accidental, such as attempted repair or modification by any unauthorised person; nor due to the action of abnormal or extreme environmental conditions such as overvoltage, liquid immersion or lightning strike.

Any equipment subject to repair under warranty must be returned by prepaid freight to RACOM direct. The serviced equipment shall be returned by RACOM to the customer by prepaid freight. If circumstances do not permit the equipment to be returned to RACOM, then the customer is liable and agrees to reimburse RACOM for expenses incurred by RACOM during servicing the equipment on site. When equipment does not qualify for servicing under warranty, RACOM shall charge the customer and be reimbursed for costs incurred for parts and labour at prevailing rates.

This warranty agreement represents the full extent of the warranty cover provided by RACOM to the customer, as an agreement freely entered into by both parties.

RACOM warrants the equipment to function as described, without guaranteeing it as befitting customer intent or purpose. Under no circumstances shall RACOM's liability extend beyond the above, nor shall RACOM, its principals, servants or agents be liable for any consequential loss or damage caused directly or indirectly through the use, misuse, function or malfunction of the equipment, always subject to such statutory protection as may explicitly and unavoidably apply hereto.

Appendix A. 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

Index

A
accessories, 19
antenna
  GSM/UMTS, 21
  mounting, 23
autentication, 80

B
basic setup, 22

C
certificates, 90
CLI, 94
client
  e-mail, 65
Command Line Interface, 94
configuration, 24
conformity, 105
connecting M!DGE, 21
connectors
  Antenna SMA, 12
  ETH RJ45, 13
  screw terminal, 13
  USB, 13

D
declaration of conformity, 105
demo case, 20
digital I/O, 37
dimensions, 12
dynamic DNS, 64

E
e-mail, 65
ethernet, 27
event manager, 66

F
F bracket, 19
factory reset, 84
features, 17
  key features, 7
file configuration, 83
firewall, 42

G
glossary, 107
grounding, 23

H
home, 24

I
implementation notes, 11
indication LEDs, 15
information
  system information, 78
installation, 23
interfaces, 25
IPsec, 49

K
keys, 90

L
LAN cable, 21
LED, 15
licensing, 91
logout, 93

M
menu
  firewall, 42
  home, 24
  interfaces, 25
  logout, 93
  routing, 38
  services, 54
  system, 77
  troubleshooting, 85
  VPN, 46
mobile, 30
models, 19

O
offerings, 19

P
power supply, 23
  connect, 21
product
  Conformity, 105

R
redundancy, 75
reset, 84
ROHS, 106
router, 7
routing, 38

S

safety instructions, 105
serial port, 34
server
  DHCP, 63
  dial-in, 53
  DNS proxy, 63
  PPTP, 52
  SSH/Telnet, 71
  web, 74
services, 54
SIM, 30
SIM card, 21
SMS, 68
SNMP agent, 72
software update, 81
specification, 17
standards, 8
start, 6
system, 77
  information, 78
  restart, 79
  setings, 77

T

technical specification, 17
time&region, 77
troubleshooting, 85, 103

U

update, 81
USB, 33

V

VPN, 46

W

WAN, 25
web configuration, 24
WEEE, 106

Appendix B. Revision History

Revision 1.1 2012-10-09
1. XML version

Revision 1.2 2012-12-07
Updated chapter 7 for FW version 3.6.40.x

Revision 1.3 2012-12-12
Updated chapter 8 – Command Line Interface