NetModule Router NB800

User Manual for Software Version 99.99

Manual Version 1.13

NetModule AG, Switzerland

October 9, 2023

NetModule Router NB800

This manual covers all variants of the *NB800* product type.

The specifications and information regarding the products in this manual are subject to change without notice. We would like to point out that NetModule makes no representation or warranties with respect to the contents herein and shall not be responsible for any loss or damage caused to the user by the direct or indirect use of this information This document may contain information about third party products or processes. Such third party information is generally out of influence of NetModule and therefore NetModule shall not be responsible for the correctness or legitimacy of this information. Users must take full responsibility for their application of any products.

Copyright ©2023 NetModule AG, Switzerland All rights reserved

This document contains proprietary information of NetModule. No parts of the work described herein may be reproduced. Reverse engineering of the hardware or software is prohibited and protected by patent law. This material or any portion of it may not be copied in any form or by any means, stored in a retrieval system, adopted or transmitted in any form or by any means (electronic, mechanical, photographic, graphic, optic or otherwise), or translated in any language or computer language without the prior written permission of NetModule.

A large amount of the source code to this product is available under licenses which are both free and open source. Most of it is covered by the GNU General Public License which can be obtained from www.gnu.org. The remainder of the open source software which is not under the GPL, is usually available under one of a variety of more permissive licenses. A detailed license information for a particular software package can be provided on request.

All other products or company names mentioned herein are used for identification purposes only and may be trademarks or registered trademarks of their respective owners. The following description of software, hardware or process of NetModule or other third party provider may be included with your product and will be subject to the software, hardware or other license agreements.

Contact

https://support.netmodule.com

NetModule AG	Tel +41 31 985 25 10
Maulbeerstrasse 10	Fax +41 31 985 25 11
CH-3011 Bern	info@netmodule.com
Switzerland	https://www.netmodule.com

Contents

1. Welcome to NetModule . . . 9
2. Conformity . . . 10
   2.1. Safety Instructions . . . 10
   2.2. Declaration of Conformity . . . 13
   2.3. Waste Disposal . . . 15
   2.4. National Restrictions . . . 15
   2.5. Open Source Software . . . 16
3. Specifications . . . 17
   3.1. Appearance . . . 17
   3.2. Features . . . 18
   3.3. Environmental Conditions . . . 18
   3.4. Interfaces . . . 19
      3.4.1. Overview . . . 19
      3.4.2. Default LED Indicators . . . 20
      3.4.3. Reset . . . 20
      3.4.4. Mobile . . . 21
      3.4.5. Bluetooth . . . 21
      3.4.6. WLAN . . . 21
      3.4.7. GNSS . . . 23
      3.4.8. USB 2.0 Host Port . . . 23
      3.4.9. RJ45 Ethernet Connector . . . 24
      3.4.10. Power Supply . . . 25
      3.4.11. COM/IO Shield . . . 26
      3.4.12. 2xCAN Shield . . . 27
      3.4.13. CanGI Shield . . . 28
4. Installation . . . 29
   4.1. Installation of the Router . . . 29
   4.2. Installation of the Micro-SIM Card . . . 29
   4.3. Installation of the Cellular Antenna . . . 29
   4.4. Installation of the WLAN Antennas . . . 30
   4.5. Installation of the Bluetooth Antenna . . . 30
   4.6. Installation of the GNSS Antenna . . . 30
   4.7. Installation of the Local Area Network . . . 30
   4.8. Installation of the Power Supply . . . 31
5. Configuration . . . 32
   5.1. First Steps . . . 32
      5.1.1. Initial Access . . . 32
      5.1.2. Automatic Mobile Data Connection . . . 33
      5.1.3. Recovery . . . 34
   5.2. HOME . . . 35
   5.3. INTERFACES . . . 38
      5.3.1. WAN . . . 38
      5.3.2. Ethernet . . . 44
      5.3.3. Mobile . . . 54
      5.3.4. WLAN . . . 62
      5.3.5. Software Bridges . . . 73
      5.3.6. USB . . . 74
      5.3.7. Serial . . . 76

5.3.8. Digital I/O . . . 81
5.3.9. Bluetooth Low Energy . . . 82
5.4. ROUTING . . . 83
5.4.1. Static Routes . . . 83
5.4.2. Extended Routing . . . 85
5.4.3. Multipath Routes . . . 86
5.4.4. Multicast . . . 87
5.4.5. BGP . . . 89
5.4.6. OSPF . . . 91
5.4.7. Mobile IP . . . 92
5.4.8. Quality Of Service . . . 96
5.5. FIREWALL . . . 98
5.5.1. Administration . . . 98
5.5.2. Adress/Port Groups . . . 98
5.5.3. Rules . . . 99
5.5.4. NAPT . . . 101
5.6. VPN . . . 104
5.6.1. OpenVPN . . . 104
5.6.2. IPsec . . . 110
5.6.3. PPTP . . . 116
5.6.4. GRE . . . 119
5.6.5. L2TP . . . 120
5.6.6. Dial-In . . . 121
5.7. SERVICES . . . 123
5.7.1. SDK . . . 123
5.7.2. DHCP Server . . . 132
5.7.3. DNS Server . . . 135
5.7.4. NTP Server . . . 138
5.7.5. Dynamic DNS . . . 139
5.7.6. E-Mail . . . 141
5.7.7. Events . . . 143
5.7.8. SMS . . . 144
5.7.9. SSH/Telnet Server . . . 146
5.7.10. SNMP Agent . . . 148
5.7.11. Let's Encrypt . . . 153
5.7.12. Web Server . . . 154
5.7.13. MQTT Broker . . . 155
5.7.14. Softflow . . . 156
5.7.15. Discovery . . . 157
5.7.16. Redundancy . . . 158
5.7.17. ITxPT . . . 160
5.7.18. Voice Gateway . . . 169
5.7.19. Access Controller WLAN-AP . . . 175
5.8. SYSTEM . . . 183
5.8.1. System . . . 183
5.8.2. Authentication . . . 189
5.8.3. Software Update . . . 192
5.8.4. Module Firmware Update . . . 193
5.8.5. Software Profiles . . . 194

5.8.6. Configuration . . . 195
5.8.7. Troubleshooting . . . 198
5.8.8. Keys and Certificates . . . 201
5.8.9. Licensing . . . 206
5.8.10. Legal Notice . . . 207
5.9. LOGOUT . . . 208
6. Command Line Interface . . . 209
6.1. General Usage . . . 209
6.2. Print Help . . . 210
6.3. Getting Config Parameters . . . 210
6.4. Setting Config Parameters . . . 211
6.5. Checking Config Completed . . . 211
6.6. Getting Status Information . . . 211
6.7. Scanning Networks . . . 212
6.8. Sending E-Mail or SMS . . . 212
6.9. Updating System Facilities . . . 212
6.10. Manage keys and certificates . . . 213
6.11. Restarting Services . . . 213
6.12. Debug System . . . 214
6.13. Resetting System . . . 214
6.14. Rebooting System . . . 215
6.15. Running Shell Commands . . . 215
6.16. Working with History . . . 215
6.17. CLI-PHP . . . 215
A. Appendix . . . 221
A.1. Abbrevations . . . 221
A.2. System Events . . . 223
A.3. Factory Configuration . . . 226
A.4. SNMP VENDOR MIB . . . 227
A.5. SDK Examples . . . 228

List of Figures

5.1. Initial Login . . . 33
5.2. Home . . . 35
5.3. WAN Links . . . 38
5.4. Link Supervision . . . 41
5.5. WAN Settings . . . 43
5.6. Ethernet Ports . . . 44
5.7. Ethernet Link Settings . . . 45
5.8. Authentication via IEEE 802.1X . . . 46
5.9. VLAN Management . . . 48
5.10. LAN IP Configuration . . . 49
5.11. LAN IP Configuration - LAN Interface . . . 50
5.12. LAN IP Configuration - WAN Interface . . . 51
5.13. SIMs . . . 54
5.14. eSIM Profiles . . . 57
5.15. Add eUICC Profile . . . 58
5.16. WWAN Interfaces . . . 60
5.17. WLAN Management . . . 62
5.18. WLAN Configuration . . . 67
5.19. WLAN IP Configuration . . . 71
5.20. USB Administration . . . 74
5.21. USB Device Management . . . 75
5.22. Serial Port Administration . . . 77
5.23. Serial Port Settings . . . 78
5.24. Digital I/O Ports . . . 81
5.25. Static Routing . . . 83
5.26. Extended Routing . . . 85
5.27. Multipath Routes . . . 86
5.28. Mobile IP . . . 94
5.29. Firewall Groups . . . 98
5.30. Firewall Rules . . . 99
5.31. Masquerading . . . 101
5.32. Inbound NAPT . . . 102
5.33. OpenVPN Administration . . . 104
5.34. OpenVPN Configuration . . . 105
5.35. OpenVPN Client Management . . . 109
5.36. IPsec Administration . . . 111
5.37. IPsec Configuration . . . 112
5.38. PPTP Administration . . . 116
5.39. PPTP Tunnel Configuration . . . 117
5.40. PPTP Client Management . . . 118
5.41. Dial-in Server Settings . . . 121
5.42. SDK Administration . . . 127
5.43. SDK Jobs . . . 128
5.44. DHCP Server . . . 132
5.45. DNS Server . . . 135
5.46. NTP Server . . . 138
5.47. Dynamic DNS Settings . . . 139

5.48. E-Mail Settings . . . 141
5.49. SMS Configuration . . . 144
5.50. SSH and Telnet Server . . . 146
5.51. SNMP Agent . . . 149
5.52. Web Server . . . 154
5.53. VRRP Configuration . . . 158
5.54. ITxPT configuration . . . 160
5.55. ITxPT FMStoIP . . . 162
5.56. ITxPT GNSS . . . 166
5.57. ITxPT Time . . . 167
5.58. ITxPT VEHICLEtoIP . . . 168
5.59. Voice Gateway Administration . . . 169
5.60. AC WLAN-AP Administration . . . 176
5.61. AC WLAN-AP Configuration . . . 178
5.62. AC WLAN-AP Profiles . . . 181
5.63. System . . . 183
5.64. Regional settings . . . 186
5.65. User Accounts . . . 189
5.66. Remote Authentication . . . 191
5.67. Manual File Configuration . . . 195
5.68. Automatic File Configuration . . . 196
5.69. Factory Configuration . . . 197
5.70. Log Viewer . . . 199
5.71. Tech Support File . . . 200
5.72. Keys and certificates . . . 201
5.73. Certificate Configuration . . . 203
5.74. Licensing . . . 206

List of Tables

3.1. Environmental Conditions . . . 18
3.2. NB800 Interfaces . . . 19
3.3. NB800 Status Indicators . . . 20
3.4. Ethernet Status Indicators . . . 20
3.5. Mobile Antenna Port Specification . . . 21
3.6. IEEE 802.11 Standards . . . 21
3.7. WLAN Antenna Port Specification . . . 22
3.8. GNSS Specifications option G . . . 23
3.9. GNSS / GPS Antenna Port Specification . . . 23
3.10. USB 2.0 Host Port Specification . . . 23
3.11. Ethernet Port Specification . . . 24
3.12. Pin Assignments of RJ45 Ethernet Connector . . . 24
3.13. Power Specifications . . . 25
3.14. Power Connector . . . 25
3.15. Pin Assignments of Terminal Block . . . 25
3.16. Specification of COM/IO Shield . . . 26
3.17. Pin Assignments of COMIO Shield . . . 26
3.18. Specification of 2xCAN Shield . . . 27
3.19. Pin Assignments of 2xCAN Shield . . . 27
3.20. Pin Assignments of CanGI Shield . . . 28

5.25. IEEE 802.11 Network Standards . . . 64
5.47. Static Route Flags . . . 84
5.95. SMS Control Commands . . . 131
5.109. SMS Number Expressions . . . 145
5.178. Certificate Sections . . . 202
5.179. Certificate Operations . . . 202

A.1. Abbreviations . . . 223
A.2. Systemereignisse . . . 225
A.3. SDK Examples . . . 230

1. Welcome to NetModule

Thank you for purchasing a NetModule product. This document should give you an introduction to the device and its features. The following chapters describe any aspects of commissioning the device, installation procedure and provide helpful information towards configuration and maintenance.

Please find further information such as sample SDK scripts or configuration samples in our wiki on https://wiki.netmodule.com.

2. Conformity

This chapter provides general information for putting the router into operation.

2.1. Safety Instructions

Please carefully observe all safety instructions in the manual that are marked with the symbol ⚠.

Compliance information: The NetModule routers must be used in compliance with any and all applicable national and international laws and with any special restrictions regulating the utilization of the communication module in prescribed applications and environments.

Information about the accessories / changes to the device:

- Please only use original accessories to prevent injuries and health risks.
- Changes made to the device or the use of non-authorized accessories will render the warranty null and void and potentially invalidate the operating license.
- NetModule routers must not be opened (SIM cards may be used according to the instructions).

Information about the device interfaces:

- All systems that are connected to the NetModule router interfaces must meet the requirements for SELV (Safety Extra Low Voltage) systems.
- Interconnections must not leave the building nor penetrate the body shell of a vehicle.
- Connections for antennas may only exit the building or the vehicle hull if transient overvoltages (according to IEC 62368-1) are limited by external protection circuits down to 1 500 V_{peak}. All other connections must remain within the building or the vehicle hull.
- Installed antennas must always be at least 40 cm away from people.
- All antennas must have a distance of at least 20cm from each other; in the case of combined antennas (mobile radio / WLAN / GNSS), there must be sufficient isolation between the radio technologies.
- Devices with a WLAN interface may be operated only with applicable Regulatory Domain configured. Special attention must be paid to country, number of antennas and the antenna gain (see also chapter 5.3.4). WLAN antennas with a higher amplification may be used with the NetModule router "Enhanced-RF-Configuration" software license and the antenna gain and cable attenuation that have been correctly configured by certified specialized personnel. A misconfiguration will lead to loss of the approval.
- The maximum gain of an antenna (incl. the attenuation of the connection cables) must not exceed the following values in the corresponding frequency range:
  - Mobile radio (600MHz .. 1GHz) < 3.2dBi
  - Mobile radio (1.7GHz .. 2GHz) < 6.0dBi
  - Mobile radio (2.5GHz .. 4.2GHz) < 6.0dBi
  - WiFi (2.4GHz .. 2.5GHz) < 3.2dBi
  - WiFi (5.1GHz .. 5.9GHz) < 4.5dBi
- Note that GNSS signals can be obfuscated or blocked by malicious third-party devices.
- Only CE-compliant power supplies with a current-limited SELV output voltage range may be used with the NetModule routers.

FCC Warning:

- Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
- This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
- (1) This device may not cause harmful interference , and
- (2) this device must accept any interference received , including interference that may cause undesired operation.

- Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver .
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected .
- Consult the dealer or an experienced radio / TV technician for help.
- Exposure Requirements: To comply with the FCC RF exposure compliance requirements, the device must be installed to provide a separation distance of at least 40 cm from all persons.

General safety instructions:

- Observe the usage limitations of radio units at filling stations, in chemical plants, in systems with explosives or potentially explosive locations.
- The devices may not be used in airplanes.
- Exercise particular caution near personal medical aids, such as pacemakers and hearing aids.
- The NetModule routers may also cause interference in the nearer distance of TV sets, radio receivers and personal computers.
- Never perform work on the antenna system during a thunderstorm.
- The devices are generally designed for normal indoor use. Do not expose the devices to extraordinary environmental conditions worse than IP40.
- Protect them against aggressive chemical atmospheres and humidity or temperatures outside specifications.
- We highly recommended creating a copy of a working system configuration. It can be easily applied to a newer software release afterwards.

2.2. Declaration of Conformity

NetModule hereby declares that under our own responsibility that the routers comply with the relevant standards following the provisions of the *RED Directive 2014/53/EU*. The signed version of the *Declaration of Conformity* can be obtained from https://www.netmodule.com/downloads

Operating frequency bands and related maximum radio frequency power transmitted is shown below, according to RED Directive 2014/53/EU, Article 10 (8a, 8b).

WLAN maximum output power

IEE 802.11b/g/n
Operation frequency range: 2412-2472 MHz (13 channels)
Maximum output power: 20.7 dBm EIRP average (on antenna port,calculated)

IEE 802.11a/n
Operation frequency range: 5180-5350 MHz / 5470-5700 MHz (19 channels)
Maximum output power: 24 dBm EIRP average (on antenna port,calculated)

Bluetooth Low Energy (BLE) maximum output power
Operation frequency range: 2402-2480 MHz (79 channels)
Maximum output power: 15.7 dBm EIRP average (on antenna port, calculated)

Cellular maximum output power

GSM Band 900
Operation frequency range: 880-915, 925-960 MHz
Maximum output power: 33.5 dBm rated

GSM Band 1800
Operation frequency range: 1710-1785, 1805-1880 MHz
Maximum output power: 30.5 dBm rated

WCDMA Band I
Operation frequency range: 1920-1980, 2110-2170 MHz
Maximum output power: 24 dBm rated

WCDMA Band VIII
Operation frequency range: 880-915, 925-960 MHz
Maximum output power: 24 dBm rated

LTE FDD Band 1
Operation frequency range: 1920-1980, 2110-2170 MHz
Maximum output power: 24 dBm rated

LTE FDD Band 3
Operation frequency range: 1710-1785, 1805-1880 MHz
Maximum output power: 24 dBm rated

LTE FDD Band 7
Operation frequency range: 2500-2570, 2620-2690 MHz
Maximum output power: 23.5 dBm rated

LTE FDD Band 8
Operation frequency range: 880-915, 925-960 MHz
Maximum output power: 24 dBm rated

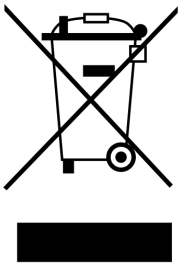
LTE FDD Band 20
Operation frequency range: 832-862, 791-821 MHz
Maximum output power: 24 dBm rated

LTE FDD Band 28
Operation frequency range: 703-748, 758-803
Maximum output power: 24 dBm rated

LTE FDD Band 38
Operation frequency range: 2570-2620 MHz
Maximum output power: 24 dBm rated

LTE FDD Band 40
Operation frequency range: 2300-2400 MHz
Maximum output power: 24 dBm rated

2.3. Waste Disposal



In accordance with the requirements of the *Council Directive 2012/19/EU* regarding Waste Electrical and Electronic Equipment (WEEE), you are urged to ensure that this product will be segregated from other waste at end-of-life and delivered to the WEEE collection system in your country for proper recycling.

2.4. National Restrictions

This product may be generally used in all EU countries (and other countries following the *RED Directive 2014/53/EU*) without any limitation. Please refer to our WLAN Regulatory Database for getting further national radio interface regulations and requirements for a particular country.

2.5. Open Source Software

We inform you that NetModule products may contain in part open-source software. We are distributing such open-source software to you under the terms of GNU General Public License (GPL)[1], GNU Lesser General Public License (LGPL)[2] or other open-source licenses[3]. These licenses allow you to run, copy, distribute, study, change and improve any software covered by GPL, Lesser GPL, or other open-source licenses without any restrictions from us or our end user license agreement on what you may do with that software. Unless required by applicable law or agreed to in writing, software distributed under open-source licenses is distributed on an "AS IS" basis, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

To obtain the corresponding open source codes covered by these licenses, please contact our technical support at router@support.netmodule.com.

Acknowledgements

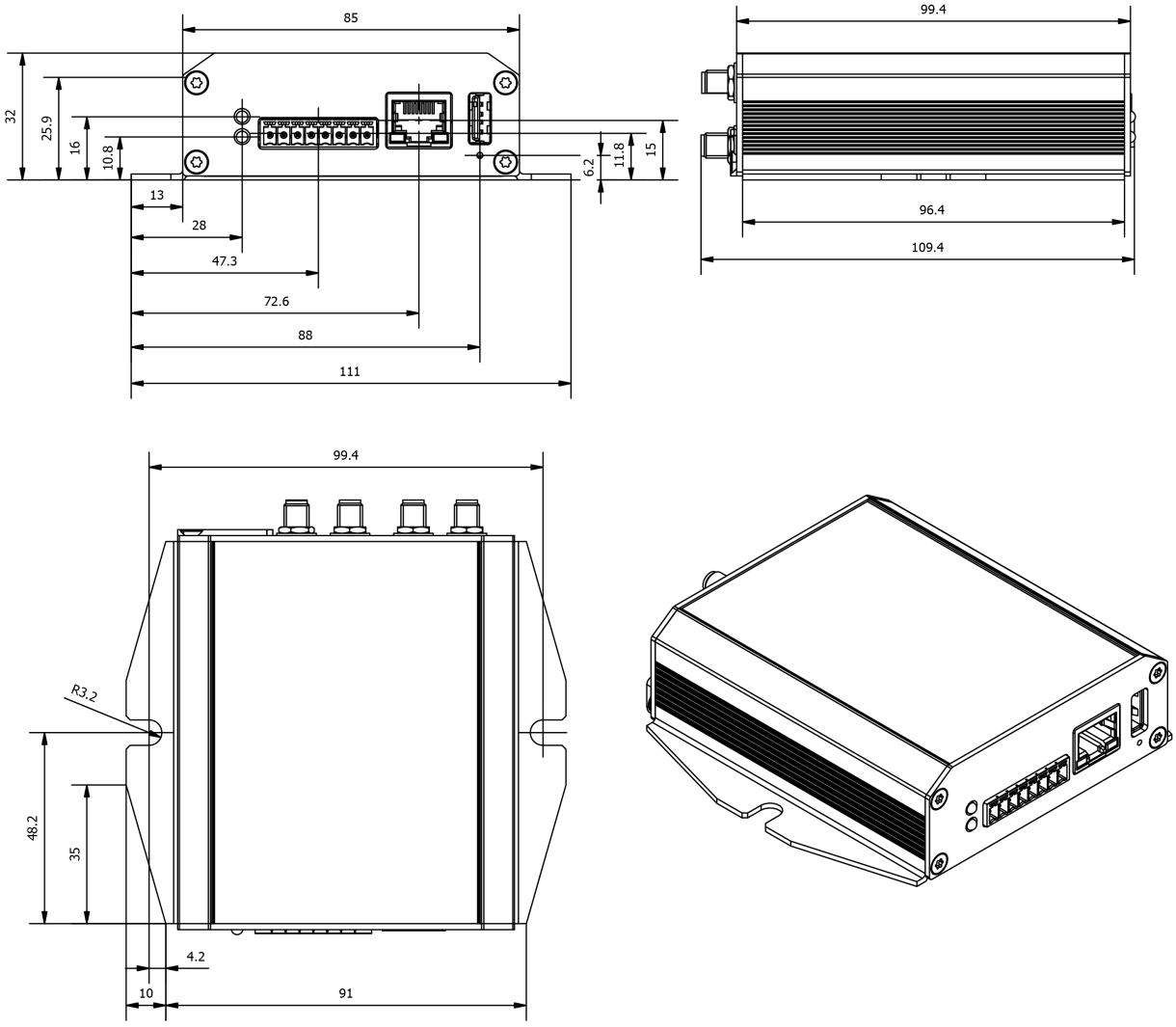
This product includes:

- PHP, freely available from http://www.php.net
- Software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org)
- Cryptographic software written by Eric Young (eay@cryptsoft.com)
- Software written by Tim Hudson (tjh@cryptsoft.com)
- Software written Jean-loup Gailly and Mark Adler
- MD5 Message-Digest Algorithm by RSA Data Security, Inc.
- An implementation of the AES encryption algorithm based on code released by Dr Brian Gladman
- Multiple-precision arithmetic code originally written by David Ireland
- Software from The FreeBSD Project (http://www.freebsd.org)

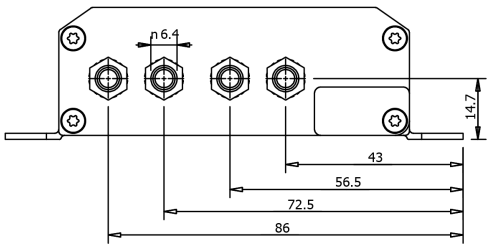
[1] Please find the GPL text under http://www.gnu.org/licenses/gpl-2.0.txt
[2] Please find the LGPL text under http://www.gnu.org/licenses/lgpl.txt
[3] Please find the license texts of OSI licenses (ISC License, MIT License, PHP License v3.0, zlib License) under http://opensource.org/licenses

3. Specifications

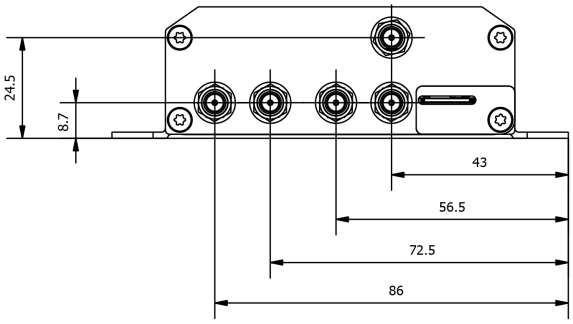
3.1. Appearance



NB800 Rev A without GNSS



NB800 Rev B02 with GNSS



3.2. Features

All models of NB800 have following standard functionalities:

- 1x Ethernet port (10/100 Mbit/s)
- 1x Micro SIM (3FF) card slot
- 1x USB
- 4 GB internal storage
- Full featured router software

The NB800 can be equipped with the following options:

- 1x LTE, UMTS, GSM or UMTS, GSM
- 1x WLAN IEEE 802.11
- 1x Bluetooth and Bluetooth Low Energy
- 1x GNSS
- 1x Extension shields
- Software Keys

Due to its modular approach, the NB800 router and its hardware components can be arbitrarily assembled according to its indented usage or application. Please contact us in case of special project requirements.

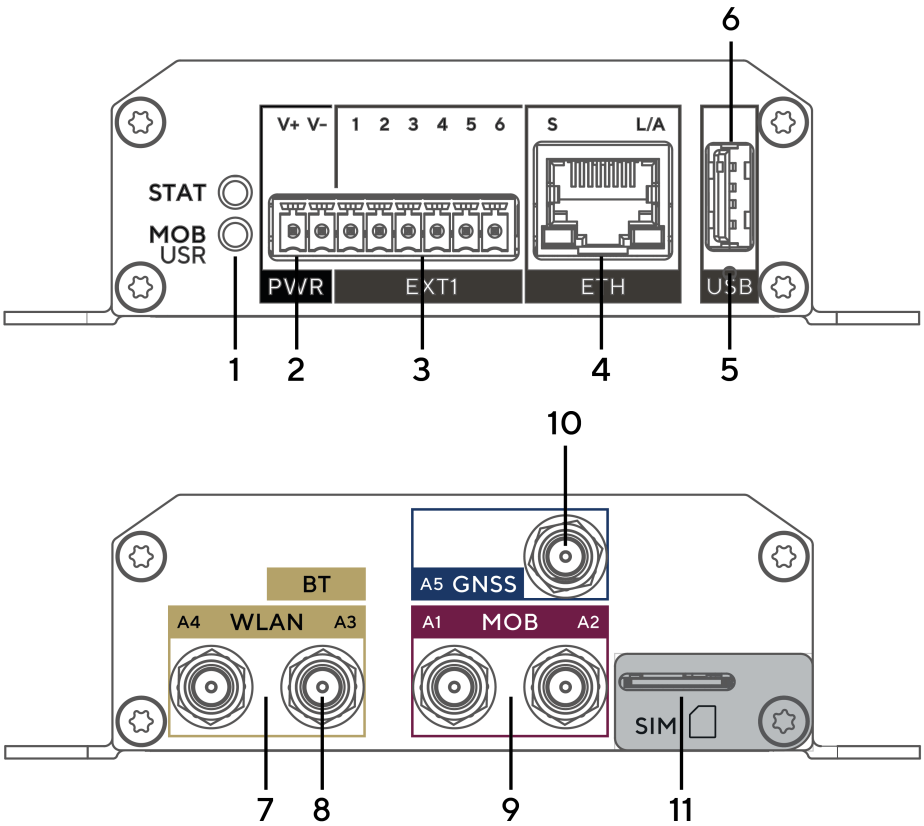
3.3. Environmental Conditions

Parameter	Rating
Input Voltage	12 V_{DC} to 24 V_{DC} (−20% / +20%)
Operating Temperature Range	$-40\,°C$ to $+70\,°C$
Storage Temperature Range	$-40\,°C$ to $+85\,°C$
Humidity	0 to 95% (non-condensing)
Altitude	up to 4000m
Over-Voltage Category	I
Pollution Degree	2
Ingress Protection Rating	IP40

Table 3.1.: Environmental Conditions

3.4. Interfaces

3.4.1. Overview



Nr.	Label	Function
1	LED Indicators	LED Indicators for the different interfaces
2	PWR	Power supply 12-24 V_{DC}.
3	EXT1	Extension connector e.g. for CAN or COM/IO
4	ETH	FastEthernet port, can be used as LAN or WAN interface.
5	Reset	Reboot and factory reset button
6	USB	USB 2.0 host port, can be used for software/configuration updates.
7	WLAN	SMA female connectors for MIMO WLAN antenna. A3 is the main port, A4 is the auxiliary port.
8	BT	SMA female connector (A3) for Bluetooth.
9	MOB	SMA female connectors for LTE/UMTS antennas. A1 is the main, A2 the auxiliary port
10	GNSS	SMA female connector for GNSS
11	SIM	Slot for 1 Micro SIM (3FF)

Table 3.2.: NB800 Interfaces

3.4.2. Default LED Indicators

The following table describes the NB800 status indicators.

Label	Color	State	Function
STAT	●	blinking	The device is busy due to startup, software or configuration update.
	●	on	The device is ready.
MOB	●	blinking	Wireless link connection is establishing.
USR	●	on	Wireless link connection is up.
	❍	off	Wireless link connection is down.

Table 3.3.: NB800 Status Indicators

Ethernet LEDs

The following table describes the Ethernet status indicators.

Label	Color	State	Function
S (Speed)	●g	On	Link (10 Mbit/s or 100 Mbit/s
	❍	Off	No Link
L/A (Link/Activity)	●y	On	Link
	●y	Blinking	Activity
	❍	Off	No Link

Table 3.4.: Ethernet Status Indicators

3.4.3. Reset

The reset button has two functions:

1. Reboot the system:
   Press at least 3 seconds to trigger a system reboot.
   The reboot is indicated with the red blinking STAT LED.
2. Factory reset:
   Press at least 10 seconds to trigger a factory reset.
   The start of the factory reset is confirmed by all LEDs lighting up for a second.

3.4.4. Mobile

The various variants of the NB800 support multiple multimode modules for mobile communication. The LTE modules supports 2x2 MIMO.
Here you will find an overview of the different modems and the individual bands
The mobile antenna ports have the following specification:

Feature	Specification
Max. allowed cable length	30 m
Min. number of antennas 4G-LTE	2
Max. allowed antenna gain including cable attenuation	Mobile radio (600MHz .. 1GHz) < 3.2dBi Mobile radio (1.7GHz .. 2GHz) < 6.0dBi Mobile radio (2.5GHz .. 4.2GHz) < 6.0dBi
Min. distance between collocated radio transmitter antennas (Example: MOB1 to MOB2)	20 cm
Min. distance between people and antenna	40 cm
Connector type	SMA

Table 3.5.: Mobile Antenna Port Specification

3.4.5. Bluetooth

The NB800supports Bluetooth 4.2 including Bluetooth Low Energy.

3.4.6. WLAN

The variants of the NB800support a IEEE 802.11a/b/g/n WLAN module.

Standard	Frequencies	Bandwidth	Max. Data Rate
802.11a	5 GHz	20 MHz	54 Mbit/s
802.11b	2.4 GHz	20 MHz	11 Mbit/s
802.11g	2.4 GHz	20 MHz	54 Mbit/s
802.11n	2.4 GHz	20 MHz	144 Mbit/s
802.11n	5 GHz	40 MHz	150 Mbit/s

Table 3.6.: IEEE 802.11 Standards

Note: 802.11n supports 2x2 MIMO in 2.4 GHz and 1x1 in 5 GHz.

The WLAN antenna ports have the following specification:

Feature	Specification
Max. allowed cable length	30 m
Max. allowed antenna gain including cable attenuation	3.2dBi (2,4GHz) resp. 4.5dBi (5GHz) [1]
Min. distance between collocated radio transmitter antennas (Example: WLAN1 to MOB1)	20 cm
Min. distance between people and antenna	40 cm
Connector type	SMA

Table 3.7.: WLAN Antenna Port Specification

[1] **Note:** WLAN antennas with a higher amplification may be used with the NetModule router "Enhanced-RF-Configuration" software license and the antenna gain and cable attenuation that have been correctly configured by certified specialized personnel.

3.4.7. GNSS

Feature	Specification
Systems	GPS/GLONASS/GALILEO/BEIDOU
Data stream	JSON or NMEA
Tracking sensitivity	up to -167 dBm
Supported antennas	Active and passive

Table 3.8.: GNSS Specifications option G

The GNSS antenna port have the following specification:

Feature	Specification
Max. allowed cable length	30 m
Antenna LNA gain	15-20 dB typ, 30 dB max.
Min. distance between collocated radio transmitter antennas (Example: GNSS to MOB1)	20 cm
Connector type	SMA

Table 3.9.: GNSS / GPS Antenna Port Specification

3.4.8. USB 2.0 Host Port

The USB 2.0 host port has the following specification:

Feature	Specification
Speed	Low, Full & Hi-Speed
Current	max. 500 mA
Max. cable length	3 m
Cable shield	mandatory
Connector type	Type A

Table 3.10.: USB 2.0 Host Port Specification

3.4.9. RJ45 Ethernet Connector

Specification

The Ethernet port is specified as follows:

Feature	Specification
Isolation	1500 V_{DC}
Speed	10/100 Mbit/s
Mode	Half- & Full-Duplex
Crossover	Automatic MDI/MDI-X
Max. cable length	100 m
Cable type	CAT5e or better
Cable shield	mandatory
Connector type	RJ45

Table 3.11.: Ethernet Port Specification

Pin Assignment

Pin	Signal
1	TX+
2	TX−
3	RX+
4	-
5	-
6	RX−
7	-
8	-

Table 3.12.: Pin Assignments of RJ45 Ethernet Connector

Note: Pairs 4-5 and 7-8 have an internal 75 Ω termination.

3.4.10. Power Supply

NB800 routers have a non-isolated power supply input. It has the following specifications:

Feature	Specification
Power supply nominal voltages	12 V_{DC} and 24 V_{DC}
Voltage range	12 V_{DC} to 24 V_{DC} (−20% / +20%)
Avg. power consumption	5 W
Max. power consumption	10 W
Max. cable length	30 m
Cable shield	not required

Table 3.13.: Power Specifications

2 Pin Terminal Block

Feature	Specification
Connector type	Terminal block header 3.5 mm

Table 3.14.: Power Connector

Pin Assignment

	Pin	Name	Description
PWR	1	V+	Power Input
	2	V-	Power Ground

Table 3.15.: Pin Assignments of Terminal Block

3.4.11. COM/IO Shield

The COM/IO Shield has the following specification:

Feature	Specification
Feature	1xRS-232/485 1xdigital input 1xdigital output
RS-232 Signals	TX, RX
RS-232 Signal Level	High > 5 V_{DC}, low < -5 V_{DC}
RS-232 Bitrate	Up to 115 200 Bit/s
RS-485 Signals	A,B
RS-485 Signal Level	Differential output, 1.5 V_{DC}- 3.5 V_{DC}
RS-485 Bitrate	Up to 115 200 Bit/s
RS-485 Termination	120 Ω configurable by SW
DI Level	Low: 0 V_{DC}- 3 V_{DC}, high: 9 V_{DC}- 32 V_{DC}
DO Level	0-32 VDC/1A
DIO Isolation	1500 V_{DC}
Connector type	8 pin terminal block header 3.5mm

Table 3.16.: Specification of COM/IO Shield

Pin Assignment

Pin	Signal
V+	V+
V−	V−, RS232 GND
1	RS232 RX (NB800 Input); RS485 A (Half-Duplex)
2	RS232 TX (NB800 Output); RS485 B (Half-Duplex)
3	In- (Digital Input isolated)
4	In+ (Digital Input isolated)
5	Out NO (Digital Output isolated, Relay contact normally open)
6	Out COM (Digital Output isolated, Relais common)

Table 3.17.: Pin Assignments of COMIO Shield

3.4.12. 2xCAN Shield

The 2xCAN Shield has the following specification:

Feature	Specification
Features	2x CAN V2.0B
Signals	CANH, CANL
Signal Level	High > 2.75 V_{DC}, low < 2.0 V_{DC}
Bitrate	Up to 1 Mbit/s
Termination[2]	No internal bus termination On request: 120 Ω configurable by software
Bus access	Passive (read access only On request: write access
Connector type	8 pin terminal block header 3.5mm

Table 3.18.: Specification of 2xCAN Shield

Pin Assignment

Pin	Signal
V+	V+
V−	V−
1	CAN1_H
2	CAN1_L
3	GND
4	CAN2_H
5	CAN2_L
6	GND

Table 3.19.: Pin Assignments of 2xCAN Shield

Note: Cables with length >30m must be shielded.

[2] **Note:** On each end of the CAN bus is a 120 Ω termination mandatory

3.4.13. CanGI Shield

- 1x GNSS to SMA
- 1x CAN on 8 pin terminal block header 3.5mm

Pin Assignment

Pin	Signal
V+	V+
V−	V−
1	CAN_H
2	CAN_L
3	GND
4	-
5	-
6	-

Table 3.20.: Pin Assignments of CanGI Shield

Note: Cables with length >30m must be shielded.

4. Installation

The NB800 is designed for mounting it on a wall or in a switch cabinet. Please consider the safety instructions in chapter 2 and the environmental conditions in chapter 3.3.

The following precautions must be taken before installing a NB800 router:

- Avoid direct solar radiation
- Protect the device from humidity, steam and aggressive fluids
- Guarantee sufficient circulation of air around the device
- The device is for indoor use only

Attention: NetModule routers are not intended for the end consumer market. The device must be installed and commissioned by a certified expert.

4.1. Installation of the Router

The NB800 is designed for mounting on a wall but it is also available with an optional mounting kit for DIN rail. Please consider the safety instructions and the environmental conditions in chapter 2.

4.2. Installation of the Micro-SIM Card

One Micro-SIM card can be inserted in a NB800 router. To install the SIM card, you will have to remove the SIM cover first. The SIM card connector has a push to insert, push to eject mechanism. So just push the SIM card into the connector until it's fix. The cover should be closed again afterwards.

Warning

- Please power off the router before inserting the SIM card.
- Do not use nano SIM card with adaptor to fit in micro SIM card slot. This can damage SIM card connector.

4.3. Installation of the Cellular Antenna

For a reliable function of the NetModule router via the mobile network, the NetModule routers require a good signal. Use suitable remote antennas with extended cables to achieve an optimal location with a sufficient signal and to maintain the distances to other antennas (at least 20cm to each other). The antenna manufacturer's instructions must be observed."

Keep in mind that effects caused by Faraday cages such as large metal surfaces (elevators, machine housings, etc.), close meshed iron constructions and others may reduce signal reception significantly.

The antenna or antenna cable has to be mounted to the MOB connector and should be fixed with a wrench. 4G-LTE antennas require both the main and auxiliary ports to be connected.

Attention:
When installing the antenna be sure to observe chapter 2

4.4. Installation of the WLAN Antennas

Any WLAN antennas must be mounted to the connectors of WLAN. The number of attached antennas can be configured in the software. If only one antenna is used, it must be attached to port A3. However, for better diversity and thus better throughput and coverage, we highly recommend using two antennas. Only use antennas with cables shorter than 3 meters.

Attention:
When installing the antenna be sure to observe chapter 2

4.5. Installation of the Bluetooth Antenna

The Bluetooth antenna must be mounted to the connector BT, A3. Only use antennas with cables shorter than 3 meters.

4.6. Installation of the GNSS Antenna

The GNSS antenna must be mounted to the connector GNSS. Whether the antenna is an active or passive GNSS antenna has to be configured in the software. We recommend active GNSS antennas for highly accurate GNSS tracking.

Attention:
When installing the antenna be sure to observe chapter 2

4.7. Installation of the Local Area Network

One 10/100 Mbps Ethernet device can be directly connected to the router, further devices can be attached via an addtional Ethernet switch. Please ensure that the connector has been plugged in properly and remains in a fixed state, you might otherwise experience sporadical link loss during operation. The L/A (Link/Activity) LED will lit up as soon as the device has synced. If not, it might be necessary to configure a different link setting as described in chapter 5.3.2 The S (Speed) LED is on when the link speed is 100 Mbit/s. It's off when the link speed is at 10 Mbit/s.

Attention:
Only a shielded Ethernet cable may be used.

4.8. Installation of the Power Supply

The router can be powered with an external source supplying between 12 V_{DC} and 24 V_{DC}. It is to be used with a certified (CE or equivalent) power supply, which must have a limited and SELV circuit output. It must be ensured by installation that the input current of each router cannot exceed 8A. This could be accomplished a) with a limited power supply output current of 8A or b) with a single series fuse (8A delayed) at V+ input of the router. Furthermore, power supply wires attached to V+ and V- inputs of the router must be able to withstand up to 8A current without heating up significantly or damaging its isolation.

Attention: Only CE-compliant power supplies with a current-limited SELV output voltage range may be used with the NetModule routers.

5. Configuration

The following chapters provide information on setting up the router and configuring its functions as provided with system software 99.99.

NetModule provides regularly updated router software with new functions, bug fixes and closed vulnerabilities. Please keep your router software up to date.
ftp://share.netmodule.com/router/public/system-software/

5.1. First Steps

NetModule routers can be easily set up by using the HTTP-based configuration interface, called the Web Manager. It is supported by the latest web browsers. Please ensure to have JavaScript turned on.

Any submitted configuration via the Web Manager will be applied immediately to the system when pressing the `Apply` button. When configuring subsystems which require multiple steps (for instance WLAN) you can use the `Continue` button to store any settings temporarily and apply them at a later time. Please note that those settings will be neglected at logout unless applied.

You may also upload configuration files via SNMP, SSH, HTTP or USB in case you intend to deploy a larger numbers of routers. Advanced users may also use the Command Line Interface (CLI) and set configuration parameters directly.

The IP address of Ethernet 1 is `192.168.1.1` and DHCP is activated on the interface by default. The following steps need to be taken to establish your first Web Manager session:

1. Connect the Ethernet port of your computer to the Ethernet 1 (FastEthernet) port of the router using a shielded CAT5 cable with RJ45 (or M12) connector.
2. If not yet activated, enable DHCP on your computer's Ethernet interface so that an IP address can be obtained automatically from the router. This usually takes a short amount of time until your PC has received the corresponding parameters (IP address, subnet mask, default gateway, name server). You may track the progress by having a look to your network control panel and check whether your PC has correctly retrieved an IP address of the range `192.168.1.100` to `192.168.1.199`.
3. Launch your favorite web browser and point it to the IP address of the router (the URL is http://192.168.1.1).
4. Please follow the instructions of the Web Manager for configuring the router. Most of the menus are self-explanatory, further details are given in the following chapters.

5.1.1. Initial Access

In factory state you will be prompted for a new administrator password. Please choose a password which is both, easy to remember but also robust against dictionary attacks (such as one that contains numbers, letters and punctuation characters). The password shall have a minimum length of 6 characters. It shall contain a minimum of 2 numbers and 2 letters.

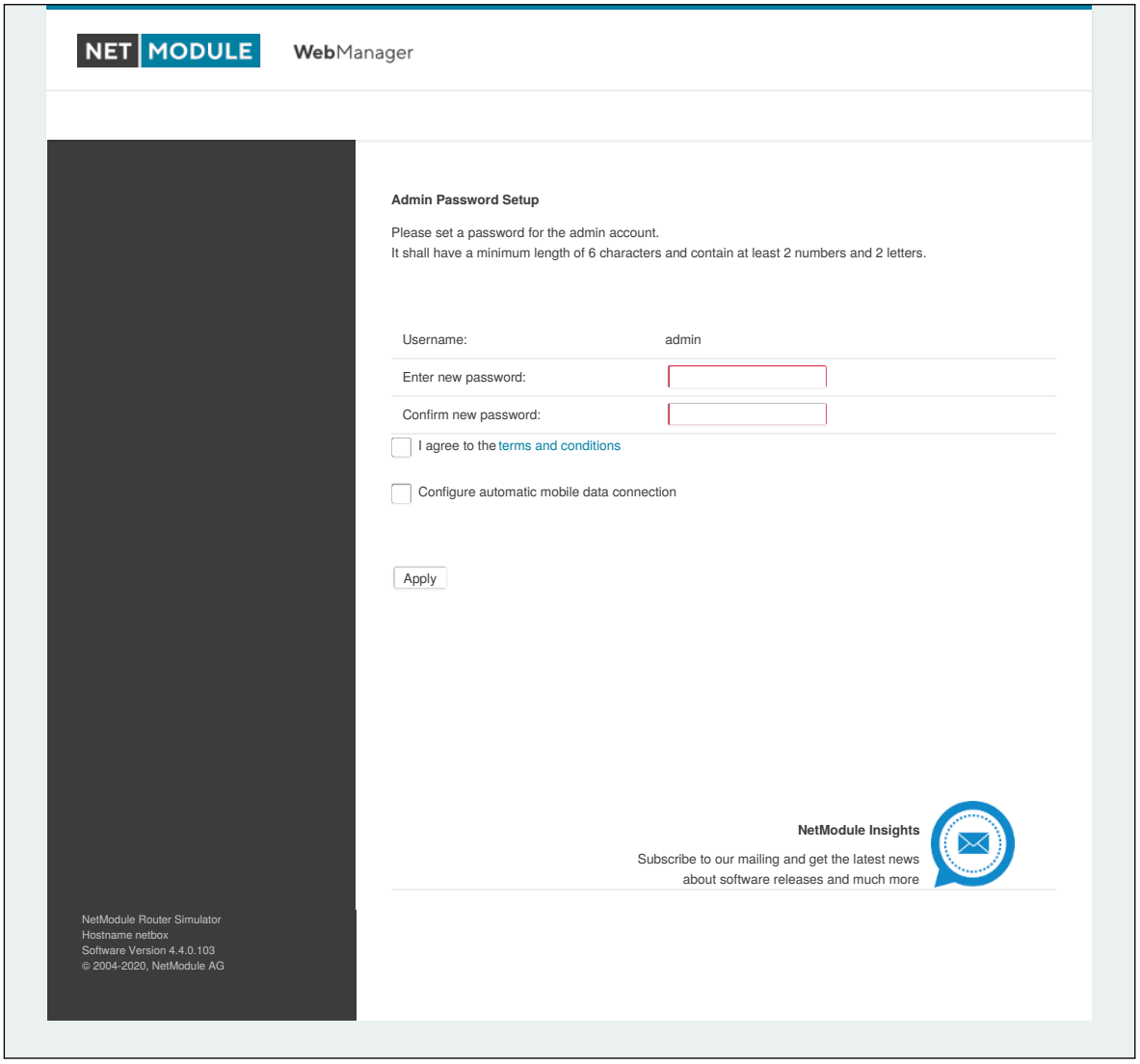


Figure 5.1.: Initial Login

Please note that the admin password will be also applied for the root user which can be used to access the device via the serial console, Telnet, SSH or to enter the bootloader. You may also configure additional users which will only be granted to access the summary page or retrieve status information but not to set any configuration parameters.

A set of services (USB Autorun, CLI-PHP) are by default activated in factory state and will be disabled as soon as the admin password has been set. They can be enabled again afterwards in the relevant sections. Other services (SSH, Telnet, Console) can be accessed in factory state by providing an empty or no password.

The passphrase which is used to store and access generated and uploaded private keys is initialized to a random value. It can be changed as described in chapter 5.8.8.

5.1.2. Automatic Mobile Data Connection

If you put a SIM with disabled PIN into the first SIM slot and select 'Configure automatic mobile data connection' the router will try to select matching credentials from a database of known providers and

esteblish a mobile data connection automatically. This feature is highly dependent on the SIM card features and the available networks.

This Option is only availble if the router is equipped with a cellular module.

5.1.3. Recovery

Following actions might be taken in case the router has been misconfigured and cannot be reached anymore:

1. Factory Reset: You can initiate a reset back to factory settings via the Web Manager, by running the command `factory-reset` or by pressing the reset button. The latter would require a slim needle or paper clip which must be inserted into the holeto the right of the Ethernet port or under the USB port. The button must be hold pressed for up to 5 seconds until all LEDs flash up.
2. Serial Console Login: It is also possible to log into the system via the serial port. This requires a terminal emulator (such as PuTTY or HyperTerminal) and an RS232 connection (115200 8N1) attached to the serial port of your local computer. You will also see the kernel messages at bootup there.
3. Recovery Image: In severe cases we can provide a recovery image on demand which can be loaded into RAM via TFTP and executed. It offers a minimal system image for running a software update or doing other modifications. You will be provided with two files, recovery-image and recovery-dtb, which must be placed in the root directory of a TFTP server (connected via LAN1 and address 192.168.1.254). The recovery image can be launched from the bootloader using a serial connection. You will have to stop the boot process by pressing `s` and enter the bootloader. You can then issue `run recovery` to load the image and start the system which can be accessed via HTTP/SSH/Telnet and its IP address `192.168.1.1` afterwards. This procedure can be also initiated by holding the factory reset button longer than 15 seconds.

5.2. HOME

This page provides a status overview of enabled features and connections.

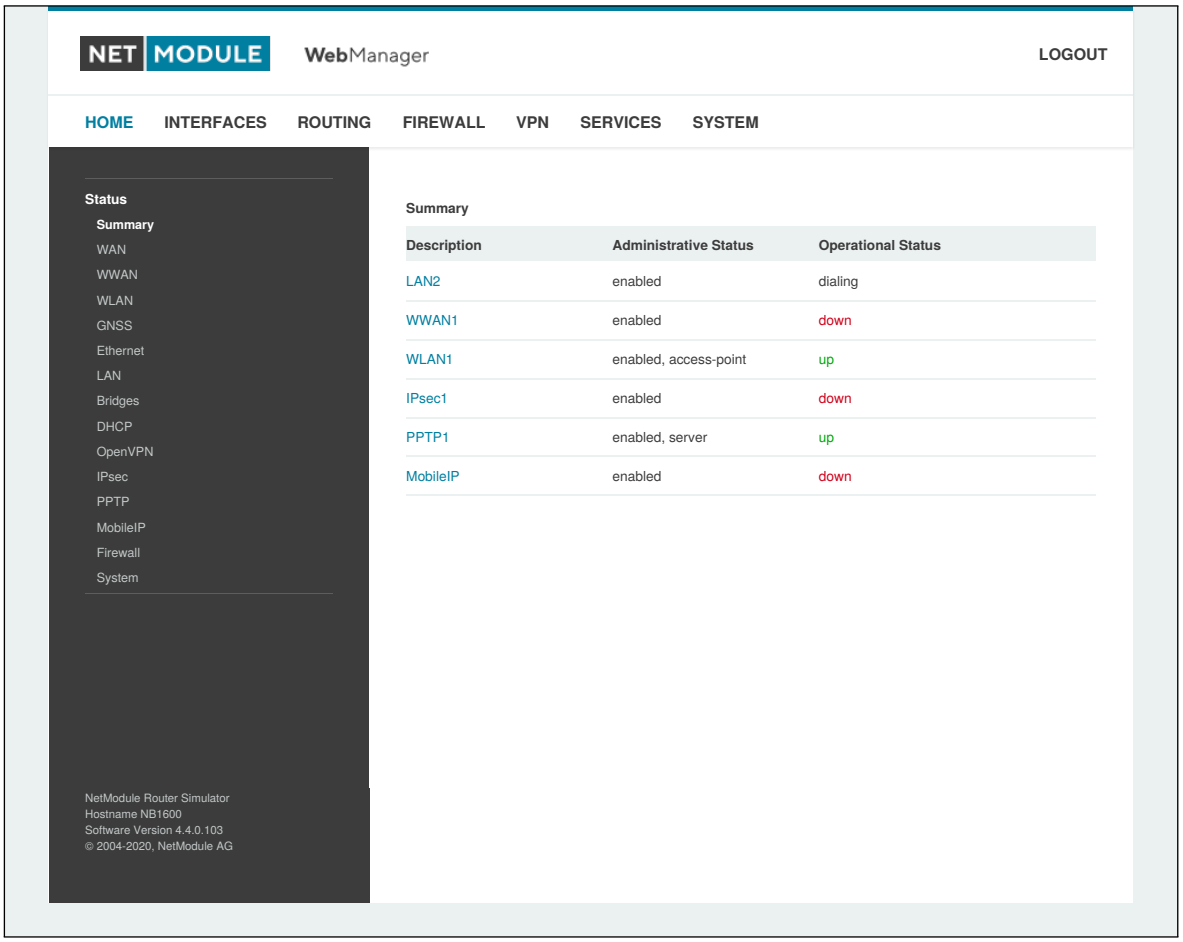


Figure 5.2.: Home

Summary

This page offers a short summary about the administrative and operational status of the router's interfaces.

WAN

This page offers details about any enabled Wide Area Network (WAN) links (such as the IP addresses, network information, signal strength, etc.) The information about the amount of downloaded/uploaded data is stored in non-volatile memory, thus survive a reboot of the system.
The counters can be reset by pressing the *Reset* button.

WWAN

This page shows information about modems and their network status.

AC

This page shows information about the Access Controller (AC) WLAN-AP. This includes the current states and status information of discovered and managed AP3400 devices.

WLAN

The WLAN page offers details about the enabled WLAN interfaces when operating in access-point mode. This includes the SSID, IP and MAC address and the currently used frequency and transmit power of the interface as well as the list of associated stations.

GNSS

This page displays the position status values, such as latitude/longitude, the satellites in view and more details about the used satellites.

Ethernet

This page shows information about the Ethernet interfaces and packet statistics information.

LAN

This page shows information about the LAN interfaces plus the neighborhood information.

Bridges

This page shows information about configured virtual bridge devices.

Bluetooth

This page shows information about Bluetooth interfaces.

DHCP

This page offers details about any activated DHCP service, including a list of issued DHCP leases.

OpenVPN

This page provides information about the OpenVPN tunnel status.

IPSec

This page provides information about the IPsec tunnel status.

PPTP

This page provides information about the PPTP tunnel status.

GRE

This page provides information about the GRE tunnel status.

L2TP

This page provides information about the L2TP tunnel status.

MobileIP

This page provides information about Mobile IP connections.

Firewall

This page offers information about any firewall rules and their matching statistics. It can be used to debug the firewall.

QoS

This page provides information about the used QoS queues.

BGP

This page provides information about the Border Gateway Protocol.

OSPF

This page provides information about the Open Shortest Path First routing protocol.

DynDNS

This page provides information about Dynamic DNS.

System Status

The system status page displays various details of your NB800 router, including system details, information about mounted modules and software release information.

SDK

This section will list all webpages generated by SDK scripts.

5.3. INTERFACES

5.3.1. WAN

Link Management

Depending on your hardware model, WAN links can be made up of either Wireless Wide Area Network (WWAN), Wireless LAN (WLAN), Ethernet or PPP over Ethernet (PPPoE) connections. Please note that each WAN link has to be configured and enabled in order to appear on this page.

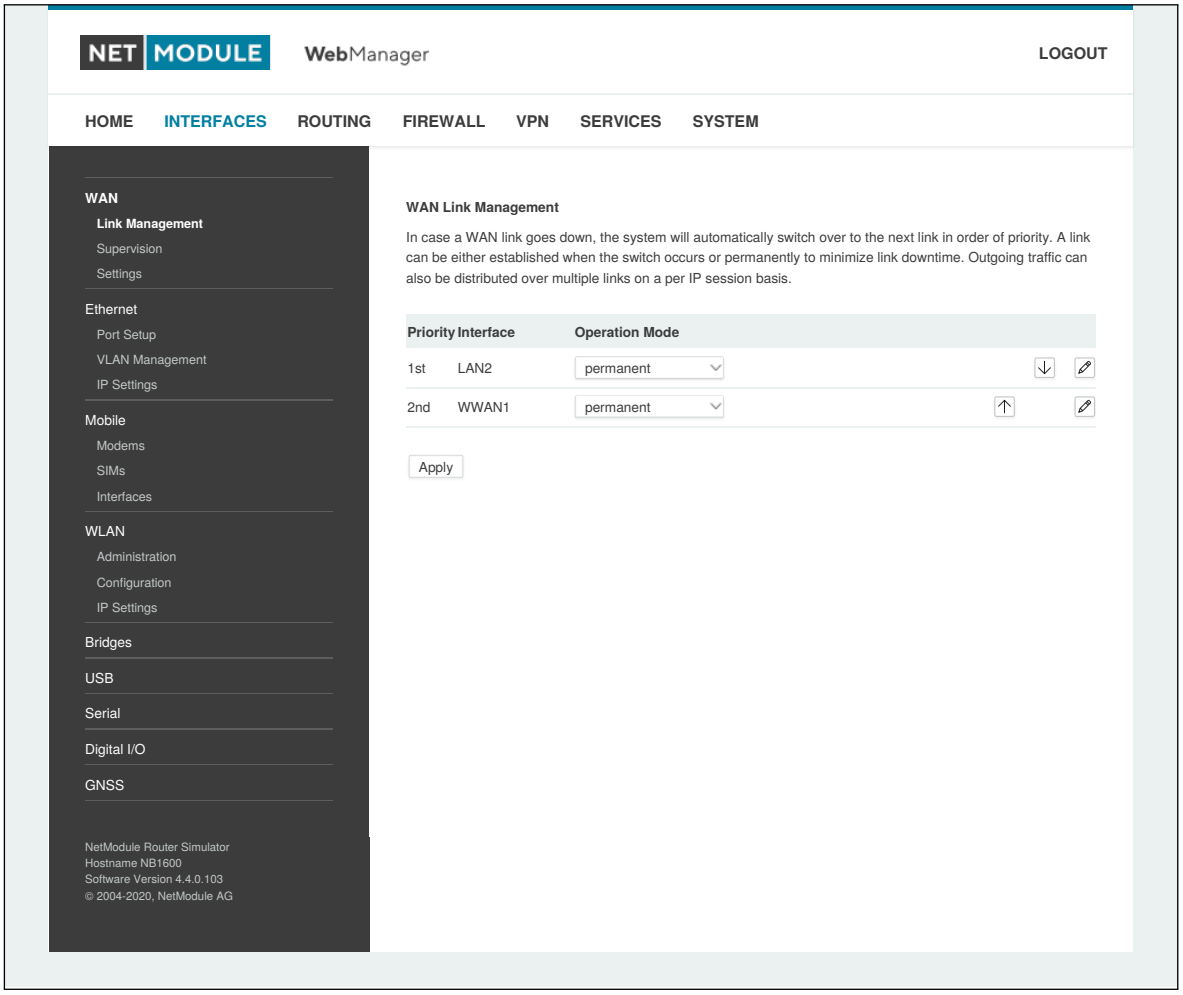


Figure 5.3.: WAN Links

In general, a link will be only dialed or declared as up if the following prerequisites are met:

Condition	WWAN	WLAN	ETH	PPPoE
Modem is registered	X			
Registered with valid service type	X			
Valid SIM state	X			
Sufficient signal strength	X	X		
Client is associated		X		
Client is authenticated		X		
Valid DHCP address retrieved	X	X	X	X
Link is up and holds address	X	X	X	X
Ping check succeeded	X	X	X	X

The menu can be used further to prioritize your WAN links. The highest priority link which has been established successfully will become the so-called `hotlink` which holds the default route for outgoing packets.

In case a link goes down, the system will automatically switch over to the next link in the priority list. You can configure each link to be either established when the switch occurs or permanently in order to minimize link downtime.

Parameter	WAN Link Priorities
1st priority	The primary link which will be used whenever possible.
2nd priority	The first fallback link, it can be enabled permanently or being dialed as soon as Link 1 goes down.
3rd priority	The second fallback link, it can be enabled permanently or being dialed as soon as Link 2 goes down.
4th priority	The third fallback link, it can be enabled permanently or being dialed as soon as Link 3 goes down.

Links are being triggered periodically and put to sleep in case it was not possible to establish them within a certain amount of time. Hence it might happen that permanent links will be dialed in background and replace links with lower priority again as soon as they got established. In case of interfering links sharing the same resources (for instance in dual-SIM operation) you may define a switch-back interval after which an active hotlink is forced to go down in order to let the higher-prio link getting dialed again.

We recommend to use the `permanent` operation mode for WAN links in general. However, in case of time-limited mobile tariffs for instance, the `switchover` mode might be applicable. By using the `distributed` mode, it is possible to distribute outgoing traffic over multiple WAN links based on their weight ratio.

Attention:
You can have concurrent WWAN links which share a common resource like one WWAN module using SIM cards of different providers. In that case it would not be possible to find out if the link with the higher priority is available without putting down the low priority link. Therefore, such a link will behave like a `switchover`, even if configured as `permanent`.

For mobile links, it is further possible to pass through the WAN address towards a local host (also called Drop-In or IP Pass-through). In particular, the first DHCP client will receive the public IP address. More or less, the system acts like a modem in such case which can be helpful in case of firewall issues. Once established, the Web Manager can be reached over port 8080 using the WAN address but still over the LAN1 interface using port 80.

Parameter	WAN Link Operation Modes
disabled	Link is disabled
permanent	Link is being established permanently
on switchover	Link is being established on switchover, it will be dialed if previous links failed
distributed	Link is member of a load distribution group

Parameter	WAN Link Settings
Operation mode	The operation mode of the link
Weight	The weight ratio of a distributed link
Switch-back	Specifies the switch-back condition of a switchover link and the time after an active hotlink will be teared down
Bridge Mode	If WLAN client, specifies the bridge mode which will be used.
Bridging interface	If WLAN client, the LAN interface to which the WAN link should be bridged.

The following bridge modes can be configured for a WLAN client:

Parameter	Bridge modes
disabled	Disables the bridge mode
pseudo bridge	Enables a bridge like behavior by relaying DHCP and broadcast messages

NetModule routers provide a feature called IP pass-through (aka Drop-In mode). If enabled, the WAN address will be be passed-through to the first DHCP client of the specified LAN interface. As Ethernet-based communication requires additional addresses, we pick an appropriate subnet to talk to the LAN host. In case this overlaps with other addresses of your WAN network, you may optionally specify the

network given by your provider to avoid any address conflicts.

Parameter	IP Pass-Through Settings
IP Pass-through	Enables or disables IP pass-through
Interface	Specifies the interface on which the address shall be passed-through
WAN network	Specifies the WAN network
WAN netmask	Specifies the WAN netmask

Supervision

Network outage detection on a per-link basis can be performed by sending pings on each link to some authoritative hosts. A link will be declared as down in case all trials have failed and only as up if at least one host can be reached.

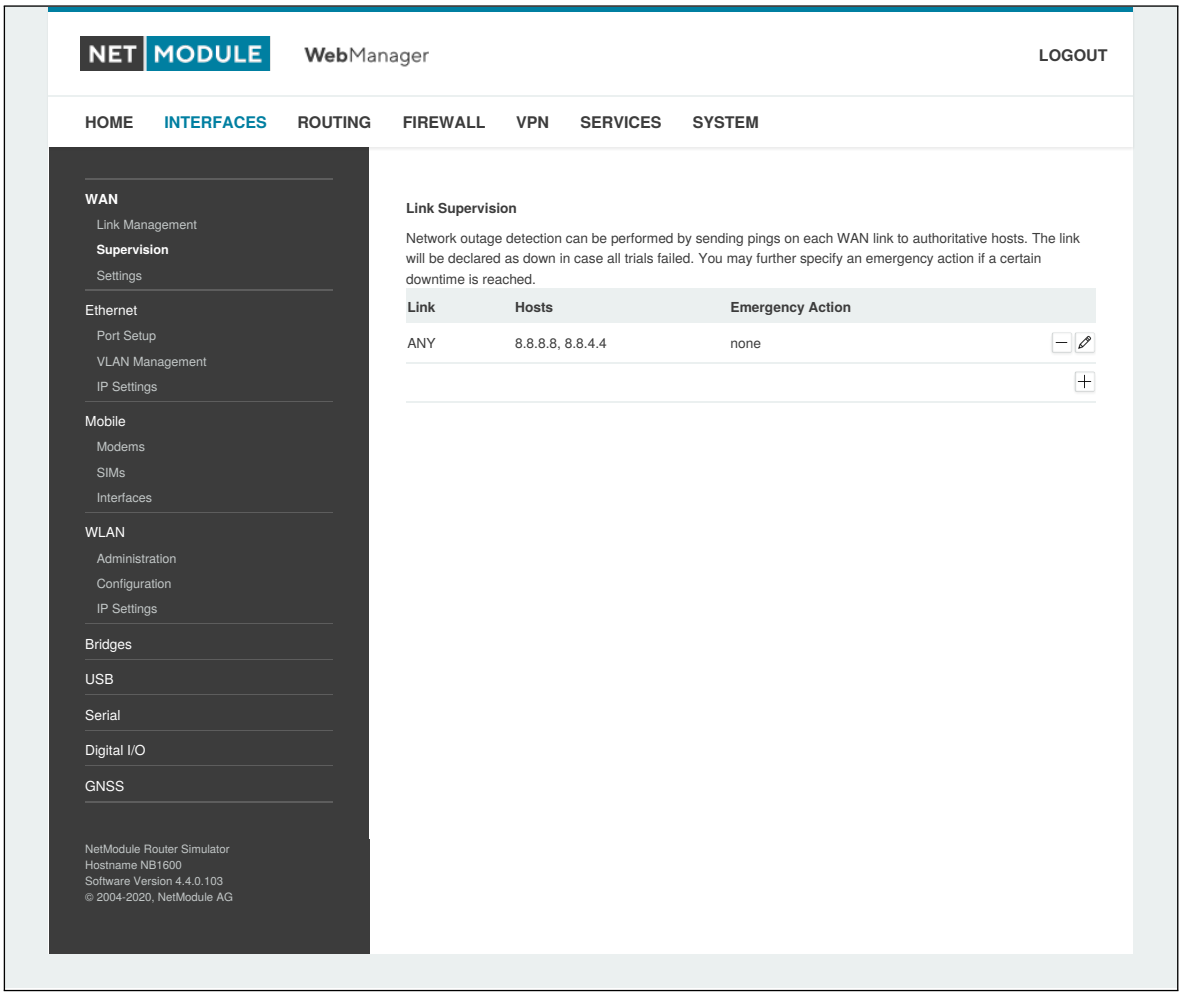


Figure 5.4.: Link Supervision

Parameter	Supervision Settings
Link	The WAN link to be monitored (can be ANY)
Mode	Specifies whether the link shall only be monitored if being up (e.g. for using a VPN tunnel) or if connectivity shall be also validated at connection establishment (default)
Primary host	The primary host to be monitored
Secondary host	The secondary host to be monitored (optional)
Ping timeout	The amount of time in milliseconds a response for a single ping can take, consider to increase this value in case of slow and tardy links (such as 2G connections)
Ping interval	The interval in seconds at which pings are transmitted on each interface
Retry interval	The interval in seconds at which pings are re-transmitted in case a first ping failed
Max. number of failed trials	The maximum number of failed ping trials until the link will be declared as down
Emergency action	The emergency action which should be taken after a maximum downtime has been reached. Using `reboot` would perform a reboot of the system, `restart link services` will restart all link-related applications including a reset of the modem.

WAN Settings

This page can be used to configure WAN specific settings like the Maximum Segment Size (MSS). The MSS corresponds to the largest amount of data (in bytes) that the router can handle in a single, unfragmented TCP segment. In order to avoid any negative side effects, the number of bytes in the data segment and the headers must not add up to more than the number of bytes in the Maximum Transmission Unit (MTU). The MTU can be configured per each interface and corresponds to the largest packet size that can be transmitted.

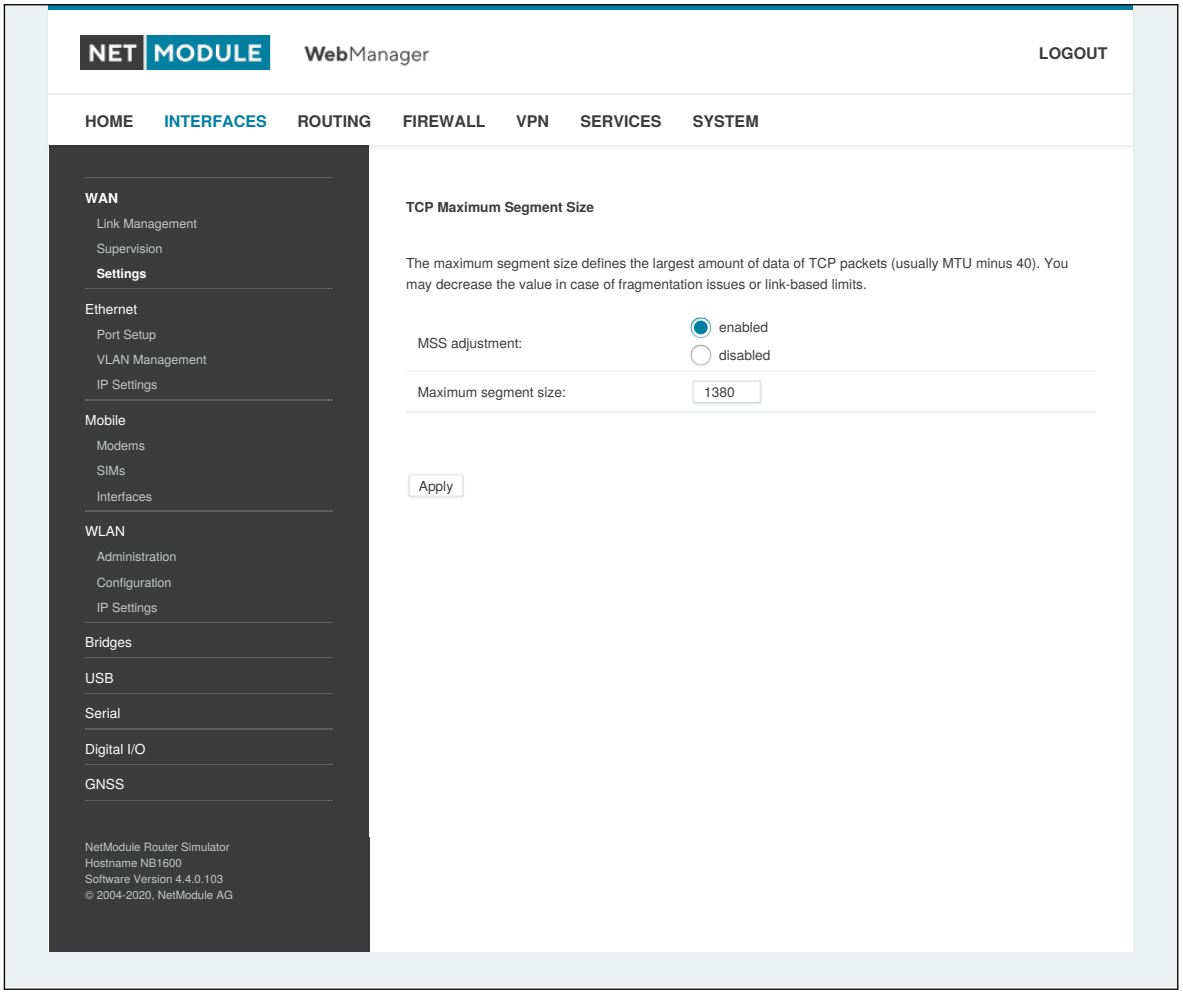


Figure 5.5.: WAN Settings

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

5.3.2. Ethernet

NB800 routers ship with one dedicated Ethernet port (ETH) which can be linked via RJ45 connectors. ETH1 usually forms the LAN1 interface which should be used for LAN purposes. Other interfaces can be used to connect other LAN segments or for configuring a WAN link. The LAN10 interface will be available as soon as a pre-configured USB Ethernet device has been plugged in.

Ethernet Port Assignment

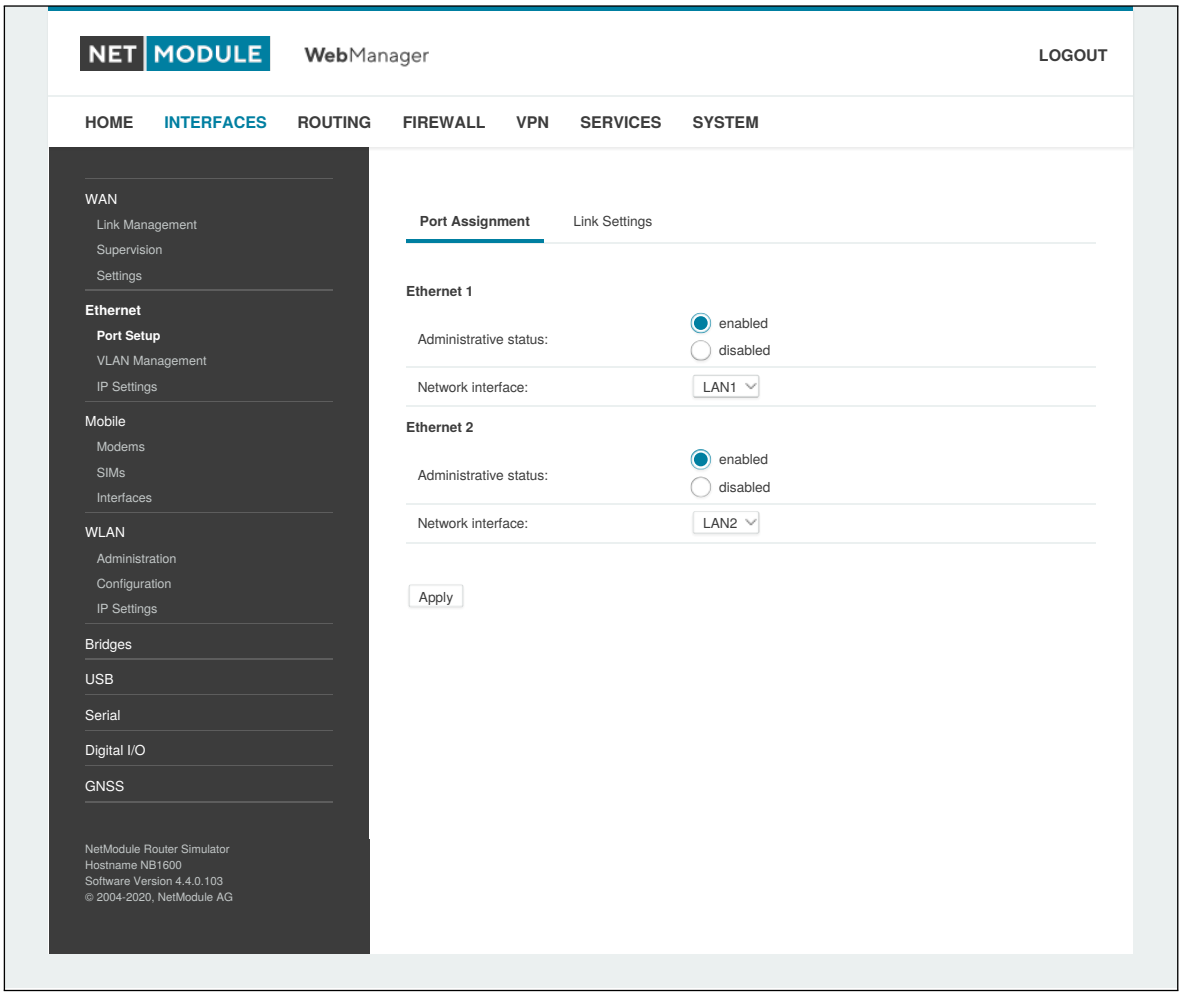


Figure 5.6.: Ethernet Ports

This menu can be used to individually assign each Ethernet port to a LAN interface, just in case you want to have different subnets per port or use one port as WAN interface. You may assign multiple ports to the same interface.

Ethernet Link Settings

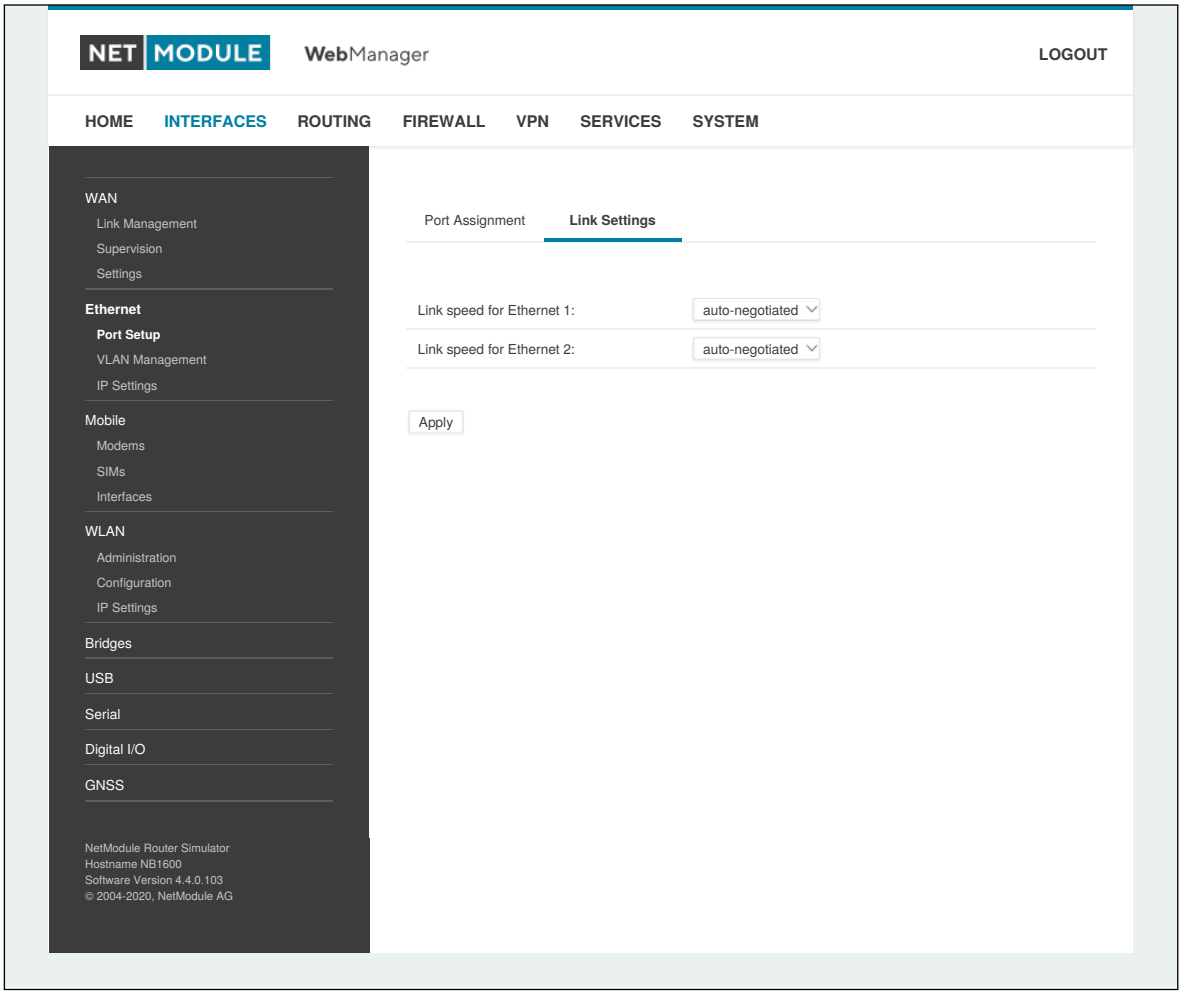


Figure 5.7.: Ethernet Link Settings

Link negotiation can be set for each Ethernet port individually. Most devices support auto-negotiation which will configure the link speed automatically to comply with other devices in the network. In case of negotiation problems, you may assign the modes manually but it has to be ensured that all devices in the network utilize the same settings then.

Authentication via IEEE 802.1X

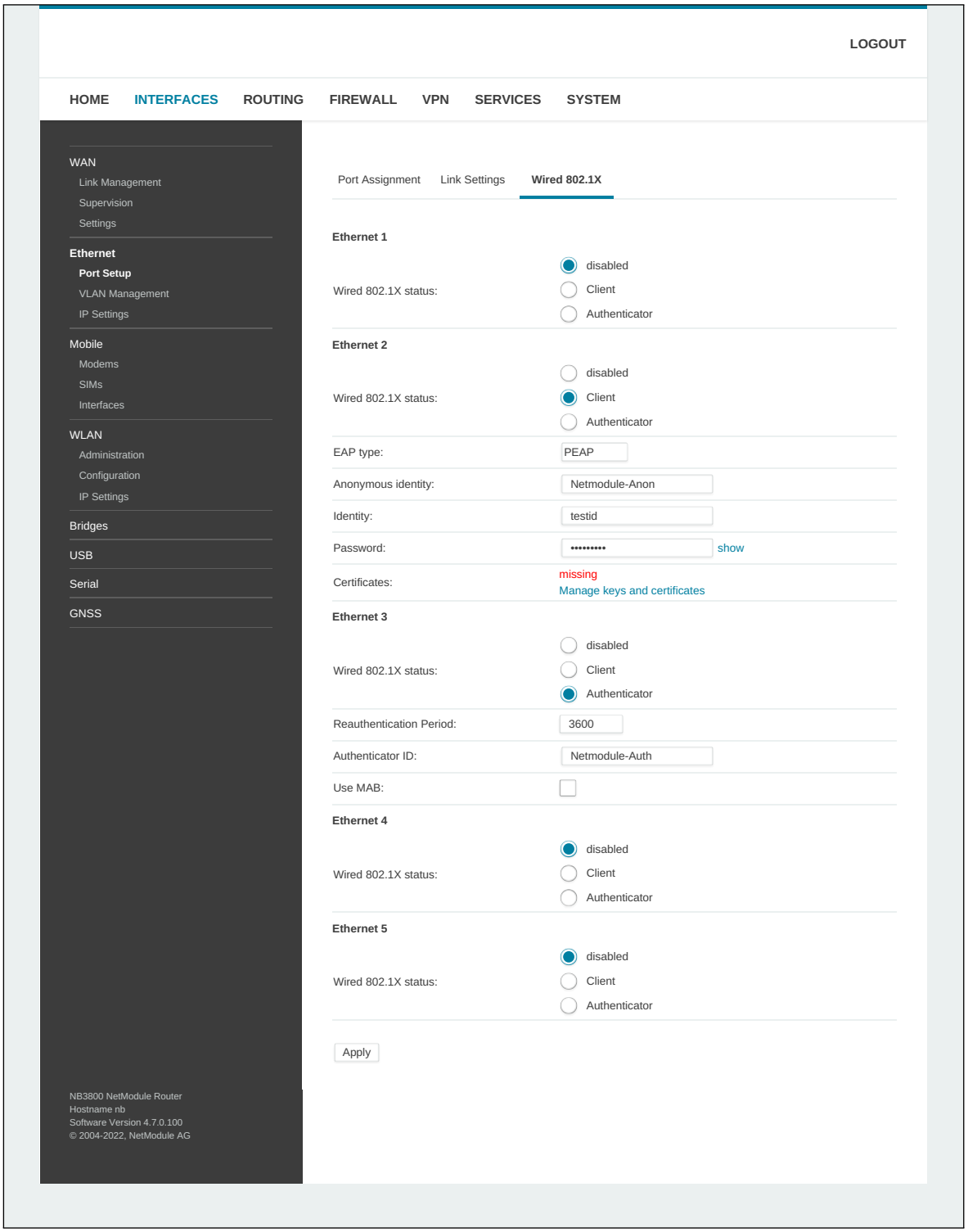


Figure 5.8.: Authentication via IEEE 802.1X

NetModule-routers support authentication via the IEEE 802.1X standard. This can be configured for each Ethernet port individually.
The following options exist:

Parameter	Wired IEEE 802.1X Client Settings
Wired 802.1X status	If set to Client, the router will authenticate on this port via IEEE 802.1X
EAP type	Which protocol to use to authenticate
Anonymous identity	The anonymous identify for PEAP authentication
Identity	The identify for EAP-TLS or PEAP authentication (required)
Password	The password for PEAP authentication (required)
Certificates	Certificates for authentication via EAP-TLS or PEAP. Can be configured in chapter 5.8.8

Parameter	Einstellungen IEEE 802.1X Authenticator
Wired 802.1X status	If set to Authenticator, the router will propagate IEEE 802.1X authentication requests on this port to a configured RADIUS server (see chapter 5.8.2)
Reauthentication Period	Time in seconds after which a connected client has to reauthenticate
Authenticator ID	This unique name identifies the authenticator at the RADIUS server
Use MAB	Activate this option if you want to allow authentication of devices which are not capable of IEEE 802.1X via MAC Authentication Bypass. These are reported to the RADIUS server with their MAC address as user name and password

VLAN Management

NetModule routers support Virtual LAN according to IEEE 802.1Q which can be used to create virtual interfaces on top of an Ethernet interface. The VLAN protocol inserts an additional header to Ethernet frames carrying a VLAN Identifier (VLAN ID) which is used for distributing the packets to the associated virtual interface. Any untagged packets, as well as packets with an unassigned ID, will be distributed to the native interface.

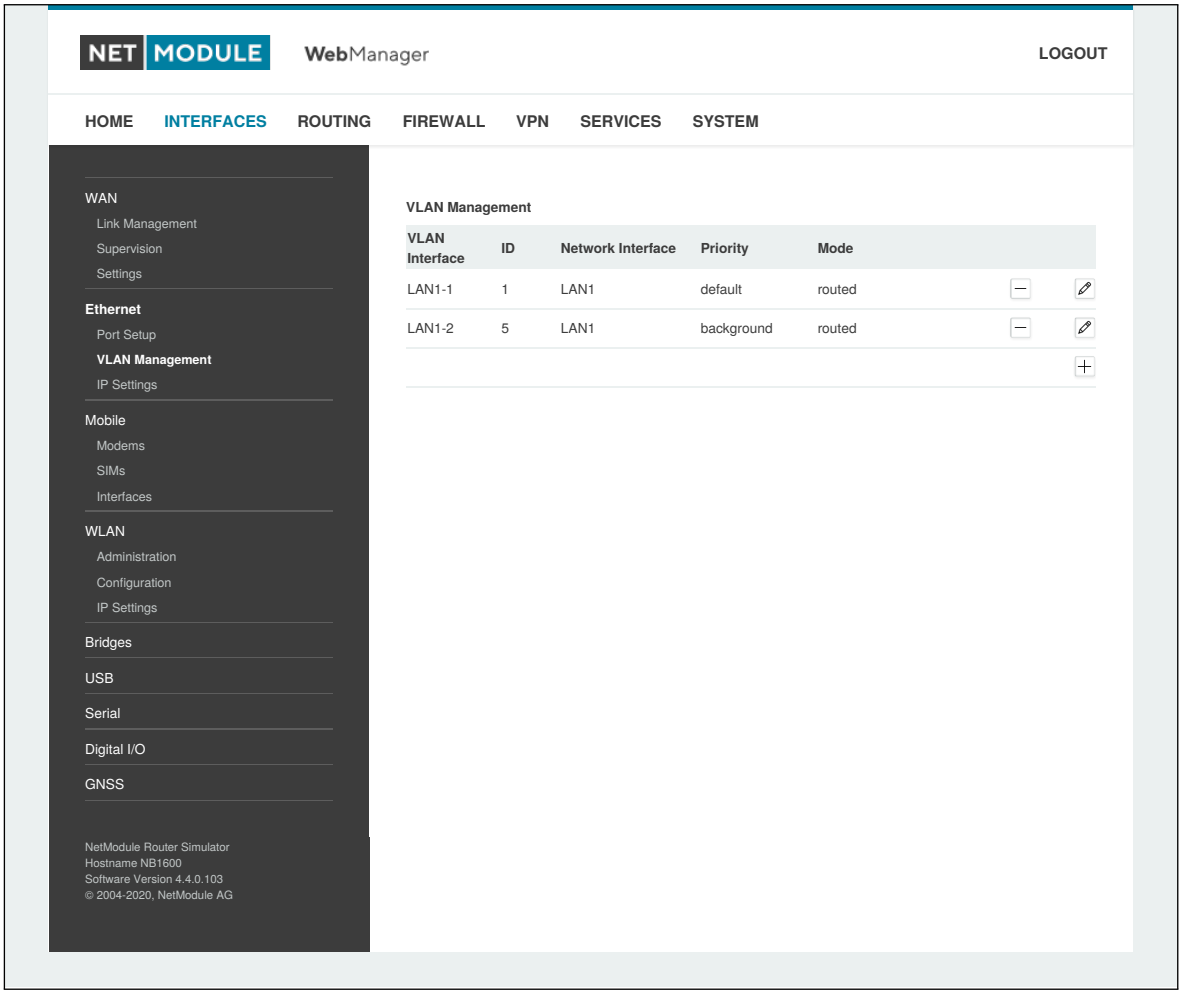


Figure 5.9.: VLAN Management

In order to form a distinctive subnet, the network interface of a remote LAN host must be configured with the same VLAN ID as defined on the router. Further, 802.1P introduces a priority field which influences packet scheduling in the TCP/IP stack.

The following priority levels (from lowest to highest) exist:

Parameter	VLAN Priority Levels
0	Background
1	Best Effort
2	Excellent Effort
3	Critical Applications
4	Video (< 100 ms latency and jitter)
5	Voice (< 10 ms latency and jitter)
6	Internetwork Control
7	Network Control

IP Settings

This page can be used to configure IP addressing for your LAN/WAN Ethernet interfaces.

Parameter	LAN IP Settings
Mode	Defines whether this interface is being used as LAN or WAN interface.
MTU	The Maximum Transmission Unit for the interface, if provided it will specify the largest size of a packet transmitted on the interface.

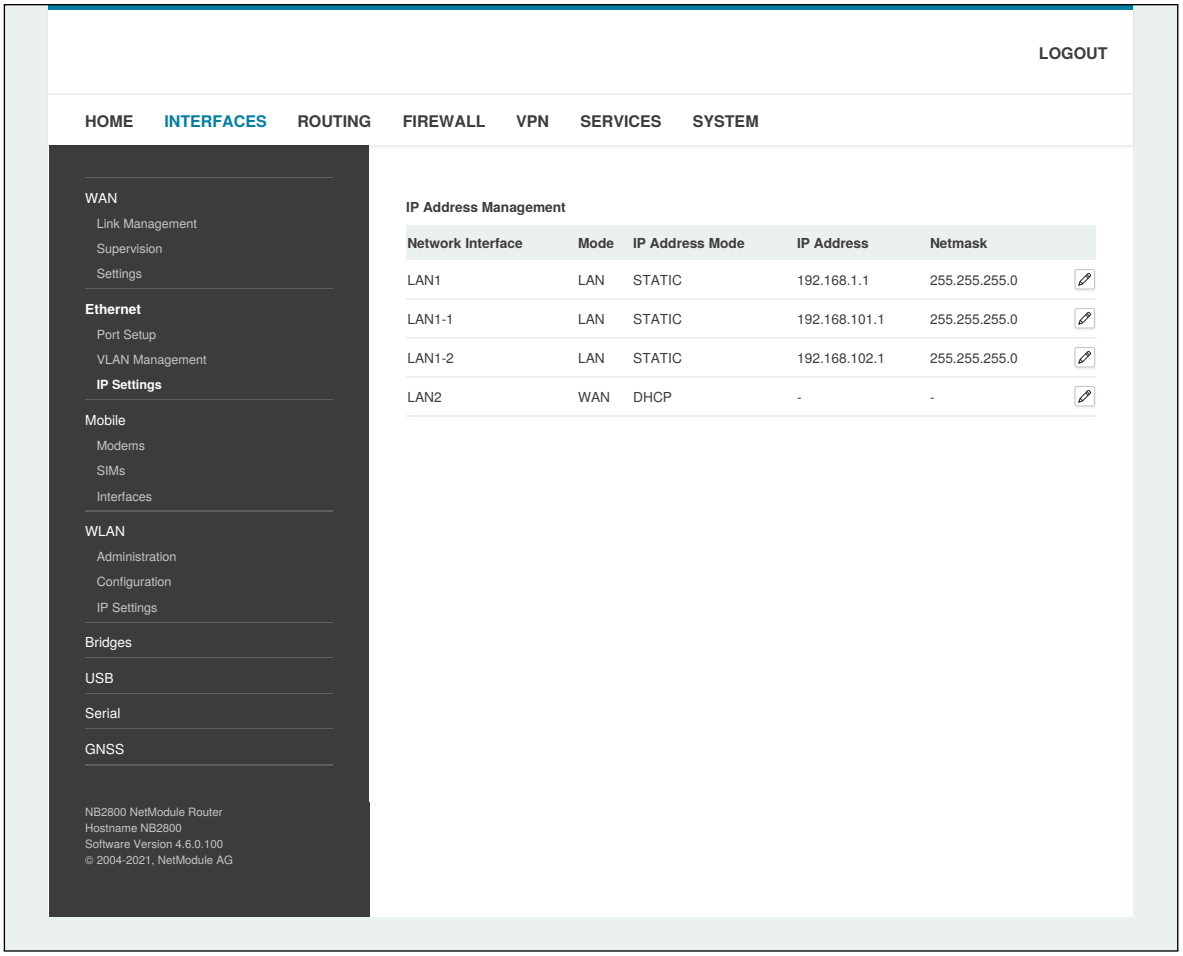


Figure 5.10.: LAN IP Configuration

LAN-Mode

When running in LAN mode, the interface may be configured with the following settings:

Parameter	LAN IP Settings
IP address	The IP interface address
Netmask	The netmask for this interface
Alias IP address	Optional alias IP interface address
Alias Netmask	Optional alias netmask for this interface
MAC	Custom MAC adress for this interface (not supported for VLANs)

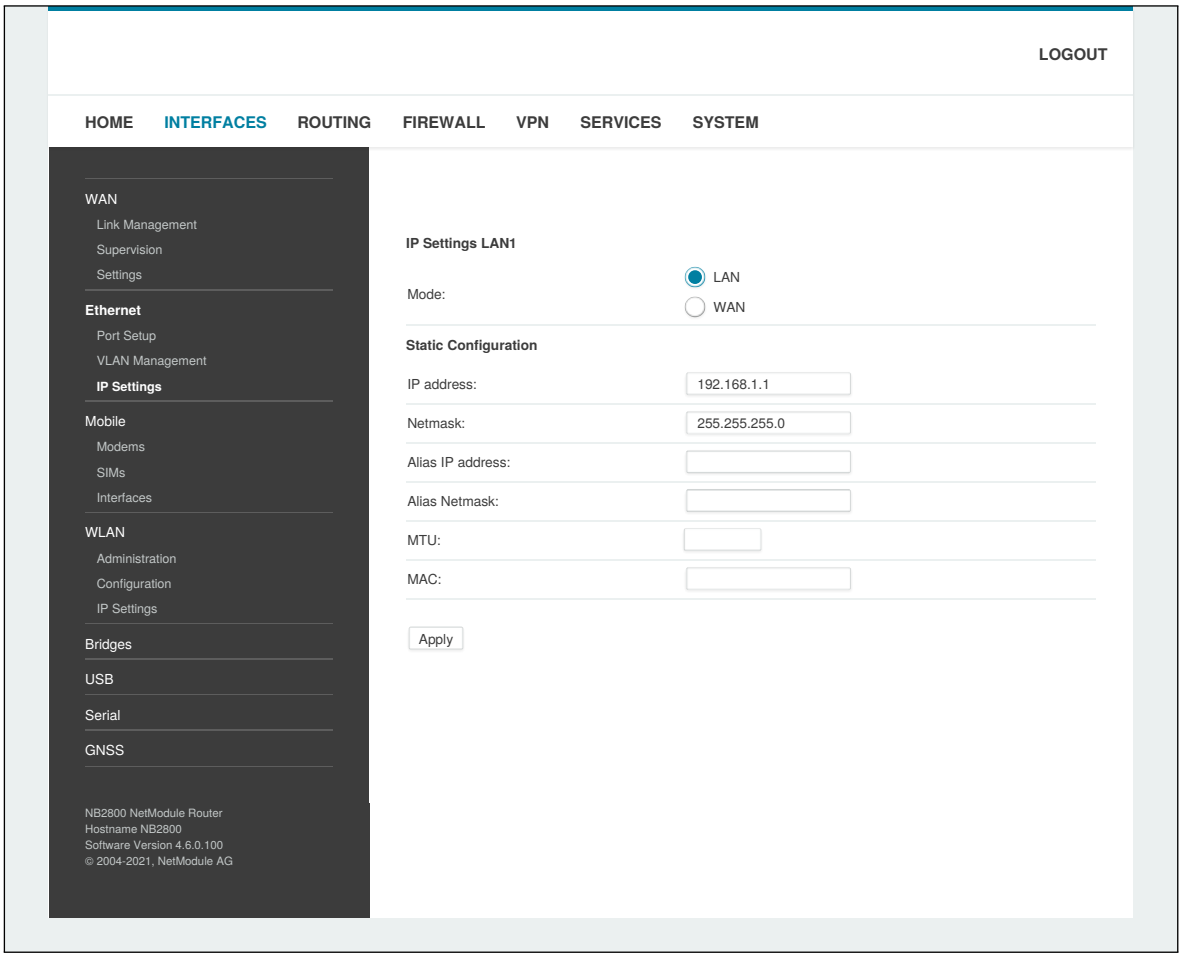


Figure 5.11.: LAN IP Configuration - LAN Interface

WAN-Mode

When running in WAN mode, the interface may be configured with two IP versions in the following way:

Parameter	Description
IPv4	Only Internet Protocol Version 4
IPv6	Only Internet Protocol Version 6
Dual-Stack	Run Internet Protocol Version 4 and Version 6 in parallel

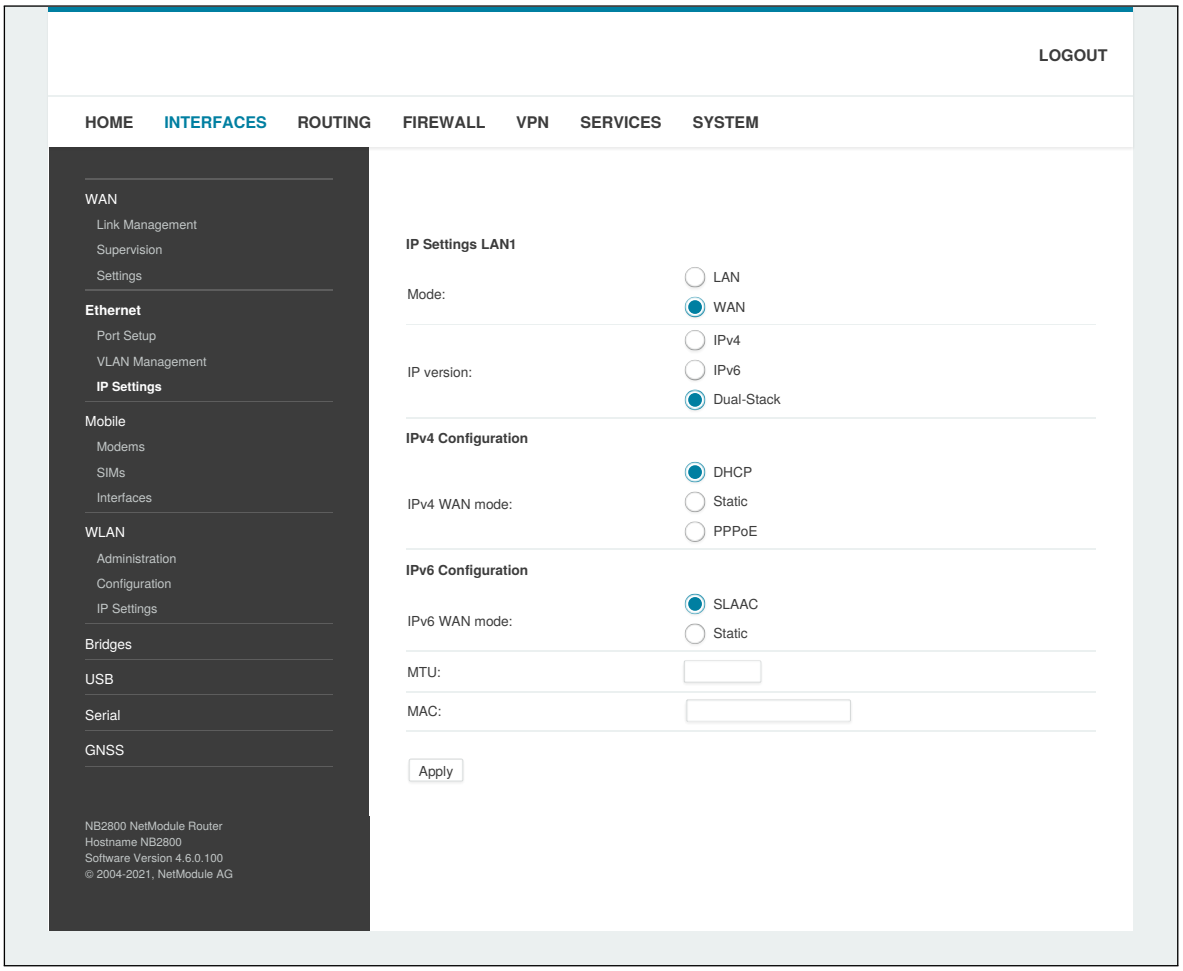


Figure 5.12.: LAN IP Configuration - WAN Interface

Depending on the selected IP version you can configure your interface with the following settings:

IPv4 Settings

The router can configure its IPv4 address the following ways:

Parameter	IPv4 WAN-Modes
DHCP	When running as DHCP client, no further configuration is required because all IP-related settings (address, subnet, gateway, DNS server) will be retrieved from a DHCP server in the network.
Static	Allows you to define static values. Caution has to be taken to assign a unique IP address as it would otherwise raise IP conflicts in the network.
PPPoE	PPPoE is commonly used when communicating with another WAN access device (like a DSL modem).

IPv4-PPPoE Settings

The following settings can be applied:

Parameter	PPPoE Configuration
User name	PPPoE user name for authenticating at the access device
Password	PPPoE password for authenticating at the access device
Service name	Specifies the service name set of the access concentrator and can be left blank unless you have multiple services on the same physical network and need to specify the one you want to connect to.
Access concentrator name	The name of the concentrator (the PPPoE client will connect to any access concentrator if left blank)

IPv6 Settings

The router can configure its IPv6 address the following ways:

Parameter	IPv6 WAN-Modes
SLAAC	All IP-related settings (address, prefix, routes, DNS server) will be retrieved by the neighbor-discovery-protocol through stateless-address-autoconfiguration.
Static	Allows you to define static values. Caution has to be taken to assign a unique IP address as it would otherwise raise IP conflicts in the network. You can only configure global addresses. The link-local address is automatically generated via the MAC address.

DNS Server

When all enabled IP versions are set to `Static`, you may configure an interface-specific nameserver. To override the interface-specific nameservers see chapter 5.7.3.

5.3.3. Mobile

Modems

Configuration

This page lists all available WWAN modems. They can be disabled on demand.

Query

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

SIMs

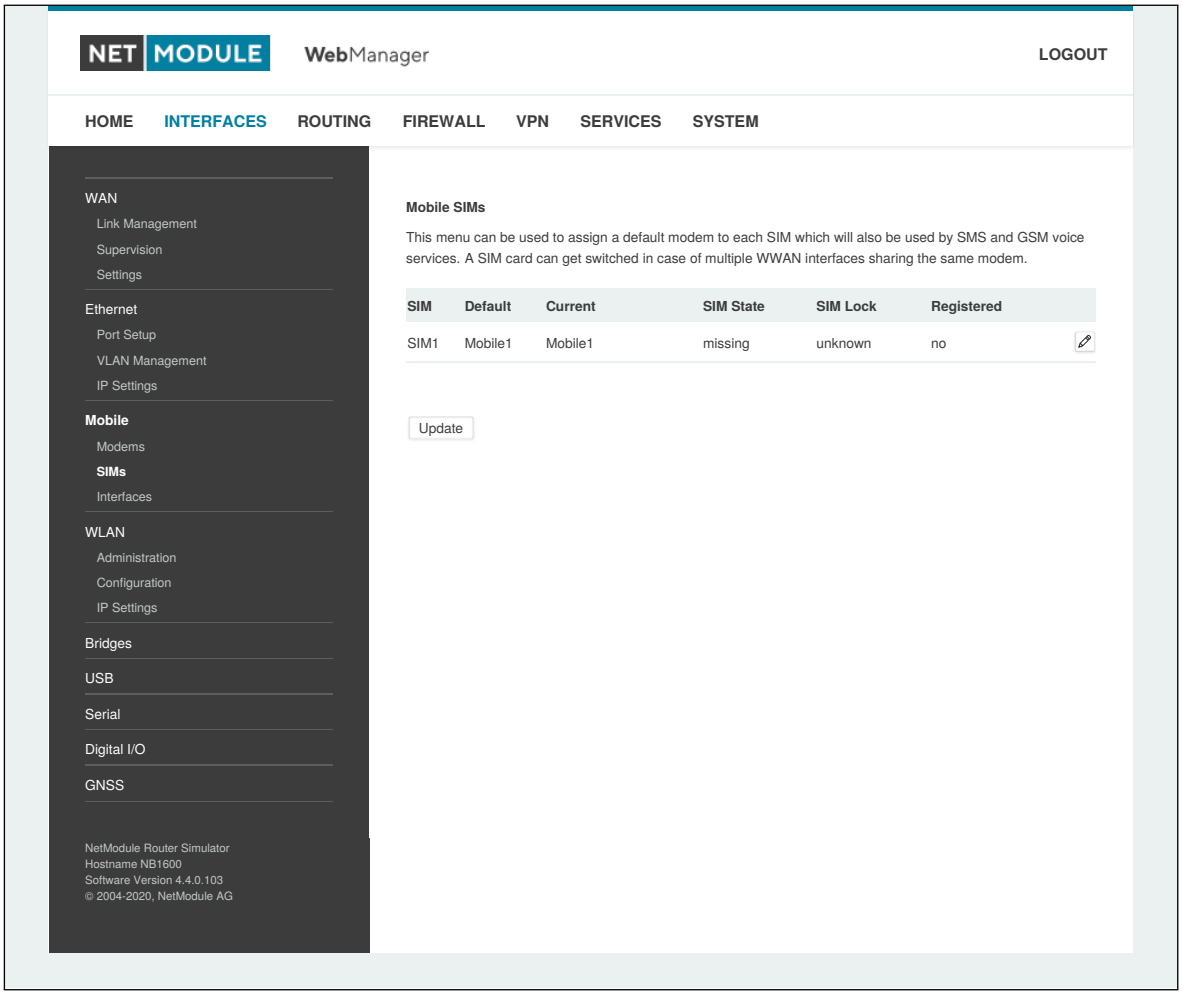


Figure 5.13.: SIMs

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`. If

not, please double-check your PIN.
Please keep in mind that registering to a network usually takes some time and depends on signal strength and possible radio interferences. You may hit the `Update` button at any time in order to restart PIN unlocking and trigger another network registration attempt.
Under some circumstances (e.g. in case the modem flaps between base stations) it might be necessary to set a specific service type or assign a fixed operator. The list of operators around can be obtained by initiating a network scan (may take up to 60 seconds). Further details can be retrieved by querying the modem directly, a set of suitable commands can be provided on request.

Configuration

A SIM card is generally assigned to a default modem but might be switched, 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 naturally affect their operation.

The following settings can be applied:

Parameter	WWAN SIM Configuration
PIN code	The PIN code for unlocking the SIM card
PUK code	The PUK code for unlocking the SIM card (optional)
Default modem	The default modem assigned to this SIM card
Preferred service	The preferred service 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.
Registration mode	The desired registration mode
Network selection	Defines which network shall be selected. This can be bound to a specific provider ID (PLMN) which can be retrieved by running a network scan.

eSIM / eUICC

Attention:
Note that eUICC profiles are NOT affected by a factory reset. To remove an eUICC profile from a device, manually remove it before performing the factory reset.

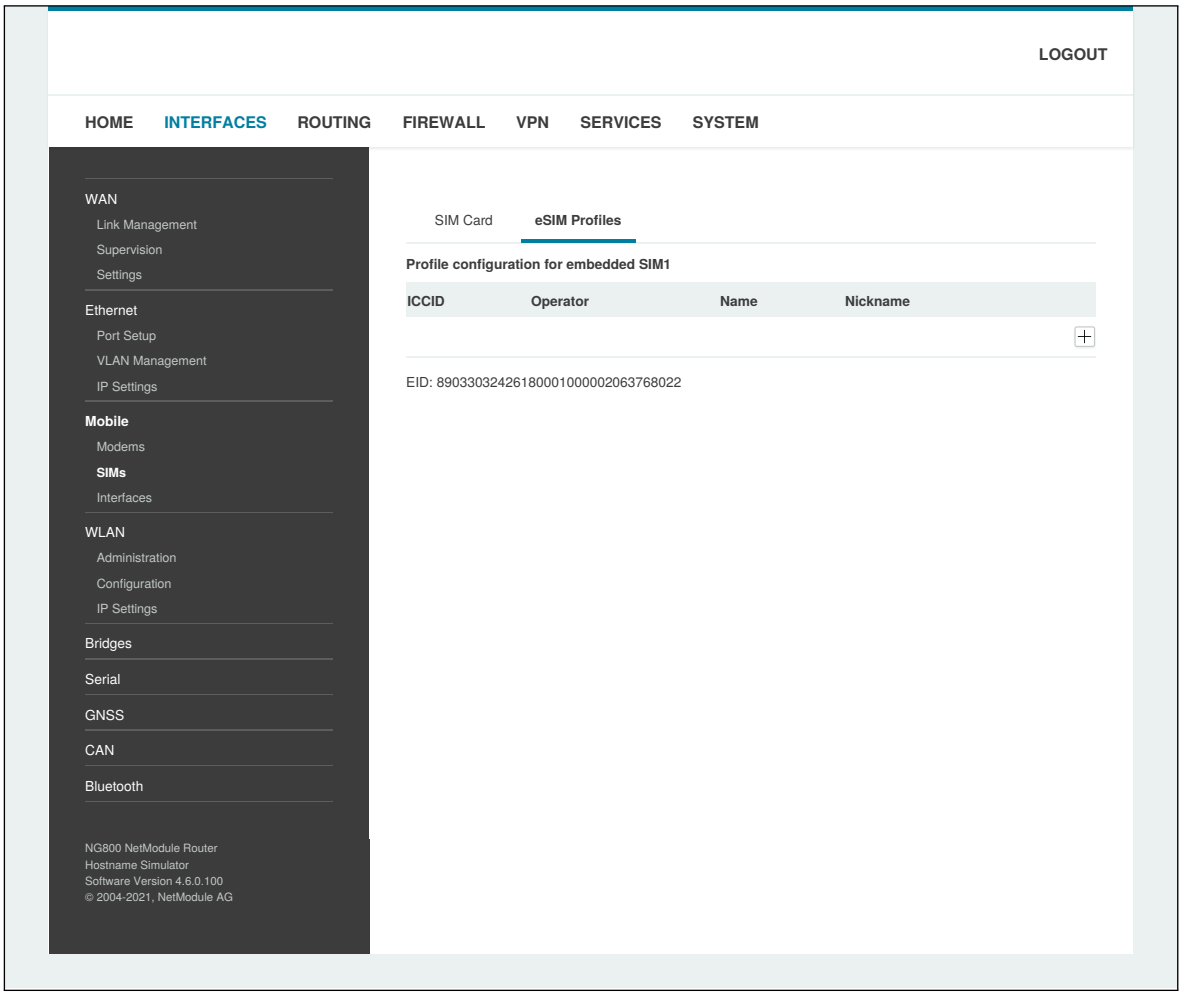


Figure 5.14.: eSIM Profiles

Selected router models contain an eUICC (embedded universal integrated circuit card) which allows you to download eSIM profiles from the internet to the router instead of having to insert a physical SIM card into the router. The eSIM profiles to be installed must be compliant to the GSMA RSP Technical Specification SGP.22. These are the same eSIM profiles that are used with current mobile phones. Profiles according to the older GSMA SGP.02 specification are not supported.
eSIM profiles can be managed on the "eSIM Profiles" tab of the "Mobile / SIMs" configuration page. The management page allows you to display all installed eSIM profiles as well as to install, enable, disable and delete eSIM profiles. It is also possible to store a nickname for each profile.
The eUICC can store up to about 7 eSIM profiles depending on the size of the profiles. Only one of those profiles can be active at a time.
In order to install new eSIM profiles, you need to first establish IP connectivity to the internet so that

the router can download the profile from the mobile network operator's server.

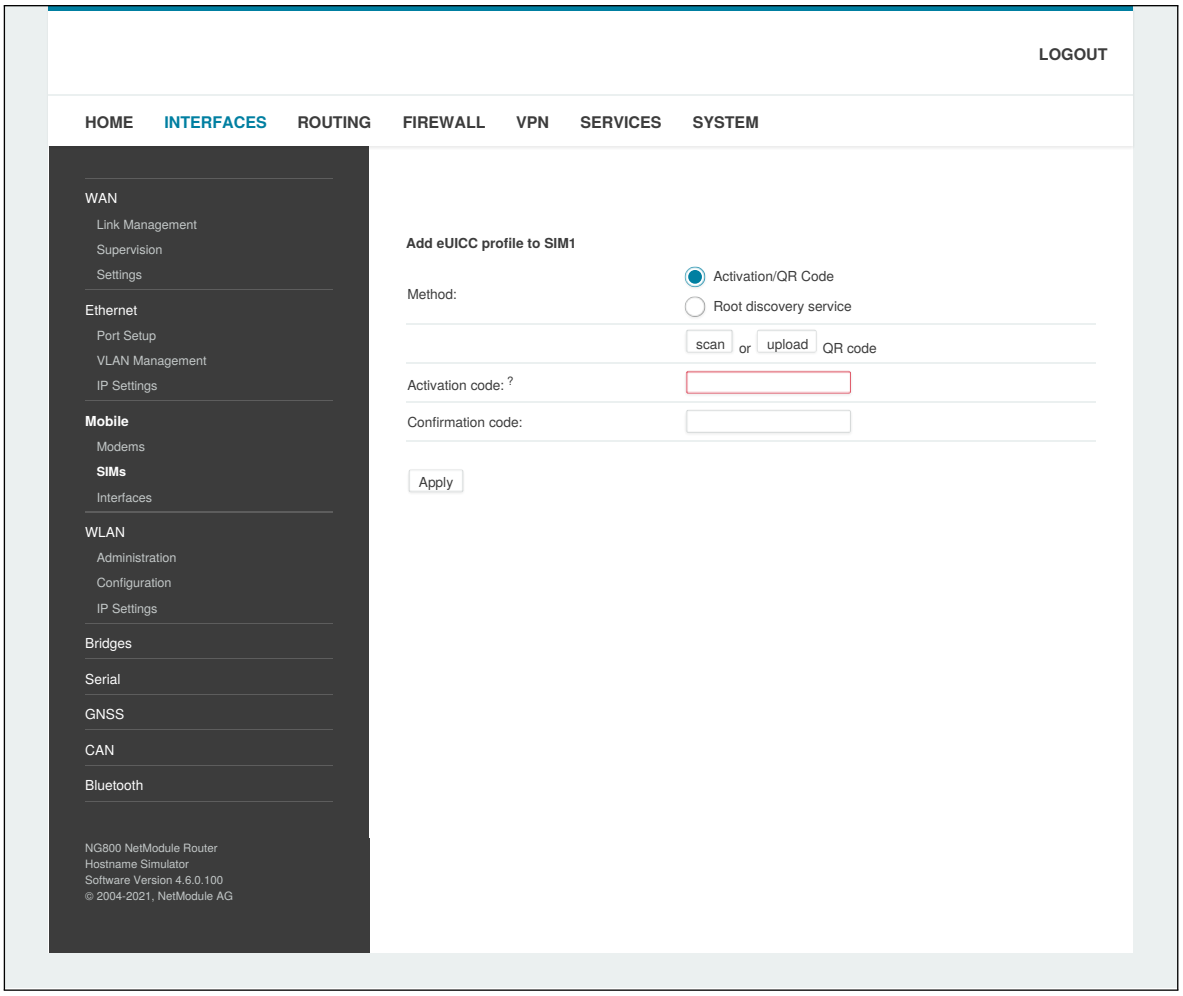


Figure 5.15.: Add eUICC Profile

The following two ways are supported to install eSIM profiles and can be selected on the eSIM profiles configuration page:

1. QR code provided by the network operator
To download the eSIM profile using this method your mobile network operator provides you a QR code which contains the information about the eSIM profile to be installed. If the device you are using to access the configuration GUI of the router has a camera, you can scan the QR code using the camera. Otherwise you can also upload an image file of the QR code. Or it is also possible to enter the contents of the QR code manually into the corresponding input field.

2. GSMA Root Discovery Service
When using this method, you need to provide the EID, which is a unique number that identifies the eUICC of the router, to your mobile network operator. The EID is displayed on the eSIM profiles configuration page. The operator will then prepare the eSIM profile for your router on his provisioning servers. Afterwards, you can use the GSMA Root Discovery Service method to retrieve the eSIM

profile without having to specify any additional information for the download.
Note: Most mobile network operators allow only one download of an eSIM profile. So, if you download the profile once and delete it afterwards, you will not be able to download the same profile a second time. In this case you would need to request a new eSIM profile from your operator.

WWAN Interfaces

This page can be used to manage your WWAN interfaces. The resulting link will pop up automatically as WAN link once an interface has been added. Please refer to chapter 5.3.1 for how to manage them. The Mobile LED will be blinking during the connection establishment process and goes on as soon as the connection is up. Refer to section 5.8.7 or consult the system log files for troubleshooting the problem in case the connection did not come up.

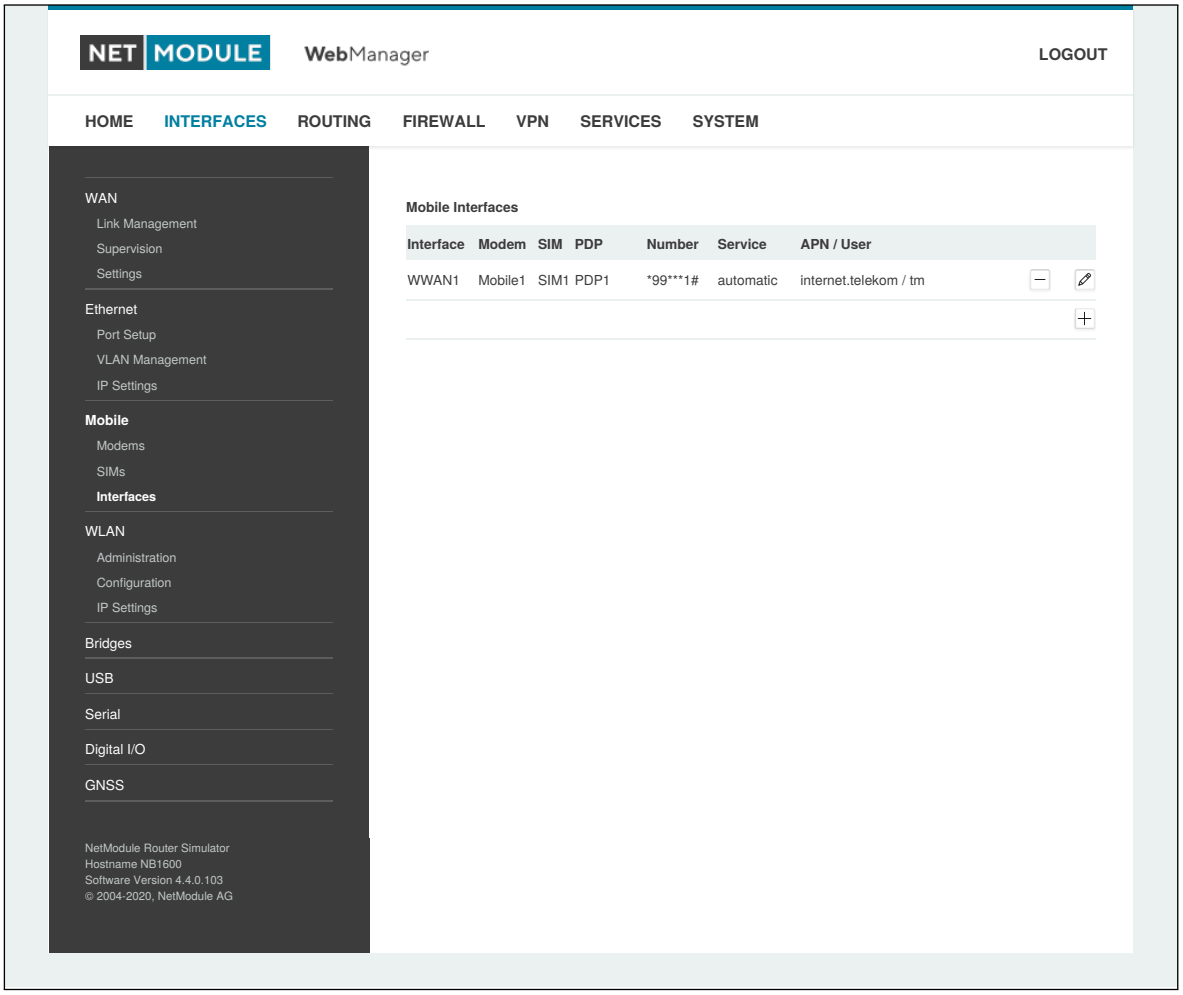


Figure 5.16.: WWAN Interfaces

The following mobile settings are required:

Parameter	WWAN Mobile Parameters
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 manually:

Parameter	WWAN Connection Parameters
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. +41xx).
Access point name	The access point name (APN) being used
IP version	What IP version to use. Dual-stack lets you use IPv4 and IPv6 together. Please note, that your provider might not support all IP versions.
Authentication	The authentication scheme being used, if required this can be PAP or/and CHAP
Username	The user-name used for authentication
Password	The password used for authentication

Furtheron, you may configure the following advanced settings:

Parameter	WAN Advanced Parameters
Required signal strength	Sets a minimum required signal strength before the connection is dialed
Home network only	Determines whether the connection should only be dialed when registered to a home network
Negotiate DNS	Specifies whether the DNS negotiation should be performed and the retrieved name-servers should be applied to the system
Call to ISDN	Has to be enabled in case of 2G connections talking to an ISDN modem
Header compression	Enables or disables 3GPP header compression which may improve TCP/IP performance over slow serial links. Has to be supported by your provider.
Data compression	Enables or disables 3GPP data compression which shrinks the size of packets to improve throughput. Has to be supported by your provider.
Client address	Specifies a fixed client IP address if assigned by the provider
MTU	The Maximum Transmission Unit for this interface

5.3.4. WLAN

WLAN Management

In case your router is shipping with a WLAN (or Wi-Fi) module you can operate it either as `client`, `access point`, `mesh point` or certain `dual modes`. As a `client` it can create an additional WAN link which for instance can be used as backup link. As access point, it can form another LAN interface which can be either bridged to an Ethernet-based LAN interface or create a self-contained IP interface which can be used for routing and to provide services (such as DHCP/DNS/NTP) in the same way like an Ethernet LAN interface does. As `mesh point`, it can create a wireless mesh network to provide a backhaul connectivity with dynamic path selection. As `dual mode`, it is possible to run access point and client or mesh point and access point functionality on the same radio module.

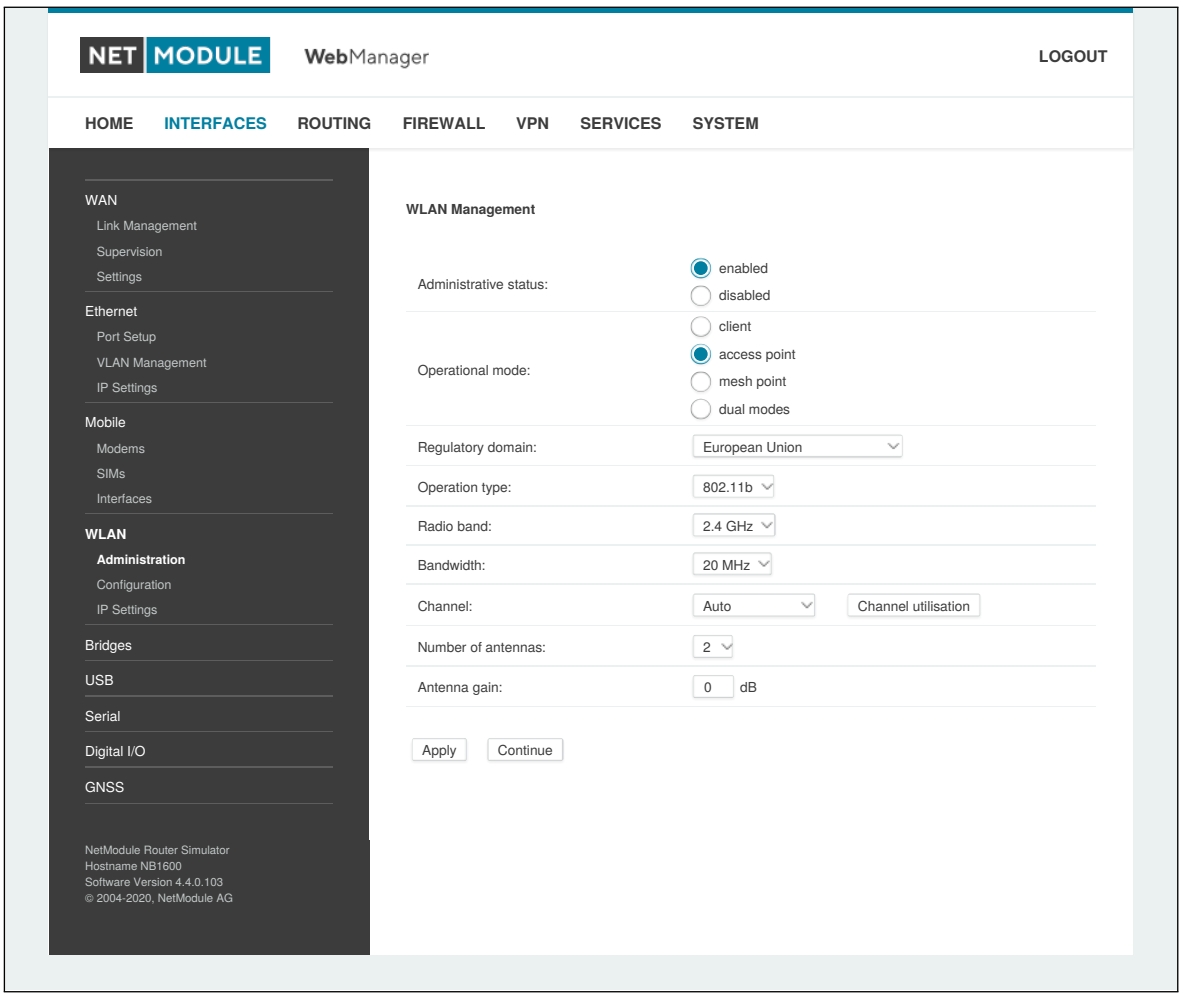


Figure 5.17.: WLAN Management

If the administrative status is set to `disabled`, the module will be powered off in order to reduce the overall power consumption. Regarding antennas, we generally recommend using two antennas for better coverage and throughput. A second antenna is definitely mandatory if you want to achieve higher throughput rates as in 802.11n.

A WLAN `client` and a `mesh point` will automatically became a WAN link and can be managed as described in chapter 5.3.1.

Configurable parameters for `access-point`, `client` mode, `mesh point` and any `dual mode`:

Parameter	WLAN Management
Regulatory Domain	Select the country the Router operates in
Number of antennas	Set the number of connected antennas
Antenna gain	Specify the antenna gain for the connected antennas. Please refer to the antennas datasheet for the correct gain value.
Tx power	Specifies the max. transmit power used in dBm.
Disable low data rates	Avoid sticky clients by disabling low data rates.

Warning
Please be aware that any inappropriate parameters can lead to an infringement of conformity regulations.

Running as `access point` or `dual mode`, you can further configure the following settings:

Parameter	WLAN Management
Operation type	Specifies the desired IEEE 802.11 operation mode
Radio band	Selects the radio band to be used for connections, depending on your module it could be 2.4 or 5 GHz
Outdoor	Shows the 5 GHz outdoor channels
Bandwidth	Specify the channel bandwidth operation mode
Channel	Specifies the channel to be used
Short Guard Interval	Enables the Short Guard Interval (SGI)

Running as `client`, you can further configure the following settings:

Parameter	WLAN Management
Scan channels	Select if all supported channels should be scanned or just user defined channels
2.4 GHz	Set the channels which should be scanned in 2.4 GHz
5 GHz	Set the channels which should be scanned in 5 GHz

Available operation modes are:

Standard	Frequencies	Bandwidth	Data Rate
802.11a	5 GHz	20 MHz	54 Mbit/s
802.11b	2.4 GHz	20 MHz	11 Mbit/s
802.11g	2.4 GHz	20 MHz	54 Mbit/s
802.11n	2.4 GHz	20 MHz	144 Mbit/s
802.11n	5 GHz	40 MHz	150 Mbit/s

Table 5.25.: IEEE 802.11 Network Standards

Running as `mesh point`, you can further configure the following settings:

Parameter	WLAN Mesh-Point Management
Radio band	Selects the radio band to be used for connections, depending on your module it could be 2.4 or 5 GHz
Channel	Specifies the channel to be used

Note: 802.11n with 2x2 MIMO in 2.4 GHz and 1x1 in 5 GHz.

Prior to setting up an access point, it is always a good idea to run a network scan for getting a list of neighboring WLAN networks and then choose the less interfering channel. Please note that two adequate channels are required for getting good throughputs with 802.11n and a bandwidth of 40 MHz.

WLAN Configuration

Running in `client` mode, it is possible to connect to one ore more remote access-points. The system will switch to the next network in the list in case one goes down and return to the highest-prioritized network as soon as it comes back. You can perform a WLAN network scan and pick the settings from the discovered information directly. The authentication credentials have to be obtained by the operator of the remote access point.

Parameter	WLAN Client Configuration
SSID	The network name (called SSID)
Security mode	The desired security mode
WPA mode	The desired encryption method. WPA3 should be preferred over WPA2 and WPA1
WPA cipher	The WPA cipher to be used, the default is to run both (TKIP and CCMP)
Identity	The identity used for WPA-RADIUS and WPA-EAP-TLS
Passphrase	The passphrase used for authentication with WPA-Personal, otherwise the key passphrase for WPA-EAP-TLS
Required signal strength	Required signal strength to esablish the connection

The `client` is performing background scans for the purpose of roaming within an ESS. The background scans are based on the current signal strenght.

Parameter	WLAN Client Background Scan Parameters
Threshold	The signal strength threshold in dBm when the long or short time interval should occur
Long interval	The time in seconds when a background scan should be performed if the threshold is above the given threshold value
Short interval	The time in seconds when a background scan should be performed if the threshold is below the given threshold value

Running in `access-point` mode you can create up to 2 SSIDs with each running their own network configuration. The networks can be individually bridged to a LAN interface or operate as dedicated interface in routing-mode.

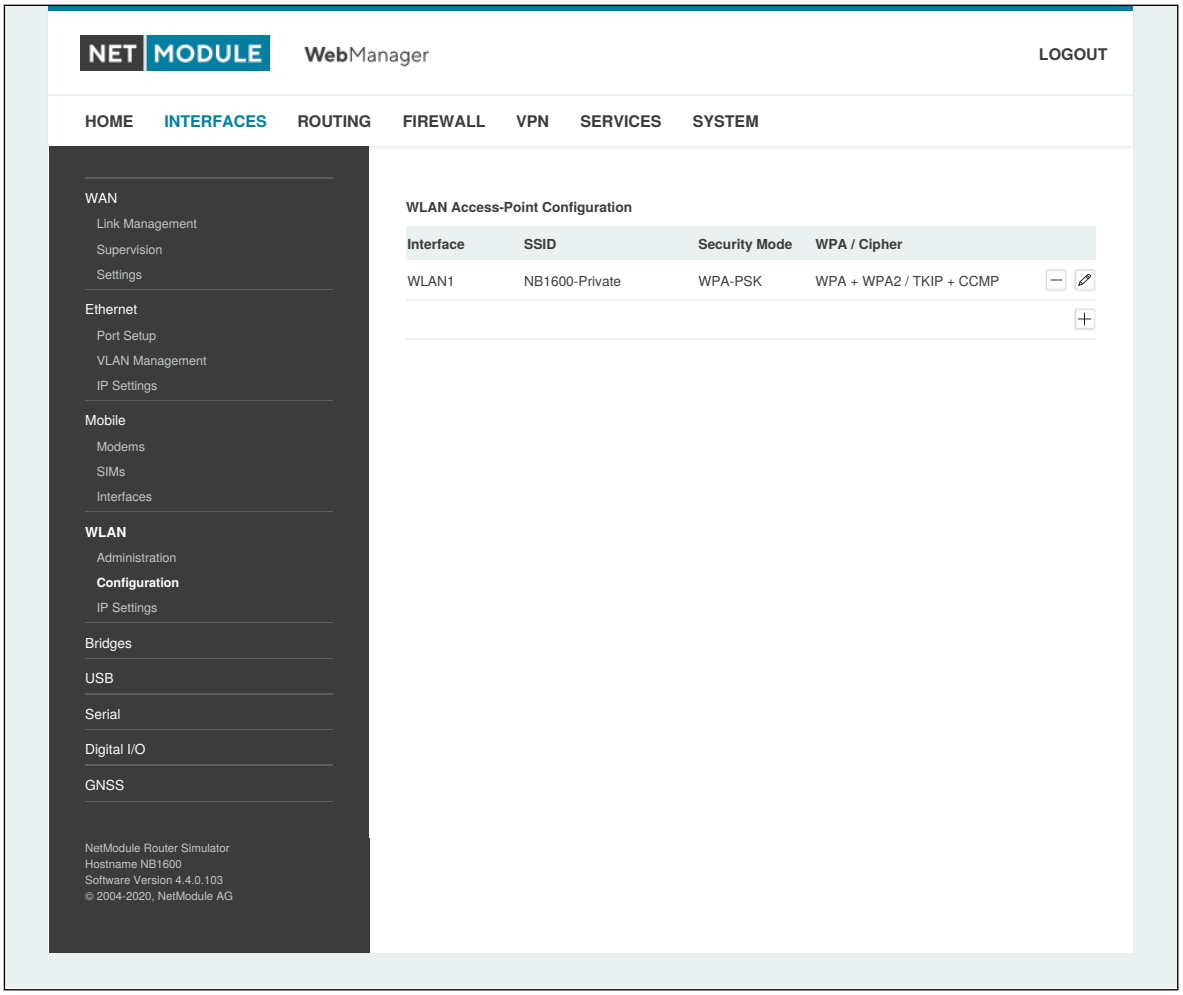


Figure 5.18.: WLAN Configuration

This section can be used to configure security-related settings.

Parameter	WLAN Access-Point Configuration
SSID	The network name (called SSID)
Security mode	The desired security mode
WPA mode	WPA2 should be preferred over WPA1, running WPA/WPA2 mixed-mode offers both.
WPA cipher	The WPA cipher to be used, the default is to run both (TKIP and CCMP)
Passphrase	The passphrase used for authentication with WPA-Personal.
Force PMF	Enables Protected Management Frames
Hide SSID	Hides the SSID
Isolate clients	Disables client-to-client communication
Band steering master	The WLAN interface which the client should be steered to
Opportunistic Wireless Encryption transition	The WLAN interface for a seamless transition from an OPEN WLAN to an OWE encrypted WLAN interface
Accounting	Sets accounting profile

The following security modes can be configured:

Parameter	WLAN Security Modes
Off	SSID is disabled
None	No authentication, provides an open network
WEP	WEP (is nowadays discouraged)
WPA-Personal	WPA-Personal (TKIP, CCMP), provides password-based authentication
WPA-Enterprise	WPA-Enterprise in AP mode, can be used to authenticate against a remote RADIUS server which can be configured in chapter 5.8.2
WPA-RADIUS	EAP-PEAP/MSCHAPv2 in client mode, can be used to authenticate against a remote RADIUS server which can be configured in chapter 5.8.2
WPA-TLS	EAP-TLS in client mode, performs authentication using certificates which can be configured in chapter 5.8.8
OWE	Opportunistic Wireless Encryption alias Enhanced OPEN provides encryption WLAN without any authentication

Running in `mesh point` mode, it is possible to connect to one or more mesh points within the mesh network at the same time. The system will automatically join the wireless network, connect to the other mesh partners with the same ID and sercurtiy credentials. The authentication credentials have to be obtained by the operator of the mesh network.

Parameter	WLAN Mesh-Point Configuration
MESHID	The network name (called MESHID)
Security mode	The desired security mode
enable gate announcements	To enable gate announcments for the mesh network

The following security modes can be configured:

Parameter	WLAN Mesh-Point Security Modes
Off	MESHID is disabled
None	No authentication, provides an open network
SAE	SAE (Simultaneous Authentication of Equals) is a secure password-based authentication and key establishment protocol

WLAN IP Settings

This section lets you configure the TCP/IP settings of your WLAN network. A `client` and `mesh point` interface can be run over DHCP or with a statically configured address and default gateway.

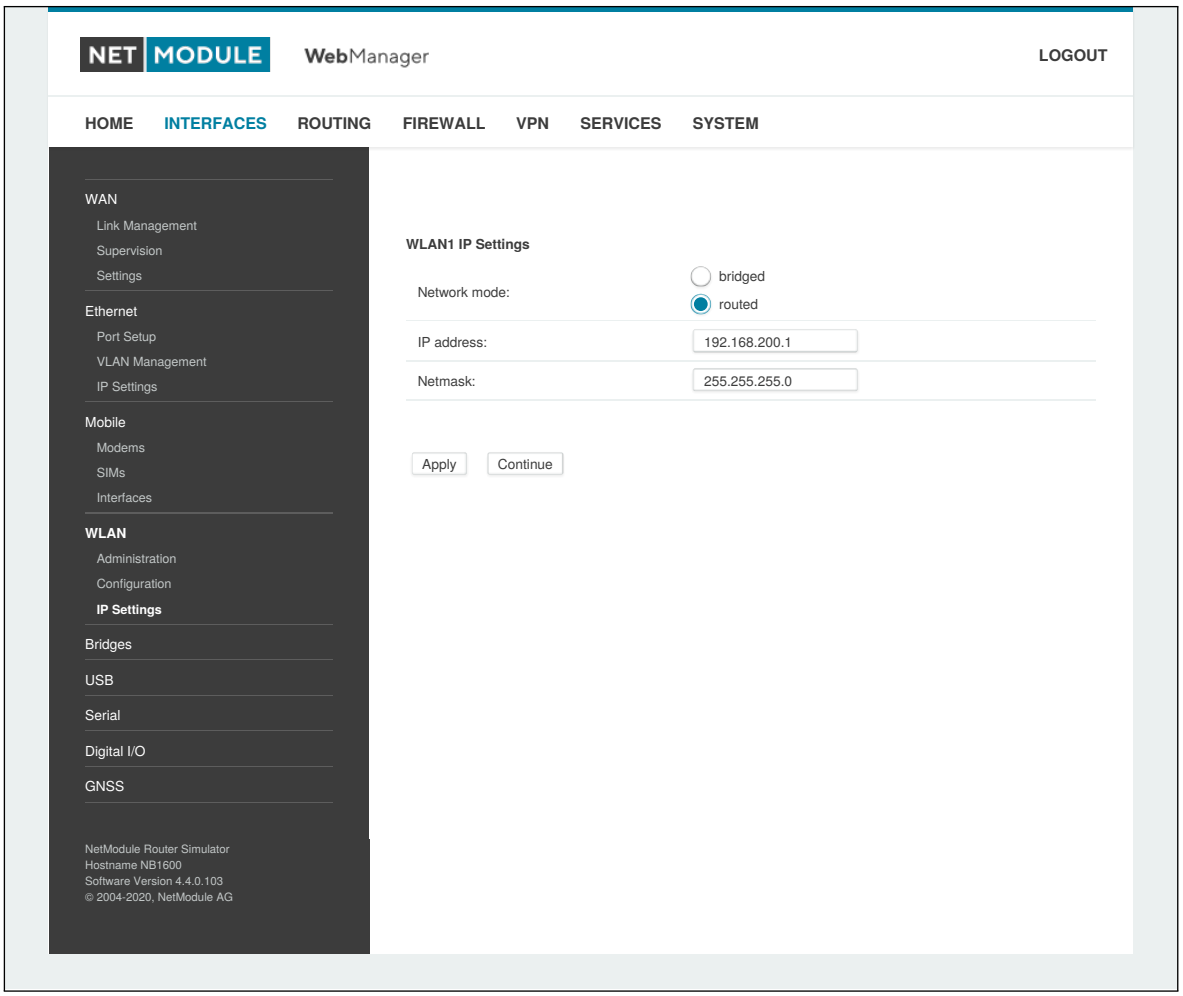


Figure 5.19.: WLAN IP Configuration

The access point networks can be bridged to any LAN interface for letting WLAN clients and Ethernet hosts operate in the same subnet. However, for multiple SSIDs we strongly recommend to set up separated interfaces in routing-mode in order to avoid unwanted access and traffic between the interfaces. The corresponding DHCP server for each network can be configured in afterwards as described in chapter 5.7.2.

Parameter	WLAN IP Settings
Network mode	Choose whether the interface shall be operated bridged or in routing-mode
Bridge interface	If bridged, the LAN interface to which the WLAN network should be bridged
IP address / netmask	In routing-mode, the IP address and netmask for this WLAN network

The following feature can be configured if the WLAN interface is bridged

Parameter	WLAN Bridging features
IAPP	Enables the Inter-Access Point Protocol feature
Pre-auth	Enables the pre-authentication mechanism for roaming clients (if supported by the client). Pre-auth is only supported with WPA2-Enterprise with CCMP

5.3.5. Software Bridges

Software bridges can be used to bridge layer-2 devices like OpenVPN TAP, GRE or WLAN interfaces without the need for a physical LAN interface.

Bridge Settings

This page can be used to enable/disable software bridges.

It can be configured as follows:

Parameter	Bridge Settings
Administrative status	Enables or disables the bridge interface. If you need an interface to the local system you need to define an IP address for the local device.
IP Address	IP address of the local interface (available only if "Enabled with local interface" was selected
Netmask	Netmask of the local interface (available only if "Enabled with local interface" was selected
MTU	Optional MTU size for the local interface (available only if "Enabled with local interface" was selected

5.3.6. USB

NetModule routers ship with a standard USB host port which can be used to connect a storage, network or serial USB device. Please contact our support in order to get a list of supported devices.

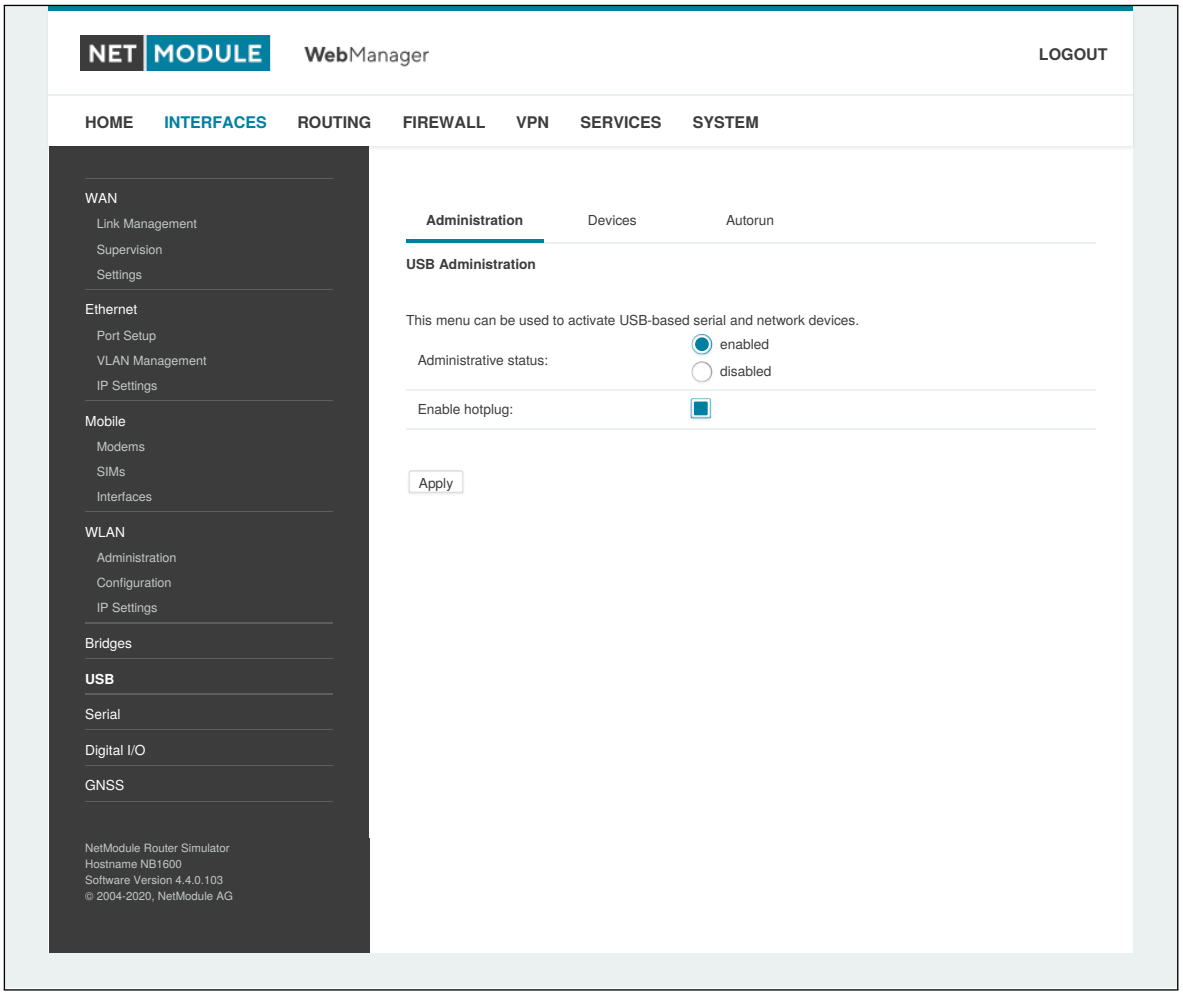


Figure 5.20.: USB Administration

USB Administration

Parameter	USB Administration
Administrative status	Specifies whether devices shall be recognized
Enable hotplug	Specifies whether device shall be recognized if plugged in during run-time or only at bootup

USB Devices

This page shows the currently connected devices and it can be used to enable a specific device based on its Vendor and Product ID. Only enabled devices will be recognized by the system and raise additional ports and interfaces.

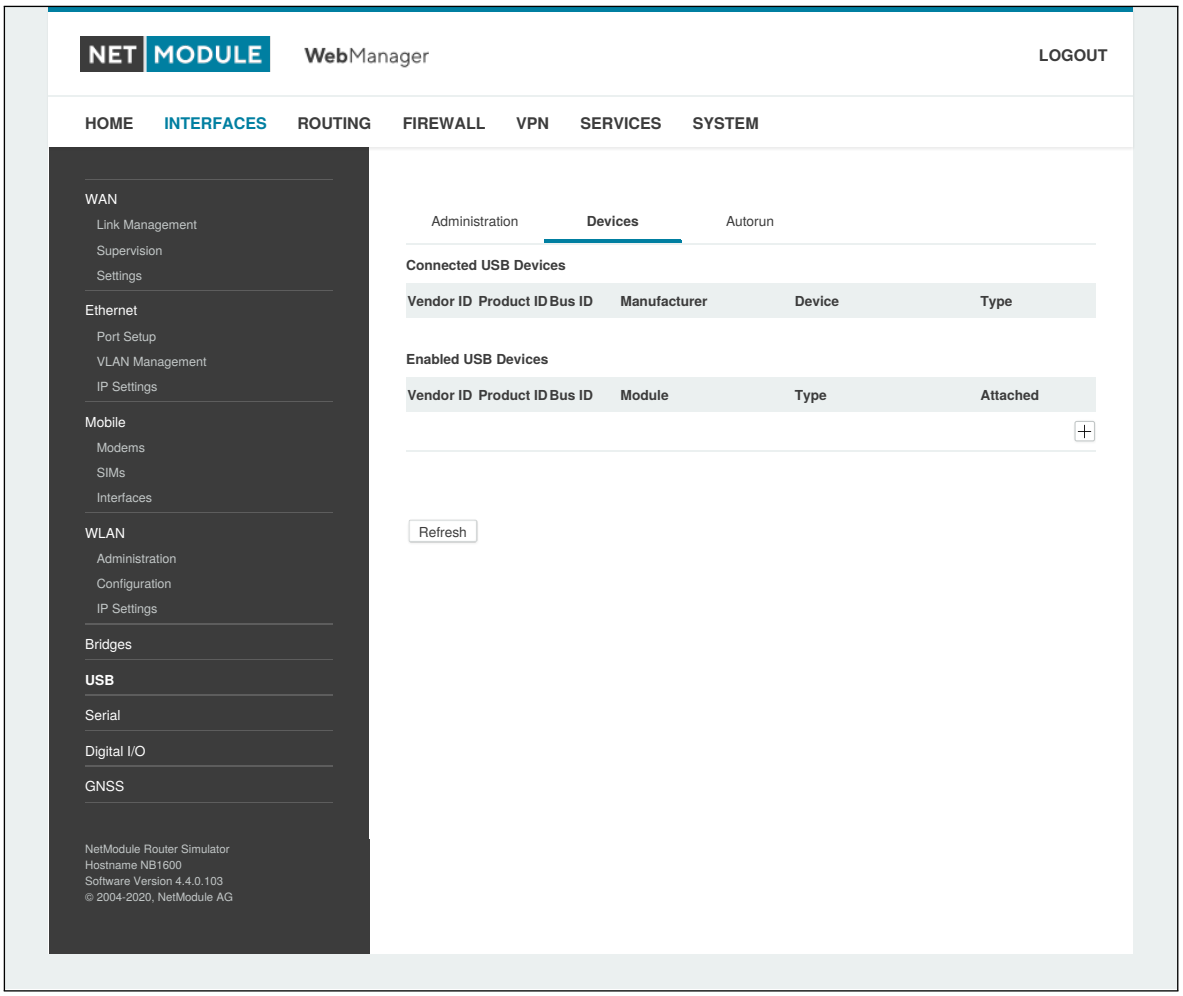


Figure 5.21.: USB Device Management

Parameter	USB Devices
Vendor ID	The USB Vendor ID of the device
Product ID	The USB Product ID of the device
Module	The USB module and type of driver to be applied for this device

Any ID must be specified in hexadecimal notation, wildcards are supported (e.g. `AB[0-1][2-3]` or `AB*`)
A USB network device will be referenced as LAN10.

5.3.7. Serial

This page can be used to manage your serial ports. A serial port can be used by:

Parameter	Serial Port Usage
none	The serial port is not used
login console	The serial port is used to open a console which can be accessed with a serial terminal client from the other side. It will provide helpful bootup and kernel messages and spawns a login shell, so that users can login to the system. If more than one serial interface is available, one serial interface can be configured as 'login console' at a time.
device server	The serial port will be exposed over a TCP/IP port and can be used to implement a Serial/IP gateway.
modem bridge	Bridges the serial interface to the Modem TTY of an intergrated WWAN Modem.
modem emulator	Emulates a classical AT command driven modem on the serial interface. See http://wiki.netmodule.com/app-notes/hayes-modem-at-simulator for detailed information.
SDK	The serial port will be reserved for SDK scripts.

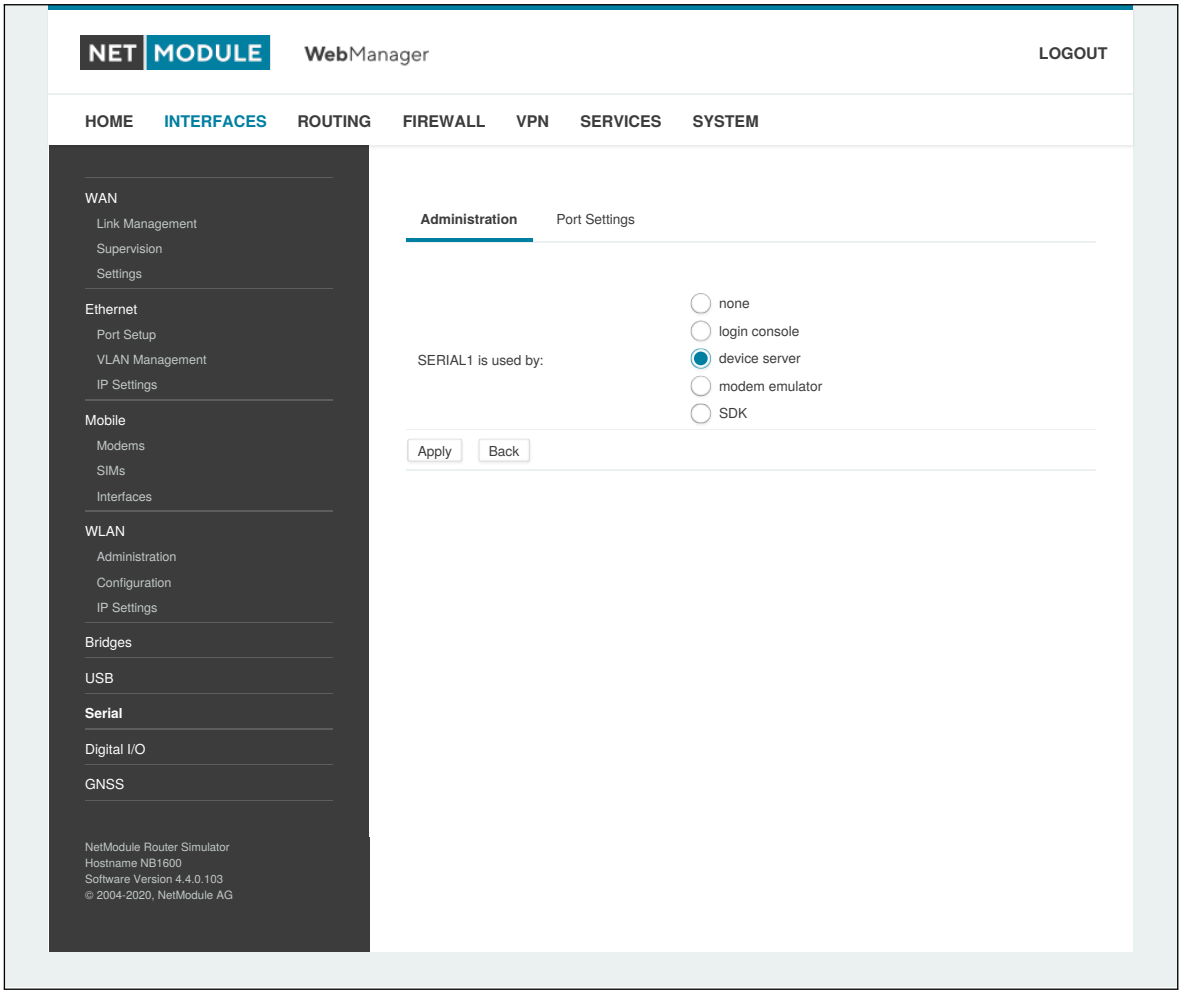


Figure 5.22.: Serial Port Administration

Running a device server, the following settings can be applied:

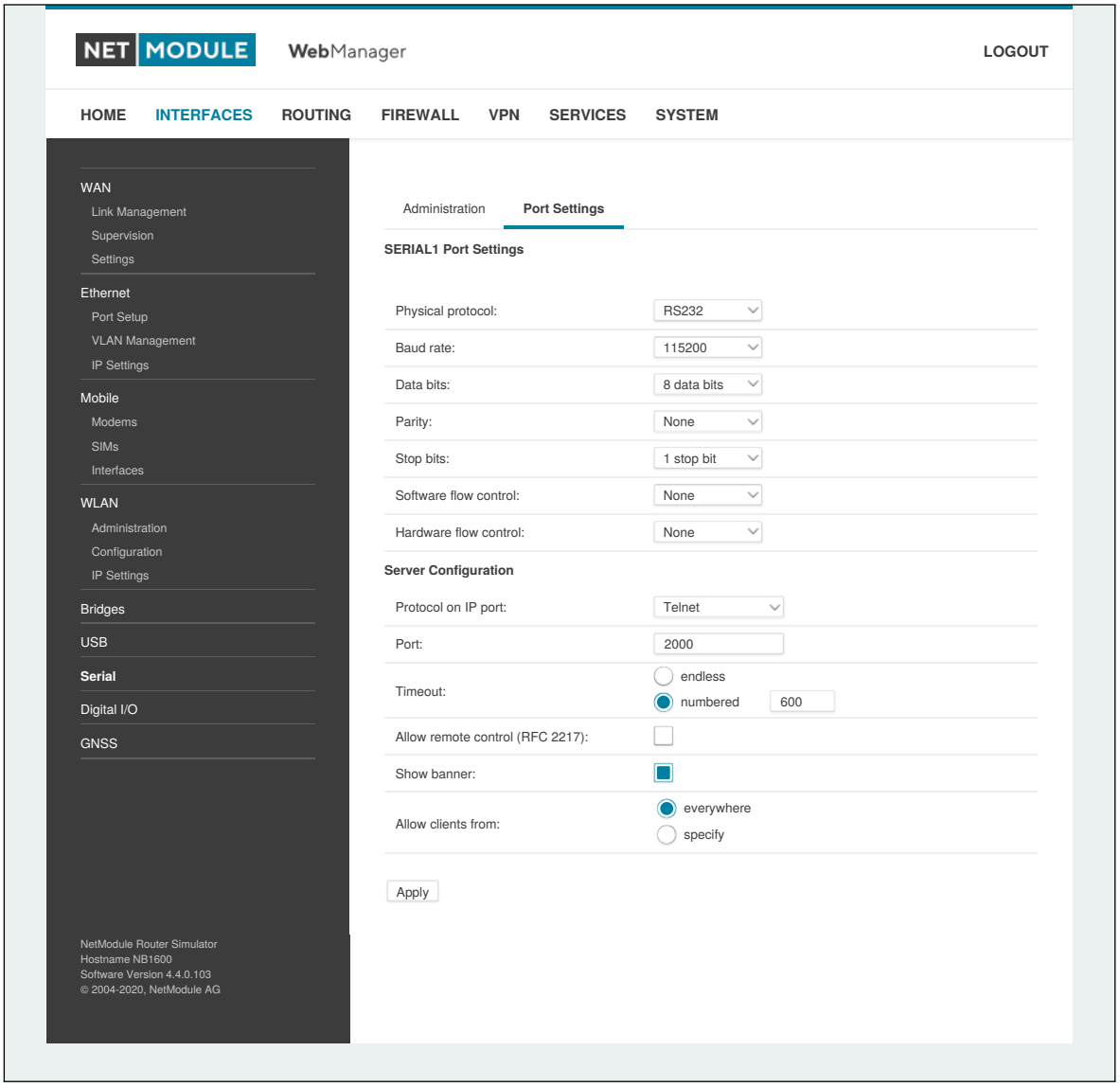


Figure 5.23.: Serial Port Settings

Parameter	Serial Settings
Physical protocol	Selects the desired physical protocol on the serial port
Baud rate	Specifies the baud rate run on the serial port
Data bits	Specifies the number of data bits contained in each frame
Parity	Specifies the parity used for every frame that is transmitted or received
Stop bits	Specifies the number of stop bits used to indicate the end of a frame

Parameter	Serial Settings
Software flow control	Defines the software flow control for the serial port, `XOFF` will send a stop, `XON` a start character to the other end to control the rate of any incoming data
Hardware flow control	You may enable RTS/CTS hardware flow control, so that the RTS and CTS lines are used to control the flow of data
Protocol on TCP/IP	You may choose the IP protocols `Telnet` or `TCP raw` for the device server
Port	The TCP port for the device server
Timeout	The timeout until a client is declared as disconnected

Parameter	Server Settings
Protocol on IP port	Selects the desired IP protocol (TCP or Telnet)
Port	Specifies the TCP port on which the server will be available
Timeout	The time in seconds before the port will be disconnected if there is no activity on it. A zero value disables this function.
Allow remote control	Allow remote control (ala RFC 2217) of the serial port
Show banner	Show a banner when clients connect
Stop bits	Specifies the number of stop bits used to indicate the end of a frame
Allow clients from	Specifies which clients are allowed to connect to the server

Please note that the device server does not provide authentication or encryption and clients will be able connect from everywhere. Please consider to restrict access to a limited network/host or block packets by using the firewall.
When running the serial port as AT modem emulator the following settings can be applied:

Parameter	Serial Port Settings
Physical protocol	Selects the desired physical protocol on the serial port
Baud rate	Specifies the baud rate run on the serial port
Hardware flow control	You may enable RTS/CTS hardware flow control, so that the RTS and CTS lines are used to control the flow of data

Parameter	Incoming connections via Telnet
Port	The TCP port for the device server

Parameter	Phonebook Entries
Number	Phone number that will get an alias

Parameter	Phonebook Entries
IP address	IP address the number will become
Port	Port value for the IP address

5.3.8. 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`.

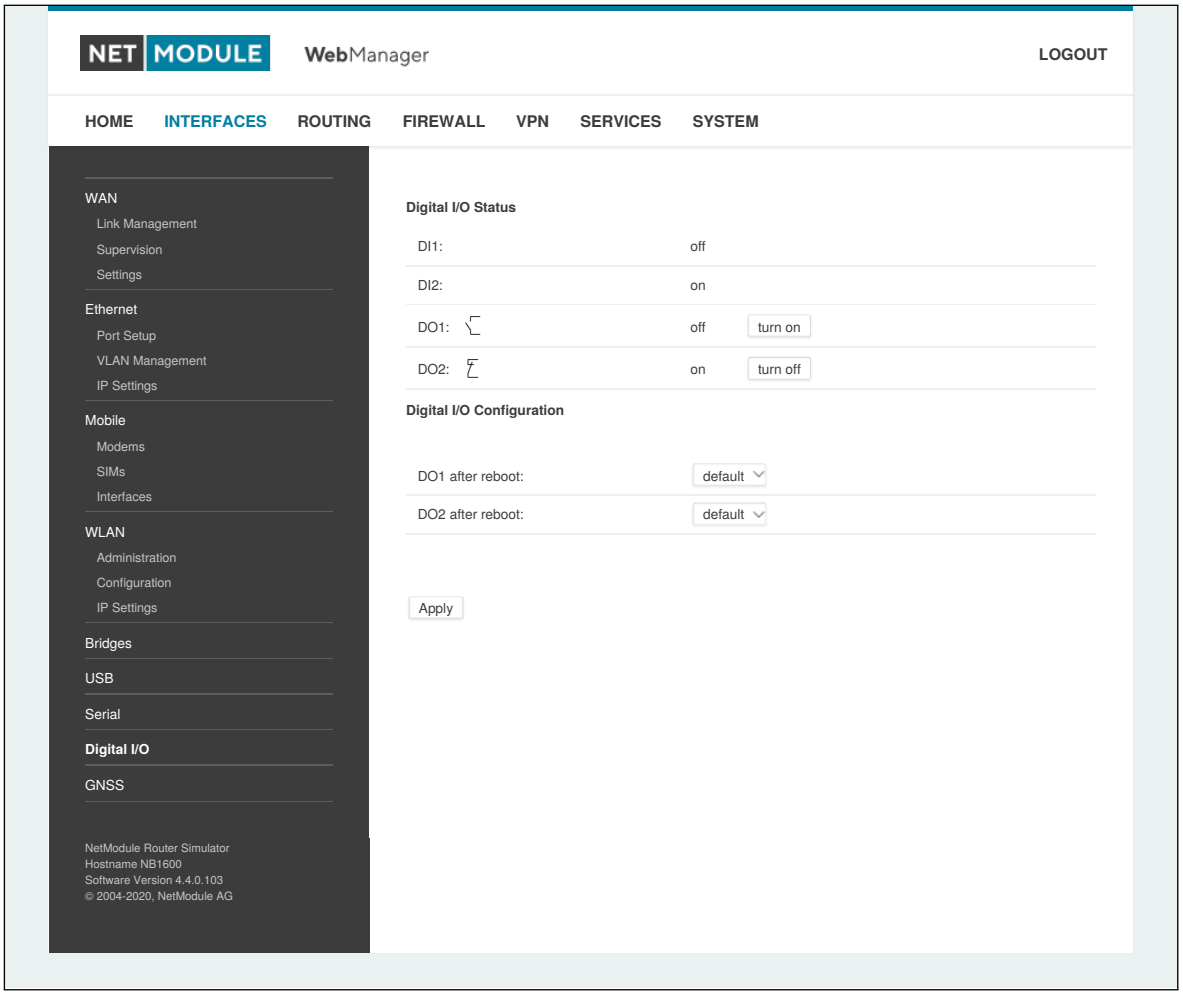


Figure 5.24.: Digital I/O Ports

You can apply the following settings:

Parameter	Digital I/O Settings
DO1 after reboot	Initial status of DO1 after system has booted
DO2 after reboot	Initial status of DO2 after system has booted

Besides `on` and `off` you may keep the `default` status as the hardware has initialized it after power-up. The digital inputs and outputs can also be monitored and controlled by SDK scripts.

5.3.9. Bluetooth Low Energy

If a Bluetooth interface is available it can be used either with the SDK scripting engine or forwarded to the Virtualization.

Bluetooth Settings

This page can be used to assign the Bluetooth module either to SDK or Virtualization or to turn Bluetooth functionality off.

It can be configured as follows:

Parameter	Bluetooth Settings
Administrative status	Enables the module for SDK or Virtualization

If you enable the module for SDK usage you need a SDK script that handles the hardware interface. You can start advertising or scanning mode and setup parameters via SDK. Please have a look at the SDK API for detailed description.

If you enable the module for Virtualization there will be no interaction to the module from the host system. It is in your responsibility to use it correctly. Please refer to our examples and documentation in the public Wiki.

5.4. ROUTING

5.4.1. Static Routes

This menu shows all routing entries of the system. They are typically formed by an address/netmask couple (represented in IPv4 dotted decimal notation) which specify the destination of a packet. The packets can be directed to either a gateway or an interface or both. If interface is set to ANY, the system will choose the route interface automatically, depending on the best matching network configured for an interface.

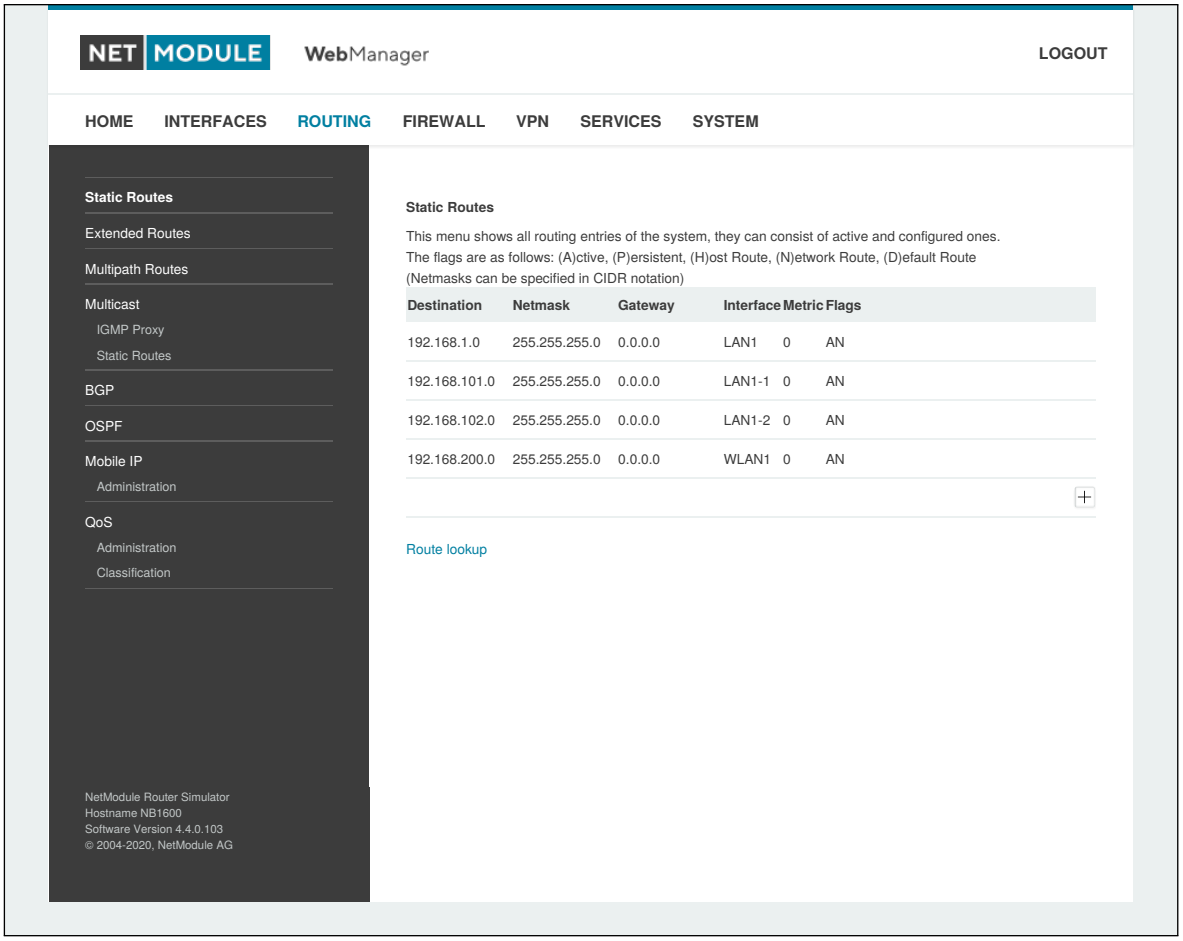


Figure 5.25.: Static Routing

In general, host routes precede network routes and network routes precede default routes. Additionally, a metric can be used to determine the priority of a route, a packet will go in the direction with the lowest metric in case a destination matches multiple routes.

Netmasks can be specified in CIDR notation (i.e. /24 expands to 255.255.255.0).

Parameter	Static Route Configuration
Destination	The destination address of a packet
Netmask	The 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	The network interface on which a packet will be transmitted in order to reach the gateway or network behind it
Metric	The routing metric of the interface (default 0), higher metrics have the effect of making a route less favorable
Flags	(A)ctive, (P)ersistent, (H)ost Route, (N)etwork Route, (D)efault Route

The flags obtain the following meanings:

Flag	Description
A	The route is considered active, it might be inactive if the interface for this route is not yet up.
P	The route is persistent, which means it is a configured route, otherwise it corresponds to an interface route.
H	The route is a host route, typically the netmask is set to 255.255.255.255.
N	The route is a network route, consisting of an address and netmask which forms the subnet to be addressed.
D	The route is a default route, address and netmask are set to 0.0.0.0, thus matching any packet.

Table 5.47.: Static Route Flags

5.4.2. Extended Routing

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

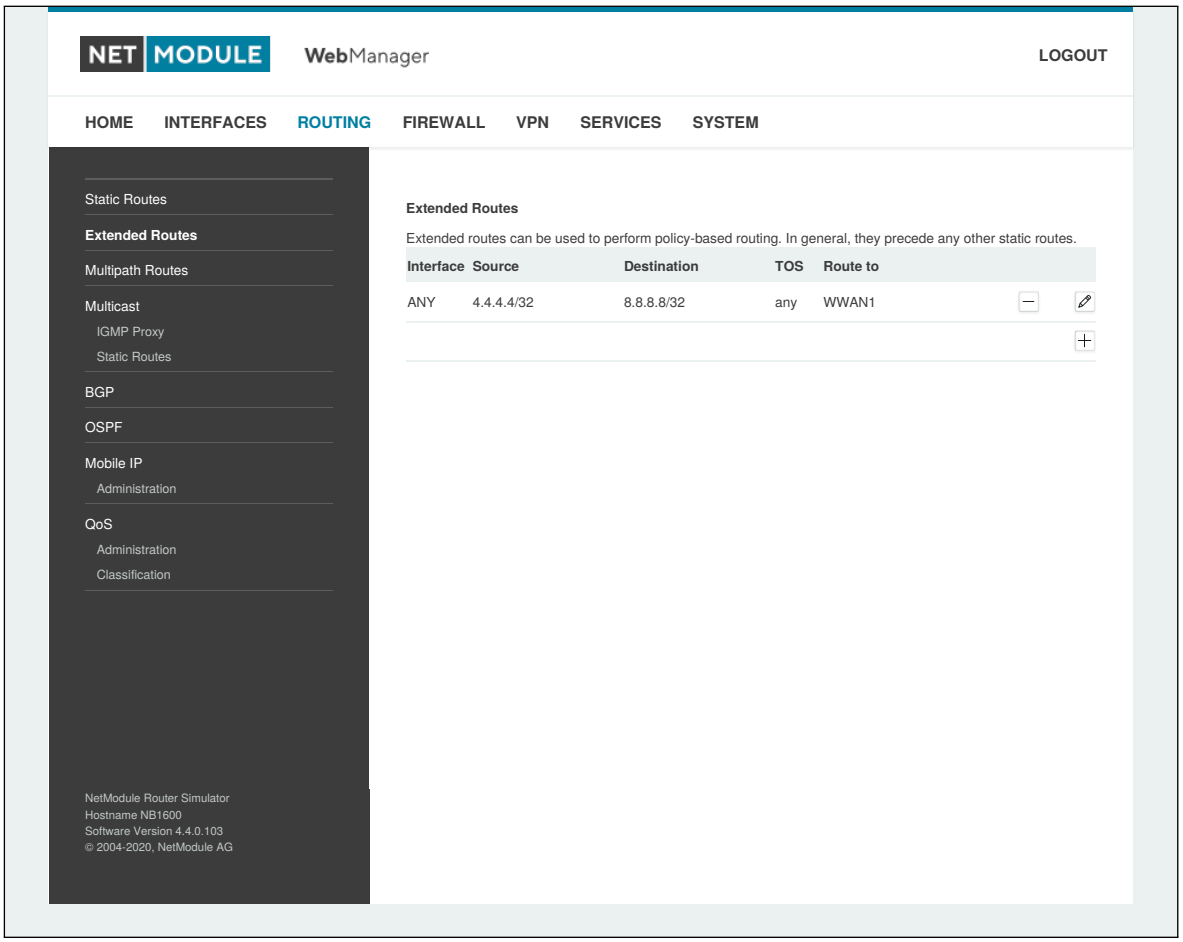


Figure 5.26.: Extended Routing

In contrast to 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.

Parameter	Extended Route Configuration
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
discard if down	Discard packets if the specified interface is down

5.4.3. Multipath Routes

Multipath routes will perform weighted IP-session distribution for particular subnets across multiple interfaces.

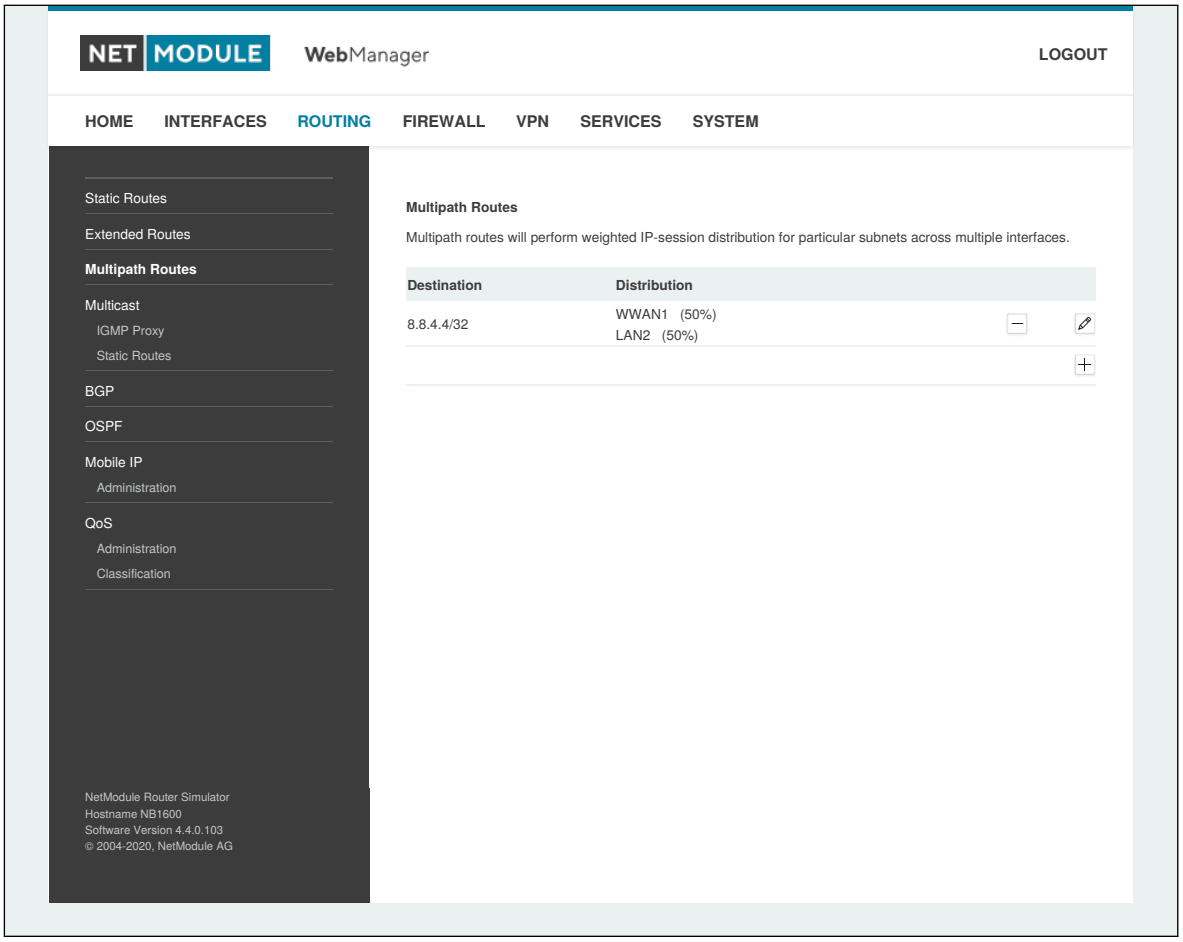


Figure 5.27.: Multipath Routes

At least two interfaces have to be defined to establish multipath routing. Additional interfaces can be added by pressing the plus sign.

Parameter	Add Multipath Routes
Target network/netmask	Defines the target network for which multipath routing shall be applied
Interface	Selects the interface for one path
Weight	Weight of the interface in relation to the others
NextHop	Overrides the default gateway of this interface

5.4.4. Multicast

Multicast distributes IP packets to subscribers in a one-to-many relationship. The subscribers use multicast messages to subscribe to a MCR group and receive the data in form of multicast packets. Therefore the messages are sent by the packet sink to the packet source.
Multicast routing (MCR) is used to farward multicast data from one network to another.

Attention:
As multicast is used to send data from one source to several destinations on the same network it is quite common for testing applications to set the TTL of multicast packets to 1 to prevent the packets from spilling into other networks. If you want to route multicast packets (that's why it is called MCR) you'll have to make sure to send your data with a TTL > 1.

Multicast routing can be configured and managed by a daemon. Only one MCR daemon can be used at a time.
NetModule routers ship with two different MCR daemons to select from depending on your dependencies:

Parameter	Administrative Status
IGMP proxy	Forwarding of multicast messages that are dynamically detected on a given interface to another interface
static routes	List of MCR rules to forward messages of dedicated source and group from a given interface to another
disabled	Disable routing of multicast messages

IGMP proxy
IGMP proxy which is able to maintain multicast groups on a particular interface and distribute incoming multicast packets towards the downstream interfaces on which hosts have joined the groups.

Parameter	Multicast Routing Settings
Incoming interface	The upstream interface on which multicast groups are joined and on which multicast packets come in
Sender network	The multicast source network address
Sender netmask	The multicast source network mask
Distribute to	Specifies the downstream interfaces to which multicast packets will be forwarded

Static Routes
Routes multicast packets in different directions depending on their origin and group based on a given set of MCR rules:

Parameter	Static Multicast Route
Group	IP address of MCR group
Source	Source-IP of the packets
Incoming interface	Interface to the packet source
Outgoing interface	Interface to forward the packets to

5.4.5. BGP

The BGP tab allows to set up peerings of the NetModule router with other Border Gateway Protocol enabled routers.

Parameter	BGP General Settings
Administrative status	Specifies whether the BGP routing protocol is active
Router ID	Optionally the router ID can be defined in form of a dotted IPv4 representation like 1.2.3.4. If the ID is omitted, the BGP daemon will try to determine a valid value or fall back to 0.0.0.0
AS number	The number of the autonomous system to which the NetModule router belongs (1-4294967295)
Redistribute connected routes	Redistribute routes to networks which are directly connected to the NetModule router
Redistribute local routes	Redistribute routes from the NetModule router's own routing table
Redistribute OSPF routes	Redistribute routes learned via the OSPF routing protocol
Disable when redundancy backup	Disables the BGP protocol when the router is set to slave mode by the VRRP redundancy protocol
Keepalive timer	The interval in seconds of sending keepalive message
Holddown timer	The time in seconds how long the router will wait for incomming BGP messages until the router will assume the neighbor is dead

The neighbors tab is used to configure all the BGP routers to peer with.

Parameter	BGP Neighbors
IP address	IP address of the peer router
As number	Autonomous system number of the peer router (1-4294967295)
Password	Password for authentication with the peer router. If left blank authentication is disabled.
Multihop	Allow multiple hops between this router and the peer router instead of requiring the peer to be directly connected.
Address Family	Select whether ipv4-unicast or l2vpn-evpn address family shall be enabled
Weight	This parameter specifies the default weight for the neighbor route

The Networks tab allows to add IP network prefixes that shall be distributed via BGP in addition to the networks that are redistributed from other sources as defined on the general tab.

Parameter	BGP Networks
Prefix	Prefix of the network to be distributed

Parameter	BGP Networks
Prefix length	Length of the prefix to be distributed

5.4.6. OSPF

The OSPF menu allows the NetModule router to be added to a network of OSPF routers.

Parameter	OSPF General Settings
Administrative status	Specifies whether the OSPF routing protocol is active
Router ID	The router-id is a unique identity to the NetModule router. If no router-id is specified, the system will automatically choose the highest IP address as the router-id.
Redistribute connected routes	Redistribute routes to networks which are directly connected to the NetModule router
Redistribute local routes	Redistribute routes from the NetModule router's own routing table
Redistribute BGP routes	Redistribute routes learned via the BGP routing protocol
Redistribute default route	Redistribute the routers default route
Disable when redundancy backup	Disables the OSPF protocol when the router is set to slave mode by the VRRP redundancy protocol

The interfaces tab is used to define OSPF specific settings for the IP interfaces of the router. If no settings are defined for a specific interface, default settings will be used.

Parameter	OSPF Interfaces
Interface	The name of the interface for which settings shall be defined
Authentication	The authentication protocol to be used on the interface to authenticate OSPF packets
Key	The key to be used for authentication
Key ID	The ID of the key to be used for authentication (1-255)
Cost	The cost for sending packets via this interface. If not specified or set to 0 OSPF defaults are used.
Passive	Do not send out OSPF packets on this interface

The networks tab defines the IP networks to be handled in OSPF as well as to which routing area they belong.

Parameter	OSPF Networks
Prefix	Prefix of the network
Prefix length	Length of the prefix
Area	Routing area to which this interface belongs (0-65535, 0 means backbone)

5.4.7. Mobile IP

Mobile IP (MIP) can be used to enable seamless switching between different kinds of WAN links (e.g. WWAN/WLAN). The `mobile node` hereby remains reachable via the same IP address (`home address`) at any time, independently of the WAN link being used. Effectively, any WAN link switch causes very small outages during switchover while keeping all IP connections alive.

Moreover, NetModule routers also support NAT-Traversal for mobile nodes running behind a firewall (performing NAT), which makes mobile nodes even there accessible from a central office via their home address, and thus, bypassing any complicated VPN setups.

The `home agent` accomplishes this by establishing a tunnel (similar to a VPN tunnel) between itself and the `mobile node`. WAN link switching works by telling the `home agent` that the WAN IP address (called the `care-of address` in MIP terms) of the `mobile node` has changed. The `home agent` will then encapsulate packets destined to a `mobile node`'s home address into a tunnel packet containing the current `care-of address` of the `mobile node` as its destination address.

To prevent problems with firewalls and private IP addressing, the MIP implementation always employs reverse tunneling, which means that all traffic sent by a `mobile node` is relayed via the tunnel to the `home agent` instead of directly being conveyed to the final destination. This fact also empowers MIP to be used as a lightweight VPN replacement (without payload secrecy).

The MIP implementation supports RFCs 3344, 5177, 3024 and 3519. For applications requiring vast numbers of mobile nodes, interoperability with the Cisco 2900 Series `home agent` implementation has been verified. However, since NetModule routers implement a `mobile node` as well as a `home agent`, a MIP network with up to 10 mobile nodes can be implemented without requiring expensive third party routers.

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

Parameter	Mobile IP Configuration
Primary home agent address	The address of the primary `home agent`
Secondary home agent address	The address of the secondary `home agent`. The mobile node will try to register with this home agent, if the primary `home agent` is not reachable.
Home address	The permanent home address of the `mobile node` which can be used to reach the mobile router at any time.
SPI	The Security Parameter Index (SPI) identifying the security context for the mobile IP tunnel between the `mobile node` and the `home agent`. This is used to distinguish mobile nodes from each other. Therefore each mobile node needs to be assigned a unique SPI. This is a 32-bit hexadecimal value.
Authentication type	The used authentication algorithm. This can be prefix-suffix-md5 (default for MIP) or hmac-md5.

Parameter	Mobile IP Configuration
Shared secret	The shared secret used for authentication of the `mobile node` at the `home agent`. This can be either a 128-bit hexadecimal value or a random length ASCII string.
Life time	The lifetime of security associations in seconds.
UDP encapsulation	Specifies whether UDP encapsulation shall be used or not. To allow NAT traversal, UDP encapsulation must be enabled.
Mobile network address	Optionally specifies a subnet which should be routed to the `mobile node`. This information is forwarded via Network Mobility (NEMO) extensions to the `home agent`. The `home agent` can then automatically add IP routes to the subnet via the `mobile node`. Note that this feature is not supported by all third party `home agent` implementations.
Mobile network mask	The network mask for the optional routed network.

If MIP is run as a `home agent`, you will have to set up a home address and network mask for the `home agent` first. Then you will need to add the configuration for all mobile nodes which is made up of the following settings:

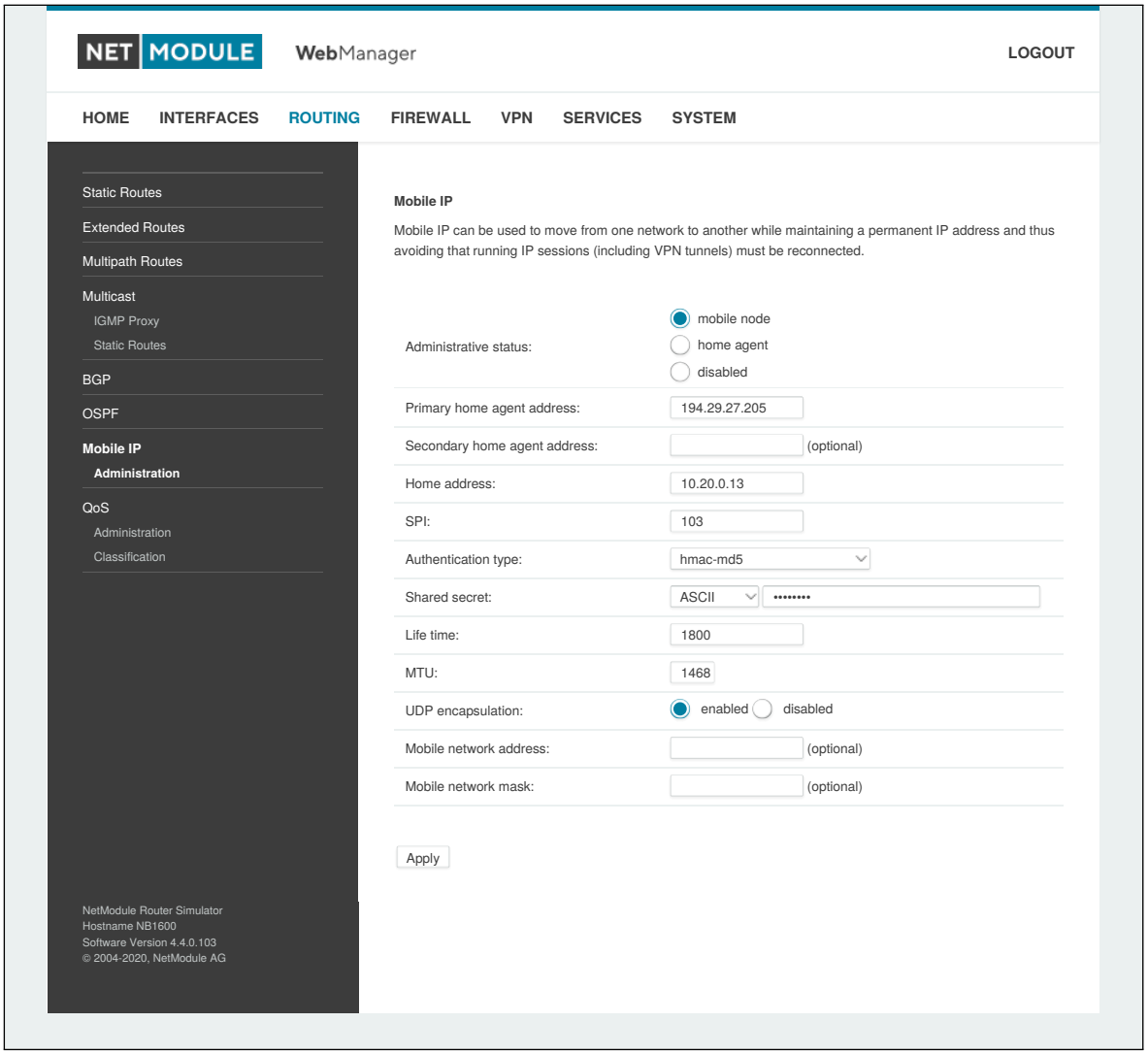


Figure 5.28.: Mobile IP

Parameter	Mobile IP Node Configuration
SPI	The Security Parameter Index (SPI) identifying the security context for the tunnel between the `mobile node` and the `home agent`. This is used to distinguish mobile nodes from each other. Therefore each `mobile node` needs to be assigned a unique SPI. This is a 32-bit hexadecimal value.
Authentication type	The used authentication algorithm. This can be prefix-suffix-md5 (default for mobile IP) or hmac-md5.

Parameter	Mobile IP Node Configuration
Shared secret	The shared secret used for authentication of the `mobile node` at the `home agent`. This can be either a 128-bit hexadecimal value or a random length ASCII string.

5.4.8. Quality Of Service

NetModule routers are able to prioritize and shape certain kinds of IP traffic. This is currently limited on egress, which means that only outgoing traffic can be stipulated.

The current QoS solution is using Stochastic Fairness Queueing (SFQ) classes in combination with Hierarchy Token Bucket (HTB) qdiscs. Its principle of operation can be summarized as ceiling the max. throughput per link and shaping traffic by reflecting the specified queue priorities. In general, the lowest priority number of a queue gets most out of the available bandwidth.

In case of demands for other class or qdisc algorithms please contact our support team in order to evaluate the best approach for your application.

QoS Administration

The administration page can be used to enable and disable QoS.

QoS Classification

The classification section can be used to define the WAN interfaces on which QoS should be active.

Parameter	QoS Interface Parameters
Interface	The WAN interface on which QoS should be active
Bandwidth congestion	The bandwidth congestion method. In case of `auto` the system will try to apply limits in a best-effort way. However, it is suggested to set fixed bandwidth limits as they also offer a way of tuning the QoS behaviour.
Downstream bandwidth	The available bandwidth for incoming traffic
Upstream bandwidth	The available bandwidth for outgoing traffic
IP to ping (primary)	An IP, which answers ICMP echo requests to determine the bandwidth of the link
IP to ping (secondary)	An IP, which answers ICMP echo requests to determine the bandwidth of the link

When defining limits, you should consider bandwidth limits which are at least possible as most shaping and queues algorithms will not work correctly if the specified limits cannot be achieved. In particular, any WWAN interfaces operating in a mobile environment are suffering variable bandwidths, thus rather lower values should be used.

In case an interface has been activated, the system will automatically create the following queues:

Parameter	QoS Default Queues
high	A high priority queue which may hold any latency-critical services (such as VoIP)
default	A default queue which will handle all other services
low	A low priority queue which may hold less-critical services for which shaping is intended

Each queue can be configured as follows:

Parameter	QoS Queue Parameters
Name	The name of the QoS queue
Priority	A numerical priority for the queue, lower values indicate higher priorities
Bandwidth	The maximum possible bandwidth for this queue in case the total bandwidth of all queues exceeds the set upstream bandwidth of "QoS Interface Parameters"
Set TOS	The TOS/DiffServ value to set on matching packets

You can now configure and assign any services to each queue. The following parameters apply:

Parameter	QoS Service Parameters
Interface	The QoS interface of the queue
Queue	The QoS queue to which this service shall be assigned
Source	Specifies a network address and netmask used to match the source address of packets
Destination	Specifies a network address and netmask used to match the destination (target) address of packets
Protocol	Specifies the protocol for packets to be matched
Source Port	Specifies the source port for packets to be matched
Destination Port	Specifies the destination port for packets to be matched
Type of Service	Specifies the TOS/DiffServ for packets to be matched

5.5. FIREWALL

5.5.1. Administration

NetModule routers use Linux's netfilter/iptables firewall framework
(see http://www.netfilter.org for more information) which supports stateful inspection, that is, granting the same permissions for inherited connections within an IP session (e.g. FTP which builds up a control and data connection).
The administration 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.

5.5.2. Adress/Port Groups

This menu can be used to form address or port groups which can be later used for firewall rules in order to reduce the number of rules. If address or port groups have been referenced, packets will match if one of the configured entities apply to the packet.

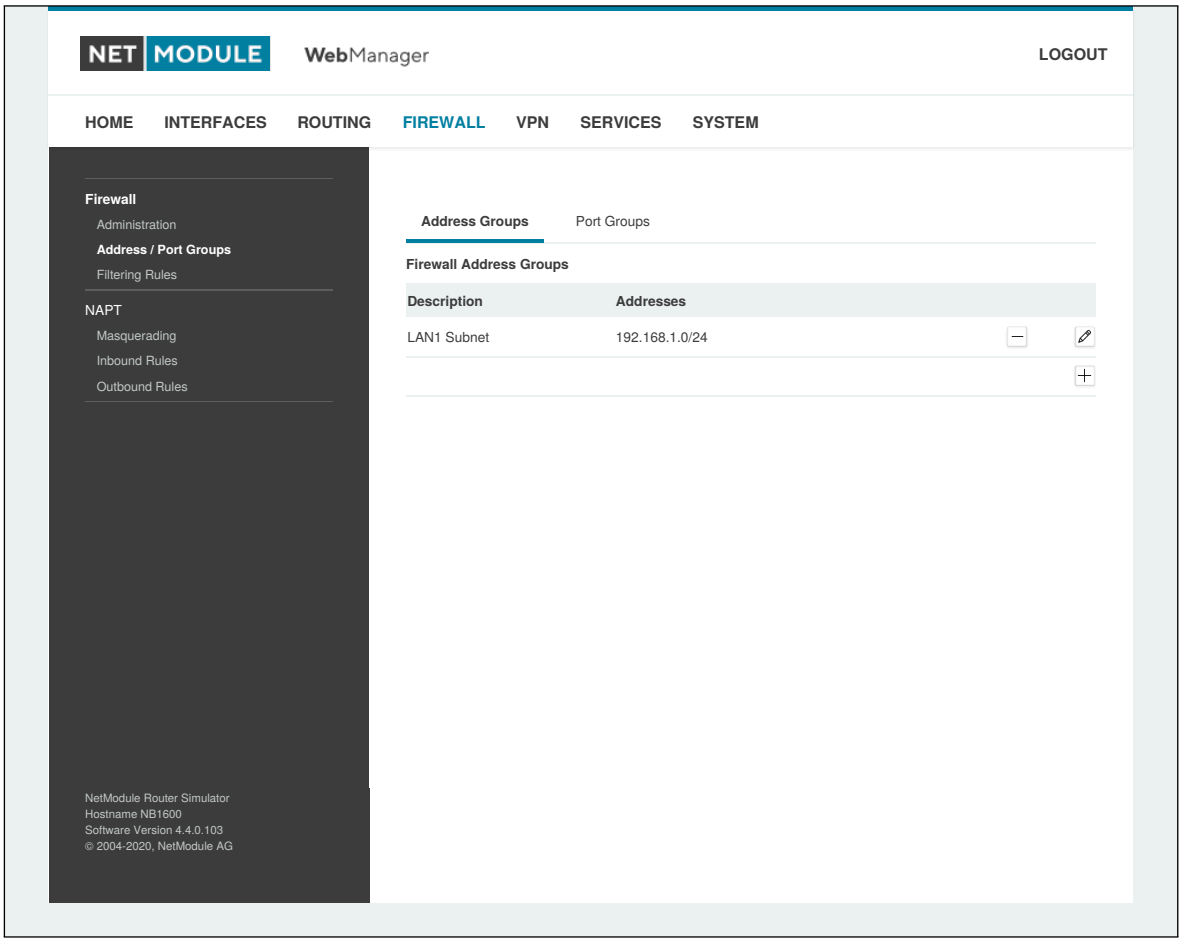


Figure 5.29.: Firewall Groups

5.5.3. Rules

In general, the firewall is set up of a range of rules which control each packet's permission to pass the router. Please note that the rules are processed by order, that means traversing the list from top to bottom until a matching rule is found. Packets which are not matching any of the rules configured will be ALLOWED.

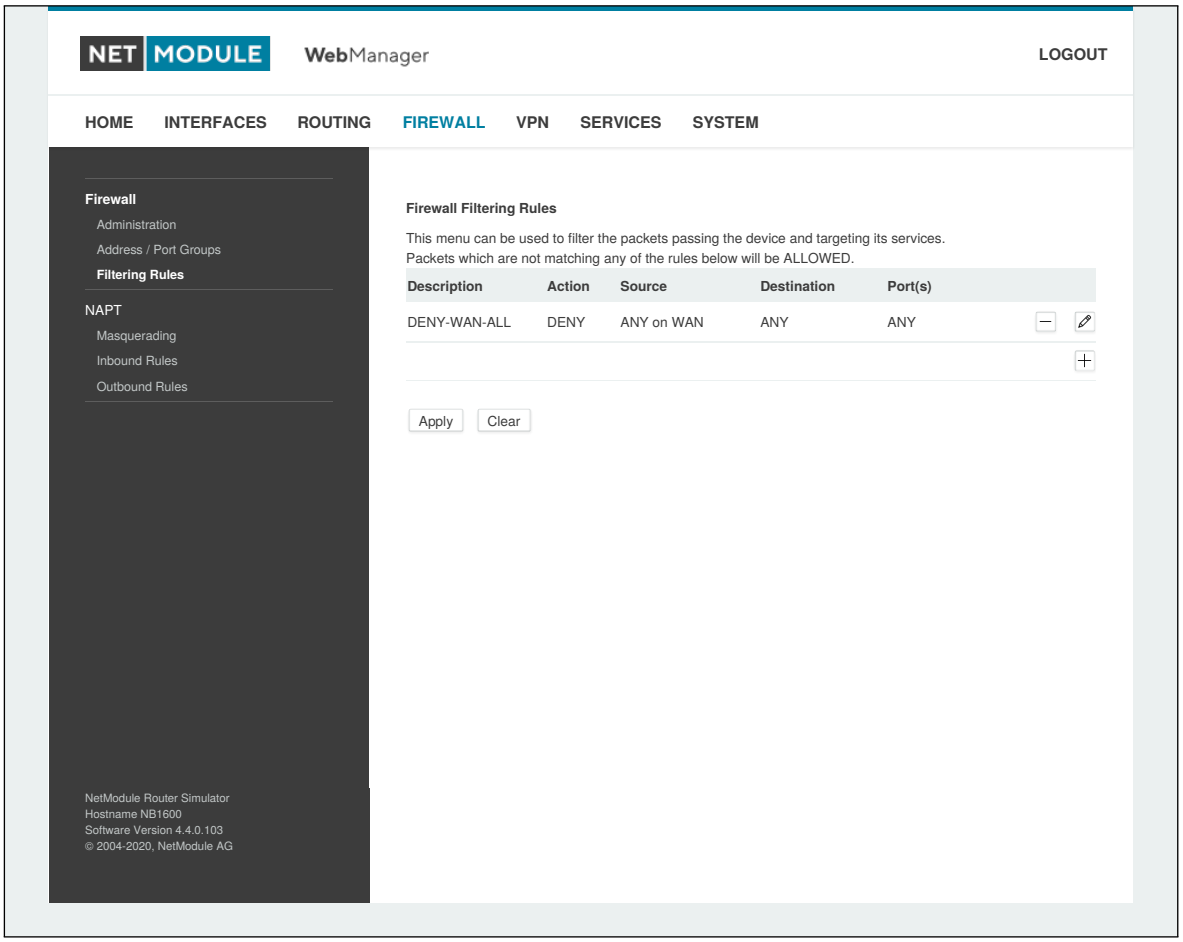


Figure 5.30.: Firewall Rules

Parameter	Firewall Rule Configuration
Description	A meaningful description about the purpose of this rule
Action	Specifies whether the packets of this rule should be allowed or denied
log matches	Throw a syslog message if rule matches
Source	The source address of matching packets, can be any or specified by address/network. Selecting on source MAC addreses is possible as well.
Destination	The destination address of matching packets, can be any, local (addressed to the system itself) or specified by address/network
Incoming interface	The interface on which matching packets are received

Parameter	Firewall Rule Configuration
Protocol	The used IP protocol of matching packets (UDP, TCP or ICMP)
Destination port(s)	The destination port of matching packets, which can be specified by a single port or a range of ports (only UDP/TCP).

The statistics page can be used to figure out if rules have matched any packets and provides a convenient way to debug your firewall setup.

5.5.4. NAPT

This page can be used to configure Network Address and Port Translation (NAPT) for packets traversing the system. NAPT hereby modifies IP addresses or/and TCP/UDP ports in matching IP packets. By tracking those connections, it will also automatically adjust the returning packets of an IP session.

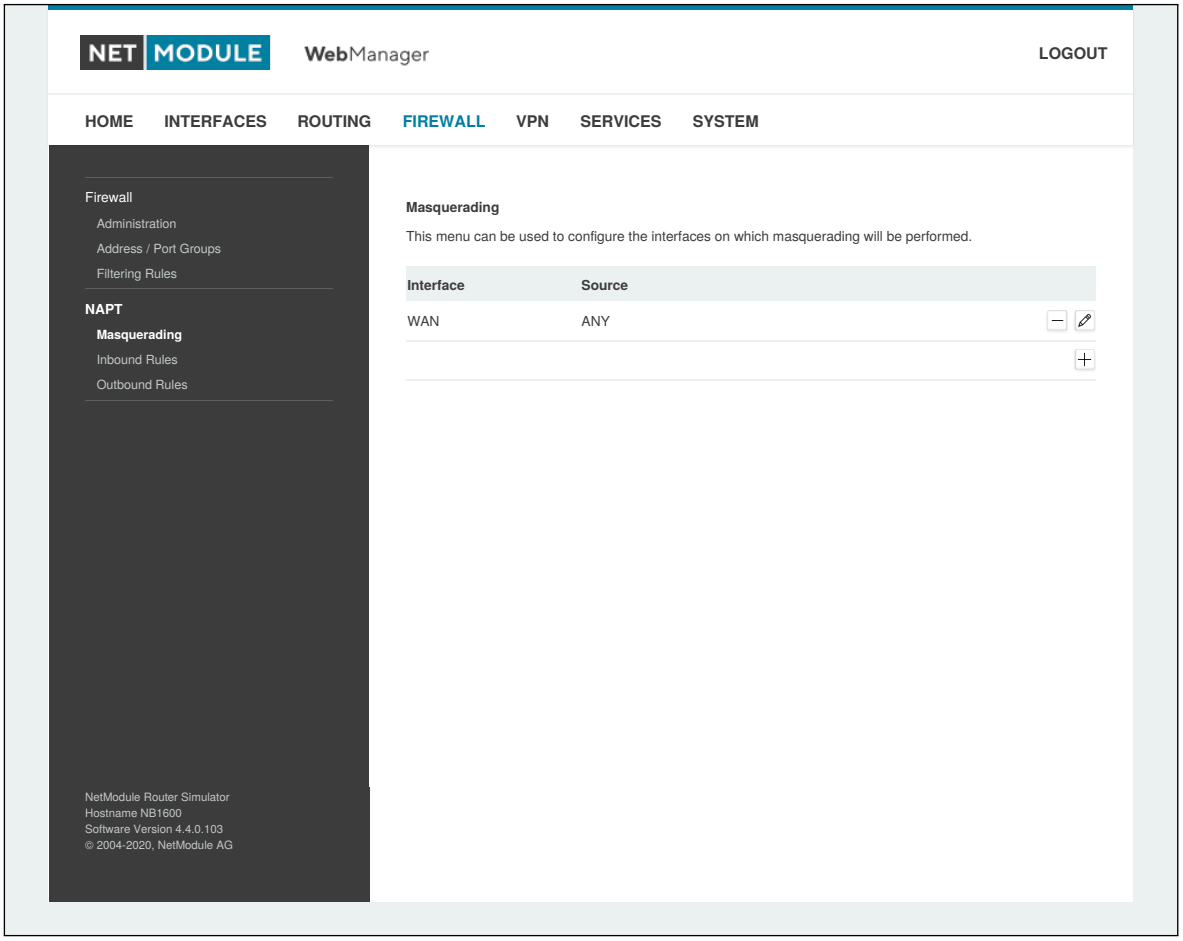


Figure 5.31.: Masquerading

The administration page lets you specify the interfaces on which masquerading will be performed. NAT will hereby use the address of the selected interface and choose a random source port for outgoing connections and thus enables communication between hosts from a private local area network towards hosts on the public network.

Parameter	Masqerading Rules
Interface	The outgoing interface on which connections will be masqueraded
Source address	The source address or network from which matching packets are masqueraded
Source netmask	The source netmask of the network from which matching packets are masqueraded

NAPT 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, you can expose that service and make it available from the Internet. You may also establish 1:1 NAT mapping for a single host using additional outbound rules.

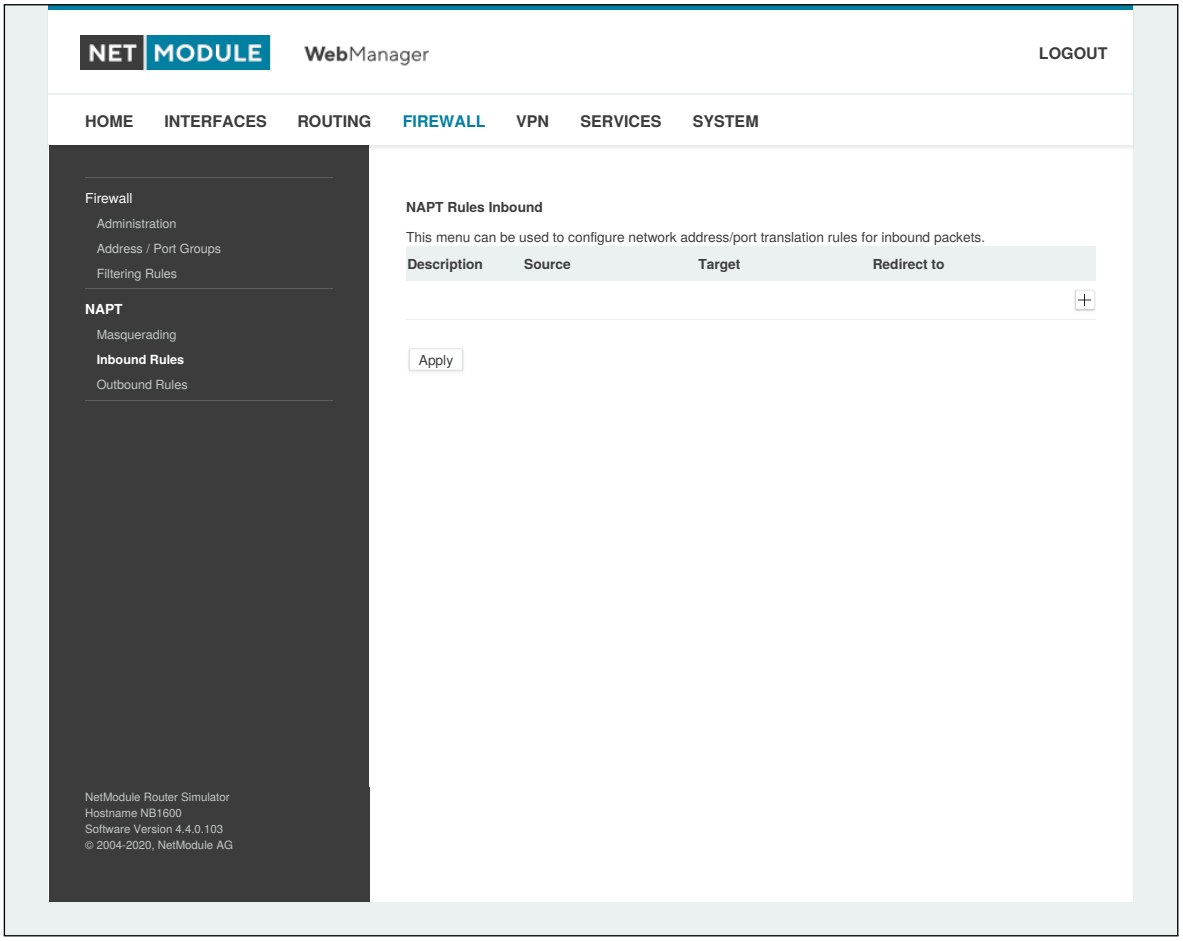


Figure 5.32.: Inbound NAPT

Please note that the specified rules are processed by order, that means, traversing the list from top to bottom until a matching rule is found. If there is no matching rule found, the packet will pass as is.

Parameter	Inbound NAPT Rules
Description	A meaningful description of this rule
Map	Context for this rule: Host, Network or Port-Range - see table below
Incoming interface	The interface from which matching packets are received
Source	The source address or network from which matching packets are received
Target address	The destination address of matching packets (optional)
Protocol	The used protocol of matching packets

Parameter	Inbound NAPT Rules
Ports	The used UDP/TCP port of matching packets
Redirect to	The address to which matching packets shall be redirected
Redirect port	The port to which matching packets will be redirected

Select mapping context according to your needs:

Parameter	Mapping contexts
host	Rewrite destination address and port for one given host (i.e. 10.0.0.1:8080 → 192.168.1.100:80
network	Rewrite destination address for a full network (i.e. 10.0.0.0/24 → 192.168.1.0/24
port range	Rewrite destination address and port based on the incoming port (i.e. 10.0.0.1:22000-22255 → 192.168.1.0/24:22). There is no corresponding rule for port range translation in outbound rules. Use network based mapping there.

NAPT Outbound Rules

Outbound rules will modify the source section of IP packets and can be used to establish 1:1 NAT mappings but also to redirect packets to a specific service.

Parameter	Outbound NAPT Rules
Description	A meaningful description of this rule
Outgoing interface	The outgoing interface on which matching packets are leaving the router
Target	The target address or network to which matching packets are destined
Source address	The source address of matching packets (optional)
Protocol	The used protocol of matching packets
Ports	The used UDP/TCP port of matching packets
Rewrite source address	The address to which the source address of matching packets shall be rewritten
Rewrite source port	The port to which the source port of matching packets shall be rewritten

5.6. VPN

5.6.1. OpenVPN

OpenVPN Administration

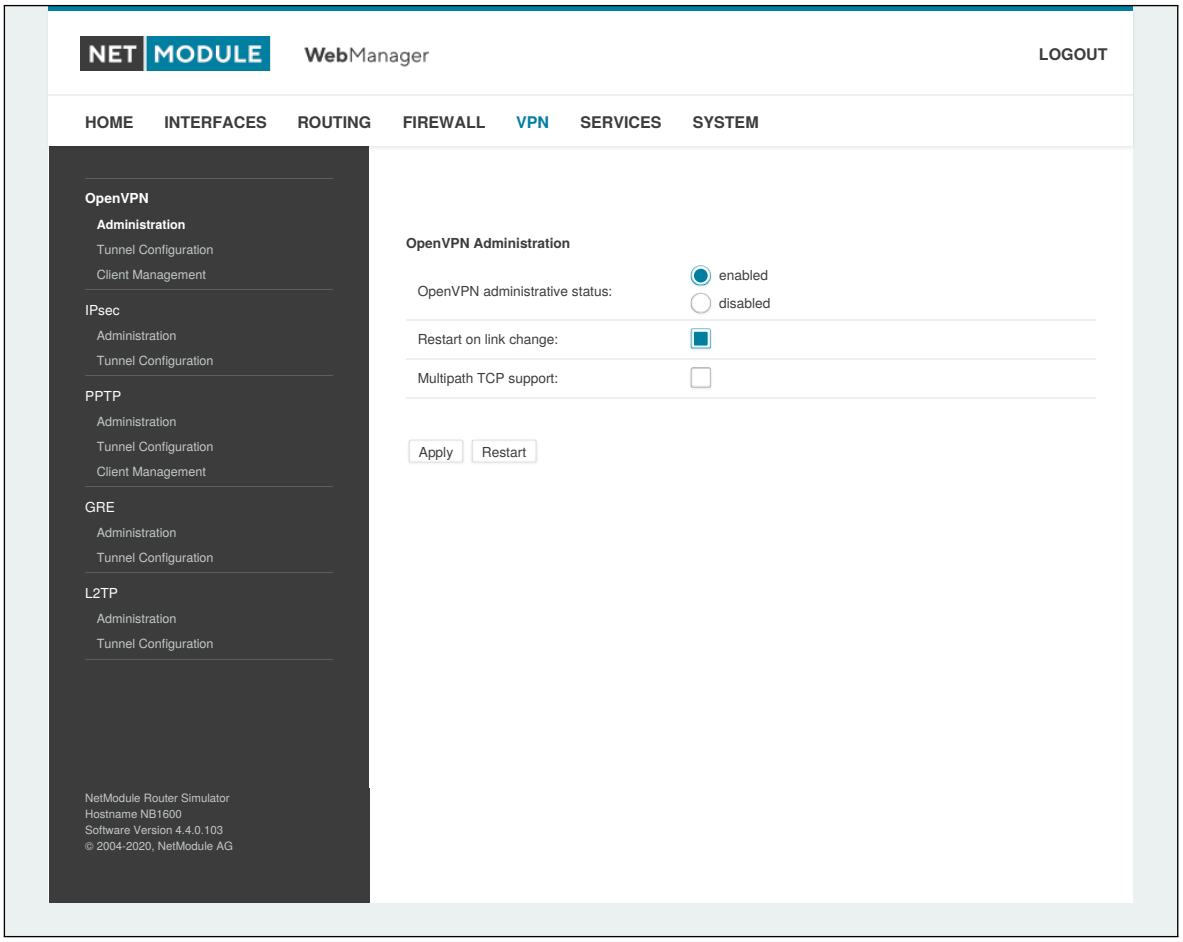


Figure 5.33.: OpenVPN Administration

Parameter	OpenVPN Administration
Administrative status	Specifies whether OpenVPN is active
Restart on link change	restarts the OpenVPN daemon in case of a wanlink change if enabled
Multipath TCP support	enables multipath TCP support

Tunnel Configuration

NetModule routers support one single server tunnel and up to four client tunnels. You can specify tunnel parameters either in standard configuration or upload an expert mode file which has been created in advance. Refer to chapter 5.6.1 to learn more about how to manage clients and generate the files.

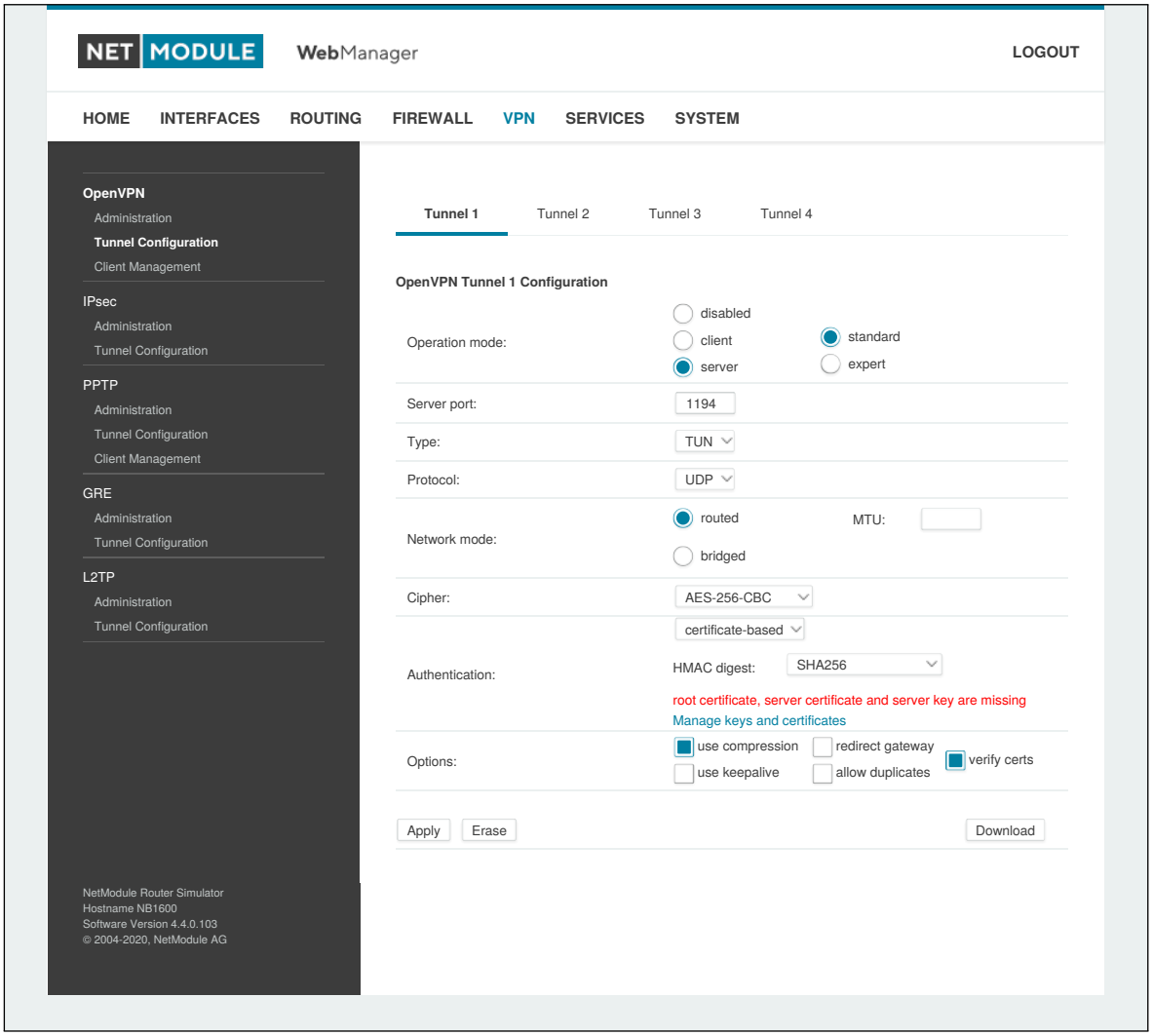


Figure 5.34.: OpenVPN Configuration

Parameter	OpenVPN Configuration
Operation mode	Specifies whether client or server mode should be used for this tunnel, it further specifies if tunnel shall be configured in a standard way or if an expert mode file shall be used.
Multipath TCP	Enables OpenVPN mulipath TCP support

If the tunnel is operated in client mode, the following settings can be applied:

Parameter	OpenVPN Client Configuration
Peer selection	Specifies how the remote peer shall be selected, besides a single server you may configure multiple servers which can, in case of failures, either be selected sequently (i.e. failover) or randomly (i.e. load balancing)
Server	The address or hostname of the remote server
Port	The port of the remote server (1194 by default)

The following settings can be used to configure a tunnel (client and server mode):

Parameter	OpenVPN Configuration
Interface type	The device type for this tunnel which can be either TUN (typically used for routed connections) or TAP (required for bridged networks)
Protocol	The tunnel protocol to be used for the transport connection
Network mode	Defines how the packets should be forwarded, which can be either routed or bridged from/to a particular LAN interface. If required, you can also specify the maximum transfer unit for the tunnel interface.
MTU	The Maximum Transmission Unit of the tunnel interface
Encryption	The required cipher mechanism used for encryption
Digest	The digest algorithm used for authenticating

Authentication can be done in the following ways:

Parameter	OpenVPN Authentication
certificate-based	Certificates and keys for authenticating the tunnel. Please take care that the proper keys/certificates have been either uploaded or generated (see 5.8.8).
credential-based	Username and password are used for authentication.
both	Verifying the tunnel uses certificates and credentials.
none	Tunnel is not authenticated (discouraged)

The following further options can be applied:

Parameter	OpenVPN Options
use compression	Enable or disable LZO packet compression
use keepalive	Can be used to send a periodic keepalive packet in order to keep the tunnel up despite of 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. In doubt, create an extra static route pointing to the correct interface.
allow duplicates	Allow multiple clients with the same common name to concurrently connect. (server mode only)
verify certs	Check peer certificate against local CRL. (server mode only)
negotiate DNS	If enabled, the system will use the nameservers which have been negotiated over the tunnel.

OpenVPN Expert Configuration (Client)

The expert configuration mode offers a straightforward way to configure a tunnel by simply uploading a zip package containing the required configuration and optionally key/certificate files. A client tunnel usually consists of the following files:

Parameter	Client Expert Files
client.conf	OpenVPN configuration file (see `http://www.openvpn.net` for available options)
ca.crt	Root certificate authority file
client.crt	Certificate file
client.key	Private key file
client.p12	PKCS#12 file
ta.key	TLS authentication key file

Please note that you may specify arbitrary file names, however, the configuration file suffix must be `.conf` and all files referred in the configuration file must correspond to relative path names.

OpenVPN Expert Configuration (Server)

A server tunnel typically requires the following files:

Parameter	Server Expert Files
server.conf	OpenVPN configuration file
ca.crt	Root certificate authority file
server.crt	Certificate file
server.key	Private key file
dh1024.pem	Diffie-Hellman parameters file
ccd	A directory containing client-specific configuration files

Keep in mind that a certificate becomes valid once its validity time has been reached, thus an accurate system time has to be set prior to creating certificates and establishing a tunnel connection. Please ensure that all NTP servers are reachable. Using host names also requires a working DNS server.

Client Management

Once you have successfully set up an OpenVPN server tunnel, you can manage and enable clients connecting to your service. Currently connected clients can be seen on this page, including the connect time and IP address. You may kick connected clients by disabling them.

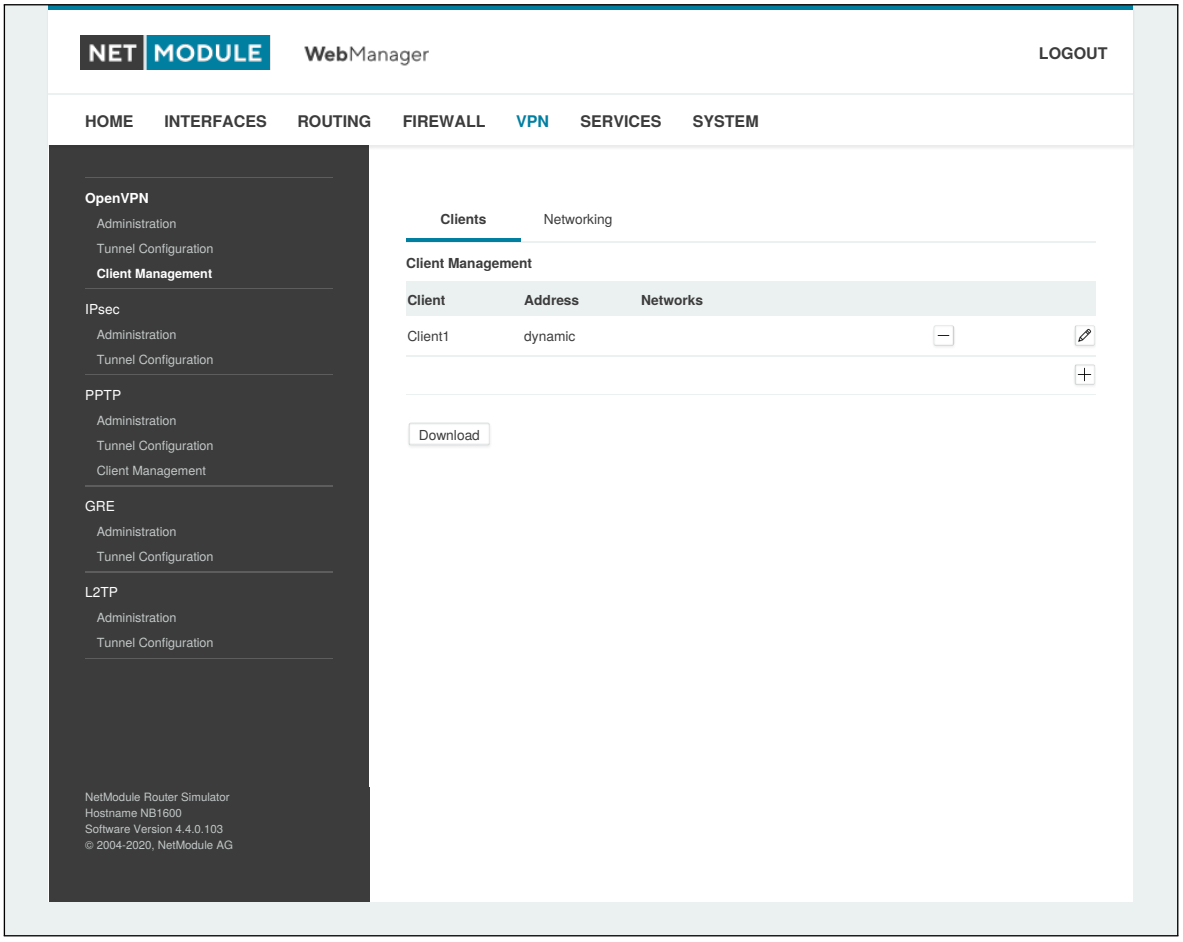


Figure 5.35.: OpenVPN Client Management

In the Networking section you can specify a fixed tunnel endpoint address for each client. Please note that, if you intend to use a fixed address for a particular client, you would have to apply fixed addresses to the other ones as well.

You may specify the network behind the clients as well as the routes to be pushed to each client. This can be useful for routing purposes, e.g. in case you want to redirect traffic for particular networks towards the server. Routing between the clients is generally not allowed but you can enable it if desired.

Finally, you can generate and download all expert mode files for enabled clients which can be used to easily populate each client.

Operating in server mode with certificates, it is possible to block a specific client by revoking a possibly stolen client certificate (see 5.8.8).

5.6.2. IPsec

IPsec is a protocol suite for securing IP communications by authenticating and encrypting each packet of a communication session and thus establishing a secure virtual private network.

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. It uses the following mechanisms:

Mechanis	Description
AH	Authentication Headers (AH) provide connectionless integrity and data origin authentication for IP datagrams and ensure protection against replay attacks.
ESP	Encapsulating Security Payloads (ESP) provide confidentiality, data-origin authentication, connectionless integrity, an anti-replay service and limited traffic-flow confidentiality.
SA	Security Associations (SA) provide a secure channel and a bundle of algorithms that provide the parameters necessary to operate the AH and/or ESP operations. The Internet Security Association Key Management Protocol (ISAKMP) provides a framework for authenticated key exchange.

Negotating keys for encryption and authentication is generally done by the Internet Key Exchange protocol (IKE) which consists of two phases:

Phase	Description
IKE phase 1	IKE authenticates the peer during this phase for setting up an ISAKMP secure association. This can be carried out by either using `main` or `aggressive` mode. The `main` mode approach utilizes the Diffie-Hellman key exchange and authentication is always encrypted with the negotiated key.The `aggressive` mode just uses hashes of the pre-shared key and therefore represents a less-secure mechanism which should generally be avoided as it is prone to dictionary attacks.
IKE phase 2	IKE finally negotiates IPSec SA parameters and keys and sets up matching IPSec SAs in the peers which is required for AH/ESP later on.

Administration

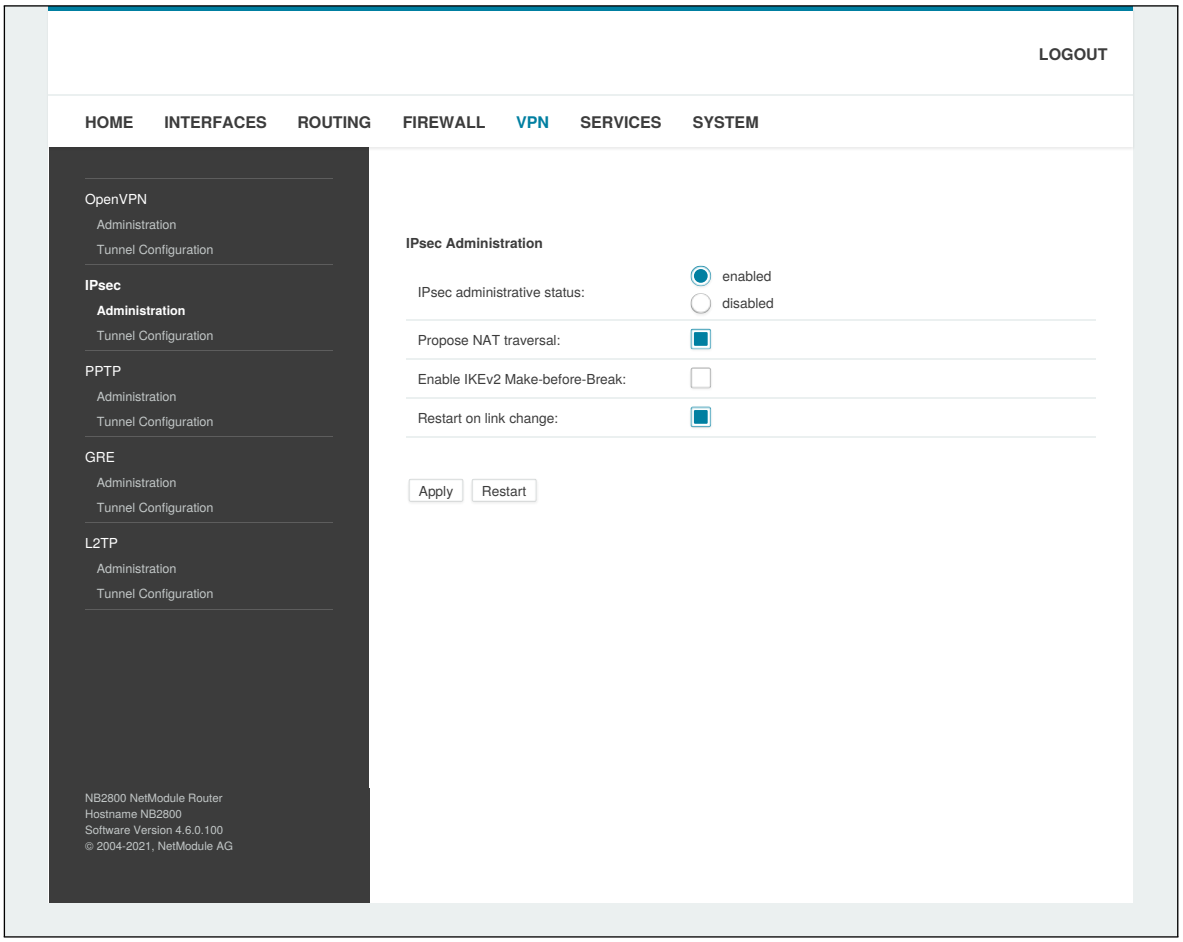


Figure 5.36.: IPsec Administration

This page can be used to enable/disable IPsec, you may also specify whether NAT-Traversal and IKEv2 Make-before-break should be used.

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.

Please note that running NAT-Traversal makes IKE using UDP port 4500 rather than 500 which has to be taken into account when setting up firewall rules.

Make-before-break is an IKEv2 option used to optimize the necessary regular reauthentification by creating an overlapping SA (=make) before deleting the currently used SA (=break). This way, the interruption of the data stream is minimized. Both peers have to be able to handle overlapping SAs to use this option.

Configuration

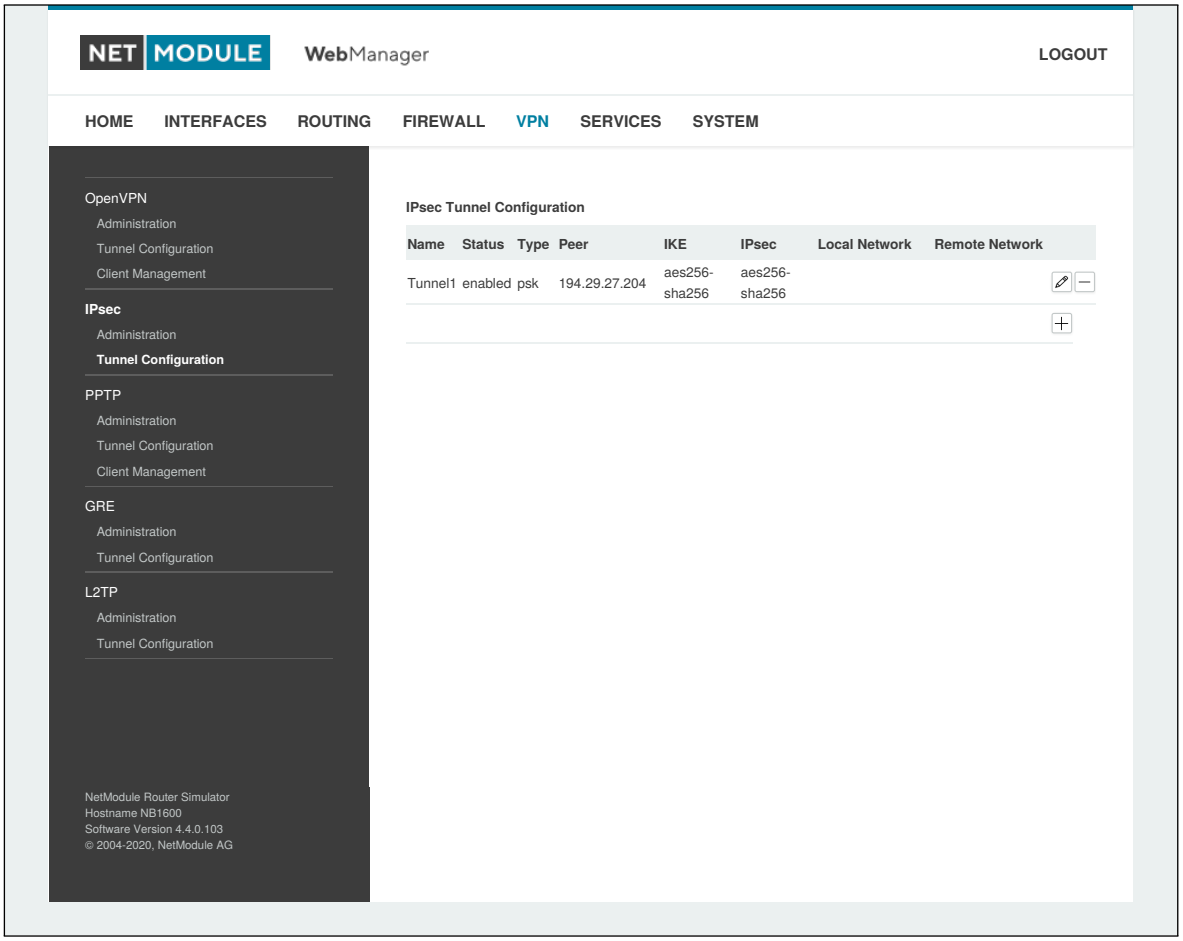


Figure 5.37.: IPsec Configuration

General

For setting up the tunnel you will have to configure the following parameters first:

Parameter	IPsec General Settings
Local IP	IP of the local interface. You may specify 0.0.0.0 to allow any IP address.
Remote peer	IP address or host name of the remote IPsec peer. You may specify 0.0.0.0 to act as a responder for roadwarrior clients.
DPD Status	Specifies whether Dead Peer Detection (see RFC 3706) shall be used. 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	The delay (in seconds) between DPD keepalives that are sent for this connection (default 30 seconds)

Parameter	IPsec General Settings
Failure threshold	The number of unanswered DPD requests until the IPsec peer is considered dead (the router will then try to re-establish a dead connection automatically)
Action	The action to perform if a peer disconnects. Available choices from the drop-down menu are to clear, hold or to Restart the peer.

IKE Authentication

NetModule routers support IKE authentication through pre-shared keys (PSK) or certificates within a public key infrastructure. Extended Authentication (XAUTH) leverages RADIUS-like authentication and can be used to apply user level access control over IPSec.
Using PSK requires the following settings:

Parameter	IPsec IKE Authentication Settings
PSK	The pre-shared key used to authenticate at the peer
Local ID Type	The type of identification for the local ID which can be a `FQDN`, `username@FQDN` or `IP address`
Local ID	The local ID value
Remote ID Type	The type of identification for the remote ID
Remote ID	The remote ID value

When using certificates you would need to specify the operation mode. When run as PKI client (initiator) you can create a Certificate Signing Request (CSR) in the certificates section which needs to be submitted at your Certificate Authority and imported to the router afterwards. In PKI server mode (concentrator), the router represents the Certificate Authority and issues the certificates for remote peers. They are revokable.
Using XAUTH the following settings can be made:

Parameter	IPsec XAUTH Settings
User name	The name of the XAUTH user
User password	The password of the XAUTH user
Group name	The group ID
Group password	The group secret

IKE Proposal

This section can be used to configure the phase 1 settings:

Parameter	IPsec IKE Proposal Settings
Negotiation mode	Choose the desired negotiation mode. Preferably, `main` mode should be used but `aggressive` mode might be applicable when dealing with dynamic endpoint addresses.
Encryption algorithm	The desired IKE encryption method (we recommend AES256)
Authentication algorithm	The desired IKE authentication method (we prefer SHA1 over MD5)
IKE Diffie-Hellman Group	The IKE Diffie-Hellman Group
SA life time	The lifetime of Security Associations
Pseudo-random function	PRF algorithms that can optionally be used.

IPsec Proposal

This section can be used to configure the phase 2 settings:

Parameter	IPsec Proposal Settings
Encapsulation mode	The desired encapsulation mode (Tunnel or Transport)
IPsec protocol	The desired IPsec protocol (AH or ESP)
Encryption algorithm	The desired IKE encryption method (we recommend AES256)
Authentication algorithm	The desired IKE authentication method (we prefer SHA1 over MD5)
SA life time	The lifetime of Security Associations
Perfect forward secrecy (PFS)	Specifies whether Perfect Forward Secrecy (PFS) should be used. This feature increases security as PFS avoids penetration of the key-exchange protocol and prevents compromisation of previous keys.
Force encapsulation	Force UDP encapsulation for ESP packets even if no NAT situation is detected.

Networks

When creating Security Associations, IPsec will keep track of routed networks within the tunnel. Packets will be only transmitted when a valid SA with matching source and destination network is present. Therefore, you may need to specify the networks right and left of the endpoints by applying the following settings:

Parameter	IPsec Network Settings
Local network	The address of your local area network
Local netmask	The netmask of your local area network

Parameter	IPsec Network Settings
Peer network	The address of the remote network behind the peer
Peer netmask	The netmask of the remote network behind the peer
NAT address	Optionally, you can apply NAT (masquerading) for packets coming from a different local network. The NAT address must reside in the network previously specified as local network. If NAT address is enabled but the value is empty the router will try to guess a valid NAT address (not recommended).

Client Management

Once you have successfully set up an IPsec tunnel, you can manage and enable clients connecting to your service. It is possible to generate and download expert mode files for enabled clients which can be used to easily populate each client.

5.6.3. PPTP

The Point-to-Point Tunneling 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, due to its weak encryption algorithms, it is nowadays considered insecure but it still provides a straightforward way for establishing tunnels.

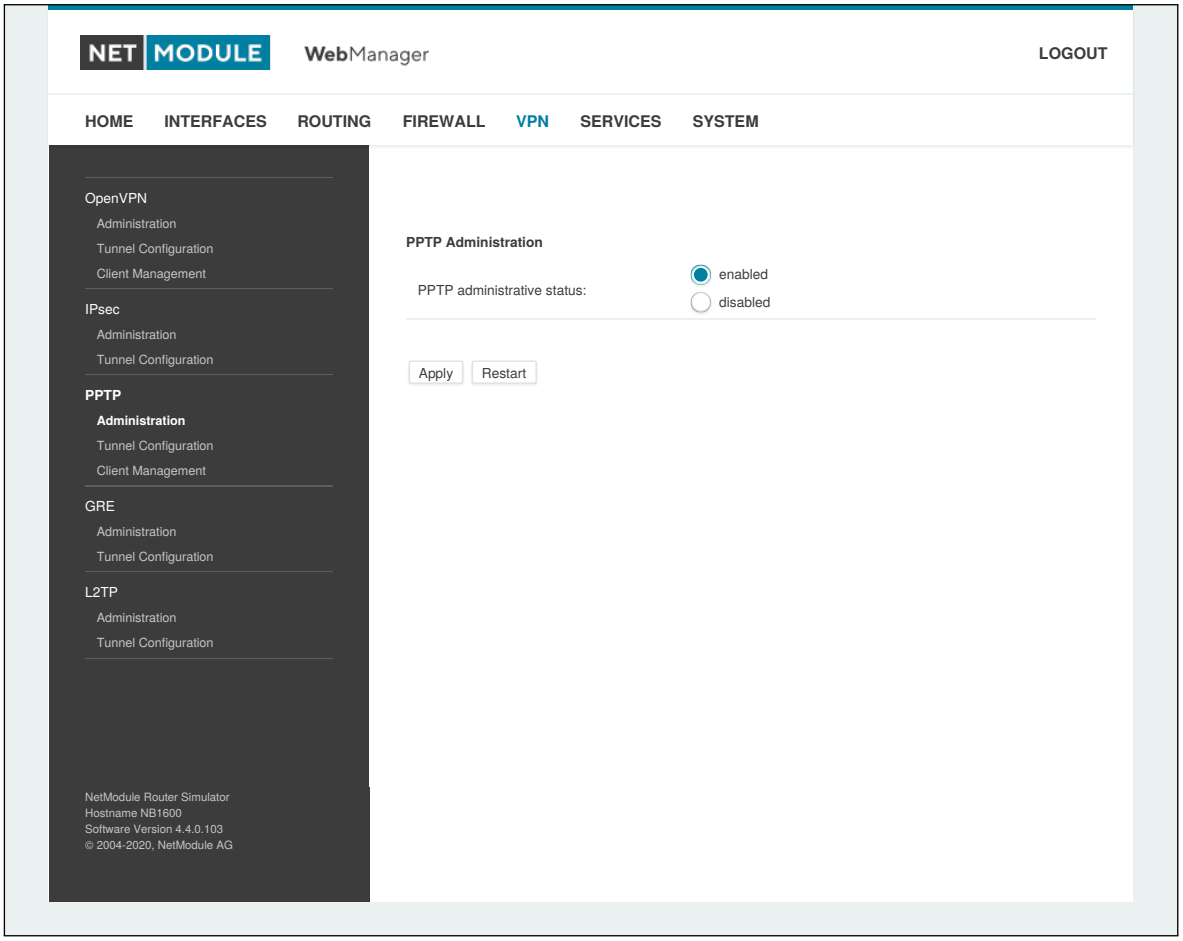


Figure 5.38.: PPTP Administration

When setting up a PPTP tunnel, you would need to choose between server or client. A client tunnel requires the following parameters to be set:

Parameter	PPTP Client Settings
Server address	The address of the remote server
Username	The user-name used for authentication
Password	The password used for authentication

Please note that username and password are not used when setting up clients with fixed addresses.

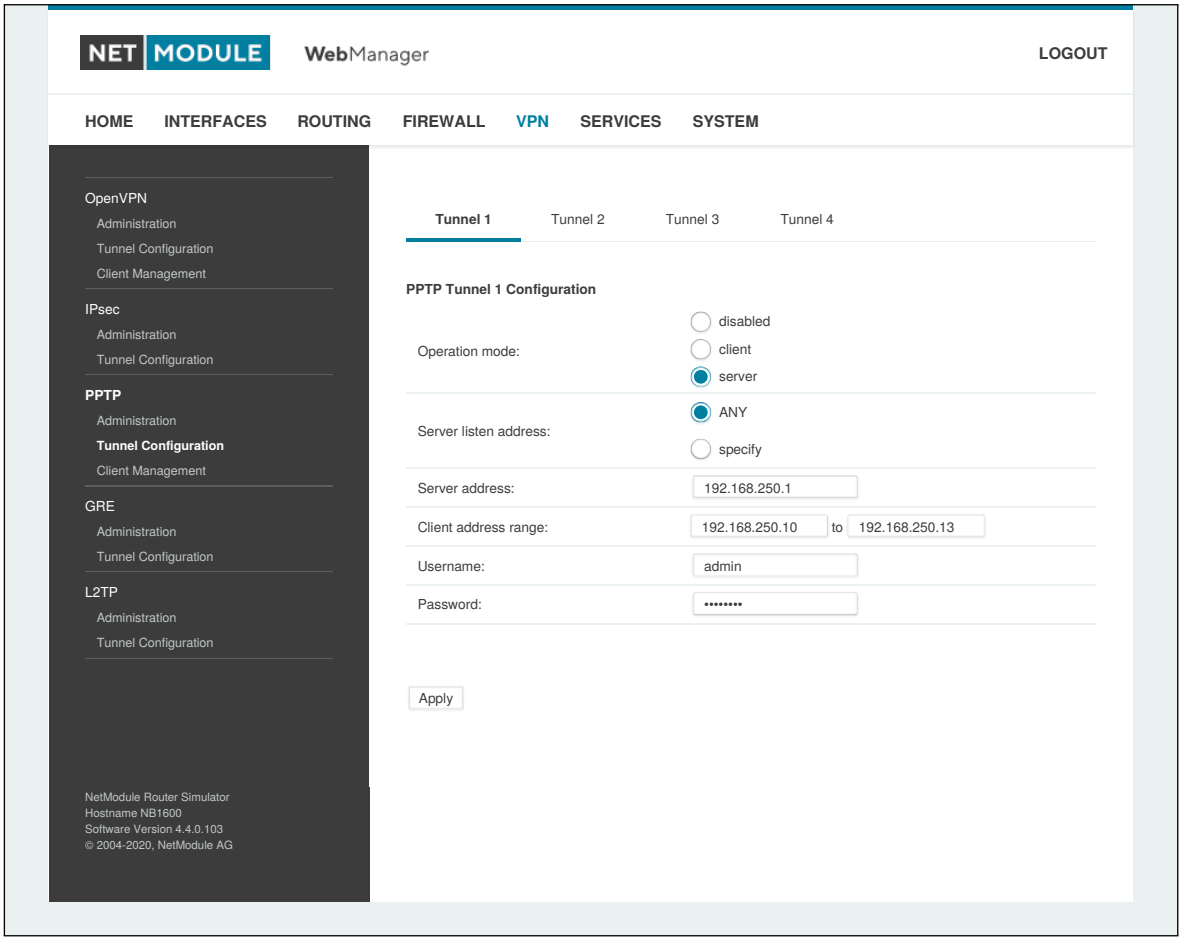


Figure 5.39.: PPTP Tunnel Configuration

Setting up a server requires the following settings:

Parameter	PPTP Server Settings
Listen address	Specifies on which IP address should be listened for incoming client connections
Server address	The server address within the tunnel
Client address range	Specifies a range of IP addresses assigned to each client

PPTP Client Management

PPTP clients for a server tunnel need to be configured here. They are made up of user-name and password. A fixed IP address can be assigned to them which can be used to point any routes to a dedicated tunnel.

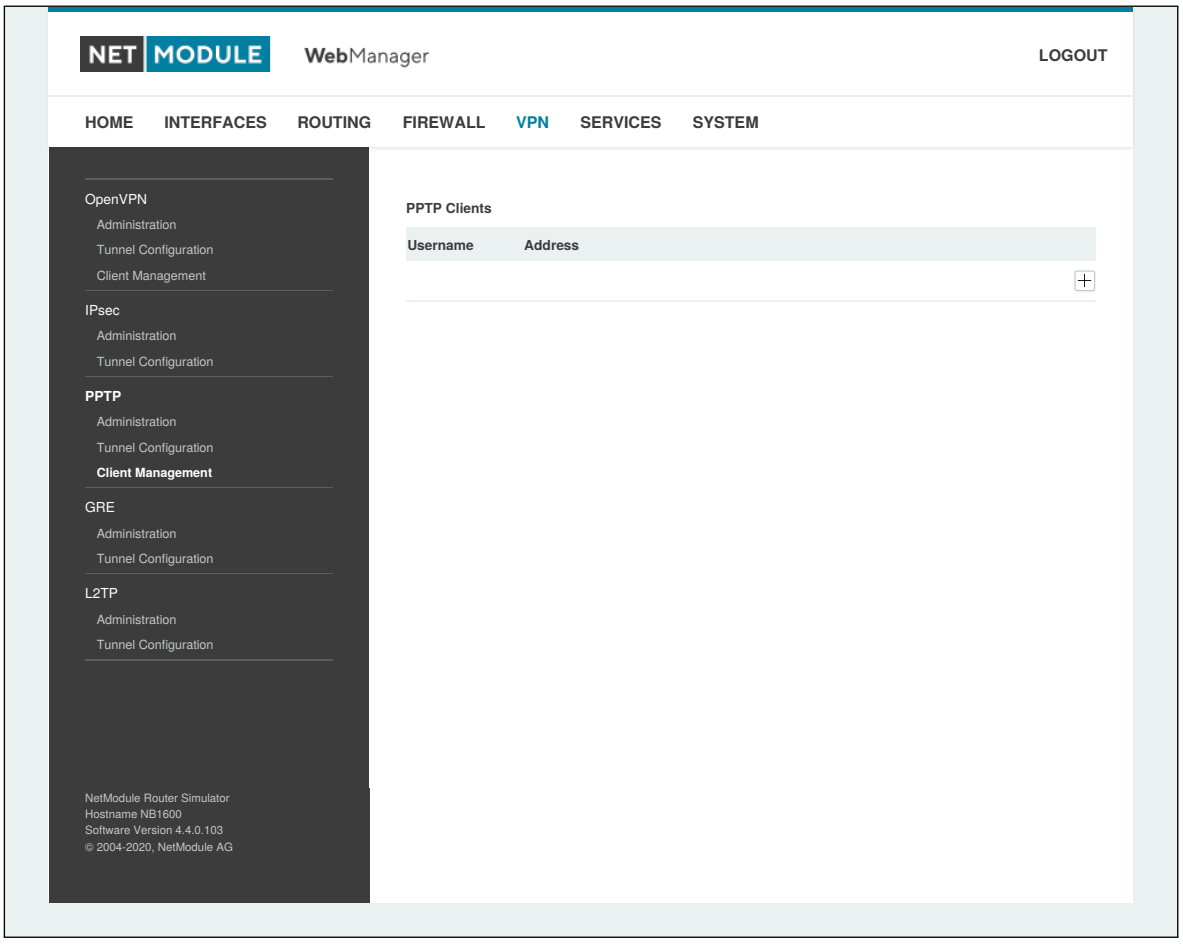


Figure 5.40.: PPTP Client Management

5.6.4. GRE

The Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over IP. GRE is defined in RFC 1701, 1702 and 2784. It does not provide encryption nor authorization but can be used on an address-basis on top of other VPN techniques (such as IPsec) for tunneling purposes.

The following parameters are required for setting up a tunnel:

Parameter	GRE Configuration
Local address	The IP address which is used as sender address of the GRE packets (optional)
Peer address	The IP address of the remote peer
Interface	The device type for this tunnel
Local tunnel address	The local IP address of the tunnel
Local tunnel netmask	The local subnet mask of the tunnel
Remote network	The remote network address of the tunnel
Remote netmask	The remote subnet mask of the tunnel
Tunnel key	Gre tunnel key allows the remote server to distinguish between GRE packets from different communication partners

In general, the local tunnel address/netmask should not conflict with any other interface addresses. The remote network/netmask will result in an additional route entry in order to control which packets should be encapsulated and transferred over the tunnel.

5.6.5. L2TP

The Layer 2 Tunneling Protocol is a tunneling protocol which does not support any encryption or confidentiality. It relies on an encryption protocol that it passes within the tunnel to provide privacy.
The following parameters are required for setting up a tunnel:

Parameter	L2TP Configuration
Transport protocol	The transport portocol which shall be used
Local IP	The local IP address of the tunnel
Remote IP	The remote IP address of the tunnel
Local port	The local port address of the tunnel
Remote port	The remote port address of the tunnel
Local tunnel ID	The local tunnel ID identifies the tunnel into which the session will be created
Remote tunnel ID	The remote tunnel ID identifies the tunnel assigned by the peer
Local Session ID	The local session ID identifies the session being created
Remote Session ID	The remote session ID identifies the session assigned by the peer
Local Cookie	The local cookie sets an optional cookie value to be assigned to the session
Remote Cookie	The remote cookie set an optional pper cookie value to be assigned to the session
MTU	The Maximum Transmission Unit of the tunnel interface
Bridge Interface	The interface to which the guest interace shall be bridged

5.6.6. Dial-In

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 outgoing WWAN interfaces and Dial-In connection is not possible.

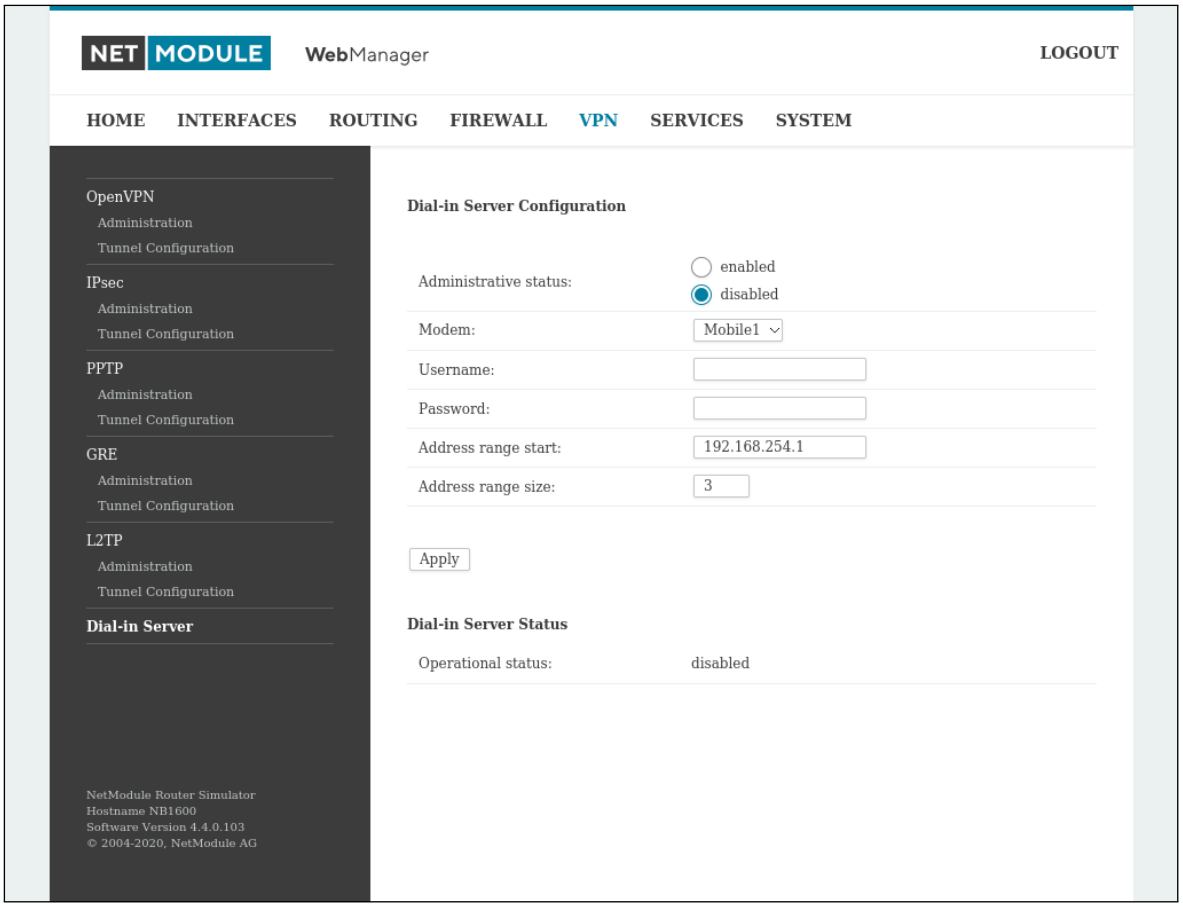


Figure 5.41.: Dial-in Server Settings

The following settings can be set:

Parameter	Dial-in Server Configuration
Administrative status	Specifies whether incoming calls shall be answered or not
Modem	Specifies the modem on which calls can come in
User	Specifies the username for the incoming PPP connection
Password	Specifies the password for the incoming PPP connection
Address range start	Start of the IP address range assigned to incoming clients
Address range size	Number of addresses for client IP address range

Please note that Dial-In connections are generally discouraged. As they are implemented as GSM voice calls, they suffer from unreliability and poor bandwidth.

5.7. SERVICES

5.7.1. SDK

NetModule 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 NetModule-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 support@netmodule.com 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:

```
/* We are going to eavesdrop on the first serial port
 * and turn on lights via a digital I/O output port,
 * otherwise we'd have to send a short message.
 */

for (attempts = 0; attempts < 3; attempts++) {
  if (nb_serial_read("serial0") == "Knock Knock!") {
    nb_serial_write("serial0", "Who's there?");

    if (nb_serial_read("serial0") == "Santa") {
      printf("Hurray!\n");
      nb_dio_set("out1", 1);
    }
  }
}
nb_sms_send("+123456789", "No presents this year :(")
```

A set of example scripts can be downloaded directly from the router, you can find a list of them in the appendix. The manual which can be obtained from the NetModule support web page 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. Perform config/software updates
13. Control the LEDs
14. Get system events, restart services or reboot system
15. Scan for networks in range
16. Create your own web pages
17. Voice control functions
18. SNMP functions
19. CAN socket functions
20. Various network-related functions
21. Other system-related functions

The SDK API manual (which can be downloaded from the router) provides an overview but also explains all functions in detail.
Please note that some functions require the corresponding services (e.g. E-Mail, SMS) or configured interfaces (e.g. CAN) 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 location */

dump(nb_status("location"));
```

The script will then generate lines like maybe these:

```
struct(8): {
  .LOCATION_STREET       = string[11]: "Bahnhofquai"
  .LOCATION_CITY         = string[10]: "Zurich"
  .LOCATION_COUNTRY_CODE = string[2]:  "ch"
  .LOCATION_COUNTRY      = string[11]: "Switzerland"
  .LOCATION_POSTCODE     = string[4]:  "8001"
  .LOCATION_STATE        = string[6]:  "Zurich"
  .LOCATION_LATITUDE     = string[9]:  "47.3778058"
  .LOCATION_LONGITUDE    = string[8]:  "8.5412757"
}
```

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 wanlink.0
cli get -c wanlink.0
Showing configuration entities (matching 'wanlink.0'):

wanlink.0.mode          wanlink.0.multipath    wanlink.0.name
wanlink.0.options       wanlink.0.passthru     wanlink.0.prio
wanlink.0.suspend       wanlink.0.switchback   wanlink.0.weight
```

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 current city and enable the second WAN link */

location = nb_status("location");
if (location) {
    city = struct_get(location, "LOCATION_CITY");

    if (city == "Wonderland") {
        for (led = 0; led < 5; led++) {
            nb_led_set(led, LED_BLINK_FAST|LED_COLOR_RED);
        }
    } else {
        printf("You'll never walk alone in %s ...\n", city);
        nb_config_set("wanlink.1.mode=1");
    }
}
```

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 Events chapter 5.7.7. 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 space of the storage device. You may, however, extend it by external USB storage or (depending on your model) extended flash storage.

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

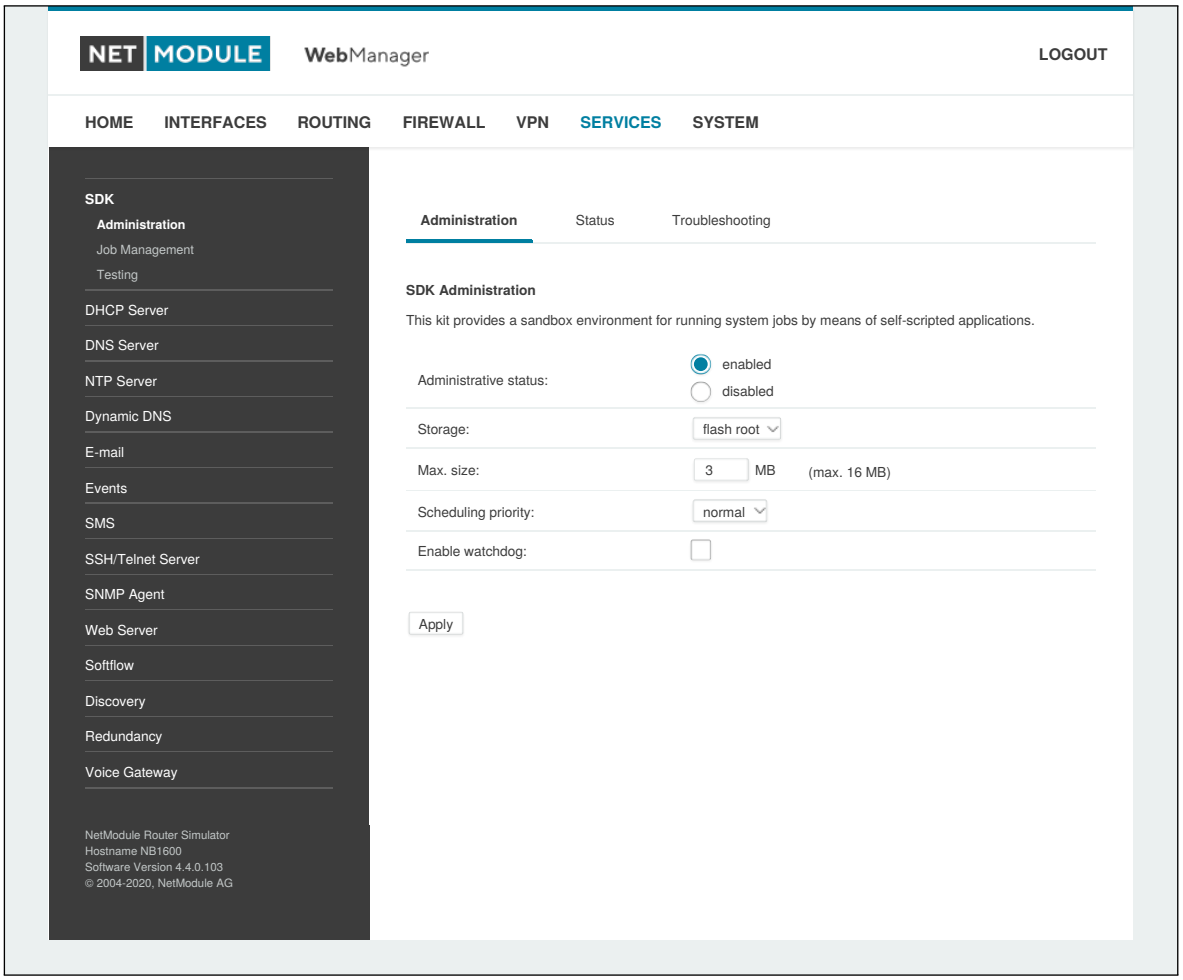


Figure 5.42.: SDK Administration

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

Parameter	SDK Administration Settings
Administrative status	Specifies whether SDK scripts should run or not
Storage	The storage device on which the sandbox shall be stored (see chapter 5.8.1)
Max. size	The maximum amount of MBytes your scripts can can consume on the storage device
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
Enable watchdog	This option will enable watchdog supervision for each script which leads to a reboot of the system if the script does not respond or stopped with an exit code not equal zero.

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

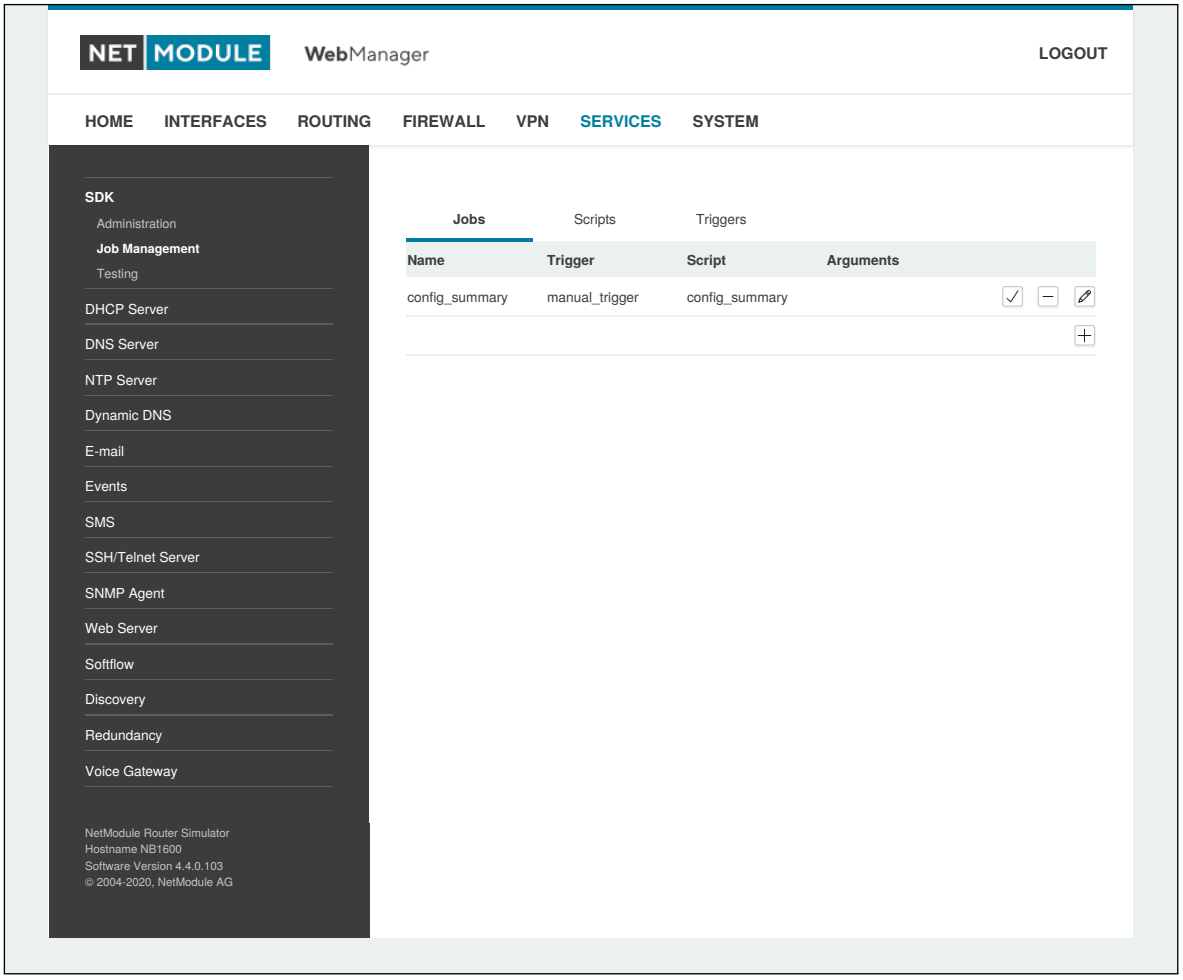


Figure 5.43.: SDK Jobs

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:

Parameter	SDK Trigger 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:

Parameter	SDK Script 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:

Parameter	SDK Job 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

You can trigger each configured job directly which can be helpful for testing purposes.

Pages

Any programmed SDK pages will show up here.

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 or upload an entire file. 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", i, 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:

Command	Action
status	Will reply a message to the sender including a short system overview
connect	Will enable the first WAN link configured on the system
disconnect	Will disable the first WAN link configured on the system
reboot	Initiates a reboot of the system
output 1 on	Turns on the first digital output port
output 1 off	Turns off the first digital output port
output 2 on	Turns on the second digital output port
output 2 off	Turns off the second digital output port

Table 5.95.: SMS Control Commands

A response to the status command typically looks like:

```
System: NB2700 hostname (00:11:22:AA:BB:CC)
WAN1: WWAN1 is up (10.0.0.1, Mobile1, UMTS, -83 dBm, LAI 12345)
GPS: lat 47.377894, lon 8.540055, alt 282.200
OVPN: client on tun0 is up (10.0.8.4)
DIO: IN1=off, IN2=off, OUT1=on, OUT2=off
```

5.7.2. DHCP Server

This section can be used to individually configure the Dynamic Host Configuration Protocol (DHCP) service for each LAN interface which will serve dynamic IP addresses to hosts in the local network. You may also have a look to the status page where you can find an overview about negotiated client addresses.

Please note that WLAN interfaces (for each SSID) will pop up here as well in case you have configured an access point respectively.

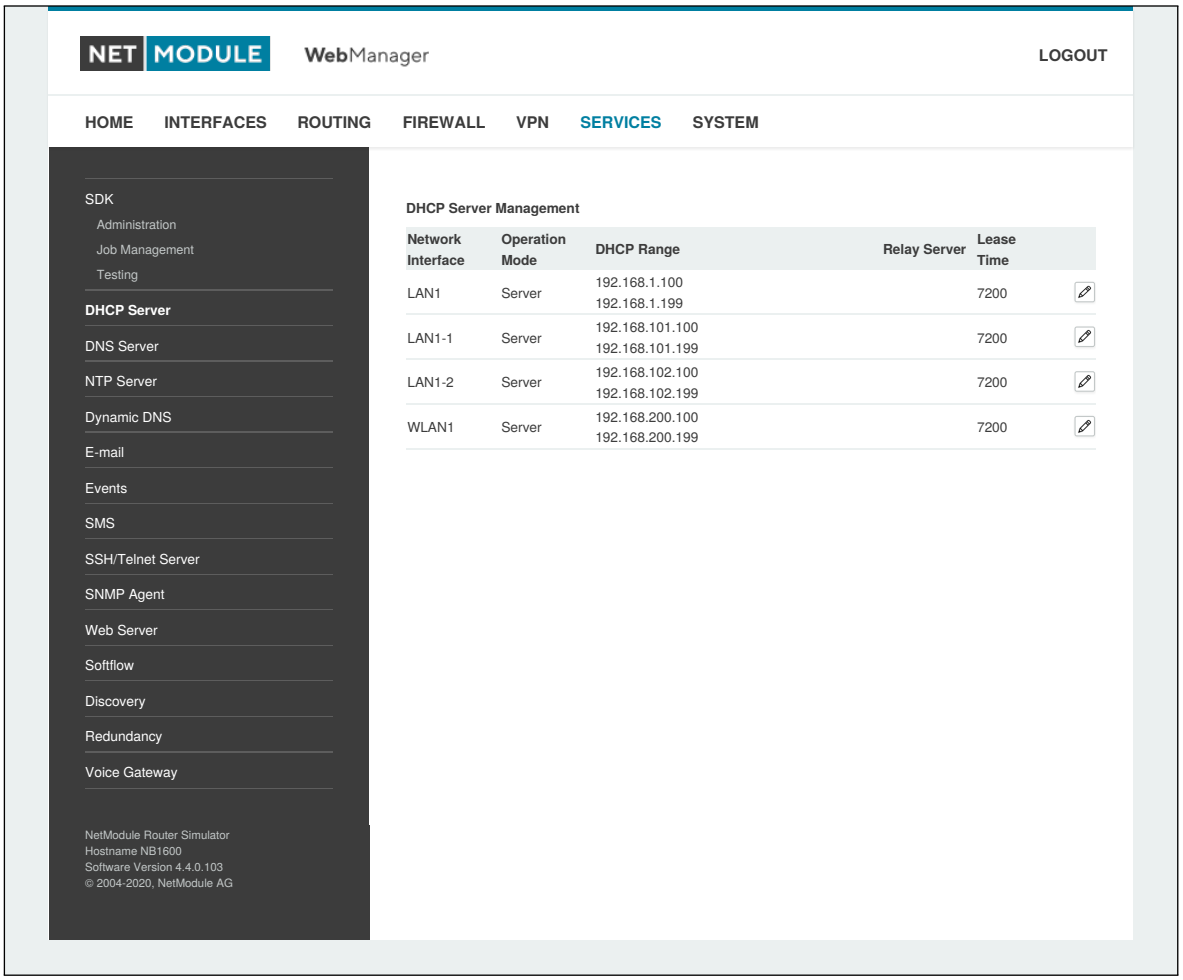


Figure 5.44.: DHCP Server

The following settings for each interface can be applied then:

Parameter	DHCP Administrative Settings
Operation mode	Specifies whether the DHCP mode is server, relay or disabled

Parameter	DHCP Server Settings
First lease address	The first address out of the range of IP addresses given to hosts

Parameter	DHCP Server Settings
Last lease address	The last address out of this range
Lease duration	Number of seconds how long a given lease shall be valid until it has to be requested again
Persistent leases	By turning on this option the router will remember issued leases even after a reboot. This can be used to ensure that the same IP address will be assigned to a particular host.
DHCP options	By default the DHCP will hand out the interface address as default gateway and the current DNS server addresses if not configured elsewise. You can specify fixed addresses here.
Only allow static hosts	Any requests coming from none-static hosts will be ignored.

Parameter	DHCP Options
Gateway address	The default gateway address
Primary DNS	The primary nameserver
Secondary DNS	The secondary nameserver
Primary WINS	The primary WINS server
Secondary WINS	The secondary WINS server
Agent ID	The relay agent ID (DHCP option 82)

Parameter	DHCP Relay Settings
Primary relay server	The primary DHCP relay server
Secondary relay server	The secondary DHCP relay server

It is also possible to configure specific lease addresses for particular clients.

Parameter	DHCP Static Hosts Settings
IP address	The IP address of the lease
Identified by	Specifies by which criteria the client shall be identified
MAC address	The MAC address of the client
hostname	The client identifier (DHCP option 61)
port	The Ethernet port on which the DHCP request is received

Additional DHCP options can be specified via the custom DHCP options.

Parameter	DHCP Custom Options
Key	The option, to be sent as a decimal number or as “option:<option-name>” (RFC2132)
Value	The value of the additional DHCP option to be sent as a string

5.7.3. 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.

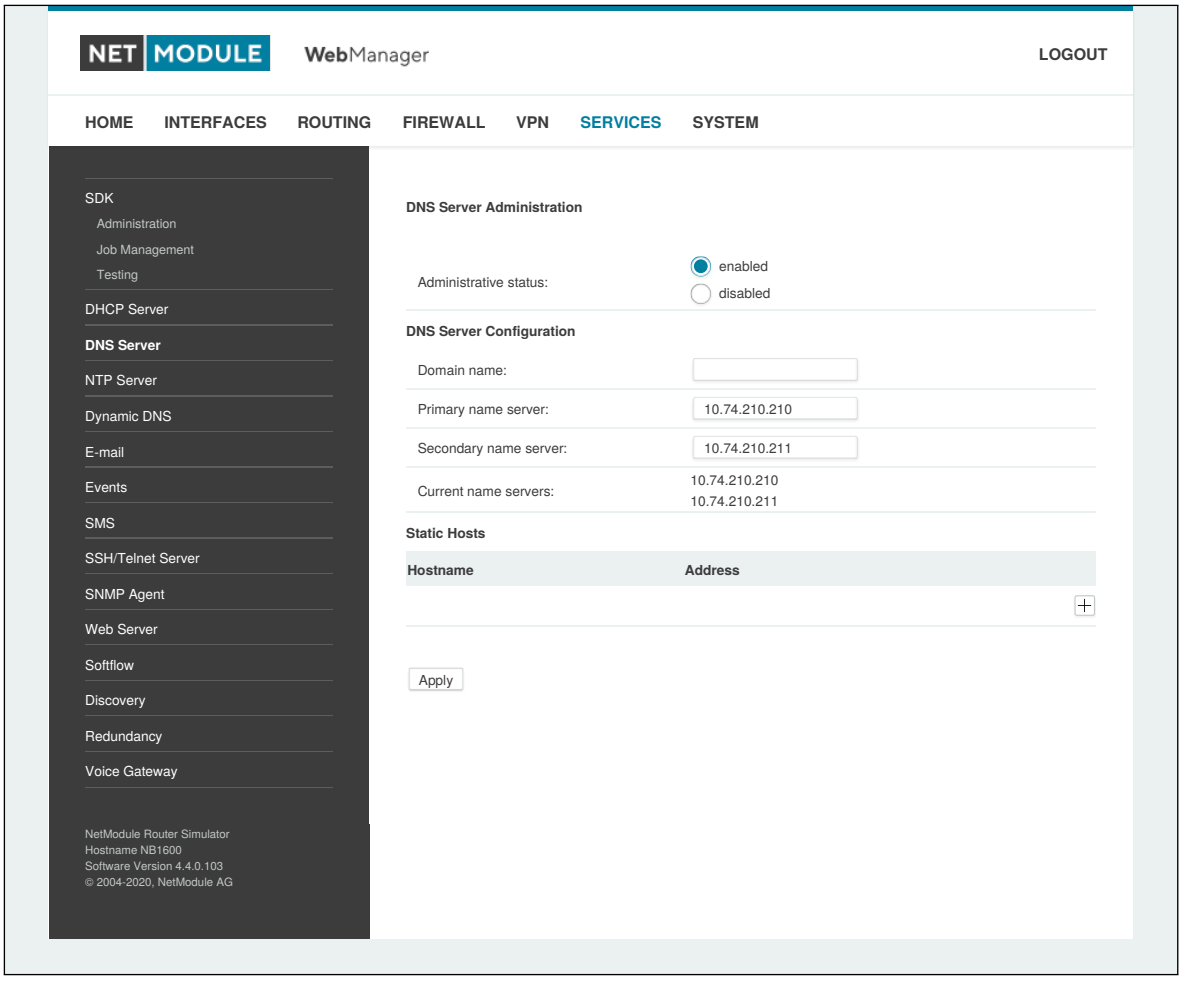


Figure 5.45.: DNS Server

The following settings can be applied:

Parameter	DNS Server Settings
Administrative status	Enables or disables the DNS server
Domain name	The domain name used for short name lookups
Primary name server	The primary default name server which will be used instead of negotiated name servers
Secondary name server	The secondary default name server which will be used instead of negotiated name servers

You may further configure static hosts for serving fixed IP addresses for various host names.

Parameter	DNS Static Hosts Settings
Address	The IP address of the static host
Hostname	The hostname of the static host

Please remember to point DNS lookups of local hosts to the router's address.

5.7.4. NTP Server

This section can be used to individually configure the Network Time Protocol (NTP) server function.

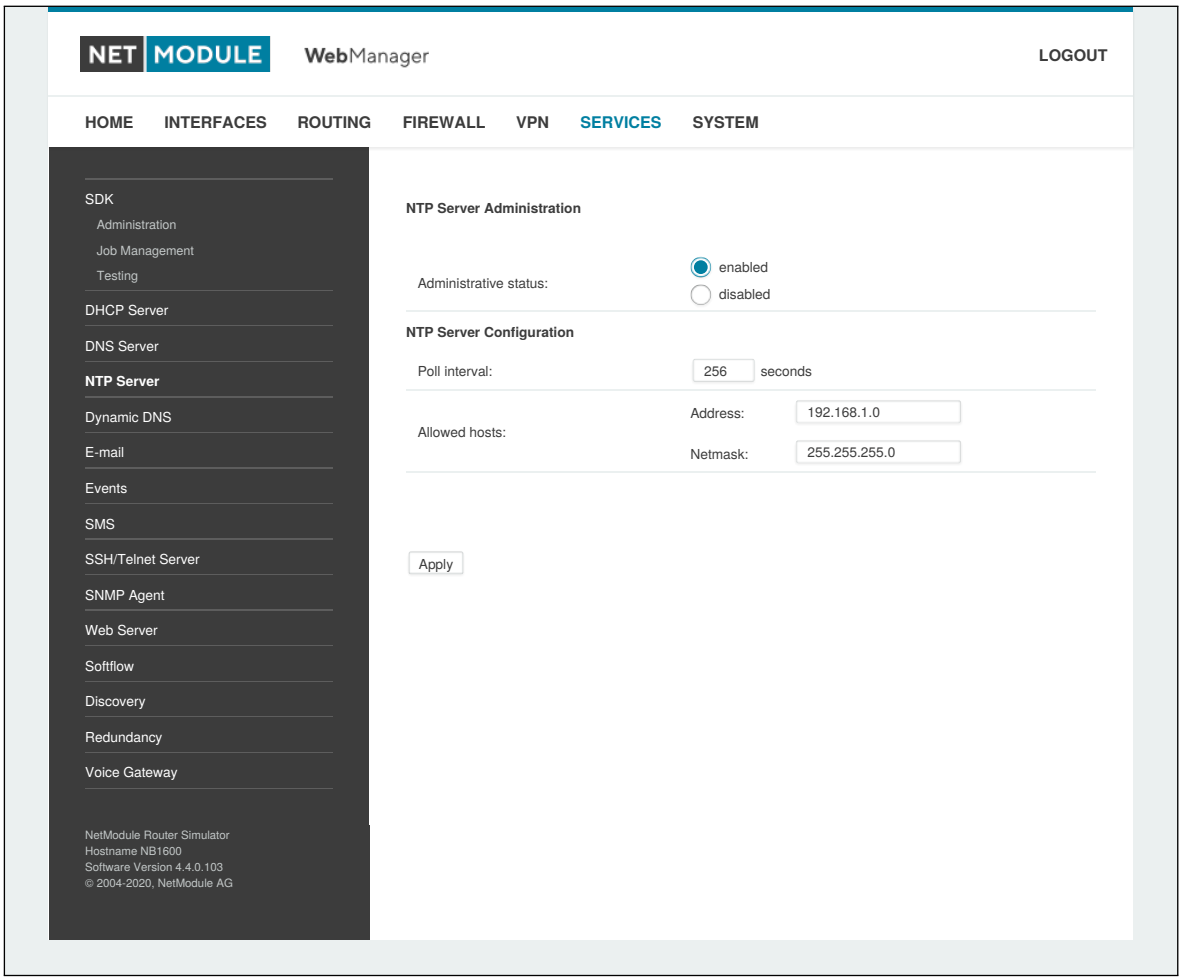


Figure 5.46.: NTP Server

The following settings for each interface can be applied then:

Parameter	NTP Server Settings
Administrative status	Specifies whether the NTP server is enabled or not
Poll interval	Defines the polling interval (64..2048 seconds) for synchronizing the time with the master clock servers
Allowed hosts	Defines the IP address range which is allowed to poll the NTP server

For setting the system time of the device see 5.8.1.

5.7.5. Dynamic DNS

The Dynamic DNS client can be used to tell one or multiple DynDNS providers the current IP address of your system. This address can be derived from the current hotlink interface or the outgoing interface which will be used when contacting the server. We further support to ask the CheckIP service at dyndns.org for obtaining the current Internet address which can be useful in NAT scenarios. The DynDNS client will be triggered whenever a WAN or VPN link comes up.

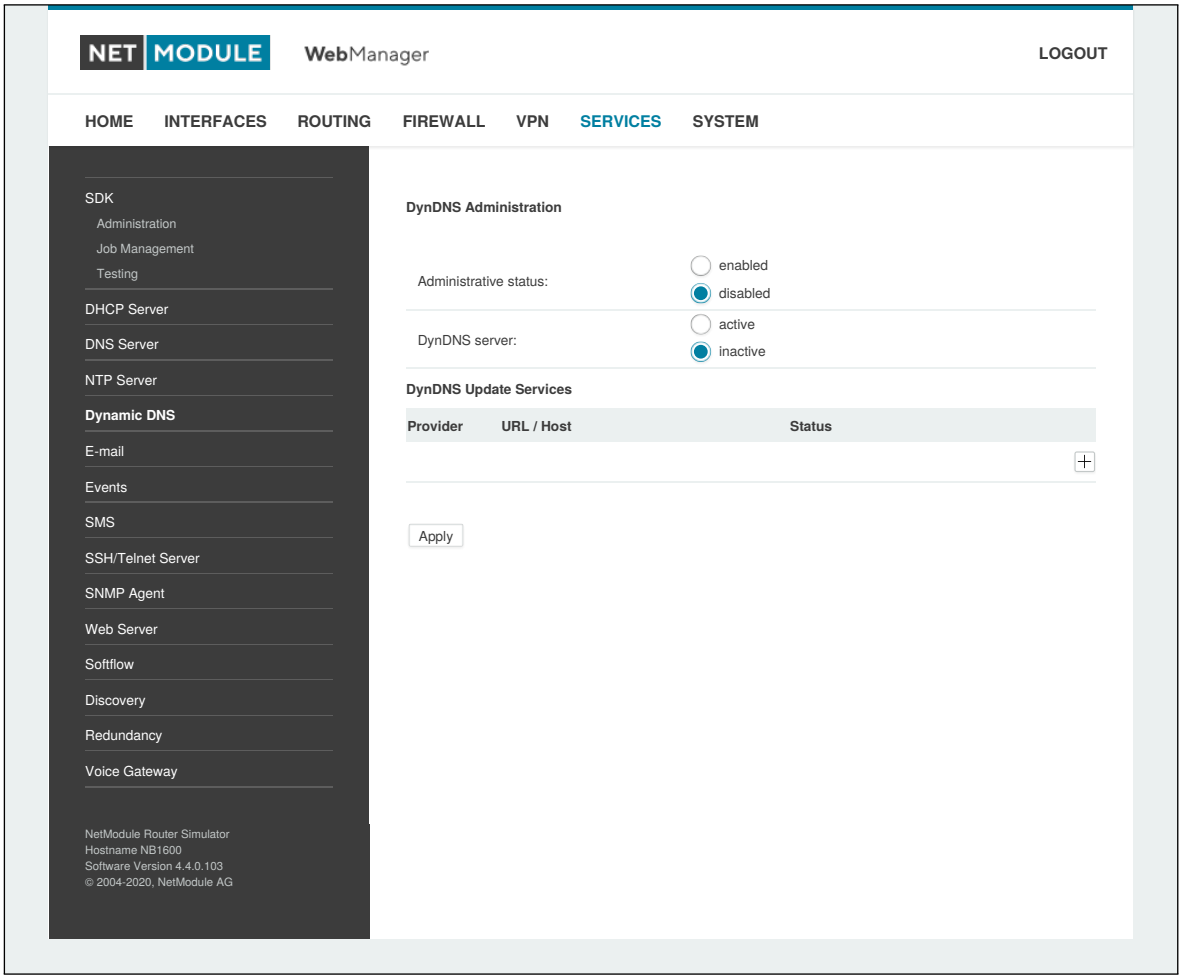


Figure 5.47.: Dynamic DNS Settings

We provide support for a bunch of common DynDNS operators but it is also possible to define a custom update URL.

Please note that your NetModule router can operate as DynDNS server on its own, provided that you have your hosts pointed to the DNS service of the router.

We can further operate the GnuDIP protocol and RFC2136-like dynamic DNS updates. The latter is in general secured by a TSIG key.

A DynDNS service can receive the following parameters:

Parameter	Dynamic DNS Settings
Provider	You can choose one of the listed providers or provide a custom URL
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. my-box.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
Protocol	The protocol used for authentication (HTTP, HTTPS)
Server address	The address of the server which shall be updated
Server port	The port of the server which shall be updated
TSIG key name	The name of the TSIG key which is allowed to perform updates
TSIG key	The TSIG key encoded in base64

5.7.6. E-Mail

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

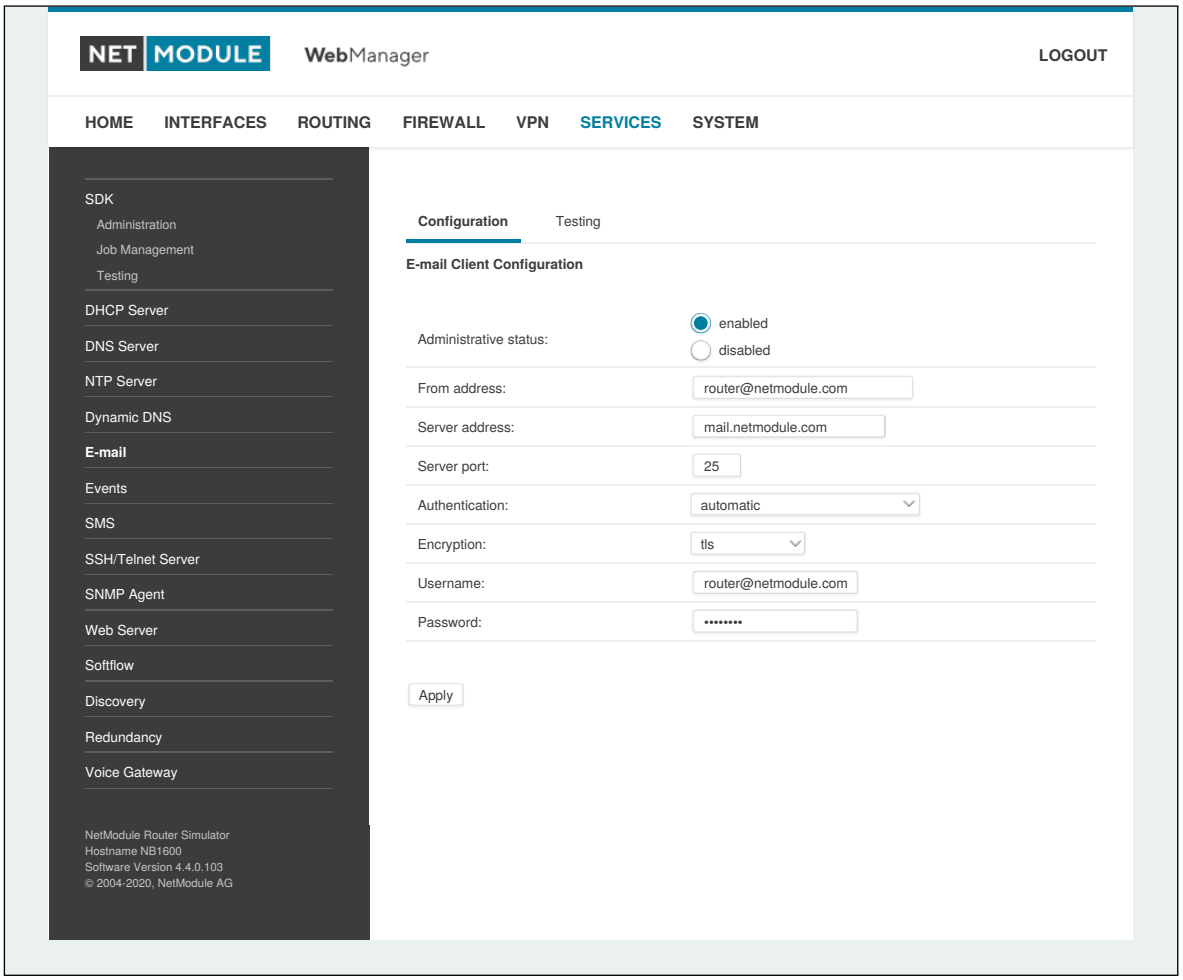


Figure 5.48.: E-Mail Settings

It can be enabled by applying the following settings.

Parameter	E-Mail Client Settings
E-mail client status	Administrative status of the E-Mail client
From e-mail address	E-Mail address of the sender
Server address	SMTP server address
Server port	SMTP server port (typically 25)
Authentication method	Select the required authentication method which will be used to authenticate against the SMTP server
Encryption	Select the encryption. Can be STARTTLS or none.
Username	User name used for authentication

Parameter	E-Mail Client Settings
Password	Password used for authentication

5.7.7. Events

By using the event manager you can notify remote systems about system events. A notification can be sent using E-Mail, SMS or SNMP traps.

Parameter	Event Notification Settings
E-Mail address	The E-Mail address to which the notification shall be sent (E-Mail client must be enabled)
Phone number	The phone number to which the notification shall be sent (SMS service must be enabled)
SNMP host	The SNMP host or address to which the trap shall be sent
SNMP port	The port of the remote SNMP service
Username	The username for accessing the remote SNMP service
Password	The password for accessing the remote SNMP service
Authentication	The authentication algorithm for accessing the remote SNMP service (MD5 or SHA)
Encryption	The encryption algorithm for accessing the remote SNMP service (DES or SHA)
Engine ID	The engine ID of the remote SNMP service

The messages will contain a description provided by you and a short system information.
A list of all system events can be found in the appendix A.2.

5.7.8. SMS

Administration

NetModule routers can receive or send short messages (SMS) if enabled by your SIM provider.

Messages are received/sent by the modem which has been assigned to a SIM, so one has to properly configure a SMS-capable default modem as described in chapter 5.3.3.

Please note that the system may switch SIMs in case you are running multiple WWAN interfaces sharing the same SIM. Thus, it may happen that a different modem will be used for communication or, if the SIM is unassigned, any operation will even stop.

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 PLMN) in the Mobile SIMs section (see 5.3.3).

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.

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.

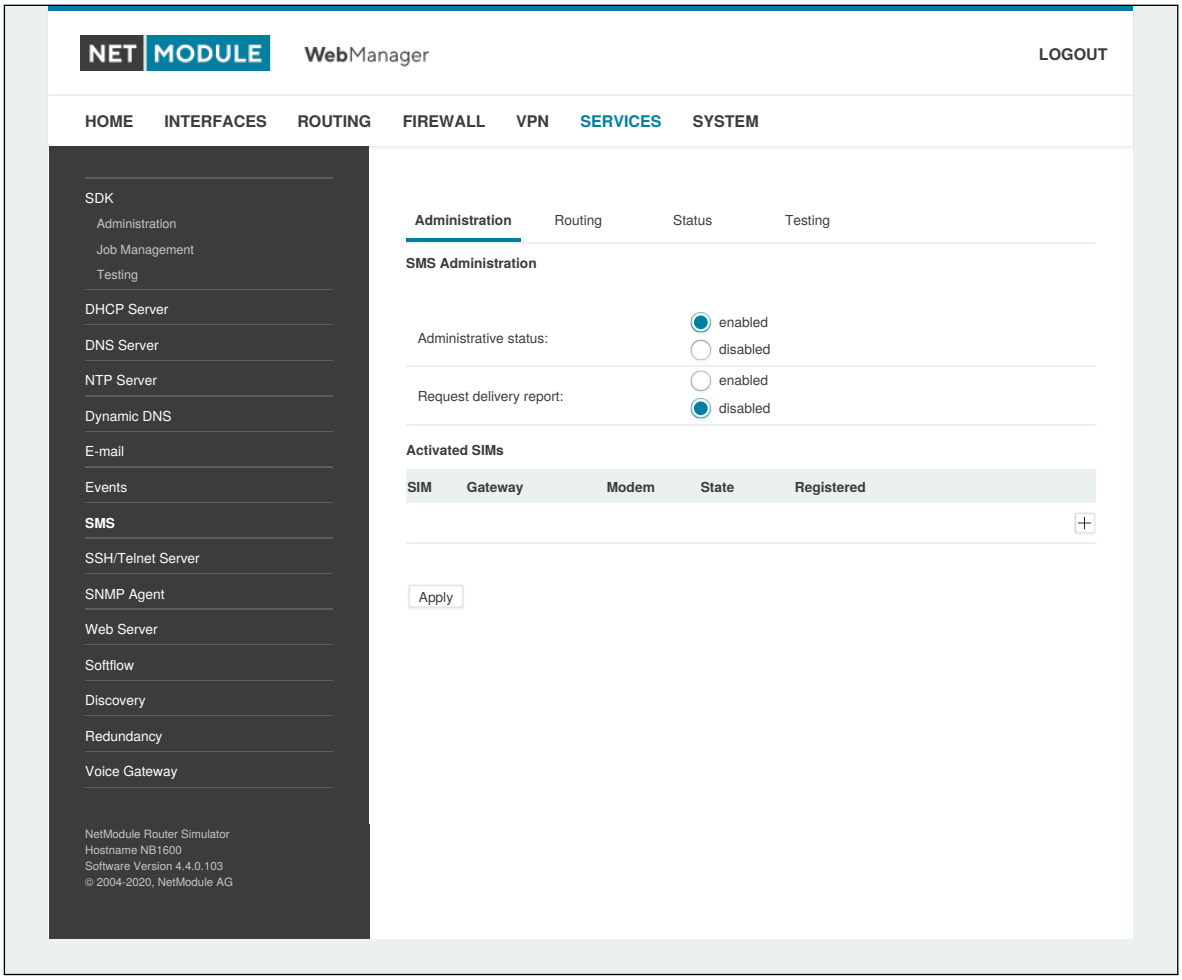


Figure 5.49.: SMS Configuration

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

identify SIMs based on their IMEI number and track their statistics in a non-volatile manner.

Parameter	SMS SIM Configuration
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.

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:

Number	Result
+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

Table 5.109.: SMS Number Expressions

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.

5.7.9. 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.

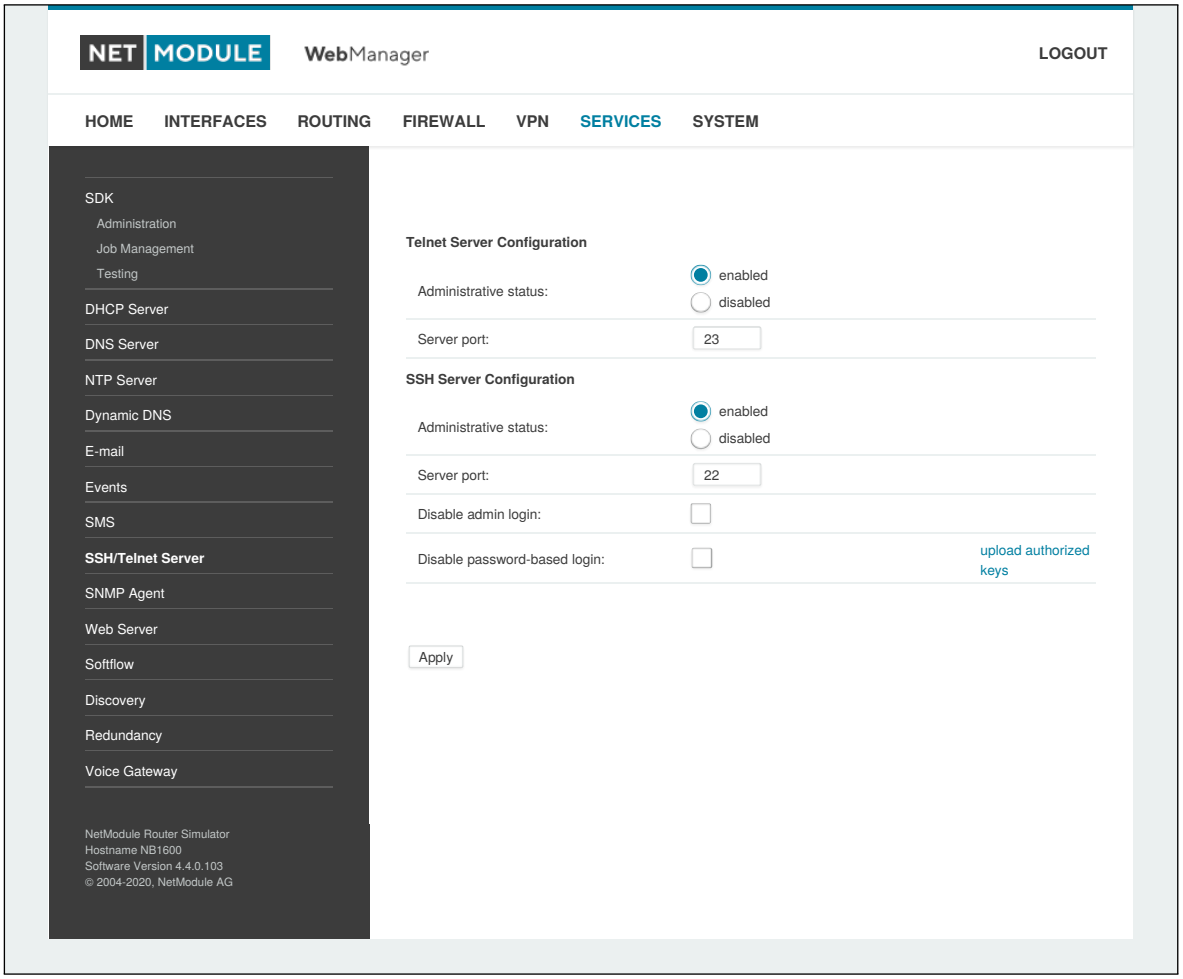


Figure 5.50.: SSH and Telnet Server

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:

Parameter	Telnet Server Settings
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:

Parameter	SSH Server Settings
Administrative status	Whether the SSH service is enabled or disabled
Server port	The TCP port of the service (usually 22)
Disable admin login	Disable login for admin users
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.

5.7.10. SNMP Agent

NetModule routers are equipped with an SNMP daemon, supporting basic MIB tables (such as ifTable), plus additional enterprise MIBs to manage multiple systems.

Parameter	Supported MIBs
.1.3.6.1.2.1	MIB-II (RFC1213), SNMPv2-MIB (RFC3418)
.1.3.6.1.2.1.2.1	IF-MIB (RFC2863)
.1.3.6.1.2.1.4	IP-MIB (RFC1213)
.1.3.6.1.2.1.10.131	TUNNEL-MIB (RFC4087)
.1.3.6.1.2.25	HOST-RESOURCES-MIB (RFC2790)
.1.3.6.1.6.3.10	SNMP-FRAMEWORK-MIB
.1.3.6.1.6.3.11	SNMPv2-SMI (RFC2578)
.1.0.8802.1.1.2	LLDP-MIB
.1.0.8802.1.1.2.1.5.4795	LLDP-EXT-MED-MIB
.1.3.6.1.4.1.31496	VENDOR-MIB

The VENDOR-MIB tables offer some additional information over the system and its WWAN, GNSS and WLAN interfaces. They can be accessed over the following OIDs:

Parameter	Vendor MIB OID Assignment
NBAdminTable	.1.3.6.1.4.1.31496.10.40
NBWwanTable	.1.3.6.1.4.1.31496.10.50
NBGnssTable	.1.3.6.1.4.1.31496.10.51
NBDioTable	.1.3.6.1.4.1.31496.10.53
NBWlanTable	.1.3.6.1.4.1.31496.10.60
NBWanTable	.1.3.6.1.4.1.31496.10.22

They offer facilities 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

Our VENDOR-MIB is listed in the appendix or can be downloaded directly from the router.

SNMP Configuration

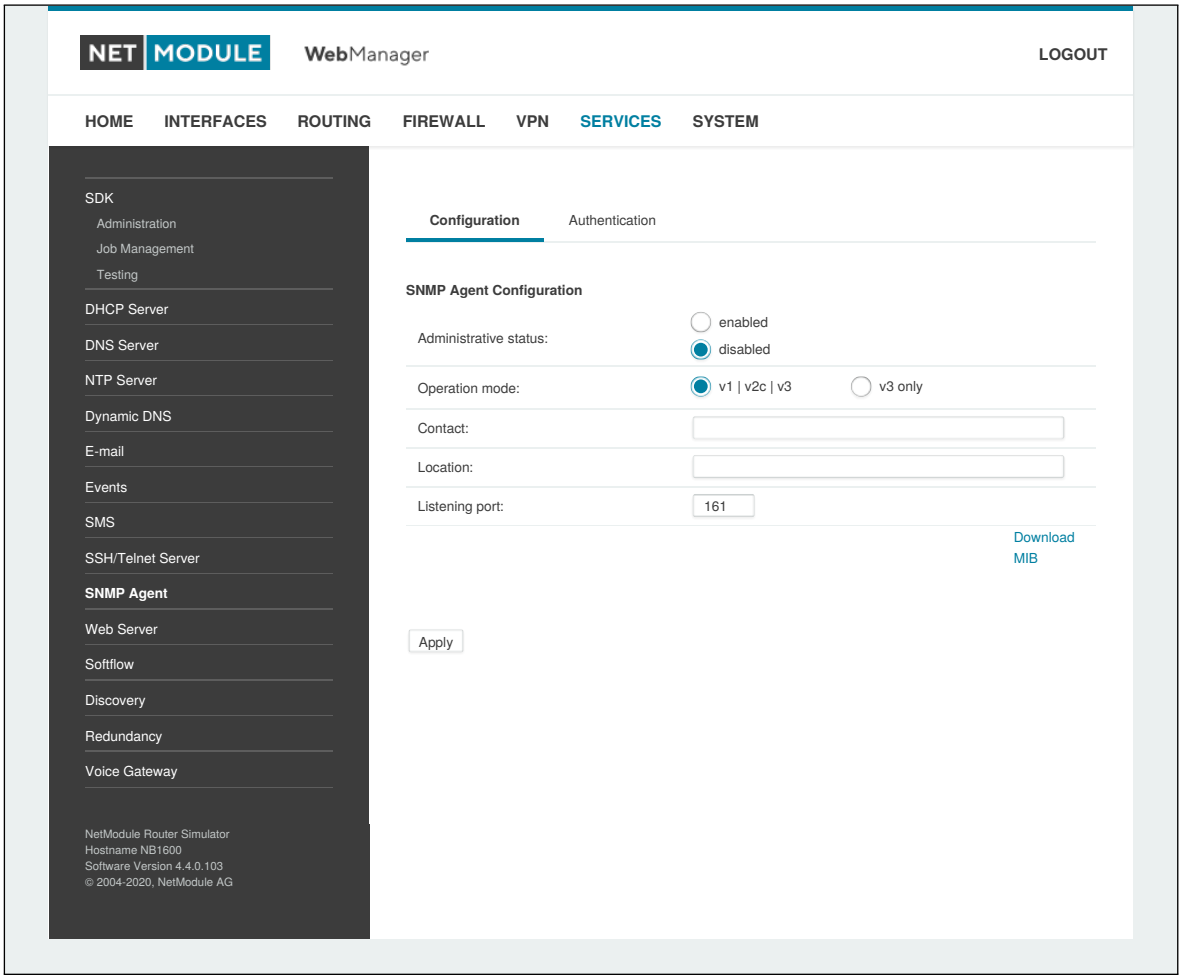


Figure 5.51.: SNMP Agent

The following parameters can be used to configure the SNMP agent:

Parameter	SNMP Configuration
Administrative status	Enable or disable the SNMP agent
Operation mode	Specifies if agent should run in compatibilty mode or for SNMPv3 only
Contact	System maintainer or other contact information
Location	Location of the device
Listening Port	SNMP agent port

Once the SNMP agent is enabled, SNMP traps can be generated using SDK scripts.

SNMP Authentication

When running in SNMPv3, it is possible to configure the following authentication settings:

Parameter	SNMPv3 Authentication
Authentication	Defines the authentication (MD5 or SHA)
Encryption	Defines the privacy protocols to use (DES or AES)

In general, the admin user can read and write any values. Read access will be granted to any other system users.
There is no authentication/encryption in SNMPv1/v2c and should not be used to set any values. However, it is possible to define its communities and authoritive host which will be granted administrative access.

Parameter	SNMPv1/v2c Authentication
Read community	Defines the community name for read access
Admin community	Defines the community name for admin access
Allowed host	Defines the host which is allowed for admin access

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`).
Due to the use of passphrases in SNMP it is mandatory to store passwords of users who shall be able to authenticate against the SNMP server. Please refer to chapter 5.8.2 for more information.
Please note that the SNMP daemon is also listening on WAN interfaces and it is therefore suggested to restrict the access with the firewall.

Typical SNMP Commands

Setting MIB values and triggering extensions is generally limited to the SNMPv3 admin user. It is possible to specify an administrative host for SNMP v1/2c.
The SNMP extensions can be read and triggered as follows:

Getting the software version of the system:

```
snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1
    1.3.6.1.4.1.31496.10.40.1.0
```

Getting the kernel version:

```
snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1
    1.3.6.1.4.1.31496.10.40.2.0
```

Getting the serial number:

```
snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1
    1.3.6.1.4.1.31496.10.40.3.0
```

Getting the current config description:

```
snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1
    1.3.6.1.4.1.31496.10.40.4.0
```

Getting the current config hash:

```
snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1
    1.3.6.1.4.1.31496.10.40.5.0
```

Restarting the device:

```
snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1
    1.3.6.1.4.1.31496.10.40.10.0 i 1
```

Running a configuration update:

```
snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1
    1.3.6.1.4.1.31496.10.40.11.0 s "http://server/directory"
```

You can use TFTP, HTTP, HTTPS and FTP URLs (specifying a username/password or a port is not yet supported).
Please note that config updates expect a zip-file named `<serial-number>.zip` in the specified directory.

Getting the configuration update status:

```
snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1
    1.3.6.1.4.1.31496.10.40.12.0
```

The return value can be one of: `succeeded (1)`, `failed (2)`, `inprogress (3)`, `notstarted (4)`.

Running a 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"
```

Getting the software update status:

```
snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1
    1.3.6.1.4.1.31496.10.40.14.0
```

The return value can be one of: `succeeded (1)`, `failed (2)`, `inprogress (3)`, `notstarted (4)`.

Setting the update operation:

```
snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1
    1.3.6.1.4.1.31496.10.40.15.0 i 1
```

By default, the update operation is set to `update` (0) which results in an immediate update of software or configuration once triggered. One may also set the operation to `store` (1) which will only store the software or configuration package. It can be later activated using the following switch operators.

Switching to alternative software:

```
snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1
    1.3.6.1.4.1.31496.10.40.16.0 i 0
```

The return value can be derived from the software update status.

Switching to alternative config:

```
snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1
    1.3.6.1.4.1.31496.10.40.16.0 i 1
```

The return value can be derived from the config update status.

Getting the alternative config description:

```
snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1
    1.3.6.1.4.1.31496.10.40.17.0
```

Getting the alternative config hash:

```
snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1
    1.3.6.1.4.1.31496.10.40.18.0
```

Getting the alternative software version:

```
snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1
    1.3.6.1.4.1.31496.10.40.19.0
```

Getting the alternative software hash:

```
snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1
    1.3.6.1.4.1.31496.10.40.20.0
```

Setting digital OUT1:

```
snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1
    .1.3.6.1.4.1.31496.10.53.10.0 i 0
snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1
    .1.3.6.1.4.1.31496.10.53.10.0 i 1
```

Setting digital OUT2:

```
snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1
    .1.3.6.1.4.1.31496.10.53.11.0 i 0
snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1
    .1.3.6.1.4.1.31496.10.53.11.0 i 1
```

Listing discovered devices:

```
snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1
    .1.0.8802.1.1
```

5.7.11. Let's Encrypt

This service allows you to automatically issue TLS certificates for the web interface of the router using the PKI provided by Let's Encrypt. If HTTPS is enabled, the web interface will automatically use the Let's Encrypt certificate, if Let's Encrypt is enabled. Make sure that the following preconditions are met in order to be able to issue and use Let's Encrypt certificates:

- HTTP and HTTPS must be enabled on the web server on the standard ports 80 and 443
- The router must be reachable from the internet using the domain name configured for Let's Encrypt via TCP ports 80 and 443

As soon as the Let's Encrypt component is enabled it automatically starts requesting a certificate for the configured domain. It also checks once a day if the certificate needs to be renewed and requests a new certificate if necessary.

Parameter	Let's Encrypt Settings
Enable	Enables/disables the component
Domain	Domain for which to request a certificate
Certificate state	Indicates if the certificate is installed or missing or if it is currently beeing issued
Certificate valid not before	Time at which the validity of the installed certificate started
Certificate valid not after	Time at which the validity of the installed certificate ends
Renew Certificate	Allows to manually request renewal of the certificate. Note that this only works if renewal is due.
Delete Certificate	Deletes the installed certificate. This is only available if Let's Encrypt is disabled.

For debugging you can use the tail-scripts command in the CLI which shows the log of the ACME client which requests the certificates. Or you also find the log of the last certificate request in the following file:

/etc/acme/<DOMAIN>/issue.log

5.7.12. 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 5.8.8.

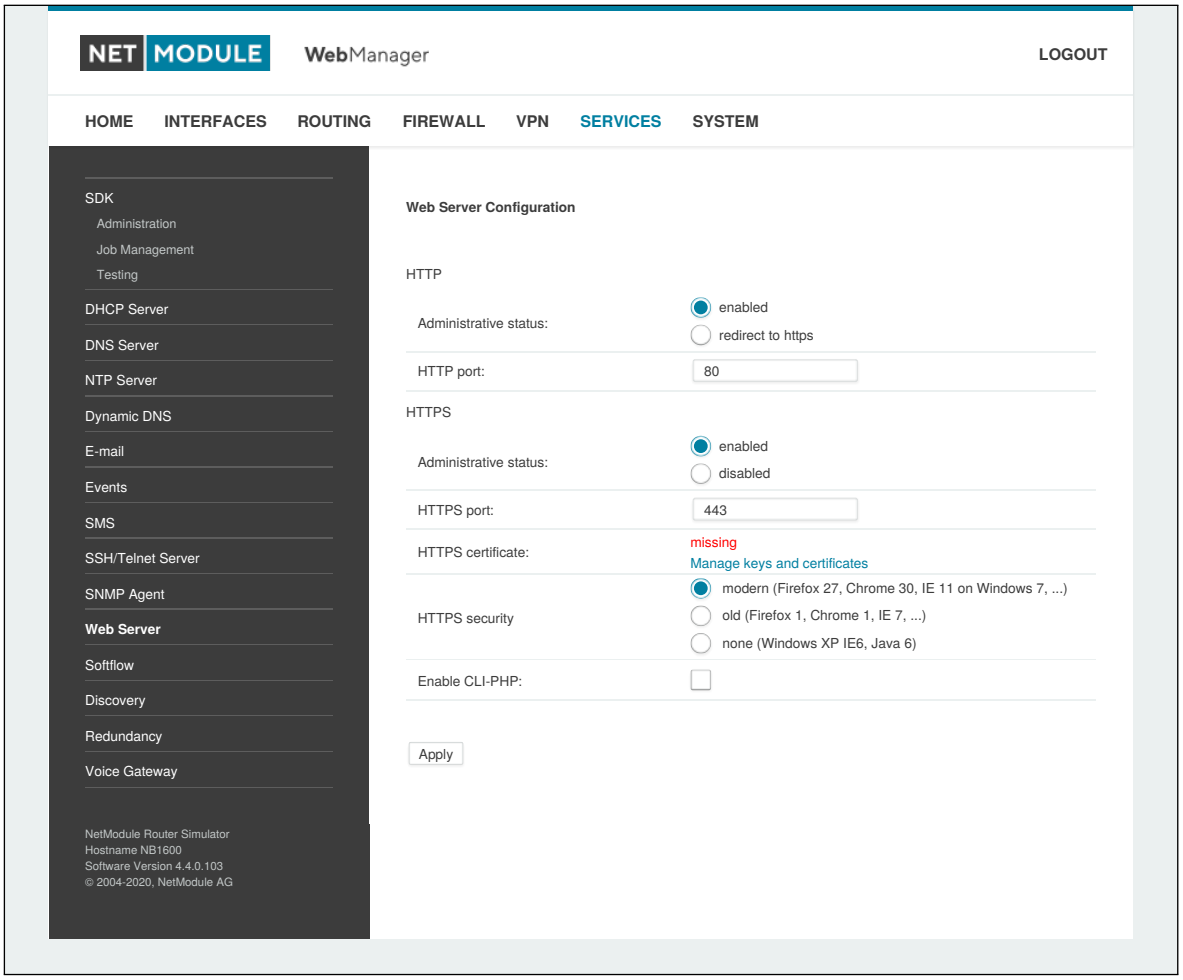


Figure 5.52.: Web Server

Parameter	Web Server Settings
Administrative Status	Enable or disable the Web server
HTTP port	Web server port for HTTP connections
HTTPS port	Web server port for HTTPS connections
Enable CLI-PHP	Enable CLI-PHP service (see chapter 6.17)

5.7.13. MQTT Broker

The MQTT Broker can be used to distribute MQTT messages between MQTT clients. Please set up appropriate firewall rules if you want to restrict access to the MQTT Broker.
Keys and certificates for TLS encryption are managed via Keys & Certificates (see chapter 5.8.8).
The MQTT Broker service can receive the following parameters:

Parameter	MQTT Broker Settings
Administrative Status	Enable or disable Service
Port	Specifies the network port to listen on
TLS Encryption	Enables or disables TLS encryption for the service

5.7.14. Softflow

This page can be used to configure the network traffic analyser daemon softflowd used for exporting NetFlow traffic data.

Parameter	Softflow Settings
Interface	Interface on which to listen for traffic
Host Address	Destination address of the traffic data
Port	Port of the destination address
Protocol Version	Protocol version of the data
Maximum Flows	The maximum number of flows to concurrently track
Track Level	Flow elements that should be used to define a flow
Sample Rate	Periodical sampling rate

5.7.15. Discovery

This page can be used to enabled discovery protocols which can be used to discover and to get discovered by other hosts.

Parameter	Discovery Configuration
Administrative status	Administrative status
Enabled protocols	List of enabled discovery protocols

The following protocols are supported:

Parameter	Discovery Configuration
LLDP	Link Layer Discovery Protocol
CDP	Cisco Discovery Protocol
FDP	Foundry Discovery Protocol
SONMP	Nortel Discovery Protocol
EDP	Extreme Discovery Protocol
IRDP	ICMP Router Discovery Protocol

IRDP implements RFC1256 and can also inform locally connected hosts about the nexthop gateway. Any discovered hosts will be exposed to the LLDP-MIB and can be queried over SNMP or CLI/GUI.

5.7.16. Redundancy

This page can be used to set up a redundant pair of NetModule routers (or other systems) by running the Virtual Router Redundancy Protocol (VRRP) between 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 not reachable anymore (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.

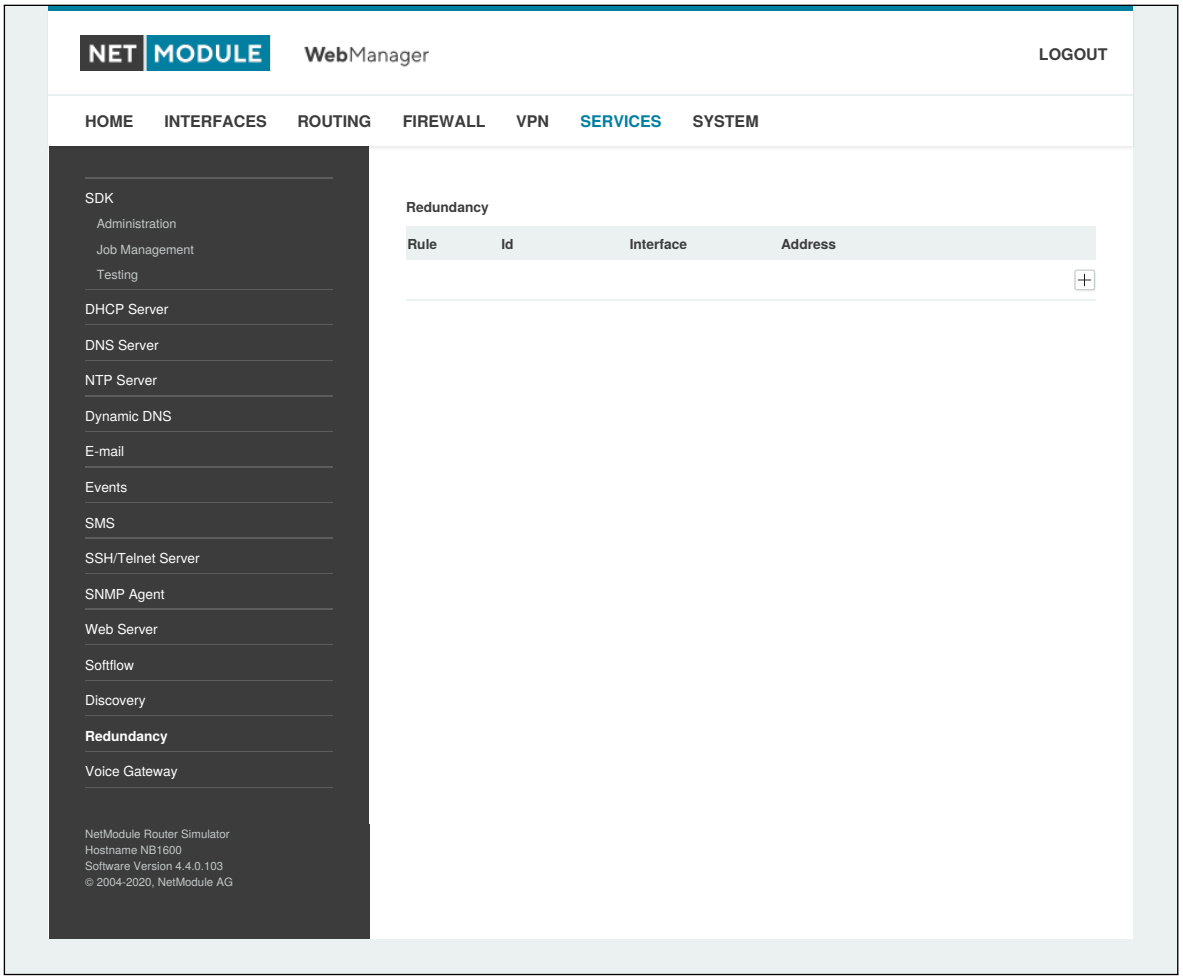


Figure 5.53.: VRRP Configuration

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 across both routers in order to prevent any lease duplication.

Parameter	Redundancy Configuration
Administrative status	Administrative status

Parameter	Redundancy Configuration
Role	The 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	The virtual gateway address formed by the participating hosts

We assign a priority of `100` to the master and `1` to the backup router. Please adapt the priority of your third-party device appropriately.

5.7.17. ITxPT

This is an integration of the ITxPT standard v2.0.1. (see ITxPT Onboard Architecture Specifications v2.0.1)

Configuration

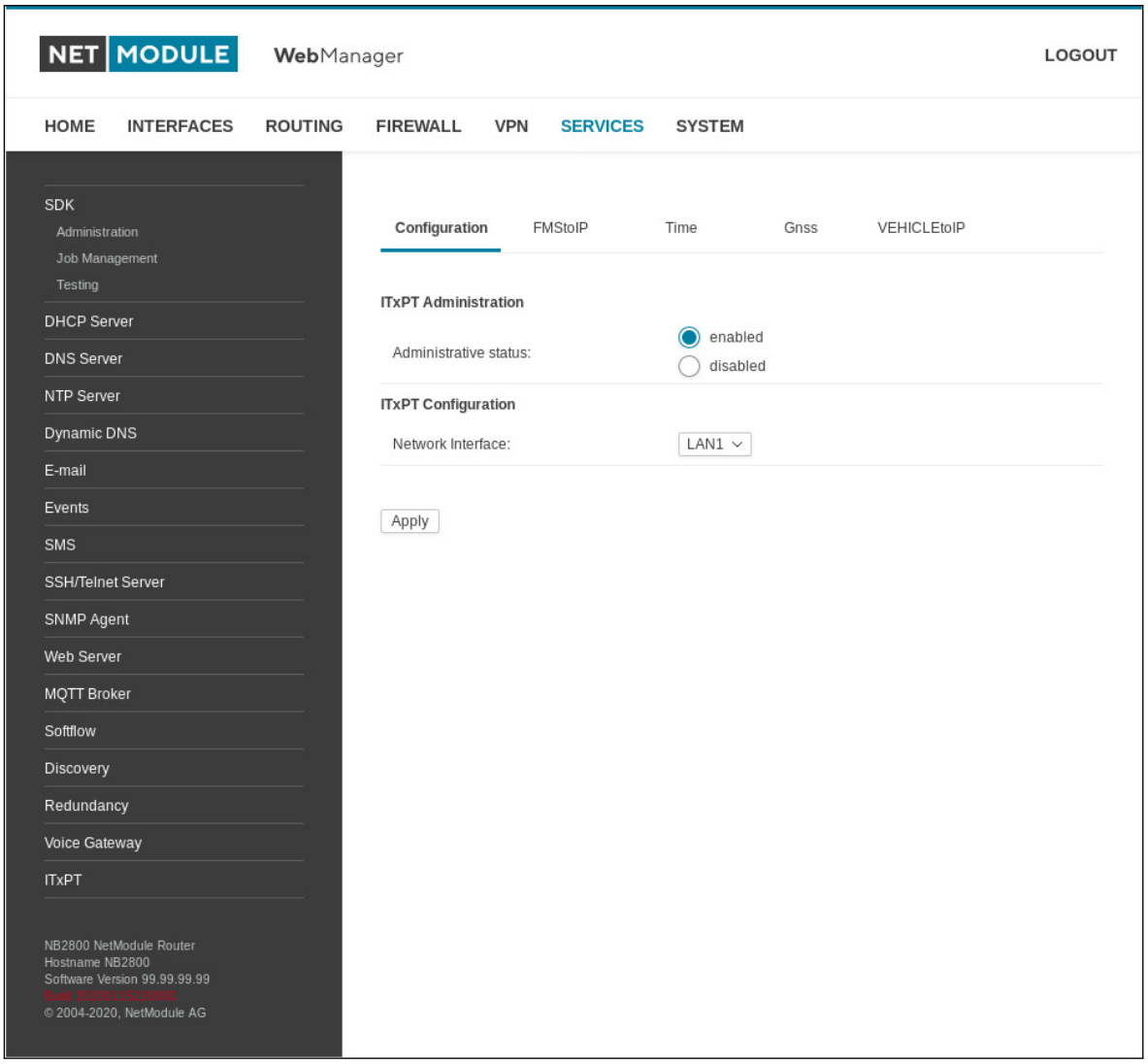


Figure 5.54.: ITxPT configuration

The following parameters can be used to set it up:

Parameter	ITxPT Administration
Administrative status	Specifies whether the ITxPT functionality should be enabled or disabled.
Network Interface	Specifies the network interface on which the Service should operate on.

Parameter	ITxPT Administration
Multicast TTL	Multicast routing (used by ITxPT Service) can be configured here and is managed by a daemon. The smc routing daemon can be configured to be available on multiple network interfaces and provides the ability to limit or extend the hop limit of the ITxPT service that traverses routers. In IPv4 multicasting, routers have a TTL threshold assigned to each interface. Only multicast packets with a TTL greater than the threshold of the interface are forwarded. Multicast TTL can be set to any value ranging from 0 to 255. The default setting is 0.
Enable mDNS reflector	Reflect incoming mDNS (used bx ITxPT Service) requests to all network interfaces across routed networks, should be enabled or disabled. Keep in mind that doing this will also mean that any device in your untrusted networks will be able to send mDNS requests into your trusted networks.
Time	Specifies whether the ITxPT Service Time should be enabled or disabled.
GNSS	Specifies whether the ITxPT Service GNSS should be enabled or disabled.
MQTT	Specifies whether the ITxPT Service MQTT should be enabled or disabled.

FMS to IP

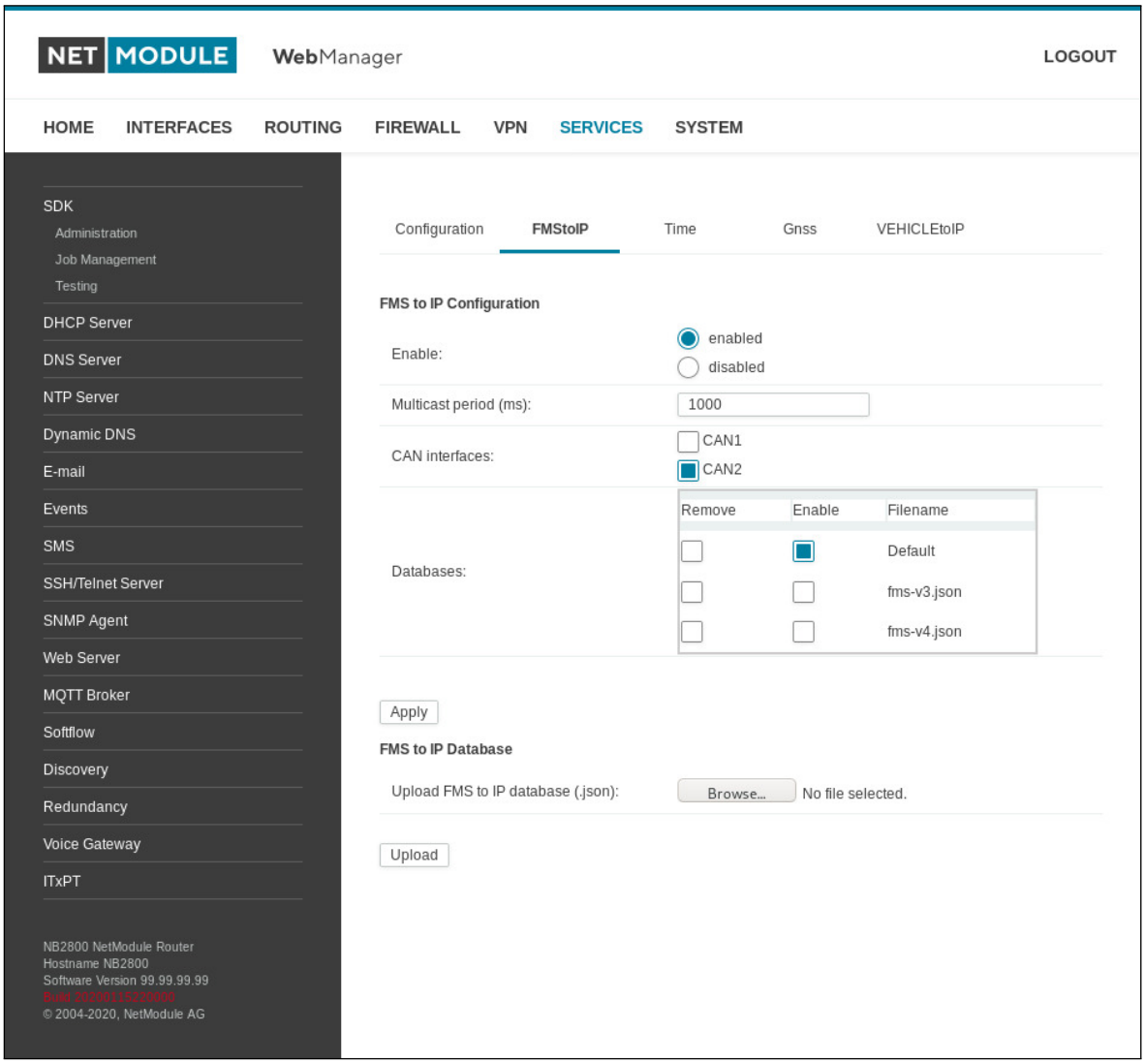


Figure 5.55.: ITxPT FMStoIP

On this page you can configure the FMS to IP functionality.

Parameter	FMS to IP options
Enable	Specifies whether the FMS to IP functionality should be enabled or disabled.
Multicast period	How frequent the FMS to IP multicast is sent. Set to zero to redirect incoming can messages immediately.
CAN interfaces	Select the can interfaces that should be processed (multiple selection).
Databases	Select the FMS to IP databases used to process the can-data (multiple selection).

FMS to IP database format

The json file format is used. The database file describes the incoming data-packages. There are two basic components to describe any signal used in the FMS standard. The Parameter Group Number (PGN) and the Suspect Parameter Number (SPN). The PGN contains of one or more signals. The SPN is used to give an unique identifier to a signal. More information can be found in SAE-J1939 standard.

```
[
  {
    "name" : "EBFF",
    "pgn" : 60415,
    "length" : 8,
    "spns" : []
  },
  {
    "name" : "CCVS",
    "pgn" : 65265,
    "length" : 8,
    "spns" :
    [
      {
        "byteSize" : 2,
        "offset" : 1,
        "formatGain" : 0.00390625,
        "formatOffset" : 0,
        "units" : "km/h",
        "name" : "Wheel Speed",
        "number" : 84,
        "type" : 0
      },
      {
        "bitSize" : 2,
        "bitOffset" : 4,
        "offset" : 3,
        "descriptions" :
        [
          "Pedal released",
          "Pedal depressed"
        ],
        "name" : "Brake Switch",
        "number" : 597,
        "type" : 1
      }
    ]
  }
]
```

The top level structure is an array. It contains PGN objects that define a PGN with the following types:

PGN Definition

Parameter	PGN definition
name	Name of the pgn.
pgn	The PGN number in decimal.
length	Length of the can message.
spns	Array containing SPN-objects.

The "spns" array can be left empty, if no decodeing is required.

SPN Definition

The SPN are divided into three types: nummerical, status and string.

Parameter	Nummerical SPN
byteSize	Size of the data in bytes.
offset	The offset in the can-data.
formatGain	The numerical factor used to give the value.
formatOffset	The numerical offset of the value.
units	The physical unit of the value.
name	Name of the SPN.
number	The SPN number.
type	0 -> Nummerical SPN.

Parameter	Status SPN
bitSize	Size of the data in bits.
bitOffset	The offset in bits in the byte.
offset	The offset in bytes.
descriptions	Array containing the status description.
name	Name of the SPN.
number	The SPN number.
type	1 -> Status SPN.

Parameter	String SPN
name	Name of the SPN.
number	The SPN number.
type	2 -> String SPN.

ITxPT GNSS

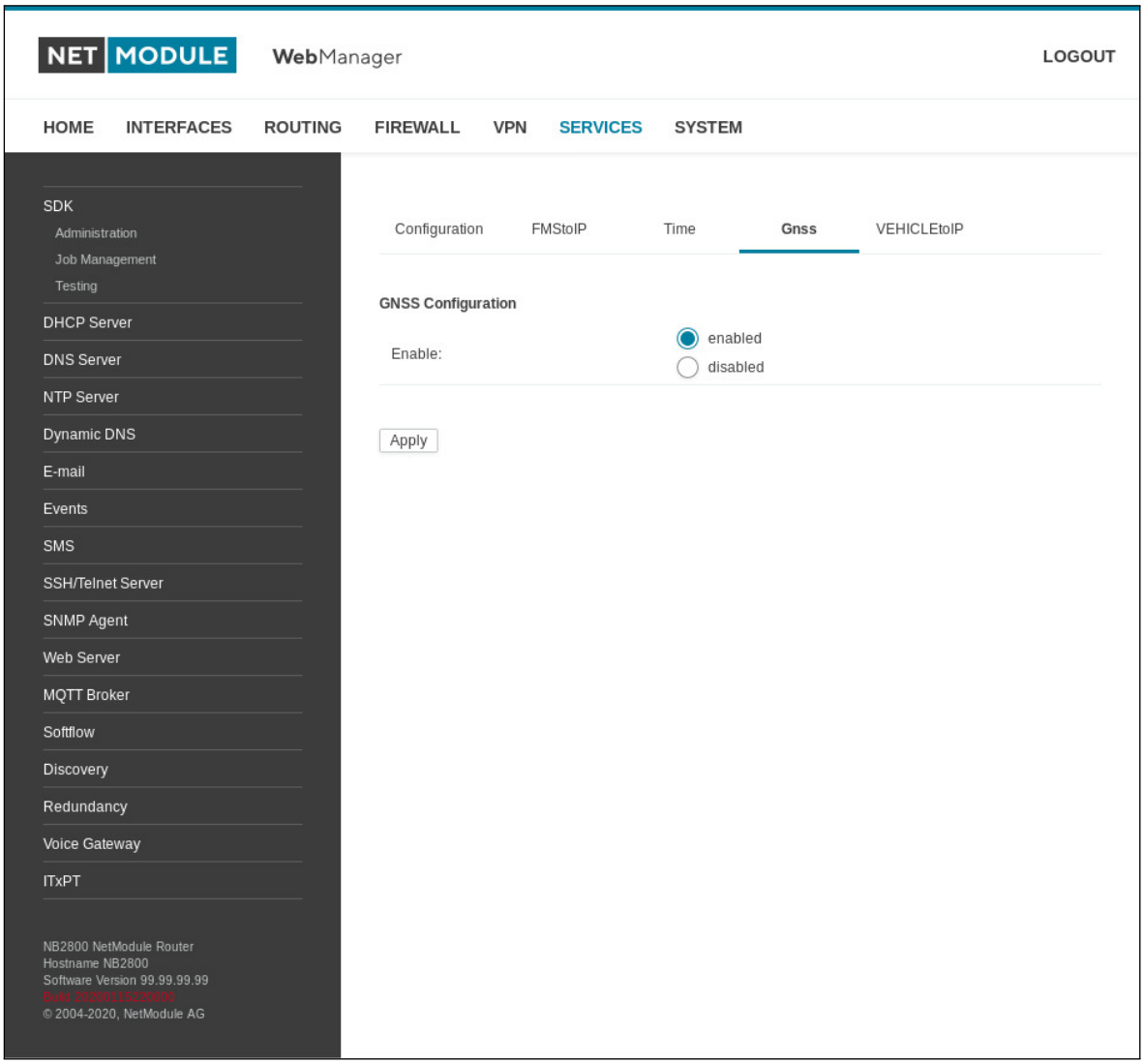


Figure 5.56.: ITxPT GNSS

Parameter	ITxPT GNSS
Enable	Specifies whether the ITxPT GNSS should be enabled or disabled.

ITxPT Time

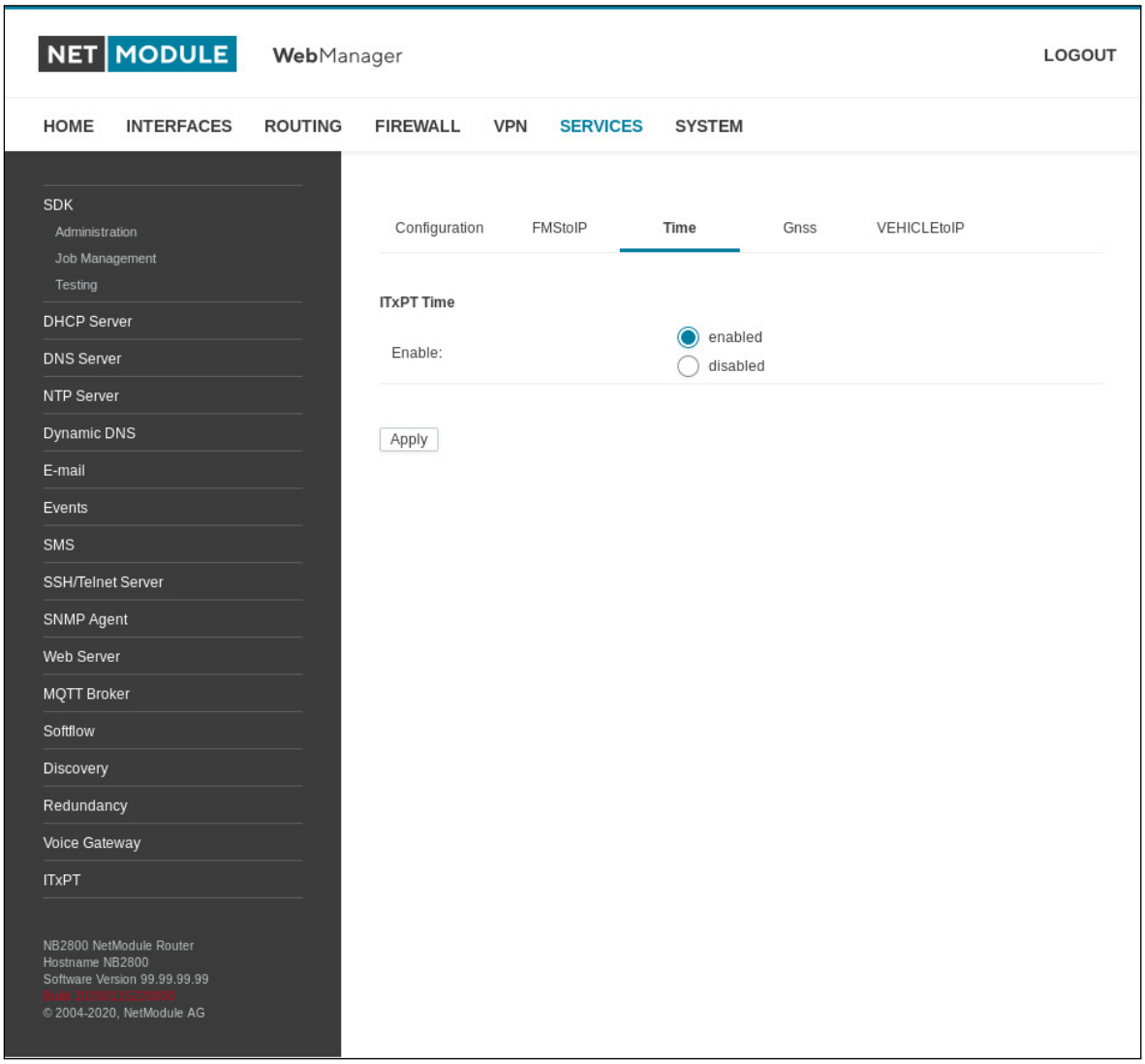


Figure 5.57.: ITxPT Time

Parameter	ITxPT Time
Enable	Specifies whether the ITxPT Time should be enabled or disabled.

VEHICLE to IP

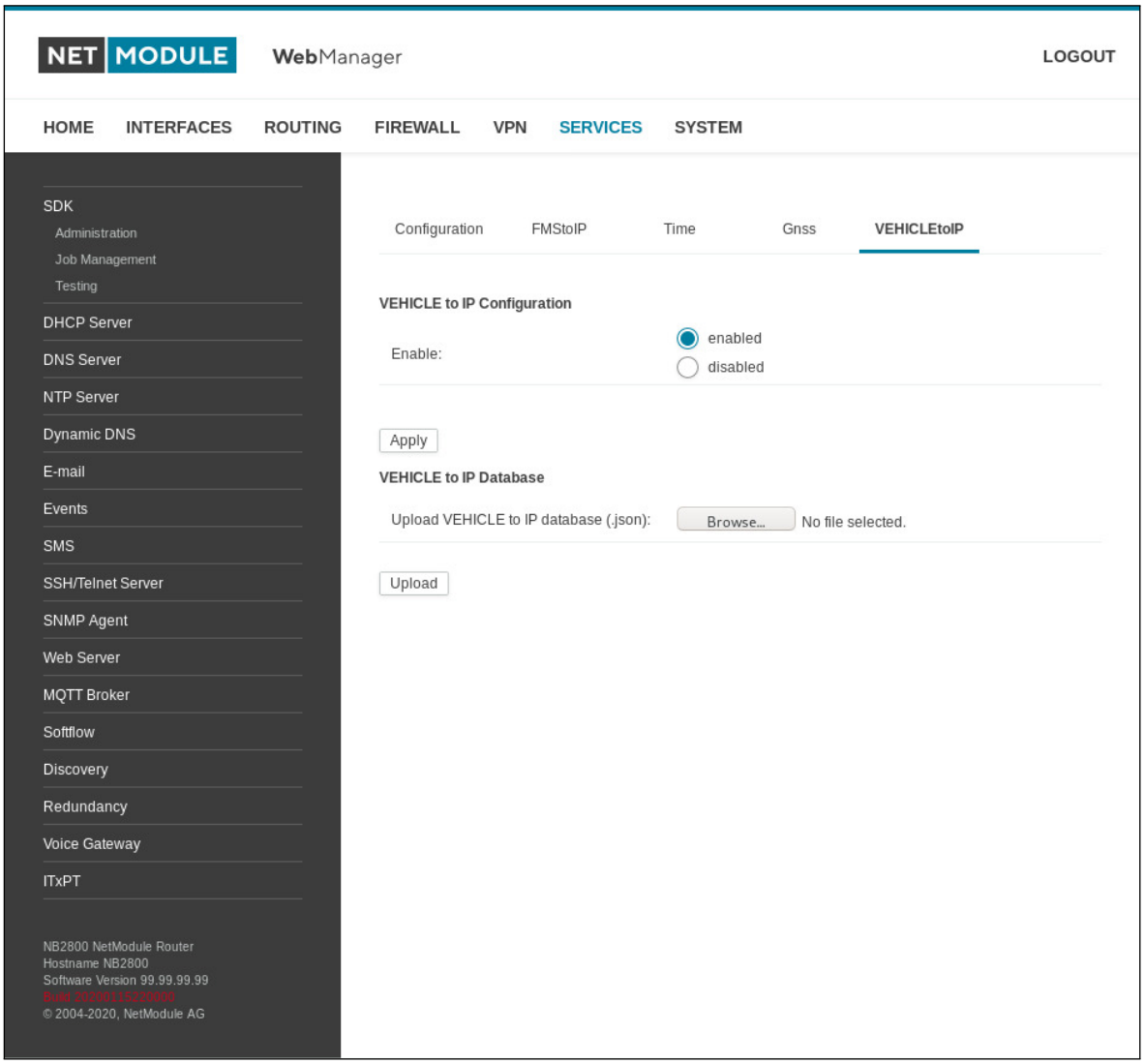


Figure 5.58.: ITxPT VEHICLEtoIP

Parameter	ITxPT VEHICLEtoIP
Enable	Specifies whether the ITxPT VEHICLEtoIP should be enabled or disabled. A VEHICLEtoIP database is necessary to enable this service.

5.7.18. Voice Gateway

Depending on your hardware, you can set up a voice gateway on the router which can be used to connect mobile calls to VoIP clients and vice versa.

Administration

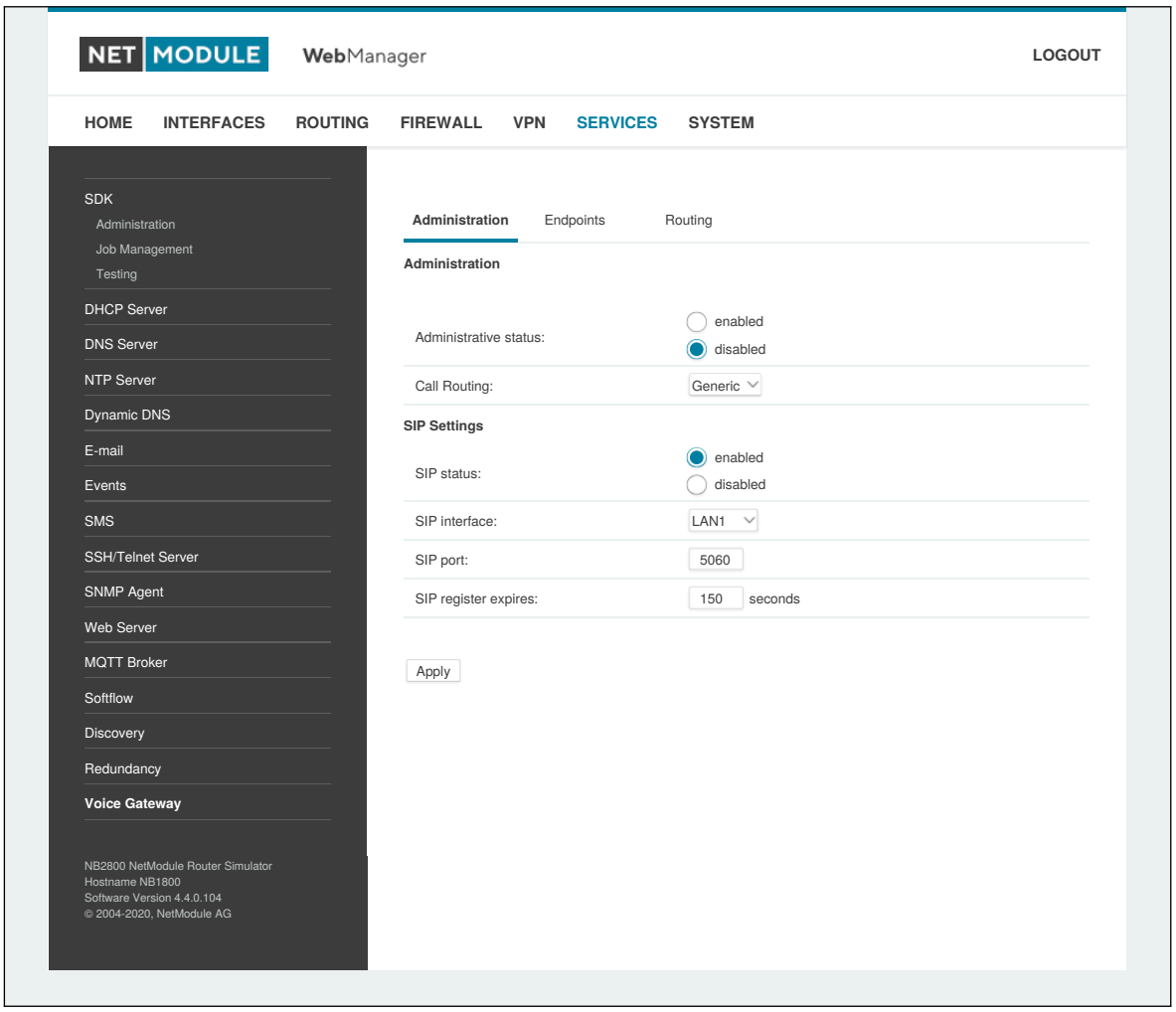


Figure 5.59.: Voice Gateway Administration

The following parameters can be used to set it up:

Parameter	Voice Gateway Administration Settings
Administrative status	Specifies whether the gateway shall be enabled or disabled
Call routing	Defines who will be responsible for call routing. If SDK has been specified you would need to install a script (see examples) which will be responsible for routing and accepting the calls. Otherwise the static routing configuration will be used.
SIP status	Specifies whether the SIP agent will be enabled or disabled

Parameter	Voice Gateway Administration Settings
SIP interface	Specifies the interface (LAN or WAN) on which the agent should listen for incoming calls
SIP port	Specifies the agent's listening port
SIP register expires	Specifies the registration interval in seconds

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

Voice Endpoints

On this page you can activate the endpoints used for voice communication, the following types are supported:

Parameter	Voice Gateway Endpoint Types
Voice-Over-Mobile	Endpoint for GSM/UMTS/LTE calls (can be used for calls to mobile or landline phones)
SIP (registrar)	SIP endpoint which can be a client registered to our registrar
SIP (direct)	Endpoint for calls directly routed to a SIP agent without registration
SIP (user-agent)	Endpoint acting as SIP user agent towards a remote registrar

Based on your equipment, we recommend to adjust the modem's audio profile for a better sound experience. The following profiles are available:

Parameter	Voice-Over-Mobile Audio Profiles
Handset	Provides a mild echo, short delay (less than 16-ms dispersion). This mode is intended for use with a well-designed handset, where the Echo Return Loss (ERL) is generally high. Full-duplex performance is easiest to achieve in this mode.
Headset	Provides a moderate echo, short delay (less than 16-ms dispersion). This mode is intended for use in situations where the echo may be loud but low in delay. There are a variety of different headsets available with a wide variety of echo characteristics and noise pickup. Although the echo delay is typically short (< 16 ms) with all headsets, the echo return loss characteristics can vary significantly and are not well known a priori to the handset designer. This mode is more robust and more aggressive at echo cancellation.

Parameter	Voice-Over-Mobile Audio Profiles
Speakerphone	Handle situations of loud echo with extreme acoustic distortion. This mode is intended for use with a car kit or speakerphone applications with high volume and high distortion. Acoustic echo in this situation has negative ERL and is impossible to cancel completely. It operates in a half-duplex manner and will be very aggressive in muting the entire signal to prevent any echo blips from being heard.
Bluetooth	Provides moderate echo, long delay (up to 64-ms dispersion). This mode is intended for bluetooth headsets and carkits which may have DSP processing on board and could give added delay to the system.

Parameter	Endpoint Settings Voice-Over-Mobile
Modem	Specifies the modem which will be used for voice-over-mobile calls
Audio profile	Specifies the modem's audio profile
Volume level	Specifies the modem's volume level - 1 = low

Parameter	Endpoint Settings SIP (registrar)
Subscriber	The subscriber name for a registering SIP client
Username	The username for a registering SIP client
Password	The password for a registering SIP client

Parameter	Endpoint Settings SIP (direct)
Subscriber	The subscriber name of the SIP agent
Host	The IP address of the SIP agent
Port	The port of the SIP agent
Username	The username to authenticate at the SIP agent
Password	The password used for autentication

Parameter	Endpoint Settings SIP (user-agent)
Host	The IP address of the remote SIP registrar
Port	The port of the registrar
Domain	The domain name used at the registrar
Subscriber	The subscriber name used at the registrar
Username	The username to authenticate at the registrar
Password	The password used for autentication

Parameter	Endpoint Settings SIP (user-agent)
Register	Selects whether the user-agent shall register at the registrar
Expires	The expiry time in seconds after registration will be triggered again

Voice Routing

This page can be used to configure generic voice routing between the endpoints.

Enhanced routing facilities are provided via the SDK interface which is able to dispatch voice calls based on their attributes (such as phone number) and other system related status information (e.g. number/duration of calls per endpoint, registration status and so on). Using the SDK, you can also initiate or accept a call, adjust its volume level or do a hangup

Anyway, for simple scenarios the generic method should be sufficient and can be configured as follows:

Parameter	Voice Gateway Routing Settings
Source	Specifies the source endpoint (i.e. where the call comes in)
Mode	The type of action which shall be applied for the call: DROP will silently hangup the call, ROUTE will route the call to the specified endpoint.
Destination	Specfies the target endpoint (i.e. where to call is routed to)

Client Configuration

Any SIP client must be configured to use the router as its registrar/proxy.

Parameter	X-Lite Configuration
User ID	SIP username used in from headers (i.e. subscriber name)
Domain	SIP Domain used in from headers (optional)
Authorization name	Username used for authentication (i.e. subscriber name)
Password	Password used for authentication
Display name	Name to be displayed on the handset

5.7.19. Access Controller WLAN-AP

This section can be used to configure the Access Controller (AC) for NetModule AP3400 access points devices. The AC is able to generate AP3400 configurations, to push the configuration and to read current status information of AP3400 devices. The AC can manage up to 15 AP3400 devices. It will be distinguished between different device states.

Parameter	AC device states
discovering	The NRSW has a valid configuration for this device but the device was not discovered
discovered	The device was discovered but there is no valid config available
unmanaged	The device was discovered, the NRSW has a valid configuration for the device and is currently pushing the configuration to the device
managed	The NRSW was successfully pushing the configuration to the device and is getting status information
update	The device is running the update process
reset	The device is performing a reset
lost	The communication between the NRSW and managed device was lost e.g. after a reboot of the managed device.

Administration

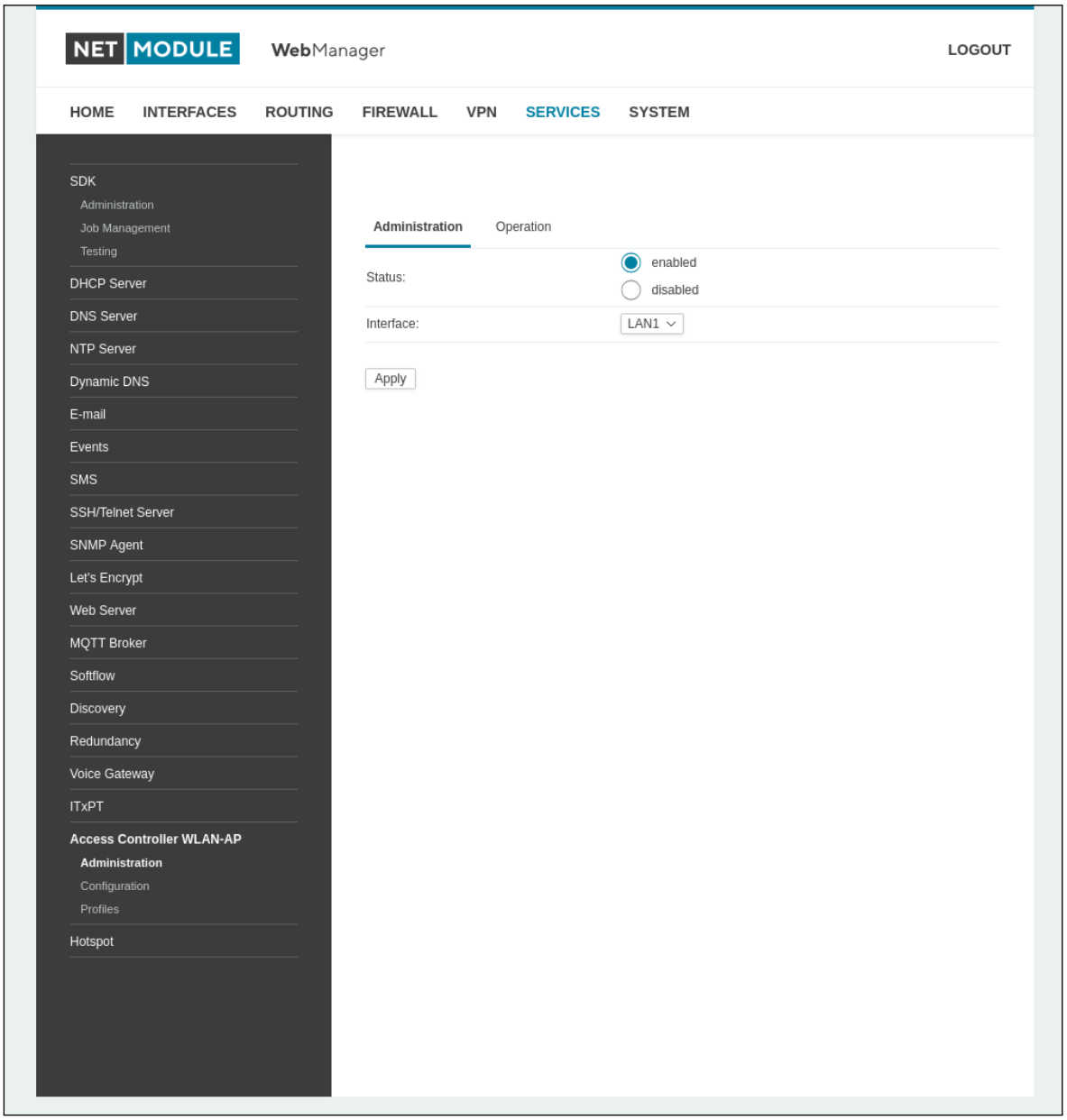


Figure 5.60.: AC WLAN-AP Administration

Parameter	AC administration parameters
Status	Enables or disables the AC functionality
Interface	The interface where the AC is listening

Parameter	AC operation parameters
Operation command	Selects the operation type which shall be performed. For the list of parameters for the 'firmware update' or 'reset' operation see table below
ID	The list of found devices where the AC can operate on.

The selected operation will take place of all selected devices listed under ID. After pressing the apply button the selected operation will be finally performed.

Parameter	AC operation parameters - firmware update
Firmware update	The possibility to load or delete a FW for the NM AP3400 to/from the internal storage of the NM Router.

Parameter	AC operation parameters - reset
Factory reset	Perform a factory reset.
Reboot	Perform a reboot.
Restart network	Restarts the network interfaces.

Configuration

With the configuration page it is possible to configure an AP3400 itself. It is required to have an unique ID for the configuration which is the serial number of the device. The device ID will be shown at the AC status page, and via drop down within the ID field while configuration if the device was discovered.

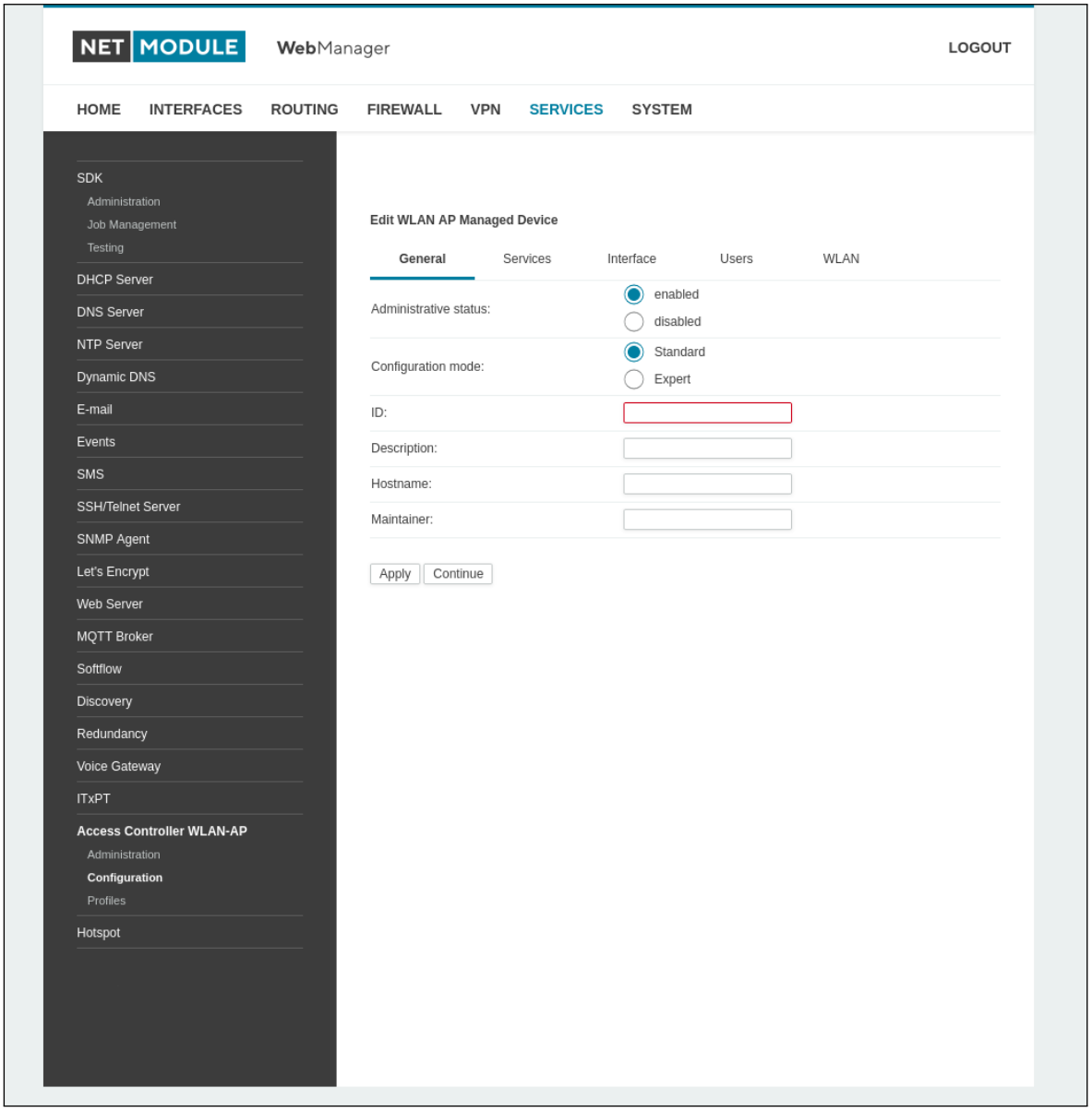


Figure 5.61.: AC WLAN-AP Configuration

Parameter	AC configuration general parameters
Administrative status	When enabled the device specified by the ID will be controlled by the AC.
Configuration mode	The option 'Standard' uses the parameters configured over the GUI. 'Expert mode' opens the possibility to upload an self generated configuration file for the AP3400. The expert mode file has to be comply with the NetModule JSON schema for the configuration. It is possible to download a copy of the current configuration in JSON format by clicking copy while expert mode option is selected.

Parameter	AC configuration general parameters
ID	The unique ID (serial number) of the managed device. All discovered devices which are choosable will be shown by using a double click at this field.
Description	The short description of the managed device
Hostname	The hostname of the managed device
Maintainer	The maintainer of the managed device

Parameter	AC configuration service parameters - HTTP
HTTP status	Enables or disables HTTP for the managed device
HTTP port	The HTTP port for the AP3400

Parameter	AC configuration service parameters - HTTPS
HTTPS status	Enables or disables HTTPS for the managed device
HTTPS port	The HTTPS port for the AP3400
HTTPS certificate	Adds the possibility to generate the certificate for the AP3400

Parameter	AC configuration service parameters - GUI
Status	Enables or disables the GUI functionality

Parameter	AC configuration service parameters - SSH
SSH status	Enables or disables SSH for the managed device
SSH port	The SSH port for the AP3400

Parameter	AC configuration interface parameters
IP mode	Selects the IP mode for the managed device. By using the option 'DHCP IPv4' the managed devices will obtain a IP address from the DHCP server. 'Static' means the AP3400 will use the IP address and netmask given by the parameters below.
Address	The IP address which the AP3400 shall use
Netmask	The netmask which the AP3400 shall use

Parameter	AC configuration user parameters
Username	The username used for the managed device
Password	The password used for the managed device

Parameter	AC configuration WLAN parameters
Administrative status	Enables or disabled the given radio of the AP3400
Operation mode	The operation mode for the seleted radio module of the AP3400. Remark only 'Access Point' mode is currently supported
Country	Select the country the AP operates in
Operation type	Specifies the desired IEEE 802.11 operation mode
Radio band	Selects the radio band to be used for connections, depending on your module it could be 2.4 or 5 GHz
Bandwidth	Specify the channel bandwidth operation mode
Channel	Specifies the channel to be used
Tx power	Specifies the max. transmit power used in dBm.
Profile IDs	The profiles (see section profiles) which the AP3400 should use

Profiles

With the NetModule Access Controller it is possible to configure up to 10 different profiles. With each profile it is possible to configure an independent SSID with encryption and VLAN.

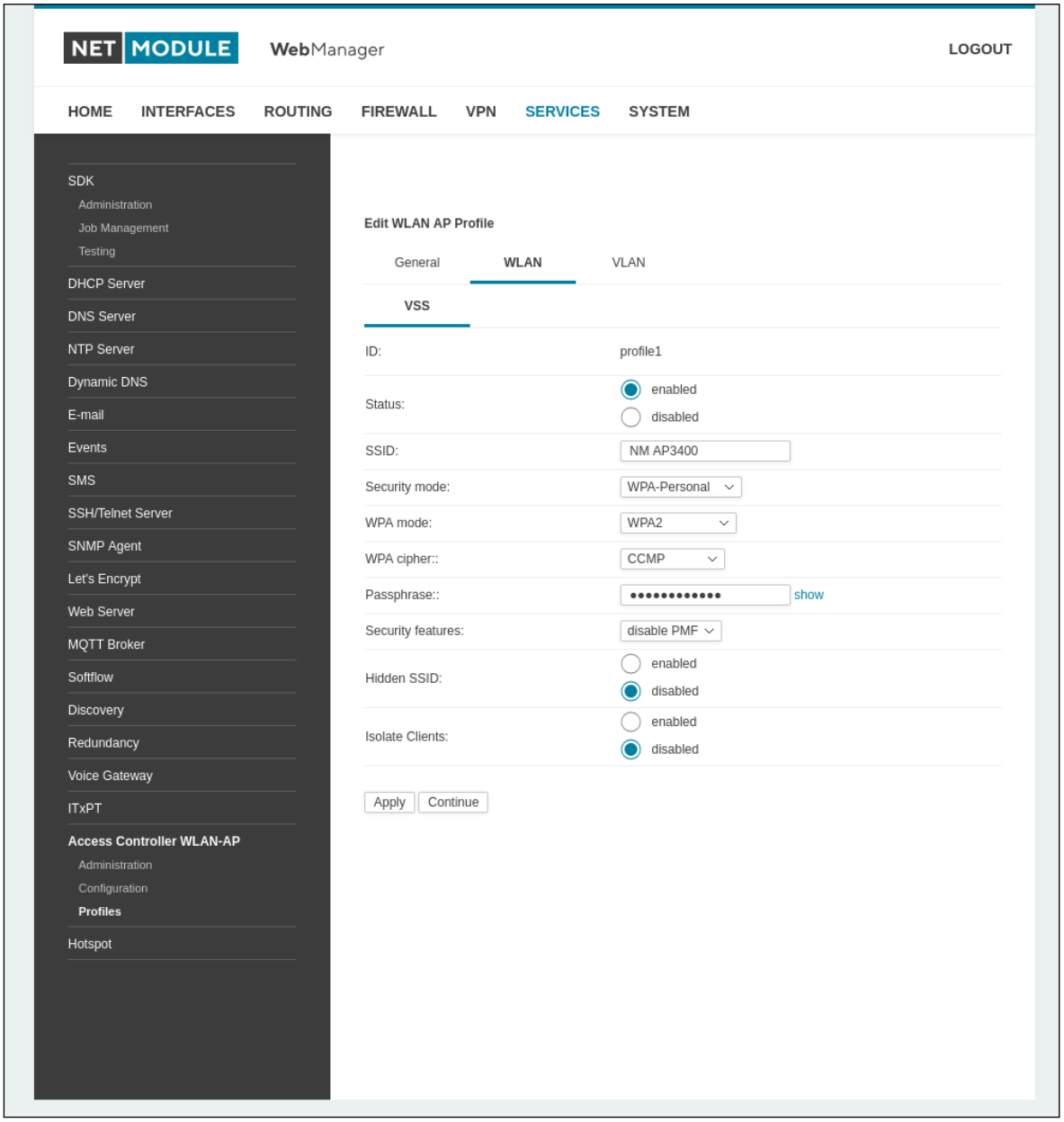


Figure 5.62.: AC WLAN-AP Profiles

Parameter	AC profile general parameters
ID	The unique name for the profile
Description	The description of the profile

Parameter	AC profile WLAN parameters
Status	Enables or disables this profile

Parameter	AC profile WLAN parameters
SSID	The network name (called SSID)
Description	The description of the profile
Security mode	The desired security mode
WPA mode	The desired encryption method. WPA3 should be preferred over WPA2 and WPA1
WPA cipher	The WPA cipher to be used, the default is to run both (TKIP and CCMP)
Passphrase	The passphrase used for authentication with WPA-Personal, otherwise the key passphrase for WPA-EAP-TLS. In case of WPA-Personal: The passphrase must be at least 8 to 63 characters long.
Security features	Enables Protected Management Frames
Hidden SSID	Hides the SSID
Isolate clients	Disables client-to-client communication
RADIUS server	The RADIUS server address
RADIUS secret	The secret used to authenticate against the RADIUS server
Authentication port	The port used for authentication
Accounting port	The port used for accounting messages

Parameter	AC profile VLAN parameters
VLAN ID	The VLAN ID for the profile. If no VLAN ID shall be used with this profile the parameter has to be emtpy

5.8. SYSTEM

5.8.1. System

System Settings

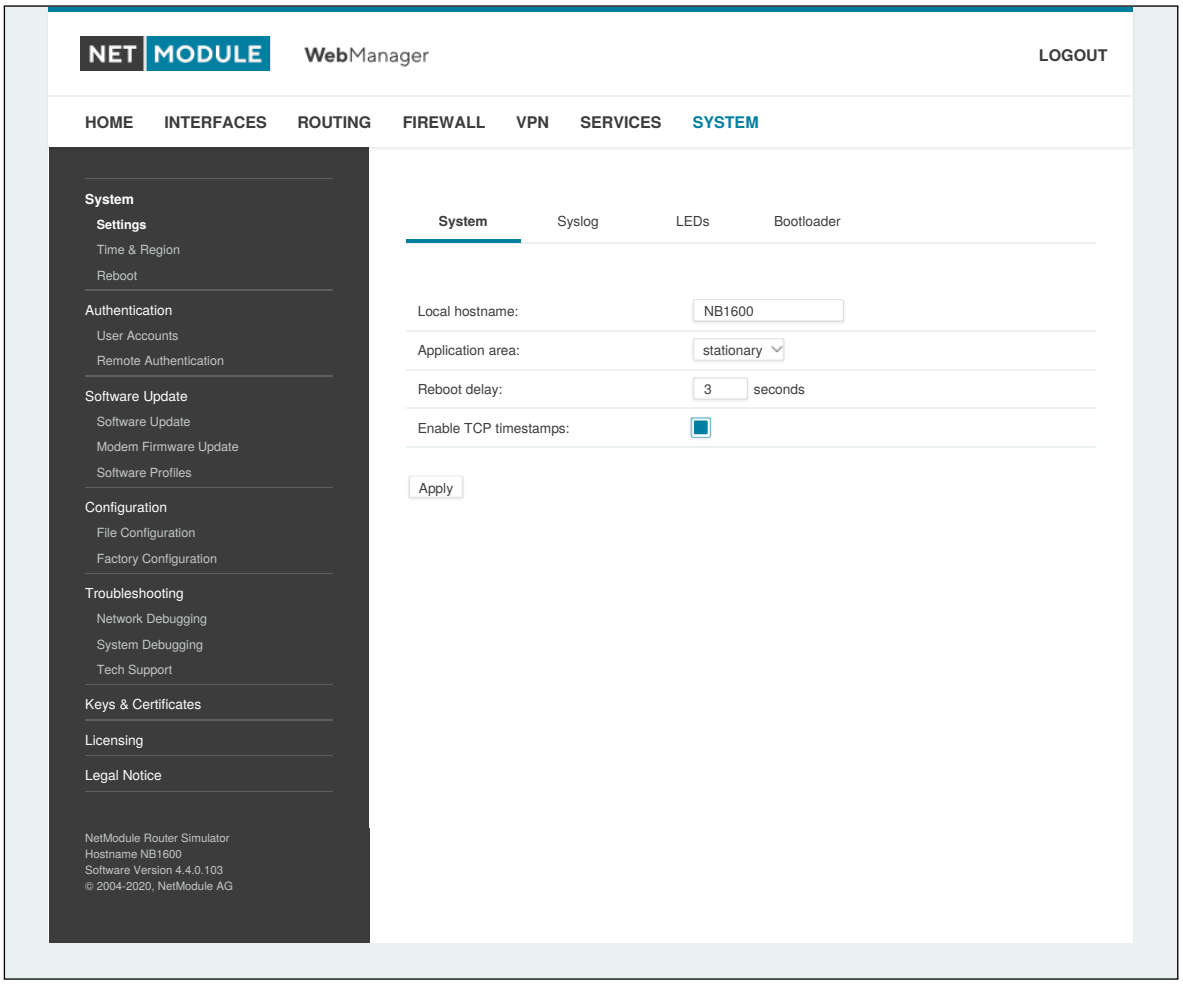


Figure 5.63.: System

System

The following system parameters can be set:

Parameter	System Settings
Local hostname	The hostname of the system
Application area	The desired application area which influences the system behaviour such as registration timeouts or other adaptions when operating in mobile environments.
Reboot delay	The number of seconds which will be waited before regular system reboots (might be needed for `system-rebooting` events)

Parameter	System Settings
Enable TCP timestamps	Enable TCP timestamps for system wide TCP communication. This is needed for Protection Against Wrapped Sequence numbers (PAWS), but with these timestamps enabled a remote attacker can guess the uptime of the system. The uptime is a lower bound for the age of the main system components like the kernel. If the system has an uptime of 3 years it's unlikely that recent security patches were applied.
Show messages and infos on log-in screen	Show error messages and notifications on login screen. If this option is enabled these messages are also shown before logging in with user credentials.

Syslog

The following syslog parameters can be set:

Parameter	Syslog Settings
Storage	The storage device on which log files shall be stored.
Max. filesize	The maximum size of the log files (in kB) until they will get rotated.
Redirect address	Specifies an IP address to which log messages should be redirected to. A tiny system log server for Windows is included in TFTP32 which can be downloaded from our website.

In general, the box comes with an internal flash device which can be used to store data. Depending on your model this can be extended by additional flash or USB disks. The following storage devices exist:

Parameter	Storage Devices
flash root	The root partition of the internal flash
flash data	The data partition of the internal flash
extended disk	An extended storage disk
USB disk	A storage disk connected to the external USB port

LEDs

The following LED parameters can be set:

Parameter	LED Settings
LED	You can customize the behavior of all status LEDs on the front panel of your device. They are usually divided into two banks (top/bottom). You may configure toggle mode, so that the LEDs periodically cycle between two separated configured LED schemes.

Bootloader

The following bootloader parameters can be set:

Parameter	Bootloader Settings
Password	The password used to unlock the bootloader. If empty, the admin password will be used.

Autorun

This feature can be used to automatically launch a shell script or perform a software/config update as soon as an external storage device has been plugged in. For authentication, a file called `autorun.key` must exist in the root directory of a FAT16/32 formatted device. It can be downloaded from that page and holds the SHA256 hash key of the autorun password. The file can hold multiple hashes which will be processed line-by-line during authentication which can be used for setting up more systems with different admin passwords.

For new devices with an empty password the hash key

`e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855`

can be used.

The hash keys can be generated by running the command `echo -n "<password>" | sha256sum` on a Linux system or an Internet hash key generator (search for "sha-256 hash calculator").

Once authentication has succeeded, the system scans for other files in the root directory which can perform the following actions:

1. For running a script: `autorun.sh`
2. For a configuration update: `cfg-<SERIALNO>.zip` (e.g. `cfg-00112B000815.zip`), or if not available `cfg.zip`
3. For a software update: `sw-update.img`

Time & Region

This page can be used for setting the system time and configuring the time zone. You may further enable daylight saving changes for your specific time zone. NetModule routers can synchronize their system time by using one or more servers by the help of the Network Time Protocol (NTP) or via GNSS. If enabled, the time synchronization is usually triggered after a WAN link has come up but before starting any VPN connections. Further time synchronization cycles are scheduled in background.

Most routers don't have a battery backed clock (RTC). In this case the system time is set during boot to the last valide time, e.g. before power off.

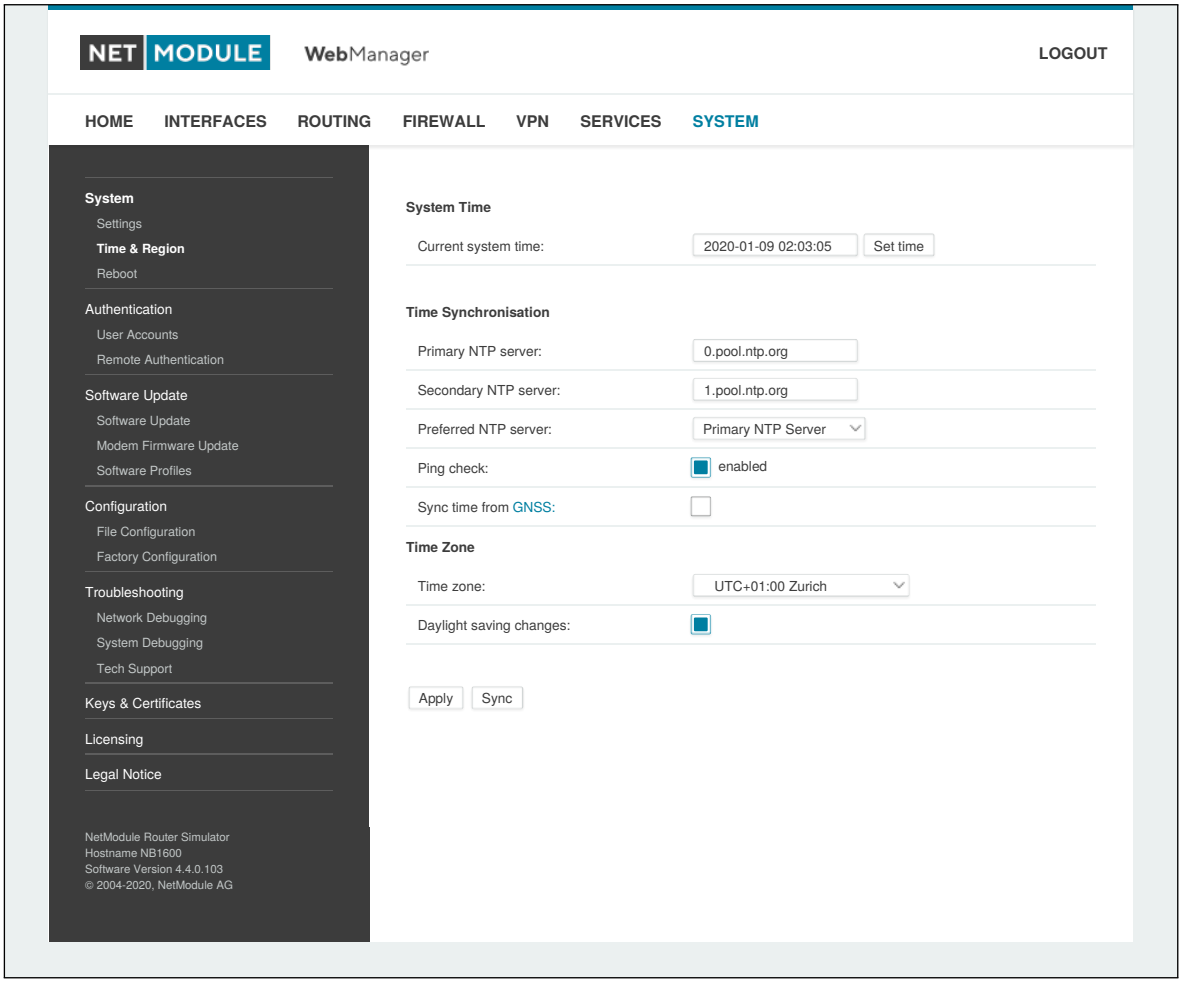


Figure 5.64.: Regional settings

Parameter	Time Synchronisation
NTP server	Address of the primary NTP server
NTP server 2	Optionally, the address of a second NTP server
Ping check	Uses an ICMP ping to check whether NTP servers are available when running initial time update
Sync time from GNSS	Derive time from first GNSS device (if enabled)

Parameter	Time Zone
Time Zone	Set the local time zone.
Daylight saving changes	Enable/disable daylight saving changes.

Virtualization

Virtualization techniques can be used to run multiple isolated guests on top of the host system. The netmodule routers use OS-level virtualization: A system is virtualized at the operating system level,

enabling multiple isolated user-space instances called containers. The same operating system kernel is used to implement the guest environments, applications running in a guest environment view it as a stand-alone system.
General settings:

Parameter	Virtualization Settings
Administrative status	Defines whether virtualization is enabled or not

The following parameters can be used to configure a virtual guest:

Parameter	Guest Settings
Type	Defines which virtualization technique is being used
Description	The description of the guest
Storage	Specifies the storage device on which the root file system of the guest will be located

To Install a root-file-sytem you can set up a URL to load a the image from and trigger the installation:

Parameter	Install
URL	The URL to load the image from. The Image needs to be provided as XZ compressed TAR archive containing the files of a root FS compatible with our CPU architecture (). Different protocols may be used for the transaction like 'http://' or 'https://', 'ftp://' or 'tftp://'. If you uploaded the the image to the router in advance you can also use 'file://' followed by the local path of the file. We can provide various tailored Linux distribution images (such as Debian) on demand.
Install	If this trigger is set the image download will start on apply. Any existing root file system will be overwritten. This parameter will not be stored in the configuration. After the installation was proceeded the value will be reset and needs to be set again if a new image shall be installed.

Communication to and from the guest can be achieved by defining network interfaces which can be either routed towards the guest or bridged with a LAN interface:

Parameter	Guest Networking
Guest interface	The name of the interface inside the guest
Mode	The network mode for this interface (either routed or bridged)
Address	The IP address of the interface inside the guest
Netmask	The netmask of the interface inside the guest
Gateway	The gateway used inside the guest which is also set on the host interface
Bridge interface	The interface to which the guest interace shall be bridged

The guest devices parameter shows a list of devices (e.g bluetooth, CAN) which can be provided to the guest system.

Parameter	Guest Devices
Enable devices	Enable or disable device for the guest

In order to limit the ressources for a guest, the following settings can be applied:

Parameter	Guest Limits
CPU	The number of CPUs used for the guest
Memory	The amount of memory available for the guest

Reboot

This page can be used to set up a periodic automatic reboot but also to trigger a manual reboot which will be issued immediately.

5.8.2. Authentication

User Accounts

By using this page you can manage the user accounts on the system.

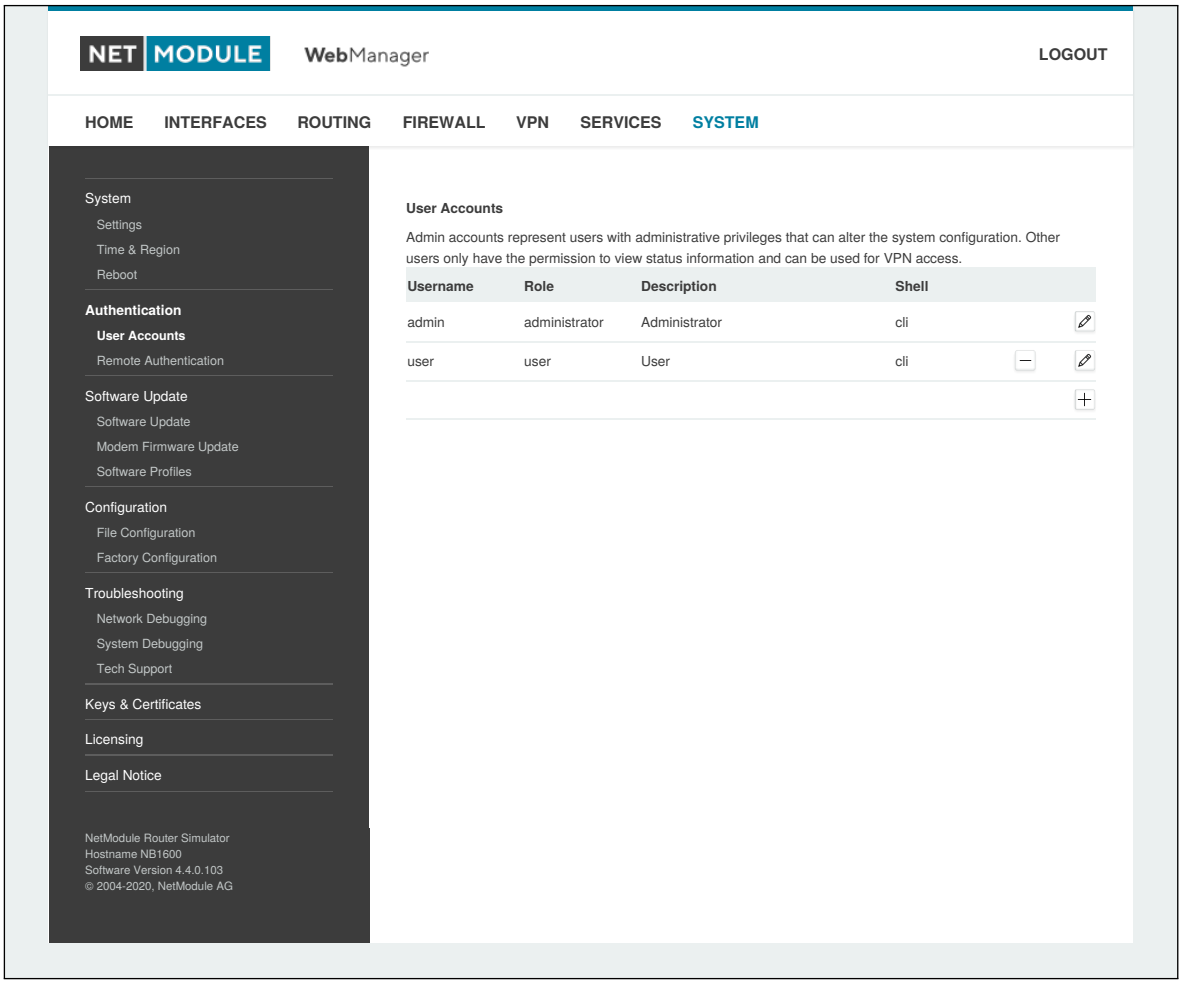


Figure 5.65.: User Accounts

The `admin` user is a built-in power user which represents the default administrator of the system. Please note that the `admin` password will be also applied to the `root` user which is able to enter a system shell. Further admin accounts with administrative privileges can be added, they can also alter the system configuration or perform administrative system tasks. Other users only have the permission to view status information. They can be also used for VPN access.

The Web Manager supports up to 5 concurrent users. Inactive users will be kicked after being idle for 30 minutes. If login was successful, any duplicate users from other remote hosts will be logged out. Remote hosts will be blocked for 5 minutes after 10 failed login attempts.

Parameter	User accounts management
Username	The name of the user
Description	A short description for the user

Parameter	User accounts management
Role	Either admin or user
Shell	Specifies if the user gets the CLI or a SHELL
Store password unencrypted	If this option is selected the user password is stored unencrypted on the device (not recommended)
Old password	The old password of the user
New password	The new password of the user
Confirm new password	The confirmed new password of the user

Please note, when adding additional admin users you are required to provide the password of the default administrator.

Storing Passwords
Normally the password for a user is only stored as a cryptographic hash, which is the recommended way to handle passwords on devices. Unfortunately the SNMP implementation makes it mandatory to store the password on the device unencrypted.
Make sure to grant access rights to your users in a restrictive manner.

Remote Authentication
A RADIUS server can be used for authenticating remote users. This applies for the Web Manager, the WLAN network and other services supporting and incorporating remote authentication.

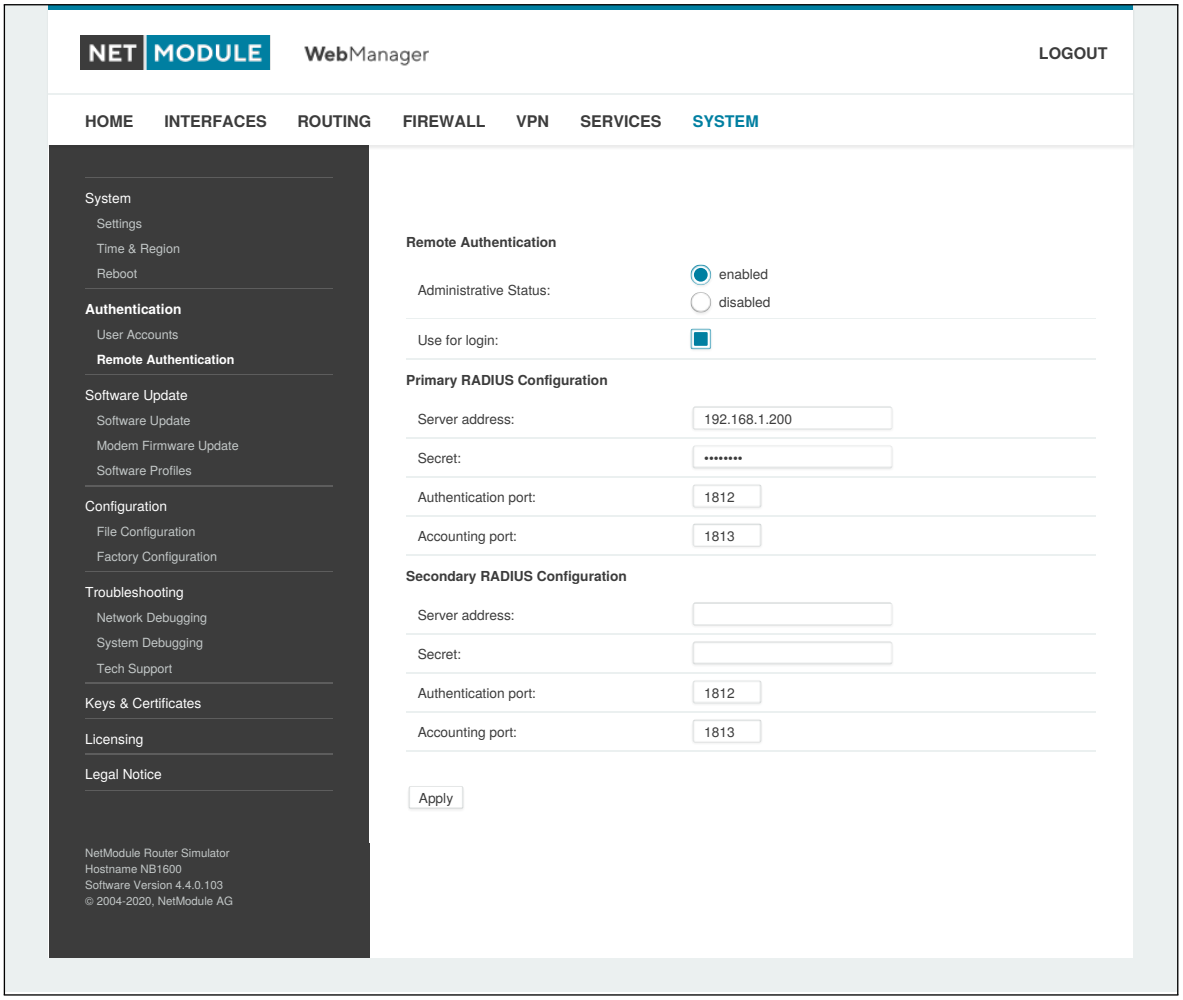


Figure 5.66.: Remote Authentication

It can be configured as follows:

Parameter	Remote authentication settings
Administrative status	Defines whether a remote server should be used for authentication
RADIUS server	The RADIUS server address
RADIUS secret	The secret used to authenticate against the RADIUS server
Authentication port	The port used for authentication
Accounting port	The port used for accounting messages
Use for login	This option enables remotely-defined users to access the Web Manager, otherwise it is only used by services which have explicitly configured it (e.g. WLAN)

5.8.3. Software Update

Manual Software Update

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

Parameter	Manual Software Update
Update operation	The update operation method being used. You can upload the image, download it from an URL or use the latest version from our server
URL	The server URL where the software update image should be downloaded from
Administrator password	Administrator password for downgrade to releases before 4.2.x

Attention

Starting with SW release 4.2 we set default to not saving passwords using password hashes instead. Storing passwords for users can be enabled, but is not recommended for new applications.

Older SW releases require the passwords to be stored encrypted on the device. As we don't have them any more in release version 4.2 and later you will have to provide the administrator password if you want to downgrade to a release 4.1.x and lower. The same passphrase will be used for bootloader login as well.

All users which have no password stored on the device will not be able to login after downgrade until new passwords have been applied.

An Uniform Resource Locator (URL) can have the following format:

```
http://<username>:<password>@<host>:<port>/<path>
https://<username>:<password>@<host>:<port>/<path>
ftp://<username>:<password>@<host>:<port>/<path>
sftp://<username>:<password>@<host>:<port>/<path>
tftp://<host>/<path>
file:///<path>
```

When issuing a software update, the current configuration (including files like keys/certificates) will be backuped. Any other modifications to the filesystem will be erased.

The configuration is generally backward-compatible. We also apply forward compatibility when downgrading to a previous software within the same release line, which is accomplished by sorting out unknown configuration directives which actually may lead to loss of settings and features. Therefore, it's always a good idea to keep a copy of the working configuration.

Attention
In case you perform a major downgrade with a previous release line (e.g. 3.7.0 to 3.6.0), please ensure to always use the latest release of that branch (i.e. 3.6.0.X) as only those tend to be fully forward-compatible. Also keep in mind, that some hardware features may not work (e.g. if not implemented in that version). In doubt, please consult our support team.

A software image can be either uploaded via the Web Manager or retrieved from a specific URL. It will be unpacked and deployed to a spare partition which gets activated if the update completed successfully. The whole procedure is accompanied by all green LEDs flashing up, the subsequent system reboot gets denoted by a slowly blinking Status LED. The backuped configuration will be applied at bootup and the Status LED will blink faster during this operation. Depending on your configuration, this may take a while.

Automatic Software Update
This menu can be used to run a automatic software update of the system.

Parameter	Automatic software update
Status	Enable/disable automatic software update
Time of day	Every day at this time the router will do a check for updates
Operation	Download latest image from the server or specify the URL where the software update package should be downloaded from. Supported protocols are TFTP, HTTP, HTTPS, and FTP. Provide a URL like `protocol://server/path/file`

Remark: SSL certificates of HTTPS URLs will be only verified if a list of CA root certificates are provided under 5.8.8.
After the new software has been installed, the latest running configuration will be applied afterwards during bootup. This is indicated by a faster green blinking of the Status LED.

5.8.4. Module Firmware Update

This menu can be used to perform a firmware update of a specific module.

Parameter	Module Firmware Update
Update operation	The update operation method being used. You can either upload a firmware package or download it from a specifc URL.
Module	The module which shall be updated.
Storage	The temporary storage which shall be used for the update procedure. For boxes with limited amount of flash it is possible to use an USB stick which must be properly set up in the USB section and hold a proper filesystem such as ext4.

Parameter	Module Firmware Update
URL	The server URL where the firmware package should be downloaded from (e.g. `protocol://server/path/file`). Supported protocols are TFTP, HTTP, HTTPS, and FTP. For boxes with limited amount of flash you may also use `usb0:// <path-to-firmware-package>`.

A firmware package (ZIP) usually consists of a flash utility, an info file and the corresponding firmware files. Please follow https://www.netmodule.com/en/support in order to get the latest version.

5.8.5. Software Profiles

The system consists of two root partitions which can hold different software versions and this menu can be used to switch between them. By doing so, you can test a newer software version and simply switch-back if things go wrong.

5.8.6. Configuration

Configuration via the Web Manager becomes tedious for larger volumes of devices. The router 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) in the root directory.

Manual File Configuration

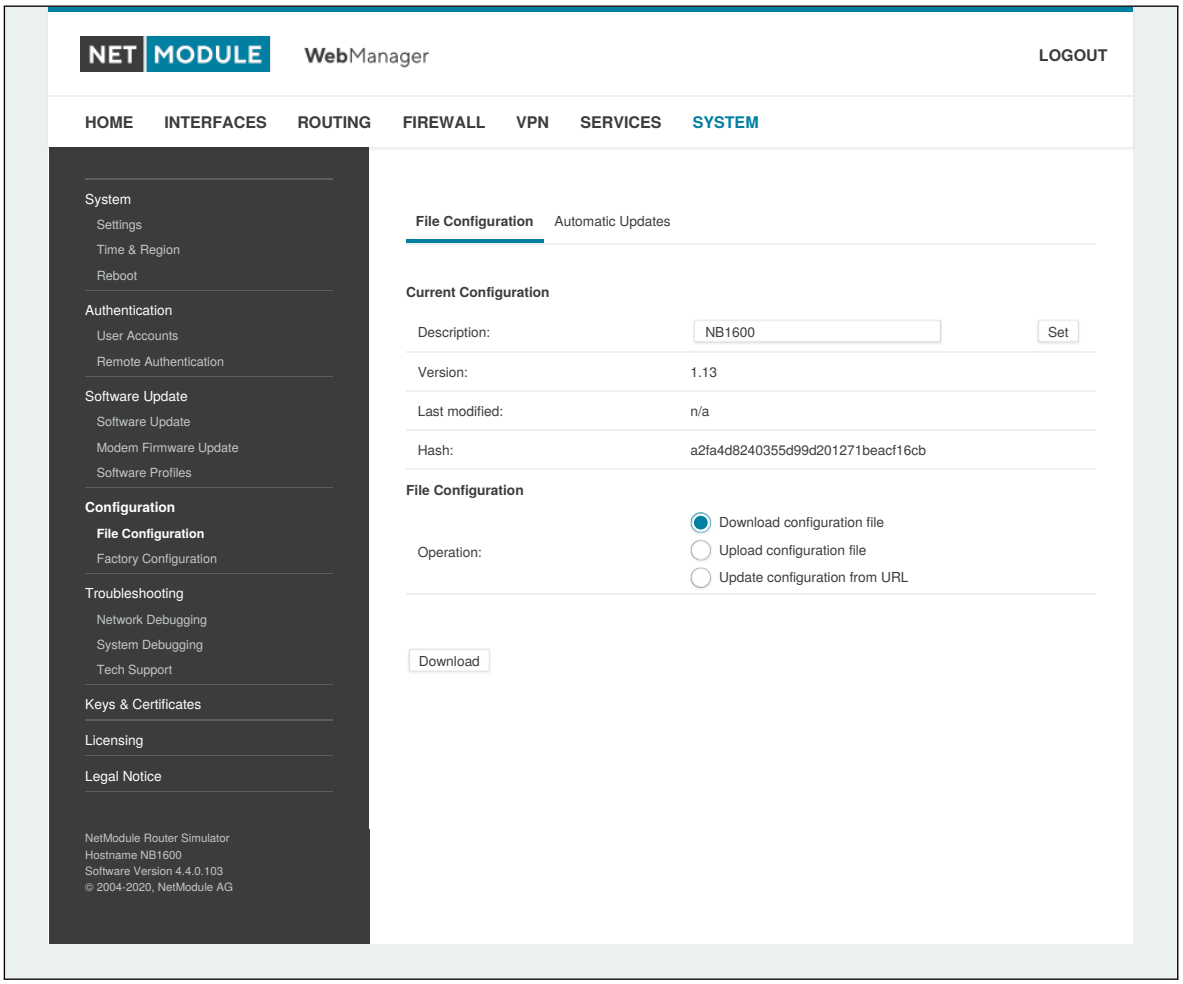


Figure 5.67.: Manual File Configuration

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

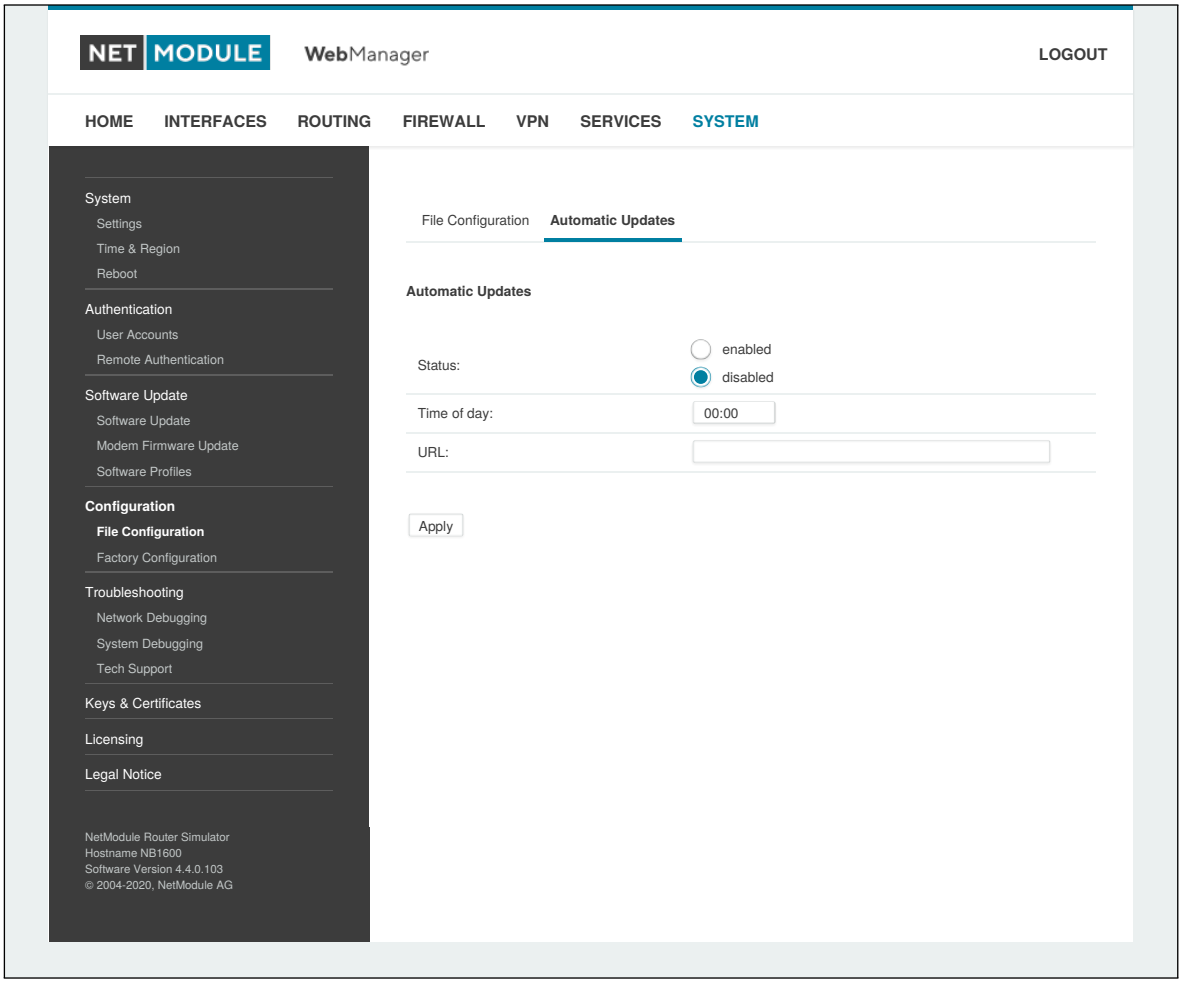


Figure 5.68.: Automatic File Configuration

This menu can be used to run an automatic configuration update of the system. It is configured as follows:

Parameter	Automatic File Configuration
Status	Enable/disable an automatic configuration update
Time of day	Time of day when the system should check for updates
URL	The URL where the configuration file should be retrieved from (supported protocols are HTTP, HTTPS, TFTP, FTP)

Factory Configuration

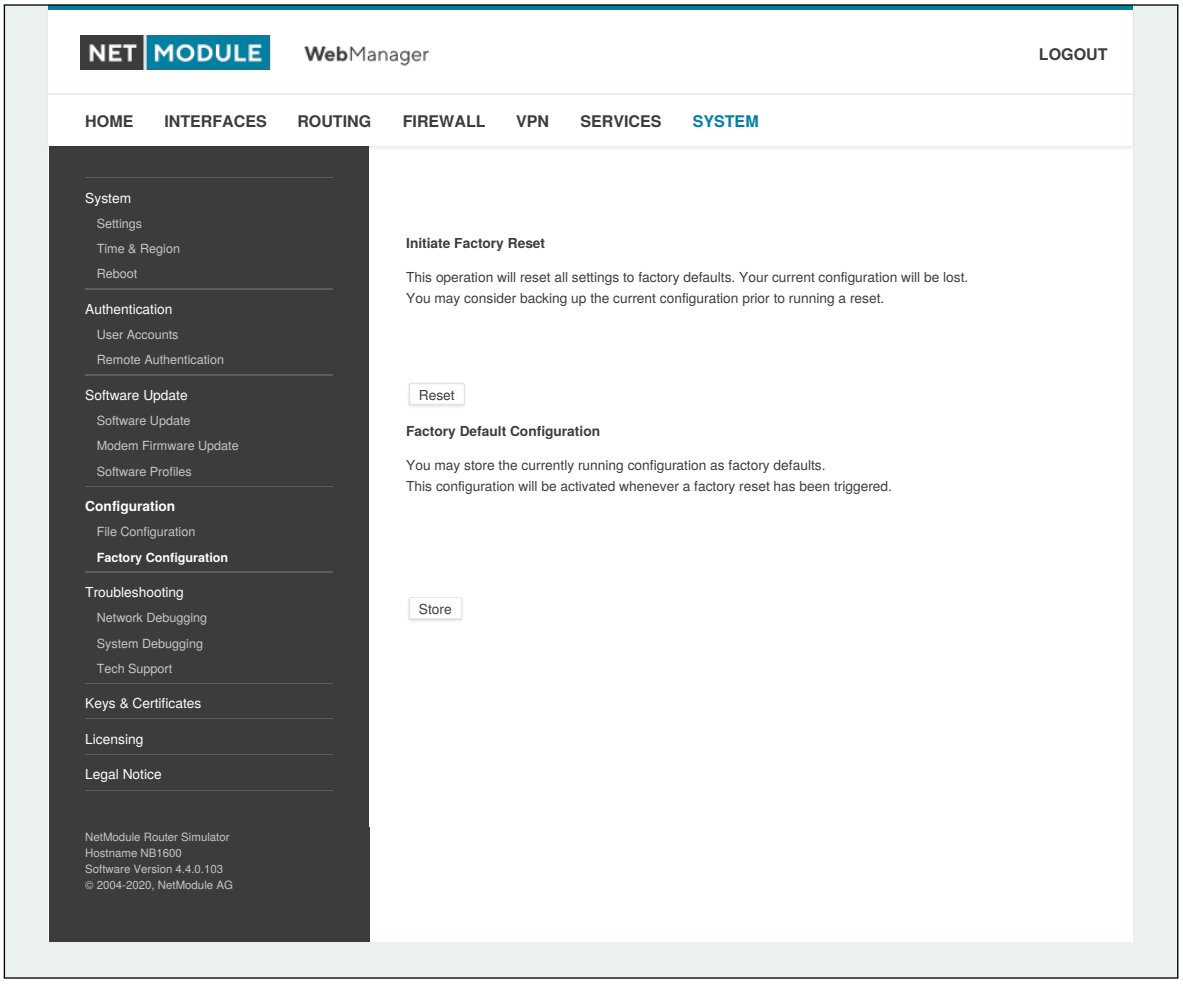


Figure 5.69.: Factory Configuration

This menu can be used to reset the device to factory defaults. Your current configuration will be lost. A successfully initiated factory reset can be noticed by all LEDs having been turned on. The 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.

5.8.7. Troubleshooting

Network Debugging

There are serveral tools for network debugging like ping, traceroute, tcpdump and darkstat.

Parameter	Automatic software update
Ping	The ping utility can be used to verify whether a remote host can be reached via IP.
Traceroute	The traceroute utility can be used to print the route packets trace to a remote host.
Tcpdump	The tcpdump utility generates a network capture (PCAP) of an interface which can be later analyzed with Wireshark.

System Debugging

You can view the system log here by selection the option *Debug log* or if you are interested in the boot log select *Boot log*.

Another way to see what is going on on the box is opening a SSH or Telnet session as *root* and typing `tail-log`. Furthermore the system log can be redirected to a syslog server, see section 5.8.1.

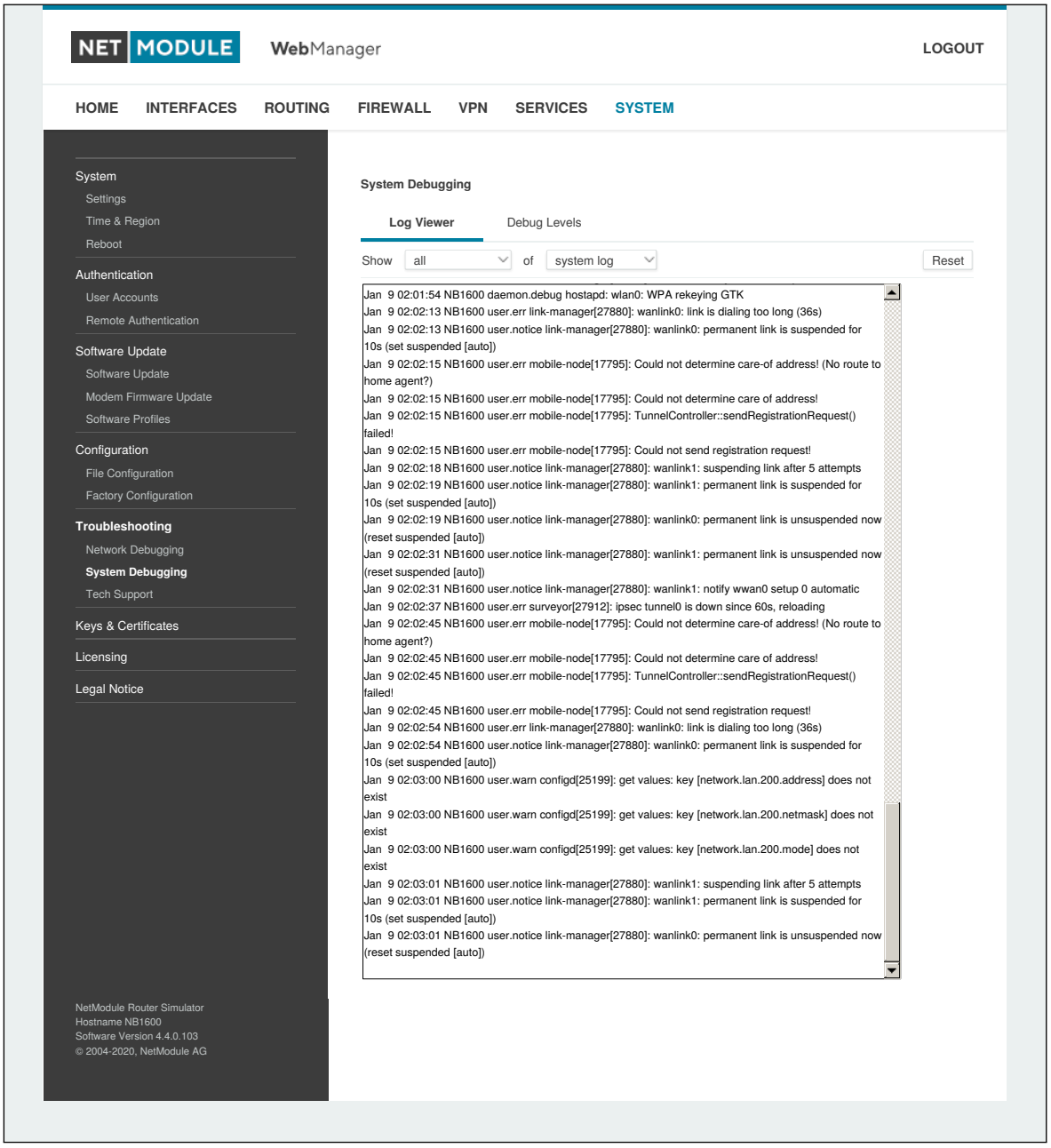


Figure 5.70.: Log Viewer

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 on-line support form, as it would significantly speed up the process of analyzing and resolving your problem. Log files can be viewed, downloaded and reset here. Please study them carefully in case of any issues. Various tools reside on this page for further analysis of potential configuration issues.

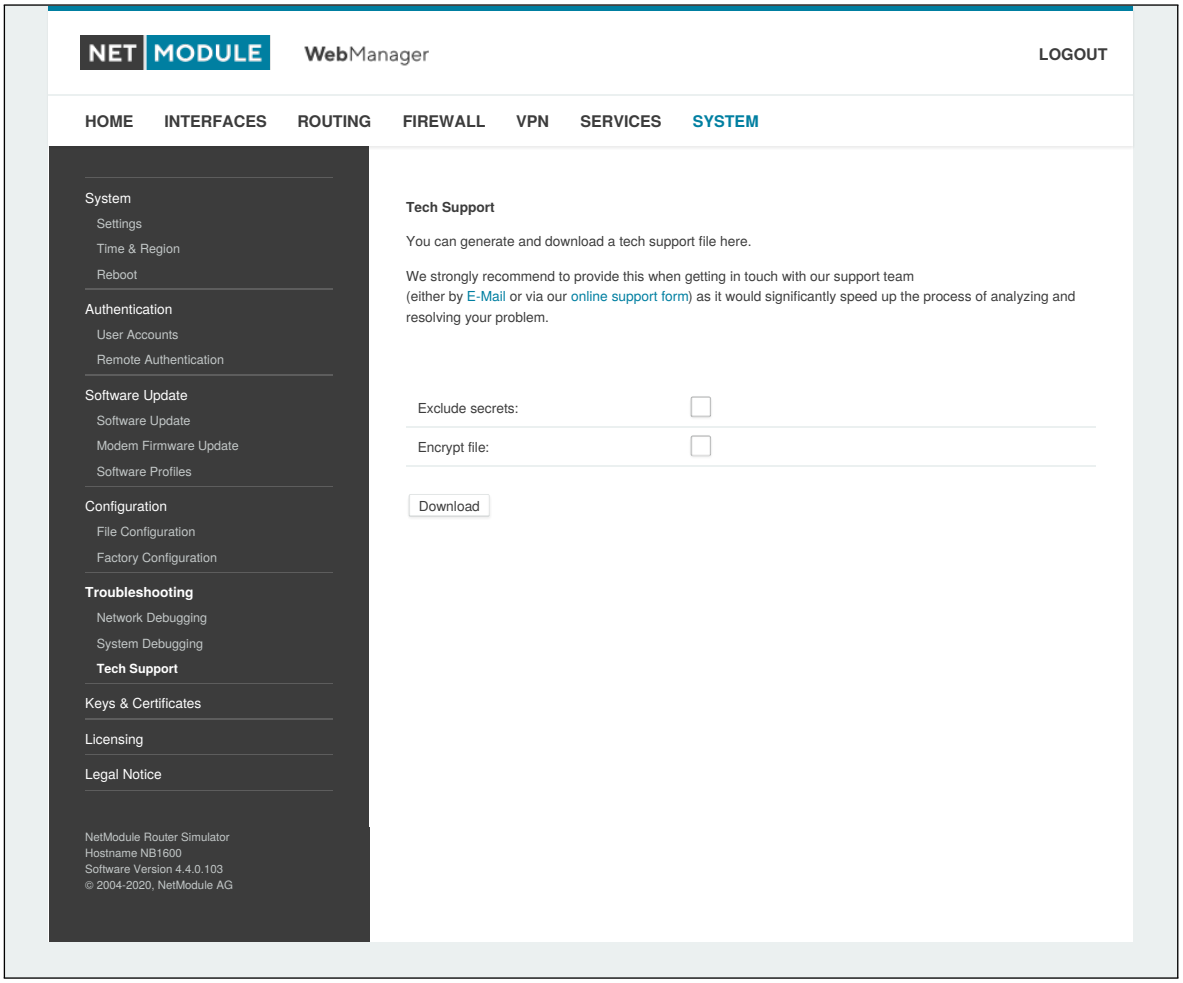


Figure 5.71.: Tech Support File

It is possible to trace any IP interface and inspect individual packet flows between hosts. This can be achieved by logging onto the box and start a network packet capture by using the tool *tcpdump*. We recommend to use the -n switch to bypass name resolution (e.g. `tcpdump -n -i lan0`). You may also generate a dump in PCAP format using the Web Manager, download it to your computer and perform further inspections with Wireshark (available at www.wireshark.org).

5.8.8. Keys and Certificates

The key and certificate page lets you generate required files for securing your services (such as HTTP and SSH server) but also to implement authentication and encryption for certificate-based VPN tunnels and WLAN clients.

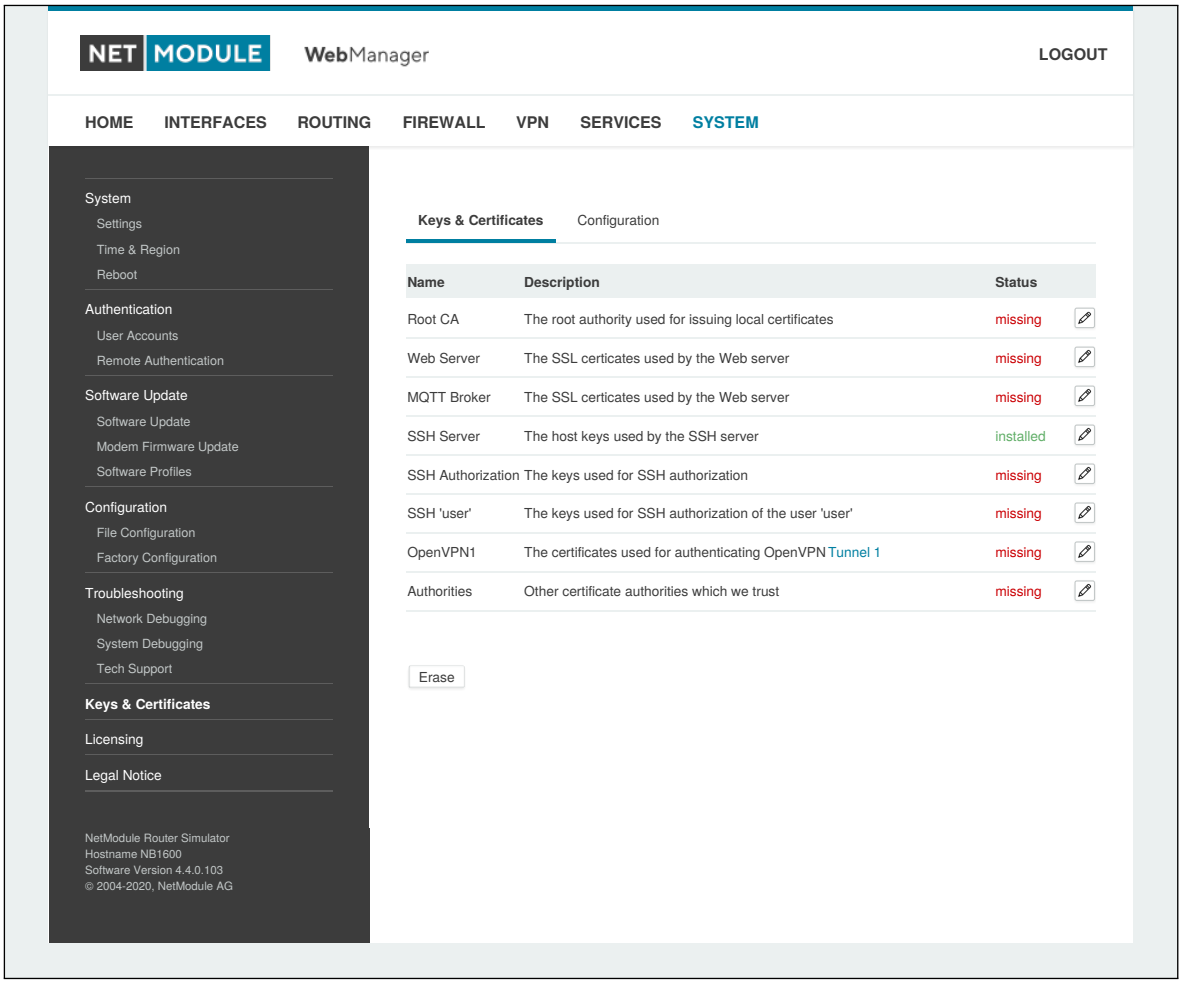


Figure 5.72.: Keys and certificates

The entry pages shows an overview about installed keys and certificates. The following sections may appear:

Type	Description
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
Web Server	The certificates for the Web server required for running HTTP over SSL (HTTPS).
MQTT Broker	The certificates for the MQTT Broker required for running MQTT over TLS encrypted connection.
SSH Server	The DSS/DSA keys for the SSH server.

Type	Description
SSH Authorization	The keys used for SSH authorization.
OpenVPN	Server or client keys and certificates for running OpenVPN tunnels.
IPsec	Server or client keys and certificates for running IPsec tunnels.
WLAN	Keys and certificates for implementing certificate-based WLAN authentication (e.g. WPA-EAP-TLS).
ETH	Keys and certificates for authentication via IEEE 802.1X on Ethernet ports.
Authorities	Other certificate authorities which we trust when establishing SSL client connections.

Table 5.178.: Certificate Sections

For each certificate section it is possible to perform the following operations:

Operation	Description
generate locally	Generate key and certificate locally on the box (see 5.8.8 for more options)
upload files	Key and certificate will be uploaded. We support files in PKCS12, PKCS7, PEM/DER format as well as RSA/DSS keys in OpenSSH or Dropbear format.
enroll via SCEP	Enroll key and certificate via SCEP (see 5.8.8 for more options)
download certificate	Download key and certificate in ZIP format (files will be encoded in PEM format)
create signing request	Generate key locally and create a signing request to retrieve a certificate signed by another authority
erase certificate	Erase all keys and certificates associated with this section

Table 5.179.: Certificate Operations

Configuration

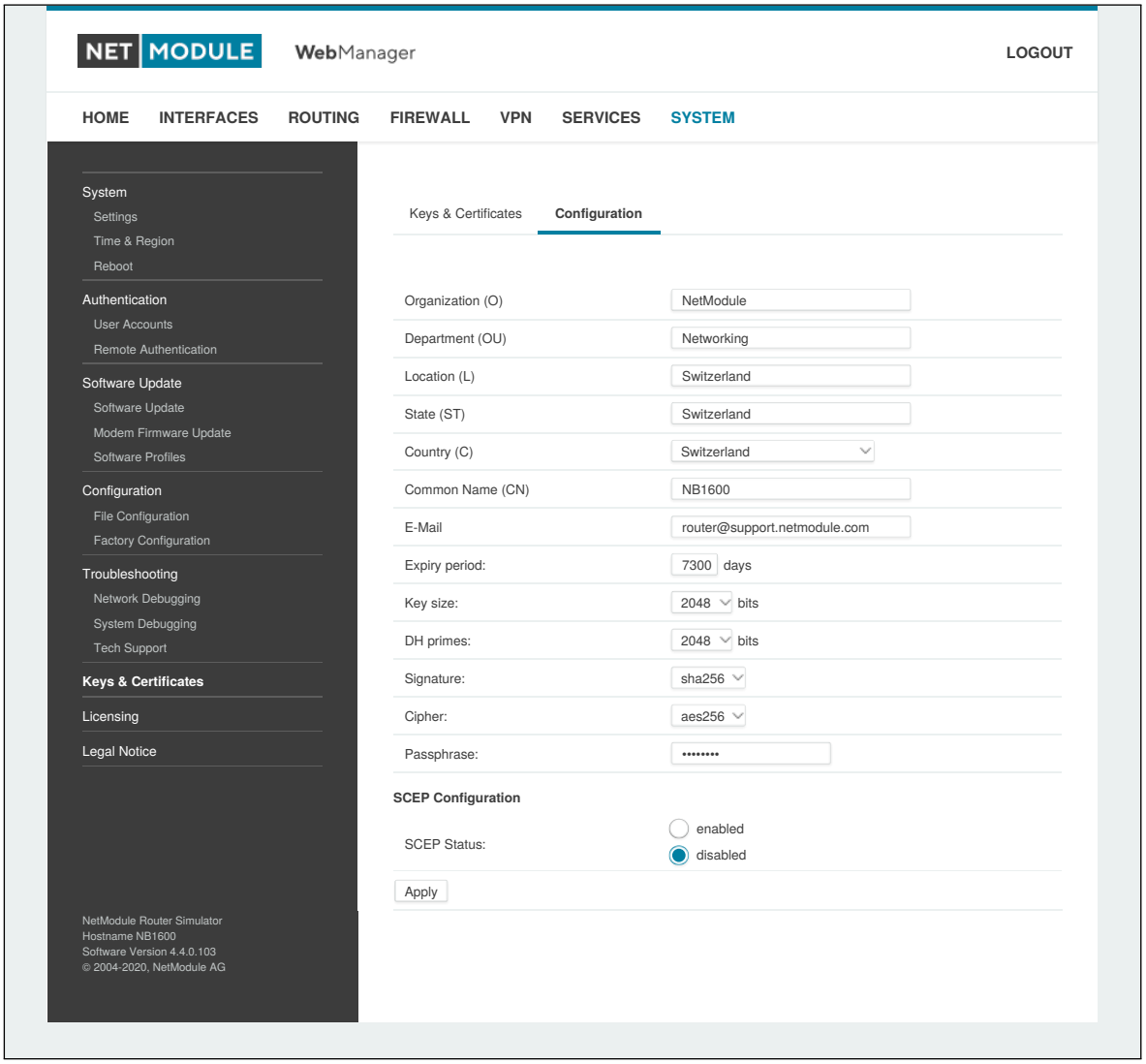


Figure 5.73.: Certificate Configuration

This page provides some general configuration options which will be applied when operating on keys and certificates.
If keys, certificates and signing requests are generated locally, the following settings will be take into account:

Parameter	Certificate Configuration
Organisation (O)	The certificate owner's organization
Department (OU)	The name of the organizational unit to which the certificate issuer belongs
Location (L)	The certificate owner's location
State (ST)	The certificate owner's state

Parameter	Certificate Configuration
Country (C)	The certificate owner's country (usually a TLD abbreviation)
Common Name (CN)	The certificate owner's common name, mainly used to identify a host
E-Mail	The certificate owner's email address
Expiry period	The number of days a certificate will be valid from now on
Key size	The length of the private key in bits
DH primes	The number of bits for custom Diffie-Hellman primes
Signature	The signature algorithm when signing certificates
Passphrase	The passphrase for accessing/opening a private key. This passphrase is initialized to a random string the first time you log in. (see 5.1.1)

Please be aware of the fact, that the local random number generator (RNG) provides pretty good randomness for most applications. If stronger cryptography is mandatory, we suggest to create the keys at an external RNG device or manage all certificates completely on a remote certification server. Nevertheless, using a local certificate authority can issue and manage all required certificates and also run a certificate revokation list (CRL).

When importing keys, the certificate and key file can be uploaded individually encoded in PEM/DER or PKCS7 format. All files (CA certificate, certificate and private key) can also be uploaded in one stroke by using the container format PKCS12. RSA/DSS keys can be converted from OpenSSH or Dropbear formats. It is possible to specify the passphrase for opening the private key. Please note that the system will generally apply the system-wide certificate passphrase on a key when installing the certificate. Thus, changing the general passphrase will result in all local keys getting equipped with the new one.

SCEP Configuration

If certificates are getting enrolled by using the Simple Certificate Enrollment Protocol (SCEP) the following settings can be configured:

Parameter	SCEP Configuration
SCEP status	Specifies whether SCEP is enabled or not
URL	The SCEP URL, usually in the form `http://<host>/<path>/pkiclient.exe`
CA fingerprint	The fingerprint of the certificate used to identify the remote authority. If left empty, any CA will be trusted.
Fingerprint algorithm	The fingerprint algorithm for identifying the CA (MD5 or SHA1)
Poll interval	The polling interval in seconds for a certificate request
Request timeout	The max. polling time in seconds for a certificate request
ID type	Can be IP, Email or DNS
Password	The password for the scep server.

When enrolling certificates, the CA certificate will be initially fetched from the specified SCEP URL using the `getca` operation. It will be shown on the configuration page and it has to be verified that it belongs to the correct authority. Otherwise, the CA must be rejected. This part is essential when using SCEP as it builds up the chain of trust.

If a certificate enrollment request times out, it is possible to re-trigger the interrupted enrollment request and it will be resumed using the previously generated key. In case a request has been rejected, you are required to erase the certificate first and then start the enrollment process all over again.

Authorities

For SSL client connections (as used by SDK functions or when downloading configuration/software images) you might upload a list of CA certificates which are considered trusted.

To obtain the CA certificate from a particular site with Mozilla Firefox, the following steps will be required:

- Point the browser to the relevant HTTPS website
- Click the padlock in the address bar
- Click the **More Information** and the **View Certificate** button
- Select the **Details** tab press the **Export** button
- Choose a path for the file (e.g. website.pem)

Certificates from self-signed authoritites can also be retrieved by running:

```
echo quit | \
openssl s_client -showcerts -connect <host>:443 | \
sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > other.crt
```

The PEM-encoded X.509 certificate files can be edited and concatenated using a simple editor (if required) and then uploaded to the box. Once installed, an SSL client connection will terminate if verification with any of those CA certificates fails.

5.8.9. Licensing

Certain features of NetModule routers require a valid license to be present in the system, some of them also depend on the mounted modules. Please contact us for getting a valid license for available components and we will provide a license file based on your serial number which can be installed to the router afterwards.

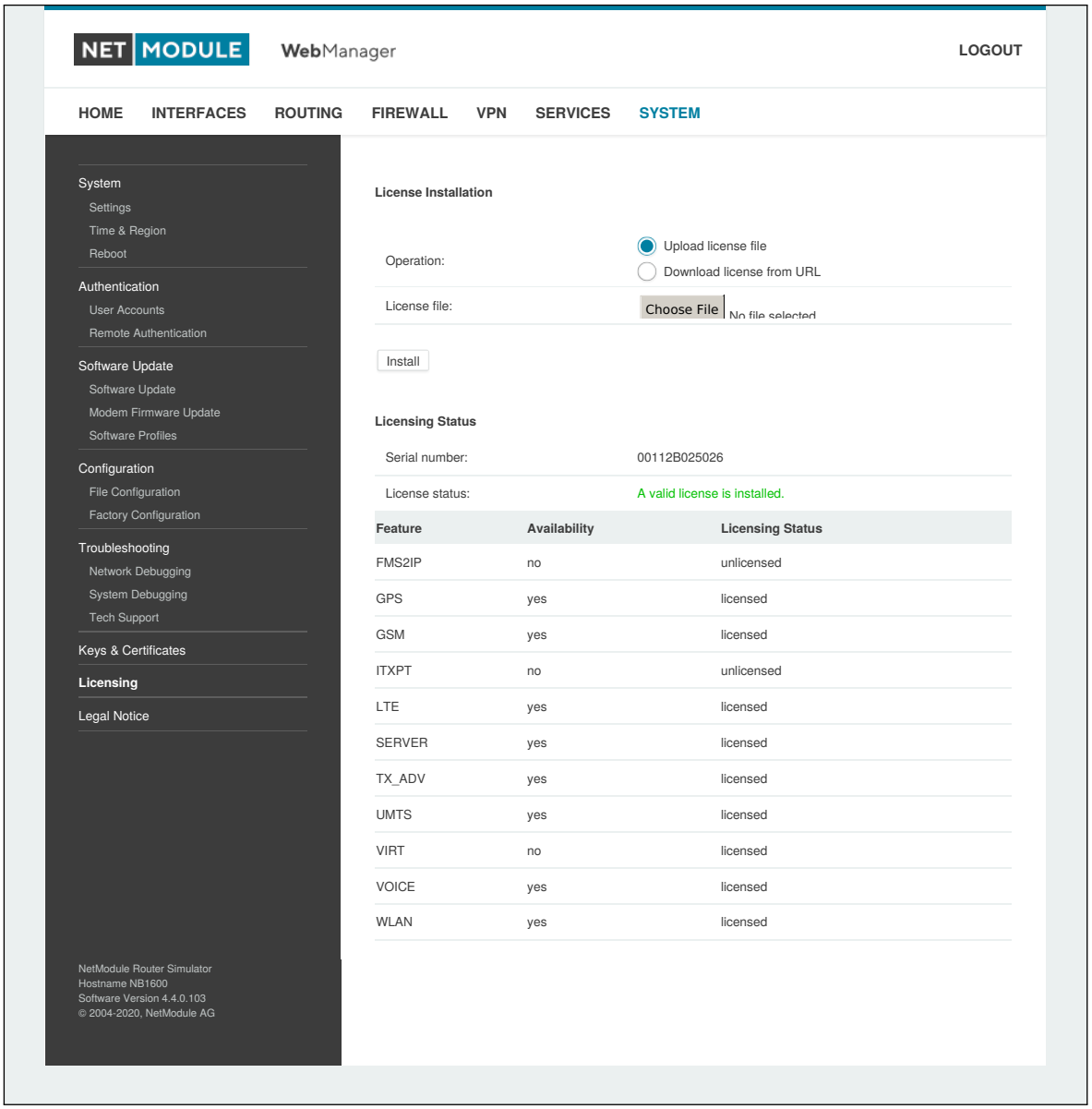


Figure 5.74.: Licensing

5.8.10. Legal Notice

OSS Notice

We inform you that NetModule products may contain in part open-source software. We are distributing such open-source software to you under the terms of GNU General Public License (GPL), GNU Lesser General Public License (LGPL) or other open-source licenses.

These licenses allow you to run, copy, distribute, study, change and improve any software covered by GPL, Lesser GPL, or other open-source licenses without any restrictions from us or our end user license agreement on what you may do with that software. Unless required by applicable law or agreed to in writing, software distributed under open-source licenses is distributed on an "AS IS" basis, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

To obtain the corresponding open source codes covered by these licenses, please contact our technical support at support@netmodule.com.

Acknowledgements

This product includes PHP, freely available from http://www.php.net.
This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).
This product includes cryptographic software written by Eric Young(eay@cryptsoft.com).
This product includes software written by Tim Hudson (tjh@cryptsoft.com).
This product includes software written Jean-loup Gailly and Mark Adler.
This product includes software MD5 Message-Digest Algorithm by RSA Data Security, Inc.
This product includes an implementation of the AES encryption algorithm based on code released by Dr Brian Gladman.
Multiple-precision arithmetic code originally written by David Ireland
Software from The FreeBSD Project (www.freebsd.org)

Copyright (C) 2023, NetModule. All rights reserved.

5.9. LOGOUT

Please use this menu to log out from the Web Manager.

6. Command Line Interface

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

It will be started automatically in interactive mode when logging in as *admin* user or by running `cli -i`. However, the same syntax can be used when calling it from the system shell. A list of available commands can be displayed by running `cli -l`.

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 some 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) has been reached. It can be turned off by the command `no-autologout`.

6.1. 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. Typing `exit` as well as 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
`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`	Freeze session
`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 the point

Key Sequence	Action
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.

6.2. 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
        done                    Check done
        update                  Update system facilities
        cert                    Manage keys and certificates
        status                  Get status information
        scan                    Scan networks
        send                    Send message, mail, techsupport or ussd
        restart                 Restart service
        debug                   Debug system
        reset                   Reset system to factory defaults
        reboot                  Reboot system
        shell                   Run shell command
        help                    Print help for command
        no-autologout           Turn off auto-logout
        history                 Show command history
        exit                    Exit
```

6.3. Getting Config Parameters

The get command can be used to get configuration values.

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

Options:
        -s          generate sourceable output
```

```
        -v        validate config parameter
        -f        get factory default rather than current value
        -c        show configuration sections
```

6.4. Setting Config Parameters

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

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

Options:
        -v     validate config parameter
```

6.5. Checking Config Completed

The `done` command can be used to check if all modify scripts have completed after a config change.

```
> done -h
Usage:
        done [-h]
```

6.6. 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:

        summary              Short status summary
        info                 System and config information
        config               Current configuration
        system               System information
        configuration        Configuration information
        license              License information
        wwan                 WWAN module status
        wlan                 WLAN module status
        gnss                 GNSS (GPS) module status
        eth                  Ethernet interface status
        lan                  LAN interface status
        wan                  WAN interface status
        openvpn              OpenVPN connection status
```

```
        ipsec                   IPsec connection status
        pptp                    PPTP connection status
        gre                     GRE connection status
        dialin                  Dial-In connection status
        mobileip                MobileIP status
        dio                     Digital IO status
        audio                   Audio module status
        can                     CAN module status
        uart                    UART module status
        ibis                    IBIS module status
        redundancy              Redundancy status
        sms                     SMS status
        firewall                Firewall status
        qos                     QoS status
        neigh                   Neighborhood status
        location                Current Location
```

6.7. Scanning Networks

The `scan` command can be used to scan for available WWAN and WLAN networks.

```
> scan -h
Usage:
        scan [-hs] <interface>

Options:
        -s      generate sourceable output
```

6.8. 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
Usage:
        send [-h] <type> <dest> <msg>

Options:
        <type>      type of message to be sent (mail, sms, techsupport, ussd)
        <dest>      destination of message (mail-address, phone-number or index)
        <msg>       message to be sent
```

6.9. Updating System Facilities

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

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

```
Options:
        -r      reboot after update
        -f      force update
        -n      don't reset missing config values with factory defaults
        -s      show update status

Available update targets:

        software            Perform software update
        firmware            Perform module firmware update
        config              Update configuration
        license             Update licenses
        sshkeys             Install SSH authorized keys

You may also run 'update software latest' to install the latest version
from our server.
```

6.10. Manage keys and certificates

The `cert` command can be used to manage keys and certificates.

```
> cert -h

Usage:
        cert [-h] [-p phrase] <operation> <cert> [<url>]

Possible operations:

        install             install a certificate from specified URL
        create              create a certificate locally
        enroll              enroll a certificate via SCEP
        erase               erase an installed certificate
        view                view an installed certificate
```

6.11. Restarting Services

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

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

Available services:

        configd               Configuration daemon
        dnsmasq               DNS/DHCP server
        dropbear              SSH server
        firewall              Firewall and NAPT
        gpsd                  GPS daemon
        gre                   GRE connections
```

```
        ipsec                   IPsec connections
        lighttpd                HTTP server
        link-manager            WAN links
        network                 Networking
        openvpn                 OpenVPN connections
        pptp                    PPTP connections
        qos                     QoS daemon
        smsd                    SMS daemon
        snmpd                   SNMP daemon
        surveyor                Supervision daemon
        syslog                  Syslog daemon
        telnet                  Telnet server
        usbipd                  USB/IP daemon
        voiced                  Voice daemon
        vrrpd                   VRRP daemon
        wlan                    WLAN interfaces
        wwan-manager            WWAN manager
```

6.12. Debug System

The `debug` command can be used to obtain debug/log messages.

```
> debug -h
Usage:
        debug [-h] <target>

Available debug targets:

        configd
        event-manager
        home-agent
        led-manager
        link-manager
        mobile-node
        qmid
        qosd
        scripts
        sdkhost
        ser2net
        smsd
        surveyor
        swupdate
        system
        voiced
        watchdog
        wwan-manager
        wwanmd
```

6.13. Resetting System

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

```
> reset -h
Usage:
        reset [-h]
```

6.14. Rebooting System

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

```
> reboot -h
Usage:
        reboot [-h]
```

6.15. Running Shell Commands

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

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

6.16. Working with History

The `history` command will print the list of entered commands on a per-user basis.

```
> history -h
Usage:
        history [-c]
```

It can be cleared by `history -c`.

6.17. CLI-PHP

CLI-PHP, the 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:

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

This section describes the CLI-PHP interface for Version 2. It accepts POST and GET requests.

Attention
The examples only show the usage of this interface for demonstration purpose. For productive environments it is recommended to use POST and HTTPS instead of GET and HTTP. Please be aware that your browser history will store GET requests including passwords and other sensitive information if you use GET requests to test this interface.

Running with GET requests, 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
      command         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 cli.

  Thus, an URL containing the following sequence:

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

  will lead to cli being called as:

   cli get "admin.password" "admin.debug"

  It supports whitespaces but please be aware that any special characters in
  the URL must be specified according to RFC1738 (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.
  Please note that the status summary 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=
  reboot
```

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=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

  http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=
  update&arg0=firmware&arg1=wwan0&arg2=tftp://192.168.1.254/firmware
```

send - Send SMS

```
Key usage:
  command=send&arg0=sms&arg1=<number>&arg2=<text>


Notes:
The phone number has to be specified in international format such as +123456789
including a leading plus sign (which can be encoded with %2B). The SMS daemon
must be properly configured prior to using that function.

Examples:

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=
send&arg0=sms&arg1=%2B123456789&arg2=test
```

send - Send E-Mail

```
Key usage:
  command=send&arg0=mail&arg1=<address>&arg2=<text>

Notes:
The address has to be a valid E-Mail address such as abc@abc.com (the at-sign can
 be encoded with %40). The E-Mail client must be properly configured prior to
using that function.

Examples:

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=
send&arg0=mail&arg1=abc%40abc.com&arg2=test
```

send - Send TechSupport

```
Key usage:
  command=send&arg0=techsupport&arg1=stdout
  command=send&arg0=techsupport&arg1=<address>&arg2=<subject>

Notes:
The address has to be a valid E-Mail address such as abc@abc.com (the at-sign can
 be encoded with %40). The E-Mail client must be properly configured prior to
using that function.
In case of stdout, the downloaded techsupport file will be called 'download'.

Examples:

http://192.168.1.1/cli.php?version=2&output=mime&usr=admin&pwd=admin01&command=
send&arg0=techsupport&arg1=stdout
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=
send&arg0=techsupport&arg1=abc%40abc.com&arg2=subject
```

send - Send USSD code

```
Key usage:
  command=send&arg0=ussd&arg1=<card>&arg2=<code>

Notes:
The argument card specifies the card module index (e.g. 0 for wwan0). The USSD
code can consist of digits, plus signs, asterisks (can be encoded with \%2A) and
dashes (can be encoded with \%23).

Examples:

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=
send&arg0=ussd&arg1=0&arg2=%2A100%23
```

A. Appendix

A.1. Abbrevations

Abbreviation	Description
ANY	Generally includes all options offered by the current section
APN	Access Point Name
ASU	Arbitrary Strength Unit
CID	A Cell ID is a generally unique number used to identify each Base Transceiver Station (BTS).
CID	Cell-ID
CLI	Command Line Interface, a generic interface to query the router or perform system tasks
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ETHx	Corresponds to Ethernet interfaces (either single or switched ones)
FQDN	Fully qualified domain name
GHz	GigaHertz
GNSSx	Specifies a Global Navigation Satellite System module
GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol
ICCID	Integrated Circuit Card Identifier
IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity
INx	Specifies a digital I/O input port (DIx)
LAC	Location Area Code
LAC	The Location Area Code corresponds to an identifier of a set of base stations that are grouped together to optimize signaling
LAI	Location Area Identification
LAI	The Location Area Identity is a globally unique number that identifies the country, network provider and location area
LANx	LAN interfaces which are generally based on Ethernet interfaces (including bridges)
MAC	Media Access Control
Mbps	Megabits per second
MCC	Mobile Country Code
MCS	Modulation Coding Scheme

Abbreviation	Description
MEID	Mobile Equipment Identifier
MHz	MegaHertz
MNC	Mobile Network Code
Mobilex	Identifies a WWAN modem
MOBILEIPx	Refers to a Mobile IP tunnel interface
MSISDN	Mobile Subscriber Integrated Services Digital Network Number
MSS	Maximum Segment Size
MTU	Maximum Transmission Unit
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NTP	Network Time Protocol
OUTx	Specifies a digital I/O output port (DOx)
PPTPx	Specifies a PPTP tunnel interface
PSK	Pre-Shared Key
RSRP	Referenz Signal Received Power
RSRQ	Reference Signal Received Quality
RSSI	Received Signal Strength Indication
SDK	Script Development Kit which can be used to program applications
SERIALx	Identifies a serial port
SIMx	Specifies the SIM slot as seen on the front panel
SIM	Subscriber Identity Module
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSID	Service Set Identifiers, can be used to define multiple WLAN networks on a module
STP	Spanning Tree Protocol
TAPx	Specifies an OpenVPN tunnel interface (based on TAP)
TUNx	Specifies an OpenVPN tunnel interface (based on TUN)
USSD	Unstructured Supplementary Service Data
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol

Abbreviation	Description
WAN	WAN links include all Wide Area Network interfaces which are currently activated in the system
WDS	Wireless Distribution System
WLANx	Refers to a Wireless LAN interface which will be represented as additional LAN interface when configured as access point
WPA2	Wi-Fi Protected Access 2
WPA3	Wi-Fi Protected Access 3
WWANx	Refers to a Wireless Wide Area Network (2G/3G/4G) connection

Table A.1.: Abbreviations

In general, internal interfaces are written lower-case and may have a different naming. Their index starts from zero, whereas interfaces seen by the user will be written in capital letters starting from one.

A.2. System Events

ID	Ereignis	Beschreibung
101	wan-up	WAN-Verbindung aufgebaut
102	wan-down	WAN-Verbindung unterbrochen
201	dio-in1-on	DIO IN1 eingeschaltet
202	dio-in1-off	DIO IN1 ausgeschaltet
203	dio-in2-on	DIO IN2 eingeschaltet
204	dio-in2-off	DIO IN2 ausgeschaltet
205	dio-out1-on	DIO OUT1 eingeschaltet
206	dio-out1-off	DIO OUT1 ausgeschaltet
207	dio-out2-on	DIO OUT2 eingeschaltet
208	dio-out2-off	DIO OUT2 ausgeschaltet
301	gps-up	GPS-Signal verfÃijgbar
302	gps-down	GPS-Signal nicht verfÃijgbar
401	openvpn-up	OpenVPN-Verbindung aufgebaut
402	openvpn-down	OpenVPN-Verbindung unterbrochen
403	ipsec-up	IPsec-Verbindung aufgebaut
404	ipsec-down	IPsec-Verbindung unterbrochen
406	pptp-up	PPTP-Verbindung aufgebaut
407	pptp-down	PPTP-Verbindung unterbrochen
408	dialin-up	Dial-In-Verbindung aufgebaut

ID	Ereignis	Beschreibung
409	dialin-down	Dial-In-Verbindung unterbrochen
410	mobileip-up	Mobile IP-Verbindung aufgebaut
411	mobileip-down	Mobile IP-Verbindung unterbrochen
412	gre-up	GRE-Verbindung aufgebaut
413	gre-down	GRE-Verbindung unterbrochen
501	system-login-failed	Anmeldung fehlgeschlagen
502	system-login-succeeded	Anmeldung erfolgtreich
503	system-logout	Benutzer abgemeldet
504	system-rebooting	Systemneustart eingeleitet
505	system-startup	System gestartet
506	test	Testereignis
507	sdk-startup	SDK gestartet
508	system-time-updated	Systemzeit aktualisiert
509	system-poweroff	Systemabschaltung ausgelÃűst
510	system-error	System befindet sich im Fehlerzustand
511	system-no-error	System hat Fehlerzustand verlassen
601	sms-sent	SMS gesendet
602	sms-notsent	SMS nicht gesendet
603	sms-received	SMS empfangen
604	sms-report-received	SMS-Bericht empfangen
701	call-incoming	Eingehender Sprachanruf
702	call-outgoing	Abgehender Sprachanruf wird aufgebaut
801	ddns-update-succeeded	Aktualisierung des Dynamic DNS erfolgreich
802	ddns-update-failed	Aktualisierung des Dynamic DNS fehlgeschlagen
901	usb-storage-added	USB-SpeichergerÃď't hinzugefÃijgt
902	usb-storage-removed	USB-SpeichergerÃď't entfernt
903	usb-eth-added	USB-Ethernet-GerÃď't hinzugefÃijgt
904	usb-eth-removed	USB-Ethernet-GerÃď't entfernt
905	usb-serial-added	Serielles USB-GerÃď't hinzugefÃijgt
906	usb-serial-removed	Serielles USB-GerÃď't entfernt
1001	redundancy-master	Router ist jetzt der Master-Router

ID	Ereignis	Beschreibung
1002	redundancy-backup	Router ist jetzt der Backup-Router

Table A.2.: Systemereignisse

A.3. Factory Configuration

The factory configuration including default values for any configuration parameter can be derived from the file `/etc/config/factory-config.cfg` on the router. You may also call `cli get -f <parameter>` for obtaining a specific default value.

A.4. SNMP VENDOR MIB

A.5. SDK Examples

Event	Description
best-operator.are	This script will scan for operators on startup and choose the one with the best signal
candump.are	This script can be used to receive CAN messages
config-summary.are	This script shows a summary of the currently running configuration.
dio.are	This script can be used to set a digital output port.
dio-monitor.are	This script monitors the DIO ports and sends a SMS to the specified phone number.
dio-server.are	This script implements a TCP server which can be used to control the DIO ports.
dynamic-operator.are	This script will scan Mobile2 and dial the appropriate SIM on Mobile1
email-to-sms.are	This script implements a lightweight SMTP server which is able to receive mail and forward them as SMS to a phone number.
etherwake.are	This script can be used to wake up a sleeping host (WakeOnLan)
gps-broadcast.are	This script sends the local GPS NMEA stream to a remote UDP server (incl. device identity).
gps-monitor.are	A script for activating WLAN as soon as GPS position (lat,lon) is within a specified range.
gps-udp-client.are	This script sends the local GPS NMEA stream to a remote UDP server.
gps-udp-client-compat.are	This script sends the local GPS NMEA stream (incl. serial/checksum) to a remote UDP server.
led.are	This script can be used to set a LED
modbus-rtu-master.are	This script can be used to read messages from the serial port.
modbus-rtu-slave.are	This script implements a modbus slave server
modbus-tcp-rtu-gateway.are	This script implements a Modbus TCP RTU gateway
mount-media.are	This script can be used to mount an USB storage stick.
opcua-browse.are	This script will browse for nodes at a remote OPC-UA server.
opcua-json.are	This script polls any temperature nodes of an OPC-UA server and sends them JSON-encoded to a remote server.
opcua-read.are	This script will read the node value at a OPC-UA server.
opcua-write.are	This script will write a new value to a node at a OPC-UA server.
ping-supervision.are	This script will supervise a specified host.
read-config.are	This script can be used to read a configuration parameter.

Event	Description
remote-mail.are	This script reads and sends mails from a remote IMAP/POP3/SMTP server
scan-mobile.are	This script can be used to switch the Mobile LAI according to available networks
scan-wlan.are	This script can be used to switch the WLAN client network according to availability
send-mail.are	This script will send an E-Mail to the specified address.
send-sms.are	This script will send an SMS to the specified phone number.
send-techsupport.are	This script will generate a techsupport and send it to the specified E-Mail address.
serial-read.are	This script can be used to read messages from the serial port.
serial-readwrite.are	This script will write to and read from the serial port.
serial-tcp-broadcast.are	This script reads messages coming from the serial port and forwards them via TCP to remote hosts (and vice versa).
serial-tcsetattr.are	This script can be used to set/get the attributes of the serial port.
serial-udp-server.are	This script reads messages coming from the serial port and forwards them via UDP to a remote host (and vice versa).
serial-write.are	This script can be used to write a message to the serial port.
set-ipsec-route.are	set route to IPSEC server depending on active WWAN / WLAN network
sms-confirm.are	This script will send out a message and confirm its delivery.
sms-control.are	This script will execute commands received by SMS.
sms-delete-inbox.are	This script can be used to flush the SMS inbox.
sms-read-inbox.are	This script can be used to read the SMS inbox.
sms-to-email.are	This script will forward incoming SMS messages to a given E-mail address.
sms-to-serial.are	This script can be used to write a received SMS to the serial port.
snmp-agent.are	This script extends MIB entries of the SNMP agent
snmp-cmd.are	This script issues SNMP set/get commands
snmp-trap.are	This script can be used to send SNMP traps
status.are	This script can be used to display all status variables
syslog.are	Throw a simple syslog message.
tcpclient.are	This script sends a message to a TCP server.
tcpserver.are	This script implements a TCP server which is able to receive messages.
techsupport.are	This transfers a techsupport to a remote FTP server

Event	Description
transfer.are	This scripts stores the latest GNSS positions in a remote FTP file
transfer-file.are	This scripts archives a remote file
udpclient.are	This script sends a message to a remote UDP server.
udp-msg-server.are	This script will run an UDP server which is able to receive messages and forward them as SMS/E-Mail.
udpserver.are	This script implements an UDP server which is able to receive messages.
update-config.are	This script can be used to perform a configuration update
voice-dispatcher-audio.are	This script implements an audio voice dispatcher
webpage.are	This script will generate a page which can be viewed in the Web Manager
write-config.are	This script can be used to set a configuration parameter.

Table A.3.: SDK Examples