NB2500

NB2600

NB2600R

User Manual
NetBox Wireless Routers

NB1310

NB2210

Table of Content

1 Safety and Conformity

Thank you for purchasing NetBox Wireless Router from NetModule. This chapter gives you an introduction to NetBox Wireless Router. The following chapters describe the installation and the configuration.

1.1 Safety Instructions

The NetBox Wireless Routers must be used in compliance with any and all applicable international and national laws and in compliance with any special restrictions regulating the utilization of the communication module in prescribed applications and environments.

Use only the original accessories to prevent possible injury to health and damage to appliances and to ensure that all the relevant provisions have been complied with. Unauthorized modifications or utilization of accessories that have not been approved may void the warranty.

The NetBox Wireless Routers must not be opened. Only the replacement of the SIM card is permitted.

All circuits connected to the interfaces of the NetBox Wireless Router must comply with the requirements of SELV (Safety Extra Low Voltage) circuits and are for indoor use only. Interconnections must not leave the building nor penetrate the body shell of a vehicle. Possible antenna circuits must be limited to overvoltage transient levels below 1500 Volts according to IEC 60950-1, TNV-1 circuit levels using safety approved components.

Use only with certified (CSA or equivalent) power supply, which must have a limited and SELV circuit output.

The NetBox Wireless Routers are designed for indoor use. Do not expose the communication module to extreme ambient conditions. Protect the communication module against dust, moisture and high temperature.

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

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

NetBox Wireless Routers may cause interference if it is in the proximity of TV sets, radio receivers and personal computers

Do not work at the antenna installation during a lightning.

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

NB2600R must be used with shielded Ethernet cables.

Consult the manual for the installation. Adhere to the instructions documented in the user manual.

1.2 Declaration of Conformity

NetModule declares that under our own responsibility the products NetBox Wireless Routers comply with the relevant standards following the provisions of the Council Directive 1999/5/EC. The signed Declarations of Conformity can be found under the following addresses:

NB1310:
http://www.netmodule.com/store/products/nb1310_conformity_declaration_e.pdf

NB2210:
http://www.netmodule.com/store/products/nb2210_conformity_declaration_e.pdf

NB2500:
http://www.netmodule.com/store/products/nb2500_conformity_declaration_e.pdf

NB2600:
http://www.netmodule.com/store/products/nb2500_conformity_declaration_e.pdf

NB2600R:
http://www.netmodule.com/store/products/nb2600R_conformity_declaration_e.pdf

1.3 Waste Disposal

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

1.4 National Restrictions

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

1.4.1 France

In case the product is used outdoors, the output power is restricted in some parts of the band. See the table below or check http://www.art-telecom.fr/ for more details.

Frequency Range (MHz)	Power (EIRP)	Restrictions
2400.0-2454	100 mW (20 dBm)	Only for indoor applications
2454–2483.5	10 mW (10 dBm)	If used outdoors
5470-5725		Relevant+ provisions for the implementation of DFS mechanism described in ETSI standard EN 301 893 V1.3.1 and subsequent versions

1.4.2 Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless operating within the boundaries of the owner's property, the use of this Wireless LAN product requires a ‘general authorization’. Please check with http://www.comunicazioni.it/ for more details.

1.4.3 Latvia

The outdoor usage of the 2.4-GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details.

1.4.4 Luxemburg

General authorization required for network and service supply.

1.4.5 Norway

Frequency Range	Restrictions
2400.0-2483.5 MHz (WLAN b/g)	This subsection does not apply for the geographical area within a radius of 20 km from the center of Ny-Ålesund

1.4.6 Russian Federation

Frequency Range (MHz)	Power (EIRP)	Restrictions
2400.0-2483.5	100 mW (20 dBm)	Only for indoor applications
5150-5250	100 mW (20 dBm)	Permitted to use only for indoor applications, closed industrial and warehouse areas, and on board aircraft
5250-5350	100 mW (20 dBm)	1. Permitted to use for local networks of aircraft crew service communications on board aircraft in area of the airport and at all stages of flight. 2. Permitted to use for public wireless access local networks on board aircraft during a flight at the altitude not less than 3000 m
5650-5825	100 mW (20 dBm)	Permitted to use on board aircraft during a flight at the altitude not less than 3000 m

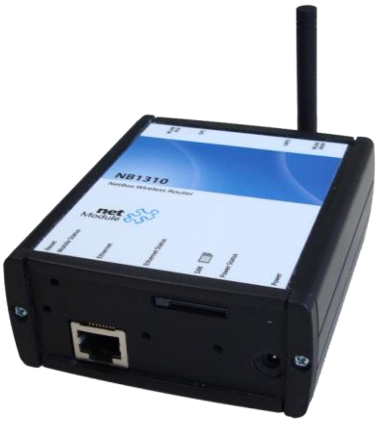
1.4.7 Turkey

Frequency Range	Restriction
5470-5725 MHz	Not implemented

2 Hardware Specifications

2.1 NB1310

2.1.1 Operating Elements and Interfaces



The following table describes the NB1310 interfaces and status indicators:

Label	Color	State	Function
Reset	-	-	Restart: press this button during run-time Factory reset: press and hold this button for at least 3 seconds during run-time.
Mobile Status	green	on	A solid light indicates a connected GSM or UMTS network
	green	blinking	The device is trying to register to a GSM or UMTS network
Ethernet	-	-	Ethernet port
Ethernet Status	green	on	A solid light indicates a connected Ethernet link.
		flashing	A flashing light indicates Ethernet activity.
SIM	-	-	SIM socket for the SIM card.
Power Status	green	on	The device is ready
		off	The device is not powered and/or does not start up
Power	-	-	Voltage feed connector (9-21 VDC) Polarity: ⊖—(•—⊕
UMTS MAIN	-	-	SMA female connector for GSM/UMTS antenna
GPS	-	-	SMA female connector for GPS antenna
WLAN MAIN	-	-	SMA female connector for WLAN antenna 1
WLAN AUX	-	-	SMA female connector for WLAN antenna 2 (for antenna diversity)

Table 1: The NB1310 interfaces and status indicators

2.1.2 Pin Assignments

2.1.2.1 Ethernet Port

Pin:	Signal: NB1310
1	TX+
2	TX-
3	RX+
4	Pair 1 for power injection 9-21VDC
5	Pair 1 for power injection 9-21VDC
6	RX-
7	Pair 2 for power injection 9-21VDC
8	Pair 2 for power injection 9-21VDC

Table 1: Pin assignment Ethernet Interface

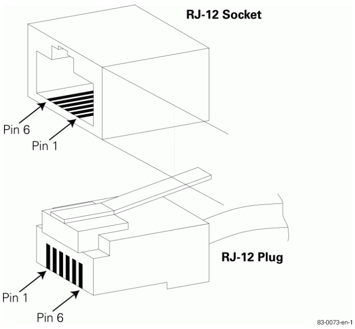


Figure 1: RJ45

NB1310 allows power feed through Ethernet. Power can be carried over the spare pairs (RJ45 pin 4/5 & 7/8) only. It is simplified PoE (not compliant with IEEE802.3af standard!). Power feed through data pairs (RJ45 pins 1/2 & 3/6) is not allowed, this can destroy the device.

Required parameters of PoE power injector:

Output voltage: 18-21VDC

Polarity on spare pairs (RJ45 pin 4/5 & 7/8) can be either.

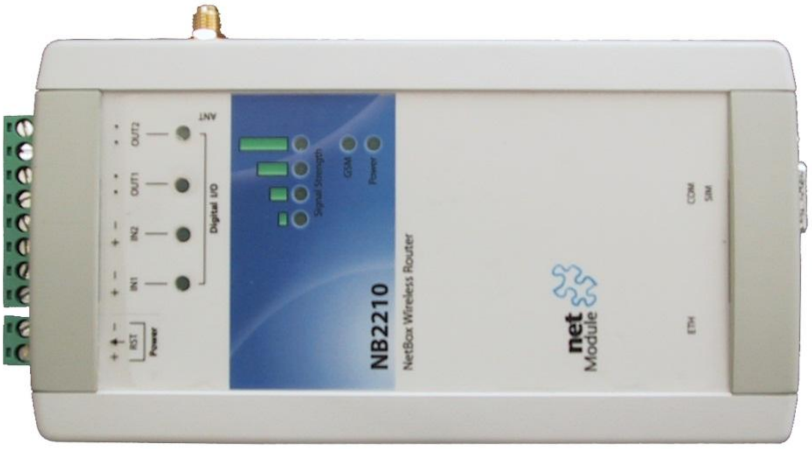
Output current: min 600mA at 18VDC

Required isolation between primary and secondary side: 1500VAC.

Estimated maximum distance from power injector to NB1310: about 15 - 30m.

2.2 NB2210

2.2.1 Operating Elements and Interfaces



The following table describes the meaning of the status indicators:

Panel	Label	Color	State	Function
Front	Power	green	blinking slowly	This indicates one of the following conditions: the device is starting up loading a new configuration factory reset initiated by Web Manager
			on	The device is ready
			off	The device is not powered and/or does not start up
			blinking fast	Restart triggered by watchdog
Front	Signal Strength	green	on	1 LED on: weak signal, 2 LEDs on: medium signal 3 LEDs on: strong signal, 4 LEDs on: very strong signal
			off	No or insufficient signal
			running	Software update
Front	GSM	green	on	Mobile connection is being established
			on	Mobile connection is up
			off	Mobile connection is down
Front	IN1 IN2	green	on	Input set
			off	Input not set
Front	OUT1 OUT2	green	on	Output on
			off	Output off
Bottom	Link	green	on	Physical link
			off	No physical link
Bottom	Activity	orange	on	Data transmission
			off	Not data transmission

Table 2: NB2210 status indicators

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

Panel	Label	Component Description
Top	RST	Restart: press this button when the status LED is on Factory reset: press and hold this button for at least 5 seconds.
Top	Power	Voltage feed connector (9-28 VDC)
Top	IN1 IN2	Digital inputs 2 opto-isolated digital inputs. Please consider the polarity.
Top	OUT1 OUT2	Digital outputs 2 relay outputs
Bottom	ETH	Ethernet port The default IP address is set to 192.168.1.1.
Bottom	COM	RS232, Sub-D 9 port The factory default is 115200 Baud, 8 Data Bits, no parity, 1 Stop Bit.
Bottom	SIM 1	SIM socket
Right	ANT	GSM antenna connector Impedance: 50 Ohm Connector: SMA female

Table 3: NB2210 Physical interfaces

2.2.2 Pin Assignments

2.2.2.1 Power

Pin:	Signal:
-	V_{GND}
+	9-28 V =

Table 2: Pin assignment power plug

2.2.2.2 Ethernet

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

Table 3: Pin assignment Ethernet

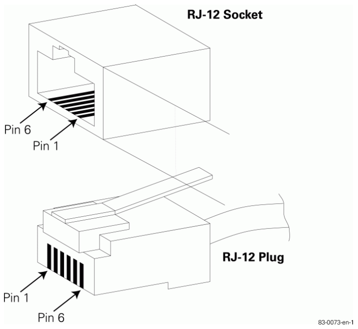


Figure 2: Ethernet

2.2.2.3 Serial Interface

Pin:	RS232:	RS485:
1	DCD	Do not connect
2	RxD	Do not connect
3	TxD	Data+
4	DTR	Do not connect
5	GND	GND
6	DSR	Do not connect
7	RTS	Do not connect
8	CTS	Data-
9	RI	Data+

Table 4: Pin assignment COM port

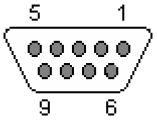
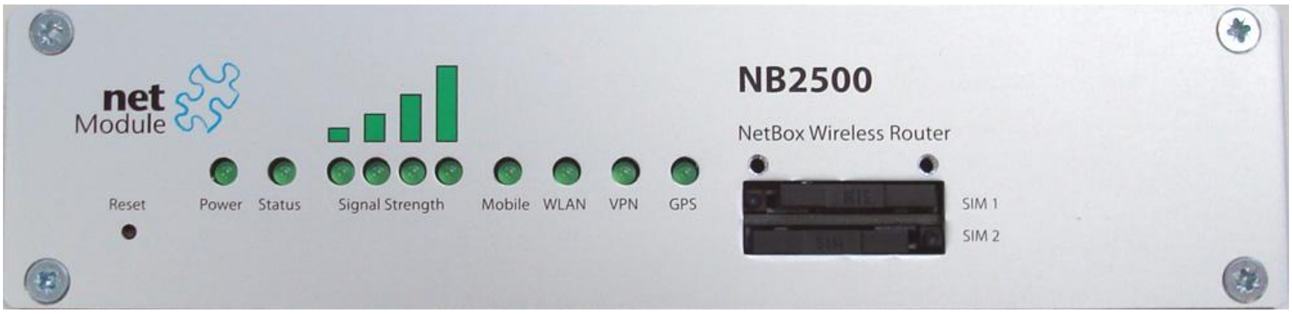


Figure 3: Sub-D 9pol plug female

2.3 NB2500

2.3.1 Operating Elements and Interfaces

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

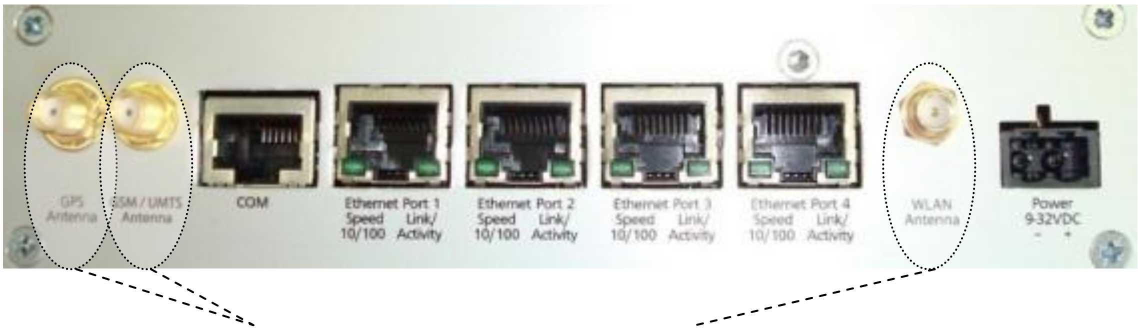


The following table describes the components on the front panel:

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

Table 4: NB2500 components on the front panel

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


GPS Antenna
GSM / UMTS Antenna
COM
Ethernet Port 1 Speed 10/100 Link/ Activity
Ethernet Port 2 Speed 10/100 Link/ Activity
Ethernet Port 3 Speed 10/100 Link/ Activity
Ethernet Port 4 Speed 10/100 Link/ Activity
WLAN Antenna
Power 9-32VDC - +

If available on the specific model

Panel	Label	Color	State	Function
Back	GPS Antenna	-	-	GPS antenna connector Impedance: 50 Ohm Connector: SMA female Support for passive GPS antennas only
Back	UMTS / GSM Antenna	-	-	UMTS / GSM antenna connector Impedance: 50 Ohm Connector: SMA female
Back	WLAN Antenna	-	-	WLAN antenna connector Impedance: 50 Ohm Connector: SMA female
Back	COM	-	-	RJ45 port (Sub-D 9 on earlier models) RS232 (default) or RS485 (configurable)
Back	Ethernet Ports	-	-	4 port Ethernet switch The default IP address is set to 192.168.1.1.
Back	Power	-	-	Voltage feed connector (9-32 VDC)
Back	Link/Activity (Ethernet Ports)	green	on	Physical link
			off	No physical link
			flashing	Data transmission
Back	Speed 10/100 (Ethernet Ports)	green	on	Data rate 100 MBit/s
			off	Data rate 10 MBit/s

Table 5: NB2500 components on the back panel

2.3.2 Pin Assignments

2.3.2.1 Power

Pin:	Signal:
-	V_{GND}
+	9-32 V =

Table 5: Pin assignment power plug

2.3.2.2 Ethernet

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

Table 6: Pin assignment Ethernet

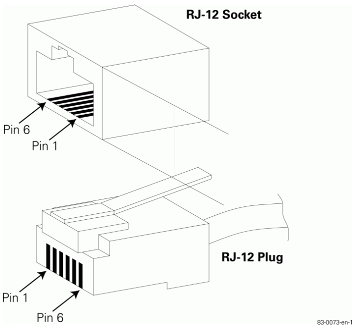


Figure 4: RJ45

2.3.2.3 Serial

Pin:	RS232	RS485
1	RTS	Do not connect
2	DTR	Do not connect
3	TXD	Do not connect
4	GND	GND
5	GND	GND
6	RXD	Do not connect
7	DSR	RxD/TxD-
8	CTS	RxD/TxD+

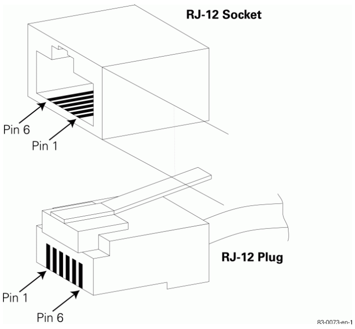


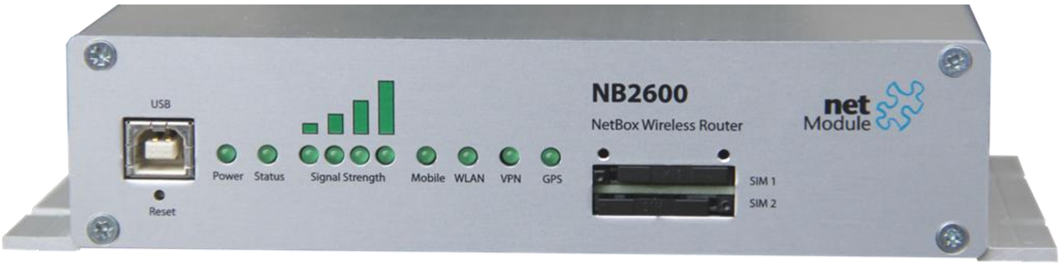
Figure 5: RJ45

Table 7: Pin assignment COM port

2.4 NB2600

2.4.1 Operating Elements and Interfaces

The front panel has 10 status indicators. In addition there is an USB device port, two SIM card slots and a reset button at the front panel.

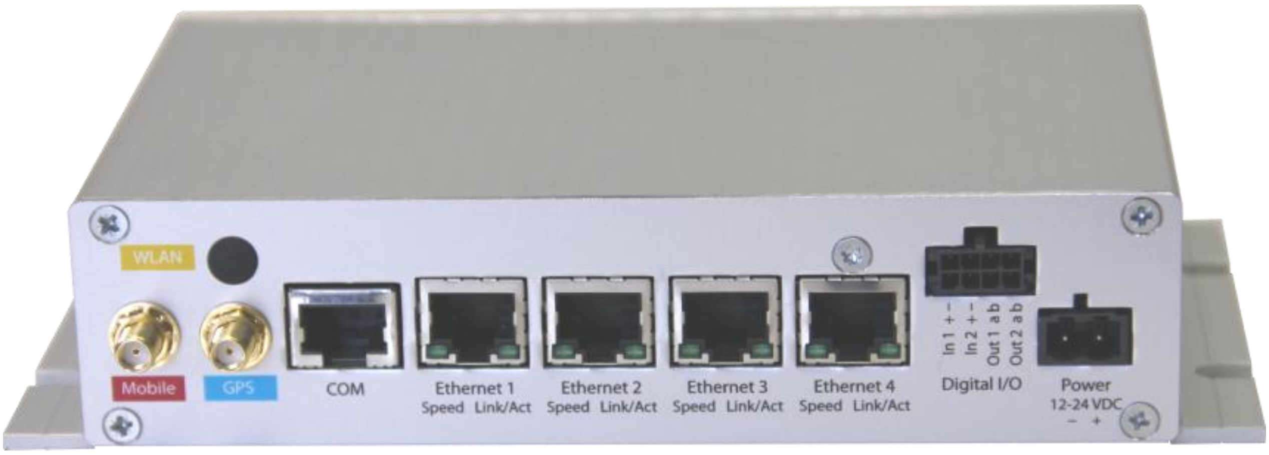


The following table describes the components on the front panel:

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

Table 6: NB2600 components on the front panel

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



Panel	Label	Color	State	Function
Back	Mobile	-	-	GSM/UMTS antenna connector Impedance: 50 Ohm Connector: SMA female
Back	GPS	-	-	GPS antenna connector Impedance: 50 Ohm Connector: SMA female Support for active and passive GPS antennas
Back	WLAN	-	-	WLAN antenna connector Impedance: 50 Ohm Connector: SMA female
Back	COM	-	-	RJ45 port RS232 (default) or RS485 (configurable)
Back	Ethernet Ports	-	-	4 port Ethernet switch The default IP address is set to 192.168.1.1.
Back	Power	-	-	Voltage feed connector (12-24 V=)
Back	Link/Activity (Ethernet Ports)	green	on	Physical link
			off	No physical link
			flashing	Data transmission
Back	Speed 10/100 (Ethernet Ports)	green	on	Data rate 100 MBit/s
			off	Data rate 10 MBit/s

Table 7: NB2600 components on the back panel

2.4.2 Pin Assignments

2.4.2.1 Power

Pin:	Signal:
-	V_{GND}
+	9-32 V =

Table 8: Pin assignment power plug

2.4.2.2 Ethernet

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

Table 9: Pin assignment Ethernet

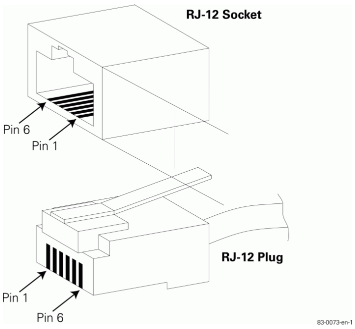


Figure 6: RJ45

2.4.2.3 Serial

Pin:	RS232	RS485
1	RTS	Do not connect
2	DTR	Do not connect
3	TXD	Do not connect
4	GND	GND
5	GND	GND
6	RXD	Do not connect
7	DSR	RxD/TxD-
8	CTS	RxD/TxD+

Table 10: Pin assignment COM port

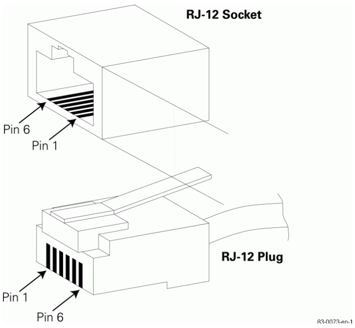
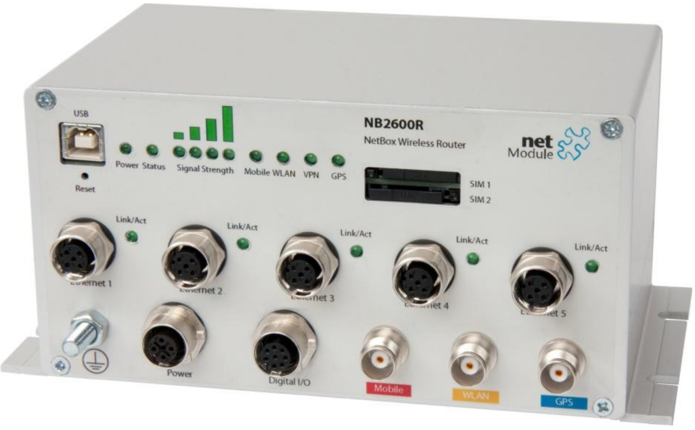


Figure 7: RJ45

2.5 NB2600R

2.5.1 Operating Elements and Interfaces

All connectors and status indicators are located at the front panel



The following table describes the indicators on the front panel:

Label	Color	State	Function
Power	green	on	The device is powered
		off	Power is missing
Status	green	blinking slowly	This indicates one of the following conditions: 1) the device is starting up, 2) loading a new configuration, 3) factory reset initiated by Web Manager
		on	The device is ready
		blinking fast	Restart triggered by watchdog
		off	The device does not start up
Signal Strength	green	on	1 LED on: weak signal, 2 LEDs on: medium signal 3 LEDs on: strong signal, 4 LEDs on: very strong signal
		off	No or insufficient signal
		running	Software update
Mobile (UMTS / GSM)	green	blinking slowly	Mobile connection is being established
		on	Mobile network connection is up
		off	Mobile network connection is down
WLAN	green	blinking slowly	Mobile connection is being established
		on	WLAN connection is up
		off	WLAN connection is down
VPN	green	on	VPN connection is up
		off	VPN connection is down
GPS	green	on	Service is enabled and valid GPS data is received and transmitted
		off	No GPS data transmitted (not available or service disabled)
Link/Activity (Ethernet Ports)	green	on	Physical link
		off	No physical link
		flashing	Data transmission

Table 8: NB2600R indicators on the front panel

The following table describes the other components on the front panel:

Label	Description
USB	USB B Port for device management
Reset	Restart: press this button when the status LED is on Factory reset: press and hold this button for at least 5 seconds.
SIM 1	SIM slot 1
SIM 2	SIM slot 2 (backup slot for SIM alternative mobile network operator)
Ethernet 1-5	M12 Ethernet Socket
⏚	Earth protection connector Use a yellow-green marked cable with at least 6mm2 cupper area. Avoid corrosion. Protect the screws against loosening.
Power	M12 power socket, max current: 1A Nominal voltages: 24VDC, 36VDC and 48VDC according to EN50155 Voltage range: 20VDC to 50VDC, -15% / +20% Galvanic isolation of the power supply, isolation voltage 1500V Maximum power consumption: 6W
Digital I/O	Digital inputs and outputs socket
Mobile	UMTS / GSM antenna socket Impedance: 50 Ohm Connector: TNC female
WLAN	WLAN antenna socket Impedance: 50 Ohm Connector: TNC female
GPS	GPS antenna socket Impedance: 50 Ohm Connector: TNC female Support for active GPS antennas

Table 9: NB2600R other components on the front panel

2.5.2 Pin Assignments

2.5.2.1 Power

Pin:	Signal
1	V+ (20-50V=)
2	Not connected
3	V_{GND}
4	Not connected

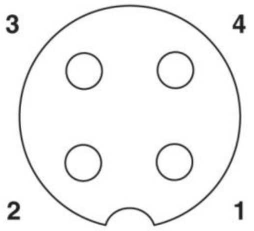


Image 1: M12 4-pole A-coded

2.5.2.2 Ethernet

Pin:	Signal
1	Tx+
2	Rx+
3	Tx-
4	Rx-

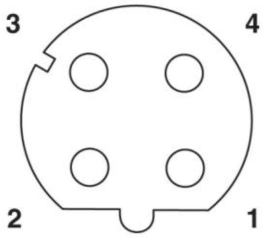


Image 2: M12 4-pole D-coded

2.5.2.3 Digital I/0

Pin:	Signal
1	In1 +
2	In1 -
3	In2 +
4	In2 -
5	Out1: Dry contact relay Normally open
6	
7	Out2: Dry contact relay Normally closed
8	

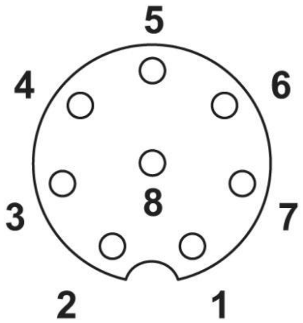


Image 3: M12 8-pole A-coded

3 Application Overview

NetBox is an access router for mobile telecom networks. NetBox can hook up a whole local area network to the mobile telecom network. Certainly NetBox can also be used to attach a single device.

3.1 Mobile Internet Access

NetBox can be used for mobile Internet access. Supported services include:

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

3.2 Access to a Remote Network

NetBox can be used to access a remote network. Possible setups are

- Access via public IP address
- Access via NetBox initiated VPN
- Access via CSD Dial-in

3.3 Virtual Private Networks (VPN)

NetBox supports various types of VPN technologies. The following components are included:

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

4 Installation

4.1 Environmental Conditions

The following precaution must be taken before installing NetBox:

- Avoid direct solar radiation.
- Protect the device from humidity, steam and aggressive fluids
- Grant sufficient circulation of air around NetBox.
- For indoor use only
- Humidity: 0 to 95% (non-condensing)
- Altitude up to 4000m
- Overvoltage Category: II
- Pollution Degree: 2

The following conditions depend on the NetBox model:

	NB1310 / NB2210	NB2500 / NB2600	NB2600R
Temperature range	0 °C to +55 °C	-25 °C to +70 °C	-25 °C to +70 °C
Mains Voltage Ripple	±10%	±10%	-15% / +20%

4.2 Installation of the Router

NetBox is designed for mounting to a panel using through holes or to be put on a worktop. Please consider the safety instructions (chapter 1.1) and the environmental conditions (chapter 4.1).

4.2.1 Installation of the SIM Card(s)

The router incorporates one or two separate SIM card sockets so that if your application demands it, you may install SIM cards for two different networks. If you only use one SIM card insert it in SIM socket 1. Make sure the SIM is suitable for data transmission.

4.2.2 Installation of the UMTS/GSM Antenna

NetBox Wireless Routers will only operate reliably over the GSM network if there is a good signal. For many applications the flexible stub antenna provided will be suitable but in some circumstances it may be necessary to use a remote antenna with an extended cable to allow the antenna itself to be positioned to provide the best possible signal reception. NetModule can supply a range of suitable antennas.

Consider the effects caused by Faraday cages such as large metal surfaces (elevators, machine housings, etc.), close meshed iron constructions.

Fit the antenna or connect the antenna cable to the GSM antenna connector.

4.2.3 Installation of the GPS Antenna

Use active GPS antennas for best signal reception. NB1310 and NB2500 require passive GPS antennas.

4.2.4 Installation of the Local Area Network

Up to five Ethernet devices can directly be connected to the NetBox.

4.2.5 Installation of the Power Supply

NetBox can be powered with the included power supply or another external source supplying between 9 and 32 Volts DC (9-28 Volts DC NB2210). NetBox is for use with certified (CSA or equivalent) power supply, which must have a limited and SELV circuit output.

5 Configuration

NetBox holds different configurations, such as the factory configuration and the user configuration. The user configuration can be modified by the user as follows:

- Using the Web Manager (chapter 5.1)
- Upload a new configuration file using the Web Manager (chapter 5.2.3)
- Using the NetBox Command Line Interface (chapter 5.2)

If you are new to NetBox we recommend configuring it using the NetBox Web Manager. For batch configuration upload configuration files.

5.1 Configuration via the NetBox Web Manager

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

The minimum configuration steps usually include:

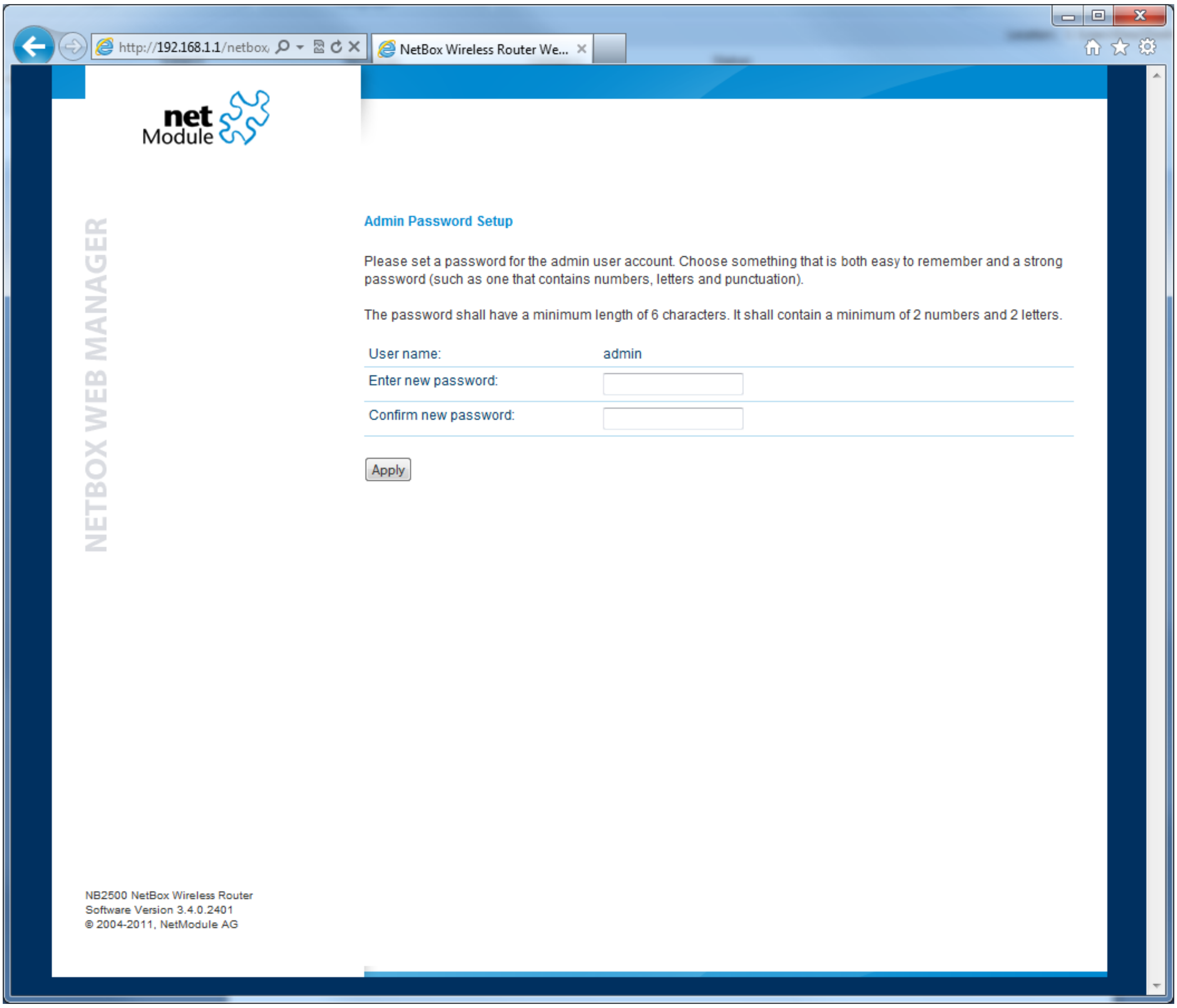
1. defining the admin password
2. entering the PIN code for the SIM card
3. configuring the Access Point Name (APN)
4. start the mobile connection

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

5.1.1 Initial Access to the Web Manager and Password Definition

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

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



Admin Password Setup

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

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

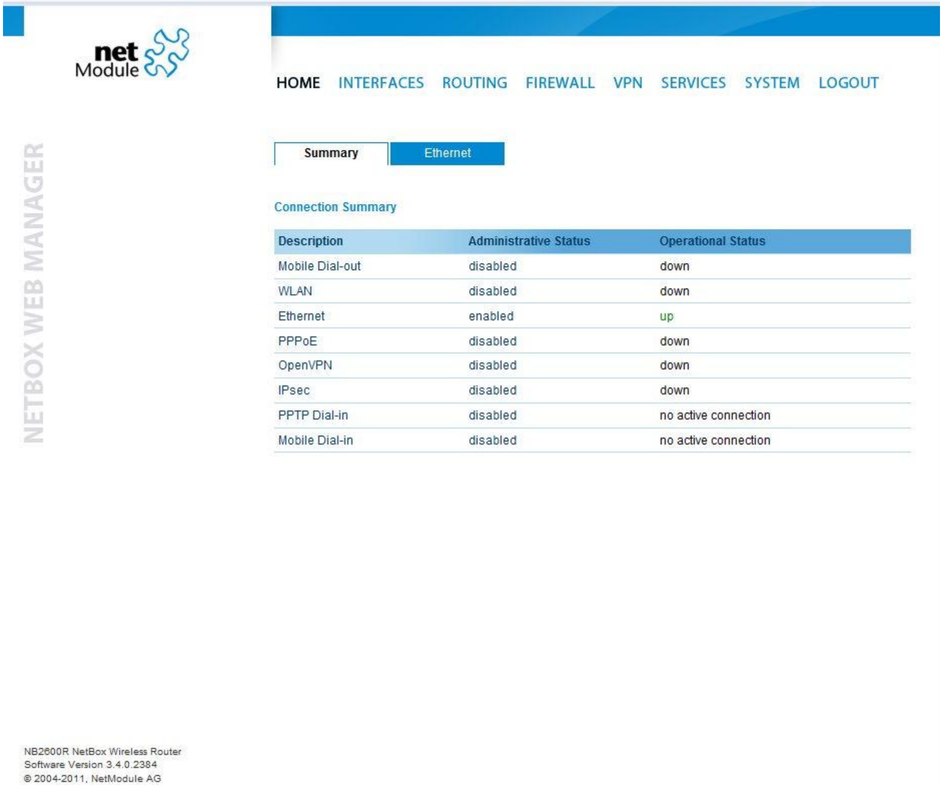
User name:	admin
Enter new password:	
Confirm new password:	

Apply

NB2500 NetBox Wireless Router
Software Version 3.4.0.2401
© 2004-2011, NetModule AG

5.1.2 Home

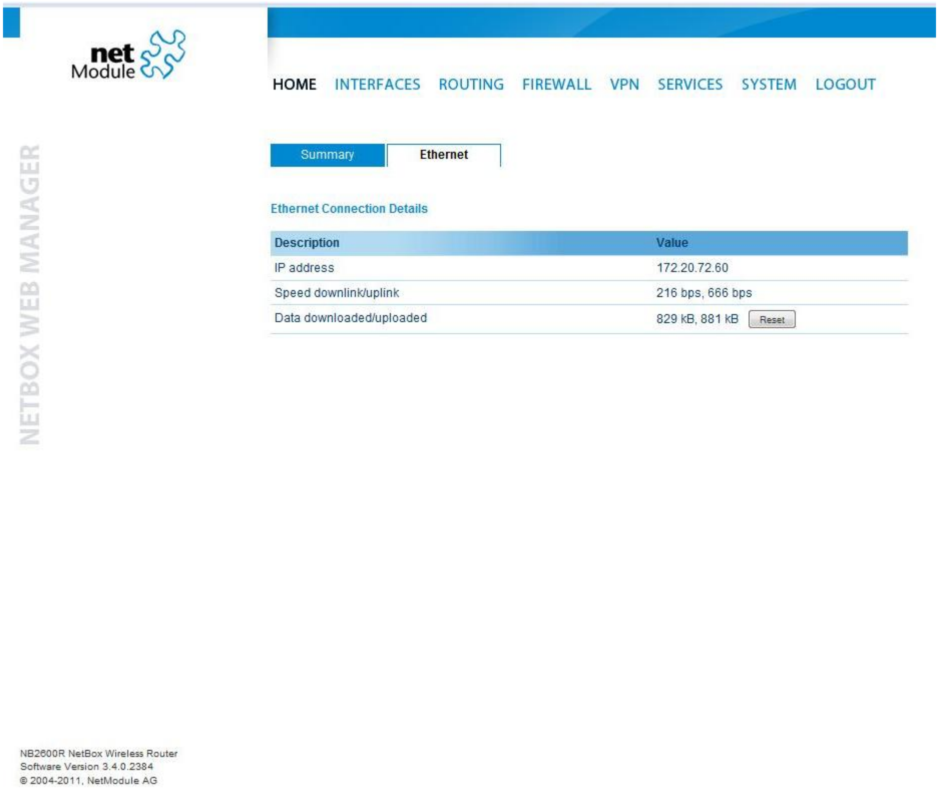
This page gives you a system overview. It helps you when initially setting up device but also functions as dashboard during normal operation.



Connection Summary

Description	Administrative Status	Operational Status
Mobile Dial-out	disabled	down
WLAN	disabled	down
Ethernet	enabled	up
PPPoE	disabled	down
OpenVPN	disabled	down
IPsec	disabled	down
PPTP Dial-in	disabled	no active connection
Mobile Dial-in	disabled	no active connection

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG



Ethernet Connection Details

Description	Value
IP address	172.20.72.60
Speed downlink/uplink	216 bps, 666 bps
Data downloaded/uploaded	829 kB, 881 kB

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG

5.1.3 Interfaces

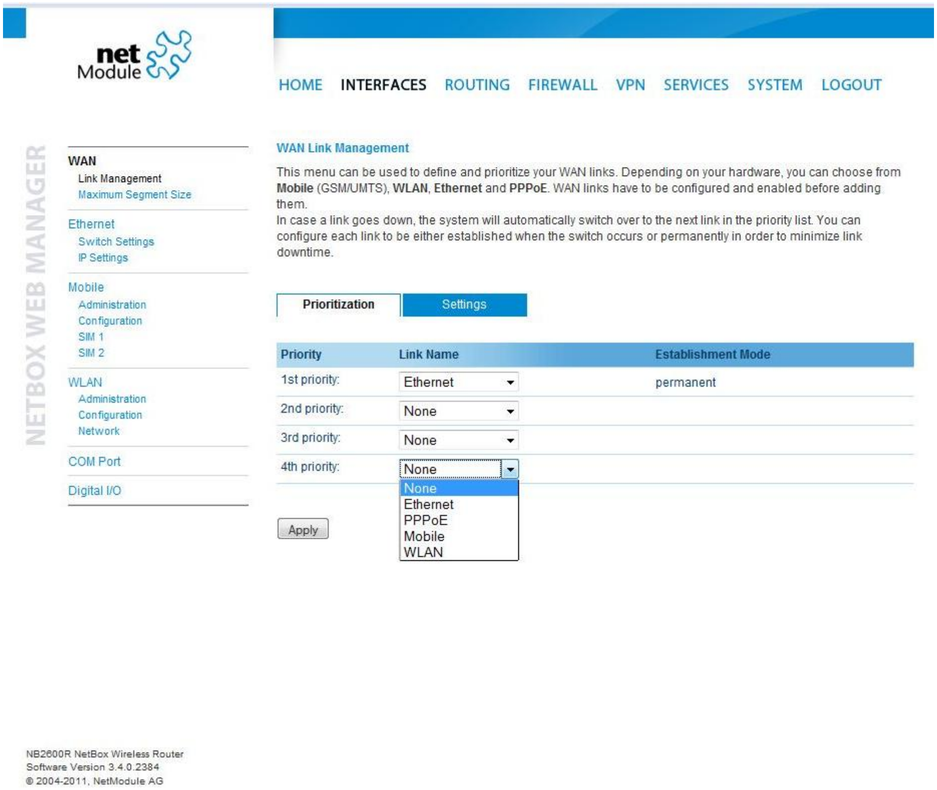
In the section the physical Interfaces of NetBox are configured.

5.1.3.1 WAN

5.1.3.1.1 Link Management

NBSW 3.4 introduces a WAN link manager. Depending on your hardware, you can choose from **Mobile** (GSM/UMTS), **WLAN**, **Ethernet** and **PPPoE**. WAN links have to be configured and enabled before adding them.

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



WAN Link Management

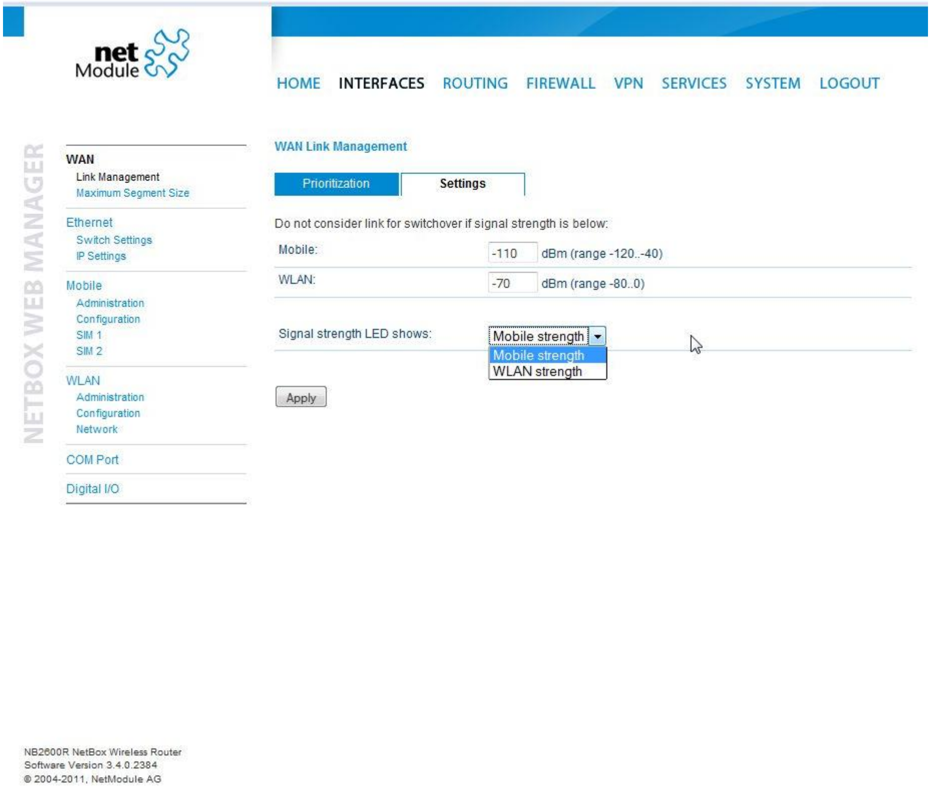
This menu can be used to define and prioritize your WAN links. Depending on your hardware, you can choose from **Mobile** (GSM/UMTS), **WLAN**, **Ethernet** and **PPPoE**. WAN links have to be configured and enabled before adding them.

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

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

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG

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



WAN Link Management

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

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

WLAN: -70 dBm (range -80..0)

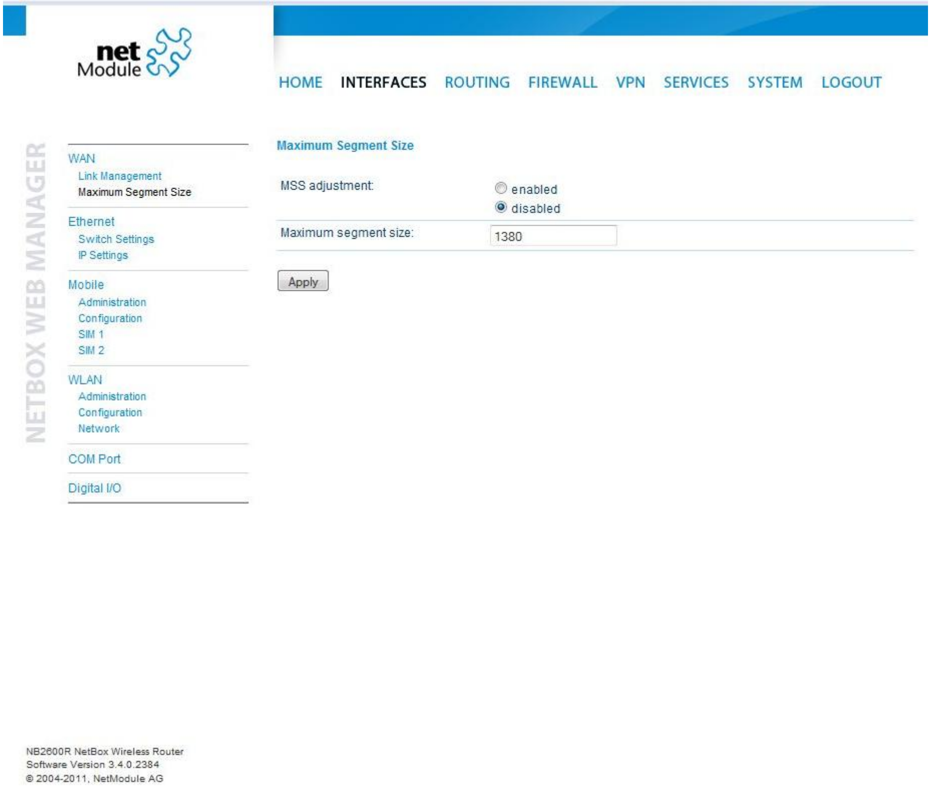
Signal strength LED shows: Mobile strength

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG

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

5.1.3.1.2 Maximum Segment Size

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



Maximum Segment Size

MSS adjustment: ○ enabled ● disabled

Maximum segment size: 1380

Apply

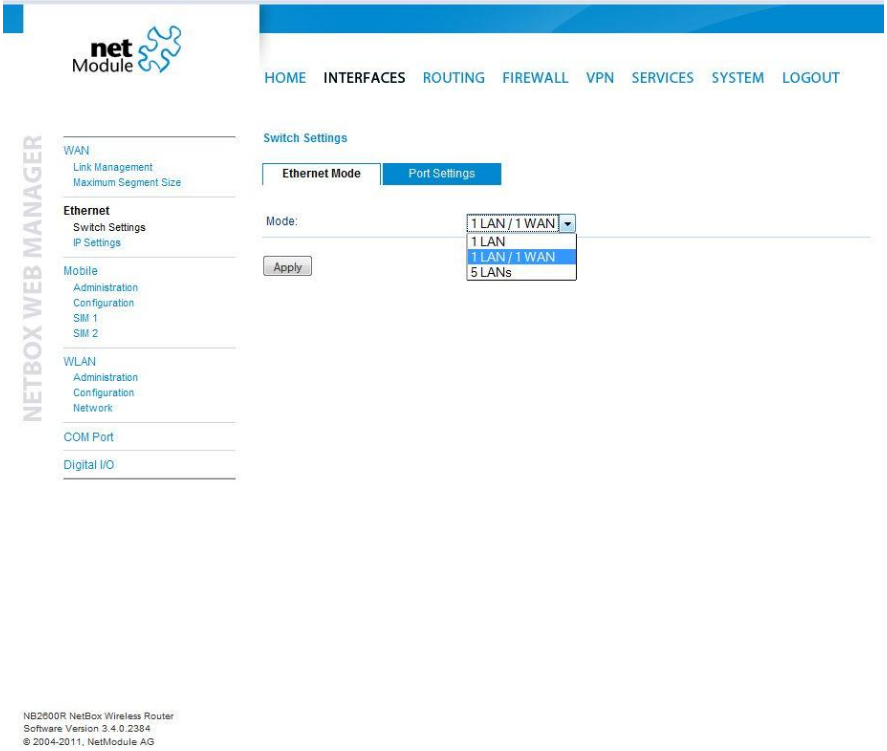
NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG

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

5.1.3.2 Ethernet Interface

5.1.3.2.1 Switch Settings

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



Switch Settings

Mode: 1 LAN / 1 WAN

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG

Depending on the Ethernet mode chosen above one network or four networks can be defined. The factory defaults are as follows:

Combined mode (LAN)

Ports	Network	NetBox IP Address
Port 1, 2, 3, 4, (5)	192.168.1.0/24	192.168.1.1

Mixed mode (LAN / WAN)

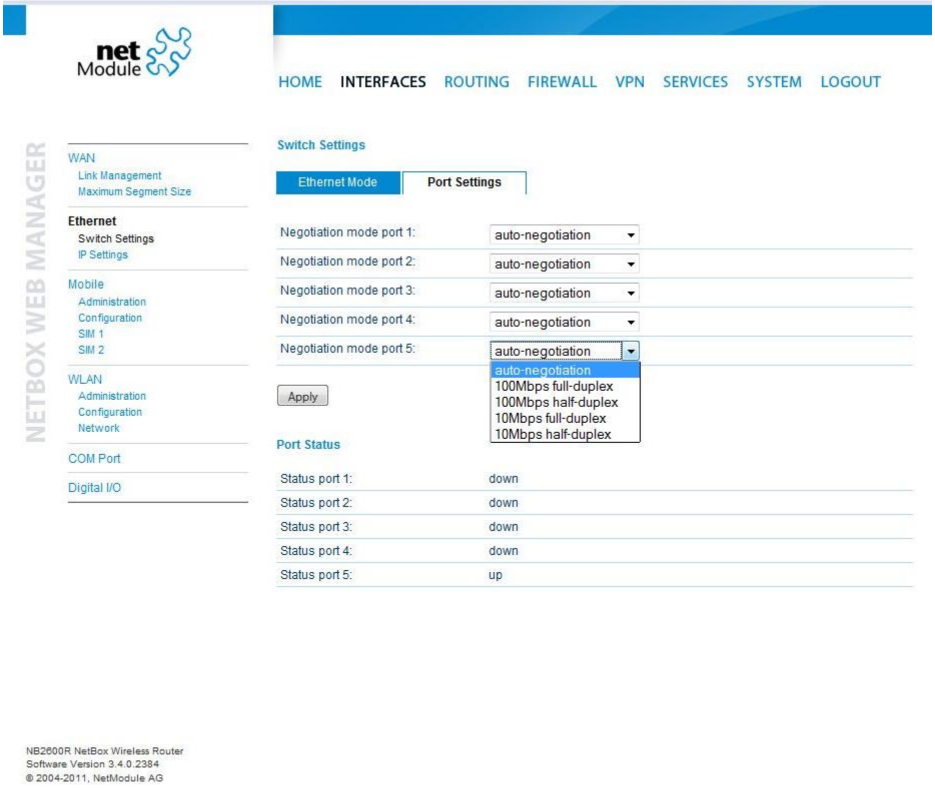
Ports	Network	NetBox IP Address
Port 1-3 (NB2500) Port 1-4 (NB2600R)	192.168.1.0/24	192.168.1.1
Port 4 (NB2500/NB2600) Port 5 (NB2600R)	192.168.2.0/24	192.168.2.1

Separated mode (LANs)

Ports	Network	NetBox IP Address
Port 1	192.168.1.0/24	192.168.1.1
Port 2	192.168.2.0/24	192.168.2.1
Port 3	192.168.3.0/24	192.168.3.1
Port 4	192.168.4.0/24	192.168.4.1
Port 5 (NB2600R)	192.168.5.0/24	192.168.5.1

Port Settings:

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



Negotiation mode port 1:	auto-negotiation
Negotiation mode port 2:	auto-negotiation
Negotiation mode port 3:	auto-negotiation
Negotiation mode port 4:	auto-negotiation
Negotiation mode port 5:	auto-negotiation

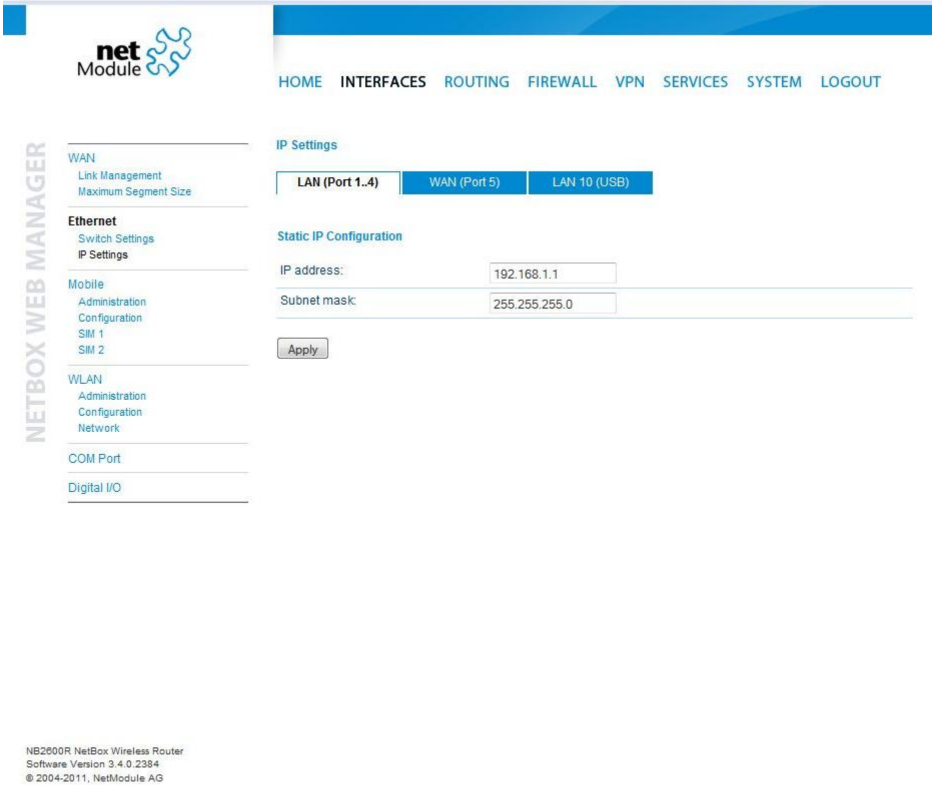
Port Status

Status port 1:	down
Status port 2:	down
Status port 3:	down
Status port 4:	down
Status port 5:	up

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG

5.1.3.2.2 IP Settings

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



IP Settings

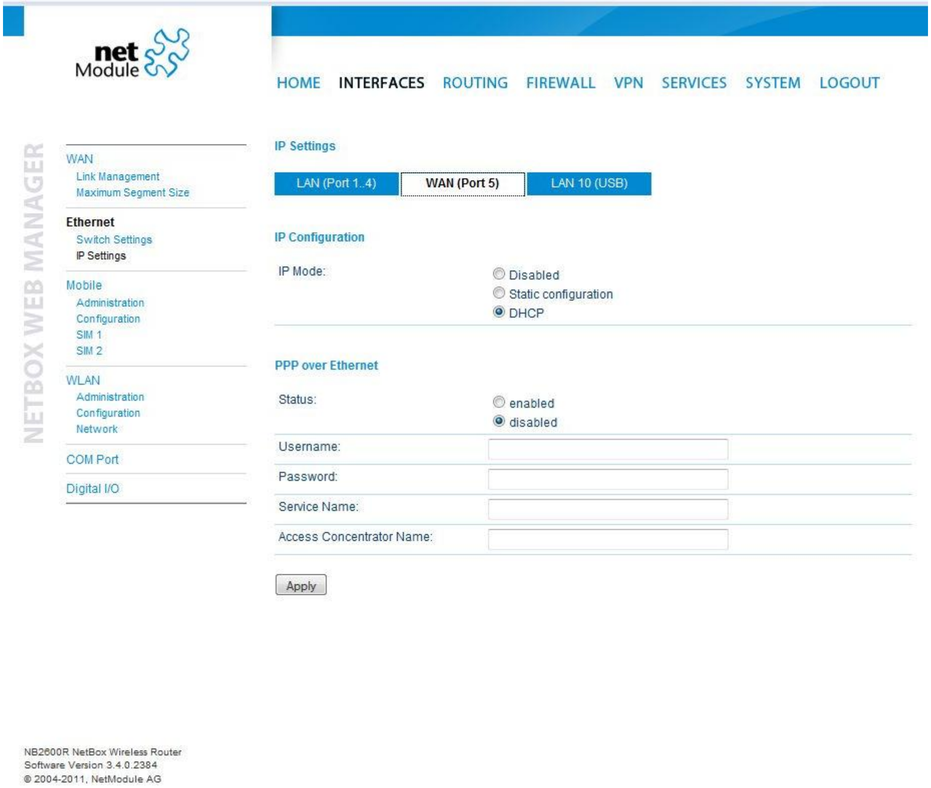
Static IP Configuration

IP address: 192.168.1.1

Subnet mask: 255.255.255.0

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG

5.1.3.2.2.1 WAN



IP Settings

IP Configuration

IP Mode: ○ Disabled ○ Static configuration ● DHCP

PPP over Ethernet

Status: ○ enabled ● disabled

Username:

Password:

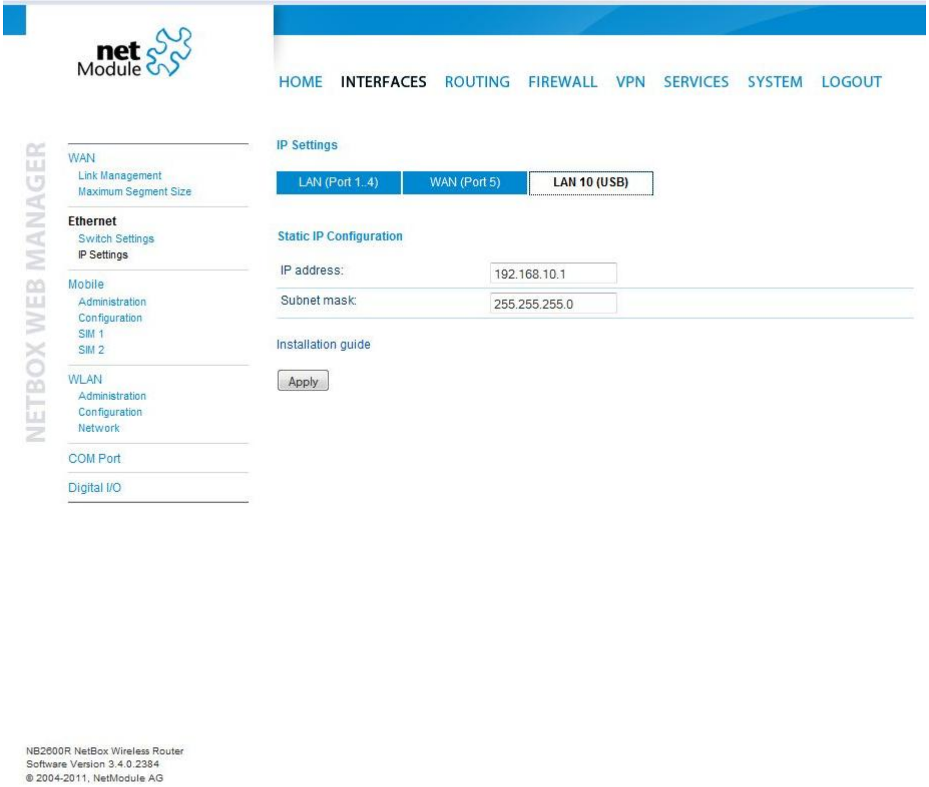
Service Name:

Access Concentrator Name:

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG

Parameter	Description
IP mode:	Disabled means that the IP interface will be left unconfigured. Static configuration allows you to set the IP parameters DHCP means that the IP configuration will be retrieved from an external DHCP server.
Status:	Enable or disable the PPPoE connection
User name:	PPPoE user name
Password:	PPPoE password
Service name:	Specifies the service name set on the access concentrator. Leave it blank unless you have many services and need to specify the one you need to connect to
Access concentrator name:	This may be left blank and the client will connect to any access concentrator.

5.1.3.2.2.2 LAN 10



IP Settings

Static IP Configuration

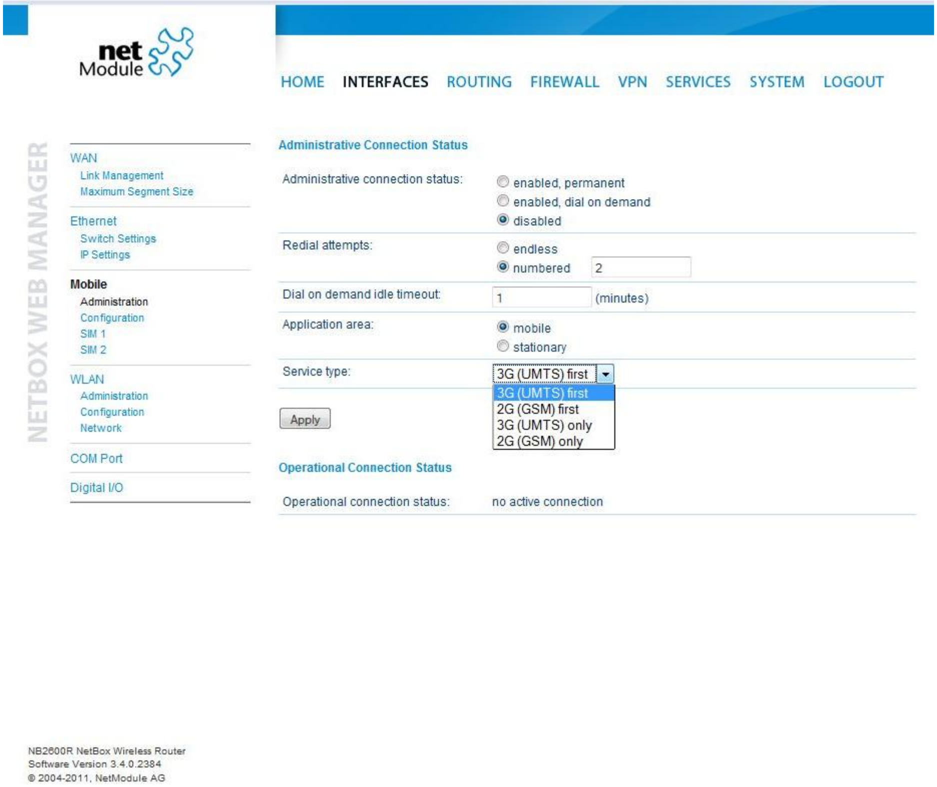
IP address:	192.168.10.1
Subnet mask:	255.255.255.0

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG

5.1.3.3 Mobile Interface

5.1.3.3.1 Administration

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



Administrative Connection Status

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

Redial attempts: ○ endless ● numbered 2

Dial on demand idle timeout: 1 (minutes)

Application area: ● mobile ○ stationary

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

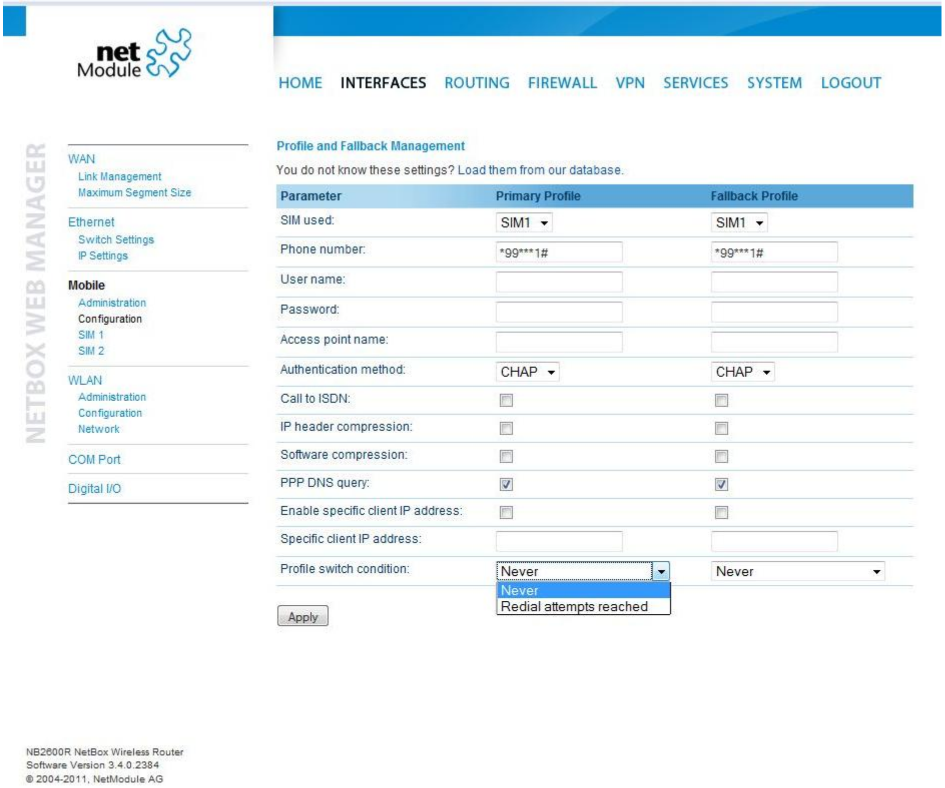
Operational Connection Status

Operational connection status: no active connection

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG

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

5.1.3.3.2 Configuration



Profile and Fallback Management

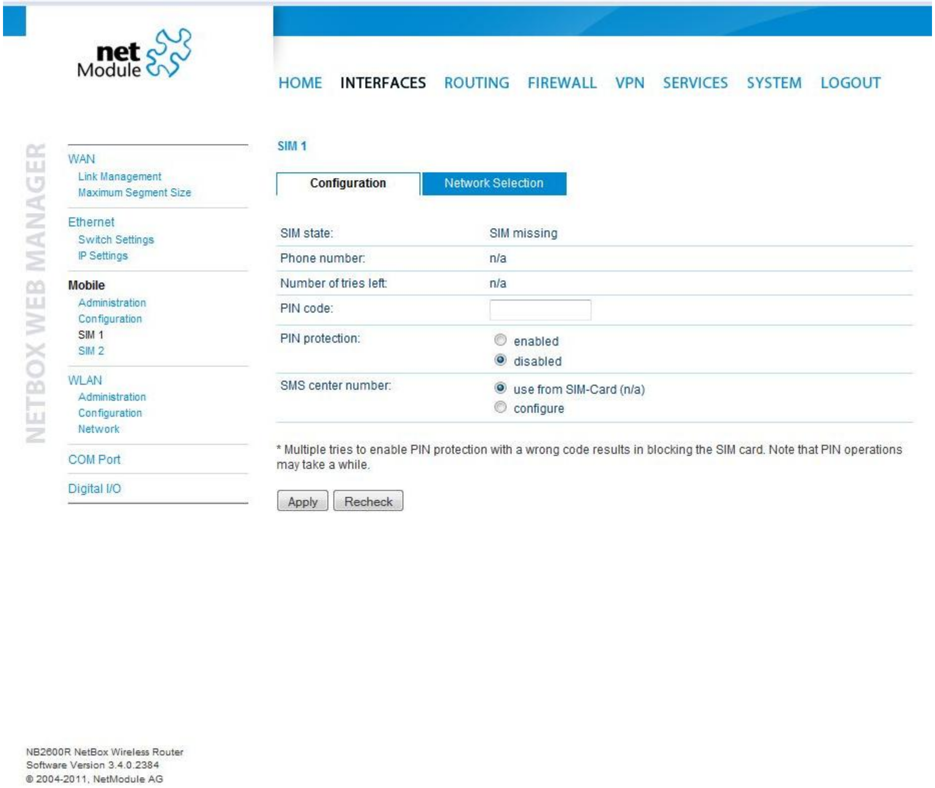
You do not know these settings? Load them from our database.

Parameter	Primary Profile	Fallback Profile
SIM used:	SIM1	SIM1
Phone number:	*99***1#	*99***1#
User name:		
Password:		
Access point name:		
Authentication method:	CHAP	CHAP
Call to ISDN:	□	□
IP header compression:	□	□
Software compression:	□	□
PPP DNS query:	☑	☑
Enable specific client IP address:	□	□
Specific client IP address:		
Profile switch condition:	Never Never Redial attempts reached	Never

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG

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

5.1.3.3.3 SIM



SIM 1

SIM state:	SIM missing
Phone number:	n/a
Number of tries left:	n/a
PIN code:	
PIN protection:	○ enabled ● disabled
SMS center number:	● use from SIM-Card (n/a) ○ configure

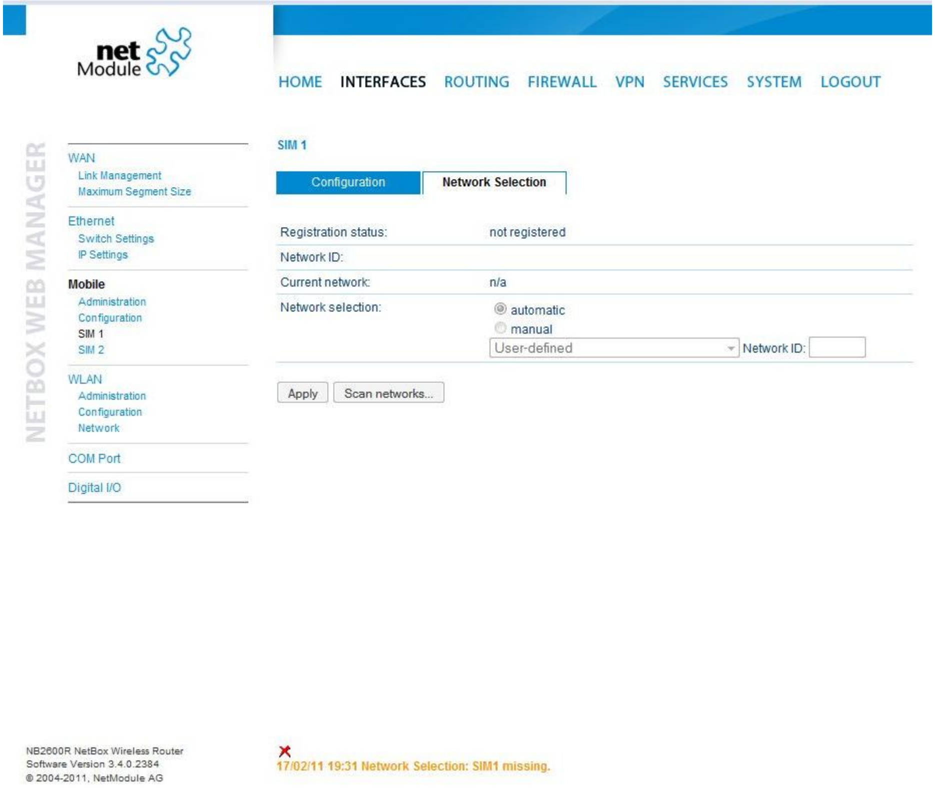
* Multiple tries to enable PIN protection with a wrong code results in blocking the SIM card. Note that PIN operations may take a while.

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG

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

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

Parameter	Description
PIN code:	The PIN code for the SIM card
PIN protection:	Enable or disable PIN protection
SMS center number:	Number of Short Message Service Centers (SMSCs) for sending Mobile Originating (MO) SMS messages Contact your mobile operator or search the Internet if you do not know the number. A list is found here: http://umtslink.at/sms/smsc_rufnummern.htm



SIM 1

Registration status: not registered

Network ID:

Current network: n/a

Network selection: ● automatic ○ manual

User-defined Network ID:

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG

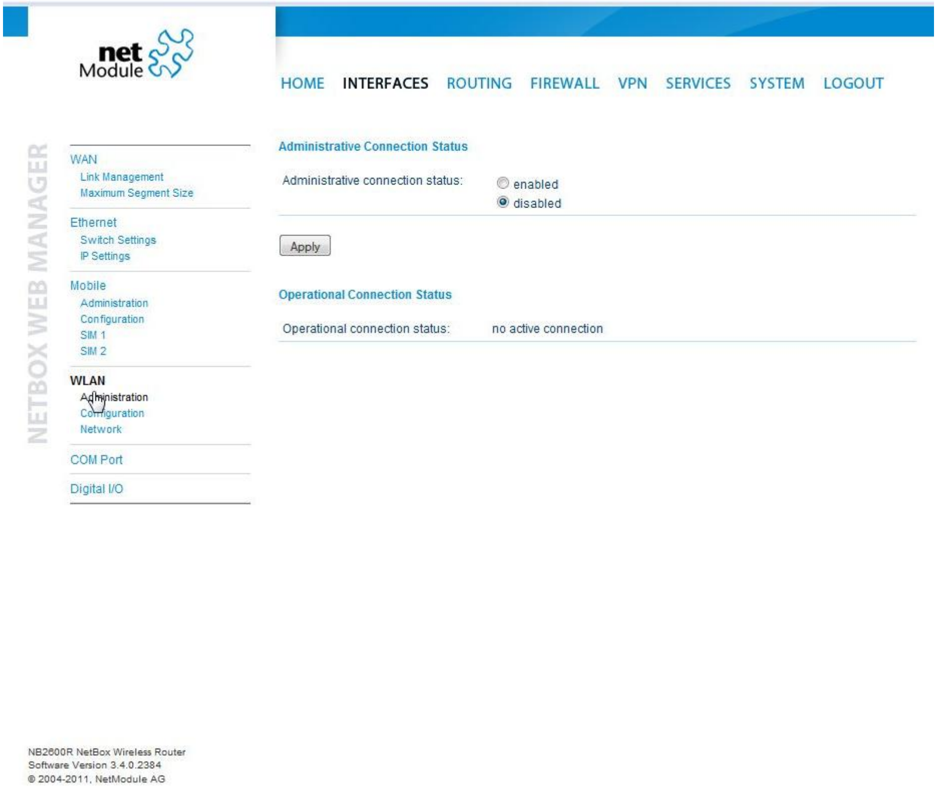
17/02/11 19:31 Network Selection: SIM1 missing.

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

5.1.3.4 WLAN

5.1.3.4.1 WLAN Administration

WLAN is enabled or disabled on this page.



Administrative Connection Status

Administrative connection status: ○ enabled ● disabled

Apply

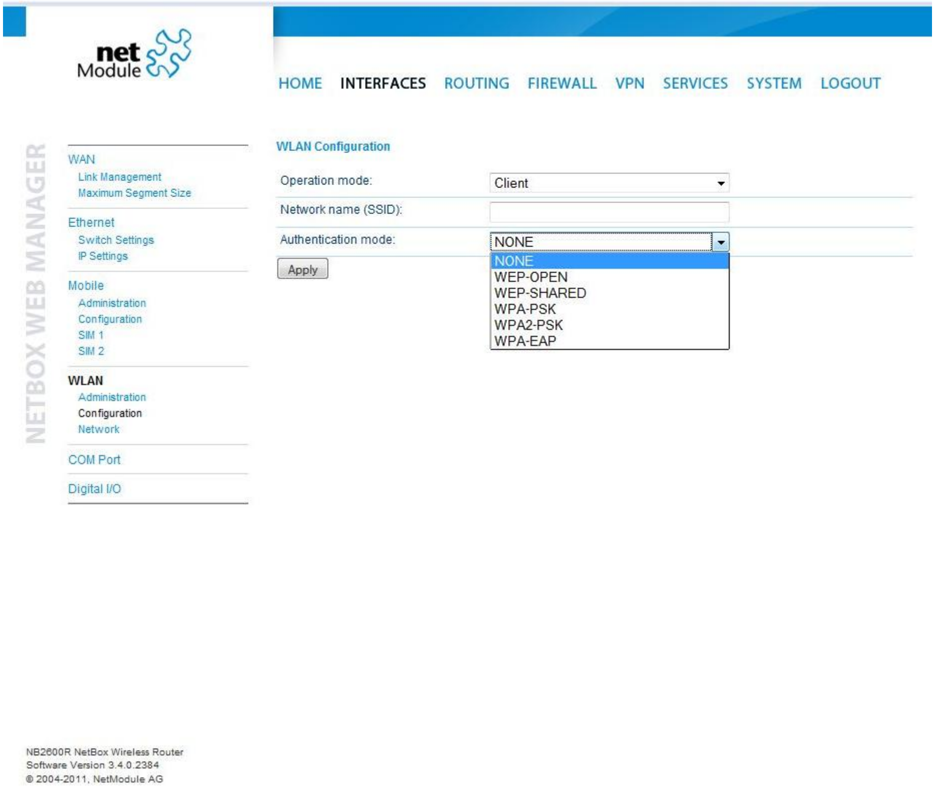
Operational Connection Status

Operational connection status: no active connection

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG

5.1.3.4.2 WLAN Configuration

The WLAN interface can be operated in client or access point mode. In client mode it will be an additional WAN link, in access point mode it will serve as WLAN access point.



WLAN Configuration

Operation mode: Client

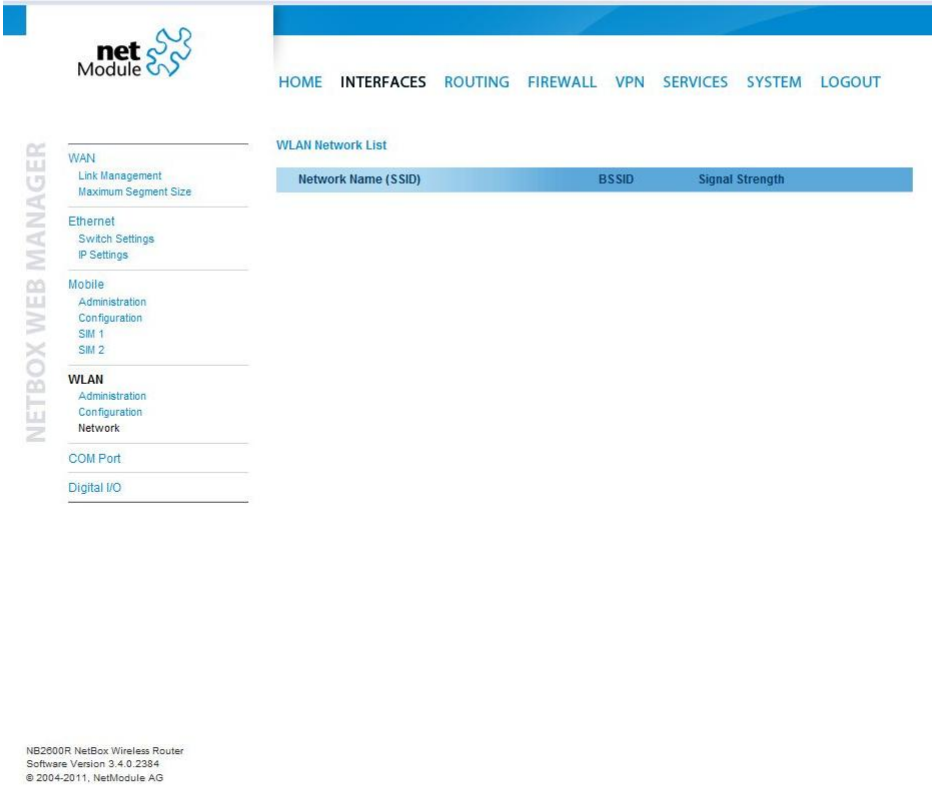
Network name (SSID):

Authentication mode: NONE

Apply

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG

5.1.3.4.3 WLAN Network List

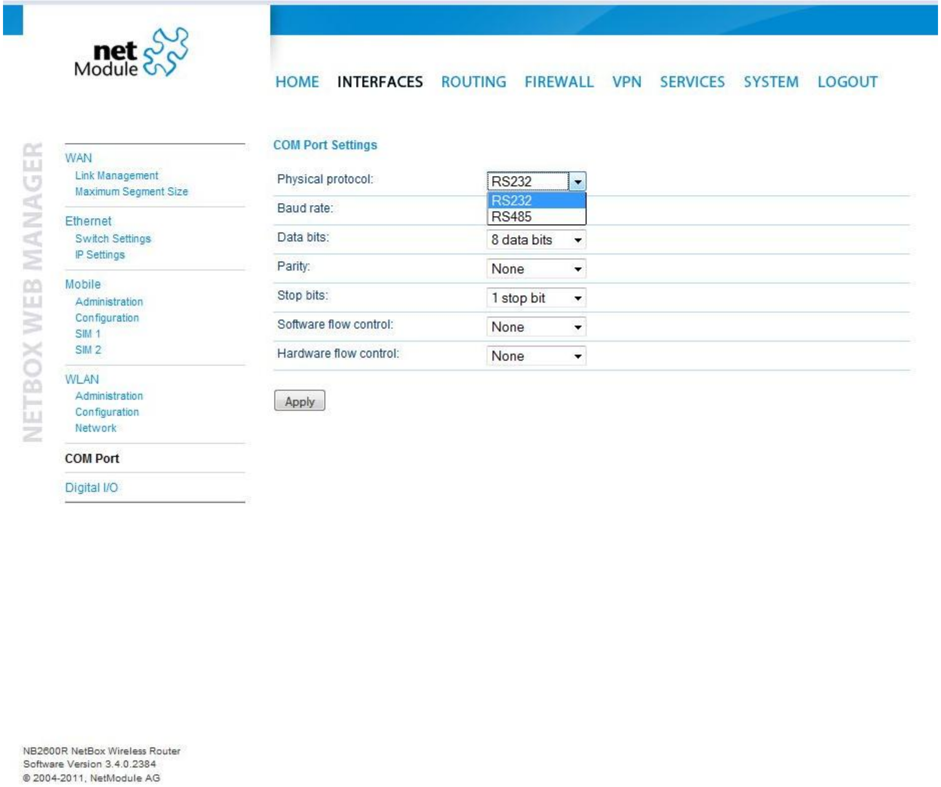


WLAN Network List

Network Name (SSID)	BSSID	Signal Strength

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG

5.1.3.5 COM Port



COM Port Settings

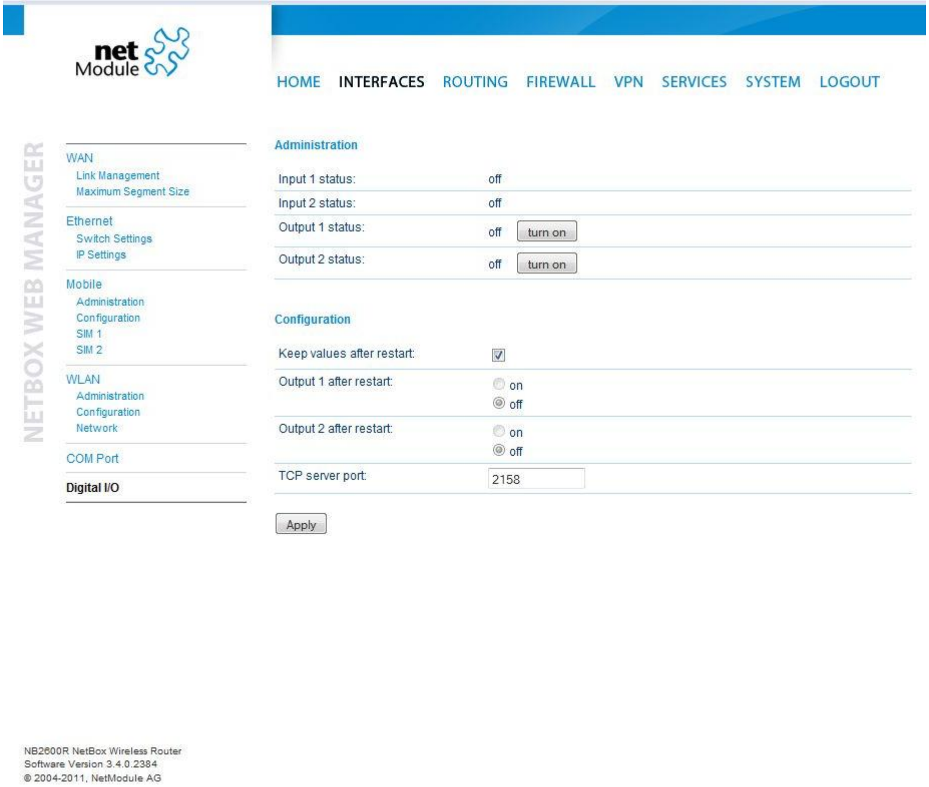
Physical protocol: RS232
Baud rate:
Data bits: 8 data bits
Parity: None
Stop bits: 1 stop bit
Software flow control: None
Hardware flow control: None

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG

Parameter	Description
Physical protocol:	RS232 or RS485.
Baud rate:	This property specifies the baud rate of the COM port
Data bits:	This property specifies the number of data bits contained in each frame.
Parity:	This property specifies the parity used with every frame that is transmitted or received.
Stop bits:	This property specifies the number of stop bits used to indicate the end of a frame.
Software support	In XON/XOFF software flow control, either end can send a stop (XOFF) or start (XON) character to the other end to control the rate of incoming data.
Hardware flow control	In RTS/CTS hardware flow control, the computer and the modem use the RTS and CTS lines respectively to control the flow of data

5.1.3.6 Digital I/O

The digital inputs and outputs can be monitored and controlled via the Web Manager or by software. See section 6.2 (Digital I/O Server) on how to control inputs and outputs by software.



Administration

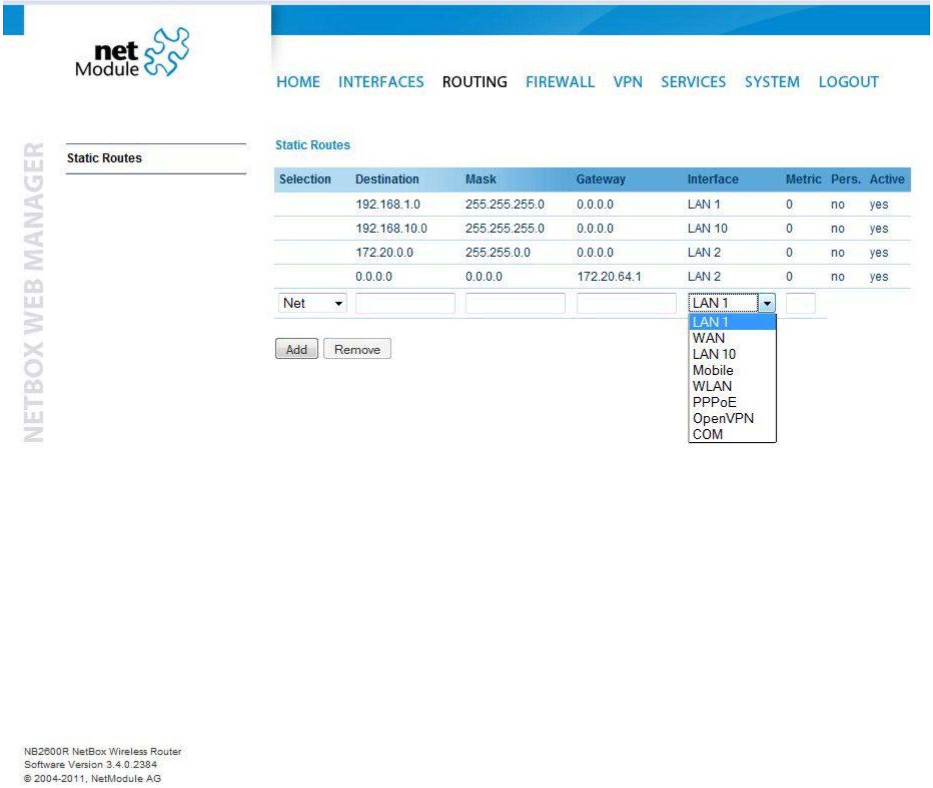
Input 1 status:	off	
Input 2 status:	off	
Output 1 status:	off	turn on
Output 2 status:	off	turn on

Configuration

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

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG

5.1.4 Routing



Static Routes

Selection	Destination	Mask	Gateway	Interface	Metric	Pers.	Active
	192.168.1.0	255.255.255.0	0.0.0.0	LAN 1	0	no	yes
	192.168.10.0	255.255.255.0	0.0.0.0	LAN 10	0	no	yes
	172.20.0.0	255.255.0.0	0.0.0.0	LAN 2	0	no	yes
	0.0.0.0	0.0.0.0	172.20.64.1	LAN 2	0	no	yes
Net				LAN 1			

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG

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

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

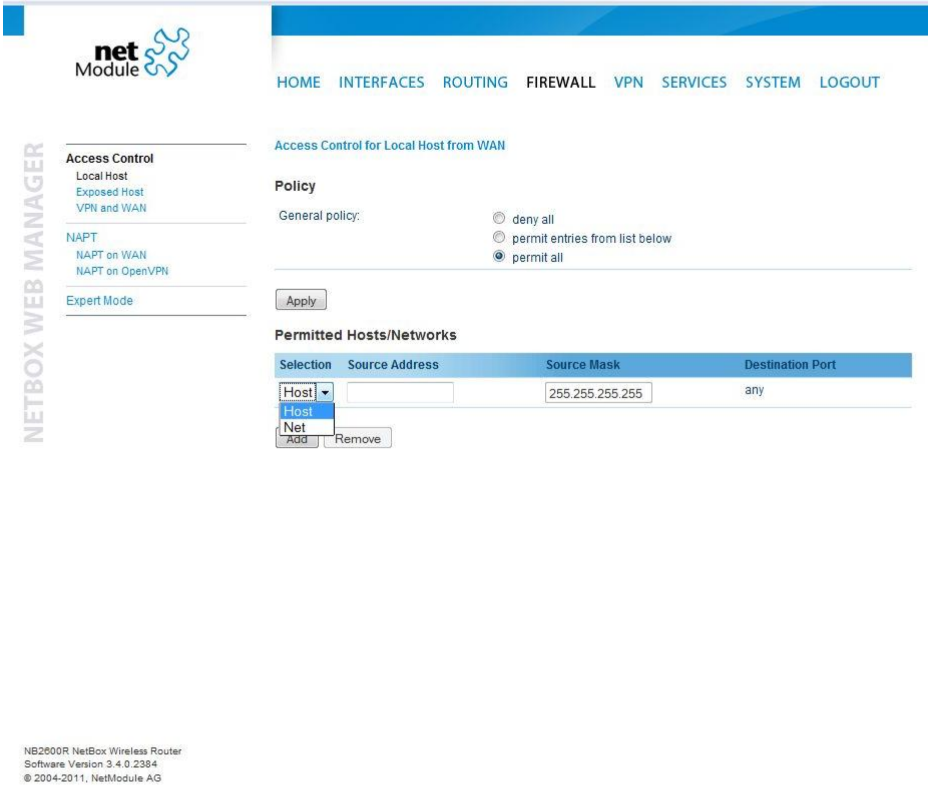
Parameter	Description
Select	To enter network route select “Net”. To enter a route to a host select “Host”.
Destination	The destination network or host. You can provide IP addresses in dotted decimal or host/network names.
Mask	The network's IP address together with its address mask defines a range of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

5.1.5 Firewall

5.1.5.1 Access Control

5.1.5.1.1 Access Control for Local Host

The access from the WAN interface to NetBox itself and its local applications can be managed using this filter.



Access Control for Local Host from WAN

Policy

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

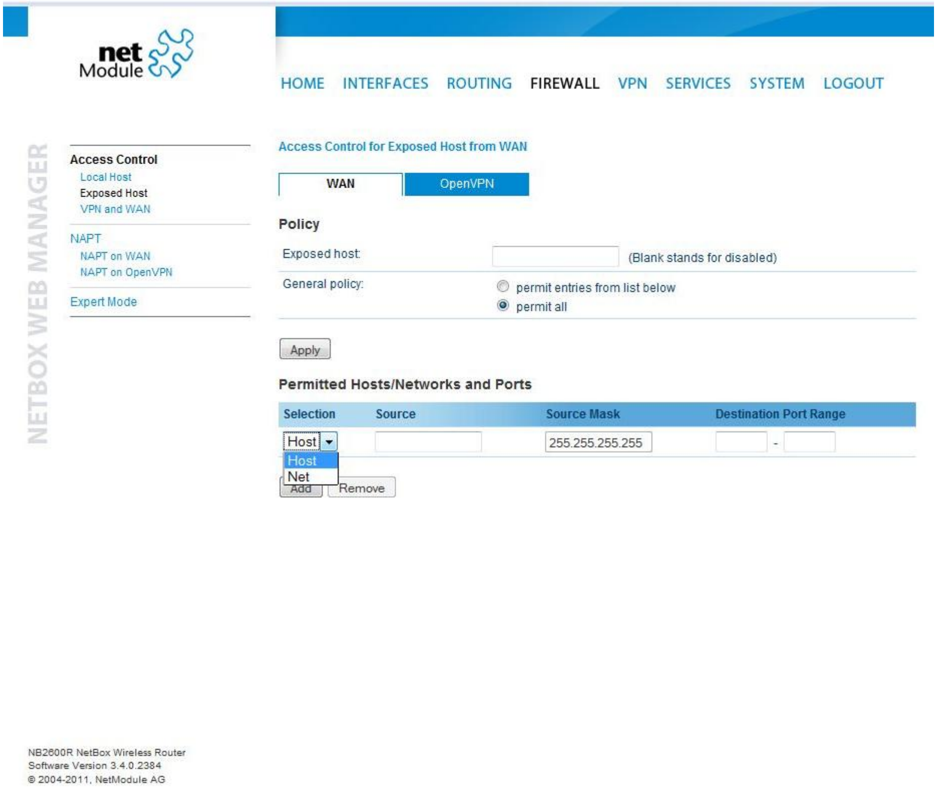
Permitted Hosts/Networks

Selection	Source Address	Source Mask	Destination Port
Host (Host, Net)		255.255.255.255	any

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG

5.1.5.1.2 Access Control for Exposed Host from WAN and OpenVPN

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



Access Control for Exposed Host from WAN

Policy

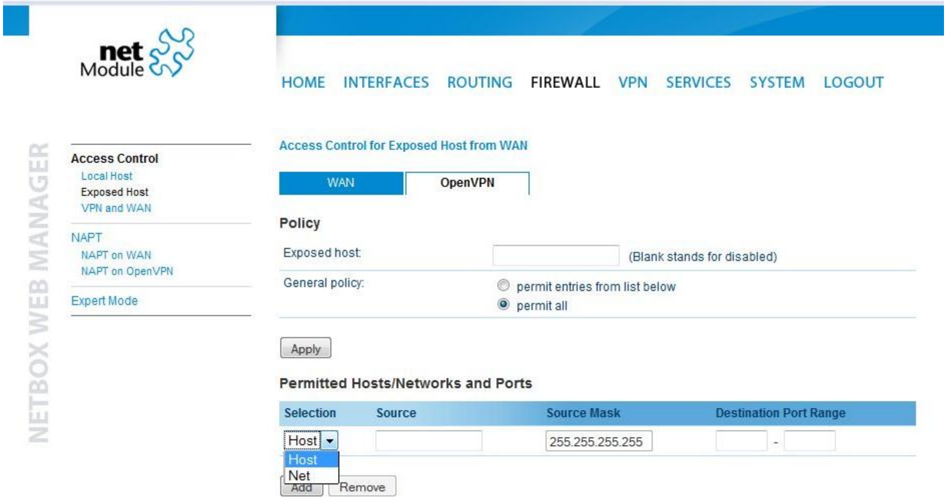
Exposed host: (Blank stands for disabled)

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

Permitted Hosts/Networks and Ports

Selection	Source	Source Mask	Destination Port Range
Host		255.255.255.255	-

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG



Access Control for Exposed Host from WAN

Policy

Exposed host: (Blank stands for disabled)

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

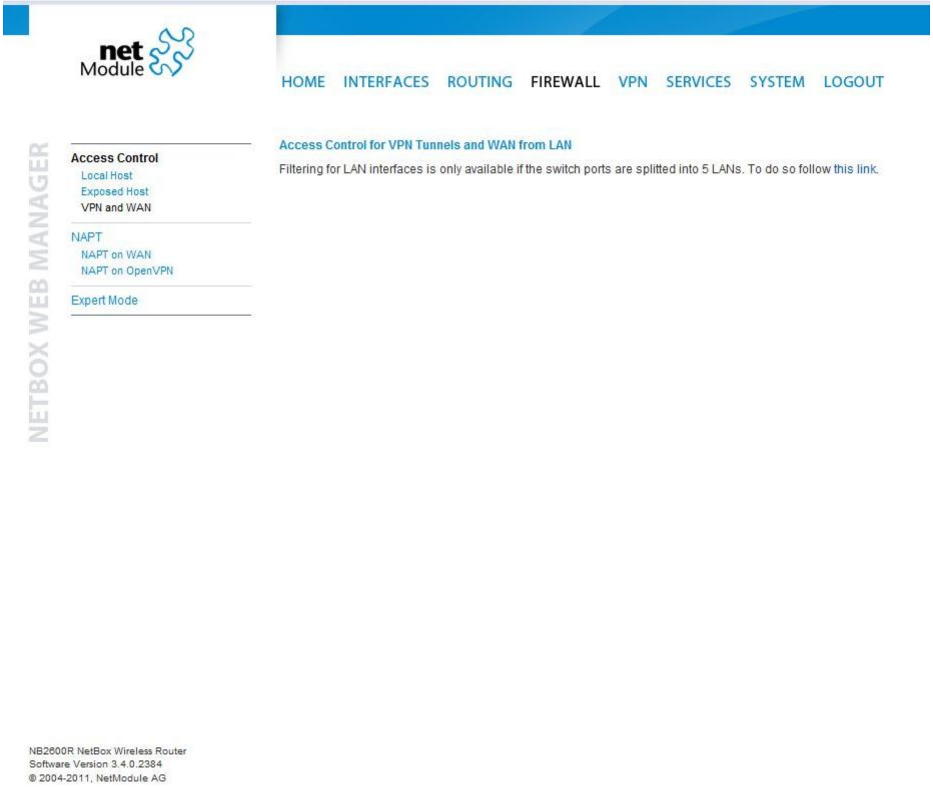
Permitted Hosts/Networks and Ports

Selection	Source	Source Mask	Destination Port Range
Host		255.255.255.255	-

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

5.1.5.1.3 Access Control for VPN Tunnels and WAN from LAN

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



Access Control for VPN Tunnels and WAN from LAN

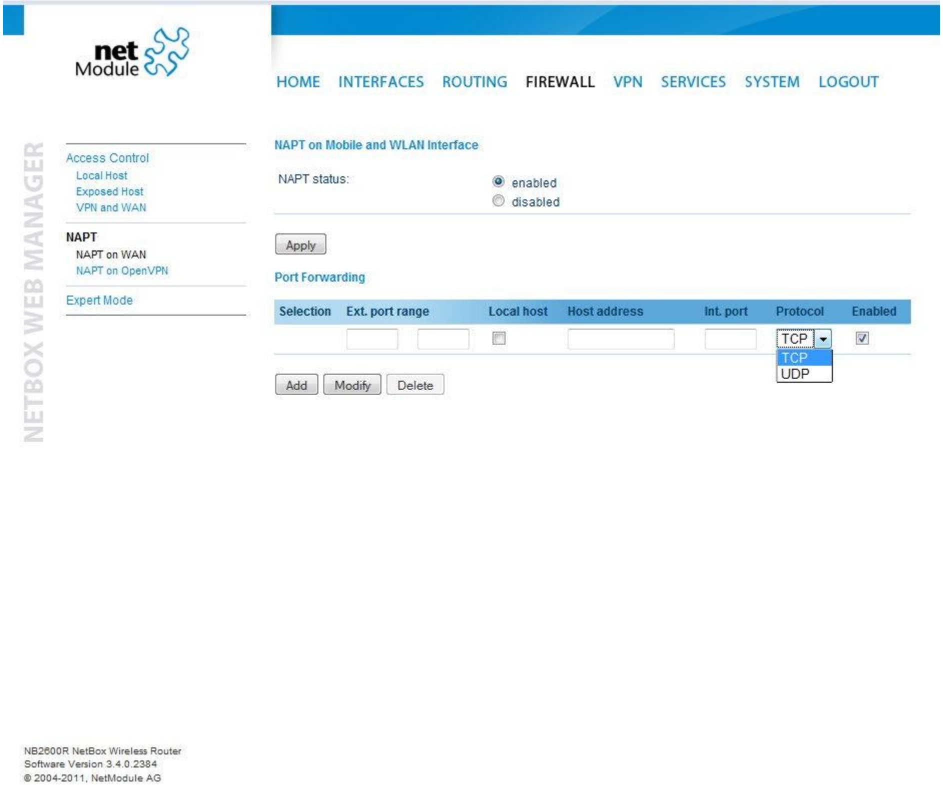
Filtering for LAN interfaces is only available if the switch ports are splitted into 5 LANs. To do so follow this link.

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG

5.1.5.2 NAPT

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

5.1.5.2.1 NAPT on Mobile Interface



NAPT on Mobile and WLAN Interface

NAPT status: ● enabled ○ disabled

Port Forwarding

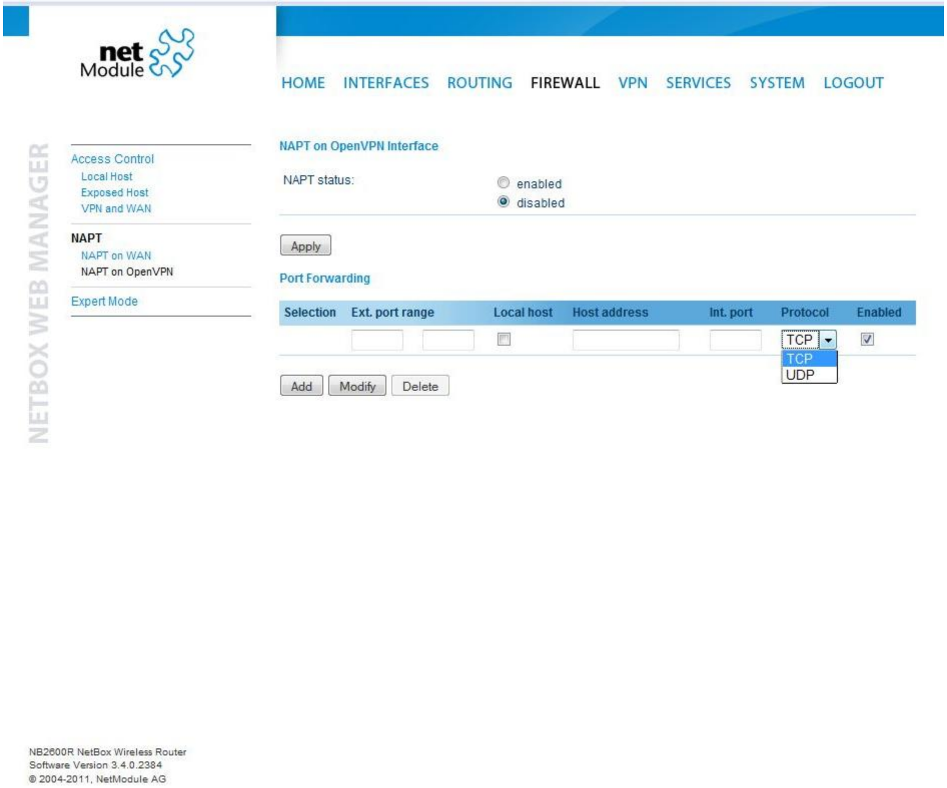
Selection	Ext. port range		Local host	Host address	Int. port	Protocol	Enabled
			□			TCP TCP UDP	☑

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG

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

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

5.1.5.2.2 NAPT on OpenVPN Interface



NAPT on OpenVPN Interface

NAPT status: ○ enabled ● disabled

Port Forwarding

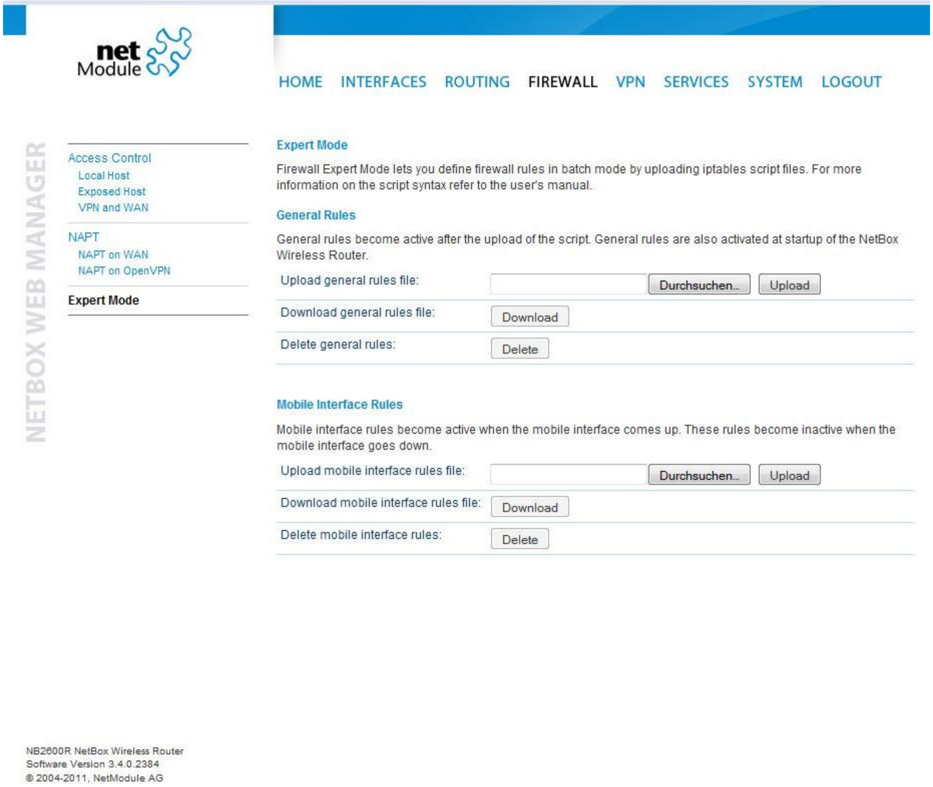
Selection	Ext. port range	Local host	Host address	Int. port	Protocol	Enabled
		□			TCP	☑

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG

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

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

5.1.5.3 Expert Mode



Expert Mode

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

General Rules

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

Upload general rules file:

Download general rules file:

Delete general rules:

Mobile Interface Rules

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

Upload mobile interface rules file:

Download mobile interface rules file:

Delete mobile interface rules:

NB2600R NetBox Wireless Router
Software Version 3.4.0.2384
© 2004-2011, NetModule AG

Upload text files with firewall rules.

5.1.6 VPN

5.1.6.1 OpenVPN

Install an OpenVPN Server or subscribe to the appropriate service. NetModule provides OpenVPN servers as hardware or as hosted service.

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

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

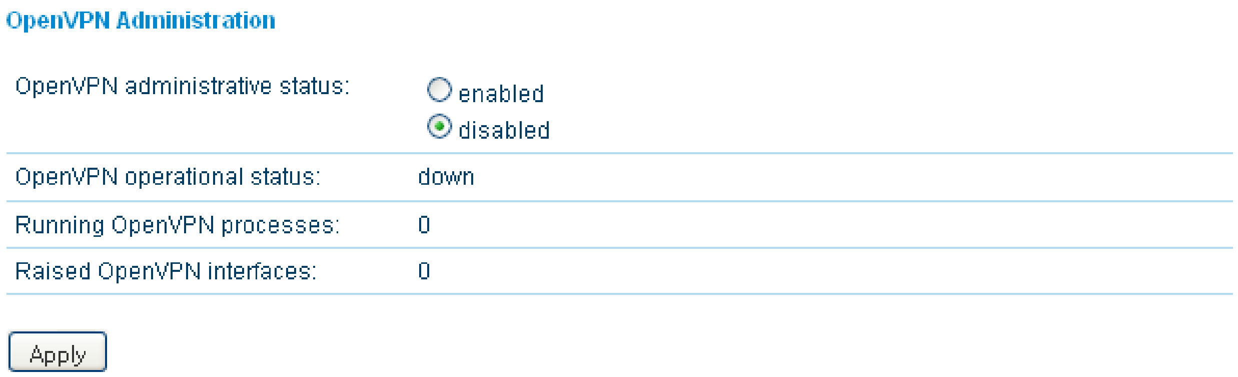
Prepare the OpenVPN certificate files. Use the tools and documentation that come with the OpenVPN software. A Guide to basic RSA Key Management is found under http://openvpn.net/easyrsa.html

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

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

Please make sure that the NetBox system time is correct when working with OpenVPN. Otherwise authentication issues may arise.

5.1.6.1.1 OpenVPN Administration

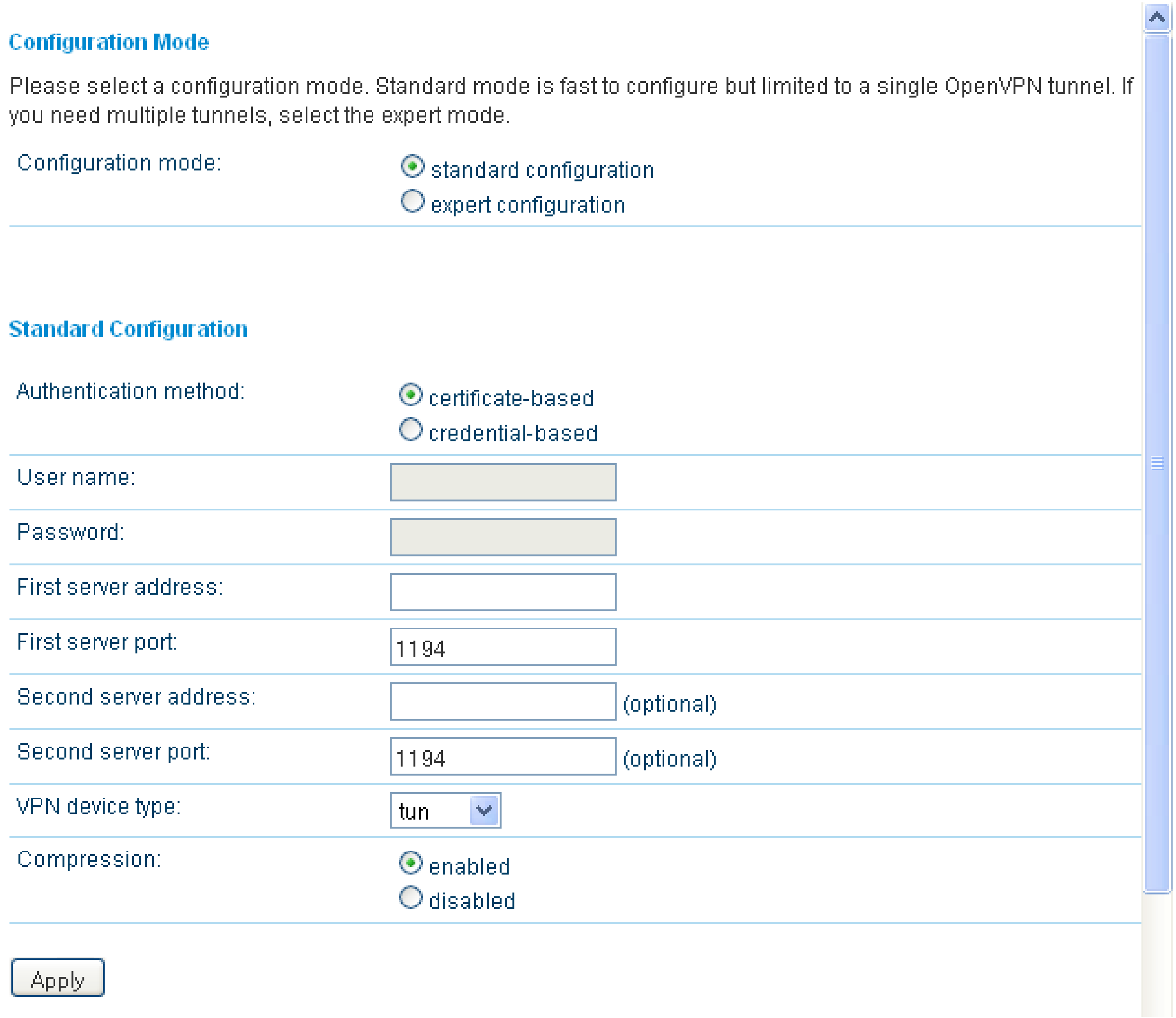


OpenVPN Administration

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

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

5.1.6.1.2 OpenVPN Configuration (Standard Client Configuration)



Configuration Mode

Please select a configuration mode. Standard mode is fast to configure but limited to a single OpenVPN tunnel. If you need multiple tunnels, select the expert mode.

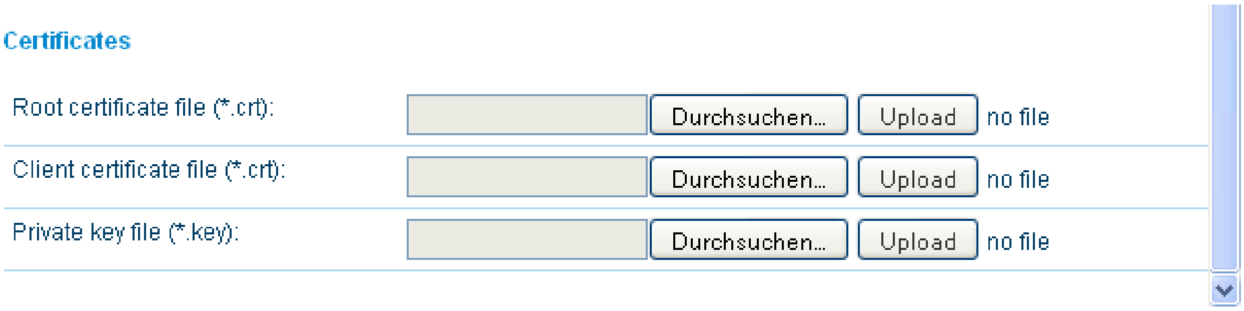
Configuration mode: ● standard configuration ○ expert configuration

Standard Configuration

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

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

5.1.6.1.3 OpenVPN Client Certificates



Certificates

Root certificate file (*.crt): Durchsuchen... Upload no file

Client certificate file (*.crt): Durchsuchen... Upload no file

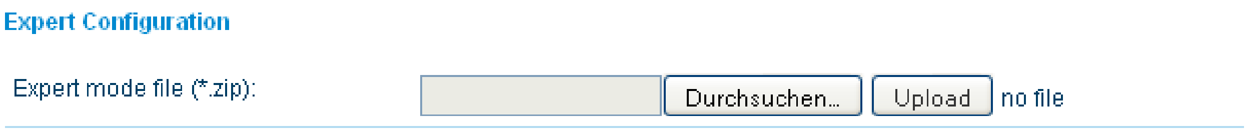
Private key file (*.key): Durchsuchen... Upload no file

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

Tip:

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

5.1.6.1.4 OpenVPN Configuration (Client Expert Configuration)



Expert Configuration

Expert mode file (*.zip): Durchsuchen... Upload no file

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

Typically such a zip file includes files such as:

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

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

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

5.1.6.1.5 OpenVPN Configuration (Server Expert Configuration)

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

Typically such a zip file includes files such as:

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

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

If OpenVPN is enabled and the configuration mode is set to "server expert configuration" all configurations (*.conf) will be started after NetBox startup.

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

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

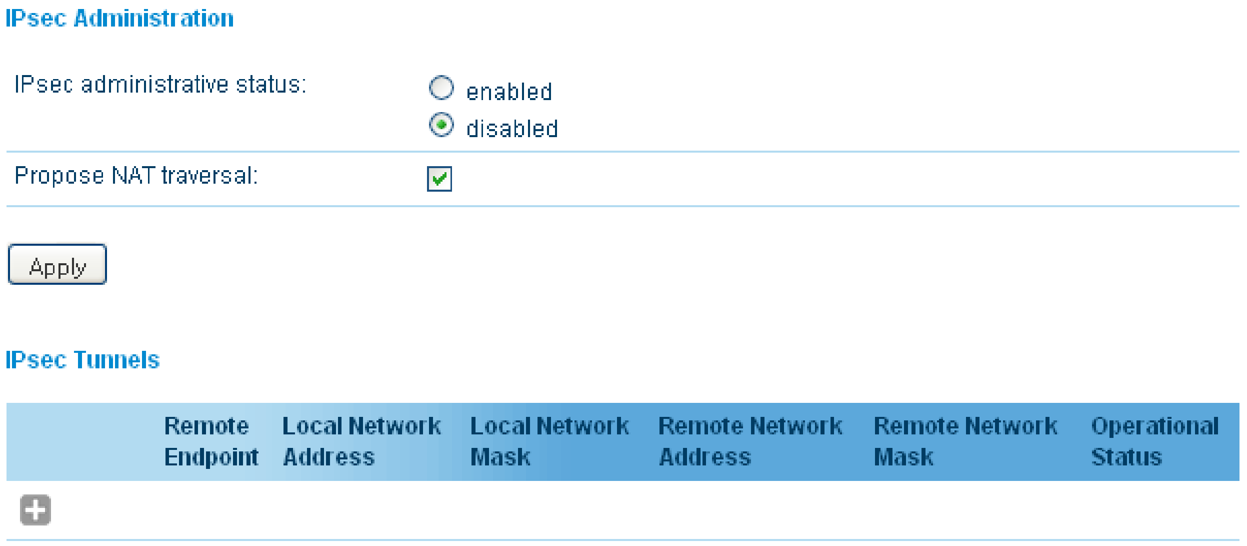
For further information and external OpenVPN documentation please see chapter 5.1.6.1.

5.1.6.2 IPsec

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

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

5.1.6.2.1 IPsec Administration



IPsec Administration

IPsec administrative status: ○ enabled ● disabled

Propose NAT traversal: ☑

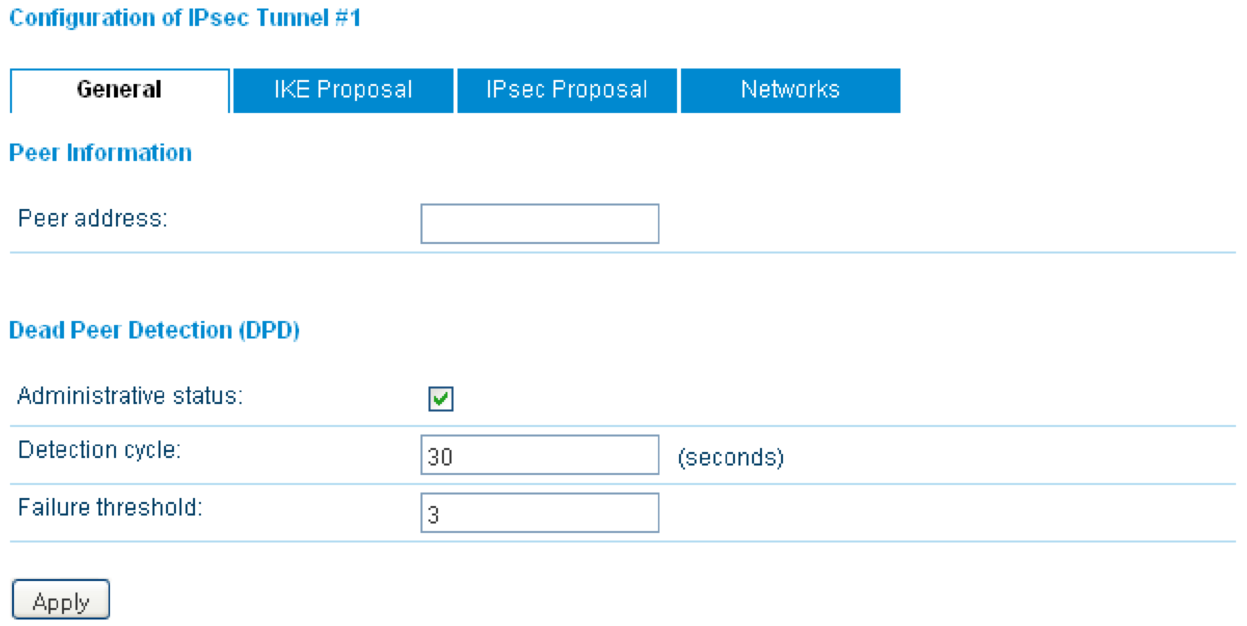
Apply

IPsec Tunnels

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

Parameter	Description
IPsec administrative status:	Enable or disable IPsec.

5.1.6.2.2 IPsec Configuration



Configuration of IPsec Tunnel #1

Peer Information

Peer address:

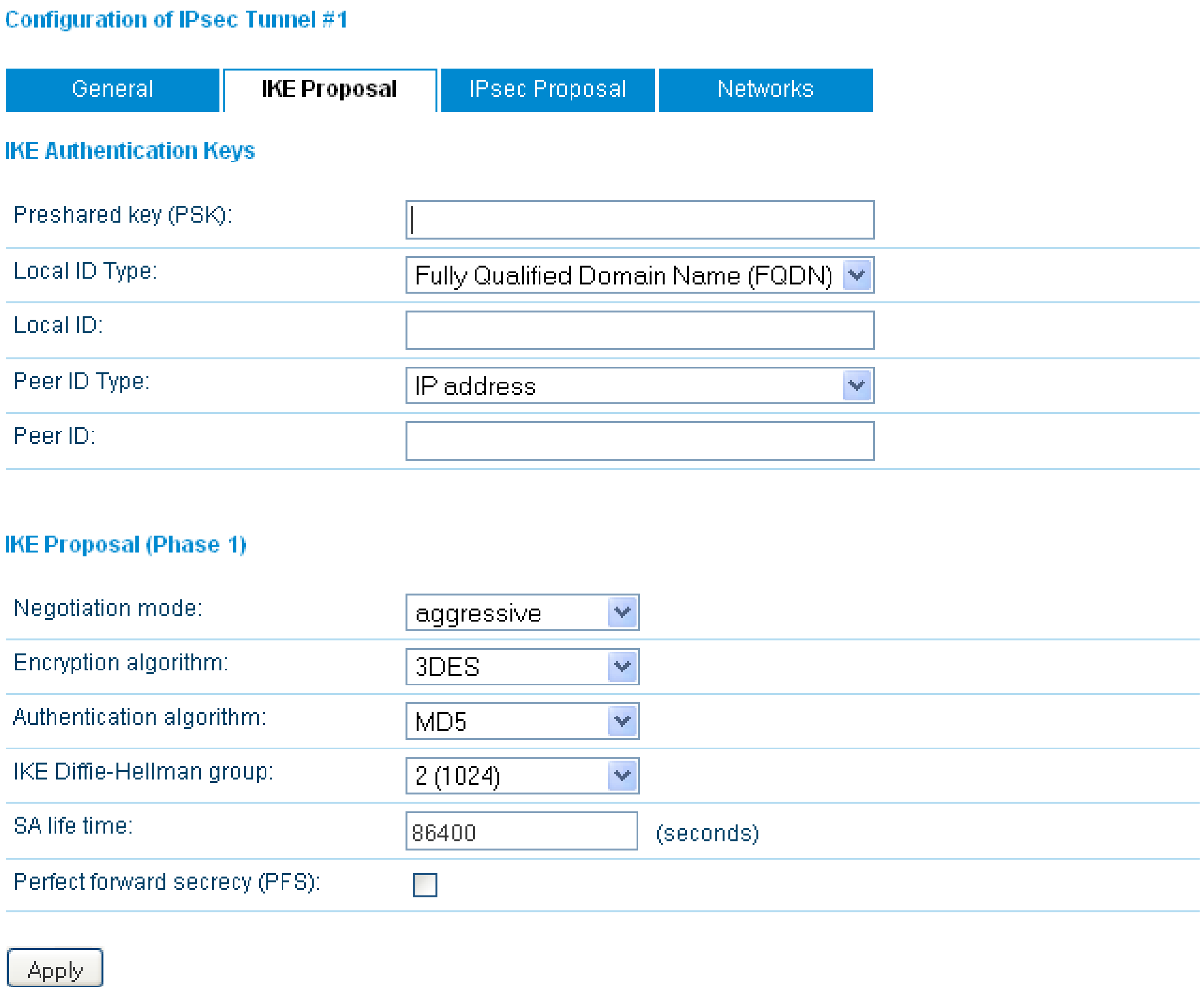
Dead Peer Detection (DPD)

Administrative status: ☑

Detection cycle: 30 (seconds)

Failure threshold: 3

Apply



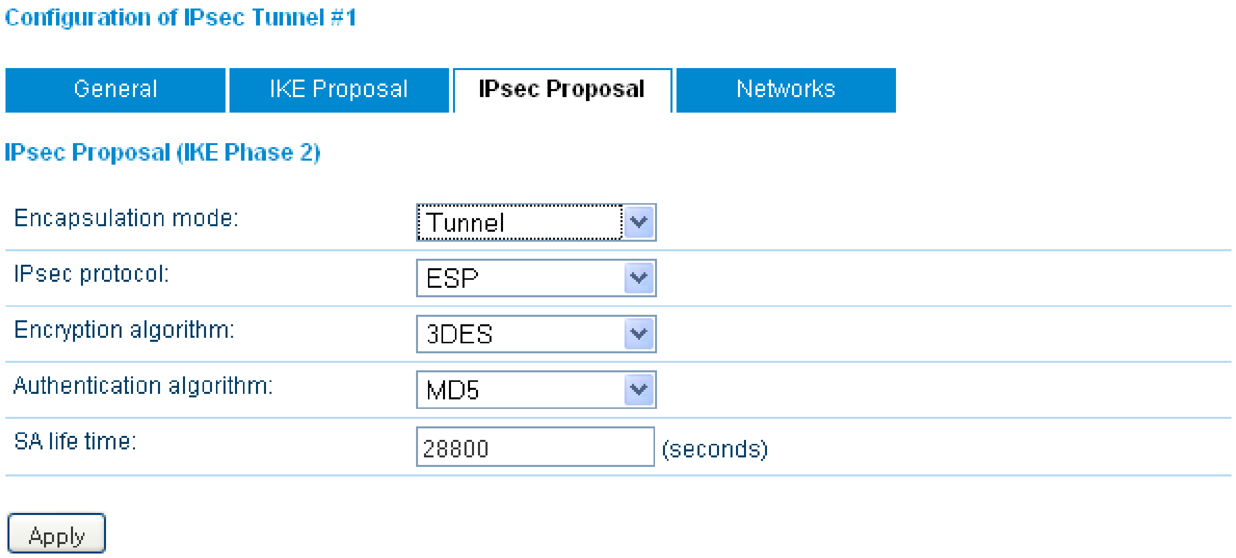
Configuration of IPsec Tunnel #1

IKE Authentication Keys

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

IKE Proposal (Phase 1)

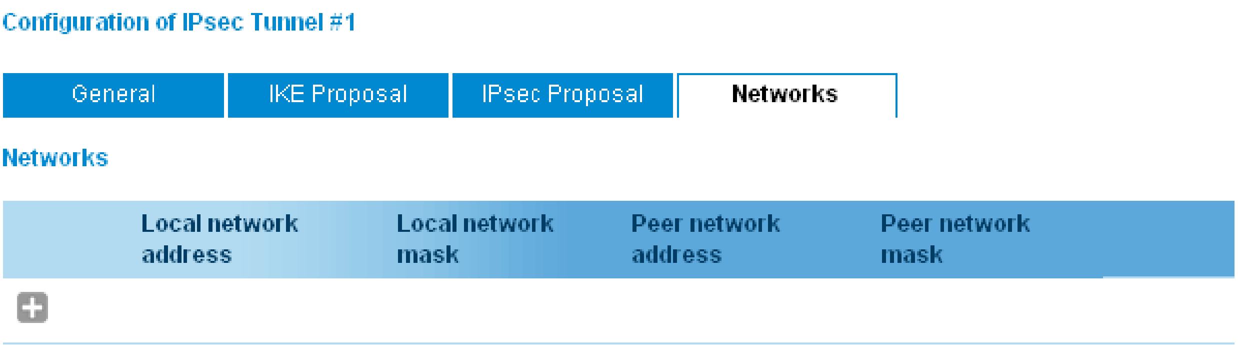
Negotiation mode:	aggressive
Encryption algorithm:	3DES
Authentication algorithm:	MD5
IKE Diffie-Hellman group:	2 (1024)
SA life time:	86400 (seconds)
Perfect forward secrecy (PFS):	□



Configuration of IPsec Tunnel #1

IPsec Proposal (IKE Phase 2)

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



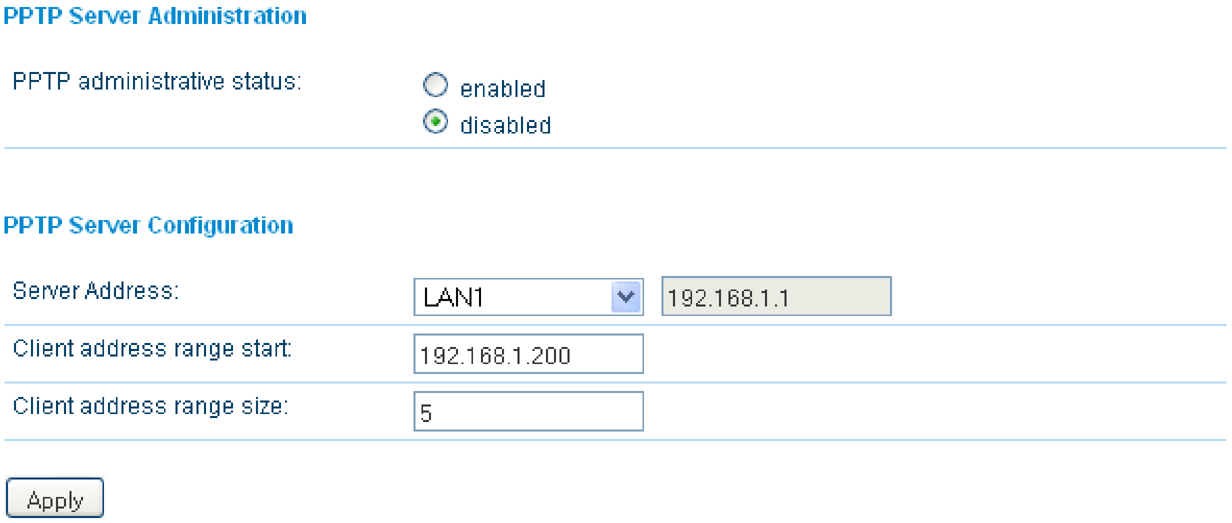
Configuration of IPsec Tunnel #1

Networks

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

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

5.1.6.3 PPTP Server



PPTP Server Administration

PPTP administrative status: ○ enabled ● disabled

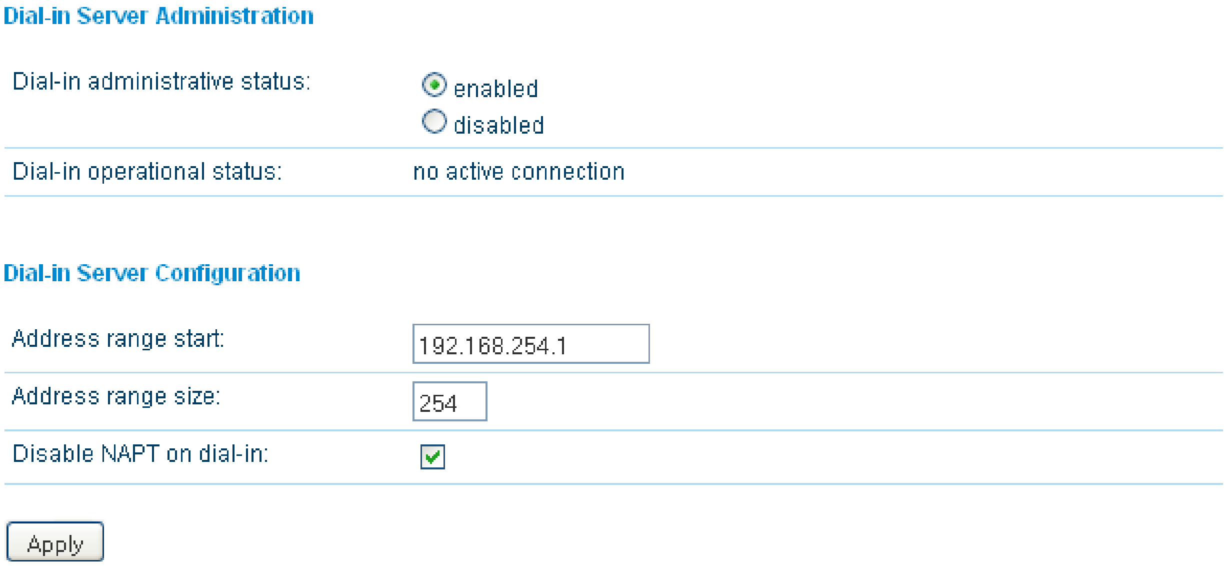
PPTP Server Configuration

Server Address:	LAN1 192.168.1.1
Client address range start:	192.168.1.200
Client address range size:	5

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

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

5.1.6.4 Dial-in Server


Dial-in Server Administration

Dial-in administrative status:	● enabled ○ disabled
Dial-in operational status:	no active connection

Dial-in Server Configuration

Address range start:	192.168.254.1
Address range size:	254
Disable NAPT on dial-in:	☑

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

5.1.6.4.1 Dial-in Server Administration

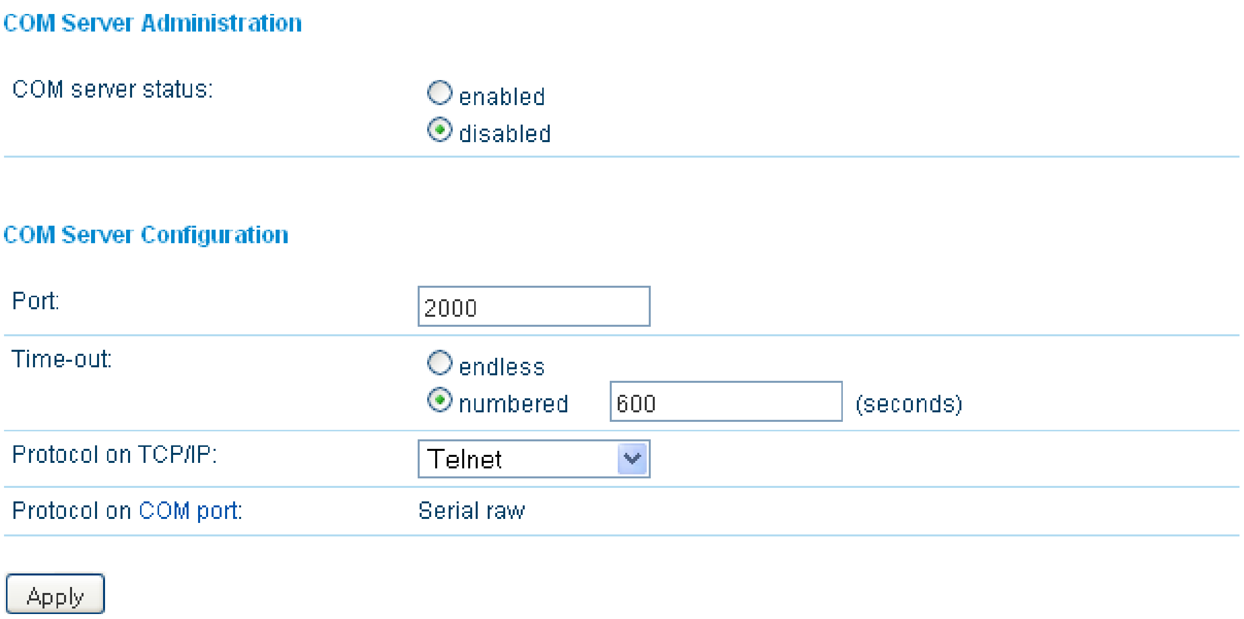
Parameter	Description
Dial-in administrative status:	The Dial-in server can be enabled or disabled. Consequently the device will allow incoming calls or not.
Dial-in operational status:	Shows whether a connection is active or not

5.1.6.4.2 Dial-in Server Configuration

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

5.1.7 Services

5.1.7.1 COM Server / Gateway



COM Server Administration

COM server status:	○ enabled ● disabled

COM Server Configuration

Port:	2000
Time-out:	○ endless ● numbered 600 (seconds)
Protocol on TCP/IP:	Telnet
Protocol on COM port:	Serial raw

5.1.7.1.1 COM Server Administration

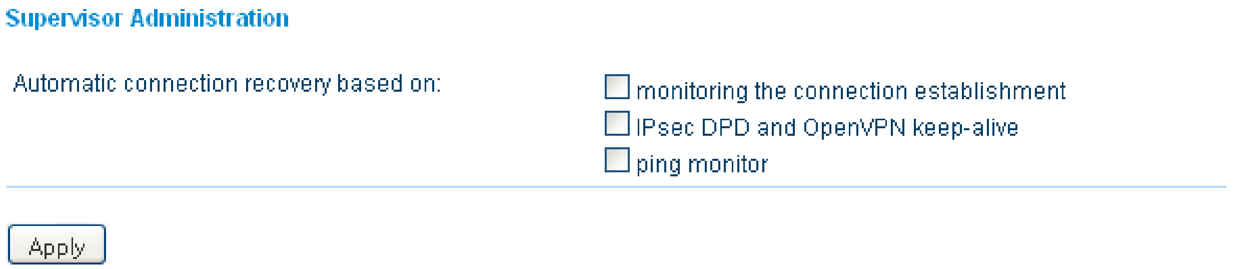
Parameter	Description
COM server status:	The COM server / ModBus gateway can be enabled or disabled.

5.1.7.1.2 COM Server Configuration

Parameter	Description
Port:	The port that is used by this application.
Protocol on TCP/IP:	“Telnet” or “TCP raw” for COM server applications, “Modbus TCP” for ModBus gateway
Protocol on COM port:	The protocol implicitly defined on the COM port.

5.1.7.2 Connection Supervisor

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



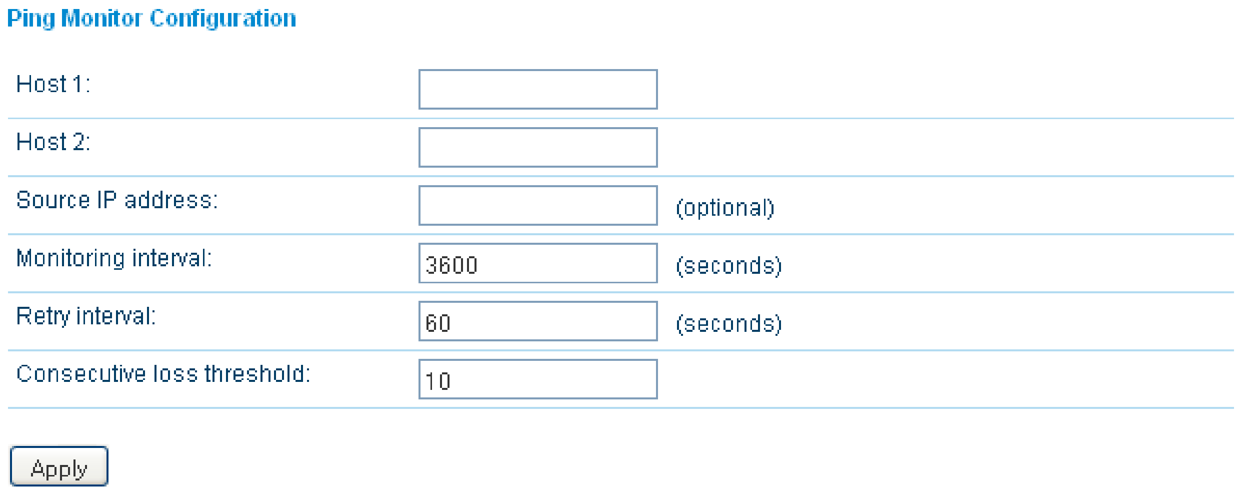
Supervisor Administration

Automatic connection recovery based on:

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

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

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



Ping Monitor Configuration

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

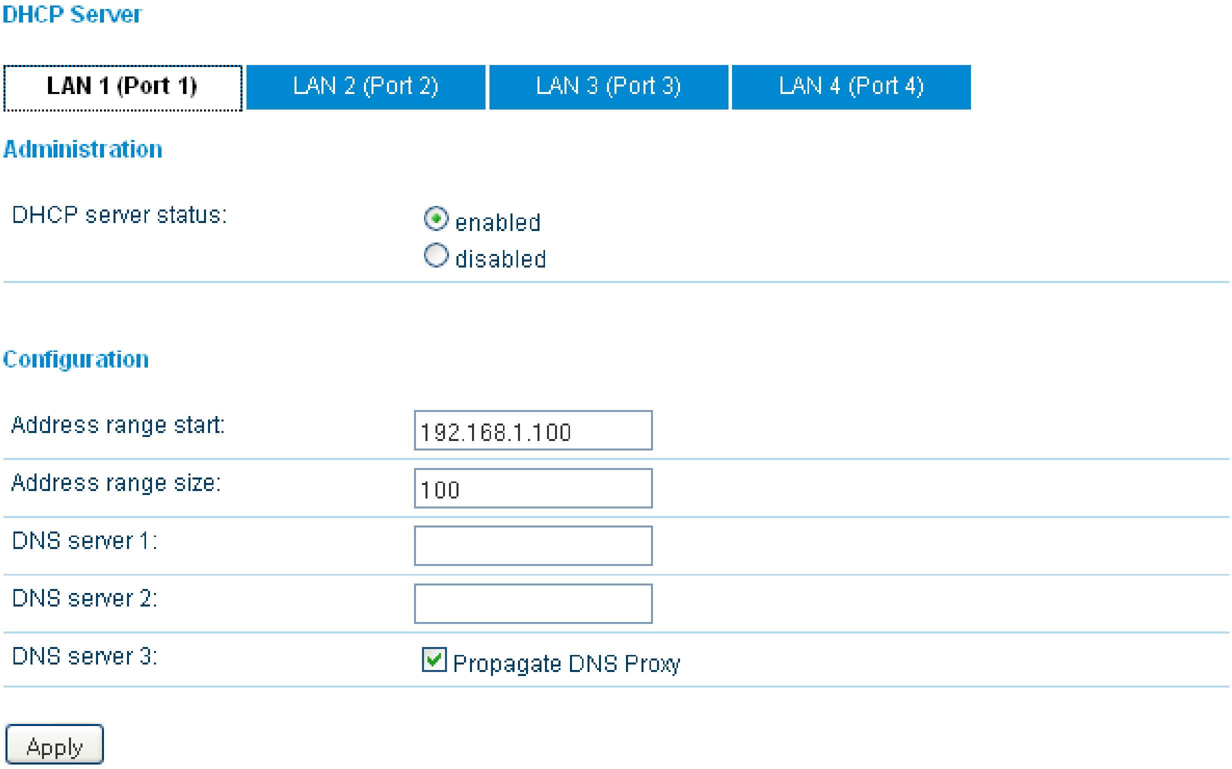
Parameter	Description
Host 1:	Reference host 1 to which IP connectivity is checked by sending probes
Host 2:	Reference host 2 to which IP connectivity is checked by sending probes (optional) The test is considered successful if host 1 or 2 answers.
Source IP address:	Source IP address to be used as source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

The recovery actions are:

1. Trying to reestablish a broken connection

2. Restart the internal modem
3. Restart the NetBox

5.1.7.3 DHCP Server



DHCP server status: ● enabled ○ disabled

Address range start: 192.168.1.100

Address range size: 100

DNS server 1:

DNS server 2:

DNS server 3: ☑ Propagate DNS Proxy

The DHCP server assigns the following information:

1. Any IP address out of the configured range
2. As default gateway the IP address of NetBox is assigned
3. As DNS server the IP address of NetBox is assigned or manually configured DNS servers

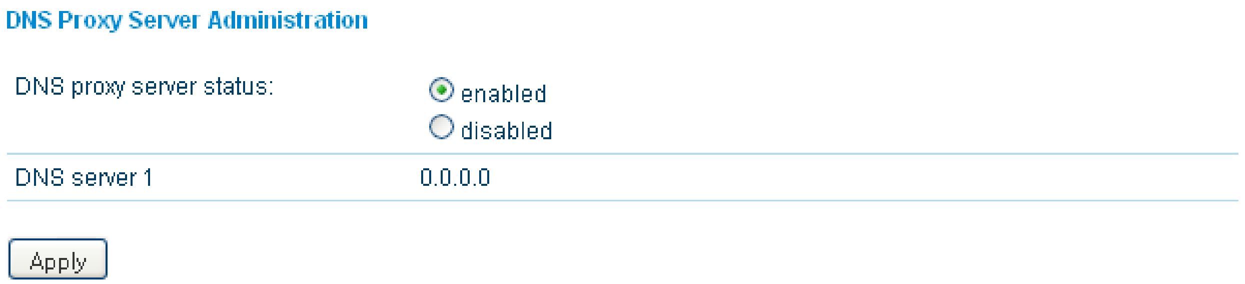
5.1.7.3.1 DHCP Server Administration

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

5.1.7.3.2 DHCP Server Configuration

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

5.1.7.4 DNS Proxy Server



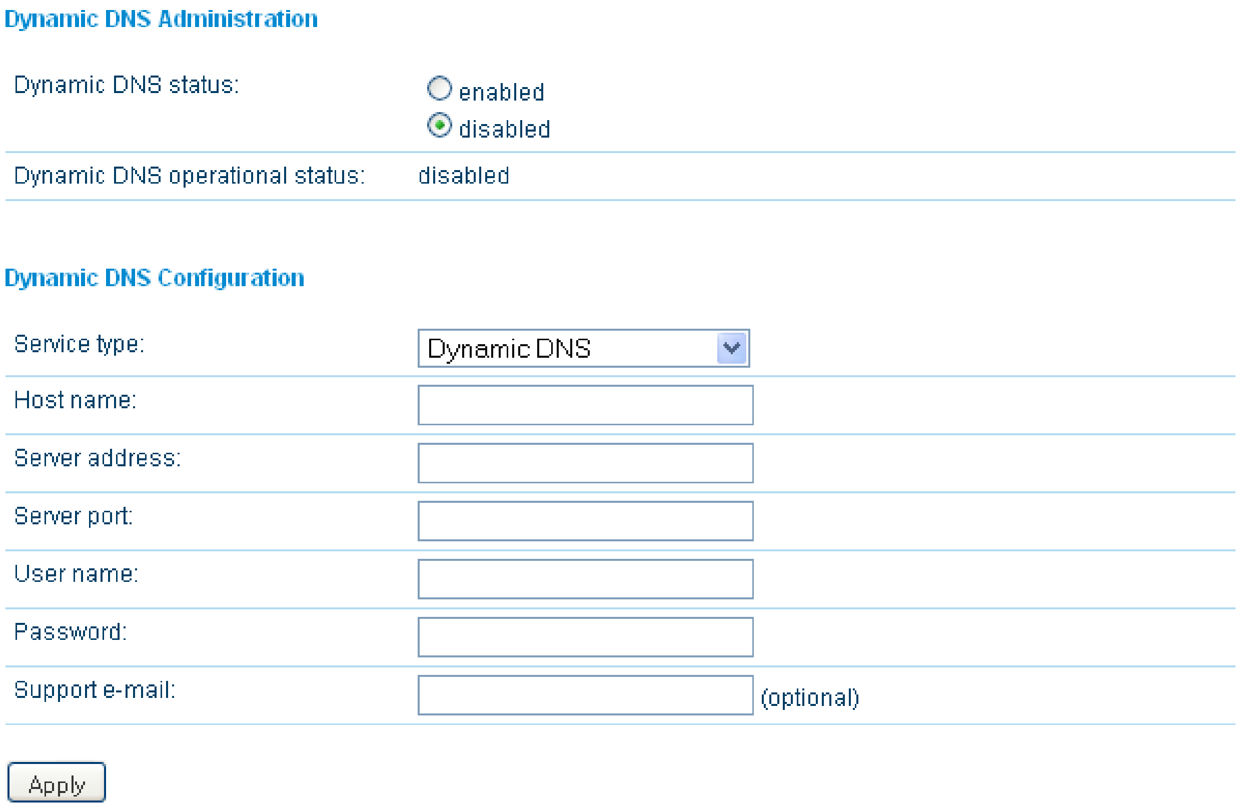
DNS Proxy Server Administration

DNS proxy server status:	● enabled ○ disabled
DNS server 1	0.0.0.0

The DNS Proxy enabled NetBox forwards DNS requests to the DNS server provided by the mobile operator. Devices within the NetBox LAN may be configured to use NetBox as DNS server.

Parameter	Description
DNS proxy server status:	Enabled or disabled

5.1.7.5 Dynamic DNS



Dynamic DNS Administration

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

Dynamic DNS Configuration

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

The Dynamic DNS Client of NetBox is completely compatible to the Dynamic Network Services provided by the organization DynDNS (www.dyndns.com).

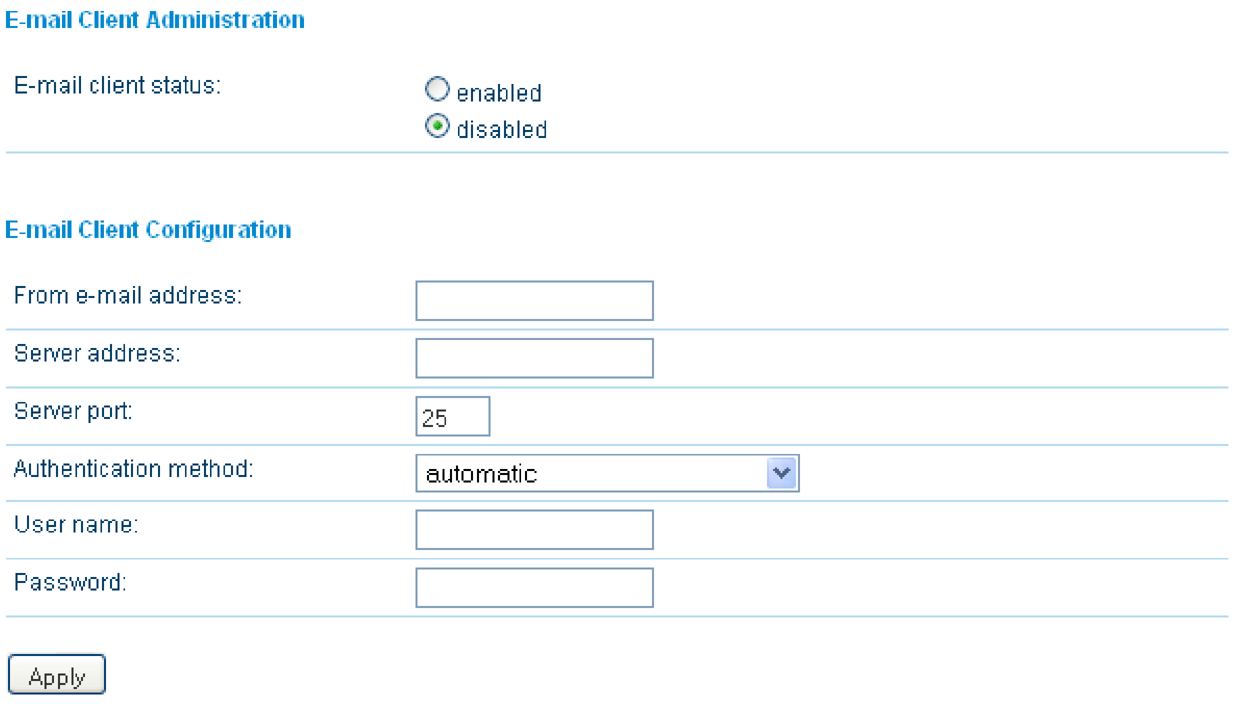
5.1.7.5.1 Dynamic DNS Administration

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

5.1.7.5.2 Dynamic DNS Configuration

Parameter	Description
Service type:	DynDNS Service according Dynamic Network Services, Inc. (www.dyndns.com). Please consult www.dyndns.com for more details.
Host name:	URL under which NetBox will be available, e.g. myNetBox.dyndns.org
Server address:	Server IP Address or URL, normally members.dyndns.org
Server port:	TCP Port of the Dynamic DNS Server, e.g. 80 or 8245
User name:	Username
Password:	Password
Support e-mail:	Optional support e-mail address

5.1.7.6 E-mail Client



E-mail Client Administration

E-mail client status: ○ enabled ● disabled

E-mail Client Configuration

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

5.1.7.7 E-Mail Client Administration

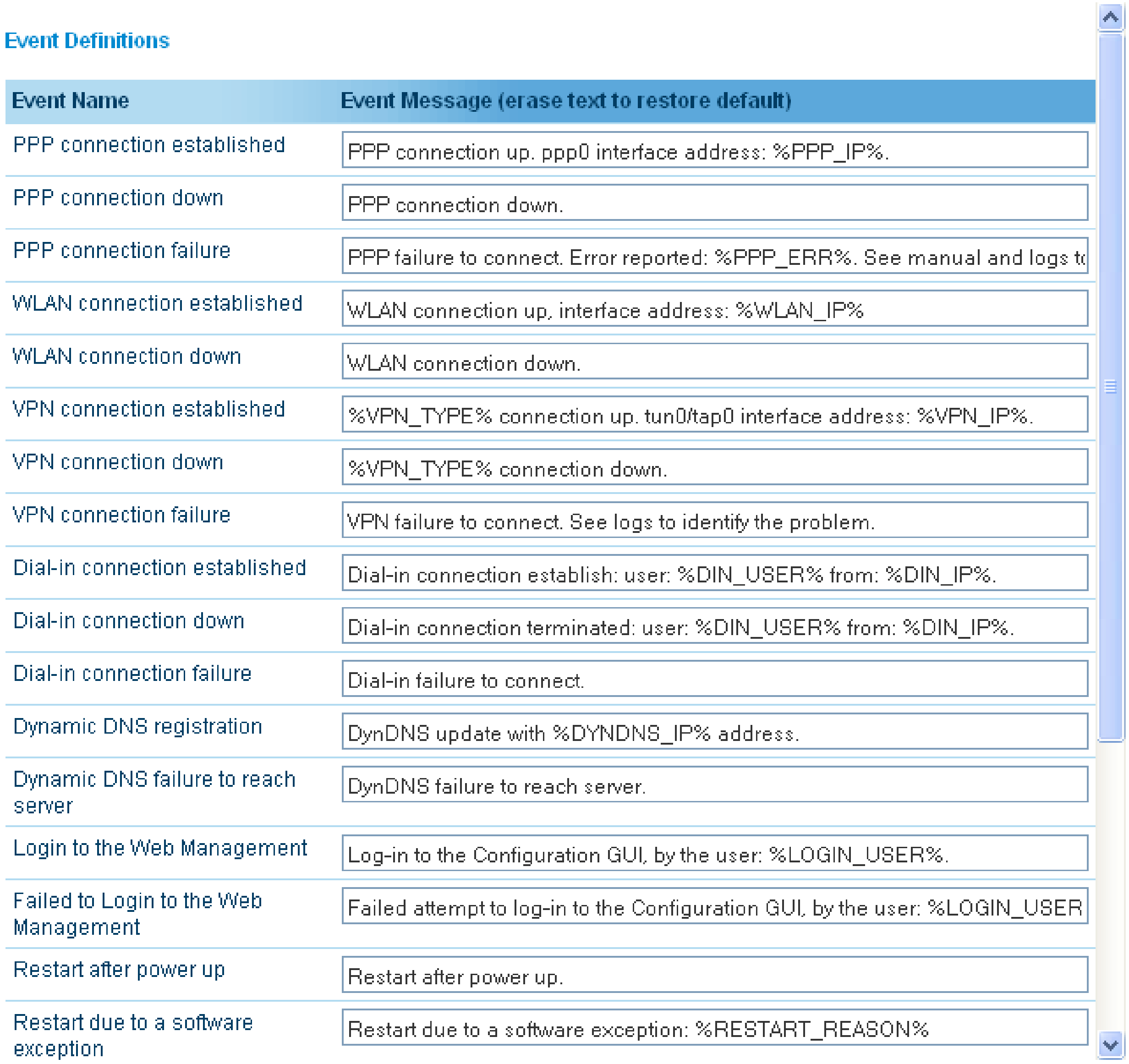
Parameter	Description
E-mail client status:	Sending e-mail can be enabled or disabled. Disabling the e-mail client means that no notification via e-mail will be performed.

5.1.7.8 E-mail Client Configuration

Parameter	Description
From e-mail address:	Sender's e-mail address
Server address:	SMTP server address
Server port:	Default port for SMTP is 25
Authentication required:	If enabled NetBox will logon to SMTP server before sending e-mails.
User name:	User name
Password:	Password

5.1.7.9 Event Manager

5.1.7.9.1 Events



Event Definitions

Event Name	Event Message (erase text to restore default)
PPP connection established	PPP connection up. ppp0 interface address: %PPP_IP%.
PPP connection down	PPP connection down.
PPP connection failure	PPP failure to connect. Error reported: %PPP_ERR%. See manual and logs t
WLAN connection established	WLAN connection up, interface address: %WLAN_IP%
WLAN connection down	WLAN connection down.
VPN connection established	%VPN_TYPE% connection up. tun0/tap0 interface address: %VPN_IP%.
VPN connection down	%VPN_TYPE% connection down.
VPN connection failure	VPN failure to connect. See logs to identify the problem.
Dial-in connection established	Dial-in connection establish: user: %DIN_USER% from: %DIN_IP%.
Dial-in connection down	Dial-in connection terminated: user: %DIN_USER% from: %DIN_IP%.
Dial-in connection failure	Dial-in failure to connect.
Dynamic DNS registration	DynDNS update with %DYNDNS_IP% address.
Dynamic DNS failure to reach server	DynDNS failure to reach server.
Login to the Web Management	Log-in to the Configuration GUI, by the user: %LOGIN_USER%.
Failed to Login to the Web Management	Failed attempt to log-in to the Configuration GUI, by the user: %LOGIN_USER
Restart after power up	Restart after power up.
Restart due to a software exception	Restart due to a software exception: %RESTART_REASON%

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

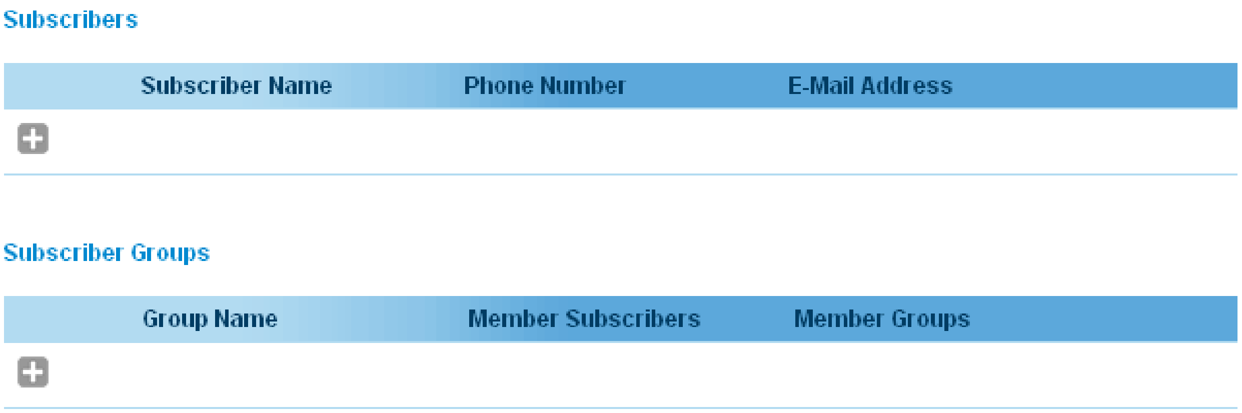
Event	Event Text
PPP connection established	PPP connection up. ppp0 interface address: %PPP_IP%.
PPP connection down	PPP connection down.
PPP connection failure	PPP failure to connect. Error reported: %PPP_ERR%. See manual and logs to identify the problem.
VPN connection established	VPN connection up.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

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

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

Event Variables	Description
%PPP_IP%	The current IP address on the mobile interface (ppp0)
%PPP_ERR%	Error message in case of mobile connection failure
%VPN_IP%	The current address of the OpenVPN interface
%VPN_TYPE%	IPsec or OpenVPN
%DYNDNS_IP%	The IP address which has been sent to the DNS server
%DIN_USER%	User name which the dial-in connection has been authenticated against
%DIN_IP%	The IP address of the dial-in peer
%LOGIN_USER%	Name of the user who tried to log on to the Web Manager
%DIO_SOURCE%	Source that triggered an output change
%UDP_MESSAGE%	Text message that has been received by the message receiver
%RESTART_REASON%	Reason why a restart happened
%DST_IN1%	Status of digital input 1, possible values include [on, off]
%DST_IN2%	Status of digital input 2, possible values include [on, off]
%DST_OUT1%	Status of digital output 1, possible values include [on, off]
%DST_OUT2%	Status of digital output 2, possible values include [on, off]

5.1.7.9.2 Subscribers



Subscribers

Subscriber Name	Phone Number	E-Mail Address
⊞		

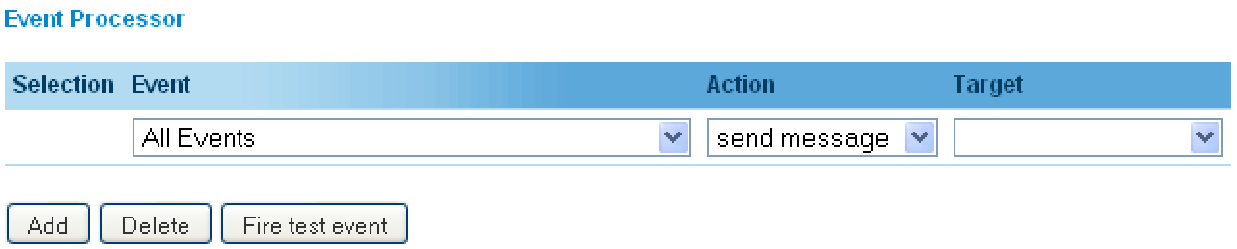
Subscriber Groups

Group Name	Member Subscribers	Member Groups
⊞		

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

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

5.1.7.9.3 Event Processor

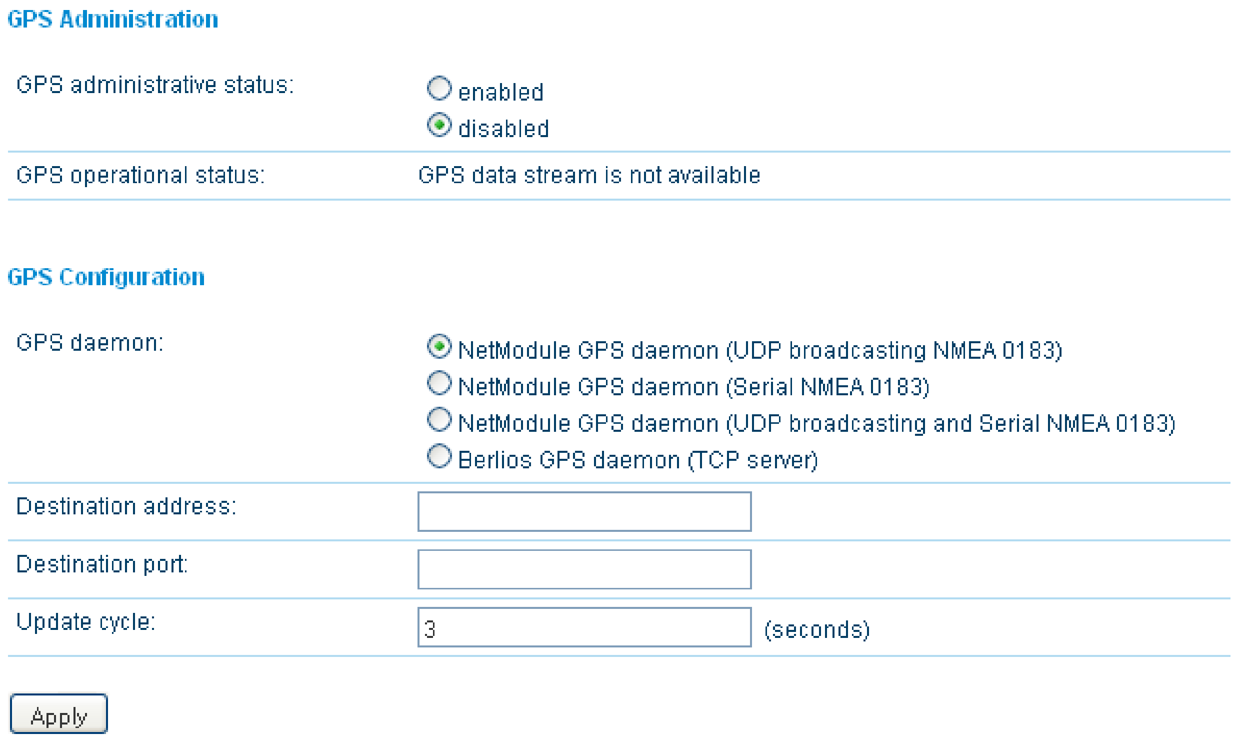


Event Processor

Selection	Event	Action	Target
	All Events	send message	

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

5.1.7.10 GPS



GPS Administration

GPS administrative status: ○ enabled
 ● disabled

GPS operational status: GPS data stream is not available

GPS Configuration

GPS daemon: ● NetModule GPS daemon (UDP broadcasting NMEA 0183)
 ○ NetModule GPS daemon (Serial NMEA 0183)
 ○ NetModule GPS daemon (UDP broadcasting and Serial NMEA 0183)
 ○ Berlios GPS daemon (TCP server)

Destination address:

Destination port:

Update cycle: 3 (seconds)

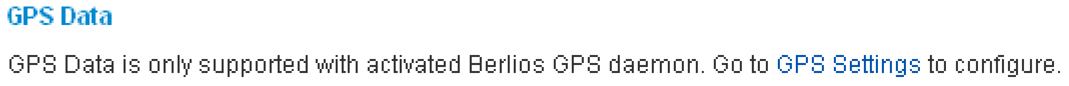
This feature is available on NB2241 and NB2341 only.

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

For more information on the GPS data stream see chapter 6.1.

Parameter	Description
GPS status:	Enable or disable GPS data stream
GPS destination host name:	The host where the GPS data will be sent to
GPS destination host name:	The IP port where the GPS data will be sent to
GPS update cycle:	The refresh cycle.

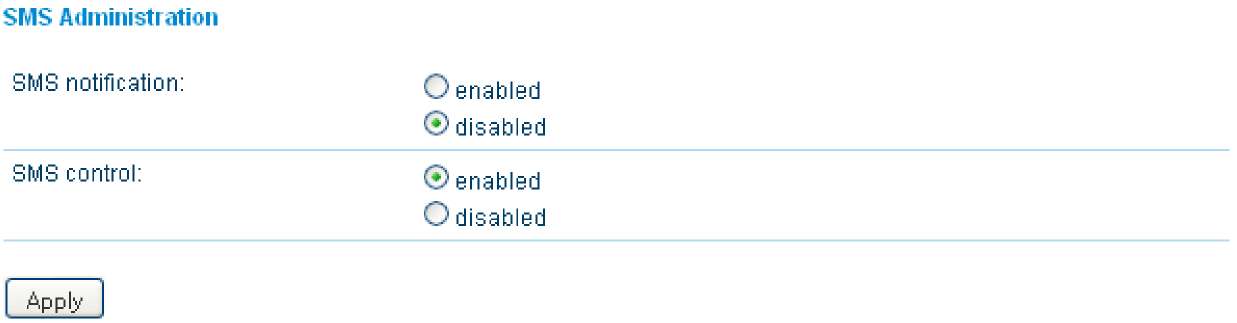
5.1.7.11 GPS Data



GPS Data

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

5.1.7.12 SMS



SMS Administration

SMS notification: ○ enabled ● disabled

SMS control: ● enabled ○ disabled

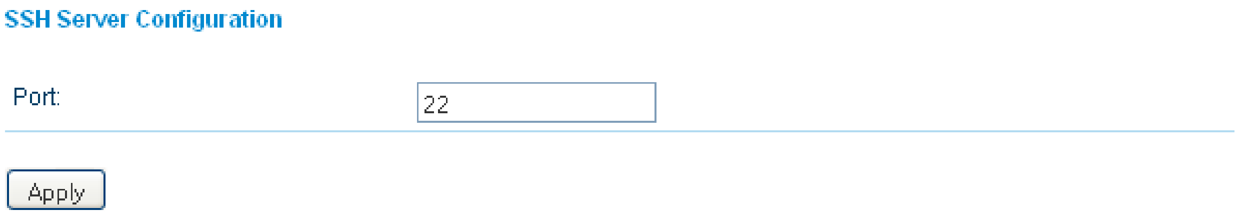
SMS can be used to control NetBox and for event notification.

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

Send a SMS to the phone number of the SIM that is inserted into your NetBox. Valid commands are listed in the table below:

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

5.1.7.13 SSH Server



SSH Server Configuration

Port: 22

Parameter	Description
Port:	SSH server port

5.1.7.14 SNMP Agent

Starting from NBSW 3.4.0 Netbox is equipped with a SNMP daemon, supporting basic MIB tables (such as ifTable), plus additional enterprise MIBs to manage the systems.

The system ID is defined as follows:

NetBox Model	ID
NB1310	1.3.6.1.4.1.31496.10.10.50
NB1600	1.3.6.1.4.1.31496.10.10.46
NB2210	1.3.6.1.4.1.31496.10.10.10
NB2240	1.3.6.1.4.1.31496.10.10.20
NB2241	1.3.6.1.4.1.31496.10.10.21
NB2340	1.3.6.1.4.1.31496.10.10.30
NB2341	1.3.6.1.4.1.31496.10.10.31
NB2500	1.3.6.1.4.1.31496.10.10.42
NB2500R	1.3.6.1.4.1.31496.10.10.43
NB2540	1.3.6.1.4.1.31496.10.10.40
NB2541	1.3.6.1.4.1.31496.10.10.41
NB2600	1.3.6.1.4.1.31496.10.10.44
NB2600R	1.3.6.1.4.1.31496.10.10.45

Up to now the Netbox extensions contain support for:

- rebooting the device
- updating to a new system software via FTP/TFTP/HTTP
- updating to a new system configuration via FTP/TFTP/HTTP
- getting the status of last software update
- getting the status of last config update

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

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, that means 'admin01' becomes 'admin01admin01'.

The SNMP extensions can be read/triggered as follows:

- get system software version:

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

- get 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
```

- get 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
```

- restart the device:

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

- run 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"
```

REMARK: configUpdate expects a zip-file named <serial-number>.zip in the specified directory which contains at least a "user-config.zip"

On NB2xxx, TFTP, HTTP and FTP are supported. NB1600 also accepts HTTPS.

Specifying a username/password or port is not yet supported.

- get configuration update status:

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

The return value can be one of:

succeeded (1),

failed (2),

inprogress (3),

notstarted (4)

- run software update:

```
$ snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1
1.3.6.1.4.1.31496.10.40.13.0 s "http://server/directory"
```

- get software update status:

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

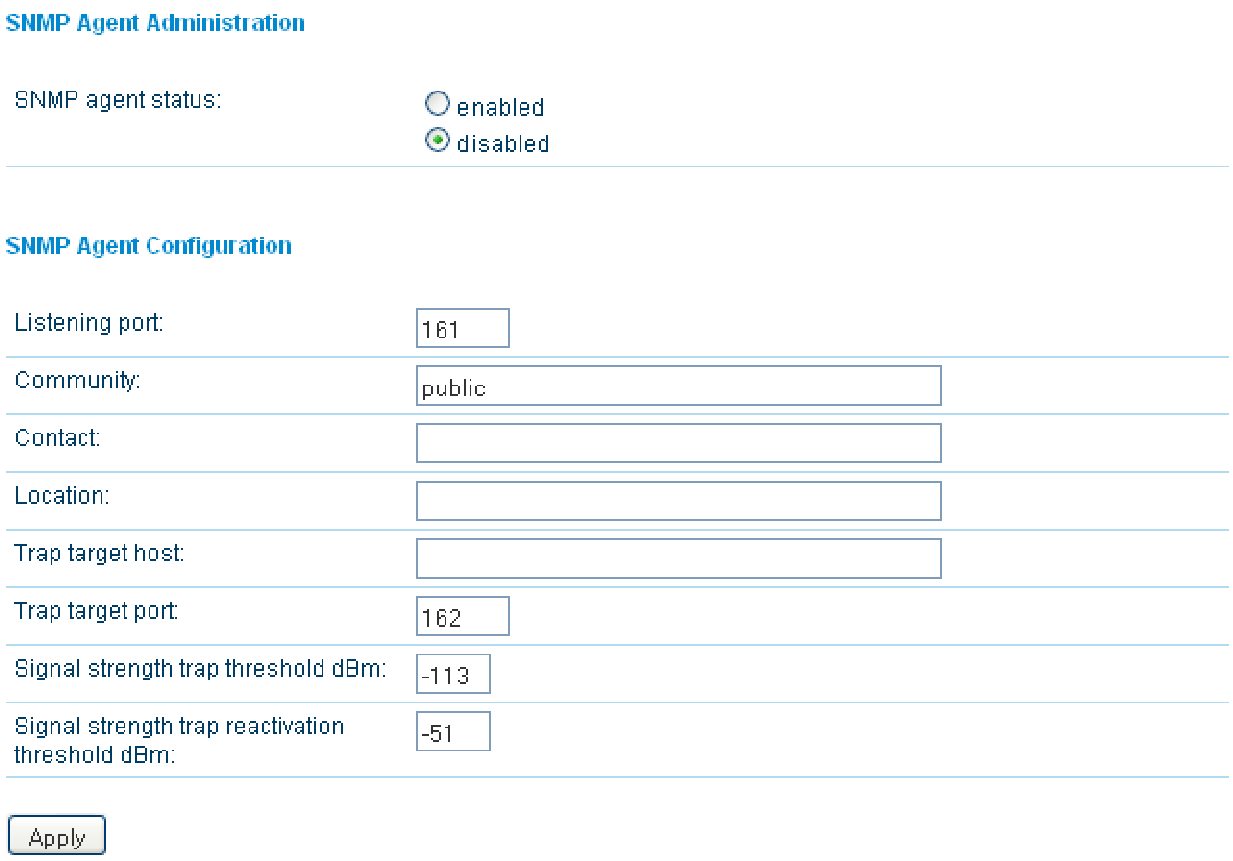
The return value can be one of:

succeeded (1),

failed (2),

inprogress (3),

notstarted (4)



SNMP Agent Administration

SNMP agent status: ○ enabled ● disabled

SNMP Agent Configuration

Listening port:	161
Community:	public
Contact:	
Location:	
Trap target host:	
Trap target port:	162
Signal strength trap threshold dBm:	-113
Signal strength trap reactivation threshold dBm:	-51

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

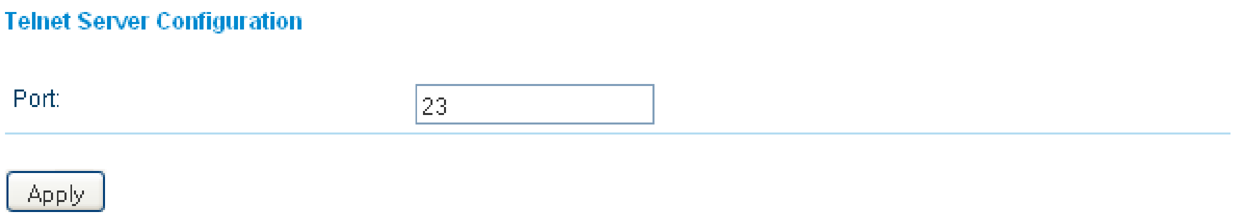
SNMP traps are generated in the following situations, if the SNMP agent is enabled:

- Startup of the NetBox
- Shutdown of the NetBox
- VPN connected
- VPN disconnected
- Signal Strength below „Signal strength trap threshold“

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

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

5.1.7.15 Telnet Server

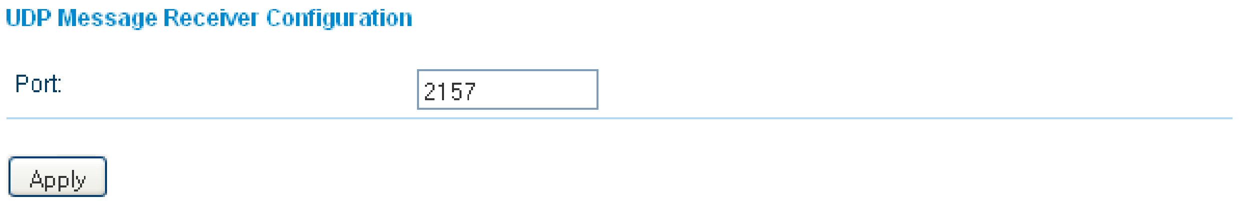


Telnet Server Configuration

Port: 23

Parameter	Description
Port:	Telnet server port

5.1.7.16 UDP Message Receiver



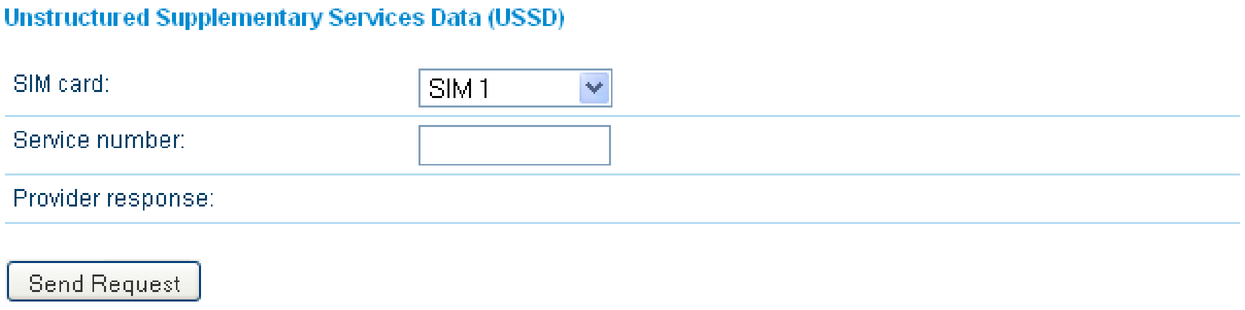
UDP Message Receiver Configuration

Port: 2157

Parameter	Description
Port:	UDP message receiver port

The UPD Message Receiver is a service that listens on the configured port (default 2157) for arriving UDP packets with a string in the payload. If an UPD package is arriving, the event "Arriving UDP Message" is fired (see chapter 5.1.7.9.1 Events). Use the Event Manager (5.1.7.9 Event Manager) to forward the message (UDP payload) to a SMS or E-mail destination.

5.1.7.17 Unstructured Supplementary Services Data (USSD)



Unstructured Supplementary Services Data (USSD)

SIM card: SIM 1

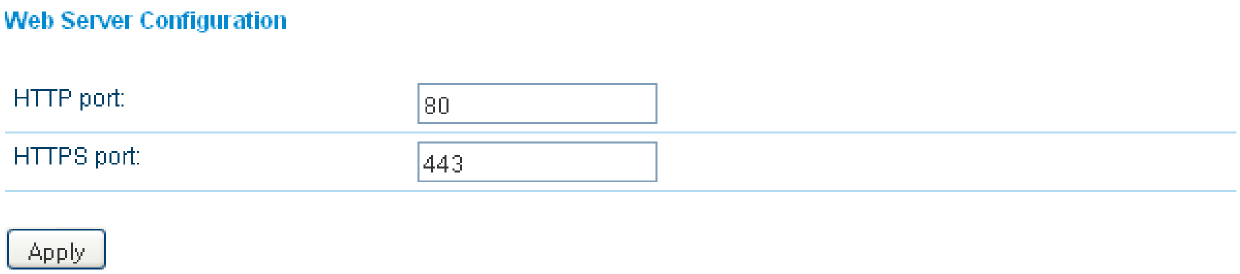
Service number:

Provider response:

Unstructured Supplementary Services Data (USSD) is a GSM service that allows high speed interactive communication between the subscribers and applications across a GSM Network. A sample USSD service is the bill status service accessed by dialing *141# or similar numbers in between * and #.

Contact your mobile operator for further information.

5.1.7.18 Web Server



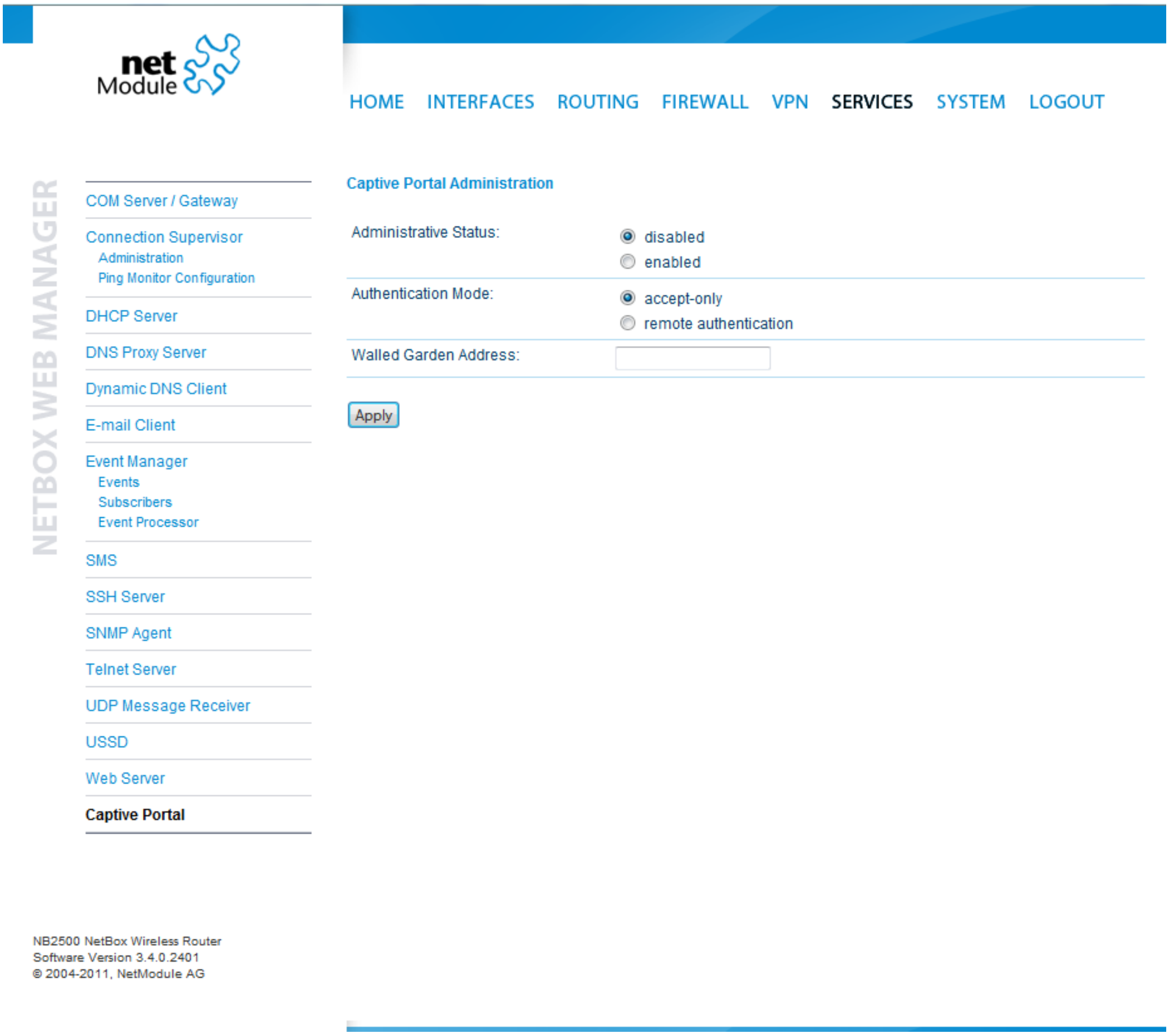
Web Server Configuration

HTTP port:	80
HTTPS port:	443

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

5.1.7.19 Captive Portal

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



Captive Portal Administration

Administrative Status: ● disabled ○ enabled

Authentication Mode: ● accept-only ○ remote authentication

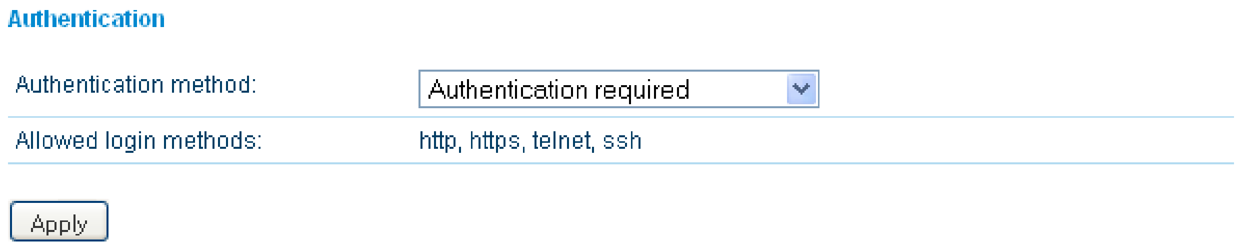
Walled Garden Address:

NB2500 NetBox Wireless Router
Software Version 3.4.0.2401
© 2004-2011, NetModule AG

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

5.1.8 System

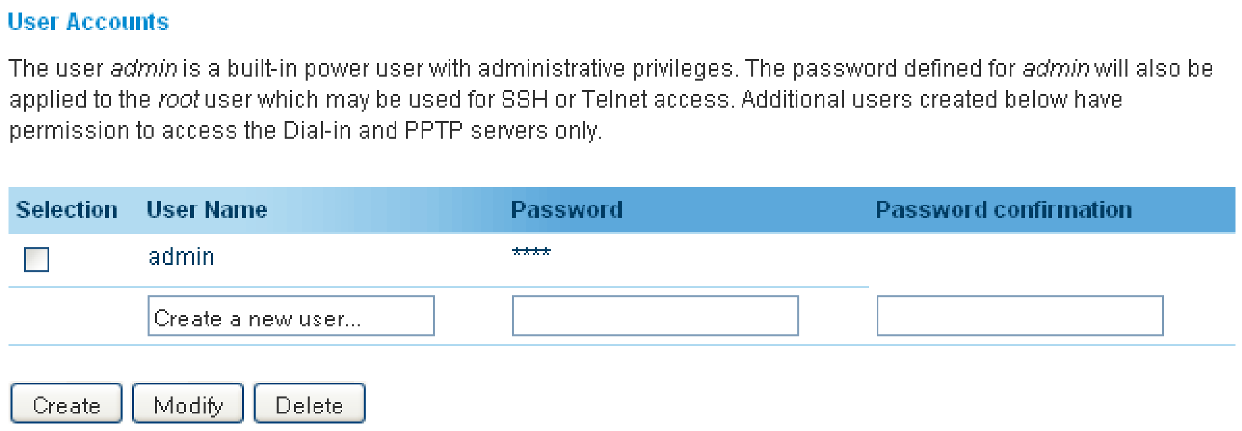
5.1.8.1 Authentication



Authentication

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

5.1.8.2 User Accounts



User Accounts

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

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

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

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

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

5.1.8.3 File Configuration

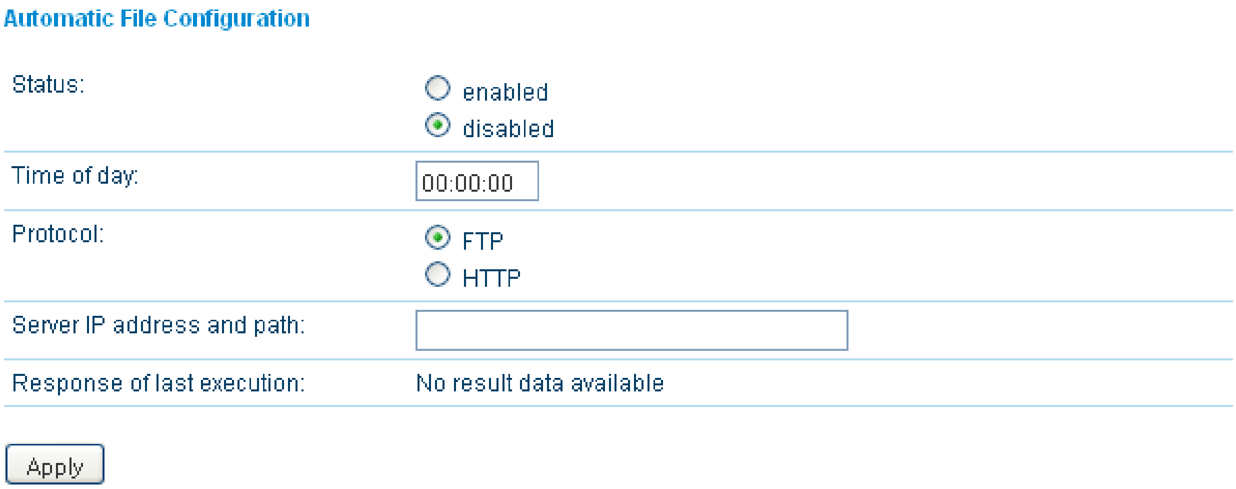
Configuration via the Web Manager becomes tedious for large volumes of devices. NetBox offers automatic and manual file-based configuration.

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

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

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

5.1.8.3.1 Automatic File Configuration


Automatic File Configuration

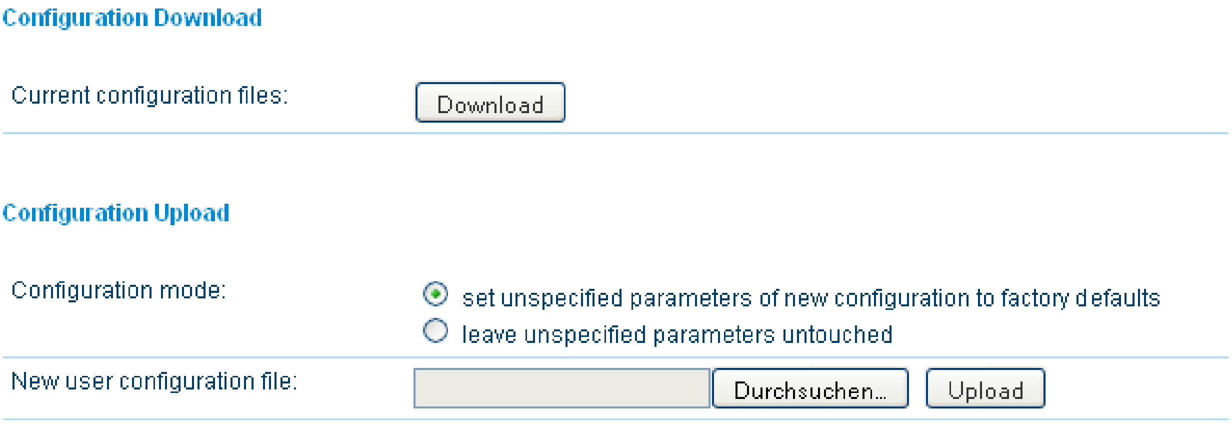
Status:	○ enabled ● disabled
Time of day:	00:00:00
Protocol:	● FTP ○ HTTP
Server IP address and path:	
Response of last execution:	No result data available

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

NetBox will only try to download the following files:

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

5.1.8.3.2 Manual File Configuration



Configuration Download

Current configuration files: Download

Configuration Upload

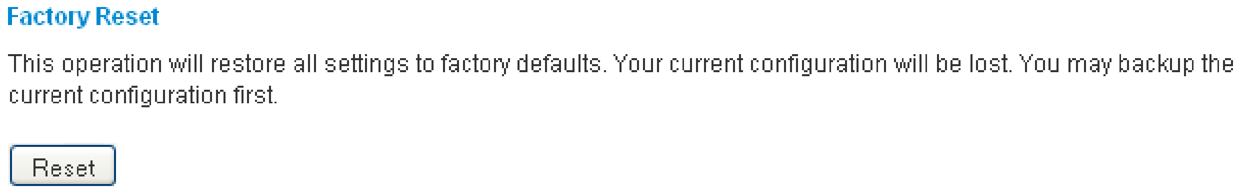
Configuration mode:
● set unspecified parameters of new configuration to factory defaults
○ leave unspecified parameters untouched

New user configuration file: Durchsuchen... Upload

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

For further information see also chapters 5.1.8.3 and 5.2.3.

5.1.8.3.3 Factory reset



Factory Reset

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

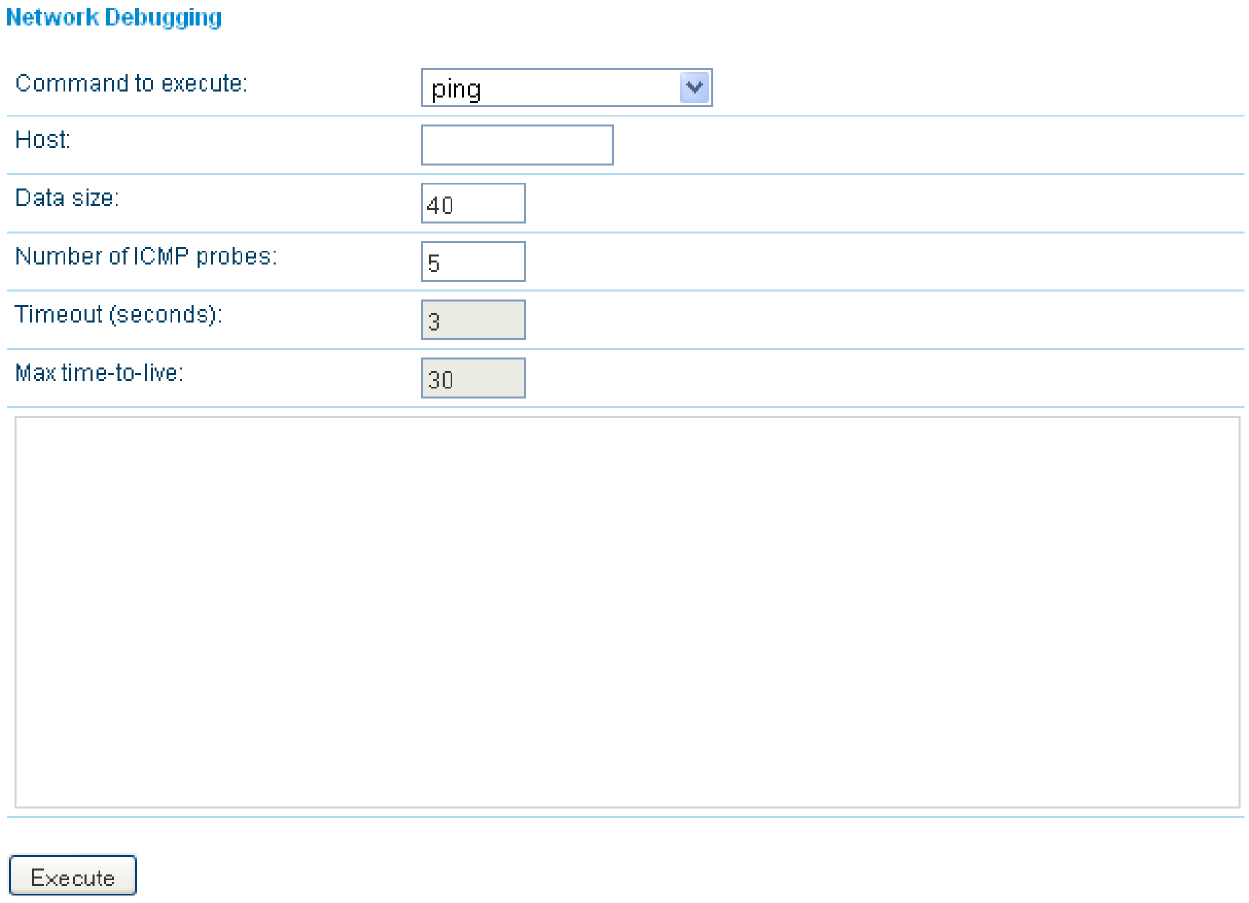
Press [Reset] to set the device to factory default. Your current configuration will be lost.

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

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

5.1.8.4 Troubleshooting

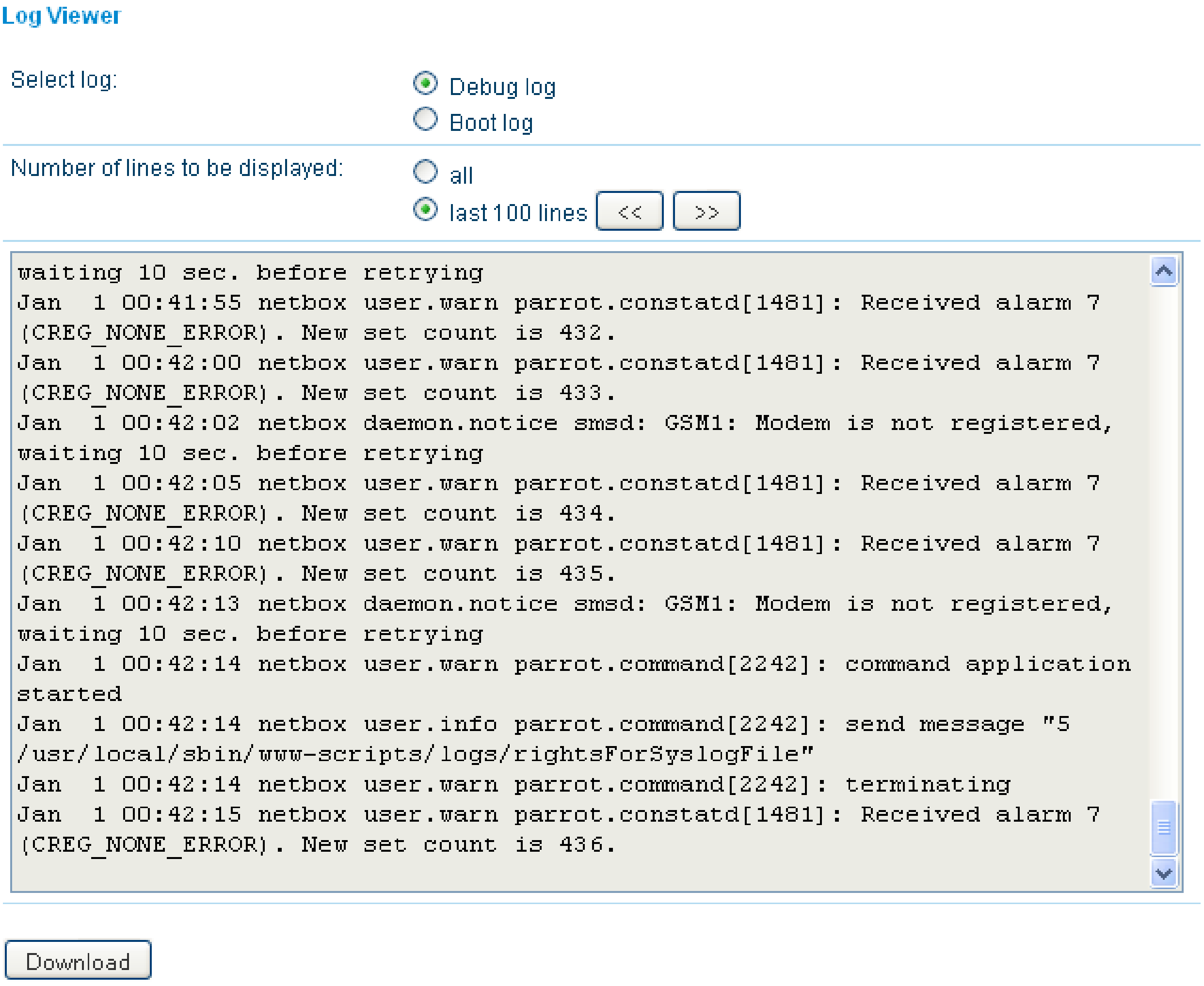
5.1.8.4.1 Network Debugging



Network Debugging

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

5.1.8.4.2 Log Files



Log Viewer

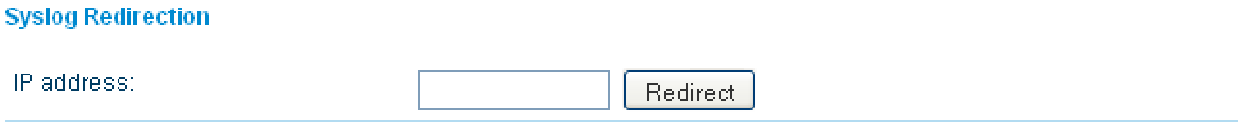
Select log: ● Debug log ○ Boot log

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

```
waiting 10 sec. before retrying
Jan  1 00:41:55 netbox user.warn parrot.constatd[1481]: Received alarm 7
(CREG_NONE_ERROR). New set count is 432.
Jan  1 00:42:00 netbox user.warn parrot.constatd[1481]: Received alarm 7
(CREG_NONE_ERROR). New set count is 433.
Jan  1 00:42:02 netbox daemon.notice smsd: GSM1: Modem is not registered,
waiting 10 sec. before retrying
Jan  1 00:42:05 netbox user.warn parrot.constatd[1481]: Received alarm 7
(CREG_NONE_ERROR). New set count is 434.
Jan  1 00:42:10 netbox user.warn parrot.constatd[1481]: Received alarm 7
(CREG_NONE_ERROR). New set count is 435.
Jan  1 00:42:13 netbox daemon.notice smsd: GSM1: Modem is not registered,
waiting 10 sec. before retrying
Jan  1 00:42:14 netbox user.warn parrot.command[2242]: command application
started
Jan  1 00:42:14 netbox user.info parrot.command[2242]: send message "5
/usr/local/sbin/www-scripts/logs/rightsForSyslogFile"
Jan  1 00:42:14 netbox user.warn parrot.command[2242]: terminating
Jan  1 00:42:15 netbox user.warn parrot.constatd[1481]: Received alarm 7
(CREG_NONE_ERROR). New set count is 436.
```

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

5.1.8.4.3 System Log Redirection



Syslog Redirection

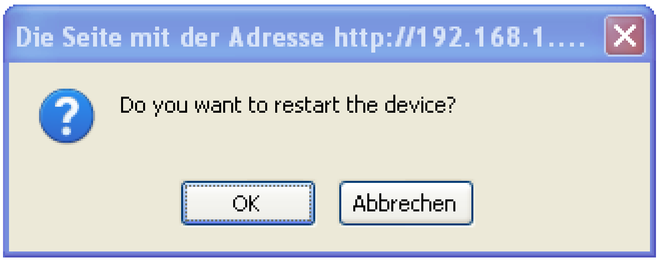
IP address:

Parameter	Description
IP address:	The host where the syslog messages will be forwarded to. A tiny syslog server is included in TFTP32 which can be downloaded from our website.

5.1.8.4.4 Restart

-

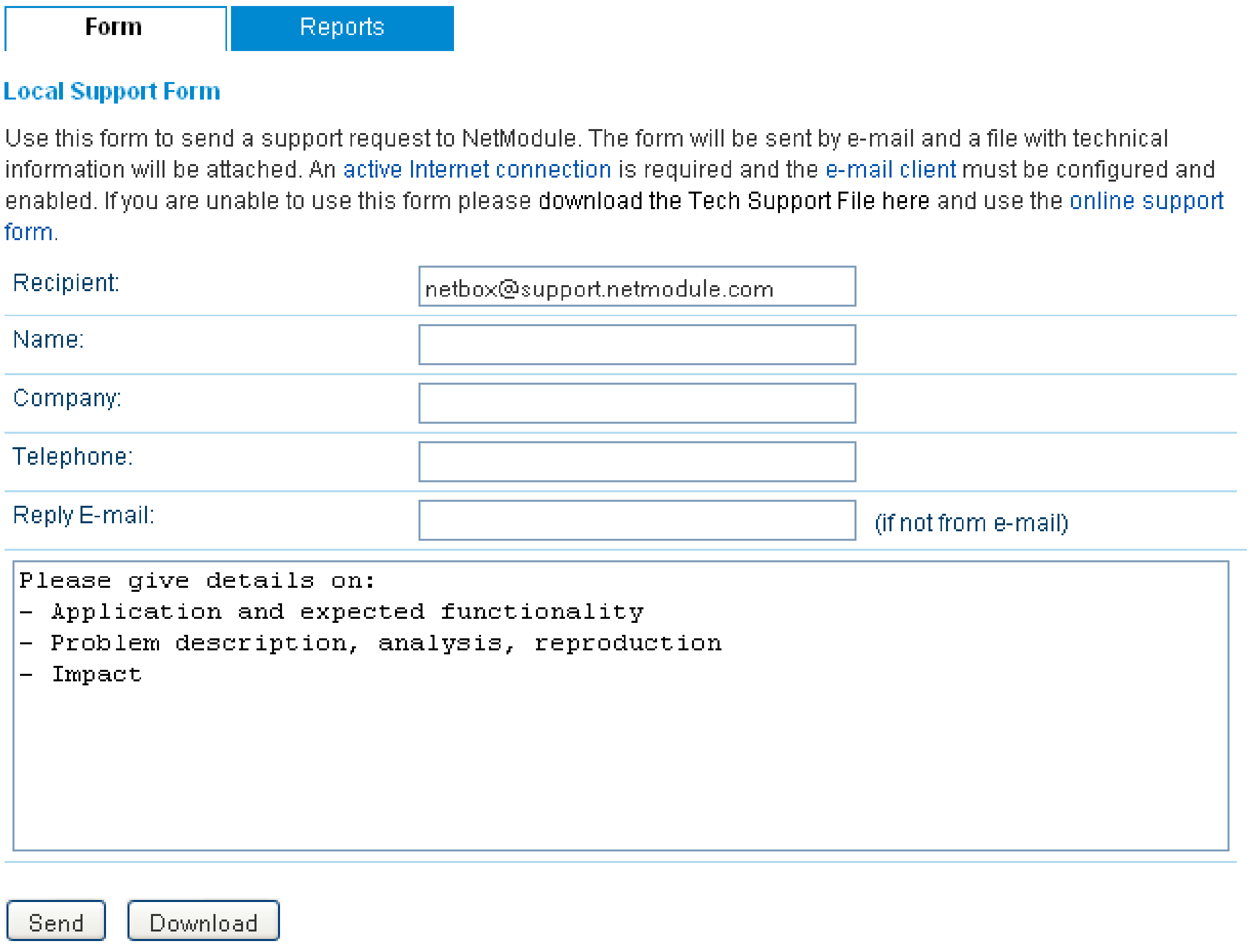
Restart



Die Seite mit der Adresse http://192.168.1....

Do you want to restart the device?

5.1.8.4.5 Tech Support

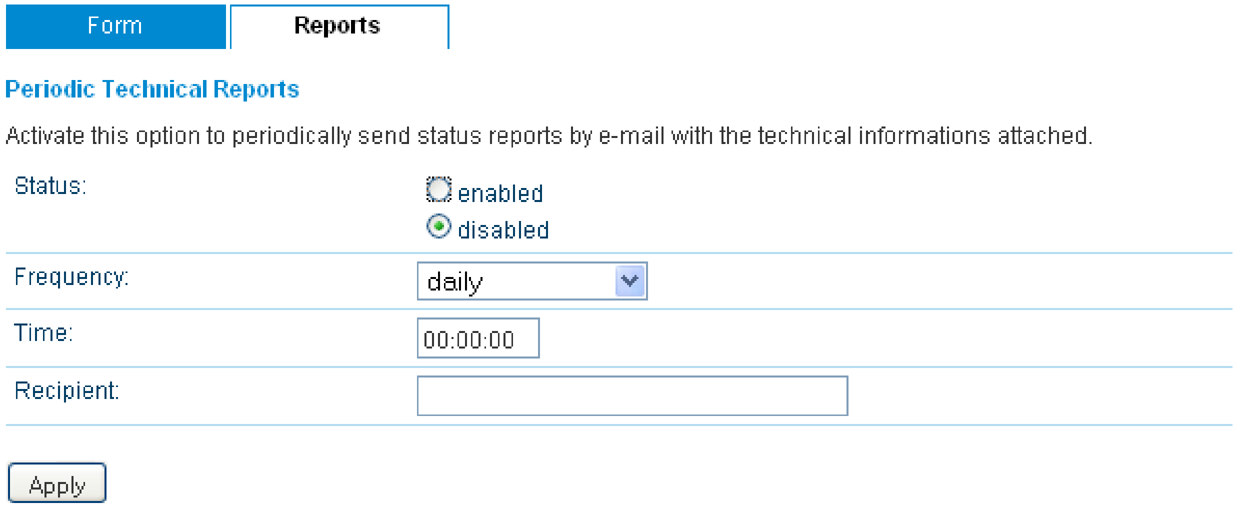


Local Support Form

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

Recipient:	netbox@support.netmodule.com	
Name:		
Company:		
Telephone:		
Reply E-mail:		(if not from e-mail)

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

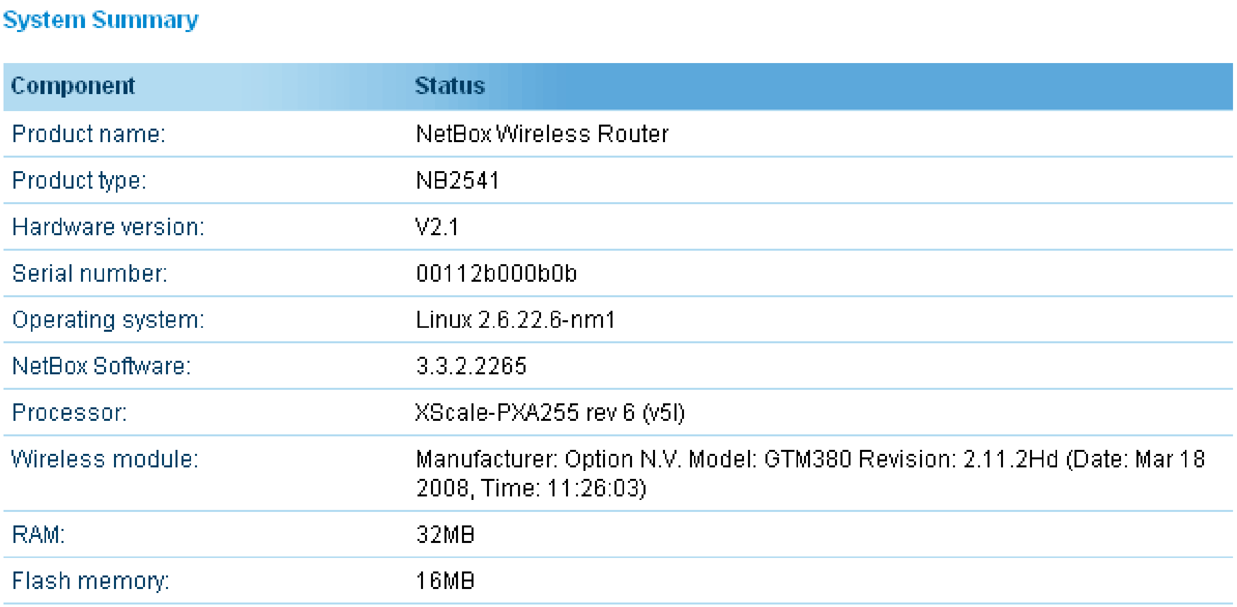


Periodic Technical Reports

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

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

5.1.8.4.6 System Information:

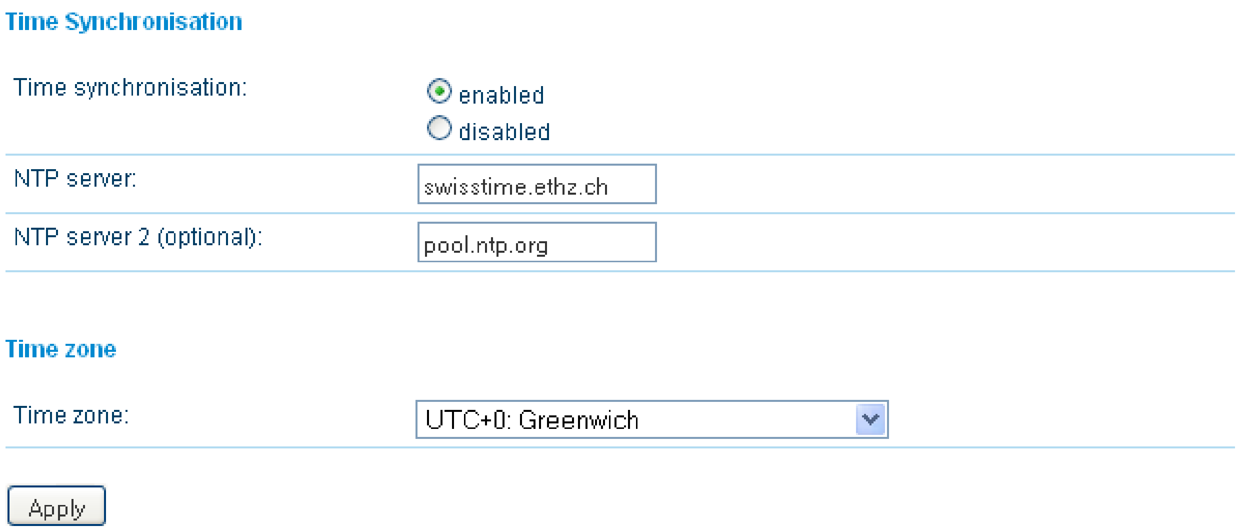


System Summary

Component	Status
Product name:	NetBox Wireless Router
Product type:	NB2541
Hardware version:	V2.1
Serial number:	00112b000b0b
Operating system:	Linux 2.6.22.6-nm1
NetBox Software:	3.3.2.2265
Processor:	XScale-PXA255 rev 6 (v5l)
Wireless module:	Manufacturer: Option N.V. Model: GTM380 Revision: 2.11.2Hd (Date: Mar 18 2008, Time: 11:26:03)
RAM:	32MB
Flash memory:	16MB

Provide this information when placing a support request.

5.1.8.4.7 Time and Region



Time Synchronisation

Time synchronisation:	● enabled ○ disabled
NTP server:	swisstime.ethz.ch
NTP server 2 (optional):	pool.ntp.org

Time zone

Time zone:	UTC+0: Greenwich

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

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

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

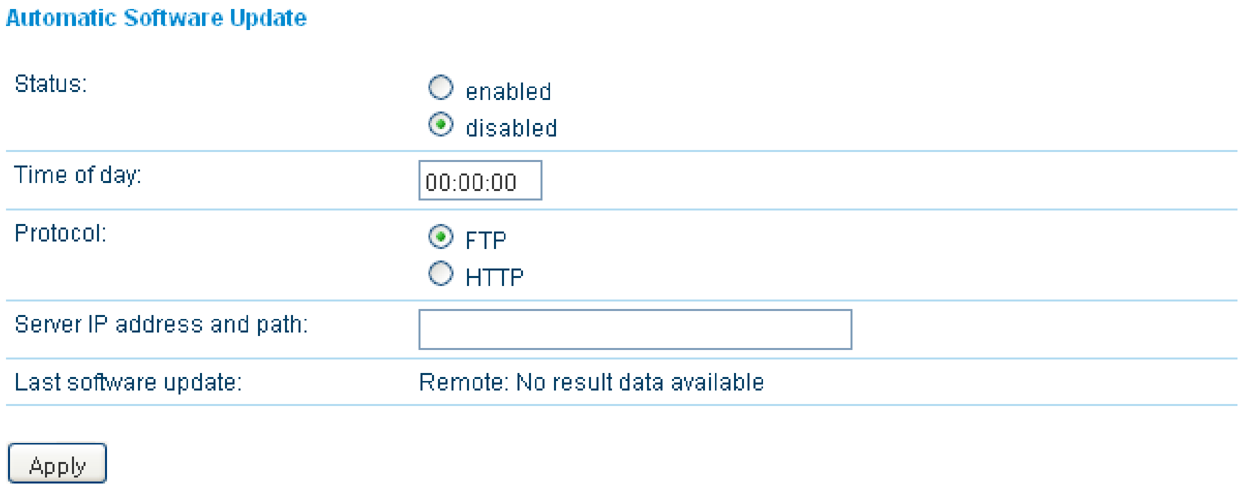
Time zone:	Time zone

5.1.8.5 Software Update

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

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

5.1.8.5.1 Automatic Software Update



Automatic Software Update

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

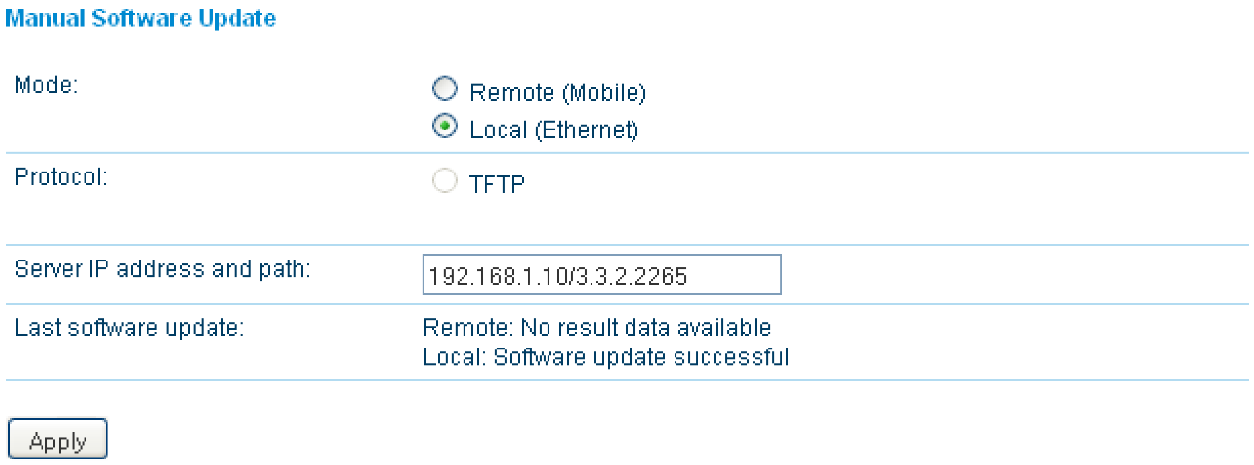
Parameter	Description
Status:	Enable/disable automatic software update
Time of day:	Every day at this time NetBox will do a check for updates
Mode;	Update over mobile or Ethernet Interface?
Protocol:	Specify the protocol used to transfer the new software to NetBox. You will need an appropriate server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

5.1.8.5.2 Manual Software Update

NB1310: The new software image (e.g. NBSW_3.3.2.4542.bin) can be uploaded using the Web Manager.

NB2xxx: The easiest way to update the NetBox Software (NBSW) is to connect NetBox to network with a TFTP server. If you only have a Notebook or a PC available the update process involves the preparation of a TFTP Server

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



Manual Software Update

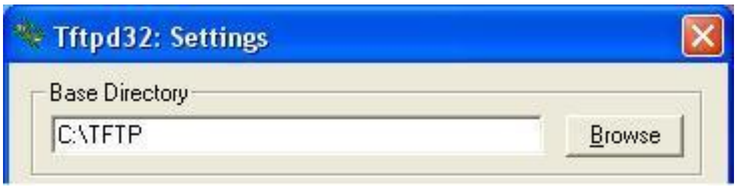
Mode:	○ Remote (Mobile) ● Local (Ethernet)
Protocol:	○ TFTP
Server IP address and path:	192.168.1.10/3.3.2.2265
Last software update:	Remote: No result data available Local: Software update successful

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

Step by Step:

Step	Description
1.	Connect your PC with NetBox using a network cable.
2.	If the IP address has been modified set it back to **192.168.1.1** and the subnet mask to **255.255.255.0** (see also chapter 0). Your PC must operate in the same subnet as NetBox.
3.	Set the IP address of your PC to **192.168.1.2** and the subnet mask to **255.255.255.0**
4.	Download the recommended TFTP server “TFTPD32” from our website, install it on your PC and start it. Configure the TFTP server as follows:

- In the dialog „Tftpd32: Settings“ choose the base directory (e.g. „C:\TFTP“). Create a new directory if there is none.



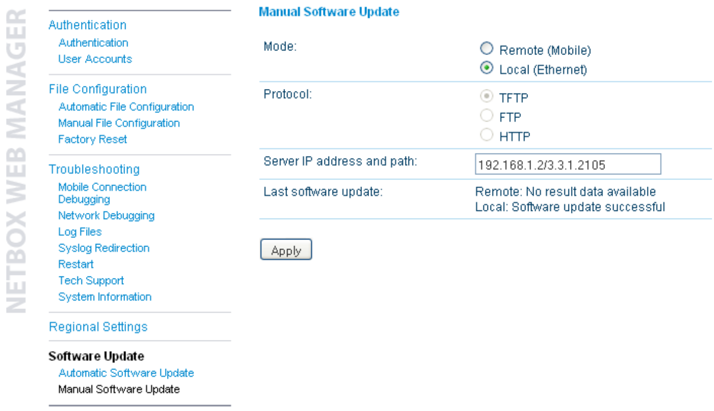
Tftpd32: Settings

Base Directory

C:\TFTP

- Unpack the new NBSW to this directory into a subfolder such as 3.3.1.2135

5. On the web page “SYSTEM->Manual Software Update” enter the IP address and path of the TFTP server (**192.168.1.2**) as follows:



Manual Software Update

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

Protocol: ● TFTP ○ FTP ○ HTTP

Server IP address and path: 192.168.1.2/3.3.1.2105

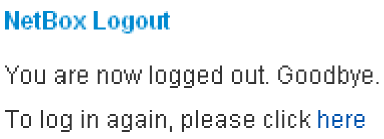
Last software update: Remote: No result data available
Local: Software update successful

6. Press [Apply] and confirm by pressing [OK].

Wait until the update is complete. See the progress bar
Do not unplug the power connector during the update!

7. Check the results of the update. Refreshing the page or even reopening the browser windows may avoid cache problem. In case of success, „Software update successful“ will be displayed, otherwise an error message.

5.1.9 Logout



NetBox Logout

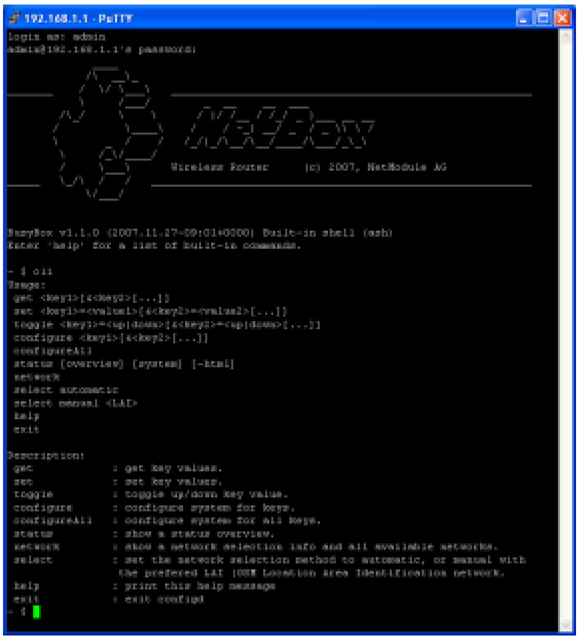
You are now logged out. Goodbye.

To log in again, please click here

Log out from Web Manager

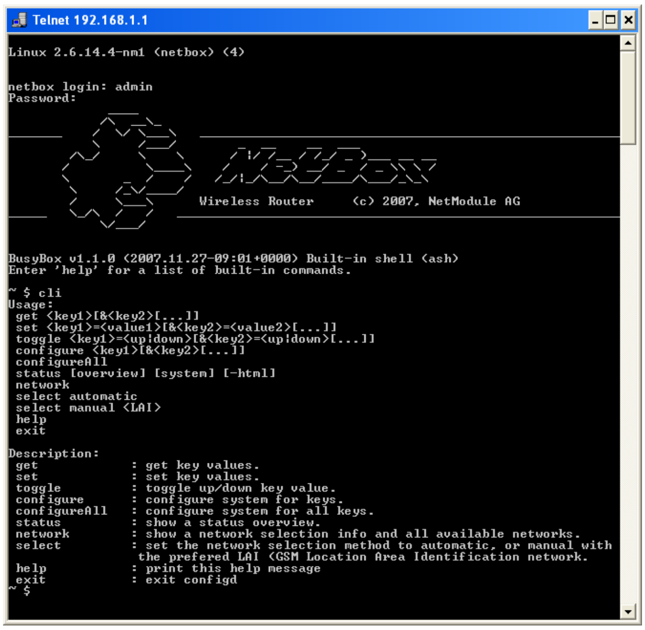
5.2 Configuration via Command Line Interface (CLI)

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



```
login as: admin
admin@192.168.1.1's password:

                                   Wireless Router      (c) 2007, NetModule AG

BusyBox v1.1.0 (2007.11.27-09:01+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

~ $ cli
Usage:
 get <key1>[&<key2>[...]]
 set <key1>=<value1>[&<key2>=<value2>[...]]
 toggle <key1>=<up|down>[&<key2>=<up|down>[...]]
 configure <key1>[&<key2>[...]]
 configureAll
 status [overview] [system] [-html]
 network
 select automatic
 select manual <LAI>
 help
 exit

Description:
 get            : get key values.
 set            : set key values.
 toggle         : toggle up/down key value.
 configure      : configure system for keys.
 configureAll   : configure system for all keys.
 status         : show a status overview.
 network        : show a network selection info and all available networks.
 select         : set the network selection method to automatic, or manual with
                  the prefered LAI (GSM Location Area Identification network.
 help           : print this help message
 exit           : exit configd
~ $
```

Logon via SSH with PuTTY



```
Linux 2.6.14.4-nm1 (netbox) (4)

netbox login: admin
Password:

                                    Wireless Router     (c) 2007, NetModule AG

BusyBox v1.1.0 (2007.11.27-09:01+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

~ $ cli
Usage:
 get <key1>[&<key2>[...]]
 set <key1>=<value1>[&<key2>=<value2>[...]]
 toggle <key1>=<up|down>[&<key2>=<up|down>[...]]
 configure <key1>[&<key2>[...]]
 configureAll
 status [overview] [system] [-html]
 network
 select automatic
 select manual <LAI>
 help
 exit

Description:
 get             : get key values.
 set             : set key values.
 toggle          : toggle up/down key value.
 configure       : configure system for keys.
 configureAll    : configure system for all keys.
 status          : show a status overview.
 network         : show a network selection info and all available networks.
 select          : set the network selection method to automatic, or manual with
                  the prefered LAI (GSM Location Area Identification network.
 help            : print this help message
 exit            : exit configd
~ $
```

Logon via Telnet via Windows Telnet Client

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

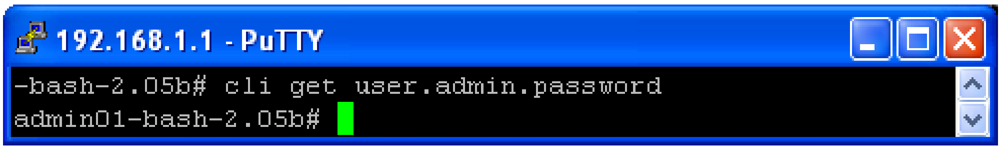
5.2.1 CLI Overview

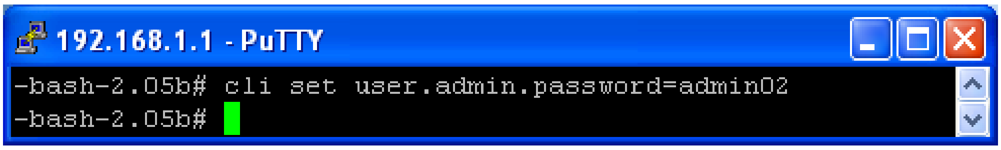
The Command Line Interface mainly provides functions to read and write values of the NetBox configuration parameters. In addition, the CLI provides functions to query status information.

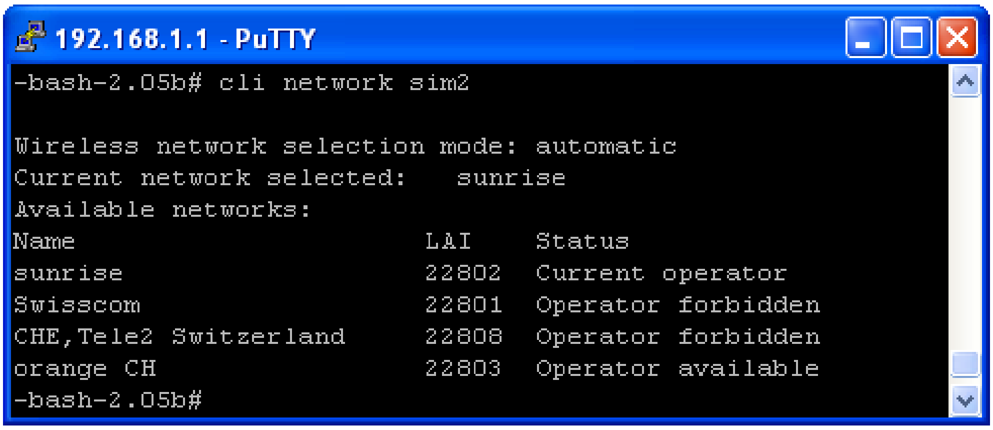
Command	Return	Description
cli get	string	Read values of one or more specified configuration parameters.
cli set	void	Write values of one or more specified configuration parameters.
cli network	string	Show available networks including Location Area Identities (LAIs)
cli select	void	Select the network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

5.2.2 CLI Usage

Command	Usage and Return Value

cli get	‘cli get’ is used to read values from configuration parameters.
	Arguments include all configuration keys as described in chapter 3.2
	Usage: cli get <key1>[&<key2>[...]]
	Example: cli get user.admin.password
	The return value is the value of the queried parameter.
	
	
	`-bash-2.05b# cli get user.admin.password`
	`admin01-bash-2.05b#`
	Note: cli get <invalidKey> returns no error message

cli set	‘cli set’ is used to assign values to configuration parameters.
	Arguments include all configuration keys as described in chapter 3.2
	Usage: set <key1>=<value1>[&<key2>=<value2>[...]]
	Example: cli set user.admin.password=admin02
	
	
	`-bash-2.05b# cli set user.admin.password=admin02`
	`-bash-2.05b#`
	‘cli set’ produces no return value and no error message. To check if the modification took place, use ‘cli get’
	Note: cli set <invalidKey>=<correctValue> returns no error message
	Note: cli set <validKey>=< inCorrectValue> returns no error message, no range check is performed

cli network	'cli network' provides mobile network information on the optionally specified SIM card. If no SIM card is specified, the command is applied to SIM1. The information returned includes the Local Area Identity (LAI)
	Usage: network [sim1/sim2]
	Example: cli network sim2
	
	
	`-bash-2.05b# cli network sim2`
	
	`Wireless network selection mode: automatic`
	`Current network selected:   sunrise`
	`Available networks:`
	`Name                          LAI    Status`
	`sunrise                       22802  Current operator`
	`Swisscom                      22801  Operator forbidden`
	`CHE,Tele2 Switzerland         22808  Operator forbidden`
	`orange CH                     22803  Operator available`
	`-bash-2.05b#`
	
	Note: The following commands are identical:
	'cli network' and 'cli network sim1'

cli select automatic	'cli select automatic' sets the network selection mode for the specified SIM card to automatic. Usage: select automatic [sim1/sim2] Note: The following commands are identical: 'cli select automatic' and 'cli select automatic sim1' Note: The following commands have the same effect: 'cli select automatic sim1' and 'cli set networkselection.mode=automatic' 'cli select automatic sim2' and 'cli set networkselection.sim2.mode=automatic'
cli select manual	'cli select manual' selects the network provider defined by the supplied Local Area Identity (LAI) for the specified SIM card Usage: select manual <LAI> [sim1/sim2] Note: The following commands are identical: 'cli select manual <lai>' and 'cli select manual sim1 <lai>' Note: The following commands have the same effect: 'cli select manual <lai> sim1' and 'cli set networkselection.network_lai=<lai> 'cli select manual <lai> sim2' and 'cli set networkselection.sim2.network_lai=<lai>

cli status	'cli status' returns both, 'cli status overview' and 'cli status system' concatenated. The option -hml is used to query a HTML version of the status information.
cli status overview	show the status of all interfaces, networks and services.
cli status overview interfaces	show the status of all interfaces
cli status overview interfaces sim_state	show the state of the SIM-Card
cli status overview interfaces pin_state	show the state of the PIN
cli status overview interfaces signal_strength	show the actual signal strength
cli status overview interfaces con_state	show the state of the wireless connection
cli status overview interfaces con_type	show the type of the wireless connection
cli status overview interfaces net_sel_mode	show the mode of the network selection
cli status overview interfaces net_sel_prov	show the current network provider
cli status overview interfaces data_rxtx	show the amount of received and transmitted data
cli status overview interfaces stream_updown	show the actual down- and upstream rates
cli status overview interfaces last_reset	show the last reset date of data counter
cli status overview networks	show the status of all networks
cli status overview networks napt_state_mob	show the state of the NAPT service on the mobile if
cli status overview networks napt_state_ovpn	show the state of the NAPT service on the vpn if
cli status overview networks openvpn_state	show the state of the OpenVPN connection
cli status overview networks ipsec_state	show the state of the IPsec connection
cli status overview networks pptp_state	show the state of the PPTP server
cli status overview services	show the status of all services
cli status overview services dyndns_state	show the state of the Dynamic DNS client
cli status overview services dialin_state	show the state of the Dial-in service
cli status overview services dhcp_state	show the state of the DHCP server
cli status overview services dns_state	show the state of the DNS Proxy server
cli status overview services gps_state	show the state of the GPS signal
cli status overview services keepalive_state	show the state of the Keep-alive service
cli status overview services sms_rec_state	show the state of the SMS receiving service
cli status overview services sms_send_state	show the state of the SMS sending service
cli status overview services email_state	show the state of the E-Mail service
cli status overview services dig_in	show the state of the digital inputs
cli status overview services dig_out	show the state of the digital outputs
cli status system	show NetBox systems information including hardware and software versions.
cli status system prod_name	show the NetBox product name
cli status system prod_type	show the NetBox product type
cli status system hw_ver	show the NetBox hardware version

cli status system serial	show the NetBox serial number
cli status system os	show the NetBox operating system
cli status system nbsw	show the NetBox software version
cli status system cpu	show the NetBox CPU
cli status system wireless_module	show the NetBox wireless module
cli status system ram	show the amount of RAM installed in the NetBox
cli status system flash	show the amount of flash installed in the NetBox
help	Print the cli help message (usage)

5.2.3 Configuration Parameters of the NetBox

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

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

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

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

5.2.4 Interfaces related Parameters

5.2.4.1 Ethernet

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

5.2.4.2 Mobile Interface and SIM Cards

Parameter	Default Value	Range	Description
simcard.check.pincode	void	4 digit numeric value	PIN code, e.g. 1234
simcard.pinStatus	0	[0,1]	0 = PIN protection disabled 1 = PIN protection enabled
simcard.sim2.check.pincode	void	4 digit numeric value	PIN code, e.g. 1234
simcard.sim2.pinStatus	0	[0,1]	0 = PIN protection disabled 1 = PIN protection enabled
networkselection.mode	automatic	[automatic,manual]	
networkselection.network_lai	void	numeric value (LAI)	Select the network provider defined by the supplied Local Area Identity (LAI)
networkselection.sim2.mode	automatic	[automatic,manual]	
networkselection.sim2.network_lai	void	numeric value (LAI)	Select the network provider defined by the supplied Local Area Identity (LAI)
dialout.connectionMethod	0	[0..2]	0 = manual only 1 = dial on demand 2 = permanent
dialout.connSetup.redialAttempt	2	[1..4294967296]	Redial attempts
dialout.connSetup.idleTimeout	1	[1..35791394]	Idle timeout in minutes (in case of dial on demand)
dialout.profiles.0.name	void	username	Profile name
dialout.profiles.0.username	void	username	Username
dialout.profiles.0.password	void	password	Password
dialout.profiles.0.phoneNumber	void	phone number	Phone number

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

dialout.profiles.0.apn	void	hostname	Acess Point Name
dialout.profiles.0.IPHC	void	[0,1]	0 = off 1 = enable IP header compression
dialout.profiles.0.IPSC	void	[0,1]	0 = off 1 = enable software compression
dialout.profiles.0.queryDNS=1	void	[0,1]	0 = do not query DNS server 1 = query DNS server
dialout.profiles.0.ESCIP	void	[0,1]	0 = off 1 = enable specific client IP address
dialout.profiles.0.SCAddress	void	ipaddress	Specific client address
dialout.profiles.0.SIM	SIM1	[SIM1,SIM2]	SIM used for primary profile
dialout.profiles.0.ISDN	void	[0,1]	0 = normal call

			1 = is ISDN call
dialout.profiles.0.switchCondition	never	[never, redialAttemptsReached]	Condition for profile switch
dialout.profiles.1.name	void	username	Profile name
dialout.profiles.1.username	void	username	Username
dialout.profiles.1.password	void	password	Password
dialout.profiles.1.phoneNumber	void	phone number	Phone number

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

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

5.2.4.3 Digital I/O

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

5.2.5 Routing related Parameters

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

5.2.6 Firewall related Parameters

5.2.6.1 NAPT on mobile Interface

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

5.2.6.2 NAPT on OpenVPN Interface

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

5.2.6.3 Access Control List Local Host

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

5.2.6.4 Access Control List for Exposed Host on Mobile Interface

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

5.2.6.5 Access Control List for Exposed Host on OpenVPN Interface

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

5.2.7 VPN related Parameters

5.2.7.1 OpenVPN

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

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

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

5.2.7.2 IPsec Parameters

Parameter	Default Value	Range	Description
ipsec.status	0	[0,1]	0 = disabled 1= enabled
ipsec.remote.serverIp	void	ipaddress	
ipsec.remote.lanAddress	void	Ipaddress	
ipsec.remote.lanMask	255.255.0.0	netmask	
ipsec.ike.psk	void	password	
ipsec.ike.mode	identity-protection	[identity-protection, aggressive]	
ipsec.ike.encryption	3des	3des	
ipsec.ike.hash	md5	[sha1, md5]	
ipsec.ike.dh	modp1024	[modp1024, modp1536]	
ipsec.ike.localId	void	username	
ipsec.ike.remoteId	void	username	
ipsec.esp.encryption	3des	3des	
ipsec.esp.hash	md5	[sha1, md5]	
ipsec.pfs	0	[0,1]	0 = disabled 1= enabled
ipsec.dpd.state	1	[0,1]	0 = disabled 1= enabled
ipsec.dpd.cycle	30	[5.. 120]	In seconds
ipsec.dpd.failureCount	3	[1.. 10]	

5.2.7.3 PPTP Server

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

5.2.7.4 Dial-in Server

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

5.2.8 Services related Parameters

5.2.8.1 COM Server

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

5.2.8.2 DNS Proxy Server

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

5.2.8.3 DHCP Server

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

5.2.8.4 Dynamic DNS

Parameter	Default Value	Range	Description

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

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

5.2.8.5 SMS Parameters

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

5.2.8.6 E-Mail Parameters

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

5.2.8.7 GPS Parameters

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

5.2.8.8 Event Manager

5.2.8.8.1 Events

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

5.2.8.8.2 Subscribers

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

5.2.8.8.3 Event Processor

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

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

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

5.2.8.9 SNMP Agent

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

5.2.8.10 SSH Server

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

5.2.8.11 Telnet Server

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

5.2.8.12 Web Server

Parameter	Default Value	Range	Description
webServer.http.port	80	[1 .. 65535]	
webServer.https.port	443	[1 .. 65535]	

5.2.8.13 UDP Message Receiver

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

5.2.8.14 Keep-Alive

Not supported anymore in the Web Manager since NBSW 3.3.1.2105

Parameter	Default Value	Range	Description
keepalive.serverIpAddress	services.netmodule .com	hostname	
keepalive.port	50001	[1 .. 65535]	Server port
keepalive.updateInterval	60	[0..2147483647]	Update interval in seconds
keepalive.identifier	void	hostname	Identifier string
keepalive.status	0	[0,1]	0 = disabled 1= enabled

5.2.9 System related Parameters

5.2.9.1 User Accounts

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

5.2.9.2 Troubleshooting

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

5.2.9.3 Time Synchronization

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

5.2.9.4 Software Update

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

5.2.9.5 Configuration Update

Parameter	Default Value	Range	Description
cfg_auto.status	1	[0,1]	0 = disabled

			1= enabled
cfg_auto.time	void	time	hh:mm:ss
cfg_auto.url	void	hostname	

6 Software Interfaces

6.1 GPS Server

6.1.1 Berlios GPS Server

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

6.1.2 NetModule GPS Server

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

6.1.2.1 $GPGGA - Global Positioning System Fix Data

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

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

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

6.1.2.2 $GPRMC - Recommended minimum specific GPS/Transit data

Format:

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

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

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

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

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

12	Mode	<mode>	A = autonomic = valid
			E = estimated
			N = not valid

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

6.1.2.3 $PNMID – NetModule Proprietary Sentence

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

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

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

6.2 Digital I/O Server

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

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

7							0
0	0	0	0	IN1	IN2	OUT1	OUT2

6.2.1 Monitor the digital inputs and outputs

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

6.2.2 Set digital outputs

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

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

6.2.3 Get status of digital inputs and output

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

Pattern	Description
00010000	Request a message with all states

6.3 HTTP Service Interface

The HTTP Service Interface is designed to administrate the NetBox with a self-written http client. It is available from NBSW 3.3.2.xxxx.

The HTTP Service Interface consists of four web pages located in the root directory of the NetBox web server:

- login.php (http clients can log in)
- logout.php (http clients can log out)
- upload.php (http clients can upload configuration files)
- download.php (http clients can download log files)
- cli.php (http clients can access the same functionality as provided by the Command Line Interface)

For further documentation regarding the HTTP Service Interface please contact NetModule.

6.3.1 Command Set

General Restrictions:

- When sending parameters within HTTP GET requests, dots (.) within variables must be replaced by colons (:). Example: The key name **user.admin.password** results in **user:admin:password**
- Authentication is required for all commands except GET /cli.php?status,[parameters]

HTTP Request	Description
GET /cli.php?status,[parameters]	Takes the same parameters as the CLI
GET /cli.php?get,[parameters]	Takes the same parameters as the CLI
GET /cli.php?set,[parameters]	Takes the same parameters as the CLI
GET /cli.php?sw-update,path=<value>	Starts a local software update from a TFTP server
GET /cli.php?reboot	Restarts the NetBox
GET /login.php?usr=<user>,pwd=<password>	Login to the HTTP Service Interface with supplied credentials
GET /logout.php	Logout from the HTTP Service Interface
GET /download.php?file=<fileName>	Download a file • Debug log: file=debuglog • Boot log: file=bootlog
POST /upload.php	Takes a new configuration file as user-config.cfg or as user-config.zip. The content of the file must be the same as provided for the Web Manager.

6.3.2 Responses

HTTP Request	Responses (String)	Description
All HTTP Service Interface Commands	0: device busy	The NetBox is busy. Resend the request later.
All HTTP Service Interface Commands	0: login required	This command requires authentication. Please use login.php first
GET /cli.php?status,[parameters]	<status>	A single or multiline string with the requested status information
GET /cli.php?get,[parameters]	<parameterValue>	The value of the requested configuration parameter
GET /cli.php?set,[parameters]	0: set failed	HTTP transfer is ok, but changing the configuration parameter failed.
	1: set ok	
GET /cli.php?sw-update,path=<value>	1: sw-update started from <path>	Software update started. Afterwards request the Software version with cli.php?status to verifiy whether it was successful or nor not
	0: maximum length of path is 26 characters	
	0: syntax error	Wrong syntax after in sw-update parameters
GET /cli.php?reboot	1: reboot initiated	A restart has been initiated
GET /login.php?usr=<user>,pwd=<password>	1: already logged in	
	1: already logged in but supplied credentials do not match	Already logged in but supplied credentials do not match
	1: login ok	Logged in successfully
	0: login failed	Login failed
GET /logout.php	1: logout ok	Logout OK
	1: already logged out	You were not logged in
GET /download.php?file=<fileName>	0: download <fileName> failed	Download failed
POST /upload.php	1: upload ok, files replaced, reconfiguration started	Upload ok, the provided files (e.g. OpenVPN certificates) were updated, the user-config.cfg will be applied
	1: upload ok, files replaced	No user-config.cfg provided but other files were updated (e.g. OpenVPN certificates)
	0: upload failed:	The upload failed

	<errorMessage>	

6.3.3 Examples

HTTP Request	Command	Description
Query the NetBox Firmware Version via HTTP	GET /cli.php?status,system,nbsw HTTP/1.1	
Login	GET /login.php?usr=admin,pwd=<password> HTTP/1.1	
Set the admin Password	GET /cli.php?set,user:admin:password=<password> HTTP/1.1	Remember: The dots (.) must be replaced by colons (:)
Upload new Configuration Files	POST /upload.php HTTP/1.1 Content-Disposition: form-data; name="UserConfigFile"; filename="user-config.zip" Content-Type: application/x-zip-compressed [Media]	A zip archive containing one or more of the following files can be uploaded. To run OpenVPN in certificate based mode, all certificate files are required. • user-config.cfg (the main configuration file) • ca.crt.certificate_mode (OpenVPN root certificate file) • client.crt.certificate_mode (OpenVPN client certificate file) • client.key.certificate_mode (OpenVPN private key file) • templateProfiles (updating provider database)
Download Debug Log	GET /download.php?file=debuglog HTTP/1.1	
Restart the NetBox	GET /cli.php?reboot HTTP/1.1	
Logout	GET /logout.php HTTP/1.1	
Start a local software update	GET /cli.php?sw-update,path=<ipTftp/path> HTTP/1.1	

7 Troubleshooting

7.1 Error Messages

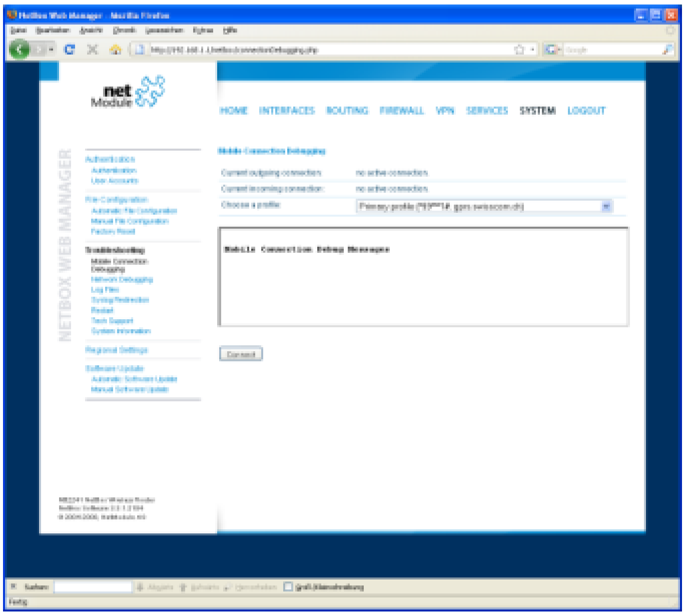
The Web Manager shows error messages in the status bar in the footer of a certain web page.

Common error messages are:

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

7.2 System Log and Log Files

Find more information about troubleshooting tools on page 78. The Web Manager provides varions debugging tools under SYSTEM/Troubleshooting:



Mobile Connection Debugging

Current outgoing connection: no active connection

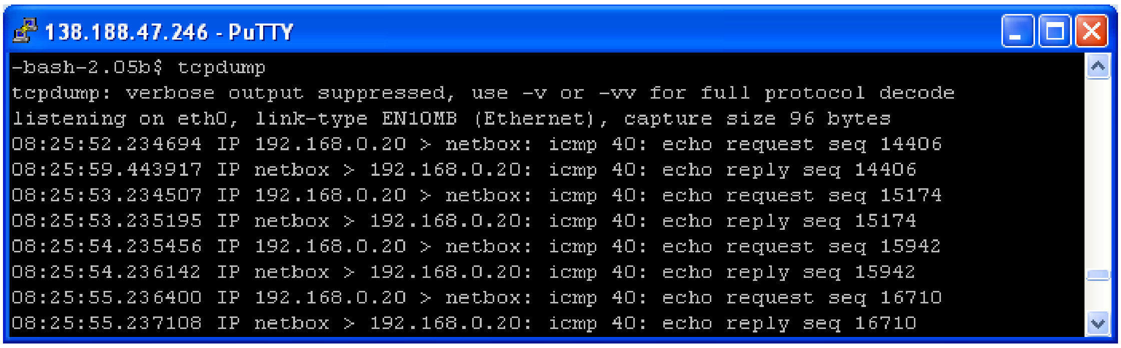
Current incoming connection: no active connection

Choose a profile: Primary profile (*99***1#, gprs.swisscom.ch)

```
Mobile Connection Debug Messages
```

7.3 Network Protocol Analyzer

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



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

8 Customer Service

8.1 Technical Support

The NetModule AG Website provides technical online support under:

http://www.netmodule.com/support

The Website also provides a download area where you can download the newest software and documentation.

For support requests please use the support form:

http://www.netmodule.com/support/supportform.aspx

8.2 Feedback

Please send comments about NetBox to:

netbox@support.netmodule.com