www.vscom.de

VPNRouter Manual

Edition: Juli 2016

Tel: +49 40 528 401 0
Fax: +49 40 528 401 99
Web: www.visionsystems.de
Support: service@visionsystems.de

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Trademarks

Disclaimer

Vision Systems reserves the right to make changes and improvements to its product without providing notice.

Vision Systems provides this document "as is", without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Vision Systems reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Vision Systems assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Contents

List of Figures

1. Introduction

The system VPNRouter impresses with its quality and robustness. This makes it possible to use the VPNRouter in different areas. Of course, the VPNRouter also has the latest security features such as a firewall or VPN. In general there is a trade-off between ease-of-use and security, VPNRouter optimizes this. The system is easy to install and use, but at the same time offers security given by strong encryption standards.

1.1. Manual Strategy and Details

This manual covers the configuration of the VPNRouter in detail.

1.2. Typing Conventions

When describing the manual has to reference some components visible on the screen. For better identification the reference is supported by showing the text in certain styles.

Software text is written in a slanted style. Such item represents *text output* written on the screen.

`User Input` Input forms require the user to `type some data` on the keyboard. Text written in style of a typewriter represents this input.

`[A Button]` Controling the software will also require to click some `[buttons]`. These buttons are represented by the name on them. The name is written in typewriter style on silver background, and surrounded by brackets.

`[A Button]` Further there are some `[blue buttons]` to control the web interface. These buttons are again represented by the name on them. This time the name is written in typewriter style white colour on blue background, still surrounded by brackets.

Component The manual will reference some components on the Device, then the **name of it** is written in bold.

2. Hardware

2.1. Product Features

	VPNRouter iR 5221/VPNRouter iR 3220
CPU	TI Sitara AM3352 ARM Cortex-A8 RISC CPU, 600MHz
RAM	256 MB DDR3 RAM
Flash	256 MB NAND Flash for boot Linux OS
SD-Slot	1 x Standard size
USB	2 x 2.0 High Speed as Host 1 x USB/OTG (VPNRouter iR 5221 only)
LAN	4 x 10/100 Fast Ethernet with integrated switch 2 x 10/100 Fast Ethernet on VPNRouter iR 3220
WAN	1 x 10/100/1000 Gigabit Ethernet
WLAN	optional, IEEE 802.11b/g/n
CAN-Bus	1 x CAN-Bus 20 kbps to 1 Mbps (VPNRouter iR 5221 only)
Serial Ports	2 x RS 232 / RS 422 / RS 485 up to 3.7 Mbps
Digital I/O	4 x input signals 4 x output signals (32 mA max.)
Console Port	RS 232, up to 115200bps
I^{2}C	max. 400 kHz
RTC	yes
Watch Dog Timer	yes
MiniPCIe-Slot	yes, with SIM Card Slot
Reset Button	HW Reset
Power Input	12-50V DC
Power Consumption	0.3A @ 12V min.
Dimensions (W x L x H)	154 x 104 x 50 mm
Antenna	The case is prepared for two antenna sockets, e.g. WLAN and GPS

Table 1: Product Hardware Specifications

	VPNRouter iR 2110
CPU	TI Sitara AM3352 ARM Cortex-A8 RISC CPU, 600MHz
RAM	256 MB DDR3 RAM
Flash	256 MB NAND Flash for boot Linux OS
SD-Slot	1 x external, size microSD
USB	1 x 2.0 High Speed as Host
LAN	1 x 10/100 Fast Ethernet
WAN	1 x 10/100/1000 Gigabit Ethernet
WLAN	optional, IEEE 802.11b/g/n
Serial Ports	1 x RS 232 / RS 422 / RS 485 up to 3.7 Mbps
Console Port	TTL internal, up to 115200bps adapter to USB available
RTC	yes
Watch Dog Timer	yes
Reset Button	HW Reset
Power Input	9-54V DC
Power Consumption	0.2A @ 12V min.
Dimensions (W x L x H)	115 x 73 x 25 mm
Antenna	The case provides two positions for an antenna socket

Table 2: Product Hardware Specifications

2.1.1. Ethernet

Two independent ports for Ethernet are available in VPNRouter, with separate MAC Addresses. One port is implemented as GigaLAN for 10/100/1000 Mbit/s, the other provides an internal Ethernet switch for Fast Ethernet function 10/100 Mbit/s. The VPNRouter iR 5221 provides four Fast Ethernet ports, on VPNRouter iR 3220 there are two of them and VPNRouter iR 2110 has only one missing the Ethernet switch.

2.1.2. USB

Two USB Host ports for USB 2.0 High Speed allow to connect any devices. The VPNRouter iR 2110 has only one port. Support for certain WLAN and 3G/4G adapters is available.

On VPNRouter iR 5221 only: there is one extra port type USB 2.0 OTG for Host and Device operation mode.

2.1.3. CAN-Bus

On VPNRouter iR 5221 only: one CAN port for CAN 2.0A and 2.0B is available. The port operates from 20 kbit/s up to 1 Mbit/s.

2.1.4. Serial Ports

Two serial ports are provided in RS 232 / 422 / 485 modes that can be configured by software or by DIP switch where as the VPNRouter iR 2110 has only one serial port configurable by software. For the detailed information about the supported modes refer to the Table 3.

	RS 232	**RS 422**	**RS 485**
Modes	full duplex	full duplex	2-wire: half duplex, without echo 4-wire: full duplex
Signals	TxD, RxD, RTS, CTS, DTR, DSR, DCD, RI, GND	Tx+/-, Rx+/-, GND	2-wire: Data+/-, GND 4-wire: Tx+/-, Rx+/-, GND
Data Direction Control			by driver, via RTS
Speed	up to 921.6 / 1000 kbps	up to 3.7 Mbps	up to 3.7 Mbps

Table 3: Serial Interface Specifications

2.1.5. Digital I/O

Four input and four output signals at TTL level are provided. For input signals the change of at least one input signal generates an interrupt. See Section 4.3 on page 17 for electrical characteristics. The VPNRouter iR 2110 does not have these.

2.1.6. I²C

One port for external I²C function is provided. The signals originate in a repeater, to protect the internal circuits from external misconfiguration or signal shorting. The VPNRouter iR 2110 does not have this port.

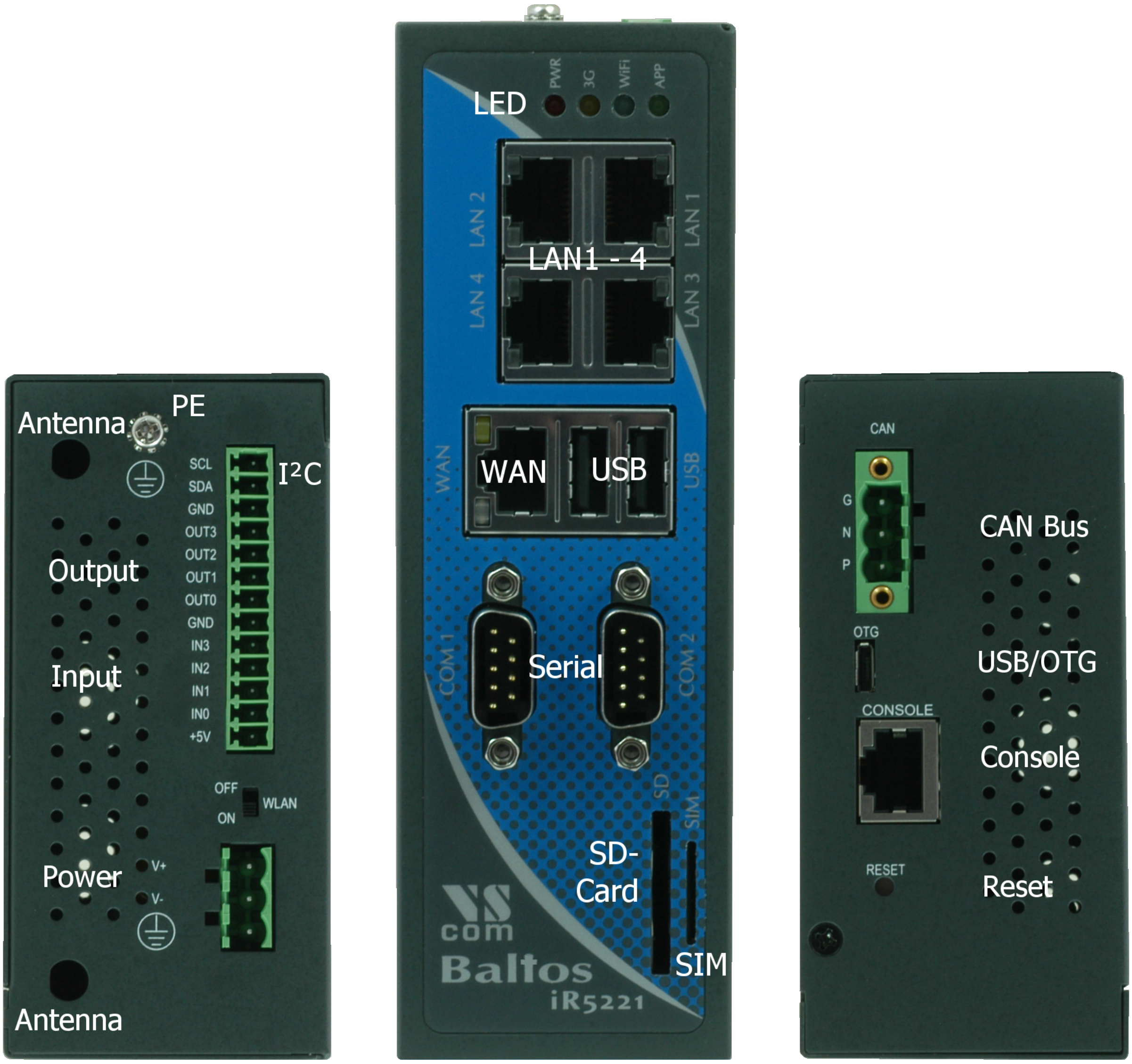
2.1.7. WLAN

The VPNRouter is available with an optional built-in WLAN function as of IEEE 802.11b/g/n for wireless connection.

3. Appearance

This is how the VPNRouter systems look like on the top, front and bottom sides.

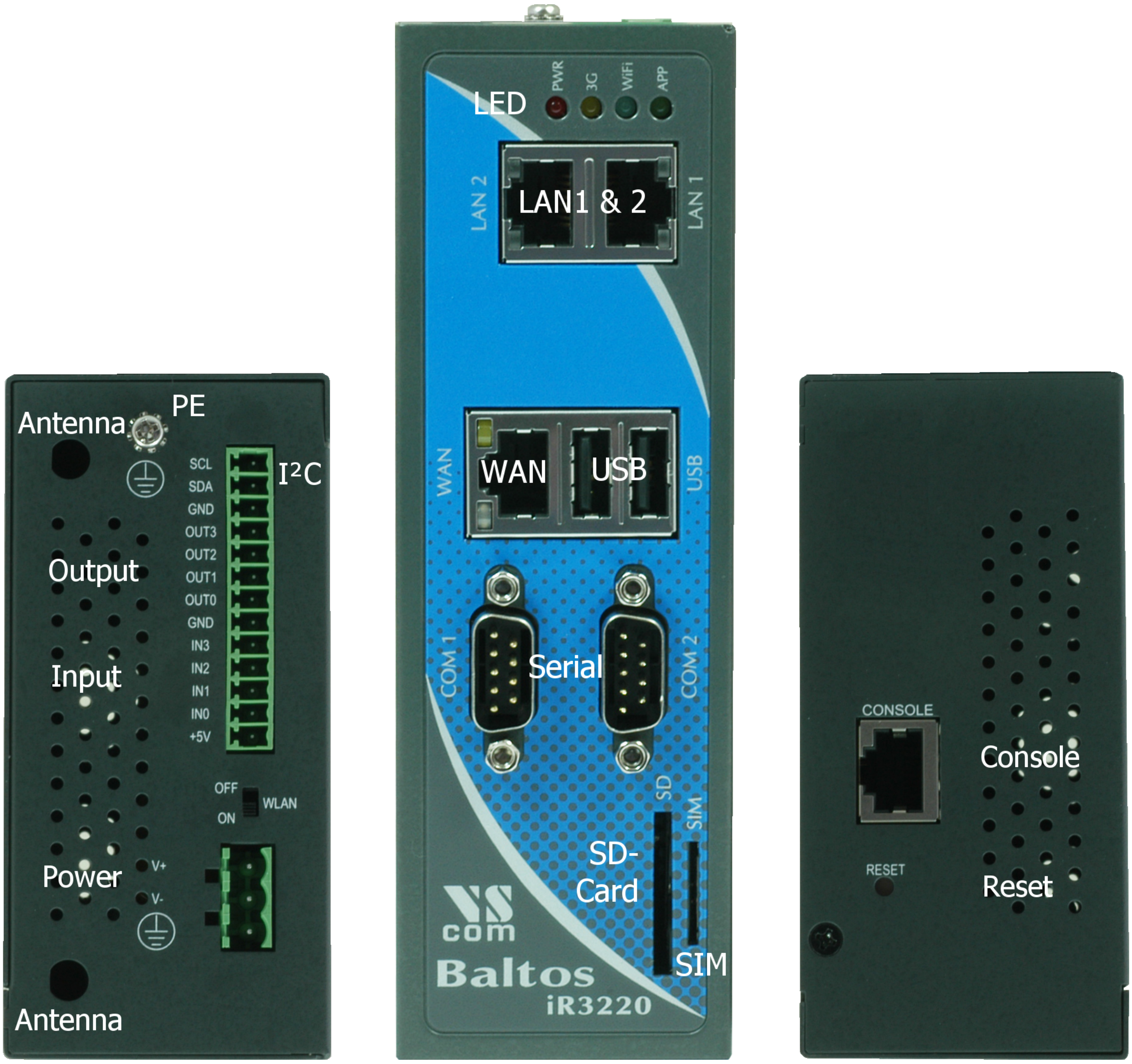
3.1. VPNRouter iR 5221



(a) Top View (b) Front View (c) Bottom View

Figure 1: Appearance VPNRouter iR 5221

3.2. VPNRouter iR 3220



(a) Top View (b) Front View (c) Bottom View

Figure 2: Appearance VPNRouter iR 3220

The VPNRouter iR 3220 provides two ports for LAN, the CAN Bus connector and the USB/OTG port are not implemented.

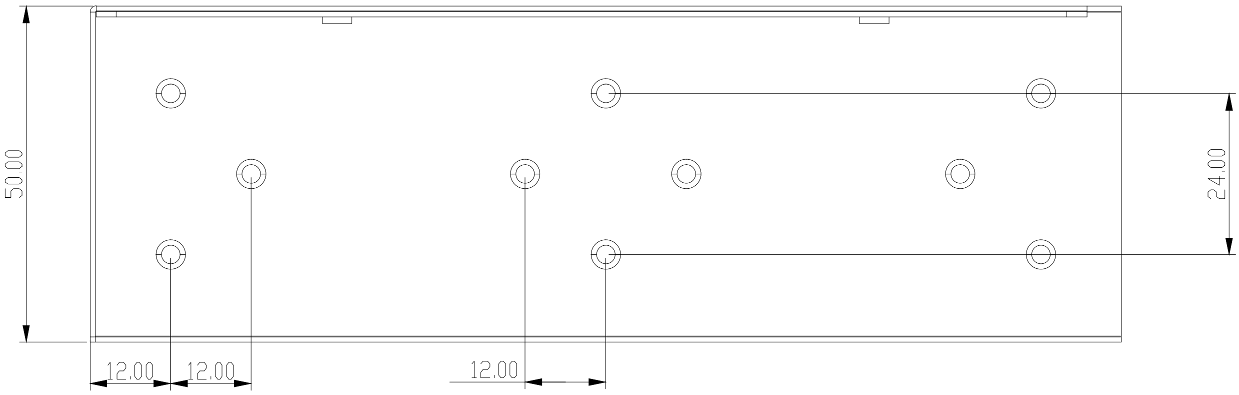
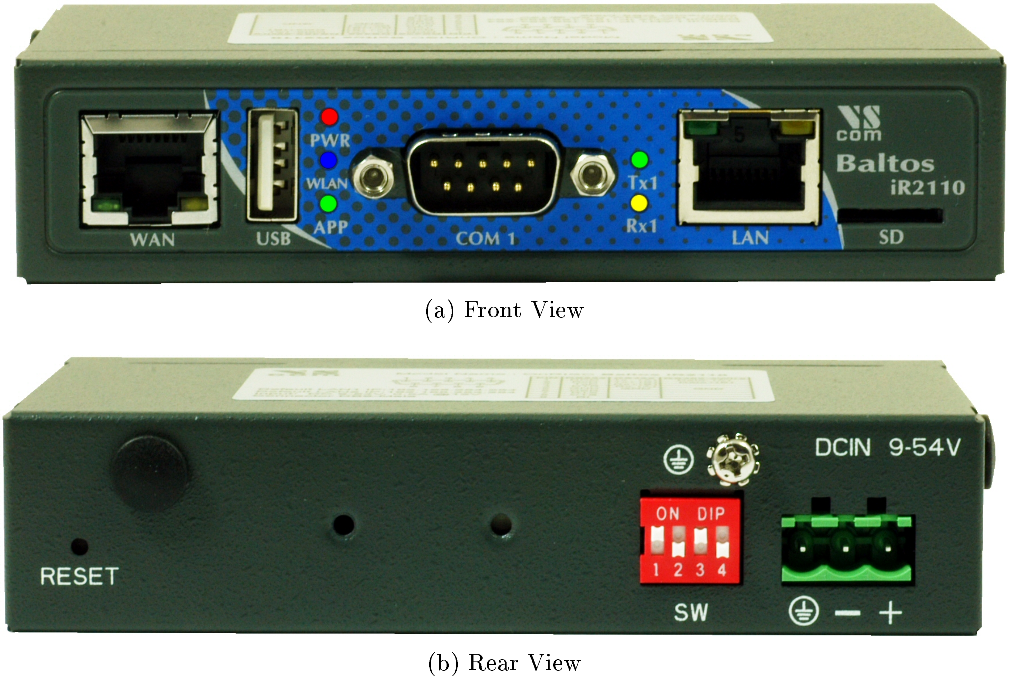


Figure 4: Mounting Positions VPNRouter iR 5221/VPNRouter iR 3220

3.3. VPNRouter iR 2110 Front and Rear



(a) Front View

(b) Rear View

Figure 3: Appearance VPNRouter iR 2110

The front side has the Gigabit WAN port and USB. Then there is the serial port and the Fast Ethernet LAN port. Small on the lower right is the slot for a microSD card.
The rear side provides the socket for the terminal block power connector. On this side also a DIN Rail clamp may be mounted. The DIP switches define the operation mode of the serial port. There is a possible location for a WLAN antenna. The Reset button is pushed by a small prick.

3.4. Mechanics for Mounting

This are the positions of screws for mounting. The groups of three on the left and right (actually top and bottom) hold the metal plates for wall mounting.

The group of four in the middle is for the DIN Rail mounting clamp. This may be mounted in standard orientation, or turned by 90° to provide for a (seldom used) horizontal fixture on the DIN Rail.

Figure 5a is a reference for the positions of front side connectors. It is for demonstration only.

Figure 5b shows the positions of screws for fixing. Note, this is upside down with respect to the front side. The two M3 screw positions in the middle allow to fix an DIN Rail clamp. There is also the position of a possible antenna socket near the Reset button.

4. Position of Connectors and Functions of VPNRouter iR 5221 and VPNRouter iR 3220

First the connectors and functions located on the top side of VPNRouter iR 5221 and VPNRouter iR 3220 are described. The next components are those on the front side, finally followed by those on the bottom side.

4.1. Power

The VPNRouter device is powered by a single power supply in a wide range from 12 V to 50 V DC. A suitable power supply adapter is available as add-on component, and part of the starter kit package. Connect the cable to the power jack at the top side of VPNRouter, and plug the adapter into the socket. The Power LED (red) on VPNRouter will light. You can connect a power supply of your choice, providing the technical requirements are met.

Warning: disconnect the VPNRouter from power supply before performing installation or wiring. The wire size must follow the maximum current specifications. The maximum possible current in the power wires as well as in the common wires must be taken under consideration. If the current rises above the maximum ratings, the wiring can overheat, causing serious damage to your equipment. When powered, the VPNRouter's internal components generate heat, and consequently the outer case may feel warm to the touch.

4.1.1. Connection and Polarity

Power is connected via three clamps on a terminal block, located on the top side of VPNRouter iR 5221/VPNRout

Warning: do not confuse the CAN connector at the bottom side for power input. Such may damage the CAN bus port.

Clamp	3	2	1
Function	PE	V-	V+

Table 4: Power Connector

V+ and V- are clamps for DC voltage supply. PE is the clamp to connect the case and shields of connection cables to Protective Earth. PE is internally connected to logic ground, which is on the level of V-supply line.

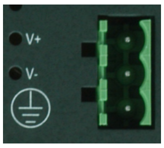
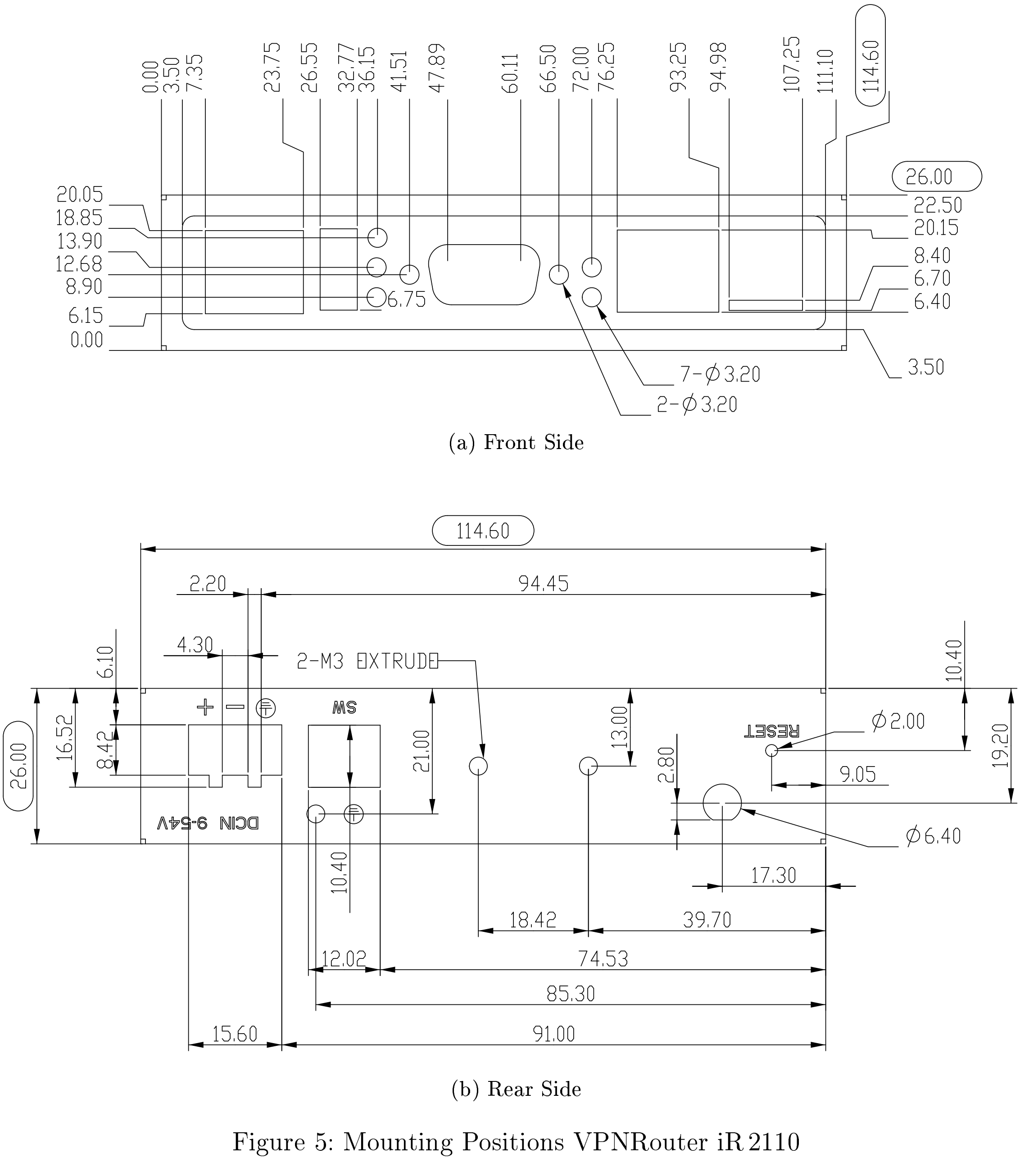


Figure 6: Power Connector



(a) Front Side

(b) Rear Side

Figure 5: Mounting Positions VPNRouter iR 2110

Attention: Never connect the Terminal block for power supply in reversed direction, i.e. turned by 180°. This would connect the power between V- (logic ground) and case/protective ground. High current is the result, causing damage inside the system.

4.1.2. Grounding

Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the ground screw to the grounding surface prior to connecting devices.

In noisy environments the case of VPNRouter shall be directly connected to Protective Earth. This is the purpose of the dedicated PE Screw on the case top/rear side.

Figure 7: PE Screw

4.2. WLAN Switch

The WLAN switch on the top side is used to disable the WLAN function. Provided the VPNRouter is equipped with a WLAN module. Otherwise software may just read this switch for other purposes.

Figure 8: WLAN Switch

4.3. Digital I/O

The functions of Digital Input and Output are located on the 13 clamp terminal block on the top side of VPNRouter. Also available on this terminal block is the function of I²C and an auxiliary power output.

1	2	3	4	5	6
+5V	IN 0	IN 1	IN 2	IN 3	GND

(a) Input connects

7	8	9	10
OUT 0	OUT 1	OUT 2	OUT 3

(b) Output connects

11	12	13
GND	SDA	SCL

(c) I²C connects

Table 5: Digital Input/Output: Connector

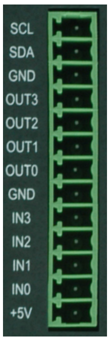


Figure 9: Digital Input / Output Connector

4.3.1. Digital Input

The VPNRouter provides four digital input channels. The signals IN 0 to IN 3 are located on clamps 2 to 5 of the terminal block, the reference GND is on clamp 6. A signal change on an input channel will generate an interrupt.

Input High	TTL level (2.0 to 5.0V)
Input Low	TTL level (0.0 to 0.8V)

Table 6: Digital Input: Electrical Characteristics

4.3.2. Digital Output

The VPNRouter provides four digital output channels. The signals OUT 0 to OUT 3 are located on clamps 7 to 10 of the terminal block, the reference GND is on clamp 6 and 11. The output ports can source some milliAmpere output in High status, with decreasing voltage when the current rises. In Low status they can sink significant current, enough to drive small relays.

Output High	Source 32mA@TTL (2.0 to 5.0V)
Output Low	Sink 64mA@TTL (0.0 to 0.6V)

Table 7: Digital Output: Electrical Characteristics

4.3.3. I²C Interface

The I²C interface operates with a maximum frequency of 400 kHz (Fast Mode). The connector for I²C is located on the terminal digital I/O block and has three contacts: SCL, SDA and GND (clamps 11 to 13). When required the I²C device can be powered with the VCC auxiliary output of the digital I/O terminal block.

4.3.4. Auxiliary Power

+5V is an auxiliary power output of 5V DC, for max. 500 milliAmpere. This may be used to drive special driver circuits connected at Digital-I/O. For example +5V may drive a relay controlled by the output signals, or power a small I²C-controlled display. The GND for auxiliary power is on clamps 6 and 11.

4.4. Antenna Locations

The VPNRouter is prepared for adding two antenna sockets of the usual SMA type. These may be used for functions like WLAN, UMTS/LTE wireless or GPS receivers. The positions are covered by plastic caps. Both antenna positions are on the top side of VPNRouter iR 5221/VPNRouter iR 3220.

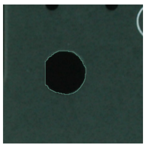


Figure 10: Antenna location

4.5. LED

The front side starts with a group of four LEDs.

PWR (Red) lights when power is applied to the VPNRouter. System software may generate short blinks for certain events.

3G (Yellow) is controlled by a UMTS/LTE modem card in the mini PCIe expansion slot.

WIFI (Blue) signals operation status of WLAN function.

APP (Green) is free to use by customers application, e.g. as some ready light.

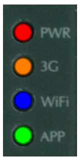


Figure 11: Front LED

4.6. LAN

The first Ethernet port in VPNRouter is for 10/100 Mbps Fast Ethernet. This connects to an internal Ethernet switch, with 2 (VPNRouter iR 3220) or 4 (VPNRouter iR 5221) external connectors. Devices or systems connected to these ports can communicate with each other, without involving the CPU of VPNRouter.
Each of the LAN ports are the usual RJ45. When the connect is done the Link LED on RJ45 (right) will light. When data traffic occurs on the network, this LED will blink. It depends on your network or devices whether a 100 Mbit or a 10 Mbit connect will be established. The Speed LED (left) lights for 100Mbps connections.

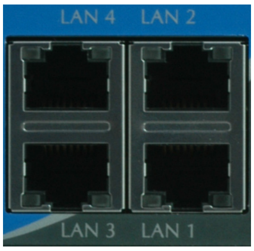


Figure 12: LAN ports

4.7. WAN

The second Ethernet port in VPNRouter is for 10/100/1000 Mbps Gigabit Ethernet. The connector is the usual RJ45, integrated with USB ports.
When the connect is done the Link LED on RJ45 (green, left) will light. When data traffic occurs on the network, this LED will blink. It depends on your network or devices whether a 1000 Mbit, a 100 Mbit or a 10 Mbit connect will be established. The Speed LED (yellow, right) lights for 10 and 100 Mbps connections.
This Ethernet interfaces supports Auto-MDI(X) feature.

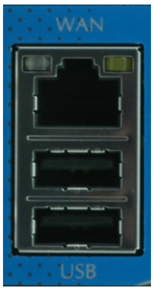


Figure 13: WAN port and USB connectors

4.8. USB

The VPNRouter provides two USB 2.0 Host interfaces. They can be used for Mass Storage Devices, like Flash- or Hard Drive, Bluetooth and WLAN adapters etc.

The ports are integrated with the Gigabit Ethernet WAN port, see figure 13.

4.9. Serial

VPNRouter iR 5221 and VPNRouter iR 3220 provide two DSub-9 male connectors. All three modes of operating RS 232, RS 422 or RS 485 are entirely configurable by software. For the pinout refer to the Table 8. If the configuration by software is not used, the default operation mode of each port is configured by a DIP switch. The DIP switch may be overridden by software, if the user chooses to do so. Check section **??** on page ?? for details.

Pin	RS 232	RS 422	RS 485 2-wire
1	DCD	Tx- (A)	Data- (A)
2	RxD	Tx+ (B)	Data+ (B)
3	TxD	Rx+ (B)	
4	DTR	Rx- (A)	
5	GND	GND	GND
6	DSR		
7	RTS		
8	CTS		
9	RI		

Table 8: Serial DSub-9 Pinout

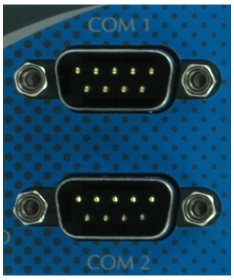


Figure 14: COM Ports

Please note the function of the GND signal in RS 422 and RS 485 modes: this signal must also be connected between the serial devices. So in reality a 2-wire and a 4-wire connection need 3 wire and 5 wire respectively. With the exception of very special configurations, a serial connection in RS 422/RS 485 mode without GND connection violates the specifications for RS 422 and RS 485 standards.

4.9.1. DIP Configuration for Serial Ports

The right side of the case has a small opening slit. This is provided to access the DIP switches for serial configuration. With a small pen or screw driver the configuration can be changed without opening the case.
The current setting of the switches is readable by software. If the user or software decides to do this, the software can override the active configuration, i.e. change the operation mode. Please check section **??** on page ?? for details about this function.

Figure 15: DIP Switches

4.10. SD-Slot

The VPNRouter provides an SD-Slot on the front side of the case, for cards in standard size. The slot supports cards as SD 2.0 or SDHC type, to allow up to 32 GB of capacity. Class 10 cards are supported as well.
If an operating system is installed on the SD Card, the VPNRouter will boot this software.

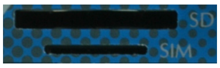


Figure 16: SD and SIM Slot

4.11. SIM-Slot

A SIM-Slot is located right next to the SD-Slot, see figure 16 on the preceding page. A Mini SIM card in this slot is accessed by a UMTS/LTE modem card in the mini PCIe expansion slot.

4.12. Reset

The Reset button is the front most component on the bottom side of VPNRouter.

With Reset button you can restart the VPNRouter without removing the power. The Reset button should be used only in situations, where reboot command is not available, to avoid file system integrity errors.

Figure 17: Reset Button

4.13. Console Port

The console port (RS 232) has an RJ45 connector on the bottom side. An adapter cable to DSub-9 female is available as part of the Starter Kit (??).

Pin	Signal
3	GND
4	TxD
5	RxD

(a) Console RJ45

Pin	Signal
2	TxD
3	RxD
5	GND

(b) Console DSub-9 female

Table 9: Serial Console Port

Figure 18: Console Port

4.14. USB/OTG

Only available on VPNRouter iR 5221: A connector of micro-AB type provides one extra USB channel. This port can operate in Host or Device Mode, the hardware detects if the connected device is a Host (PC) or some device (printer, external HDD etc.). Hence the designation as USB/OTG.

Figure 19: OTG

4.15. CAN Bus

CAN bus is only available on VPNRouter iR 5221. The connector for CAN bus is a terminal block with three clamps. Available signals are CAN High, CAN Low and CAN GND. Termination of CAN bus (120 Ω) shall be implemented on the cable.

Clamp	G	N	P
Function	CAN_GND	CAN_L	CAN_H

Table 10: CAN bus Connector

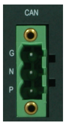


Figure 20: CAN Bus

5. Position of Connectors and Functions of VPNRouter iR 2110

5.1. Power

The VPNRouter device is powered by a single power supply in a wide range from 9 V to 54 V DC. The socket for a terminal block clamp is on the rear side. A suitable power supply adapter is available as an add-on component, and part of the Starter Kit package. Connect the cable to the power jack, and plug the adapter into the socket. The Power LED (red) on VPNRouter will light. You can connect a power supply of your choice, providing the technical requirements are met.

Warning: disconnect the VPNRouter from power supply before performing installation or wiring. The wire size must follow the maximum current specifications. The maximum possible current in the power wires as well as in the common wires must be taken under consideration. If the current rises above the maximum ratings, the wiring can overheat, causing serious damage to your equipment. When powered, the VPNRouter internal components generate heat, and consequently the outer case may feel warm to the touch.

5.1.1. Connection and Polarity

Power is connected via three clamps on a terminal block, located on the rear side of VPNRouter.

Clamp	3	2	1
Function	PE	V-	V+

Table 11: Power Connector

V+ and V- are clamps for DC voltage supply. PE is the clamp to connect the case and shields of connection cables to Protective Earth. PE is internally connected to logic ground, which is on the level of V- supply line.

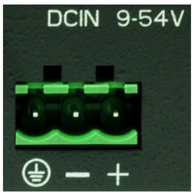


Figure 21: Power Connector

Attention: Never connect the Terminal block for power supply in reversed direction, i.e. turned by 180°. This would connect the power between V- (logic ground) and case/protective ground. High current is the result, causing damage inside the system.

5.1.2. Grounding

Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the ground screw to the grounding surface prior to connecting devices.

In noisy environments the case of VPNRouter shall be directly connected to Protective Earth. This is the purpose of the dedicated PE Screw on the case rear side.

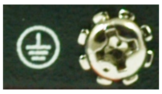


Figure 22: PE Screw

5.2. DIP Switches

The rear side of the case holds a group of four DIP switches. There is no special purpose coupled to the switches. Customers softwar can read the configuration, and evaluate for own intentions.

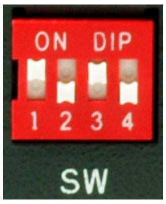


Figure 23: DIP Switches

5.3. Antenna Locations

The VPNRouter is prepared for adding one antenna socket of the usual SMA type. Possible locations are on the rear and on the left side (top wide when mounted on a DIN Rail). Both are covered by plastic caps.

Figure 24: Antenna location

5.4. Reset

The Reset button is on the rear side of VPNRouter. Push it by using a small prick.

With Reset button you can restart the VPNRouter without removing the power. The Reset button should be used only in situations, where reboot command is not available, to avoid file system integrity errors.

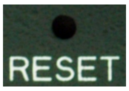


Figure 25: Reset Button

5.5. WAN

The WAN Ethernet port in VPNRouter is for 10/100/1000 Mbps Gigabit Ethernet. When the connect is done the Link LED on RJ45 (green, left) will light. When data traffic occurs on the network, this LED will blink. It depends on your network or devices whether a 1000 Mbit, a 100 Mbit or a 10 Mbit connect will be established. The Speed LED (yellow, right) lights for 10 and 100 Mbps connections.
This Ethernet interface supports Auto-MDI(X) feature.

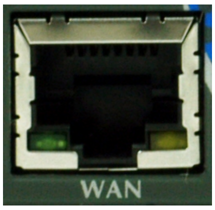


Figure 26: WAN Port

5.6. USB

The OnRISC VPNRouter iR 2110 provides a USB 2.0 Host interface. This can be used for Mass Storage Devices, like Flash- or Hard Drive, Bluetooth and WLAN adapters etc.

Figure 27: USB Connector

5.7. LED

The front side holds a group of three LEDs.

PWR (Red) lights when power is applied to the VPNRouter. System software may generate short blinks for certain events.

WIFI (Blue) signals operation status of WLAN function.

APP (Green) is free to use by customers application, e.g. as some ready light.

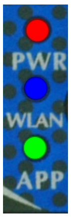


Figure 28: Front LED

5.8. Serial

The VPNRouter provides one DSub-9 male connector. All three modes of operating RS 232, RS 422 or RS 485 are entirely configured by software. For the pinout refer to the Table 12 on the next page.

Pin	RS 232	RS 422	RS 485 2-wire
1	DCD	Tx- (A)	Data- (A)
2	RxD	Tx+ (B)	Data+ (B)
3	TxD	Rx+ (B)	
4	DTR	Rx- (A)	
5	GND	GND	GND
6	DSR		
7	RTS		
8	CTS		
9	RI		

Table 12: Serial DSub-9 Pinout

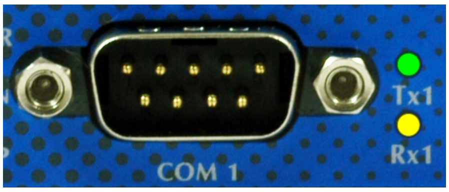


Figure 29: COM Port

Please note the function of the GND signal in RS422 and RS485 modes: this signal must also be connected between the serial devices. So in reality a 2-wire and a 4-wire connection need 3 wire and 5 wire respectively. With the exception of very special configurations, a serial connection in RS422/RS485 mode without GND connection violates the specifications for RS422 and RS485 standards.

In RS232 and RS422 Mode data may be received while transmitting. This also applies to RS485 Full Duplex Mode, which is also referred to as 4-wire connection (same signal assignment as the RS 422).

The RS485 Standard Mode is alternatively referred to as Half Duplex Mode, 2-wire connection or Bus Mode. It uses the same two wires for transmit and receive. So it would be possible to simultaneously receive the same data the port just transmitted, this is often named an Echo. The serial port in VPNRouter intentionally suppresses this Echo. In the rare situations where this Echo is required, the port should be set as this:

- Configure the port for RS485 Full Duplex Mode
- Connect Tx+ with Rx+ in the cable
- Connect Tx- with Rx- in the cable

5.9. LAN

The LAN Ethernet port in VPNRouter is for 10/100 Mbps Fast Ethernet. When the connect is done the Link LED on RJ45 (right) will light. When data traffic occurs on the network, this LED will blink. It depends on your network or devices whether a 100 Mbit or a 10 Mbit connect will be established. The Speed LED (left) lights for 100Mbps connections.

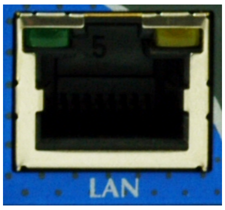


Figure 30: LAN Port

5.10. SD-Slot

The VPNRouter provides an SD-Slot on the front side of the case, for cards in microSD size. The slot supports cards as SD 2.0 or SDHC type, to allow up to 32 GB of capacity. Class 10 cards are supported as well.
If an operating system is installed on the SD Card, the VPNRouter will boot this software.

Figure 31: SD Slot

6. Logon to the Device

The Device is configured via an internal web interface. In part this is similar to many SOHO-Routers on the market. Consequently you need a network connection to the Device, where you then open your browser to access the web interface. Basically there is one way to get the required access. In the description here it is assumed the Device is in factory configuration.

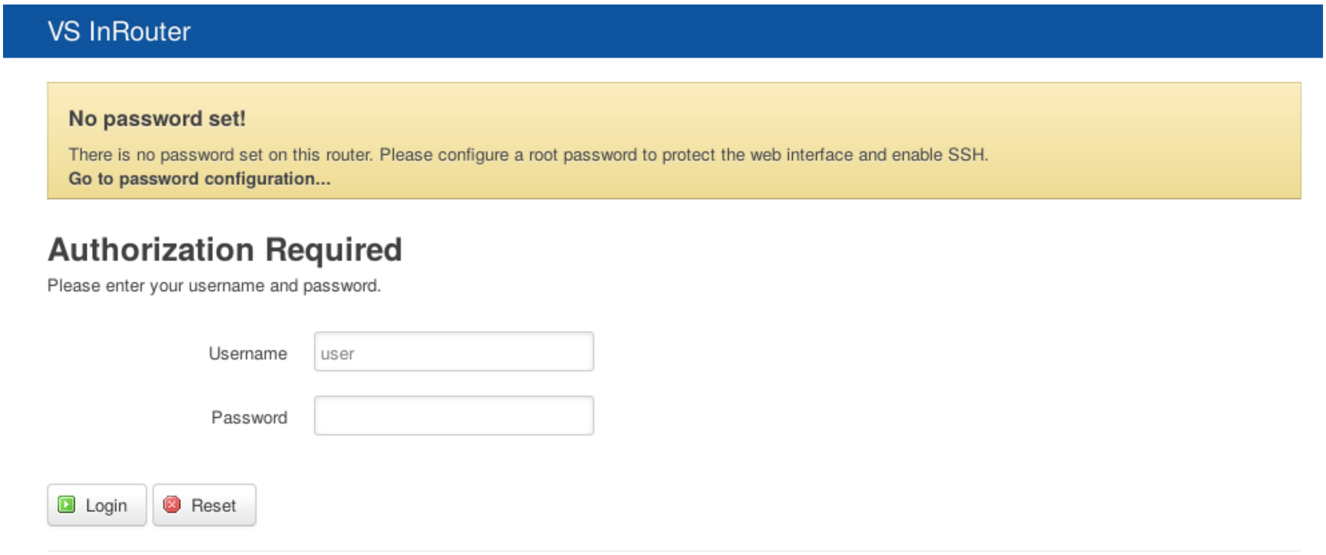
6.1. Connect to the Device

6.1.1. Ethernet Cable to LAN Port

That is the option for on-site access, i.e. you are in front of the Device. Plug the Ethernet cable from your PC into a LAN port (not the WAN port). Your PC uses DHCP to get an IP Address from the Device. Then open your browser and type the IP Address 192.168.178.1 into the address bar.

6.2. Logon to Device Web Interface

By default there is no password set. The Username is fixed as “user”.



VS InRouter

No password set!

There is no password set on this router. Please configure a root password to protect the web interface and enable SSH.
Go to password configuration...

Authorization Required

Please enter your username and password.

Username: user

Password:

Figure 32: Logon Mask

Click on “Login” to get access to the configuration. On top of the screen is a classic Pull-Down Menu, but you may also click on the buttons itself. For function of *Logout* this is mandatory.

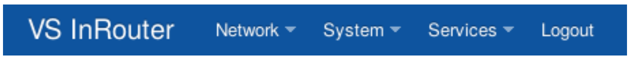


Figure 33: Pull Down Menu

Note the down-arrow on the buttons *Network*, *System*, *Services* and *Logout*. When the mouse hovers over one of these buttons, the list of menu items opens. Use the mouse to click on one of the items. There are two views (“Administation” and “Essentials”) of the web interface, we only describe the “Essentials” view. Use the Administration view if you are experienced and need special features.

Applying changes

Configuration applied.

(a) Save and Reset buttons

(b) Apply Changes

Figure 34: Save Configuration Changes

The pages use two buttons on the bottom right to apply the parameters, or discard the changes. Button `[Save]` will save the new parameters, and apply them automatically. For a short time a display like figure 34b will appear. The Button `[Reset]` will discard any modifications in the configuration forms, back to the last operation of saving or entry to the page.

7. Network

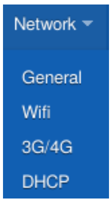
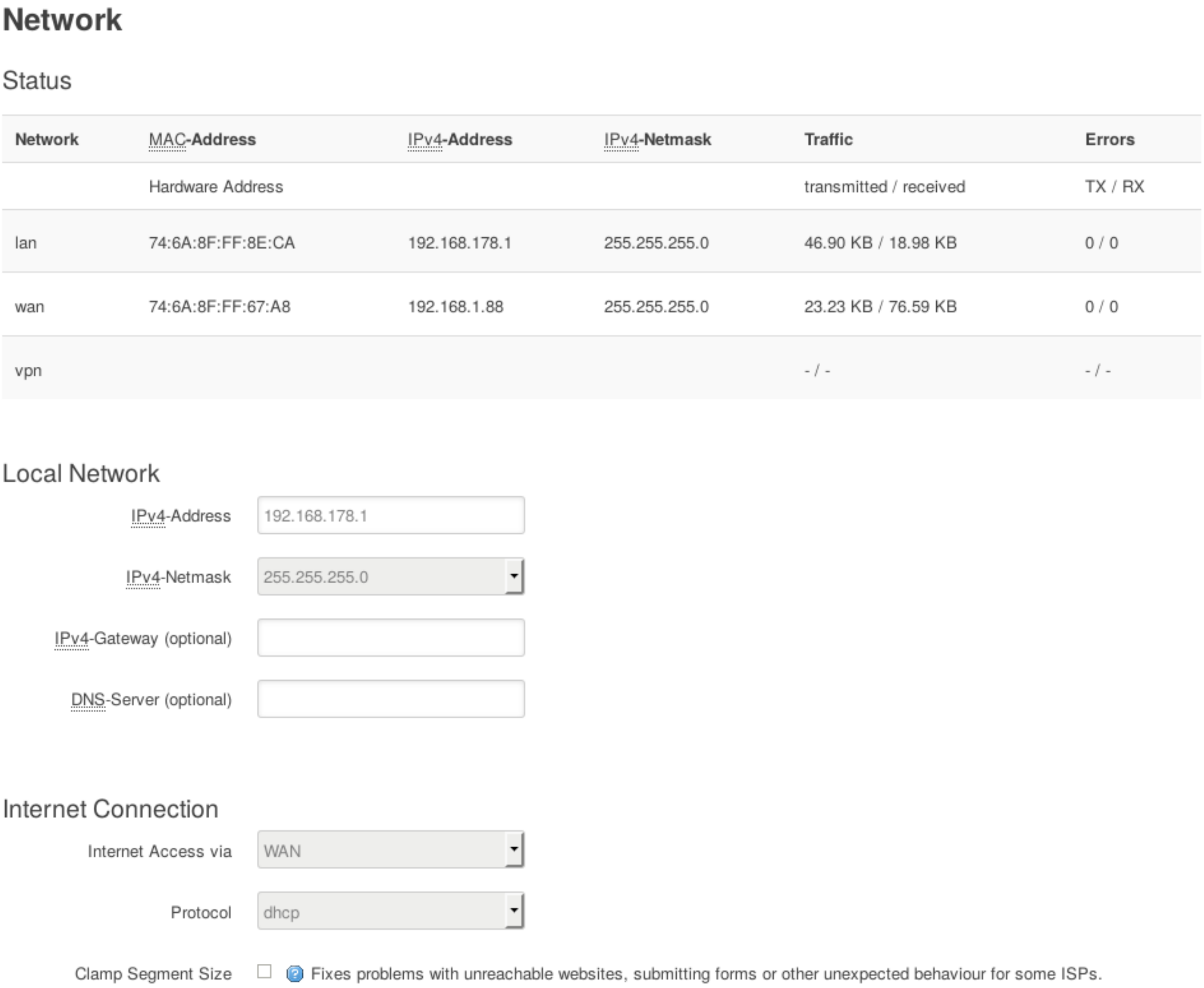


Figure 35: Menu Network

The Menu *Network* lists the items of *General*, *Wifi*, *3G/4G* and *DHCP*. *Wifi* is for WLAN function and *3G/4G* configures an interface for 3G/UMTS or 4G/LTE communication via mobile communication networks. These two items only appear if the required interface hardware is available, otherwise they are hidden. A click on the top button `[Network]` opens the item *General*.

7.1. General

There are many sections on the web page, explained block by block.



Network

Status

Network	MAC-Address	IPv4-Address	IPv4-Netmask	Traffic	Errors
	Hardware Address			transmitted / received	TX / RX
lan	74:6A:8F:FF:8E:CA	192.168.178.1	255.255.255.0	46.90 KB / 18.98 KB	0 / 0
wan	74:6A:8F:FF:67:A8	192.168.1.88	255.255.255.0	23.23 KB / 76.59 KB	0 / 0
vpn				- / -	- / -

Local Network

IPv4-Address	192.168.178.1
IPv4-Netmask	255.255.255.0
IPv4-Gateway (optional)	
DNS-Server (optional)	

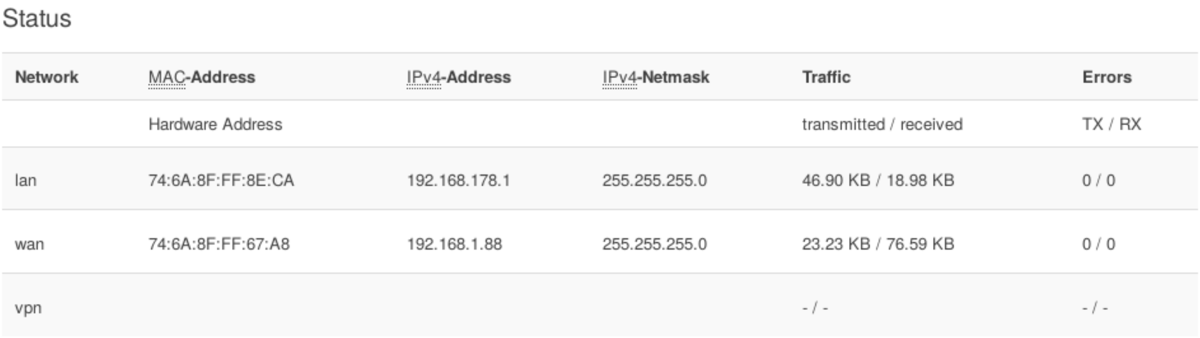
Internet Connection

Internet Access via	WAN
Protocol	dhcp
Clamp Segment Size	□ Fixes problems with unreachable websites, submitting forms or other unexpected behaviour for some ISPs.

Figure 36: Network General Overview

Save configuration changes using the buttons on the bottom line, see figure 34a on page 27.

7.1.1. Status



Status

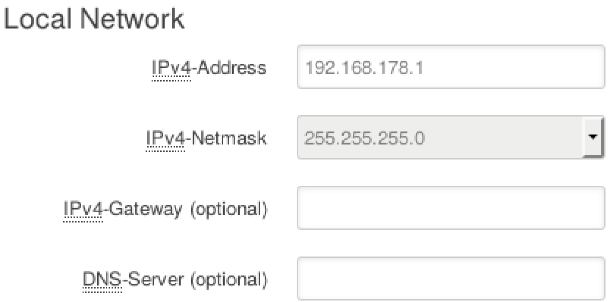
Network	MAC-Address	IPv4-Address	IPv4-Netmask	Traffic	Errors
	Hardware Address			transmitted / received	TX / RX
lan	74:6A:8F:FF:8E:CA	192.168.178.1	255.255.255.0	46.90 KB / 18.98 KB	0 / 0
wan	74:6A:8F:FF:67:A8	192.168.1.88	255.255.255.0	23.23 KB / 76.59 KB	0 / 0
vpn				- / -	- / -

Figure 37: Status of Network Interfaces

All available network interfaces are listet here, with status information. *Wifi* and *3G/4G* only appear if the required interface hardware is available. Each interface is listed with the common values of *MAC Address*, *IP Address* and *Netmask*. Further the data *Traffic* on the interface is listed, separated for *transmitted* and *received*. Appended are *Errors*, all these values counted from the last reboot or power-on of the Device.

7.1.2. Local Network

The *Local Network* references the Ethernet ports labelled **LAN** on the front side.



Local Network

IPv4-Address: 192.168.178.1

IPv4-Netmask: 255.255.255.0

IPv4-Gateway (optional):

DNS-Server (optional):

Figure 38: Local Network Configuration

This adress should be from the IPv4 address ranges assigned to private networks. The following IP blocks are reserved for private IP addresses.

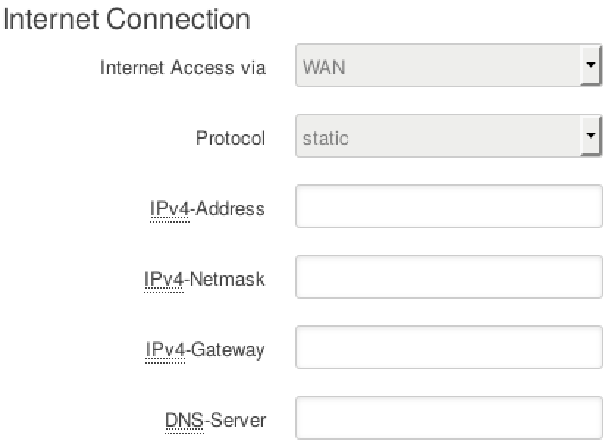
Class	Starting IP Address	Ending IP Address	# of Hosts
Class A	10.0.0.0	10.255.255.255	16,777,216
Class B	172.16.0.0	172.31.255.255	1,048,576
Class C	192.168.0.0	192.168.255.255	65,536

Table 13: Private IPv4 addresses

7.1.3. Internet Connection

Usually the Ethernet Port labelled **WAN** is used for Internet access. This is configured by selecting *WAN port* in the drop-down list of *Internet Access via* (see figure 39). The other options are *Wifi* and *3G/4G*, provided the referenced hardware is available.

7.1.3.1. by WAN Connection By default the *IP-Address Assignment* on WAN interface is done *by DHCP (automatic)*. With this configuration on startup the Device will send a special request to get a valid configuration.



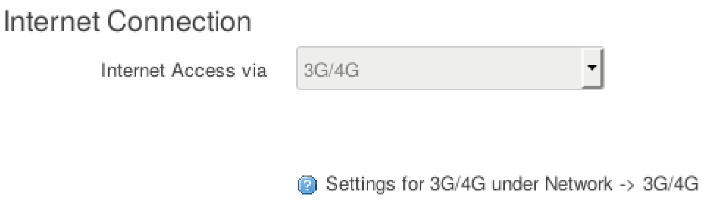
Internet Connection

Internet Access via	WAN
Protocol	static
IPv4-Address	
IPv4-Netmask	
IPv4-Gateway	
DNS-Server	

Figure 39: WAN connection

If that automatic is disabled by selecting *static* in the drop-down, the next four input fields appear. A static IP Address configuration is necessary, and the network administrator has to provide this information to you. Enter correct values in the fields of *IP-Address*, *Netmask*, *ISP* or *Gateway* and *DNS-Server*.

7.1.3.2. by 3G/4G Connection When the Internet access is configured for 3G/4G communication (figure 39), the configuration of the IP Address is done entirely by the provider.



Internet Connection

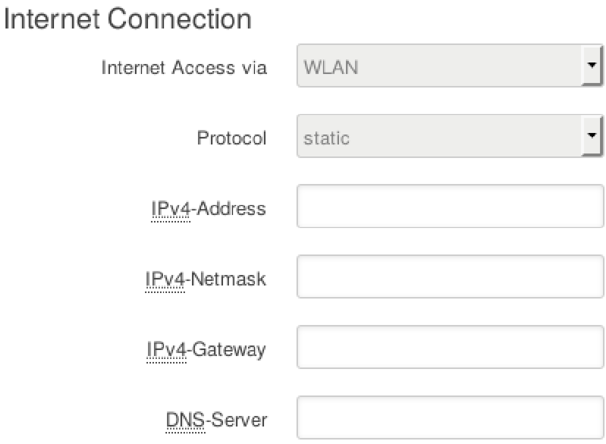
Internet Access via: 3G/4G

Settings for 3G/4G under Network -> 3G/4G

Figure 40: 3G/4G Configuration

So there is nothing to configure specifically, the access parameters are defined in section 7.3 on page 37.

7.1.3.3. by Wifi Connection The access to Internet may be done by the WLAN function. Then this is configured for the Operation Mode as Client (see section 7.2.3 on page 35).



Internet Connection

Internet Access via: WLAN

Protocol: static

IPv4-Address:

IPv4-Netmask:

IPv4-Gateway:

DNS-Server:

Figure 41: Wifi Configuration

By default the configuration of the WLAN Client connection is automatic like for the WAN port (see 7.1.3.1 on the previous page). Then the other parameters are hidden from view. If the field *Protocol* has a the value *static*, a static IP Address configuration is necessary. Again the network administrator has to provide this information to you. Enter correct values in the fields of *IP-Address*, *Netmask*, *Gateway* and *DNS-Server*.

7.2. Wifi

The Wifi adapter in the Device may be deactivated (switched-off) by the **WLAN** switch on the case. This has precedence to any internal configurations. If the external switch is **On**, for operation it needs a check mark in the box *Enable*; otherwise it is still inactive.

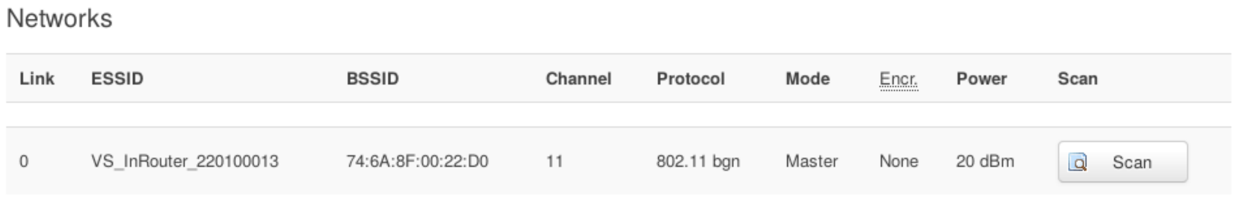
An active adapter has two operation modes, as Client or as Access Point (AP). The second is the default configuration, and it allows access to the LAN side of the Device. Configured as Client the adapter connects to on-site network for Internet access. In Client Mode there is no access to the web interface via WLAN.

The parameters are explained in the following sections, to save configuration changes using the buttons on the bottom line (figure 34a on page 27). A suggested sequence of configuration steps is at the end of this section (7.2.4).

Configuration Transfer: If the Wifi Adapter in target and source is configured for operation as Access Point, there is no risk in transfering the configuration. However if either is configured in Client Mode, often it is used for Internet Access then. A transfer of parameters will likely disrupt the Internet connection.

Even if both source and target shall share the same SSID and similar parameters, they must use different IP Addresses. The only save configuration then is DHCP for WLAN.

7.2.1. Networks



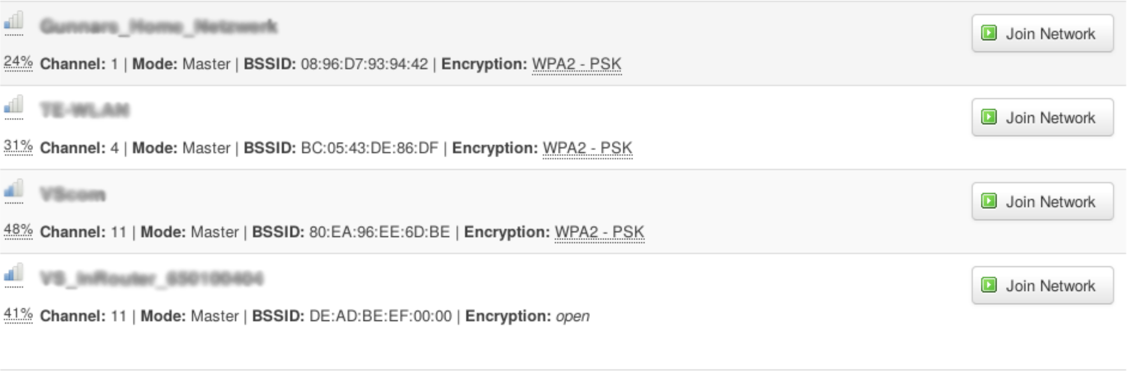
Networks

Link	ESSID	BSSID	Channel	Protocol	Mode	Encr.	Power	Scan
0	VS_InRouter_220100013	74:6A:8F:00:22:D0	11	802.11 bgn	Master	None	20 dBm	Scan

Figure 42: Wifi Networks

In Client operation mode the Wifi Adapter shall connect to an existing WLAN network. The network and the connection parameters are shown when this is successful. The button `[Scan]` searches for WLAN networks in the vicinity.

7.2.1.1. WLAN scanned Scanning for WLAN networks may help in select the parameters for a connection to the target network.



[redacted]
24% **Channel:** 1 | **Mode:** Master | **BSSID:** 08:96:D7:93:94:42 | **Encryption:** WPA2 - PSK

[redacted]
31% **Channel:** 4 | **Mode:** Master | **BSSID:** BC:05:43:DE:86:DF | **Encryption:** WPA2 - PSK

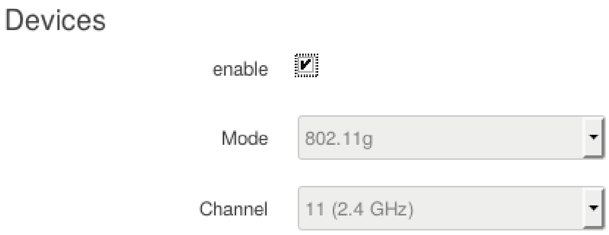
[redacted]
48% **Channel:** 11 | **Mode:** Master | **BSSID:** 80:EA:96:EE:6D:BE | **Encryption:** WPA2 - PSK

[redacted]
41% **Channel:** 11 | **Mode:** Master | **BSSID:** DE:AD:BE:EF:00:00 | **Encryption:** *open*

Figure 43: Wifi Scan Results

7.2.2. Adapter

When the Wifi *Adapter* is *Enable*d, some parameters need selection.



Devices

enable ☑

Mode: 802.11g

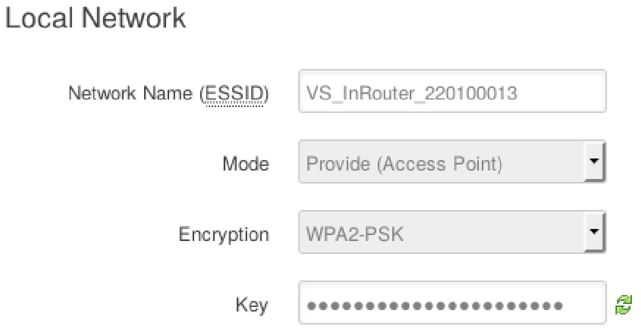
Channel: 11 (2.4 GHz)

Figure 44: Wifi Radio Parameters

The *Mode* has five values to select from: *auto*, *802.11b*, *802.11g*, *802.11a* and *802.11b+g*. In Client Mode choose the value which best matches the configuration provided by the network administrator.

In Client mode you do not need to select the *Channel*, the Adapter follows the configuration of the Access Point it connects to (figure 43). In AP mode you have to select the channel to operate on, please check with the network administrator which parameter to use. The selectable values range from *1 (2.4GHz)* to *14 (2.4GHz)* plus *auto*. Please also check with local regulations if there are forbidden channels, for example in Europe you often are not allowed to use channel 14. The configuration of *auto* lets the Adapter search for the best free range.

7.2.3. Local Network



Local Network

Network Name (ESSID): VS_InRouter_220100013

Mode: Provide (Access Point)

Encryption: WPA2-PSK

Key: ••••••••••••••••••••••

Figure 45: Wifi Network

These are the final parameters for WLAN configuration. *Network Name (ESSID)* defnes which WLAN network to connect to. The *Operation* mode is either *Join (Client)* or *Provide (Access Point)*. The *Encryption* mode supports:

- *No Encryption*: Only use that in Client Mode, when the WLAN net does not support security.
- *WEP*: This is an old and weak way of security. Only use that in Client Mode, when the WLAN net does not support better security.
- *WPA-PSK*, *WPA2-PSK* and *WPA-PSK, WPA2-PSK Mixed Mode*: This is state of the art encryption. Use this in Access Point Mode, and select a secure Pre-Shared-Key (PSK). WPA2 is the best choice, but WPA is still secure.
- *WPA-Radius* and *WPA2-Radius*: These are usable in Client Mode only, since in AP Mode the Device does not have access to a Radius Server for Authentication.

In the field *Key* enter the so-called Passphrase for the Wireless LAN. In combination with the *ESSID* this defines the PSK for encryption.

7.2.4. Configuration Procedures

These are suggested sequences to configure the WLAN function

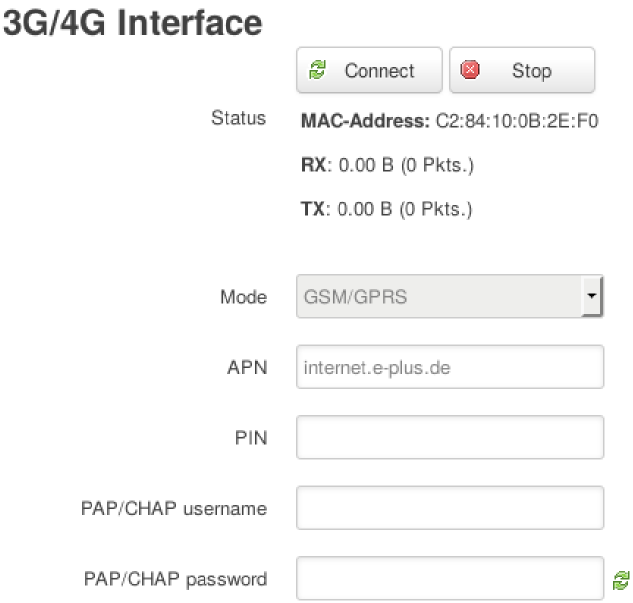
7.2.4.1. as Access Point

1. Under *Adapter* check *Enable*.
2. Under *Adapter* select the *Mode*.
3. Under *Adapter* select a *Channel* for communication.
4. Under *Local Network* provide a unique name (*ESSID*) for your WLAN communication. The default value of `VS_InRouter_<SNo.>` is fine for start, other values are OK.
5. Under *Local Network* select *Operation* as *Provide (Access Point)*.
6. Under *Local Network* select *Encryption* as *WPA2-PSK*.
7. Under *Local Network* define a secure *Key* for encryption. About 16 random letters or digits are a good start.
8. Click on the `[Save]` button and wait for the changes to be applied.

7.2.4.2. as Client

1. Under *Adapter* check *Enable*.
2. Under *Local Network* select *Operation* as *Join (Client)*.
3. Click on the `[Save]` button and wait for the changes to be applied.
4. Under *Networks* click the button for `[Scan]`, and wait for the results. Check if the target WLAN network is visible.
5. Under *Adapter* select the *Mode* according to the result of the Scan.
6. Under *Local Network* enter the *ESSID* for the target WLAN network.
7. Under *Local Network* select the appropriate mode for *Encryption*. In case of doubt ask the network administrator.
8. Under *Local Network* enter the *Key* for encryption. You get that from the network administrator as well.
9. Again click on the button `[Save]` and wait for the changes to be applied.

7.3. 3G/4G



3G/4G Interface

Status MAC-Address: C2:84:10:0B:2E:F0

RX: 0.00 B (0 Pkts.)

TX: 0.00 B (0 Pkts.)

Mode GSM/GPRS

APN internet.e-plus.de

PIN

PAP/CHAP username

PAP/CHAP password

Figure 46: 3G/4G Interface

A *3G/4G Interface* is available when the Device is equipped with a supported 3G/4G communication card. For proper operation it needs to have a card inserted in the **SIM** slot on the case. Such an interface may be used as an alternative for Ethernet (on the **WAN** port), for example when the location does not have wired Internet access. The parameters to use the interface are provided by the mobile communication provider, together with the SIM Card.

In the field *Mode* may select from a set of options like *All*, *LTE UMTS*, *GSM/UMTS* or *CDMA*. The actual values available depend on the model of communication card, and what is provided by use of the given SIM Card.

Enter *APN* for Internet access and *PIN* to authenticate for the SIM Card. The *PAP/CHAP username* and *PAP/CHAP password* are rarely used.

On the bottom line are the usual buttons, click on [Save] to save your new configuration. To use the *3G/4G Interface* click on the button *Connect*.

7.4. DHCP

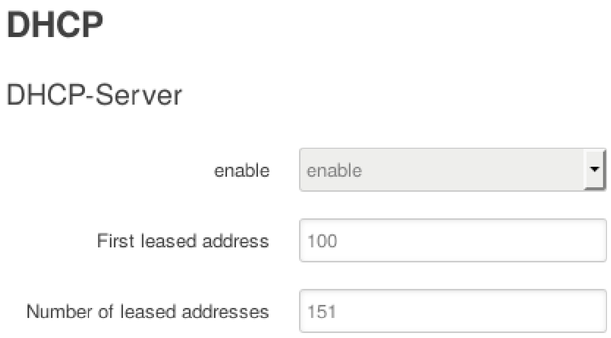
DHCP is the "Dynamic Host Configuration Protocol", the Device has a server component for this built-in. The protocol is designed to provide correct configuration of IP Address and related parameters to clients. Clients in this context are any computers/machines/adapters connected to the **LAN** ports of the Device. The purpose of using DHCP is to have non-conflicting configurations without manually placing parameters into each client.

When the client is started it sends a special request on the network, and it receives an offer from the server. The server has a range of IP Addresses to choose from. It will attempt to offer the same IP Address to the client as it did before. If that is not possible for some reason it will offer a different IP Address. An IP Address assigned to a client is named as a Lease in context of DHCP.

The server has a list of known clients, it will identify them by their MAC Address. If the client is on this list, it gets the pre-defined IP Address reserved for this client as an offer. No other client will ever get this IP Address. For clients not on this list on their first contact to the server they receive an offer with an IP Address from the range, which does not conflict with the IP Addresses of known clients.

There are some issues to consider with DHCP, see 7.4.4 on page 41.

7.4.1. DHCP-Server



DHCP

DHCP-Server

enable: enable

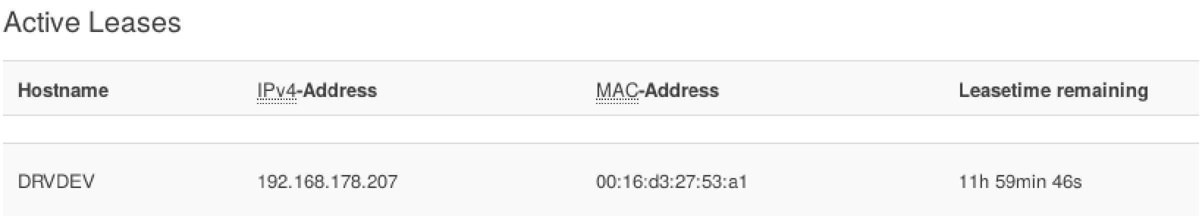
First leased address: 100

Number of leased addresses: 151

Figure 47: DHCP Address Range

The *Start address* and *End address* define the available address range for the *DHCP-Server*, both addresses are included in the range. The values like `100` represent the fourth/last number of an IP Address, the preceeding three numbers are identical to the Device's IP Address (see section 7.1.2 on page 30).

7.4.2. Active Leases



Active Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
DRVDEV	192.168.178.207	00:16:d3:27:53:a1	11h 59min 46s

Attention!

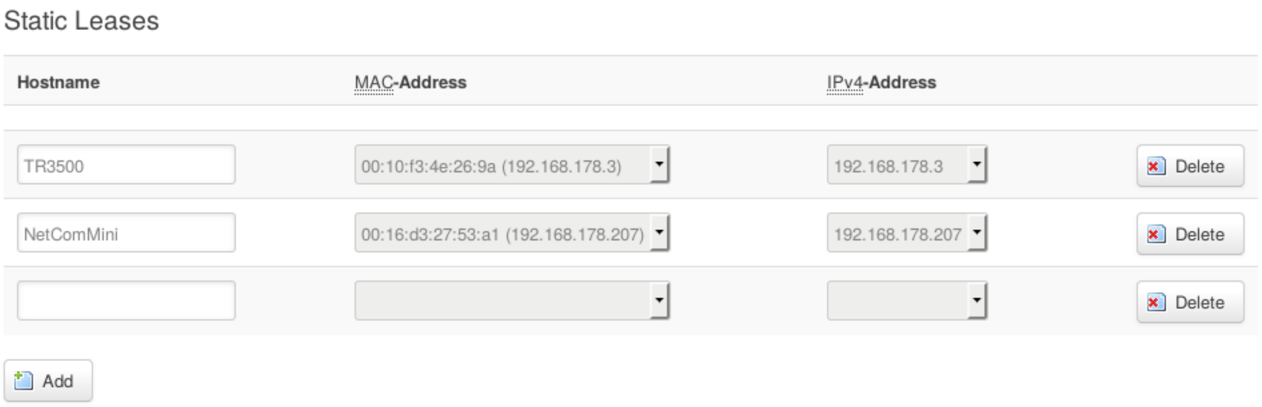
Figure 48: Active Leases

When a client received an IP Address from the DHCP server, it has a "Lease" on this address. This is active for a given time, and the client may request to renew this lease. Clients with a lease are listed for informational purposes.

To have a *Hostname* appear in the list the client transmits its name, or the client is from the list of known clients. Otherwise that field is just empty. Also listed are *IP Address* and *MAC-Address*, followed by the *Leasetime remaining*.

7.4.2.1. Automatic Detection of local Devices happens under a few restrictions. If a device uses static IP Address configuration, it will not send a request to the DHCP server. So at first the server has no knowledge about that device. But the server monitors certain local network traffic, and will detect static devices when they become active on the network. These are added to the list of *Active Leases* for information. Since This page displays many information for reference.there can't be a name there is a question mark, and the Lease information is *not DHCP*.

7.4.3. Static Leases



Static Leases

Hostname	MAC-Address	IPv4-Address	
TR3500	00:10:f3:4e:26:9a (192.168.178.3)	192.168.178.3	Delete
NetComMini	00:16:d3:27:53:a1 (192.168.178.207)	192.168.178.207	Delete
			Delete

Figure 49: Static Leases

The *Static Leases* are the methode to configure the list of known clients. The button `[Add]` creates a new entry in the list, with empty values.

1. You should enter the *Hostname* like `MyMachine`. The name follows the rules for computer names: It shall start with a letter, and consist of letters and digits only; special characters and spaces are not allowed.
2. Provide the *MAC-Address*. Either there is already an entry in the drop down list, this happens when the client previously was active on the local network. Or select *– custom –* from the list, and manually type the value (e.g. `03:10:17:76:0D:0A`).
3. Select the *IP Address*. If the client was active on the local network, you may just select the entry from the drop-down list. Or again select *– custom –* and type the complete IP Address.

You may later change the entry by modifying the values in the same way. The button for `[Delete]` removes an entry from the list.

7.4.4. Issues

- Startup times: When Device and clients are switched on at the same time, the client may issue the DHCP request before the DHCP-server in the Device is operating. Then the request will fail. The client may repeat the request until it gets a sufficient offer.
  Otherwise the client has to use static IP Address configuration. Either the IP Address is not in the Start-to-End range of the server, or better there shall be an entry in the Static Leases to reserve this address.
- Wifi: When the Wifi adapter is operating in AP mode, connected clients receive their IP Address configuration from the Device's DHCP-server. In general this is a positive effect.

8. System

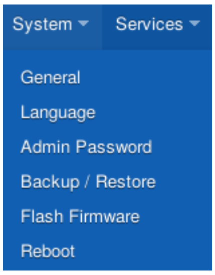
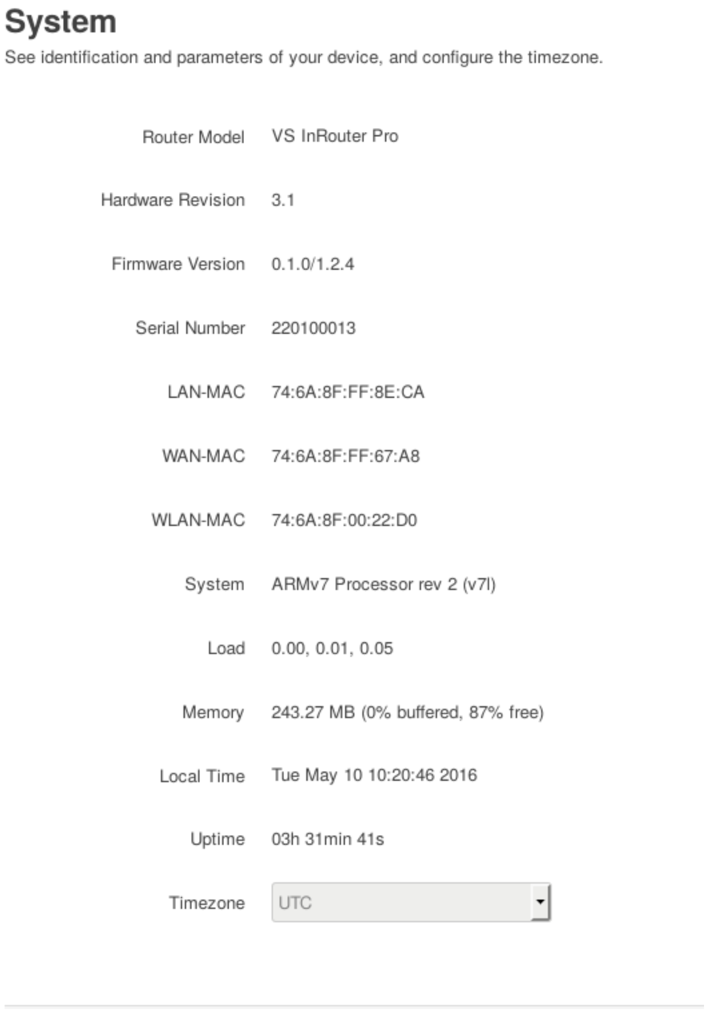


Figure 50: Menu System

The Menu *System* lists the items of *General*, *Language*, *Admin Password*, *Backup/Restore*, *Flash Firmware* and *Reboot*. A click on the top button `[System]` opens the item *General*.

8.1. General

A lot of information is displayed here, but only the *Timezone* is available for configuration.



System

See identification and parameters of your device, and configure the timezone.

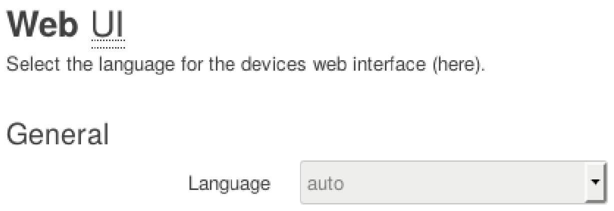
Router Model	VS InRouter Pro
Hardware Revision	3.1
Firmware Version	0.1.0/1.2.4
Serial Number	220100013
LAN-MAC	74:6A:8F:FF:8E:CA
WAN-MAC	74:6A:8F:FF:67:A8
WLAN-MAC	74:6A:8F:00:22:D0
System	ARMv7 Processor rev 2 (v7l)
Load	0.00, 0.01, 0.05
Memory	243.27 MB (0% buffered, 87% free)
Local Time	Tue May 10 10:20:46 2016
Uptime	03h 31min 41s
Timezone	UTC

Figure 51: System General Information

This page displays information for reference. There is the VPNRouter *Router Model* with its *Hardware Revision*, these are fixed. The firmware in the Device consists of two components, so the *Firmware Version* actually displays two values. With firmware upgrades these values will change of course.

The *Serial Number* is printed on the case of the Device. Some statistical parameters like *Uptime*, System *Load* and usable *Memory* are shown.

8.2. Language



Web UI

Select the language for the devices web interface (here).

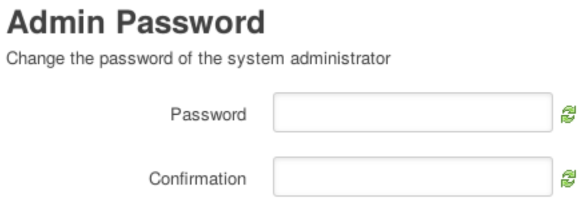
General

Language: auto

Figure 52: Select Language

The *Web UI* (User Interface) supports different languages. In the drop-down you may select *auto*, *Deutsch* and *English*. With *auto* the *Web UI* tries to follow your system configuration, i.e. the language your browser uses. In certain configurations this may fail. The other entries do not need explanation. Save the configuration using the button [Save] as usual.

8.3. Admin Password



Admin Password

Change the password of the system administrator

Password:

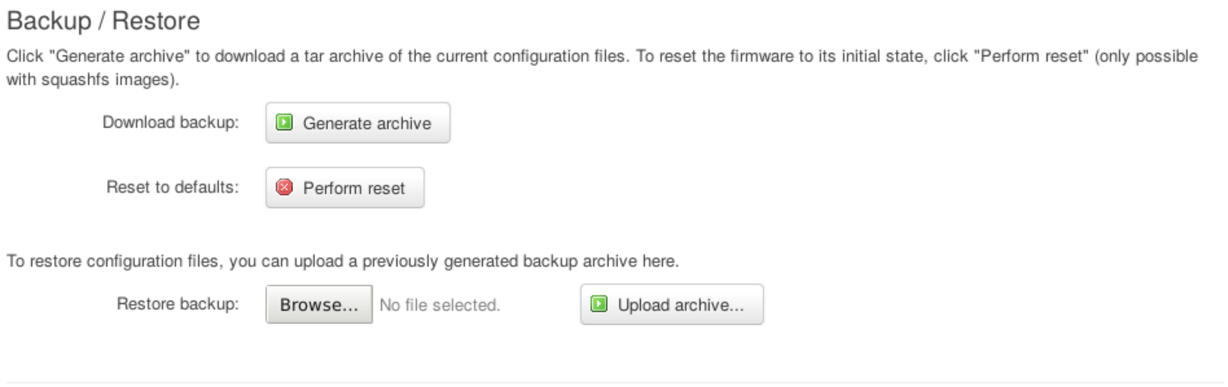
Confirmation:

Figure 53: Set Admin Password

By default there is no password set. On this page you can set a password. Click on the button [Submit] and wait for the changes to be applied. A password protects the *Web UI* (User Interface) against unauthorized access.

8.4. Backup/Restore

The purpose of this functions are given on the web interface. There are some functions on the web page, explained block by block.



Backup / Restore

Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Download backup: Generate archive

Reset to defaults: Perform reset

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup: Browse... No file selected. Upload archive...

Figure 54: Backup/Restore

8.4.1. Download backup

Click *Generate archive* to download a tar archive of the current configuration files.

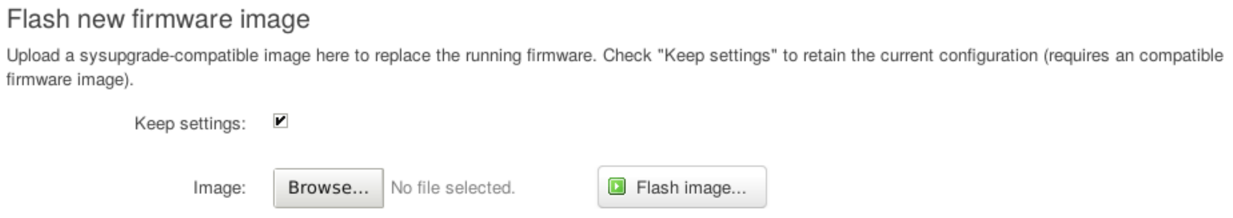
8.4.2. Reset to defaults

Reset this device to factory settings. *Attention*: This is not a start configuration your company may have provided. Also it is possible this operation disconnects the device from the Internet. So it is recommended to only perform this in person at the device. To discard the configuration in the Device click on the *Perform reset* link.

8.4.3. Restore backup

To restore configuration files, you can upload a previously generated backup archive.

8.5. Flash Firmware



Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an compatible firmware image).

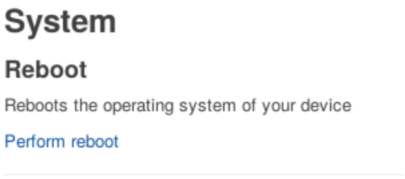
Keep settings: ☑

Image: Browse... No file selected. Flash image...

Figure 55: Flash Firmware

To flash the firmware upload the new firmware image. The current firmware image of the VPNRouter can be downloaded from .... Attention: By default the checkmark is set. Please make sure that the checkmark in the box is set to keep the current configuration. Otherwise the settings will be reset to the default configuration when the flash process is done.

8.6. Reboot



System

Reboot

Reboots the operating system of your device

Figure 56: Reboot the Device

In normal circumstances it is not necessary to reboot the Device. If you feel you need to do this, click on the *Perform reboot* link.

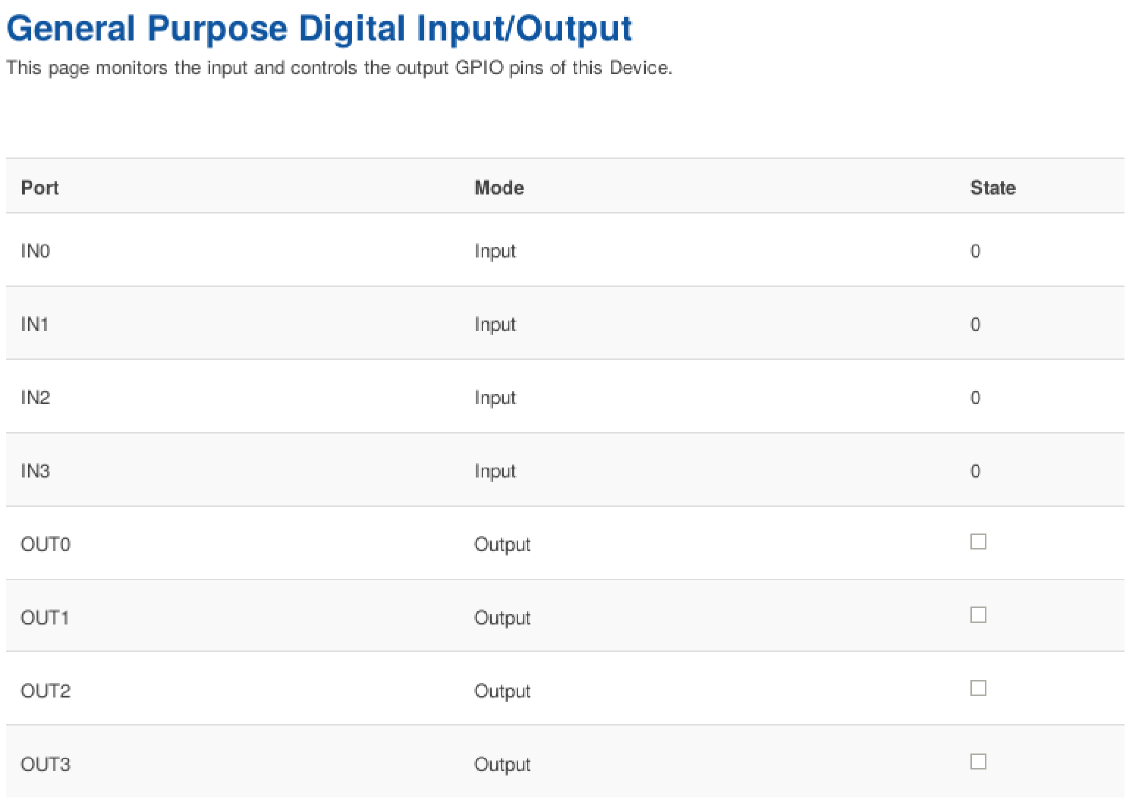
9. Services

Figure 57: Menu Services

The menu of *Services* provides the four entries named as *GPIO*, *NetCom*, *NET-CAN* and *SimpleVPN*. These reference certain interfaces in the Device, which may be used to connect to special hardware. *GPIO* is for digital input and output signals, controlled via the web interface. *NetCom* refers to the two serial ports, and allows to use them in the same way as the VScom NetCom Mini devices. And *NET-CAN* refers to a **CAN** bus interface, available for remote control via the VPNRouter tunnel in the same way as the VScom NET-CAN 110. The function of *NET-CAN* is only available if a **CAN** bus interface exists on the model. *SimpleVPN* serves for configuration of an virtual private network (VPN) with two devices. The click on `[Services]` opens the *GPIO* configuration.

9.1. GPIO

The changes in this function are automatically applied, there is no [Save] buttom at the bottom.



General Purpose Digital Input/Output

This page monitors the input and controls the output GPIO pins of this Device.

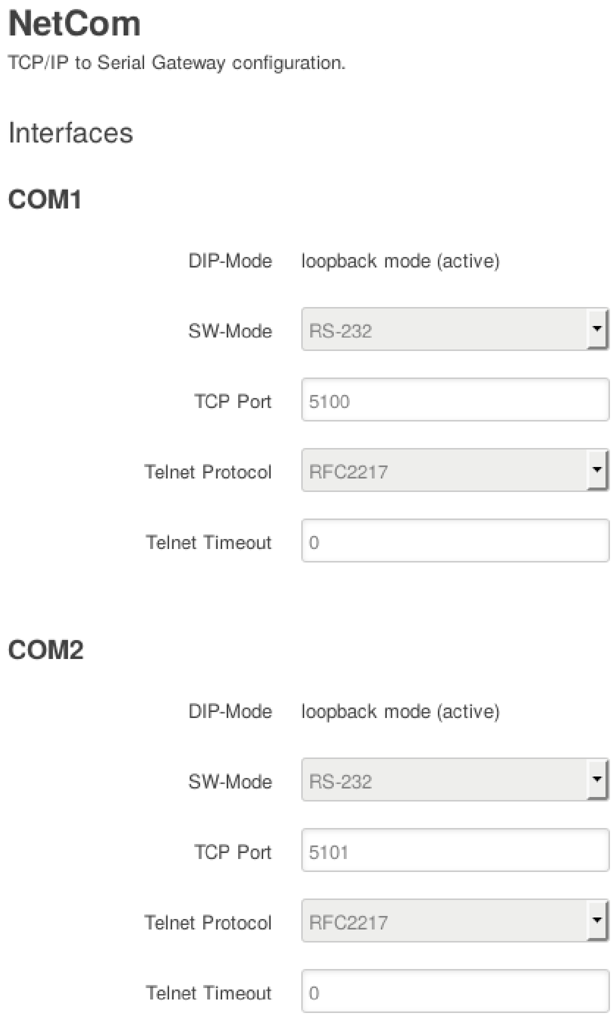
Port	Mode	State
IN0	Input	0
IN1	Input	0
IN2	Input	0
IN3	Input	0
OUT0	Output	□
OUT1	Output	□
OUT2	Output	□
OUT3	Output	□

Figure 58: GPIO Control

In column *Port* the name represents special contacts on the Device, like **OUT3** or **IN1**. In this example figure 58 the *Mode* is fixed as *Input* and *Output*. For *Input* direction you can read the *State* of the external signal. "0" is for low voltage or an inactive signal, while "1" represents high voltage on an active signal. For *Output* direction you may check a signal to make it active, then the output is high voltage. Without checkmark the *State* is inactive, i.e. low voltage.

9.2. NetCom

The Device offers serial ports named as **COM1** and **COM2**. For remote control of the serial ports the protocol known as RFC 2217 is used.



NetCom

TCP/IP to Serial Gateway configuration.

Interfaces

COM1

DIP-Mode loopback mode (active)

SW-Mode RS-232

TCP Port 5100

Telnet Protocol RFC2217

Telnet Timeout 0

COM2

DIP-Mode loopback mode (active)

SW-Mode RS-232

TCP Port 5101

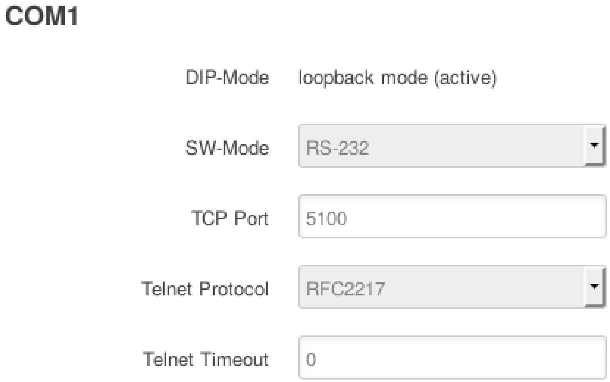
Telnet Protocol RFC2217

Telnet Timeout 0

Figure 59: NetCom Configuration

The upper section *COM1* configures operation of serial port **COM1**, while section *COM2* configures the **COM2** port. By default the positions of the DIP switches decisive of the active mode. The DIP switches are on the underside or back of the device. If the position of the DIP switches is *select by software* (OFF OFF ON ON) the configuration of the *SW-Mode* is valid. The *SW-Mode* supports the modes: *RS-232*, *RS-422*, *RS-422 with termination*, *RS-485 full duplex*, *RS-485 full duplex with termination*, *RS-485 half duplex*, *RS-485 half duplex with termination*, *DIP switches configured mode* and *loopback mode*.

The connection for remote control is via TCP/IP, so a *TCP Port* is required. By default the first serial port uses `5100`, the next ports use `5101` and following (if there are more than two ports). The serial ports then operate in the same way as the VScom NetCom Mini Serial Device Servers. There is a driver for Windows operating system, which allows to use the remote serial port like a virtual local Com Port on your computer. Other drivers or libraries using RFC 2217 are supported in the same way, and on different operating systems.



COM1

DIP-Mode loopback mode (active)

SW-Mode RS-232

TCP Port 5100

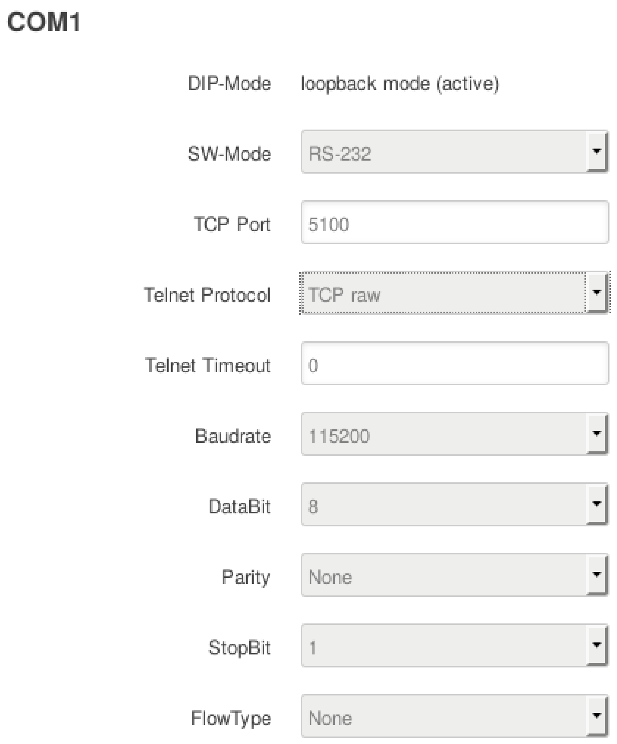
Telnet Protocol RFC2217

Telnet Timeout 0

Figure 60: Configuration RFC2217

The remote control functions are not limited to transmit and receive serial data to a connected machine. It is also possible to control the status and operation mode of the serial port. The *Telnet Protocol* extension known as *RFC 2217* is used for that purpose, the other choice is *TCP raw*. With that second choice indeed only transmit and receive with a fixed configuration is possible. Let the *Telnet Timeout* stay at the value of 0.

The following parameters only have an effect when *TCP raw* is selected for communication. They are fairly common and do not need much explanation.



COM1

DIP-Mode	loopback mode (active)
SW-Mode	RS-232
TCP Port	5100
Telnet Protocol	TCP raw
Telnet Timeout	0
Baudrate	115200
DataBit	8
Parity	None
StopBit	1
FlowType	None

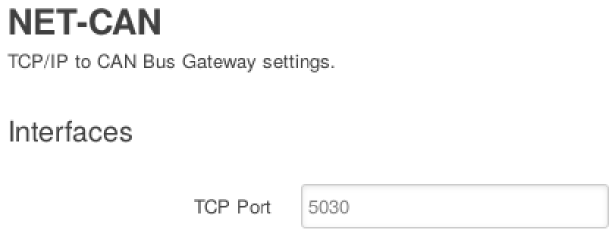
Figure 61: Configuration TCP raw

- The *Baudrate* is selectable from a drop-down list of common values. At the bottom the entry of – *custom* – let you type the desired rate into the box (e.g. `31250`).
- The *DataBits* are possible as *8* or *7*.
- The *Parity* is available with the choice of *None*, *Even* and *Odd*.
- The *StopBit* may have a duration of *1* or *2* data bits.
- Finally the *FlowType* is usable as *None* (no control), *XON/XOFF* (software flow control) and *RTS/CTS* (hardware handshake).

Activate the new configuration using the `[Save]` button.

9.3. NET-CAN

Some models also support an interface to **CAN** Bus. This interface is usable via network by TCP/IP, from remote locations and the LAN ports. It supports the same VSCAN library as the VScom NET-CAN CAN Gateways.



NET-CAN

TCP/IP to CAN Bus Gateway settings.

Interfaces

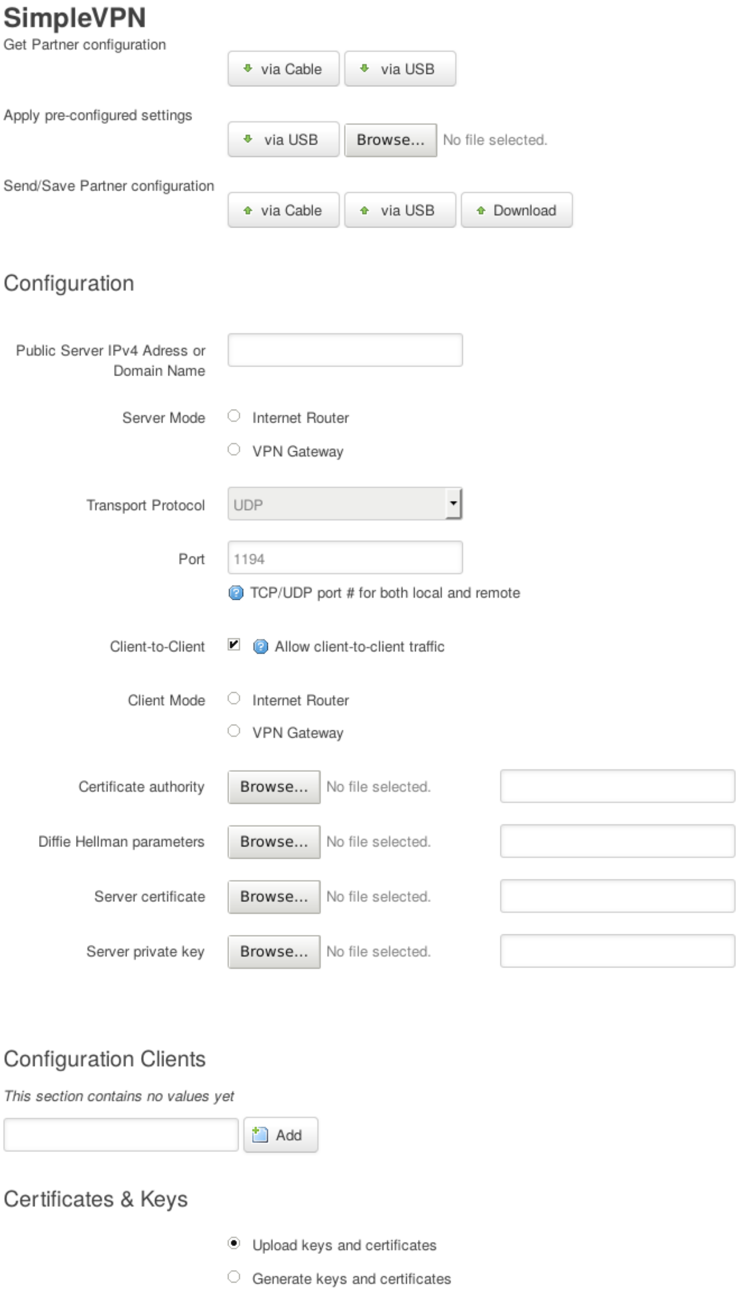
TCP Port 5030

Figure 62: NET-CAN Configuration

The configuration for remote control just requires to define the network parameters. Here only the *TCP Port* is necessary, the default value is `5030`.

9.4. SimpleVPN

The service SimpleVPN allows easy configuration of an virtual private network (VPN) connecting two or more locations with an encrypted tunnel. This service can configure a pair or more industrial routers; so that all routers have a functional configuration after this dialog. Note: The service SimpleVPN is only important if you have a set of industrial routers. There are several options on this web page that will be explained block by block. You can make all relevant settings which are needed for a virtual private network (VPN) on this page.



SimpleVPN

Get Partner configuration: via Cable | via USB

Apply pre-configured settings: via USB | Browse... No file selected.

Send/Save Partner configuration: via Cable | via USB | Download

Configuration

Public Server IPv4 Adress or Domain Name: □

Server Mode: ○ Internet Router ○ VPN Gateway

Transport Protocol: UDP

Port: 1194

TCP/UDP port # for both local and remote

Client-to-Client: ☑ Allow client-to-client traffic

Client Mode: ○ Internet Router ○ VPN Gateway

Certificate authority: Browse... No file selected.

Diffie Hellman parameters: Browse... No file selected.

Server certificate: Browse... No file selected.

Server private key: Browse... No file selected.

Configuration Clients

This section contains no values yet

Add

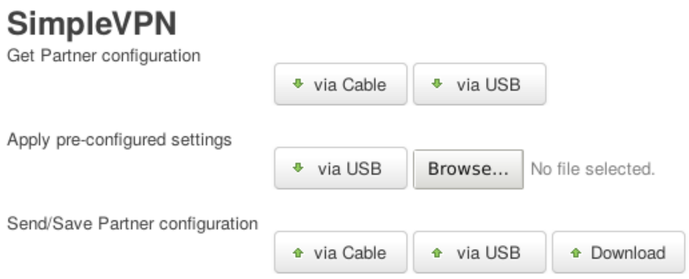
Certificates & Keys

● Upload keys and certificates

○ Generate keys and certificates

Figure 63: Overview SimpleVPN

9.4.1. Configuration transfer



SimpleVPN

Get Partner configuration

Apply pre-configured settings

Send/Save Partner configuration

Figure 64: Area configuration transfer

This area is for transfering the configurations files. There are two options:

1. Transfer the new configuration to VPNRouter Clients see section 9.4.1.1 on the next page. Note: This point is only important if you are configuring the industrial routers for the first time.
2. Modify existing configurations and transfer the new configuration to VPNRouter Clients see section 9.4.1.2 on page 55.

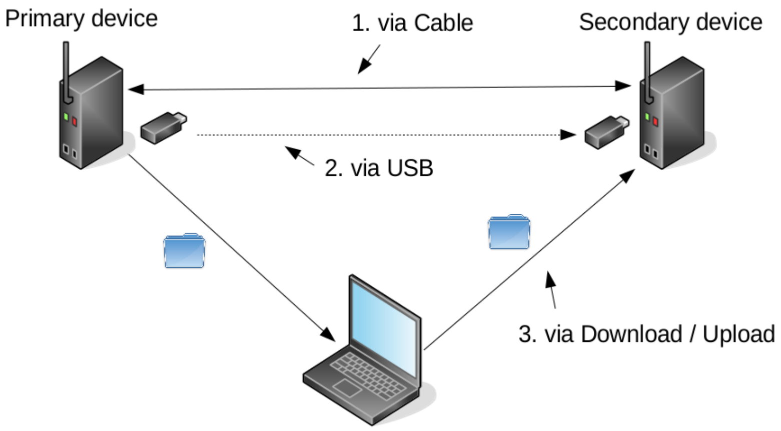


Figure 65: Overview transfer SimpleVPN

The figure 65 shows the different ways to transfer configurations.

9.4.1.1. New configuration

There are three different options to send the new configuration to a other device.

1. ***via Cable*** :

   corresponds to point 1 of figure 65 on the preceding page.

   a) Make sure that the devices are connected together via the *LAN port*. A switch may be needed to connect all Clients.

   b) Check that the configuration is correct and certificates and keys are present.

   c) To send the configuration to the partner device use the button `[via Cable]` in the area "Send/Save Partner configuration".

   d) A list of all connected VPNRouters is presented.

   e) Choose a VPNRouter by clicking on it. The SimpleVPN page is shown (after authentication if a password was already set). The APP LED will also light to show which Router you are configuring.

   f) Please choose a Client. Use the button `[Selected]` to apply the Client configurations. The button `[Selected]` will be displayed in green.

   g) Continue with the remaining Routers at e).

2. ***via USB***:

   corresponds to point 2 of figure 65 on the previous page.

   a) Make sure that the USB stick is connected to the USB port on the device.

   b) Check that the configuration is correct and certificates and keys are present.

   c) When you use the button `[via USB]` in the area "Send/Save Partner configuration" a new folder will be created on the USB Stick with configurations, certificates and keys in it.

   d) Disconnect the USB stick from the USB port.

   e) Disconnect the device from the LAN port.

   f) Connect a VPNRouter Client to your PC via the LAN port with an Ethernet cable.

   g) Connect the USB stick to the Router.

   h) Then open your browser and type the IP Address 192.168.178.1 into the address bar.

   i) Logon the Web UI (Webinterface) see section 6.2 on page 26.

   j) Open the SimpleVPN site.

   k) To apply the configuration for the Client use the button `[via USB]` in the area "Apply pre-configured settings".

   l) Please choose the corresponding Client. Use the button `[Selected]` to apply the Client configurations. The button `[Selected]` will be displayed in green.

   m) Disconnect the USB stick from the USB port.

n) Continue with the remaining Routers at e).

3. ***via Download / Upload***:

   corresponds to point 1 of figure 65 on page 53.

   a) Use the button `[Download]` to generate a tgz file.

   b) Now you can save the tgz file on your own computer.

   c) Disconnect the Server from the LAN port.

   d) Connect a Client to your PC via the LAN port with an Ethernet cable.

   e) Then open your browser and type the IP Address 192.168.178.1 into the address bar.

   f) Logon the Web UI (Webinterface) see section 6.2 on page 26.

   g) Open the SimpleVPN site.

   h) You can upload the generated tgz file in the area “Apply pre-configured settings” to apply the configuration to the secondary device. Click on `[Browse]` and select the tgz file from your computer.

   i) Please choose the corresponding Client. Use the button `[Selected]` to apply the Client configurations. The button `[Selected]` will be displayed in green.

   j) Continue with the remaining Routers at e).

9.4.1.2. Existing configurations

Attention: Changes in the exsiting VPN network should only be made if it is necessary. There are two options to modify existing configurations.

1. ***via Cable***:

   a) Make sure that the devices are connected together via the *LAN port*.

   b) Using the button `[via Cable]` in the area “Get Partner configuration” to get the configuration from the secondary device .

   c) Now you can modify the configuration.

   d) When the necessary settings have been made, click on the button `[Save & Apply]` and wait for the changes to be applied.

   e) Transfer the configuration see in section 1 on the previous page.

2. ***via USB***:

   a) Check that the configuration is available on your USB stick. It is the folder “VS-Router” with configurations, certificates and keys files.

   b) Connect the USB stick with the USB port on the device.

   c) Using the button `[via USB]` in the area “Get Partner configuration” to get the configuration from the secondary device.

   d) Now you can modify the configuration.

e) When the necessary settings hnd cannot be used. The following table shows the generalave been made, click on the button [Save & Apply] and wait for the changes to be applied.

f) Transfer the configuration see section 2 on page 54.

9.4.2. Configuration

In this section you can make all relevant settings which are needed for a virtual private network (VPN). If all settings are correct and complete click on the button [Save & Apply] and wait for the changes to be applied. The goal of this service is to build a virtual private network (VPN) to connect two or more locations with an encrypted tunnel. The advantage of a VPN is that it expands an existing network over the Internet while ensuring to transmit sensitive data in a way that protects it from tampering and interception. This service helps to make the necessary settings step by step. The current device is automatically the *Server*. It allows to configure multiple devices. The figure 66 shows an exemplary topology.

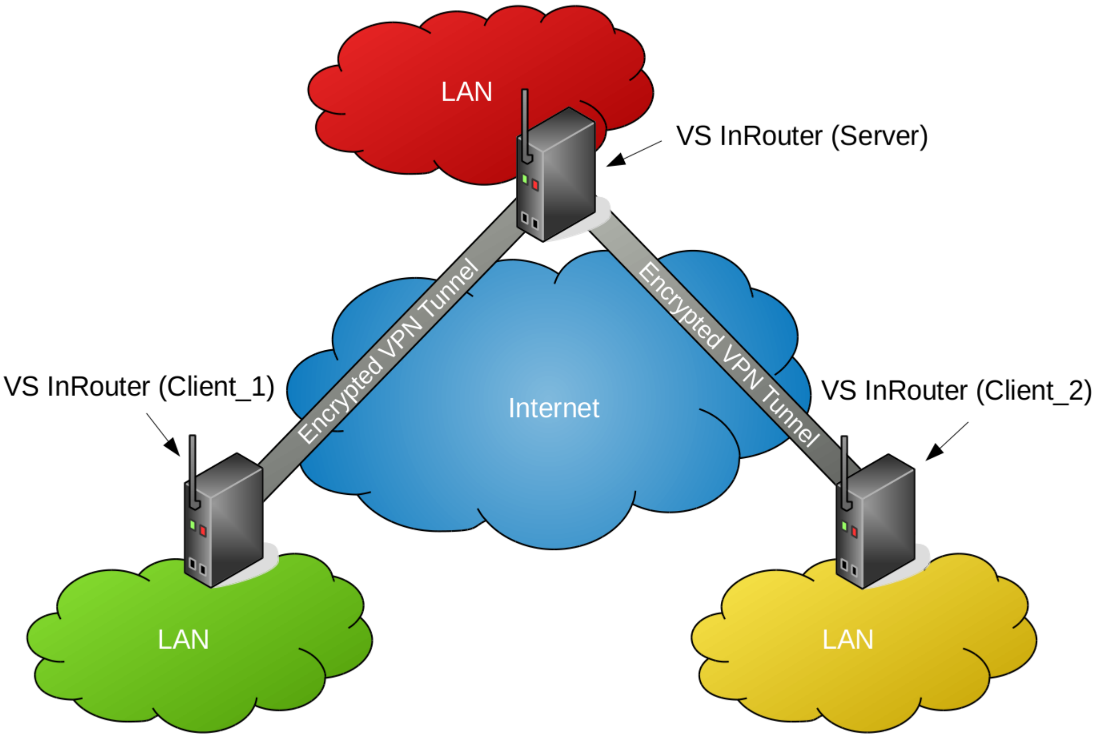


Figure 66: Topology

9.4.2.1. Server Settings

In this section you can make the necessary settings for the *Server*.

9.4.2.1.1. Public Server IPv4 Adress or Domain Name

Please fill in this field the *Public Server IPv4 Adress* or the *Domain Name*.

Public Server IPv4 Adress or Domain Name

Figure 67: SimpleVPN- Public Server IPv4 Address

The must be the public IP address under which the *Server* VPNRouter is or will be accessible over the Internet. You may use services like https://www.whatismyip.com/. The Internet Service Provider may (preferibly) assign a static IP address to your Internet access. If only a dynamic IP address is available, a DynDNS service is necessary. The resulting DNS name belongs in this field in that case. To make the Router accessible you may need to do a few more steps explained in the following section.

9.4.2.1.2. Server Mode and Client Mode

It is possible to use the devices in two different variation. You can use the device as *Internet Router* or *VPN Gateway*.

Server Mode ○ Internet Router
○ VPN Gateway

Client Mode ○ Internet Router
○ VPN Gateway

(a) Server Mode

(b) Client Mode

Figure 68: Server and Client Mode

Difference between *Internet Router* and *VPN Gateway*.

Internet Router:

- Provides its own network on LAN-Ports with DHCP Server
- Provides the firewall to protect the local network
- Provides access to the other site over an encrypted VPN tunnel
- All device on the LAN side have access to the VPN.
- The WAN-Port is directly (or possibly indirectly behind a modem) attached to the Internet.

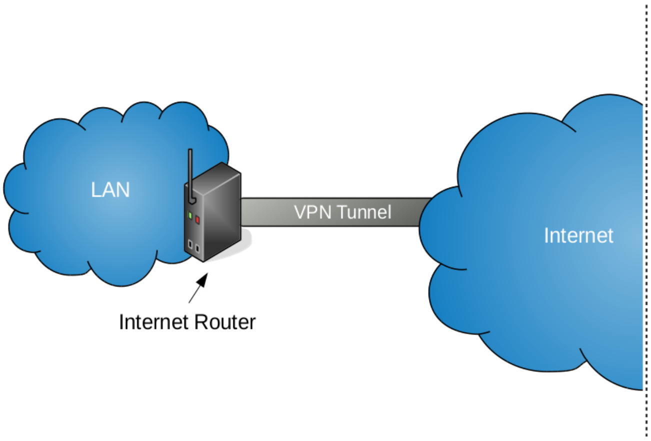


Figure 69: Internet Router

VPN Gateway:

- Is a device in a already existing local network
- Can be used as a switch
- Provides access to the other site over an encrypted VPN tunnel
- If the VPNRouter acts as VPN Server, the router of the existing local network has to assign the VPN port to this VPN router (port forwarding).
- Every device that may use the VPN has to have a route to the VPNRouter for every subnet it may access. This may be done in the router or in every device.

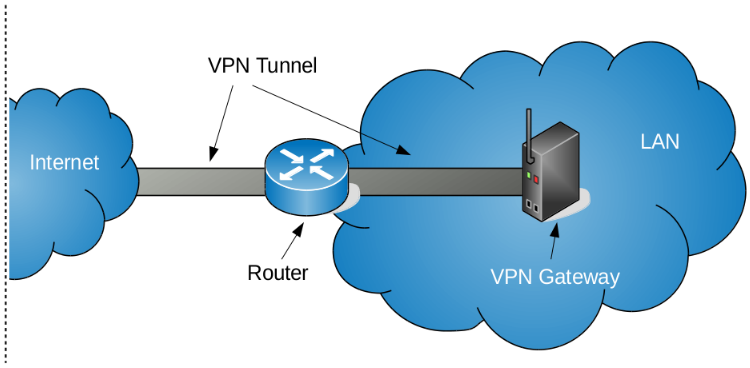


Figure 70: VPN Gateway

9.4.2.1.3. Server LAN IPv4-Address It is the local IP address of the *Server*. This IP address should be from the IPv4 address ranges assigned to private networks. The table 13 in section 7.1.2 shows the reserved private IPv4 addresses.

Server LAN IPv4-Address

Figure 71: SimpleVPN - Server IPv4-Address

By default it is the best option to use private addresses from the class C block. If you need more than 65,536 Hosts you can use one of the other classes. In an IP network, two addresses are always automatically assigned. For example, in 192.168.1.0/24, "0" is the assigned network address. In 192.168.1.255/24, "255" is the assigned broadcast address. The 0 and 255 are always assigned and should not be used for hosts. Please do not use the two IPv4 addresses which are used to connect the encrypted VPN tunnel, also do not use addresses of the 10.8.0.0/24 range.

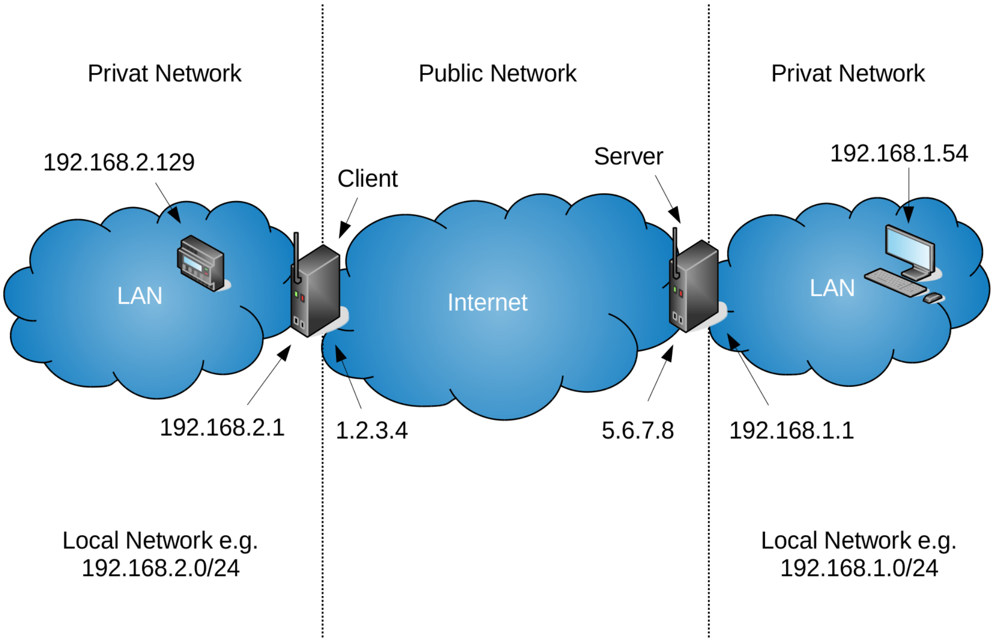


Figure 72: Difference between public and private addresses

The figure 72 shows the difference between public and private IP addresses.

9.4.2.1.4. Server LAN Netmask Please choose the corresponding netmask for the private IPv4 address. A netmask is a 32-bit mask used to divide an IP address into subnets and specify the networks available hosts.

Figure 73: SimpleVPN - Server LAN Netmask

The following table shows common netmasks

Class	Netmask length	# of networks	# of hosts	Netmask
Class A	8	126	16,777,214	255.0.0.0
Class B	16	16,382	65,534	255.255.0.0
Class C	24	2,097,150	254	255.255.255.0

Table 14: Common netmasks

9.4.2.1.5. Transport Protocol It is possible to change the transport protocol. By default the transport protocol UDP is selected.

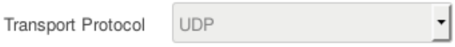
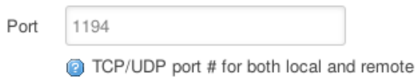

Transport Protocol: UDP

Figure 74: SimpleVPN - Transport Protocol

TCP is a connection oriented stream over an IP network. It guarantees that all sent packets will reach the destination in the correct order. This imply the use of acknowledgement packets sent back to the sender, and automatic retransmission, causing additional delays and a general less efficient transmission than UDP. UDP is a connection-less protocol. Communication is datagram oriented. The integrity is guaranteed only on the single datagram. Datagrams reach destination and can arrive out of order or don't arrive at all. It is more efficient than TCP because it does not use ACKs. It's generally used for real time communication, where a little percentage of packet loss rate is preferable to the overhead of a TCP connection.

9.4.2.1.6. Port The VPN Server will listen for client connections on a UDP or TCP port. By default it is port 1194 (OpenVPN's official port number).



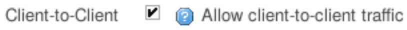
Port 1194

TCP/UDP port # for both local and remote

Figure 75: OpenVPN Port

You can change the port if it is necessary. It is recommended to use the port 1194.

9.4.2.1.7. Allow Client-to-Client traffic Enable client-to-client communication by placing a checkmark in the box if you would like connecting clients to be able to reach each other over the VPN. By default, clients will only be able to reach the server.



Client-to-Client ☑ Allow client-to-client traffic

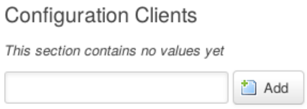
Figure 76: OpenVPN client-to-client

9.4.2.1.8. Upload Server Certificates and Keys You will need the following certificates and keys for the server:

- Certificate authority
- Diffie Hellman parameters
- Server certificate
- Server private key

Click on the button `[Browse]` and select the file to upload a certificate or a key. One can also generate these keys and certificates on the device itself at bottom of the page.

9.4.2.2. Add a Client Please enter the name of the client in the appropriate field. For example *Client_1*. To add the client please click on the button `[Add]`.

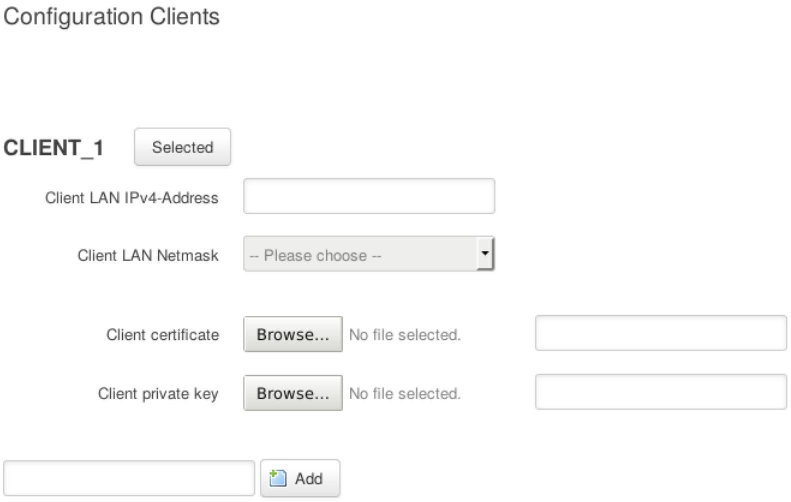


Configuration Clients

This section contains no values yet

Figure 77: Add a Client

It appears an area where you can configure the *Client*. See section 9.4.2.3.



Configuration Clients

CLIENT_1

Client LAN IPv4-Address

Client LAN Netmask: -- Please choose --

Client certificate: No file selected.

Client private key: No file selected.

Figure 78: Client overview

9.4.2.3. Client Settings

In this section you can make the necessary settings for each *Client*.

9.4.2.3.1. Client LAN IPv4-Address

It is the local network IP address of the *Client*. This adress should be from the IPv4 address ranges assigned to private networks. The table 13 on section 7.1.2 shows the reserved private IPv4 addresses.

Client LAN IPv4-Address

Figure 79: SimpleVPN - Client LAN IPv4-Address

By default it is the best option to use private adresses from the class C block. If you need more than 65,536 Hosts you can use one of the other classes. Please use not the two IPv4 addresses which are used to connect the encrypted VPN tunnel, also do not use addresses of the 10.8.0.0/24 range. The figure 72 shows the difference between public and private IP addresses.

9.4.2.3.2. Client LAN IPv4-Netmask

Please choose the corresponding netmask for the private IPv4 address. A netmask is a 32-bit mask used to divide an IP address into subnets and specify the networks available hosts.

Client LAN Netmask

Figure 80: SimpleVPN - Client LAN Netmask

The table 14 in section 9.4.2.1.4 shows common netmasks.

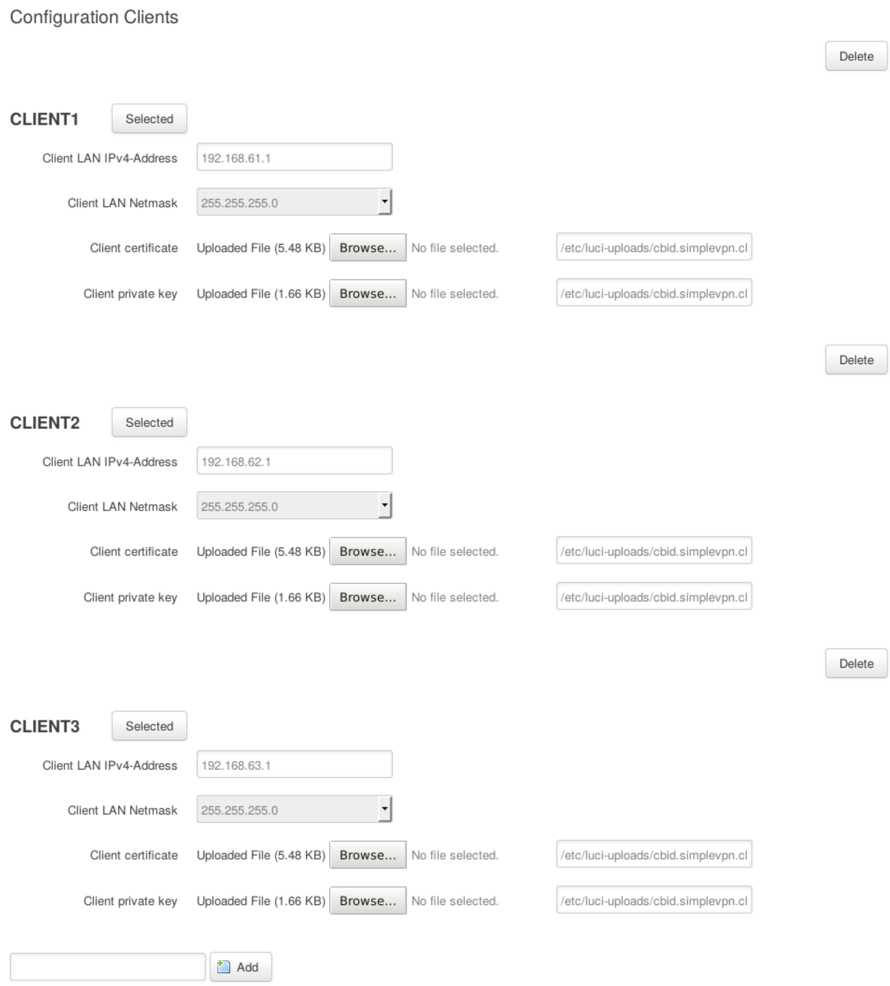
9.4.2.3.3. Upload Client Certificates and Keys

You will need the following certificates and keys for each client:

- Client certificate
- Client private key

Click on the button `[Browse]` and select the file to upload a certificate or a key. One can also generate these keys and certificates on the device itself at bottom of the page.

9.4.2.4. Delete a Client It is possible to delete a created client. The client will be removed from the virtual private network (VPN). Use the button `[Delete]` on the right side to remove a created client.



Configuration Clients

CLIENT1
Client LAN IPv4-Address: 192.168.61.1
Client LAN Netmask: 255.255.255.0
Client certificate: Uploaded File (5.48 KB) No file selected. /etc/luci-uploads/cbid.simplevpn.cl
Client private key: Uploaded File (1.66 KB) No file selected. /etc/luci-uploads/cbid.simplevpn.cl

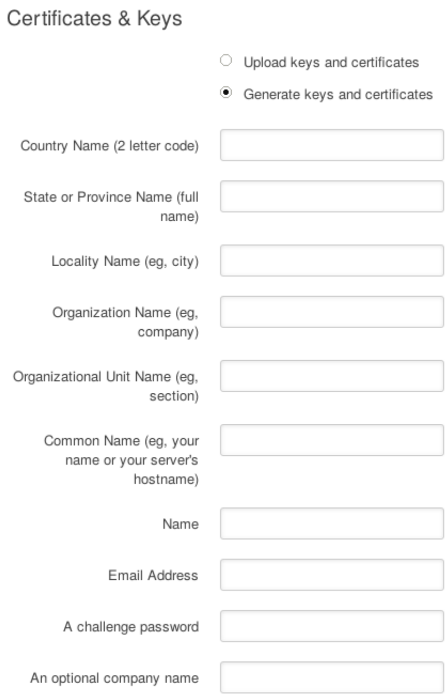
CLIENT2
Client LAN IPv4-Address: 192.168.62.1
Client LAN Netmask: 255.255.255.0
Client certificate: Uploaded File (5.48 KB) No file selected. /etc/luci-uploads/cbid.simplevpn.cl
Client private key: Uploaded File (1.66 KB) No file selected. /etc/luci-uploads/cbid.simplevpn.cl

CLIENT3
Client LAN IPv4-Address: 192.168.63.1
Client LAN Netmask: 255.255.255.0
Client certificate: Uploaded File (5.48 KB) No file selected. /etc/luci-uploads/cbid.simplevpn.cl
Client private key: Uploaded File (1.66 KB) No file selected. /etc/luci-uploads/cbid.simplevpn.cl

Figure 81: Client delete

9.4.3. Generate Certificates and Keys

You have the option to generate new certificates and keys on the VPNRouter. The generation process is very simple.



Certificates & Keys

○ Upload keys and certificates

● Generate keys and certificates

Country Name (2 letter code)	
State or Province Name (full name)	
Locality Name (eg, city)	
Organization Name (eg, company)	
Organizational Unit Name (eg, section)	
Common Name (eg, your name or your server's hostname)	
Name	
Email Address	
A challenge password	
An optional company name	

Figure 82: Generate Certificates and Keys

Please fill in all necessary fields. Click the button `[Save]`. After the store process the button `[Generate]` and `[Generate DH Parameters]` will be displayed.

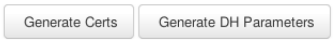


Figure 83: Buttons Generate and Generate DH Parameters

If you click on the button `[Generate]` the certificates and keys will automatically be generated in the background. A set of Diffie–Hellman parameters are already on the Router because the generation process on the device may take a considerable time. They will become visible after the generation the other keys and certificates. Use the button `[Generate DH Parameters]` to calculate and get new Diffie–Hellman parameters. After the generation process the certificates and keys will be displayed as if they were uploaded. You may need to reload the page.

A. History

Juli 2016 Release Manual

B. License

Figure 66, 69, 70, 65, 72 build upon VRT Network Equipment (Shape Gallery for LibreOffice/OpenOffice) by VRT Systems licensed under CC BY-SA 3.0 .