

# BENUTZERHANDBUCH



## Impressum

Copyright © 2015 TELTONIKA Ltd. Alle Rechte vorbehalten. Reproduktion, Übertragung, Verteilung oder Speicherung von Teilen oder die gesamte Inhalt in diesem Dokument in irgendeiner Form ohne die vorherige schriftliche Zustimmung der TELTONIKA Ltd ist verboten. Der Hersteller behält sich das Recht vor, das Produkt und Handbuch zum Zwecke der technischen zu ändern Verbesserung ohne vorherige Ankündigung.

**Andere Produkt- und Firmennamen können Marken oder Handelsnamen ihrer jeweiligen sein Inhaber.**

## Beachtung

Vor Inbetriebnahme des Gerätes empfehlen wir zuerst diese Bedienungsanleitung zu lesen.

Sie reißen das Gerät nicht geöffnet. Sie das Gerät nicht berühren, wenn das Gerät Block gebrochen.

Alle Wireless-Geräte für die Datenübertragung können Störungen, anfällig sein, die könnten die Leistung beeinträchtigen.

Das Gerät ist nicht wasserdicht. Halten Sie es trocken.

Gerät wird durch niedrige Spannung + 9V-DC-Netzteil mit Strom versorgt.

## Inhaltsverzeichnis

Impressum .....	2
Beachtung .....	2
SICHERHEITSINFORMATION .....	8
Geräteanschluss .....	9
<u>1 Einführung</u> .....	<u>10</u>
<u>2 Spezifikationen</u> .....	<u>10</u>
2.1 Ethernet .....	10
2.2 Wi-Fi .....	10
2.3 Hardware .....	10
2.4 Elektrische, mechanische und Umwelt .....	10
2.5 Anwendungen .....	11
<u>3 Einrichten des Routers</u> .....	<u>11</u>
3.1 Installation .....	11
3.1.1 Frontplatte und Rückseite .....	12
3.1.2 Hardware installation .....	12
3.2 Protokollierung in .....	13
<u>4 Betriebsarten</u> .....	<u>16</u>
<u>5 Powering Optionen</u> .....	<u>16</u>
5.1 Einschalten des Gerätes aus höheren Spannung .....	17
<u>6 Der Status</u> .....	<u>18</u>
6.1 Übersicht .....	18
6.2 Systeminformationen .....	19
6.3 Network Information .....	20
6.4 Geräteinformation .....	31
6.5 Dienstleistungen .....	32
6.6 Routen .....	32
6.6.1 ARP .....	32
6.6.2 Aktive IP-Routen .....	33
6.6.3 Aktive IPv6-Routen .....	33
6.7 Echtzeit-Graphen .....	34
6.7.1 Mobile Signal Strenght .....	34
6.7.2 Realtime Load .....	35
6.7.3 Verkehr .....	36

6.7.4 Realtime Wireless .....	37
6.7.5 Echtzeit-Verbindungen .....	38
6.8 Mobile Verkehrs .....	39
6.9 Speed Test .....	39
6.10 Events Log .....	40
6.10.1 Alle Veranstaltungen .....	40
6.10.2 Systemereignisse .....	41
6.10.3 Netzwerk Veranstaltungen .....	42
6.10.4 Events Berichterstattung .....	43
6.10.5 Berichterstattung Konfiguration .....	44
7Netzwerk .....	46
7.1 Mobil .....	46
7.1.1 Allgemeine .....	46
7.1.2 SIM Management .....	48
7.1.3 Netzbetreiber .....	49
7.1.4 Mobile Data-Grenze .....	50
7.1.5 Sim Standby-Schutz .....	51
7.2 WAN .....	52
7.2.1 Operation Mode .....	52
7.2.2 Allgemeine Konfiguration .....	53
7.3 LAN .....	59
7.3.1 Konfiguration .....	59
7.3.2 DHCP-Server .....	60
7.4 VLAN .....	61
7.4.1 VLAN-Netzwerke .....	61
7.4.2 LAN-Netzwerke .....	63
7.5 Drahtlose .....	63
7.6 Firewall .....	66
7.6.1 Allgemeine Einstellungen .....	66
7.6.2 DMZ .....	67
7.6.3 Port Forwarding .....	67
7.6.4 Verkehrsregeln .....	69
7.6.5 Benutzerdefinierte Regeln .....	74
7.6.6 DDOS Prävention .....	75
7.7 Statische Routen .....	78

8 Dienstleistungen .....	79
8.1 VRRP .....	79
8.1.1 VRRP LAN Konfigurationseinstellungen .....	79
8.1.2 überprüfen Internetverbindung .....	79
8.2 TR-069.....	80
8.2.1 TR-069 Parameter Konfiguration .....	80
8.3 Web filter .....	81
8.3.1 Site-Blocker .....	81
8.3.2 Proxy basierte URL Content-Blocker .....	81
8.4 NTP .....	82
8.5 RS232 / RS485 .....	83
8.5.1 RS232 .....	83
8.5.2 RS485 .....	85
8.5.3 Modi der verschiedenen Serientypen in RS232 und RS485 .....	88
8.6 VPN .....	90
8.6.1 OpenVPN .....	90
8.6.2 IPSec .....	94
8.6.3 GRE Tunnel .....	97
8.6.4 PPTP .....	99
8.6.5 L2TP .....	100
8.7 Dynamic DNS .....	101
8.8 SNMP .....	102
8.8.1 SNMP-Einstellungen .....	102
8.8.2 TRAP Einstellungen .....	103
8.9 SMS Dienstprogramme .....	104
8.9.1 SMS Dienstprogramme .....	104
8.9.2 Anruf Dienstprogramme .....	107
8.9.3 Benutzergruppen .....	107
8.9.4 SMS Management .....	108
8.9.5 Remote-Konfiguration .....	109
8.9.6 Statistiken .....	113
8.10 SMS Gateway .....	113
8.10.1 Pfosten- / Get Konfiguration .....	113
8.10.2 E-Mail an SMS .....	115
8.10.3 Geplante Nachrichten .....	116

8.10.4 Auto Antworten Konfiguration .....	118
8.10.5 SMS Forwarding .....	119
8.10.6 SMPP .....	122
8.11 GPS .....	123
8.11.1 GPS .....	123
8.11.2 GPS-Einstellungen .....	123
8.12 CLI .....	124
8.13 Netzwerkfreigaben .....	124
8.13.1 hängen Dateisysteme .....	124
8.13.2 Samba .....	125
8.13.3 Samba Benutzer .....	126
8.14 Hotspot .....	127
8.14.1 Allgemeine Einstellungen .....	127
8.14.2 Internet Zugriffsbeschränkung Einstellungen .....	128
8.14.3 Logging .....	129
8.14.4 Zielseite .....	130
8.14.5 Radius-Server-Konfiguration .....	132
8.14.6 Statistiken .....	133
8.15 Auto Reboot .....	133
8.15.1 Ping Reboot .....	133
8.15.2 Periodic Reboot .....	134
8.16 QoS .....	135
8.17 Input / Output .....	136
8.17.1 Der Status .....	136
8.17.2 Eingang .....	136
8.17.3 Ausgabe .....	138
8.17.4 Input / Output Hardwareinformation .....	141
8.18 UPNP (Universal Plug & Play) .....	147
9 System .....	148
9.1 Konfigurations-Assistent .....	148
9.2 Profile .....	150
9.3 Verwaltung .....	151
9.3.1 Allgemeines .....	151
9.3.2 Fehlerbehebung .....	152
9.3.3 Backup-.....	153

9.3.4 Diagnose .....	155
9.3.5 MAC Clone .....	155
9.3.6 Übersicht .....	156
9.3.7 Überwachung .....	157
9.4 User-Skripte .....	157
9.5 Safe mode .....	158
9.6 Firmware .....	158
9.6.1 Firmware .....	158
9.6.2 FOTA .....	159
9.7 Wiederherstellungspunkt .....	160
9.7.1 Wiederherstellungspunkt erstellen .....	160
9.7.2 Wiederherstellen Punktlast.....	160
9.8 Reboot .....	160
10 Gerätewiederherstellungs .....	160
10.1 Reset-Taste .....	161
10.2 Safemode .....	161
10.3 Bootloader's WebUI .....	161
11 Glossar: .....	162

## **SICHERHEITSINFORMATION**

In diesem Dokument werden Sie eingeführt, wie sicher einen Router zu verwenden. Wir empfehlen Ihnen, zur Einhaltung der

folgende Empfehlungen, um Verletzungen und oder Sachschäden zu vermeiden.

Sie müssen vertraut sein mit den Sicherheitsanforderungen vor Inbetriebnahme des Gerätes!

Um zu vermeiden, Brennen und Spannung verursachte Traumata des Personals mit dem Gerät arbeiten, folgen Sie bitte diesen

Sicherheitsanforderungen.

Das Gerät ist für die Versorgung von einer Limited Power Source (LPS), die den Stromverbrauch bestimmt nicht mehr als 15 VA und Nennstrom von Überstrom-Schutzeinrichtung sollte nicht 2A nicht überschreiten sollte.

Die höchste transiente Überspannung in den Ausgang (Sekundärkreis) der verwendeten PSU soll nicht überschreiten 36V Spitze.

Das Gerät kann mit dem Personal Computer (erste Sicherheitsklasse) oder Notebook (zweite verwendet werden

Sicherheitsklasse). Zugehörige Ausrüstung: PSU (Netzteil) (LPS) und Personal-Computer (PC) wird erfüllt die Anforderungen der Norm EN 60950-1.

Montieren Sie nicht oder das Gerät während eines Gewitters warten.

Um mechanische Schäden am Gerät zu vermeiden empfiehlt es sich für den Transport in eine gepackte bruchssicher Packung.

Schutz in Primärkreise der dazugehörigen PC und PSU (LPS) gegen Kurzschluss und Erde

Störungen der zugehörigen PC gelten als Teil der Gebäudeinstallation vorgesehen werden.

Zur Vermeidung von mechanischen Schäden am Gerät zu transportieren empfiehlt es sich in einem bruchssicher Packung verpackt.

Während das Gerät verwendet wird, sollte es so platziert werden, dass seine Anzeige-LEDs sichtbar sein würde, wie sie in dem Arbeits informieren

Modus ist das Gerät und wenn es irgendwelche Arbeits Probleme.

Schutz gegen Überstrom, sollte Kurzschlüsse und Erdschlüsse als Teil des Gebäudes zur Verfügung gestellt werden

installation.

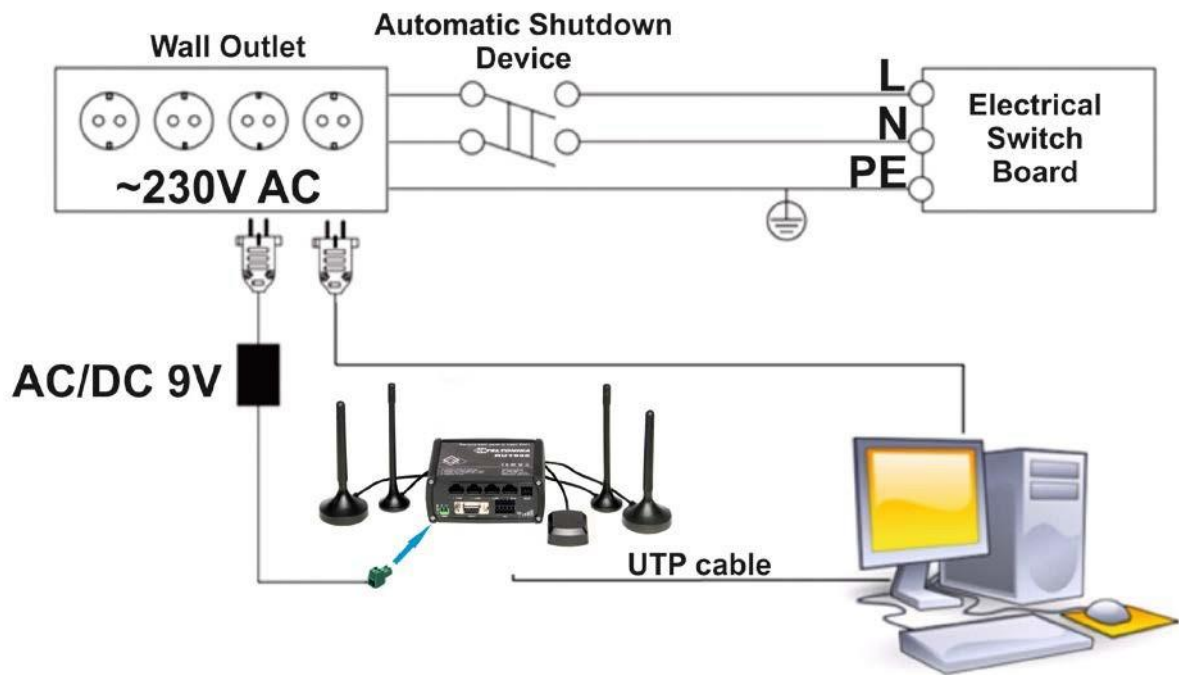
Signalpegel der Vorrichtung ist abhängig von der Umgebung, in der sie arbeitet. Für den Fall, beginnt das Gerät Arbeits

unzureichend entnehmen Sie bitte qualifiziertes Personal, um dieses Produkt zu reparieren. Wir empfehlen die Weiterleitung an eine Reparatur

Zentrum oder der Hersteller. Es sind keine austauschbaren Teile im Inneren des Gerätes.



Geräteanschluss



## 1. Einleitung

Vielen Dank für einen RUT955 LTE-Router entschieden haben!

RUT955 ist Teil der RUT9xx Serie von kompakten mobilen Router mit hoher Geschwindigkeit und drahtlose Ethernet

Verbindungen.

Dieser Router ist ideal für Leute, die gerne ihr Internet unterwegs teilen, da es nicht durch eine umständliche eingeschränkt

Kabelverbindung. Uneinnehmbar, aber nicht vergessen: der Router noch Internet-Verteilung über ein Breitband-Kabel unterstützt,

stecken Sie einfach es um die WAN-Port, den Router in den richtigen Modus eingestellt und Sie sind bereit zu suchen.

## 2 Technische Daten

### 2.1 Ethernet

- IEEE 802.3, IEEE 802.3u
- 3 x LAN 10/100Mbps Ethernet ports
- 1 x WAN 10/100Mbps Ethernet port
- Unterstützt Auto-MDI / MDIX

### 2.2 Wi-Fi

- IEEE 802.11b / g / n WiFi-Standards
- 2x2 MIMO
- AP und STA-Modi
- 64/128-Bit-WEP, WPA, WPA2, WPA & WPA2 Verschlüsselungsverfahren
- 2.401 - 2.495GHz Wi-Fi-Frequenzbereich
- 20dBm max WiFi TX-Leistung
- SSID Stealth-Modus und Zugriffskontrolle basierend auf MAC-Adresse

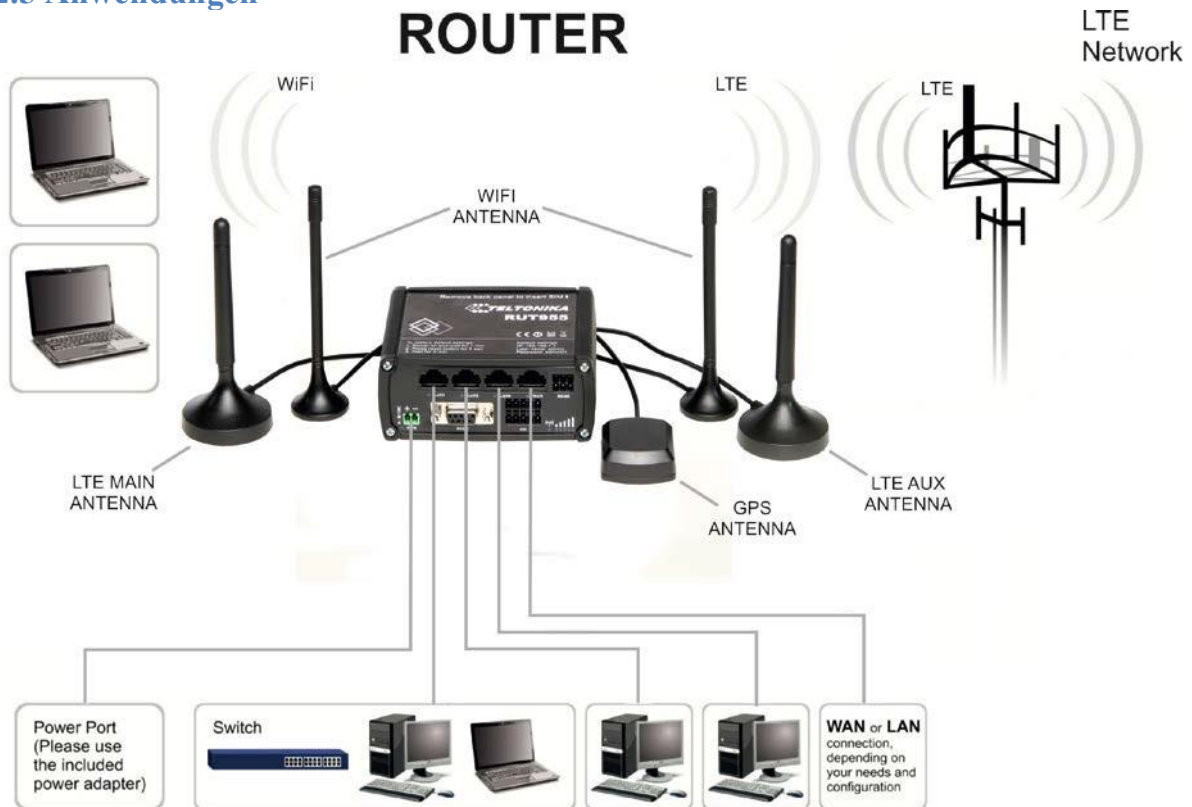
### 2.3 Hardware

- Hohe Leistung 560 MHz CPU mit 128 MB DDR2-Speicher
- 5,5 / 2,5 mm DC-Steckdose
- Reset • / Restore-Taste auf dem Standard
- 2 x SMA für LTE, 2 x RP-SMA für WiFi Antennenanschlüsse
- 4 x Ethernet-LEDs, 1 x Power-LED
- 1 x Bi-Color-Verbindungsstatus-LED, 5 x Verbindungsstärke LEDs

### 2.4 Elektrische, mechanische und Umwelt

- Abmessungen (H x B x T)  
80mm x 106mm x 46mm
- Gewicht  
250g
- Energieversorgung  
100 - 240 V AC -> 9 VDC Wandadapter
- Eingangsspannungsbereich  
9 - 30VDC
- Energieverbrauch  
<7W
- Betriebstemperatur  
-40 ° bis 75 ° C
- Lagertemperatur  
-45 ° bis 80 ° C
- Luftfeuchtigkeit bei Betrieb  
10% bis 90% kondensations
- Luftfeuchtigkeit bei Lagerung  
5% bis 95% kondensations

## 2.5 Anwendungen



## 3 Einrichten des Routers

### 3.1 Installation

Nachdem Sie das Auspacken, folgen Sie den Schritten unten dokumentiert, um richtig das Gerät zu anschließen. Zum bessere Wi-Fi-Leistung, setzen Sie das Gerät in gut sichtbaren Stelle, als Hindernisse wie Wände und Tür hinder das Signal.

1. Zuerst Ihre Router zusammenbauen, indem die notwendigen Antennen angebracht und die SIM-Karte einsetzen.
2. Geben Sie Ihren Router an, sondern bitte das Netzteil im Lieferumfang enthalten verwenden. (WICHTIG: Die Verwendung eines anderen Netzteil kann die Garantie für dieses Produkt beschädigt werden und erlischt.).
3. Wenn Sie einen verkabelten Breitbandverbindung haben, werden Sie es auch an den WAN-Port des Routers anschließen müssen.

### 3.1.1 Frontplatte und Rückseite



#### 1,2,3 LAN Ethernet ports

4 WAN Ethernet port

5,6,7 LAN LEDs

8 WAN LED

9 RS485 connector

10 Power socket

11 RS232 connector

12 Inputs and outputs connector

13 Power LED

14 Anschluss LED

15 Signalstärke LED

#### 1 LTE auxiliary antenna connector

2 GPS-Antennenanschluss

3 LTE main antenna connector

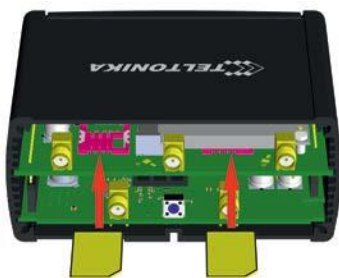
4 USB connector

5,7 WiFi Antenne connectors

6 Reset button

### 3.1.2 Hardware installation

1. Entfernen Rückseite und SIM-Karte einsetzen, die von Ihrem ISP (Internet Service Provider) gegeben wurde. Richtige SIM-Karte Orientierung wird in der Abbildung dargestellt.



2. Bringen LTE Haupt- und Wi-Fi-Antennen

3. Schließen das Netzteil an die Buchse an der Frontplatte des Gerätes. Anschließend das andere Ende des Stromes

Adapter in eine Steckdose oder Steckerleiste.

4. Eine Verbindung mit dem Gerät drahtlos (SSID: **Teltonika\_Router**) oder Verwendung Ethernet - Kabel und Stecker es in jedes LAN Ethernet

### 3.2 Anmelden bei

Nachdem Sie oben mit der Einrichtung, wie im Abschnitt beschrieben vollständig sind, dann sind Sie bereit, die Protokollierung starten in und der Router beginnen, es zu konfigurieren. Dieses Beispiel zeigt, wie auf Windows 7 auf Windows Vista verbinden: Klicken Sie auf Start ->

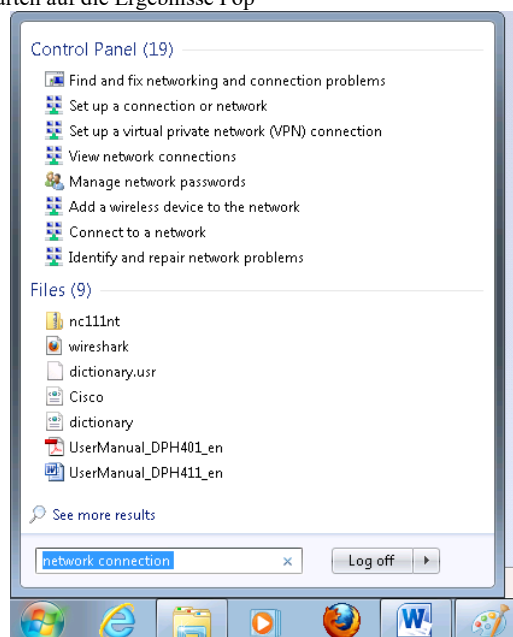
Systemsteuerung -> Netzwerk- und Freigabecenter -> Netzwerkverbindungen verwalten -> (Gehen Sie zu Schritt 4). Unter Windows XP: Klicken Sie

Start -> Einstellungen -> Netzwerkverbindungen -> (siehe Schritt 4). Sie werden nicht die „Internetprotokoll Version 4 (TCP / IPv4)“ zu sehen, statt

Sie „TCP / IP-Einstellungen“ auswählen und klicken Sie auf Optionen müssen -> (Go zu Schritt 6)

Wir müssen zuerst unsere Netzwerkkarte so einrichten, dass es ordnungsgemäß mit dem Router kommunizieren kann.

1. Drücken Sie die Starttaste
2. Geben Sie in „ Netzwerkverbindungen“, warten auf die Ergebnisse Pop

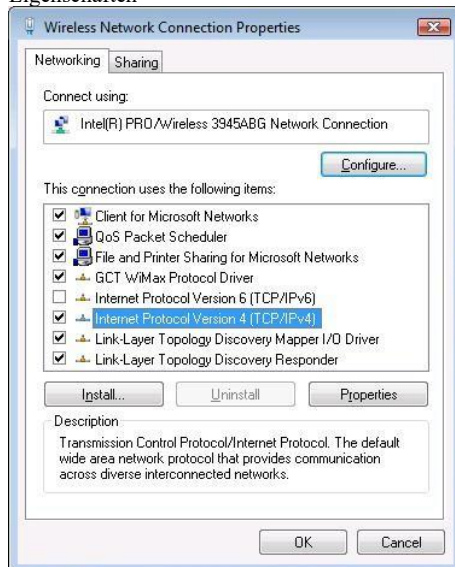


3. „Netzwerkverbindungen anzeigen“ klicken

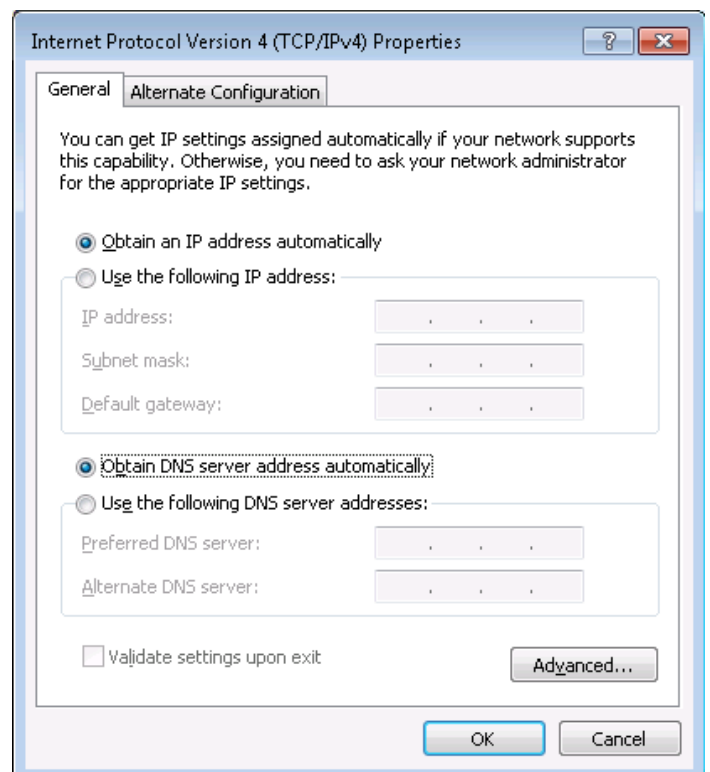


4. Klicken Sie dann rechts auf dem drahtlosen Gerät, das Sie verwenden, um Verbindung zu anderen Access Points (Es ist der mit dem Namen „Wireless Network Connection“ und hat Signalbalken auf seinem Symbol).

5. Wählen Sie Internetprotokoll Version 4 (TCP / IPv4) und klicken Sie dann auf Eigenschaften



6. Standardmäßig wird der Router einen DHCP aktiviert ist, die bedeutet, dass, wenn Sie „IP-Adresse automatisch beziehen“ wählen und „DNS-Serveradresse automatisch beziehen“, den Router sollten Sie eine IP-leasen und Sie sollten sich anmelden bereit sein.



7. Wenn Sie konfigurieren wählen manuell hier, was Sie tun können:

Wählen Sie zunächst eine IP-Adresse. Durch die Aktien Einstellungen, dass der Router in Ihnen angekommen ist, kann nur eine IP in der Eingabe

Bildung von 192.168.1.XXX, wobei XXX eine Zahl im Bereich von 2-254 (192.168.1.2, 192.168.1.254, 192.168.1.155 und

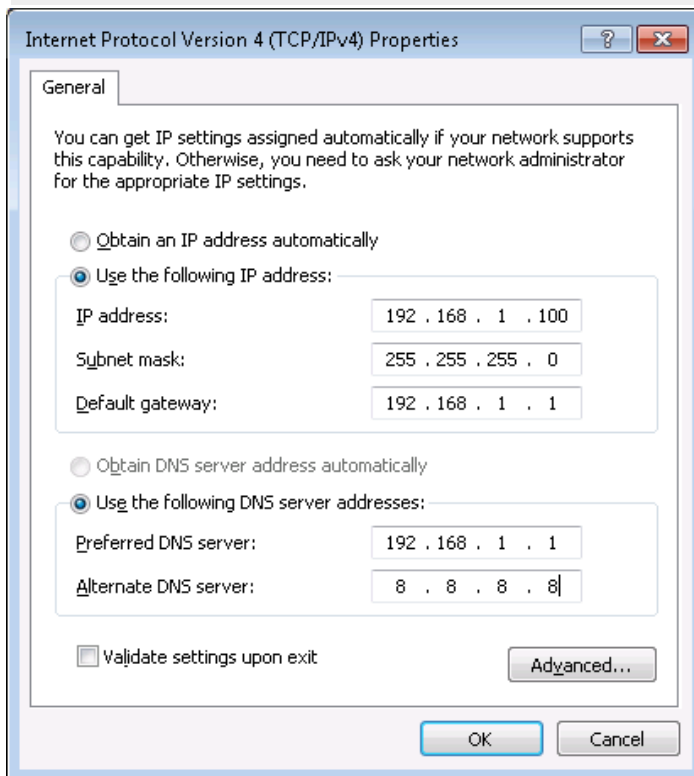
so weiter ... gültig sind; 192.168.1.0, 192.168.1.1, 192.168.1.255, 192.168.1.699 und so weiter ... sind nicht). Als nächstes werden wir geben die

Subnetz-Maske: dies hat „255.255.255.0“ sein. Dann haben wir das Standard-Gateway eingeben: dies hat „192.168.1.1“ sein. Endlich

wir geben primäre und sekundäre DNS-Server IP-Adressen. Man wird genügen, wenn es gut ist, als auch einen sekundären, einen zu haben, wie es

wird als Backup fungieren, wenn der erste ausfallen sollte. Die DNS können Ihre Router IP (192.168.1.1) sein, aber es kann auch einige extern

DNS-Server (wie das Google lautet: 8.8.8.8).



Rechtsklick auf das Wireless - Netzwerk - Symbol und wählen Sie **Verbinden / Trennen** . Es sollte eine Liste mit allen verfügbaren Pop - up drahtlose Netzwerke. Wählen Sie „Teltonika“ und klicken Sie **connect** .Dann wir unsere Lieblings - Browser starten und die Router eingeben IP in das Adressfeld:



Drücken Sie Enter. Wenn es keine Probleme gibt, sollten Sie mit einem Login-Bildschirm wie dies begrüßt:

### Authorization Required

Please enter your username and password.

Username

Password

Geben Sie das Standardpasswort, das „admin01“ in das Feld „Passwort“ und dann entweder Anmeldung klicken Sie mit Maus oder drücken Sie die Eingabetaste. Sie haben nun erfolgreich in die RUT955 angemeldet! Von hier an Sie fast jeden Aspekt Ihres Routers konfigurieren.

## 4 Betriebsarten

Die RUT9xx Serie Router unterstützt verschiedene Betriebsmodi. Es kann mit dem Internet (WAN) verbunden werden über

Mobile, Standard-Ethernet-Kabel oder über ein drahtloses Netzwerk. Wenn Sie mit dem Internet über ein Ethernet-Kabel or Wi-Fi Verbindung,

Sie können auch ein Backup Ihrer Verbindung mit für zusätzliche Stabilität mobil. Auf jeden Fall, außer wenn Sie eine Verbindung zu der

Internet über Wi-Fi, können Sie Ihr Internet über ein Ethernet-Kabel (3 Ports) und / oder ein drahtloses Netzwerk verteilen. Wenn du

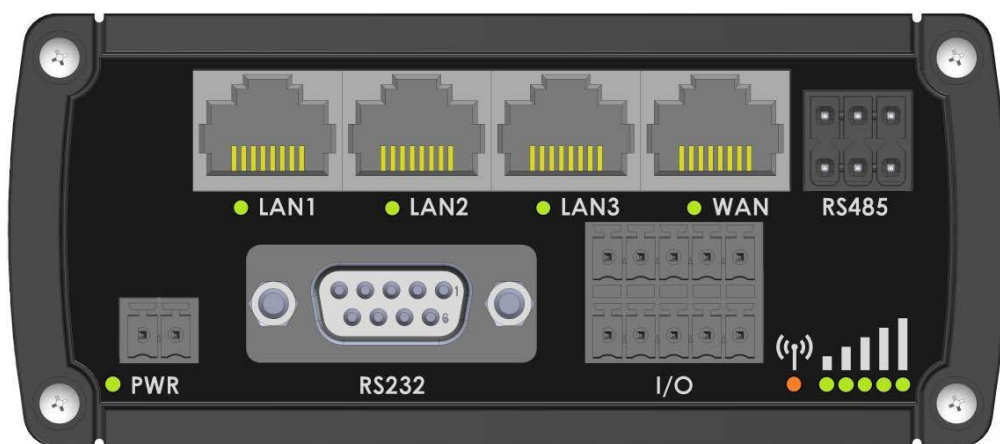
Verbindung über Wi-Fi, können Sie nicht Wi-Fi in Ihrem LAN.

WAN	LAN		Mobile Backup link
	Ethernet	Wi-Fi	
Mobile	√	√	x
Ethernet	√	√	√
Wi-Fi	√	√	√

In späteren Abschnitten wird erläutert, im Detail, wie Sie Ihren Router arbeiten in einem gewünschten Modus zu konfigurieren.

## 5 Stromversorgungsoptionen

Der RUT9xx Router kann von der Steckdose oder über Ethernet-Port mit Strom versorgt werden. Je nach Netz Architektur können Sie LAN 1-Anschluss Verwenden Sie das Gerät mit Strom zu versorgen.



RUT9xx kann gleichzeitig von der Steckdose und über Ethernet mit Strom versorgt werden. Steckdose hat eine höhere Priorität

was bedeutet, dass die Vorrichtung Leistung von der Steckdose, solange sie verfügbar ist ziehen wird.

Wenn RUT9xx wird von einer Stromquelle an den anderen Schalt verliert er Kraft für einen Bruchteil der Sekunde und

kann neu gestartet werden. Das Gerät funktioniert richtig nach dem Neustart.



Pin	Signal ID	T568A Color	T568B Color	Pins on plug face (socket is reversed)
1	TX+	 white/green stripe	 white/orange stripe	
2	TX-	 green solid	 orange solid	
3	RX+	 white/orange stripe	 white/green stripe	
4		 blue solid	 blue solid	
5	7 - 30VDC	 white/blue stripe	 white/blue stripe	
6	RX-	 orange solid	 green solid	
7	GROUND	 white/brown stripe	 white/brown stripe	
8	GROUND	 brown solid	 brown solid	

Obwohl das Gerät über Ethernet-Port mit Strom versorgt werden ist es nicht kompatibel mit IEEE 802.3af-2003-Standard.

Powering RUT9xx von IEEE 802.3af-2003 Stromversorgung **wird das Gerät beschädigt** werden, da es nicht für Eingangsspannungen von bewertet PoE-Standard.

### 5.1 Einschalten des Gerätes aus höheren Spannung

Wenn Sie sich entscheiden, nicht unsere Standard-9 VDC Wandadapter zu verwenden und möchten das Gerät von höherer Spannung versorgen (15 - 30 VDC) stellen Sie sicher, dass Sie Stromversorgung von hoher Qualität wählen. Einige Stromversorgungen können Spannung erzeugen Spitzen deutlich höher als die angegebene Ausgangsspannung, vor allem während der Verbindung und sie trennen.

Während sich das Gerät ist so konzipiert, 30 VDC Spitzen von der Hochspannungsstromversorgungen Eingangsspannung von bis zu akzeptieren schadet das Gerät. Wenn Sie Hochspannungsstromversorgungen verwenden möchten wird empfohlen, auch zusätzliche Sicherheit zu verwenden


Ausrüstung zur Unterdrückung von Spannungsspitzen von der Stromversorgung. Eine der Optionen ist „Teltonika“ PR1000 Überspannung zu verwenden, Schutzvorrichtung ISO konforme 7637-2.

## 6 Status



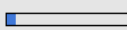



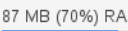















Der Statusabschnitt enthält verschiedene Informationen, wie aktuelle IP-Adressen von verschiedenen Netzwerkschnittstellen; der Staat der Router-Speicher; Firmware Version; DHCP-Leasing; assoziierten drahtlosen Stationen; Graphen, die Last, Verkehr, etc .; und vieles mehr.

### 6.1 Übersicht

Übersicht Abschnitt enthält verschiedene zusammenfassende Informationen.

 **TELTONIKA**
Status ▾ Network ▾ Services ▾ System ▾
Logout ▾

### Overview

<b>System</b>  		7.0% CPU load 		<b>Mobile</b>  		-79 dBm 	
Router uptime	0d 2h 21m 28s (since 2015-05-11, 11:35:24)			Data connection	Disconnected		
Local device time	2015-05-11, 13:56:52			State	Registered (home); LT BITE GSM; 3G (WCDMA)		
Free memory	87 MB (70%) RAM 	0.9 MB (75%) FLASH 		SIM card slot in use	SIM 1 (Ready)		
Firmware version	RUT9XX_R_00.01.290			Bytes received/sent *	2.7 KB / 3.1 KB		
<b>Wireless</b>  				ON 			
SSID	Teltonika_Router (AP)			<b>WAN</b>  			
Mode	1- AP; 11 CH (2.462 GHz)			Wired 			
<b>Local Network</b>  				<b>Access Control</b>  			
IP / netmask	192.168.1.1/255.255.255.0			LAN	SSH;HTTP;HTTPS;		
Clients connected	0			WAN	HTTP;		
<b>Recent System Events</b>  				<b>Recent Network Events</b>  			
1	2015-05-11, 13:52:14 - Port: Wired WAN connection operational			1	2015-05-11, 13:51:07 - Mobile data disconnected		
2	2015-05-11, 13:51:09 - Config: Network configuration has been ...			2	2015-05-11, 11:36:17 - Mobile data connected, IP: 10.1.12.123 ...		
3	2015-05-11, 11:56:27 - Config: Access Control configuration ha ...			3	2015-03-18, 16:32:14 - Joined 3G (WCDMA)		
4	2015-05-11, 11:56:27 - Config: Firewall configuration has been ...			4	2015-03-18, 16:04:26 - Joined 3G (WCDMA)		

\* Your carrier's data usage accounting may differ. Teltonika is not liable should any accounting discrepancies occur.

## 6.2 Systeminformationen

Die Systeminformationen Registerkarte enthält Daten, dass bezieht sich auf die Router-Betriebssystem.

System Information	
<b>System</b>	
Router name	Teltonika
Host name	Teltonika
Router model	Teltonika RUT9XX
Firmware version	RUT9XX_T_00.00.372
Kernel version	3.10.36
Local device time	2014-11-03, 14:29:09
Uptime	0h 35m 56s (since 2014-11-03, 13:53:13)
Load average	1 min: 10%; 5 mins: 18%; 15 mins: 17%
Temperature	-
<b>Memory</b>	
Free	94556 kB / 126452 kB (74%)
Cached	10828 kB / 126452 kB (8%)
Buffered	4308 kB / 126452 kB (3%)

Field Name	Sample value	Explanation
1. Router Name	Teltonika	Name des Routers (Hostname des Routersystems). Kann unter System -> Administration geändert werden.
2. Host name	Teltonika	Gibt an, wie der Router von anderen Geräten im Netzwerk gesehen wird. Kann unter System -> Administration geändert werden.
3. Router Model	Teltonika RUT9xx	Routers model.
4. Firmware Version	RUT9XX_T_00.00.372	Zeigt die Version der Firmware an, die aktuell in den Router geladen ist. Neuere Versionen können verfügbar werden, wenn neue Funktionen hinzugefügt werden. Verwenden Sie dieses Feld, um zu entscheiden, ob Sie eine Firmware installieren.
5. Kernel Version	3.10.36	Die Version des Linux-Kernels, die derzeit auf dem Computer läuft.
6. Local Time	2014-11-03, 14:33:14	Zeigt die aktuelle Systemzeit an. Kann sich von Ihrem Computer unterscheiden, da der Router die Zeit mit einem NTP synchronisiert. server.Format [year-month-day, hours:minutes:seconds].
7. Uptime	0h 40m 46s (since 2014-11-03, 13:53:13)	Gibt an, wie lange es her ist, seit der Router hochgefahren ist. Reboots setzen diesen Timer auf 0.Format[Stunden Minuten Sekunden des Tages (seit Jahr-Monatstag, Stunden: Minuten: Sekunden)] zurück.
8. Load Average	1 min: 11%; 5 mins: 18%; 15 mins: 17%	Zeigt an, wie beschäftigt der Router ist. Lassen Sie uns einige Beispielausgaben betrachten: "1 Minute: 11%, 5 Minuten: 18%, 15 Minuten: 17%". Die erste Zahl bedeutet, dass in der letzten Minute durchschnittlich 11% der Prozesse laufen oder auf eine Ressource warten.
9. Temperature		Gerätetemperatur

**Speicher Erklärung:**

Field Name	Sample Value	Explanation
1. Free	94532 kB / 126452 kB (74%)	Die Menge an Speicher, die vollständig frei ist. Sollte dies schnell abnehmen oder nahe an 0 herankommen, würde dies darauf hindeuten, dass der Router keinen Speicher mehr hat, was zu Abstürzen und unerwarteten Neustarts führen könnte.
2. Cached	10828 kB / 126452 kB (8%)	Die Größe des Speicherbereichs, der für die Speicherung häufig abgerufener Daten vorgesehen ist.
3. Buffered	4308 kB / 126452 kB (3%)	Die Größe des Bereichs, in dem die Daten zwischengespeichert werden, bevor sie an einen anderen Ort verschoben werden.

**6.3 Network Information****6.3.1.1 Mobil**

Zeigt Informationen aboutmobile Modemanschluss.

The screenshot displays the 'Mobile Information' section of a network management interface. It includes a navigation bar with tabs for WAN, LAN, Wireless, OpenVPN, VRRP, Topology, and Access. The main content area shows a 'Mobile' status indicator and a table of network parameters. A 'SIM card slot in use: SIM 1' is noted in the top right. At the bottom, there are 'Reset modem' and 'Refresh' buttons.

Field	Sample Value	Explanation
Data connection state	Connected	Status der mobilen Datenverbindung
IMEI	860461024164561	IMEI-Nummer des Modems (International Mobile Equipment Identity)
IMSI	246020100070220	IMSI (International Mobile Subscriber Identity) wird zur Identifizierung des Benutzers in einem Mobilfunknetz verwendet.
Sim card state	Ready	Zeigt den Status der SIM-Karte an, z.B. PIN erforderlich, Nicht eingelegt, etc.
Signal strength	-65 dBm	
Cell ID	FD90B	
RSRP	-88 dBm	
RSRQ	-7 dBm	
SINR	-21.4 dBm	
Operator	LT BITE GSM	
Operator state	Registered (home)	
Connection type	4G (LTE)	
Bytes received *	3.3 KB (3345 bytes)	
Bytes sent *	3.4 KB (3487 bytes)	

**Mobile information:**

Field	Sample Value	Explanation
1. Data connection state	Connected	Status der mobilen Datenverbindung
2. IMEI	860461024164561	IMEI-Nummer des Modems (International Mobile Equipment Identity)
3. IMSI	246020100070220	IMSI (International Mobile Subscriber Identity) wird zur Identifizierung des Benutzers in einem Mobilfunknetz verwendet.
4. SIM card	Ready	Zeigt den Status der SIM-Karte an, z.B. PIN erforderlich, Nicht eingelegt, etc.

5.	Signal strengt	-65dBm	Anzeige der empfangenen Signalstärke (RSSI). Signalstärke gemessen in dBm
6.	Cell ID	FD90B	ID der Bedienerzelle, mit der das Gerät aktuell verbunden ist.
7.	RSRP	-88dBm	Zeigt die empfangene Leistung des Referenzsignals an.
8.	RSRQ	-7dBm	Zeigt die Qualität des empfangenen Referenzsignals an.
9.	SINR	-21.4dBm	Zeigt den Signal-Störrauschabstand an.
10.	Operator state	LT BITE GSM	Name des Betreibers des angeschlossenen GSM-Netzes
11.	Operator	Registered (home)	Status des GSM-Netzes
12.	Connection type	4G (LTE)	Zeigt die Zugangstechnologie des GSM-Netzes an.
13.	Bytes receive	3.3 Kb (3345 bytes)	Wie viele Bytes wurden über eine mobile Datenverbindung empfangen?
14.	Bytes sent	3.4 kb (3487 bytes)	Wie viele Bytes wurden über eine mobile Datenverbindung gesendet?

### 6.3.1.2 WAN

Zeigt Informationen about WAN Verbindung.


**Mobile** | **WAN** | LAN | Wireless | OpenVPN | VRRP | Topology | Access

**WAN Information**

**WAN**

Interface	Wired
Type	Static
IP address	192.168.99.69
WAN MAC	00:1E:42:00:00:01
Netmask	255.255.255.0
Gateway	192.168.99.254
DNS 1	8.8.8.8
Connected	1h 45m 27s

**Ports**



The image shows the rear panel of a router with four ports labeled LAN1, LAN2, LAN3, and WAN. There is also a power button labeled PWR and a signal strength indicator.

#### WAN-Informationen:

	Field Name	Sample Value	Explanation
1.	Interface	Wired	Gibt an, über welches Medium sich der Router mit dem Internet verbindet. Dies kann entweder drahtgebunden, mobil oder Wi-Fi sein.
2.	Type	Static	Gibt die Art der Verbindung an. Dies kann entweder statisch oder DHCP sein.
3.	IP address	192.168.99.69	Die IP-Adresse, die der Router verwendet, um eine Verbindung zum Internet
4.	WAN MAC	00:1E:42:00:00:01	MAC-Adresse (Media Access Control), die für die Kommunikation in einem Ethernet verwendet wird.


5.	Netmask*	255.255.255.0	Gibt eine Maske an, mit der definiert wird, wie groß das WAN-Netzwerk ist.
6.	Gateway*	192.168.99.254	Zeigt das Standard-Gateway an, eine Adresse, an die der für das Internet bestimmte Datenverkehr weitergeleitet wird.
7.	DNS*	8.8.8.8	Domain Name Server(s).
8.	Connected*	1h 45m 27s	Wie lange die Verbindung erfolgreich aufrecht erhalten wurde.

\* -Diese Felder zeigen auf andere Anschlussarten auf.

\*\* - Exklusiv für andere Modi mit DHCP.

### 6.3.1.3 LAN

Zeigt Informationen about LAN Verbindung.

Mobile	WAN	LAN	Wireless	OpenVPN	VRRP	Topology	Access
<b>LAN Information</b>							
LAN Information							
Name	IP address	Netmask	Ethernet MAC address	Connected for			
Lan	192.168.99.218	255.255.255.0	00:1E:42:00:00:00	1h 53m 56s			
DHCP Leases							
Hostname	IP address	LAN name	MAC address	Lease time remaining			
?	192.168.99.120	Lan	D4:85:64:65:2B:D4	10h 11m 13s			
Ports							
							

#### LAN Informationen:

Field Name	Sample Value	Explanation
1. Name	Lan	Lan-Instanzname
2. IP address	192.168.99.218	Adresse, die der Router im LAN-Netzwerk verwendet.
3. Netmask	255.255.255.0	Eine Maske, mit der definiert wird, wie groß das LAN-Netzwerk ist.
4. Ethernet LAN MAC	00:1E:42:00:00:00	MAC-Adresse (Media Access Control), die für die Kommunikation in einem Ethernet verwendet wird.
5. Connected for	1h 53m 56s	LAN (Lokales Netzwerk)

#### DHCP-Leases

Wenn Sie einen DHCP-Server dieses Feld aktiviert haben wird zeigen, wie viele Geräte haben eine IP-Adresse erhalten und was diese IP-Adressen sind.

Field Name	Sample Value	Explanation
1. Hostname	?	Der Hostname des DHCP-Clients.
2. IP address	192.168.99.120	Jede Leasing-Erklärung enthält eine einzelne IP-Adresse, die an den Client vermietet wurde.

3.	Lan name	Lan	Lan-Instanzname
4.	MAC address	D4:85:64:65:2B:D4	Die MAC-Adresse (Media Access Control) der Netzwerkschnittstelle, auf der der Leasingvertrag verwendet wird. MAC wird als eine Reihe von hexadezimalen Oktetts angegeben, die durch Doppelpunkte getrennt sind.
5.	Lease time	10h 11m 13s	Restmietzeit für an Kunden ausgehändigte Adressen

### 6.3.1.4 Wireless

Wireless kann in zwei Modi arbeiten, Access Point (AP) oder Station (STA). AP ist, wenn das drahtlose Funkgerät verwendet wird, einen Access Point erstellen, dass andere Geräte angeschlossen werden können. STA ist, wenn das Radio zu einem Access Point verbinden ist über WAN.

#### 6.3.1.4.1 Station

Zeigt Informationen über eine drahtlose Verbindung (Stationsmodus).

Wireless Information						
<b>Wireless Information</b>						
Channel	1 (2.41 GHz)					
Country code	00 (World)					
<b>Wireless Status</b>						
SSID	Mode	Encryption	Wireless MAC	Signal quality	Bit rate	
Teltonika_Router	Station (STA)	no encryption	00:1E:42:10:80:22	61%	43.3 MBit/s	
Teltonika_Router_Test	Access Point (AP)	no encryption	02:1E:42:00:11:03	79%	1.0 MBit/s	
<b>Associated Stations</b>						
MAC Address	Device Name	Signal	RX Rate	TX Rate		
00:1E:42:10:80:22	?	-67 dBm	1.0 Mbit/s, MCS 0, 20MHz	43.3 Mbit/s, MCS 10, 20MHz		

#### Client mode information

Field Name	Sample Value	Explanation
1. Channel	1 (2.41 GHz)	Der Kanal, den der AP, an den die Router angeschlossen sind, verwendet. Ihr drahtloses Funkgerät ist gezwungen, in diesem Kanal zu arbeiten, um die Verbindung aufrechtzuerhalten.
2. Country	00	Ländercode.
3. SSID	Teltonika_Router	Die SSID, die der AP, mit dem die Router verbunden sind, verwendet.
4. Mode	Station (STA)	Verbindungsmodus - Client zeigt an, dass der Router ein Client für einen lokalen AP ist.
5. Encryption	WPA2 PSK (CCMP)	Der AP, an den der Router angeschlossen ist, bestimmt die Art der Verschlüsselung.
6. Wireless MAC	00:1E:42:10:80:22	Die MAC-Adresse des Funkgeräts der Zugangspunkte.
7. Signal Quality	61%	Die Qualität zwischen Routern Radio und einem anderen Gerät, das ist


Verbinden mit dem Router. Zeigt 0% an, wenn keine Geräte versuchen, eine Verbindung herzustellen oder gerade eine Verbindung aufrecht erhalten.

8. Bit rate 43.3 MBit/s

Der physikalisch maximal mögliche Durchsatz, den der Router-Funk bewältigen kann. Beachten Sie, dass dieser Wert kumulativ ist - Die Bitrate wird zwischen dem Router und anderen möglichen Geräten, die sich mit dem lokalen AP verbinden, geteilt.

### 6.3.1.4.2 Access Point

Zeigt Informationen über eine drahtlose Verbindung (Access Point-Modus).

Mobile	WAN	LAN	Wireless	OpenVPN	VRRP	Topology	Access
<b>Wireless Information</b>							
<b>Wireless Information</b>							
Channel		11 (2.46 GHz)					
Country code		00 (World)					
<b>Wireless Status</b>							
<b>SSID</b>	<b>Mode</b>	<b>Encryption</b>	<b>Wireless MAC</b>	<b>Signal quality</b>	<b>Bit rate</b>		
Teltonika_Router_Test	Access Point (AP)	no encryption	00:1E:42:00:11:03	80%	54.0 MBit/s		
<b>Associated Stations</b>							
<b>MAC Address</b>	<b>Device Name</b>	<b>Signal</b>	<b>RX Rate</b>	<b>TX Rate</b>			
FC:C2:DE:91:36:A6	android-9aed2b2077a54c74	-54 dBm	24.0 Mbit/s, MCS 0, 20MHz	54.0 Mbit/s, MCS 0, 20MHz			
Refresh 							

### Wireless AP Informationen

Field Name	Sample Value	Explanation
1. Channel	11 (2.46 GHz)	Der Kanal, der zur Übertragung der SSID und zum Aufbau neuer Verbindungen zu Geräten verwendet wird.
2. Country code	00(World)	Ländercode.
3. SSID	Teltonika_Router_Test	Die SSID, die gerade gesendet wird. Andere Geräte werden dies sehen und können sich mit Ihrem drahtlosen Netzwerk verbinden.
4. Mode	Access Point (AP)	Verbindungsmodus - Der Master zeigt an, dass Ihr Router ein Zugangspunkt ist.
5. Encryption	No Encryption	Die Art der Verschlüsselung, mit der der Router eine Verbindung authentifiziert, aufbaut und aufrechterhält.
6. Wireless MAC	00:1E:42:00:00:03	MAC-Adresse Ihres drahtlosen Radios.
7. Signal Quality	80%	Die Qualität zwischen Routern Radio und einem anderen Gerät, das sich mit dem Router verbindet. Zeigt 0% an, wenn keine Geräte versuchen, eine Verbindung herzustellen oder gerade eine Verbindung aufrecht erhalten.
8. Bit rate	54.0 MBit/s	Die Bitrate wird zwischen allen Geräten geteilt, die sich mit dem drahtlosen Netzwerk des Routers verbinden.



Zusätzlicher Hinweis: MBit / s zeigt die Bits nicht Bytes. Um den Durchsatz in Bytes, die den Bit-Wert von 8 unterteilt, für

zB 54Mbits / s würde 6.75MB / s (Megabytes pro Sekunde) sein.

### 6.3.1.5 Assoziierte Stationen

Gibt eine Liste aller Geräte und die MAC-Adressen, die eine Verbindung mit dem Router jetzt halten sind. Dies kann entweder die Informationen des Access Points sein, dass der Router in STAmode verbindet oder eine Liste aller

Geräte, die mit dem Router-Modus in AP verbinden:

Field Name	Sample Value	Explanation
1. MAC Address	FC:C2:DE:91:36:A6	MAC-Adresse (Media Access Control) der zugehörigen Station
2. Device Name	Android- 9aed2b2077a54c74	Der Hostname des DHCP-Clients.
3. Signal	-54dBm	Anzeige der empfangenen Signalstärke (RSSI). Signalstärke gemessen in dBm
4. RX Rate	24.0Mbit/s, MCS 0, 20MHz	Die Rate, mit der Pakete von der zugehörigen Station empfangen werden.
5. TX Rate	54.0Mbit/s, MCS 0, 20MHz	Die Geschwindigkeit, mit der Pakete an die zugehörige Station gesendet werden.

### 6.3.1.6 OpenVPN Client (muss aktualisiert werden)

Zeigt OpenVPN Client-Seite Informationen.

Field Name	Sample Value	Explanation
Status	Enabled	OpenVPN-Status
Type	Client	Ein Typ einer OpenVPN-Instanz, der erstellt wurde.
IP	172.16.1.6	IP-Adresse des entfernten virtuellen Netzwerks
Mask	255.255.255.255	Subnetzmaske des entfernten virtuellen Netzwerks
Server IP	172.16.1.0	IP-Adresse des entfernten virtuellen Servers
Time	0h 48m 43s	Wie lange ist die Verbindung aufgebaut?

Field Name	Sample Value	Explanation
1. Status	Enabled	OpenVPN-Status
2. Type	Client	Ein Typ einer OpenVPN-Instanz, der erstellt wurde.
3. IP	172.16.1.6	IP-Adresse des entfernten virtuellen Netzwerks
4. Mask	255.255.255.255	Subnetzmaske des entfernten virtuellen Netzwerks
5. Server IP	172.16.1.0	IP-Adresse des entfernten virtuellen Servers
6. Time	0h 48m 43s	Wie lange ist die Verbindung aufgebaut?

### 6.3.1.7 OpenVPN Server

Zeigt OpenVPN Server-Seite Informationen.

Mobile	WAN	LAN	Wireless	OpenVPN	VRRP	Topology	Access
<b>OpenVPN Information</b>							
Server_Server							
<b>OpenVPN</b>							
Status	Enabled						
Type	Server						
IP	172.16.1.1						
Mask	255.255.255.255						
Time	20h 13m 9s						
<b>Clients Information</b>							
<b>Common Name</b>	<b>Real Address</b>	<b>Virtual Address</b>	<b>Connection Since</b>				
Client1	192.168.99.91:50850	172.16.1.6	2015-05-15 08:07:15				

Field Name	Sample Value	Explanation
1. Status	Enabled	OpenVPN-Status
2. Type	Server	Ein Typ einer OpenVPN-Instanz, der erstellt wurde.
3. IP	172.16.1.1	IP-Adresse des entfernten virtuellen Netzwerks
4. Mask	255.255.255.255	Subnetzmaske des entfernten virtuellen Netzwerks
5. Time	20h 13m 9s	Wie lange ist die Verbindung aufgebaut?

### 6.3.1.8 Client-Informationen

Field Name	Sample Value	Explanation
1. Common Name	Client1	Kundenverbindung
2. Real Address	192.168.99.91:50850	IP-Adresse und Portnummer des Kunden
3. Virtual Address	172.16.1.6	Virtuelle Adresse, die an einen Kunden weitergegeben wurde.
4. Connection Since	2015-05-15 08:07:15	Seit wann ist die Verbindung hergestellt?

### 6.3.1.9 VRRP


VRRP (Virtual Router Redundancy Protocol) für LAN

Mobile WAN LAN Wireless OpenVPN **VRRP** Topology Access

**VRRP Information**

**VRRP LAN Status**

Status	Enabled
Virtual ip	192.168.1.253
Priority	100
Router	Master

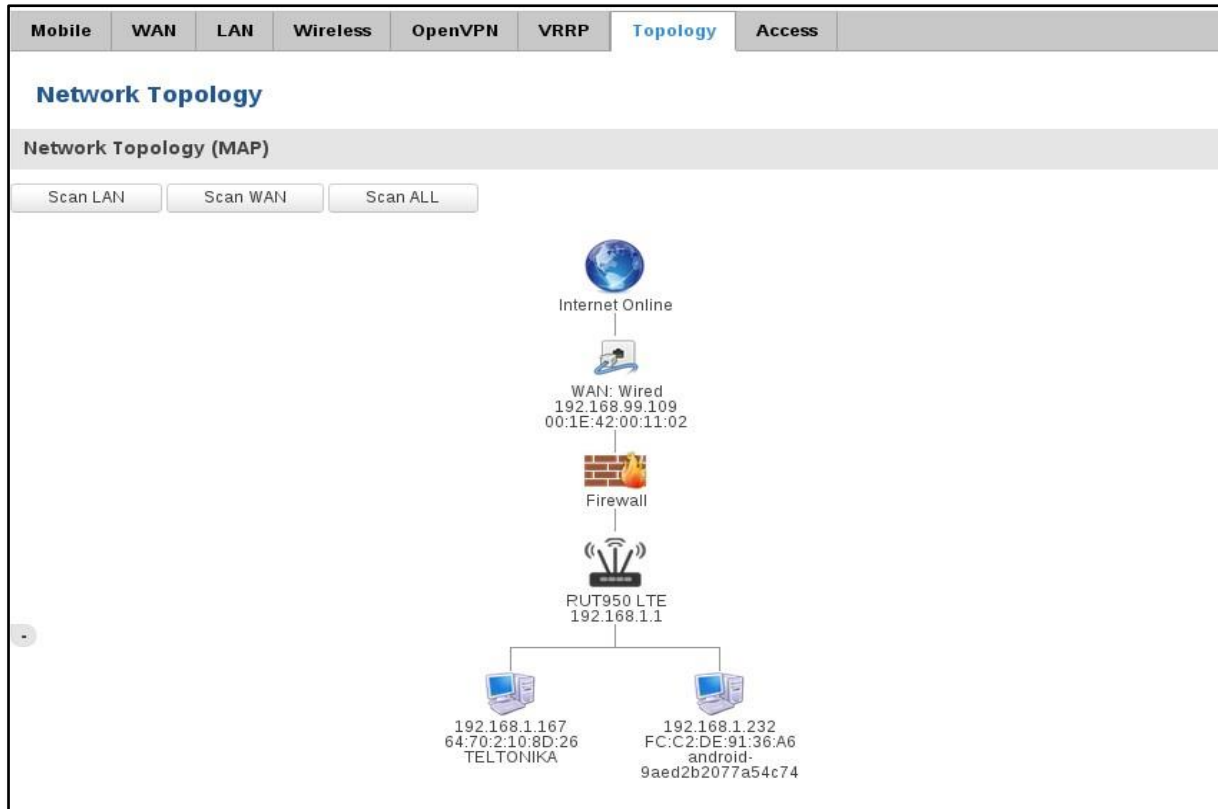
Refresh 

Field Name	Sample Value	Explanation
1. Status	Enabled	VRRP-Status
2. Virtual IP	192.168.1.253	Virtuelle IP-Adresse(n) für LAN's VRRP (Virtual Router Redundancy)
3. Priority	100	Protokoll) Cluster
4. Router**	Master	Router mit höchstem Prioritätswert auf dem gleichen VRRP (Virtual

\*\* - Exklusiv für andere Modi mit Slave.


### 6.3.1.10 Topologie

Netzwerk-Scanner ermöglicht es Ihnen, schnell Informationen über die Netzwerk-Geräte abzurufen.



### 6.3.1.11 Zugang

Zeigt Informationen aboutlocal und Remote-aktiven Verbindungen Status.


Mobile	WAN	LAN	Wireless	OpenVPN	VRRP	Topology	Access
<b>Access Status</b>							
<b>Access information</b>		<b>Last Connections</b>					
<b>Local Access</b>							
Type	Status	Port	Active Connections				
SSH	Enabled	22	0 ( 0.00 B )				
HTTP	Enabled	80	1 ( 9.26 KB )				
HTTPS	Enabled	443	0 ( 0.00 B )				
<b>Remote Access</b>							
Type	Status	Port	Active Connections				
SSH	Disabled	22	0 ( 0.00 B )				
HTTP	Disabled	80	0 ( 0.00 B )				
HTTPS	Enabled	443	6 ( 558.12 KB )				
Refresh 							

Field Name	Sample Value	Explanation
1. Type	SSH;HTTP;HTTPS	Art des Verbindungsprotokolls
2. Status	Disabled/Enabled	Verbindungsstatus
3. Port	22; 80; 443	Verwendete Verbindungsschnittstelle
4. Active Connections	0(0.00B);1(9.26 KB); 6(558.12 KB)	Anzahl der aktiven Verbindungen und übertragene Datenmenge in KB

\*\* - Exklusiv für andere Modi mit Slave.

### 6.3.1.11.1 Letzte Anschlüsse

Zeigt Informationen aboutlocal und Fern letzten 3 Verbindungsstatus

Access Status			
Access information		Last Connections	
<b>Last Local Connections</b>			
Type	Date	IP	Authentications Status
SSH	2015-05-11, 10:36:59	192.168.1.167	Succeeded
	2015-05-11, 10:37:54	192.168.1.167	Succeeded
	2015-05-11, 10:38:41	192.168.1.167	Succeeded
HTTP	2015-03-18, 15:56:44	192.168.1.167	Succeeded
	2015-03-18, 16:31:47	192.168.1.167	Succeeded
	2015-05-11, 11:36:23	192.168.1.167	Succeeded
HTTPS	2015-05-07, 09:07:22	192.168.1.167	Succeeded
	2015-05-08, 10:48:52	192.168.1.167	Succeeded
	2015-05-08, 13:39:11	192.168.1.167	Succeeded
<b>Last Remote Connections</b>			
Type	Date	IP	Authentications Status
SSH	2015-05-07, 10:36:01	192.168.99.109	Failed
	2015-05-07, 10:36:13	192.168.99.109	Failed
	2015-05-07, 10:36:16	192.168.99.109	Succeeded
HTTP	2015-05-07, 09:07:17	192.168.99.109	Succeeded
	2015-05-08, 08:44:13	192.168.99.109	Succeeded
	2015-05-08, 09:45:21	192.168.99.109	Succeeded
HTTPS	<i>There are no records yet.</i>		
			Refresh 

Field Name	Sample Value	Explanation
1. Type	SSH;HTTP;HTTPS	Art des Verbindungsprotokolls
2. Date	2015-05-11, 10:36:59	Datum und Uhrzeit der Verbindung
3. IP	192.168.1.167	IP-Adresse, von der aus die Verbindung hergestellt wurde
4. Authentications Status	Failed; Succeeded	Status des Authentifizierungsversuchs

## 6.4 Geräte-Informationen

Die Seite zeigt Fabrik Informationen, die in das Gerät während des Herstellungsprozesses geschrieben wurden.


Device Information	
<b>Device</b>	
Serial number	02345678
Product code	RUT900101010
Batch number	0222
Hardware revision	0321
IMEI	860461024164561
IMSI	246020100070220
Ethernet LAN MAC address	3E:83:6F:84:E1:A4
Ethernet WAN MAC address	AE:F4:F3:5B:9D:CC
Wireless MAC address	N/A
<b>Modem</b>	
Model	ME909u-521
FW version	11.235.07.00.00

Field Name	Sample Value	Explanation
1. Serial number	02345678	Seriennummer des Gerätes
2. Product code	RUT955101010	Produktcode des Gerätes
3. Batch number	0222	Chargennummer, die während des Herstellungsprozesses des
4. Hardware revision	0321	Hardware-Revision des Gerätes
5. IMEI	860461024164561	Identifikationsnummer des internen Modems
6. IMSI	246020100070220	Teilnehmeridentifikationsnummer des internen Modems
6. Ethernet LAN MAC	3E:83:6F:84:E1:A4	MAC-Adresse der Ethernet-LAN-Ports
7. Ethernet WAN MAC	AE:F4:F3:5B:9D:CC	MAC-Adresse des Ethernet-WAN-Ports
8. Wireless MAC	N/A	MAC-Adresse der Wi-Fi-Schnittstelle
9. Model	ME909-521	Modemmodell des Routers
10. FW version	11.235.07.00.00	Version der Modem-Firmware des Routers

## 6.5 Dienstleistungen

Die Seite zeigt die Nutzung der verfügbaren Dienste.

Services			
Services Status			
VRRP LAN	Disabled	DDNS	Disabled
OpenVPN servers	Disabled	Site blocking	Disabled
OpenVPN clients	Disabled	Privoxy	Enabled
SNMP agent	Disabled	SMS utils rules	Enabled
SNMP trap	Disabled	Hotspot	Disabled
NTP client	Enabled	Hotspot logging	Disabled
IPsec	Disabled	GRE tunnel	Disabled
Ping reboot	Disabled	QoS	Disabled

[Refresh](#) 

## 6.6 Routen

Die Seite zeigt ARP-Tabelle aktive IP-Routen des Gerätes.

### 6.6.1 ARP

Zeigt die Router aktiv ARP-Tabelle. Eine ARP-Tabelle enthält Adressen von jedem unmittelbaren kürzlich MAC zwischengespeichert

Vorrichtung, die mit dem Router wurde in Verbindung steht.

ARP		
IP Address	MAC Address	Interface
10.0.207.217	02:50:F3:00:00:00	eth2
192.168.99.17	00:25:22:D7:CA:A7	br-lan
192.168.99.36	38:2C:4A:64:2D:E5	br-lan
192.168.99.155	00:00:00:00:00:00	br-lan

Field Name	Sample Value	Explanation
1. IP Address	192.168.99.17	Kürzlich eingezahlte IP-Adressen aller unmittelbaren Geräte, die mit dem Router kommunizierten.
2. MAC Address	00:25:22:D7:CA:A7	Kürzlich eingezahlte MAC-Adressen aller unmittelbaren Geräte, die mit dem Router kommunizierten.
3. Interface	br-lan	Für den Anschluss verwendete Schnittstelle



### 6.6.2 Aktive IP-Routen

Zeigt die Router-Routing-Tabelle. Die Routing-Tabelle zeigt an, wo ein TCP / IP-Paket mit einer bestimmten IP-Adresse, weitergeleitet werden soll.

Active IP Routes			
Network	Target	IP Gateway	Metric
ppp	0.0.0.0/0	10.0.207.217	0
ppp	10.0.207.216/29	0.0.0.0	0
ppp	10.0.207.217	0.0.0.0	0
lan	192.168.99.0/24	0.0.0.0	0

Field Name	Sample Value	Explanation
1. Network	ppp	Schnittstelle zur Übertragung von TCP/IP-Paketen durch
2. Target	192.168.99.0/24	Gibt an, wohin ein TCP/IP-Paket mit einer bestimmten IP-Adresse geleitet werden soll.
3. IP Gateway	0.0.0.0	Gibt an, über welches Gateway ein TCP/IP-Paket geleitet werden soll.
4. Metric	0	Metrische Zahl, die die Schnittstellenpriorität der Nutzung angibt.

### 6.6.3 Aktive IPv6-Routen

Zeigt aktive IPv6-Routen für Datenpaket transmission

Active IPv6-Routes			
Network	Target	IPv6-Gateway	Metric
loopback	0:0:0:0:0:0:0:0/0	0:0:0:0:0:0:0:0/0	FFFFFFFF
loopback	0:0:0:0:0:0:0:0/0	0:0:0:0:0:0:0:0/0	FFFFFFFF
loopback	0:0:0:0:0:0:0:1	0:0:0:0:0:0:0:0/0	00000000
ppp	FF00:0:0:0:0:0:0:0/8	0:0:0:0:0:0:0:0/0	00000100
loopback	0:0:0:0:0:0:0:0/0	0:0:0:0:0:0:0:0/0	FFFFFFFF

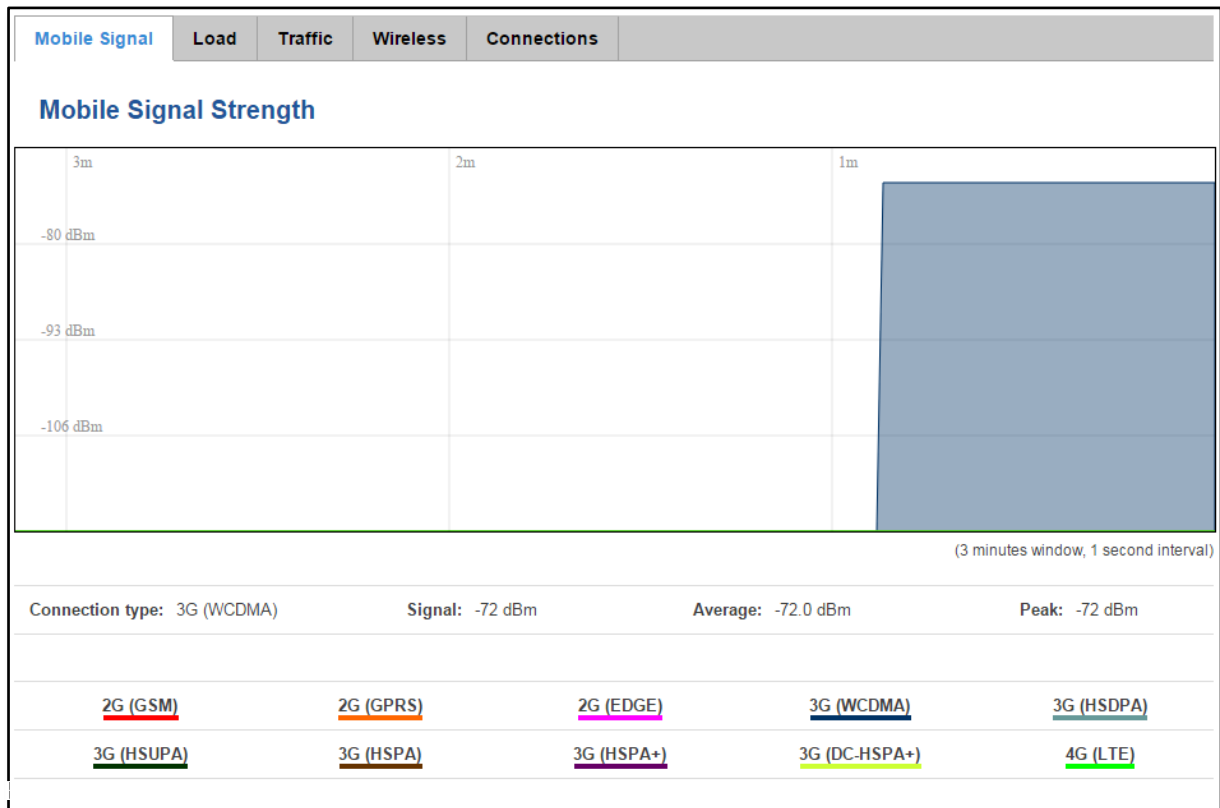
Field Name	Sample Value	Explanation
1. Network	loopback	Verwendete Netzwerkschnittstelle
2. Target	0:0:0:0:0:0:0:0/0	Gibt an, wohin ein TCP/IP-Paket mit einer bestimmten IP-Adresse geleitet werden soll.
3. IPv6-Gateway	0:0:0:0:0:0:0:0/0	Gibt an, über welches Gateway ein TCP/IP-Paket geleitet werden soll.
4. Metric	FFFFFFFF	Metrische Zahl, die die Schnittstellenpriorität der Nutzung angibt.

## 6.7 Echtzeit-Graphen

Echtzeit-Grafiken zeigen, wie verschiedene statistische Daten über die Zeit verändert.

### 6.7.1 Mobile Signal Strength

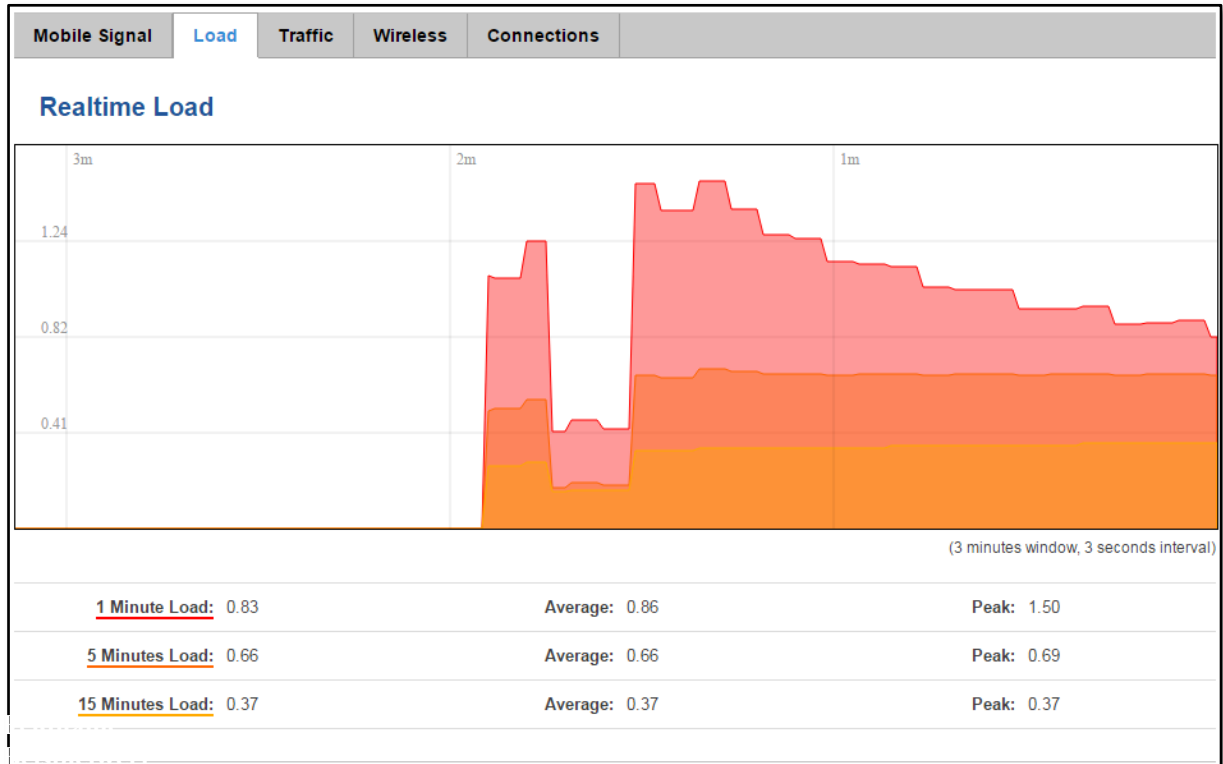
Displays mobile Signalstärke zeitliche Änderung (gemessen in dBm)



Field Name	Sample Value	Explanation
1. Connection type	3G (WCDMA)	Art der verwendeten Mobilfunkverbindung
2. Signal	-72 dBm	Aktueller Signalstärkewert
3. Average	-72.0 dBm	Durchschnittlicher Signalstärkewert
4. Peak	-72 dBm	Spitzenwert der Signalstärke

### 6.7.2 Realtime Load

Das Tri-Diagramm stellt die durchschnittlichen CPU-Lastwerte in Echtzeit. Der Graph besteht aus drei farbcodierten Graphen, jeder zu der durchschnittlichen CPU Last über 1 (rot), entsprechend, 5 (orange) und 15 (gelb) letzte Minuten.



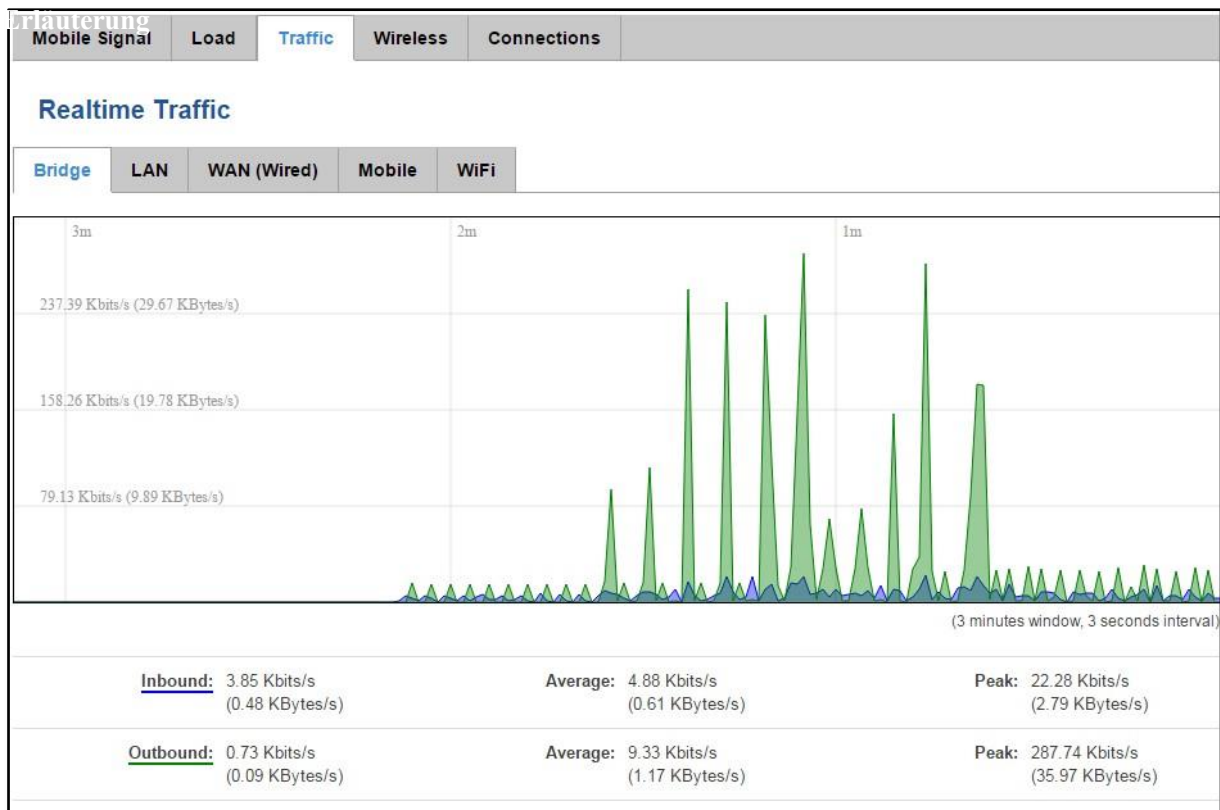
Field Name	Sample Value	Explanation
1. 1/5/15 Minutes Load	0.83	Zeitintervall für die Lastmittelwertbildung, Farbe des Diagramms
2. Average	0.86	Durchschnittlicher CPU-Lastwert über Zeitintervall (1/5/15)
3. Peak	1.50	Spitzenwert der CPU-Last des Zeitintervalls

### 6.7.3 Verkehr

Das Tri-Diagramm stellt die durchschnittliche Systemlast über den Verlauf von ~ 3 Minuten; jede neue Messung durchgeführt

alle 3 Sekunden. Der Graph besteht aus drei farbcodiert Graphen, von denen jeder auf die durchschnittliche System entspricht

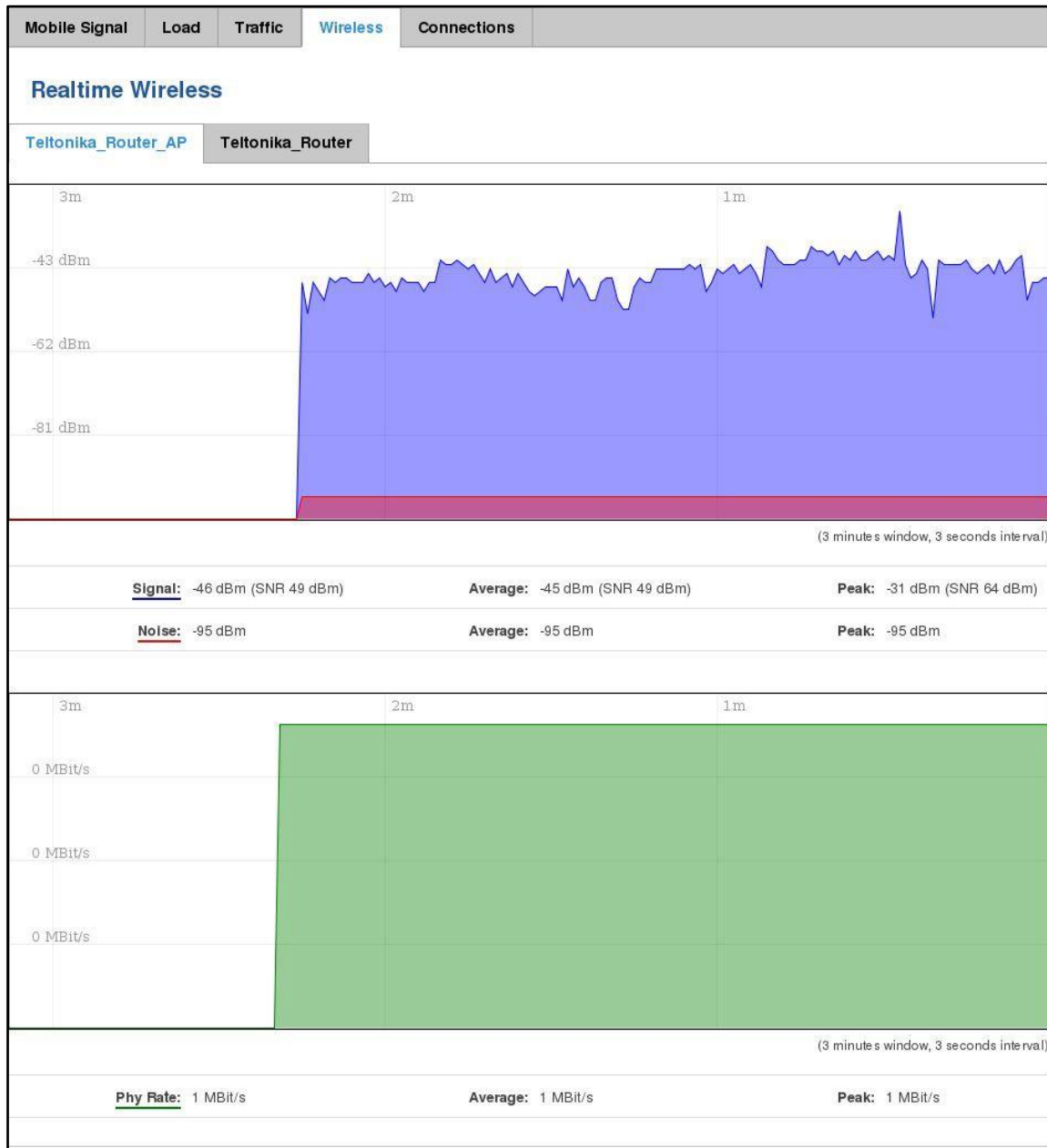
Last über 1 (rot), 5 (orange) und 15 (gelb) letzte Minuten. Obwohl nicht grafisch dargestellt, zeigt die Seite auch Spitzen Lasten über 1, 5 und 15 Minuten.



Field Name	Explanation
1. Bridge	Summendiagramm, das kabelgebundenes Ethernet-LAN und das drahtlose Netzwerk umfasst.
2. LAN	Grafische Darstellung des Gesamtverkehrs, der über beide LAN-Netzwerkschnittstellen fließt.
3. WAN (Wired)	Stellt die Menge des Datenverkehrs dar, der durch die aktuell aktive WAN-Verbindung geleitet wurde.
4. Mobile	Grafische Darstellung der Verkehrsmenge, die durch die Mobilfunkverbindung geleitet wurde.
5. Wi-Fi	Zeigt die Menge des Datenverkehrs an, der über das drahtlose Funkgerät gesendet und empfangen wurde.

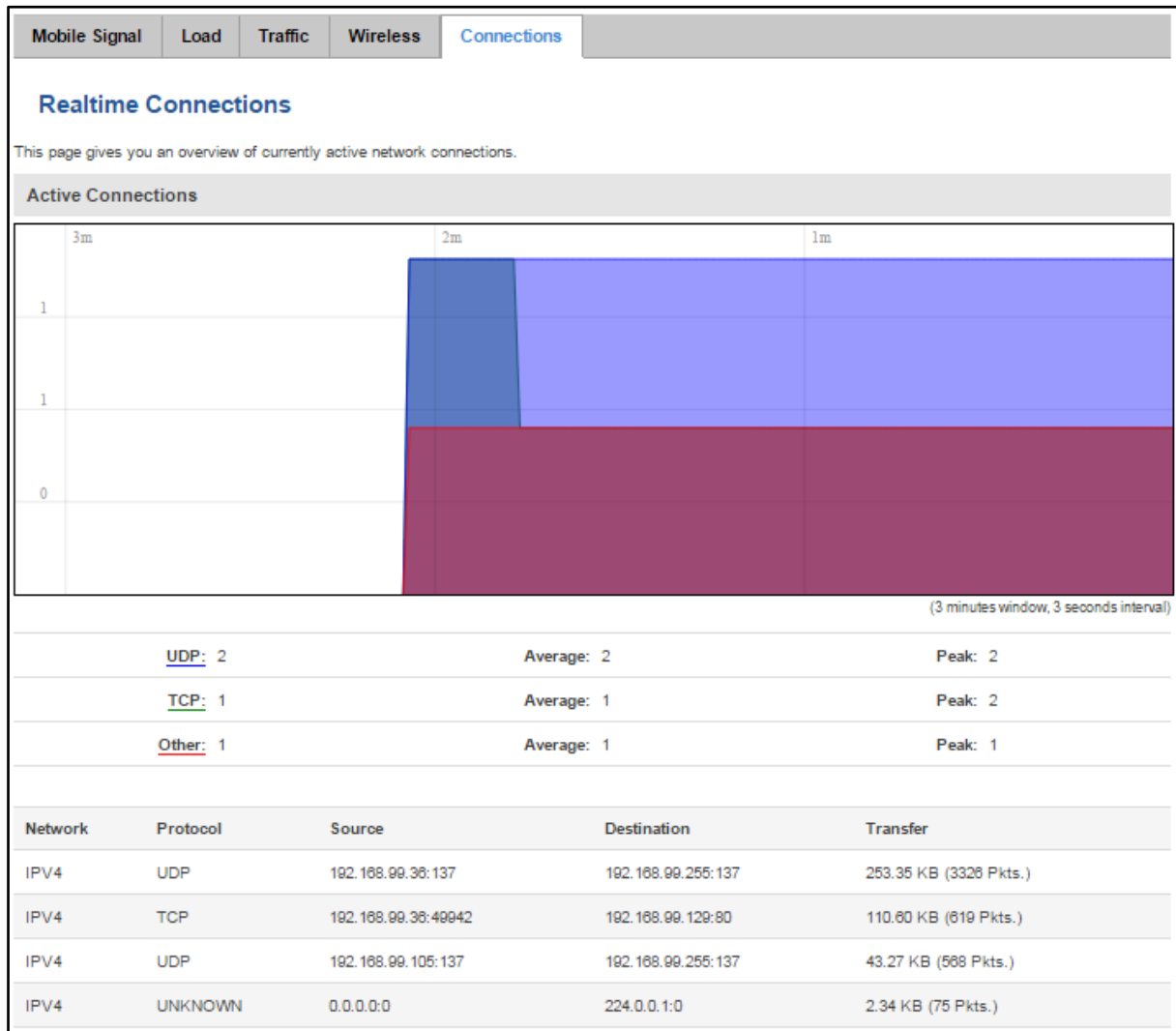
### 6.7.4 Realtime Wireless

Displaythe drahtloses Funksignal, Signalrauschen und theoretische maximale Kanaldurchlässigkeit. Durchschnitts- und Spitzen Signalpegel wird angezeigt.



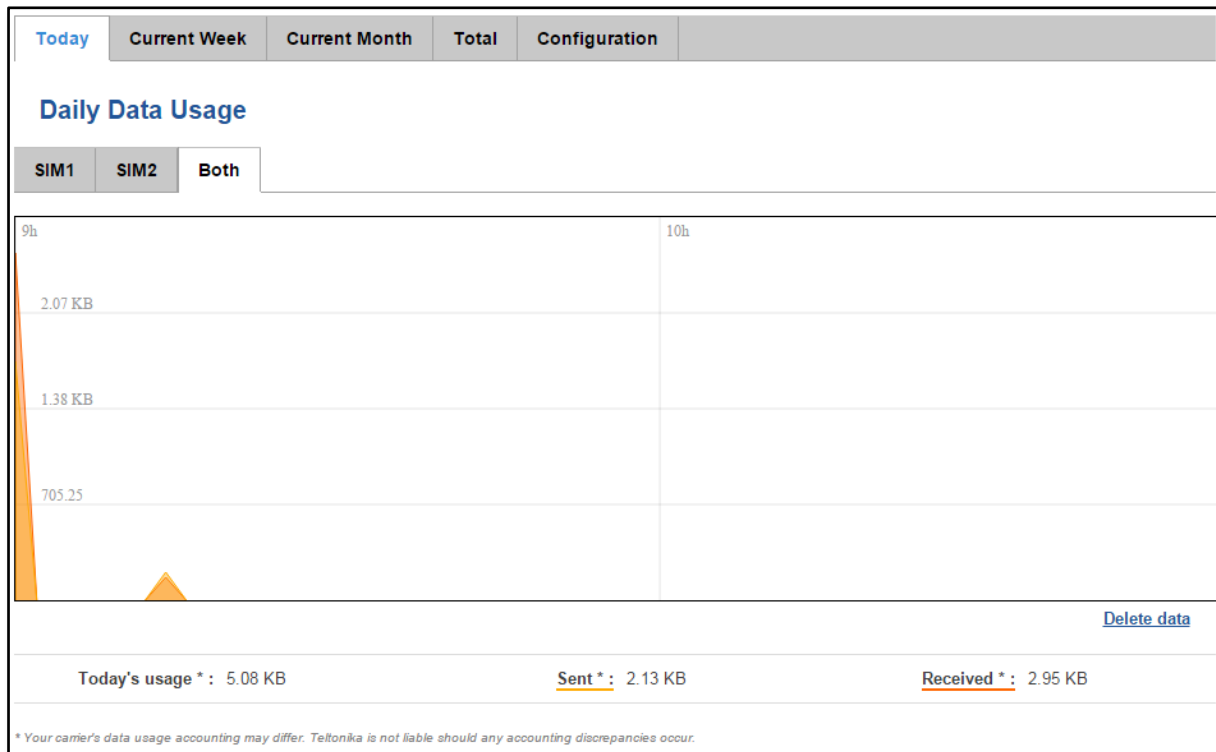
### 6.7.5 Echtzeit-Verbindungen

Zeigt die aktuell aktive Netzwerkverbindungen. Mit den Informationen über Netzwerk, Protokoll, Quell- und Ziel Adressen, Übertragungsgeschwindigkeit.



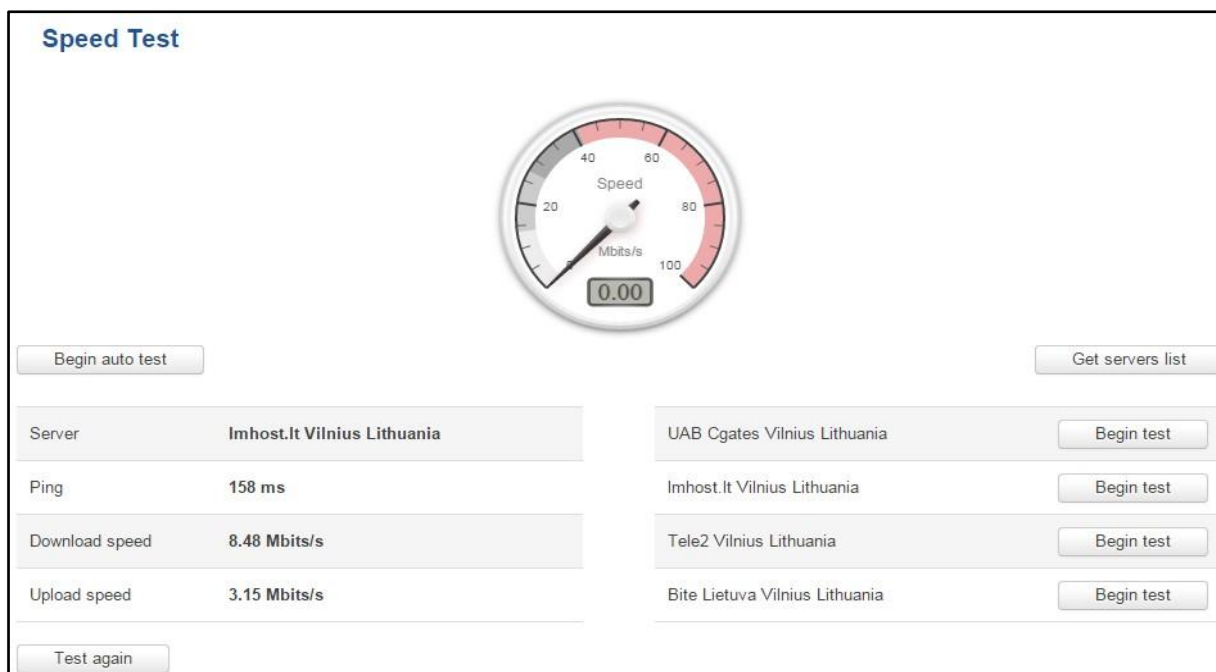
## 6.8 Mobile Verkehr

Zeigt mobile Verbindungsdaten gesendet und in KB an diesem Tag, Woche, Monat erhalten.



## 6.9 Speed Test

Speed-Test ist ein Werkzeug für Ihre Internetverbindung Upload- und Download-Geschwindigkeiten zu messen. Sie können Server auswählen zur manuellen Prüfung oder die Verwendung von Autotest.



## 6.10 Ereignisprotokoll

Ereignisprotokoll zeigt solche Aktionen wie: Login, Neustart, Firmware zu blinken und zurückgesetzt.

### 6.10.1 Alle Veranstaltungen

Zeigt alle Router Ereignisse, deren Art und Zeitpunkt des Auftretens.

All Events	System Events	Network Events	Events Reporting	Reporting Configuration
<b>Events Log</b>				
Events Log				
Events per page	10 ▼	Search		<input type="text"/>
ID ↕	Date ↕	Event type ↕	Event ↕	
3181S	2015-05-11, 16:11:47	Config	Firewall configuration has been changed	
3180S	2015-05-11, 16:09:29	Port	Wired WAN connection operational	
3179S	2015-05-11, 16:05:13	Port	Wired WAN connection non operational	
3178S	2015-05-11, 16:02:39	DHCP	Leased 192.168.1.232 IP address for client FC:C2:DE:91:36:A6 - android-9aed2b2077a54c74 in WiFi	
3177S	2015-05-11, 16:02:39	Port	Wired WAN connection operational	
3176S	2015-05-11, 16:02:38	DHCP	Leased 192.168.1.232 IP address for client FC:C2:DE:91:36:A6 - android-9aed2b2077a54c74 in WiFi	
3175S	2015-05-11, 16:02:37	DHCP	Leased 192.168.1.232 IP address for client FC:C2:DE:91:36:A6 - android-9aed2b2077a54c74 in WiFi	
3174S	2015-05-11, 16:02:36	DHCP	Leased 192.168.1.232 IP address for client FC:C2:DE:91:36:A6 - android-9aed2b2077a54c74 in WiFi	
3173S	2015-05-11, 16:02:36	DHCP	Leased 192.168.1.232 IP address for client FC:C2:DE:91:36:A6 - android-9aed2b2077a54c74 in WiFi	
3172S	2015-05-11, 16:02:35	DHCP	Leased 192.168.1.232 IP address for client FC:C2:DE:91:36:A6 - android-9aed2b2077a54c74 in WiFi	
Showing 1 to 10 of 1912 entries				<a href="#">Next &gt;&gt;</a>



### 6.10.2 Systemereignisse

Zeigt alle Systemereignisse, deren Art und Zeitpunkt des Auftretens. Ereignisse umfassen die Authentifizierung oder Neustartanforderungen, abgesicherten Modus, eingehende und ausgehende SMS und Anrufe, Konfigurationsänderungen, DHCP Ereignisse.

All Events
System Events
Network Events
Events Reporting
Reporting Configuration

### System Log

All
Authentication
Reboot
Safemode
SMS/Call
Configuration
DHCP

**Events Log**

Events per page 10 ▼ Search

ID <span style="font-size: 0.8em;">▲</span>	Date <span style="font-size: 0.8em;">▲</span>	Event type <span style="font-size: 0.8em;">▲</span>	Event <span style="font-size: 0.8em;">▲</span>
3181	2015-05-11, 16:11:47	Config	Firewall configuration has been changed
3180	2015-05-11, 16:09:29	Port	Wired WAN connection operational
3179	2015-05-11, 16:05:13	Port	Wired WAN connection non operational
3178	2015-05-11, 16:02:39	DHCP	Leased 192.168.1.232 IP address for client FC:C2:DE:91:36:A6 - android-9aed2b2077a54c74 in WiFi
3177	2015-05-11, 16:02:39	Port	Wired WAN connection operational
3176	2015-05-11, 16:02:38	DHCP	Leased 192.168.1.232 IP address for client FC:C2:DE:91:36:A6 - android-9aed2b2077a54c74 in WiFi
3175	2015-05-11, 16:02:37	DHCP	Leased 192.168.1.232 IP address for client FC:C2:DE:91:36:A6 - android-9aed2b2077a54c74 in WiFi
3174	2015-05-11, 16:02:36	DHCP	Leased 192.168.1.232 IP address for client FC:C2:DE:91:36:A6 - android-9aed2b2077a54c74 in WiFi
3173	2015-05-11, 16:02:36	DHCP	Leased 192.168.1.232 IP address for client FC:C2:DE:91:36:A6 - android-9aed2b2077a54c74 in WiFi
3172	2015-05-11, 16:02:35	DHCP	Leased 192.168.1.232 IP address for client FC:C2:DE:91:36:A6 - android-9aed2b2077a54c74 in WiFi

Showing 1 to 10 of 1600 entries
Next >>

### 6.10.3 Netzwerk Veranstaltungen

Zeigt Informationen über die jüngsten Ereignisse im Netzwerk wie Verbindungsstatus ändern, Leasing Statusänderung, Netzwerk Typ oder Betreiber ändern.

All Events	System Events	Network Events	Events Reporting	Reporting Configuration
<b>Connections Log</b>				
All	Wireless	Mobile Data	Network Type	Network Operator
<b>Connections Log</b>				
Events per page	10 ▼	Search		<input type="text"/>
ID ▲	Date ▲	Action ▲	Result ▲	
312	2015-05-11 15:48:49	WiFi	WiFi client connected: FC:C2:DE:91:36:A6 android-9aed2b2077a54c74	
311	2015-05-11 15:48:43	WiFi	WiFi client disconnected: FC:C2:DE:91:36:A6 android-9aed2b2077a54c74	
310	2015-05-11 15:48:37	WiFi	WiFi client connected: FC:C2:DE:91:36:A6 android-9aed2b2077a54c74	
309	2015-05-11 15:48:31	WiFi	WiFi client disconnected: 20:34:47:41:4B:45	
308	2015-05-11 15:36:56	WiFi	WiFi client connected: 20:34:47:41:4B:45	
307	2015-05-11 15:36:55	WiFi	WiFi client disconnected: 00:1E:42:10:80:22	
306	2015-05-11 15:30:32	WiFi	WiFi client connected: 00:1E:42:10:80:22	
305	2015-05-11 15:30:26	WiFi	WiFi client disconnected: 00:1E:42:10:80:22	
304	2015-05-11 15:19:58	WiFi	WiFi client connected: 00:1E:42:10:80:22	
303	2015-05-11 15:19:52	WiFi	WiFi client disconnected: FC:C2:DE:91:36:A6 android-9aed2b2077a54c74	
Showing 1 to 10 of 312 entries				<a href="#">Next &gt;&gt;</a>

### 6.10.4 Events Berichterstattung

Ermöglicht anzuzeigen, zu aktivieren, zu deaktivieren oder modifizieren erstellt Regeln für Ereignisse berichten.

All Events	System Events	Network Events	Events Reporting	Reporting Configuration
<b>Events Reporting</b>				
Create rules for events reporting.				
<b>Events Reporting Rules</b>				
Event type	Event subtype	Action	Enable	Sort
FW upgrade	From file	Send SMS	<input checked="" type="checkbox"/>	<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;">             ↑ ↓           </div> <div>Edit</div> <div>Delete</div> </div>
New DHCP client	Connected from LAN	Send SMS	<input checked="" type="checkbox"/>	<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;">             ↑ ↓           </div> <div>Edit</div> <div>Delete</div> </div>
Config change	All	Send SMS	<input type="checkbox"/>	<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;">             ↑ ↓           </div> <div>Edit</div> <div>Delete</div> </div>
<i>* All rules are executed in current list order.</i>				
<b>Events Reporting Configuration</b>				
Event type	Event subtype	Action		
Config change ▼	All ▼	Send SMS ▼	Add	

#### 6.10.4.1 Events Configuration Berichterstattung

Ermöglicht erstellt Regeln Details zu überprüfen und ändern sie, so nach dem Auftreten des Ereignisses, Nachrichten oder E-Mails zu senden angegebene Adresse oder Telefonnummern mit Informationen über die Veranstaltung.

All Events	System Events	Network Events	Events Reporting	Reporting Configuration
<b>Event Reporting Configuration</b>				
<b>Modify event reporting rule</b>				
Enable <input checked="" type="checkbox"/>				
Event type <span>Reboot ▼</span>				
Event subtype <span>After unexpected shut down ▼</span>				
Action <span>Send SMS ▼</span>				
Custom message <input type="checkbox"/>				
Recipient's phone number <input type="text" value="+123456789"/>				

Field Name	Sample Value	Explanation
1. Enable	Enable/Disable	Eine Regel aktiv/inaktiv setzen
2. Event type	Reboot	Wählen Sie den Ereignistyp aus, über den die
3. Event subtype	After unexpected shut down	Geben Sie den Ereignis-Subtyp an, um die Regel zu aktivieren.
4. Action	Send SMS	Aktion, die ausgeführt werden soll, wenn ein Ereignis eintritt.
5. Custom message	Enable/Disable	Wenn eine Aktion eintritt, wird eine benutzerdefinierte
6. Recipient's phone	+123456789	Für wen Sie eine SMS senden möchten

### 6.10.5 Berichterstattung Konfiguration

Zeigt konfigurierte Dienste für Ereignisberichterstattung ermöglicht, disable, Ansicht zu aktivieren und die Parameter ändern.

All Events
System Events
Network Events
Events Reporting
Reporting Configuration

### Events Log Files Report

Create rules for Events Log reporting.

**Events Log Report Rules**

Events log	Transfer type	Enable	Sort	
System	Email	<input checked="" type="checkbox"/>	↕	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Network	FTP	<input checked="" type="checkbox"/>	↕	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

<sup>\*</sup> All rules are executed in current list order.

**Events Log Reporting Configuration:**

Events log	Transfer type	
System ▼	Email ▼	<input type="button" value="Add"/>

### 6.10.5.1 Events Log Report Konfiguration

Ermöglicht die Konfiguration von periodischen Ereignissen ändern Berichterstattung an E-Mail oder FTP.

Beispielwert  
Erläuterung

[All Events](#)
[System Events](#)
[Network Events](#)
[Events Reporting](#)
[Reporting Configuration](#)

## Events Log Report Configuration

### Modify events log file report rule

Enable

Events log

Transfer type

Compress file

Host

User name

Password

Interval between reports

Weekday

Hour

	Field Name	Sample Value	Explanation
1.	Enable	Enable/Disable	Eine Regel aktiv/inaktiv setzen
2.	Events log	System	Ereignistyp, auf den die Regel angewendet wird
3.	Transfer type	FTP	Ereignis-Subtyp, auf den die Regel angewendet wird: E-Mail/ftp
4.	Compress file	Enable	Aktion, die ausgeführt werden soll, wenn ein Ereignis eintritt.
5.	Host	192.168.123.123	FTP (File transfer Protocol) Hostname, z.B. ftp.example.com,
6.	User name	Username	192.168.123.123.
7.	Password	password	/=?_`{ }~. )
8.	Interval between reports	Week	Benutzername für die Authentifizierung am SMTP- (Simple Mail Transfer Protocol) oder FTP- (File Transfer Protocol) Server. Erlaubte Zeichen (a-z-A-Z0-9!@#\$\$%^&*+/-=?_`{ }~. )
9.	Weekday	Monday	Passwort für die Authentifizierung am SMTP (Simple Mail Transfer Protocol)
10.	Hour	12	oder FTP (File Transfer Protocol) Server. Erlaubte Zeichen (a-z-A-Z0-0)

## 7 Netzwerk

### 7.1 Mobil

#### 7.1.1 Allgemeine

##### 7.1.1.1 Mobile-Konfiguration

Hier können Sie Einstellungen konfigurieren, die verwendet werden, wenn Sie zu Ihrem lokalen 3G / LTE-Netz zu verbinden.

### Mobile Configuration

Mobile Configuration

SIM 1
SIM 2

Connection type NDIS ▾

Mode NAT ▾

APN

PIN number

Dialing number

Authentication method None ▾

Service mode 4G (LTE) preferred ▾

Deny data roaming

Use IPv4 only

Field Name	Sample value	Explanation
1. Mobile connection	PPP / NDIS	Der PPP-Modus verwendet eine Einwahlnummer, um eine Datenverbindung herzustellen. Der NDIS-Modus (Standard) verwendet keine Anwahl und kein PPP-Protokoll, um eine Datenverbindung herzustellen, es ist normalerweise schneller als der PPP-Modus.
2. Mode	NAT / Passthrough / Use bridge	Der NAT-Modus aktiviert die Übersetzung der Netzwerkadresse auf dem Router. Der Bridge-Modus überbrückt die LTE-Datenverbindung mit dem LAN. In diesem Modus hat der Router keine Internetverbindung, da der ISP die IP direkt auf das Endgerät (PC, Tablett oder Smartphone) überträgt. Der Bridge-Modus deaktiviert die meisten Router-Funktionen und Sie können nur über die statische IP-Adresse auf Ihrem Endgerät auf die Einstellungen Ihres Routers zugreifen. Der Durchreichmodus ist ähnlich dem Brückenmodus, außer dass der Router im Durchreichmodus über eine Internetverbindung verfügt.
3. APN	"APN"	Access Point Name (APN) ist ein konfigurierbarer Netzwerkidentifikator, der von einer mobilen Vorrichtung verwendet wird, wenn sie sich mit einem Mobilfunknetz verbindet.
4. PIN number	"1234" or any number that falls between 0000 and 9999	Eine persönliche Identifikationsnummer ist ein geheimes numerisches Passwort, das zwischen einem Benutzer und einem System geteilt wird und mit dem der Benutzer gegenüber dem System authentifiziert werden kann.
5. Dialing number	*99***1#	Die Rufnummer wird verwendet, um eine mobile PPP-Verbindung (Point-to-Point- Protocol) herzustellen.
6. Authentication	CHAP, PAP or none	Authentifizierungsmethode, mit der sich Ihr Carrier neu authentifiziert.

7.	method Username	“username”	Verbindungen. (Diese Auswahl ist beim alternativen Modell nicht verfügbar) Ihr Benutzername, mit dem Sie sich mit Ihrem Carrier-Netzwerk verbinden möchten. Dieses Feld wird verfügbar, wenn Sie eine Authentifizierungsmethode auswählen (d.h. die Authentifizierungsmethode ist nicht "keine"). Diese Felder sind bei dem alternativen Modell immer aktiviert.
8.	Password	“password”	Ihr Passwort, mit dem Sie sich mit Ihrem Carrier-Netzwerk verbinden können. Dieses Feld wird verfügbar, wenn Sie eine Authentifizierungsmethode auswählen (d.h. die Authentifizierungsmethode ist nicht "keine"). Diese Felder sind bei dem alternativen Modell immer aktiviert.
9.	Service mode	2G only, 2G preferred, 3G only, 3G preferred, 4G (LTE) only, 4G (LTE) preferred or automatic.	Ihre Netzwerkeinstellung. Wenn Ihr lokales Mobilfunknetz 2G,
10.	Deny data roaming	Enable/Disable	3G und 4G (LTE) können Sie angeben, mit welchem Netzwerk Sie sich verbinden möchten. Z.B.: Wenn Sie 2G wählen, verbindet sich der Router mit
11.	Use IPv4 only	Enable / Disable	Wenn diese Funktion aktiviert ist, verhindert das Gerät den Aufbau einer mobilen Datenverbindung, wenn es sich nicht im Heimnetzwerk befindet.

**Achtung:** Wird eine ungültige PIN-Nummer eingegeben wurde (dh die eingegebene PIN mit der man nicht übereinstimmt, der verwendet wurde, um Schutz der SIM-Karte), erhalten Sie Ihre SIM-Karte gesperrt. Zur Vermeidung solcher Pannen wird dringend empfohlen, eine ungeschützte zu verwenden SIM-Karte. Wenn Sie eine geschützte SIM einzufügen passieren und die PIN-Nummer falsch ist, wird Ihre Karte nicht sofort blockiert werden, obwohl nach ein paar Neustarts ODER-Konfiguration spart es wird.

#### 7.1.1.2 Mobile Data On Demand

Field name	Possible values	Explanation
1. Enable	Enable/Disable	Die Mobile Data On Demand-Funktion ermöglicht es Ihnen, die mobile Datenverbindung nur dann aufrechtzuerhalten, wenn sie in Betrieb ist.
2. No data timeout(sec)	1-99999999	Eine mobile Datenverbindung wird beendet, wenn während des Timeout-Zeitraums keine Daten übertragen werden.

#### 7.1.1.3 Force LTE network

Field name	Possible values	Explanation
1. Enable	Enable/Disable	Die LTE-Netzwerkfunktion Force deaktiviert periodisch die mobile Datenverbindung (für einige Sekunden), damit das Gerät Folgendes ausführen kann switch to LTE

Netzwerk. Dies könnte daran liegen, dass einige Betreiber den Wechsel von 3G- zu LTE-Netzen während der Datenübertragung nicht unterstützen.

2. Interval (sec) 180 - 3600

Intervall in Sekunden, mit dem das Gerät die mobile Datenverbindung regelmäßig deaktiviert.

### 7.1.2 SIM Management

Field name	Possible values	Explanation
1. Primary SIM card	SIM 1 / SIM 2	SIM-Karte, die im System als primäre SIM-Karte verwendet
2. Enable automatic	Enable/Disable	Automatischer Wechsel zwischen primären und sekundären SIM-Karten basierend auf den verschiedenen Regeln und
3. Check interval	20-3600	Überprüfungsintervall in Sekunden
4. On weak signal	Enable/Disable	Führen Sie einen SIM-Kartenwechsel durch, wenn die Signalstärke unter einen bestimmten Schwellenwert fällt.
5. On data limit	Enable/Disable	Führen Sie einen SIM-Kartenwechsel durch, wenn die Anzahl der mobilen Daten für Ihre aktuelle Situation begrenzt ist.
6. On sms limit	Enable/Disable	SIM-Karte wird überschritten
7. On roaming	Enable/Disable	Führen Sie einen SIM-Kartenwechsel durch, wenn die SMS-
8. On data connection fail	Enable/Disable	Führen Sie einen SIM-Kartenwechsel durch, wenn Roaming erkannt wird.
9. Switch back to primary SIM card after	Enable/Disable	Führen Sie einen SIM-Kartenwechsel durch, wenn die Datenverbindung fehlschlägt.



### 7.1.3 Netzbetreiber

Mit dieser Funktion können Sie scannen, wählen Sie und geben Sie manuell Netzbetreiber, an dem Router verbinden soll. Funktion wird großen Nutzen bieten, wenn Router in Roaming conditions. Operator ist nur für die aktive SIM-Karte ausgewählt ist. In Ordnung angeben Operator für die andere SIM-Karte muss er zunächst als primär SIM in „SIM-Management“ ausgewählt werden.

#### Network Operators

**Current SIM**

SIM card in use	SIM 1
Current operator	TELE2

**Scan For Network Operators**

Status	Operator name	Short name	Numeric name	Network access type	Connect
Available	Tele2 LT	Tele2 LT	24603	3G/2G	<input type="button" value="Connect"/>
Forbidden	LT BITE GSM	BITE	24602	3G/2G	<input type="button" value="Connect"/>
Available	OMNITEL LT	OMT	24601	2G/3G/4G	<input type="button" value="Connect"/>

Field Name	Sample Value	Explanation
1.	SIM card in use	SIM 1 / SIM 2 Zeigt die aktuell verwendeten SIM-Karten an.
2.	Current operator	„TELE2“ Name des Betreibers des angeschlossenen GSM-Netzes

Hinweis: **nach dem Scan klicken Knopf- Sie aktuelle mobile Verbindung verlieren!** Zum Ändern Status Netzbetreiber müssen verfügbar sein. Es ist die manuelle Verbindung zum Netzbetreiber, haben Sie numerische Namen zu füllen, und es ist sein müssen verfügbar.

### 7.1.4 Mobile Data-Grenze

Mit dieser Funktion können Sie maximale Datenmenge übertragen auf WAN-Schnittstelle begrenzen, um zu minimieren unerwünscht Traffic-Kosten.

#### 7.1.4.1 Datenverbindungslimit-Konfiguration

Fieldname	General	SIM Management	Network Operators	Mobile Data Limit	SIM Idle Protection
<b>Mobile Data Limit Configuration</b>					
SIM1 SIM2					
<b>Data Connection Limit Configuration</b>					
Enable data connection limit <input checked="" type="checkbox"/>					
Data limit* (MB) <input type="text" value="200"/>					
Period <input type="text" value="Month"/>					
Start day <input type="text" value="1"/>					

Field Name	Sample value	Explanation
1. Enable data connection	Enable/Disable	Disables mobile data when a limit for current period is reached
2. Data limit (MB)	200	Disable mobile data after limit value in MB is reached
3. Period	Month/Week/Da	Period for which mobile data limiting should apply
4. Start day/ Start hour	1	A starting time for mobile data limiting period

#### 7.1.4.2 SMS Warnung Konfiguration

SMS Warning Configuration	
Enable SMS warning	<input checked="" type="checkbox"/>
Data limit (MB)	<input type="text" value="300"/>
Period	<input type="text" value="Month"/>
Start day	<input type="text" value="1"/>
Phone number	<input type="text" value="+37012345678"/>

Field Name	Sample value	Explanation
1. Enable SMS warning	Enable/Disable	Ermöglicht das Versenden einer Warn-SMS bei Erreichen des mobilen Datenlimits für die aktuelle Periode.
2. Data limit (MB)	200	SMS-Warmmeldung nach Erreichen des Grenzwertes in MB senden
3. Period	Month/Week/Da	Zeitraum, für den die Beschränkung der mobilen Daten gelten sollte
4. Start day/ Start hour	1	Eine Startzeit für die mobile Datenbegrenzungsperiode
5. Phone number	+37012345678	Eine Telefonnummer, an die eine Warn-SMS-Nachricht gesendet werden soll, z.B.

### 7.1.5 Sim Standby-Schutz

Einige Netzbetreiber blockieren Benutzer SIM-Karten nach dem Zeitraum der Inaktivität. Diese Funktion ermöglicht es Router periodisch Schalter zum sekundären SIM-Karte und Datenverbindung mit Mobilfunknetz, um SIM-Karten-Blockierung zu verhindern, herzustellen.

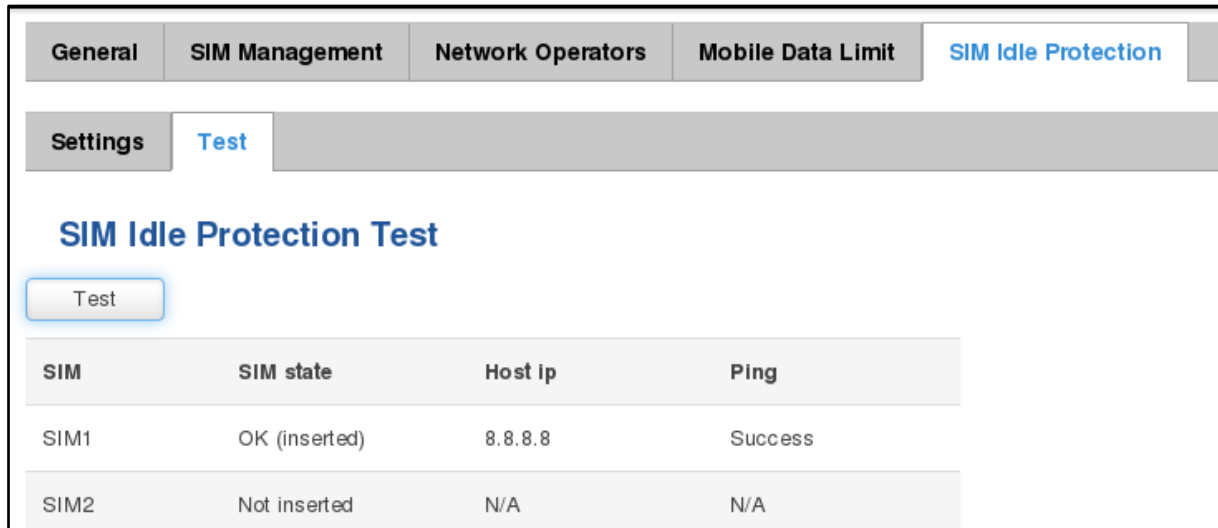
#### 7.1.5.1 Einstellungen

The screenshot shows the 'SIM Idle Protection Configuration' page for SIM1. The 'Enable' checkbox is unchecked. The 'Period' is set to 'Week', 'Day' to 'Monday', 'Hour' to '1', and 'Minute' to '0'. The 'Host to ping' is '8.8.8.8', 'Ping package size' is '56', and 'Ping requests' is '2'.

Field Name	Sample value	Explanation
1. Enable	Enable/Disable	Ermöglicht den Leerlaufschutz der SIM-Karte.
2. Period	Month / Week	Wechselt zwischen monatlichen und wöchentlichen Sim-Aktivierungszeiträumen.
3. Day	1-31 / Monday - Sunday	Gibt den Tag für die Aktivierung des Leerlaufschutzes der SIM-Karte an, 1-31 wenn Periode ist.
4. Hour	1-24	Monat, und Montag - Sonntag, wenn der Zeitraum Woche ist.
5. Minute	1-60	Gibt die Stunde für die Aktivierung des Leerlaufschutzes der SIM-Karte an.
6. Host to ping	8.8.8.8	Gibt die Minute für die Aktivierung des Leerlaufschutzes der SIM-Karte an.
7. Ping package size	56	Gibt die IP-Adresse oder den Domännennamen an, an die Datenpakete gesendet werden sollen.
8. Ping requests	2	Gibt die Größe des Ping-Pakets in Bytes an.

### 7.1.5.2-Test

Testet die Funktion der Leerlaufschutz mit Ihren Parametern auf Einstellungen Registerkarte eingegeben.

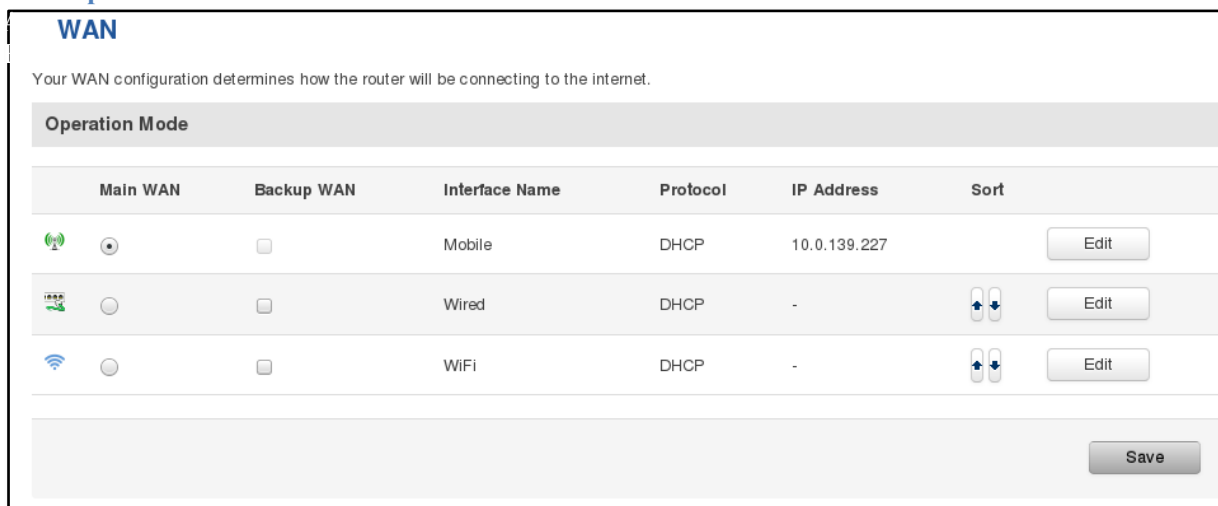


SIM	SIM state	Host ip	Ping
SIM1	OK (inserted)	8.8.8.8	Success
SIM2	Not inserted	N/A	N/A

Field Name	Sample value	Explanation
1. SIM	SIM1 / SIM2	Zeigt die SIM-Nummer an
2. SIM state	OK (inserted)	Zeigt den Status der SIM-Karte an.
3. Host IP	1-31 / Monday - Sunday	Zeigt die IP des Hosts an.
4. Ping	Success	Zeigt den Status des Ping-Versuchs an.

## 7.2 WAN

### 7.2.1 Operation Mode



Main WAN	Backup WAN	Interface Name	Protocol	IP Address	Sort
<input checked="" type="radio"/>	<input type="checkbox"/>	Mobile	DHCP	10.0.139.227	Edit
<input type="radio"/>	<input type="checkbox"/>	Wired	DHCP	-	↑ ↓ Edit
<input type="radio"/>	<input type="checkbox"/>	WiFi	DHCP	-	↑ ↓ Edit

Save

Type	Explanation
1. Main WAN	Switches between Mobile, Wired and WiFi interface for main WAN
2. Backup WAN	Let's user to select one or two interfaces for WAN backup
3. Interface Name	Displays Wan interface name, and changes interface priority, the interface at the table top has the highest priority
4. Protocol	Displays protocol used by Wan interface

- |    |            |   |
|----|------------|---|
| 5. | IP Address | Displays IP address acquired by specific interface  |
| 6. | Sort       | Sorts table rows and changes interface priority, the highest interface has highest priority |

### 7.2.2 Allgemeine Konfiguration

Gemeinsame Konfiguration können Sie Ihre TCP / IP-Einstellungen konfigurieren, für das Netzwerk wan. Sie können zwischen dem Static, DHCP oder PPPoE-Protokoll wechseln, indem Sie das Protokoll auswählen, die Sie verwenden möchten, und dann drücken **Switch – Protokoll**.

#### 7.2.2.1 Allgemeine Einstellungen

##### 7.2.2.1.1 Statisch:

The screenshot shows the 'Common Configuration' interface with the 'Advanced Settings' tab selected. The 'Protocol' dropdown is set to 'Static'. The following fields are visible:

- IPv4 address: 192.168.99.162
- IPv4 netmask: 255.255.255.0
- IPv4 gateway: 192.168.99.254
- IPv4 broadcast: 192.168.99.255
- Use custom DNS servers: 8.8.8.8 (with a red 'x' icon) and 8.8.6.6 (with a red 'x' and a green '+' icon).

Dies ist die Konfiguration Setup für, wenn Sie das statische Protokoll auswählen.

Filed name	Sample	Explanation
1. IPv4 address	192.168.99.162	Ihre Router-Adresse im WAN-Netzwerk
2. IPv4 netmask	255.255.255.0	Eine Maske, mit der definiert wird, wie "groß" das WAN-Netzwerk ist.
3. IPv4 gateway	192.168.99.254	Adresse, an die der Router den gesamten ausgehenden Datenverkehr senden soll.
4. IPv4 broadcast	192.168.99.255	Broadcast-Adresse (automatisch generiert, wenn nicht gesetzt). Es ist am besten, dieses Feld leer zu lassen, es sei denn, Sie wissen, was Sie tun.
5. custom DNS servers	8.8.8.8 8.8.6.6	Normalerweise verfügt das Gateway über einige vordefinierte DNS-Server. Wenn der Router also einen Hostnamen ("www.google.com", "www.cnn.com", etc...) für eine IP-Adresse auflösen muss, leitet er alle DNS-Anfragen an das Gateway weiter. Durch die Eingabe von benutzerdefinierten DNS-Servern kümmert sich der Router um die Auflösung der Hostnamen. Sie können mehrere DNS-Server eingeben, um die Redundanz zu gewährleisten, wenn einer der Server ausfällt.

### 7.2.2.1.2 DHCP:

General Setup **Advanced Settings**

Protocol

Hostname to send when requesting DHCP

**IP Aliases**

IP aliases are a way of defining or reaching a subnet that works in the same space as the regular network

*There are no IP aliases created yet*

Wenn Sie das DHCP-Protokoll auswählen, können Sie es so verwenden, wie es ist, da die meisten Netzwerke keine zusätzlichen Ressourcen benötigen.  
erweiterte Konfiguration

### 7.2.2.1.3 PPPoE

Dieses Protokoll wird hauptsächlich von DSL-Anbietern verwendet:

Common Configuration

General Setup **Advanced Settings**

Protocol

PAP/CHAP username

PAP/CHAP password

Access Concentrator

Service Name

Dies ist die Konfigurationseinstellung für die Auswahl des PPPoE-Protokolls.

Filed name	Sample	Explanation
1. PAP/CHAP username	test	Ihr Benutzername und Ihr Passwort, mit dem Sie sich mit Ihrem Carrier-Netzwerk verbinden möchten.
2. PAP/CHAP password	your_password	Eine Maske, mit der definiert wird, wie "groß" das WAN-Netzwerk ist.
3. Access Concentrator	isp	Gibt den Namen des Zugriffskonzentrators an. Lassen Sie das Feld leer, um die automatische Erkennung zu aktivieren.
4. Service Name	isp	Gibt den Namen des Dienstes an. Lassen Sie das Feld leer, um die automatische Erkennung zu aktivieren.

### 7.2.2.2 Advanced

Dies sind die erweiterten Einstellungen für jedes der Protokolle. Wenn Sie sich nicht sicher sind, wie Sie diese Attribute ändern können, wird dringend empfohlen, sie einem geschulten Fachmann zu überlassen:

#### 7.2.2.2.1 Static

Common Configuration

General Setup **Advanced Settings**

Disable NAT

Override MAC address

Override MTU

Use gateway metric

Field name	Sample value	Explanation
1. Disable NAT	On/Off	Schaltet NAT ein und aus.
2. Override MAC address	86:48:71:B7:E9:E4	Übersteuern der MAC-Adresse der WAN-Schnittstelle. Wenn Ihr ISP Ihnen eine statische IP-Adresse gibt, kann er diese auch an die MAC-Adresse Ihres Computers binden (d.h. diese IP-Adresse funktioniert nur mit Ihrem Computer). In diesem Feld können Sie die MAC-Adresse Ihres Computers eingeben und das Gateway täuschen, indem Sie denken, dass es mit Ihrem Computer kommuniziert.
3. Override MTU	1500	Maximale Übertragungseinheit - gibt die größtmögliche Größe eines Datenpakets an.
4. Use gateway metric	0	Die WAN-Konfiguration erzeugt standardmäßig einen Eintrag in der Routingtabelle. Mit diesem Feld können Sie die Metrik dieses Eintrags ändern.

#### 7.2.2.2.2 DHCP

Common Configuration

General Setup **Advanced Settings**

Disable NAT

Use broadcast flag

Use default gateway

Use DNS servers advertised by peer

Use gateway metric

Client ID to send when requesting DHCP

Vendor Class to send when requesting DHCP

Override MAC address

Override MTU

Field name	Sample value	Explanation
1. Disable NAT	Enable/Disable	Wenn diese Option aktiviert ist, führt der Router auf dieser Schnittstelle kein NAT (Masquerade) aus.
2. Use broadcast flag	Enable/Disable	Erforderlich für bestimmte ISPs, z.B. Charter mit DOCSIS 3

3.	Use default gateway	Enable/Disable	Wenn dieses Kontrollkästchen deaktiviert ist, wird keine Standardroute
4.	Use DNS server advertised by	Enable/Disable	Wenn dieses Kontrollkästchen deaktiviert ist, werden die angegebenen DNS-Serveradressen ignoriert.
5.	User gateway metric	0	Die WAN-Konfiguration erzeugt standardmäßig einen Eintrag in der Routingtabelle.
6.	Client ID to send when requesting		
7.	Vendor Class to send when requesting		
8.	Override MAC address	86:48:71:B7:E9:E4	Übersteuern der MAC-Adresse der WAN-Schnittstelle. Wenn Ihr ISP Ihnen eine statische IP-Adresse gibt, kann er diese auch an die MAC-Adresse Ihres Computers binden (d.h. diese IP-Adresse funktioniert nur mit Ihrem Computer). In diesem Feld können Sie die MAC-Adresse Ihres Computers eingeben und das Gateway täuschen, indem Sie denken, dass es mit Ihrem Computer kommuniziert
9.	Override MTU	1500	Maximale Übertragungseinheit - gibt die größtmögliche Größe eines Datenpakets an.

### 7.2.2.2.3 PPPoE

	Field name	Sample value	Explanation
1.	Disable NAT	Enable/Disable	Wenn diese Option aktiviert ist, führt der Router auf dieser Schnittstelle kein NAT (Masquerade) aus.
2.	Use default gateway	Enable/Disable	Wenn dieses Kontrollkästchen deaktiviert ist, wird keine
3.	Use gateway metric	0	
4.	Use DNS servers advertised by	Enable/Disable	Wenn dieses Kontrollkästchen deaktiviert ist, werden die angegebenen DNS-Serveradressen ignoriert.
5.	LCP echo failure	0	Angenommen, der Peer ist nach einer bestimmten Anzahl von LCP-Echo-Ausfällen tot, verwenden Sie 0, um Fehler zu
6.	LCP echo interval	5	Senden von LCP-Echo-Anfragen im angegebenen Intervall in Sekunden, nur in Verbindung mit der Fehlerschwelle
7.	Inactivity timeout	0	Inaktive Verbindung nach der angegebenen Anzahl von Sekunden schließen, verwenden Sie



### 7.2.2.2.4 IP Aliases

IP-Aliase sind eine Möglichkeit, ein Subnetz zu definieren oder zu erreichen, das im gleichen Raum wie das normale Netzwerk arbeitet.

The screenshot shows the configuration page for an IP Alias. The 'Advanced Settings' tab is selected. The configuration includes:

- IP Address: 192.168.99.161
- Netmask: 255.255.255.0
- Gateway: 192.168.99.254

Buttons for 'Delete', 'Add', and 'Save' are visible.

Wie Sie sehen können, ist die Konfiguration sehr ähnlich wie beim statischen Protokoll; nur im Beispiel ist ein 99.

definiert. Wenn nun ein Gerät eine IP im 99er Subnetz (192.168.99.xxx) hat und die Metrik des Subnetz-Gateways "höher" ist und

die Vorrichtung versucht, das Internet zu erreichen, wird sie ihren Verkehr nicht an das Gateway umleiten, das gemeinsam definiert ist.

Konfigurationen, sondern durch diejenige, die in IP-Aliassen angegeben ist.

The screenshot shows the configuration page for an IP Alias. The 'Advanced Settings' tab is selected. The configuration includes:

- IP Broadcast: [Empty field]
- DNS Server: [Empty field]

Buttons for 'Delete', 'Add', and 'Save' are visible.

Sie können auch optional eine Broadcast-Adresse und einen benutzerdefinierten DNS-Server definieren.

### 7.2.2.2.5 Backup WAN configuration

Backup WAN ist eine Funktion, die es Ihnen ermöglicht, Ihre primäre Verbindung zu sichern, falls sie ausfällt. Es kann sein

zwei Backup-Verbindungen, die gleichzeitig ausgewählt wurden, in diesem Fall, wenn die primäre Verbindung fehlschlägt, versucht der Router, Folgendes zu verwenden

Backup mit höherer Priorität und wenn das nicht verfügbar ist oder auch nicht funktioniert, dann versucht der Router das Backup mit niedrigerer Priorität.

The screenshot shows the 'Backup Configuration' page. It includes the following settings:

- Health monitor interval: 10 sec.
- Health monitor ICMP host(s): 8.8.4.4
- Health monitor ICMP timeout: 3 sec.
- Attempts before failover: 3
- Attempts before recovery: 3

A note at the top states: "Timing and other parameters will indicate how and when it will be determined that your conventional connection has gone down."

Die Mehrheit der Optionen besteht aus Timing und anderen wichtigen Parametern, die helfen, den Zustand von Ihre primäre Verbindung. Regelmäßige Zustandsüberprüfungen werden ständig in Form von ICMP-Paketen (Pings) an Ihren Geräten durchgeführt.

primäre Verbindung. Wenn sich der Verbindungszustand zu ändern beginnt (READY->NOT READY und umgekehrt), ist eine notwendige

Die Anzahl der fehlgeschlagenen oder bestandenen Zustandsprüfungen muss erreicht sein, bevor sich der Zustand vollständig ändert. Diese Verzögerung wird eingeleitet.

um "Spitzen" bei der Verbindungsverfügbarkeit zu minimieren, aber es verlängert auch die Zeit, bis die Backup-Verbindung hergestellt werden kann. auf oder ab.

Field Name	Sample value	Explanation
1. Gesundheitsmonitor Intervall	Disable/5/10/20/30/60/120	Das Intervall, in dem die Gesundheitschecks durchgeführt werden.
2. Zustandsüberwachung ICMP-Host(s)	Disable/DNS Server(s) /WAN GW/Custom	Where to Ping für einen Gesundheitscheck. Da es keine endgültige Möglichkeit gibt, festzustellen, wann die Verbindung zum Internet endgültig unterbrochen ist, müssen Sie einen Host definieren, dessen Verfügbarkeit die des Internets als Ganzes ist.
3. Zustandsüberwachung ICMP-Timeout	1/3/4/5/10 Seconds	Wie lange kann man warten, bis eine ICMP-Anfrage zurückkommt? Setzen Sie einen höheren Wert, wenn Ihre Verbindung eine hohe Latenz oder einen hohen Jitter (Latenzenitzen) aufweist.
4. Versuche vor dem Ausfallsicherung	1/3/5/10/15/20	Wie viele Prüfungen sollten für Ihr WAN fehlschlagen?
5. Versuche vor der Wiederherstellung	1/3/5/10/15/20	Verbindung ist endgültig als DOWN zu deklarieren.

#### 7.2.2.2.3 Wie richte ich einen Backup-Link ein?

Zuerst müssen wir einen Hauptverknüpfung auswählen und im WAN-Bereich eine oder zwei Backup-Links auswählen. Drücken Sie dann die Taste "Edit".

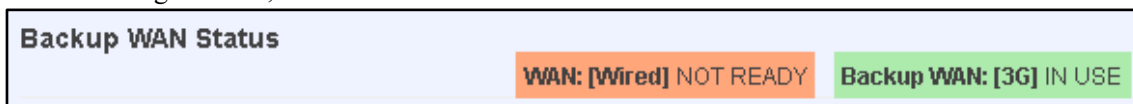
und konfigurieren Sie Ihre WAN- und Backup-Wan-Einstellungen nach Ihren Wünschen. Klicken Sie auf Speichern und warten Sie, bis die Einstellungen übernommen wurden. Jetzt

Auf der Seite Status -> Netzwerkinformationen -> WAN sollte eine Statusanzeige für das Backup-WAN erscheinen. Wenn alles korrekt funktioniert, sollten Sie so etwas wie dieses sehen:

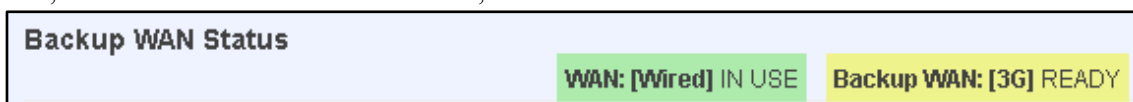


Das obige Bild zeigt den Status für das Backup-WAN, das über eine verkabelte Hauptverbindung konfiguriert ist. Sie können nun eine Downed Link durch einfaches Ziehen des Ethernet-WAN-Kabels.

Wenn du das getan hast, solltest du das sehen:



Und, wenn du das Kabel wieder einsteckst, solltest du das noch einmal sehen:



## 7.3 LAN

Diese Seite wird verwendet, um das LAN-Netzwerk zu konfigurieren, in dem alle Ihre Geräte und Computer, mit denen Sie eine Verbindung herstellen, mit der Router wird sich befinden.

### 7.3.1 Configuration

#### 7.3.1.1 General Setup

The screenshot shows the 'Configuration' section with two tabs: 'General Setup' (selected) and 'Advanced Settings'. Under 'General Setup', there are three input fields: 'IP address' with the value '192.168.1.1', 'IP netmask' with a dropdown menu showing '255.255.255.0', and 'IP broadcast' which is currently empty.

Field name	Sample value	Explanation
1. IP address	192.168.1.1	Adresse, die der Router im LAN-Netzwerk verwendet.
2. IP netmask	255.255.255.0	Eine Maske, mit der definiert wird, wie groß das LAN-Netzwerk ist.
3. IP broadcast	0	IP-Übertragungen werden von BOOTP- und DHCP-Clients verwendet, um Anfragen zu finden und an ihre jeweiligen Server zu senden.

#### 7.3.1.2 Advanced settings

The screenshot shows the 'Configuration' section with two tabs: 'General Setup' and 'Advanced Settings' (selected). Under 'Advanced Settings', there are four configuration options: 'Accept router advertisements' with an unchecked checkbox, 'Override MTU' with a text input field containing '1500', 'Use gateway metric' with a text input field containing '0', and 'Use WAN port as LAN' with an unchecked checkbox.

Field name	Sample value	Explanation
1. Accept router advertisement	Enable/Disable	Wenn aktiviert, erlaubt es, Routerwerbung anzunehmen (standardmäßig deaktiviert).
2. Override MTU	1500	MTU (Maximum Transmission Unit) gibt die größtmögliche Größe eines Datenpakets an.
3. Use gateway metric	0	Mit diesem Feld können Sie die Metrik dieses Eintrags ändern.
4. Use WAN port as LAN	Enable/Disable	

### 7.3.2 DHCP Server

Der DHCP-Server ist der routerseitige Dienst, der die TCP/IP-Einstellungen jedes Geräts automatisch konfigurieren kann. einen solchen Dienst anfordert. Wenn Sie ein Gerät anschließen, das so konfiguriert wurde, dass es automatisch die IP-Adresse erhält, wird der DHCP Server wird eine Adresse gemietet und das Gerät kann vollständig mit dem Router kommunizieren.

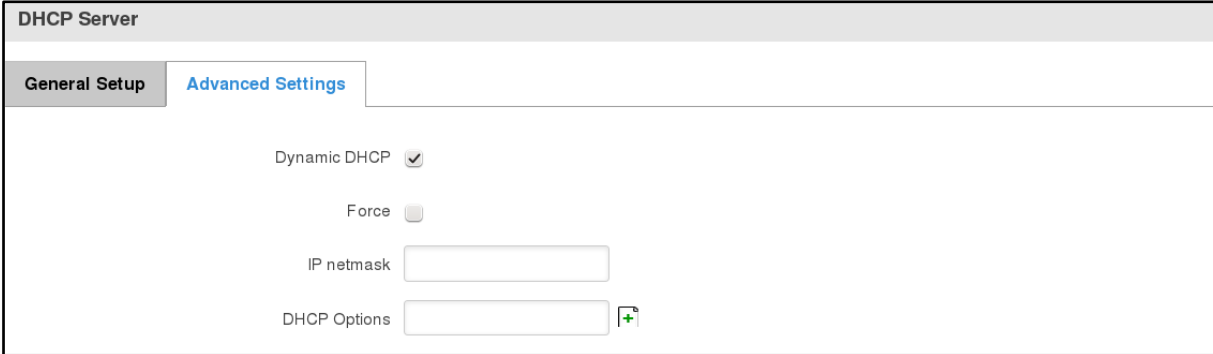
#### 7.3.2.1 General Setup

Field Name	Sample value	Explanation
<b>DHCP Server</b>		
<div style="display: flex; justify-content: space-between;"> <span>General Setup</span> <span>Advanced Settings</span> </div>		
DHCP	Enable	
Start	100	
Limit	150	
Lease time	12	Hours

Field Name	Sample value	Explanation
1. DHCP	Enable/Disable	DHCP-Serververwaltung
2. Start	100	Die Startadresse des Bereichs, den der DHCP-Server verwenden kann, um Geräte zu versorgen. Z.B.: wenn Ihre LAN-IP 192.168.2.1 und Ihre Subnetzmaske 192.168.2.1 ist. 255.255.255.255.255.0 bedeutet, dass in Ihrem Netzwerk eine gültige IP-Adresse verwendet werden muss. im Bereich von[192.168.2.1 - 192.168.2.2.254](192.168.2.0 und 192.168.2.255 sind spezielle, nicht verfügbare Adressen). Wenn der Startwert auf 100, dann kann der DHCP-Server nur Adressen ab 192.168.2.100 vergeben.
3. Limit	150	Wie viele Adressen der DHCP-Server zur Verfügung stellen darf. Fortfahren mit dem obigen Beispiel: Wenn die Startadresse 192.168.2.100 ist, dann ist die Endadresse 192.168.2.2.254 (100 + 150 - 1 = 254).
4. Lease time	12	Wie lange kann ein gemietetes IP als gültig angesehen werden? Eine IP-Adresse nach Ablauf der angegebenen Zeit verfällt und das Gerät, das sie gemietet hat, muss eine neue anfordern. Wählen Sie Stunde oder Minute (mindestens 2 Minuten).

### 7.3.2.2 Erweiterte Einstellungen

Sie können auch einige erweiterte Optionen definieren, die festlegen, wie der DHCP-Server in Ihrem LAN-Netzwerk arbeiten soll.



**DHCP Server**

General Setup    **Advanced Settings**

Dynamic DHCP

Force

IP netmask

DHCP Options  +

Field Name	Sample Value	Explanation
1. Dynamic DHCP	Checked/Unchecked	Dynamische Zuweisung von Kundenadressen, wenn auf 0 gesetzt, werden nur die in den Ether-Dateien vorhandenen Kunden bedient.
2. Force	Checked/Unchecked	Erzwingt die DHCP-Bedienung, auch wenn ein anderer DHCP-Server im gleichen Netzwerksegment erkannt wird.
3. IP netmask		Sie können Ihre LAN-Netzmaske hier überschreiben, damit der DHCP-Server denkt, dass er ein größeres oder kleineres Netzwerk bedient, als er tatsächlich ist.
4. DHCP-Options		Zusätzliche Optionen, die für diesen DHCP-Server hinzugefügt werden sollen. Beispielsweise können Sie mit '26,1470' oder 'option:mtu, 1470' eine MTU per DHCP zuweisen. Ihr Kunde muss die MTU per DHCP akzeptieren, damit dies funktioniert.

## 7.4 VLAN

Auf dieser Seite können Sie Ihre virtuellen LAN-Einstellungen konfigurieren, entweder Port basierend oder Tag basierend.

### 7.4.1 VLAN Networks

#### 7.4.1.1 VLAN Functionality



**VLAN Functionality**

VLAN mode

Field Name	Sample Value	Explanation
1. VLAN mode	Disabled / Port based / Tag based	Ermöglicht es dem Benutzer, den VLAN-Modus zu wählen oder die VLAN-Funktionalität zu deaktivieren.

### 7.4.1.2 VLAN Network List

Wenn VLAN-Modus - Portbasiert:

VLAN Networks List					
VLAN ID	LAN ports			Wireless access points	LAN
	1	2	3	Teletonika_Router	
1	On	On	On	<input type="checkbox"/>	None <input type="button" value="Delete"/>

Field Name	Sample Value	Explanation
1. VLAN ID	1	VLAN Identifizierungsnummer, erlaubt in Reichweite (1-4094)
2. LAN ports 1 / 2 / 3	on	Schaltet jeden LAN-Anschluss zwischen EIN, AUS oder markiertem Zustand um.
3. Wireless access	Enabled / Disabled	Weisen Sie ausgewählte Access Points dem ausgewählten LAN zu.
4. LAN		Wählen Sie, welchem LAN Sie ausgewählte LAN-Ports und drahtlose Zugangspunkte zuweisen möchten.

Wenn VLAN-Modus - Taged basiert:

VLAN Networks List		
VLAN ID	Wireless access points	LAN
	Teletonika_Router	
2	<input type="checkbox"/>	None <input type="button" value="Delete"/>

Field Name	Sample Value	Explanation
1. VLAN ID	1	VLAN Identifizierungsnummer, erlaubt in Reichweite (1-4094)
3. Wireless access	Enabled / Disabled	Weisen Sie ausgewählte Access Points dem ausgewählten LAN zu.
4. LAN		Wählen Sie aus, zu welchem LAN die drahtlosen Zugangspunkte gehören.

### 7.4.2 LAN Networks

Auf dieser Seite können Sie zusätzliche LAN-Netzwerke erstellen und diese mit LAN-Ports und Wireless Access Points zuweisen. Du können Sie zusätzliche Informationen darüber erhalten, wie Sie die Einstellungen Ihres LANs konfigurieren können, siehe Abschnitt - 6.3 LAN.

## LAN

**LAN Networks List**

LAN name	Interface name	
Lan	eth0 tap0	<input type="button" value="Edit"/>

LAN name:

Field Name	Sample Value	Explanation
1. LAN name	LAN2	Specifies new LAN name

### 7.5 Wireless

Auf dieser Seite können Sie Ihre WLAN-Einstellungen konfigurieren. Je nachdem, ob Ihr WAN-Modus auf Wi-Fi eingestellt ist oder nicht, wird die Seite entweder die Optionen für die Konfiguration eines Access Points oder die Optionen für die Konfiguration einer Verbindung zu folgendem anzeigen einen lokalen Zugangspunkt.  
Zugangspunkt:

Wireless General
Site Survey

## Wireless Access Point

Here you can configure your wireless settings like radio frequency, mode, encryption etc...

**Device Configuration**

General Setup
Advanced Settings

Enable wireless

Channel

**Interface Configuration**

General Setup
Wireless Security
MAC Filter
Advanced Settings

SSID

Hide SSID

Hier sehen Sie die Übersicht über die drahtlose Konfiguration. Es ist in zwei Hauptabschnitte unterteilt - Gerät und Schnittstelle. Eine davon ist der Konfiguration von Hardwareparametern anderer Art - Software - gewidmet.

Hier können Sie die Verfügbarkeit des drahtlosen Radios und die physikalische Kanalfrequenz umschalten.

**Wichtiger Hinweis:** Wie auf dem Bild zu sehen, sollten Sie immer speichern, bevor Sie das Radio ein- und ausschalten.

ESSID - Ihre Identifikationszeichenkette für drahtlose Netzwerke. Dies ist der Name Ihres Wi-Fi-Netzwerks. Wenn anderes Wi-Fi

fähige Computer oder Geräte scannen das Gebiet nach Wi-Fi-Netzwerken, sie werden Ihr Netzwerk mit diesem Namen sehen.

ESSID ausblenden - Macht Ihre SSID unsichtbar für andere Geräte, die versuchen, den Bereich zu scannen.

### 7.5.1.1 Device

#### 7.5.1.1.1 Erweiterte Einstellungen

The screenshot shows the 'Advanced Settings' tab for a wireless device. The settings are as follows:

- Mode: 802.11g+n
- Country code: 00 - World
- Transmit power: 100 %
- Fragmentation threshold: 2346
- RTS/CTS threshold: 2346

Hier können Sie erweiterte Parameter konfigurieren:

Field name	Sample value	Explanation
1. Mode	Auto, b, g, g+n	Verschiedene Modi bieten unterschiedliche Durchsatz- und Sicherheitsoptionen.
2. Country Code	Any ISO/IEC 3166 alpha2 country code	Wenn Sie dies auswählen, kann das drahtlose Funkgerät seine internen Parameter so konfigurieren, dass sie den Vorschriften Ihres Landes entsprechen.
3. Transmit power	20%/40%/60%/80%/100	WiFi-Signalleistung auswählen
4. Frag. Threshold	2346	Die kleinste Paketgröße, die fragmentiert und von mehreren Frames übertragen werden kann. In Bereichen, in denen Interferenzen ein Problem darstellen, könnte die Einstellung eines niedrigeren Fragment-Schwellenwerts dazu beitragen, die Wahrscheinlichkeit von erfolglosen Paketübertragungen zu verringern und so die Geschwindigkeit zu erhöhen
5. RTS/CTS Threshold	2346	Anforderung der Sendeschwelle. Es kann helfen, Probleme zu lösen, die auftreten, wenn sich mehrere Access Points im selben Bereich befinden.



### 7.5.1.2 Schnittstelle

#### 7.5.1.2.1 Sicherheit

Verschlüsselung - Es gibt viele Arten der Verschlüsselung, eine unverwechselbare Klasse, die unten beschrieben wird.

Wählen Sie zunächst eine Verschlüsselungsmethode aus: TKIP, CCMP, TKIP&CCMP und auto. Hinweis: Einige Authentifizierungsmethoden werden nicht unterstützt. unterstützt TKIP (und TKIP&CCMP) Verschlüsselung. Nachdem Sie Ihre Verschlüsselungsmethode ausgewählt haben, sollten Sie Ihre Passphrase, die mindestens 8 Zeichen lang sein muss.

#### 7.5.1.2.2 MAC-Filter

Filter - Sie können eine Regel definieren, was mit der von Ihnen definierten MAC-Liste geschehen soll. Sie können entweder nur die aufgelisteten MACs oder erlauben ALLE, aber verbieten Sie nur die aufgeführten.

#### 7.5.1.2.3 Erweiterte Einstellungen

Getrennte Clients - verhindert, dass Wi-Fi-Clients im gesunden Subnetz miteinander kommunizieren.

### 7.5.1.3 Client

RUT9xx kann als Wi-Fi-Client eingesetzt werden (siehe 6.5 Kapitel dieses Handbuchs). Der Client-Modus ist fast identisch mit dem AP, mit Ausnahme von für die Tatsache, dass die meisten Optionen durch den drahtlosen Zugangspunkt bestimmt werden, mit dem sich der Router verbindet. Ändern

können sie zu einer unterbrochenen Verbindung zu einem AP führen.

Zusätzlich zu den Standardoptionen können Sie auch auf die Schaltfläche Scannen klicken, um die Umgebung neu zu scannen und zu versuchen.

Verbindung zu einem neuen drahtlosen Zugangspunkt herstellen.

## 7.6 Firewall

In diesem Abschnitt werden wir einen Blick auf die verschiedenen Firewall-Funktionen werfen, die mit dem Router ausgeliefert werden.

### 7.6.1 General Settings

Die Router-Firewall ist ein Standard-Linux-iptables-Paket, das Routing-Ketten und -Richtlinien verwendet, um Folgendes zu ermöglichen Kontrolle über den eingehenden und ausgehenden Datenverkehr.

Field Name	Sample value	Explanation
1. Drop Invalid packets	Gepprüft/ungeprüft	Eine Aktion "Drop" wird für ein Paket ausgeführt, das als ungültig eingestuft wird.
2. Input	Ablehnen/Ablehnen/Ablehnen/Akzeptieren	DEFAULT*-Aktion, die für Pakete durchgeführt werden soll, die die Input-Kette durchlaufen.
3. Output	Ablehnen/Ablehnen/Ablehnen/Akzeptieren	DEFAULT*-Aktion, die für Pakete durchgeführt werden soll, die die Output-Kette durchlaufen.
4. Forward	Ablehnen/Ablehnen/Ablehnen/Akzeptieren	DEFAULT*-Aktion, die für Pakete durchgeführt werden soll, die die Forward-Kette durchlaufen.

\*STANDARD: Wenn ein Paket durch eine Firewall-Kette geht, wird es gegen alle Regeln für diese spezielle Kette abgeglichen. Wenn keine Regel mit dem Paket übereinstimmt, wird eine entsprechende Aktion (entweder Drop oder Reject oder Accept) durchgeführt.

Akzeptieren - Paket wird in der nächsten Kette fortgesetzt.

Drop - Paket wird gestoppt und gelöscht.

Ablehnen - Das Paket wird gestoppt, gelöscht und, anders als Drop, ein ICMP-Paket mit einer Ablehnungsmeldung.

wird an die Quelle des abgelegten Pakets gesendet.

### 7.6.2 DMZ

### DMZ Configuration

Enable

DMZ host IP address

Indem Sie DMZ für einen bestimmten internen Host (z.B.: Ihren Computer) aktivieren, stellen Sie diesen Host und seine Dienste folgenden Anforderungen aus das Router-WAN-Netzwerk (z.B. - Internet).

### 7.6.3 Portweiterleitung

Hier können Sie Ihre eigenen Portweiterleitungsregeln definieren.

General Settings
Port Forwarding
Traffic Rules
Custom Rules

### Firewall - Port Forwarding

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

**Port Forwarding Rules**

Name	Protocol	Source	Via	Destination	Enable	Sort	
localWebsite	TCP	From any host in wan	To any router IP at port 12345	Forward to IP 192.168.1.109, port 80 in lan	<input checked="" type="checkbox"/>	↑ ↓	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

**New Port Forward Rule**

Name	Protocol	External port	Internal IP	Internal port	
<input style="width: 100px;" type="text" value="localWebsite"/>	<span style="border: 1px solid gray; padding: 2px;">TCP</span>	<input style="width: 100px;" type="text" value="12345"/>	<span style="border: 1px solid gray; padding: 2px;">192.168.1.109</span>	<input style="width: 100px;" type="text" value="80"/>	<input type="button" value="Add"/>

Mit der Port-Forwarding können Sie Server und Dienste auf lokalen LAN-Maschinen einrichten. Das obige Bild zeigt, wie die Sie können eine Regel einrichten, die es ermöglicht, eine Website, die am 192.168.1.109 gehostet wird, von außen zu erreichen. indem Sie `http://routersExternalIp:12345/` eingeben.

Field Name	Sample value	Explanation
1. Name	"localWebsite"	Name der Regel. Wird lediglich verwendet, um die Verwaltung von Regeln zu erleichtern.
2. Protocol	TCP/UDP/TCP+UDP/Other	Art des Protokolls des eingehenden Pakets.
3. External Port	1-65535	Von welchem Port des WAN-Netzwerks wird der Datenverkehr weitergeleitet.
4. Internal IP address	IP-Adresse eines Computers in Ihrem LAN	Die IP-Adresse des internen Computers, auf dem sich ein Dienst befindet, auf den wir von außen zugreifen möchten.
5. Internal port	1-65535	Zu welchem Port auf der internen Maschine würde die Regel den Datenverkehr umleiten?

Wenn Sie auf Bearbeiten klicken, können Sie eine Regel auf nahezu perfekte Weise feinabstimmen, wenn Sie dies wünschen.

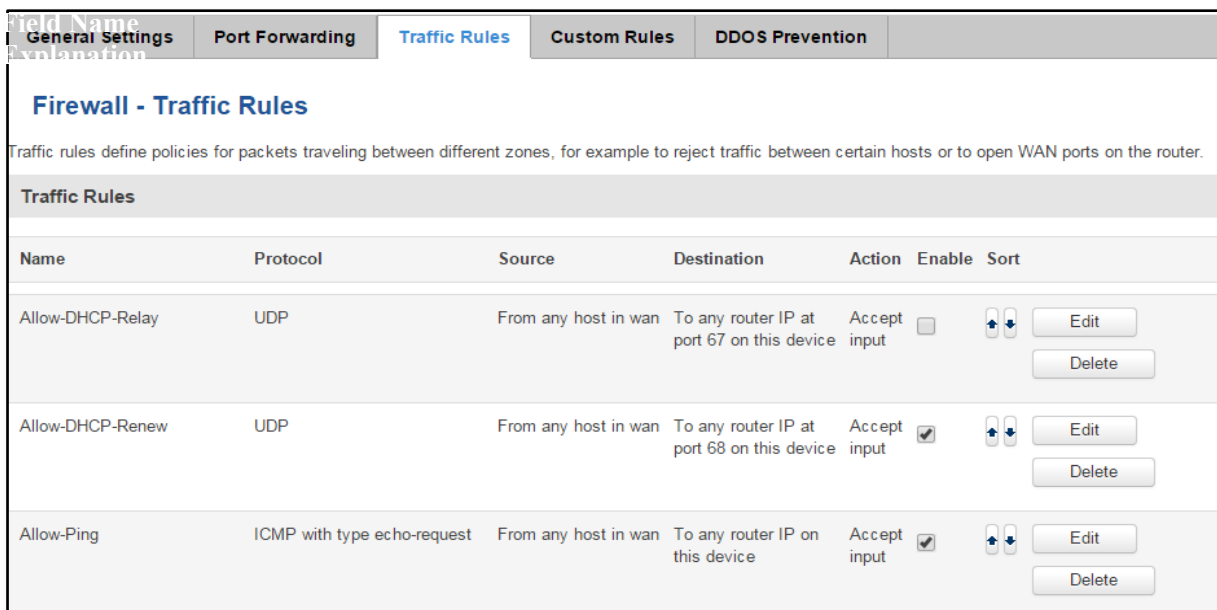
The screenshot shows a configuration window for a firewall rule. At the top, there is a toggle for 'Rule is enabled' set to 'Disable'. Below this, the 'Name' field contains 'localWebsite'. The 'Protocol' is set to 'TCP'. Under 'Source zone', three radio buttons are visible: 'lan: lan:', 'vpn: (empty)', and 'wan: wan: ppp: wan2:'. The 'wan' zone is selected. The 'Source MAC address' is 'any', 'Source IP address' is 'any', and 'Source port' is 'any'. The 'External IP address' is 'any' and 'External port' is '12345'. Under 'Internal zone', three radio buttons are visible: 'lan: lan:', 'vpn: (empty)', and 'wan: wan: ppp: wan2:'. The 'lan' zone is selected. The 'Internal IP address' is '192.168.1.109' and 'Internal port' is '80'. The 'Enable NAT loopback' checkbox is checked. The 'Extra arguments' field is empty.

	Field Name	Sample value	Explanation
1.	Name	"localWebsite"	Name der Regel. Wird lediglich verwendet, um die Verwaltung von Regeln zu erleichtern.
2.	Protocol	TCP/UDP/TCP+ UDP/ICMP/Custo	Sie können mehrere Protokolle angeben, indem Sie (benutzerdefiniert) auswählen und dann Protokolle eingeben, die durch Leerzeichen
3.	Quellzone	LAN/VPN/WAN	Nur eingehenden Traffic aus dieser Zone zuordnen
4.	Quell-MAC-Adresse	Any	Nur eingehenden Datenverkehr von diesen MACs zuordnen
5.	Quell IP address	any	Abgleich des eingehenden Datenverkehrs von dieser IP oder nur des
7.	Quell port	any	Abgleich des eingehenden Datenverkehrs, der vom angegebenen Quellport oder Portbereich auf dem Client-Host stammt.

8.	External IP address	any	Abgleich des eingehenden Datenverkehrs, der nur an die angegebene IP-
9.	External port	12345	Übereinstimmen des eingehenden Datenverkehrs, der auf den angegebenen Ziel-Port oder Port-Bereich auf diesem Host gerichtet ist.
10.	Internal zone	LAN/VPN/WAN	Umleitung des angepassten eingehenden Verkehrs an die angegebene interne Zone
11.	Internal IP address	192.168.1.109	Umleitung von angepasstem eingehenden Datenverkehr auf den angegebenen internen Host
12.	Internal port	80	Umleitung des angepassten eingehenden Datenverkehrs an den angegebenen Port auf dem internen Host
13.	NAT-Schleife aktivieren	Enable/Disable	NAT Loopback ermöglicht es Ihrem lokalen Netzwerk (d.h. hinter Ihrem Router/Modem), sich mit einer nach vorne gerichteten IP-Adresse (z.B. 208.112.93.73) einer Maschine zu verbinden, die es auch in Ihrem lokalen Netzwerk verwendet.
14.	Extra arguments		Übergibt zusätzliche Argumente an iptables. Mit Vorsicht verwenden!

### 7.6.4 Traffic Rules

Die Verkehrsregel-Seite enthält eine allgemeinere Regeldefinition. Damit kannst du Ports blockieren oder öffnen, die Art und Weise ändern. Der Datenverkehr wird zwischen LAN und WAN und vielen anderen Dingen weitergeleitet.



Field Name	Explanation
1. Name	Name der Regel. Wird nur für einfachere Regelmanagementzwecke verwendet.
2. Protocol	Protokolltyp des eingehenden oder ausgehenden Pakets
3. Source	Abgleich des eingehenden Datenverkehrs von dieser IP oder nur des Bereichs
4. Destination	Umleitung von angepasstem Datenverkehr an die angegebene IP-Adresse und den Zielport
5. Action	Maßnahmen, die für das Paket zu ergreifen sind, wenn es der Regel entspricht.
6. Enable	Selbsterklärend. Deaktivieren Sie die Markierung, um die Regel zu deaktivieren. Die Regel wird nicht gelöscht, aber auch nicht in die Firewall geladen.
7. Sort	Wenn ein Paket ankommt, wird es auf eine passende Regel überprüft. Wenn es mehrere Regeln gibt, die mit der Regel übereinstimmen, wird die erste angewendet, d.h. die Reihenfolge der Regelliste wirkt sich auf den Betrieb Ihrer Firewall aus, daher haben Sie die Möglichkeit, Ihre Liste nach Ihren Wünschen zu sortieren.

Sie können die Firewall-Regel konfigurieren, indem Sie auf die Schaltfläche Bearbeiten klicken.

Rule is disabled

Name

Restrict to address family

Protocol

Match ICMP type

Source zone

Any zone

lan: lan:

vpn: (empty)

wan: wan: ppp: wan2:

Source MAC address

Source address

Source port

Destination zone

Device (input)

Any zone (forward)

lan: lan:

vpn: (empty)

wan: wan: ppp: wan2:

Destination address

Destination port

Action

Extra arguments

Field Name	Sample value	Explanation
1. Name	"Allow-DHCP-Relay"	Wird verwendet, um das Regelmanagement zu erleichtern.
2. Beschränkung auf die Adresse der Familie	IPv4-only	Abgleich des Datenverkehrs nur von ausgewählten Adressfamilien
3. Protocol	TCP/UDP/Any/ICMP/Custom	Protokoll des Pakets, das mit den Verkehrsregeln abgeglichen wird.
4. Match ICMP type	any	Abgleich des Datenverkehrs nur mit dem ausgewählten ICMP-Typ
5. Source zone	Any zone/LAN/VPN/WAN	Nur eingehenden Traffic aus dieser Zone zuordnen
6. Source MAC address	any	Nur eingehenden Datenverkehr von diesen MACs zuordnen
7. Source address	any	Abgleich des eingehenden Datenverkehrs von dieser IP oder nur des Bereichs

### 7.6.4.1 Open Ports On Router

8.	Source port	any	Abgleich des eingehenden Datenverkehrs, der vom angegebenen Quellport oder Portbereich auf dem Client-Host stammt.
9.	Zielzone	Device/Any zone/LAN/VPN/WA	Abgleich des weitergeleiteten Verkehrs nur mit der angegebenen Zielzone
10.	Zieladdress	any	Abgleich des weitergeleiteten Datenverkehrs mit der angegebenen Ziel-IP
11.	Zielport	67	Übermitteln Sie den weitergeleiteten Datenverkehr nur an den angegebenen Ziel-Port oder Port-Bereich.
12.	Action	Drop/Accept/Reject + chain + additional rules	Maßnahmen, die auf dem Paket zu ergreifen sind, wenn es der Regel entspricht. Sie können auch zusätzliche Optionen definieren, wie z.B. die Begrenzung des Paketvolumens und die Definition, zu welcher Kette die Regel gehört.

Field Name	Sample value	Explanation
1. Name	Open_Port_rule	Wird verwendet, um das Regelmanagement zu erleichtern.
2. Protocol	TCP/UDP/Any/ICMP/Custom	Protokoll des Pakets, das mit den Verkehrsregeln abgeglichen wird.
3. External port	1-65535	Übereinstimmen des eingehenden Datenverkehrs, der auf den angegebenen Ziel-Port oder Port-Bereich auf diesem Host

### 7.6.4.2 Neue Forward-Regel

**New Forward Rule**

Name	Source	Destination	
<input type="text" value="Forward rule new"/>	<input type="button" value="LAN"/> ▾	<input type="button" value="WAN"/> ▾	<input type="button" value="Add"/>

Field Name	Sample value	Explanation
1. Name	Forward_rule_new	Wird verwendet, um das Regelmanagement zu erleichtern.
2. Source	LAN/VPN/WAN	Nur eingehenden Datenverkehr von ausgewählten
3. Protocol	TCP/UDP/Any/ICMP/Custom	Protokoll des Pakets, das mit den Verkehrsregeln abgeglichen wird.

## 7.6.4.3 Source NAT

**Source NAT**

Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.

Name	Protocol	Source	Destination	SNAT	Enable	
SNAT	TCP+UDP	From any host in lan	To any host, port 22 in wan	Rewrite to source IP 10.101.1.10, port 22	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

**New Source NAT**

Name	Source	Destination	Source IP	Source port	
<input type="text" value="SNAT"/>	<input type="text" value="LAN"/>	<input type="text" value="WAN"/>	<input type="text" value="10.101.1.10"/>	<input type="text" value="22"/>	<input type="button" value="Add"/>

Field Name	Sample value	Explanation
1. Name	Forward_rule_new	Wird verwendet, um das Regelmanagement zu erleichtern.
2. Protocol	TCP/UDP/Any/ICMP/Custom	Protokoll des Pakets, das mit den Verkehrsregeln abgeglichen wird.
3. Source	LAN/VPN/WAN	Nur eingehenden Datenverkehr von ausgewählten Adressfamilien
4. Zielort		Umleitung von angepasstem Datenverkehr an die angegebene IP-Adresse und den Zielport
5. SNAT		SNAT (Source Network Address Translation) schreibt die Quell-IP-Adresse und den Port des Pakets neu.
6. Enable	Enable/Disable	Eine Regel aktiv/inaktiv setzen



Sie können die NAT-Regel der Firewall-Source konfigurieren, indem Sie auf die Schaltfläche Bearbeiten klicken.

Rule is enabled

Name

Protocol

Source zone  lan: lan:  vpn: (empty)  wan: wan: ppp: wan2:

Source MAC address

Source IP address

Source port

Destination zone  lan: lan:  vpn: (empty)  wan: wan: ppp: wan2:

Destination IP address

Destination port

SNAT IP address

SNAT port

Extra arguments

Field Name	Sample value	Explanation
1. Name	"Allow-DHCP-Relay"	Wird verwendet, um das Regelmanagement zu erleichtern.
2. Protocol	TCP/UDP/Any/ICMP/Custom	Protokoll des Pakets, das mit den Verkehrsregeln abgeglichen wird.
3. Quelle	LAN/VPN/WAN	Nur eingehenden Traffic aus dieser Zone zuordnen
4. Quelle MAC address	any	Nur eingehenden Datenverkehr von diesen MACs zuordnen
5. Quelle address	any	Abgleich des eingehenden Datenverkehrs von dieser IP oder nur
6. Quelle port	any	Abgleich des eingehenden Datenverkehrs, der vom angegebenen Quellport oder Portbereich auf dem Client-Host stammt.
7. Zielort zone	LAN/VPN/WAN	Abgleich des weitergeleiteten Verkehrs nur mit der angegebenen Zielzone

8. Zielortaddress	Select from the list	Abgleich des weitergeleiteten Datenverkehrs mit der angegebenen Ziel-IP
9. Zielort port	any	Übermitteln Sie den weitergeleiteten Datenverkehr nur an den angegebenen Ziel-Port oder Port-Bereich.
10. SNAT IP address	"10.101.1.10"	Schreiben Sie den angepassten Datenverkehr auf die angegebene IP-Adresse neu.
11. SNAT port	"22"	Schreiben Sie den angepassten Traffic auf den angegebenen Quellport neu. Kann leer gelassen werden, um nur die IP-Adresse' neu zu schreiben.
12. Extra arguments		Übergibt zusätzliche Argumente an iptables. Mit Vorsicht verwenden!

### 7.6.5 Custom Rules

Hier haben Sie die ultimative Freiheit, Ihre Regeln zu definieren - Sie können sie direkt in die iptables eingeben.

Programm. Gib sie einfach in das Textfeld ein und es wird als Linux-Shell-Skript ausgeführt. Wenn Sie sich nicht sicher sind, wie Sie sich verhalten sollen.

Verwenden Sie iptables, besuchen Sie das Internet für Handbücher, Beispiele und Erklärungen.

General Settings
Port Forwarding
Traffic Rules
Custom Rules

### Firewall - Custom Rules

Custom rules allow you to execute arbitrary iptables commands which are not otherwise covered by the firewall framework. The commands are executed after each firewall restart, right after the default ruleset has been loaded.

```
# This file is interpreted as shell script.
# Put your custom iptables rules here, they will
# be executed with each firewall (re-)start.

# Internal uci firewall chains are flushed and recreated on reload, so
# put custom rules into the root chains e.g. INPUT or FORWARD or into the
# special user chains, e.g. input_wan_rule or postrouting_jan_rule.
```

Reset
Submit

## 7.6.6 DDOS Prevention

### 7.6.6.1 SYN Flood Protection

SYN Flood Protection ermöglicht es Ihnen, sich vor Angriffen zu schützen, die einen Teil des normalen TCP Dreiwege-Handshakes ausnutzen, um Ressourcen auf dem Zielsystem zu verbrauchen und ihn inaktiv zu machen. Im Wesentlichen, mit SYN flood DDoS, dem Täter, sendet TCP-Verbindungsanforderungen schneller, als der Zielcomputer sie verarbeiten kann, was zu einer Netzwerksättigung führt.

The screenshot shows the 'DDOS Prevention' configuration page. The 'SYN Flood Protection' section is active, with the following settings:

- Enable SYN flood protection:
- SYN flood rate:
- SYN flood burst:
- TCP SYN cookies:

	Field Name	Sample value	Explanation
1.	Enable SYN flood	Enable/Disable	Macht den Router resistenter gegen SYN-Flood-Angriffe.
2.	SYN flood rate	"25"	Legen Sie eine Ratenbegrenzung (Pakete/Sekunde) für SYN-Pakete fest, bei deren Überschreitung der Datenverkehr als Flut betrachtet wird.
3.	SYN flood burst	"50"	Setzen Sie eine Burst-Limitierung für SYN-Pakete, oberhalb derer der Datenverkehr als Flood angesehen wird, wenn er die zulässige Rate überschreitet.
4.	TCP SYN cookies	Enable/Disable	Aktivieren Sie die Verwendung von SYN-Cookies (bestimmte Auswahlmöglichkeiten bei der Erstinstallation).

### 7.6.6.2 Entfernte ICMP-Anfragen

Angreifer verwenden ICMP-Echo-Anforderungspakete, die an IP-Broadcast-Adressen von entfernten Standorten an folgende Adressen gerichtet sind  
Denial-of-Service-Angriffe erzeugen.

**Remote ICMP requests**

Enable ICMP requests

Enable ICMP limit

Limit period Second ▾

Limit

Limit burst

	Field Name	Sample value	Explanation
1.	Enable ICMP requests	Enable/Disable	Blockiert den entfernten ICMP-Echo-Anfragetyp.
2.	Enable ICMP limit	Enable/Disable	ICMP Echo-Request Limit im ausgewählten Zeitraum aktivieren
3.	Limit period	Second/Minute/Hour/Day	Wählen Sie, in welchem Zeitraum die ICMP-Echo-Anfrage
4.	Limit	"10"	Maximale ICMP-Echo-Anfragen während des Zeitraums
5.	Limit burst	"5"	Anzeige des maximalen Bursts, bevor der obige Grenzwert eintritt.

### 7.6.6.3 SSH-Angriffsprävention

Prevent SSH( Ermöglicht es einem Benutzer, Befehle in der Eingabeaufforderung einer Maschine auszuführen, ohne dass sie physisch vorhanden sind.  
in der Nähe der Maschine vorhanden sind. ) Angriffe durch Begrenzung der Verbindungen in einem definierten Zeitraum.

**SSH Attack Prevention**

Enable SSH limit

Limit period Second ▾

Limit

Limit burst

	Field Name	Sample value	Explanation
1.	Enable SSH limit	Enable/Disable	Aktiviert die Grenze für ssh-Verbindungen im ausgewählten
2.	Limit period	Second/Minute/Hour/Day	Wählen Sie, in welchem Zeitraum die ssh-Verbindungen begrenzt werden sollen.
3.	Limit	"10"	Maximale ssh-Verbindungen während des Zeitraums
4.	Limit burst	"5"	Anzeige des maximalen Bursts, bevor der obige Grenzwert eintritt.

#### 7.6.6.4 HTTP-Angriffsverhinderung

HTTP-Angriff sendet einen vollständigen, legitimen HTTP-Header, der ein Feld "Content-Length" enthält, um die Größe festzulegen. des Nachrichtentextes, der folgen soll. Allerdings fährt der Angreifer dann fort, den eigentlichen Nachrichtentext an einem extrem hohen Punkt zu senden. langsame Geschwindigkeit (z.B. 1 Byte/110 Sekunden). Da die gesamte Nachricht korrekt und vollständig ist, wird der Zielservers Folgendes tun Versuchen Sie, dem Feld'Content-Length' im Header zu gehorchen und warten Sie, bis der gesamte Text der Nachricht gesendet wurde, und verlangsamt es dadurch.

**HTTP Attack Prevention**

Field Name

Enable HTTP limit

Limit period Second ▼

Limit 10

Limit burst 10

	Field Name	Sample value	Explanation
1.	Enable HTTP limit	Enable/Disable	Begrenzt HTTP-Verbindungen pro Periode
2.	Limit period	Second/Minute/Hour/Day	Wählen Sie, in welchem Zeitraum die HTTP-Verbindungen eingeschränkt werden sollen.
3.	Limit	"10"	Maximale HTTP-Verbindungen während des Zeitraums
4.	Limit burst	"10"	Anzeige des maximalen Bursts, bevor der obige Grenzwert eintritt.

#### 7.6.6.5 HTTPS-Angriffsverhinderung

**HTTPS Attack Prevention**

Field Name

Sample value

Enable HTTPS limit

Limit period Second ▼

Limit 10

Limit burst 10

	Field Name	Sample value	Explanation
1.	Enable HTTPS limit	Enable/Disable	Begrenzt HTTPS-Verbindungen pro Periode
2.	Limit period	Second/Minute/Hour/Day	Wählen Sie, in welchem Zeitraum die HTTPS-Verbindungen
3.	Limit	"10"	Maximale HTTPS-Verbindungen während des Zeitraums
4.	Limit burst	"10"	Anzeige des maximalen Bursts, bevor der obige Grenzwert eintritt.

## 7.7 Statische Routen

Statische Routen bieten die Möglichkeit, eigene Einträge in die interne Routingtabelle des Routers einzugeben.

### Routes

Routes specify over which interface and gateway a certain host or network can be reached.

Static IP Routes

Interface	Target	Netmask	Gateway	Metric	
LAN	192.168.55.0	255.255.255.0	192.168.55.145	0	Delete
Add					
Save					

Field name	Value	Explanation
1. Interface	LAN/WAN/PPP/WAN	Die Zone, in der sich das "Ziel" befindet.
2. Target	IP address	Die Quelle des Datenverkehrs.
3. Netmask	IP mask	Maske, die auf das Ziel angewendet wird, um zu bestimmen, auf welche tatsächliche IP es sich bezieht.
4. Gateway	IP address	Adressen, für die die Routingregel gilt
5. Metric	integer	An wen der Router den gesamten Datenverkehr senden soll, der für die Regel gilt.

Zusätzlicher Hinweis zu Target & Netmask: Sie können eine Regel definieren, die für eine einzelne IP gilt, wie folgt: Ziel - einige IP; Netzmaske - 255.255.255.255.255.255.

Außerdem können Sie eine Regel definieren, die für ein Segment von IPs wie diese gilt: Ziel - einige IP, die das Segment startet; Netzmaske - Netzmaske, die definiert, wie groß das Segment ist. Z.B.:

192.168.55.161	255.255.255.255	Only applies to 192.168.55.161
192.168.55.0	255.255.255.0	Applies to IPs in range 192.168.55.0-192.168.55.255
192.168.55.240	255.255.255.240	Applies 192.168.55.240 - 192.168.55.255
192.168.55.161	255.255.255.0	192.168.55.0 - 192.168.55.255
192.168.0.0	255.255.0.0	192.168.0.0 - 192.168.255.255


## 8 Services

### 8.1 VRRP

#### 8.1.1.1 VRRP LAN-Konfigurationseinstellungen

**VRRP LAN Configuration Settings**

Enable

IP address  

Virtual ID

Priority

Field name	Sample	Explanation
1. Enable	Enable/Disable	VRRP (Virtual Router Redundancy Protocol) für LAN aktivieren
2. IP address	192.168.1.253	Virtuelle IP-Adresse für LANs VRRP (Virtual Router Redundancy
3. Virtual ID	1	Protokoll) Cluster
4. Priority	100	Router mit gleichen IDs werden in derselben VRRP (Virtual VRRP) gruppiert.

#### 8.1.2 Internetverbindung prüfen

**Check internet connection**

Enable

Ping IP address

Ping interval

Ping timeout (sec)

Ping packet size

Ping retry count

Field name	Sample	Explanation
1. Enable	Enable/Disable	Aktivieren Sie die WAN-Verbindungsüberwachung.
2. Ping IP address	8.8.4.4	Ein Host, der ICMP-Pakete (Internet Control Message Protocol) an folgende Adressen sendet
3. Ping interval	10	Zeitintervall in Minuten zwischen zwei Pings
4. Ping timeout (sec)	1	Reaktions-Timeout-Wert, Intervall[1 - 9999].
5. Ping packet size	50	ICMP (Internet Control Message Protocol) Paketgröße, Intervall[0 -]. 1000]
6. Ping retry count	10	Anzahl der fehlgeschlagenen Ping-Versuche, bevor festgestellt wird, dass die Verbindung unterbrochen wurde.

## 8.2 TR-069

TR-069 ist ein Standard, der für die automatische Konfiguration und Verwaltung von Remote-Geräten durch Auto entwickelt wurde.  
Konfigurationsserver (ACS).

### 8.2.1 TR-069 Parameterkonfiguration


**TR-069 Parameters Configuration**

Enable

Enable Periodic Transmission

Sending Interval

User name

Password  

URL

Field name	Sample	Explanation
1. Aktivieren/Deaktivi	Aktivieren/Deaktivieren	Aktivieren/Deaktivieren Aktivieren/Deaktivieren Aktivieren TR-069-Client
2. Periodisch aktivieren	Periodisch aktivieren	Periodisch aktivieren
3. Übertragung	Übertragung aktivieren /	Übertragung aktivieren / deaktivieren Aktivieren Sie die periodische
4. Sendeintervall 100	Sendeintervall 100 Periodische	Sendeintervall 100 Periodische Datenübertragung zur Serverperiode
5. Benutzername	Benutzername admin	Benutzername admin Benutzername für die Authentifizierung am TR-069-
6. Passwort ***** ***** Passwort für die Authentifizierung am TR-069-Server	Passwort ***** Passwort für die Authentifizierung am TR-069-Server	Passwort ***** Passwort für die Authentifizierung am TR-069-Server



## 8.3 Web filter

### 8.3.1 Standortsperr

Site Blocking
Proxy Based Content Blocker

### Site Blocking Settings

**Site Blocking**

Enable

Mode Whitelist ▼

Enable	Host name	
<input checked="" type="checkbox"/>	<input style="width: 100%;" type="text" value="www.yahoo.com"/>	<input type="button" value="Delete"/>

Field name	Sample	Explanation
1. Enable	Enable/Disable	Aktivieren Sie die Blockierung von Websites, die auf dem Hostnamen basieren.
2. Mode	Whitelist/Blacklist	Whitelist - erlaubt jede Seite auf der Liste und blockiert alles andere. Blacklist - blockiert jede Seite auf der Liste und erlaubt alles andere.

### 8.3.2 Proxy-basierter URL-Inhaltsblocker

Site Blocking
Proxy Based Content Blocker

### Proxy Based URL Content Blocker Configuration

**Proxy Based URL Content Blocker**

Enable

Mode Blacklist ▼

**URL Filter Rules**

Enable	URL content	
<input checked="" type="checkbox"/>	<input style="width: 100%;" type="text" value="example.com"/>	<input type="button" value="Delete"/>

Field name	Sample	Explanation
1. Enable	Enable/Disable	Aktivieren Sie die URL-Inhaltsblockierung auf Proxy-Server-Basis. Funktioniert mit HTTP
2. Mode	Whitelist/Blacklist	Whitelist - erlaubt jeden Teil der URL auf der Liste und blockiert alles andere. Blacklist - blockiert jeden Teil der URL auf der Liste und erlaubt alles andere.

## 8.4 NTP

Mit der NTP-Konfiguration können Sie die Zeit des Routers einstellen und synchronisieren.

Field name	Description	Notes
1. Current System time	Lokale Zeit des Routers.	---
2. Time zone	Zeitzone Ihres Landes	---
3. Enable NTP	Aktiviert die Funktionalität	---
4. Update interval	Wie oft wird der Router aktualisiert?	---
5. Count of time synchronization	Gesamtzahl der Zeiten, in denen der Router die folgenden Schritte durchführt	Wenn leer gelassen - die Anzahl ist unendlich.
6. Offset frequency	Stellen Sie die geringe Abweichung der Uhr so ein, dass sie genauer ist.	

Beachten Sie, dass unter Zeitserver mindestens ein Server vorhanden sein muss, da NTP sonst seinen Zweck nicht erfüllt.

## 8.5 RS232/RS485

Die RS232- und RS485-Funktionen sind so konzipiert, dass sie die verfügbaren seriellen Schnittstellen des Routers nutzen. Serielle Schnittstellen die Möglichkeit für ältere Geräte, Zugang zu IP-Netzen zu erhalten.

### 8.5.1 RS232

**RS232 Serial Configuration**

Enabled

Baud rate

Data bits

Parity

Stop bits

Flow control

Serial type

Field name	Sample	Explanation
1. Enabled	Enable/Disable	Aktivieren Sie das Kontrollkästchen, um die Funktion der seriellen Schnittstelle
2. Baud rate	300 / 115200	Wählen Sie die Kommunikationsgeschwindigkeit der seriellen Schnittstelle.
3. Data bits	5 - 8	Gibt an, wie viele Bits für ein Zeichen verwendet werden sollen.
4. Parity	None / Odd / Even	Wählen Sie die Einstellung des Paritätsbits, das für die Fehlererkennung bei der Datenübertragung verwendet wird.
5. Stop bits	1 / 2	Gibt an, wie viele Stoppbits verwendet werden, um das Ende des Zeichens zu erkennen.
6. Flow control	None / RTS- CTS / Xon- Xoff	Gibt an, welche Art von Zeichen für die Ablaufsteuerung verwendet werden sollen.
7. Serial type	Console / over IP / Modem	Gibt die Funktion der seriellen Schnittstelle an

#### 8.5.1.1 RS232 Steckerbelegung

Der RS232-Anschluss dieses Geräts ist eine DCE-Buchse. DCE steht für Datenkommunikationsgeräte.



Pin	Name*	Description*	Direction on this device
1	DCD	Data Carrier Detect	Output
2	RXD	Receive Data	Output
3	TXD	Transmit Data	Input
4	DTR	Data Terminal Ready	Input
5	GND	Signal Ground	-
6	DSR	Data Set Ready	Output
7	RTS	Ready To Send	Input
8	CTS	Clear to send	Output
9	RI	Ring indicator	Output (connected to +5V permanently via 4.7k resistor)

\*Die Namen und Beschreibungen, die die Signalrichtung angeben (z.B. TXD, RXD, RTS, RTS, CTS, DTR und DSR), werden genannt. aus Sicht der DEE-Vorrichtung.

#### 8.5.1.2 Kabel

RUT9xx hat eine DCE-Buchse. Um ein Standard-DTE-Gerät daran anzuschließen, verwenden Sie eine durchgehende Buchse/Stecker.

RS232-Kabel:



Um ein anderes DCE-Gerät an den RUT9xx anzuschließen, sollte ein Nullmodem (gekreuzt) Female/Female Kabel verwendet werden:



Die maximale Kabellänge beträgt 15 Meter, oder die Kabellänge entspricht einer Kapazität von 2500-pF (bei einer 19200 Baudrate).

Die Verwendung von Kabeln mit geringerer Kapazität kann den Abstand vergrößern. Die Reduzierung der Kommunikationsgeschwindigkeit kann auch das Maximum erhöhen.

Kabellänge. Die folgende Tabelle listet die Übertragungsrate im Verhältnis zur maximalen Kabellänge auf.

### 8.5.2 RS485

RS-485 ist ein Standard für die differentielle serielle Datenübertragung für den Einsatz in großen Entfernungen oder rauen Umgebungen.

**RS485 Serial Configuration**

Enabled

Baud rate

Data bits

Parity

Stop bits

Flow control

Serial type

Field name	Sample	Explanation
1. Enabled	Enable/Disable	Aktivieren Sie das Kontrollkästchen, um die Funktion der seriellen Schnittstelle zu aktivieren.
2. Baud rate	300 / 115200	Wählen Sie die Kommunikationsgeschwindigkeit der seriellen Schnittstelle.
3. Data bits	5 - 8	Gibt an, wie viele Bits für ein Zeichen verwendet werden sollen.
4. Parity	None / Odd / Even	Wählen Sie die Einstellung des Paritätsbits, das für die Fehlererkennung bei der Datenübertragung verwendet wird.
5. Stop bits	1 / 2	Gibt an, wie viele Stoppbits verwendet werden, um das Ende des Zeichens zu erkennen.
6. Flow control	None / RTS- CTS / Xon- Xoff	Gibt an, welche Art von Zeichen für die Ablaufsteuerung verwendet werden sollen.
7. Serial type	Console / over IP / Modem	Gibt die Funktion der seriellen Schnittstelle an

#### 8.5.2.1 Maximale Datenrate vs. Übertragungsleitungslänge

RS-485-Standard kann für Netzwerklängen bis zu 1200 Metern verwendet werden, aber die maximal nutzbare Datenrate sinkt.

mit zunehmender Übertragungslänge. Gerät, das mit maximaler Datenrate (10Mbps) arbeitet, ist auf die Übertragungslänge beschränkt.

von etwa 12 Metern, während die Datenrate von 100kbps eine Entfernung von bis zu 1200 Metern erreichen kann.

maximale Übertragungslänge und Datenrate können mit Hilfe von Näherungswerten berechnet werden.

:

$$L_{\max}(\text{m}) = 10^8$$

DR (bit/s) Dabei ist  $L_{\max}$  die maximale Übertragungslänge in Metern und DR die maximale Datenrate in Bit pro Sekunde.

Twisted Pair ist das bevorzugte Kabel für RS-485-Netzwerke. Twisted-Pair-Kabel nehmen Störungen und andere Störungen auf.

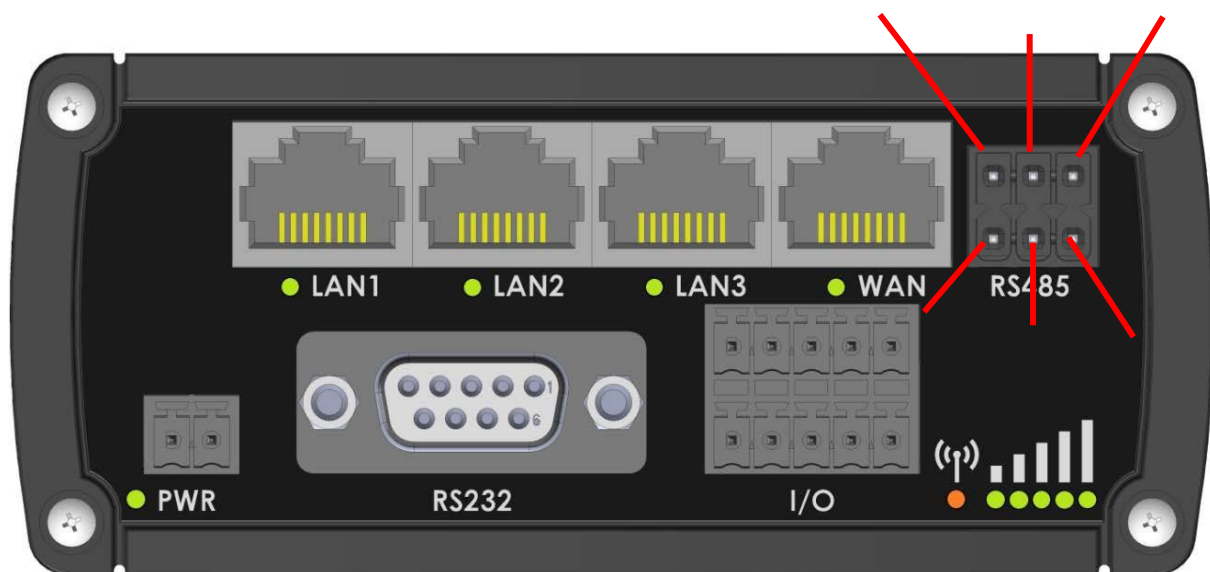
elektromagnetisch induzierte Spannungen als Gleichtaktsignale, die von den Differenzempfängern abgelehnt werden.

### 8.5.2.2 Cable type

Empfohlene Kabelparameter:

Parameter	Value
Cable Type	22-24 AWG, 2 – pair (used for full-duplex networks ) or 1-pair (used for half duplex networks). One additional wire for ground connection is needed.
Characteristic cable Impedance	120 $\Omega$ @ 1MHz
Capacitance (conductor to conductor)	36 pF/m
Propagation Velocity	78% (1.3 ns/ft)

### 8.5.2.3 RS485 Stecker-Pin-Belegung



Name	Description	Type
D_P	Driver positive signal	Differential Output
D_N	Driver negative signal	Differential Output
R_P	Receiver positive signal	Differential input
R_N	Receiver negative signal	Differential input
Ground	Device ground	Differential Output

### 8.5.2.4 2- Kabel- und 4-Draht-Netzwerke

Nachfolgend finden Sie ein Beispiel für eine elektrische 4-Draht-Netzwerkverbindung. Im Beispiel sind 3 Geräte dargestellt. Einer von die Geräte sind Master und weitere zwei Slaves. An jedem Kabelende befinden sich Abschlusswiderstände. Vierdrahtnetze

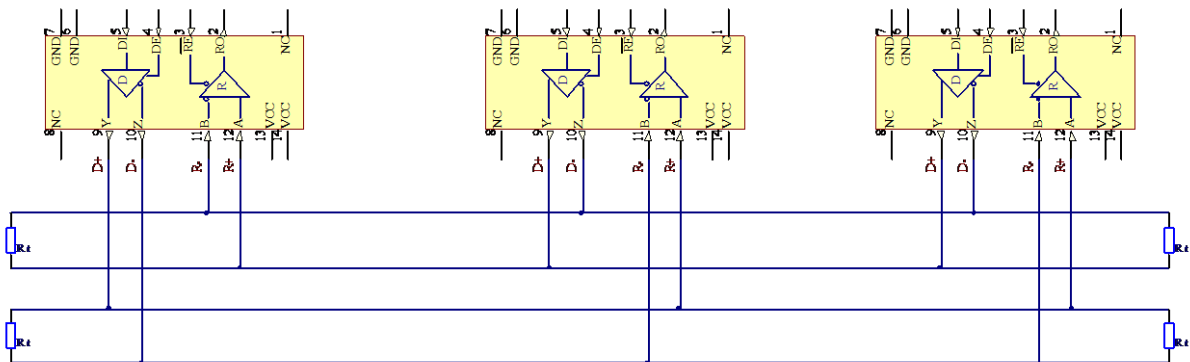
besteht aus einem "Master", dessen Sender mit jedem der "Slave"-Empfänger auf einem verdrehten Paar verbunden ist. Der "Sklave".

Die Sender sind alle über ein zweites Twisted-Pair mit dem "Master"-Empfänger verbunden.

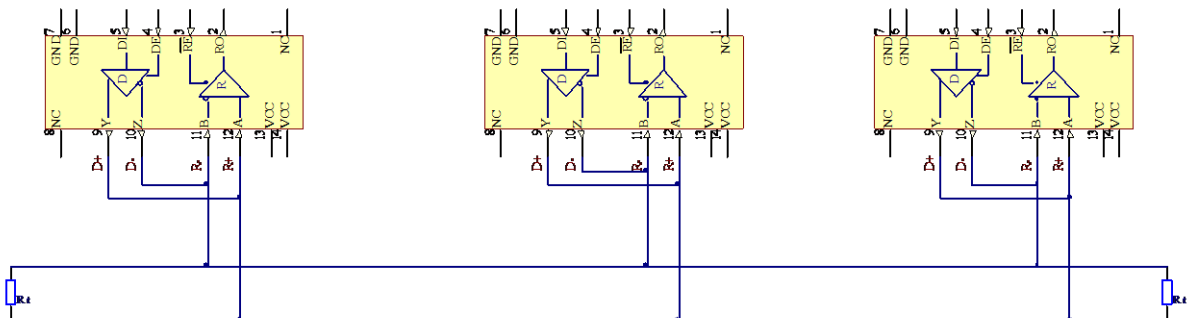
**D\_P R\_P N/C**

**D\_N**

**R\_N Ground**



Beispiel 2-Draht-Netzwerk-Elektroanschluss: Um die 2-Draht-RS-485-Konfiguration im Teltonika-Router zu ermöglichen, können Sie `D_P` mit `R_P` und `D_N` mit `R_N` an der RS-485-Buchse des Gerätes verbunden werden. Die Abschlusswiderstände sind an jedem Kabel angebracht.  
Ende.



### 8.5.2.5 Kündigung

#### Wann ist zu verwenden (Jumper setzen)?

Der Abschlusswiderstand, der dem Wellenwiderstand des Kabels entspricht, muss an jedem Ende der Leitung angeschlossen werden.

Kabel, um die Reflexion und das Klingeln der Signale zu reduzieren, wenn die Kabellängen relativ lang werden. Anstiegszeit des RUT9XX

Der RS-485-Treiber ist ca. 5ns, so dass die maximale Länge des unbeendeten Kabels ca. 12cm beträgt. Als Übertragungsleitung werden Kabel verwendet.

immer länger als 12 cm, der Abschluss ist immer zwingend erforderlich, wenn sich RUT9xx am Ende des Kabels befindet.

#### Wenn nicht verwendet (Jumper entfernen)

Wenn Ihre RS-485 aus mehr als zwei Geräten besteht und sich der RUT9xx-Router nicht am Ende der Leitung befindet, für

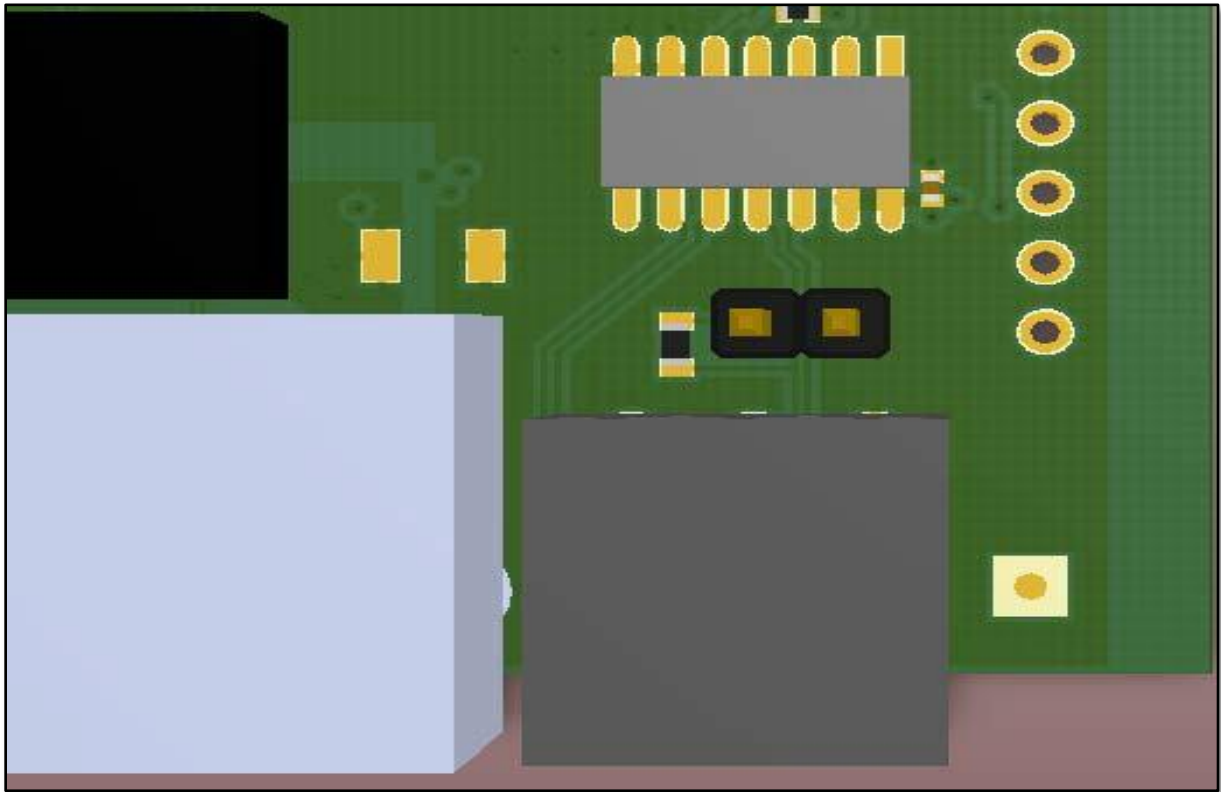
Beispiel in der Mitte, der Abschlusswiderstand RUT9xx muss deaktiviert werden, in diesem Fall bitte bei anderen

Vorrichtungen, die sich an den Enden der Linie befinden.

#### So aktivieren Sie die Kündigung

120  $\Omega$  Der Abschlusswiderstand ist auf der RUT9xx-Platine enthalten und kann durch Kurzschlusskontakte aktiviert werden (siehe Abschnitt

Bild unten) und setzen Sie einen Jumper im Raster 2,54 mm:



#### 8.5.2.6 Anzahl der Geräte im RS-485-Netzwerk

Ein RUT9xx RS-485-Treiber kann maximal 32 Empfänger ansteuern, vorausgesetzt, die Eingangsimpedanz des Empfängers ist  $12k\Omega$ . Wenn die Empfängerimpedanzen höher sind, steigt die maximale Anzahl der Empfänger im Netzwerk. Jede Kombination von Empfängertypen können miteinander verbunden werden, sofern ihre Parallelimpedanz  $R_{Load} > 375\Omega$  nicht überschreitet.

### 8.5.3 Modi verschiedener serieller Typen in RS232 und RS485

#### 8.5.3.1 Konsolenmodus

In diesem Modus wird die serielle Schnittstelle als Linux-Konsole des Gerätes eingerichtet. Es kann für Debug-Zwecke verwendet werden, um zu erhalten den Status der Vorrichtung oder um sie zu steuern.

#### 8.5.3.2 Über IP-Modus

In diesem Modus stellt der Router die Verbindung zum TPC/IP-Netzwerk für die über serielle Schnittstellen angeschlossenen Geräte her.



Serial type	Over IP
Protocol	TCP
Mode	Client
Server Address	1.1.1.1
Keepalive interval (s)	120
Port	123

Field name	Explanation
1. Protocol	Wählen Sie das für die Verbindung verwendete Protokoll aus.
2. Mode	Wählen Sie die Rolle des angeschlossenen Geräts aus. Es kann entweder auf den Eingang warten.
3. Server Address	Geben Sie die IP-Adresse oder den Hostnamen des Remote-Servers an, mit dem die Verbindung hergestellt werden soll.
4. Aufbewahrungsintervall	Geben Sie das Intervall in Sekunden an, das verwendet wird, um die Verbindung am Leben zu erhalten.
5. TCP port	Geben Sie die Portnummer an, die verwendet wird, um auf eingehende Verbindungen zu warten. (Server) oder Port des entfernten Servers (Client)

### 8.5.3.3 Modem mode

In diesem Modus imitiert der Router ein DFÜ-Modem. Die Verbindung zum TCP/IP-Netzwerk kann über AT hergestellt werden.

Die Verbindung kann durch das über die serielle Schnittstelle mit ATD-Befehl angeschlossene Gerät eingeleitet werden:

ATD<host>:<port>. Wenn die Einstellungen für die direkte Verbindung angegeben sind, ist die Verbindung zum Server immer aktiv. Der Datenmodus kann

Die eingehende Verbindung wird durch Senden von RING an die serielle Schnittstelle angezeigt.

Serial type	Modem
Direct connect	1.1.1.1:321
TCP port	123

Field name	Explanation
1. Direct connect	Geben Sie IP-Adresse (oder Hostname) und TCP-Port des Remote-Servers an.
2. TCP port	Geben Sie die TCP-Portnummer an, die verwendet wird, um auf eingehende Verbindungen zu warten. Lassen Sie es leer, um eingehende Verbindungen zu deaktivieren.

Dies ist der AT-Befehlssatz, der im Modemmodus der seriellen Schnittstellen verwendet wird:

Command	Description	Usage
A	Eingehenden Anruf	Um eine eingehende Verbindung zu beantworten: ATA
D	Wählen Sie eine Nummer	Um eine Datenverbindung herzustellen: ATD<host>:<port>:<port> Um in den Datenmodus mit den Einstellungen für die Direktverbindung zu gelangen: ATD
E	Lokales Echo	Schalten Sie das lokale Echo ein: ATE1 Schalten Sie das lokale Echo aus: ATE0
H	Aktuellen Anruf auflegen	Um die Datenverbindung zu beenden: ATH
O	Zurück zum Datenmodus	Um aus dem Befehlsmodus in den Datenmodus zurückzukehren: ATO
Z	Auf Standard zurücksetzen	So setzen Sie das Modem auf die Standardkonfiguration zurück: ATZ

#### 8.5.3.4 Modbus-Gateway-Modus

Serial type: Modbus gateway

Listening IP: 0.0.0.0

Port: 502

Slave ID: 1

Field name	Explanation
1. Listening IP	IP-Adresse, an der das Modbus-Gateway auf eingehende Verbindungen warten soll.
2. Port	Port zur Verwendung für die Kommunikation
3. Slave ID	ID des mit dem Router verbundenen Slave-Gerätes

## 8.6 VPN

### 8.6.1 OpenVPN

VPN (*Virtual Private Network*) ist ein Verfahren zur sicheren Datenübertragung über ein unsicheres öffentliches Netzwerk. Dieser Abschnitt erklärt, wie man OpenVPN konfiguriert, die Implementierung von VPN, das vom Router unterstützt wird. Ein Bild unten zeigt die Standardliste der OpenVPN-Konfigurationen, die leer ist, so dass Sie eine neue definieren müssen.

Konfiguration, um eine beliebige OpenVPN-Verbindung herzustellen. Um es zu erstellen, geben Sie unter "Neu" den gewünschten Konfigurationsnamen ein.

Konfigurationsname" Feld, wählen Sie die Geräterolle aus der Dropdown-Liste "Rolle". Um z.B. einen OpenVPN-Client zu erstellen mit

Konfigurationsname Demo, wählen Sie die Client-Rolle, nennen Sie sie "Demo" und drücken Sie die Schaltfläche "Add New", wie im Folgenden gezeigt.

Bild.

OpenVPN IPsec GRE Tunnel PPTP L2TP

## OpenVPN

### OpenVPN Configuration

Tunnel name	TUN/TAP	Protocol	Port	Enabled
<i>There are no openVPN configurations yet</i>				

Role:  New configuration name:

OpenVPN IPsec GRE Tunnel PPTP L2TP

New OpenVPN instance was created successfully. Configure it now

## OpenVPN

### OpenVPN Configuration

Tunnel name	TUN/TAP	Protocol	Port	Enabled	
Client_demo	Tun_c_demo	UDP	1194	No	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Role:  New configuration name:

Um bei bestimmten Konfigurationseinstellungen zu sehen, drücken Sie die Schaltfläche "Bearbeiten", die sich im neu erstellten Konfigurationseintrag befindet. Eine neue Seite mit detaillierter Konfiguration erscheint, wie in der folgenden Abbildung gezeigt (TLS-Clientbeispiel).

OpenVPN	IPsec	GRE Tunnel	PPTP	L2TP
<b>OpenVPN Instance: Client_demo</b>				
<b>Main Settings</b>				
Enable <input type="checkbox"/>				
TUN/TAP <input type="text" value="TUN (tunnel)"/>				
Protocol <input type="text" value="UDP"/>				
Port <input type="text" value="1194"/>				
LZO <input checked="" type="checkbox"/>				
Encryption <input type="text" value="BF-CBC 128 (default)"/>				
Authentication <input type="text" value="TLS"/>				
Remote host/IP address <input type="text" value="215.45.60.66"/>				
Resolve retry <input type="text" value="Infinite"/>				
Keep alive <input type="text" value="10 60"/>				
Remote network IP address <input type="text" value="10.0.0.0"/>				
Remote network IP netmask <input type="text" value="255.255.255.0"/>				
Certificate authority <input type="text" value=""/> <input type="button" value="Browse..."/>				
Client certificate <input type="text" value=""/> <input type="button" value="Browse..."/>				
Client key <input type="text" value=""/> <input type="button" value="Browse..."/>				

Es kann mehrere Server/Client-Instanzen geben.

OpenVPN	IPsec	GRE Tunnel	PPTP	L2TP
<b>OpenVPN Instance: Client_demo</b>				
<b>Main Settings</b>				
Enable <input type="checkbox"/>				
TUN/TAP <input type="text" value="TUN (tunnel)"/>				
Protocol <input type="text" value="UDP"/>				
Port <input type="text" value="1194"/>				
LZO <input checked="" type="checkbox"/>				
Encryption <input type="text" value="BF-CBC 128 (default)"/>				
Authentication <input type="text" value="TLS"/>				
Remote host/IP address <input type="text" value="215.45.60.66"/>				
Resolve retry <input type="text" value="Infinite"/>				
Keep alive <input type="text" value="10 60"/>				
Remote network IP address <input type="text" value="10.0.0.0"/>				
Remote network IP netmask <input type="text" value="255.255.255.0"/>				
Certificate authority <input type="text"/> <input type="button" value="Browse..."/>				
Client certificate <input type="text"/> <input type="button" value="Browse..."/>				
Client key <input type="text"/> <input type="button" value="Browse..."/>				

Sie können hier benutzerdefinierte Einstellungen für Ihre VPN-Anforderungen vornehmen. Nachfolgend finden Sie eine Zusammenfassung der einstellbaren Parameter:

Field name	Explanation
1. Enabled	Schaltet die Konfiguration ein und aus. Dies muss ausgewählt werden, damit die Konfiguration aktiv wird.
2. TUN/TAP	Wählt den Typ der virtuellen VPN-Schnittstelle aus. TUN wird jedoch am häufigsten in typischen VPN-Verbindungen auf IP-Ebene eingesetzt, Für einige Ethernet-Bridging-Konfigurationen ist TAP erforderlich.
3. Protocol	Definiert ein Transportprotokoll, das von der Verbindung verwendet wird. Sie können hier zwischen TCP und UDP wählen.
4. Port	Definiert die TCP- oder UDP-Portnummer (stellen Sie sicher, dass dieser Port von der Firewall zugelassen
5. LZO	Diese Einstellung aktiviert die LZO-Kompression. Mit LZO-Komprimierung erzeugt Ihre VPN-Verbindung weniger Netzwerkverkehr, was jedoch eine höhere CPU-Last des Routers bedeutet. Verwenden Sie es vorsichtig bei hohem Datenverkehr oder niedrigen CPU-Ressourcen.
6. Encryption	Wählt den Algorithmus für die Paketverschlüsselung aus.
7. Authentication	Legt den Authentifizierungsmodus fest, der zur Sicherung von Datensitzungen verwendet wird. Zwei Möglichkeiten hast du hier: "Statisch" bedeutet, dass OpenVPN-Client und -Server den gleichen geheimen Schlüssel verwenden, der mit der Option "Static pre-shared key" auf den Router hochgeladen werden muss. Der "Tls"-Authentifizierungsmodus verwendet Zertifikate vom Typ X.509. Abhängig vom gewählten OpenVPN-Modus (Client oder Server) müssen Sie diese Zertifikate auf den Router hochladen:

- Für den Kunden: Zertifizierungsstelle (CA), Kundenzertifikat, Kundenschlüssel.  
 Für Server: Zertifizierungsstelle (CA), Serverzertifikat, Serverschlüssel und Diffie-Hellman (DH) Zertifikat, das für den Schlüsselaustausch über unsichere Datennetze verwendet wird.  
 Alle Erwähnungszertifikate können mit Hilfe von OpenVPN- oder OpenSSL-Dienstprogrammen auf jedem beliebigen Host-Computer generiert werden. Die Erstellung und Theorie des Zertifikats liegt außerhalb des Umfangs dieser Bedienungsanleitung.
8. Remote host IP address IP-Adresse des OpenVPN-Servers (gilt nur für die Client-Konfiguration).
  9. Resolve Retry Legt die Zeit in Sekunden fest, in der versucht wird, den Server-Hostnamen periodisch aufzulösen, falls der Fehler beim ersten Auflösen auftritt, bevor eine Service-Exception generiert wird.
  10. Keep alive Definiert zwei Zeitintervalle: eines wird verwendet, um periodisch ICMP-Anfragen an den OpenVPN-Server zu senden, und ein weiteres definiert ein Zeitfenster, das zum Neustart des OpenVPN-Dienstes verwendet wird, wenn während des Zeitfensters keine ICMP-Anfrage empfangen wird. Beispiel Keep Alive "10 60" halten
  11. Remote network IP address IP-Adresse des entfernten Netzwerks, ein aktuelles LAN-Netzwerk hinter einem anderen VPN-Endpoint.
  12. Remote network IP netmask Subnetzmaske des entfernten Netzwerks, ein aktuelles LAN-Netzwerk hinter einem anderen VPN-Endpoint.
  13. Certificate Die Zertifizierungsstelle ist eine Einrichtung, die digitale Zertifikate ausstellt. Ein digitales Zertifikat bescheinigt das Eigentum an einem öffentlichen Schlüssel durch den genannten Gegenstand des Zertifikats.
  14. Client certificate Client-Zertifikat ist eine Art digitales Zertifikat, das von Client-Systemen verwendet wird, um authentifizierte Anfragen an einen Remote-Server zu stellen. Client-Zertifikate spielen eine Schlüsselrolle bei vielen gegenseitigen Authentifizierungsdesigns und bieten eine starke Sicherheit für die Identität eines Antragstellers.
  15. Client key Authentifizierung des Clients am Server und Feststellung, wer genau er ist.

Nach der Einstellung eines dieser Parameter drücken Sie die Taste "Save". Einige der ausgewählten Parameter werden im Fenster

Konfigurationslistentabelle. Sie sollten sich auch darüber im Klaren sein, dass der Router für jeden OpenVPN-Dienst einen eigenen OpenVPN-Dienst startet.

Konfigurationseintrag (wenn er natürlich als aktiv definiert ist), so dass der Router die Möglichkeit hat, gleichzeitig als Server und Client zu fungieren.  
 Zeit.

### 8.6.2 IPsec

Der IPsec-Protokoll-Client ermöglicht es dem Router, eine sichere Verbindung zu einem IPsec-Peer über das Internet herzustellen.

IPsec wird in zwei Modi unterstützt - Transport und Tunnel. Der Transportmodus erzeugt einen sicheren Punkt-zu-Punkt-Kanal zwischen

zwei Wirte. Der Tunnelmodus kann verwendet werden, um eine sichere Verbindung zwischen zwei entfernten LANs aufzubauen, die als VPN-Lösung dienen.

Das IPsec-System verwaltet zwei Datenbanken: Security Policy Database (SPD), die definiert, ob IPsec auf einen

Paket oder nicht und geben Sie an, welches/welche IPsec-SA angewendet wird und Security Association Database (SAD), die den Schlüssel von jedes IPsec-SA.

Für die IPsec-Kommunikation ist der Aufbau der Security Association (IPsec-SA) zwischen zwei Peers erforderlich. Es

kann durch manuelle oder automatisierte Konfiguration erfolgen.

Hinweis: Der Router beginnt mit der Einrichtung des Tunnels, wenn Daten vom Router an den entfernten Standort über den Tunnel gesendet werden. Für automatische

Tunnelaufbau verwendet Tunnel Keep Alive Funktion.

Explanation

OpenVPN IPsec GRE Tunnel PPTP L2TP

## IPsec

### IPsec Configuration

Enable

Mode

Enable NAT traversal

Enable initial contact

My identifier type

My identifier

Pre shared key

Remote VPN endpoint

Enable DPD

Delay (sec)

Field name	Explanation
1. Enable	Kontrollkästchen zur Aktivierung von IPsec.
2. Mode	Wählen Sie den Modus "Main", "Aggressive" oder "Base" entsprechend Ihrer IPsec-Serverkonfiguration.
3. Enable NAT traversal	Aktivieren Sie diese Funktion, wenn Client zu Client Anwendungen verwendet werden
4. Enable initial contact	Aktivieren Sie dies, um eine INITIAL-KONTAKT-Nachricht zu senden.
5. My identifier type	Setzt die Geräteerkennung für den IPsec-Tunnel. Z.B. können Sie Ihre IP-Adresse
6. My identifier	Setzt die Geräteerkennung für den IPsec-Tunnel.
7. Preshare key	Falls RUT über eine private IP verfügt, sollte sein Identifikator seine eigene LAN-Netzwerkadresse sein. Auf diese Weise ist der RoadWarrior-Ansatz möglich.
8. Remote VPN endpoint	Geben Sie das Authentifizierungsgeheimnis[string] an. Die Länge des Secrets hängt vom gewählten Algorithmus ab, z.B. 128 Bit langes Secret ist 16 Zeichen lang, 128 / 8 Bit (ein Zeichen) = 16.
9. Enable DPD	
10. Delay (sec)	Setzt die IP-Adresse des entfernten IPsec-Servers.

**Phase 1** and **Phase 2** muss entsprechend der IPSec-Serverkonfiguration, also Algorithmen, konfiguriert werden, Authentifizierung und Lebensdauer der einzelnen Phasen müssen identisch sein.

**Phase**

The phase must match with another incoming connection to establish IPSec

**Phase 1** **Phase 2**

Encryption algorithm 3DES ▼

Hash algorithm SHA1 ▼

DH group MODP768 ▼

Lifetime (sec) 28800

**Phase**

The phase must match with another incoming connection to establish IPSec

**Phase 1** **Phase 2**

Encryption algorithm 3DES ▼

PFS group MODP768 ▼

Authentication HMAC\_SHA1 ▼

Life time (sec) 3600

**Remote Network Secure Group** - Legen Sie die Informationen zum Remote-Netzwerk (Secure Policy Database) fest. Es muss LAN sein. Netzwerk des entfernten IPSec-Hosts.

**Remote Network Secure Group**

IP address

Subnet mask

**Tunnel Keep Alive**

Allows sending ICMP echo requests to the remote tunnel network

Enable

Host

Ping period (sec)

Field name	Explanation
1. Tunnel keep alive	Ermöglicht das Senden von ICMP-Echo-Anforderungen (Ping-Dienstprogramm) an das entfernte Tunnelnetzwerk. Mit dieser Funktion kann der IPSec-Tunnel automatisch gestartet werden.
2. Enable	Diese Funktion sollte jedes Mal verwendet werden.
3. Host	Ermöglicht das Senden von ICMP-Echo-Anfragen an das entfernte Tunnelnetzwerk.
4. Ping period (sec)	Geben Sie die IP-Adresse ein, an die ICMP-Echo-Anfragen gesendet werden sollen.

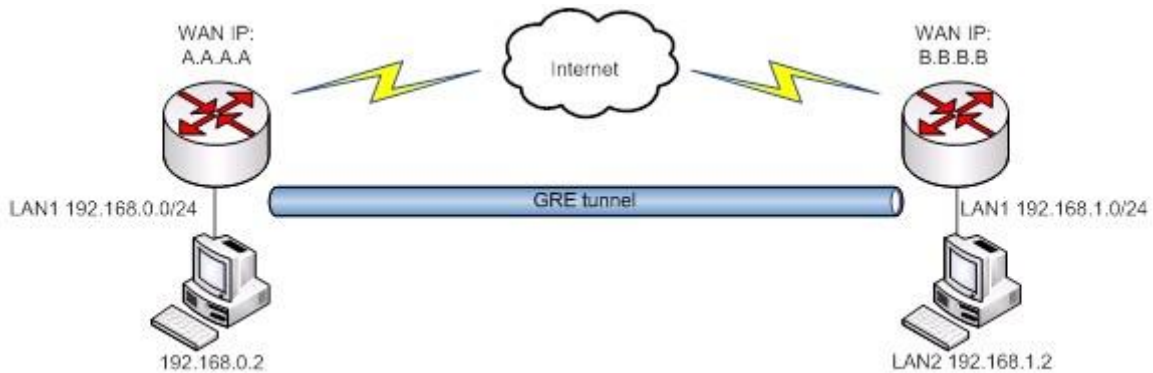


### 8.6.3 GRE Tunnel

GRE (Generic Routing Encapsulation RFC2784) ist eine Lösung zum Tunneling von RFC1812 privatem Adressraumverkehr.

über ein TCP/IP-Zwischennetzwerk wie das Internet. GRE-Tunneling verwendet keine Verschlüsselung, sondern kapselt einfach nur.

Daten und sendet sie über das WAN.



Im Beispiel-Netzwerkdiagramm sind zwei entfernte Netzwerke LAN1 und LAN2 verbunden.

Um einen GRE-Tunnel zu erstellen, muss der Benutzer die folgenden Parameter kennen:

1. Quell- und Ziel-IP-Adressen.
2. Lokale IP-Adresse des Tunnels
3. IP-Adresse des entfernten Netzwerks und Subnetzmaske.

Field name	OpenVPN	IPsec	GRE Tunnel	PPTP	L2TP
<b>Gre-tunnel Instance: Gre_tunnel</b>					
<b>Main Settings</b>					
Enabled	<input checked="" type="checkbox"/>				
Remote endpoint IP address	<input type="text" value="84.148.7.87"/>				
Remote network	<input type="text" value="192.168.2.0"/>				
Remote network netmask	<input type="text" value="24"/>				
Local tunnel IP	<input type="text" value="10.0.0.1"/>				
Local tunnel netmask	<input type="text" value="24"/>				
MTU	<input type="text" value="1500"/>				
TTL	<input type="text" value="255"/>				
PMTUD	<input checked="" type="checkbox"/>				
Enable Keep alive	<input checked="" type="checkbox"/>				
Keep Alive host	<input type="text"/>				
Keep Alive interval	<input type="text"/>				

Field name	Explanation
1. Enabled	Aktivieren Sie das Kontrollkästchen, um die Funktion GRE Tunnel zu aktivieren.
2. Remote endpoint IP address	Geben Sie die Remote-WAN-IP-Adresse an.
3. Remote network	IP-Adresse des LAN-Netzwerks auf dem Remote-Gerät.
4. Remote network netmask	Netzwerk des LAN-Netzwerks auf dem Remote-Gerät. Bereich[0-32].
5. Local tunnel IP	Lokale virtuelle IP-Adresse. Kann nicht im gleichen Subnetz wie das LAN-Netzwerk liegen.
6. Local tunnel netmask	Netzwerk mit lokaler virtueller IP-Adresse. Bereich (0-32)
7. MTU	Geben Sie die maximale Übertragungseinheit (MTU) eines Kommunikationsprotokolls einer Schicht in Bytes an.
8. TTL	Geben Sie den festen Time-to-Live (TTL)-Wert für getunnelte Pakete an[0-255]. Die 0 ist ein spezieller Wert, was bedeutet, dass Pakete den TTL-Wert erben.
9. PMTUD	Aktivieren Sie das Kontrollkästchen, um die Erkennung der maximalen Übertragungseinheit zu aktivieren. (PMTUD) Status in diesem Tunnel.
10. Aktivieren Sie Keep alive	Es gibt einer Seite die Möglichkeit, Keepalive-Pakete von und zu einem entfernten Router zu senden und zu empfangen, auch wenn der entfernte Router GRE Keepalives nicht unterstützt.
11. Alive Host beibehalten	Behalten Sie die IP-Adresse des aktiven Hosts. Vorzugsweise IP-Adresse, die zum LAN gehört. Netzwerk auf dem Remote-Gerät.
12. Keep Alive interval	Zeitintervall für Keep Alive. Bereich [0 - 255].

### 8.6.4 PPTP

Point-to-Point Tunneling Protocol (PPTP) ist ein Protokoll (Satz von Kommunikationsregeln), das es Unternehmen ermöglicht, Folgendes zu tun  
 ihr eigenes Unternehmensnetzwerk durch private "Tunnel" über das öffentliche Internet zu erweitern. Effektiv verwendet ein Unternehmen eine Weitverkehrsnetz als ein einziges großes lokales Netz. Ein Unternehmen muss keine eigenen Leitungen mehr für großflächige Anwendungen mieten. Kommunikation, kann aber die öffentlichen Netze sicher nutzen. Diese Art der Zusammenschaltung wird als Virtual Private bezeichnet. Netzwerk (VPN).

OpenVPN	IPsec	GRE Tunnel	PPTP	L2TP
<b>PPTP Server Instance: Pptpd_server</b>				
<b>Main Settings</b>				
Enable <input type="checkbox"/>				
Local IP <input type="text" value="192.168.0.1"/>				
Remote IP range start <input type="text" value="192.168.0.20"/>				
Remote IP range end <input type="text" value="192.168.0.30"/>				
User name	Password	User IP		
<input type="text" value="youruser"/>	<input type="password" value="....."/>	<input type="text"/>	<input type="button" value="Delete"/>	
<input type="button" value="Add"/>				
<input type="button" value="Save"/>				

Field name	Explanation
1. Enable	Aktivieren Sie das Kontrollkästchen, um die PPTP-Funktion zu aktivieren.
2. Local IP	IP-Adresse dieses Gerätes (RUT)
3. Remote IP range begin	IP-Adressvermietungen beginnen
4. Remote IP range end	IP-Adressvermietungen Ende
5. Username	Benutzername für die Verbindung zum PPTP-Server (dieser)
6. Password	Passwort für die Verbindung zum PPTP-Server

### 8.6.5 L2TP

Ermöglicht die Einrichtung eines L2TP-Servers oder -Clients und bei Bedarf die Verwendung mit IPsec (L2TP/IPSec). Nachfolgend finden Sie L2TP Beispiel einer Serverkonfiguration.

The screenshot shows a web interface for configuring an L2TP server instance. At the top, there are tabs for 'OpenVPN', 'IPsec', 'GRE Tunnel', 'PPTP', and 'L2TP'. The current instance is named 'L2tpd\_server'. Under the 'Main Settings' section, there is an 'Enable' checkbox, a 'Local IP' field containing '192.168.0.1', a 'Remote IP range begin' field containing '192.168.0.20', and a 'Remote IP range end' field containing '192.168.0.30'. Below this is a table for user management with columns 'User name' and 'Password'. One user is listed with the name 'user' and a masked password. There are 'Add', 'Delete', and 'Save' buttons.

Field name	Explanation
1. Enable	Aktivieren Sie das Kontrollkästchen, um die Funktion GRE Tunnel zu aktivieren.
2. Local IP	IP-Adresse dieses Gerätes (RUT)
3. Beginn des Remote-IP-Bereichs	IP-Adressvermietungen beginnen
4. Ferngesteuertes IP-Bereichsende	IP-Adressvermietungen Ende
5. Username	Benutzername für die Verbindung zum L2TP-Server (dieser)
6. Password	Passwort für die Verbindung zum L2TP-Server

Die Client-Konfiguration ist noch einfacher, da **nur Server IP, Benutzername und Passwort benötigt werden.**

## 8.7 Dynamic DNS

Dynamic DNS (DDNS) ist ein Domain Name Service, der es ermöglicht, dynamische IP-Adressen mit statischem Hostnamen zu verknüpfen.

Um diese Funktion nutzen zu können, sollten Sie sich zunächst beim DDNS-Dienstleister registrieren (Beispielliste ist in der Beschreibung angegeben).

Sie verfügen über Hinzufügen/Löschen-Schaltflächen, um verschiedene DDNS-Konfigurationen gleichzeitig zu verwalten und zu nutzen!

Sie können viele verschiedene DDNS-Hostnamen im Hauptabschnitt DDNS-Konfiguration konfigurieren.

DDNS Configuration			
DDNS Name	Hostname	Status	Enabled
Myddns	yourhost.example.org	N/A	No
Demo	mypersonaldomain.dyndns.org	N/A	No

New configuration name:

Um die ausgewählte Konfiguration zu bearbeiten, klicken Sie auf Bearbeiten.

DDNS	
Enable	<input type="checkbox"/>
Status	N/A
Service	3322.org
Hostname	yourhost.example.org
User name	your_username
Password	..... <input type="button" value="eye"/>
IP source	Custom
Network	WAN
IP renew interval (min)	10
Force IP renew (min)	472

Field name	Value	Explanation
1. Enable	-	Enables current DDNS configuration.
2. Status	-	Zeitstempel des letzten IP-Checks oder Updates.
3. Service	1. dydns.org 2. 3322.org 3. no-ip.com 4. easydns.com 5. zoneedit.com	Ihr dynamischer DNS-Dienstleister, der aus der Liste ausgewählt wurde. Falls Ihr DDNS-Provider nicht von den bereitgestellten vorhanden ist, können Sie gerne "custom" verwenden und den Hostnamen der Update-URL hinzufügen.
4. Hostname	Yourhost.example.or	Domainname, der mit der dynamischen IP-Adresse verknüpft wird.

5. Username	your_username	Name des Benutzerkontos.
6. Password	your_password	Passwort des Benutzerkontos.
7. IP Source	Public Private Custom	Mit dieser Option können Sie eine bestimmte RUT-Schnittstelle auswählen und dann die IP-Adresse dieser Schnittstelle an den DDNS-Server senden. Wenn also z.B. Ihr RUT eine Private IP (z.B. 10.140.56.57) auf seinem WAN (3G/LTE-Schnittstelle) hat, dann können Sie diese genaue IP an den DDNS-Server senden, indem Sie "Private" oder die Schnittstelle "Custom" und "WAN" auswählen. Der DDNS-Server löst dann Hostnamenabfragen an diese spezifische IP auf.
8. IP renew interval (min)	10 (minutes)	Zeitintervall (in Minuten), um zu überprüfen, ob sich die IP-Adresse des Gerätes geändert hat.
9. Force IP renew	472 (minutes)	Zeitintervall (in Minuten), um die Erneuerung der IP-Adresse zu erzwingen.

## 8.8 SNMP

Das SNMP-Einstellungsfenster ermöglicht es Ihnen, GSM-Ereignisinformationen aus der Ferne zu überwachen und an den Server zu senden.

### 8.8.1 SNMP Einstellungen

### SNMP Configuration

SNMP Service Settings

SNMP Settings

TRAP Settings

Enable SNMP service

Enable remote access

Port

Community

Location

Contact

Name

Field name	Sample	Explanation
1. Enable SNMP service	Enable/Disable	Führen Sie den SNMP-Dienst (Simple Network Management Protocol) beim Systemstart aus.
2. Enable remote access	Enable/Disable	Öffnen Sie den Port in der Firewall, so dass SNMP (Simple Network)
3. Port	161	Managementprotokoll) Dienst kann über das WAN erreicht werden.
4. Community	Public/Private/Custom	SNMP (Simple Network Management Protocol) Service Port des Dienstes
5. Community name	custom	Die SNMP (Simple Network Management Protocol) Community ist eine
6. Location	Location	Benutzerdefinierten Namen für den Zugriff auf SNMP festlegen
7. Contact	email@example.com	Falle namens sysLocation
8. Name	Name	Falle namens sysContact

## Variables/OID

OID	Description
1. 1.3.6.1.4.1.99999.1.1.1	Modem IMEI
2. 1.3.6.1.4.1.99999.1.1.2	Modem model
3. 1.3.6.1.4.1.99999.1.1.3	Modem manufacturer
4. 1.3.6.1.4.1.99999.1.1.4	Modem revision
5. 1.3.6.1.4.1.99999.1.1.5	Modem serial number
6. 1.3.6.1.4.1.99999.1.1.6	SIM status
7. 1.3.6.1.4.1.99999.1.1.7	Pin status
8. 1.3.6.1.4.1.99999.1.1.8	IMSI
9. 1.3.6.1.4.1.99999.1.1.9	Mobile network registration status
10. 1.3.6.1.4.1.99999.1.1.1	Signal level
11. 1.3.6.1.4.1.99999.1.1.1	Operator currently in use
12. 1.3.6.1.4.1.99999.1.1.1	Operator number (MCC+MNC)
13. 1.3.6.1.4.1.99999.1.1.1	Data session connection state
14. 1.3.6.1.4.1.99999.1.1.1	Data session connection type
15. 1.3.6.1.4.1.99999.1.1.1	Signal strength trap
16. 1.3.6.1.4.1.99999.1.1.1	Connection type trap

## 8.8.2 TRAP Settings

### TRAP Service Settings

SNMP Trap

Host/IP

Port

Community

---

### TRAP Rules

Action	Enable	
Connection type trap	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Signal strength trap	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

---

### New TRAP Rule

Action

Field name	Sample	Explanation
1. SNMP Trap	Enable/Disable	SNMP (Simple Network Management Protocol) Trap-Funktionalität aktivieren
2. Host/IP	192.168.99.155	Host zur Übertragung von SNMP (Simple Network Management Protocol)
3. Port	162	Traffic zu
4. Community	Public/Private	Port für den Host des Traps

## 8.9 SMS Utilities

Der RUT955 verfügt über eine große Anzahl verschiedener SMS-Dienstprogramme. Diese sind in 6 Abschnitte unterteilt: SMS-Dienstprogramme, Anrufe Dienstprogramme, Benutzergruppen, SMS-Management, Fernkonfiguration, Statistiken.

### 8.9.1 SMS Utilities

SMS Utilities	Call Utilities	User Groups	SMS Management	Remote Configuration	Statistics
<b>SMS Utilities</b>					
<b>SMS Rules</b>					
Action	SMS Text	Enable	Sort		
Reboot	reboot	<input checked="" type="checkbox"/>	↑ ↓	Edit	Delete
Get status	status	<input checked="" type="checkbox"/>	↑ ↓	Edit	Delete
Switch WiFi on	wifion	<input checked="" type="checkbox"/>	↑ ↓	Edit	Delete
Switch WiFi off	wifioff	<input checked="" type="checkbox"/>	↑ ↓	Edit	Delete
Switch mobile data on	mobileon	<input checked="" type="checkbox"/>	↑ ↓	Edit	Delete
Switch mobile data off	mobileoff	<input checked="" type="checkbox"/>	↑ ↓	Edit	Delete
Change mobile data settings	cellular	<input checked="" type="checkbox"/>	↑ ↓	Edit	Delete
Get list of profiles	profdisp	<input checked="" type="checkbox"/>	↑ ↓	Edit	Delete
Change profile	pr	<input checked="" type="checkbox"/>	↑ ↓	Edit	Delete
SSH access Control	ssh	<input checked="" type="checkbox"/>	↑ ↓	Edit	Delete
Web access Control	web	<input checked="" type="checkbox"/>	↑ ↓	Edit	Delete

Sie können im Hauptmenü Ihr SMS-Keyword (zu sendender Text) und Ihre autorisierte Telefonnummer auswählen. Du kannst jede erstellte Regel bearbeiten, indem Sie auf die Schaltfläche Bearbeiten klicken. Alle Konfigurationsoptionen sind unten aufgeführt:



Field name	Explanation	Notes
1. <b>Enable SMS Reboot</b>	This check box will enable and disable SMS reboot function.	Wenn Sie Status erhalten wählen, wird der Routerstatus gesendet, sobald er neu gestartet wurde und wieder betriebsbereit ist. Für die Beschreibung des Get Status siehe Punkt Nr. 4 dieser Tabelle.
2. SMS text	SMS text which will reboot router.	SMS-Text kann Buchstaben, Zahlen, Leerzeichen und Sonderzeichen enthalten. Auch Großbuchstaben sind wichtig.
3. Sender phone number	Phone number of person who can reboot router via SMS message	Sie können so viele Telefonnummern hinzufügen, wie Sie benötigen. Die Dropdown-Liste mit zusätzlichen Zeilen wird angezeigt, wenn Sie auf das Symbol "Hinzufügen" am Ende der Rufnummernreihe klicken.
4. <b>Get status</b>	Aktivieren Sie dieses Kontrollkästchen, um Informationen zu erhalten.	Dies ist sowohl eine separate SMS-Regel als auch eine Option unter SMS Neustart Regel.
5. Enable SMS Status	Dieses Kontrollkästchen aktiviert und deaktiviert die SMS-	Der SMS-Status ist standardmäßig deaktiviert.
6. SMS text	SMS-Text, der den Status des Routers sendet.	SMS-Text kann Buchstaben, Zahlen, Leerzeichen und Sonderzeichen enthalten. Auch Großbuchstaben sind wichtig.
7. Sender phone number	Telefonnummer der Person, die den Router-Status per SMS erhalten kann.	Sie können so viele Telefonnummern hinzufügen, wie Sie benötigen. Die Dropdown-Liste mit zusätzlichen Zeilen wird angezeigt, wenn Sie auf das Symbol "Hinzufügen" am Ende der Rufnummernreihe klicken.
8. Get Information	Datenzustand Betreiber Verbindungstyp Signalstärke Verbindungsstatus IP	Sie können auswählen, welche Stauselemente angezeigt werden sollen.
9. <b>Wireless On/Off via SMS</b>	Dieses Kontrollkästchen aktiviert und deaktiviert diese Funktion.	Ermöglicht Wi-Fi-Steuerung per SMS
10. Wireless on SMS text	SMS-Text, der Wi-Fi verwandelt. EIN	SMS-Text kann Buchstaben, Zahlen, Leerzeichen und Sonderzeichen enthalten. Auch Großbuchstaben sind wichtig.
11. Wireless on SMS text	SMS-Text, der Wi-Fi verwandelt. AUS	SMS-Text kann Buchstaben, Zahlen, Leerzeichen und Sonderzeichen enthalten. Auch Großbuchstaben sind wichtig.
12. Sender Phone number	Telefonnummer der Person, die den Router-Status per SMS erhalten kann.	Sie können so viele Telefonnummern hinzufügen, wie Sie benötigen. Die Dropdown-Liste mit zusätzlichen Zeilen wird angezeigt, wenn Sie auf das Symbol "Hinzufügen" am Ende der Rufnummernreihe klicken.
13. Write to config	Speichert dauerhaft den Wi-Fi-Status	Wenn diese Einstellung aktiviert ist, bleibt der Wi-Fi-Status des Routers auch nach einem Neustart erhalten. Wenn er nicht ausgewählt ist, kehrt der Router nach dem Neustart zum Wi-Fi-Zustand zurück.
14. <b>Mobile Settings via SMS</b>	Dieses Kontrollkästchen aktiviert und deaktiviert die Funktion der mobilen Einstellungen.	Ermöglicht die zellulare Steuerung per SMS
15. SMS text	Schlüsselwort, das den aktuellen Konfigurationsparametern vorangestellt wird.	SMS-Text kann Buchstaben, Zahlen, Leerzeichen und Sonderzeichen enthalten. Auch Großbuchstaben sind wichtig.
16. Sender phone number	Telefonnummer der Person, die den Router-Status per SMS erhalten kann.	Sie können so viele Telefonnummern hinzufügen, wie Sie benötigen. Die Dropdown-Liste mit zusätzlichen Zeilen wird angezeigt, wenn Sie auf das Symbol "Hinzufügen" am Ende der Rufnummernreihe klicken.

## Mobile Einstellungen über SMS-Parameter

Parameter	Value(s)	Explanation
1. apn=	i.e. internet.gprs	Setzt APN. z.B.: apn=internet.gprs
2. dialnumber=	i.e. *99***1#	Stellt die Rufnummer ein
3. auth_mode=	none pap chap	Setzt den Authentifizierungsmodus
4. service=	auto 3 bevorzugt 3 schwächling 2bevorzugt 2schwächling	Sie können so viele Telefonnummern hinzufügen, wie Sie benötigen. Die Dropdown-Liste mit zusätzlichen Zeilen wird angezeigt, wenn Sie auf das Symbol "Hinzufügen" am Ende der Rufnummernreihe klicken.
5. username=	user	Wird nur verwendet, wenn die Berechtigung PAP oder CHAP ausgewählt ist.
6. password=	user	Wird nur verwendet, wenn die Berechtigung PAP oder CHAP ausgewählt ist.

:Alle Mobile-Einstellungen können in einer SMS geändert werden. Zwischen jedem <parameter=value> Paar befindet sich ein Leerzeichen.

notwendig.

Beispiel: cellular apn=internet.gprs dialnumber=\*99\*\*\*1#auth\_mode=pap service=3gonly username=user password=user

Field name	Explanation	Notes
1. <b>3G On/Off via SMS</b>	Dieses Kontrollkästchen aktiviert und deaktiviert diese Funktion.	Funktion standardmäßig deaktiviert
2. 3G on SMS text	Text zum Aktivieren der 3G-Verbindung	SMS-Text kann Buchstaben, Zahlen, Leerzeichen und Sonderzeichen enthalten. Auch Großbuchstaben sind wichtig.
3. 3G off SMS text	Text, um die 3G-Verbindung	
4. Write to config	Speichert dauerhaft den 3G-Netzstatus	Wenn diese Einstellung aktiviert ist, bleibt der 3G-Zustand des Routers auch nach einem Neustart erhalten. Wenn er nicht ausgewählt ist, kehrt der Router nach dem Neustart zum 3G-Zustand zurück.
5. <b>Change profile via SMS</b>	Dieses Kontrollkästchen aktiviert und deaktiviert diese Funktion.	Funktion standardmäßig deaktiviert
6. SMS text to change profile	Schlüsselwort, das dem Profilnamen vorangestellt	SMS-Text kann Buchstaben, Zahlen, Leerzeichen und Sonderzeichen enthalten. Auch Großbuchstaben sind wichtig.
7. SMS text to get list of profiles	Nach dem Empfang dieses SMS-Routers wird eine Liste der erstellten Profile an die Absendernummer gesendet.	
8. Sender Phone number	Telefonnummer der Person, die diese Funktion steuern kann.	Sie können so viele Telefonnummern hinzufügen, wie Sie benötigen. Die Dropdown-Liste mit zusätzlichen Zeilen wird angezeigt, wenn Sie auf das Symbol "Hinzufügen" am Ende der Rufnummernreihe klicken.

**Wichtige Hinweise:**

- Die 3G-Einstellungen müssen korrekt konfiguriert sein. Wenn die SIM-Karte eine PIN-Nummer hat, müssen Sie diese unter "Netzwerk" > "3G" eingeben.

Einstellungen. Andernfalls funktioniert die SMS-Neustartfunktion nicht.

- Die Absender-Rufnummer muss die Landesvorwahl enthalten. Sie können das Format der Absender-Rufnummer überprüfen, indem Sie Folgendes lesen  
die Details der alten SMS-Textmassagen, die Sie in der Regel erhalten.

### 8.9.2 Aufrufen von Dienstprogrammen

Ermöglicht es Benutzern, den Router anzurufen, um eine der Aktionen auszuführen: Neustart, Status erhalten, WiFi EIN/AUS schalten, einschalten Mobile Daten EIN/AUS. Das Einzige, was benötigt wird, ist, die SIM-Kartenummer des Routers vom erlaubten Telefon (Benutzer) anzurufen und RUT955 führt alle Aktionen aus, die für diese bestimmte Nummer zugeordnet sind. Um eine neue Aktion für Anrufregeln zu konfigurieren, gehen Sie wie folgt vor müssen Sie nur auf die Schaltfläche Add im Abschnitt "New Call rule" klicken. Danach gelangen Sie in den Abschnitt "Anrufregel ändern".

Field name	Sample	Explanation
1. Enable	Enable/Disable	Aktiviert die Regel
2. Action	Reboot	Maßnahmen, die nach dem Empfangen eines Anrufs zu ergreifen sind, können Sie aus folgenden Aktionen wählen: Neustart, Sendestatus, Switch WiFi, Switch mobile data, Switch output
3. Allowed users	From all numbers	Ermöglicht die Begrenzung der Aktionsauslösung von allen Benutzern, auf Benutzergruppen oder einzelne Benutzernummern.
4. Get status via SMS after reboot	Enable/Disable	Ermöglicht das automatische Versenden von Nachrichten mit Router-Statusinformationen nach einem Neustart.

### 8.9.3 User Gruppen

Bietet die Möglichkeit, Telefonnummern für die SMS-Verwaltung zu gruppieren. Sie können diese Gruppen später auch in folgenden Bereichen verwenden alle zugehörigen SMS-Funktionalitäten. Diese Option hilft, wenn es mehrere Benutzer gibt, die bei der Verwaltung gleiche Rollen haben sollten. Router per SMS. Sie können eine neue Benutzergruppe erstellen, indem Sie den Gruppennamen eingeben und auf die Schaltfläche Hinzufügen unter "Neuen Benutzer erstellen" klicken. Gruppe". Danach gelangen Sie zum Abschnitt "Benutzergruppe ändern".

Field name	Sample	Explanation
1. Group name	Group1	Ihr Name der Rufnummerngruppe
2. Phone number	+37061111111	Nummer, die zur Benutzergruppe hinzugefügt werden soll, muss dem internationalen Format entsprechen. Sie können viele Felder für Telefonnummern hinzufügen, indem Sie auf das grüne + Symbol klicken.

## 8.9.4 SMS Management

### 8.9.4.1 SMS lesen

Auf der Seite SMS-Verwaltung SMS lesen können Sie empfangene/gespeicherte SMS lesen und löschen.

### 8.9.4.2 Send SMS

Field name	Sample	Explanation
1. Phone number	+3701111111	Telefonnummer des Empfängers. Sollte mit einem Ländercode versehen werden, z.B. "+370".
2. Message	My text.	Nachrichtentext, Sonderzeichen sind erlaubt.

### 8.9.4.3 Storage

Mit der Speicheroption können Sie wählen, dass der Router KEINE SMS von der SIM-Karte löscht. Wenn diese Option nicht verwendet wird, wird der Router löscht automatisch alle eingehenden Nachrichten, nachdem sie gelesen wurden. Der Nachrichtenstatus "gelesen/ungelesen" wird überprüft. alle 60 Sekunden. Alle "gelesenen" Nachrichten werden gelöscht.

Field name	Sample	Explanation
1. Nachrichten auf der SIM-Karte speichern	Enabled / Disabled	Ermöglicht die Speicherung empfangener Nachrichten auf der SIM-Karte.
2. Leave free space	1	Gibt an, wie viel Platz für SMS auf der SIM-Karte jederzeit frei bleiben soll.

### 8.9.5 Remote Configuration

RUT9xx kann per SMS von einem anderen RUT9xx aus konfiguriert werden. Sie müssen nur auswählen, welche Konfigurationsdetails es sind.

zu senden, generieren Sie den SMS-Text, geben Sie die Telefonnummer und Seriennummer des Routers ein, den Sie konfigurieren möchten, und senden Sie die SMS.

Die Gesamtzahl der SMS wird automatisch verwaltet. Sie sollten sich der möglichen Anzahl von SMS bewusst sein und diese verwenden.

auf eigene Verantwortung. Es sollte im Allgemeinen nicht verwendet werden, wenn Sie hohe Kosten pro SMS haben. Dies gilt insbesondere für relevant, wenn Sie versuchen werden, die gesamte OpenVPN-Konfiguration zu senden, was zu einer Ansammlung von ~40 SMS führen kann.

#### 8.9.5.1 Receive configuration

Dieser Abschnitt steuert, wie sich der Initiator der Konfiguration identifizieren soll. In diesem Szenario hat RUT955 selbst wird gerade konfiguriert.

Field name	Values	Notes
1. Enable	Enabled / Disabled	Ermöglicht es dem Router, die Konfiguration zu empfangen.

1.	Authorization method	Keine Berechtigung / Durch Serienschaltung Mit Verwaltungspasswor	Methode an Empfangs- und Sendeende muss übereinstimmen
2.	Allowed users	Von allen Zahlen Von der Gruppe Von der Einzelnummer	Bietet bessere Kontroll- und Sicherheitsmaßnahmen

**Beachten Sie, dass die Autorisierungsmethode aus Sicherheitsgründen vor der Bereitstellung des Routers konfiguriert werden sollte.**

#### 8.9.5.2 Send configuration

In diesem Abschnitt können Sie Remote-Geräte konfigurieren. Die Berechtigungseinstellungen müssen mit denen übereinstimmen, die am die empfangende Partei.

Generate SMS

WAN

Interface

Protocol

IP address

IP netmask

IP gateway

IP broadcast

Network **name** **VPN**

Generate

Wan

Interface

Mobile connection

APN

Dialing number

Authentication method

Username

Password

Service mode

Lan

IP address

IP netmask

IP broadcast

Send Configuration Message

Generate

Phone number

Serial number

Send

Field name	Values	Notes
1. Generate SMS	Neu Aus der aktuellen Konfiguration	Neue SMS-Einstellungen generieren oder aktuelle Gerätekonfiguration verwenden
2. Mobile	Enable/Disable	Inklusive Konfiguration für das Mobilfunknetz
3. WAN	Enable/Disable	Konfiguration für WAN (Wide Area Network) einbinden
4. LAN	Enable/Disable	Konfiguration für LAN (Local Area Network) einbinden
5. Interface	Wired Mobile	Schnittstellentyp für WAN (Wide Area Network) Verbindung
6. Protocol	Static/DHCP	Netzwerkprotokoll, das für die Verwaltung der Netzwerkkonfigurationsparameter verwendet wird.
7. IP address	"217.147.40.44"	IP-Adresse, die der Router für die Verbindung zum Internet verwendet.
8. IP netmask	"255.255.255.0"	Damit wird definiert, wie groß das WAN (Wide Bereichsnetzwerk) Netzwerk ist
11. IP gateway	"217.147.40.44"	Die Adresse, an der der Datenverkehr für das Internet bestimmt ist, ist

12. IP broadcast	"217.147.40.255"	weitergeleitet an Eine logische Adresse, an der alle mit einem Kommunikationsnetzwerk mit mehreren Zugriffen verbundenen Geräte zum Empfangen von Datagrammen aktiviert sind.
13. Primary SIM card	SIM1/SIM2	Eine SIM-Karte, die verwendet wird.
14. Mobile connection	Use pppd mode Use ndis mode	Ein zugrunde liegender Agent, der für die Erstellung und Verwaltung von mobilen Datenverbindungen verwendet wird.
15. APN	"internet.mnc012.mcc345.gprs"	(APN) ist der Name eines Gateways zwischen einem GPRS-, 3G- oder 4G-Mobilfunknetz und einem anderen Computernetz, häufig dem öffentlichen Internet.
16. Dialing number	"+37060000001"	Eine Telefonnummer, die zum Aufbau einer mobilen PPP-Verbindung (Point-to-Point Protocol) verwendet wird.
17. Authentication method	CHAP/PAP/None	Wählen Sie eine Authentifizierungsmethode, die zur Authentifizierung neuer Verbindungen im Netz Ihres GSM-Carriers verwendet wird.
18. User name	"admin"	Benutzername, der für die Authentifizierung an Ihrem GSM verwendet wird. Carrier-Netzwerk
19. Password	"password"	Passwort, das zur Authentifizierung an Ihrem GSM verwendet wird. Carrier-Netzwerk
20. Service mode	2G nur für 2G bevorzugt 3G nur für 3G bevorzugt 4G (LTE) nur für 4G (LTE) bevorzugt Automatic	Wählen Sie die Einstellung des Netzwerks. Wenn Ihr lokales Mobilfunknetz GSM (2G), UMTS (3G) oder LTE (4G) unterstützt, können Sie angeben, mit welchem Netz Sie sich vorzugsweise verbinden möchten.
21. IP address	"192.168.1.1"	IP-Adresse, die der Router im LAN verwenden wird (lokaler Bereich Network) network
22. IP netmask	"255.255.255.0"	Eine Subnetzmaske, die verwendet wird, um zu definieren, wie groß das LAN Netzwerk(Local Area Network) ist.
23. IP broadcast	"192.168.1.255"	Eine logische Adresse, an der alle mit einem Kommunikationsnetzwerk mit mehreren Zugriffen verbundenen Geräte zum Empfangen von Datagrammen aktiviert sind.

```
network.wan.ipaddr=217.147.40.44, network.wan.netmask=255.255.255.0,
network.wan.gateway=217.147.40.44, network.wan.broadcast=217.147.40.255
```

Phone number

Authorization method

Field name	Values	Notes
1. Message text field	Generated configuration	Hier können Sie die Konfiguration überprüfen und ändern.



2. Phone number	message "+37060000001"	zu sendender Nachrichtentext Eine Telefonnummer des Routers, der die Konfiguration erhält.
3. Autorisierungsmethode	Keine Berechtigung Durch die serielle Durch Router Admin-Passwort	Welche Art von Berechtigung soll für die Fernkonfiguration verwendet werden?

### 8.9.6 Statistik


Auf der Statistikseite können Sie überprüfen, wie viele SMS auf beiden SIM-Kartensteckplätzen gesendet und empfangen wurden. Sie können auch zurücksetzen die Zähler

SMS Utilities	Call Utilities	User Groups	SMS Management	Remote Configuration	Statistics
<b>Statistics</b>					
<b>SMS Statistics</b>					
SIM Card	Sent SMS	Received SMS			
SIM 1	0	0		Reset	
SIM 2	0	0		Reset	

## 8.10 SMS Gateway

### 8.10.1 Post/Get Configuration

Post/Get Configuration ermöglicht es Ihnen, Aktionen durchzuführen, indem Sie diese AnforderungsURI nach der IP-Adresse Ihres Geräts schreiben.

Post/Get	Email To SMS	Scheduled SMS	Auto Reply	SMS Forwarding	SMPP
<b>Post/Get Configuration</b>					
<b>SMS Post/Get Settings</b>					
Enable <input checked="" type="checkbox"/>					
User name <input type="text" value="admin"/>					
Password <input type="password" value="*****"/> 					
Save					

Field name	Values	Notes
1. Enable	Enabled / Disabled	Aktivieren Sie die SMS-Verwaltungsfunktionalität durch POST/GET
2. User name	admin	Benutzername, der für die Autorisierung verwendet wird
3. Password	*****	Für die Autorisierung verwendetes Passwort (default-admin01)

Vergiss nicht, die Parameter in der URL entsprechend deiner POST/GET-Konfiguration zu ändern!

### 8.10.1.1 SMS über HTTP POST/GET

Es ist möglich, SMS mit einer gültigen HTTP POST/GET-Syntax zu lesen und zu senden. Verwenden Sie einen Webbrowser oder einen anderen Browser.

kompatible Software, um HTTP POST/GET Zeichenkette an den Router zu senden. Der Router muss mit dem GSM-Netz verbunden sein, wenn er verwendet wird.

"SMS senden" Funktion.

Action	POST/GET url e.g.
1. View mobile messages	/cgi-bin/sms_list?username=admin&password=admin01
2. Read mobile	/cgi-bin/sms_read?username=admin&password=admin01&number=+37060000001
3. Send mobile messages	/cgi-bin/sms_send?username=admin&password=admin01&number=+37060000001&text=testmessage
4. View mobile messages	/cgi-bin/sms_total?username=admin&password=admin01
5. Delete mobile	/cgi-bin/sms_delete?username=admin&password=admin01&number=+37060000001

### 8.10.1.2 Syntax der HTTP POST/GET Zeichenkette

HTTP POST/GET string	Explanation
http://{IP_ADDRESS}/cgi-bin/sms_read?number={MESSAGE_INDEX}	Read message
{/cgi-bin/sms_send?number={MESSAGE_INDEX}&text={MESSAGE_TEXT}}	Send message
{/cgi-bin/sms_delete?number={MESSAGE_INDEX}}	Delete message
{/cgi-bin/sms_list?}	List all messages
{/cgi-bin/sms_total?}	Number of messages in memory

Hinweis: Die Parameter der HTTP POST/GET-Zeichenkette werden in geschweiften Klammern in Großbuchstaben geschrieben. Geschweifte Klammern ("{}") sind keine wird beim Senden von HTTP POST/GET-Strings benötigt.

### 8.10.1.3 Parameter der HTTP POST/GET Zeichenkette

Parameter	Explanation
1. IP_ADDRESS	IP address of your router
2. MESSAGE_INDEX	SMS index in memory
3. PHONE_NUMBER	Telefonnummer des Nachrichteneempfängers. Hinweis: Die Telefonnummer muss die Landesvorwahl enthalten. Das Format der Telefonnummer ist: 00{LÄNDERCODE}{EMPFÄNGERNUMMER}. Z.B...: 0037062312345 (370 ist Landesvorwahl und 62312345 ist Empfänger-Rufnummer)
4. MESSAGE_TEXT	Text der SMS. Hinweis: Die maximale Anzahl der Zeichen pro SMS beträgt 160. Du kannst keine längeren Nachrichten senden. Es wird empfohlen, nur alphanumerische Zeichen zu verwenden.

Nach jedem ausgeführten Befehl antwortet der Router mit einem Rückgabestatus.

### 8.10.1.4 Possible responses after command execution

Response	Explanation
1. OK	Befehl erfolgreich ausgeführt

2. ERROR	Bei der Ausführung des Befehls ist ein Fehler aufgetreten.
3. TIMEOUT	Keine Antwort vom Modul empfangen
4. WRONG_NUMBER	Das Zahlenformat des SMS-Empfängers ist falsch oder die SMS-Indexnummer ist falsch.
5. NO MESSAGE	Es gibt keine Meldung im Speicher bei gegebenem Index.
6. NO MESSAGES	Es sind keine Nachrichten im Speicher gespeichert.

#### 8.10.1.5 HTTP POST/GET string examples

http://192.168.1.1/cgi-bin/sms\_read?number=3

http://192.168.1.1/cgi-bin/sms\_send?number=0037061212345&text=test

http://192.168.1.1/cgi-bin/sms\_delete?number=4

http://192.168.1.1/cgi-bin/sms\_list

http://192.168.1.1/cgi-bin/sms\_total

#### 8.10.2 Email to SMS

Post/Get
Email To SMS
Scheduled SMS
Auto Reply
SMS Forwarding
SMPP

### POP3 Email To SMS Configuration

Email To SMS Settings

Enable

POP3 server

Server port

User name

Password

Secure connection (SSL)

Check email every

Field name	Values	Notes
1. Enable	Enable/Disable	Ermöglicht die Konvertierung empfangener E-Mails in SMS.
2. POP3 server	"pop.gmail.com"	POP3 server address
3. Server port	"995"	Server-Authentifizierungsport
4. User name	" <a href="#">admin</a> "	Benutzername, der für die Serverauthentifizierung verwendet wird.
5. Password	"admin01"	Passwort für die Serverauthentifizierung
6. Secure connection (SLL)	Enable/Disable	(SSL) ist ein Protokoll zur Übertragung privater Dokumente über das Internet. SSL verwendet ein kryptographisches System, das zwei Schlüssel zur Verschlüsselung von Daten verwendet - einen öffentlichen Schlüssel, der jedem bekannt ist, und einen privaten oder geheimen Schlüssel, der nur dem Empfänger der Nachricht bekannt ist.
7. Check mail every	Min utes Hour	Zeitraum der Mail-Prüfung

### 8.10.3 Geplante Nachrichten

Geplante Nachrichten ermöglichen es, regelmäßig mobile Nachrichten an eine bestimmte Nummer zu senden.

Post/Get Configuration	Email To SMS	Scheduled Messages	Auto Reply														
<h2>Scheduled Messages</h2> <p>Configure time and text for scheduled messages.</p> <h3>Messages To Send</h3> <table border="1"><thead><tr><th>Recipients number</th><th>Sending Interval</th><th>Enable</th><th>Sort</th></tr></thead><tbody><tr><td colspan="4"><i>There are no scheduled messages created yet</i></td></tr></tbody></table> <p>Scheduled messages Configuration:</p> <table><tr><td>Phone number</td><td>Message sending interval</td></tr><tr><td><input type="text"/></td><td>Day <input type="button" value="▼"/></td></tr><tr><td colspan="2"><input type="button" value="Add"/></td></tr></table>				Recipients number	Sending Interval	Enable	Sort	<i>There are no scheduled messages created yet</i>				Phone number	Message sending interval	<input type="text"/>	Day <input type="button" value="▼"/>	<input type="button" value="Add"/>	
Recipients number	Sending Interval	Enable	Sort														
<i>There are no scheduled messages created yet</i>																	
Phone number	Message sending interval																
<input type="text"/>	Day <input type="button" value="▼"/>																
<input type="button" value="Add"/>																	

## 8.10.3.1 Konfiguration der Konfiguration von geplanten Nachrichten

Post/Get	Email To SMS	Scheduled SMS	Auto Reply	SMS Forwarding	SMPP
<b>Scheduled Messages Configuration</b>					
<b>Modify scheduled message</b>					
Enable <input type="checkbox"/>					
Recipient's phone number <input type="text" value="+37060000001"/>					
Message text <input type="text" value="Test"/>					
SMS 1 (156 characters left)					
Message sending Interval <input type="text" value="Day"/>					
Hour <input type="text" value="1"/>					
Minute <input type="text" value="1"/>					
<a href="#">Back to Overview</a>					<input type="button" value="Save"/>

Field name	Values	Notes
1. Enable	Enable/Disable	Aktiviert das periodische Senden von Nachrichten.
2. Recipient's phone number	"+37060000001"	Telefonnummer, die Nachrichten empfängt
3. Message text	"Test"	Nachricht, die gesendet wird.
4. Message sending interval	Day Week Month Year	Sendezeitraum der Nachricht.

### 8.10.4 Konfiguration der automatischen Antwort

Die automatische Antwort ermöglicht die Beantwortung jeder Nachricht, die der Router an alle oder nur an aufgelistete Nummern erhält.

Post/Get Configuration	Email To SMS	Scheduled Messages	Auto Reply	SMS Forwarding
<b>Auto Reply Configuration</b>				
<b>Reply Configuration</b>				
Enable <input type="checkbox"/>				
Don't save recieved message <input checked="" type="checkbox"/>				
Mode <input type="text" value="Everyone"/>				
Message <input type="text"/>				

Field name	Values	Notes
1. Enable	Enable/Disable	Aktivieren Sie die automatische Antwort auf jede empfangene mobile Nachricht.
2. Don't save received message	Enable/Disable	Wenn aktiviert, werden empfangene Nachrichten nicht gespeichert.
3. Mode	Everyone / Listed	Gibt an, von welchen Absendern empfangene Nachrichten beantwortet werden sollen.
4. Message	"Text"	Nachrichtentext, der als Antwort gesendet wird.

## 8.10.5 SMS Weiterleitung

### 8.10.5.1 SMS-Weiterleitung an HTTP

Diese Funktionalität leitet mobile Nachrichten von allen oder nur bestimmten Absendern an HTTP weiter, entweder über POST oder GET. Methoden

Post/Get	Email To SMS	Scheduled SMS	Auto Reply	SMS Forwarding	SMPP
SMS Forwarding To HTTP					
SMS Forwarding To SMS		SMS Forwarding To Email			
<h2>SMS Forwarding To HTTP Configuration</h2> <h3>SMS Forwarding To HTTP Settings</h3> <p>Enable <input type="checkbox"/></p> <p>Method <input type="text" value="Get"/></p> <p>URL <input type="text" value="192.168.99.250/getpost/in"/></p> <p>Number value name <input type="text" value="sender"/></p> <p>Message value name <input type="text" value="text"/></p> <p>Extra data pair 1 <input type="text" value="var1"/> <input type="text" value="17"/></p> <p>Extra data pair 2 <input type="text" value="var2"/> <input type="text" value="go"/></p> <p>Mode <input type="text" value="All messages"/></p>					

Field name	Values	Notes
1. Enable	Enable / Disable	Mobile Nachrichtenweiterleitung an HTTP aktivieren
2. Method	POST / GET	Definiert die HTTP-Übertragungsmethode
3. URL	192.168.99.250/getpost/index.p	URL-Adresse zum Weiterleiten von Nachrichten an
4. Number value name	“sender”	Zuweisender Name für den Wert der Telefonnummer des Absenders in der Abfragezeichenfolge
5. Message value name	“text”	Zuweisender Name für den Wert des Nachrichtentextes im Query-String
6. Extra data pair 1	Var1 - 17	Wenn Sie zusätzliche Informationen über die HTTP-Abfrage übertragen möchten, geben Sie den Variablennamen in das linke Feld und seinen Wert in das rechte Feld ein.
7. Extra data pair 2	Var2 – “go”	Wenn Sie zusätzliche Informationen über die HTTP-Abfrage übertragen möchten, geben Sie den Variablennamen in das linke Feld und seinen Wert in das rechte Feld ein.
8. Mode	All messages/From listed numbers	Gibt an, welche Absendernachrichten weitergeleitet werden sollen.

### 8.10.5.2 SMS-Weiterleitung an SMS

Diese Funktionalität ermöglicht es, mobile Nachrichten von bestimmten Absendern an einen oder mehrere Empfänger weiterzuleiten.

SMS Forwarding To HTTP
SMS Forwarding To SMS
SMS Forwarding To Email

## SMS Forwarding To SMS Configuration

SMS Forwarding To SMS Settings

Enable

Add sender number

Mode All messages

recipients phone numbers

Field name	Values	Notes
1. Enable	Enable / Disable	Mobile Nachrichtenweiterleitung aktivieren
2. Add sender number	Enable / Disable	Wenn aktiviert, wird die Nummer des ursprünglichen Absenders am Ende der weitergeleiteten Nachricht hinzugefügt.
3. Mode	All message / From listed numbers	Gibt an, von welchen Absendern empfangene Nachrichten weitergeleitet werden sollen.
4. Recipients phone numbers	+37060000001	Telefonnummern, an die die Nachricht weitergeleitet werden soll.



### 8.10.5.3 SMS-Weiterleitung an E-Mail

Diese Funktionalität leitet mobile Nachrichten von einem oder mehreren angegebenen Absendern an die E-Mail-Adresse weiter.

**SMS Forwarding To Email Settings**

Enable

Add sender's number


Subject

SMTP server


SMTP server port

Secure connection

User name

Password  

Sender's email address

Recipient's email address  

Mode

Field name	Values	Notes
1. Enable	Enable / Disable	Mobile Nachrichtenweiterleitung an E-Mail aktivieren
2. Add sender number	Enable / Disable	Wenn aktiviert, wird die Nummer des ursprünglichen Absenders am Ende der weitergeleiteten Nachricht hinzugefügt.
3. Subject	"forwarded message"	Text, der in das Betrefffeld der E-Mail eingefügt wird.
4. SMTP server	mail.teltonika.it	Die Adresse Ihres SMTP-Servers
5. SMTP server port	25	Die Portnummer Ihres SMTP-Servers
6. Secure connection	Enable / Disable	Ermöglicht die Verwendung von kryptographischen Protokollen, nur aktivieren, wenn Ihr SMTP-Server SSL oder TLS unterstützt.
7. User name	"admin"	Ihr vollständiger Benutzername für das E-Mail-Konto
8. Password	*****	Ihr Passwort für Ihr E-Mail-Konto
9. Sender's email address	name.surname@gmail.com	Ihre Adresse, die zum Versenden von E-Mails verwendet wird.
10. Recipient's email	name2.surname2@gmail.co	Adresse, an die Sie Ihre Nachrichten weiterleiten möchten
11. Mode	All messages / from listed numbers	Wählen Sie aus, welche Absendernachrichten an E-Mails weitergeleitet werden sollen.

### 8.10.6 SMPP

Der SMPP (Short Message Peer to Peer) Server ermöglicht es Clients, sich über das SMPP-Protokoll mit dem Router zu verbinden und dann zu senden.

SMS über das Mobilfunknetz. Diese SMPP-Server-Implementierung ermöglicht das Senden von Nachrichten, aber das Empfangen eingehender Nachrichten. wird derzeit nicht unterstützt.

## SMPP Server Configuration

**Transmitter Configuration**

Enable

User name

Password

Server port

Field name	Values	Notes
1. Enable	Enable / Disable	Aktiviert den SMPP-Server auf dem Router.
2. User name	admin	Benutzername, welche Clients eine Verbindung zu SMPP herstellen müssen.
3. Password	*****	Passwort, welche Clients für die Verbindung zu SMPP benötigt werden.
4. Server port	7777	Server-Port, der für die SMPP-Kommunikation verwendet werden soll. Sie können jeden unbenutzten Port auswählen (0 - 65535).

## 8.11 GPS

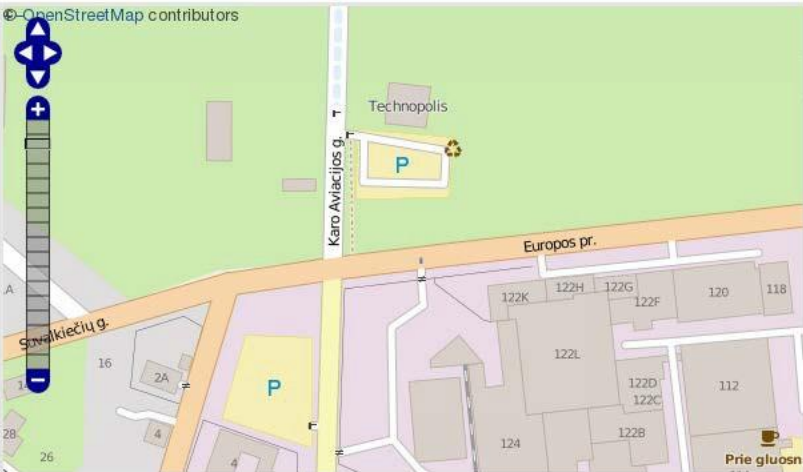
### 8.11.1 GPS

Auf dieser Seite können Sie Ihre aktuellen Koordinaten und Positionen auf der Karte anzeigen.

GPS GPS Settings

### GPS

MAP



Latitude	Longitude	Fix time
N/A	N/A	N/A

### 8.11.2 GPS Einstellungen

Dies ist die Seite zur Konfiguration der GPS-Parameter.

GPS GPS Settings

### GPS Configuration

GPS Settings

Enable GPS service

Enable GPS Data to server

IP address

Port

Data sending interval

Data collection interval

Protocol TCP ▾

	Field name	Values	Notes
1.	Enable GPS service	Enable / Disable	Aktiviert den GPS-Dienst
2.	Enable GPS Data to server	Enable / Disable	Ermöglicht die Datenprotokollierung von GPS-Koordinaten auf dem Server.
3.	IP address	212.47.99.61	IP-Adresse des Datenloggerservers

4.	Port	17050	Portnummer des Datenloggerservers
5.	Data sending interval	10	Intervall für die Übertragung von GPS-Daten an den Server
6.	Data collection interval	5	Intervall für die Datenerfassung vom GPS-Modul
7.	Protocol	TCP	Gibt das Protokoll an, das für die Datenübertragung verwendet werden soll.

## 8.12 CLI

CLI- oder Befehlszeilenschnittstelle ermöglicht die Eingabe und Ausführung von Befehlen in Router-Terminals..

```

TELTONIKA Status Network Services System Logout
Teltonika login: root
Password:

BusyBox v1.19.4 (2015-09-18 08:28:46 EEST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

      _ _ _ _ _
     / / / / /
    / / / / /
   / / / / /
  / / / / /
 / / / / /
/_/_/_/_/_

Teltonika 2014
root@Teltonika:~#

```

Use "CTRL + ATL + SHIFT + T" keyboard shortcut to open CLI in new tab

## 8.13 Netzwerkfreigaben

### 8.13. 1 Angehängte Dateisysteme

Auf dieser Seite können Sie gemountete Dateisysteme (z.B. USB-Stick) betrachten.

Mounted file systems	Samba	Samba user	
<b>Network Shares</b>			
<b>Mounted file systems</b>			
Filesystem	Mount Point	Available	Used
/dev/sda1	/mnt/sda1	7.84 GB / 14.65 GB	47% (6.81 GB)
			Safely Remove Disk
			Refresh

### 8.13.2 Samba

Die Samba-Funktionalität ermöglicht die Netzwerkfreigabe für bestimmte Verzeichnisse.

Field name	Values	Notes
1. Enable	Enable / Disable	Aktiviert den Samba-Service
2. Hostname	Router_Share	Name des Samba-Servers
3. Description	Teltonika_Router_Share	Kurze Serverbeschreibung
4. Workgroup	WORKGROUP	Name der Arbeitsgruppe

Im Abschnitt Gemeinsame Verzeichnisse können Sie zu freigebende Verzeichnisse hinzufügen und einige Nutzungsparameter konfigurieren:

Field name	Values	Notes
1. Name	My_dir	Name des gemeinsamen Verzeichnisses
2. Path	/mnt/sda1	Pfad zum zu teilenden Verzeichnis
3. Allow guests	Enable / Disable	Aktivieren Sie die Anzeige des Verzeichnisses als Gast.
4. Allowed users	root	Geben Sie Benutzer an, die dieses Verzeichnis freigeben dürfen.
5. Read-only	Enable / Disable	Setzt die Rechte des Benutzers im angegebenen Verzeichnis auf Nur-Lesen.

### 8.13.3 Samba-Benutzer

Auf dieser Seite kannst du neue Samba-Benutzer hinzufügen.

Values

Mounted file systems
Samba
Samba user

## Samba users

**Users**

**Username**

*This section contains no values yet*

**Add user:**

**Username**

**Password**

	Field name	Values	Notes
1.	Username	user	Name des neuen Benutzers
2.	Password	Pass1	Passwort des neuen Benutzers

## 8.14 Hotspot

Wireless Hotspot bietet wesentliche Funktionen für die Verwaltung eines drahtlosen Open-Access-Netzwerks. Zusätzlich zu Standard-RADIUS-Server-Authentifizierung gibt es auch die Möglichkeit, detaillierte Protokolle über die einzelnen Geräte zu sammeln und hochzuladen. (bezeichnet als MAC-Adresse) im Netzwerk (welche Standorte wurden durchquert, etc.).

### 8.14.1 Allgemeine Einstellungen

Field name	Explanation
1. Enabled	Aktivieren Sie dieses Flag, um die Hotspot-Funktionalität auf dem Router zu aktivieren.
2. AP IP	IP-Adresse des Zugangspunktes. Dies ist die Adresse des Routers im Hotspot-Netzwerk. Der Router erstellt automatisch ein Netzwerk entsprechend seiner eigenen IP und der CIDR-Nummer, die Sie nach dem Slash angeben. Z.B. "192.168.2.254/24" bedeutet, dass der Router Folgendes erstellen wird ein Netzwerk mit der IP-Adresse 192.168.182.0, Netzmaske 255.255.255.255.0 für den ausdrücklichen Zweck, alle drahtlosen Clients zu enthalten. Ein solches Netzwerk wird 253 Clients haben können (ihre IP-Adressen werden ihnen automatisch zugewiesen und reichen von 192.168.2.1 bis 192.168.2.253).
3. Authentication mode	External radius
4. Radius server #1	Die IP-Adresse des RADIUS-Servers, der für die Authentifizierung Ihrer WLAN-Clients verwendet werden soll.

5.	Radius server #2	Die IP-Adresse des zweiten RADIUS-Servers.
6.	Authentication	RADIUS-Server-Authentifizierungsport.
7.	Accounting port	RADIUS Server Accounting Port.
8.	Authentication mode	Internal radius
9.	IP address or network of the client	E.g.(192.168.1.1 or 192.168.1.0/24)
10.	Authentication mode	Without radius
11.		Erfordert keine RADIUS-Konfiguration. Ermöglicht eine einfache Benutzerverbindung basierend auf Benutzername/Passwort.
12.	External landing page	Ermöglicht die Verwendung einer externen Zielseite.
13.	Landing page	Die Adresse der externen Zielseite
14.	Protocol	HTTP or HTTPS.
15.	HTTPS redirect	Leitet HTTP-Seiten zur Zielseite um.

### 8.14.2 Einstellungen zur Internet-Zugangsbeschränkung

Ermöglicht die Deaktivierung des Internetzugangs an einem bestimmten Tag und zu einer bestimmten Uhrzeit jeder Woche.

General
Restricted Internet Access
Logging
Landing Page
Radius Server

Teltonika\_Router

### Internet Access Restriction Settings

Select Time To Restrict Access On Hotspot Teltonika\_Router

Days/Hours	0-1h	1-2h	2-3h	3-4h	4-5h	5-6h	6-7h	7-8h	8-9h	9-10h	10-11h	11-12h	12-13h	13-14h	14-15h	15-16h	16-17h	17-18h	18-19h	19-20h	20-21h	21-22h	22-23h	23-24h
Monday																								
Tuesday																								
Wednesday																								
Thursday																								
Friday																								
Saturday																								
Sunday																								

Internet access allowed

Internet access blocked



## 8.14.3 Protokollierung

Field name	General	Restricted Internet Access	Logging	Landing Page	Radius Server
Explanation					
<b>Wireless Hotspot Logging Settings</b>					
<b>Logging To FTP Settings</b>					
Enable	<input type="checkbox"/>				
Server address	<input type="text" value="your.ftp.server"/>				
User name	<input type="text" value="username"/>				
Password	<input type="password" value="....."/>				
Port	<input type="text" value="21"/>				

Field name	Explanation
1. Enable	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die drahtlose Traffic-Protokollierung aktivieren möchten. Diese Funktion erzeugt Protokolle, die Daten darüber enthalten, welche Websites jeder Kunde während der Zeit, in der er mit Ihrem Hotspot verbunden war, besucht hat.
2. Server address	Die IP-Adresse des FTP-Servers, auf den die Protokolle hochgeladen werden sollen.
3. Username	Der Benutzername des Benutzers auf dem oben genannten FTP-Server.
4. Password	Das Passwort des Benutzers.
5. Port	Der TCP/IP-Port des FTP-Servers.

FTP Upload Settings	
You can configure your timing settings for the log upload via FTP feature here.	
Mode	<input type="text" value="Fixed"/>
Hours	<input type="text" value="8"/>
Minutes	<input type="text" value="15"/>
Days	<input type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input type="checkbox"/> Friday <input type="checkbox"/> Saturday <input type="checkbox"/> Sunday

Field name	Explanation
1. Mode	Der Modus des Zeitplans. Verwenden Sie "Fixed", wenn Sie möchten, dass das Hochladen zu einer bestimmten Tageszeit erfolgt. Verwenden Sie "Intervall", wenn Sie möchten, dass der Upload in einem festen Intervall erfolgt.
2. Weekdays	Dieses Feld gibt an, an welchen Wochentagen das Hochladen erfolgen soll. Das Eingabeformat sind Zahlen von 1 bis 7, die nur durch Kommas getrennt sind. Wenn Sie z.B. die Protokolle am Montag, Mittwoch und Samstag hochladen möchten, geben Sie "1,3,6" ein.
3. Interval	Wird nur angezeigt, wenn "Mode" auf Intervall eingestellt ist. Gibt das Intervall der regelmäßigen Uploads an einem bestimmten Tag an. Wenn Sie z.B. 4 Stunden wählen, wird das Hochladen um Mitternacht, 4:00 Uhr, durchgeführt, 8:00, 12:00, 16:00 und 20:00 Uhr.

Hours, Minutes                      Wird nur angezeigt, wenn "Mode" auf Fixed gesetzt ist. Das Hochladen erfolgt zu dieser bestimmten Tageszeit. Wenn du z.B. deine Logs am 6:48 Uhr hochladen möchtest, musst du einfach Stunden eingeben: 6 und Minuten: 48.

#### 8.14.4 Landing Page

##### 8.14.4.1 General Landing Page Settings

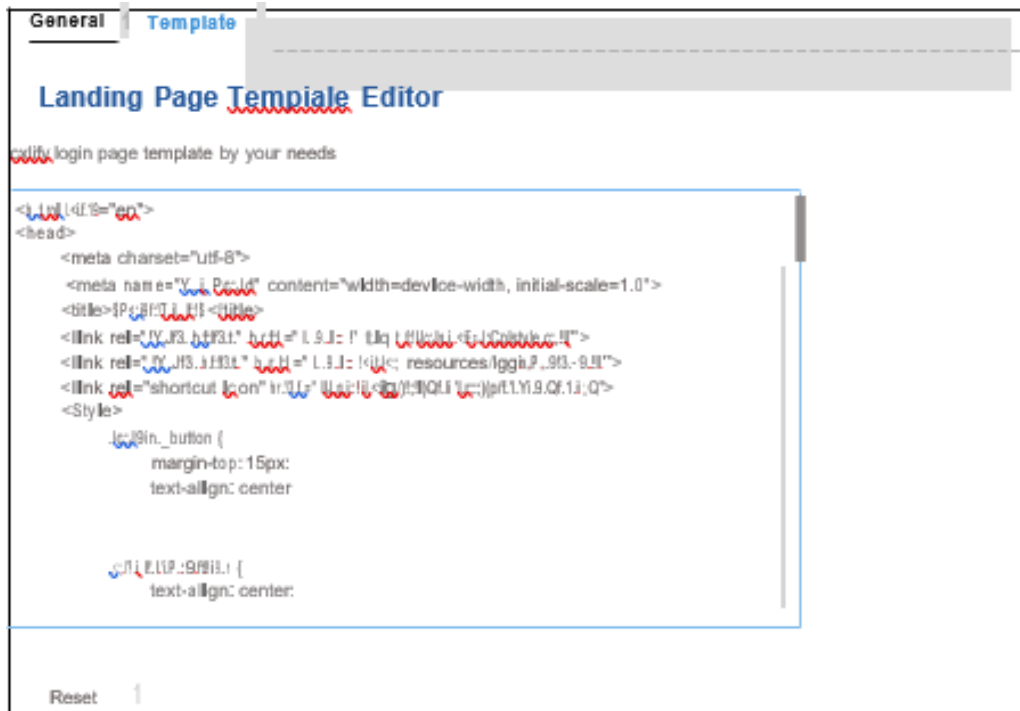
Mit dieser Funktionalität können Sie Ihre Hotspot Landing Seite anpassen.

Field name	Explanation
1. Page title	Wird als Titel der Zielseite angesehen.
2. Theme	Themenauswahl für die Landing Page
3. Upload login page	Ermöglicht das Hochladen von benutzerdefinierten Landing Page Themes.
4. Login page file	Ermöglicht das Herunterladen und Speichern der Landing Page Datei.

In den Abschnitten - "Nutzungsbedingungen", "Hintergrundkonfiguration", "Logobild-Konfiguration", "Link Konfiguration", "Textkonfiguration" können Sie verschiedene Parameter von Landing Page Komponenten anpassen.

### 8.14.4.2 Vorlage

Auf dieser Seite können Sie den HTML-Code der Landing Page Template überprüfen und ändern.



The screenshot shows the 'Landing Page Template Editor' interface. At the top, there are two tabs: 'General' and 'Template', with 'Template' being the active tab. Below the tabs, the title 'Landing Page Template Editor' is displayed. The main content area contains the following HTML code:

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>P&#246;rtal&#228;nde</title>
  <link rel="stylesheet" href="lib/jquery-ui/css/themes/default/jquery-ui.css">
  <link rel="stylesheet" href="lib/jquery-ui/resources/jquery-ui.css">
  <link rel="shortcut icon" href="lib/jquery-ui/resources/jquery-ui.png">
</head>
<body>
  <div class="login_button">
    margin-top: 15px;
    text-align: center;
  </div>
  <div class="login">
    text-align: center;
  </div>
</body>
</html>
```

At the bottom left of the editor, there is a 'Reset' button.

### 8.14.5 Radius-Server-Konfiguration

Ein Authentifizierungs- und Abrechnungssystem, das von vielen Internet Service Providern (ISPs) verwendet wird. Wenn Sie sich in den Bereich der ISP müssen Sie Ihren Benutzernamen und Ihr Passwort eingeben. Diese Informationen werden an einen RADIUS-Server weitergeleitet, der überprüft, ob die Informationen sind korrekt und autorisieren dann den Zugriff auf das ISP-System.

General	Restricted Internet Access	Logging	Landing Page	Radius Server	Statistics	
<b>Radius Server Configuration</b>						
<b>General Settings</b>						
Enable <input type="checkbox"/>						
Remote access <input type="checkbox"/>						
Accounting port <input type="text" value="1813"/>						
Authentication port <input type="text" value="1812"/>						
<b>Users Configuration Settings</b>						
Enable	User name	Reply message	Idle timeout	Session timeout	Download bandwidth	Upload bandwidth
<i>There are no users created yet.</i>						
<b>Username</b>			<b>Password</b>			
<input type="text"/>			<input type="text"/>			<input type="button" value="Add"/>
<b>Clients Configuration Settings</b>						
Enable	Client name	IP address	Netmask	Radius shared secret		
<i>There are no clients created yet.</i>						
<input type="button" value="Add"/>						

Field name	Erläuterung
1. Enable	Aktiviert ein Authentifizierungs- und Abrechnungssystem
2. Remote access	Aktiviert den Fernzugriff auf den Radius-Server.
3. Accounting port	Port, an dem auf das Zählen gehört werden soll.
4. Authentication port	Port, auf dem die Authentifizierung abgehört werden soll

### 8.14.6 Statistik

Auf der Statistikseite können Sie verschiedene statistische Informationen über Hotspot-Instanzen einsehen.

## 8.15 Automatischer Neustart

### 8.15.1 Ping Neustart

Die Ping Reboot-Funktion sendet periodisch den Ping-Befehl an den Server und wartet auf den Echoempfang. Wenn kein Echo vorhanden ist

Empfangener Router wird versuchen, nach einem definierten Zeitintervall erneut einen Ping-Befehl mit definierter Anzahl zu senden. Wenn kein Echo vorhanden ist

nach der definierten Anzahl erfolgloser Wiederholungen empfangen, wird der Router neu gestartet. Es ist möglich, den Router auszuschalten.

Neustart nach definierten erfolglosen Versuchen. Daher kann diese Funktion als "Keep Alive"-Funktion verwendet werden, wenn der Router

Pingt den Host unbegrenzt oft an.

Field name	Explanation	Notes
1. Enable	Dieses Kontrollkästchen aktiviert oder deaktiviert die Ping-Reboot-Funktion.	Der Ping-Reboot ist standardmäßig deaktiviert.
2. Reboot router if no echo received	Dieses Kontrollkästchen deaktiviert den Neustart des Routers nach der definierten Anzahl erfolgloser Wiederholungen.	Dieses Kontrollkästchen muss deaktiviert werden, wenn Sie die Ping-Reboot-Funktion als "Keep Alive"-Funktion verwenden möchten.

3. Interval between Pings	Zeitintervall in Minuten zwischen zwei Pings.	Das minimale Zeitintervall beträgt 5 Minuten.
4. Ping timeout (sec)	Zeit, nach der man bedenkt, dass Ping fehlgeschlagen ist.	Range(1-9999)
5. Packet size	Dieses Feld ermöglicht es, die Größe der gesendeten Pakete zu ändern.	Sollte beibehalten werden, sofern nicht anders erforderlich.
6. Retry count	Anzahl der Male, um zu versuchen, Ping nach Ablauf der Zeitspanne an den Server zu senden, wenn der Echoempfang erfolglos war.	Die minimale Wiederholungszahl ist 1, die zweite Wiederholung erfolgt nach einem definierten Zeitintervall.
7. Host to ping from SIM 1	IP-Adresse oder Domänenname, der verwendet wird, um Ping-Pakete zu senden. Z.B. 192.168.1.1.1 (oder www.host.com, wenn der DNS-Server korrekt konfiguriert ist).	Ping-Pakete werden von SIM1 gesendet.
8. Host to ping from SIM 2	IP-Adresse oder Domänenname, der verwendet wird, um Ping-Pakete zu senden. Z.B. 192.168.1.1.1 (oder www.host.com, wenn der DNS-Server korrekt konfiguriert ist).	Ping-Pakete werden von SIM2 gesendet.

### 8.15.2 Periodic Reboot

Field name	Explanation
1. Enable	Dieses Kontrollkästchen aktiviert oder deaktiviert die Funktion Periodischer Neustart.
2. Days	Dieses Kontrollkästchen aktiviert den Neustart des Routers an den definierten Tagen.
3. Hours, Minutes	Das Hochladen erfolgt zu dieser bestimmten Zeit des Tages.

## 8.16 QoS

QoS (Quality of Service) ist die Idee, dass Übertragungsraten, Fehlerraten und andere Merkmale gemessen werden können, verbessert und teilweise im Voraus garantiert. QoS ist besonders wichtig für die kontinuierliche Übertragung von Video- und Multimedia-Informationen mit hoher Bandbreite.

QoS kann mit Traffic-Shaping-Techniken wie Paket-, Netzwerk- und Port-Priorisierung verbessert werden.

### Quality of Service

With QoS you can prioritize network traffic selected by addresses, ports or services.

**Interfaces**

Interface	Enable	Calculate overhead	Half-duplex	Download speed (kbit/s)	Upload speed (kbit/s)	
WAN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1024	128	Delete

Interface name: WAN Add

**Classification Rules**

Target	Source host	Destination host	Service	Protocol	Ports	Number of bytes	Sort	
Priority	All	All	All	All	22,53		↑ ↓	Delete
Normal	All	All	All	TCP	20,21,25,80		↑ ↓	Delete
Express	All	All	All	All	5190		↑ ↓	Delete

Add

## 8.17 Ein-/Ausgang

### 8.17.1 Status

Auf dieser Seite können Sie den aktuellen Zustand aller Ein- und Ausgänge des Routers überprüfen.

### Input/Output Status

Input/Output	
<span style="color: blue;">■</span> Digital input	Inactive
<span style="color: green;">■</span> Digital galvanically isolated input	Inactive
<span style="color: teal;">■</span> Analog input	N/A
<span style="color: orange;">■</span> Digital OC output	Inactive
<span style="color: purple;">■</span> Digital relay output	Inactive

<span style="color: blue;">1</span> Digital input	<span style="color: blue;">6</span> GND (digital & analog input)
<span style="color: green;">2</span> Digital isolated input	<span style="color: green;">7</span> GND (digital isolated input)
<span style="color: orange;">3</span> Digital OC output	<span style="color: orange;">8</span> GND (OC output)
<span style="color: orange;">4</span> External VCC	<span style="color: teal;">9</span> Analog input (0-24V)
<span style="color: purple;">5</span> Relay output (COM)	<span style="color: purple;">10</span> Relay output (NO)



### 8.17.2 Input

Ermöglicht es Ihnen, Eingabeparameter einzurichten und festzulegen, welche Aktionen nach dem Auslösen eines Ereignisses durchgeführt werden sollen.

Eingabe. Im Analogteil können Sie das Abtastintervall des Analogeingangs ändern.

Status
Input
Output

### Input/Output

Create rules for Input/Output configuration.

**Check Analog**

Interval [sec]

In the input rules section you can create and modify the rules for action after specific input triggering.

**Input Rules**

Type	Triger	Action	Enable	Sort
Digital	Input open	Output	<input type="checkbox"/>	<div style="display: flex; align-items: center; gap: 5px;"> <div style="border: 1px solid #ccc; padding: 2px;"> <span style="font-size: small;">↓</span> <span style="font-size: small;">↑</span> </div> <div style="border: 1px solid #ccc; padding: 2px 5px; font-size: x-small;">Edit</div> <div style="border: 1px solid #ccc; padding: 2px 5px; font-size: x-small;">Delete</div> </div>

\* All rules are executed in current list order.



Field name	Sample	Explanation
1. Type	Digital/Digital an isoliert/Analog	Gibt die Art Eingabe
2. Triger	Input open	Gibt an, auf welche Triggerregel angewendet wird.
3. Action	Send SMS	Gibt an, welche Aktion ausgeführt wird.
4. Enable	Enable/Disable	Eingangskonfiguration aktivieren

The screenshot shows the 'Input Configuration' form. It has three dropdown menus: 'Input type' set to 'Digital', 'Trigger' set to 'Input Open', and 'Action' set to 'Send SMS'. There is an 'Add' button to the right of the 'Action' dropdown. At the bottom right, there is a 'Save' button.

Field name	Sample	Explanation
1. Input type	Digital/Digital isolated/Analog	Eingangsart festlegen
2. Triger	Input open / Input shorted/ both	Geben Sie an, auf welche Triggerregel angewendet werden soll.
3. Action	SMS senden/ SIM-Karte ändern/ E-Mail senden/ Profil ändern/ WiFi einschalten oder einschalten/ Neustart/Ausgabe	Wählen Sie, welche Aktion nach dem Auslösen der Eingabe ausgeführt werden soll.

Nach dem Klicken auf die Schaltfläche HINZUFÜGEN (oder Bearbeiten, wenn die Regel bereits erstellt ist) erhalten Sie die zweite Seite zur Konfiguration der Eingabe, mit zusätzlichen Parametern zum Einstellen.

The screenshot shows the 'Input Configuration' form with the following settings: 'Enable' is checked, 'Input type' is 'Digital', 'Trigger' is 'Input open', 'Action' is 'Activate output', 'Output activated for (s)' is an empty text box, and 'Output type' is 'Digital OC output'. There are 'Back to Overview' and 'Save' buttons at the bottom.

Field name	Sample	Explanation
1. Enable	Enable/Disable	Diese Eingaberegeln aktivieren
2. Input type	Digital/Digital isolated/Analo	Geben Sie die Art der Eingabe an
3. Min	10	Geben Sie den minimalen Spannungsbereich an. Wird nur angezeigt, wenn der Eingangstyp analog ist.
4. Max	20	Geben Sie den maximalen Spannungsbereich an. Wird nur angezeigt, wenn der Eingangstyp analog ist.
5. Triger	Input open	Geben Sie an, auf welche Triggerregel angewendet werden soll.
6. Action	Send SMS	Geben Sie an, welche Aktion ausgeführt werden soll
7. SMS text	Input	Geben Sie den Text für den Versand von SMS an. Wird nur angezeigt, wenn die Aktion SMS senden ist.
8. Sender's phone	+37012345678	Telefonnummer, unter der Sie eine SMS erhalten. Wird nur angezeigt, wenn die Aktion ausgeführt wird.

	number		Send SMS
9.	Subject	Input	Geben Sie den Betreff der E-Mail an. Wird nur angezeigt, wenn die Aktion E-Mail senden ist.
10.	Message	Input	Geben Sie die Nachricht an, die in der E-Mail gesendet werden soll. Wird nur angezeigt, wenn die Aktion E-Mail senden ist.
11.	SMTP server	mail.example.com	Geben Sie den SMTP-Server (Simple Mail Transfer Protocol) an. Wird nur angezeigt, wenn Aktion ist E-Mail senden
12.	SMTP server	12	Geben Sie den SNMP-Serverport an. Wird nur angezeigt, wenn die Aktion E-Mail senden ist.
13.	Secure	Enable/Disabl	Geben Sie an, ob der Server SSL oder TLS unterstützt. Wird nur angezeigt, wenn die Aktion E-Mail senden ist.
14.	User name	username	Geben Sie den Benutzernamen für die Verbindung zum SNMP-Server an. Wird nur angezeigt, wenn die Aktion ausgeführt wird.
15.	Password	password	Geben Sie das Passwort des Benutzers an. Wird nur angezeigt, wenn die Aktion gesendet wird.
16.	Sender's email address	sender@example.com	Geben Sie Ihre E-Mail-Adresse an. Wird nur angezeigt, wenn die Aktion E-Mail senden ist.
17.	Recipient's email address	recipient@example.com	Geben Sie an, an wen Sie E-Mails senden möchten. Wird nur angezeigt, wenn die Aktion ausgeführt wird. E-Mail senden
18.	Sim	Primary/ Secondary	Geben Sie an, welche SIM-Karte gewechselt werden soll. Wird nur angezeigt, wenn die Aktion ausgeführt wird. SIM-Karte wechseln
19.	Profile	Admin	Geben Sie an, welches Profil eingestellt und verwendet werden soll. Wird nur angezeigt, wenn die Aktion ausgeführt wird. Profil ändern
20.	Reboot after (s)	4	Das Gerät wird nach einer bestimmten Zeit (in Sekunden) neu geladen. Wird nur angezeigt, wenn Aktion ist Neustart
21.	Output activated for (s)	10	Der Ausgang wird für eine bestimmte Zeit (in Sekunden) aktiviert. Nur angezeigt wenn Aktion aktiviert ist Ausgang aktivieren
22.	Output type	Digital OC output/ Relay	Geben Sie die Ausgabeart an, die in Abhängigkeit von der Ausgabezeit aktiviert wird.

### 8.17.3 Ausgang

#### 8.17.3.1 Ausgangskonfiguration

The screenshot shows the 'Output Configuration' page in a web interface. At the top, there are tabs for 'ON/OFF', 'Post/Get Configuration', 'Periodic Control', and 'Scheduler'. The 'Output Configuration' tab is active. Below the tabs, the page title is 'Output Configuration'. Underneath, there is a section titled 'Output configuration in active state'. This section contains two dropdown menus: 'Open collector output' is set to 'Low level' and 'Relay output' is set to 'Contacts closed'. A 'Save' button is located at the bottom right of the configuration area.

Field name	Sample	Explanation
1. Open collector	Low level / High level	Wählen Sie, welcher Open-Collector-Ausgang im aktiven Zustand sein soll.
2. Relay output	Contacts closed / Contacts open	Wählen Sie, welcher Relaisausgang im aktiven Zustand sein soll.

### 8.17.3.2 ON/OFF

Field name	Sample	Explanation
1. Digital OC output	Turn on / Turn Off	Manuelles Umschalten des digitalen OC-Ausgangs
2. Digital relay output	Turn on / Turn Off	Manuelles Umschalten des digitalen Relaisausgangs

### 8.17.3.3 Post/Get-Konfiguration

Field name	Sample	Explanation
1. Enable	Enable /Disable	POST/GET-Ausgabefunktionalität aktivieren
2. Username	User1	Service-Benutzername
3. Password	Pass1	Benutzerpasswort zur Authentifizierung

### 8.17.3.4 Periodic Control

Die periodische Steuerungsfunktion ermöglicht es dem Benutzer, einen Zeitplan einzurichten, nach dem die Ausgänge entweder eingeschaltet oder zu einem bestimmten Zeitpunkt eingeschaltet werden.

## Periodic Output Control

### Edit Output Control Rule

Enable

Output

Action

Action timeout

Timeout (sec)

Mode

Hours

Minutes

Days  Monday  
 Tuesday  
 Wednesday  
 Thursday  
 Friday  
 Saturday  
 Sunday

	Field name	Sample	Explanation
1.	Enable	Enable/Disable	Diese Ausgaberegeln aktivieren
2.	Output	Digital/Digital isolated/Analo	Geben Sie die Nachrichtenart an
3.	Action	On / Off	Geben Sie die zu ergreifenden Maßnahmen an
4.	Action timeout	Enabled / Disabled	Timeout für diese Regel aktivieren
5.	Timeout (sec)	10	Zeit in Sekunden, nach deren Ablauf der Ausgangszustand wieder in den Normalzustand übergeht.
6.	Mode	Fixed / Interval	Geben Sie den Modus der Ausgangsaktivierung an
7.	Hours	15	Geben Sie die Stunde für die Aktivierung der Regel an.
8.	Minutes	25	Geben Sie die Minute für die Aktivierung der Regel an.
9.	Days	Monday	Auswahl der Wochentage für die Regelaktivierung

### 8.17.3.5 Zeitplan

Mit dieser Funktion können Sie den periodischen, stündlichen Zeitplan für die Ausgaben einrichten. Sie können wählen, in welcher Woche Sie möchten. Tage, an denen die Ausgänge ein- oder ausgeschaltet werden.

Output Configuration
ON/OFF
Post/Get Configuration
Periodic Control
Scheduler

#### Output Scheduler

Configure Scheduled Outputs

Output: Digital relay output

Days/Hours	0-1h	1-2h	2-3h	3-4h	4-5h	5-6h	6-7h	7-8h	8-9h	9-10h	10-11h	11-12h	12-13h	13-14h	14-15h	15-16h	16-17h	17-18h	18-19h	19-20h	20-21h	21-22h	22-23h	23-24h
Monday																								
Tuesday																								
Wednesday																								
Thursday																								
Friday																								
Saturday																								
Sunday																								

Digital OC output active

Digital relay output active (relay contacts closed)

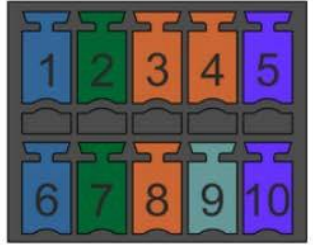
Both active

Save

### 8.17.4 Input/Output hardware information

Der Input/Output (I/O)-Anschluss befindet sich auf der Frontplatte neben den LEDs. Pinbelegung des I/O-Anschlusses:

1	Digital input (only for passive sensors)	6	GND (digital & analog input)
2	Digital isolated input (0..4V: low logic level / 9..30V: high logic level)	7	GND (digital isolated input)
3	Open collector output (0.3A Max)	8	GND (OC output)
4	External VCC (0-30V)	9	Analog input (0-24V)
5	Relay output (COM) (24V, 4A)	10	Relay output (NO)



Type	Description	Ratings	QTY
Input (digital)	Digital non-isolated input for passive sensors	3V Max	1
Input(digital)	Digital input with galvanic isolation	0..4V – low level 9..30V – high level	1
Input (analog)	Analog input (0-24V)	24V Max	1
Output (Open)	Open collector (OC) output	30V, 0.3A	1
Output (relay)	SPST relay output	24V, 4A	1

### 8.17.4.1 Digitaleingang für passive Sensoren




#### Absolute Maximalwerte:

Maximale Spannung am Eingang Pin1 in Bezug auf Pin6: 3V

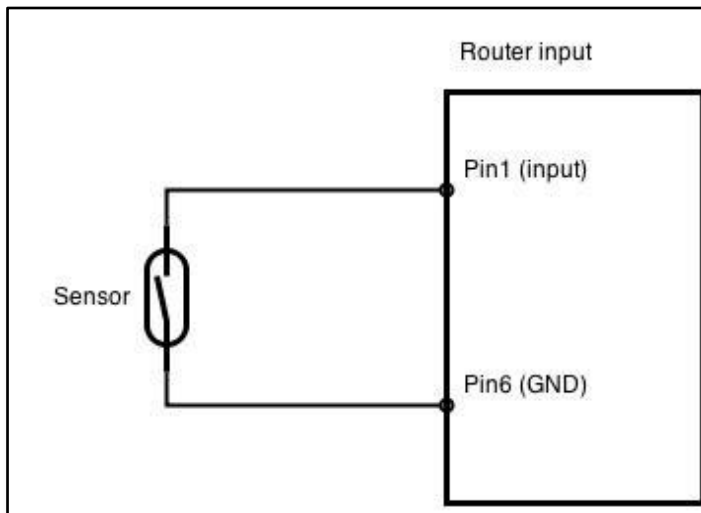
Minimale Spannung am Eingang Pin1 in Bezug auf Pin6: 0V

Der Eingang ist gegen kurze positive oder negative ESD-Transienten geschützt.

Dieser Eingang ist für den Anschluss von Sensoren mit passivem Ausgang (keine Ausgangsspannung) vorgesehen, wie z.B.:

<p>Passiv-Infrarot-(PIR)-Sensoren zur Bewegungserkennung (Sensoren mit Open-Collector- oder Relaisausgang sind für den Einsatz geeignet)</p>	
<p>Mechanische Schalter, Taster, Drucktaster</p>	 <p>SPST</p>
<p>Reedschalter, der seine Kontakte öffnet oder schließt, wenn sich das Magnetfeld nähert</p>	
<p>Jeder Sensor mit Open-Collector- oder Open-Drain-Ausgang (Verwendung ohne Pull-up-Widerstand)</p>	

Beispielschema für den Einsatz von PIR-Sensoren, mechanischen Schaltern, Reedschaltern:

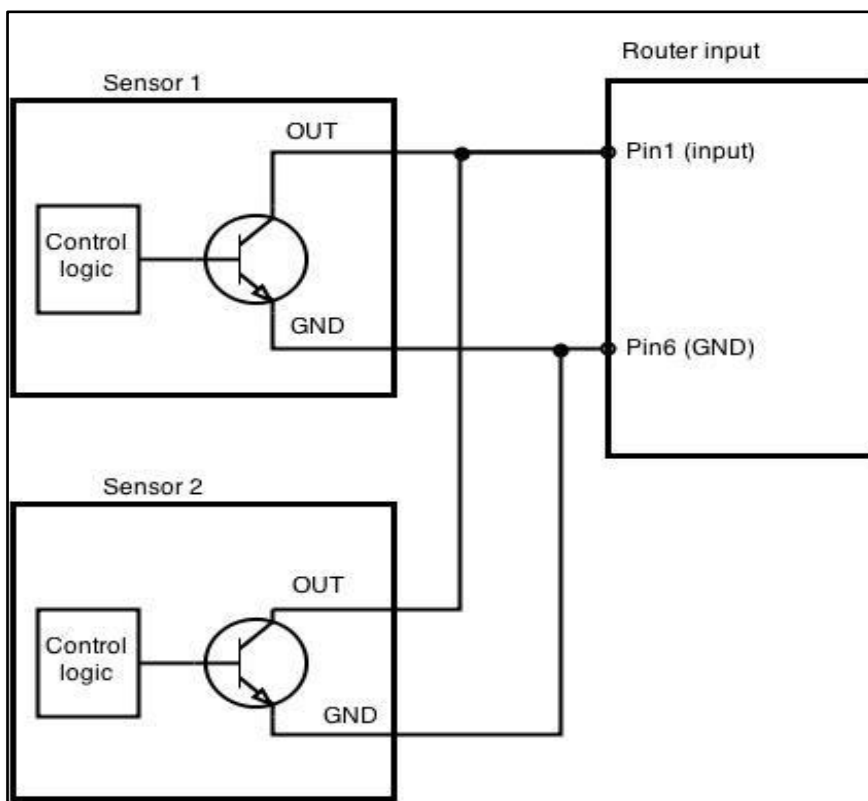


**Beispielschema für den Anschluss mehrerer Sensoren mit Open-Collector-Ausgängen:**

Mehrere Sensoren können parallel geschaltet werden, wie in der folgenden Abbildung dargestellt. In dieser Konfiguration wird jeder Sensor den Eingang aktiviert. Das Beispiel könnte mehrere Bewegungssensoren an mehreren Stellen sein. Wenn einer von ihnen es tut.

Bewegung erfassen, wird das konfigurierte Ereignis (z.B. Alarm) aktiviert. Dies ist geeignet, wenn Sie nur wissen müssen, dass

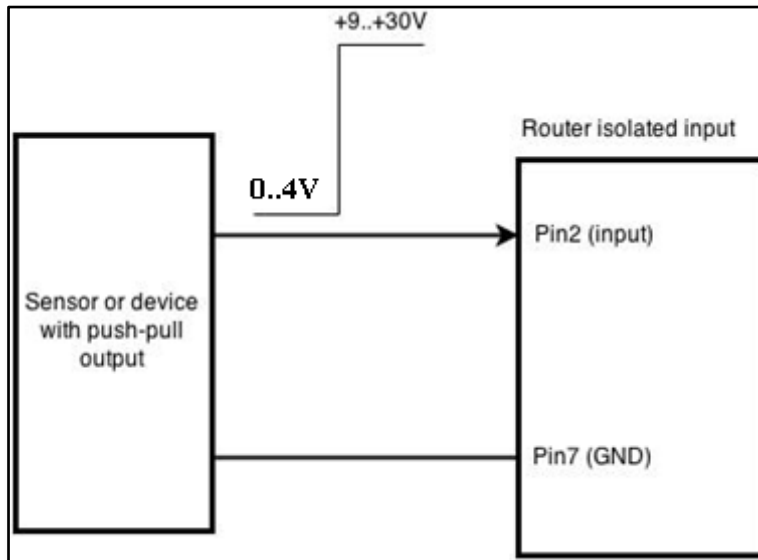
Der Alarm wird ausgelöst, aber es ist nicht notwendig zu wissen, welcher Sensor einen Alarm ausgelöst hat.



### 8.17.4.2 Digitaler, galvanisch getrennter Eingang

An diesen Eingang können Sensoren mit Gegentakt-Endstufe angeschlossen werden. Ein Beispiel für eine solche Schaltung ist im Abschnitt

Bild unten. Die Schaltung verwendet einen Optokoppler, um den Eingang zu isolieren. Im Falle eines Fehlers am Eingang wird der Rest des Stromkreises bleibt sicher.



Der Widerstand der Signalquelle sollte kleiner als  $100\Omega$  sein.

Eingangsspannungspegel:

- Niederspannung:  $0..+4V$
- Hochspannung:  $+9..30V$

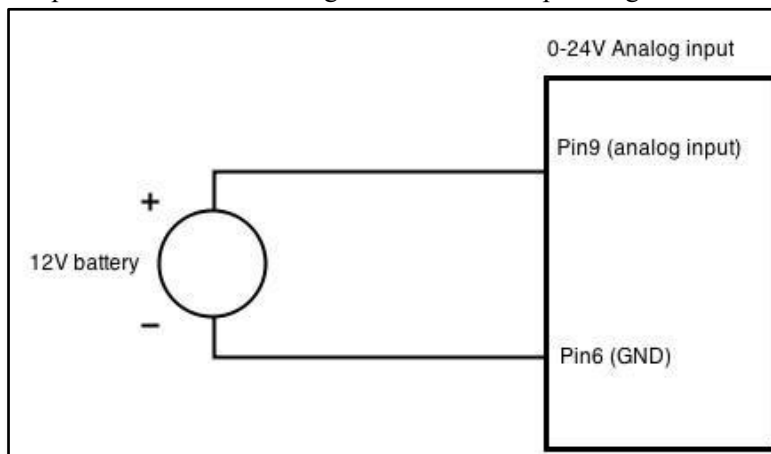
Maximale Werte:

- Die maximale Spannung, die an Pin2 in Bezug auf Pin7 angeschlossen werden kann, beträgt  $30V$ . Diese Spannung darf nicht überschritten werden!
- Der Eingang ist gegen Verpolung bis zu  $-200V$  geschützt.

### 8.17.4.3 Analog input

Der Analogeingang wurde entwickelt, um analoge Spannungen im Bereich von  $0-24V$  zu messen und in eine digitale Domäne umzuwandeln.

Beispiel für die Überwachung der  $12V$  Batteriespannung:





Elektrische Eigenschaften des Eingangs:

Parameter	Value
Maximum voltage	24V
Minimum voltage	0V
Resolution	5.859mV
Input low-pass filter cut-off frequency (-3dB)	10Hz
Input resistance (seen between I/O header pins 9 and 6)	131k $\Omega$

Eingabegenauigkeit:

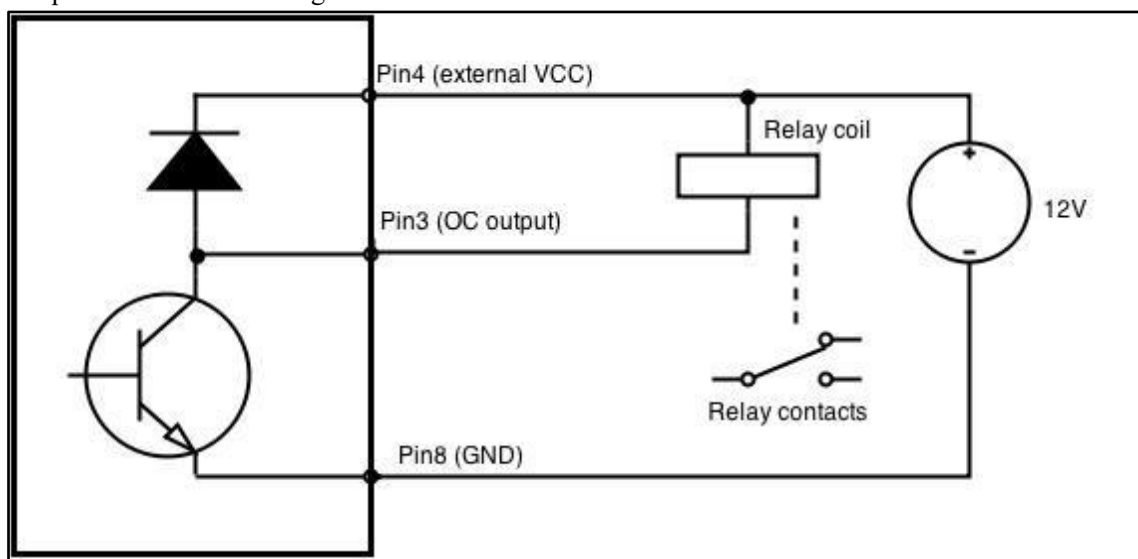
Input voltage range, V	Measurement error, %
0 <V <sub>in</sub> ≤ 1	<20
1 <V <sub>in</sub> ≤ 2	<10
2 <V <sub>in</sub> ≤ 5	<5
5 <V <sub>in</sub> ≤ 10	<1
10 <V <sub>in</sub> ≤ 24	<0.5

#### 8.17.4.4 Open-Collector-Ausgang

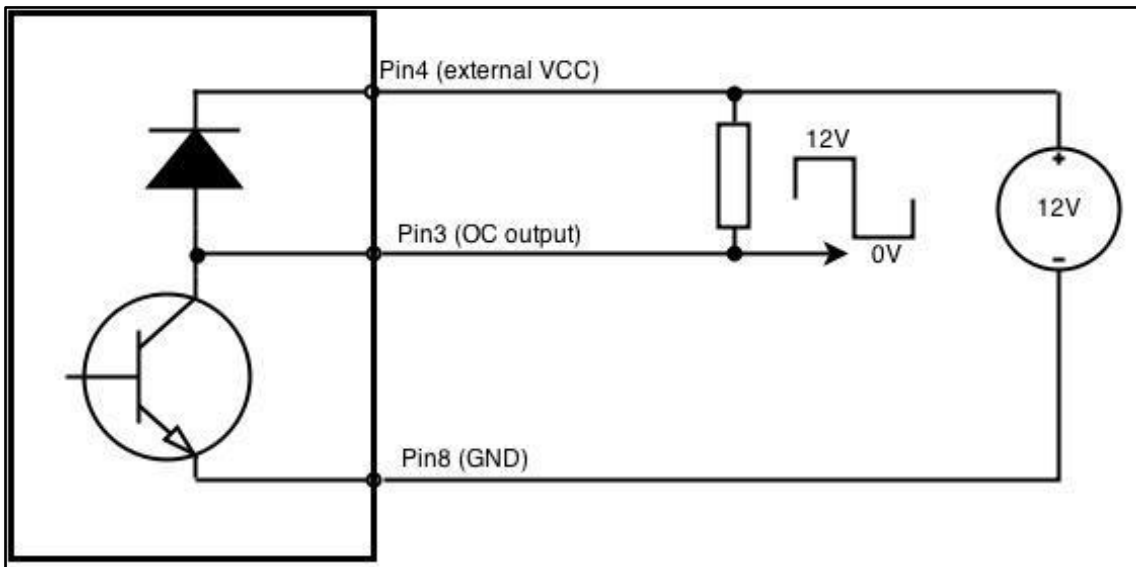
Dieser Ausgang kann zur Ansteuerung eines externen Relais verwendet werden. Damit der Ausgang korrekt funktioniert, muss die externe Spannung, die aus der die mit einem Relais verbunden ist, muss auch mit dem I/O-Stiftleisten-Pin 4 verbunden werden. Es befindet sich eine Sperrdiode im Inneren des Geräts, um die schützen Sie es vor Spitzen, die beim plötzlichen Abschalten der induktiven Last (Relaisspule) auftreten können, so dass der Anschluss der externen Diode ist nicht erforderlich. Der Ausgang ist mit einem Optokoppler vom Rest der Schaltung isoliert. Im Falle der Ausgabe Ausfall, der Rest der Schaltung bleibt geschützt.

Maximum external DC voltage	30V
Maximum output sink current	0.3A

Beispiel für die Ansteuerung eines Relais:



Der Ausgang kann auch verwendet werden, um Signale mit der gewünschten Amplitude zu erzeugen. Der Widerstand könnte z.B. 4.7kΩ sein.

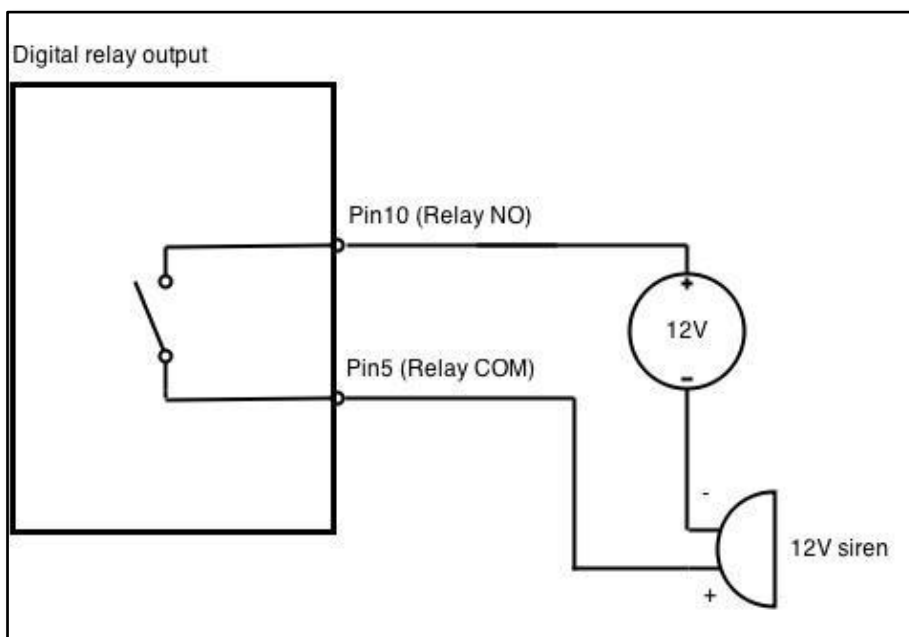


#### 8.17.4.5 Relay output

Der Relaisausgang hat zwei Pins: COM und NO. Wenn das Relais nicht angezogen ist (Ausgang nicht aktiv), sind diese Pins getrennt. Wenn das Relais aktiviert ist (Ausgang aktiv), werden diese Pins miteinander verbunden, die zum Betreiben von Wechselspannungen bestimmt sind.

Maximum DC voltage across relay contacts	24V
Maximum relay DC current	4A

Beispiel für den Anschluss der Alarmsirene an den Relaisausgang:



## 8.18 UPnP (Universal Plug & Play)

Universal Plug and Play ist ein Protokoll, das es Programmen, die auf einem Host laufen, ermöglicht, den Port automatisch zu konfigurieren. Weiterleitungen auf ihrem NAT-Router. UPnP erlaubt es grundsätzlich einem Programm, den Router dazu zu bringen, notwendige Ports zu öffnen, ohne dass er jede Intervention des Benutzers, und zwar ohne jegliche Kontrolle. Aus diesem Grund besteht ein Sicherheitsrisiko durch UPnP auf Ihrem Router aktivieren: Technisch gesehen könnte ein Wurm- oder Malwareprogramm diese Funktion nutzen, um die Sicherheit zu beeinträchtigen. für das gesamte LAN.

Settings  
field name

General Settings | **Advanced Settings**

Enable

Use secure mode

	Field name	Sample	Explanation
1.	Enable	Enable/Disable	Enable UPnP service
2.	Use secure mode	Enable/Disable	Aktivieren Sie den sicheren Modus - erlauben Sie das Hinzufügen von Weiterleitungen nur zur Anforderung von IP.

General Settings | **Advanced Settings**

Use UPnP port mapping

Use NAT-PMP port mapping

Device UUID

	Field name	Sample	Explanation
1.	Enable UPnP port aktivieren	Enable/Disable	UPnP-Portzuordnungsfunktionalität
2.	Use NAT-PMP port	Enable/Disable	NAT-PMP Mapping-Funktionalität aktivieren
3.	Device UUID	109f5a62-aca2-4654-9aed	Geben Sie die universelle eindeutige ID des Geräts an.

UPnP ACLs

ACLs specify which external ports may be redirected to which internal addresses and ports

Comment	External ports	Internal addresses	Internal ports	Action	Sort
Allow high ports	1024-65535	0.0.0.0/0	1024-65535	allow	Sort

Add

	Field name	Sample	Explanation
1.	Comment	Allow high ports	Kommentar zu dieser Regel hinzufügen
2.	External ports	1024-65535	Externe Ports, die umgeleitet werden können
3.	Internal addresses	0.0.0.0/0	Interne Adresse, die umgeleitet werden soll an

4.	Internal ports	1024-65535	Internal ports to be redirected to
5.	Action	Allow/Deny	Allow or forbid UPNP service to open the specified port

## 9 System

### 9.1 Konfigurations-Assistent

Der Konfigurationsassistent bietet eine einfache Möglichkeit, das Gerät schnell zu konfigurieren, um es auf die Basis zu bringen.

Der Assistent besteht aus 4 Schritten und ist wie folgt aufgebaut:

#### Schritt 1 (Allgemeine Änderung)

Zuerst fordert Sie der Assistent auf, das Standardpasswort zu ändern. Geben Sie einfach das gleiche Passwort in beide Felder ein.

Passwort- und Bestätigungsfelder und drücken Sie Weiter.

The screenshot displays the 'Step 1 - General' configuration screen. At the top, there are four tabs: 'Step 1 - General' (active), 'Step 2 - Mobile', 'Step 3 - LAN', and 'Step 4 - WIFI'. Below the tabs, the title 'Step - General' is shown. A message reads: 'First, let's change your router password from the default one.' The 'Password settings' section contains two input fields: 'New password' (with a masked password of seven dots and an eye icon) and 'Confirm new password' (with an empty field and an eye icon). The 'Time zone settings' section shows the 'Current system time' as '2015-05-13 06:59:23' and a 'Time zone' dropdown menu currently set to 'UTC'. A 'Sync with browser' button is located to the right of the time display. At the bottom of the form, there are two buttons: 'Skip Wizard' on the left and 'Save' on the right.

### Schritt 2 (Mobile Konfiguration)

Als nächstes müssen wir deine mobile Konfiguration eingeben. Eine detaillierte Anleitung, wie dies zu tun ist, finden Sie im Abschnitt Mobilesektion unter Netzwerk

**Step 1 - General**   **Step 2 - Mobile**   Step 3 - LAN   Step 4 - WIFI

### Mobile Configuration

Next, let's configure your mobile settings so you can start using internet right away.

#### Mobile Configuration (SIM1)

Operator profile: None

APN:

PIN number:

Dialing number: \*99#

Authentication method: None

Service mode: 4G (LTE) preferred

Show mobile info at login page:

### Schritt 3 (LAN)

Als nächstes haben Sie die Möglichkeit, Ihre LAN- und DHCP-Serveroptionen zu konfigurieren. Für eine detaillierte Erklärung siehe LAN unter Netzwerk.

**Step 1 - General**   **Step 2 - Mobile**   **Step 3 - LAN**   Step 4 - WIFI

### Step - LAN

Here we will setup the basic settings of a typical LAN configuration. The wizard will cover 2 basic configurations: static IP address LAN and DHCP client.

#### General Configuration

IP address: 192.168.1.1

Netmask: 255.255.255.0

Enable DHCP:

Start: 100

Limit: 150

Lease time: 12h

### Schritt 4 (Wi-Fi)

Im letzten Schritt können Sie Ihre WLAN-Einstellungen konfigurieren, um einen rudimentären Access Point einzurichten.

**Step 1 - General**   **Step 2 - Mobile**   **Step 3 - LAN**   **Step 4 - WiFi**

### Step - Wireless

Now let's configure your wireless radio. (Note: if you are currently connecting via wireless and you change parameters, like SSID, encryption, etc. your connection will be dropped and you will have to reconnect with a new set of parameters.)

#### WiFi Configuration

Enable wireless

SSID

Mode

Channel

Encryption

Country Code

Wenn Sie mit dem Konfigurationsassistenten fertig sind, klicken Sie auf **Speichern**.

## 9.2 Profile

Der Router kann praktisch unbegrenzt viele oder Konfigurationsprofile haben, die Sie später entweder über das WebUI anwenden können.

oder per SMS. Wenn Sie ein neues Profil hinzufügen, speichern Sie die aktuelle vollständige Konfiguration des Routers.

Hinweis: Die Profilnamen dürfen 10 Symbole nicht überschreiten.

## Configuration Profiles

### Manage Profiles

Profile name

Profile name	Created	Action
first	2014-12-03	<input type="button" value="Apply"/> <input type="button" value="Delete"/>

## 9.3 Administration

### 9.3.1 Allgemeines

General	Troubleshoot	Backup	Access Control	Diagnostics	MAC Clone	Overview	Monitoring
---------	--------------	--------	----------------	-------------	-----------	----------	------------

### Administration Settings

**Router Name And Host Name**

Router name

Host name

**Administrator Password**

New password

Confirm new password

**Language Settings**

Language

**IPv6 Support**

Enable

**Login Page**

Show mobile info at login page

Show WAN IP at login page

**Leds indication**

Enable

**Restore Default Settings**

Restore to default

Field name	Explanation
1. Router name	Geben Sie Ihren neuen Routernamen ein.
2. Host name	Geben Sie Ihren neuen Hostnamen ein
3. New Password	Geben Sie Ihr neues Administrator-Passwort ein. Wenn du dieses Passwort änderst, ändert sich auch das SSH-Passwort.
4. Confirm new password	Geben Sie Ihr neues Administrator-Passwort erneut ein.
5. Language	Die Website wird in die ausgewählte Sprache übersetzt.
6. IPv6 support	IPv6-Unterstützung für Router aktivieren
7. Show mobile info at login page	Zeigt Bediener und Signalstärke auf der Login-Seite an.
8. Show WAN IP at login page	WAN IP auf der Login-Seite anzeigen.
9. On/Off leds	Wenn Sie die Markierung entfernen, sind alle Router-LEDs ausgeschaltet.
10. Restore to default	Der Router wird auf die werkseitigen Standardeinstellungen zurückgesetzt.

**Wichtige Hinweise:**

Der einzige Weg, Zugang zur Webverwaltung zu erhalten, wenn Sie das Administratorkennwort vergessen haben, ist das Zurücksetzen der

werkseitige Standardeinstellungen des Geräts. Die Standard-Administrator-Login-Einstellungen sind:

Benutzername: admin

Passwort: admin01

**9.3.2 Fehlerbehebung**

Field name	Explanation
1. System log level	Der Debug-Level sollte immer verwendet werden, sofern nicht anders angegeben.
2. Save log in	Der Standard-RAM-Speicher sollte immer verwendet werden, sofern nicht anders angegeben.
3. Include GSMD information	Die Standardeinstellung - aktiviert - sollte verwendet werden, sofern nicht anders angegeben.
4. Include PPPD information	Die Standardeinstellung - deaktiviert - sollte verwendet werden, sofern nicht anders
5. Include Chat script information	Die Standardeinstellung - aktiviert - sollte verwendet werden, sofern nicht anders angegeben.
6. Include network topology information	Die Standardeinstellung - deaktiviert - sollte verwendet werden, sofern nicht anders angegeben.
7. System Log	Bietet Informationen zur Systemprotokollierung auf dem Bildschirm. Sie ersetzt jedoch nicht die Fehlerbehebungsdatei, die Sie aus dem Menü System -> Backup und Firmware herunterladen können.
8. Kernel Log	Bietet Informationen zur Kernel-Protokollierung auf dem Bildschirm. Sie ersetzt jedoch nicht die Fehlerbehebungsdatei, die Sie aus dem Menü System -> Backup und Firmware herunterladen können.
9. Troubleshoot	Herunterladbares Archiv, das die vollständige Router-Konfiguration und alle Systemprotokolldateien enthält.



## 9.3.3 Backup

General	Troubleshoot	Backup	Access Control	Diagnostics	MAC Clone	Overview	Monitoring
<b>Backup</b>							
<b>Backup Configuration</b>							
Backup archive: <input type="button" value="Download"/>							
<b>Restore Configuration</b>							
<input type="button" value="Upgrade from file"/>							
Restore from backup: <input type="button" value="Browse..."/> No file selected.							
<input type="button" value="Upload archive"/>							

Field name	Explanation
1. Backup archive	Laden Sie die aktuelle Router-Einstellungsdatei auf den PC herunter. Diese Datei kann in einen anderen RUT900 mit gleicher Firmware-Version geladen werden, um sie schnell zu konfigurieren.
2. Restore from backup	Auswählen, Hochladen und Wiederherstellen der Router-Einstellungsdatei vom PC aus.

## 9.3.3.1 Zutrittskontrolle Allgemein

General	Safety
<b>Access Control</b>	
<b>SSH Access Control</b>	
Enable SSH access <input checked="" type="checkbox"/>	
Remote SSH access <input type="checkbox"/>	
Port <input type="text" value="22"/>	
<b>Web Access Control</b>	
Enable HTTP access <input checked="" type="checkbox"/>	
Enable remote HTTP access <input type="checkbox"/>	
Port <input type="text" value="80"/>	
Enable remote HTTPS access <input type="checkbox"/>	
Port <input type="text" value="443"/>	
<b>CLI Configuration</b>	
Enable CLI <input checked="" type="checkbox"/>	
Enable remote CLI <input type="checkbox"/>	
Port <input type="text" value="4200"/>	

Field name	Explanation
1. Enable SSH access	Aktivieren Sie das Kontrollkästchen, um den SSH-Zugriff zu aktivieren.
2. Remote SSH access	Aktivieren Sie das Kontrollkästchen, um den Remote-SSH-Zugriff zu aktivieren.
3. Port	Port, der für die SSH-Verbindung verwendet werden soll.
4. Enable HTTP access	Ermöglicht HTTP-Zugriff auf den Router
5. Enable remote HTTP access	Ermöglicht Remote-HTTP-Zugriff auf den Router
6. Port	Port, der für die HTTP-Kommunikation verwendet werden soll.
7. Enable remote HTTPS access	Ermöglicht den entfernten HTTPS-Zugriff auf den Router.
8. Port	Port, der für die HTTPS-Kommunikation verwendet werden soll.
9. Enable CLI	Aktiviert die Befehlszeilenschnittstelle
10. Enable remote CLI	Aktiviert die entfernte Befehlszeilenschnittstelle
11. Port	Port, der für die CLI-Kommunikation verwendet werden soll.

Hinweis: Der Router hat 2 Benutzer: "admin" für das WebUI und "root" für SSH. Wenn Sie sich über SSH anmelden, verwenden Sie "root".

### 9.3.3.2 Sicherheit der Zugangskontrolle

The screenshot shows the 'Access Control' configuration page. The 'Block Unwanted Access' section is active. Under 'SSH Access Secure', there are three options: 'Enable' (checkbox), 'Clean after reboot' (checkbox), and 'Fail count' (input field with value 5). Similarly, under 'WebUI Access Secure', there are three options: 'Enable' (checkbox), 'Clean after reboot' (checkbox), and 'Fail count' (input field with value 5). Below this is a table titled 'List Of Blocked Addresses' with columns 'Service' and 'Blocked address'. The table is empty, and a message below it states 'There are no addresses blocked'.

Field name	Explanation
1. SSH access secure enable	Aktivieren Sie das Kontrollkästchen, um die sichere Funktionalität für den SSH-Zugriff zu aktivieren.
2. Clean after reboot	Wenn das Kontrollkästchen aktiviert ist - blockierte Adressen werden nach jedem Neustart entfernt.
3. Fail count	Gibt die maximale Anzahl der Verbindungsversuche vor der Zugriffsblockierung an.
4. WebUIaccess secure enable	Aktivieren Sie das Kontrollkästchen, um den sicheren WebUI-Zugriff zu aktivieren.

### 9.3.4 Diagnostics

Field name

Field name	Explanation
1. Host	Geben Sie die IP-Adresse des Servers oder den Hostnamen ein.
2. Ping	Dienstprogramm, das verwendet wird, um die Erreichbarkeit eines Hosts in einem Internet-IP-Netzwerk zu testen und die Umlaufzeit für Nachrichten zu messen, die vom Ursprungshost an einen Zielservers gesendet werden. Die Server-Echo-Antwort wird nach wenigen Sekunden angezeigt, wenn der Server erreichbar ist.
3. Traceroute	Diagnosetool zum Anzeigen der Route (des Pfades) und zum Messen von Transitverzögerungen von Paketen über eine Internet IP-Netzwerk. Ein Protokoll mit Routeninformationen wird nach wenigen Sekunden angezeigt.
4. Nslookup	Befehlszeilen-Tool zur Netzwerkadministration zum Abfragen des Domain Name System (DNS), um Domännennamen oder IP-Adressenzuordnungen oder andere spezifische DNS-Einträge zu erhalten. Das Protokoll, das Informationen über die DNS-Suche des angegebenen Servers enthält, wird nach einigen Sekunden angezeigt.

### 9.3.5 MAC Clone

Field name	Explanation
1. WAN MAC address	Neue WAN-MAC-Adresse eingeben

## 9.3.6 Übersicht

General	Troubleshoot	Backup	Access Control	Diagnostics	MAC Clone	Overview	Monitoring
<b>Overview Page Configuration</b>							
<b>Overview Tables</b>							
			Mobile	<input checked="" type="checkbox"/>			
			SMS counter	<input type="checkbox"/>			
			System	<input checked="" type="checkbox"/>			
			Wireless	<input checked="" type="checkbox"/>			
			WAN	<input checked="" type="checkbox"/>			
			Local network	<input checked="" type="checkbox"/>			
			Access control	<input checked="" type="checkbox"/>			
			Recent system events	<input checked="" type="checkbox"/>			
			Recent network events	<input checked="" type="checkbox"/>			
			Teltonika_Router Hotspot	<input type="checkbox"/>			
			VRRP	<input type="checkbox"/>			
			Monitoring	<input type="checkbox"/>			

Field name	Explanation
1. Mobile	Kontrollkästchen, um die mobile Tabelle auf der Übersichtsseite anzuzeigen.
2. SMS counter	Kontrollkästchen zum Anzeigen der SMS-Zählertabelle auf der Übersichtsseite
3. System	Kontrollkästchen zum Anzeigen der Systemtabelle auf der Übersichtsseite
4. Wireless	Aktivieren Sie das Kontrollkästchen, um die Wireless-Tabelle auf der Übersichtsseite anzuzeigen.
5. WAN	Kontrollkästchen zum Anzeigen der WAN-Tabelle auf der Übersichtsseite
6. Local network	Kontrollkästchen, um die Tabelle des lokalen Netzwerks auf der Übersichtsseite anzuzeigen.
7. Access control	Kontrollkästchen, um die Zugriffskontrolltabelle auf der Übersichtsseite anzuzeigen.
8. Recent system events	Kontrollkästchen, um die Tabelle der letzten Systemereignisse auf der Übersichtsseite anzuzeigen.
9. Recent network events	Kontrollkästchen, um die Tabelle der letzten Netzwerkereignisse auf der Übersichtsseite anzuzeigen.
10. <Hotspot name> Hotspot	Kontrollkästchen, um die Hotspot-Instanzentabelle auf der Übersichtsseite anzuzeigen.
11. VRRP	Kontrollkästchen zum Anzeigen der VRRP-Tabelle auf der Übersichtsseite
12. Monitoring	Kontrollkästchen, um die Überwachungstabelle auf der Übersichtsseite anzuzeigen.

### 9.3.7 Überwachung

Die Überwachungsfunktionalität ermöglicht die Verbindung Ihres Routers mit dem Fernüberwachungssystem. Auch Mac-Adresse und Router-Seriennummern werden zur Vereinfachung auf dieser Seite angezeigt, da sie beim Hinzufügen von Gerät an das Überwachungssystem.

General	Troubleshoot	Backup	Access Control	Diagnostics	MAC Clone	Overview	Monitoring
---------	--------------	--------	----------------	-------------	-----------	----------	------------

### Remote Monitoring

**Remote Access Control**

Enable remote monitoring

**Status**

Monitoring	Disabled
Router LAN MAC address	00:1E:42:00:00:00
Router serial number	00000001

Refresh

Save

Field name	Explanation
------------	-------------

- |                             |   |
|-----------------------------|---|
| 1. Enable remote monitoring | Enables the device to connect to remote monitoring system |
|-----------------------------|---|

### 9.4 Benutzerskripte

Fortgeschrittene Benutzer können ihre eigenen Befehle eingeben, die am Ende des Bootvorgangs ausgeführt werden.

```
# Put your custom commands here that should be executed once
# the system init finished. By default this file does nothing.

exit 0
```

Upload script file  No file selected.

Backup script file

## 9.5 Abgesicherter Modus

Der Router enthält zwei Firmware-Images in seinem internen Flash-Speicher. Das Master-Firmware-Image ist das Standard-Image und wird vom Benutzer ständig genutzt. Eine weitere ist die Safe Mode Firmware, d.h. die Sicherung der Master-Firmware.

Die Safe Mode Firmware ist ähnlich wie die Master-Firmware, aber um ihre Größe zu reduzieren, werden einige Funktionen wie - Drahtloser Hotspot, VRRPD, SNMP, Webfilter werden entfernt.

Die Safe Mode Firmware ist an einem anderen Logo und einem reduzierten Menü im WebUI zu erkennen. Der einzige Zweck von Safe Mode Firmware soll es dem Benutzer ermöglichen, die Master-Firmware zu aktualisieren und dabei alle vorherigen Konfigurationen zu entfernen. Einstellungen. Um den abgesicherten Modus nützlich zu machen, wird dringend empfohlen, die Konfiguration der Master-Firmware zu sichern, wenn der Benutzer ist mit dem Setup zufrieden. Nachdem das Konfigurations-Backup erstellt wurde, kann es durch Aufrufen des abgesicherten Modus getestet werden.

### Safe Mode

**Status**

Safe mode FW version RUT9XX\_SM\_00.01.292

Safe mode config backup date 2015-05-12, 12:12:09

**Safe Mode Configuration**

Write configuration to config partition

Delete configuration from config partition

Request safemode after reboot

## 9.6 Firmware

### 9.6.1 Firmware

Firmware
FOTA

### Firmware

**Current Firmware Information**

**Firmware Available On Server**

Firmware version	RUT9XX_R_00.01.299	Firmware version	RUT9XX_R_00.01.50
Firmware build date	2015-05-13, 11:26:59		
Kernel version	3.10.36		

**Firmware Upgrade Settings**

Keep all settings <input type="checkbox"/>	Keep dynamic DNS settings <input type="checkbox"/>
Keep network settings <input type="checkbox"/>	Keep wireless settings <input type="checkbox"/>
Keep mobile settings <input type="checkbox"/>	Keep firewall settings <input type="checkbox"/>
Keep LAN settings <input type="checkbox"/>	Keep OpenVPN settings <input type="checkbox"/>

Upgrade from file ▼
Firmware image file  No file selected.

**Einstellungen beibehalten** - wenn das Kontrollkästchen aktiviert ist, behält der Router die gespeicherten Benutzerkonfigurationseinstellungen nach der Firmware.

Upgrade. Wenn das Kontrollkästchen nicht aktiviert ist, werden alle Router-Einstellungen nach dem Firmware-Upgrade auf die Werkseinstellungen zurückgesetzt.

Beim Aktualisieren der Firmware können Sie Einstellungen wählen, die Sie nach dem Upgrade beibehalten möchten. Diese Funktion ist nützlich

wenn die Firmware über das Internet (remote) aktualisiert wird und Sie danach die Verbindung zum Router nicht verlieren dürfen.

**FW-Bild** - Router-Firmware-Upgrade-Datei.

**Warnung:** Entfernen Sie niemals die Stromversorgung des Routers und drücken Sie während des Upgrade-Vorgangs nicht die Reset-Taste! Dies würde Ihren Router ernsthaft beschädigen und ihn unzugänglich machen. Wenn Sie irgendwelche Probleme im Zusammenhang mit einem Firmware-Upgrade haben, können Sie sollte sich immer an den örtlichen Händler wenden.

## 9.6.2 FOTA

Field name	Explanation
1. Server address	Specify server address to check for firmware updates. E.g. "http://teltonika.sritis.lt/rut9xx_auto_update/clients/"
2. User name	Benutzername für die Serverberechtigung
3. Password	Passwortname für die Serverberechtigung
4. Enable auto check	Kontrollkästchen, um die automatische Überprüfung auf neue Firmware-Updates zu aktivieren.
5. Auto check mode	Wählen Sie aus, wann die automatische Überprüfungsfunktion ausgeführt werden soll.
6. WAN wired	Ermöglicht das Aktualisieren der Firmware vom Server nur, wenn der Router über ein WAN verfügt (wenn das Kontrollkästchen aktiviert ist).

## 9.7 Wiederherstellungspunkt

### 9.7.1 Wiederherstellungspunkt erstellen

Ermöglicht die Erstellung von Firmware-Restorepoints mit allen benutzerdefinierten Konfigurationen. Sie können die erstellten Wiederherstellungspunkte herunterladen, oder speichern Sie sie auf dem externen Speichergerät des Routers.

### 9.7.2 Punktlast wiederherstellen

Ermöglicht die Wiederherstellung der Konfiguration aus dem zuvor gespeicherten Wiederherstellungspunkt. Sie können den Wiederherstellungspunkt von Ihrem Computer oder aus dem externen Speicher des Routers.

## 9.8 Neustart

Starten Sie den Router neu, indem Sie die Taste "Reboot" drücken.

## 10 Gerätewiederherstellung

Im folgenden Abschnitt werden die verfügbaren Optionen zur Behebung von Fehlfunktionen des Geräts beschrieben. Normalerweise kann das Gerät nicht erreichbar werden, weil die Stromversorgung während des Firmware-Upgrades unterbrochen wurde oder wenn seine Kerndateien in der Datei falsch geändert wurden. System. Die Router von Teltonika bieten mehrere Möglichkeiten, sich von diesen Situationen zu erholen.



## 10.1 Reset-Taste

Die Reset-Taste befindet sich auf der Rückseite des Gerätes. Die Reset-Taste hat mehrere Funktionen: Starten Sie das Gerät neu. Nach dem Start des Gerätes, wenn die Reset-Taste bis zu 4 Sekunden lang gedrückt wird.

wird das Gerät neu gestartet. Der Start des Neustarts wird durch Blinken aller 5 Signalstärke-LEDs angezeigt.

zusammen mit der grünen Verbindungsstatus-LED.

Zurücksetzen auf die Standardeinstellungen. Nach dem Start des Gerätes, wenn die Reset-Taste mindestens 5 Sekunden lang gedrückt wird.

Das Gerät setzt alle Benutzeränderungen auf die Werkseinstellungen zurück und startet neu. Um dem Benutzer zu helfen, zu bestimmen, wie lange er benötigt.

die Reset-Taste gedrückt werden sollte, zeigen die Signalstärke-LEDs die abgelaufene Zeit an. Alle 5 leuchtenden LEDs bedeuten

dass 5 Sekunden vergangen sind und die Reset-Taste losgelassen werden kann. Der Beginn des

Zurücksetzens auf die Standardeinstellungen ist

wird durch Blinken aller 5 Signalstärke-LEDs zusammen mit der roten Verbindungsstatus-LED angezeigt.

SIM-PIN ein

die HauptsIM-Karte ist der einzige Benutzerparameter, der nach dem Zurücksetzen auf die Standardeinstellungen beibehalten wird.

## 10.2 Safemode

Der Router enthält zwei Firmware-Images in seinem internen Flash-Speicher. Eine davon ist die Master-Firmware, die der Standard ist.

Firmware on wird vom Benutzer ständig verwendet. Eine weitere ist die Safemode-Firmware, die die Rolle des Backups auf die

Master-Firmware.

Safemode Firmware hat die meiste Funktion der Master-Firmware, aber um die Größe des Wireless Hotspots zu reduzieren,

VRRPD-, SNMP- und Webfilterfunktion wurden entfernt. Die Safemode-Firmware kann an verschiedenen Logos erkannt werden.

reduziertes Menü im WebUI. Der einzige Zweck der Safemode-Firmware ist es, dem Benutzer zu ermöglichen, die Master-Firmware zu aktualisieren.

den Router und um dabei alle vorherigen Konfigurationsänderungen zurückzusetzen. Um den Safemode nützlich zu machen, ist es wichtig.

empfohlen, die Konfiguration der Master-Firmware zu sichern, wenn der Benutzer mit dem Setup zufrieden ist (beschrieben unter **Error!**

**Referenzquelle nicht gefunden**

**.section).** Nachdem das Konfigurations-Backup erstellt wurde und es durch Anfordern des Safemode getestet werden kann.

## 10.3 Bootloader's WebUI

Der Bootloader bietet auch eine Möglichkeit, die Router-Funktionalität wiederherzustellen, wenn die Firmware beschädigt ist. Um es zu schaffen easierto use bootloader hat einen eigenen Webserver, der mit jedem Webbrowser erreichbar ist. Vorgehensweise zum Starten des Webservers des Bootloaders:

### Automatisch

. Es passiert, wenn der Bootloader weder Master noch Safemode erkennt.

Firmware. Das Blinken aller 4 Ethernet-LEDs zeigt an, dass der Webserver des Bootloaders gestartet ist.

### Manuell

. Der Webserver des Bootloaders kann angefordert werden, indem man die Reset-Taste 3 Sekunden lang gedrückt hält. Einschalten des Gerätes. Das Blinken aller 4 Ethernet-LEDs zeigt an, dass der Webserver des Bootloaders gestartet ist. Auf das WebUI des Bootloaders kann durch Eingabe dieser Adresse im Webbrowser zugegriffen werden:

<http://192.168.1.1/index.html>

Hinweis: Es kann notwendig sein, den Cache des Webbrowsers zu leeren und das incognito/anonyme Fenster für den Zugriff zu verwenden. WebUI des Bootloaders.

## 11 Glossary:

WAN - Wide Area Network ist ein Telekommunikationsnetzwerk, das ein breites Gebiet abdeckt (d.h. jedes Netzwerk, das eine Verbindung herstellt). über metropolitane, regionale oder nationale Grenzen hinweg). Hier verwenden wir den Begriff WAN für das externe Netzwerk, das von der mit dem der Router das Internet erreicht. LAN - Ein lokales Netzwerk (LAN) ist ein Computernetzwerk, das Computer in einem begrenzten Bereich, wie beispielsweise einem Heim, Schule, Computerlabor oder Bürogebäude. DHCP - Das Dynamic Host Configuration Protocol (DHCP) ist ein Netzwerkkonfigurationsprotokoll für Hosts im Internet. Protokoll (IP) Netzwerke. Computer, die mit IP-Netzwerken verbunden sind, müssen konfiguriert werden, bevor sie kommunizieren können. mit anderen Hosts. Die wichtigsten Informationen, die benötigt werden, sind eine IP-Adresse sowie eine Standardroute und ein Routing-Präfix. DHCP eliminiert die manuelle Aufgabe durch einen Netzwerkadministrator. Es bietet auch eine zentrale Datenbank mit Geräten, die verbunden sind. an das Netzwerk und eliminiert doppelte Ressourcenzuweisungen.

ETHERNET-KABEL - Bezieht sich auf das CAT5 UTP-Kabel mit einem RJ-45-Anschluss.

AP - Zugangspunkt. Ein Zugangspunkt ist jede Vorrichtung, die eine drahtlose Verbindung für drahtlose Clients bereitstellt. In diesem

Wenn Sie Wi-Fi auf Ihrem Router aktivieren, wird Ihr Router zu einem Zugangspunkt.

DNS - Domain Name Resolver. A Server, der Namen wie z.B. [www.google.lt](http://www.google.lt) zu ihren jeweiligen IPs. In

Damit Ihr Computer oder Router mit einem externen Server kommunizieren kann, muss er seine IP-Adresse und seinen Namen kennen.

["www.something.com"](http://www.something.com) Das reicht einfach nicht. Es gibt spezielle Server, die diese spezielle Aufgabe der Lösung übernehmen.

Namen in IPs, sogenannte Domain Name Server. Wenn Sie keinen DNS angegeben haben, können Sie trotzdem im Web surfen, vorausgesetzt, dass Sie kennen die IP der Website, die Sie zu erreichen versuchen.

ARP - Abkürzung für Adress Resolution Protocol, ein Netzwerkschichtprotokoll, das verwendet wird, um eine IP-Adresse in eine physikalische umzuwandeln.

Adresse (genannt *DLC address*), wie z.B. eine Ethernet-Adresse.

PPPoE - Punkt-zu-Punkt-Protokoll über Ethernet. PPPoE ist eine Spezifikation für die Verbindung der Benutzer über ein Ethernet mit der

das Internet über ein gängiges Breitbandmedium, wie z.B. DSL-Anschluss, drahtloses Gerät oder Kabelmodem.

DSL - Digitaler Teilnehmeranschluss - es ist eine Familie von Technologien, die den Internetzugang durch Übertragung digitaler Daten ermöglichen.

unter Verwendung eines lokalen Telefonnetzes, das das öffentliche Telefonnetz verwendet.

NAT - network address translation - ein Internetstandard, der es einem lokalen Netzwerk (LAN) ermöglicht, einen Satz zu verwenden.

von IP-Adressen für den Internetverkehr und einem zweiten Satz von Adressen für den externen Verkehr.

LCP - Link Control Protocol - ein Protokoll, das Teil des PPP (Point-to-Point Protocol) ist. Das LCP prüft die Identität der verknüpften Vorrichtung und akzeptiert oder lehnt die Peer-Vorrichtung ab, bestimmt die zulässige Paketgröße für Übertragung, sucht nach Konfigurationsfehlern und kann die Verbindung abbrechen, wenn die Parameter nicht erfüllt sind. BOOTP - Bootstrap Protocol - ein Internet-Protokoll, das es einem plattenlosen Arbeitsplatz ermöglicht, seine eigene IP zu entdecken.

Adresse, die IP-Adresse eines BOOTP-Servers im Netzwerk und eine Datei, die in den Speicher geladen werden soll, um den Rechner zu starten.

Dadurch kann die Workstation ohne Festplatte oder Diskettenlaufwerk gestartet werden.

TCP - Transmission Control Protocol - eines der wichtigsten Protokolle in TCP/IP-Netzwerken. Während das IP-Protokoll behandelt nur Pakete, TCP ermöglicht es zwei Hosts, eine Verbindung aufzubauen und Datenströme auszutauschen. TCP garantiert

Lieferung von Daten und garantiert auch, dass die Pakete in der gleichen Reihenfolge zugestellt werden, in der sie gesendet wurden.

TKIP - Temporal Key Integrity Protocol - verschlüsselt die Schlüssel mit Hilfe von Hashing-Algorithmen und durch Hinzufügen einer Integrität. Überprüfungsfunktion, stellen Sie sicher, dass die Schlüssel nicht manipuliert wurden.

CCMP - Counter Mode Cipher Block Chaining Message Authentication Code Protocol – Verschlüsselungsprotokoll entwickelt für Wireless LAN-Produkte, die die Standards der IEEE 802.11i Änderung zum Original umsetzen.

Norm IEEE802.11. CCMP ist eine unveränderte Datenkryptographiekapselung, die für die Vertraulichkeit von Daten entwickelt wurde. basierend auf dem Counter Mode mit CBC-MAC (CCM) des AES (Advanced Encryption Standard) Standards.

MAC - Media Access Control - Hardware-Adresse, die jeden Knoten eines Netzwerks eindeutig identifiziert. In IEEE 802

Netzwerken ist die Data Link Control (DCL)-Schicht des ISO-Referenzmodells in zwei Teilschichten unterteilt: die Logische Verbindung

Control (LLC)-Schicht und die Media Access Control-Schicht. Die MAC-Schicht ist direkt mit dem Netzwerkmedium verbunden. Folglich erfordert jede Art von Netzwerkmedium eine andere MAC-Schicht.

DMZ - Demilitarisierte Zone - ein Computer oder ein kleines Subnetz, das sich zwischen einem vertrauenswürdigen internen Netzwerk befindet, wie beispielsweise

ein privates Firmen-LAN und ein nicht vertrauenswürdigen externes Netzwerk, wie beispielsweise das öffentliche Internet. UDP - User Datagram Protocol - ein verbindungsloses Protokoll, das, wie TCP, auf IP-Netzwerken läuft. Bietet sehr wenige Fehlerbehebungsdienste, die stattdessen einen direkten Weg zum Senden und Empfangen von Datagrammen über ein IP-Netzwerk bieten.

VPN - Virtual Private Network - ein Netzwerk, das unter Verwendung öffentlicher Leitungen - in der Regel des Internets - aufgebaut wird, um

Verbindung zu einem privaten Netzwerk, wie beispielsweise dem internen Netzwerk eines Unternehmens.

VRRP - Virtual Router Redundancy Protocol - ein Wahlprotokoll, das dynamisch die Verantwortung für einen Router zuweist.

oder mehrere virtuelle Router zu den VRRP-Routern in einem LAN, so dass mehrere Router auf einer Multi-Access-Verbindung die Möglichkeit haben, die gleiche virtuelle IP-Adresse.

GRE Tunnel - Generic Routing Encapsulation - ein von Cisco Systems entwickeltes Tunneling-Protokoll, das Folgendes ermöglicht

kapselt eine Vielzahl von Netzwerkschichtprotokollen in virtuellen Punkt-zu-Punkt-Verbindungen über ein Internet-Protokoll. Internetwork.

PPPD - Point to Point Protocol Daemon - es wird verwendet, um Netzwerkverbindungen zwischen zwei Knoten unter Unix zu verwalten.

wie Betriebssysteme. Die Konfiguration erfolgt über Kommandozeilenargumente und Konfigurationsdateien.

SSH - Secure SHell - ein Programm, um sich über ein Netzwerk an einem anderen Computer anzumelden, um Befehle in einer entfernten Umgebung auszuführen.

Maschine, und um Dateien von einer Maschine auf eine andere zu verschieben. Es bietet starke Authentifizierung und sichere Kommunikation. über unsichere Kanäle.

VRRPD - Virtual Router Redundancy Protocol - es wurde entwickelt, um den Single Point of Failure zu eliminieren.

mit statisch gerouteten Netzwerken, indem es automatisch ein Failover mit mehreren LAN-Pfaden über alternative Router bereitstellt.

SNMP - Simple Network Management Protocol - eine Reihe von Protokollen zur Verwaltung komplexer Netzwerke. SNMP funktioniert

durch Senden von Nachrichten, sogenannten Protokolldateneinheiten (PDUs), an verschiedene Teile eines Netzwerks.

\*\*\* Übersetzt mit [www.DeepL.com/Translator](http://www.DeepL.com/Translator) (kostenlose Version) \*\*\*