HSPA+-Router Toni



Basis FW-Stand: NW_00.02.21

© by PI 2013 - 2017

Inhal	t
-------	---

1 Beschreibung:	4
2 Sicherheitsvorschriften:	4
3 Betriebs-/ Einsatzarten:	5
4 Installation:	5
4.1 SIM-Karte einbauen:	6
4.2 Antennen anschrauben	7
4.3 Gerät das erste Mal verbinden	7
4.4 W-LAN Verbindung	8
4.5 Der erste Start	
4.6 Einrichtungs-Assistent	13
5 Stromoptionen	
6 MVC300 Kamera	
7 Internet-Plattform	
7.1 Status	
7.1.1 System Informationen	
7.1.2 Network Information.	
7.1.3 Routes.	
7 1 4 Realtime Graphs	28
7 2 Network	33
7 2 1 3G	33
7 2 2 WAN	34
7 2 3 I AN	
7 2 4 Wireless	43
7.2.5 Wie stelle ich einen Backunlink ein?	
7.2.6 Firewall	
7 2 7 Static Routes	50
7.2.8 Diagnostics	51
7 3 Services	52
7.3.1 PING Reboot	
7 3 2 SMS Reboot	53
7 3 3 Status via SMS	53
7.3.4 NTP	
7.3.5 Dynamic DNS	
7.3.6 Wireless hotspot	
7.3.7 OpenVPN	
7 3 8 IPsec	
7.3.0 GRE Tunnel	
7 / Systems	
7.4 1 Administration	
7.4.2 Backup und Firmware	
7.4.2 Dackup und Finnware	
7.5 Logout	
9 Open VDN	
9 1 Installation	07
8.1.1 Download	0/ ∠7
0.1.1 Dowilloau	0/
0.1.2 Flogrammin mistameren	0/ 20
0.2 Letuiikate eistellell.	08
0.2.1 Fasswoll setZell	
0.2.2 Server Zerunkat erstellen	
8.2.3 Gerate Zertifikat erstellen	

	8.3 TONI als OpenVPN "TL's" Server	.70
	8.4 TONI als OpenVPN "TL's" Gerät	.72
	8.5 Computer als OpenVPN "TL's" Server	.74
	8.5 Computer als OpenVPN "TL's" Gerät	.76
	8.5 Computer als "Static Key" Gerät	.77
	8.6 TONI als OpenVPN "Static Key" Server	.78
9 7	Sechnische Daten:	.80

Legal notice

Copyright © 2012 TELTONIKA Ltd. All rights reserved. Reproduction, transfer, distribution or storage of part or all of the contents in this document in any form without the prior written permission of TELTONIKA Ltd is prohibited. The manufacturer reserves the right to modify the product and manual for the purpose of technical improvement without prior notice. Other product and company names mentioned herein may be trademarks or trade names of their respective owners

<u>1 Beschreibung:</u>

TONI ist ein kompakter Highspeed W-LAN-, 3G- und Ethernetrouter.

2 Sicherheitsvorschriften:



Bevor Sie das Gerät benutzen, lesen Sie bitte das Handbuch.



Das Gerät nicht gewaltsam öffnen. Bei zerstörtem Gehäuse das Gerät nicht mehr anfassen!



Alle Geräte, die drahtlose Funkverbindungen aufbauen, können Störungen hervorrufen.



Das Gerät ist nicht wasserfest! Halten Sie es trocken.



Gerät arbeitet bei niedriger Spannung - Netzteil +24V DC .

<u>3 Betriebs-/ Einsatzarten:</u>

© by PI 2013 - 2017



<u>4 Installation:</u>

Nachdem Sie den TONI ausgepackt haben, muss er aufgebaut und mit dem Computer verbunden werden. Für besseren W-LAN Empfang bringen Sie TONI so an, dass er möglichst wenig von Türen und Wänden behindert wird.

4.1 SIM-Karte einbauen:

Schrauben Sie TONI hinten auf und setzen Sie dort die SIM-Karte ein.



4.2 Antennen anschrauben

	 2 3 	3	
•	Se ware Name		

Schrauben Sie die W-LAN- und 3G-Antennen in die dafür vorgesehenen Schrauben.

1	GSM Main-Antennenkontakt
2	W-LAN-Antennenkontakt
3	GSM AUX-Antennenkontakt (Alternativ-Modell)
4	Reset Schalter
5	GSM LED

4.3 Gerät das erste Mal verbinden



4.4 W-LAN Verbindung

Um sich mit einer W-LAN-Verbindung einzuloggen, gehen Sie wie folgt vor: (XP Benutzer können zu Schritt 4.4.6 springen!)

Drücken Sie den Start Button.



Im Start Fenster geben Sie nun "network connection" ein.



Da Sie eine neue Verbindung aufbauen möchten, klicken Sie nun auf "View network connections".



Nun rechtsklicken Sie auf "Wireless Network Connection" und dann auf "Eigenschaften".

Organize Disable this netwo	rk device Diagnose this connection
Wireless Network Connect Disabled	tion
atto inter(k) PKO/Wireless 59	Enable Status Diagnose
	Create Shortcut Delete Rename
	Properties

Hier legen Sie nun Netzwerkeinstellungen im "Internet Protokoll Version 4(TCP/IPv4)" fest.

Connect using:		
🔮 Intel(R) PR07	Wireless 3945ABG Netv	vork Connection
		Configure
This c <u>o</u> nnection use	s the following items:	
🗹 📑 Client for M	icrosoft Networks	
🗹 县 QoS Packe	et Scheduler	
🗹 📑 File and Pri	nter Sharing for Microsof	t Networks
🗹 📥 GCT WiMa	x Protocol Driver	
📋 📥 Internet Pro	otocol Version 6 (TCP/IP	v6)
Internet Pro	tocol Version 4 [TUP/IP	V4) HO Driver
Link-Layer	i opology Discovery Map Topology Discovery Res	per 170 Driver ponder
		ponder
I <u>n</u> stall] [<u>U</u> ninstall]	P <u>r</u> operties
Description	7018° (*	474 0.0498
Transmission Con wide area networl	trol Protocol/Internet Pro < protocol that provides	otocol. The default communication
	erconnected networks.	
across diverse int		

Bei den Werkseinstellungen des TONIs ist der DHCP Server eingeschaltet. Sodass dem PC eine IP-Adresse zugewiesen wird. Daher muss die Einstellung so aussehen:

Internet Protocol Version 4 (TCP/IPv4)	Properties
General Alternate Configuration	
You can get IP settings assigned auton this capability. Otherwise, you need to for the appropriate IP settings.	matically if your network supports o ask your network administrator
Obtain an IP address automatical	ly
O Use the following IP address:	
IP address:	
S <u>u</u> bnet mask:	
Default gateway:	
Obtain DNS server address auton	natically
O Use the following DNS server add	Iresses:
Preferred DNS server:	
<u>A</u> lternate DNS server:	
Valjdate settings upon exit	Ad <u>v</u> anced
	OK Cancel

Sie müssen nur auf manuelle Adresse umstellen, wenn Sie den Router so einstellen, dass der DHCP Server aus ist und er somit Ihrem Computer keine IP mehr zuweist.

Die IP Adresse kann in der Form 192.168.1.XXX eingetragen werden.

XXX steht hierbei für die Zahl des Computers.

Beispiele dafür sind: 192.168.1.2, 192.168.1.254, 192.168.1.15.

Als nächstes tragen Sie nun die "Subnetzmaske" ein. Diese ist in Ihrem Gerät hinterlegt und lautet 255.255.255.0. Wenn Sie diese jedoch umstellen, kann diese auch 255.255.0.0 oder 255.0.0.0 lauten. Der "Default Gateway" Lautet 192.168.1.1.

Zum Schluss geben Sie die bevorzugte DNS-Server-Adresse (**192.168.1.1**) und die Alternative DNS-Server-Adresse (**8.8.8.8**) an. Die DNS-Server-Adresse kann auch eine Adresse aus dem Internet sein wie sie Google anbietet (8.8.8.8).

Internet Protocol Version 4 (TCP/IPv4)	Properties 💦 🔀					
General						
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.						
Obtain an IP address automatical	Obtain an IP address automatically					
• Use the following IP address:						
IP address:	192.168.1.100					
S <u>u</u> bnet mask:	255 . 255 . 255 . 0					
Default gateway:	192.168.1.1					
Obtain DNS server address auton	natically					
• Use the following DNS server add	resses:					
Preferred DNS server:	192.168.1.1					
<u>A</u> lternate DNS server:	8 . 8 . 8 . 8					
🔲 Vaļidate settings upon exit	Ad <u>v</u> anced					
	OK Cancel					

Um nun die Verbindung aufzubauen, klicken Sie wieder mit einem Rechtsklick auf "**Wireless** Network Connection" und dann auf: "Verbinden/Trennen"



4.5 Der erste Start

Um das erste Mal auf die Weboberfläche zu gelangen, öffnen Sie Ihren Webbrowser und geben die IP-Adresse des TONIs (Default-IP: 192.168.1.1) ein.



Geben Sie den Default-Benutzernamen (admin) und das Default-Passwort (admin01) ein. Anschließend klicken Sie auf "Login".

Authorization Required				
Please enter your username and password.				
Username	admin			
Password	•••••			
Login Reset				

4.6 Einrichtungs-Assistent

Nach dem ersten Login startet automatisch ein Einrichtungs-Assistent. Dieser kann über "Skip Wizard" beendet werden. Wenn Sie ihn jedoch nutzen möchten, fordert Sie der Assistent auf, zuerst ein neues Passwort einzutragen und dieses zu bestätigen. Um zum nächsten Schritt zu gelangen, drücken Sie auf "Next"

Step 1 - Password	Step 2 - 3G	Step 3 - LAN	Step 4 - WiFi				
Step - Password							
First, let's change your router password from the default one.							
Pa	ssword ••••••	•	2 12				
Confi	rmation		2				
			Skip Wizard Ne	×t			

Im nächsten Schritt geben Sie bitte ihre 3G Einstellungen ein. Diese finden Sie in den Unterlagen ihres Netzanbieters. Wenn Sie damit fertig sind oder diesen Schritt überspringen möchten, klicken Sie auf "Next".

Step 1 - Password	Step 2	2 - 3G	Step 3 - LAN	Step	4 - WiFi
3G Configuration	ı				
Next, let's configure your 30	G setti	ings so you	u can start using	internet	right away.
3G Configuration					
A	APN [
PIN nun	nber 🛛				
Dialing nun	nber 💈	*99#			
3G authentication met	thod 🛛	none		*	
Service m	node 🛛	3G preferre	ed	*	
					_
					Next

In Schritt 3 wird die LAN Konfiguration eingestellt. Hier kann auch der DHCP Server ausgeschaltet werden.

Step 1 - Password	Step 2 - 3G	Step 3 - LAN	Step 4 - WiFi		
Step - LAN					
Here we will configure the	basic settings o	of a typical LAN cont	figuration. The wiza	rd will cover 2 basic configurations: static IP address LAN and DHCP client.	
Common Configura	tion				
Pro	otocol Static a	ddress	~		
IPv4 ad	dress 192.168.	1.1			
IPv4 net	mask 255.255	.255.0	~		
IPv4 broa	dcast				
Use custom DNS si	ervers		*		
DHCP Server					
Di	isable 📃				
	Start 100				
	Limit 150				
Leas	etime 12h				
	😰 Expire	y time of leased add	resses, minimum i	s 2 Minutes (2m).	
				_	
				Next	

Im letzen Schritt wird das W-LAN eingestellt.

Step 1 - Password	Step 2 - 3G	Step 3 - LAN	Step 4 - WiFi				
Step - Wireless	Step - Wireless						
Now let's configure your v connection will be droppe	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 parametes.)						
Device Configuratio	on						
Wireless network is er	nabled Disable						
	😰 Impor	tant note: Do not d	isable if the only wa	y to reach the router is your wireless network.			
Cł	nannel 11 (2.46	2 GHz)	~				
	Mode 802.11g		~				
Country	Code 00 - Wo	rld	~				
Interface Configura	tion						
E							
Hide E	ESSID 📃						
Encr	yption No Encr	ryption	~				
				Finish			

Wenn Sie auf "Finish" klicken wird der Assistent beendet und speichert die Einstellungen. Wenn alles gespeichert ist, wird der Status angezeigt. Ab jetzt können Sie alle Einstellungen ändern.

System information					
System					
Router Name	TONI				
Router Model	Teltonika RUT500				
Firmware Version	RUT5XX_R_01.00.811				
Kernel Version	3.2.15				
Local Time	Mon Apr 8 16:49:30 2013				
Uptime	4h 6m 49s				
Load Average	0.15, 0.25, 0.29				
Memory					
Total Available	13296 kB / 29944 kB (44%)				
Free	2692 kB / 29944 kB (8%)				
Cached	768 <mark>8 kB / 29944 kB (25%)</mark>				
Buffered	2916 kB / 29944 kB (9%)				

Operationsmodi

Der Router TONI hat mehrere Operationsmodi. Er kann sich mit dem Internet (WAN) via 3G, Ethernetkabel oder W-LAN verbinden. Als Backupoption können Sie eine andere verfügbare Verbindung verwenden. Wenn jedoch eine Internet Verbindung via Ethernet Kabel genutzt wird, kann keine W-LAN-Verbindung als Backup verwendet werden.

WAN	LAN		3G Backup Link
	Ethernet	Wi-Fi	
3G			Х
Ethernet	\checkmark		
Wi-Fi	\checkmark	х	\checkmark

5 Stromoptionen

Der TONI-Router kann sowohl über den Stromanschluss (1) als auch über die Ethernet Ports betrieben werden. (Nur neue Hardware Version*) Je nach Netzwerkarchitektur kann LAN3 (2) oder WAN (3) für die Stromversorgung ihres Gerätes benutzt werden.



Benutzen Sie nur eine der Möglichkeiten.

Benutzen Sie nicht den Stromanschluss und einen Ethernetanschluss gleichzeitig zur Stromversorgung!

Benutzen Sie nicht die Anschlüsse LAN3 und WAN gleichzeitig zur Stromversorgung! Die Pinbelegung für die Ethernet Ports lautet:

<u>Pin</u>	Belegung	
1		
2		
3		
4		
5	Positive Spannung +	
6		
7	Negative Spannung (Erde) -	
8	Negative Spannung (Erde) -	



Obwohl nur Pin 5 für die positive Stromversorgung genutzt wird, kann kein Netzteil benutzt werden, das Pin 4 und 5 zu Stromversorgung benutzt.

Wenn der TONI Router über die Anschlüsse LAN3 oder WAN mit Strom versorgt werden soll, müssen Sie die Jumper mit den Pins J4.1, J4.2 Bzw. J3.1, J3.2 (Siehe Bild) entfernen. Vorsicht! Es ist ein Risiko für das Gerät, wenn die Jumper nicht richtig eingestellt sind! Um die Jumper zu verändern, nehmen sie das Frontpanel (Dieses befindet sich auf der Seite, auf der auch der Stromanschluss ist).



6 MVC300 Kamera

Alle Ethernet Ports haben eine Option, um eine MVC300 Kamera anzuschließen. Die Kamera benutzt Pin 4 und 5 des Ethernet Ports (4 ist der Negative Anschluss, 5 ist die Positive Spannung). Bevor Sie eine MVC300 Kammer anschließen, entfernen Sie das Front- und Backpanel. Anschließend entfernen Sie die Platine aus dem Gehäuse und stellen Sie die Jumper neu ein. (Bei neuen Geräten sind keine Jumper gesetzt)

LAN Port 1- bitte den Jumper auf J1 setzen.



LAN Port 2 - bitte den Jumper auf J2 setzen.



LAN Port 3 - bitte die Jumper auf J3.1 und J3.2 setzen.





WAN Port 4 - bitte die Jumper auf J4.1 und J4.2 setzen.

Wenn Sie an allen 4 Ports Kameras anschließen wollen, müssen die 6 Jumper gesetzt werden: J1, J2, J3.1, J3.2, J4.1, J4.2





Wenn die Jumper gesetzt sind, dürfen keine andere Geräte, zum Beispiel Computer, angeschlossen werden. Nur die Kamera darf an einem Anschluss mit gesetztem Jumper angeschlossen werden! Sonst besteht das Risiko eines Defektes!

7 Internet-Plattform

Der Router verfügt über eine Internetplattform, um Einstellungen vorzunehmen.

7.1 Status

Im Status werden alle Informationen über das Gerät angezeigt.

7.1.1 System Informationen

In "System Information" werden alle wichtigen Daten über das Betriebssystem des Routers angezeigt.

System information

System				
Router Name	TONI			
Router Model	Teltonika RUT500			
Firmware Version	RUT5XX_R_01.00.811			
Kernel Version	3.2.15			
Local Time	Mon Apr 8 16:49:30 2013			
Uptime	4h 6m 49s			
Load Average	0.15, 0.25, 0.29			
Memory				
Total Available	13296 kB / 29944 kB (44%)			
Free	2692 kB / 29944 kB (8%)			
Cached	768 <mark>8 kB / 29944 kB (25%)</mark>			
Buffered	2916 kB / 29944 kB (9%)			

System:

	Feld Name	Beispieldaten	Erklärung
1	Router Name	TONI	Name des Router (Hostname des Routersystems)
2	Router Model	Teltonika RUT500	Router-Modell
3	Firmware	RUT5XX_T_00.00.436	Die Firmwareversion, die in den Router geladen ist.
	Version		Es können neue Versionen von Ihnen aufgespielt
			werden wodurch sie mehr Extras und einen größeren
			Komfort erhalten.
4	Kernel	3.2.15	Die Linux Kernel Version, die auf dem Router
	Version		installiert ist
5	Local Time	Fri Jun 29 16:38:48 2012	Die Systemzeit des Routers. Diese wird aus einem
			lokalen Computer oder FTP-Server gelesen
6	Uptime	4h 29m 3s	Die Zeit, seit dem der Router in Funktion ist. Sie
			wird mit einem Reset oder Ausschalten des Routers
			wieder auf 0 gesetzt.
7	Load Average	0.98, 0.57, 0.30	Zeigt die durchschnittliche Auslastung der letzten
			Minute, 10 Minuten und 14 Minuten in Prozent

Memory:

	Feld Name	Beispiel Daten	Erklärung	
1	Total Available	14416/29964	Speicher für die Funktionalität des Routers	
2	Free	1476/29964	Zeigt den gesamten freien Speicher. Wenn dieser	
			schnell gegen 0 geht oder nahe 0 ist, steht ein	
			Absturz oder Neustart des Routers bevor.	
3	Cached	9868/29964	Reservierter Speicher für Zugangsdaten.	
4	Buffered	3072/29964	Speicher für temporäre Dateien, bevor diese an	
			einen anderen Punkt gehen.	

7.1.2 Network Information

Hier finden sie Informationen zum aktuellen Netzwerk, Leistung und Adressen.

30	3G:				
	3G 📶				
	State	connected			
	IMEI	354043050050436			
	Sim card state	OK			
	Signal strength	-105 dBm			
	Operator	Bite			
	Connection type	3G (HSDPA)			
	Bytes recieved	12564			
	Bytes sent	12034			

	Feldname	Erklärung
1	State	Zeigt den Status der Verbindung
2	IMEI	Zeigt die 3G Modem Nummer
3	SIM card State	Zeigt, ob eine SIM-Karte eingelegt ist oder nicht.
4 Signal Stregth Zeigt die Signalstärke		Zeigt die Signalstärke
5	5 Operator Zeigt den verbundenen Mobilfunkanbieter	
6	6 Connection type Der Typ, mit dem eine Verbindung aufgebaut wird	
7	Bytes recieved Wie viele Bytes empfangen wurden	
8	Bytes sent	Wie viele Bytes gesendet wurden

WAN:

WAN			
Interface	3G-ppp		
Туре	Зg		
IPv4 address	10.12.18.71		
Netmask	255.255.255.255		
Gateway	10.12.18.71		
DNS 1	213.226.131.131		
DNS 2	193.219.88.36		
Connected	0h 40m 32s		

	Feld Name	Beispiel Daten	Erklärung
1	Interface	3G	Zeigt, wie der Router mit dem Internet
			verbunden ist. Über Ethernet, 3G oder W-
			LAN
2	Туре	DHCP	Typ der Verbindung. DHCP oder PPPoE
3	IPv4 address	10.12.104.103	Die IP-Adresse, mit der der Router zum
			Internet verbunden ist.
4	Netmask	255.255.255.240	Zeigt die Netzwerkmaske
5	Gateway	10.12.104.97	Zeigt die Standardadresse, mit der der
	-		Router die Verbindung aufbaut.
			_
6	DNS #	8.8.8.8	Domain Name des Servers
7	Expires	1h 57m 25s	Zeigt die Zeit, bis die DHCP Lease abläuft.
8	Connected	0h 2m 2s	Zeigt, wie lange der Router schon mit dem
			Internet verbunden ist.

Lan:

LAN	
IPv4 address	192.168.1.161
Netmask	255.255.255.0
Connected	0h 6m 14s

	Feld Name	Beispiel Daten	Erklärung
1	IPv4 address	192.168.1.161	IP Adresse die vom Router im Netzwerk
			benutzt wird
2	Netmask	255.255.255.0	Netzwerk-Maske
3	Connected	0h 6m 14s	Zeigt, wie lange sich der Router im
			Netzwerk aufhält

Wireless:

Es gibt zwei W-LAN Modi, AP oder Client. Um AP handelt es ich dann wenn der Router ein Access Point Entstehen lässt mit dem sich andere Geräte verbinden lassen. Um einen Client handelt es sich, wenn der Router mit einen anderen Access Point Kontakt aufnimmt.

Wireless	
SSID	TONI
Mode	Master
Channel	11 (2.46 GHz)
BSSID	00:1E:42:12:52:92
Encryption	None
Bit rate	0.0 MBit/s
Country	00

	Feld Name	Beispiel Daten	Erklärung
1	SSID	teltonika_rnd_division_ap	Der Name, unter dem der Router zu finden
			ist bzw. das Netwerk, in dem er sich
			befindet.
2	Mode	Client	Kontaktmodus. Client oder AP (Access
			Point = Master).
3	Channel	6 (2.44 GHz)	Der Kanal, in dem sich der Router befindet.
4	BSSID	C8:3A:53:02:FC:B0	Die Mac Adresse des W-LAN
5	Encryption	WPA2 PSK (CCMP)	Der Verschlüsselungstyp
6	Bit rate	65.0 MBit/s	Die physikalisch höchstmögliche Bitrate
7	Country	LT	Ländercode

Associated Stations:

Liste aller angeschlossenen Geräte und deren Mac Adresse. Diese Anzeige steht nur zur Verfügung, wenn Sie den DHCP Server aktiviert haben und der Router Accesspoint benutzt wird.

Associated Stations				
MAC-Address	Network	Signal	RX Rate	TX Rate
BC:76:70:FE:AC:45	Master "Teltonika_demo_ap"	-48 dBm	72.2 Mbit/s, MCS 7, 20MHz	43.3 Mbit/s, MCS 4, 20MHz
00:37:6D:C5:37:44	Master "Teltonika_demo_ap"	-70 dBm	52.0 Mbit/s, MCS 5, 20MHz	6.5 Mbit/s, MCS 0, 20MHz
© by PI 2013 - 2	2017			Seite 26

DHCP Leases:

Wenn Sie den DHCP Server aktiviert haben, werden hier Geräte angezeigt, die eine Ip-Adresse zugewiesen bekommen haben.

DHCP Leases			
Hostname	IPv4-Address	MAC-Address	Leasetime remaining
android_68594c78df714b08	192.168.1.101	bc:76:70:fe:ac:45	11h 59m 40s

Backup WAN:

Wenn Sie diese Funktion aktiviert haben, kann Ihnen der Status folgendes anzeigen:

IN USE	Die Verbindung ist bereit für "Main traffic".
READY	Die Verbindung ist aufgebaut und wird benutzt.
NOT READY	Die Verbindung ist nicht aufgebaut

Backup WAN Status			
	WAN: [Wired] IN USE	Backup WAN: [36] READY	
Backup WAN Status			
	MAN: [Wired] NOT READ)	Backup WAN: [36] IN USE	

7.1.3 Routes

Routes					
The following rules are currently active on this system.					
ARP					
IPv4-Address		MAC-Address		Interface	
192.168.0.30		70:71:bc:0c:f9:f5		br-lan	
192.168.99.254		00:00:00:00:00:00		eth0.2	
Active IPv4-Routes					
Network	Target		IPv4-Gateway		Metric
wan	0.0.0/0		192.168.99.254		0
lan	192.168.0.0/24		0.0.0.0		0
wan	192.168.99.0/24		0.0.0.0		0
Teltonika solutions: www.teltoni	ka.lt				

ARP

Diese Liste zeigt die Macadresse aller Geräte die jemals an den Router angeschlossen waren.

Active IPv4-Routes

Zeigt die Routing Tabelle an in der die TCP/IP Pakete vermerkt werden.

7.1.4 Realtime Graphs

Echtzeit Grafiken zeigen Statistiken.

Load:



Die Grafik Zeigt 3 Minuten an, aktualisiert alle 3 Sekunden neu und ist durch 3 Farben codiert.

1 Minute Load	Rot
5 Minute Load	Orange
15 Minute Load	Gelb

Traffic, Bridge:

Realtime Traffic		
Bridge LAN+WAN LAN WAN (Wired)	3G WiFi	
3m	2m	lm
90.93 KBit/s (11.37 KByte/s) 60.62 KBit/s (7.58 KByte/s)		
30.31 KBit/s (3.79 KByte/s)		
Inbound: 5.61 KBit/s (0.7 KByte/s)	Average: 4.72 KBit/s (0.59 KByte/s	Peak: 33.34 KBit/s /s) (4.17 KByte/s)
Outbound: 0.94 KBit/s (0.12 KByte/s)	Average: 8.11 KBit/s (1.01 KByte/s	Peak: 110.22 KBit/s /s) (13.78 KByte/s)

Kommunikations-Grafik von Ethernet LAN und W-LAN

Traffic, LAN+WAN:

Realtime Traffic		
Bridge LAN+WAN LAN WAN (Wired)	3G WiFi	
	-	
3m	2m	1m
91.54 KBit/s (11.44 KByte/s)		
61.02 KBit/s (7.63 KByte/s)		
30.51 KBit/s (3.81 KByte/s)		
		MARANA WANNAMANA MARANA
		(3 minute window, 3 second interval)
	August 0.50 (/D)//-	D = -1 = -20 E7 1/01/4
(1.3 KByte/s)	Average: 0.59 KBit/s (1.07 KByte/s)	(4.57 KBit/s) (4.57 KByte/s)
Outbound: 27.01 KBit/s	Average: 43.28 KBit/s	Peak: 110.95 KBit/s
(3.38 KByte/s)	(5.41 KByte/s)	(13.87 KByte/s)

Diese Grafik zeigt alles, was über WAN und LAN geht.

Traffic, LAN:

Realtime Traffic					
Bridge LAN+WAN	LAN WAN (Wired)	3G WiFi			
3m		2m		1m	
90.49 KBit/s (11.31 KByte.	's)				
60.33 KBit/s (7.54 KByte/s)				
30.16 KBit/s (3.77 KByte/s)				
				mphantal	
				(3 minu	te window, 3 second interval)
Inbound:	6.87 KBit/s (0.86 KByte/s)	Average:	5.43 KBit/s (0.68 KByte/s)	Peak:	11.7 KBit/s (1.46 KByte/s)
Outbound:	0.94 KBit/s (0.12 KByte/s)	Average:	15.33 KBit/s (1.92 KByte/s)	Peak:	109.69 KBit/s (13.71 KByte/s)

Grafik zeigt Traffic von LAN Verbindung.

Traffic, WAN:

Realtim	e Traffic															
Bridge	LAN+WAN	LAN	WAN (Wired)	3G	WiFi											
2				2			1									
Sm				⊿m				m	 		п					
0.27 KBit	/s (0.03 KByte/s)															
0.18 KBit	/s (0.02 KByte/s)															
0.09 KBit	/s (0.01 KByte/s)															
										(3 min	ute w	indo	v,3s	econo	d inter	val)
	Inbound:	0 KBit/s (0 KByte/s)			Average:	0 KBit/s (0 KByte/s)				Peak	: 01 (0	KBit/: KByt	s :e/s)			
	Outbound:	0.33 KBit/s (0.04 KByte	e/s)		Average:	0.26 KBit/s (0.03 KByte/s)				Peak	: 0.3 (0.	33 KB 04 K	Bit/s Byte/	/s)		

Grafik ist nur bei aktiver Verbindung sichtbar und zeigt die Datenmengen an.

Traffic,	W-I	LAN
----------	-----	-----



Diese Grafik zeigt den Traffic über W-LAN an

Wireless, WiFi:

Realtime Wireless		
3m	2m	im
-82 dBm		V.
-141 dBm		
-200 dBm		
		(3 minute window, 3 second interval)
Signal: -49 dBm (SNR 206 dBm)	Average: -48 dBm (SNR 206 dBr	n) Peak: -45 dBm (SNR 210 dBm)
Noise: -255 dBm	Average: -255 dBm	Peak: -255 dBm

Die Grafik zeigt an, wie stark das Signal ist.



Die Grafik zeigt die Datenmenge, die geschickt und empfangen wird.

Connections:



Das Blaue in der Grafik stellt die UDP-Verbindungen dar. Grün die TCP-Verbindungen. Andere Typen (ICMP, etc.) werden rot dargestellt.

Network	Protocol	Source	Destination	Transfer
IPV4	TCP	192.168.0.156:37706	192.168.99.30:3389	613.24 KB (8338 Pkts.)
IPV4	UDP	192.168.0.19:137	192.168.0.255:137	7.24 KB (84 Pkts.)
IPV4	UDP	192.168.0.19:138	192.168.0.255:138	5.20 KB (24 Pkts.)
IPV4	TCP	192.168.0.156:52547	173.194.78.139:80	3.30 KB (11 Pkts.)
IPV4	TCP	192.168.0.156:38821	199.127.194.80:80	1.97 KB (17 Pkts.)
IPV4	UDP	192.168.1.9:67	255.255.255.255:68	1.13 KB (2 Pkts.)
IPV4	TCP	192.168.0.156:42797	209.85.148.148:80	930.00 B (5 Pkts.)
IPV4	TCP	192.168.0.30:55669	192.168.0.161:80	703.00 B (3 Pkts.)
IPV4	UDP	0.0.0.0:68	255.255.255.255:67	688.00 B (2 Pkts.)
IPV4	UDP	192.168.0.5:67	255.255.255.255:68	604.00 B (2 Pkts.)
IPV4	UDP	192.168.0.156:54245	8.8.8.8:53	142.00 B (2 Pkts.)
IPV4	UDP	192.168.0.156:41391	8.8.8.8:53	66.00 B (1 Pkts.)

Auf der selben Seite können Sie analysieren, welche Verbindungen der Router aufbaut. Es werden IPv4 Adressen angezeigt sowie die übermittelte Paketgröße.

7.2 Network

<u>7.2.1 3G</u>

Hier können Sie Einstellungen an ihrer 3G Verbindung einstellen.

3G Configuration					
Here you can configure yo	our 3G settings.				
3G Configuration					
APN	bangapro				
PIN number	5555				
3G authentication method	СНАР				
Username	user				
Password	•••••	P			
Prefered network	UMTS				
		Save			

Alternativmodell:

3G Configuration				
Here you can configure your 3G	settings.			
3G Configuration				
APN				
PIN number				
Username				
Password	Ø			
Prefered network	auto			

Die Konfiguration ist simpel:

	Feld Name	Beispiel Daten	Erklärung
1	APN	"bangapro"	Access Point Name des Mobilfunkanbieters
2	PIN Number	"5555"	Ihr persönlicher Pin der SIM-Karte
3	3G authentication	CHAP, PAP oder none	Aufenthalts Autorisierungs-Methode (Diese
	method		Option ist beim Alternativmodell nicht
			vorhanden.)
4	Username	"User"	Passwort und Benutzername erhalten Sie von
5	Password	"passwd"	ihrem Mobilfunkanbieter. Wenn Sie diese
			nicht haben, stellen Sie "3G authentication
			method" auf "none"
6	Preferred network	GSM, UMTS oder auto.	Die Modi, mit der das 3G Modem sich
		Alternativ Modell:	einloggen soll.
		2G. 3G oder none.	



Vorsicht! Achten Sie darauf, dass der Pin der Richtige ist! Die SIM-Karte wird sonst gesperrt und kann unter Umständen nicht mehr freigeschaltet werden.

<u>7.2.2 WAN</u>

In der WAN Konfiguration legen Sie fest, wie der Router mit dem Internet verbindet.

Operation Mode:

Operation Mode						
Interface	۲	🕼 3G				
	\bigcirc	😥 Wifi				
	\bigcirc	🛒 Wired				

	Typ der Verbindung	Beschreibung der Verbindung
1	3G	Der Router verbindet sich mit einer SIM-Karte ins 3G-Netz
2	WiFi	Der Router verbindet via. W-LAN an einen anderen Access Point und
		bezieht von dort aus Internet
3	Wired	Ein WAN-Kabel am Ethernet Anschluss sorgt für Internet.

Bitte beachten:

Bei einer Verbindung ins Internet über das 3G-Netz kann im Gerät keine MTU-size geändert werden. Diese steht fest auf 1500.

Normalkonfiguration: Konfigurieren Sie ihre TCP/IP-Einstellungen.

Common Configuration					
General Setup					
Protoc Really swite protocc	col DHCP client ch Switch protocol pl?				

Sie können zwischen Static, DHCP und PPPoE Protokoll wählen.

Static Address:

Common Configuration						
General Setup	Advanced Settings					
Protocol	Static address	•				
IPv4 address	192.168.99.162					
IPv4 netmask	255.255.255.0	-				
IPv4 gateway	192.168.99.254					
IPv4 broadcast						
Use custom DNS	8.8.8.8	×				
servers	8.8.6.6	2				

	Feld Name	Beispiel Daten	Beschreibung
1	IPv4 address	192.168.99.162	Ihre Router-Adresse ins WAN Netzwerk
2	IPv4 netmask	255.255.255.0	Ihre Netzmaske im WAN Netzwerk
3	IPv4 gateway	192.168.99.254	Adresse, die der Router sendet, wenn Traffic gesendet wird.
4	IPv4 broadcast	192.168.99.255	Broadcastadresse (automatisch generiert, nicht einstellbar).
			Feld bitte frei lassen!
5	Use custom	8.8.8.8 8.8.6.6	Die Adresse, über die der Router von außen erreichbar sein
	DNS Servers		soll. Es kann eine alternative DNS Adresse eingegeben
			werden, falls von der ersten DNS Adresse die Hoster nicht
			erreichbar sind.

DHCP:

Common configuration							
General Setup	Advanced Settings						
	Protocol	DHCP	×				
Hostname to reques	send when sting DHCP	TONI					

Wenn Sie das DHCP Protokoll verändern und kein anderer DHCP Server vorhanden ist, kann es passieren, dass der Router nicht mehr erreichbar ist.

PPPoE für DSL Verbindungen:

Common configuration							
General Setup	Ad	lvanced Settings					
Protocol							
PAP/CHAP username		test					
PAP/CHAP password		•••	ð				
Access Concentrator		auto					
		Leave empty to autodetect					
Service Name		auto					
		😰 Leave empty to autodetect					

	Feld Name	Beispiel Daten	Beschreibung
1	PAP/CHAP	test	Ihr Passwort und Benutzername das Ihnen vom
	username		Internetbetreiber mitgeteilt wurde.
2	PAP/CHAP	your_password	
	password		
3	Access	isp	Spezifischer Name für Accessconcentrator. Lassen
	Concentrator		Sie diese Einstellung auf Auto.
4	Service Name	isp	Name von Service. Lassen sie diese Einstellung auf
		_	Auto
Advanced Settings

Spezielle Einstellungen für alle Protokolle. Dies sollte nur von Profis umgestellt werden.

Static:

Common Config	uration
General Setup	Advanced Settings
Bring up on boo	t 🔽
Disable NAT	Г 🔲 😰 If checked, router will not perform NAT (Masquerade) on this interface
Override MAC address	00:0C:43:30:50:D4
Override MTU	1500
Use gateway metric	. 0

	Feld Name	Beispiel Daten	Beschreibung
1	Bring up on boot	On	Dient dazu, beim Starten des Routers eine
			Verbindung zum Router aufzubauen. Wenn die
			Option deaktiviert ist kann keine WAN Verbindung
			mehr aufgebaut werden.
2	Disable NAT	On/Off	Toggle NAT an und aus
3	Override MAC	00:0C:43:30:50:38	Override MAC address vom WAN interface
	address		Computer.
4	Override MTU	1500	Maximale Übertragungs-Rate des längsten Daten
			Paketes.
5	Use gateway	0	WAN configuration von automatisch generierten
	metric		Routing-Tabellen.

Handbuch HSPA+-Router Toni

DHCP:

Common configuration	
General Setup Advance	d Settings
Disable NAT Use broadcast flag Use default gateway Use DNS servers advertised by	 If checked, router will not perform NAT (Masquerade) on this interface Required for certain ISPs, e.g. Charter with DOCSIS 3 If unchecked, no default route is configured If unchecked, the advertised DNS server addresses are ignored
peer Use gateway metric	0
Client ID to send when requesting DHCP	
Vendor Class to send when requesting DHCP	
Override MAC address	00:1e:42:12:52:91
Override MTU	1500

PPPoE:

Common configuration

General Setup	Advanced Settings
Disable N/	AT 🛛 😰 If checked, router will not perform NAT (Masquerade) on this interface
Use default gatewa	ay 🛛 😰 If unchecked, no default route is configured
Use gateway metr	ic O
Use DNS serve advertised by pe	rs 🛛 😰 If unchecked, the advertised DNS server addresses are ignored er
LCP echo failu	
thresho	ld 🕜 Presume peer to be dead after given amount of LCP echo failures, use 0 to ignore failures
LCP echo interv	al 5
Inactivity timeo	Send LCP echo requests at the given interval in seconds, only effective in conjunction with failure threshold O O O O O O O

IP Aliases

Zum Suchen und Definieren im Internet und im regulären Netzwerk.

IP-Aliases				
SUBNET55				
General Setup	Ad	vanced Settings		
IPv4-Addre	ss	192.168.55.161		
IPv4-Netmask		255.255.255.0	•	
IPv4-Gateway		192.168.55.153		
Delete				
Add				

Sie können die Konfiguration des Status-Protokolls sehen. Im Beispiel ist das Subnetz ,55'. es können nur Geräte mit gleicher Subnetz (55) ins Netzwerk eingebunden werden.

IP-Aliases	
SUBNET55	
General Setup	Advanced Settings
IPv4-Broadca DNS-Sen Delete	er
	Add

Sie können optional eine Broadcast Adresse und DNS Server definieren.

Wie funktioniert ein WiFi WAN Setup?

Als Erstes stellen Sie unter "Network-WAN" den Operation Mode auf WiFi um, dann die Seite neu laden. Als Nächstes stellen Sie ein, ob Sie den DHCP Server benutzen möchten oder eine statische (Static) Adresse benutzen möchten. Wenn Sie Diese Einstellungen gespeichert haben, speichern sie die Einstellungen über "Save" ab. Als Nächstes gehen Sie auf "Network->Wireless" und warten kurz, bis alle Einstellungen fertig geladen sind und Sie diese einstellen können.

Nun sollten Sie ihr W-LAN Netzwerk, mit dem Sie sich verbinden möchten in den Einstellungen sehen. Wählen Sie es aus und geben Sie den Sicherheits-Schlüssel ein. Wenn Sie auf Submit klicken wird versucht, eine Verbindung aufzubauen. Wenn dies funktioniert können Sie weitere Einstellungen einstellen. Wenn Sie damit fertig sind, klicken Sie auf "Save" und können ab diesem Zeitpunkt ins Internet.



Nur mit fester LAN Verbindung umstellen! Gerät ist sonst nicht mehr erreichbar!

<u>7.2.3 LAN</u>

Diese Seite ist zur Konfiguration eines LAN Netzwerkes.

LAN			
On this page you ca	n con	figure your LAN settings.	
Common Confi	gura	tion	
General Setup	Ad	vanced Settings	
Proto	col	Static address	
IPv4 addre	SS	192.168.0.161	
IPv4 netmask		255.255.255.0	
IPv4 gateway			
IPv4 broadcast			
Use custom DNS		[]*	
servers			
IP-Aliases			
This section contains no values yet			
Add			

DHCP Server:

Der DHCP Server ist beim ersten Start so konfiguriert, dass der Router funktioniert. Wenn Sie ein Gerät anschließen, identifiziert es sich automatisch und bekommt die IP-Adresse vom Router zugewiesen. Es ist dann verbunden.

DHCP Server	
General Setup	Advanced Settings
Disabl	e 📃
Sta	rt 100
Lim	it 150
Leasetim	e 12h
	🔞 Expiry time of leased addresses, minimum is 2 Minutes (2m).

	Feldname	Beispieldaten	Beschreibung
1	Disable	Checked/unchecked	DHCP Server Abschalten/Einschalten
2	Start	100	Die Start-Adresse mit der der DHCP anfangen soll, die
			Adressen zu vergeben. Beispiel: Das erste Gerät, das
			angeschlossen wird, bekommt die IP-Adresse
			192.168.1.100, das zweite Gerät die IP-Adresse
			102.168.1.101. Wenn ein Gerät die Verbindung zum Router
			trennt ist diese Adresse wieder frei und kann einem Gerät,
			was sich danach mit dem Router verbindet, zugewiesen
			werden.
3	Limit	150	Diese Zahl gibt an wie viele IP-Adressen zugewiesen
			werden dürfen und damit, wie viele Geräte sich mit dem
			Router verbinden können. Wenn die Start Adresse also
			192.168.1.100 ist und 150 unter dem Feld eingetragen ist,
			ist die letzte Adresse, die vergeben wird 192.168.1.249.
			Danach kann sich kein weiteres Gerät mit dem Router
			verbinden.
4	Lease time	12h	Diese Einstellung ist dafür da, dass IP-Adressen von
			Geräten, die nicht mehr verbunden sind, 12 Stunden für
			diese Geräte gespeichert sind.

Advanced settings:

Hier können spezielle Einstellungen für den DHCP Server getätigt werden.

DHOF Server		
General Setup	Advanced Settings	
Dynamic DHCP		
Force	🔲 🔞 Force DHCP	on this network even if another server is detected.
IPv4 netmask		
DHCP-Options		<u>ت</u>
	Define additiona clients.	DHCP options, for example "6,192.168.2.1,192.168.2.2" which advertises different DNS servers to

	Feld Name	Beispiel Daten	Beschreibung
1	Dynamic DHCP	Checked/Unchecked	Dynamic DHCP aktivieren und deaktivieren.
2	Force	Checked/Unchecked	Forces DHCP ist da, falls sich noch ein anderer DHCP Server im Netzwerk befindet bzw. einer gefunden wird.
3	IPv4 netmask	255.255.255.0	Hier können sie die LAN Netmaske umstellen.
4	DHCP-Options	6,192.168.2.1,192.168.2.2 26,1470 option:mtu, 1470	Hier können noch andere Optionen für Ihren DHCP Server festgelegt werden. Benutzen können Sie zum Beispiel die Option 'option:mtu, 1470' oder '26,1470' festlegen. Ihre Geräte, die sich mit dem Router verbinden wollen, müssen für diese Option MPU-fähig sein.

7.2.4 Wireless

Auf dieser Seite können die W-LAN Einstellungen geändert werden. Auch Einstellung zum WAN über WiFi und Access Points finden Sie hier.

Access Point:

Wireless Ac	cess Point	
Here you can config	ure your wireless setting	gs like radio frequency, mode, encryption etc
Device Configu	ration	
General Setup	Advanced Settings	
Wireless network	is enabled Disable 2 Don't for	orget to save before toggling the wireless radio on and off.
	Channel 11 (2.462 (GHz)
Interface Config	guration	
General Setup	Wireless Security	MAC-Filter
ł	ESSID TONI	
WRP100 config Connection	uration et WRP100 🗹 tomatically	Save

Hier kann man eine Übersicht der W-LAN Einstellungen sehen. Hier können Parameter geändert und auch das gesamte W-LAN Netzwerk abgeschaltet werden.

Device, General:

Device Cor	nfigura	tion			
General Se	tup	Advanced Settings			
Wireless net ¢ C	work is nabled hannel	Disable Don't forget to sa 11 (2.462 GHz)	ave before toggl	ing the wireless rad	io on and off.

Hier kann das W-LAN Netzwerk mit einem Klick auf "Disable" abgeschaltet werden. Der Kanal, auf dem das Netzwerk arbeitet, kann hier auch umgestellt werden.

Device, Advanced:

Device Configurati	on				
General Setup Advanced Settings					
Mode	802.11g+n 💌				
HT mode	20MHz				
Country Code	00 - World				
	😰 Use ISO/IEC 3166 alpha2 country codes.				
Distance					
Optimization	😰 Distance to farthest network member in meters.				
Fragmentation					
Threshold					
RTS/CTS Threshold					

Hier können noch mehr Parameter konfiguriert werden.

	Feld Name	Beispiel Daten	Beschreibung
1	Mode	Auto, b, g, g+n	Sicherheitsoptionen
2	Country Code	Any ISO/IEC 3166 alpha2	Auswählen einer Region (Land)
		country Code	
3	Distance	100	Um einzustellen, mit welcher Stärke das W-
	Optimization		LAN Netzwerk senden soll (in Metern)
4	Frag. Threshold	2346	Das kleinste Paket, das gesendet werden darf.
			Dies hat Auswirkungen auf die
			Geschwindigkeit und kann bei falschen
			Einstellungen zu Problemen führen.
5	RTS/CTS	2346	Diese Einstellung kann helfen, wenn Sie
	Threshold		Probleme mit Accespoints in der Umgebung
			haben.

Interface, General:

Interface Configuration					
General Setup Wireless Security MAC-Filter					
ł	ESSID TONI				

ESSID – ist der W-LAN-Intendifikationsstring.

Interface, Security:

Interface Configuration					
General Setup	Wireless Security		MAC-Filter		
Encrypti Cipł K	ion her íey	WPA2-PSK auto		•	R.

Encryption ist die Verschlüsselung des W-LAN-Netzes. Es gibt mehrere Optionen:

WEB:

Encryption	WEP Open System	•
Used Key Slot	Кеү #1	•
Key #1		8
Key #2		8
Key #3		8
Key #4		8

Geben sie die gewünschten Keys ein.

Achtung:

Die Keys dürfen

in ASCII nur 5 **oder** 13 Zeichen in HEX (Zahlen zwischen 0-9) nur 10 **oder** 26 Zeichen

haben.

WPA:

Key	******	đ
Cipher	auto 💌	
Encryption	WPA-PSK	

Hier zuerst die Methode (Ciper) einstellen: TKIP, CCMP, TKIP&CCMP, Auto. Der Key darf 8 Zeichen lang sein.

Handbuch HSPA+-Router Toni

Interface, Mac-Filter:

Interface Configuration					
General Setup Wireless Security MAC-Filter					
MAC-Address Fil MAC-L	ter .ist	Allow listed only		•	

Im MAC Filter können Sie Mac Adressen eingeben, die sich mit dem Netzwerk verbinden dürfen. Neue Geräte müssen erst eingetragen werden, bevor sie sich verbinden können.

Client:

Ein Client ist ein Gerät, das sich mit einem Accesspoint verbindet und im Regelfall eine IP-Adresse zugewiesen bekommt. Es ist nicht möglich, mit einem Client ein Netzwerk zu eröffnen.

Backup WAN:

Backup WAN ist eine Funktion, falls sie zum Beispiel über W-LAN mit dem Internet verbunden sind und diese Verbindung abbricht, automatisch eine Verbindung über 3G hergestellt werden kann.

Backup Link		
Here you can setup you to keep the router conn	r backup link. If your conventional W acted.	AN connection, such as wired Ethernet or Wifi, fails, the backup link will enable and take over
Enable	V	
Timing & other par	ameters	
Timing & other parame	ters will indicate how and when it wi	II be determined that your conventional connection has gone down.
Health Monitor Interval	5 sec. 💌	
Health Monitor ICMP Host(s)	DNS Server(s)]
Health Monitor ICMP Timeout	1 sec.	
Attempts Before WAN Failover	1]
Attempts Before WAN Recovery	1]
DNS Server(s)	Auto]
Backup ICMP host		
A remote host that will k	e used to test wether your backup I	ink is alive.
ICMP host	8.8.4.4	
		Save

	Feld Name	Auswählbare Daten	Beschreibung
1	Health Monitor	Dsb/5/10/20/30/60/120	Der Intervall, in dem die Verbindung
	Intervall	Sekunden	geprüft wird.
2	Health Monitor	Dsb/DNS/WAN GW/Custom	Wie soll der Router testen, ob er mit dem
	ICMP HOST		Internet verbunden ist.
3	Health Monitor	$\frac{1}{2}/3/4/5/10$ Seconds	Wie lange soll gewartet werden, bis die
	ICMP Timeout		alternative Verbindung (3G) benutzt
			wird.
4	Attempts Before	1/3/5/10/15/20	Wie viele Verbindungsversuche sollen
	WAN Failover		unternommen werden, bis die alternative
			Verbindung (3G) in Kraft tritt.
5	Attempts Before	1/3/5/10/15/20	Wie oft soll kontrolliert werden, ob die
	WAN Recovery		Standardverbindung wieder erreichbar
			ist, bis sie wieder benutzt wird.
6	DNS Servers	Auto/Custom	Eine benutzerdefinierte DNS-
			Serveradresse ergibt Sinn, wenn Sie den
			Health Monitor ICMP HOST wählen.
7	Backup ICMP host	IPv4 address	Hier wird die IP-Adresse des ISMP-Hosts
			eingetragen, mit der über einen
			Pingbefehl überprüft wird, ob die 3G-
			Verbindung funktioniert.

7.2.5 Wie stelle ich einen Backuplink ein?

Zunächst müssen Sie ihre Standard-Verbindung aufbauen. Konfigurieren Sie die Verbindung so, dass Sie ohne Probleme Zugriff auf das Internet haben. Als Nächstes kann der Backuplink eingestellt werden. Gehen Sie zu der Seite "Backup WAN", stellen Sie dort das Backup nach Ihren Wünschen ein. Um zu kontrollieren, ob es funktioniert, gehen Sie auf Status->Network Information-> WAN Backup.

Backup WAN Status		
	WAN: [Wired] IN USE	Backup WAN: [3G] READY

Dieses Bild zeigt den Status der W-LAN Verbindung an (IN USE) und ob dass Backup WAN (3G) in Bereitschaft ist, falls die W-LAN Verbindung zum Internet abbricht (READY)

Wenn die W-LAN Verbindung nun abbricht sieht es so aus:

Backup WAN Status		
	WAN: [Wired] NOT READY	Backup WAN: [36] IN USE
Die W-LAN Verbindung ist unterbrochen (N	JOT READY) und die 3G V	/erbindung ist nun aktiv (IN

Die W-LAN Verbindung ist unterbrochen (NOT READY) und die 3G Verbindung ist nun aktiv (IN USE).

Wenn nun die Verbindung zum W-LAN wieder hergestellt werden kann sieht es so aus:

WAN: [Wired] IN USE Backup WAN: [36] READY

Die W-LAN Verbindung ist wieder aktiv (IN USE) und die 3G Verbindung hält sich bereit (READY)

Backup WAN Status

7.2.6 Firewall

General Settings:

Die Integrierte Firewall im Router ist ein Standardlinuxpaket. Sie kontrolliert eingehende und ausgehende Datenpakete und Verbindungen.

General Settings	
Enable SYN-flood protection	
Drop invalid packets	
Input	accept 💌
Output	accept 🗨
Forward	reject 💌

	Feld Name	Auswählbare Daten	Beschreibung
1	Enable SYN-	Checked/Unchecked	Wenn diese Option aktiviert ist, ist der
	flood		Router besser gegen SYN-flood Attacken
	protection		geschützt.
2	Drop Invalid	Checked/Unchecked	"Drop" sind Dateien, die ins Internet
	packets		geschickt werden.
3	Input	Reject/Drop/Accept	Eingehende Dateien zulassen.
4	Output	Reject/Drop/Accept	Ausgehende Dateien zulassen
5	Forward	Reject/Drop/Accept	Die Standardaktion für die Pakete, die die
			vordere Kette passieren.

In Traffic Rules können sie einzelne Verbindungen zulassen oder unterbinden.

General, DMZ:

DMZ configuration				
Enabled				
DMZ host IP address				

Durch Aktivierung von DMZ für einen bestimmten internen Host (z.B. Ihren Computer), wird dieser dem WAN-Netzwerk des Routers ausgesetzt (z.B. Internet)

Port Forwarding:

Hier können sie neue Ports freigeben und Regeln erstellen.

Firewall - Port Forwarding

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

Name	Protocol	Source	Via	Destination	Enable	Sort
Mustername	TCP, UDP	From <i>any host</i> in war	To <i>any router IP</i> at port 12345	Forward to IP 192.168.1.202, port 80 in	n lan 💌	e Edit Delet
New port f	orward:					
Name		Protocol	External port	Internal IP address Internal por	t	
New port fo	irward	TCP+UDP				Add

Sie können einzelne Geräte in ihrem Netzwerk für spezielle Zugriffe zulassen. (Dafür geben Sie die IP-Adresse des internen Gerätes, den externen und internen Port und das Protokoll an).

	Feld Name	Beispiel Daten	Beschreibung
1	Name	"localWebsite"	Name der Regel
2	Protocol	TCP/UDP/TCP+UDP/Other	Typ des Protokolls des eingehenden Paketes.
3	External Port	1- 65535	Welcher Port wird im WAN Netzwerk benutzt?
4	Internal IP	IPv4 Adresse von einem	Die IP-Adresse des Geräts, dass im Netz der
	address	Gerät aus Ihrem LAN	Firewall eine Freigabe bekommen soll.
5	Internal port	1-65535	Port, der von dem Gerät intern zur Datenübertragung
			genutzt wird.

Der externe Port ist 12345 und nicht 80. Wenn sie 80 als externen Port benutzen, dann ist eine Funktion in der Regel nicht möglich.

Traffic Rules:

In "Traffic rules" können Sie genaue Regeln in verschiedenen Bereichen aufstellen, Ports blocken und freigeben

	Feld Name	Beispiel Daten	Beschreibung
1	Name	"ruleName"	Name der Regel.
2	Family	IPv4	Nur IPv4 Wirt überwacht.
3	Protocol	TCP/UDP/Other	Das Protokoll um das es sich handelt.
4	Source	IPv4 address	Herkunft Adresse.
5	Destination	IPv4 address	Ziel der Daten.
6	Action	Drop/Accept/Reject + chain +	Aktion die die Firewall ausführen soll.
		additional rules	z.B. Verbindung Akzeptieren.
7	Enable	Checked/Unchecked	Regel aktiv/nicht aktiv
8	Sort	Up/Down	Die Regeln in eine andere Reihenfolge
			(roch, runter) bringen.

Custom Rules:

Programme, die auf ihrem Computer installiert sind und eine spezielle Verbindung mit dem Internet aufbauen, müssen hier freigegeben werden. Die genauen Daten, die das Programm braucht (Port, usw.) stehen ihm Handbuch des Programms.

7.2.7 Static Routes

Static Routes bieten die Möglichkeit der Eingabe von benutzerdefinierten Einträgen in den interne Routentabelle des Routers.

	of wor which interface and a	ratoway a cortain boot or notwork o	an ho roachod		
Jules sper	chy over which menace and g	galeway a certain nost of network c	an be reached.		
totio IDu	d Dautaa				
	4 Roules	Dec 6 Martine and a	ID: 1.0-1	Madala	
Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric	
	Host-IP or Network	if target is a network			
lan 💌	192.168.55.0	255.255.255.0	192.168.55.145		Dele

	Feld Name	Beispiel Daten	Beschreibung
1	Interface	Lan/wan	Netwerkverbindung, die freigeben werden soll.
2	Target	IPv4 address	Netzwerk, das freigegeben werden soll.
3	IPv4-Netmask	IPv4 mask	Netzmaske, die vom Gerät benutzt wird.
4	IPv4-Gateway	IPv4 address	IP-Adresse des Geräts, das freigegeben wird.
5	Metric	Integer	Wird zur Sortierung benutzt. Wenn ein Paket zwei Regeln erfüllt, wird die mit der höheren Metrik
			angewandt.

Zusätzliche Anmerkung zu "Target" und "Netmask": Sie können eine Regel für eine Einzel-IP wie folgt definieren:

Netmask – 255.255.255.255. Außerdem kann eine Regel, die auf IP-Segmente angewandt wird, definiert werden: Target – eine IP, die ANFÄNGT im Segment; Netmask – Netzmaske, die die Größe des Segments definiert:

192.168.55.161	255.255.255.255	Nur Verbindung zu 192.168.55.161
192.168.55.0	255.255.255.0	Verbindung zu 192.168.55.0-192.168.55.255
192.168.55.240	255.255.255.240	Verbindung 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

7.2.8 Diagnostics

Nützliches Tool, um Ihr Netzwerk zu testen.

Network Utilities			
Pi	ng	Traceroute	Nslookup

Ping – mit diesem Tool können Sie Verbindungen testen und schauen, ob Geräte im Netzwerk verfügbar sind. Sie geben dazu die IP-Adresse des Gerätes an, das gesucht werden soll und klicken dann auf Ping. Nun werden Daten Pakete an die von Ihnen eingegebene IP-Adresse gesendet, die das Gerät zurück schicken muss. Wenn die Datenpakete wieder beim Router ankommen, ist das Gerät erreichbar.

Tracerroute – ist ein diagnostisches Tool, um die Route-Strecke anzuzeigen und eine Messung der Transitverzögerung zu messen. Geben Sie die Server-IP oder den Host-Namen ein und klicken Sie auf "Traceroute".

Nslookup – ist eine Netzwerk-Kommandozeile. Sie geben den gewünschten Befehl und den Hostnamen oder die IP-Adresse des Gerätes ein, das sie ansprechen möchten. Wenn Sie damit fertig sind und auf Nslookup klicken wird der Befehl ausgeführt. Befehle zu Nslookup finden Sie in einem Linux-Handbuch.

Anmerkung: Bevor Sie ein Gerät ansprechen können muss es richtig konfiguriert sein.

7.3 Services

7.3.1 PING Reboot

PING Reboot ist eine Funktion, die beim Start des Routers und dann in einem bestimmten Intervall (einstellbar) einen Server pingt. Er sendet dazu ein Pingbefehl und wartet auf ein Echo. Wenn der Router kein Echo bekommt und somit der Server nicht erreichbar ist startet der Router erneut.

Normalkonfiguration:

Enable PING Reboot	
Reboot router if no echo received	
Interval between	30
PINGs (min)	Ø Minimum 5 minutes
Retry count	5
Server to PING	127.0.0.1
	e.g. 192.168.1.1 (or www.host.com if DNS server configured correctly)

	Feldname	Beschreibung	Notiz
1	Enable PING Reboot	Checkbox zum Aktivieren	PING Reboot ist bei
		des PIN-Reboot	Werkseinstellungen deaktiviert
2	Reboot router if no	Router, wenn er kein Echo	Diese Checkbox muss unmakiert sein,
	echo received	bekommt, neu starten.	um das Extra "Keep Alive" zu
			verwenden.
3	Interval between	Zeitintervall, bis wieder die	Kürzestes Zeitintervall ist 5 Minuten.
	PINGs	Verbindung geprüft wird.	
4	Retry count	Wie oft soll der Vorgang	Kleinste mögliche Zahl ist 1
		nach dem Intervall wiederholt	
		werden.	
5	Server to PING	Server IP-Adresse oder	Wenn Sie einen Host-Namen
		Hostname, die der Router	verwenden, müssen Sie zunächst den
		pingen soll.	DNS Server einstellen.

Anmerkung:

Testen Sie, bevor sie PING-Reboot einstellen, ob der Server den Befehl PING versteht und er Ihnen ein Echo zurück schickt. Sie können dies unter "Network > Diagnostics" testen.

7.3.2 SMS Reboot

Man kann den Router auch über eine SMS-Text-Message Neustarten. Dies empfiehlt sich vor allem bei Routern, die nicht gut per Hand neu zu starten sind.

Enable SMS Reboot	
SMS text	
Sender phone	
number	😰 e.g. +37012345678
Get status	Get detailed router connection information via SMS message after SMS reboot

	Feldname	Beschreibung	Notiz
1	Enable SMS Reboot	SMS Reboot	Die Funktion ist bei
		aktivieren/deaktivieren	Werkseinstellung deaktiviert.
2	SMS text	SMS-Text bei dem der Router	Der SMS-Text kann aus
		neu starten soll.	Buchstaben, Nummern,
			Leerzeichen und Spezial-
			Symbolen bestehen.
3	Sender phone number	Handy-Nummer der Person, die	Sie können mehre Nummern
	_	den Router via SMS neu starten	freigeben um den Router neu zu
		darf.	starten. Klicken Sie dafür auf den
			Button hinter dem Textfeld.
4	Get status	Aktivieren Sie dies, wenn Sie	Deaktiviert bei
		möchten das der Router Ihnen	Werkseinstellungen.
		eine Status-SMS nach dem	
		Neustart schicken soll.	

7.3.3 Status via SMS

Eine SMS mit dem aktuellen Status des Routers senden.

Enable SMS Status		
SMS text		
Sender phone		Ď
number	😰 e.g. +37012345678	

	Feldname	Beschreibung	Notiz
1	Enable SMS	Funktion aktivieren/deaktivieren.	Ist bei Werkseinstellungen deaktiviert.
	Status		_
2	SMS text	Der Text in einer SMS um einen	Der SMS-Text kann aus Buchstaben,
		Status zu senden.	Nummern, Leerzeichen und Spezial-
			Symbolen bestehen.
3	Sender phone	Handy-Nummer der Person, die den	Sie können mehre Nummern freigeben
	number	Status vom Router via SMS abrufen	um den Router neu zu starten. Klicken
		darf.	Sie dafür auf den Button hinter dem
			Textfeld.

<u>7.3.4 NTP</u>

Systemeinstellungen von TONI

NTP		
Hostname, NTP and timezone c	onfiguration.	
System Properties		
Local Time	Mon Apr 8 16:47:59 2013 Sy	nc with browser
Hostname	TONI	
Timezone	UTC	*
Time Synchronization		
Enable builtin NTP		
NTP server candidates	O.europe.pool.ntp.org	×
	3.europe.pool.ntp.org	*
		_
		Save

"Sync with browser": Synchronisiert die Zeit des Routers mit der des Computers.

	Feld Name	Beschreibung	Notiz
1	Local Time	Lokale Zeit des Routers	
2	Hostname	Hostname des Router	
3	Timezone	Zeit-Zone ihres Landes	
4	Enable builtin NTP	Automatische Zeit Abfrage über	
		NTP Server	
5	NTP server	NTP server hostname.	Sie können mehrere NTP Server
	candidates		Eintragen. Dazu klicken Sie auf den
			Button hinter dem Textfeld.

7.3.5 Dynamic DNS

Dynamic DNS (DDNS) ist eine Möglichkeit, den Router auch über das Internet zu erreichen wenn Sie keine feste IP-Adresse von ihrem Provider zugewiesen bekommen.

ЕМО			
Enable	•		
Status	N/A		
Service	custom	~	
Custom update-URL]&domain=[DOMAIN]&updater=othe	er	
Hostname	http://meineDomain.dyndnss.net/		
Username	myusername		
Password	•••••	1	2
IP source	Private	•	
P renew interval (min)	10		
Force IP renew (min)	72		
Delete			

	Feld Name	Erklärung		
1	Enable	Aktivieren von DDNS Option		
2	Status	Wenn ihre IP-Adresse erkannt wurde, wird sie hier angezeigt.		
3	Service	Einen DDNS-Betreiber von dieser Liste:		
		1. dyndns.org		
		2. 3322.org		
		3. no-ip.com		
		4. easydns.com		
		5. zoneedit.com		
		Wenn ihr DDNS Provider nicht im Router ist, fügen Sie ihn unter		
		"custom" hinzu (URL)		
4	Hostname	Die Domain, unter der der Router erreichbar sein soll und Ihnen von		
		Ihrem DDNS-Anbieter zugewiesen wurde.		
5	Username	Benutzer-Name Ihres Accounts.		
6	Passwort	Passwort Ihres Accounts.		
7	IP source	Hier wählen Sie aus ob Sie aus privatem oder öffentlichen Netz kommen		
8	IP renew interval	Zeitintervall in dem Überprüft werden soll, ob die IP Adresse noch		
		stimmt.		
9	Force IP renew	Zeitintervall, um die IP-Adresse zu erneuern.		

7.3.6 Wireless hotspot

General Settings		
Enabled	✓	
AP IP	192.168.2.254/24	
	The IP address of the router on the	e hotspot network.
Radius server #1	12.23.45.56	
Radius server #2	12.23.45.57	
Authentication port	1812	
Accounting port	1813	
Hotspot name	Toni	
Secret key	••••	2 2

In dem Bild ist eine Beispiel-Konfiguration eingetragen.

	Feldname	Erklärung
1	Enabled	Aktivieren der Hotspot Funktion.
2	AP IP	Die IP-Adresse des Access Point Netzwerkes
		Um eine eigene IP-Adresse zu definieren, muss man nach dem Slash die
		Netzmasken-Nummer (CIDR) angeben.
		Im Fall "192.168.182.254/24" ist "/24" die Netzmaske:
		"255.255.255.0". Das heißt, dass der Router automatisch IP-Adressen
		zwischen 192.168.182.1 und 19.168.182.253 (Maximal 253 Adressen)
		an Geräte im Hotspot-Netzwerk vergibt.
3	Radius server #1	Die IP-Adresse des Radius Servers, der eine Aufenthaltszertifizierung
		von ihrem W-LAN Client braucht.
4	Radius server #2	Die IP-Adresse des zweiten RADIUS Servers.
5	Authentication port	RADIUS Server Aufenthaltszertifizierungs-Port
6	Accounting port	RADIUS Server Kontoführungs-Port
7	Hotspot name	Name des Hotspots
8	Secret Key	Geheimer Schlüssel des Hotspots
9	Allowed hosts	Eine Liste von Hosts, damit ihre Kunden in der Lage sind, unabhänig
		davon, ob sie aufenthaltszertifiziert sind, zuzugreifen.

Logging and FTP settings:

Logging Settings		
Enabled		
Upload via FTP Settings		
Enabled		
Server address	your.ftp.server	
Username	username	
Password	•••••	20 10
Port	9999	
Intervals		
You configure upload timing sett	ings here.	
Description		
Mode	Interval 💌	
Weekdays	1,2,5	
	Enter numbers corresponding we	ekdays separated by commas. E.g. Monday, Tuesday and Friday would be 1,2,5
Upload interval	4 Hours	
Delete		
Add		

	Feldname	Erklärung
1	Logging enabled	Log-Dateien vom Hotspot-Speichern.
2	FTP enabled	Aktivieren von FTP Upload
3	Server address	Die IP-Adresse des FTP Servers, auf dem Sie das Log speichern
		möchten.
4	Username	Benutzer-Name des FTP Servers
5	Passwort	Passwort des FTP Servers
6	Port	Der TCP/IP Port des FTP Servers
7	Description	Beschreibung
8	Mode	Die Modi, wie die Logdateien gespeichert werden sollen.
		"Fixed"=immer zu einem bestimmten Zeitpunkt. "Interval"= in einem
		bestimmten Zeitabstand.
9	Weekdays	Hier können Sie Zahlen eingeben, die für den oder die jeweiligen Tage
		stehen. 1=Montag. Wenn Sie also jeden Dienstag und Samstag
		speichern wollen, geben Sie "2,6" ein.
10	Interval	Sie können angeben, wie oft die Daten gespeichert werden. Zum
		Beispiel alle 4 Stunden.
11	Hours, Minutes	Wenn der Modus "Fixed" ausgewählt ist, muss hier eine Zeit angegeben
		werden, wann der Router die Daten speichern soll.
		Beispiel: Hours=8, Minutes= 15 - dann wird an den eingestellten Tagen
		immer um 8:15 Uhr gespeichert.

•

7.3.7 OpenVPN

VPN (Virtual Private Network) eine Möglichkeit von außen auf das private Netzwerk zuzugreifen als ob man lokal im Netzwerk wäre.

OpenVPN				
OpenVPN instances	PN instances and their current at			
Tunnel Name Tun/Tap Protocol Port Status				
This section contains no values ye	t			
Role: Client	New configuration name:		Add New	

Wählen Sie aus, ob sich der Router zu einem VPN-Netzwerk einwählen soll (Client) oder ob er eines erstellen soll (Server). Danach geben Sie einen Namen bei "New configuration Name:" ein. Klicken anschließend auf "Add New" um die Verbindung zu erstellen.

Role:	Client	💌 New configuration name:	Demo	Add New
-------	--------	---------------------------	------	---------

Jetzt steht in der Tabelle eine neue Verbindung.

Tunnel Name	Tun/Tap	Protocol	Port	Status		
client_Demo	-	-	1194	Disabled	Edit Dele	te

Um nun die Einstellungen der Verbindung zu ändern, klicken Sie auf "Edit"

Ein neues Fenster öffnet sich: OpenVPN instance: client_testclient

Main settings

•				
Enable				
Tun/Tap	Tun (tunnel)	~		
	😰 Type of used device			
Protocol	UDP	~		
Port	1194			
	TCP/UDP port for both,	local and remo	ote	
LZO	🔲 😰 Use fast LZO compr	ression		
Authentication	TIs	×		
Remote host/IP address				
Resolve Retry	infinite			
Keep alive				
	Helper directive to simpl	ify the expres	sion ofping a	ndping-restart
Certificate authority		Durchsuchen.		
Client certificate		Durchsuchen.		
Client key		Durchsuchen.		
				Save

	Feld Name	Erklärung
1	Enable	Aktivieren und deaktivieren dieser Verbindung.
2	Port	Definieren Sie die TCP- oder UDP- Portnummer.
3	LZO	Mit dieser Einstellung können die LZO Kompression einschalten. Mit
		eingeschalteter LZO Kompression erzeugt die VPN-Verbindung
		weniger Netzwerk verkehr. Jedoch erhöht sich die CPU-Last.
		Verwenden Sie LZO Kompression mit Route Traffic oder niedrigen
		CPU-Ressourcen.
4	Authentication	Stellen Sie eine Aufenthaltszertifikationsmodus ein.
5	Remote host IP	IP-Adresse vom VPN Server.
	address	
6	Resolve Retry	Setzt die Zeit in Sekunden, um im Falle eines Fehlers den Hostnamen
		zu erreichen, bevor eine Fehlermeldung generiert wird
7	Keep alive	Es gibt zwei Zeitintervalle: eins um periodisch eine ICMP-Anfrage an
		den VPN-Server zu senden und eins, das ein Zeitfenster definiert, um
		den VPN-Dienst zu starten.
8	Local tunnel endpoint	IP-Adresse des VPN-Interface. (Nur bei point to point Verbindungen)
9	Remote tunnel	IP-Adresse des VPN-Interface.
	endpoint	
10	Remote network IP	IP-Adresse des Remote Virtual Network.
	address	
11	Remote network IP	Subnetmaske des Remote Virtual Network.
	netmask	

7.3.8 IPsec

Wenn IPsec protocol Client eingeschaltet ist kann sich der Router mit einem IPsec via Internet verbinden. Es gibt zwei IPsec Modi. Transport und Tunnel. In der Transportmodus wird eine reine Point zu Point Verbindung zu zwei Hosts aufgebaut. In der Tunnelmode können im LAN Netzwerk arbeiten wie in einer VPN Verbindung.

Das IPsec System hat zwei Datenarten. Security Policy Database (SPD) und Security Association Database (SAD).

Automatic IPSec Key exchange:

Description	
Enable IPsec	
IPSec key exchange mode	Auto Key (IKE)
Mode	aggressive
Enable NAT traversal	
Enable initial contact	
My identifier type	address
My identifier	qwe
Preshare Key	123456789
	😢 (Length [6-32])
Remote VPN endpoint	81.81.81.81
	IP address

	Feldname	Erklärung
1	Enable IPSec	Deaktivieren und aktivieren von IPSec
2	IPSec key exchange	Wählen Sie zwischen manuellen Key, den Sie einrichten wollen oder
	mode	einem automatischen, der generiert werden soll.
3	Enable NAT traversal	Ist diese Funktion aktiviert, können Sie die client-to-client Funktion
		benutzen
4	Enable initial contact	Aktivieren und der Router sendet eine INITIAL-CONTACT Nachricht.
5	Peers identifier type	Wählen zwischen "fqdn" oder "user fqdn",
		dies kommt auf die Einstellungen des IPSec Servers an.
6	Mode	Auswahl zwischen Main oder Aggressive, dies kommt auf die
		Einstellungen des IPSec Servers an.
7	My identifier	Stellen Sie den device identifier für den IPSec Tunnel ein.
8	Preshare key	Geben Sie einen 16 Stelligen Preshare key ein.
9	Remote VPN Endport	Die IP-Adresse des IPSec Server.

Phase 1			
Encryption	3des 💌		
Hash	sha1 💌		
Dh group	modp1024		
Phase 2			
PFS group	modp1024		
Encryption	3des 💌		
Authentication	hmac_sha1		
Remote network secure group			
IP address	192.168.2.0		
Subnet mask	24		
	😰 (Number [0-32])		

In Phase 1 und Phase 2 werden die Einstellungen vom IPSec Server konfiguriert. In Remote network secure group werden remote network (Secure Policy Database) Informationen eingegeben.

Tunnel keep alive		
Enable keep alive		
Ping IP address		
Ping period (seconds)		

	Feld Name	Erklärung
1	Tunnel keep alive	Aktivieren der Sendefunktion eines ICMP Echos (Ping utility) zum
		Remote Tunnel Netzwerk. Diese Funktion startet dann automatisch
		beim Starten eines IPSec Tunnels.
2	Ping IP address	Tragen Sie die IP-Adresse ein, an die das ICMP echo gesendet werden
	-	soll.
3	Ping period (seconds)	Setzt gesendete ICMP-Anfrage in Sekunden

7.3.9 GRE Tunnel

GRE (Generic Routing Encapsulation RFC2784) ist eine Erweitern von RFC1812 Tunneln. Die private IP-Adresse wird im Internet gesucht und wenn sie gefunden wurde, verbindet sich der Tunnel. Nun können Daten Empfangen und gesendet werden.



In dem Beispiel-Netzwerk-Diagramm sind zwei Netze miteinander verbunden.

Um einen GRE Tunnel einzustellen und zu benutzen, brauchen Sie folgende Parameter:

- 1. Ihre und die entfernte IP-Adresse
- 2. Ihre Netzwerk IP-Adresse
- 3. Die entfernte Netzwerk IP-Adresse und Subnetzmaske.

Enable GRE Tunnel	
TTL	
	😰 Value [0-255]
PMTUD	
Remote tunnel network address	
Remote CIDR	
	😰 CIDR (netmask) value [0-32]
Remote IP address	
MTU	1500
	😰 MTU value (0-1500)

	Feld Name	Erklärung
1	Enable GRE Tunnel	Aktivieren des GRE Tunnels.
2	TTL	Spezifizieren Sie die time-to-live Menge an getunnelten Paketen.
		(TTL) möglich sind (0-255)
3	PMTUD	Die Checkbox aktiviert den "Pathmaximum Transmission Unit
		Discovery (PMTUD)"-Status für diesen Tunnel.
4	Remote tunnel	Tragen Sie die Remote LAN Subnetz-Adresse ein.
	network address	
5	Remote CIDR	Tragen Sie die Remote LAN Subnetz CIDR Menge ein.
6	Remote IP address	Tragen Sie die Remote WAN IP-Adresse ein.
7	MTU	Tragen Sie die Maximum Transmission Unit (MTU) für das
		Kommunikations-Protokoll in Bytes ein.

7.4 Systems

7.4.1 Administration

Administration password:

Administrator Password			
Password	•••••	2	
Confirmation		2	

	Feldname	Erklärung
1	Passwort	Geben Sie Ihr neues Administrator-Kennwort ein.
2	Confirmation	Wiederholen Sie das neue Administrator-Kennwort.

Anmerkung:

Der einzige Weg, sich ins Internetportal einzuloggen ist dieses Passwort und der Benutzername "Admin". Wenn Sie Ihr Passwort vergessen ist die einzige Möglichkeit, wieder ins Gerät zu kommen, ein Reset auf Werkseinstellungen. Dann ist der Benutzername "Admin" und das Passwort "admin01"

Logging:

Logging		
System log level	Debug	
Save log in	RAM memory	
Include GSMD information		
Include PPPD information		
Include Chat script information	✓	
System Log	Show	
Kernel Log	Show	

System Mitteilungen werden in folgende Kategorien aufgeteilt:

mio (mios)
Notice (Notizen)
Warning (Warnungen)
Error (Fehler)
Critical
Alert (Notfall)
Emergency

Um das Systemlog (Protokoll) zu sehen, klicken Sie hinter "System Log" auf "Show"

SSH Access Control:

SSH Access control		
SSH Access	Enabled	4
Port	22	
	Port to listen for SSH access.	
Remote SSH Access		

	Feld Name	Erklärung
1	SSH Access	SSH können Sie aktivieren und deaktivieren.
2	Port	Spezieller Port für SSH-Zugang. Standartport ist 22.
3	Remote SSH access	Wenn die Checkbox aktiviert ist kann der Benutzer sich von außen über WAN in den Router einloggen. Wenn Sie nicht aktiviert ist kann man nur vom Internet des Netwerks (LAN) auf den Router zugreifen und sich einloggen.

Anmerkung: Der Router hat zwei Benutzer "admin" für internen Zugriff (LAN) und "root" für das SSH.

Web Access control:

Web Access control	
HTTP Web Server port	80
Remote HTTP Access	
HTTPS Web Server port	443
Remote HTTPS Access	

	Feld Name	Erklärung	
1	HTTP Web Server	Port-Nummer, die der Router für seine Web-Oberfläche benutzt.	
	port	Standard ist 80 und er benutzt das HTTP Protokoll.	
2	Remote HTTP access	Ist die Checkbox aktiviert, kann der Benutzer via HTTP WEB	
		Interface von außen (WAN) Erreicht werden. Wenn die Checkbox	
		nicht aktiviert ist kann der Benutzer nur über die Interne LAN-	
		Verbindung auf den Router zugreifen.	
3	HTTPS Server Port	Port-Nummer, die der Router für seine Web-Oberfläche benutzt.	
		Standard ist 443 und er benutzt das HTTPS Protokoll	
4	Remote HTTPS	Ist die Checkbox aktiviert, kann der Benutzer via HTTPS WEB	
	Access	Interface von außen (WAN) erreicht werden. Wenn die Checkbox	
		nicht aktiviert ist kann der Benutzer nur über die Interne LAN-	
		Verbindung auf den Router zugreifen.	

7.4.2 Backup und Firmware

Backup and reset configuration:

Backup a	nd reset	configuration
----------	----------	---------------

Backup archive:	Download
Reset to defaults:	Reset

Backup archive – Speichert die Routereinstellungen auf ihren Computer. Reset to defaults – Reset zu Werkseinstellungen.

Restore configuration :

Restore configuration		
Restore backup:		Durchsuchen
	Upload archive	

Restore backup – Hier können ie von Ihnen speicherten Routereinstellungen wieder in den Router geladen werden.

Firmware upgrade:

Firmware upgrade	
Keep settings: 🗹	
Image:	Durchsuchen
Upgrade	

Keep settings – wenn die Checkbox aktiviert ist, speichert der Router die Einstellungen für den Neustart nach dem Firmware Upgrade. Image – Router Firmware Upgrade Datei.

Firmware Upgrade – Verify:

Firmware upgrade - Verify

The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity. Click "Proceed" below to start the flash procedure.

Size: 4.38 MB (7.69 MB available)

Configuration files will be kept.

Wenn die angezeigten Daten stimmen klicken Sie auf "Proceed" und warten, bis das Upgrade komplett aufgespielt ist.

Anmerkung:

Wenn sie "Keep Settings" nicht aktivieren dann ist die IP-Adresse, unter der Router zu ereichen ist 192.168.1.1 und die Anmeldedaten sind: Benutzername=Admin, Passwort=admin01.



Warnung: Während des Upgrades bitte nicht die Stomverbindung für den Router unterbrechen oder die Reset-Taste drücken. Dies würde den Router sofort zerstören! Wenn Sie Probleme mit ihrem Upgrade haben wenden Sie sich bitte an Ihren Händler!

7.4.3 Reboot

Click to reboot

Reboot

Der Router startet neu, wenn Sie auf "Reboot" klicken.

7.5 Logout

Ausloggen aus dem Internetinterface.

8 Open VPN

8.1 Installation

8.1.1 Download

Die "OpenVPN" Installationsdatei mit Hilfe des nachfolgenden Links herunterladen. (http://openvpn.net/index.php/open-source/downloads.html)

8.1.2 Programm installieren

Die Installation bis zu folgender Auswahl fortsetzen:

🞧 OpenVPN 2.3.1-I001 Setup	-	• 🔀
	hoose Components Thoose which features of OpenVPN 2.3.1-I001 you war hstall.	nt to
Select the components to insta service if it is running. All DLLs	all/upgrade. Stop any OpenVPN processes or the Open are installed locally.	VPN
Select components to install:	TAP Virtual Ethernet Adapter OpenVPN GUI OpenVPN File Associations OpenSL Utilities OpenVPN RSA Certificate Management Scrip Add OpenVPN to PATH Description	E ts
Space required: 3.6MB	Position your mouse over a component to see its description.	
Nullsoft Install System v2.46-101	< Back Next >	Cancel

Wenn Sie mit dem Computer Zertifikate erstellen möchten:

Installieren sie zusätzlich "OpenSSL Utilities" und "Open VPN RSA Certificates Management Scripts". Alle anderen Installationsmöglichkeiten sollten ausgewählt sein. Installation mit "Next" fortsetzen und abschließen.

8.2 Zertifikate erstellen

8.2.1 Passwort setzen

Öffnen Sie die die cmd.exe (Start -> Ausführen -> cmd.exe)



Wenn Sie die OpenVPN Installation in das Standard Verzeichnis installiert haben. Geben Sie "cd \Program Files\OpenVPN\easy-rsa" in die Befehlszeile ein. (Bei Installation in einem anderen Verzeichnis, dass von Ihnen gewählte Verzeichnis eingeben).

Wenn Sie mit Ihrem Computer zum ersten Mal Zertifikate erstellen oder keine Zertifikate wiederherstellen möchten, geben Sie "init-config" in die Befehlszeile ein. Ansonsten diesen Schritt überspringen.

Um Ihr Passwort zu definieren, geben Sie in die Befehlszeile "vars", "clean-all" und "build-ca" ein.

Country Name (2 letter code) [US]:us State or Province Name (full name) [CA]:ca Locality Name (eg, city) [SanFrancisco]:san Organization Name (eg, company) [OpenUPN]:name Organizational Unit Name (eg, section) [changeme]:name Common Name (eg, your name or your server's hostname) [changeme]:Unique_name Name [changeme]:name Email Address [mail@host.domain]:email@company.com

Es wird nach den jeweiligen Informationen des Zertifikates gefragt, welche Sie in der Befehlszeile eingeben können.

Anmerkung:

- > Nur "Common Name" Name muss einzigartig gegenüber den anderen Namen sein.
- > "A challenge Password" Wird für alle Zertifikate Ihrer Geräte genutzt.

Anschließend haben Sie unter "C:\OpenVPN\easy-rsa\keys catalog\" die Datei "ca.crt". (Dieser Schritt muss nur einmal gemacht werden. Die erstellte Datei wird vom Server und allen Geräteeinstellungen genutzt).

8.2.2 Server Zertifikat erstellen

Um Server Zertifikate zu erstellen, geben Sie in die Befehlzeile "vars" und "build-key-server server" ein.

```
Country Name (2 letter code) [US]:us

State or Province Name (full name) [CA]:ca

Locality Name (eg, city) [SanFrancisco]:san

Organization Name (eg, company) [OpenUPN]:open

Organizational Unit Name (eg, section) [changeme]:name

Common Name (eg, your name or your server's hostname) [changeme]:Unique_name_2

Name [changeme]:name

Email Address [mail@host.domain]:mail

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:password

An optional company name []:name
```

Anschließend können Sie mit "y" die Angaben bestätigen. Jetzt haben Sie zwei neue Dateien erstellt ("server.key" und "server.crt"). Zu finden unter: (C:\OpenV-PN\easy-rsa\keys catalog\).

Um eine "Diffie Hellman" Datei zu erstellen, schreiben Sie in der Befehlszeile "build-dh" .Jetzt haben Sie unter (C:\OpenVPN\easy-rsa\keys catalog\ eine neue Datei ("dh1024.pem").

8.2.3 Geräte Zertifikat erstellen

Um ein Geräte Zertifikat zu erstellen, geben Sie in der Befehlszeile "vars" und "build-key <username>" ein.

```
Country Name (2 letter code) [US]:us
State or Province Name (full name) [CA]:ca
Locality Name (eg, city) [SanFrancisco]:sa
Organization Name (eg, company) [OpenUPN]:op
Organizational Unit Name (eg, section) [changeme]:uni
Common Name (eg, your name or your server's hostname) [changeme]:unique
Name [changeme]:name
Email Address [mail@host.domain]:mail
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:password
An optional company name []:name
```

Sie werden wieder nach den Informationen für das Zertifikat gefragt. Geben Sie diese ein und bestätigen Sie Diese mit "y".

Anmerkung:

- ➢ Bei "Common Name" den vorher definierten Namen angeben.
- > "A challenge Password" das vorherige Passwort angeben.

Anschließend haben Sie im Verzeichnis (C:\OpenVPN\easy-rsa\keys catalog\) zwei neue Dateien ("unique.crt" und "unique.key").

8.3 TONI als OpenVPN "TL's" Server

Öffnen Sie das TONI Webinterface (z.B. 192.168.1.1 in Adresszeile des Browsers eingeben) und gehen Sie zum Menüpunk (Services -> OpenVPN). Erstellen Sie einen Server mit beliebigen Namen.

OpenVPN				
OpenVPN instances				
Below is a list of configured Open ^v	/PN instances and their current sta	te		
Tunnel Name	Tun/Tap	Protocol	Port	Status
This section contains no values y	<i>ret</i>			
Role: Server	 New configuration name: 	server	Add New	
Teltonika solutions: www.teltonika	.lt			

Anschließend sehen Sie folgendes:

server_server	TUN	UDP	1194	Disabled	Edit Delete
---------------	-----	-----	------	----------	-------------

Klicken Sie auf "Edit" um Einstellungen vorzunehmen.

Main settings	
Enable	
Tun/Tap	Tun (tunnel)
	Type of used device
Protocol	UDP 💌
Port	1194
	TCP/UDP port for both, local and remote
LZO	🗌 😰 Use fast LZO compression
Authentication	TIs
Client to client	Image: Allow client-to-client traffic
Keep alive	10 120
	P Helper directive to simplify the expression ofping andping-restart in server mode configurations
Virtual network IP address	
Virtual network netmask	
Certificate authority	Durchsuchen
Server certificate	Durchsuchen
Server key	Durchsuchen
Diffie Hellman parameters	Durchsuchen
TLS Clients Here you can add your VPN clie	ents so that they may be reachable from the server.
This section contains no values	yet
	Add

OpenVPN instance: server_test

Falls der OpenVPN-Server nicht anläuft obwohl "enabled" gesetzt ist, dann bitte folgende Punkte beachten:

- ggfls. Zertifikate nochmals neu in den Toni hochzuladen
- prüfen Sie nochmals die eingegeben Daten und ggf. IP-Adresse abändern
- wenn obige Punkte keine Besserung bringen dann bitte **TONI** auf Werkseinstellung setzen und Konfiguration neu einstellen

Feld	Beschreibung
Enable	VPN aktivieren oder deaktivieren.
Tun/Tap	Angaben über die Art des VPN Servers.
	Tunnel oder Brücke
Protocol	Art vom Port: UDP oder TCP.
Port	Standard Port für OpenVPN ist 1194
LZO	Kompressionsverfahren aktivieren oder deakti-
	vieren (Einsparung von Bandbreite).
Authentication	TIs für mehrere Geräte
Client to client	Um Geräte untereinander Verbindungen möglich
	zu machen.
Keep alive	Standardwerte sind 10 120
Virtual network IP address	Ihre virtuelle Netzwerk IP-Adresse. Sie können
	nur den 2. Wert definieren. (10.X.0.0).
Virtual network netmask	Standardwert (255.255.255.0) als Netzwerkmas-
	ke.
Certificate authority	Vorher erstellte Datei ca.crt hochladen.
Server certificate	Vorher erstellte Datei server.crt hochladen.
Server key	Vorher erstellte Datei server.key hochladen.
Diffie Hellmanparameters	Vorher erstellte Datei dh1024.pem hochladen.

Standardmäßig kann jeder der sich mit dem Server verbindet untereinander mit den virtuellen IP-Adressen verbinden. Wenn Sie aber auf eine lokale IP-Adresse zugreifen wollen, müssen Sie diese Geräte hier hinzufügen.

TLS Clients

Here you can add your VPN clients so that they may be reachable from the server.	
This section contains no values yet	
Add	Save

Einstellungen beim Hinzufügen eines Gerätes:

test	
VPN Instance name	server_test
	With what openVPN Instance should this entry be associated v
Endpoint Name	
	Your endpoint name. E.g.: "MyHomeComputer"
Common Name (CN)	
	😰 Client certificate CN field. E.g.: " name.surname@domain.com'
Virtual Local Endpoint	
	😰 E.g.: "10.8.1.10"
Virtual Remote Endpoint	
	😰 E.g.: "10.8.1.9"
Private Network	
	The IP of the private NETWORK. E.g.: "192.168.1.0"
Private Netmask	
	Phe Netmask of the private network. E.g.: "255.255.255.0"
Delete	

Feld	Beschreibung
VPN Instance name	Standardname (Default)

Endpoint Name	Gerätename (Computer)
Common Name (CN)	Vordefinierter Name
Virtual Local Endpoint	Benutzen Sie die IP-Endungen von der nachfol-
	genden Tabelle.
Virtual Remote Endpoint	Benutzen Sie die IP-Endungen von der nachfol-
	genden Tabelle.
Private Network	Standard-IP des Gerätes eintragen
Private Netmask	Standardwert (255.255.255.0).

Benutzen Sie die nachfolgenden Vorgaben für die Endung der IP-Adresse.

8.4 TONI als OpenVPN "TL's" Gerät

Öffnen Sie das TONI Webinterface (z.B. 192.168.1.1 in Adresszeile des Browsers eingeben) und gehen Sie zum Menüpunk (Services -> OpenVPN). Erstellen Sie einen Client mit beliebigen Namen.

OpenVPN				
OpenVPN instances				
Below is a list of configured Oper	nVPN instances and their current stat	te		
Tunnel Name	Tun/Tap	Protocol	Port	Status
This section contains no values Role: <mark>Client</mark>	<i>yet</i> New configuration name:	config.	Add New	

Anschließend sehen Sie folgendes:

New OpenVPN instance created successfully, configure it					
OpenVPN					
OpenVPN instances					
Below is a list of configured OpenVPN instances and their current state					
Tunnel Name	Tun/Tap	Protocol	Port	Status	
client_config	TUN	UDP	1194	Disabled	Edit Delete
Role: Client	 New configuration 	uration name:		Add New	

Klicken Sie auf "Edit" um Einstellungen vorzunehmen.
OpenVPN instance: client_test

Main	settings
I VI CIIII	settings

Enable	
Tun/Tap	Tun (tunnel)
	😰 Type of used device
Protocol	UDP 💌
Port	1194
	TCP/UDP port for both, local and remote
LZO	🔲 😰 Use fast LZO compression
Authentication	TIs 💌
Remote host/IP address	
Resolve Retry	infinite
Keep alive	
	Helper directive to simplify the expression ofping andping-restart
Certificate authority	Durchsuchen
Client certificate	Durchsuchen
Client key	Durchsuchen
	Save

Feld	Beschreibung
Enable	Gerät aktivieren oder deaktivieren
Port	Standardport ist 1194
LZO	Kompressionsverfahren aktivieren oder deakti-
	vieren (Einsparung von Bandbreite)
Authentication	Benutzen Sie TIs
Remote host/IP address	Server IP-Adresse
Resolve Retry	Standardwert infinite
Keep alive	Standardwert 10 120
Certificate authority	Vorher erstellte Datei ca.crt hochalden
Client certificate	Vorher erstellte Datei unique.crt hochladen
Client key	Vorher erstellte Datei unique.key hochladen.

8.5 Computer als OpenVPN "TL's" Server

Im Verzeichnis (C:\Program Files\OpenVPN\config) eine "server.opvn" Datei erstellen und mit dem Windows Editor folgende Informationen eintragen:

server.ovpn
port 1194
proto udp
dev tun
ca <mark>ca.crt</mark>
cert <mark>server.crt</mark>
key <mark>server.key</mark>
dh <mark>dh1024.pem</mark>
server <mark>10.8.0.0</mark> 255.255.255.0
ifconfig-pool-persist ipp.txt
keepalive 10 120
<mark>comp-lzo</mark>
persist-key
persist-tun
status openvpn-status.log
verb 3

Zuerst wählen Sie Ihre virtuelle IP-Adresse "10.X.0.0". Standard wäre "10.8.0.0". Wenn Sie die Übertragung komprimieren möchten. Lassen Sie "com-lzo" stehen. Ansonsten können Sie diese Zeile löschen.

Die grün markierten Dateien sollten mit selben Dateinamen in das Verzeichnis (C:\Program Files\OpenVPN\config) kopiert werden. (Gleicher Ordner wie die Server-Konfigurations-Dateien.

Um ein Gerät mit einer Statischen und virtuellen IP zu erstellen, müssen Sie eine Datei mit einem einzigartigen Namen erstellen. Zum Beispiel: "unique" mit folgendem Inhalt.

ifconfig-push 10.8.0.10 10.8.0.9 iroute 192.168.2.0 255.255.255.0 push route 192.168.99.0 255.255.255.0 push route 192.168.3.0 255.255.255.0

Zeile	Beschreibung
ifconfig-push	virtual local and endpoint address
iroute	Adresse des Gerätes, welches Sie gerade Konfi-
	gurieren (IP und Netzwerkmaske).
push route	Die Server IP-Adresse und Netzwerkmaske.
push route	Weitere Adressen anderer Geräte (IP und Netz-
-	werkmaske).

Wenn Sie anderen Geräten ins Subnetzwerk verbinden möchten, zum Beispiel wenn Sie einen Server mit Subnetz 192.168.2.0 und 3 andere Geräte mit Subnetze wie 192.168.3.0, 192.168.4.0 und 192.168.5.0 haben, dann müssen Sie Ihr Gerät mit 192.168.3.0 wie nachfolgend Im Bild beschrieben konfigurieren.

ifconfig-push 10.8.0.150 10.8.0.149 iroute 192.168.3.0 255.255.255.0 push route 192.168.2.0 255.255.255.0 push route 192.168.4.0 255.255.255.0 push route 192.168.5.0 255.255.255.0

8.5 Computer als OpenVPN "TL's" Gerät

Erstellen Sie im Verzeichnis (C:\Program Files\OpenVPN\config" eine "unique.opvn" Datei mit folgendem Inhalt:

## remote.ovpn ##	
client	
dev tun	
proto udp	
remote <mark>192.168.99.151 1194</mark>	
resolv-retry infinite	
nobind	
persist-key	
persist-tun	
ca <mark>ca.crt</mark>	
cert <mark>unique.crt</mark>	
key <mark>unique.key</mark>	
comp-lzo	
verb 3	
route-delay	

Zeile	Beschreibung
remote	Die Server IP-Adresse mit Port (Standard =
	1194).
ca ca.crt	Diese Dateien sollten in Ihrem Verzeichnis
cert unique.crt	(C:\Program Files\OpenVPN\config) sein.
key unique.key	
	Dieser Ordner ist der selbe, wie der der Geräte-
	konfigurationsdatei.

Anschließend öffnen Sie mit Ihrem Computer das "OpenVPN GUI" Programm. Es sollte durch den OpenVPN Installationsdatei vom vorherigen Schritt installiert sein.

Nun sehen Sie in Ihrerer Taskleiste folgendes Symbol:



Klicken Sie mit der rechten Maustaste und wählen "Connect".

8.5 Computer als "Static Key" Gerät

Öffnen Sie "Generate a static OpenVPN key". Anschließend finden Sie unter (C:\Program Files\OpenVPN\config" eine neue Datei ("key.txt").

Öffnen Sie das oben angegebene Verzeichnis und erstellen Sie eine Datei mit die exakt "static.ovpn" heißt und im Windows Editor folgende Informationen enthält:

remote <mark>192.168.99.156</mark>
verb 3
proto udp
dev tun
ifconfig <mark>10.8.0.</mark> 6 <mark>10.8.0.</mark> 5
<mark>key.txt</mark>

Tragen Sie bei

- "ifconfig" die Virtuelle und Locale IP-Adresse ein.

8.6 TONI als OpenVPN "Static Key" Server

Öffnen Sie das TONI Webinterface (z.B. 192.168.1.1 in Adresszeile des Browsers eingeben) und gehen Sie zum Menüpunk (Services -> OpenVPN). Erstellen Sie einen Server mit beliebigen Namen.

OpenVPN				
OpenVPN instances				
Below is a list of configured OpenV	PN instances and their current stat	e		
Tunnel Name	Tun/Tap	Protocol	Port	Status
This section contains no values ye	ət			
Role: Server	▼ New configuration name: s	erver	Add New	
Teltonika solutions: www.teltonika.	t			

Anschließend sehen Sie folgende Aufstellung:

server_server	TUN	UDP	1194	Disabled	Edit Delete
---------------	-----	-----	------	----------	-------------

Um Einstellungen vornehmen zu können, klicken Sie auf "Edit".

OpenVPN instance: server_test		
Main settings		
Enable		
Protocol	UDP 💌	
Port	1194	
	TCP/UDP port for both, local and	remote
LZO	🔲 🔞 Use fast LZO compression	
Authentication	Static key 💌	
Local tunnel endpoint IP	10.8.0.1	
Remote tunnel endpoint IP	10.8.0.2	
Resolve Retry	infinite	
Remote network IP address	192.168.3.0	
Remote network netmask	255.255.255.0	
Static pre-shared key	Durchsuc	hen

Feld	Beschreibung
Enable	Gerät aktivieren oder deaktivieren
Port	Standardport ist 1194
LZO	Kompressionsverfahren aktivieren oder deakti-
	vieren (Einsparung von Bandbreite)
Authentication	Benutzen Sie Static key

Remote host/IP address	Server IP-Adresse
Resolve Retry	Standardwert infinite
Local tunnel endpoint IP	Wählen Sie die lokale IP von der Konfiguration
Remote tunnel endpoint IP	Wählen Sie die virtuelle IP von der Konfigurati-
	on
Remote network IP address	Wählen Sie die Geräte IP-Adresse.
Remote network netmask	Wählen Sie Ihre Geräte Netzwerkmaske
Static pre-shared key	Laden Sie Ihre key.txt Datei hoch.

Anschließend öffnen Sie mit Ihrem Computer das "OpenVPN GUI" Programm. Es sollte durch den OpenVPN Installationsdatei vom vorherigen Schritt installiert sein.

Nun sehen Sie in Ihrerer Taskleiste folgendes Symbol:



Klicken Sie mit der rechten Maustaste und wählen "Connect".

9 Technische Daten:

LAN und W-LAN:

- ▶ Wireless AP, Router, 4-Port Switch und Firewall sind im Gerät integriert
- > 320MHZ CPU mit 256Mbits SDRAM
- ▶ IEEE 802.11b/g/n, IEEE 802.3, IEEE 802.3u Standards
- ▶ 64/128-bit WEP, WPA, WPA2, WPA&WPA2 Verschlüsselungen
- ➤ 3xLAN 10/100Mbps Ethernet Ports
- > 1xWAN 10/100Mbps Ethernet Port
- Automatische Auswahl zwischen MDI/MDIX
- Remote/lokal Web Oberfläche
- SSID Sicherheits-Mode und Zugriff-Kontrolle über MAC Adressen
- System Protokoll um den Status vom Router aus zu zeichnen
- Auto Suche/Manuelle Suche für IEEE 802.11b/g/n
- > Dynamische DNS
- LAN Access Kontrolle über Internet-Verbindung
- Virtual Server
- Automatisch W-LAN Kanal Auswahl
- Open VPN
- Backup über WAN
- ➢ IPSec
- SMS und Ping Neustart
- Power über WAN und LAN
- ➢ 1x 5dBi W-LAN Antenne
- Montage auf Hutschiene (Din rail) optional möglich

HSUPA/HSDPA/UMTS:

- ▶ Power Klasse 3 (0.25W,24dBm) für UMTS
- ▶ UMTS mode: 383Kbps DL/384 Kbps UL
- ► HSUPA mode: 5.76 Mbps (Cat 6) uplinkspeed
- ➢ 3dBi Antenne
- Modulspezifische Frequenzen und Downlinkgeschwindigkeit (bis zu 21 Mbps (Cat14))

GSM/GPRS/EDGE

- ➢ 850/900/1800/1900 MHz
- > Power Klasse 4 (2 W, 33 dBm) für GSM/GPRS 850/900 MHz band
- > Power Klasse 1 (1 W, 30 dBm) für GSM/GPRS 1800/1900 Mhz band
- ▶ Power Klasse E2 (0.5 W, 27 dBm) für EDGE 850/900 MHz band
- > Power Klasse E2 (0.4 W, 26 dBm) für EDGE 1800/1900 MHz band
- ➢ GSM: 14.4 Kbps DL/14.4 Kbps UL
- Module specific GPRS DL/UL speeds (up to 107 kbps (class 33))
- Module specific EDGE DL/UL speeds (up to 296 kbps (class 33))

Elektrisch, Mechanisch & Environmental:

- Maße: (H x B x H) 100mm x 85 mm x 36mm
- ➢ Gewicht: 210-260g
- Spannung 100 -230 VAC \rightarrow 9 VDC Adapter
- Eingangs Spannung: 7 30VDC (8 18 VDC für ältere Generationen*)
- ➢ Benötigter Strom < 7W</p>

- 2xSMA Anntennenkontakte f
 ür 3G (1 x SMA f
 ür andere Modelle), 1x RP-SMA f
 ür W-LAN
- ➢ 4 LEDs für Ethernet, eine Power LED, eine 3G LED
- Betriebs-Umgebungstemperatur: 0°C bis +50°C
- Lager-Umgebungstemperatur -20°C bis +70°C
- Luftfeuchtigkeit während dem Betrieb 10% bis 90% nicht kondensierend
- Luftfeuchtigkeit während dem Lagern 5%bis 95%

*– Neue Hardwarerevision hat 7 – 30VDC Es steht auf dem Gerät was für eine Spannung Sie benötigen. Ältere Hardware braucht 9V - 1A

10 Bezeichnungen:

WAN – Wide Area Network ist ein Telekomunikations Netzwerk, das außerhalb des eigenen Netzwerk in Kraft tritt. (Internet)

LAN – Local Area Network ist ein internes Computer-Netzwerk, das Computer untereinander verbindet

DHCP – Das Dynamic Host Configuration Protocol ist ein Netzwerk-Konfigurations-Protokoll und für IP-Adressen zuständig.

ETHERNET CABLE – ist ein CAT 5 UTP Kable mit einem RJ-45 Kontakt. Mit anderen Worten das Standard Internet Kabel.

AP – Access Point ist dafür zuständig, dass die W-LAN Geräte in das Netzwerk als Client verbinden können.

DNS – Domain Name Resolver ist ein Server, der, wenn sie den Namen "www.google.com" suchen, das ganze wieder zu einer IP-Adressen umwandelt, damit der gesuchte Server (in dem Fall Google) gefunden werden kann.