HSPA+-Router
Toni

Basis FW-Stand: NW_00.02.21

Inhalt

1 Beschreibung:

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!

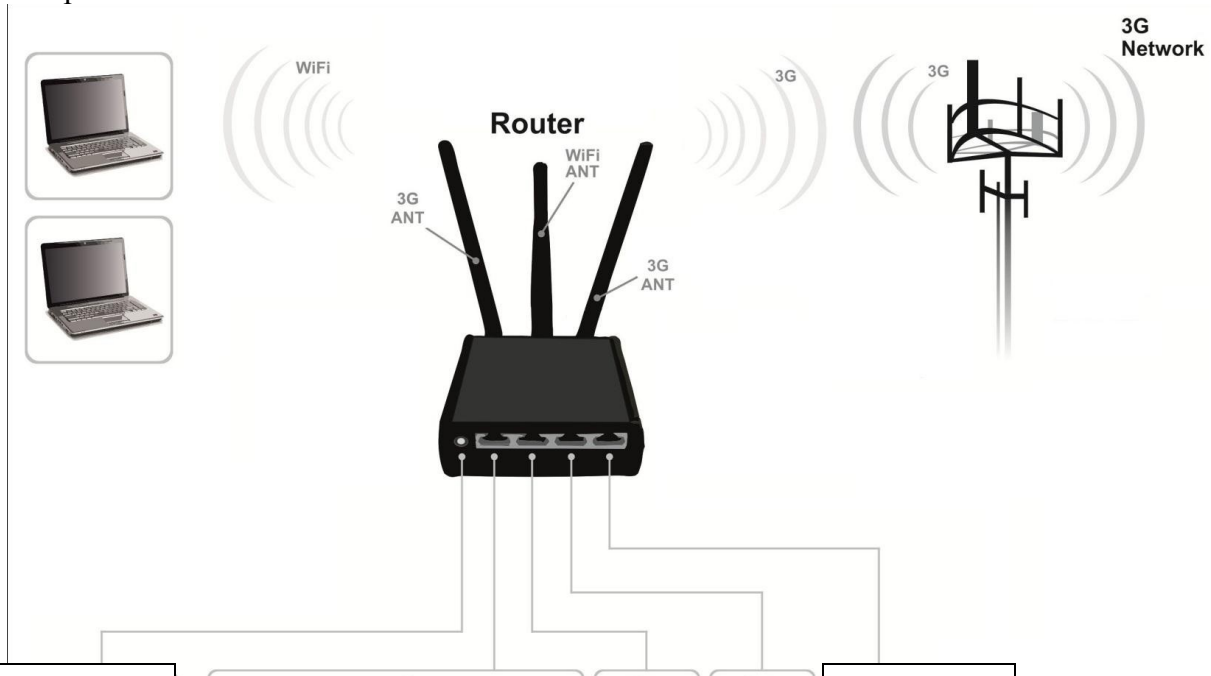
Alle Geräte, die drahtlose Funkverbindungen aufbauen, können Störungen hervorrufen.

Das Gerät ist nicht wasserfest! Halten Sie es trocken.

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

3 Betriebs-/ Einsatzarten:

Beispiel:



Strom 24V (nur den Original-adapter verwenden)

WAN- oder LAN-Adapter

4 Installation:

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:

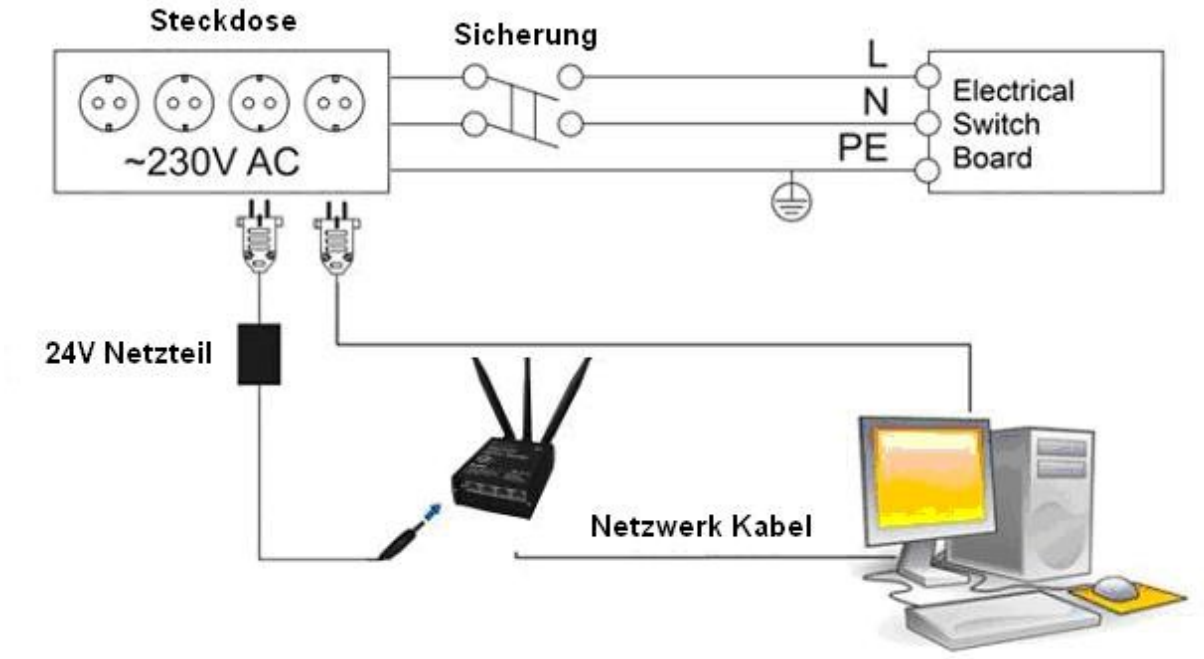
Schrauben Sie TONI hinten auf und setzen Sie dort die SIM-Karte ein.

4.2 Antennen anschrauben

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

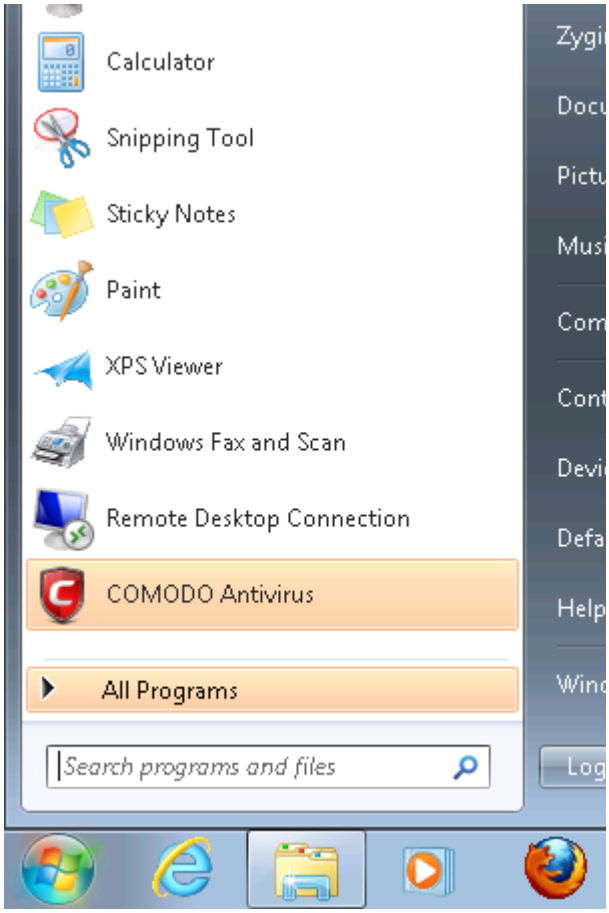
4.3 Gerät das erste Mal verbinden



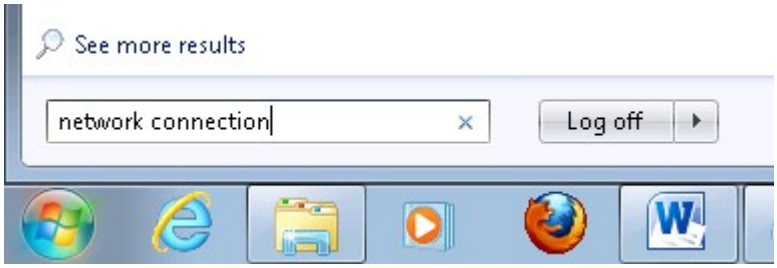
4.4 W-LAN Verbindung

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

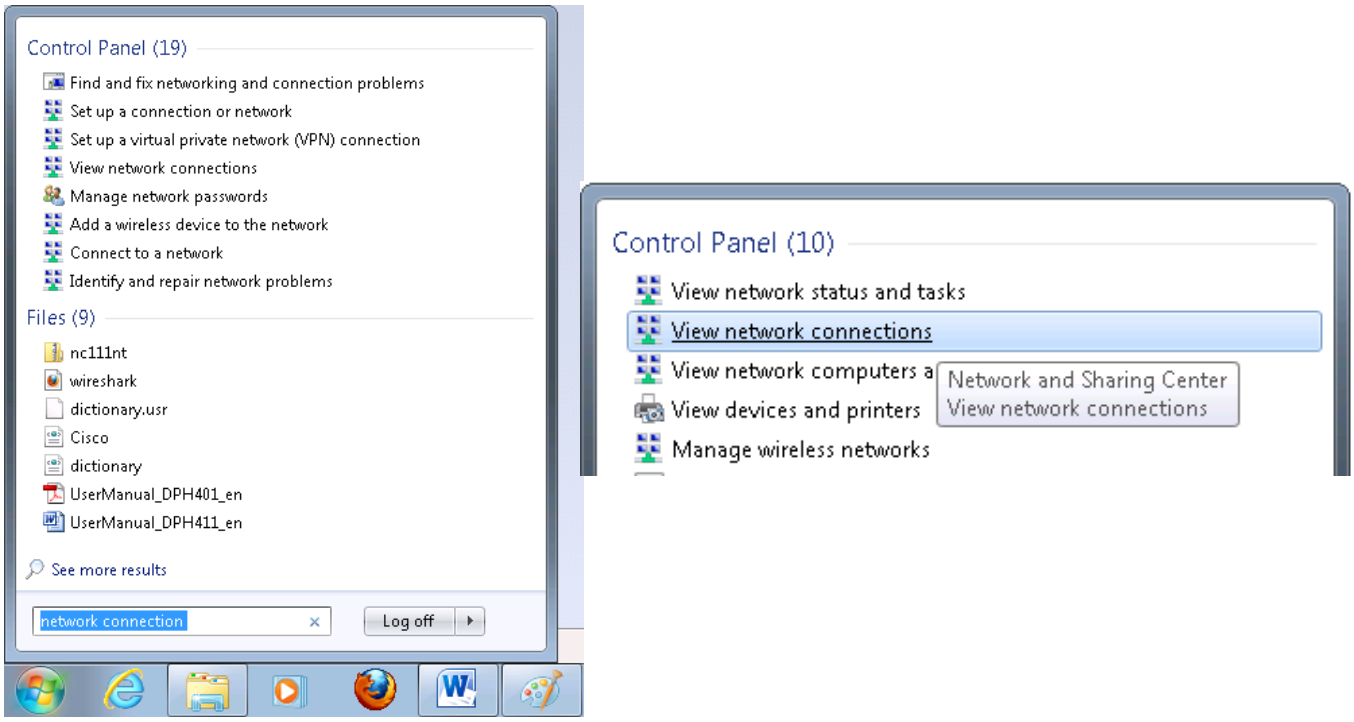
Drücken Sie den Start Button.



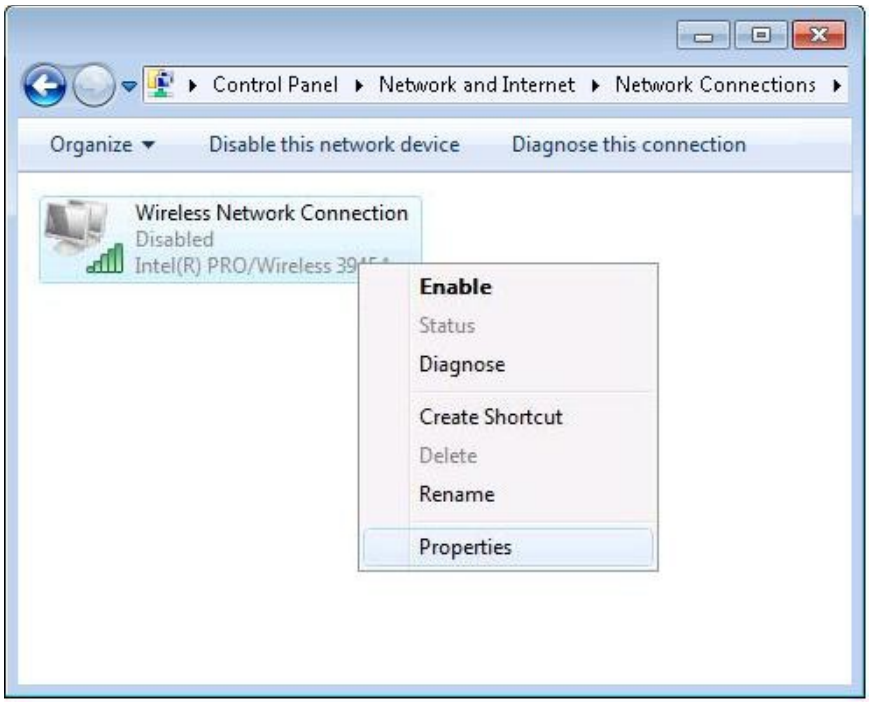
Im Start Fenster geben Sie nun **„network connection“** ein.



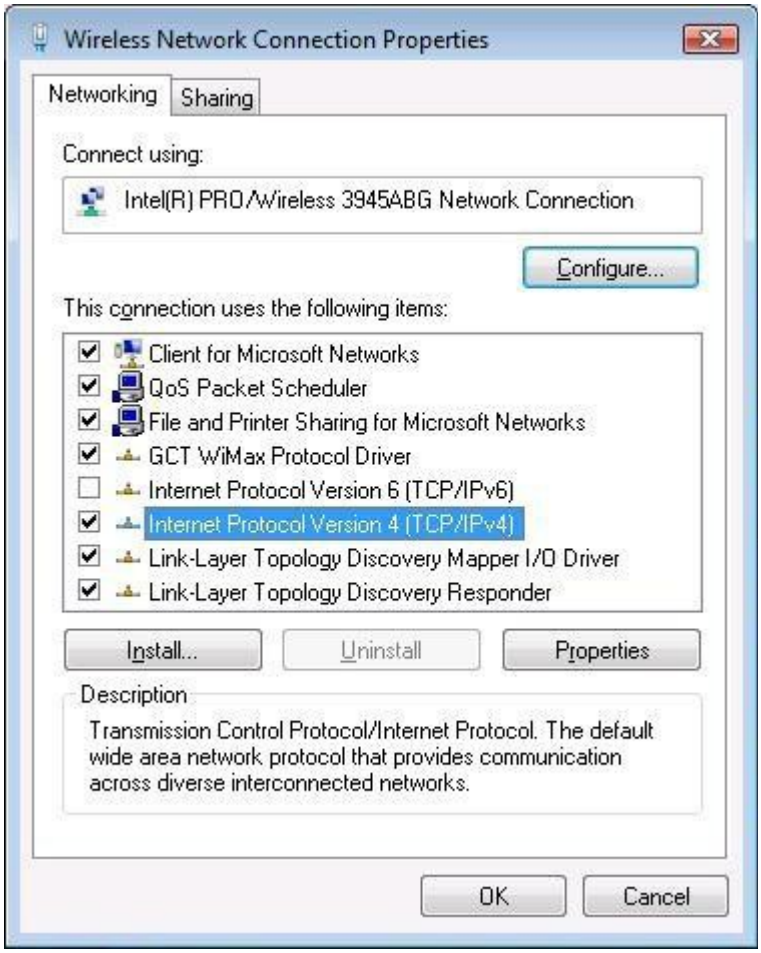
Da Sie eine neue Verbindung aufbauen möchten, klicken Sie nun auf **„View network connections“**.



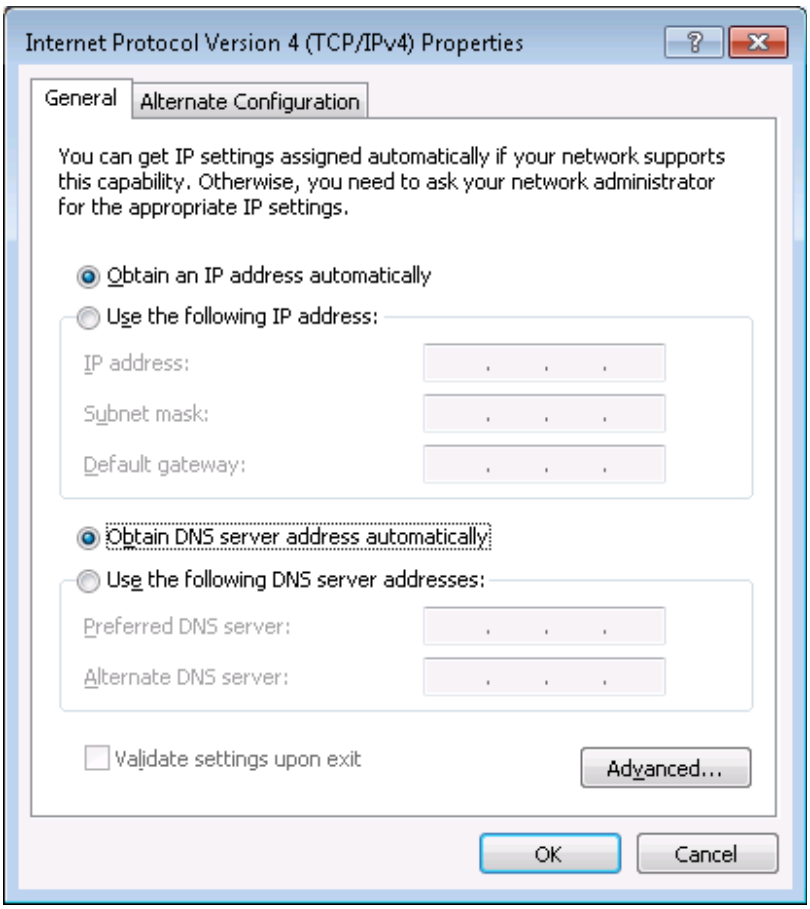
Nun rechtsklicken Sie auf „**Wireless Network Connection**“ und dann auf „Eigenschaften“.



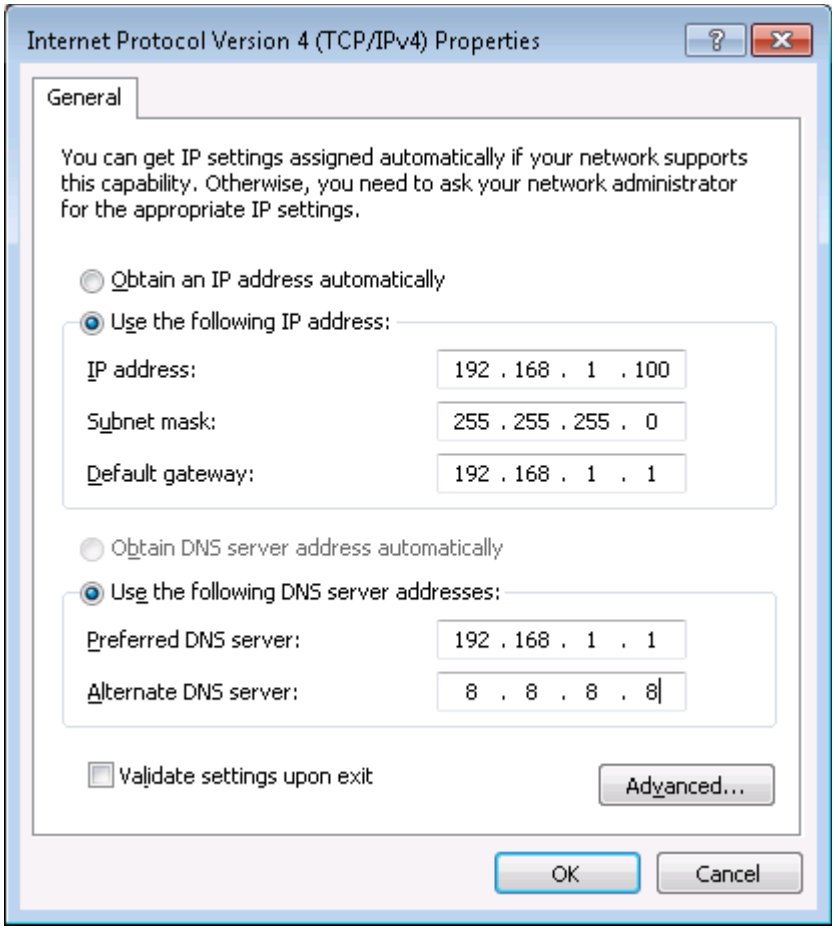
Hier legen Sie nun Netzwerkeinstellungen im **„Internet Protokoll Version 4(TCP/IPv4)“** fest.



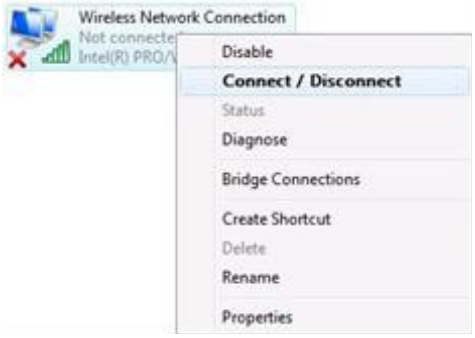
Bei den Werkseinstellungen des TONIs ist der DHCP Server eingeschaltet. Sodass dem PC eine IP-Adresse zugewiesen wird. Daher muss die Einstellung so aussehen:



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).



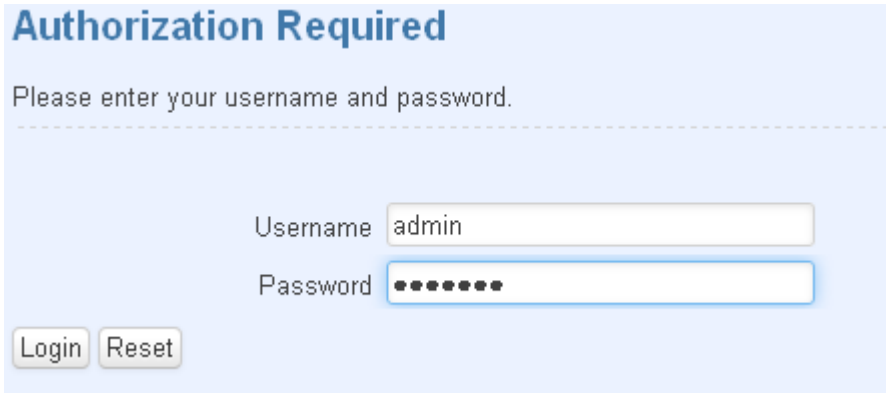
Um nun die Verbindung aufzubauen, klicken Sie wieder mit einem Rechtsklick auf „**Wireless Network Connection**“ und dann auf: „Verbinden/Trennen“



4.5 Der erste Start

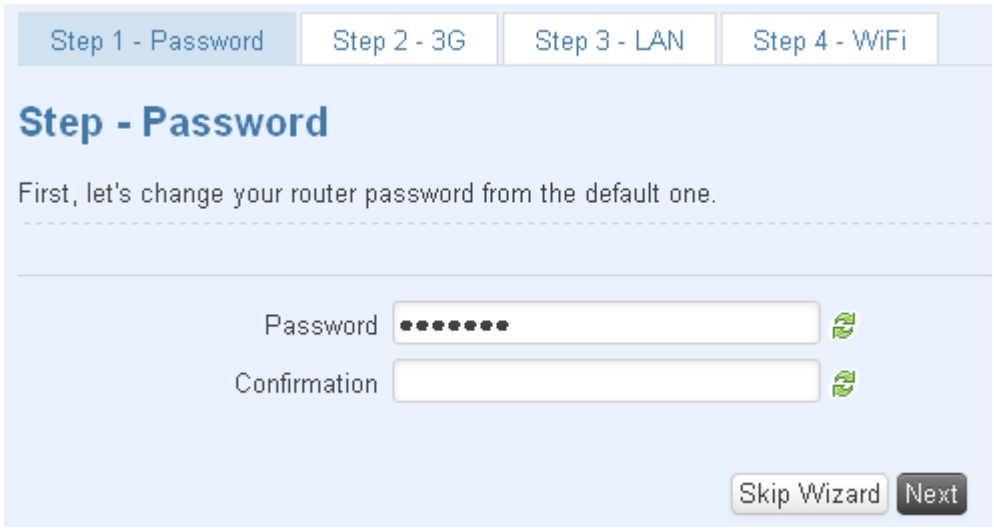
Um das erste Mal auf die Weboberfläche zu gelangen, öffnen Sie Ihren Webbrowser und geben die IP-Adresse des TONIs (Default-IP: 192.168.1.1) ein.

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

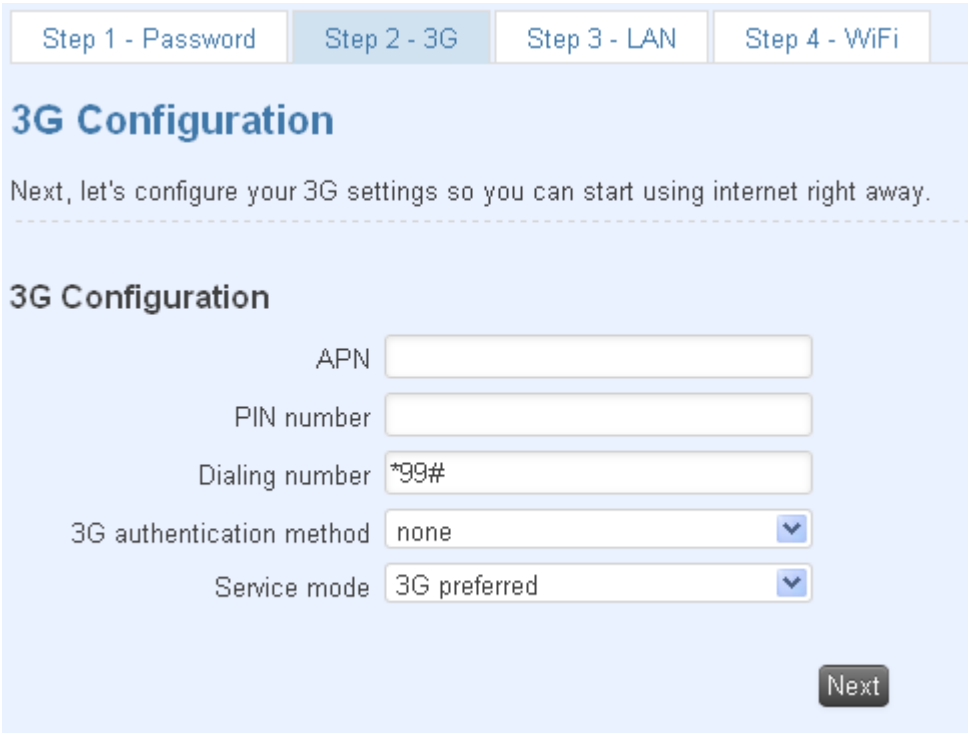


4.6 Einrichtungs-Assistent

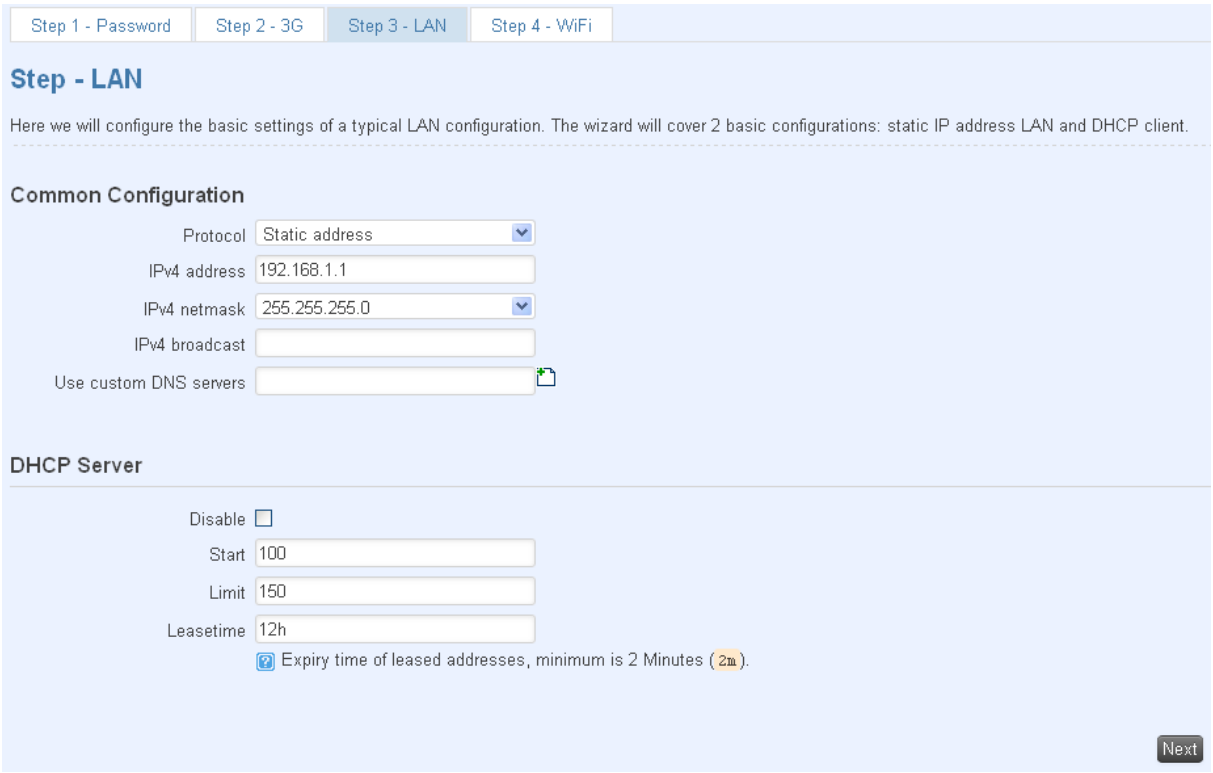
Nach dem ersten Login startet automatisch ein Einrichtungs-Assistent. Dieser kann über „Skip Wizard“ beendet werden. Wenn Sie ihn jedoch nutzen möchten, fordert Sie der Assistent auf, zuerst ein neues Passwort einzutragen und dieses zu bestätigen. Um zum nächsten Schritt zu gelangen, drücken Sie auf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



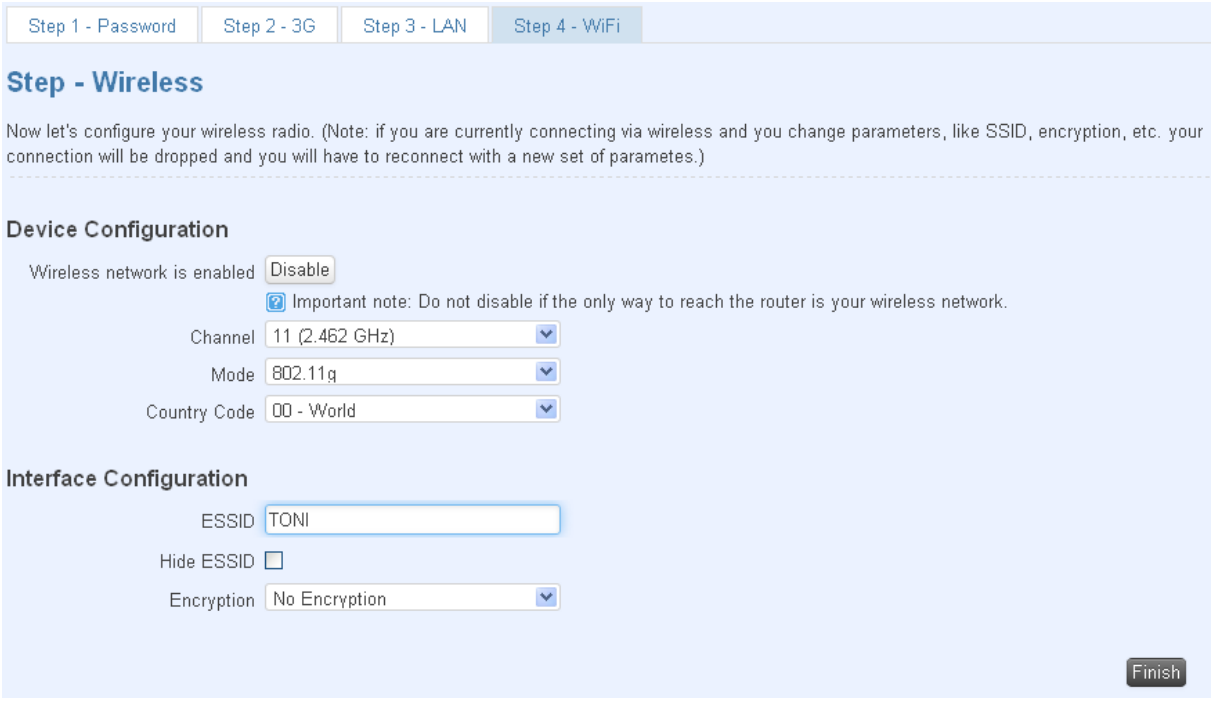
Im nächsten Schritt geben Sie bitte ihre 3G Einstellungen ein. Diese finden Sie in den Unterlagen ihres Netzanbieters. Wenn Sie damit fertig sind oder diesen Schritt überspringen möchten, klicken Sie auf „Next“.



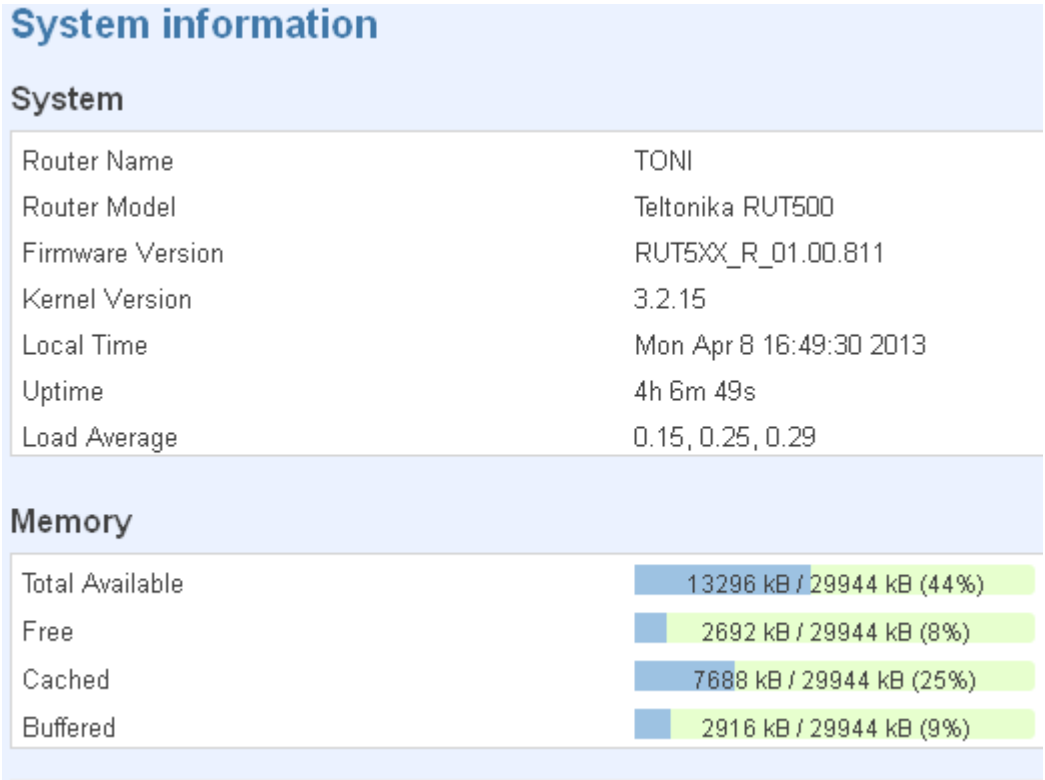
In Schritt 3 wird die LAN Konfiguration eingestellt. Hier kann auch der DHCP Server ausgeschaltet werden.



Im letzen Schritt wird das W-LAN eingestellt.



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.



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.

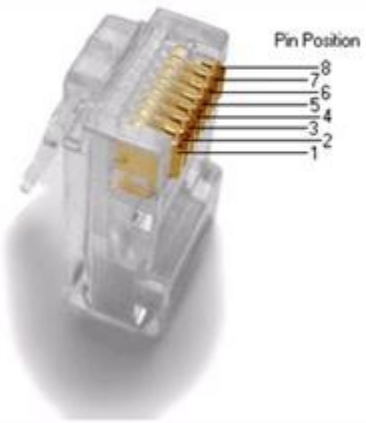
WAN	LAN		3G Backup Link
	Ethernet	Wi-Fi	
3G	√	√	x
Ethernet	√	√	√
Wi-Fi	√	x	√

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.

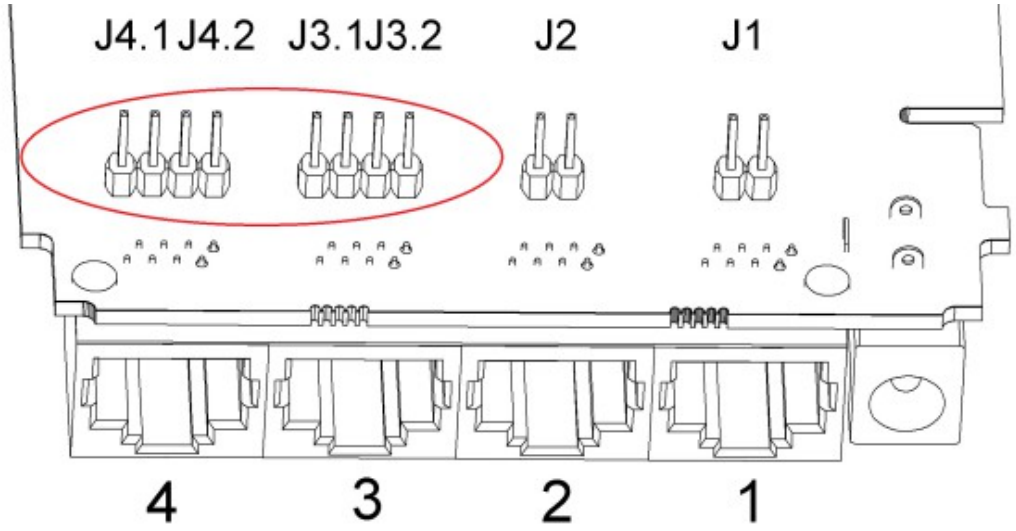
Benutzen Sie nur eine der Möglichkeiten.
Benutzen Sie nicht den Stromanschluss und einen Ethernetanschluss gleichzeitig zur Stromversorgung!
Benutzen Sie nicht die Anschlüsse LAN3 und WAN gleichzeitig zur Stromversorgung!
Die Pinbelegung für die Ethernet Ports lautet:

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

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

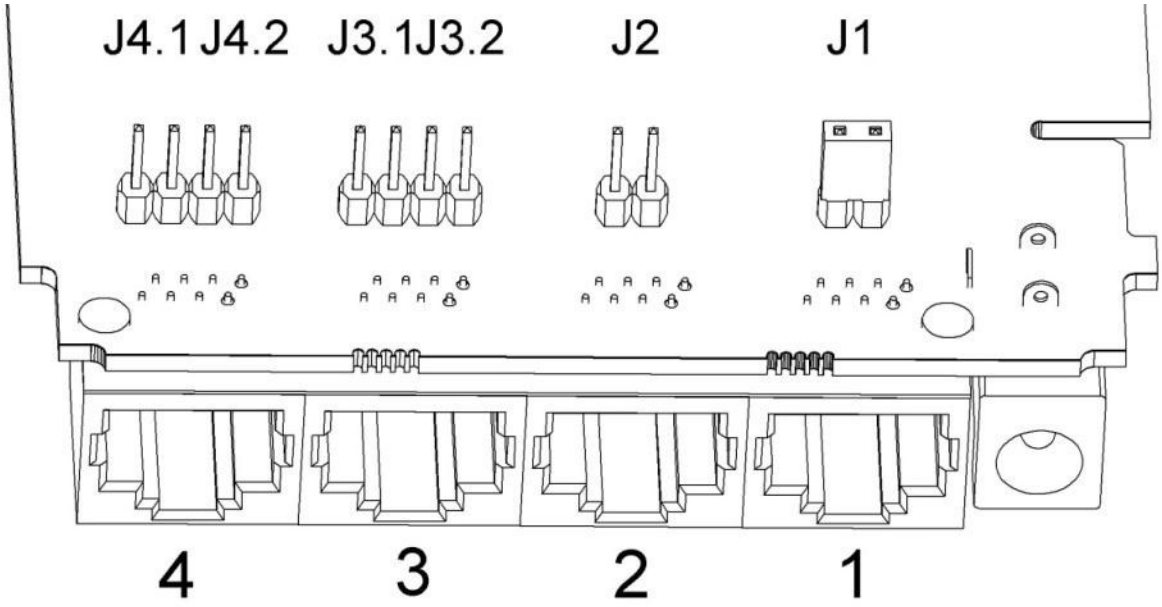
Wenn der TONI Router über die Anschlüsse LAN3 oder WAN mit Strom versorgt werden soll, müssen Sie die Jumper mit den Pins J4.1, J4.2 Bzw. J3.1, J3.2 (Siehe Bild) entfernen.
Vorsicht! Es ist ein Risiko für das Gerät, wenn die Jumper nicht richtig eingestellt sind!
Um die Jumper zu verändern, nehmen sie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



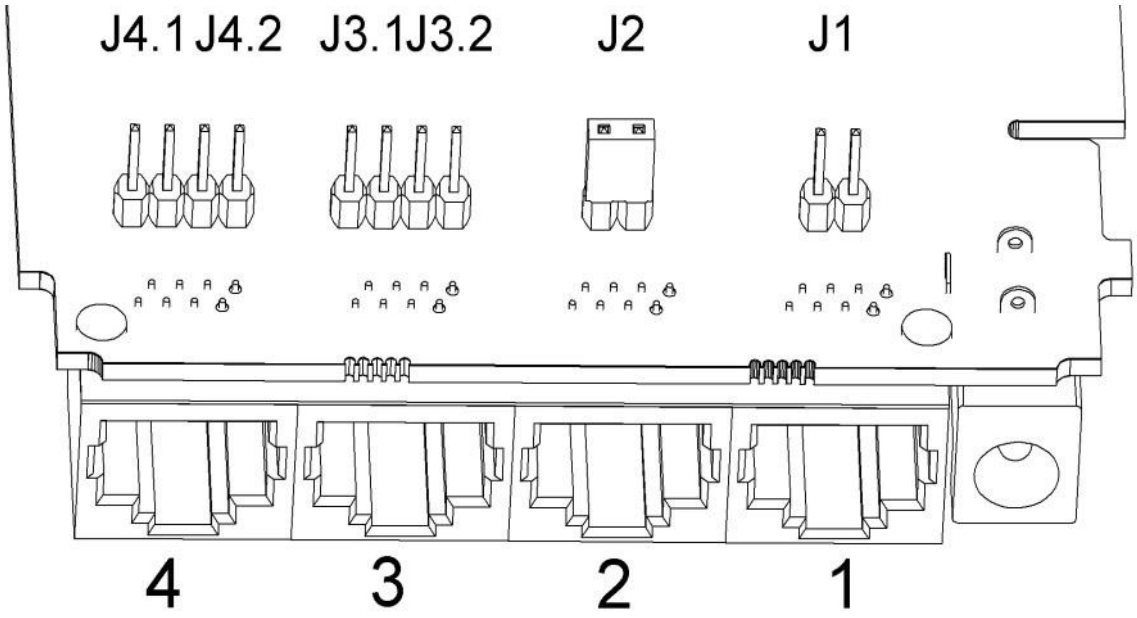
6 MVC300 Kamera

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.

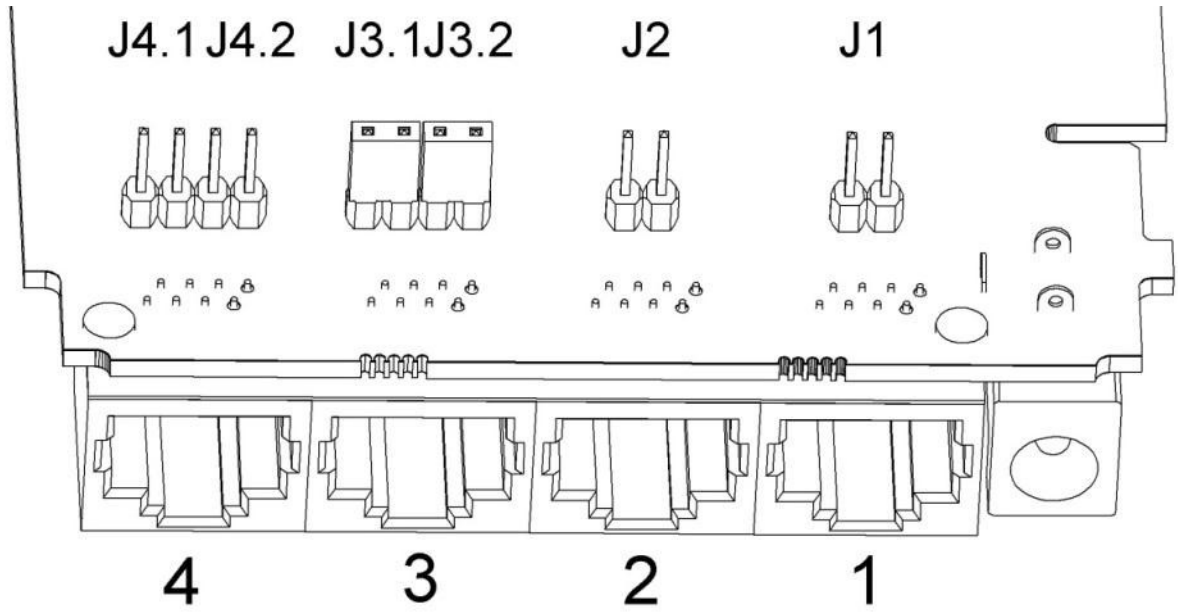


LAN Port 2 - bitte den Jumper auf J2 setzen.

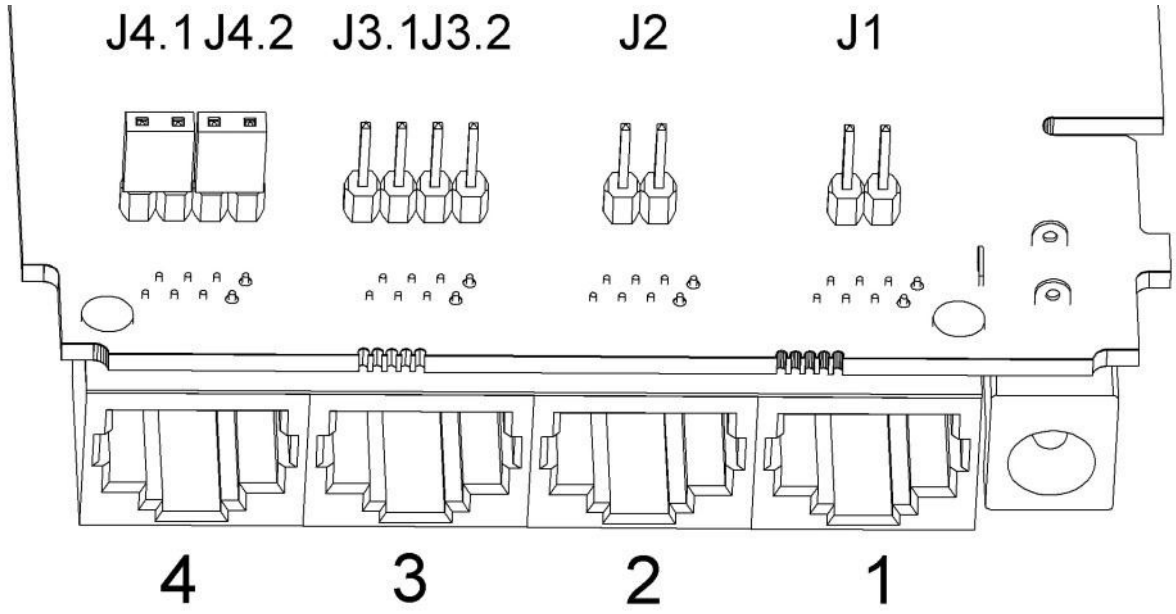


LAN Port 3 - bitte die Jumper auf J3.1 und J3.2 setzen.

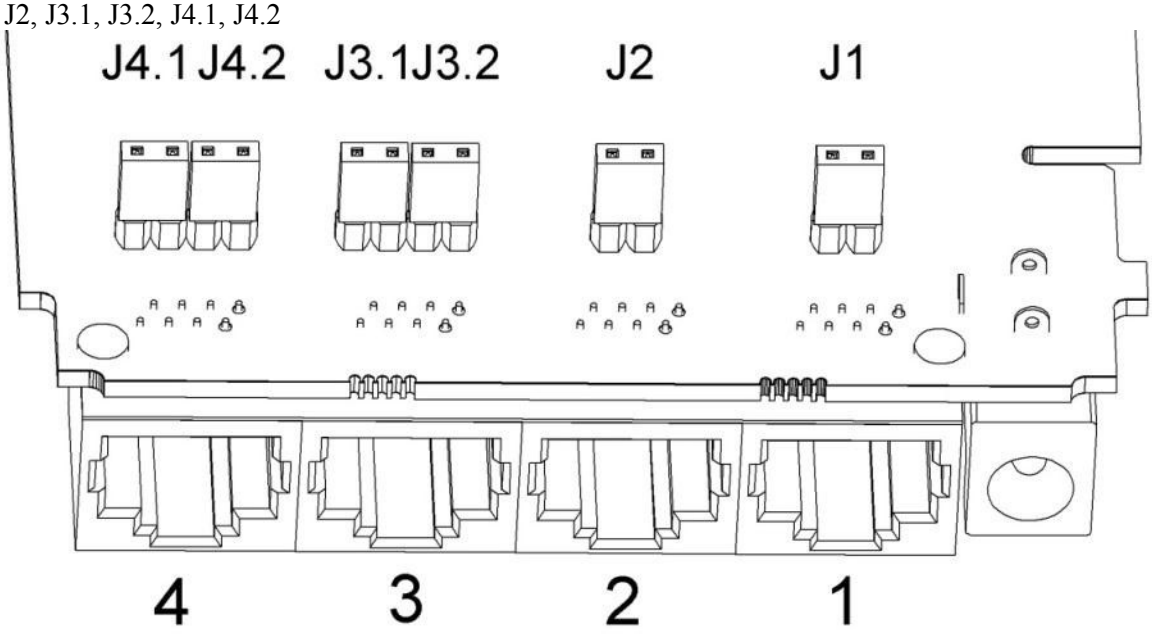
.



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

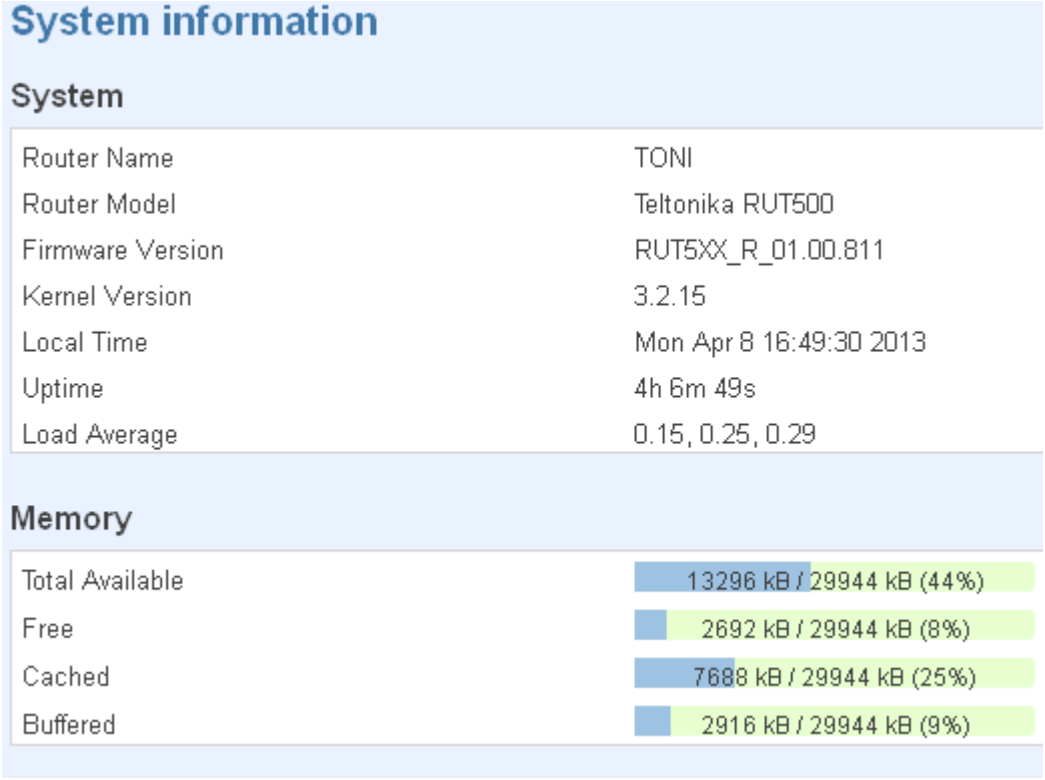
Der Router verfügt über eine Internetplattform, um Einstellungen vorzunehmen.

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:

	Feld Name	Beispieldaten	Erklärung
1	Router Name	TONI	Name des Router (Hostname des Routersystems)
2	Router Model	Teltonika RUT500	Router-Modell
3	Firmware Version	RUT5XX_T_00.00.436	Die Firmwareversion, die in den Router geladen ist. Es können neue Versionen von Ihnen aufgespielt werden wodurch sie mehr Extras und einen größeren Komfort erhalten.
4	Kernel Version	3.2.15	Die Linux Kernel Version, die auf dem Router 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

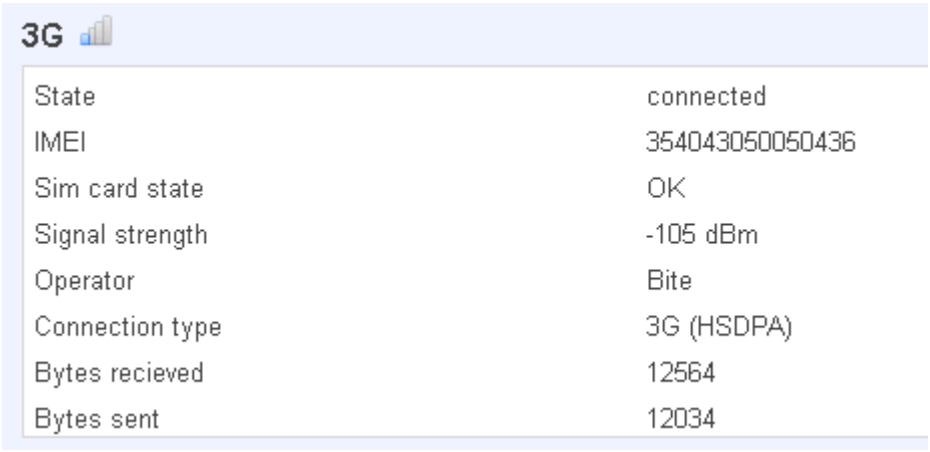
Memory:

	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

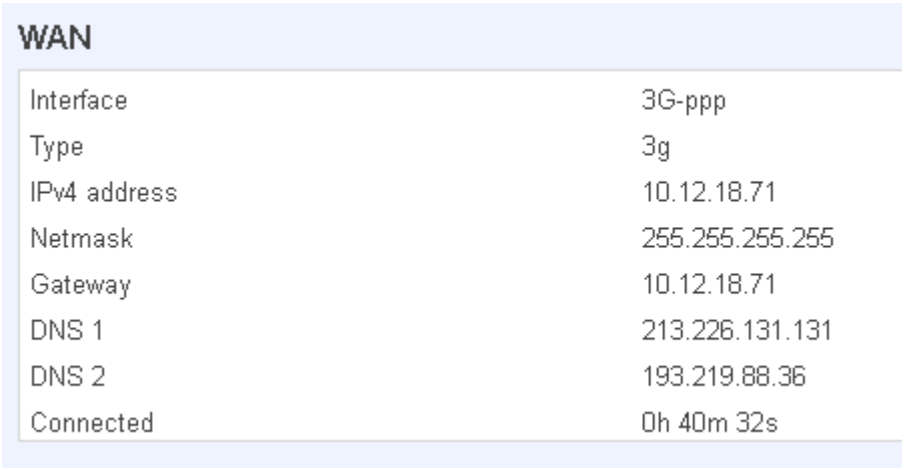
Hier finden sie Informationen zum aktuellen Netzwerk, Leistung und Adressen.

3G:



	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
5	Operator	Zeigt den verbundenen Mobilfunkanbieter
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:

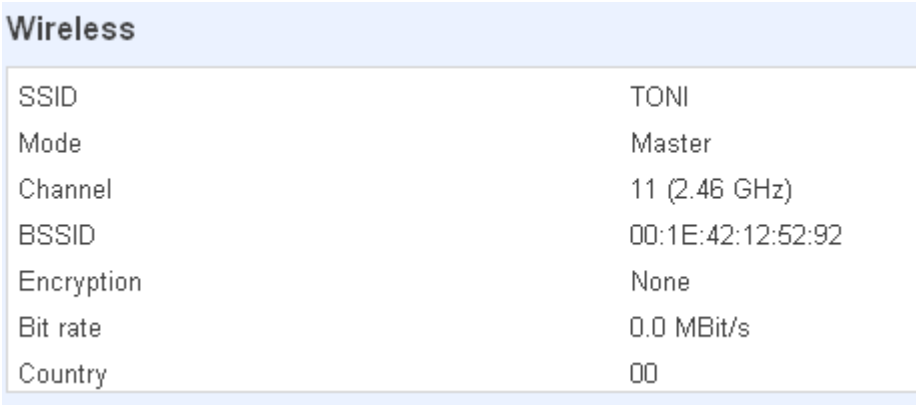


	Feld Name	**Beispiel Daten**	**Erklärung**
1	Interface	3G	Zeigt, wie der Router mit dem Internet verbunden ist. Über Ethernet, 3G oder W-LAN
2	Type	DHCP	Typ der Verbindung. DHCP oder PPPoE
3	IPv4 address	10.12.104.103	Die IP-Adresse, mit der der Router zum Internet verbunden ist.
4	Netmask	255.255.255.240	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:

	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

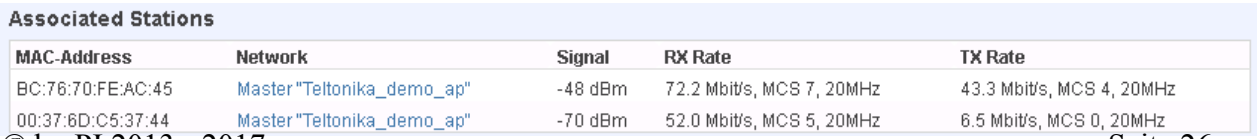
Wireless:
Es gibt zwei W-LAN Modi, AP oder Client. Um AP handelt es ich dann wenn der Router ein Access Point Entstehen lässt mit dem sich andere Geräte verbinden lassen. Um einen Client handelt es sich, wenn der Router mit einen anderen Access Point Kontakt aufnimmt.



	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.



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

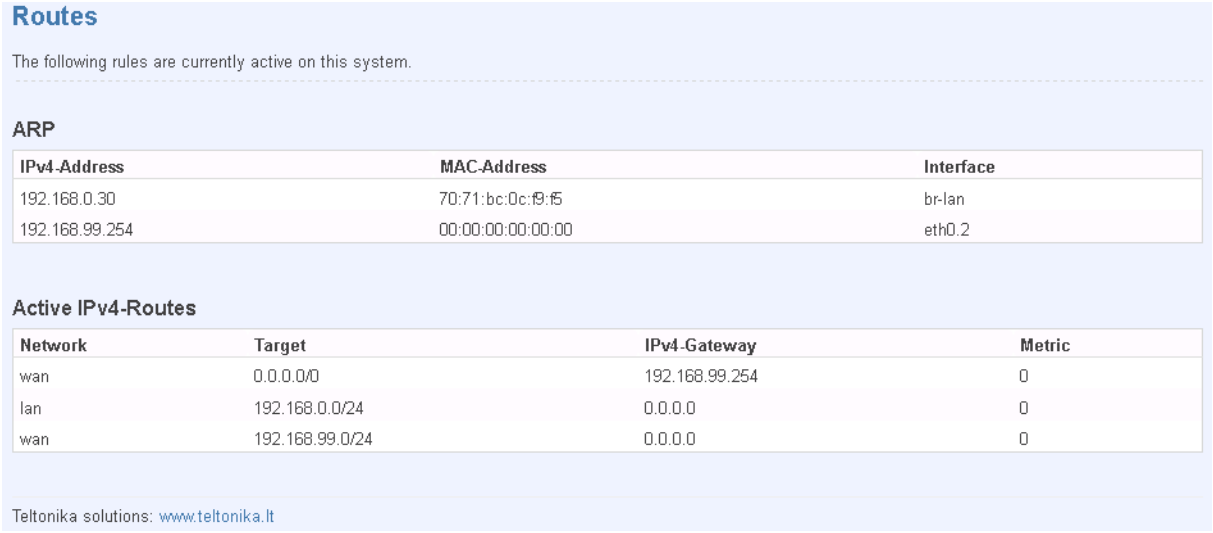
Backup WAN Status

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

Backup WAN Status

WAN: [Wired] NOT READY **Backup WAN: [3G]** 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	0.0.0.0/0	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.teltonika.lt

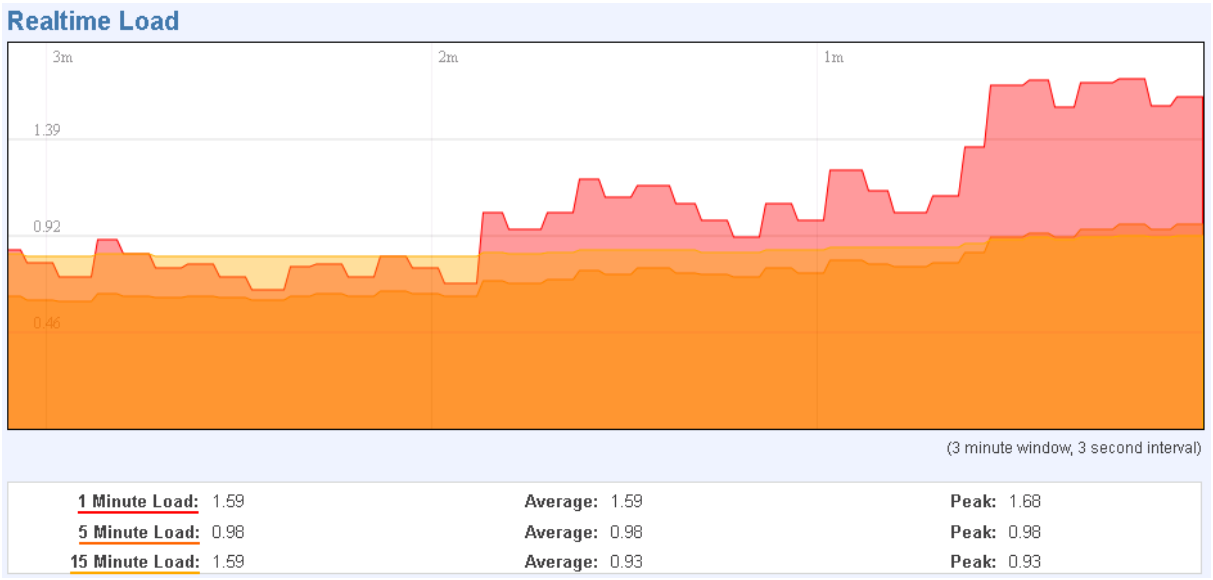
ARP
Diese Liste zeigt die Macadresse aller Geräte die jemals an den Router angeschlossen waren.

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.

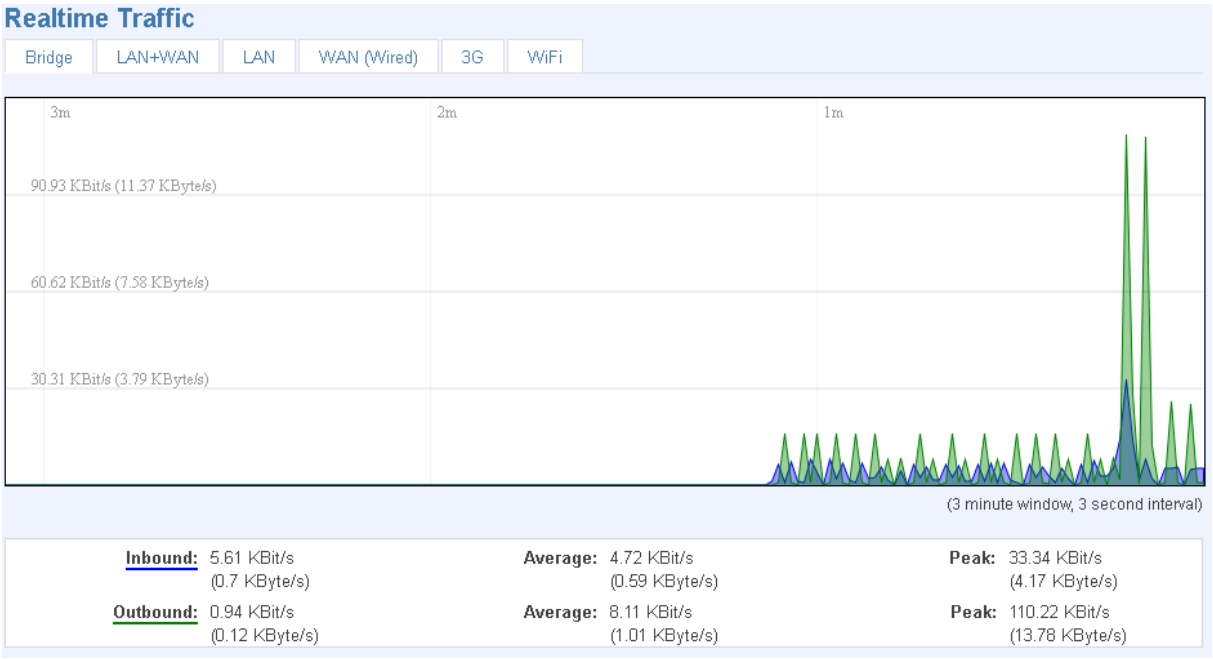
Load:



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

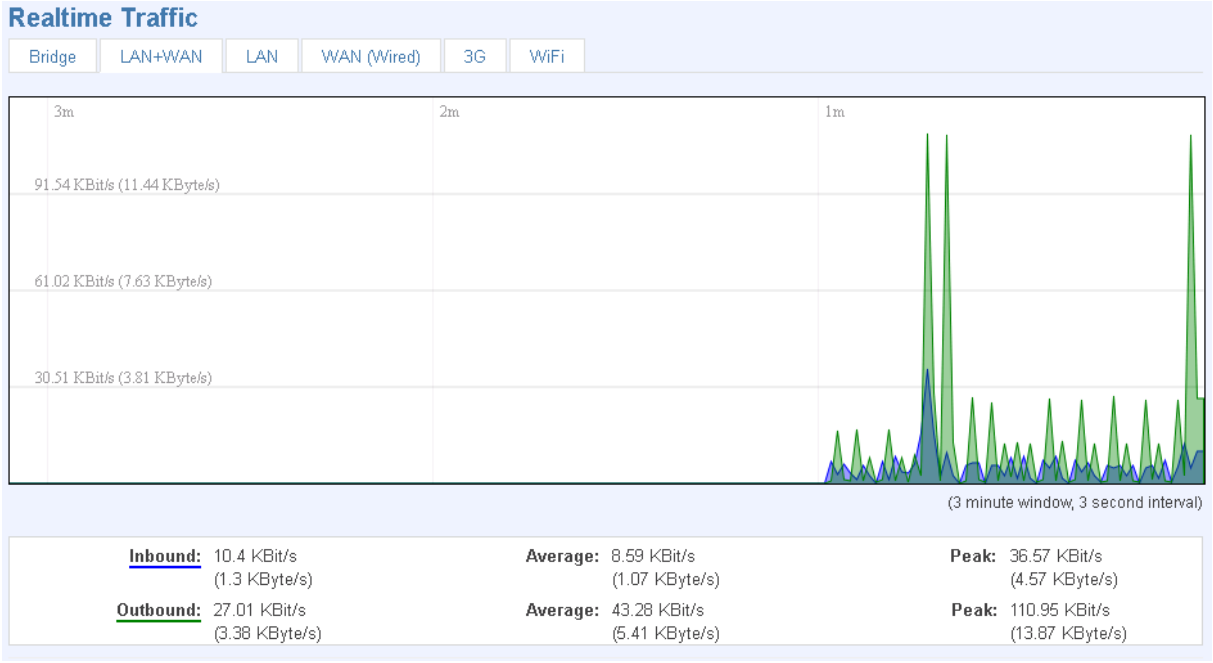
1 Minute Load	Rot
5 Minute Load	Orange
15 Minute Load	Gelb

Traffic, Bridge:



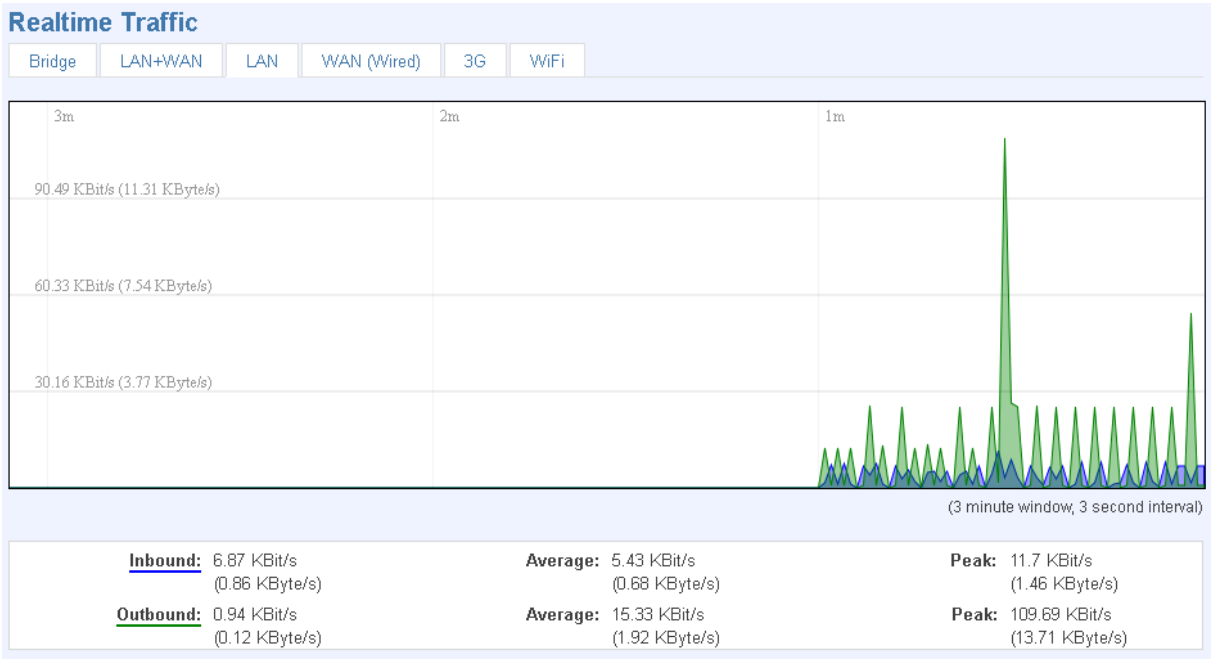
Kommunikations-Grafik von Ethernet LAN und W-LAN

Traffic, LAN+WAN:



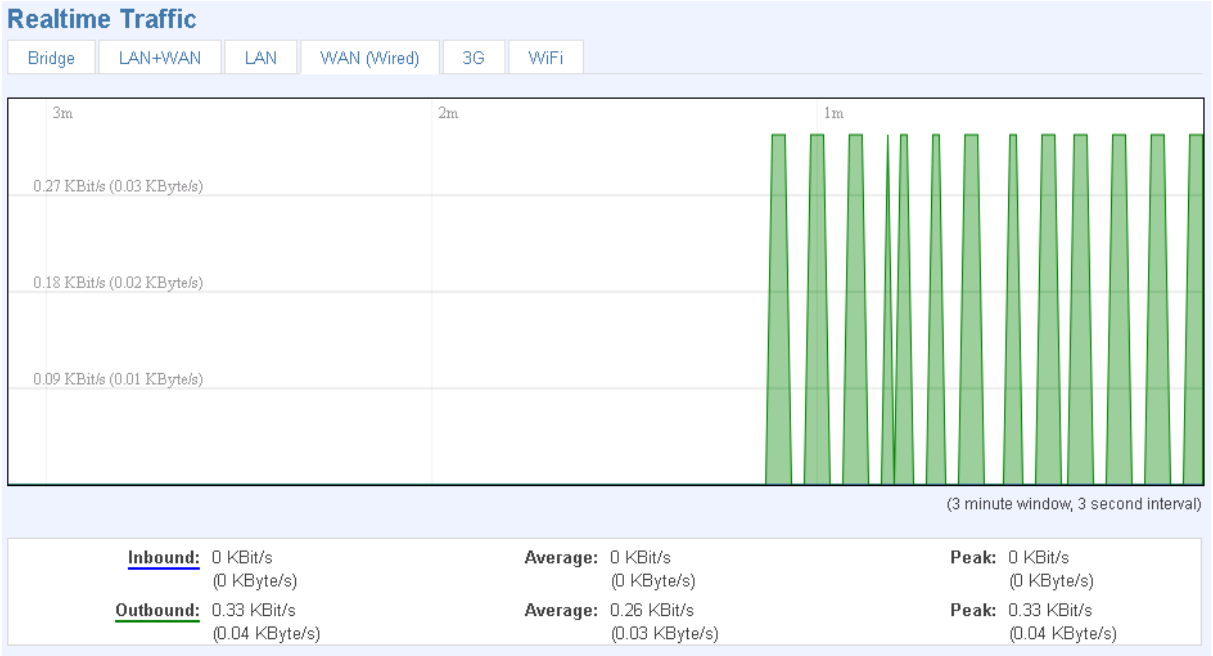
Diese Grafik zeigt alles, was über WAN und LAN geht.

Traffic, LAN:



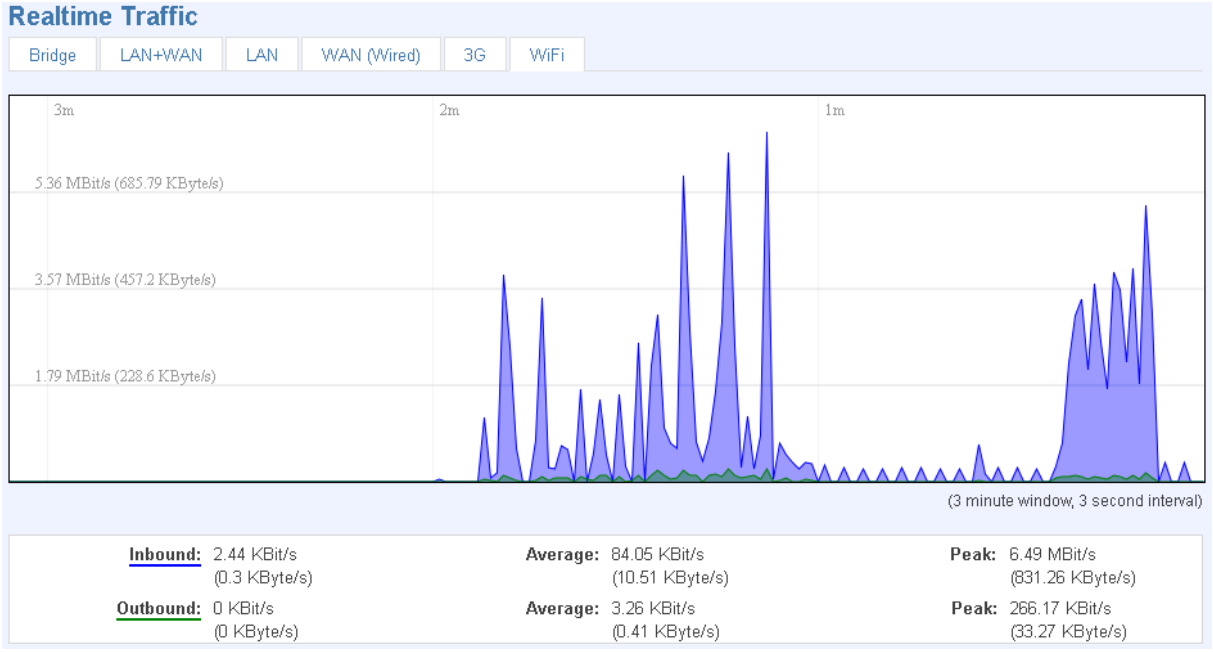
Grafik zeigt Traffic von LAN Verbindung.

Traffic, WAN:



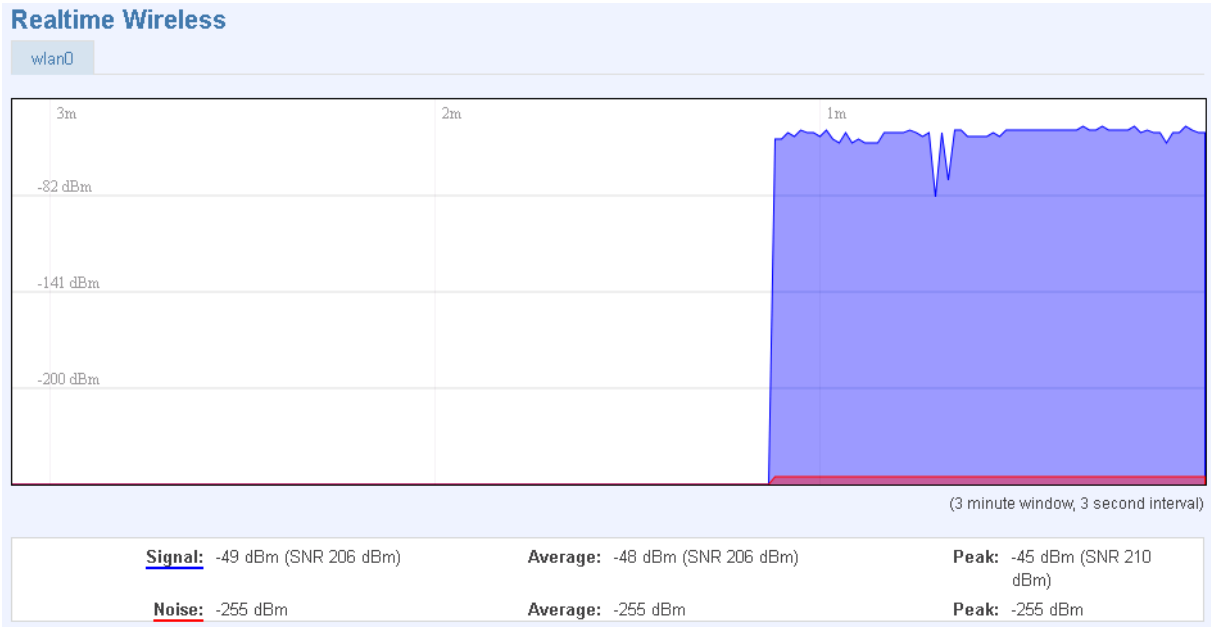
Grafik ist nur bei aktiver Verbindung sichtbar und zeigt die Datenmengen an.

Traffic, W-LAN:

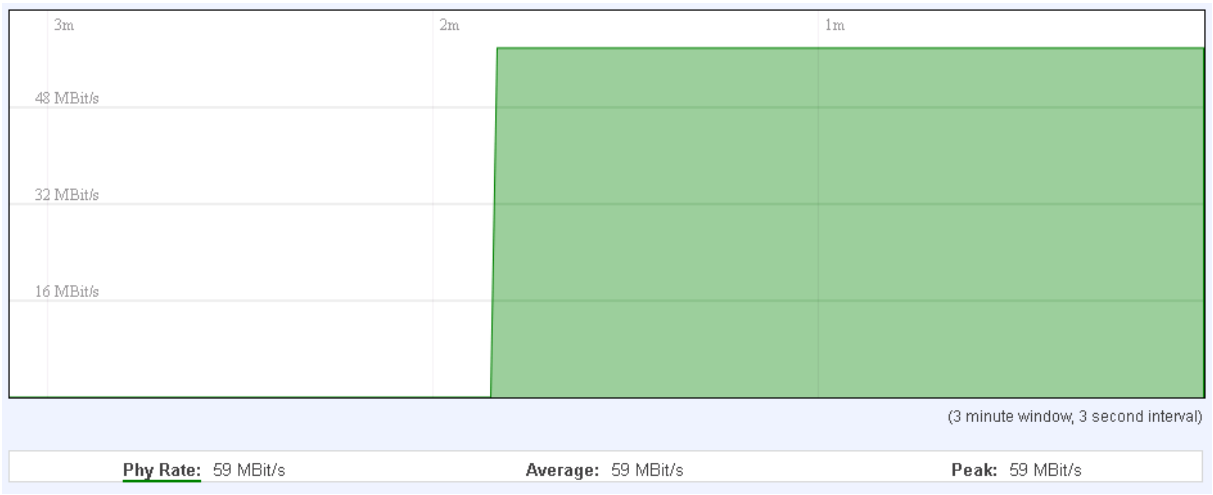


Diese Grafik zeigt den Traffic über W-LAN an

Wireless, WiFi:

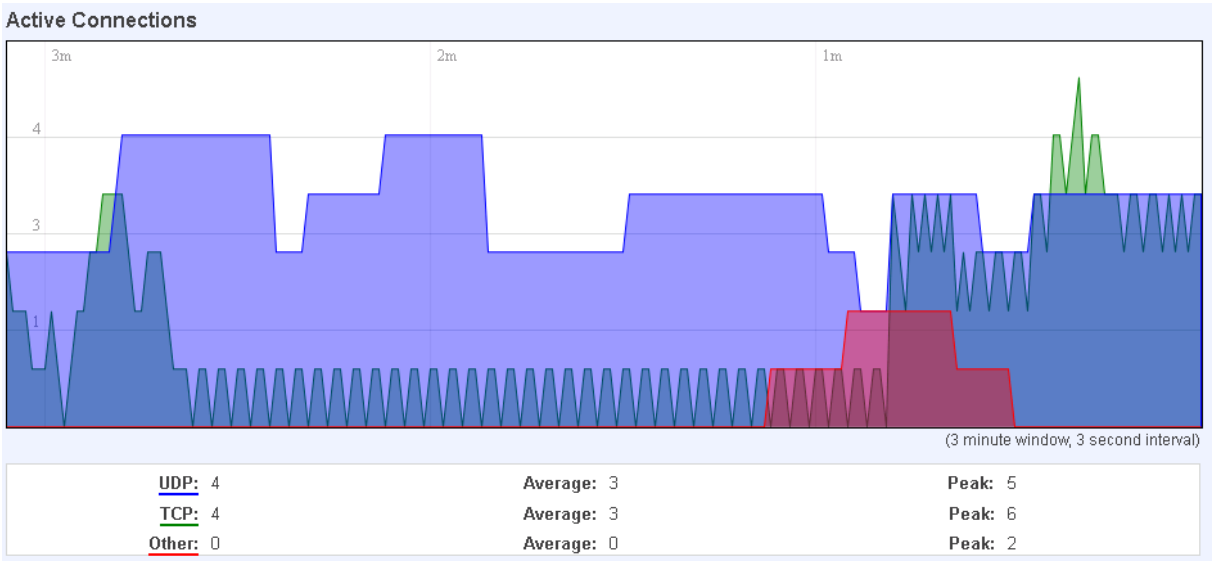


Die Grafik zeigt an, wie stark das Signal ist.



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.

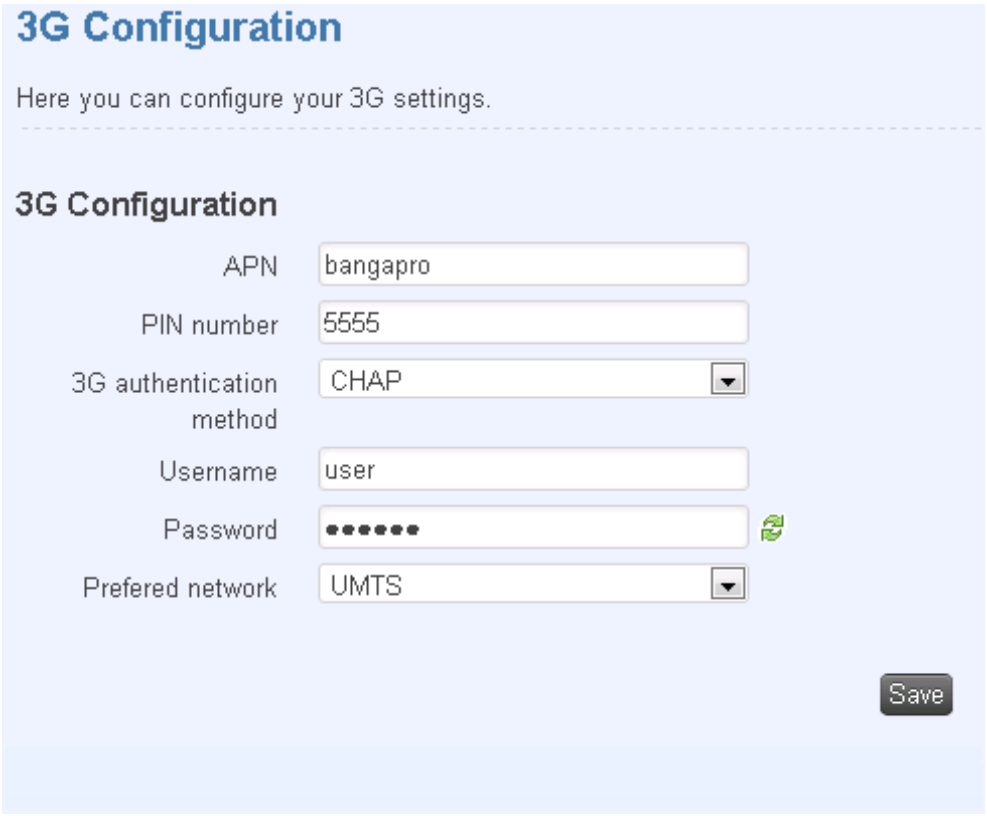
Network	Protocol	Source	Destination	Transfer
IPV4	TCP	192.168.0.156:37706	192.168.99.30:3389	613.24 KB (8338 Pkts.)
IPV4	UDP	192.168.0.19:137	192.168.0.255:137	7.24 KB (84 Pkts.)
IPV4	UDP	192.168.0.19:138	192.168.0.255:138	5.20 KB (24 Pkts.)
IPV4	TCP	192.168.0.156:52547	173.194.78.139:80	3.30 KB (11 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.

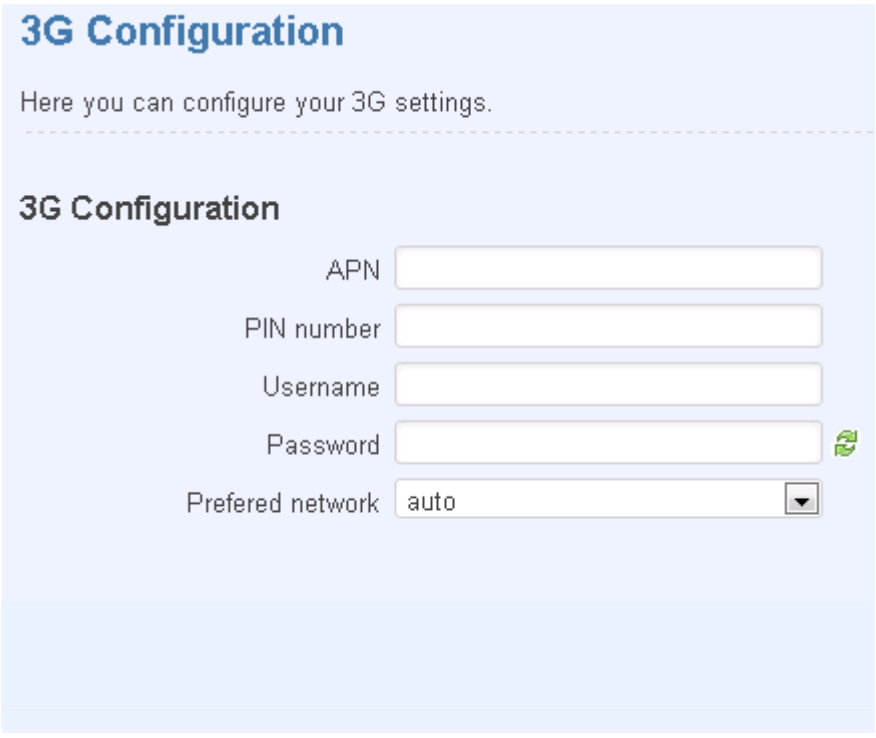
7.2 Network

7.2.1 3G

Hier können Sie Einstellungen an ihrer 3G Verbindung einstellen.



Alternativmodell:



Die Konfiguration ist simpel:

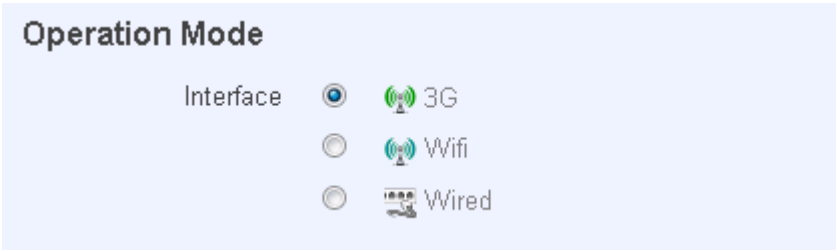
	Feld Name	Beispiel Daten	Erklärung
1	APN	“bangapro”	**A**ccess **P**oint **N**ame des Mobilfunkanbieters
2	PIN Number	“5555”	Ihr persönlicher Pin der SIM-Karte
3	3G authentication method	CHAP, PAP oder none	Aufenthalts Autorisierungs-Methode (Diese Option ist beim Alternativmodell nicht vorhanden.)
4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

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

7.2.2 WAN

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

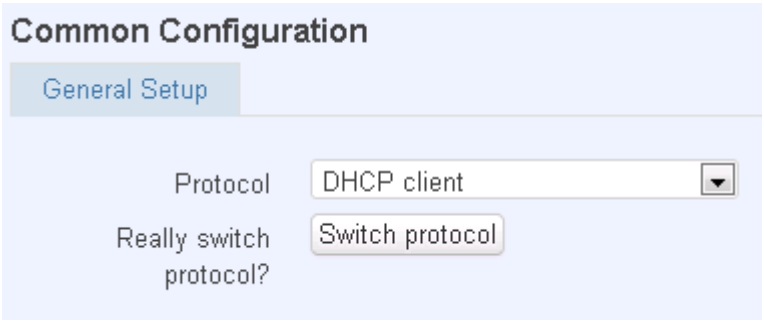
Operation Mode:



	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.

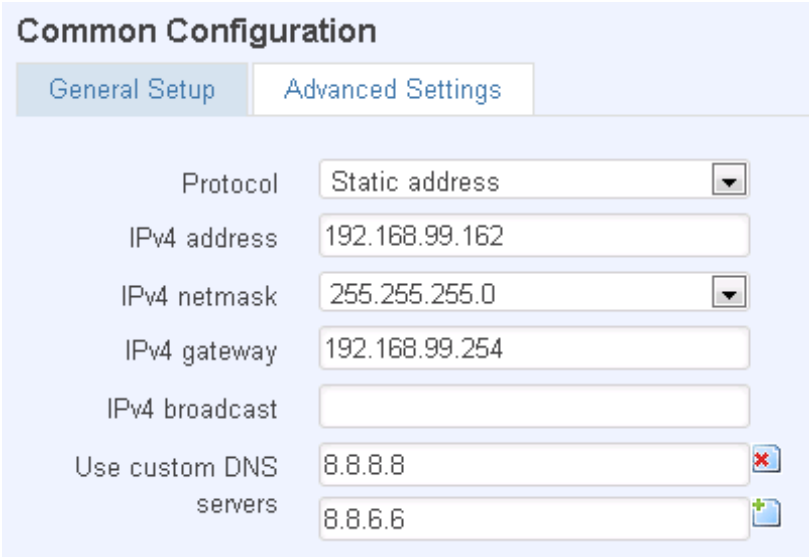
Bitte beachten:
Bei einer Verbindung ins Internet über das 3G-Netz kann im Gerät keine MTU-size geändert werden. Diese steht fest auf 1500.

Normalkonfiguration:
Konfigurieren Sie ihre TCP/IP-Einstellungen.



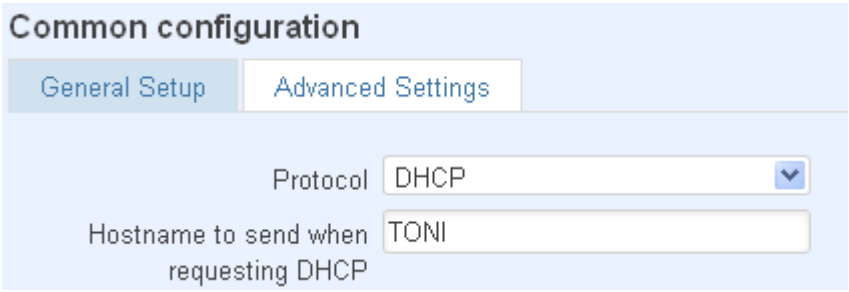
Sie können zwischen Static, DHCP und PPPoE Protokoll wählen.

Static Address:



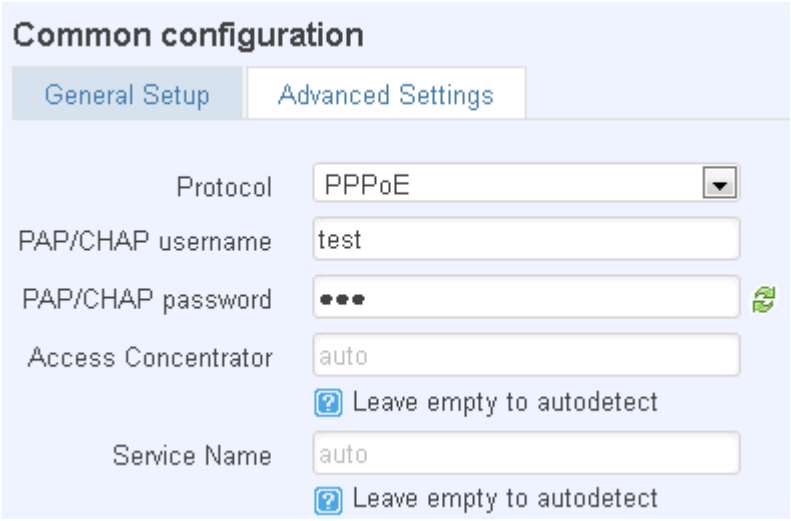
	Feld Name	**Beispiel Daten**	**Beschreibung**
1	IPv4 address	192.168.99.162	Ihre Router-Adresse ins WAN Netzwerk
2	IPv4 netmask	255.255.255.0	Ihre Netzmaske im WAN Netzwerk
3	IPv4 gateway	192.168.99.254	Adresse, die der Router sendet, wenn Traffic gesendet wird.
4	IPv4 broadcast	192.168.99.255	Broadcastadresse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

DHCP:



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:

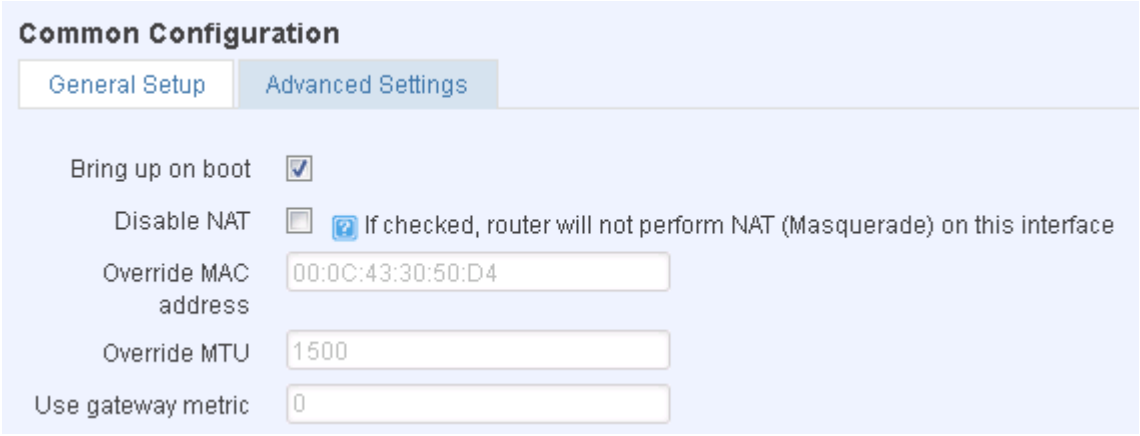


	Feld Name	Beispiel Daten	Beschreibung
1	PAP/CHAP username	test	Ihr Passwort und Benutzername das Ihnen vom Internetbetreiber mitgeteilt wurde**.**
2	PAP/CHAP password	your_password	
3	Access Concentrator	isp	Spezifischer Name für Accessconcentrator. Lassen Sie diese Einstellung auf Auto.
4	Service Name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

Advanced Settings

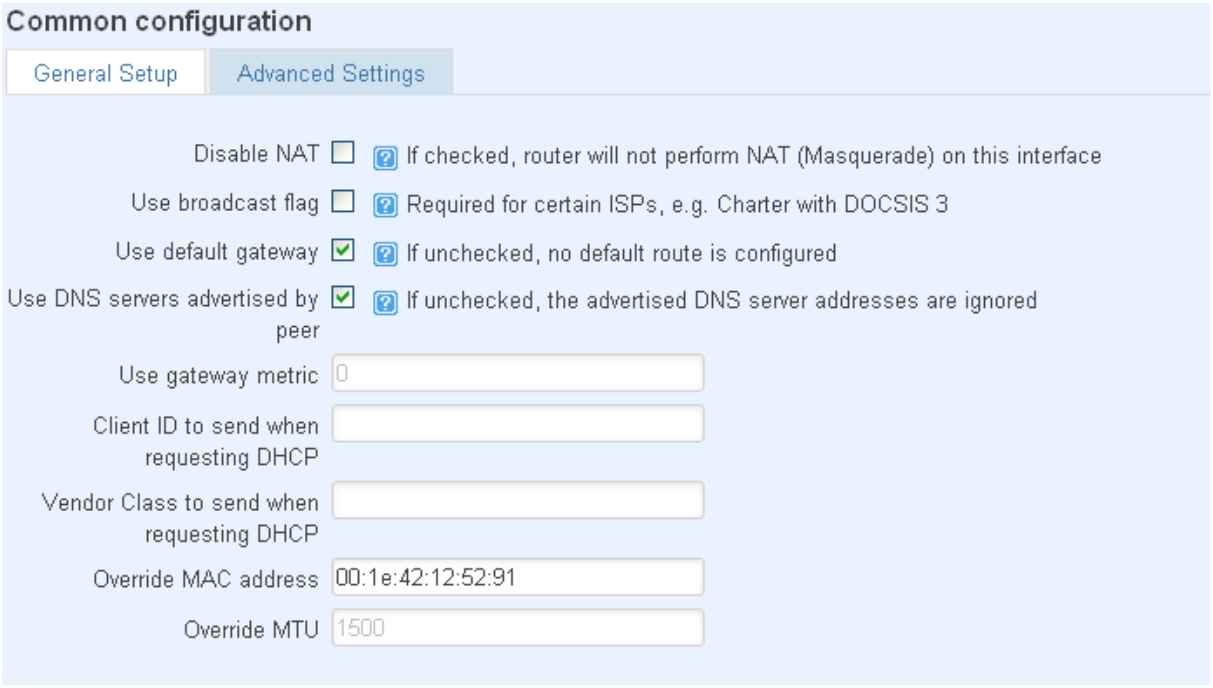
Spezielle Einstellungen für alle Protokolle. Dies sollte nur von Profis umgestellt werden.

Static:

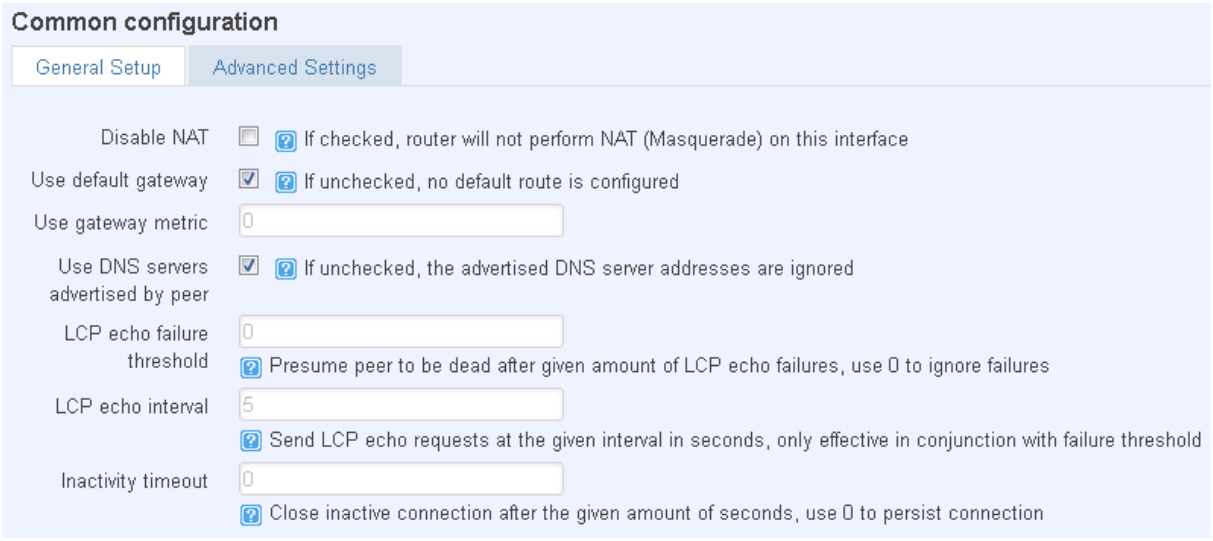


	Feld Name	Beispiel Daten	Beschreibung
1	Bring up on boot	On	Dient dazu, beim Starten des Routers eine Verbindung zum Router aufzubauen. Wenn die Option deaktiviert ist kann keine WAN Verbindung mehr aufgebaut werden.
2	Disable NAT	On/Off	Toggle NAT an und aus
3	Override MAC address	00:0C:43:30:50:38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

DHCP:

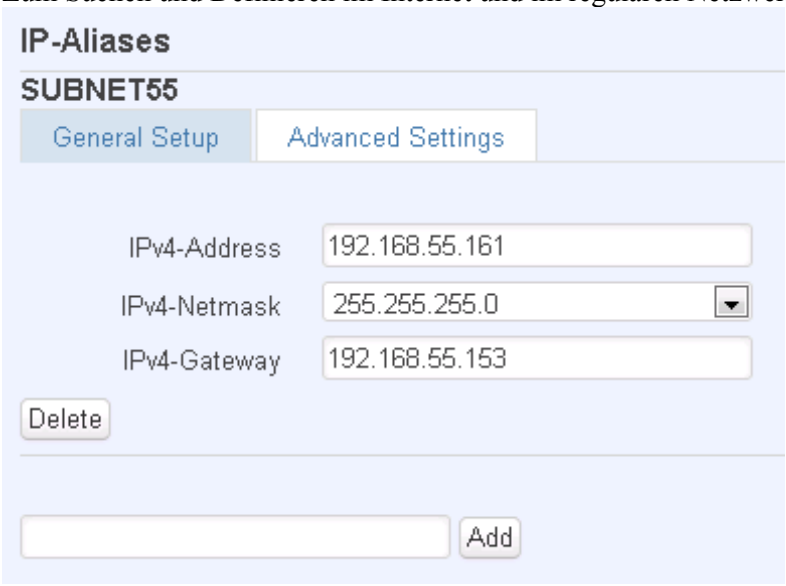


PPPoE:

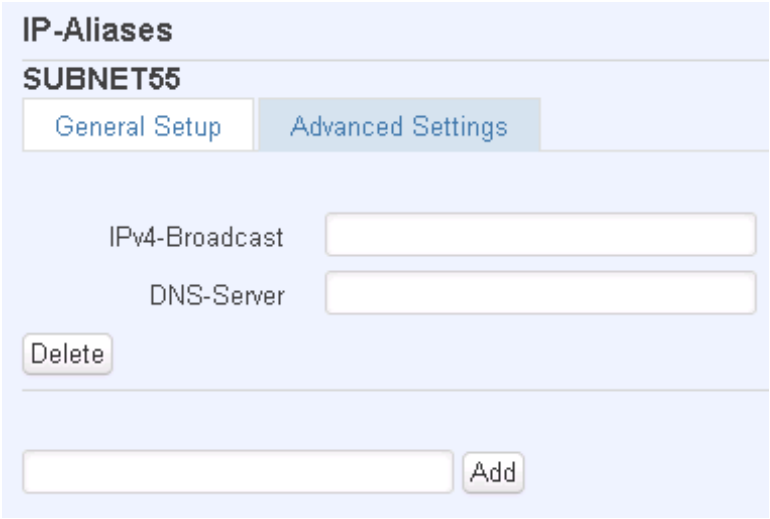


IP Aliases

Zum Suchen und Definieren im Internet und im regulären Netzwerk.



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.



Sie können optional eine Broadcast Adresse und DNS Server definieren.

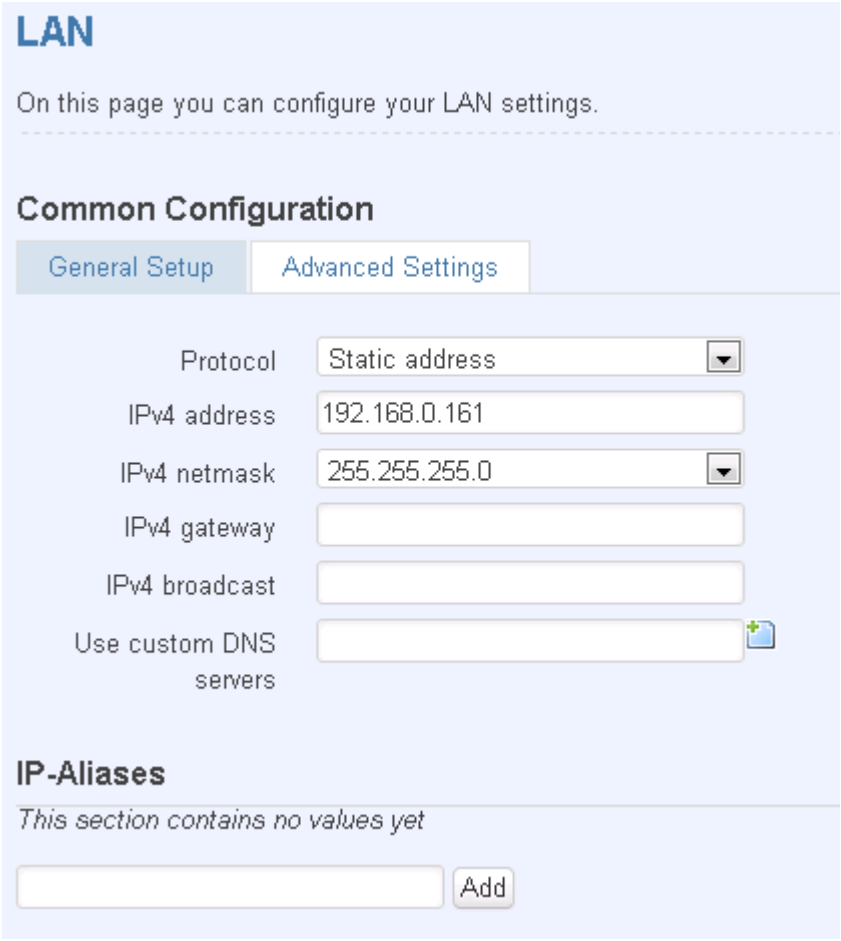
Wie funktioniert ein WiFi WAN Setup?

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!

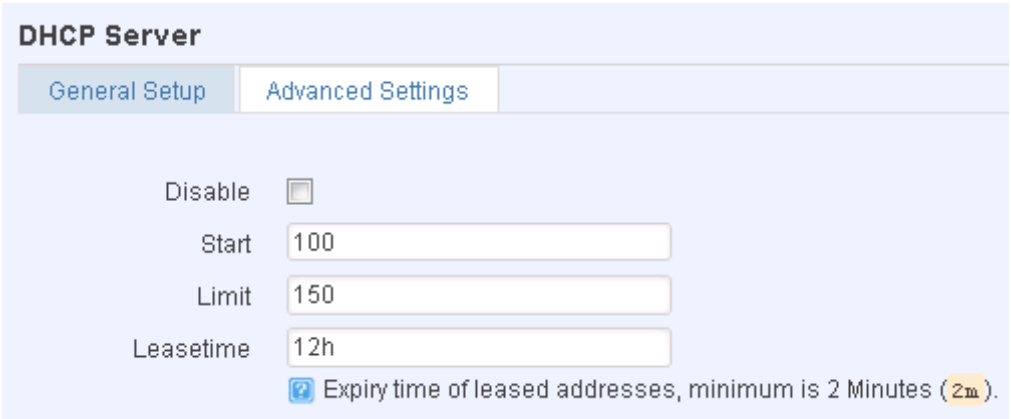
7.2.3 LAN

Diese Seite ist zur Konfiguration eines LAN Netzwerkes.



DHCP Server:

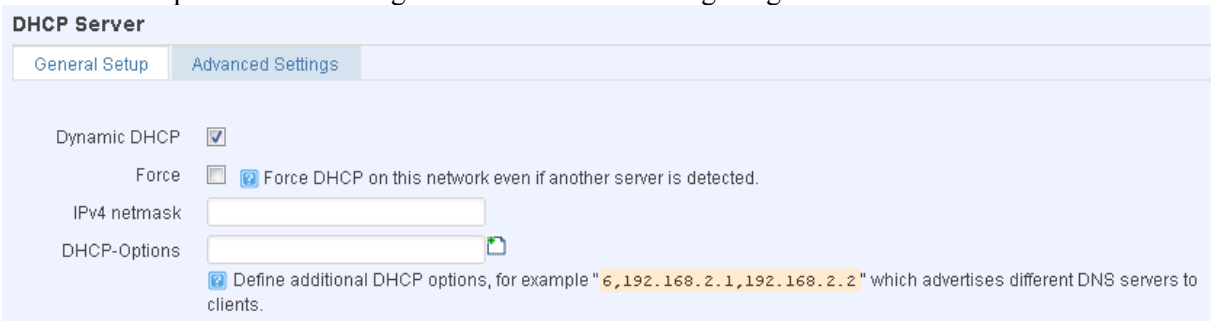
Der DHCP Server ist beim ersten Start so konfiguriert, dass der Router funktioniert.
Wenn Sie ein Gerät anschließen, identifiziert es sich automatisch und bekommt die IP-Adresse vom Router zugewiesen. Es ist dann verbunden.



	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.

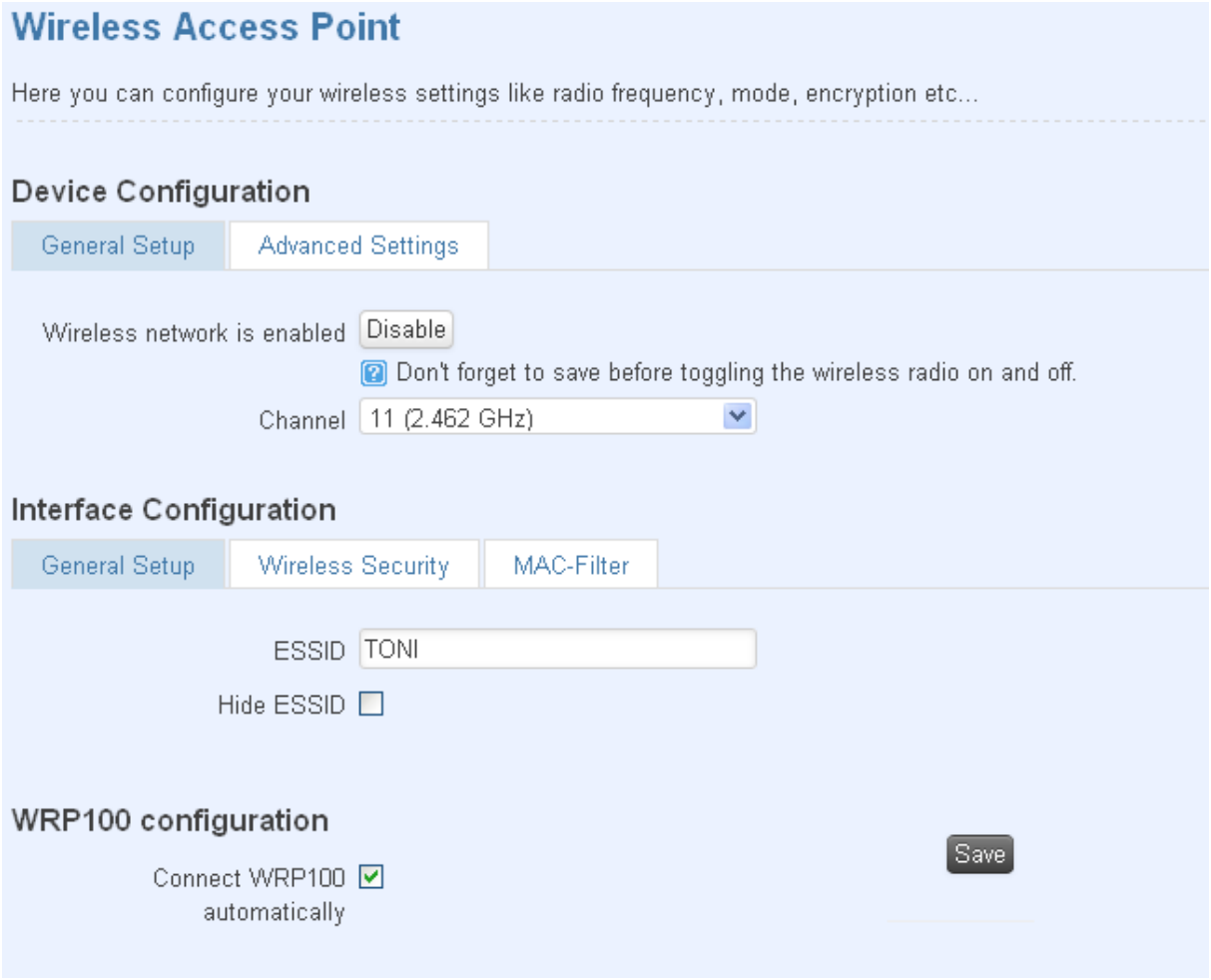


	Feld Name	Beispiel Daten	Beschreibung
1	Dynamic DHCP	Checked/Unchecked	Dynamic DHCP aktivieren und deaktivieren.
2	Force	Checked/Unchecked	Forces DHCP ist da, falls sich noch ein anderer DHCP Server im Netzwerk befindet bzw. einer gefunden wird.
3	IPv4 netmask	255.255.255.0	Hier können sie die LAN Netmaske 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

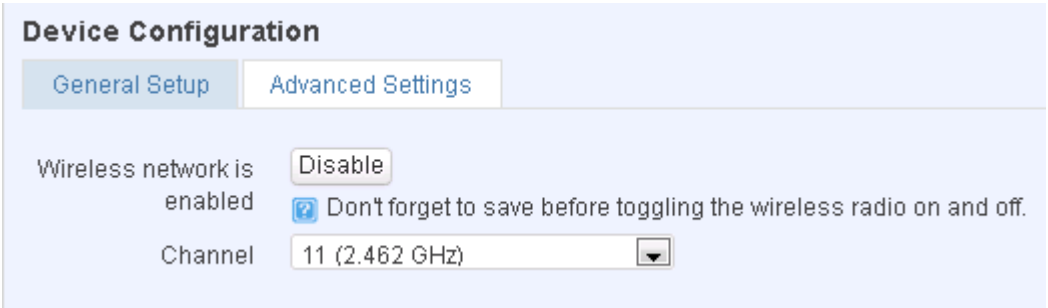
Auf dieser Seite können die W-LAN Einstellungen geändert werden. Auch Einstellung zum WAN über WiFi und Access Points finden Sie hier.

Access Point:



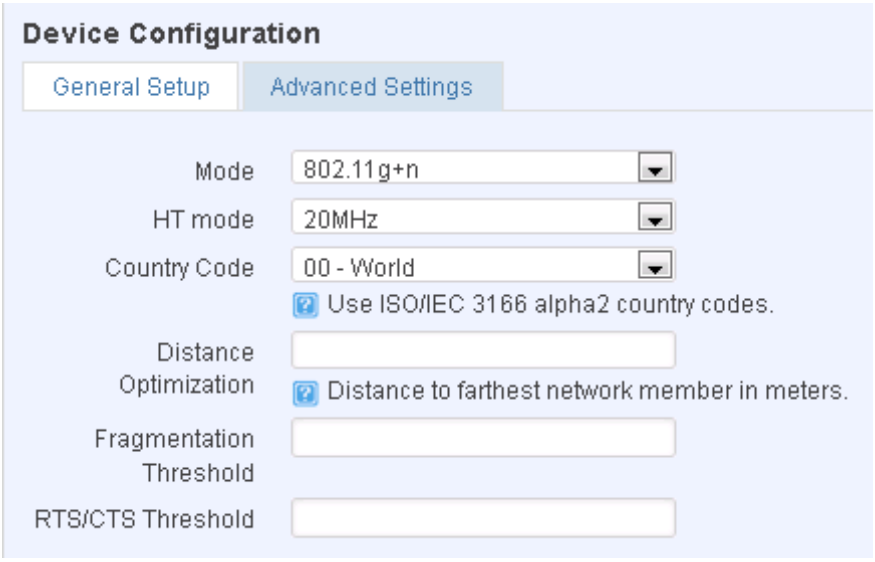
Hier kann man eine Übersicht der W-LAN Einstellungen sehen. Hier können Parameter geändert und auch das gesamte W-LAN Netzwerk abgeschaltet werden.

Device, General:



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.

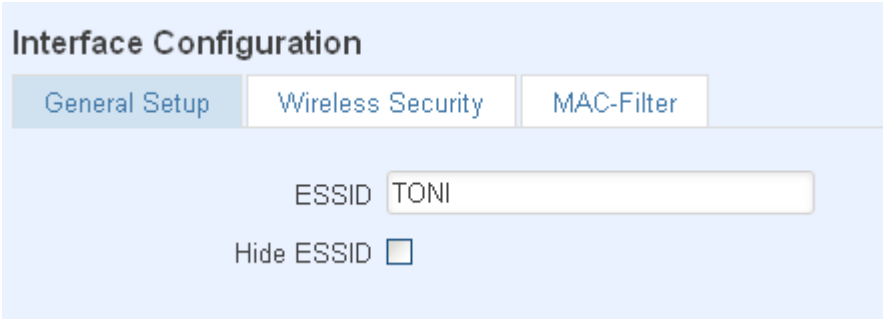
Device, Advanced:



Hier können noch mehr Parameter konfiguriert werden.

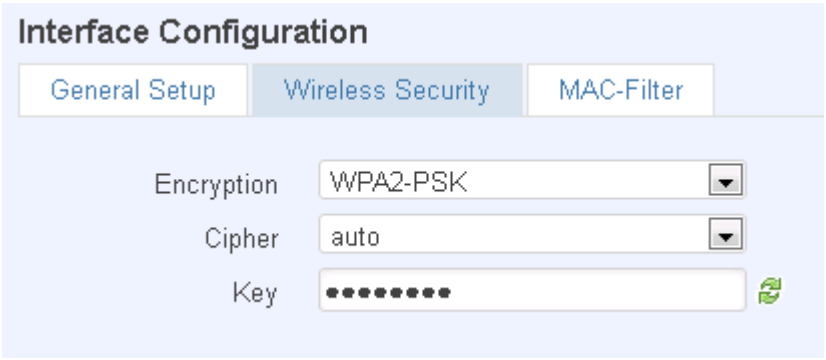
	Feld Name	**Beispiel Daten**	**Beschreibung**
1	Mode	Auto, b, g, g+n	Sicherheitsoptionen
2	Country Code	Any ISO/IEC 3166 alpha2 country Code	Auswählen einer Region (Land)
3	Distance Optimization	100	Um einzustellen, mit welcher Stärke das W-LAN Netzwerk senden soll (in Metern)
4	Frag. Threshold	2346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

Interface, General:



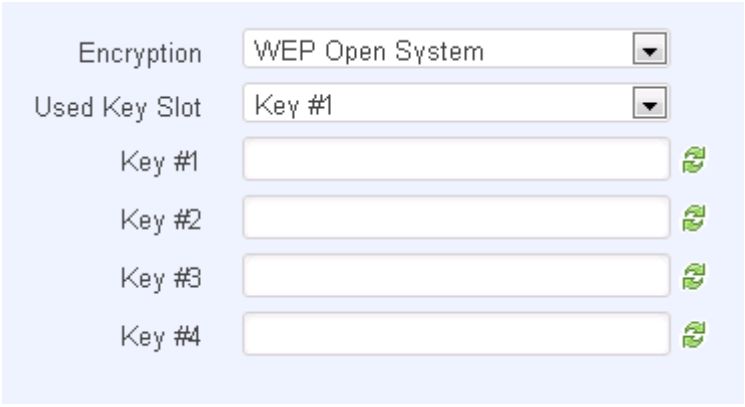
ESSID – ist der W-LAN-Intendifikationsstring.

Interface, Security:



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

WEB:



Geben sie die gewünschten Keys ein.

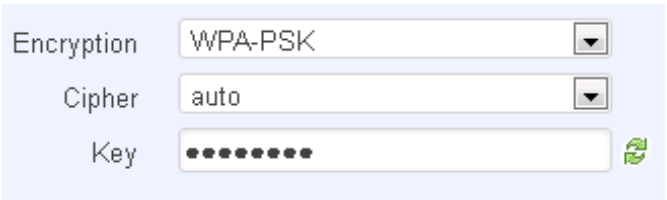
Achtung:

Die Keys dürfen

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

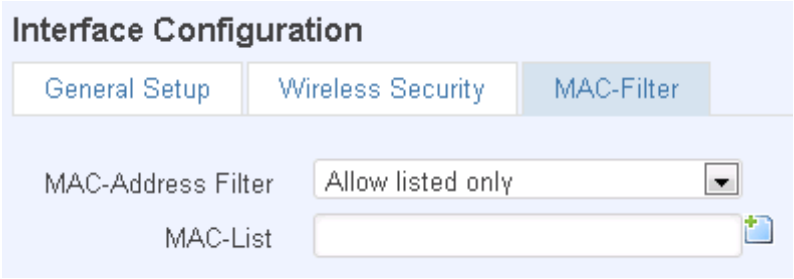
haben.

WPA:



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

Interface, Mac-Filter:



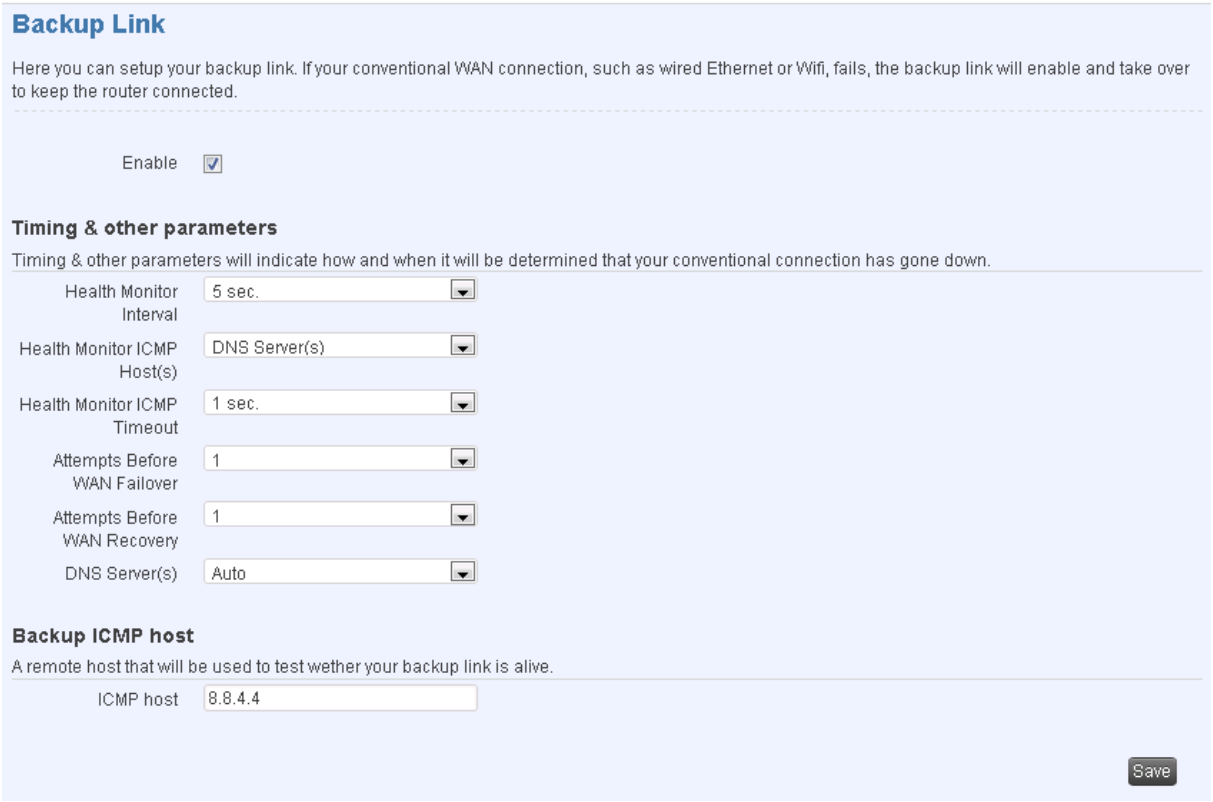
Im MAC Filter können Sie Mac Adressen eingeben, die sich mit dem Netzwerk verbinden dürfen. Neue Geräte müssen erst eingetragen werden, bevor sie sich verbinden können.

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.



	Feld Name	Auswählbare Daten	Beschreibung
1	Health Monitor Intervall	Dsb/5/10/20/30/60/120 Sekunden	Der Intervall, in dem die Verbindung geprüft wird.
2	Health Monitor ICMP HOST	Dsb/DNS/WAN GW/Custom	Wie soll der Router testen, ob er mit dem Internet verbunden ist.
3	Health Monitor ICMP Timeout	½/3/4/5/10 Seconds	Wie lange soll gewartet werden, bis die alternative Verbindung (3G) benutzt wird.
4	Attempts Before WAN Failover	1/3/5/10/15/20	Wie viele Verbindungsversuche sollen unternommen werden, bis die alternative Verbindung (3G) in Kraft tritt.
5	Attempts Before WAN Recovery	1/3/5/10/15/20	Wie oft soll kontrolliert werden, ob die 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.

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:

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

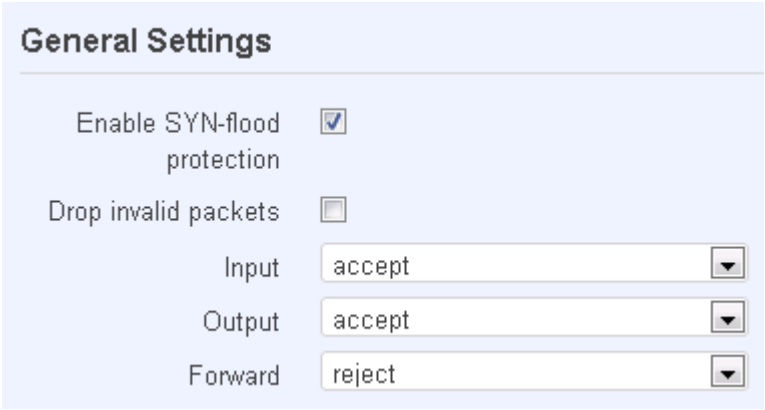
Wenn nun die Verbindung zum W-LAN wieder hergestellt werden kann sieht es so aus:

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

7.2.6 Firewall

General Settings:

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



	Feld Name	Auswählbare Daten	Beschreibung
1	Enable SYN-flood protection	Checked/Unchecked	Wenn diese Option aktiviert ist, ist der Router besser gegen SYN-flood Attacken geschützt.
2	Drop Invalid packets	Checked/Unchecked	“Drop” sind Dateien, die ins Internet 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:

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.

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 address	IPv4 Adresse von einem Gerät aus Ihrem LAN	Die IP-Adresse des Geräts, dass im Netz der 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 + additional rules	Aktion die die Firewall ausführen soll. 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.

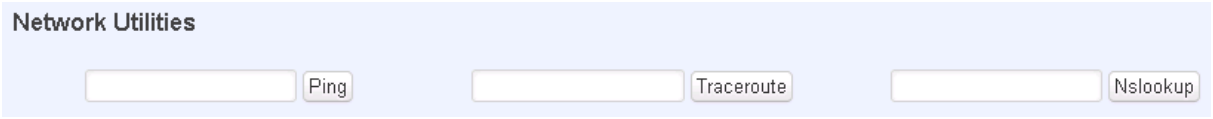
	Feld Name	Beispiel Daten	Beschreibung
1	Interface	Lan/wan	Netwerkverbindung, die freigeben werden soll.
2	Target	IPv4 address	Netzwerk, das freigegeben werden soll.
3	IPv4-Netmask	IPv4 mask	Netzmaske, die vom Gerät benutzt wird.
4	IPv4-Gateway	IPv4 address	IP-Adresse des Geräts, das freigegeben wird.
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.



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.

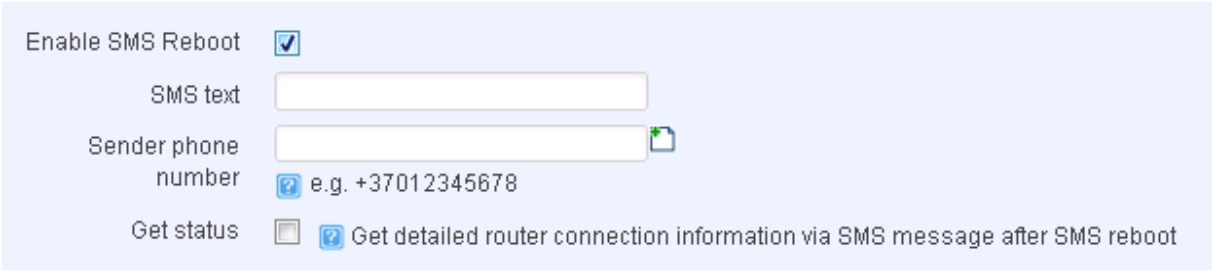
Normalkonfiguration:

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

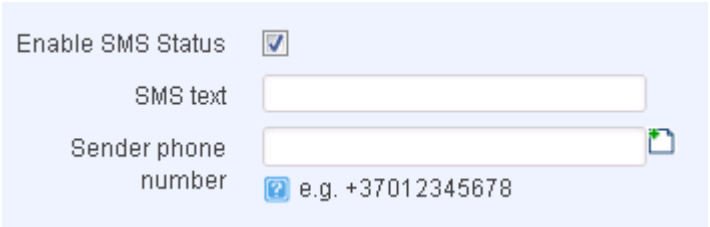
Man kann den Router auch über eine SMS-Text-Message Neustarten. Dies empfiehlt sich vor allem bei Routern, die nicht gut per Hand neu zu starten sind.



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

7.3.3 Status via SMS

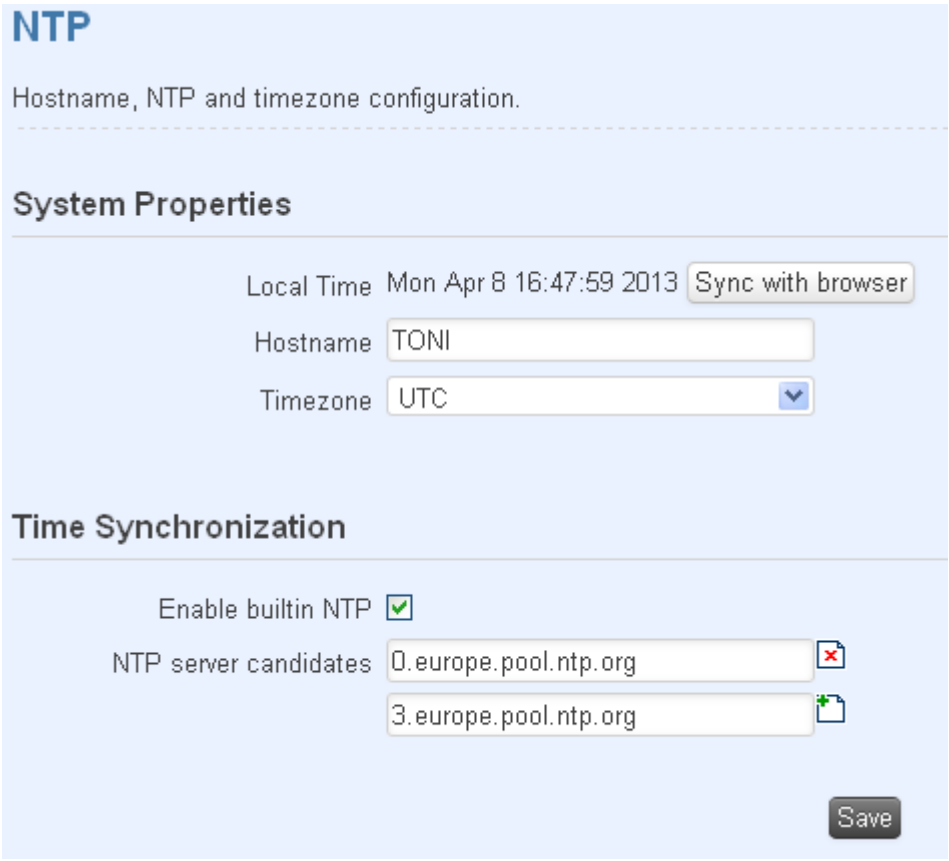
Eine SMS mit dem aktuellen Status des Routers senden.



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

7.3.4 NTP

Systemeinstellungen von TONI

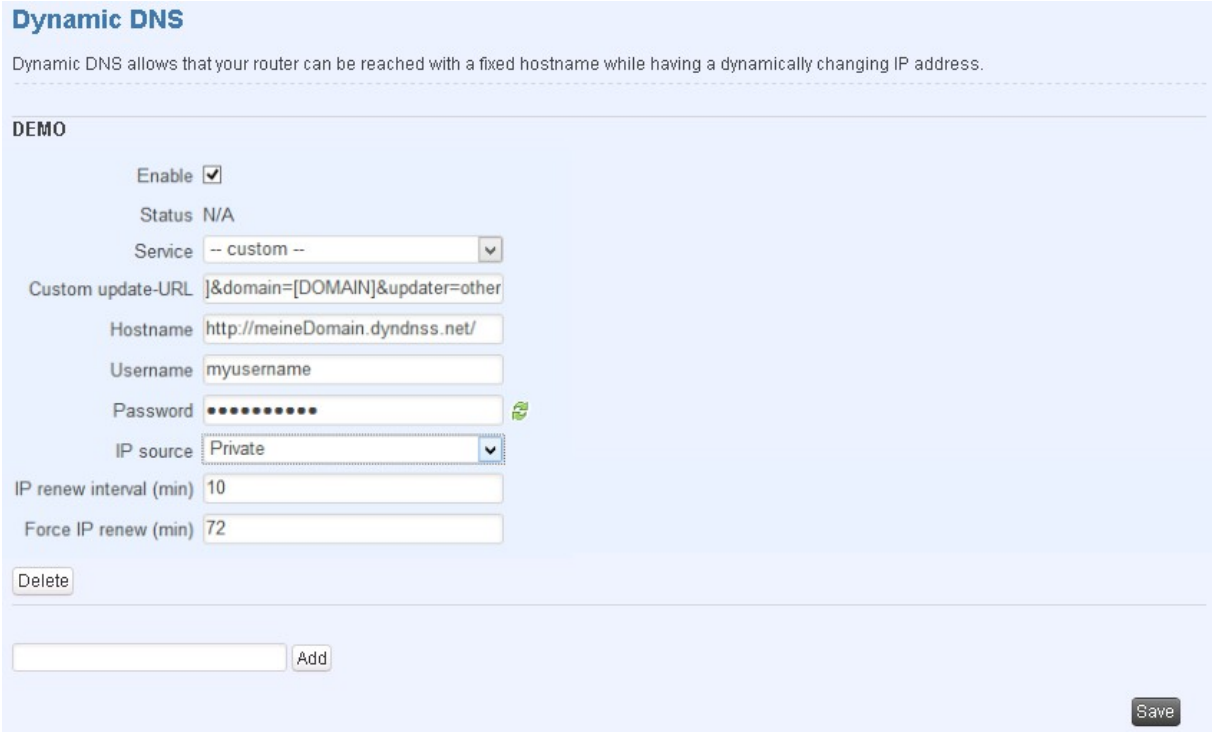


“Sync with browser”: Synchronisiert die Zeit des Routers mit der des Computers.

	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 candidates	NTP server hostname.	Sie können mehrere NTP Server Eintragen. Dazu klicken Sie auf den Button hinter dem Textfeld.

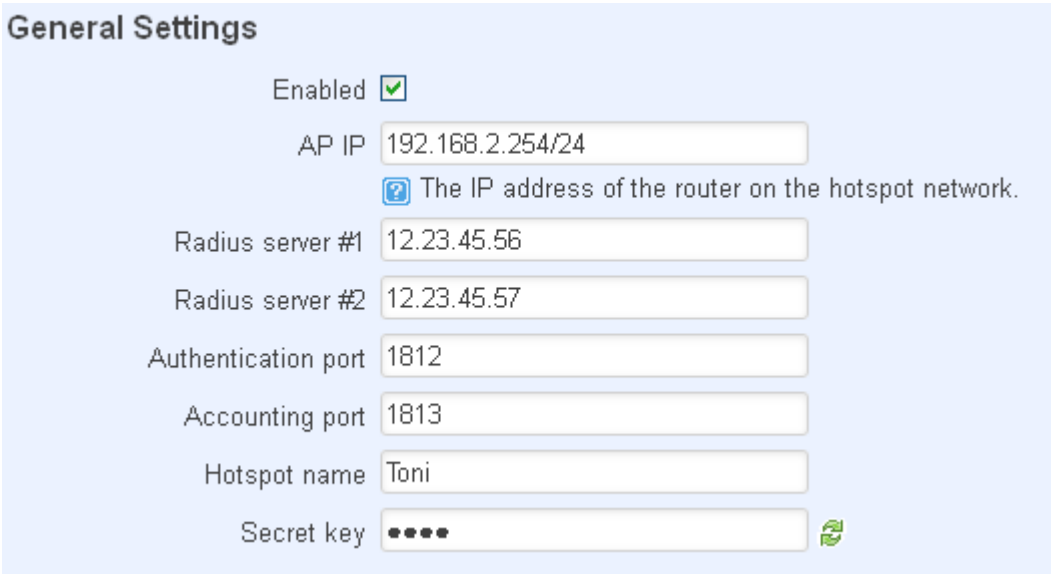
7.3.5 Dynamic DNS

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.



	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.

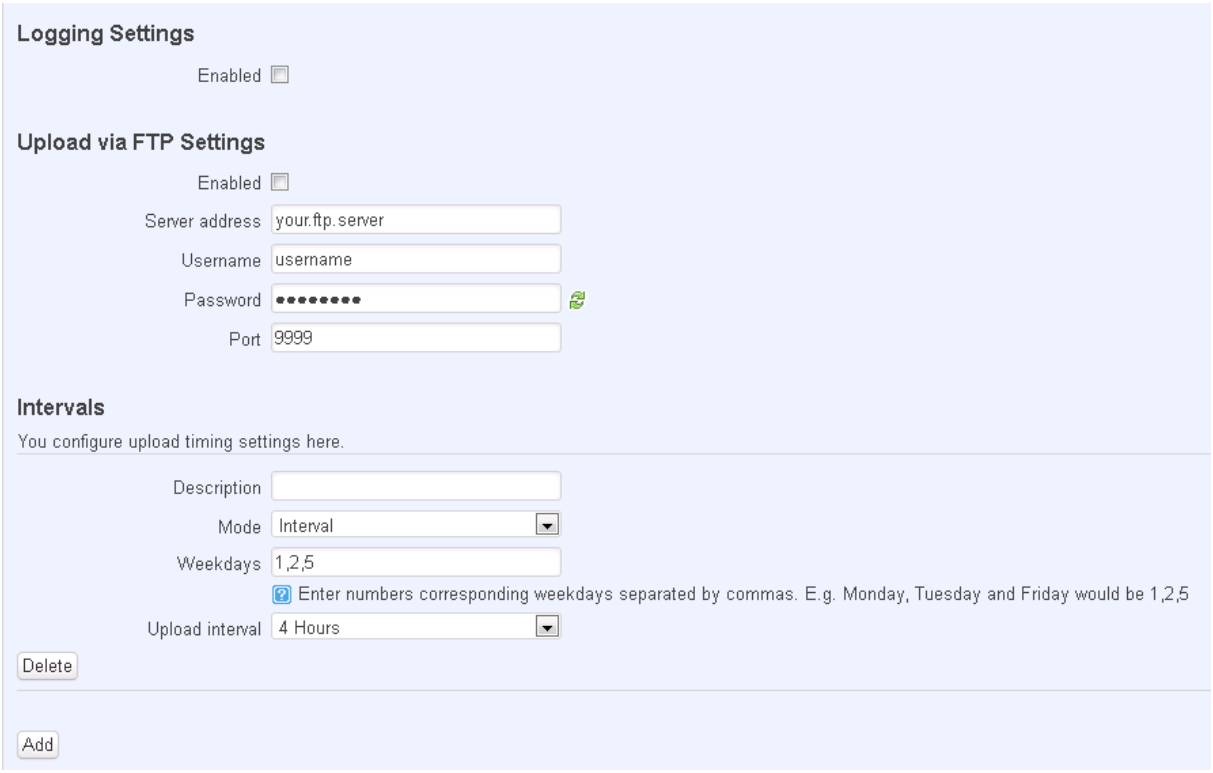
7.3.6 Wireless hotspot



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:

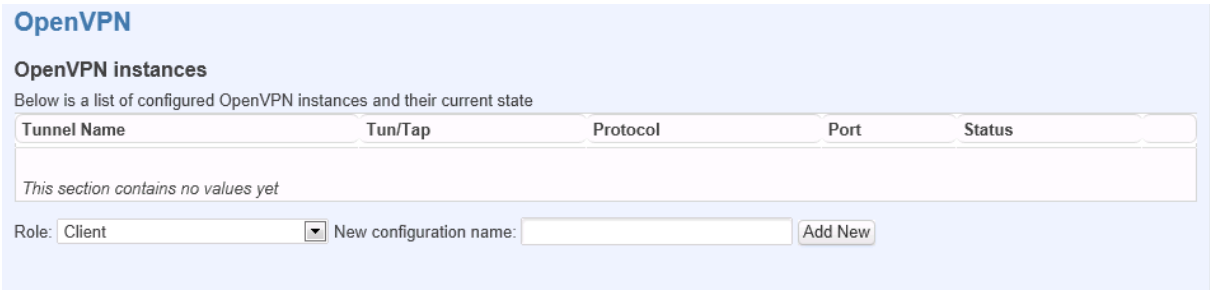


	Feldname	**Erklärung**
1	Logging enabled	Log-Dateien vom Hotspot-Speichern.
2	FTP enabled	Aktivieren von FTP Upload
3	Server address	Die IP-Adresse des FTP Servers, auf dem Sie das Log speichern möchten.
4	Username	Benutzer-Name des FTP Servers
5	Passwort	Passwort des FTP Servers
6	Port	Der TCP/IP Port 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.

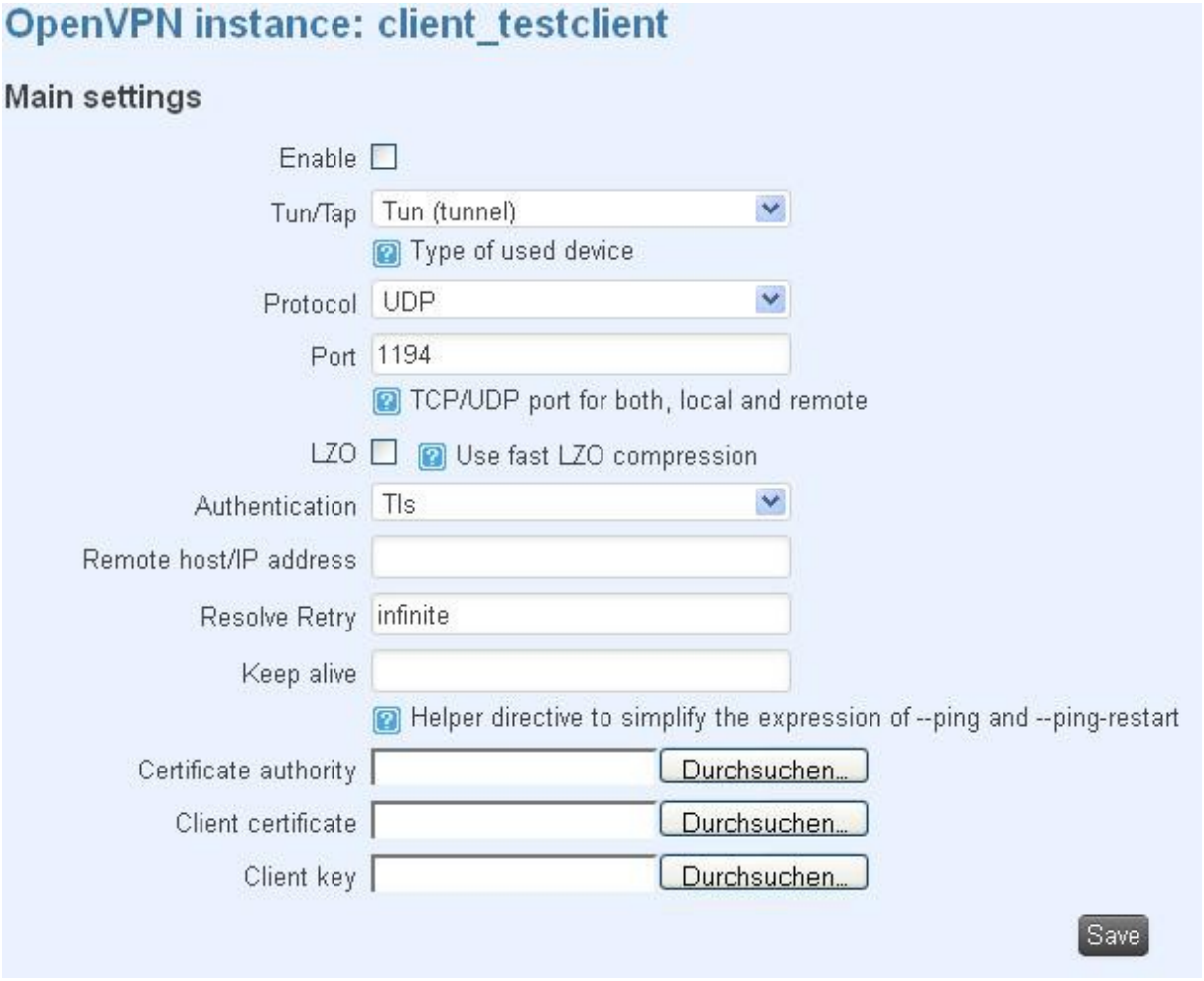


Wählen Sie aus, ob sich der Router zu einem VPN-Netzwerk einwählen soll (Client) oder ob er eines erstellen soll (Server). Danach geben Sie einen Namen bei „New configuration Name:“ ein. Klicken anschließend auf „Add New“ um die Verbindung zu erstellen.

Jetzt steht in der Tabelle eine neue Verbindung.

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

Ein neues Fenster öffnet sich:

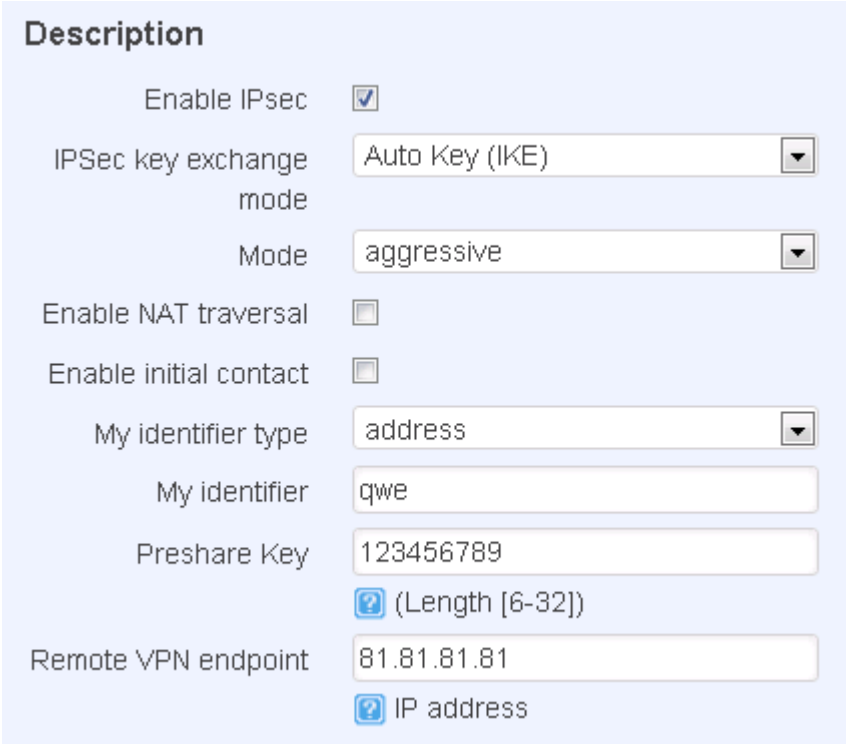


	Feld Name	**Erklärung**
1	Enable	Aktivieren und deaktivieren dieser Verbindung.
2	Port	Definieren Sie die TCP- oder UDP- Portnummer.
3	LZO	Mit dieser Einstellung können die LZO Kompression einschalten. Mit eingeschalteter LZO Kompression erzeugt die VPN-Verbindung weniger Netzwerk verkehr. Jedoch erhöht 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 address	IP-Adresse vom VPN Server.
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 endpoint	IP-Adresse des VPN-Interface.
10	Remote network IP address	IP-Adresse des Remote Virtual Network.
11	Remote network IP netmask	Subnetmaske des Remote Virtual Network.

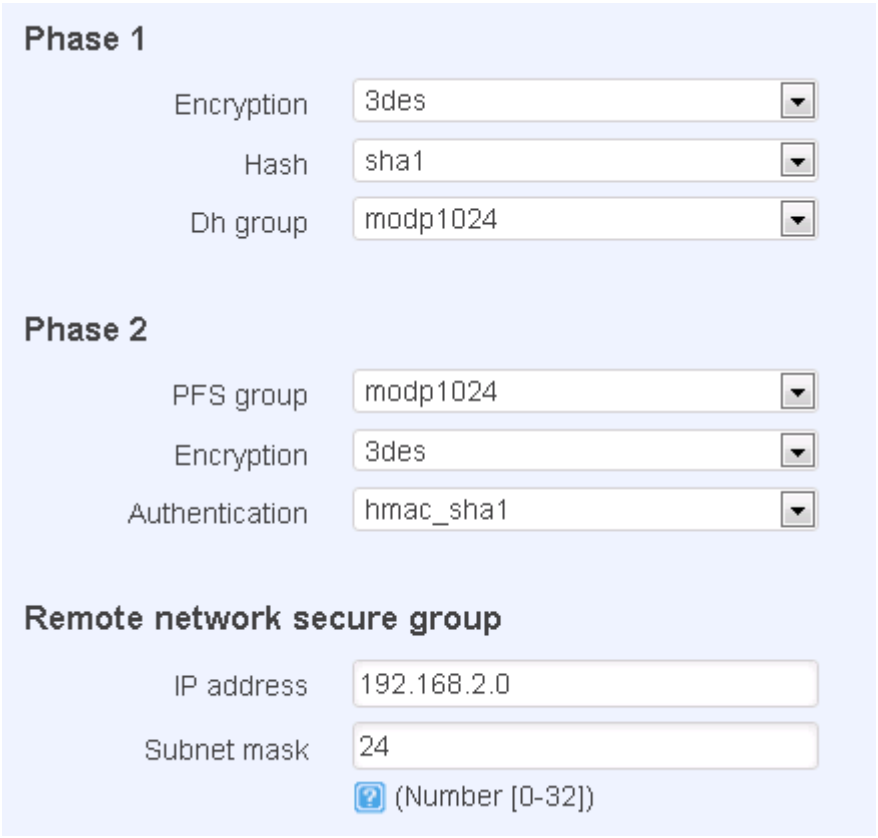
7.3.8 IPsec

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:



	Feldname	Erklärung
1	Enable IPSec	Deaktivieren und aktivieren von IPSec
2	IPSec key exchange mode	Wählen Sie zwischen manuellen Key, den Sie einrichten wollen oder 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.

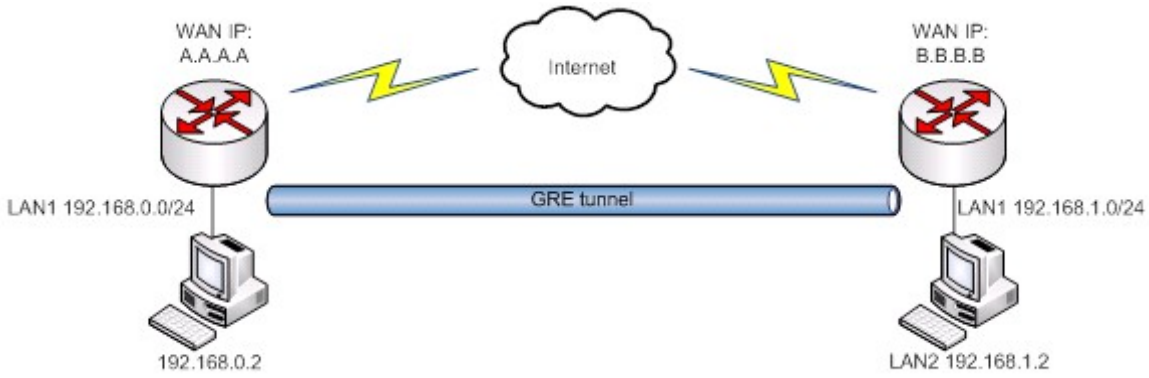


In Phase 1 und Phase 2 werden die Einstellungen vom IPSec Server konfiguriert. In Remote network secure group werden remote network (Secure Policy Database) Informationen eingegeben.

	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

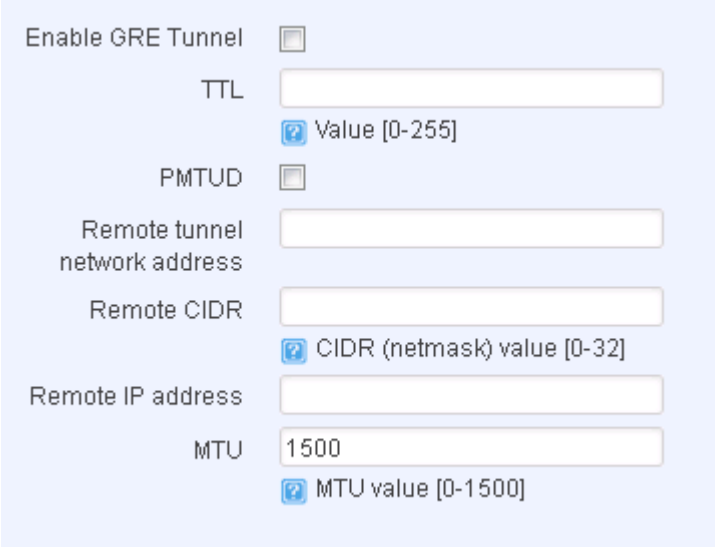
7.3.9 GRE Tunnel

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.

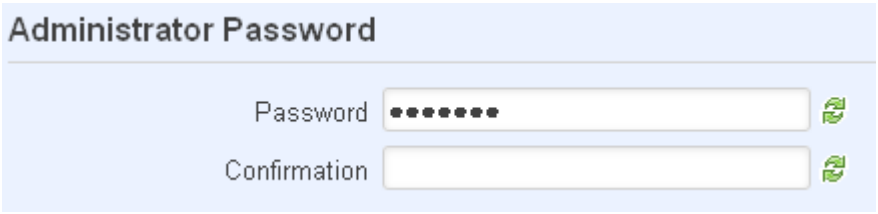


	Feld Name	Erklärung
1	Enable GRE Tunnel	Aktivieren des GRE Tunnels.
2	TTL	Spezifizieren Sie die time-to-live Menge an getunnelten Paketen. (TTL) möglich sind (0-255)
3	PMTUD	Die Checkbox aktiviert den „Pathmaximum Transmission Unit Discovery (PMTUD)“-Status für diesen Tunnel.
4	Remote tunnel network address	Tragen Sie die Remote LAN Subnetz-Adresse ein.
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

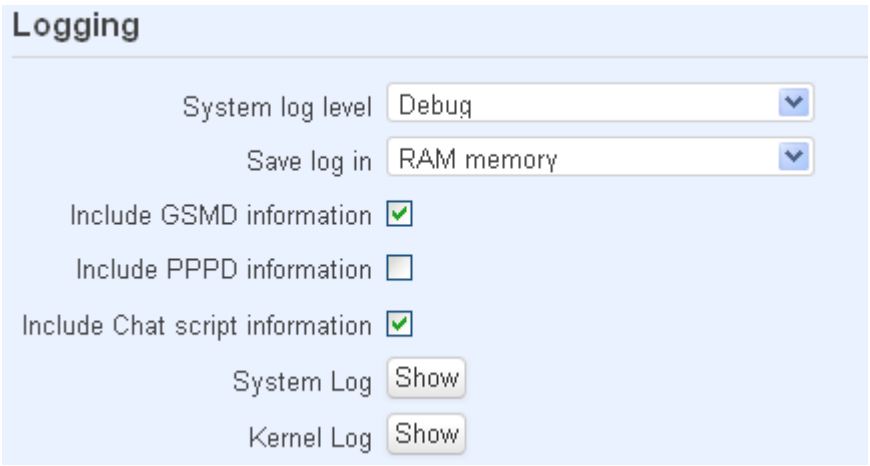
Administration password:



	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:

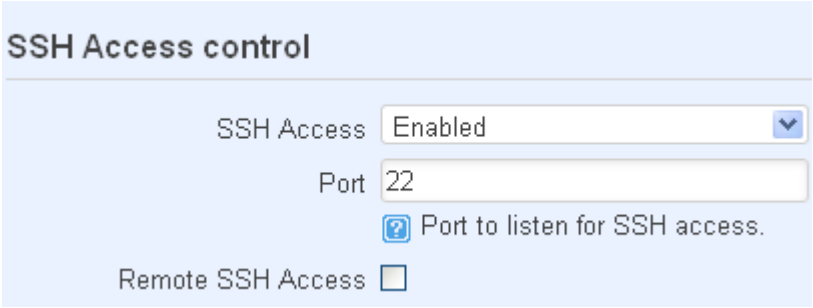


System Mitteilungen werden in folgende Kategorien aufgeteilt:

Info (Infos)
Notice (Notizen)
Warning (Warnungen)
Error (Fehler)
Critical
Alert (Notfall)
Emergency

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

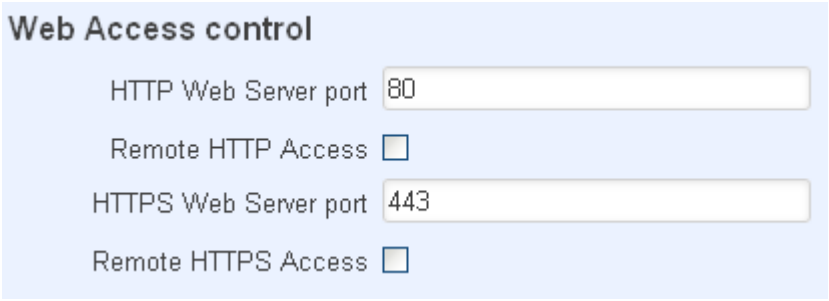
SSH Access Control:



	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.

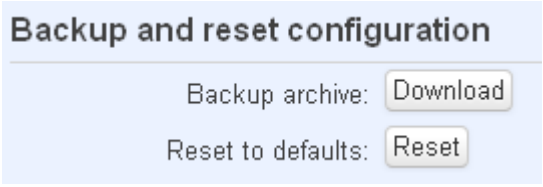
Web Access control:



	Feld Name	Erklärung
1	HTTP Web Server port	Port-Nummer, die der Router für seine Web-Oberfläche benutzt. 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 Access	Ist die Checkbox aktiviert, kann der Benutzer via HTTPS 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.

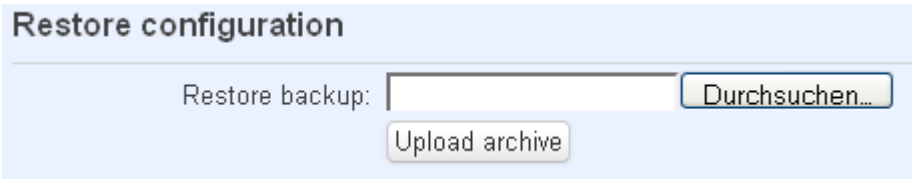
7.4.2 Backup und Firmware

Backup and reset configuration:



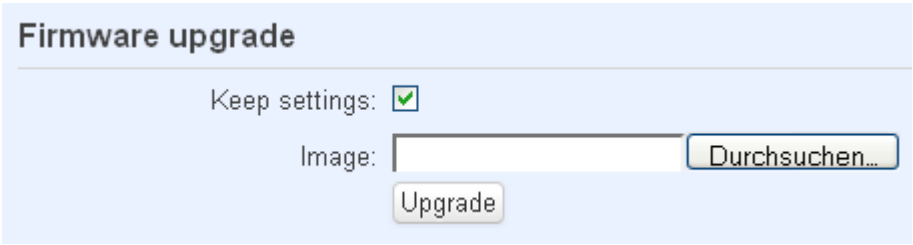
Backup archive – Speichert die Routereinstellungen auf ihren Computer.
Reset to defaults – Reset zu Werkseinstellungen.

Restore configuration :



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

Firmware 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.

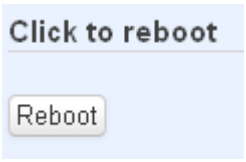
Firmware Upgrade – Verify:

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 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



Der Router startet neu, wenn Sie auf „Reboot“ klicken.

7.5 Logout

Ausloggen aus dem Internetinterface.

8 Open VPN

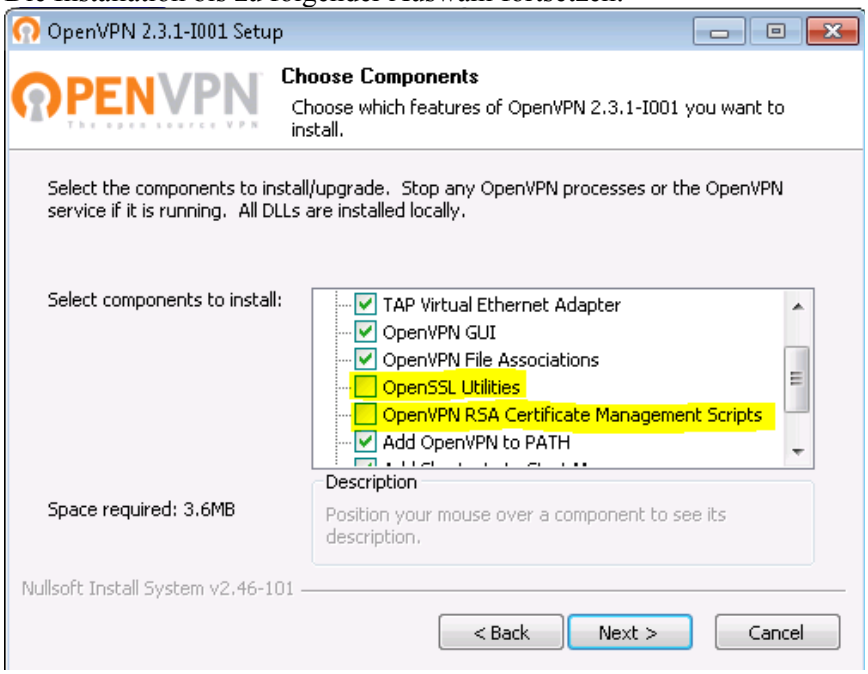
8.1 Installation

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:

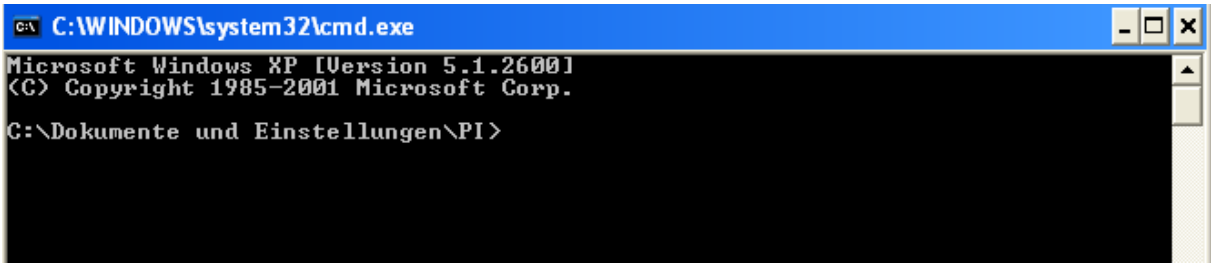


Wenn Sie mit dem Computer Zertifikate erstellen möchten:
Installieren sie zusätzlich “OpenSSL Utilities“ und “Open VPN RSA Certificates Management Scripts“. Alle anderen Installationsmöglichkeiten sollten ausgewählt sein.
Installation mit “Next“ fortsetzen und abschließen.

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.

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

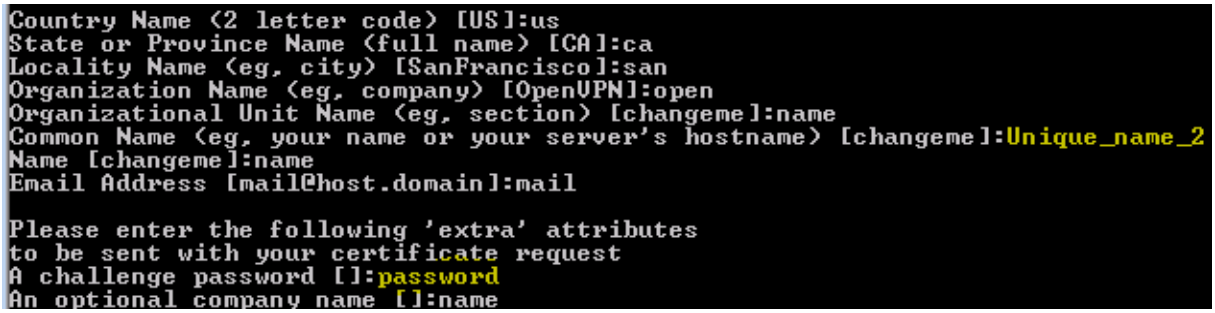
Anmerkung:

- 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 Gerä-teeinstellungen genutzt).

8.2.2 Server Zertifikat erstellen

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

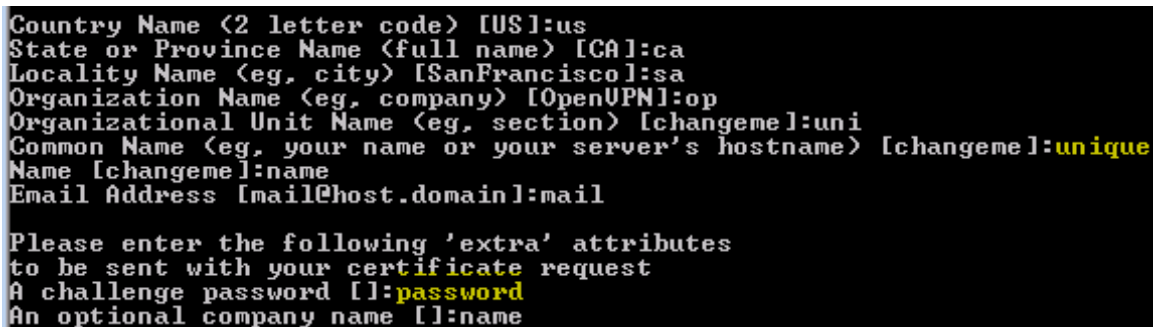


Anschließend können Sie mit “y“ die Angaben bestätigen.
Jetzt haben Sie zwei neue Dateien erstellt (“server.key“ und “server.crt“). Zu finden unter: (C:\OpenV-PN\easy-rsa\keys catalog\).

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.



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

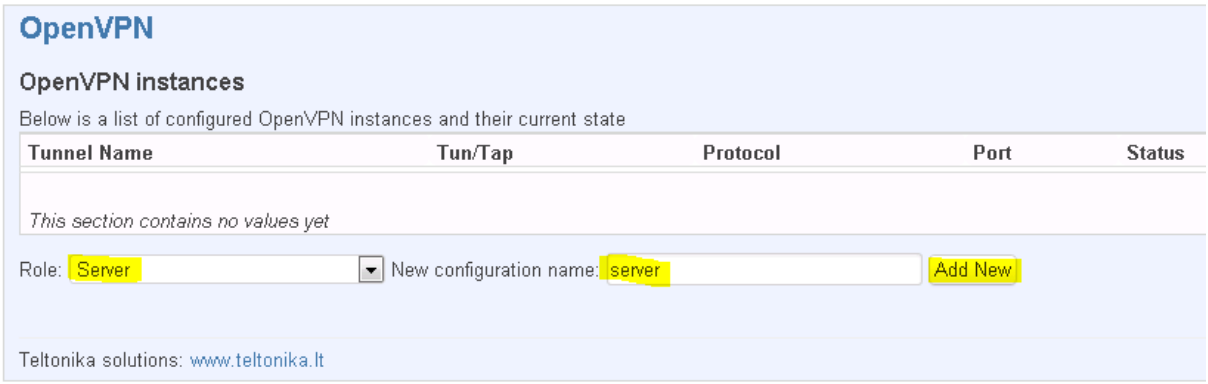
Anmerkung:

- 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“).

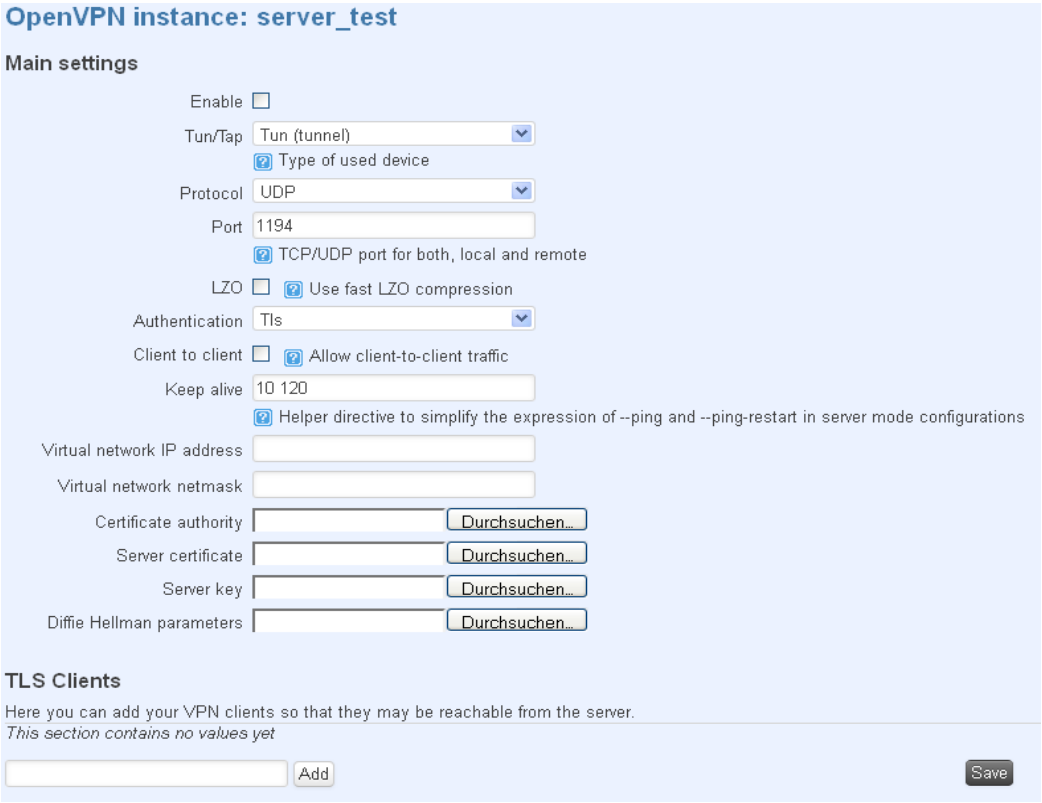
8.3 TONI als OpenVPN „TL's" Server

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.



Anschließend sehen Sie folgendes:

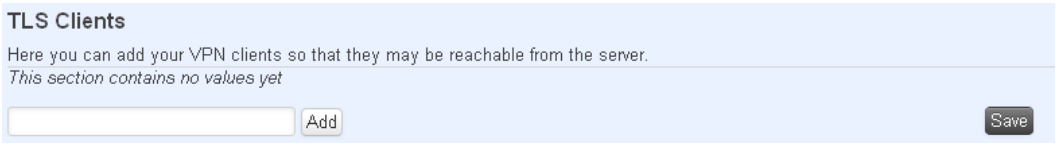
Klicken Sie auf "Edit" um Einstellungen vorzunehmen.



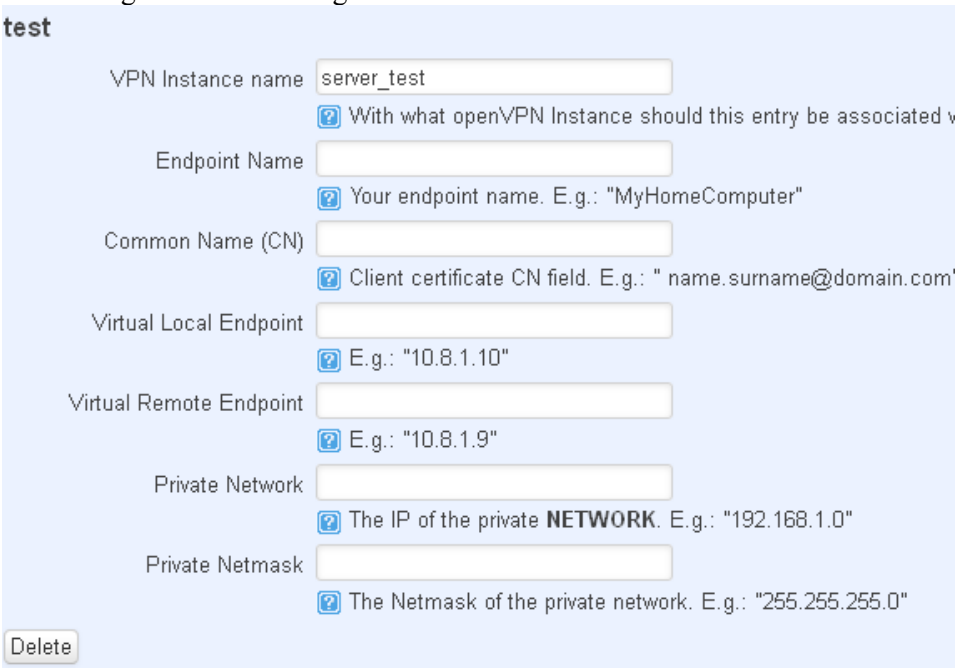
Falls der OpenVPN-Server nicht anläuft obwohl „enabled" gesetzt ist, dann bitte folgende Punkte beachten:
- ggfls. Zertifikate nochmals neu in den **Toni** hochzuladen
- prüfen Sie nochmals die eingegeben Daten und ggf. IP-Adresse abändern
- wenn obige Punkte keine Besserung bringen dann bitte **TONI** 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 deaktivieren (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 Netzwerkmaske.
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.



Einstellungen beim Hinzufügen eines Gerätes:



Feld	Beschreibung
VPN Instance name	Standardname (Default)

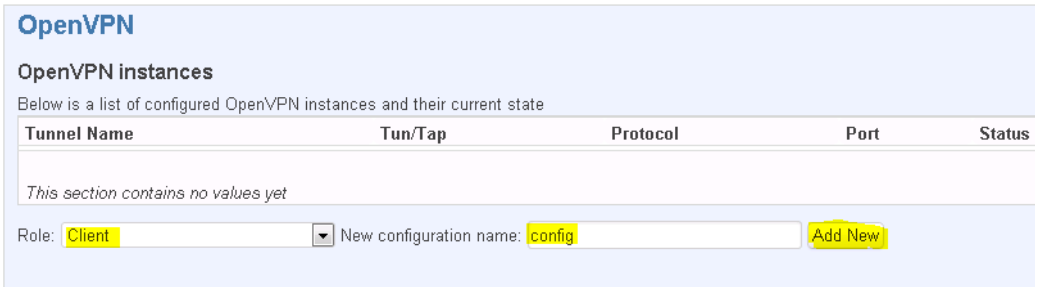
Endpoint Name	Gerätename (Computer)
Common Name (CN)	Vordefinierter Name
Virtual Local Endpoint	Benutzen Sie die IP-Endungen von der nachfolgenden Tabelle.
Virtual Remote Endpoint	Benutzen Sie die IP-Endungen von der nachfolgenden Tabelle.
Private Network	Standard-IP des Gerätes eintragen
Private Netmask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

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

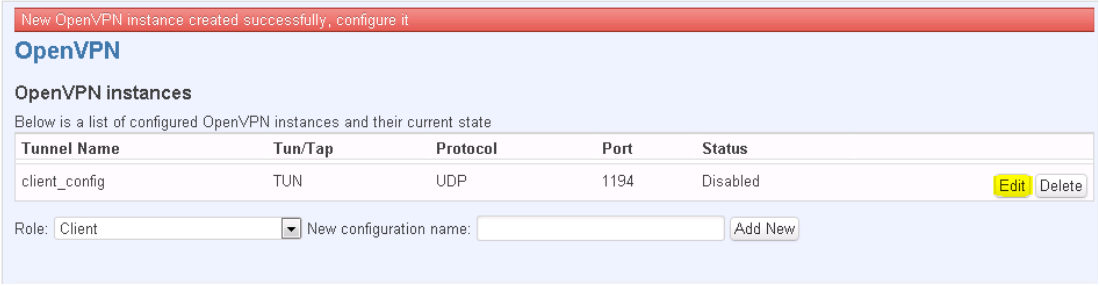
```
[  1,  2] [  5,  6] [  9, 10] [ 13, 14] [ 17, 18]
[ 21, 22] [ 25, 26] [ 29, 30] [ 33, 34] [ 37, 38]
[ 41, 42] [ 45, 46] [ 49, 50] [ 53, 54] [ 57, 58]
[ 61, 62] [ 65, 66] [ 69, 70] [ 73, 74] [ 77, 78]
[ 81, 82] [ 85, 86] [ 89, 90] [ 93, 94] [ 97, 98]
[101,102] [105,106] [109,110] [113,114] [117,118]
[121,122] [125,126] [129,130] [133,134] [137,138]
[141,142] [145,146] [149,150] [153,154] [157,158]
[161,162] [165,166] [169,170] [173,174] [177,178]
[181,182] [185,186] [189,190] [193,194] [197,198]
[201,202] [205,206] [209,210] [213,214] [217,218]
[221,222] [225,226] [229,230] [233,234] [237,238]
[241,242] [245,246] [249,250] [253,254]
```

8.4 TONI als OpenVPN „TL's“ Gerät

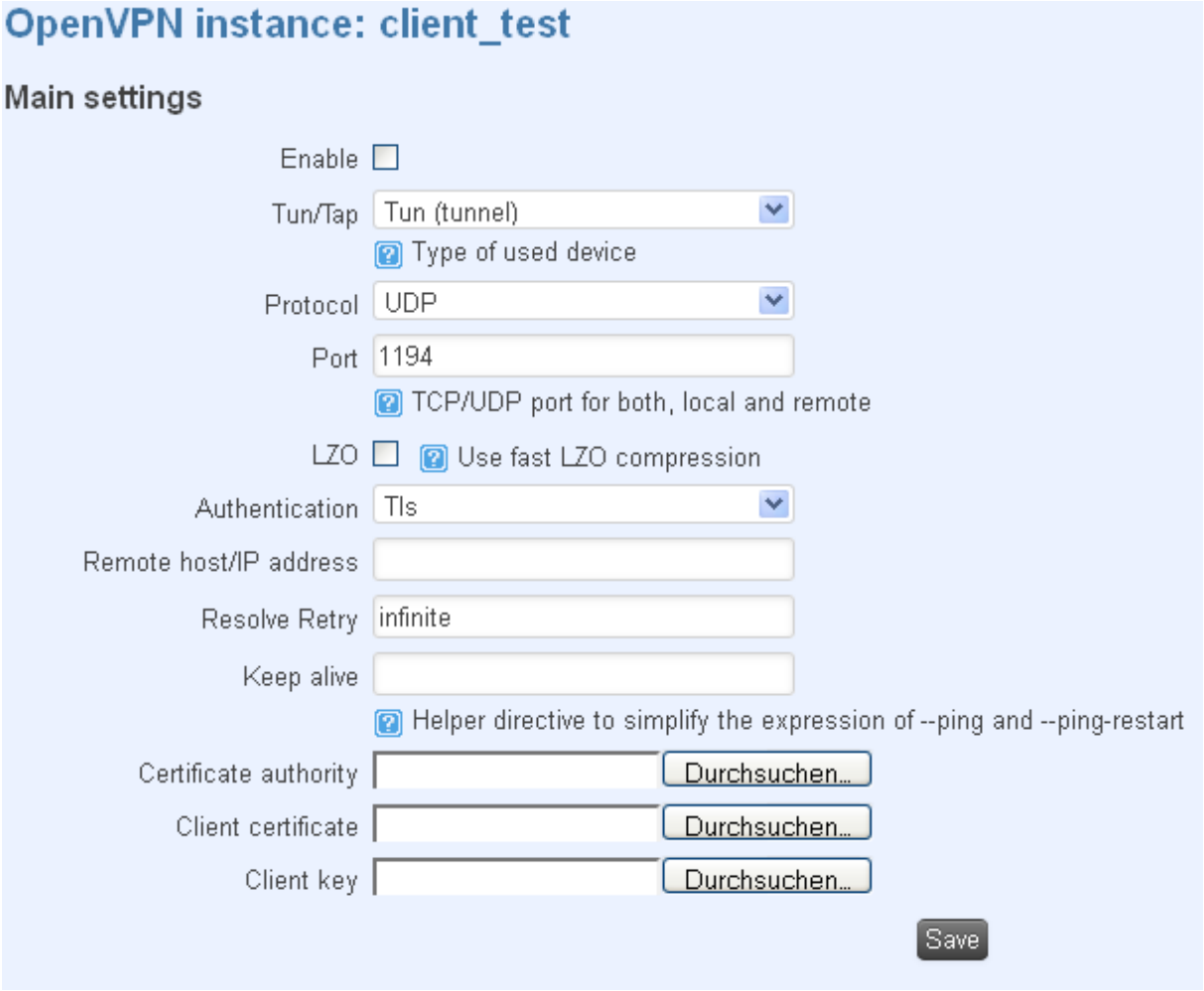
Öffnen Sie das TONI Webinterface (z.B. 192.168.1.1 in Adresszeile des Browsers eingeben) und gehen Sie zum Menüpunk (Services -> OpenVPN). Erstellen Sie einen Client mit beliebigen Namen.



Anschließend sehen Sie folgendes:



Klicken Sie auf “Edit“ um Einstellungen vorzunehmen.



Feld	**Beschreibung**
Enable	Gerät aktivieren oder deaktivieren
Port	Standardport ist 1194
LZO	Kompressionsverfahren aktivieren oder deaktivieren (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 ca.crt
cert server.crt
key server.key
dh dh1024.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
keepalive 10 120
comp-lzo
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.

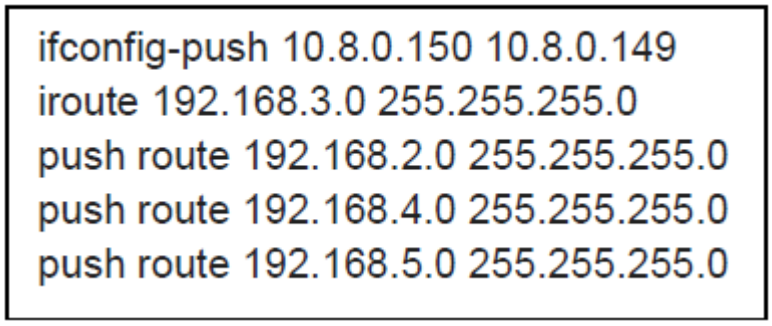
Die grün markierten Dateien sollten mit selben Dateinamen in das Verzeichnis (C:\Program Files\OpenVPN\config) kopiert werden. (Gleicher Ordner wie die Server-Konfigurations-Dateien.

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 Konfigurieren (IP und Netzwerkmaske).
push route	Die Server IP-Adresse und Netzwerkmaske.
push route	Weitere Adressen anderer Geräte (IP und Netzwerkmaske).

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.



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 192.168.99.151 1194

resolv-retry infinite

nobind

persist-key

persist-tun

ca ca.crt

cert unique.crt

key unique.key

comp-lzo

verb 3

route-delay
```

Zeile	Beschreibung
remote	Die Server IP-Adresse mit Port (Standard = 1194).
ca ca.crt cert unique.crt key unique.key	Diese Dateien sollten in Ihrem Verzeichnis (C:\Program Files\OpenVPN\config) sein. 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:

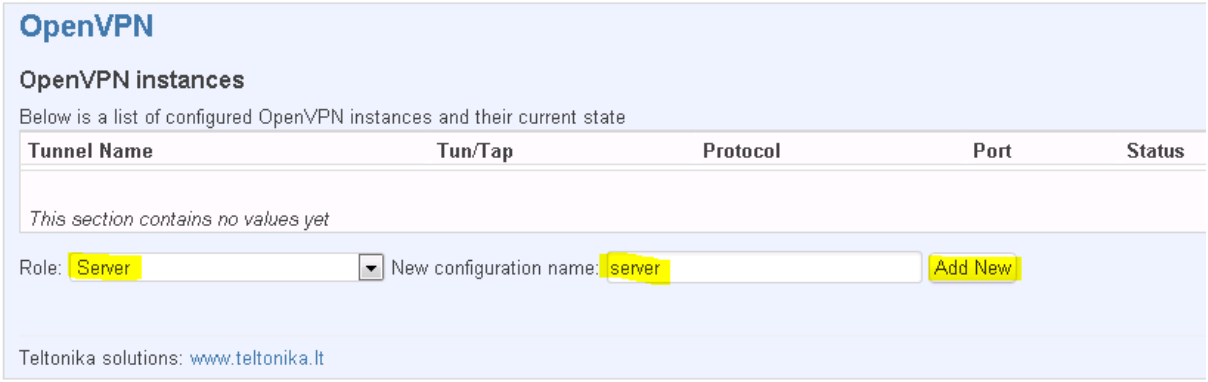
```
remote 192.168.99.156

verb 3

proto udp

dev tun

ifconfig 10.8.0.6 10.8.0.5

key.txt
```

Tragen Sie bei

- „remote“ Ihre Server IP-Adresse ein
- „ifconfig“ die Virtuelle und Locale IP-Adresse ein.

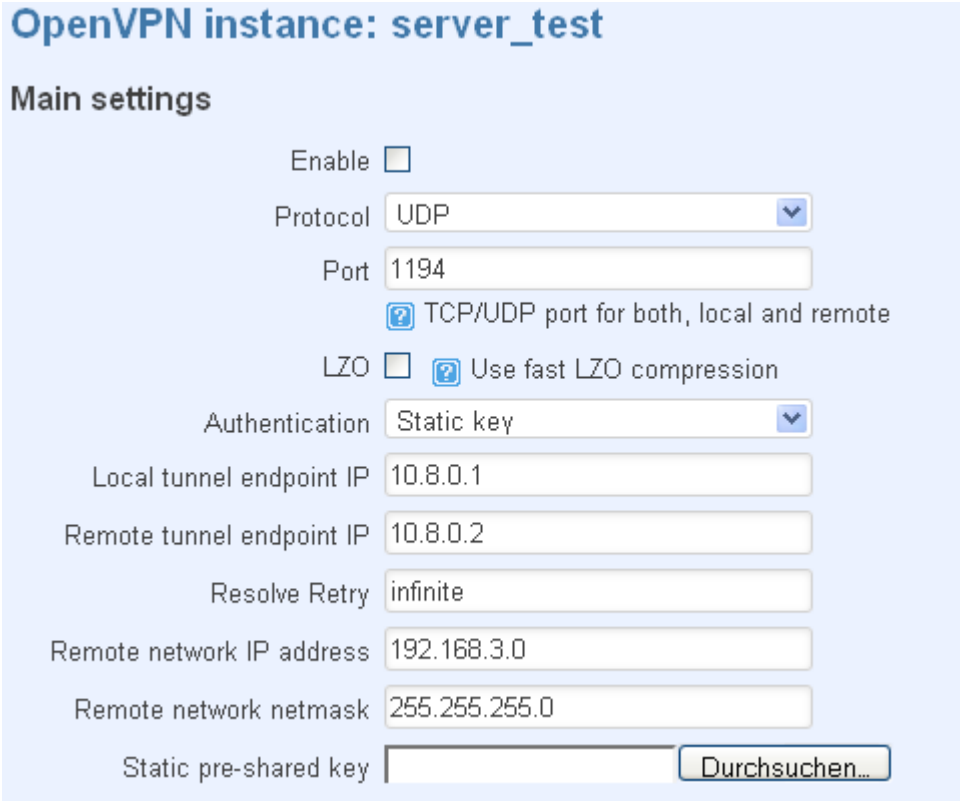
8.6 TONI als OpenVPN „Static Key“ Server

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.



Anschließend sehen Sie folgende Aufstellung:

Um Einstellungen vornehmen zu können, klicken Sie auf „Edit“.



Feld	Beschreibung
Enable	Gerät aktivieren oder deaktivieren
Port	Standardport ist 1194
LZO	Kompressionsverfahren aktivieren oder deaktivieren (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 Konfiguration
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 → 9 VDC Adapter
- Eingangs Spannung: 7 – 30VDC (8 – 18 VDC für ältere Generationen*)
- Benötigter Strom < 7W

- 2xSMA Anntennenkontakte für 3G (1 x SMA für andere Modelle), 1x RP-SMA für 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.