TK800

Ausführung:
v1.0.0

Datum:
13.10.2023

Inhaltsverzeichnis

1 1. Einführung

1.1 Hinweis zum Copyright

1.2 Marken

Welotec ist eine eingetragene Marke der Welotec GmbH. Andere in diesem Handbuch genannte Marken sind Eigentum der jeweiligen Unternehmen.

1.3 Rechtlicher Hinweis

Die Informationen in diesem Dokument können ohne Vorankündigung geändert werden und sind für die Welotec GmbH nicht verbindlich.

Es ist möglich, dass dieses Benutzerhandbuch technische oder typografische Fehler enthält. Es werden regelmäßig Korrekturen vorgenommen, ohne dass darauf in neuen Versionen hingewiesen wird.

1.4 Kontaktinformationen für technischen Support

Welotec GmbH

Zum Hagenbach 7

48366 Laer

Tel.: +49 2554 9130 00

Fax.: +49 2554 9130 10

Email: info@welotec.com

1.5 Beschreibung

Die Router der TK800-Serie für den Industriebereich stellen eine stabile Verbindung zwischen Remotegeräten und Kundenstandorten über 2G/3G/4G-Netzwerke bereit. Sie können in einem Spannungsbereich von 12-48V DC betrieben werden und verfügen über einen Temperaturbereich von -25°C bis 70°C bei einer relativen Luftfeuchtigkeit von 95 % sowie die Einhaltung zahlreicher EMV-Normen, wodurch eine hohe Stabilität und Zuverlässigkeit unter strengen industriellen Bedingungen gewährleistet ist. Der TK800 kann auf dem Arbeitsplatz verwendet oder auf DIN-Schienen montiert werden. Produkte der TK800-Serie unterstützen VPN (IPSec/L2TP/GRE/OpenVPN), was sichere Verbindungen zwischen Remotegeräten und Kundenstandorten garantiert.

1.6 *Wichtige Sicherheitshinweise*:

Dieses Produkt ist für folgende Einsatzbereiche nicht geeignet

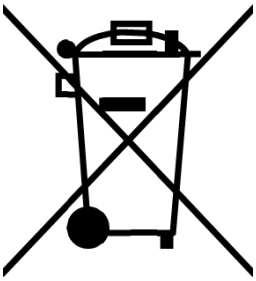
- Bereiche, in denen keine Funkanwendungen (wie Handys) erlaubt sind
- Krankenhäuser und andere Orte, an denen der Einsatz von Handys nicht zulässig ist
- Tankstellen, Treibstofflager und Orte, an denen Chemikalien gelagert werden
- Chemische Anlagen oder andere Orte mit Explosionsgefahr
- Metalloberflächen, die den Funksignalpegel schwächen können

1.7 Warnung

Dies ist ein Produkt der Klasse A. Im Wohnbereich kann der Einsatz zu Funkstörungen führen, die vom Benutzer mit entsprechenden Maßnahmen zu beheben sind.

1.8 WEEE-Hinweis

Die am 13. Februar 2003 in Kraft getretene europäische Richtlinie zur Entsorgung elektrischer und elektronischer Altgeräte (WEEE) hat zu großen Veränderungen hinsichtlich der Wiederverwendung und des Recyclings elektrischer Geräte geführt. Das Hauptziel dieser Richtlinie ist die Vermeidung von Abfällen von Elektro- und Elektronikgeräten sowie das Fördern der Wiederwendung, des Recyclings und anderer Formen der Wiederverwertung. Das WEEE-Logo auf dem Produkt oder der Verpackung weist darauf hin, dass das Produkt nicht im normalen Hausmüll entsorgt werden darf. Sie sind dafür verantwortlich, alle ausgedienten elektrischen und elektronischen Geräte an entsprechenden Sammelstellen zu entsorgen. Eine getrennte Sammlung und sinnvolle Wiederverwertung Ihres Elektroschrotts hilft dabei, sparsamer mit den natürlichen Ressourcen umzugehen. Zudem stellt eine sachgemäße Wiederverwertung elektrischer und elektronischer Altgeräte die menschliche Gesundheit und den Schutz der Umwelt sicher.



Weitere Informationen zur Entsorgung, Wiederverwertung sowie zu Sammelstellen elektrischer und elektronischer Altgeräte erhalten Sie bei Ihrer örtlichen Stadtverwaltung, den Entsorgungsbetrieben, dem Vertreiber oder dem Hersteller des Geräts.

2 2. Quick Start

Leitfaden zur Installation und Inbetriebnahme der TK800 Serie. Bitte stellen Sie sicher, dass alle Paketinhalte bei der Lieferung vorhanden sind. Sollten Sie eine SIM-Karte benötigen, wenden Sie sich an Ihren örtlichen Netzbetreiber.

2.1 2.1. Paket Checkliste

Jeder TK800 wird in einer Box mit Standardzubehör geliefert. Außerdem können optionale Zubehörteile bestellt werden. Prüfen Sie den Inhalt der Box. Sollte etwas fehlen, kontaktieren Sie Welotec.

2.1.1 2.1.1. Bestandteile Router

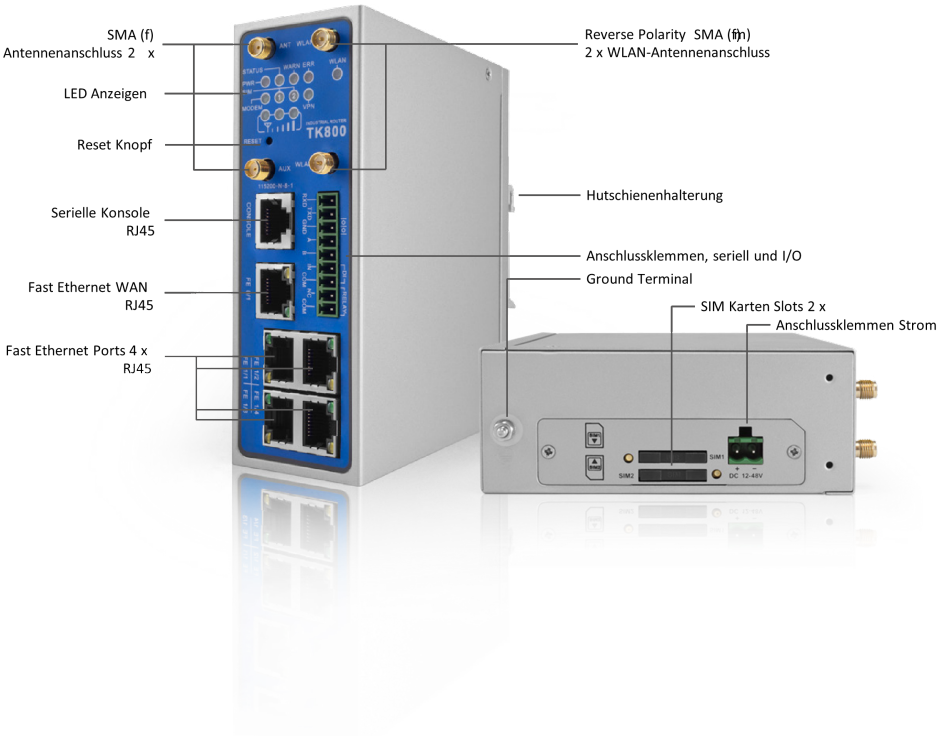
Produkt	Anzahl	Beschreibung
TK800	1	Industrieller Router der Serie TK800
Anschlussklemme	1	Anschlussklemme, 2-polig
Anschlussklemmen Seriell und I/O	1	Anschlussklemme, 9-polig (nur EX0 / EXW Varianten)

2.1.2 2.1.2. Bestandteile Set

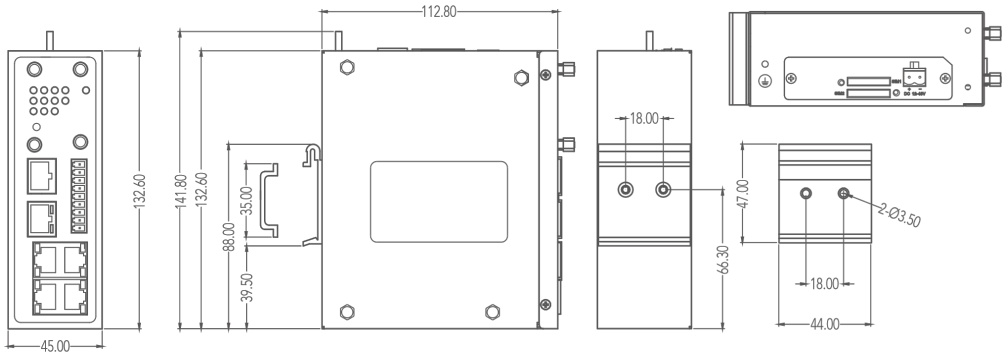
Produkt	Anzahl	Beschreibung
TK800	1	Industrieller Router der Serie TK800
Anschlussklemme	1	Anschlussklemme, 2-polig
Netzwerkkabel	1	1,5 m
Antenne	2 (4)	3G/4G Antenne Wi-fi Antenne (Nur EXW Variante)
Netzteil	1	230 V AC auf 12 V DC
Anschlussklemmen Seriell und I/O	1	Anschlussklemme, 9-polig (nur EX0 / EXW Varianten)

2.2 2.2. Informations- und Bedienpanel

2.2.1 2.2.1. Bedienpanel



2.2.2 2.2.2. Maßzeichnungen



2.3 2.3. Installationsleitfaden

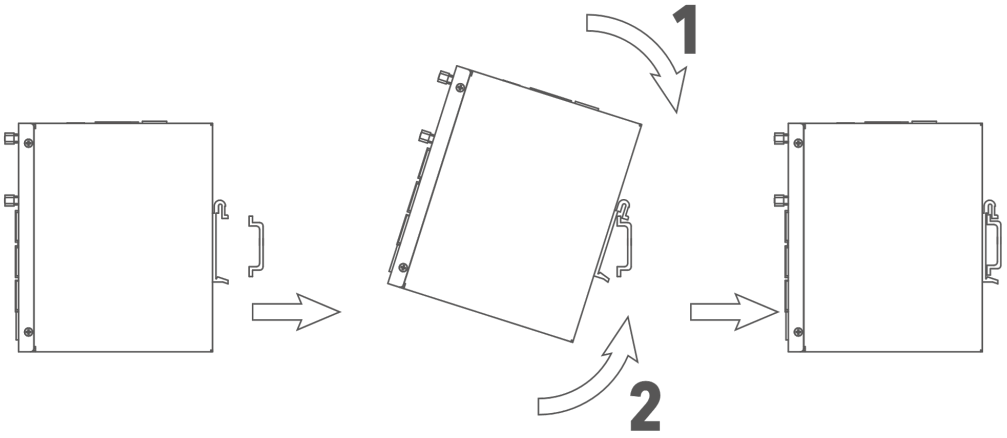
2.3.1 2.3.1. Vorbereitungen

Bereiten Sie die Spannungsversorgung vor (12 - 48 V DC). Stellen Sie sicher, dass das Gerät unter den angegebenen Umgebungsbedingungen (Arbeitstemperaturbereich -25 – +70 °C, Feuchtigkeit: 5 – 95 % relative Luftfeuchtigkeit) arbeiten kann. Das Gerät sollte nicht direkter Sonneneinstrahlung ausgesetzt werden und sollte von Wärmequellen und Umgebungen mit starken elektromagnetischen Interferenzen getrennt installiert werden. Der Router kann auf einer DIN-Schiene (Hutschiene) montiert oder auch am Arbeitsplatz verwendet werden.

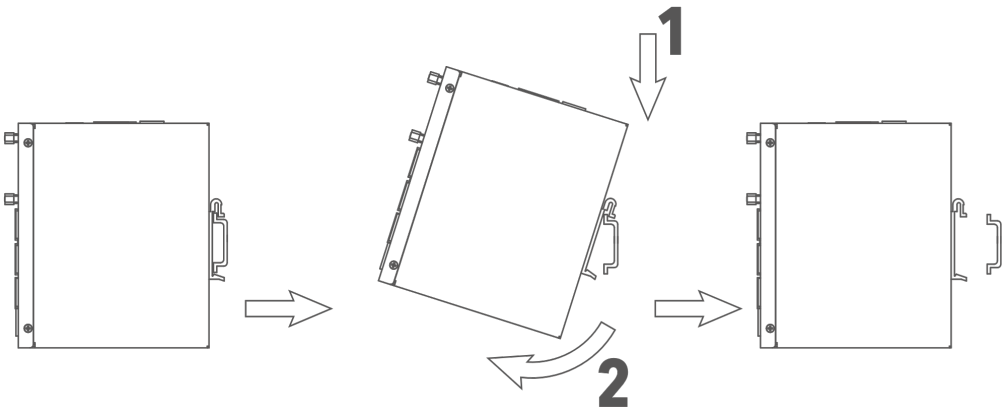
2.3.2 2.3.2. Montage des Gerätes

Hutschiene:

Wählen Sie eine Position mit genügend Platz auf der Hutschiene. Platzieren Sie dann das obere Teil der Hutschienenmontage auf die Hutschiene. Im Anschluss daran drücken Sie die untere Seite der Hutschienenaufnahme nach unten bis das Gerät eingerastet ist. Zur Veranschaulichung dient dieses Bild:



Zur Demontage drücken Sie das Gerät von oben nach unten und ziehen dann die untere Seite des Gerätes von der Hutschiene (siehe Abbildung).



2.4 2.4. Installation der SIM-Karte

Der TK800 unterstützt Dual-SIM. Zum Einsetzen der Karten drücken Sie den gelben „Auswerfen“-Knopf z.B. mit einem kleinen Schraubenzieher auf der Oberseite des Gerätes. Der jeweilige SIM-Karten-Slot wird herausgedrückt. Wenn der TK800 nicht im Dual-SIM-Modus betrieben wird, nutzen Sie den SIM-Karten-Slot „SIM1“.

Legen Sie dann die SIM-Karte ein. Der SIM-Karten Slot ist nicht Hot-Plug fähig. Der Router muss nach einlegen der SIM-Karte also neu gestartet werden.

2.5 2.5. Installation der Antennen

Stecken Sie die Antennen auf die SMA-Anschlüsse und drehen Sie die äußere Befestigung am Antennenkabel, bis die Verbindung fest ist.

Hinweis

Für eine optimale Leistung sollten die Antennen in einem Abstand von mindestens 20 cm zueinander platziert werden.

2.6 2.6. Installation der Spannungsversorgung

Entfernen Sie den Anschlussblock von der Oberseite des Routers. Lösen Sie die entsprechenden Schrauben am Anschlussblock und führen Sie die Adern auf die entsprechenden Klemmen. Die Klemmen sind auf der Oberseite des Routers entsprechend gekennzeichnet. Ziehen Sie die Schrauben im Anschluss daran wieder fest und stecken Sie dann den Anschlussblock wieder in den Router.

Zur Erdung des Gerätes nutzen Sie die Erdungsschraube am Gerät.

Hinweis

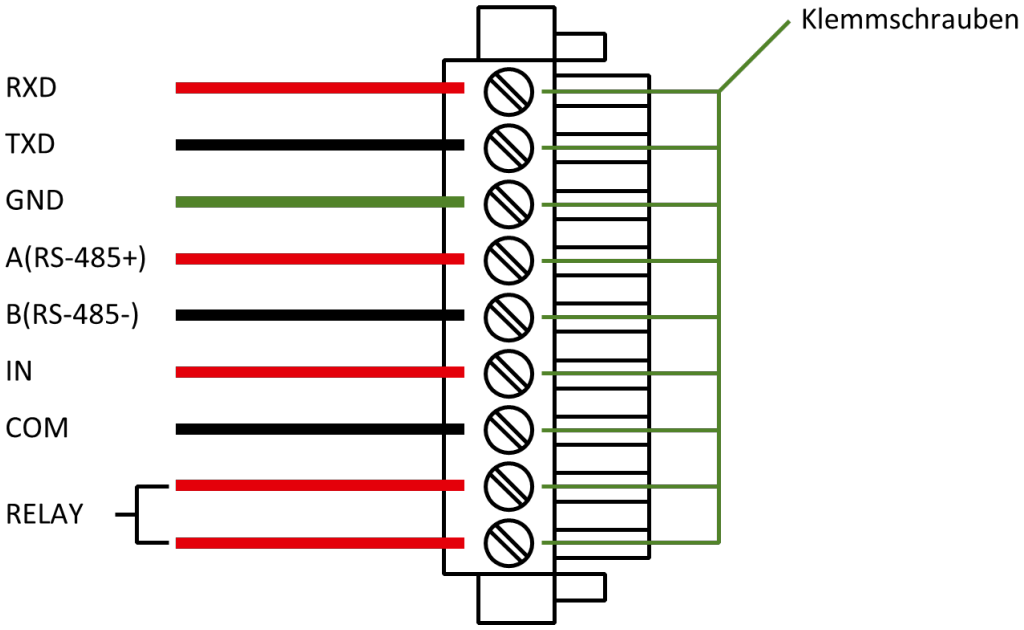
Um Störungen durch elektromagnetischen Einfluss auszuschließen, muss das Gehäuse des Routers über die Erdungsschraube geerdet werden.

2.7 2.7. Kabelverbindungen

Verbinden Sie den Router über ein Netzwerkkabel (RJ45) mit Ihrem PC. Wir empfehlen bei allen TK8x2 Modellen den Port FE 0/2 und bei allen TK8x5 Modellen den Port FE 1/4.

2.8 2.8. Anschluss der seriellen Schnittstellen und I/O´s

Zum Anschluss der seriellen Schnittstellen und der I/O´s finden Sie auf der Vorderseite des Gerätes einen Anschlussblock. Die einzelnen Kontakte hierfür sind auf der Vorderseite des Gerätes beschriftet. Verbinden Sie die Leitungen entsprechend dieser Beschriftungen. Der Kontakt „IN“ repräsentiert hier den digitalen Eingang, während der Ausgang mit „Relay“ beschriftet ist. „COM“ stellt die Masse dar. Es handelt sich hierbei um einen potentialfreien Kontakt, d.h. was man am IN-Kontakt rein gibt, kommt am Relaiskontakt wieder heraus, sofern der Kontakt geschlossen ist. Geschaltet werden kann hierbei per SMS und über das Webinterface. Bei 230 VAC kann der Kontakt mit 2 Ampere belastet werden. Bei der Installation ziehen Sie bitte den Anschlussblock vom Gerät ab und schließen die einzelnen Adern an den entsprechenden Klemmen an. Im Anschluss stecken Sie den Anschlussblock wieder auf das Gerät.



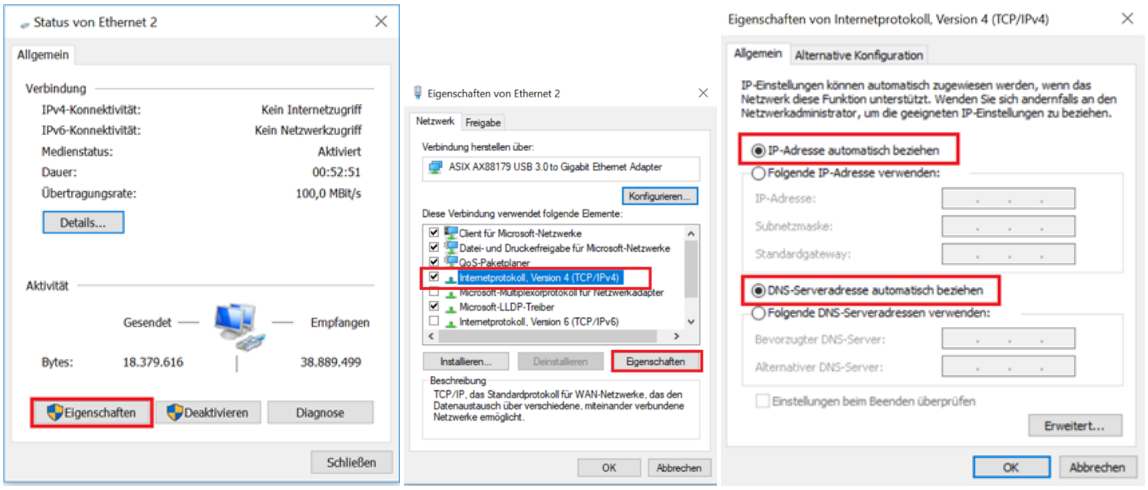
Hinweis

Dieses Kapitel beschreibt nur Router in den Ausführungen mit seriellen Schnittstellen und I/O´s TK8XXX-EX.

2.9 2.9. Inbetriebnahme des Routers

2.9.1 2.9.1. Automatische Konfiguration (DHCP)

Konfigurieren Sie den PC so, dass er als DHCP Client arbeitet (IP-Adresse automatisch beziehen). Schließen Sie den PC mit einem Netzwerkkabel an die Schnittstelle FE0/2 oder FE1/1 - FE1/4 (Nur TK8X5 Varianten) an. Der PC bekommt somit IP-Adresse, Standardgateway und DNS Server vom Router zugewiesen. Das nachfolgende Bild zeigt den Ablauf der Konfiguration per DHCP auf einem PC mit dem Betriebssystem Windows 10. Zu erreichen sind die Einstellungen über das Netzwerk- und Freigabecenter in Windows 10.



Nach der Konfiguration der IP-Adresse des PCs und dem Verbinden mit dem Router öffnen Sie einen Webbrowser.

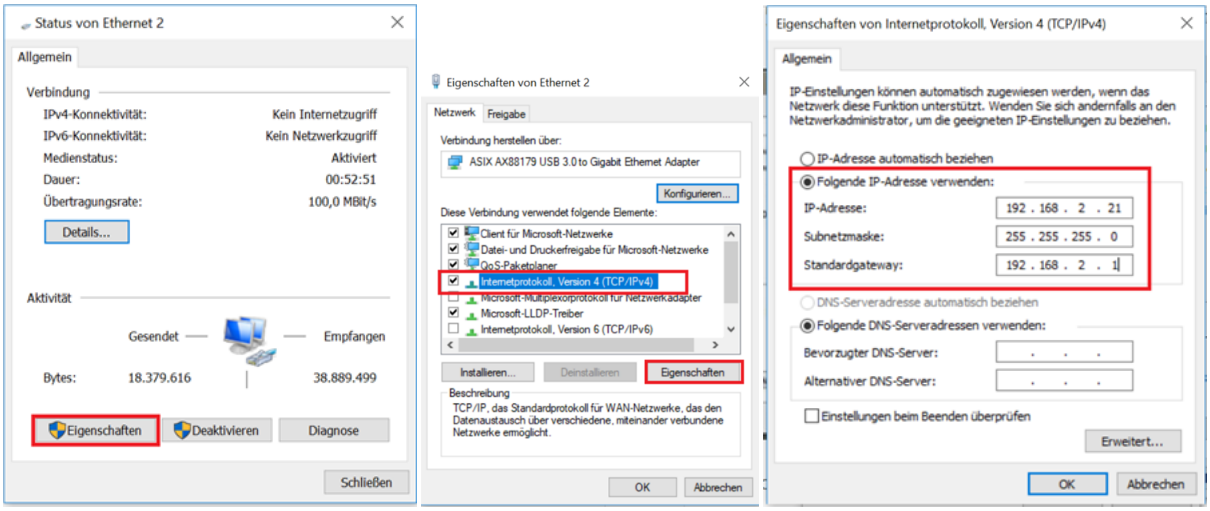
Geben Sie dann in die Adresszeile Ihres Browsers (z.B. Google Chrome) „**http://192.168.2.1**“ ein. Nach dem Bestätigen mit der „Enter“-Taste erscheint ein Pop-up als Login-Seite des Routers. Geben Sie hier den Benutzernamen (Standard: „***adm***“) und das Passwort (Standard: „***123456***“) ein und bestätigen Sie mit „Enter“. Nun werden Sie auf die Konfigurationswebseite weitergeleitet. Konfigurieren Sie nun den Router nach Ihren Anforderungen.

Um zu überprüfen, ob Sie mit dem Internet verbunden sind, wählen Sie aus dem Navigationspanel ***Network > Cellular > Status***. Hier sehen Sie die Daten der Mobilfunkeinheit im Router. Alternativ öffnen Sie einfach eine Webseite in Ihrem Browser.

IP:	192.168.2.1
Benutzername:	adm
Passwort:	123456

2.9.2 2.9.2. Manuelle Konfiguration

Konfigurieren Sie Ihren PC so, dass er sich im selben Subnetz wie der Router (192.168.2.1) befindet. Die Subnetzmaske muss 255.255.255.0 sein. Das nachfolgende Bild zeigt den Ablauf der Konfiguration der IP-Adresse auf einem PC mit dem Betriebssystem Windows 10.



Nach der Konfiguration der IP-Adresse des PCs und dem Verbinden mit dem Router öffnen Sie einen Webbrowser.

Geben Sie dann in die Adresszeile Ihres Browsers„**http://192.168.2.1**“ ein. Nach dem Bestätigen mit der „Enter“-Taste erscheint ein Pop-up als Login-Seite des Routers. Geben Sie hier den Benutzernamen (Standard: „***adm***“) und das Passwort (Standard: „***123456***“) ein und bestätigen Sie mit „Enter“. Nun werden Sie auf die Konfigurationswebseite weitergeleitet. Konfigurieren Sie nun den Router nach Ihren Anforderungen.

Um zu überprüfen, ob Sie mit dem Internet verbunden sind, wählen Sie aus dem Navigationspanel ***Network > Cellular > Status***. Hier sehen Sie die Daten der Mobilfunkeinheit im Router. Alternativ öffnen Sie einfach eine Webseite in Ihrem Browser.

IP:	192.168.2.1
Benutzername:	adm
Passwort:	123456

2.10

2.11 2.10. LED-Statusleuchten

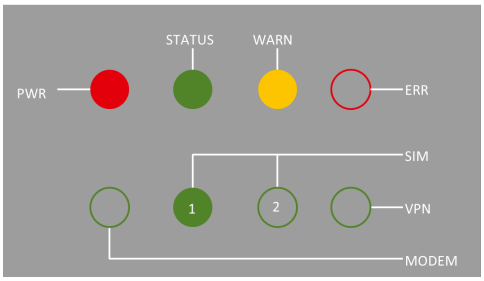
2.11.1 *Symbol-Erklärung*

= LED leuchtet = LED leuchtet nicht = LED blinkt

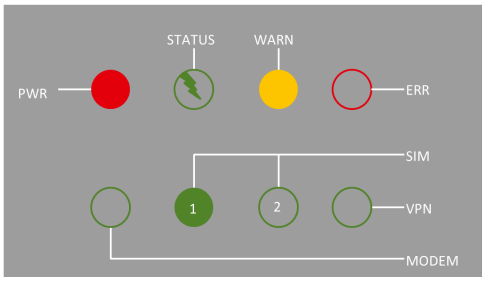
Hinweis

Es gibt zwei SIM-Karten-LED´s. Wenn der Router hochfährt, leuchtet die SIM-Karten-LED für die SIM-Karte 1. In allen anderen Fällen leuchtet die SIM-Karten-Empfangsanzeige:

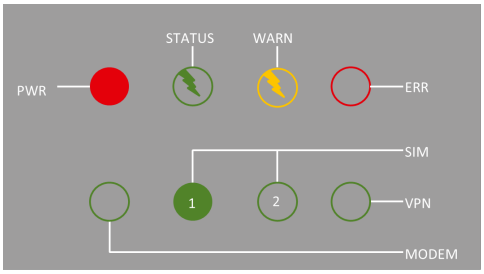
Systemstart:



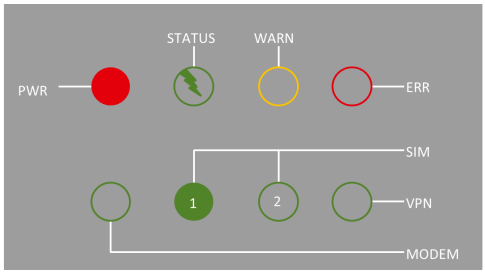
Systemstart erfolgreich:



Einwahl:



Einwahl erfolgreich:



Reset erfolgreich:

STATUS WARN STATUS WARN

Firmwareaktualisierung:

SIM

VPN

PWR ERR PWR ERR

SIM

VPN

MODEM MODEM

2.11.2 *Signalstärke*

Signal: 1-9

(schlechtes Signal, der Router kann nicht korrekt arbeiten, bitte überprüfen Sie die Antennenverbindung und die örtliche Signalstärke des Mobilfunknetzes.)

Signal: 10-19

(Router arbeitet normal)

Signal: 20-31

(Perfektes Signallevel)

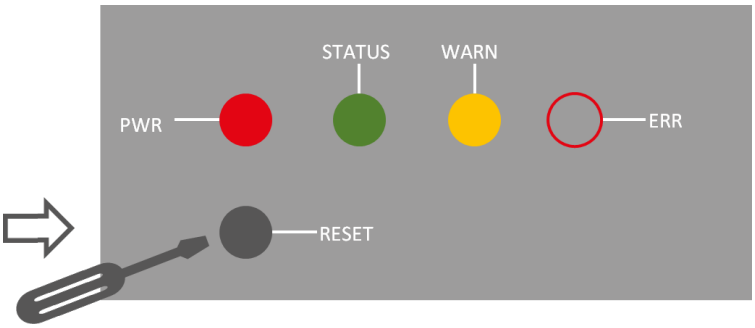
2.12 2.11. Zurücksetzen auf Werkseinstellungen

2.12.1 2.11.1. Hardwaremethode

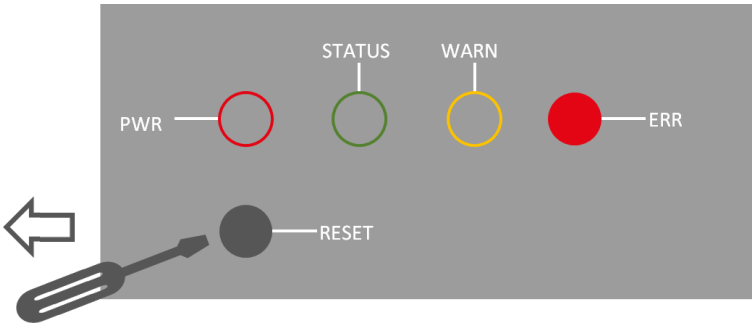
Symbol-Erklärung

 = LED leuchtet  = LED leuchtet nicht  = LED blinkt

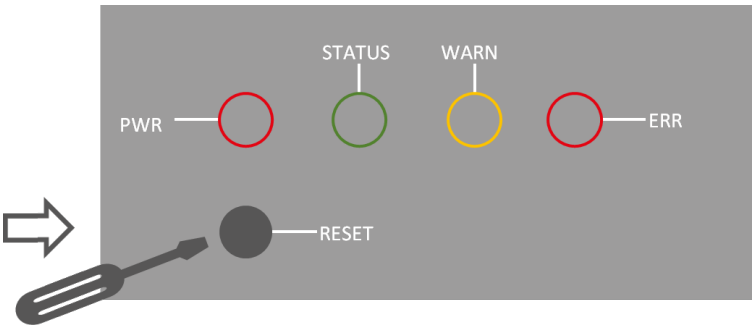
1) Halten Sie die RESET-Taste gedrückt, während Sie den TK800 einschalten:



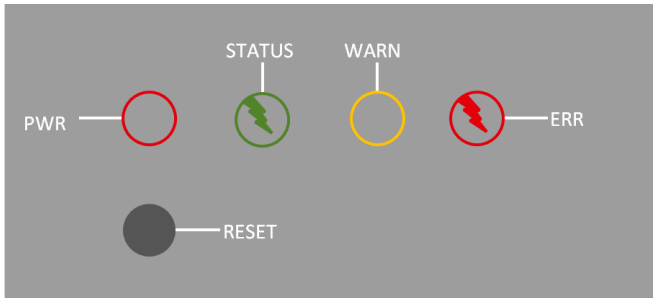
2) Sobald die LED-Leuchte ERROR aufleuchtet (ca. 10 Sekunden nach dem Einschalten), lassen Sie die RESET Taste los:



3) Nach einigen Sekunden leuchtet die LED-Leuchte ERROR nicht mehr. Nun drücken Sie erneut die RESET Taste bis die Error Leuchte blinkt und lassen die Taste dann los:



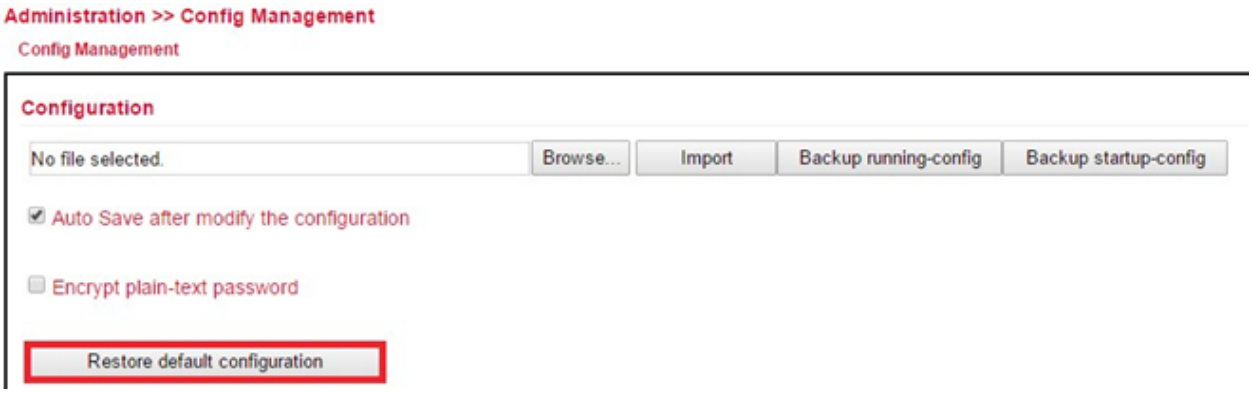
4) Nun blinken die LED-Leuchten ERROR und STATUS, was bedeutet, dass das Zurücksetzen auf die Standardeinstellung erfolgreich war.



Werkseitige Standardeinstellungen	
IP:	192.168.2.1
Netzmaske:	255.255.255.0
Benutzername:	adm
Passwort:	123456
Serieller Parameter:	115200-N-8-1

2.12.2 2.11.2. Webmethode

1) Gehen Sie über das Menü ***Administration*** auf den Unterpunkt ***Config Management***:

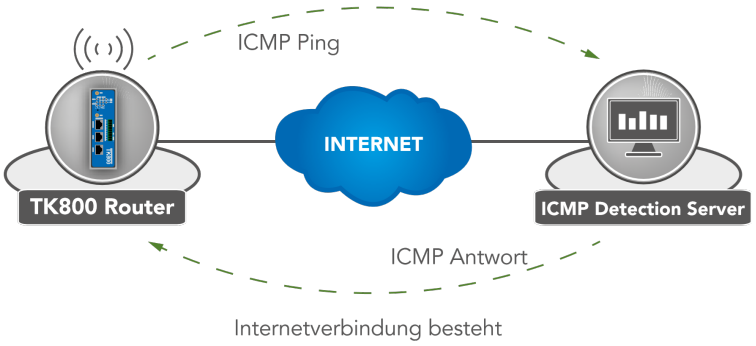


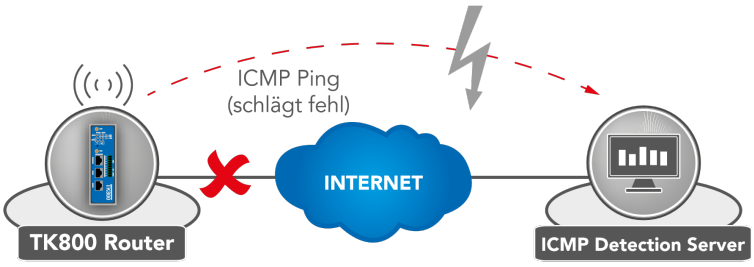
2) Klicken Sie auf ***Restore Default Configuration***, um den TK800 auf seine Standardeinstellungen zurückzusetzen. Nach einigen Sekunden erhalten Sie folgende Meldung. Der Router ist nun erfolgreich zurückgesetzt.

3) Nach einem Klick auf ***reboot*** startet der Router neu und befindet sich in Werkseinstellungen.

2.13 2.12. Watchdog

2.13.1 2.12.1. Selbstständige Überwachung des Routers

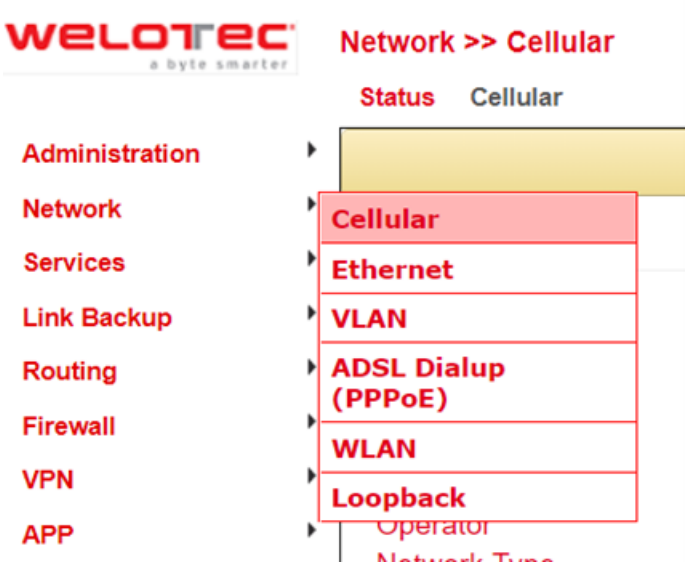




Watchdog greift

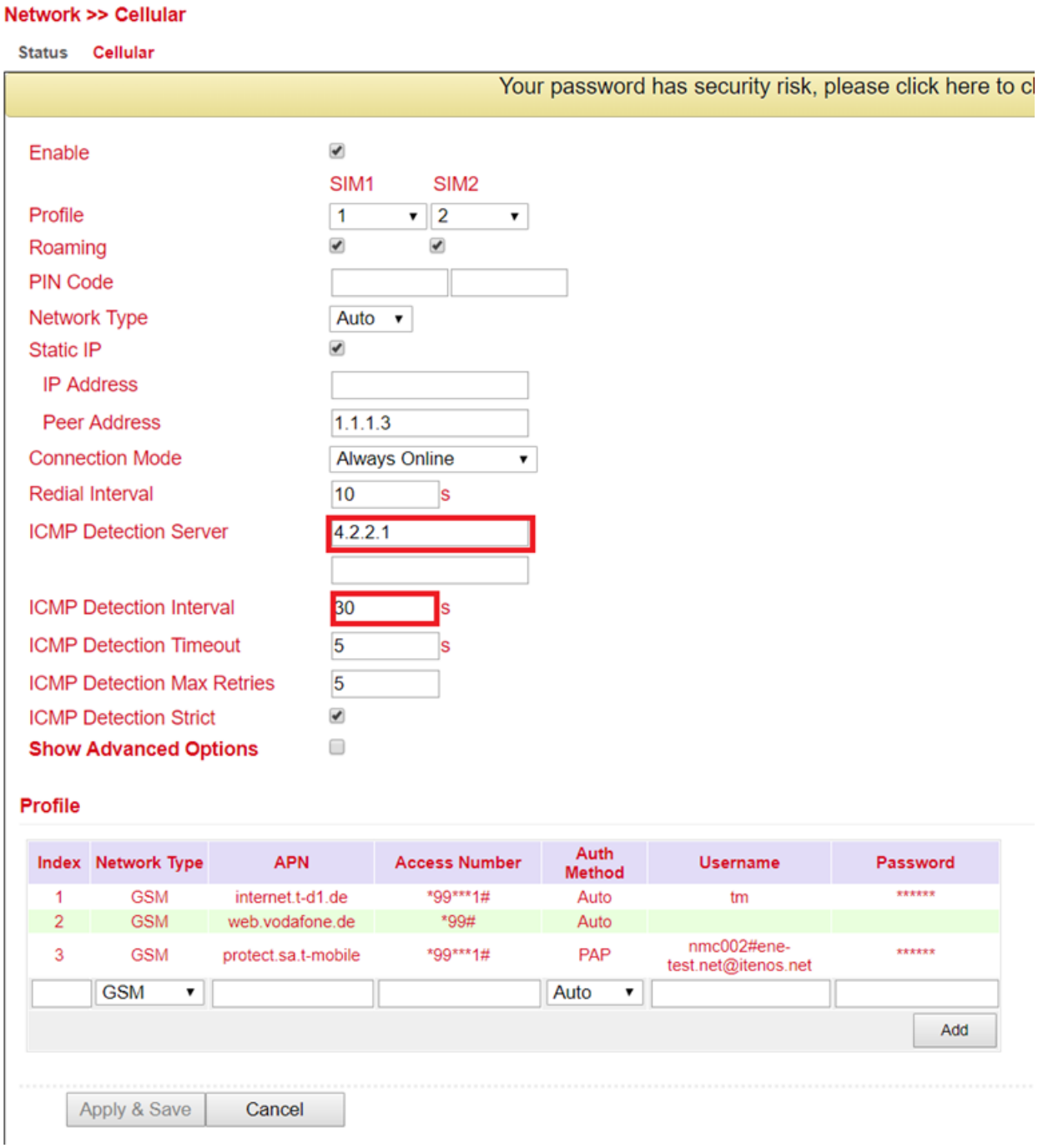
Der Watchdog überwacht den Router hinsichtlich der Internetverbindung. Der Router überprüft selbst, ob wie gewünscht eine Internetverbindung besteht. Dazu sendet er ICMP-Pakete zu einem individuell definierten Server (ICMP-Detection-Server). Sollte diese Abfrage fehlschlagen, startet der Router selbstständig erst die Einwahl neu, dann das Modem, und falls erforderlich das gesamte System. Der Watchdog sorgt für eine zuverlässige Internetverbindung im Mobilfunknetz. Dadurch wird gewährleistet, dass der Router nahezu immer erreichbar ist.

1) Gehen Sie über den Menüpunkt ***Network*** auf den Unterpunkt ***Cellular***



2) Wählen Sie die Registerkarte ***Cellular***

3) Tragen Sie nun einen geeigneten ***ICMP Detection Server*** in das entsprechende Feld ein und ändern Sie das ***ICMP Detection Interval***



Anmerkung: Der eingetragene ICMP-Detection-Server sollte eine sehr hohe Erreichbarkeit haben. Ein Server von Google eignet sich hierfür nicht mehr, da die ICMP-Anfragen dort geblockt werden.

2.14 2.13. Port Mapping / Port Forwarding

2.14.1 2.13.1. Zugriff auf angeschlossene Geräte über das Internet

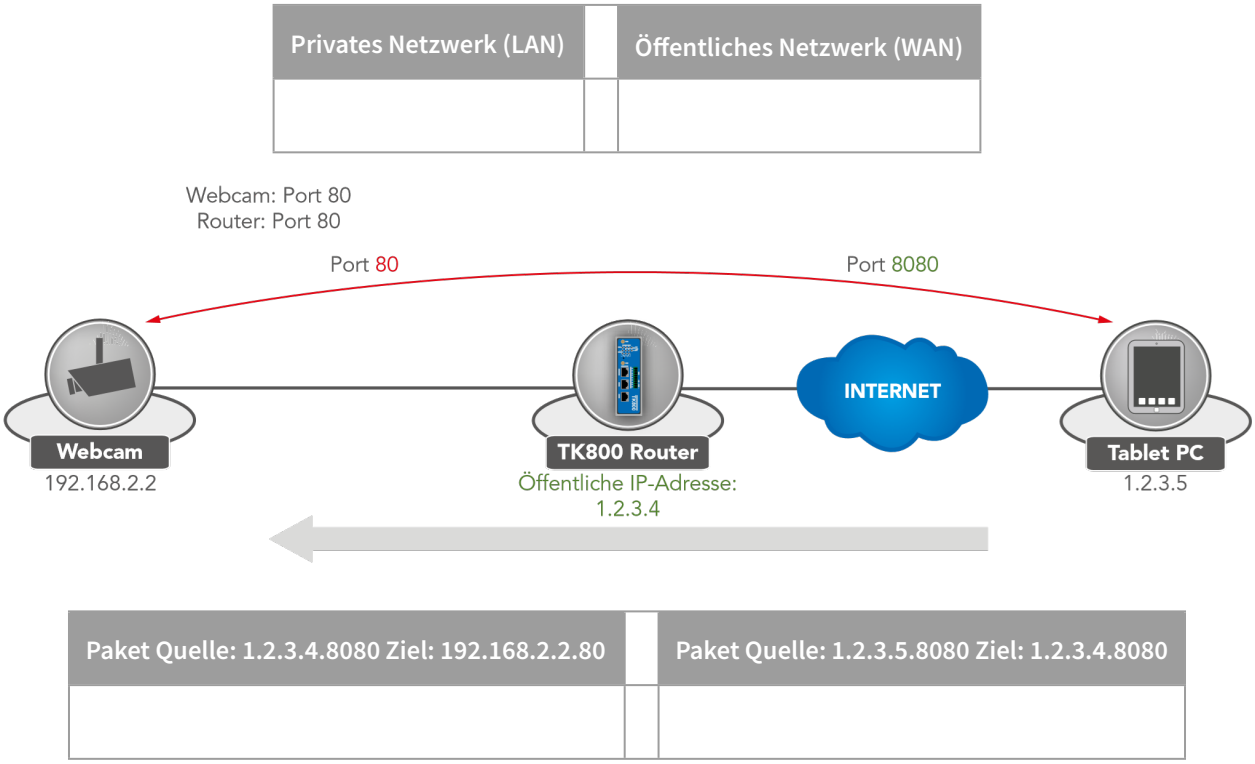
Um über das Internet auf Geräte zuzugreifen, welche an den Welotec Router angeschlossen sind, kann man Port Mapping bzw. Port Forwarding nutzen. Dies wird im TK800 Router über NAT-Regeln konfiguriert.

Hinweis

Für Port Mapping benötigt man eine öffentliche IP-Adresse im Mobilfunknetz (Public IP). Erkundigen Sie sich danach ggfs. bei Ihrem Mobilfunkanbieter oder Dienstleister!

Die Anleitung bezieht sich auf alle TK800 Router mit Firmware ***1.0.0.r10406*** oder höher.

Das folgende Bild veranschaulicht das Anwendungsbeispiel (http verwendet standardmäßig den TCP Port 80):



Erläuterung:

Welotec Router	
LAN IP-Adresse:	192.168.2.1
Subnetzmaske:	255.255.255.0

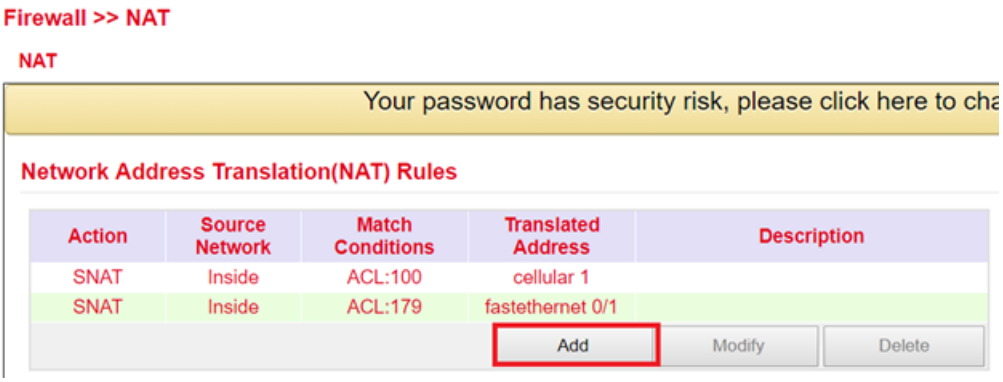
IP Kamera	
LAN IP-Adresse:	192.168.2.2
Subnetzmaske:	255.255.255.0
Standard Gateway	192.168.1.1

Die IP Kamera hat eine Oberfläche, die mit einem Browser über **http://192.168.2.2** erreicht werden kann (Anm.: http-Protokoll hat TCP Port 80).

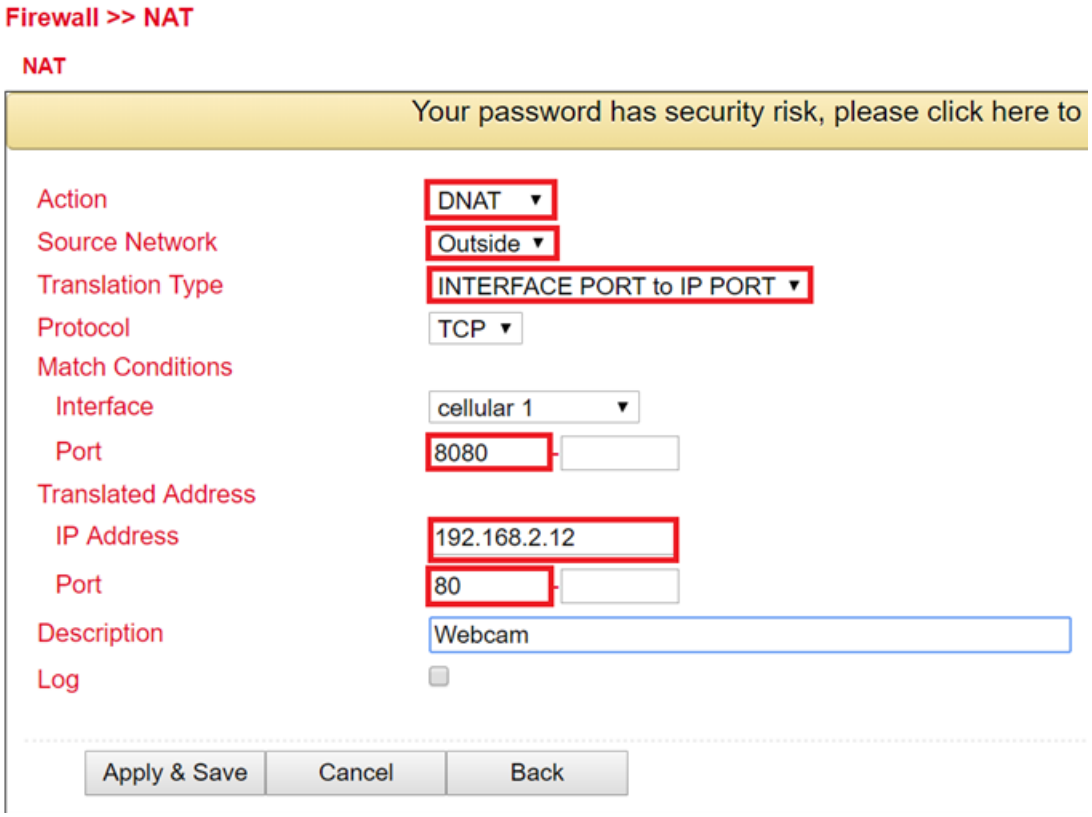
2.14.2 2.13.2. Anleitung zum Port Mapping

1) Gehen Sie über den Menüpunkt ***Firewall*** auf den Unterpunkt ***NAT***

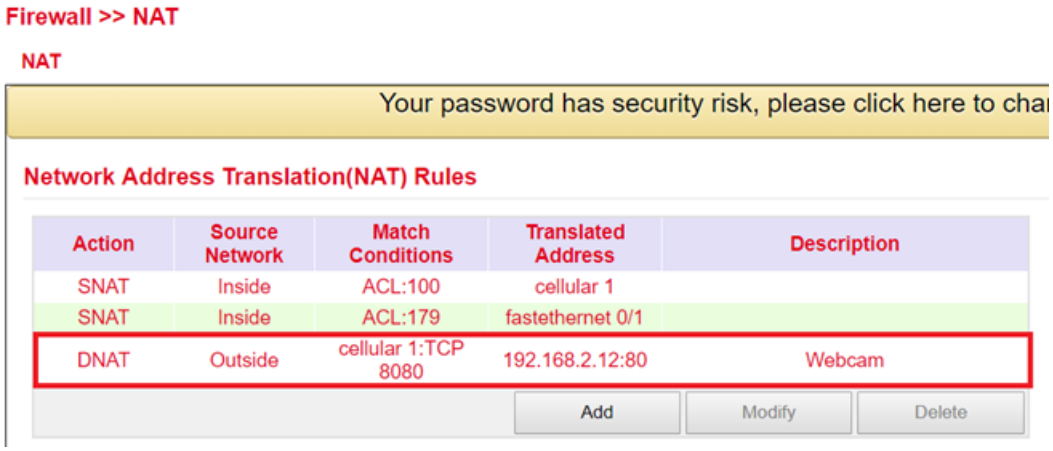
2) Fügen Sie nun mit ***Add*** eine neue NAT-Regel hinzu



3) Tragen Sie die Daten wie in dem Beispiel ein



4) Im Anschluss taucht die NAT Regel wie unten abgebildet in der Tabelle ***Network Address Translation (NAT) Rules*** auf



Die Regel ist nun aktiv. Die entsprechenden Dienste starten sich neu und das Port Mapping ist vollständig eingerichtet.

Für ein funktionierendes Port Mapping ist es hilfreich, wenn man die Einstellungen der angeschlossenen Geräte vorab überprüft. Folgende Checkliste ist dabei hilfreich (nach dem o.g. Beispiel):

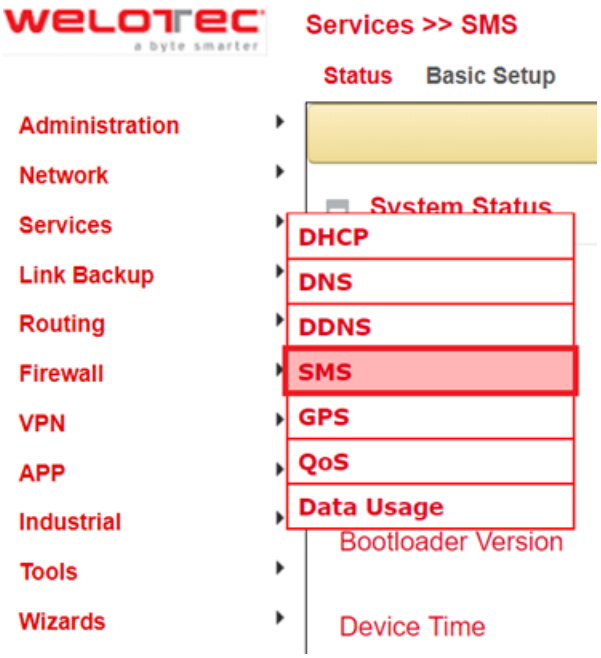
- Hat die Kamera die IP-Adresse 192.168.2.12?
- Antwortet diese bei „ping 192.168.2.12“?
- Ist die Weboberfläche der Kamera über **http://192.168.2.12** erreichbar?
- Ist bei der Kamera als Standard Gateway der Welotec Router eingetragen (192.168.2.1)?

2.15 2.14. SMS-Funktionen

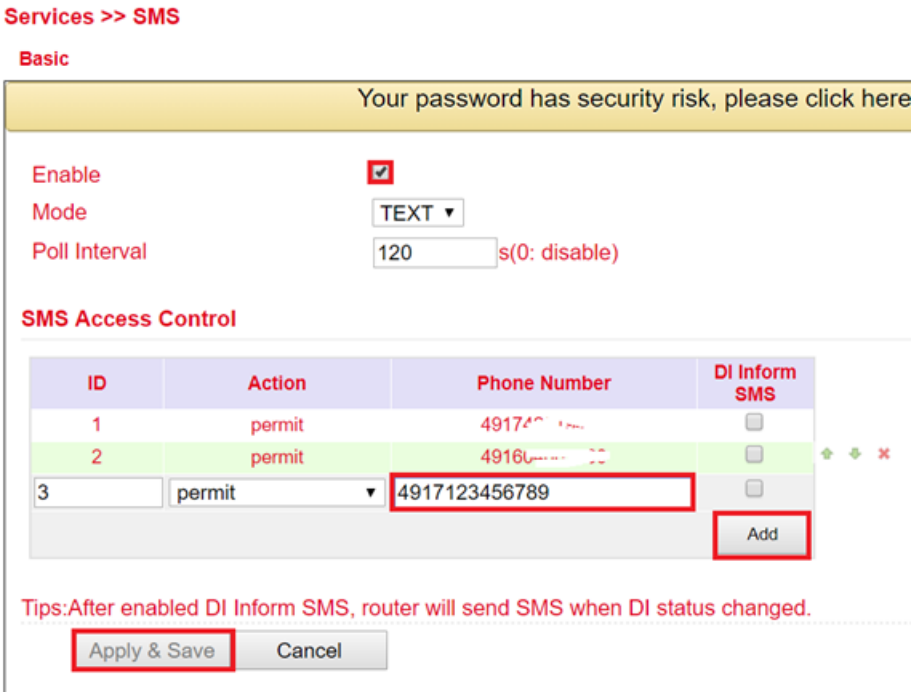
Der TK800 ist per SMS von außen erreichbar und reagiert auf verschiedene Befehle, die per SMS gesendet werden. Man hat die Möglichkeit, den Status des Gerätes abzufragen, die Einwahl zu starten / zu stoppen oder das Gerät neu zu starten.

2.15.1 2.14.1. Statusabfrage / Neustart

1) Gehen Sie über den Menüpunkt ***Network*** auf den Unterpunkt ***SMS***



2) Klicken Sie auf die Checkbox ***Enable***, um die Funktion einzuschalten



3) Geben Sie in die Tabelle ***SMS Access Control*** die Telefonnummern (Phone Number) ein (Format 4917123456789, **kein 0049 oder +49!**), welche SMS an den Router senden dürfen. Tragen Sie als Action „***permit***“ ein.

Wird nun eine SMS mit dem Inhalt ***show*** an die Mobilfunknummer des Routers gesendet, so sendet der Router seinen aktuellen Status als Antwort

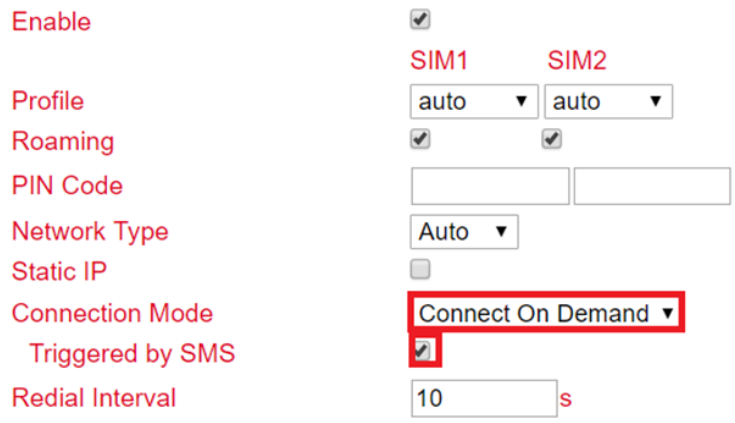
Wird eine SMS mit dem Inhalt ***reboot*** an den Router gesendet, so startet dieser neu. Man kann diesen Prozess auch im Log des Routers verfolgen

2.15.2 2.14.2. Herstellen oder Trennen der Internetverbindung

Nach erfolgreicher Konfiguration können Sie die Internetverbindung des Routers ebenfalls per SMS steuern. Dazu ist es allerdings notwendig, dass der Router auf „Connect On Demand“ steht!

1) Gehen Sie über den Menüpunkt ***network*** auf den Unterpunkt ***cellular***

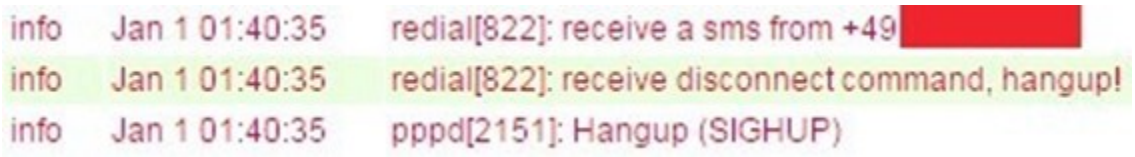
2) Wählen Sie nun den Reiter ***cellular*** aus



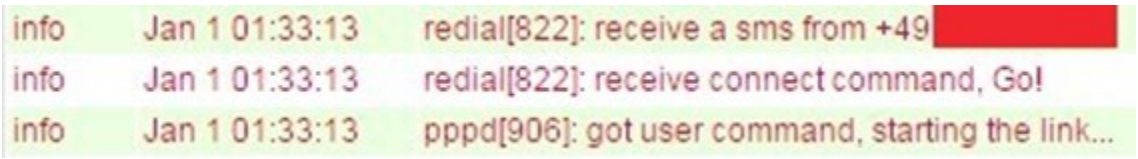
3) Wählen Sie hier unter ***Connection Mode*** den Modus ***Connect on Demand*** aus und aktivieren Sie das Feld ***Triggered by SMS***

Nun können Sie folgende Befehle per SMS an den Router senden:

- ***cellular 1 ppp down*** - trennt die Internetverbindung

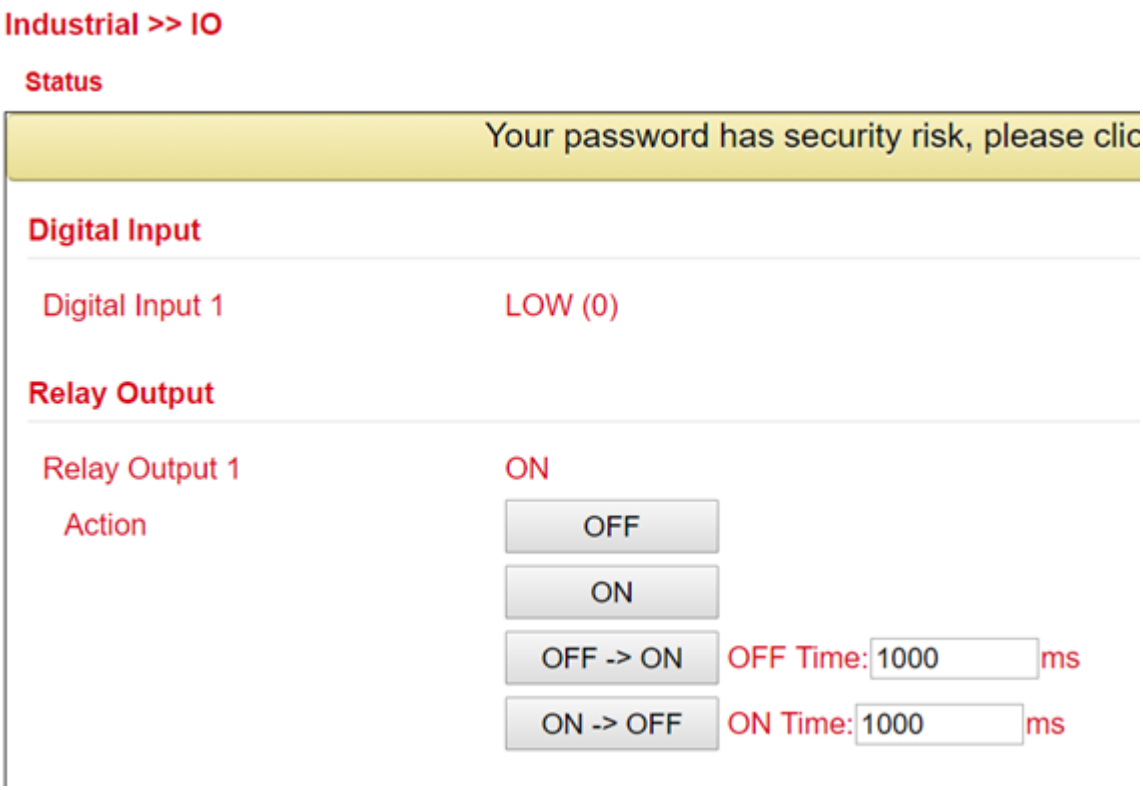


- ***cellular 1 ppp up*** - stellt die Internetverbindung her



2.15.3 2.14.3. Digitales Relay ein- oder ausschalten

Ein weiterer wichtiger SMS-Befehl ist das ein- bzw. ausschalten des digitalen Relays per SMS.

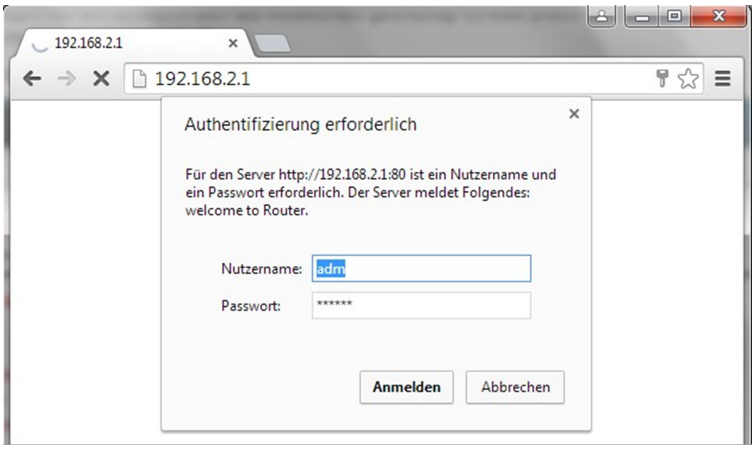


Folgende SMS Befehle können dafür verwendet werden

- *io output 1 on - schaltet das Relay ein*
- *io output 1 off schaltet das Relay aus*

3 3. WEB Konfiguration

Die Router der TK800 Serie verfügen über einen eingebauten Webserver für die Konfiguration. Rufen Sie **http://192.168.2.1** im Browser auf. Geben Sie den Benutzernamen (Standard: ***adm***) und das Passwort (Standard: ***123456***) ein und bestätigen Sie mit ***Anmelden***.



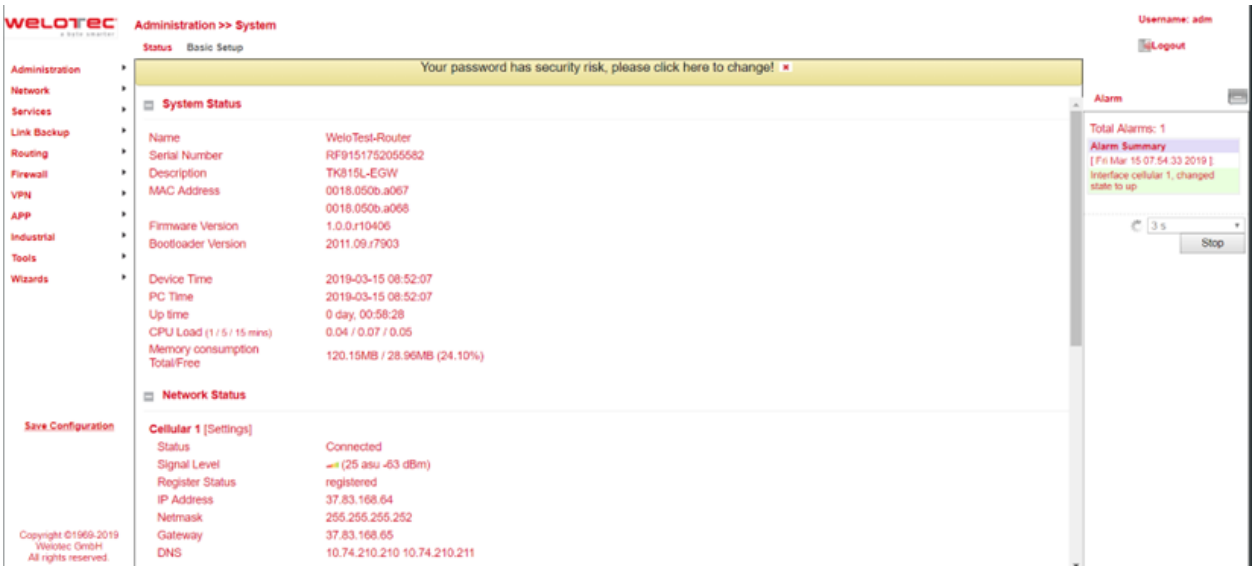
Hinweis

Aus Sicherheitsgründen sollte das Passwort nach dem ersten Login geändert werden. Wählen Sie ein Passwort mit mindestens 10 Stellen, Groß- und Kleinbuchstaben, Sonderzeichen und Zahlen.

Tipp

Der Router erlaubt den parallelen Zugriff von bis zu vier Benutzern über das Webinterface. Es sollte jedoch vermieden werden, gleichzeitig an der Konfiguration des Routers zu arbeiten.

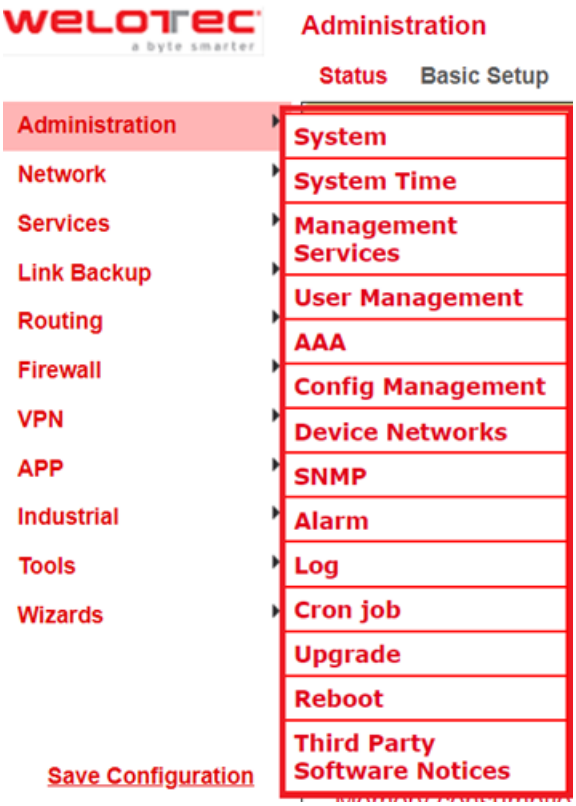
Nach dem erfolgreichen Login erscheint das Webinterface des Routers.



Das Webinterface des TK800 ist in 4 Bereiche aufgeteilt. Auf der linken Seite ist die ***Hauptnavigation*** mit den Punkten Administration, Network usw. Im oberen Bereich ist die ***Detailnavigation***. In diesem Beispiel mit Status (aktiv) und Basic Setup. In der Mitte des Webinterfaces wird der aktuelle Status und die Konfigurationsmöglichkeiten dargestellt. Auf der rechten Seite werden aktive Alarme dargestellt.

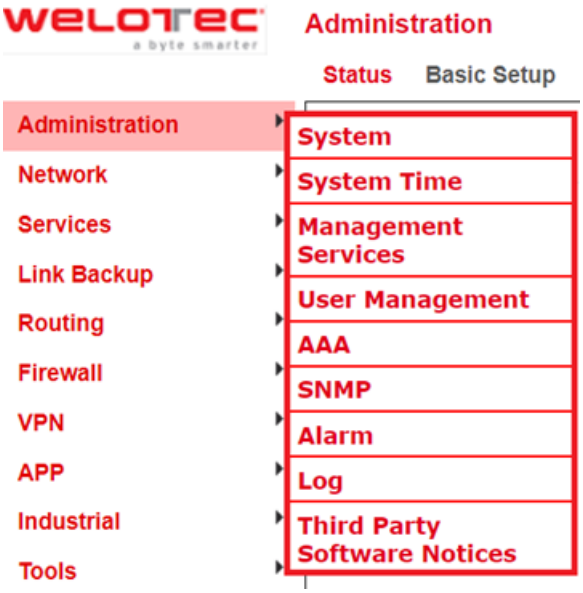
3.1 3.1. Administration

Auf der linken Seite befindet sich der Menüpunkt „***Administration***“. Bei Berühren mit der Maus öffnet sich ein ***Untermenü***. Im Administrationsbereich ist die Statusübersicht und die Konfiguration für die Verwaltung des Routers.



Hinweis

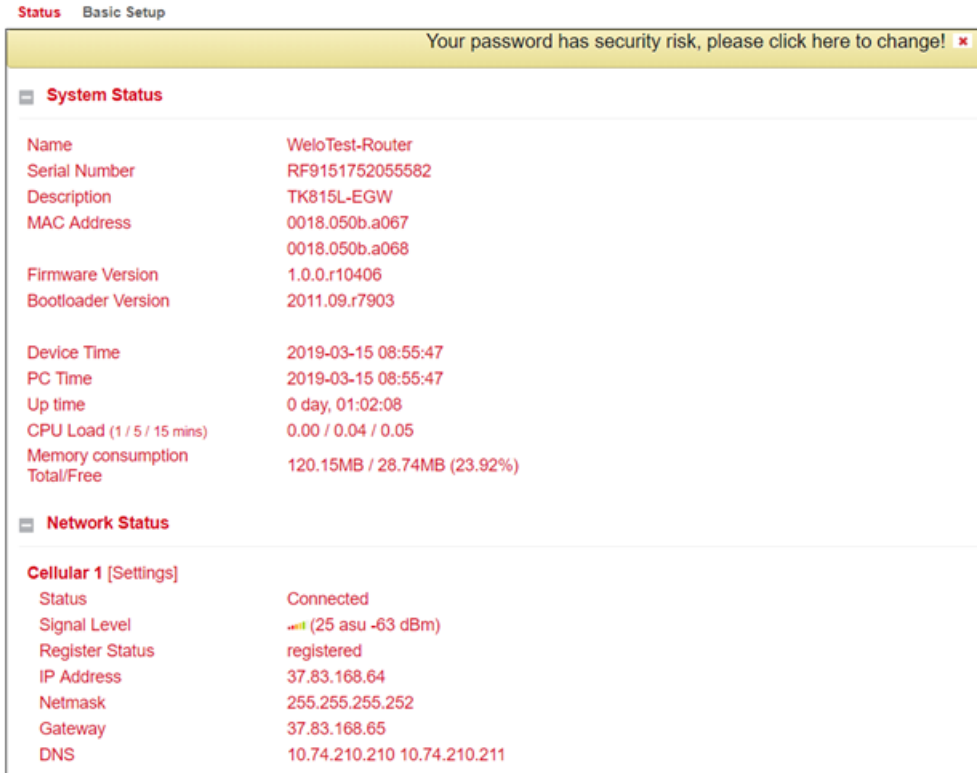
Bei Eingeschränkten Benutzerrechten (nicht Administrator) fehlen im Menü einige Punkte. Eingeschränkte Benutzer können den Router nicht konfigurieren, es fehlt die ***Apply & Save*** Option.



3.1.1 3.1.1. System

3.1.1.1. Status

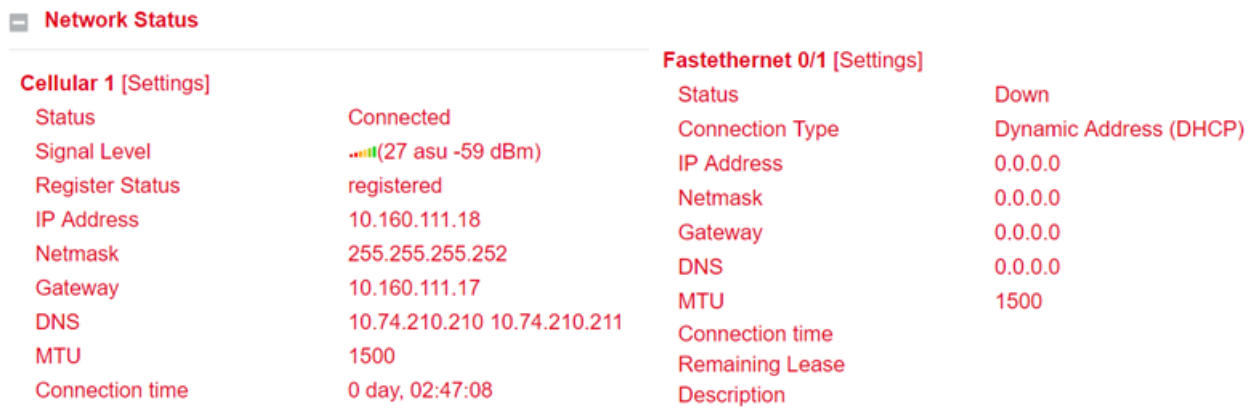
Unter ***Administration > System > Status*** finden Sie die wichtigsten ***Statusinformationen*** des Routers auf einen Blick. Über den Button ***Sync Time*** kann die Uhrzeit vom Router mit der Uhrzeit vom angeschlossenen PC Synchronisiert werden. Wenn Sie zur Anmeldung das Standard-Kennwort nutzen (123456), dann erscheint in einem gelben Balken, dass dieses ein Sicherheitsrisiko darstellt und geändert werden sollte. Dies können Sie mit einem Klick auf den Hinweis tun. Wir empfehlen Ihnen ausdrücklich dies aus Sicherheitsgründen zu tun!



Unter dem System Status befindet sich der Network Status. Durch Klick auf das graue *[+]* erscheinen die Informationen zu den einzelnen Netzwerkschnittstellen. Hier finden Sie alle wichtigen Informationen über den Status der einzelnen Schnittstellen.

Tipp

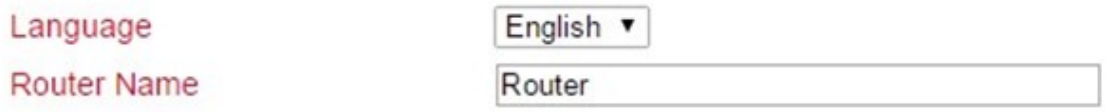
Durch Klick auf ***[Settings]*** neben den einzelnen Schnittstellen (z.B. Cellular 1) kommen Sie direkt zur Konfiguration der Schnittstellen.



Bridge 1 [Settings]	
Status	Up
IP Address	192.168.2.10
Netmask	255.255.255.0
Gateway	0.0.0.0
DNS	0.0.0.0
MTU	1500
Connection time	
Remaining Lease	
Vlan 1 [Settings]	
Status	Down
IP Address	0.0.0.0
Netmask	0.0.0.0
Gateway	0.0.0.0
DNS	0.0.0.0

3.1.1.2. Basic Setup

Unter ***Administration > System > Basic Setup*** können Sie die Sprache des Routers und den Router Namen anpassen. Momentan wird als Sprache nur English unterstützt. Der Router Name kann als eindeutiger Name des Routers genutzt werden. Hier sollte eine aussagekräftige Bezeichnung gewählt werden.



3.1.2 3.1.2. System Time

Um die Koordination zwischen dem TK800 Router und anderen Geräten zu gewährleisten, sollte die Systemzeit auf allen Geräten gleich und die Zeitzone richtig eingestellt sein. Unter ***Administration > System Time*** finden Sie alle Einstellungen für die Systemzeit des TK800 Routers. Die Zeit kann manuell eingestellt werden oder über das Simple Network Time Protocol (SNTP) von einem Zeitserver automatisch aktualisiert werden. Zudem gibt es die Möglichkeit über den NTP Server an den Router angeschlossene Geräte automatisch mit der aktuellen Zeitinformation zu versorgen.

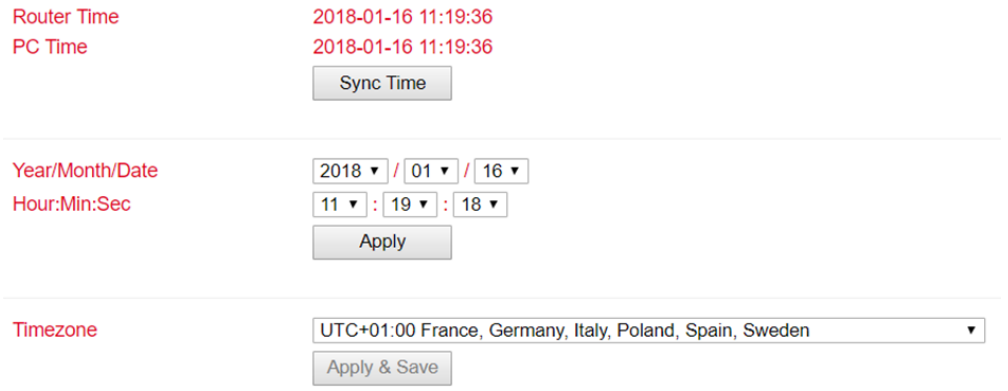
3.1.2.1. System Time Konfiguration

Unter ***Administration > System Time*** befinden sich eine Übersicht und lokale Einstellungen zu der Systemzeit des Routers. Über ***Sync Time*** können Sie die Uhrzeit des Routers mit der Uhrzeit des PC's synchronisieren.

Unter den Einstellungen befindet sich auch die Möglichkeit, die Router Zeit und das Datum manuell einzustellen.

Unter ***Timezone*** kann die aktuelle Zeitzone ausgewählt werden.

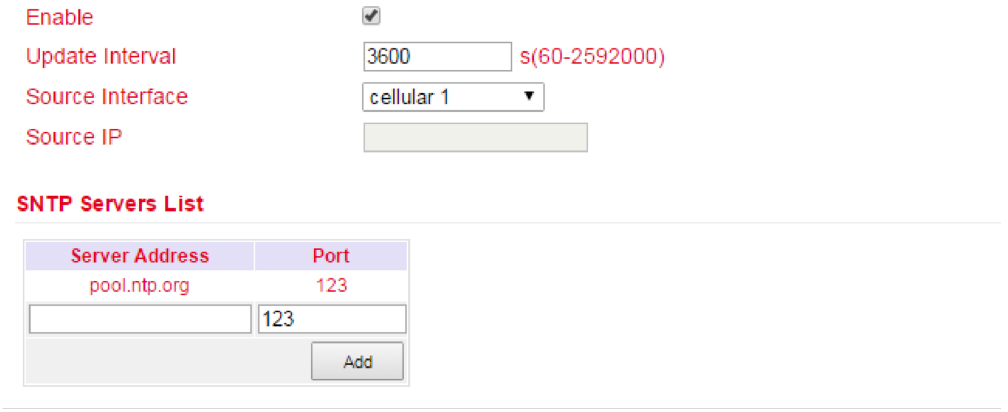
Standard ist hier UTC+1 (Zeitzone in Deutschland, Österreich und der Schweiz).



3.1.2.2. SNTP Client

SNTP (Simple Network Time Protocol) ist ein Protokoll für die Zeitsynchronisierung der Uhren von Netzwerkgeräten. SNTP bietet umfangreiche Mechanismen, um die Uhrzeit über ein Subnetz, Netzwerk oder das Internet zu synchronisieren. In der Regel können durch SNTP Genauigkeiten von 1 bis 50 ms, abhängig von den Eigenschaften der Synchronisierungsquelle und den Routern, erreicht werden. Ziel von SNTP ist es alle Geräte in einem Netzwerk mit einer Uhr zu synchronisieren, um verteilte Anwendungen auf der Basis einer Zeitquelle zu betreiben.

Unter ***Administration > System Time > SNTP Client*** können die Einstellungen für die aktuelle Uhrzeit vorgenommen werden. Der Router kann dann über einen öffentlichen oder privaten Zeitserver die Uhrzeit aktualisieren.



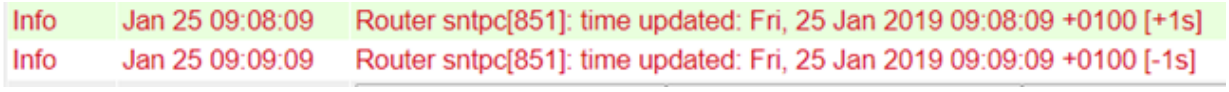
Hinweis

Bevor ein SNTP Server eingerichtet wird, sollte sichergestellt werden, dass der SNTP Server erreichbar ist. Besonders im Falle eines Domain Namens sollte überprüft werden, ob der DNS Server für die Namensauflösung richtig konfiguriert ist.

Hinweis

Es kann entweder ein Source Interface oder eine Source IP konfiguriert werden.

Nach dem erfolgreichen Update der Uhrzeit erscheint folgendes im Log unter ***Administration > Log***.



3.1.2.3. NTP Server

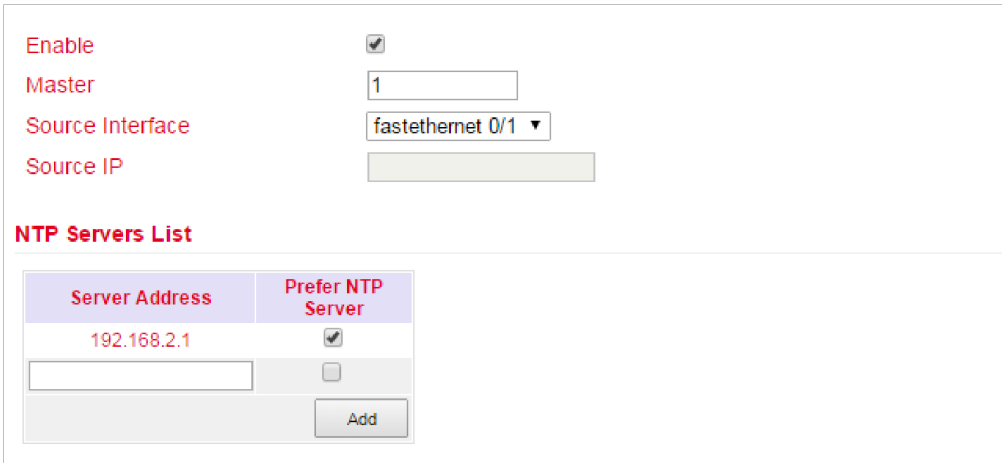
Unter ***Administration > System Time > NTP Server*** befinden sich die Einstellungen für den Zeitserver. In diesem Fall kann der TK800 als Zeitserver für die angeschlossenen Geräte arbeiten.

Über ***Master*** kann das Stratum angegeben werden. Dieses zeigt an, wie präzise der Server ist. Es können Werte zwischen 2 und 15 angegeben werden. Je niedriger, desto näher ist der Router an einer Atom- oder Funkuhr (aus topologischer Sicht).

Das ***Source Interface*** gibt an, an welchem Interface die Geräte den NTP-Dienst des Routers anfragen können. Alternativ dazu kann eine ***Source IP*** bestimmt werden, über die der NTP-Dienst bereitgestellt wird.

Hinweis

Wichtig ist, dass NTP Server und NTP-Client unabhängig voneinander arbeiten, das bedeutet auch, dass sowohl bei NTP-Client wie auch bei NTP-Server ein NTP-Dienst aus dem Internet einzutragen ist. Dazu wird die Adresse des NTP-Dienstes unter ***Server Address*** eingetragen. Es ist möglich mehrere Dienste anzugeben.



3.1.3 3.1.3. Management Services

Unter ***Administration > Management Services*** kann der Zugriff auf das Webinterface mit HTTP und HTTPS sowie auf das Command Line Interface (CLI) via Telnet und SSH konfiguriert werden.

HTTP

HTTP ist die Abkürzung für Hypertext Transfer Protocol und wird genutzt, um auf das Webinterface des Routers zuzugreifen.

HTTPS

HTTPS ist die Abkürzung für Hypertext Transfer Protocol Secure und nutzt SSL (Security Socket Layer) für die verschlüsselte Übertragung von HTTP.

TELNET

TELNET wird genutzt um auf das Command Line Interface (CLI) des Routers zuzugreifen.

SSH

SSH ist die Abkürzung für Secure Shell und ist ein zu Telnet vergleichbarer verschlüsselter Dienst.

Konfiguration

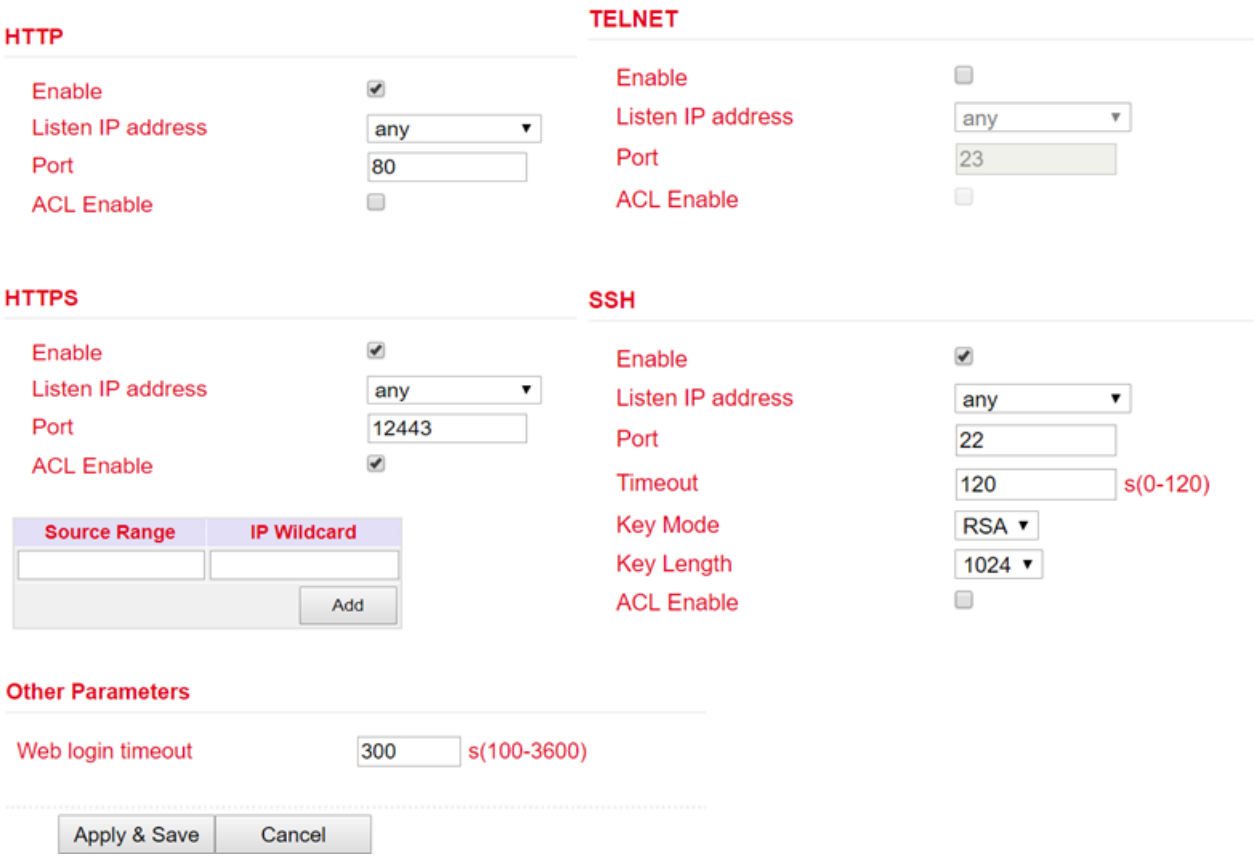
Für jeden Dienst kann ausgewählt werden, ob er aktiviert oder deaktiviert werden soll und auf welcher IP-Adresse dieser Dienst angesprochen werden darf.

Setzen Sie hierfür einfach den Haken bei ***Enable*** oder entfernen diesen. Unter ***Port*** kann der TCP Port für den jeweiligen Dienst ausgewählt werden. Mit ACL Enable kann für jeden Port eine Zugriffsbeschränkung eingerichtet werden. Wird **ACL Enable** aktiviert, können Sie in den Feldern Source Range und IP Wildcard eintragen, welche IP-Adresse oder IP-Adresskreise über diesen Port auf den Router zugreifen dürfen. Für SSH kann zudem noch das ***Timeout*** für eine SSH Session zum Router definiert werden.

Wenn während der Timeout Zeit keine Aktivität stattfindet wird die Verbindung beendet. Unter ***Key Mode*** und ***Key Length*** kann der Verschlüsselungsstandard und die Schlüssellänge gewählt werden.

Über ***Other Parameters*** können Sie den ***Web login timeout*** setzen. Dieser gibt an, wie lange eine Webinterface Session bestehen bleibt, wenn keine Eingabe erfolgt.

Wenn die Timeout Zeit abgelaufen ist, ohne dass Sie eine Eingabe gemacht haben, dann wird der angemeldete Benutzer automatisch ausgeloggt.



3.1.4

3.1.5 3.1.4. User Management

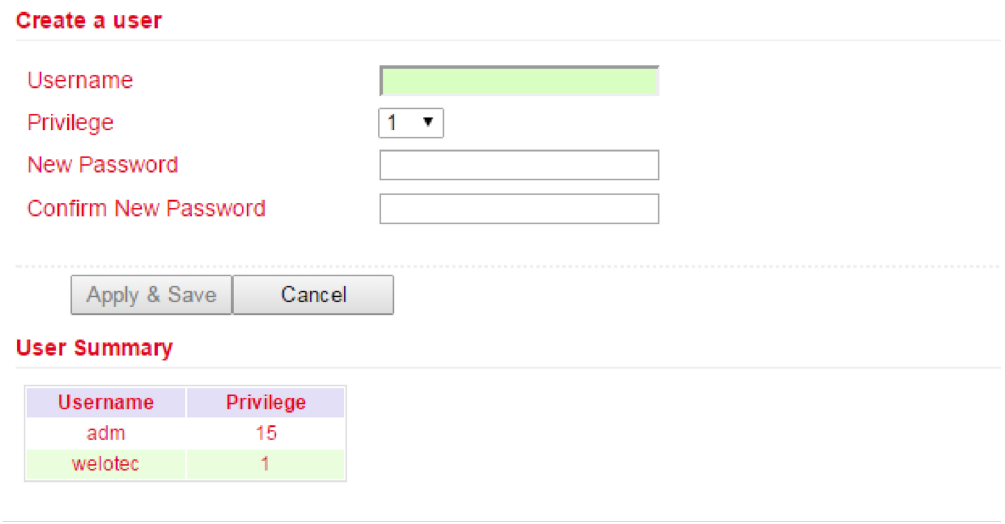
Unter ***Administration*** > ***User Management*** können die Benutzer, die Zugriff auf den Router haben, konfiguriert werden. Der Router unterscheidet zwischen dem Administrator und dem Standardbenutzer. Der Administrator wird vom System angelegt (adm). Der Administrator kann weitere Standardbenutzer mit eingeschränkten Rechten anlegen.

Der Benutzer Administrator eignet sich zur Konfiguration und Management des Routers. Der Standardbenutzer eignet sich zum Überwachen und Überprüfen des Routers.

3.1.4.1. Create a User

Unter ***Administration*** > ***User Management*** > ***Create a User*** können Sie weitere Benutzer anlegen.

Es muss ein ***Username*** und ***Password*** angelegt und die ***Berechtigung (Privilege)*** eingetragen werden. Privilege 1 bis 14 ist für Standardbenutzer (Nur Leserechte) und Privilege 15 für Administratoren (Voller Zugriff). Unter ***User Summary*** befindet sich eine Liste mit allen Benutzern und die zugehörigen Rechte (Privilege).



Hinweis

Ein sicheres Passwort sollte aus mindestens 8 Zeichen bestehen und möglichst Groß- / Kleinschreibung, Zahlen und Sonderzeichen enthalten. Der Username root ist für das Betriebssystem des Routers reserviert.

3.1.4.2. Modify a User

Wenn Sie Anpassungen an Benutzern vornehmen möchten, dann können Sie diese unter ***Administration*** > ***User Management*** > ***Modify a User*** bearbeiten. Es können die Berechtigungen und Passwörter geändert werden.

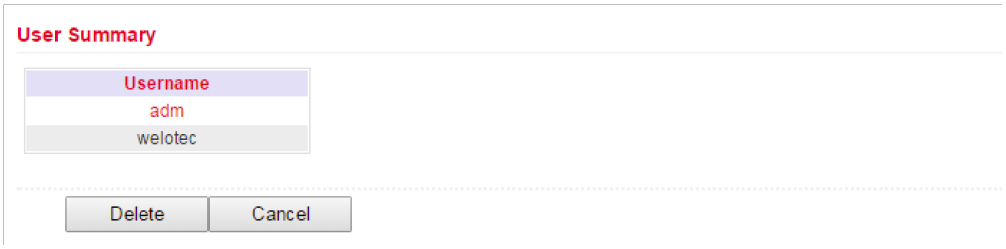
Unter ***User Summary*** kann ein Benutzer ausgewählt und dann unter ***Modify a user*** bearbeitet werden.

Hinweis

Bei Auswahl des Benutzers adm kann ab der Firmware Version V1.0.0.r10406 der Benutzername geändert werden, z.B. in admin. Denken Sie bitte immer daran das Standardkennwort (123456) des Benutzers adm in ein sicheres Kennwort zu ändern.

3.1.4.3. Remove Users

Unter ***Administration*** > ***User Management*** > ***Remove Users*** können Sie Benutzer vom TK800 löschen. Wählen Sie unter ***User Summary*** den Benutzer, der gelöscht werden soll, und löschen diesen über den ***Delete*** Button.



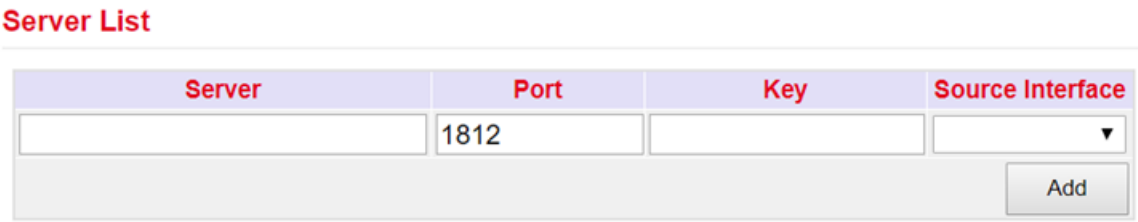
3.1.6 3.1.5. AAA

AAA oder Triple-A steht für ***Authentifizierung (Authentication), Autorisierung (Authorization) und Abrechnung (Accounting)***. Hierbei übernimmt die Authentifizierung die Zugriffssteuerung, ob ein Nutzer das Gerät oder das Netzwerk nutzen darf. Die Autorisierung überprüft, welche Dienste der Nutzer im Netzwerk nutzen darf. Durch die Abrechnung wird sichergestellt, dass alle Zugriffe und Ereignisse und die Nutzung von Ressourcen im Netzwerk richtig protokolliert werden.

Bei AAA müssen nicht alle Sicherheitsdienste genutzt werden. Es ist auch möglich das in einem Netzwerk nur ein oder zwei Dienste genutzt werden. Eine AAA Infrastruktur ist in der Regel als Client - Server Architektur aufgebaut. Der TK800 agiert hier als AAA Client. Hierfür wird Radius, Tacacs+ und LDAP unterstützt.

3.1.5.1. Radius

Radius steht für ***Remote Authentication Dial-In User Service*** und ist ein Client-Server-Protokoll, welches zur Authentifizierung, Autorisierung und zum Accounting dient.

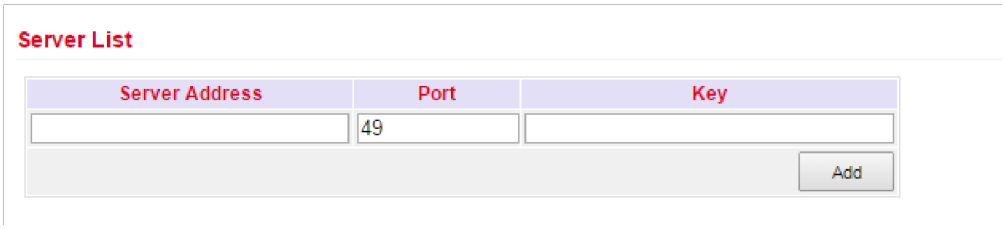


Sie können hier den FQDN oder die IP-Adresse des Servers, den Port, den Key für den Radius Server und das Source Interface eingeben.

3.1.5.2. Tacacs+

Tacacs+ steht für ***Terminal Access Controller Access Control System*** und ist ein Client-Server-Protokoll, welches zur Authentifizierung, Autorisierung und zum Accounting dient.

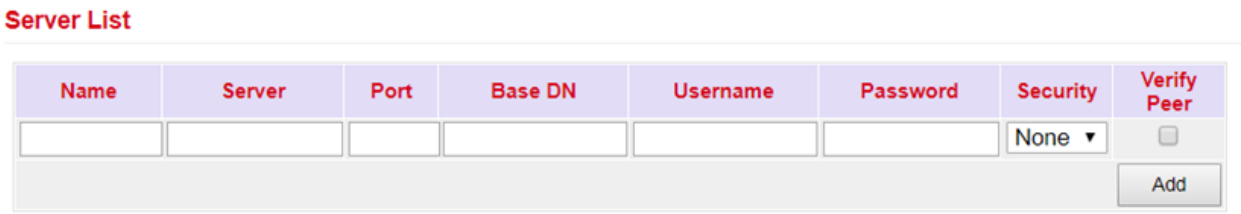
Es dient der Client-Server-Kommunikation zwischen AAA-Servern und einem Network Access Server (NAS).



Sie können hier die entsprechenden Daten bei ***Server Address***, ***Port*** und ***Key*** eintragen.

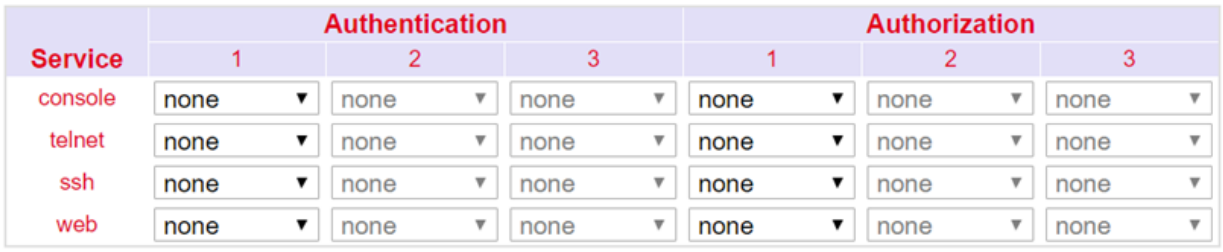
3.1.5.3. LDAP

LDAP steht für ***Lightweight Directory Access Protocol*** und eignet sich für die Abfrage und Modifikation von Informationen aus Verzeichnisdiensten. LDAP basiert auf dem Client-Server Modell.



Tragen Sie hier die Daten für Ihren LDAP Server ein.

3.1.5.4. AAA Settings



3.1.7 3.1.6. Config Management

Unter ***Administration*** > ***Config Management*** kann die aktuelle Konfiguration abgespeichert, eine bestehende Konfiguration hochgeladen oder der Router auf die Standardkonfiguration zurückgesetzt werden.

Import einer bestehenden Konfiguration

Um eine bestehende Konfiguration zu importieren muss über ***Browse…*** eine bestehende Konfigurationsdatei ausgewählt werden. Nachdem die richtige Datei gewählt wurde kann über ***Import*** die Konfiguration in den Router geladen werden. Nach dem erfolgreichen Lesen der Konfiguration bietet der Router einen Button zum Restart. Nach dem Restart ist die neue Konfiguration im Router.

Abspeichern einer bestehenden Konfiguration

Über ***Backup running-config*** kann die aktuelle Konfiguration inkl. der nicht bestätigten Änderungen im Betrieb heruntergeladen werden. Über ***Backup startup-config*** kann die Konfiguration ohne die nicht bestätigten Änderungen heruntergeladen werden.

Automatisches Speichern

Wenn der Haken vor ***Auto Save after modify the configuration*** gesetzt ist, werden alle Änderungen im Router direkt aktiv und sind auch nach dem Neustart verfügbar. Wenn der Haken nicht gesetzt ist, gehen die Änderungen beim Neustart verloren. Die Änderungen können jedoch alternativ über den unteren Punkt in der linken Navigation, ***Save Configuration***, gespeichert werden.

Konfiguration auf Werkseinstellungen zurücksetzen

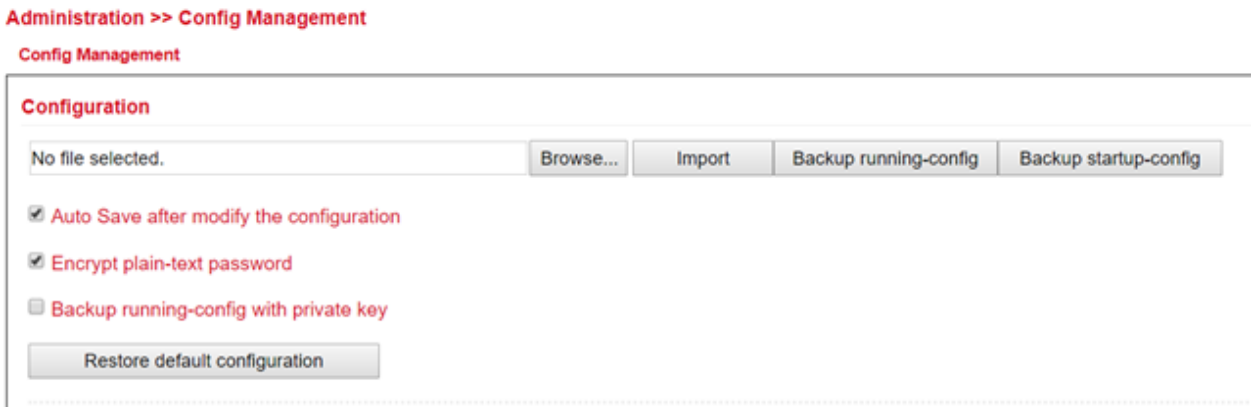
Über ***Restore default configuration*** kann die Konfiguration des Routers auf die Standardeinstellungen zurückgesetzt werden.

Passwörter in der Konfigurationsdatei verschlüsseln

Um Passwörter in der Konfigurationsdatei nicht im Klartext anzuzeigen, setzten Sie den Haken bei ***Encrypt plain-text password***.

Sichern der running-config inklusive des privaten Schlüssels

Um die running-config zusätzlich mit den importierten privaten Schlüsseln (private key) aus der Zertifikatsverwaltung zu sichern, setzen Sie den Haken bei **Backup running-config with private key**



3.1.8 3.1.7. Device Networks

Hinweis

Diese Funktion wird nicht unterstützt!

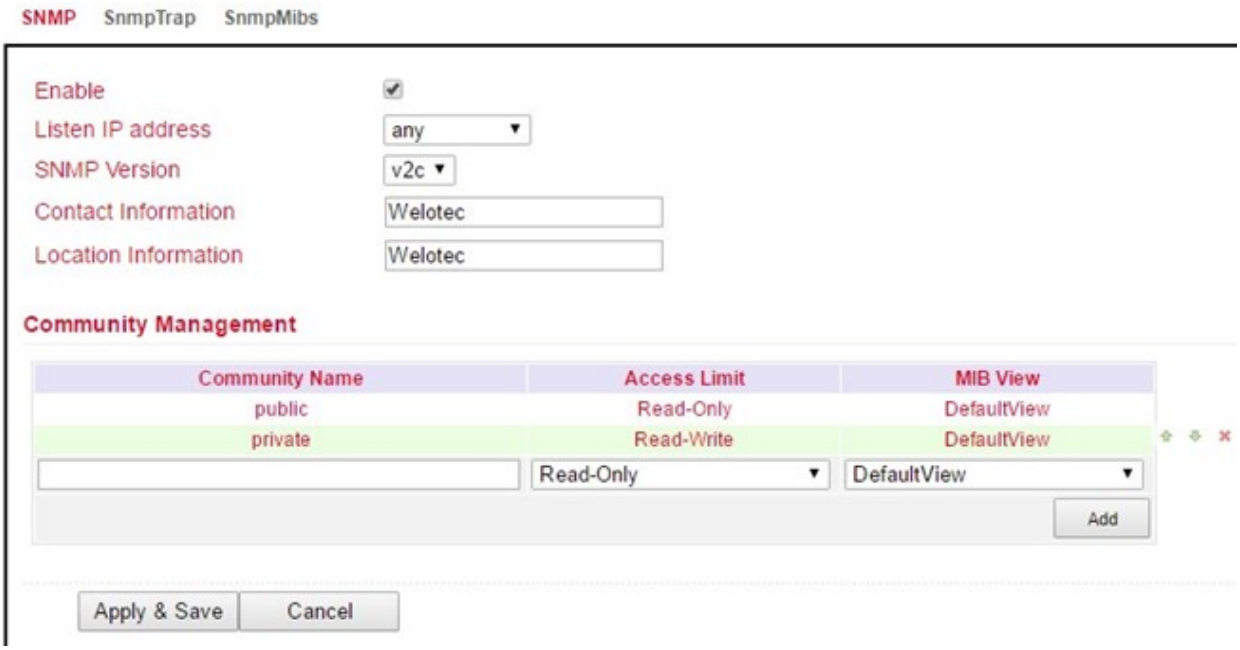
3.1.9 3.1.8. SNMP

Das Simple Network Management Protocol (**SNMP**; Deutsch Einfaches Netzwerkverwaltungsprotokoll) ist ein Netzwerkprotokoll, das von der IETF entwickelt wurde, um Netzwerkelemente (z. B. Router, Server, Switches, Drucker, Computer usw.) von einer zentralen Station aus überwachen und steuern zu können. Das Protokoll regelt dabei die Kommunikation zwischen den überwachten Geräten und der Überwachungsstation. SNMP beschreibt den Aufbau der Datenpakete, die gesendet werden können, und den Kommunikationsablauf. Es wurde dabei so ausgelegt, dass jedes netzwerkfähige Gerät mit in die Überwachung aufgenommen werden kann.

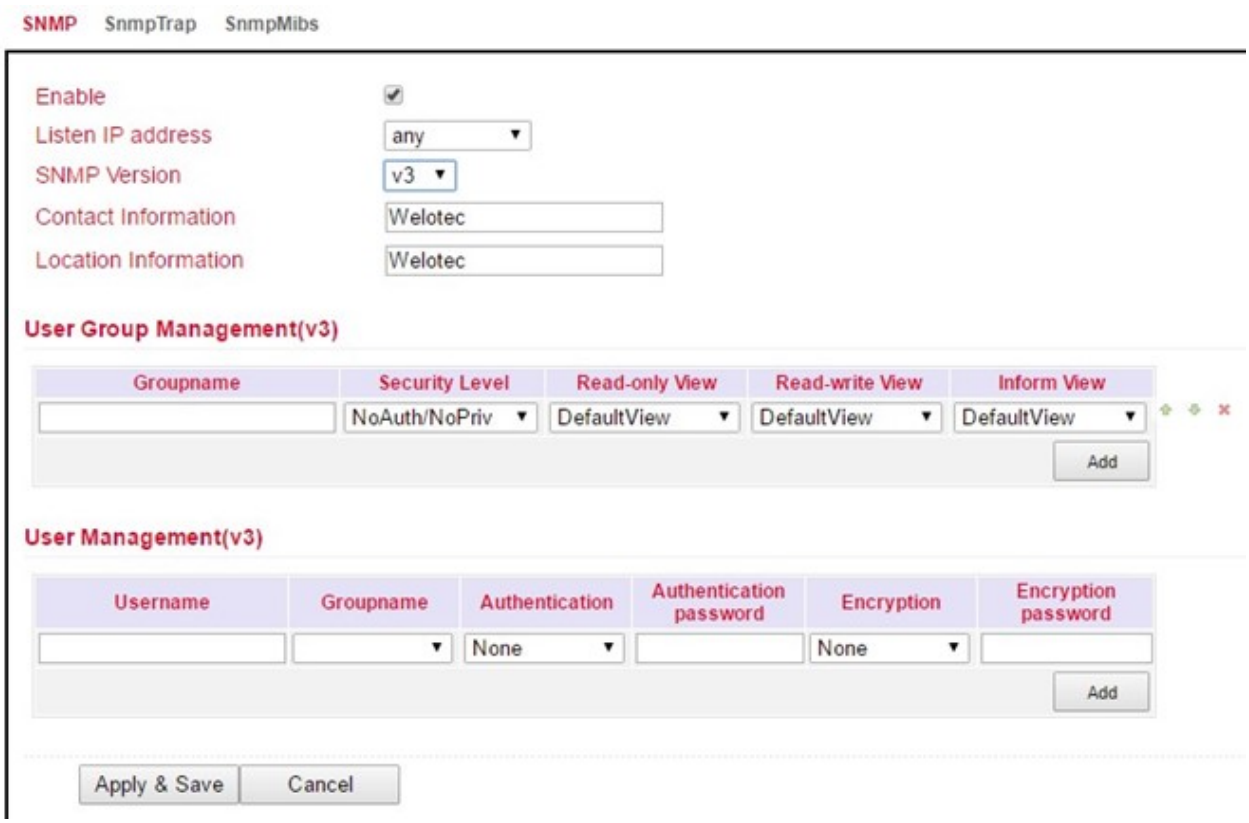
3.1.8.1. SNMP Konfiguration

Es werden die SNMP Versionen v1, v2c und v3 unterstützt.

SNMPv1 und SNMPv2 benutzen den Community Name zur Authentifizierung mit ***Nur-Lesen*** und ***Lesen-Schreiben*** Rechten. Unter ***Listen IP address*** kann die IP-Adresse ausgewählt werden, unter welcher der SNMP Dienst zur Verfügung steht.



SNMPv3 unterstützt Benutzernamen und Passwort zur Authentifizierung. Ein Gruppenmanagement ist implementiert. Dies ist ein Vorteil gegenüber den SNMPv1 und SNMPv2 Versionen, da hier gezielt einzelne Benutzer für die Zugriffe berechtigt werden können (s. folgende Abbildung).

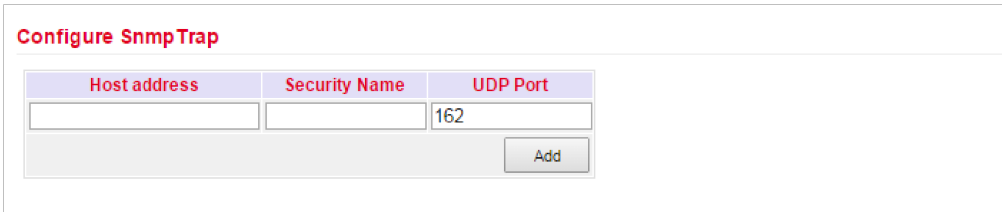


Bei SNMPv3 gibt es ein Gruppen- und Benutzermanagement.

Authentication unterstützt SHA oder MD5.
Encryption unterstützt AES oder DES.

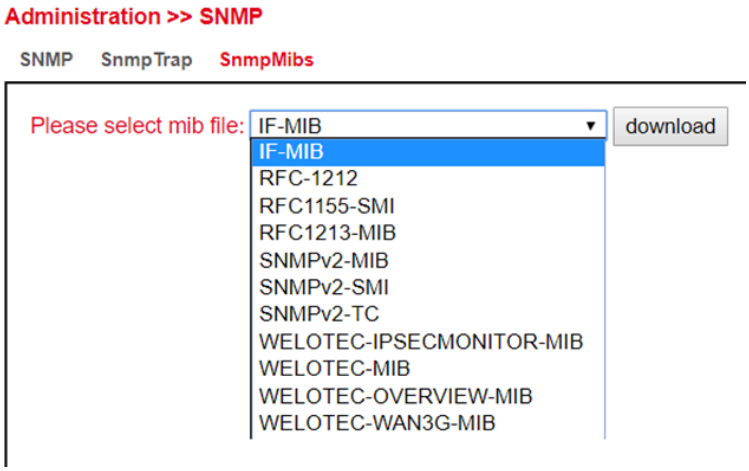
3.1.8.2. SnmpTrap

Es kann ein SnmpTrap Server eingegeben werden. Hierbei kann der Router aktiv SNMP Nachrichten an den SNMP Management Server schicken und wartet nicht, bis er eine SNMP Anfrage vom Management Server bekommt.



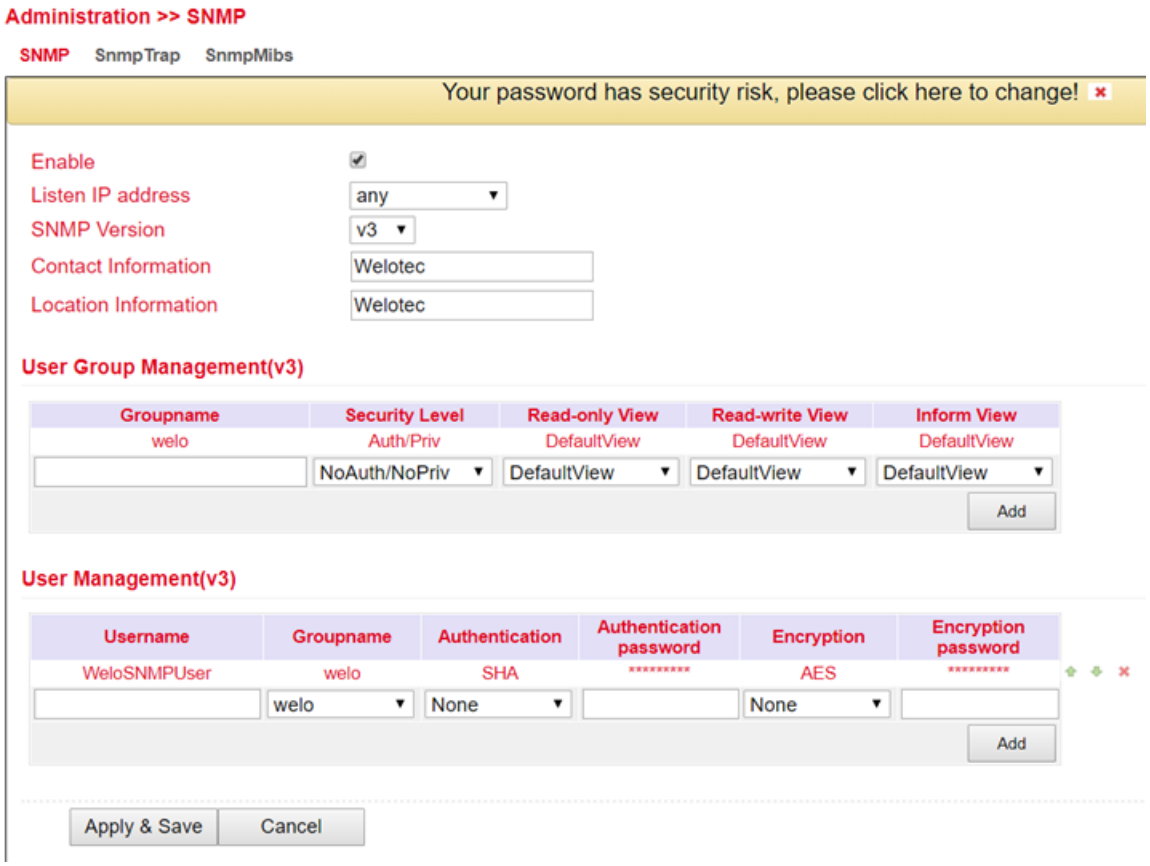
3.1.8.3. SnmpMibs

Die ***SnmpMibs*** zur Abfrage des Routers können Sie an dieser Stelle herunterladen und für entsprechende Auswertungen nutzen. Wählen Sie bitte das gewünschte MIB-File und klicken dann den download Button.



3.1.8.4. SNMP Mibs mittels SNMPWALK auslesen.

1) ***SNMP konfigurieren,*** wie z.B. unten gezeigt:



Auslesen der oben eingegebenen Daten per SMTPWALK auf z.B. einem LINUX-Rechner:

snmpwalk -v3 -u WeloSNMPUser -l AuthPriv -a SHA -A 123456789 -x AES -X 123456789 10.255.229.10

snmpwalk -v3 -u WeloSNMPUser -l AuthPriv -a SHA -A 123456789 -x AES -X 123456789 udp6:[2a02:d20:8:c01::1]

2) *MIBS vom TK800 herunterladen*

3) **MIBS einlesen** (entweder über einen LINUX-Rechner oder einen gängigen MIB-Browser)

mkdir -p .snmp/mibs cp Downloads/WELOTEC* .snmp/mibs/ danach sind die folgenden MIBS vorhanden:

WELOTEC-MIB

WELOTEC-OVERVIEW-MIB

WELOTEC-PORTSETTING-MIB

WELOTEC-SERIAL-PORT-MIB

WELOTEC-SYSTEM-MAN-MIB

WELOTEC-WAN3G-MIB

3) **SNMPWALK Starten** (entweder über einen LINUX-Rechner oder einen gängigen MIB-Browser)

snmpwalk -m +WELOTEC-MIB -v3 -u WeloSNMPUser -l AuthPriv -a SHA -A 123456789 -x AES -X 123456789 192.168.2.1 WELOTEC

WELOTEC-MIB::ihOverview.1.0 = STRING: „TK800“

WELOTEC-MIB::ihOverview.2.0 = STRING: „RF9151408241109“

WELOTEC-MIB::ihOverview.3.0 = STRING: „2011.09.r7903“

WELOTEC-MIB::ihOverview.4.0 = STRING: „1.0.0.r9919“

WELOTEC-MIB::ihWan3g.1.1.1.0 = INTEGER: 3

WELOTEC-MIB::ihWan3g.1.1.2.0 = INTEGER: 1

WELOTEC-MIB::ihWan3g.1.1.3.0 = Hex-STRING: 0B 00 00 00

WELOTEC-MIB::ihWan3g.1.1.4.0 = Timeticks: (149600) 0:24:56.00

WELOTEC-MIB::ihWan3g.1.1.5.0 = INTEGER: 11

WELOTEC-MIB::ihWan3g.1.1.6.0 = INTEGER: 2

WELOTEC-MIB::ihWan3g.1.1.7.0 = INTEGER: 0

WELOTEC-MIB::ihWan3g.1.1.8.0 = INTEGER: 2

WELOTEC-MIB::ihWan3g.1.1.9.0 = INTEGER: 21

WELOTEC-MIB::ihWan3g.1.1.10.0 = Counter32: 2698992

WELOTEC-MIB::ihWan3g.1.1.11.0 = Counter32: 35344140

WELOTEC-MIB::ihWan3g.1.2.1.1.0 = STRING: „860461024084629“

WELOTEC-MIB::ihWan3g.1.2.1.2.0 = STRING: „262010052709611“

WELOTEC-MIB::ihWan3g.1.2.1.3.0 = „“

WELOTEC-MIB::ihWan3g.1.2.1.4.0 = „“

WELOTEC-MIB::ihWan3g.1.2.1.5.0 = „“

WELOTEC-MIB::ihWan3g.1.2.2.1.0 = INTEGER: 0

WELOTEC-MIB::ihWan3g.1.2.2.2.0 = INTEGER: 0

WELOTEC-MIB::ihWan3g.1.2.3.1.0 = „“

WELOTEC-MIB::ihWan3g.1.2.3.2.0 = „“

WELOTEC-MIB::ihWan3g.1.2.3.3.0 = „“

WELOTEC-MIB::ihWan3g.1.2.3.4.0 = INTEGER: 0

WELOTEC-MIB::ihWan3g.1.2.3.5.0 = INTEGER: 0

WELOTEC-MIB::ihWan3g.1.2.3.6.0 = „“

WELOTEC-MIB::ihWan3g.1.2.4.1.0 = INTEGER: 0

WELOTEC-MIB::ihWan3g.1.2.4.2.0 = INTEGER: 0

WELOTEC-MIB::ihWan3g.1.2.4.3.0 = Gauge32: 0

WELOTEC-MIB::ihWan3g.1.3.1.1.0 = STRING: „262010052709611“

WELOTEC-MIB::ihWan3g.1.3.1.2.0 = STRING: „860461024084629“

WELOTEC-MIB::ihWan3g.1.3.2.1.0 = Gauge32: 0

WELOTEC-MIB::ihWan3g.1.3.2.3.0 = INTEGER: 0

WELOTEC-MIB::ihWan3g.1.3.2.4.0 = INTEGER: 0

WELOTEC-MIB::ihWan3g.1.3.2.5.0 = Gauge32: 193

WELOTEC-MIB::ihWan3g.1.3.2.6.0 = Gauge32: 0

WELOTEC-MIB::ihWan3g.1.3.3.1.0 = „“

WELOTEC-MIB::ihWan3g.1.3.3.2.0 = „“

WELOTEC-MIB::ihWan3g.1.3.3.3.0 = INTEGER: 1

WELOTEC-MIB::ihWan3g.1.3.3.4.0 = „“

WELOTEC-MIB::ihWan3g.1.3.3.5.0 = „“

WELOTEC-MIB::ihWan3g.1.3.3.6.0 = „“

WELOTEC-MIB::ihWan3g.1.3.3.7.0 = INTEGER: 0

WELOTEC-MIB::ihWan3g.1.3.3.8.0 = INTEGER: 0

WELOTEC-MIB::ihWan3g.1.3.3.9.0 = „“

WELOTEC-MIB::ihWan3g.1.3.4.1.0 = INTEGER: 0

WELOTEC-MIB::ihWan3g.1.3.4.2.0 = INTEGER: 0

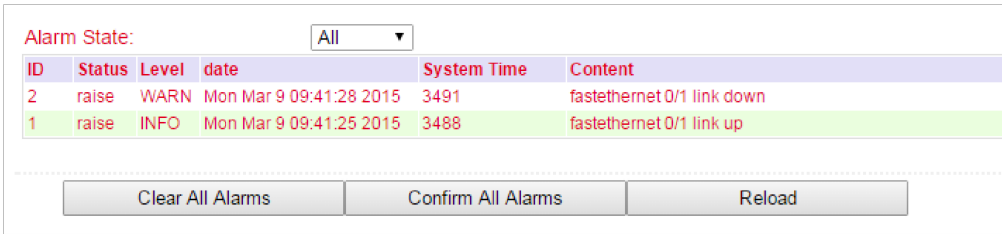
WELOTEC-MIB::ihWan3g.1.3.4.3.0 = Gauge32: 0

3.1.10 3.1.9. Alarm

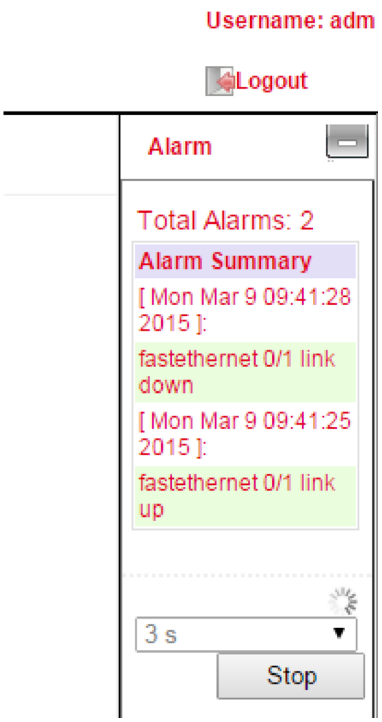
3.1.9.1. Status

Der Alarmstatus zeigt eine Übersicht der ausgelösten Alarme an.

In diesem Beispiel wird in der INFO Meldung ID 1 angezeigt, dass der Fastethernet Port 0/1 verbunden wurde. ID 2 zeigt eine Warnmeldung, dass der Fastethernet Port 0/1 getrennt wurde (Abb.1).

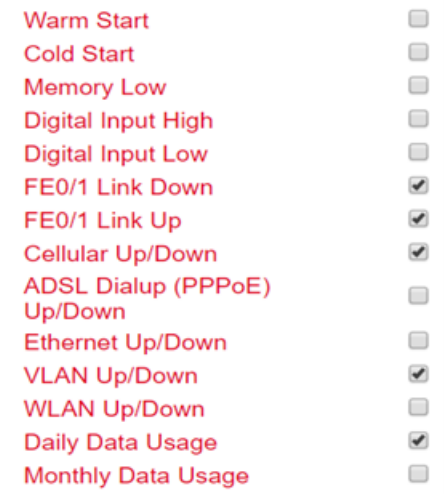


Auf der rechten Seite der Weboberfläche sieht man die Alarmmeldungen permanent unabhängig davon in welchem Menü man sich befindet (Abb. 2).



3.1.9.2. Alarm Input

Im ***Alarm Input*** Menü definieren Sie, welche Alarmmeldungen der Router ausgeben soll. Durch Setzen der Haken neben jedem Eintrag wird ein Alarm aktiviert oder deaktiviert.



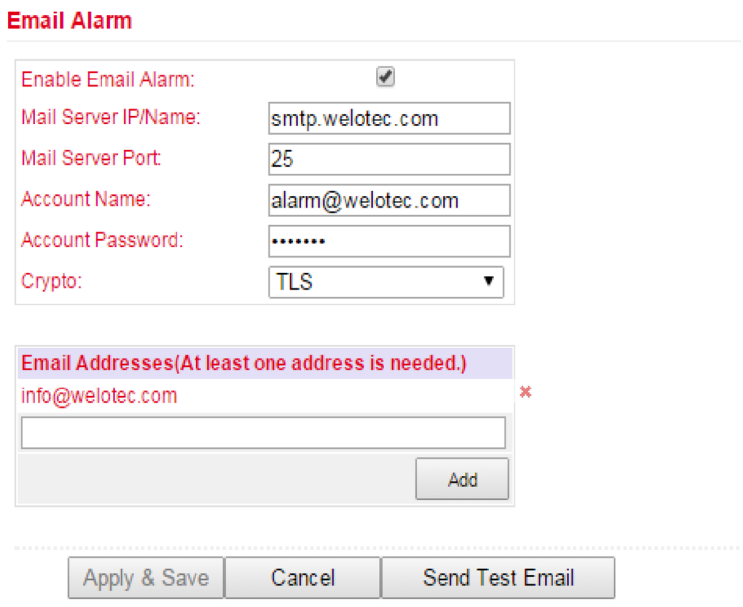
Folgende Alarmmeldungen stehen zur Verfügung.

Parameter	Beschreibung
Warm Start	Warmstart/Neustart des Routers (reboot)
Cold Start	Kaltstart = Start des Routers, wenn dieser ausgeschaltet war oder vorher kein Strom hatte
Memory Low	Wenig Arbeitsspeicher
Digital Input High	Hoher digitaler Dateneingang
Digital Input Low	Niedriger digitaler Dateneingang
FE0/1 Link Down	Fast Ethernet Port 0/1 getrennt
FE0/1 Link Up	Fast Ethernet Port 0/1 verbunden
Cellular Up/Down	Funkverbindung GPRS/UMTS/LTE verbunden oder getrennt
ADSL Dialup (PPPoe) Up/Down	ADSL Einwahl verbunden oder getrennt
Ethernet Up/Down	Ethernet verbunden oder getrennt
VLAN Up/Down	VLAN verbunden oder getrennt
WLAN Up/Down	WLAN verbunden oder getrennt
Daily Data Usage	Anzeige der täglichen verbrauchten Daten der SIM-Karte (nur bei aktivierter Data Usage Funktion, s. Services > Data Usage)
Monthly Data Usage	Anzeige der monatlich verbrauchten Daten der SIM-Karte (nur bei aktivierter Data Usage Funktion, s. Services > Data Usage)

3.1.9.3. Alarm Output

Beim Alarm Output Menü wird der E-Mail Server konfiguriert, der die Warnmeldungen per Mail weiterleiten soll.

Wird ein Alarm ausgelöst, wird vom Router eine Nachricht generiert und über den angegebenen E-Mail Server an die hinterlegten E-Mail-Adressen versendet.



Parameter	Beschreibung
Enable Email Alarm	Haken setzen für Ein-/ Ausstellen der E-Mail Server Funktionalität
Mail Server IP/Name	Hostname (FQDN) oder IP Adresse des E-Mail Server
Mail Server Port	Port des Mailservers, default 25, aber auch 465 für SSL/TLS oder 587 möglich
Account Name	Benutzerkonto auf dem E-Mail Server, über welchen die Nachrichten versendet werden sollen
Account Passwort	Passwort des Benutzerkontos auf dem E-Mail Server
Crypto	Verschlüsselung TLS
Email Addresses	E-Mail Adressat an den die Mails versendet werden sollen

3.1.9.4. Alarm Map

Auf der Alarm Map wird festgelegt, ob die Warnmeldungen im Webbrowser angezeigt werden oder auch per E-Mail oder SMS verschickt werden sollen. Setzen Sie den Haken für Aktivieren oder Deaktivieren der Funktion.

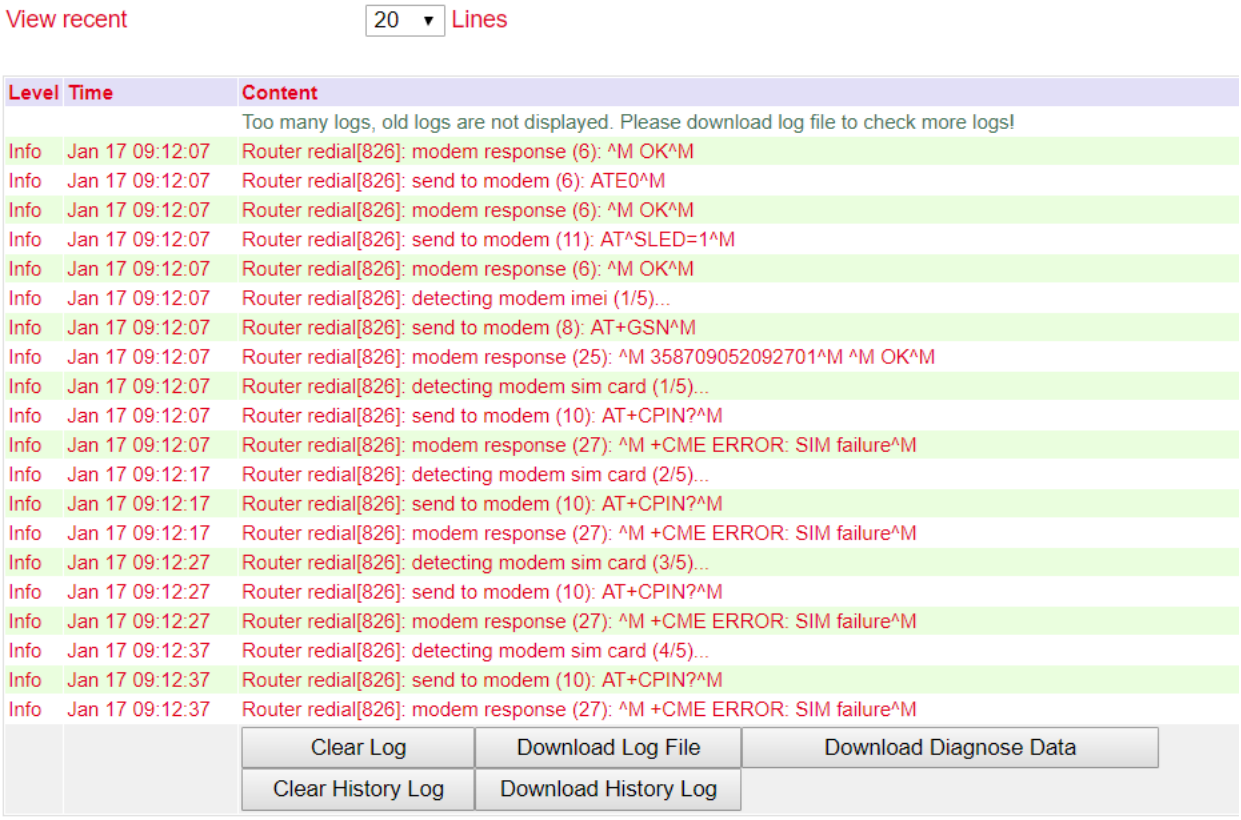
Output Type	Console	Email	SMS
Warm Start	☐	☐	☐
Cold Start	☐	☐	☐
Memory Low	☐	☐	☐
Digital Input High	☐	☐	☐
Digital Input Low	☐	☐	☐
FE0/1 Link Down	☐	☐	☐
FE0/1 Link Up	☐	☐	☐
Cellular Up/Down	☐	☐	☐
ADSL Dialup (PPPoE) Up/Down	☐	☐	☐
Ethernet Up/Down	☐	☐	☐
VLAN Up/Down	☐	☐	☐
WLAN Up/Down	☐	☐	☐
Daily Data Usage	☐	☐	☐
Monthly Data Usage	☐	☐	☐

3.1.11 3.1.10. Log

3.1.10.1. Log

Im Log Menü werden die aktuellen Meldungen des Routers ausgegeben.

Das Log enthält Informationen über Netzwerk, Betriebszustand, Konfigurationsänderungen, Verbindungsinformationen zum Provider, IPSec, OpenVPN Status und vieles mehr.

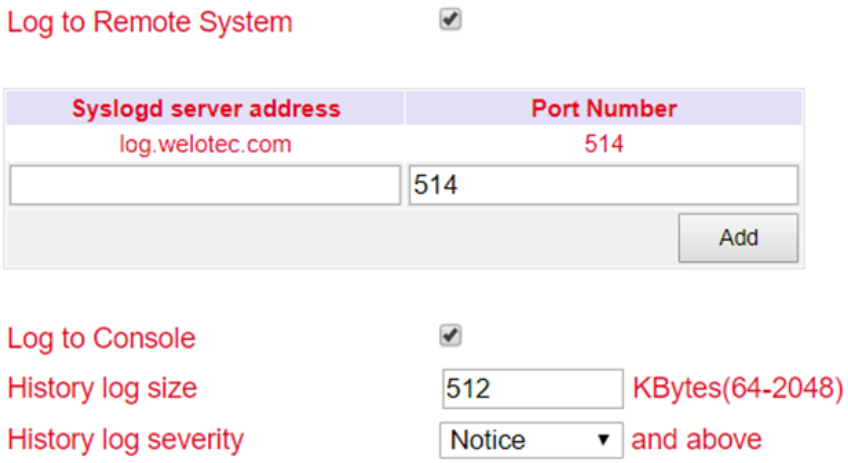


Unter dem Log-Bereich gibt es die Optionen, die angezeigten Logs zu löschen, das Log herunterzuladen, die Diagnose Datei herunterzuladen, die Historie zu löschen und die Historie herunterzuladen.

Option	Beschreibung
Clear Log	Angezeigte Log-Dateien löschen
Download Log File	Log-Dateien herunterladen
Download Diagnose Data	Diagnosedatei herunterladen
Clear History Log	Log Historie löschen
Download History Log	Log Historie herunterladen

3.1.10.2. System Log

Im ***System Log*** kann man einen Syslog Server angeben, an welchen die Logs über das Netzwerk geschickt werden sollen.



Unter ***Syslog server address*** wird der Hostname des Syslog Server (FQDN) oder die IP Adresse angegeben. Der Port 514 ist der Standard-Port für Syslogserver.

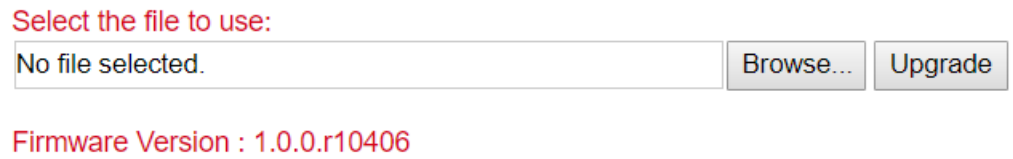
3.1.12 3.1.11. Cron Job

Unter ***Time Schedule*** können Sie Aktivitäten zu bestimmten Zeitpunkten auf dem Router ausführen lassen, wie z.B. einen Neustart (reboot) des Routers. Hier könnten Sie den Router immer zu einem bestimmten Zeitpunkt neu starten.

Unter Time Schedule können Sie das Schedule Command auswählen (momentan nur reboot). Bei Day wählen Sie täglich (everyday) und mit Hours und Minutes steuern Sie die Startzeit. Durch klicken auf den Add-Button übernehmen Sie die Einstellungen.

3.1.13 3.1.12. Upgrade

Im ***Upgrade*** Menü können Firmwareupdates des Routers durchgeführt werden. Ein Firmwareupdate kann neue Funktionen enthalten oder auch Fehler beseitigen. Die installierte Firmware wird unter dem Feld ***Select the file to use*** angezeigt.



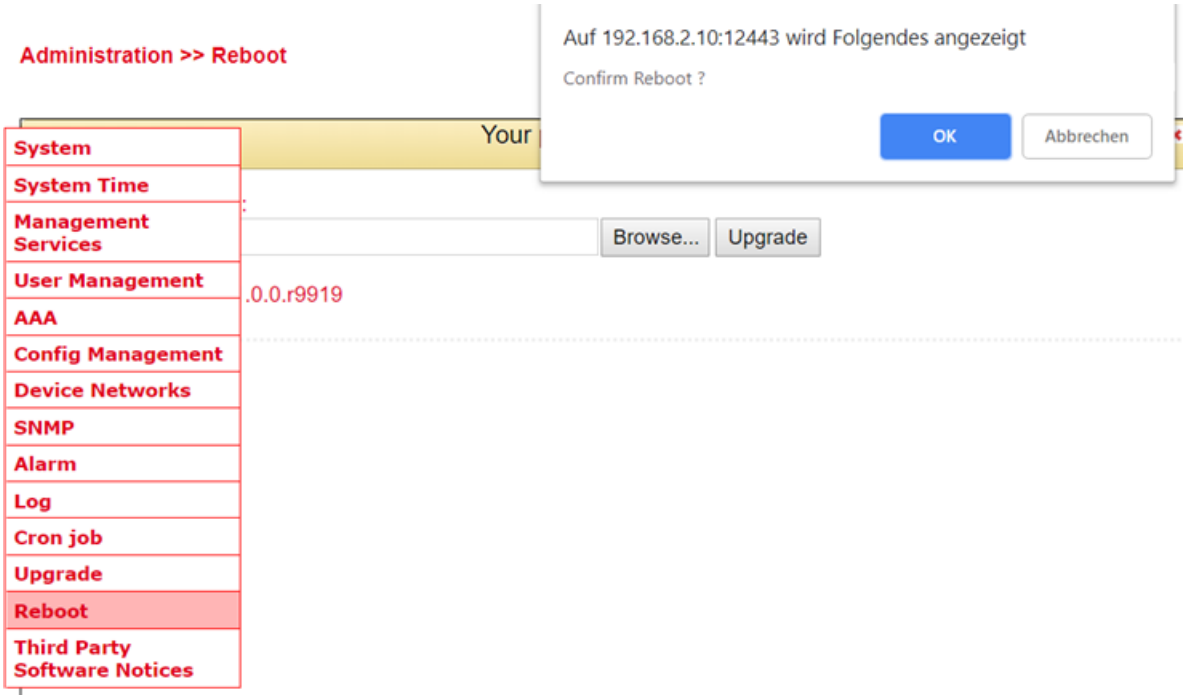
Unter Browse wählen Sie die Firmware Datei aus, welche Sie sich vorher heruntergeladen haben (diese muss entpackt entweder als *.bin oder *.pkg File vorliegen). Mit einem Klick auf ***Upgrade*** wird die Firmware auf den Router aufgespielt.

⚠ Hinweis

Beachten Sie bitte, dass bei deutlich älterem Firmwarestand ggfs. der Bootloader und das IO-Board gesondert upgedatet werden müssen. Bei Fragen wenden Sie sich gerne an unseren Support.

3.1.14 3.1.13. Reboot

Mit ***Reboot*** wird der Router neu gestartet.



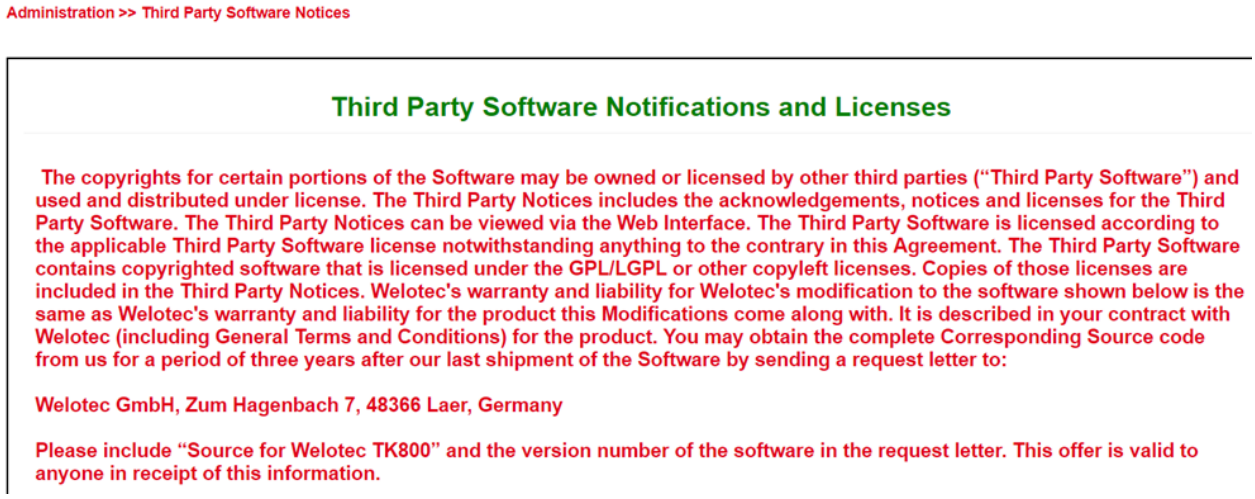
Mit einem Klick auf ***OK*** bestätigen Sie den Neustart des Routers.

Hinweis

Speichern Sie die Konfiguration des Routers ab, bevor Sie den Router neu starten. Sonst kann es sein, dass die Konfiguration beim Neustart verloren geht.

3.1.15 3.1.14. Third Party Software Notices

Hier sind die Softwarebestimmungen und Lizenzen von allen Drittanbietern aufgeführt, die im Zusammenhang mit der Routerserie TK800 stehen.



3.2 3.2. Network

3.2.1 3.2.1. Cellular

Cellular ist die Mobilfunkschnittstelle des Routers. Wenn in dem Router eine SIM Karte eingesetzt ist, kann man sich über GPRS, EDGE, UMTS oder LTE, je nach Routermodell, ins Internet einwählen.

3.2.1.1. Cellular Status

Unter ***Status*** befindet sich eine Übersicht über den aktuellen Status (Connected oder Disconnected).

Entscheidend ist im Register Status der Network Type und unter dem Bereich Network die IP Adresse. Im Bereich Modem ist auch der Bereich der Signal Stärke (Signal Level), RSRP und RSRQ ersichtlich.

Unter Umständen kann es dazu kommen, dass der Router keinen richtigen DNS Server vom Provider zugewiesen bekommt. Achten Sie darauf ob unter DNS kein Eintrag oder ein Eintrag wie z.B. 10.74.210.210 (Telekom) vorhanden ist.

Hinweis

Der RSRP-Wert ist einer der wichtigsten Werte, wenn es um die Beurteilung des eigenen Empfangswertes bzw. der Empfangsqualität geht. Er wird direkt vom Endgerät gemessen. Dieses bestimmt mit Hilfe des RSRPs auch die momentan stärkste Funkzelle in der Umgebung.

SRP	Schulnote	Kommentar
-50 bis -65 dBm	1 (sehr gut)	es liegt exzellenter Empfang vor - perfekt!
-65 dBm bis -80 dBm	2 (gut)	gute, ausreichende Empfangsbedingungen
-80 dBm bis -95 dBm	3 (befriedigend)	nicht perfekt aber ausreichend für stabile Verbindungen
-95 dBm bis -105 dBm	4 (ausreichend)	noch akzeptable Bedingungen mit Einschränkungen beim Speed; ggf. auch Abbrüche
-110 dBm bis -125 dBm	5 (mangelhaft)	sehr schlechter Pegel - dringender Handlungsbedarf; wahrscheinlich kaum Verbindung möglich
-125 dBm bis -140 dBm	6 (ungenügend)	extrem schlecht - wahrscheinlich keine Verbindung möglich

Hinweis

Der RSRQ ist ein errechneter Verhältniswert, der sich aus dem Wert für RSRP und dem RSSI ergibt. Er ist für die Beurteilung einer LTE-Verbindung, bzw. der Empfangsqualität enorm wichtig. Zur optimalen Ausrichtung von Antennen bei einer stationären Nutzung von LTE, ist die Analyse dieses Wertes unerlässlich. Zusammen mit dem RSRP ergibt das für den Nutzer die Möglichkeit, die optimale Position und Ausrichtung für sein Equipment (z.B. [Antenne]) zu finden.

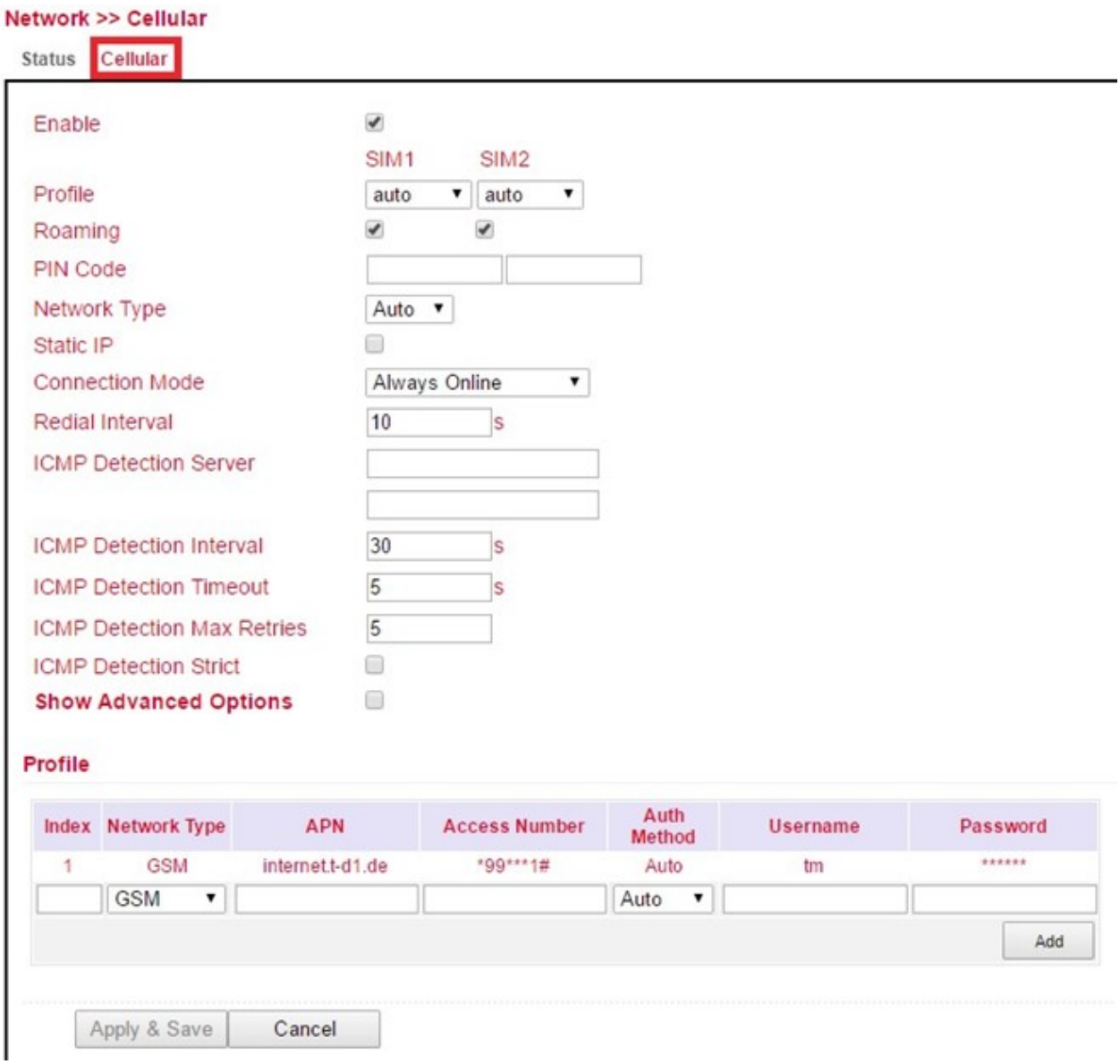
RSRQ	Schulnote	Kommentar
-3 dB	1 (sehr gut)	Optimale Verbindungsqualität, keine Beeinflussung durch Störer
-4 … -5 dB	2 (gut)	störende Einflüsse vorhanden, sind aber ohne Auswirkungen
-6 … -8 dB	3 (befriedigend)	störende Einflüsse, leichte Beeinflussung d. Verbindung
-9 … -11 dB	4 (ausreichend)	störende Einflüsse, spürbare Beeinflussung der Verbindung
-12 … -15 dB	5 (mangelhaft)	Stark störende Einflüsse vorhanden, Verbindung sehr instabil
-16 … -20 dB	6 (ungenügend)	Extrem störende Einflüsse, keine nutzbare Verbindung möglich

Hinweis

Bei den meisten Providern werden private IP Adressen vergeben oder IP Adressen, die nicht über das Internet geroutet werden. Ein erfolgreicher oder nicht erfolgreicher Ping gibt keine Aussage darüber, ob die IP Adresse des Routers wirklich erreichbar ist.

3.2.1.2. Cellular Configuration

Unter ***Network > Cellular > Cellular*** können Sie Einstellungen für den Zugriff über das Mobilfunknetz machen.

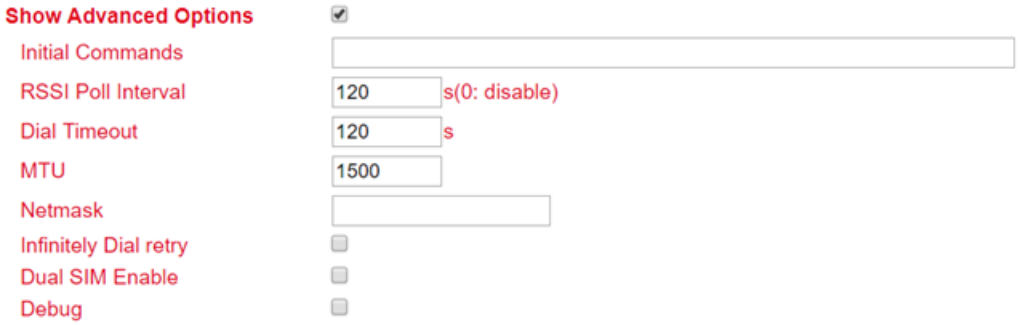

Network >> Cellular
Status
Cellular
Enable
SIM1
SIM2
Profile
auto
auto
Roaming
PIN Code
Network Type
Auto
Static IP
Connection Mode
Always Online
Redial Interval
10
s
ICMP Detection Server
ICMP Detection Interval
30
s
ICMP Detection Timeout
5
s
ICMP Detection Max Retries
5
ICMP Detection Strict
Show Advanced Options
Profile
Index
Network Type
APN
Access Number
Auth Method
Username
Password
1
GSM
internet.t-d1.de
*99***1#
Auto
tm
******
GSM
Auto
Add
Apply & Save
Cancel

Parame	Beschreibung	Werkseinstellung
Enable	Aktivieren oder Deaktivieren der Mobilfunkverbindung	Aktivert
Profile	APN Profil für SIM Karte 1 und SIM Karte 2	Auto / Auto Automatische Selektion des APN basierend auf der SIM Karte.
Roaming	Aktiveren oder Deaktivieren ob die SIM Karte Roaming erlauben soll. ⚠ **Hinweis** Ob diese Funktion funktioniert ist abhängig vom Provider. Es kann trotz Deaktivierung zu Roaming kommen.	Aktiviert / Aktiviert
PIN Code	PIN code für die SIM Karte. ⚠ **Hinweis** PIN Code sollte vor dem Einlegen der SIM Karte eingetragen werden!!!	Leer / Leer
Network Type	Auswahl: Auto (automatische Wahl des Netzes), 2G (GPRS / EDGE), 3G (UMTS, HSDPA, HSUPA, HSPA+), 4G (LTE)	Auto
Static IP	⚠ **Hinweis** Nur in wenigen Ausnahmen relevant. Bei den meisten Providern, die feste IP Adressen vergeben, darf die Funktion nicht gesetzt werden.	Deaktiviert
Connection Mode	Auswahl, ob der Router immer mit dem Mobilfunknetz verbunden sein soll oder sich nur bei Bedarf einwählen soll.	Always Online
Redial Interval	Wiedereinwahlintervall	10 Sekunden
ICMP Detection Server	Hier können bis zu zwei ICMP Detection Server zur Verbindungsüberwachung eingetragen werden. ⚠ **Hinweis** Die IP Adressen oder DNS Namen müssen über den Router erreichbar sein und auf einen Ping antworten. Es empfiehlt sich daher nicht die Google-Server 8.8.8.8 und 8.8.4.4 zu nehmen, da diese die Anfragen öfter blocken. Wählen Sie z.B. 4.2.2.1 o.ä.	leer
ICMP Detection Interval	Intervall, in dem der ICMP Detection Server die Internetverbindung überprüft.	30 Sekunden
ICMP Detection Timeout	ICMP Timeout oder auch Ping Timeout. Zeit die der Ping maximal dauern darf (Round Trip Time).	5 Sekunden
ICMP Detection Max Retries	Anzahl der Wiederholungen bei Fehlgeschlagenem ICMP Ping.	5
ICMP Detection Strict	Wenn deaktiviert, wird der ICMP Ping nur dann gesendet, wenn keine Daten gesendet oder empfangen werden. ⚠ **Hinweis** Wenn ICMP Detection Strict aktiviert ist, wird der ICMP Ping immer ausgeführt, auch dann, wenn Nutzdaten gesendet oder empfangen werden. Für Anwendungen, wo es auf hohe Verfügbarkeit ankommt, sollte Strict aktiviert werden.	Deaktiviert
Show Advanced Options	Wenn aktiviert werden mehr Konfigurationsmöglichkeiten sichtbar.	Deaktiviert

Connect on Demand

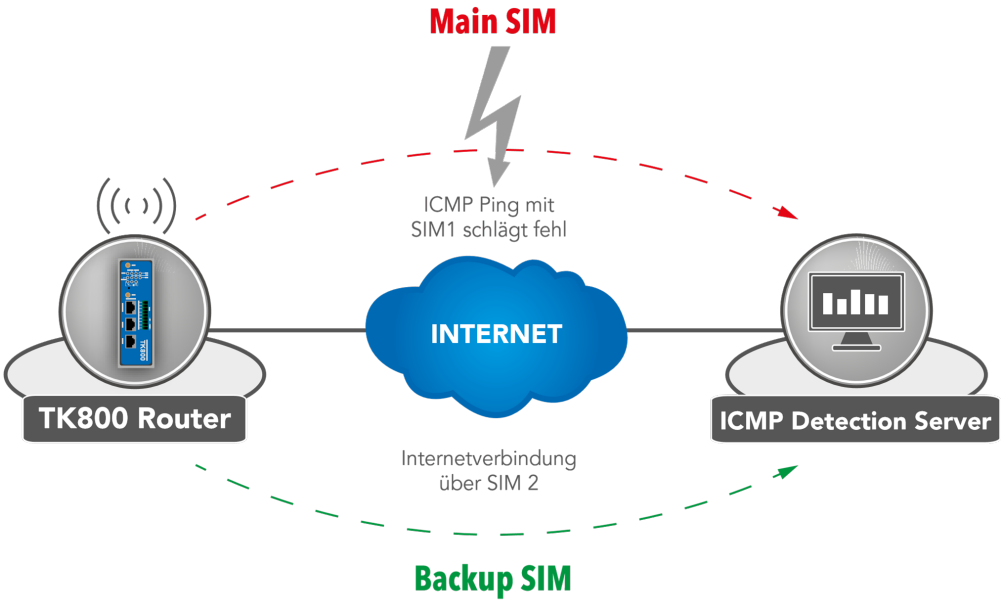
Hier muss der Haken bei ***Triggered by SMS*** gesetzt werden. Der Router verbindet sich nur mit dem Internet, wenn er zuvor per SMS den Befehl dazu erhalten hat.

Show Advanced Options



Parameter	Beschreibung	Werkseinstell
Initial Commands	Startbefehle für z.B., wenn Triggered by SMS gewählt ist oder spezielle AT Commands genutzt werden sollen	leer
RSSI Poll Interval	Abfrageintervall der Signalstärke	120 sekunden
Dial Timeout	Maximale Zeit für den Einwahlversuch	120 sekunden
MTU	Maximale Paketgröße eines Paketes	1500 bytes
Netmask	Hier kann eine zusätzliche Netzmaske eingetragen werden	leer
Infinitely Dial Retry	Wenn Triggered by SMS gewählt ist kann hier die Anwahl auf unendlich gestellt werden	aus
Dual SIM Enable	Ein-/Ausschalten der Dual-SIM-Option. Ist dieser Punkt aktiviert, stehen spezielle Auswahlfelder zur Verfügung s.u.	disabled
Main SIM	Die Hauptsimkarte, die genutzt werden soll	SIM1
Max Number of Dial	Maximale Verbindungsversuche, danach Neustart des Modems	5
Min Connected Time	Minimale Verbindungszeit	0 Sekunden
CSQ Threshold	Minimale Signalstärke SIM1 / SIM2	0
CSQ Detect Interval	Intervall für die Signalstärkeabfrage SIM1 / SIM2	0 Sekunden
CSQ Detect Retries	Wiederholungsversuche für die Signalstärkeabfrage SIM1 / SIM2	0
Backup SIM Timeout	Zeit, nach der wieder auf die Hautpsimkarte gewechselt wird	0 Sekunden
Debug	Wenn aktiviert, dann wird ausführlicher geloggt.	disabled

Dual SIM Enabled



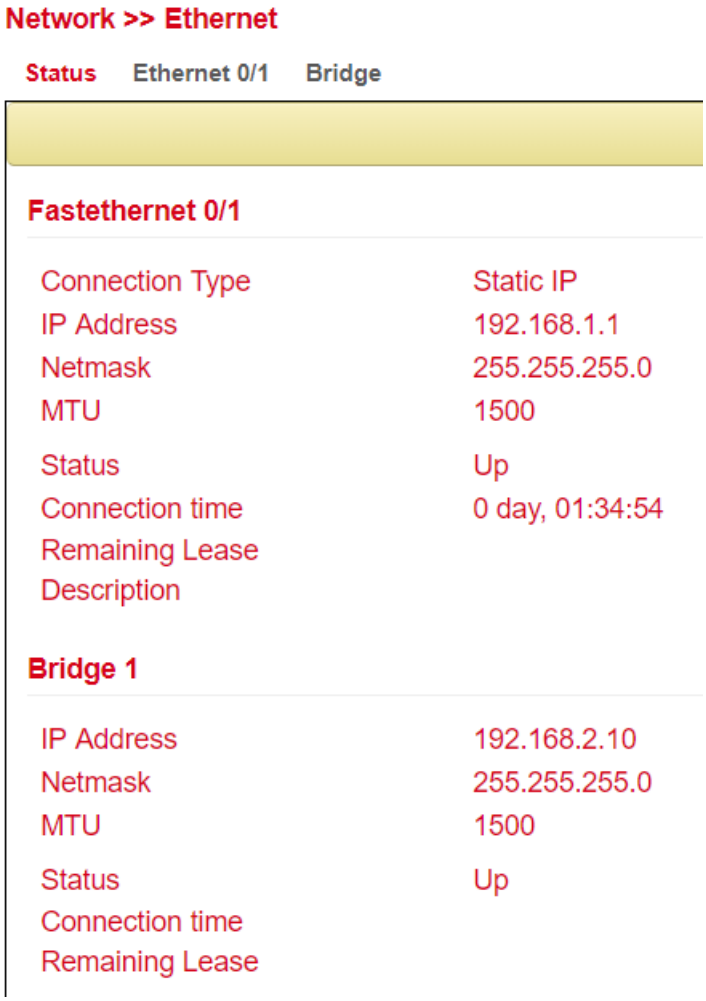
Bei Ausfall eines Providers wird auf den Alternativprovider umgeschaltet. Gleiches gilt bei Verbrauch des mobilen Datenvolumens. Der TK 800 überwacht dabei mittels ICMP die Datenverbindung. Steht diese nicht mehr zur Verfügung (weil der Ping fehlschlägt) schaltet der Router auf die andere Verbindung um.

3.2.2 3.2.2. Ethernet

Im Bereich Ethernet haben Sie die Möglichkeit Einstellungen an den Netzwerkports vorzunehmen. Dabei können Sie, je nach Modell die Schnittstellen individuell anpassen. Wichtig ist es hier zu wissen, dass es bei den Routermodellen eine Netzwerkschnittstelle mit der Bezeichnung FE 0/1 gibt und eine Netzwerkbrücke (Bridge), die je nach Modell mit FE 1/1 bis1/4 bezeichnet ist.

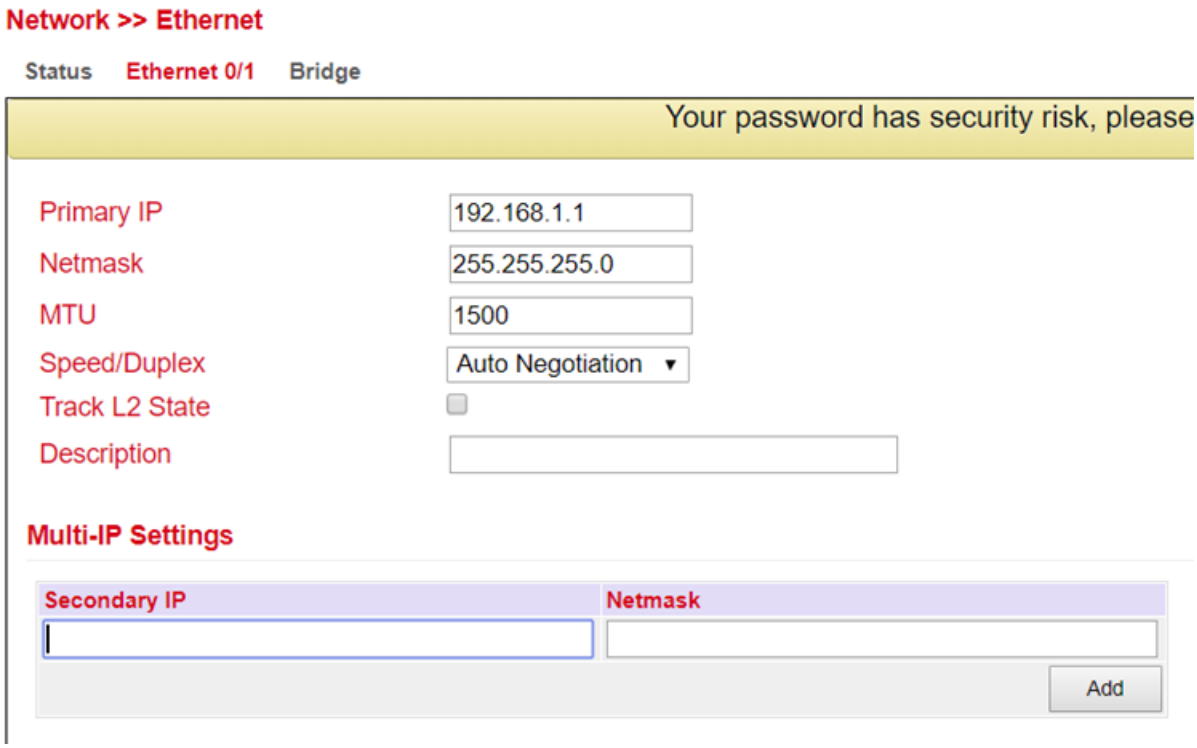
3.2.2.1. Ethernet Status

Die Statusseite zeigt den aktuellen Status der Netzwerkports (abhängig von dem Model) an.



3.2.2.2. Fast Ethernet 0/1

Hier können Sie die Einstellungen der Netzwerkschnittstelle mit der Bezeichnung FE 0/1 anpassen.



Param	Beschreibung	Werksei
Primary IP	Primäre IP Adresse kann hier eingetragen und geändert werden	192.168.1.1
Netmask	Subnetzmaske	255.255.255.0
MTU	Maximum Transmission Unit = maximale Größe eines unfragmentierten Datenpakets	1500
Speed/Duplex	Fünf Optionen stehen zur Auswahl: Auto Negotiation: Automatische Aushandlung der Geschwindigkeit 100M Full-duplex: 100 Megabit Voll-duplex 100M Half-duplex: 100 Megabit Halb-duplex 10M Full-duplex: 10 Megabit Voll-duplex 10M Half-duplex: 10 Megabit Halb-duplex	Auto
Track L2 State	Haken gesetzt: Port Status bleibt nach dem getrennt werden administrativ getrennt (Down) Haken nicht gesetzt: Port Status verbindet sich wieder nachdem dieser getrennt wurde (UP)	Haken nicht gesetzt
Description	Beschreibung des Ports - Frei wählbarer Name	-

Im unteren Menü können weitere IP Adressen für den FastEthernet 0/1 Port vergeben werden.

Hinweis

Die Konfiguration als DHCP Client wird unter ***DHCP*** beschrieben. Die Konfiguration eines WAN Interfaces wird unter

Wizard beschrieben

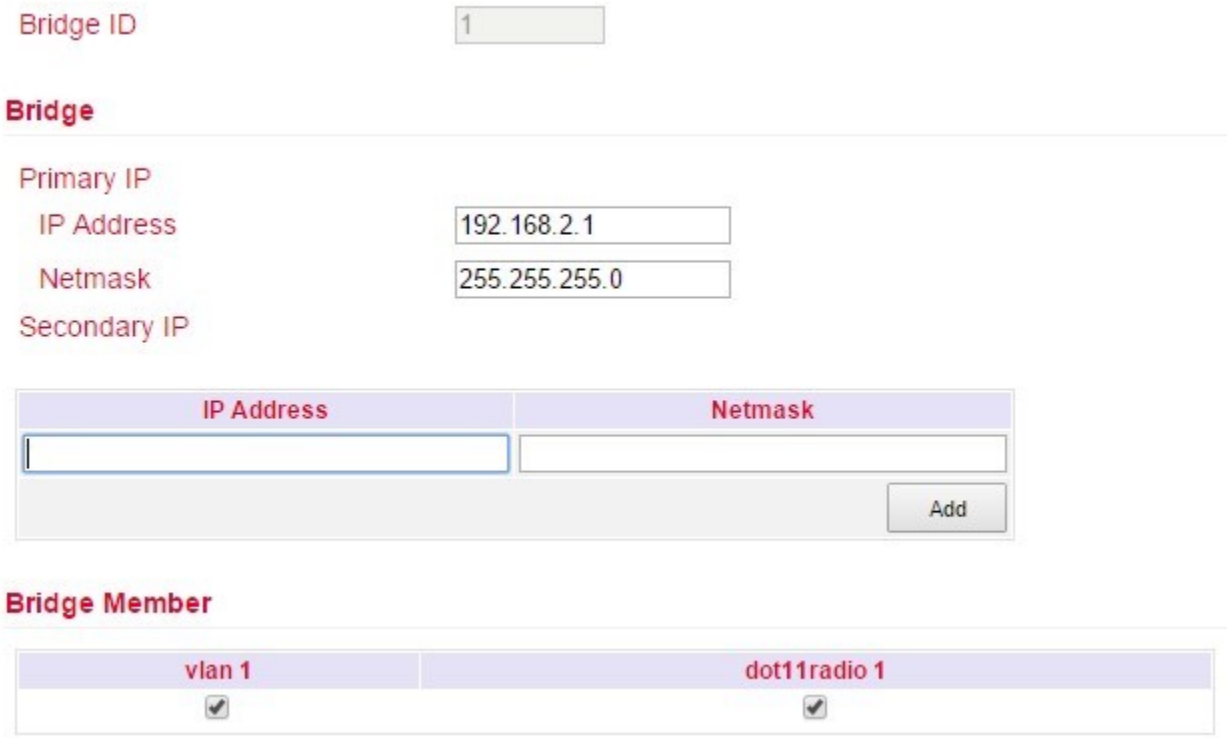
3.2.2.3. Bridge (TK8x5-EXW)

Übersicht der vorhandenen Bridge. Es ist nur eine Bridge möglich!

Hinweis

Wenn Sie die Bridge löschen, ist keine IP-Adresse mehr auf den Interfaces FE1/1 - FE1/4 gesetzt. Der Router ist dann nur noch über FE0/1 oder Konsole erreichbar!!!

Zum Bearbeiten der Bridge wählen Sie den vorhandenen Eintrag aus und klicken anschließend auf ***Modify***.



Bridge:

Hier lässt sich die IP Adresse der Bridge ändern. Unter ***Secondary IP*** können Sie der Bridge noch weitere IP Adressen zuweisen.

Bridge Member:

Das Interface ***dot11radio1*** ist das WLAN Interface. Über die Haken kann ein Bridge Member der Bridge hinzugefügt oder herausgenommen werden.

Hinweis

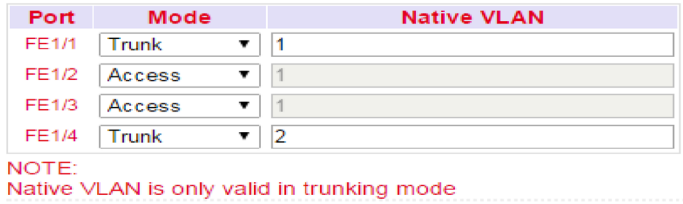
Das Entfernen eines Bridge Members aus der Bridge führt dazu, dass die IP Adresse des Interfaces leer ist. Somit empfiehlt es sich eine Änderung nur über das Interface FE0/1 durchzuführen, da dieses nicht Bridge Member ist.

3.2.3 3.2.3. VLAN (TK8x5-x)

Ein ***Virtual Local Area Network (VLAN)*** ist ein logisches Teilnetz innerhalb eines Switches oder eines gesamten physischen Netzwerks. Ein VLAN trennt physische Netze in Teilnetze auf, indem es dafür sorgt, dass VLAN-fähige Switches die Frames (Datenpakete) eines VLANs nicht in ein anderes VLAN weiterleiten. Dies geschieht obwohl die Teilnetze an gemeinsamen Switches angeschlossen sein können.

3.2.3.1. VLAN Trunk

Im Menü ***VLAN Trunk*** können den Netzwerkports FastEthernet 1/1 bis 1/4 verschiedene VLAN IDs zugeordnet werden.



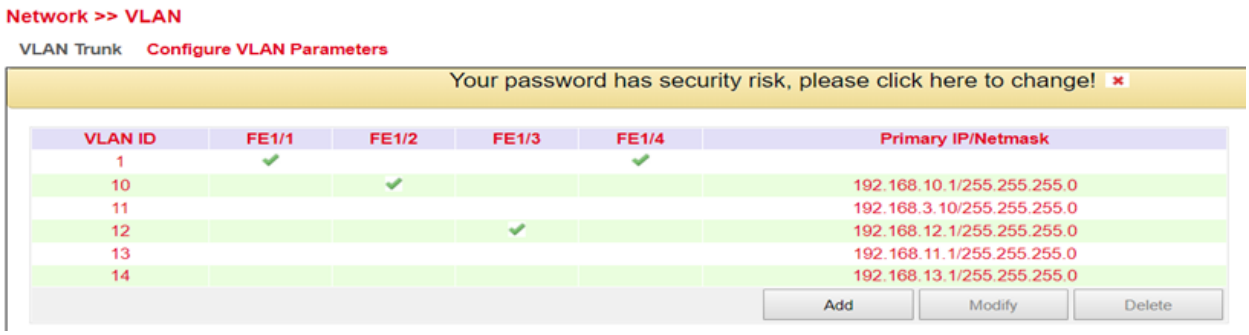
Es stehen die Optionen ***Access*** und ***Trunk*** für die FastEthernet Ports zur Verfügung.

Im Access Mode ist immer das VLAN 1 ausgewählt.

Im Trunk Mode können Sie den FastEthernet Ports VLAN IDs zwischen 1-4000 zuweisen.

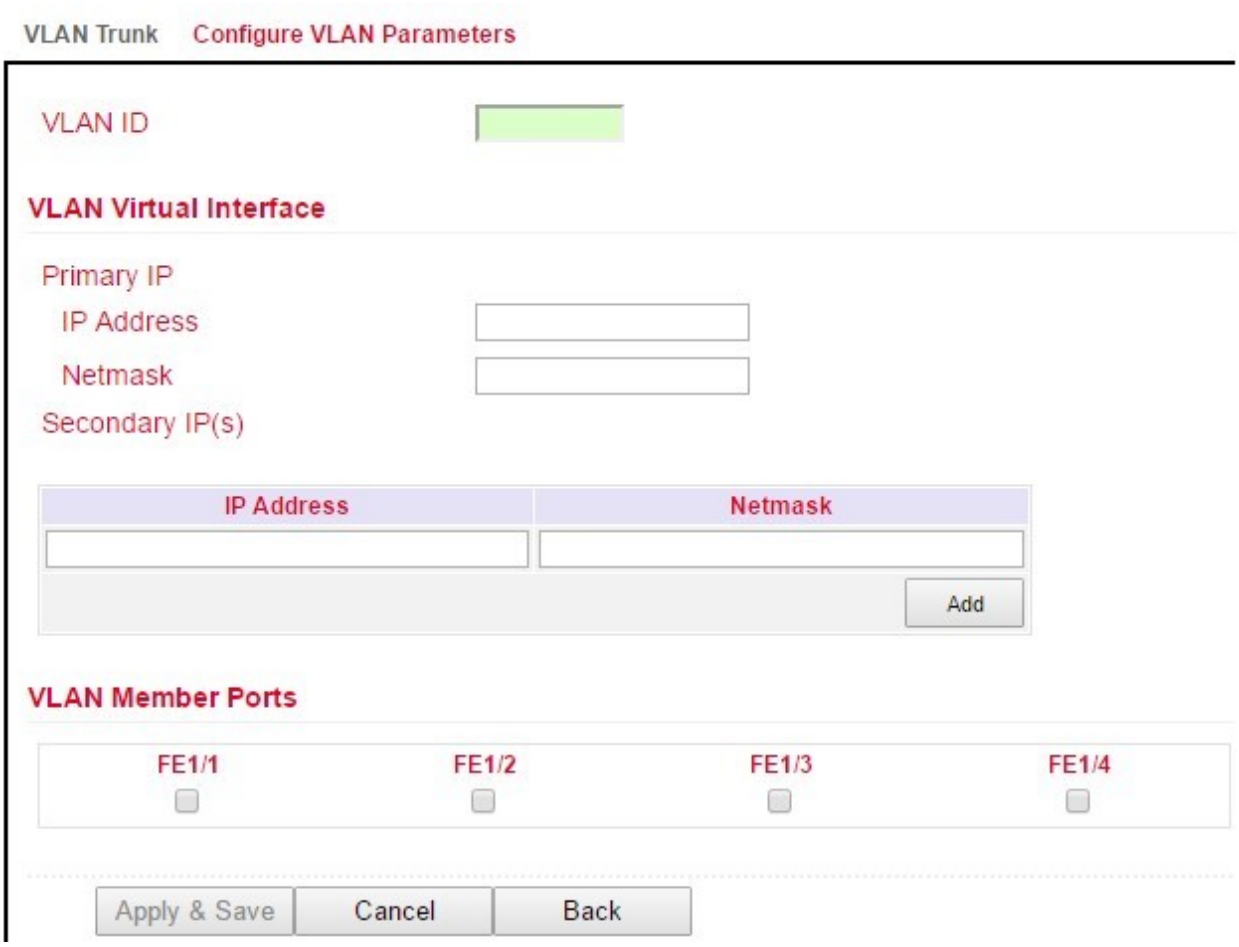
3.2.3.2. Configure VLAN Parameters

Im Menü ***Configure VLAN Parameters*** können Sie die Zuweisung von VLANs zu FastEthernet Ports ändern und neue VLANs anlegen.



Butt	Beschreibung
Add	Über den Button Add kann ein neues VLAN hinzugefügt werden.
Modify	Die vorhandenen VLANs kann man durch auswählen und anschließendem Klick auf Modify bearbeiten. ⚠ **Hinweis** Bei dem Model TK8x5-EXW kann das VLAN mit der ID1 nicht bearbeitet werden, solange die Bridge aktiv ist.
Delete	Mit Delete kann ein zuvor ausgewähltes VLAN gelöscht werden. ⚠ **Hinweis** Das VLAN mit der ID 1 kann nicht gelöscht werden!!!

Hinzufügen eines neuen VLANs:



Vergeben Sie eine neue ***VLAN ID*** (z.B. 3) und dann eine Primäre IP Adresse. Bei Bedarf können mehrere IP Adressen unter ***Secondary IP(s)*** eingetragen werden (nach jedem Hinzufügen mit Add bestätigen).

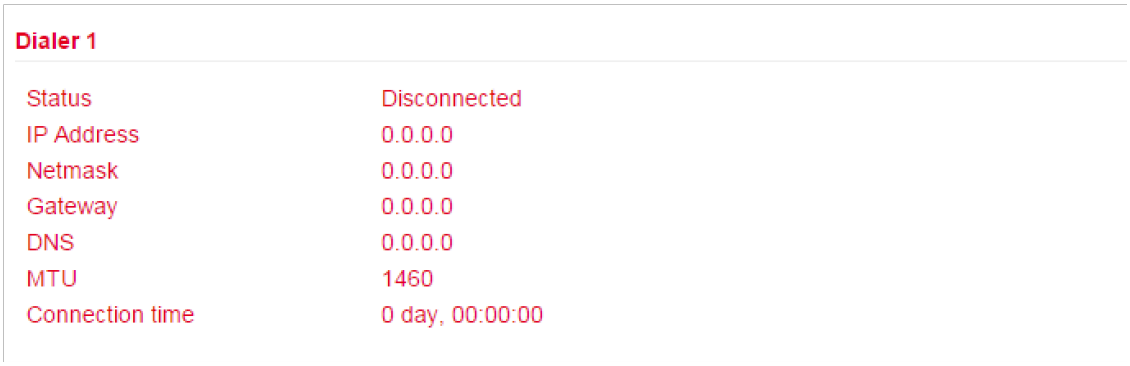
Unter ***VLAN Member Ports*** wird durch Setzen des Hakens in der Checkbox dem VLAN ein/mehrere FastEthernet Port/s zugewiesen.

⚠ Hinweis

Die Router der TK800 Serie verfügen nicht über ein eingebautes ADSL Modem. Für die Nutzung von ADSL Dialup muss ein externes ADSL Modem an den WAN Port angeschlossen werden.

3.2.4 3.2.4. ADSL Dialup (PPPoE)

3.2.4.1. Status



Hinweis

Die Router der TK800 Serie verfügen nicht über ein eingebautes ADSL Modem. Für die Nutzung von ADSL Dialup muss ein externes ADSL Modem an den WAN Port angeschlossen werden. Für die digitale Übertragungstechnik ist ein entsprechendes DSL-Modem nötig, das die neuen IP Technologien beherrscht.

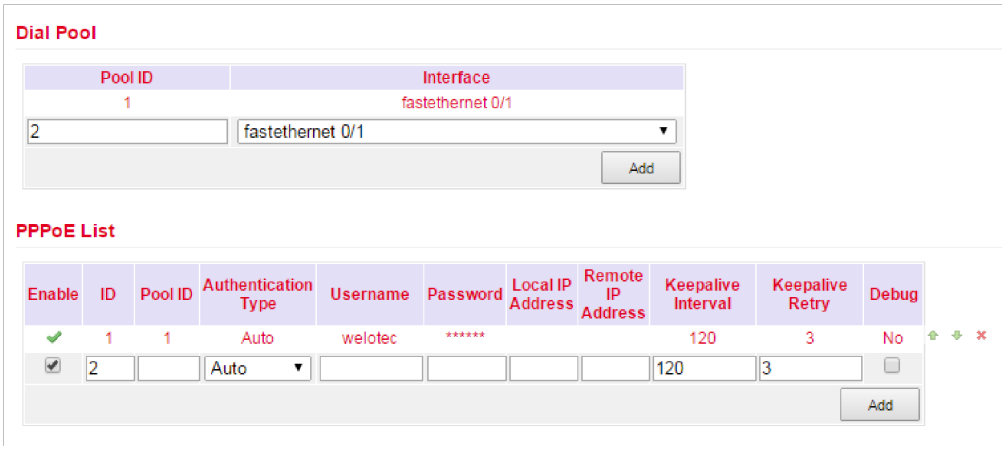
3.2.4.2. ADSL Dialup (PPPoE)

Hier können Sie die Einwahl über das DSL-Modem für PPPoE konfigurieren. Der TK800 hat kein eigenes DSL-Modem, so dass diese sich nicht eigenständig einwählen können.

Für diesen Fall ist ein entsprechendes DSL-Modem nötig, das die neuen IP Technologien beherrscht. Folgende Kriterien sollte das Modem erfüllen:

- VDSL2/ADSL2 Ethernet-Modem
- Annex A/B/M/J kompatibel
- PPPoE-Bridge-Betrieb
- IPv4 und IPv6-kompatibel
- DSL-Standards
  - ANSI T1.413 Issue 2
  - ITU G.992.1 A/B (G.dmt)
  - ITU G.992.2 (G.lite)
  - ITU G.992.3 (VDSL2)
  - ITU G.992.4 (G.HS)
  - ITU G.992.5 (ADSL2+)

Sie sollten daher gewährleisten, dass das Modem am Router angeschlossen ist bevor Sie die Konfiguration starten. Das DSL-Modem sollte an der FE 0/1 Schnittstelle oder an einem definierten VLAN-Port angeschlossen werden.



Dial Pool

Über die ***Pool ID*** wird das ***Interface*** für den PPPoE Dial up festgelegt.

Parameter	Beschreibung
Enable	Aktiviert oder deaktiviert den PPPoE Eintrag
ID	Eine beliebige eindeutige ID vergeben
Pool ID	Die zuvor über Dial Pool angelegte Pool ID für das Interface, über das die Verbindung aufgebaut werden soll.
Authentication Type	Auto, PAP, CHAP ist wählbar. In den meisten Fällen kann dieser Parameter auf Auto gestellt werden.
Username	Der Benutzername, den Sie von Ihrem Provider für die Einwahl bekommen haben.
Password	Das Passwort, das Sie von Ihrem Provider für die Einwahl bekommen haben.
Local IP Address	Ihre lokale IP-Adresse
Remote IP Address	IP-Adresse des Remote-Gerätes (Modem)
Keepalive Interval	Zeit, nach der die Verbindung überprüft werden soll.
Keepalive Retry	Anzahl der Versuche, wenn eine Verbindungsüberprüfung fehlschlägt.
Debug	Bei Aktivierung wird ausführlich geloggt.

Hinweis

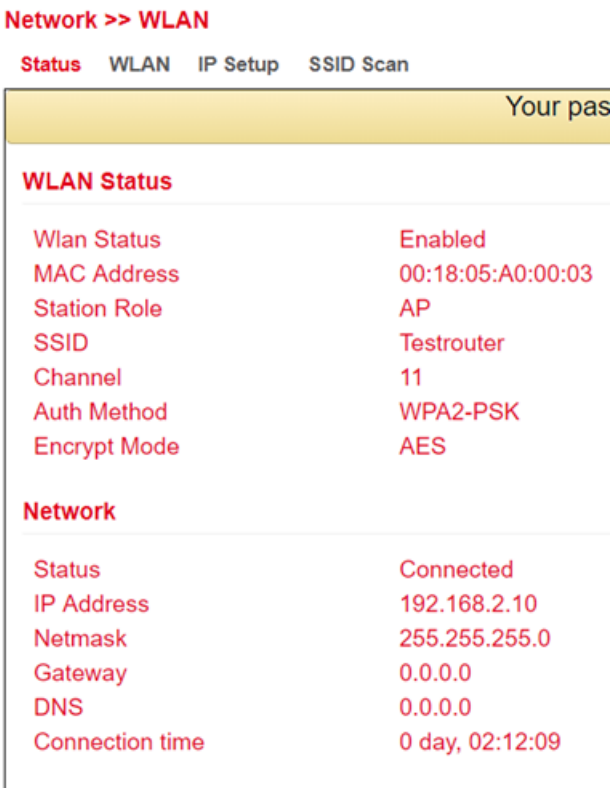
Über den Wizard kann über ***New WAN*** auch eine PPPoE Verbindung eingerichtet werden. Dies ist einfacher als die manuelle Konfiguration!

3.2.5 3.2.5. WLAN (TK8x5-EXW)

3.2.5.1. WLAN Status

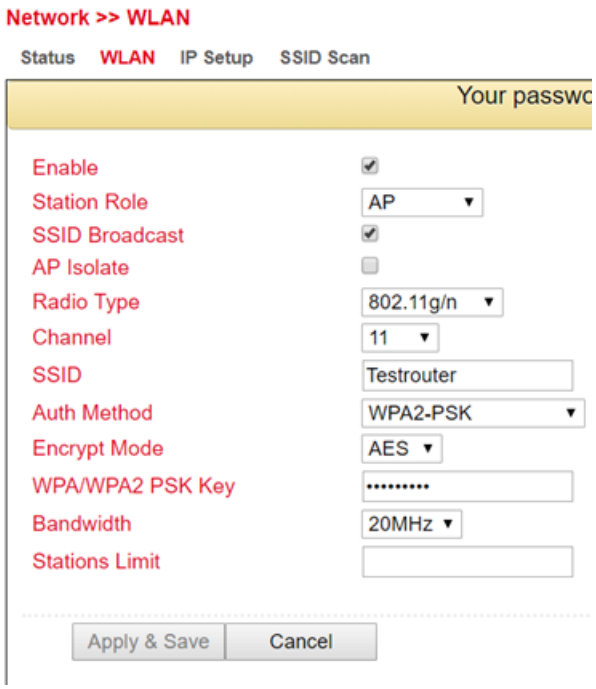
Unter ***Network > WLAN*** können Sie zunächst den Status des WLAN einsehen.

Hier kann z.B. die aktuelle SSID des Routers, die IP Adresse oder auch die Rolle des WLAN Moduls (Access Point oder Client) abgelesen werden.



3.2.5.2. WLAN Konfiguration

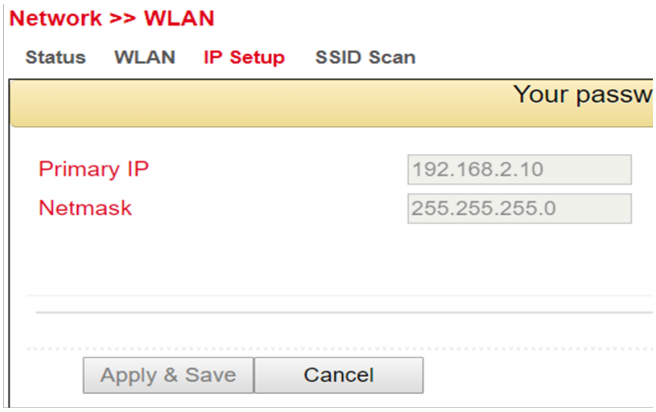
Unter ***Network*** > ***WLAN*** > ***WLAN*** können Sie das WLAN konfigurieren.



Paramet	Beschreibung	Werkseins
Enable	Aktiviert oder deaktiviert das WLAN	Deaktiviert
Station Role	AP (Access Point), Client oder AP-Client	AP
SSID Broadcast	Anzeigen der SSID, wenn diese sichtbar sein soll	Aktiviert
AP Isolate	Aktiviert oder deaktiviert die AP-Isolierung	Deaktiviert
Radio Type	Hier kann der Funkstandard ausgewählt werden	802.11g/n
Channel	Hier kann der Funkkanal ausgewählt werden	11
SSID	Die SSID, die Ihr WLAN kennzeichnet und die beim Suchen nach WLAN Netzen angezeigt werden soll.	TK800
Auth Method	Der Verschlüsselungsstandard, der genutzt werden soll. OPEN, wenn das WLAN nicht geschützt sein soll (nicht empfohlen).	OPEN
Encrypt Mode	Bei Auswahl Open oder Shared: WEP40 oder WEP104, beides wird heute eigentlich nicht mehr eingesetzt, da es nicht sicher ist. Bei Auswahl der anderen Möglichkeiten TKIP oder AES	NONE
Bandwidth	20MHz oder 40MHz Kanalbandbreite. Eine größere Kanalbandbreite kann die Geschwindigkeit erhöhen, jedoch gibt es weniger überlappungsfreie Kanäle.	20MHz
Stations Limit	Maximale Anzahl gleichzeitig verbundener Clients	leer

3.2.5.3. IP Setup

Unter ***Network > WLAN > IP Setup*** kann die IP Adresse des WLAN Interfaces geändert werden.

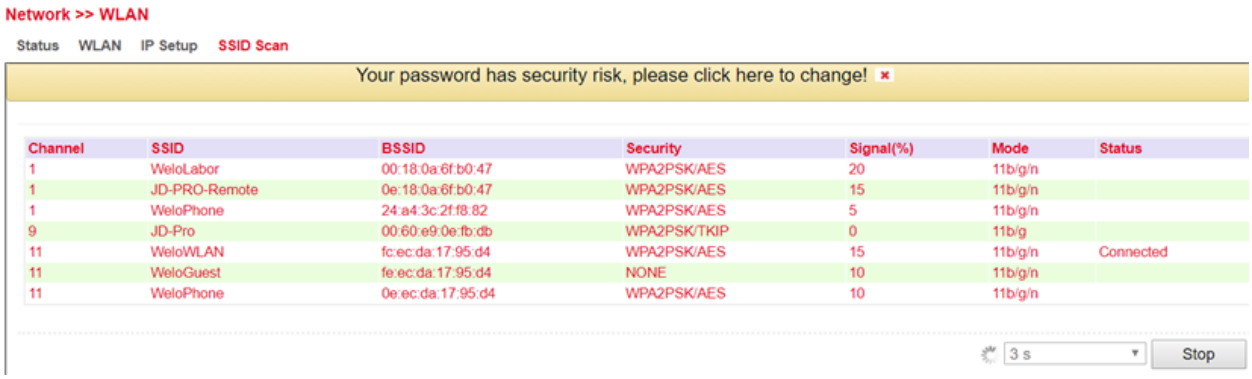


Hinweis

Die IP Adresse kann nur geändert werden, wenn das WLAN Interface kein Bridge Member ist.

3.2.5.4. SSID Scan

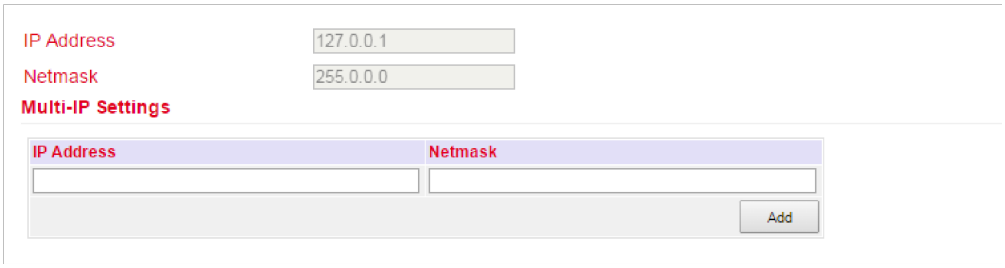
Unter ***Network > WLAN > SSID Scan*** kann nach verfügbaren WLAN-Netzen gesucht werden. Wenn Sie den TK 800 als WLAN Client konfiguriert haben, ist es möglich an dieser Stelle die in Reichweite befindlichen WLAN-Netze nach ihrer SSID zu scannen. Ist der TK 800 als Client mit einem WLAN verbunden, wird Ihnen dies im Status mit Connected angezeigt.



3.2.6 3.2.6. Loopback

3.2.6.1. Loopback Configuration

Unter ***Network > Loopback*** können Sie weitere Loopback IP-Adressen eintragen. Die Standard Loopback IP-Adresse 127.0.0.1 kann nicht bearbeitet werden.



3.3 3.3. Services

3.3.1 3.3.1. DHCP

Das **Dynamic Host Configuration Protocol** (**DHCP**) ist ein Kommunikationsprotokoll in der Computertechnik. Es ermöglicht die Zuweisung der Netzwerkkonfiguration an Clients durch einen Server.

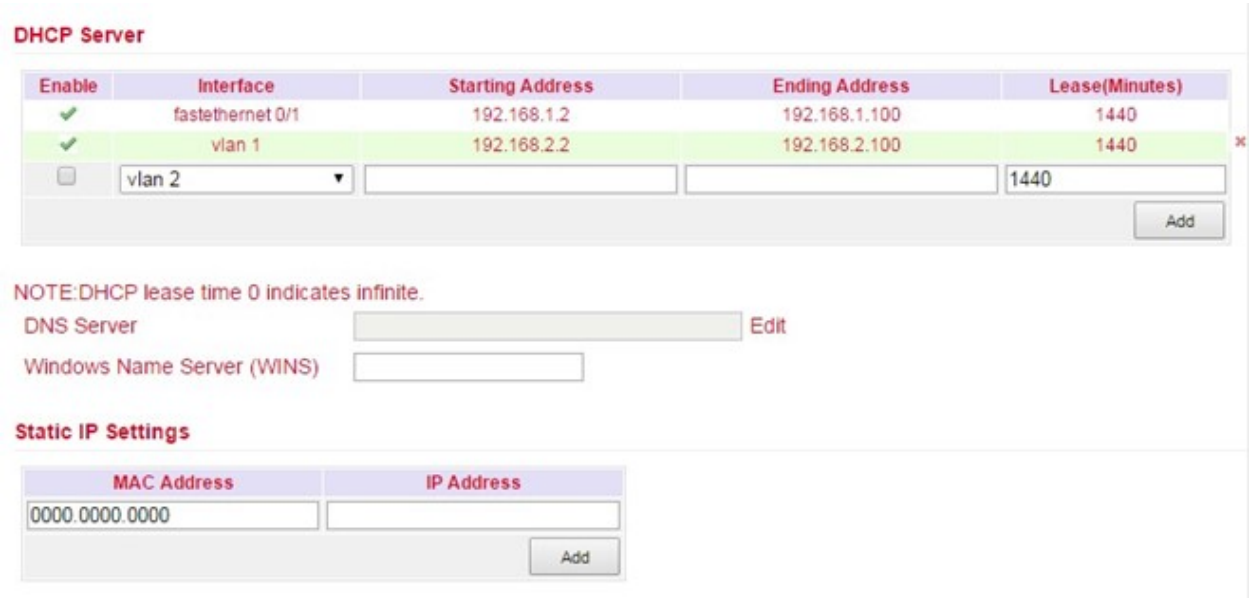
3.3.1.1. DHCP Status

Unter ***Services > DHCP > Status*** können Sie einsehen, wer gerade mit dem Router über welches Interface verbunden ist.

Interface	MAC Address	IP Address	Host	Lease
Vlan1	00:0E:C6:CD:23:FE	192.168.2.12		
vlan 1	00:18:05:0C:C3:9C	192.168.2.75	Router	0 day, 21:44:48
Vlan1	00:0E:C6:CD:23:FE	192.168.2.77	NB-Holm	0 day, 23:57:58

3.3.1.2. DHCP Server

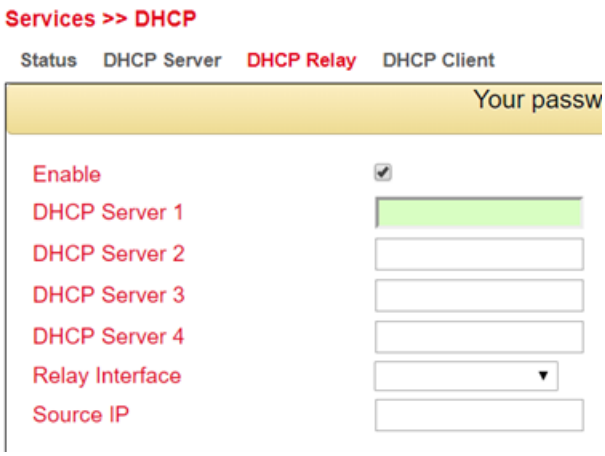
Unter ***Services*** > ***DHCP*** > ***DHCP Server*** können Sie Einstellungen für den DHCP Server konfigurieren. Das entsprechende Interface auswählen und die Start- bzw. End-IP-Adresse, sowie das Lease eintragen, s. Beispiel.



Mit ***Static IP Settings*** kann einer bestimmten MAC Adresse eine IP Adresse zugewiesen werden.

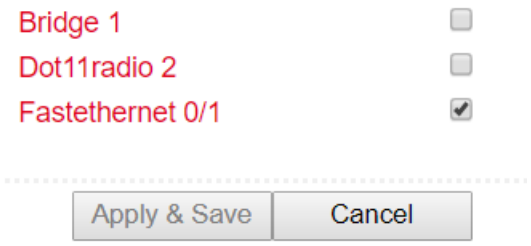
3.3.1.3. DHCP Relay

Unter ***Services*** > ***DHCP*** > ***DHCP Relay*** können Sie entfernte DHCP Server angeben, die dann die DHCP Verwaltung für die am Router angeschlossenen Netze übernehmen. Durch Anklicken von Enable, aktivieren Sie diese Funktion.



3.3.1.4. DHCP Client

Unter ***Services*** > ***DHCP*** > ***DHCP Client*** kann der Router selbst eine DHCP Adresse von einem DHCP Server erhalten. Dazu wählen Sie das Interface aus, welches per DHCP konfiguriert werden soll. Die Interfaces können je nach Routermodell variieren.



3.3.2 3.3.2. DNS

Das **Domain Name System** (**DNS**) ist einer der wichtigsten Dienste in vielen IP-basierten Netzwerken. Seine Hauptaufgabe ist die Beantwortung von Anfragen zur Namensauflösung.

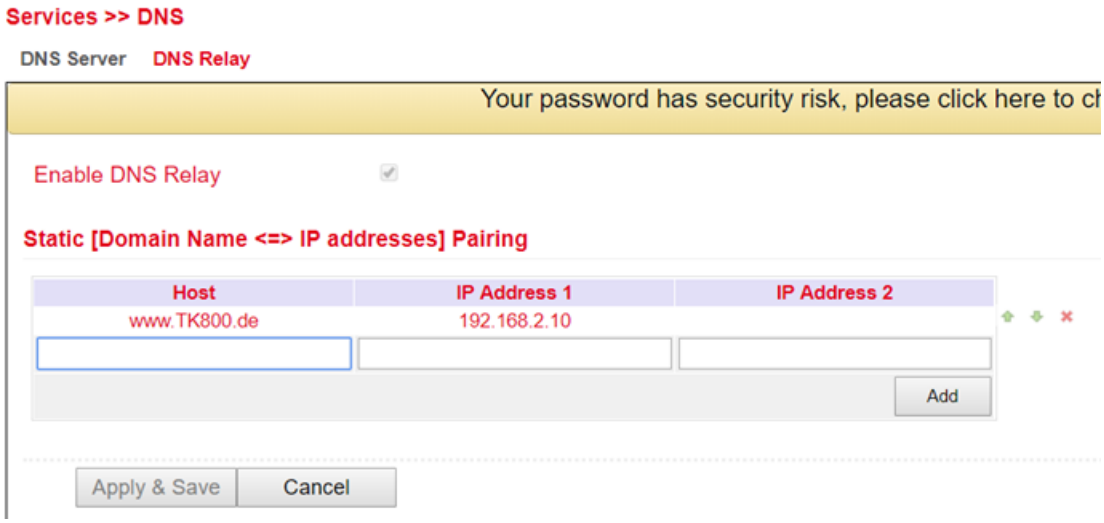
Das DNS funktioniert ähnlich wie eine Telefonauskunft. Der Benutzer kennt die Domain (Name eines Servers im Internet) z. B. welotec.com und sendet diese als Anfrage in das Internet. Die Domain wird dann dort vom DNS in die zugehörige IP-Adresse (wenn man so will die „Anschlussnummer“ im Internet) umgewandelt. Z.B. eine IPv4-Adresse der Form 192.168.2.1 und führt so zum richtigen Server.

3.3.2.1. DNS Server

Unter ***Services*** > ***DNS*** > ***DNS Server*** können Sie zwei DNS Server eintragen. Diese gelten dann für alle Interfaces, außer es wurde per DHCP ein anderer DNS Server zugewiesen.

3.3.2.2. DNS Relay

Unter ***Services*** > ***DNS*** > ***DNS Relay*** können Sie DNS Auflösungen auch manuell eintragen. Durch klicken auf Add fügen Sie den Eintrag hinzu und mit Apply & Save übernehmen Sie diesen.

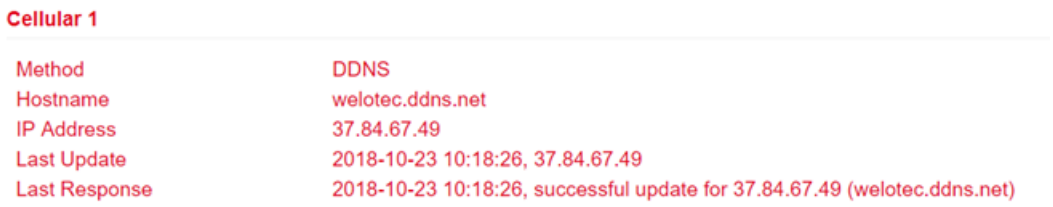


3.3.3 3.3.3. DDNS

Dynamisches DNS oder **DDNS** ist eine Technik, um Domains im Domain Name System (DNS) dynamisch zu aktualisieren. Der Zweck ist, dass ein Computer (bspw. ein PC oder ein Router) nach dem Wechsel seiner öffentlichen IP-Adresse automatisch und schnell den dazugehörigen Domaineintrag ändert. So ist der Rechner immer unter demselben Domainnamen erreichbar, auch wenn die aktuelle IP-Adresse für den Nutzer unbekannt ist. Gängige Anbieter für diesen Dienst sind z.B. DynDNS oder NoIP.

3.3.3.1. DDNS Status

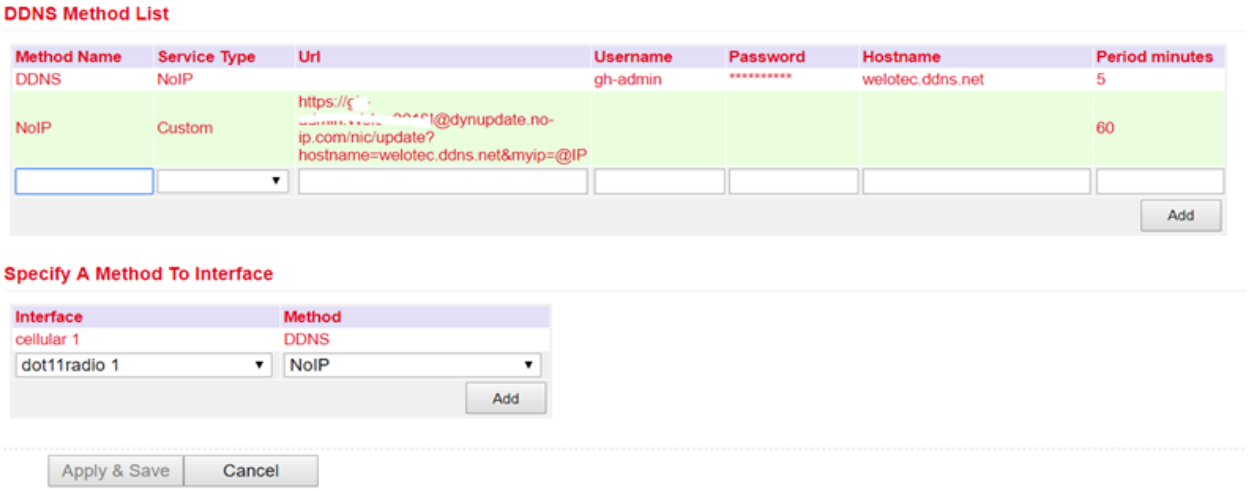
Unter ***Services*** > ***DDNS*** > ***Status*** werden Ihnen die aktuell genutzten DDNS Services angezeigt.



3.3.3.2. DDNS

Unter ***Services*** > ***DDNS*** > ***DDNS*** können Sie einen neuen DDNS-Dienst hinzufügen. Wichtig ist, dass zunächst ein neuer DDNS-Service unter DDNS Method List angelegt wird.

Anschließend müssen Sie diesen noch einem Interface zuordnen, dies geschieht unter ***Specify A Method To Interface.***



DDNS Method List	
Method Name	Frei wählbarer Name für den Service.
Service Type	Hier sind die gängigsten DDNS-Services aufgeführt. Wenn der DDNS-Service nicht aufgeführt ist, so kann über Custom ein individueller DDNS-Service genutzt werden.
Url	Wird nur für die Auswahl Custom bei Service Type genutzt. Hier wird dann die vollständige Url des DDNS-Services eingetragen inkl. Username und Passwort, z.B. für NoIP https://username:password@dynupdate.no-ip.com/nic/update?hostname=welotec.ddns.net&myip=@IP Der Parameter @IP aktualisiert immer die zugewiesene IP-Adresse
Username	Hier wird der Benutzername für den DDNS-Service eingetragen.
Password	Hier wird das Passwort für den DDNS-Service eingetragen.
Hostname	Der Name der Domain, die verwendet wird.
Period minutes	Gibt an, wie oft ein Update der IP-Adresse durchgeführt werden soll. Eingabewerte können von 1 bis 999999 Minuten eingegeben werden.

Specify A Method To Interface	
Interface	Das Interface des Routers, dessen IP-Adresse über den DDNS-Service erreichbar sein soll.
Method	Eine zuvor unter DDNS Method List angelegter DDNS-Service.

Hinweis

Sie benötigen einen Account eines DDNS Anbieters, den Sie vorher konfigurieren müssen. Dieser Account kann kostenpflichtig sein, je nach Anbieter.

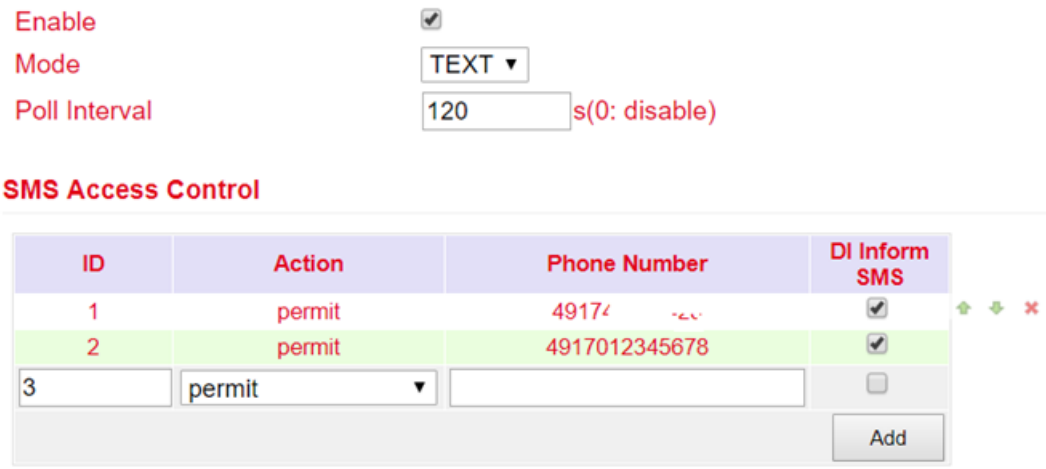
3.3.4 3.3.4. SMS

Einleitung

Der TK800 ist per SMS von außen erreichbar und reagiert auf verschiedene Befehle, die per SMS gesendet werden. So ist es möglich, den Status des Gerätes abzufragen, die Einwahl zu starten / zu stoppen oder das Gerät neu zu starten.

Statusabfrage / Neustart

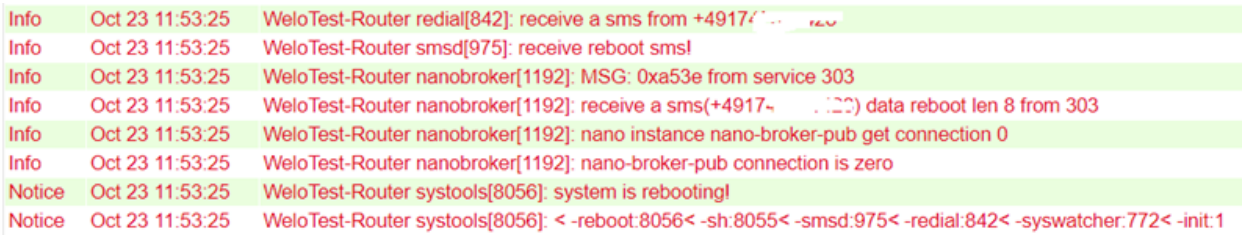
1. Gehen Sie über den Menüpunkt ***Services*** auf den Unterpunkt ***SMS***
2. Klicken Sie auf die Checkbox ***Enable***, um die Funktion einzuschalten



3. Geben Sie in die Tabelle ***SMS Access Control*** die Telefonnummern ein, welche SMS an den Router senden dürfen (Format 4917123456789, kein 0049 oder +49!) und tragen Sie als Action ***permit*** ein

Wird nun eine SMS mit dem Inhalt ***show*** an die Mobilfunknummer des Routers gesendet, so sendet der Router seinen aktuellen Status als Antwort

Wird eine SMS mit dem Inhalt ***reboot*** an den Router gesendet, so startet dieser neu. Man kann diesen Prozess auch im Log des Routers verfolgen.

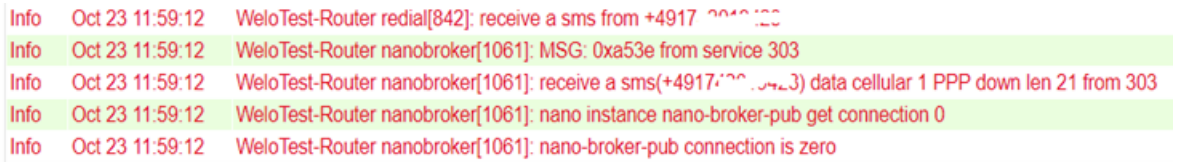


Herstellen oder Trennen der Internetverbindung

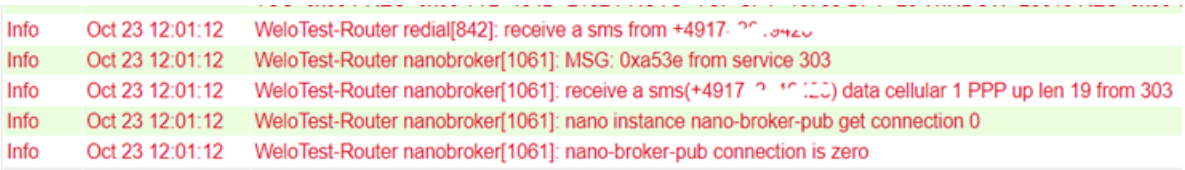
Nach erfolgreicher Konfiguration können Sie die Internetverbindung des Routers ebenfalls per SMS steuern. Dazu ist es allerdings notwendig, dass der Router auf „Connect On Demand“ steht!

1. Gehen Sie über den Menüpunkt ***Network*** auf den Unterpunkt ***Cellular***
2. Wählen Sie nun den Reiter ***Cellular*** aus

3. Wählen Sie hier unter ***Connection Mode*** den Modus ***Connect On Demand*** aus und aktivieren Sie das Feld ***Triggered by SMS***. Nun können Sie folgende Befehle per SMS an den Router senden:
   cellular 1 ppp down - trennt die Internetverbindung (s. Abb.)

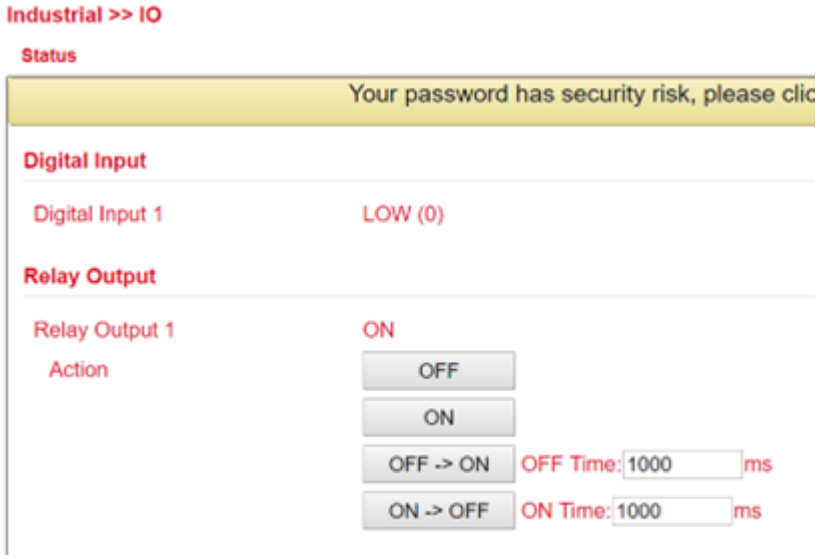


cellular 1 ppp up - stellt die Internetverbindung wieder her (s. Abb.)



Digitales Relay ein- oder ausschalten

Ein weiterer wichtiger SMS-Befehl ist das ein- bzw. ausschalten des digitalen Relays per SMS.



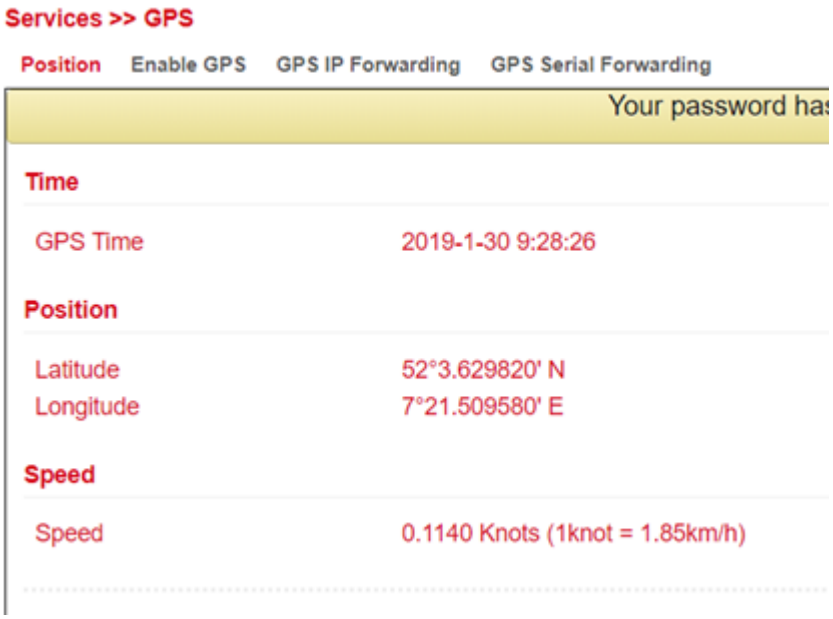
Folgende SMS Befehle können dafür verwendet werden

- *io output 1 on - schaltet das Relay ein*
- *io output 1 off - schaltet das Relay aus*

3.3.5 3.3.5. GPS (TK8x5L-EGW bzw. TK8x5L-EDW)

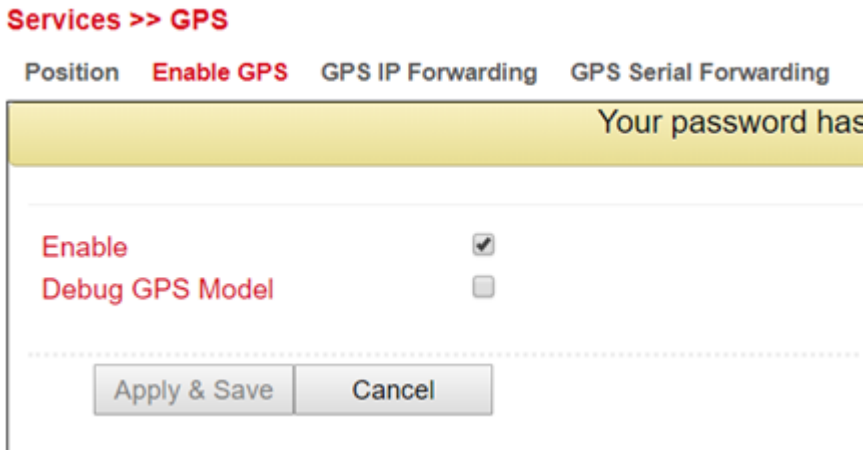
3.3.5.1. Position

Unter ***Services*** > ***GPS*** > ***Position*** werden Ihnen die Daten zur aktuellen Position angezeigt, wenn die entsprechende Antenne am Router angeschlossen ist.



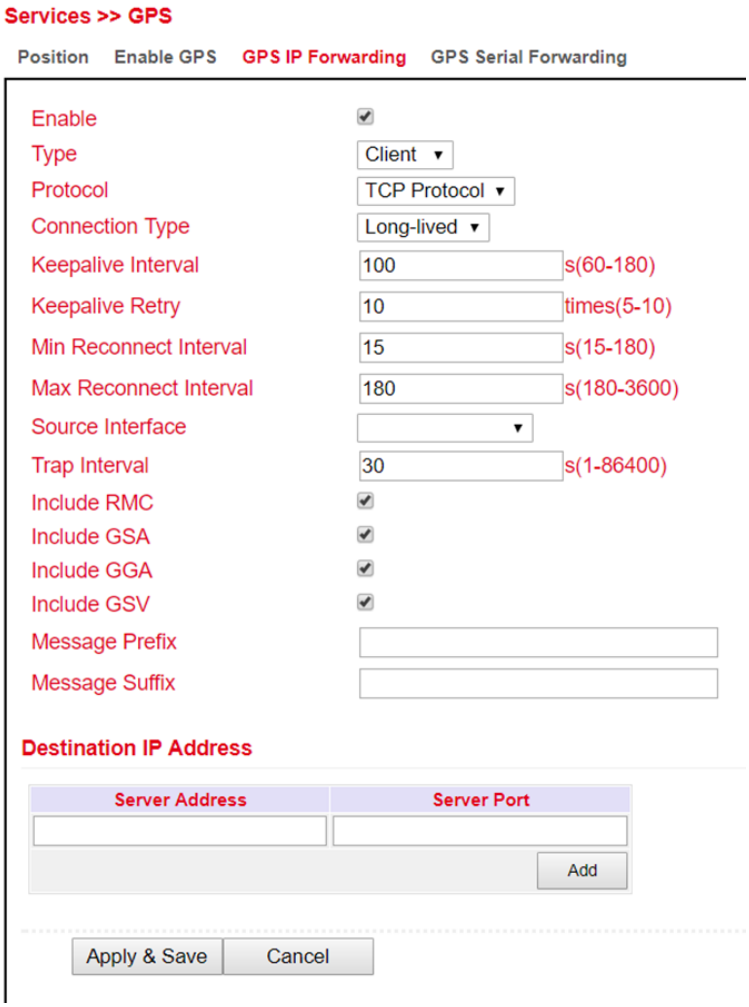
3.3.5.2. Enable GPS

Um die GPS Funktion des Routers zu aktivieren öffnen Sie das Menü unter ***Services*** > ***GPS*** > ***Enable GPS*** und klicken Sie auf die Checkbox ***Enable***, um die Funktion einzuschalten. Mit ***Apply & Save*** speichern Sie die Einstellungen und aktivieren das GPS.



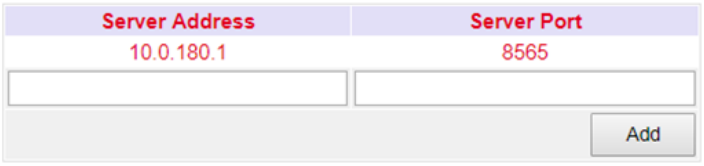
3.3.5.3. GPS IP Forwarding

Öffnen Sie das Menü unter ***Services > GPS > GPS IP Forwarding*** und klicken Sie auf die Checkbox ***Enable***, um die Funktion einzuschalten. Diese Funktion steht nur zur Verfügung, wenn das Debug GPS Model (aus dem vorherigen Kapitel) deaktiviert ist. Hier können Sie nun die entsprechenden Einstellungen vornehmen. Mit ***Apply & Save*** speichern Sie die Einstellungen und aktivieren diese.



GPS IP Forward List	
Type	Auswahl zwischen Client und Server
Protocol	Es kann hier zwischen den Protokollarten TCP- oder UDP gewählt werden.
Connection Type	Auswahl von Long-lived oder Short-lived möglich. Standard ist Long-lived
Keepalive Interval	Eintrag zwischen 60 und 180 Sekunden möglich. Standard = 100s.
Keepalive Retry	Die Anzahl der Wiederholungen darf hier zwischen 5- und 10-mal liegen. Standard = 10
Min Reconnect Interval	Min. Intervall für die Wiederverbindung zw. 15 und 180 Sekunden. Standard = 15s.
Max Reconnect Interval	Min. Intervall für die Wiederverbindung zw. 180 und 3600 Sekunden. Standard = 180s.
Source Interface	Auswahl des entsprechenden Interfaces an das weitergeleitet werden soll
Trap Interval	Das Intervall darf zwischen 1 und 86400 Sekunden liegen. Standard = 30
Include RMC	Empfohlener Minimumdatensatz. Bei Auswahl wird das Minimum des GPS-Empfängers ausgegeben
Include GSA	Aktive Satelliten. Hier werden Informationen über PRN-Nummern der Satelliten ausgegeben, deren Signal zur Pos.-Bestimmung verwendet werden
Include GGA	Wichtigster Datensatz mit Zeit, Position, Höhe und Qualität der Messung
Include GSV	Sichtbare Satelliten. Liefert Informationen über Satelliten, die zurzeit möglicherweise empfangen werden können und Informationen zu deren Position, Signalstärke usw. Da pro Satz nur die Informationen von vier Satelliten übertragen werden können (Beschränkung auf 82 Zeichen), kann es bis zu drei solche Datensätze geben
Message Prefix	Eingabe eines Nachrichten Präfix möglich. Freie Eingabe
Message Suffix	Eingabe eines Nachrichten Suffix möglich. Freie Eingabe

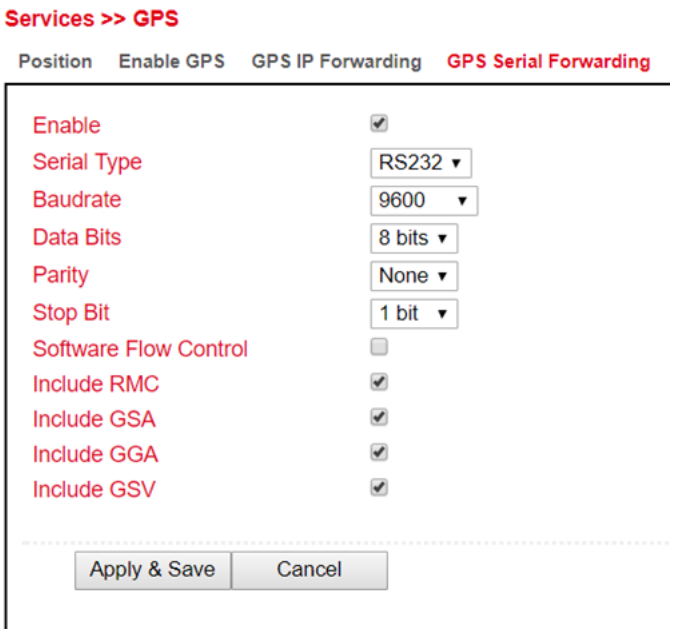
Destination IP Address



Eingabe einer Zieladresse für einen Server ist an dieser Stelle möglich.

3.3.5.4. GPS Serial Forwarding

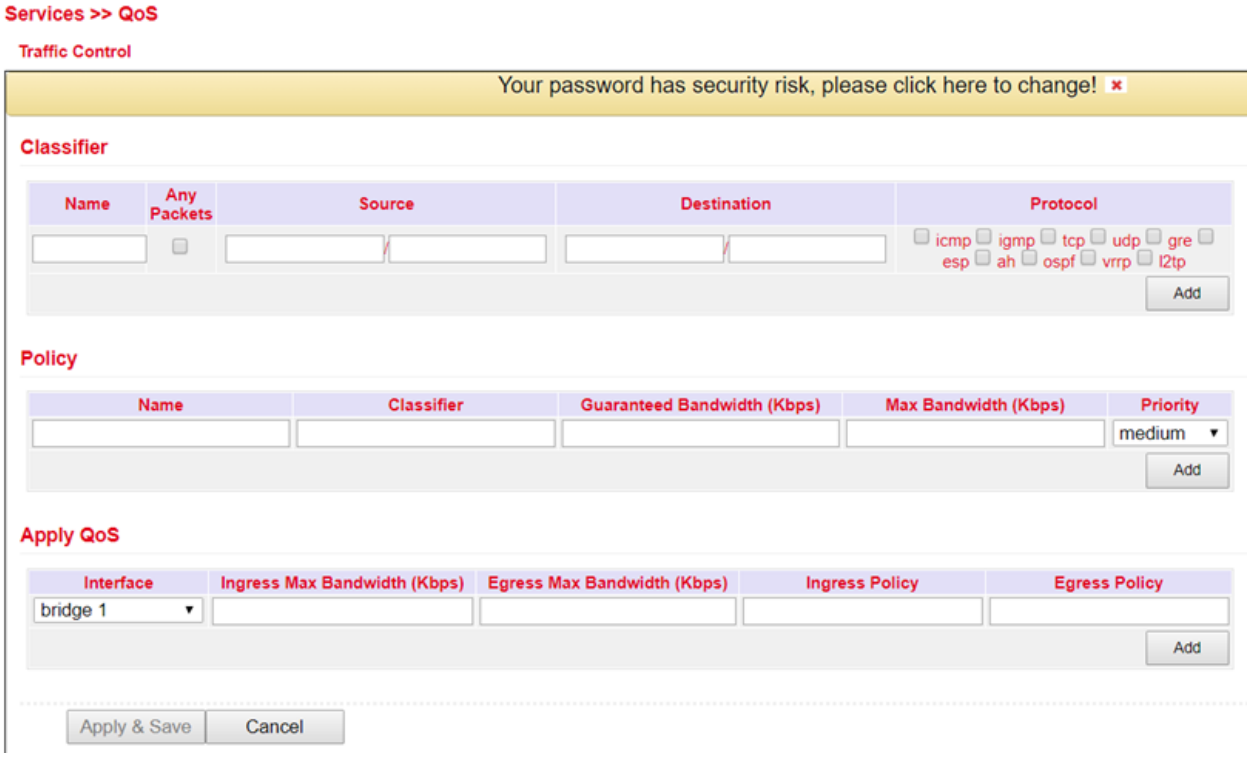
Öffnen Sie das Menü unter ***Services*** > ***GPS*** > ***GPS*** Serial Forwarding und klicken Sie auf die Checkbox ***Enable***, um die Funktion einzuschalten. Hier können Sie nun die entsprechenden Einstellungen vornehmen. Mit ***Apply & Save*** speichern Sie die Einstellungen und aktivieren diese.



GPS Serial Forwardi List	
Serial Type	Auswahl der seriellen Schnittstelle. RS232 oder RS485.
Baudrate	Hier kann die Übertragungsrate gewählt werden. Wert zwischen 300 und 230400 möglich. Standard = 9600
Data Bits	Einstellung der Datenbits. Auswahl zwischen 7 bits und 8 bits. Standard = 8 bits
Parity	Hier kann die Parität für die Schnittstelle eingestellt werden. Standard = none
Stop Bit	Einstellung der Stop Bits. Standard = 1 bit
Software Flow Control	Kann ein oder ausgeschaltet werden. Standard = aus
Include RMC	Empfohlener Minimumdatensatz. Bei Auswahl wird das Minimum des GPS-Empfängers ausgegeben
Include GSA	Aktive Satelliten. Hier werden Informationen über PRN-Nummern der Satelliten ausgegeben, deren Signal zur Pos.-Bestimmung verwendet werden
Include GGA	Wichtigster Datensatz mit Zeit, Position, Höhe und Qualität der Messung
Include GSV	Sichtbare Satelliten. Liefert Informationen über Satelliten, die zurzeit möglicherweise empfangen werden können und Informationen zu deren Position, Signalstärke usw. Da pro Satz nur die Informationen von vier Satelliten übertragen werden können (Beschränkung auf 82 Zeichen), kann es bis zu drei solche Datensätze geben

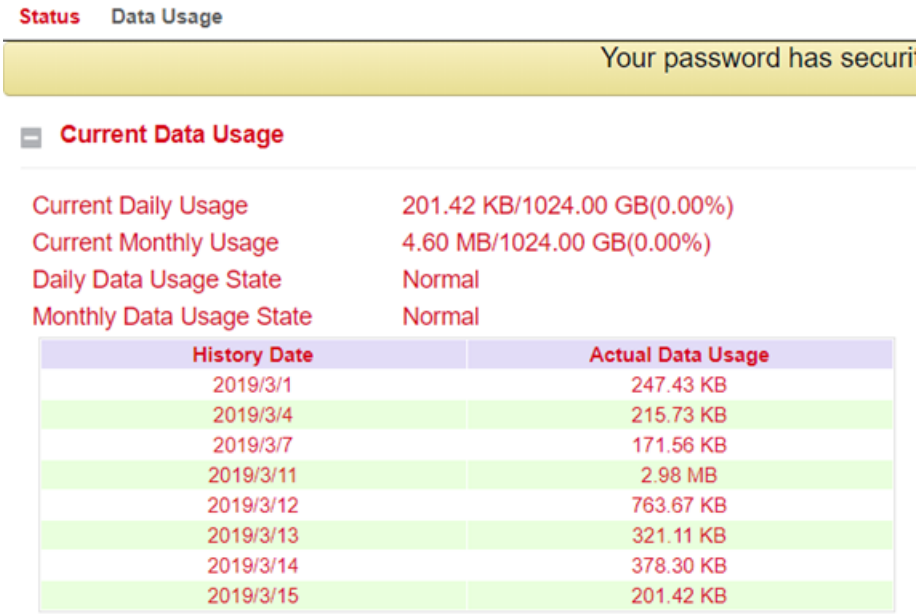
3.3.6 3.3.6. QoS

An dieser Stelle ist die Definition eines Quality of Service möglich. Wählen Sie ***Services > QoS.***



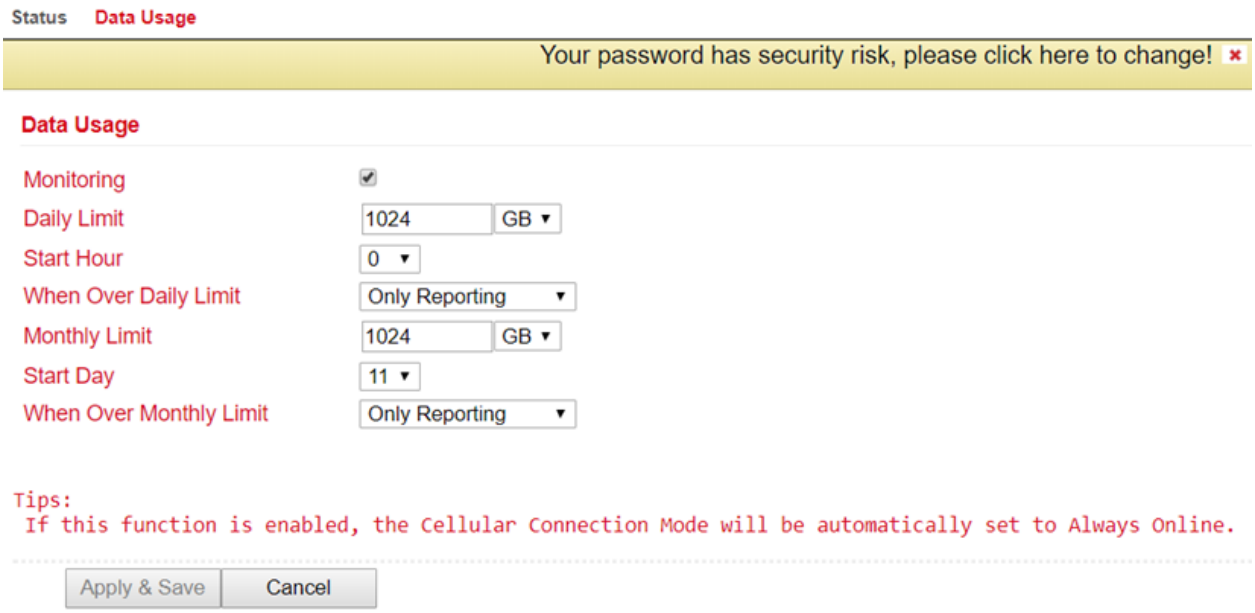
3.3.7 3.3.7. Data Usage

In diesem Bereich können Sie den Verbrauch Ihre Daten sehen, wenn Sie dies unter Data Usage konfiguriert haben. Wählen Sie ***Services > Data Usage.***



3.3.7.1 Data Usage

Öffnen Sie das Menü unter Service > Data Usage und Data Usage. Setzen Sie nun den Haken bei Monitoring, um diesen Bereich zu aktivieren. Tragen Sie nun Ihre Daten ein.



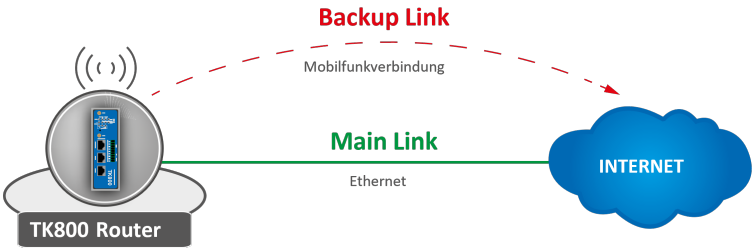
Data Usage	
Monitoring	Aktivieren Sie hier Ihre Datenverbrauchs-Anzeige
Daily Limit	Tragen Sie hier einen Richtwert für das Tageslimit ein. Angaben können in KB, MB oder GB gemacht werden.
Start Hour	Zeitpunkt zu der die Messung gestartet werden soll.
When Over Daily Limit	Hier können Sie eintragen was passieren soll, wenn das eingegebene Limit erreicht bzw. überschritten wird. Auswahlmöglichkeiten sind: Only Reporting Hier wird lediglich der Verbrauchswert angezeigt Stop Forward Hier wird der weitere Verbrauch von Daten gestoppt Shutdown Interface Hier wird das Interface ausgeschaltet
Monthly Limit	Tragen Sie hier einen Richtwert für das Monatslimit ein. Angaben können in MB oder GB gemacht werden.
Start Day	Wählen Sie hier den Tag aus an dem die Messung für das Monatslimit starten soll
When Over Monthly Limit	Hier können Sie eintragen was passieren soll, wenn das eingegebene Limit erreicht bzw. überschritten wird. Auswahlmöglichkeiten sind: Only Reporting Hier wird lediglich der Verbrauchswert angezeigt Stop Forward Hier wird der weitere Verbrauch von Daten gestoppt Shutdown Interface Hier wird das Interface ausgeschaltet

3.4 3.4. Link Backup

Mit dem TK800 ist es möglich, zwei verschiedene Internetverbindungen (kabelgebunden und Mobilfunk) zur Erhöhung der Erreichbarkeit zu nutzen.

Der Router überprüft dabei die primäre Internetverbindung periodisch und schaltet bei Ausfall automatisch auf die sekundäre Internetverbindung um. Sobald die primäre Internetverbindung wieder verfügbar ist, schaltet der Router wieder automatisch auf diese Verbindung um.

In diesem Beispiel wird eine kabelgebundene (Ethernet, DHCP) als primäre und Mobilfunk (4G LTE) als sekundäre Internetverbindung verwendet.



Konfigurieren eines WAN-Ports – Bridge modifizieren (nur TK8X2-X)

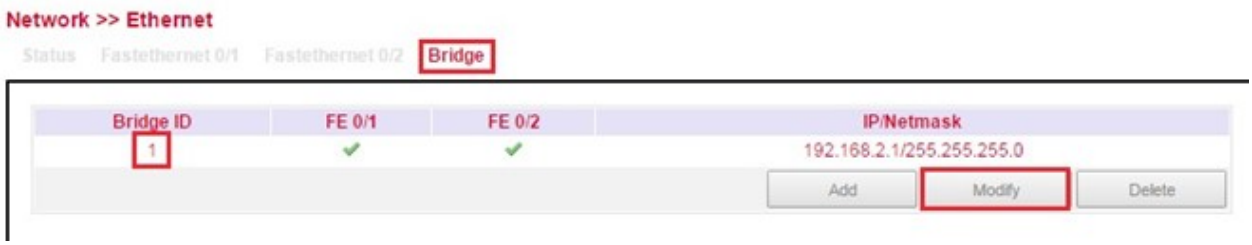
Hinweis

Voraussetzung für das Link Backup ist der Internetzugang über das Mobilfunknetz. Konfigurieren Sie also die Mobilfunkschnittstelle (Cellular) entsprechend, um eine Verbindung zum Internet herstellen zu können. Der Router ist für T-Mobile SIM-Karten vorkonfiguriert, hier sind also in der Regel keine Konfigurationsschritte nötig.

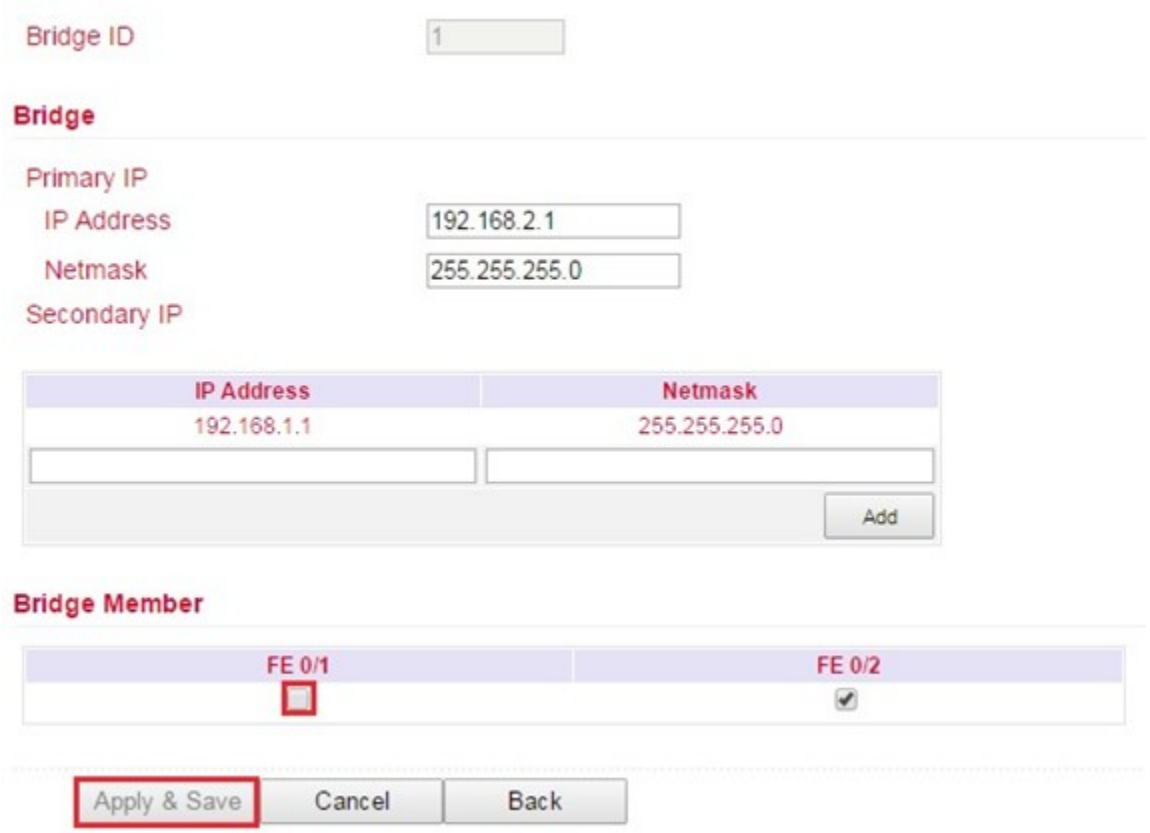
Beim TK8X2-X hängen die beiden Ethernet-Ports werkseitig über eine Bridge zusammen. Für die Konfiguration eines der Ports zum WAN-Port muss der entsprechende Port aus der Bridge ausgeschlossen werden.

Führen Sie dazu die folgenden Schritte aus:

1. Gehen Sie über den Unterpunkt ***Network*** auf den Unterpunkt ***Ethernet***
2. Wählen Sie nun den Reiter ***Bridge***
3. Klicken Sie hier in die Zeile mit der Bridge ID 1 und Bearbeiten Sie den Eintrag durch Klicken auf ***Modify***



4. Entfernen Sie den Haken für das Interface FE 0/1 und bestätigen Sie die Änderung mit ***Apply & Save***

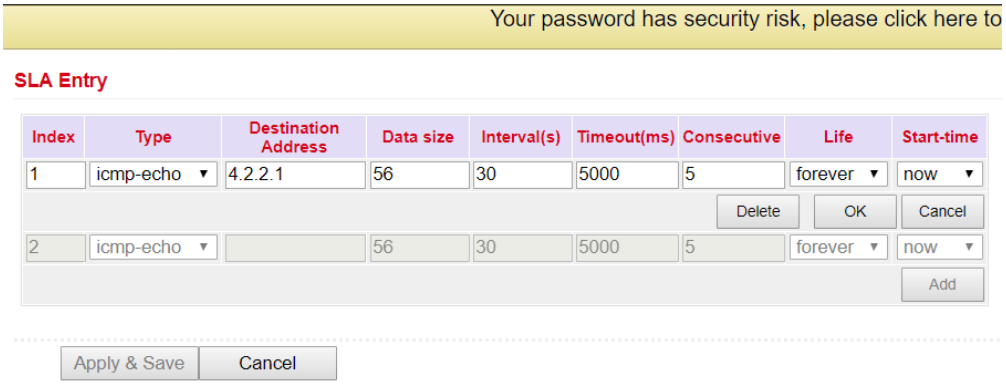


Konfigurieren eines WAN-Ports

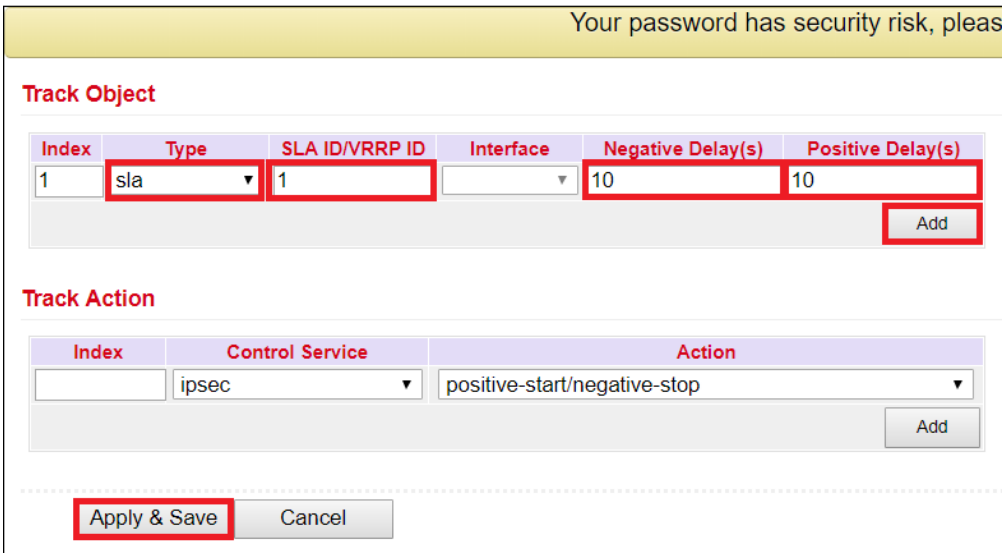
In dieser Anleitung wird der Port FE 0/1 als WAN-Port definiert. Hierfür wird der Wizard New WAN verwendet.

- Im Menü Wizard kann über den Unterpunkt New WAN ein neuer WAN-Port konfiguriert werden
- als Interface wird der gerade von der Bridge gelöste Ethernet-Port (FE 0/1) angegeben, exemplarisch wird außerdem DHCP für den Port verwendet
- NAT muss aktiviert werden, wenn die angeschlossenen Geräte eine Verbindung ins Internet aufbauen sollen

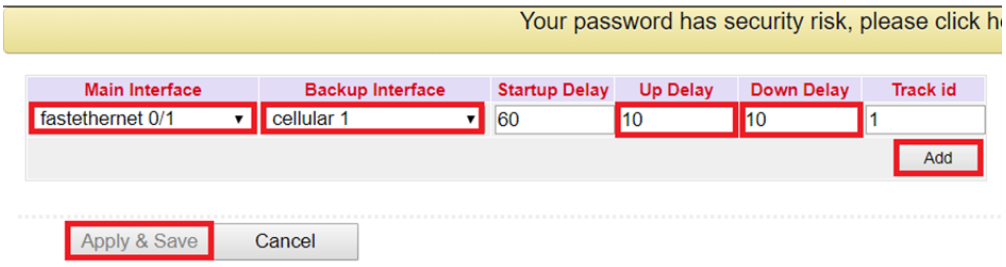
- im nächsten Schritt wird das ICMP-Programm (SLA) konfiguriert
- unter IP Addresse (Destination Address) sollte eine pingbare IP-Adresse mit hoher Verfügbarkeit eingetragen werden (Anm.: In diesem Beispiel wurde 4.2.2.1 eingetragen, da diese Adresse eine sehr hohe Verfügbarkeit vorweist.)
- alle weiteren Daten können aus dem Beispiel übernommen werden



- das soeben erstellte SLA-Programm wird mit Hilfe des Trackings überwacht, um eine Unterbrechung der Hauptleitung registrieren zu können
- konfiguriert wird dies wie im folgenden Beispiel



- um zu definieren, welche als Haupt- und welche als Backup-Leitung fungiert, wird das Interface Backup eingerichtet
- konfiguriert wird dies wie im folgenden Beispiel



Beschreibung der Konfigurationselemente:

Main Interface	primäre Leitung, die überwacht werden soll
Backup Interface	sekundäre Leitung, auf die bei Ausfall der Primärleitung zurückgegriffen wird
Startup Delay	Einschaltverzögerung der Interfaceüberwachung
Up Delay	Umschaltverzögerung
Down Delay	Umschaltverzögerung
Track ID	Verweis auf ICMP-Überwachung

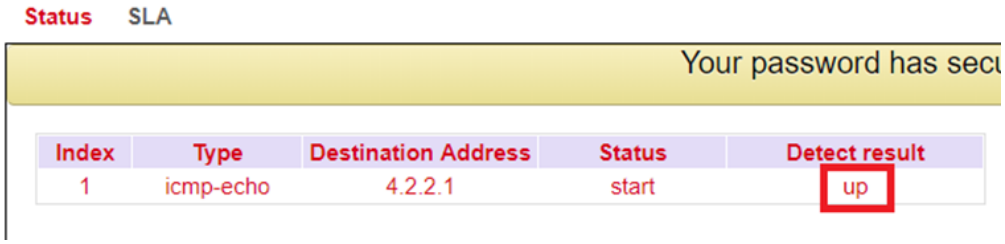
Im letzten Schritt werden die Routingeinträge wie im folgenden Beispiel angelegt bzw. angepasst. Wichtig ist, dass die Distance der Hauptleitung (hier: FE 0/1) einen kleineren Wert hat, als die der Backup-Leitung. Mit der TrackID wird die Hauptleitung an die ICMP-Überwachung gebunden, die im vorherigen Schritt erstellt wurde ***Beschreibung der Konfigurationselemente:***

Destination	Zieladresse, wohin geroutet werden soll
Netmask	zur Zieladresse gehörige Subnetzmaske
Interface	Interface, über das gesendet werden soll
Gateway	IP-Adresse, über die gesendet werden soll
Distance	Präferenz/Kosten der Route
Track ID	Verweis auf ICMP-Überwachung

Hauptleitung funktioniert (Internetverbindung über WAN)

Wenn die Hauptleitung funktioniert und eine Internetverbindung darüber aufgebaut ist, lässt sich folgendes nachvollziehen:

1. SLA-Status



2. Track-Status

3. Status der Mobilfunkverbindung

Status Cellular

Your pa

Modem

Active SIM	SIM 1
IMEI Code	358709051708661
IMSI Code	262011404043251
ICCID Code	89490200001377159697
Phone Number	+491713020694
Signal Level	(22 asu -69 dBm)
RSRP	-78 dBm
RSRQ	-7 dB
Register Status	registered
Operator	Telekom.de
Network Type	4G
LAC	2EE3
Cell ID	1E13100

4. Status der WAN-Verbindung (Ethernet)

Status Ethernet 0/1 Bridge

Your pas

Fastethernet 0/1

Connection Type	Dynamic Address (DHCP)
IP Address	192.168.111.67
Netmask	255.255.255.0
Gateway	192.168.111.1
DNS	192.168.111.20
MTU	1500
Status	Up
Connection time	0 day, 00:00:16
Remaining Lease	4 days, 23:59:44
Description	

5. Routing-Tabelle

Route Table Static Routing

Your password has security risk, please click here to ch

Type: All

Type	Destination	Netmask	Gateway	Interface	Distance/Metric	Time
S	0.0.0.0	0.0.0.0	192.168.111.1	fastethernet 0/1	1/0	
C	127.0.0.0	255.0.0.0		loopback 1	0/0	
C	192.168.2.0	255.255.255.0		bridge 1	0/0	
C	192.168.111.0	255.255.255.0		fastethernet 0/1	0/0	

Hauptleitung funktioniert nicht (Internetverbindung über Mobilfunk)

Wenn die Hauptleitung nicht funktioniert und eine Internetverbindung über das Mobilfunkinterface (Cellular) aufgebaut ist, lässt sich folgendes nachvollziehen:

1. SLA-Status

Status SLA

Your password has secu

Index	Type	Destination Address	Status	Detect result
1	icmp-echo	4.2.2.1	start	down

2. Track-Status

Status Track

Index	Status
1	negative

3. Status der Mobilfunkverbindung

Status Cellular

Your pass

Modem

Active SIM	SIM 1
IMEI Code	358709051708661
IMSI Code	262011404043251
ICCID Code	89490200001377159697
Signal Level	(23 asu -67 dBm)
RSRP	-80 dBm
RSRQ	-6 dB
Register Status	registered
Operator	Telekom.de
Network Type	4G
LAC	2EE3
Cell ID	1E13100

Network

Status	Connected
IP Address	37.81.115.149
Netmask	255.255.255.252
Gateway	37.81.115.150
DNS	10.74.210.210 10.74.210.211
MTU	1500
Connection time	0 day, 00:00:04

4. Routing-Tabelle

Route Table Static Routing

Your password has security risk, please click here to

Type: All

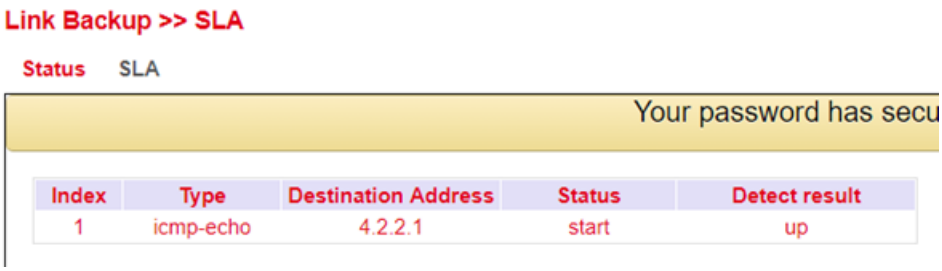
Type	Destination	Netmask	Gateway	Interface	Distance/Metric	Time
C	37.81.115.148	255.255.255.252		cellular 1	0/0	
C	127.0.0.0	255.0.0.0		loopback 1	0/0	
C	192.168.2.0	255.255.255.0		bridge 1	0/0	

3.4.1 3.4.1. SLA

Das SLA-Monitoring überwacht die Verbindungen zu Gegenstellen innerhalb einer Netzwerkstruktur. Ping-Tests zu definierten Zielen geben Aufschluss über die Verfügbarkeit der Peers und zeigen im Status den Zustand der Leitung an (up oder down).

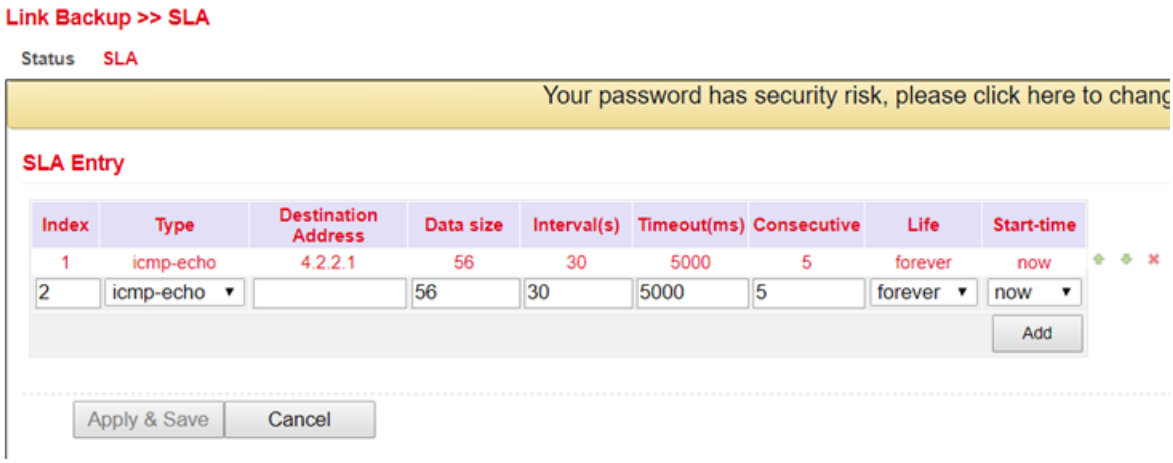
3.4.1.1. Status

Der SLA Status zeigt an, ob der Pingversuch erfolgreich ***(Detect result up)*** oder nicht erfolgreich ist ***(Detect result down)***.



3.4.1.2. SLA Konfiguration

Tragen Sie unter ***Link Backup*** > ***SLA*** > ***SLA*** die gewünschten Daten ein, um den Status der Leitung zu überwachen.



Parameter	Bedeutung
Index	Frei wählbar, dient zur Identifizierung des Eintrags.
Type	icmp-echo, ein einfacher Ping zur Prüfung der Verbindung.
Destination Address	Die Adresse, die angepingt wird. Sie sollte nach Möglichkeit hochverfügbar sein, z.B. ein Google-DNS-Server (8.8.8.8).
Data size	Die Paketgröße eines Pings, üblicherweise 56 Byte.
Interval(s)	Das Zeitintervall in Sekunden, in dem der Ping ausgeführt wird.
Timeout(ms)	Timeout für einen Ping.
Consecutive	Anzahl der Wiederholungen, bei einem fehlgeschlagenen ping.
Life	forever, der Ping soll immer ausgeführt werden.
Start-time	now, die Überprüfung soll sofort starten.

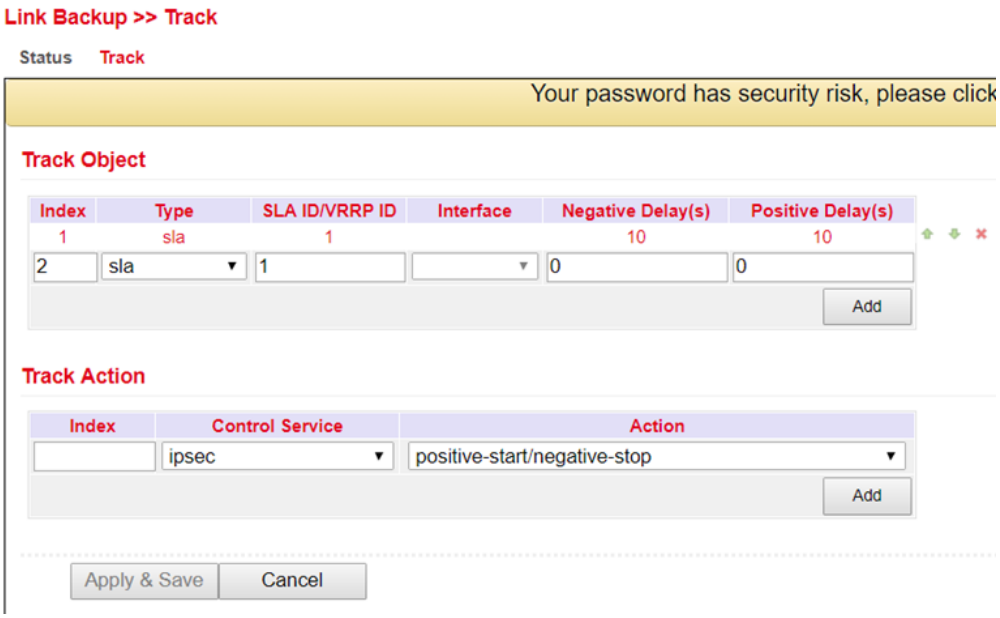
3.4.2 3.4.2. Track

3.4.2.1. Status

Zeigt den Track-Status an, positive bedeutet, dass der Pingversuch erfolgreich oder das Interface mit dem Internet verbunden ist. Sie können den Status Track über ***Link Backup*** > ***Track*** > ***Status*** einsehen, wenn dieser konfiguriert wurde.

3.4.2.2. Track Konfiguration

Richten Sie unter ***Link Backup*** > ***Track*** > ***Track*** Ihr Track Objekt ein.

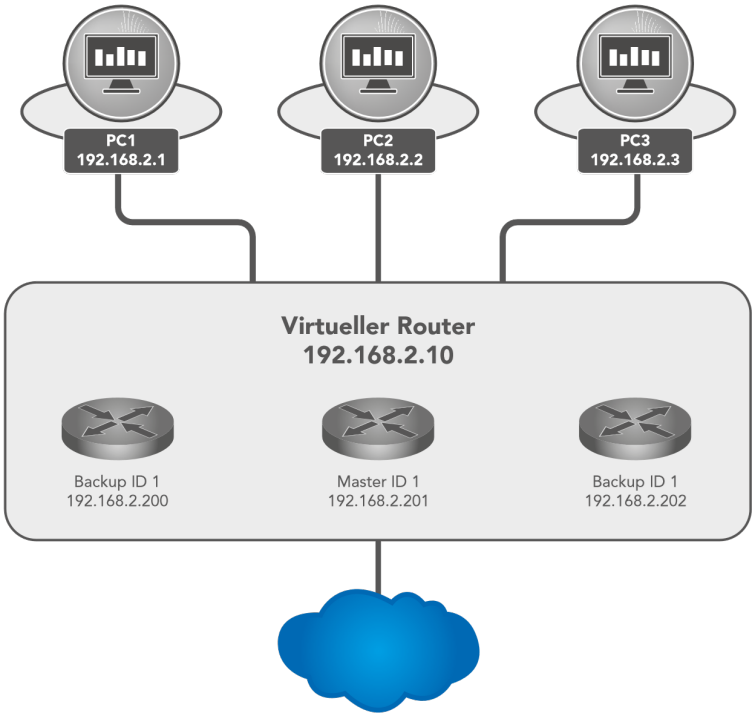


Parameter	Bedeutung
Index	Frei wählbar. Dient zu Identifizierung des Eintrags.
Type	sla oder interface.
SLA ID	Index, der SLA die zuvor angelegt wurde.
Interface	Wird bei sla nicht verwendet.
Negative Delay(s)	Verzögerung beim Wechsel auf das Backup-Interface, wenn die Internetverbindung auf dem Main-Interface wegfällt.
Positive Delay(s)	Verzögerung beim Wechsel auf das Main-Interface, wenn die Internetverbindung wieder verfügbar ist.

3.4.3 3.4.3. VRRP

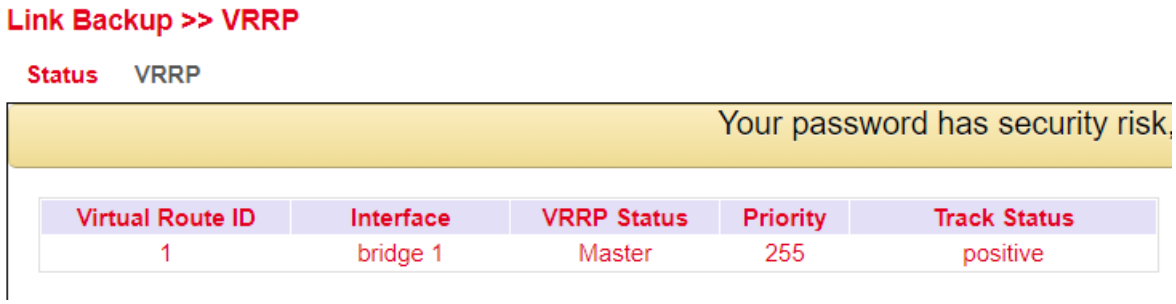
In einem Netzwerk haben alle Teilnehmer ein gemeinsames Gateway zur Kommunikation mit anderen Netzwerken. Wenn dieses Gateway ausfällt, so ist die Kommunikation mit anderen Netzen (und dem Internet) nicht mehr möglich.

Aus diesem Grund gibt es das ***Virtual Router Redundancy Protocol (VRRP)***. Dieses ermöglicht es mehrere Router (Gateways) parallel zu betreiben, wobei jedoch immer nur einer aktiv (Master) ist. Die anderen Router dienen als Backup, sollte der Master ausfallen. Dabei stellen alle Router gemeinsam einen virtuellen Router dar. Innerhalb dieses virtuellen Routers regelt dann VRRP die Kommunikation, sodass bei einem Ausfall des Masters sofort ein Backup-Router zum neuen Master wird und somit zum neuen Gateway für das Netzwerk.



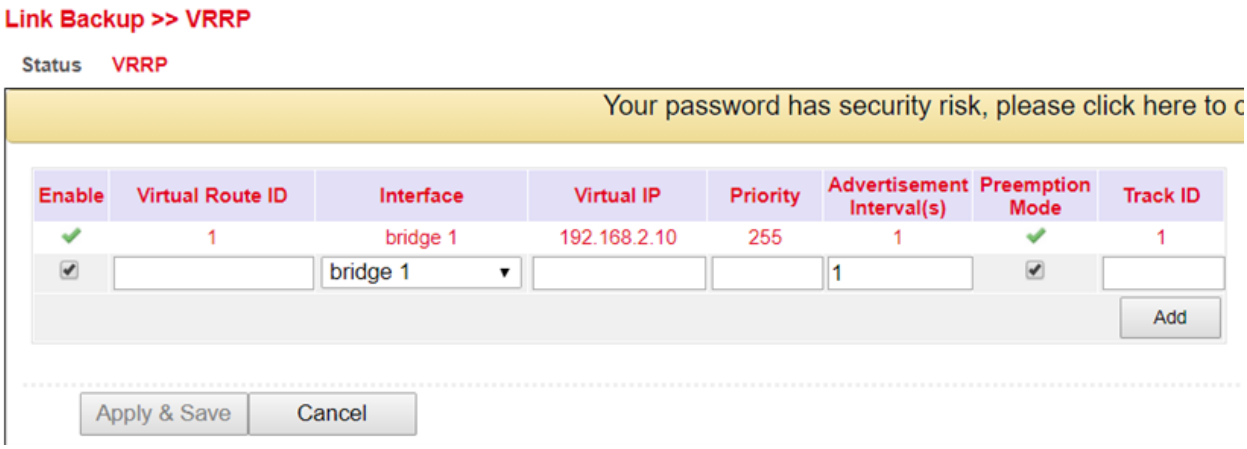
3.4.3.1. VRRP Status

Zeigt den Status des VRRP an. Die Einzelheiten entnehmen Sie bitte der Beschreibung.



Parameter	Beschreibung
Virtual Route ID	Zeigt die Router-Gruppe an, in der der Router sich befindet
Interface	Zeigt das LAN interface an
VRRP Status	Gibt den aktuellen Status an, Master oder Backup
Priority	Zeigt die Priorität des Routers an
Track Status	Zeigt an, ob der Verbindungscheck erfolgreich ist

3.4.3.2. VRRP Configuration



Parameter	Beschreibung
Enable	Schaltet die Konfiguration ein oder aus
Virtual Route ID	Frei wählbar, gibt die Virtuelle Router Gruppe an. Muss bei allen Routern innerhalb der Gruppe identisch sein
Interface	Das LAN Interface
Virtual IP	Die virtuelle Router IP, muss bei allen Routern innerhalb der gleichen Gruppe identisch sein
Priority	0-254 je höher, desto stärker. Der höchste Wert innerhalb der Gruppe wird automatisch zum Master.
Advertisement Interval(s)	Check-Zeit innerhalb der Gruppe um herauszufinden wer Master ist.
Preemption Mode	Wenn eingeschaltet, dann schaut der Router automatisch ob die Priorität höher ist als die des aktuellen Masters. Wenn dem so ist, dann veranlasst er, dass er selbst zum Master wird und der aktuelle Master zum Backup-Router wird.
Track ID	Zuvor angelegte Track zum Verbindungscheck

VRRP Beispiel:

Zunächst richten Sie unter ***Link Backup > SLA*** eine neue SLA ein und danach unter ***Link Backup > Track*** einen Track. Anschließend konfigurieren Sie ***Router A*** über ***Link Backup > VRRP > VRRP*** sowie in Abbildung 1 gezeigt.

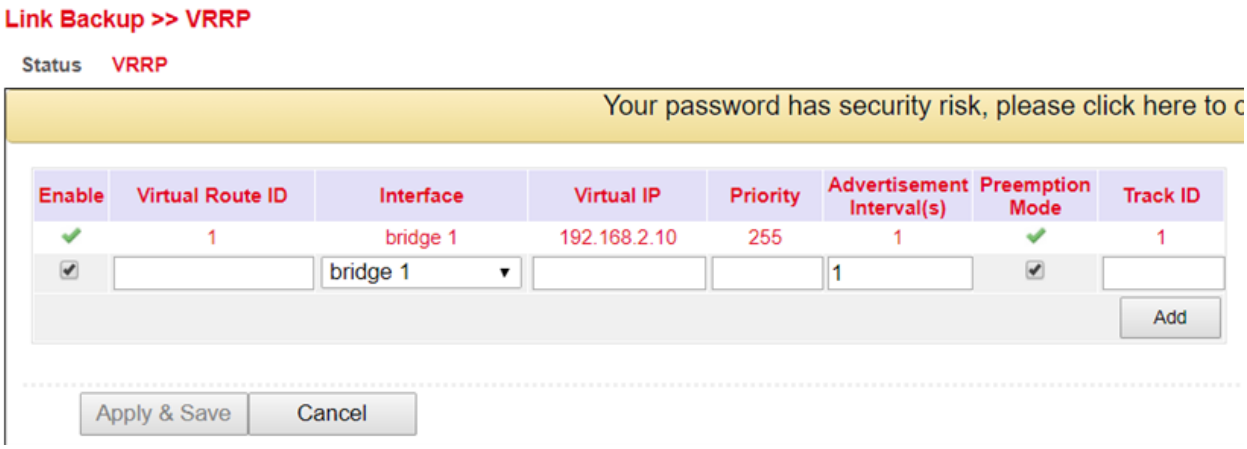


Abbildung 1 (Interface kann je nach Routermodell abweichen)

Nun können Sie ***Router B*** wie in Abbildung 2 konfigurieren.

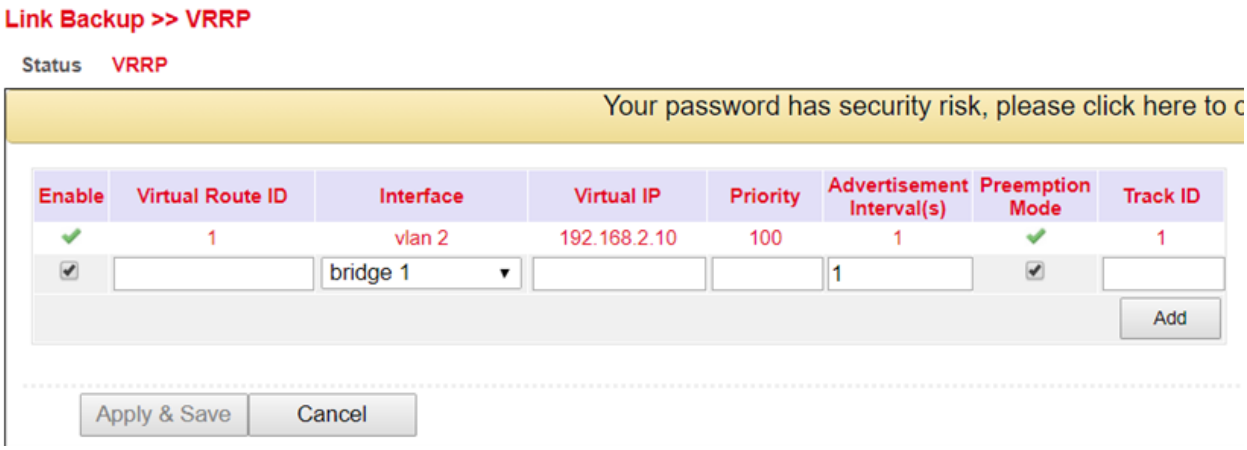
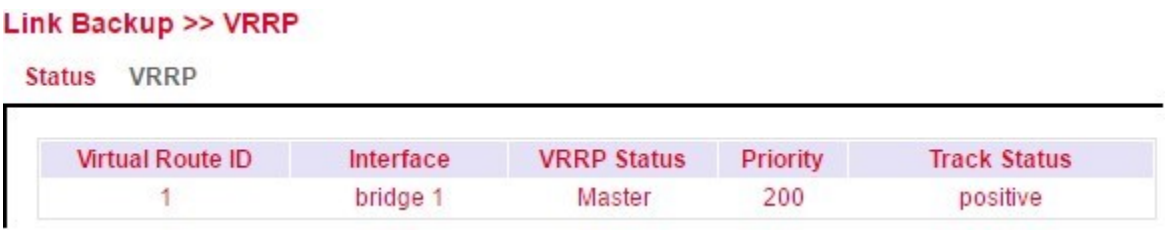


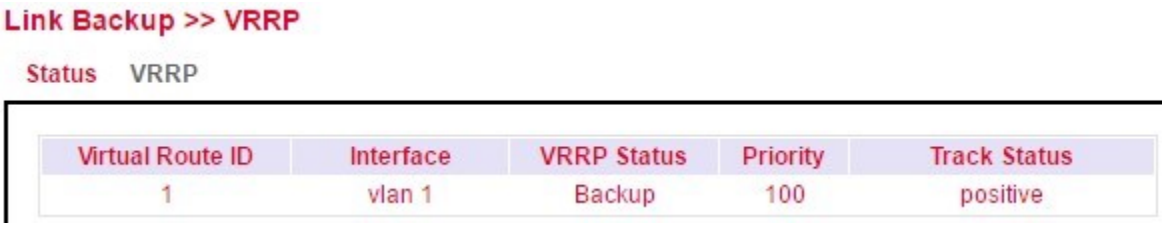
Abbildung 2 (Interface kann je nach Routermodell abweichen)

Wenn Sie jetzt die Statusseite von VRRP aufrufen ***(Link Backup > VRRP > Status)*** sollten Sie folgendes auf den Routern sehen:

Router A

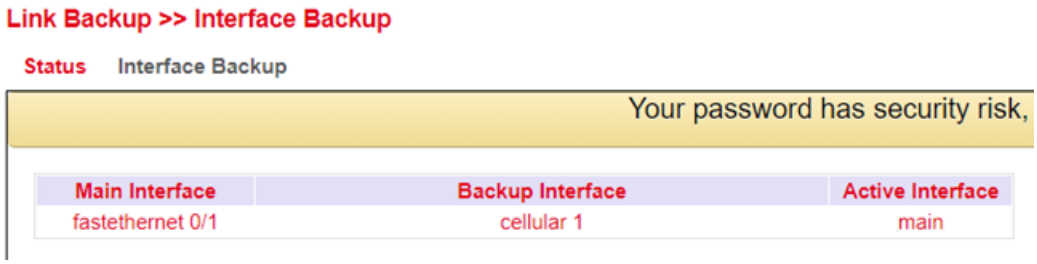


Router B



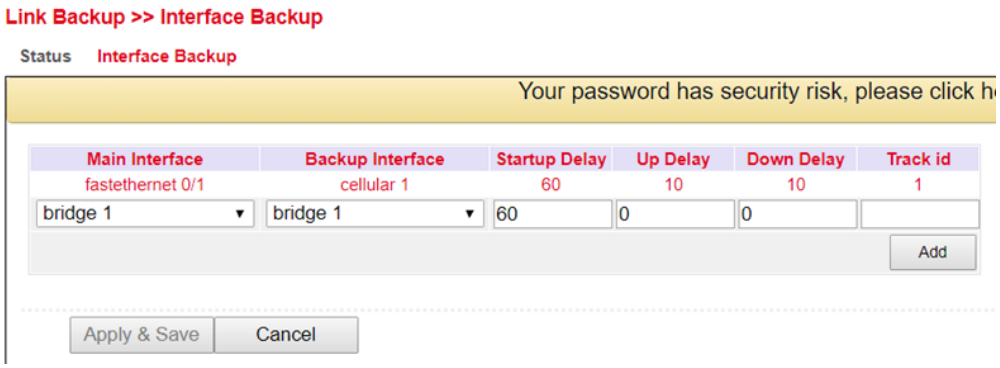
3.4.4 3.4.4. Interface Backup

Hier können Sie ein Backup der Interfaces Ihres Routers erstellen. Fällt ein Interface aus, übernimmt das andere Interface die Funktionen. Zu erreichen unter ***Link Backup > Interface Backup.***



3.4.4.1. Interface Backup Konfiguration

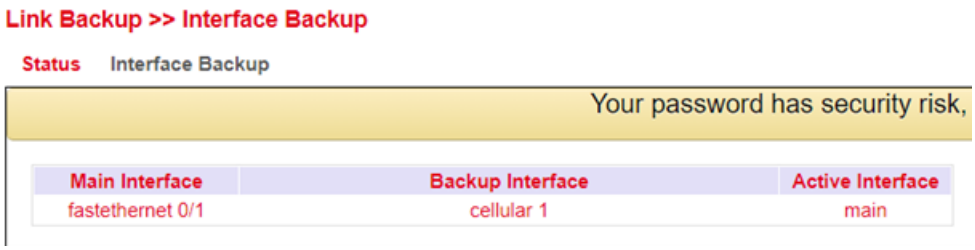
Unter Link Backup > Interface Backup und Interface Backup können Sie definieren, welches Interface das Haupt-Interface und welches das Backup-Interface sein soll.



Parameter	Bedeutung
Main Interface	Hier wird das Maininterface definiert.
Backup Interface	Hier wird das Backupinterface definiert.
Startup Delay	Verzögerung in Sekunden beim Systemstart.
Up Delay	Verzögerung beim Wechsel vom Backup Interface auf das Maininterface.
Down Delay	Verzögerung beim Wechsel vom Maininterface auf das Backupinterface.
Track ID	Der Trackindex, von dem zuvor angelegten Trackeintrag.

3.4.4.2. Interface Backup Status

Auf der Status-Seite sieht man, welche Interfaces als Main und Backup definiert wurden. Außerdem ist zu erkennen, welches Interface gerade aktiv ist (Active Interface main).



3.5 3.5. Routing

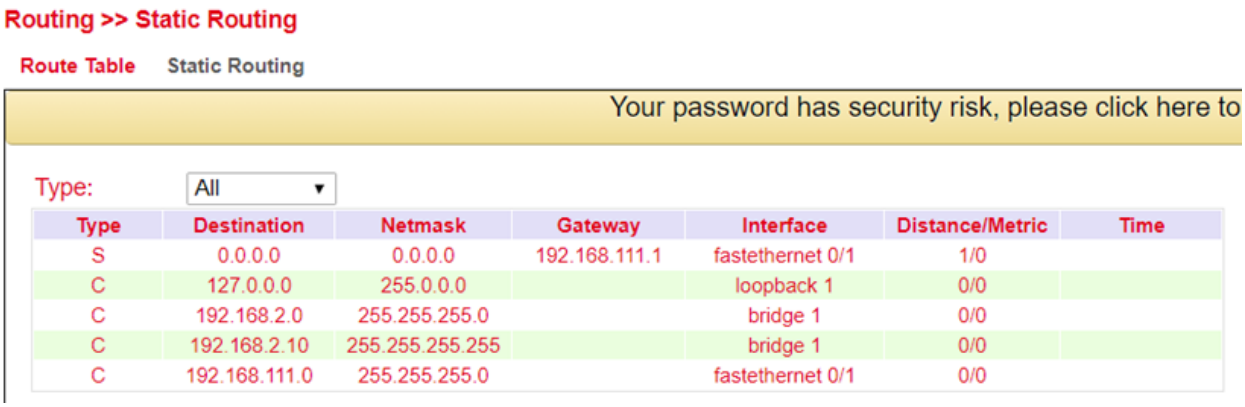
Routing ist ein Oberbegriff für den von Routern geregelten Transportweg von Datenpaketen zwischen verschiedenen Netzwerken. Im Internet können die Datenpakete dabei durchaus vollkommen verschiedene Wege nehmen, da es im Internet keine direkten Verbindungen zwischen Rechnern gibt. Das Ziel der Daten ist im so genannten Header enthalten. Erst beim Empfänger werden die Datenpakete wieder korrekt zusammengesetzt. Durch das Routing kann der Datenverkehr sehr flexibel und ausfallsicher erfolgen.

3.5.1 3.5.1 Static Routing

Statisches Routing (Static Routing) basiert, wie der Name schon sagt, auf einer festen Vorgabe des Weges zwischen zwei beliebigen Endsystemen. Die Vorgabe wird bei der Installation eines Netzwerks getroffen und in der Regel als feste Routingtabelle im Router gespeichert. Die Endgeräte sind jeweils einem Router zugeordnet, über den sie erreichbar sind und andere Ziele erreichen können. Zu erreichen unter ***Routing*** > ***Static Routing.***

3.5.1.1. Route Table

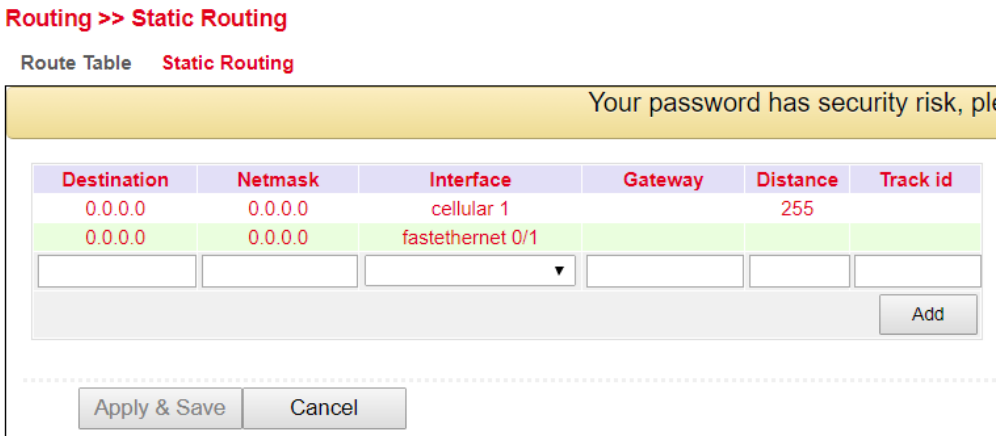
Die Routing Tabelle findet man in der Navigation unter: ***Routing*** > ***Static Routing*** > ***Routing Table*** und ***Routing*** > ***Dynamic Routing*** > ***Routing Table***



Paran	Beschreibung
Type	C = Connected / direkt verbundene Route, Sie werden automatisch in eine Routingtabelle übernommen, wenn ein Interface mit einer IP-Adresse konfiguriert wird S = Static Route / manuell vom Administrator eingetragene Route R = RIP (Routing Information Protocol) / dynamische Route durch RIP hinzugefügt O = OSPF (Open Shortest Path First) / dynamische Route durch OSPF hinzugefügt
Destination	Das Ziel ist der Zielhost, die Subnetzadresse, die Netzwerkadresse oder die Standardroute. Das Ziel für eine Standardroute ist 0.0.0.0.
Netmask	Die Netzwerkmaske wird zusammen mit dem Ziel verwendet, um zu bestimmen, wann eine Route verwendet wird. Eine Hostroute hat beispielsweise die Maske 255.255.255.255, eine Standardroute die Maske 0.0.0.0, und eine Subnetz- oder Netzwerkroute hat eine Maske zwischen diesen beiden Werten.
Gateway	Das Gateway ist die IP-Adresse des nächsten Routers, an den ein Paket gesendet werden muss.
Interface	Das Interface ist die Netzwerk-Schnittstelle, die verwendet werden soll, um zum nächsten Router zu gelangen. Cellular 1 = Funkschnittstelle GSM Loopback 1 = interne Loopback Adresse (Schleifenschaltung) FastEthernet 0/1 = Netzwerkport FastEthernet 0/1 auf dem Router VLAN 1 = Netzwerkports, welche dem VLAN 1 zugeordnet sind.
Distance/ Metric	Distance/Metrik ist die Priorität der Route. Wenn mehrere Routen zum selben Ziel führen, gilt die Route mit der niedrigsten Metrik als beste Route.
Time	Zeit

3.5.1.2. Static Routing

Statische Routen werden in der Navigation unter ***Routing*** > ***Static Routing*** > ***Static Routing*** eingerichtet. Normalerweise muss keine statische Route eingetragen werden. Der Router trägt die Routen durch Änderungen in der Konfiguration selber ein.



Parar	Beschreibung
Destination	Das Ziel ist der Zielhost, die Subnetzadresse, die Netzwerkadresse oder die Standardroute. Das Ziel für eine Standardroute ist 0.0.0.0.
Netmask	Die Netzwerkmaske wird zusammen mit dem Ziel verwendet, um zu bestimmen, wann eine Route verwendet wird. Eine Hostroute hat beispielsweise die Maske 255.255.255.255, eine Standardroute die Maske 0.0.0.0, und eine Subnetz- oder Netzwerkroute hat eine Maske zwischen diesen beiden Werten.
Interface	Das Interface ist die Netzwerk-Schnittstelle, die verwendet werden soll, um zum nächsten Router zu gelangen. cellular 1 = Funkschnittstelle GSM fastethernet 0/1 = Netzwerkport FastEthernet 0/1 auf dem Router VLAN 1 = Netzwerkports, welche dem VLAN 1 zugeordnet sind. bridge 1 = bei TK8X5-EXW und TK8X2
Gateway	Das Gateway ist die IP-Adresse des nächsten Routers, an den ein Paket gesendet werden muss.
Distance	Distance/Metrik ist die Priorität der Route. Wenn mehrere Routen zum selben Ziel führen, gilt die Route mit der niedrigsten Metrik als beste Route.
Track id	Track index oder Identifikationsnummer

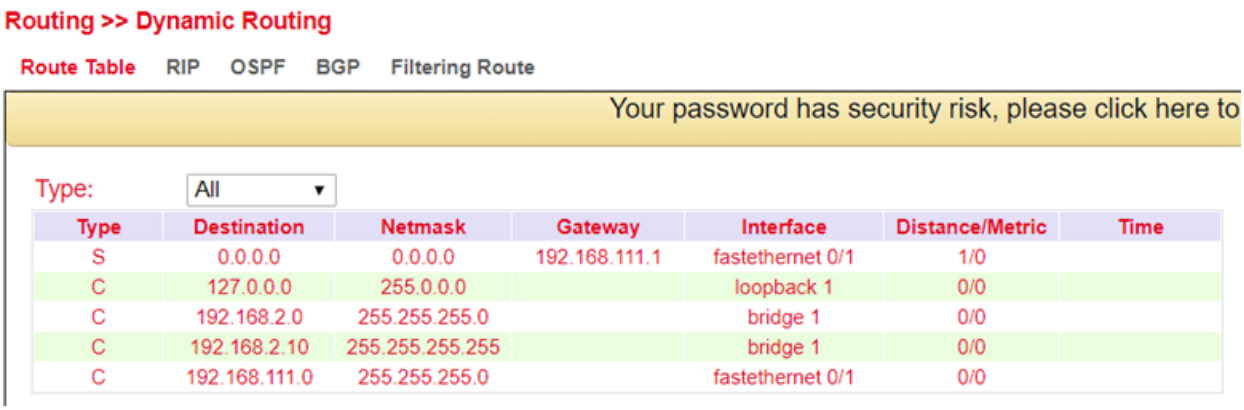
3.5.2 3.5.2. Dynamic Routing

Dynamisches Routing wird eingesetzt, um Routen automatisch vom eingesetzten Routingprotokoll steuern zu lassen. Der Vorteil des dynamischen Routings gegenüber dem statischen Routing liegt darin, dass die Wegwahl dynamisch, also bei laufendem Betrieb erfolgt. Routen werden vom Algorithmus des Routingprotokolls automatisch gelernt und gesetzt.

3.5.2.1. Route Table

Die Routing Tabelle findet man in der Navigation unter:

Routing > Dynamic Routing > Routing Table

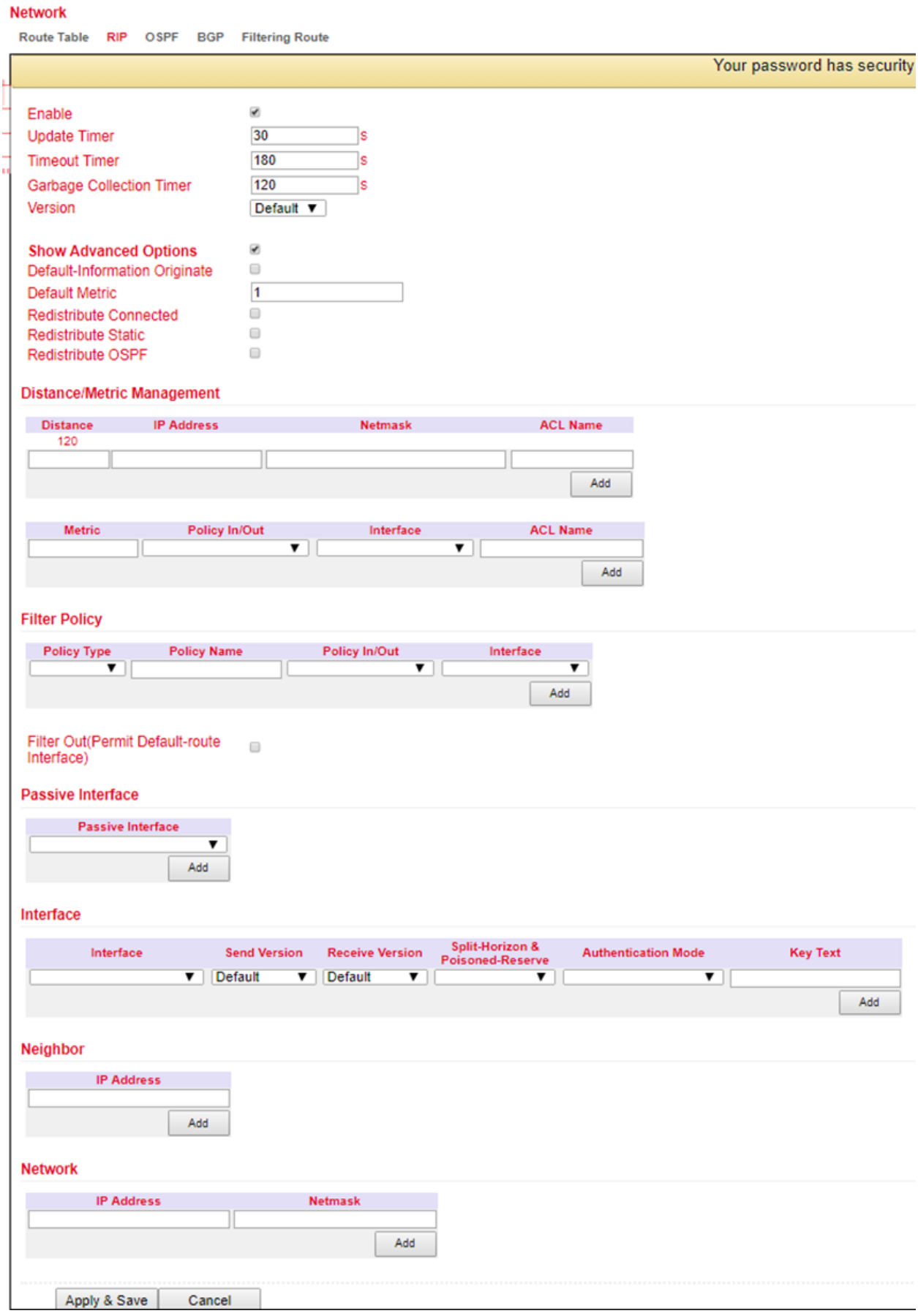


Parameter Beschreibung siehe 3.5.1.1

3.5.2.2. RIP

RIP (Routing Information Protocol) ist ein dynamisches Routing Protokoll, welches mit Distance-Vector-Algorithmus arbeitet. RIP erlernt von anderen Routern dynamische Routing Adressen und legt diese in seinen Routingtabellen ab. Dabei werden die Entfernung und Kosten zu anderen Netzwerken aus der Sicht des Routers in Relation gesetzt und der kostengünstigste Weg zum Zielnetzwerk mit in die Routingtabellen angegeben. Aufgrund dieser Informationen kann der günstigste und kürzeste Weg zum Zielnetzwerk bestimmt und genommen werden. 15 Hops sind die maximale Entfernung, die ein Weg zum Zielnetzwerk beim RIP betragen darf.

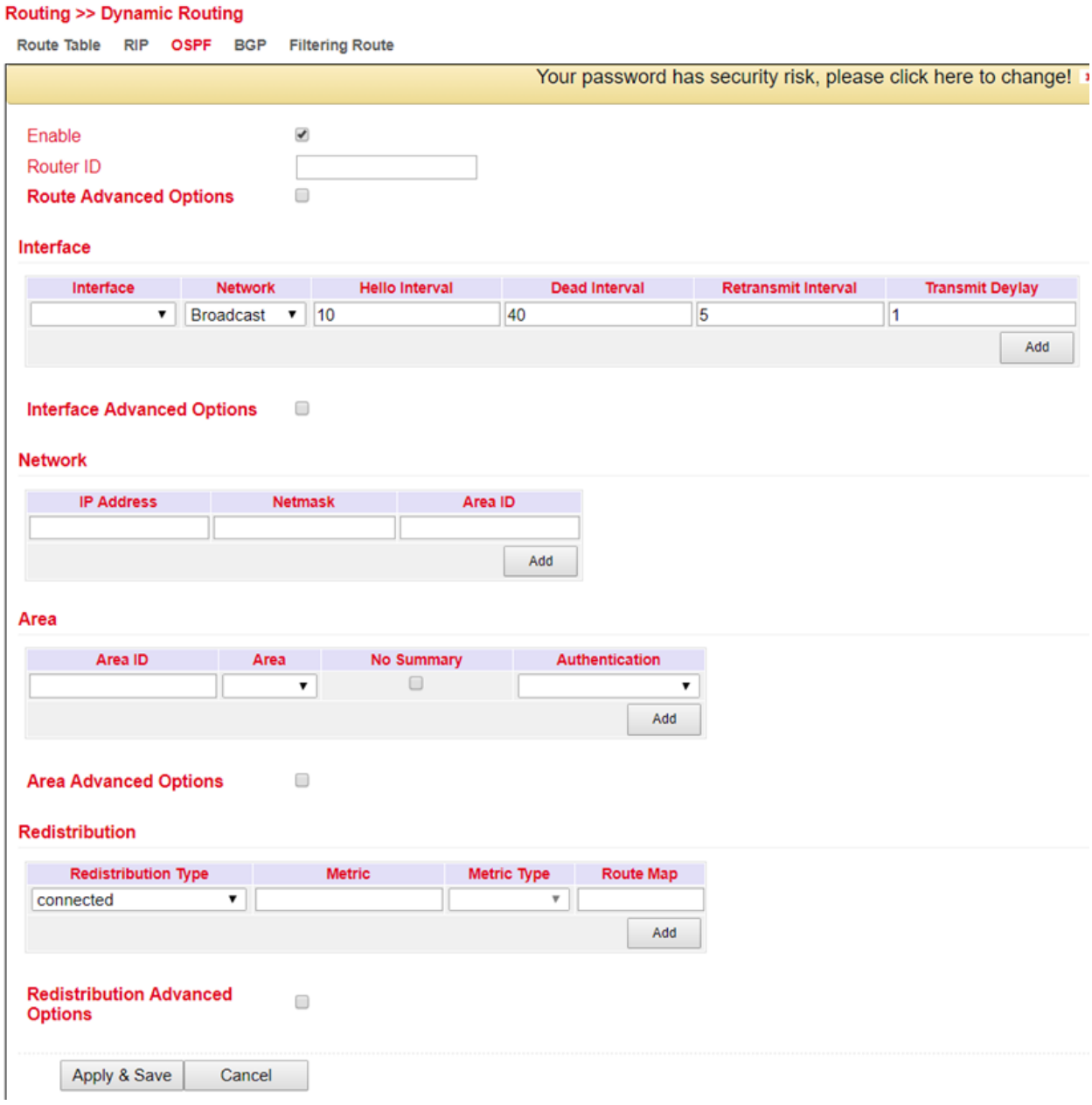
Im Menü ***Routing > Dynamic Routing > RIP*** können Sie folgende Einstellungen vornehmen:


Network
Route Table
RIP
OSPF
BGP
Filtering Route
Your password has security
Enable
Update Timer
30
s
Timeout Timer
180
s
Garbage Collection Timer
120
s
Version
Default
Show Advanced Options
Default-Information Originate
Default Metric
1
Redistribute Connected
Redistribute Static
Redistribute OSPF
Distance/Metric Management
Distance
IP Address
Netmask
ACL Name
120
Add
Metric
Policy In/Out
Interface
ACL Name
Add
Filter Policy
Policy Type
Policy Name
Policy In/Out
Interface
Add
Filter Out(Permit Default-route Interface)
Passive Interface
Passive Interface
Add
Interface
Interface
Send Version
Receive Version
Split-Horizon & Poisoned-Reserve
Authentication Mode
Key Text
Default
Default
Add
Neighbor
IP Address
Add
Network
IP Address
Netmask
Add
Apply & Save
Cancel

3.5.2.3. OSPF

OSPF (Open Shortest Path First) ist ein dynamisches Routing Protokoll, welches beschreibt wie Router untereinander die Verfügbarkeit von Verbindungswegen zwischen Datennetzen propagieren. Es unterstützt hierarchische Netzstrukturen und im Gegensatz zu RIP mehrere gleichzeitige Verbindungswege gleicher Kosten zu einem Teilnetz. Es ist in der Lage, den auftretenden Datenverkehr über verschiedene Verbindungswege zu übertragen. Das OSPF-Protokoll ist besonders schnell in Bezug auf Veränderungen in der Netzwerktopologie und zeichnet sich durch eine sparsame Nutzung der Bandbreite beim Erstellen neuer Routingtabellen aus.

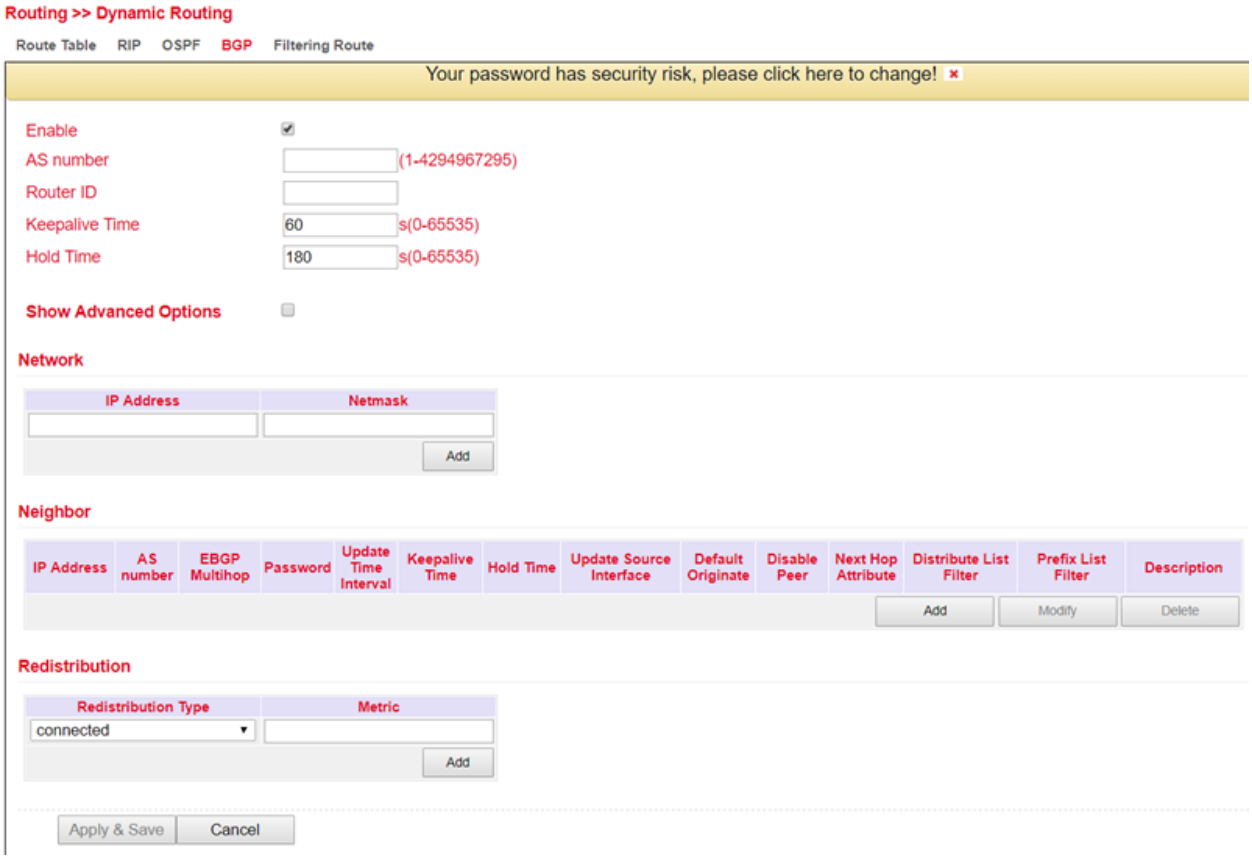
Im Menü ***Routing > Dynamic Routing > OSPF*** können folgende Einstellungen vorgenommen werden:



3.5.2.4. BGP

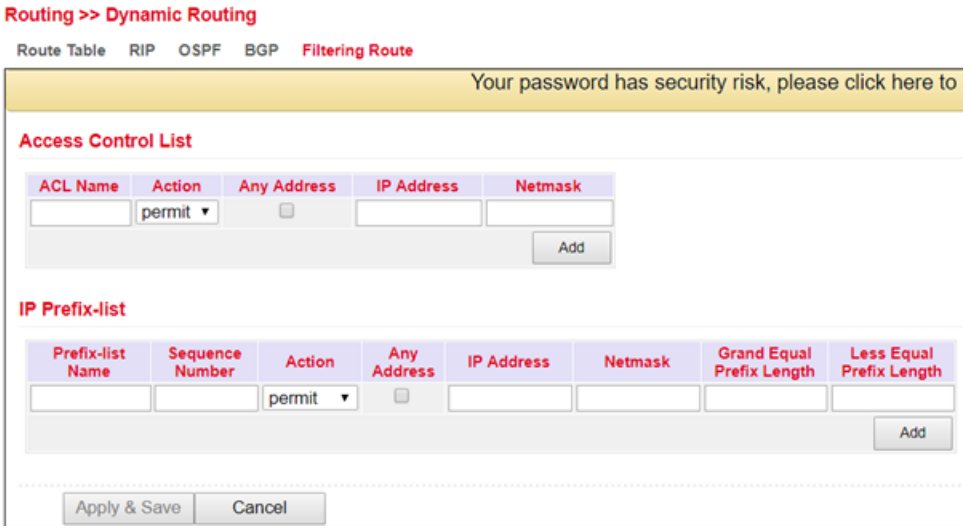
Das Border Gateway Protocol (BGP) ist das im Internet eingesetzte Routingprotokoll und verbindet autonome Systeme (AS) miteinander. Diese autonomen Systeme werden in der Regel von Internetdienstanbietern gebildet. BGP wird allgemein als Exterior-Gateway-Protokoll (EGP) und Pfadvektorprotokoll bezeichnet und verwendet für Routing-Entscheidungen sowohl strategische wie auch technisch-metrische Kriterien, wobei in der Praxis meist betriebswirtschaftliche Aspekte berücksichtigt werden. Innerhalb autonomer Systeme kommen Interior Gateway Protokolle (IGP) wie z.B. OSPF zum Einsatz.

Im Menü ***Routing*** > ***Dynamic Routing*** > ***BGP*** können für BGP die folgenden Einstellungen vorgenommen werden:



3.5.2.5. Filtering Route

Im Menü ***Routing*** > ***Dynamic Routing*** > ***Filtering Route*** können Sie folgende Einstellungen vornehmen:

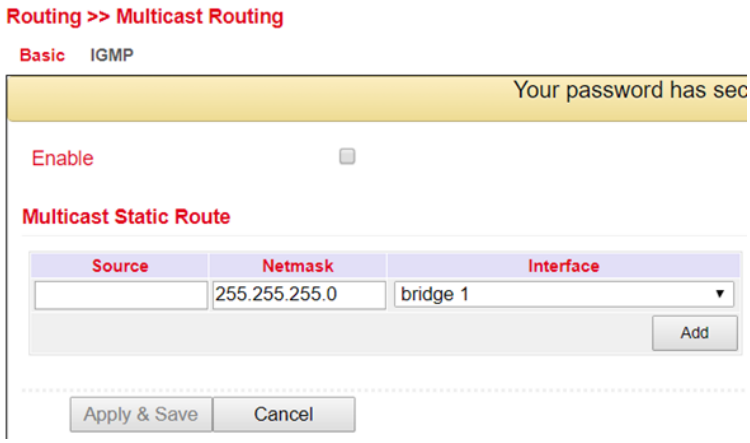


3.5.3 3.5.3. Multicast Routing

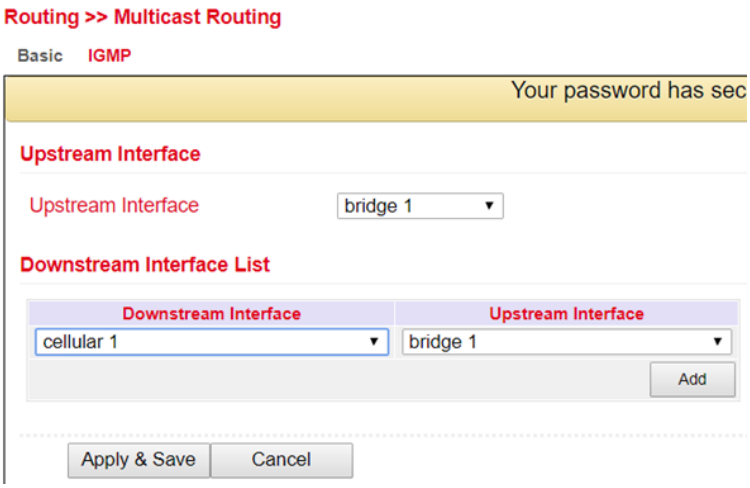
Das Internet Group Management Protocol (IGMP) basiert auf dem Internet Protocol (IP) und ermöglicht IPv4-Multicasting (Gruppenkommunikation) im Internet. IP-Multicasting ist die Verteilung von IP-Paketen unter einer IP-Adresse an mehrere Stationen gleichzeitig.

3.5.3.1. Basic

Im Menü ***Routing*** > ***Multicast Routing*** > ***Basic*** können die folgenden Einstellungen vorgenommen werden:



3.5.3.2. IGMP



Beim ***Upstream Interface*** wird die Schnittstelle ausgewählt, über welche der Multicast verbreitet werden soll.

Bei der ***Downstream Interface List*** werden die Schnittstellen für das Down- und Upstream Interface aus dem Drop-Down Menü ausgewählt.

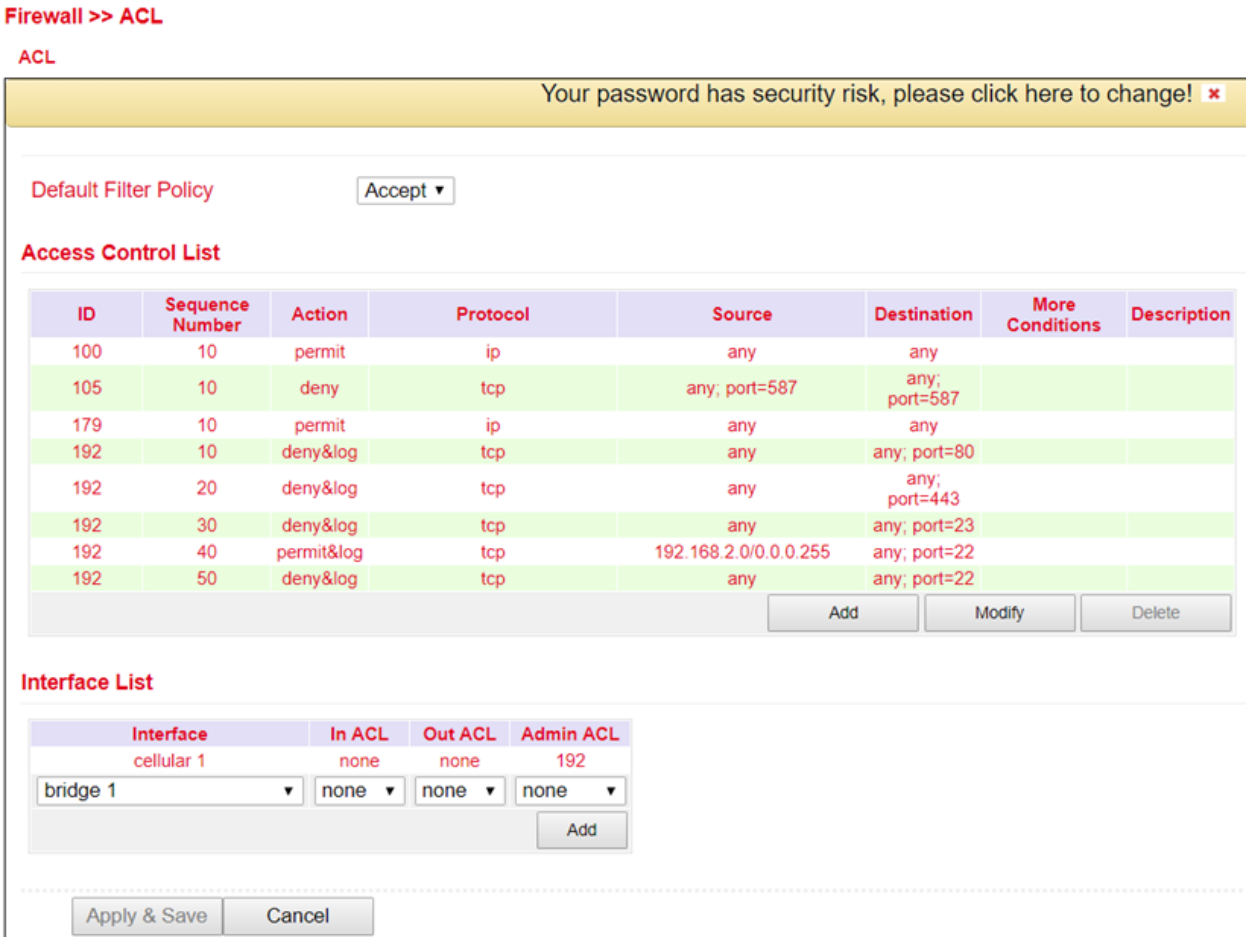
Die Interfaces können je nach Modell abweichen.

3.6 3.6. Firewall

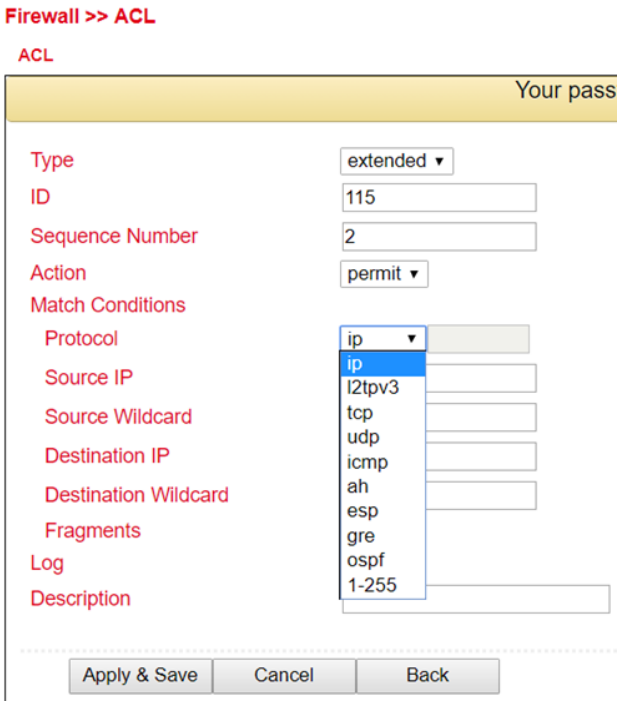
3.6.1 3.6.1. ACL

Die ACL (Access Control List) ist eine Zugriffskontrollliste, um die Nutzung und die Administration zu kontrollieren. Durch die ACL wird festgelegt, welche Rechner oder Netze auf den Router oder Netze hinter dem Router zugreifen können. Bei der ACL werden ein- und ausgehende Datenpakete analysiert und gemäß dem ACL Regelwerk verwaltet.

ACL Regeln lassen sich auf Quell- und Ziel IP-Adressen, TCP und UDP Port Nummern, etc. erstellen, um die Zugriffe zu steuern.



Hier ist eine Übersicht der vorhandenen ACL Regeln. Um eine neue ACL zu erstellen muss man auf ***Add*** klicken.



Standard ACL kann jegliche Kommunikation von einem Netzwerk oder zu einem Netzwerk erlauben oder blockieren oder auch die gesamte Kommunikation verbieten.

Extended ACL bietet erweiterte Einstellmöglichkeiten für Quell und Ziel Netzwerke innerhalb einer ACL. Es können Protokolle aus verschiedenen Ebenen gewählt werden. Somit kann man gezielt einzelne Dienste wie Web (http), FTP, Telnet etc. erlauben oder verbieten.

Parameter	Beschreibung
Type	extended oder standard
ID	ID 100 ist standardmäßig vorkonfiguriert. Weitere IDs können frei konfiguriert werden.
Action	Permit = Erlauben / Deny = Verbieten
Protocol	Protokolle, die zur Verfügung stehen
Source IP	Quell IP-Adresse oder Netzwerk z.B. 192.168.2.0
Source Wildcard	Quell Wildcard ist die Wildcard-Adresse des Subnetzes. Z.B. bei der Subnetzmaske 255.255.255.0 ist die Wildcard Adresse 0.0.0.255
Destination IP	Ziel IP Adresse oder Netzwerk z.B. 172.16.0.0
Destination Wildcard	Ziel Wildcard ist die Wildcard-Adresse des Ziel Subnetzes z.B. bei der Subnetzmaske 255.255.0.0 ist die Wildcard Adresse 0.0.255.255
Description	Text Beschreibungsfeld für die ACL

3.6.2 3.6.2. NAT

Network Address Translation (NAT)

Network Address Translation (NAT) ist in Rechnernetzen der Sammelbegriff für Verfahren, die automatisiert Adressinformationen in Datenpaketen durch andere ersetzen, um verschiedene Netze zu verbinden. Daher kommen sie typischerweise auf Routern zum Einsatz.

Verwendung von Source-NAT

Es ermöglicht Geräten mit privaten Netzwerkadressen, eine Verbindung ins Internet aufzubauen. Private IP-Adressen können üblicherweise nicht vom Provider geroutet werden, daher müssen diese in eine öffentliche, routbare IP-Adresse übersetzt werden. Der TK800 hat diese Funktion implementiert, wodurch eine Kommunikation zwischen verschiedenen Netzen ermöglicht wird. Außerdem findet sich im NAT ein relevanter Sicherheitsaspekt, da eine öffentliche IP-Adresse nicht auf die dazugehörige private IP-Adresse zurückgeführt werden kann. Diese Funktion ist beim TK800 Router werksseitig konfiguriert.

Verwendung von Destination-NAT

Dies wird eingesetzt, um Serverdienste, die auf Computern betrieben werden, unter einer einzigen IP-Adresse anzubieten. Häufig wird es als Port-Mapping oder Port-Forwarding bezeichnet. Diese Funktion muss beim TK800 explizit eingerichtet werden.

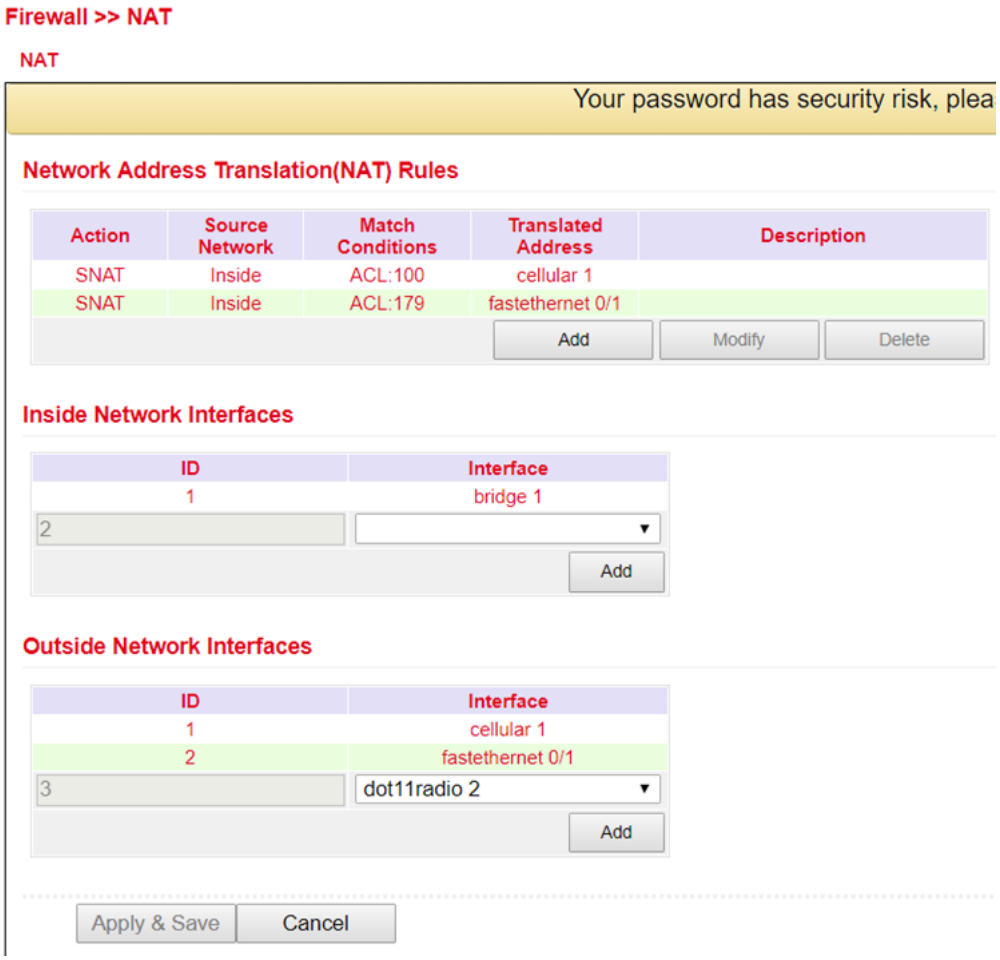
Verwendung von 1:1-NAT

Eine Sonderform von Destination-NAT ist 1:1-NAT. Es wird zum Beispiel verwendet, wenn eine zentrale Stelle mittels VPN auf unterschiedliche Standorte zugreifen möchte, welche alle mit dergleichen IP-Netzwerkadressen konfiguriert sind. Dies ist in Maschinen-Netzen häufig anzutreffen.

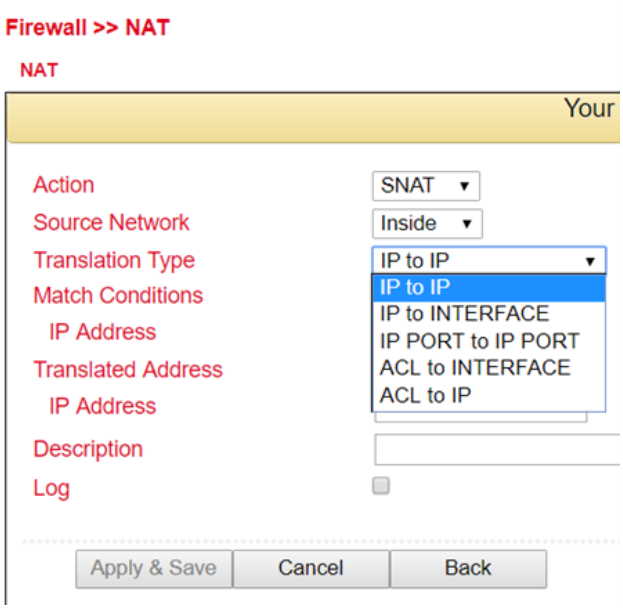
Konfiguration

- zur Konfiguration von NAT geht man über den Menüpunkt ***Firewall*** in den Unterpunkt ***NAT***
- hier findet sich eine Auflistung aller vorhandenen NAT-Regeln und die Definition der ***Inside***-(LAN-) und ***Outside***-(WAN-) Interfaces

(***Anmerkung***: Für manche Anwendungsfälle ist es erforderlich, eine ***ACL*** (Access Control List) anzulegen und zu verwenden.)



- durch Klicken auf ***Add*** lässt sich im folgenden Menü eine neue NAT-Regel konfigurieren (Abb. 2)

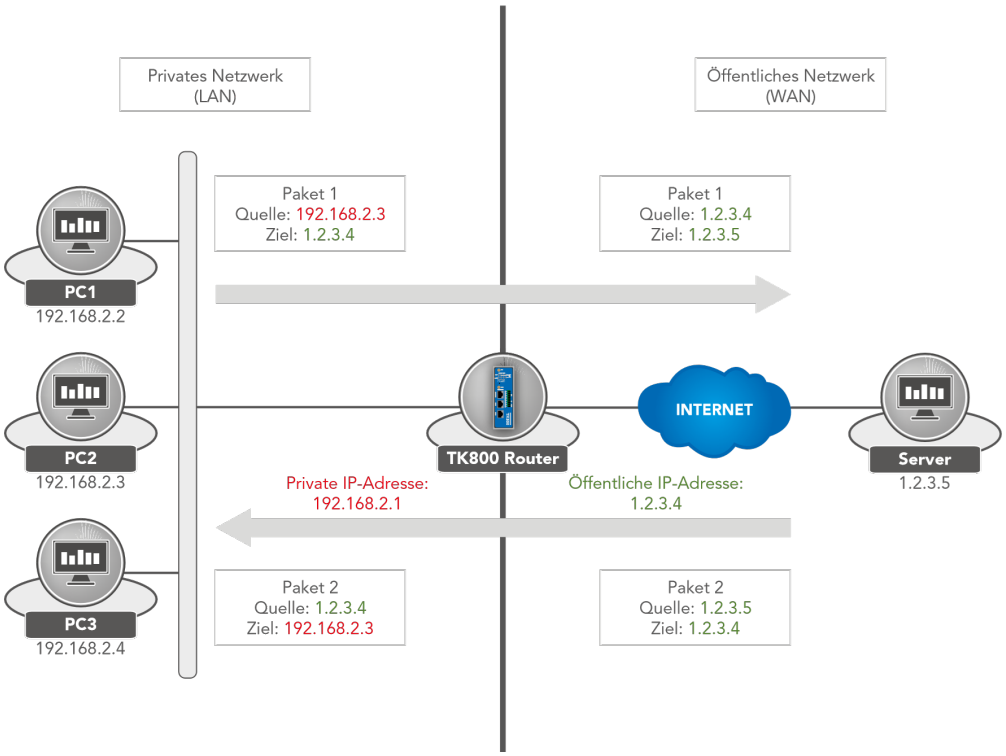


	Action
SNAT	IP-Adresse des Computers umschreiben, der die Verbindung aufbaut
DNAT	IP-Adresse des angesprochenen Computers umschreiben
1:1NAT	IP-Adresse eins zu eins übersetzen
	Source Network
Inside	Pakete stammen von einem internen Interface (LAN)
Outside	Pakete stammen von einem externen Interface (WAN)
	Translation Type
IP to IP	eine IP-Adresse in eine andere übersetzen
IP to Interface	eine IP-Adresse in die IP-Adresse eines einzelnen Interfaces übersetzen
IP Port to IP Port	eine Kombination aus IP-Adresse und Port in eine andere übersetzen
ACL to Interface	eine IP-Adresse nach ACL-Regel in eine IP-Adresse eines einzelnen Interfaces übersetzen
ACL to IP	Eine IP-Adresse nach ACL-Regel in eine andere IP-Adresse übersetzen

Beispiele Fall 1: SNAT (TK-Router als Internet-Gateway)

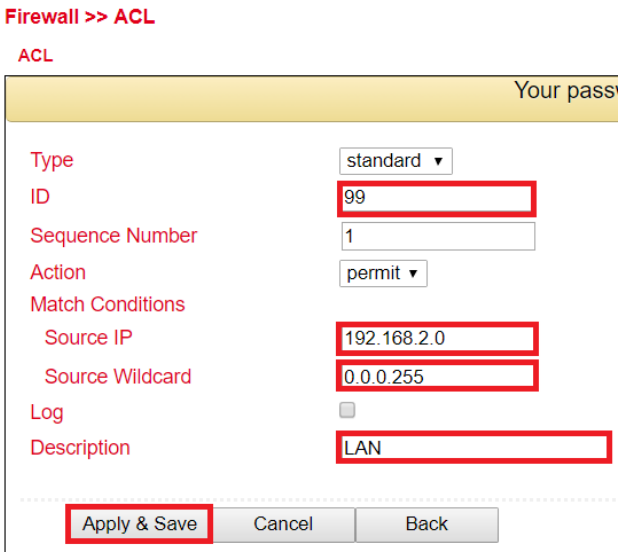
Der TK800 arbeitet hierbei als Internet-Gateway für angeschlossene Geräte mit privater IP-Adresse. Er übersetzt private IP-Adressen aus dem LAN in eine öffentliche, routbare Internet-Adresse.

(***Anmerkung***: Dies ist die Werkseinstellung aller Welotec-Router.)

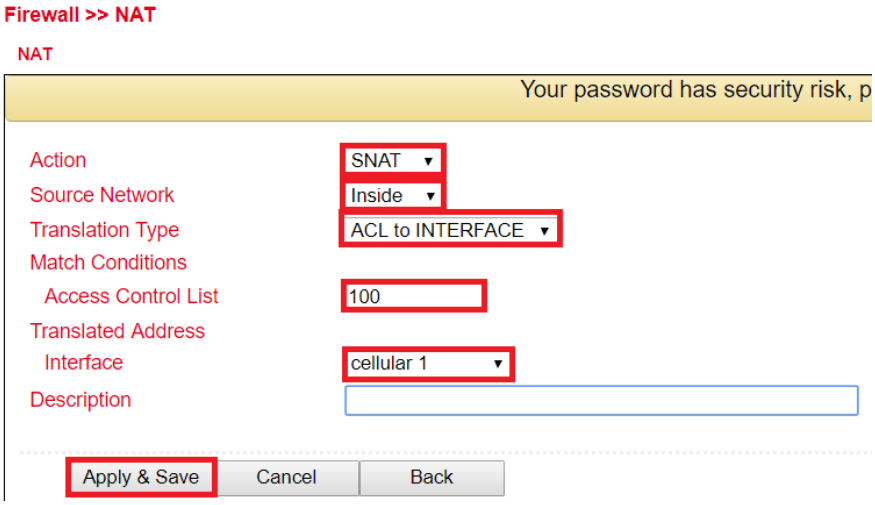


1. Konfigurieren Sie die ACL-Regel. Gehen Sie hierzu im Menü ***Firewall*** auf den Unterpunkt ***ACL***
2. Vergeben Sie nun eine ***ID*** für die Regel und geben Sie die ***IP-Adresse*** und die entsprechende ***Wildcard Maske*** ein.

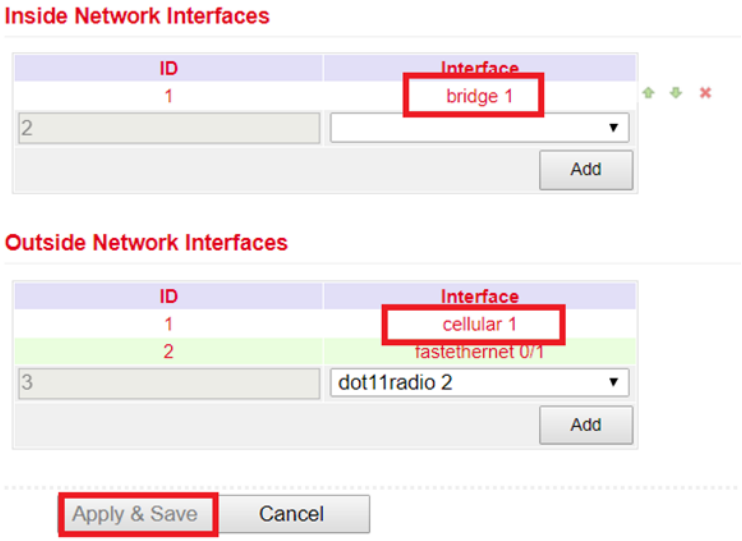
(***Anmerkung***: Die Wildcard-Maske ist die invertierte Netzmaske und wird von Routern zur Bearbeitung von ***ACLs*** (Access Control Lists) verwendet.)



3. Konfigurieren Sie nun die ***SNAT-Regel.***

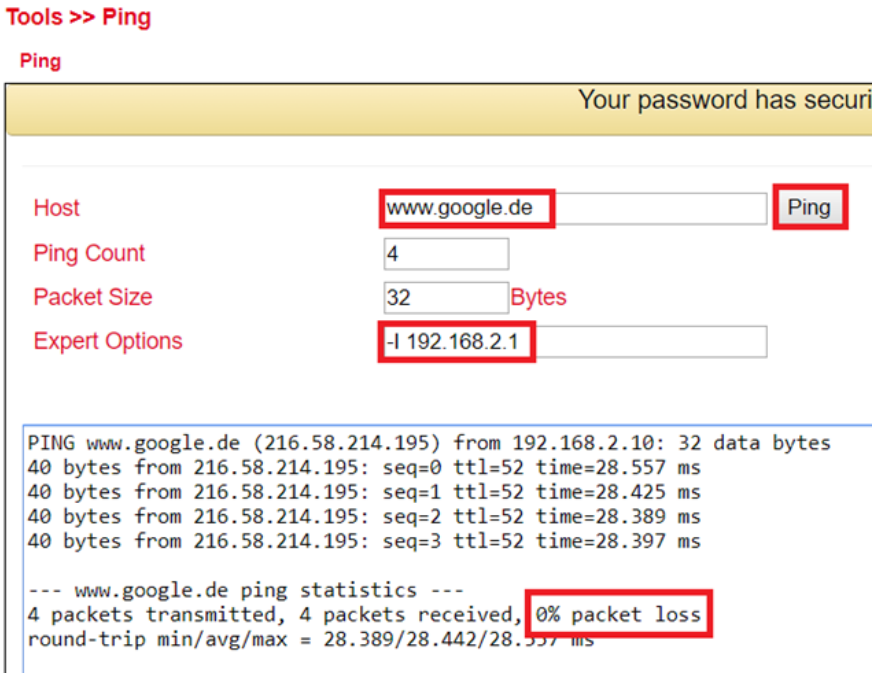


4. Definieren Sie nun das ***Inside***- und ***Outside-Interface***



5. Testen Sie den Zugriff über das Tool ***ping***. Dies kann direkt vom Router aus geschehen. Gehen Sie hierzu im Menü ***Tools*** auf den Unterpunkt ***Ping*** und tragen Sie die Werte nach dem Beispiel ein.

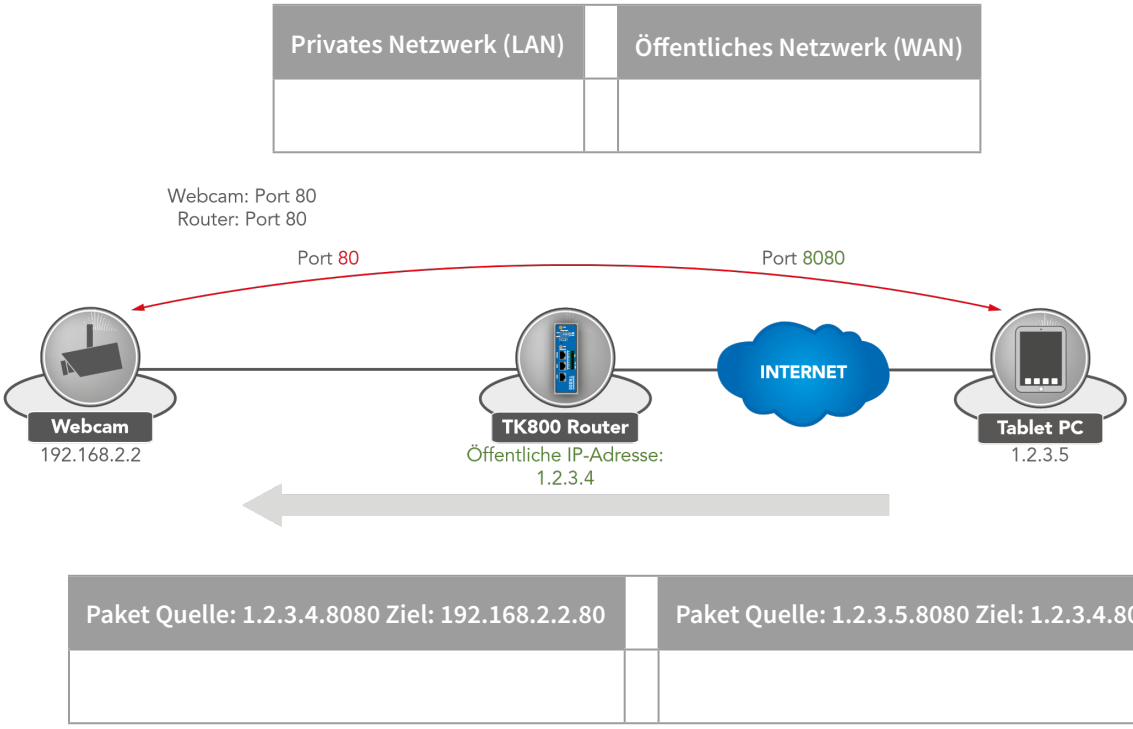
(***Anmerkung***: Verwenden Sie die ***Expert Option*** –I 192.168.2.1 (großes i), damit der Zugriff vom Inside-(LAN-) Interface des TK800 Router aus geschieht)



Fall 2: DNAT (Portmapping / Port Forwarding)

Zugriff über das Internet auf angeschlossene Geräte

In der Regel wollen Anwender auf Geräte, die an den Welotec Router angeschlossen sind, über das Internet zugreifen. Da diese Geräte (z.B. Webcam, Steuerung einer SPS, usw.) keinen eigenen Mobilfunk- oder Internetzugang haben, muss der Welotec Router die Anfragen aus dem Internet an die Geräte weiterleiten. Dabei bedient man sich der sog. Port Forwarding- / Port Mapping-Funktion.



Voraussetzungen

- Öffentliche IP-Adresse im Mobilfunknetz (oder auch bei kabelgebundenen Internetverbindungen)

(***Anmerkung:*** Viele Mobilfunkbetreiber bieten für Geschäftskunden Tarife an, um auf mobile Geräte zuzugreifen, u.a. T-Mobile IP VPN oder Vodafone CDA. Des Weiteren gib es Anbieter, welche Ihnen über eine herkömmliche Mobilfunkkarte eine öffentliche IP-Adresse zur Verfügung stellen.)

Hinweis

- Router Firmware **1.0.0.r9919** oder höher

Hinweise zum Port Mapping

Folgende Informationen müssen vorliegen, damit Port Mapping eingerichtet werden kann:

- IP-Adresse des Gerätes, auf das zugegriffen werden soll
- Port, der umgeleitet werden soll (z.B. http/80 vom Gerät, auf das zugegriffen werden soll)

Beispiel Welotec Router

LAN IP-Adresse:	192.168.2.1
Subnetzmaske: Webcam	255.255.255.0
LAN IP-Adresse:	192.168.2.2
Subnetzmaske:	255.255.255.0
Standard Gateway:	192.168.2.1

Die Webcam hat eine Oberfläche, die über **http://192.168.2.2** erreicht werden kann.

(Anmerkung: http Protokoll verwendet TCP Port 80)

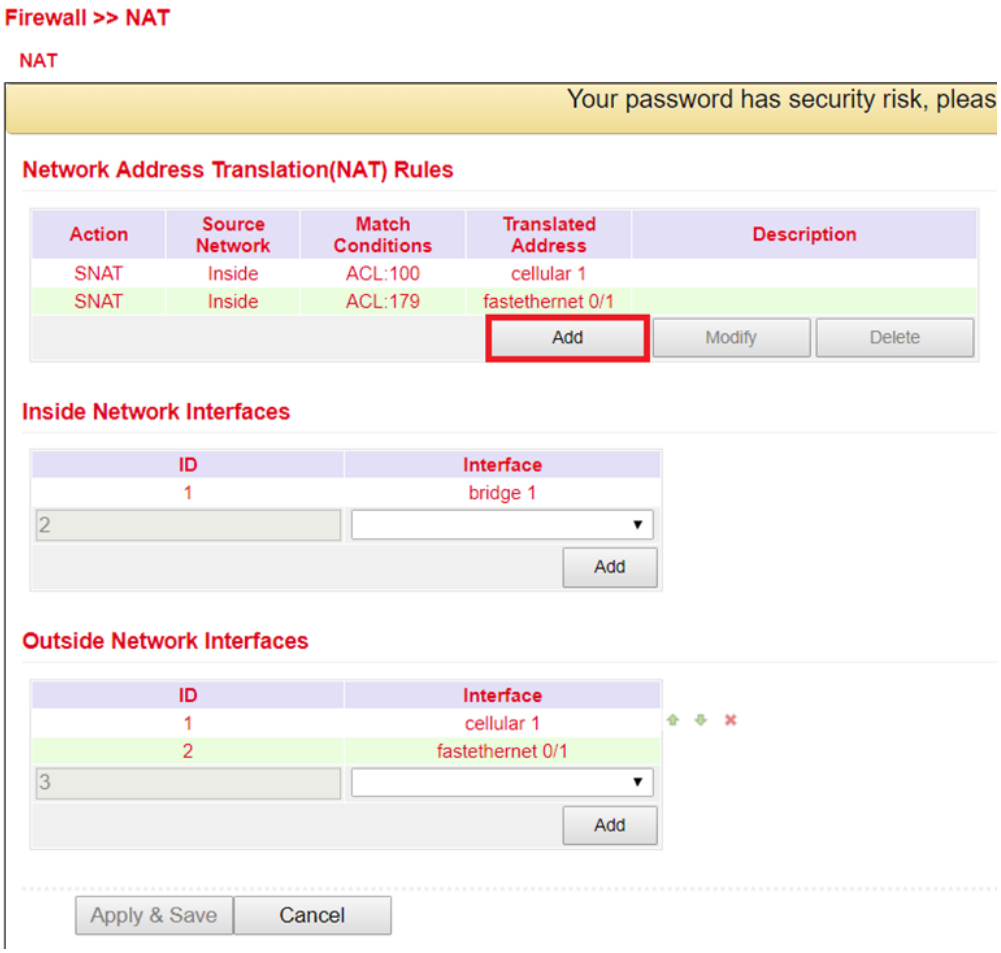
Für ein funktionierendes Port Mapping ist es hilfreich, wenn man die Einstellungen der angeschlossenen Geräte vorab überprüft. Folgende Checkliste ist dabei hilfreich (nach dem o.g. Beispiel):

- Hat die Kamera die IP-Adresse 192.168.2.2?
- Antwortet diese bei „ping 192.168.2.2“?
- Ist die Weboberfläche der Kamera über http://192.168.2.2 erreichbar?
- Ist bei der Kamera als Standard Gateway der Welotec Router eingetragen (192.168.2.1)?

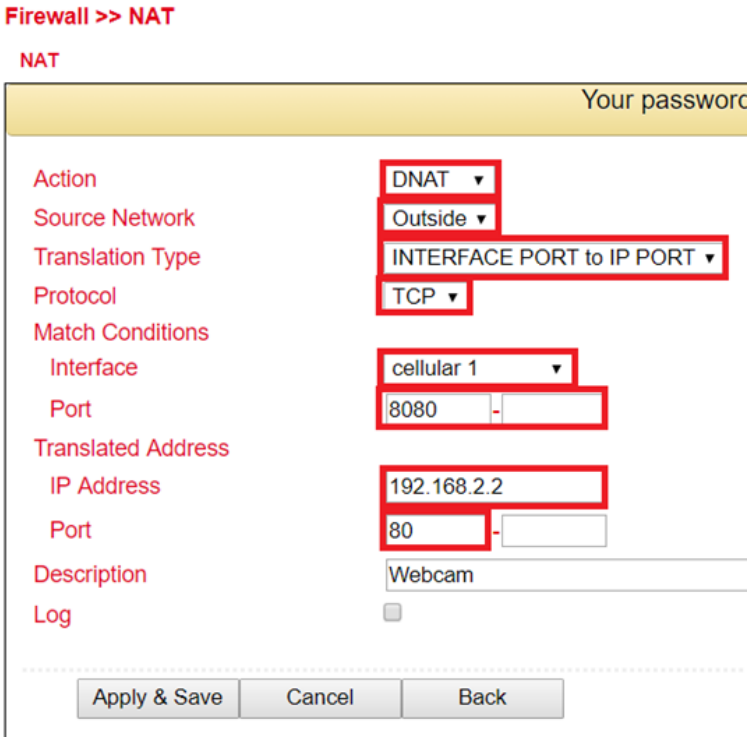
Sofern diese Bedingungen erfüllt sind, kann das Port Mapping nachfolgender Anleitung eingerichtet werden.

Konfiguration

1. Gehen Sie über den Menüpunkt ***Firewall*** auf den Unterpunkt ***NAT***
2. Fügen Sie nun mit ***Add*** eine neue NAT-Regel hinzu



3. Tragen Sie die Daten wie in dem Beispiel ein

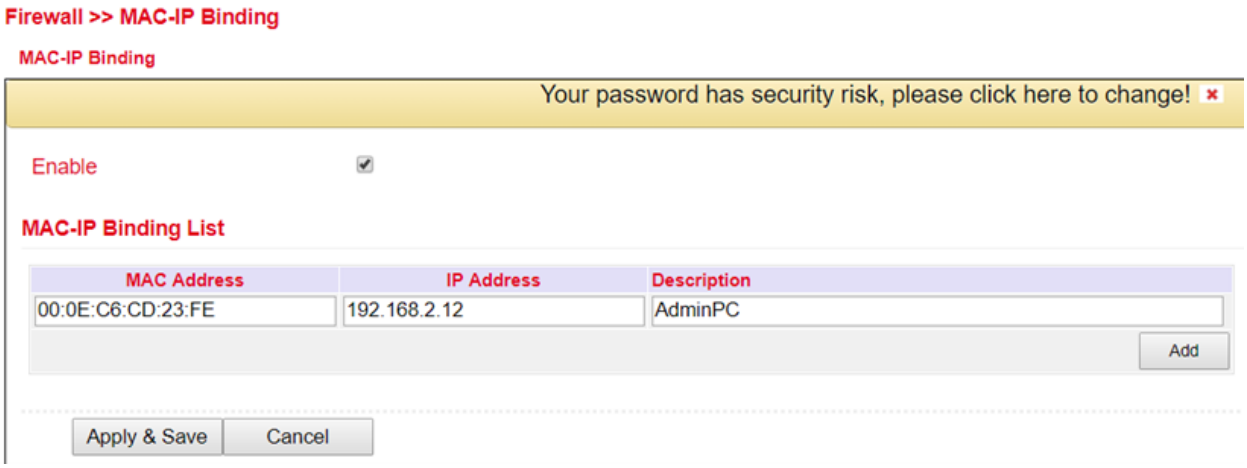


4. Durch Aufrufen der Router-IP mit entsprechendem Port kann das angeschlossene Gerät erreicht werden

3.6.3 3.6.3. MAC-IP Binding

MAC-IP Binding finden Sie im Navigationsbaum unter ***Firewall > MAC-IP Binding*** .

Mit MAC-IP Binding kann sichergestellt werden, dass ein Gerät (PC, Server etc.) auf den Router nur zugreifen kann, wenn die hier eingetragene MAC- und IP Adresse übereinstimmen.



Parameter	Beschreibung
MAC-Address	Die MAC-Adresse des Geräts hier eingeben im Format XX : XX : XX : XX: XX : XX. Eine typische MAC-Adresse sieht folgendermaßen aus: 00:FF:4E:85:F1:B5
IP-Address	IP Adresse eingeben, welche das Gerät bekommen soll. z.B. 192.168.2.150
Description	Text Beschreibungsfeld

3.7 3.7. VPN

Virtual Private Network, kurz VPN. Das VPN dient dazu, Teilnehmer des bestehenden Kommunikationsnetzes an ein anderes Netz zu binden. So kann beispielsweise der Computer eines Mitarbeiters von Zuhause aus Zugriff auf das Firmennetz erlangen, gerade so, als säße er mittendrin.

3.7.1 3.7.1. IPsec

IPsec (Kurzform für Internet Protocol Security) ist eine Protokoll-Suite, die eine gesicherte Kommunikation über potentiell unsichere IP-Netze wie das Internet ermöglichen soll. Ziel ist es, eine verschlüsselungsbasierte Sicherheit auf Netzwerkebene bereitzustellen. IPsec bietet durch die verbindungslose Integrität sowie die Zugangskontrolle und Authentifikation der Daten diese Möglichkeit an. Zudem wird durch IPsec die Vertraulichkeit sowie Authentizität der Paketreihenfolge durch Verschlüsselung gewährleistet.

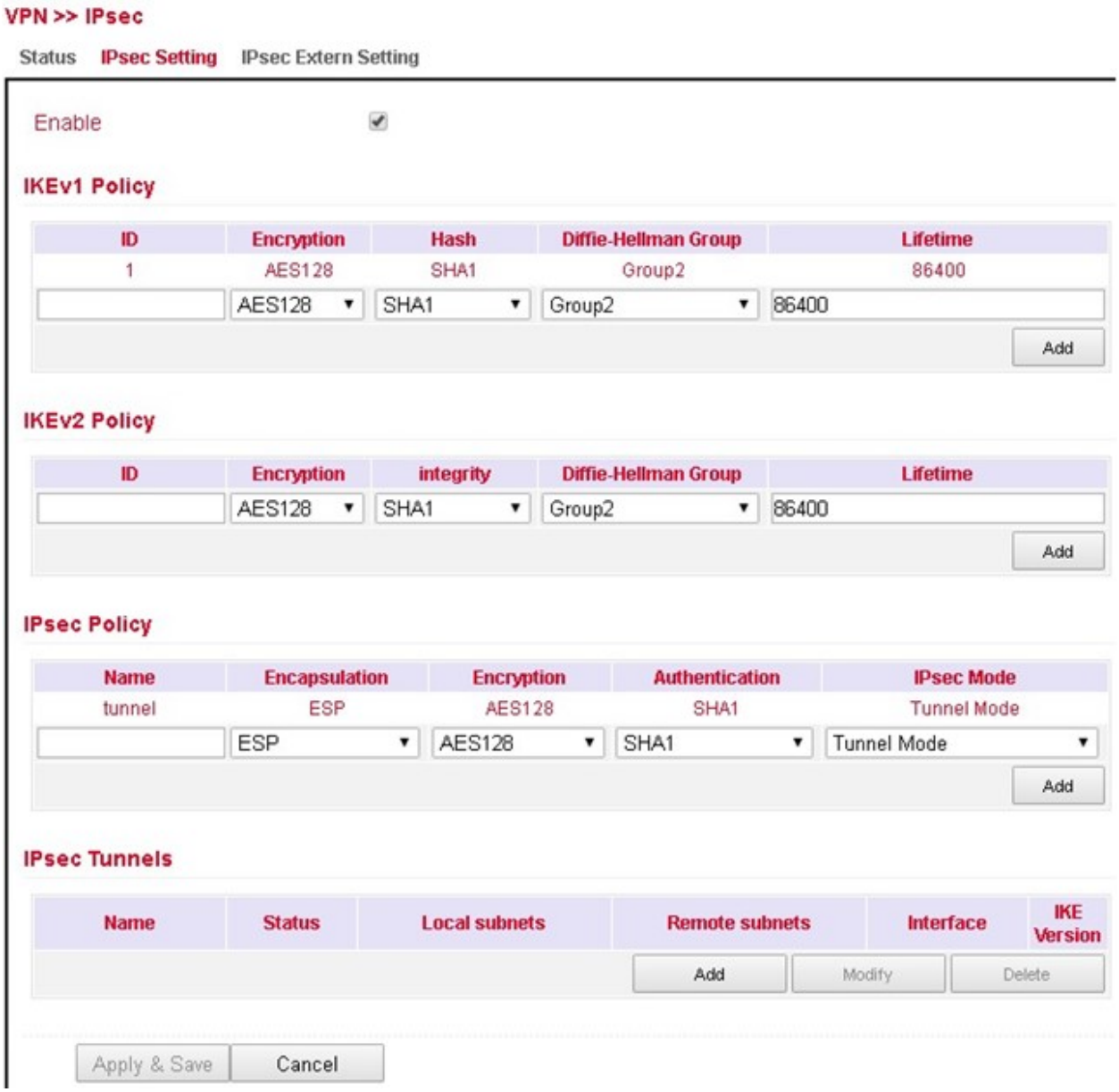
3.7.1.1. Status

Wenn der oder die IPsec Tunnel erfolgreich aufgebaut wurden, dann sieht man folgendes in der Status-Übersicht.

3.7.1.2. IPsec Setting

Unter ***VPN > IPsec > IPsec Setting*** können bestehende Einstellungen angepasst oder ein neuer IPsec Tunnel angelegt werden. Bei Neuanlage eines IPsec-Tunnels muss zunächst eine ***IKE Policy*** und eine ***IPsec Policy*** angelegt werden.

Anschließend muss diese Einstellung zunächst mit ***Apply & Save*** bestätigt werden. Dann kann der eigentliche IPsec Tunnel über ***Add*** angelegt werden.



IKEv1 Policy:

Parameter	Beschreibung
ID	Ganzzahl, kann frei gewählt werden. Dient der Identifizierung der Policy in der Tunnel-Konfiguration
Encryption	Verschlüsselungsmethode
Hash	Hashalgorithmus
Diffie-Hellman Group	DH-Group für den Schlüsselaustausch
Lifetime	Gültigkeitsdauer der IKE, bevor diese neu ausgehandelt wird

IKEv2 Policy:

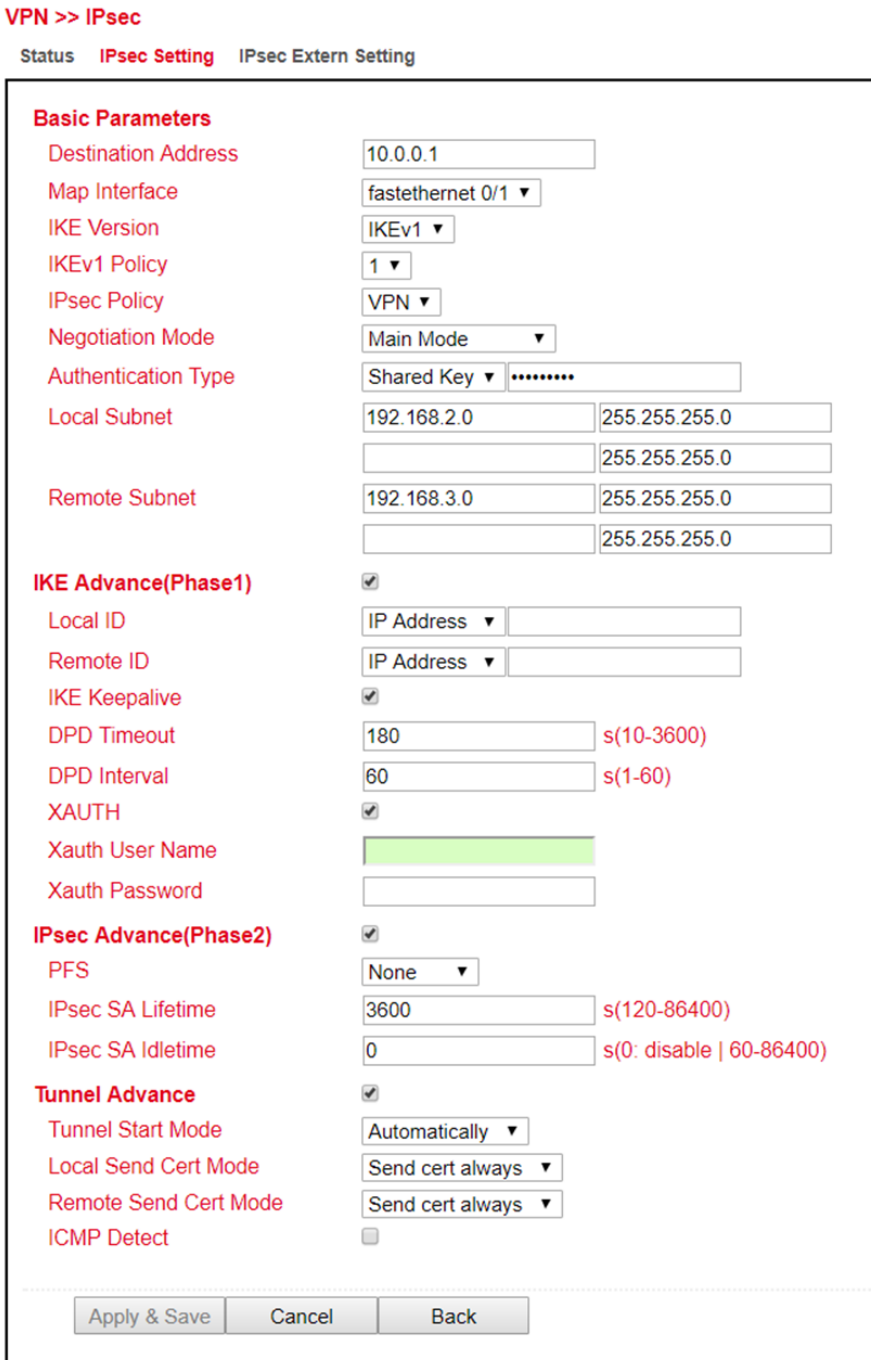
Parameter	Beschreibung
ID	Ganzzahl, kann frei gewählt werden. Dient der Identifizierung der Policy in der Tunnel-Konfiguration
Encryption	Verschlüsselungsmethode
integrity	Hashalgorithmus
Diffie-Hellman Group	DH-Group für den Schlüsselaustausch
Lifetime	Gültigkeitsdauer der IKE, bevor diese neu ausgehandelt wird

IPsec Policy:

Parameter	Beschreibung
Name	Frei wählbarer Name der IPsec Policy. Dient der Identifizierung der Policy in der Tunnel-Konfiguration
Encapsulation	ESP oder AH
Encryption	Verschlüsselungsmethode
Authentication	Hashalgortihmus
IPsec Mode	Tunnel oder Transport Mode

3.7.1.2.1. IPsec Tunnel

Über ***VPN > IPsec > IPsec Setting*** kann man unter dem Punkt ***IPsec Tunnels*** mit ***Add*** einen neuen IPsec Tunnel (IKEv1 und IKEv2) anlegen. Voraussetzung ist, dass zuvor eine IKEv1 bzw. IKEv2 Policy und eine IPsec Policy angelegt worden sind.



Basic Parameters:

Parameter	Beschreibung
Destination Address	IP-Adresse der Tunnel-Gegenstelle
Map Interface	Interface des Routers, über das die Verbindung aufgebaut werden soll
IKE Version	IKEv1 oder IKEv2
IKEv1 Policy	Die ID Nummer der zuvor angelegten IKEv1 Policy
IPsec Policy	Der Name der zuvor angelegten IPsec Policy
Negotiation Mode	Main Mode oder Agressive Mode
Authentication Type	Shared Key oder Certificate
Local Subnet	Das Subnetz des Routers
Remote Subnet	Das Subnetz der Gegenstelle

IKE Advance(Phase1):

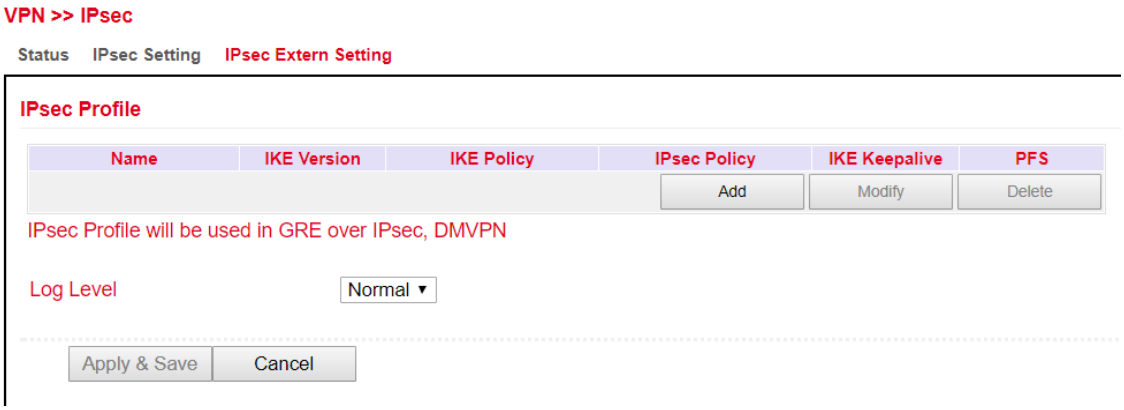
Parameter	Beschreibung
Local ID	IP Address, FQDN oder User FQDN
Remote ID	IP Address, FQDN oder User FQDN
IKE Keepalive	Schaltet IKE Keepalive ein oder aus
DPD Timeout	Timeout für ein DPD Paket
DPD Interval	Intervall der DPD Pakete
XAUTH	Schaltet XAUTH ein oder aus
Xauth User Name	XAUTH Benutzername
Xauth Password	XAUTH Passwort

IPsec Advance(Phase2):

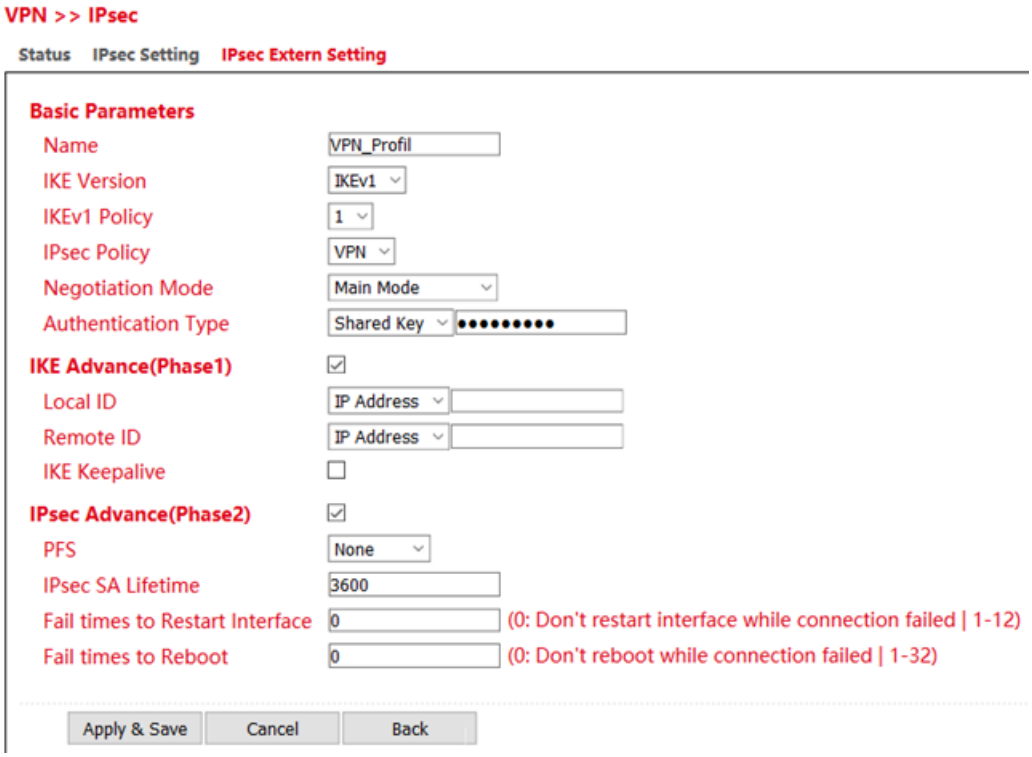
Parameter	Beschreibung
PFS	Perfect Forward Secrecy Gruppe
IPsec SA Lifetime	Gültigkeitsdauer der SA, bevor diese neu erstellt wird
IPsec SA Idletime	SAs, die mit inaktiven Peers verknüpft sind, können gelöscht werden, bevor die globale Lebensdauer abgelaufen ist.
Tunnel Advance:	

Parameter	Beschreibung
Tunnel Start Mode	Auswahl des Startmodus für den Tunnel. Automatisch ist Standard.
Local Send Cert Mode	Legt fest wann das Zertifikat gesendet werden soll
Remote Send Cert Mode	Legt fest wann das Zertifikat gesendet werden soll
ICMP Detect	Schaltet den ICMP Watchdog ein oder aus
ICMP Detection Server	Zum Testen der IPsec Tunnelverbindung muss hier ein Server angegeben werden, der nur durch den Tunnel erreichbar ist
ICMP Detection Local IP	Hier wird die Router Interface IP des Local Subnet angegeben
ICMP Detection Interval	Intervall in dem das ICMP Paket gesendet wird
ICMP Detection Timeout	Zeit, nach dem das ICMP Paket verworfen wird
ICMP Detection Max Retries	Maximale Versuche, nach einem Fehlgeschlagenen ICMP Ping

3.7.1.3. IPsec Extern Setting



IPsec Profile werden bei GRE over IPsec genutzt. Angelegt wird das Profil über den ADD Button.



Parameter	Beschreibung
Name	Eindeutiger Name für die externen Einstellungen des IPsec
IKE Version	IKEv1 oder IKEv2
IKEv1 Policy	Die ID Nummer der zuvor angelegten IKEv1 Policy
IPsec Policy	Der Name der zuvor angelegten IPsec Policy
Negotiation Mode	Main Mode oder Agressive Mode
Authentication Type	Shared Key oder Certificate

IKE Advance (Phase1)

Parameter	Beschreibung
Local ID	IP Address, FQDN oder User FQDN
Remote ID	IP Address, FQDN oder User FQDN
IKE Keepalive	Schaltet IKE Keepalive ein oder aus
DPD Timeout	Timeout für ein DPD Paket
DPD Interval	Intervall der DPD Pakete
***\	
IPsec Advance (Phase2)***	

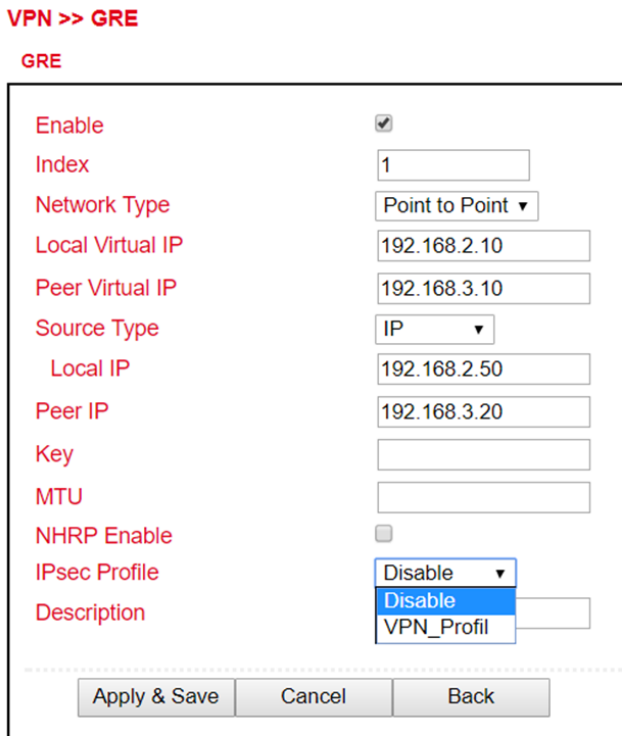
Parameter	Beschreibung
PFS	Perfect Forward Secrecy Gruppe
IPsec SA Lifetime	Gültigkeitsdauer der SA, bevor diese neu erstellt wird
Fail times to Restart Interface	Anzahl der fehlgeschlagenen Verbindungsversuche, nach denen der IPsec Tunnel neu gestartet werden soll
Fail times to Reboot	Anzahl der fehlgeschlagenen Verbindungsversuche, nach denen der Router neu gestartet werden soll.

3.7.2 3.7.2. GRE

Das GRE (Generic Routing Encapsulation) Protokoll wird benutzt, um andere Protokolle einzukapseln und über Tunnel zu transportieren.

GRE wird verwendet, wenn dynamisches Routing über den IPSec Tunnel realisiert werden soll.

Übersichtsseite. **Mit Add wird ein neuer GRE Eintrag hinzugefügt.**

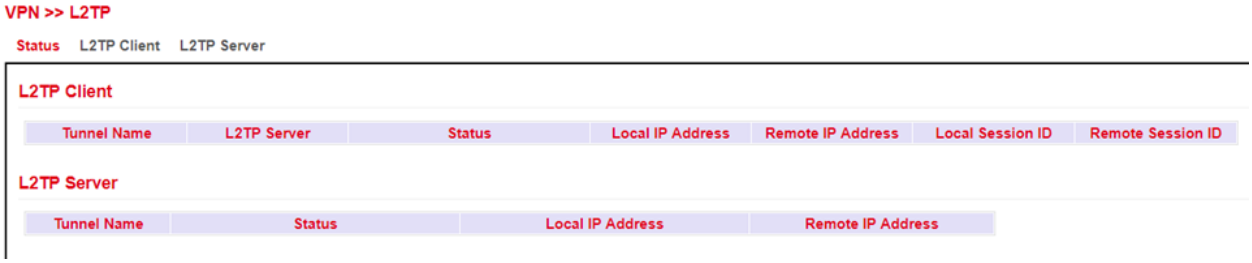


Unter IPsec Profile ist jetzt das Profil in der Auswahlliste, das unter ***VPN > IPsec > IPsec Extern Setting*** angelegt wurde.

3.7.3 3.7.3. L2TP

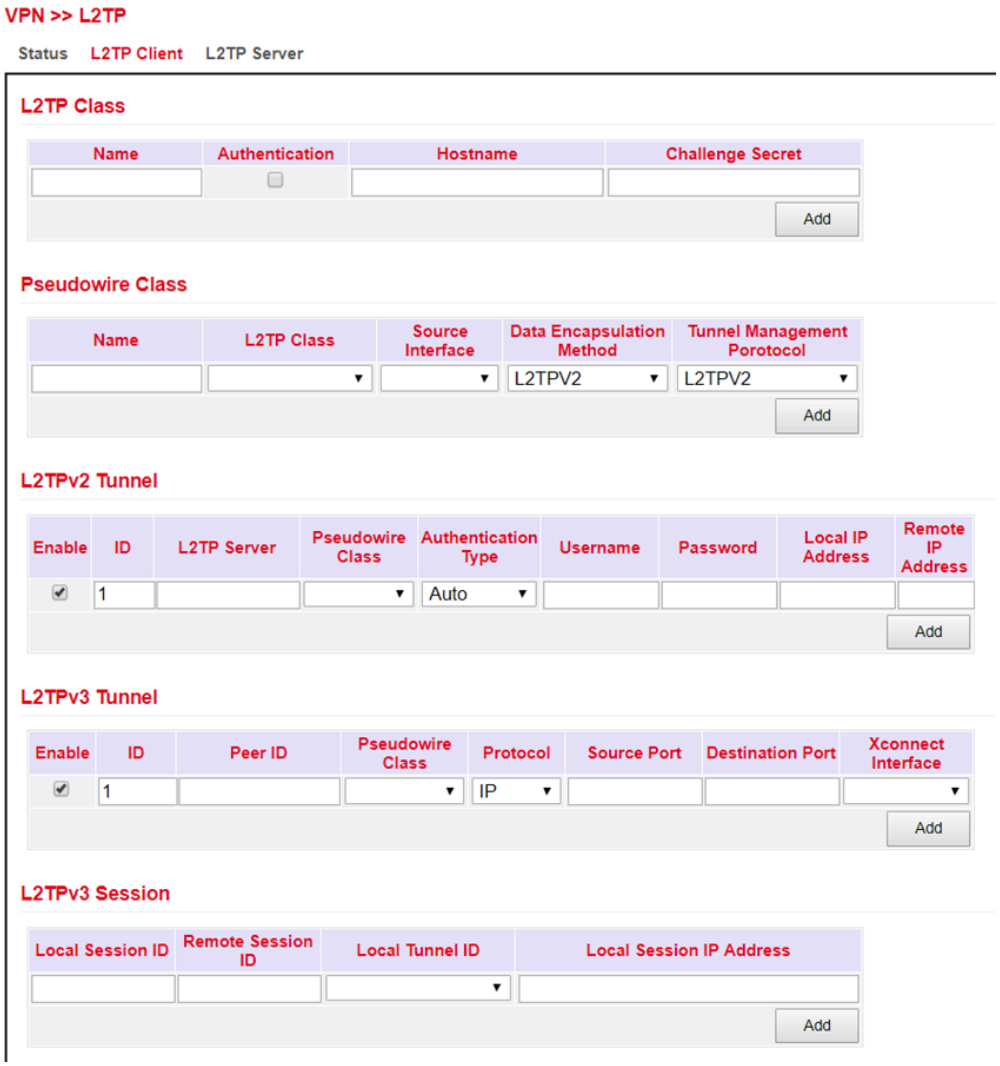
L2TP (Layer-2-Tunneling-Protocol) kombiniert PPTP (Point to Point Tunneling Protokoll) und L2F (Layer 2 Forwarding). L2TP unterstützt lediglich eine Benutzerauthentifizierung, aber keine Verschlüsselung. Daher wird L2TP in Verbindung mit einem IPSec Tunnel verwendet um die Verschlüsselung zu garantieren. L2TP wird oft eingesetzt um Einzelrechner (Stichwort: Road-Warrior) ans Netzwerk anzubinden.

3.7.3.1. L2TP Status



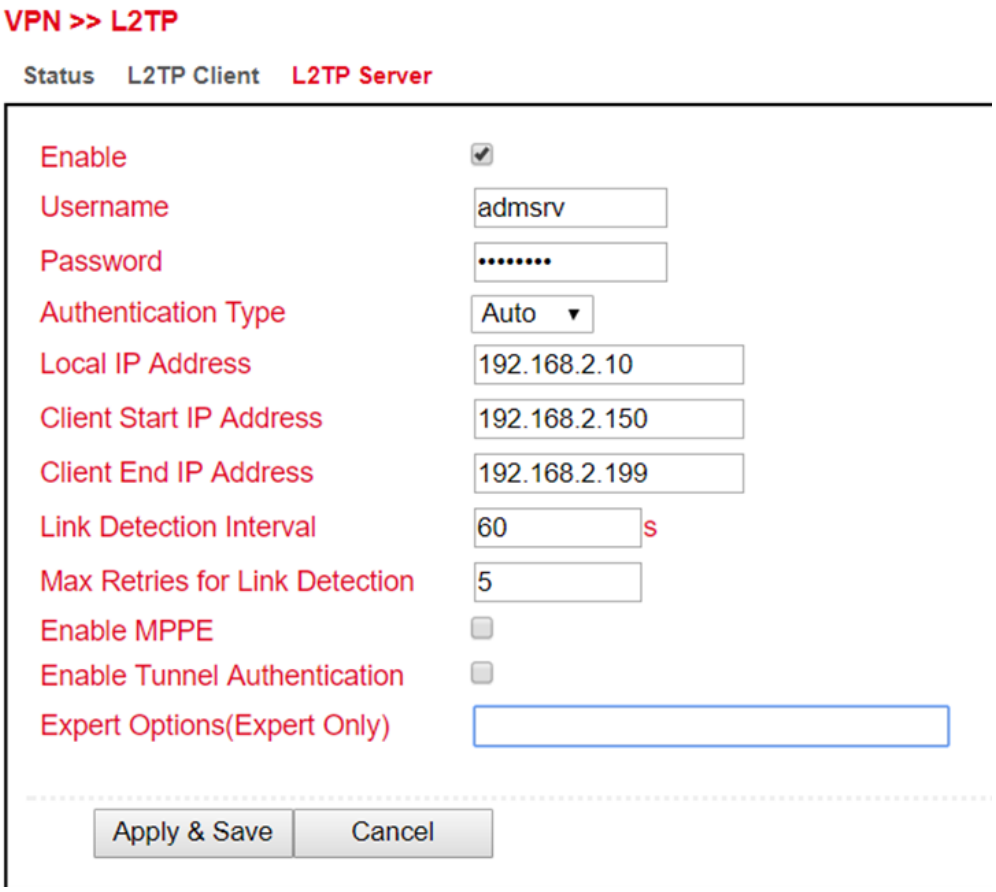
3.7.3.2. L2TP Client

Hier wird unter ***VPN > L2TP > L2TP Client*** der entsprechende Client für den Tunnel angelegt. Die jeweiligen Einträge müssen Sie mit dem Add Button hinzufügen und werden erst komplett gespeichert, wenn der Apply & Save Button angeklickt wird.



3.7.3.3. L2TP Server

Hier können Sie einen entsprechender L2TP Server anlegen.



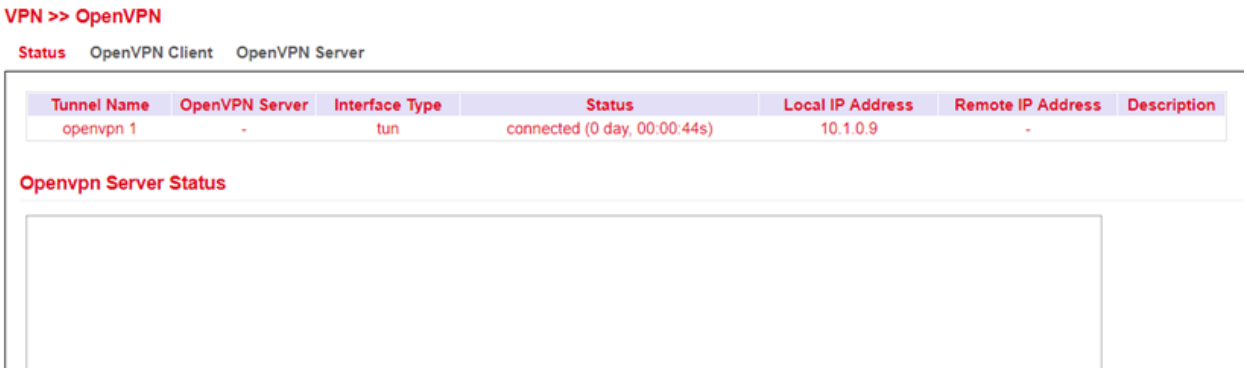
3.7.4 3.7.4. OpenVPN

OpenVPN ist eine freie Software zum Aufbau eines Virtuellen Privaten Netzwerkes (VPN) über eine verschlüsselte TLS-Verbindung. Zur Verschlüsselung wird die Bibliothek OpenSSL benutzt. OpenVPN verwendet wahlweise UDP oder TCP zum Transport.

3.7.4.1. OpenVPN Status

Überblick über den Status des eingerichteten OpenVPN.

Client Status:

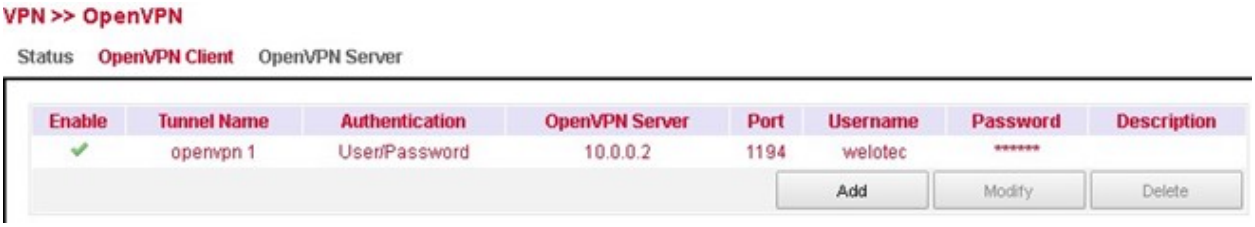


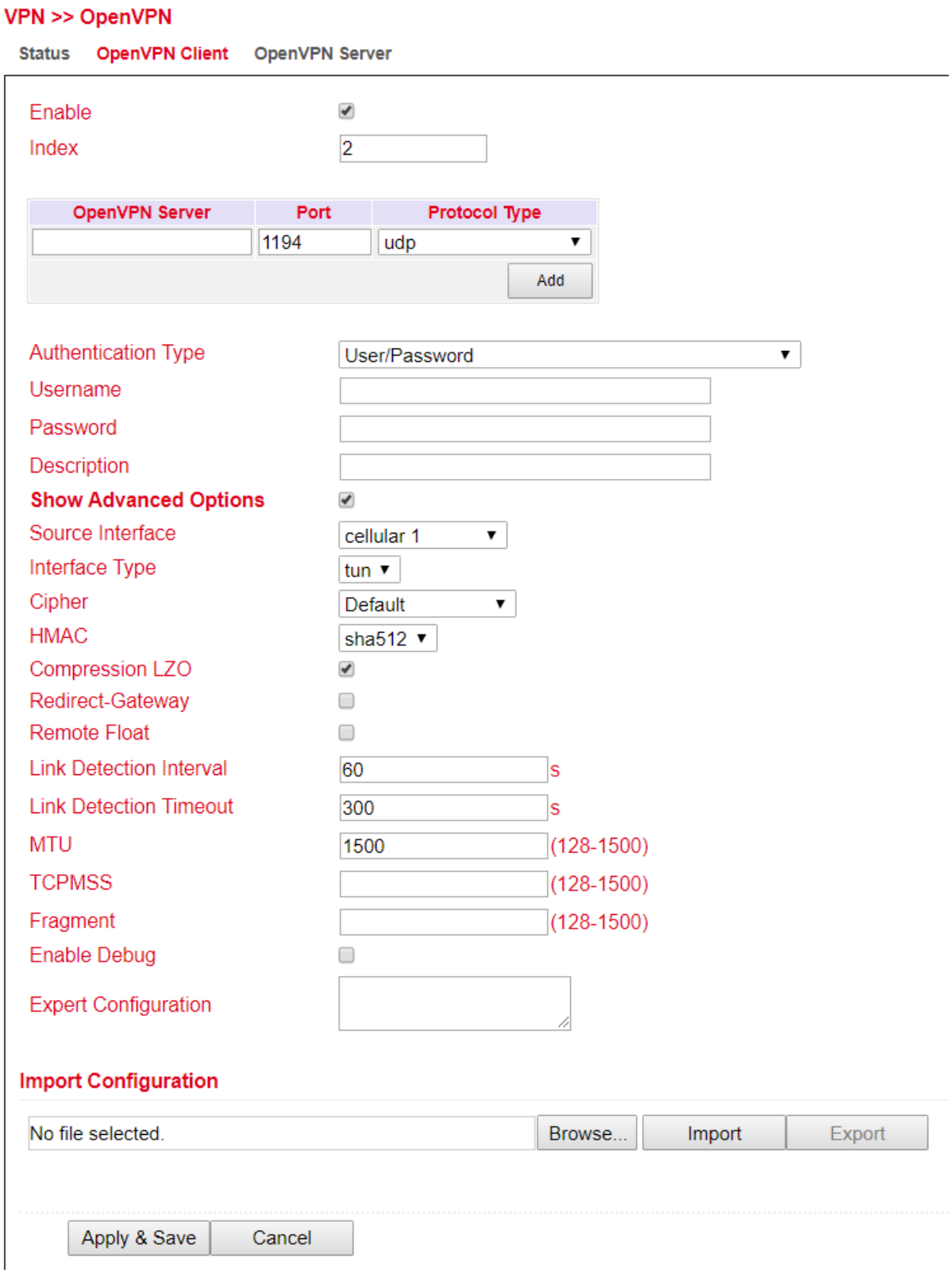
Server Status:

3.7.4.2. OpenVPN Client

Unter ***VPN > OpenVPN > OpenVPN Client*** kann ein neuer OpenVPN Tunnel hinzugefügt werden. Der Router ist dabei als Client zu konfigurieren.

Über den Button „***Add***“ kann eine neue Konfiguration angelegt werden.





Hinweis

Abhängig von der gewählten Authentifizierung sind unterschiedliche Eingaben möglich. In diesem Beispiel wird Username / Password behandelt.

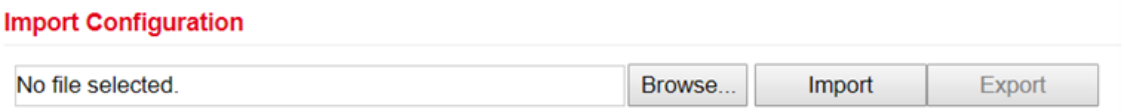
Parameter	Beschreibung
Enable	Schaltet den OpenVPN Client ein oder aus
Index	Frei wählbar, dient lediglich der Identifizierung
OpenVPN Server	Die IP-Adresse oder der FQDN des OpenVPN Servers
Authentication Type	Authentifizierungsmethode (empfohlen x509-cert)
Username	Benutzername
Password	Passwort
Description	kurze Beschreibung des Clients

Show Advanced Options:

Parameter	Beschreibung
Source Interface	Das Interface, über das der OpenVPN Tunnel aufgebaut werden soll
Interface Type	tun oder tap (empfohlen tun)
Cipher	Verschlüsselungmethode
HMAC	Signiert alle Pakete die bei der TLS Handshake involviert sind. Sha1 ist Standard
Compression LZO	Kompression der Daten aktivieren oder deaktivieren
Redirect-Gateway	Wenn Redirect-Gateway eingeschaltet ist, wird der gesmmte Traffic durch den Tunnel geroutet
Remote Float	Wenn Remote Float aktiviert ist, nimmt der Client auch Pakete entgegen die der Authentifizierung entsprechen, aber nicht von der Server-Adresse stammen. Diese Option ist Sinnvoll, wenn der Server eine Dynamische IP-Adresse hat
Link Detection Interval	Intervall, in dem die Tunnelverbindung überprüft wird.
Link Detection Timeout	Timeout für ein Paket zur Tunnelverbindungsprüfung.
MTU	Maximale Paketgröße
TCPMSS	Legt die maximale Größe für TCP-Pakete fest
Fragment	Maximale Paketgröße für UDP Pakete
Enable Debug	Schaltet den Debug-Modus ein oder aus
Expert Configuration	Hier können direkt OpenVPN Tunneloptionen eingetragen werden, die nicht über das Webinterface verfügbar sind.

Hinweis

Der Client benötigt immer das CA Zertifikat des Servers, andernfalls kann er sich nicht authentifizieren.



Hierüber kann eine bereits existierende OpenVPN Konfiguration importiert oder die aktuelle Konfiguration exportiert werden. Die OpenVPN Konfiguration kann vom OpenVPN Server exportiert werden. Diese hat dann die Datei-Endung .ovpn.

Hinweis

Achten Sie bitte darauf, dass die OVPN-Datei keine Leerzeichen enthält. Leerzeichen werden vom Router anders interpretiert.

3.7.4.3. OpenVPN Server

Über ***VPN > OpenVPN > OpenVPN Server*** konfigurieren Sie den Router als OpenVPN. Voraussetzung hierfür ist, dass der Router eine ***öffentliche IP-Adresse*** hat.

VPN >> OpenVPN

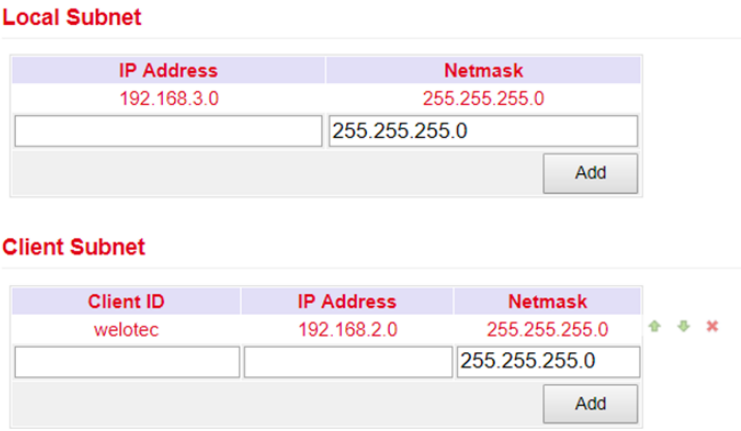
Status | OpenVPN Client | OpenVPN Server

Enable	☑
Config Mode	Manual Config
Authentication Type	User/Password
Virtual Network	10.0.0.1
Virtual Netmask	255.255.255.0
Description	WeloVPN
Show Advanced Options	☑
Source Interface	fastethernet 0/1
Interface Type	tun
Network Type	net30
Protocol Type	udp
Port	1194
Cipher	Default
HMAC	sha1
Client-to-Client	☐
Compression LZO	☑
Link Detection Interval	60 s
Link Detection Timeout	300 s
MTU	1500 (128-1500)
TCPMSS	(128-1500)
Fragment	(128-1500)
Enable Debug	☐
Expert Configuration	

User Password

Username	Password
welotec	******

Add



Abhängig von der gewählten Authentifizierung sind unterschiedliche Eingaben möglich. In diesem Beispiel wird Username / Password behandelt.

Parameter	Beschreibung
Enable	Schaltet den OpenVPN Server ein oder aus
Config Mode	Hier kann zwischen der manuellen Konfiguration und dem Import einer fertigen Konfiguration gewählt werden
Authentication Type	Authentifizierungsmethode
Virtual Network	Das Virtuelle Netzwerk für den OpenVPN Tunnel
Virtual Netmask	Die Netzmaske für das Virtuelle Netzwerk des OpenVPN Tunnels
Description	Kurze Beschreibung zum Server

Advanced Options:

Parameter	Beschreibung
Source Interface	Das Interface, über das der OpenVPN Tunnel aufgebaut werden soll
Interface Type	tun oder tap (empfohlen tun)
Network Type	Verbindungstyp (empfohlen net30)
Protocol Type	UDP oder TCP
Port	Port, auf dem der OpenVPN Server laufen soll
Cipher	Verschlüsselungsmethode
HMAC	Message Authentication Code(MAC), dessen Konstruktion auf einer kryptografischen Hash-Funktion basiert
Client-to-Client	Client to Client Verbindung aktivieren oder deaktivieren
Compression LZO	Kompression der Daten aktivieren oder deaktivieren
Link Detection Interval	Intervall, in dem die Tunnelverbindung überprüft wird.
Link Detection Timeout	Timeout für ein Paket zur Tunnelverbindungsprüfung.
MTU	Maximale Paketgröße
TCPMSS	Legt die maximale Größe für TCP-Pakete fest
Fragment	Maximale Paketgröße für UDP Pakete
Enable Debug	Schaltet den Debug-Modus ein oder aus
Expert Configuration	Hier können direkt OpenVPN Tunneloptionen eingetragen werden, die nicht über das Webinterface verfügbar sind.

User Password:

Hier können Clients hinzugefügt werden, die sich dann mit dem Benutzernamen und Passwort anmelden können.

Local Subnet:

Hier werden die lokalen Subnetze des Routers eingetragen, die für die Clients erreichbar sein sollen.

Client Subnet:

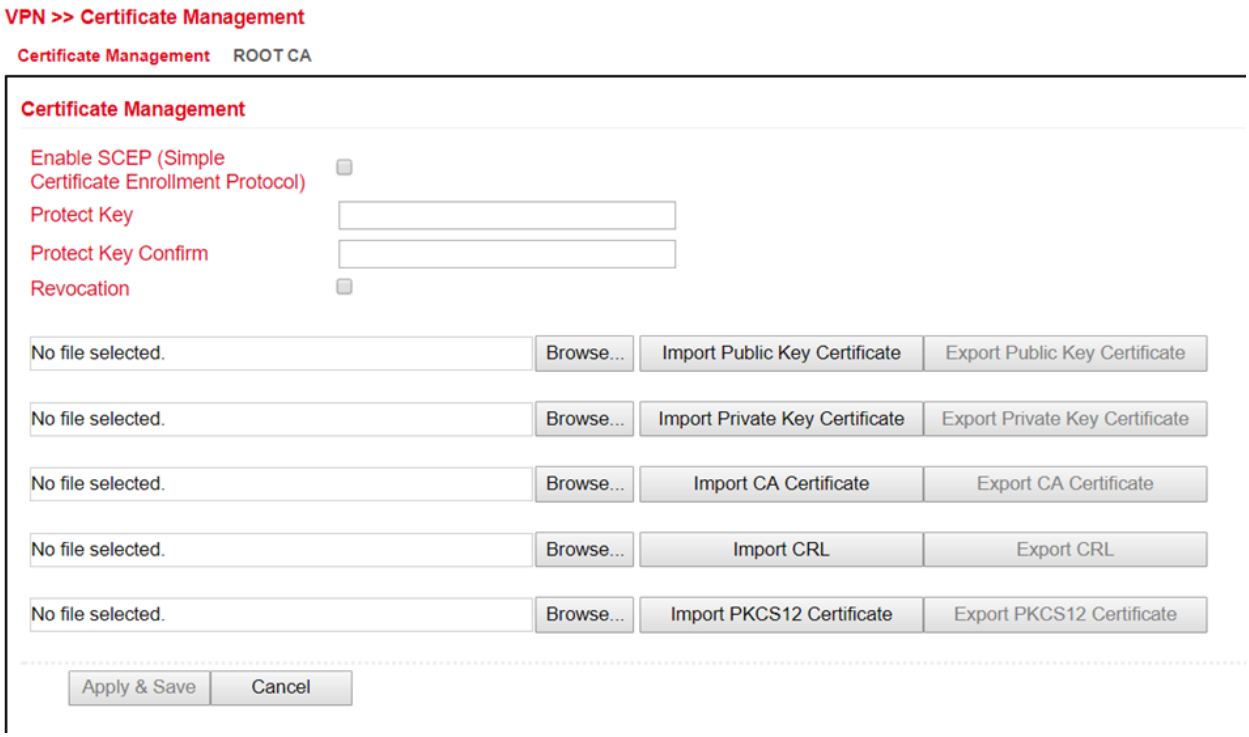
Hier werden die Client Subnetze eingetragen, die von der Serverseite aus erreichbar sein sollen. Dabei ist die ***Client ID*** bei der Authentifizierungsmethode Username/Password der Username des Clients und bei Zertifikaten der Common Name.

Hinweis

Der OpenVPN Server benötigt immer ein CA Zertifikat, sowie einen Public Key und einen Private Key. Diese werden über ***VPN > Certificate Management*** hochgeladen. Wenn diese Zertifikate nicht vorhanden sind, startet der Server nicht!

3.7.5 3.7.5. Certificate Management

Im Zertifikat Management (Certificate Management) werden die Zertifikate für einen IPSec Tunnel oder einen OpenVPN Tunnel hinterlegt, sofern diese nicht über einen Pre Shared Key (PSK) gesichert werden.



Um ein Zertifikat hochzuladen, müssen Sie auf „***Browse***“ klicken, das lokal gespeicherte Zertifikat auswählen und im Anschluss auf „***Import***…“ klicken.

Über die „***Export Funktion***“ kann überprüft werden, ob die Zertifikate ordnungsgemäß hochgeladen wurden.

Sofern die Dateien eine Größe von 0-Byte haben, versuchen Sie die Zertifikate mit einem anderen Browser oder PC hochzuladen.

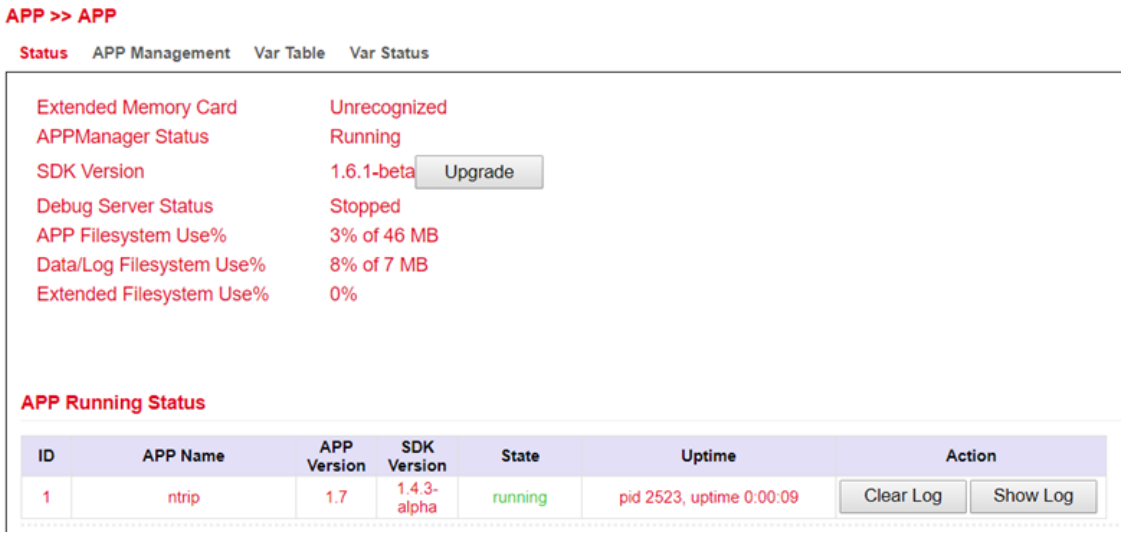
Wenn ein PKCS12 Zertifikatssatz importiert wurde und Passwortgeschützt ist, muss nach dem Import noch das Passwort unter Protect Key und Protect Key Confirm eingetragen werden.

Im Anschluss unten auf „***Apply & Save***“ klicken, um die importierten Zertifikate in der Konfiguration zu speichern.

Parameter	Beschreibung
Enable SCEP	SCEP (Simple Certificate Enrollment Protocol) wird benutzt um gesicherte Zertifikate an Netzwerkgeräte und Benutzer auszurollen. Haken Setzen um diese Funktion zu aktivieren.
Protect Key	Wenn das Zertifikat mit einem Passwort geschützt ist, dann muss in dieses Feld das Passwort für das Zertifikat eingegeben werden, da es ansonsten nicht korrekt hochgeladen werden kann.
Protect Key Confirm	Das Zertifikatpasswort erneut eingeben um die Richtigkeit des eingegebenen Passwortes zu bestätigen.
Revocation	Aktivieren dieser Funktion ermöglicht das Anlegen einer Sperrliste für ungültige Zertifikate
Import Public Key Certificate	Public Key Certificate ist das Zertifikat des öffentlichen Schlüssels
Import Private Key Certivicate	Private Key Certificate ist das Zertifikat des privaten Schlüssels.
Import CA Certificate	Certificate Authority (CA) ist das Zertifikat der Zertifizierungsstelle.
Import CRL	Certificate Revocation List ist die Zertifikatsperrliste.
Import PKCS12 Certificate	PKCS12 Zertifikat

3.8 3.8. APP

Unter dem Menüpunkt ***Administration*** > ***APP*** können Python Skripte hochgeladen werden. Die Python Skripte können über das Command Line Interface (CLI) ausgeführt und bearbeitet werden.



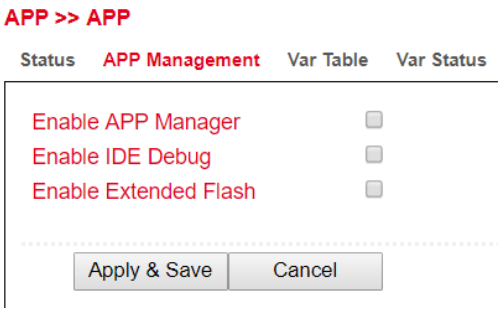
3.8.1 3.8.1. Status

Unter dem Menüpunkt ***APP > APP und Status*** kann eingesehen werden, welche Python SDK Version installiert ist und welche APP unter Python läuft. Diese APPs stehen dann den Python Skripten zur Verfügung. Über den Upgrade-Button haben Sie dann auch die Möglichkeit Ihre Python SDK Version zu aktualisieren.

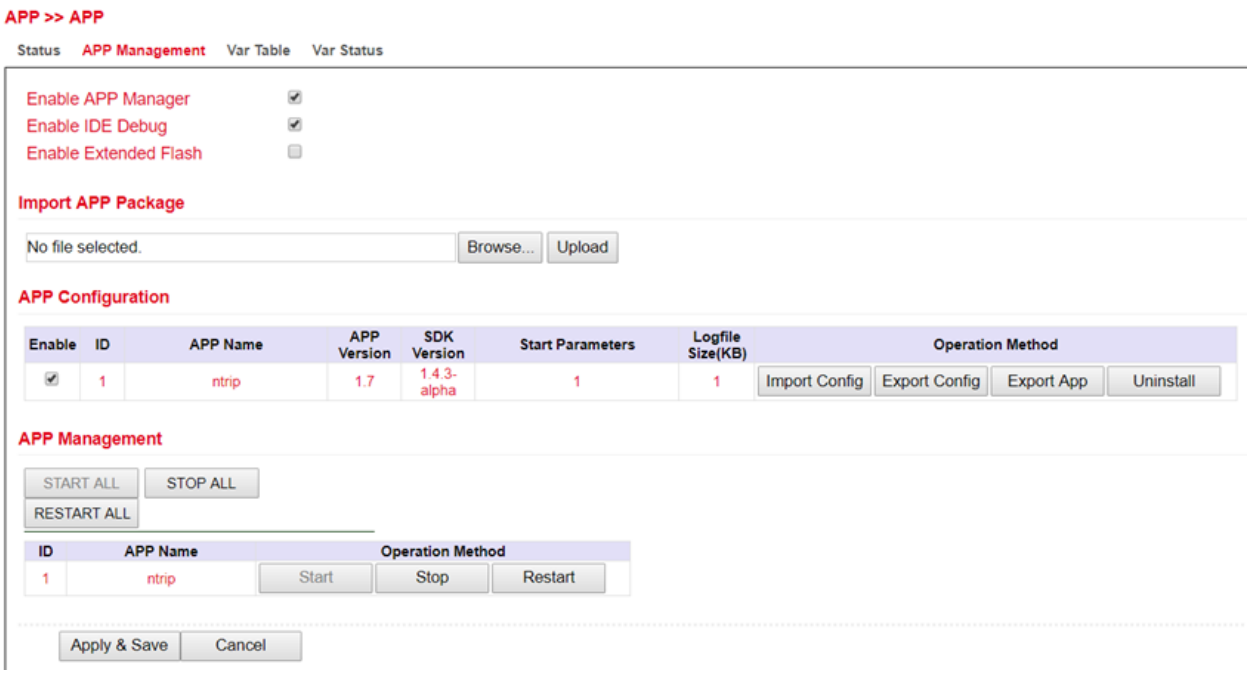
3.9

3.9.1 3.8.2. APP Management

Für die Nutzung der Client-IDE ist es notwendig, die Funktion Enable IDE-Debug auf dem TK800 zu aktivieren. Darüber hinaus ist es wichtig, dass empfehlen wir an dieser Stelle, auch den APP-Manager zu aktivieren. Der App Manager gibt Ihnen die Möglichkeit, APPs unter Python zu installieren und die vorhandenen Apps im Router-WebUI zu managen.



Aktivieren Sie dazu bitte die Funktionen Enable APP Manager und Enable IDE Debug. Klicken Sie dann Apply & Save.



Anwendung hochladen

Sobald Sie Ihre Anwendung erstellt haben, können Sie sie auf andere TK800-Router importieren.

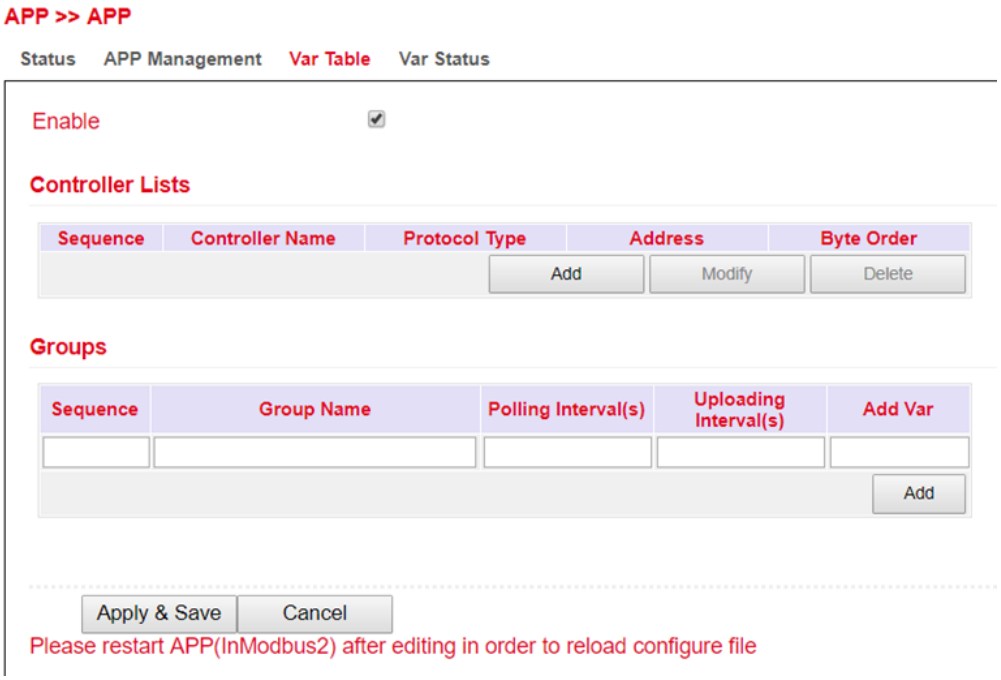
Dazu können Sie „APP -> APP -> APP-Management“ auswählen und bei Import APP Package auf „Browse“ klicken.

Wählen Sie Ihre .tar-Datei aus und klicken Sie auf Hochladen.

Nachdem Sie den Upload mit „OK“ bestätigt haben, wird die Anwendung in das System hochgeladen.

Danach können Sie bei Bedarf Ihre Konfiguration hochladen und die Anwendung aktivieren, indem Sie auf „Aktivieren“ (Enable) klicken.

3.9.2 3.8.3. Var Table



In diesem Bereich haben Sie die Möglichkeit mit APPs auf Modbus zuzugreifen. Momentan unterstützen wir diese Funktion nicht.

3.9.3 3.8.4. Var Status

Wenn Sie eigene APPs für den Zugriff auf Modbus nutzen, haben Sie hier die Möglichkeit sich den Status anzuzeigen. Momentan unterstützen wir diese Funktion nicht.

3.10 3.9. Industrial

Hinweis

Die Industrial Funktionen sind bei allen Modellen der TK800 Serie mit EX im Namen verfügbar. Beispiel: TK8X2L-EX0.

Folgende Funktionen sind verfügbar:

- Digitaler Eingang
- Relais Ausgang
- RS-232 Schnittstelle
- RS-485 Schnittstelle

3.10.1 3.9.1. DTU

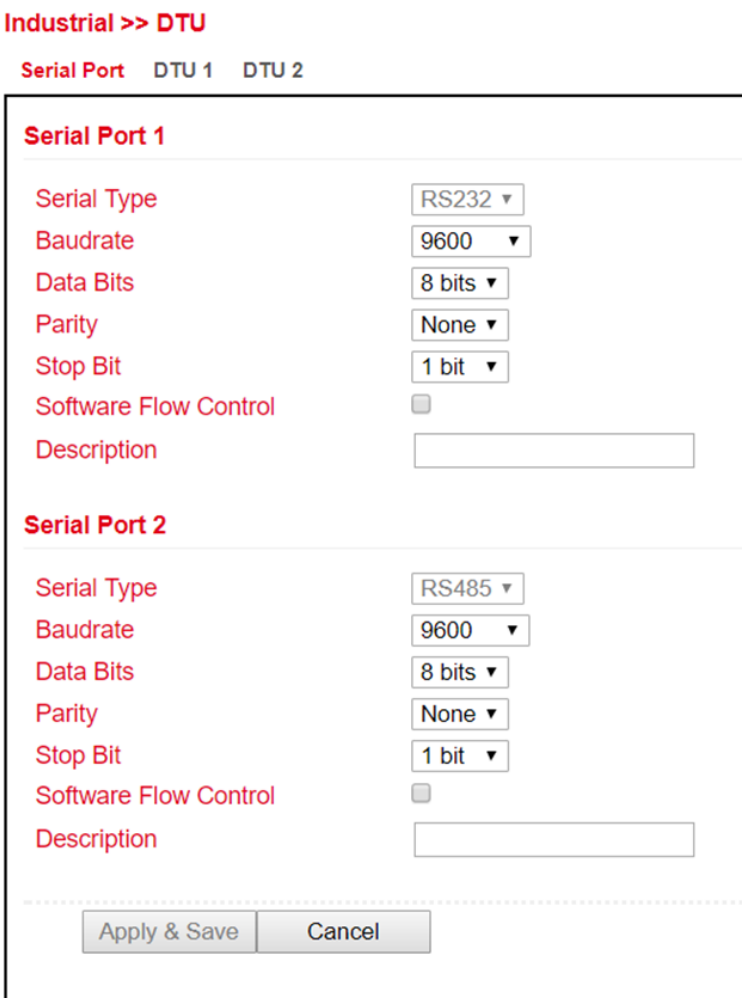
DTU steht für Data Terminal Unit und dient dazu, Geräte mit serieller Schnittstelle (RS-232 und RS-485) anzubinden. Die Konfiguration von den DTU Eigenschaften besteht immer aus zwei Teilen.

Unter dem Punkt ***Serial Port*** können die Eigenschaften der Schnittstelle definiert werden. Hier finden sich die Parameter für die RS-232 und für die RS-485 Schnittstelle.

Unter dem Punkt ***DTU 1 (RS-232)*** und dem Punkt ***DTU 2 (RS-485)*** können die Protokolle und die Parameter für die Protokolle eingestellt werden.

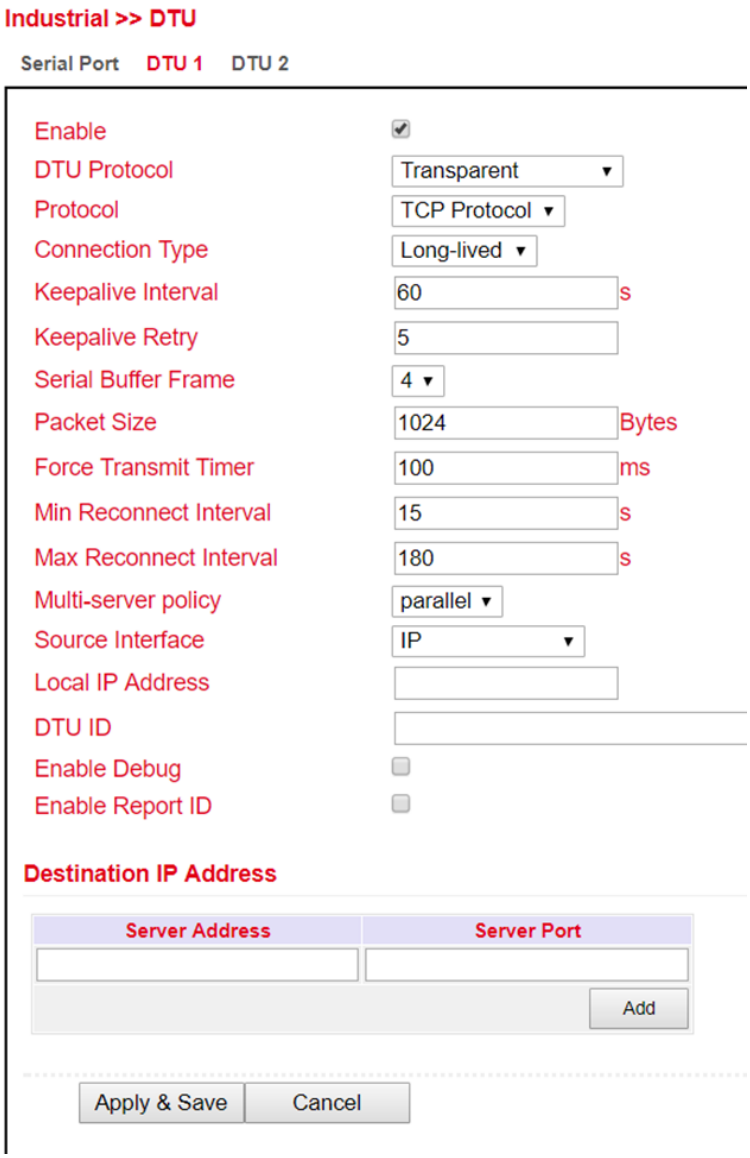
3.9.1.1. Serial Port

An dieser Stelle lassen sich die seriellen Ports 1 (RS232) und 2 (RS485) konfigurieren.

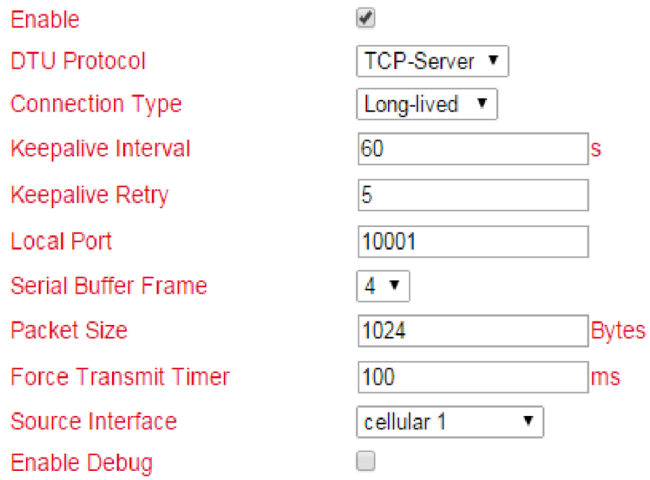


3.9.1.2. DTU 1 / DTU 2

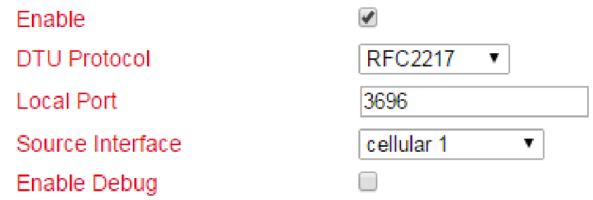
Transparent



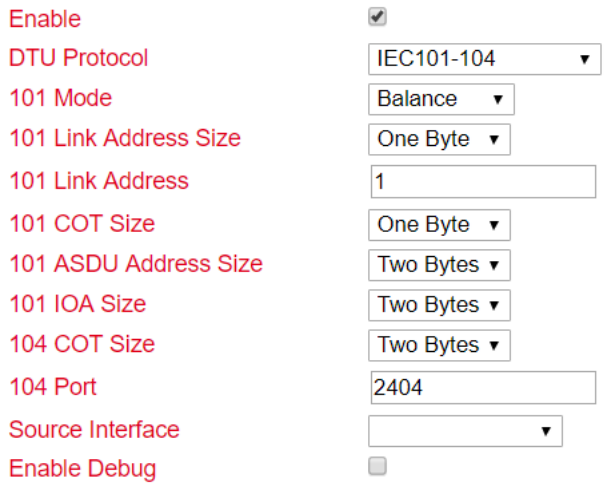
Auswahl TCP-Server bei DTU Protocol



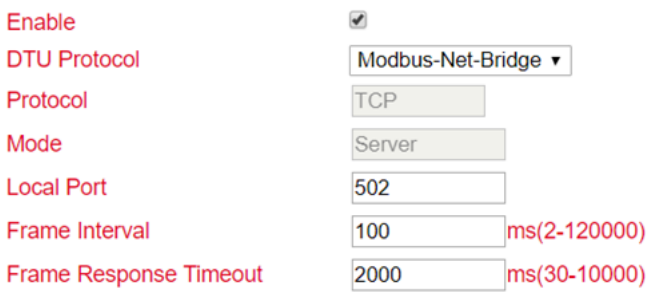
Auswahl RFC2217 bei DTU Protocol



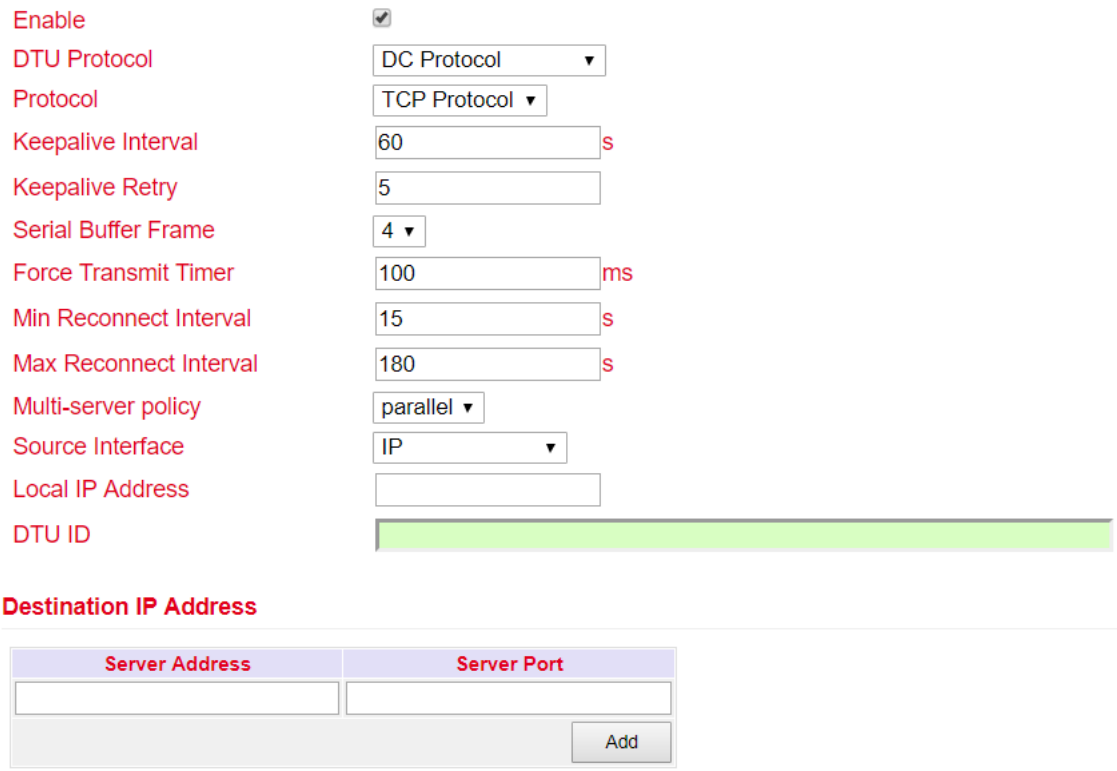
Auswahl IEC60870-5-101/104 bei DTU Protocol



Auswahl Modbus-Net-Bridge bei DTU Protocol

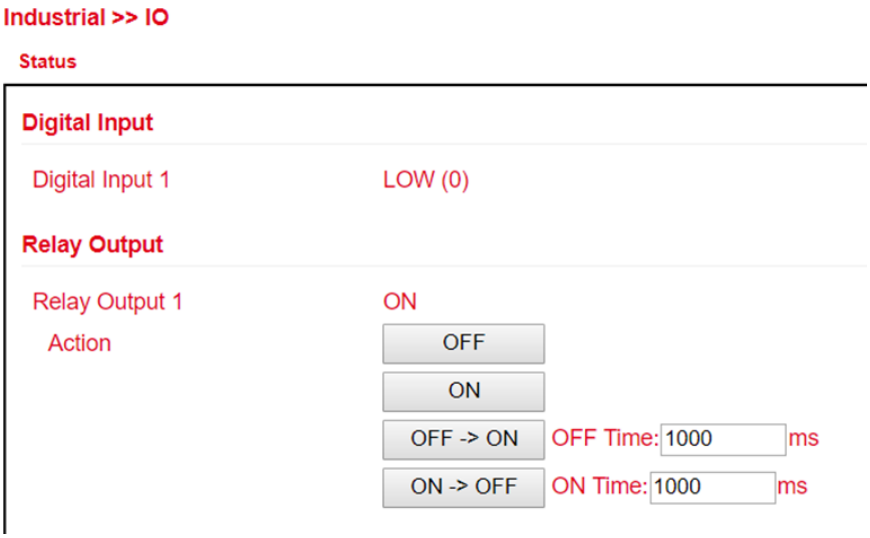


Auswahl DC Protocol bei DTU Protocol



3.10.2 3.9.2. IO

Unter ***Industrial > IO*** können Sie konfigurieren, ob der digitale Eingang zum Schalten der VPN Verbindungen dienen soll. Das Relay ist dabei standardmäßig immer auf ON.

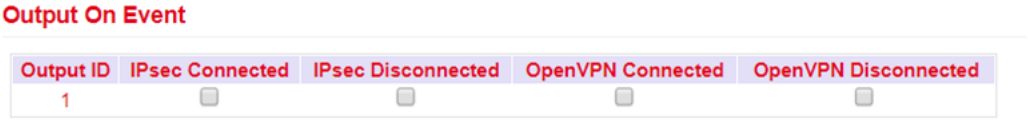


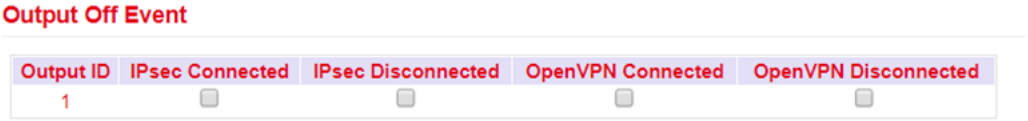
Digital Input:

Zeigt den Status vom digitalen Eingang an.

Relay Output:

Parameter	Beschreibung
Relay Output 1	Status des Relaisausgangs
Action	Einschalten, Ausschalten oder einen Zyklus definieren





Input High/Low Action: Beschreibung

Default Relais Einstellungen ein oder aus. Damit kann der Status des Relaisausgangs ein- oder ausgeschaltet werden oder man definiert einen entsprechenden Zyklus.

Hier kann über den digitalen Eingang ein OpenVPN- oder IPsec Tunnel gestartet oder gestoppt werden.

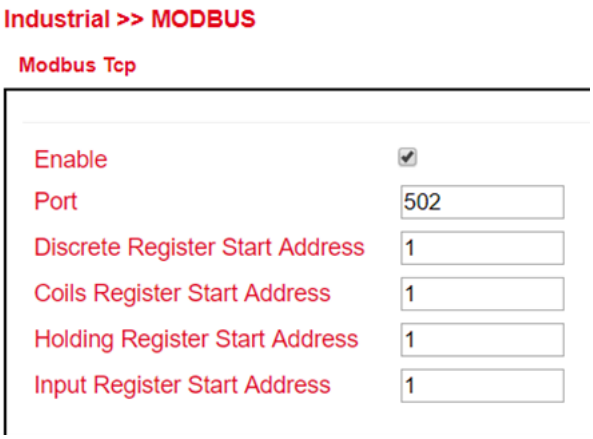
Output On/Off Event:

Hier kann der Relaisausgang verwendet werden um IPsec und OpenVPN zu starten oder zu stoppen.

3.10.3 3.9.3. Modbus

Kommunikationsprotokoll, das auf einer Master / Slave- bzw. Client / Server-Architektur basiert. Modbus/TCP ist RTU sehr ähnlich, allerdings werden TCP/IP-Pakete verwendet, um die Daten zu übermitteln. Der TCP-Port 502 ist für Modbus/TCP reserviert.

Über ***Industrial*** > ***Modbus*** > ***Modbus Tcp*** können Sie die entsprechenden Einstellungen ein- bzw. ausschalten.

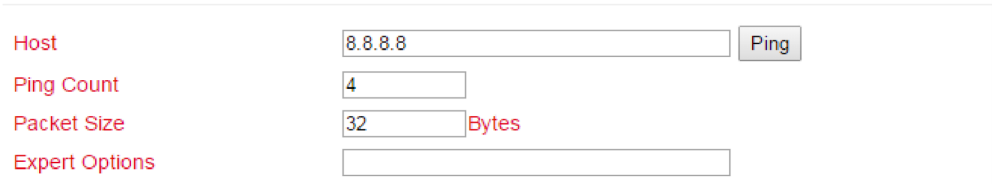


3.11 3.10. Tools

Nützliche Werkzeuge (Tools), die zum Pingen, Tracern usw. genutzt werden können.

3.11.1 3.10.1. Ping

An dieser Stelle in der Router-Software kann ein Ping abgesetzt werden um z.B. Verbindungen zu überprüfen.

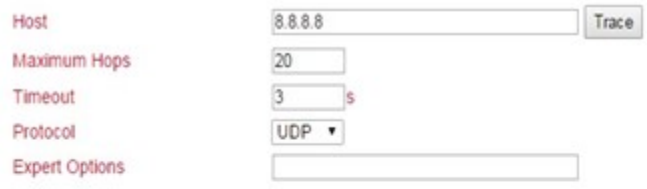


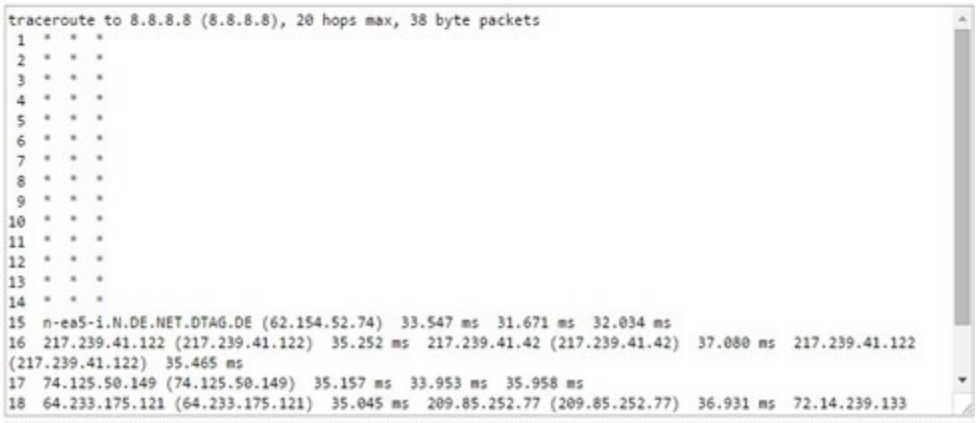

```
PING 8.8.8.8 (8.8.8.8): 32 data bytes
40 bytes from 8.8.8.8: seq=0 ttl=48 time=72.138 ms
40 bytes from 8.8.8.8: seq=1 ttl=48 time=36.295 ms
40 bytes from 8.8.8.8: seq=2 ttl=48 time=35.832 ms
40 bytes from 8.8.8.8: seq=3 ttl=48 time=36.538 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 35.832/45.200/72.138 ms
```

Parameter	Beschreibung
Host	Eingabe der anzupingenden Adresse
Ping Count	Anzahl der ausgeführten Pings. Eingabe von 1 bis 50 möglich. Standard ist 4
Packet Size	Größe des Pakets das versendet werden soll. Standard ist 32 Bytes
Expert Options	Erweiterte Funktionen

3.11.2 3.10.2. Traceroute

Traceroute (tracert) ermittelt, über welche Router und Internet-Knoten IP-Datenpakete bis zum abgefragten Rechner gelangen.



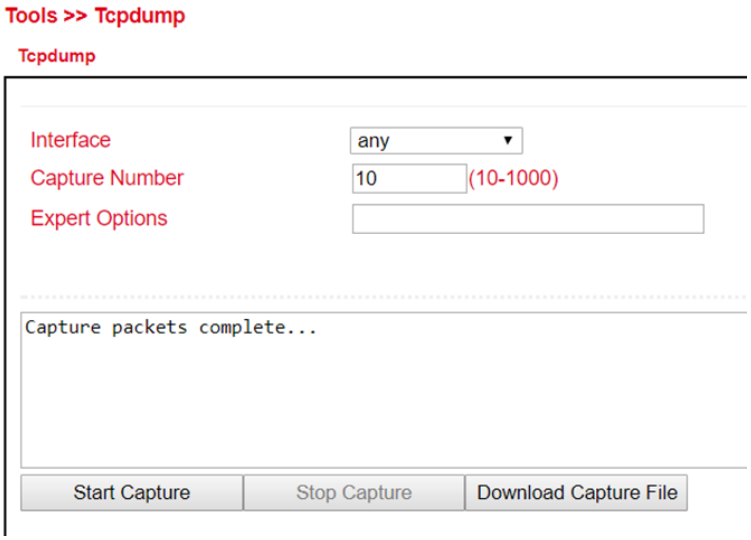


Parameter	Beschreibung
Host	Eingabe des zu ermittelnden Ziel-Hosts
Maximum Hops	Anzahl der ausgeführten Hops. Eingabe von 2 bis 40 möglich. Standard ist 20
Timeout	Eingabe des Timeout in Sekunden. Wert kann zw. 2 und 10s liegen.
Protocol	Optional entweder ICMP oder UDP. Standard ist UDP
Expert Options	Erweiterte Funktionen

3.11.3 3.10.3. Tcpdump

Bekannter und weitverbreiteter Paket-Sniffer. Ermöglicht das Mitschneiden von TCP-Paketen.

Über ***Tools*** > ***Tcpdump*** erreichen Sie diesen Sniffer.

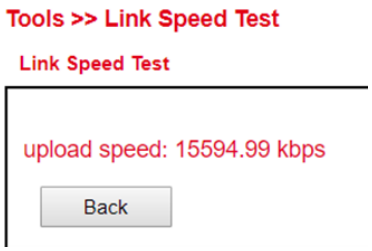


Parameter	Beschreibung
Interface	Auswahl des Interfaces, das mitgeschnitten werden soll
Capture Number	Anzahl der Mitschnitte. Standard ist 10
Expert Options	Erweiterte Funktionen
Start Capture (Button)	Startet das Mitschneiden der Datenpakete
Stop Capture (Button)	Stoppt das Mitschneiden der Datenpakete
Download Capture File (Button)	Lädt den Mitschnitt als tcpdump.pcap File herunter. Auslesbar z.B. mit Wireshark

3.11.4 3.10.4. Link Speed Test

Bestimmen der Verbindungsgeschwindigkeit durch Hoch- und Herunterladen von Dateien.

Über den Button ***Browse*** können Sie eine entsprechende Datei vom Rechner hochladen. Die Datei sollte zwischen 10 und 2000MB groß sein. Nach Auswahl der Datei klicken Sie auf den ***Upload*** Button. Das Resultat wird dann angezeigt.



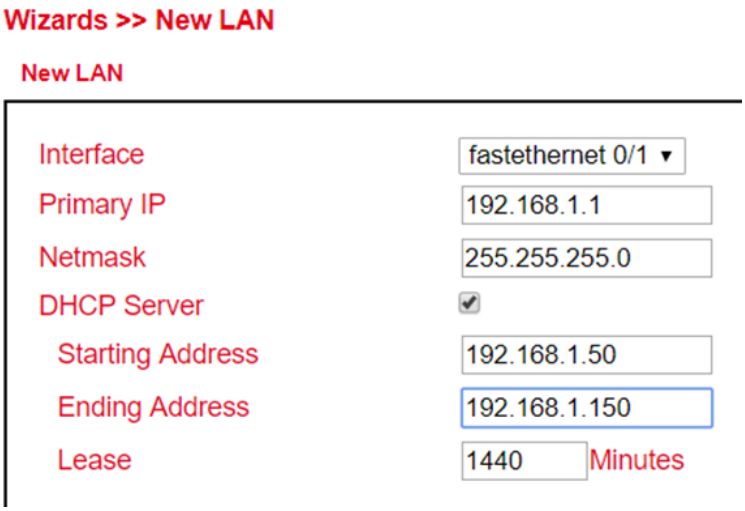
Über den ***download*** Button wird ein 130MB großes File (test.bin) heruntergeladen über das man die Download-Geschwindigkeit während des Downloads sehen kann.

3.12 3.11. Wizards

Hierbei handelt es sich um Assistenten (Wizards), die die Neuanlage der folgenden Prozesse erleichtern sollen.

3.12.1 3.11.1. New LAN

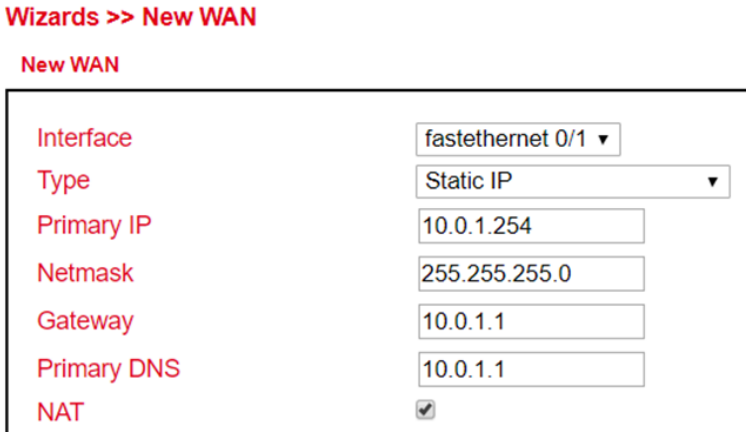
Wenn Sie eine neue LAN Schnittstelle einrichten möchten, dann können Sie dazu den Wizard unter ***Wizards > New LAN*** verwenden. Dieser legt dann im Hintergrund alle benötigten Daten an.



Parameter	Beschreibung
Interface	Die zur Verfügung stehenden Interfaces des Routers
Primary IP	Die IP-Adresse, die das gewählte Interface erhalten soll
Netmask	Die Netzmaske die das gewählte Interface bekommen soll
DHCP Server	Schaltet den DHCP Server für dieses Interface ein oder aus
Starting Address	Wenn der DHCP Server eingeschaltet ist, kann hier die DHCP-Startadresse eingetragen werden
Ending Address	Wenn der DHCP Server eingeschaltet ist, kann hier die DHCP-Endadresse eingetragen werden
Lease	Wenn der DHCP Server eingeschaltet ist, kann hier die Leasedauer einer zugewiesenen Adresse eingetragen werden

3.12.2 3.11.2. New WAN

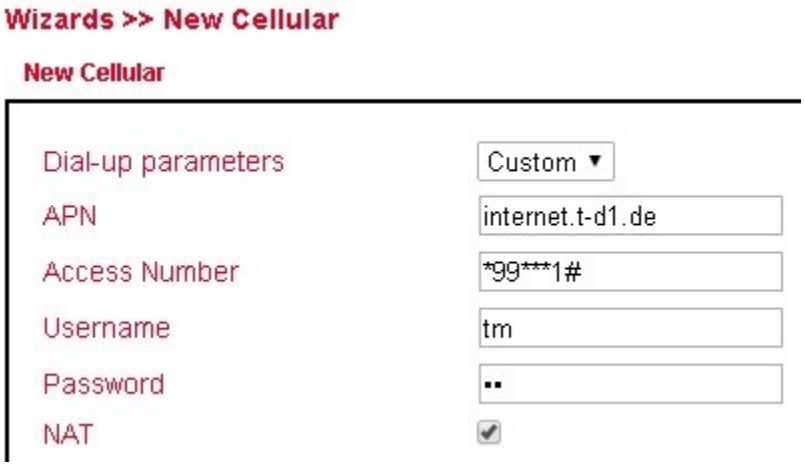
Mit Hilfe von ***Wizards > New WAN*** kann eine neue WAN Schnittstelle eingerichtet werden. Wir empfehlen Ihnen dies auch über den Wizard zu machen, da hierbei mehrere Parameter gesetzt werden.



Parameter	Beschreibung
Interface	Das neue WAN Interface
Type	Static IP / DHCP oder PPPoE, je nach Auswahl ändern sich die Parameter
Primary IP	Die IP-Adresse des Interfaces
Netmask	Die Subnetzmaske des Interfaces
Gateway	Das Gateway des Routers
Primary DNS	Der Primäre DNS Server des Routers
NAT	Schaltet NAT ein oder aus
Username	Bei Auswahl PPPoE unter Type: Username des Providers für den ADSL Zugang. Wichtig: Dafür wird ein DSL Modem benötigt
Password	Bei Auswahl PPPoE unter Type: Password des Providers für den ADSL Zugang. Wichtig: Dafür wird ein DSL Modem benötigt

3.12.3 3.11.3. New Cellular

Unter ***Wizards > New Cellular*** legen Sie ein Mobilfunkinterface als WAN Schnittstelle neu an und können es konfigurieren.



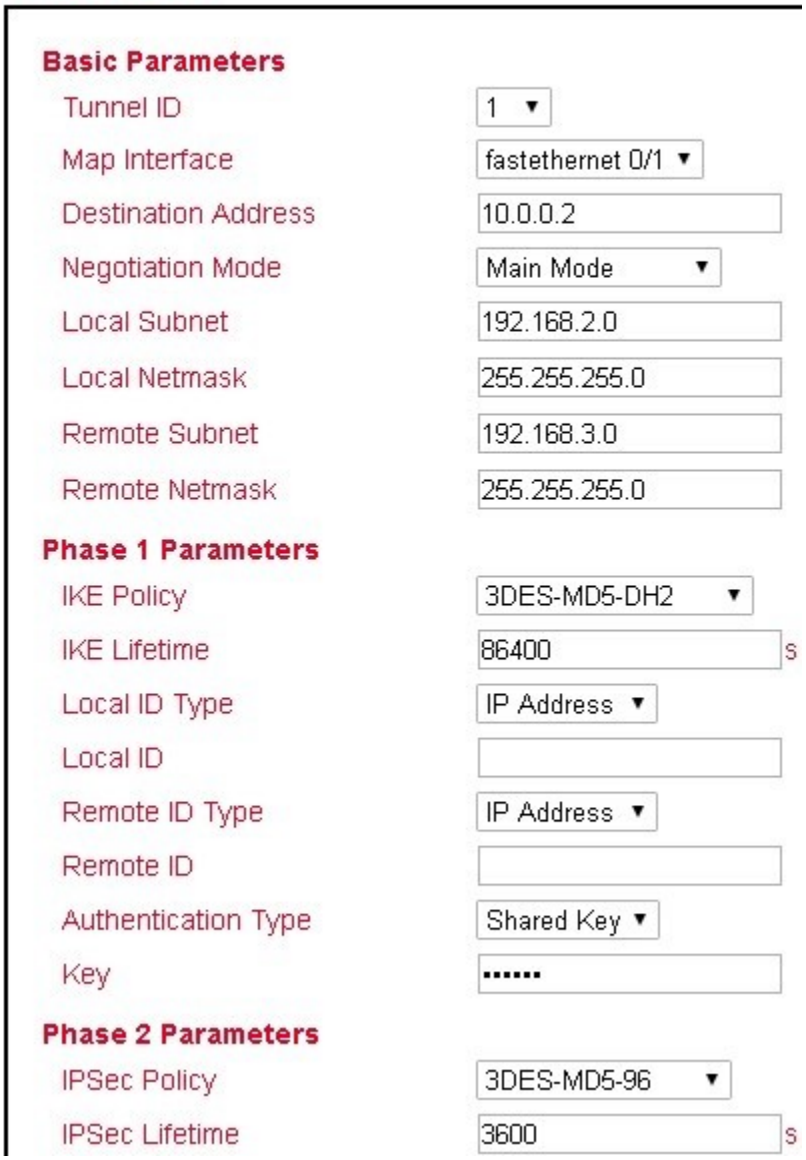
Parameter	Beschreibung
Dial-up parameters	Auto oder Custom
APN	Hier wird der APN des Internetproviders eingetragen
Access Number	Fast immer *99**1#
Username	Benutzername für den o.g. APN, sofern dieser nötig ist
Password	Passwort für den Benutzernamen zum o.g. APN, sofern dieser nötig ist
NAT	NAT aktivieren oder Deaktivieren

3.12.4 3.11.4. New IPsec Tunnel

Unter ***Wizards*** > ***New IPsec Tunnel*** können Sie einen einfachen IPsec Tunnel anlegen. Er kann später unter ***VPN*** > ***IPsec*** nachkonfiguriert werden.

Wizards >> New IPsec Tunnel

New IPsec Tunnel



Basic Parameters:

Parameter	Beschreibung
Tunnel ID	Dient zur Identifikation des Tunnels
Map Interface	Interface, über welches der IPsec Tunnel aufgebaut werden soll
Destination Address	Gegenstelle des IPsec Tunnels
Negotiation Mode	Main Mode oder Aggressive Mode (empfohlen Main Mode)
Local Subnet	Das Subnetz des Routers, welches von der Gegenstelle erreicht werden soll
Local Netmask	Subnetzmaske des Routers
Remote Subnet	Das Subnetz der Gegenstelle
Remote Netmask	Die Subnetzmaske der Gegenstelle

Phase 1 Parameters:

Parameter	Beschreibung
IKE Policy	Encryption / Hash / Diffie-Hellman-Group
IKE Lifetime	Gültigkeitsdauer der IKE Policy
Local ID Type	IP Adresse / FQDN / User FQDN
Local ID	IP Adresse oder FQDN
Remote ID Type	IP Adresse / FQDN / User FQDN
Remote ID	IP Adresse oder FQDN
Authentication Type	Authentifizierungsmethode Pre-Shared-Key oder Zertifikat
Key	Pre-Shared-Key

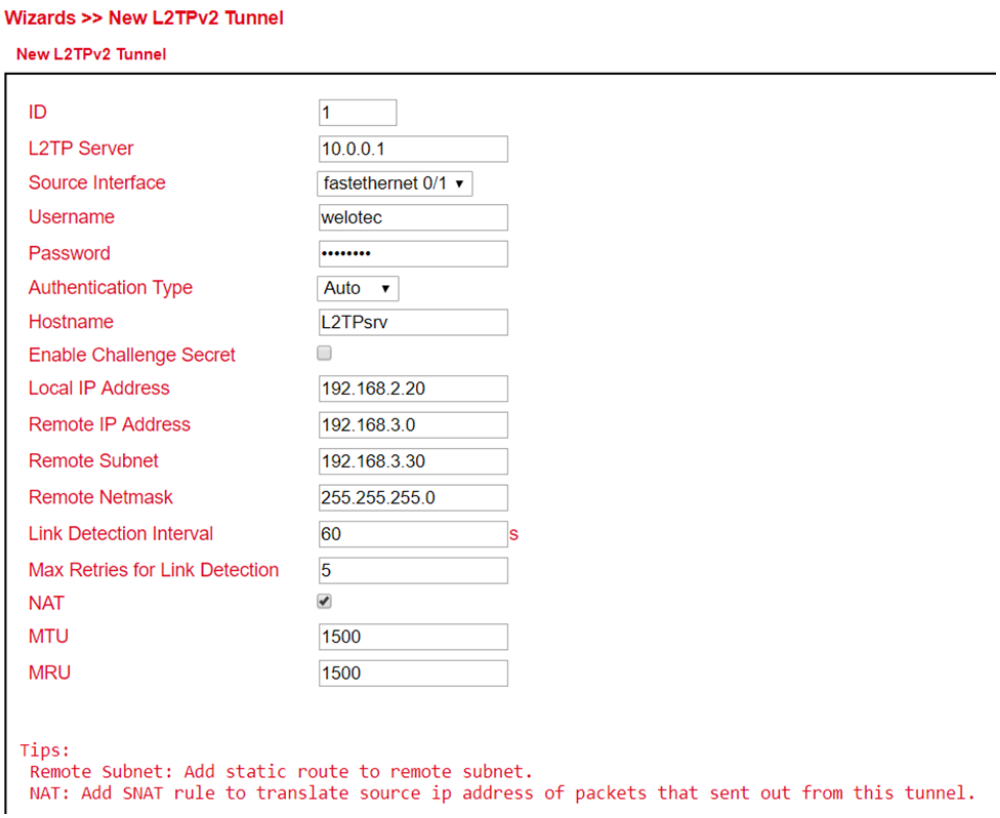
Phase 2 Parameters:

Parameter	Beschreibung
IPSec Policy	Encryption / Hash
IPSec Lifetime	Gültigkeitsdauer der IPsec Policy

3.12.5 3.11.5. IPsec Expert Config

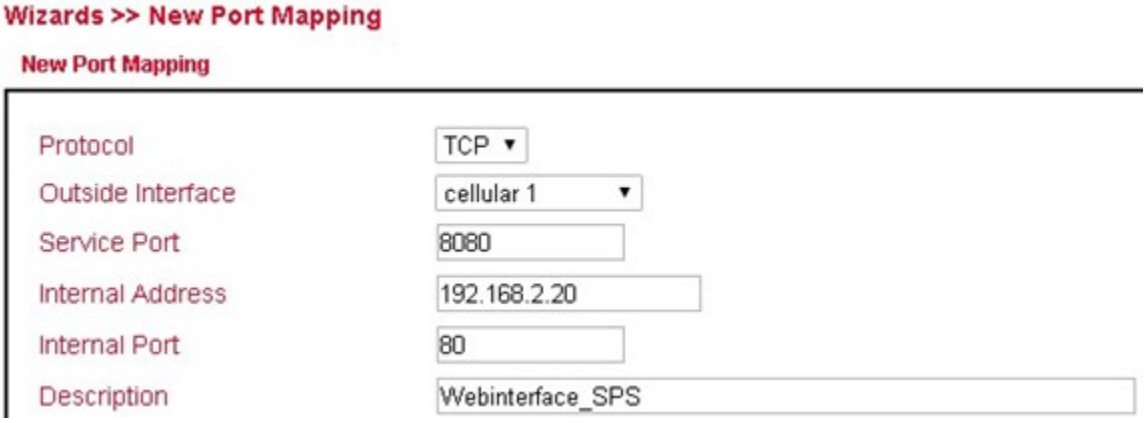
Unter ***Wizards > IPsec Expert Config*** können Sie den IPsec-Tunnelstatus durch klicken auf Refresh überprüfen. Ferner können IPsec Konfigurationen über die Schnittstelle importiert werden.

3.12.6 3.11.6. New L2TPv2 Tunnel



3.12.7 3.11.7. New Port Mapping

Unter ***Wizards*** > ***New Port Mapping*** kann einfach ein neues Port Mapping eingerichtet werden.

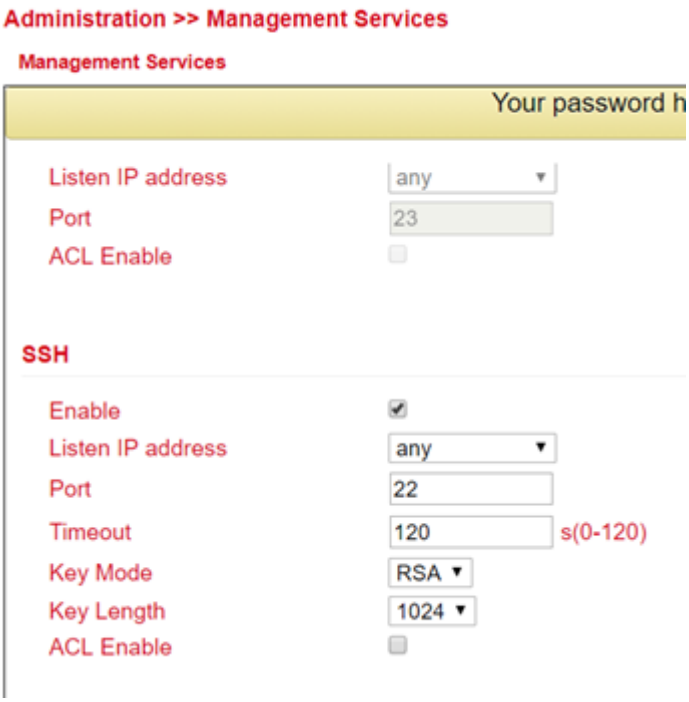


Parameter	Beschreibung
Protocol	TCP oder UDP
Outside Interface	Das Interface, von dem aus zugegriffen werden soll
Service Port	Der Port, der nach außen hin geöffnet ist
Internal Address	Die interne IP-Adresse, die erreicht werden soll
Internal Port	Der interne Port der erreicht werden soll
Description	Kurze Beschreibung
Wenn als Outside Interface Cellular 1 gewählt ist, so funktioniert das Port Mapping nur dann, wenn das Mobilfunkinterface eine öffentliche IP-Adresse erhält!	

3.13 3.12. CLI Befehle

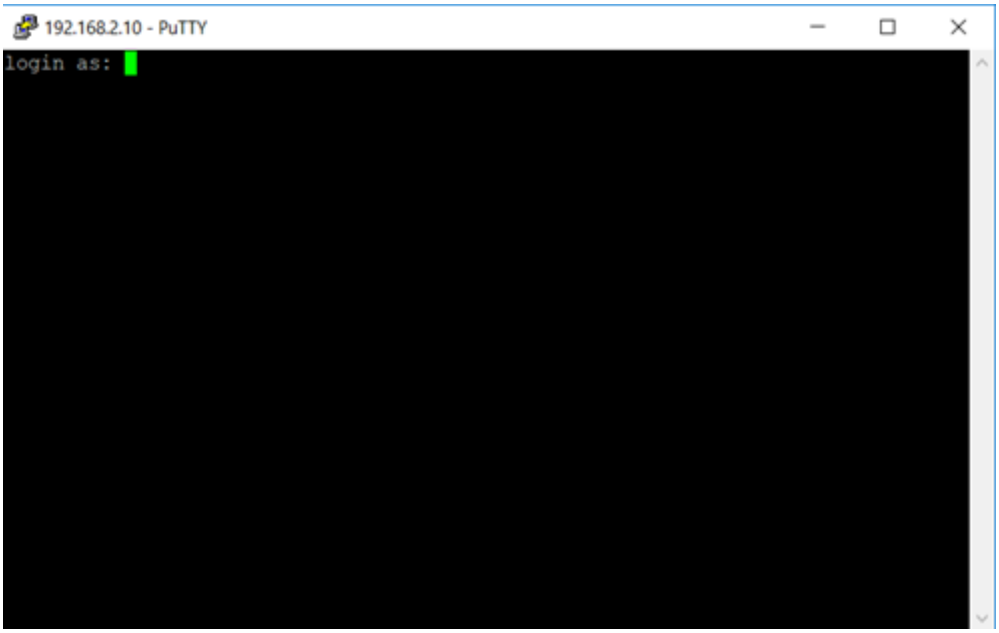
Neben dem Web-Interface, das man über die IP-Adresse des Routers aufrufen kann, besteht auch die Möglichkeit den Router über das CLI (Command Line Interface) zu konfigurieren und managen. Dazu gibt es mehrere Möglichkeiten sich mit dem Router über das CLI zu verbinden. Als Tool dafür hat sich z.B. putty bewährt.

Eine Möglichkeit sich über das CLI zu verbinden ist über SSH. Dazu muß diese Funktion im Router aber erst aktiviert werden. Dies geschieht über Administration > Management Services. Hier muß unter SSH der Haken bei enable gesetzt werden. Die zweite Möglichkeit sich mit dem Router zu Verbinden ist über Telnet in Verbindung mit einem seriellen Konsolenkabel. Dazu muß Telnet, wie bei SSH auch, unter Administration > Management Services aktiviert werden und das Konsolenkabel an dem mit Console bezeichneten Anschluß des Routers mit einem Computer verbunden sein. Die Änderungen bitte mit Apply&Save speichern.

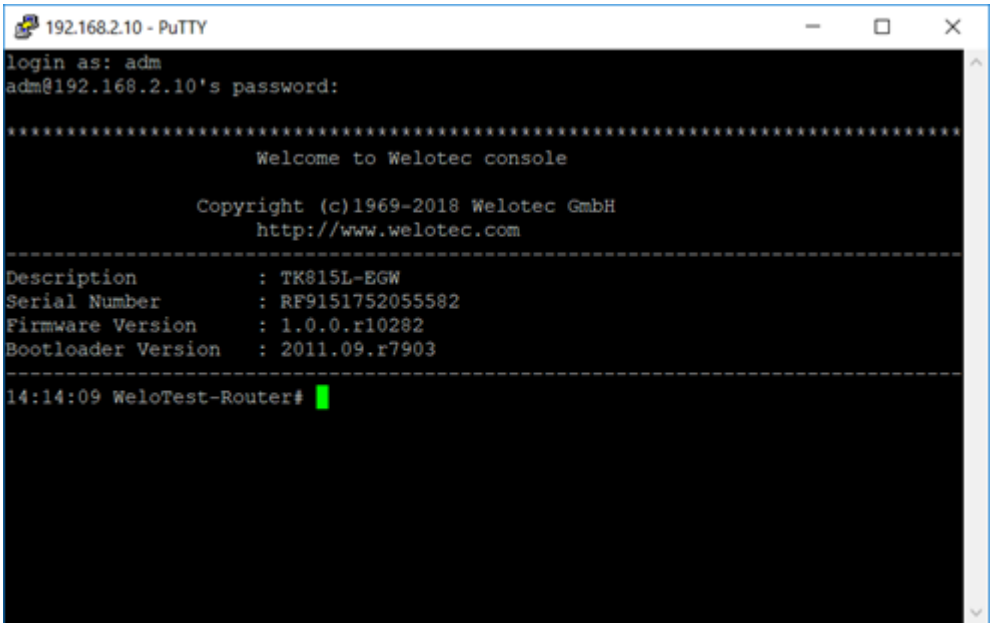


Danach starten Sie z.B. putty und tragen dort die IP-Adresse Ihres Routers ein und wählen SSH oder TELNET als Port bzw. Connection type aus. Klicken Sie dann auf open um die Verbindung zum Router aufzubauen. Ist der

Verbindungsaufbau erfolgreich, erhalten Sie das CLI-Fenster mit der Anmeldung für den Router.



Melden Sie sich hier mit den Anmeldedaten Ihres Routers an (Standard user ist adm und Standard Kennwort ist 123456). Haben Sie sich erfolgreich angemeldet, erhalten Sie den folgenden Screen.

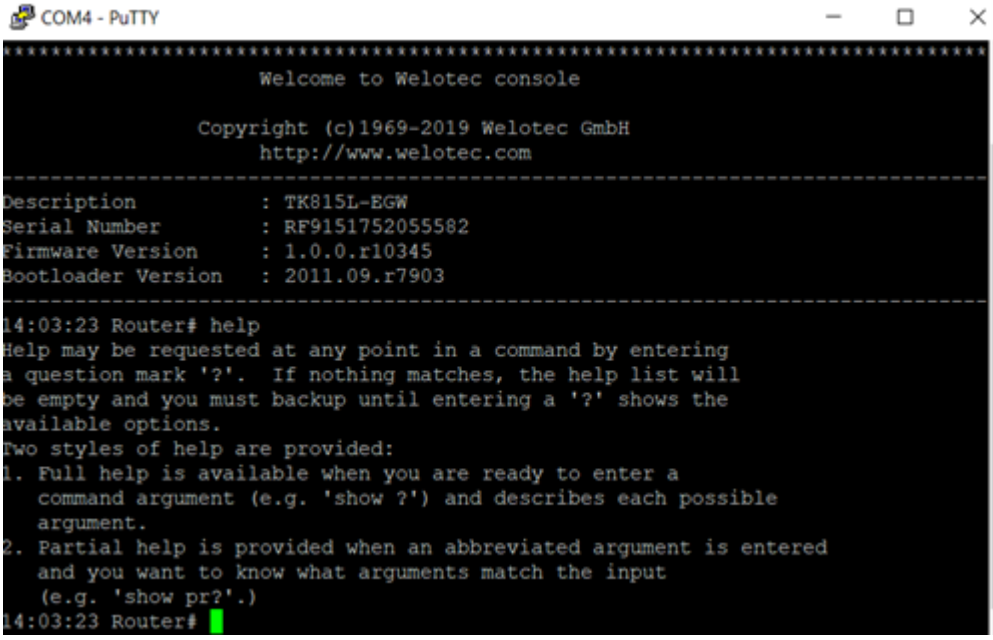


Ab hier können Sie die nachfolgenden Kommandos zur Hilfe, Analyse, Konfiguration usw. verwenden.

Eine weitere Möglichkeit sich mit dem Router über das CLI zu verbinden ist über ein serielles Konsolenkabel. Dies wird auf den Konsolenport des Routers gesteckt und mit dem PC verbunden.

3.13.1 3.12.1. Help Command

Die Hilfe kann nach Eingabe von help oder „?“ in die Konsole abgerufen werden, „?“ kann während der Befehlseingabe jederzeit eingegeben werden, um den aktuellen Befehl oder die Hilfe aus den Befehlsparametern zu erhalten, und der Befehl oder die Parameter können automatisch ergänzt werden, wenn nur der Befehl oder der Befehlsparameter vorhanden ist.



Die Eingabe von help an der Eingabe-Aufforderung gibt eine Kurzbeschreibung der Verwendung des Help-Befehls aus. Hängt man an einen Befehl das „?“ werden einem die Möglichkeiten angezeigt, die man im Zusammen hang mit dem Befehl nutzen kann. Gibt es keine Ausgabe, existiert kein oder kein weiterer Befehl zu dieser Eingabe.

3.13.2 3.12.2. Show Command

Mit dem show Befehl lassen sich Parameter des Routers oder der Konfiguration des Routers anzeigen. Der help-Befehl oder das „?“ zeigen die Befehle an, die man im Zusammenhang mit show nutzen kann.

```
14:33:33 Router# show
  access-list        Show access lists
  alarm              Show alarm information
  arp                Show ARP table
  backup             Show backup information
  bridge             The config of bridge
  cellular           Show cellular information
  channel-group      Port channel group
  clock              Show system time
  crypto             Show crypto module
  cert-info          con.cert_show_info
  data-usage         Show Data usage
  debugging
  dot11              Dot11 configuration
  dot1x              IEEE 802.1x
  fastethernet       Fastethernet interface
  gps                Show the position of gps fix
  tcpclient-gps      Show the IP address of tcp client peer
  interface          Interface
  io                 Show io information
  ip                 Global IP configuration
  log                Show system log
  l2tps-status
  mac                MAC address setting
  mibs               show snmp mib files
  monitor            Port monitoring
  mqtt               Show Device Network Connection Status
  openvpn            Show Openvpn brief information
  obd                Show OBDII status
  python             Show python files
  port-security      Port security
  qos                Quality of service
  running-config     Current operating configuration
  serial
  sla                Show SLA information
  snmp-server        Show SNMP running configuration
  spanning-tree      Show spanning tree protocol configuration
  startup-config     Show startup system configuration
  system             Show system status
  track              Show track information
  traffic-stated     Set Traffic statistic
  traffic            Traffic control
  users              Show user info
  version            Show system version
  vlan               Vlan
  vrrp               Show VRRP status information
14:33:34 Router# show
```

show version zum Beispiel zeigt Ihnen Daten zum Router, wie die Beschreibung, Serien-Nummer, Firmware- und Bootloader-Version.

```
14:44:19 Router> show version
Description            : TK815L-EGW
Serial Number          : RF91517520555582
Firmware Version       : 1.0.0.r10345
Bootloader Version     : 2011.09.r7903
14:44:20 Router>
```

3.13.3 3.12.3. Ping Command

Mit dem Ping-Befehl lässt sich prüfen, ob der Router eine Verbindung ins Internet hat. Die Eingabeform ist, wie bei Windows üblich, **Ping Hostname** oder **IP-Adresse.**

```
14:50:41 Router> ping 8.8.4.4
PING 8.8.4.4 (8.8.4.4): 32 data bytes
40 bytes from 8.8.4.4: seq=0 ttl=117 time=176.387 ms
40 bytes from 8.8.4.4: seq=1 ttl=117 time=31.315 ms
40 bytes from 8.8.4.4: seq=2 ttl=117 time=21.189 ms
40 bytes from 8.8.4.4: seq=3 ttl=117 time=30.354 ms

--- 8.8.4.4 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 21.189/64.811/176.387 ms
14:50:54 Router> ping google.de
PING google.de (172.217.18.163): 32 data bytes
40 bytes from 172.217.18.163: seq=0 ttl=51 time=19.719 ms
40 bytes from 172.217.18.163: seq=1 ttl=51 time=28.166 ms
40 bytes from 172.217.18.163: seq=2 ttl=51 time=21.849 ms
40 bytes from 172.217.18.163: seq=3 ttl=51 time=21.409 ms

--- google.de ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 19.719/22.785/28.166 ms
14:50:58 Router>
```

3.13.4 3.12.4. Traceroute Command

Mit Traceroute testen Sie das aktive Routing des angegebenen Ziels. Mit **traceroute hostname** oder **IP-Adresse** starten Sie die Abfrage.

```
15:14:59 Router# traceroute
  <domain-name/ip>
                  Host name or ip address
15:15:10 Router# traceroute www.google.de
traceroute to www.google.de (108.177.119.94), 5 hops max, 38 byte packets
 1  *  *  *
 2  *  *  *
 3  *  *  *
 4  *  *  *
 5  *  *  *


15:15:57 Router#
```

3.13.5 3.12.5. Reboot Command

Um den Router neu zu starten, können Sie den reboot Befehl nutzen. Geben Sie diesen im CLI ein und der Router wird neu gestartet.

```
11:59:21 Welo-Testrouter# reboot
Are you sure to Reboot system?[Y|N] y
Rebooting system...
The system is going down NOW!
Sent SIGTERM to all processes
Sent SIGKILL to all processes
Requesting system reboot
[91978.036327] Restarting system.
```

3.13.6 3.12.6. Configuration Command

In der Superuser-Ansicht kann der Router den Befehl configure verwenden, um die Konfigurationsansicht zur Verwaltung umzuschalten. Ein Einstellbefehl kann no und default unterstützen, wobei no die Einstellung des Abbruchs eines Parameters und default die Wiederherstellung der Standardeinstellung eines Parameters anzeigt. Der Befehl configure terminal (oder kurz conf t) schaltet das System in den Konfigurationsmodus um. In dieser Einstellung kann der Router konfiguriert werden. Um den Konfigurations-Modus zu beenden nutzt man den Befehl exit. Alle eingegebenen Befehle müssen mit dem wr Befehl abgeschlossen werden, damit die Änderungen in den Router übernommen werden.

```
******************************************************************************
                    Welcome to Welotec console

               Copyright (c)1969-2019 Welotec GmbH
                    http://www.welotec.com
------------------------------------------------------------------------------
Description           : TK815L-EGW
Serial Number         : RF9151752055582
Firmware Version      : 1.0.0.r10345
Bootloader Version    : 2011.09.r7903
------------------------------------------------------------------------------
16:14:49 Router# conf t
16:14:49 Router(config)#
```

3.12.6.1 Hostname Command

Im Konfigurationsmodus kann nun z.B. der Router-Name geändert werden. Dies geht mit dem Befehl hostname Name-des-Routers. Dieser Befehl setzt den Router-Namen auf den von Ihnen eingegebenen Namen um. Wenn Sie den Standardnamen des Routers zurücksetzen wollen, nutzen Sie den Befehl default hostname. Dies setzt den Routernamen auf den Standardnamen Router zurück.

```
16:18:04 Router(config)# hostname
  <routername>       Set host name
16:18:21 Router(config)# hostname Welo-Testrouter

16:18:22 Welo-Testrouter(config)#
```

3.12.6.2 Clock set Command

Mit dem clock set Befehl können Sie das Systemdatum und die -Uhrzeit des Routers über die CLI konfigurieren. Das Fomat für Datum und Uhrzeit lautet dabei, wie folgt:

YYYY.MM.DD-HH:MM:SS

Vollständig würde der Befehl dann z.B. so aussehen

clock set 2019.01.24-12:00:00

```
10:59:21 Welo-Testrouter(config)# clock set 2019.01.24-12:00:00

12:00:00 Welo-Testrouter(config)#
```

Device Time	2019-01-24 12:00:10	
PC Time	2019-01-24 11:21:03	Sync Time

3.12.6.3 Enable password Command

Es ist jederzeit möglich über das CLI das Kennwort des Super Users (adm) zu ändern. Dies können Sie mit dem enable password Befehl tun. Die Eingabeform lautet hierfür

Enable password *password*

```
13:49:41 Router(config)# enable password
  level              Change enable password
  <password>         Enable password
13:49:51 Router(config)# enable password 123456

13:49:55 Router(config)# wr

13:49:56 Router(config)#
```

3.12.6.3 Username Command

Mit dem Befehl Username können Sie Benutzer für den Zugriff auf den Router anlegen. Die Syntax für die Eingabe lautet

Username *[Name des Users]*

```
13:54:35 Router(config)# username Mustermann
New password :
Confirm password :

13:54:46 Router(config)# wr

13:54:47 Router(config)#
```

Bei der Anlage des Benutzers werden Sie nach einem neuen Kennwort gefragt, dass Sie hier vergeben können. Der Benutzer, der angelegt wird, ist immer ein Standard-Benutzer.

Administration >> User Management

User Management

User Summary

Username	Privilege
adm	15(Administrator)
Mustermann	1

Delete

4 4. Technische Daten

4.1 Geräteeigenschaften

Eigenschaft	Wert
Abmessungen (B x H x T)	45 x 132,6 x 112,8 mm
Betriebsspannung	230 V AC auf 12 V – 48V DC
Leistungsaufnahme Standby	3,8 W
Leistungsaufnahme Aktiv	5,3 W
Zulassung	CE-konform

4.2 Umgebungsbedingungen

Eigenschaft	Wert
Einsatztemperaturbereich	-25 bis + 70 °C
Lagertemperaturbereich	-40 bis +85 °C
Luftfeuchtigkeit	5 - 95 %, nicht kondensierend
Erschütterungen	IEC 60068-2-27
Freier Fall	IEC 60068-2-32
Vibration	IEC 60068-2-6

4.3 Funkfrequenzen LTE Europa

Freque	Frequenzbereich und Sendeleistung	Router
Band 1	Frequenzbereich Down: 2110 MHz – 2170 MHz Frequenzbereich Up: 1920 MHz – 1980 MHz Max. Sendeleistung:199 mW	TK812L, TK815L-EX0, TK815L-EXW, TK815L-EGW
Band 3	Frequenzbereich Down: 1805 MHz – 1880 MHz Frequenzbereich Up: 1710 MHz – 1785 MHz Max. Sendeleistung:199 mW	TK812L, TK815L-EX0, TK815L-EXW, TK815L-EGW
Band 7	Frequenzbereich Down: 2620 MHz – 2690 MHz Frequenzbereich Up: 2500 MHz – 2570 MHz Max. Sendeleistung:199 mW	TK812L, TK815L-EX0, TK815L-EXW, TK815L-EGW
Band 8	Frequenzbereich Down: 925 MHz – 960 MHz Frequenzbereich Up: 880 MHz – 915 MHz Max. Sendeleistung:199 mW	TK812L, TK815L-EX0, TK815L-EXW, TK815L-EGW
Band 20	Frequenzbereich Down: 791 MHz – 821 MHz Frequenzbereich Up: 832 MHz – 862 MHz Max. Sendeleistung: 199 mW	TK812L, TK815L-EX0, TK815L-EXW, TK815L-EGW

4.4 Funkfrequenzen UMTS Europa

Freque	Frequenzbereich und Sendeleistung	Router
Band 1	Frequenzbereich Down: 2110 MHz – 2170 MHz Frequenzbereich Up: 1920 MHz – 1980 MHz Max. Sendeleistung: 251 mW	TK802U, TK812L, TK815L-EX0, TK815L-EXW, TK815L-EGW
Band 3	Frequenzbereich Down: 1805 MHz – 1880 MHz Frequenzbereich Up: 1710 MHz – 1785 MHz Max. Sendeleistung:251 mW	TK802U, TK812L, TK815L-EX0, TK815L-EXW, TK815L-EGW
Band 8	Frequenzbereich Down: 925 MHz – 960 MHz Frequenzbereich Up: 880 MHz – 915 MHz Max. Sendeleistung:251 mW	TK802U, TK812L, TK815L-EX0, TK815L-EXW, TK815L-EGW

4.5 Funkfrequenzen GSM Europa

Freque	Frequenzbereich und Sendeleistung	Router
GSM 900	Frequenzbereich Down: 925 MHz – 960 MHz Frequenzbereich Up: 880 MHz – 915 MHz Max. Sendeleistung: 1995 mW	TK802U, TK812L, TK815L-EX0, TK815L-EXW, TK815L-EGW
GSM 1800	Frequenzbereich Down: 1805 MHz – 1880 MHz Frequenzbereich Up: 1710 MHz – 1785 MHz Max. Sendeleistung: 1000 mW	TK802U, TK812L, TK815L-EX0, TK815L-EXW, TK815L-EGW

4.6 Funkfrequenzen LTE Asien

Frequenz	Frequenzbereich und Sendeleistung	Router
Band 1	Frequenzbereich Down: 1920 MHz – 1980 MHz Frequenzbereich Up: 2110 MHz – 2170 MHz Max. Sendeleistung: 200 mW	TK822L, TK825L-EXW, TK825L-EX0
Band 2	Frequenzbereich Down: 1930 MHz – 1990 MHz Frequenzbereich Up: 1850 MHz – 1910 MHz Max. Sendeleistung: 200 mW	TK822L, TK825L-EXW, TK825L-EX0
Band 3	Frequenzbereich Down: 1805 MHz – 1880 MHz Frequenzbereich Up: 1710 MHz – 1785 MHz Max. Sendeleistung: 200 mW	TK822L, TK825L-EXW, TK825L-EX0
Band 5	Frequenzbereich Down: 869 MHz – 894 MHz Frequenzbereich Up: 824 MHz – 849 MHz Max. Sendeleistung: 200 mW	TK822L, TK825L-EXW, TK825L-EX0
Band 7	Frequenzbereich Down: 2620 MHz – 2690 MHz Frequenzbereich Up: 2500 MHz – 2570 MHz Max. Sendeleistung: 200 mW	TK822L, TK825L-EXW, TK825L-EX0
Band 38 China	Frequenzbereich Down: 2570 MHz – 2620 MHz Frequenzbereich Up: n.b. Max. Sendeleistung: 200 mW	TK822L, TK825L-EXW, TK825L-EX0
Band 39 China	Frequenzbereich Down: 1880 MHz – 1920 MHz Frequenzbereich Up: n.b. Max. Sendeleistung: 200 mW	TK822L, TK825L-EXW, TK825L-EX0
Band 40 China	Frequenzbereich Down: 2300 MHz – 2400 MHz Frequenzbereich Up: n.b. Max. Sendeleistung: 200 mW	TK822L, TK825L-EXW, TK825L-EX0
Band 41 China	Frequenzbereich Down: 2496 MHz – 2690 MHz Frequenzbereich Up: n.b. Max. Sendeleistung: 200 mW	TK822L, TK825L-EXW, TK825L-EX0

4.7 Funkfrequenzen UMTS Asien

Frequer	Frequenzbereich und Sendeleistung	Router
Band 1	Frequenzbereich Down: 2110MHz – 2170 MHz Frequenzbereich Up: 1920 MHz – 1980 MHz Max. Sendeleistung: 251 mW	TK822L, TK825L-EXW, TK825L-EX0
Band 5	Frequenzbereich Down: 869 MHz – 894 MHz Frequenzbereich Up: 824 MHz – 849 MHz Max. Sendeleistung: 251 mW	TK822L, TK825L-EXW, TK825L-EX0
Band 8	Frequenzbereich Down: 925 MHz – 960 MHz Frequenzbereich Up: 880 MHz – 915 MHz Max. Sendeleistung: 251 mW	TK822L, TK825L-EXW, TK825L-EX0

4.8 Funkfrequenzen GSM Asien

Frequer	Frequenzbereich und Sendeleistung	Router
GSM 900	Frequenzbereich Down: 925 MHz – 960 MHz Frequenzbereich Up: 880 MHz – 915 MHz Max. Sendeleistung: 1995 mW	TK822L, TK825L-EXW, TK825L-EX0
GSM 1800	Frequenzbereich Down: 1805 MHz – 1880 MHz Frequenzbereich Up: 1710 MHz – 1785 MHz Max. Sendeleistung: 1000 mW	TK822L, TK825L-EXW, TK825L-EX0

4.9 Funkfrequenzen LTE USA

Freque	Frequenzbereich und Sendeleistung	Router
Band 2	Frequenzbereich Down: 1930 MHz – 1990 MHz Frequenzbereich Up: 1850 MHz – 1910 MHz Max. Sendeleistung: 200mW	TK832L, TK835L-EXW, TK835L-EX0, TK842L, TK845L-EXW, TK845L-EX0
Band 4	Frequenzbereich Down: 2110 MHz – 2155 MHz Frequenzbereich Up: 1710 MHz – 1755 MHz Max. Sendeleistung: 200mW	TK832L, TK835L-EXW, TK835L-EX0, TK842L, TK845L-EXW, TK845L-EX0
Band 5	Frequenzbereich Down: 869 MHz – 894 MHz Frequenzbereich Up: 824 MHz – 849 MHz Max. Sendeleistung: 200mW	TK832L, TK835L-EXW, TK835L-EX0, TK842L, TK845L-EXW, TK845L-EX0
Band 17	Frequenzbereich Down: 734 MHz – 746 MHz Frequenzbereich Up: 788 MHz – 798 MHz Max. Sendeleistung: 200mW	TK832L, TK835L-EXW, TK835L-EX0, TK842L, TK845L-EXW, TK845L-EX0

4.10 Funkfrequenzen UMTS USA

Freque	Frequenzbereich und Sendeleistung	Router
Band 2	Frequenzbereich Down: 1930 MHz – 1990 MHz Frequenzbereich Up: 1850 MHz – 1910 MHz Max. Sendeleistung: 251 mW	TK832L, TK835L-EXW, TK835L-EX0, TK842L, TK845L-EXW, TK845L-EX0
Band 4	Frequenzbereich Down: 2110 MHz – 2155 MHz Frequenzbereich Up: 1710 MHz – 1755 MHz Max. Sendeleistung: 251 mW	TK832L, TK835L-EXW, TK835L-EX0, TK842L, TK845L-EXW, TK845L-EX0
Band 5	Frequenzbereich Down: 869 MHz – 894 MHz Frequenzbereich Up: 824 MHz – 849 MHz Max. Sendeleistung: 251 mW	TK832L, TK835L-EXW, TK835L-EX0, TK842L, TK845L-EXW, TK845L-EX0

4.11 Funkfrequenzen GSM USA

Freque	Frequenzbereich und Sendeleistung	Router
GSM 850	Frequenzbereich Down: 869 MHz – 894 MHz Frequenzbereich Up: 824 MHz – 849 MHz Max. Sendeleistung: 1995 mW	TK832L, TK835L-EXW, TK835L-EX0, TK842L, TK845L-EXW, TK845L-EX0
GSM 1900	Frequenzbereich Down: 1930 MHz – 1990 MHz Frequenzbereich Up: 1850 MHz – 1910 MHz Max. Sendeleistung: 1000 mW	TK832L, TK835L-EXW, TK835L-EX0, TK842L, TK845L-EXW, TK845L-EX0

4.12 Funkfrequenzen LTE für weitere Länder weltweit

Frequer	Frequenzbereich und Sendeleistung	Router
Band 1	Frequenzbereich Down: 2110 MHz – 2170 MHz Frequenzbereich Up: 1920 MHz – 1980 MHz Max. Sendeleistung:199 mW	TK882L, TK885L-EX0, TK885L-EXW
Band 3	Frequenzbereich Down: 1805 MHz – 1880 MHz Frequenzbereich Up: 1710 MHz – 1785 MHz Max. Sendeleistung:199 mW	TK882L, TK885L-EX0, TK885L-EXW
Band 5	Frequenzbereich Down: 869 MHz – 894 MHz Frequenzbereich Up: 824 MHz – 849 MHz Max. Sendeleistung:199 mW	TK882L, TK885L-EX0, TK885L-EXW
Band 7	Frequenzbereich Down: 2620 MHz – 2690 MHz Frequenzbereich Up: 2500 MHz – 2570 MHz Max. Sendeleistung:199 mW	TK882L, TK885L-EX0, TK885L-EXW
Band 8	Frequenzbereich Down: 925 MHz – 960 MHz Frequenzbereich Up: 880 MHz – 915 MHz Max. Sendeleistung:199 mW	TK882L, TK885L-EX0, TK885L-EXW
Band 20	Frequenzbereich Down: 791 MHz – 821 MHz Frequenzbereich Up: 832 MHz – 862 MHz Max. Sendeleistung: 199 mW	TK882L, TK885L-EX0, TK885L-EXW

4.13 Funkfrequenzen UMTS für weitere Länder weltweit

Frequer	Frequenzbereich und Sendeleistung	Router
Band 2	Frequenzbereich Down: 1930 MHz – 1990 MHz Frequenzbereich Up: 1850 MHz – 1910 MHz Max. Sendeleistung: 251 mW	TK882L, TK885L-EX0, TK885L-EXW
Band 4	Frequenzbereich Down: 2110 MHz – 2155 MHz Frequenzbereich Up: 1710 MHz – 1755 MHz Max. Sendeleistung:251 mW	TK882L, TK885L-EX0, TK885L-EXW
Band 5	Frequenzbereich Down: 869 MHz – 894 MHz Frequenzbereich Up: 824 MHz – 894 MHz Max. Sendeleistung:251 mW	TK882L, TK885L-EX0, TK885L-EXW

4.14 Funkfrequenzen GSM für weitere Länder weltweit

Frequer	Frequenzbereich und Sendeleistung	Router
GSM 900	Frequenzbereich Down: 925 MHz – 960 MHz Frequenzbereich Up: 880 MHz – 915 MHz Max. Sendeleistung: 1995 mW	TK882L, TK885L-EX0, TK885L-EXW
GSM 1800	Frequenzbereich Down: 1805 MHz – 1880 MHz Frequenzbereich Up: 1710 MHz – 1785 MHz Max. Sendeleistung: 1000 mW	TK882L, TK885L-EX0, TK885L-EXW

4.15 Funkfrequenzen WLAN

Frequer	Frequenzbereich und Sendeleistung	Router
2,4 GHz	Frequenzbereich: 2400 MHz – 2483,5 MHz Max. Sendeleistung: 40 mW	TK805-EXW, TK815L-EXW, TK815L-EGW , TK825L-EXW, TK835L-EXW, TK845L-EXW

5 5. CE Deklaration

CE declaration of conformity

welotec
a byte smarter

The manufacturer:
Welotec GmbH
Zum Hagenbach 7
48366 Laer
GERMANY

herewith declares that the products:

Product:
Wireless Router

Identification:
TK802U, TK812L, TK815L-EX0, TK815L-EXW, TK815L-EGW, TK862L, TK865L-EX0, TK865L-EXW, TK865L-EGW, TK872L, TK875L-EX0, TK875L-EXW, TK875L-EGW, TK892L, TK885L-EX0, TK885L-EXW, TK885L-EGW, TK805W-EX0, TK805W-EXW

Complies with:

- Radio Equipment Directive 2014/53/EU,
  - ETSI EN 301 489-1 V2.1.1 (2017-02)
  - ETSI EN 301 489-3 V2.1.1 (2017-03)
  - ETSI EN 301 489-17 V3.2.0 (2017-03)
  - ETSI EN 301 489-52 V1.1.0 (2016-11)
  - ETSI EN 301 511 V12.5.1 (2017-03)
  - ETSI EN 300 328 V2.1.1 (2016-11)
  - ETSI EN 300 440 V2.1.1 (2017-03)
  - ETSI EN 301 908-1 V11.1.1 (2016-07)
  - ETSI EN 301 908-2 V11.1.1 (2016-07)
  - ETSI EN 301 908-13 V11.1.1 (2016-07)
  - EN 62311:2008
  - EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013
  - EN 55032:2012
  - EN 55024:2010
  - EN 61000-3-2:2014
  - EN 61000-3-3:2013
- RoHS 2 Compliant Directive 2011/65/EU

CE

The corresponding markings appear under the appliance.

This devices are designed for use in all countries of the European Union and in Switzerland, Norway, Lichtenstein and Iceland.

15.07.2017
Date

Jos Zenner

Welotec GmbH
Zum Hagenbach 7
D-48366 Laer
Fon: +49(0)2554 9130 00
E-mail: info@welotec.com

6 TK800-Serie - FAQ: IPsec

6.1 Vorwort

IPsec ist eine Erweiterung des Internet-Protokolls (IP) um Verschlüsselungs- und Authentifizierungsmechanismen. Damit erhält das Internet-Protokoll die Fähigkeit IP-Pakete kryptografisch gesichert über öffentliche und unsichere Netze zu transportieren. IPsec wurde von der Internet Engineering Task Force (IETF) als integraler Bestandteil von IPv6 entwickelt. Weil das Internet-Protokoll der Version 4 ursprünglich keine Sicherheitsmechanismen hatte, wurde IPsec für IPv4 nachträglich spezifiziert.

6.1.1 *Bestandteile von IPsec-VPNs*

- Interoperabilität
- kryptografischer Schutz der übertragenen Daten
- Zugangskontrolle
- Datenintegrität
- Authentisierung des Absenders (Benutzerauthentisierung)
- Verschlüsselung
- Authentifizierung von Schlüsseln
- Verwaltung von Schlüsseln (Schlüsselmanagement)

Hinter diesen Bestandteilen stehen Verfahren, die miteinander kombiniert eine zuverlässige Sicherheit für die Datenübertragung über öffentliche Netze bieten. VPN-Sicherheitslösungen mit hohen Sicherheitsanforderungen setzen daher generell auf IPsec.

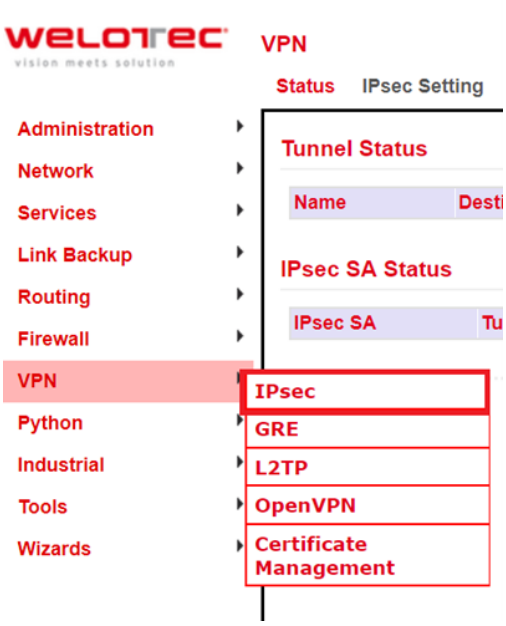
6.1.2 *Einsatz-Szenarien*

- Subnet-to-Subnet-VPN
- Host-to-Subnet-VPN
- Host-to-Host-VPN

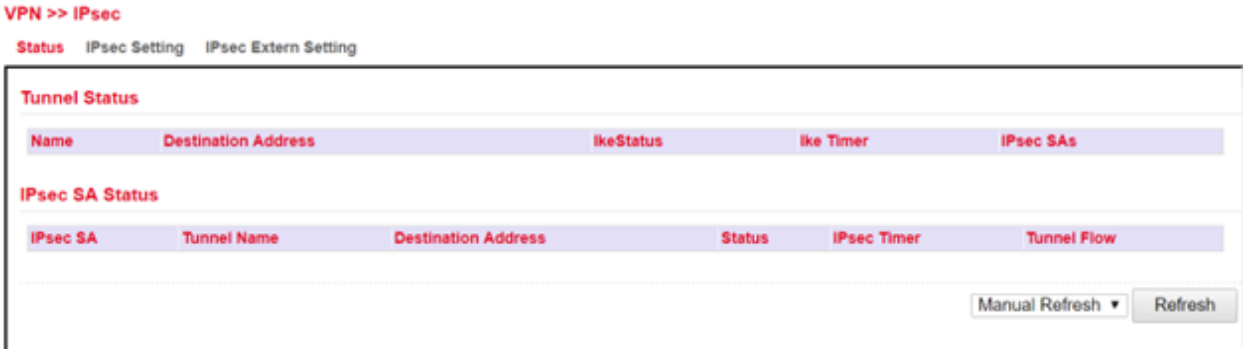
Prinzipiell eignet sich IPsec für Gateway-zu-Gateway-Szenarien. Also die Verbindung zwischen Netzen über ein drittes unsicheres Netz.

6.1.3 IPsec

Unter ***VPN > IPsec*** können Sie zunächst den Status Ihres IPsec Tunnels einsehen, wenn Sie bereits einen angelegt haben.

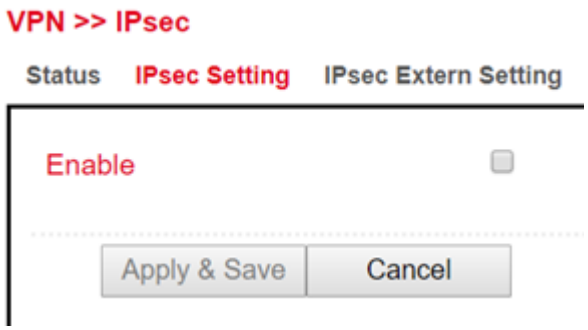


Von hier aus stehen Ihnen die Möglichkeiten *„IPsec Setting“* und *„IPsec Extern Setting“* zur Verfügung.

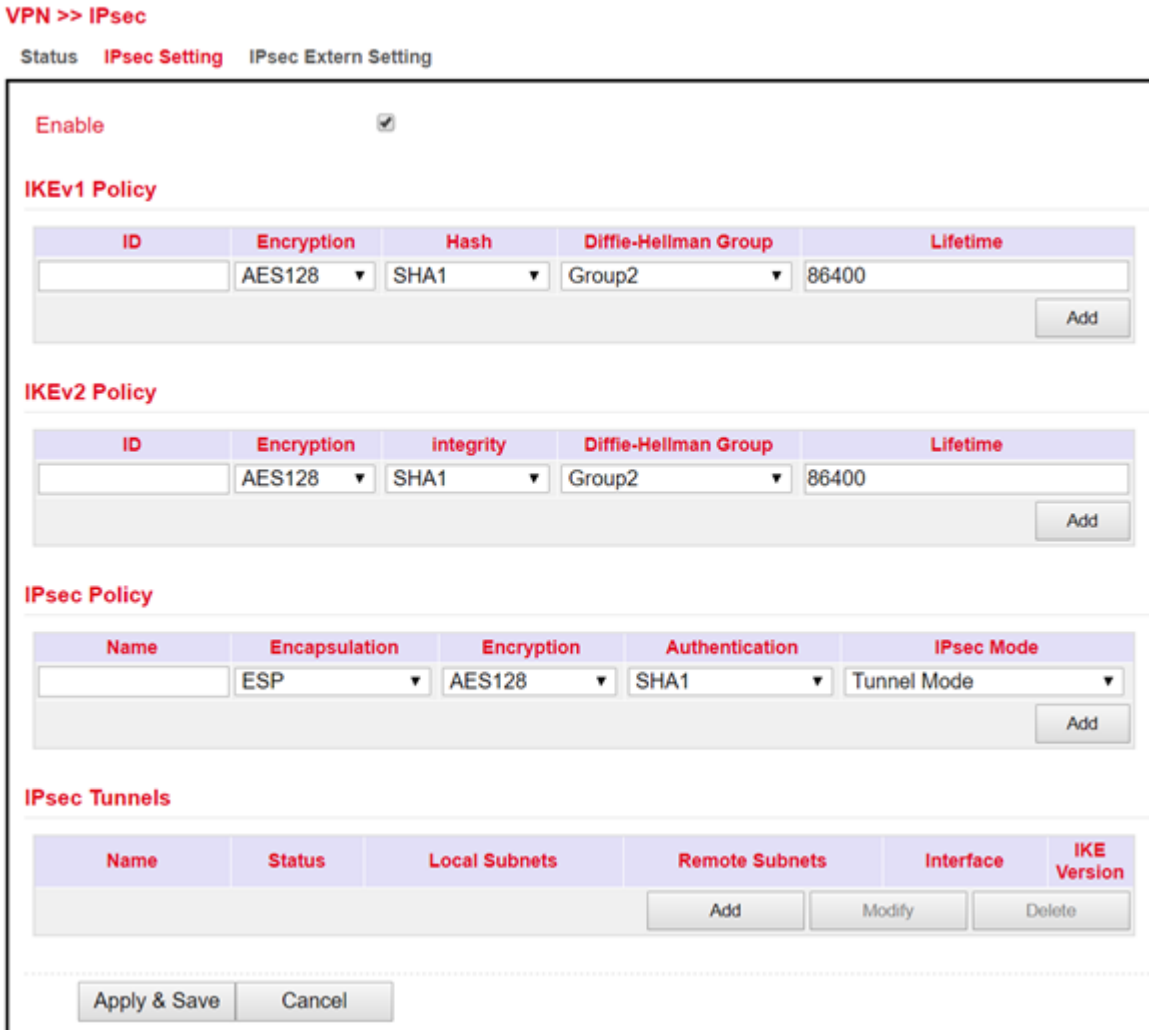


Um einen neuen IPsec Tunnel anzulegen, gehen Sie nun wie folgt vor:

1. Klicken Sie oben auf **„IPsec Setting“**



2. Klicken Sie auf **„Enable“**



Nun können Sie mit der Konfiguration beginnen. Gehen Sie dabei wie folgt vor:

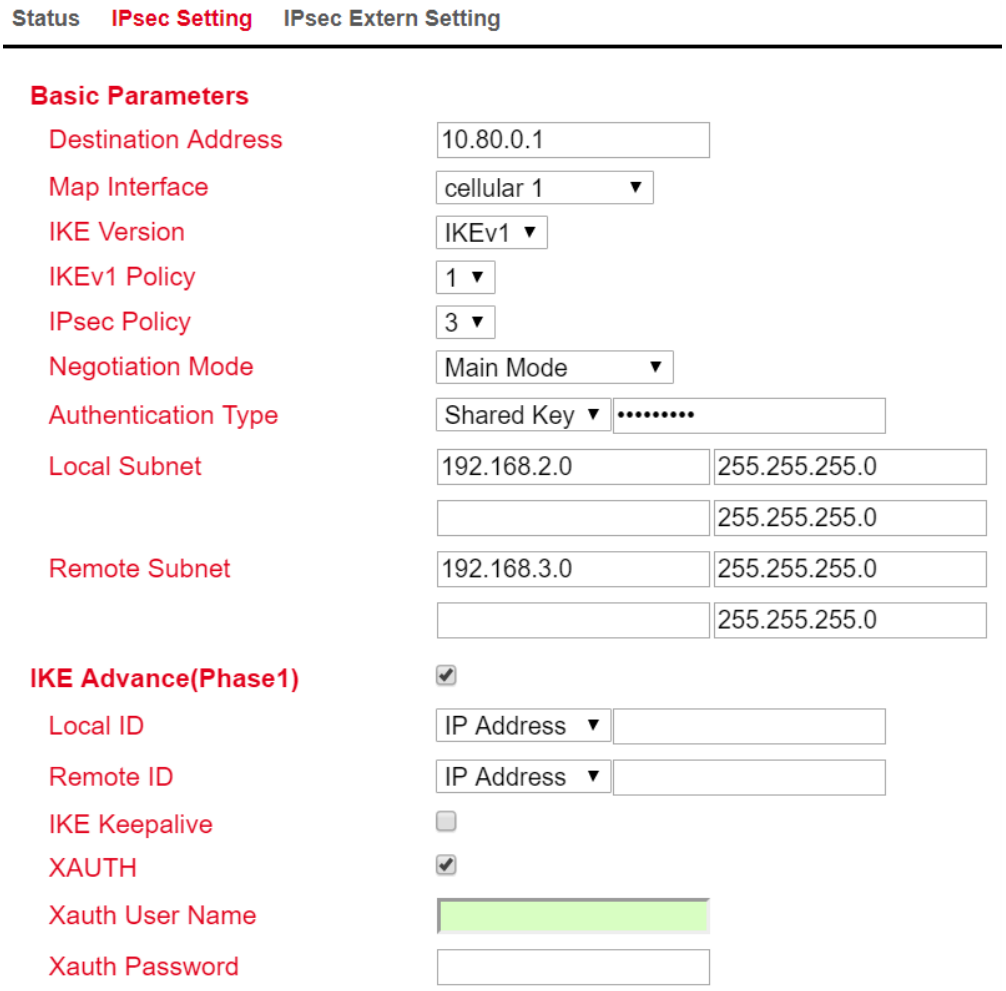
1. *IKEv1 und IKEv2 Policy:*
   - Hinzufügen Ihrer Einstellungen werden mit dem „Add“-Button bestätigt.
   - ID dient der Identifizierung der Policy in der Tunnel-Konfiguration und kann frei gewählt werden. Das Feld ist ein Ganzzahlfeld.
   - Encryption enthält eine Auswahlliste an Verschlüsselungsmethoden, wie z.B. AES256.
   - Hash beinhaltet den Hashalgorithmus, wie z.B. SHA1 oder SHA2-256.
   - Diffie-Hellman Group bietet die Möglichkeit die Schlüsselstärke während des Schlüsselaustausch-Prozesses zu wählen. Je höher die Gruppe, desto höher die Verschlüsselung, z.B. Group2 = 1024 Bit.
   - Lifetime ist die Gültigkeitsdauer der IKE, bevor sie neu ausgehandelt wird.
2. *IPsec Policy:*
   - Der Name dient der Identifizierung der Policy in der Tunnel-Konfiguration und kann frei gewählt werden.
   - Encapsulating Security Payload (***ESP***) sorgt innerhalb von IPsec für die Authentisierung, Integrität und Vertraulichkeit der IP-Pakete. Im Unterschied zu Authentication Header (***AH***) werden die Nutzdaten verschlüsselt übertragen. Während AH „nur die Integrität und Echtheit“ der Daten sicherstellen kann, erhöht ESP die Datensicherheit in Abhängigkeit des gewählten Verschlüsselungsalgorithmus. Deshalb wird in der Regel ESP und nicht AH verwendet. ESP sorgt für die Vertraulichkeit der Kommunikation. Die

Pakete werden verschlüsselt. Zusätzlich schützt eine Integritätssicherung vor Manipulation. Wählen Sie bei **„Encapsulation“** das entsprechende Protokoll aus.

- Tragen Sie die Verschlüsselung (Encryption) im gleichnamigen Feld ein. Der **Advanced Encryption Standard** (**AES**) ist der Nachfolgeverschlüsse-lungsstandard von **DES** (Data Encryption System). **3DES** mit 128 Bit gilt zwar immer noch als sicher, ist aber wegen der Dreifachverschlüsselung um Faktoren langsamer als AES. AES unterstützt 128, 192 und 256 Bit lange Schlüssel.
- Die ***Authentication*** dient der Authentifizierung und kann mit MD5, SHA1 und SHA2 gewählt werden.
- Zusätzlich zur Wahl zwischen AH und ESP haben Sie die Möglichkeit, die Pakete im Transport- oder Tunnel-Mode über das Netz zu verschicken. Beim Transport-Mode wird der Original-IP-Header, also IP-Adresse plus IP-Optionen, weiter benutzt. Im Tunnel-Mode kapselt IPsec das ganze Paket samt IP-Header und schreibt einen neuen IP-Header davor. Die Original-IP-Adresse ist nicht mehr sichtbar. Erst bei der Entschlüsselung auf der gegenüberliegenden Seite wird die IP-Adresse mitsamt dem restlichen Paket wieder sichtbar. Stellen Sie hier den entsprechenden Modus ein.

3. *IPsec Tunnels:*

   Klicken Sie zur Anlage des IPsec Tunnels zunächst auf den „Add“-Button



- *Basic Parameters*

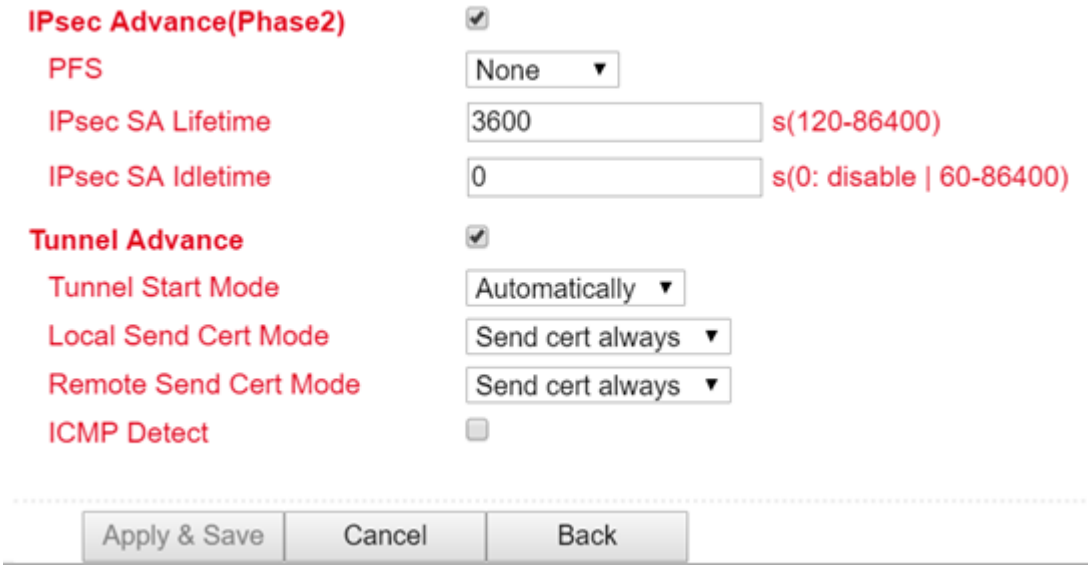
  1. Die **„Destination Address“** ist die IP-Adresse der Tunnel-Gegenstelle. Tragen Sie hier die entsprechende IP-Adresse ein.
  2. Bei **„Map Interface“** tragen Sie bitte das Interface ein, über das die Verbindung aufgebaut werden soll.

3. Wählen Sie unter **„IKE Version“** die von Ihnen unter IKEv1 oder IKEv2 erstellte Version aus. Je nach Vorgaben werden die Werte in dem Listenfeld übernommen.
4. Im Feld **„IPsec Policy“** erscheint der zuvor angelegte Name der IPsec Policy.
5. Unter **„Negotiation Mode“** können Sie zwischen zwei Optionen bei der Aushandlung des IPsec Tunnels wählen. Im Main Mode handeln der Initiator (derjenige, der die Verbindung aufnehmen will) und der Antwortende (der Responder) miteinander eine ISAKMP-SA aus. Diese Verhandlung geschieht in mehreren Schritten. Im Aggressive Mode werden die obigen Schritte bis auf drei zusammengefasst, die Hashwerte der Pre-shared Keys im Klartext übertragen. Ein Grund für den Einsatz dieses Modus kann jedoch gegeben sein, wenn die Adresse des Initiators dem Responder nicht von vornherein bekannt ist, und beide Seiten Pre-shared Keys zur Authentifizierung einsetzen wollen. Der Aggressive Mode ist jedoch mit Vorsicht zu verwenden, da in der Praxis oft aus Bequemlichkeit keine starken Schlüssel verwendet werden.
6. Wählen Sie bei *„Authentication Type“* den Typ der Authentifizierung aus. Sie haben hier zwei Möglichkeiten. Einmal über Shared Key, den gemeinsamen Schlüssel zur Authentifizierung (einzugeben im Feld danach) oder über Certificate, d.h. über vorhandene Zertifikate, die dann über **„VPN > Certificate Management“** importiert werden müssen.
7. Tragen Sie unter **„Local Subnet“** das Subnetz des Routers ein. Im ersten Feld die IP-Adresse und im zweiten die Subnetmaske. Sie können bis zu vier Einträge erstellen.
8. Im Bereich **„Remote Subnet“** können Sie dann das Subnetz der Gegenstelle eintragen. Auch hier haben Sie die Möglichkeit bis zu vier Einträge zu erstellen.

- *IKE Advance (Phase 1)*

  Nach Aktivierung stehen Ihnen die folgenden Möglichkeiten zur Verfügung:

  1. Über die **„Local ID“** haben Sie die Möglichkeit aus dem Listenfeld verschiedene Einträge auszuwählen und in dem folgenden Feld dann die entsprechenden Daten einzutragen, z.B. IP Address und dann die gewünschte IP-Adresse in das Folgefeld eintragen.
  2. In das Feld **„Remote ID“** tragen Sie dann die Daten für die Gegenstelle ein.
  3. **„IKE Keepalive“** können Sie ein- oder ausschalten um die IKE Phase eins aufrechtzuerhalten.
  4. Sie können die Verwendung des XAUTH-Protokolls für die VPN-Gegenstelle separat vornehmen, indem Sie diese Funktion bei XAUTH aktivieren. Sie können dann einen entsprechenden Benutzernamen (Xauth User Name) und ein Kennwort (Xauth Password) vorgeben bzw. verwenden.



- *IPsec Advance (Phase 2)*

  Nach Aktivierung stehen Ihnen die folgenden Möglichkeiten zur Auswahl:

1. **Perfect Forward Secrecy(PFS)**, auf Deutsch etwa *perfekte vorwärts gerichtete Geheimhaltung*, ist in der Kryptographie eine Eigenschaft bestimmter Schlüsselaustauschprotokolle. Diese verwenden zuvor ausgetauschte Langzeitschlüssel, um für jede zu verschlüsselnde Sitzung einen neuen geheimen Sitzungsschlüssel zu vereinbaren. Ein Protokoll hat Perfect Forward Secrecy nicht, damit die verwendeten Sitzungsschlüssel nach der Beendigung der Sitzung nicht mehr aus den geheimen Langzeitschlüsseln rekonstruiert werden können. Damit kann eine aufgezeichnete verschlüsselte Kommunikation auch bei Kenntnis des Langzeitschlüssels nicht nachträglich entschlüsselt werden. Hier können Sie zwischen mehreren Gruppen wählen, die mit Diffie Hellman Schlüsseln arbeiten. Group 1 hat z.B eine Verschlüsselung von 768 Bits, Group2 hat 1024 Bits und Group 5 nutzt 1536 Bits usw.
2. Die Gültigkeitsdauer der SA (Security Association) können Sie unter **„IPsec SA Lifetime“** eintragen. Eine Security Association fasst IP-Pakete zusammen, anhand von einem SPI (Security Parameter Index), der IP-Ziel-Adresse und dem Security Protocol Identifier. Eine SA gilt jeweils nur für EINE Richtung, daher werden immer zwei SAs genutzt.
3. Bei **„IPsec SA Idletime“** legen Sie fest, ob SA´s, die mit inaktiven Peers verknüpft sind, gelöscht werden können bevor die globale Lebensdauer abgelaufen ist. Die 0 bedeutet, dass die Funktion deaktiviert ist.

- *Tunnel Advance*

  Nach Aktivieren dieser Funktion, stehen Ihnen folgende Möglichkeiten zur Verfügung:

  1. Stellen Sie bei **„Tunnel Start Mode“** ein, wie der Tunnel gestartet werden soll. Die Standardeinstellung ist immer automatisch.
  2. Im Feld **„Local Send Cert Mode“** legen Sie fest, wann ein Zertifikat für den lokalen Bereich gesendet werden soll. Die Standardeinstellung ist, dass das Zertifikat immer gesendet werden soll (Send cert always).
  3. Bei **„Remote Send Cert Mode“** legen Sie fest, wann ein Zertifikat für den Bereich der Gegenstelle gesendet werden soll. Die Standardeinstellung ist, dass das Zertifikat immer gesendet werden soll (Send cert always).

  image

  4. Mit **„ICMP Detect“** können Sie die Funktion für den ICMP Watchdog aktivieren oder deaktivieren.
  5. Geben Sie bei **„ICMP Detection Server“** die Adresse eines Servers an, der nur durch den Tunnel erreichbar ist.
  6. Bei **„ICMP Detection Local IP“** wird die Router Interface IP des lokalen Subnetzes eingetragen.
  7. Legen Sie bei **„ICMP Detection Interval“** das Intervall fest in dem das ICMP Paket gesendet werden soll.
  8. **„ICMP Detection Timeout“** ist die Zeit nach der das ICMP Pakte verworfen wird. Tragen Sie hier einen Wert von 1 bis 60 Sec. ein.
  9. **„ICMP Detection Max Retries“** sind die maximalen Versuche nach einem fehlgeschlagenen ICMP Ping, die Sie hier eintragen können.

6.1.4 IPsec Status

Wenn der oder die IPsec Tunnel erfolgreich aufgebaut wurden, dann sieht man folgendes in der Status-Übersicht.