# TK800 Serie - Benutzerhandbuch

wireless | m2m-networks | sensors

welotec®

vision meets solution

1. TK800 Manual . . . 3
1.1 Einführung . . . 3
1.2 Quick Start . . . 5
1.3 Web Konfiguration . . . 27
1.3.1 Administration . . . 29
1.3.1.1 System . . . 30
1.3.1.1.1 Status . . . 30
1.3.1.1.2 Basic Setup . . . 31
1.3.1.2 System Time . . . 31
1.3.1.2.1 System Time Konfiguration . . . 32
1.3.1.2.2 SNTP Client . . . 32
1.3.1.2.3 NTP Server . . . 33
1.3.1.3 Admin Access . . . 33
1.3.1.3.1 Create a User . . . 34
1.3.1.3.2 Modify a User . . . 34
1.3.1.3.3 Remove Users . . . 34
1.3.1.3.4 Management Services . . . 35
1.3.1.4 AAA . . . 37
1.3.1.4.1 Radius . . . 37
1.3.1.4.2 Tacacs+ . . . 37
1.3.1.4.3 LDAP . . . 37
1.3.1.4.4 AAA Settings . . . 38
1.3.1.5 Config Management . . . 38
1.3.1.6 Device Management . . . 38
1.3.1.7 SNMP . . . 39
1.3.1.7.1 SNMP Konfiguration . . . 39
1.3.1.7.2 SnmpTrap . . . 40
1.3.1.7.3 SnmpMibs . . . 41
1.3.1.7.4 SNMP Mibs auslesen . . . 41
1.3.1.8 Alarm . . . 42
1.3.1.8.1 Alarm Status . . . 42
1.3.1.8.2 Alarm Input . . . 43
1.3.1.8.3 Alarm Output . . . 44
1.3.1.8.4 Alarm Map . . . 45
1.3.1.9 Log . . . 47
1.3.1.9.1 Show Log . . . 47
1.3.1.9.2 System Log . . . 47
1.3.1.10 Upgrade . . . 48
1.3.1.11 Reboot . . . 48
1.3.2 Layer2 Switch . . . 50
1.3.2.1 Layer2 Switch Status . . . 50
1.3.2.2 Port Basic Parameters . . . 50
1.3.2.3 Port Mirroring . . . 51
1.3.2.4 Broadcast Storm Control . . . 51
1.3.3 Network . . . 53
1.3.3.1 Ethernet . . . 53
1.3.3.1.1 Ethernet Status . . . 53
1.3.3.1.2 Fast Ethernet 0/1 . . . 53
1.3.3.2 VLAN . . . 54
1.3.3.2.1 VLAN Trunk . . . 54
1.3.3.2.2 Configure VLAN Parameters . . . 54
1.3.3.3 Cellular . . . 56
1.3.3.3.1 Cellular Status . . . 56
1.3.3.3.2 Cellular Configuration . . . 56
1.3.3.4 ADSL Dialup (PPPoE) . . . 60
1.3.3.4.1 PPPoE Status . . . 60
1.3.3.4.2 ADSL Dialup (PPPoE) Configuration . . . 61
1.3.3.5 Loopback . . . 61
1.3.3.5.1 Loopback Configuration . . . 61
1.3.3.6 DHCP . . . 62
1.3.3.6.1 DHCP Status . . . 62
1.3.3.6.2 DHCP Server . . . 62
1.3.3.6.3 DHCP Relay . . . 62
1.3.3.6.4 DHCP Client . . . 62
1.3.3.7 DNS . . . 63
1.3.3.7.1 DNS Server . . . 63
1.3.3.7.2 DNS Relay . . . 63
1.3.3.8 DDNS . . . 63
1.3.3.8.1 DDNS Configuration . . . 63
1.3.3.8.2 DDNS Status . . . 63
1.3.3.9 SMS . . . 64
1.3.4 Link Backup . . . 67

1.3.4.1 SLA . . . 73
1.3.4.1.1 SLA Configuration . . . 73
1.3.4.1.2 SLA Status . . . 74
1.3.4.2 Track . . . 74
1.3.4.2.1 Status Track . . . 74
1.3.4.2.2 Track Configuration . . . 74
1.3.5 Routing . . . 75
1.3.5.1 Route Table . . . 75
1.3.5.2 Static Routing . . . 75
1.3.5.3 Dynamic Routing . . . 76
1.3.5.3.1 RIP . . . 76
1.3.5.3.2 OSPF . . . 78
1.3.5.3.3 Filtering Route . . . 78
1.3.5.4 Multicast Routing . . . 79
1.3.6 Firewall . . . 81
1.3.6.1 ACL . . . 81
1.3.6.2 NAT . . . 82
1.3.6.3 MAC-IP Binding . . . 90
1.3.7 VPN . . . 92
1.3.7.1 IPSec ( Site-to-Site ) . . . 92
1.3.7.2 GRE . . . 101
1.3.7.3 Certificate Management . . . 102
1.3.8 Industrial . . . 104
1.3.8.1 DTU . . . 104
1.3.8.1.1 DTU 1 / DTU 2 . . . 104
1.3.8.1.2 Serial Port . . . 106
1.3.8.2 Status IO . . . 107
1.3.9 Tools . . . 108
1.3.9.1 Ping . . . 108
1.3.9.2 Traceroute . . . 108
1.3.9.3 Link Speed Test . . . 109
1.4 CE Deklaration . . . 110

# TK800 Manual

## Einführung

**Hinweis zum Copyright**
Copyright © 2015 Welotec GmbH
Alle Rechte vorbehalten.
Eine Vervielfältigung ohne Genehmigung ist nicht gestattet.

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

**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.

**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

**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 werden oder auf DIN-Schienen montiert werden. Produkte der TK800-Serie unterstützen VPN (IPSec/L2TP/GRE/OpenVPN), was sichere Verbindungen zwischen Remotegeräten und Kundenstandorten garantiert.

**Wichtige Sicherheitshinweise**
**Dieses Produkt ist für folgende Einsatzbereiche nicht geeignet**

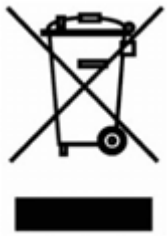
- Bereiche, in denen keine Funkanwendungen (wie Handys) erlaubt sind
- Krankenhäuser und andere Orte, an denen der Einsatz von Handys nicht zulässig ist
- Tankstellen, Treibstofflager und Orte, an denen Chemikalien gelagert werden
- Chemische Anlagen oder andere Orte mit Explosionsgefahr
- Metalloberflächen,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

**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.

**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.

# 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.

## 1. Paket Checkliste

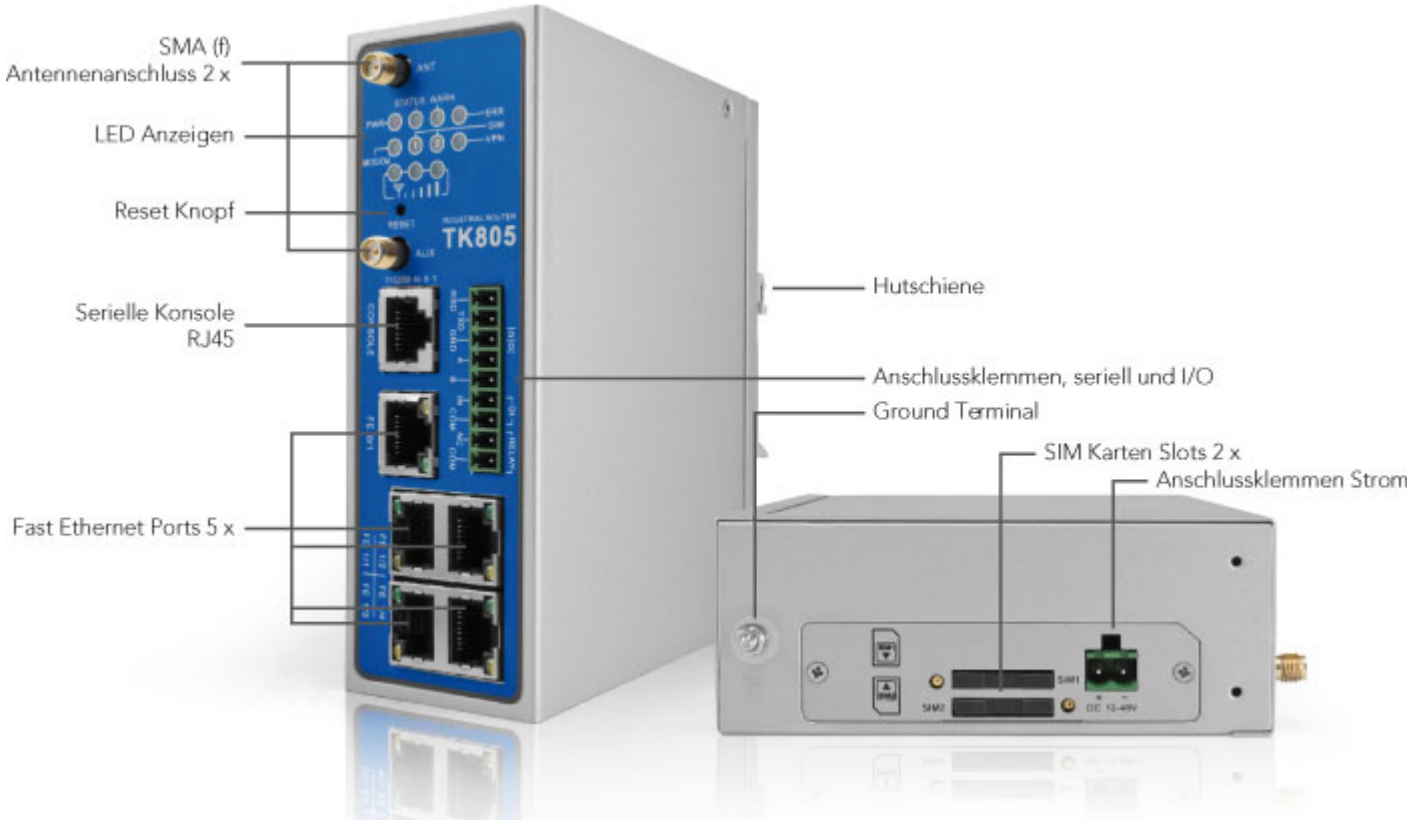
Jeder TK800 wird in einer Box mit Standardzubehör geliefert. Außerdem können optionale Zubehörteile bestellt werden. Prüfen Sie den Inhalt der Box. Sollte etwas fehlen, kontaktieren Sie Welotec.

*1.1 Standardzubehör*

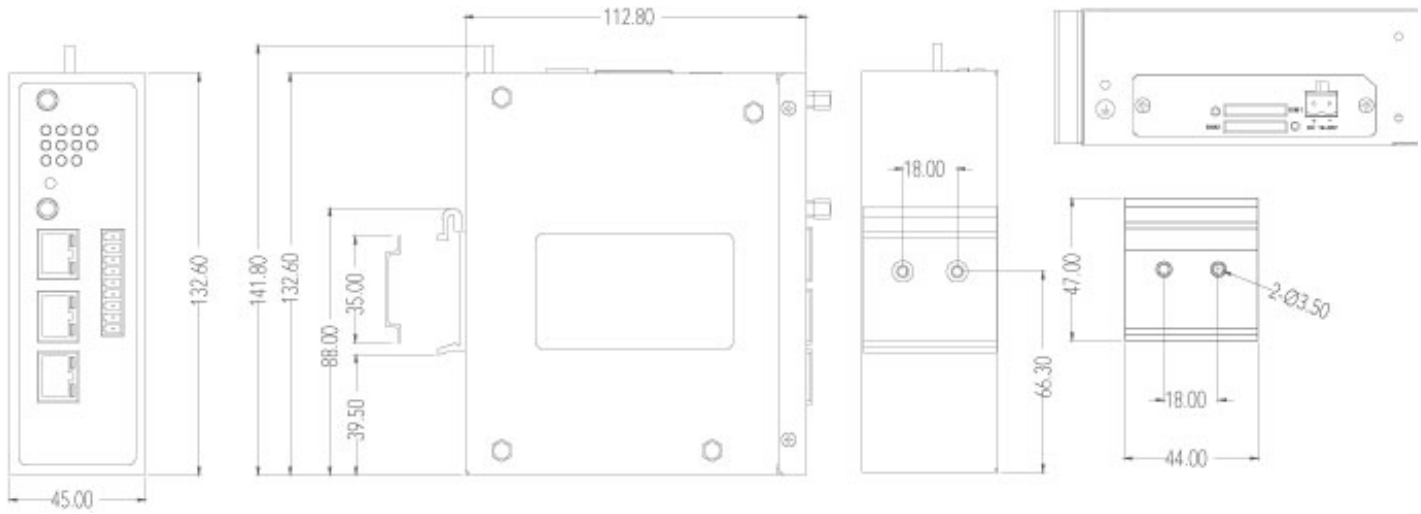
| Produkt | Anzahl | Beschreibung |
|---|---|---|
| TK800 | 1 | Industrieller Router der Serie TK800 |
| Anschlussklemme | 1 | Anschlussklemme, 2-polig |
| Netzwerkkabel | 1 | 1,5 m |
| Antenne | 2 | 3G/4G Antenne |
| Netzteil | 1 | 230 V AC auf 12 V DC |
| Anschlussklemmen Seriell und I/O | 1 | Anschlussklemme,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

## 2. Informations- und Bedienpanel

*2.1 Bedienpanel*



*2.2 Maßzeichnungen*



# 3. Installationsleitfaden

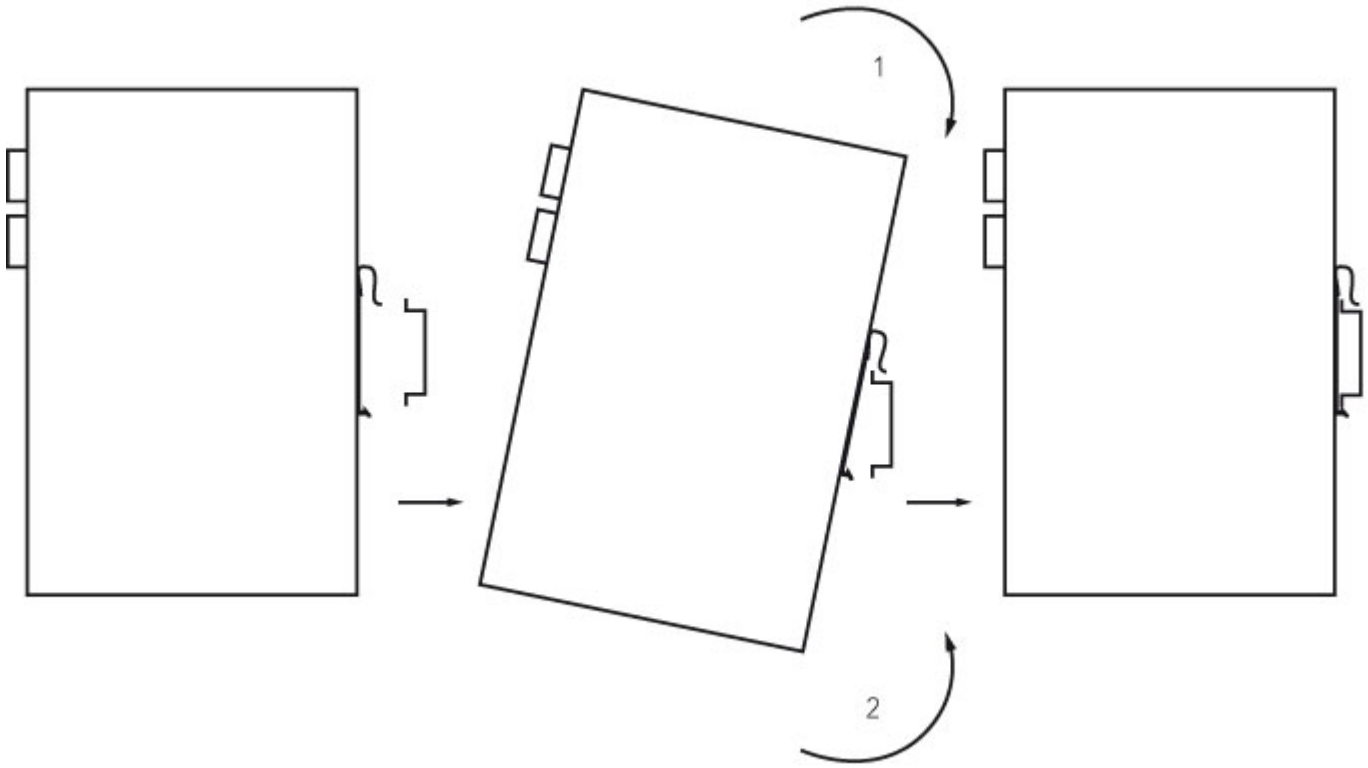
*3.1 Vorbereitungen*

Bereiten Sie die Spannungsversorgung vor (12 - 48 VDC). 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 wird auf einer DIN-Schiene (Hutschiene) montiert.

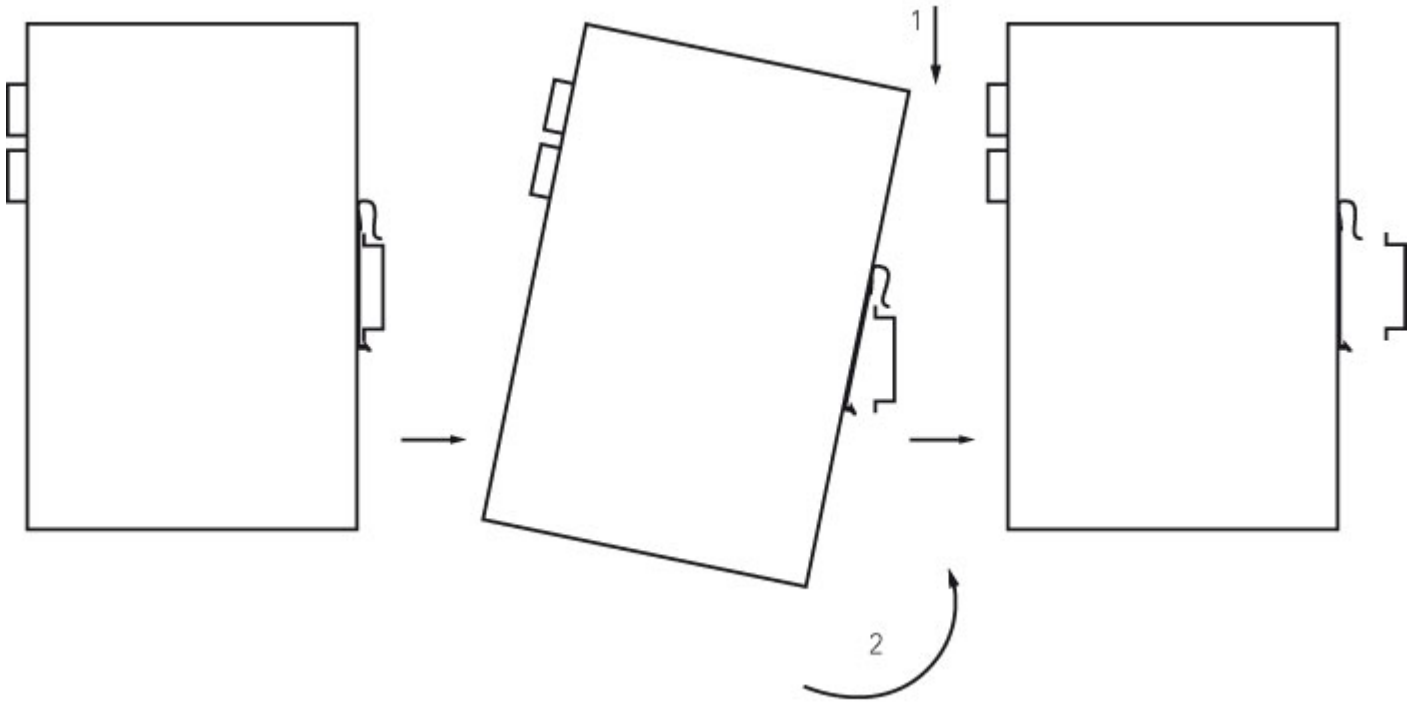
*3.2 Montage des Gerätes*

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).



## 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. Legen Sie dann die SIM-Karte wie in der Abbildung gezeigt ein.

## 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.

## 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.

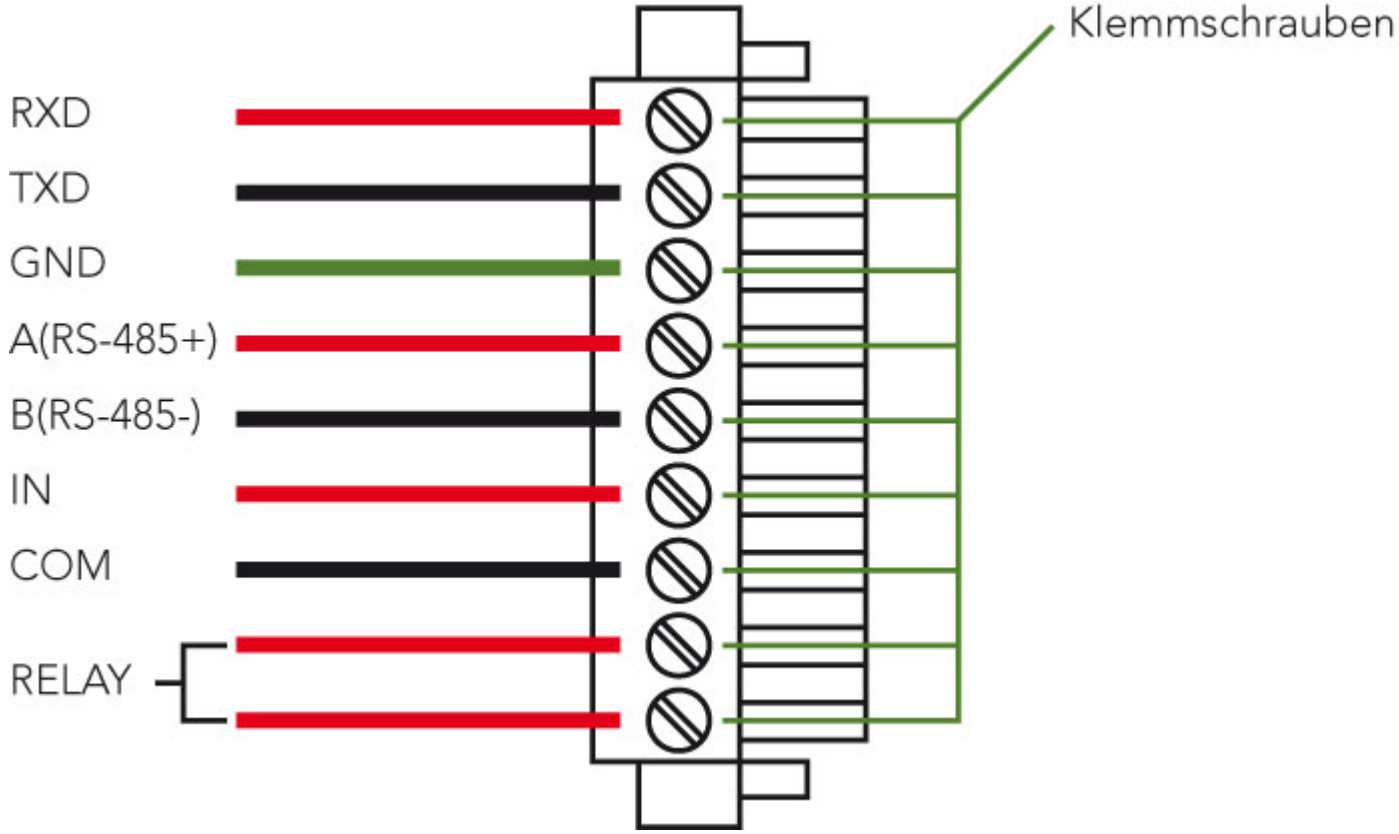
⚠ Um Störungen durch elektromagnetischen Einfluss auszuschließen, muss das Gehäuse des Routers über die Erdungsschraube geerdet werden.

## 7. Kabelverbindungen

Verbinden Sie den Router über Netzwerkleitungen mit Ihrem PC.

## 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. Bei der Installation ziehen Sie bitten 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.

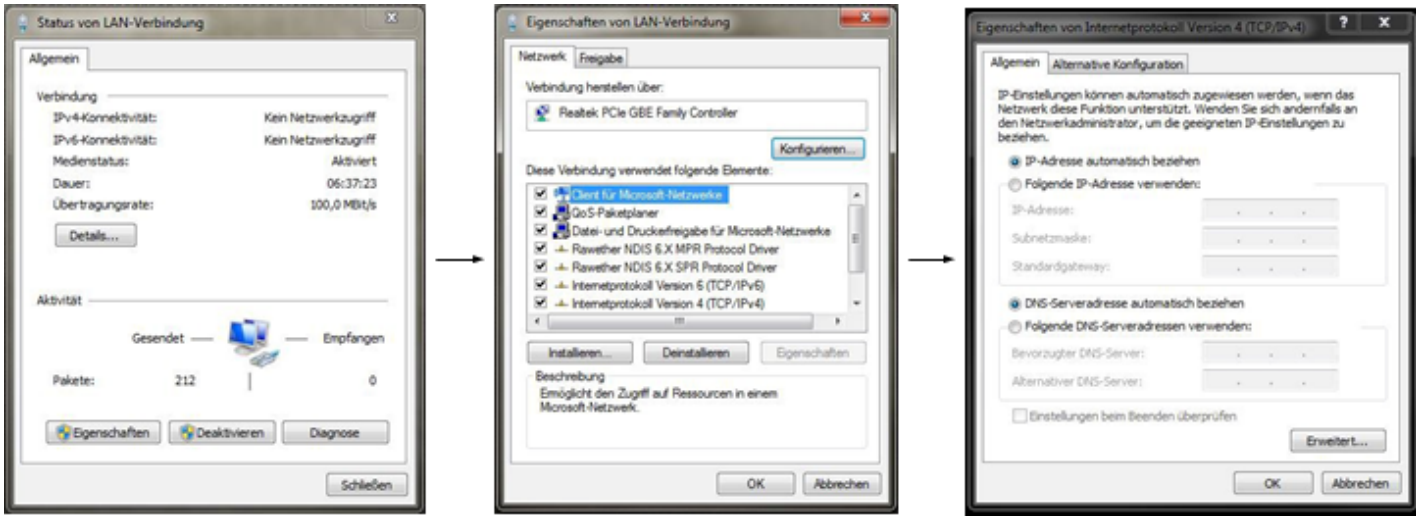



⚠ Dieses Kapitel beschreibt nur Router in den Ausführungen mit seriellen Schnittstellen und I/O´s TK8XXX-**EX**.

# 9. Inbetriebnahme des Routers

*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 FE0/1 oder FE0/2 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 7 und bei der Nutzung der Schnittstelle FE0/1 oder FE0/2.




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

Geben Sie dann in die Adresszeile **„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.

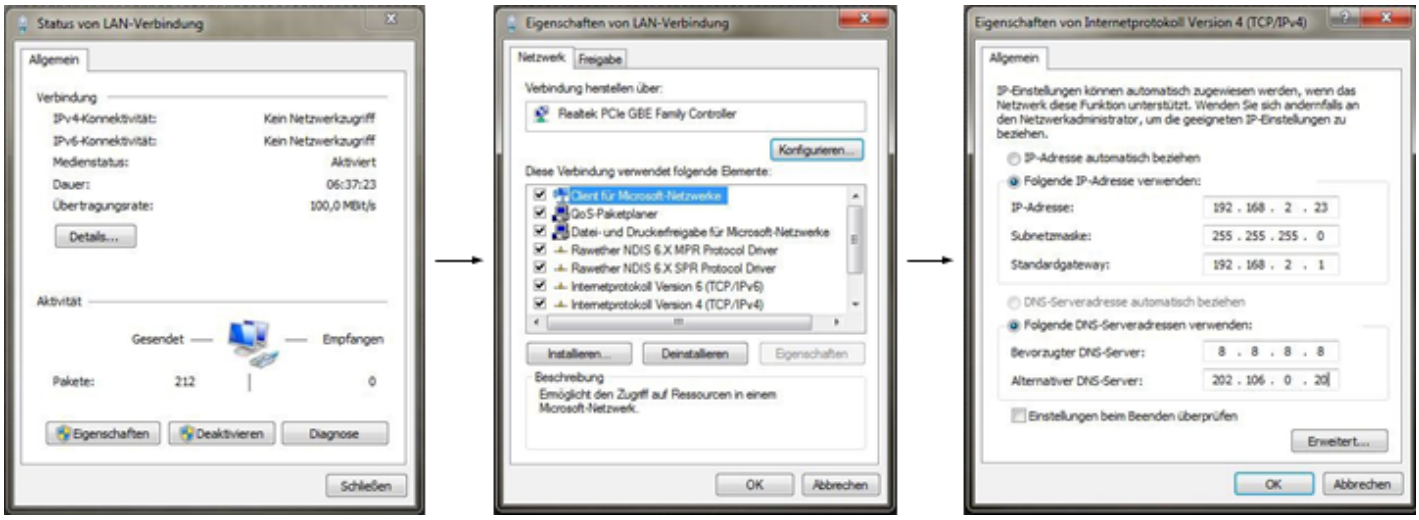
IP: 192.168.2.1

Benutzername: adm

Passwort: 123456

*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 7.




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

Geben Sie dann die Adresszeile **„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

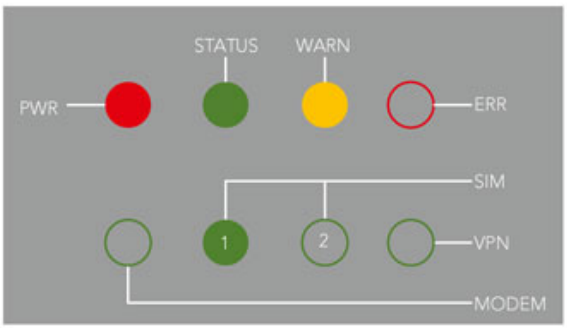
Passwort: 123456

## 10. LED-Statusleuchten

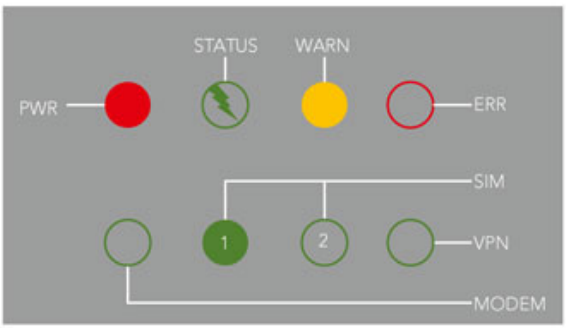
Beschreibung: leuchtet aus blinkt

⚠ 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:

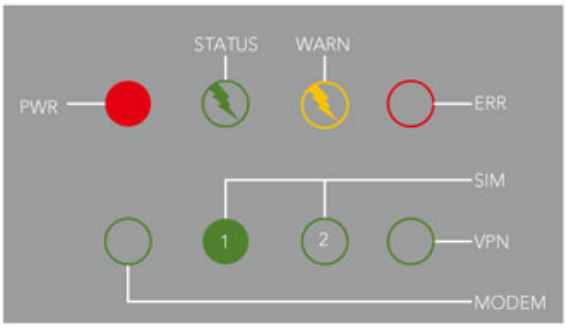
Systemstart:



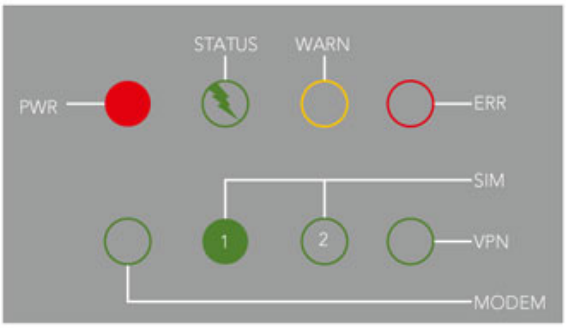

Systemstart erfolgreich:



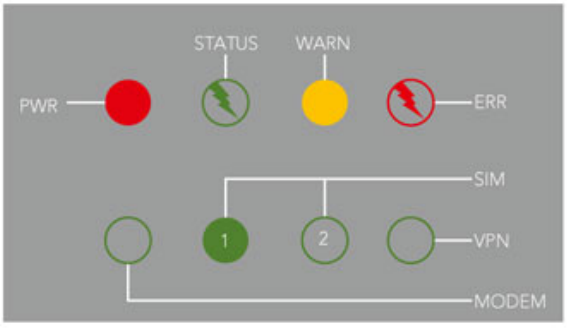

Einwahl:



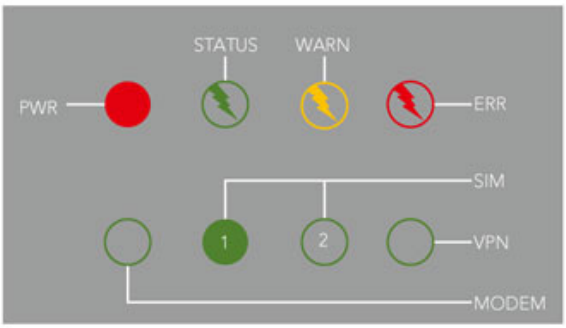

Einwahl erfolgreich:




Reset erfolgreich:




Firmwareaktualisierung:



**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)

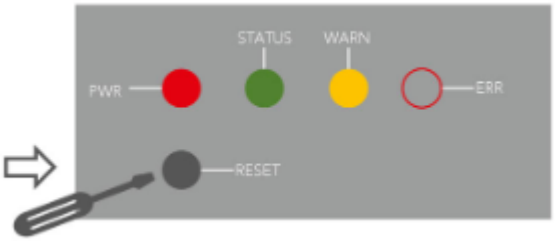
Signal:  20-31 (Perfektes Signallevel)

# 11. Zurücksetzten auf Werkseinstellungen

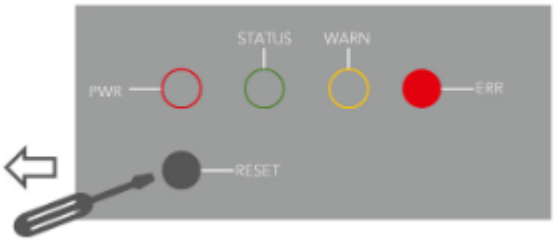
*11.1 Hardwaremethode*

Beschreibung: leuchtet aus blinkt

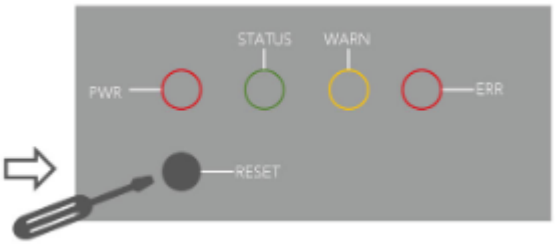
1) Drücken Sie die RESET-Taste, während Sie den TK800 einschalten:



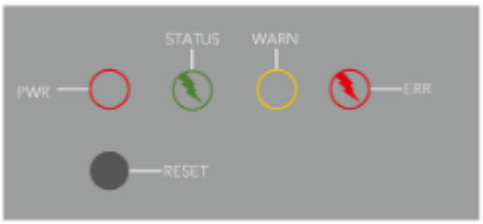

2) Sobald die LED-Leuchte ERROR aufleuchtet (ca. 10 Sekunden nach dem Einschalten), lassen Sie die RESET-Taste los:




3) Nach einigen Sekunden leuchtet die LED-Leuchte ERROR nicht mehr. Nun drücken Sie erneut die RESET-Taste:




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




Werkseitige Standardeinstellungen:

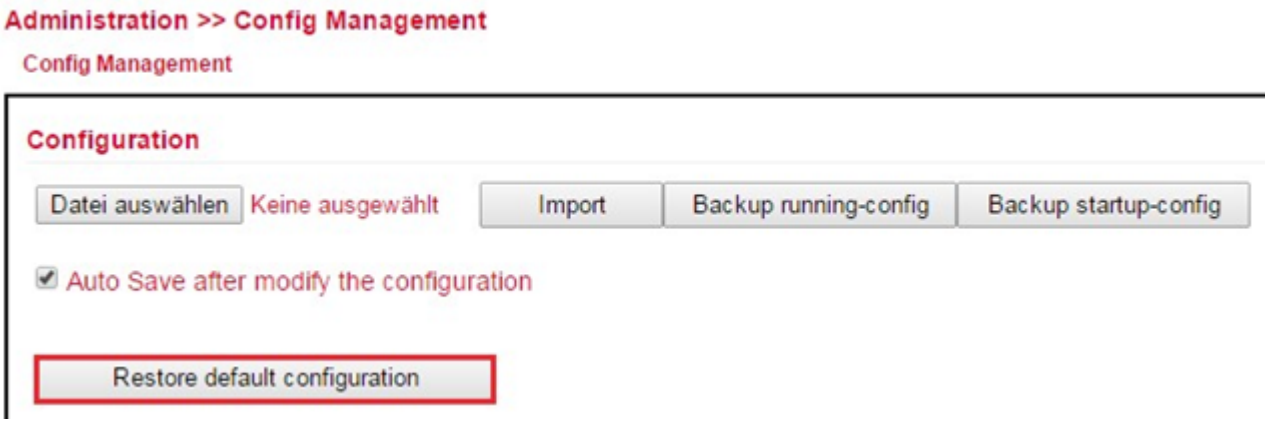
IP: 192.168.2.1

Netzmaske: 255.255.255.0

Serieller Parameter: 115200-N-8-1

*11.2 Webmethode*

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

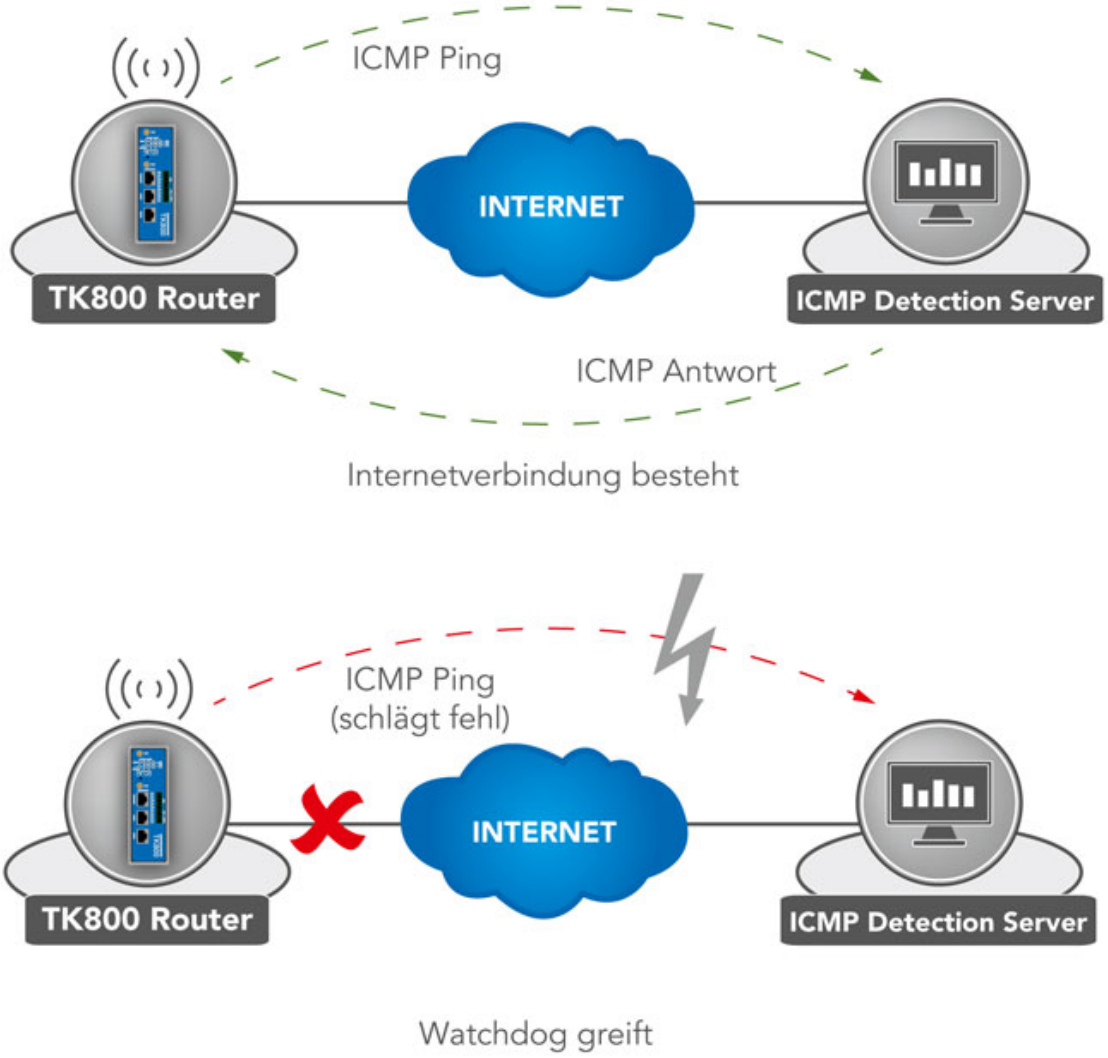



2) Klicken Sie auf **Restore Default Configuration**, um den TK800 auf seine Standardeinstellungen zurückzusetzen. Nach einigen Sekunden erhalten Sie folgende Meldung. Der Router ist nun erfolgreich zurückgesetzt.

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

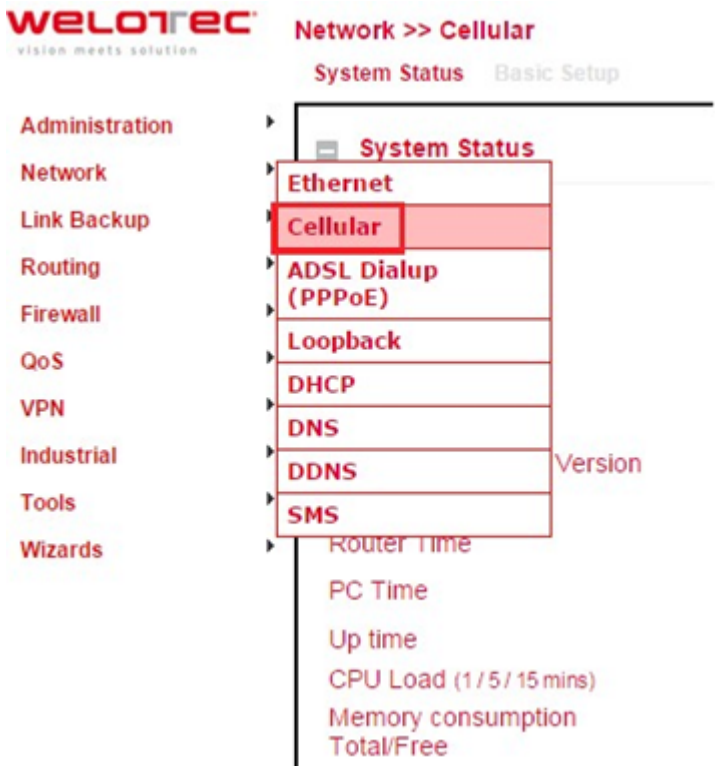
## 12. Watchdog

*12.2 Selbstständige Überwachung des Routers*

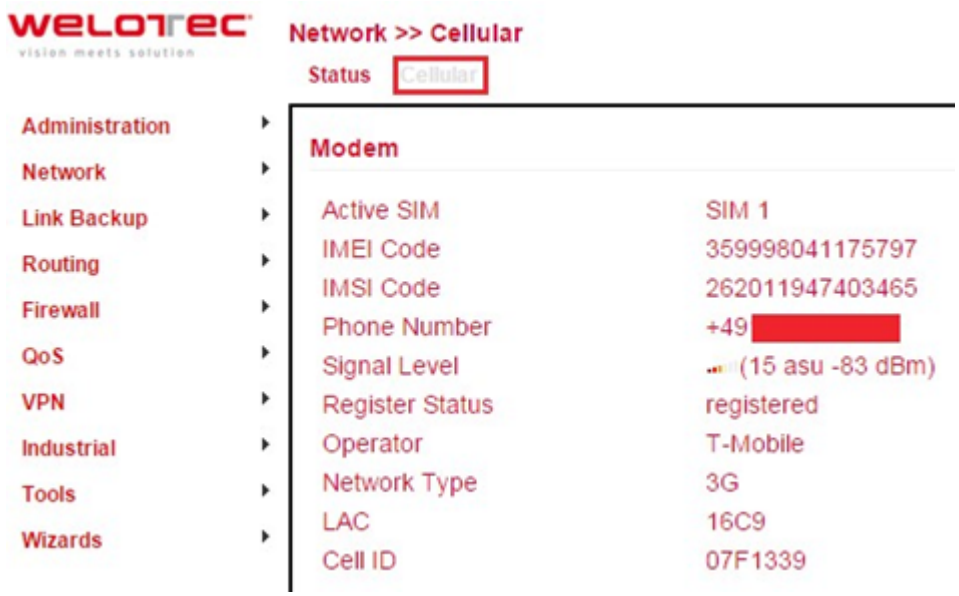



Der Watchdog überwacht den Router hinsichtlich der Internetverbindung. Der Router überprüft selbst, ob wie gewünscht eine Internetverbindung besteht. Dazu sendet er ICMP-Pakete zu einem individuell definierten Server (ICMP-Detection-Server). Sollte diese Abfrage fehlschlagen, startet der Router selbstständig 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.

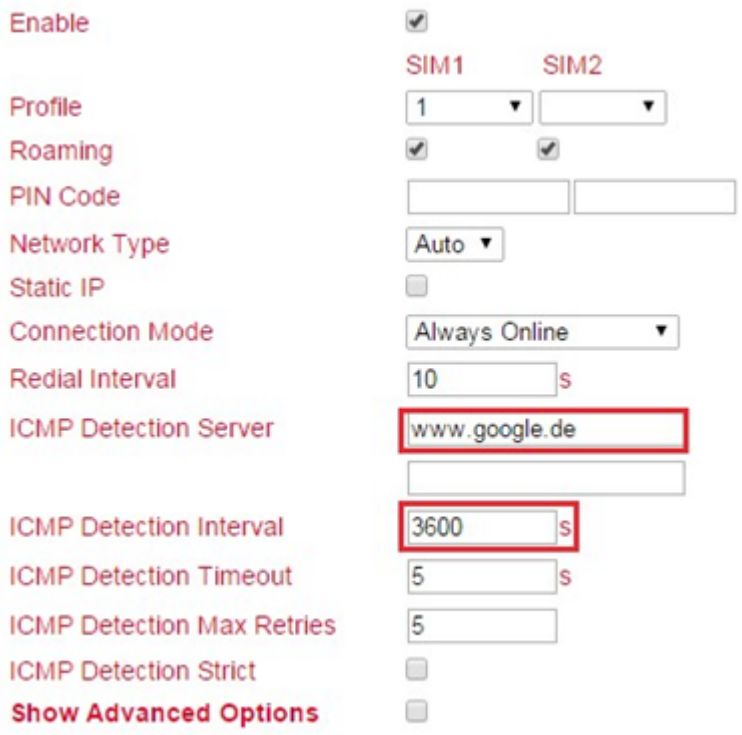
1) Gehen Sie über den Menüpunkt **Network** auf den Unterpunkt **Cellular**




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 sehr gut.

# 13. Port Mapping / Port Forwarding

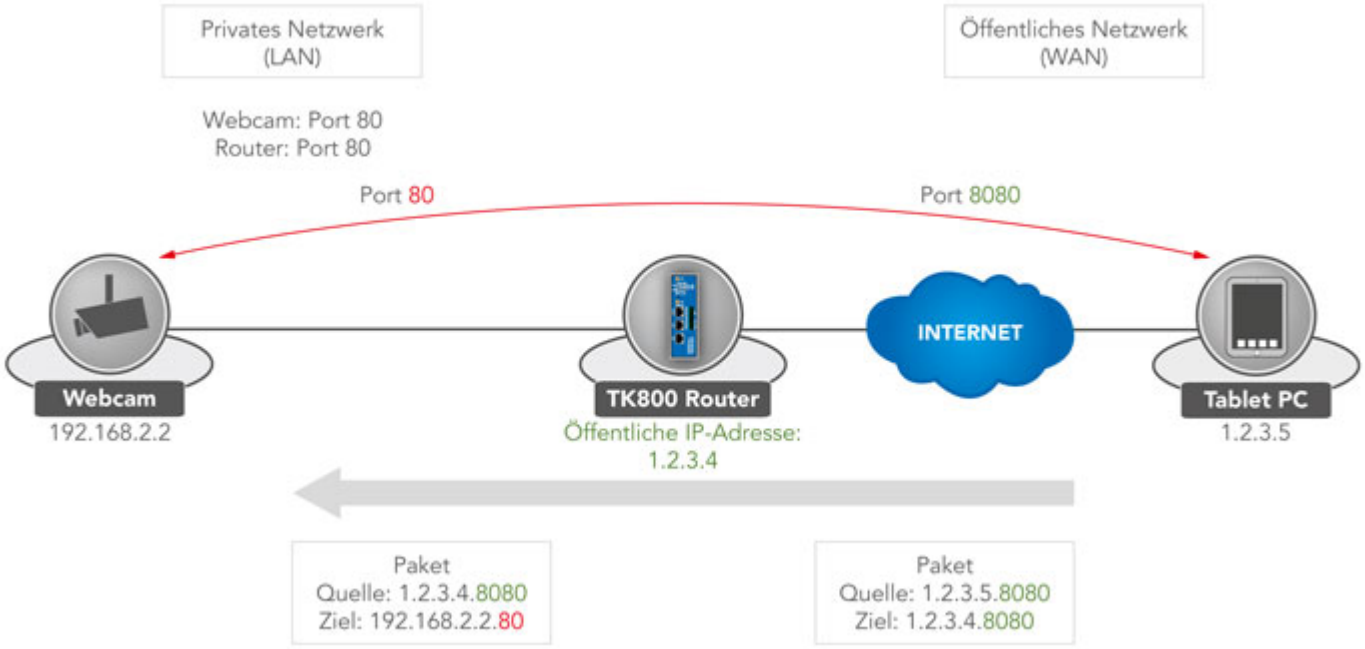
*13.1 Zugriff auf angeschlossene Geräte über das Internet*

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.

⚠ 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.r5034** oder höher.

Das folgende Bild veranschaulicht das Anwendungsbeispiel:




Erläuterung:

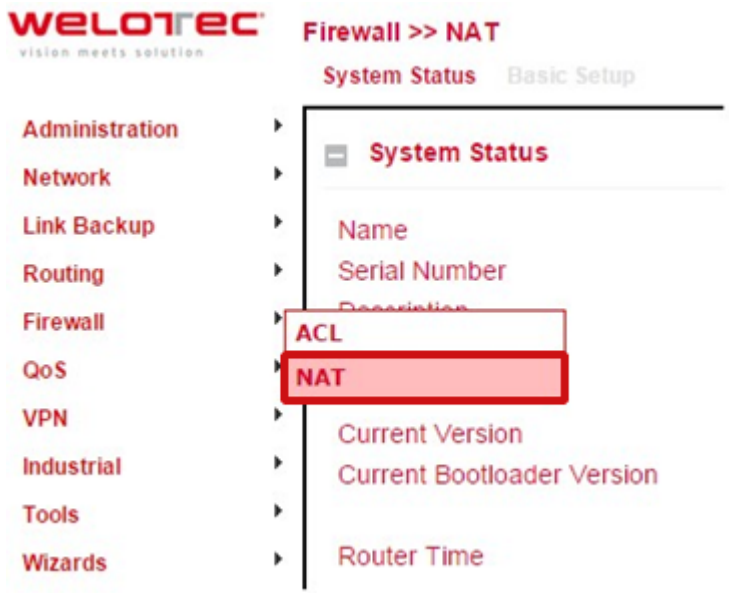
| Welotec Router: | |
|---|---|
| LAN IP-Adresse: | 192.168.2.1 |
| Subnetzmaske: | 255.255.255.0 |

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

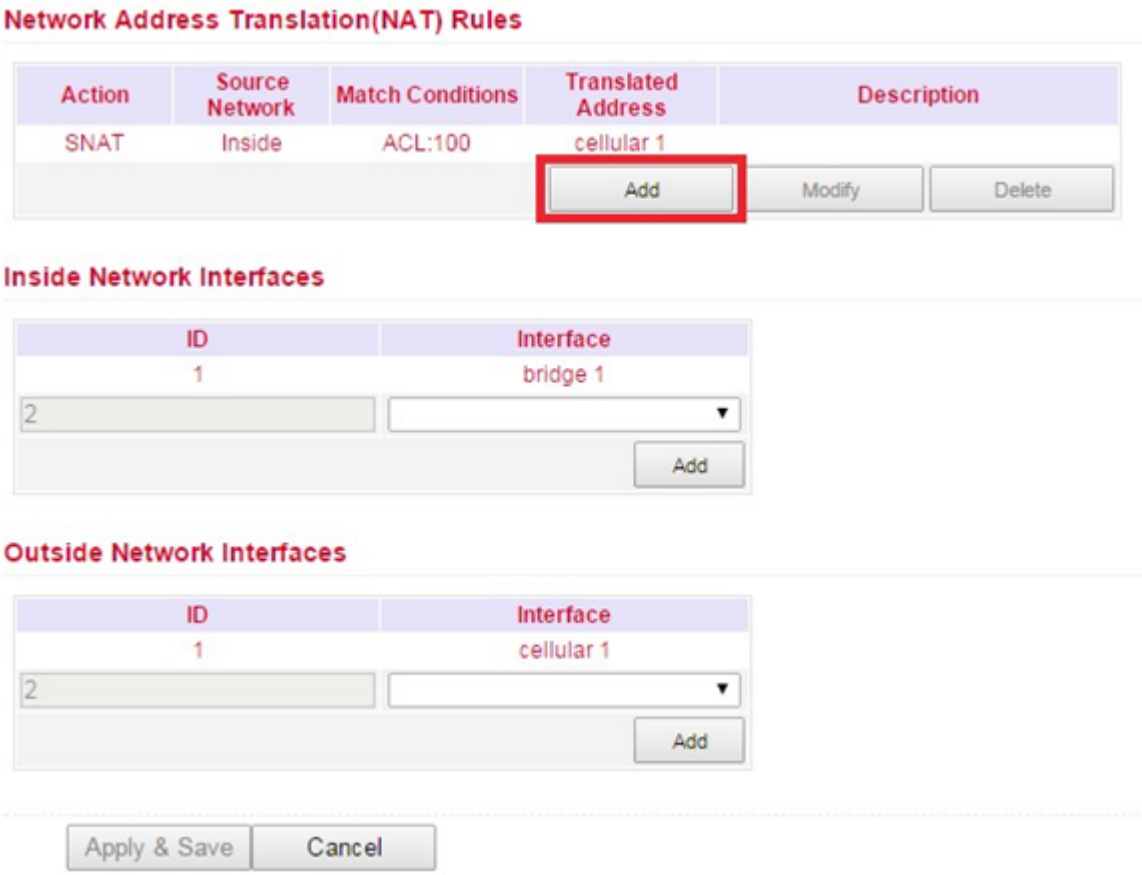
Die IP Kamera hat eine Oberfläche, die mit einem Browser über http://192.168.2.2 erreicht werden kann (Anm.: http-Protokoll hat TCP Port 80).

*13.2 Anleitung zum Port Mapping*

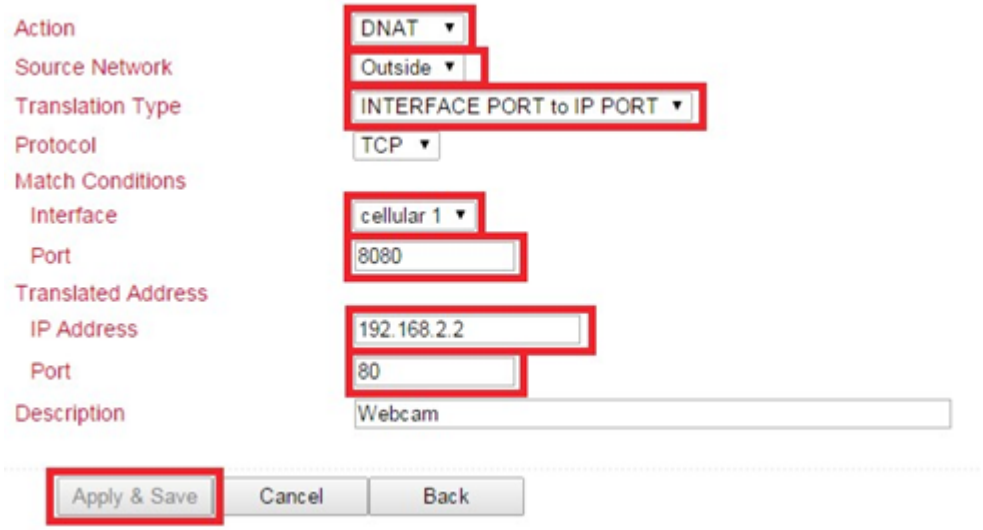
1) Gehen Sie über den Menüpunkt **Firewall** auf den Unterpunkt **NAT**



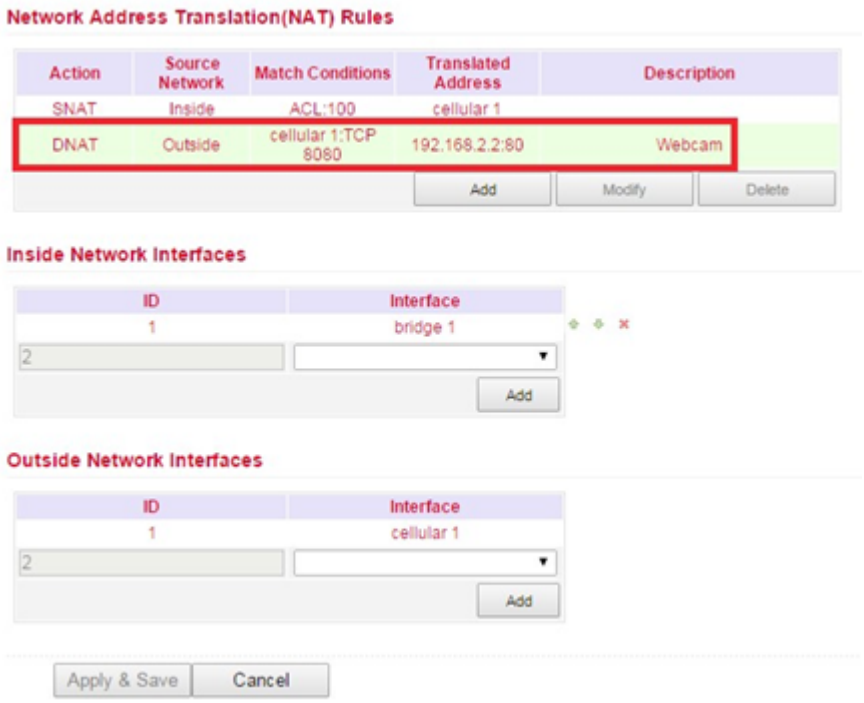

2) Fügen Sie nun mit **Add** eine neue NAT-Regel hinzu



3) Tragen Sie die Daten wie in dem Beispiel ein




4) Im Anschluss taucht die NAT Regel wie unten abgebildet in der Tabelle N**etwork 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 192.168.2.2?
- 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)?

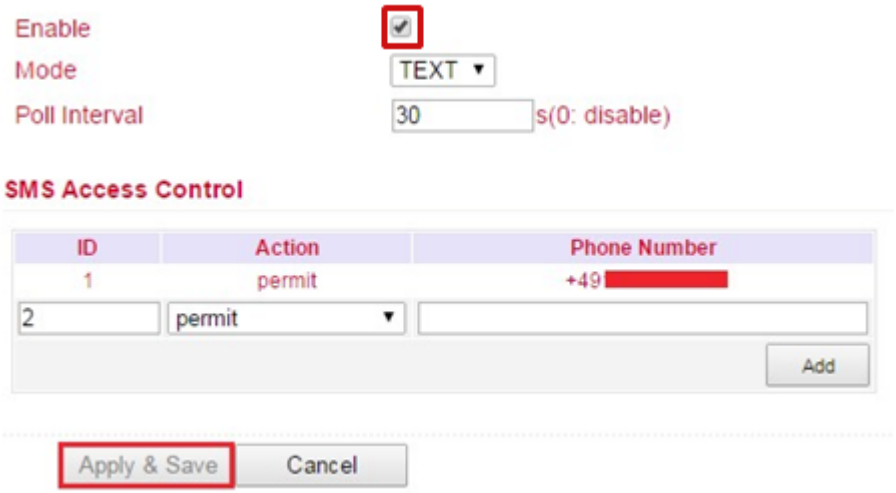
## 14. SMS-Funktionen

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.

*14.1 Statusabfrage / Neustart*

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

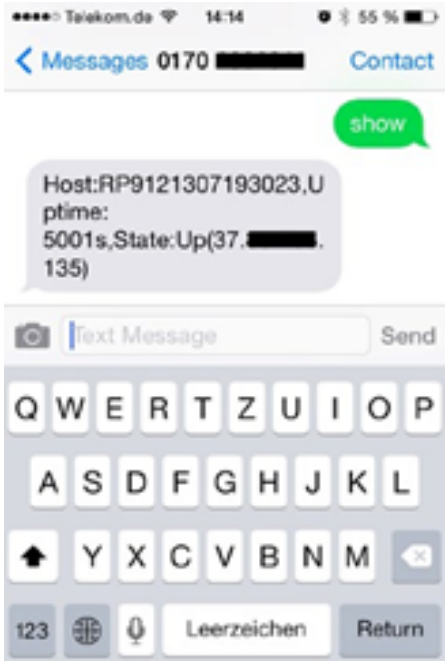
2) Klicken Sie auf die Checkbox **enable**, um die Funktion einzuschalten




3) Geben Sie in die Tabelle **SMS Access Control** die Telefonnummern ein, 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

| | | |
|---|---|---|
| info | Jan 1 01:59:13 | redial[822]: receive a sms from +49[redacted] |
| info | Jan 1 01:59:13 | smsd[869]: receive reboot sms! |
| notice | Jan 1 01:59:13 | systools[1492]: system is rebooting! |

*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

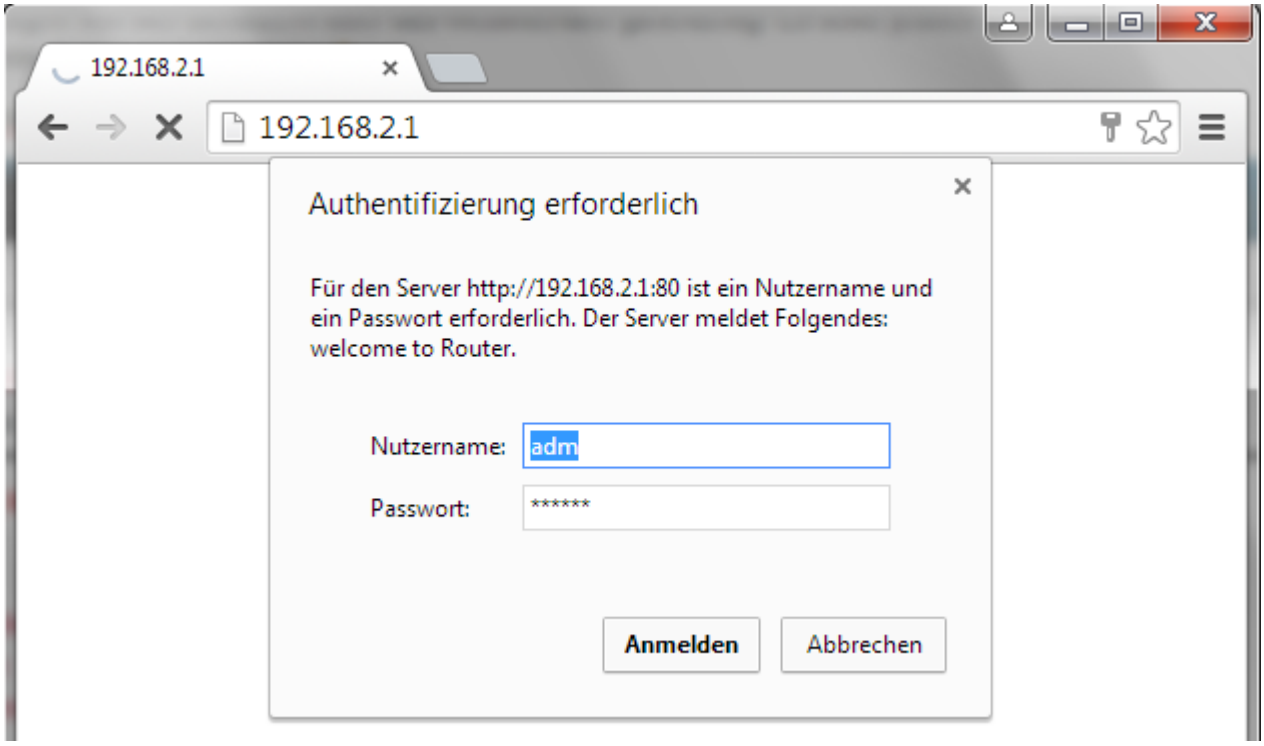
| | | |
|---|---|---|
| info | Jan 1 01:40:35 | redial[822]: receive a sms from +49[redacted] |
| info | Jan 1 01:40:35 | redial[822]: receive disconnect command, hangup! |
| info | Jan 1 01:40:35 | pppd[2151]: Hangup (SIGHUP) |

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

| | | |
|---|---|---|
| info | Jan 1 01:33:13 | redial[822]: receive a sms from +49[redacted] |
| info | Jan 1 01:33:13 | redial[822]: receive connect command, Go! |
| info | Jan 1 01:33:13 | pppd[906]: got user command, starting the link... |

# Web Konfiguration

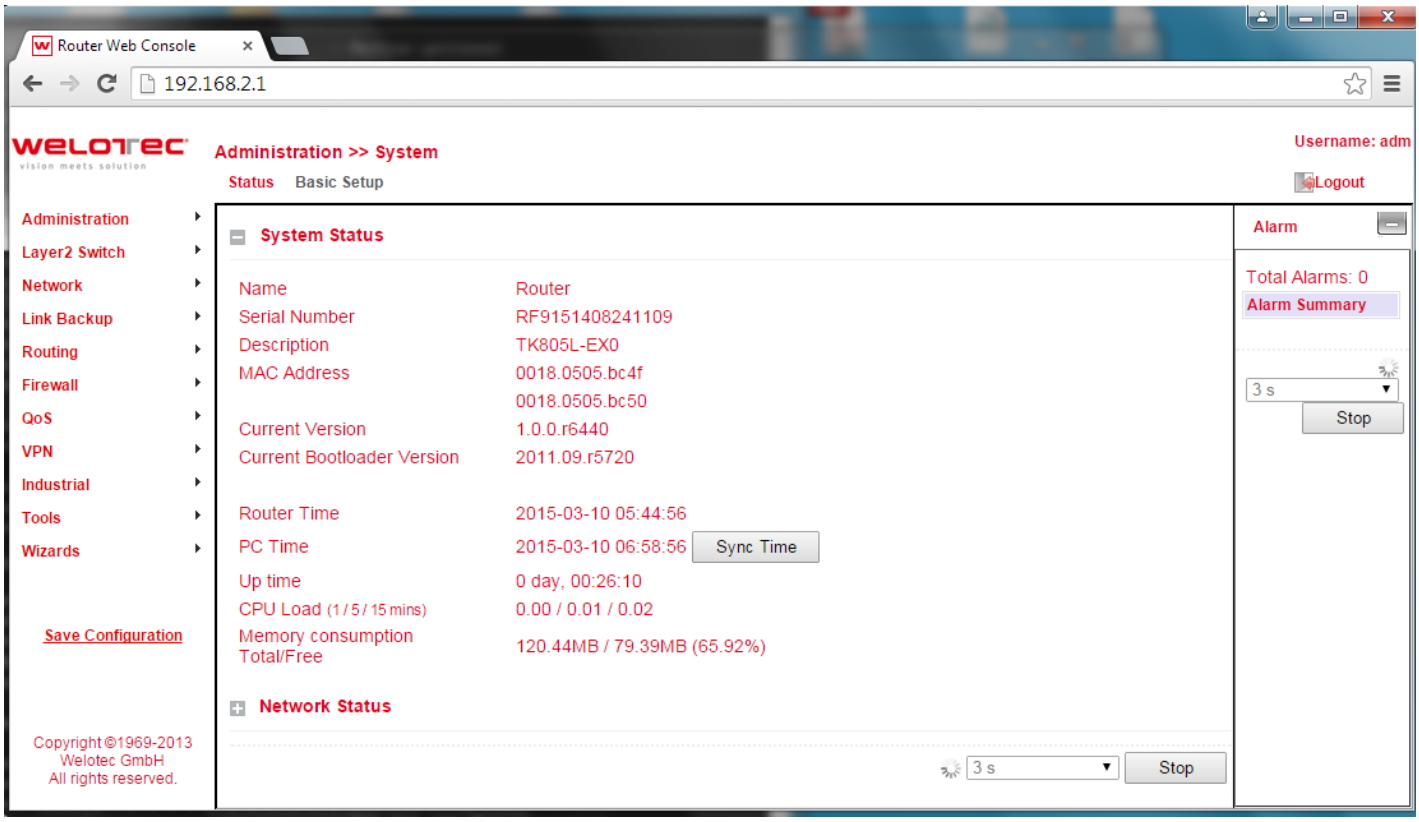
Die Router der TK800 Serie verfügen über einen eingebauten Webserver für die Konfiguration. Rufen Sie **http://192.168.2.1** im Browser auf. Geben Sie den **Benutzernamen (Standard: adm)** und das **Passwort (Standard: 123456)** ein und bestätigen Sie mit Anmelden.




⚠️ Aus Sicherheitsgründen sollte das Passwort nach dem ersten Login geändert werden. Wählen Sie ein Passwort mit Sonderzeichen, Zahlen und Groß- und Kleinschreibung. ⚠️

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

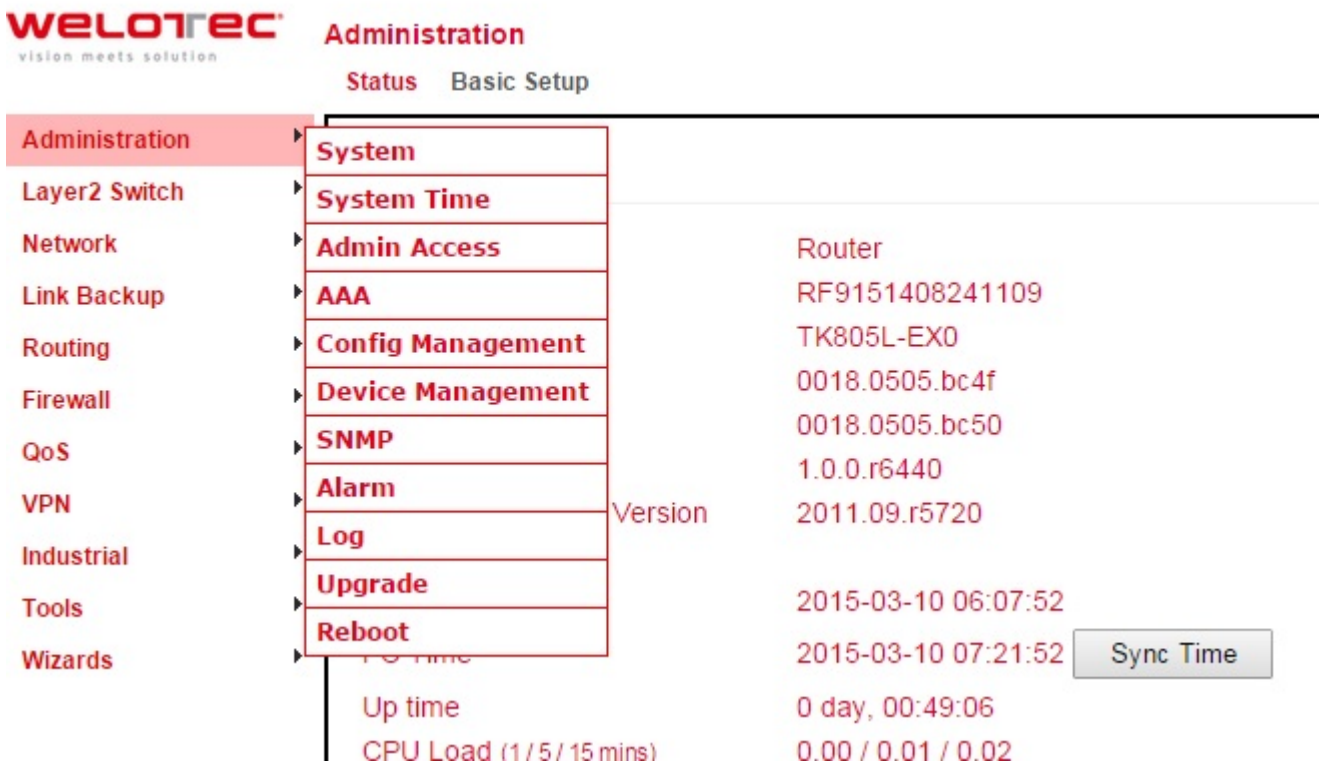
Nach dem erfolgreichen Login erscheint das Webinterface des Routers.



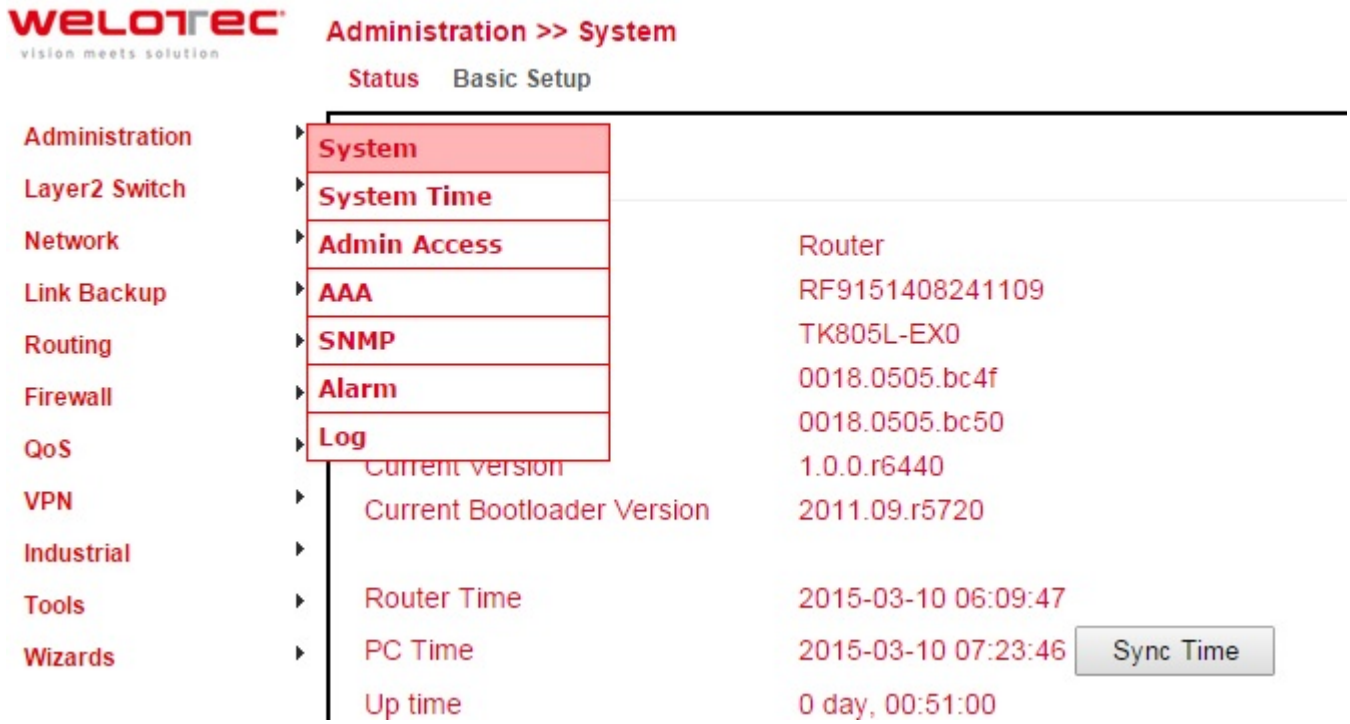

Das Webinterface des TK800 ist in 4 Bereiche aufgeteilt. Auf der linken Seite ist die Hauptnavigation mit den Punkten Administration, Layer2 Switch usw. Im oberen Bereich ist die Detailnavigation. In diesem Beispiel mit Status (aktiv) und Basic Setup. In der Mitte des Webinterfaces wird der aktuelle Status und die Konfigurationsmöglichkeiten dargestellt. Auf der rechten Seite werden aktive Alarme dargestellt.

## Administration

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




⚠ Bei Eingeschränkten Benutzerrechten (nicht Administrator) fehlen im Menü einige Punkte. Eingeschränkte Benutzer können den Router nicht konfigurieren. ⚠



## System

### Status

Unter Administration / System / Status befinden sich 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.

**System Status**

| | |
|---|---|
| Name | Router |
| Serial Number | RF9151408241109 |
| Description | TK805L-EX0 |
| MAC Address | 0018.0505.bc4f |
| | 0018.0505.bc50 |
| Current Version | 1.0.0.r6430 |
| Current Bootloader Version | 2011.09.r4223 |
| Router Time | 2015-03-09 08:49:41 |
| PC Time | 2015-03-09 08:47:50 Sync Time |
| Up time | 0 day, 00:04:32 |
| CPU Load (1 / 5 / 15 mins) | 0.00 / 0.00 / 0.00 |
| Memory consumption Total/Free | 120.44MB / 81.28MB (67.49%) |

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

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

**Network Status**

**Cellular 1** [Settings]

| | |
|---|---|
| Status | Connected |
| Signal Level | (28 asu -57 dBm) |
| Register Status | registered |
| IP Address | 37.84.187.183 |
| Netmask | 255.255.255.255 |
| Gateway | 1.1.1.3 |
| DNS | 10.74.210.210 10.74.210.211 |
| MTU | 1500 |
| Connection time | 0 day, 00:05:21 |

**Fastethernet 0/1** [Settings]

| | |
|---|---|
| Status | Up |
| Connection Type | Static IP |
| IP Address | 192.168.1.1 |
| Netmask | 255.255.255.0 |
| Gateway | 0.0.0.0 |
| DNS | 0.0.0.0 |
| MTU | 1500 |
| Connection time | 0 day, 00:05:25 |
| Remaining Lease | |
| Description | |

**Vlan 1** [Settings]

| | |
|---|---|
| Status | Up |
| IP Address | 192.168.2.1 |
| Netmask | 255.255.255.0 |
| Gateway | 0.0.0.0 |
| DNS | 0.0.0.0 |
| MTU | 1500 |

## Basic Setup

Unter Administration / System / Basic Setup kann die Sprache des Routers und der Router Name angepasst werden. 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.

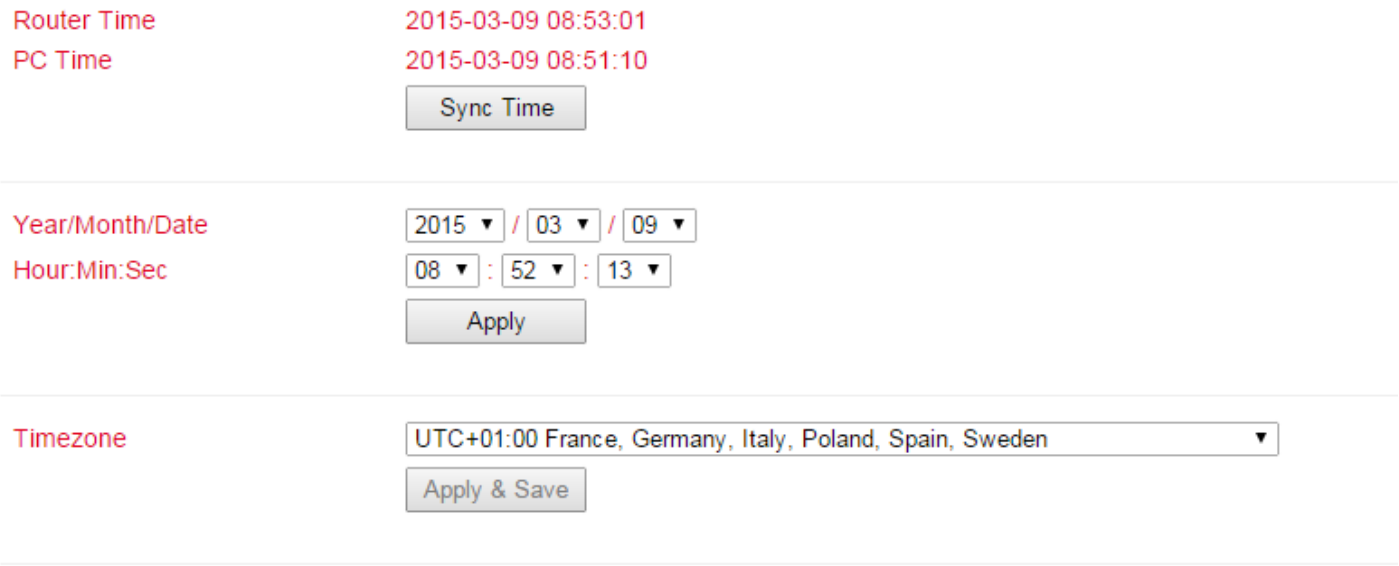
| | |
|---|---|
| Language | English ▼ |
| Router Name | Router |

## System Time

Um die Koordination zwischen dem TK800 Router und anderen Geräten zu gewährleisten, sollte die Systemzeit auf allen Geräten gleich sein 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 Zeit auszurüsten.

## System Time Konfiguration

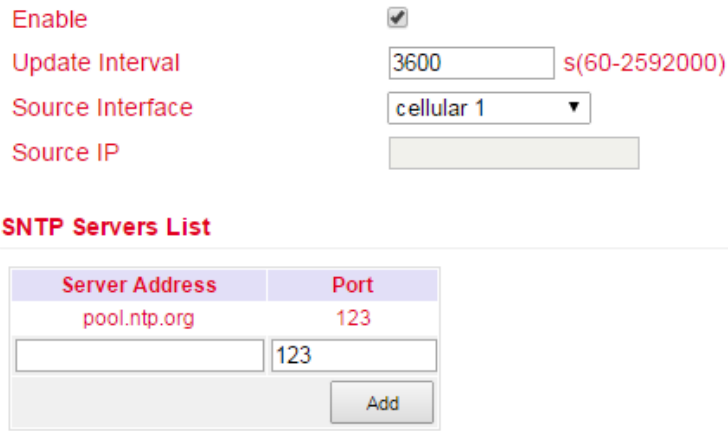
Unter Administration / System Time befinden sich eine Übersicht und lokale Einstellungen zu der Systemzeit des Routers. Über Sync Time kann die Uhrzeit des Routers mit der Uhrzeit des PC's synchronisiert werden. Unter den Einstellungen befindet sich die Möglichkeit, die Router Zeit und das Datum manuell einzustellen. Unter Timezone kann die aktuelle Zeitzone ausgewählt werden. Standard ist hier UTC+1 (Zeitzone in Deutschland, Österreich und der Schweiz).




## 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 Syncronisierungsquelle 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.




⚠ Bevor ein SNTP Server eingerichtet wird, sollte sichergestellt werden, dass der SNTP Server erreichbar ist. Besonders im Fall von einem Domain Namen sollte überprüft werden, ob der DNS Server für die Namensauflösung richtig konfiguriert ist. ⚠

⚠ 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.

| | | |
|---|---|---|
| info | Mar 9 08:57:12 | sntpc[823]: time updated: Mon, 09 Mar 2015 08:57:12 +0100 [-112s] |

## 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.

## Admin Access

Unter Administration / Admin Access 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 Administrator eignet sich zur Konfiguration und Management des Routers. Der Standardbenutzer eignet sich zum Überwachen und Überprüfen des Routers.

## Create a User

Unter Administration / Admin Access / Create a User können weitere Benutzer angelegt werden.

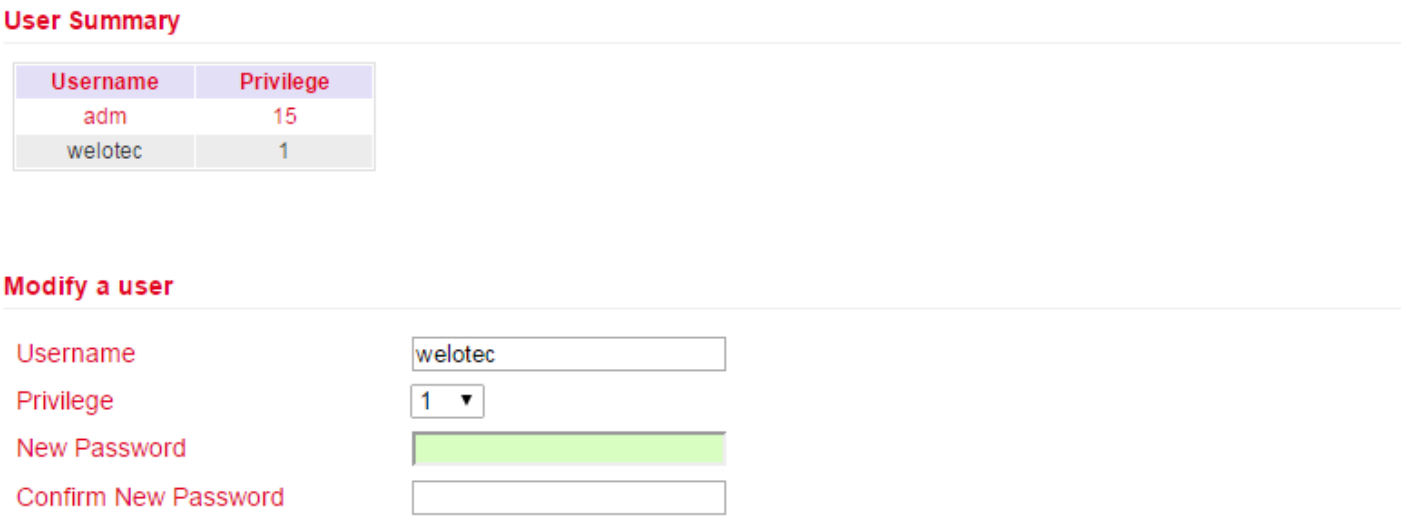
Es muss ein Username und Password anglegt werden und die Berechtigung (Privilege) eingetragen werden. Privilege 1 bis 14 ist für Standardbenutzer (Nur Leserechte) und Privilege 15 für Administratoren (Voller Zugriff).

Unter User Summary befindet sich eine Liste mit allen Benutzern und die zugehörigen Rechte (Privilege).

⚠ Ein sicheres Passwort sollte mindestens 8 Zeichen bestehend aus Groß- und Kleinschreibung, Zahlen und Sonderzeichen bestehen. ⚠

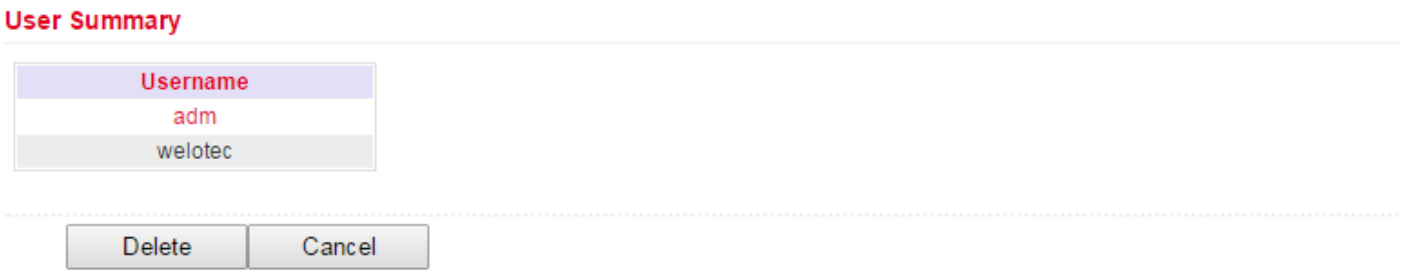
## Modify a User

Unter Administration / Admin Access / Modify a User kann ein Benutzer bearbeitet werden. Es können die Berechtigungen und Passwörter geändert werden. Unter User Summary kann ein Benutzer ausgewählt werden und dann unter Modify a user bearbeitet werden. Mit Apply & Save kann die Änderung bestätigt werden.




## Remove Users

Unter Administration / Admin Access / Remove Users kann ein Benutzer vom TK800 gelöscht werden. Unter User Summary kann der Benutzer ausgewählt werden und dann über den Delete Button gelöscht werden.




## Management Services

Unter Administration / Admin Access / Management Services kann der Zugriff auf das Webinterface mit HTTP und HTTPS sowie auf das Command Line Interface (CLI) via Telnet und SSH.

**HTTP**

HTTP ist die Abkürzung für Hypertext Transfer Protocol und wird genutzt um Webseiteninformationen über ein Netzwerk oder das Internet zu übertragen.

**HTTPS**

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

**TELNET**

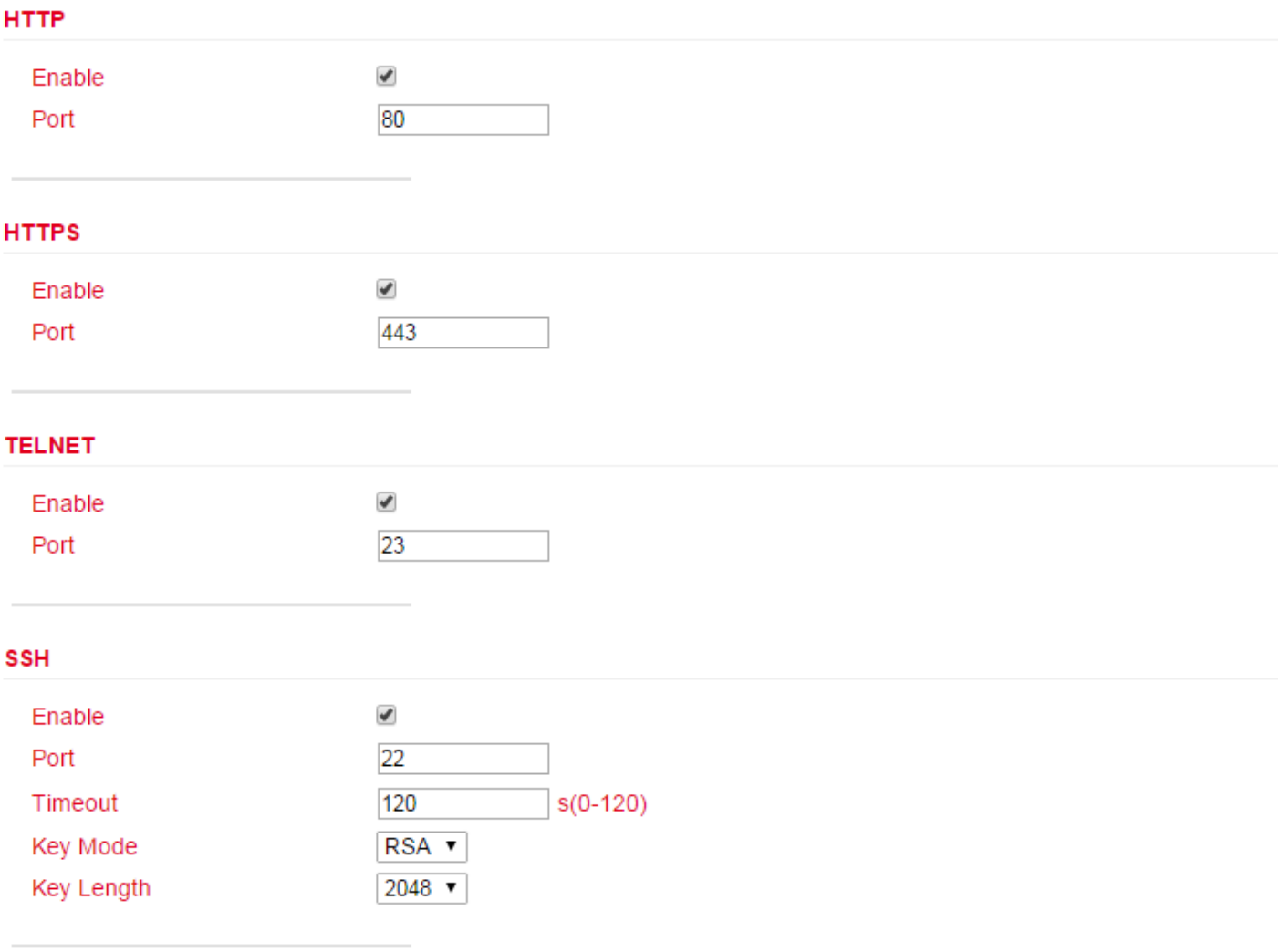
TELNET wird genutzt um auf das Command Line Interface (CLI) des Routers zuzugreifen.

**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. Hierfür einfach den Haken bei Enable setzen oder entfernen. Unter Port kann der TCP Port für den jeweiligen Dienst ausgewählt werden. Für SSH kann zudem noch der 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.



## 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.

### Radius

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

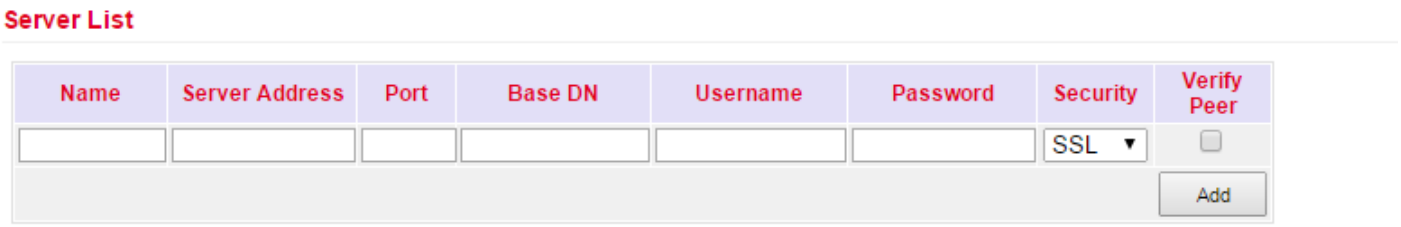
Hier kann der FQDN oder die IP-Adresse des Server, der Port und der Key für den Radius Server eingegeben werden.

### 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).

### 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.



## AAA Settings

| Service | Authentication 1 | Authentication 2 | Authentication 3 | Authorization 1 | Authorization 2 | Authorization 3 |
|---|---|---|---|---|---|---|
| console | none | none | none | none | none | none |
| telnet | none | none | none | none | none | none |
| ssh | tacacs+ | radius | none | tacacs+ | ldap | none |
| web | none | none | none | none | none | none |

## Config Management

Unter Administration / Config Management kann die aktuelle Konfiguration abgespeichert werden, eine bestehende Konfiguration hochgeladen werden oder der Router kann 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 Button 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**

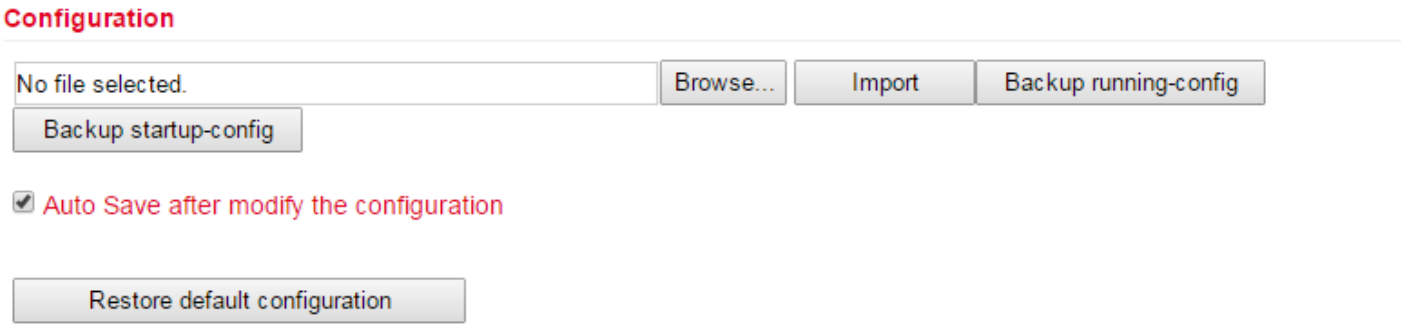
Über Backup running-config kann die aktuelle Konfiguration inkl. der nicht bestätigten Änderungen im Betrieb heruntergeladen werden. Über Backup startup-config kann die Konfiguration ohne die nicht bestätigten Änderungen heruntergeladen werden.

**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 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 den Button Restore default configuration kann die Konfiguration des Routers auf die Standardeinstellungen zurück gesetzt werden.




## Device Management

⚠ Keine Funktion hinterlegt. Kommt in einem späteren Firmware Release. ⚠

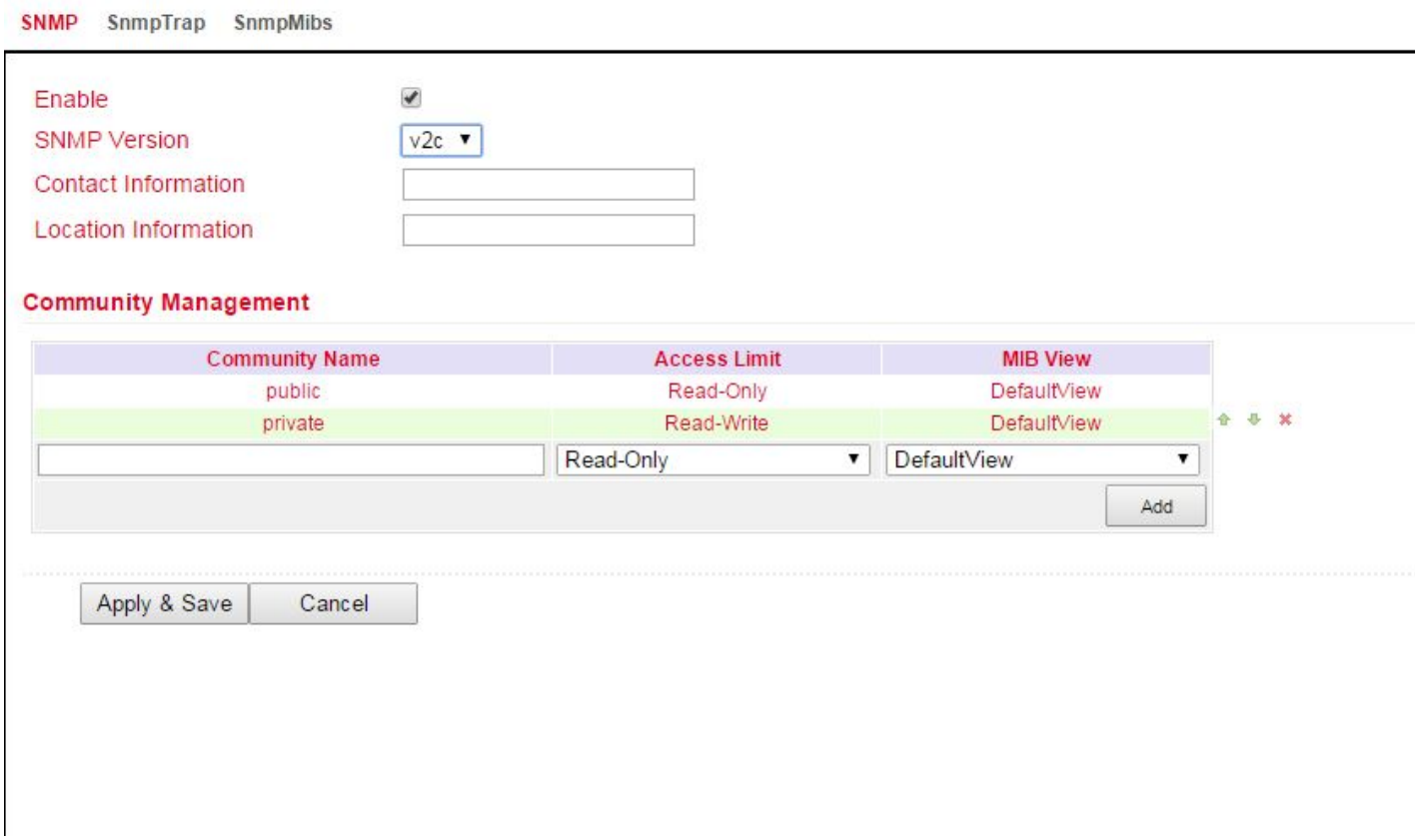
## SNMP

SNMP steht für **Simple Network Management Protocol** und ist ein Netzwerkprotokoll, um Netzwerkgeräte (Router, Switches, Server etc.) zentralisiert überwachen und steuern zu können.

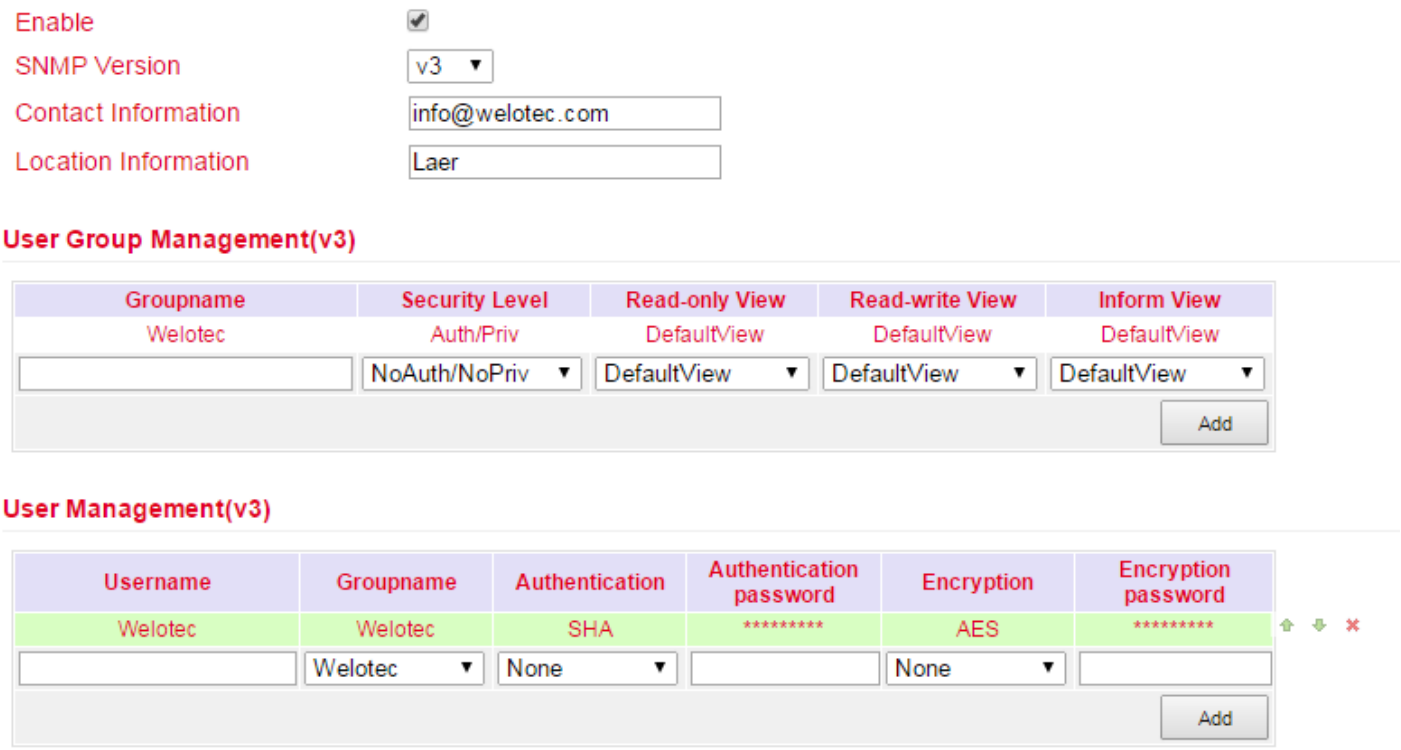
### SNMP Konfiguration

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.




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 (Abb. 2).



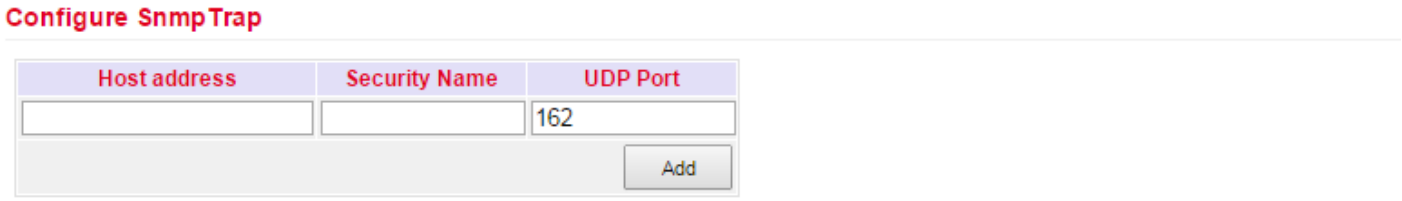

Bei SNMPv3 gibt es ein Gruppen- und Benutzermangement.

Authentication unterstützt SHA oder MD5.

Encryption unterstützt AES oder DES.

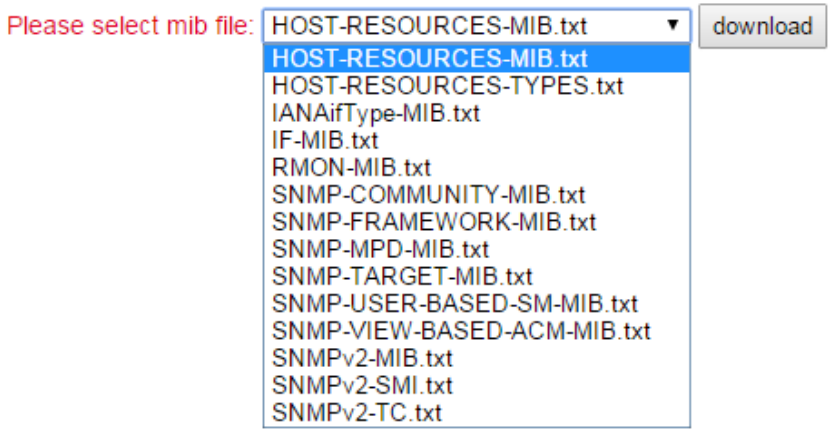
## SnmpTrap

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 Abfrage vom Management Server bekommt.




## SnmpMibs

Die SnmpMips zur Abfrage des Routers können heruntergeladen werden.




## SNMP Mibs auslesen

***1) MIBS vom TK800 herunterladen:***

***2) MIBS einlesen***

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***

snmpwalk -m +WELOTEC-MIB -v3 -u WeloSNMPUser -l AuthPriv -a MD5 -A 123456789 -x AES -X 123456789 192.168.2.1 WELOTEC

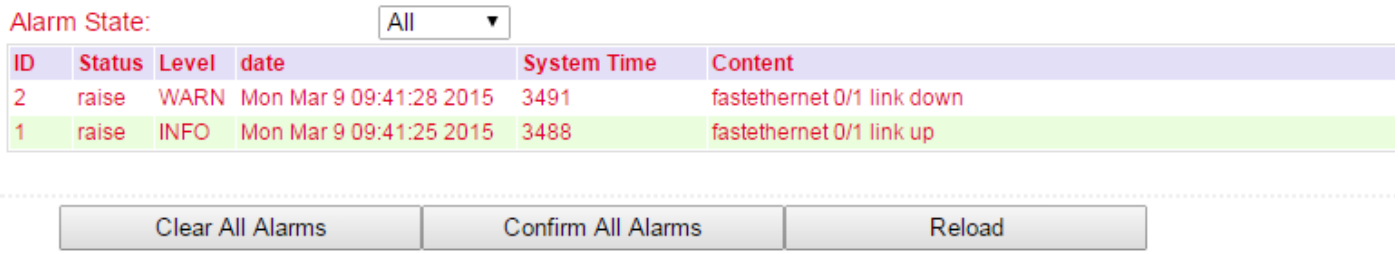
```
WELOTEC-MIB::ihOverview.1.0 = STRING: "TK800"
WELOTEC-MIB::ihOverview.2.0 = STRING: "RF9151408241109"
WELOTEC-MIB::ihOverview.3.0 = STRING: "2011.09.r6460"
WELOTEC-MIB::ihOverview.4.0 = STRING: "1.0.0.r6496"
WELOTEC-MIB::ihWan3g.1.1.1.0 = INTEGER: 3
WELOTEC-MIB::ihWan3g.1.1.2.0 = INTEGER: 1
WELOTEC-MIB::ihWan3g.1.1.3.0 = 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
```

## Alarm

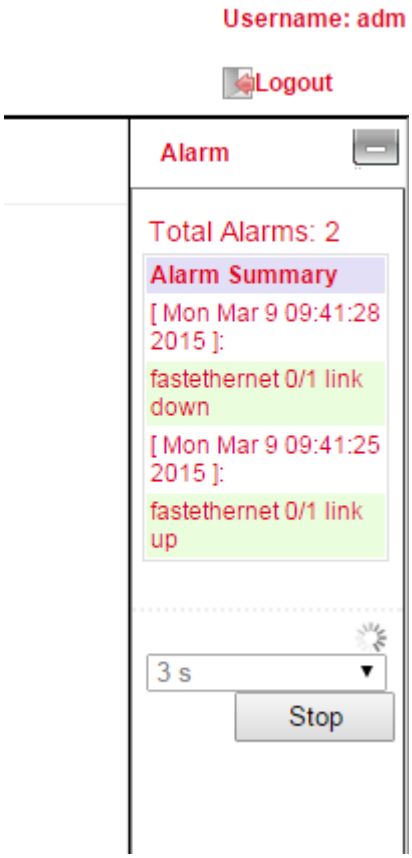
### Alarm Status

Der Alarmstatus zeigt eine Übersicht der ausgelösten Alarme an.

An diesem Beispiel wird in der INFO Meldung ID 1 angezeigt, dass der Fastethernet Port 0/1 verbunden wurde und mit der ID 2, dass die 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).




## Alarm Input

Beim Alarm Input Menü wird definiert, welche Alarmmeldungen der Router ausgeben soll. Durch Setzen der Haken neben jedem Eintrag wird ein Alarm aktiviert oder deaktiviert.

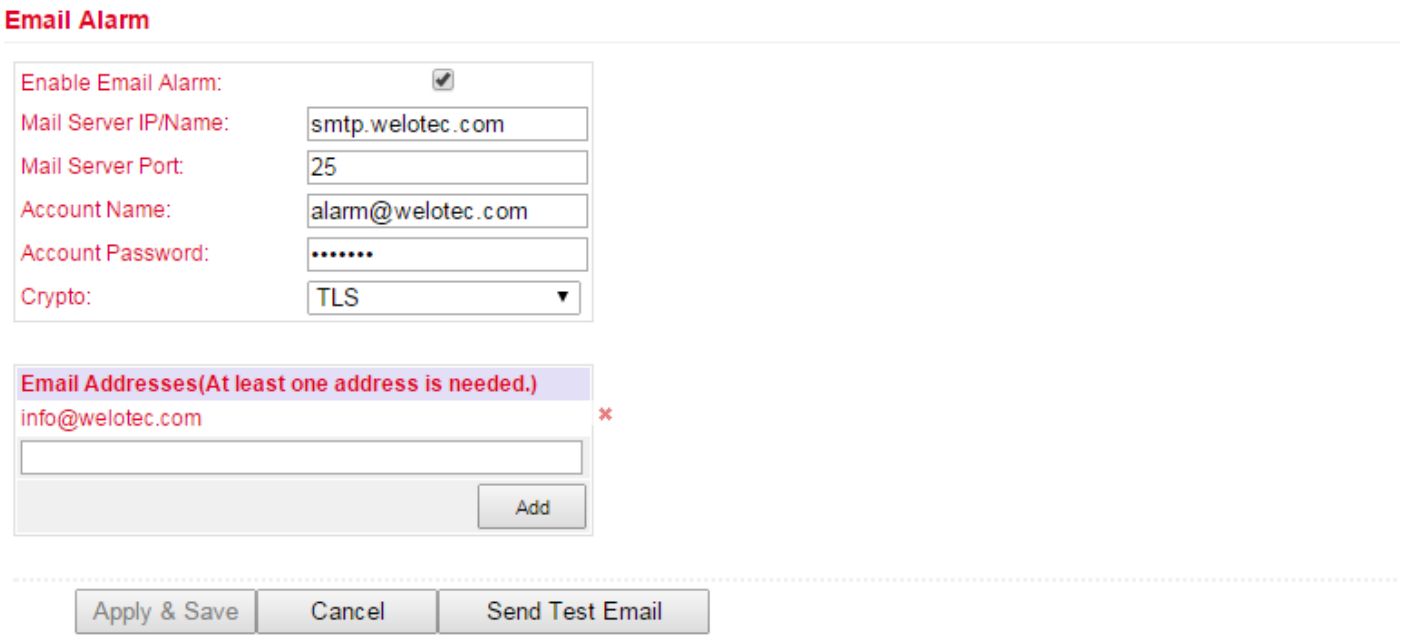
Warm Start ☑
Cold Start ☑
Memory Low ☑
Digital Input High ☑
Digital Input Low ☑
FE0/1 Link Down ☑
FE0/1 Link Up ☑
Cellular Up/Down ☑
ADSL Dialup (PPPoE) Up/Down ☐
Ethernet Up/Down ☑
VLAN Up/Down ☑

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 | Fastethernet Port 0/1 getrennt |
| FE0/1 Link Up | Fastethernet 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 |

## Alarm Output

Beim Alarm Output Menü wird der E-Mail Server konfiguriert, welcher die Warnmeldungen empfangen soll. Wird ein Alarm ausgelöst, wird vom Router eine Nachricht generiert und an den E-Mail Server gesendet.




| 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 |
| 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 |

## Alarm Map

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

| Output Type | Console ☑ | Email ☐ |
|---|---|---|
| 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 | ☑ | ☐ |

## Log

### Show Log

Im Log Menü werden die aktuellen Mitteilungen des Routers ausgegeben.

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

View recent 20 Lines

| Level | Time | Content |
|---|---|---|
| | | Too many logs, old logs are not displayed. Please download log file to check more logs! |
| info | Mar 9 09:47:06 | redial[817]: receive disconnect command, hangup! |
| info | Mar 9 09:47:06 | pppd[911]: Hangup (SIGHUP) |
| info | Mar 9 09:47:06 | pppd[911]: Connect time 63.7 minutes. |
| info | Mar 9 09:47:06 | pppd[911]: Sent 7716448 bytes, received 121670509 bytes. |
| notice | Mar 9 09:47:06 | pppd[911]: Connection terminated. |
| info | Mar 9 09:47:06 | ih_updown[994]: wan1 down: ppp1 37.84.187.183 < = > 1.1.1.3 |
| info | Mar 9 09:47:06 | ih_updown[994]: Bytes sent: 7716448 |
| info | Mar 9 09:47:06 | ih_updown[994]: Bytes recevid: 121670509 |
| info | Mar 9 09:47:06 | chat[997]: send (\K^M) |
| info | Mar 9 09:47:06 | chat[997]: send (+++ATH^M) |
| info | Mar 9 09:47:07 | pppd[911]: Serial link disconnected. |
| info | Mar 9 09:47:08 | pppd[911]: set exit timer |
| info | Mar 9 09:47:08 | pppd[911]: Exit. |
| info | Mar 9 09:47:08 | redial[817]: child pppd exited! |
| info | Mar 9 09:47:09 | redial[817]: receive connect command, Go! |
| info | Mar 9 09:47:12 | redial[817]: Interface Cellular1, changed state to down |
| info | Mar 9 09:47:12 | redial[817]: waiting 10 seconds for redial |
| info | Mar 9 09:47:12 | dnsmasq[916]: read /etc/hosts - 1 addresses |
| info | Mar 9 09:47:12 | dnsmasq[916]: using nameserver 8.8.8.8#53 |
| info | Mar 9 09:47:15 | redial[817]: receive connect command, Go! |

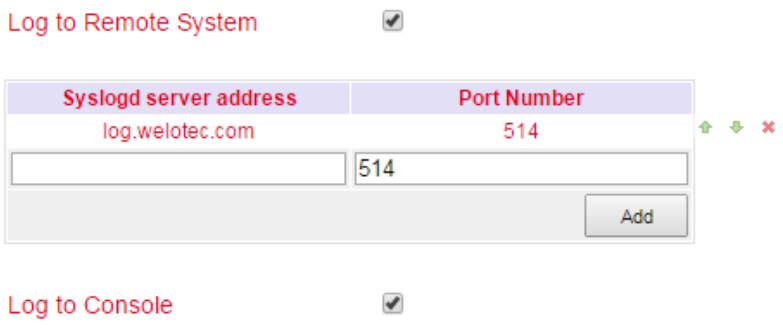
Clear Log | Download Log File | Download Diagnose Data
Clear History Log | Download History Log

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

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

### System Log

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




Unter "Syslogd server adress" wird der Hostname des Syslog Server (FQDN) oder IP Adresse angegeben.
Der Port 514 ist typisch für Syslogserver.

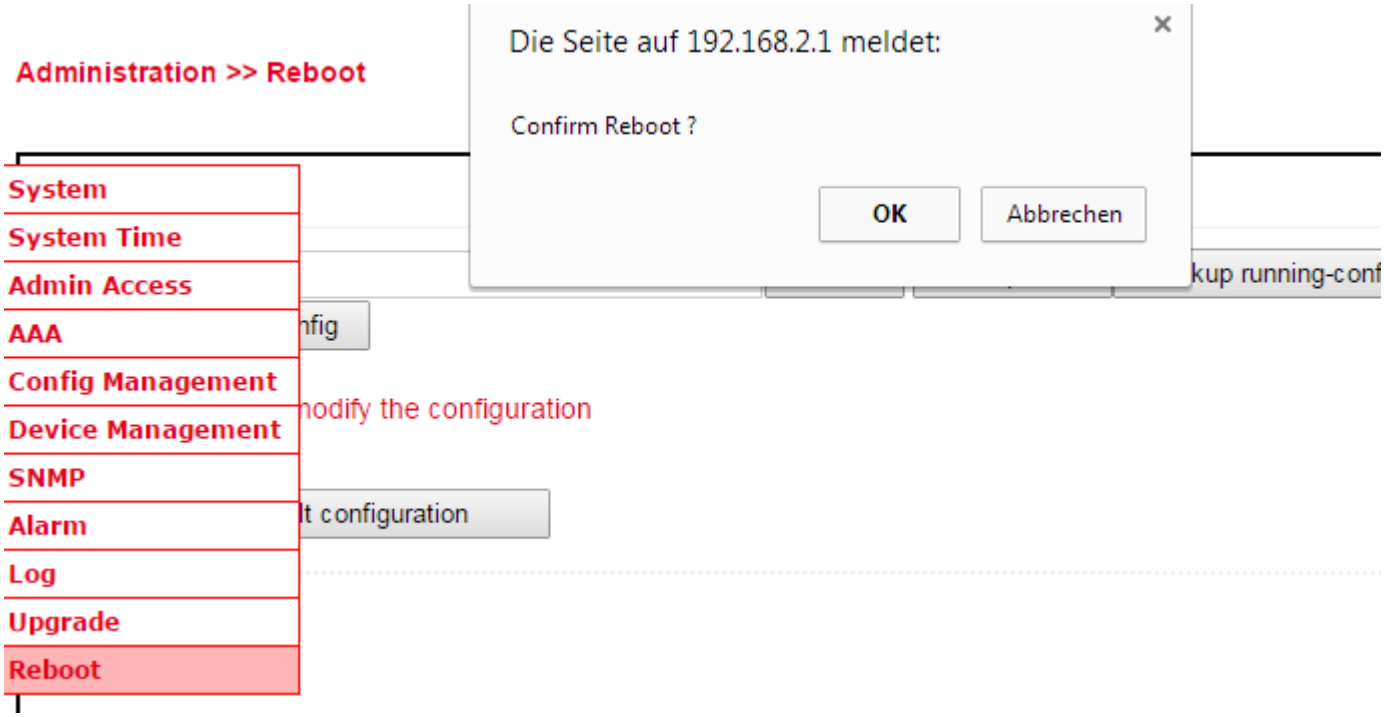
## Upgrade

Im Upgrade Menü können Firmwareupdates des Routers durchgeführt. Ein Firmwareupdate kann neue Funktionen enthalten oder auch Fehler beseitigen.

Unter Browse wählt man die Firmware Datei aus, welche man sich vorher heruntergeladen hat.
Mit einem Klick auf "Upgrade" wird die Firmware auf den Router aufgespielt.

## Reboot

Mit Reboot wird der Router neugestartet.




Durch "OK" bestätigen wird ein Neustart des Routers durchgeführt.

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

## Layer2 Switch

Nur die Versionen mit 5 Ethernet Ports (TK8X**5**X-X) unterstützen die Funktionen des Layer 2 Switches.

### Layer2 Switch Status

Im Status Menü "Layer2 Switch" wird angezeigt, welche Netzwerkports (FastEthernet) verbunden sind und welchem VLAN dieser Port zugeordnet ist.

**Layer2 Switch >> Ports**

Status | Port Basic Parameters | Port Mirroring | Broadcast Storm Control

| Port | Link Status | PVID |
|---|---|---|
| FE1/1 | LINK DOWN | 1 |
| FE1/2 | LINK UP | 1 |
| FE1/3 | LINK DOWN | 1 |
| FE1/4 | LINK DOWN | 1 |

Port zeigt den Netzwerkport an. FE1/1 steht für den Netzwerkport FastEthernet 1/1.
Link Status gibt an, ob der Netzwerkport verbunden ist. LINK DOWN = getrennt. LINK UP = verbunden.
PVID gibt die VLAN ID des Netzwerkports an.

### Port Basic Parameters

Im Menü "Port Basic Parameters" kann man die Netzwerkports administrieren.

| Port | Admin Status | Speed | Duplex |
|---|---|---|---|
| FE1/1 | shutdow | 100 | auto |
| FE1/2 | up | auto | auto |
| FE1/3 | up | 10 | auto |
| FE1/4 | up | auto | auto |

Unter "**Port**" stehen die verfügbaren FastEthernet Netzwerkports. In diesem Beispiel 4 Ports.

| | |
|---|---|
| FE1/1 | FastEthernet Port 1 |
| FE1/2 | FastEthernet Port 2 |
| FE1/3 | FastEthernet Port 3 |
| FE1/4 | FastEthernet Port 4 |

Unter "**Admin Status**" kann man den Port aktivieren oder deaktivieren.

| | |
|---|---|
| Up | Port ist aktiviert |
| Shutdown | Port ist deaktiviert |

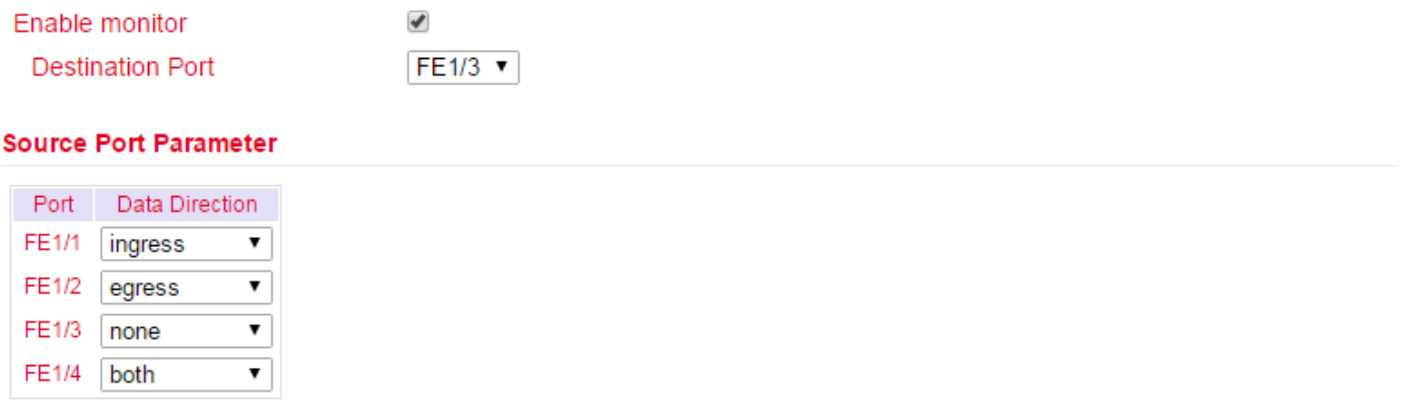
Unter "**Speed**" kann man manuell festlegen mit welcher Geschwindigkeit der Port arbeitet.

| Auto | Geschwindigkeit wird automatisch ausgehandelt |
|---|---|
| 100 | 100 Megabit pro Sekunde (MBit's) |
| 10 | 10 Megabit pro Sekunde (MBit's) |

Unter "**Duplex**" kann man die Optionen **Auto**, **full** und **half** auswählen.

| | |
|---|---|
| Auto | Automatische Aushandlung des Duplex Modus |
| full | Bei full duplex können die Teilnehmer gleichzeitig senden und empfangen |
| half | Bei half duplex wird abwechselnd gesendet oder empfangen |

## Port Mirroring




## Broadcast Storm Control

Ein **Broadcast** *in einem Netzwerk* ist eine Nachricht, bei der Datenpakete von einem Punkt aus an alle Teilnehmer eines Nachrichtennetzes übertragen werden.
Ein **Broadcast-Sturm** ist die starke Anhäufung von Broadcasts in einem Netzwerk und kann das Netzwerk stark beeinträchtigen und zum Erliegen bringen.

Um Broadcast Stürme im Netzwerk über den Router zu kontrollieren, kann man die Bandbreite in Kilobyte per Sekunde (kbps) auf den Netzwerkports begrenzen.

Storm Rate 1000 kbps

**Port**

| Port | EnableStorm Control |
|---|---|
| FE1/1 | ☐ |
| FE1/2 | ☐ |
| FE1/3 | ☑ |
| FE1/4 | ☐ |

"**Storm Rate**" in kbps z.B. auf 1000 kbps stellen und den Haken bei dem Netzwerkport FastEthernet 1/1 bis 1/4 setzen, auf welchem der Broadcaststurm kontrolliert werden soll.

# Network

## Ethernet

### Ethernet Status

Die Statusseite zeigt den aktuellen Status des Netzwerkports FastEthernet 0/1 an.

**Fastethernet 0/1**

| | |
|---|---|
| Connection Type | Static IP |
| IP Address | 192.168.1.1 |
| Netmask | 255.255.255.0 |
| Gateway | 0.0.0.0 |
| DNS | 0.0.0.0 |
| MTU | 1500 |
| Status | Up |
| Connection time | 0 day, 00:06:26 |
| Remaining Lease | |
| Description | |

### Fast Ethernet 0/1

Der FastEthernet 0/1 Port bietet drei Verbindungsmethoden.

- Automatisch: Konfiguration als DHCP Client, der Port bezieht in diesem Fall die IP Adresse vom DHCP Server. Konfiguration über das Menü "Netzwerk" "DHCP" "DHCP Client".
- PPPoE: Konfiguration als PPPoE Client (Point-to-Point Protocol over Ethernet). Typischerweise DSL Einwahl über einen Internet Provider. Konfiguration über das Menü "Netzwerk" "ADSL Dialup (PPPoE)"
- Manuell: Statische Konfiguration der IP Adresse (feste IP Adresse)

Hier kann man manuell statisch eine feste IP Adressse für den Netzwerkport FastEthernet 0/1 konfigurieren.

| | |
|---|---|
| Primary IP | 192.168.1.1 |
| Netmask | 255.255.255.0 |
| MTU | 1500 |
| Speed/Duplex | Auto Negotiation ▼ |
| Track L2 State | ☐ |
| Description | |

**Multi-IP Settings**

| Secondary IP | Netmask |
|---|---|
| | |

Add

| Parameter | Beschreibung | Werkseinstellung |
|---|---|---|

| | | |
|---|---|---|
| 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:<br>• Auto Negotiation: Automatische Aushandlung der Geschwindigkeit<br>• 100M Full-duplex: 100 Megabit Voll-duplex<br>• 100M Half-duplex: 100 Megabit Halb-duplex<br>• 10M Full-duplex: 10 Megabit Voll-duplex<br>• 10M Half-duplex: 10 Megabit Halb-duplex | Auto |
| Track L2 State | Haken gesetzt: Port Status bleibt nach dem Getrennt werden administrativ getrennt (Down)<br>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 kann eine zweite IP Adresse für den FastEthernet 0/1 Port vergeben werden.

| **Multi IP Settings** | |
|---|---|
| Secondary IP | Netmask |

## VLAN

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 und das, obwohl die Teilnetze an gemeinsamen Switches angeschlossen sein können.

### VLAN Trunk

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

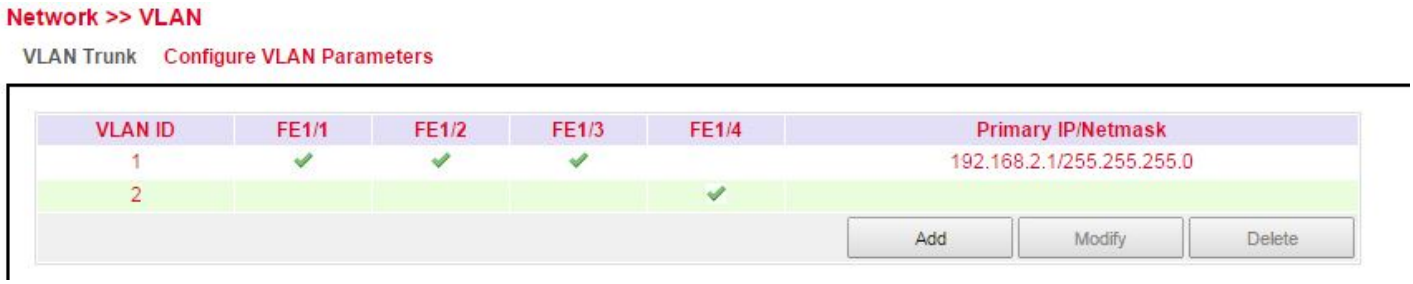
| Port | Mode | Native VLAN |
|---|---|---|
| FE1/1 | Trunk | 1 |
| FE1/2 | Access | 1 |
| FE1/3 | Access | 1 |
| FE1/4 | Trunk | 2 |

NOTE:
Native VLAN is only valid in trunking mode

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 kann man den FastEthernet Ports VLAN IDs zwischen 1-4000 zuweisen.

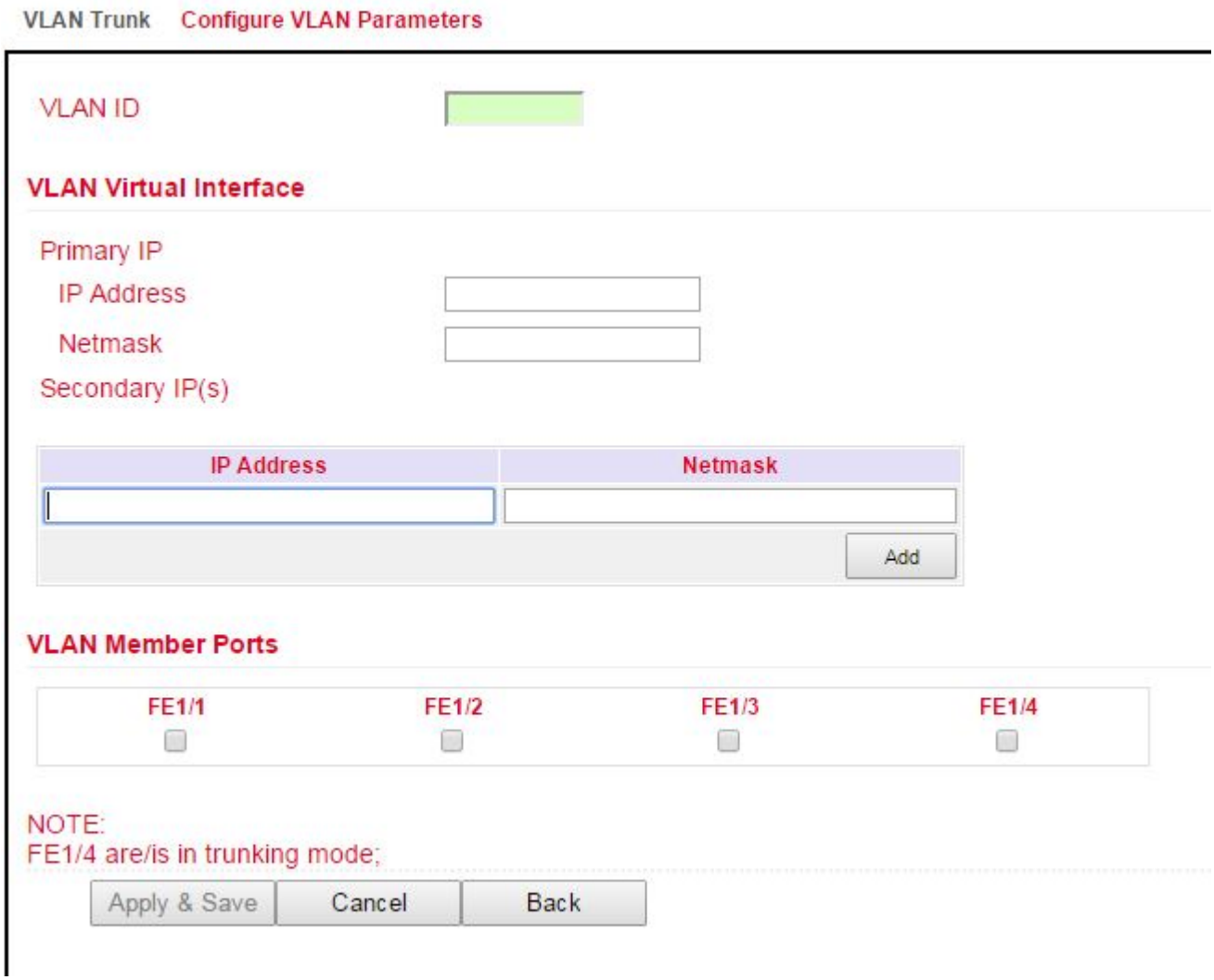
### Configure VLAN Parameters

Im Menü "Configure VLAN Parameters" kann man die Zuweisung von VLANs zu FastEthernet Ports einfach und ändern.




Die vorhandenen VLANs kann man durch "Modify" einfach den FastEthernet Ports zuweisen und ändern.

Wenn man auf "Add" klickt (Abb. 1) kann man ein neues VLAN erstellen und einem oder mehreren Fastethernet Ports zuweisen (Abb. 2).




Man vergibt eine neue VLAN ID (z.B. 3) und kann dann eine Primäre IP Adresse vergeben. Bei Bedarf kann eine zweite IP Adresse (Secondary IP(s)) eingerichtet.

Unter "VLAN Member Ports" wird durch Setzen des Haken in der Checkbox dem VLAN ein FastEthernet Port zugewiesen.
Mit "Apply & Save" wird die Konfiguration gespeichert.

## Cellular

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

### Cellular Status

Unter Network / Cellular / Cellular Status befindet sich eine Übersicht über den aktuellen Status.

Entscheidend ist der Register Status, Network Type und unter Network die IP Adresse.

**Modem**

| | |
|---|---|
| Active SIM | SIM 1 |
| IMEI Code | 860461024084629 |
| IMSI Code | 262010053296632 |
| Phone Number | +491719662843 |
| Signal Level | (29 asu -55 dBm) |
| Register Status | registered |
| Operator | T-Mobile |
| Network Type | 4G (LTE) |
| LAC | FFFE |
| Cell ID | 1E13100 |

**Network**

| | |
|---|---|
| Status | Connected |
| IP Address | 37.84.145.113 |
| Netmask | 255.255.255.255 |
| Gateway | 1.1.1.3 |
| DNS | 10.74.210.210 10.74.210.211 |
| MTU | 1500 |
| Connection time | 0 day, 00:27:12 |

Connect Disconnect

⚠ 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 vorhanden ist oder ein Eintrag wie 10.11.12.13. ⚠

⚠ 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. ⚠

### Cellular Configuration

Unter Network / Cellular / Cellular Configuration können die Einstellungen für den Zugriff über das Mobilfunknetz gemacht werden.

| | | |
|---|---|---|
| Enable | ☑ | |
| | SIM1 | SIM2 |
| Profile | 1 | auto |
| Roaming | ☑ | ☑ |
| PIN Code | | |
| Network Type | Auto | |
| Static IP | ☐ | |
| Connection Mode | Always Online | |
| Redial Interval | 10 s | |
| ICMP Detection Server | 8.8.8.8 | |
| | 8.8.4.4 | |
| 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

| Parameter | Beschreibung | Werkseinstellungen |
|---|---|---|
| Enable | Aktivieren oder Deaktivieren der Mobilfunkverbindung | Aktivert |
| Profile | APN Profil für SIM Karte 1 und SIM Karte 2 | Auto / Auto<br>Automatische Selektion des APN basierend auf der SIM Karte. |
| Roaming | Aktiveren oder Deaktivieren ob die SIM Karte Roaming erlauben soll.<br>⚠ Ob diese Funktion funktioniert ist abhängig vom Provider.<br>Es kann trotz Deaktivierung zu Roaming kommen. ⚠ | Aktiviert / Aktiviert |
| PIN Code | PIN code für die SIM Karte.<br>⚠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 | ⚠ 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 | Zwei ICMP Detection Server. Ziel für den Ping zur Verbindungsüberwachung.<br>⚠️ Die IP Adressen oder DNS Namen müssen über den Router erreichbar sein und auf einen Ping antworten. ⚠️ | |
| 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 brauchen darf (Round Trip Time). | 5 Sekunden |
| ICMP Detection Max Retries | Anzahl der Wiederhohlung bei Fehlgeschlagenem ICMP Ping. | 5 |
| ICMP Detection Strict | Wenn deaktiviert, wird das Modem nur dann neu gestartet, wenn kein Datentransfer auf der Mobilfunk Schnittstelle vorhanden ist.<br>⚠️ Wenn ICMP Detection Strict aktiviert ist, wird das Modem immer nach einem fehlgeschlagenen ICMP Zyklus neu gestartet. ⚠️<br>👍 Für Anwendungen, wo es auf hohe Verfügbarkeit ankommt, sollte Strict aktiviert werden. 👍 | Deaktiviert |
| Show Advanced Options | Wenn aktiviert werden mehr Konfigurationsmöglichkeiten sichtbar. | Deaktiviert |

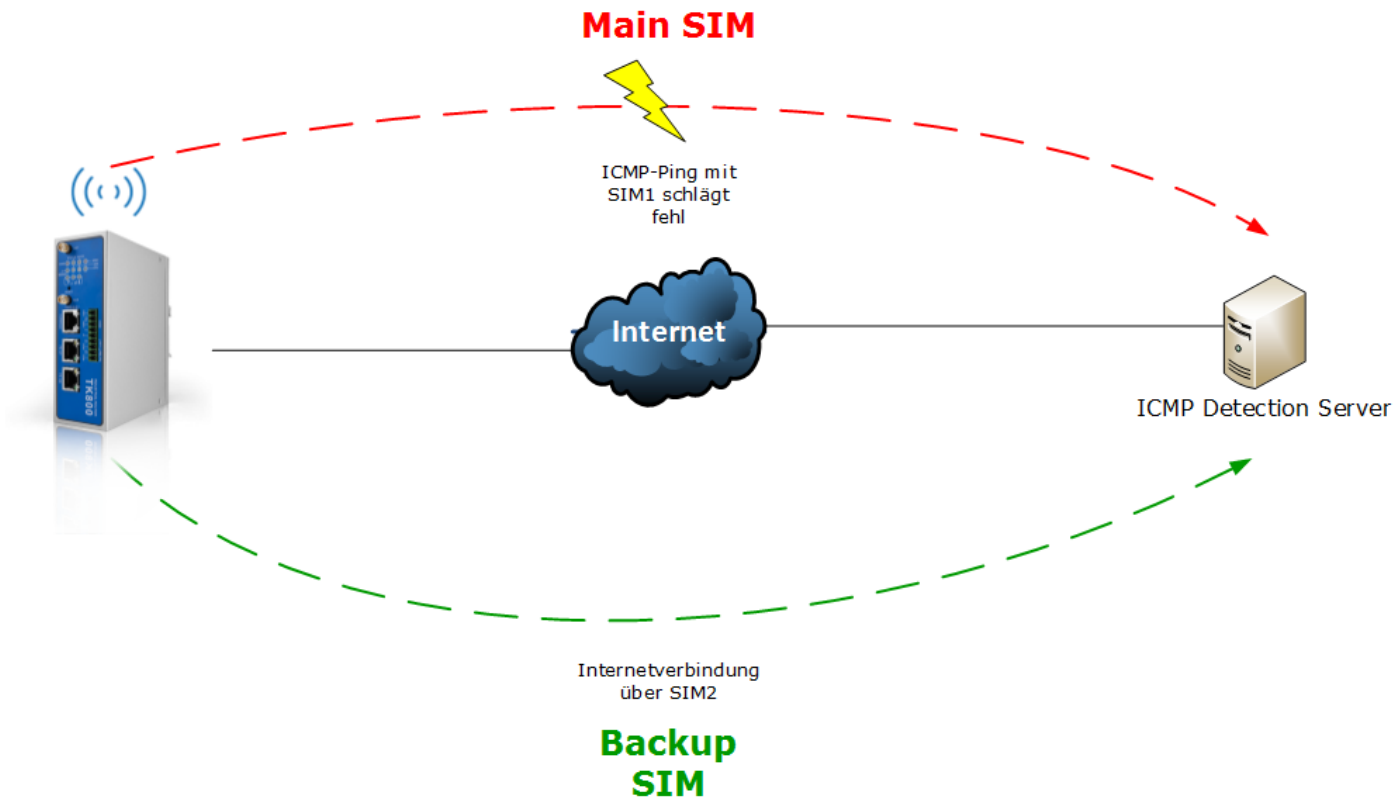
**Connect on Demand**

| | |
|---|---|
| Connection Mode | Connect On Demand ▼ |
| Triggered by Data | ☐ |
| Triggered by SMS | ☑ |

**Show Advanced Options**

| | |
|---|---|
| **Show Advanced Options** | ☑ |
| Initial Commands | |
| RSSI Poll Interval | 120 s(0: disable) |
| Dial Timeout | 120 s |
| MTU | 1500 |
| MRU | 1500 |
| Use default asyncmap | ☐ |
| Use Peer DNS | ☑ |
| LCP Interval | 55 s(0: disable) |
| LCP Max Retries | 5 |
| Dual SIM Enable | ☐ |
| Debug | ☐ |
| Expert Options | |

**Dual SIM Enabled**




| | | |
|---|---|---|
| Dual SIM Enable | ☑ | |
| Main SIM | SIM1 | |
| Max Number of Dial | 5 | |
| Min Connected Time | 0 | s(0: disable) |
| CSQ Threshold | 0 / 0 | (0: disable) |
| CSQ Detect Interval | 0 / 0 | (0: disable) |
| CSQ Detect Retries | 0 / 0 | |
| Backup SIM Timeout | 0 | s(0: disable) |

## ADSL Dialup (PPPoE)

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.

### PPPoE Status

**Dialer 1**

| | |
|---|---|
| Status | Disconnected |
| IP Address | 0.0.0.0 |
| Netmask | 0.0.0.0 |
| Gateway | 0.0.0.0 |
| DNS | 0.0.0.0 |
| MTU | 1460 |
| Connection time | 0 day, 00:00:00 |

## ADSL Dialup (PPPoE) Configuration

**Dial Pool**

| Pool ID | Interface |
|---|---|
| 1 | fastethernet 0/1 |
| 2 | fastethernet 0/1 |

Add

**PPPoE List**

| Enable | ID | Pool ID | Authentication Type | Username | Password | Local IP Address | Remote IP Address | Keepalive Interval | Keepalive Retry | Debug |
|---|---|---|---|---|---|---|---|---|---|---|
| ✔ | 1 | 1 | Auto | welotec | ****** | | | 120 | 3 | No |
| ☑ | 2 | | Auto | | | | | 120 | 3 | ☐ |

Add

# Loopback

## Loopback Configuration

| | |
|---|---|
| IP Address | 127.0.0.1 |
| Netmask | 255.0.0.0 |

**Multi-IP Settings**

| IP Address | Netmask |
|---|---|
| | |

Add

## DHCP

### DHCP Status

| Interface | MAC Address | IP Address | Host | Lease |
|---|---|---|---|---|
| Vlan1 | 8C:89:A5:F9:38:14 | 192.168.2.36 | JOSPC | 0 day, 23:30:20 |

### DHCP Server

**DHCP Server**

| Enable | Interface | Starting Address | Ending Address | Lease(Minutes) |
|---|---|---|---|---|
| ✔ | fastethernet 0/1 | 192.168.1.2 | 192.168.1.100 | 1440 |
| ✔ | vlan 1 | 192.168.2.2 | 192.168.2.100 | 1440 |
| ☐ | vlan 2 | | | 1440 |

Add

NOTE:DHCP lease time 0 indicates infinite.

DNS Server Edit

Windows Name Server (WINS)

**Static IP Settings**

| MAC Address | IP Address |
|---|---|
| 0000.0000.0000 | |

Add

### DHCP Relay

Enable ☑

DHCP Server 1

DHCP Server 2

DHCP Server 3

DHCP Server 4

Source IP

### DHCP Client

Fastethernet 0/1 ☐
Vlan 1 ☐
Vlan 2 ☐

## DNS

### DNS Server

| | |
|---|---|
| Primary DNS | 8.8.8.8 |
| Secondary DNS | 8.8.4.4 |

### DNS Relay

**Static [Domain Name <=> IP addresses] Pairing**

| Host | IP Address 1 | IP Address 2 |
|---|---|---|
| | | |

Add

## DDNS

### DDNS Configuration

**DDNS Method List**

| Method Name | Service Type | Url | Username | Password | Hostname |
|---|---|---|---|---|---|
| welotec | NoIP | | welotec | ******** | router.welotec-router.com |
| | | | | | |

Add

**Specify A Method To Interface**

| Interface | Method |
|---|---|
| cellular 1 | welotec |
| dialer 1 | |

Add

Apply & Save Cancel

### DDNS Status

**Cellular 1**

| | |
|---|---|
| Method | welotec |
| Hostname | router.welotec-router.com |
| IP Address | 37.84.145.113 |
| Last Update | 2015-03-09 10:43:35, 37.84.145.113 |
| Last Response | 2015-03-09 10:43:35, IP address is current. No update required. |

# SMS

## Einleitung

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.

## Statusabfrage / Neustart

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

| | |
|---|---|
| Enable | ☑ |
| Mode | TEXT |
| Poll Interval | 120 s(0: disable) |

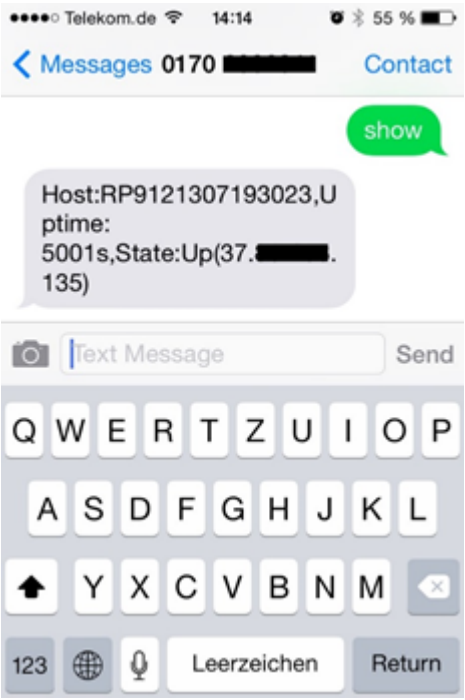
**SMS Access Control**

| ID | Action | Phone Number | DI Inform SMS |
|---|---|---|---|
| 1 | permit | +4917012345678 | ☑ |
| 2 | permit | | ☐ |
| | | | Add |

Tips:After enabled DI Inform SMS, router will send SMS when DI status changed.

3. Geben Sie in die Tabelle **SMS Access Control** die Telefonnummern ein, welche SMS an den Router senden dürfen 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



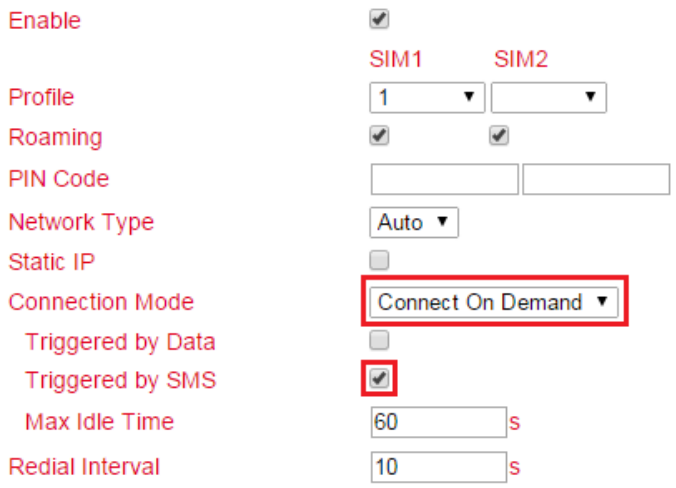

Wird eine SMS mit dem Inhalt **reboot** an den Router gesendet, so startet dieser neu. Man kann diesen Prozess auch im Log des Routers verfolgen.

| | | |
|---|---|---|
| info | Jan 1 01:59:13 | redial[822]: receive a sms from +49[redacted] |
| info | Jan 1 01:59:13 | smsd[869]: receive reboot sms! |
| notice | Jan 1 01:59:13 | systools[1492]: system is rebooting! |

## 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. 5)

| | | |
|---|---|---|
| info | Jan 1 01:40:35 | redial[822]: receive a sms from +49[redacted] |
| info | Jan 1 01:40:35 | redial[822]: receive disconnect command, hangup! |
| info | Jan 1 01:40:35 | pppd[2151]: Hangup (SIGHUP) |

**cellular 1 ppp up** - stellt die Internetverbindung her (s. Abb. 6)

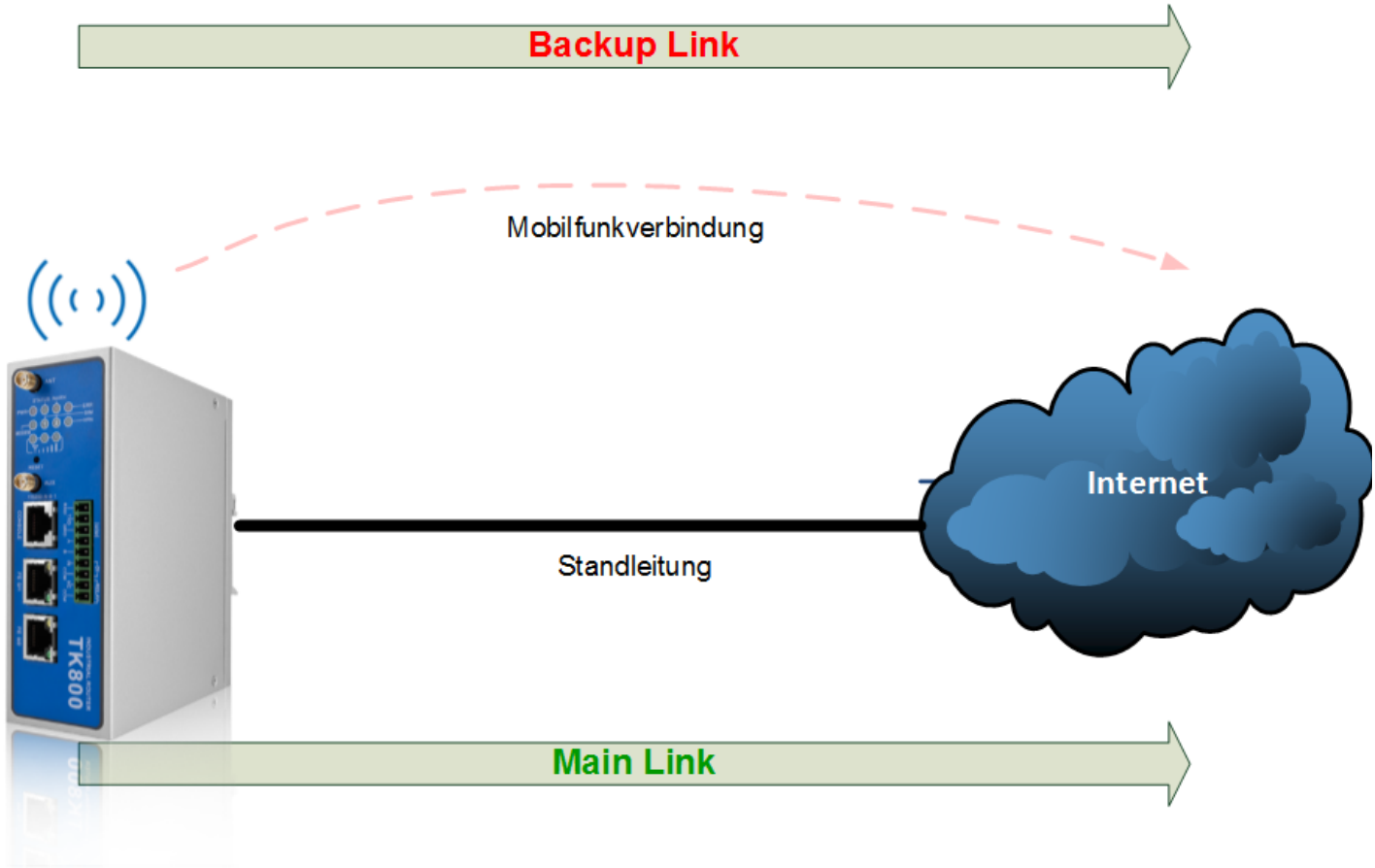
| | | |
|---|---|---|
| info | Jan 1 01:33:13 | redial[822]: receive a sms from +49[redacted] |
| info | Jan 1 01:33:13 | redial[822]: receive connect command, Go! |
| info | Jan 1 01:33:13 | pppd[906]: got user command, starting the link... |

## Link Backup

Mit dem TK800 ist es möglich, zwei verschiedene Internetverbindungen (kabel gebunden 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 kabel gebundene (Ethernet, DHCP) als primäre und Mobilfunk (4G LTE) als sekundäre Internetverbindung verwendet.

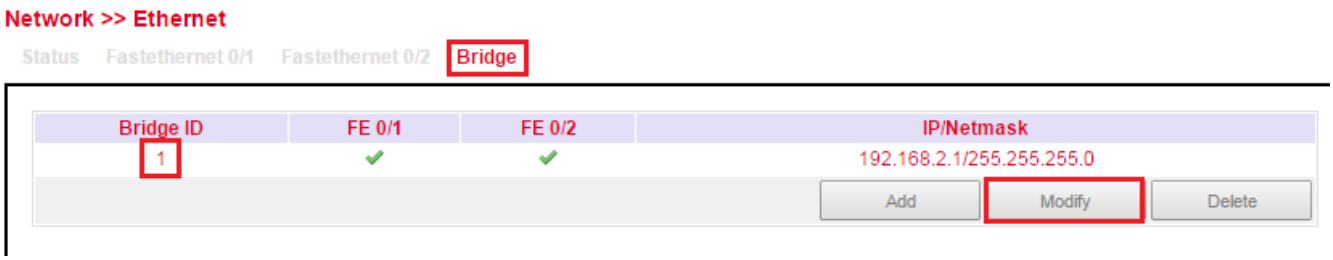



**Konfigurieren eines WAN-Ports – Bridge modifizieren (nur TK8X2-X)**

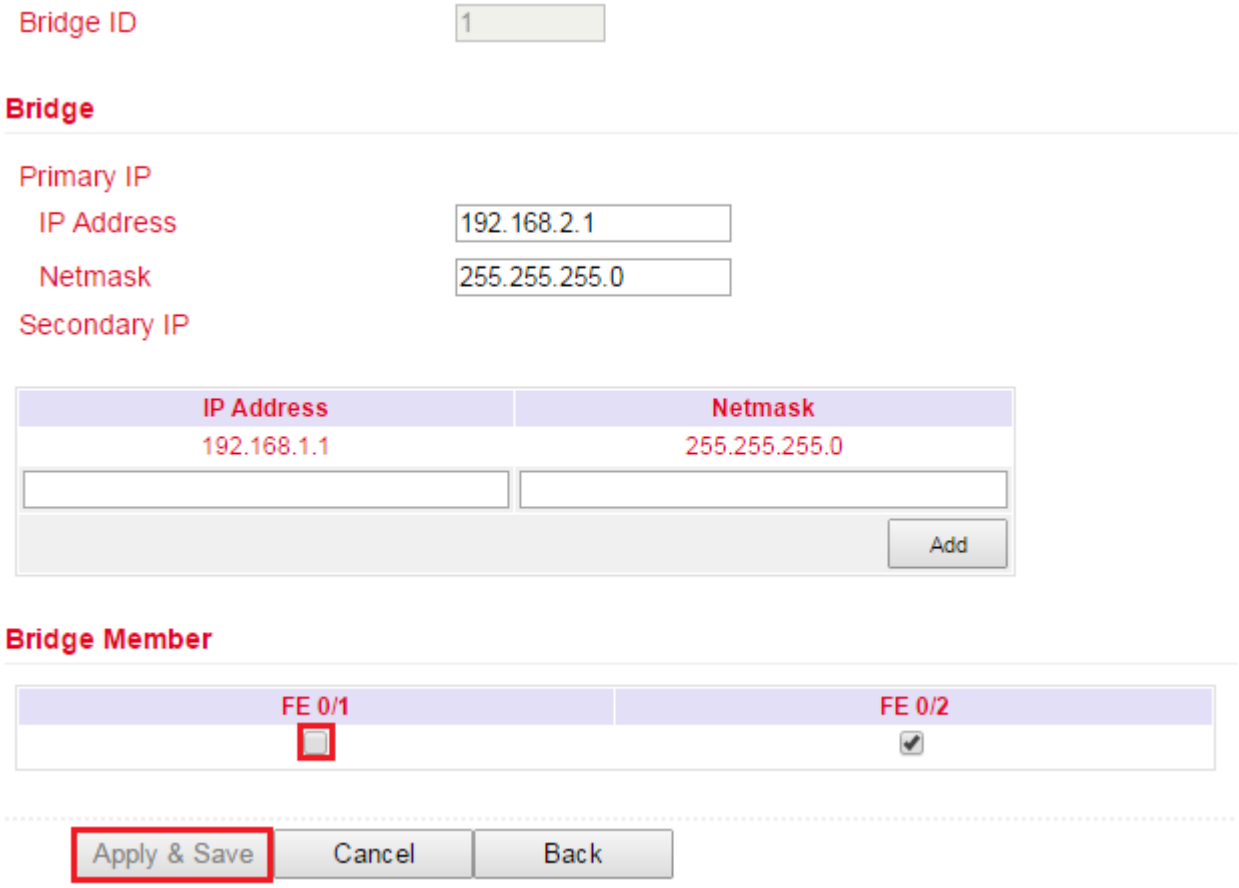
⚠ Voraussetzung für das Link Backup ist der Internetzugang über das Mobilfunknetz. Konfigurieren Sie also die Mobilfunkschnittstelle (Cellular) entsprechend, um eine Verbindung zum Internet herstellen zu können. Der Router ist für T-Mobile SIM-Karten vorkonfiguriert, hier sind also in der Regel keine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



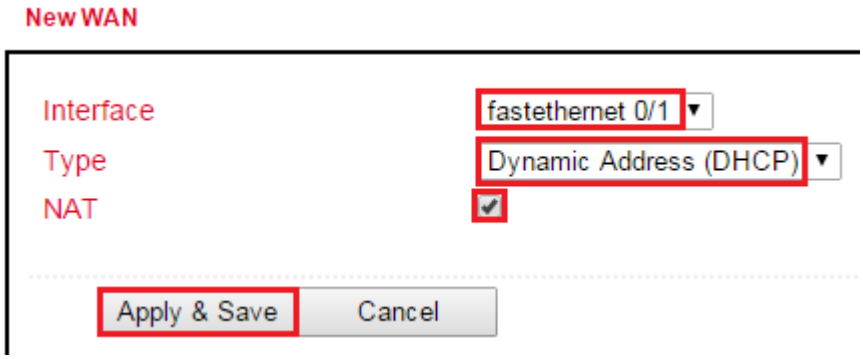

4. Entfernen Sie den Haken für das Interface FE 0/1 und bestätigen Sie die Änderung mit Apply & Save



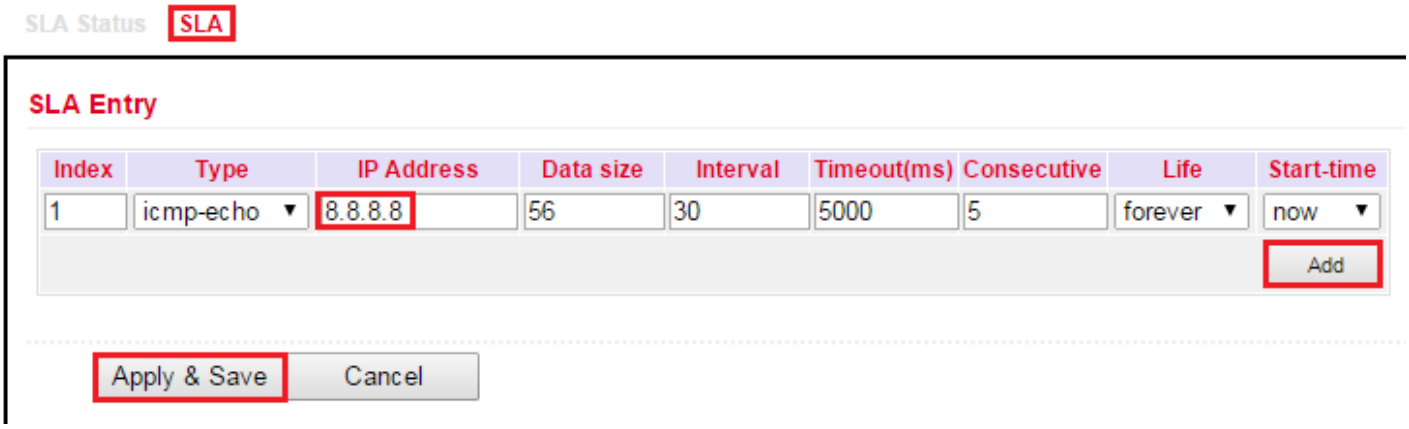

**Konfigurieren eines WAN-Ports**

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

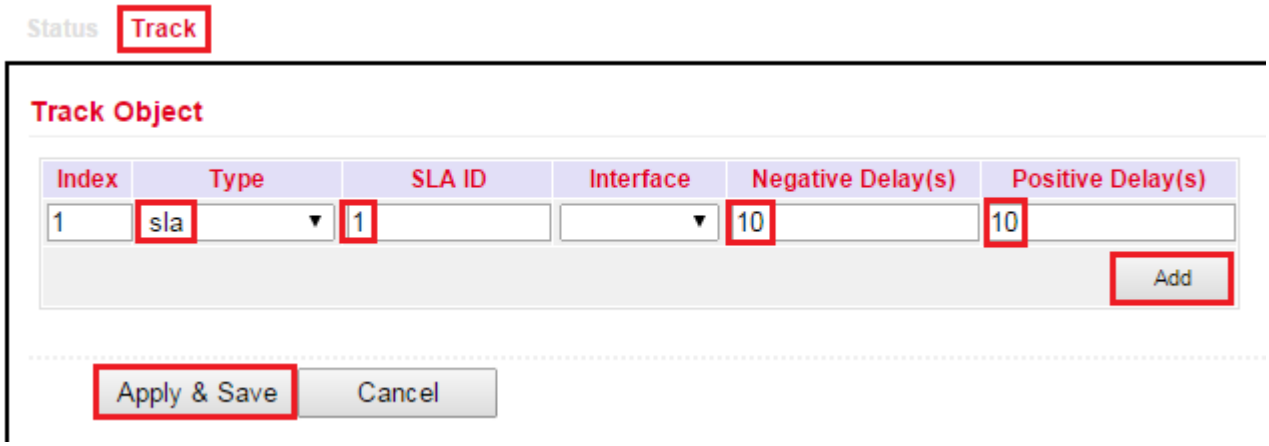
- im Menü Wizard kann über den Unterpunkt New WAN ein neuer WAN-Port konfiguriert werden
- als Interface wird der gerade von der Bridge gelöste Ethernet-Port (FE 0/1) angegeben, exemplarisch wird außerdem DHCP für den Port verwendet
- NAT muss aktiviert werden, wenn die angeschlossenen Geräte eine Verbindung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



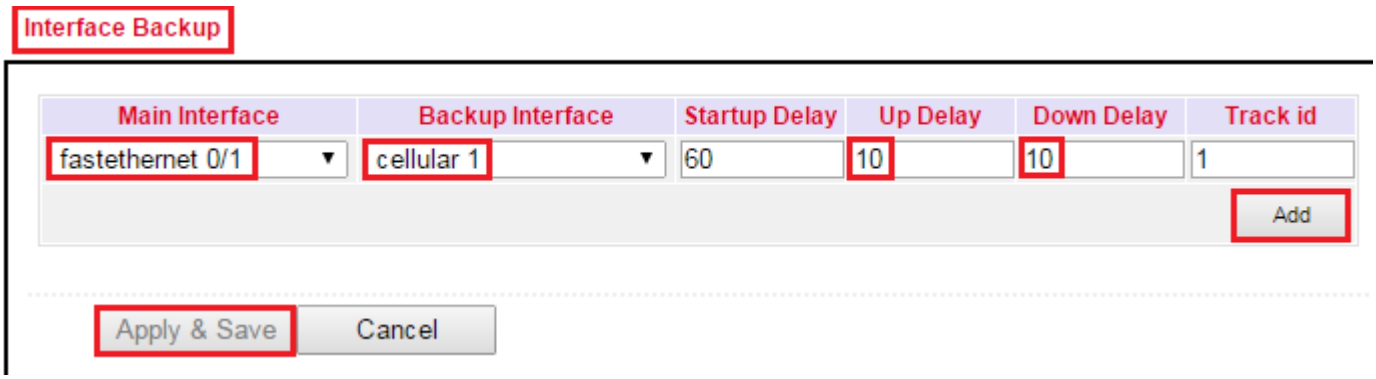
- im nächsten Schritt wird das ICMP-Programm (SLA) konfiguriert
- unter IP Address sollte eine pingbare IP-Adresse mit hoher Verfügbarkeit eingetragen werden (Anm.: In diesem Beispiel wurde 8.8.8.8 – ein Server von Google – eingetragen, da diese Adresse eine sehr hohe Verfügbarkeit vorweist.)
- alle 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 Leitung als Haupt- und welche die Backup-Leitung fungiert, wird das Interface Backup eingerichtet
- konfiguriert wird dies wie in folgendem 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 in folgendem 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

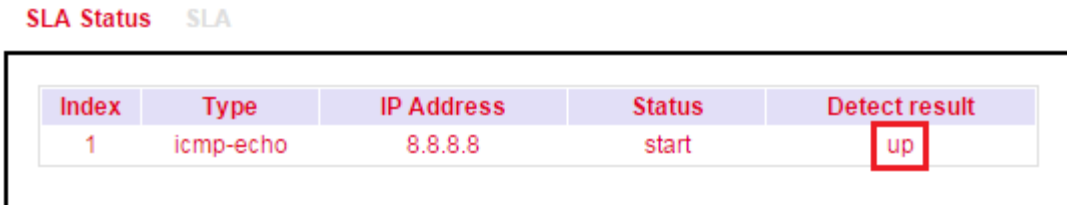
Beschreibung der Konfigurationselemente:

| | |
|---|---|
| **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 |

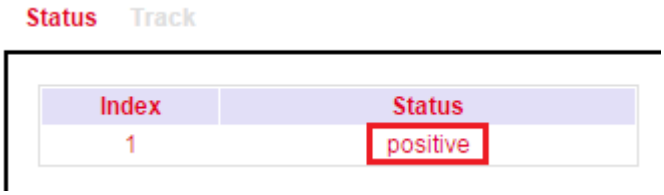
**Hauptleitung funktioniert (Internetverbindung über WAN)**

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

**Modem**

| | |
|---|---|
| Active SIM | SIM 1 |
| IMEI Code | 359998041175797 |
| IMSI Code | 262010053294973 |
| Phone Number | |
| Signal Level | (14 asu -85 dBm) |
| Register Status | registered |
| Operator | T-Mobile |
| Network Type | 3G |
| LAC | 16C9 |
| Cell ID | 07F1339 |

**Network**

| | |
|---|---|
| Status | Disconnected |
| IP Address | 0.0.0.0 |
| Netmask | 0.0.0.0 |
| Gateway | 0.0.0.0 |
| DNS | 0.0.0.0 |
| MTU | 1500 |
| Connection time | 0 day, 00:00:00 |

4. Status der WAN-Verbindung (Ethernet)

Status Fastethernet 0/1 Fastethernet 0/2 Bridge

**Fastethernet 0/1**

| | |
|---|---|
| Connection Type | Dynamic Address (DHCP) |
| IP Address | 192.168.111.101 |
| Netmask | 255.255.255.0 |
| Gateway | 192.168.111.1 |
| DNS | 192.168.111.254 |
| MTU | 1500 |
| Status | Up |
| Connection time | 0 day, 00:04:44 |
| Remaining Lease | 7 days, 23:55:16 |

5. Routing-Tabelle

Route Table Static Routing

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 | |
| S | 8.8.8.8 | 255.255.255.255 | 192.168.111.1 | fastethernet 0/1 | 1/0 | |
| C | 127.0.0.0 | 255.0.0.0 | | loopback 1 | 0/0 | |
| C | 192.168.1.0 | 255.255.255.0 | | bridge 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

SLA Status SLA

| Index | Type | IP Address | Status | Detect result |
|---|---|---|---|---|
| 1 | icmp-echo | 8.8.8.8 | start | down |

2. Track-Status

Status Track

| Index | Status |
|---|---|
| 1 | negative |

3. Status der Mobilfunkverbindung

Status Cellular

**Modem**

| | |
|---|---|
| Active SIM | SIM 1 |
| IMEI Code | 359998041175797 |
| IMSI Code | 262010053294973 |
| Phone Number | |
| Signal Level | (18 asu -77 dBm) |
| Register Status | registered |
| Operator | T-Mobile |
| Network Type | 3G |
| LAC | 16C9 |
| Cell ID | 07F7098 |

**Network**

| | |
|---|---|
| Status | Connected |
| IP Address | 37.84.44.240 |
| Netmask | 255.255.255.255 |
| Gateway | 1.1.1.3 |
| DNS | 10.74.210.210 10.74.210.211 |
| MTU | 1500 |
| Connection time | 0 day, 00:01:32 |

4. Routing-Tabelle

Route Table Static Routing

Type: All

| Type | Destination | Netmask | Gateway | Interface | Distance/Metric | Time |
|---|---|---|---|---|---|---|
| S | 0.0.0.0 | 0.0.0.0 | 1.1.1.3 | cellular 1 | 1/0 | |
| C | 1.1.1.3 | 255.255.255.255 | | cellular 1 | 0/0 | |
| S | 8.8.8.8 | 255.255.255.255 | 192.168.111.1 | fastethernet 0/1 | 1/0 | |
| C | 127.0.0.0 | 255.0.0.0 | | loopback 1 | 0/0 | |
| C | 192.168.1.0 | 255.255.255.0 | | bridge 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 | |

## SLA

### SLA Configuration

**SLA Entry**

| Index | Type | IP Address | Data size | Interval | Timeout(ms) | Consecutive | Life | Start-time |
|---|---|---|---|---|---|---|---|---|
| 1 | icmp-echo | 8.8.8.8 | 56 | 30 | 5000 | 5 | forever | now |
| 2 | icmp-echo | 1.2.3.4 | 56 | 30 | 5000 | 5 | forever | now |
| 3 | icmp-echo | | 56 | 30 | 5000 | 5 | forever | now |

Add

## SLA Status

| Index | Type | IP Address | Status | Detect result |
|---|---|---|---|---|
| 1 | icmp-echo | 8.8.8.8 | start | up |
| 2 | icmp-echo | 1.2.3.4 | start | down |

# Track

## Status Track

| Index | Status |
|---|---|
| 1 | positive |
| 2 | positive |
| 3 | negative |

## Track Configuration

**Track Object**

| Index | Type | SLA ID | Interface | Negative Delay(s) | Positive Delay(s) |
|---|---|---|---|---|---|
| 1 | interface | | cellular 1 | 10 | 10 |
| 2 | sla | 1 | | 10 | 10 |
| 3 | sla | 2 | | 10 | 10 |
| 4 | sla | 1 | | 0 | 0 |

Add

# Routing

## Route Table

Die Routing Tabelle findet man in der Navigation unter:

**Routing  Static Routing** "Reiter" **Routing Table**
und
**Routing  Dynamic Routing** "Reiter" **Routing Table.**

Route Table  RIP  OSPF  Filtering Route

Type: All

| Type | Destination | Netmask | Gateway | Interface | Distance/Metric | Time |
|---|---|---|---|---|---|---|
| S | 0.0.0.0 | 0.0.0.0 | 1.1.1.3 | cellular 1 | 1/0 | |
| C | 1.1.1.3 | 255.255.255.255 | | cellular 1 | 0/0 | |
| C | 127.0.0.0 | 255.0.0.0 | | loopback 1 | 0/0 | |
| C | 192.168.1.0 | 255.255.255.0 | | fastethernet 0/1 | 0/0 | |
| C | 192.168.2.0 | 255.255.255.0 | | vlan 1 | 0/0 | |

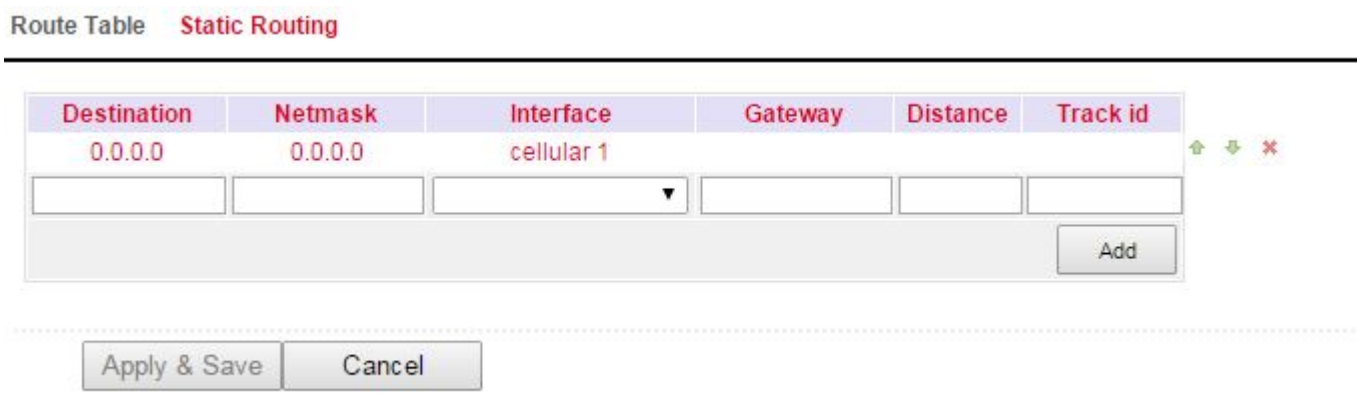
| Parameter | Beschreibung |
|---|---|
| Type | C = Connected / direkt verbundene Route, Sie werden automatisch in eine Routingtabelle übernommen, wenn ein Interface mit einer IP-Adresse konfiguriert wird<br>S = Static Route / manuell vom Administrator eingetragene Route<br>R = RIP (Routing Information Protocol) / dynamische Route durch RIP hinzugefügt<br>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.<br>Cellular 1 = Funkschnittstelle GSM<br>Loopback 1 = interne Loopback Adresse (Schleifenschaltung)<br>FastEthernet 0/1 = Netzwerkport FastEthernet 0/1 auf dem Router<br>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 |

## Static Routing

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

Statische Routing Einträge müssen gesetzt werden, wenn z.B. IPSec VPN Tunnel aufgebaut werden. Hier muss dem Router das entfernte Netz auf

der gegenüberliegenden Seite bekannt gemacht werden.




| Parameter | Beschreibung |
|---|---|
| Destination | Das Ziel ist der Zielhost, die Subnetzadresse, die Netzwerkadresse oder die Standardroute. Das Ziel für eine Standardroute ist 0.0.0.0. |
| Netzmask | 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.<br>Cellular 1 = Funkschnittstelle GSM<br>Loopback 1 = interne Loopback Adresse (Schleifenschaltung)<br>FastEthernet 0/1 = Netzwerkport FastEthernet 0/1 auf dem Router<br>VLAN 1 = Netzwerkports, welche dem VLAN 1 zugeordnet sind. |
| 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 |

## Dynamic Routing

Dynamisches Routing wird eingesetzt, um Routen automatisch vom eingesetzten Routingprotokoll steuern zu lassen. Der Vorteil des dynamischen Routing 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.

### RIP

RIP (Routing Information Protocol) ist ein dynamisches Routing Protokoll, welches mit Distance-Vector-Algortithmus arbeitet. RIP erlernt von anderen Routern dynamisch Routing Adressen 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 kürzteste Weg zum Zielnetzwerk bestimmt und genommen werden. 15 Hops sind die maximale Entfernung, die ein Weg zum Zielnetzwerk beim RIP betragen darf.

| | |
|---|---|
| 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 | ☐ |

## Disatnace/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) | ☐ |

## Interface

| Interface | Passive 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

## 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, es unterstützt im Gegensatz zu RIP mehrere gleichzeitige Verbindungswege gleicher Kosten zu einem Zeilnetz und 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.

Enable ☑

Router ID

**Route Advanced Options** ☐

**Interface**

| Interface | Network | Hello Interval | Dead Interval | Retransmit Interval | Transmit Deylay |
|---|---|---|---|---|---|
| | Broadcast | 10 | 40 | 5 | 1 |

Add

**Interface Advanced Options** ☐

**Network**

| IP Address | Netmask | Area ID |
|---|---|---|
| | | |

Add

**Area**

| Area ID | Area | No Summary | Authentication |
|---|---|---|---|
| | | ☐ | |

Add

**Area Advanced Options** ☐

**Redistribution**

| Redistribution Type | Metric | Metric Type | Route Map |
|---|---|---|---|
| connected | | | |

Add

**Redistribution Advanced Options** ☐

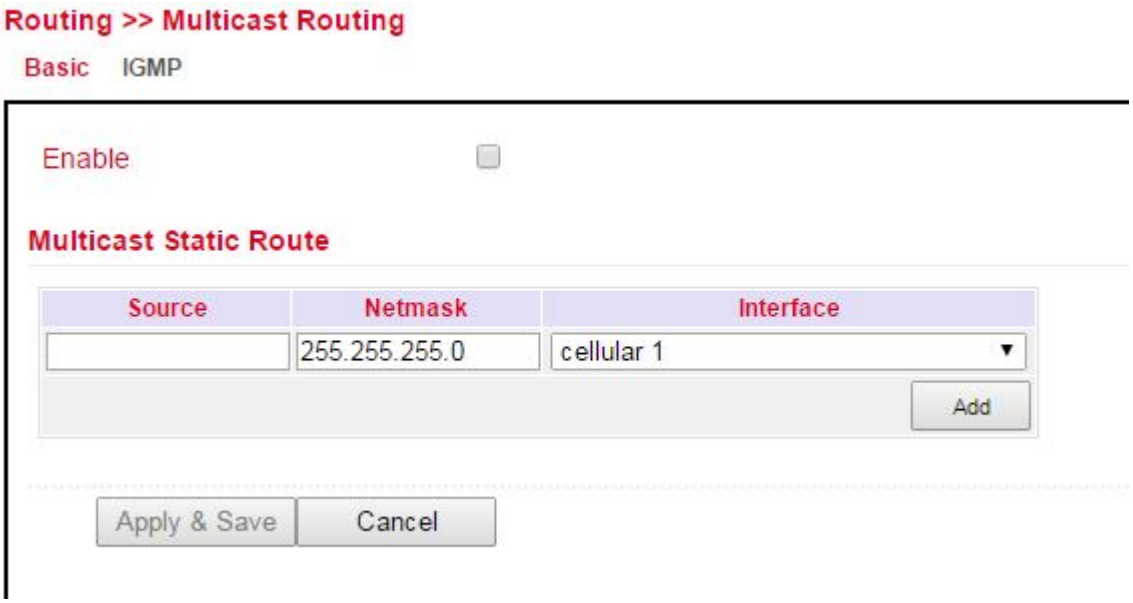
Apply & Save | Cancel

## Filtering Route

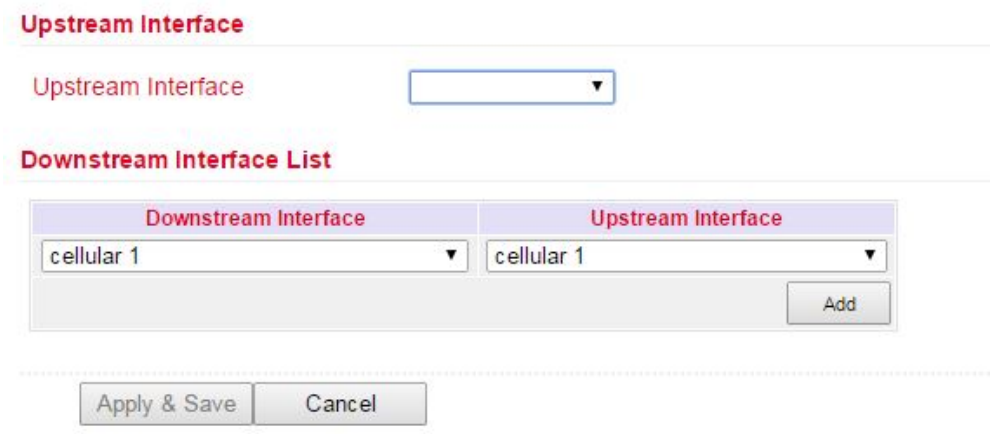
Im Menü **Routing  Dynamic Routing** "Reiter" **Filtering Route** können folgend Einstellungen vorgenommen werden:

## 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.




Um Multicastrouting zu benutzen muss bei **Enable** der Haken gesetzt ist. Dann muss als **Source** die Quelle angegeben werden, sowie die Netzmaske und die Schnittstelle.




IGMP Konfiguration

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.

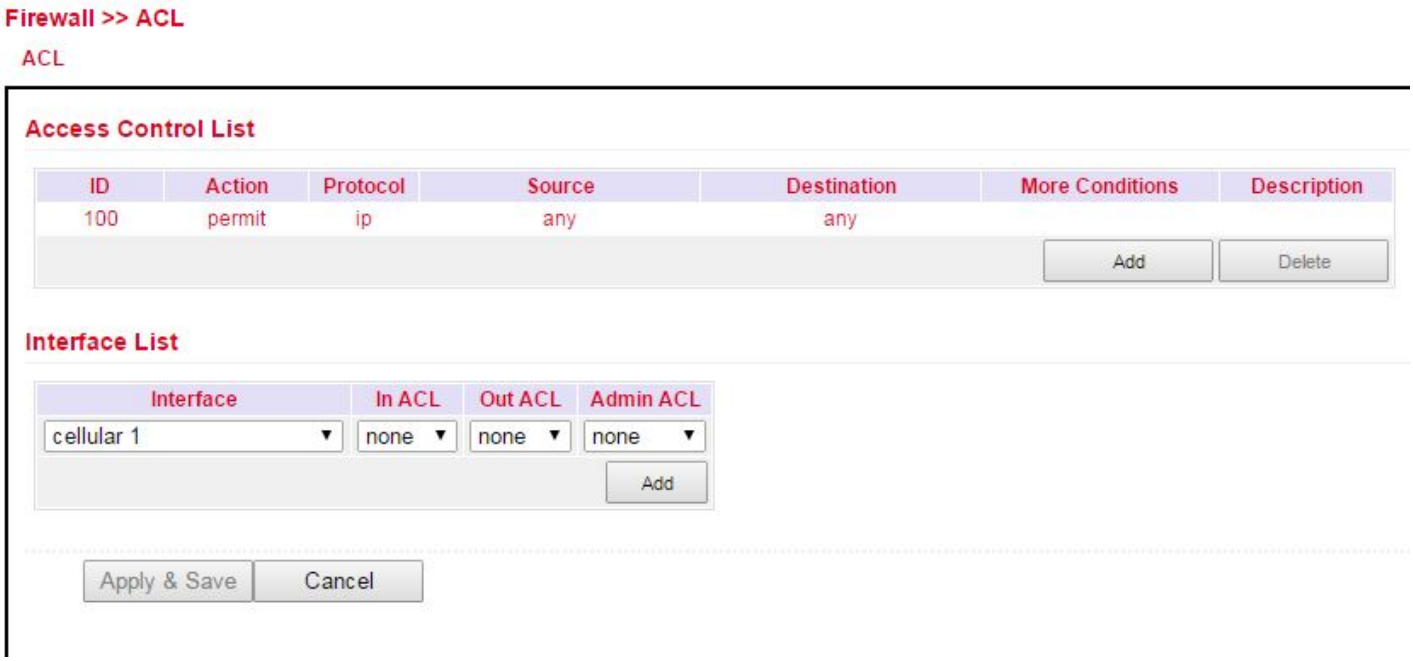
# Firewall

## ACL

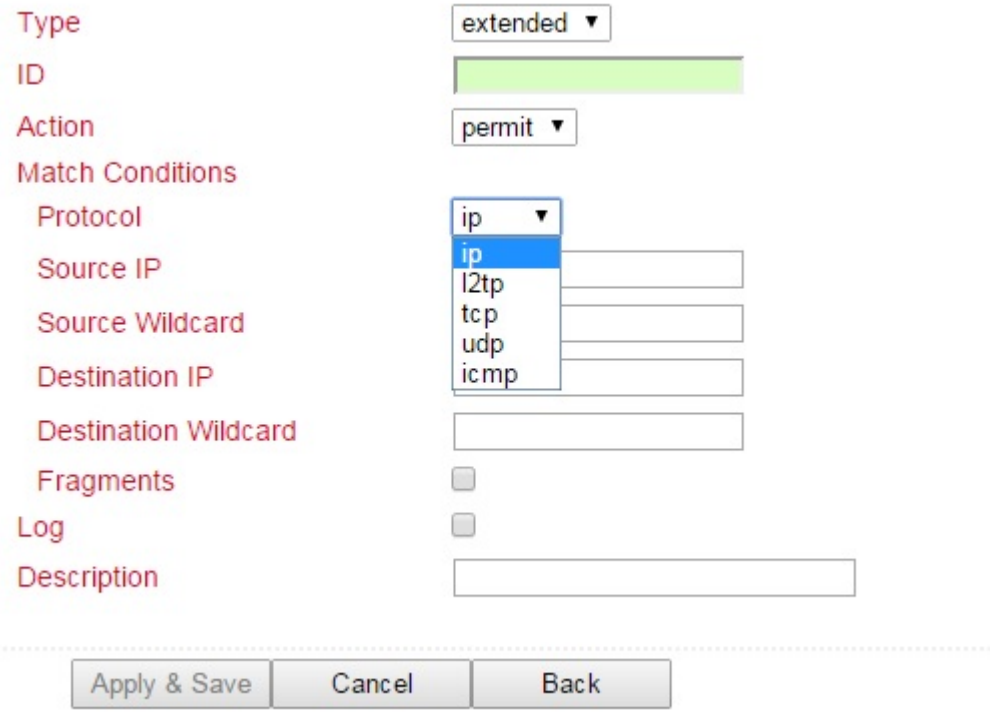
Die ACL (Access Control List) ist eine Zugriffskontrollliste, um die Nutzung und die Administration zu kontrollieren. Durch die ACL wird festgelegt, welche Rechner oder Netze auf den Router oder Netze hinter dem Router zugreifen können. Bei der ACL werden ein- und ausgehende Datenpakete analysiert und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

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

Von der Navigationsleiste Firewall  ACL (Enter) auswählen um auf die ACL zu kommen.




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



Unter Type hat man die Möglichkeiten, **Standard** und **Extended** auszuwählen.

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 auf IP-, L2TP-, TCP-, UDP-, ICMP-Ebene konfiguriert werden. Somit kann man gezielt einzelne Dienste wie Web (http), FTP, Telnet etc. erlauben oder verbieten.

| Parameter | Beschreibung |
|---|---|
| ID | ID 100 ist standardmäßig vorkonfiguriert.<br>Weitere IDs können frei konfiguriert werden. |
| Action | Permit = Erlauben / Deny = Verbieten |
| Protocol | Protokolle: IP, L2TP-, TCP-, UDP-, ICMP |
| Source | 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 | 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 |

# 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.

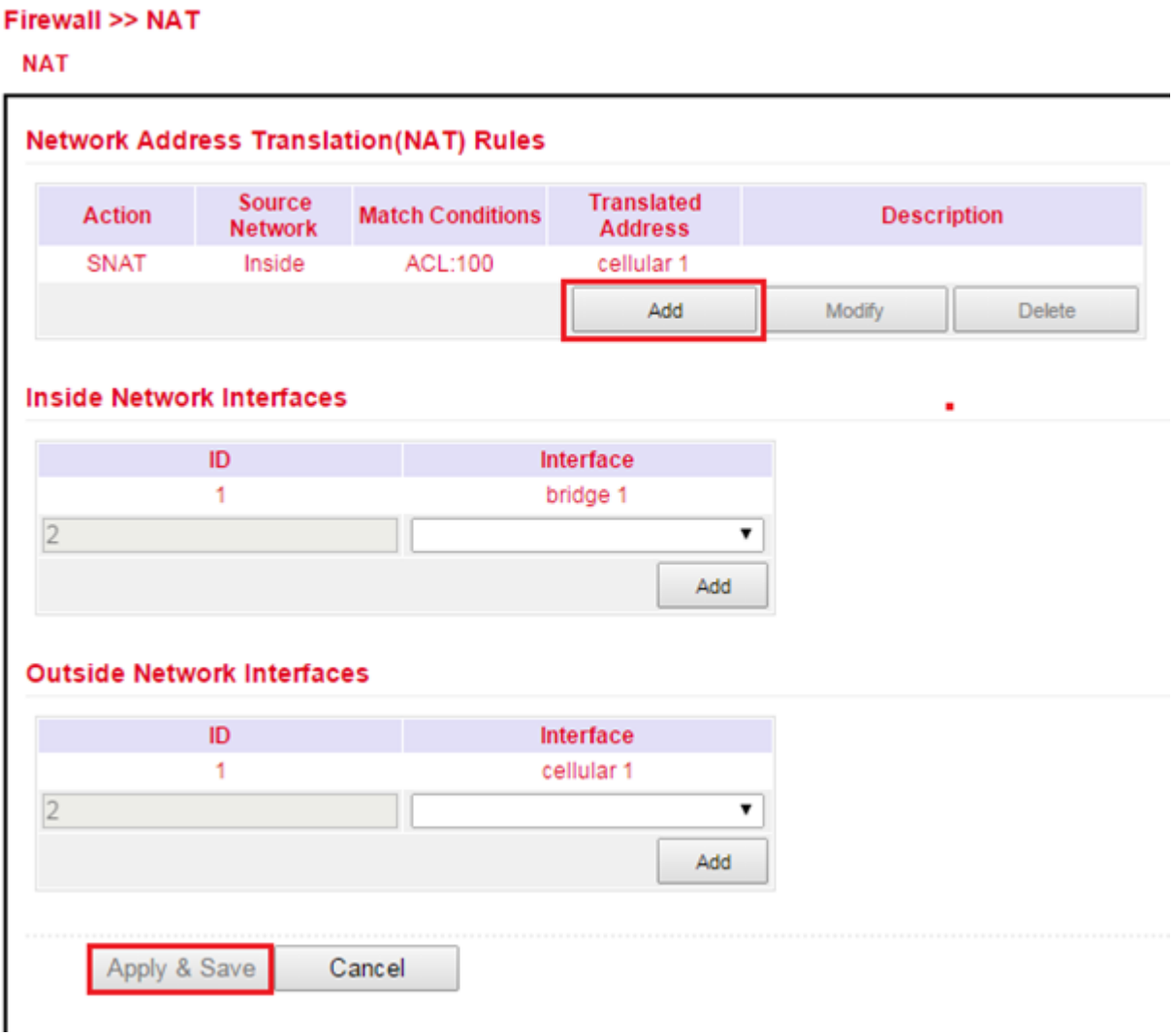
**Verwendung von 1:1-NAT**

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.

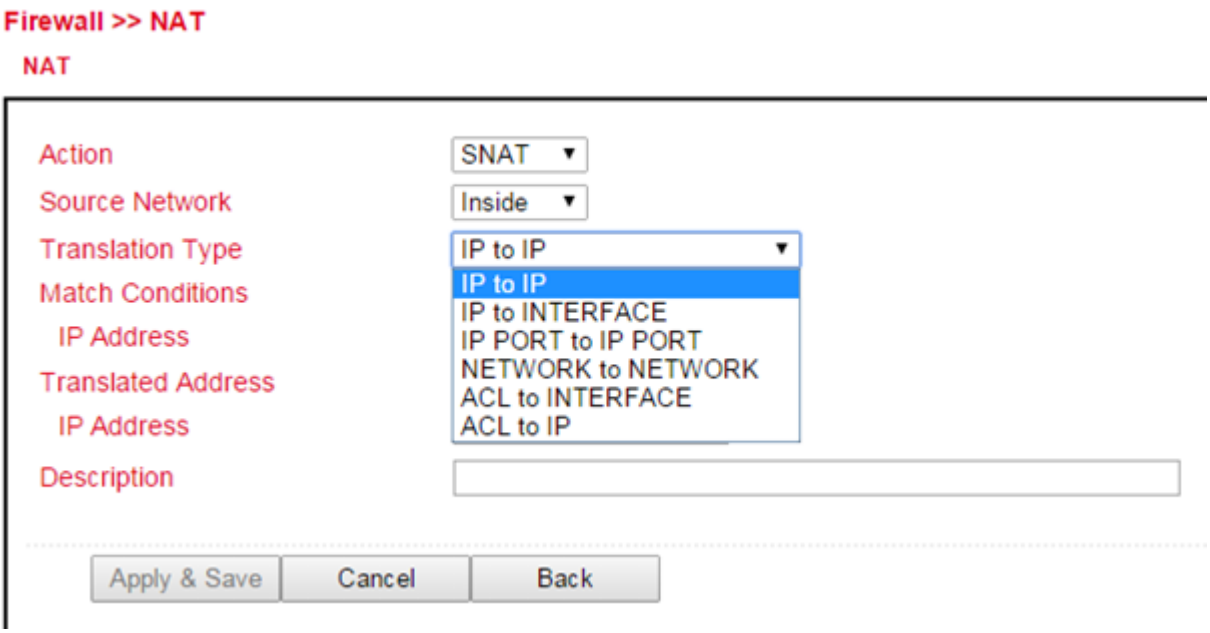
## Konfiguration

- 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 |

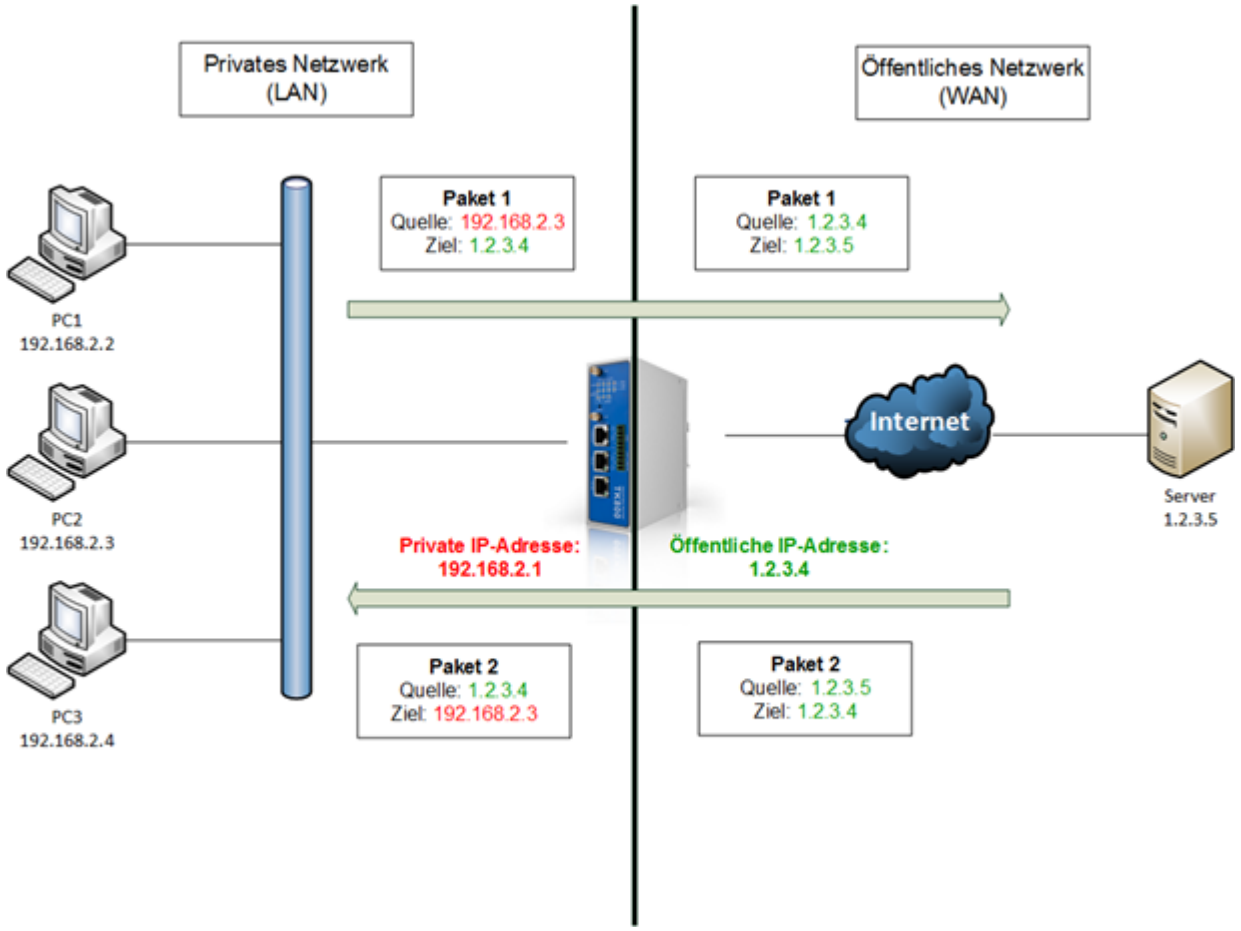
| | |
|---|---|
| Network to Network | eine Netzadresse in eine andere übersetzen |
| ACL to Interface | eine IP-Adresse nach ACL-Regel in eine IP-Adresse eines einzelnen Interfaces übersetzen |
| ACL to IP | Eine IP-Adresse nach ACL-Regel in eine<br>andere IP-Adresse übersetzen |
| Interface Port to IP Port | Portmapping |

## Beispiele

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

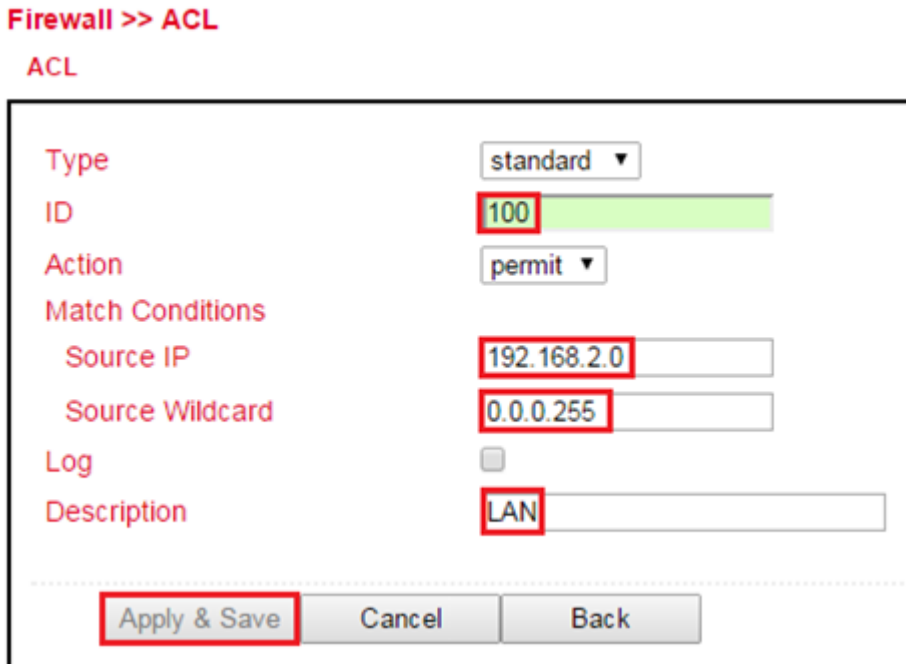
Der TK800 arbeitet hierbei als Internet-Gateway für angeschlossene Geräte mit privater IP-Adresse. Er übersetzt private IP-Adressen aus dem LAN in eine öffentliche, routbare Internet-Adresse.

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

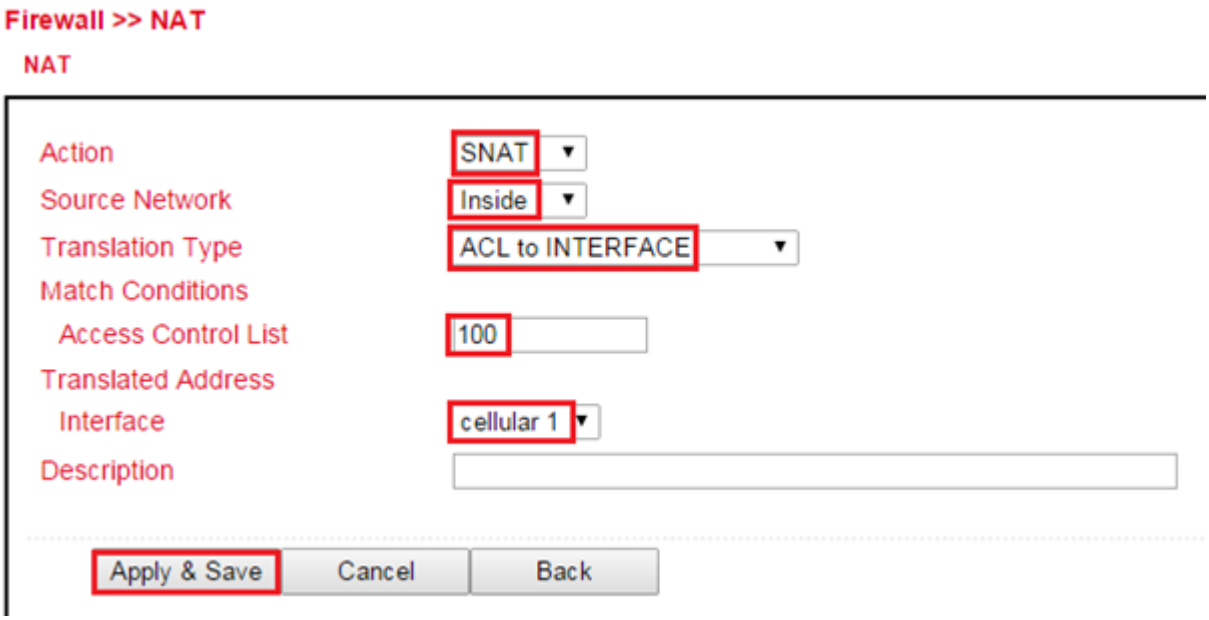



1. Konfigurieren Sie die ACL-Regel. Gehen Sie hierzu im Menü **Firewall** auf den Unterpunkt **ACL**
2. Vergeben Sie nun eine **ID** für die Regel und geben Sie die **IP-Adresse** und die entsprechende **Wildcard**-Maske ein.

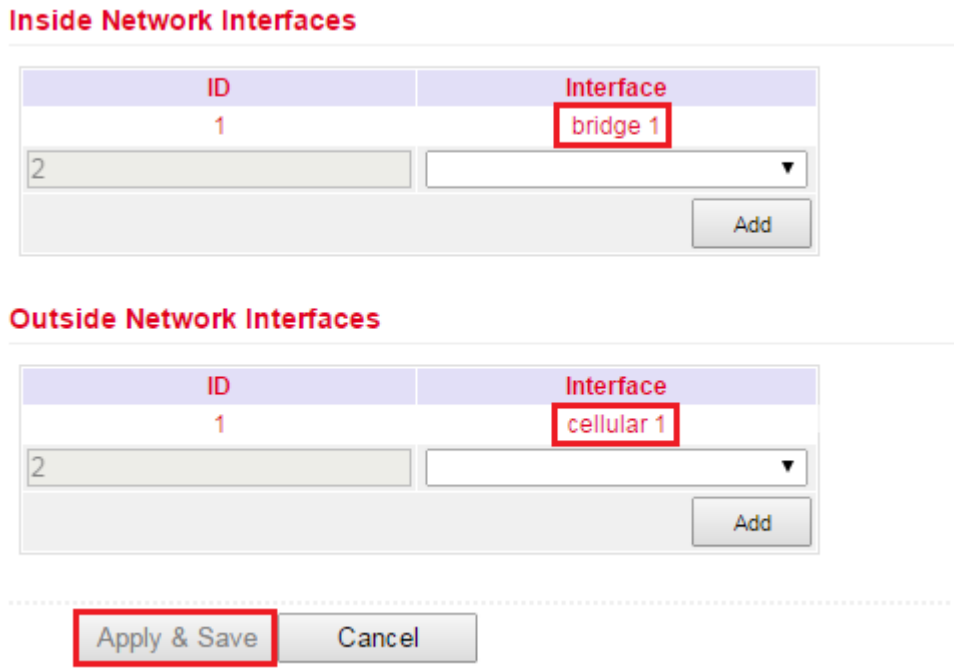
(**Anmerkung:** Die Wildcard-Maske ist die invertierte Netzmaske und wird von Routern zur Bearbeitung von **ACLs** (Access Control Lists) verwendet.)




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

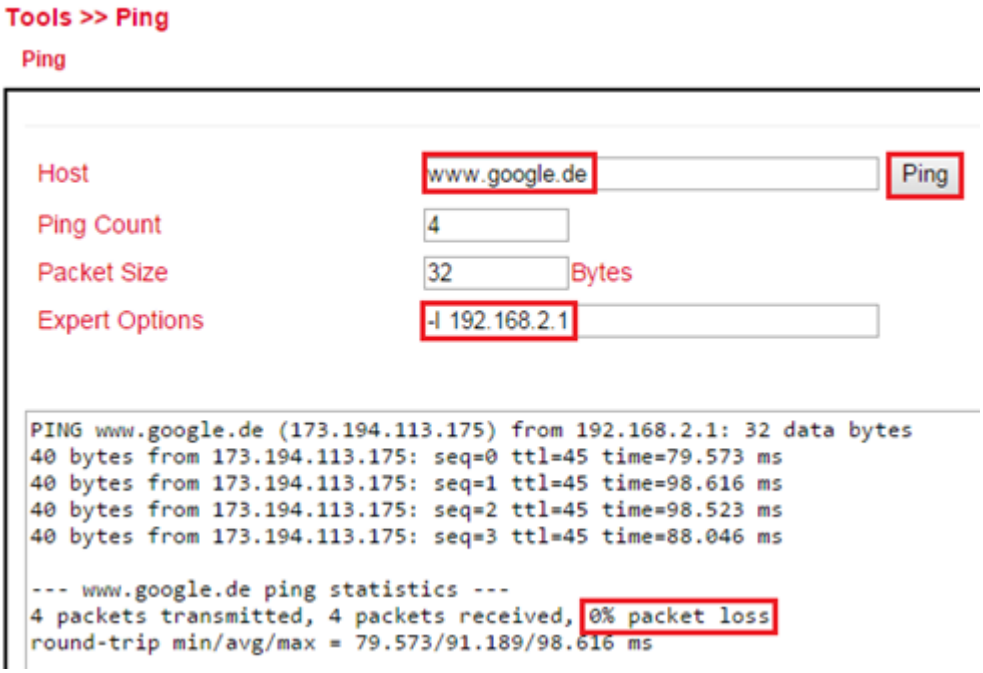



4. Definieren Sie nun das **Inside**- und **Outside-Interface**



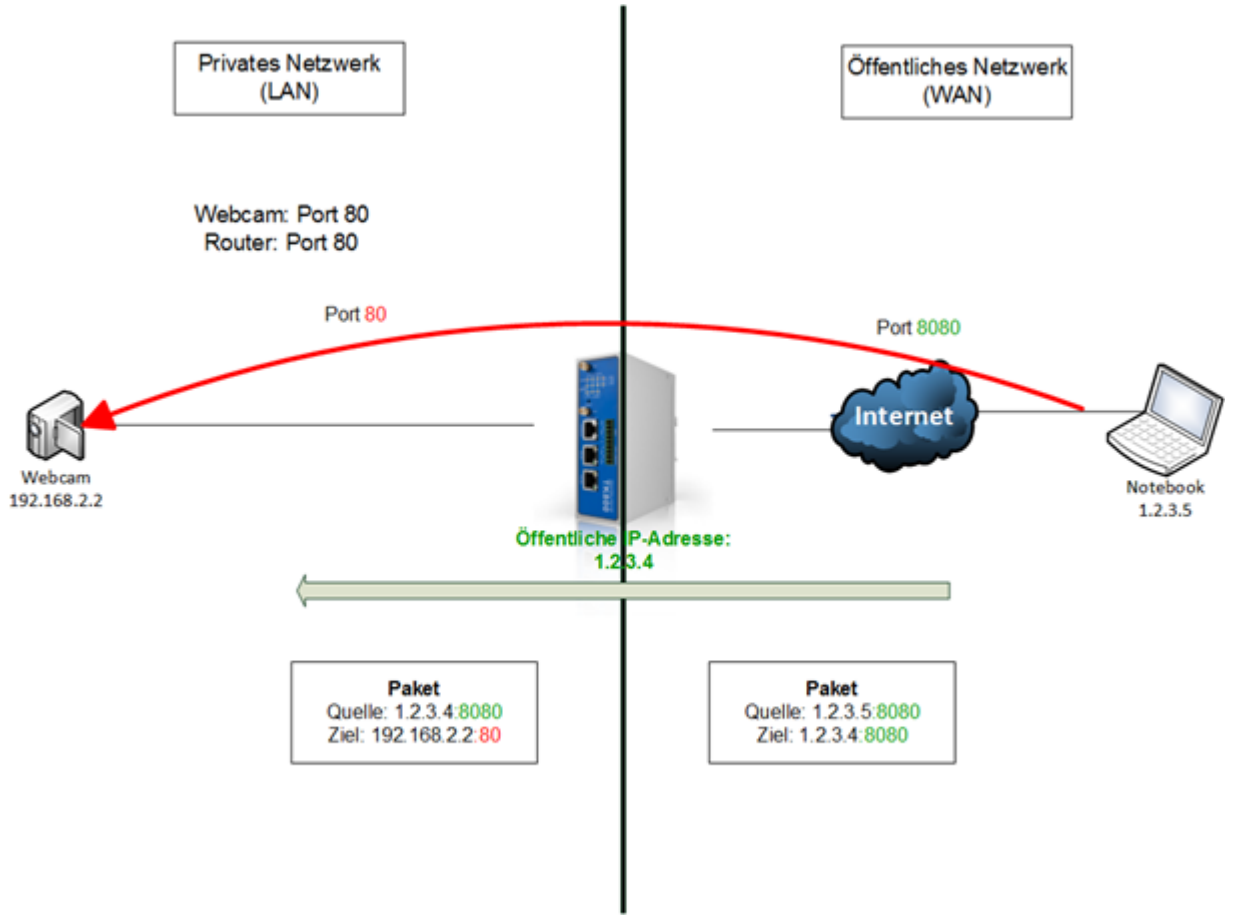

5. Testen Sie den Zugriff über das Tool **ping**. Dies kann direkt vom Router aus geschehen. Gehen Sie hierzu im Menü **Tools** auf den Unterpunkt **Ping** und tragen Sie die Werte nach dem Beispiel ein

(**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)



### *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

  (**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.)

- ⚠ Router Firmware 1.0.0.r5034 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: | 255.255.255.0 |

**Webcam**

| | |
|---|---|
| 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)

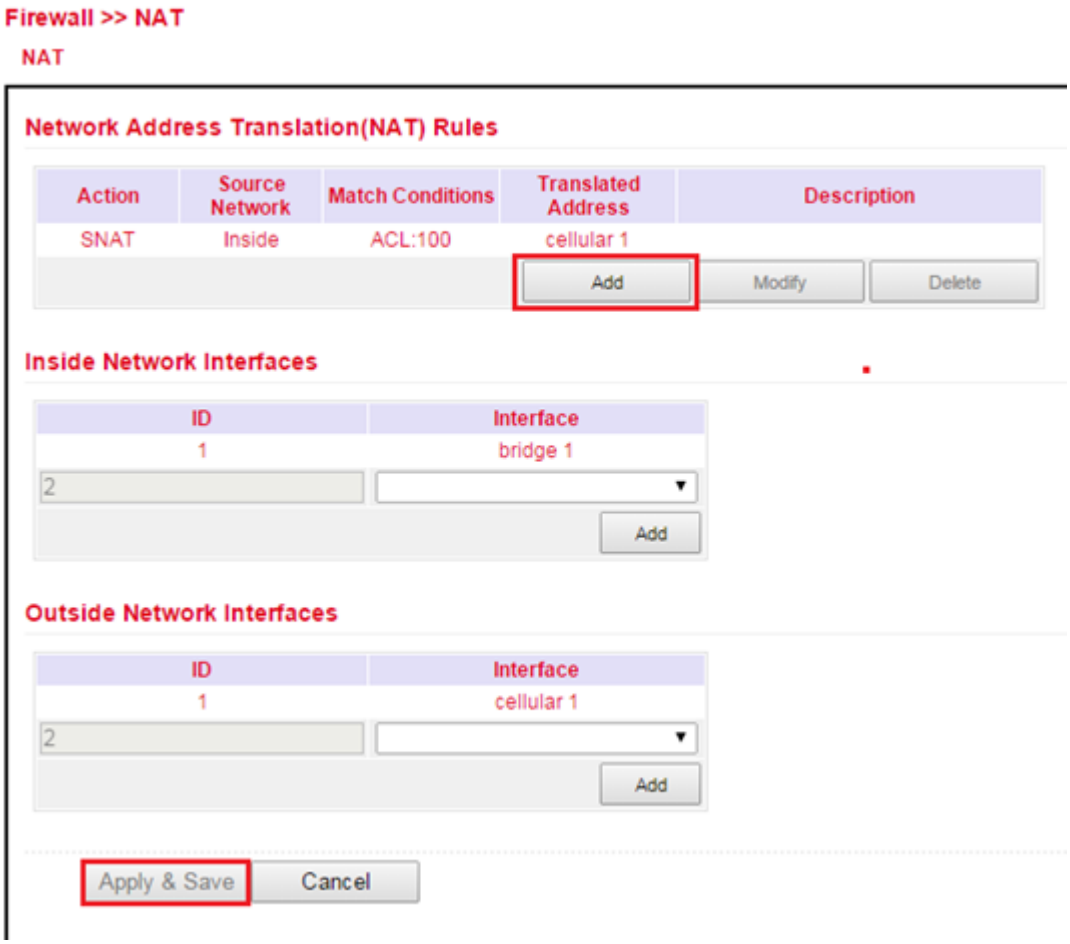
Für ein funktionierendes Port Mapping ist es hilfreich, wenn man die Einstellungen der angeschlossenen Geräte vorab überprüft. Folgende Checkliste ist dabei hilfreich (nach dem o.g. Beispiel):

- 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)?

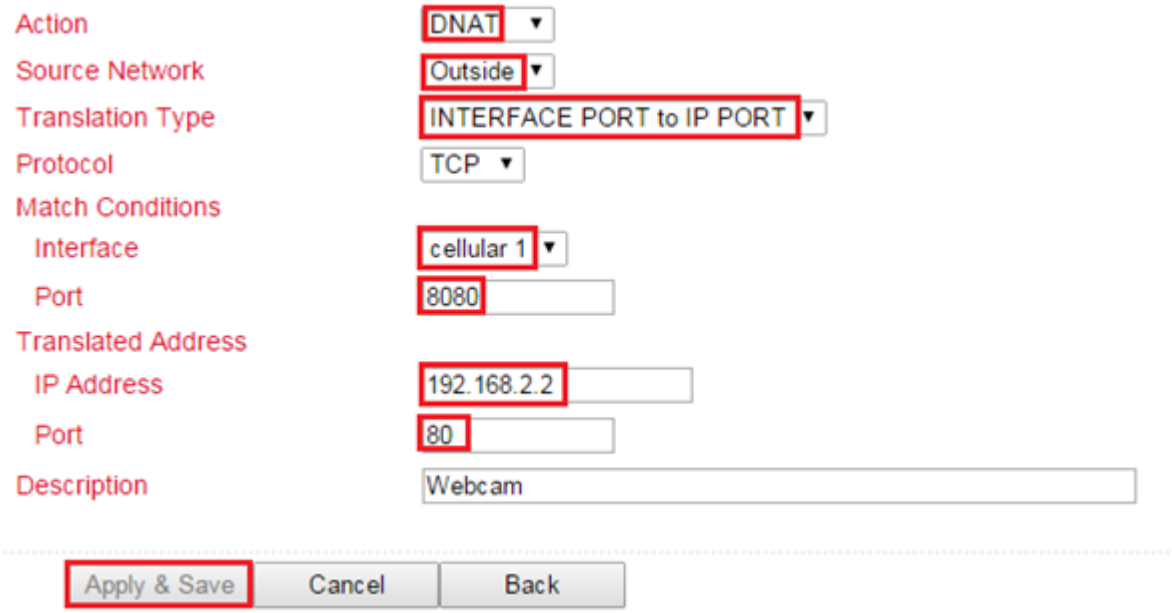
Sofern diese Bedingungen erfüllt sind, kann das Port Mapping nach folgender Anleitung eingerichtet werden.

## 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

## MAC-IP Binding

MAC-IP Binding ist im Navigationsbaum unter Firewall  MAC-IP Binding (Enter) zu finden.

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-Adress | 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, welch das Gerät bekommen soll. z.B. 192.168.2.150 |
| Description | Text Beschreibungsfeld |

# VPN

## IPSec ( Site-to-Site )

IPSec Site-to-Site VPN kann über dem Wizard im Navigationsmenü konfiguriert werden (Web unter **Wizards**).

Manuell können IPSec Tunnel im Navigationsmenü unter **VPN  IPSec** konfiguriert werden.

### Einleitung:

Bei VPN Tunnel (Site-To-Site) ist darauf zu achten, dass die Subnetze sich nicht mit der Gegenseite überschneiden. Bei sich überschneidenden Subnetzen würde der Router das Paket nicht routen können.

**Beispiel 1:** IPSec Tunnel und Routing funktioniert, weil die Subnetze verschieden sind.

Lokal ist der Host Adressen Bereich 192.168.2.1 - 192.168.2.254.
Remote ist der Host Adressen Bereich 172.16.2.1 - 172.16.2.254.

| Netz | Subnetz | Subnetzmaske | Routing funktioniert Ja/Nein |
|---|---|---|---|
| Lokales Netzwerk | 192.168.2.0 | 255.255.255.0 | JA |
| Remote Netzwerk | 172.16.2.0 | 255.255.255.0 | |

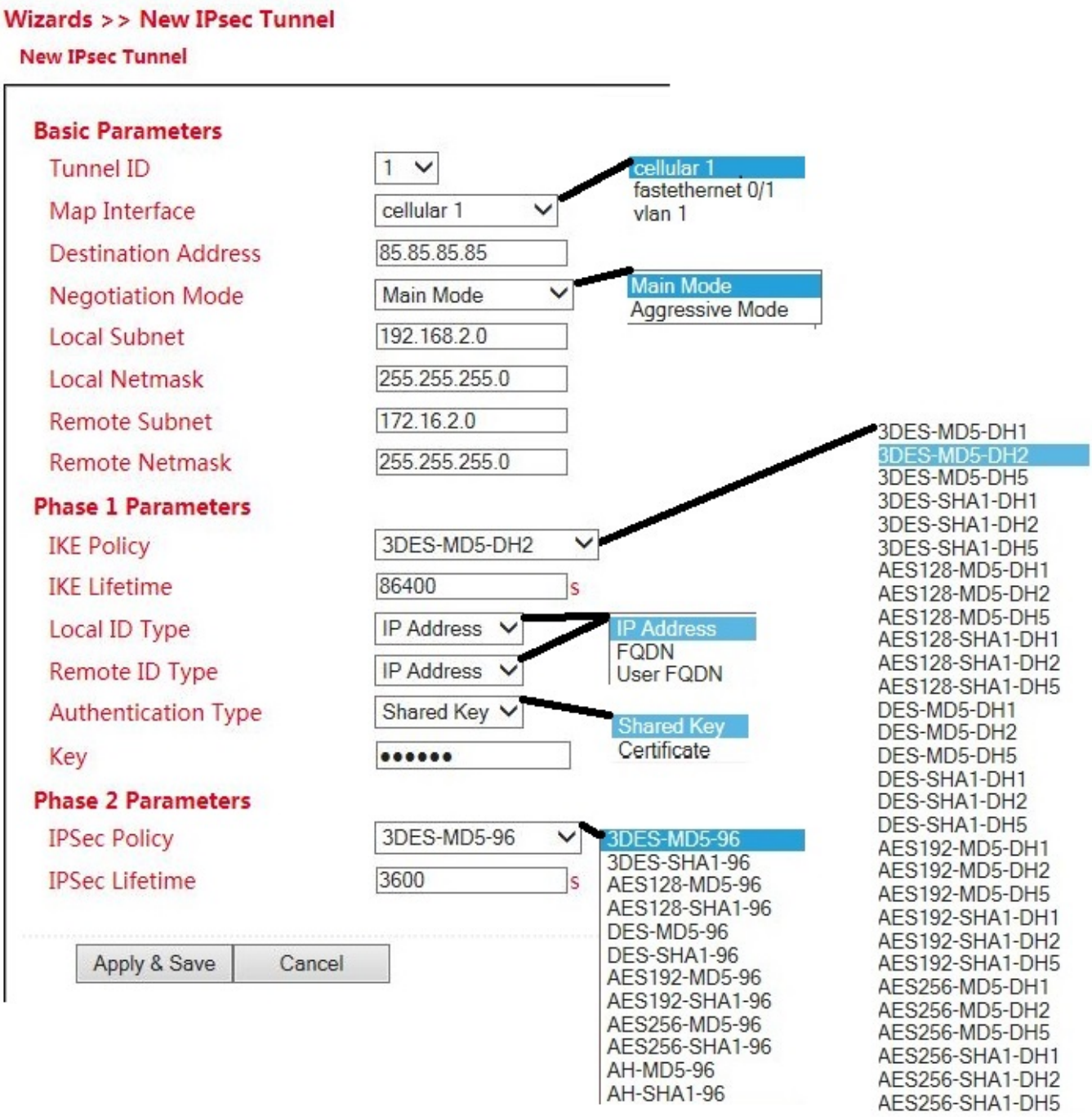
**Beispiel 2:** IPSec Tunnel funktioniert nicht, da die Netze sich durch eine Klasse B Subnetzmaske überschneiden. Routing wird nicht funktionieren, da bei beiden Netzwerken die Subnetze von 192.168.0.1 - 192.168.255.254 gehen. Lokales Netzwerk und Remote Netzwerk haben den gleichen Host Adressen Bereich.

| Netz | Subnetz | Subnetzmaske | Routing funktioniert Ja/Nein |
|---|---|---|---|
| Lokales Netzwerk | 192.168.2.0 | 255.255.0.0 | Nein |
| Remote Netzwerk | 192.168.10.0 | 255.255.0.0 | |

## IPSec Tunnel mit dem Wizard erstellen

Mit dem Wizard lassen sich Standard IPSec Tunnel ohne großen Aufwand erstellen.

In diesem Beispiel wird mit dem **Wizard** ein IPSec Tunnel konfiguriert.




| Parameter | Beschreibung |
|---|---|
| **Basic Parameters** | |
| Tunnel ID | Numerische Tunnel Identifikationsnummern 1-10 |

| | |
|---|---|
| Map Interface | Die Schnittstelle, über welchen der Tunnel aufgebaut werden soll:<br>cellular 1 = GSM/UMTS/LTE<br>fastethernet 0/1 = FastEthernet Port 0/1<br>vlan 1 = Netzwerkports, auf welchen das VLAN 1 liegt. |
| Destination Address | Ziel Adresse des gegenüberliegenden Netzwerkes.<br><br>Meistens ist das die öffentliche IP Adresse des gegenüberliegenden Routers, mit dem der Tunnel aufgebaut werden soll. |
| Negotiation Mode | Main Mode oder Aggressive Mode |
| Local Subnet | Lokales Subnetz. Bei den Welotec Routern Werkseinstellung 192.168.2.0. |
| Local Netzmask | Lokale Subnetzmaske. Bei den Welotec Routern Werkseinstellung Klasse C Subnetzmaske: 255.255.255.0. |
| Remote Subnet | Entferntes Subnetz, welches hinter dem Router auf der gegenüberliegenden Seite erreicht werden soll. z.B. 172.16.2.0 |
| Remote Netzmask | Entfernte Netzmaske des Subnetzes. z.B. 255.255.255.0 |
| **Phase 1 Parameters** | |
| IKE Policy | Hier wird die IKE (*Internet-Key-Exchange*) Regel definiert. IKE wird benötigt um eine SA (Security association) im IPSec Protokol aufzubauen.<br>Zur Auswahl im Drop Down Menü sind zusammengestellte Parameterwerte auszuwählen.<br><br>**Werte**<br>Encryption / Verschlüsselung: 3des, des, aes128, aes192, aes256<br>Hash: md5, sha1<br>Diffie-Hellman Group (DH): Gruppe 1, Gruppe 2, Gruppe 5 |
| IKE Lifetime | Zeit in Sekunden. Standardwert 86400 Sekunden. |
| Local ID Type | Lokaler Identifikationstyp. Zur Auswahl stehen "IP Adresse", "FQDN" und "User FQDN".<br><br>**Parameter** / **Beschreibung**<br>IP Adress: IP Adresse. Hier wird die öffentliche IP Adresse des Routers verwendet.<br>FQDN: FQDN (Fully qualified Domain Name) z.B. router1.welotec.com<br>User FQDN: Benutzerdefinierter FQDN (Fully qualified Domain Name), z.B. @router1 |
| Remote ID Type | Remote Identifikationstyp. Identifikation der Gegenstelle. Zur Auswahl stehen "IP Adresse", "FQDN" und "User FQDN".<br>Die Parameter sind analog zur lokalen Identifikation anzuwenden. Bei User FQDN z.B. @router2 des gegenüberliegenden Routers. |
| Authentication Type | "Shared Key" oder "Certificate".<br><br>**Parameter** / **Beschreibung**<br>Shared Key: Shared Key oder Pre Shared Key (PSK) ist ein Passwort, welches auf beiden Routern gesetzt wird und übereinstimmen muss.<br>Es wird empfohlen, ein möglichst langes Passwort auszuwählen. Empfehlung: Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen verwenden.<br>Certificate: Zertifikat Authentifizierung. |

| | |
|---|---|
| Key | In dieses Feld ist das Passwort (PSK) einzutragen, wenn die Option "Shared Key" ausgewählt wurde. |
| **Phase 2 Parameters** | |
| IPSec Policy | Die IPSec Verschlüsselungsparameter der Phase 2 des IPSec Tunnels sind hier aus dem Drop-Down Menü auszuwählen.<br><br>**Werte**<br>Encapsulation: ESP (Encapsulating Security Payload). ESP wird standardmäßig genommen, ansonsten steht "AH" davor.<br>AH (Authentication Header)<br>Encryption: • 3des • des • aes128 • aes192 • aes256<br>Authentication: • md5 • sha1 |
| IPSec Lifetime | IPSec Lebenszeit in Sekunden. Standardwert sind 3600 Sekunden. |

### Status

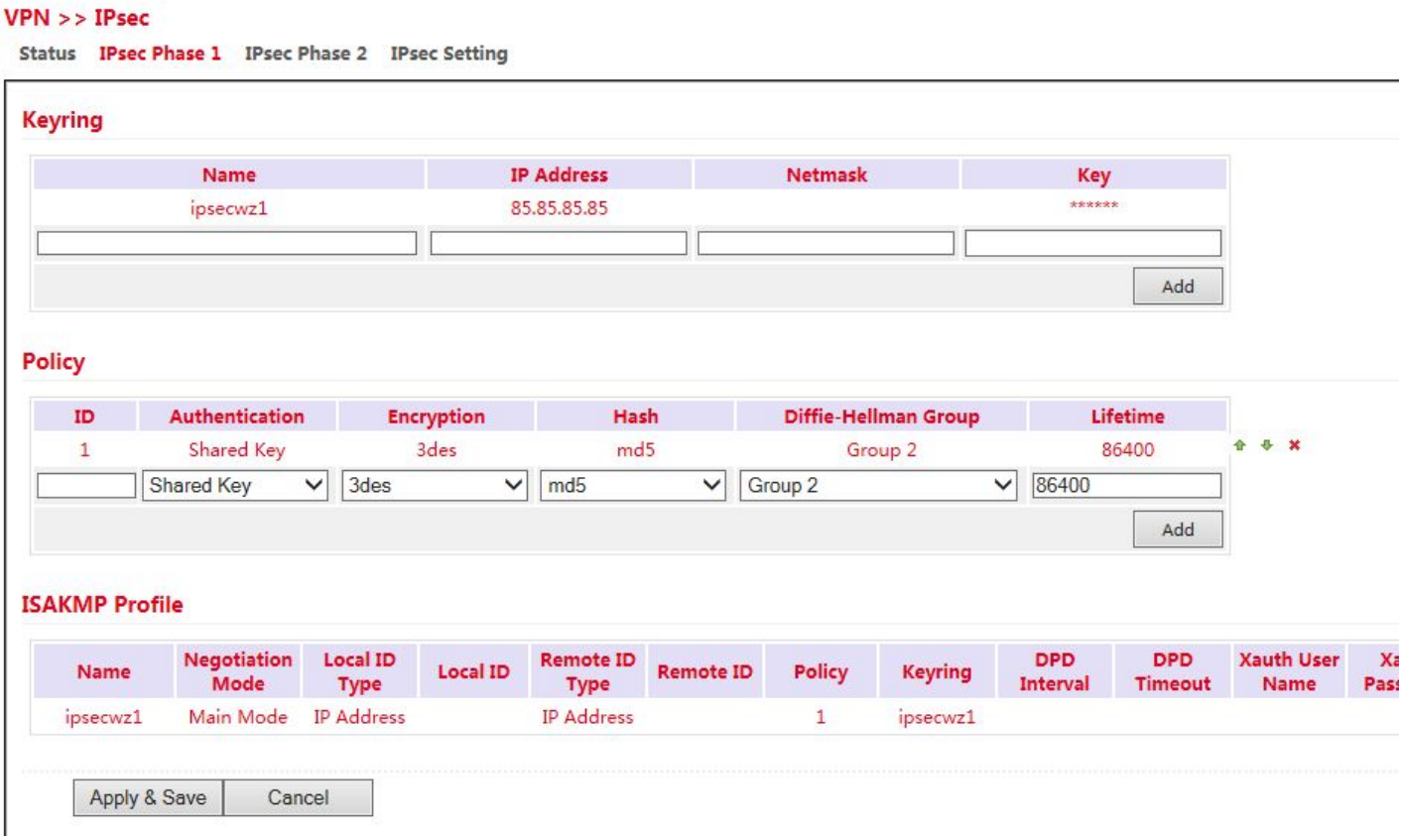
Im "Reiter" Status sieht man den aktuellen Status des IPSec Tunnels.

| Parameter | Beschreibung |
|---|---|
| Name | Logischer Name des IPSec Tunnels. In diesem Fall "IPSec_1". |
| Tunnel Description | Tunnel Beschreibung. Hier wird die Zieladresse zum gegenüberliegenden Router angezeigt, zu welchem der IPSec Tunnel aufgebaut wird. |
| Status | • Disconnected = IPSec Tunnel ist nicht verbunden. Es besteht kein aufgebauter IPSec Tunnel.<br>• Connected = IPSec Tunnel ist verbunden. Es besteht ein aktiver IPSec Tunnel. |

### IPSec Phase 1

Im "Reiter" IPSec Phase 1 werden die Parameter des IPSec Tunnels der Phase 1 angezeigt bzw. konfiguriert.

In diesem Fall wurden die Parameter durch Benutzung des Wizards für den IPSec Tunnel übernommen und eingetragen.
Ein IPSec Tunnel kann natürlich manuell konfiguriert werden. Dazu auf "Add" (Hinzufügen) klicken und die gewünschten Parameter eintragen.




### *Keyring (Phase 1 Parameters)*

Im "Keyring" werden die "Pre Shared Keys" (PSK) hinterlegt. Wenn ein PSK lediglich für einen bestimmten IPSec Tunnel verwendet wird, wird die öffentliche IP Adresse des gegenüberliegenden Routers festgelegt. Somit ist sichergestellt, dass dieses Passwort angewendet wird, wenn der gegenüberliegende Router diese bestimmte öffentliche IP Adresse hat.
Wenn mehrere IPSec Tunnel mit dem gleichen Passwort aufgebaut werden, dann kann ein angelegter Key mehrfach verwendet werden. In diesem Fall haben die gegenüber liegenden Router verschiedene öffentliche IP Adressen. Dann ist im Feld "IP Address" der Wert "0.0.0.0" einzutragen. Dann wird jede IP Adresse des gegenüberliegenden Routers akzeptiert.

| Parameter "Keyring" | Beschreibung |
|---|---|
| Name | Logischer Name des Keyrings |
| IP Address | IP Adresse des gegenüberliegenden Routers, für welchen dieser Key verwendet werden soll. |
| Netmask | Netzmaske |
| Key | Passwort (Pre Shared Key) |

### *Policy (Phase 1 Parameters)*

In der Policy (Regelwerk) werden die Verschlüsselungsparameter hinterlegt.

| Parameter | Beschreibung |
|---|---|
| ID | Identifikationsnummer |

| | |
|---|---|
| Authentication | Authentifizierung. Zur Auswahl stehen:<br>• Shared Key (PSK) = Passwort für den Tunnel, welcher auf beiden Routern übereinstimmen muss.<br>• Certificate = Zertifikat |
| Encryption | Verschlüsselungsparameter:<br>• 3des<br>• des<br>• aes128<br>• aes192<br>• aes256 |
| Hash | Hash Parameter:<br>• md5<br>• sha1 |
| Diffie-Hellman Group (DH) | Diffie-Hellman Gruppen:<br>• Gruppe 1<br>• Gruppe 2<br>• Gruppe 5 |
| Lifetime | Zeit in Sekunden. Standardwert sind 86400 Sekunden. |

### *ISAKMP Profile (Phase 1 Parameters)*

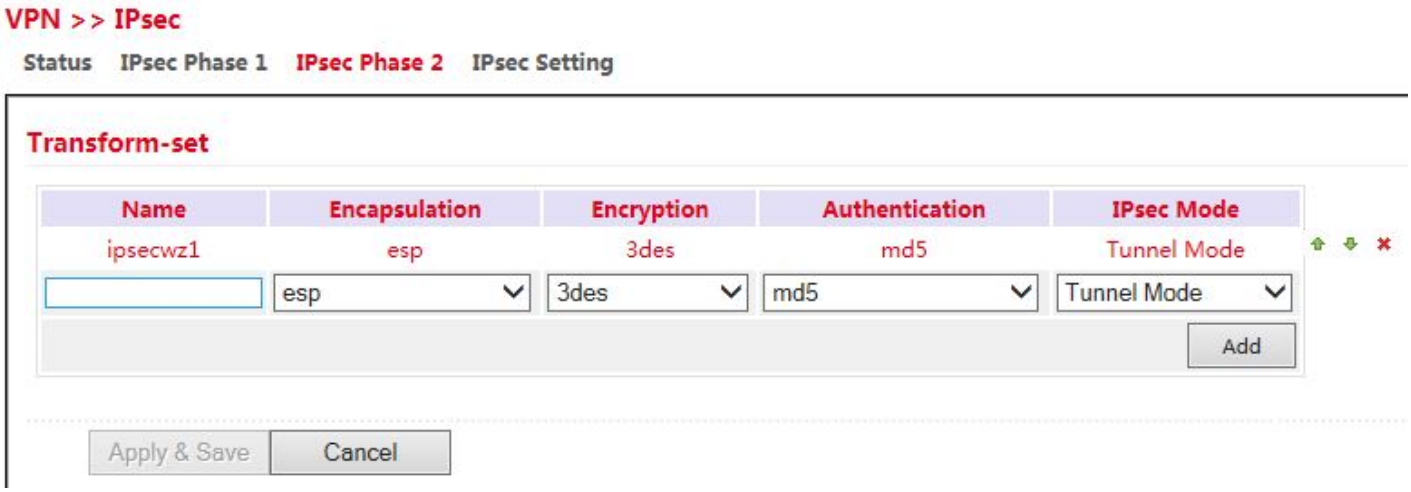
ISAKMP (Internet Security Association and Key Management Protocol) ist für die Authentisierung und den sicheren Schlüsselaustausch über unsgesicherte Netzwerke zwischen den VPN Partnern zuständig.

| Parameter | Beschreibung |
|---|---|
| Name | Logischer Name des ISAKMP Profils |
| Negotiation Mode | Aushandlungsmethode. Zur Auswahl stehen:<br>• Main Mode<br>• Aggressive Mode |
| Local ID Type | Lokaler Identifikationstyp. Zur Auswahl stehen "IP Adresse", "FQDN" und "User FQDN".<br>**Parameter** / **Beschreibung**<br>IP Adress: IP Adresse. Hier wird die öffentliche IP Adresse des Routers verwendet.<br>FQDN: FQDN (Fully qualified Domain Name) z.B. router1.welotec.com<br>User FQDN: Benutzerdefinierter FQDN (Fully qualified Domain Name), z.B. @router1 |
| Local ID Type | Lokale Identifikation. Wenn "IP Address" ausgewählt wird, dann wird die öffentliche IP Adresse des Routers zur Authentifizierung benutzt.<br>Bei der Auswahl von "FQDN" oder "User FQDN" ist der voll qualifizierte Domain Name z.B. router1.welotec.com oder der Benutzerdefinierte FQDN z.B. @router1 einzutragen. |
| Remote ID Type | Remote Identifikation. Wenn "IP Address" ausgewählt wird, dann wird die öffentliche IP Adresse des gegenüberliegenden Routers zur Authentifizierung benutzt.<br>Bei der Auswahl von "FQDN" oder "User FQDN" ist der voll qualifizierte Domain Name z.B. router2.welotec.com oder der Benutzer-definierte FQDN z.B. @router2 einzutragen. |
| Policy | Hier ist die Regel Nummer einzutragen. Fortlaufende Nummern von 1 bis X. |
| Keyring | Der Keyring (PSK), welcher benutzt wird ist hier einzutragen. |
| DPD Interval | DPD Interval (Dead Peer Interval) bedeutet, dass überprüft wird, ob der gegenüberliegende Router, zu welchem der Tunnel aufgebaut wird, erreichbar ist. Wenn dieser nicht erreichbar ist, wird der Tunnel im definierten Zeitabstand versuchen, neu aufzubauen. |
| DPD Timeout | Beim Parameter DPD Timeout (Dead Peer Timeout) wird die Zeit in Sekunden definiert, in welcher versucht wird, den Tunnel erneut aufzubauen. |

| | |
|---|---|
| Xauth User Name | Xauth wird verwendet, um einen Client-to-Side IPSec Tunnel aufzubauen. Xauth User Name ist der Benutzername des Clients, welcher einen IPSec Tunnel zum Router aufbauen will. |
| Xauth Password | Xauth Password ist das zugehörige Passwort des Benutzers, welcher eine Client-to-Side IPSec Verbindung zum Router aufbauen will. |

### IPSec Phase 2 Parameters - Transfom Set

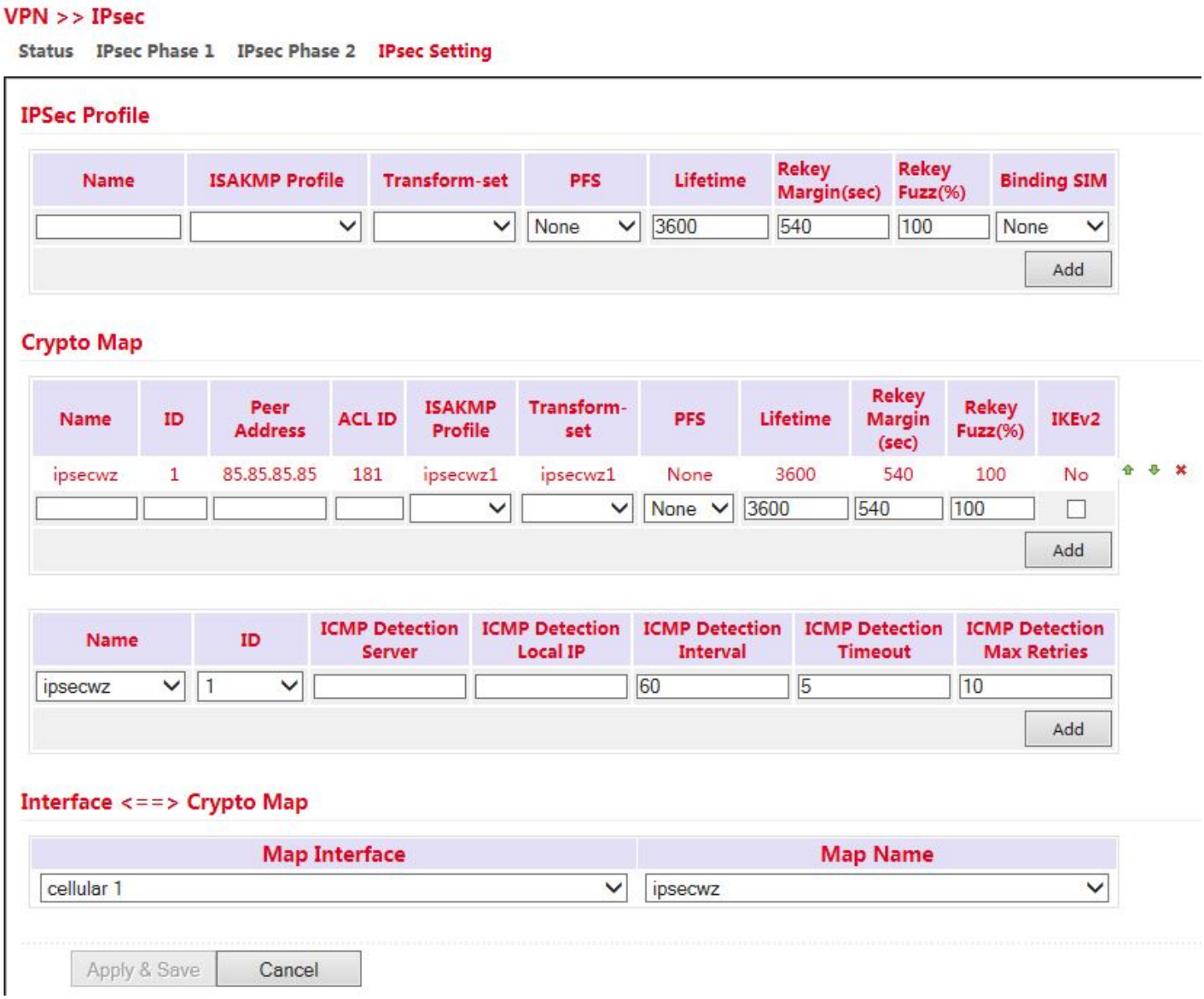
In der IPSec Phase 2 werden die Parameter der zweiten Phase des IPSec Tunnel Aufbaus konfiguriert.




Im Transform-Set werden die ausgewählten Security Assotiations (SA) für IKE Phase 2 konfiguriert.

| Parameter | Beschreibung |
|---|---|
| Name | Logischer Name |
| Encapsulation | • ESP (Encapsulating Security Payload)<br>• AH (Authentication Header) |
| Encryption | • 3des<br>• des<br>• aes128<br>• aes192<br>• aes256 |
| Authentication | • md5<br>• sha1 |
| IPSec Mode | Zur Auswahl stehen "Tunnel mode" und "Transport mode".<br>• Tunnel Mode =Tunnelmodus. Im Tunnelmode wird ein komplettes IP-Paket (welches die Daten sowie die virtuelle Firmen-Netz-IP-Adresse enthält, die der Client bei VPN Aufbau bekommt) in ein anderes Paket (welches die "realen" IPs des Clients u. VPN Servers enthält) gekapselt.<br>Wird vor allem für Site-to-Site VPN's genutzt, wenn ganze Subnetze durch den Tunnel gerouted werden sollen.<br>• Transport Mode = Transportmodus. Im Transportmode werden die Daten verschlüsselt, der IP-Header bleibt jedoch erhalten.<br>Wird vor allem bei Ende-zu Ende-Verschlüsselungen und in Verbindung mit GRE genutzt. |

### IPSec Setting Parameters




### *IPSec Profile*

IPSec Profile Einstellungen werden für DMVPN (Dynamic Multipoint Virtual Private Network) konfiguriert.

### *Crypto Map*

In der Crypto Map werden die verschiedenen IPSec Konfigurationen zu einem Profil zusammengefasst.

| Parameter | Beschreibung |
|---|---|
| Name | Logischer Name |
| ID | Identifikationsnummer |
| Peer Address | IP Adresse des gegenüberliegenden Routers, mit welchem der IPSec Tunnel aufgebaut werden soll. |

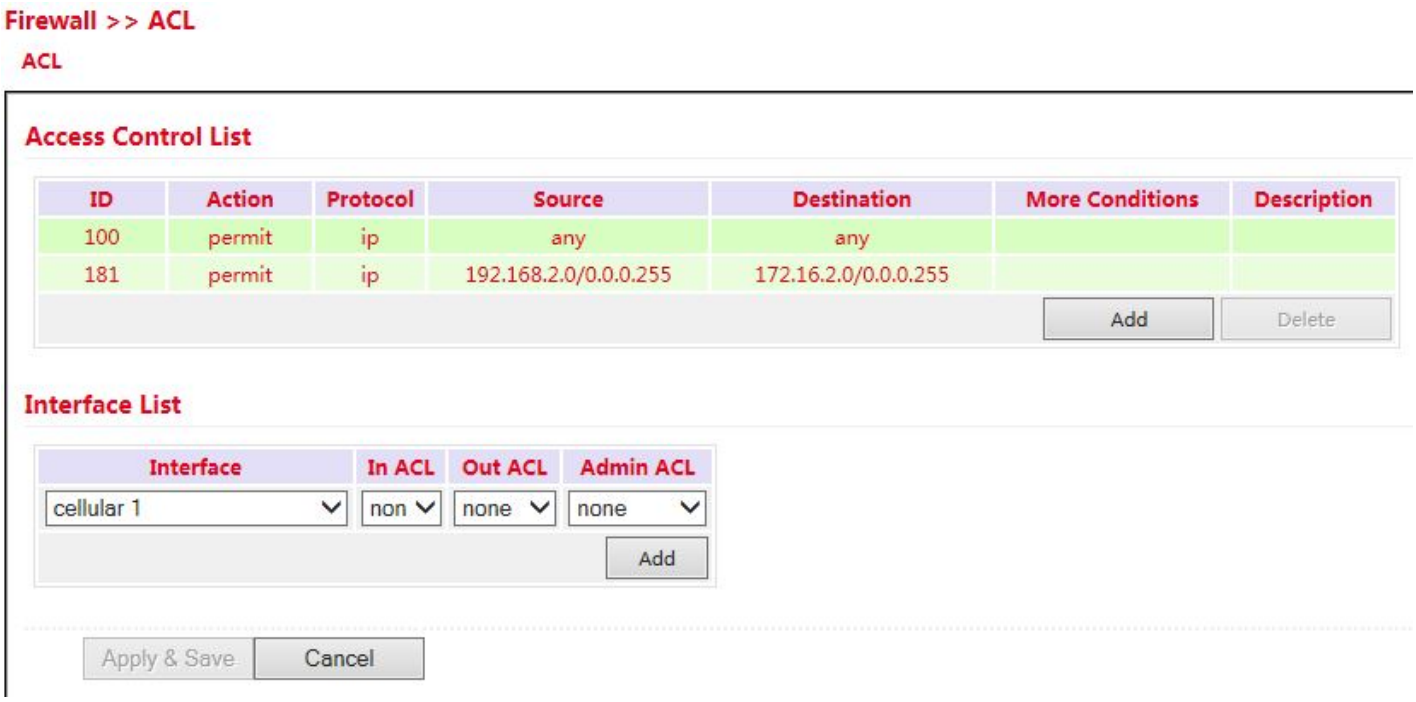
| | |
|---|---|
| ACL ID | ACL (Access Control List) Identifikationsnummer |
| ISAKMP Profile | ISAKMP Profil |
| Transform Set | Transformset |
| PFS | PFS (Perfect Forward Secrecy) |
| Lifetime | Lebenszeit in Sekunden |
| Rekey Margin (sec) | Zeit bis der Schlüssel ausläuft und neu ausgehandelt wird. |
| Rekey Fuzz (%) | Rekey Fuzz in Prozent |
| IKEv2 | Haken setzten, damit IKEv2 anstatt IKEv1 genommen wird. |

### *Interface <==> Crypto Map*

Hier wird eingestellt, über welche Schnittstelle der IPSec Tunnel aufgebaut wird.

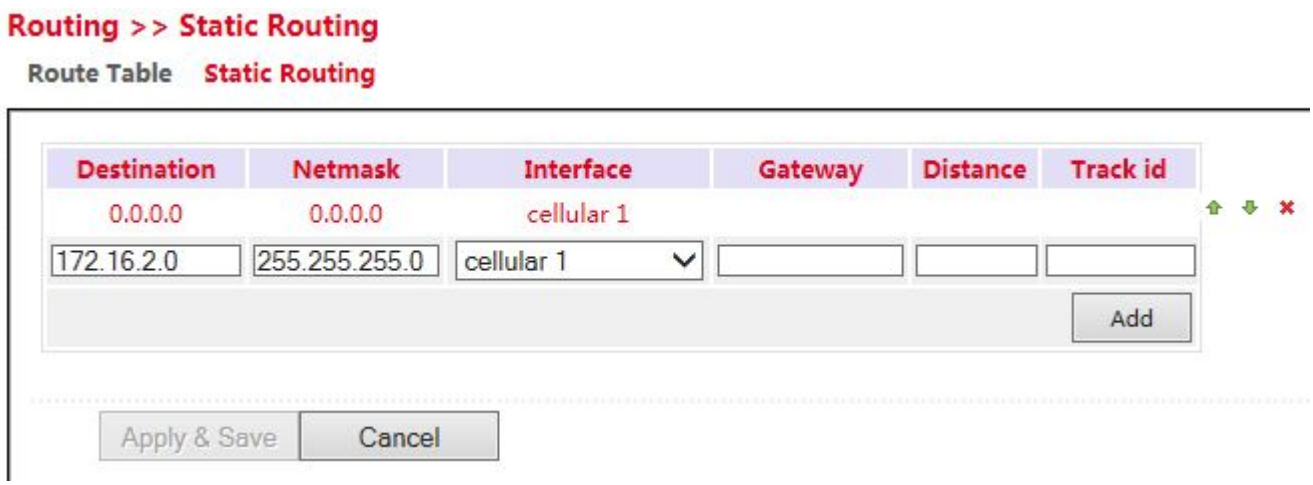
| Parameter | Beschreibung |
|---|---|
| Map Interface | Folgende Schnittstellen stehen zur Auswahl:<br>• cellular 1<br>• fastethernet 0/1<br>• vlan 1 |
| MAP Name | Der zugehörige Map Name muss dem Interface zugeordnet werden. |

Die ACL (Access Control List) muss erstellt werden, wenn der IPSec Tunnel manuell konfiguriert wird. Die ACL Einstellung wird im Navigationsmenü unter **Firewall  ACL konfiguriert**




Die ACL mit der ID 181 wurde durch den Wizard erstellt. Wenn der Tunnel manuell konfiguriert wird, dann muss eine ACL für den Tunnel erstellt werden. Weitere Erläuterungen zum Erstellen einer ACL sind im Handbuch über **Firewall  ACL** zu finden.

Es muss noch eine statische Route eingerichtet werden. Die statische Route wird unter **Routing  Static Routing** "Reiter" **Static Routing** konfigu riert




Auf "**Add**" klicken und eine statische Route zum Subnetz des gegenüberliegenden Routers setzen. In diesem Fall ist das Subnetz, welches durch den VPN Tunnel erreicht werden soll, 172.16.2.0.
Das Interface ist in diesem Fall "cellular 1" (über die Mobilfunkschnittstelle).

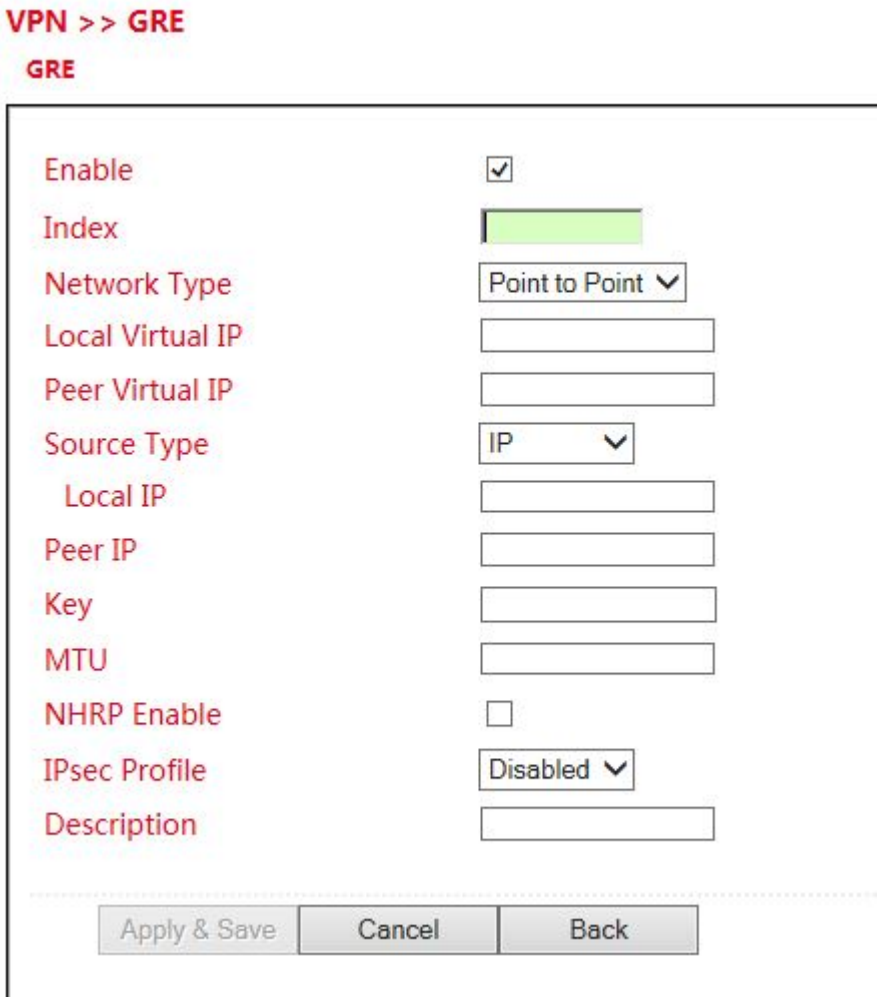
Danach mit "**Apply & Save**" die Konfiguration abspeichern.

## GRE

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

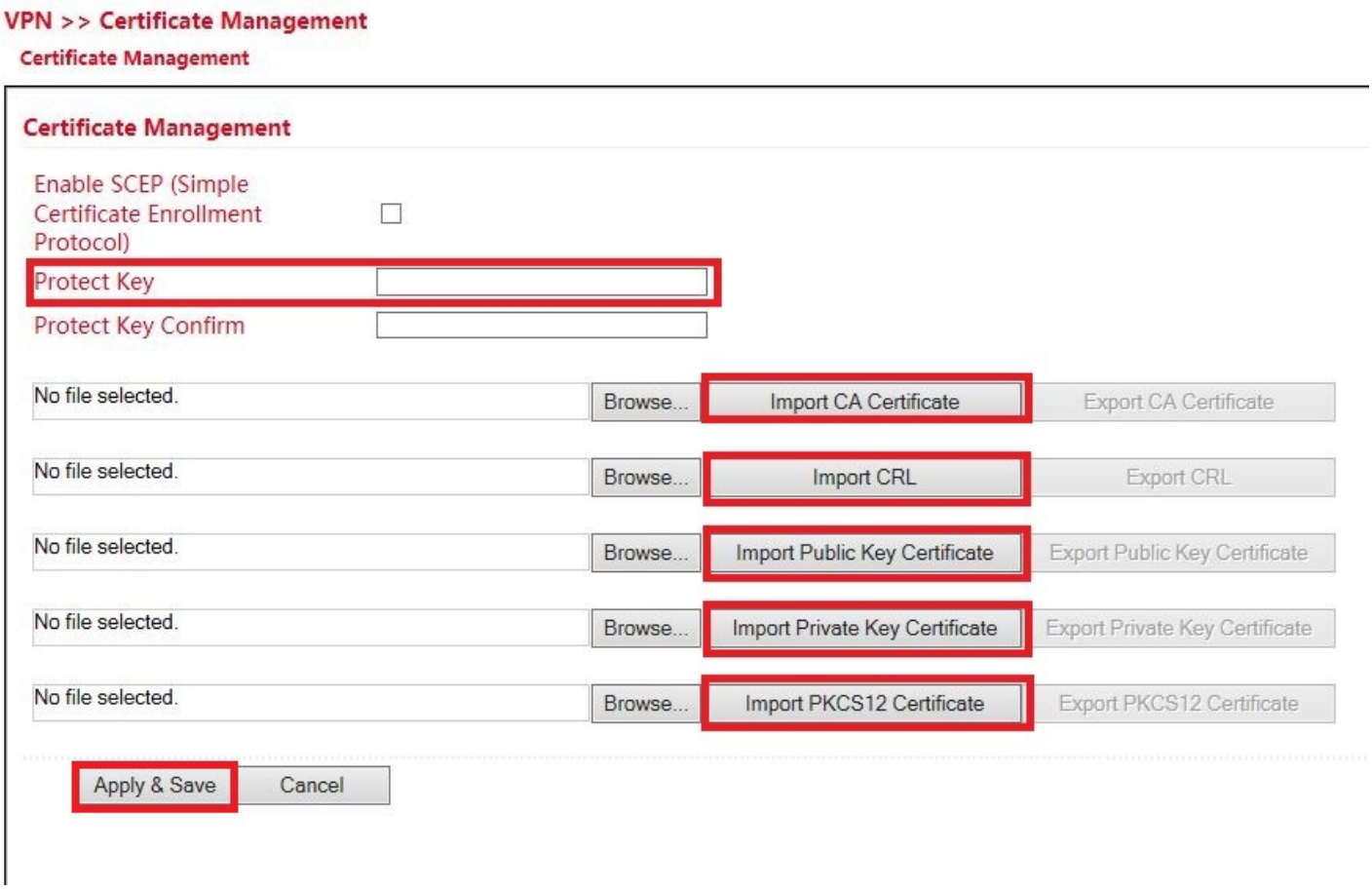
GRE wird verwendet, wenn dynamisches Routing über den IPSec Tunnel realisiert werden soll.

**Übersichtsseite**




## Certificate Management

Im Zertifikat Management (Certificat 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, muss man 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.
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. |
| Protec Key Confirm | Das Zertifikatpasswort erneut eingeben um die Richtigkeit des eingegebenen Passwortes zu bestätigen. |
| Import CA Certificate | Certificate Authority (CA) ist das Zertifikat der Zertifizierungsstelle. |
| Import CRL | Certificate Revocation List ist die Zertifikatsperrliste. |
| 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 PKCS12 Certifikate | PKCS12 Zertifikat |

## Industrial

Die Industrial Funktionen sind bei allen Modellen der TK800 Serie mit EX im Namen verfügbar. Beispiel: TK802L-**EX**0.

Folgende Funktionen sind verfügbar:

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

## 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. Unter dem Punkt finden sich die Parameter für die RS-232 Schnittstelle 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.

### DTU 1 / DTU 2

**Transparent**

| | |
|---|---|
| Enable | ☑ |
| DTU Protocol | Transparent |
| Protocol | TCP Protocol |
| Connection Type | Long-lived |
| Keepalive Interval | 60 s |
| Keepalive Retry | 5 |
| Serial Buffer Frame | 4 |
| Packet Size | 1024 Bytes |
| Force Transmit Timer | 100 ms |
| Min Reconnect Interval | 15 s |
| Max Reconnect Interval | 180 s |
| Multi-server policy | parallel |
| Source Interface | IP |
| Local IP Address | |
| DTU ID | |
| Enable Debug | ☐ |

**Destination IP Address**

| Server Address | Server Port |
|---|---|
| | |

Add

**TCP-Server**

| | |
|---|---|
| Enable | ☑ |
| DTU Protocol | TCP-Server |
| Connection Type | Long-lived |
| Keepalive Interval | 60 s |
| Keepalive Retry | 5 |
| Local Port | 10001 |
| Serial Buffer Frame | 4 |
| Packet Size | 1024 Bytes |
| Force Transmit Timer | 100 ms |
| Source Interface | cellular 1 |
| Enable Debug | ☐ |

**RFC2217**

| | |
|---|---|
| Enable | ☑ |
| DTU Protocol | RFC2217 |
| Local Port | 3696 |
| Source Interface | cellular 1 |
| Enable Debug | ☐ |

**IEC60870-5-101/104**

| | |
|---|---|
| Enable | ☑ |
| DTU Protocol | IEC101-104 |
| 101 Mode | Balance |
| 101 Link Address Size | One Byte |
| 101 Link Address | 1 |
| 101 COT Size | One Byte |
| 101 ASDU Address Size | Two Bytes |
| 101 IOA Size | Two Bytes |
| 104 COT Size | Two Bytes |
| 104 Port | 2404 |
| Source Interface | cellular 1 |
| Enable Debug | ☐ |

## Serial Port

**Serial Port 1**

| | |
|---|---|
| Serial Type | RS232 |
| Baudrate | 9600 |
| Data Bits | 8 bits |
| Parity | None |
| Stop Bit | 1 bit |
| Software Flow Control | ☐ |
| Description | RS232 |

**Serial Port 2**

| | |
|---|---|
| Serial Type | RS485 |
| Baudrate | 9600 |
| Data Bits | 8 bits |
| Parity | None |
| Stop Bit | 1 bit |
| Software Flow Control | ☐ |
| Description | RS485 |

## Status IO

**Digital Input**

| | |
|---|---|
| Digital Input 1 | LOW (0) |

**Relay Output**

| | |
|---|---|
| Relay Output 1 | ON |
| Action | OFF |
| | ON |
| | OFF -> ON OFF Time: 1000 ms |

## Tools

### Ping

| | | |
|---|---|---|
| Host | 8.8.8.8 | Ping |
| Ping Count | 4 | |
| Packet Size | 32 | Bytes |
| Expert Options | | |

```
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
```

### Traceroute

| | | |
|---|---|---|
| Host | 8.8.8.8 | Trace |
| Maximum Hops | 20 | |
| Timeout | 3 s | |
| Protocol | UDP ▼ | |
| Expert Options | | |

```
traceroute to 8.8.8.8 (8.8.8.8), 20 hops max, 38 byte packets
 1  *  *  *
 2  *  *  *
 3  *  *  *
 4  *  *  *
 5  *  *  *
 6  *  *  *
 7  *  *  *
 8  *  *  *
 9  *  *  *
10  *  *  *
11  *  *  *
12  *  *  *
13  *  *  *
14  *  *  *
15  n-ea5-i.N.DE.NET.DTAG.DE (62.154.52.74)  33.547 ms  31.671 ms  32.034 ms
16  217.239.41.122 (217.239.41.122)  35.252 ms  217.239.41.42 (217.239.41.42)  37.080 ms  217.239.41.122
(217.239.41.122)  35.465 ms
17  74.125.50.149 (74.125.50.149)  35.157 ms  33.953 ms  35.958 ms
18  64.233.175.121 (64.233.175.121)  35.045 ms  209.85.252.77 (209.85.252.77)  36.931 ms  72.14.239.133
```

## Link Speed Test

C:\fakepath\test.file | Browse... | upload | download

# CE Deklaration

wireless | m2m-networks | sensors

welotec

vision meets solution

## CE declaration of conformity

**Holder:**
Welotec GmbH
Zum Hagenbach 7
48366 Laer
GERMANY

declares that the products:

**Product:**
Wireless Router

**Identification:**
TK802U
TK802U-EX0
TK802L
TK802L-EX0
TK805L-EX0

**Complies with:**
- R&TTE Directive 1999/5/EC of 09 March 1999,
- Council Recommendation 1999/519/EC of 12 July 1999,
- Regulations of standard ETSI EN 301 489-7 V1.3.1 (05),
- ROHS Compilant: Directive 2002/95/CE,

**Safety:**
- EN 60950-1: 2006

**EMC:**
- EN301511

CE

The corresponding markings appear under the appliance.

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

07.01.15
Date

Tobias Kiwitt (Welotec GmbH)