

TK500v2 Router Serie

Ausführung:
v1.0.42

Datum:
16.12.2024



Inhaltsverzeichnis

1	Einführung	3
1.1	Hinweis zum Copyright	3
1.2	Marken	3
1.3	Rechtlicher Hinweis	3
1.4	Kontaktinformationen für technischen Support	3
1.5	Beschreibung	3
1.6	Wichtiger Sicherheitshinweis:	4
1.7	Checkliste für Inhalt	4
1.8	Produktinformationen	5
2	Regulatory Compliances	7
2.1	CE and UKCA Notice	7
3	Installationshandbuch	8
3.1	Typische Anwendung	8
3.2	Anschlussplan	8
3.3	Schneller Internetanschluss	9
3.4	Zurücksetzen auf Werkseinstellungen	16
4	System	18
4.1	Vorbereitung	18
4.2	Basic Setup	20
4.3	Time	20
4.4	Serial Port	21
4.5	Admin Access	22
4.6	System Log	24
4.7	Config Management	24
4.8	Scheduler	25
4.9	Upgrade	25
4.10	Reboot	26
4.11	Logout	27
5	Netzwerk	28
5.1	Cellular	28
5.2	WAN	30
5.3	WAN(STA)	34
5.4	VLAN	35
5.5	Switch WLAN Mode	36
5.6	WLAN Client	37
5.7	Link Backup	37
5.8	VRRP	38
5.9	IP Passthrough	40
5.10	Static Route	41
5.11	OSPF	41
6	Services	44
6.1	DHCP Service	44
6.2	DNS	45
6.3	DNS Relay	45
6.4	DDNS (Dynamic DNS)	46

6.5	DTU	48
6.6	SMS	49
6.7	Traffic Manager	51
6.8	Alarm Manager	52
7	Firewall	53
7.1	Basic	53
7.2	Filtering	53
7.3	Content Filtering	54
7.4	Port Mapping	54
7.5	Virtual IP Mapping	55
7.6	DMZ	56
7.7	MAC-IP Bundling	57
7.8	NAT	57
8	QoS	59
8.1	IP BW Limit	59
9	VPN	60
9.1	IPSec Settings	60
9.2	IPSec Tunnels	61
9.3	GRE Tunnels	63
9.4	L2TP Clients	64
9.5	PPTP Clients	66
9.6	OpenVPN Tunnels	68
9.7	OpenVPN Advanced	70
9.8	Certificate Management	71
10	Tools	73
10.1	PING	73
10.2	Traceroute	73
10.3	Link Speed Test	74
10.4	TCPDUMP	75
11	Application	76
11.1	SMART-EMS	76
12	Status	77
12.1	System	77
12.2	Modem	77
12.3	Traffic Statistics	78
12.4	Alarm	78
12.5	WLAN	79
12.6	Network Connections	79
12.7	Route Table	80
12.8	Device List	80
12.9	Log	80
12.10	Third Party Software	81
13	Technische Daten	82
13.1	Geräteeigenschaften	82
13.2	Umgebungsbedingungen	82
13.3	Funkfrequenzen	82
13.4	Funkfrequenzen UMTS Asien	83
14	Support	85

1 Einführung

1.1 Hinweis zum Copyright

Copyright © 2018 Welotec GmbH Alle Rechte vorbehalten.

Eine Vervielfältigung ohne Genehmigung ist nicht gestattet.

1.2 Marken

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

1.3 Rechtlicher Hinweis

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

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

1.4 Kontaktinformationen für technischen Support

Welotec GmbH Zum Hagenbach 7

48366 Laer

Tel.: +49 2554 9130 00

Fax.: +49 2554 9130 10

Email: support@welotec.com

1.5 Beschreibung

Die Router der TK500-Serie für den Industriebereich stellen eine stabile Hochgeschwindigkeitsverbindung zwischen Remotegeräten und Kundenstandorten über LAN und (modellabhängig) über WLAN bzw. 2G/3G/4G Netzwerke bereit. Sie können in einem Spannungsbereich von 12 bis 24 V DC betrieben werden und verfügen über einen Temperaturbereich von -15°C bis 70°C bei einer relativen Luftfeuchtigkeit von 95 %, wodurch eine hohe Stabilität und Zuverlässigkeit unter strengen Bedingungen gewährleistet ist. Der TK500 kann auf dem Arbeitsplatz verwendet werden oder auf DIN-Schienen montiert werden.

Produkte der TK500-Serie unterstützen VPN (IPSec/PPTP/ L2TP/GRE/SSL VPN), was sichere Verbindungen zwischen Remotegeräten und Kundenstandorten garantiert.

1.6 Wichtiger Sicherheitshinweis:

1.6.1 Dieses Produkt ist für folgende Einsatzbereiche nicht geeignet

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

1.6.2 Warnung

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

1.6.3 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 Wiederverwendung, des Recyclings und anderer Formen der Wiederverwertung. Das WEEE-Logo (siehe Abbildung links) 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.

1.7 Checkliste für Inhalt

Jeder TK500-Funkrouter wird in einem Paket mit Standardzubehör ausgeliefert. Weiteres Zubehör kann bestellt werden. Überprüfen Sie den Inhalt Ihres Pakets sorgfältig, und falls etwas fehlt oder beschädigt ist, wenden Sie sich an Ihren Vertriebspartner von der Welotec GmbH.

1.7.1 Lieferumfang

Standardzubehör

Zubehör	Anzahl	Beschreibung
TK500-Router	1	Industrieller Router der Serie TK500
Netzwerkkabel	1	Netzwerk-Kabel CAT5, 1,5 Meter
Handbuch	1	Datenträger mit Handbuch
Lizenzbedingungen	1	“Third Party Software Notifications and Licenses”
Stromversorgung		
Terminalblock	1	7-Polige Anschlussklemme für Stromversorgung

Bestandteile Set (Modellabhängig)

Produkt	Anzahl	Beschreibung
TK500-Router	1	Industrieller Router der Serie TK500
Netzwerkkabel	1	Netzwerk-Kabel CAT5, 1,5 Meter
Mobilfunkantenne	1	5 m Magnetfußantenne (TK515L, TK515L-W, TK505U) 2G/3G/
WLAN-Antenne	2	Aufsteckantennen (WLAN) (TK515L-W)
Handbuch	1	Datenträger mit Handbuch
Lizenzbedingungen	1	“Third Party Software Notification and Licenses”
Stromversorgung		
		Tischnetzteil, Eingang 100-240 V AC, Ausgang 12 V DC (für TK5xx), inkl. 7-poliger Terminalblock
	1	Stecker, europäischer Standard

1.8 Produktinformationen

1.8.1 Umgebungsbedingungen

Betriebstemperatur: -15 bis 70°C

Relative Luftfeuchtigkeit während des Betriebs: 5 bis 95 % nicht kondensierend

Lagertemperatur: -40 bis +85°C

1.8.2 Stromversorgung

Stromversorgung: 1 Klemmleiste (7-polig) inkl. Spannungsbuchse und serieller Anschluss

Eingangsspannung: 12 - 24 V DC

1.8.3 Physikalische Eigenschaften

Gehäuse: Stahl, Schutzart IP30

Gewicht: 450 g

Abmessungen (mm): 35 x 127 x 108,2 mm

2 Regulatory Compliances

2.1 CE and UKCA Notice

2.1.1 Complies with: RADIO EQUIPMENT DIRECTIVE 2014/53/EU and Radio Equipment Regulations 2017 (SI 2017 No. 1206)

Article 3.1a Safety: Low Voltage Directive 2014/35/EU

- EN 62368-1 :2020

Article 3.1a Health:

- EN 62311:2020

Article 3.1b EMC: EMC Directive 2014/30/EU

- EN 55032:2020
- EN 55035:2019
- EN 61000-3-2:2019
- EN 61000-3-3:2019

Article 3.2 Radio:

- ETSI EN 301 328 V2.2.2 (2019-07)
- ETSI EN 301 489-1 V2.2.3 (2019-11)
- ETSI EN 301 489-17 V3.2.4 (2020-09)
- ETSI EN 301 489-52 V1.2.1 (2021-11)
- ETSI EN 301 511 V12.5(2017-03)
- ETSI EN 908-1 V15.1 (2021-09)
- ETSI EN 908-2 V13.1.1 (2020-06)
- ETSI EN 908-13 V13.2.1 (2022-02)

RoHS 2 Directive 2011/65/EU & 2015/863/EU

The corresponding markings are located on the device:



3 Installationshandbuch

3.1 Typische Anwendung

Mit Routern der TK500-Serie können Sie Geräte mit Ethernet, WLAN oder RS-232/485 über GPRS/HSUPA/UMTS/LTE mit dem Internet verbinden. Zur Gewährleistung der Sicherheit und eines unterbrechungsfreien Zugriffs unterstützt die TK500-Serie VPN-Verbindungen und ermöglicht somit den Remotezugriff und eine sichere Datenübertragung über das Internet.

3.2 Anschlussplan

Schnittstelle	Beschreibung
Stromanschluss	12-24 V DC
Seriell	RS 232, RS 485
Ethernet-Ports	Fünf 10/100Base-TX RJ45-Ports
Antennenanschluss (Mobilfunk)	SMA (f)
Antennenanschluss (WLAN)	SMA-R (f)
SIM-Kartenfach	Fach zum Einlegen der SIM-Karte (TK525L-W, TK525L, TK525U)

3.2.1 Anschluss der seriellen Schnittstellen und I/O's

Beschreibung der LED-Leuchten:

 = LED leuchtet
  = LED leuchtet nicht
  = LED blinkt

Legende: Leuchtet: Ein- Leuchtet nicht: Aus- Blinkt: Blinkend-

Signal	Ein	Aus	Blinkend
Einschalten	PWR, STATUS, WARN	ERR	
Ausführung der Firmware	PWR, WARN	ERR	STATUS
Einwahl ins Internet	PWR	ERR	STATUS, WARN
Verbindung herstellen	PWR	WARN, ERR	STATUS
Firmware aktualisieren	PWR		STATUS, WARN, ERR
Werkseinstellungen zurücksetzen	PWR	WARN	STATUS, ERR

Beschreibung der LED-Signale



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)

3.3 Schneller Internetanschluss

3.3.1 Einstecken der SIM-Karte

Öffnen Sie das TK-Router SIM/UIM-Fach oben am Gerät und legen Sie die SIM-Karte in den Kartenträger ein.

3.3.2 Installation der Antenne

Verbinden Sie nach der Installation des TK500 die Antenne und schrauben Sie die Antenne fest. Stellen Sie die Antenne dort auf, wo eine gute Signalstärke erreicht wird.



Hinweis

Position und Winkel können sich auf die Signalstärke auswirken.

3.3.3 Stromversorgung

Verbinden Sie die im Lieferumfang enthaltene Spannungsversorgung mit dem Gerät, und achten Sie darauf, ob die LED-Anzeige für „Power“ aufleuchtet. Wenden Sie sich an den technischen Support von Welotec, wenn keine Anzeige aufleuchtet. Sie können den TK500 konfigurieren, wenn die Power-Anzeige blinkt.

3.3.4 Verbinden

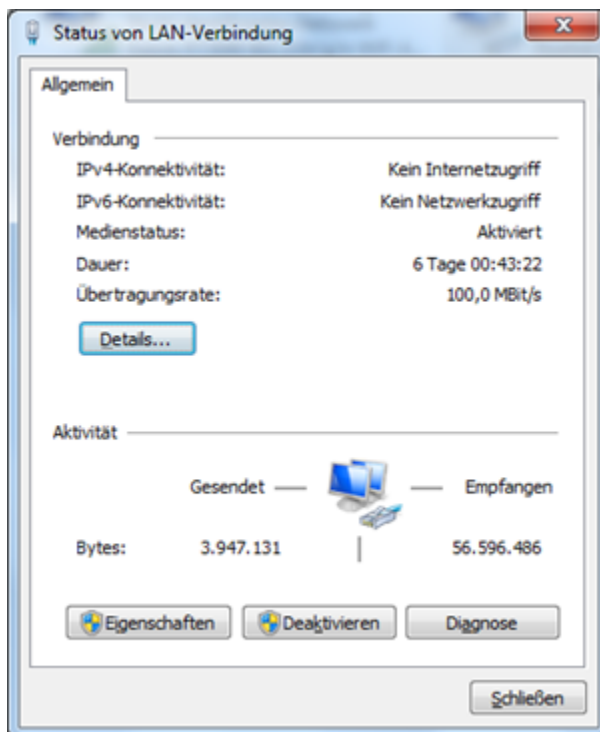
Verbinden Sie den TK500 mit dem PC:

1. Schließen Sie das Ethernet Kabel des TK500 an den PC an.
2. Anschließend leuchtet eine LED-Anzeige der RJ45-Schnittstelle grün auf und die anderen Anzeigen blinken.

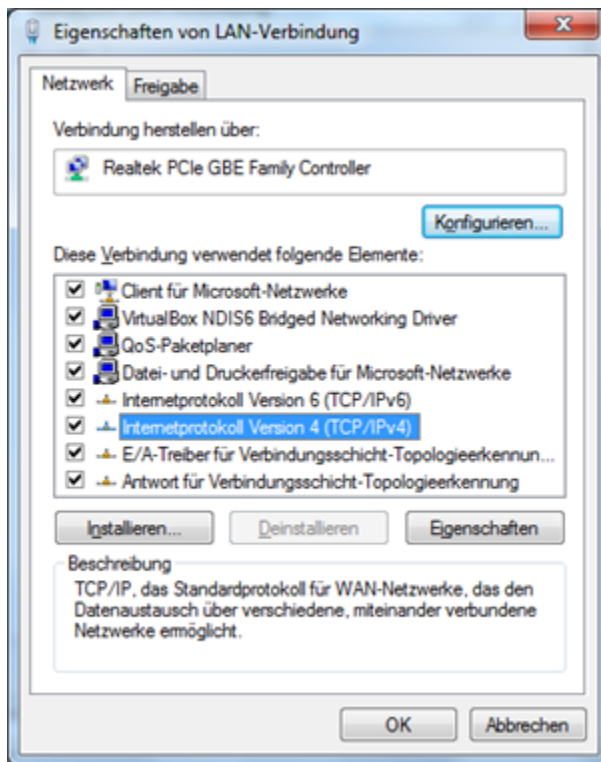
3.3.5 Erstes Anschließen des TK-Router-Geräts an den PC

Der TK500-Router kann IP-Adressen für den PC automatisch vergeben. Richten Sie den PC so ein, dass IP- Adressen über DHCP automatisch abgerufen werden. (Grundlage ist das Windows-Betriebssystem):

1. Öffnen Sie die Systemsteuerung, doppelklicken Sie auf das Symbol „*Netzwerk- und Freigabecenter*“ und öffnen Sie so den Bildschirm „*Netzwerk- und Freigabecenter*“.
2. Klicken Sie auf „*LAN-Verbindung*“ und öffnen Sie den Bildschirm mit dem „*Status von LAN-Verbindung*“:

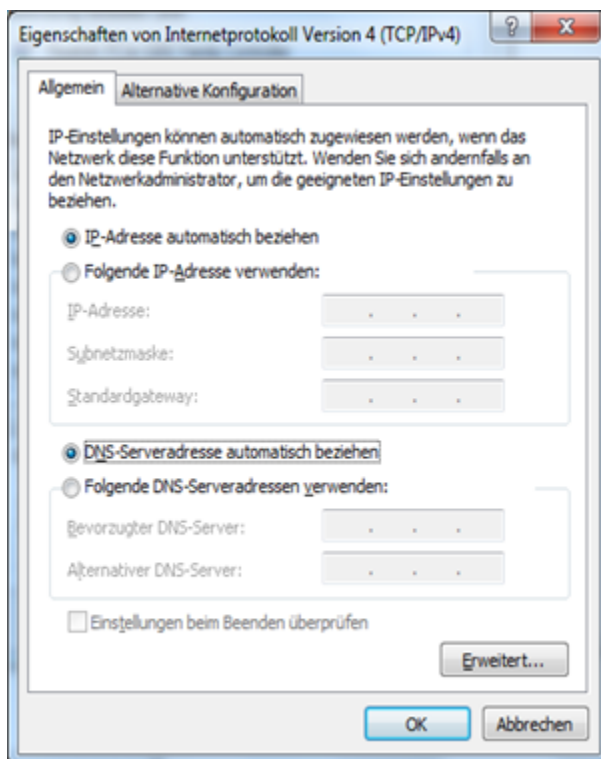


3. Klicken Sie auf „*Eigenschaften*“, und öffnen Sie den Bildschirm mit den Eigenschaften der LAN-Verbindung:



4. Wählen Sie „*Internetprotokoll Version 4 (TCP/IPv4)*“ aus, klicken Sie auf die Schaltfläche „*Eigenschaften*“, und überprüfen Sie, ob Ihr PC IP- und DNS-Adresse automatisch beziehen kann. (Sie können den PC auch im Subnetz einrichten: 192.168.2.0/24, z. B. IP: 192.168.2.10, Netzmaske: 255.255.255.0, Standardgateway: 192.168.2.1)

Durch Klicken auf „*OK*“ weist der TK-Router dem PC eine IP-Adresse zu: 192.168.2.X, sowie das Gateway: 192.168.2.1 (die Standardadresse des TK500).



Nach dem Konfigurieren der TCP/IP-Protokolle können Sie mit dem Ping-Befehl überprüfen, ob die Verbindung

zwischen PC und Router fehlerfrei aufgebaut wird. Es folgt ein Beispiel für das Ausführen des Ping-Befehls unter Windows 7 :

Windows-Taste+R -> Eingabe "cmd" -> Entertaste -> Eingabe "Ping 192.168.2.1" -> Entertaste Bei dieser Anzeige:

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\>ping 192.168.2.1

Ping wird ausgeführt für 192.168.2.1 mit 32 Bytes Daten:
Antwort von 192.168.2.1: Bytes=32 Zeit=1ms TTL=64
Antwort von 192.168.2.1: Bytes=32 Zeit<1ms TTL=64
Antwort von 192.168.2.1: Bytes=32 Zeit<1ms TTL=64
Antwort von 192.168.2.1: Bytes=32 Zeit<1ms TTL=64

Ping-Statistik für 192.168.2.1:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 1ms, Mittelwert = 0ms

C:\Users\>_
```

Die Verbindung zwischen PC und Router wurde richtig aufgebaut.

Im folgenden Beispiel gibt es Fehler:

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\>ping 192.168.2.1

Ping wird ausgeführt für 192.168.2.1 mit 32 Bytes Daten:
PING: Fehler bei der Übertragung. Allgemeiner Fehler.
PING: Fehler bei der Übertragung. Allgemeiner Fehler.
PING: Fehler bei der Übertragung. Allgemeiner Fehler.
PING: Fehler bei der Übertragung. Allgemeiner Fehler.

Ping-Statistik für 192.168.2.1:
    Pakete: Gesendet = 4, Empfangen = 0, Verloren = 4
    (100% Verlust),

C:\Users\>_
```

Die Verbindung funktioniert nicht richtig, und Sie sollten die Anweisungen erneut durchgehen und Ihre Einstellungen überprüfen.

3.3.6 Konfigurieren des TK500 (Optional)

Nachdem Sie die im vorherigen Kapitel beschriebenen Schritte ausgeführt haben, können Sie den Router konfigurieren:

1. Öffnen Sie einen beliebigen Internet Browser (z.B. Google Chrome) und geben Sie die Standard-IP-Adresse des Routers ein: <http://192.168.2.1>. Es wird folgende Anmeldeseite geöffnet:



Geben Sie den Benutzernamen (Standard: adm) sowie das Kennwort (Standard: 123456) ein, und klicken Sie dann auf „**Login**“, um den Konfigurationsbildschirm zu öffnen.

2. Ändern Sie die IP-Konfiguration:

Wenn Sie eine eigene IP festlegen möchten, befolgen Sie die nachstehenden Anweisungen:

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								

System Status

Name	Router
Serial Number	RF6152104290001
Description	TK525L-W-v2
Current Version	V1.0.10
Current Bootloader Version	1.1.3.r4955
Router Time	2021-09-24 15:47:02
PC Time	2021-09-24 15:47:02
Up time	0 day, 00:13:20
CPU Load (1 / 5 / 15 mins)	0.03 / 0.03 / 0.03
Memory consumption Total/Free	121.27MB / 94.93MB (78.28%)

1. Klicken Sie auf **Network >VLAN**.

2. Um eine VLAN ID hinzuzufügen, klicken Sie auf „**Add**“

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								

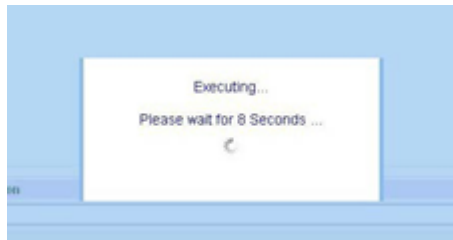
VLAN

VLAN ID	LAN1	LAN2	LAN3	LAN4	Primary IP/Netmask
1	✓	✓	✓	✓	192.168.2.1/255.255.255.0 ✖
<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>					

Ändern Sie die IP-Adresse bspw. in **192.168.1.254** und wählen Sie die LAN-Ports aus, die dieser IP-Adresse zugewiesen werden sollen.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
VLAN								
VLAN ID	<input type="text" value="2"/>							
VLAN Virtual Interface								
Primary IP								
IP Address	<input type="text" value="192.168.1.254"/>							
Netmask	<input type="text" value="255.255.255.0"/>							
MTU	<input type="text" value="1500"/>							
Secondary IP(s)								
	IP Address		Netmask					
	<input type="text"/>		<input type="text"/>					
	<input type="button" value="Add"/>							
VLAN Member Ports								
LAN1	LAN2	LAN3	LAN4					
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>					
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Back"/>								

3. Klicken Sie auf „**Apply**“, und folgender Bildschirm wird angezeigt:



Die IP-Adresse des TK500 wurde geändert. Damit Sie nun wieder auf die Konfigurationsseite zugreifen können, muss der PC in demselben Subnetz eingerichtet sein, beispielsweise: **192.168.1.10/24** – Geben Sie dann die geänderte IP-Adresse (**192.168.1.254**) in Ihrem Browser ein.

3.3.7 Den TK-Router mit dem Internet verbinden

Führen Sie die folgenden Konfigurationsschritte aus, um eine Verbindung zwischen dem TK500 und dem Internet herzustellen.

Klicken Sie auf **Network > Cellular**, und aktivieren Sie die Funktion durch **Enable**:

System Network Services Firewall QoS VPN Tools Application Status

Your password have security risk, please click here to change!

Cellular

Enable
 Time schedule Schedule Management
 PPPoE Bridge
 Shared Connection(NAT)
 Default Route
 SIM1 Network Provider Manage
 Network Select Type
 Static IP
 Connection Mode
 Redial Interval Seconds
 Show Advanced Options

Profiles

Index	APN	Access Number	Authentication Type	Username	Password
1		*99#	Auto		
		*99#	Auto		

Add

Apply Cancel

Überprüfen Sie die Einträge und wählen Sie unter **SIM1 Network Provider** einen voreingestellten Netzwerk-Provider aus, oder fügen Sie ein selbsterstelltes Profil eines Providers hinzu:

Sie erhalten die APN, die Einwahlnummer, den Benutzernamen und das Kennwort von Ihrem lokalen Netzwerkanbieter. Erkundigen Sie sich dort nach den Einzelheiten.

Über **Show Advanced Options** können Sie weitere Einstellungen tätigen, wie z.B. den PIN Code, wenn dieser auf der SIM-Karte gesetzt ist.

Show Advanced Options

Dual SIM Enable

Initial Commands

Binding ICCID

PIN Code

Dial Timeout Seconds

MTU

MRU

TX Queue Length

Enable IP head compression

Use default asyncmap

Use Peer DNS

Link Detection Interval Seconds(0: disable)

Link Detection Max Retries

Debug

Debug Modem

Expert Options

ICMP Detection Mode

ICMP Detection Server

ICMP Detection Interval Seconds

ICMP Detection Timeout Seconds

ICMP Detection Retries

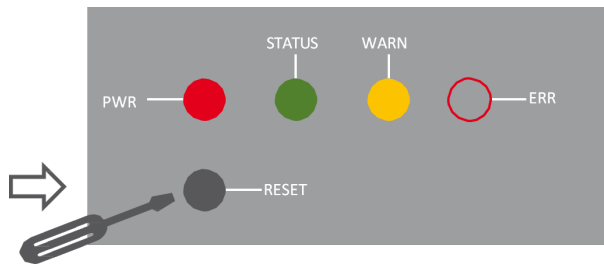
Wenn Sie die richtige Konfiguration festgelegt haben, kann der TK500 nun eine Verbindung mit dem Internet herstellen. Öffnen Sie einen Internet Browser, geben Sie „www.welotec.com“ ein, und die Website von Welotec wird geöffnet.

3.4 Zurücksetzen auf Werkseinstellungen

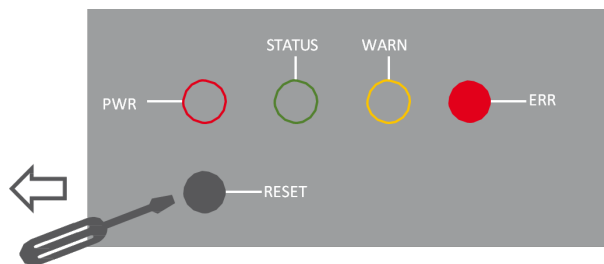
3.4.1 Hardwaremethode

 = LED leuchtet
  = LED leuchtet nicht
  = LED blinkt

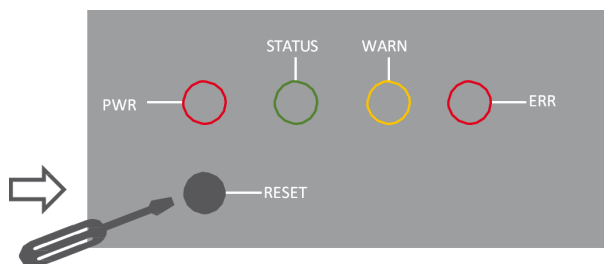
1. Drücken Sie die **RESET-Taste**, während Sie den TK500 einschalten:



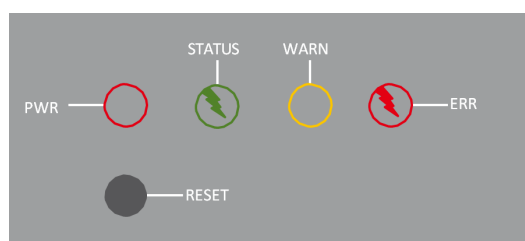
2. Sobald die LED-Leuchte ERROR aufleuchtet (ca. 10 Sekunden nach dem Einschalten), lassen Sie die **RESET-Taste** los:



3. Nach einigen Sekunden hört die LED-Leuchte ERROR auf zu leuchten. 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

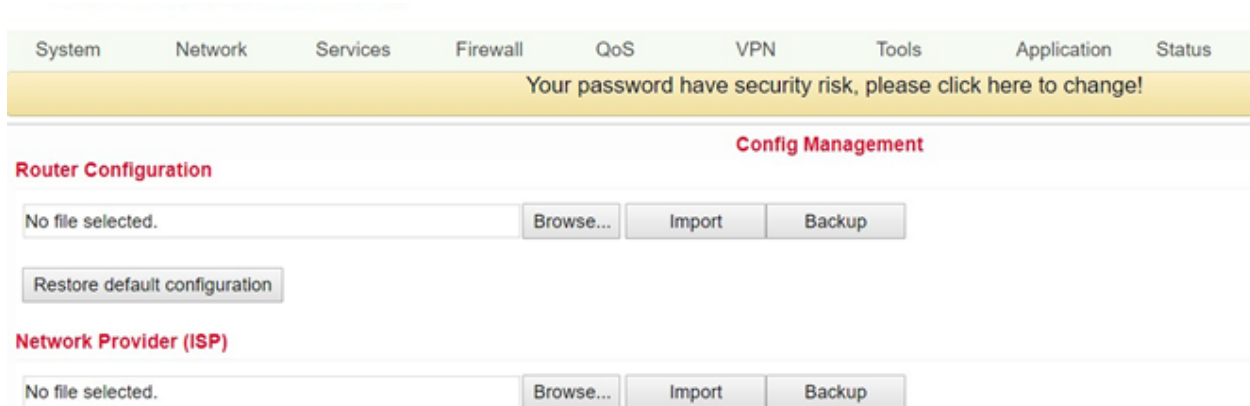
- Benutzername: adm

- Passwort: 123456

- Serieller Parameter: 115200-N-8-1

3.4.2 Webmethode

1.) Melden Sie sich an der webbasierten Benutzeroberfläche des TK500 an und wählen Sie *System > Config Management* aus:



The screenshot shows the web interface of the TK500 router. At the top, there is a navigation menu with tabs: System, Network, Services, Firewall, QoS, VPN, Tools, Application, and Status. Below the menu is a yellow warning banner that reads: "Your password have security risk, please click here to change!". The main content area is titled "Config Management" and is divided into two sections: "Router Configuration" and "Network Provider (ISP)".

Router Configuration

No file selected.

Network Provider (ISP)

No file selected.

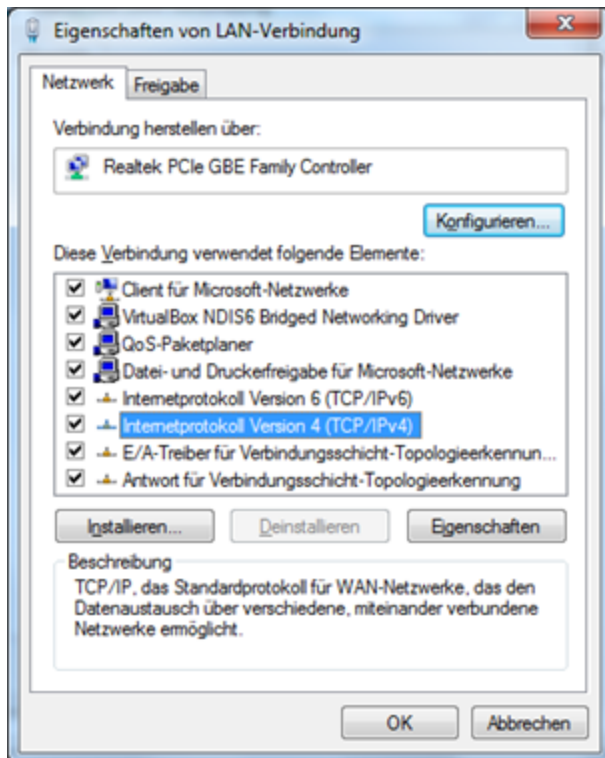
2.) Klicken Sie auf *Restore default configuration*, um den TK500 auf seine Werkseinstellungen zurückzusetzen. Danach wird der Router neu gebootet.

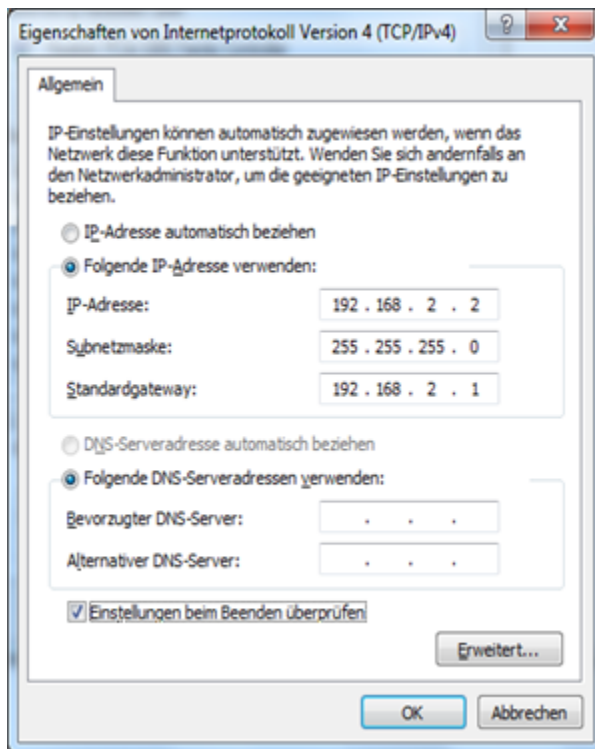
4 System

Der TK-500 Router muss vor der Verwendung ordnungsgemäß konfiguriert sein. In diesem Kapitel wird die webbasierte Konfiguration beschrieben.

4.1 Vorbereitung

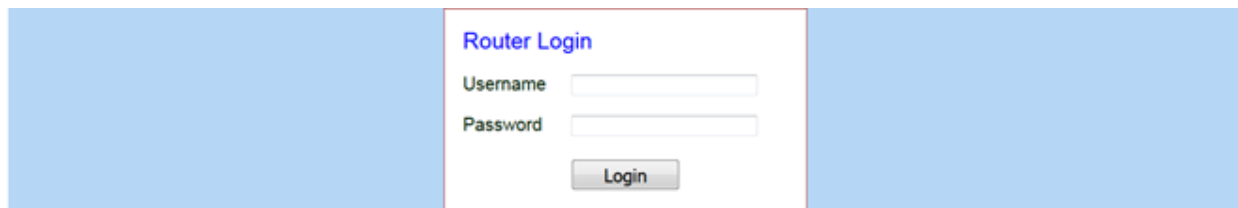
Verbinden Sie Ihre Geräte zunächst per Kabel oder Hub (Switch) mit dem TK500 und legen Sie die IP-Adresse für den PC und TK500 in demselben Subnetz fest, z. B.: legen Sie die PC-IP-Adresse auf 192.168.2.2 fest, Netzmaske: 255.255.255.0, Gateway (Standard-IP des TK500: 192.168.2.1):





Öffnen Sie einen Internet Browser, und geben Sie die IP-Adresse des TK500 ein: <http://192.168.2.1> (Standard-IP des TK500).

Auf der folgenden Anmeldeseite müssen Sie sich als Administrator anmelden. Geben Sie den Benutzernamen und das Kennwort ein (Standard: *adm/123456*).



Klicken Sie auf „Login“, um die Konfigurationsseite zu öffnen.



System Status	
Name	Router
Serial Number	RL6151823435201
Description	TK525L
Current Version	2.3.0.r4648
Current Bootloader Version	1.1.3.r4560
Router Time	2018-10-01 13:58:23
PC Time	2018-10-01 13:58:24 Sync Time
Up time	0 day, 00:08:19
CPU Load (1 / 5 / 15 mins)	1.00 / 0.48 / 0.20
Memory consumption	27.73MB / 7,140.00KB (25.14%)
Total/Free	

System

Die Systemeinstellungen umfassen die folgenden zehn Bereiche: Basic Setup, Time, Serial Port, Admin Access,

System Log, Config Management, Scheduler, Upgrade, Reboot und Logout.

System	Net
Basic Setup	
Time	
Serial Port	
Admin Access	
System Log	
Config Management	
Scheduler	
Upgrade	
Reboot	
Logout	

4.2 Basic Setup

Im Basic Setup können Sie die Sprachführung des Menüs, sowie den Hostnamen anpassen. Erreichbar ist dieser Menüpunkt über *System > Basic Setup*.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
Basic Setup								
Language	English ▾							
Hostname	Router							
Apply		Cancel						

Parametername	Beschreibung	Standard	Beispiel
Language	Sprache für Konfigurationsseite festlegen	English	English
Host Name	Hostname des TK500	Router	Mein Router

4.3 Time

In diesem Menüpunkt lässt sich die Systemzeit des Routers anpassen. Weiter ist es hier möglich einen Zeitserver (NTP Time Server) einzurichten um die Systemzeit automatisch aktuell zu halten.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
Time								
Router Time	2018-10-01 14:05:36							
PC Time	2018-10-01 14:05:37							<input type="button" value="Sync Time"/>
Timezone	UTC+01:00 France, Germany, Italy							
Auto Daylight Savings Time	<input checked="" type="checkbox"/>							
Auto Update Time	Every 1 hour							
Trigger Connect On Demand	<input type="checkbox"/>							
NTP Time Servers	0.de.pool.ntp.org							
	1.de.pool.ntp.org							
	2.de.pool.ntp.org							
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

Name	Beschreibung	Standard
Router Time	Uhrzeit des Routers	2017-08-01 16:00:00
PC Time	Uhrzeit des PCs (bzw. die Uhrzeit des mit dem Router verbundenen Geräts)	Über den Button Sync Time lässt sich die Zeit mit dem angeschlossenen Gerät synchronisieren
Timezone	Zeitzone festlegen	wählbare zeitzone
Auto Daylight Savings Time	Automatische Umstellung: Sommerzeit/Winterzeit	Deaktiviert
Auto Update Time	Zeitpunkt der automatischen Uhrzeitaktualisierung	Deaktiviert
NTP Time Servers (nach Aktivierung der Option „Auto Update Time“)	Einstellung für NTP-Zeitserver (Höchstens drei Einträge)	pool.ntp.org

4.4 Serial Port

Sie können über den Menüpunkt *System* > *Serial Port* die Einstellungen für die serielle Schnittstelle des Routers anpassen.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
Serial Port								
Baudrate	115200							
Data Bits	8							
Parity	None							
Stop Bit	1							
Software Flow Control	<input type="checkbox"/>							
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

Name	Beschreibung	Standard
Baud Rate	Serielle Baudrate	115200
Data Bits	Serielle Datenbits	8
Parity	Paritätsbit serieller Daten festlegen	None
Stop Bit	Stoppbit serieller Daten festlegen	1
Software Flow Control	Softwareflusssteuerung	Deaktiviert

4.5 Admin Access

In diesem Bereich können Sie wichtige Einstellungen ändern bzw. anpassen, wie z.B. das Kennwort des Administrators oder die Portbelegung für den Zugriff auf den Router. Zu erreichen sind diese Einstellungen über **System > Admin Access**.

Admin Access

Username / Password

Username

Old Password

New Password

Confirm New Password

Management

Enable	Service Type	Service Port	Local access	Remote access	Allowed addresses from WAN (Optional)	Description
<input checked="" type="checkbox"/>	HTTP	<input type="text" value="80"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/>	
<input type="checkbox"/>	HTTPS	<input type="text" value="443"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/>	
<input checked="" type="checkbox"/>	TELNET	<input type="text" value="23"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	
<input type="checkbox"/>	SSHD	<input type="text" value="22"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	
<input type="checkbox"/>	HTTP_API	<input type="text" value="4444"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	
<input type="checkbox"/>	Console					

Non-privileged users

Username	Password
<input type="text"/>	<input type="password"/>

Other Parameters

Login timeout Seconds

Name	Beschreibung	Standard
Username/Password		
Username	Benutzername für Anmeldung an der Konfigurationsseite	adm
Old Password	Zum Ändern des Kennworts ist die Eingabe des alten Kennworts erforderlich	123456
New Password	Neues Kennwort eingeben	
Confirm New Password	Neues Kennwort erneut eingeben	
Management		
HTTP/HTTPS/TELNET/SSHD/HTTP_API/Console		
Enable	Zum Aktivieren auswählen	Aktiviert
Service Type	HTTP/HTTPS/TELNET/SSHD/HTTP_API/Console	80/443/23/22/4444/Blank
Local Access	Aktiviert – Zulassen, dass Router über LAN verwaltet wird (z. B.: HTTP)	Aktiviert
Remote Access	Aktiviert – Zulassen, dass der TK500 über WAN verwaltet wird (z. B.: HTTP)	Aktiviert
Allowed addresses from WAN (Optional)	Legt den Bereich zulässiger IP-Adressen für WAN fest	Server für Steuerungsdienste können festgelegt werden, wie 192.168.2.1/30 oder 192.168.2.1
Description	Verwaltungsparameter beschreiben (ohne Auswirkung auf den TK500)	
Non-privileged users		
Username	Benutzernamen ohne Administrator-Rechte anlegen	
Password	Password für Benutzer ohne Administrator-Rechte anlegen	
Andere Parameter		
Login Timeout	Protokollzeitüberschreitung festlegen, nach diesem Wert wird Verbindung mit der Konfigurationsseite getrennt und man muss sich neu einloggen	500 Sekunden

4.6 System Log

Einstellungsmöglichkeiten für das Protokollieren von Log-Dateien. Sie erreichen diese über *System > System Log*.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
System Log								
Log to Remote System		<input checked="" type="checkbox"/>						
IP Address / Port(UDP)		<input type="text" value="192.168.2.254"/>		<input type="text" value="514"/>				
Log to Console		<input type="checkbox"/>						
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

Name	Beschreibung	Standard
Log to Remote System	Remoteprotokollserver aktivieren	Deaktiviert (wenn aktiviert, kann IP-Adresse und Port eingegeben werden)
IP Address/Port (UDP)	IP-Adresse und Port des Remoteprotokollservers festlegen	Port: 514
Log to Console	Ausgabe des Logs auf der seriellen Schnittstelle	Deaktiviert

4.7 Config Management

Sichern und Importieren von Router Konfigurationen, sowie zurücksetzen auf Werkseinstellungen des Routers und sichern bzw. wiederherstellen der Provider-Daten. Sie können diesen Menüpunkt über *System > Config Management* erreichen.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
Config Management								
Router Configuration								
No file selected.				<input type="button" value="Browse..."/>		<input type="button" value="Import"/>		<input type="button" value="Backup"/>
<input type="button" value="Restore default configuration"/>								
Network Provider (ISP)								
No file selected.				<input type="button" value="Browse..."/>		<input type="button" value="Import"/>		<input type="button" value="Backup"/>

Name	Beschreibung
Router Configuration	Konfigurationsdatei für Import/Backup hochladen/speichern
Restore default configuration	Zum Zurücksetzen des TK500 anklicken (zum Aktivieren der Standardkonfiguration muss der TK500 neu gestartet werden.)
Network Provider (ISP)	Zum Importieren oder sichern von APN, Benutzername, Kennwort und anderer Parameter von herkömmlicher Betreiber
Durchsuchen	Mit dem Durchsuchen Button können Sie die Datei mit den Einstellungen auswählen, die über Import hochgeladen werden sollen

4.8 Scheduler

Der Scheduler dient dazu den automatischen Reboot für den Router einzustellen. Sie können die Einstellungen dafür über **System > Scheduler** festlegen.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
Scheduler								
<p>Reboot</p> <p>Enable <input checked="" type="checkbox"/></p> <p>Time <input type="text" value="0:00"/></p> <p>Days <input type="text" value="Everyday"/></p> <p><input type="button" value="Apply"/> <input type="button" value="Cancel"/></p>								

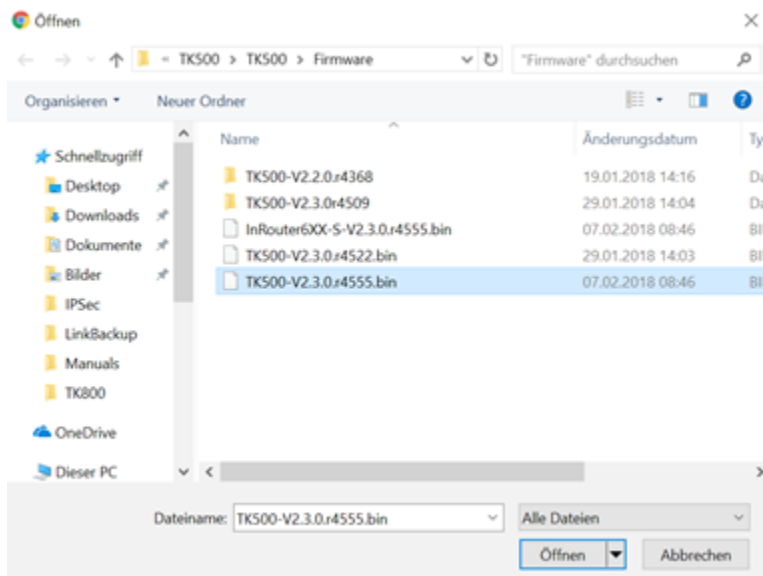
Name	Beschreibung
Enable	Schaltet den Auto Reboot ein oder aus
Time	Uhrzeit zu der der TK500 Router neu gebootet werden soll
Days	Auswahl Everyday für das tägliche neu starten

4.9 Upgrade

In diesem Bereich bietet Ihnen der Router eine Schnittstelle zum Aktualisieren der Firmware. Zu erreichen über **System > Upgrade**.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
Upgrade								
<p>Select the file to use:</p> <p>No file selected. <input type="button" value="Browse..."/> <input type="button" value="Upgrade"/></p> <p>Current Version : V1.0.10 Current Bootloader Version : 1.1.3.r4955</p>								

Wählen Sie zum Aktualisieren des Systems über den Button **Datei auswählen** die Aktualisierungsdatei (z.B. TK500-V2.2.0v4xxx.bin) in Ihrem Dateisystem aus.



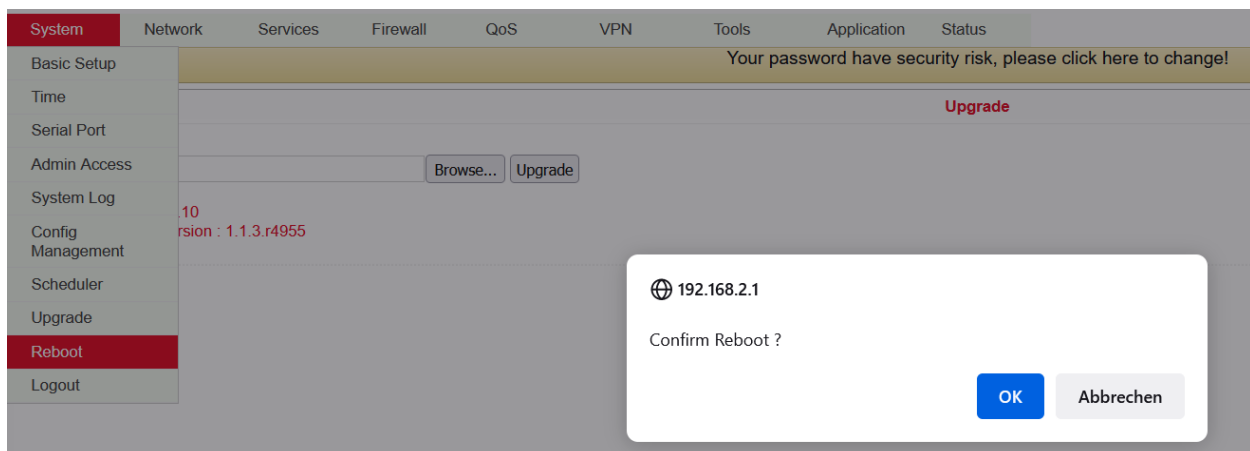
Klicken Sie auf den Button „**Upgrade**“, und bestätigen Sie den Start der Aktualisierung



Klicken Sie nach erfolgreicher Aktualisierung der Firmware auf **Reboot**, um den TK500 neu zu starten.

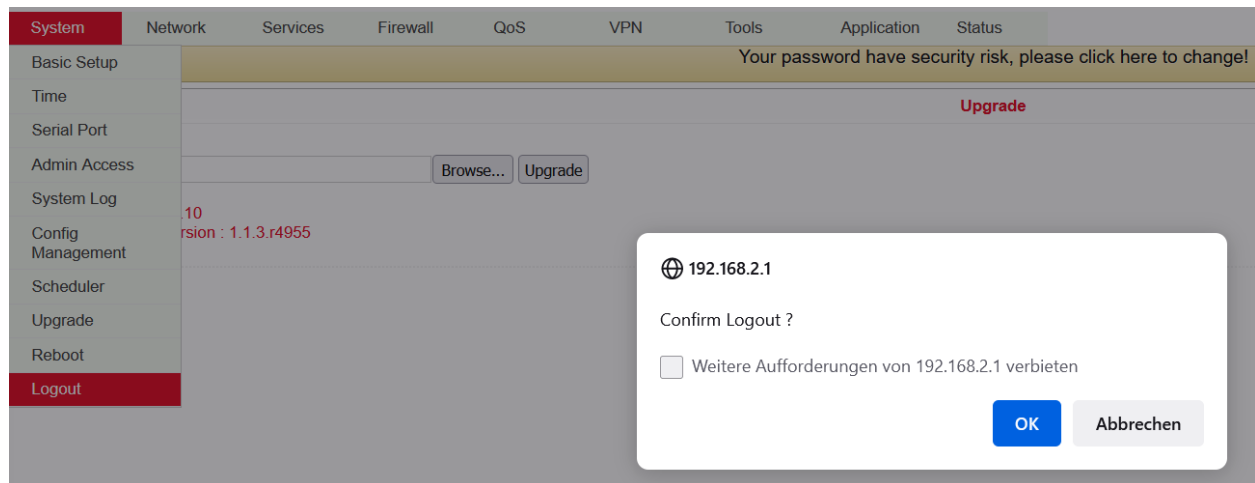
4.10 Reboot

Wenn Sie einen Neustart Ihres Routers durchführen müssen, wählen Sie **System > Reboot** aus. Klicken Sie dann auf „**OK**“, um das System neu zu starten.



4.11 Logout

Klicken Sie zum Abmelden vom System auf **System > Logout** und bestätigen Sie das Abmelden mit „OK“.



The screenshot shows the Welotec web interface with the 'System' menu selected. A confirmation dialog is displayed in the foreground, asking to confirm the logout from IP address 192.168.2.1. The dialog includes a checkbox for 'Weitere Aufforderungen von 192.168.2.1 verbieten' and buttons for 'OK' and 'Abbrechen'. The background interface shows a navigation menu on the left with 'Logout' highlighted, and a main content area with a warning message: 'Your password have security risk, please click here to change!' and an 'Upgrade' button.

5 Netzwerk

Über die Netzwerkeinstellungen konfigurieren Sie Cellular, WAN, WAN(STA), VLAN, Switch WLAN Mode, WLAN Client, Link Backup, VRRP, IP Passthrough, Static Route, OSPF

5.1 Cellular

In diesem Menübereich legen Sie die Einwahl Ihres Routers fest und konfigurieren diese. Zu erreichen über **Network > Cellular**.

System
Network
Services
Firewall
QoS
VPN
Tools
Application
Status

Your password have security risk, please click here to change!

Cellular
⌵ ⌵

Enable

Time schedule ALL Schedule Management

PPPoE Bridge

Shared Connection(NAT)

Default Route

SIM1 Network Provider T-Mobile (public IP) Manage

Network Select Type Auto

Static IP

Connection Mode Always Online

Redial Interval 30 Seconds

Show Advanced Options

Profiles

Index	APN	Access Number	Authentication Type	Username	Password
1	<input type="text"/>	*99#	Auto	<input type="text"/>	<input type="text"/>
	<input type="text"/>	*99#	Auto	<input type="text"/>	<input type="text"/>

Name	Beschreibung	Standard
Enable	Aktiviert die Dialup Funktion	Aktiviert
Time Schedule	Zeit für online und offline festlegen (s. auch 3.2.1.1)	ALL
Shared Connection (NAT)	Aktiviert – mit Router verbundenes Gerät	Aktiviert
Default Route	Mobilfunk Interface als Standard Route ins Internet	Aktiviert
Network Provider (ISP)	Lokalen ISP auswählen, falls hier nicht aufgeführt, „Custom“ auswählen	Custom
APN	APN-Parameter, die vom Provider geliefert wird	internet.t-d1.de (Telekom)
Access Number	Einwahlparameter, die vom lokalen ISP bereitgestellt werden	*99***1#
Username	Benutzername, der vom Provider bereitgestellt wird	tm
Password	Kennwort das vom lokalen ISP bereitgestellt wird	tm
Network Select Type	Mobilen Netzwerktyp auswählen (2G, 3G, 4G only)	Auto
Connection Mode	Verbindungsmodus: Router ist immer online	Always Online
Redial Interval	Wenn das Einwählen fehlschlägt, wählt der TK-Router nach diesem Intervall erneut an	30 Sekunden
Show Advanced Options	Ermöglicht das Konfigurieren erweiterter Optionen	Deaktiviert
PIN Code	Feld für die PIN Nummer der SIM Karte	Leer
MTU	MTU (Maximum Transmission Unit) festlegen	1500
Authentication Type	PAP, CHAP	Auto
Use Peer DNS	Diese Option aktivieren, um Peer-DNS zu akzeptieren	Aktiviert
Link Detection Interval	Intervall für Verbindungserkennung festlegen (0 = deaktiviert)	55 Sekunden
Debug	Debug-Modus aktivieren	deaktiviert
Debug Modem	Debug Modem aktivieren	deaktiviert
ICMP Detection Mode	Monitor Traffic: Nur wenn keine Daten fließen wird in regelmäßigen Abständen ein Keep Alive Ping gesendet.	Monitor Traffic
ICMP Detection Server	Server für ICMP-Erkennung festlegen; leeres Feld bedeutet, es ist keiner vorhanden	Leer
ICMP Detection Interval	Intervall für ICMP-Erkennung festlegen	30 Sekunden
ICMP Detection Timeout	Zeitüberschreitung für ICMP-Erkennung festlegen (TK500 wird bei ICMP-Zeitüberschreitung neu gestartet)	20 Sekunden
ICMP Detection Retries	Höchstanzahl der Wiederholungen festlegen, wenn ICMP fehlschlägt	5

5.1.1 Schedule Management

Zeitplanverwaltung (neben "Time schedule"):

Enable

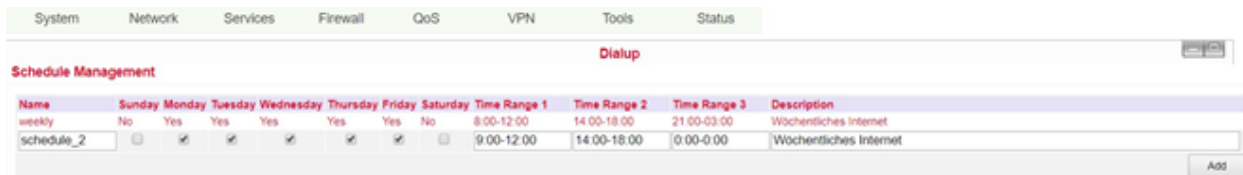


Time schedule

ALL ▾

Schedule Management

Hier kann eine eigene Dialup-Strategie gefahren werden, d.h. Sie können hier über drei Zeitbereiche festlegen, wann der Router online sein soll.



Name	Beschreibung	Standard
Name	Name für den Zeitplan	Schedule_1
Sunday	Sonntag	Leer
Monday	Montag	Aktiviert
Tuesday	Dienstag	Aktiviert
Wednesday	Mittwoch	Aktiviert
Thursday	Donnerstag	Aktiviert
Friday	Freitag	Aktiviert
Saturday	Samstag	Leer
Time Range 1	Zeitbereich 1 festlegen	9:00-12:00
Time Range 2	Zeitbereich 2 festlegen	14:00-18:00
Time Range 3	Zeitbereich 3 festlegen	0:00-0:00
Description	Konfiguration beschreiben	Leer

Sie können auch mehrere Zeitpläne erstellen, wenn z.B. an einem Arbeitstag andere Arbeitszeiten gelten.

5.2 WAN

Hier können Sie ein neues WAN (Wide Area Network) einrichten. Zu erreichen über **Network > WAN**.



Auf dieser Seite kann der Typ des WAN-Ports festgelegt werden:

Name	Beschreibung	Standard
Type	Static IP Dynamic Address(DHCP)ADSL Dialup(PPPoE)Disabled	Deaktiviert (Disabled)

Es kann immer nur ein WAN-Typ aktiviert sein. Durch die Aktivierung eines Typs wird ein anderer deaktiviert.

5.2.1 Static IP

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
WAN								
Type	Static IP ▼							
Shared Connection(NAT)	<input checked="" type="checkbox"/>							
Default Route	<input checked="" type="checkbox"/>							
MAC Address	00:18:05:0C:C3:9B		Default Clone					
IP Address	192.168.2.254							
Netmask	255.255.255.0							
Gateway	192.168.2.1							
MTU	Default ▼ 1500							
Multi-IP Settings								
IP Address	Netmask	Description						
<input type="text"/>	<input type="text"/>	<input type="text"/>						
Apply Cancel								

Name	Beschreibung	Standard
Type	Static IP	disabled
Shared Connection (NAT)	Aktiviert – mit Router verbundenes lokales Gerät kann auf das Internet zugreifen	Aktiviert
Default Route	Mobilfunk Interface als Standard Route ins Internet	Aktiviert
MAC Address	MAC-Adresse festlegen (Button Default = Standard, Clone = neuerstellte MAC Adresse)	Default
IP Address	IP-Adresse für WAN-Port festlegen	192.168.1.29
Netmask	Netzmaske für WAN-Port festlegen	255.255.255.0
Gateway	WAN-Gateway festlegen	192.168.1.1
MTU	Maximum Transmission Unit (MTU) festlegen, möglich sind die Optionen „Default“ und „Manual“	Default = 1500
„Multi-IP Settings“ (es können höchstens 8 weitere IP-Adressen festgelegt werden)		
IP Address	Weitere IP-Adresse für LAN festlegen	Leer
Netmask	Netzmaske festlegen	Leer
Description	Einstellungen beschreiben	Leer

5.2.2 Dynamic Address (DHCP)

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
WAN								
Type	Dynamic Address (DHCP) ▾							
Shared Connection(NAT)	<input checked="" type="checkbox"/>							
Default Route	<input checked="" type="checkbox"/>							
MAC Address	00:18:05:0C:C3:9B		Default		Clone			
MTU	Default ▾		1500					
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

Name	Beschreibung	Standard
Type	Dynamic Address (DHCP)	
Share Connection (NAT)	Aktiviert – mit Router verbundenes lokales Gerät kann auf das Internet zugreifen	Aktiviert
Default Route	Mobilfunk Interface als Standard Route ins Internet	Aktiviert
MAC Address	MAC-Adresse festlegen	
MTU	Maximum Transmission Unit (MTU) festlegen, möglich sind die Optionen „Default“ und „Manual“	Default = 1500

5.2.3 ADSL Dialup (PPPoE)

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
WAN								
Type	ADSL Dialup (PPPoE) ▼							
Shared Connection(NAT)	<input checked="" type="checkbox"/>							
Default Route	<input checked="" type="checkbox"/>							
MAC Address	00:18:05:0C:C3:9B		Default		Clone			
MTU	Default ▼		1492					
ADSL Dialup (PPPoE) Settings								
Username	<input type="text"/>							
Password	<input type="text"/>							
Static IP	<input type="checkbox"/>							
Connection Mode	Always Online ▼							
Show Advanced Options	<input checked="" type="checkbox"/>							
Service Name	<input type="text"/>							
TX Queue Length	<input type="text" value="3"/>							
Enable IP head compression	<input type="checkbox"/>							
Use Peer DNS	<input checked="" type="checkbox"/>							
Link Detection Interval	<input type="text" value="55"/>		Seconds					
Link Detection Max Retries	<input type="text" value="10"/>							
Debug	<input type="checkbox"/>							
Expert Options	<input type="text"/>							
ICMP Detection Server	<input type="text"/>							
ICMP Detection Interval	<input type="text" value="30"/>		Seconds					
ICMP Detection Timeout	<input type="text" value="20"/>		Seconds					
ICMP Detection Retries	<input type="text" value="3"/>							
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

Name	Beschreibung	Standard
Type	ADSL Dialup (PPPoE)	
Share Connection (NAT)	Aktiviert – mit Router verbundenes lokales Gerät kann auf das Internet zugreifen	Aktiviert
Default Route	Mobilfunk Interface als Standard Route ins Internet	Aktiviert
MAC Address	MAC-Adresse festlegen	
MTU	Maximum Transmission Unit (MTU) festlegen, möglich sind die Optionen „Default“ und „Manual“	Default = 1492
ADSL Dialup (PPPoE) Settings		
Username	Benutzernamen zum Einwählen festlegen	Leer
Password	Kennwort zum Einwählen festlegen	Leer
Static IP	Statische IP-Adressen aktivieren	Deaktiviert
Connection Mode	Verbindungsmodus festlegen („Connect on Demand“/„Always Online“/„Manual“)	Always Online
Show Advanced Options/erweiterte Optionen		
Show advanced options	Erweiterte Konfiguration aktivieren	Deaktiviert
Service Name	Hier kann ein Name für den Service vergeben werden	Leer
TX Queue Length	Länge der Übertragungswarteschlange festlegen	3
Enable IP head compression	Klicken, um die IP-Headerkomprimierung zu aktivieren	Leer
User Peer DNS	Peer-DNS für Benutzer aktivieren	Deaktiviert
Link Detection Interval	Intervall für Verbindungserkennung festlegen	55 Sekunden
Link Detection Max Retries	Höchstanzahl der Wiederholungen für Verbindungserkennung festlegen	10 (Mal)
Debug	Auswählen, um Debug-Modus zu aktivieren	Deaktiviert
Expert Options	Expertenparameter festlegen	Leer
ICMP Detection Server	Server für ICMP-Erkennung festlegen	Leer
ICMP Detection Intervall	Zeit für ICMP-Erkennung festlegen	30
ICMP Detection Timeout	Zeitüberschreitung für ICMP-Erkennung festlegen	3
ICMP Detection Retries	Höchstanzahl der Wiederholungen für ICMP-Erkennung festlegen	3

5.3 WAN(STA)

Unter diesem Menüpunkt *Network > WAN(STA)* können Sie den TK500 als WAN Station konfigurieren. Die Einstellungen in diesem Menüpunkt gleichen denen aus dem der WAN-Einstellungen.

System	Network	Services	Firewall	QoS	VPN	Tools	Status
							WAN(STA)
Type	<input type="text" value="Disabled"/>						
<input type="button" value="Apply"/>		<input type="button" value="Cancel"/>					

5.4 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. Dies geschieht obwohl die Teilnetze an gemeinsamen Switches angeschlossen sein können.

5.4.1 VLAN-Tabelle

In der VLAN-Tabelle können Sie die Zuweisung von VLANs zu FastEthernet Ports ändern und neue VLANs anlegen.

System	Network	Services	Firewall	QoS	VPN	Tools	Application
Your password have security risk, please click here to change!							
							VLAN
VLAN ID	LAN1	LAN2	LAN3	LAN4	Primary IP/Netmask		
1	✓	✓	✓	✓	192.168.2.1/255.255.255.0		
					<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>		

5.4.2 Port Mode

Im Menü Port Mode können den Netzwerports FastEthernet LAN1 bis LAN4 verschiedene VLAN IDs zugeordnet werden.

VLAN

Port Mode

MAC Address

Port	Enable	Speed Duplex	Mode	Native VLAN
LAN1	<input checked="" type="checkbox"/>	Auto Negotiation ▾	Access ▾	<input type="text" value="1"/>
LAN2	<input checked="" type="checkbox"/>	Auto Negotiation ▾	Access ▾	<input type="text" value="1"/>
LAN3	<input checked="" type="checkbox"/>	Auto Negotiation ▾	Access ▾	<input type="text" value="1"/>
LAN4	<input checked="" type="checkbox"/>	Auto Negotiation ▾	Access ▾	<input type="text" value="1"/>

NOTE:
Native VLAN is only valid in trunking mode

Es stehen die Optionen Acces und Trunk für die FastEthernet Ports zur Verfügung. Im Access Mode ist immer das VLAN1 ausgewählt. Im Trunk Mode können Sie den FastEthernet Ports VLAN-IDs zwischen 1-4000, die Sie zuvor erstellt haben, zuweisen.

5.5 Switch WLAN Mode

Einstellungen für den WLAN Typ können Sie an dieser Stelle machen. Dabei wird zwischen Access Point (AP) und Station (STA) unterschieden. Zu erreichen unter *Network > Switch WLAN Mode*.

System	Network	Services	Firewall	QoS	VPN	Tools	Status
Switch WLAN Mode							
WLAN Type		AP ▾ (*Reboot to take effect)					
<input type="button" value="Apply"/>		<input type="button" value="Cancel"/>					

Name	Beschreibung	Standard
AP	Access Point Modus	AP
STA	Client Modus	

Wird als *WLAN TYP STA* (für Station) gewählt, ändert sich das Menü unter Network. Es ist dann möglich unter 3.2.3 *WAN(STA)* zu konfigurieren und unter 3.2.6.a *WLAN Client* nur einen Client für ein existierendes WLAN einzurichten.

5.6 WLAN Client

Wurde bei der Konfiguration des *Switch WLAN Mode* (s. 3.2.6.) als WLAN Type der Punkt *STA* ausgewählt, ist keine Konfiguration eines WLAN mehr möglich. Sie können den TK 500 dann nur als WLAN Client konfigurieren. Das funktioniert dann unter *Network > WLAN Client*.

System	Network	Services	Firewall	QoS	VPN	Tools	Status
							WLAN Client
Enable		<input type="checkbox"/>					
		<input type="button" value="Apply"/> <input type="button" value="Cancel"/>					

Um den Router als WLAN Client zu konfigurieren, aktivieren Sie bitte Enable.

System	Network	Services	Firewall	QoS	VPN	Tools	Status
							WLAN Client
Enable		<input checked="" type="checkbox"/>					
Mode		802.11b/g/n ▾					
SSID		welotec					
Auth Mode		WPA2-PSK ▾					
Encryption Method		AES ▾					
WPA/WPA2 PSK		*****					
		<input type="button" value="Apply"/> <input type="button" value="Cancel"/>					

Tragen Sie nun die Daten ein, um den TK500 mit einem existierenden WLAN zu verbinden.

5.7 Link Backup

Mit dieser Option werden Verbindungen zwischen Funk-WAN und Ethernet-WAN gesichert. Fällt ein WAN aus, wird vom TK500 das jeweils andere automatisch verwendet. Sie können dies unter *Network > Link Backup* konfigurieren.

[Link Backup](#)

Enable
Backup Mode ▼
Main Link ▼
ICMP Detection Server
Backup Link ▼
ICMP Detection Interval Seconds
ICMP Detection Timeout Seconds
ICMP Detection Retries
Restart Interface When ICMP Failed

Name	Beschreibung	Standard
Enable	Den Service für Verbindungs-Backup aktivieren	Deaktiviert
Main Link	Auswahl von WAN, Dialup und WAN(STA) als Haupt-WAN möglich	WAN
ICMP Detection Server	ICMP kann eine Verbindung zu einem bestimmten Ziel sicherstellen	Leer
ICMP Detection Interval	Zeitintervall zwischen ICMP-Paketen	10
ICMP Detection Timeout	Zeitüberschreitung für die einzelnen ICMP-Pakete	3 (Sekunden)
ICMP Detection Retries	War keine Wiederholung der ICMP-Erkennung erfolgreich, wird die Backup-Verbindung angewählt	3
Backup Link	Backup-Verbindung auswählen	Dialup
Backup Mode	Hot Backup / Cold Backup	Hot Backup

5.8 VRRP

Das Virtual Router Redundancy Protocol (VRRP) ist ein Verfahren zur Steigerung der Verfügbarkeit wichtiger Gateways in lokalen Netzen durch redundante Router. Mehrere physische Router werden zu einer logischen Gruppe zusammengefasst. Diese Gruppe von Routern präsentiert sich im Netzwerk nun als ein logischer virtueller Router. Hierzu wird dem logischen Router eine virtuelle IP-Adresse und eine virtuelle MAC-Adresse zugeordnet. Einer der Router innerhalb der Gruppe wird als der virtuelle Master-Router definiert, dieser bindet daraufhin die virtuelle MAC- und die virtuelle IP-Adresse an sein Netzwerkinterface und informiert die anderen Router der Gruppe, die als virtuelle Backup-Router agieren. Diese Funktion können Sie unter **Services > VRRP** einrichten.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
VRRP								
Enable VRRP-I		<input checked="" type="checkbox"/>						
Group ID	1 ▾							
Priority	20 ▾ (254:highest)							
Advertisement Interval	60 ▾ Seconds							
Virtual IP	<input type="text"/>							
Authentication Type	None ▾							
Monitor	None ▾							
Enable VRRP-II		<input checked="" type="checkbox"/>						
Group ID	2 ▾							
Priority	10 ▾ (254:highest)							
Advertisement Interval	60 ▾ Seconds							
Virtual IP	<input type="text"/>							
Authentication Type	None ▾							
Monitor	None ▾							
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

Die TK500 Serie bietet die Möglichkeit zwei unterschiedliche VRRP (VRRP I und VRRP II) Gruppen zu bilden.

Name	Beschreibung	Standard
Enable VRRP-I	Zum Aktivieren von VRRP auswählen	Deaktiviert
Group ID	Gruppen-ID für Router auswählen (Bereich 1-255)	1
Priority	Priorität für Router auswählen (Bereich 1 - 254)	20 (je größer die Zahl, desto höher die Priorität)
Advertisement Interval	Anzeigenintervall festlegen	60 Sekunden
Virtual IP	Virtuelle IP für die Gruppe festlegen	Leer
Authentication Type	Optional: Typ „None/Password Authentication“	None. Wenn Password Authentication gewählt ist, kann ein Kennwort vergeben werden
Virtual MAC	Virtuelle MAC Adresse	Deaktiviert
Monitor	Überprüfen der WAN Verbindung	None
Enable VRRP-II	Zum Aktivieren von VRRP auswählen	Deaktiviert
Group ID	Gruppen-ID für Router auswählen (Bereich 1-255)	2
Priority	Priorität für Router auswählen (Bereich 1 - 254)	10 (je größer die Zahl, desto höher die Priorität)
Advertisement Interval	Anzeigenintervall festlegen	60 Sekunden
Virtual IP	Virtuelle IP für die 2. Gruppe festlegen	Leer
Authentication Type	Optional: Typ „None/Password Authentication“	None. Wenn Password Authentication gewählt ist, kann ein Kennwort vergeben werden
Virtual MAC	Virtuelle MAC Adresse	Deaktiviert
Monitor	Überprüfen der WAN Verbindung	None

5.9 IP Passthrough

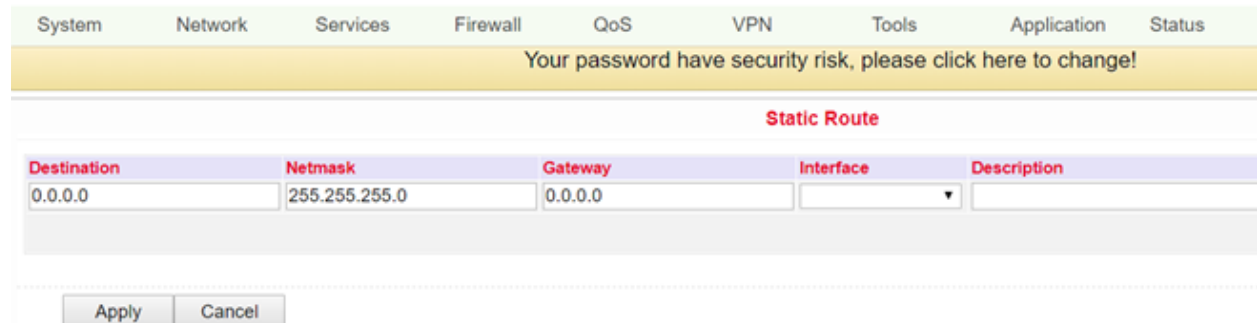
Hier können Sie die WAN IP an ein Gerät vergeben, das an einem LAN Port angeschlossen ist.

System	Network	Services	Firewall	QoS	VPN	Tools
Your password have security risk, please click here to change!						
IP Passthrough						
Enable IP Passthrough		<input checked="" type="checkbox"/>				
IP Passthrough Mode		DHCP Dynamic ▾				
DHCP Lease		2 Minutes				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>						

Nur ein Gerät kann diese IP-Adresse erhalten und auf das Internet zugreifen. Der LAN-Anschluss sollte vom Typ Static sein. Die Funktion funktioniert nicht mit einem Link Backup.

5.10 Static Route

Hier ist das Hinzufügen von statischen Routen möglich. Statische Routen liefern Ihrem Router zusätzliche Routinginformationen. Unter normalen Umständen verfügt der Router über ausreichende Informationen, wenn er für den Internetzugang konfiguriert wurde, und es müssen keine weiteren statischen Routen konfiguriert werden. Statische Routen müssen nur in Ausnahmefällen festgelegt werden, z. B. wenn Ihr Netzwerk mehrere Router oder IP-Subnetze enthält. Sie können statische Routen unter **Network > Static Route** hinzufügen, indem Sie den Add Button anklicken.



Name	Beschreibung	Standard
Destination	IP-Adresse des Ziels festlegen	Leer
Netmask	Subnetzmaske des Ziels festlegen	255.255.255.0
Gateway	Gateway des Ziels festlegen	Leer
Interface	Optionaler LAN/WAN-Portzugriff auf Ziel	Leer
Description	Frei wählbarer Name für die statische Route	Leer

5.11 OSPF

Open Shortest Path First bezeichnet ein von der IETF entwickeltes Link-State-Routing-Protokoll.

Es handelt sich um ein Protokoll für dynamisches Routing in IP-Netzen. Dynamisches Routing erkennt Veränderungen im Netzwerk selbständig, indem sich die Router untereinander austauschen. Die Routingtabellen passen sich dynamisch der jeweiligen Situation an.

Optimale Wege zu einem Ziel lassen sich auf Basis verschiedener Eigenschaften und Metriken wie die Anzahl der Hops, die Bandbreite, die Auslastung eines Links oder konfigurierte Kosten bestimmen. Ausfälle einzelner Verbindungen werden erkannt und binnen kurzer Zeit alternative Wege berechnet.

OSPF

Enable

Router ID

Route Advanced Options

ABR Type

RFC1583 Compatibility

OSPF Opaque-LSA

SPF Delay Time mseconds

SPF Initial-holdtime mseconds

SPF Max-holdtime mseconds

Reference Bandwidth

User Commands

Network

IP Address	Netmask	Area ID
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="Add"/>		

Interface

Interface	Network	Hello Interval	Dead Interval	Retransmit Interval	Transmit Delay
<input type="text" value=""/>	<input type="text" value="Broadcast"/>	<input type="text" value="10"/>	<input type="text" value="40"/>	<input type="text" value="5"/>	<input type="text" value="1"/>
<input type="button" value="Add"/>					

Interface Advanced Options

Interface	Passive Interface	Cost	Priority	Authentication	Key ID	Key	MTU Ignore
<input type="text" value=""/>	<input type="checkbox"/>	<input type="text" value="10"/>	<input type="text" value="10"/>	<input type="text" value=""/>	<input type="text" value="adm"/>	<input type="text" value="....."/>	<input type="checkbox"/>
<input type="button" value="Add"/>							

Area

Area ID	Area	No Summary	Authentication
<input type="text"/>	<input type="text" value=""/>	<input type="checkbox"/>	<input type="text" value=""/>
<input type="button" value="Add"/>			

Area Advanced Options

Area Range

Area ID	IP Address	Netmask	Not Advertisement	Cost
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>
				<input type="button" value="Add"/>

Area Virtual Link

Area ID	ABR Address	Authentication	Key ID	Key	Hello Interval	Dead Interval	Retransmit Interval	Transmit Delay
<input type="text"/>	<input type="text"/>	<input type="text" value="v"/>	<input type="text"/>	<input type="text"/>	10	40	5	1
								<input type="button" value="Add"/>

Redistribution

Redistribution Type	Metric	Metric Type
<input type="text" value="connected"/>	<input type="text"/>	<input type="text" value="v"/>
		<input type="button" value="Add"/>

Redistribution Advanced Option

Always Redistribute Default Route

Redistribute Default Route Metric

Redistribute Default Route Metric Type

Default Metric

Distance Management

Area Type	Distance
<input type="text" value="inter-area"/>	<input type="text"/>
<input type="button" value="Add"/>	

6 Services

Im Rahmen der Serviceeinstellungen konfigurieren Sie den DHCP-Dienst, die DNS-Weiterleitung, VRRP und andere zugehörige Parameter.

6.1 DHCP Service

Das Dynamic Host Configuration Protocol (DHCP) ist ein Kommunikationsprotokoll in der Netzwerktechnik. Es ermöglicht die Zuweisung der Netzwerkkonfiguration an Clients durch einen Server. So können Geräten im Netzwerk dynamisch IP-Adressen zugewiesen werden. Sie erreichen diesen Dienst unter *Services > DHCP Service*.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
DHCP Service								
Enable DHCP		<input checked="" type="checkbox"/>						
IP Pool Starting Address		<input type="text" value="192.168.2.2"/>						
IP Pool Ending Address		<input type="text" value="192.168.2.100"/>						
Lease		<input type="text" value="60"/> Minutes						
DNS		<input type="text" value="192.168.2.1"/>					Edit	
Windows Name Server (WINS)		<input type="text" value="0.0.0.0"/>						
Static DHCP								
MAC Address	IP Address	Host						
<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="192.168.2.2"/>	<input type="text"/>						
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

Name	Beschreibung	Standard
Enable DHCP	Klicken, um DHCP zu aktivieren	Aktiviert
IP Pool Starting Address	Start-IP-Adresse des DHCP-Pools festlegen	192.168.2.2
IP Pool Ending Address	End-IP-Adresse des DHCP-Pools festlegen	192.168.2.100
Lease	Gültige Lease-Time für die vom DHCP-Server erhaltene IP-Adresse festlegen	60 Minuten
DNS	DNS-Server festlegen (klick über Edit)	192.168.2.1
Windows Name Server	WINS festlegen	Leer
Static DHCP (es können höchstens 20 IP-Adressen festgelegt werden)		
MAC Address	MAC-Adresse einer vorgesehenen IP-Adresse festlegen	Leer
IP Address	Statische IP-Adresse festlegen	192.168.2.2
Host	Hostnamen festlegen	Leer

6.2 DNS

Hier können bis zu zwei DNS Server eingetragen werden, wenn der Router Teil eines Domänen-Netzwerks ist, das DNS zur Adressauflösung nutzt. Sie können die Daten unter **Network > DNS** eintragen.

System Network Services Firewall QoS VPN Tools Application Status

Your password have security risk, please click here to change!

DNS

Primary DNS

Secondary DNS

Apply Cancel

Name	Beschreibung	Standard
Primary DNS	Primären DNS festlegen	Leer
Secondary DNS	Sekundären-DNS festlegen	Leer

6.3 DNS Relay

Wenn DNS-Relay aktiviert ist (standardmäßig, wenn DHCP eingerichtet ist), wird den DHCP-Clients die IP-Adresse des Routers als DNS-Server zugeteilt. Alle DNS-Anfragen an den Router werden an die DNS-Server Ihres Internet-Diensteanbieters weitergeleitet. Wenn DNS-Relay deaktiviert ist, werden den DHCP-Clients vom Router die DNS-Server des Internet-Diensteanbieters zugewiesen. Sie können diese Einstellungen über **Services > DNS Relay** erreichen.

System Network Services Firewall QoS VPN Tools Application Status

Your password have security risk, please click here to change!

DNS Relay

Enable DNS Relay

Static [IP address <=> Domain Name] Pairing

IP Address	Host	Description
<input type="text"/>	<input type="text"/>	<input type="text"/>

Add

Apply Cancel

Mit dem **Add** Button können bis zu 20 DNS-Paare angelegt werden.

Name	Beschreibung	Standard
Enable DNS Relay	Klicken, um DNS-Weiterleitung zu aktivieren	Aktiviert (nach Aktivierung von DHCP)
Static (IP Address <-> Domain Name) Pairing (höchstens 20 DNS-Paare)		
IP Address	IP-Adresse <-> DNS-Paare festlegen	Leer
Host	Namen der IP-Adresse<->DNS-Paare festlegen	Leer
Description	IP-Adresse<->DNS-Paare beschreiben	Leer

6.4 DDNS (Dynamic DNS)

DDNS oder auch dynamisches DNS wird genutzt, wenn der WAN-Anschluss keine feste öffentliche IP-Adresse hat, aber dennoch von extern auf Dienste zugegriffen werden soll. Da sich bei einem normalen WAN-Anschluss die IP-Adresse des Providers immer wieder ändern kann, ist ein gesicherter Aufbau z.B. eines VPN-Tunnels nicht möglich. Daher nutzt man Anbieter von dynamischen DNS Servern, die dafür sorgen, dass Ihr WAN-Anschluss immer über die IP-Adresse bekommt. Die Konfiguration erreichen Sie über **Network > DDNS**.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
DDNS								
Dynamic DNS ==> WAN								
Current Address								
Service Type <input type="text" value="Disabled"/>								
Dynamic DNS ==> Dialup								
Current Address 37.80.83.157								
Service Type <input type="text" value="No-IP.com"/>								
URL <input type="text" value="http://www.no-ip.com/"/>								
Username <input type="text" value="gh-admin"/>								
Password <input type="password" value="....."/>								
Hostname <input type="text" value="welotec.ddns.net"/>								
Wildcard <input type="checkbox"/>								
MX <input type="text"/>								
Backup MX <input type="checkbox"/>								
Force Update <input type="checkbox"/>								
Last Update 2018-10-01 13:49:17								
Last Response 2018-10-01 13:49:17 Update successful.								
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

Name	Beschreibung	Standard
Current Address	Aktuelle IP-Adresse anzeigen	Leer
Service Type	DDNS-Anbieter auswählen	Deaktiviert

Es gibt diverse Einstellungsmöglichkeiten für diverse Anbieter von DDNS-Diensten. Diese wählt man über den

Service Type aus.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
DDNS								
Dynamic DNS ==> WAN								
Current Address								
Service Type								
<div style="border: 1px solid black; padding: 2px;"> Disabled Disabled Oray - Dynamic QDNS(3322) - Dynamic QDNS(3322) - Static DynDNS - Dynamic DynDNS - Static DynDNS - Custom No-IP.com Custom </div>								
Dynamic DNS ==> Dialup								
Current Address								
Service Type								
URL								
Username								
Password								
Hostname								
Wildcard								
MX								
Backup MX								
Force Update								

Als Beispiel für die Einrichtung dient hier No-IP. Hierfür benötigen Sie einen No-IP-Account, den Sie sich selbst anlegen müssen. Hier gibt es diverse Anbieter, die teilweise kostenlos, aber auch kostenpflichtig sind. Die Zuordnung des Dynamischen DNS kann sowohl dem WAN als auch dem Dialup-Anschluß zugeordnet werden.

Dynamic DNS ==> Dialup

Current Address	37.80.83.157
Service Type	No-IP.com
URL	http://www.no-ip.com/
Username	gh-admin
Password
Hostname	welotec.ddns.net
Wildcard	<input type="checkbox"/>
MX	
Backup MX	<input type="checkbox"/>
Force Update	<input type="checkbox"/>
Last Update	2018-10-01 13:49:17
Last Response	2018-10-01 13:49:17 Update successful.

Name	Beschreibung	Standard
Service Type	DynDNS - Dynamic	disabled
URL	http://www.dyndns.com/	gesetzt
Username	Registrierter Benutzername für	
DDNS	Leer	
Password	Registriertes Kennwort für DDNS	Leer
Hostname	Registrierter Hostname für DDNS	Leer
Wildcard	Kann aktiviert werden, wenn Wildcard genutzt werden soll	Deaktiviert
MX	Eintragen eines MX-Records	Leer
Backup MX	Kann aktiviert werden, wenn MX-Record als Backup laufen soll	Deaktiviert
Force Update	Erzwingt die Aktualisierung des Accounts	Deaktiviert
Last Update	Zeigt an, wann die IP-Adresse das letzte Mal geändert wurde	
Last Response	Zeigt an, wann das letzte Mal mit dem Service kommuniziert wurde	

6.5 DTU

DTU steht für Data Terminal Unit und dient dazu, Geräte mit serieller Schnittstelle (RS-232 und RS-485) anzubinden. Die Konfiguration können Sie unter **Services > DTU** erstellen. Wird DTU aktiviert, wird automatisch der Konsolen-Port deaktiviert.

System Network **Services** Firewall QoS VPN Tools Application Status

Your password have security risk, please click here to change!

DTU

Enable

DTU Protocol Transparent

Protocol UDP

Mode Client

Frame Interval 100 mseconds

Serial Buffer Frames 4

Multi-Server Policy Parallel

Min Reconnect Interval 15 Seconds

Max Reconnect Interval 180 Seconds

DTU ID

Source IP

DTU ID Report Interval 0 Seconds

Multi Server

Server Address	Server Port

Apply
Cancel

Name	Beschreibung	Standard
Enable	Klicken, um DTU zu aktivieren	Deaktiviert
DTU Protocol	DTU-Protokoll festlegen	Transparent
Protocol	Möglich sind die Optionen „TCP“ und „UDP“	UDP
Mode	DTU als Client oder Server festlegen, je nach Auswahl des DTU Protocol möglich	Client
Frame Interval	Festlegen des Frame Intervalls in Millisekunden	100 msec
Serial Buffer Frames	Vorgabe der Buffer Frames	4
Multi-Server Policy	Auswahl zwischen Parallel und Poll	Parallel
Min Reconnect Interval	Minimum Verbindungsintervall	15 Sec
Max Reconnect Interval	Maximales Verbindungsintervall	180 Sec
DTU ID	Vorgabe einer ID für das DTU	leer
Source IP	IP-Adresse des Quellrechners	leer
DTU ID Report Interval	Zeitintervall zum Senden der DTU ID	0
Source IP	IP-Adresse des Quellrechners	leer
DTU ID Report Interval	Zeitintervall zum Senden der DTU ID	0
Multi Server		
IP-Adresse	IP-Adresse für Empfang von Daten einrichten	Leer
Server Port	Serverport für Empfang von Daten einrichten	Leer

Je nach Auswahl des DTU-Protokolls können die Auswahlfelder variieren.

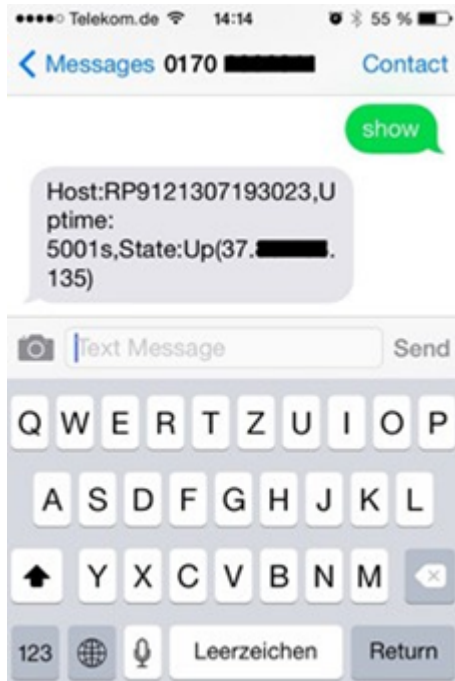
6.6 SMS

Der TK500 ist per SMS von außen erreichbar und reagiert auf verschiedene Befehle, die per SMS gesendet werden. Sie haben dabei die Möglichkeit, den Status des Gerätes abzufragen oder das Gerät neu zu starten. Konfiguriert wird der Router über **Services > SMS**.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
SMS								
Enable	<input checked="" type="checkbox"/>							
Status Query	<input type="text"/>	(English Only)						
Reboot	<input type="text"/>	(English Only)						
SMS Access Control								
Default Policy	Accept ▾							
Phone Number			Action			Description		
4917212345678			Accept ▾			1. SMS Empfänger		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

Name	Beschreibung	Standard
Enable	Klicken, um SMS-Kontrolle zu aktivieren oder zu deaktivieren	Deaktiviert
Status Query	Statusabfrage-SMS festlegen, um den Status des Routers per SMS anzuzeigen (z. B.: show status).	leer
Reboot	Lässt den Router neu starten (z.B. reboot)	leer
SMS Access Control		
Default Policy	Kontroll-SMS von bestimmten Telefon blockieren (Block) oder akzeptieren (Accept)	Accept
Phone Number	Eingabe der Telefonnummern zum Senden von SMS an Router. Das Format für die Mobilnummer lautet 491712345678 (bitte kein +49 oder 0049 eingeben)	leer
Action	Einstellung von Zulassen (Accept) oder Blockieren (Block) der zuvor eingegebenen Telefonnummer	Accept
Description	Beschreibung für den angelegten Datensatz	leer

Um eine SMS an den Router schicken zu können, muss die Mobilnummer der eingesetzten Karte bekannt sein. An diese wird dann die SMS versendet.



SMS, die Sie auf Ihrem Mobiltelefon erhalten:

Host: (SN);

Uptime: (die Betriebszeit des Routers zum Zeitpunkt dieses Neustarts);

State: (Online/Offline) (Funk-WAN-IP)

LAN: (Bereit) (LAN-IP)

6.7 Traffic Manager

Der Traffic Manager kann genutzt werden um den Datenverbrauch des Einwahl-Verbindungsinterfaces zur Verfügung zu stellen. Sie können diesen Dienst unter **Services > Traffic Manager** konfigurieren.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
Traffic Manager								
Enable		<input checked="" type="checkbox"/>						
Alarm Threshold		<input type="text" value="50000"/> MB/Month						
Disconnect Threshold		<input type="text" value="0"/> MB/Month						
<input type="button" value="Apply"/>		<input type="button" value="Cancel"/>						

Name	Beschreibung	Standard
Enable	Klicken, um SMS-Kontrolle zu aktivieren oder zu deaktivieren	Deaktiviert
Alarm Threshold	Legt die Datenmenge in MB pro Monat fest zu der ein Alarm generiert werden soll. Wird 0 als Wert gesetzt, wird kein Alarm generiert.	leer
Disconnect Threshold	Wird der eingestellte Wert erreicht, wird die Einwahlverbindung unterbrochen.	Leer

Die genutzte Datenmenge kann jederzeit unter der Traffic Statistic nachgesehen werden (s. 3.8.3)

6.8 Alarm Manager

Der Alarm Manager kann genutzt werden um verschiedene Alarme zu generieren. Sie können diesen Dienst unter *Services > Alarm Manager* konfigurieren.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
Alarm Manager								
Alarm Input								
System Service Fault		<input type="checkbox"/>						
Memory Low		<input type="checkbox"/>						
WAN Link-Up/Down		<input checked="" type="checkbox"/>						
LAN Link-Up/Down		<input type="checkbox"/>						
Dialup Up/Down		<input checked="" type="checkbox"/>						
Traffic Alarm		<input type="checkbox"/>						
Traffic Disconnect Alarm		<input type="checkbox"/>						
SIM/UM Card Fault		<input type="checkbox"/>						
Signal Quality Fault		<input type="checkbox"/>						
Alarm Output								
Console		<input checked="" type="checkbox"/>						
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

Name	Beschreibung	Standard
Alarm Input	Wählen Sie hier die Bereiche aus, für die ein Alarm generiert werden soll	keiner
Alarm Output	Hier können Sie wählen, ob die Alarme über die Konsole ausgegeben werden sollen oder nicht.	ausgewählt

7 Firewall

Über den Menüpunkt *Firewall* können Sie die Parameter für die Firewall des Routers festlegen. Hier sind verschiedene Einstellungen möglich.

7.1 Basic

Hier können die Basis-Einstellungen der Firewall konfiguriert werden.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
Basic								
Default Filter Policy		Accept ▾						
Block Anonymous WAN Requests (ping)		<input type="checkbox"/>						
Filter Multicast		<input checked="" type="checkbox"/>						
Defend DoS Attack		<input checked="" type="checkbox"/>						
Apply		Cancel						

Name	Beschreibung	Standard
Default Filter Policy	Möglich sind die Optionen „Accept“ und „Block“, also zulassen oder blockieren	Zulassen
Block Anonymous WAN Request (ping)	Aktivieren um Ping-Anforderungen, die Anonym aus dem Netz generiert werden, zu blocken	Deaktiviert
Filter Multicast	Klicken, um Filtern von Multicast zu aktivieren	Aktiviert
Defend DoS Attack	Klicken, um Abwehren von DoS-Angriffen zu aktivieren	Aktiviert

7.2 Filtering

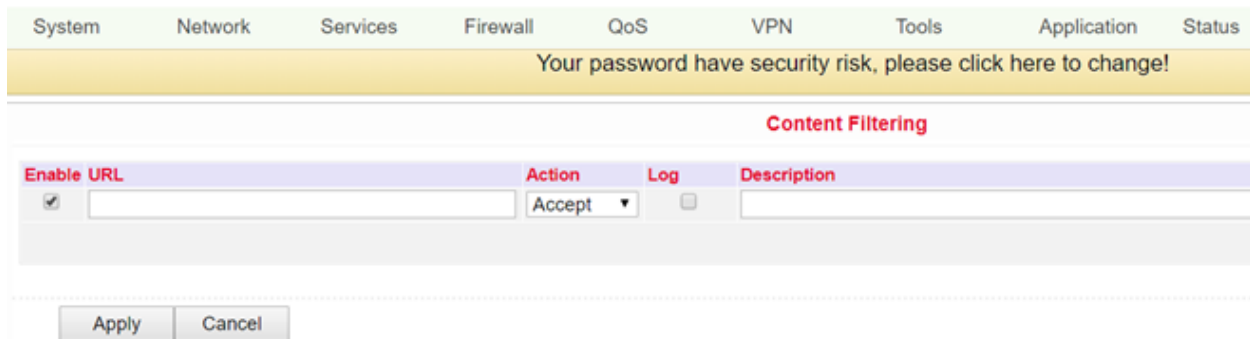
An dieser Stelle kann gefiltert werden, was die Firewall durchlassen soll und was nicht. Hier sind verschiedene Konfigurationen möglich, die Sie über *Firewall > Filtering* erreichen können.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
Filtering								
Enable	Proto	Source	Source Port	Destination	Destination Port	Action	Log	Description
Yes	TCP	0.0.0.0/0	7110-7113	192.168.2.12	7110	Accept	Yes	Test
<input checked="" type="checkbox"/>	ALL ▾	0.0.0.0/0				Accept ▾	<input type="checkbox"/>	
Apply		Cancel						

Name	Beschreibung	Standard
Enable	Klicken, um das Filtering zu aktivieren	Aktiviert
Proto	Auswahl des Protokolls. Möglich sind die Optionen „TCP“/„UDP“/„ICMP“	All
Source	Quell-IP-Adresse festlegen	Leer
Source Port	Quell-Port festlegen, wenn entsprechendes Protokoll gewählt wurde	Leer
Destination	Ziel-IP festlegen	Leer
Destination Port	Ziel-Port festlegen, wenn entsprechendes Protokoll gewählt wurde	Leer
Action	Auswahl, ob Einstellung erlaubt (Accept) oder geblockt (Block) werden soll	Erlaubt
Log	Klicken, um das Loggen der Einstellung zu aktivieren	Deaktiviert
Description	Konfiguration beschreiben	Leer

7.3 Content Filtering

Der Content Filter in der Firewall erlaubt es den Aufruf spezieller URL's zu filtern, die dann geblockt oder zugelassen werden können. Die Konfiguration können Sie unter **Firewall > Content Filtering** erstellen.



The screenshot shows the 'Content Filtering' configuration page. At the top, there is a navigation menu with tabs for System, Network, Services, Firewall, QoS, VPN, Tools, Application, and Status. Below the menu is a yellow warning banner: 'Your password have security risk, please click here to change!'. The main heading is 'Content Filtering'. Below this, there is a table with columns: 'Enable URL', 'Action', 'Log', and 'Description'. The 'Enable URL' column has a checked checkbox and an empty text input field. The 'Action' column has a dropdown menu set to 'Accept'. The 'Log' column has an unchecked checkbox. The 'Description' column has an empty text input field. At the bottom of the form, there are 'Apply' and 'Cancel' buttons.

Name	Beschreibung	Standard
Enable	Aktivieren oder deaktivieren der Content Filterfunktion	Aktiviert
URL	Eintragen der zu sperrenden bzw. filternden URL	Leer
Action	Auswahl ob URL geblockt (Block) oder erlaubt (Accept) wird	Erlaubt
Log	Kann zum Loggen aktiviert werden	Deaktiviert
Description	Konfiguration beschreiben	Leer

7.4 Port Mapping

NAT-PMP (NAT Port Mapping) ermöglicht es einem Computer, in einem privaten Netzwerk (hinter einem NAT-Router) den Router automatisch so zu konfigurieren, dass Geräte hinter dem Router von außerhalb des privaten Netzwerks erreichbar sind. Es regelt im Wesentlichen das sogenannte Port Forwarding. NAT-PMP, wie UPnP auch, ermöglicht es einem Programm, alle von außen ankommenden Daten auf einem bestimmten TCP- oder UDP-Port anzufordern. Die Konfiguration können Sie unter **Firewall > Port Mapping** durchführen.

System Network Services Firewall QoS VPN Tools Application Status

Your password have security risk, please click here to change!

Port Mapping

Enable	Proto	Source	Service Port	Internal Address	Internal Port	Log	External Address(Optional)/Tunnel Name(OpenVPN)	Description
<input checked="" type="checkbox"/>	TCP	0.0.0.0/0	8080	192.168.2.12	12080	<input type="checkbox"/>		Port an Client

Add

Apply Cancel

Name	Beschreibung	Standard
Enable	Portzuordnung aktivieren oder deaktivieren	Aktiviert
Proto	Auswahl der Protokolle TCP, UDP oder TCP&UDP	TCP
Source	Quell-IP eintragen	0.0.0.0/0
Service Port	Port des Dienstes eintragen	8080
Internal Address	Interne IP für Zuordnung festlegen	Leer
Internal Port	Portzuordnung auf „intern“ festlegen	8080
Log	Klicken, um Protokollierung der Portzuordnung zu aktivieren	Deaktiviert
External Address (Optional) / Tunnel Name (OpenVPN)	Wird in Verbindung mit VPN genutzt. Für die Portweiterleitung mit VPN muss hier die Virtuelle VPN IP Adresse des TK-Routers eingetragen werden.	Leer
Description	Bedeutung der einzelnen Zuordnungen beschreiben	Leer

7.5 Virtual IP Mapping

Die IP eines internen PCs kann einer virtuellen IP zugeordnet werden. Über diese virtuelle IP-Adresse kann ein externes Netzwerk auf den internen PC zugreifen. Sie können diese Konfiguration unter **Firewall > Virtual IP Mapping** einrichten.

System Network Services Firewall QoS VPN Tools Application Status

Your password have security risk, please click here to change!

Virtual IP Mapping

Virtual IP for Router

Source IP Range (Example: "1.1.1.1", "1.1.1.0/24", "1.1.1.1 - 2.2.2.2")

Enable Virtual IP	Real IP	Log	Description
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>

Add

Apply Cancel

Name	Beschreibung	Standard
Virtual IP for Router	Virtuelle IP für Router festlegen	Leer
Source IP Range	Bereich von Quell-IP-Adressen festlegen	Leer
Virtual IP	Virtuelle IP festlegen	Leer
Real IP	Reale IP festlegen	Leer
Log	Protokollierung für virtuelle IP aktivieren	Deaktiviert
Description	Konfiguration beschreiben	Leer

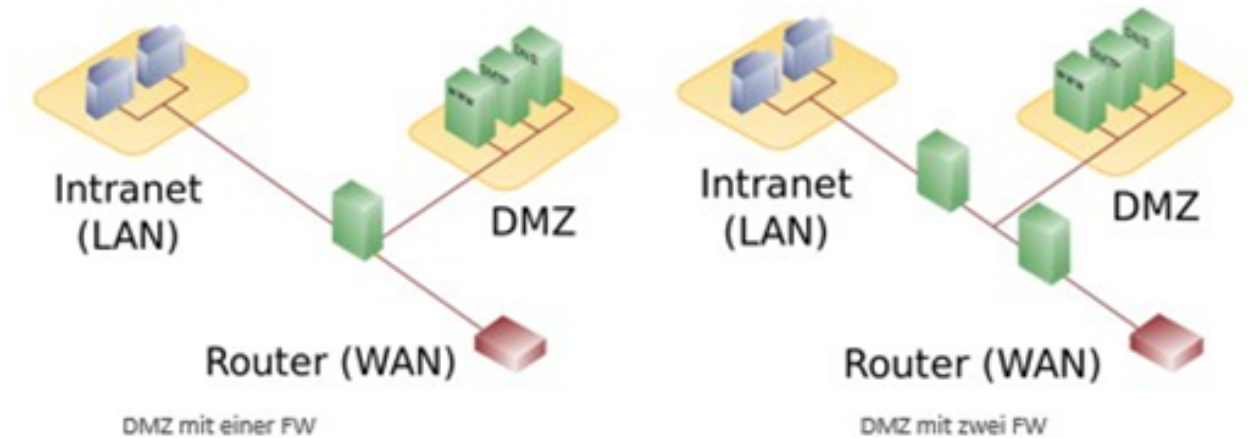
7.6 DMZ

Eine Demilitarized Zone (**DMZ**, auch *ent- oder demilitarisierte Zone*) bezeichnet ein Computernetzwerk mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf die daran angeschlossenen Server.

Die in der DMZ aufgestellten Systeme werden durch eine oder mehrere Firewalls gegen andere Netze (z.B. Internet, LAN) abgeschirmt. Durch diese Trennung kann der Zugriff auf öffentlich erreichbare Dienste gestattet und gleichzeitig das interne Netz (LAN) vor unberechtigten Zugriffen von außen geschützt werden.

Der Sinn besteht darin, auf möglichst sicherer Basis Dienste des Rechnernetzes sowohl dem Internet (WAN) als auch dem Intranet (LAN) zur Verfügung zu stellen.

Schutzwirkung entfaltet eine DMZ durch die Isolation eines Systems gegenüber zwei oder mehr Netzen.



System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
DMZ								
Enable DMZ		<input checked="" type="checkbox"/>						
DMZ Host		<input type="text"/>						
Source Address Range		<input type="text"/> (Optional Example: "1.1.1.1", "1.1.1.0/24", "1.1.1.1 - 2.2.2.2")						
Interface		<input type="text"/>						
Apply		Cancel						

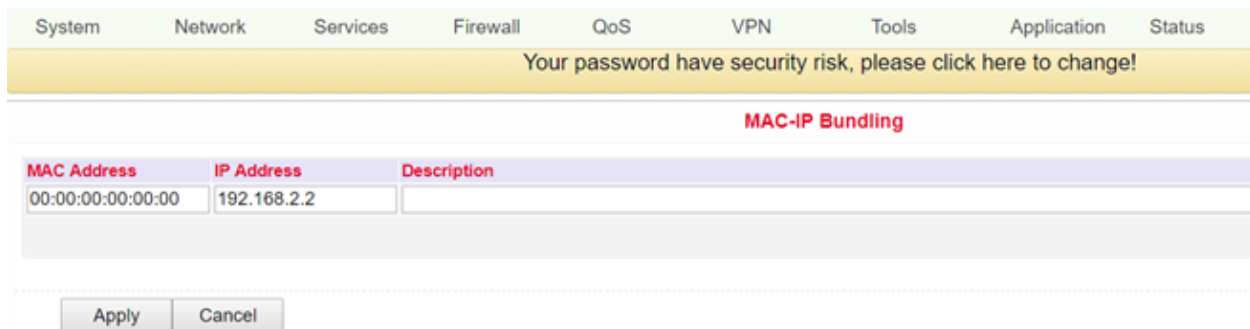
Durch die Zuordnung aller Ports und des externen PCs können Sie auf alle Ports des mit dem TK500 verbundenen Geräts zugreifen.

Mit dieser Funktion ist es nicht möglich, den Verwaltungspport des TK500 (z. B.: 80 TCP) dem Port des Geräts zuzuordnen. Um Port 80 weiterzuleiten, ändern Sie den Verwaltungspport des Routers unter **System > Admin Access**.

Name	Beschreibung	Standard
Enable DMZ	Klicken, um DMZ zu aktivieren	Deaktiviert
DMZ Host	DMZ-Host-IP festlegen	Leer
Source Address Range	IP-Adresse mit eingeschränktem IP-Zugriff festlegen	Leer
Interface	Auswahl des entsprechenden Interfaces	Leer

7.7 MAC-IP Bundling

MAC IP Bundling bedeutet, einer definierten MAC-Adresse eine vorgegebene IP-Adresse zuzuweisen. Somit bekommt die vorgegebene MAC-Adresse immer die gleiche IP-Adresse. Sie erreichen diesen Menüpunkt unter **Firewall > MAC-IP Bundling**.



Wird durch eine Firewall der gesamte Zugriff auf das externe Netzwerk blockiert, erhalten nur PCs mit MAC-IP Bundling Zugriff auf das externe Netzwerk.

Name	Beschreibung	Standard
MAC Address	MAC-Adresse für Bündelung festlegen	Leer
IP Address	IP-Adresse für Bündelung festlegen	192.168.2.2
Description	Konfiguration beschreiben	Leer

7.8 NAT

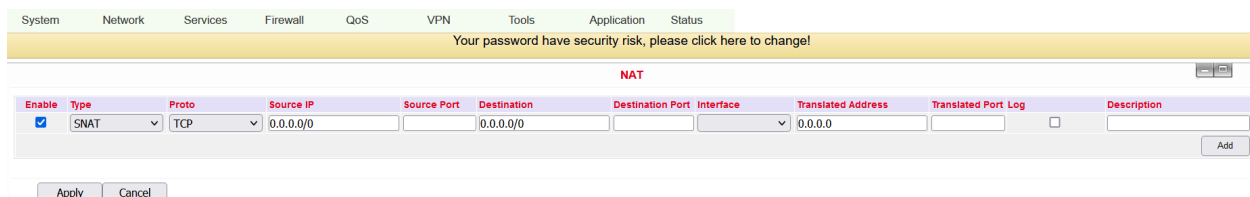
Network Address Translation (NAT) Network Address Translation ist in Rechnernetzen der Sammelbegriff für Verfahren, die automatisiert Adressinformationen in Datenpaketen durch andere ersetzen, um verschiedene Netze zu verbinden. Daher kommen sie typischerweise auf routern zum Einsatz.

7.8.1 Verwendung von Source-NAT (SNAT)

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 TK500v2 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.

7.8.2 Verwendung von Destination-NAT (DNAT)

Dies wird eingesetzt, um Servicedienste, die auf Computern betrieben werden, unter einer einzigen IP-Adresse anzubieten. Häufig wird es als Port-Mapping oder Port-Forwarding bezeichnet.



7.8.3 Konfiguration

- Zur Konfiguration von NAT geht man über den Menüpunkt *Firewall* in den unterpunkt *NAT*
- Hier findet sich eine Auflistung aller vorhandenen NAT-Regeln
- Über den *Add* Button können neue NAT-Regeln hinzugefügt werden

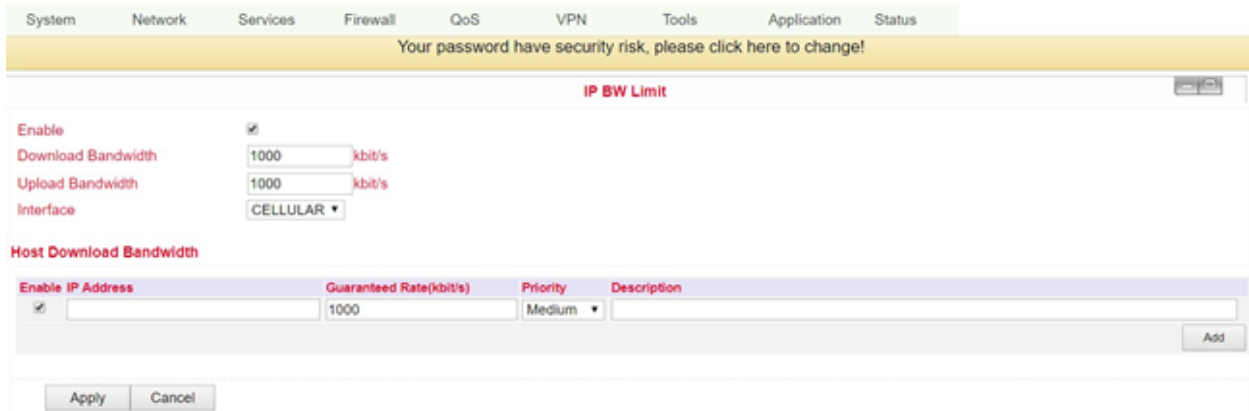
8 QoS

QoS beschreibt in der TCP/IP-Welt die Güte eines Kommunikationsdienstes aus Sicht des Anwenders. Dabei wird häufig die Netzwerk-Service-Qualität anhand der Parameter Bandbreite, Verzögerung, Paketverluste und Jitter definiert.

Die Netzbelastung beeinflusst dabei die Qualität der Übertragung. Wie lange dauert es z.B. bis ein Datenpaket beim Empfänger ankommt? Deshalb wird versucht Datenpakete mit entsprechenden Dienstklassen zu kennzeichnen. Priorisierte Datenpakete werden in Routern oder Switchen dann bevorzugt weitergeleitet. In der TK 500 Serie ist es daher möglich die Bandbreiten entsprechend zu begrenzen und zuzuordnen. Sie können dies über „QoS“ einrichten.

8.1 IP BW Limit

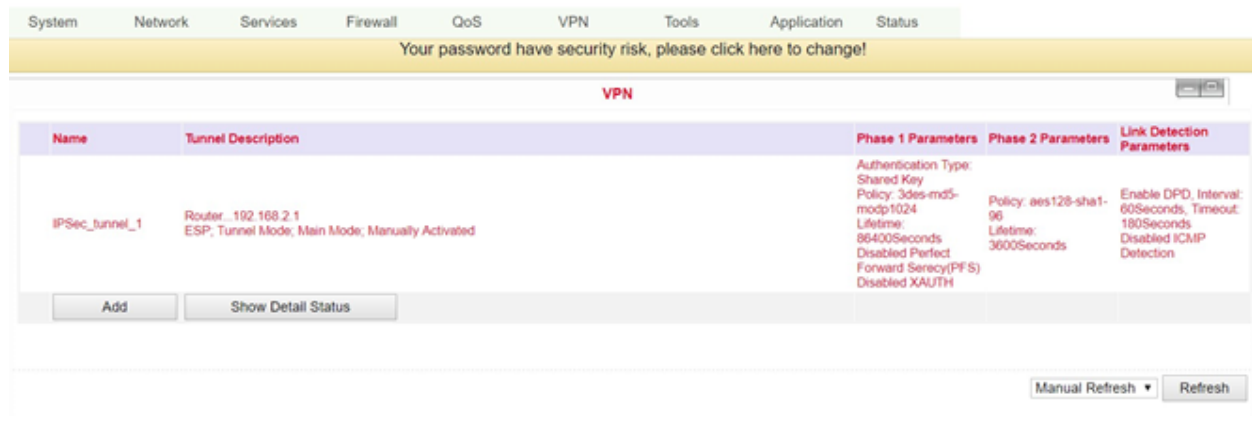
Unter dem Menüpunkt *QoS > IP BW Limit* können Sie die Down- bzw. Upload Bandbreite beschränken und an IP-Adressen binden, sowie diese dann priorisieren.



Name	Beschreibung	Standard
Enable	Zum Aktivieren klicken	Deaktiviert
Download Bandwith	Festlegen der Bandbreite für den Download	1000kbit/s
Upload Bandwith	Festlegen der Bandbreite für den Upload	1000kbit/s
Interface	Auswahl des Interfaces dem die Bandbreite zugeordnet werden soll	Cellular
Host Download Bandwidth		
Enable	Aktivieren der Funktion	Aktiviert
IP Adresse	Angabe der IP-Adresse für die Zuordnung	Leer
Guaranteed Rate (kbit/s)	Angabe der garantierten Bandbreite in kbit/s	1000
Priority	Zuweisung der Priorität	Medium
Description	Beschreibung der Regel	Leer

9 VPN

Bei einem VPN (Virtuelles privates Netzwerk) handelt es sich um ein geschlossenes logisches Netzwerk, bei dem die Teilnehmer räumlich voneinander getrennt, über einen IP-Tunnel verbunden sind. Mit diesem VPN kann man von unterwegs oder dem Home-Office auf ein lokales Netzwerk zugreifen, z.B. dem Firmennetzwerk. Dazu wird eine VPN-Software benötigt, die sowohl mit dem Router des Netzwerks kommuniziert als auch auf dem Computer installiert ist, mit dem Sie auf das Netzwerk zugreifen möchten. Es gibt verschiedene Arten von VPN-Verbindungen (Tunnel), die unter diesem Menüpunkt bei der TK 500 Serie konfiguriert werden können.

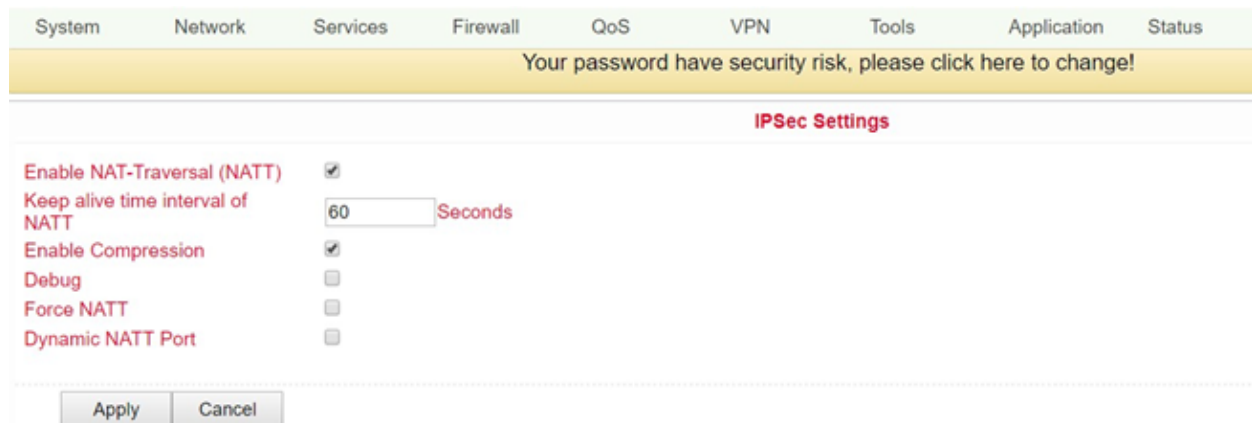


Name	Tunnel Description	Phase 1 Parameters	Phase 2 Parameters	Link Detection Parameters
IPSec_tunnel_1	Router_192.168.2.1 ESP, Tunnel Mode, Main Mode, Manually Activated	Authentication Type: Shared Key Policy: 3des-md5-modp1024 Lifetime: 86400Seconds Disabled Perfect Forward Secrecy(PFS) Disabled XAUTH	Policy: aes128-sha1-96 Lifetime: 3600Seconds	Enable DPD, Interval: 60Seconds, Timeout: 180Seconds Disabled ICMP Detection

Übersicht über die vorhandenen VPN-Verbindungen. Mit **Add** kann ein neuer Tunnel erstellt werden, siehe 3.6.2.

9.1 IPSec Settings

In diesem Menüpunkt konfigurieren Sie die Einstellungen für das IPSec. Zu erreichen über **VPN > IPSec Settings**.



Enable NAT-Traversal (NATT)
 Keep alive time interval of NATT: Seconds
 Enable Compression
 Debug
 Force NATT
 Dynamic NATT Port

Name	Beschreibung	Standard
Enable NAT-Traversal (NATT)	Zum Aktivieren klicken	Deaktiviert
Keep alive time interval of NATT	Festlegen der Dauer für die Aufrechterhaltung des NATT	60 Seconds
Enable Compression	Komprimierung ein- bzw. ausschalten	Aktiviert
Debug	Debugmodus ein- bzw. ausschalten	Deaktiviert
Enable	Aktivieren der Funktion	Aktiviert
Force NATT	NATT forcieren ein- bzw. ausschalten	Deaktiviert
Dynamic NATT Port	Ein- bzw. ausschalten eines dynamischen NATT Ports	Deaktiviert

Die Adressänderung über NAT wird von einem VPN-Gateway als sicherheitskritische Veränderung der Datenpakete gewertet, die VPN-Verhandlung scheitert, es kommt keine Verbindung zustande. Diese Probleme treten z.B. bei der Einwahl über manche UMTS-Mobilfunknetze auf, bei denen die Server des Netzbetreibers die Adress-Umsetzung in Verbindung mit IPSec-basierten VPNs nicht unterstützen.

Um in diesen Fällen eine VPN-Verbindung erfolgreich aufbauen zu können, steht mit NATT (NAT Traversal) ein Verfahren bereit, diese Probleme bei der Behandlung von Datenpaketen mit geänderten Adressen zu überwinden.

NATT kann nur bei VPN-Verbindungen eingesetzt werden, die zur Authentifizierung ESP (Encapsulating Security Payload) verwenden. ESP berücksichtigt im Gegensatz zu AH (Authentication Header) bei der Ermittlung des Hashwertes zur Authentifizierung nicht den IP-Header der Datenpakete. Der vom Empfänger berechnete Hashwert entspricht daher dem in den Paketen eingetragenen Hashwert

9.2 IPSec Tunnels

Über *VPN > IPSec Tunnels* können Sie einen entsprechenden Tunnel einrichten.

System	Network	Services	Firewall	QoS	VPN	Tools	Status
							IPSec Tunnels
Edit IPSec tunnel							
Show Advanced Options		<input checked="" type="checkbox"/>					
Basic Parameters							
Tunnel Name	<input type="text" value="IPSec_tunnel_1"/>						
Destination Address	<input type="text" value="0.0.0.0"/>						
Startup Modes	<input type="text" value="Auto Activated"/>						
Restart WAN when failed	<input checked="" type="checkbox"/>						
Negotiation Mode	<input type="text" value="Main Mode"/>						
IPSec Protocol	<input type="text" value="ESP"/>						
IPSec Mode	<input type="text" value="Tunnel Mode"/>						
VPN over IPSec	<input type="text" value="None"/>						
Tunnel Type	<input type="text" value="Subnet - Subnet"/>						
Local Subnet	<input type="text" value="192.168.2.1"/>						
Local Netmask	<input type="text" value="255.255.255.0"/>						
Remote Subnet	<input type="text" value="0.0.0.0"/>						
Remote Netmask	<input type="text" value="255.255.255.0"/>						

Phase 1 Parameters

IKE Policy: 3DES-MD5-DH2 ▾

IKE Lifetime: 86400 Seconds

Local ID Type: IP Address ▾

Remote ID Type: IP Address ▾

Authentication Type: Shared Key ▾

Key:

XAUTH Parameters

XAUTH Mode:

XAUTH Username:

XAUTH Password:

MODECFG:

Phase 2 Parameters

IPSec Policy: 3DES-MD5-96 ▾

IPSec Lifetime: 3600 Seconds

Perfect Forward Serecy(PFS): None ▾

Link Detection Parameters

DPD Time Interval: 60 Seconds(0: disable)

DPD Timeout: 180 Seconds

ICMP Detection Server:

ICMP Detection Local IP:

ICMP Detection Interval: 60 Seconds

ICMP Detection Timeout: 5 Seconds

ICMP Detection Retries: 10

Save Cancel

Auf dieser Seite werden die webbasierten Parameter für den TK500 vorgestellt.

Name	Beschreibung
Show Advanced Options	Klicken, um erweiterte Optionen zu aktivieren
Basic Parameters	
Tunnel Name	Name für den Tunnel
Destination Address	Zieladresse des IPSec-VPN-Servers festlegen
Startup Modes	Mögliche Modi sind „Auto Activate“ / „Triggered by Data“ / „Passive“ / „
Restart WAN when failed	WAN Interface wird bei fehlgeschlagenem Tunnelaufbau neu gestartet
Negotiation Mode	Optional: „Main Mode“ oder „Aggressive Mode“
IPSec Protocol	Optional: „ESP“ oder „AH“
IPSec Mode	Optional: „Tunnel Mode“ oder „Transport Mode“

Tab. 1 – Fortsetzung der vorherigen Seite

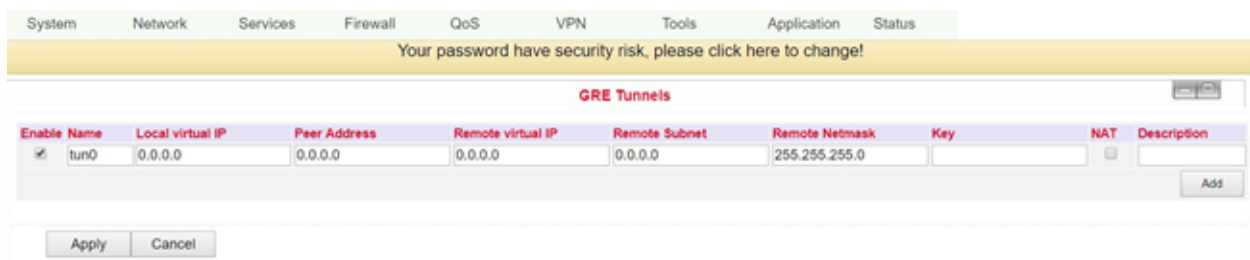
Name	Beschreibung
VPN over IPSec	L2TP oder GRE over IPSec
Tunnel Type	Auswahlfeld für div. Einstellungsmöglichkeiten
Local Subnet	Geschütztes IPSec-Subnetz festlegen (Lokal)
Local Netmask	Geschützte IPSec-Subnetzmaske festlegen (Lokal)
Remote Subnet	Geschütztes IPSec-Subnetz festlegen (Remote)
Remote Netmask	Geschützte IPSec-Subnetzmaske festlegen (Remote)
	Phase 1 Parameters
IKE Policy	MultiAuswahlliste für die Policy
IKKE Lifetime	IKE-Gültigkeitsdauer festlegen
Local ID Type	Auswahl von „FQDN“; „USERFQDN“ oder „IP-Adresse“ möglich
Remote ID Type	Auswahl von „IP-Adress“; „USERFQDN“; oder „FQDN“ möglich
Authentication Type	Auswahl von „Shared Key“ oder „Certificate“ möglich
Key (bei Auswahl des Authentifizierungstyps „Shared Key“)	IPSec-Schlüssel für VPN-Verhandlung festlegen
	XAUTH Parameters
XAUTH Mode	XAUTH Aktivieren
XAUTH Username	XAUTH Username
XAUTH Password	XAUTH Password
MODECFG	MODECFG aktivieren
	Phase 2 Parameters
IPSec Policy	Multi-Auswahlliste für die Policy
IPSec Lifetime	IPSec-Gültigkeitsdauer festlegen
Perfect Forward Secrecy (PFS)	Optional: „Disable“; „GROUP1“; „Group2“; „Group5“
	Link Detection Parameters
DPD Time Interval	DPD Zeitintervall festlegen
DPD Timeout	DPD Zeitüberschreitung festlegen
ICMP Detection Server	Server für ICMP-Erkennung festlegen
ICMP Detection Local IP	Lokale IP für ICMP-Erkennung festlegen
ICMP Detection Interval	Intervall für ICMP-Erkennung festlegen
ICMP Detection Timeout	Timeout für ICMP-Erkennung festlegen
ICMP Detection Max Retries	Höchstanzahl der Wiederholungen für ICMP-Erkennung festlegen

9.3 GRE Tunnels

Das Generic Routing Encapsulation (GRE) ist ein Netzwerkprotokoll, das von der Firma Cisco entwickelt wurde und im RFC 1701 definiert ist. Über GRE können andere Protokolle eingepackt und so in einem IP-Tunnel transportiert werden. GRE verwendet das IP Protokoll 47, der GRE-Header ist wie folgt aufgebaut:

C	R	K	S	s	Recur	Flags	Ver	Protocol Type
Checksum (optional)				Offset (optional)				
Key (optional)								
Sequence Number (optional)								
Routing (optional)								

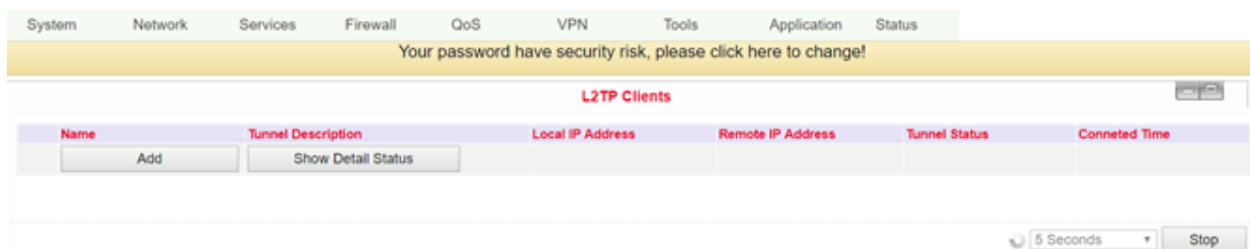
Ein GRE-Paket setzt sich also aus einem IP-Header, einem GRE-Header und der eigentlichen Nutzlast zusammen. Einrichten können Sie diesen GRE Tunnel unter **VPN > GRE Tunnels**.



Name	Beschreibung	Standard
Enable	Zum Aktivieren klicken	Aktiviert
Tunnel Name	Namen für GRE-Tunnel festlegen	tun0
Local Virtual IP	Lokale virtuelle IP festlegen	0.0.0.0
Peer Address	Peer-Adresse festlegen	0.0.0.0
Remote Virtual IP	Virtuelle-IP festlegen des Remote Netzwerks festlegen	0.0.0.0
Remote Subnet Address	Remote-Subnetzadresse festlegen	0.0.0.0
Remote Subnet Netmask	Remote-Subnetzmaske festlegen	255.255.255.0
Key	Schlüssel für die Verschlüsselung des Tunnels festlegen	Leer
NAT	Klicken, um NAT-Funktion zu aktivieren	Deaktiviert
Description	Beschreibung hinzufügen	Leer

9.4 L2TP Clients

Layer 2 Tunneling Protocol (L2TP) ist ein Netzwerkprotokoll, das Frames von Protokollen der Sicherungsschicht des OSI-Modells durch Router zwischen zwei Netzwerken über ein IP-Netz tunnelt. L2TP-Router sowie die IP-Verbindungen zwischen diesen erscheinen als L2-Switch. Der L2TP Client baut hier die Verbindung zum L2TP-Server auf. Sie erreichen die Konfiguration über **VPN > L2TP Clients**.



Durch klicken auf den **Add**-Button startet man die Konfiguration des L2TP Clients.

Your password have security risk, please click here to cha

L2TP Clients

Enable	<input checked="" type="checkbox"/>
Tunnel name	<input type="text" value="L2TP_tunnel_1"/>
L2TP Server	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
L2TP Server Name	<input type="text" value="l2tpserver"/>
Startup Modes	<input type="text" value="Auto Activated"/> ▾
Authentication Type	<input type="text" value="CHAP"/> ▾
Enable Challenge Secrets	<input type="checkbox"/>
Local IP Address	<input type="text"/>
Remote IP Address	<input type="text"/>
Remote Subnet	<input type="text"/>
Remote Netmask	<input type="text" value="255.255.255.0"/>
Multi Remote Subnet	<input type="checkbox"/>
Link Detection Interval	<input type="text" value="60"/> Seconds
Max Retries for Link Detection	<input type="text" value="5"/>
Enable NAT	<input type="checkbox"/>
MTU	<input type="text" value="1500"/>
MRU	<input type="text" value="1500"/>
Enable Debug	<input type="checkbox"/>
Expert Options(Expert Only)	<input type="text"/>

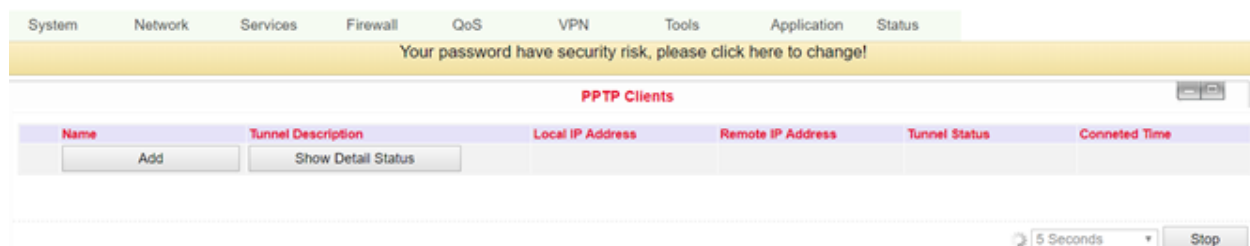
Save

Cancel

Name	Beschreibung	Standard
Enable	Aktiviert die Tunnel-Einstellungen	Aktiviert
Tunnel Name	Namen für Tunnel festlegen	L2TP_TUNNEL_1
L2TP Server	Adresse des L2TP-Server eintragen	leer
Username	Benutzername für Server festlegen	Leer
Password	Kennwort für Server festlegen	Leer
L2TP Server Name	Namen für Server festlegen	l2tpserver
Startup Modes	Modi für Start festlegen: „Auto Activated“, „Triggered by Data“, „Manually Activated“, „L2TPo- verIPSec“	Auto Activated
Authentication Type	Authentifizierungstyp festlegen: „CHAP“, „PAP“	CHAP
Enable Challenge Secrets	Zum Aktivieren von geheimen Schlüsseln (Challenge) auswählen	Deaktiviert
Challenge Secrets	Wenn Enable Challenge Secrets aktiviert ist, kann hier der geheime Schlüssel eingetragen werden	leer
Local IP Address	Lokale IP-Adresse festlegen	Leer
Remote IP Address	Remote-IP-Adresse festlegen	Leer
Remote Subnet	Remote-Subnetz festlegen	Leer
Remote Subnet Netmask	Remote-Subnetzmaske festlegen	255.255.255.0
Link Detection Interval	Intervall für Verbindungserkennung festlegen	60
Max Retries for Link Detection	Höchstanzahl der Wiederholungen für Verbindungserkennung festlegen	5
Enable NAT	Klicken, um NAT zu aktivieren	Deaktiviert
MTU	MTU-Parameter festlegen	1500
MRU	MRU-Parameter festlegen	1500
Enable Debug Mode	Klicken, um Debug-Modus zu aktivieren	Deaktiviert
Expert Options	Expertenoptionen festlegen	Leer

9.5 PPTP Clients

PPTP (Point to Point Tunneling Protocol) ist ein VPN-Tunneling-Verfahren für Remote-Access-Verbindungen. Es baut auf den Remote Access Server für Microsoft Windows NT inklusive der Authentisierung auf. Ein PPTP-Client ist nicht nur in Windows, sondern auch in Linux und MacOS integriert. Richten Sie unter **VPN > PPTP Clients** den PPTP Client ein.



Zur Einrichtung eines neuen PPTP Clients klicken Sie auf den Add Button. Um Details zu einem bereits bestehenden PPTP Client einzusehen, klicken Sie bitte auf den **Show Detail Status** Button. Wenn Sie auf den **Add** Button geklickt haben, können Sie folgende Konfigurationseinstellungen machen.

Edit PPTP Tunnel

Enable	<input checked="" type="checkbox"/>
Tunnel name	<input type="text" value="PPTP_tunnel_1"/>
PPTP Server	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Startup Modes	<input type="text" value="Auto Activated"/>
Authentication Type	<input type="text" value="Auto"/>
Local IP Address	<input type="text"/>
Remote IP Address	<input type="text"/>
Remote Subnet	<input type="text"/>
Remote Netmask	<input type="text" value="255.255.255.0"/>
Link Detection Interval	<input type="text" value="60"/> Seconds
Max Retries for Link Detection	<input type="text" value="5"/>
Enable NAT	<input type="checkbox"/>
Enable MPPE	<input type="checkbox"/>
Enable MPPC	<input type="checkbox"/>
MTU	<input type="text" value="1500"/>
MRU	<input type="text" value="1500"/>
Enable Debug	<input type="checkbox"/>
Expert Options(Expert Only)	<input type="text"/>

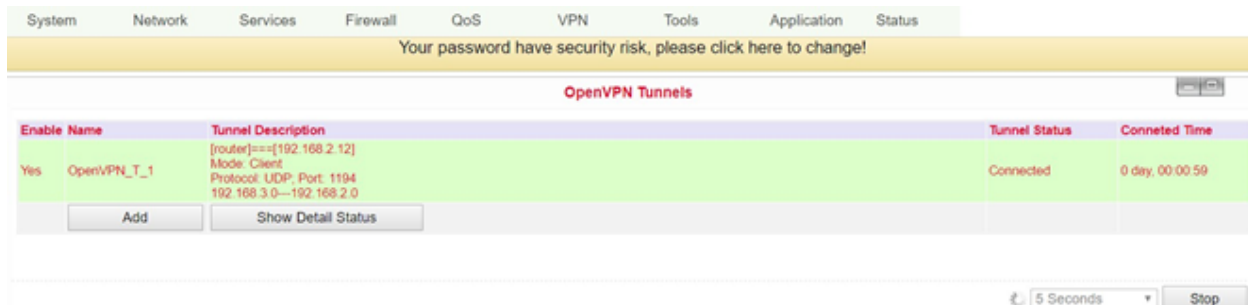
Name	Beschreibung	Standard
Enable	Zum Aktivieren klicken	Aktiviert
Tunnel Name	Der Name für den Tunnel (automatisch gesetzt)	PPTP_tunnel_1
PPTP Server	Adresse für PPTP-Server festlegen	Leer
Username	Benutzername für Server festlegen	Leer
Password	Kennwort für Server festlegen	Leer
Startup Mode:	Modi für Start festlegen „Auto Activated“, „Triggered by Data“, „Manually Activated“	Auto Activated
Authentication Type	Authentifizierungstyp festlegen: „PAP“, „CHAP“, „MS-CHAPv1“, „MS-CHAPv2“	Auto
Local IP Address	Lokale IP-Adresse festlegen	Leer
Remote IP Address	Remote-IP-Adresse festlegen	Leer
Remote Subnet	Remote-Subnetz festlegen	Leer
Remote Subnet Net-mask	Remote-Subnetzmaske festlegen	255.255.255.0
Link Detection Interval	Intervall für Verbindungserkennung festlegen	60
Max Retries for Link Detection	Höchstanzahl der Wiederholungen für Verbindungserkennung festlegen	5
Enable NAT	Klicken, um NAT zu aktivieren	Leer
Enable MPPE	Klicken, um MPPE (Microsoft Point to Point Encryption) zu aktivieren	Leer
Enable MPPC	Klicken, um MPPC (Microsoft Point to Point Compression) zu aktivieren	Leer
MTU	MTU-Parameter festlegen	1500
MRU	MRU-Parameter festlegen	1500
Enable Debug Mode	Klicken, um Debug-Modus zu aktivieren	Leer
Expert Options	Nur für Welotec R&D	Leer

9.6 OpenVPN Tunnels

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

OpenVPN steht unter der GNU GPL und unterstützt Betriebssysteme, wie z.B. Linux, Windows, iOS und eine Vielzahl von angepassten Linux-basierten Endgeräten, wie z.B. Router der Serien TK 500 und TK 800.

Wählen Sie auf der Konfigurationsseite des TK500 die Optionen **VPN > Open VPN Tunnels**, wie unten gezeigt:



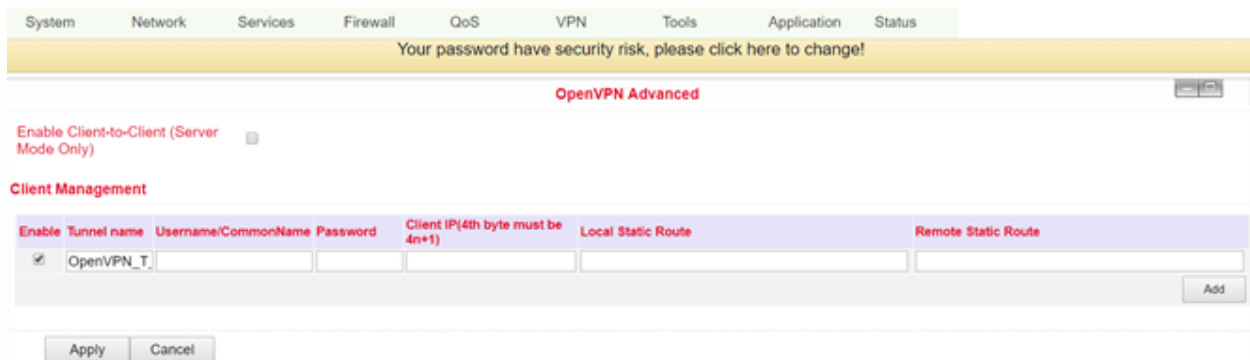
Klicken Sie auf **Add**, um einen neuen OpenVPN-Tunnel hinzuzufügen. Mit **Show Detail Status** können Sie sich den Status eines bereits konfigurierten OpenVPN Tunnels ansehen.

System	Network	Services	Firewall	QoS	VPN	Tools
Your password have security risk, please						
						OpenVPN Tunnels
Edit OPENVPN Tunnel						
Tunnel name	OpenVPN_T_1					
Enable	<input checked="" type="checkbox"/>					
Mode	Client ▾					
Protocol	UDP ▾					
Port	1194					
OPENVPN Server	192.168.2.12					
Authentication Type	X.509 Cert ▾					
Pre-shared Key	<input type="text"/>					
Local IP Address	192.168.3.0					
Remote IP Address	192.168.2.0					
Remote Subnet	<input type="text"/>					
Remote Netmask	255.255.255.0					
Link Detection Interval	60	Seconds				
Link Detection Timeout	300	Seconds				
Renegotiate Interval	86400	Seconds				
Enable NAT	<input checked="" type="checkbox"/>					
Enable LZO	<input type="checkbox"/>					
Encryption Algorithms	AES(256) ▾					
MTU	1500					
Max Fragment Size	<input type="text"/>					
Debug Level	Warn ▾					
Interface Type	TUN ▾					
Expert Options(Expert Only)	<input type="text"/>					
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Delete"/>						

Name	Beschreibung
Tunnel name	Vorgegeben
Enable	Diese Konfiguration aktivieren
Mode	„Client“ oder „Server“ Modus wählen
Protocol	Auswahl des Protokolls „UDP“ oder „TCP“
Port	Standard Port für OpenVPN ist 1194
OPENVPN Server	IP oder DNS des OpenVPN-Servers
Authentication Type	Auswahl des Authentifizierungstyps. Je nach Auswahl stehen unterschiedliche Felder zur Verfügung
Pre-shared Key	Bei Auswahl Pre shared Key, gemeinsamen Schlüssel oder TLS-AUTH statisches Kennwort festlegen
Remote Subnet, Remote Netmask	Statische Route des Routers festlegen, immer in Richtung Subnetz des Peers
Username/Password	Bei Auswahl User/Password werden in diesen Feldern die entsprechenden Daten eingegeben
Link Detection Interval, Link Detection Timeout	Immer Standard verwenden
Renegotiate Interval	Immer Standard verwenden
Enable NAT	NAT-Modus festlegen, zwischenzeitlich wird Routing-Modus deaktiviert
Enable LZO	LZO-Komprimierung aktivieren
Encryption Algorithms	Verschlüsselungs-Algorithmus festlegen, muss mit Server übereinstimmen
MTU	Immer Standard verwenden, 1500
Max Fragment Size	Maximale Größe einzelner Pakete
Debug Level	Auswahl der Debug Ausgaben im Log
Interface Type	TUN / TAP
Expert Options (Expert Only)	Weitere OpenVPN Befehle (nur für erfahrene Benutzer)

9.7 OpenVPN Advanced

Diese Konfigurationsseite wird nur für den OpenVPN-Server verwendet und stellt erweiterte Funktionen zur Verfügung. Sie können diesen Punkt erreichen über **VPN > OpenVPN Advanced**.

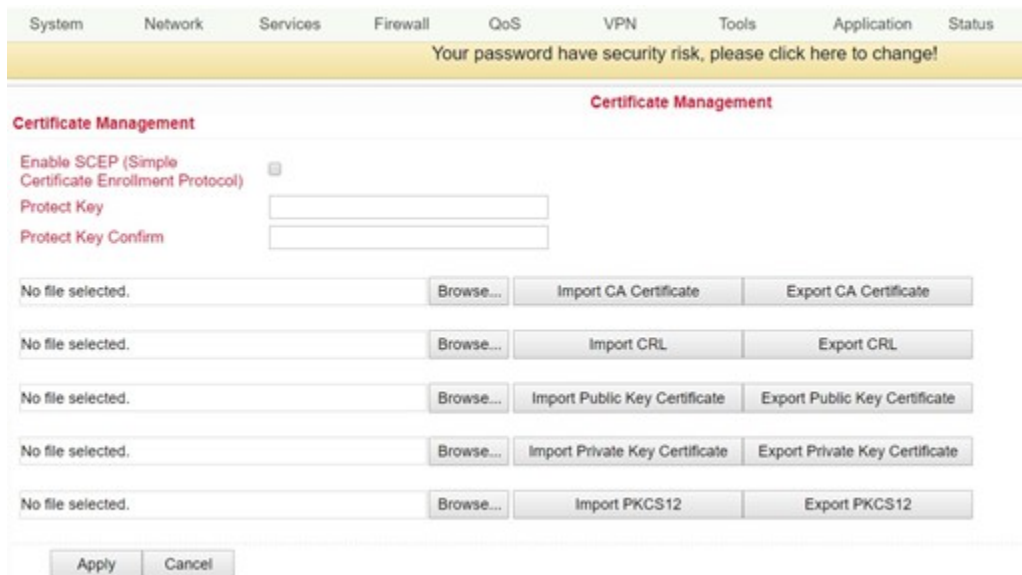


Name	Beschreibung
Enable Client-to-Client (Server Mode Only)	Clientzugriff auf andere Clients ermöglichen
Client Management	
Enable	Aktivieren der Funktion
Tunnel Name	Tunnelname des Clients
Username/Common Name	Benutzername (Verwendung des Modus „Username/Password“) oder allgemeiner Name in CA (CA-Modus)
Client IP	Angabe der Client IP-Adresse
Local Static Route	Subnetz des Clients
Remote Static Route	Subnetz des Servers

CA kann nur vom PC des Kunden erstellt werden, nicht vom TK500.

9.8 Certificate Management

Unter dem Menüpunkt *VPN > Certificate Management* können Sie die Zertifikate einbinden, die Sie für Ihre VPN-Verbindungen nutzen möchten. Ebenfalls können Sie bereits existierende Zertifikate exportieren.



Name	Beschreibung	Standard
Enable SCEP	Zum Aktivieren klicken	
Protect Key	Festlegen eines Schlüssels zum Schutz der Zertifikate	Leer
Protect Key Confirm	Bestätigen des Schlüssels zum Schutz der Zertifikaten	Leer
Import/Export CA Certificate	CA-Zertifikat importieren oder exportieren	Leer
Import/Export Certificate (CRL)	CRL Zertifikat importieren oder exportieren	Leer
Import/Export Public Key Certificate	Zertifikat für öffentlichen Schlüssel importieren/ exportieren	Leer
Import/Export Private Key Certificate	Zertifikat für privaten Schlüssel importieren oder exportieren	Leer
Import/Export PKCS12	PKCS12 (Privater Schlüssel und X.509 Zertifikat) importieren oder exportieren	Leer
Durchsuchen	Über Durchsuchen wird die jeweilige Datei ausgewählt und kann dann importiert werden	Keine Datei ausgewählt

10 Tools

Die Tools sind nützliche Werkzeuge und umfassen PING-Erkennung, Trace Route, Tests der Verbindungsgeschwindigkeit usw.

10.1 PING

Wählen Sie den Punkt *Tools > Ping* wenn Sie testen möchten, ob eine Verbindung ins Netzwerk/Internet besteht.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
PING								
Host	<input type="text" value="8.8.8.8"/>		<input type="button" value="Ping"/>					
Ping Count	<input type="text" value="4"/>							
Packet Size	<input type="text" value="32"/>	Bytes						
Expert Options	<input type="text"/>							
<pre> PING 8.8.8.8 (8.8.8.8): 32 data bytes 40 bytes from 8.8.8.8: icmp_seq=0 ttl=117 time=138.2 ms 40 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=26.0 ms 40 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=25.0 ms 40 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=24.2 ms --- 8.8.8.8 ping statistics --- 4 packets transmitted, 4 packets received, 0% packet loss round-trip min/avg/max = 24.2/53.3/138.2 ms </pre>								

Name	Beschreibung	Standard
Host	Ziel für PING	Leer
Ping Count	Anzahl der PINGs festlegen	4 Mal
Packet Size	Paketgröße für PING festlegen	32 Byte
Expert Options	Erweiterte Parameter	Leer

10.2 Traceroute

Traceroute (tracert) ermittelt, über welche Router und Internet-Knoten IP-Datenpakete bis zum abgefragten Rechner gelangen. Die Daten können Sie unter *Tools > Traceroute* eingeben.

System Network Services Firewall QoS VPN Tools Application Status

Your password have security risk, please click here to change!

Traceroute

Host:

Maximum Hops:

Timeout: Seconds

Protocol:

Expert Options:

```

1 * * *
2 * * *
3 * * *
4 * * *
5 * * *
6 * * *
7 * * *
8 80.156.5.17 (80.156.5.17) 27.680 ms 18.820 ms 21.380 ms
9 217.5.118.14 (217.5.118.14) 27.020 ms 27.240 ms 26.680 ms
10 87.128.238.134 (87.128.238.134) 25.740 ms 24.280 ms 26.660 ms
11 * * *
12 66.249.94.146 (66.249.94.146) 43.600 ms 216.239.56.150 (216.239.56.150) 26.720 ms 216.239.63.254 (216.239.63.254) 27.940 ms
13 209.85.240.177 (209.85.240.177) 25.120 ms 108.170.233.35 (108.170.233.35) 25.180 ms 216.239.48.79 (216.239.48.79) 27.200 ms
14 google-public-dns-a.google.com (8.8.8.8) 25.040 ms 26.000 ms 23.800 ms
  
```

Name	Beschreibung	Standard
Host	Ziel für Trace Route	Leer
Max Hops	Höchstanzahl der Hops festlegen	20
Time Out	Zeitüberschreitung festlegen	3 Sekunden
Protocol	Optional: „ICMP“/„UDP“	UDP
Expert Options	Erweiterte Parameter	Leer

10.3 Link Speed Test

Test der Verbindungsgeschwindigkeit über Upload oder Download. Diesen Bereich wählen Sie bitte über „Tools > Link Speed Test“.

System Network Services Firewall QoS VPN Tools Application Status

Your password have security risk, please click here to change!

Link Speed Test

No file selected.

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

10.4 TCPDUMP

Die Funktion TCPDUMP liest Daten in Form von Paketen, die über das Netzwerk gesendet werden, und stellt diese auf dem Bildschirm dar oder speichert sie in Dateien.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change								
TCPDUMP								
Interface		<input type="text" value="ANY"/>						
Capture Number		<input type="text" value="10"/> (10-1000)						
Expert Options		<input type="text"/>						
<input type="button" value="Start Capture"/>			<input type="button" value="Stop Capture"/>			<input type="button" value="Download Capture File"/>		

11 Application

Der Menüpunkt „*Application*“ wird momentan nicht supportet.

11.1 SMART-EMS

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change								
SMART-EMS								
Server URL	<input type="text"/>							
Username	<input type="text" value="adm"/>							
Password	<input type="password" value="....."/>							
Contact Interval	<input type="text"/>							Hours
Send running config	<input type="checkbox"/>							
Write startup	<input type="checkbox"/>							
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

12 Status

Unter „*Status*“ erhalten Sie Informationen zu System, Modem, Netzwerkverbindungen, Routingtabelle, Geräteliste und Protokoll.

12.1 System

Wählen Sie aus dem Menü *Status > System* um Informationen über Ihr System abzurufen.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
System								
Name	Router							
Serial Number	RL6151823435201							
Description	TK525L							
Current Version	2.3.0.r4648							
Current Bootloader Version	1.1.3.r4560							
Router Time	2018-10-01 16:21:57							
PC Time	2018-10-01 16:21:58 <input type="button" value="Sync Time"/>							
Up time	0 day, 02:31:53							
CPU Load (1 / 5 / 15 mins)	0.36 / 0.16 / 0.11							
Memory consumption Total/Free	27.73MB / 5,864.00KB (20.65%)							

Auf dieser Seite wird der Status des Systems angezeigt, u. a. Informationen zum Namen, Modelltyp, zur aktuellen Version usw.

12.2 Modem

Prüfen Sie den Status Ihres Modems unter *Status > Modem*.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
Modem								
Dialup								
Status	modem is ready							
Signal Level	📶 (22)							
RSSI	-69 dBm							
Register Status	registered							
IMEI(ESN) Code	867377025051750							
IMSI Code	262011406930165							
Network Type	4G							
PLMN	26201							
LAC	2EE2							
Cell ID	01E13103							

Hier können Sie den Status des Modems einschließlich der Signalstärke anzeigen.

12.3 Traffic Statistics

Wenn Sie den Datenverbrauch der SIM-Karte im TK500 ansehen möchten, dann können Sie dies unter **Status > Traffic Statistics**.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
Traffic Statistics								
Dialup								
Month Receive Traffic	1,743KB							
Month Transmit Traffic	3,547KB							
Day Receive Traffic	1,743KB							
Day Transmit Traffic	3,547KB							
Hour Receive Traffic	7991B							
Hour Transmit Traffic	7876B							
<input type="button" value="Clear"/>								

Hier sehen Sie die Daten, die Monatlich, täglich und Stündlich empfangen bzw. übermittelt wurden. Über den Button „Clear“ können Sie die Einträge auf 0 zurücksetzen.

12.4 Alarm

Überprüfen Sie die vom TK500 generierten Alarmer, die z.B. unter 3.3.7. im Alarm Manager angelegt wurden. Sie können diesen Menüpunkt unter **Status > Alarm** aufrufen.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
Alarm								
ID	Status	Level	Date			Content		
1	raise	INFO	Fri Sep 28 16:36:50 2018			Interface cellular,changed state to up		
2	raise	INFO	Thu Sep 27 16:53:14 2018			Interface cellular,changed state to up		
3	raise	INFO	Tue Aug 1 15:01:12 2017			Interface cellular,changed state to up		
4	raise	INFO	Thu Sep 20 15:47:27 2018			Interface cellular,changed state to down		
5	raise	INFO	Tue Sep 18 15:28:15 2018			Interface cellular,changed state to up		
6	raise	INFO	Thu Sep 20 14:57:49 2018			Interface cellular,changed state to down		
7	raise	INFO	Tue Sep 18 15:26:36 2018			Interface cellular,changed state to up		
8	raise	INFO	Tue Sep 18 15:29:40 2018			Interface cellular,changed state to up		
9	raise	INFO	Tue Sep 18 15:26:16 2018			Interface cellular,changed state to up		
10	raise	INFO	Tue Sep 18 16:01:10 2018			Interface cellular,changed state to down		
11	raise	INFO	Tue Aug 1 14:00:21 2017			Interface cellular,changed state to up		
<input type="button" value="Clear All Alarms"/> <input type="button" value="Confirm All Alarms"/>								

In diesem Beispiel wurde das monatliche Limit der SIM-Karte erreicht. Über den Button „Clear All Alarms“ können Sie alle Alarmmeldungen löschen und mit „Confirm All Alarms“ bestätigen Sie, dass Sie den Alarm zur Kenntnis genommen haben.

12.5 WLAN

Über **Status > WLAN** können Sie alle WLAN-Netze einsehen, die sich im Empfangsbereich des TK500 befinden. Dazu muss die Funktion WLAN im TK500 aktiviert sein (s. 3.2.6)

Channel	SSID	BSSID	Security	Signal(%)	Mode	Status
1	JD-PRO-Remote	0e:18:0a:9f:b0:47	WPA2PSK/AES	34	11b/g/n	
1	WeioLabor	00:18:0a:9f:b0:47	WPA2PSK/AES	39	11b/g/n	

3 Seconds

12.6 Network Connections

Über **Status > Network Connections** können Sie sich einen Überblick über die Netzwerk-Verbindungen des TK500 verschaffen.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
Network Connections								
WAN								
MAC Address	00:18:05:0C:C3:9B							
Connection Type	Dynamic Address (DHCP)							
IP Address	0.0.0.0							
Netmask	0.0.0.0							
Gateway	0.0.0.0							
DNS	0.0.0.0							
MTU	1500							
Status	Renewing...							
Connection time								
Remaining Lease	0 day, 00:00:00							
<input type="button" value="Renew"/> <input type="button" value="Release"/>								
Dialup								
Connection Type	Dialup							
IP Address	37.80.83.157							
Netmask	255.255.255.252							
Gateway	37.80.83.158							
DNS	10.74.210.210,10.74.210.211							
MTU	1500							
Status	Connected							
Connection time	0 day, 02:36:53							
<input type="button" value="Connect"/> <input type="button" value="Disconnect"/>								
LAN								
Connection Type	Static IP							
MAC Address	00:18:05:0C:C3:9C							
IP Address	192.168.2.1							
Netmask	255.255.255.0							
Gateway								
DNS								
MTU	1500							

Hier sehen Sie auf einen Blick die Netzwerkverbindungen über WAN, Dialup oder LAN.

12.7 Route Table

Wenn Sie einen Überblick über die Routingtabelle im TK500 haben möchten, wählen Sie aus dem Menü **Status > Route Table**.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
Route Table								
Destination	Netmask	Gateway	Metric	Interface				
192.168.2.0	255.255.255.255	0.0.0.0	0	tun0				
37.80.83.156	255.255.255.252	0.0.0.0	0	cellular				
192.168.2.0	255.255.255.0	0.0.0.0	0	lan0				
127.0.0.0	255.0.0.0	0.0.0.0	0	lo				
default	0.0.0.0	37.80.83.158	0	cellular				

Nach Aufruf sehen Sie die Routingtabelle des TK500.

12.8 Device List

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
Device List								
Interface	MAC Address	IP Address	Host					
usb0	4C:54:99:45:E5:D5	37.80.83.158						
lan0	00:0E:C6:CD:23:FE	192.168.2.12						

Unter dem Menüpunkt **Status > Device List** werden Ihnen alle Geräte angezeigt, die mit dem TK500 verbunden sind. Überblick über die mit dem TK500 verbundenen Geräte.

12.9 Log

Dokumentation der System-Ereignisse (Logs) des TK500. Diesen Bereich erreichen Sie unter **Status > Log**.

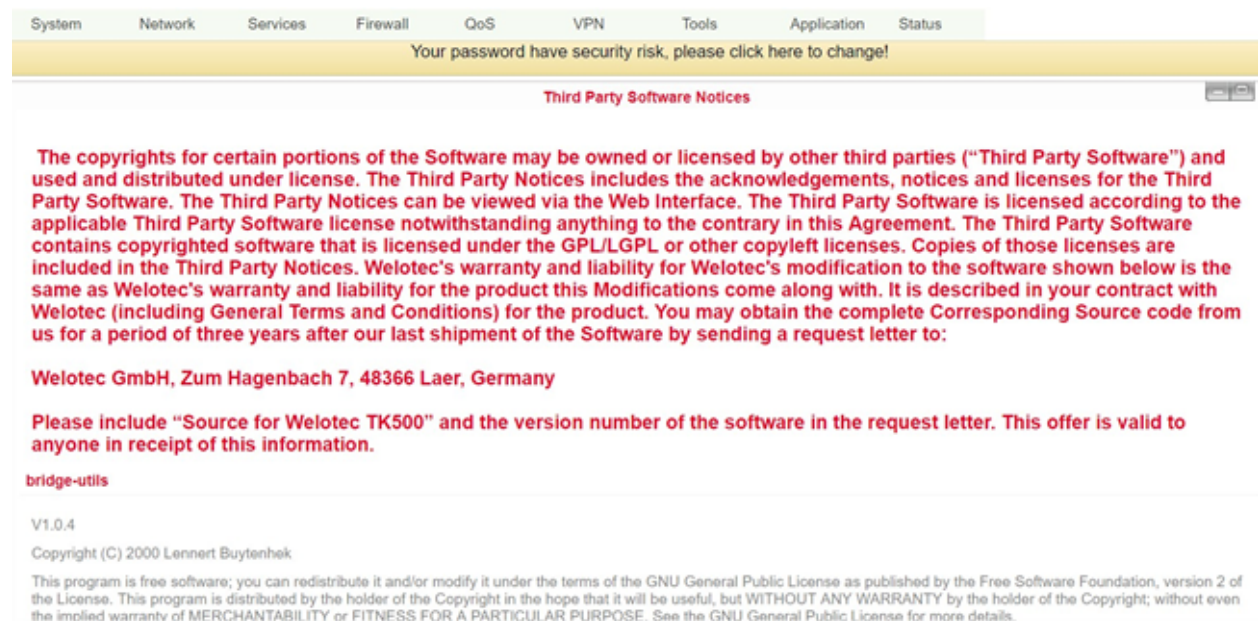
System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
Log								
								when local/remote addresses exist within the same /24 subnet as --ifconfig endpoints. (silence this warning with --ifconfig-nowarn)
notice	Oct 1 16:29:12	opemvpn[4015]	TUN/TAP device tun0 opened					
notice	Oct 1 16:29:12	opemvpn[4015]	TUN/TAP TX queue length set to 100					
notice	Oct 1 16:29:12	opemvpn[4015]	do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0					
notice	Oct 1 16:29:12	opemvpn[4015]	/sbin/ifconfig tun0 192.168.3.0 pointopoint 192.168.2.0 mtu 1500					
notice	Oct 1 16:29:12	opemvpn[4015]	/tmp/OpenVPN_T_1.up tun0 1500 1557 192.168.3.0 192.168.2.0 init					
info	Oct 1 16:29:12	opemvpn-up[29129]	tunnel(OpenVPN_T_1),tun0 up: 192.168.3.0 <=> 192.168.2.0, tun mtu:1500, link mtu:1557					
debug	Oct 1 16:29:12	opemvpn-up[29129]	add ACL rule: enabled to accept & log, [proto: 1, 0.0.0.0/0 port 7110:7113 => 192.168.2.12 port 7110], Test					
debug	Oct 1 16:29:12	opemvpn-up[29129]	applying MAC-IP rules					
info	Oct 1 16:29:12	opemvpn-up[29129]	stop_qoslimit.old interface name not get					
info	Oct 1 16:29:12	opemvpn-up[29129]	rateimit_enable is 0					
info	Oct 1 16:29:12	opemvpn-up[29129]	firewall ACL does not exist for domain rules.					
info	Oct 1 16:29:12	opemvpn-up[29129]	Clear connection table in opemvpn up...					
notice	Oct 1 16:29:12	opemvpn[4015]	UDPv4 link local: [undef]					
notice	Oct 1 16:29:12	opemvpn[4015]	UDPv4 link remote: [AF_INET]192.168.2.12:1194					
info	Oct 1 16:29:12	udhcp[460]	Sending discover...					
info	Oct 1 16:29:15	udhcp[460]	Sending discover...					
<input type="button" value="Clear Log"/> <input type="button" value="Download Log File"/> <input type="button" value="Download System Diagnosing Data"/>								

Auf dieser Seite wird das Systemprotokoll angezeigt, das hier heruntergeladen werden kann.

Es kann vorkommen, dass Probleme nicht sofort diagnostiziert und behoben werden können. In diesen Fällen bitten wir Sie, das Diagnoseprotokoll an Welotec zu senden. Klicken Sie dazu auf „[Download System Diagnosing Data](#)“, und schicken Sie uns das Protokoll mit einer Fehlerbeschreibung dann an support@welotec.com

12.10 Third Party Software

Hier sind die Softwarebestimmungen und Lizenzen von allen Drittanbietern aufgeführt, die im Zusammenhang mit der Routerreihe TK500 stehen.



The screenshot shows a web interface with a navigation menu at the top: System, Network, Services, Firewall, QoS, VPN, Tools, Application, Status. Below the menu is a yellow warning bar: "Your password have security risk. please click here to change!". The main content area is titled "Third Party Software Notices" and contains the following text:

The copyrights for certain portions of the Software may be owned or licensed by other third parties ("Third Party Software") and used and distributed under license. The Third Party Notices includes the acknowledgements, notices and licenses for the Third Party Software. The Third Party Notices can be viewed via the Web Interface. The Third Party Software is licensed according to the applicable Third Party Software license notwithstanding anything to the contrary in this Agreement. The Third Party Software contains copyrighted software that is licensed under the GPL/LGPL or other copyleft licenses. Copies of those licenses are included in the Third Party Notices. Welotec's warranty and liability for Welotec's modification to the software shown below is the same as Welotec's warranty and liability for the product this Modifications come along with. It is described in your contract with Welotec (including General Terms and Conditions) for the product. You may obtain the complete Corresponding Source code from us for a period of three years after our last shipment of the Software by sending a request letter to:

Welotec GmbH, Zum Hagenbach 7, 48366 Laer, Germany

Please include "Source for Welotec TK500" and the version number of the software in the request letter. This offer is valid to anyone in receipt of this information.

bridge-utils

V1.0.4
Copyright (C) 2000 Lennert Buytenhek

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, version 2 of the License. This program is distributed by the holder of the Copyright in the hope that it will be useful, but WITHOUT ANY WARRANTY by the holder of the Copyright; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

13 Technische Daten

13.1 Geräteeigenschaften

Eigenschaft	Wert
Abmessungen (B x H x T)	35 x 127 x 108,2 mm
Betriebsspannung	230 V AC auf 12 V – 24 V DC
Zulassung	CE-konform

13.2 Umgebungsbedingungen

Eigenschaft	Wert
Einsatztemperaturbereich	-15 bis +70 °C
Luftfeuchtigkeit	5 - 95 %, nicht kondensierend
Erschütterungen	IEC 60068-2-27
Freier Fall	IEC 60068-2-32
Vibration	IEC 60068-2-6

13.3 Funkfrequenzen

13.3.1 Funkfrequenzen LTE Europa

Frequenz	Frequenzbereich und Sendeleistung	Router
Band 1	Frequenzbereich Down: 2110 MHz – 2170 MHz Frequenzbereich Up: 1920 MHz – 1980 MHz Max. Sendeleistung: 200 mW	TK525U, TK525L, TK525L W, TK525W
Band 3	Frequenzbereich Down: 1805 MHz – 1880 MHz Frequenzbereich Up: 1710 MHz – 1785 MHz Max. Sendeleistung: 200 mW	TK525U, TK525L, TK525L-W, TK525W
Band 7	Frequenzbereich Down: 2620 MHz – 2690 MHz Frequenzbereich Up: 2500 MHz – 2570 MHz Max. Sendeleistung: 200 mW	TK525U, TK525L, TK525L-W, TK525W
Band 8	Frequenzbereich Down: 925 MHz – 960 MHz Frequenzbereich Up: 880 MHz – 915 MHz Max. Sendeleistung: 200 mW	TK525U, TK525L, TK525L-W, TK525W
Band 20	Frequenzbereich Down: 791 MHz – 821 MHz Frequenzbereich Up: 832 MHz – 862 MHz Max. Sendeleistung: 200 mW	TK525U, TK525L, TK525L W, TK525W
Band 28	Frequenzbereich Down: 703 MHz – 748 MHz Frequenzbereich Up: 758 MHz – 803 MHz Max. Sendeleistung: 200 mW	TK525U, TK525L, TK525L-W, TK525W

13.3.2 Funkfrequenzen UMTS Europa

Freque	Frequenzbereich und Sendeleistung	Router
Band 1	Frequenzbereich Down: 2110 MHz – 2170 MHz Frequenzbereich Up: 1920 MHz – 1980 MHz Max. Sendeleistung: 251 mW	TK525U, TK525L, TK525L-W, TK525W
Band 8	Frequenzbereich Down: 925 MHz – 960 MHz Frequenzbereich Up: 880 MHz – 915 MHz Max. Sendeleistung: 251 mW	TK525U, TK525L, TK525L-W, TK525W

13.3.3 Funkfrequenzen GSM Europa

Frequer	Frequenzbereich und Sendeleistung	Router
GSM 900	Frequenzbereich Down: 925 MHz – 960 MHz Frequenzbereich Up: 880 MHz – 915 MHz Max. Sendeleistung: 1995 mW	TK525U, TK525L, TK525L-W, TK525W
GSM 1800	Frequenzbereich Down: 1805 MHz – 1880 MHz Frequenzbereich Up: 1710 MHz – 1785 MHz Max. Sendeleistung: 40 mW	TK525U, TK525L, TK525L-W, TK525W

13.3.4 Funkfrequenzen LTE Asien

Frequenz	Frequenzbereich und Sendeleistung	Router
Band 1	Frequenzbereich Down: 1920 MHz – 1980 MHz Frequenzbereich Up: 2110 MHz – 2170 MHz Max. Sendeleistung: 200 mW	TK525U, TK525L, TK525L-W, TK525W
Band 3	Frequenzbereich Down: 1805 MHz – 1880 MHz Frequenzbereich Up: 1710 MHz – 1785 MHz Max. Sendeleistung: 200 mW	TK525U, TK525L, TK525L-W, TK525W
Band 7	Frequenzbereich Down: 2620 MHz – 2690 MHz Frequenzbereich Up: 2500 MHz – 2570 MHz Max. Sendeleistung: 200 mW	TK525U, TK525L, TK525L-W, TK525W
Band 38 China	Frequenzbereich Down: 2570 MHz – 2620 MHz Frequenzbereich Up: n.b. Max. Sendeleistung: 200 mW	TK525U, TK525L, TK525L-W, TK525W
Band 40 China	Frequenzbereich Down: 2300 MHz – 2400 MHz Frequenzbereich Up: n.b. Max. Sendeleistung: 200 mW	TK525U, TK525L, TK525L-W, TK525W
Band 41 China	Frequenzbereich Down: 2496 MHz – 2690 MHz Frequenzbereich Up: n.b. Max. Sendeleistung: 200 mW	TK525U, TK525L, TK525L-W, TK525W

13.4 Funkfrequenzen UMTS Asien

Freque	Frequenzbereich und Sendeleistung	Router
Band 1	Frequenzbereich Down: 2110 MHz – 2170 MHz Frequenzbereich Up: 1920 MHz – 1980 MHz Max. Sendeleistung: 251 mW	TK525U, TK525L, TK525L-W, TK525W
Band 8	Frequenzbereich Down: 925 MHz – 960 MHz Frequenzbereich Up: 880 MHz – 915 MHz Max. Sendeleistung: 251 mW	TK525U, TK525L, TK525L-W, TK525W

13.4.1 Funkfrequenzen GSM Asien

Frequeer	Frequenzbereich und Sendeleistung	Router
GSM 900	Frequenzbereich Down: 925 MHz – 960 MHz Frequenzbereich Up: 880 MHz – 915 MHz Max. Sendeleistung: 1995 mW	TK525U, TK525L, TK525L-W, TK525W
GSM 1800	Frequenzbereich Down: 1805 MHz – 1880 MHz Frequenzbereich Up: 1710 MHz – 1785 MHz Max. Sendeleistung: 1000 mW	TK525U, TK525L, TK525L-W, TK525W

13.4.2 Funkfrequenzen UMTS Global

Frequeer	Frequenzbereich und Sendeleistung	Router
Band 1	Frequenzbereich Down: 2110 MHz – 2170 MHz Frequenzbereich Up: 1920 MHz – 1980 MHz Max. Sendeleistung: 251 mW	TK525U, TK525L, TK525L-W, TK525W
Band 8	Frequenzbereich Down: 925 MHz – 960 MHz Frequenzbereich Up: 880 MHz – 915 MHz Max. Sendeleistung: 251 mW	TK525U, TK525L, TK525L-W, TK525W

13.4.3 Funkfrequenzen GSM Global

Frequeer	Frequenzbereich und Sendeleistung	Router
GSM 850	Frequenzbereich Down: 869 MHz – 894 MHz Frequenzbereich Up: 824 MHz – 849 MHz Max. Sendeleistung: 1995 mW	TK525U, TK525L, TK525L-W, TK525W
GSM 1900	Frequenzbereich Down: 1930 MHz – 1990 MHz Frequenzbereich Up: 1850 MHz – 1910 MHz Max. Sendeleistung: 1000 mW	TK525U, TK525L, TK525L-W, TK525W

13.4.4 Funkfrequenzen WLAN

Frequenz	Frequenzbereich und Sendeleistung	Router
2,4 GHz	Frequenzbereich: 2400 MHz – 2483,5 MHz Max. Sendeleistung: 40 mW	TK525L-W

14 Support

Senden Sie bei Problemen mit der Installation und dem Betrieb eine E-Mail an folgende Adresse:
support@welotec.com