

TK500v2 Router Series

Version:
v1.0.42

Date:
16.12.2024



Contents

1	Introduction	3
1.1	Copyright Notice	3
1.2	Trademark	3
1.3	Legal Notice	3
1.4	Contact information for technical support	3
1.5	Description	3
1.6	Important safety note:	4
1.7	Content checklist	4
1.8	Product information	5
2	Regulatory Compliances	7
2.1	CE and UKCA Notice	7
3	Installation guide	8
3.1	Typical use	8
3.2	Wiring diagram	8
3.3	Fast internet connection	9
3.4	Reset to factory settings	16
4	System	18
4.1	Preparation	18
4.2	Basic Setup	20
4.3	Time	21
4.4	Serial Port	22
4.5	Admin Access	22
4.6	System Log	24
4.7	Config Management	25
4.8	Scheduler	26
4.9	Upgrade	26
4.10	Reboot	27
4.11	Logout	28
5	Network	29
5.1	Cellular	29
5.2	WAN	31
5.3	WAN(STA)	35
5.4	VLAN	36
5.5	Switch WLAN Mode	37
5.6	WLAN Client	38
5.7	Link Backup	38
5.8	VRRP	39
5.9	IP Passthrough	41
5.10	Static Route	41
5.11	OSPF	42
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	51
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	74
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	Technical specifications	82
13.1	Device properties	82
13.2	Environmental conditions	82
13.3	Radio frequencies	82
13.4	Radio frequencies UMTS Asia	83
14	Support	85

1 Introduction

1.1 Copyright Notice

Copyright © 2018 Welotec GmbH All rights reserved.

Duplication without authorization is not permitted.

1.2 Trademark

Welotec is a registered trademark of Welotec GmbH. Other trademarks mentioned in this manual are the property of their companies.

1.3 Legal Notice

The information in this document is subject to change without notice and is not a commitment by Welotec GmbH.

It is possible that this user manual contains technical or typographical errors. Corrections are made regularly without being pointed out in new versions.

1.4 Contact information for technical support

Welotec GmbH Zum Hagenbach 7

48366 Laer

Tel.: +49 2554 9130 00

Fax.: +49 2554 9130 10

Email: support@welotec.com

1.5 Description

The TK500 series of routers for industrial applications provides a stable high-speed connection between remote devices and customer sites over LAN and (depending on model) WLAN or 2G/3G/4G networks. They can operate over a voltage range of 12 to 24 V DC and have a temperature range from -15°C to 70°C at a relative humidity of 95 %, ensuring high stability and reliability under severe conditions. The TK500 can be used at a workstation or mounted on a DIN rail.

TK500 series products support VPN (IPSec/PPTP/ L2TP/GRE/SSL VPN), which ensures secure connections between remote devices and customer locations.

1.6 Important safety note:

1.6.1 This product is not suitable for the following applications

- Areas where radio applications (such as cell phones) are not allowed
- Hospitals and other places where the use of cell phones is not permitted
- Gas stations, fuel depots and places where chemicals are stored
- Chemical plants or other places where there is a risk of explosion Metal surfaces that can weaken the radio signal level

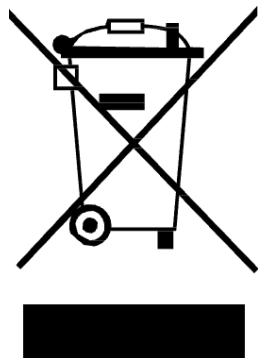
1.6.2 Warning

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

1.6.3 WEEE Notice

The European Directive on Waste Electrical and Electronic Equipment (WEEE), which became effective on February 13, 2003, has led to major changes regarding the reuse and recycling of electrical equipment.

The main objective of this directive is to prevent waste from electrical and electronic equipment and to promote reuse, recycling and other forms of recovery. The WEEE logo on the product or packaging indicates that the product must not be disposed of with other household waste. You are responsible for disposing of all discarded electrical and electronic equipment at appropriate collection points. Separate collection and sensible recycling of your electronic waste helps to use natural resources more sparingly. In addition, proper recycling of waste electrical and electronic equipment ensures human health and environmental protection.



For more information on disposal, recycling, and collection points for waste electrical and electronic equipment, contact your local municipal authority, waste disposal companies, the distributor, or the manufacturer of the equipment.

1.7 Content checklist

Each TK500 wireless router is delivered in a package with standard accessories. Additional accessories can be ordered. Check the contents of your package carefully and if anything is missing or damaged, contact your sales partner from Welotec GmbH.

1.7.1 Scope of delivery

Standard accessories

Accessory	Quantity	Description
TK500 router	1	TK500 series industrial router
Network cable	1	Network cable CAT5, 1.5 meters
Manual	1	Data medium with manual
Licensing conditions	1	"Third Party Software Notifications and Licenses"
Power supply		
Terminal block	1	7-pole terminal block for power supply

Components set (depending on model)

Product	Quantity	Description
TK500 router	1	TK500 series industrial router
Network cable	1	Network cable CAT5, 1.5 meters
Mobile antenna	1	5 m magnetic base antenna (TK515L, TK515L-W, TK505U) 2G/3G/4G
WLAN antenna	2	Plug-on antennas (WLAN) (TK515L-W)
Manual	1	Data medium with manual
Licensing conditions	1	"Third Party Software Notification and Licenses"
Power supply		
		Table power supply, input 100-240 V AC, output 12 V DC (for TK5xx), incl. 7-pin terminal block
	1	Plug, European standard

1.8 Product information

1.8.1 Environmental conditions

Operating temperature: -15 to 70°C

Relative humidity during operation: 5 to 95 % non-condensing

Storage temperature: -40 to +85°C

1.8.2 Power supply

Power supply: 1 terminal strip (7-pin) incl. voltage socket and serial connection

Input voltage: 12 - 24 V DC

1.8.3 Physical properties

Housing: steel, protection class IP30

Weight: 450 g

Dimensions (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 Installation guide

3.1 Typical use

With routers of the TK500 series you can connect devices with Ethernet, WLAN or RS-232/485 via GPRS/HSUPA/UMTS/LTE to the Internet. To ensure security and uninterrupted access, the TK500 series supports VPN connections, enabling remote access and secure data transmission over the Internet.

3.2 Wiring diagram

Interface	Description
Power connection	12-24 V DC
Serial	RS 232, RS 485
Ethernet ports	Five 10/100Base-TX RJ45-Ports
Antenna connection (mobile radio)	SMA (f)
Antenna connection (WLAN)	SMA-R (f)
SIM card slot	Slot for inserting the SIM card (TK525L-W, TK525L, TK525U)

3.2.1 Connection of the serial interfaces and I/O's

Description of LED lights:

 = LED on
  = LED off
  = LED flashing

Signal	On	Off	Flashing
Power on	PWR, STATUS, WARN	ERR	
Firmware execution	PWR, WARN	ERR	STATUS
Dial-up to the Internet	PWR	ERR	STATUS, WARN
Establishing a connection	PWR	WARN, ERR	STATUS
Update firmware	PWR		STATUS, WARN, ERR
Reset to factory settings	PWR	WARN	STATUS, ERR

Description of the LED signals



Signal: 1-9

(Poor signal, the router can not work correctly, please check the antenna connection and the local signal strength of the mobile network.)



Signal: 10-19

(Router operates normally)



Signal: 20-31

(Perfect signal level)

3.3 Fast internet connection

3.3.1 Inserting the SIM card

Open the TK router SIM/UiM compartment at the top of the device and insert the SIM card into the card holder.

3.3.2 Antenna installation

After installing the TK500, connect the antenna and screw the antenna tight. Place the antenna where a good signal strength is achieved.



Note

Position and angle can affect signal strength.

3.3.3 Power supply

Connect the power supply included in the scope of delivery to the device and check whether the LED display for “Power” lights up. Contact Welotec technical support if no indicator lights up. You can configure the TK500 when the power indicator is flashing.

3.3.4 Connecting

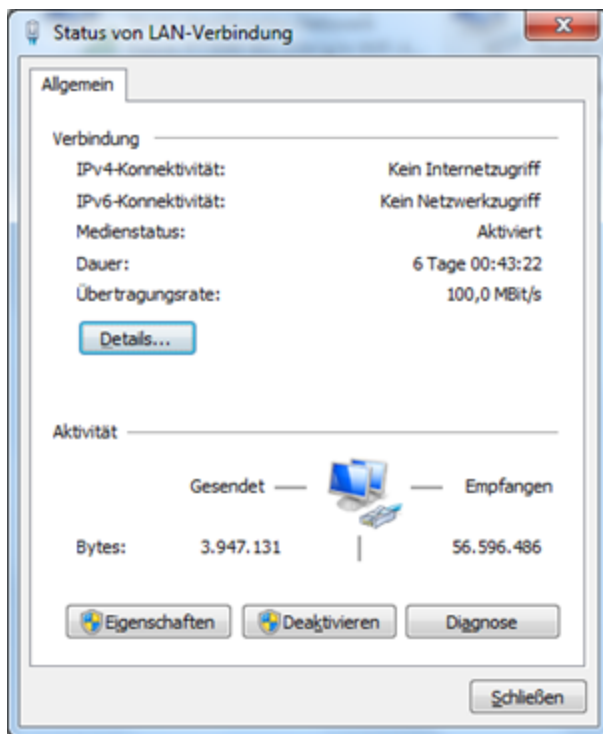
Connect the TK500 to the PC:

1. Connect the Ethernet cable of the TK500 to the PC.
2. Then one LED indicator of the RJ45 interface lights up green and the other indicators flash.

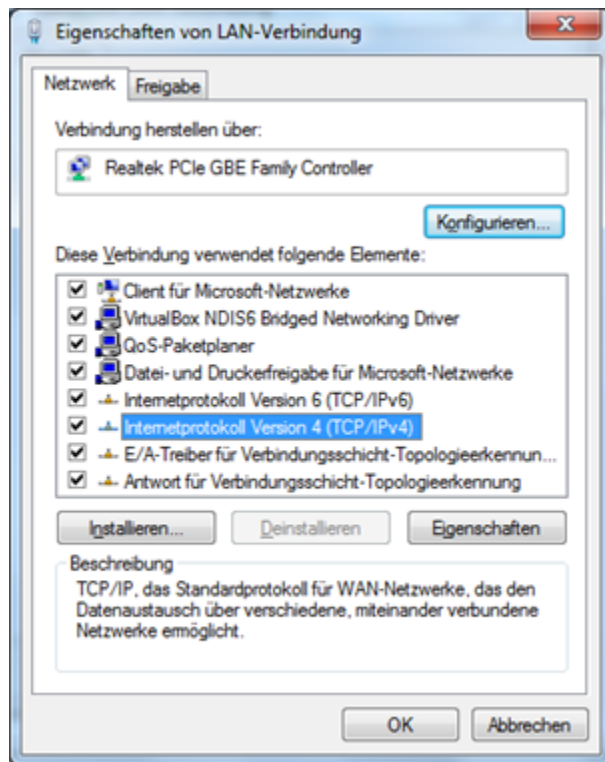
3.3.5 Connecting the TK router device to the PC for the first time

The TK500 router can assign IP addresses for the PC automatically. Set up the PC so that IP addresses are retrieved automatically via DHCP. (Basis is the Windows operating system):

1. Open the Control Panel, double-click the “*Network and Sharing Center*” icon to open the “*Network and Sharing Center*” screen.
2. Click “*LAN Connection*” and open the screen with the “*Status of LAN Connection*”:

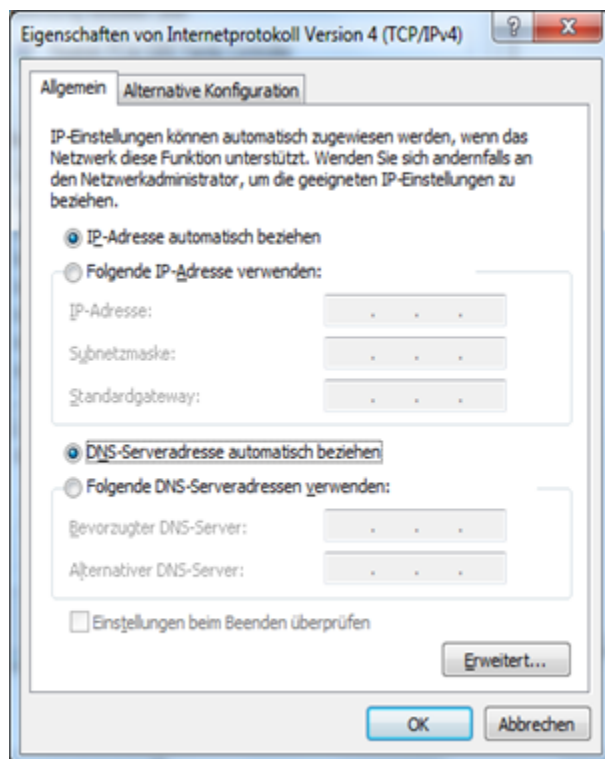


3. Click “*Properties*” and open the LAN connection properties screen:



4. Select "**Internet Protocol Version 4 (TCP/IPv4)**", click the "**Properties**" button, and check if your PC can obtain IP and DNS address automatically. (You can also set up the PC in the subnet: 192.168.2.0/24, e.g. IP: 192.168.2.10, netmask: 255.255.255.0 Default gateway: 192.168.2.1)

By clicking "**OK**", the TK router assigns an IP address to the PC: 192.168.2.X, as well as the gateway: 192.168.2.1 (the default address of the TK500).



After configuring the TCP/IP protocols, you can use the ping command to check whether the connection between

the PC and the router is established without errors. The following is an example of running the ping command under Windows 7:

Windows key+R -> Enter “cmd” -> press Enter -> Enter “*Ping 192.168.2.1*” -> press Enter With this display:

```
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\>_
```

The connection between the PC and the router has been established correctly.

The following example contains errors:

```
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),

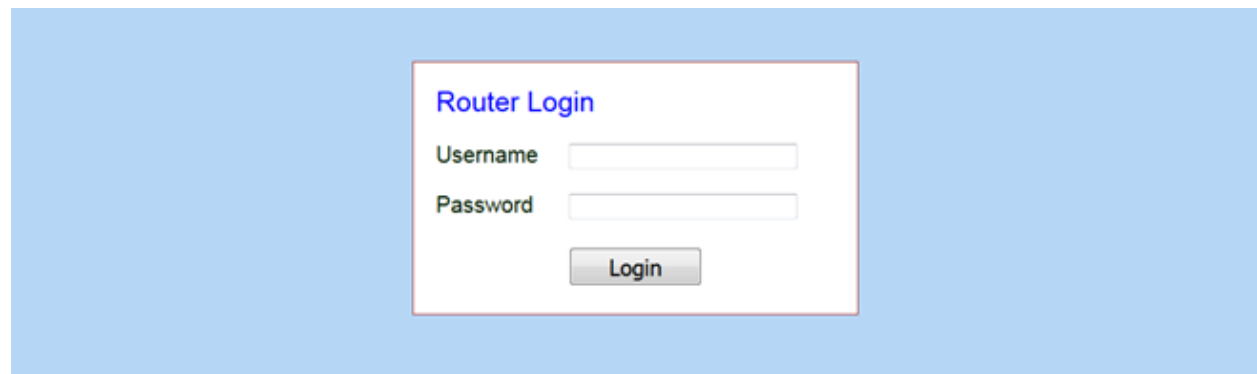
C:\Users\>_
```

The connection is not working properly and you should go through the instructions again and check your settings.

3.3.6 Configuring the TK500 (Optional)

After you have performed the steps described in the previous chapter, you can configure the router:

1. Open any Internet browser (e.g. Google Chrome) and enter the default IP address of the router: <http://192.168.2.1>. The following login page pops up:



The image shows a web browser window with a light blue background. In the center, there is a white box with a red border titled "Router Login". Inside this box, there are two input fields: "Username" and "Password". Below these fields is a "Login" button. The "Username" field is empty, and the "Password" field is also empty.

Enter the user name (default: adm) and password (default: 123456), and then click “**Login**” to open the configuration screen.

2. Change the IP configuration:

If you want to set your own IP, follow the instructions below:

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. Click **Network > VLAN**.

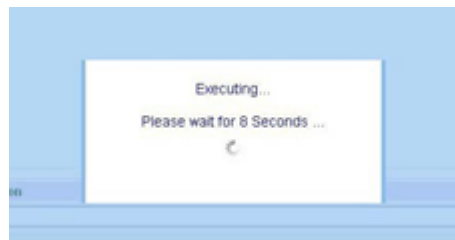
2. To add a VLAN ID, click “**Add**”.

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"/>			

For example, change the IP address to **192.168.1.254** and select the LAN ports to be assigned to this IP address.

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)												
		<table border="1"> <thead> <tr> <th>IP Address</th> <th>Netmask</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </tbody> </table>							IP Address	Netmask	<input type="text"/>	<input type="text"/>
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. Click “**Apply**” and the following screen will be displayed:



The IP address of the TK500 has been changed. In order for you to access the configuration page again the PC must be set up in the same subnet, for example: **192.168.1.10/24** - Then enter the changed IP address (**192.168.1.254**) in your browser.

3.3.7 Connecting the TK router to the Internet

Perform the following configuration steps to establish a connection between the TK500 and the Internet.

Click **Network > Cellular**, and enable the function by **Enable**:

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		*99#	Auto		

Check the entries and select a preset network provider under **SIM1 Network Provider**, or add a self-created profile of a provider:

You can obtain the APN, dial-in number, user name and password from your local network provider. Check with them for the details.

Via **Show Advanced Options** you can make further settings, such as the PIN code if it is set on the SIM card.

Show Advanced Options ☒

Dual SIM Enable ☐
 Initial Commands: AT
 Binding ICCID:
 PIN Code:
 Dial Timeout: 120 Seconds
 MTU: 1500
 MRU: 1500
 TX Queue Length: 64
 Enable IP head compression ☒
 Use default asyncmap ☐
 Use Peer DNS ☒
 Link Detection Interval: 55 Seconds(0: disable)
 Link Detection Max Retries: 3
 Debug ☐
 Debug Modem ☐
 Expert Options: nomppe nompppc nodeflate nobsdcomp novj novjccomp noccp
 ICMP Detection Mode: Ignore Traffic
 ICMP Detection Server:
 ICMP Detection Interval: 30 Seconds
 ICMP Detection Timeout: 20 Seconds
 ICMP Detection Retries: 5

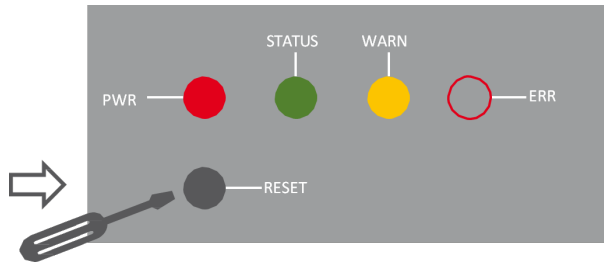
If you have set the correct configuration, the TK500 can now connect to the Internet. Open an Internet browser, type “www.welotec.com” and the Welotec website will open.

3.4 Reset to factory settings

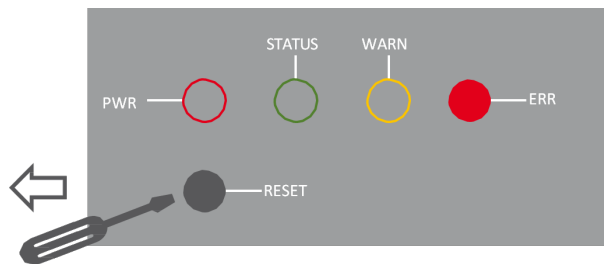
3.4.1 Hardware method

 = LED on
  = LED off
  = LED flashing

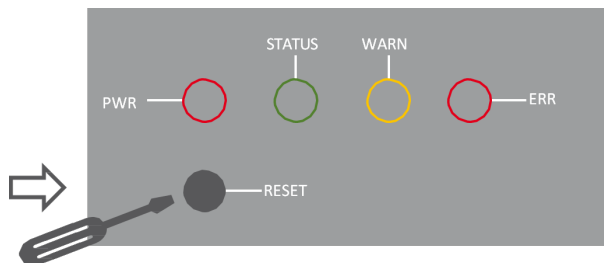
1. Press the **RESET** key while switching on the TK500:



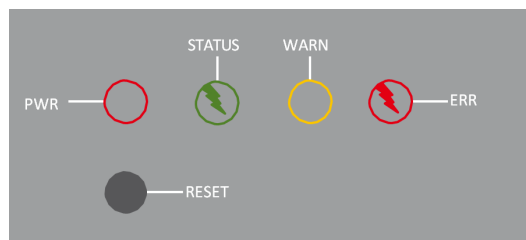
2. As soon as the ERROR LED lights up (approx. 10 seconds after switching on), release the **RESET** key:



3. After a few seconds, the ERROR LED light will stop illuminating. Now press the **RESET** key again:



4. The ERROR and STATUS LED lights will then flash, indicating that the reset to the default setting was successful.



Factory default settings:

- IP: 192.168.2.1

- Net mask: 255.255.255.0

- Username: adm

- Password: 123456

- Serial parameter: 115200-N-8-1

3.4.2 Web method

1.) Log in to the TK500 web-based user interface and select **System > Config Management**:



The screenshot displays the TK500 web-based user interface. At the top, there is a navigation bar with tabs: System, Network, Services, Firewall, QoS, VPN, Tools, Application, and Status. Below the navigation bar, a yellow warning message states: "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)". Under "Router Configuration", there is a text input field containing "No file selected.", followed by "Browse...", "Import", and "Backup" buttons. Below this is a button labeled "Restore default configuration". Under "Network Provider (ISP)", there is another text input field containing "No file selected.", followed by "Browse...", "Import", and "Backup" buttons.

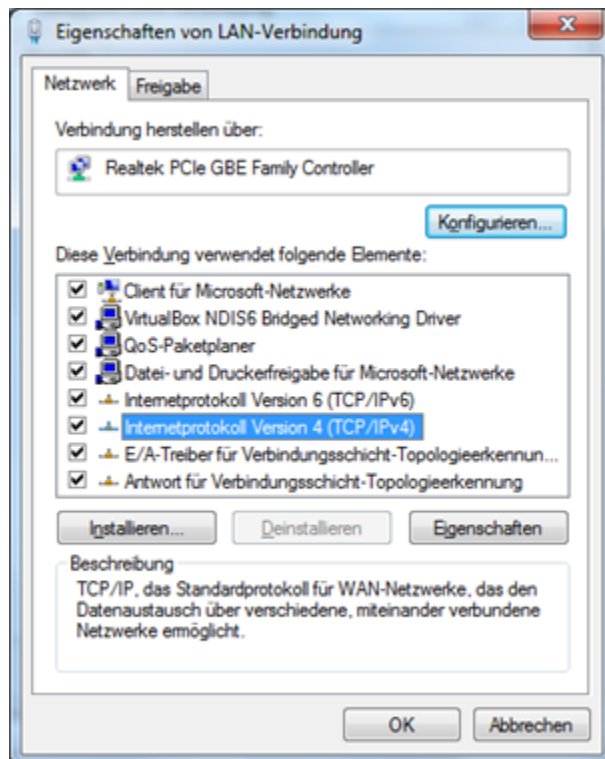
2.) Click **Restore default configuration** to reset the TK500 to its factory settings. After that the router will be re-booted.

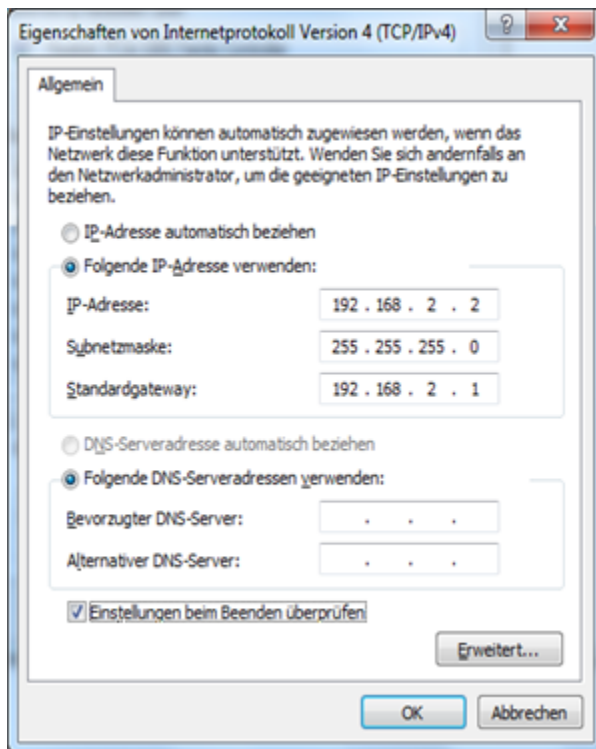
4 System

The TK-500 Router must be properly configured before use. This chapter describes the web-based configuration.

4.1 Preparation

First connect your devices to the TK500 via cable or hub (switch) and set the IP address for the PC and TK500 in the same subnet, e.g.: set the PC IP address to 192.168.2.2, netmask: **255.255.255.0**, gateway (default IP of TK500: **192.168.2.1**):





Open an Internet browser and enter the IP address of the TK500: <http://192.168.2.1> (default IP of the TK500).

On the following login page, you must log in as an administrator. Enter the user name and password (default: *adm/123456*).

Router Login

Username
Password

Click on “**Login**” to open the configuration page.

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		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 <input type="button" value="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

The system settings include the following ten areas: Basic Setup, Time, Serial Port, Admin Access, System Log, Config Management, Scheduler, Upgrade, Reboot and Logout.

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

4.2 Basic Setup

In the Basic Setup you can change the language of the menu and the host name. This menu item can be accessed via **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						

Parameter name	Description	Default	Example
Language	Set language for configuration page	English	English
Host Name	Host name of the TK500	Router	My Router

4.3 Time

In this menu item the system time of the router can be adjusted. It is also possible to set up a time server (NTP Time Server) to automatically keep the system time up to date.

System
Network
Services
Firewall
QoS
VPN
Tools
Application
Status

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

Time

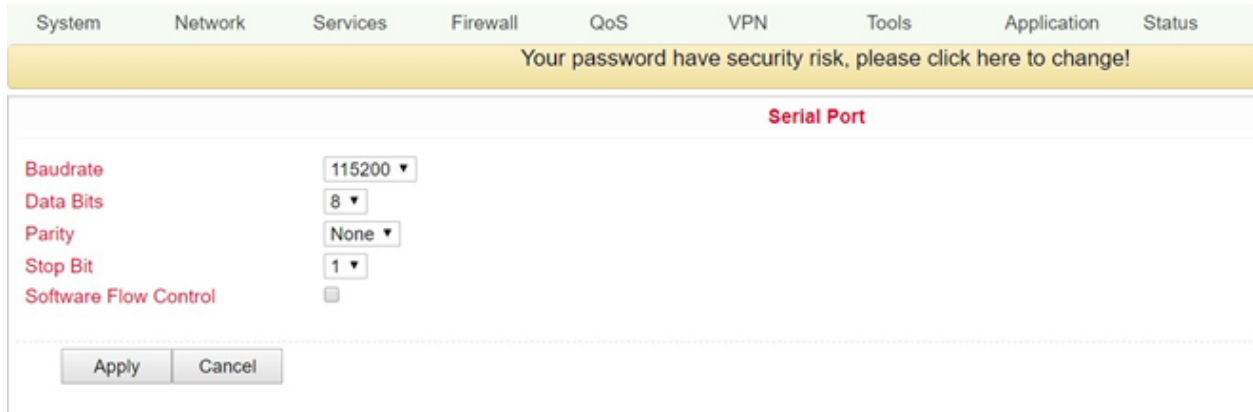
Router Time2018-10-01 14:05:36
PC Time2018-10-01 14:05:37 Sync Time
TimezoneUTC+01:00 France, Germany, Italy
Auto Daylight Savings Time☒
Auto Update TimeEvery 1 hour
Trigger Connect On Demand☐
NTP Time Servers0.de.pool.ntp.org
1.de.pool.ntp.org
2.de.pool.ntp.org

Apply
Cancel

Name	Description	Default
Router Time	Router time	2017-08-01 16:00:00
PC Time	Time of the PC (or the time of the device connected to the router)	The Sync Time button allows you to synchronize the time with the connected device
Timezone	Set time zone	selectable time zone
Auto Daylight Savings Time	Automatic changeover: daylight saving time/winter time	Disabled
Auto Update Time	Time of the automatic time update	Disabled
NTP Time Servers (after enabling the "Auto Update Time" option)	Setting for NTP time server (maximum three entries)	pool.ntp.org

4.4 Serial Port

You can adjust the settings for the serial port of the router via the menu item **System > Serial Port**.



The screenshot shows the 'Serial Port' configuration page. At the top, there is a navigation bar with tabs: System, Network, Services, Firewall, QoS, VPN, Tools, Application, and Status. Below the navigation bar is a yellow warning message: 'Your password have security risk, please click here to change!'. The main content area is titled 'Serial Port' and contains the following settings:

- Baudrate: 115200 (dropdown menu)
- Data Bits: 8 (dropdown menu)
- Parity: None (dropdown menu)
- Stop Bit: 1 (dropdown menu)
- Software Flow Control: ☐ (checkbox)

At the bottom of the settings area, there are two buttons: 'Apply' and 'Cancel'.

Name	Description	Default
Baud Rate	Serial baud rate	115200
Data Bits	Serial data bits	8
Parity	Set parity bit of serial data	None
Stop Bit	Set stop bit of serial data	1
Software Flow Control	Software flow control	Disabled

4.5 Admin Access

In this area you can change or adjust important settings, such as the password of the administrator or the port assignment for access to the router. These settings can be reached via **System > Admin Access**.

Username / Password

Username	<input type="text" value="adm"/>
Old Password	<input type="password" value="•••••"/>
New Password	<input type="password"/>
Confirm New Password	<input type="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

Apply

Cancel

Name	Description	Default
User-name/Password		
Username	Username for login to the configuration page	adm
Old Password	To change the password, it is necessary to enter the old password	123456
New Password	Enter new password	
Confirm New Password	Enter new password again	
Management		
HTTP/HTTPS/TELNET/SSHD/HTTP_API/Console		
Enable	Select to enable	Enabled
Service Type	HTTP/HTTPS/TELNET/SSHD/HTTP_API/Console	80/443/23/22/4444/Blank
Local Access	Enabled - Allow router to be managed via LAN (e.g.: HTTP).	Enabled
Remote Access	Enabled - Allow the TK500 to be managed over WAN (e.g.: HTTP).	Enabled
Allowed addresses from WAN (Optional)	Sets the range of allowed IP addresses for WAN	Servers for control services can be specified, such as 192.168.2.1/30 or 192.168.2.1
Description	Describe management parameters (without effect on the TK500)	
Non-privileged users		
Username	Create user names without administrator rights	
Password	Create password for user without administrator rights	
Other parameters		
Login Timeout	Set log timeout, after this value connection with the configuration page is disconnected and you have to log in again	500 Seconds

4.6 System Log

Setting options for logging log files. You can reach these via **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)		192.168.2.254 : 514						
Log to Console		<input type="checkbox"/>						
Apply		Cancel						

Name	Description	Default
Log to Remote System	Enable remote log server	Disabled (if enabled, IP address and port can be entered)
IP Address/Port (UDP)	Set IP address and port of the remote protocol server	Port: 514
Log to Console	Output of the log on the serial interface	Disabled

4.7 Config Management

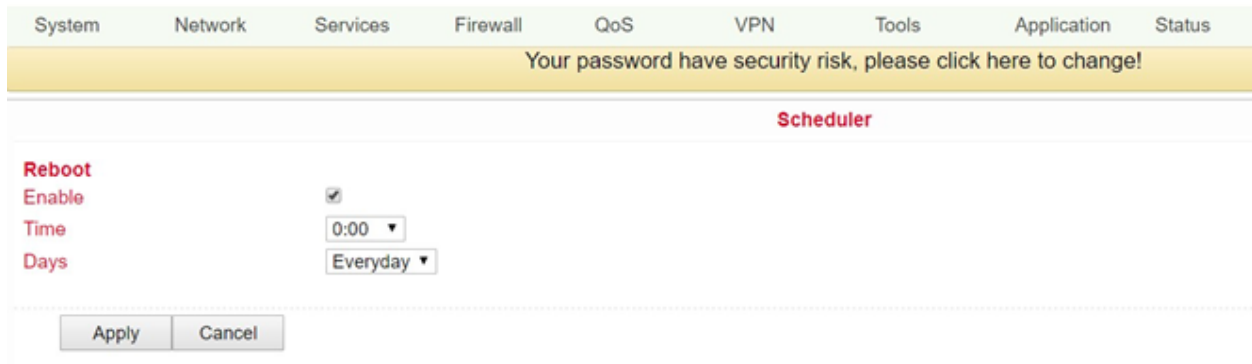
Backup and import of router configurations, as well as reset to factory settings of the router and backup or restore the provider data. You can reach this menu item via **System > Config Management**.

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.			Browse...		Import		Backup	
Restore default configuration								
Network Provider (ISP)								
No file selected.			Browse...		Import		Backup	

Name	Description
Router Configuration	Upload/save configuration file for import/backup
Restore default configuration	Click to reset the TK500 (to activate the default configuration, the TK500 must be restarted).
Network Provider (ISP)	To import or save APN, username, password and other parameters from traditional operator.
Browse	Using the Browse button you can select the file with the settings to be uploaded via Import

4.8 Scheduler

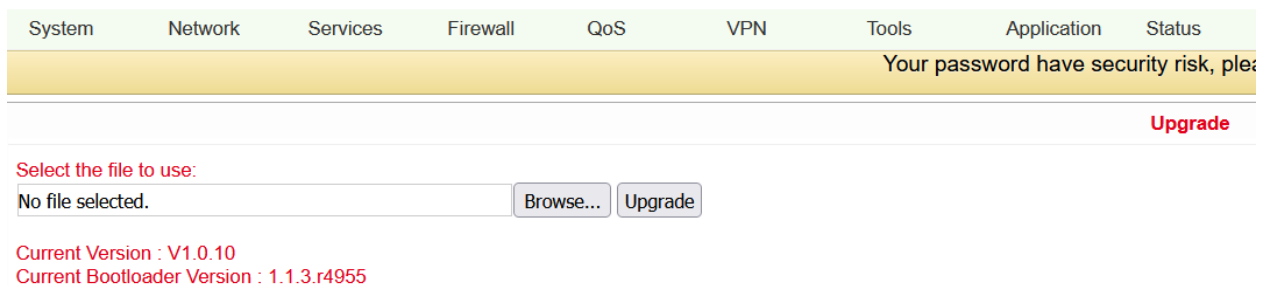
The scheduler is used to set the automatic reboot for the router. You can define the settings for this via **System > Scheduler**.



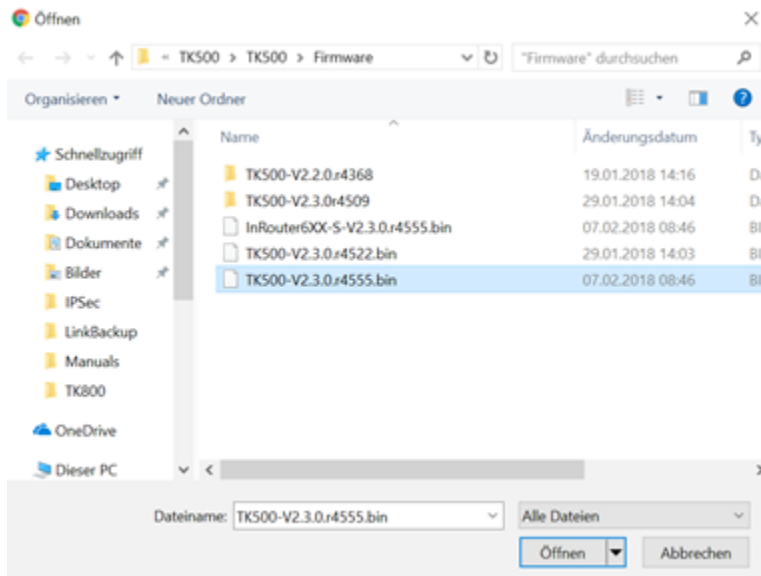
Name	Description
Enable	Switches the Auto Reboot on or off
Time	Time at which the TK500 router is to be rebooted
Days	Everyday selection for daily restart

4.9 Upgrade

In this area, the router provides you with an interface for updating the firmware. To be reached via **System > Upgrade**.



To update the system, select the update file (e.g. TK500-V2.2.0v4xxx.bin) in your file system via the **Select_file_** button.



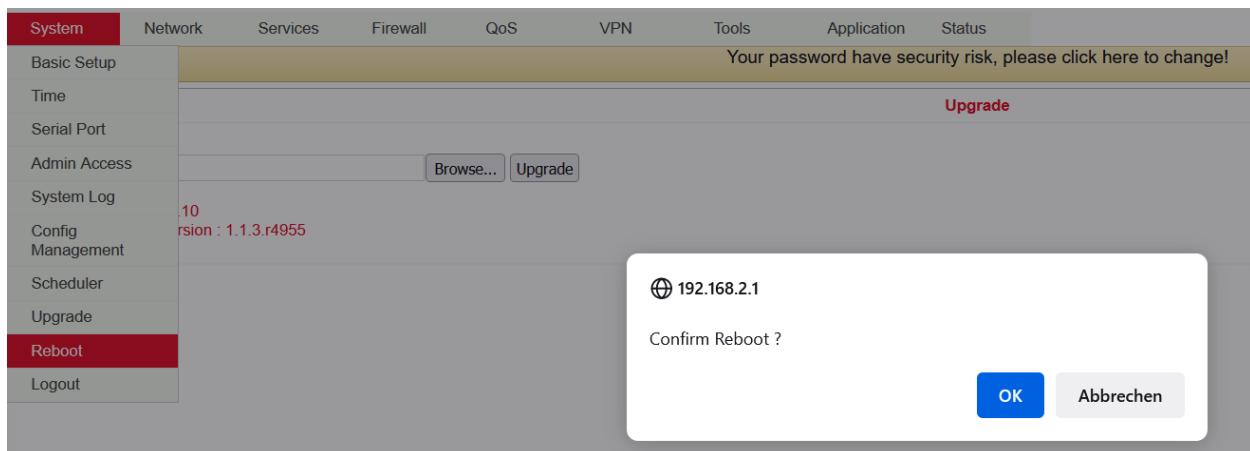
Click the “**Upgrade**” button and confirm the start of the upgrade



After successfully updating the firmware, click **Reboot** to restart the TK500.

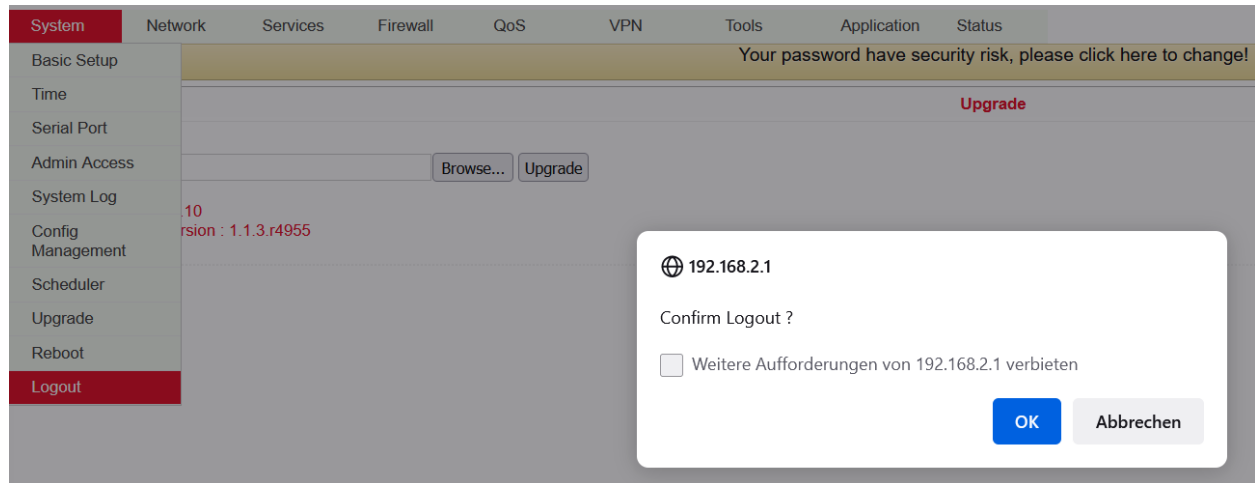
4.10 Reboot

If you need to reboot your router, select **System > Reboot**. Then click “**OK**” to reboot the system.



4.11 Logout

To log out of the system, click **System > Logout** and confirm the logout with “OK”.



5 Network

Use the network settings to configure Cellular, WAN, WAN(STA), VLAN, Switch WLAN Mode, WLAN Client, Link Backup, VRRP, IP Passthrough, Static Route, OSPF

5.1 Cellular

In this menu area you define and configure the dial-up of your router. Can be reached via **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		*99#	Auto		
<input type="button" value="Add"/>					

Name	Description	Default
Enable	Activates the dialup function	Enabled
Time Schedule	Set time for online and offline (see also 3.2.1.1)	ALL
Shared Connection (NAT)	Enabled - device connected to router	Enabled
Default Route	Mobile radio interface as standard route to the Internet	Enabled
Network Provider (ISP)	Select local ISP, if not listed here, select "Custom"	Custom
APN	APN parameters supplied by the provider	internet.t-d1.de (Telekom)
Access Number	Dial-up parameters provided by the local ISP	*99***1#
Username	Username provided by the provider	tm
Password	Password provided by the local ISP	tm
Network Select Type	Select mobile network type (2G, 3G, 4G only)	Auto
Connection Mode	Connection mode: Router is always online	Always Online
Redial Interval	If dial-up fails, the TC router dials again after this interval	30 Seconds
Show Advanced Options	Allows configuring advanced options	Disabled
PIN Code	Field for the PIN number of the SIM card	Blank
MTU	Set MTU (Maximum Transmission Unit)	1500
Authentication Type	PAP, CHAP	Auto
Use Peer DNS	Enable this option to accept peer DNS	Enabled
Link Detection Interval	Set interval for connection detection (0 = disabled)	55 Seconds
Debug	Enable debug mode	Disabled
Debug Modem	Enable Debug Modem	Disabled
ICMP Detection Mode	Monitor Traffic: Only when no data is flowing, a Keep Alive ping is sent at regular intervals	Monitor Traffic
ICMP Detection Server	Set server for ICMP detection; empty field means none is available	Blank
ICMP Detection Interval	Set interval for ICMP detection	30 Seconds
ICMP Detection Timeout	Set timeout for ICMP detection (TK500 is restarted on ICMP timeout)	20 Seconds
ICMP Detection Retries	Set maximum number of retries if ICMP fails	5

5.1.1 Schedule Management

Schedule management (next to “Time schedule”):

Enable

Time schedule



ALL ▾

Schedule Management

Here you can run your own dialup strategy, i.e. you can define here over three time ranges when the router should be online.

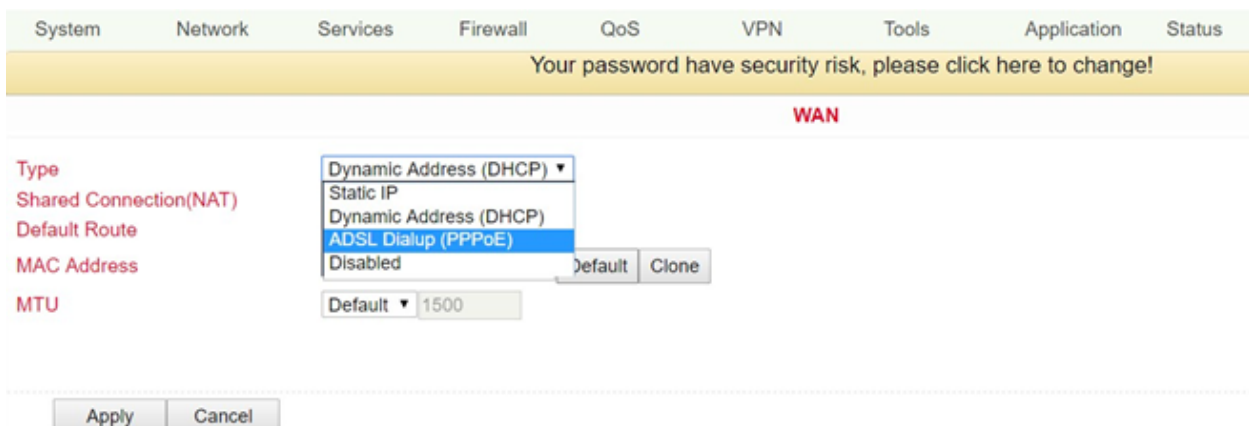


Name	Description	Default
Name	Name for the schedule	Schedule_1
Sunday	Sunday	Blank
Monday	Monday	Enabled
Tuesday	Tuesday	Enabled
Wednesday	Wednesday	Enabled
Thursday	Thursday	Enabled
Friday	Friday	Enabled
Saturday	Saturday	Blank
Time Range 1	Set time range 1	9:00-12:00
Time Range 2	Set time range 2	14:00-18:00
Time Range 3	Set time range 3	0:00-0:00
Description	Describe configuration	Blank

You can also create multiple schedules if, for example, different working hours apply on one working day.

5.2 WAN

Here you can set up a new WAN (Wide Area Network). To be reached via **Network > WAN**.



On this page the type of the WAN port can be set:

Name	Description	Default
Type	Static IPDynamic Address(DHCP)ADSL Dialup(PPPoE)Disabled	Disabled

Only one WAN type can be enabled at a time. Enabling one type disables another.

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)
☒

Default Route
☒

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

Apply
Cancel

Name	Description	Default
Type	Static IP	Dis-abled
Shared Connection (NAT)	Enabled - local device connected to router can access the Internet	Enabled
Default Route	Mobile radio interface as standard route to the Internet	Enabled
MAC Address	Set MAC address (button Default = standard, Clone = newly created MAC address)	Default
IP Address	Set IP address for WAN port	192.168.1.29
Netmask	Set netmask for WAN port	255.255.255.0
Gateway	Set WAN gateway	192.168.1.1
MTU	Set the maximum transmission unit (MTU), the options "Default" and "Manual" are possible	Default = 1500
"Multi-IP Settings" (a maximum of 8 additional IP addresses can be set)		
IP Address	Set another IP address for LAN	Blank
Netmask	Set netmask	Blank
Description	Describe settings	Blank

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)
☒

Default Route
☒

MAC Address
00:18:05:0C:C3:9B
Default
Clone

MTU
Default
1500

Apply
Cancel

Name	Description	Default
Type	Dynamic Address (DHCP)	
Share Connection (NAT)	Enabled - local device connected to router can access the Internet	Enabled
Default Route	Mobile radio interface as standard route to the Internet	Enabled
MAC Address	Set MAC address	
MTU	Set the maximum transmission unit (MTU), the options "Default" and "Manual" are possible	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="password"/>							
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	Description	Default
Type	ADSL Dialup (PPPoE)	
Share Connection (NAT)	Enabled - local device connected to router can access the Internet	Enabled
Default Route	Mobile radio interface as standard route to the Internet	Enabled
MAC Address	Set MAC address	
MTU	Set the maximum transmission unit (MTU), the options "Default" and "Manual" are possible	Default = 1492
ADSL Dialup (PPPoE) Settings		
Username	Set user name to dial in	Blank
Password	Set password to dial in	Blank
Static IP	Enable static IP addresses	Disabled
Connection Mode	Set connection mode ("Connect on Demand"/"Always On-line"/"Manual")	Always Online
Show Advanced Options/erweiterte Optionen		
Show advanced options	Enable advanced configuration	Disabled
Service Name	Here you can assign a name for the service	Blank
TX Queue Length	Set the length of the transfer queue	3
Enable IP head compression	Click to enable IP header compression	Blank
User Peer DNS	Enable peer DNS for users	Disabled
Link Detection Interval	Set interval for connection detection	55 Seconds
Link Detection Max Retries	Set maximum number of repetitions for connection detection	10 (times)
Debug	Select to enable debug mode	Disabled
Expert Options	Set expert parameters	Blank
ICMP Detection Server	Set server for ICMP detection	Blank
ICMP Detection Intervall	Set time for ICMP detection	30
ICMP Detection Timeout	Set timeout for ICMP detection	3
ICMP Detection Retries	Set maximum number of retries for ICMP detection	3

5.3 WAN(STA)

Under this menu item **Network > WAN(STA)** you can configure the TK500 as a WAN station. The settings in this menu item are the same as those in the WAN settings.

System	Network	Services	Firewall	QoS	VPN	Tools	Status
WAN(STA)							
Type	<div>Disabled ▾</div>						
<div> <div>Apply</div> <div>Cancel</div> </div>							

5.4 VLAN

A Virtual Local area Network (VLAN) is a logical subnet within a switch or an entire physical network. A VLAN separates physical networks into subnets by ensuring that VLAN-capable switches do not forward the frames (data packets) of one VLAN to another VLAN. This happens even though the subnets may be connected to common switches.

5.4.1 VLAN table

In the VLAN table you can change the assignment of VLANs to FastEthernet ports and create new VLANs.

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 ✕		
					Add	Modify	Delete

5.4.2 Port Mode

In the Port Mode menu, different VLAN IDs can be assigned to the network ports FastEthernet LAN1 to LAN4.

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

The options Acces and Trunk are available for the FastEthernet ports. In Access Mode, VLAN1 is always selected. In Trunk Mode you can assign VLAN IDs between 1-4000, which you have created before, to the FastEthernet ports.

5.5 Switch WLAN Mode

Settings for the WLAN type can be made here. A distinction is made between Access Point (AP) and Station (STA). This can be accessed under *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	Description	Default
AP	Access Point Mode	AP
STA	Client Mode	

If *WLAN TYPE STA* (for station) is selected, the menu under Network changes. It is then possible to configure *WAN(STA)* under 3.2.3 and to set up only one client for an existing WLAN under 3.2.6.a *WLAN Client*.

5.6 WLAN Client

If the item *STA* was selected as WLAN type when configuring the *Switch WLAN Mode* (see 3.2.6.), it is no longer possible to configure a WLAN. You can then only configure the TK 500 as a WLAN client. This then works under *Network > WLAN Client*.

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

To configure the router as a WLAN client, please click 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		*****					
<div> <div>Apply</div> <div>Cancel</div> </div>							

Now enter the data to connect the TK500 to an existing WLAN.

5.7 Link Backup

This option secures connections between wireless WAN and Ethernet WAN. If one WAN fails, the TK500 automatically uses the other. You can configure this under *Network > Link Backup*.

[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	Description	Default
Enable	Activate the service for connection backup	Disabled
Main Link	Selection of WAN, dialup and WAN(STA) as main WAN possible	WAN
ICMP Detection Server	ICMP can ensure a connection to a specific destination	Blank
ICMP Detection Interval	Time interval between ICMP packets	10
ICMP Detection Timeout	Timeout for the individual ICMP packets	3 (Seconds)
ICMP Detection Retries	If no retry of ICMP detection was successful, the backup connection is selected	3
Backup Link	Select backup connection	Dialup
Backup Mode	Hot Backup / Cold Backup	Hot Backup

5.8 VRRP

The Virtual Router Redundancy Protocol (VRRP) is a method for increasing the availability of important gateways in local networks by means of redundant routers. Several physical routers are combined into a logical group. This group of routers now presents itself in the network as a logical virtual router. For this purpose, the logical router is assigned a virtual IP address and a virtual MAC address. One of the routers within the group is defined as the virtual master router, which then binds the virtual MAC address and the virtual IP address to its network interface and informs the other routers of the group, which act as virtual backup routers. You can set up this function under **Services > VRRP**.

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

The TK500 series offers the possibility to create two different VRRP (VRRP I and VRRP II) groups.

Name	Description	Default
Enable VRRP-I	Select to activate VRRP	Disabled
Group ID	Select group ID for router (range 1-255)	1
Priority	Select priority for router (range 1 - 254)	20 (the larger the number, the higher the priority)
Advertisement Interval	Set advertisement interval	60 Seconds
Virtual IP	Set virtual IP for the group	Blank
Authentication Type	Optional: Typ „None/Password Authentication“	None. If Password Authentication is selected, a password can be assigned
Virtual MAC	Virtual MAC address	Disabled
Monitor	Checking the WAN connection	None
Enable VRRP-II	Select to activate VRRP	Disabled
Group ID	Select group ID for router (range 1-255)	2
Priority	Select priority for router (range 1 - 254)	10 (the larger the number, the higher the priority)
Advertisement Interval	Set advertisement interval	60 Seconds
Virtual IP	Set virtual IP for the 2nd group	Blank
Authentication Type	Optional: Typ „None/Password Authentication“	None. If Password Authentication is selected, a password can be assigned
Virtual MAC	Virtual MAC address	Disabled
Monitor	Checking the WAN connection	None

5.9 IP Passthrough

Here you can assign the WAN IP to a device connected to a LAN port.

System
Network
Services
Firewall
QoS
VPN
Tools

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

IP Passthrough

Enable IP Passthrough
☒

IP Passthrough Mode

DHCP Dynamic

DHCP Lease

2

Minutes

Apply

Cancel

Only one device can obtain this IP address and access the Internet. The LAN port should be of the Static type. The function does not work with a link backup.

5.10 Static Route

Here it is possible to add static routes. Static routes provide your router with additional routing information. Under normal circumstances, the router has sufficient information when configured for Internet access, and no additional static routes need to be configured. Static routes need to be set only in exceptional circumstances, such as when your network contains multiple routers or IP subnets. You can add static routes under **Network > Static Route** by clicking the Add button.

System
Network
Services
Firewall
QoS
VPN
Tools
Application
Status

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

Static Route

Destination	Netmask	Gateway	Interface	Description
0.0.0.0	255.255.255.0	0.0.0.0		

Apply

Cancel

Name	Description	Default
Destination	Set IP address of the destination	Blank
Netmask	Set subnet mask of the destination	255.255.255.0
Gateway	Set gateway of the destination	Blank
Interface	Optional LAN/WAN port access to target	Blank
Description	Freely selectable name for the static route	Blank

5.11 OSPF

Open Shortest Path First refers to a link-state routing protocol developed by the IETF.

This is a protocol for dynamic routing in IP networks. Dynamic routing detects changes in the network independently by the routers exchanging information with each other. The routing tables adapt dynamically to the respective situation.

Optimal routes to a destination can be determined based on various properties and metrics such as the number of hops, the bandwidth, the utilization of a link or configured costs. Failures of individual links are detected and alternative paths are calculated within a short time.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status																
Your password have security risk, please click here to change!																								
OSPF																								
Enable <input checked="" type="checkbox"/>																								
Router ID <input type="text"/>																								
Route Advanced Options <input checked="" type="checkbox"/>																								
ABR Type <input type="text" value="cisco"/>																								
RFC1583 Compatibility <input type="checkbox"/>																								
OSPF Opaque-LSA <input type="checkbox"/>																								
SPF Delay Time <input type="text" value="200"/> mseconds																								
SPF Initial-holdtime <input type="text" value="1000"/> mseconds																								
SPF Max-holdtime <input type="text" value="10000"/> mseconds																								
Reference Bandwidth <input type="text" value="100"/>																								
User Commands <input type="text"/>																								
Network																								
<table border="1"> <thead> <tr> <th>IP Address</th> <th>Netmask</th> <th>Area ID</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </tbody> </table>			IP Address	Netmask	Area ID	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>															
IP Address	Netmask	Area ID																						
<input type="text"/>	<input type="text"/>	<input type="text"/>																						
Interface																								
<table border="1"> <thead> <tr> <th>Interface</th> <th>Network</th> <th>Hello Interval</th> <th>Dead Interval</th> <th>Retransmit Interval</th> <th>Transmit Delay</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text" value="Broadcast"/></td> <td><input type="text" value="10"/></td> <td><input type="text" value="40"/></td> <td><input type="text" value="5"/></td> <td><input type="text" value="1"/></td> </tr> </tbody> </table>									Interface	Network	Hello Interval	Dead Interval	Retransmit Interval	Transmit Delay	<input type="text"/>	<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"/>				
Interface	Network	Hello Interval	Dead Interval	Retransmit Interval	Transmit Delay																			
<input type="text"/>	<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 <input checked="" type="checkbox"/>																								
<table border="1"> <thead> <tr> <th>Interface</th> <th>Passive Interface</th> <th>Cost</th> <th>Priority</th> <th>Authentication</th> <th>Key ID</th> <th>Key</th> <th>MTU Ignore</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="checkbox"/></td> <td><input type="text" value="10"/></td> <td><input type="text" value="10"/></td> <td><input type="text"/></td> <td><input type="text" value="adm"/></td> <td><input type="text" value="....."/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>									Interface	Passive Interface	Cost	Priority	Authentication	Key ID	Key	MTU Ignore	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="10"/>	<input type="text" value="10"/>	<input type="text"/>	<input type="text" value="adm"/>	<input type="text" value="....."/>	<input type="checkbox"/>
Interface	Passive Interface	Cost	Priority	Authentication	Key ID	Key	MTU Ignore																	
<input type="text"/>	<input type="checkbox"/>	<input type="text" value="10"/>	<input type="text" value="10"/>	<input type="text"/>	<input type="text" value="adm"/>	<input type="text" value="....."/>	<input type="checkbox"/>																	
							<input type="button" value="Add"/>																	
Area																								
<table border="1"> <thead> <tr> <th>Area ID</th> <th>Area</th> <th>No Summary</th> <th>Authentication</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="checkbox"/></td> <td><input type="text"/></td> </tr> </tbody> </table>									Area ID	Area	No Summary	Authentication	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>								
Area ID	Area	No Summary	Authentication																					
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>																					
				<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"/>	<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"/>								

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

In the service settings, you configure the DHCP service, DNS forwarding, VRRP, and other related parameters.

6.1 DHCP Service

The Dynamic Host Configuration Protocol (DHCP) is a communication protocol in network technology. It enables the assignment of the network configuration to clients through a server. In this way, devices in the network can be assigned IP addresses dynamically. You can access this service under **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	Description	Default
Enable DHCP	Click to enable DHCP	Enabled
IP Pool Starting Address	Set start IP address of the DHCP pool	192.168.2.2
IP Pool Ending Address	Set end IP address of the DHCP pool	192.168.2.100
Lease	Set valid lease time for the IP address received from the DHCP server	60 minutes
DNS	Set DNS server (click via Edit)	192.168.2.1
Windows Name Server	Set WINS	Blank
Static DHCP (a maximum of 20 IP addresses can be set)		
MAC Address	Set MAC address of a designated IP address	Blank
IP Address	Set static IP address	192.168.2.2
Host	Set hostname	Blank

6.2 DNS

Up to two DNS servers can be entered here if the router is part of a domain network that uses DNS for address resolution. You can enter the data under **Network > DNS**.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
DNS								
Primary DNS		<input type="text" value="192.168.2.100"/>						
Secondary DNS		<input type="text" value="8.8.8.8"/>						
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

Name	Description	Default
Primary DNS	Set primary DNS	Blank
Secondary DNS	Set secondary DNA	Blank

6.3 DNS Relay

When DNS relay is enabled (by default, if DHCP is set up), the IP address of the router is assigned to the DHCP clients as the DNS server. All DNS requests to the router are forwarded to your ISP's DNS servers. If DNS Relay is disabled, the Router assigns the ISP's DNS servers to the DHCP clients. You can access these settings via **Services > DNS Relay**.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
DNS Relay								
Enable DNS Relay		<input checked="" type="checkbox"/>						
Static [IP address <=> Domain Name] Pairing								
IP Address	Host	Description						
<input type="text"/>	<input type="text"/>	<input type="text"/>						
		<input type="button" value="Add"/>						
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

With the **Add** button up to 20 DNS pairs can be created.

Name	Description	Default
Enable DNS Relay	Click to enable DNS forwarding	Enabled (after enabling DHCP)
Static (IP Address <-> Domain Name) Pairing (maximum 20 DNS pairs)		
IP Address	Set IP address <-> DNS pairs	Blank
Host	Set names of IP address<->DNS pairs	Blank
Description	Describe IP address<->DNS pairs	Blank

6.4 DDNS (Dynamic DNS)

DDNS or dynamic DNS is used if the WAN connection does not have a fixed public IP address, but services are still to be accessed externally. Since the IP address of the provider can change again and again with a normal WAN connection, a secure setup, e.g. of a VPN tunnel, is not possible. Therefore one uses providers of dynamic DNS servers, which ensure that your WAN connection always gets over the IP address. You can reach the configuration via **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 Disabled ▼								
Dynamic DNS ==> Dialup								
Current Address 37.80.83.157 Service Type No-IP.com ▼ URL 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.								
<div> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </div>								

Name	Description	Default
Current Address	Show current IP address	Blank
Service Type	Select DDNS provider	Disabled

There are various setting options for different DDNS service providers. These are selected via the service type.

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> Disabled Disabled Oray - Dynamic QDNS(3322) - Dynamic QDNS(3322) - Static DynDNS - Dynamic DynDNS - Static DynDNS - Custom No-IP.com Custom gh-admin </div>								
Dynamic DNS ==> Dialup								
Current Address Service Type URL Username Password Hostname Wildcard MX Backup MX Force Update								

No-IP is used here as an example for the setup. For this, you need a No-IP account, which you have to create yourself. There are various providers here, some of which are free of charge, but some of which are subject to a charge. The assignment of the Dynamic DNS can be assigned to the WAN as well as to the dialup connection.

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.
<div> <div>Apply</div> <div>Cancel</div> </div>	

Name	Description	Default
Service Type	DynDNS - Dynamic	Disabled
URL	http://www.dyndns.com/	Set
Username	Registered username for	
DDNS	Blank	
Password	Registered password for DDNS	Blank
Hostname	Registered hostname for DDNS	Blank
Wildcard	Can be activated if wildcard is to be used	Disabled
MX	Entering an MX record	Blank
Backup MX	Can be activated if MX-Record should run as backup	Disabled
Force Update	Forces the update of the account	Disabled
Last Update	Shows when the IP address was last changed	
Last Response	Indicates the last time communication was made with the service	

6.5 DTU

DTU stands for Data Terminal Unit and is used to connect devices with serial interface (RS-232 and RS-485). You can create the configuration under **Services > DTU**. If DTU is activated, the console port is automatically deactivated.

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
<input type="text"/>	<input type="text"/>

Name	Description	Default
Enable	Click to activate DTU	Disabled
DTU Protocol	Set DTU protocol	Transparent
Protocol	Possible options are “TCP” and “UDP	UDP
Mode	Set DTU as client or server, depending on DTU Protocol selection possible	Client
Frame Interval	Set the frame interval in milliseconds	100 msec
Serial Buffer Frames	Default buffer frames	4
Multi-Server Policy	Selection between Parallel and Poll	Parallel
Min Reconnect Interval	Min Reconnect Interval	15 Sec
Max Reconnect Interval	Max Reconnect Interval	180 Sec
DTU ID	Default ID for the DTU	Blank
Source IP	IP address of the source computer	Blank
DTU ID Report Interval	Time interval for sending the DTU ID	0
Source IP	IP address of the source computer	Blank
DTU ID Report Interval	Time interval for sending the DTU ID	0
Multi Server		
IP-Adresse	Set up IP address for receiving data	Blank
Server Port	Set up server port for receiving data	Blank

Depending on the selection of the DTU protocol, the selection fields may vary.

6.6 SMS

The TK500 can be reached from outside via SMS and reacts to various commands sent via SMS. You have the possibility to query the status of the device or to restart the device. The router is configured via **Services > SMS**.

System
Network
Services
Firewall
QoS
VPN
Tools
Application
Status

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

SMS

Enable ☒

Status Query (English Only)

Reboot (English Only)

SMS Access Control

Default Policy

Phone Number	Action	Description
4917212345678	Accept	1. SMS Empfänger

Name	Description	De- fault
Enable	Click to enable or disable SMS control	Dis- abled
Status Query	Set status request SMS to display the status of the router via SMS (e.g.: show status).	Blank
Reboot	Lets the router restart (e.g. reboot)	Blank
SMS Access Control		
Default Policy	Block or Accept control SMS from specific phone.	Ac- cept
Phone Number	Enter phone numbers to send SMS to router. The format for mobile number is 491712345678 (please do not enter +49 or 0049)	Blank
Action	Accept or block the previously entered phone number	Ac- cept
Description	Description for the created dataset	Blank

To be able to send an SMS to the router, the mobile number of the inserted card must be known. The SMS is then sent to this number.



SMS that you receive on your cell phone:

Host: (SN);

Uptime: (the operating time of the router at the time of this reboot);

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

LAN: (Ready) (LAN-IP)

6.7 Traffic Manager

The Traffic Manager can be used to provide the data consumption of the dial-up connection interface. You can configure this service under **Services > Traffic Manager**.

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

Name	Description	De- fault
Enable	Click to enable or disable SMS control	Dis- abled
Alarm Thresh- old	Sets the amount of data in MB per month at which an alarm should be generated. If 0 is set as value, no alarm will be generated	Blank
Disconnect Threshold	If the set value is reached, the dial-up connection is interrupted	Blank

The amount of data used can be checked at any time under Traffic Statistics (see 3.8.3).

6.8 Alarm Manager

The Alarm Manager can be used to generate various alarms. You can configure this service under **Services > Alarm Manager**.

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

Name	Description	Default
Alarm Input	Select here the areas for which an alarm is to be generated	none
Alarm Output	Here you can choose whether the alarms should be issued via the console or not	selected

7 Firewall

The **Firewall** menu item allows you to set the parameters for the router's firewall. Various settings are possible here.

7.1 Basic

Here you can configure the basic settings of the firewall.

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"/>						
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

Name	Description	Default
Default Filter Policy	Possible options are allow and block	Allow
Block Anonymous WAN Request (ping)	Enable to block ping requests generated anonymously from the network	Dis-abled
Filter Multicast	Click to enable filtering of multicast	En-abled
Defend DoS Attack	Click to enable fending off DoS attacks	En-abled

7.2 Filtering

At this point you can filter what the firewall should let through and what not. Various configurations are possible here, which you can reach via **Firewall > Filtering**.

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"/>	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

Name	Description	Default
Enable	Click to activate filtering	Enabled
Proto	Selection of the protocol. The options "TCP"/"UDP"/"ICMP" are possible	All
Source	Set source IP address	Blank
Source Port	Set source port if corresponding protocol was selected	Blank
Destination	Set destination IP	Blank
Destination Port	Set destination port if corresponding protocol was selected	Blank
Action	Selection whether setting should be accepted or blocked	Allowed
Log	Click to enable logging of the setting	Disabled
Description	Describe configuration	Blank

7.3 Content Filtering

The content filter in the firewall allows you to filter the call of special URLs, which can then be blocked or allowed. You can create the configuration under **Firewall > Content Filtering**.

System
Network
Services
Firewall
QoS
VPN
Tools
Application
Status

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

Content Filtering

Enable URL	Action	Log	Description
<input checked="" type="checkbox"/>	Accept	<input type="checkbox"/>	

Apply
Cancel

Name	Description	Default
Enable	Enable or disable the content filter function	Enabled
URL	Entering the URL to be blocked or filtered	Blank
Action	Selection whether URL is blocked or accepted	Enabled
Log	Can be activated for logging	Disabled
Description	Describe configuration	Blank

7.4 Port Mapping

NAT-PMP (NAT Port Mapping) allows a computer in a private network (behind a NAT router) to automatically configure the router so that devices behind the router can be reached from outside the private network. It essentially controls what is known as port forwarding. NAT-PMP, like UPnP also, and allows a program to request all incoming data from outside on a specific TCP or UDP port. You can perform the configuration under **Firewall > Port Mapping**.

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	Description	De- fault
Enable	Enable or disable port mapping	En- abled
Proto	Selection of TCP, UDP or TCP&UDP protocols	TCP
Source	Enter source IP	0.0.0.0/0
Service Port	Enter port of the service	8080
Internal Address	Set internal IP for mapping	Blank
Internal Port	Set port mapping to "internal"	8080
Log	Click to enable logging of port mapping	Dis- abled
External Address (Optional) / Tunnel Name (OpenVPN)	Used in conjunction with VPN. For port forwarding with VPN, the virtual VPN IP address of the TC router must be entered here	Blank
Description	Describe the meaning of the individual classifications	Blank

7.5 Virtual IP Mapping

The IP of an internal PC can be assigned to a virtual IP. An external network can access the internal PC via this virtual IP address. You can set up this configuration under **Firewall > Virtual IP Mapping**.

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	Description	Default
Virtual IP for Router	Set virtual IP for router	Blank
Source IP Range	Set range of source IP addresses	Blank
Virtual IP	Set virtual IP	Blank
Real IP	Set real IP	Blank
Log	Enable logging for virtual IP	Disabled
Description	Describe configuration	Blank

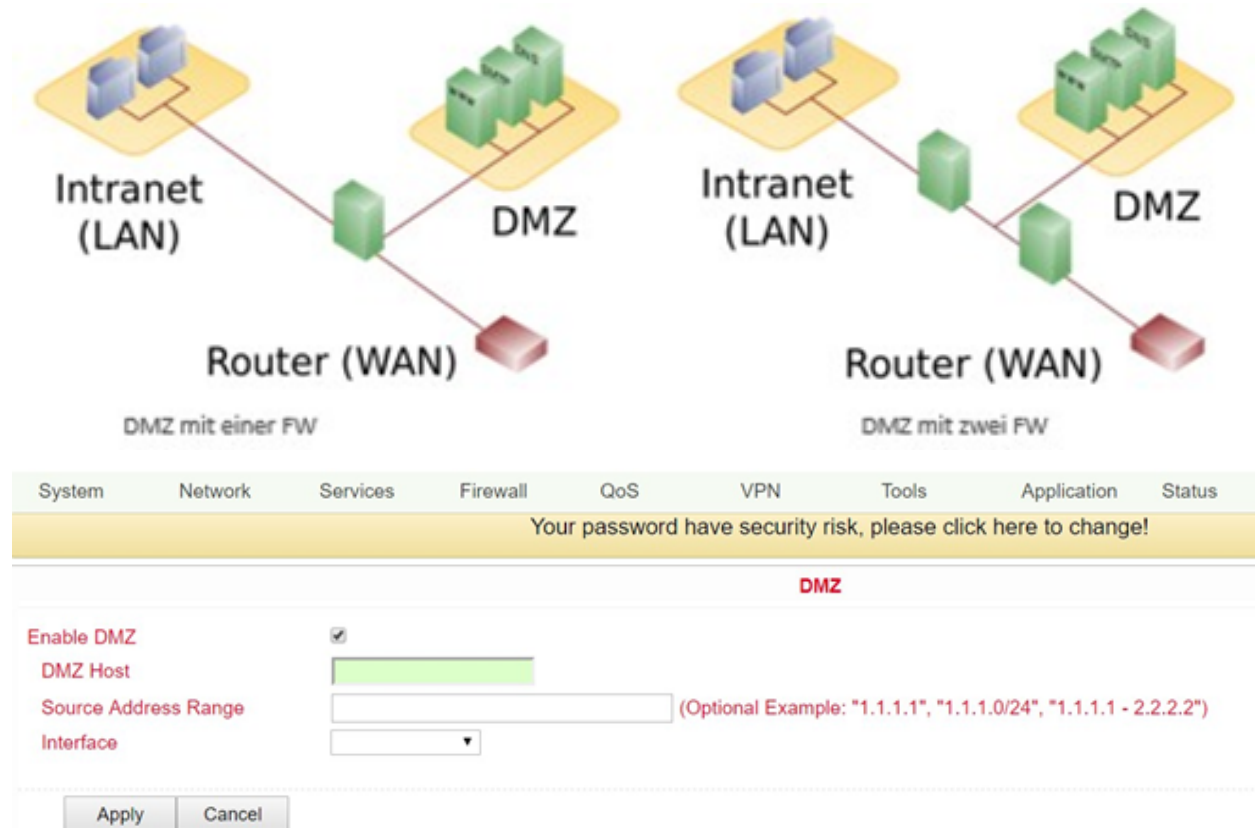
7.6 DMZ

A Demilitarized Zone (**DMZ**) refers to a computer network with security-controlled access to the servers connected to it.

The systems set up in the DMZ are shielded from other networks (e.g. Internet, LAN) by one or more firewalls. This separation allows access to publicly accessible services while protecting the internal network (LAN) from unauthorized access from the outside.

The purpose is to make services of the computer network available to both the Internet (WAN) and the intranet (LAN) on as secure a basis as possible.

A DMZ provides protection by isolating a system from two or more networks.



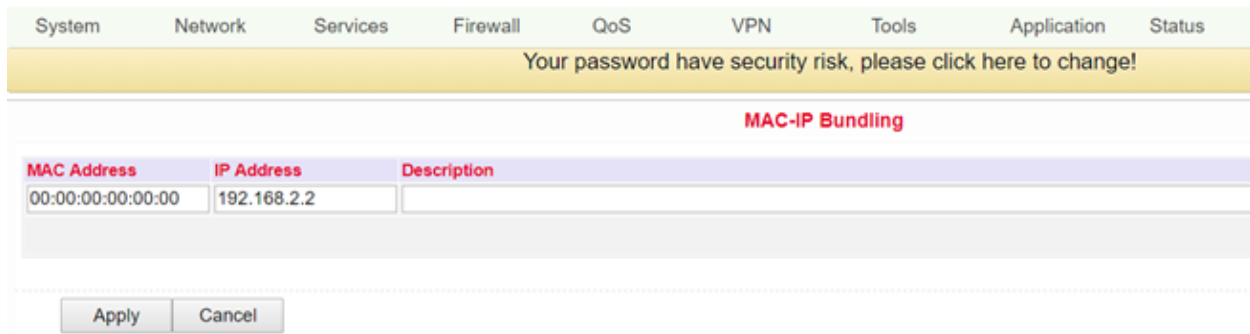
By mapping all ports and the external PC, you can access all ports of the device connected to the TK500.

With this function it is not possible to assign the administration port of the TK500 (e.g.: 80 TCP) to the port of the device. To forward port 80, change the management port of the router under **System > Admin Access**.

Name	Description	Default
Enable DMZ	Click to enable DMZ	Disabled
DMZ Host	Set DMZ host IP	Blank
Source Address Range	Set IP address with restricted IP access	Blank
Interface	Selection of the appropriate interface	Blank

7.7 MAC-IP Bundling

MAC IP bundling means assigning a predefined IP address to a defined MAC address. Thus the given MAC address always gets the same IP address. You can reach this menu item under **Firewall > MAC-IP Bundling**.



If a firewall blocks all access to the external network, only PCs with MAC-IP bundling will gain access to the external network.

Name	Description	Default
MAC Address	Set MAC address for bundling	Blank
IP Address	Set IP address for bundling	192.168.2.2
Description	Describe configuration	Blank

7.8 NAT

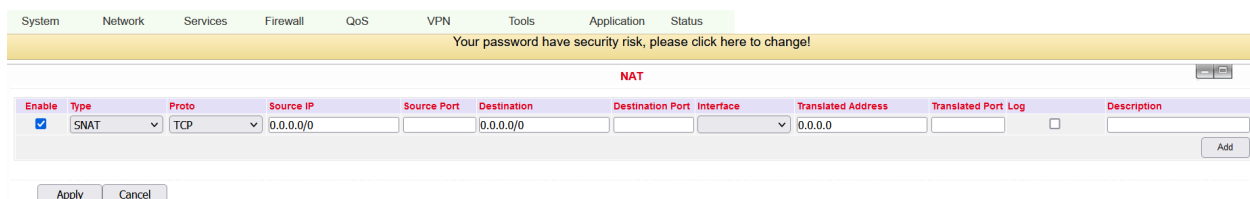
Network Address Translation (NAT) In computer networks, Network Address Translation is the collective term for procedures that automatically replace address information in data packets with other information in order to connect different networks. They are therefore typically used on routers.

7.8.1 Use of Source-NAT (SNAT)

It allows devices with private network addresses to connect to the Internet. Private IP addresses cannot usually be routed by the provider, so they must be translated into a public, routable IP address. The TK500v2 has implemented this function, which enables communication between different networks. In addition, a relevant security aspect is found in NAT, since a public IP address cannot be traced back to the associated private IP address.

7.8.2 Use of Destination-NAT (DNAT)

This is used to offer services that are operated on computers under a single IP address. It is often referred to as port mapping or port forwarding.



7.8.3 Configuration

- To configure NAT, go to the menu item *Firewall* and select the subitem *NAT*.
- Here you can find a list of all existing NAT rules
- New NAT rules can be added via the *Add* button

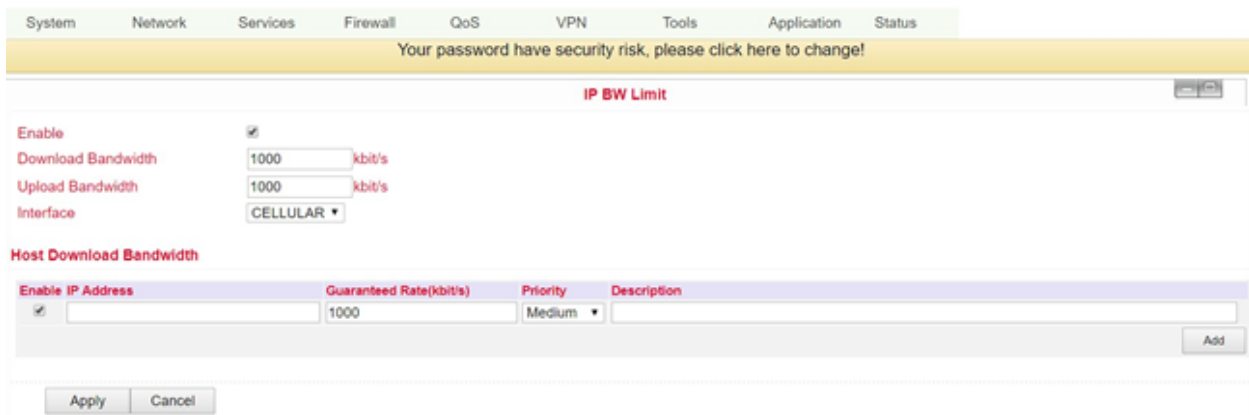
8 QoS

In the TCP/IP world, QoS describes the quality of a communication service from the user's point of view. Network service quality is often defined on the basis of the parameters bandwidth, delay, packet loss and jitter.

The network load influences the quality of the transmission. For example, how long does it take for a data packet to reach the recipient? For this reason, attempts are made to mark data packets with corresponding service classes. Prioritized data packets are then forwarded preferentially in routers or switches. In the TK 500 series it is therefore possible to limit and allocate the bandwidths accordingly. You can set this up via "QoS".

8.1 IP BW Limit

Under the menu item *QoS > IP BW Limit* you can limit the down- or upload bandwidth and bind it to IP addresses, as well as prioritize them.



The screenshot shows the 'IP BW Limit' configuration page. At the top, there's a navigation bar with tabs: System, Network, Services, Firewall, QoS, VPN, Tools, Application, and Status. Below the navigation bar is a yellow warning banner: 'Your password have security risk, please click here to change!'. The main title is 'IP BW Limit'. The configuration options include:

- Enable:** A checkbox that is checked.
- Download Bandwidth:** A text input field with '1000' and a unit dropdown set to 'kbit/s'.
- Upload Bandwidth:** A text input field with '1000' and a unit dropdown set to 'kbit/s'.
- Interface:** A dropdown menu currently showing 'CELLULAR'.
- Host Download Bandwidth:** A section containing a table with columns: 'Enable', 'IP Address', 'Guaranteed Rate(kbit/s)', 'Priority', and 'Description'. The table has one row with 'Enable' checked, 'IP Address' empty, 'Guaranteed Rate(kbit/s)' set to '1000', and 'Priority' set to 'Medium'. There is an 'Add' button to the right of the table.

 At the bottom, there are 'Apply' and 'Cancel' buttons.

Name	Description	Default
Enable	Click to enable	Disabled
Download Bandwith	Set the bandwidth for the download	1000kbit/s
Upload Bandwith	Set the bandwidth for upload	1000kbit/s
Interface	Selection of the interface to which the bandwidth is to be assigned	Cellular
Host Download Bandwidth		
Enable	Enable the function	Enabled
IP Adresse	Specify the IP address for allocation	Blank
Guaranteed Rate (kbit/s)	Indication of guaranteed bandwidth in kbit/s	1000
Priority	Assigning priority	Medium
Description	Rule description	Blank

9 VPN

A VPN (virtual private network) is a closed logical network in which the participants are physically separated from each other and connected via an IP tunnel. With this VPN, you can access a local network, e.g. the company network, while on the road or from your home office. This requires VPN software that both communicates with the network's router and is installed on the computer you want to use to access the network. There are different types of VPN connections (tunnels) that can be configured under this menu item on the TK 500 series.

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

Overview of the existing VPN connections. With **Add** a new tunnel can be created, see 3.6.2.

9.1 IPSec Settings

In this menu item you configure the settings for IPSec, which can be reached via **VPN > IPSec Settings**.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
IPSec Settings								
<div> <div>Enable NAT-Traversal (NATT)</div> <div><input checked="" type="checkbox"/></div> </div> <div> <div>Keep alive time interval of NATT</div> <div>60</div> <div>Seconds</div> </div> <div> <div>Enable Compression</div> <div><input checked="" type="checkbox"/></div> </div> <div> <div>Debug</div> <div><input type="checkbox"/></div> </div> <div> <div>Force NATT</div> <div><input type="checkbox"/></div> </div> <div> <div>Dynamic NATT Port</div> <div><input type="checkbox"/></div> </div>								
<div> <div>Apply</div> <div>Cancel</div> </div>								

Name	Description	Default
Enable NAT-Traversal (NATT)	Click to enable	Disabled
Keep alive time interval of NATT	Setting the duration for maintaining the NATT	60 Seconds
Enable Compression	Switch compression on or off	Enabled
Debug	Switch debug mode on or off	Disabled
Enable	Activate the function	Enabled
Force NATT	Switch NATT force on or off	Disabled
Dynamic NATT Port	Switching a dynamic NATT port on or off	Disabled

The address change via NAT is interpreted by a VPN gateway as a security-critical change to the data packets, the VPN negotiation fails, and no connection is established. These problems occur, for example, when dialing in via some UMTS mobile networks, where the network operator's servers do not support address conversion in connection with IPSec-based VPNs.

In order to be able to successfully establish a VPN connection in these cases, NATT (NAT Traversal) provides a method for overcoming these problems when handling data packets with changed addresses.

NATT can only be used for VPN connections that use ESP (Encapsulating Security Payload) for authentication. Unlike AH (Authentication Header), ESP does not take the IP header of the data packets into account when determining the hash value for authentication. The hash value calculated by the receiver therefore corresponds to the hash value entered in the packets

9.2 IPSec Tunnels

Via *VPN > IPSec Tunnels* you can set up a corresponding tunnel.

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	<input type="text"/>

XAUTH Parameters

XAUTH Mode	<input checked="" type="checkbox"/>
XAUTH Username	<input type="text"/>
XAUTH Password	<input type="text"/>
MODECFG	<input type="checkbox"/>

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	<input type="text"/>
ICMP Detection Local IP	<input type="text"/>
ICMP Detection Interval	60 Seconds
ICMP Detection Timeout	5 Seconds
ICMP Detection Retries	10

This page presents the web-based parameters for the TK500.

Name	Description
Show Advanced Options	Click to enable advanced options
Basic Parameters	
Tunnel Name	Tunnel Name
Destination Address	Set the destination address of the IPSec VPN server
Startup Modes	Possible modes are "Auto Activate"/ "Triggered by Data"/"Passive"/"Manu
Restart WAN when failed	WAN Interface is restarted if tunnel setup fails
Negotiation Mode	Optional: "Main Mode" or "Aggressive Mode"
IPSec Protocol	Optional: "ESP" or "AH"
IPSec Mode	Optional: "Tunnel Mode" or "Transport Mode"

Table 1 – continued from previous page

Name	Description
VPN over IPSec	L2TP or GRE over IPSec
Tunnel Type	Selection field for various setting options
Local Subnet	Set protected IPSec subnet (Local)
Local Netmask	Set protected IPSec subnet mask (Local)
Remote Subnet	Set protected IPSec subnet (remote)
Remote Netmask	Set protected IPSec subnet mask (remote)
	Phase 1 Parameters
IKE Policy	Multi-selection list for the policy
IKE Lifetime	Set IKE validity period
Local ID Type	Selection of “FQDN”; “USERFQDN” or “IP address” possible
Remote ID Type	Selection of “IP address”; “USERFQDN”; or “FQDN” possible
Authentication Type	Selection of “Shared Key” or “Certificate” possible
Key (if authentication type “Shared Key” is selected)	Set IPSec key for VPN negotiation
	XAUTH Parameters
XAUTH Mode	Enable XAUTH
XAUTH Username	XAUTH Username
XAUTH Password	XAUTH Password
MODECFG	Enable MODECFG
	Phase 2 Parameters
IPSec Policy	Multi-selection list for the policy
IPSec Lifetime	Set IPSec validity period
Perfect Forward Secrecy (PFS)	Optional: “Disable”; “GROUP1”; “Group2”; “Group5”
	Link Detection Parameters
DPD Time Interval	Set DPD Time Interval
DPD Timeout	Set DPD Timeout
ICMP Detection Server	Set server for ICMP detection
ICMP Detection Local IP	Set local IP for ICMP discovery
ICMP Detection Interval	Set interval for ICMP detection
ICMP Detection Timeout	Set timeout for ICMP detection
ICMP Detection Max Retries	Set maximum number of retries for ICMP detection

9.3 GRE Tunnels

Generic Routing Encapsulation (GRE) is a network protocol developed by Cisco and defined in RFC 1701. GRE can be used to wrap other protocols and thus transport them in an IP tunnel. GRE uses the IP protocol 47, the GRE header is structured as follows:

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

A GRE packet is therefore composed of an IP header, a GRE header and the actual payload. You can set up this GRE tunnel under **VPN > GRE Tunnels**.

System Network Services Firewall QoS VPN Tools Application Status

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

GRE Tunnels

Enable	Name	Local virtual IP	Peer Address	Remote virtual IP	Remote Subnet	Remote Netmask	Key	NAT	Description
<input checked="" type="checkbox"/>	tun0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	255.255.255.0		<input type="checkbox"/>	

Add

Apply Cancel

Name	Description	Default
Enable	Click to enable	Enabled
Tunnel Name	Set names for GRE tunnels	tun0
Local Virtual IP	Set local virtual IP	0.0.0.0
Peer Address	Set peer address	0.0.0.0
Remote Virtual IP	Set virtual IP of the remote network	0.0.0.0
Remote Subnet Address	Set remote subnet address	0.0.0.0
Remote Subnet Netmask	Set remote subnet mask	255.255.255.0
Key	Set the key for the encryption of the tunnel	Blank
NAT	Click to enable NAT function	Disabled
Description	Add description	Blank

9.4 L2TP Clients

Layer 2 Tunneling Protocol (L2TP) is a network protocol that tunnels frames of OSI model link layer protocols through routers between two networks over an IP network. L2TP routers and the IP connections between them appear as L2 switches. The L2TP client establishes the connection to the L2TP server here. You can reach the configuration via **VPN > L2TP Clients**.

System Network Services Firewall QoS VPN Tools Application Status

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

L2TP Clients

Name	Tunnel Description	Local IP Address	Remote IP Address	Tunnel Status	Conncted Time
<input type="button" value="Add"/>	<input type="button" value="Show Detail Status"/>				

5 Seconds Stop

Clicking on the **Add** button starts the configuration of the L2TP client.

Your password have security risk, please click here to change

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	Description	Default
Enable	Enables the tunnel settings	Enabled
Tunnel Name	Set name for tunnel	L2TP_TUNNEL_1
L2TP Server	Enter the address of the L2TP server	Blank
Username	Set username for server	Blank
Password	Set password for server	Blank
L2TP Server Name	Set name for server	l2tpserver
Startup Modes	Set modes for startup: "Auto Activated", "Triggered by Data", "Manually Activated", "L2TPo- verIPSec"	Auto Activated
Authentication Type	Set authentication type: "CHAP", "PAP"	CHAP
Enable Challenge Secrets	Select to enable secret keys (challenge)	Disabled
Challenge Secrets	If Enable Challenge Secrets is enabled, the secret key can be entered here	Blank
Local IP Address	Set local IP address	Blank
Remote IP Address	Set remote IP address	Blank
Remote Subnet	Set remote subnet	Blank
Remote Subnet Net-mask	Set remote subnet mask	255.255.255.0
Link Detection Interval	Set interval for link detection	60
Max Retries for Link Detection	Set maximum number of retries for link detection	5
Enable NAT	Click to enable NAT	Disabled
MTU	Set MTU parameters	1500
MRU	Set MRU parameters	1500
Enable Debug Mode	Click to enable debug mode	Disabled
Expert Options	Set expert options	Blank

9.5 PPTP Clients

PPTP (Point to Point Tunneling Protocol) is a VPN tunneling method for remote access connections. It is based on the Remote Access Server for Microsoft Windows NT including authentication. A PPTP client is integrated not only in Windows, but also in Linux and MacOS. Set up the PPTP client under **VPN > PPTP Clients**.

System
Network
Services
Firewall
QoS
VPN
Tools
Application
Status

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

PPTP Clients

Name	Tunnel Description	Local IP Address	Remote IP Address	Tunnel Status	Conncted Time
<button>Add</button>	<button>Show Detail Status</button>				

5 Seconds
Stop

To set up a new PPTP client, click on the **Add** button. To view details of an existing PPTP client, click the **Show Detail Status** button. When you have clicked the **Add** button, you can make the following configuration settings.

PPTP Clients**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="password"/>
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"/>

Save

Cancel

Name	Description	Default
Enable	Click to enable	Enabled
Tunnel Name	Tunnel Name (set automatically)	PPTP_tunnel_1
PPTP Server	Set address for PPTP server	Blank
Username	Set username for the server	Blank
Password	Set password for the server	Blank
Startup Mode:	Set modes for start “Auto Activated”, “Triggered by Data”, “Manually Activated	Auto Activated
Authentication Type	Set authentication type: “PAP”, “CHAP”, “MS-CHAPv1”, “MS-CHAPv2”	Auto
Local IP Address	Set local IP address	Blank
Remote IP Address	Set remote IP address	Blank
Remote Subnet	Set remote subnet	Blank
Remote Subnet Netmask	Set remote subnet mask	255.255.255.0
Link Detection Interval	Set interval for link detection	60
Max Retries for Link Detection	Set maximum number of retries for link detection	5
Enable NAT	Click to enable NAT	Blank
Enable MPPE	Click to enable MPPE (Microsoft Point to Point Encryption)	Blank
Enable MPPC	Click to enable MPPC (Microsoft Point to Point Compression)	Blank
MTU	Set MTU parameters	1500
MRU	Set MRU parameters	1500
Enable Debug Mode	Click to enable debug mode	Blank
Expert Options	Only for Welotec R&D	Blank

9.6 OpenVPN Tunnels

OpenVPN is a free software for setting up a Virtual Private Network (VPN) over an encrypted TLS connection. The OpenSSL library is used for encryption. OpenVPN uses either UDP or TCP for transport.

OpenVPN is licensed under the GNU GPL and supports operating systems such as Linux, Windows, iOS and a variety of customized Linux-based endpoints such as TK 500 and TK 800 series routers.

On the TK500 configuration page, select the **VPN > Open VPN Tunnels** options as shown below:

System Network Services Firewall QoS VPN Tools Application Status

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

OpenVPN Tunnels

Enable	Name	Tunnel Description	Tunnel Status	Conncted Time
Yes	OpenVPN_T_1	[router]===[192.168.2.12] Mode: Client Protocol: UDP: Port: 1194 192.168.3.0---192.168.2.0	Connected	0 day, 00:00:59
Add		Show Detail Status		

5 Seconds Stop

Click **Add** to add a new OpenVPN tunnel. With **Show Detail Status** you can view the status of an already configured OpenVPN tunnel.

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						
Local IP Address	192.168.3.0					
Remote IP Address	192.168.2.0					
Remote Subnet						
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						
Debug Level	Warn ▾					
Interface Type	TUN ▾					
Expert Options(Expert Only)						
<div> <div>Save</div> <div>Cancel</div> <div>Delete</div> </div>						

Name	Description
Tunnel name	Predefined
Enable	Enable this configuration
Mode	Select “Client” or “Server” mode
Protocol	Selection of the “UDP” or “TCP” protocol
Port	Default port for OpenVPN is 1194
OPENVPN Server	IP or DNS of the OpenVPN server
Authentication Type	Selection of the authentication type. Depending on the selection, different fields are available
Pre-shared Key	Set static password if Pre shared Key, shared key or TLS-AUTH is selected
Remote Subnet, Remote Netmask	Set static route of the router, always in the direction of the peer’s subnet
Username/Password	If User/Password is selected, the corresponding data is entered in these fields
Link Detection Interval, Link Detection Timeout	Always use default
Renegotiate Interval	Always use default
Enable NAT	Set NAT mode, in the meantime routing mode is disabled
Enable LZO	Enable LZO compression
Encryption Algorithms	Set encryption algorithm, must match server
MTU	Always use default, 1500
Max Fragment Size	Maximum size of individual packets
Debug Level	Selection of debug outputs in the log
Interface Type	TUN / TAP
Expert Options (Expert Only)	More OpenVPN commands (only for experienced users)

9.7 OpenVPN Advanced

This configuration page is only used for the OpenVPN server and provides advanced functions. You can reach this point via **VPN > OpenVPN Advanced**.

System Network Services Firewall QoS VPN Tools Application Status

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

OpenVPN Advanced

Enable Client-to-Client (Server Mode Only) ☐

Client Management

Enable	Tunnel name	Username/CommonName	Password	Client IP(4th byte must be 4n+1)	Local Static Route	Remote Static Route
<input checked="" type="checkbox"/>	OpenVPN_T_					

Add

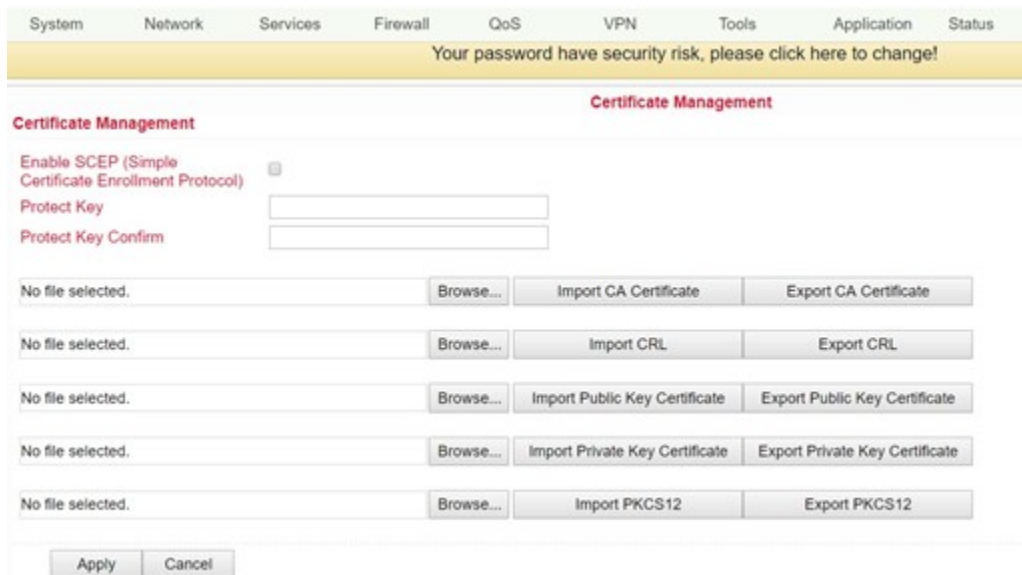
Apply Cancel

Name	Description
Enable Client-to-Client (Server Mode Only)	Enable client access to other clients
Client Management	
Enable	Enable the function
Tunnel Name	Tunnel name of the client
Username/Common Name	Username (using username/password mode) or common name in CA (CA mode)
Client IP	Specification of the client IP address
Local Static Route	Subnet of the client
Remote Static Route	Subnet of the server

CA can only be created from the customer's PC, not from TK500.

9.8 Certificate Management

Under the menu item *VPN > Certificate Management* you can include the certificates that you want to use for your VPN connections. You can also export already existing certificates.



The screenshot shows the 'Certificate Management' page in a web interface. At the top, there is a navigation bar with tabs: System, Network, Services, Firewall, QoS, VPN, Tools, Application, and Status. Below the navigation bar, a yellow banner displays the message: 'Your password have security risk, please click here to change!'. The main heading 'Certificate Management' is centered. Below the heading, there is a section for 'Enable SCEP (Simple Certificate Enrollment Protocol)' with a checkbox. Underneath, there are two input fields labeled 'Protect Key' and 'Protect Key Confirm'. The interface then lists five rows of file management options, each with a 'Browse...' button and two action buttons: 'Import CA Certificate', 'Export CA Certificate', 'Import CRL', 'Export CRL', 'Import Public Key Certificate', 'Export Public Key Certificate', 'Import Private Key Certificate', 'Export Private Key Certificate', and 'Import PKCS12', 'Export PKCS12'. At the bottom, there are 'Apply' and 'Cancel' buttons.

Name	Description	Default
Enable SCEP	Click to enable	
Protect Key	Set a key to protect the certificates	Blank
Protect Key Confirm	Confirm the key to protect the certificates	Blank
Import/Export CA Certificate	Import or export CA certificate	Blank
Import/Export Certificate (CRL)	Import or export CRL certificate	Blank
Import/Export Public Key Certificate	Import/export public key certificate	Blank
Import/Export Private Key Certificate	Import or export private key certificate	Blank
Import/Export PKCS12	Import or export PKCS12 (private key and X.509 certificate)	Blank
Browse	Via Browse the respective file is selected and can then be imported	No file selected

10 Tools

The tools are useful tools and include PING detection, trace route, connection speed tests, etc.

10.1 PING

Select the item *Tools > Ping* if you want to test if there is a connection to the network/Internet.

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	Description	Default
Host	Destination for PING	Blank
Ping Count	Set number of PINGs	4 Mal
Packet Size	Set packet size for PING	32 Byte
Expert Options	Advanced parameters	Blank

10.2 Traceroute

Traceroute (tracert) determines via which routers and Internet nodes the IP data packets reach the queried computer. You can enter the data under **Tools > Traceroute**.

System
Network
Services
Firewall
QoS
VPN
Tools
Application
Status

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

Traceroute

Host
8.8.8.8
Trace

Maximum Hops
20

Timeout
3
Seconds

Protocol
UDP

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	Description	Default
Host	Destination for Trace Route	Blank
Max Hops	Set maximum number of hops	20
Time Out	Set timeout	3 Seconds
Protocol	Optional: "ICMP"/"UDP"	UDP
Expert Options	Advanced parameters	Blank

10.3 Link Speed Test

Test the connection speed via upload or download. Please select this area via **"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.
Browse...
upload
download

Via the **Browse** button you can upload a corresponding file from the computer. The file should be between 10 and 2000MB in size. After selecting the file, click on the **Upload** button. The result will be displayed.

10.4 TCPDUMP

The TCPDUMP function reads data in the form of packets sent over the network and displays them on the screen or saves them to files.

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

11 Application

The menu item “*Application*” is currently not supported.

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"/>							
<div>Apply Cancel</div>								

12 Status

Under “**Status**” you get information about system, modem, network connections, routing table, device list and protocol.

12.1 System


Select from the menu **Status > System** to get information about your system.

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%)							

This page displays the status of the system, including information about the name, model type, current version, etc.

12.2 Modem

Check the status of your modem under **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							

Here you can view the status of the modem including the signal strength.

12.3 Traffic Statistics

If you want to view the data consumption of the SIM card in the TK500, then you can do this under **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						
<div>Clear</div>								

Here you can see the monthly, daily and hourly data that has been received or transmitted. Via the button “**Clear**” you can reset the entries to 0.

12.4 Alarm

Check the alarms generated by the TK500, for example created under 3.3.7. in the Alarm Manager. You can access this menu item under **Status > Alarm**.

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		
.....								
Clear All Alarms		Confirm All Alarms						

In this example the monthly limit of the SIM card has been reached. With the button “**Clear All Alarms**” you can delete all alarm messages and with “**Confirm All Alarms**” you confirm that you have taken note of the alarm.

12.5 WLAN

Via **Status > WLAN** you can view all WLAN networks that are in the reception range of the TK500. For this, the WLAN function must be activated in the TK500 (see 3.2.6).

System	Network	Services	Firewall	QoS	VPN	Tools	Status
WLAN							
Channel	SSID	BSSID	Security	Signal(%)	Mode	Status	
1	JD-PRO-Remote	0e:18:0a:9f:b0:47	WPA2PSK/AES	34	11b/g/n		
1	WeloLabor	00:18:0a:9f:b0:47	WPA2PSK/AES	39	11b/g/n		
<div> 3 Seconds Stop </div>							

12.6 Network Connections

Via **Status > Network Connections** you can get an overview of the network connections of the TK500.

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						
<div>RenewRelease</div>								
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						
<div>ConnectDisconnect</div>								
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						

Here you can see at a glance the network connections via WAN, dialup or LAN.

12.7 Route Table

If you want to have an overview of the routing table in the TK500, select **Status > Route Table** from the menu.

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				

After clicking on it, you will see the routing table of the 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						

Under the menu item **Status > Device List** all devices are displayed which are connected to the TK500.

Overview of the devices connected to the TK500.

12.9 Log

Documentation of the system events (logs) of the TK500. You reach this area under **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	openvpn[4015]	TUN/TAP device tun0 opened					
notice	Oct 1 16:29:12	openvpn[4015]	TUN/TAP TX queue length set to 100					
notice	Oct 1 16:29:12	openvpn[4015]	do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0					
notice	Oct 1 16:29:12	openvpn[4015]	/sbin/ifconfig tun0 192.168.3.0 pointopoint 192.168.2.0 mtu 1500					
notice	Oct 1 16:29:12	openvpn[4015]	/tmp/OpenVPN_T_1.up tun0 1500 1557 192.168.3.0 192.168.2.0 init					
info	Oct 1 16:29:12	openvpn-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	openvpn-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	openvpn-up[29129]	applying MAC-IP rules					
info	Oct 1 16:29:12	openvpn-up[29129]	stop_qoslimit:old interface name not get					
info	Oct 1 16:29:12	openvpn-up[29129]	ratelimit_enable is 0					
info	Oct 1 16:29:12	openvpn-up[29129]	firewall ACL does not exist for domain rules.					
info	Oct 1 16:29:12	openvpn-up[29129]	Clear connection table in openvpn up...					
notice	Oct 1 16:29:12	openvpn[4015]	UDPv4 link local: [undef]					
notice	Oct 1 16:29:12	openvpn[4015]	UDPv4 link remote: [AF_INET]192.168.2.12:1194					
info	Oct 1 16:29:12	udhcpd[460]	Sending discover...					
info	Oct 1 16:29:15	udhcpd[460]	Sending discover...					
			Clear Log	Download Log File	Download System Diagnosing Data			

This page displays the system log, which can be downloaded here.

It may occur that problems cannot be diagnosed and rectified immediately. In these cases, we ask you to send the diagnostic log to Welotec. To do this, click on “**Download System Diagnosing Data**”, and then send us the log with a description of the error to support@welotec.com

12.10 Third Party Software

Here are the software terms and licenses from all third party vendors related to the TK500 router series.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
<div>Third Party Software Notices</div> <p>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:</p> <p>Welotec GmbH, Zum Hagenbach 7, 48366 Laer, Germany</p> <p>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.</p> <hr/> <p>bridge-utils</p> <hr/> <p>V1.0.4</p> <p>Copyright (C) 2000 Lennert Buytenhek</p> <p>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.</p>								

13 Technical specifications

13.1 Device properties

Property	Value
Dimensions (W x H x D)	35 x 127 x 108,2 mm
Operating voltage	230 V AC to 12 V – 24 V DC
Approval	CE compliant

13.2 Environmental conditions

Property	Value
Operating temperature range	-15 to +70 °C
Air humidity	5 - 95 %, non condensing
Concussions	IEC 60068-2-27
Free fall	IEC 60068-2-32
Vibration	IEC 60068-2-6

13.3 Radio frequencies

13.3.1 Radio frequencies LTE Europe

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

13.3.2 Radio frequencies UMTS Europe

Fre- quency	Frequency range and transmission power	Router
Band 1	Frequency range Down: 2110 MHz – 2170 MHz Frequency range Up: 1920 MHz – 1980 MHz Max. transmission power: 251 mW	TK525U, TK525L, TK525L-W, TK525W
Band 8	Frequency range Down: 925 MHz – 960 MHz Frequency range Up: 880 MHz – 915 MHz Max. transmission power: 251 mW	TK525U, TK525L, TK525L-W, TK525W

13.3.3 Radio frequencies GSM Europe

Fre- quency	Frequency range and transmission power	Router
GSM 900	Frequency range Down: 925 MHz – 960 MHz Frequency range Up: 880 MHz – 915 MHz Max. transmission power: 1995 mW	TK525U, TK525L, TK525L-W, TK525W
GSM 1800	Frequency range Down: 1805 MHz – 1880 MHz Frequency range Up: 1710 MHz – 1785 MHz Max. transmission power: 40 mW	TK525U, TK525L, TK525L-W, TK525W

13.3.4 Radio frequencies LTE Asia

Fre- quency	Frequency range and transmission power	Router
Band 1	Frequency range Down: 1920 MHz – 1980 MHz Frequency range Up: 2110 MHz – 2170 MHz Max. transmission power: 200 mW	TK525U, TK525L, TK525L-W, TK525W
Band 3	Frequency range Down: 1805 MHz – 1880 MHz Frequency range Up: 1710 MHz – 1785 MHz Max. transmission power: 200 mW	TK525U, TK525L, TK525L-W, TK525W
Band 7	Frequency range Down: 2620 MHz – 2690 MHz Frequency range Up: 2500 MHz – 2570 MHz Max. transmission power: 200 mW	TK525U, TK525L, TK525L-W, TK525W
Band 38 China	Frequency range Down: 2570 MHz – 2620 MHz Frequency range Up: n.b. Max. transmission power: 200 mW	TK525U, TK525L, TK525L-W, TK525W
Band 40 China	Frequency range Down: 2300 MHz – 2400 MHz Frequency range Up: n.b. Max. transmission power: 200 mW	TK525U, TK525L, TK525L-W, TK525W
Band 41 China	Frequency range Down: 2496 MHz – 2690 MHz Frequency range Up: n.b. Max. transmission power: 200 mW	TK525U, TK525L, TK525L-W, TK525W

13.4 Radio frequencies UMTS Asia

Fre- quency	Frequency range and transmission power	Router
Band 1	Frequency range Down: 2110 MHz – 2170 MHz Frequency range Up: 1920 MHz – 1980 MHz Max. transmission power: 251 mW	TK525U, TK525L, TK525L-W, TK525W
Band 8	Frequency range Down: 925 MHz – 960 MHz Frequency range Up: 880 MHz – 915 MHz Max. transmission power: 251 mW	TK525U, TK525L, TK525L-W, TK525W

13.4.1 Radio frequencies GSM Asia

Fre- quency	Frequency range and transmission power	Router
GSM 900	Frequency range Down: 925 MHz – 960 MHz Frequency range Up: 880 MHz – 915 MHz Max. transmission power: 1995 mW	TK525U, TK525L, TK525L-W, TK525W
GSM 1800	Frequency range Down: 1805 MHz – 1880 MHz Frequency range Up: 1710 MHz – 1785 MHz Max. transmission power: 1000 mW	TK525U, TK525L, TK525L-W, TK525W

13.4.2 Radio frequencies UMTS Global

Fre- quency	Frequency range and transmission power	Router
Band 1	Frequency range Down: 2110 MHz – 2170 MHz Frequency range Up: 1920 MHz – 1980 MHz Max. transmission power: 251 mW	TK525U, TK525L, TK525L-W, TK525W
Band 8	Frequency range Down: 925 MHz – 960 MHz Frequency range Up: 880 MHz – 915 MHz Max. transmission power: 251 mW	TK525U, TK525L, TK525L-W, TK525W

13.4.3 Radio frequencies GSM Global

Fre- quency	Frequency range and transmission power	Router
GSM 850	Frequency range Down: 869 MHz – 894 MHz Frequency range Up: 824 MHz – 849 MHz Max. transmission power: 1995 mW	TK525U, TK525L, TK525L-W, TK525W
GSM 1900	Frequency range Down: 1930 MHz – 1990 MHz Frequency range Up: 1850 MHz – 1910 MHz Max. transmission power: 1000 mW	TK525U, TK525L, TK525L-W, TK525W

13.4.4 Radio frequencies WLAN

Frequency	Frequency range and transmission power	Router
2,4 GHz	Frequency range: 2400 MHz – 2483,5 MHz Max. transmission power: 40 mW	TK525L-W

14 Support

In case of problems with installation and operation, send an e-mail to the following address: support@welotec.com