

welotec®

TK500 ROUTER SERIES MANUAL

Version 2.1.1



welotec®

Welotec GmbH
Zum Hagenbach 7, D-48366 Laer
T: +49 (0)2554/9130-00
F: +49 (0)2554/9130-10
info@welotec.com

www.welotec.com

TABLE OF CONTENTS

1.	TK500-Series - Introduction	4
1.1.	Package checklist	6
1.2.	Product information	7
1.2.1.	Environmental conditions.....	7
1.2.2.	Power supply.....	7
1.2.3.	Physical characteristics	7
2.	Installation manual	8
2.1.	Typical application.....	8
2.2.	Connection plan.....	8
2.2.1.	Connection of serial interfaces and I/O's.....	8
2.3.	Fast internet connection	10
2.3.1.	Insert the SIM card	10
2.3.2.	Installation of the antenna.....	10
2.3.3.	Power supply.....	10
2.3.4.	Connect	10
2.3.5.	First connecting of the TK-Router device to the PC	10
2.3.6.	Configuring the TK500 (optional).....	13
2.3.7.	Connect the TK router with the Internet.....	15
2.4.	Reset to factory settings.....	17
2.4.1.	Hardware method	17
2.4.2.	Web method	18
3.	System	19
3.1.	System.....	21
3.1.1.	Basic Setup.....	21
3.1.2.	Time	22
3.1.3.	Serial Port.....	23
3.1.4.	Admin Access.....	23
3.1.5.	System Log.....	24
3.1.6.	Config Management	25
3.1.7.	Scheduler	25
3.1.8.	Upgrade	26
3.1.9.	Reboot	27
3.1.10.	Logout.....	27
3.2.	Network.....	28
3.2.1.	Dialup.....	28
3.2.1.1.	Schedule Management	30
3.2.2.	WAN (only for TK5x5L-W, TK5x5L, TK5x5U)	31
3.2.2.1.	Static IP	31
3.2.2.2.	Dynamic Address (DHCP).....	32
3.2.2.3.	ADSL Dialup (PPPoE).....	33
3.2.3.	WAN(STA)	34
3.2.4.	Link Backup	34
3.2.5.	LAN	35
3.2.6.	Switch WLAN Mode.....	36
3.2.7.	WLAN.....	36
3.2.7.1.	WLAN Client	38
3.2.8.	DNS	38
3.2.9.	DDNS (Dynamic DNS).....	39
3.2.10.	Static Route	41
3.3.	Services	42
3.3.1.	DHCP Service.....	42
3.3.2.	DNS Relay	43
3.3.3.	VRRP	43
3.3.4.	DTU	45
3.3.5.	SMS	46
3.3.6.	Traffic Manager	47

3.3.7.	Alarm Manager	48
3.4.	Firewall	49
3.4.1.	Basic	49
3.4.2.	Filtering	49
3.4.3.	Content Filtering	50
3.4.4.	Port Mapping	51
3.4.5.	Virtual IP Mapping.....	51
3.4.6.	DMZ	52
3.4.7.	MAC-IP Bundling	53
3.5.	QoS	54
3.5.1.	Bandwidth Control	54
3.5.2.	IP BW Limit.....	54
3.6.	VPN	56
3.6.1.	IPSec Settings.....	56
3.6.2.	IPSec Tunnels	57
3.6.3.	GRE Tunnels	60
3.6.4.	L2TP Clients	61
3.6.5.	PPTP Clients	62
3.6.6.	OpenVPN Tunnels.....	64
3.6.7.	OpenVPN Advanced.....	65
3.6.8.	Certificate Management	66
3.7.	Tools	68
3.7.1.	PING	68
3.7.2.	Traceroute	69
3.7.3.	Link Speed Test	69
3.8.	Application	70
3.8.1.	Smart ATM	70
3.9.	Status	71
3.9.1.	System.....	71
3.9.2.	Modem.....	71
3.9.3.	Traffic Statistics.....	72
3.9.4.	Alarm.....	72
3.9.5.	WLAN.....	72
3.9.6.	Network Connections	73
3.9.7.	Route Table	73
3.9.8.	Device List.....	74
3.9.9.	Log	74
3.9.10.	Third Party Software Notices.....	75
4.	Technical Data	76
4.1.	Device characteristics.....	76
4.2.	Enviromental characteristics.....	76
4.3.	Radio frequencies.....	76
4.3.1.	Radio frequencies 4G LTE Europe	76
4.3.2.	Radio frequencies 3G UMTS Europa.....	77
4.3.3.	Radio frequencies 2G GSM Europe	77
4.3.4.	Radio frequencies 4G LTE Asia	77
4.3.5.	Radio frequencies 3G UMTS Asia	78
4.3.6.	Radio frequencies 2G GSM Asia	78
4.3.7.	Radio frequencies 3G UMTS global.....	78
4.3.8.	Radio frequencies 2G GSM global.....	78
4.3.9.	Radio frequencies WLAN	79
5.	Support	80
6.	CE declaration	81

1. TK500-SERIES - INTRODUCTION

Note on Copyright

Copyright © 2018 Welotec GmbH

All rights reserved.

Reproduction without permission is prohibited.

Brands

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

Legal notice

The information in this document is subject to change without notice and is not binding for Welotec GmbH. This manual may contain technical or typographical errors. Corrections are made regularly without being mentioned in new versions.

Contact information for technical support

Welotec GmbH

Zum Hagenbach 7

D-48366 Laer

Phone: +49 2554 9130 00

Fax: +49 2554 9130 10

Email: support@welotec.com

Description

The TK500 industrial routers provide a stable, high-speed connection between remote devices and customer locations over LAN and (depending on the model) over Wi-Fi or 2G / 3G / 4G networks. They can be used in a voltage range of 12 to 24 V DC and have a temperature range of -15 °C to +70 °C with a relative humidity of 95%, which ensures high stability and reliability under severe conditions. The TK500 can be used on the workplace or mounted on DIN rails.

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

Important safety instructions

This product is not suitable for the following applications

- areas where no wireless applications (such as mobile phones) are allowed
- hospitals and other places where the use of mobile phones is not permitted
- petrol stations, fuel depots and places where chemicals are stored
- chemical plants or other places with a explosion hazard
- metal surfaces which can weaken the radio signal level

Warning

This is a class A product. In living areas, the use of this equipment can lead to radio interference, which the user must remedy with appropriate measures.

WEEE notice

The European Directive on the Disposal of Waste Electrical and Electronic Equipment (WEEE), which entered into force on 13 February 2003, has led to major changes in the reuse and recycling of electrical equipment. The main objective of this Directive is the prevention of waste electrical and electronic equipment and the promotion of re-use, recycling and other forms of recycling. The WEEE logo on the product or packaging indicates that the product must not be disposed of in normal household waste. It is your responsibility to dispose of all used electrical and electronic equipment at appropriate collection points. Separate collection and sensible recycling of your electronic waste helps to conserve natural resources. In addition, proper recycling of waste electrical and electronic equipment ensures human health and environmental protection.



For further information on disposal, recycling and collection points for electrical and electronic equipment, please contact your local city office, waste disposal service, or the device's distributor or manufacturer.

1.1. Package checklist

Each TK500 wireless router comes bundled with standard accessories. Additional accessories can be ordered. Carefully check the contents of your package, and if something is missing or damaged, contact your distributor from Welotec GmbH.

Delivery:

Standard equipment:

Equipment	Amount	Description
TK500 router	1	TK500 series industrial router
Network cable	1	Network cable CAT5, 1.5 meter
Manual	1	Disk with manual
License conditions	1	“Third Party Software Notifications and Licenses”
Power supply		
Terminal block	1	7-pin terminal for power supply

Components Set (depending on model)

Product	Amount	Description
TK500 router	1	TK500 series industrial router
Network cable	1	Network cable CAT5, 1.5 meter
Cellular antenna	1	5 m magnetic base antenna (TK515L, TK515L-W, TK505U) 2G/3G
Wi-Fi antenna	2	Plug-on antenna (Wi-Fi) (TK515L-W)
Manual	1	Disk with manual
License conditions	1	“Third Party Software Notification and Licenses”
		Power supply
		Desktop power supply, input 100-240 V AC, output 12 V DC (for TK5xx), incl. 7-pin terminal block
	1	Plug, european standard

1.2. Product information

1.2.1. Environmental conditions

Operating temperature: -15°C to +70°C

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

Storage temperature: -40°C to +85°C

1.2.2. Power supply

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

Input voltage: 12 - 24 V DC

1.2.3. Physical characteristics

Housing: steel, protection class IP30

Weight: 450 g

Dimensions (mm): 35 x 127 x 108.2 mm

2. INSTALLATION MANUAL

2.1. Typical application

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

2.2. Connection plan

Interface	Description
Power supply	12-24 V DC
Serial	Serial Interface
Ethernet ports	Five 10/100Base-TX RJ45 ports
Antenna connection (cellular)	SMA (f)
Antenna connection (Wi-Fi)	SMA-R (f)
SIM card slot	Slot for inserting the SIM card (TK525L-W, TK525L, TK525U)

2.2.1. Connection of serial interfaces and I/O's

Description of LED lights



= LED on



= LED off



= LED flashing

Legend: glows: on-- glows not: off-- flashes: flashing--

Signal	On	Off	Flashing
Turn on	PWR, STATUS, WARN	ERR	
Execution of firmware	PWR, WARN	ERR	STATUS
Dial-up to Internet	PWR	ERR	STATUS, WARN
Establish connection	PWR	WARN, ERR	STATUS
Firmware update	PWR		STATUS, WARN, ERR
Factory reset	PWR	WARN	STATUS, ERR

Description of LED signal



Signal: 1-9
(bad signal, the router cannot operate properly. Please check the antenna connection and the local signal strength of the mobile network.)



Signal: 10-19
(router is operating normally)



Signal: 20-31
(perfect signal level)

2.3. Fast internet connection

2.3.1. Insert the SIM card

Open the TK-Router SIM / UIM tray at the top of the device and insert the SIM card into the card carrier.

2.3.2. Installation of the antenna

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



Position and angle can affect signal strength.

2.3.3. Power supply

Connect the supplied power supply to the unit, and make sure that the Power LED is on. Contact Welotec Technical Support if no indicator lights up. You can configure the TK500 when the power indicator is flashing.

2.3.4. Connect

Connect the TK500 with your PC:

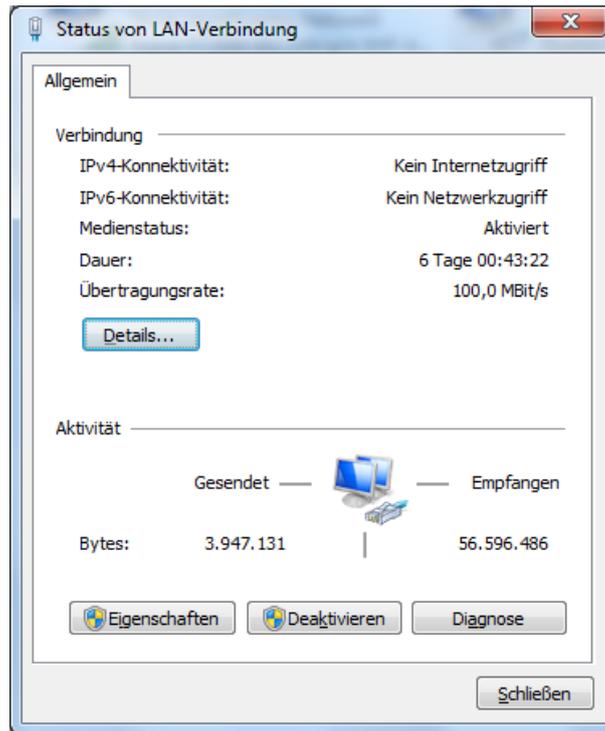
- 1) Connect the Ethernet cable of the TK500 to the PC.
- 2) Then an LED indicator of the RJ45 interface lights up in green and the other displays are flashing.

2.3.5. First connecting of the TK-Router device to the PC

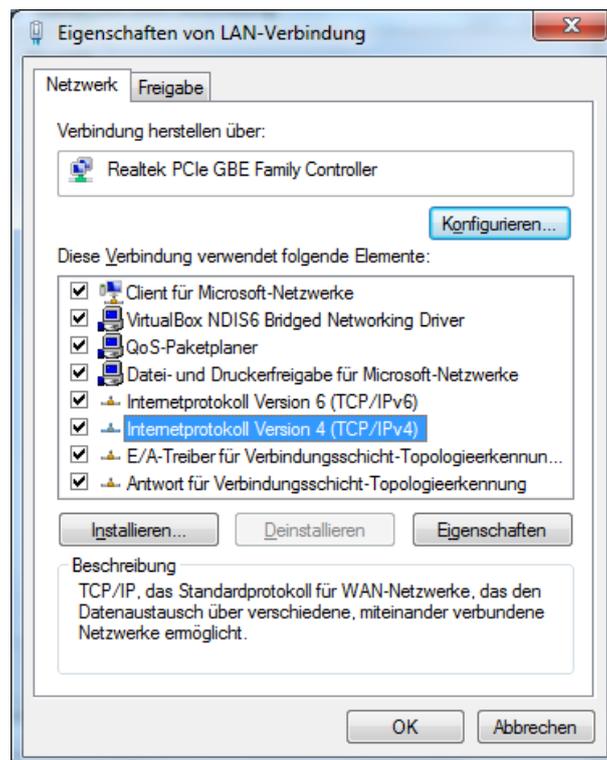
The TK500 router can automatically assign IP addresses for the PC. Set up the PC so that IP addresses are automatically retrieved via DHCP. (Based on the Windows operating system):

- 1) Open the Control Panel, double-click the „**Network and Sharing Center**“ icon to open the „**Network and Sharing Center**“ screen.

- 2) Click on „**LAN connection**“ and open the screen with the “**Status of LAN connection**“:

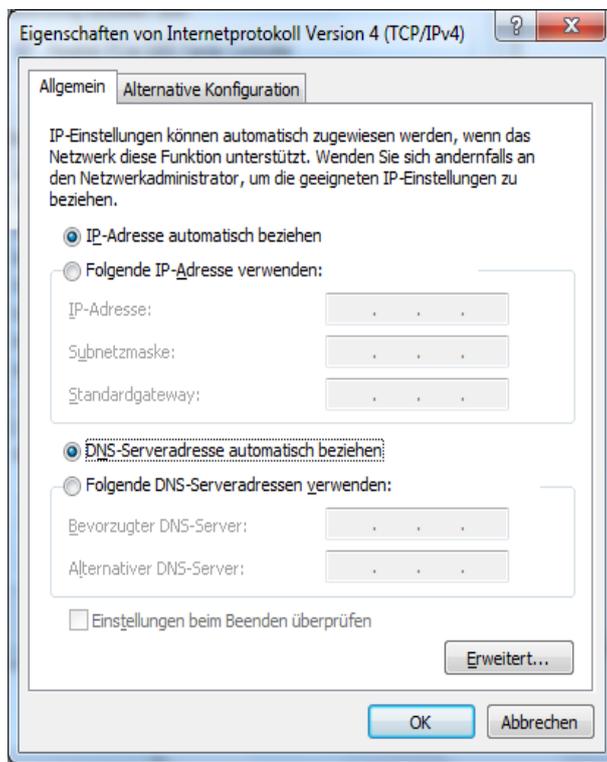


- 3) Click on „**Properties**“ and open the LAN connection properties screen:



- 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, eg IP: 192.168.2.10, Netmask: 255.255.255.0, Default Gateway: 192.168.2.1)

Clicking on „**OK**“ the TK router assigns the PC an IP address: 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 correctly. Here is an example of running the ping command on Windows 7:

Windows-Key+R -> Input "cmd" -> Enter key -> Input "Ping 192.168.2.1" -> Enter with this display:

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

C:\Users\ [redacted] >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\ [redacted] >_
```

The connection between PC and router has been set up correctly.

The following example has 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-Statistik für 192.168.2.1:
    Pakete: Gesendet = 4, Empfangen = 0, Verloren = 4
    (100% Verlust),

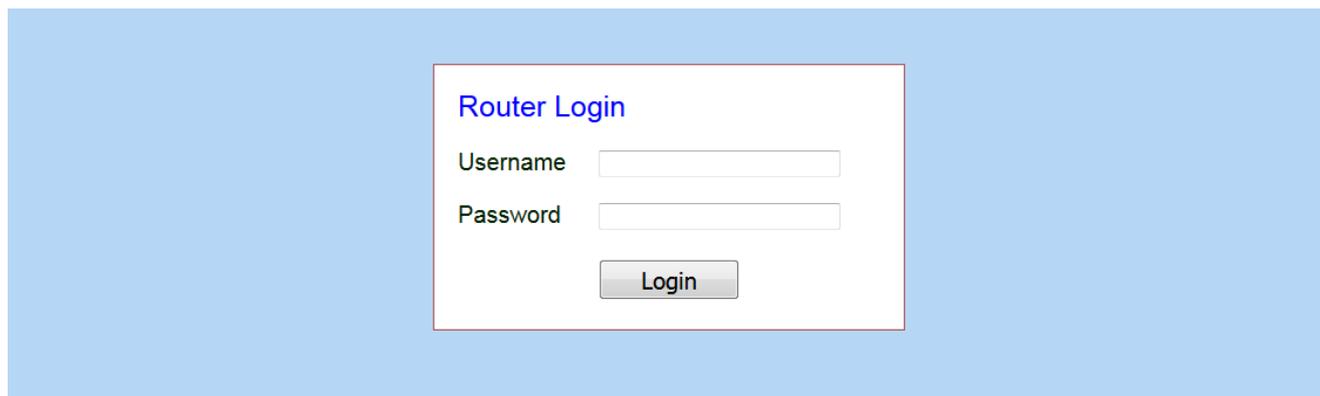
C:\Users\ >_
```

The connection is not working properly and you should review the instructions and improve your settings.

2.3.6. Configuring the TK500 (optional)

After completing the steps in the previous chapter, you can configure the router:

- 1) Open any internet browser (such as Google Chrome) and enter the default IP address of the router: **http://192.168.2.1**. The following login page opens:



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

2) Change the IP configuration:

! Note

After configuring, click „**Apply**“ to activate the 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	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								

Click on **Network > LAN**. Change the IP address in **192.168.1.254**:

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
LAN								
Type	Static IP <input type="button" value="Default"/>							
MAC Address	00:18:05:0C:C3:9C <input type="button" value="Default"/>							
IP Address	<input type="text" value="192.168.2.1"/>							
Netmask	<input type="text" value="255.255.255.0"/>							
MTU	Default <input type="text" value="1500"/>							
LAN Mode	Auto Negotiation <input type="button" value="Default"/>							
Multi-IP Settings								
IP Address	Netmask	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"/>								

3) Click on „**Apply**“, and you will see the following:



The IP address of the TK500 has been changed. In order 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.

2.3.7. Connect the TK router with the Internet

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

Click on **Network > Dialup** and activate **Enable**:

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
Dialup								
Enable	<input checked="" type="checkbox"/>							
Time schedule	ALL ▾	Schedule Management						
Shared Connection(NAT)	<input checked="" type="checkbox"/>							
Default Route	<input checked="" type="checkbox"/>							
Network Provider (ISP)	Custom ▾	Manage						
APN	internet.t-d1.de							
Access Number	*99***1#							
Username	tm							
Password	..							
Network Select Type	Auto ▾							
Connection Mode	Always Online ▾							
Redial Interval	30	Seconds						
Show Advanced Options	<input type="checkbox"/>							
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

Check the entries for APN, dial-in number, username and password: You will receive the dial-in number, username and password from your local network provider. Inquire about the details there.

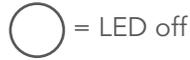
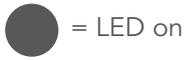
Show Advanced Options allows you to make additional settings, such as the PIN code if this is set on the SIM card.

Show Advanced Options	<input checked="" type="checkbox"/>	
PIN Code	<input type="text"/>	
MTU	<input type="text" value="1500"/>	
Authentication Type	<input type="text" value="Auto"/>	
Use Peer DNS	<input checked="" type="checkbox"/>	
Link Detection Interval	<input type="text" value="55"/>	Seconds(0: disable)
Debug	<input type="checkbox"/>	
Debug Modem	<input type="checkbox"/>	
ICMP Detection Mode	<input type="text" value="Ignore Traffic"/>	
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="5"/>	

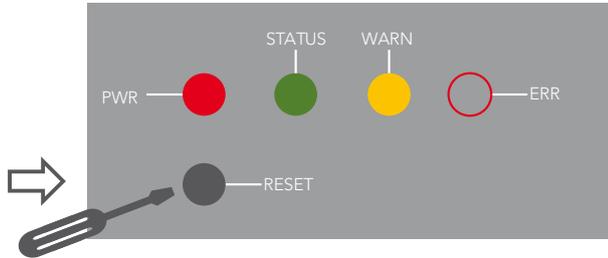
Once you have set the correct configuration, the TK500 can now connect to the Internet. Open an Internet browser, enter „www.welotec.com“ and the Welotec website will open.

2.4. Reset to factory settings

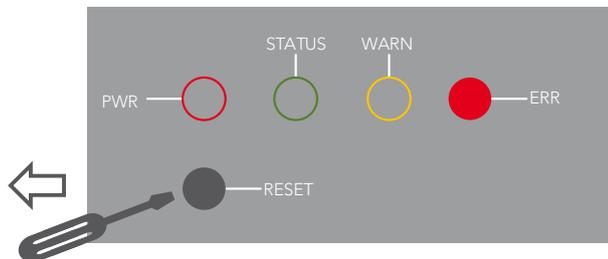
2.4.1. Hardware method



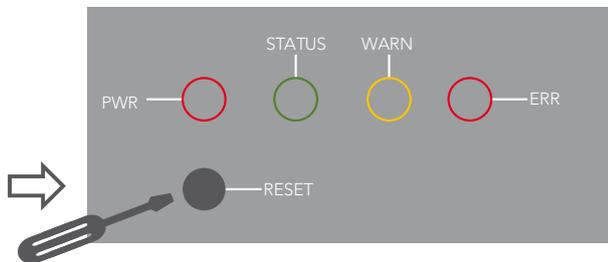
- 1) Press the **RESET button** while turning on the TK500:



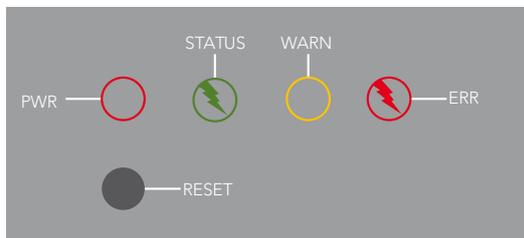
- 2) As soon as the ERROR LED lights (about 10 seconds after switching on), release the **RESET button**:



- 3) After a few seconds, the ERROR LED light stops lighting. Now press the **RESET button** again:



- 4) The ERROR and STATUS LED will flash, indicating that 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

2.4.2. Web method

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

The screenshot shows the web-based UI of the TK500 router. At the top, there is a navigation menu with tabs: System, Network, Services, Firewall, QoS, VPN, Tools, Application, and Status. Below the menu, a yellow warning banner reads: "Your password have security risk, please click here to change!". The main content area is titled "Config Management" and contains two sections: "Router Configuration" and "Network Provider (ISP)". Each section has a text input field with "No file selected.", a "Browse..." button, and "Import" and "Backup" buttons. The "Router Configuration" section also includes a "Restore default configuration" button.

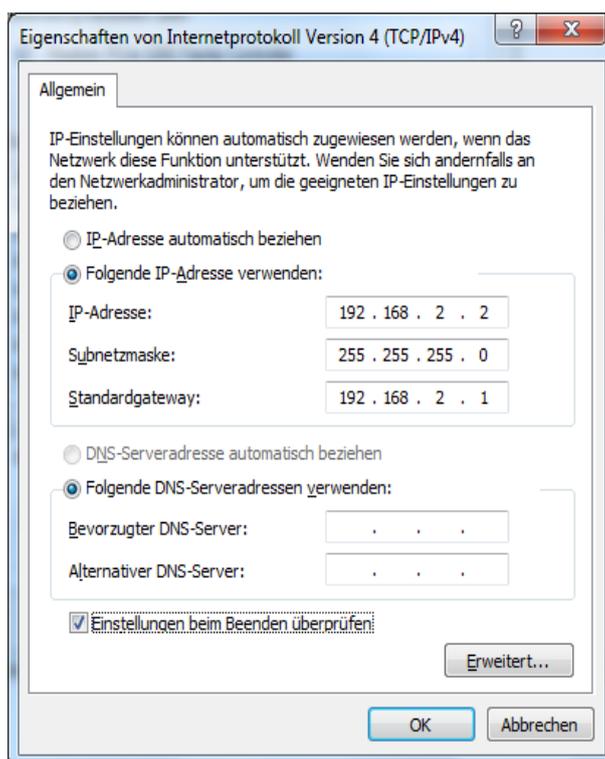
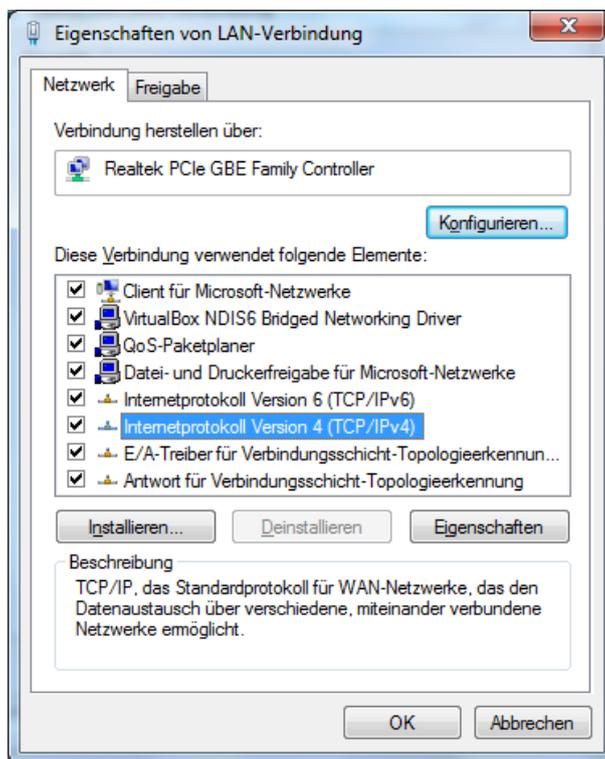
2.) Click **Restore default configuration** to reset the TK500 to its factory defaults. Then the router is re-booted.

3. SYSTEM

Before using the TK500 router it must be properly configured. This chapter describes the web-based configuration.

Preparation

First connect your devices to the TK500 via cable or hub (switch) and set the IP address for the PC and TK500 on the same subnet, for example: set the PC IP address to 192.168.2.2, Netmask: **255.255.255.0**, Gateway (default IP of the 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 username and password (default: **adm/123456**).

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								
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%)							

3.1. System

The system settings include the following nine sections: 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	

3.1.1. Basic Setup

In the Basic Setup you can adjust the voice guidance of the menu as well as 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		<input type="text" value="English"/>						
Hostname		<input type="text" value="Router"/>						
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

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

3.1.2. Time

This menu item allows you to adjust the system time of the router. Furthermore, it is 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 Time	2018-10-01 14:05:36							
PC Time	2018-10-01 14:05:37		<input type="button" value="Sync Time"/>					
Timezone	UTC+01:00 France, Germany, Italy ▼							
Auto Daylight Savings Time	<input checked="" type="checkbox"/>							
Auto Update Time	Every 1 hour ▼							
Trigger Connect On Demand	<input type="checkbox"/>							
NTP Time Servers	0.de.pool.ntp.org							
	1.de.pool.ntp.org							
	2.de.pool.ntp.org							
			<input type="button" value="Apply"/> <input type="button" value="Cancel"/>					

Name	Description	Standard
Router Time	Time of the router	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 synchronizes the time with the connected device
Time zone	Set time zone	selectable time zone
Auto Daylight Savings Time	Automatic change summer time / winter time	disabled
Auto Update Time	Time of automatic time update	disabled
NTP Time Servers (after activating the „Auto Update Time“ option)	Setting for NTP time server. (maximum three entries)	pool.ntp.org

3.1.3. Serial Port

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

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

Name	Description	Standard
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

3.1.4. Admin Access

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

Admin Access						
Username / Password						
Username	adm					
Old Password	<input type="text"/>					
New Password	<input type="text"/>					
Confirm New Password	<input type="text"/>					
Management						
Enable	Service Type	Service Port	Local access	Remote access	Allowed addresses from WAN (Optional)	Description
<input checked="" type="checkbox"/>	HTTP	80	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	HTTPS	443	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input checked="" type="checkbox"/>	TELNET	23	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	SSHD	22	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input checked="" type="checkbox"/>	Console					<input type="text"/>
Non-privileged users						
Username	Password					
<input type="text"/>	<input type="text"/>					
Other Parameters						
Login timeout	500	Seconds				
			<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

Name	Description	Standard
Username/Password		
Username	Username for login to the configuration page	adm
Old Password	Changing the password requires entering the old password	123456
New Password	Enter new password	
Confirm New Password	Enter new password again	
Management		
HTTP/HTTPS/TELNET/SSHD/Console		
Enable	Select to activate	enabled
Service Type	HTTP/HTTPS/TELNET/SSHD/Console	80/443/23/22/Blank
Local Access	Enabled - Allow router to be managed over LAN (eg: HTTP)	enabled
Remote Access	Enabled - Allow the TK500 to be managed over WAN (for example: HTTP)	enabled
Allowed addresses from WAN (Optional)	Sets the range of allowed IP addresses for WAN	Control Services servers can be set, such as 192.168.2.1/30 or 192.168.2.1
Description	Describe management parameters (without affecting the TK500)	
Non-privileged users		
Username	Create user name without administrator rights	
Password	Create password for users without administrator rights	
Other parameter		
Login Timeout	Set log timeout, after this value connection with the configuration page is disconnected and you have to log in again	500 seconds

3.1.5. 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)		<input type="text" value="192.168.2.254"/>		<input type="text" value=":514"/>				
Log to Console		<input type="checkbox"/>						
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

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

3.1.6. Config Management

Backing up and importing router configurations, as well as reverting to the factory settings of the router and saving or restoring the provider data. You can select this menu item under **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 enable the default configuration, the TK500 must be restarted.)
Network Provider (ISP)	To import or save APN, username, password and other parameters from conventional operators
Durchsuchen	With the Browse button you can select the file with the settings that should be uploaded via Import

3.1.7. Scheduler

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

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

Apply		Cancel						

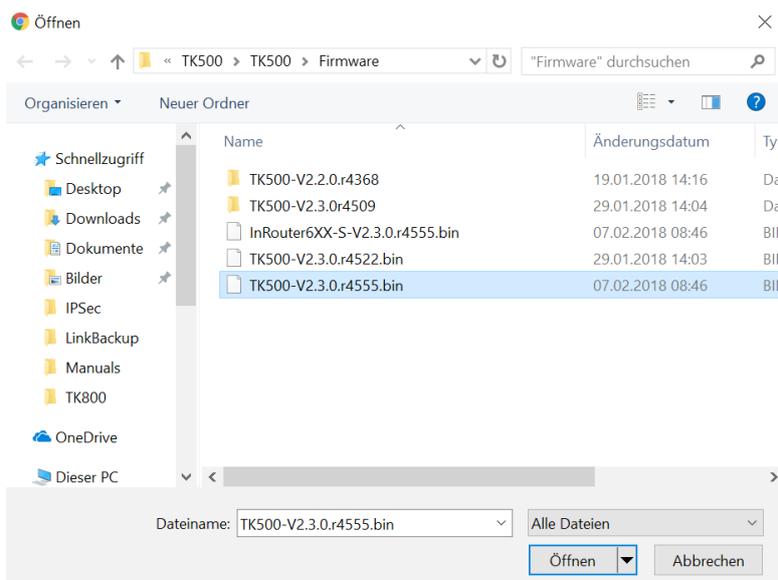
Name	Description
Enable	Turn the auto reboot on or off
Time	Time at which the TK500 router should be rebooted
Days	Selection Everyday for the daily restart

3.1.8. Upgrade

In this area, the router provides an interface for updating the firmware. Select **System > Upgrade**.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
Upgrade								
<p>Select the file to use:</p> <p>No file selected. <input type="button" value="Browse..."/> <input type="button" value="Upgrade"/></p> <p>Current Version : 2.3.0.r4648 Current Bootloader Version : 1.1.3.r4560</p>								

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



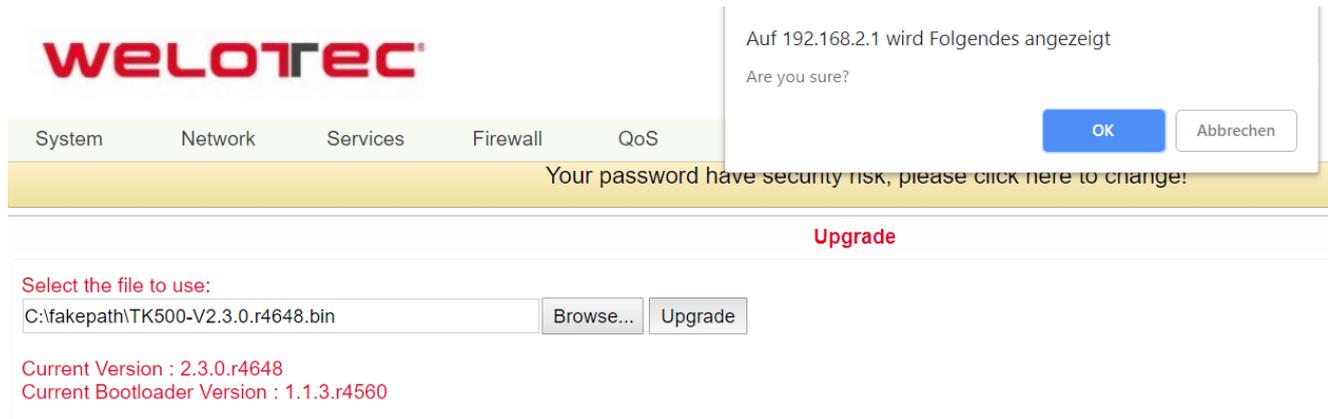
Click on the „**Upgrade**“ button and confirm the start of the update

Upgrading firmware...
It will take about 1-5 minutes depending on network. Please wait and don't interrupt!

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

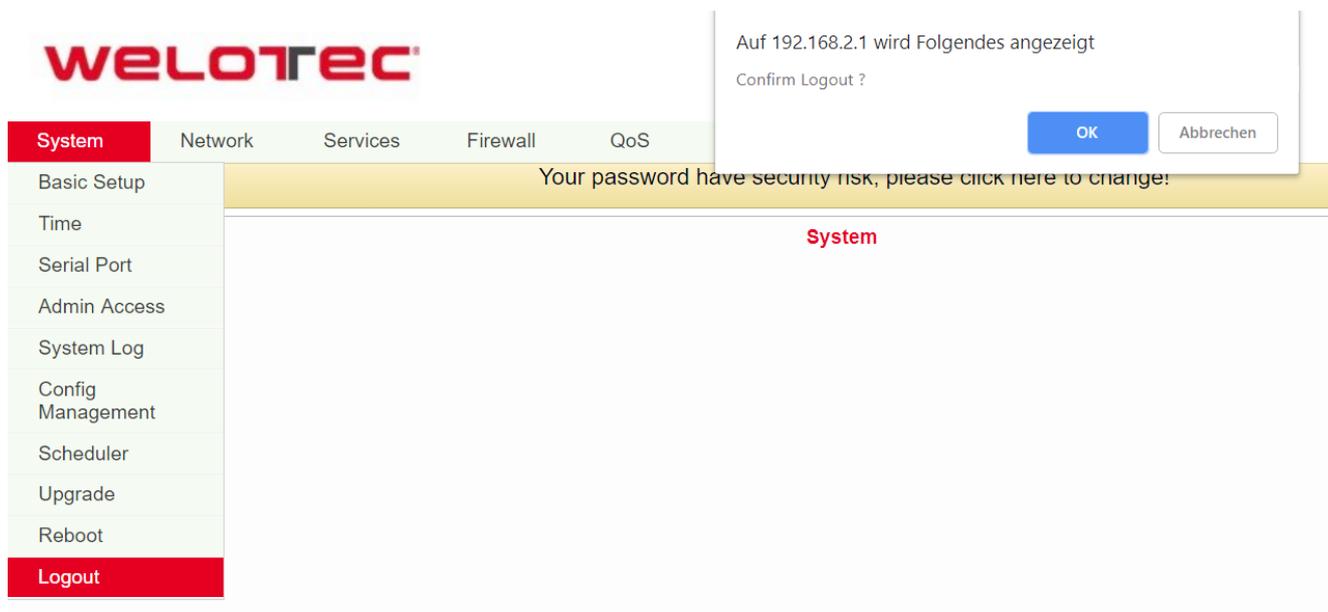
3.1.9. Reboot

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



3.1.10. Logout

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



3.2. Network

Network settings allow you to configure Dial-up, WAN, Link Backup, LAN, WLAN, DNS, DDNS, Static route, etc.

3.2.1. Dialup

In this menu area, you define and configure the dial-in of your router. Select **Network > Dialup**.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
Dialup								
Enable	<input checked="" type="checkbox"/>							
Time schedule	ALL ▾	Schedule Management						
Shared Connection(NAT)	<input checked="" type="checkbox"/>							
Default Route	<input checked="" type="checkbox"/>							
Network Provider (ISP)	Custom ▾	Manage						
APN	<input type="text" value="internet.t-d1.de"/>							
Access Number	<input type="text" value="*99**1#"/>							
Username	<input type="text" value="tm"/>							
Password	<input type="password" value="**"/>							
Network Select Type	Auto ▾							
Connection Mode	Always Online ▾							
Redial Interval	30	Seconds						
Show Advanced Options	<input checked="" type="checkbox"/>							
Initial Commands	<input type="text" value="AT"/>							
PIN Code	<input type="text"/>							
MTU	<input type="text" value="1500"/>							
Authentication Type	Auto ▾							
Use Peer DNS	<input checked="" type="checkbox"/>							
Link Detection Interval	55	Seconds(0: disable)						
Debug	<input type="checkbox"/>							
Debug Modem	<input type="checkbox"/>							
ICMP Detection Mode	Ignore Traffic ▾							
ICMP Detection Server	<input type="text"/>							
ICMP Detection Interval	30	Seconds						
ICMP Detection Timeout	20	Seconds						
ICMP Detection Retries	5							
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

Name	Description	Standard
Enable	Enables 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 interface as a standard route to the Internet	enabled
Network Provider (ISP)	Select Local ISP, if not listed here, select "Custom "	Custom
APN	APN parameter supplied by the provider	internet.t-d1.de (Telekom)
Access Number	Dial-in 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 dialing fails, the TK router will dial again after this interval	30 seconds
Show Advanced Options	Allows you to configure advanced options	disabled
PIN Code	Field for the PIN number of the SIM card	empty
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 discovery; empty field means there is none	empty
ICMP Detection Interval	Set interval for ICMP detection	30 seconds
ICMP Detection Timeout	Set timeout for ICMP discovery (TK500 is restarted on ICMP timeout)	20 seconds
ICMP Detection Retries	Set the maximum number of retries if ICMP fails	5

3.2.1.1. Schedule Management

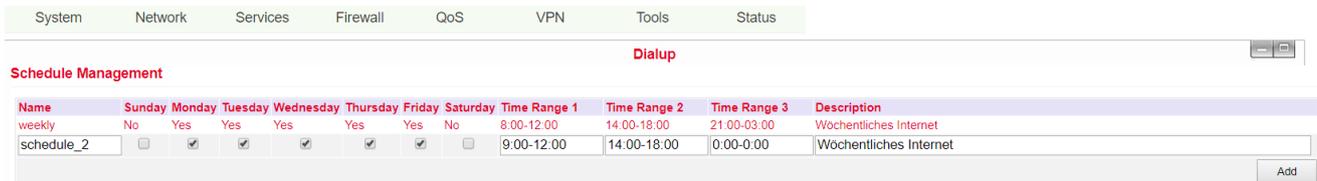
Schedule management (next to *"Time schedule"*):

Enable

Time schedule

 ALL ▾ Schedule Management

Here you can run your own dialup strategy, which means that you can specify over three time periods here when the router should be online.



Name	Description	Standard
Name	Name for time schedule	Schedule_1
Sunday	Sunday	empty
Monday	Monday	enabled
Tuesday	Tuesday	enabled
Wednesday	Wednesday	enabled
Thursday	Thursday	enabled
Friday	Friday	enabled
Saturday	Saturday	empty
Time Range 1	Set Time Range 1	9:00-12:00 a.m.
Time Range 2	Set Time Range 2	02:00-06:00 p.m.
Time Range 3	Set Time Range 3	0:00-0:00
Description	Describe the configuration	empty

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

3.2.2. WAN (only for TK5x5L-W, TK5x5L, TK5x5U)

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

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
WAN								
Type	<div style="border: 1px solid black; padding: 2px;"> Dynamic Address (DHCP) ▾ Static IP Dynamic Address (DHCP) ADSL Dialup (PPPoE) Disabled </div>							
Shared Connection(NAT)	<input type="checkbox"/>							
Default Route	<input type="checkbox"/>							
MAC Address	<input type="text" value="00:18:05:0C:C3:9B"/> <input type="button" value="Default"/> <input type="button" value="Clone"/>							
MTU	Default ▾ <input type="text" value="1500"/>							
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

On this page you can specify the type of WAN port:

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



Note

Only one WAN type can be activated at a time. Activating one type deactivates another type.

3.2.2.1. Static IP

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
WAN								
Type	<div style="border: 1px solid black; padding: 2px;"> Static IP ▾ </div>							
Shared Connection(NAT)	<input checked="" type="checkbox"/>							
Default Route	<input checked="" type="checkbox"/>							
MAC Address	<input type="text" value="00:18:05:0C:C3:9B"/> <input type="button" value="Default"/> <input type="button" value="Clone"/>							
IP Address	<input type="text" value="192.168.2.254"/>							
Netmask	<input type="text" value="255.255.255.0"/>							
Gateway	<input type="text" value="192.168.2.1"/>							
MTU	Default ▾ <input type="text" value="1500"/>							

Multi-IP Settings

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

Name	Description	Standard
Type	Static IP	disabled
Shared Connection (NAT)	Enabled - local device connected to the router can access the Internet	enabled
Default Route	Mobile interface as standard route to the Internet	enabled
MAC Address	Set MAC address (button Default = default, 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	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 specified)		
IP Address	Set an additional IP address for LAN	empty
Netmask	Set Netmask	empty
Description	Describe settings	empty

3.2.2.2. Dynamic Address (DHCP)

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

Name	Description	Standard
Type	Dynamic Address (DHCP)	
Share Connection (NAT)	Enabled - local device connected to the router can access the Internet	enabled
Default Route	Mobile interface as standard route to the Internet	enabled
MAC Address	Set MAC address	
MTU	Set Maximum Transmission Unit (MTU), the options "Default" and "Manual" are possible.	Default = 1500

3.2.2.3. ADSL Dialup (PPPoE)

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

Name	Description	Standard
Type	ADSL Dialup (PPPoE)	
Share Connection (NAT)	Enabled - local device connected to the router can access the Internet	Enabled
Default Route	Mobile interface as standard route to the Internet	Enabled
MAC Address	Set MAC address	
MTU	Set Maximum Transmission Unit (MTU), the options "Default" and "Manual" are possible.	Default = 1492
ADSL Dialup (PPPoE) Settings		
Username	Set user name to dial in	empty
Password	Set password to dial in	empty
Static IP	Activate static IP address	disabled
Connection Mode	Set connection mode ("Connect on Demand"/"Always Online"/"Manual")	Always Online
Show Advanced Options		
Show advanced options	Enable advanced options	disabled
Service Name	Here you can assign a name for the service	empty
TX Queue Length	Specifying the length of the transfer queue	3
Enable IP head compression	Click to enable IP head compression	disabled
User Peer DNS	Activate Peer DNS for User	disabled
Link Detection Interval	Setting the connection detection interval	55 Seconds
Link Detection Max Retries	Set maximum number of repetitions for connection detection	10 (times)
Debug	Select to activate Debug mode	disabled

Expert Options	Determine expert parameters	empty
ICMP Detection Server	Set server for ICMP detection	empty
ICMP Detection Intervall	Set time for ICMP detection	30
ICMP Detection Timeout	Set timeout for ICMP detection	3
ICMP Detection Retries	Set the Maximum Number of Repetitions for ICMP Detection	3

3.2.3. WAN(STA)

Under this menu item **Network > WAN(STA)** you can configure the TK500 as a WAN station.

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

3.2.4. Link Backup

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

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
								Link Backup
Enable	<input checked="" type="checkbox"/>							
Main Link	WAN							
ICMP Detection Server	8.8.8.8							
ICMP Detection Interval	10	Seconds						
ICMP Detection Timeout	3	Seconds						
ICMP Detection Retries	3							
Backup Link	Dialup							
Backup Mode	Hot Backup							
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

Name	Description	Standard
Enable	Activate Service for Connection Backup	Deactivated
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	Empty
ICMP Detection Interval	Time interval between ICMP packets	10
ICMP Detection Timeout	Timeout for the individual ICMP packets	3 (Seconds)
ICMP Detection Retries	If the ICMP detection was not repeated successfully, the backup connection is selected.	3
Backup Link	Select Backup Connection	Dialup
Backup Mode	Hot Backup / Cold Backup	Hot Backup

3.2.5. LAN

Use the LAN menu area to adjust the settings for the LAN connection of the router and add Multi-IP settings. Accessible via **Network > LAN**.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
LAN								
Type	Static IP ▼							
MAC Address	00:18:05:0C:C3:9C							Default
IP Address	192.168.2.254							
Netmask	255.255.255.0							
MTU	Default ▼							1500
LAN Mode	Auto Negotiation ▼							
Multi-IP Settings								
IP Address	Netmask	Description						
<input type="text"/>	<input type="text"/>	<input type="text"/>						
								Add
Apply		Cancel						

Name	Description	Standard
Type	Selection between static IP address (Static IP) or DHCP (Dynamic Address)	Static IP
MAC Address	The MAC address in the LAN	Default can be restored via Button
IP Address	Set IP address in the LAN	192.168.2.1 (If it has been changed, you have to enter the new address on the configuration site)
Netmask	Set network mask of the LAN	255.255.255.0
MTU	St MTU-Length. Possible Options are "Manual" or "Default"	Default 1500
LAN Mode	Auto Negotiation, automatically selects connection type	Auto Negotiation
„Multi-IP Settings“ (a maximum of 8 additional IP addresses are supported)		
IP Address	Set further IP address for LAN	Empty
Description	Description of this IP address	Empty

If **Dynamic Address (DHCP)** is selected, the router is assigned a dynamic IP address.

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

3.2.6. Switch WLAN Mode

You can make settings for the WLAN type here. A distinction is made between Access Point (AP) and Station (STA). You can reach it 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	Standard
AP	Access Point Modus	AP
STA	Client Modus	

If **STA** is selected as WLAN TYPE (for station), the menu changes under **Network**. It is then possible to configure WAN(STA) under 3.2.3.3 and only one client for an existing WLAN under 3.2.6.a **WLAN Client**.

3.2.7. WLAN

The WLAN can be configured in this area of the router. It is deactivated as standard. You can start the configuration via **Network > WLAN**.

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

To turn on the WLAN, click on the **Enable** selection field.

System	Network	Services	Firewall	QoS	VPN	Tools	Status
WLAN							
Enable	<input checked="" type="checkbox"/>						
SSID Broadcast	<input checked="" type="checkbox"/>						
Mode	<input type="text" value="802.11b/g/n"/>						
Channel	<input type="text" value="11"/> (Note: if you want to use wireless WDS function, the channel must be consistent with the top AP)						
SSID	<input type="text" value="welotec"/>						
Auth Mode	<input type="text" value="WPA2-PSK"/>						
Encryption Method	<input type="text" value="TKIP"/>						
WPA/WPA2 PSK	<input type="text" value="....."/>						
Group Key Update Cycle	<input type="text" value="0"/> Seconds(0: disable)						
Bandwidth	<input type="text" value="20MHz"/>						
Enable WDS	<input type="checkbox"/>						
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>							

Name	Description	Standard
Enable	Switching WLAN on/off	off
SSID Broadcast	When enabled, the SSID is sent	enabled
Mode	Choice between various WLAN modes, e.g. 802.11 b/g/n	802.11 b/g/n
Channel	Transmission channel. Selection between 1 and 13 or automatic	11
SSID	Service Set Identifier or SSID for short stands for the WLAN name	welotec
Auth. Mode	Authentication mode for the WLAN, the selection fields change depending on the selection	OPEN
Encryption Method	Encryption method. TKIP, AES or TKIP/AES selection	none
WPA/WPA2 PSK	Enter the key to be used for accessing the WLAN	none
Group Key Update Cycle	Cycle for updating the group key in seconds	0
Bandwidth	WLAN bandwidth. 29 or 40 MHz are selectable	20MHz
Enable WDS	Enables WDS on the Router	off

Depending on the selection of the Auth. Mode, the input fields can vary greatly. We are happy to offer you our support in the creation of an ideal and secure WLAN.

3.2.7.1. WLAN Client

If the point **STA** was selected as WLAN type when configuring the **Switch WLAN Mode** (s. 3.2.6.) WLAN configuration is no longer possible. Then you can only configure the TK 500 as WLAN Client. This can be done under **Network > WLAN Client**.

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

Please activate **Enable** to configure the Router as WLAN client.

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

Enter the data to connect the TK500 to an existing WLAN.

3.2.8. 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	Status
							DNS
Primary DNS		0.0.0.0					
Secondary DNS		0.0.0.0					
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>							

Name	Description	Standard
Primary DNS	Set primary DNS	Empty
Secondary DNS	Set secondary DNS	Empty

3.2.9. 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, it is not possible to set up a secure VPN tunnel, for example. Therefore, providers of dynamic DNS servers are used, which ensure that your WAN connection always gets the IP address. The configuration can be reached 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		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.						
Apply		Cancel						

Name	Description	Standard
Current Address	Display current IP-address	Empty
Service Type	Select DDNS-Provider	Deactivated

There are various setting options for various providers of DDNS services. You select these using 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

Dynamic DNS ==> Dialup

Current Address
Service Type
URL
Username
Password
Hostname
Wildcard
MX
Backup MX
Force Update

Disabled
Disabled
Oray - Dynamic
QDNS(3322) - Dynamic
QDNS(3322) - Static
DynDNS - Dynamic
DynDNS - Static
DynDNS - Custom
No-IP.com
Custom
gh-admin

.....

welotec.ddns.net

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. Here there are various providers, some of which are free, but also liable to pay costs. 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

MX

Backup MX

Force Update

Last Update 2018-10-01 13:49:17

Last Response 2018-10-01 13:49:17 Update successful.

Apply Cancel

Name	Description	Standard
Service Type	DynDNS - Dynamic	disabled
URL	http://www.dyndns.com/	dignified
Username	Registered Username for	

DDNS	Empty	
Password	Registered Password for DDNS	Empty
Hostname	Registered Hostname for DDNS	Empty
Wildcard	Can be activated if wildcard should be used	Deactivated
MX	Entering an MX Record	Empty
Backup MX	Can be activated if MX-Record is to be activated	Deactivated
Force Update	Forces the Update of the Account	Deactivated
Last Update	Shows when the IP address was last changed	
Last Response	Shows the last time the Service was communicated with	

3.2.10. Static Route

Here you can add static routes. Static routes provide your router with additional routing information. Under normal circumstances, the router has sufficient information if configured for Internet access, and no further static routes need to be configured. Static routes only need to be specified in exceptional cases, for example, if 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						
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

Name	Description	Standard
Destination	Set the IP address of the destination	Empty
Netmask	Specifying the target's subnet mask	255.255.255.0
Gateway	Defining the Gateway of the Destination	Empty
Interface	Optional LAN/WAN port access to destination	Empty
Description	Freely selectable name for the static route	Empty

3.3. Services

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

3.3.1. DHCP Service

The Dynamic Host Configuration Protocol (DHCP) is a communication protocol in network technology. It allows the assignment of the network configuration to clients by a server. This allows devices in the network to be dynamically assigned IP addresses. 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														
<p>Enable DHCP <input checked="" type="checkbox"/></p> <p>IP Pool Starting Address <input type="text" value="192.168.2.2"/></p> <p>IP Pool Ending Address <input type="text" value="192.168.2.100"/></p> <p>Lease <input type="text" value="60"/> Minutes</p> <p>DNS <input type="text" value="192.168.2.1"/> Edit</p> <p>Windows Name Server (WINS) <input type="text" value="0.0.0.0"/></p> <p>Static DHCP</p> <table border="1"> <thead> <tr> <th>MAC Address</th> <th>IP Address</th> <th>Host</th> </tr> </thead> <tbody> <tr> <td>00:00:00:00:00:00</td> <td>192.168.2.2</td> <td></td> </tr> </tbody> </table> <p style="text-align: center;"> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </p>									MAC Address	IP Address	Host	00:00:00:00:00:00	192.168.2.2	
MAC Address	IP Address	Host												
00:00:00:00:00:00	192.168.2.2													

Name	Description	Standard
Enable DHCP	Click to enable DHCP	Enabled
IP Pool Starting Address	Setting the start IP address of the DHCP pool	192.168.2.2
IP Pool Ending Address	Setting the 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 on Edit)	192.168.2.1
Windows Name Server	Set WINS	Empty
Static DHCP (only 20 IP-addresses can be set up)		
MAC Address	Specify the MAC address of a intended IP address	Empty
IP Address	Set static IP	192.168.2.2
Host	Set Hostname	Empty

3.3.2. DNS Relay

If DNS relay is enabled (by default, if DHCP is set up), DHCP clients are assigned the IP address of the router as DNS server. All DNS requests to the router are sent to your Internet service provider’s DNS servers. If DNS relay is disabled, the router assigns the Internet service provider’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

Static [IP address <=> Domain Name] Pairing

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

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

Name	Description	Standard
Enable DNS Relay	Click to enable DNS forwarding	Activated (after activation of DHCP)
Static (IP Address <-> Domain Name) Pairing (maximum 20 DNS Pairs)		
IP Address	IP Address <-> Set DNS pairs	Empty
Host	Set names of IP-addresses<->DNS-Pairs	Empty
Description	Describe IP-Adresse<->DNS-Pairs	Empty

3.3.3. VRRP

The Virtual Router Redundancy Protocol (VRRP) is a method for increasing the availability of important gateways in local networks through 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, a virtual IP address and a virtual MAC address are assigned to the logical router. One of the routers within the group is defined as the virtual master router, which then binds the virtual MAC and virtual IP addresses to its network interface and informs the other routers in the group that 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																																																																																																																																						
<table> <tr> <td>Enable VRRP-I</td> <td><input checked="" type="checkbox"/></td> <td colspan="7"></td> </tr> <tr> <td>Group ID</td> <td><input type="text" value="1"/></td> <td colspan="7"></td> </tr> <tr> <td>Priority</td> <td><input type="text" value="20"/> (254:highest)</td> <td colspan="7"></td> </tr> <tr> <td>Advertisement Interval</td> <td><input type="text" value="60"/> Seconds</td> <td colspan="7"></td> </tr> <tr> <td>Virtual IP</td> <td><input type="text"/></td> <td colspan="7"></td> </tr> <tr> <td>Authentication Type</td> <td><input type="text" value="None"/></td> <td colspan="7"></td> </tr> <tr> <td>Monitor</td> <td><input type="text" value="None"/></td> <td colspan="7"></td> </tr> <tr> <td>Enable VRRP-II</td> <td><input checked="" type="checkbox"/></td> <td colspan="7"></td> </tr> <tr> <td>Group ID</td> <td><input type="text" value="2"/></td> <td colspan="7"></td> </tr> <tr> <td>Priority</td> <td><input type="text" value="10"/> (254:highest)</td> <td colspan="7"></td> </tr> <tr> <td>Advertisement Interval</td> <td><input type="text" value="60"/> Seconds</td> <td colspan="7"></td> </tr> <tr> <td>Virtual IP</td> <td><input type="text"/></td> <td colspan="7"></td> </tr> <tr> <td>Authentication Type</td> <td><input type="text" value="None"/></td> <td colspan="7"></td> </tr> <tr> <td>Monitor</td> <td><input type="text" value="None"/></td> <td colspan="7"></td> </tr> </table>									Enable VRRP-I	<input checked="" type="checkbox"/>								Group ID	<input type="text" value="1"/>								Priority	<input type="text" value="20"/> (254:highest)								Advertisement Interval	<input type="text" value="60"/> Seconds								Virtual IP	<input type="text"/>								Authentication Type	<input type="text" value="None"/>								Monitor	<input type="text" value="None"/>								Enable VRRP-II	<input checked="" type="checkbox"/>								Group ID	<input type="text" value="2"/>								Priority	<input type="text" value="10"/> (254:highest)								Advertisement Interval	<input type="text" value="60"/> Seconds								Virtual IP	<input type="text"/>								Authentication Type	<input type="text" value="None"/>								Monitor	<input type="text" value="None"/>							
Enable VRRP-I	<input checked="" type="checkbox"/>																																																																																																																																					
Group ID	<input type="text" value="1"/>																																																																																																																																					
Priority	<input type="text" value="20"/> (254:highest)																																																																																																																																					
Advertisement Interval	<input type="text" value="60"/> Seconds																																																																																																																																					
Virtual IP	<input type="text"/>																																																																																																																																					
Authentication Type	<input type="text" value="None"/>																																																																																																																																					
Monitor	<input type="text" value="None"/>																																																																																																																																					
Enable VRRP-II	<input checked="" type="checkbox"/>																																																																																																																																					
Group ID	<input type="text" value="2"/>																																																																																																																																					
Priority	<input type="text" value="10"/> (254:highest)																																																																																																																																					
Advertisement Interval	<input type="text" value="60"/> Seconds																																																																																																																																					
Virtual IP	<input type="text"/>																																																																																																																																					
Authentication Type	<input type="text" value="None"/>																																																																																																																																					
Monitor	<input type="text" value="None"/>																																																																																																																																					
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>																																																																																																																																						

The TK500 Series offers the opportunity to build two different groups VRRP (VRRP I and VRRP II).

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

⚠ Note

The selection fields may vary depending on the selection of the DTU protocol.

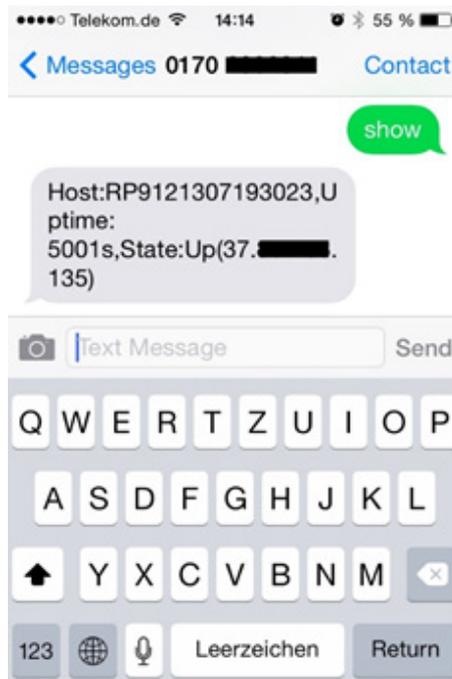
3.3.5. SMS

The TK500 can be reached via SMS from outside 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	<input checked="" type="checkbox"/>							
Status Query	<input type="text"/>	(English Only)						
Reboot	<input type="text"/>	(English Only)						
SMS Access Control								
Default Policy	Accept ▾							
Phone Number			Action			Description		
4917212345678			Accept ▾			1. SMS Empfänger		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

Name	Description	Standard
Enable	Click to enable or disable SMS control	Deactivated
Status Query	Set Status request SMS to show the status of the router (e.g.: show status).	Empty
Reboot	Restarts the router (e.g. reboot)	Empty
SMS Access Control		
Default Policy	Block or accept control SMS from a specific phone	Accept
Phone Number	Enter the phone numbers to send SMS to the router. The format for the mobile number is 491712345678 (please do not enter +49 or 0049)	Empty
Action	Setting of Allow (Accept) or Block (Block) of the previously entered phone number	Accept
Description	Description for the created data record	Empty

To send an SMS to the router, the mobile number of the inserted card must be known. Then the SMS is sent to it.



SMS that you receive on your mobile phone:

- Host: (SN);
- Uptime: (the operating time of the router at the time of this reboot);
- State: (Online/Offline) (Wireless WAN IP)
- LAN: (Ready) (LAN-IP)

3.3.6. 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								
Enable		<input checked="" type="checkbox"/>						
Alarm Threshold		<input type="text" value="50000"/> MB/Month						
Disconnect Threshold		<input type="text" value="0"/> MB/Month						
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

Name	Description	Standard
Enable	Click to activate or deactivate SMS Control	Deactivated
Alarm Threshold	Defines the amount of data in MB per month for which an alarm is to be generated. If 0 is set as value, no alarm is generated.	Empty
Disconnect Threshold	If the set value is reached, the dial-up connection is interrupted.	Empty

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

3.3.7. Alarm Manager

The Alarm Manager can be used to generate various alarms. You can configure this option 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								
System Service Fault		<input type="checkbox"/>						
Memory Low		<input type="checkbox"/>						
WAN Link-Up/Down		<input checked="" type="checkbox"/>						
LAN Link-Up/Down		<input type="checkbox"/>						
Dialup Up/Down		<input checked="" type="checkbox"/>						
Traffic Alarm		<input type="checkbox"/>						
Traffic Disconnect Alarm		<input type="checkbox"/>						
SIM/UIM Card Fault		<input type="checkbox"/>						
Signal Quality Fault		<input type="checkbox"/>						
Alarm Output								
Console		<input checked="" type="checkbox"/>						
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

Name	Description	Standard
Alarm Input	Here you select the areas for which an alarm is to be generated.	none
Alarm Output	Here you can select, whether the alarms should or should not be output via the console.	selected

3.4. Firewall

Via the **Firewall** menu item you can set the parameters for the firewall of the router. Various settings are possible here.

3.4.1. 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"/>						
Apply		Cancel						

Name	Description	Standard
Default Filter Policy	The options „Accept“ and „Block“ are possible	Allow
Block Anonymous WAN Request (ping)	Activate to block ping requests that are generated anonymously from the network.	Deactivated
Filter Multicast	Click to enable multicast filtering	Enabled
Defend DoS Attack	Click to enable blocking of DoS attacks	Enabled

3.4.2. Filtering

At this point you can filter what you want the firewall to let through and what not. Various configurations are possible here, which you can access 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"/>	
Apply		Cancel						

Name	Description	Standard
Enable	Click to enable filtering	Enabled
Proto	Selection of the protocol. The options "TCP"/"UDP"/"ICMP" are possible.	All
Source	Set source IP address	Empty
Source Port	Set source port if appropriate protocol is selected	Empty
Destination	Set Target IP	Empty
Destination Port	Set destination port if appropriate protocol is selected	Empty
Action	Selection whether setting should be allowed (Accept) or blocked (Block)	Accepted
Log	Click to enable logging of the setting	Deactivated
Description	Describe Configuration	Empty

3.4.3. Content Filtering

The content filter in the firewall allows to filter the call of special URL's, 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"/>	<input type="text"/>		Accept ▾	<input type="checkbox"/>	<input type="text"/>			
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

Name	Description	Standard
Enable	Activating or deactivating the content filter function	Enabled
URL	Enter the URL to be blocked or filtered	Empty
Action	Selection whether URL is blocked (block) or allowed (accept)	Accepted
Log	Can be activated for logging	Deactivated
Description	Describe Configuration	Empty

3.4.4. Port Mapping

NAT-PMP (NAT Port Mapping) allows a computer on a private network (behind a NAT router) to automatically configure the router so that devices behind the router are accessible from outside the private network. It essentially regulates the so-called port forwarding. NAT-PMP, like UPnP, allows a program to request all externally incoming data 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

Name	Description	Standard
Enable	Enable or disable port assignment	Enabled
Proto	Selection of the protocols TCP, UDP or TCP&UDP	TCP
Source	Quell-IP eintragen	0.0.0.0/0
Service Port	Enter the Port of the service	8080
Internal Address	Set internal IP for assignment	Empty
Internal Port	Set port mapping to "internal"	8080
Log	Click to enable Port mapping logging	Deactivated
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.	Empty
Description	Describe the meaning of the individual assignments	Empty

3.4.5. 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 in **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"/>

Name	Description	Standard
Virtual IP for Router	Set virtual IP for router	Empty
Source IP Range	Set range of source IP addresses	Empty
Virtual IP	Set virtual IP	Empty
Real IP	Set real IP	Empty
Log	Enable logging for virtual IP	Deactivated
Description	Describe Configuration	Empty

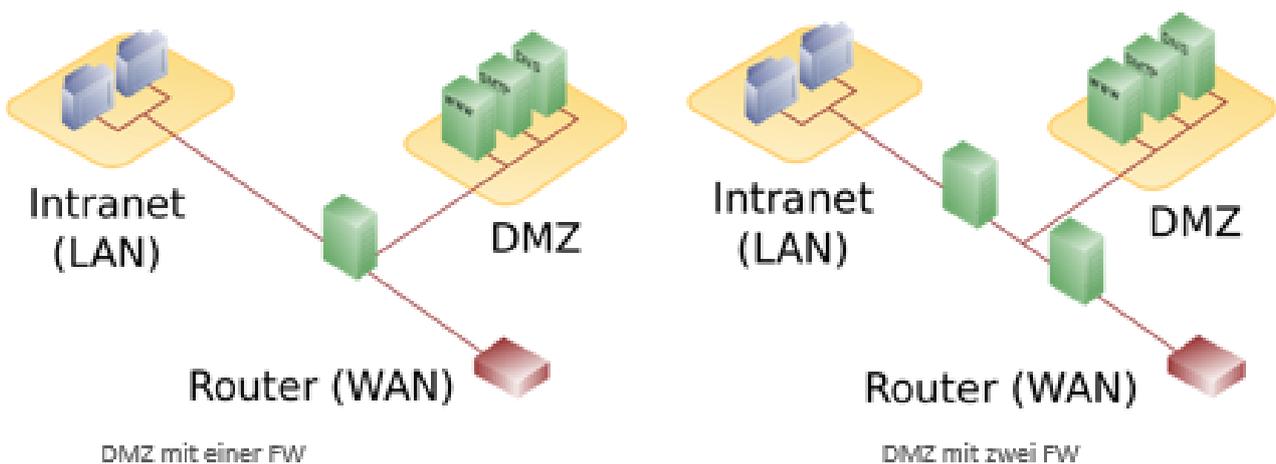
3.4.6. DMZ

A demilitarized zone (**DMZ**) is a computer network with security controlled access to the connected servers.

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 available services and at the same time protects the internal network (LAN) from unauthorized external access.

The purpose is to provide services of the computer network to both the Internet (WAN) and the Intranet (LAN) on the most secure basis possible.

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



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

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

 **Note**

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

Name	Description	Standard
Enable DMZ	Click to activate DMZ	Deactivated
DMZ Host	Set DMZ host IP	Empty
Source Address Range	Set IP address with restricted IP access	Empty
Interface	Auswahl des entsprechenden Interfaces	Empty

3.4.7. 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 reach this menu item under **Firewall > MAC-IP Bundling**.

System
Network
Services
Firewall
QoS
VPN
Tools
Application
Status

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

MAC-IP Bundling

MAC Address	IP Address	Description
00:00:00:00:00:00	192.168.2.2	

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

Name	Description	Standard
MAC Address	Set MAC address for bundling	Empty
IP Address	Specify IP address for bundling	192.168.2.2
Description	Describe configuration	Empty

3.5. QoS

In the TCP/IP world, QoS describes the quality of a communication service from the user’s point of view. The network service quality is often defined by 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, an attempt is made to identify data packages with corresponding service classes. Prioritized data packets are then preferably forwarded 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“.

3.5.1. Bandwidth Control

Here you can limit the bandwidth inbound or outbound. This can be configured under **QoS > Bandwith Control**.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
Bandwidth Control								
Enable	<input checked="" type="checkbox"/>							
Outbound Limit: Max BW	<input type="text" value="100000"/>	kbit/s						
Inbound Limit: Max BW	<input type="text" value="100000"/>	kbit/s						
<input type="button" value="Apply"/>		<input type="button" value="Cancel"/>						

Name	Description	Standard
Enable	Click to activate	Deactivated
Outbound Limit Max BW	Setting Outbound Bandwidth Limits	100000 kbps
Inbound Limit Max BW	Set incoming bandwidth limit	100000 kbps

3.5.2. IP BW Limit

Under the menu item **QoS > IP BW Limit** you can limit the download or upload bandwidth and bind it to IP addresses and then prioritize them.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
IP BW Limit								
Enable	<input checked="" type="checkbox"/>							
Download Bandwidth	<input type="text" value="1000"/>	kbit/s						
Upload Bandwidth	<input type="text" value="1000"/>	kbit/s						
Interface	CELLULAR ▾							
Host Download Bandwidth								
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text" value="1000"/>	<input type="text" value="Medium"/>	<input type="text"/>				
								<input type="button" value="Add"/>
<input type="button" value="Apply"/>		<input type="button" value="Cancel"/>						

Name	Description	Standard
Enable	Click to activate	Deactivated
Download Bandwith	Specifying the bandwidth for the download	1000 kbps
Upload Bandwith	Setting the bandwidth for the upload	1000 kbps
Interface	Selection of the interface to which the bandwidth is to be assigned	Cellular
Host Download Bandwidth		
Enable	Activating the function	Enabled
IP Adresse	Specification of the IP address for the assignment	Empty
Guaranteed Rate (kbit/s)	Indication of the guaranteed bandwidth in kbit/s	1000
Priority	Assignment of priority	Medium
Description	Description of the rule	Empty

3.6. VPN

A VPN (Virtual Private Network) is a closed logical network in which the subscribers are spatially separated from each other and connected via an IP tunnel. With this VPN you can access a local network, e.g. the company network, on the road or from your home office. This requires VPN software that communicates with the router of the network and is installed on the computer with which you want to access the network. There are different types of VPN connections (tunnels) that can be configured in this menu item for the TK500 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 Serecy(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 existing VPN connections. With **Add** a new tunnel can be created, see 3.6.2.

3.6.1. IPSec Settings

In this menu item you configure the settings for the IPSec, which can be accessed 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

Enable NAT-Traversal (NATT)

Keep alive time interval of NATT Seconds

Enable Compression

Debug

Force NATT

Dynamic NATT Port

Apply Cancel

Name	Description	Standard
Enable NAT-Traversal (NATT)	Click to enable	Deactivated
Keep alive time interval of NATT	Determining the duration for the maintenance of NATT	60 Seconds
Enable Compression	Switch compression on/off	Enabled
Debug	Switch debug mode on or off	Deactivated
Enable	Activating the function	Enabled
Force NATT	Forcing NATT on/off	Deactivated
Dynamic NATT Port	Switching a dynamic NATT Port on or off	Deactivated

The change of address via NAT is evaluated by a VPN gateway as a security-critical change of the data packets, the VPN negotiation fails, 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 successfully establish a VPN connection in these cases, NATT (NAT Traversal) provides a method to overcome these problems when handling data packets with changed addresses.

 **Note**

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 recipient therefore corresponds to the hash value entered in the packets.

3.6.2. IPSec Tunnels

Construct the corresponding tunnel under **VPN > IPSec Tunnels**.

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

Phase 1 Parameters

IKE Policy: 3DES-MD5-DH2

IKE Lifetime: 86400 Seconds

Local ID Type: IP Address

Remote ID Type: IP Address

Authentication Type: Shared Key

Key:

XAUTH Parameters

XAUTH Mode:

XAUTH Username:

XAUTH Password:

MODECFG:

Phase 2 Parameters

IPSec Policy: 3DES-MD5-96

IPSec Lifetime: 3600 Seconds

Perfect Forward Serecy(PFS): None

Link Detection Parameters

DPD Time Interval: 60 Seconds(0: disable)

DPD Timeout: 180 Seconds

ICMP Detection Server:

ICMP Detection Local IP:

ICMP Detection Interval: 60 Seconds

ICMP Detection Timeout: 5 Seconds

ICMP Detection Retries: 10

Save Cancel

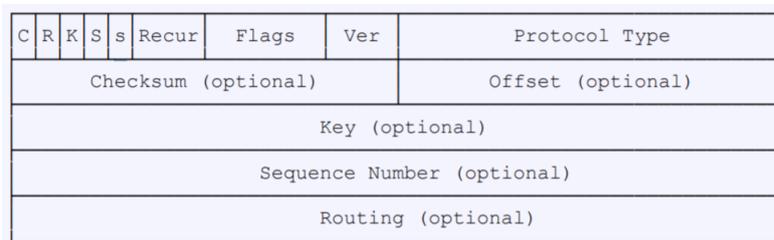
On this page the web-based parameters for the TK500 are presented.

Name	Description	Standard
Show Advanced Options	Click to activate advanced options	Deactivated
Basic Parameters		
Tunnel Name	Name for the tunnel	IPSec_tunnel_1
Destination Address	Specifying the destination address of the IPSec VPN server	Empty
Startup Modes	Possible modes are "Auto Activate"/"Triggered by Data"/"Passive"/"- Manually Activated".	Enabled
Restart WAN when failed	WAN interface is restarted in case of failed tunnel construction.	Enabled
Negotiation Mode	Optional: „Main Mode“ or „Aggressive Mode“	Main Mode
IPSec Protocol	Optional: „ESP“ or „AH“	ESP
IPSec Mode	Optional: „Tunnel Mode“ or „Transport Mode“	Tunnel Mode
VPN over IPSec	LT2P oder GRE over IPsec	None

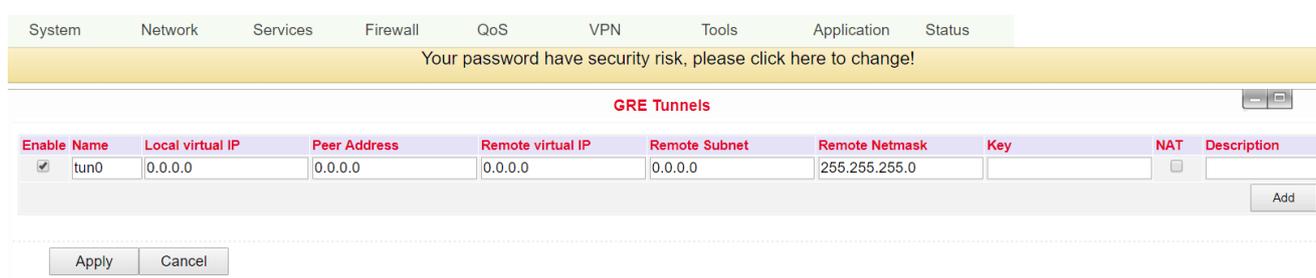
Tunnel Type	Selection field for various setting options	Subnet – Subnet Mode
Local Subnet	Set Protected IPSec Subnet (Local)	192.168.2.1
Local Netmask	Set Protected IPSec Subnet Mask (Local)	255.255.255.0
Remote Subnet	Setting a Protected IPSec Subnet (Remote)	0.0.0.0
Remote Netmask	Set protected IPSec subnet mask (remote)	255.255.255.0
Phase 1 Parameters		
IKE Policy	Multi-selection list for the policy	3DES-MD5-96
IKE Lifetime	Set IKE validity period	86400 Seconds
Local ID Type	Selection of "FQDN", "USERFQDN" or "IP address" possible	IP Address
Remote ID Type	Selection of "IP address", "User FQDN" or "FQDN" possible	IP Address
Authentication Type	Selection of "Shared Key" or "Certificate" possible	Shared Key
Key (bei Auswahl des Authentifizierungstyps „Shared Key“)	Set IPSec key for VPN negotiation	Empty
XAUTH Parameters		
XAUTH Mode	Enable XAUTH	Deactivated
XAUTH Username	XAUTH Username	Empty
XAUTH Password	XAUTH Password	Empty
MODECFG	Enable MODECFG	Deactivated
Phase 2 Parameters		
IPSec Policy	Multi-selection list for the policy	3DES-MD5-96
IPSec Lifetime	Set IPSec validity period	3600 Sekunden
Perfect Forward Secrecy (PFS)	Optional: „Disable“, „GROUP1“, „GROUP2“, „GROUP5“	Deactivated (Enable advanced options)
Link Detection Parameters		
DPD Time Interval	Set DPD time Interval	60 Seconds
DPD Timeout	Set DPD timeout	180 Seconds
ICMP Detection Server	Specify server for ICMP detection	Empty
ICMP Detection Local IP	Set local IP for ICMP	Empty
ICMP Detection Interval	Set interval for ICMP Detection	60 Seconds
ICMP Detection Timeout	Set timeout for ICMP Detection	5 Seconds
ICMP Detection Max Retries	Setting the Maximum Number of Receptions for ICMP Detection	10

3.6.3. GRE Tunnels

Generic Routing Encapsulation (GRE) is a network protocol developed by Cisco and defined in RFC 1701. Via GRE other protocols can be packed and transported in an IP tunnel. GRE uses the IP protocol 47, the GRE header is structured as follows:



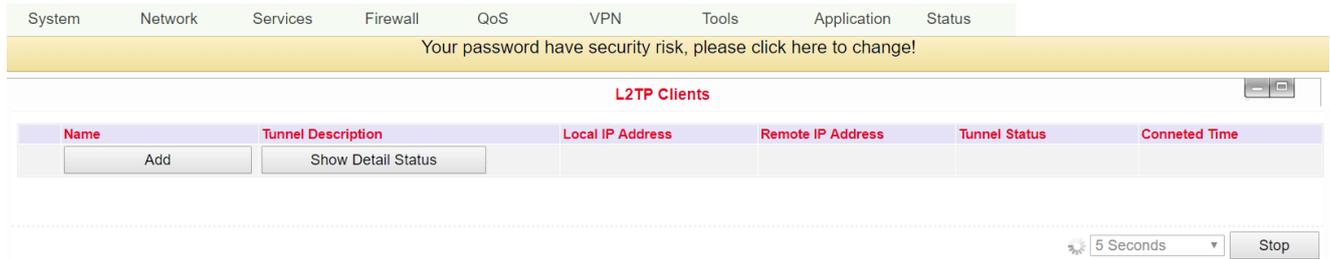
A GRE package consists of an IP-Header, a GRE-Header and the actual payload. You can set up this GRE tunnel under **VPN > GRE Tunnels**.



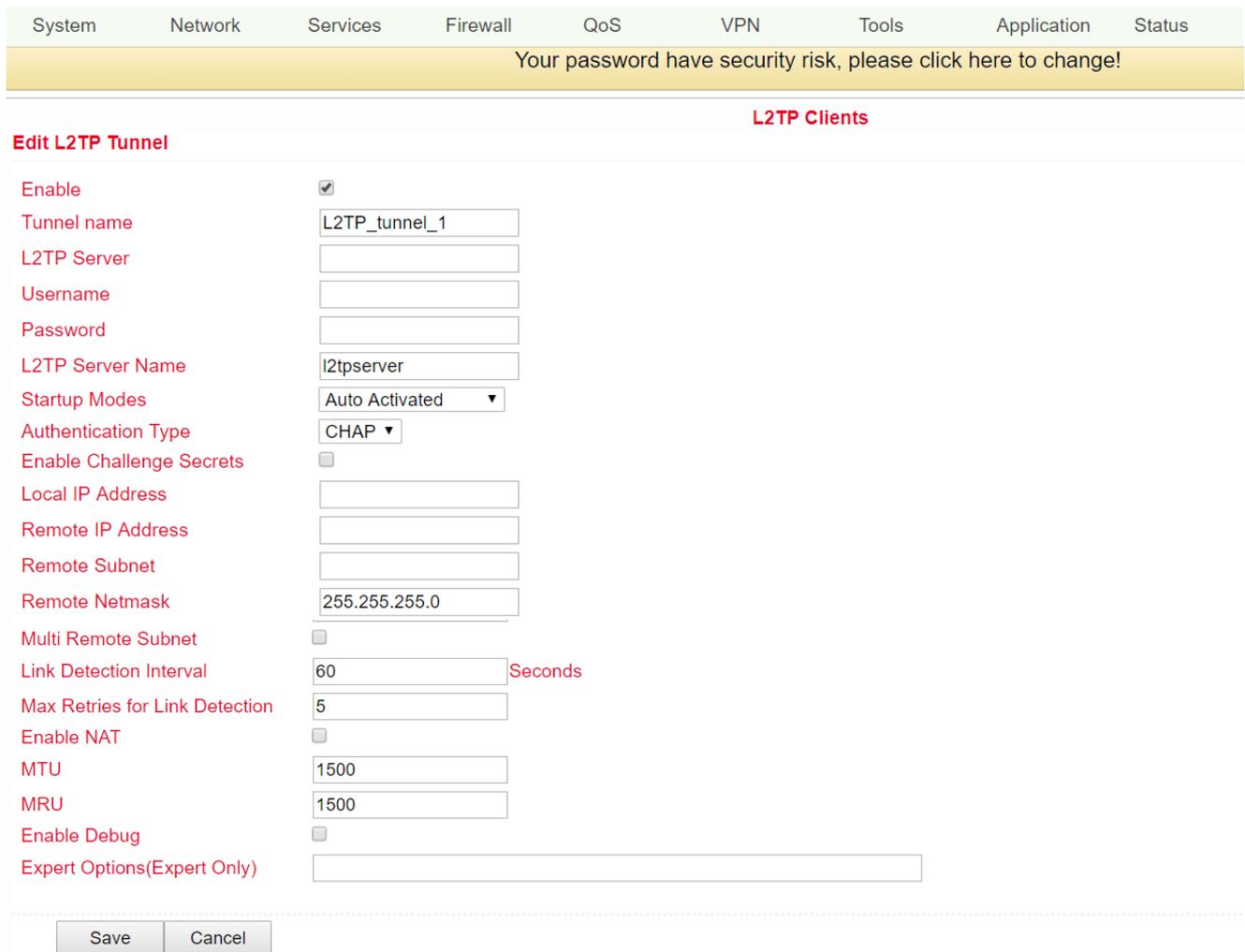
Name	Description	Standard
Enable	Click to enable	Enabled
Tunnel Name	Define names for GRE tunnels	tun0
Local Virtual IP	Set local virtual IP	0.0.0.0
Peer Address	Set peer address	0.0.0.0
Remote Virtual IP	Specifying the virtual IP of the remote network	0.0.0.0
Remote Subnet Address	Set Remote Subnet Address	0.0.0.0
Remote Subnet Netmask	Defining a Remote Subnet Mask	255.255.255.0
Key	Define the key for encrypting the tunnel	Empty
NAT	Click to enable NAT function	Deactivated
Description	Add Description	Empty

3.6.4. L2TP Clients

Layer 2 Tunneling Protocol (L2TP) is a network protocol that tunnels frames of OSI model backup 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. You reach the configuration via **VPN > L2TP Clients**.



By clicking the **Add** button you start the configuration of the L2TP client.



Name	Description	Standard
Enable	Enables the tunnel settings	Enables
Tunnel Name	Define Tunel Name	L2TP_TUNNEL_1
L2TP Server	Enter the address of the L2TP Server	Empty
Username	Set Username for Server	Empty

Password	Set Password for Server	Empty
L2TP Server Name	Define names for Servers	l2tpserver
Startup Modes	Set start modes: "Auto Activated", "Triggered by Data", "Manually Activated", "L2TPOverIP-Sec".	Auto Activated
Authentication Type	Set the authentication type: "CHAP", "PAP".	CHAP
Enable Challenge Secrets	To activate secret keys (Challenge) select	Deactivated
Challenge Secrets	If Enable Challenge Secrets is activated, the secret key can be entered here	Empty
Local IP Address	Set local IP address	Empty
Remote IP Address	Set Remote IP address	Empty
Remote Subnet	Set a Remote Subnet	Empty
Remote Subnet Netmask	Define a Remote Subnet Mask	255.255.255.0
Link Detection Interval	Set Interval for connection detection	60
Max Retries for Link Detection	Setting the Maximum Number of Repetitions for Connection Detection	5
Enable NAT	Click to enable NAT	Deactivated
MTU	Set MTU parameters	1500
MRU	Set MRU parameters	1500
Enable Debug Mode	Click to activate debug mode	Deactivated
Expert Options	Set Expert options	Empty

3.6.5. PPTP Clients

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

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

PPTP Clients

Edit PPTP Tunnel

Enable

Tunnel name

PPTP Server

Username

Password

Startup Modes

Authentication Type

Local IP Address

Remote IP Address

Remote Subnet

Remote Netmask

Link Detection Interval Seconds

Max Retries for Link Detection

Enable NAT

Enable MPPE

Enable MPPC

MTU

MRU

Enable Debug

Expert Options(Expert Only)

Name	Description	Standard
Enable	Click to enable	Enabled
Tunnel Name	The name for the tunnel (set automatically)	PPTP_tunnel_1
PPTP Server	Specify Address for PPTP Server	Empty
Username	Set Username for Server	Empty
Password	Set Password for Server	Empty
Startup Mode:	Set start modes "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	Empty
Remote IP Address	Set Remote IP-address	Empty
Remote Subnet	Defining a Remote Subnet Mask	Empty
Remote Subnet Net-mask	Defining a Remote Subnet Mask	255.255.255.0
Link Detection Interval	Setting the connection detection interval	60
Max Retries for Link Detection	Set the Maximum Number of Repetitions for Connection Detection	5
Enable NAT	Click to enable NAT	Empty
Enable MPPE	Click to enable MPPE (Microsoft Point to Point Encryption)	Empty
Enable MPPC	Click to enable MPPC (Microsoft Point to Point Compression)	Empty
MTU	Set MTU parameters	1500
MRU	Set MRU parameters	1500
Enable Debug Mode	Click to enable Debug Mode	Empty
Expert Options	Only for Welotec R&D	Empty

3.6.6. OpenVPN Tunnels

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

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

Choose the options **VPN > Open VPN Tunnels**, on the configuration page of the TK500, as shown below:

The screenshot shows the 'OpenVPN Tunnels' configuration page. At the top, there is a navigation menu with tabs for System, Network, Services, Firewall, QoS, VPN, Tools, Application, and Status. A yellow warning banner reads 'Your password have security risk, please click here to change!'. Below this is the 'OpenVPN Tunnels' title and a refresh icon. A table lists the tunnels:

Enable	Name	Tunnel Description	Tunnel Status	Conneted 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

Below the table are 'Add' and 'Show Detail Status' buttons. At the bottom right, there is a refresh icon, a '5 Seconds' dropdown, and a 'Stop' button.

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

The screenshot shows the 'Edit OPENVPN Tunnel' configuration page. It features a navigation menu and a yellow warning banner. The page title is 'OpenVPN Tunnels'. The configuration fields are as follows:

- Tunnel name: OpenVPN_T_1
- Enable:
- Mode: Client
- Protocol: UDP
- Port: 1194
- OPENVPN Server: 192.168.2.12
- Authentication Type: X.509 Cert
- Pre-shared Key: (empty text area)
- Local IP Address: 192.168.3.0
- Remote IP Address: 192.168.2.0
- Remote Subnet: (empty text area)
- Remote Netmask: 255.255.255.0
- Link Detection Interval: 60 Seconds
- Link Detection Timeout: 300 Seconds
- Renegotiate Interval: 86400 Seconds
- Enable NAT:
- Enable LZO:
- Encryption Algorithms: AES(256)
- MTU: 1500
- Max Fragment Size: (empty text area)
- Debug Level: Warn
- Interface Type: TUN
- Expert Options(Expert Only): (empty text area)

At the bottom, there are 'Save', 'Cancel', and 'Delete' buttons.

Name	Description
Tunnel name	Given
Enable	Activate this configuration
Mode	"Select "Client" or "Server" mode
Protocol	Selection of the "UDP" or "TCP" protocol
Port	Standard port for OpenVPN is 1194
OPENVPN Server	IP or DNS of OpenVPN-Servers
Authentication Type	Select the Authentication Type
Pre-shared Key	If Pre shared key, common key or TLS-AUTH is selected, set static password
Remote Subnet, Remote Netmask	Set static route of router, always in direction of peer subnet
Username/Password	If User/Password is selected, the corresponding data is entered in these fields
Link Detection Interval, Link Detection Timeout	Always use standard
Renegotiate Interval	Always use standard
Enable NAT	Set NAT mode, routing mode is deactivated in the meantime
Enable LZO	Enable LZO-compression
Encryption Algorithms	Encryption Algorithm must match the server
MTU	Always use standard, 1500
Max Fragment Size	Maximum size of individual packages
Debug Level	Selection of Debug Output in Log
Interface Type	TUN / TAP
Expert Options (Expert Only)	Other OpenVPN commands (for advanced users only)

3.6.7. OpenVPN Advanced

This configuration page is only used for the OpenVPN server and provides advanced features. 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	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Name	Description
Enable Client-to-Client (Server Mode Only)	Allow client access to other clients
Client Management	
Enable	Activating the function
Tunnel Name	Tunnel name of the client
Username/Common Name	User name (using the "User name/Password" mode) or general 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



Note

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

3.6.8. Certificate Management

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

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
Certificate Management								
<p>Certificate Management</p> <p>Enable SCEP (Simple Certificate Enrollment Protocol) <input type="checkbox"/></p> <p>Protect Key <input type="text"/></p> <p>Protect Key Confirm <input type="text"/></p>								
No file selected.			Browse...		Import CA Certificate		Export CA Certificate	
No file selected.			Browse...		Import CRL		Export CRL	
No file selected.			Browse...		Import Public Key Certificate		Export Public Key Certificate	
No file selected.			Browse...		Import Private Key Certificate		Export Private Key Certificate	
No file selected.			Browse...		Import PKCS12		Export PKCS12	
<div style="display: flex; justify-content: center; gap: 20px;"> Apply Cancel </div>								

Name	Description	Standard
Enable SCEP	Click to activate	
Protect Key	Set a key to protect the certificate	Empty
Protect Key Confirm	Confirm the key to protect the certificates	Empty
Import/Export CA Certificate	Import or export CA Certificates	Empty
Import/Export Certificate (CRL)	Import or export CRL certificate	Empty
Import/Export Public Key Certificate	Import or export private key certificate	Empty

Import/Export Private Key Certificate	Import or export PKCS12 (private key and X.509 certificate)	Empty
Import/Export PKCS12	Import or export PKCS12 (private key and X.509 certificate)	Empty
Searching	The respective file is selected via Browse and can then be imported	No file selected

3.7. Tools

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

3.7.1. PING

Select **Tools > Ping** if you want to test whether a connection to the network/internet is established.

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	Standard
Host	Target for PING	Empty
Ping Count	Set number of PINGS	4 times
Packet Size	Set packet size for PING	32 Byte
Expert Options	Advanced parameters	Empty

3.7.2. Traceroute

Traceroute (tracert) determines via which router and Internet node 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

Maximum Hops

Timeout Seconds

Protocol

Expert Options

```

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

Name	Description	Standard
Host	Target for Trace Route	Empty
Max Hops	Set Maximun number of Hops	20
Time Out	Set Timeout	3 Seconds
Protocol	Optional: „ICMP“/„UDP“	UDP
Expert Options	Advanced Parameters	Empty

3.7.3. 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.

Use the **Browse** button to upload a file from your computer. The file should be between 10 and 2000MB in size. After selecting the file, click the **Upload** button. The result is then displayed.

3.8. Application

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

3.8.1. Smart ATM

The Smart ATM point is not supported by us at the moment. This is a special function for vertical markets.

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

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

Smart ATM

Enable Smart ATM Cloud

Enable SSL Proxy

Multi Server

Protocol	Incoming TCP Port	Outgoing IP/Host	Outgoing TCP Port	Outgoing TCP Source Port(0 for any)
<input type="button" value="Add"/>				

3.9. Status

Under „**Status**“ you will find information on the system, modem, network connections, routing table, device list and protocol.

3.9.1. System

Select **Status > System** from the menu to retrieve 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 on the name, model type, current version, etc.

3.9.2. Modem

Check the status of your modem under **System > 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 display the status of the modem including the signal strength.

3.9.3. Traffic Statistics

If you want to view the data consumption of the SIM card in the TK500, 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						

<input type="button" value="Clear"/>								

Here you can see the data that was received or transmitted monthly, daily and hourly. Use the „**Clear**“ button to reset the entries to 0.

3.9.4. Alarm

Check the alarms generated by the TK500, e.g. 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		

<input type="button" value="Clear All Alarms"/> <input type="button" value="Confirm All Alarms"/>								

In this example, the monthly limit of the SIM card has been reached. Use the „**Clear All Alarms**“ button to delete all alarm messages and „**Confirm All Alarms**“ to confirm that you have taken note of the alarm.

3.9.5. WLAN

Via **Status > WLAN** you can view all WLAN networks in the receiving area of the TK500. To do 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:6fb0:47	WPA2PSK/AES	34	11b/g/n		
1	WeloLabor	00:18:0a:8fb0:47	WPA2PSK/AES	39	11b/g/n		

3 Seconds

3.9.6. 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							
<input type="button" value="Renew"/> <input type="button" value="Release"/>								
Dialup								
Connection Type	Dialup							
IP Address	37.80.83.157							
Netmask	255.255.255.252							
Gateway	37.80.83.158							
DNS	10.74.210.210,10.74.210.211							
MTU	1500							
Status	Connected							
Connection time	0 day, 02:36:53							
<input type="button" value="Connect"/> <input type="button" value="Disconnect"/>								
LAN								
Connection Type	Static IP							
MAC Address	00:18:05:0C:C3:9C							
IP Address	192.168.2.1							
Netmask	255.255.255.0							
Gateway								
DNS								
MTU	1500							

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

3.9.7. Route Table

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

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

After calling, you will see the routing table of the TK500.

3.9.8. Device List

All devices connected to the TK500 are displayed under the menu item **Status > 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						

Overview of the devices connected to the TK500.

3.9.9. Log

Documentation of the system events (Log) of the TK500 can be found under **Status > Log**.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status	
Your password have security risk, please click here to change!									
Log									
notice	Oct 1 16:29:12	openvpn[4015]	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	udhcpc[460]	Sending discover...						
info	Oct 1 16:29:15	udhcpc[460]	Sending discover...						
			Clear Log	Download Log File	Download System Diagnosing Data				

This page displays the system log that can be downloaded here

Problems may not be diagnosed and resolved immediately. In these cases, please send the diagnostic pro-

to col to Welotec. To do this, click on „**Download System Diagnosing Data**“ and send us the protocol with a description of the error to support@welotec.com

3.9.10. Third Party Software Notices

Here are the software terms and licenses of all third party vendors associated with the TK500 router series.

System	Network	Services	Firewall	QoS	VPN	Tools	Application	Status
Your password have security risk, please click here to change!								
Third Party Software Notices								
<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> <p>bridge-utils</p> <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 warrantv of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.</p>								

4. TECHNICAL DATA

4.1. Device characteristics

Characteristic	Value
Dimensions (W x H x D)	35 x 127 x 108.2 mm
Operating voltage	230 V AC at 12 V – 24 V DC
Approval	CE-compliant

4.2. Environmental characteristics

Characteristic	Value
Operating temperature range	-15 bis +70 °C
Humidity	5 - 95 %, non-condensing
Shock	IEC 60068-2-27
Free Fall	IEC 60068-2-32
Vibration	IEC 60068-2-6

4.3. Radio frequencies

4.3.1. Radio frequencies 4G LTE Europe

Frequency	Frequency range and transmission power	Router
Band 1	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Frequency range Down: 703 MHz – 748 MHz • Frequency range Up: 758 MHz – 803 MHz • Max. transmission power: 200 mW 	TK525U, TK525L, TK525L-W, TK525W

4.3.2. Radio frequencies 3G UMTS Europa

Frequency	Frequency range and transmission power	Router
Band 1	<ul style="list-style-type: none"> • 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 3	<ul style="list-style-type: none"> • Frequency range Down: 1805 MHz – 1880 MHz • Frequency range Up: 1710 MHz – 1785 MHz • Max. transmission power: 251 mW 	TK525U, TK525L, TK525L-W, TK525W
Band 8	<ul style="list-style-type: none"> • Frequency range Down: 925 MHz – 960 MHz • Frequency range Up: 880 MHz – 915 MHz • Max. transmission power: 251 mW 	TK525U, TK525L, TK525L-W, TK525W

4.3.3. Radio frequencies 2G GSM Europe

Frequency	Frequency range and transmission power	Router
GSM 900	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Frequency range Down: 1805 MHz – 1880 MHz • Frequency range Up: 1710 MHz – 1785 MHz • Max. transmission power: 40 mW 	TK525U, TK525L, TK525L-W, TK525W

4.3.4. Radio frequencies 4G LTE Asia

Frequency	Frequency range and transmission power	Router
Band 1	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 5	<ul style="list-style-type: none"> • Frequency range Down: 869 MHz – 894 MHz • Frequency range Up: 824 MHz – 849 MHz • Max. transmission power: 200 mW 	TK525U, TK525L, TK525L-W, TK525W
Band 7	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Frequency range Down: 2570 MHz – 2620 MHz • Frequency range Up: not known • Max. transmission power: 200 mW 	TK525U, TK525L, TK525L-W, TK525W
Band 39 China	<ul style="list-style-type: none"> • Frequency range Down: 1880 MHz – 1920 MHz • Frequency range Up: not known • Max. transmission power: 200 mW 	TK525U, TK525L, TK525L-W, TK525W
Band 40 China	<ul style="list-style-type: none"> • Frequency range Down: 2300 MHz – 2400 MHz • Frequency range Up: not known • Max. transmission power: 200 mW 	TK525U, TK525L, TK525L-W, TK525W
Band 41 China	<ul style="list-style-type: none"> • Frequency range Down: 2496 MHz – 2690 MHz • Frequency range Up: not known • Max. transmission power: 200 mW 	TK525U, TK525L, TK525L-W, TK525W

4.3.5. Radio frequencies 3G UMTS Asia

Frequency	Frequency range and transmission power	Router
Band 1	<ul style="list-style-type: none"> • 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 5	<ul style="list-style-type: none"> • Frequency range Down: 869 MHz – 894 MHz • Frequency range Up: 824 MHz – 849 MHz • Max. transmission power: 251 mW 	TK525U, TK525L, TK525L-W, TK525W
Band 8	<ul style="list-style-type: none"> • Frequency range Down: 925 MHz – 960 MHz • Frequency range Up: 880 MHz – 915 MHz • Max. transmission power: 251 mW 	TK525U, TK525L, TK525L-W, TK525W

4.3.6. Radio frequencies 2G GSM Asia

Frequency	Frequency range and transmission power	Router
GSM 900	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Frequency range Down: 1805 MHz – 1880 MHz • Frequency range Up: 1710 MHz – 1785 MHz • Max. transmission power: 1000 mW 	TK525U, TK525L, TK525L-W, TK525W

4.3.7. Radio frequencies 3G UMTS global

Frequency	Frequency range and transmission power	Router
Band 1	<ul style="list-style-type: none"> • 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 2	<ul style="list-style-type: none"> • Frequency range Down: 1930 MHz – 1990 MHz • Frequency range Up: 1850 MHz – 1910 MHz • Max. transmission power: 251 mW 	TK525U, TK525L, TK525L-W, TK525W
Band 5	<ul style="list-style-type: none"> • Frequency range Down: 869 MHz – 894 MHz • Frequency range Up: 824 MHz – 849 MHz • Max. transmission power: 251 mW 	TK525U, TK525L, TK525L-W, TK525W
Band 8	<ul style="list-style-type: none"> • Frequency range Down: 925 MHz – 960 MHz • Frequency range Up: 880 MHz – 915 MHz • Max. transmission power: 251 mW 	TK525U, TK525L, TK525L-W, TK525W

4.3.8. Radio frequencies 2G GSM global

Frequency	Frequency range and transmission power	Router
GSM 850	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Frequency range Down: 1930 MHz – 1990 MHz • Frequency range Up: 1850 MHz – 1910 MHz • Max. transmission power: 1000 mW 	TK525U, TK525L, TK525L-W, TK525W

4.3.9. Radio frequencies WLAN

Frequency	Frequency range and transmission power	Router
2.4 GHz	<ul style="list-style-type: none"> • Frequency range: 2400 MHz – 2483.5 MHz • Max. transmission power: 40 mW 	TK525L-W

5. SUPPORT

If there are any problems with installation and operation, please send an e-mail to the following address:
support@welotec.com

6. CE DECLARATION

a byte smarter

WELOTEC®

Declaration of conformity

Holder:

Welotec GmbH
 Zum Hagenbach 7
 48366 Laer
 GERMANY

declares that the product(s):

Product:

Industrial Cellular Router

Identification:

TK505U, TK515L, TK515L-W, TK505W, TK525U, TK525L, TK525L-W, TK525W

Complies with:

Radio Equipment Directive 2014/53/EU,

- ETSI EN 301 489-1 V2.1.1 (2017-02 - Class A)
- ETSI EN 301 489-3 V1.6.1 (2013-08)
- ETSI EN 301 489-17 V3.1.1 (2017-02)
- ETSI EN 301 489-52 V1.1.0 (2016-11)
- ETSI EN 301 511 V12.5.1 (2017-03)
- ETSI EN 300 328 V2.1.1 (2016-11)
- ETSI EN 301 908-1 V11.1.1 (2016-07)
- ETSI EN 301 908-2 V11.1.1 (2016-07)
- ETSI EN 301 908-13 V11.1.1 (2016-07)
- EN 62311:2008

Low Voltage Directive 2014/35/EU

EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013

EMC Directive 2014/30/EU

- EN 55032:2012
- EN 55024:2010
- EN 61000-3-2:2014
- EN 61000-3-3:2013

RoHS 2 Directive 2011/65/EU

for use in industrial environments.



The corresponding markings appear under the appliance.

These devices are designed for the use in all countries of the EU, Switzerland, Norway, Lichtenstein and Iceland.

2017-09-29

 Date

Welotec GmbH
 Zum Hagenbach 7
 D-48366 Laer
 Fon: +49 (0)2554-913000
 www.welotec.com

 Signature
 (Jos Zenner, Business Development)

www.welotec.com

Welotec GmbH
 Zum Hagenbach 7 · D-48366 Laer
 Fon: +49 (0)25 54/91 30-00
 Fax: +49 (0)25 54/91 30-10
 info@welotec.com

Geschäftsführer: Dr. Reinhard Lüff
 Handelsregister Steinfurt, HRB 3363
 Ust-IdNr. DE121631449
 Steuer-Nr. 311/5830/2243

Deutsche Bank AG Vreden
 Konto-Nr 3 920 840 · BLZ 403 700 24
 IBAN DE 36403700240392084000
 SWIFT DEUTDE3303

Kreissparkasse Steinfurt
 Konto-Nr 3 020 203 · BLZ 403 510 60
 IBAN DE 13403510600003020203
 SWIFT WELADED1STF