TK800

Version:
v1.0.0

Date:
13.10.2023

Contents

1 1. Introduction

1.1 Copyright Notice

1.2 Trademarks

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

1.3 Legal Notice

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

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

1.4 Technical Support Contact Information

Welotec GmbH

Zum Hagenbach 7

48366 Laer

Tel.: +49 2554 9130 00

Fax.: +49 2554 9130 10

Email: info@welotec.com

1.5 Description

The TK800 series industrial routers provide stable connectivity between remote devices and customer sites over 2G/3G/4G networks. They can operate in a voltage range of 12-48V DC and have a temperature range of -25°C to 70°C with a relative humidity of 95%, as well as adhering to numerous EMC standards, ensuring high stability and reliability under severe industrial conditions. The TK800 can be used on the workstation or mounted on DIN rails. TK800 series products support VPN (IPSec/L2TP/GRE/OpenVPN), which ensures a secure connection between remote devices and customer sites.

1.6 *Important Safety Notes*:

This product is not suitable for the following areas of application

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

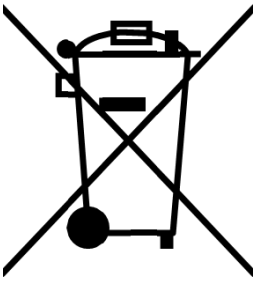
1.7 Warning

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

1.8 WEEE Notice

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

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



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

2 2. Quick Start

Guide to installation and comissioning of the TK800 series. Please ensure that all package contents are present upon delivery. If you need a SIM card, contact your local network operator.

2.1 2.1. Package checklist

Each TK800 is supplied in a box with standard accessories. Optional accessories can also be ordered. Check the contents of the box. If something is missing, contact Welotec.

2.1.1 2.1.1. Components Router

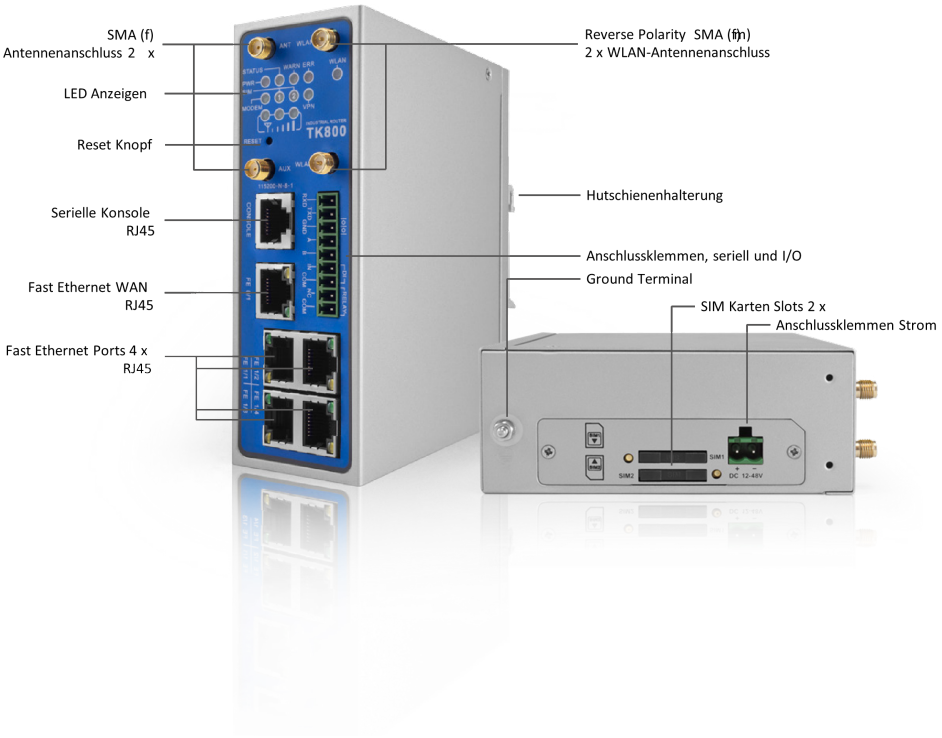
Product	Amount	Description
TK800	1	TK800 series industrial router
Terminal block	1	Terminal block, 2-pin
Terminals Serial and I/O	1	Terminal block, 9-pin (EX0 / EXW variants only)

2.1.2 2.1.2. Components Set

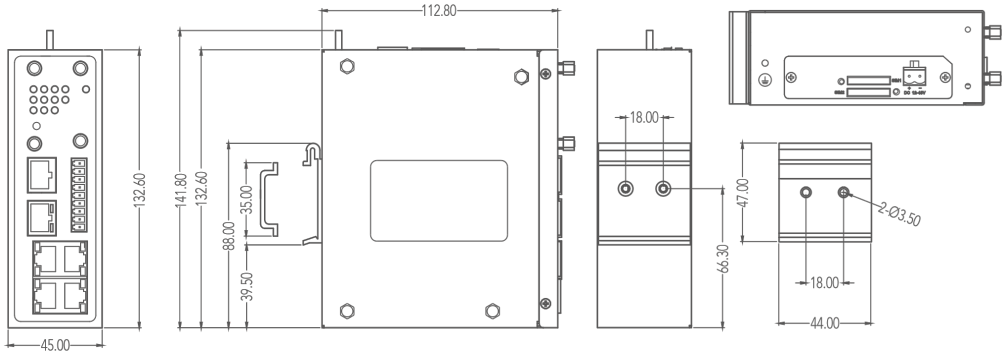
Product	Amount	Description
TK800	1	TK800 series industrial router
Terminal block	1	Terminal block, 2-pin
Network cable	1	1,5 m
Antenna	2 (4)	3G/4G Antenna Wi-fi Antenna (EXW variant only)
Power supply unit	1	230 V AC to 12 V DC
Terminals Serial and I/O	1	Terminal block, 9-pin (EX0 / EXW variants only)

2.2 2.2. Information and Control Panel

2.2.1 2.2.1. Control Panel



2.2.2 2.2.2. Dimension Drawings



2.3 2.3. Installation Guide

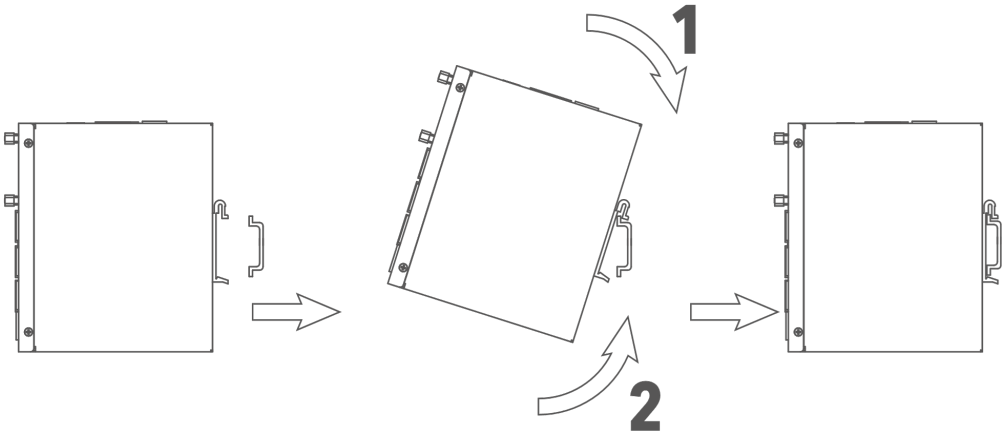
2.3.1 2.3.1. Preparations

Prepare the power supply (12 - 48 V DC). Make sure that the device can operate under the specified environmental conditions (working temperature range -25 – +70 °C, humidity: 5 – 95 % relative humidity). The device should not be exposed to direct sunlight and should be installed away from heat sources and environments with strong electromagnetic interference. The router can be mounted on a DIN rail (top-hat rail) or used at a workstation.

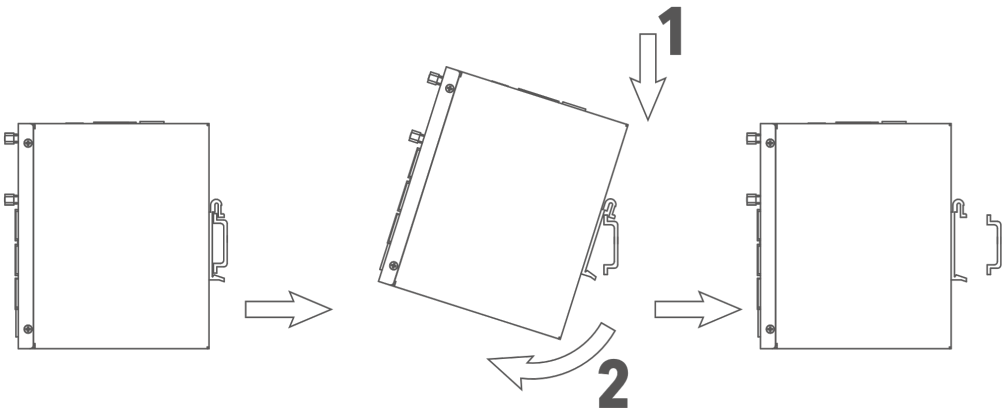
2.3.2 2.3.2. Mounting the Device

DIN rail:

Select a position with sufficient space on the DIN rail. Then place the upper part of the DIN rail mount on the DIN rail. Subsequently, press the lower side of the DIN rail mount down until the device is locked in place. This picture serves as an illustration:



For demounting press the device from top to bottom and then pull the lower side of the device from the DIN rail (see figure).



2.4 2.4. Installing the SIM Card

The TK800 supports dual SIM. To insert the cards, press the yellow “Eject” button with a small screwdriver on the top of the device, for example. The respective SIM card slot is pushed out. If the TK800 is not operated in dual SIM mode, use the SIM card slot “SIM1”.

Then insert the SIM card. The SIM card slot is not hot-pluggable. The router must be restarted after inserting the SIM card.

2.5 2.5. Antennas Installation

Plug the antennas onto the SMA connectors and turn the external attachment on the antenna cable until the connection is tight.

Hinweis

For optimal performance, place the antennas at least 20 cm apart.

2.6 2.6. Installation of the Power Supply

Remove the terminal block from the top of the router. Loosen the corresponding screws on the terminal block and route the wires to the corresponding terminals. The terminals are marked accordingly on the top of the router. Tighten the screws and then reinsert the connector block into the router.

To ground the device, use the grounding screw on the device.

Hinweis

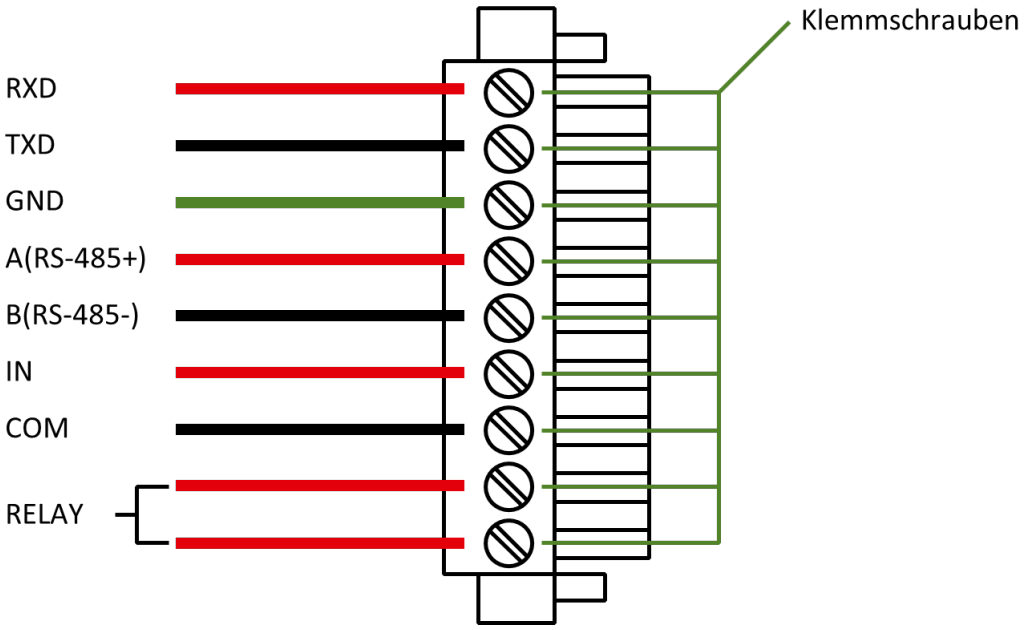
To prevent interference due to electromagnetic influence, the housing of the router must be grounded via the grounding screw.

2.7 2.7. Cable Connections

Connect the router to your PC via a network cable (RJ45). We recommend port FE 0/2 for all TK8x2 models and port FE 1/4 for all TK8x5 models.

2.8 2.8. Connection of the Serial Interfaces and I/O's

For the connection of the serial interfaces and the I/O's you will find a terminal block on the front of the device. The individual contacts for this are labeled on the front of the device. Connect the lines according to these labels. The "IN" contact here represents the digital input, while the output is labeled "Relay". "COM" represents the ground. This is a potential-free contact, i.e. what you put in at the IN contact comes out again at the relay contact, provided the contact is closed. Switching can be done via SMS and via the web interface. At 230 VAC the contact can be loaded with 2 Ampere. During installation, please remove the connection block from the device and connect the individual wires to the corresponding terminals. Then plug the connection block back onto the device.



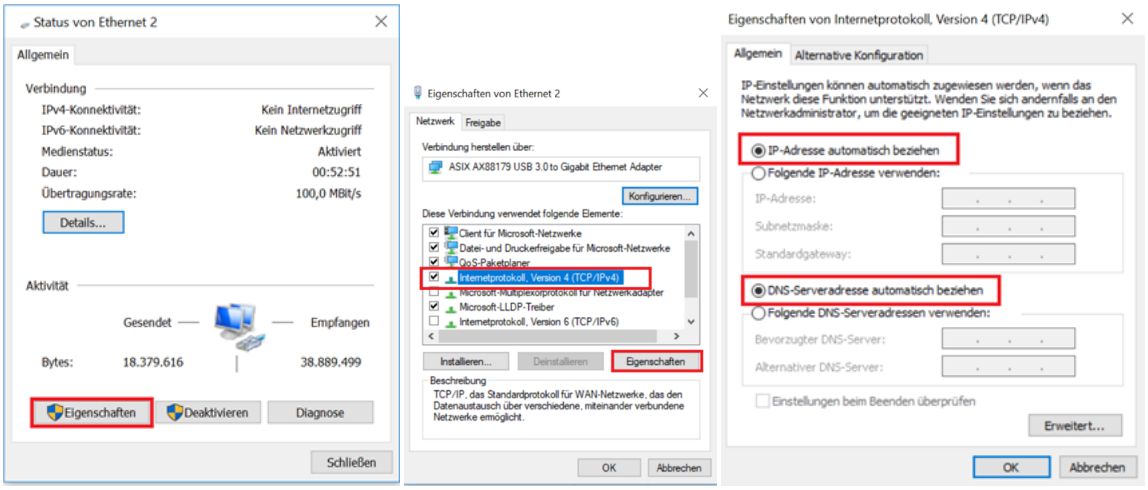
Hinweis

This chapter describes only routers in the versions with serial interfaces and I/Os TK8XXX-EX.

2.9 2.9. Startup of the Router

2.9.1 2.9.1. Automatic Configuration (DHCP)

Configure the PC so that it works as a DHCP client (obtain IP address automatically). Connect the PC with a network cable to the interface FE0/2 or FE1/1 - FE1/4 (TK8X5 variants only). The PC is then assigned an IP address, standard gateway and DNS server by the router. The following figure shows the configuration process via DHCP on a PC with the Windows 10 operating system. The settings can be accessed via the Network and Sharing Center in Windows 10.



After configuring the IP address of the PC and connecting to the router, open a web browser.

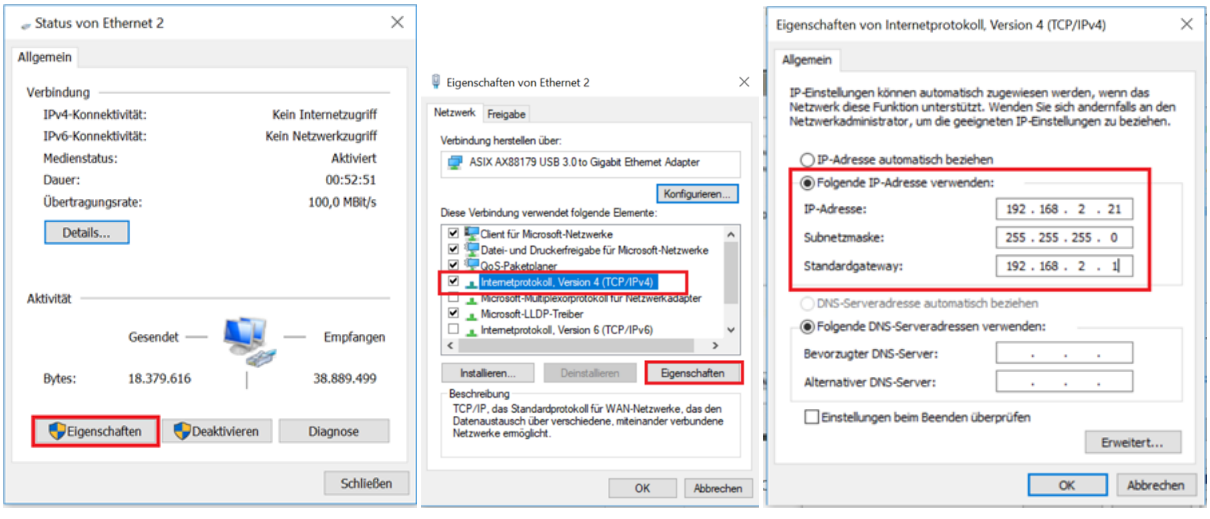
Then enter "**http://192.168.2.1**" in the address line of your browser (e.g. Google Chrome). After confirming with the "Enter" key, a pop-up appears as the login page of the router. Enter the username (default: "***adm***") and password (default: "***123456***") here and confirm with "Enter". Now you will be redirected to the configuration web page. Now configure the router according to your requirements.

To check if you are connected to the Internet, select ***Network*** > ***Cellular*** > ***Status*** from the navigation panel. Here you can see the data of the cellular unit in the router. Alternatively, simply open a web page in your browser.

IP:	192.168.2.1
Username:	adm
Password:	123456

2.9.2 2.9.2. Manual Configuration

Configure your PC so that it is in the same subnet as the router (192.168.2.1). The subnet mask must be 255.255.255.0. The following image shows the process of configuring the IP address on a PC with the Windows 10 operating system.



After configuring the IP address of the PC and connecting to the router, open a web browser.

Then enter "**http://192.168.2.1**" in the address line of your browser. After confirming with the "Enter" key, a pop-up appears as the login page of the router. Enter the user name (default: "***adm***") and the password (default: "***123456***")

and confirm with “Enter”. Now you will be redirected to the configuration web page. Now configure the router according to your requirements.

To check if you are connected to the Internet, select ***Network > Cellular > Status*** from the navigation panel. Here you can see the data of the cellular unit in the router. Alternatively, simply open a web page in your browser.

IP:	192.168.2.1
Username:	adm
Password:	123456

2.10

2.11 2.10. LED status lamps

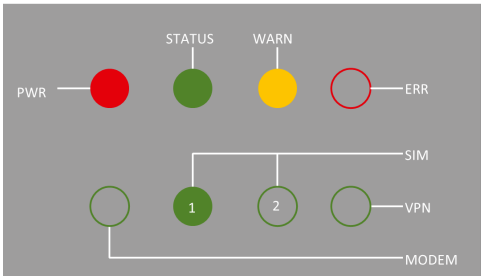
2.11.1 *Symbol explanation*

= LED leuchtet = LED leuchtet nicht = LED blinkt

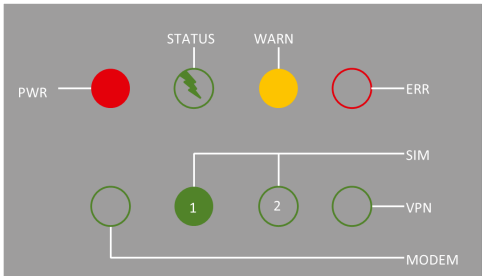
Hinweis

There are two SIM card LEDs. When the router boots up, the SIM card LED for SIM card 1 is lit. In all other cases, the SIM card reception indicator is lit:

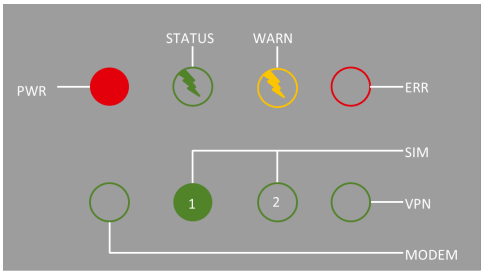
Systemstart:



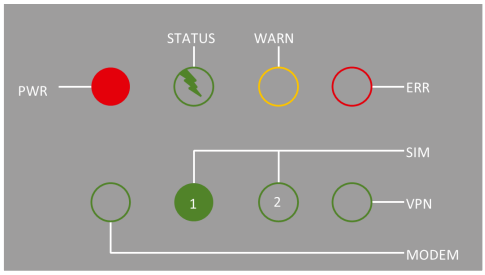
Systemstart erfolgreich:



Dial-in:



Dial-in successful:



Reset erfolgreich:

STATUS WARN STATUS WARN

Firmwareaktualisierung:

SIM

PWR ERR PWR ERR

SIM

VPN

MODEM MODEM

2.11.2 *Signal strength*

Signal: 1-9

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

Signal: 10-19

(Router operates normally)

Signal: 20-31

(Perfect signal level)

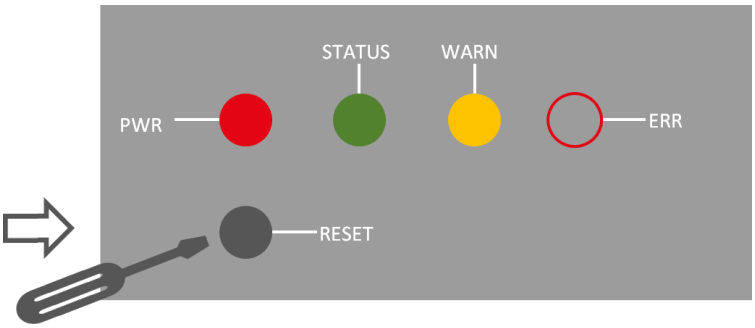
2.12 2.11. Factory Reset

2.12.1 2.11.1. Hardware Method

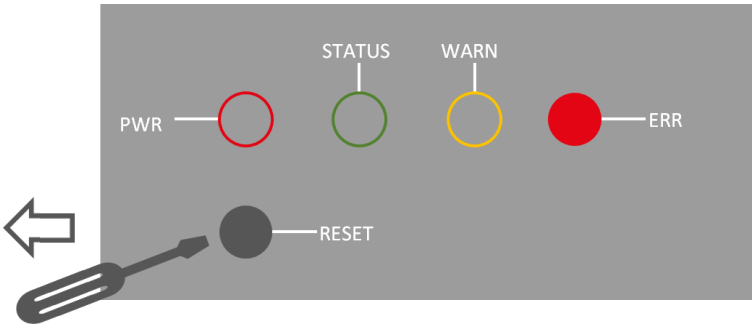
Symbol explanation

 = LED lights up  = LED does not light up  = LED flashes

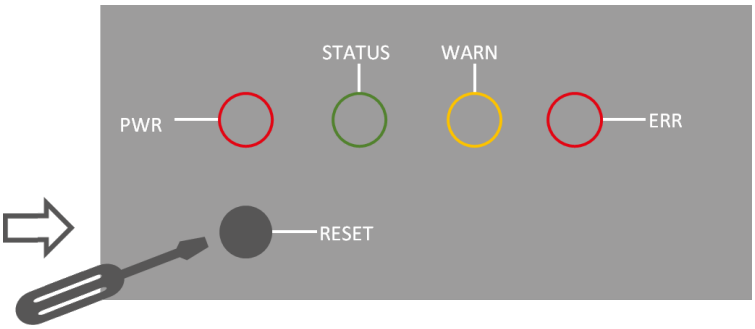
1) Press and hold the RESET button while turning on the TK800:



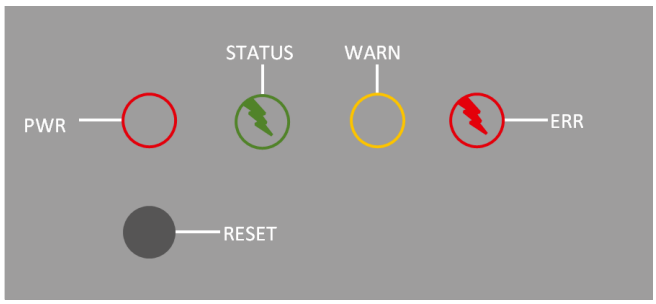
2) As soon as the ERROR LED lights up (approx. 10 seconds after switching on), release the RESET key:



3) After a few seconds, the ERROR LED no longer lights up. Now press the RESET key again until the error light flashes and then release the key:



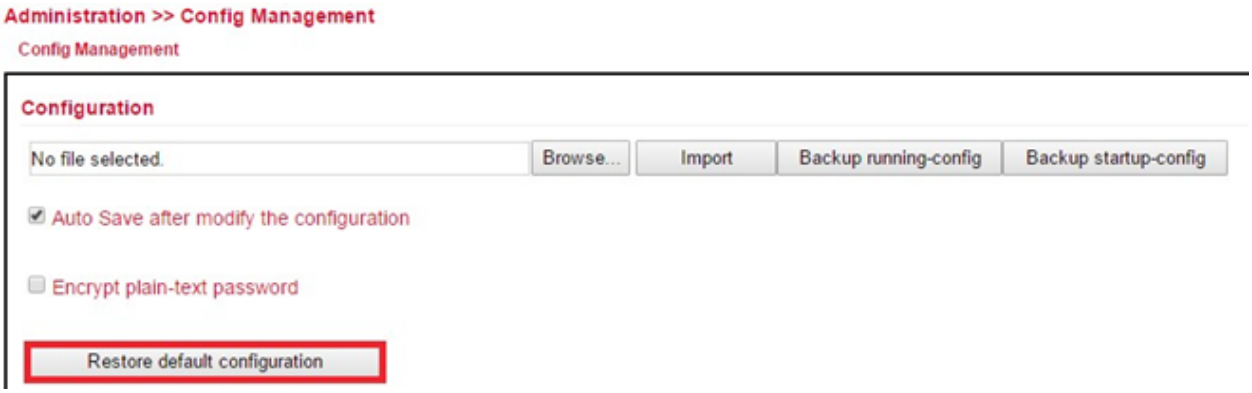
4) Now the ERROR and STATUS LED lights will flash, indicating that the factory reset was successful.



Factory default settings	
IP:	192.168.2.1
Netmask:	255.255.255.0
Username:	adm
Password:	123456
Serial parameter:	115200-N-8-1

2.12.2 2.11.2. Web Method

1) Go to the ***Config Management*** submenu via the ***Administration*** menu:

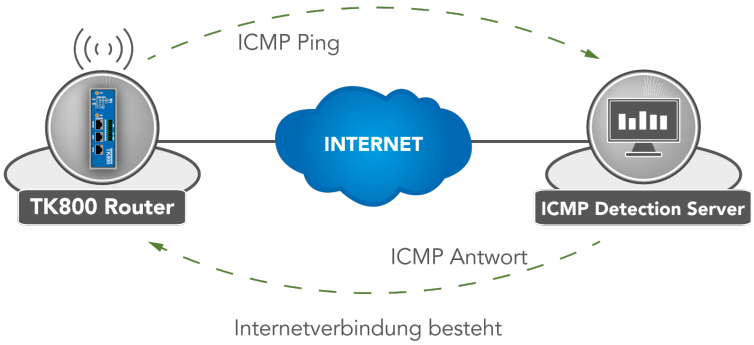


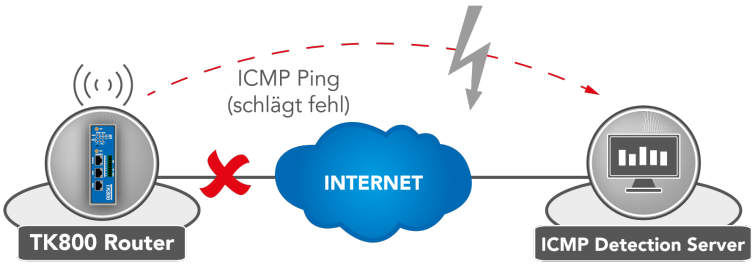
2) Click ***Restore Default Configuration*** to reset the TK800 to its default settings.
After a few seconds you will receive the following message. The router has now been successfully reset.

3) After clicking ***reboot*** the router reboots to factory defaults.

2.13 2.12. Watchdog

2.13.1 2.12.1. Self Monitoring of the Router

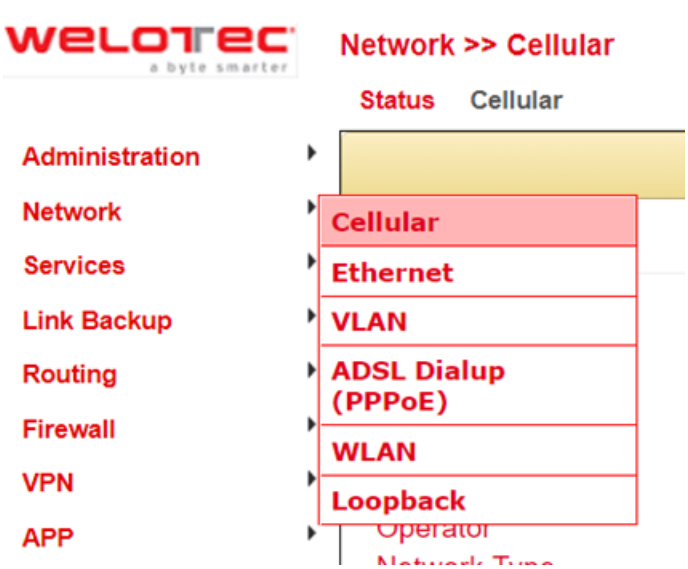




Watchdog greift

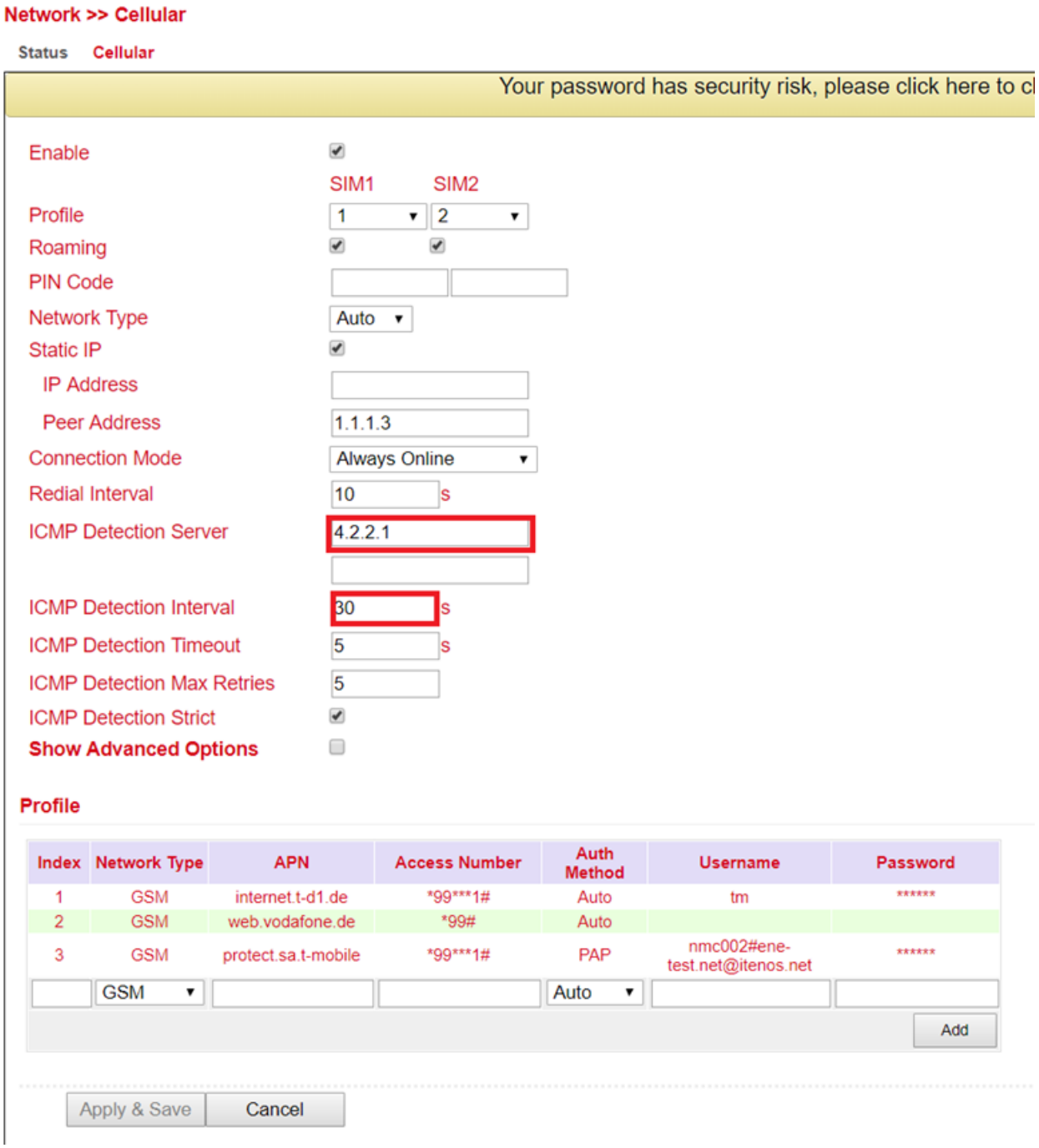
The watchdog monitors the router with regard to the Internet connection. The router itself checks whether there is an Internet connection as required. For this purpose, it sends ICMP packets to an individually defined server (ICMP detection server). If this query fails, the router first automatically restarts the dial-up, then the modem, and if necessary the entire system. The watchdog ensures a reliable Internet connection in the mobile network. This ensures that the router is almost always available.

1) Go via the menu item ***Network*** to the submenu item ***Cellular***.



2) Select the ***Cellular*** tab

3) Now enter a suitable ***ICMP Detection Server*** in the corresponding field and change the ***ICMP Detection Interval***.



Note: The registered ICMP detection server should have a very high accessibility. A server from Google is no longer suitable for this, since the ICMP requests are blocked there.

2.14 2.13. Port Mapping / Port Forwarding

2.14.1 2.13.1. Access to Connected Devices via the Internet

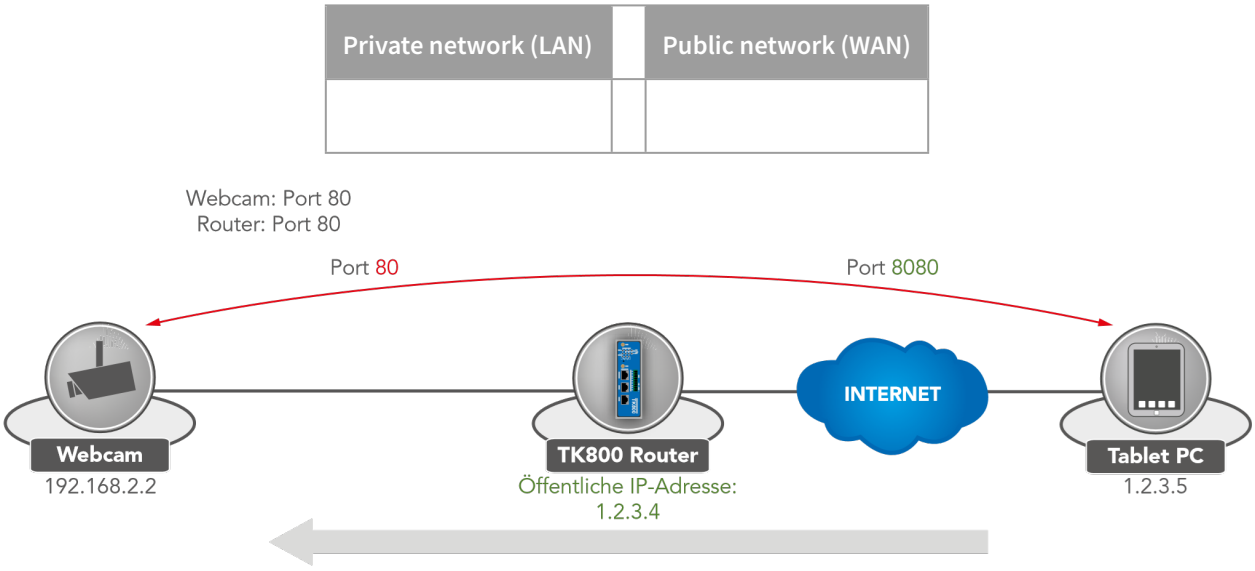
To access devices connected to the Welotec router via the Internet, port mapping or port forwarding can be used. This is configured in the TK800 router via NAT rules.

Hinweis

Port mapping requires a public IP address in the mobile network (Public IP). If necessary, ask your mobile network provider or service provider about this!

The instructions refer to all TK800 routers with firmware ***1.0.0.r10406*** or higher.

The following image illustrates the application example (http uses TCP port 80 by default):



Package source: 1.2.3.4.8080 Destination: 192.168.2.2.80	Package source: 1.2.3.5.8080 Destination: 1.2.3.4.8080

Explanation:

Welotec Router	
LAN IP address:	192.168.2.1
Subnet mask:	255.255.255.0

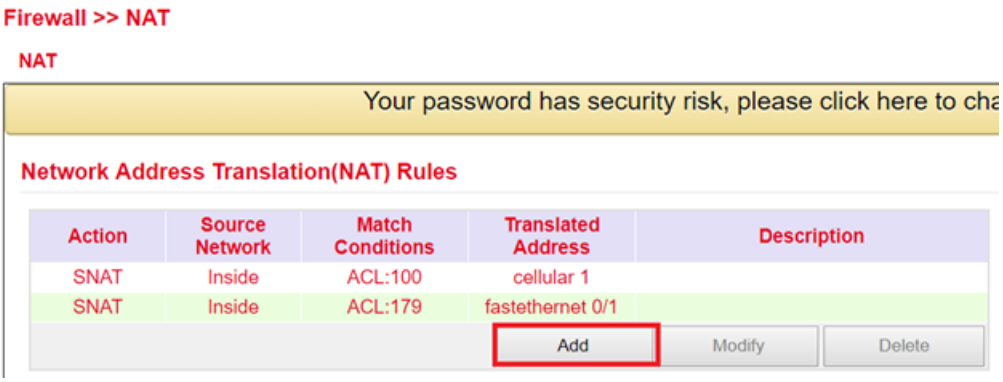
IP camera	
LAN IP-Adresse:	192.168.2.2
Subnet mask:	255.255.255.0
Standard Gateway	192.168.1.1

The IP camera has an interface that can be reached with a browser via **http://192.168.2.2** (note: http protocol has TCP port 80).

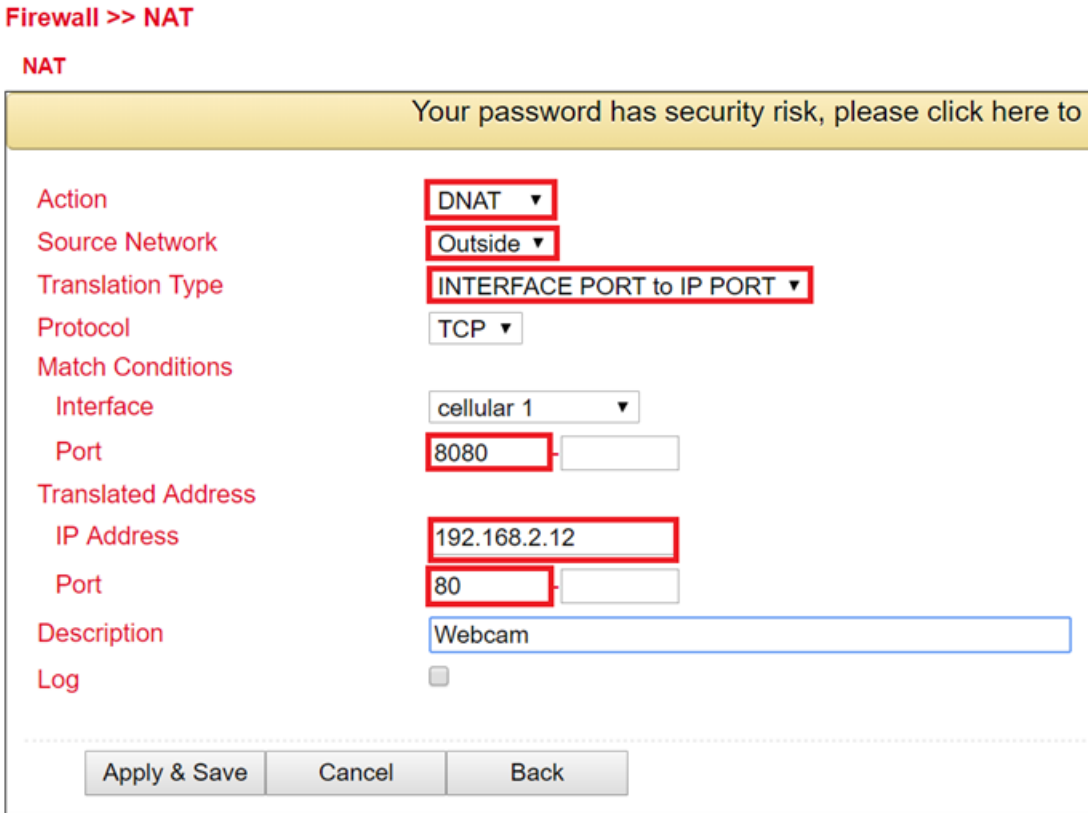
2.14.2 2.13.2. Port Mapping Guide

1) Go to the submenu item ***NAT*** via the menu item ***Firewall***

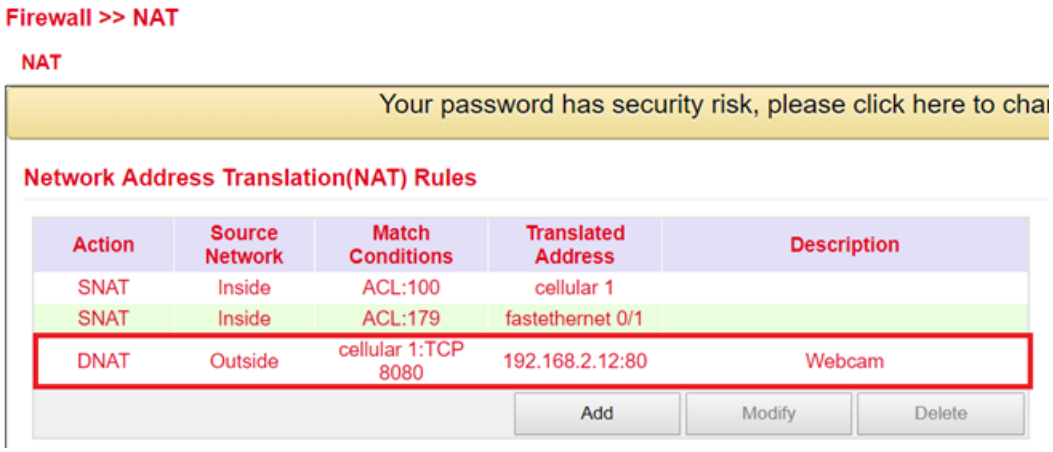
2) Now add a new NAT rule with ***Add***



3) Enter the data as in the example



4) Afterwards the NAT rule appears in the ***Network Address Translation (NAT) Rules*** table as shown below



The rule is now active. The corresponding services restart and the port mapping is fully set up.

For a working port mapping it is helpful to check the settings of the connected devices in advance. The following checklist is helpful (according to the example above):

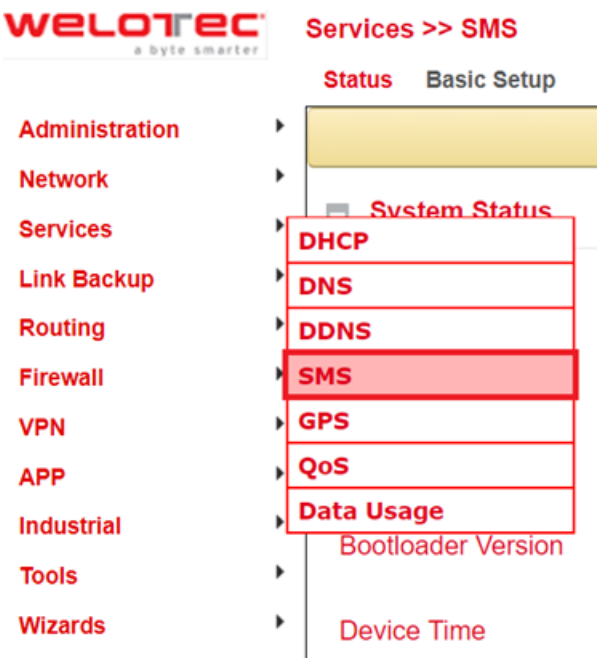
- Does the camera have the IP address 192.168.2.12?
- Does it respond at “ping 192.168.2.12”?
- Is the web interface of the camera accessible via **http://192.168.2.12**?
- Is the Welotec router entered as the default gateway for the camera (192.168.2.1)?

2.15 2.14. SMS Functions

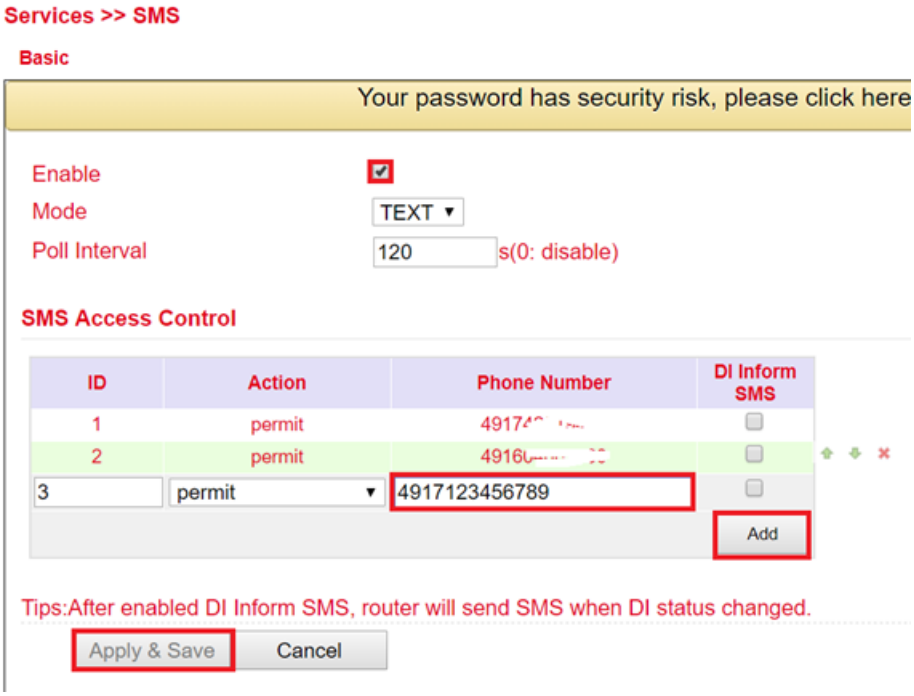
The TK800 can be reached by SMS from the outside and reacts to various commands sent by SMS. One has the possibility to query the status of the device, to start / stop the dial-up or to restart the device.

2.15.1 2.14.1. Status Request / Restart

1) Go via the menu item ***Network*** to the submenu item ***SMS***



2) Click the ***Enable*** checkbox to turn on the function



3) Enter in the table ***SMS Access Control*** the phone numbers (Phone Number) (format 4917123456789, **no 0049 or +49!**), which are allowed to send SMS to the router. Enter "***permit***" as action.

If now an SMS with the content ***show*** is sent to the mobile phone number of the router, the router sends its current status as response

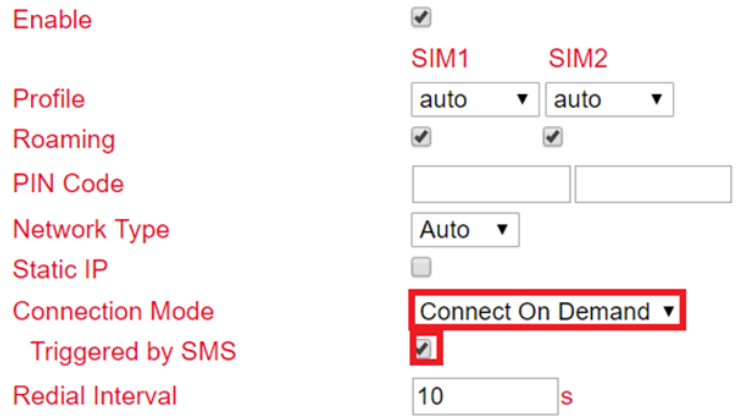
If an SMS with the content ***reboot*** is sent to the router, it will reboot. You can also monitor this process in the log of the router

2.15.2 2.14.2. Connecting or Disconnecting from the Internet

After successful configuration, you can also control the router's Internet connection via SMS. However, this requires the router to be set to "Connect On Demand"!

1) Go to the submenu item ***cellular*** via the menu item ***network***.

2) Now select the ***cellular*** tab



3) Under ***Connection Mode***, select the ***Connect on Demand*** mode and activate the ***Triggered by SMS*** field.

Now you can send the following commands to the router via SMS:

- *cellular 1 ppp down* - disconnects from the Internet

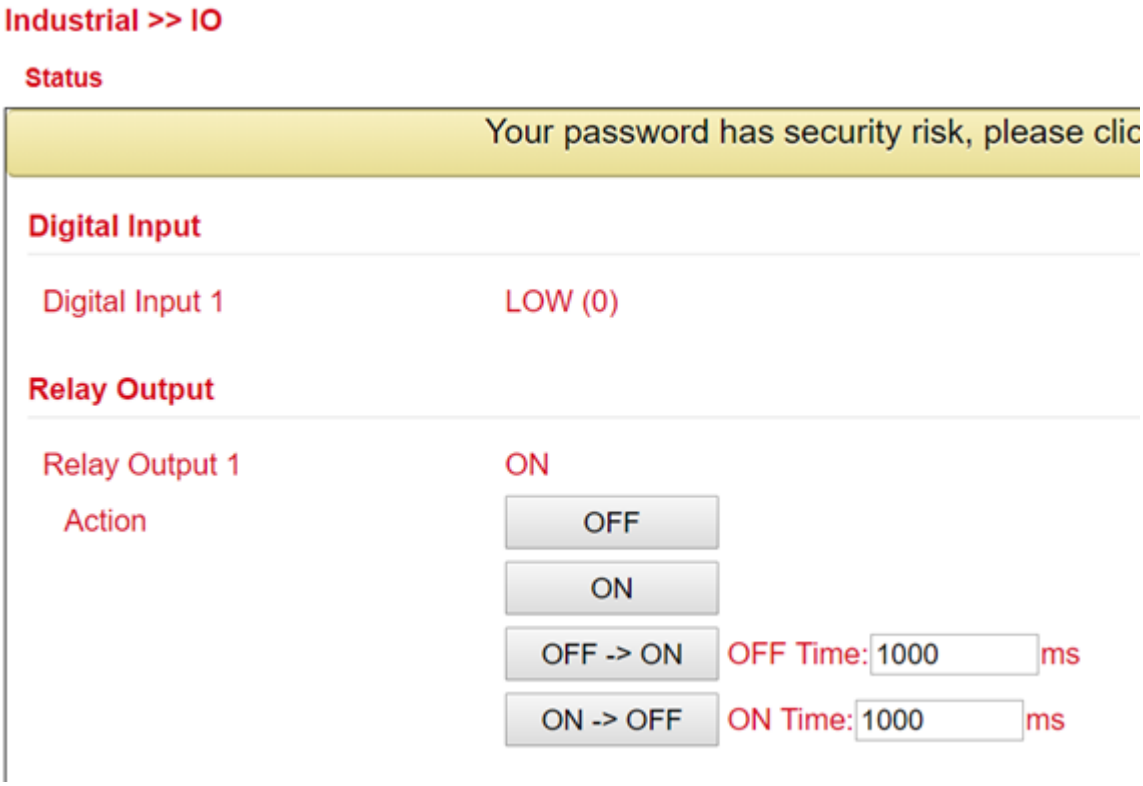
```
info    Jan 1 01:40:35    redial[822]: receive a sms from +49[redacted]
info    Jan 1 01:40:35    redial[822]: receive disconnect command, hangup!
info    Jan 1 01:40:35    pppd[2151]: Hangup (SIGHUP)
```

- *cellular 1 ppp up* - establishes the Internet connection

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

2.15.3 2.14.3. Switch digital relay on or off

Another important SMS command is to switch the digital relay on or off via SMS.

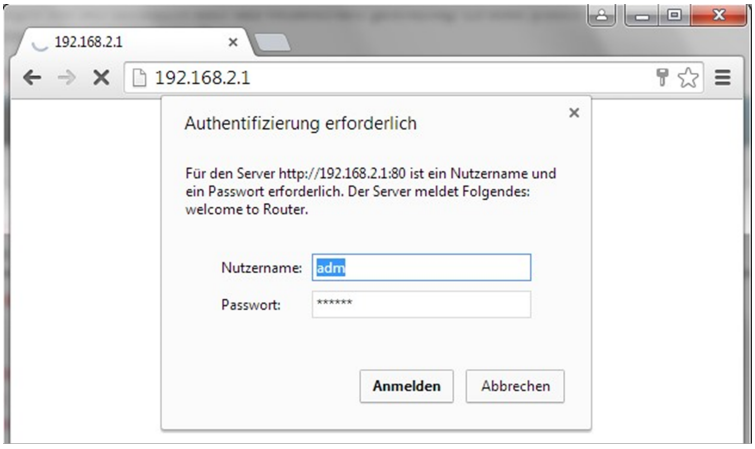


The following SMS commands can be used for this

- *io output 1 on - switches on the relay*
- *io output 1 off switches off the relay*

3 3. WEB Configuration

The TK800 series routers have a built-in web server for configuration. Open **http://192.168.2.1** in the browser. Enter the user name (default: ***adm***) and password (default: ***123456***) and confirm with ***Login***.



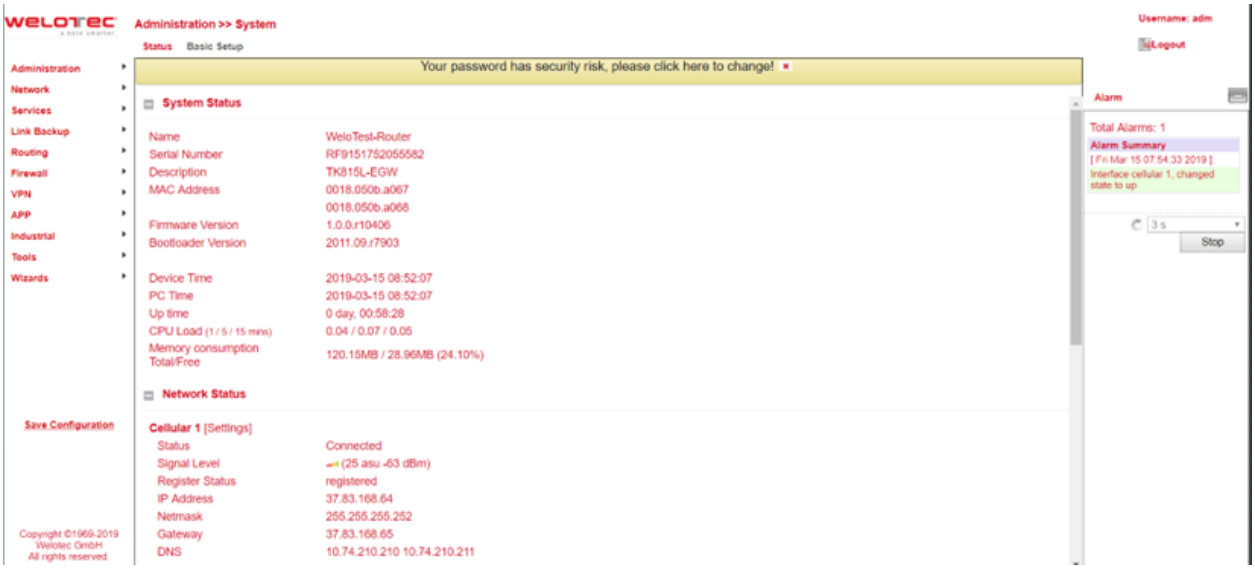
Hinweis

For security reasons, the password should be changed after the first login. Choose a password with at least 10 digits, upper and lower case letters, special characters and numbers.

Tipp

The router allows parallel access of up to four users via the web interface. However, it should be avoided to configure the router simultaneously.

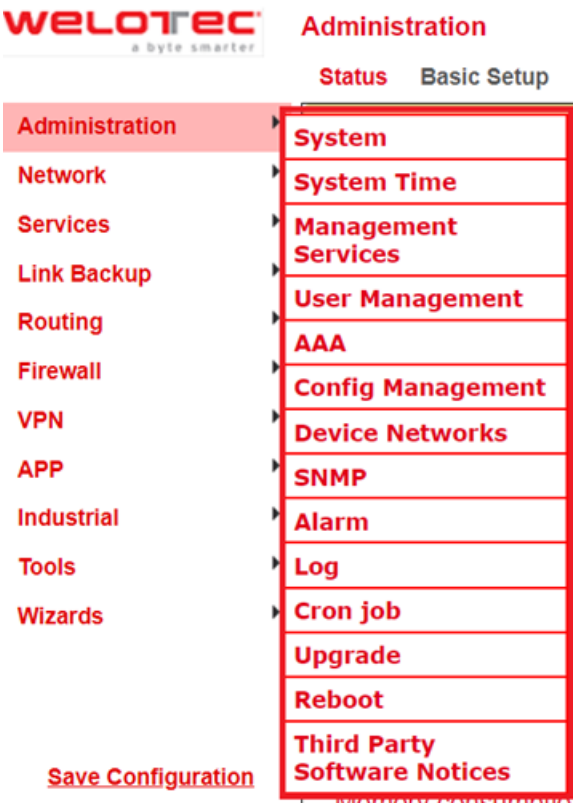
After the successful login, the web interface of the router appears.



The web interface of the TK800 is divided into 4 areas. On the left side is the ***Main navigation*** with the items Administration, Network, etc. In the upper area is the ***Detail navigation***. In this example with Status (active) and Basic Setup. In the middle of the web interface the current status and configuration options are shown. On the right side active alarms are displayed.

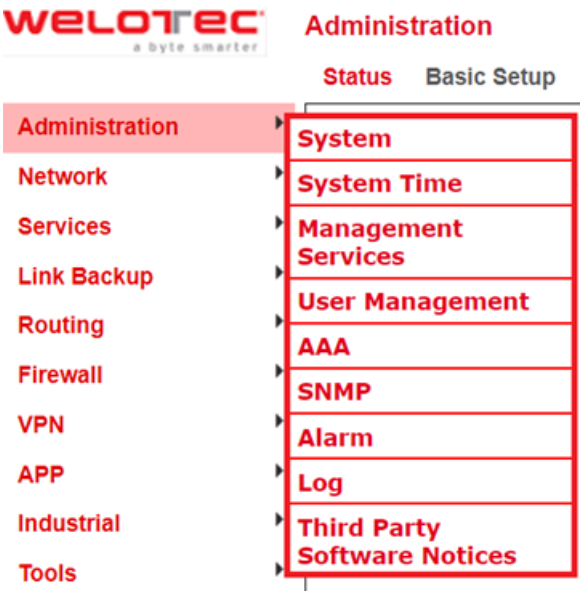
3.1 3.1. Administration

On the left side you will find the menu item "***Administration***". Touching it with the mouse opens a ***submenu***. In the administration area is the status overview and the configuration for the administration of the router.



Hinweis

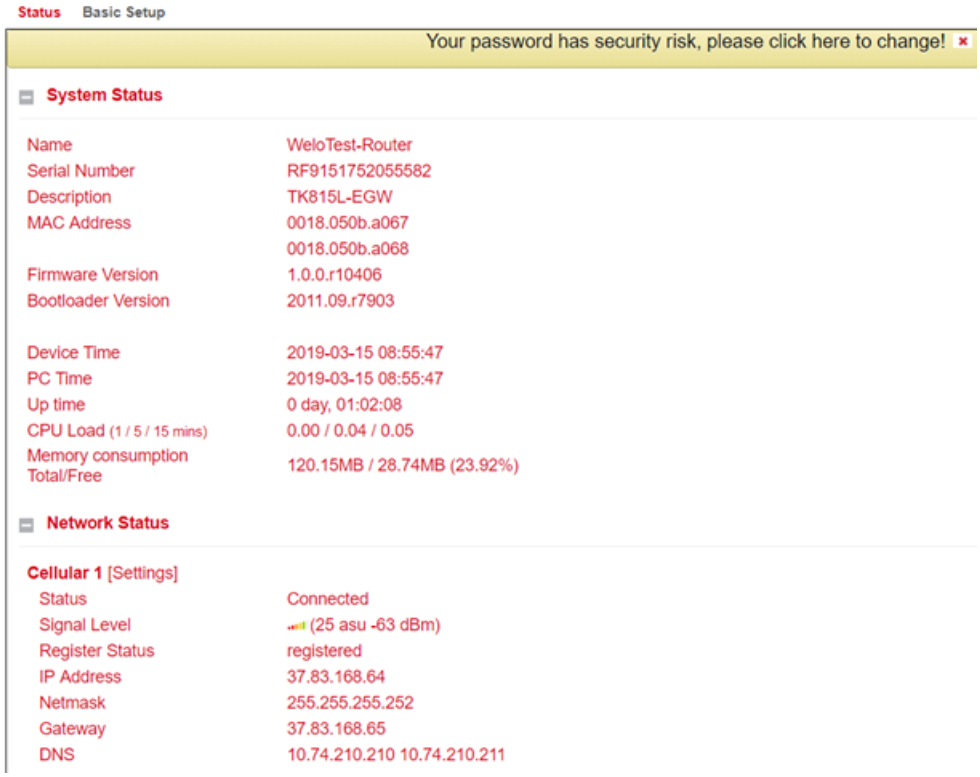
With Restricted user rights (not administrator) some items are missing in the menu. Restricted users cannot configure the router, the ***Apply & Save*** option is missing.



3.1.1 3.1.1. System

3.1.1.1. Status

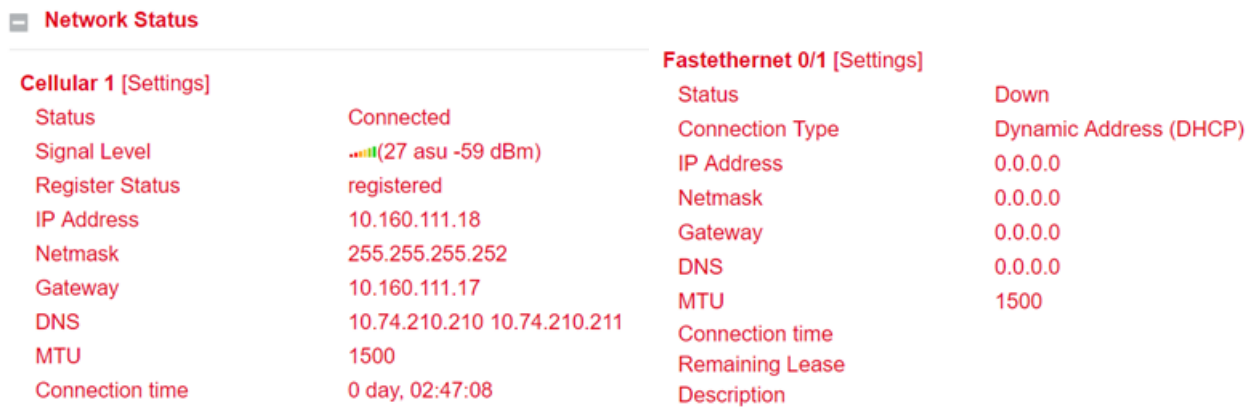
Under ***Administration*** > ***System*** > ***Status*** you will find the most important ***Status*** information of the router at a glance. Via the button ***Sync Time*** the time of the router can be synchronized with the time of the connected PC. If you use the default password for login (123456), a yellow bar will indicate that this is a security risk and should be changed. You can do this by clicking on the hint. We strongly recommend that you do this for security reasons!



The Network Status is located under the System Status. By clicking on the gray *[+]* the information about the individual network interfaces appears. Here you will find all important information about the status of the individual interfaces.

Tipp

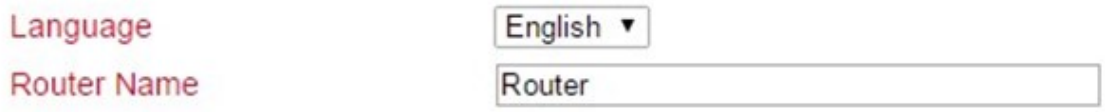
By clicking on *[**Settings**]* next to the individual interfaces (e.g. Cellular 1) you will be taken directly to the configuration of the interfaces.



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

3.1.1.2. Basic Setup

Under ***Administration*** > ***System*** > ***Basic Setup*** you can change the language of the router and the router name. Currently only English is supported as language. The router name can be used as unique name of the router. Here a meaningful name should be chosen.



3.1.2 3.1.2. System Time

To ensure coordination between the TK800 router and other devices, the system time should be the same on all devices and the time zone should be set correctly. Under ***Administration*** > ***System Time*** you will find all the settings for the system time of the TK800 Router. The time can be set manually or automatically updated by a time server via the Simple Network Time Protocol (SNTP). In addition, it is possible to automatically supply devices connected to the router with the current time information via the NTP server.

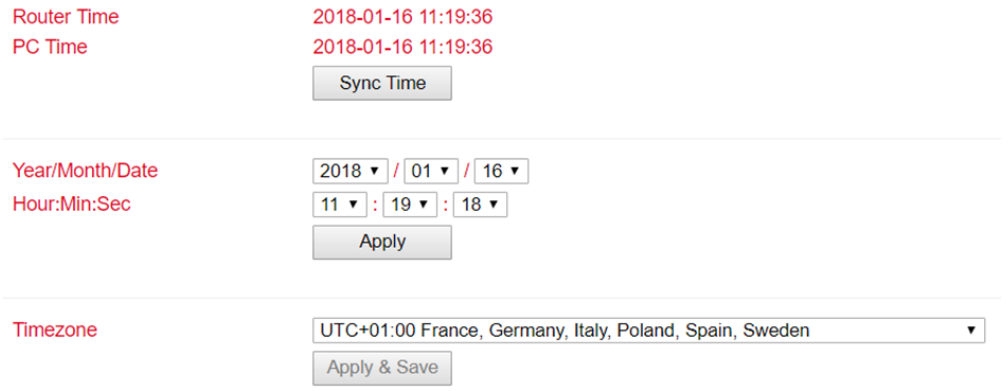
3.1.2.1. System Time Configuration

Under ***Administration*** > ***System Time*** you will find an overview and local settings for the system time of the router. Via ***Sync Time*** you can synchronize the time of the router with the time of the PC.

Among the settings there is also the possibility to set the router time and date manually.

Under ***Timezone*** the current time zone can be selected.

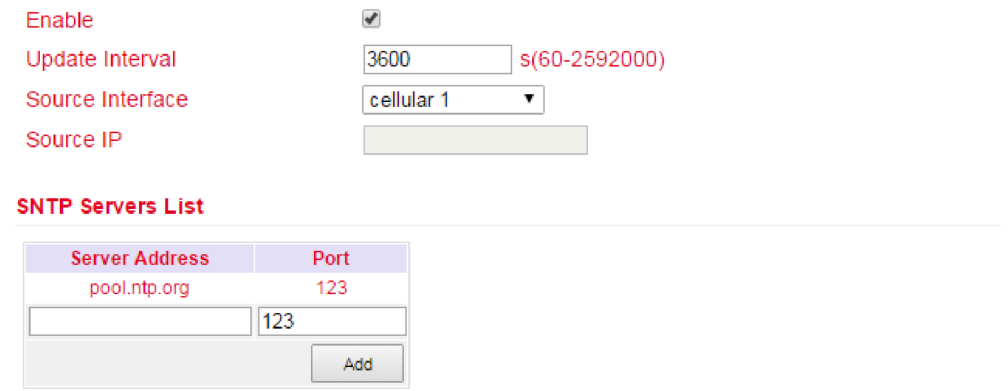
The default is UTC+1 (time zone in Germany, Austria and Switzerland).



3.1.2.2. SNTP Client

SNTP (Simple Network Time Protocol) is a protocol for time synchronization of the clocks of network devices. SNTP provides extensive mechanisms to synchronize the time over a subnet, network, or the Internet. Typically, SNTP can achieve accuracies of 1 to 50 ms, depending on the characteristics of the synchronization source and routers. The goal of SNTP is to synchronize all devices in a network with a clock in order to run distributed applications based on one time source.

Under ***Administration*** > ***System Time*** > ***SNTP Client*** the settings for the current time can be made. The router can then update the time via a public or private time server.



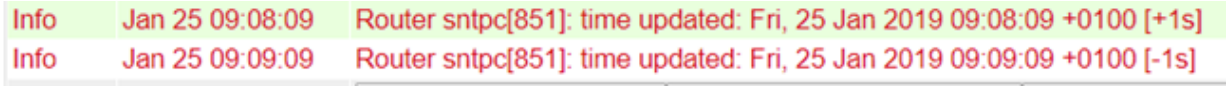
Hinweis

Before setting up an SNTP server, make sure that the SNTP server is reachable. Especially in the case of a domain name, it should be checked whether the DNS server is configured correctly for name resolution.

Hinweis

Either a source interface or a source IP can be configured.

After the successful update of the time, the following appears in the log under ***Administration*** > ***Log***.



3.1.2.3. NTP Server

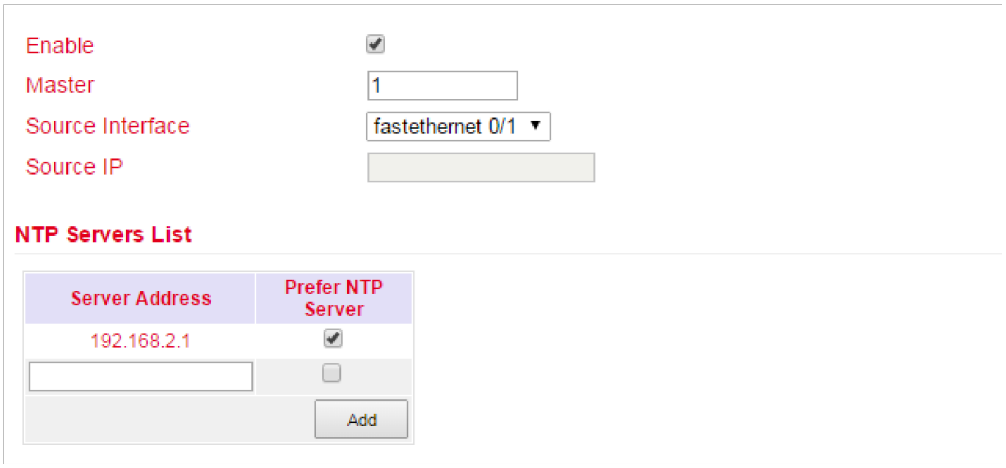
The settings for the time server are located under ***Administration > System Time > NTP Server***. In this case, the TK800 can work as a time server for the connected devices.

Via ***Master*** the stratum can be specified. This indicates how precise the server is. Values between 2 and 15 can be specified. The lower, the closer the router is to an atomic or radio clock (from a topological point of view).

The ***Source Interface*** specifies the interface at which the devices can request the NTP service of the router. Alternatively, a ***Source IP*** can be determined via which the NTP service is provided.

Hinweis

It is important that NTP server and NTP client work independently of each other, this also means that for both NTP client and NTP server an NTP service from the Internet must be entered. For this purpose the address of the NTP service is entered under ***Server Address***. It is possible to enter more than one service.



3.1.3 3.1.3. Management Services

Under ***Administration > Management Services*** the access to the web interface with HTTP and HTTPS as well as to the Command Line Interface (CLI) via Telnet and SSH can be configured.

HTTP

HTTP is the abbreviation for Hypertext Transfer Protocol and is used to access the router's web interface.

HTTPS

HTTPS is the abbreviation for Hypertext Transfer Protocol Secure and uses SSL (Security Socket Layer) for encrypted transmission of HTTP.

TELNET

TELNET is used to access the Command Line Interface (CLI) of the router.

SSH

SSH is the abbreviation for Secure Shell and is an encrypted service comparable to Telnet.

Configuration

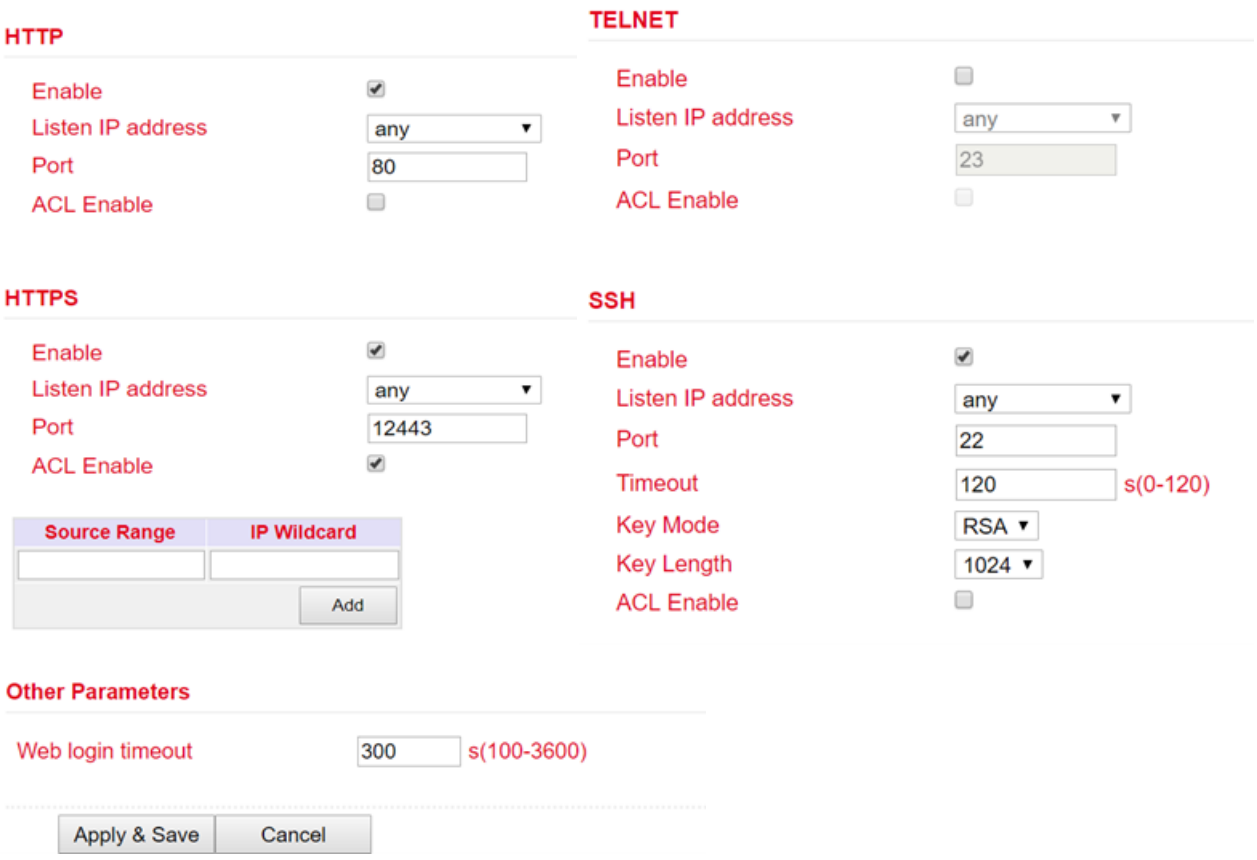
For each service it is possible to select whether it should be activated or deactivated and on which IP address this service may be addressed.

To do this, simply check or uncheck ***Enable***. Under ***Port*** the TCP port for the respective service can be selected. With ACL Enable an access restriction can be set up for each port. If **ACL Enable** is activated, you can enter in the Source Range and IP Wildcard fields which IP address or IP address ranges are allowed to access the router via this port. For SSH, you can also define the ***Timeout*** for an SSH session to the router.

If there is no activity during the timeout period, the connection is terminated. Under ***Key Mode*** and ***Key Length*** the encryption standard and the key length can be selected.

Via ***Other Parameters*** you can set the ***Web login timeout***. This specifies how long a web interface session remains if no input is made.

If the timeout time has expired without any input, then the logged in user will be logged out automatically.



3.1.4

3.1.5 3.1.4. User Management

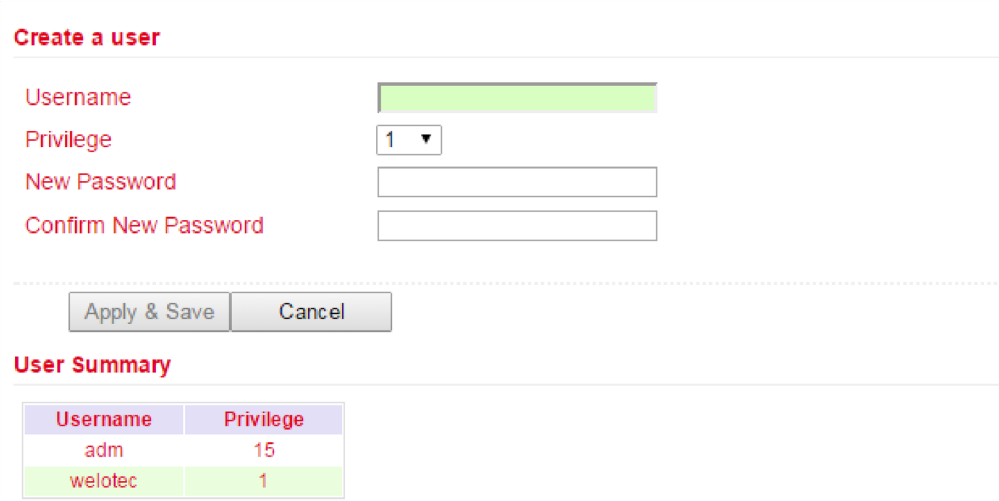
Under ***Administration*** > ***User Management*** the users that have access to the router can be configured. The router distinguishes between the administrator and the standard user. The administrator is created by the system (adm). The administrator can create other standard users with limited rights.

The Administrator user is suitable for configuring and managing the router. The Standard user is suitable for monitoring and checking the router.

3.1.4.1. Create a User

Under ***Administration*** > ***User Management*** > ***Create a User*** you can create additional users.

A ***Username*** and ***Password*** must be created and the ***Permission (Privilege)*** must be entered. Privilege 1 to 14 is for standard users (read only) and privilege 15 for administrators (full access). Under ***User Summary*** you will find a list of all users and their privileges.



Hinweis

A secure password should consist of at least 8 characters and preferably contain upper/lower case, numbers and special characters. The username root is reserved for the operating system of the router.

3.1.4.2. Modify a User

If you want to make adjustments to users, then you can edit them under ***Administration*** > ***User Management*** > ***Modify a User***. Permissions and passwords can be changed.

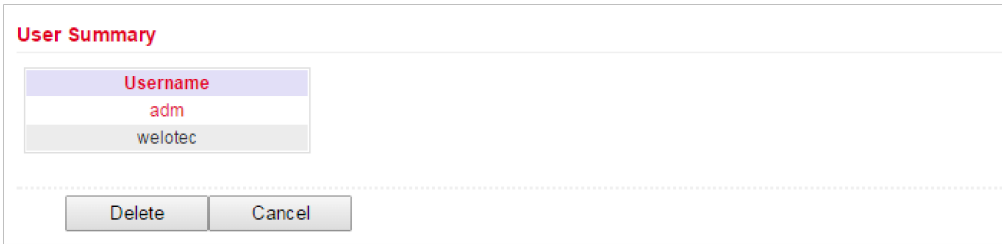
Under ***User Summary*** a user can be selected and then edited under ***Modify a user***.

Hinweis

When selecting the adm user, the user name can be changed, e.g. to admin, as of firmware version V1.0.0.r10406. Please always remember to change the default password (123456) of the adm user to a secure password.

3.1.4.3. Remove Users

Under ***Administration > User Management > Remove Users*** you can delete users from the TK800. Select the user to be deleted under ***User Summary*** and delete it via the ***Delete*** button.



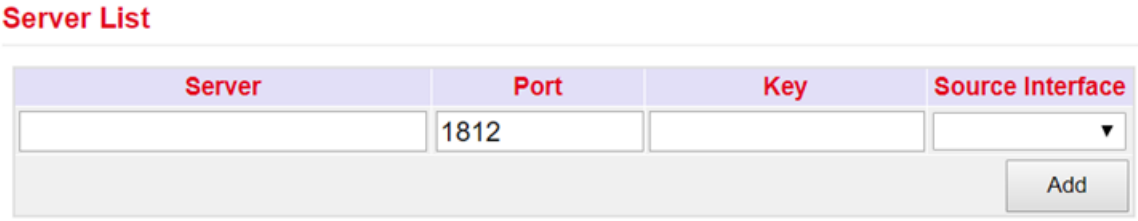
3.1.6 3.1.5. AAA

AAA or Triple-A stands for ***Authentication, Authorization and Accounting***. Here, authentication takes over access control, whether a user is allowed to use the device or the network. Authorization checks which services the user is allowed to use on the network. Accounting ensures that all accesses and events and the use of resources in the network are logged correctly.

With AAA, not all security services have to be used. It is also possible that only one or two services are used in a network. A AAA infrastructure is usually set up as a client-server architecture. The TK800 acts here as AAA client. Radius, Tacacs+ and LDAP are supported for this purpose.

3.1.5.1. Radius

Radius stands for ***Remote Authentication Dial-In User Service*** and is a client-server protocol used for authentication, authorization and accounting.

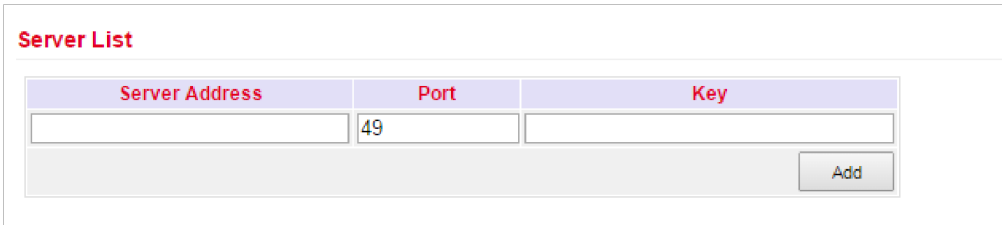


You can enter the FQDN or IP address of the server, the port, the key for the Radius server and the source interface here.

3.1.5.2. Tacacs+

Tacacs+ stands for ***Terminal Access Controller Access Control System*** and is a client-server protocol used for authentication, authorization and accounting.

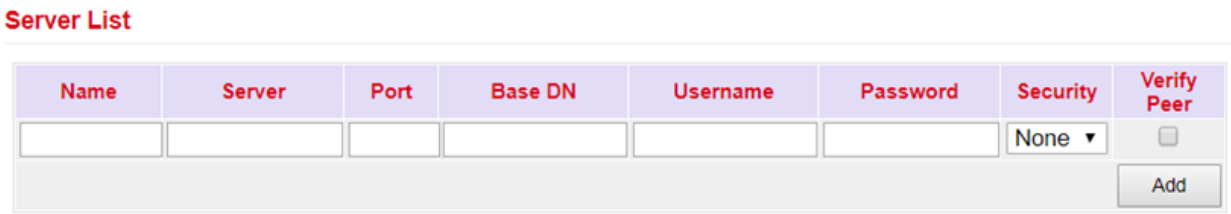
It is used for client-server communication between AAA servers and a Network Access Server (NAS).



You can enter the corresponding data here at ***Server Address***, ***Port*** and ***Key***.

3.1.5.3. LDAP

LDAP stands for ***Lightweight Directory Access Protocol*** and is suitable for querying and modifying information from directory services. LDAP is based on the client-server model.



Enter the data for your LDAP server here.

3.1.5.4. AAA Settings

Service	Authentication			Authorization		
	1	2	3	1	2	3
console	none	none	none	none	none	none
telnet	none	none	none	none	none	none
ssh	none	none	none	none	none	none
web	none	none	none	none	none	none

3.1.7 3.1.6. Config Management

Under ***Administration*** > ***Config Management*** the current configuration can be saved, an existing configuration can be uploaded or the router can be reset to the default configuration.

Importing an existing configuration

To import an existing configuration, an existing configuration file must be selected via ***Browse…***. After the correct file has been selected, the configuration can be imported to the router via ***Import***. After successfully importing the configuration, the router displays a button for restarting. After the restart the router will have the new configuration.

Saving an existing configuration

Via ***Backup running-config*** the current configuration incl. the unconfirmed changes during operation can be downloaded. Via ***Backup startup-config*** the configuration can be downloaded without the unconfirmed changes.

Automatic saving

If the checkmark in front of ***Auto Save after modify the configuration*** is set, all changes in the router are immediately active and are also available after reboot. If the checkmark is not set, the changes will be lost on reboot. However, the changes can alternatively be saved via ***Save Configuration***, the bottom item in the left navigation.

Reset configuration to factory defaults

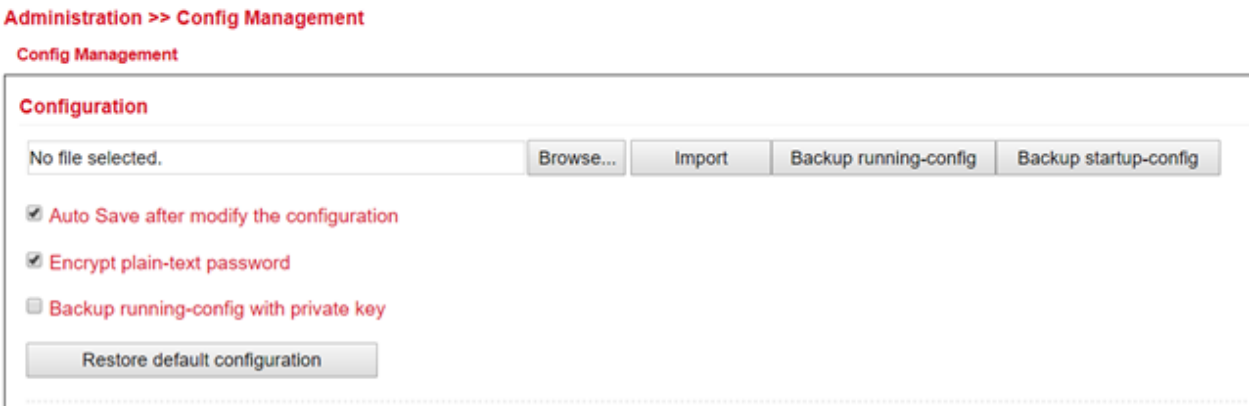
Via ***Restore default configuration*** the configuration of the router can be reset to the default settings.

Encrypt passwords in the configuration file

To prevent passwords in the configuration file from being displayed in plain text, check ***Encrypt plain-text password***.

Back up the running-config including the private key

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



3.1.8 3.1.7. Device Networks

Hinweis

This feature is not supported!

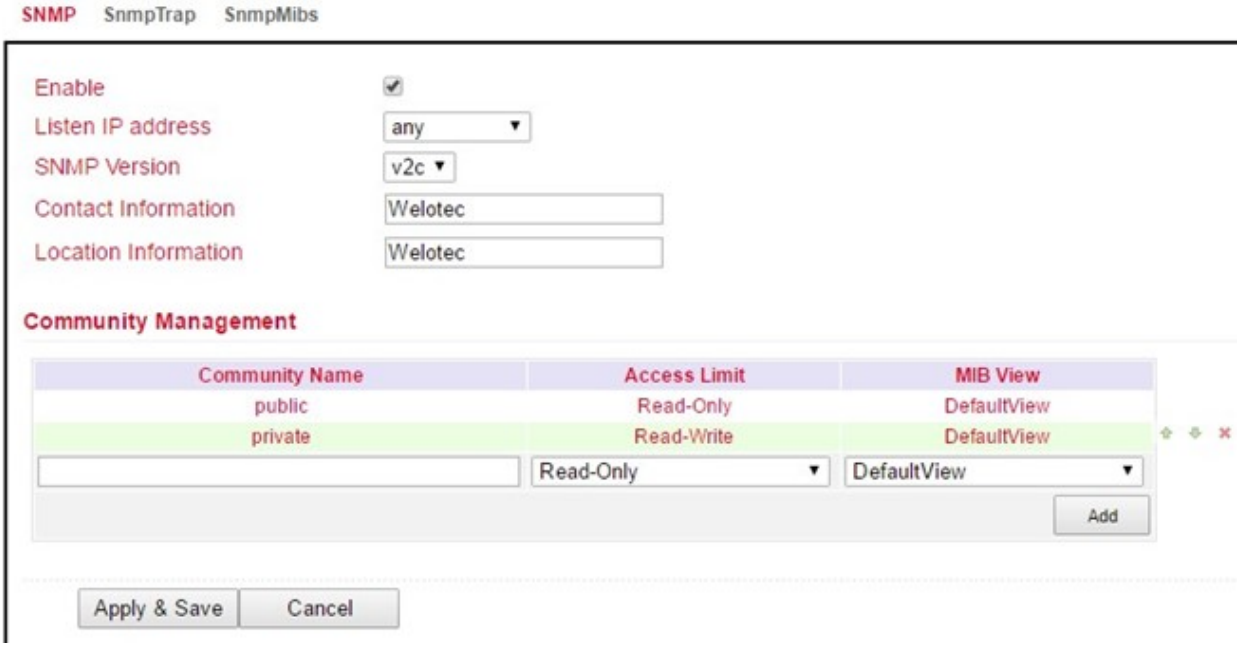
3.1.9 3.1.8. SNMP

The Simple Network Management Protocol (**SNMP**) is a network protocol developed by the IETF to monitor and control network elements (e.g. routers, servers, switches, printers, computers, etc.) from a central station. The protocol regulates the communication between the monitored devices and the monitoring station. SNMP describes the structure of the data packets that can be sent and the communication flow. It was designed in such a way that every network-compatible device can be included in the monitoring.

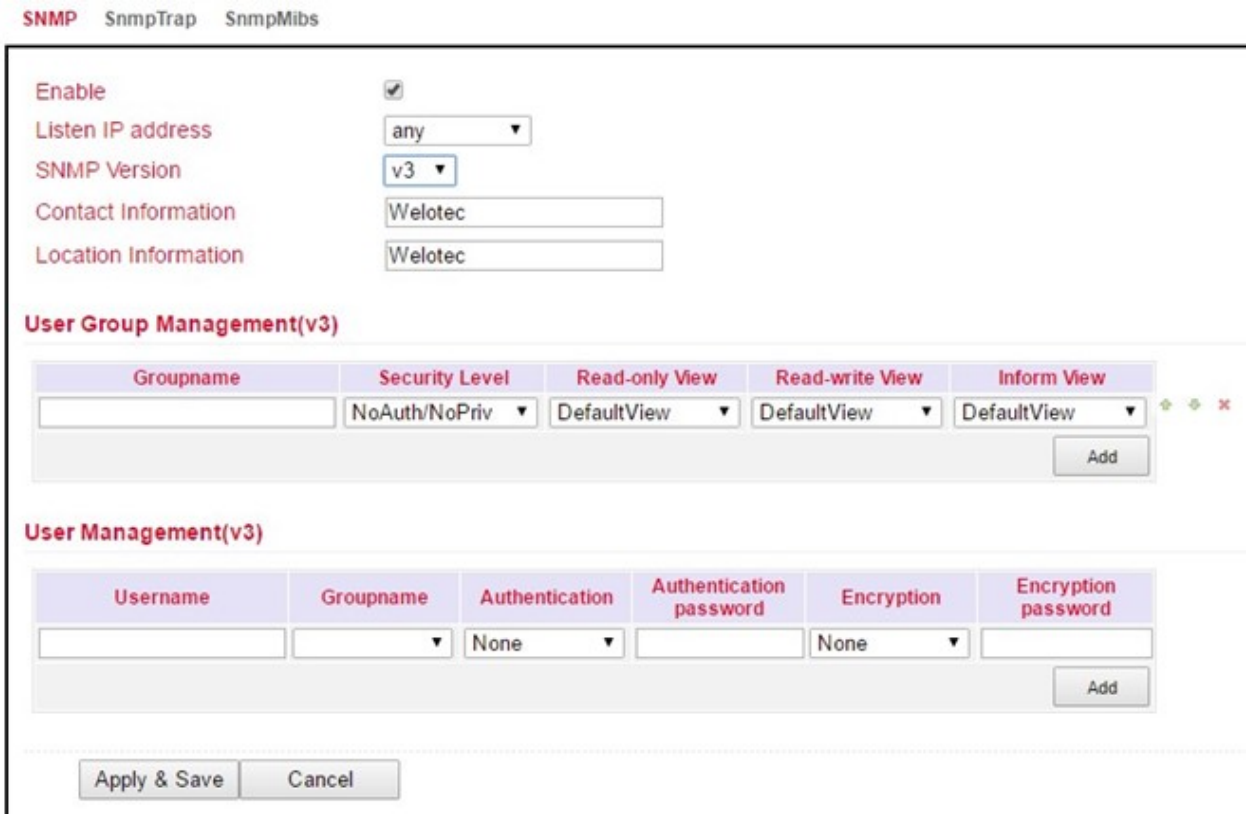
3.1.8.1. SNMP Configuration

SNMP versions v1, v2c and v3 are supported.

SNMPv1 and SNMPv2 use the community name for authentication with ***read-only*** and ***read-write*** rights. The IP address under which the SNMP service is available can be selected under ***Listen IP address***.



SNMPv3 supports user name and password for authentication. A group management is implemented. This is an advantage over the SNMPv1 and SNMPv2 versions, since here individual users can be specifically authorized for access (see following figure).

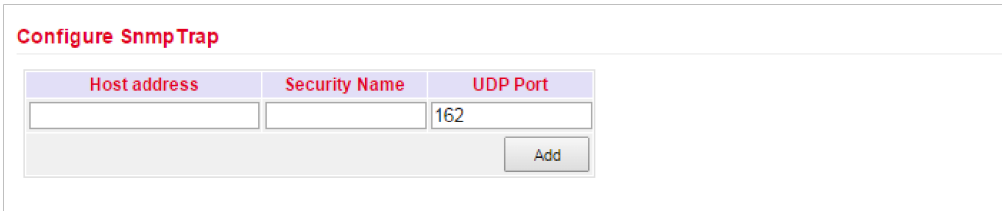


With SNMPv3, there is group and user management.

Authentication supports SHA or MD5.
Encryption supports AES or DES.

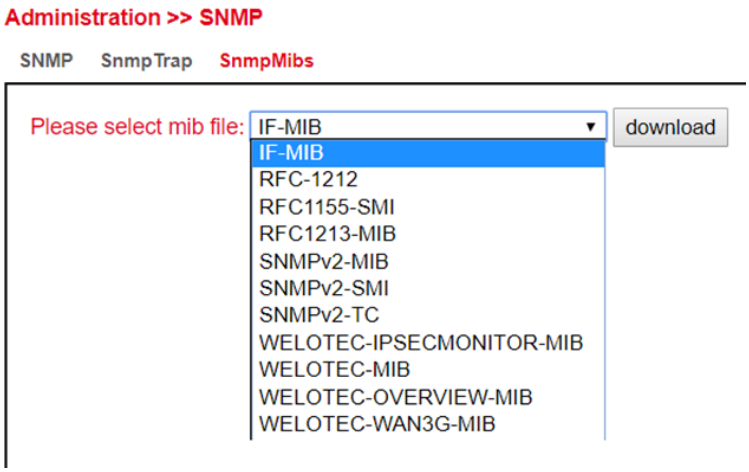
3.1.8.2. SnmpTrap

A SnmpTrap server can be entered. Here the router can actively send SNMP messages to the SNMP management server and does not wait until it receives an SNMP request from the management server.



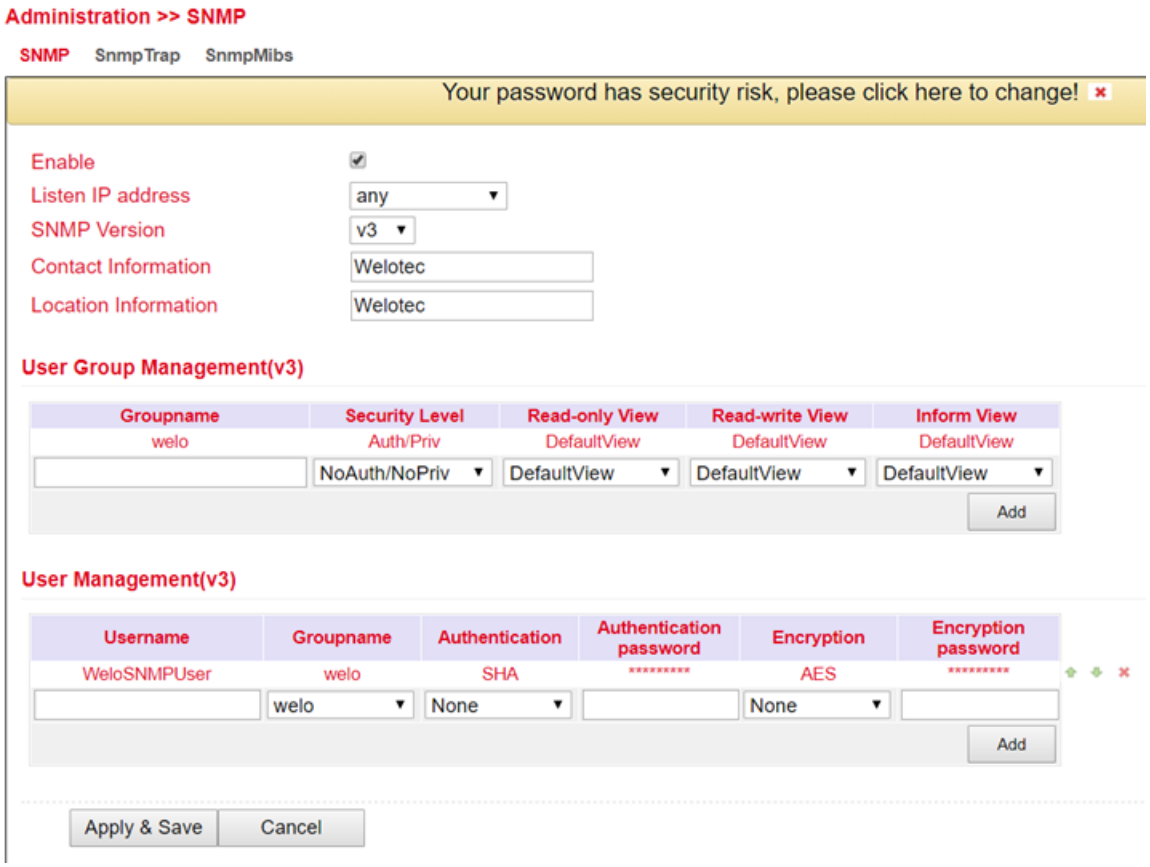
3.1.8.3. SnmpMibs

The ***SnmpMips*** for monitoring the router can be downloaded here and used for corresponding evaluations. Please select the desired MIB file and then click the download button.



3.1.8.4. Read SNMP Mibs using SNMPWALK.

1) ***Configure SNMP,*** such as shown below:



Read out the data entered above via SMTPWALK on e.g. a LINUX computer:

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

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

2) ***Download MIBS from TK800***

3) **Read MIBS** (either via a LINUX computer or a common MIB browser)

mkdir -p .snmp/mibs cp Downloads/WELOTEC* .snmp/mibs/ after that the following MIBS are available:

WELOTEC-MIB

WELOTEC-OVERVIEW-MIB

WELOTEC-PORTSETTING-MIB

WELOTEC-SERIAL-PORT-MIB

WELOTEC-SYSTEM-MAN-MIB

WELOTEC-WAN3G-MIB

3) **Start SNMPWALK** (either via a LINUX computer or a common MIB browser)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

WELOTEC-MIB::ihWan3g.1.2.1.3.0 = “”

WELOTEC-MIB::ihWan3g.1.2.1.4.0 = “”

WELOTEC-MIB::ihWan3g.1.2.1.5.0 = “”

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

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

WELOTEC-MIB::ihWan3g.1.2.3.1.0 = “”

WELOTEC-MIB::ihWan3g.1.2.3.2.0 = “”

WELOTEC-MIB::ihWan3g.1.2.3.3.0 = “”

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

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

WELOTEC-MIB::ihWan3g.1.2.3.6.0 = “”

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

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

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

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

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

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

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

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

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

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

WELOTEC-MIB::ihWan3g.1.3.3.1.0 = “”

WELOTEC-MIB::ihWan3g.1.3.3.2.0 = “”

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

WELOTEC-MIB::ihWan3g.1.3.3.4.0 = “”

WELOTEC-MIB::ihWan3g.1.3.3.5.0 = “”

WELOTEC-MIB::ihWan3g.1.3.3.6.0 = “”

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

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

WELOTEC-MIB::ihWan3g.1.3.3.9.0 = “”

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

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

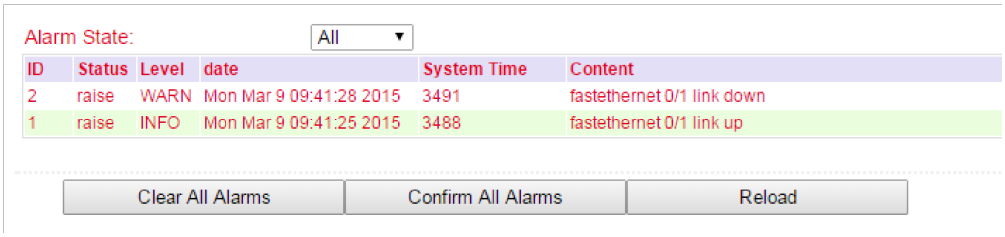
WELOTEC-MIB::ihWan3g.1.3.4.3.0 = Gauge32: 0

3.1.10 3.1.9. Alarm

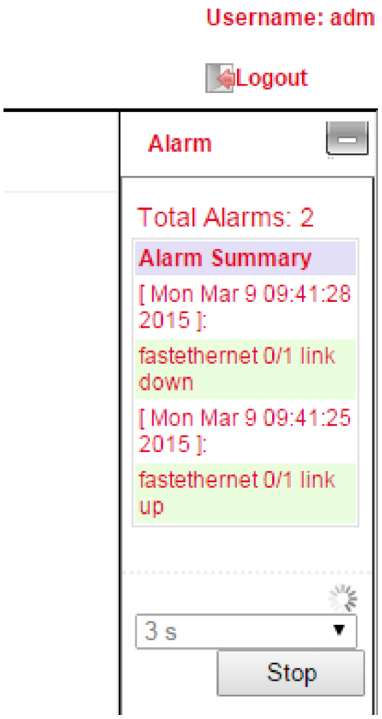
3.1.9.1. Status

The alarm status shows an overview of the triggered alarms.

In this example, INFO message ID 1 shows that Fastethernet port 0/1 has been connected. ID 2 shows a warning message that the Fastethernet port 0/1 has been disconnected (Fig.1).

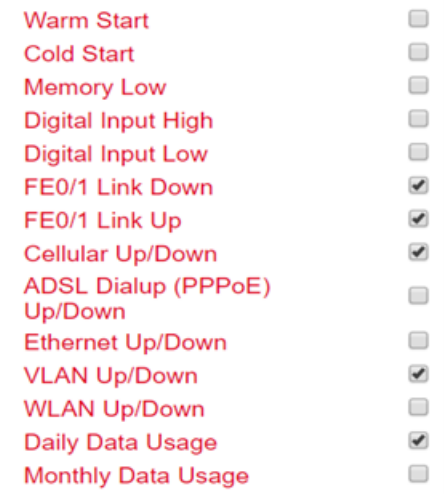


On the right side of the web interface you can see the alarm messages permanently regardless of which menu you are in (Fig. 2).



3.1.9.2. Alarm Input

In the ***Alarm Input*** menu you define which alarm messages the router should output. By setting the checkmarks next to each entry, an alarm is activated or deactivated.



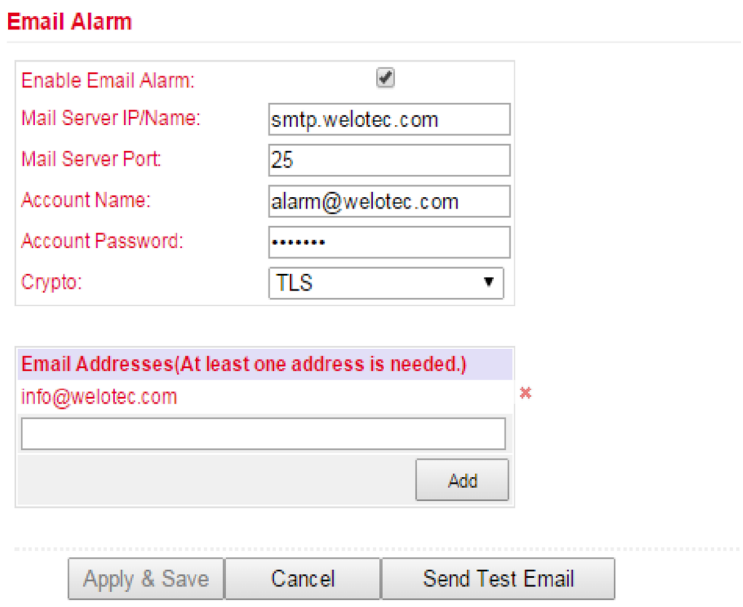
The following alarm messages are available.

Parameter	Description
Warm Start	Warm start/reboot of the router
Cold Start	Cold start = booting the router if it was switched off or had no power before
Memory Low	Memory Low
Digital Input High	Digital Input High
Digital Input Low	Digital Input Low
FE0/1 Link Down	Fast Ethernet Port 0/1 disconnected
FE0/1 Link Up	Fast Ethernet Port 0/1 connected
Cellular Up/Down	Mobile connection GPRS/UMTS/LTE conected or disconnected
ADSL Dialup (PPPoe) Up/Down	ADSL Dialup connected or disconnected
Ethernet Up/Down	Ethernet connected or disconnected
VLAN Up/Down	VLAN connected or disconnected
WLAN Up/Down	WLAN connected or disconnected
Daily Data Usage	Displays the daily data used by the SIM card (only if the Data Usage function is activated, see Services > Data Usage)
Monthly Data Usage	Displays the monthly data used by the SIM card (only if the Data Usage function is activated, see Services > Data Usage)

3.1.9.3. Alarm Output

The Alarm Output menu is used to configure the e-mail server that will forward the alerts by mail.

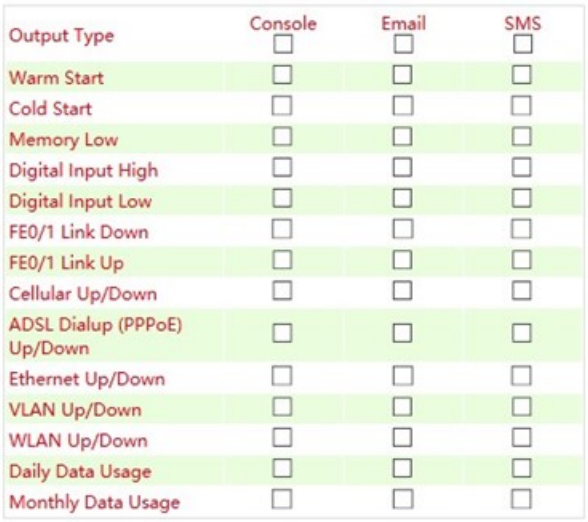
If an alarm is triggered, a message is generated by the router and sent to the stored e-mail addresses via the specified e-mail server.



Parameter	Description
Enable Email Alarm	Check the box for enabling/disabling the e-mail server functionality
Mail Server IP/Name	Host name (FQDN) or IP address of the e-mail server
Mail Server Port	Port of the mail server, default 25, but also 465 for SSL/TLS or 587 possible
Account Name	User account on the e-mail server through which the messages are to be sent
Account Passwort	Password of the user account on the e-mail server
Crypto	Encryption TLS
Email Addresses	E-mail address to which the mails are to be sent

3.1.9.4. Alarm Map

On the Alarm Map you define whether the alerts should be displayed in the web browser or also sent by e-mail or SMS. Set the checkmark to Enable or Disable the feature.

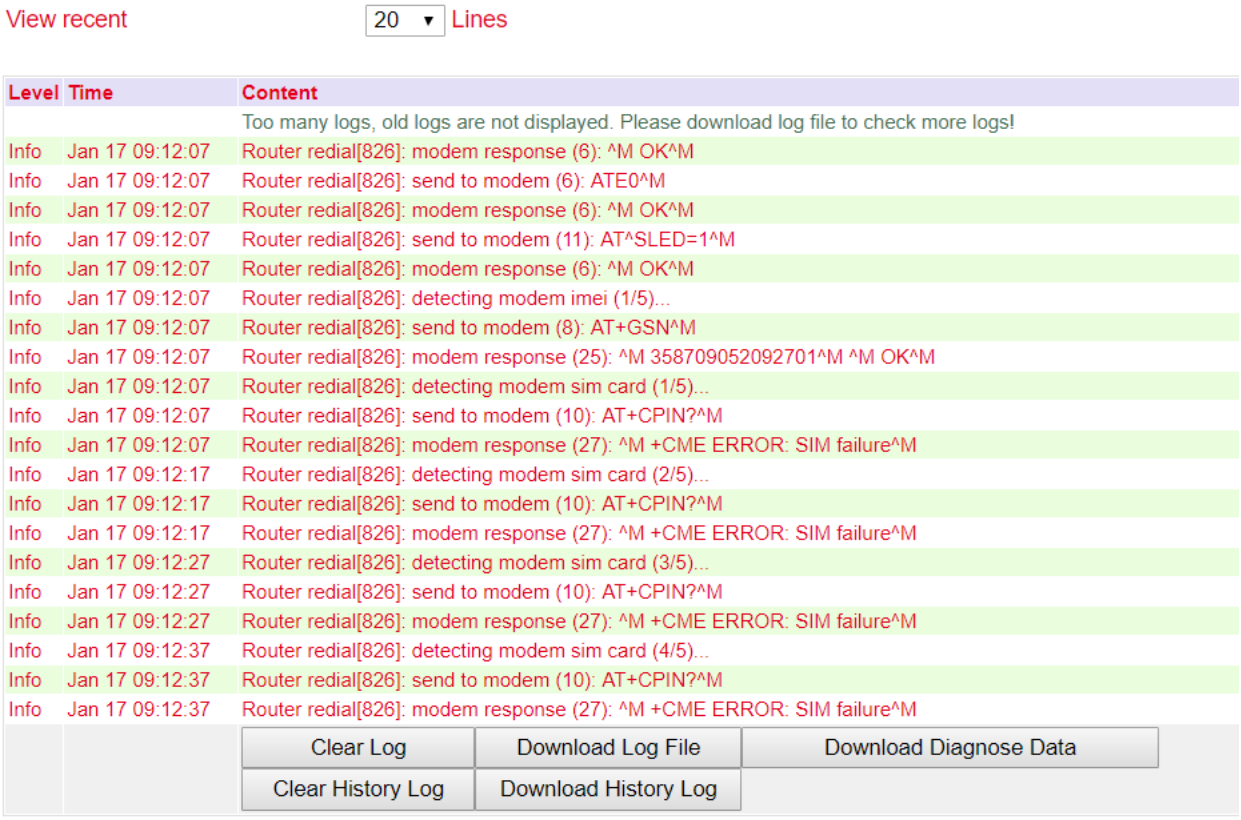


3.1.11 3.1.10. Log

3.1.10.1. Log

The current messages of the router are displayed in the Log menu.

The log contains information about network, operational status, configuration changes, ISP connection information, IPSec, OpenVPN status and much more.

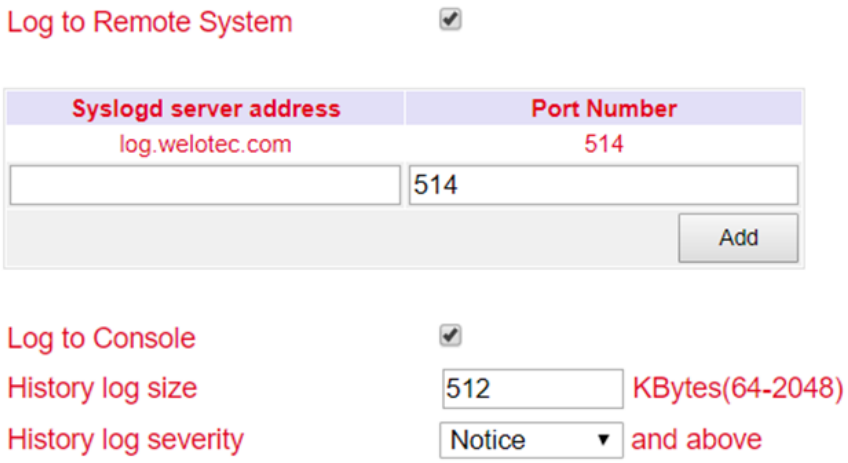


Under the log section there are options to clear the displayed logs, download the log, download the diagnostic file, clear the history and download the history.

Option	Description
Clear Log	Delete displayed log files
Download Log File	Download log files
Download Diagnose Data	Download diagnostic data file
Clear History Log	Delete log history
Download History Log	Log history download

3.1.10.2. System Log

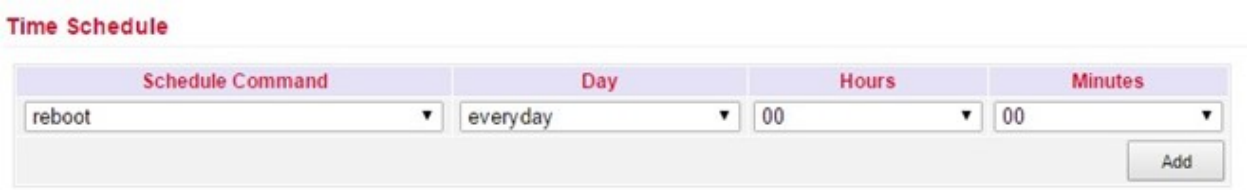
In ***System Log*** you can specify a syslog server to which the logs should be sent over the network.



Under ***Syslog server address*** the host name of the syslog server (FQDN) or the IP address is specified. Port 514 is the default port for syslog servers.

3.1.12 3.1.11. Cron Job

Under ***Time Schedule*** you can have actions executed on the router at specific times, such as a reboot of the router. Here you could always reboot the router at a certain time.



Under Time Schedule you can select the schedule command (currently only reboot). With Day you select daily (everyday) and with Hours and Minutes you control the start time. Click on the Add button to apply the settings.

3.1.13 3.1.12. Upgrade

Firmware updates of the router can be performed in the ***Upgrade*** menu. A firmware update can contain new functions or also eliminate errors. The installed firmware is displayed under the ***Select the file to use*** field.

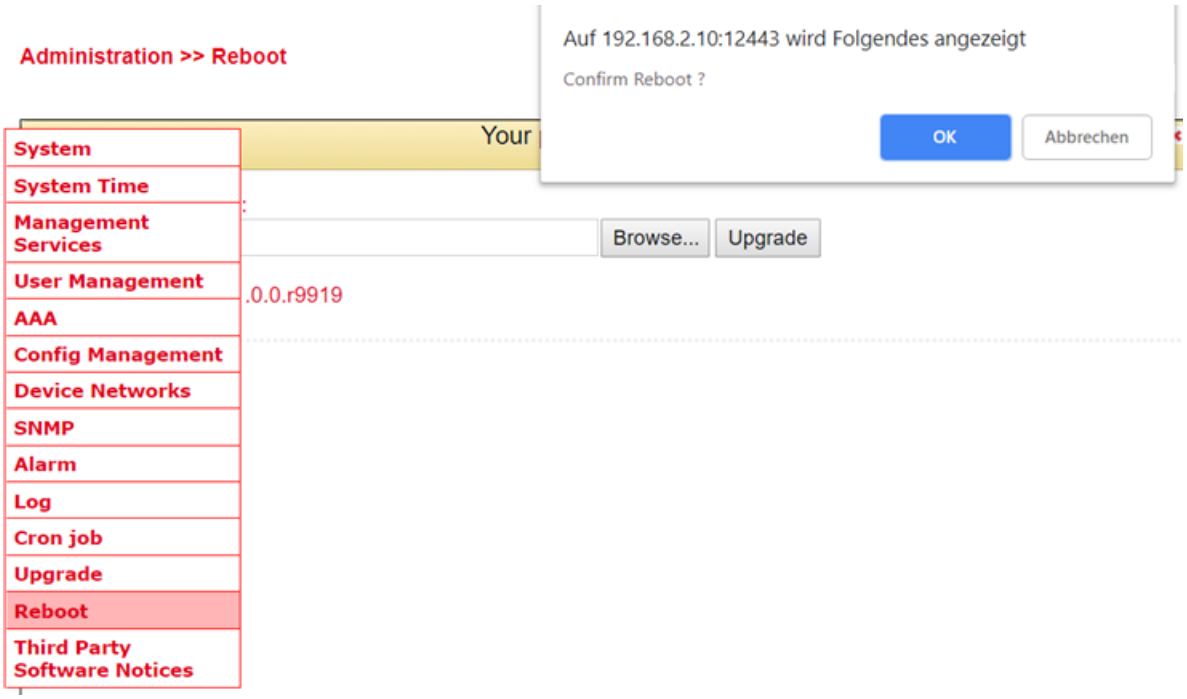
Under Browse you select the firmware file which you have downloaded before (this must be unpacked either as *.bin or *.pkg file). By clicking on ***Upgrade*** the firmware will be installed on the router.

Hinweis

Please note that the bootloader and the IO board may have to be updated separately if the firmware version is significantly older. If you have any questions, please contact our support.

3.1.14 3.1.13. Reboot

The router is restarted with ***Reboot***.



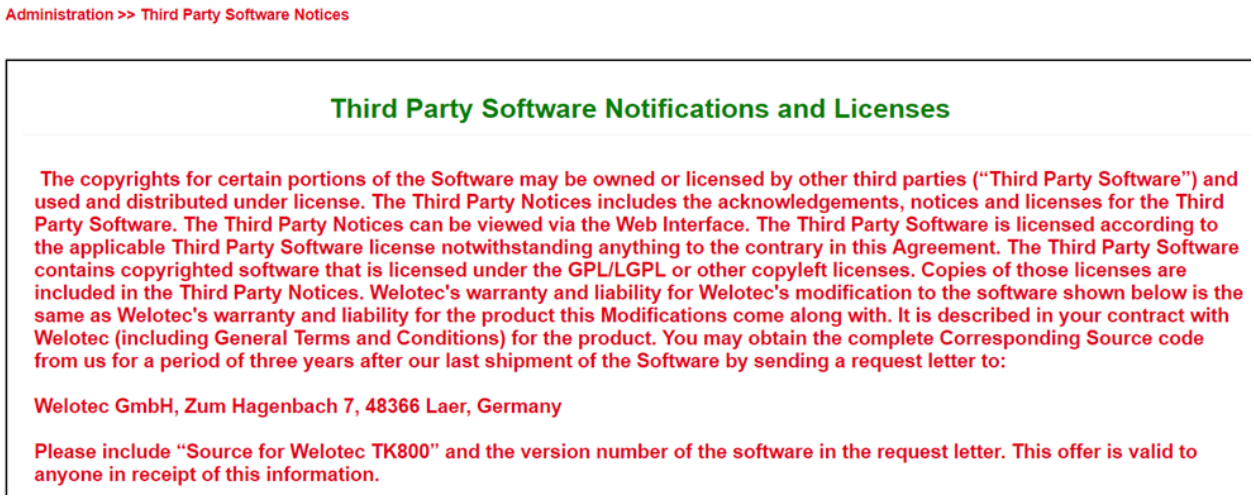
By clicking ***OK*** you confirm the restart of the router.

Hinweis

Save the configuration of the router before you restart the router. Otherwise, the configuration may be lost when you restart.

3.1.15 3.1.14. Third Party Software Notices

Here are the software terms and licenses from all third-party vendors related to the TK800 router series.



3.2 3.2. Network

3.2.1 3.2.1. Cellular

Cellular is the mobile communication interface of the router. If a SIM card is inserted in the router, you can dial into the Internet via GPRS, EDGE, UMTS or LTE, depending on the router model.

3.2.1.1. Cellular Status

Under ***Status*** there is an overview of the current status (Connected or Disconnected).

The Network Type in the Status tab and the IP address in the Network area is the deciding factor. In the Modem area you can also see the signal level, RSRP and RSRQ.

Under certain circumstances, the router may not be assigned the correct DNS server by the provider. Check whether there is no entry under DNS or an entry such as 10.74.210.210 (Telekom).

Hinweis

The RSRP value is one of the most important values when it comes to assessing one's own reception value or reception quality. It is measured directly by the terminal device. The RSRP is also used to determine the currently

strongest radio cell in the vicinity.

SRP	School Grade	Comment
-50 bis -65 dBm	1 (very good)	excellent reception is available - perfect!
-65 dBm bis -80 dBm	2 (good)	good, sufficient reception conditions
-80 dBm bis -95 dBm	3 (satisfactory)	not perfect but sufficient for stable connections
-95 dBm bis -105 dBm	4 (sufficient)	still acceptable conditions with speed restrictions; possibly also interruptions
-110 dBm bis -125 dBm	5 (poor)	very poor level - urgent need for action; probably hardly any connection possible
-125 dBm bis -140 dBm	6 (insufficient)	extremely poor - probably no connection possible

Hinweis

The RSRQ is a calculated ratio value that results from the value for RSRP and the RSSI. It is enormously important for evaluating an LTE connection and the reception quality. The analysis of this value is indispensable for the optimal alignment of antennas for stationary use of LTE. Together with the RSRP, this enables the user to find the optimal position and alignment for his equipment (e.g. [antenna]).

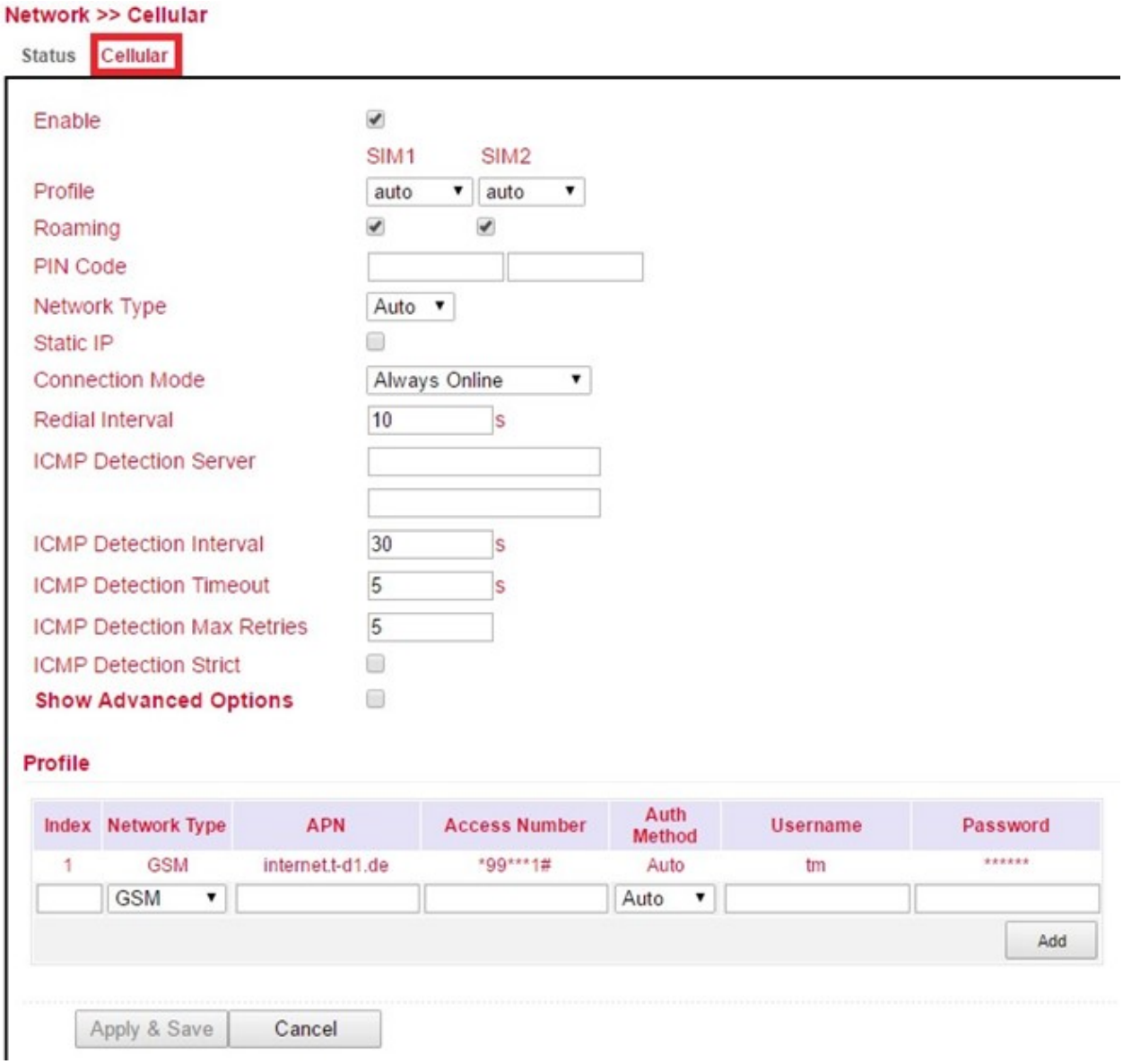
RSRQ	School Grade	Comment
-3 dB	1 (very good)	optimal connection quality, no interference from disruptors
-4 … -5 dB	2 (good)	disruptive influences are present, but have no impact
-6 … -8 dB	3 (satisfactory)	interfering influences, slight influence on the connection
-9 … -11 dB	4 (sufficient)	disruptive interference, noticeable influence on the connection
-12 … -15 dB	5 (poor)	heavy interference present, connection very unstable
-16 … -20 dB	6 (insufficient)	extremely disruptive interference, no usable connection possible

Hinweis

Most providers assign private IP addresses or IP addresses that are not routed via the Internet. A successful or unsuccessful ping does not indicate whether the IP address of the router can really be reached.

3.2.1.2. Cellular Configuration

Under ***Network*** > ***Cellular*** > ***Cellular*** you can change access settings for the cellular network.

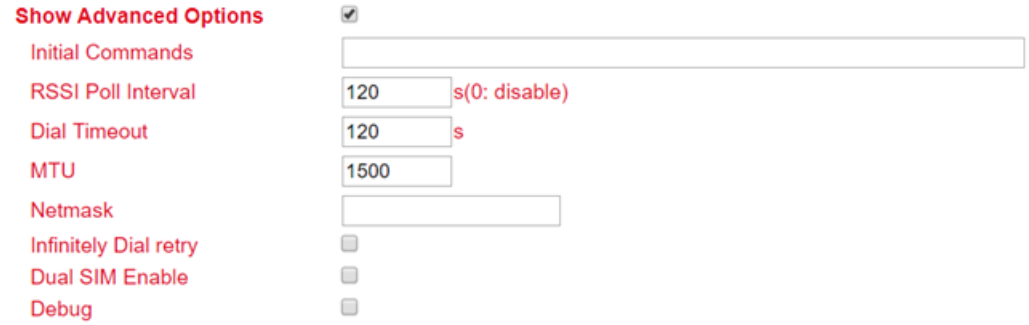


Parameter	Description	Factory settings
Enable	Enable or disable the cellular connection	Enabled
Profile	APN profile for SIM card 1 and SIM card 2	Auto / Auto Automatic selection of APN based on SIM card
Roaming	Enable or disable whether the SIM card should allow roaming. ⚠ **Hinweis** Whether this function works depends on the provider. Roaming may occur despite being deactivated.	Enabled / Enabled
PIN Code	PIN code for the SIM card. ⚠ **Hinweis** PIN code should be entered before inserting the SIM card!!!	Blank / Blank
Network Type	Selection: Auto (automatic network selection), 2G (GPRS / EDGE), 3G (UMTS, HSDPA, HSUPA, HSPA+), 4G (LTE)	Auto
Static IP	⚠ **Hinweis** Only relevant in a few exceptions. With most providers that assign fixed IP addresses, the function must not be set.	Disabled
Connection Mode	Select whether the router should always be connected to the cellular network or only dial in when needed.	Always Online
Redial Interval	Redial interval	10 seconds
ICMP Detection Server	Up to two ICMP detection servers can be entered here to monitor the connection. ⚠ **Hinweis** The IP addresses or DNS names must be accessible via the router and respond to a ping. It is therefore not recommended to take the Google servers 8.8.8.8 and 8.8.4.4, since these block the requests more often. Choose e.g. 4.2.2.1 or similar.	blank
ICMP Detection Interval	Interval at which the ICMP Detection Server checks the Internet connection.	30 seconds
ICMP Detection Timeout	ICMP timeout or ping timeout. Maximum time that the ping may take (Round Trip Time).	5 seconds
ICMP Detection Max Retries	Number of retries on failed ICMP ping.	5
ICMP Detection Strict	If disabled, the ICMP ping is sent only when no data is sent or received. ⚠ **Hinweis** If ICMP Detection Strict is enabled, the ICMP ping is always executed, even if user data is sent or received. For applications where high availability is important, Strict should be enabled.	Disabled
Show Advanced Op-	When enabled, more configuration options become visible.	Disabled

Connect on Demand

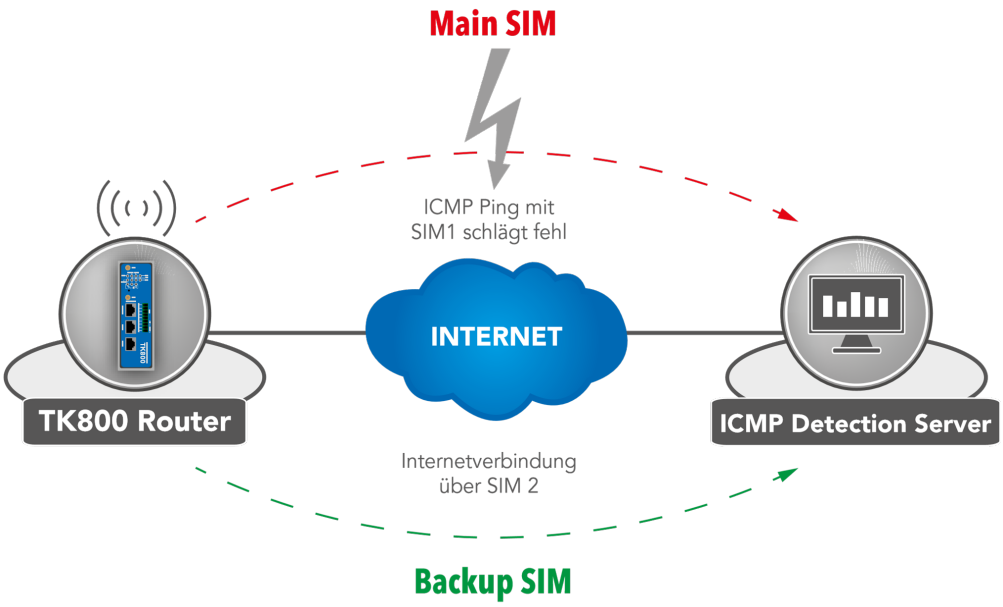
Here you have to set the checkmark at ***Triggered by SMS***. The router will only connect to the Internet if it has received the command to do so via SMS beforehand.

Show Advanced Options



Parameter	Description	Factory settings
Initial Commands	Start commands e.g. if Triggered by SMS is selected or special AT commands are to be used.	blank
RSSI Poll Interval	Polling interval of the signal strength	120 seconds
Dial Timeout	Maximum time for the dial-up attempt	120 seconds
MTU	Maximum size of a package	1500 bytes
Netmask	An additional netmask can be entered here	blank
Infinitely Dial Retry	If Triggered by SMS is selected, the dialing can be set to infinite here	off
Dual SIM Enable	Enable/disable the dual SIM option. If this option is activated, special selection fields are available (see below)	disabled
Main SIM	The main sim card that will be used	SIM1
Max Number of Dial	Maximum connection attempts, then restart of the modem	5
Min Connected Time	Minimum connection time	0 seconds
CSQ Threshold	Minimum signal strength SIM1 / SIM2	0
CSQ Detect Interval	Interval for signal strength query SIM1 / SIM2	0 seconds
CSQ Detect Retries	Repeat attempts for signal strength query SIM1 / SIM2	0
Backup SIM Timeout	Time after which it is switched back to the main SIM card	0 Sekunden
Debug	If enabled, more detailed logging is done	disabled

Dual SIM Enabled



If a provider is unavailable, the system switches to the alternative provider. The same applies when the mobile data

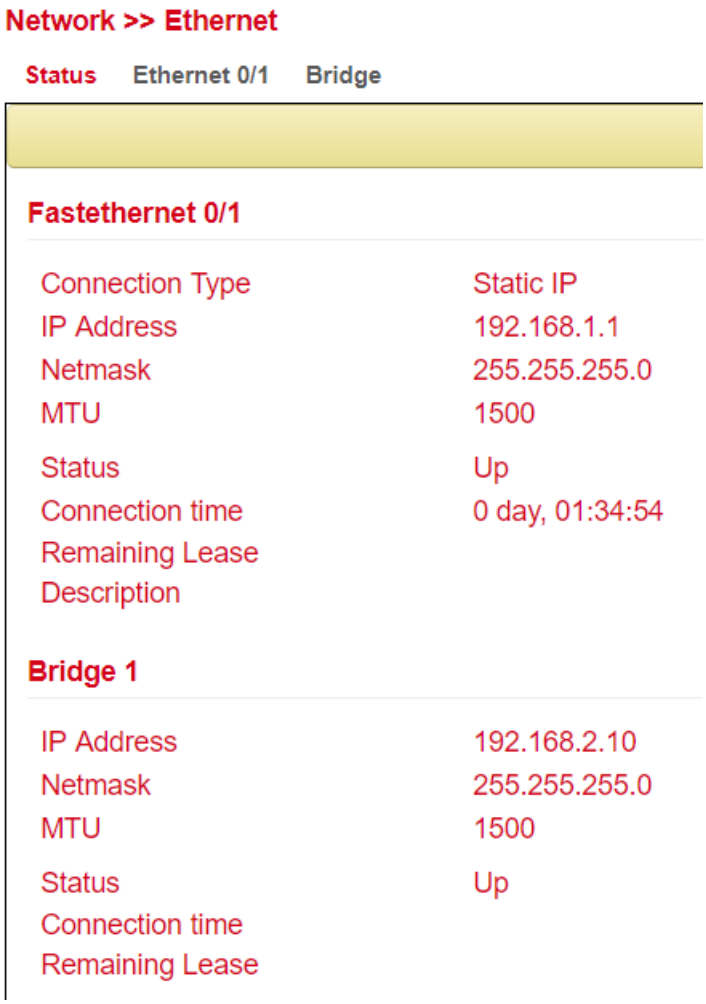
volume is used up. The TK 800 uses ICMP to monitor the data connection. If this is no longer available (because the ping fails), the router switches to the other connection.

3.2.2 3.2.2. Ethernet

In the Ethernet area, you have the option to make settings for the network ports. Depending on the model, you can adjust the interfaces individually. It is important to know that the router models have a network interface with the designation FE 0/1 and a network bridge, which is designated FE 1/1 to 1/4 depending on the model.

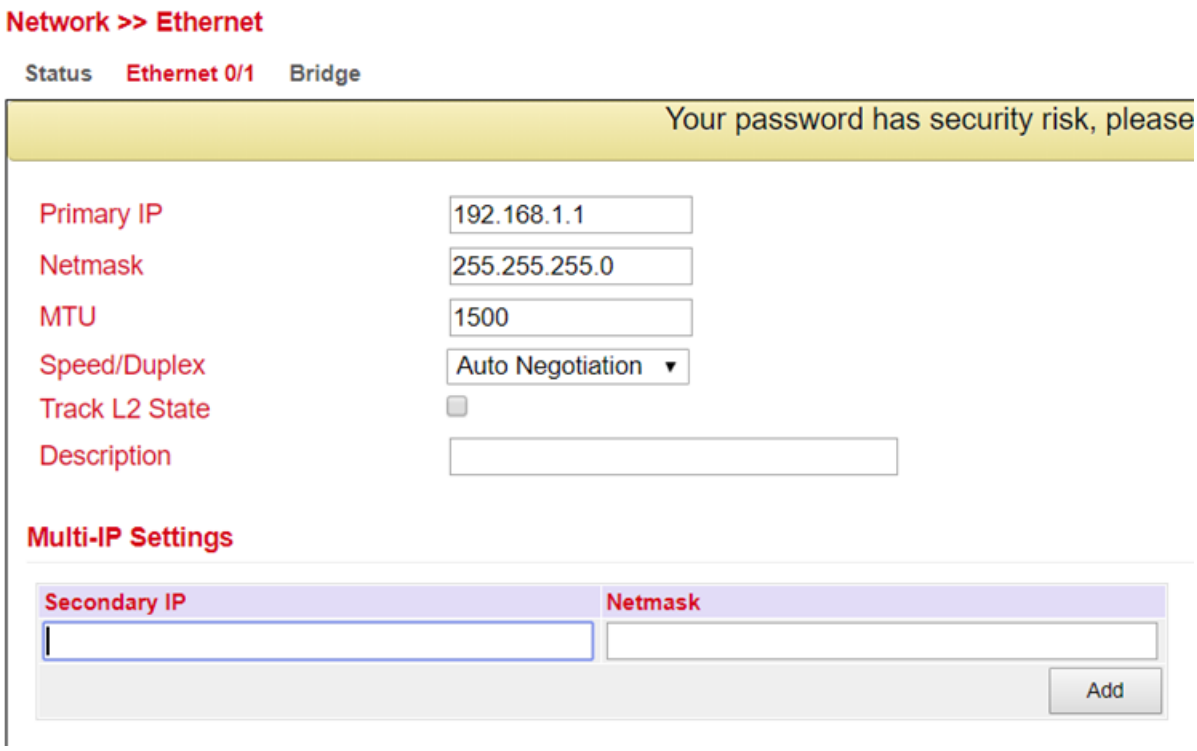
3.2.2.1. Ethernet Status

The status page shows the current status of the network ports (depending on the model).



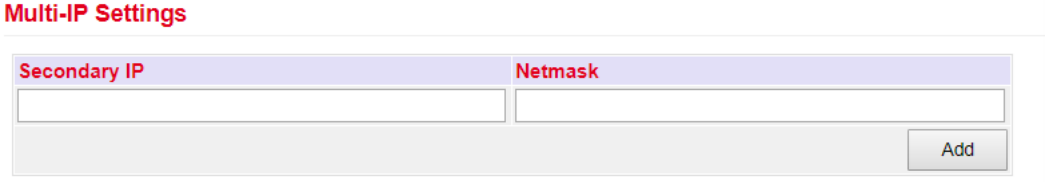
3.2.2.2. Fast Ethernet 0/1

Here you can adjust the settings of the network interface with the label FE 0/1.



Parameter	Description	Factory settings
Primary IP	Primary IP address can be entered and changed here	192.168.1.1
Netmask	Subnet mask	255.255.255.0
MTU	Maximum Transmission Unit = maximum size of an unfragmented data packet	1500
Speed/Duplex	Five options are available: Auto Negotiation: automatic negotiation of speed 100M full-duplex: 100 megabits full-duplex 100M half-duplex: 100 megabits half-duplex 10M full-duplex: 10 megabits full-duplex 10M half-duplex: 10 megabits half-duplex	Auto
Track L2 State	Checkmark set: Port status remains administratively disconnected after being disconnected (Down) Checkmark not set: Port status reconnects after being disconnected (UP)	Checkmark not set
Description	Description of the port - Freely selectable name	-

In the lower menu additional IP addresses can be assigned for the FastEthernet 0/1 port.



Hinweis

The configuration as DHCP client is described under ***DHCP***. The configuration of a WAN interface is described under ***Wizard***.

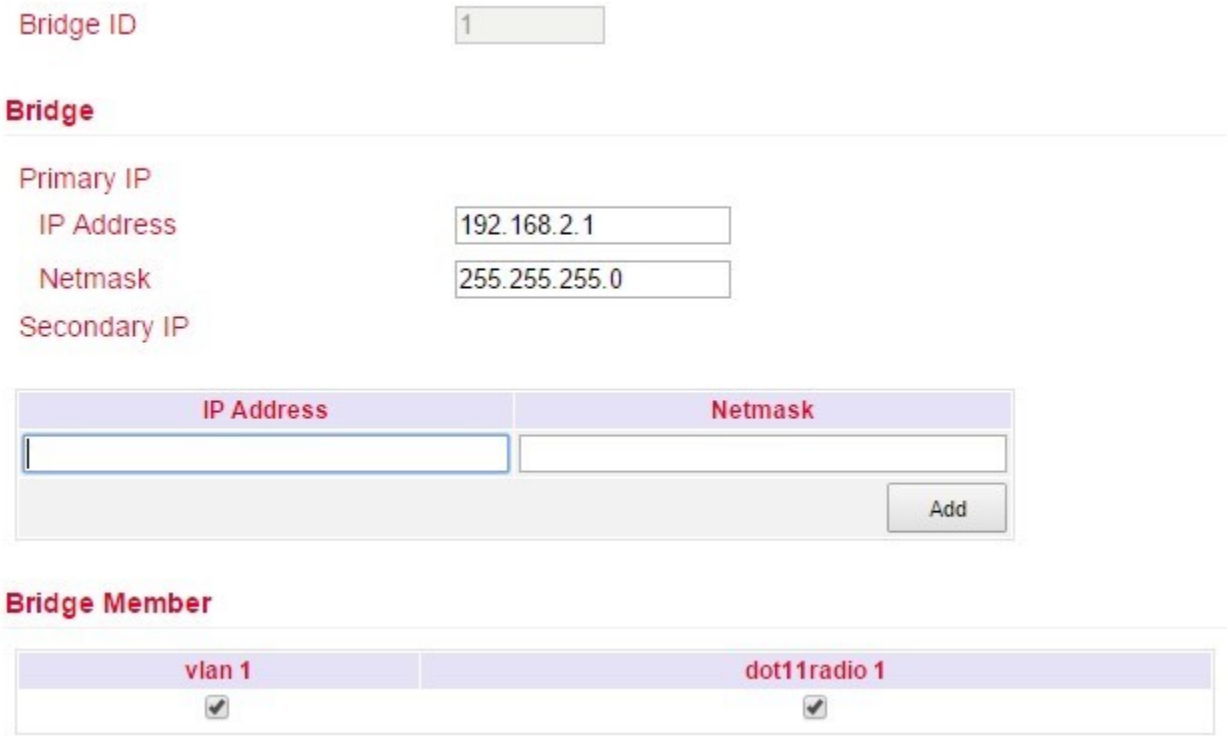
3.2.2.3. Bridge (TK8x5-EXW)

Overview of the existing bridge. Only one bridge is possible!

Hinweis

If you delete the bridge, no more IP address is set on the interfaces FE1/1 - FE1/4. The router is then only accessible via FE0/1 or console!!!

To edit the bridge, select the existing entry and then click ***Modify***.



Bridge:

Here you can change the IP address of the bridge. Under ***Secondary IP*** you can assign additional IP addresses to the bridge.

Bridge Member:

The interface ***dot11radio1*** is the WLAN interface. Via the hooks a bridge member can be added or removed from the bridge.

Hinweis

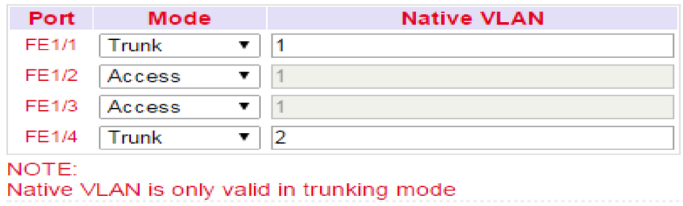
Removing a bridge member from the bridge results in the IP address of the interface being empty. It is therefore recommended to only make changes via the interface FE0/1, as this is not a bridge member.

3.2.3 3.2.3. VLAN (TK8x5-x)

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

3.2.3.1. VLAN Trunk

In the ***VLAN Trunk*** menu, different VLAN IDs can be assigned to the FastEthernet 1/1 to 1/4 network ports.



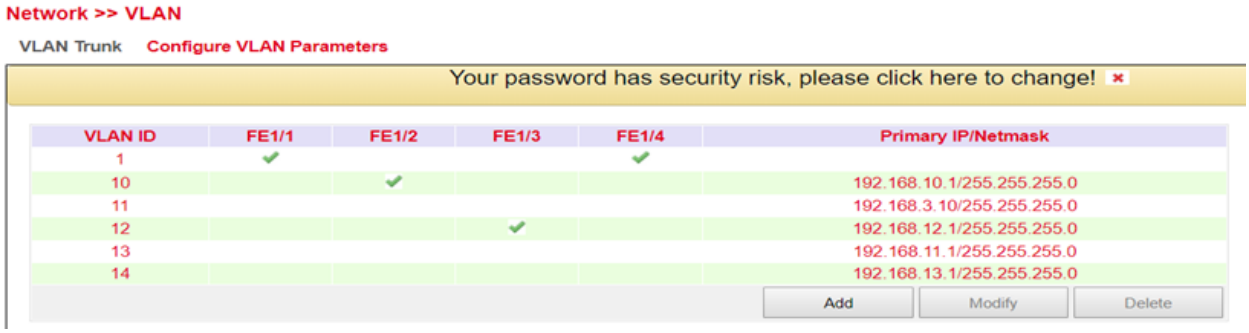
The options ***Access*** and ***Trunk*** are available for the FastEthernet ports.

In Access Mode, VLAN 1 is always selected.

In Trunk Mode, you can assign VLAN IDs between 1-4000 to the FastEthernet ports.

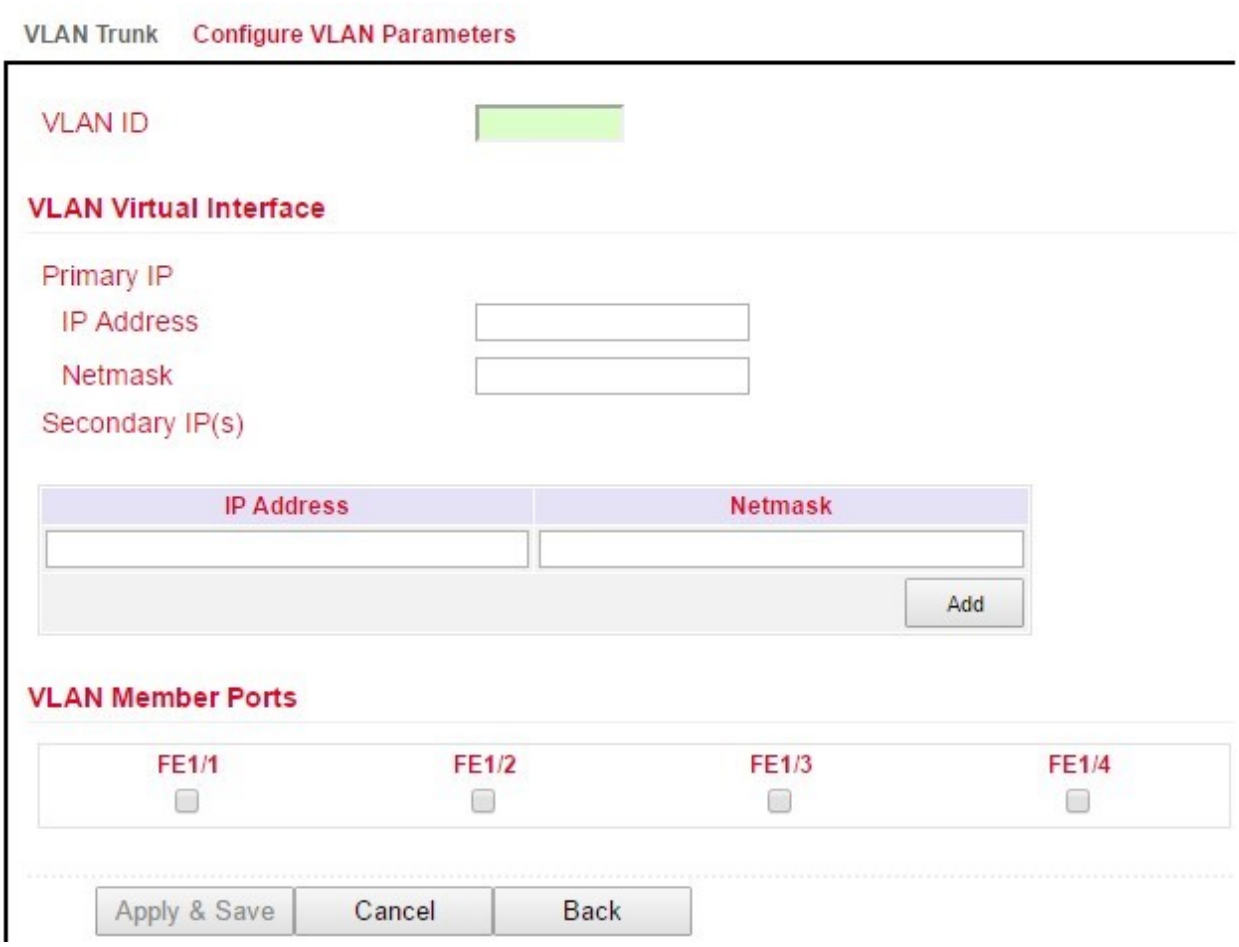
3.2.3.2. Configure VLAN Parameters

In the ***Configure VLAN Parameters*** menu you can change the assignment of VLANs to FastEthernet ports and create new VLANs.



Button	Description
Add	A new VLAN can be added via the Add button.
Modify	The existing VLANs can be edited by selecting them and then clicking on Modify. ⚠ **Hinweis** For the TK8x5-EXW model, the VLAN with ID1 cannot be edited as long as the bridge is active.
Delete	With Delete a previously selected VLAN can be deleted. ⚠ **Hinweis** The VLAN with ID 1 cannot be deleted!!!

Adding a new VLAN:



Assign a new ***VLAN ID*** (e.g. 3) and then a Primary IP address. If required, multiple IP addresses can be entered under ***Secondary IP(s)*** (confirm with Add after each addition).

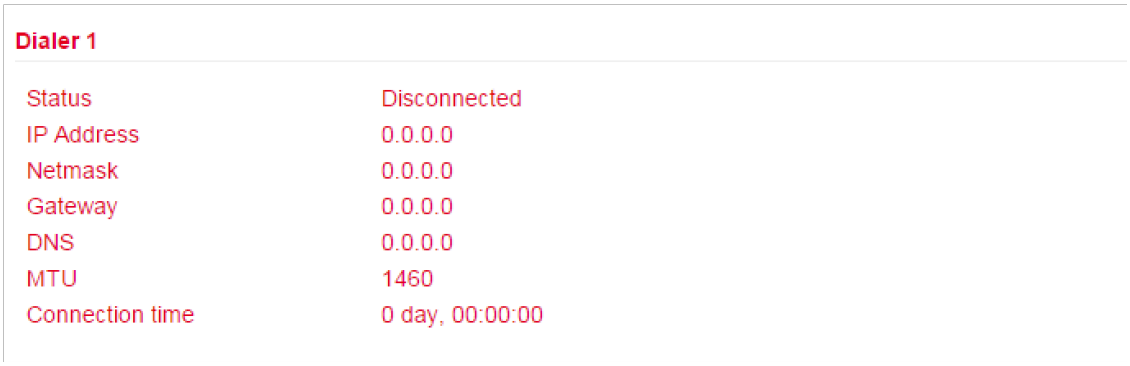
Under ***VLAN Member Ports***, one or more FastEthernet port/s are assigned to the VLAN by checking the checkbox.

Hinweis

The TK800 series routers do not have a built-in ADSL modem. For the use of ADSL Dialup, an external ADSL modem must be connected to the WAN port.

3.2.4 3.2.4. ADSL Dialup (PPPoE)

3.2.4.1. Status



Hinweis

The TK800 series routers do not have a built-in ADSL modem. For the use of ADSL dialup, an external ADSL modem must be connected to the WAN port. For the digital transmission technology, an appropriate DSL modem that supports the new IP technologies is required.

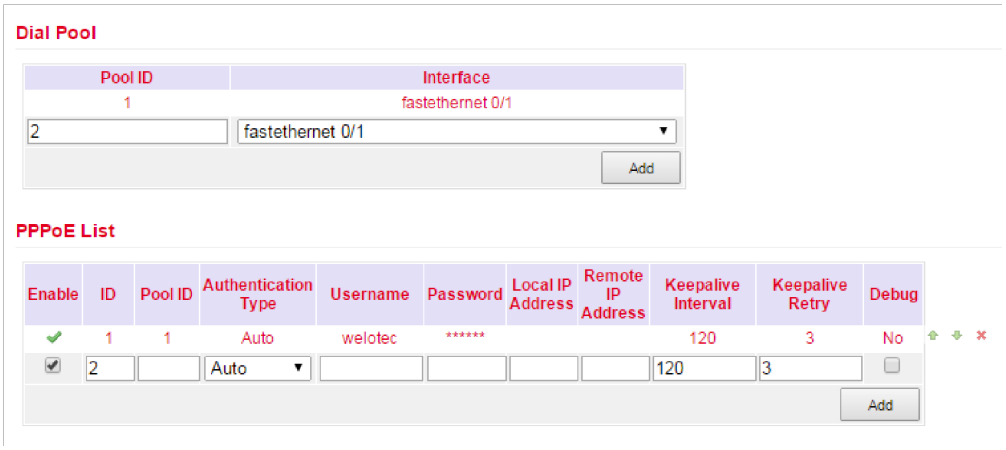
3.2.4.2. ADSL Dialup (PPPoE)

Here you can configure the dial-in via the DSL modem for PPPoE. The TK800 does not have its own DSL modem, so these cannot dial in independently.

In this case, an appropriate DSL modem that can handle the new IP technologies is required. The modem should meet the following criteria:

- VDSL2/ADSL2 Ethernet-Modem
- Annex A/B/M/J compatible
- PPPoE bridge operation
- IPv4 and IPv6 compatible
- DSL standards
  - ANSI T1.413 Issue 2
  - ITU G.992.1 A/B (G.dmt)
  - ITU G.992.2 (G.lite)
  - ITU G.992.3 (VDSL2)
  - ITU G.992.4 (G.HS)
  - ITU G.992.5 (ADSL2+)

You should therefore ensure that the modem is connected to the router before you start the configuration. The DSL modem should be connected to the FE 0/1 interface or to a defined VLAN port.



Dial Pool

The ***Pool ID*** is used to define the ***Interface*** for the PPPoE dial up.

Parameter	Description
Enable	Enables or disables the PPPoE entry
ID	Assign any unique ID
Pool ID	The pool ID previously created via Dial Pool for the interface via which the connection is to be established.
Authentication Type	Auto, PAP, CHAP can be selected. In most cases this parameter can be set to Auto.
Username	The username you received from your provider for dial-up.
Password	The password you received from your provider for dial-up.
Local IP Address	Your local IP address
Remote IP Address	IP address of the remote device (modem)
Keepalive Interval	Time after which the connection should be checked.
Keepalive Retry	Number of attempts when a connection check fails.
Debug	Detailed logging is performed when activated.

Hinweis

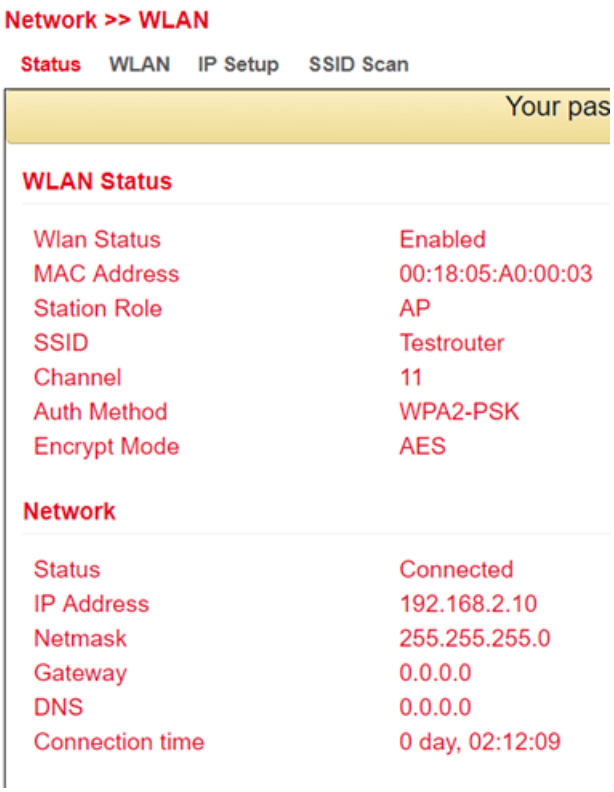
The wizard can also be used to set up a PPPoE connection via ***New WAN***. This is easier than the manual configuration!

3.2.5 3.2.5. WLAN (TK8x5-EXW)

3.2.5.1. WLAN Status

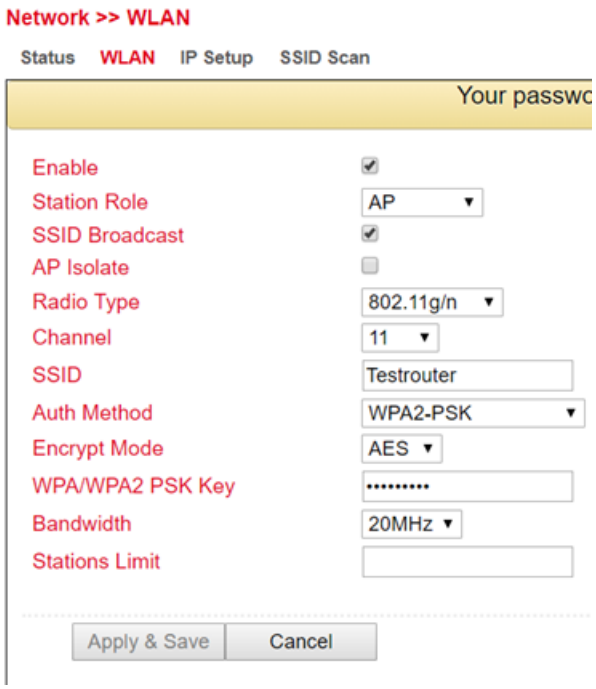
Under ***Network*** > ***WLAN*** you can first view the status of the WLAN.

For example, the current SSID of the router, the IP address or the role of the WLAN module (access point or client) can be read here.



3.2.5.2. WLAN Configuration

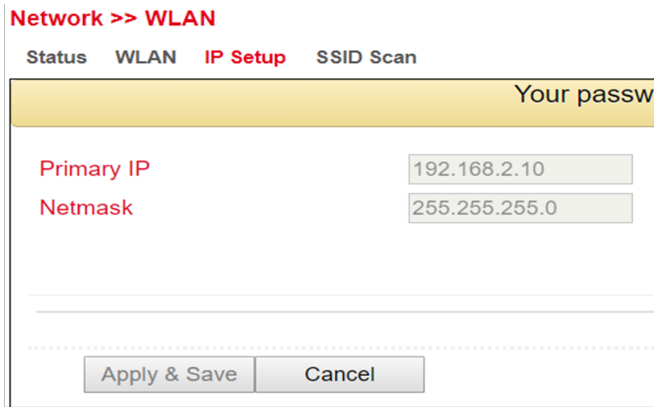
Under ***Network*** > ***WLAN*** > ***WLAN*** you can configure the WLAN.



Parameter	Description	Factory settings
Enable	Enables or disables the WLAN	Disabled
Station Role	AP (Access Point), Client or AP Client	AP
SSID Broadcast	Display the SSID if it is supposed to be visible	Enabled
AP Isolate	Enables or disables AP isolation	Disabled
Radio Type	The radio standard can be selected here	802.11g/n
Channel	The radio channel can be selected here	11
SSID	The SSID that identifies your WLAN and will be displayed when searching for WLAN networks.	TK800
Auth Method	The encryption standard to be used. OPEN, if the WLAN is not to be protected (not recommended).	OPEN
Encrypt Mode	If Open or Shared is selected: WEP40 or WEP104, both are actually no longer used today because they are not secure. When selecting the other options TKIP or AES	NONE
Bandwidth	20MHz or 40MHz channel bandwidth. A larger channel bandwidth can increase the speed, but there are fewer overlap-free channels.	20MHz
Stations Limit	Maximum number of simultaneously connected clients	blank

3.2.5.3. IP Setup

Under ***Network > WLAN > IP Setup*** the IP address of the WLAN interface can be changed.

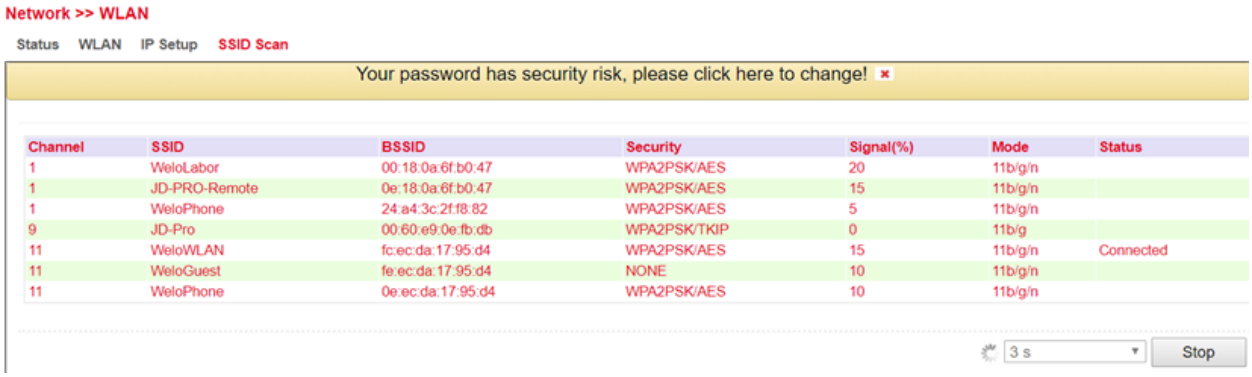


Hinweis

The IP address can only be changed if the WLAN interface is not a bridge member.

3.2.5.4. SSID Scan

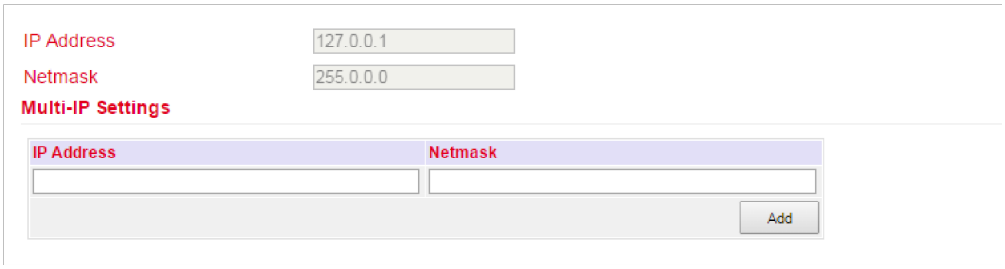
Under ***Network*** > ***WLAN*** > ***SSID Scan*** you can search for available WLAN networks. If you have configured the TK 800 as a WLAN client, it is possible to scan the WLAN networks within range for their SSID at this point. If the TK 800 is connected to a WLAN as a client, this is indicated in the status with Connected.



3.2.6 3.2.6. Loopback

3.2.6.1. Loopback Configuration

Under ***Network*** > ***Loopback*** you can enter further loopback IP addresses. The default loopback IP address 127.0.0.1 cannot be edited.



3.3 3.3. Services

3.3.1 3.3.1. DHCP

The **Dynamic Host Configuration Protocol** (**DHCP**) is a communication protocol in computer technology. It allows the assignment of the network configuration to clients by a server.

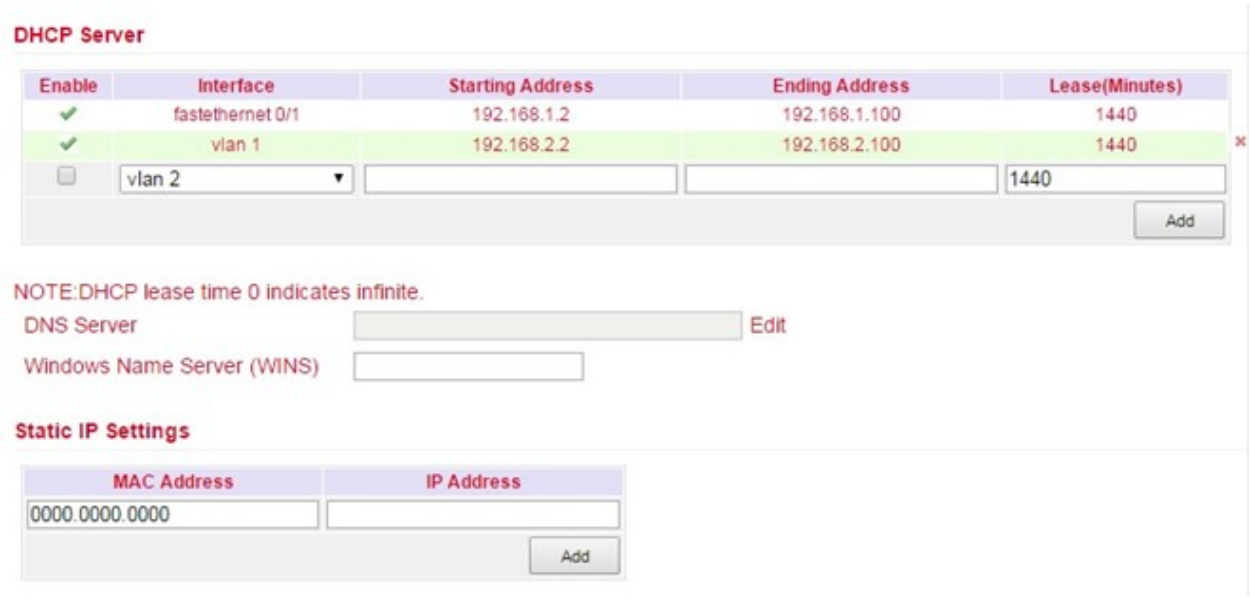
3.3.1.1. DHCP Status

Under ***Services*** > ***DHCP*** > ***Status*** you can see who is currently connected to the router via which interface.

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

3.3.1.2. DHCP Server

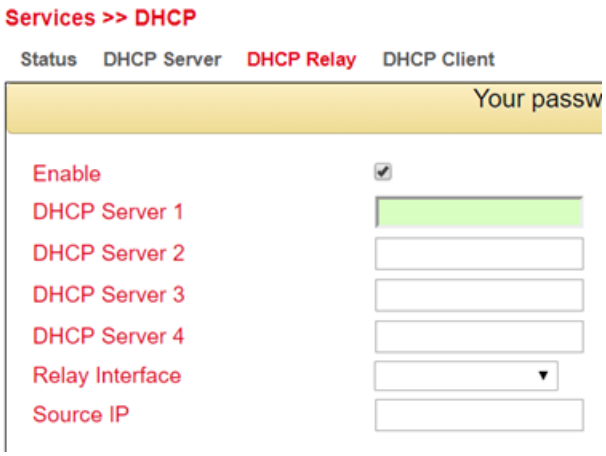
Under ***Services > DHCP > DHCP Server*** you can configure settings for the DHCP server. Select the appropriate interface and enter the start or end IP address and the lease, see example.



With ***Static IP Settings*** an IP address can be assigned to a specific MAC address.

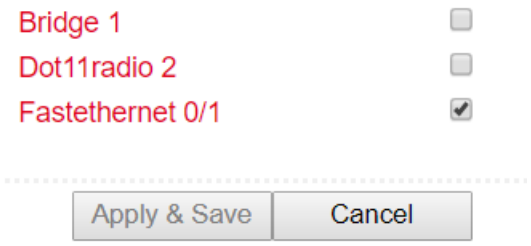
3.3.1.3. DHCP Relay

Under ***Services > DHCP > DHCP Relay*** you can specify remote DHCP servers, which then take over the DHCP management for the networks connected to the router. By clicking Enable, you activate this function.



3.3.1.4. DHCP Client

Under ***Services > DHCP > DHCP Client*** the router itself can receive a DHCP address from a DHCP server. To do this, select the interface that is to be configured via DHCP. The interfaces can vary depending on the router model.



3.3.2 3.3.2. DNS

The **Domain Name System** (**DNS**) is one of the most important services in many IP-based networks. Its main task is to answer name resolution requests.

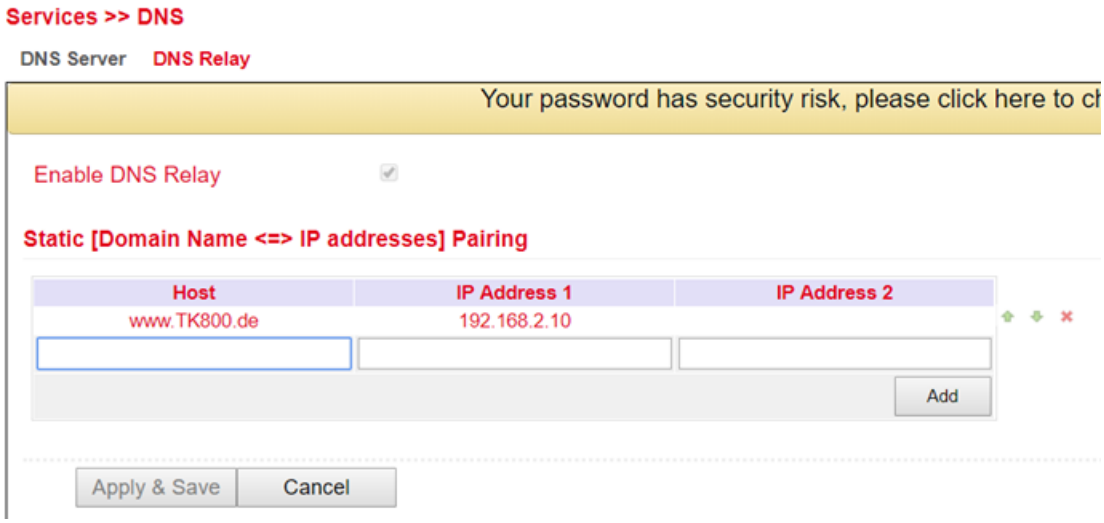
The DNS works similar to a telephone directory assistance. The user knows the domain (name of a server on the Internet), e.g. welotec.com, and sends this as a request to the Internet. The domain is then converted by the DNS into the corresponding IP address (if you like, the “connection number” on the Internet). E.g. an IPv4 address of the form 192.168.2.1 and thus leads to the correct server.

3.3.2.1. DNS Server

Under ***Services > DNS > DNS Server*** you can enter two DNS servers. These are then valid for all interfaces, unless a different DNS server was assigned via DHCP.

3.3.2.2. DNS Relay

Under ***Services > DNS > DNS Relay*** you can also enter DNS resolutions manually. Click Add to add the entry and Apply & Save to apply it.

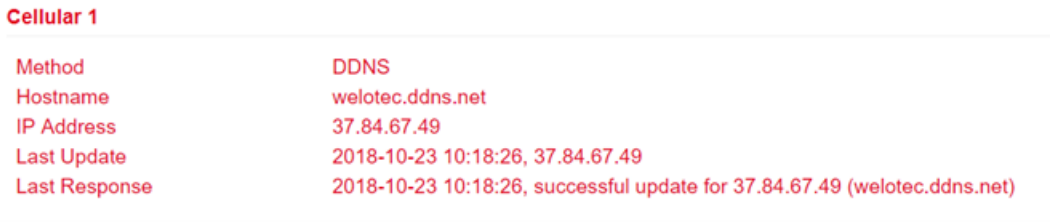


3.3.3 3.3.3. DDNS

Dynamic DNS or **DDNS** is a technique to dynamically update domains in the Domain Name System (DNS). The purpose is that a computer (e.g. a PC or a router) automatically and quickly changes the associated domain entry after changing its public IP address. This way the computer is always reachable under the same domain name, even if the current IP address is unknown to the user. Common providers for this service are e.g. DynDNS or NoIP.

3.3.3.1. DDNS Status

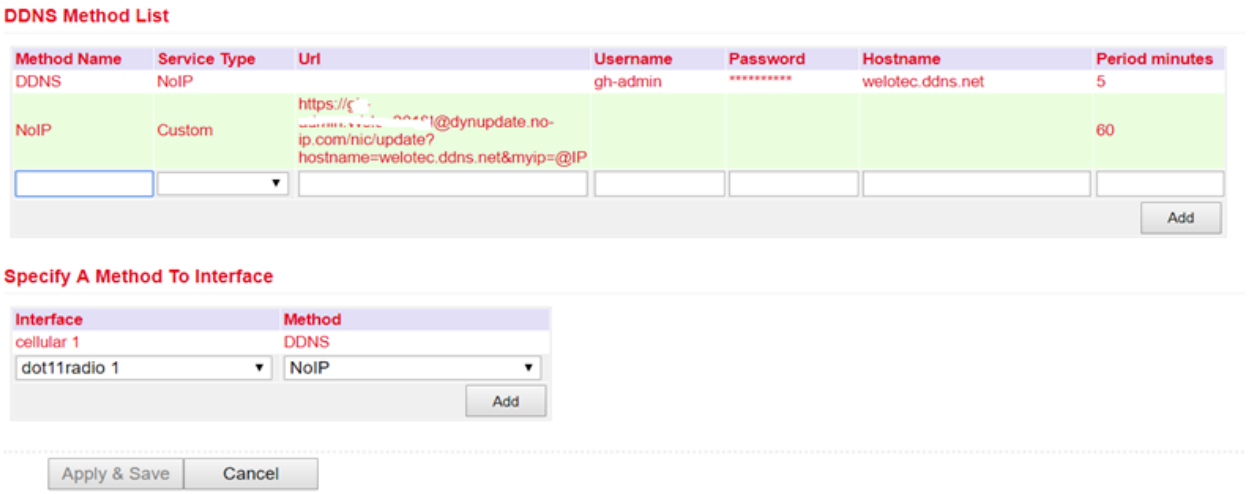
Under ***Services > DDNS > Status*** the currently used DDNS services are displayed.



3.3.3.2. DDNS

Under ***Services > DDNS > DDNS*** you can add a new DDNS service. It is important that a new DDNS service is created under DDNS Method List first.

Afterwards you have to assign it to an interface, this is done under ***Specify A Method To Interface***.



DDNS Method List	
Method Name	Freely selectable name for the service.
Service Type	The most common DDNS services are listed here. If the DDNS service is not listed, an individual DDNS service can be used via Custom.
Url	Only used for the selection Custom at Service Type. The complete url of the DDNS service including username and password is entered here, e.g. for NoIP https://username:password@dynupdate.no-ip.com/nic/update?hostname=welotec.ddns.net&myip=@IP The @IP parameter always updates the assigned IP address.
Username	The user name for the DDNS service is entered here.
Password	The password for the DDNS service is entered here.
Hostname	The name of the domain that is being used.
Period minutes	Specifies how often an update of the IP address is to be performed. Input values can be entered from 1 to 999999 minutes.

Specify A Method To Interface	
Interface	The interface of the router whose IP address should be accessible via the DDNS service.
Method	A DDNS service previously created under DDNS Method List.

Hinweis

You need an account of a DDNS provider, which you have to configure before. This account may be chargeable, depending on the provider.

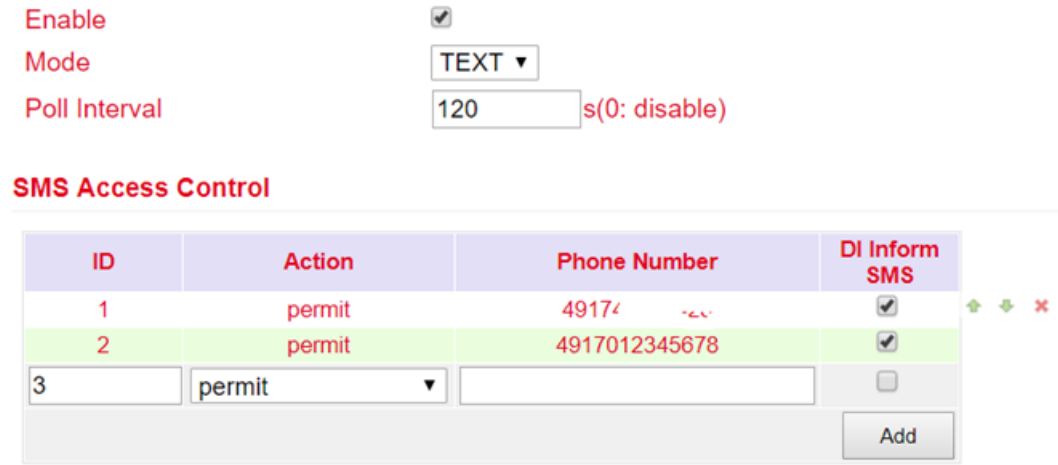
3.3.4 3.3.4. SMS

Introduction

The TK800 can be reached from outside via SMS and reacts to various commands sent via SMS. Thus, it is possible to query the status of the device, start / stop dial-up or restart the device.

Status query / restart

1. Go to the ***SMS*** subitem via the ***Services*** menu item
2. Click the ***Enable*** checkbox to turn on the feature



3. Enter in the table ***SMS Access Control*** the phone numbers which are allowed to send SMS to the router (format 4917123456789, no 0049 or +49!) and enter ***permit*** as action

If an SMS with the content ***show*** is now sent to the mobile phone number of the router, the router sends its current status as a reply

If an SMS with the content ***reboot*** is sent to the router, it restarts. You can also follow this process in the router's log.

Info	Oct 23 11:53:25	WeloTest-Router redial[842]: receive a sms from +4917
Info	Oct 23 11:53:25	WeloTest-Router smsd[975]: receive reboot sms!
Info	Oct 23 11:53:25	WeloTest-Router nanobroker[1192]: MSG: 0xa53e from service 303
Info	Oct 23 11:53:25	WeloTest-Router nanobroker[1192]: receive a sms(+4917) data reboot len 8 from 303
Info	Oct 23 11:53:25	WeloTest-Router nanobroker[1192]: nano instance nano-broker-pub get connection 0
Info	Oct 23 11:53:25	WeloTest-Router nanobroker[1192]: nano-broker-pub connection is zero
Notice	Oct 23 11:53:25	WeloTest-Router systools[8056]: system is rebooting!
Notice	Oct 23 11:53:25	WeloTest-Router systools[8056]: < -reboot:8056< -sh:8055< -smsd:975< -redial:842< -syswatcher:772< -init:1

Connecting or disconnecting from the Internet

After successful configuration, you can also control the router's Internet connection via SMS. However, this requires that the router is set to "Connect On Demand"!

1. Go to the ***Network*** menu item and select the ***Cellular*** subitem.
2. Now select the ***Cellular*** tab

3. Select the ***Connect On Demand*** mode here under ***Connection Mode*** and activate the ***Triggered by SMS*** field. Now you can send the following commands to the router via SMS:
   disconnects the Internet connection (see fig.)

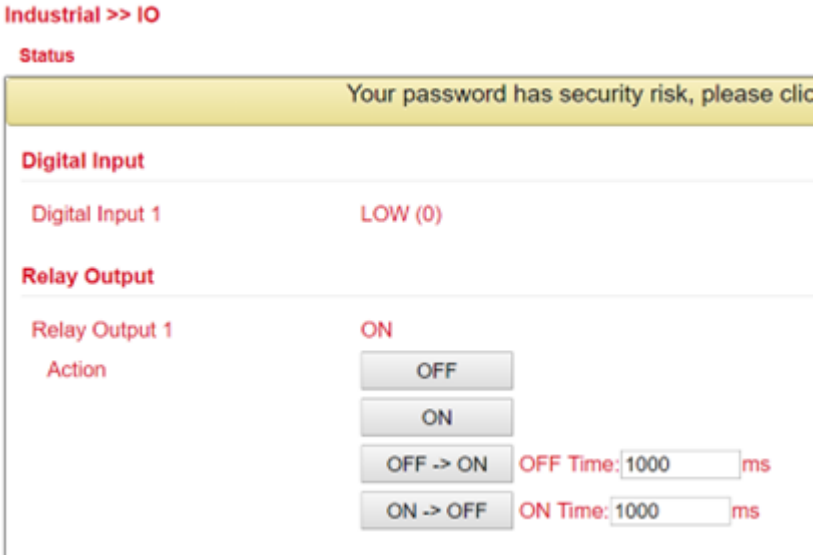
Info	Oct 23 11:59:12	WeloTest-Router redial[842]: receive a sms from +4917
Info	Oct 23 11:59:12	WeloTest-Router nanobroker[1061]: MSG: 0xa53e from service 303
Info	Oct 23 11:59:12	WeloTest-Router nanobroker[1061]: receive a sms(+4917) data cellular 1 PPP down len 21 from 303
Info	Oct 23 11:59:12	WeloTest-Router nanobroker[1061]: nano instance nano-broker-pub get connection 0
Info	Oct 23 11:59:12	WeloTest-Router nanobroker[1061]: nano-broker-pub connection is zero

cellular 1 ppp up - restores the Internet connection (see fig.)

Info	Oct 23 12:01:12	WeloTest-Router redial[842]: receive a sms from +4917
Info	Oct 23 12:01:12	WeloTest-Router nanobroker[1061]: MSG: 0xa53e from service 303
Info	Oct 23 12:01:12	WeloTest-Router nanobroker[1061]: receive a sms(+4917) data cellular 1 PPP up len 19 from 303
Info	Oct 23 12:01:12	WeloTest-Router nanobroker[1061]: nano instance nano-broker-pub get connection 0
Info	Oct 23 12:01:12	WeloTest-Router nanobroker[1061]: nano-broker-pub connection is zero

Switch digital relay on or off

Another important SMS command is to switch the digital relay on or off via SMS.



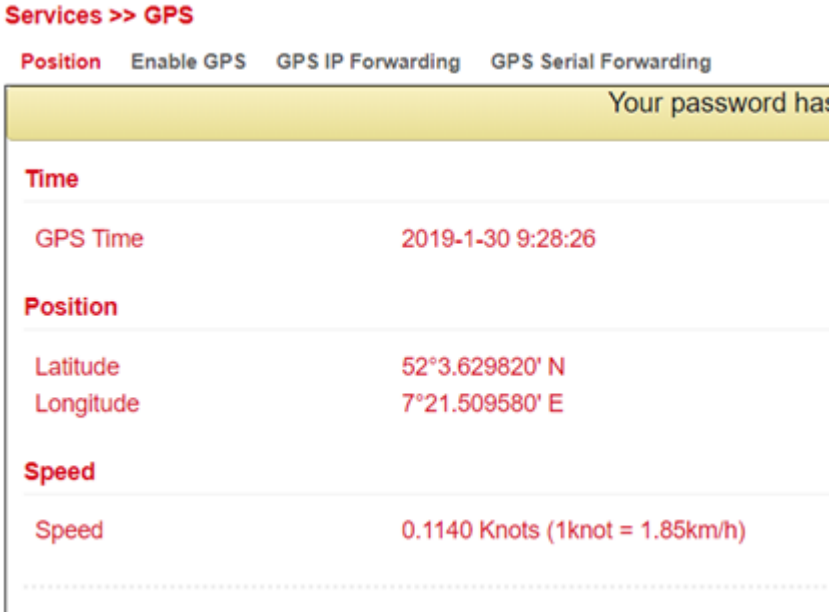
The following SMS commands can be used for this

- *io output 1 on - switches on the relay*
- *io output 1 off - switches the relay off*

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

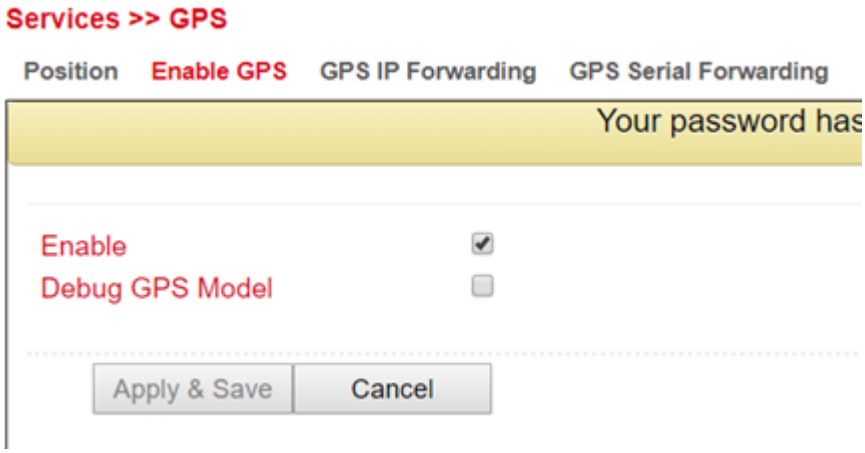
3.3.5.1. Position

Under ***Services*** > ***GPS*** > ***Position*** you will see the data about the current position if the corresponding antenna is connected to the router.



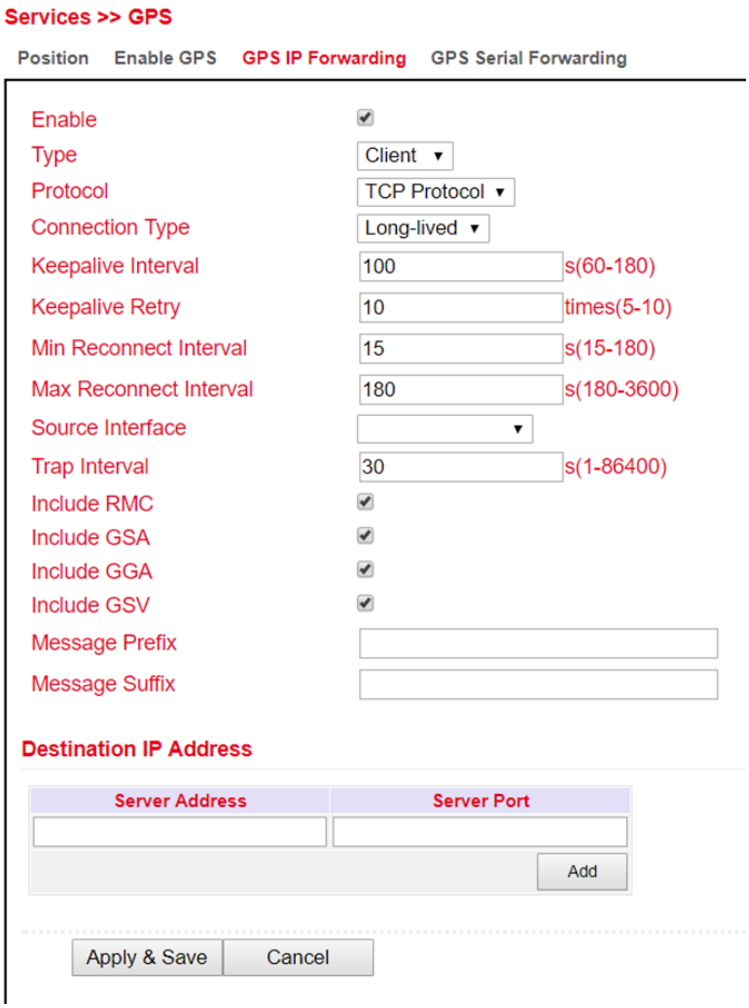
3.3.5.2. Enable GPS

To enable the GPS function of the router open the menu under ***Services*** > ***GPS*** > ***Enable GPS*** and click on the check-box ***Enable*** to switch on the function. With ***Apply & Save*** you save the settings and enable the GPS.

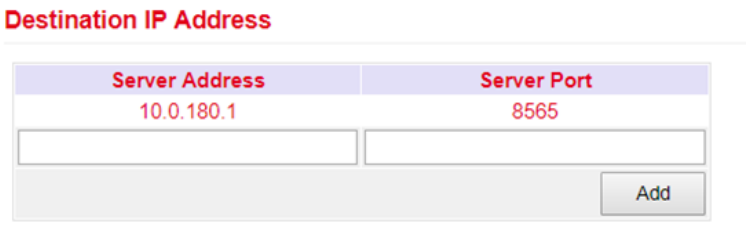


3.3.5.3. GPS IP Forwarding

Open the menu under ***Services*** > ***GPS*** > ***GPS IP Forwarding*** and click the ***Enable*** checkbox to turn on the function. This function is only available if the Debug GPS Model (from the previous chapter) is disabled. Here you can now make the appropriate settings. With ***Apply & Save*** you save the settings and activate them.



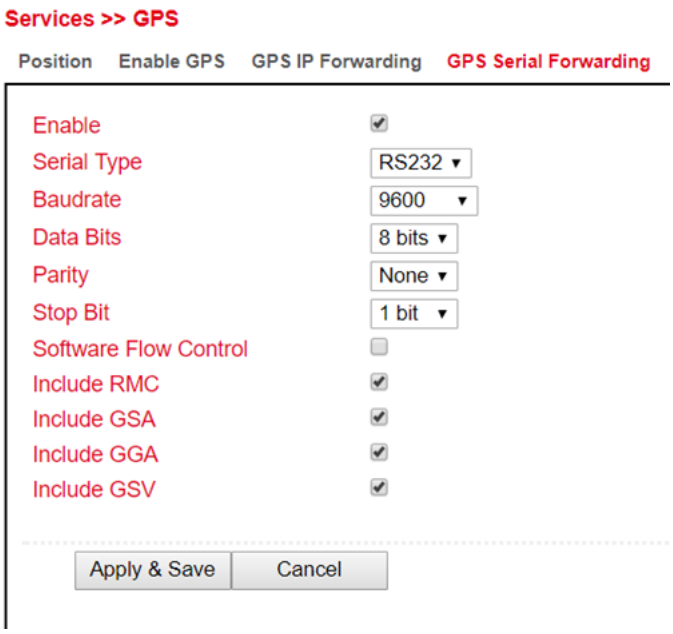
GPS IP Forwarding List	
Type	Selection between client and server
Protocol	Here you can choose between the protocol types TCP or UDP.
Connection Type	Selection between long-lived and short-lived is possible. Standard is Long-lived
Keepalive Interval	Entry between 60 and 180 seconds possible. Default = 100s.
Keepalive Retry	The number of repetitions here may be between 5 and 10 times. Standard = 10
Min Reconnect Interval	Min. reconnection interval between 15 and 180 seconds. Default = 15s.
Max Reconnect Interval	Min. reconnection interval between 180 and 3600 seconds. Default = 180s.
Source Interface	Selection of the corresponding interface that is to be redirected to
Trap Interval	The interval may be between 1 and 86400 seconds. Default = 30
Include RMC	Recommended minimum data set. When selected, the minimum of the GPS receiver is output
Include GSA	Active satellites. Information about PRN numbers of the satellites whose signal is used for position determination is output here.
Include GGA	Most important data set with time, position, height and quality of the measurement
Include GSV	Visible satellites. Provides information about satellites that can possibly be received at present and information about their position, signal strength, etc. Since only the information of four satellites can be transmitted per record (limitation to 82 characters), there can be up to three such records
Message Prefix	Input of a message prefix possible. Free input
Message Suffix	Input of a message suffix possible. Free input



Entering a destination address for a server is possible at this point.

3.3.5.4. GPS Serial Forwarding

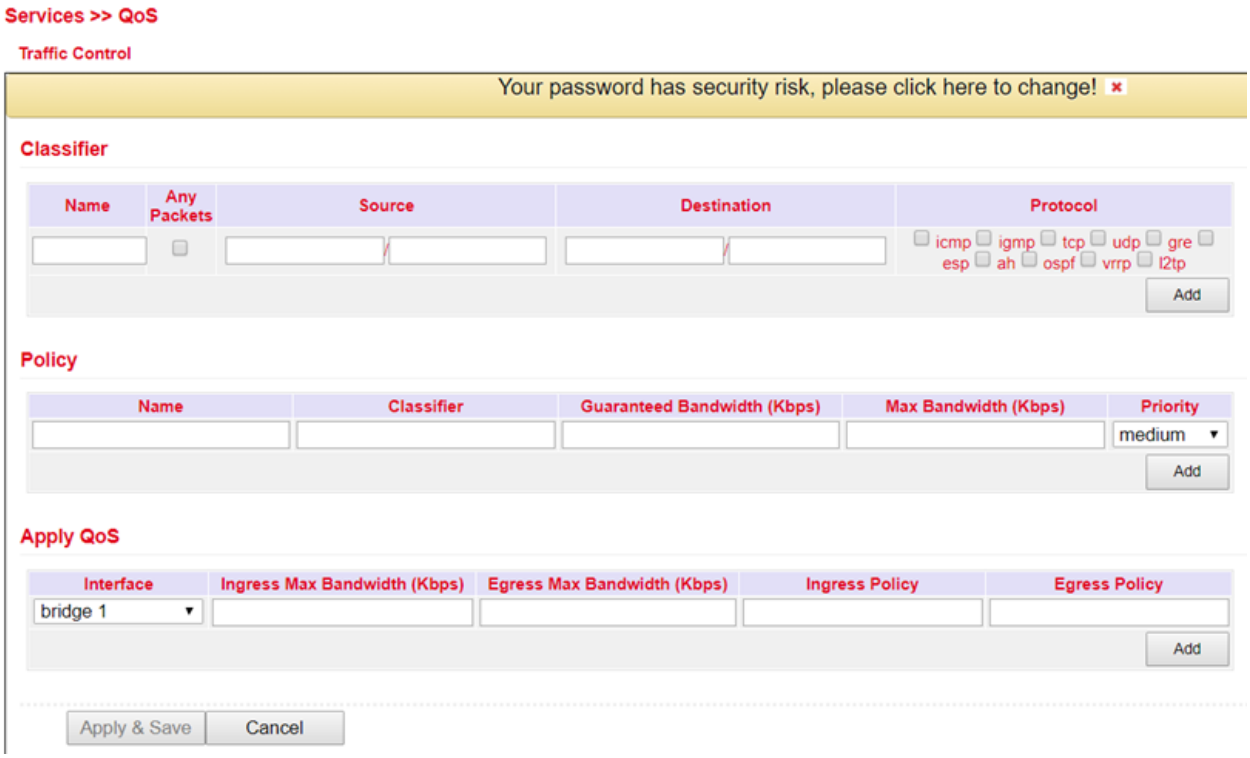
Open the menu under ***Services*** > ***GPS*** > ***GPS*** Serial Forwarding and click on the ***Enable*** checkbox to switch on the function. Here you can now make the appropriate settings. With ***Apply & Save*** you save the settings and activate them.



GPS Serial For-warding List	
Serial Type	Selection of the serial interface. RS232 or RS485.
Baud rate	Here the transmission rate can be selected. Value between 300 and 230400 possible. Default = 9600
Data Bits	Setting of the data bits. Selection between 7 bits and 8 bits. Default = 8 bits
Parity	Here the parity for the interface can be set. Default = none
Stop Bit	Setting of the stop bits. Default = 1 bit
Software Flow Control	Can be switched on or off. Default = off
Include RMC	Recommended minimum data set. When selected, the minimum of the GPS receiver is output
Include GSA	Active satellites. Information about PRN numbers of the satellites whose signal is used for position determination is output here.
Include GGA	Most important data set with time, position, height and quality of the measurement
Include GSV	Visible satellites. Provides information about satellites that can possibly be received at present and information about their position, signal strength, etc. Since only the information of four satellites can be transmitted per record (limitation to 82 characters), there can be up to three such records

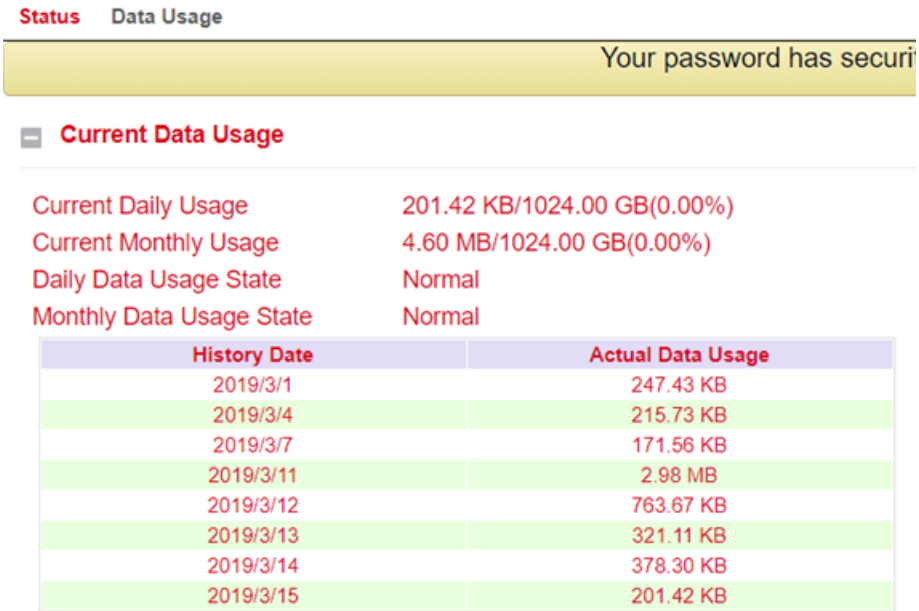
3.3.6 3.3.6. QoS

At this point the definition of Quality of Service is possible. Select ***Services > QoS.***



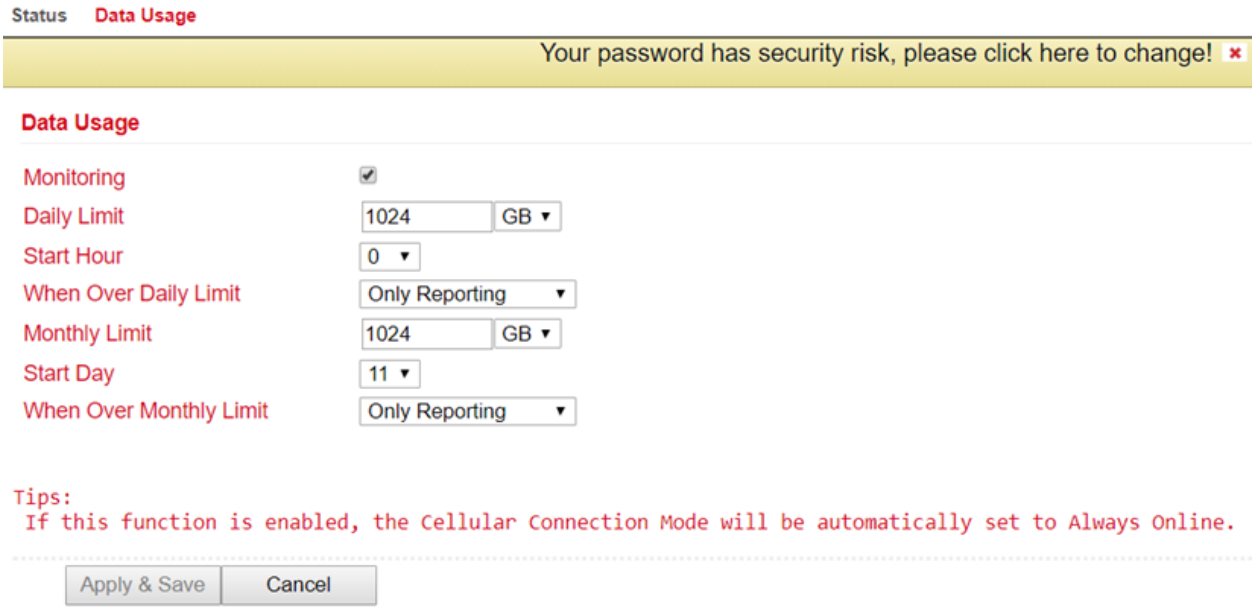
3.3.7 3.3.7. Data Usage

In this area you can see the consumption of your data if you have configured this under Data Usage. Select ***Services > Data Usage.***



3.3.7.1 Data Usage

Open the menu under Service > Data Usage and Data Usage. Now check the Monitoring box to activate this section. Now enter your data.



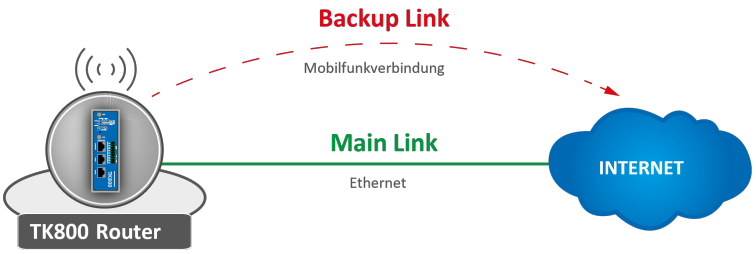
Data Usage	
Monitoring	Activate your data consumption display here
Daily Limit	Enter a guideline value for the daily limit here. Data can be entered in KB, MB or GB.
Start Hour	Time at which the measurement is to be started.
When Over Daily Limit	Here you can enter what should happen when the entered limit is reached or exceeded. Options are: Only Reporting Here, only the consumption value is displayed Stop Forward Here, the further consumption of data is stopped Shutdown Interface Here, the interface is switched off.
Monthly Limit	Enter an approximate value for the monthly limit here. Data can be entered in MB or GB.
Start Day	Select here the day on which the measurement for the monthly limit should start
When Over Monthly Limit	Here you can enter what should happen when the entered limit is reached or exceeded. Options are: Only Reporting Here, only the consumption value is displayed Stop Forward Here, the further consumption of data is stopped Shutdown Interface Here, the interface is switched off.

3.4 3.4. Link Backup

With the TK800, it is possible to use two different Internet connections (wired and cellular) to increase accessibility.

The router periodically checks the primary Internet connection and automatically switches to the secondary Internet connection in case of failure. As soon as the primary Internet connection is available again, the router automatically switches back to this connection.

In this example, a wired (Ethernet, DHCP) is used as the primary Internet connection and cellular (4G LTE) as the secondary.



Configuring a WAN Port – Modify Bridge (TK8X2-X only)

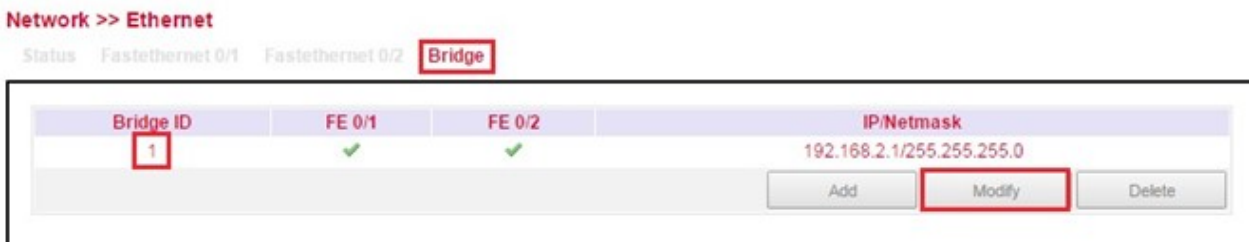
Hinweis

The prerequisite for Link Backup is Internet access via the cellular network. Therefore, configure the mobile network interface (Cellular) accordingly to be able to connect to the Internet. The router is preconfigured for T-Mobile SIM cards, so no configuration steps are usually necessary here.

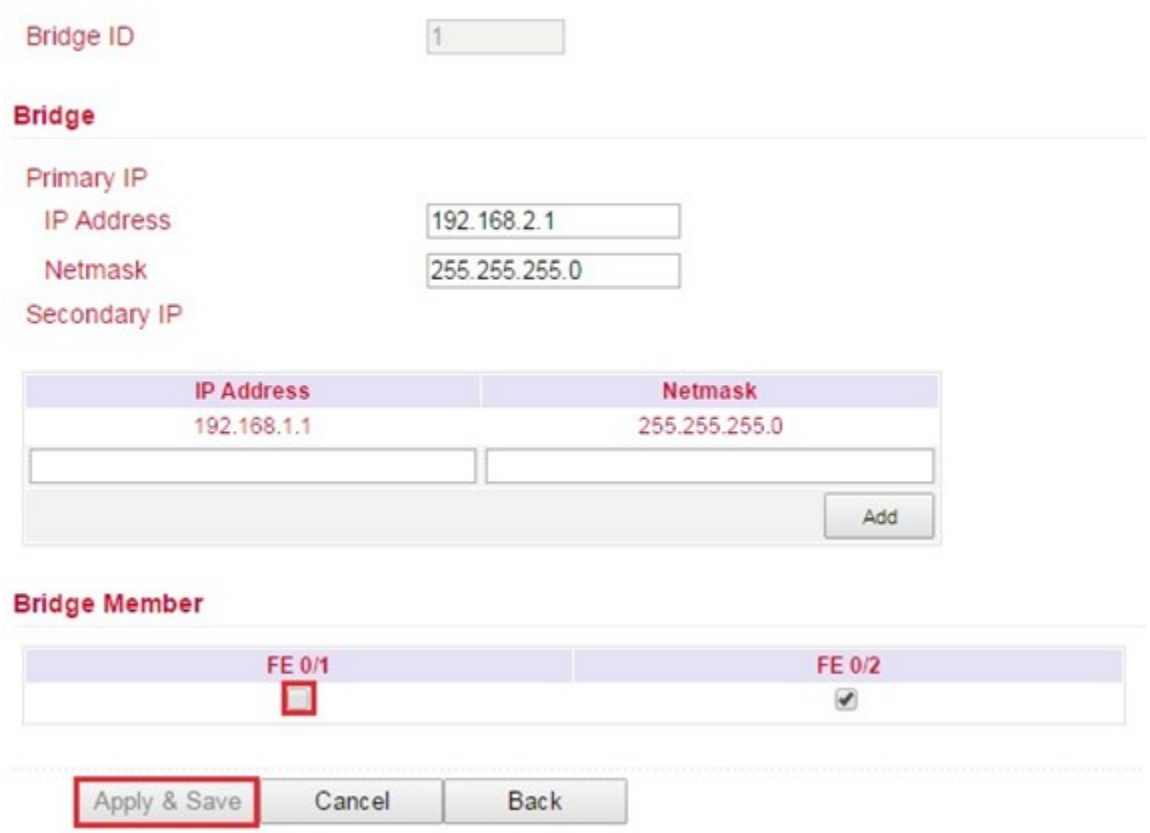
On the TK8X2-X, the two Ethernet ports are connected via a bridge at the factory. To configure one of the ports to the WAN port, the corresponding port must be excluded from the bridge.

To do this, perform the following steps:

1. Go to the subitem ***Ethernet*** via the subitem ***Network***.
2. Now select the ***Bridge*** tab
3. Click here in the line with the Bridge ID 1 and edit the entry by clicking ***Modify***.



4. Remove the check mark for the interface FE 0/1 and confirm the change with ***Apply & Save***.

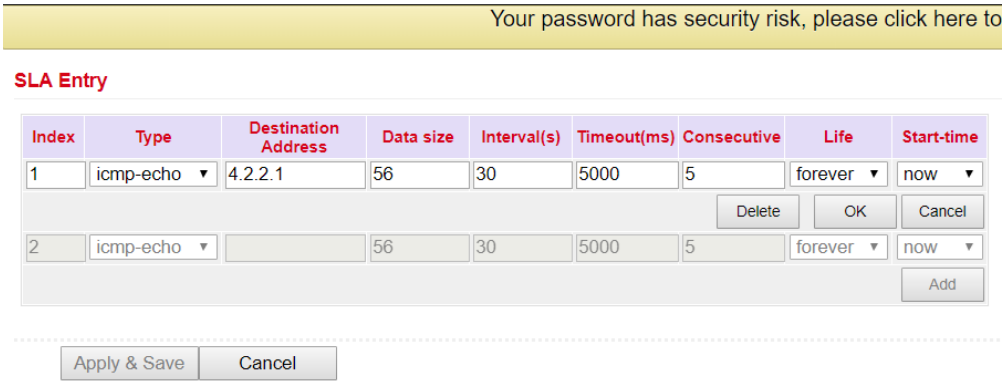


Configuring a WAN port

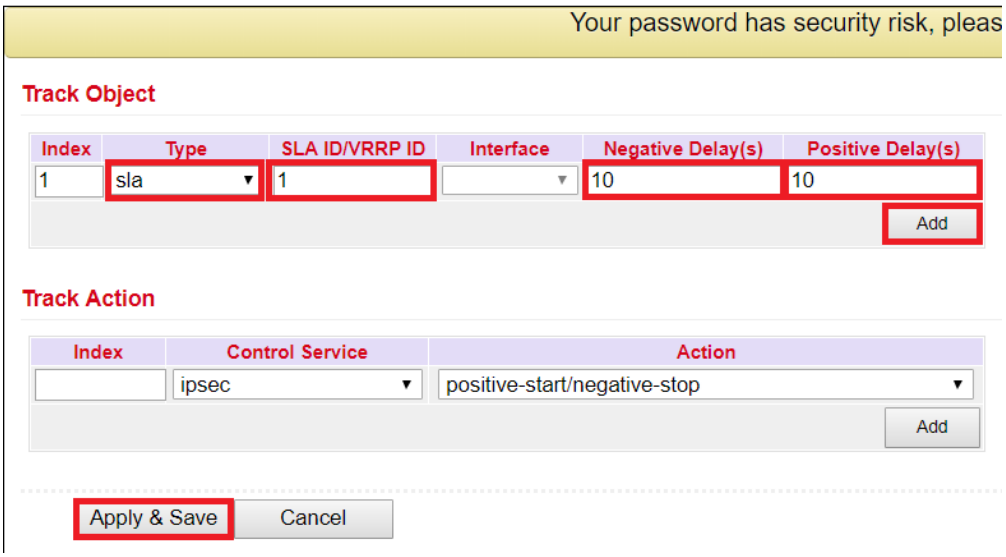
In this manual the port FE 0/1 is defined as WAN port. The New WAN Wizard is used for this purpose.

- In the Wizard menu, a new WAN port can be configured via the subitem New WAN
- as interface the Ethernet port (FE 0/1) currently detached from the bridge is specified, exemplary DHCP is also used for the port
- NAT must be activated if the connected devices are to establish a connection to the Internet

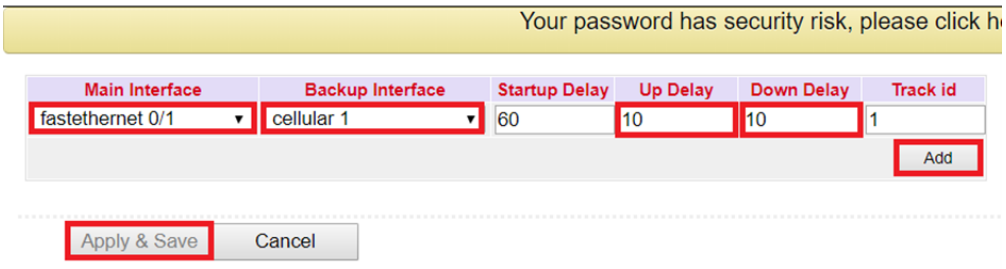
- in the next step the ICMP program (SLA) is configured
- Under IP Address (Destination Address) a pingable IP address with high availability should be entered (Note: In this example 4.2.2.1 was entered, since this address has a very high availability)
- all other data can be copied from the example



- the just created SLA program is monitored with the help of tracking to be able to register an interruption of the main line
- this is configured as shown in the following example



- to define which one acts as the main line and which one acts as the backup line, the backup interface is set up
- this is configured as shown in the following example



Description of the Configuration Elements:

Main Interface	primary line to be monitored
Backup Interface	secondary line, which is used in case of failure of the primary line
Startup Delay	switch-on delay of the interface monitoring
Up Delay	switching delay
Down Delay	switching delay
Track ID	Reference to ICMP monitoring

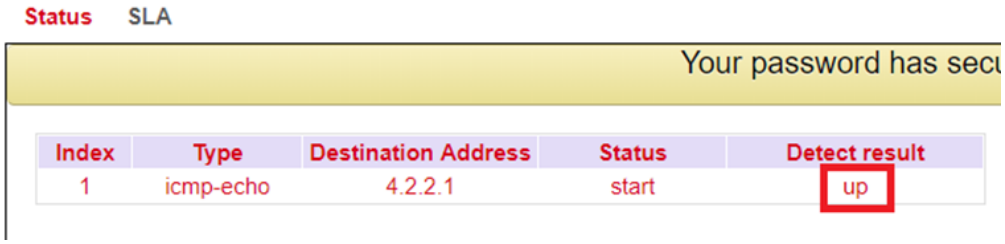
In the last step, the routing entries are created or adjusted as in the following example. It is important that the distance of the main line (here: FE 0/1) has a smaller value than that of the backup line. With the TrackID, the main line is bound to the ICMP monitoring that was created in the previous step ***Description of the configuration elements:***

Destination	Destination address where to be routed
Netmask	Subnet mask belonging to the destination address
Interface	Interface via which to send
Gateway	IP address via which to send
Distance	Route preference/cost
Track ID	Reference to ICMP monitoring

Main line works (Internet connection via WAN)

If the main line is working and an Internet connection is established through it, the following can be seen:

1. SLA-Status



2. Track-Status

3. Status of the cellular connection

Status Cellular

Your pa

Modem

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

4. Status of the WAN connection (Ethernet)

Status Ethernet 0/1 Bridge

Your pas

Fastethernet 0/1

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

5. Routing table

Route Table Static Routing

Your password has security risk, please click here to ch

Type: All

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

Main line does not work (Internet connection via cellular radio)

If the main line is not working and an Internet connection is established via the cellular interface, the following can be seen:

1. SLA-Status

Status SLA

Your password has secu

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

2. Track-Status

Status Track

Index	Status
1	negative

3. Status of the cellular connection

Status Cellular

Your pass

Modem

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

Network

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

4. Routing table

Route Table Static Routing

Your password has security risk, please click here to

Type: All

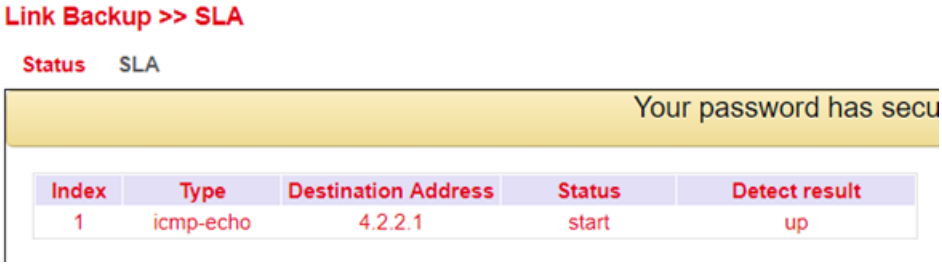
Type	Destination	Netmask	Gateway	Interface	Distance/Metric	Time
C	37.81.115.148	255.255.255.252		cellular 1	0/0	
C	127.0.0.0	255.0.0.0		loopback 1	0/0	
C	192.168.2.0	255.255.255.0		bridge 1	0/0	

3.4.1 3.4.1. SLA

SLA monitoring monitors the connections to peers within a network structure. Ping tests to defined destinations provide information about the availability of the peers and show the state of the line in the status (up or down).

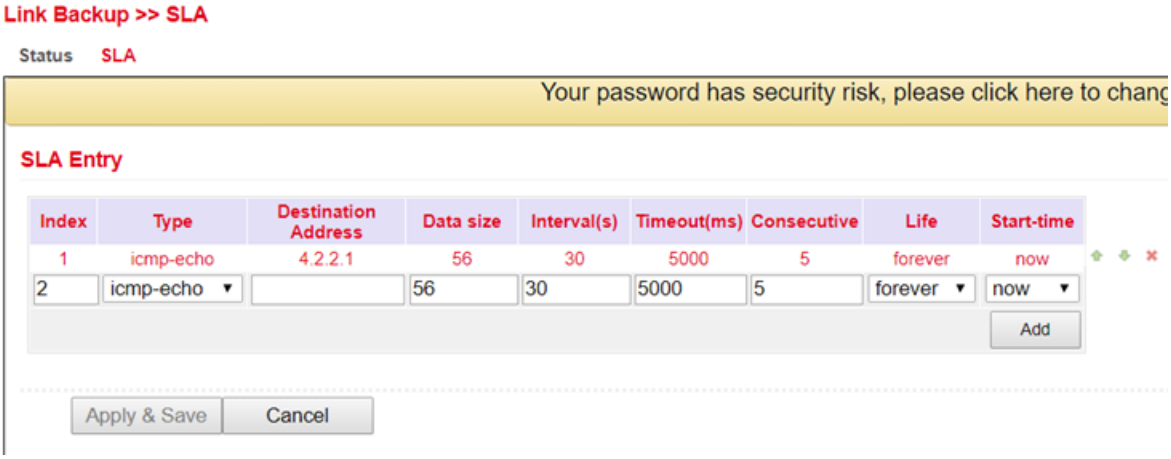
3.4.1.1. Status

The SLA status indicates whether the ping attempt is successful ***(Detect result up)*** or unsuccessful ***(Detect result down)***.



3.4.1.2. SLA Configuration

Enter the desired data under ***Link Backup*** > ***SLA*** > ***SLA*** to monitor the status of the line.



Parameter	Description
Index	Freely selectable, used to identify the entry.
Type	icmp-echo, a simple ping to check the connection.
Destination Address	The address that will be pinged. It should be highly available if possible, e.g. a Google DNS server (8.8.8.8).
Data size	The packet size of a ping, usually 56 bytes.
Interval(s)	The time interval in seconds at which the ping is executed.
Timeout(ms)	Timeout for a ping.
Consecutive	Number of retries, in case of a failed ping.
Life	forever, the ping should always be executed.
Start-time	now, the check should start immediately.

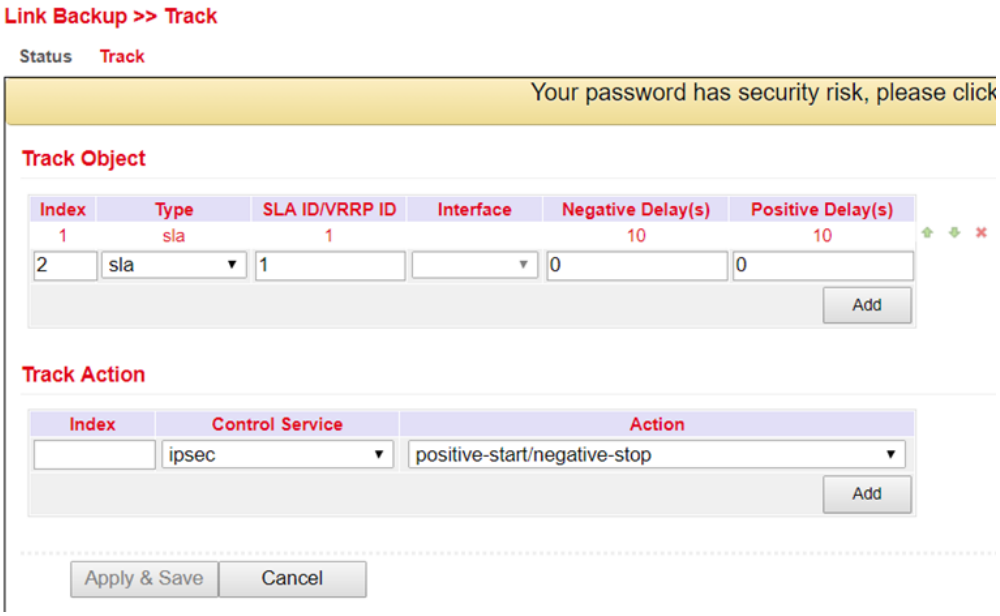
3.4.2 3.4.2. Track

3.4.2.1. Status

Displays the Track status, positive means that the ping attempt is successful or the interface is connected to the Internet. You can view the track status via ***Link Backup*** > ***Track*** > ***Status*** if it has been configured.

3.4.2.2. Track Configuration

Set up your track object under ***Link Backup*** > ***Track*** > ***Track***.

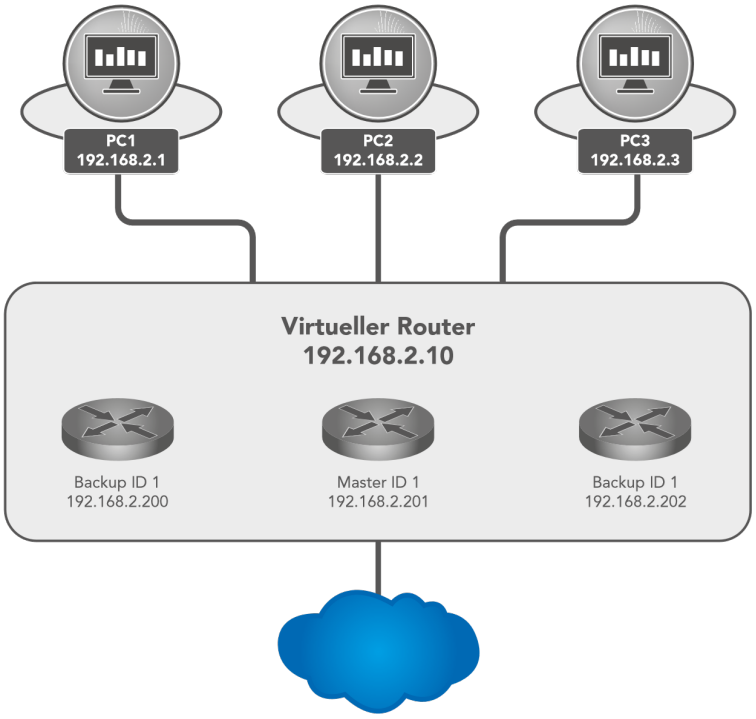


Parameter	Description
Index	Freely selectable. Used to identify the entry.
Type	SLA or interface.
SLA ID	Index, the SLA that was previously created.
Interface	Not used with SLA.
Negative Delay(s)	Delay when switching to the backup interface if the Internet connection on the main interface is lost.
Positive Delay(s)	Delay when switching to the main interface when the Internet connection is available again.

3.4.3 3.4.3. VRRP

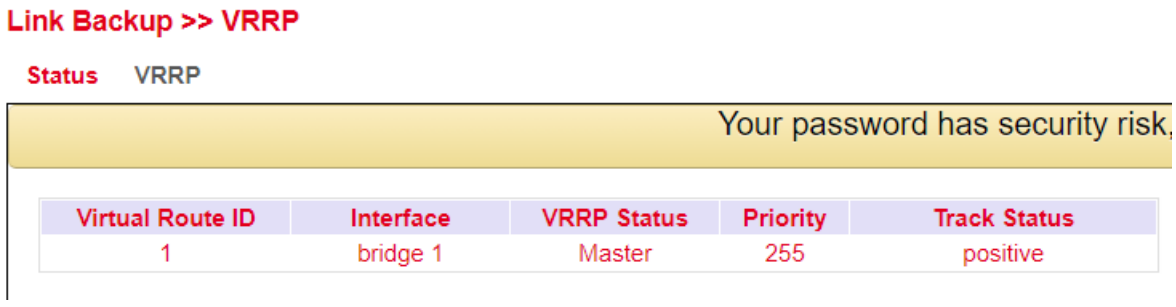
In a network, all participants have a common gateway for communication with other networks. If this gateway fails, communication with other networks (and the Internet) is no longer possible.

For this reason, there is the ***Virtual Router Redundancy Protocol (VRRP)***. This makes it possible to operate several routers (gateways) in tandem, but only one is active (master) at any given time. The other routers serve as backup if the master fails. All routers together represent a virtual router. Within this virtual router, VRRP then regulates the communication, so that if the master fails, a backup router immediately becomes the new master and thus the new gateway for the network.



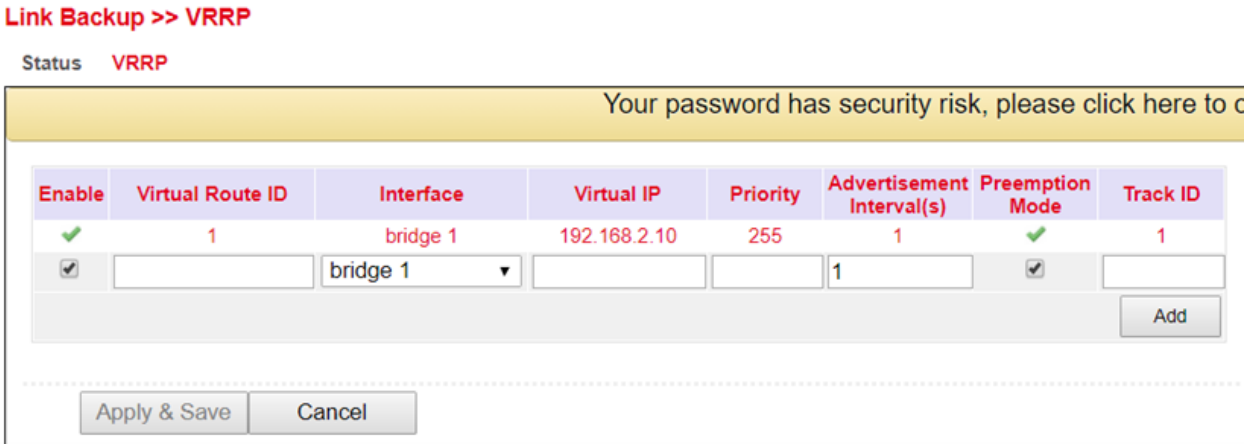
3.4.3.1. VRRP Status

Displays the status of the VRRP. Please refer to the description for details.



Parameter	Description
Virtual Route ID	Displays the router group in which the router is located
Interface	Displays the LAN interface
VRRP Status	Displays the current status, master or backup
Priority	Displays the priority of the router
Track Status	Displays whether the connection check is successful

3.4.3.2. VRRP Configuration



Parameter	Description
Enable	Enables or disables the configuration
Virtual Route ID	Freely selectable, specifies the virtual router group. Must be identical for all routers within the group.
Interface	The LAN Interface
Virtual IP	The virtual router IP, must be identical for all routers within the same group.
Priority	0-254 the higher, the stronger. The highest value within the group automatically becomes the master.
Adver-tisement Interval(s)	Time to check within the group to find out who is the master.
Preemption Mode	If switched on, the router automatically checks whether the priority is higher than that of the current master. If it is, then it makes itself the master and the current master becomes the backup router.
Track ID	Previously created track for connection check

VRRP Example:

First, set up a new SLA under ***Link Backup*** > ***SLA*** and then a track under ***Link Backup*** > ***Track***. Then configure ***Router A*** via ***Link Backup*** > ***VRRP*** > ***VRRP*** as shown in Figure 1.

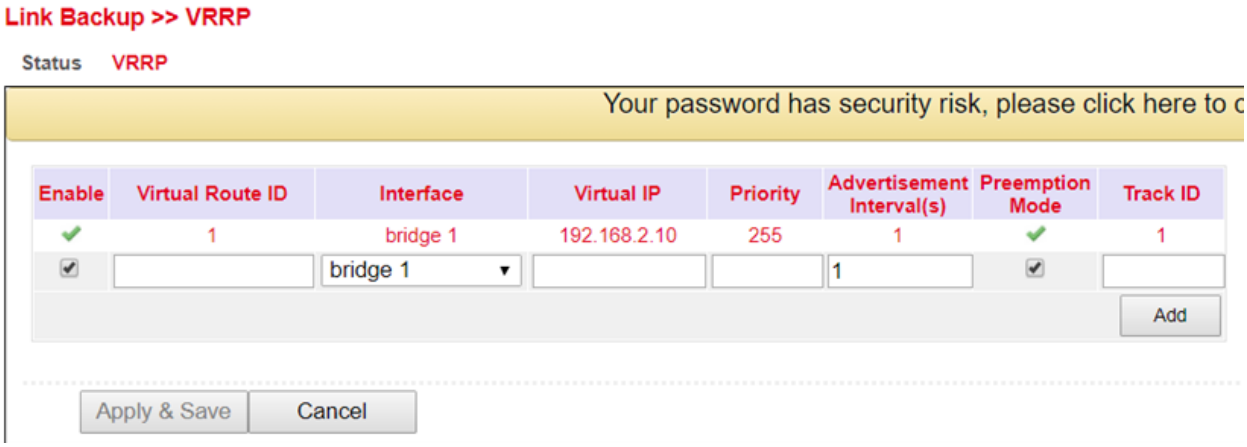


Figure 1 (Interface may differ depending on router model)

Now you can configure ***Router B*** as shown in Figure 2.

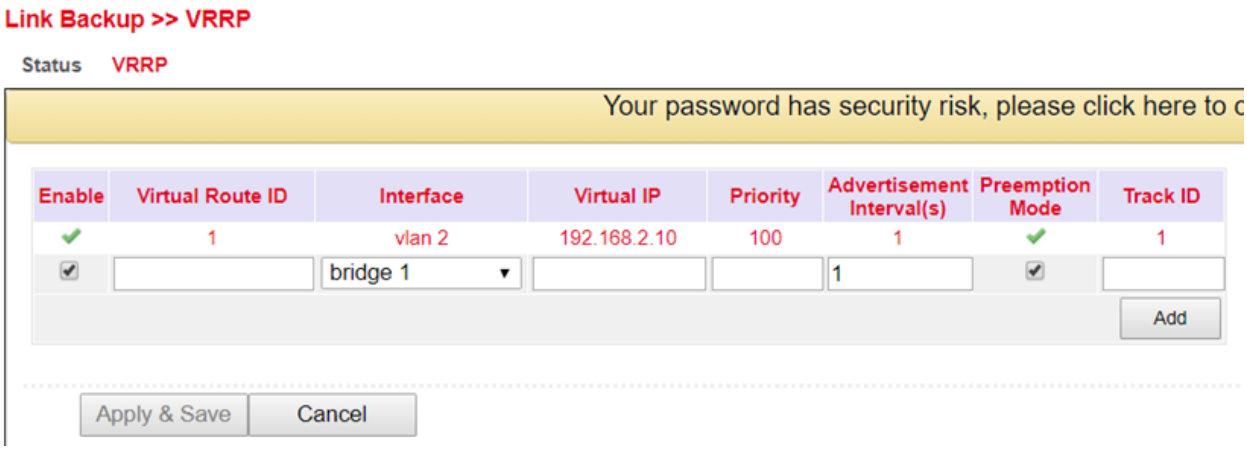
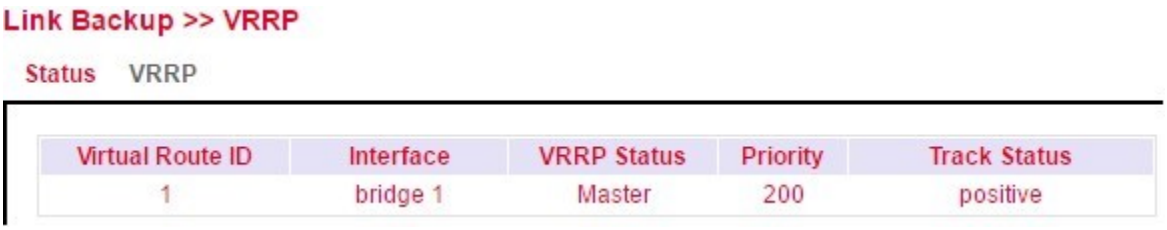


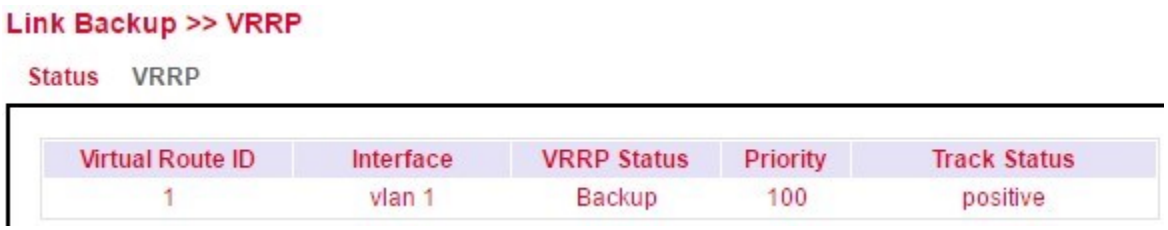
Figure 2 (Interface may differ depending on router model)

If you now go to the status page of VRRP ***(Link Backup > VRRP > Status)*** you should see the following on the routers:

Router A

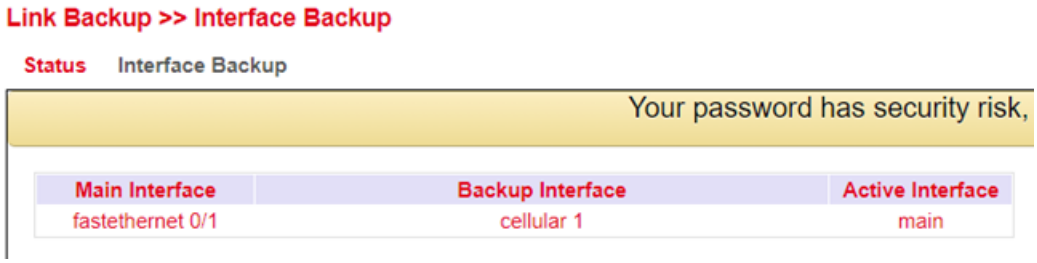


Router B



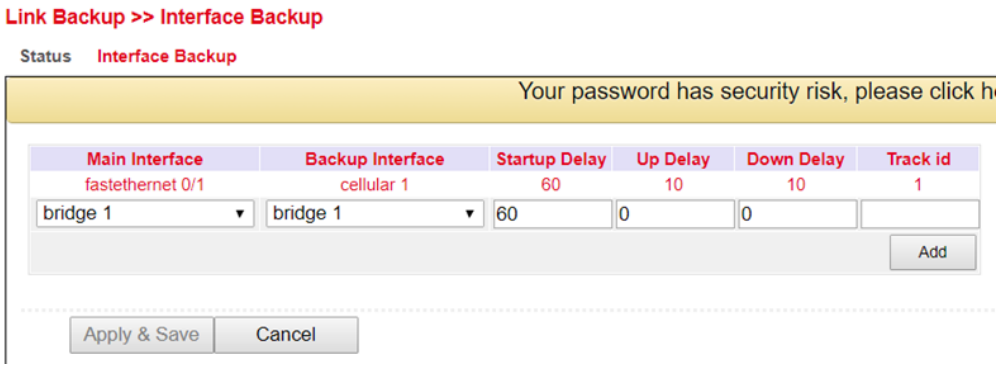
3.4.4 3.4.4. Interface Backup

Here you can create a backup of the interfaces of your router. If one interface fails, the other interface takes over the functions. To be accessed under ***Link Backup > Interface Backup.***



3.4.4.1. Interface Backup Configuration

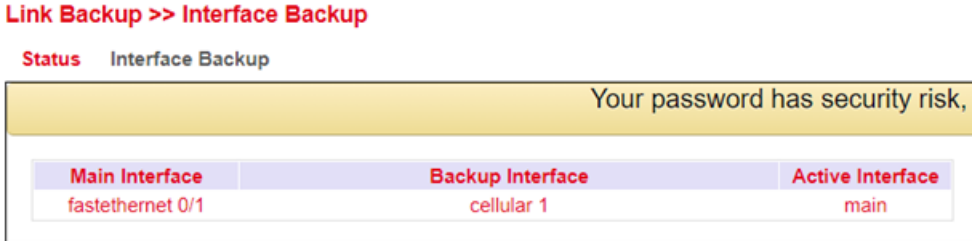
Under Link Backup > Interface Backup and Interface Backup you can define which interface should be the main interface and which should be the backup interface.



Parameter	Description
Main Interface	The main interface is defined here.
Backup Interface	The backup interface is defined here.
Startup Delay	Delay in seconds at system startup.
Up Delay	Delay when switching from the backup interface to the main interface.
Down Delay	Delay when switching from the main interface to the backup interface.
Track ID	The track index, from the previously created track entry.

3.4.4.2. Interface Backup Status

On the status page you can see which interfaces have been defined as main and backup. You can also see which interface is currently active (Active Interface main).



3.5 3.5. Routing

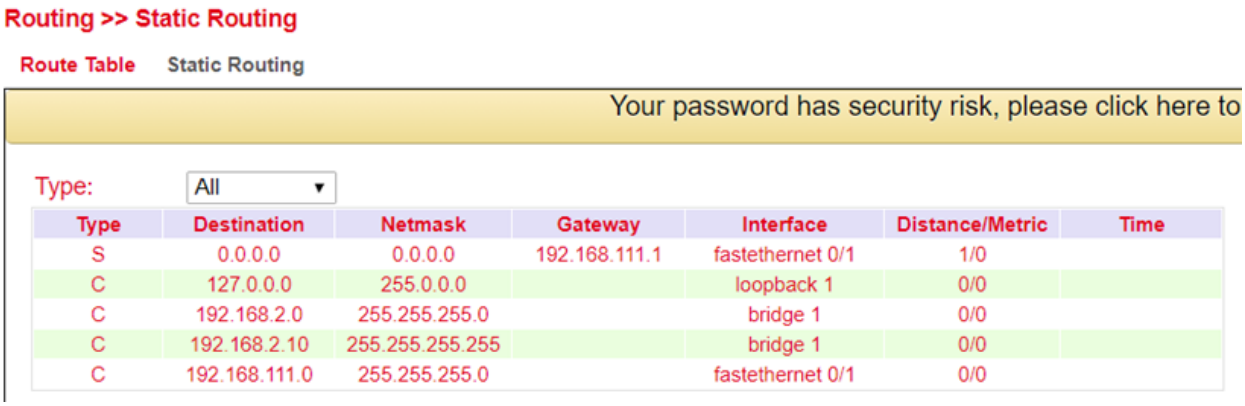
Routing is a generic term for the transport route of data packets between different networks controlled by routers. On the Internet, data packets can take completely different routes, since there are no direct connections between computers on the Internet. The destination of the data is contained in the so-called header. The data packets are not reassembled correctly until they reach the recipient. Routing allows data traffic to be very flexible and fail-safe.

3.5.1 3.5.1 Static Routing

Static routing, as the name suggests, is based on a fixed default path between any two end systems. The default is made when a network is installed and is usually stored as a fixed routing table in the router. The end devices are each assigned to a router via which they can be reached and can reach other destinations. To be reached under ***Routing > Static Routing.***

3.5.1.1. Route Table

The routing table can be found in the navigation under: ***Routing > Static Routing > Routing Table*** and ***Routing > Dynamic Routing > Routing Table***

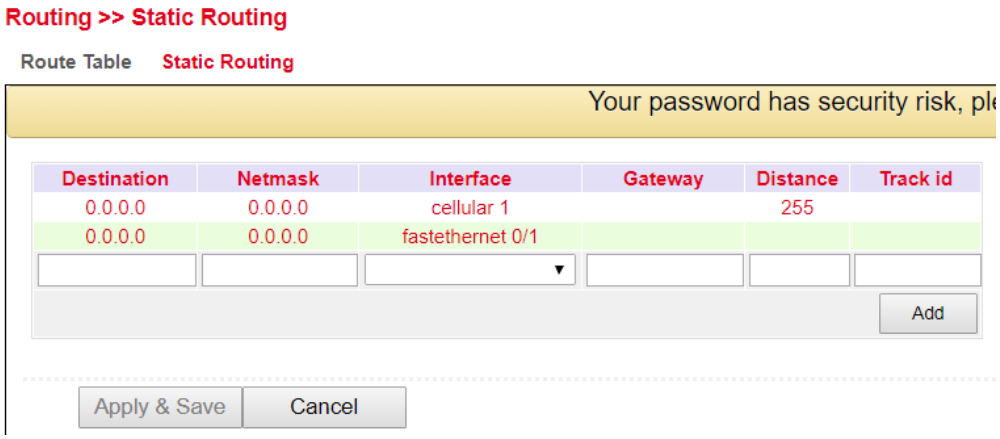


Type	Destination	Netmask	Gateway	Interface	Distance/Metric	Time
S	0.0.0.0	0.0.0.0	192.168.111.1	fastethernet 0/1	1/0	
C	127.0.0.0	255.0.0.0		loopback 1	0/0	
C	192.168.2.0	255.255.255.0		bridge 1	0/0	
C	192.168.2.10	255.255.255.255		bridge 1	0/0	
C	192.168.111.0	255.255.255.0		fastethernet 0/1	0/0	

Parameter	Description
Type	C = Connected / directly connected route, you are automatically added to a routing table when an interface is configured with an IP address S = Static route / manually entered route by the administrator R = RIP (Routing Information Protocol) / dynamic route added by RIP O = OSPF (Open Shortest Path First) / dynamic route added by OSPF
Destination	The destination is the target host, subnet address, network address, or default route. The destination for a default route is 0.0.0.0.
Netmask	The network mask is used with the destination to determine when a route is used. For example, a host route has a mask of 255.255.255.255, a default route has a mask of 0.0.0.0, and a subnet or network route has a mask between these two values.
Gateway	The gateway is the IP address of the next router to which a packet must be sent.
Interface	The interface is the network interface to be used to get to the next router. Cellular 1 = radio interface GSM Loopback 1 = internal loopback address (loopback) FastEthernet 0/1 = network port FastEthernet 0/1 on the router VLAN 1 = network ports which are assigned to VLAN 1.
Distance/Metric	Distance/Metric is the priority of the route. If several routes lead to the same destination, the route with the lowest metric is considered the best route.
Time	Time

3.5.1.2. Static Routing

Static routes are set up in the navigation under ***Routing*** > ***Static Routing*** > ***Static Routing***. Normally no static route has to be entered. The router enters the routes itself by making changes in the configuration.



Parameter	Description
Destination	The destination is the destination host, subnet address, network address, or default route. The destination for a default route is 0.0.0.0.
Netmask	The network mask is used with the destination to determine when a route is used. For example, a host route has a mask of 255.255.255.255, a default route has a mask of 0.0.0.0, and a subnet or network route has a mask between these two values.
Interface	The interface is the network interface to be used to get to the next router. cellular 1 = radio interface GSM fastethernet 0/1 = network port FastEthernet 0/1 on the router VLAN 1 = network ports, which are assigned to VLAN 1. bridge 1 = at TK8X5-EXW and TK8X2
Gateway	The gateway is the IP address of the next router to which a packet must be sent.
Distance	Distance/Metric is the priority of the route. If several routes lead to the same destination, the route with the lowest metric is considered the best route.
Track id	Track index or identification number

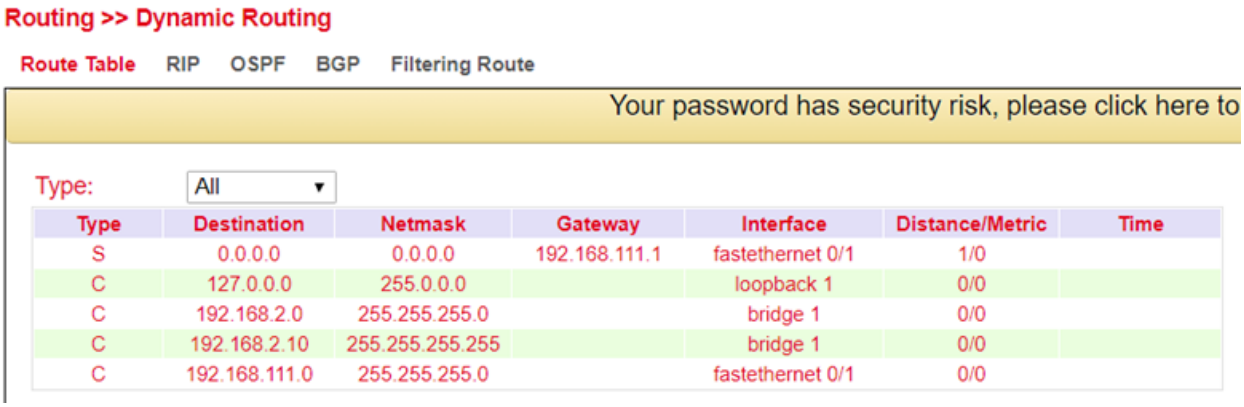
3.5.2 3.5.2. Dynamic Routing

Dynamic routing is used to have routes controlled automatically by the routing protocol used. The advantage of dynamic routing over static routing is that the route selection is dynamic, i.e. it takes place during operation. Routes are learned and set automatically by the algorithm of the routing protocol.

3.5.2.1. Route Table

The routing table can be found in the navigation under:

Routing > Dynamic Routing > Routing Table

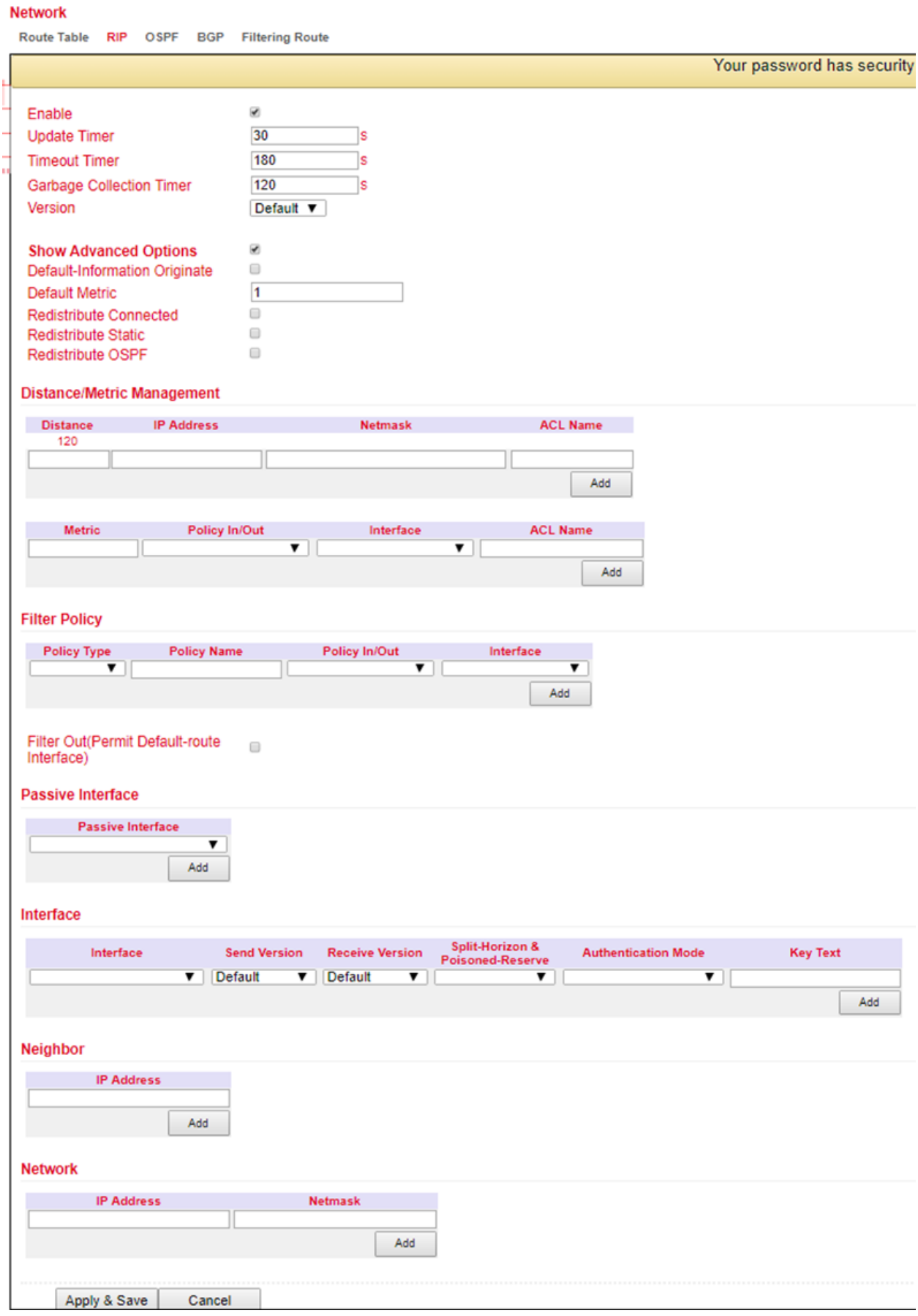


Parameter description see 3.5.1.1

3.5.2.2. RIP

RIP (Routing Information Protocol) is a dynamic routing protocol that uses a distance vector algorithm. RIP learns dynamic routing addresses from other routers and stores them in its routing tables. The distance and costs to other networks are put into relation from the router's point of view and the cheapest way to the destination network is also specified in the routing tables. Based on this information, the cheapest and shortest path to the destination network can be determined and taken. 15 hops is the maximum distance that a path to the destination network may be during RIP.

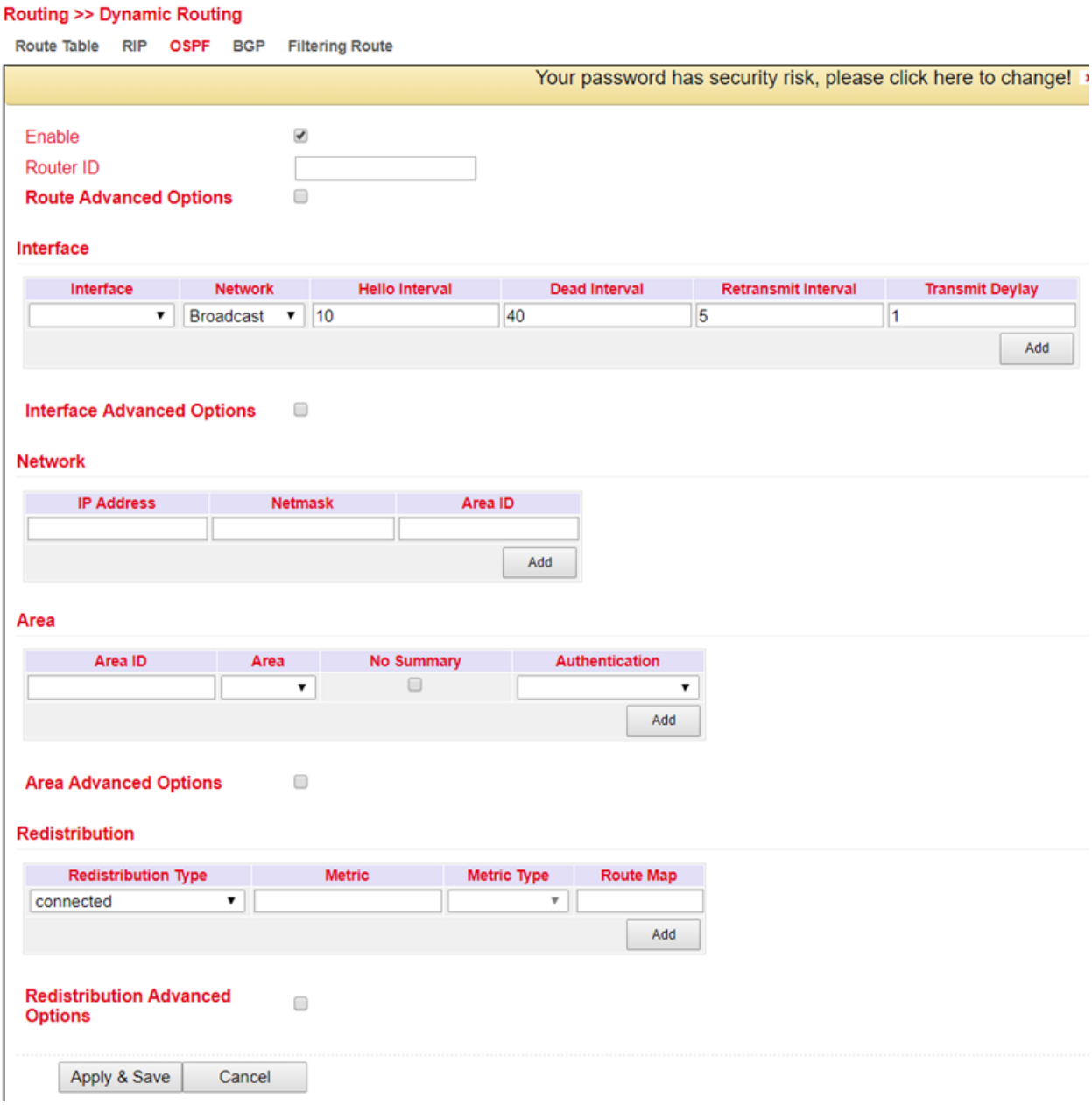
In the menu ***Routing*** > ***Dynamic Routing*** > ***RIP*** you can adjust the following settings:


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

3.5.2.3. OSPF

OSPF (Open Shortest Path First) is a dynamic routing protocol that describes how routers propagate the availability of connection paths between data networks. It supports hierarchical network structures and, in contrast to RIP, several simultaneous connection paths of the same cost to a subnetwork. It is able to transmit the occurring data traffic over different connection paths. The OSPF protocol is particularly fast with respect to changes in the network topology and is characterized by economical use of bandwidth when creating new routing tables.

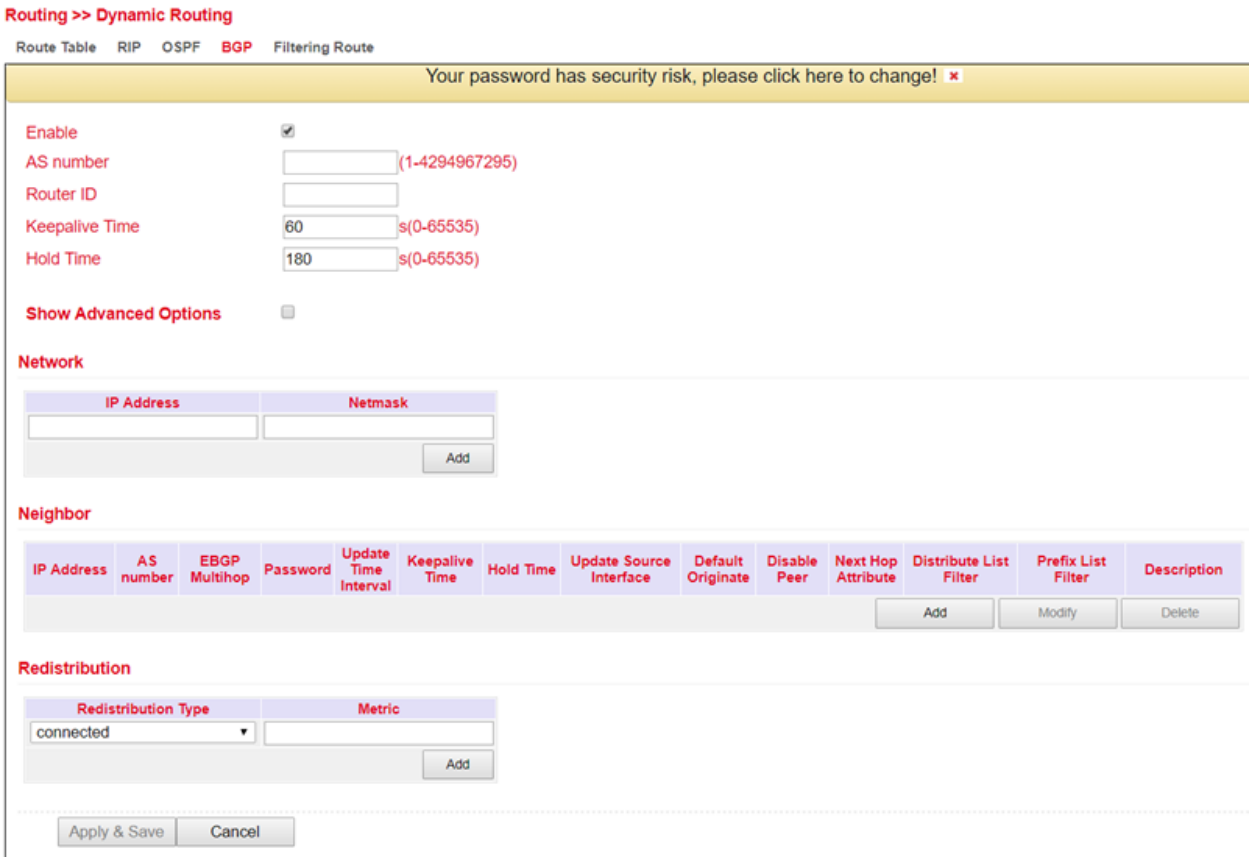
In the menu ***Routing*** > ***Dynamic Routing*** > ***OSPF*** you can adjust the following settings:



3.5.2.4. BGP

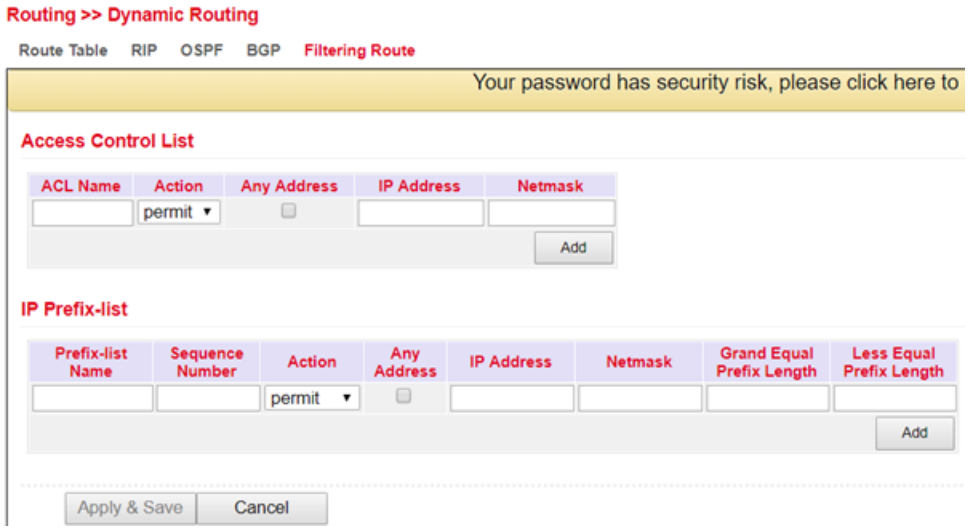
The Border Gateway Protocol (BGP) is the routing protocol used on the Internet and connects autonomous systems (AS) with each other. These autonomous systems are usually formed by Internet service providers. BGP is commonly referred to as Exterior Gateway Protocol (EGP) and Path Vector Protocol and uses both strategic and technical-metric criteria for routing decisions, although in practice business aspects are usually taken into account. Interior gateway protocols (IGP) such as OSPF are used within autonomous systems.

In the menu ***Routing*** > ***Dynamic Routing*** > ***BGP*** you can adjust the following settings for BGP:



3.5.2.5. Filtering Route

In the menu ***Routing*** > ***Dynamic Routing*** > ***Filtering Route*** you can adjust the following settings:

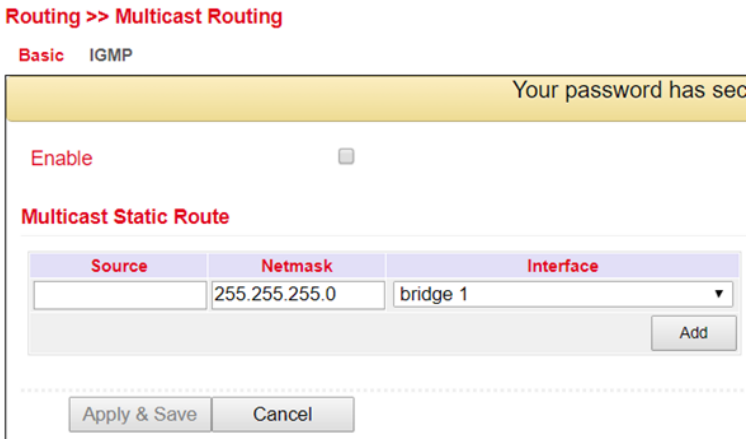


3.5.3 3.5.3. Multicast Routing

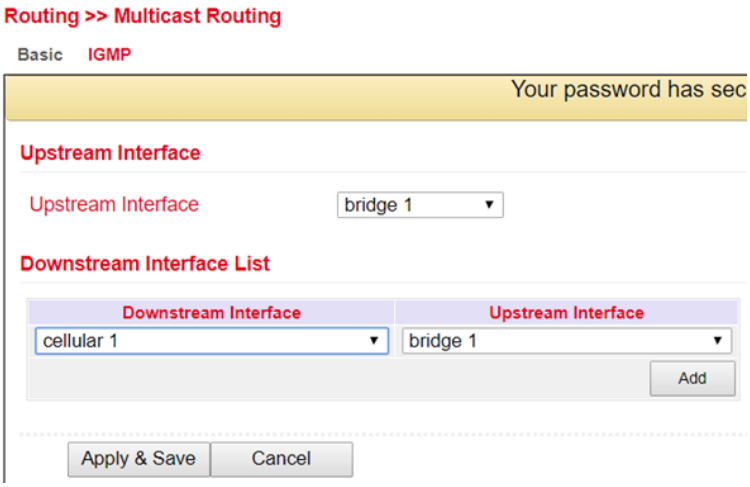
The Internet Group Management Protocol (IGMP) is based on the Internet Protocol (IP) and enables IPv4 multicasting (group communication) on the Internet. IP multicasting is the distribution of IP packets under one IP address to multiple stations simultaneously.

3.5.3.1. Basic

In the menu ***Routing*** > ***Multicast Routing*** > ***Basic*** you can adjust the following settings:



3.5.3.2. IGMP



The ***Upstream Interface*** is used to select the interface over which the multicast is to be distributed.

With the ***Downstream Interface List*** the interfaces for the downstream and upstream interface are selected from the drop-down menu.

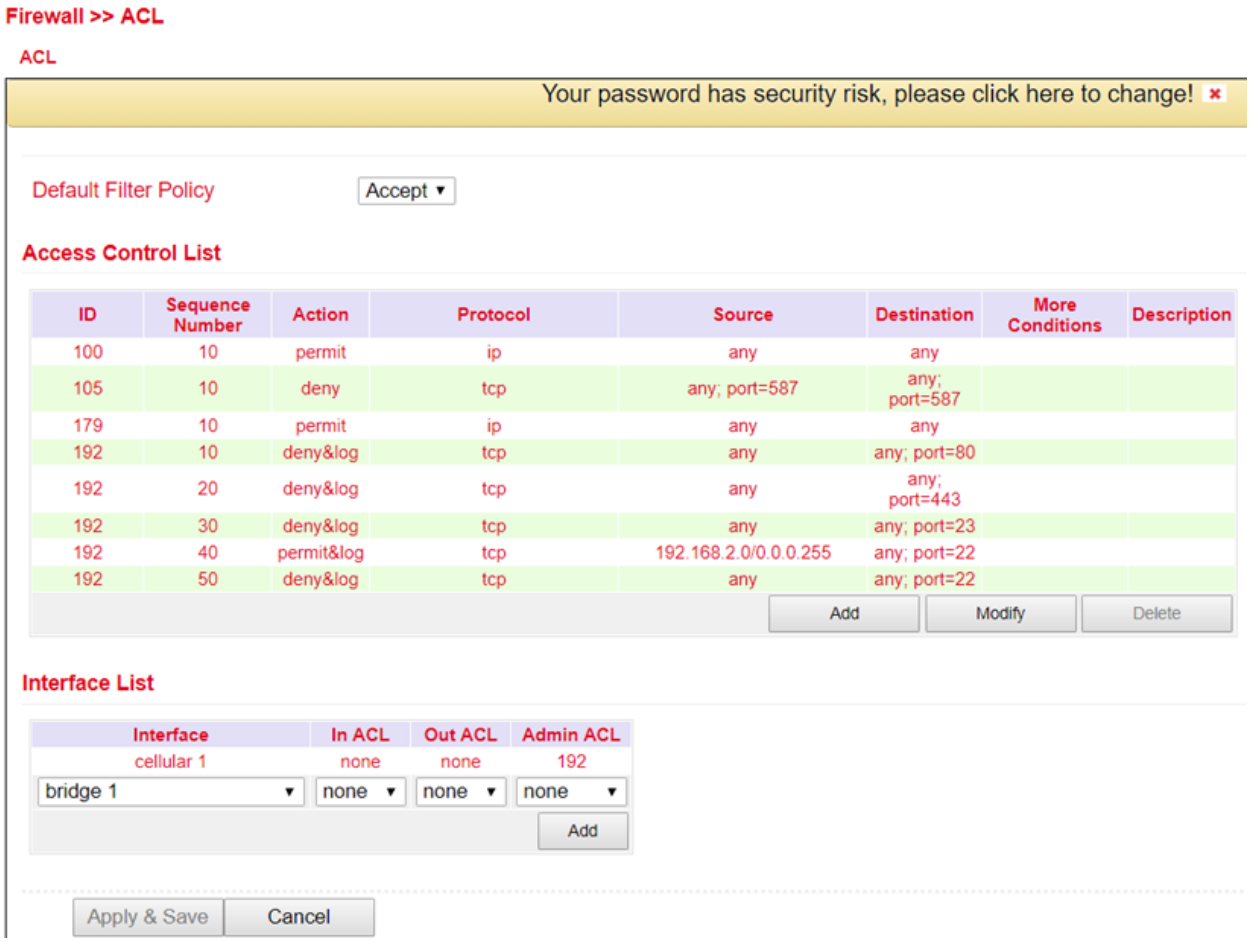
The interfaces may vary depending on the model.

3.6 3.6. Firewall

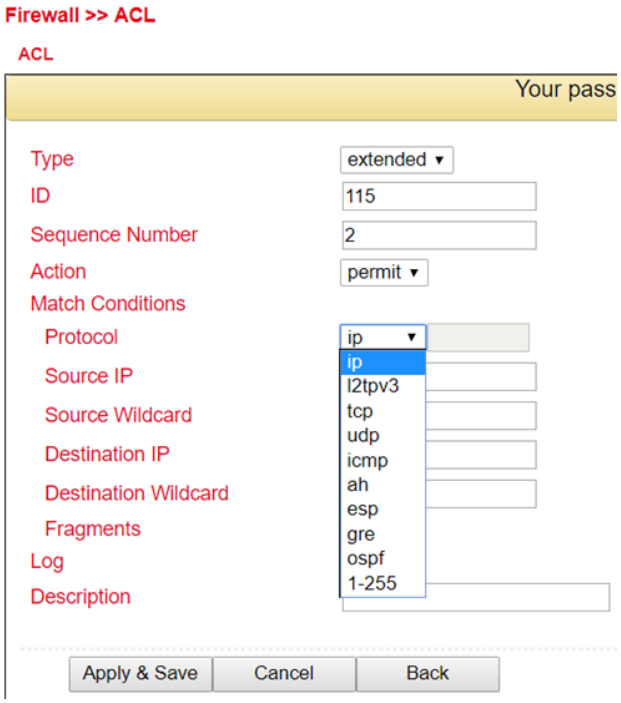
3.6.1 3.6.1. ACL

The ACL (Access Control List) is an access control list to control usage and administration. The ACL defines which computers or networks can access the router or networks behind the router. With the ACL, incoming and outgoing data packets are analyzed and managed according to the ACL ruleset.

ACL rules can be created on source and destination IP addresses, TCP and UDP port numbers, etc. to control access.



Here is an overview of the existing ACL rules. To create a new ACL you should click ***Add***.



Standard ACL can allow or block any communication from a network or to a network, or prohibit all communication.

Extended ACL provides extended setting options for source and destination networks within an ACL. Protocols from different levels can be selected. This means that individual services such as Web (http), FTP, Telnet, etc. can be allowed or forbidden.

Parameter	Description
Type	extended or standard
ID	ID 100 is preconfigured by default. Further IDs can be configured freely.
Action	Permit / Deny
Protocol	Protocols that are available
Source IP	Source IP address or network e.g. 192.168.2.0
Source Wildcard	Source wildcard is the wildcard address of the subnet. E.g. for the subnet mask 255.255.255.0 the wildcard address is 0.0.0.255
Destination IP	Destination IP address or network e.g. 172.16.0.0
Destination Wildcard	Target wildcard is the wildcard address of the target subnet e.g. with subnet mask 255.255.0.0 the wildcard address is 0.0.255.255
Description	Text Description field for the ACL

3.6.2 3.6.2. NAT

Network Address Translation (NAT)

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

Use of Source NAT

It allows devices with private network addresses to connect to the Internet. Private IP addresses cannot usually be routed by the provider, so they must be translated into a public, routable IP address. The TK800 has implemented this function, which enables communication between different networks. In addition, a relevant security aspect is found in NAT, since a public IP address cannot be traced back to the associated private IP address. This function is configured in the TK800 router at the factory.

Use of Destination NAT

This is used to provide server services running on computers under a single IP address. It is often referred to as port mapping or port forwarding. This function must be explicitly set up on the TK800.

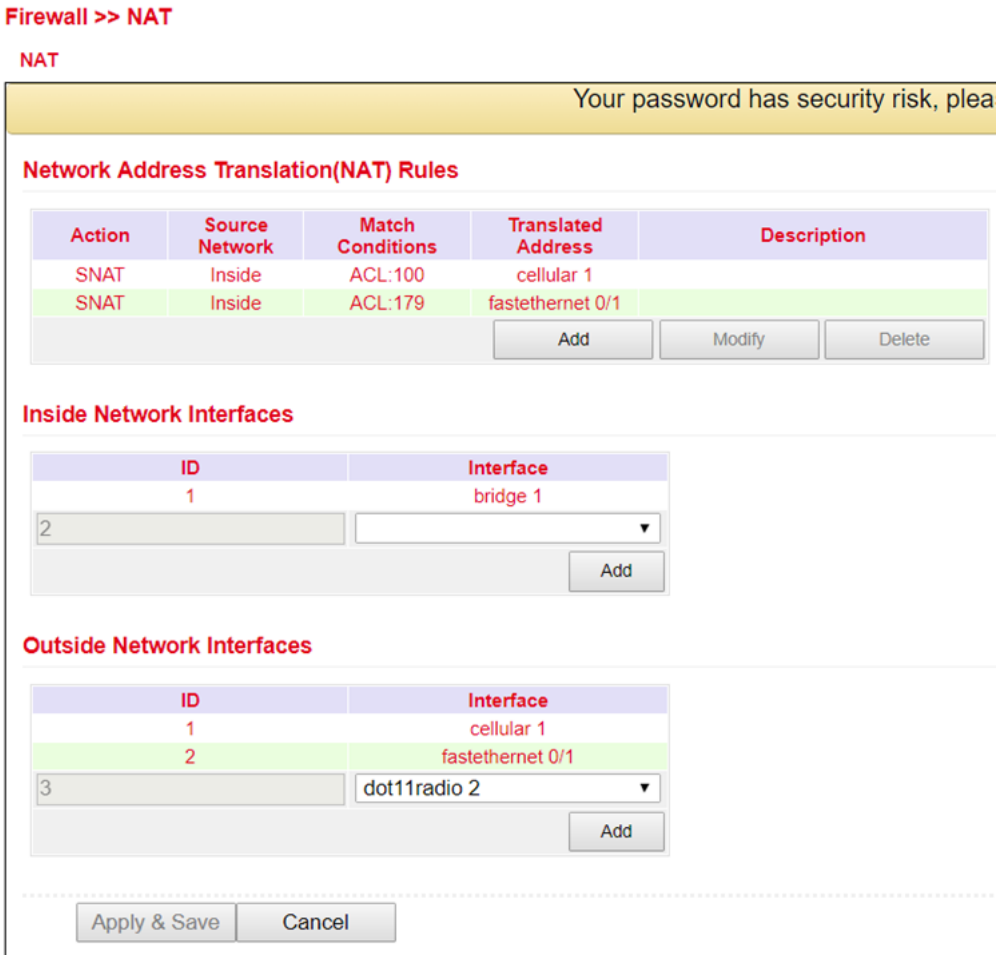
Use of 1:1-NAT

A special form of destination NAT is 1:1 NAT. It is used, for example, when a central location wants to access different sites via VPN, which are all configured with the same IP network addresses. This is frequently encountered in machine networks.

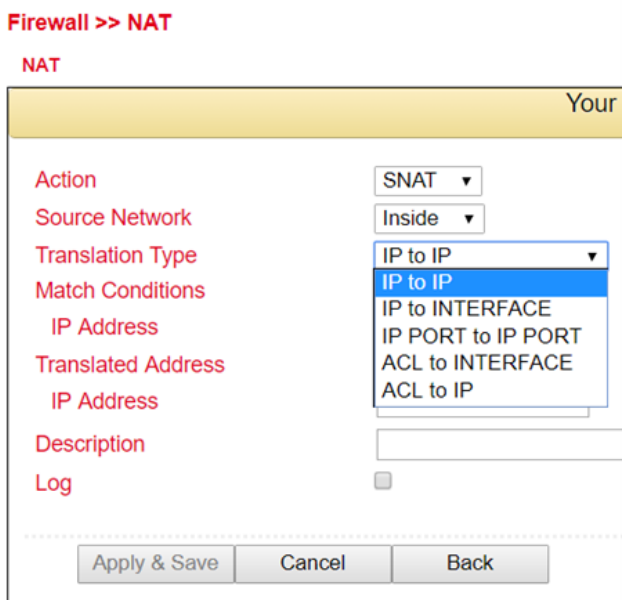
Configuration

- to configure NAT, go to the ***Firewall*** menu item and select ***NAT***
- here you can find a list of all existing NAT rules and the definition of the ***Inside***-(LAN-) and ***Outside***-(WAN-) interfaces

(***Note***: For some use cases it is necessary to create and use an ***ACL*** (Access Control List))



- by clicking *Add* a new NAT rule can be configured in the following menu (Fig. 2)

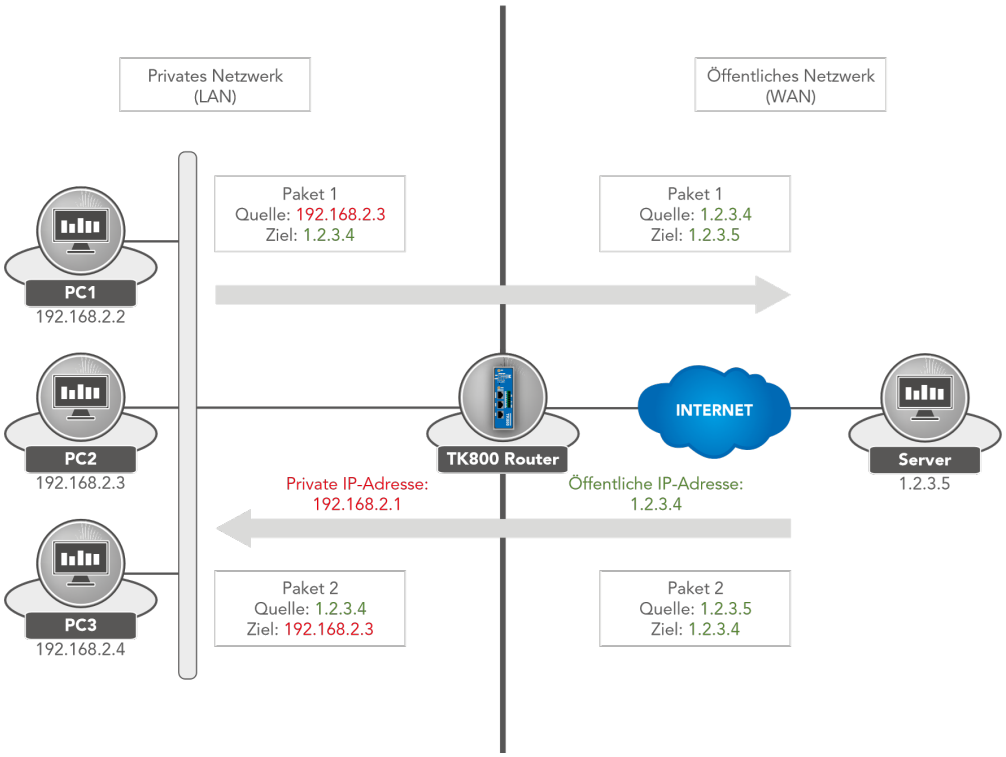


	Action
SNAT	Rewrite IP address of the computer that establishes the connection
DNAT	Rewrite IP address of the addressed computer
1:1NAT	Translate IP address one-to-one
	Source Network
Inside	Packets originate from an internal interface (LAN)
Outside	Packets originate from an external interface (WAN)
	Translation Type
IP to IP	Translate one IP address to another
IP to Interface	Translate an IP address to the IP address of a single interface
IP Port to IP Port	Translate one combination of IP address and port to another
ACL to Interface	Translate an IP address according to ACL rule into an IP address of a single interface
ACL to IP	Translate an IP address to another IP address according to ACL rule

Examples Case 1: SNAT (TC router as Internet gateway)

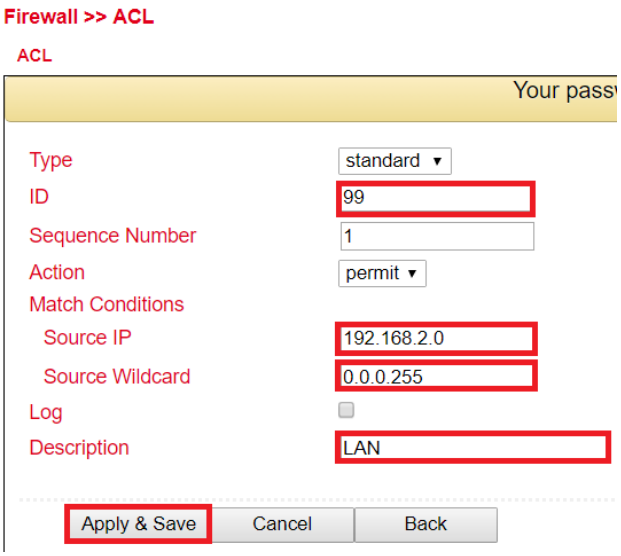
The TK800 works as an Internet gateway for connected devices with private IP addresses. It translates private IP addresses from the LAN into a public, routable Internet address.

(***Note***: This is the factory setting of all Welotec routers).

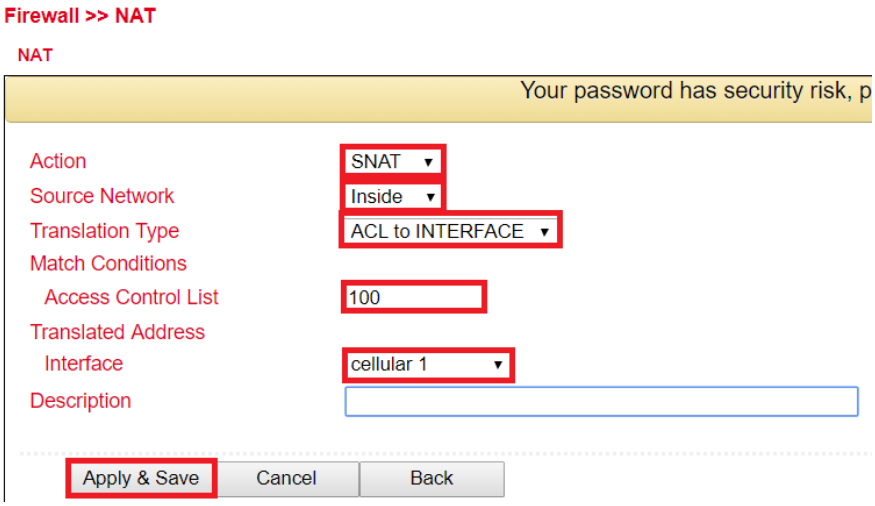


1. Configure the ACL rule. To do this, go to the ***Firewall*** menu and select the ***ACL*** subitem.
2. Now assign an ***ID*** for the rule and enter the ***IP address*** and the corresponding ***Wildcard mask***.

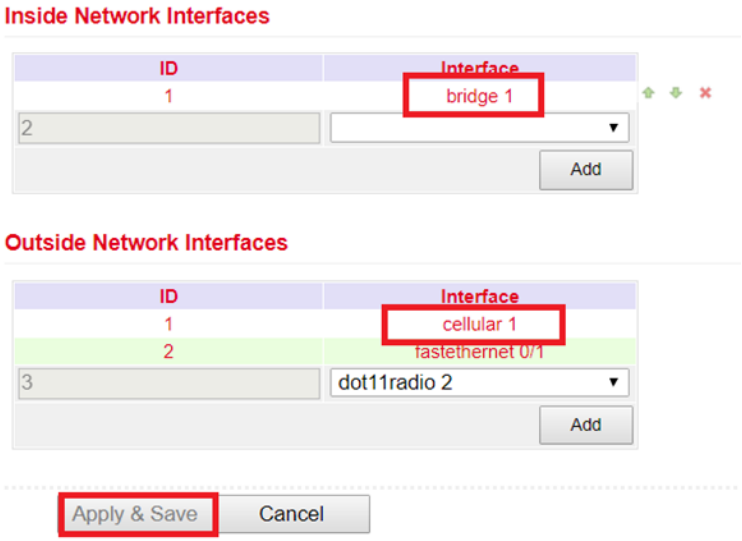
(***Note***: The wildcard mask is the inverted netmask and is used by routers to edit ***ACLs*** (Access Control Lists)).



3. Now configure the ***SNAT rule.***



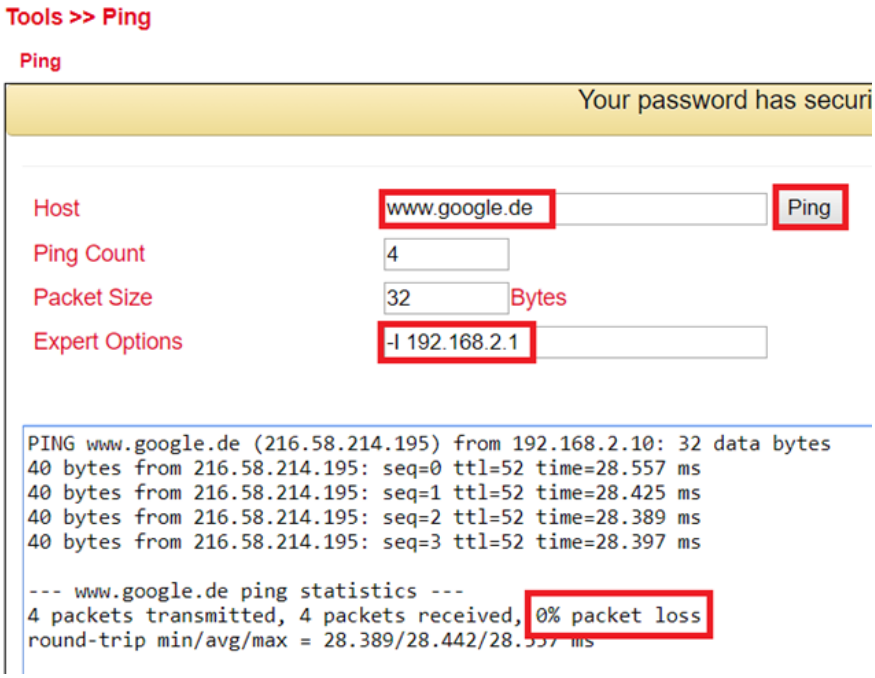
4. Now define the ***inside*** and ***outside interface***.



5. Test the access via the tool ***ping***. This can be done directly from the router. To do this, go to the ***Tools*** menu to

the ***Ping*** subitem and enter the values according to the example.

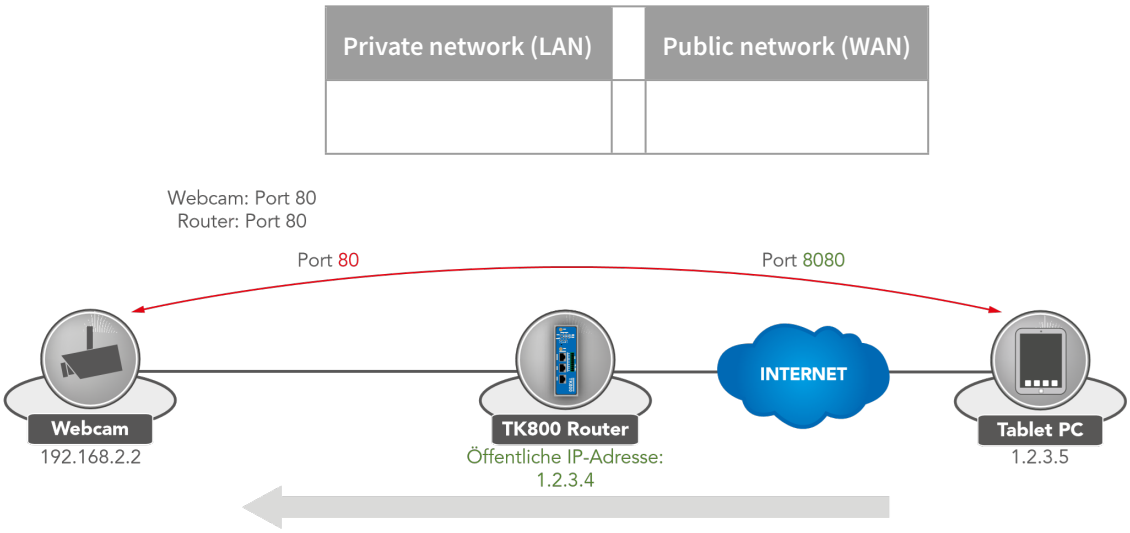
(***Note***: Use the ***Expert option*** –I 192.168.2.1 (capital i) so that access is from the inside (LAN) interface of the TK800 router).



Case 2: DNAT (Portmapping / Port Forwarding)

Access to connected devices via the Internet

Usually, users want to access devices connected to the Welotec Router via the Internet. Since these devices (e.g. webcam, control of a PLC, etc.) do not have their own mobile or Internet access, the Welotec Router must forward the requests from the Internet to the devices. This is done using the so-called port forwarding / port mapping function.



Packet Source: 1.2.3.4.8080 Destination: 192.168.2.2.80		Package Source: 1.2.3.5.8080 Destination: 1.2.3.4.8080

Requirements

- Public IP address in the mobile network (or also for wired Internet connections).

(***Note:*** Many mobile operators offer tariffs for business customers to access mobile devices, e.g. T-Mobile IP VPN or Vodafone CDA. Furthermore, there are providers who provide you with a public IP address via a conventional mobile phone card).

Hinweis

- Router Firmware **1.0.0.r9919** or higher

Port Mapping Notes

The following information must be available for port mapping to be set up:

- IP address of the device that is to be accessed
- Port to be redirected (e.g. http/80 from the device that is to be accessed).

Example Welotec Router

LAN IP address:	192.168.2.1
Subnet mask: Webcam	255.255.255.0
LAN IP address:	192.168.2.2
Subnet mask:	255.255.255.0
Standard Gateway:	192.168.2.1

The webcam has an interface that can be accessed via **http://192.168.2.2**.

(Note: http protocol uses TCP port 80)

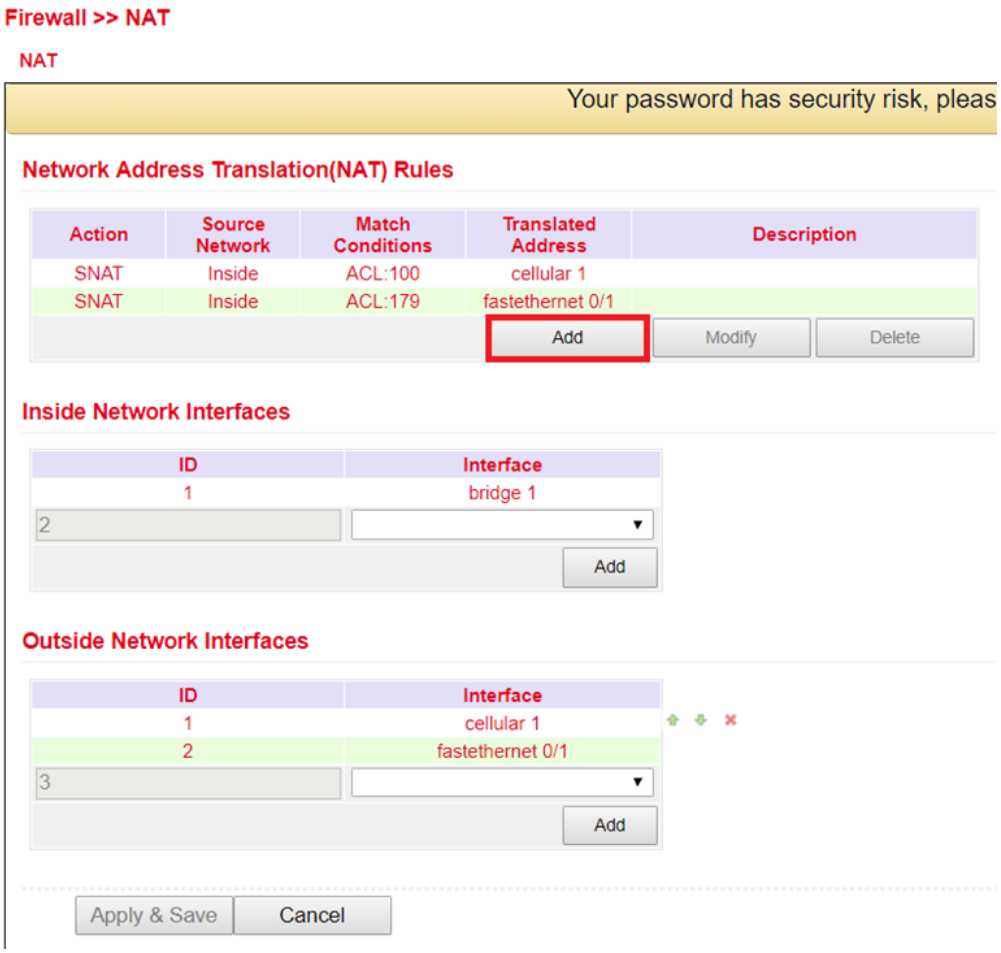
For a working port mapping it is helpful to check the settings of the connected devices in advance. The following checklist is helpful (according to the example above):

- Does the camera have the IP address 192.168.2.2?
- Does it respond to “ping 192.168.2.2”?
- Is the web interface of the camera accessible via http://192.168.2.2?
- Is the Welotec router entered as the default gateway for the camera (192.168.2.1)?

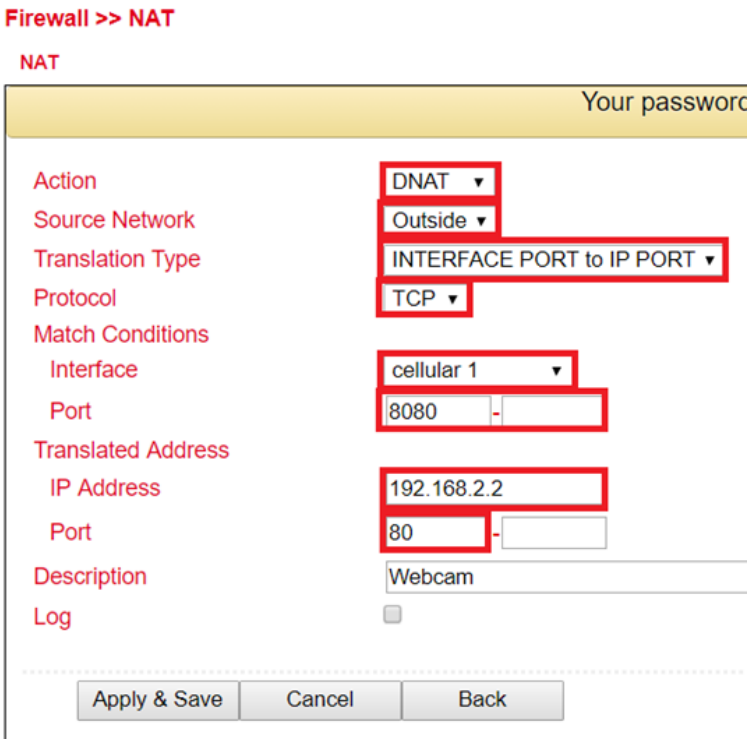
If these conditions are met, the port mapping can be set up according to the following instructions.

Configuration

1. Go to the menu item ***Firewall*** and select the sub-item ***NAT***.
2. Now add a new NAT rule with ***Add***



3. Enter the data as shown in the example

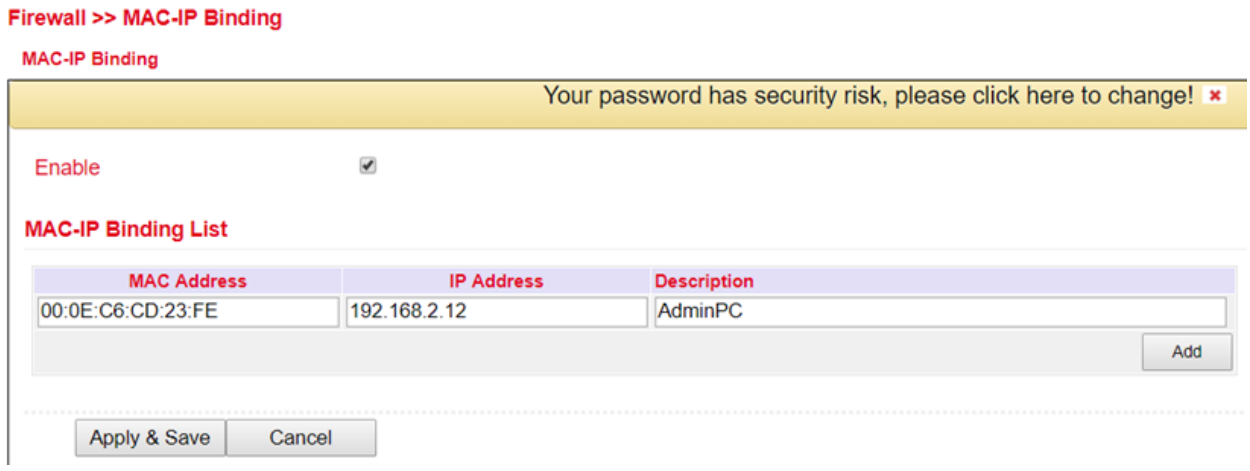


4. By calling the router IP with the corresponding port, the connected device can be reached

3.6.3 3.6.3. MAC-IP Binding

MAC-IP Binding can be found in the navigation tree under ***Firewall > MAC-IP Binding*** .

MAC-IP Binding can be used to ensure that a device (PC, server, etc.) can only access the router if the MAC and IP addresses entered here match.



Parame-ter	Description
MAC-Address	Enter the MAC address of the device here in the format XX : XX : XX : XX: XX : XX. A typical MAC address looks like this: 00:FF:4E:85:F1:B5
IP-Address	Enter the IP address which the device should get, e.g. 192.168.2.150
Descrip-tion	Text description field

3.7 3.7. VPN

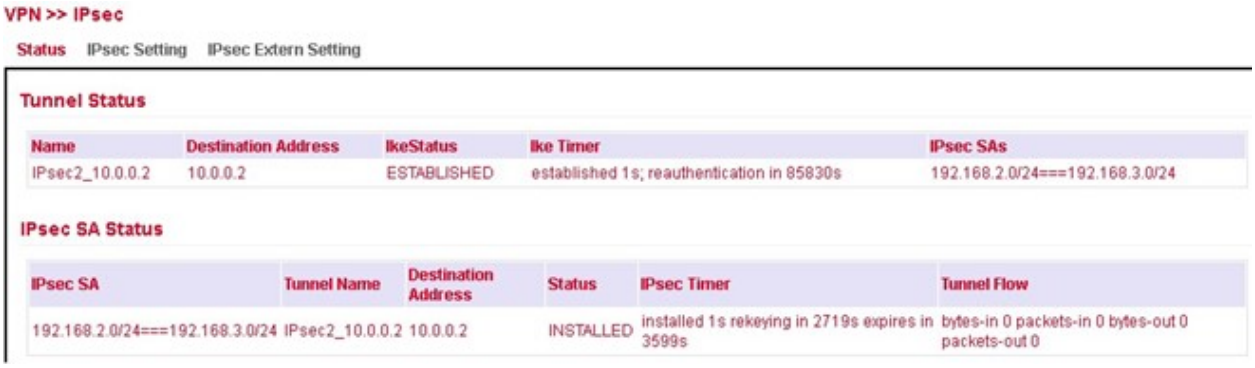
Virtual Private Network, or VPN for short. The VPN is used to link participants in the existing communications network to another network. For example, an employee's computer can gain access to the company network from home, just as if he were sitting right in the middle of it.

3.7.1 3.7.1. IPsec

IPsec (short for Internet Protocol Security) is a protocol suite designed to enable secure communications over potentially insecure IP networks such as the Internet. The goal is to provide encryption-based security at the network level. IPsec provides this capability through connectionless integrity and access control and authentication of data. In addition, IPsec ensures confidentiality as well as authenticity of the packet sequence through encryption.

3.7.1.1. Status

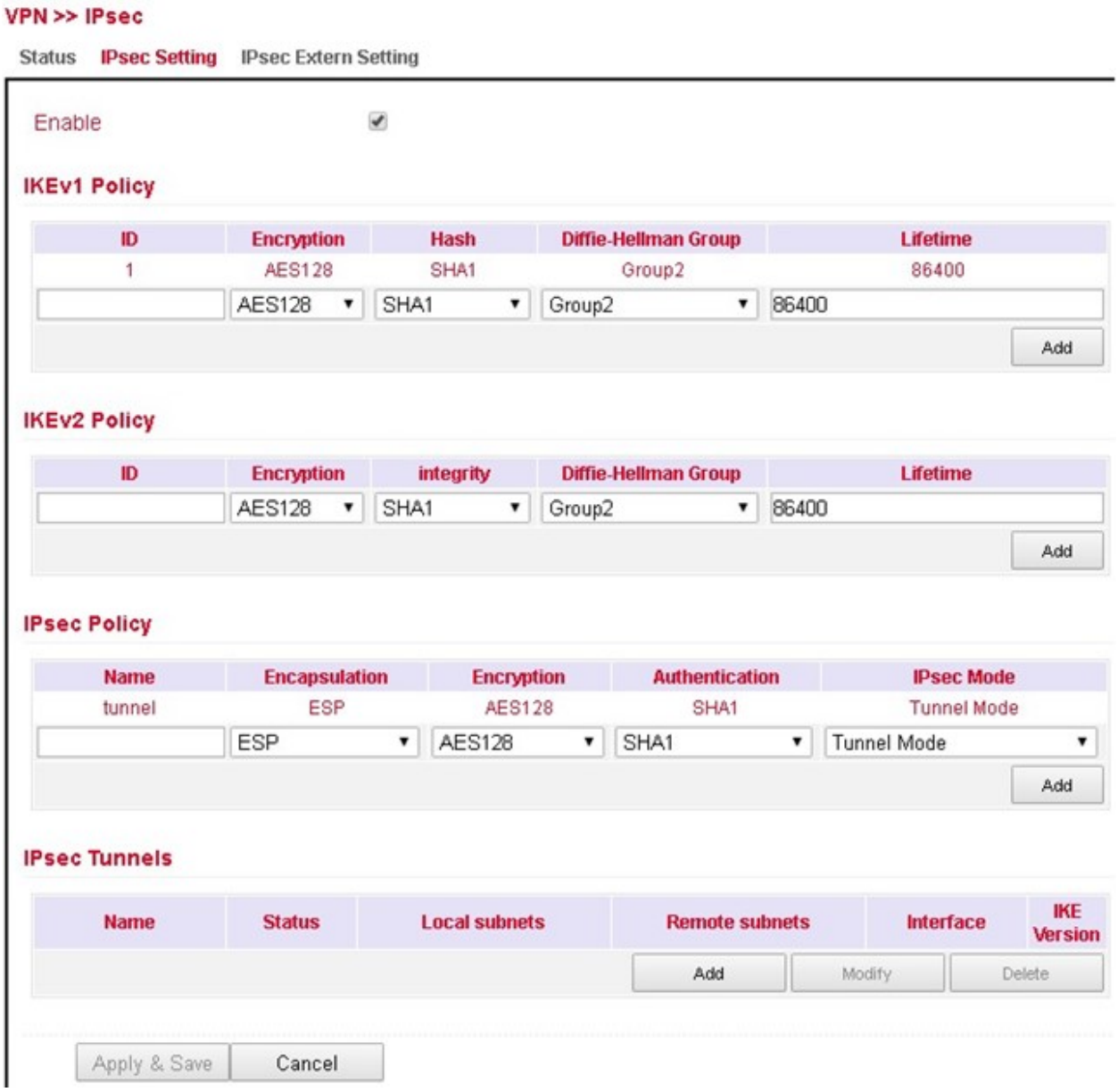
If the IPsec tunnel(s) have been successfully established, you will see the following in the status overview.



3.7.1.2. IPsec Setting

Under ***VPN*** > ***IPsec*** > ***IPsec Setting***, existing settings can be adjusted or a new IPsec tunnel can be created. When creating a new IPsec tunnel, an ***IKE policy*** and an ***IPsec policy*** must first be created.

Afterwards, this setting must first be confirmed with ***Apply & Save***. Then the actual IPsec tunnel can be created via ***Add***.



IKEv1 Policy:

Parameter	Description
ID	Integer, can be freely selected. Used to identify the policy in the tunnel configuration
Encryption	Encryption method
Hash	Hash algorithm
Diffie-Hellman Group	DH Group for key exchange
Lifetime	Period of validity of the IKE before it is renegotiated

IKEv2 Policy:

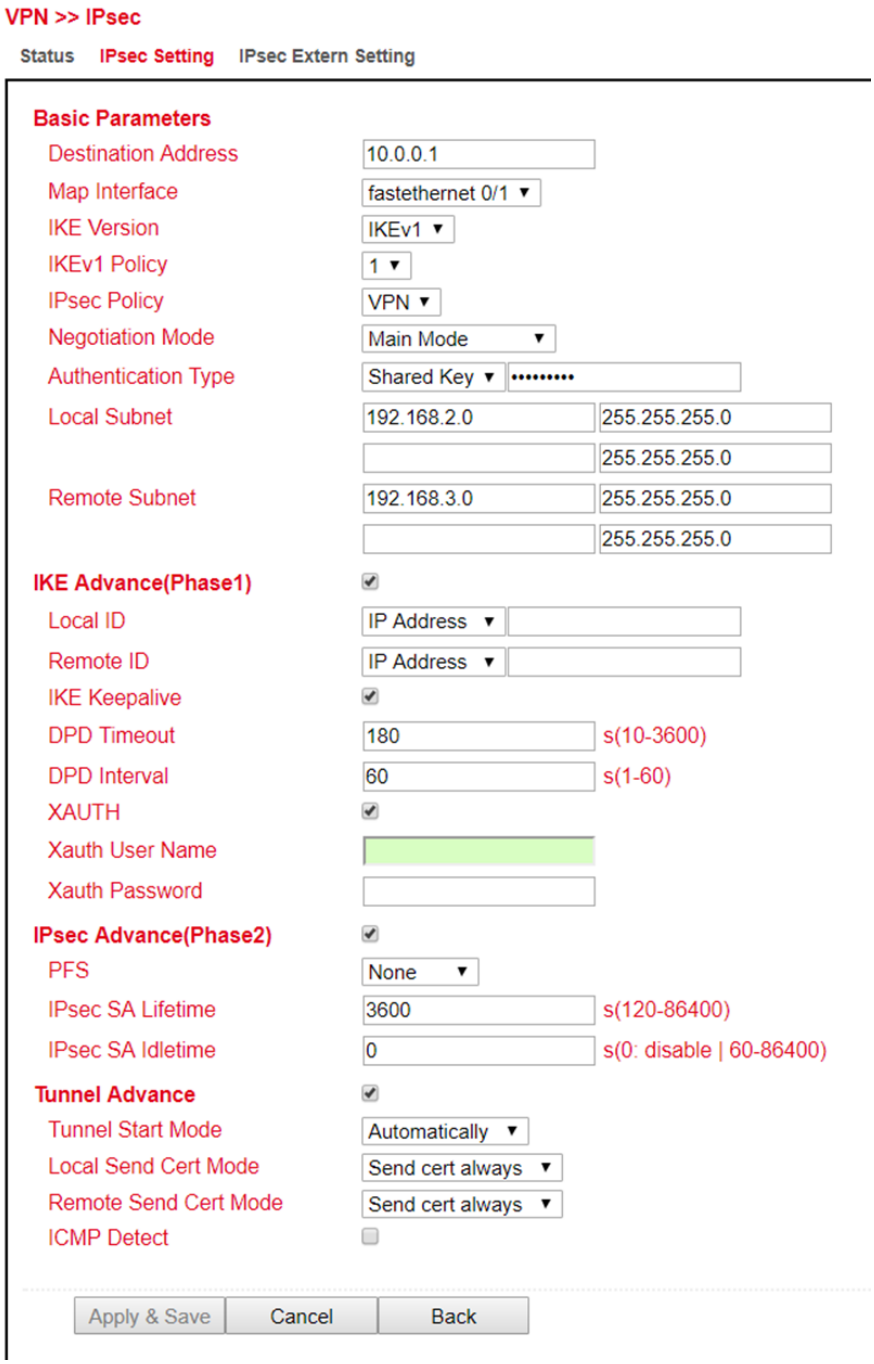
Parameter	Description
ID	Integer, can be freely selected. Used to identify the policy in the tunnel configuration
Encryption	Encryption method
integrity	Hash algorithm
Diffie-Hellman Group	DH Group for key exchange
Lifetime	Period of validity of the IKE before it is renegotiated

IPsec Policy:

Parameter	Description
Name	Freely selectable name of the IPsec policy. Used to identify the policy in the tunnel configuration
Encapsulation	ESP or AH
Encryption	Encryption method
Authentication	Hash algortihm
IPsec Mode	Tunnel or Transport Mode

3.7.1.2.1. IPsec Tunnel

Via ***VPN*** > ***IPsec*** > ***IPsec Setting*** you can create a new IPsec tunnel (IKEv1 and IKEv2) under ***IPsec Tunnels*** with ***Add***. The prerequisite is that an IKEv1 or IKEv2 policy and an IPsec policy have been created beforehand.



Basic Parameters:

Parameter	Description
Destination Address	IP address of the tunnel remote station
Map Interface	Interface of the router through which the connection is to be established
IKE Version	IKEv1 or IKEv2
IKEv1 Policy	The ID number of the previously created IKEv1 policy.
IPsec Policy	The name of the previously created IPsec policy
Negotiation Mode	Main Mode or Agressive Mode
Authentication Type	Shared Key or Certificate
Local Subnet	The router subnet
Remote Subnet	The remote station subnet

IKE Advance(Phase1):

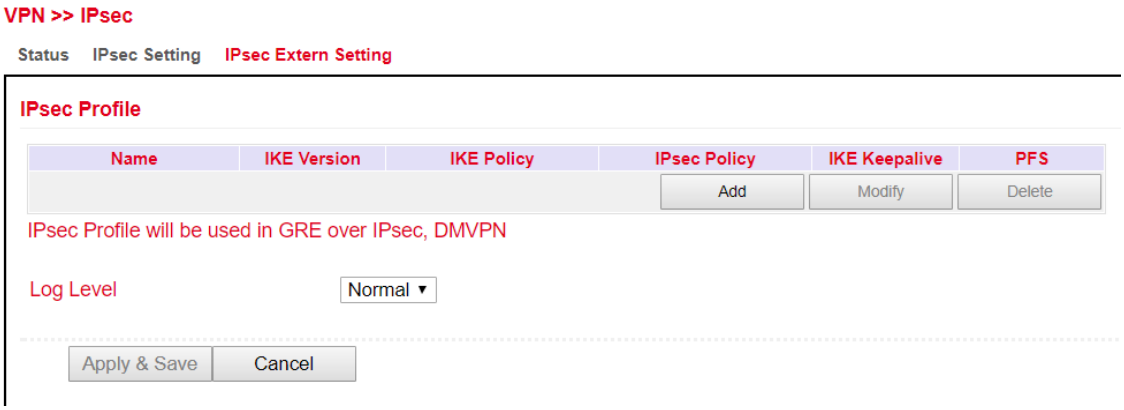
Parameter	Description
Local ID	IP Address, FQDN or User FQDN
Remote ID	IP Address, FQDN or User FQDN
IKE Keepalive	Switches IKE Keepalive on or off
DPD Timeout	Timeout for a DPD packet
DPD Interval	Interval of DPD packets
XAUTH	Switches XAUTH on or off
Xauth User Name	XAUTH User Name
Xauth Password	XAUTH Password

IPsec Advance(Phase2):

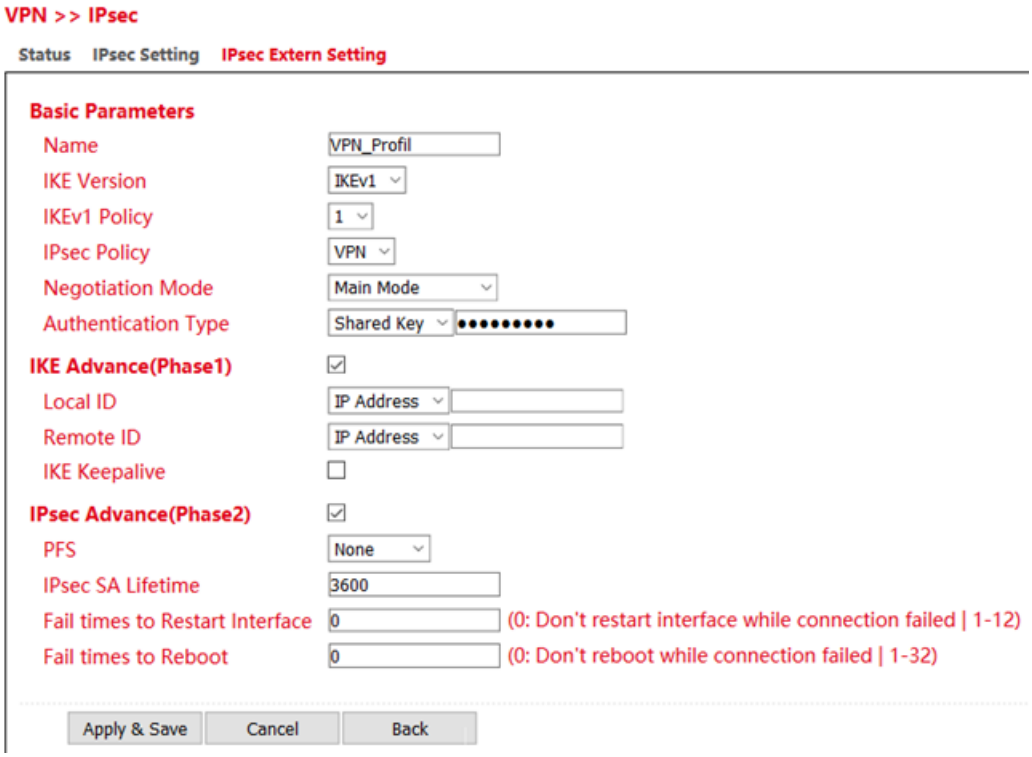
Parameter	Description
PFS	Perfect Forward Secrecy Group
IPsec SA Lifetime	Validity period of SA before it is recreated
IPsec SA Idletime	SAs associated with inactive peers can be deleted before the global lifetime expires.
Tunnel Advance:	

Parameter	Description
Tunnel Start Mode	Selection of the start mode for the tunnel. Automatic is the default.
Local Send Cert Mode	Specifies when the certificate should be sent
Remote Send Cert Mode	Specifies when the certificate should be sent
ICMP Detect	Switches the ICMP watchdog on or off
ICMP Detection Server	To test the IPsec tunnel connection, a server must be specified here that can only be reached through the tunnel
ICMP Detection Local IP	The router interface IP of the local subnet is specified here
ICMP Detection Inter-val	Interval at which the ICMP packet is sent
ICMP Detection Timeout	Time after which the ICMP packet is discarded
ICMP Detection Max Retries	Maximum attempts after a failed ICMP ping

3.7.1.3. IPsec Extern Setting



IPsec profiles are used with GRE over IPsec. The profile is created via the ADD button.



Parameter	Description
Name	Unique name for the external settings of the IPsec
IKE Version	IKEv1 or IKEv2
IKEv1 Policy	The ID number of the previously created IKEv1 policy
IPsec Policy	The name of the previously created IPsec policy
Negotiation Mode	Main Mode or Agressive Mode
Authentication Type	Shared Key or Certificate

IKE Advance (Phase1)

Parameter	Description
Local ID	IP Address, FQDN or User FQDN
Remote ID	IP Address, FQDN or User FQDN
IKE Keepalive	Switches IKE Keepalive on or off
DPD Timeout	Timeout for a DPD packet
DPD Interval	Interval of DPD packets
***\	
IPsec Advance (Phase2)***	

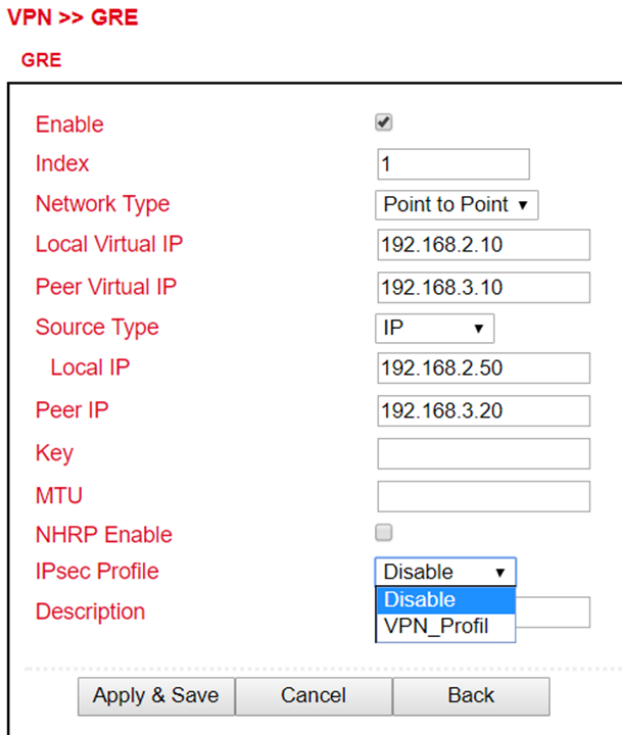
Parameter	Description
PFS	Perfect Forward Secrecy Group
IPsec SA Lifetime	Validity period of the SA before it is recreated
Fail times to Restart Interface	Number of failed connection attempts after which the IPsec tunnel should be restarted
Fail times to Reboot	Number of failed connection attempts after which the router should be restarted

3.7.2 3.7.2. GRE

The GRE (Generic Routing Encapsulation) protocol is used to encapsulate other protocols and transport them over tunnels.

GRE is used when dynamic routing is to be implemented via the IPSec tunnel.

Overview page. A new GRE entry is added with Add.

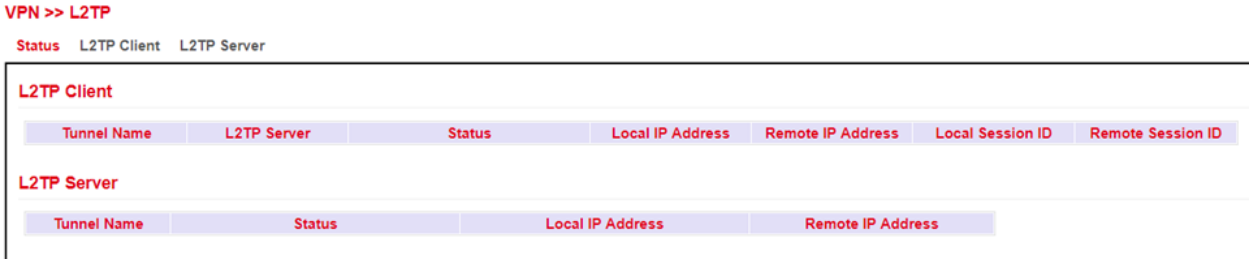


Under IPsec Profile the profile created under ***VPN > IPsec > IPsec External Setting*** is now in the selection list.

3.7.3 3.7.3. L2TP

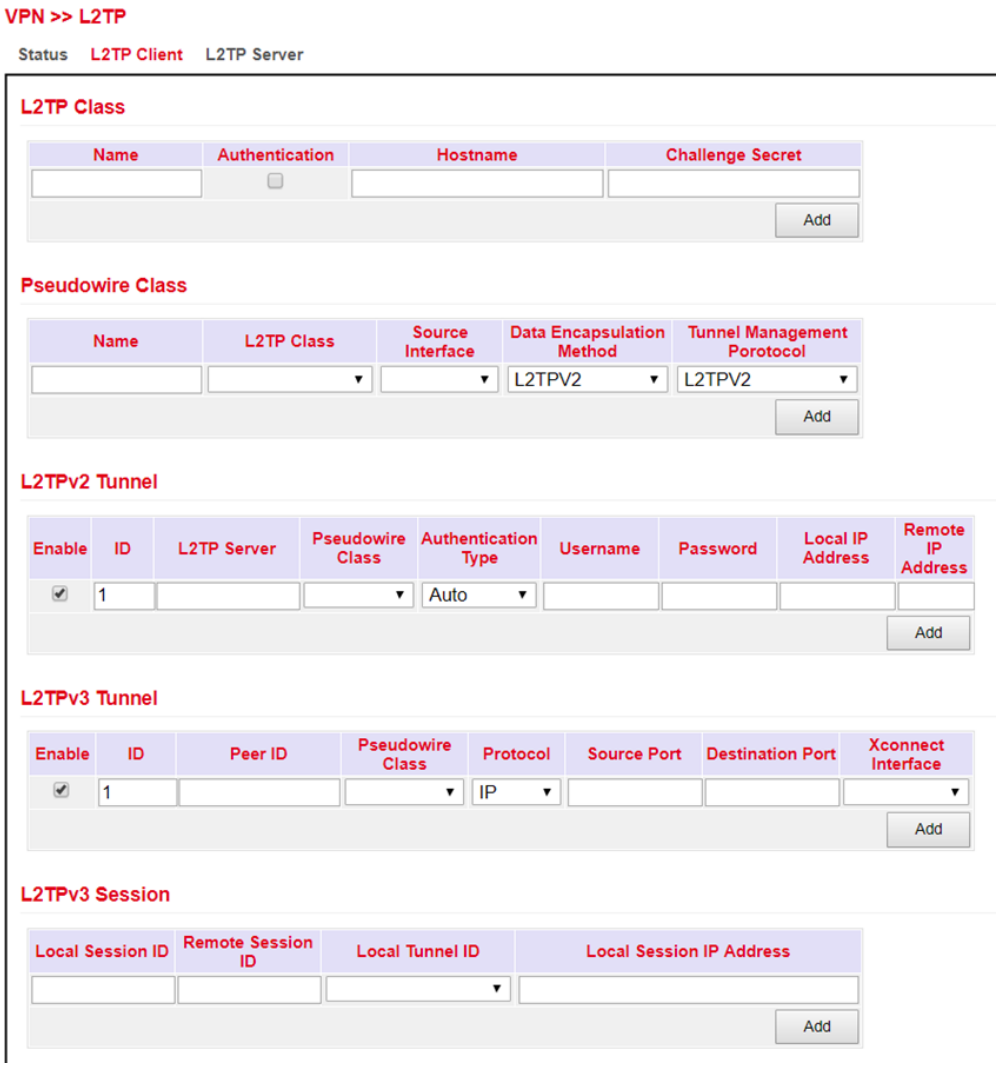
L2TP (Layer 2 Tunneling Protocol) combines PPTP (Point to Point Tunneling Protocol) and L2F (Layer 2 Forwarding). L2TP only supports user authentication, but no encryption. Therefore, L2TP is used in conjunction with an IPSec tunnel to guarantee encryption. L2TP is often used to connect single computers (keyword: road warrior) to the network.

3.7.3.1. L2TP Status



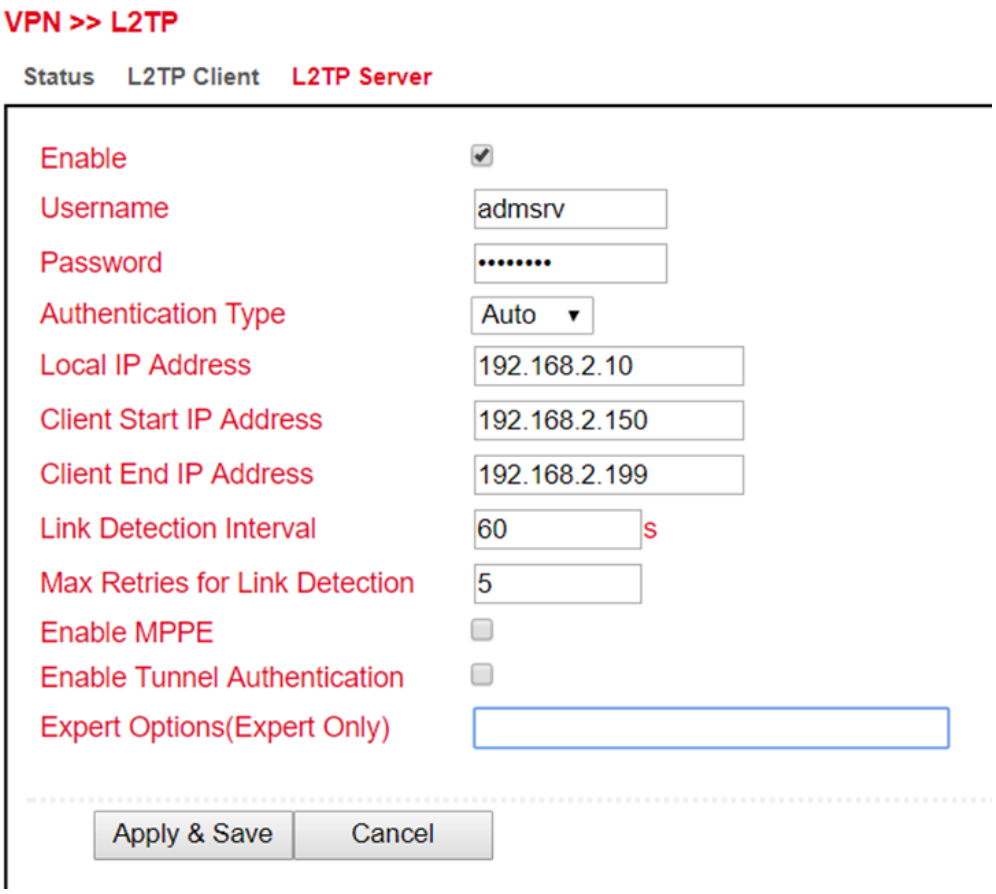
3.7.3.2. L2TP Client

Under *VPN > L2TP > L2TP Client* the corresponding client for the tunnel is created. The respective entries must be added with the Add button and are only completely saved when the Apply & Save button is clicked.



3.7.3.3. L2TP Server

Here you can create a corresponding L2TP server.



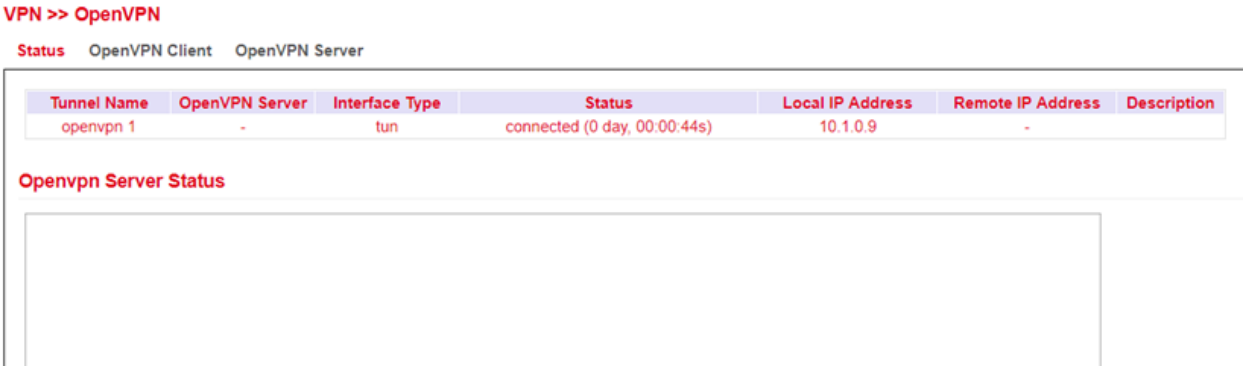
3.7.4 3.7.4. OpenVPN

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

3.7.4.1. OpenVPN Status

Status overview of the OpenVPN that has been configured.

Client Status:

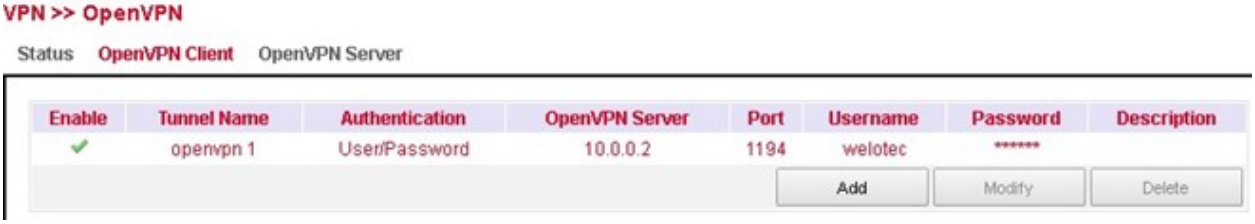


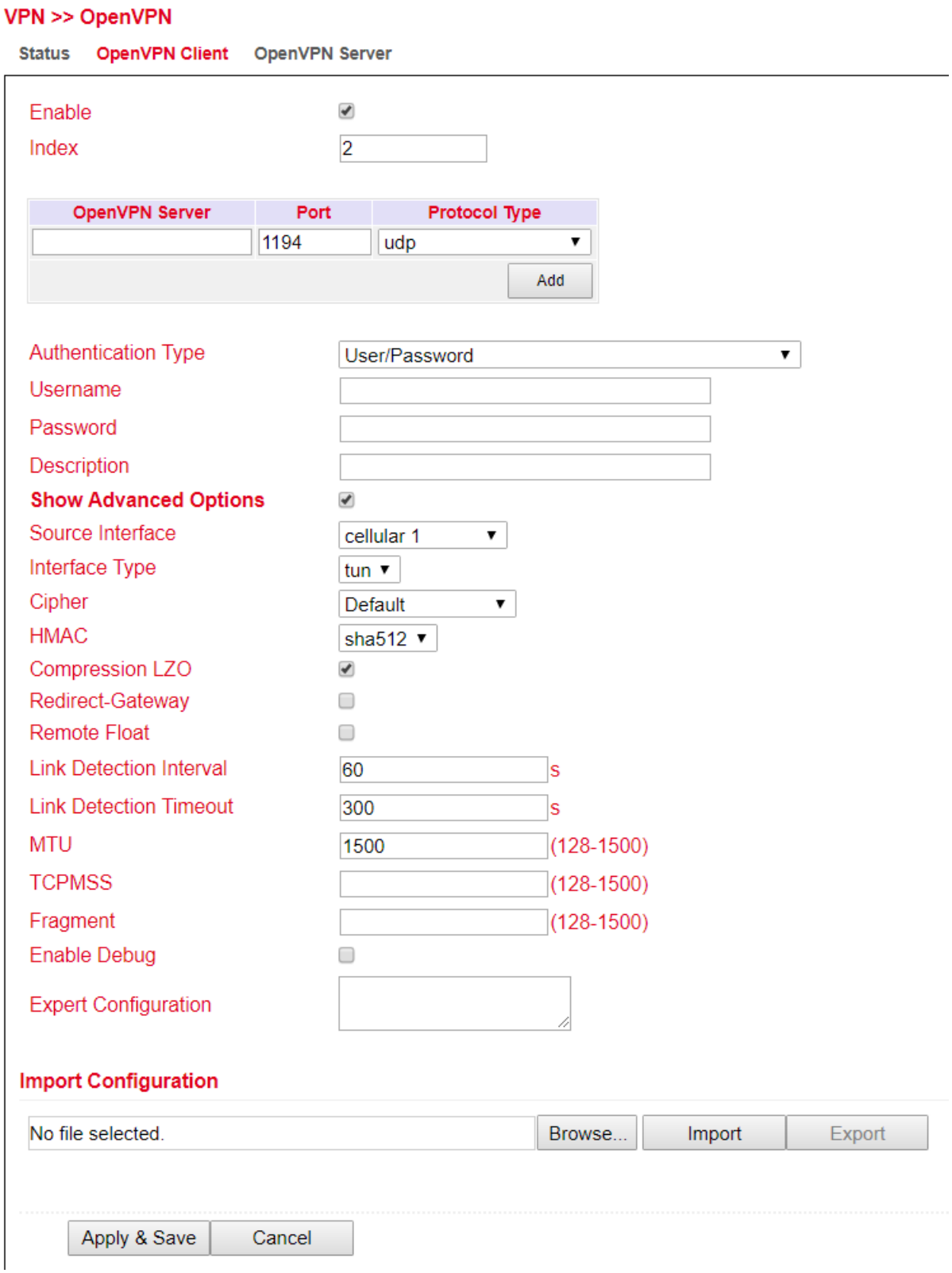
Server Status:

3.7.4.2. OpenVPN Client

A new OpenVPN tunnel can be added under ***VPN > OpenVPN > OpenVPN Client***. The router has to be configured as a client.

A new configuration can be created via the ***"Add "*** button.





Hinweis

Depending on the selected authentication, different inputs are possible. This example deals with username / password.

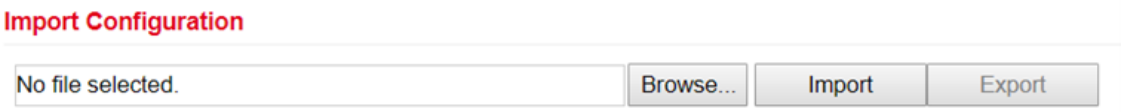
Parameter	Description
Enable	Switches the OpenVPN client on or off
Index	Freely selectable, for identification purposes only
OpenVPN Server	The IP address or the FQDN of the OpenVPN server
Authentication Type	Authentication method (recommended x509-cert)
Username	Username
Password	Password
Description	Brief description of the client

Show Advanced Options:

Parameter	Description
Source Interface	The interface over which the OpenVPN tunnel is to be established
Interface Type	tun or tap (recommended tun)
Cipher	Encryption method
HMAC	Signs all packets involved in the TLS handshake. Sha1 is default
Compression LZO	Enable or disable compression of data
Redirect-Gateway	If redirect gateway is enabled, the traffic is routed through the tunnel
Remote Float	If Remote Float is enabled, the client will also accept packets that match the authentication but do not originate from the server address. This option is useful if the server has a dynamic IP address
Link Detection Interval	Interval at which the tunnel connection is checked
Link Detection Timeout	Timeout for a tunnel connection check packet
MTU	Maximum packet size
TCPMSS	Specifies the maximum size for TCP packets
Fragment	Maximum packet size for UDP packets
Enable Debug	Switches debug mode on or off
Expert Configuration	OpenVPN tunnel options that are not available via the web interface can be entered here directly

Hinweis

The client always needs the CA certificate of the server, otherwise it cannot be authenticated.



This can be used to import an already existing OpenVPN configuration or to export the current configuration. The OpenVPN configuration can be exported from the OpenVPN server. This then has the file extension .ovpn.

Hinweis

Please make sure that the OVPN file does not contain any spaces. Spaces are interpreted differently by the router.

3.7.4.3. OpenVPN Server

Via ***VPN > OpenVPN > OpenVPN Server*** you configure the router as OpenVPN. The prerequisite for this is that the router has a ***public IP address***.

VPN >> OpenVPN

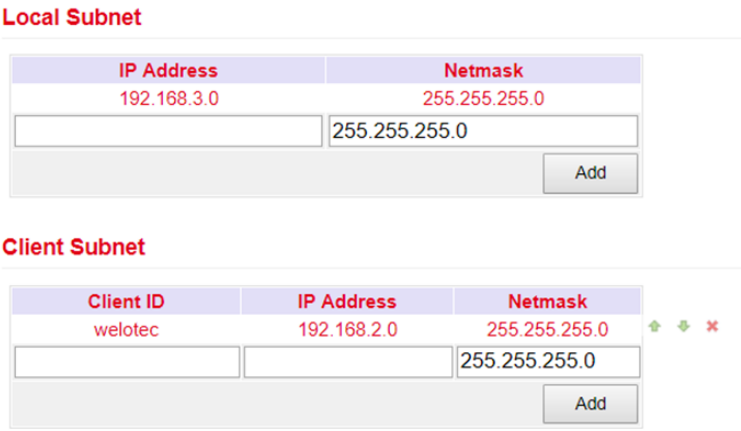
Status | OpenVPN Client | OpenVPN Server

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

User Password

Username	Password
welotec	******

Add



Depending on the selected authentication, different entries are possible. This example deals with username / password.

Parameter	Description
Enable	Switches the OpenVPN server on or off
Config Mode	Here you can choose between the manual configuration and the import of a finished configuration
Authentication Type	Authentication method
Virtual Network	The virtual network for the OpenVPN Tunnel
Virtual Netmask	The netmask for the virtual network of the OpenVPN tunnel
Description	Brief description of the server

Advanced Options:

Parameter	Description
Source Interface	The interface over which the OpenVPN tunnel is to be established
Interface Type	tun or tap (recommended tun)
Network Type	Connection type (recommended net30)
Protocol Type	UDP or TCP
Port	Port on which the OpenVPN server will run
Cipher	Encryption method
HMAC	Message Authentication Code(MAC) whose construction is based on a cryptographic hash function
Client-to-Client	Enable or disable client-to-client connection
Compression LZO	Enable or disable compression of data
Link Detection Interval	Interval at which the tunnel connection is checked
Link Detection Timeout	Timeout for a tunnel connection check packet
MTU	Maximum packet size
TCPMSS	Sets the maximum size for TCP packets
Fragment	Maximum packet size for UDP packets
Enable Debug	Switches the debug mode on or off
Expert Configuration	OpenVPN tunnel options that are not available via the web interface can be directly entered here.

User Password:

Clients can be added here, which can then log in with the user name and password.

Local Subnet:

Here the local subnets of the router are entered, which will be accessible for the clients.

Client Subnet:

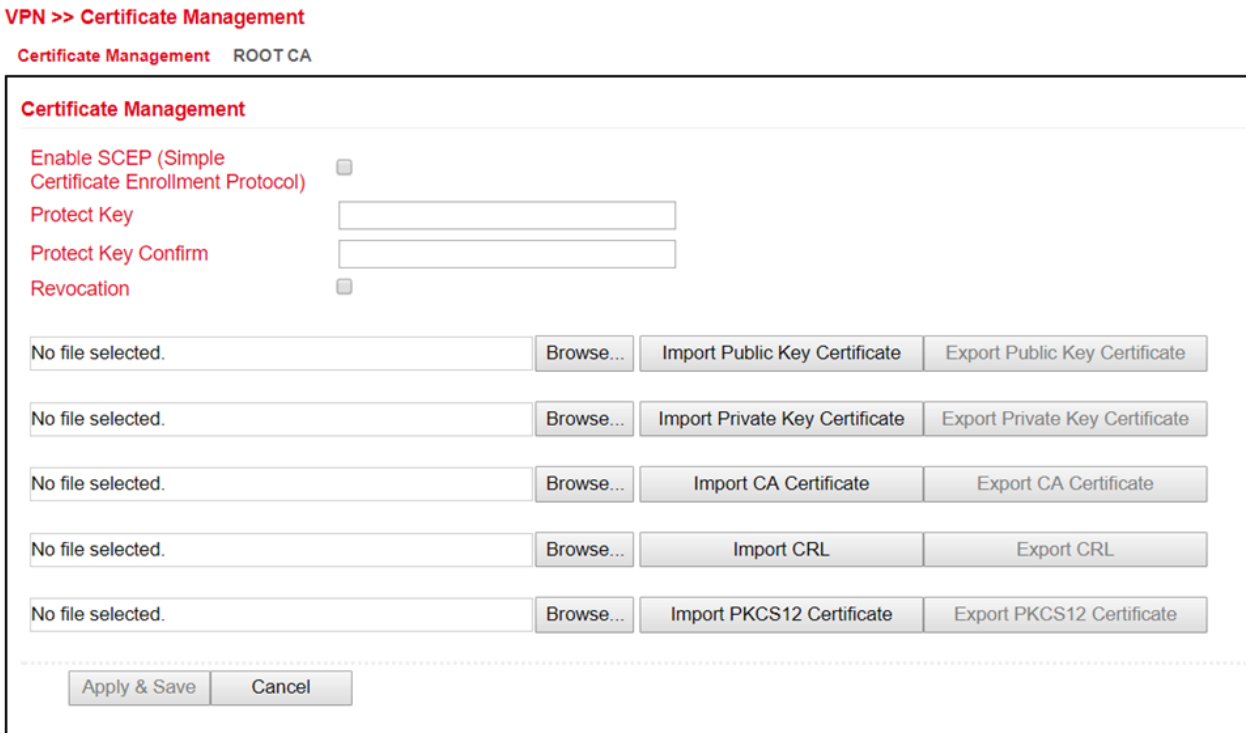
The client subnets that are to be accessible from the server side are entered here. The ***Client ID*** is the username of the client for the authentication method Username/Password and the Common Name for certificates.

Hinweis

The OpenVPN server always requires a CA certificate, as well as a public key and a private key. These are uploaded via ***VPN > Certificate Management***. If these certificates are not available, the server will not start!

3.7.5 3.7.5. Certificate Management

The certificates for an IPSec tunnel or an OpenVPN tunnel are stored in Certificate Management, provided that they are not secured via a Pre Shared Key (PSK).



To upload a certificate, you have to click on "***Browse***", select the locally stored certificate and then click on "***Import…***".

The "***Export Function***" can be used to check whether the certificates have been uploaded properly.

If the files have a size of 0 bytes, try to upload the certificates with another browser or PC.

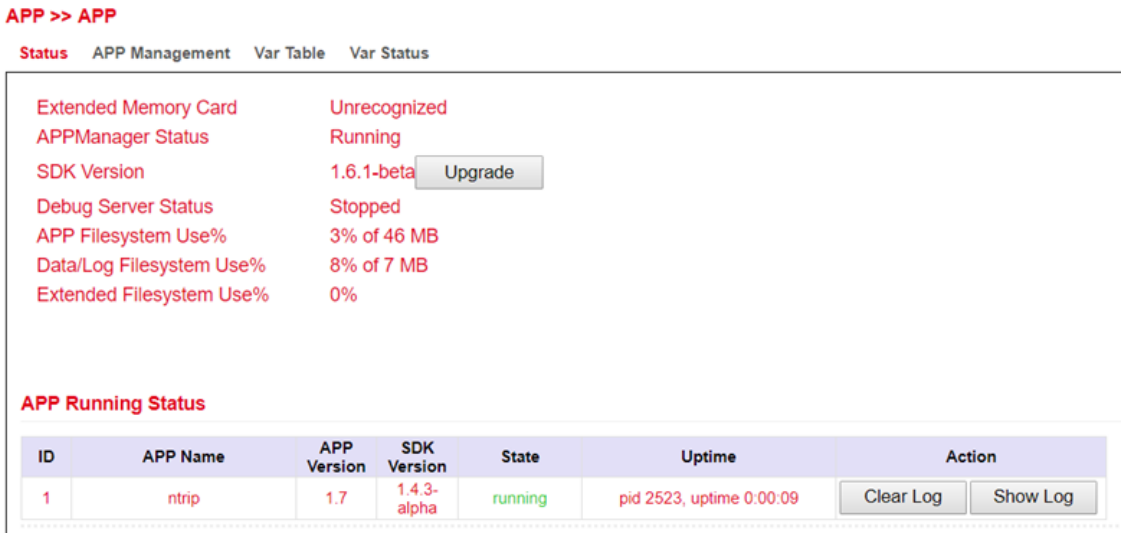
If a PKCS12 certificate set has been imported and is password protected, the password must still be entered under Protect Key and Protect Key Confirm after the import.

Then click on "***Apply & Save***" at the bottom to save the imported certificates in the configuration.

Parameter	Description
Enable SCEP	SCEP (Simple Certificate Enrollment Protocol) is used to roll out secured certificates to network devices and users. Check the box to enable this feature.
Protect Key	If the certificate is password protected, then the password for the certificate must be entered in this field, otherwise it cannot be uploaded correctly.
Protect Key Confirm	Enter the certificate password again to confirm the correctness of the entered password.
Revocation	Enabling this function enables the creation of a revocation list for invalid certificates
Import Public Key Certificate	Public Key Certificate is the certificate of the public key
Import Private Key Certivicate	Private Key Certificate is the certificate of the private key.
Import CA Certificate	Certificate Authority (CA) is the certificate of the certification authority.
Import CRL	Certificate Revocation List is the certificate revocation list.
Import PKCS12 Certificate	PKCS12 Certificate

3.8 3.8. APP

Python scripts can be uploaded under the menu item ***Administration > APP***. The Python scripts can be executed and edited via the Command Line Interface (CLI).



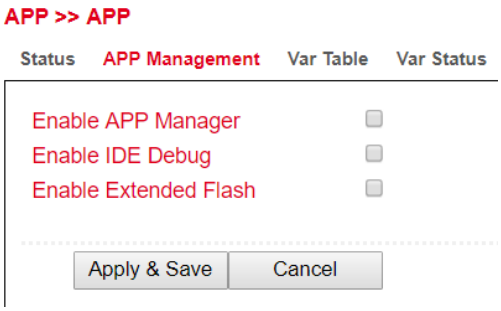
3.8.1 3.8.1. Status

Under the menu item ***APP > APP and Status*** you can see which Python SDK version is installed and which APP is running under Python. These APPs are then available to the Python scripts. You can also upgrade your Python SDK version via the upgrade button.

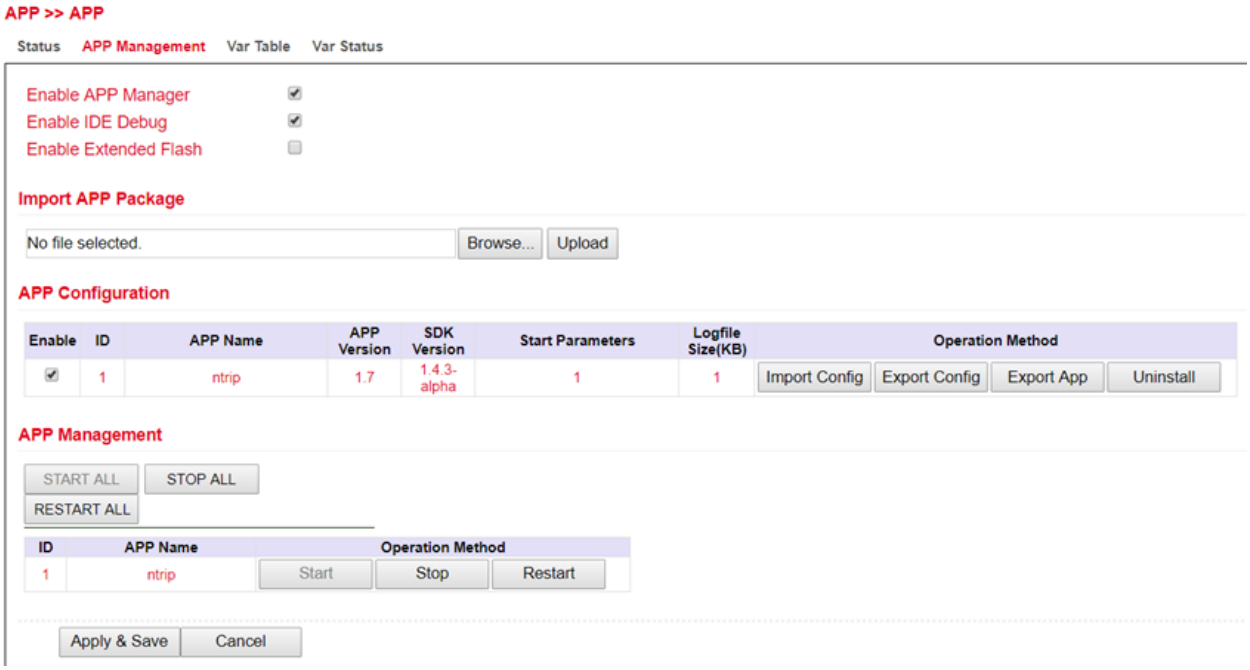
3.9

3.9.1 3.8.2. APP Management

To use the client IDE, it is necessary to enable the Enable IDE Debug function on the TK800. In addition, we recommend also enabling the APP Manager at this point. The App Manager gives you the possibility to install APPs under Python and to manage the existing apps in the Router-WebUI.



To do this, please enable the Enable APP Manager and Enable IDE Debug functions. Then click Apply & Save.



Upload application

Once you have created your application, you can import it to other TK800 routers.

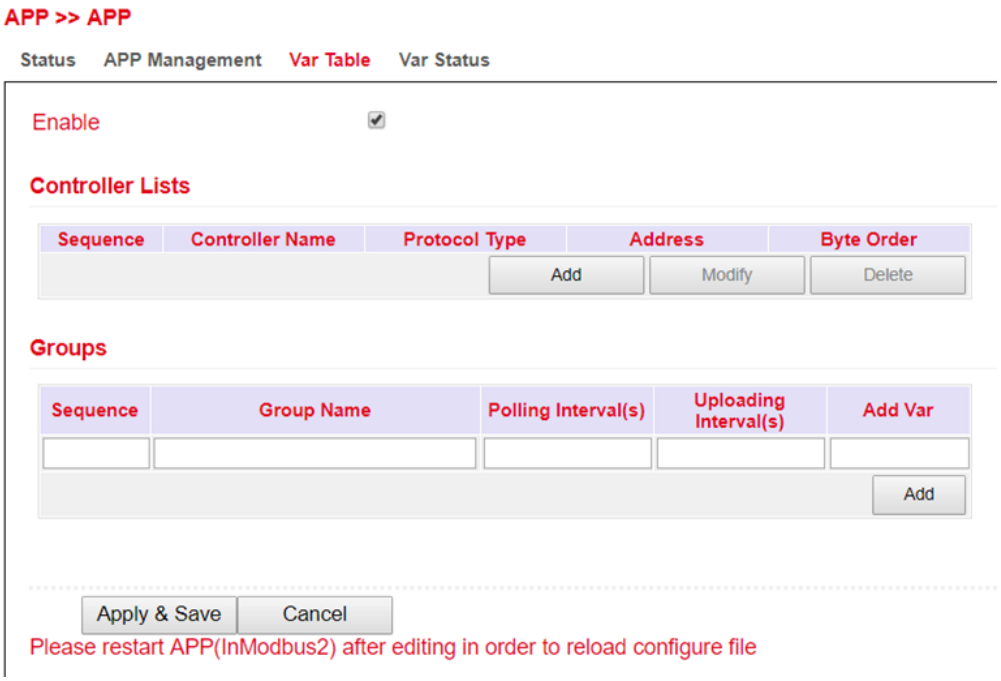
To do this, you can select “APP -> APP -> APP-Management” and click “Browse” at Import APP Package.

Select your .tar file and click Upload.

After you confirm the upload with “OK”, the application will be uploaded to the system.

After that you can upload your configuration if needed and enable the application by clicking “Enable”.

3.9.2 3.8.3. Var Table



In this area you have the possibility to access Modbus with APPs. At the moment we do not support this function.

3.9.3 3.8.4. Var Status

If you use your own APPs for the access to Modbus, you have the possibility to display the status here. At the moment we do not support this function.

3.10 3.9. Industrial

Hinweis

The Industrial functions are available on all models of the TK800 series with EX in the name. Example: TK8X2L-EX0.

The following functions are available:

- Digital input
- Relay output
- RS-232 interface
- RS-485 interface

3.10.1 3.9.1. DTU

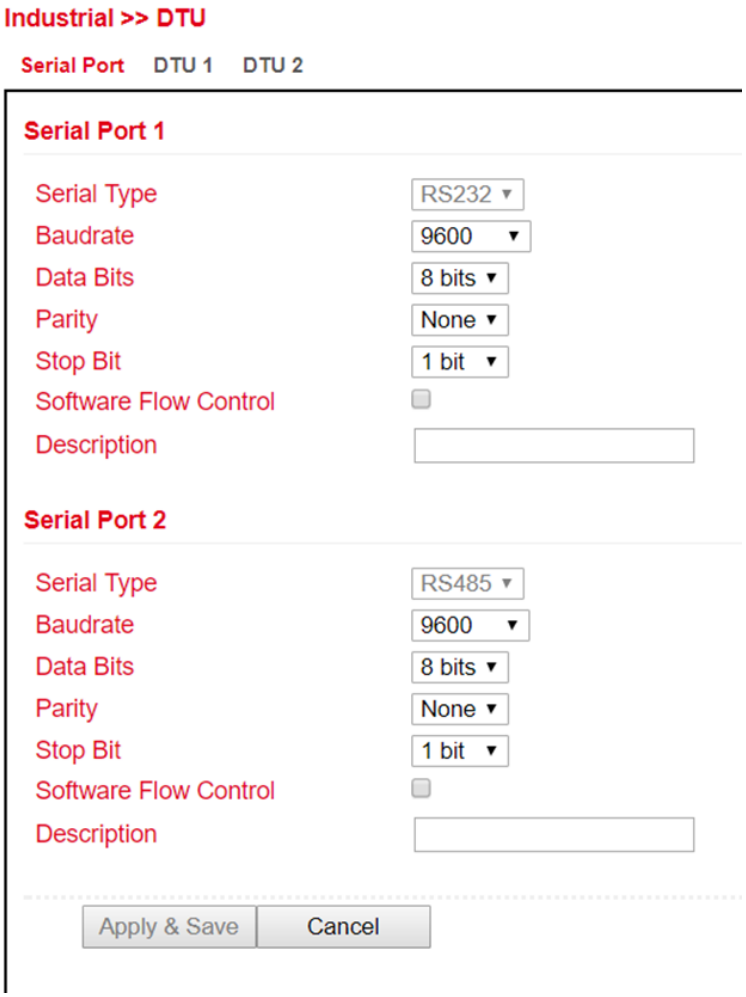
DTU stands for Data Terminal Unit and is used to connect devices with serial interface (RS-232 and RS-485). The configuration of the DTU properties always consists of two parts.

Under the item ***Serial Port*** the properties of the interface can be defined. Here you can find the parameters for the RS-232 and for the RS-485 interface.

Under the item ***DTU 1 (RS-232)*** and the item ***DTU 2 (RS-485)*** the protocols and the parameters for the protocols can be set.

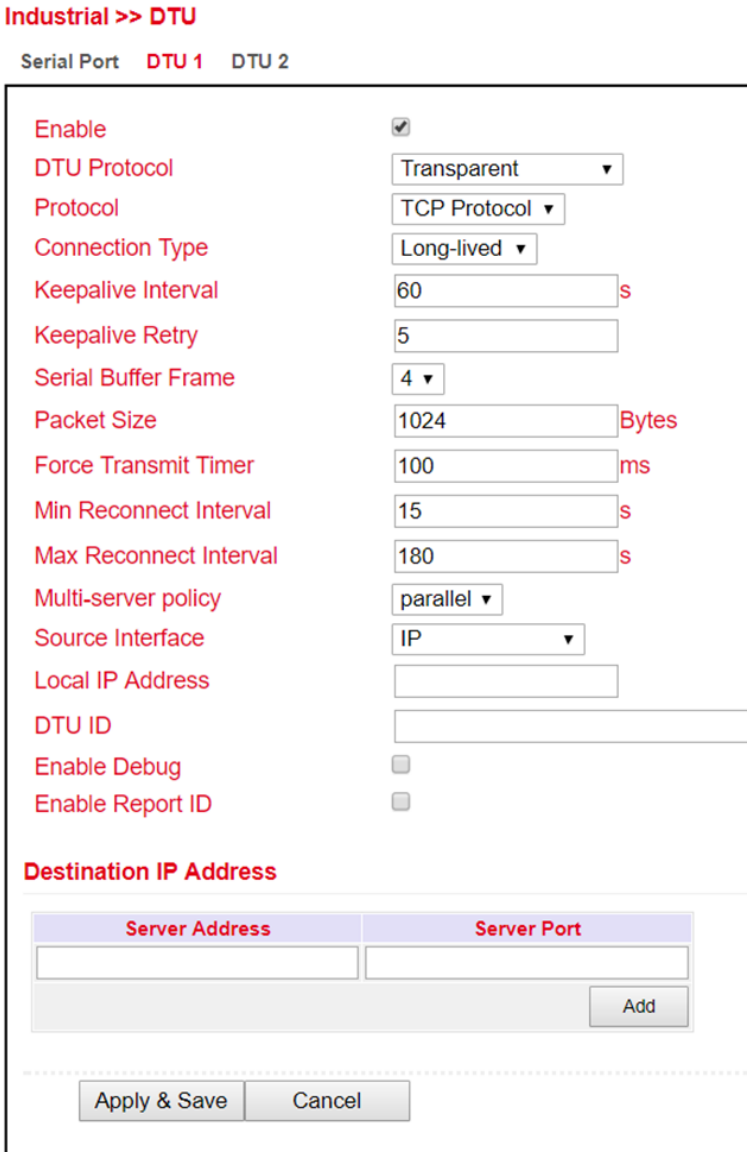
3.9.1.1. Serial Port

At this point the serial ports 1 (RS232) and 2 (RS485) can be configured.

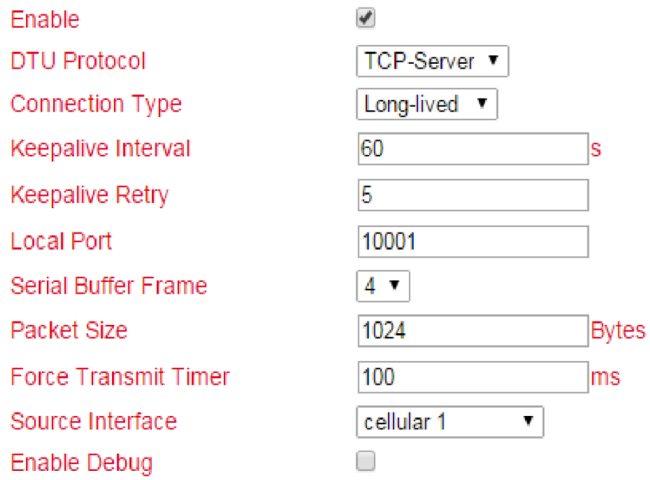


3.9.1.2. DTU 1 / DTU 2

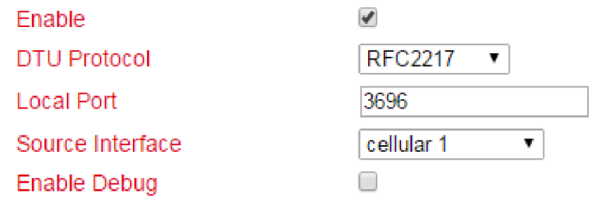
Transparent



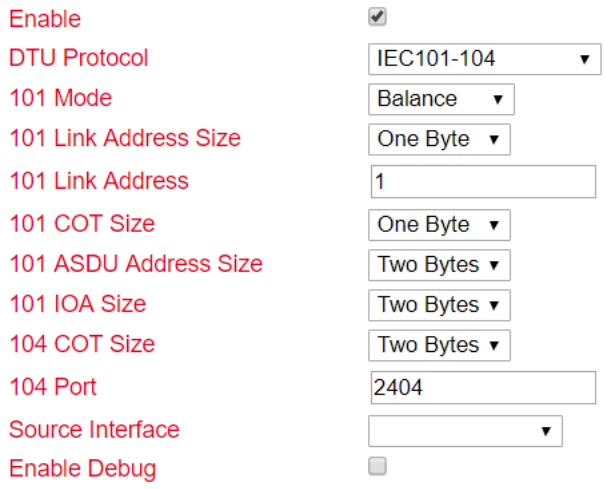
TCP server selection at DTU Protocol



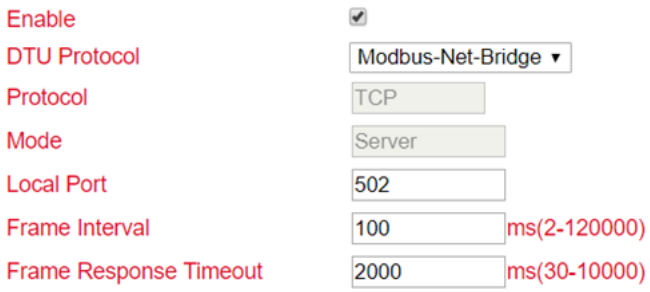
RFC2217 selection at DTU Protocol



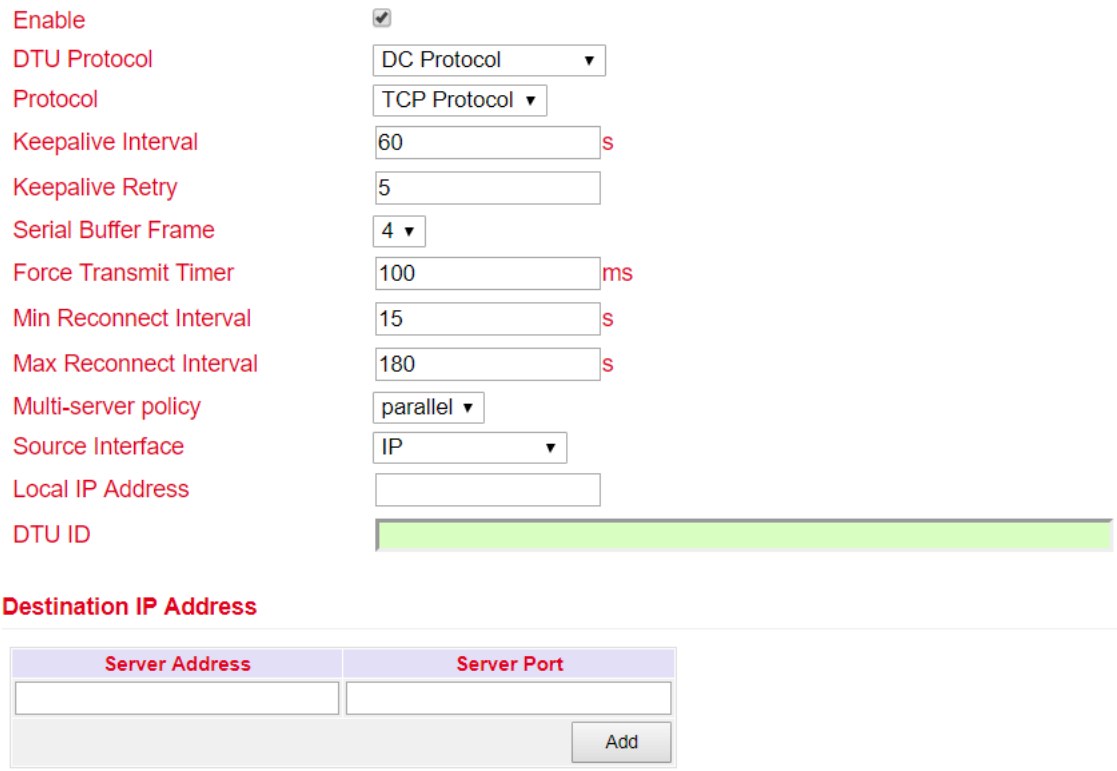
IEC60870-5-101/104 selection at DTU Protocol



Select Modbus-Net-Bridge at DTU Protocol

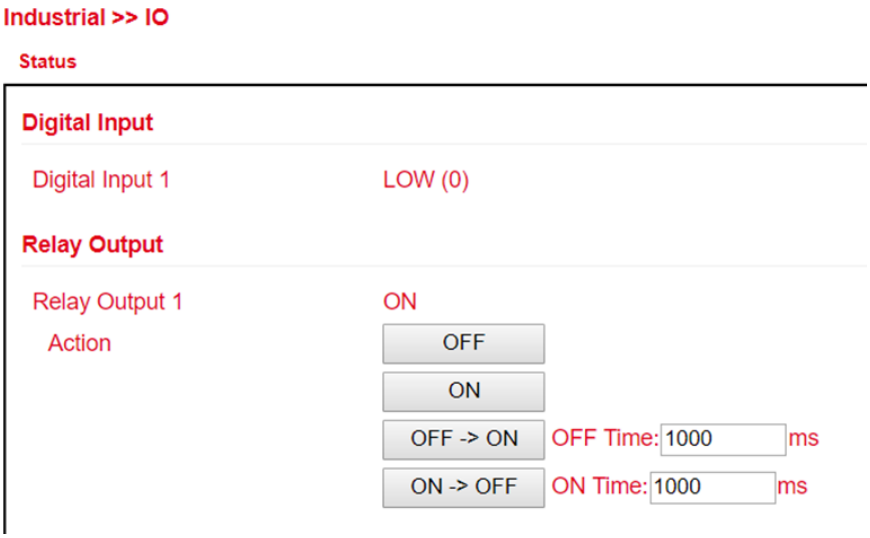


Selection DC Protocol at DTU Protocol



3.10.2 3.9.2. IO

Under ***Industrial > IO*** you can configure whether the digital input is to be used for switching the VPN connections. The relay is always ON by default.

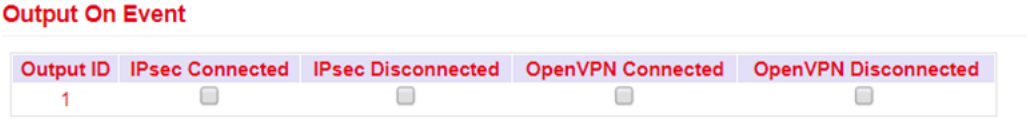


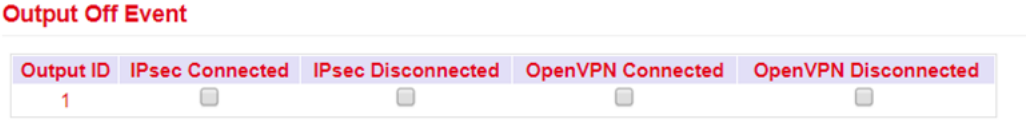
Digital Input:

Displays the status of the digital input.

Relay Output:

Parameter	Description
Relay Output 1	Relay output status
Action	Switch on, switch off or define a cycle





Input High/Low Action: Description

Default relay settings on or off. This can be used to switch the status of the relay output on or off or to define a corresponding cycle.

Here, an OpenVPN or IPsec tunnel can be started or stopped via the digital input.

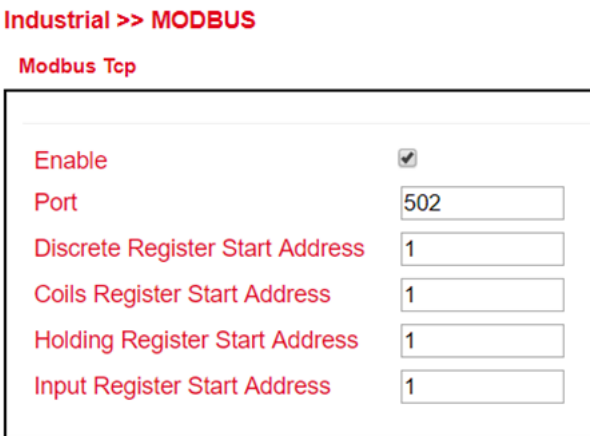
Output On/Off Event:

Here the relay output can be used to start or stop IPsec and OpenVPN.

3.10.3 3.9.3. Modbus

Communication protocol based on a master / slave or client / server architecture. Modbus/TCP is very similar to RTU, but TCP/IP packets are used to transmit the data. TCP port 502 is reserved for Modbus/TCP.

Via ***Industrial*** > ***Modbus*** > ***Modbus Tcp*** you can switch the corresponding settings on or off.

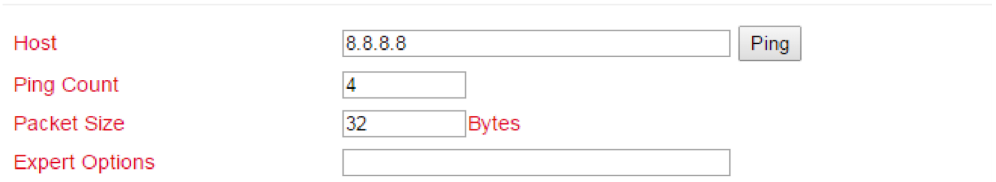


3.11 3.10. Tools

Useful tools that can be used for pinging, tracing, etc.

3.11.1 3.10.1. Ping

At this point in the router software, a ping can be sent to check connections, for example.

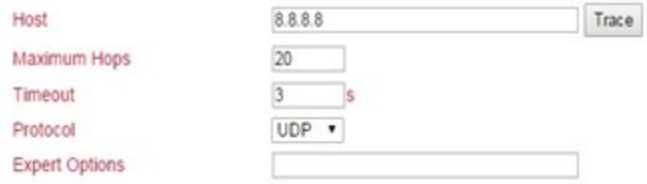


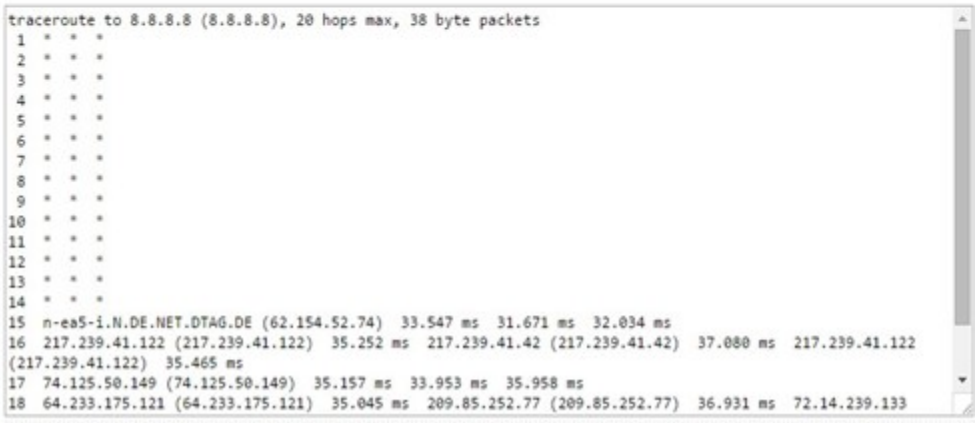

```
PING 8.8.8.8 (8.8.8.8): 32 data bytes
40 bytes from 8.8.8.8: seq=0 ttl=48 time=72.138 ms
40 bytes from 8.8.8.8: seq=1 ttl=48 time=36.295 ms
40 bytes from 8.8.8.8: seq=2 ttl=48 time=35.832 ms
40 bytes from 8.8.8.8: seq=3 ttl=48 time=36.538 ms

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

Parameter	Description
Host	Enter the address to be pinged
Ping Count	Number of pings executed. Entry from 1 to 50 possible. Default is 4
Packet Size	Size of the packet to be sent. Default is 32 bytes
Expert Options	Expert Options

3.11.2 3.10.2. Traceroute

Traceroute (tracert) determines via which routers and Internet nodes IP data packets reach the queried computer.



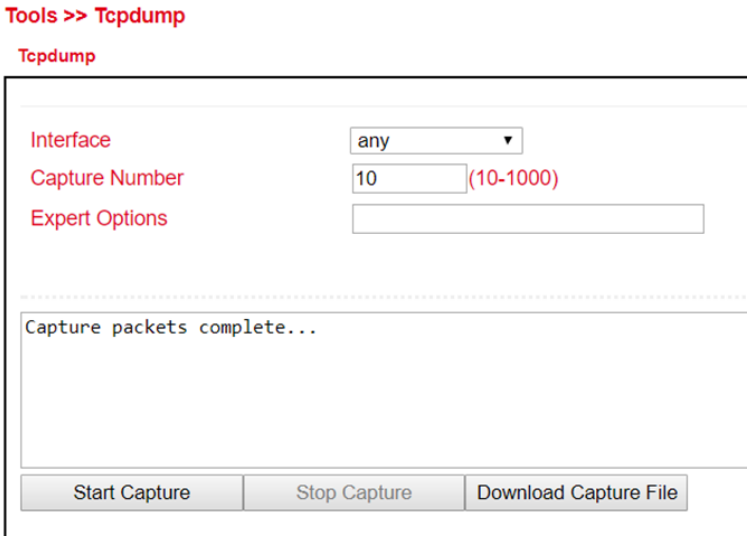


Parameter	Description
Host	Enter the destination host to be detected
Maximum Hops	Number of executed hops. Input from 2 to 40 possible. Default is 20
Timeout	Input of the timeout in seconds. Value can be between 2 and 10s.
Protocol	Optionally either ICMP or UDP. Default is UDP
Expert Options	Expert Options

3.11.3 3.10.3. Tcpdump

Well-known and widely used packet sniffer. Allows TCP packets to be sniffed.

Via ***Tools*** > ***Tcpdump*** you can access this sniffer.

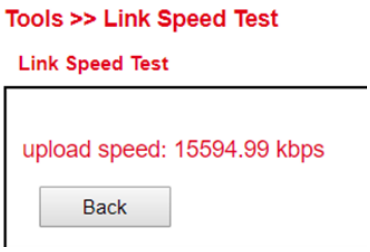


Parameter	Description
Interface	Selection of the interface to be captured
Capture Number	Number of captures. Default is 10
Expert Options	Expert Options
Start Capture (Button)	Starts capturing the data packets
Stop Capture (Button)	Stops capturing the data packets
Download Capture File (Button)	Downloads the capture as tcpdump.pcap file. Readable e.g. with Wireshark

3.11.4 3.10.4. Link Speed Test

Determine the connection speed by uploading and downloading files.

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



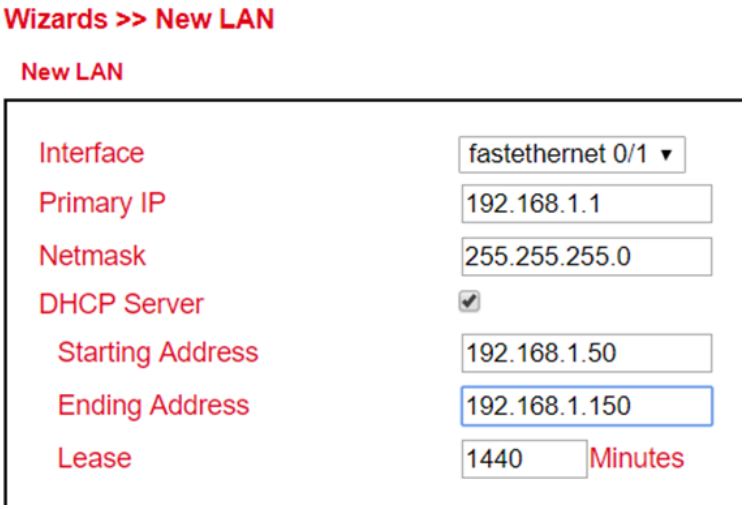
The ***download*** button downloads a 130MB file (test.bin) which shows the download speed during the download.

3.12 3.11. Wizards

These are wizards designed to facilitate the creation of the following processes.

3.12.1 3.11.1. New LAN

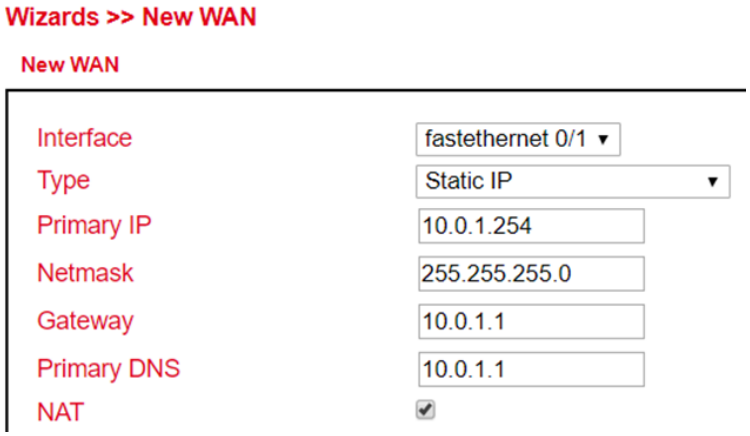
If you want to set up a new LAN interface, you can use the wizard under ***Wizards > New LAN***. This will then create all the necessary data in the background.



Parameter	Description
Interface	The available interfaces of the router
Primary IP	The IP address to be assigned to the selected interface
Netmask	The netmask that the selected interface will receive
DHCP Server	Switches the DHCP server for this interface on or off
Starting Address	If the DHCP server is switched on, the DHCP start address can be entered here
Ending Address	If the DHCP server is switched on, the DHCP end address can be entered here
Lease	If the DHCP server is switched on, the lease duration of an assigned address can be entered here.

3.12.2 3.11.2. New WAN

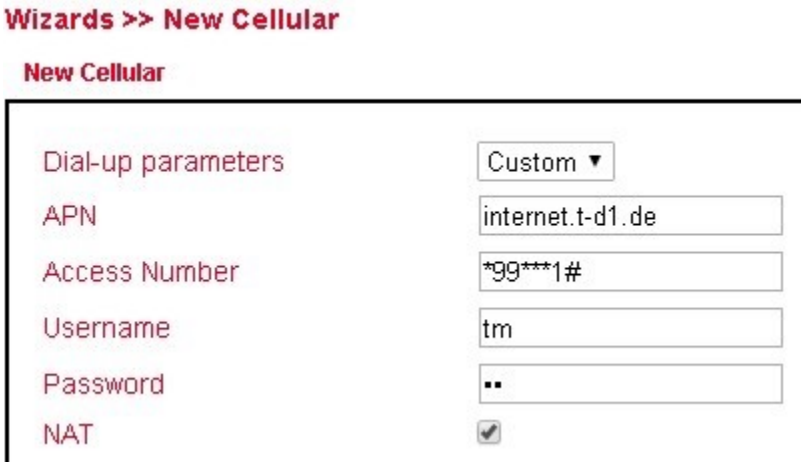
With the help of ***Wizards > New WAN*** a new WAN interface can be set up. We recommend that you also do this via the wizard, since several parameters are set here.



Parame-ter	Description
Interface	The new WAN interface
Type	Static IP / DHCP or PPPoE, depending on the selection the parameters change
Primary IP	The IP address of the interface
Netmask	The subnet mask of the interface
Gateway	The gateway of the router
Primary DNS	The primary DNS server of the router
NAT	Turns NAT on or off
Username	If PPPoE is selected under Type: User name of the provider for ADSL access. Important: A DSL modem is required for this.
Password	If PPPoE is selected under Type: Password of the provider for ADSL access. Important: A DSL modem is required for this.

3.12.3 3.11.3. New Cellular

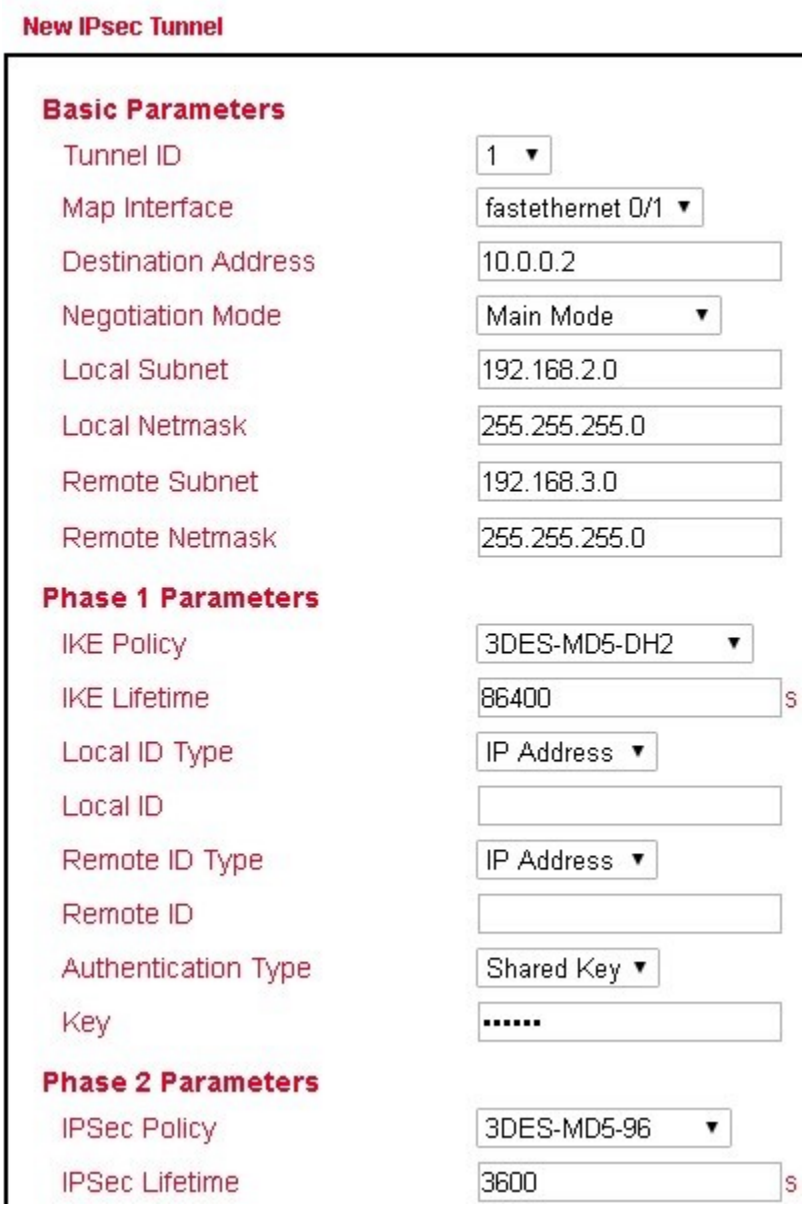
Under ***Wizards > New Cellular*** you create a new cellular interface as WAN interface and can configure it.



Parameter	Description
Dial-up parameters	Auto or Custom
APN	The APN of the Internet provider is entered here
Access Number	Almost always *99**1#
Username	Username for the above APN, if necessary
Password	Password for the user name to the above APN, if it is necessary
NAT	Enable or disable NAT

3.12.4 3.11.4. New IPsec Tunnel

Under ***Wizards*** > ***New IPsec Tunnel*** you can create a simple IPsec tunnel. It can be reconfigured later under ***VPN*** > ***IPsec***.



Basic Parameters:

Parameter	Description
Tunnel ID	Serves for identification of the tunnel
Map Interface	Interface over which the IPsec tunnel is to be established.
Destination Address	Remote station of the IPsec tunnel
Negotiation Mode	Main Mode or Aggressive Mode (recommended Main Mode)
Local Subnet	The subnet of the router, which is to be reached by the remote station
Local Netmask	Subnet mask of the router
Remote Subnet	The subnet of the remote station
Remote Netmask	The subnet mask of the remote station

Phase 1 Parameters:

Parameter	Description
IKE Policy	Encryption / Hash / Diffie-Hellman-Group
IKE Lifetime	Period of validity of the IKE Policy
Local ID Type	IP address / FQDN / User FQDN
Local ID	IP address or FQDN
Remote ID Type	IP address / FQDN / User FQDN
Remote ID	IP address or FQDN
Authentication Type	Authentication method pre-shared key or certificate
Key	Pre-shared key

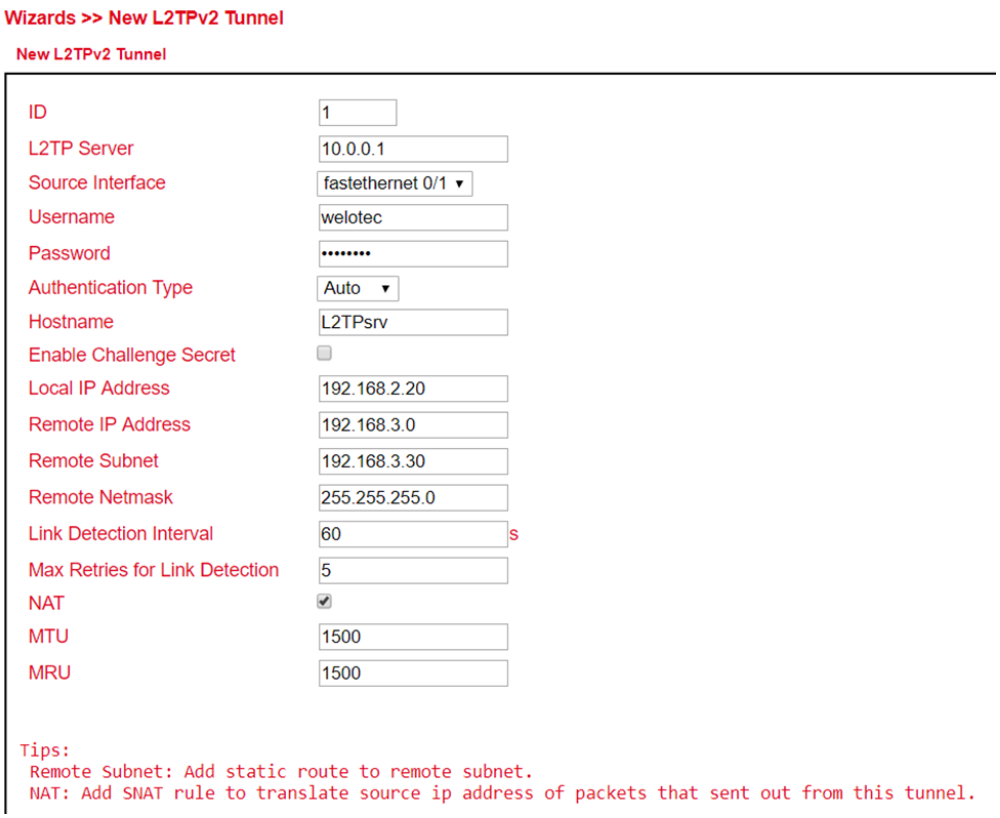
Phase 2 Parameters:

Parameter	Description
IPSec Policy	Encryption / Hash
IPSec Lifetime	Period of validity of the IPsec policy

3.12.5 3.11.5. IPsec Expert Config

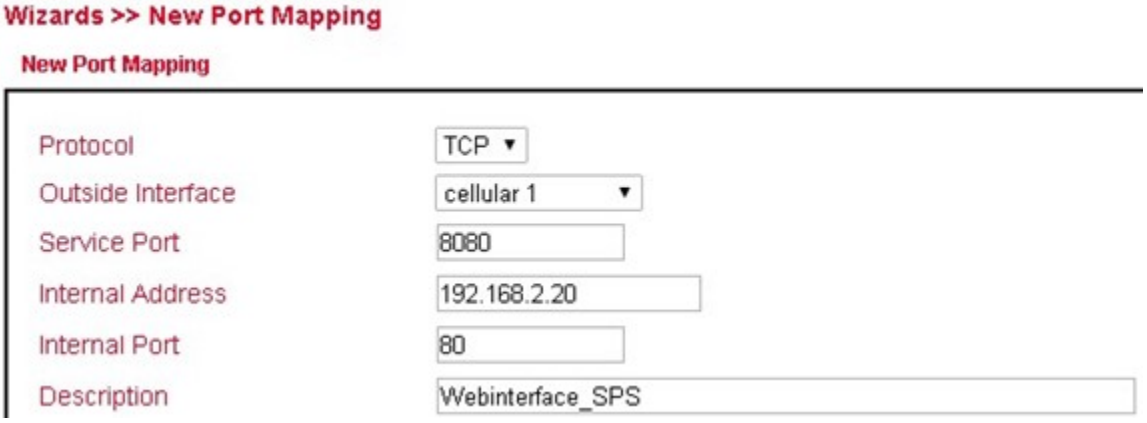
Under ***Wizards > IPsec Expert Config*** you can check the IPsec tunnel status by clicking Refresh. Furthermore, IPsec configurations can be imported via the interface.

3.12.6 3.11.6. New L2TPv2 Tunnel



3.12.7 3.11.7. New Port Mapping

Under *Wizards* > *New Port Mapping* a new port mapping can easily be set up.

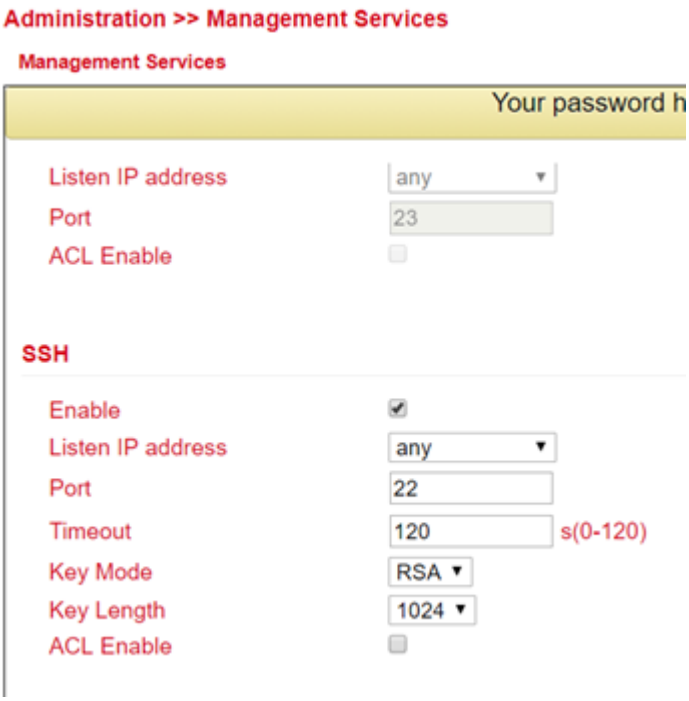


Parameter	Description
Protocol	TCP or UDP
Outside Interface	The interface to be accessed from
Service Port	The port that is open to the outside
Internal Address	The internal IP address to be reached
Internal Port	The internal port to be reached
Description	Brief description
If Cellular 1 is selected as Outside Interface, the port mapping only works if the cellular interface is assigned a public IP address!	

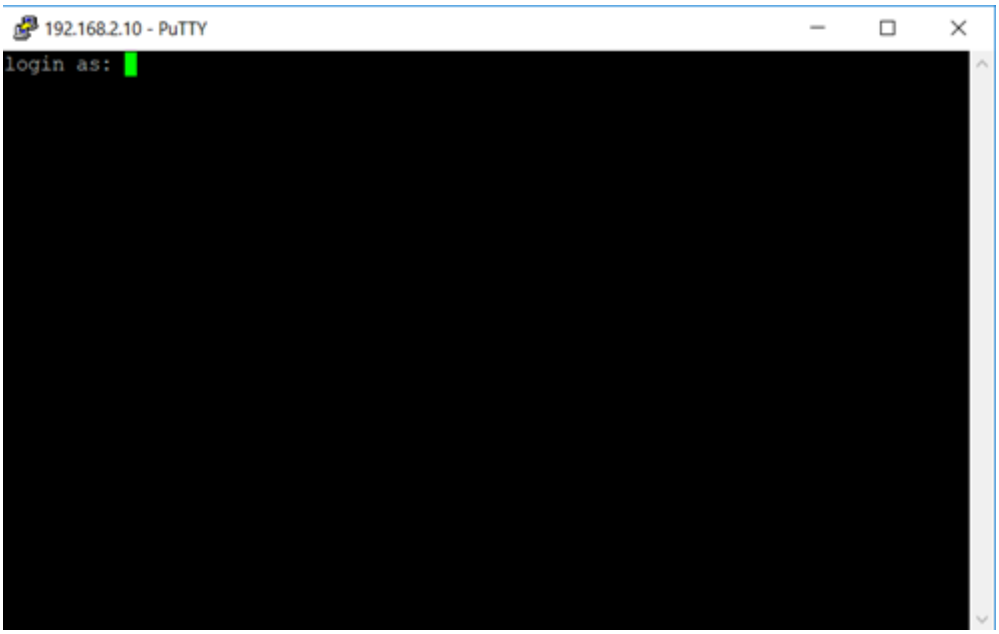
3.13 3.12. CLI Commands

In addition to the web interface, which can be accessed via the IP address of the router, it is also possible to configure and manage the router via the CLI (Command Line Interface). There are several ways to connect to the router via the CLI. For example, putty has proven itself as a tool for this.

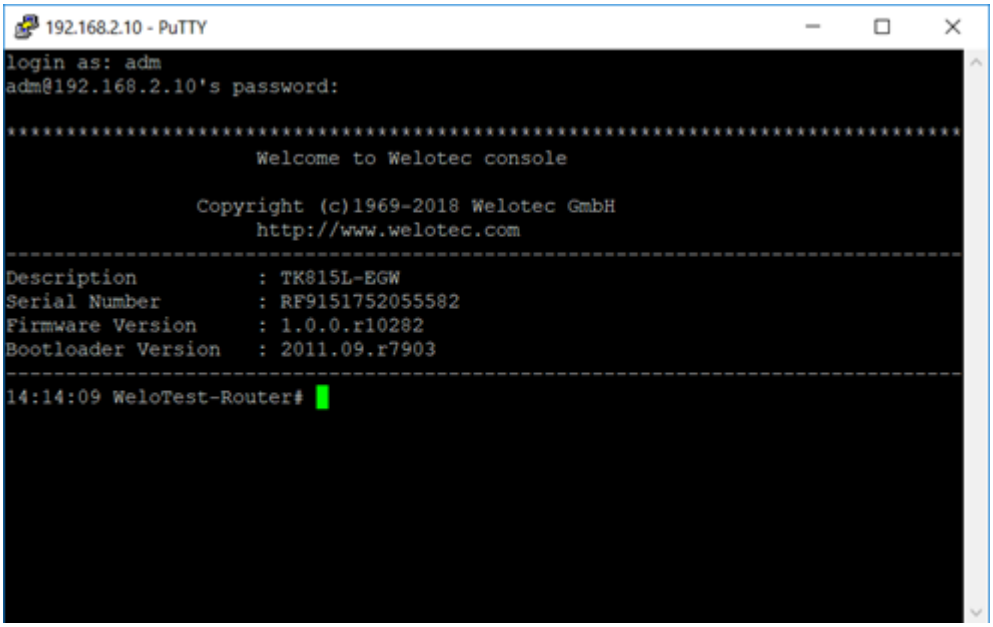
One way to connect via the CLI is via SSH. However, this function must first be activated in the router. This is done via Administration > Management Services. Here the SSH function has to be enabled. The second way to connect to the router is via Telnet in connection with a serial console cable. To do this, Telnet must be enabled under Administration > Management Services, as with SSH, and the console cable must be connected to a computer at the router port labeled Console. Please save the changes with Apply&Save.



Then start e.g. putty and enter the IP address of your router and select SSH or TELNET as port or connection type. Then click on open to establish the connection to the router. If the connection is established successfully, you will get the CLI window with the login for the router.



Log in here with the credentials of your router (default user is adm and default password is 123456). If you have logged in successfully, you will see the following screen.

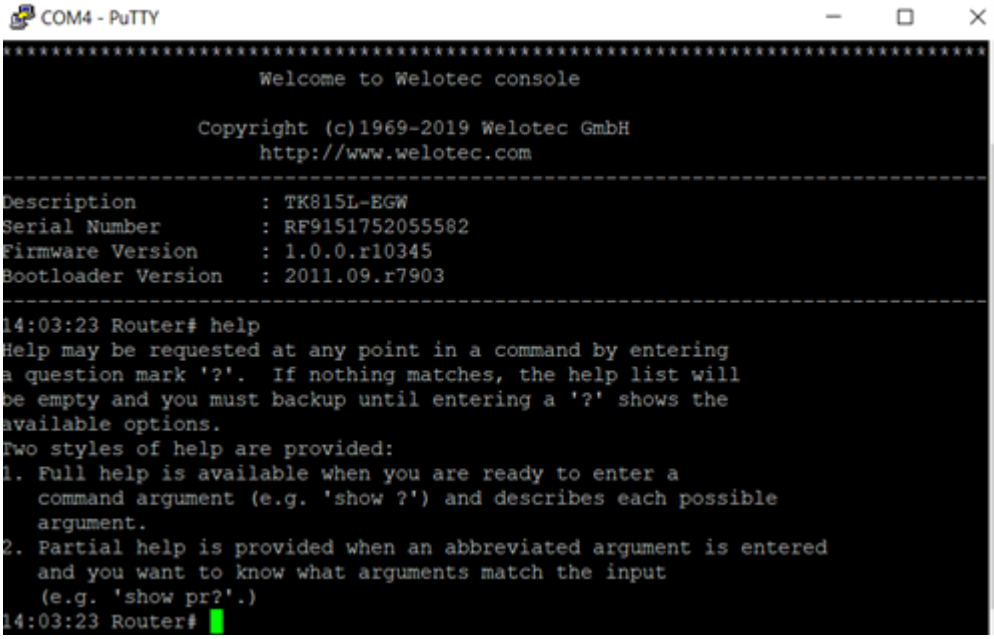


From here on you can use the following commands for help, analysis, configuration, etc.

Another way to connect to the router via the CLI is via a serial console cable. This is plugged into the console port of the router and connected to the PC.

3.13.1 3.12.1. Help Command

Help can be retrieved after entering help or “?” into the console, “?” can be entered at any time during command entry to get the current command or help from the command parameters, and the command or parameters can be auto-completed if only the command or command parameter is present.



Entering help at the command prompt gives a short description of how to use the help command. If you append the “?” to a command, the possibilities that you can use in connection with the command are displayed. If there is no output, no or no further command exists for this input.

3.13.2 3.12.2. Show Command

The show command can be used to display parameters of the router or the configuration of the router. The help command or the “?” indicate the commands that can be used in combination with show.

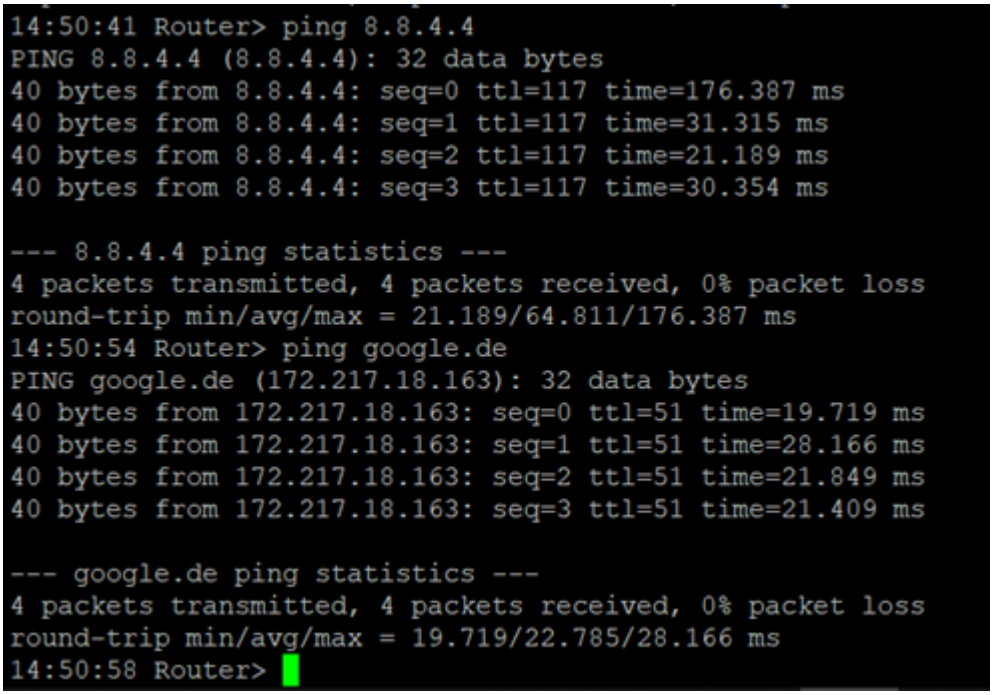
```
14:33:33 Router# show
  access-list       Show access lists
  alarm             Show alarm information
  arp               Show ARP table
  backup            Show backup information
  bridge            The config of bridge
  cellular          Show cellular information
  channel-group     Port channel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

show version for example shows you data about the router, like the description, serial number, firmware and boot-loader version.

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

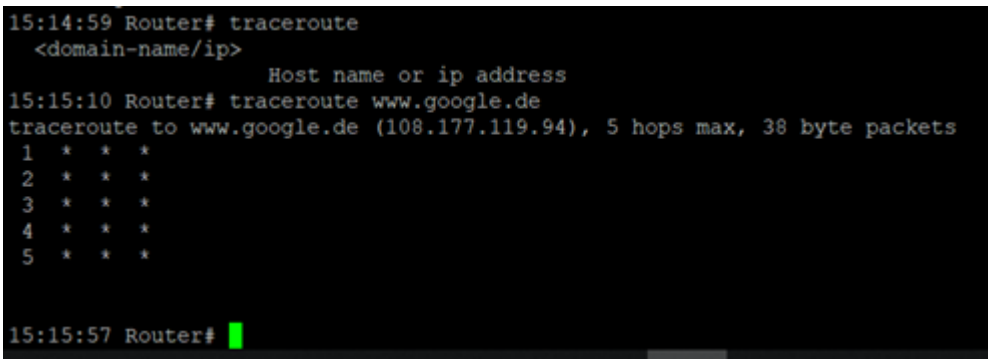
3.13.3 3.12.3. Ping Command

The ping command can be used to check whether the router has a connection to the Internet. The input form is, as usual with Windows, **Ping Hostname** or **IP-Address.**



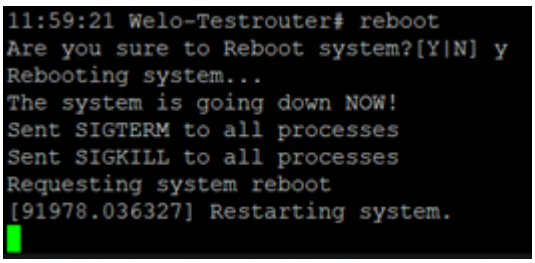
3.13.4 3.12.4. Traceroute Command

With traceroute you test the active routing of the specified destination. With **traceroute hostname** or **IP address** you start the query.



3.13.5 3.12.5. Reboot Command

To restart the router, you can use the reboot command. Enter it in the CLI and the router will be restarted.

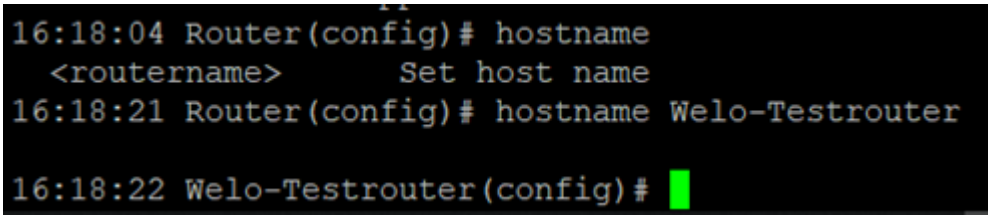


3.13.6 3.12.6. Configuration Command

In the superuser view, the router can use the configure command to switch the configuration view for management. A configure command can support no and default, where no indicates setting the abort of a parameter and default indicates restoring the default setting of a parameter. The configure terminal (or conf t for short) command switches the system to configuration mode. In this setting the router can be configured. To exit the configuration mode use the exit command. All entered commands must be terminated with the wr command so that the changes are applied to the router.

3.12.6.1 Hostname Command

In configuration mode, the router name can now be changed, for example. This is done with the command hostname name-of-router. This command changes the router name to the name you entered. If you want to reset the default name of the router, use the default hostname command. This resets the router name to the default router name.



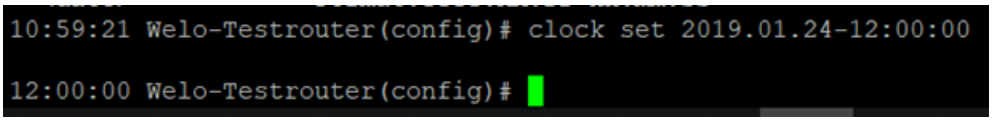
3.12.6.2 Clock set Command

With the clock set command you can configure the system date and time of the router via the CLI. The date and time format is as follows:

YYYY.MM.DD-HH:MM:SS

The complete command would then look like this

clock set 2019.01.24-12:00:00



3.12.6.3 Enable password Command

It is always possible to change the password of the super user (adm) via the CLI. You can do this with the enable password command. The input format for this is

Enable password *[password]*

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

13:49:55 Router(config)# wr

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

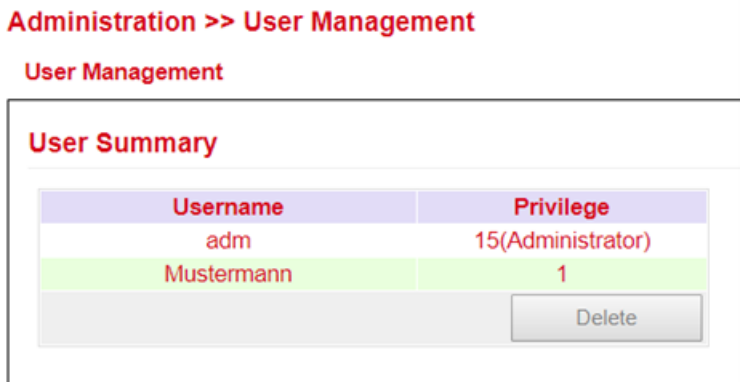
3.12.6.3 Username Command

The Username command allows you to create users to access the router. The syntax for the input is

Username *[Username]*

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

13:54:46 Router(config)# wr

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

When creating the user, you will be asked for a new password that you can assign here. The user that is created is always a standard user.



4 4. Technical Specifications

4.1 Device Properties

Property	Value
Dimensions (W x H x D)	45 x 132,6 x 112,8 mm
Operating voltage	230 V AC to 12 V – 48V DC
Power consumption Standby	3,8 W
Power consumption Active	5,3 W
Approval	CE compliant

4.2 Environmental Conditions

Property	Value
Operating temperature range	-25 to + 70 °C
Storage temperature range	-40 to +85 °C
Air humidity	5 - 95 %, non condensing
Concussions	IEC 60068-2-27
Free fall	IEC 60068-2-32
Vibration	IEC 60068-2-6

4.3 Radio Frequencies LTE Europe

Fre-quency	Frequency Range and Transmit Power	Router
Band 1	Frequency Range Down: 2110 MHz – 2170 MHz Frequency Range Up: 1920 MHz – 1980 MHz Max. Transmit Power:199 mW	TK812L, TK815L-EX0, TK815L-EXW, TK815L-EGW
Band 3	Frequency Range Down: 1805 MHz – 1880 MHz Frequency Range Up: 1710 MHz – 1785 MHz Max. Transmit Power:199 mW	TK812L, TK815L-EX0, TK815L-EXW, TK815L-EGW
Band 7	Frequency Range Down: 2620 MHz – 2690 MHz Frequency Range Up: 2500 MHz – 2570 MHz Max. Transmit Power:199 mW	TK812L, TK815L-EX0, TK815L-EXW, TK815L-EGW
Band 8	Frequency Range Down: 925 MHz – 960 MHz Frequency Range Up: 880 MHz – 915 MHz Max. Transmit Power:199 mW	TK812L, TK815L-EX0, TK815L-EXW, TK815L-EGW
Band 20	Frequency Range Down: 791 MHz – 821 MHz Frequency Range Up: 832 MHz – 862 MHz Max. Transmit Power: 199 mW	TK812L, TK815L-EX0, TK815L-EXW, TK815L-EGW

4.4 Radio Frequencies UMTS Europe

Frequency	Frequency Range and Transmit Power	Router
Band 1	Frequency Range Down: 2110 MHz – 2170 MHz Frequency Range Up: 1920 MHz – 1980 MHz Max. Transmit Power: 251 mW	TK802U, TK812L, TK815L-EX0, TK815L-EXW, TK815L-EGW
Band 3	Frequency Range Down: 1805 MHz – 1880 MHz Frequency Range Up: 1710 MHz – 1785 MHz Max. Transmit Power:251 mW	TK802U, TK812L, TK815L-EX0, TK815L-EXW, TK815L-EGW
Band 8	Frequency Range Down: 925 MHz – 960 MHz Frequency Range Up: 880 MHz – 915 MHz Max. Transmit Power:251 mW	TK802U, TK812L, TK815L-EX0, TK815L-EXW, TK815L-EGW

4.5 Radio Frequencies GSM Europe

Frequency	Frequency Range and Transmit Power	Router
GSM 900	Frequency Range Down: 925 MHz – 960 MHz Frequency Range Up: 880 MHz – 915 MHz Max. Transmit Power: 1995 mW	TK802U, TK812L, TK815L-EX0, TK815L-EXW, TK815L-EGW
GSM 1800	Frequency Range Down: 1805 MHz – 1880 MHz Frequency Range Up: 1710 MHz – 1785 MHz Max. Transmit Power: 1000 mW	TK802U, TK812L, TK815L-EX0, TK815L-EXW, TK815L-EGW

4.6 Radio Frequencies LTE Asia

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

4.7 Radio Frequencies UMTS Asia

Frequency	Frequency Range and Transmit Power	Router
Band 1	Frequency Range Down: 2110MHz – 2170 MHz Frequency Range Up: 1920 MHz – 1980 MHz Max. Transmit Power: 251 mW	TK822L, TK825L-EXW, TK825L-EX0
Band 5	Frequency Range Down: 869 MHz – 894 MHz Frequency Range Up: 824 MHz – 849 MHz Max. Transmit Power: 251 mW	TK822L, TK825L-EXW, TK825L-EX0
Band 8	Frequency Range Down: 925 MHz – 960 MHz Frequency Range Up: 880 MHz – 915 MHz Max. Transmit Power: 251 mW	TK822L, TK825L-EXW, TK825L-EX0

4.8 Radio Frequencies GSM Asia

Frequency	Frequency Range and Transmit Power	Router
GSM 900	Frequency Range Down: 925 MHz – 960 MHz Frequency Range Up: 880 MHz – 915 MHz Max. Transmit Power: 1995 mW	TK822L, TK825L-EXW, TK825L-EX0
GSM 1800	Frequency Range Down: 1805 MHz – 1880 MHz Frequency Range Up: 1710 MHz – 1785 MHz Max. Transmit Power: 1000 mW	TK822L, TK825L-EXW, TK825L-EX0

4.9 Radio Frequencies LTE USA

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

4.10 Radio Frequencies UMTS USA

Frequency	Frequency Range and Transmit Power	Router
Band 2	Frequency Range Down: 1930 MHz – 1990 MHz Frequency Range Up: 1850 MHz – 1910 MHz Max. Transmit Power: 251 mW	TK832L, TK835L-EXW, TK835L-EX0, TK842L, TK845L-EXW, TK845L-EX0
Band 4	Frequency Range Down: 2110 MHz – 2155 MHz Frequency Range Up: 1710 MHz – 1755 MHz Max. Transmit Power: 251 mW	TK832L, TK835L-EXW, TK835L-EX0, TK842L, TK845L-EXW, TK845L-EX0
Band 5	Frequency Range Down: 869 MHz – 894 MHz Frequency Range Up: 824 MHz – 849 MHz Max. Transmit Power: 251 mW	TK832L, TK835L-EXW, TK835L-EX0, TK842L, TK845L-EXW, TK845L-EX0

4.11 Radio Frequencies GSM USA

Frequency	Frequency Range and Transmit Power	Router
GSM 850	Frequency Range Down: 869 MHz – 894 MHz Frequency Range Up: 824 MHz – 849 MHz Max. Transmit Power: 1995 mW	TK832L, TK835L-EXW, TK835L-EX0, TK842L, TK845L-EXW, TK845L-EX0
GSM 1900	Frequency Range Down: 1930 MHz – 1990 MHz Frequency Range Up: 1850 MHz – 1910 MHz Max. Transmit Power: 1000 mW	TK832L, TK835L-EXW, TK835L-EX0, TK842L, TK845L-EXW, TK845L-EX0

4.12 Radio Frequencies LTE for Additional Countries Worldwide

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

4.13 Radio Frequencies UMTS for Additional Countries Worldwide

Frequency	Frequency Range and Transmit Power	Router
Band 2	Frequency Range Down: 1930 MHz – 1990 MHz Frequency Range Up: 1850 MHz – 1910 MHz Max. Transmit Power: 251 mW	TK882L, TK885L-EX0, TK885L-EXW
Band 4	Frequency Range Down: 2110 MHz – 2155 MHz Frequency Range Up: 1710 MHz – 1755 MHz Max. Transmit Power:251 mW	TK882L, TK885L-EX0, TK885L-EXW
Band 5	Frequency Range Down: 869 MHz – 894 MHz Frequency Range Up: 824 MHz – 894 MHz Max. Transmit Power:251 mW	TK882L, TK885L-EX0, TK885L-EXW

4.14 Radio Frequencies GSM for Additional Countries Worldwide

Frequency	Frequency Range and Transmit Power	Router
GSM 900	Frequency Range Down: 925 MHz – 960 MHz Frequency Range Up: 880 MHz – 915 MHz Max. Transmit Power: 1995 mW	TK882L, TK885L-EX0, TK885L-EXW
GSM 1800	Frequency Range Down: 1805 MHz – 1880 MHz Frequency Range Up: 1710 MHz – 1785 MHz Max. Transmit Power: 1000 mW	TK882L, TK885L-EX0, TK885L-EXW

4.15 Radio Frequencies WLAN

Frequency	Frequency Range and Transmit Power	Router
2,4 GHz	Frequency Range: 2400 MHz – 2483,5 MHz Max. Transmit Power: 40 mW	TK805-EXW, TK815L-EXW, TK815L-EGW , TK825L-EXW, TK835L-EXW, TK845L-EXW

5 5. CE Declaration

CE declaration of conformity

WELOTEC
a byte smarter

The manufacturer:
Welotec GmbH
Zum Hagenbach 7
48366 Laer
GERMANY

herewith declares that the products:

Product:
Wireless Router

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

Complies with:

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

CE

The corresponding markings appear under the appliance.

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

15.07.2017
Date

Jos Zenner

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

6 TK800-Series - FAQ: IPsec

6.1 Preface

IPsec is an extension of the Internet Protocol (IP) with encryption and authentication mechanisms. This gives the Internet Protocol the ability to transport IP packets over public and insecure networks in a cryptographically secured manner. IPsec was developed by the Internet Engineering Task Force (IETF) as an integral part of IPv6. Because the Internet Protocol version 4 originally had no security mechanisms, IPsec was subsequently specified for IPv4.

6.1.1 *Components of IPsec-VPNs*

- Interoperability
- Cryptographic protection of transmitted data
- Access Control
- Data Integrity
- Authentication of the sender (user authentication)
- Encryption
- Key authentication
- Administration of keys (key management)

Behind these components are processes that, when combined, provide reliable security for data transmission over public networks. VPN security solutions with high security requirements therefore generally rely on IPsec.

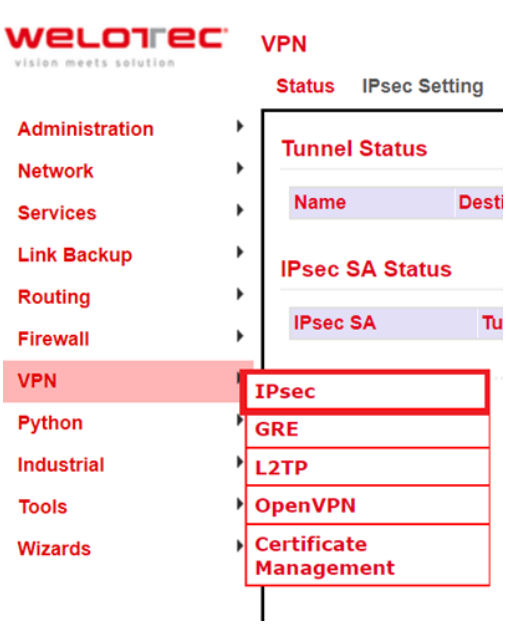
6.1.2 *Deployment scenarios*

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

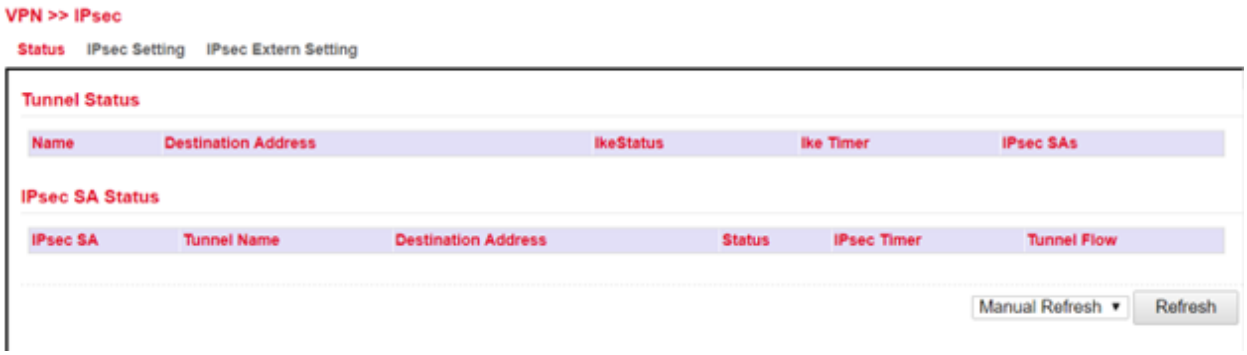
In principle, IPsec is suitable for gateway-to-gateway scenarios. In other words, the connection between networks via a third insecure network.

6.1.3 IPsec

By clicking ***VPN > IPsec***, you can initially view the status of your IPsec tunnel, if you have already created one.

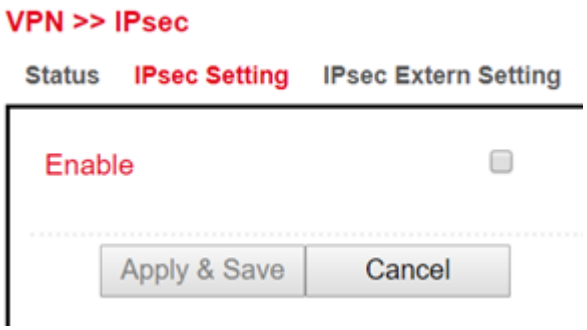


Here the options *"IPsec Setting"* and *"IPsec Extern Setting"* are available.

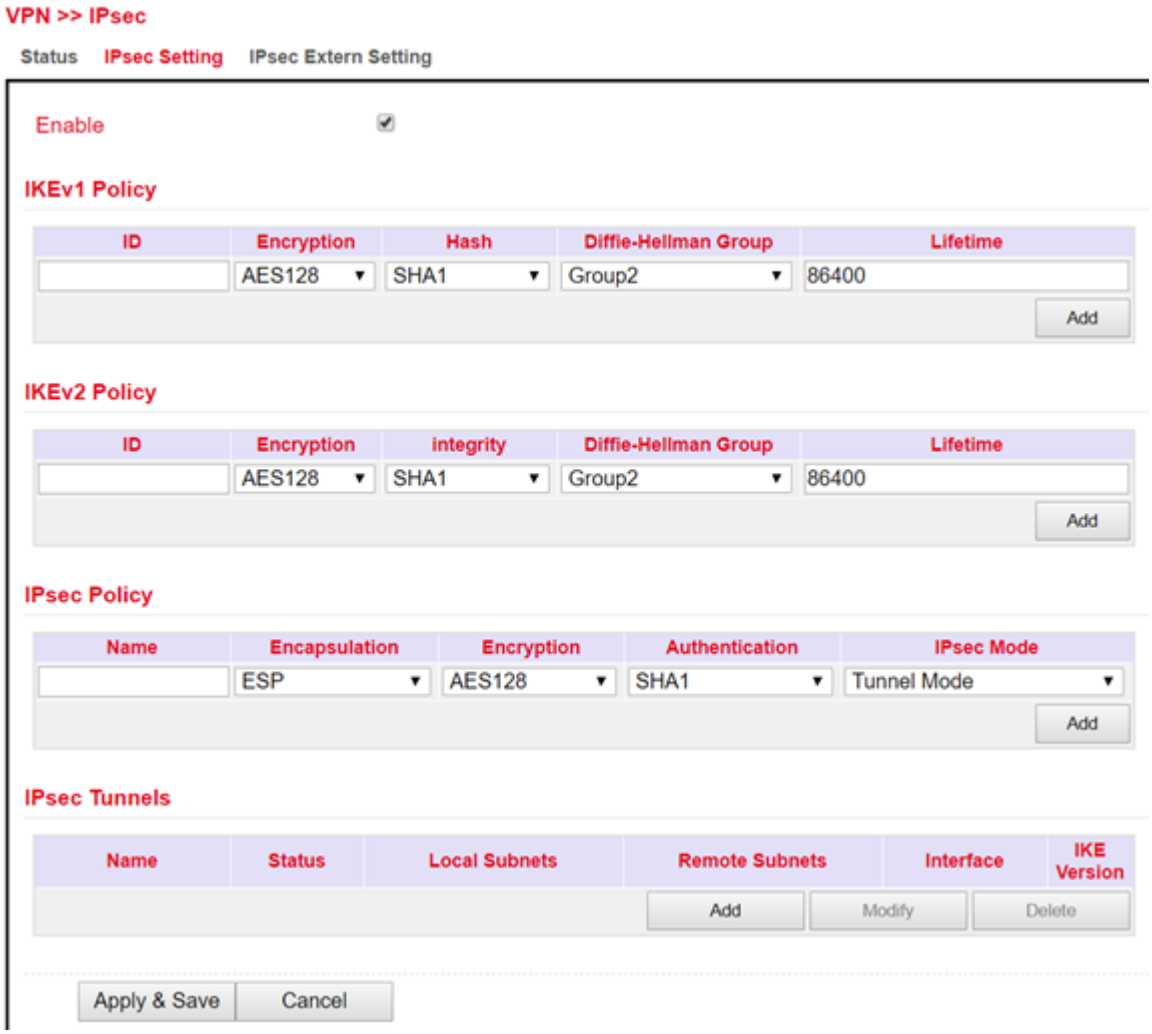


To create a new IPsec tunnel, proceed as follows:

1. Click on **"IPsec Setting"**



2. Click on **"Enable"**



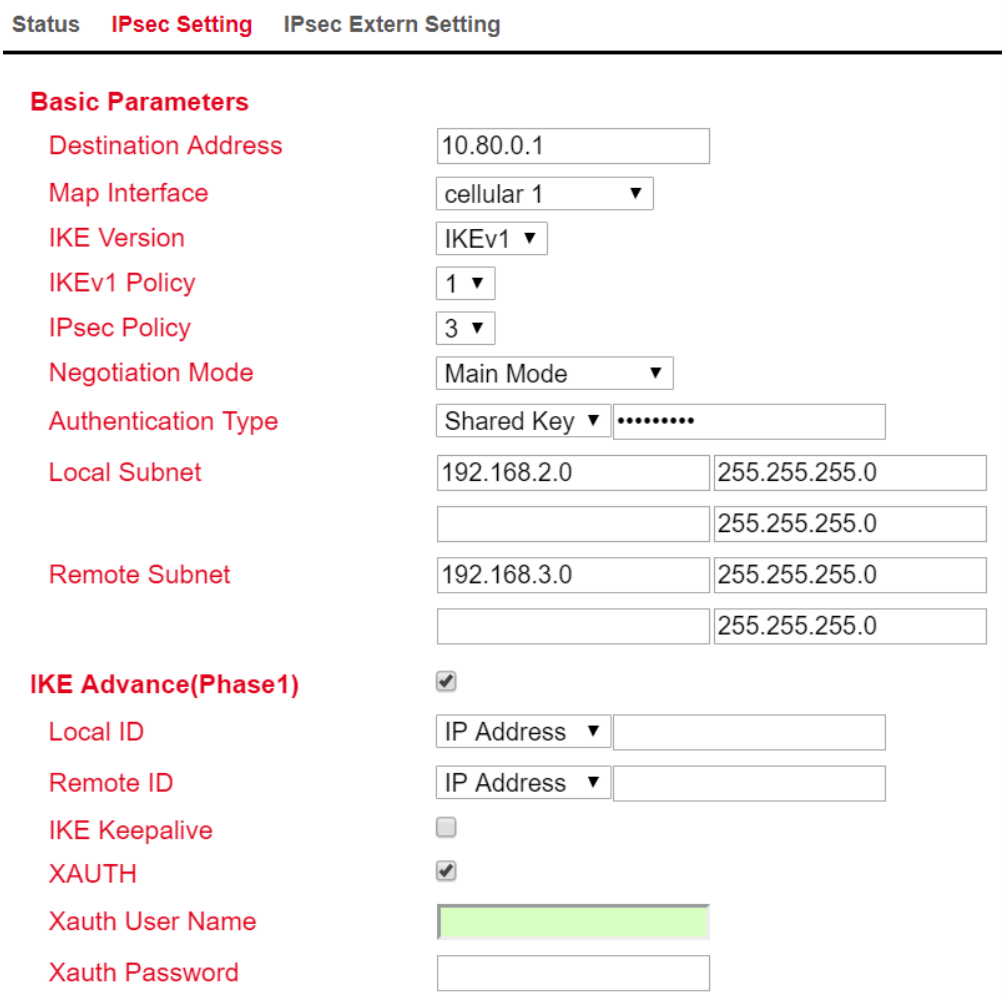
Now you can start with the configuration. Proceed as follows:

1. *IKEv1 and IKEv2 Policy:*
   - To confirm your settings, press the **"Add"** button.
   - ID is used to identify the policy in the tunnel configuration and can be selected freely. The input field is an integer field.
   - Encryption contains a selection list of encryption methods, e.g. AES256.
   - Hash contains the hash algorithm, e.g. SHA1 or SHA2-256.
   - Diffie-Hellman Group offers the possibility to choose the key strength during the key exchange process. The higher the group, the higher the encryption, e.g. Group2 = 1024 Bit.
   - Lifetime is the period of validity of the IKE before it is renegotiated.
2. *IPsec Policy:*
   - The name is used to identify the policy in the tunnel configuration and can be freely chosen.
   - Encapsulating Security Payload (***ESP***) provides authentication, integrity and confidentiality of IP packets within IPsec. In contrast to Authentication Header (***AH***), the user data is transmitted in encrypted form. While AH can "only ensure the integrity and authenticity" of data, ESP increases data security depending on the encryption algorithm chosen. That is why ESP is usually used instead of AH. ESP ensures the confidentiality of the communication. The packets are encrypted. In addition, an integrity protection protects against manipulation. Choose the appropriate protocol for **"Encapsulation"**.

- Enter the encryption in the corresponding field. The **Advanced Encryption Standard** (**AES**) is the successor encryption standard to **DES** (Data Encryption System). **3DES** with 128 bits is still considered secure but is significantly slower than AES because of the triple encryption. AES supports 128, 192 and 256 bit long keys.
- ***Authentication*** is used for authentication and can be selected with MD5, SHA1 und SHA2.
- In addition to the choice between AH and ESP, you have the option of sending the packets over the network in transport or tunnel mode. In transport mode, the original IP header, i.e. IP address plus IP options, will still be used. In tunnel mode, IPsec encapsulates the entire packet including the IP header and writes a new IP header in front of it. The original IP address is no longer visible. Only when decrypting on the opposite side, the IP address together with the rest of the packet becomes visible again. Set the appropriate mode here.

3. *IPsec Tunnels:*

   To create the IPsec tunnel, first click the **"Add"** button



- *Basic Parameters*

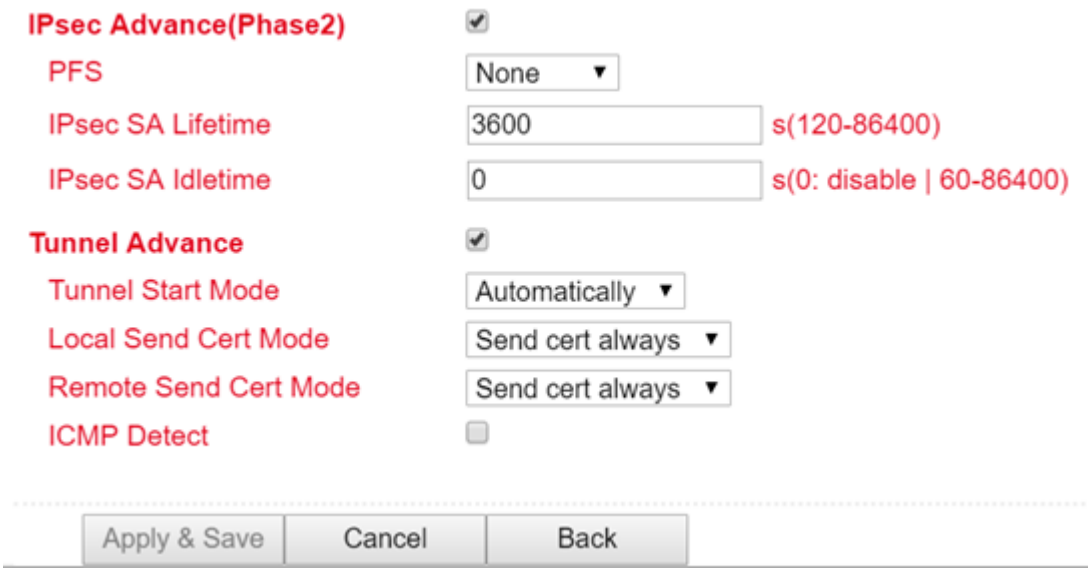
  1. The **"Destination Address"** is the IP address of the tunnel remote station. Enter the corresponding IP address here.
  2. For **"Map Interface"**, please enter the interface via which the connection is to be established.
  3. Under **"IKE Version"**, select the version you created under IKEv1 or IKEv2. Depending on the defaults, the values in the list box will be applied.
  4. The name of the IPsec policy created previously appears in the **"IPsec Policy"** field.

5. Under **“Negotiation Mode”** you can choose between two options when negotiating the IPsec tunnel. In *Main Mode*, the initiator (the one who wants to establish the connection) and the responder negotiate an ISAKMP-SA with each other. This negotiation happens in several steps. In *Aggressive Mode*, all but three of the above steps are combined, and the hash values of the pre-shared keys are transmitted in clear text. However, there may be a reason for using this mode if the initiator’s address is not known to the responder in advance, and both sides want to use pre-shared keys for authentication. Aggressive Mode should be used with caution, however, because in practice strong keys are often not used for reasons of convenience.
6. Select the type of authentication for ***“Authentication Type”***. You have two options here. Either via Shared Key, the common key for authentication (to be entered in the following field) or via Certificate, i.e. via existing certificates, which then have to be imported via **“VPN > Certificate Management”**.
7. Enter the subnet of the router under **“Local Subnet”**. In the first field enter the IP address and in the second the subnet mask. You can create up to four entries.
8. Under **“Remote Subnet”** you can then enter the subnet of the remote station. Here, you also have the option of creating up to four entries.

- *IKE Advance (Phase 1)*

  After activation, the following options are available:

  1. Via the **“Local ID”** you have the option to select different entries from the list box and then enter the corresponding data in the following field, e.g. IP Address and then enter the desired IP address in the following field.
  2. In the **“Remote ID”** field, you then enter the data for the remote station.
  3. **“IKE Keepalive”** you can switch on or off to maintain the IKE phase one.
  4. You can use the XAUTH protocol for the VPN remote terminal separately by activating this function for XAUTH. You can then specify or use a corresponding username (Xauth User Name) and password (Xauth Password).



- *IPsec Advance (Phase 2)*

  After activation, the following options are available:

  1. **Perfect Forward Secrecy (PFS)** is a characteristic of certain key exchange protocols in cryptography. These use previously exchanged long-term keys to arrange a new secret session key for each session that needs to be encrypted. Perfect Forward Secrecy does not have a log so that the session keys used cannot be reconstructed from the long-term secret keys after the session is closed. This means that a recorded encrypted communication cannot be subsequently decrypted even if the long-term key is known. Here you

can choose between several groups that work with Diffie Hellman keys. For example, Group 1 has an encryption of 768 bits, Group2 has 1024 bits and Group 5 uses 1536 bit, etc.

2. You can enter the validity period of the SA (Security Association) under **"IPsec SA Lifetime"**. A Security Association groups IP packets together based on an SPI (Security Parameter Index), the IP destination address and the Security Protocol Identifier. An SA is only valid for ONE direction at a time, so there are always two SAs in use.
3. With **"IPsec SA Idletime"** you specify whether SAs associated with inactive peers can be deleted before the global lifetime has expired. The 0 means that the function is disabled.

- *Tunnel Advance*

  After activation, the following options are available:

1. For **"Tunnel Start Mode"**, set how the tunnel should start. The default setting is always automatic.
2. In the **"Local Send Cert Mode"** field, you specify when a certificate should be sent for the local area. The default setting is that the certificate should always be sent (Send cert always).
3. With **"Remote Send Cert Mode"** you define when a certificate should be sent for the remote site. The default setting is that the certificate should always be sent (Send cert always).

image

4. With **"ICMP Detect"** you can activate or deactivate the ICMP Watchdog function.
5. For **"ICMP Detection Server"**, specify the address of a server that can only be reached through the tunnel.
6. Under **"ICMP Detection Local IP"**, enter the router interface IP of the local subnet.
7. Under **"ICMP Detection Interval"**, specify the interval at which the ICMP packet is to be sent.
8. **"ICMP Detection Timeout"** is the timer after which the ICMP packet is discarded. Enter a value here between 1 and 60 sec.
9. **"ICMP Detection Max Retries"** are the maximum attempts after a failed ICMP ping, which you can enter here.

6.1.4 IPsec Status

If the IPsec tunnel(s) have been successfully established, then you will see the following in the status overview.