TK800 ROUTER SERIES
MANUAL

Version 2.1

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

www.welotec.com

TABLE OF CONTENTS

1. INTRODUCTION

Note on copyright

Trademarks

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

Legal notice

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

Contact information for technical support

Welotec GmbH
Zum Hagenbach 7
48366 Laer
Phone.: +49 2554 9130 00
Fax.: +49 2554 9130 10
Email: info@welotec.com

Description

The TK800 series industrial routers provide a stable connection between remote devices and customer locations via 2G/3G/4G networks. They can be used in a voltage range of 12 - 48V DC and have a temperature range of -25°C to 70°C at a relative humidity of 95 % and compliance with numerous EMC standards, ensuring high stability and reliability under strict industrial conditions. The TK800 can be used at the workplace or mounted on DIN rails. TK800 Series products support VPN (IPSec/L2TP/GRE/OpenVPN) for secure connections between remote devices and customer locations.

Important safety instructions

This product is not suitable for the following applications

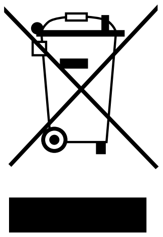
- areas where no wireless applications (such as mobile phones) are allowed
- hospitals and other places where the use of mobile phones is not permitted
- petrol stations, fuel depots and places where chemicals are stored
- chemical plants or other places with a explosion hazard
- metal surfaces which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

Warning

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

WEEE Notice

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



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

2. QUICK START

TK800 series installation and commissioning guide. Please make sure that all package contents are present on delivery. If you need a SIM card, contact your local network operator.

2.1. Package Checklist

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

2.1.1. Components router

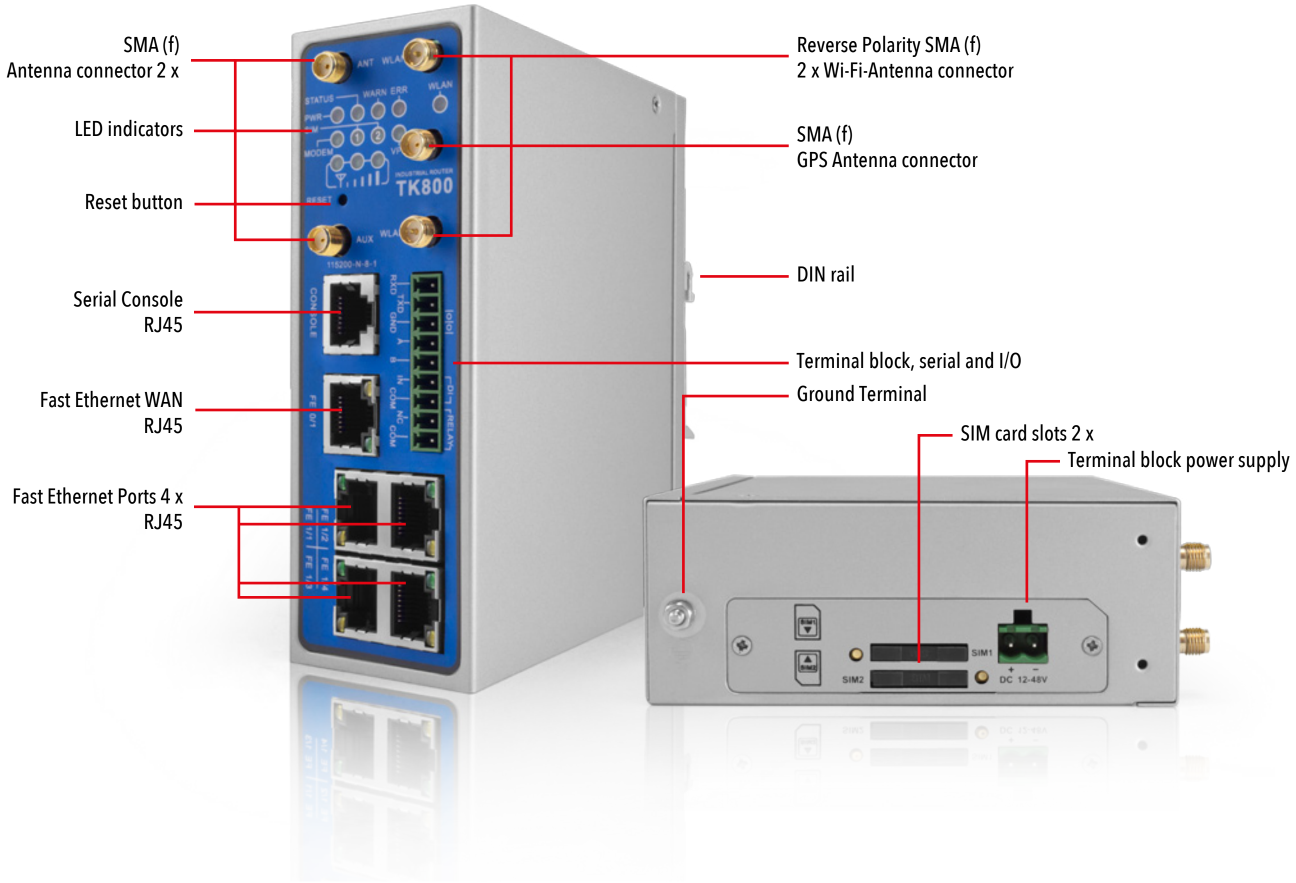
Product	Amount	Description
TK800	1	Industrial Router of the TK800 series
Terminal block	1	Terminal block, 2-pin
Terminal block serial and I/O	1	Terminal block, 9-pin (EXO / EXW versions only)

2.1.2. Components Set

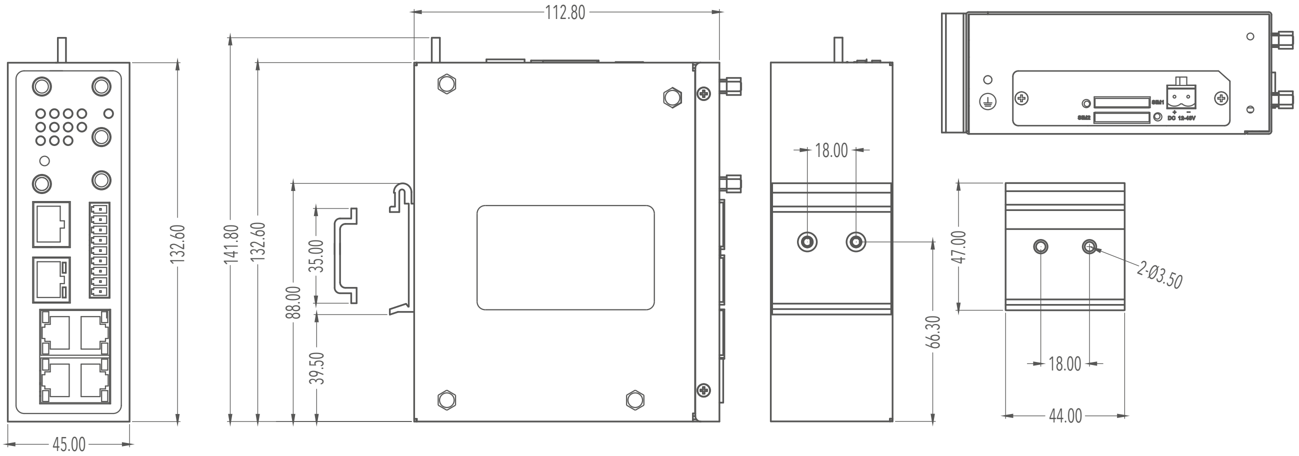
Product	Amount	Description
TK800	1	Industrial Router of the TK800 series
Terminal block	1	Terminal block, 2-pin
Network cable	1	1.5 m
Antenna	2 (4)	3G/4G Antenna Wi-fi Antenna (EXW version only)
Power supply	1	230 V AC to 12 V DC
Terminal block serial and I/O	1	Terminal block, 9-pin (EXO / EXW versions only)

2.2. Information and control panel

2.2.1. Control panel



2.2.2. Dimensional drawings



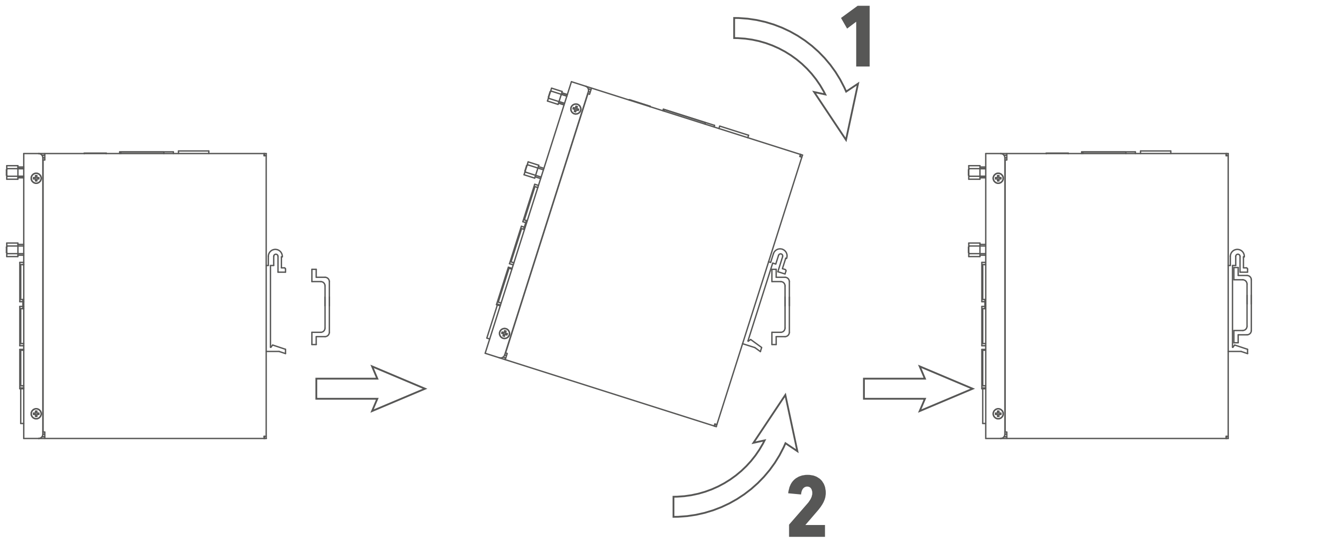
2.3. Installation guide

2.3.1. Preparations

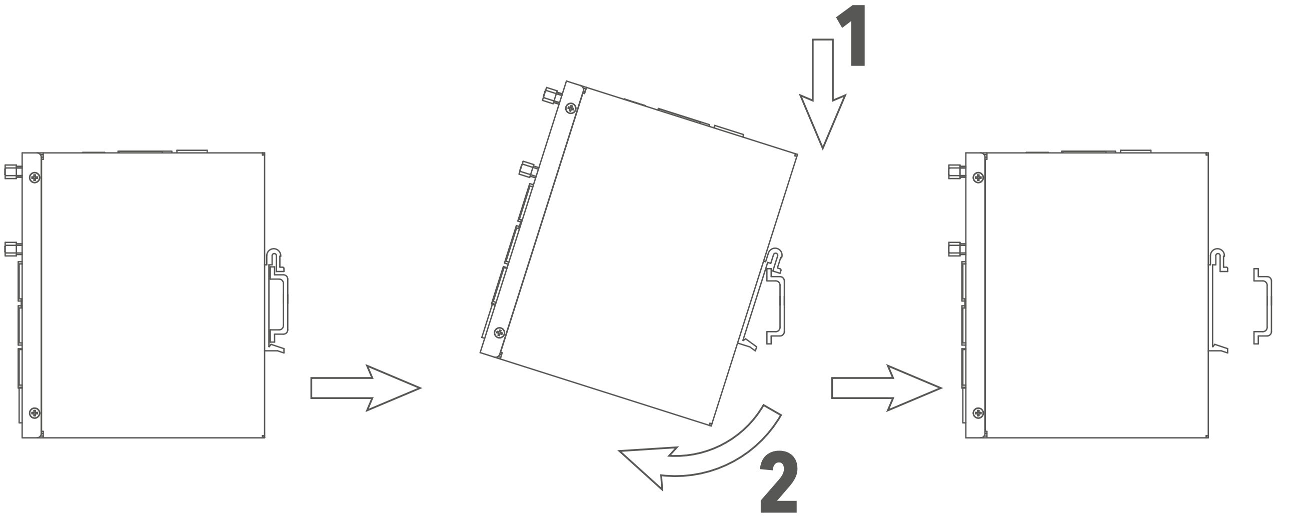
Prepare the power supply (12 - 48 V DC). Ensure that the device can operate under the specified ambient conditions (operating temperature range -25 - +70 °C, humidity: 5 - 95 % relative humidity). The device should not be exposed to direct sunlight and should be installed separately from heat sources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

2.3.2. Mounting the device

Mounting rail:
Select a location with enough space on the mounting rail. Then place the upper part of the mounting on the mounting rail. Afterwards, press the lower side of the mounting rail receptacle downward until the device is locked. This is illustrated in this image:

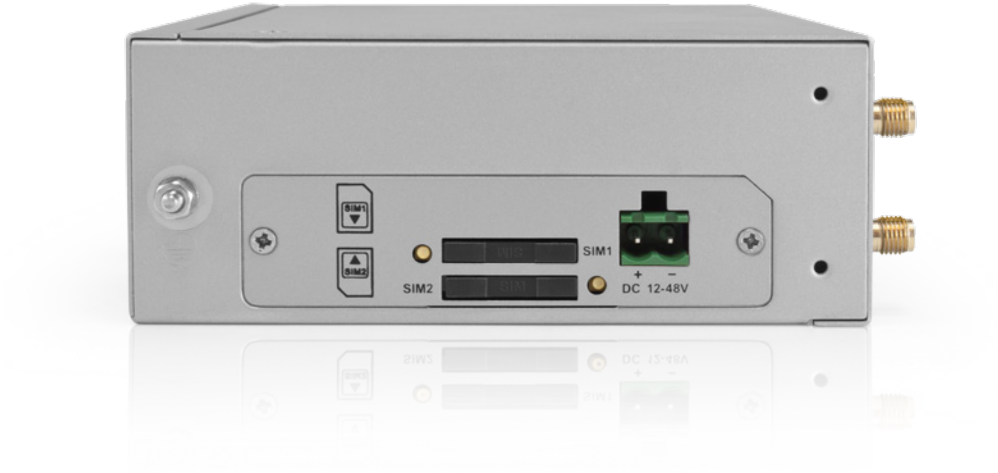


To disassemble press the device from the top toward the bottom, and then pull the bottom side of the device from the mounting rail (see Figure).



2.4. Installing the SIM card

The TK800 supports dual SIM. To insert the cards, press the yellow „Eject" button e. g. with a small screwdriver on top of the device. The respective SIM card slot is pressed 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-plug capable. The router must be restarted after inserting the SIM card.



2.5. Installation of the antennas

Plug the antennas into the SMA connectors and turn the outer mounting on the antenna cable until the connection is secure.

⚠ **Note**

For optimal performance, the antennas should be placed at least 20 cm apart from each other.

2.6. Installation of the power supply

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

Use the grounding screw on the unit to ground the unit.

⚠ **Note**

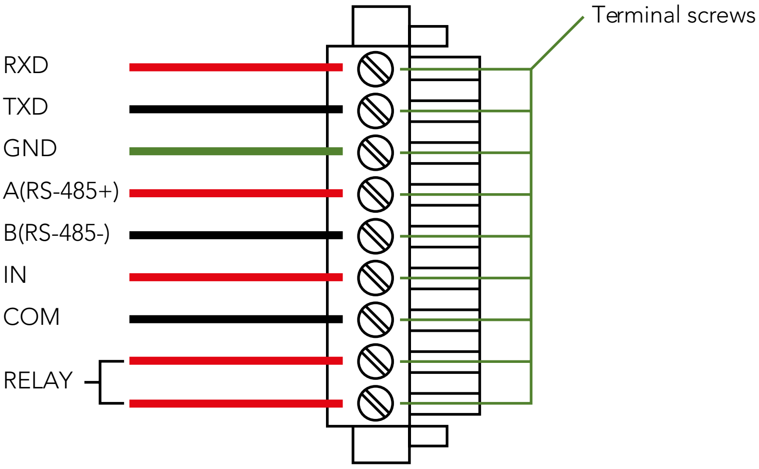
To eliminate electromagnetic interference, the housing of the router must be earthed via the grounding screw.

2.7. Cable connections

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

2.8. Connection of serial interfaces and I/Os

To connect the serial interfaces and the I/Os, you will find a connection block on the front panel of the device. The individual contacts for this are marked on the front of the device. Connect the cables according to these labels. The contact „IN" represents the digital input here, while the output is labeled „Relay". „COM" represents the ground. During installation, remove the connection block from the device and connect the individual cores to the corresponding terminals. Then plug the terminal block back into the device.



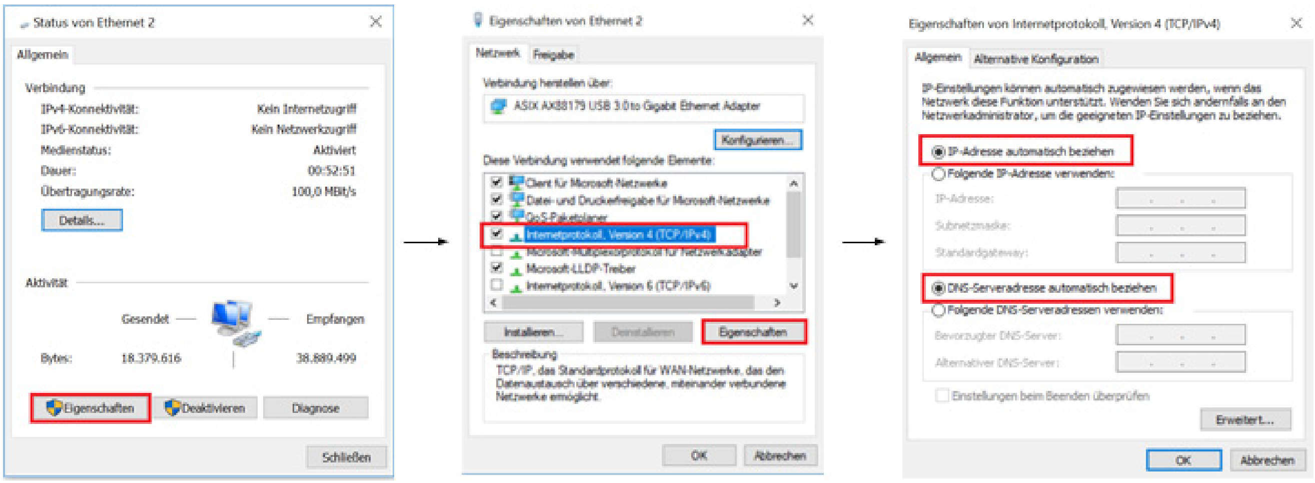
⚠ **Note**

This chapter only describes routers with serial interfaces and I/O's TK8XXX-EX.

2.9. Setting up the router

2.9.1. Automatic Configuration (DHCP)

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



Status von Ethernet 2

Allgemein

Verbindung

IPv4-Konnektivität:	Kein Internetzugriff
IPv6-Konnektivität:	Kein Netzwerkzugriff
Medienstatus:	Aktiviert
Dauer:	00:52:51
Übertragungsrate:	100,0 MBit/s

Aktivität

	Gesendet	Empfangen
Bytes:	18.379.616	38.889.499

Eigenschaften von Ethernet 2

Netzwerk | Freigabe

Verbindung herstellen über:

ASIX AX88179 USB 3.0 to Gigabit Ethernet Adapter

Diese Verbindung verwendet folgende Elemente:

- ☑ Client für Microsoft-Netzwerke
- ☑ Datei- und Druckerfreigabe für Microsoft-Netzwerke
- ☑ QoS-Paketplaner
- ☑ Internetprotokoll, Version 4 (TCP/IPv4)
- □ Microsoft-Multiplexorprotokoll für Netzwerkadapter
- ☑ Microsoft-LLDP-Treiber
- □ Internetprotokoll, Version 6 (TCP/IPv6)

Beschreibung

TCP/IP, das Standardprotokoll für WAN-Netzwerke, das den Datenaustausch über verschiedene, miteinander verbundene Netzwerke ermöglicht.

Eigenschaften von Internetprotokoll, Version 4 (TCP/IPv4)

Allgemein | Alternative Konfiguration

IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.

- ● IP-Adresse automatisch beziehen
- ○ Folgende IP-Adresse verwenden:
  - IP-Adresse: . . .
  - Subnetzmaske: . . .
  - Standardgateway: . . .
- ● DNS-Serveradresse automatisch beziehen
- ○ Folgende DNS-Serveradressen verwenden:
  - Bevorzugter DNS-Server: . . .
  - Alternativer DNS-Server: . . .
- □ Einstellungen beim Beenden überprüfen

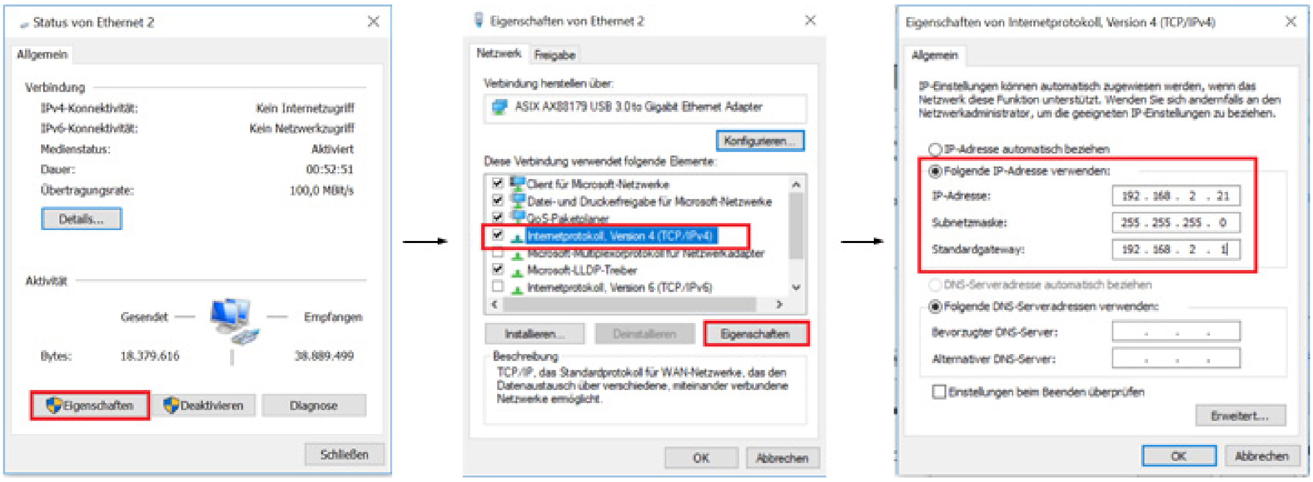
After configuring the IP address of the PC and connecting to the router, open a web browser.

Then enter „**http://192.168.2.1**" in the address bar of your browser (e. g. Google Chrome). After confirming with the „Enter" key, a pop-up window appears as 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 website. 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 mobile radio unit in the router. Alternatively, just open a webpage in your browser.

IP:	192.168.2.1
Username:	adm
Password:	123456

2.9.2. Manual configuration

Configure your PC to be located in the same subnet as the router (192.168.2.1). The subnet mask must be 255.255.255.0. The following figure shows the procedure for configuring the IP address on a PC with the Windows 10 operating system.



Status von Ethernet 2

Allgemein

Verbindung
IPv4-Konnektivität: Kein Internetzugriff
IPv6-Konnektivität: Kein Netzwerkzugriff
Medienstatus: Aktiviert
Dauer: 00:52:51
Übertragungsrate: 100,0 MBit/s

Aktivität
Gesendet — — Empfangen
Bytes: 18.379.616 38.889.499

Eigenschaften von Ethernet 2

Netzwerk | Freigabe

Verbindung herstellen über:
ASIX AX88179 USB 3.0 to Gigabit Ethernet Adapter

Diese Verbindung verwendet folgende Elemente:
- ☑ Client für Microsoft-Netzwerke
- ☑ Datei- und Druckerfreigabe für Microsoft-Netzwerke
- ☑ QoS-Paketplaner
- ☑ Internetprotokoll, Version 4 (TCP/IPv4)
- ☐ Microsoft-Multiplexorprotokoll für Netzwerkadapter
- ☑ Microsoft-LLDP-Treiber
- ☐ Internetprotokoll, Version 6 (TCP/IPv6)

Beschreibung
TCP/IP, das Standardprotokoll für WAN-Netzwerke, das den Datenaustausch über verschiedene, miteinander verbundene Netzwerke ermöglicht.

Eigenschaften von Internetprotokoll, Version 4 (TCP/IPv4)

Allgemein

IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.

○ IP-Adresse automatisch beziehen
● Folgende IP-Adresse verwenden:
IP-Adresse: 192 . 168 . 2 . 21
Subnetzmaske: 255 . 255 . 255 . 0
Standardgateway: 192 . 168 . 2 . 1

○ DNS-Serveradresse automatisch beziehen
● Folgende DNS-Serveradressen verwenden:
Bevorzugter DNS-Server: . . .
Alternativer DNS-Server: . . .

☐ Einstellungen beim Beenden überprüfen

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 bar of your browser. After confirming with the „Enter" key a pop-up window appears as 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 website. 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 mobile radio unit in the router. Alternatively, just open a webpage in your browser.

IP:	192.168.2.1
Username:	adm
Password:	123456

2.10.LED status lights

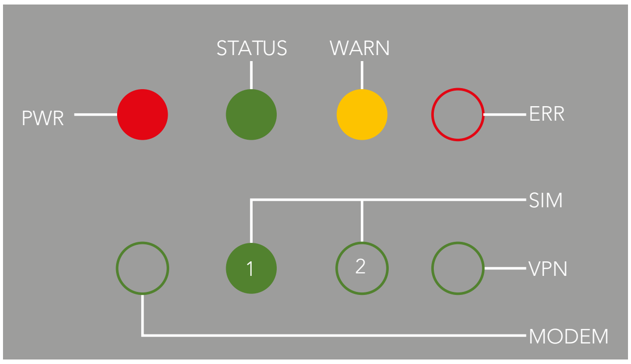
Explanation of symbols

● = LED on ○ = LED off ⚡ = LED flashing

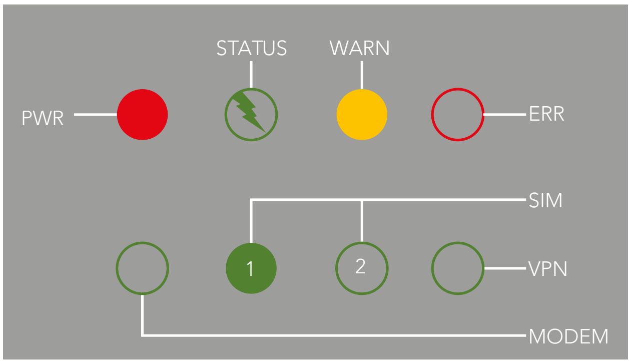
⚠ **Note**

There are two SIM card LEDs. When the router starts up, the SIM card LED for SIM card 1 lights up; in all other cases, the SIM card reception indicator lights up:

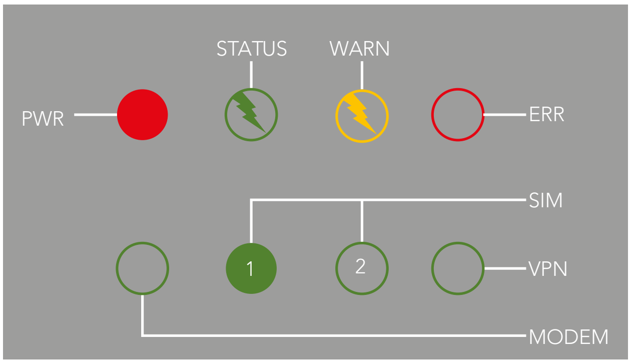
System start:



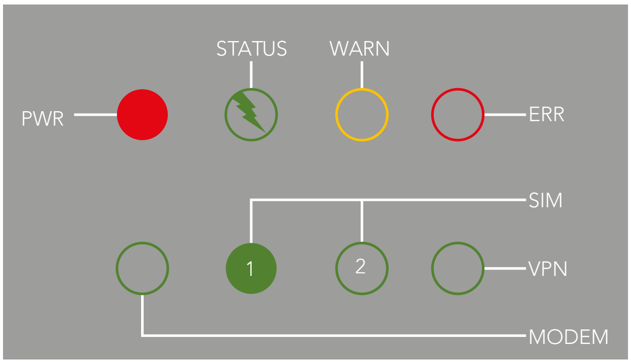
System start successful:



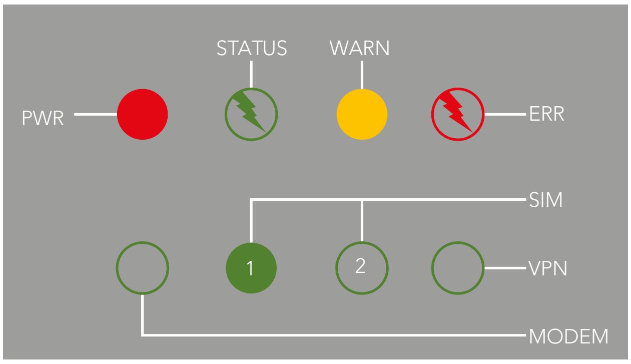
Dialing:



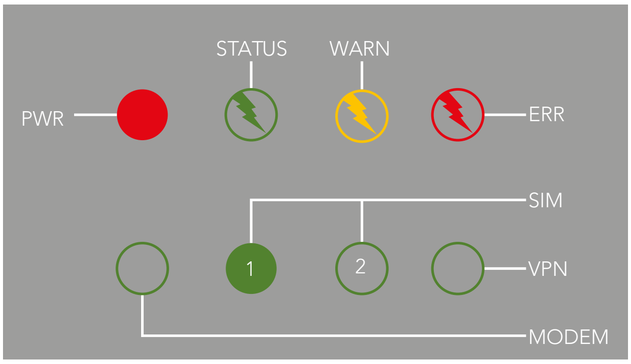
Dialing successful:



Reset successful:



Firmware update:



Signal strength

● ○ ○

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

● ● ○

Signal: 10-19
(router is operating normally)

● ● ●

Signal: 20-31
(perfect signal level)

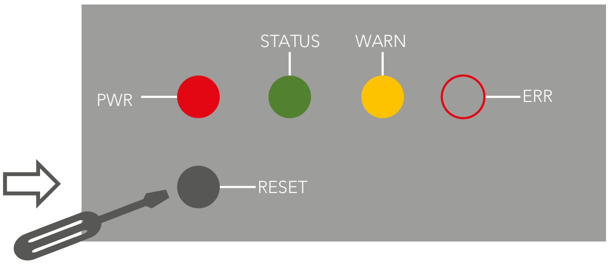
2.11.Resetting to factory settings

2.11.1. Hardware method

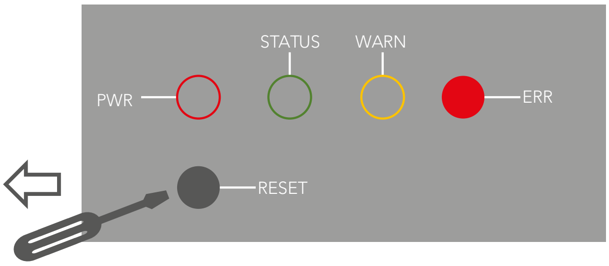
Explanation of symbols

● = LED on ○ = LED off ⚡ = LED flashing

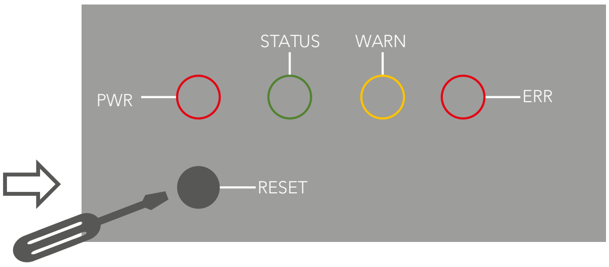
1) Press the RESET button while turning the TK800 on:



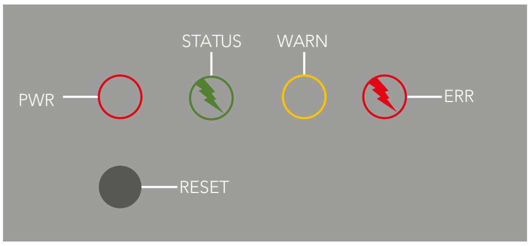
2) As soon as the ERROR LED lights up (approx. 10 seconds after switching on), release the RESET button:



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



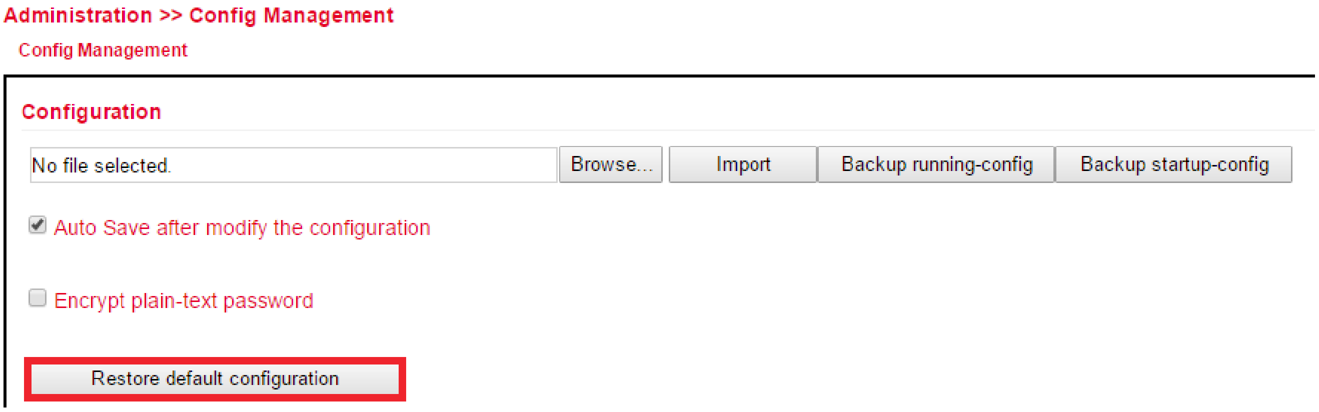
4) Now the LED lights ERROR and STATUS are flashing, which means that the reset to the default setting was successful.



Default factory settings	
IP:	192.168.2.1
Net mask:	255.255.255.0
Username:	adm
Password:	123456
Serial parameter:	115200-N-8-1

2.11.2. Web method

1) Via the **Administration** menu, go to the submenu **Config Management**:



Administration >> Config Management

Config Management

Configuration

☑ Auto Save after modify the configuration

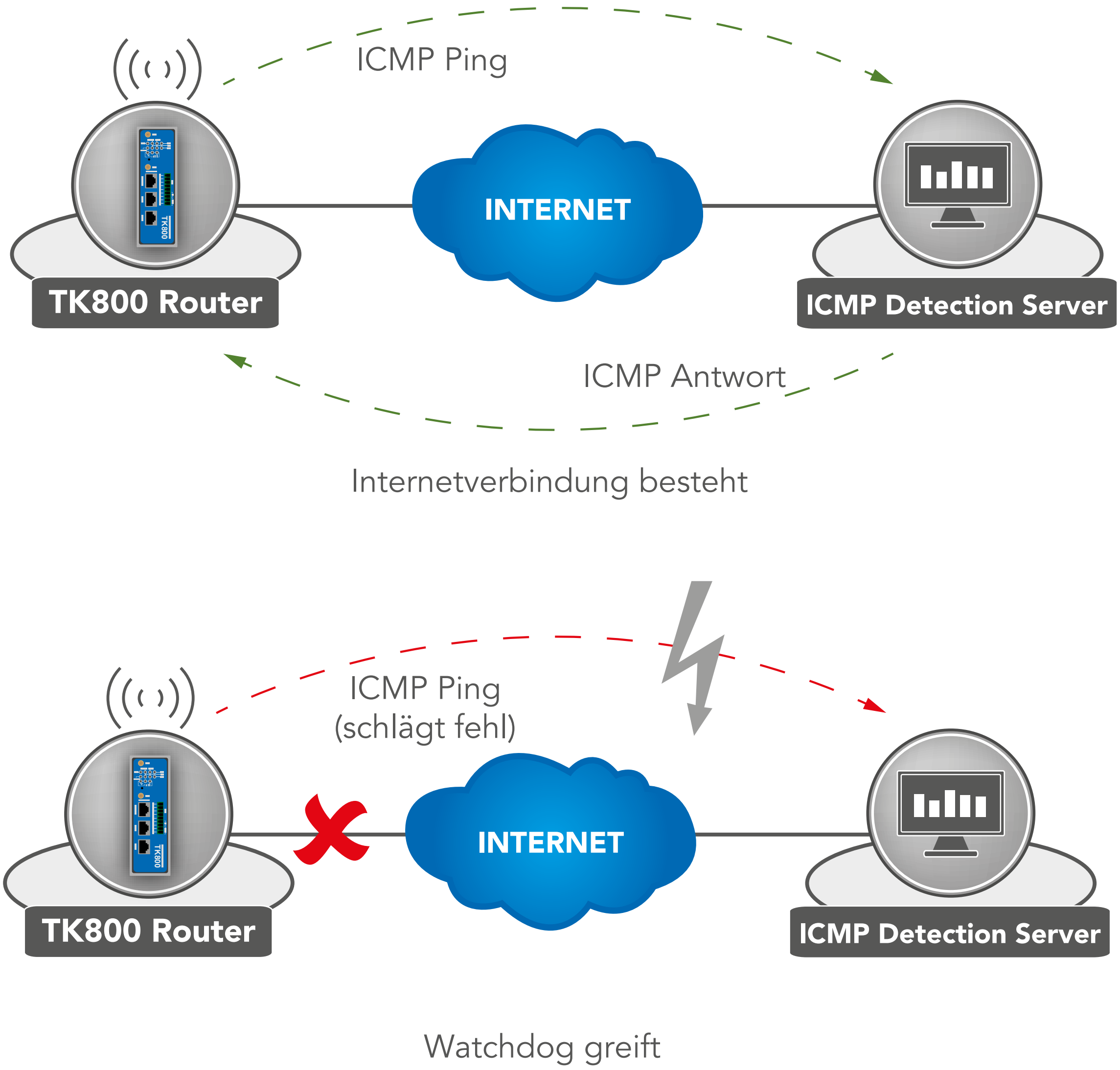
□ Encrypt plain-text password

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 is now successfully reset.

3) After a click on **reboot** the router restarts and is in factory settings.

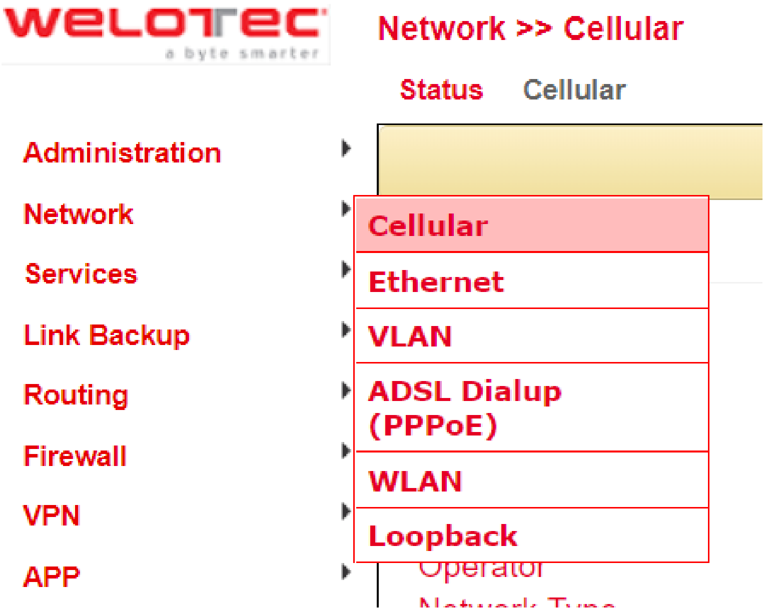
2.12.Watchdog

2.12.1. Automatic monitoring of the router

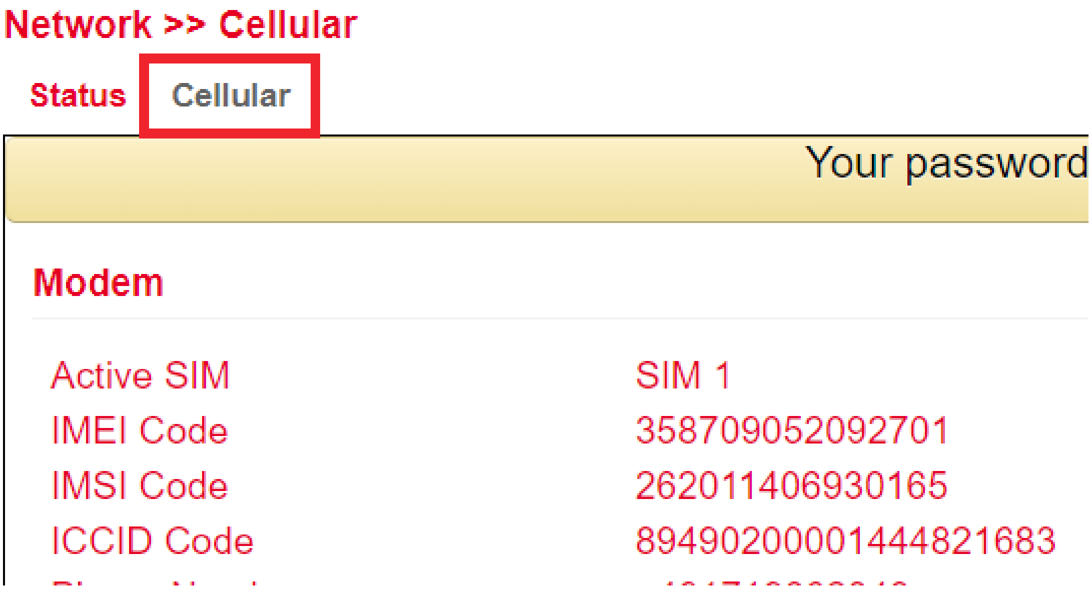


The watchdog monitors the router for Internet connection. The router itself checks whether an Internet connection is available as desired. For this, it sends ICMP packets to an individually defined server (ICMP detection server). If this query fails, the router will automatically restart the dial-up, then the modem, and if necessary the entire system. The watchdog provides a reliable internet connection in the mobile network. This ensures that the router is almost always reachable.

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



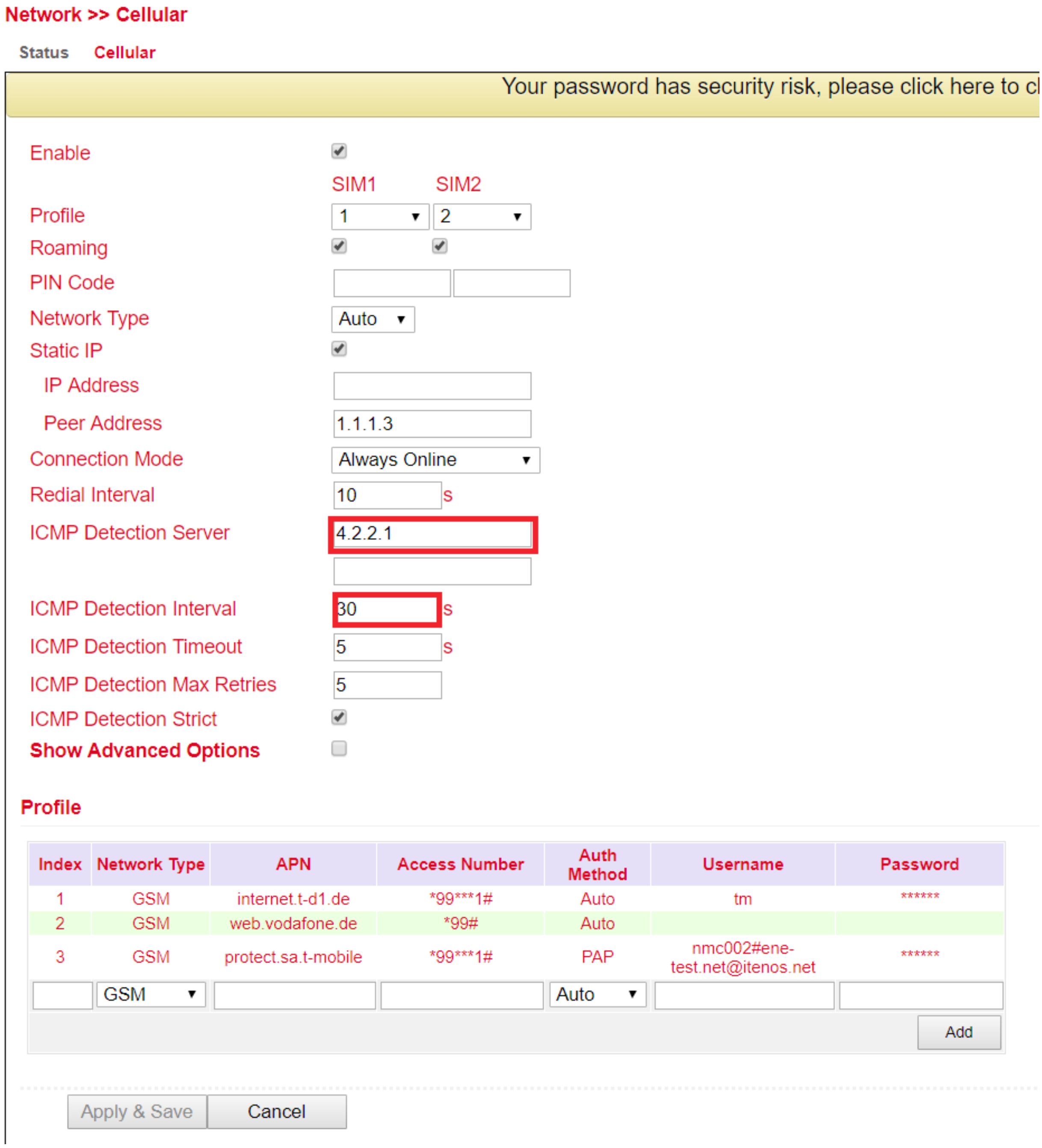
2) Select the **Cellular** tab



Modem

Active SIM	SIM 1
IMEI Code	358709052092701
IMSI Code	262011406930165
ICCID Code	89490200001444821683

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



Network >> Cellular

Status Cellular

Your password has security risk, please click here to cl

Enable	☑	
	SIM1	SIM2
Profile	1 ▾	2 ▾
Roaming	☑	☑
PIN Code		
Network Type	Auto ▾	
Static IP	☑	
IP Address		
Peer Address	1.1.1.3	
Connection Mode	Always Online ▾	
Redial Interval	10 s	
ICMP Detection Server	4.2.2.1	
ICMP Detection Interval	30 s	
ICMP Detection Timeout	5 s	
ICMP Detection Max Retries	5	
ICMP Detection Strict	☑	
Show Advanced Options	□	

Profile

Index	Network Type	APN	Access Number	Auth Method	Username	Password
1	GSM	internet.t-d1.de	*99***1#	Auto	tm	******
2	GSM	web.vodafone.de	*99#	Auto		
3	GSM	protect.sa.t-mobile	*99***1#	PAP	nmc002#ene-test.net@itenos.net	******
	GSM ▾			Auto ▾		

Note: The registered ICMP detection server should have a very high availability. A Google server is no longer suitable for this because ICMP requests are blocked there.

2.13.Port Mapping / Port Forwarding

2.13.1. Access to connected devices via the Internet

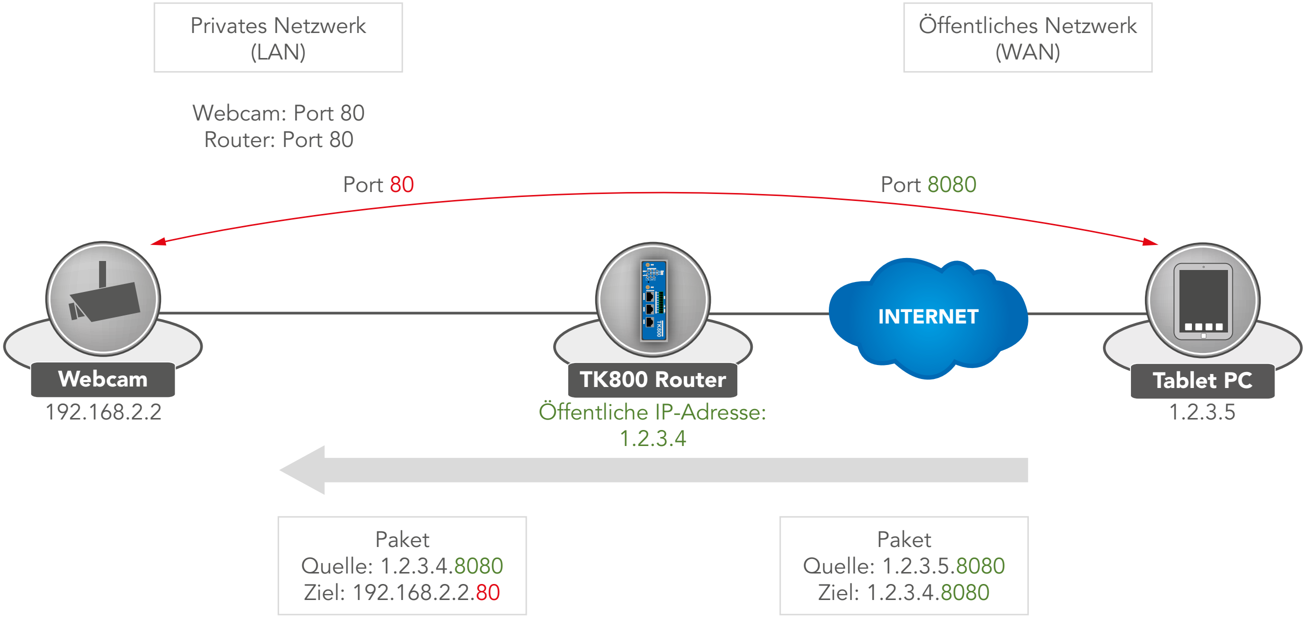
To access devices connected to the Welotec router via the Internet, you can use port mapping or port forwarding. This is configured in the TK800 router via NAT rules.

⚠ **Note**

Port mapping requires a public IP address in the mobile network (Public IP). Ask your mobile operator or service provider for more information!

This manual applies to all TK800 routers with firmware **1.0.0.r9338** or higher.

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



Explanation:

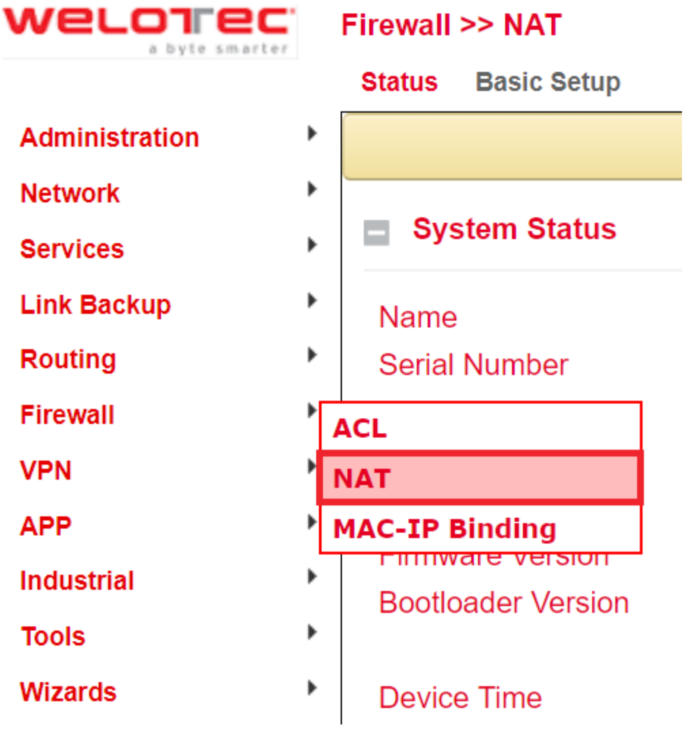
Welotec Router	
LAN IP address:	192.168.2.1
Subnet mask:	255.255.255.0

IP Camera	
LAN IP address:	192.168.2.2
Subnet mask:	255.255.255.0
Standard Gateway	192.168.1.1

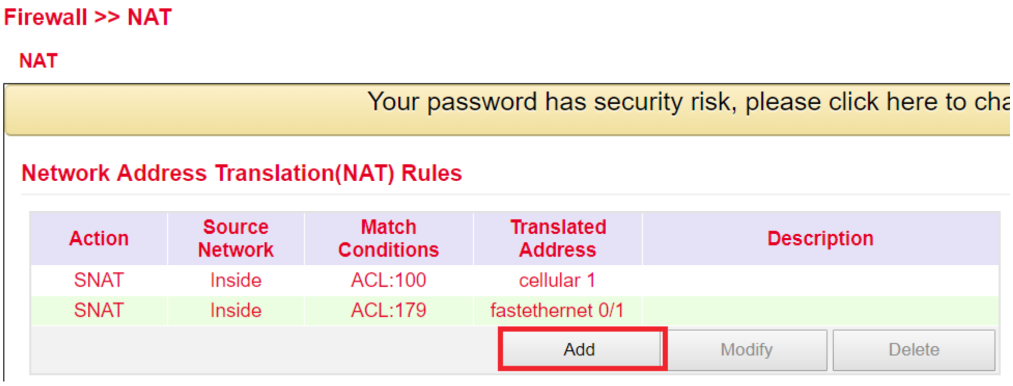
The IP camera has an interface that can be accessed with a browser via **http://192.168.2.2** (Note: http protocol has TCP port 80).

2.13.2. Instructions for port mapping

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



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


Firewall >> NAT

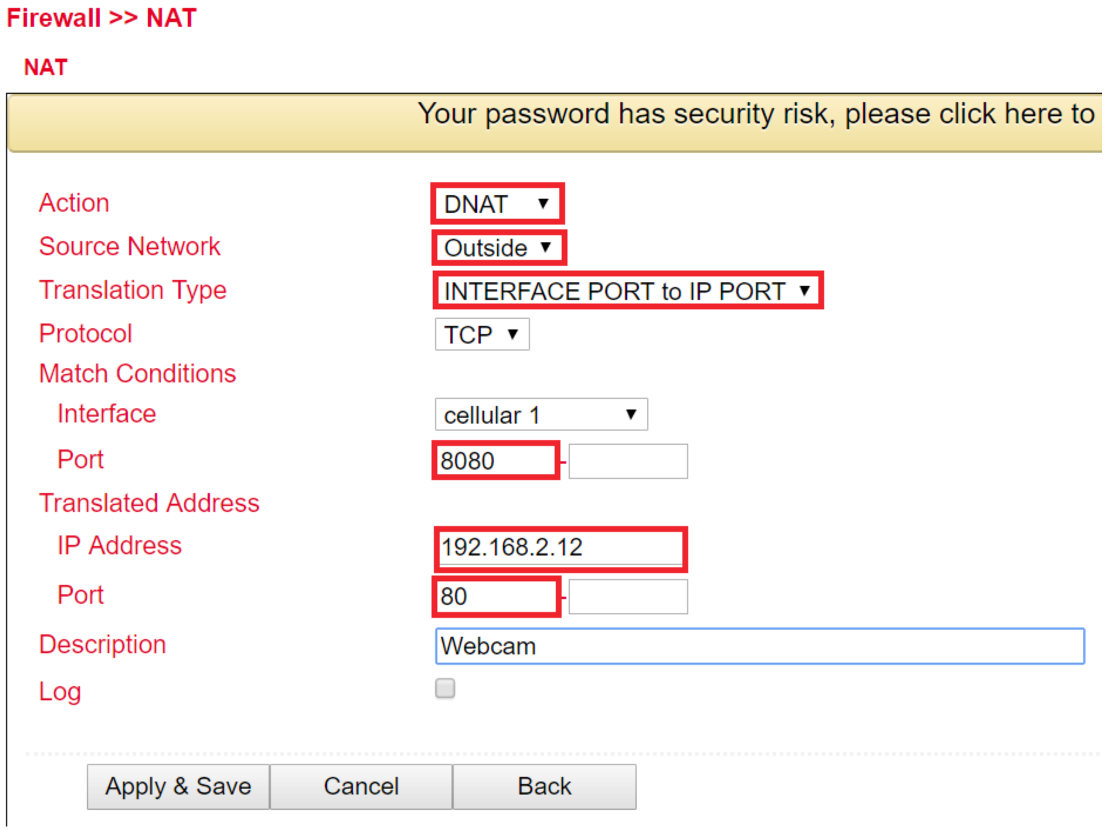
NAT

Your password has security risk, please click here to cha

Network Address Translation(NAT) Rules

Action	Source Network	Match Conditions	Translated Address	Description
SNAT	Inside	ACL:100	cellular 1	
SNAT	Inside	ACL:179	fastethernet 0/1	

3) Enter the data as in the example



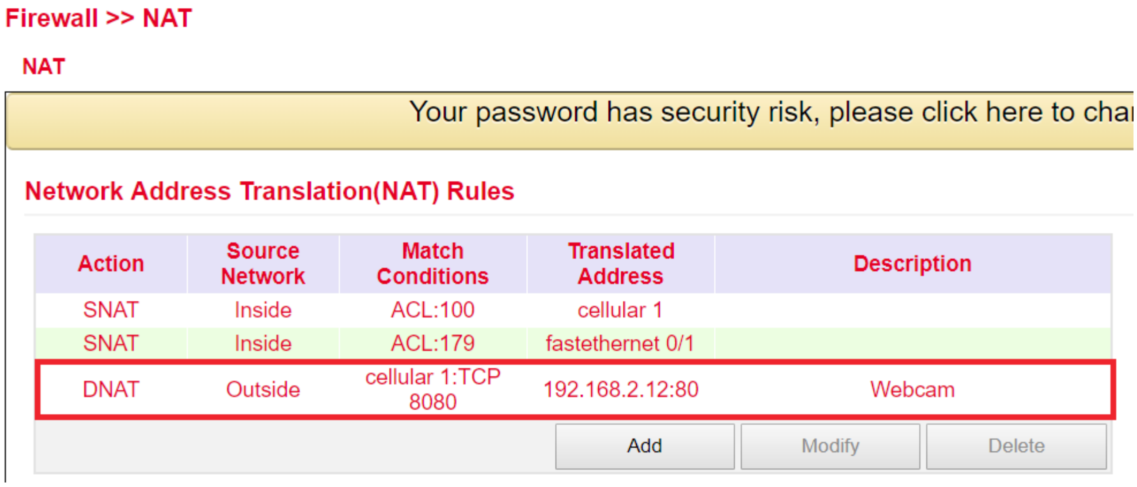
Firewall >> NAT

NAT

Your password has security risk, please click here to

Action	DNAT ▾
Source Network	Outside ▾
Translation Type	INTERFACE PORT to IP PORT ▾
Protocol	TCP ▾
Match Conditions	
Interface	cellular 1 ▾
Port	8080 -
Translated Address	
IP Address	192.168.2.12
Port	80 -
Description	Webcam
Log	□

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



Firewall >> NAT

NAT

Your password has security risk, please click here to cha

Network Address Translation(NAT) Rules

Action	Source Network	Match Conditions	Translated Address	Description
SNAT	Inside	ACL:100	cellular 1	
SNAT	Inside	ACL:179	fastethernet 0/1	
DNAT	Outside	cellular 1:TCP 8080	192.168.2.12:80	Webcam

The rule is now active. The corresponding services restart and the port mapping is completely configured.
For a working port mapping it is helpful to check the settings of the connected devices beforehand. The following checklist is helpful (like the above example):

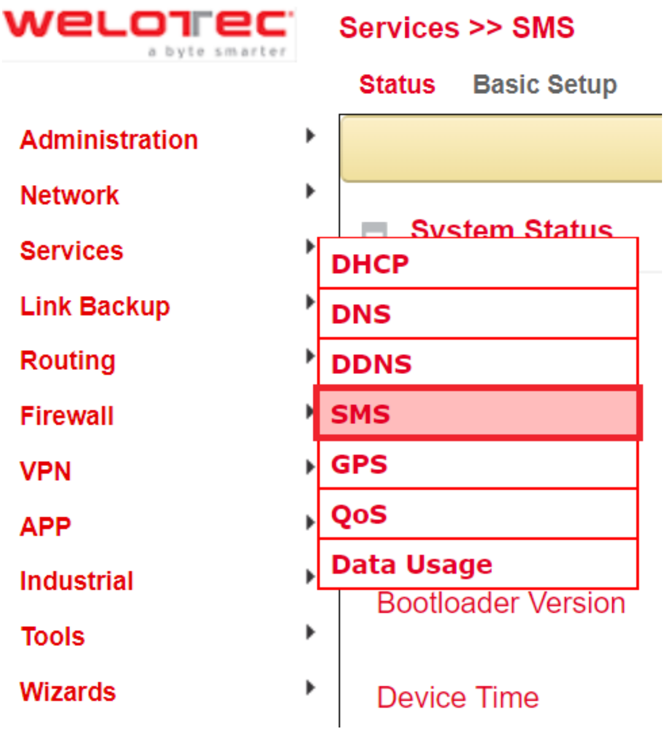
- Does the camera have the IP address 192.168.2.2?
- Does it answer with „ping 192.168.2.2"?
- Is the web interface of the camera accessible via **http://192.168.2.2**?
- Is the Welotec router registered as the default gateway for the camera (192.168.2.1)?

2.14.SMS functions

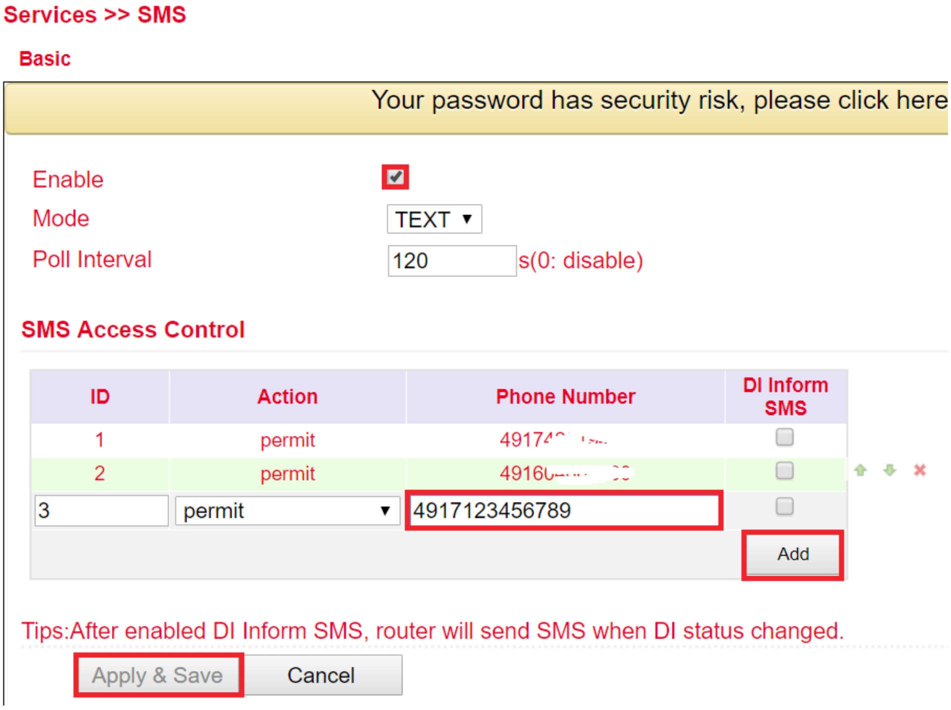
The TK800 can be accessed via SMS from the outside and reacts to various commands sent by SMS. You can check the status of the device, start / stop dial-up or restart the device.

2.14.1. Status query / restart

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



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


Services >> SMS

Basic

Your password has security risk, please click here

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

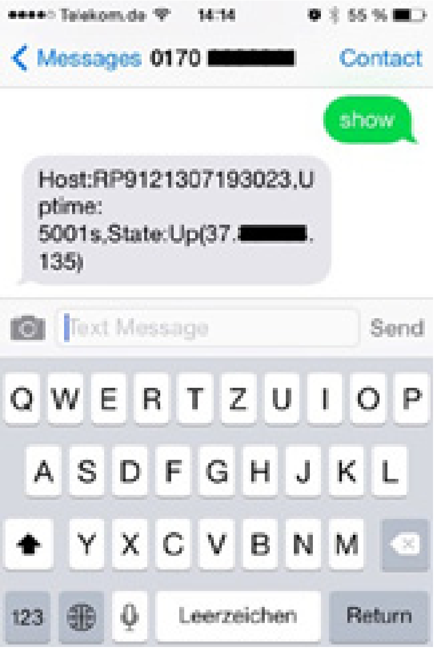
SMS Access Control

ID	Action	Phone Number	DI Inform SMS
1	permit	4917[redacted]	□
2	permit	4916[redacted]	□
3	permit ▾	4917123456789	□
			Add

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

Apply & Save   Cancel

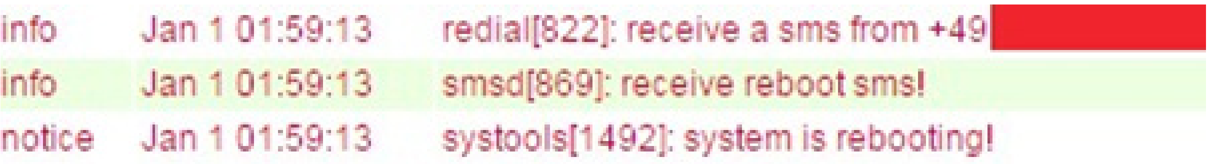
3) In the **SMS Access Control** table, enter the phone numbers (Phone Number) (format 4917123456789, not 0049 or +49!) that may send SMS messages to the router. Enter „**permit**" as action.
If an SMS with the content **show** is now sent to the router's mobile phone number, the router sends its current status as an answer.



show

Host:RP9121307193023,Uptime:
5001s,State:Up(37.[redacted].135)

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



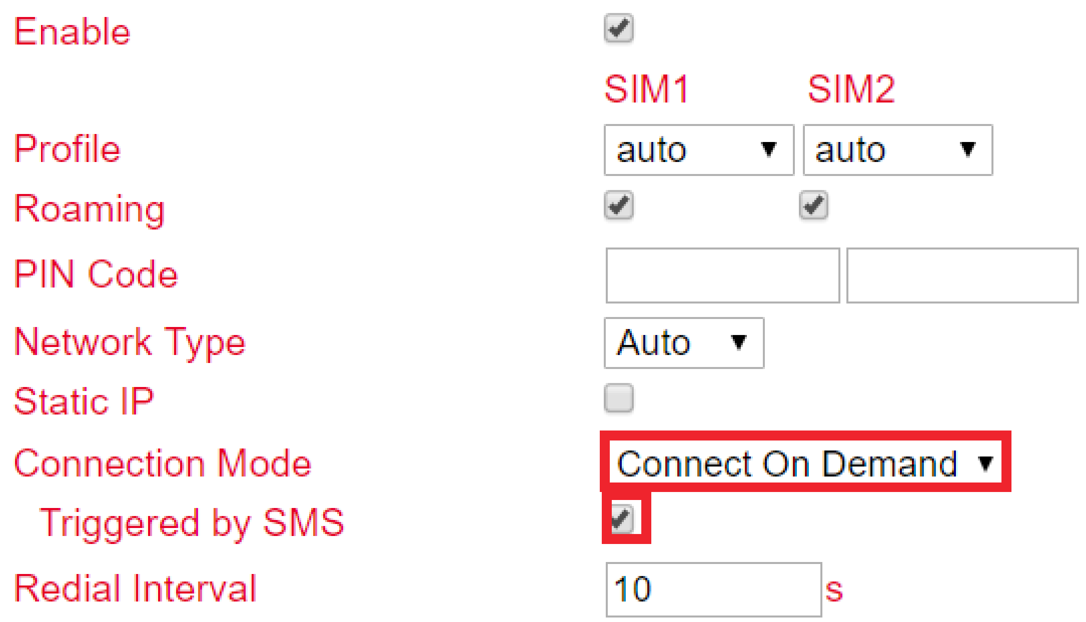
```
info     Jan 1 01:59:13     redial[822]: receive a sms from +49[redacted]
info     Jan 1 01:59:13     smsd[869]: receive reboot sms!
notice   Jan 1 01:59:13     systools[1492]: system is rebooting!
```

2.14.2. Establishing or disconnecting the Internet connection

After successful configuration, you can also control the router's Internet connection via SMS. For this, however, it is necessary that the router is set to „Connect On Demand"!

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

2) Now select the tab **Cellular**

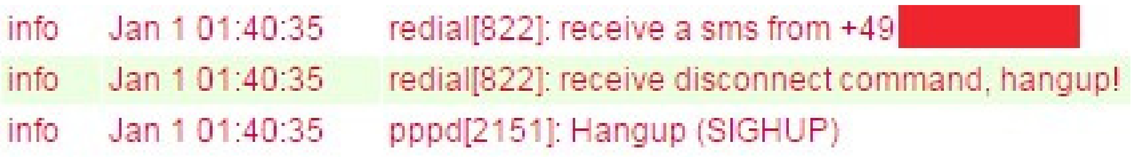


	SIM1	SIM2
Enable	☑	
Profile	auto ▼	auto ▼
Roaming	☑	☑
PIN Code		
Network Type	Auto ▼	
Static IP	□	
Connection Mode	Connect On Demand ▼	
Triggered by SMS	☑	
Redial Interval	10 s	

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

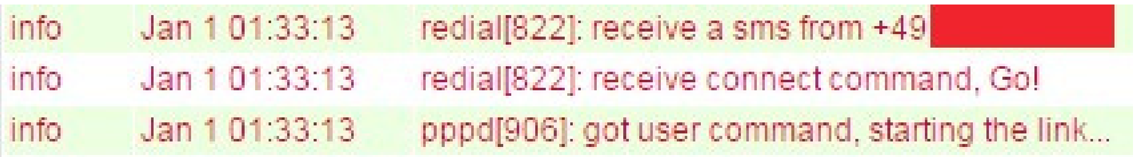
Now you can send the following commands via SMS to the router:

- **cellular 1 ppp down** - disconnects the internet connection



```
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)
```

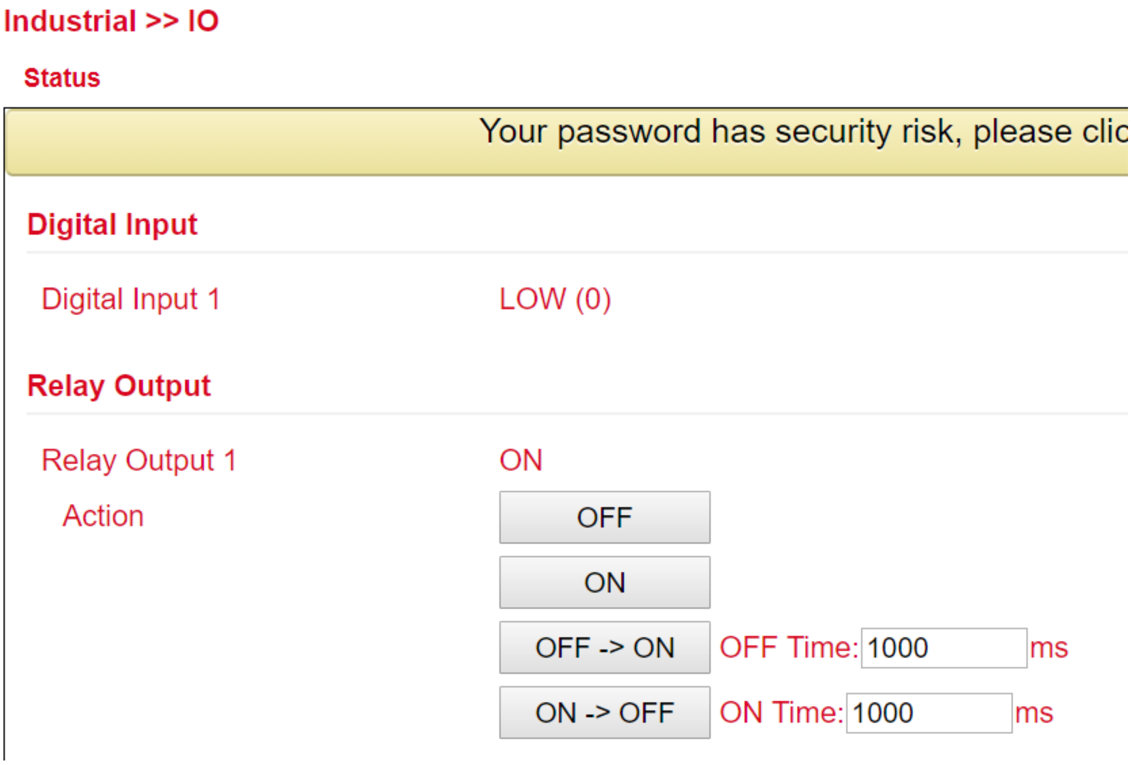
- **cellular 1 ppp up** - establishes internet connection



```
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...
```

2.14.3. Switching digital relay on or off

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



Industrial >> IO

Status

Your password has security risk, please clic

Digital Input

Digital Input 1 LOW (0)

Relay Output

Relay Output 1 ON

Action

OFF

ON

OFF -> ON OFF Time: 1000 ms

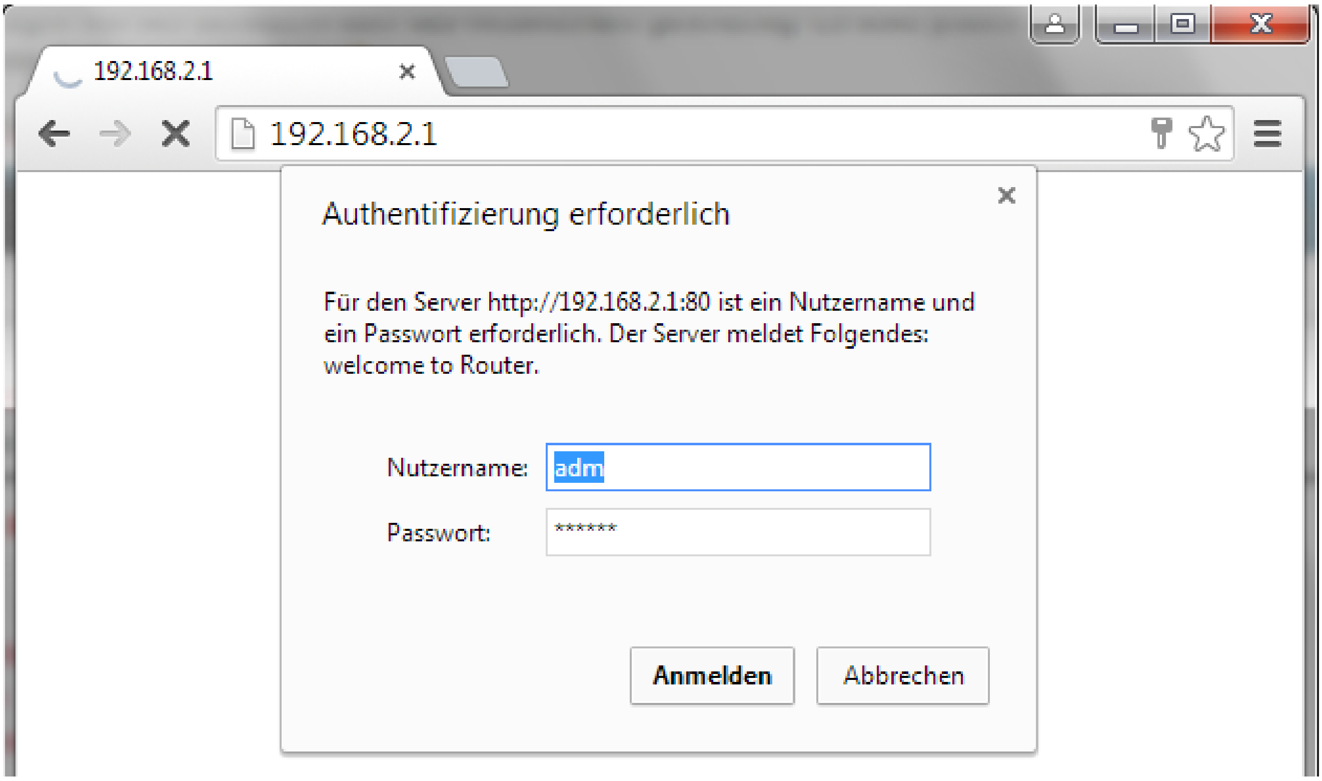
ON -> OFF ON Time: 1000 ms

The following SMS commands can be used for this purpose

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

3. WEB CONFIGURATION

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



Authentifizierung erforderlich

Für den Server http://192.168.2.1:80 ist ein Nutzername und ein Passwort erforderlich. Der Server meldet Folgendes: welcome to Router.

Nutzername: adm

Passwort: ******

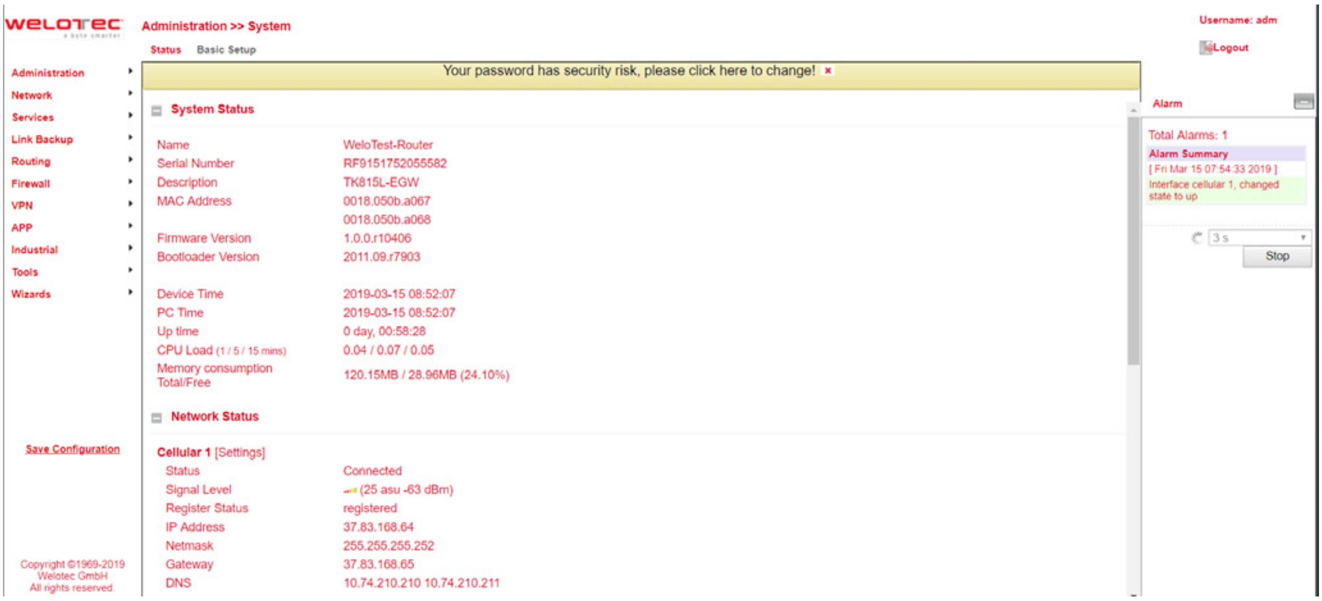
⚠ Note

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.

Hint

The router allows parallel access for up to four users via the web interface. However, you should avoid working on the router configuration at the same time.

After successful login, the router's web interface appears.



Your password has security risk, please click here to change! ×

System Status

Name	WeloTest-Router
Serial Number	RF9151752055582
Description	TK815L-EGW
MAC Address	0018.050b.a067 0018.050b.a068
Firmware Version	1.0.0.r10406
Bootloader Version	2011.09.r7903
Device Time	2019-03-15 08:52:07
PC Time	2019-03-15 08:52:07
Up time	0 day, 00:58:28
CPU Load (1 / 5 / 15 mins)	0.04 / 0.07 / 0.05
Memory consumption Total/Free	120.15MB / 28.96MB (24.10%)

Network Status

Cellular 1 [Settings]

Status	Connected
Signal Level	(25 asu -63 dBm)
Register Status	registered
IP Address	37.83.168.64
Netmask	255.255.255.252
Gateway	37.83.168.65
DNS	10.74.210.210 10.74.210.211

Total Alarms: 1

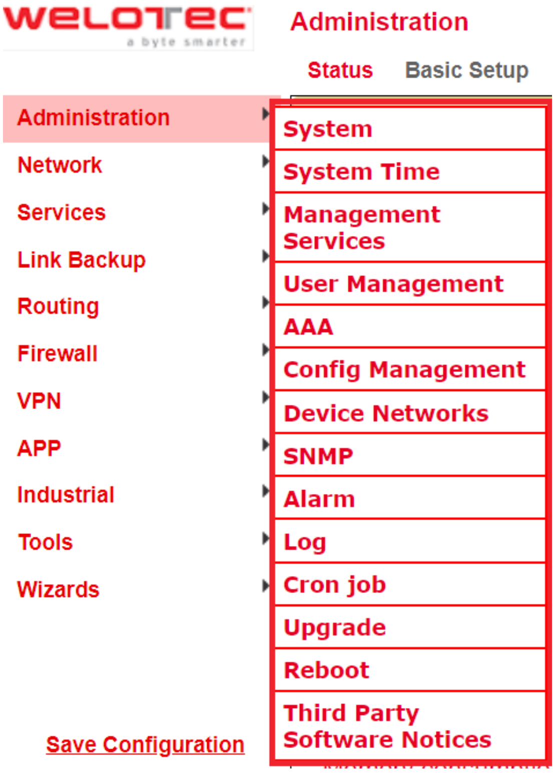
Alarm Summary

[Fri Mar 15 07:54:33 2019]:
Interface cellular 1, changed state to up

The web interface of the TK800 is divided into 4 sections. On the left side is the **main navigation** with the items Administration, Network etc. In the upper area is the **detailed navigation**. In this example with status (active) and basic setup. The current status and configuration options are displayed in the middle of the web interface. On the right side active alarms are displayed.

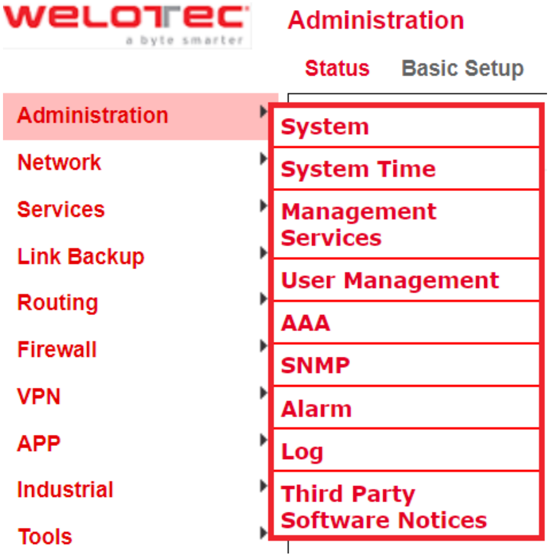
3.1. Administration

The menu item „**Administration**" is located on the left-hand side. Touching with the mouse opens a **submenu**. The administration area contains the status overview and the configuration for managing the router.



Note

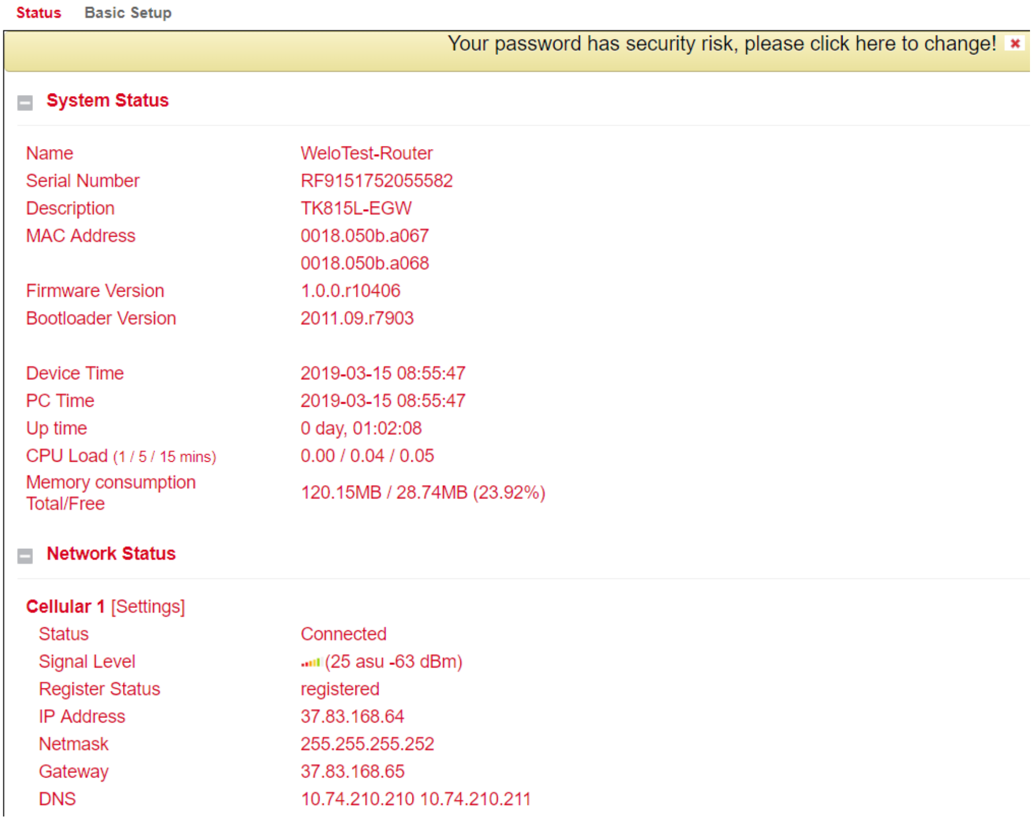
For restricted user rights (not administrator) some items are missing in the menu. Limited users cannot configure the router, the **Apply & Save** option is missing.



3.1.1. System

3.1.1.1. Status

Under **Administration > System > Status**, you can find the router's most important **status information** at a glance. With 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 appear indicating 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!



Your password has security risk, please click here to change! ×

⊟ System Status

Name WeloTest-Router
Serial Number RF9151752055582
Description TK815L-EGW
MAC Address 0018.050b.a067
0018.050b.a068
Firmware Version 1.0.0.r10406
Bootloader Version 2011.09.r7903

Device Time 2019-03-15 08:55:47
PC Time 2019-03-15 08:55:47
Up time 0 day, 01:02:08
CPU Load (1 / 5 / 15 mins) 0.00 / 0.04 / 0.05
Memory consumption Total/Free 120.15MB / 28.74MB (23.92%)

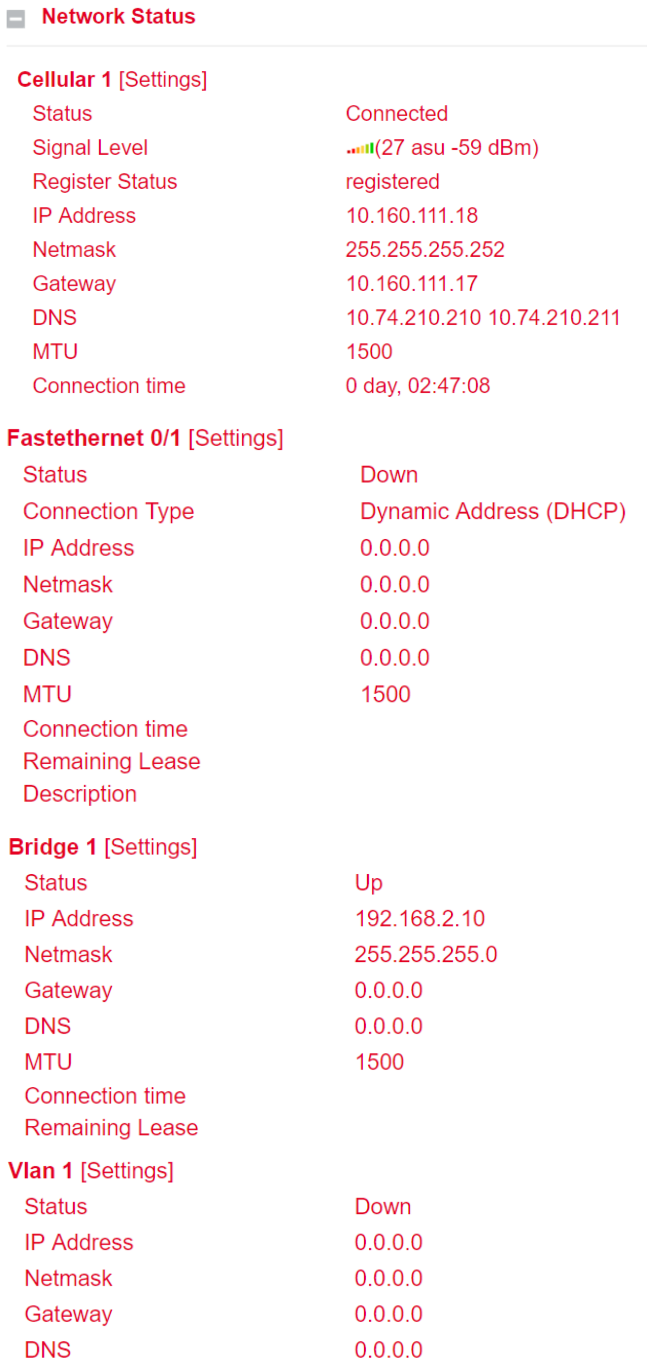
⊟ Network Status

Cellular 1 [Settings]
Status Connected
Signal Level (25 asu -63 dBm)
Register Status registered
IP Address 37.83.168.64
Netmask 255.255.255.252
Gateway 37.83.168.65
DNS 10.74.210.210 10.74.210.211

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

Hint

Click on **[Settings]** next to the individual interfaces (e. g. Cellular 1) to go directly to the configuration of the interfaces.



Network Status

Cellular 1 [Settings]

Status	Connected
Signal Level	(27 asu -59 dBm)
Register Status	registered
IP Address	10.160.111.18
Netmask	255.255.255.252
Gateway	10.160.111.17
DNS	10.74.210.210 10.74.210.211
MTU	1500
Connection time	0 day, 02:47:08

Fastethernet 0/1 [Settings]

Status	Down
Connection Type	Dynamic Address (DHCP)
IP Address	0.0.0.0
Netmask	0.0.0.0
Gateway	0.0.0.0
DNS	0.0.0.0
MTU	1500
Connection time	
Remaining Lease	
Description	

Bridge 1 [Settings]

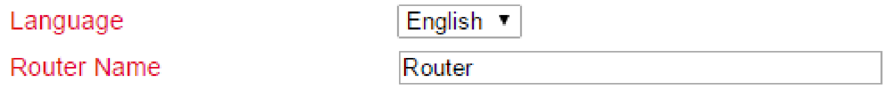
Status	Up
IP Address	192.168.2.10
Netmask	255.255.255.0
Gateway	0.0.0.0
DNS	0.0.0.0
MTU	1500
Connection time	
Remaining Lease	

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 adjust the language of the router and the router name. Currently only English is supported as language. The router name can be used as the unique name of the router. A meaningful name should be chosen here.



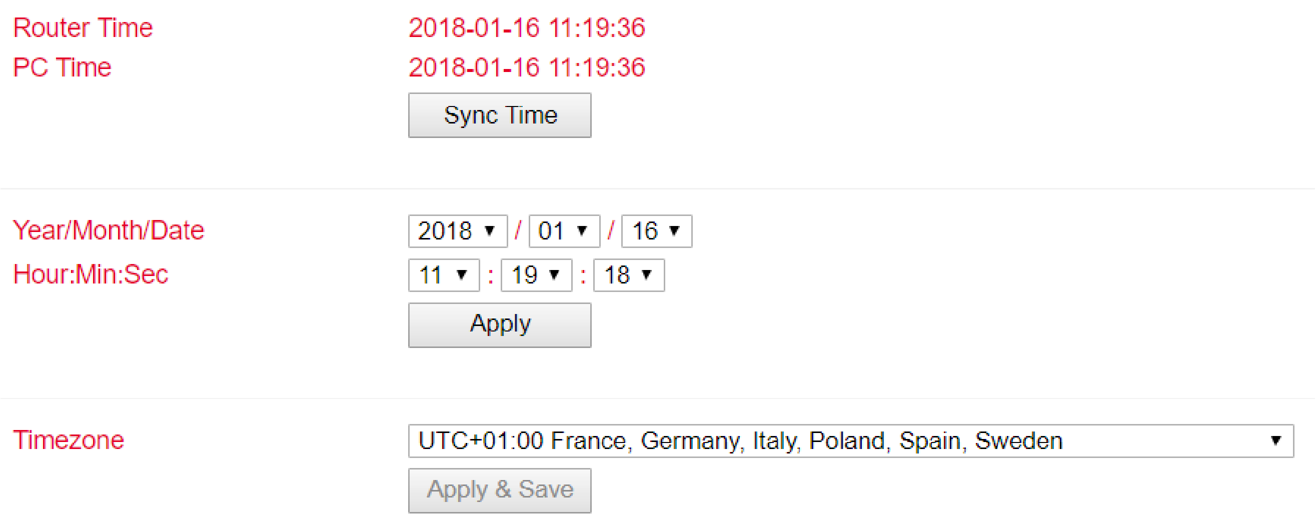
Language	English ▼
Router Name	Router

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 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, devices connected to the router via the NTP server can be automatically supplied with the current time information.

3.1.2.1. System Time Configuration

Under **Administration > System Time** you will find an overview and local settings for the router's system time. **Sync Time** allows you to synchronize the router's time with the PC's time.
The settings also include the possibility of setting the router's time and date manually. Under **Timezone** you can select the current time zone. The default is UTC+1 (time zone in Germany, Austria and Switzerland).



Router Time 2018-01-16 11:19:36
PC Time 2018-01-16 11:19:36

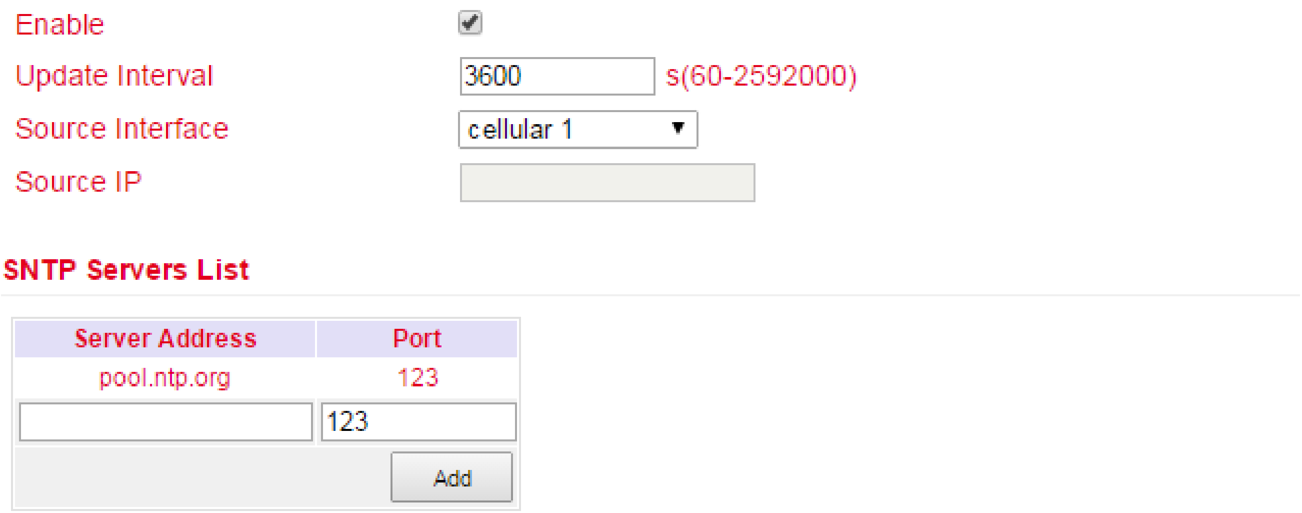
Year/Month/Date 2018 ▾ / 01 ▾ / 16 ▾
Hour:Min:Sec 11 ▾ : 19 ▾ : 18 ▾

Timezone UTC+01:00 France, Germany, Italy, Poland, Spain, Sweden ▾

3.1.2.2. SNTP Client

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



Enable	☑
Update Interval	3600 s(60-2592000)
Source Interface	cellular 1 ▼
Source IP	

SNTP Servers List

Server Address	Port
pool.ntp.org	123
	123

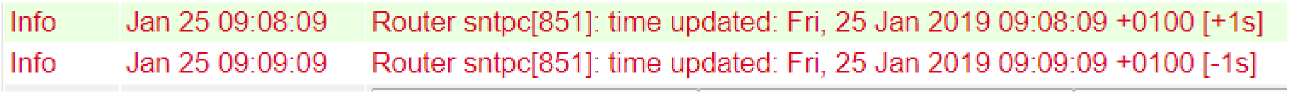
Note

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

Note

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**.



```
Info    Jan 25 09:08:09    Router sntpc[851]: time updated: Fri, 25 Jan 2019 09:08:09 +0100 [+1s]
Info    Jan 25 09:09:09    Router sntpc[851]: time updated: Fri, 25 Jan 2019 09:09:09 +0100 [-1s]
```

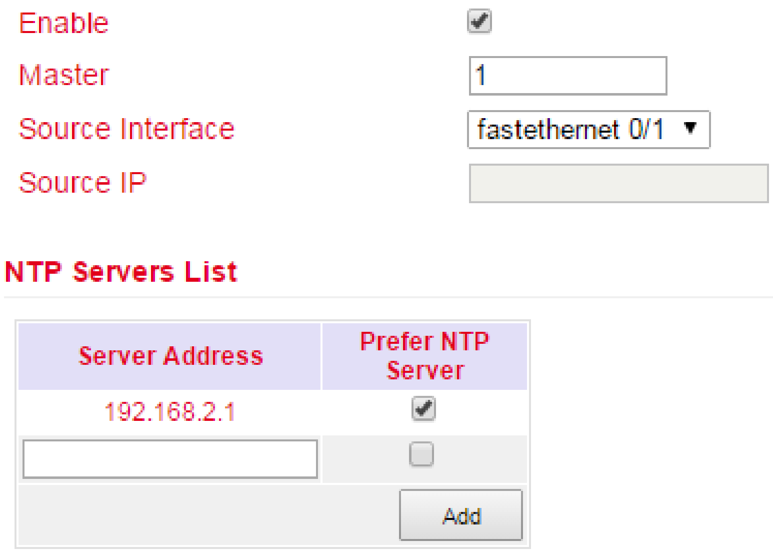
3.1.2.3. NTP Server

Under **Administration > System Time > NTP Server** you will find the settings for the time server. In this case, the TK800 can work as a time server for the connected devices.

The stratum can be specified via **Master**. This shows 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 at which interface the devices can request the NTP service of the router. Alternatively, a **Source IP** can be specified to provide the NTP service.

⚠ **Note**

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



Enable	☑
Master	1
Source Interface	fastethernet 0/1 ▼
Source IP	

NTP Servers List

Server Address	Prefer NTP Server
192.168.2.1	☑
	☐
	Add

3.1.3. Management Services

Under **Administration > Management Services**, you can configure access to the Web interface with HTTP and HTTPS as well as to the Command Line Interface (CLI) via Telnet and SSH.

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

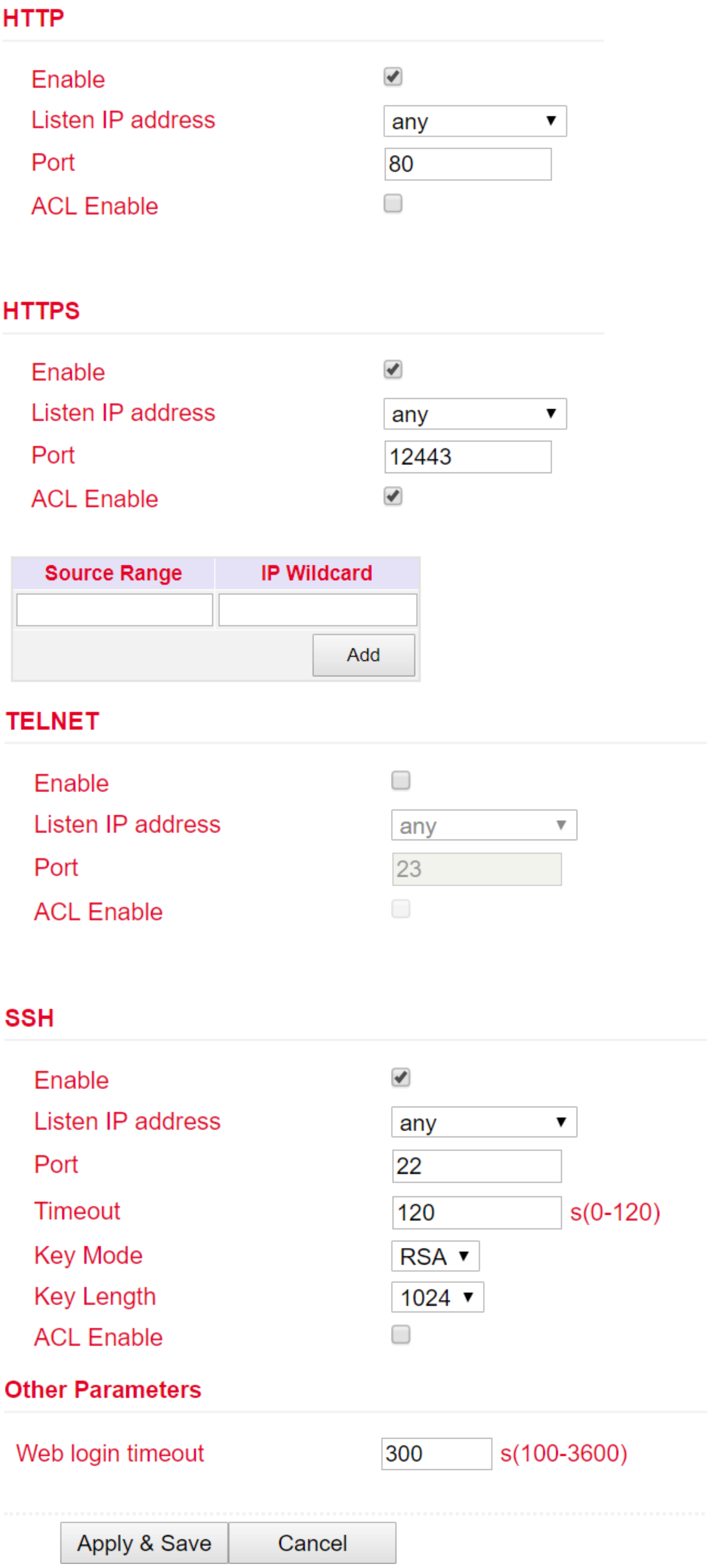
HTTPS
HTTPS is the abbreviation for Hypertext Tranfer Protocol Secure and uses SSL (Security Socket Layer) for the encrypted transmission of HTTP.

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.

Konfiguration
For each service, you can select whether it is to be activated or deactivated and on which IP this service may be addressed.

To do this, simply check or uncheck **Enable**. Under **Port** you can select the TCP port for the respective service. With **ACL Enable** you can set an access restriction 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 may 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 time, the connection will be terminated. Under **Key Mode** and **Key Length** the encryption standard and the key length can be selected.
With **Other Parameters** you can set the **Web login timeout**. This specifies how long a web interface session remains active if no entry is made.
If the timeout time has expired without you having made an entry, the logged-in user is automatically logged out.



HTTP

Enable	☑
Listen IP address	any ▼
Port	80
ACL Enable	□

HTTPS

Enable	☑
Listen IP address	any ▼
Port	12443
ACL Enable	☑

Source Range	IP Wildcard
	Add

TELNET

Enable	□
Listen IP address	any ▼
Port	23
ACL Enable	□

SSH

Enable	☑
Listen IP address	any ▼
Port	22
Timeout	120 s(0-120)
Key Mode	RSA ▼
Key Length	1024 ▼
ACL Enable	□

Other Parameters

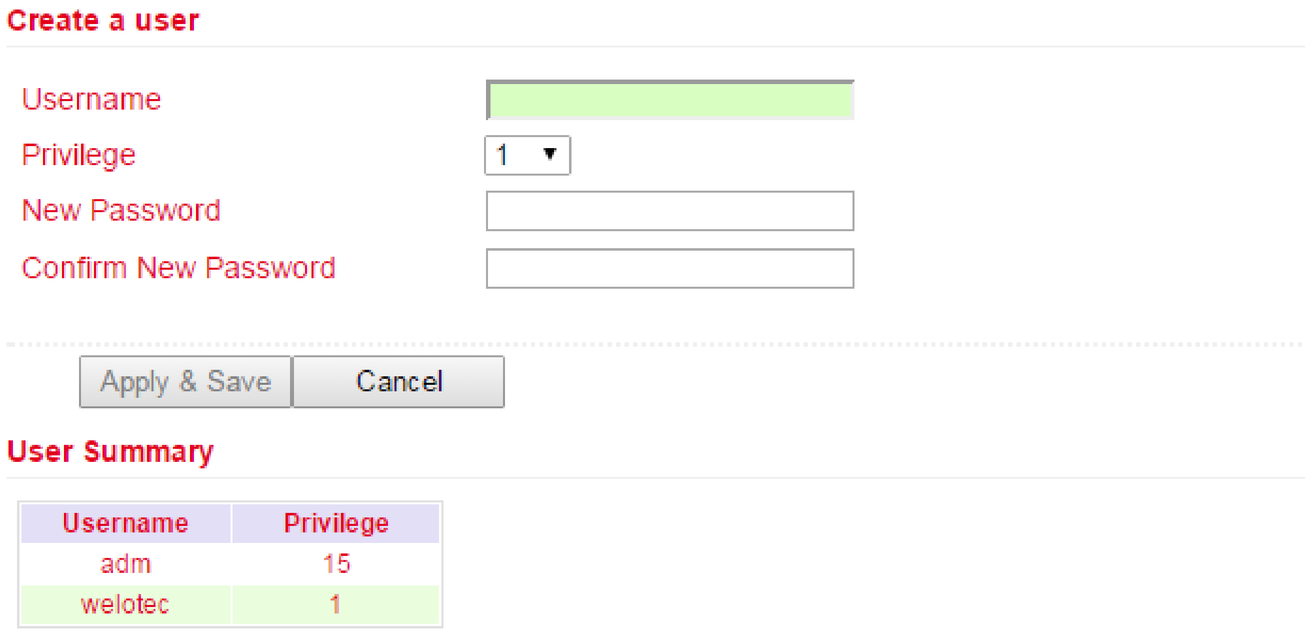
Web login timeout	300 s(100-3600)

3.1.4. User Management

Under **Administration > User Management**, users who 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 additional standard users with restricted rights.
The Administrator user is suitable for configuring and managing the router. The default user is suitable for monitoring and checking the router.

3.1.4.1. Create a User

You can create additional users under **Administration > User Management > Create a User**.
A **Username** and **Password** must be created and the **authorization (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 with all users and the corresponding rights (privilege).



Create a user

Username	
Privilege	1 ▼
New Password	
Confirm New Password	

User Summary

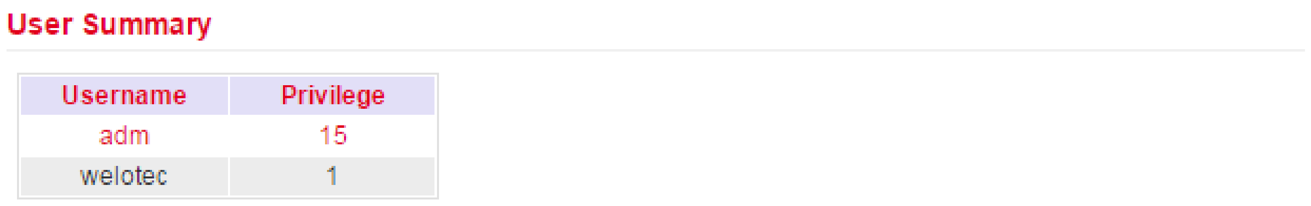
Username	Privilege
adm	15
welotec	1

⚠ **Note**

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.

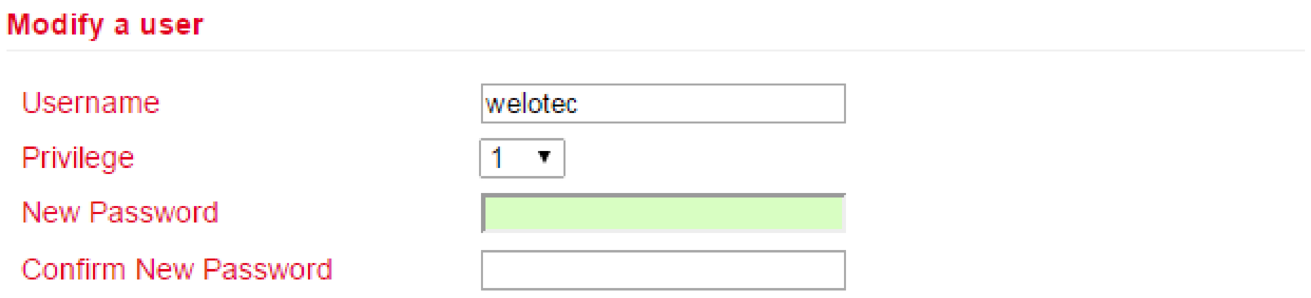
3.1.4.2. Modify a User

If you want to make adjustments to users, you can edit them under **Administration > User Management > Modify a User**. The permissions and passwords can be changed.
A user can be selected under **User Summary** and then edited under **Modify a User**.



User Summary

Username	Privilege
adm	15
welotec	1



Modify a user

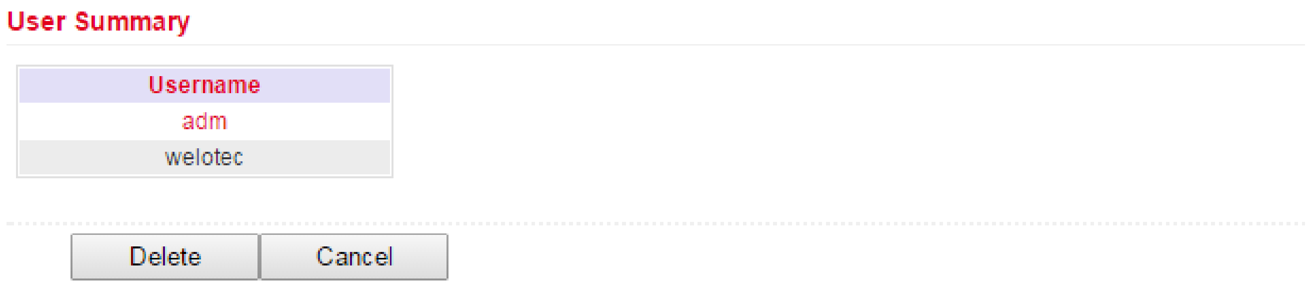
Username	welotec
Privilege	1 ▾
New Password	
Confirm New Password	

Note

If the user adm is selected, the user name can be changed from firmware version V1.0.0.r10406 onwards, e.g. in admin. Always remember to change the default password (123456) of the user adm to a secure password.

3.1.4.3. Remove Users

Under **Administration > User Management > Remove Users** you can delete users from the TK800. Under **User Summary**, select the user to be deleted and delete it using the **Delete Button**.



User Summary

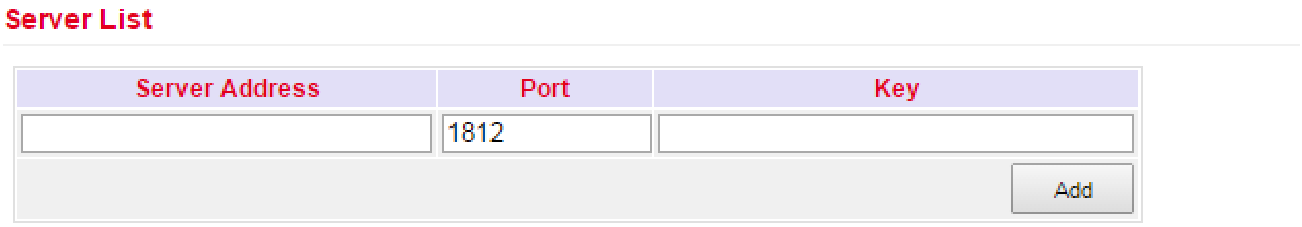
Username
adm
welotec

3.1.5. AAA

AAA or Triple-A stands for **Authentication**, **Authorization** and **Accounting**. Authentication takes over the access control, whether a user is allowed to use the device or the network. The authorization checks which services the user is allowed to use on the network. Billing ensures that all accesses and events and the use of resources in the network are logged correctly.
AAA does not require all security services to be used. It is also possible that only one or two services are used in a network. An AAA infrastructure is usually built as a client-server architecture. The TK800 acts here as an AAA client. Radius, Tacacs+ and LDAP are supported for this.

3.1.5.1. Radius

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



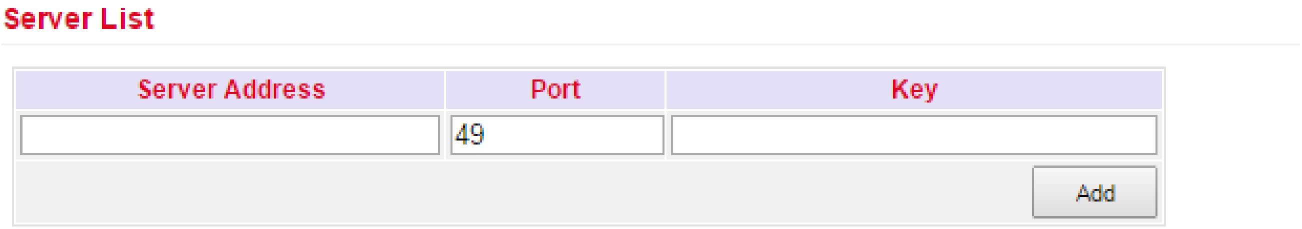
Server List

Server Address	Port	Key
	1812	

Here you can enter the FQDN or the IP address of the server, the port, the key for the Radius Server and the source interface.

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).



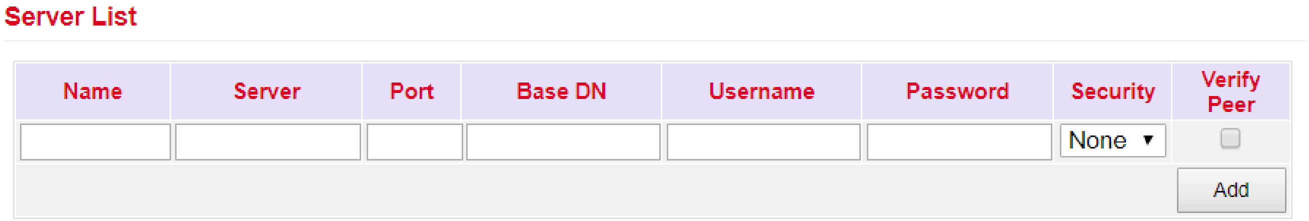
Server List

Server Address	Port	Key
	49	

You can enter the corresponding data for the **Server Adress**, **Port** and **Key** here.

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.

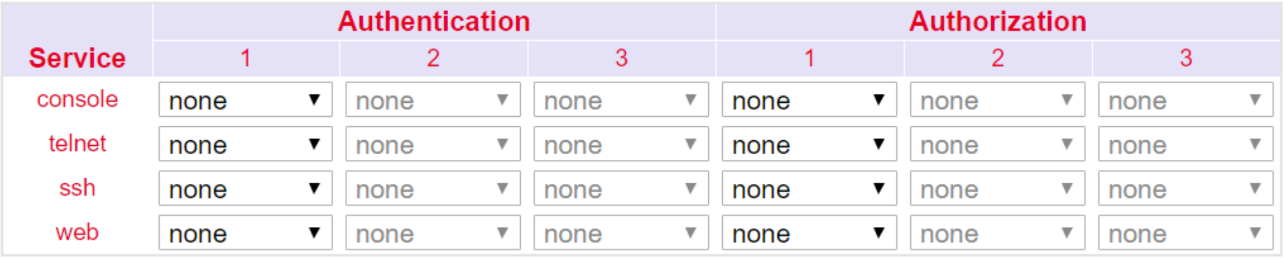


Server List

Name	Server	Port	Base DN	Username	Password	Security	Verify Peer
						None ▾	☐
							Add

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 ▾

3.1.6. 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 standard configuration.

Import of an existing configuration
To import an existing configuration you have to use **Browse...** an existing configuration file can be selected. Once the correct file has been selected, the configuration can be loaded into the router via **Import**. After successfully reading the configuration, the router offers a button for restarting. After restarting, the new configuration is in the router.

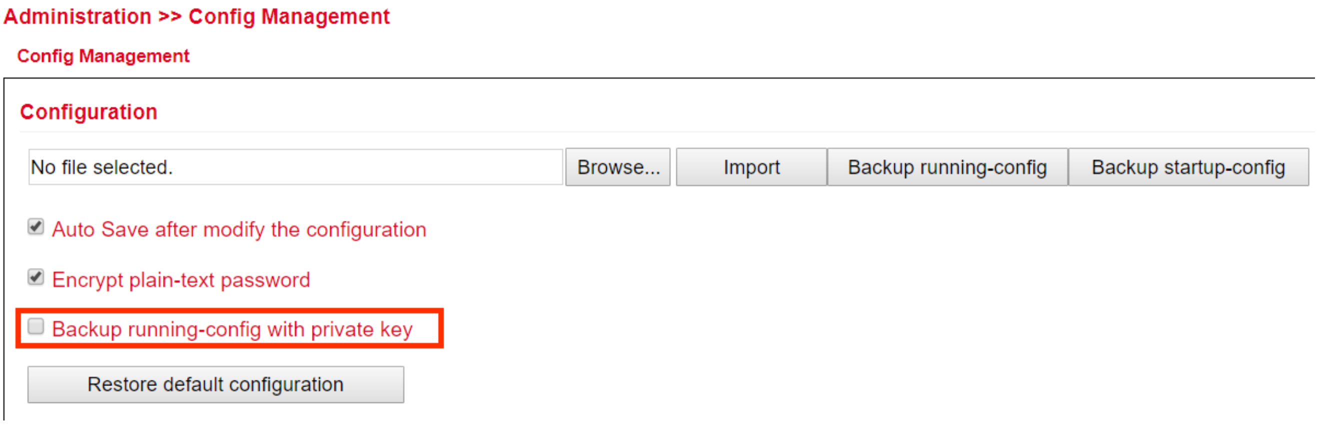
Saving an existing configuration
With **Backup running-config** you can download the current configuration including the unconfirmed changes during operation. With **Backup startup-config** the configuration can be downloaded without the unconfirmed changes.

Automatic saving
If the check mark in front of **Auto Save after modify the configuration** is set, all changes in the router become active immediately and are also available after the restart. If the checkbox is unchecked, the changes will be lost during restart. Alternatively, the changes can be saved via the lower menu item in the left navigation bar, **Save Configuration**.

Reset configuration to factory settings
Restore default configuration can be used to reset the router's configuration to its default settings.

Encrypt passwords in the configuration file
To avoid displaying passwords in plain text in the configuration file, check the **Encrypt plain-text password** box.

Saving the running-config including the private key
To additionally save the running-config with the imported private keys from the certificate administration, check the box **Backup running-config with private key.**



Administration >> Config Management

Config Management

Configuration

No file selected.

☑ Auto Save after modify the configuration

☑ Encrypt plain-text password

☐ Backup running-config with private key

3.1.7. Device Networks

⚠ **Note**

This function is not supported!

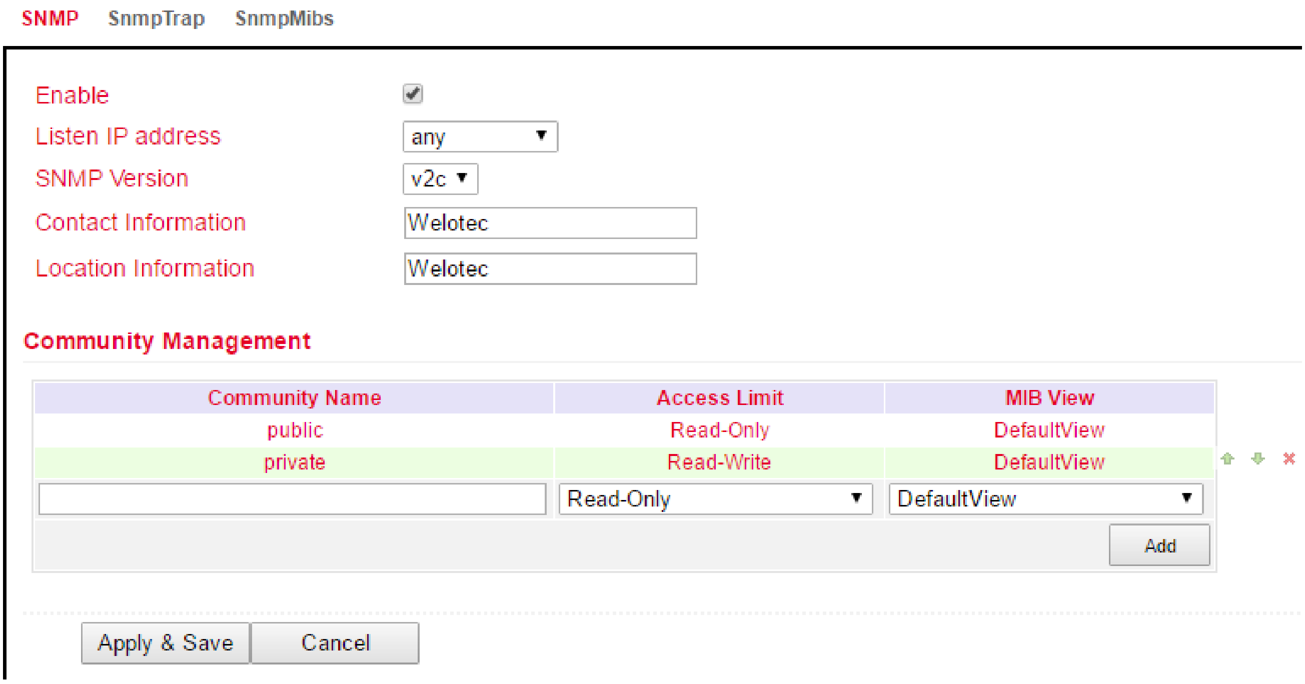
3.1.8. SNMP

The Simple Network Management Protocol (SNMP) is a network protocol developed by 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 process. It was designed in such a way that every network-enabled 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 **read-only** and **read-write** authentication. Under **Listen IP address** you can select the IP address under which the SNMP service is available.

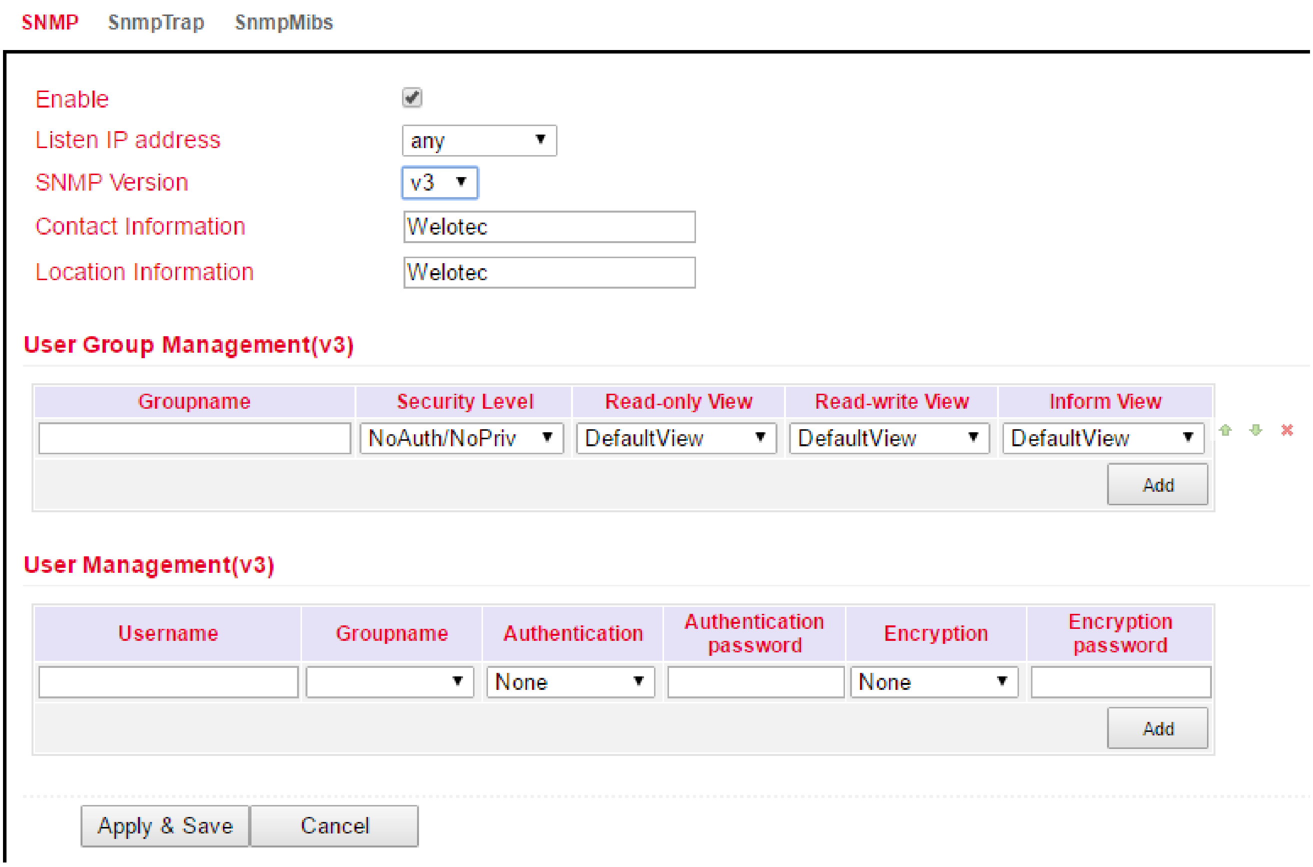


Enable	☑
Listen IP address	any ▼
SNMP Version	v2c ▼
Contact Information	Welotec
Location Information	Welotec

Community Management

Community Name	Access Limit	MIB View
public	Read-Only	DefaultView
private	Read-Write	DefaultView
	Read-Only ▼	DefaultView ▼

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



Enable	☑
Listen IP address	any ▼
SNMP Version	v3 ▼
Contact Information	Welotec
Location Information	Welotec

User Group Management(v3)

Groupname	Security Level	Read-only View	Read-write View	Inform View
	NoAuth/NoPriv ▼	DefaultView ▼	DefaultView ▼	DefaultView ▼

User Management(v3)

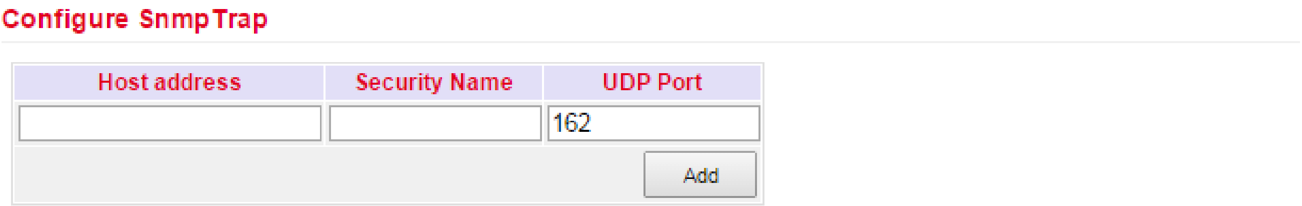
Username	Groupname	Authentication	Authentication password	Encryption	Encryption password
	▼	None ▼		None ▼	

SNMPv3 has group and user management.

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

3.1.8.2. SnmpTrap

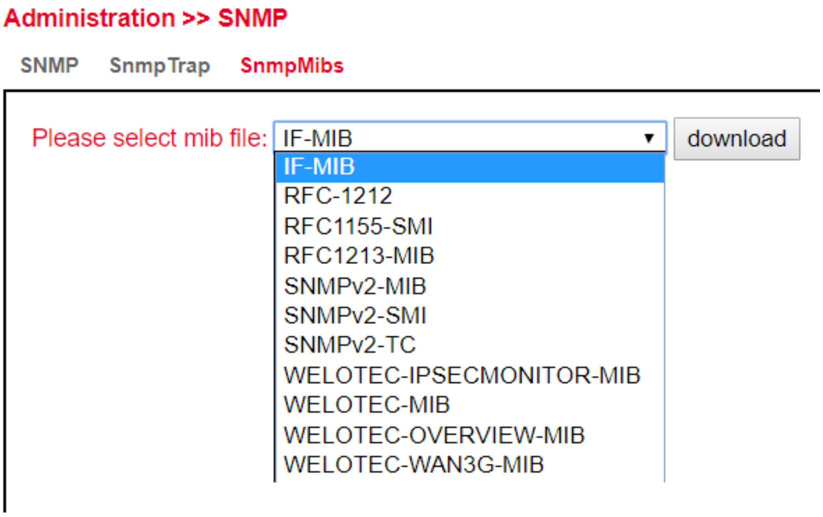
A SnmpTrap server can be entered. The router can actively send SNMP messages to the SNMP management server and does not wait until it receives an SNMP request from the management server.


Configure SnmpTrap

Host address	Security Name	UDP Port
		162

3.1.8.3. SnmpMibs

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



Administration >> SNMP

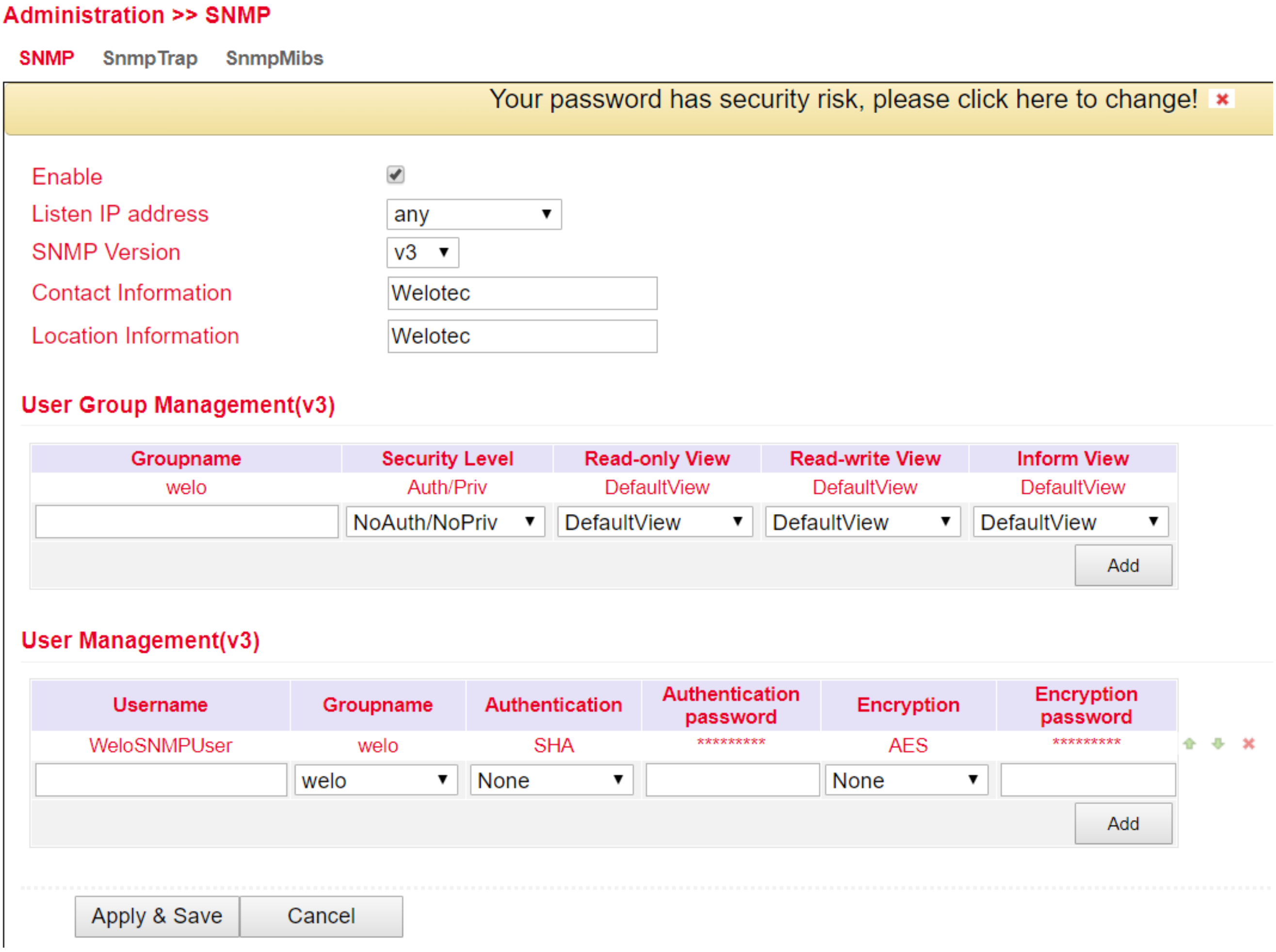
SNMP SnmpTrap SnmpMibs

Please select mib file: IF-MIB ▼ download

- IF-MIB
- RFC-1212
- RFC1155-SMI
- RFC1213-MIB
- SNMPv2-MIB
- SNMPv2-SMI
- SNMPv2-TC
- WELOTEC-IPSECMONITOR-MIB
- WELOTEC-MIB
- WELOTEC-OVERVIEW-MIB
- WELOTEC-WAN3G-MIB

3.1.8.4. Reading SNMP Mibs with SNMPWALK

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



Administration >> SNMP

SNMP SnmpTrap SnmpMibs

Your password has security risk, please click here to change! ×

Enable	☑
Listen IP address	any ▼
SNMP Version	v3 ▼
Contact Information	Welotec
Location Information	Welotec

User Group Management(v3)

Groupname	Security Level	Read-only View	Read-write View	Inform View
welo	Auth/Priv	DefaultView	DefaultView	DefaultView
	NoAuth/NoPriv ▼	DefaultView ▼	DefaultView ▼	DefaultView ▼

Add

User Management(v3)

Username	Groupname	Authentication	Authentication password	Encryption	Encryption password
WeloSNMPUser	welo	SHA	*********	AES	*********
	welo ▼	None ▼		None ▼	

Add

Apply & Save Cancel

Readout of the data entered above via SMTPWALK to e. g. a LINUX computer:

```
snmpwalk -v3 -u WeloSNMPUser -l AuthPriv -a MD5 -A 123456789 -x
AES -X 123456789 10.255.229.10
snmpwalk -v3 -u WeloSNMPUser -l AuthPriv -a MD5 -A 123456789 -x
AES -X 123456789 udp6:[2a02:d20:8:c01::1]
```

2) **Download MIBS from TK800**

3) **Read in MIBS** (either via a LINUX computer or via a MIB-Browser)

mkdir -p .snmp/mibs cp
Downloads/WELOTEC* .snmp/mibs/

After that the following MIBs exist:

WELOTEC-MIB
WELOTEC-OVERVIEW-MIB
WELOTEC-PORTSETTING-MIB
WELOTEC-SERIAL-PORT-MIB
WELOTEC-SYSTEM-MAN-MIB
WELOTEC-WAN3G-MIB

4) **Start SNMPWALK** (either via a LINUX computer or via a MIB-Browser)

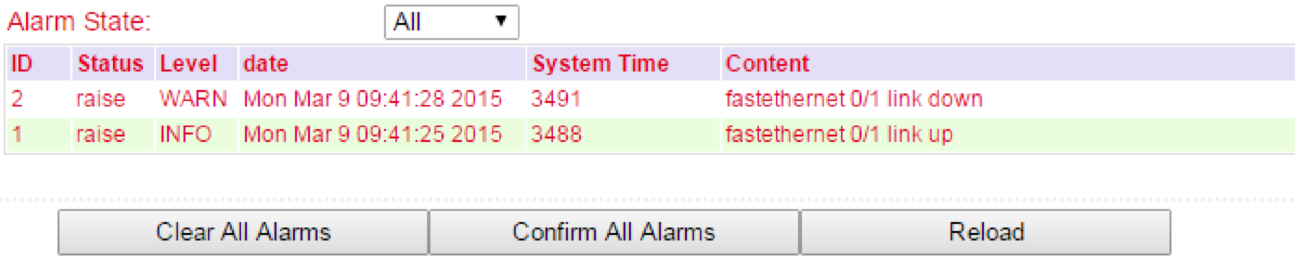
snmpwalk -m +WELOTEC-MIB -v3 -u WeloSNMPUser -l AuthPriv -a MD5 -A 123456789 -x AES -X 123456789 192.168.2.1 WELOTEC

```
WELOTEC-MIB::ihOverview.1.0 = STRING: “TK800”
WELOTEC-MIB::ihOverview.2.0 = STRING: “RF9151408241109”
WELOTEC-MIB::ihOverview.3.0 = STRING: “2011.09.r7903”
WELOTEC-MIB::ihOverview.4.0 = STRING: “1.0.0.r9338”
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
```

3.1.9. Alarm

3.1.9.1. Alarm Status

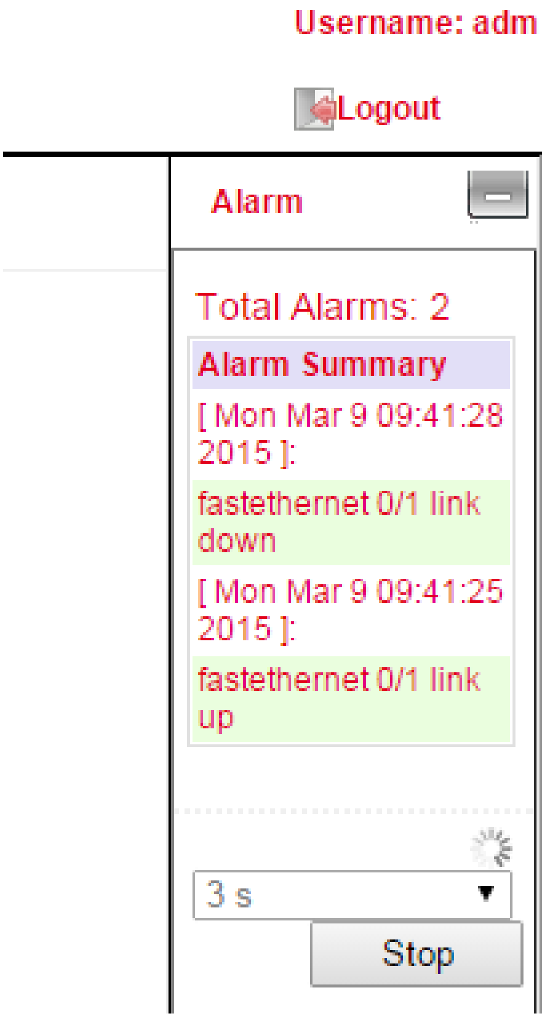
The alarm status displays an overview of the triggered alarms.
In this example, INFO message ID 1 shows that the Fastethernet port 0/1 has been connected. ID 2 shows a warning message that the Fastethernet port 0/1 has been disconnected (Fig. 1).



Alarm State: All

ID	Status	Level	date	System Time	Content
2	raise	WARN	Mon Mar 9 09:41:28 2015	3491	fastethernet 0/1 link down
1	raise	INFO	Mon Mar 9 09:41:25 2015	3488	fastethernet 0/1 link up

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



Username: adm

Total Alarms: 2

Alarm Summary

[Mon Mar 9 09:41:28 2015]:

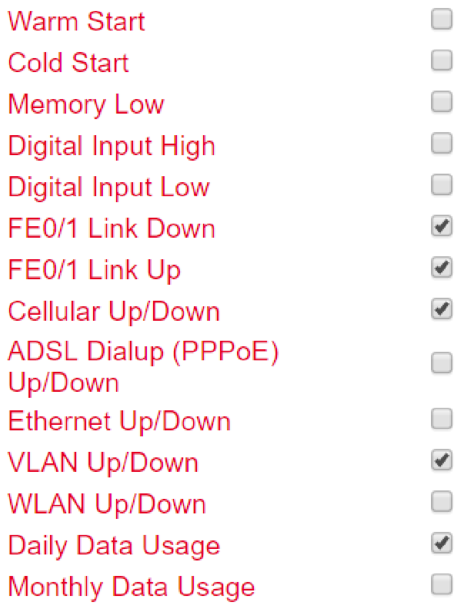
fastethernet 0/1 link down

[Mon Mar 9 09:41:25 2015]:

fastethernet 0/1 link up

3.1.9.2. Alarm Input

In the **Alarm Input** Menu, you define which alarm messages the router should send. Setting the check mark next to each entry activates or deactivates an alarm.



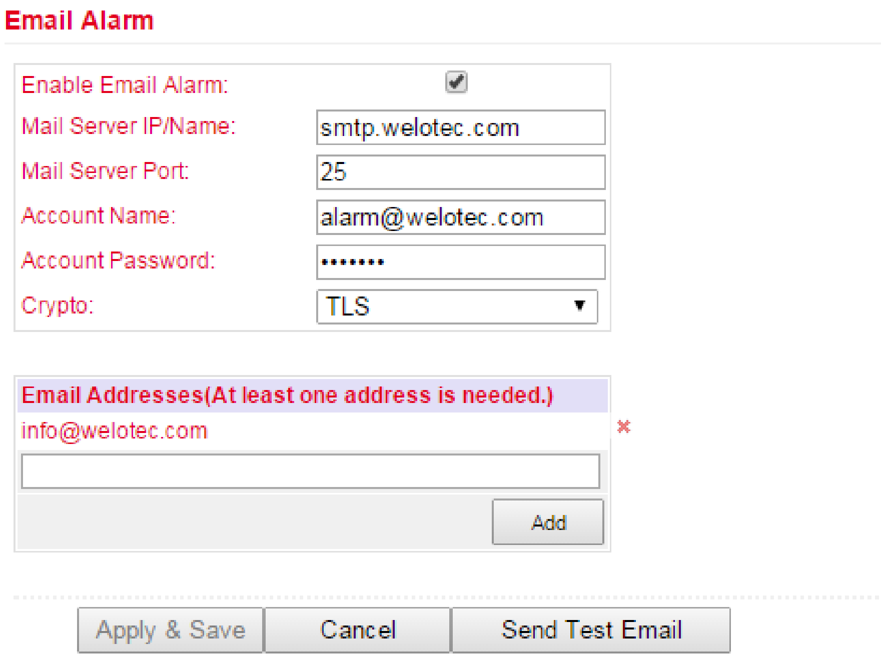
Warm Start	☐
Cold Start	☐
Memory Low	☐
Digital Input High	☐
Digital Input Low	☐
FE0/1 Link Down	☑
FE0/1 Link Up	☑
Cellular Up/Down	☑
ADSL Dialup (PPPoE) Up/Down	☐
Ethernet Up/Down	☐
VLAN Up/Down	☑
WLAN Up/Down	☐
Daily Data Usage	☑
Monthly Data Usage	☐

The following alarm alerts are possible

Parameter	Description
Warm Start	Warm start/Restart of the router (reboot)
Cold Start	Cold start = Start of the router if it was off or did not have power before.
Memory Low	Low RAM usage
Digital Input High	High digital data input
Digital Input Low	Low digital data input
FE0/1 Link Down	Fastethernet Port 0/1 disconnected
FE0/1 Link Up	Fastethernet Port 0/1 connected
Cellular Up/Down	Radio connection GPRS/UMTS/LTE connected 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	Display of the daily used data of the SIM card (only with activated Data Usage function, see Services > Data Usage)
Monthly Data Usage	Display of the monthly used data of the SIM card (only with activated Data Usage function, see Services > Data Usage)

3.1.9.3. Alarm Output

In the Alarm Output menu, the e-mail server is configured to receive and transmit alerts. If an alarm is triggered, the router generates a message and sends it to the stored e-mail addresses via the specified e-mail server.



Email Alarm

Enable Email Alarm:	☑
Mail Server IP/Name:	smtp.welotec.com
Mail Server Port:	25
Account Name:	alarm@welotec.com
Account Password:	•••••••
Crypto:	TLS

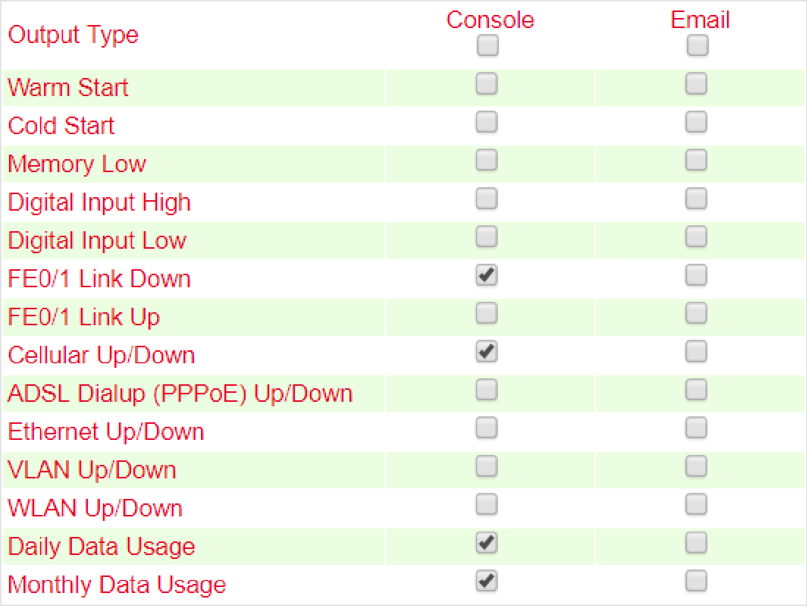
Email Addresses(At least one address is needed.)

info@welotec.com ✖

Parameter	Description
Enable Email Alarm	Check the box to disable e-mail server functionality
Mail Server IP/Name	Hostname (FQDN) or IP address of 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 via which the messages are to be sent
Account Passwort	Password of user account on the E-Mail Server
Crypto	Encryption TLS
Email Addresses	E-mail addressee to whom the mails should be sent

3.1.9.4. Alarm Map

The alarm map determines whether the warnings are displayed in the web browser or whether they should also be sent by e-mail. Check Enable or disable the function.

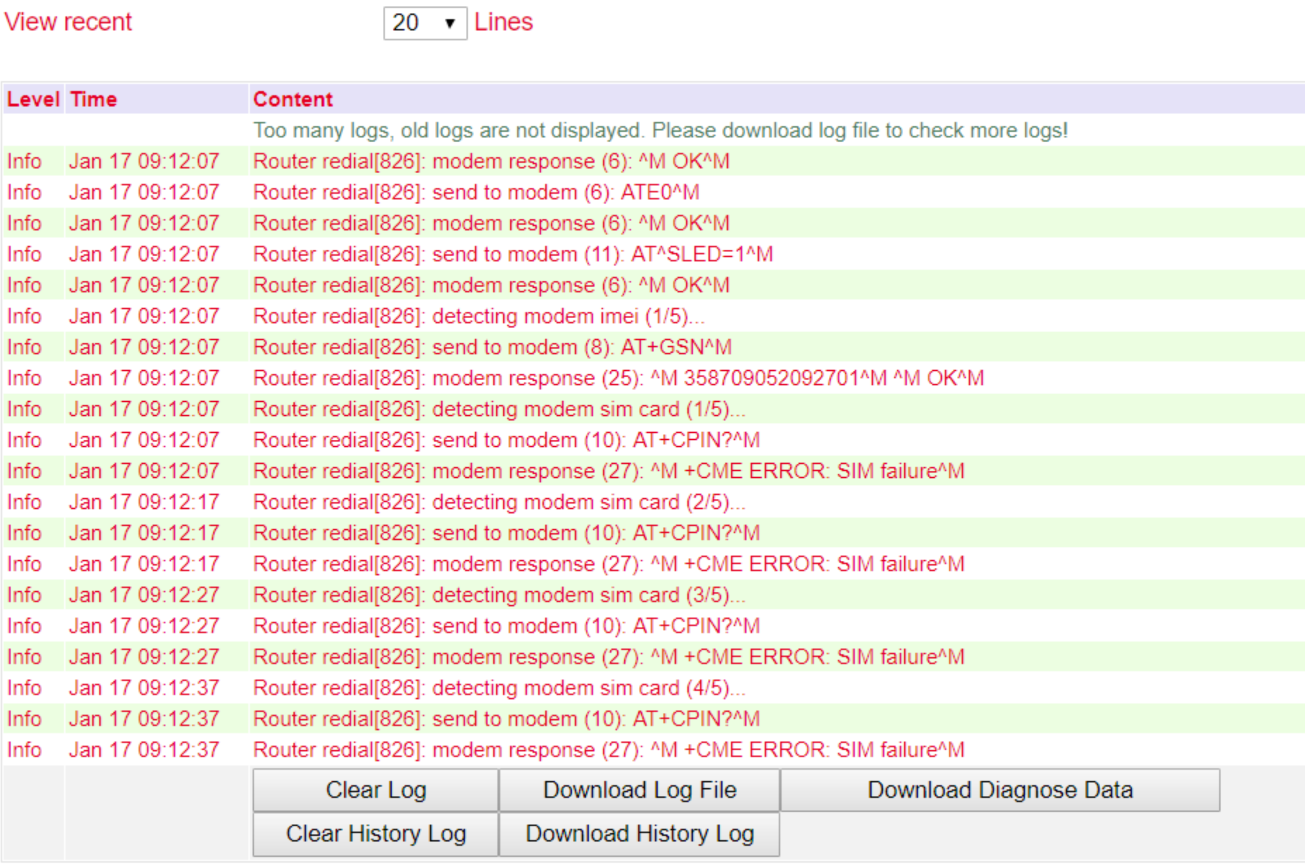


Output Type	Console □	Email □
Warm Start	□	□
Cold Start	□	□
Memory Low	□	□
Digital Input High	□	□
Digital Input Low	□	□
FE0/1 Link Down	☑	□
FE0/1 Link Up	□	□
Cellular Up/Down	☑	□
ADSL Dialup (PPPoE) Up/Down	□	□
Ethernet Up/Down	□	□
VLAN Up/Down	□	□
WLAN Up/Down	□	□
Daily Data Usage	☑	□
Monthly Data Usage	☑	□

3.1.10. Log

3.1.10.1. Log

The Log menu displays the current messages of the router.
The log contains information about the network, operating status, configuration changes, connection information of the provider, IPSec, OpenVPN status and much more.



View recent 20 ▾ Lines

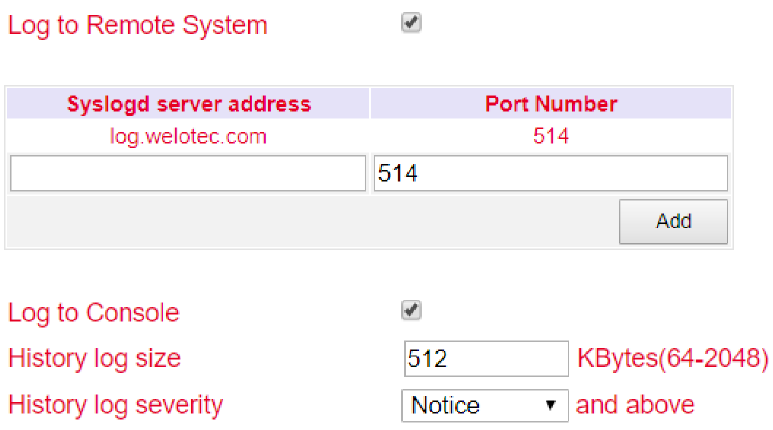
```
Level Time            Content
                      Too many logs, old logs are not displayed. Please download log file to check more logs!
Info  Jan 17 09:12:07 Router redial[826]: modem response (6): ^M OK^M
Info  Jan 17 09:12:07 Router redial[826]: send to modem (6): ATE0^M
Info  Jan 17 09:12:07 Router redial[826]: modem response (6): ^M OK^M
Info  Jan 17 09:12:07 Router redial[826]: send to modem (11): AT^SLED=1^M
Info  Jan 17 09:12:07 Router redial[826]: modem response (6): ^M OK^M
Info  Jan 17 09:12:07 Router redial[826]: detecting modem imei (1/5)...
Info  Jan 17 09:12:07 Router redial[826]: send to modem (8): AT+GSN^M
Info  Jan 17 09:12:07 Router redial[826]: modem response (25): ^M 358709052092701^M ^M OK^M
Info  Jan 17 09:12:07 Router redial[826]: detecting modem sim card (1/5)...
Info  Jan 17 09:12:07 Router redial[826]: send to modem (10): AT+CPIN?^M
Info  Jan 17 09:12:07 Router redial[826]: modem response (27): ^M +CME ERROR: SIM failure^M
Info  Jan 17 09:12:17 Router redial[826]: detecting modem sim card (2/5)...
Info  Jan 17 09:12:17 Router redial[826]: send to modem (10): AT+CPIN?^M
Info  Jan 17 09:12:17 Router redial[826]: modem response (27): ^M +CME ERROR: SIM failure^M
Info  Jan 17 09:12:27 Router redial[826]: detecting modem sim card (3/5)...
Info  Jan 17 09:12:27 Router redial[826]: send to modem (10): AT+CPIN?^M
Info  Jan 17 09:12:27 Router redial[826]: modem response (27): ^M +CME ERROR: SIM failure^M
Info  Jan 17 09:12:37 Router redial[826]: detecting modem sim card (4/5)...
Info  Jan 17 09:12:37 Router redial[826]: send to modem (10): AT+CPIN?^M
Info  Jan 17 09:12:37 Router redial[826]: modem response (27): ^M +CME ERROR: SIM failure^M
```

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

Option	Description
Clear Log	Delete displayed log
Download Log File	Download log
Download Diagnose Data	Diagnostic file Download
Clear History Log	Delete log history
Download History Log	Download log history

3.1.10.2. System Log

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



Log to Remote System ☑

Syslogd server address	Port Number
log.welotec.com	514
	514

Log to Console ☑

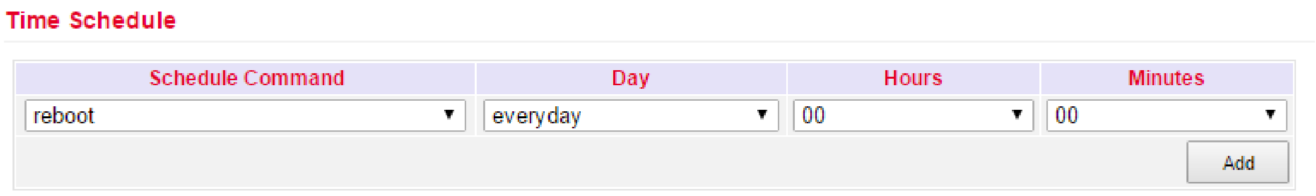
History log size 512 KBytes(64-2048)

History log severity Notice and above

Under **Syslogd server address** the hostname of the Syslog server (FQDN) or IP address is specified. Port 514 is typical for Syslogserver.

3.1.11. Cron Job

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



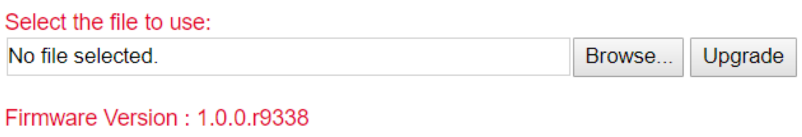
Time Schedule

Schedule Command	Day	Hours	Minutes
reboot	everyday	00	00

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

3.1.12. Upgrade

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



Select the file to use:

No file selected.

Firmware Version : 1.0.0.r9338

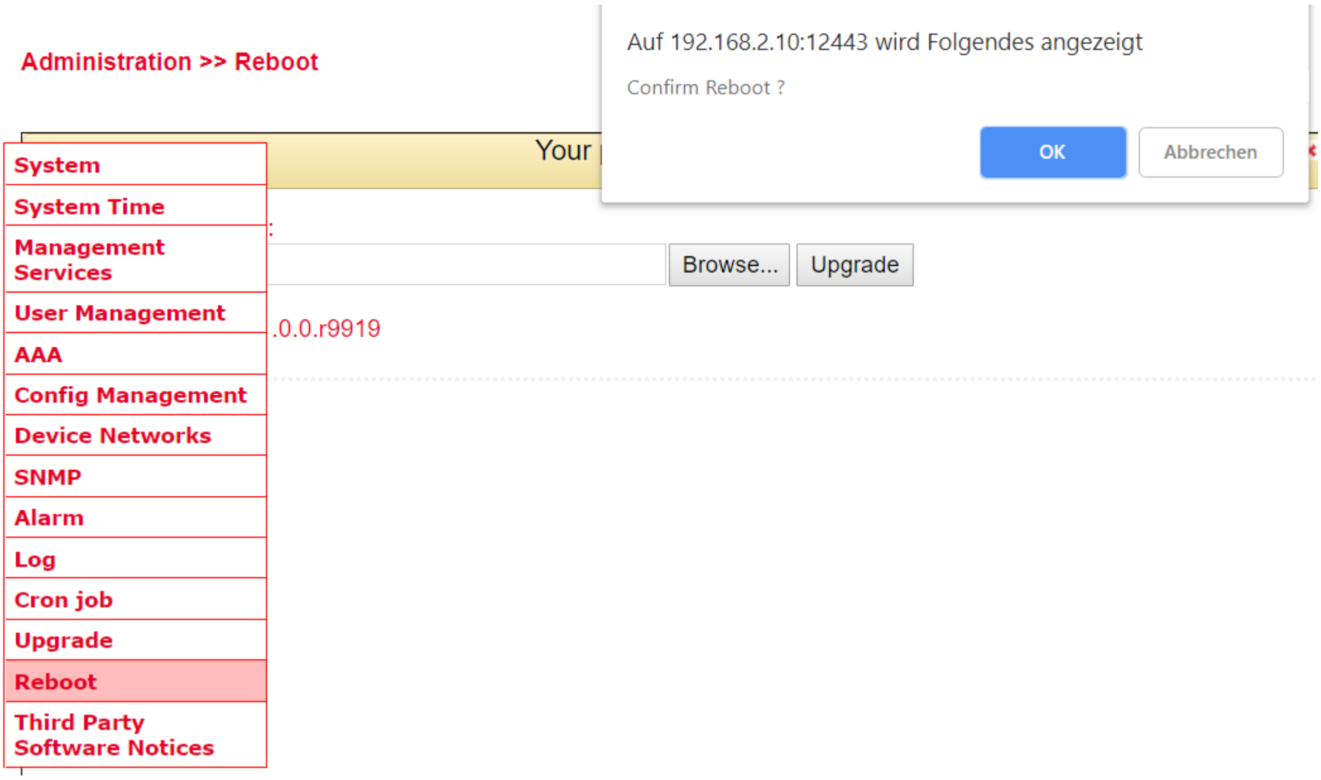
Under Browse select the firmware file you downloaded before (it must be unpacked as either *.bin or *.pkg file). Click on **Upgrade** to install the firmware on the router.

⚠ **Note**

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

3.1.13. Reboot

Reboot restarts the router.



Auf 192.168.2.10:12443 wird Folgendes angezeigt

Confirm Reboot ?

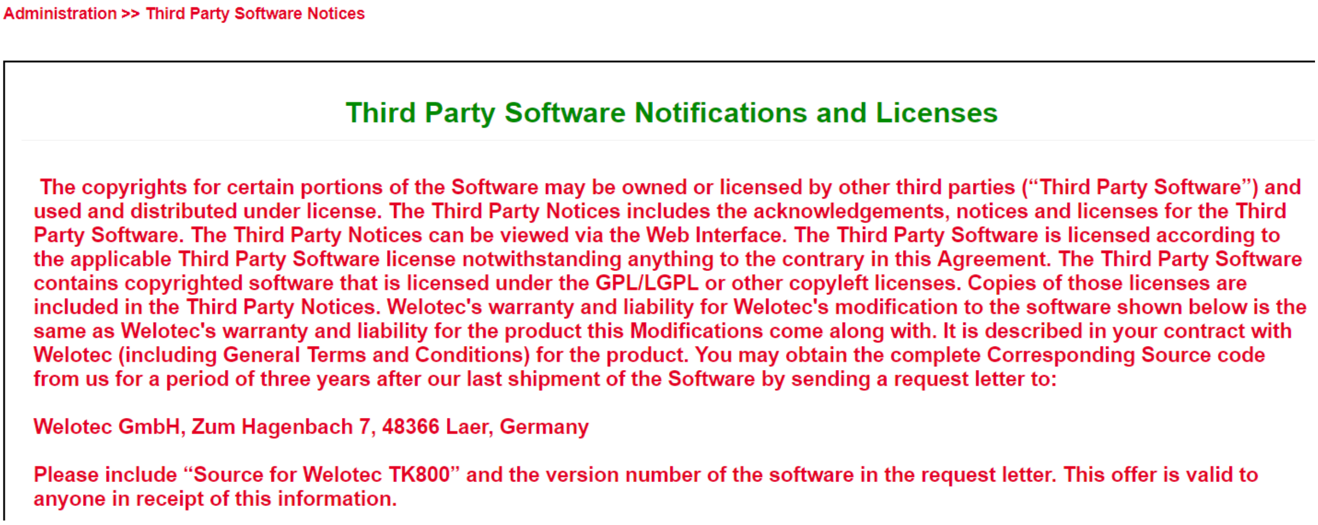
Click **OK** to confirm the restart of the router.

⚠ **Note**

Save the router configuration before restarting the router. Otherwise, the configuration may be lost during restart.

3.1.14. Third Party Software Notices

This section lists the software terms and licenses of all third party providers associated with the TK800 router series.



Administration >> Third Party Software Notices

Third Party Software Notifications and Licenses

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

Welotec GmbH, Zum Hagenbach 7, 48366 Laer, Germany

Please include “Source for Welotec TK800” and the version number of the software in the request letter. This offer is valid to anyone in receipt of this information.

3.2. Network

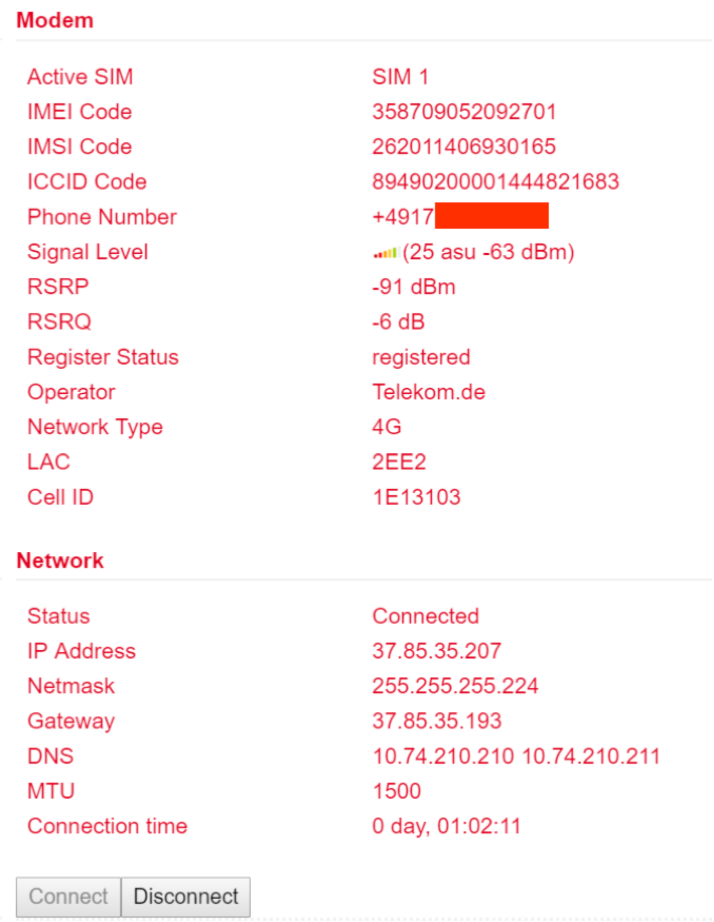
3.2.1. Cellular

Cellular is the mobile radio interface of the router. If a SIM card is installed in the router, you can dial up to the Internet via GPRS, EDGE, UMTS or LTE, depending on the router model.

3.2.1.1. Cellular Status

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

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



Modem

Active SIM	SIM 1
IMEI Code	358709052092701
IMSI Code	262011406930165
ICCID Code	89490200001444821683
Phone Number	+4917[redacted]
Signal Level	(25 asu -63 dBm)
RSRP	-91 dBm
RSRQ	-6 dB
Register Status	registered
Operator	Telekom.de
Network Type	4G
LAC	2EE2
Cell ID	1E13103

Network

Status	Connected
IP Address	37.85.35.207
Netmask	255.255.255.224
Gateway	37.85.35.193
DNS	10.74.210.210 10.74.210.211
MTU	1500
Connection time	0 day, 01:02:11

Under certain circumstances it may happen that the router is not assigned a correct DNS server by the provider. Make sure that there is no entry under DNS or an entry such as 10.74.210.210 (Telekom).

⚠ **Note**

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. With the help of the RSRP, this also determines the currently strongest radio cell in the environment.

RSRP	School grades	Comment
-50 up to -65 dBm	1 (very good)	there is excellent reception - perfect!
-65 dBm up to -80 dBm	2 (good)	good, sufficient reception conditions
-80 dBm up to -95 dBm	3 (satisfactory)	not perfect but sufficient for stable connections
-95 dBm up to -105 dBm	4 (sufficient)	still acceptable conditions with speed restrictions; if necessary also aborts
-110 dBm up to -125 dBm	5 (poor)	very low level - urgent need for action; probably no connection possible
-125 dBm up to -140 dBm	6 (deficient)	extremely bad - probably no connection possible

⚠ **Note**

The RSRQ is a calculated ratio value that results from the value for RSRP and the RSSI. It is extremely important for the evaluation of an LTE connection and the reception quality. The analysis of this value is essential for the optimal alignment of antennas during stationary use of LTE. Together with the RSRP, this allows the user to find the optimal position and orientation for his equipment (e.g. antenna).

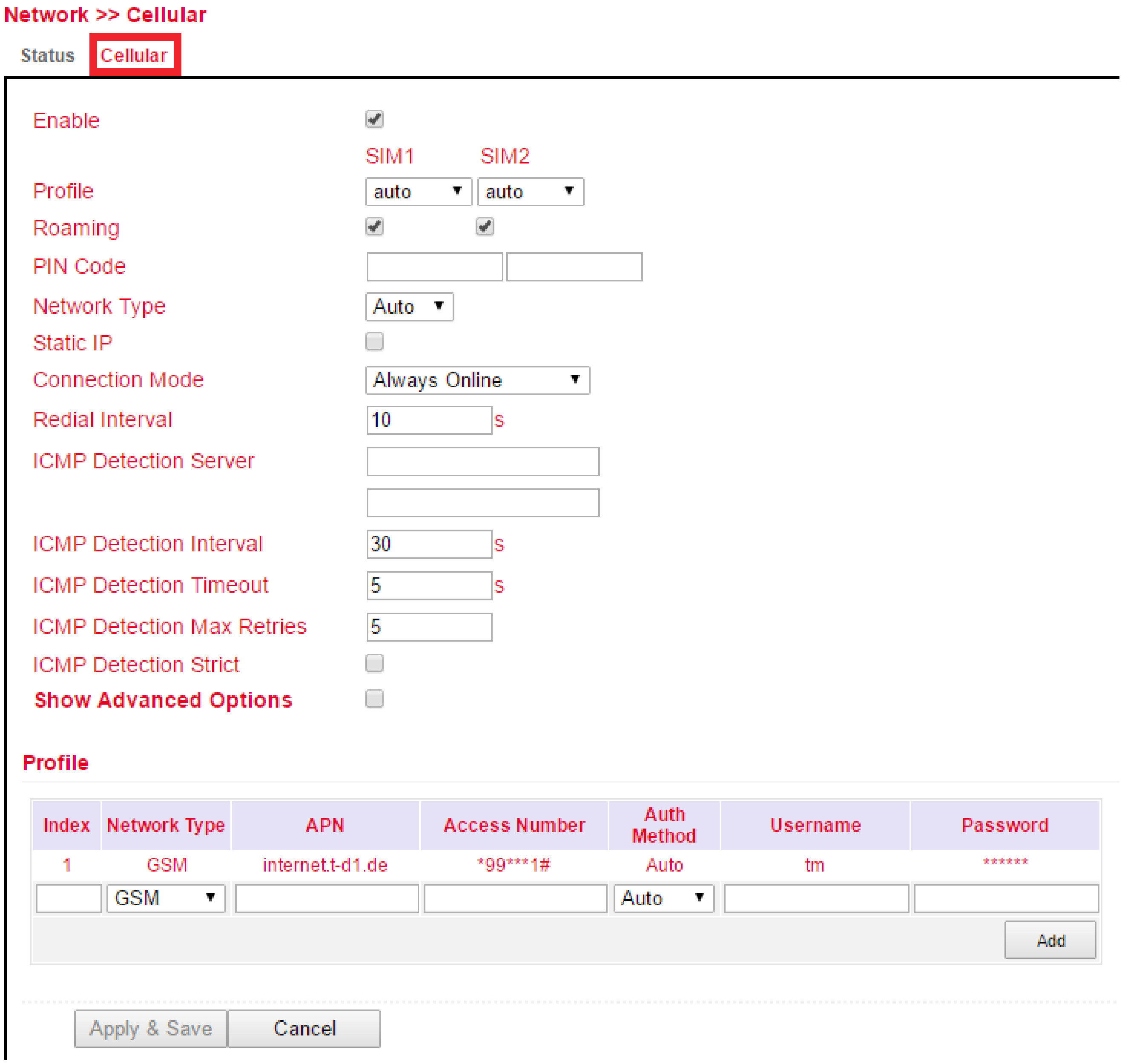
RSRQ	School grades	Comment
-3 dB	1 (very good)	Optimum connection quality, no interference from interferers
-4 up to -5 dB	2 (good)	interfering influences are present, but without effects
-6 up to -8 dB	3 (satisfactory)	Interfering influences, slight influence on the connection
-9 up to -11 dB	4 (sufficient)	Interfering influences, perceptible influence on the connection
-12 up to -15 dB	5 (poor)	Strongly disturbing influences present, connection very unstable
-16 up to -20 dB	6 (deficient)	Extremely disturbing influences, no usable connection possible

⚠ **Note**

Most providers assign private IP addresses or IP addresses that are not routed over the Internet. A successful or unsuccessful ping does not indicate whether the router’s IP address is really reachable.

3.2.1.2. Cellular Configuration

Under **Network > Cellular > Cellular** you can make settings for access via the mobile network.



Network >> Cellular

Status | Cellular

Enable	☑	
	SIM1	SIM2
Profile	auto ▼	auto ▼
Roaming	☑	☑
PIN Code		
Network Type	Auto ▼	
Static IP	☐	
Connection Mode	Always Online ▼	
Redial Interval	10 s	
ICMP Detection Server		
ICMP Detection Interval	30 s	
ICMP Detection Timeout	5 s	
ICMP Detection Max Retries	5	
ICMP Detection Strict	☐	
Show Advanced Options	☐	

Profile

Index	Network Type	APN	Access Number	Auth Method	Username	Password
1	GSM	internet.t-d1.de	*99***1#	Auto	tm	******
	GSM ▼			Auto ▼		

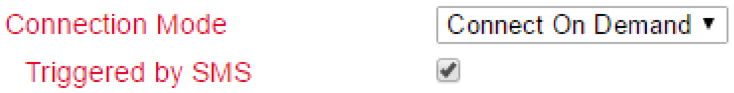
Add

Apply & Save | Cancel

Parameter	Description	Factory settings
Enable	Enable or disable of mobile networking connection	Activated
Profile	APN profile for SIM card 1 und SIM card 2	Auto / Auto automatic selection of the APN based on the SIM card
Roaming	Enable or disable whether the SIM card shall allow roaming. ⚠ **Note** Whether this function works depends on the provider. Despite deactivation, roaming may occur.	Activated / Activated

PIN Code	PIN code for SIM card ⚠ **Note** PIN Code shall be typed in, before the SIM card is in!!!	Empty / Empty
Network Type	Selection: Auto (automatic network selection), 2G (GPRS / EDGE), 3G (UMTS, HSDPA, HSUPA, HSPA+), 4G (LTE)	Auto
Static IP	⚠ **Note** Only relevant in a few exceptions. For most providers that assign fixed IP addresses, the function may not be set.	Deactivated
Connection Mode	Select whether the router should always be connected to the mobile phone network or only dial up if necessary.	Always Online
Redial Interval	Redial Interval	10 Seconds
ICMP Detection Server	Up to two ICMP detection servers can be used for connection monitoring. ⚠ **Note** The IP addresses or DNS names must be accessible via the router and must respond to a ping. It is therefore not recommended to use the Google servers 8.8.8.8 and 8.8.4.4, as these often block the requests. For example, select 4.2.2.1 or similar.	empty
ICMP Detection Interval	Interval at which the ICMP Detection Server checks the Internet connection.	30 Seconds
ICMP Detection Timeout	ICMP Timeout or Ping Timeout. The maximum time the ping may last (Round Trip Time).	5 Seconds
ICMP Detection Max Retries	Number of repetitions in case of ICMP ping failure.	5
ICMP Detection Strict	If disabled, the ICMP ping will only be sent if no data is sent or received. ⚠ **Note** If ICMP Detection Strict is enabled, the ICMP ping is always executed even when payload data is sent or received. For applications where high availability is important, Strict should be activated.	Deactivated
Show Advanced Options	If enabled, more configuration options become visible.	Deactivated

Connected on Demand

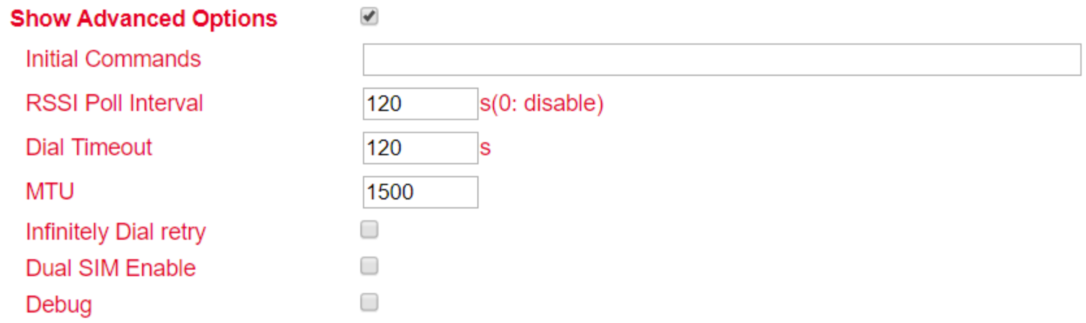


Connection Mode: Connect On Demand ▾

Triggered by SMS ☑

Here the check mark must be set for **Triggered by SMS**. The router only connects to the Internet if it has previously received the SMS command.

Show Advanced Options



Show Advanced Options ☑

Initial Commands

RSSI Poll Interval 120 s(0: disable)

Dial Timeout 120 s

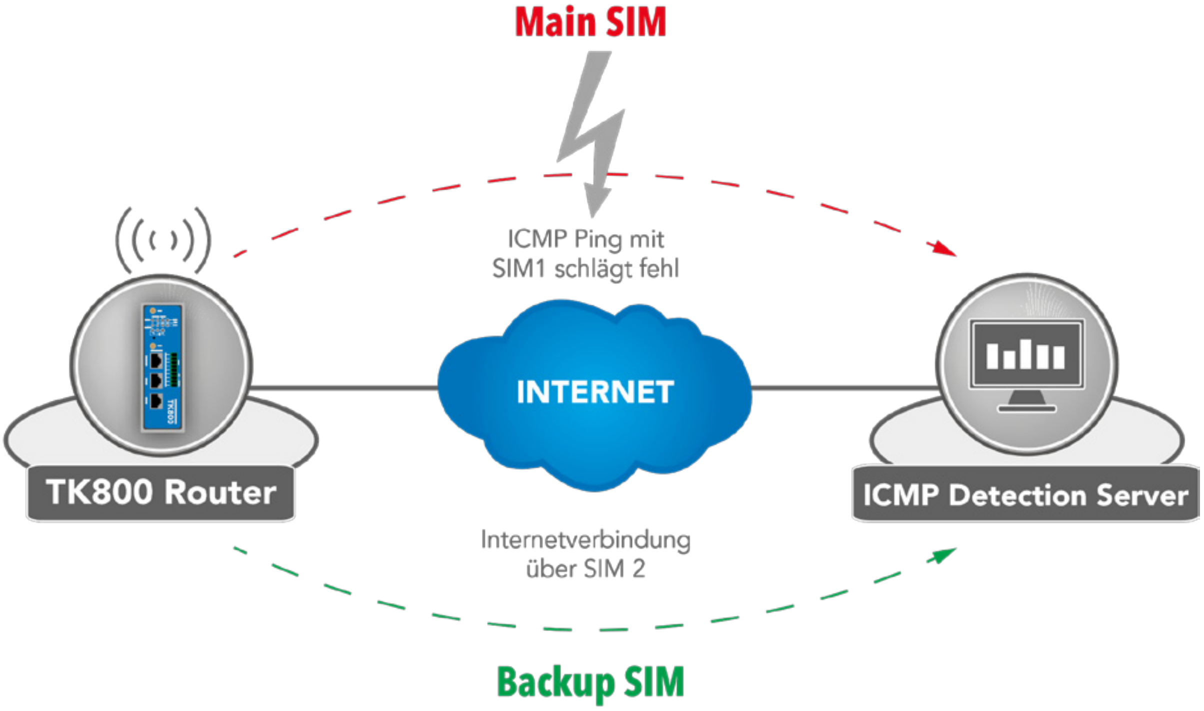
MTU 1500

Infinitely Dial retry □

Dual SIM Enable □

Debug □

Parameter	Description	Factory settings
Initial Commands	Start commands for e.g., if Triggered by SMS is selected or special AT commands are to be used	empty
RSSI Poll Interval	Request interval of signal strength	120 Seconds
Dial Timeout	Maximum time for a dialing attempt	120 Seconds
MTU	Maximum size of a packet	1500 byte
Netmask	An additional netmask can be entered here.	empty
Infinitely Dial Retry	If Triggered by SMS is selected, the dialing can be set to infinity	off
Dual SIM Enable	Turn on/off the Dual SIM option. If this item is activated, special selection fields are available (see below).	disabled
Main SIM	The main sim card to be used	SIM1
Max Number of Dial	Maximum amount of connection attempts, then restart of modem	5
Min Connected Time	Minimal connection time	0 Seconds
CSQ Threshold	Minimal signal strength SIM1 / SIM2	0
CSQ Detect Interval	Interval for the signal strength interrogation SIM1 / SIM2	0 Seconds
CSQ Detect Retries	Retries for signal strength interrogation SIM1 / SIM2	0
Backup SIM Timeout	Time after which it is switched back to the main SIM card	0 Seconds
Debug	If activated, then more detailed logging is done	disabled



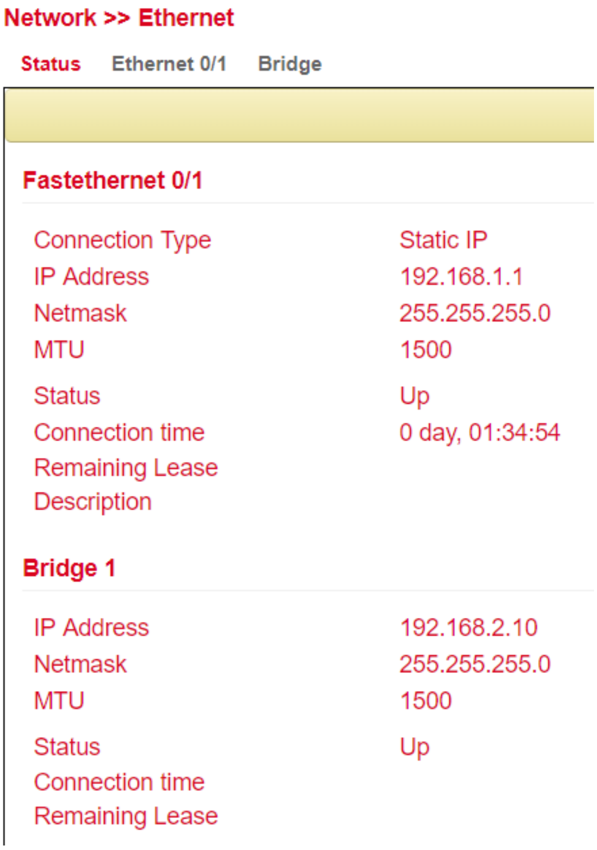
If one provider fails, the system switches to the alternative provider. The same applies to the consumption of mobile data volume. The TK800 uses ICMP to monitor the data connection. If this is no longer available (because the ping fails), the router switches to the other connection.

3.2.2. Ethernet

In the Ethernet area you have the possibility to make settings on 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 FE 1/4 depending on the model.

3.2.2.1. Ethernet Status

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



Fastethernet 0/1

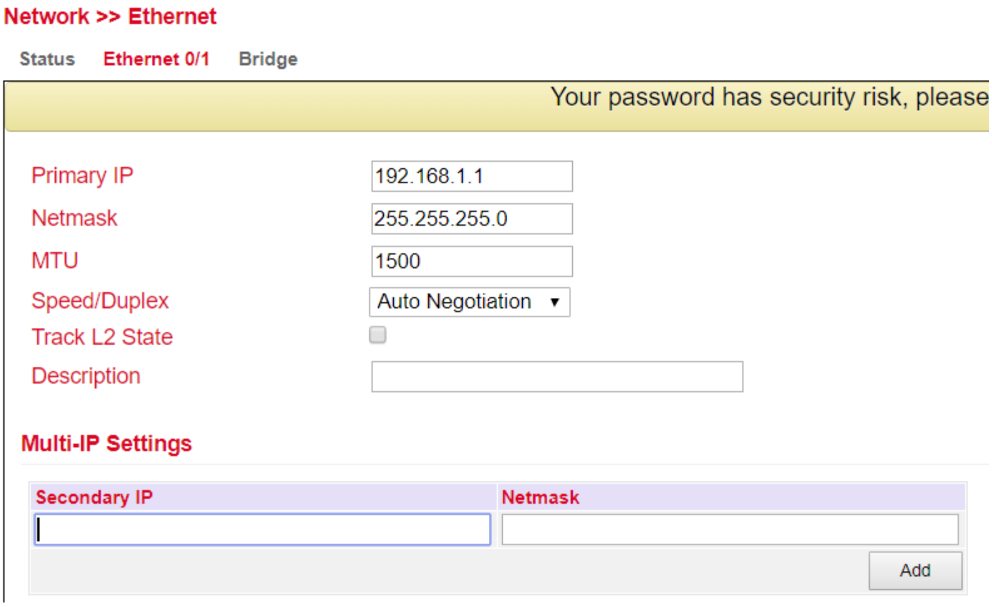
Connection Type	Static IP
IP Address	192.168.1.1
Netmask	255.255.255.0
MTU	1500
Status	Up
Connection time	0 day, 01:34:54
Remaining Lease	
Description	

Bridge 1

IP Address	192.168.2.10
Netmask	255.255.255.0
MTU	1500
Status	Up
Connection time	
Remaining Lease	

3.2.2.2. Fast Ethernet 0/1

Here you can adapt the settings of the network interface with the designation FE 0/1.



Network >> Ethernet

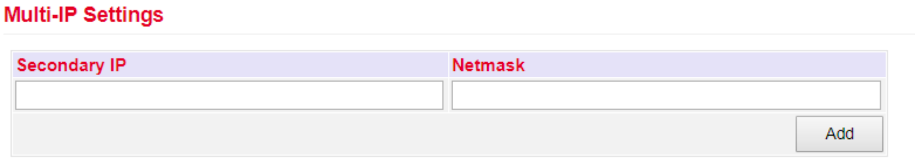
Primary IP	192.168.1.1
Netmask	255.255.255.0
MTU	1500
Speed/Duplex	Auto Negotiation ▾
Track L2 State	□
Description	

Multi-IP Settings

Secondary IP	Netmask

Parameter	Description	Factory setting
Primary IP	Primary IP-address can be entered in 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 choosable: • Auto Negotiation: Automatic negotiation of the speed • 100M Full-duplex: 100 Megabit Voll-duplex • 100M Half-duplex: 100 Megabit Halb-duplex • 10M Full-duplex: 10 Megabit Voll-duplex • 10M Half-duplex: 10 Megabit Halb-duplex	Auto
Track L2 State	• Check is set: Port status remains disconnected after being disconnected administratively (down) • Check not set: Port status reconnects after disconnection (UP)	Check not set
Description	Description of the port - freely selectable name	-

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



Multi-IP Settings

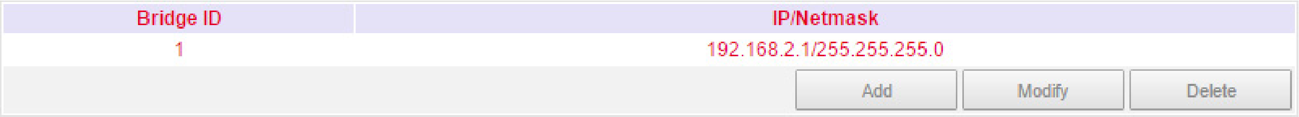
Secondary IP	Netmask

⚠ **Note**

The Configuration as DHCP Client is described under **DHCP**. The Configuration of WAN Interfaces is described under **Wizard**.

3.2.2.3. Bridge (TK8x5-EXW)

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

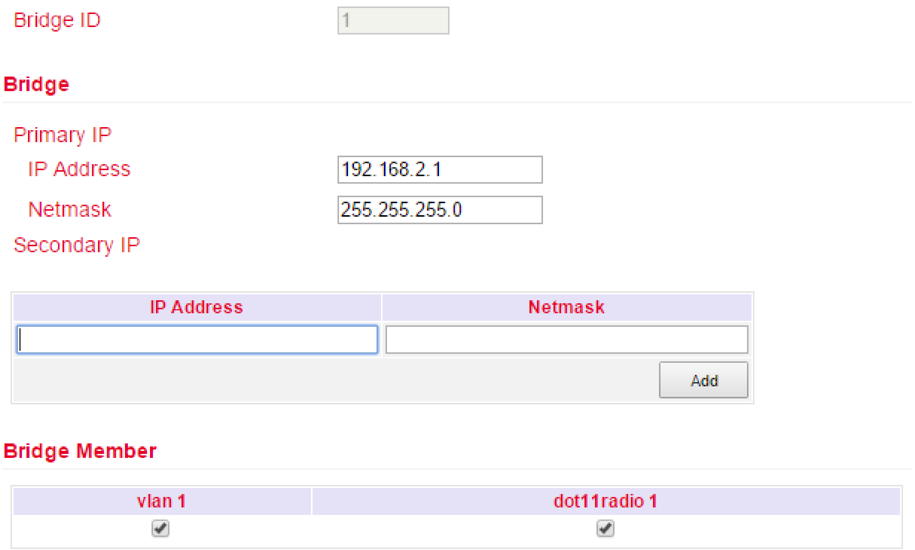


Bridge ID	IP/Netmask
1	192.168.2.1/255.255.255.0

Note

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

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



Bridge ID: 1

Bridge

Primary IP

IP Address: 192.168.2.1

Netmask: 255.255.255.0

Secondary IP

IP Address	Netmask

Bridge Member

vlan 1	dot11radio 1
☑	☑

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 **dot11radio1** interface is the WLAN interface. A bridge member can be added or removed from the bridge via the check markers.

Note

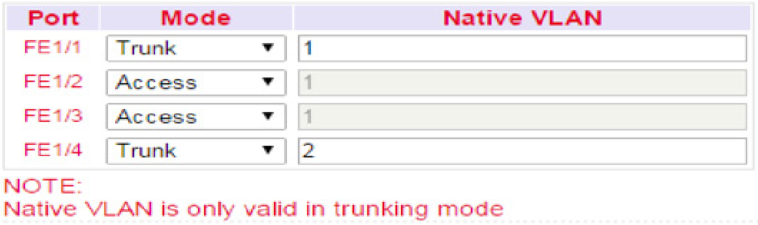
Removing a bridge member from the bridge will empty the interface's IP address. Thus, it is recommended to make a change only via the FE0/1 interface, because this is not a Bridge Member.

3.2.3. VLAN (TK8x5-x)

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

3.2.3.1. VLAN Trunk

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



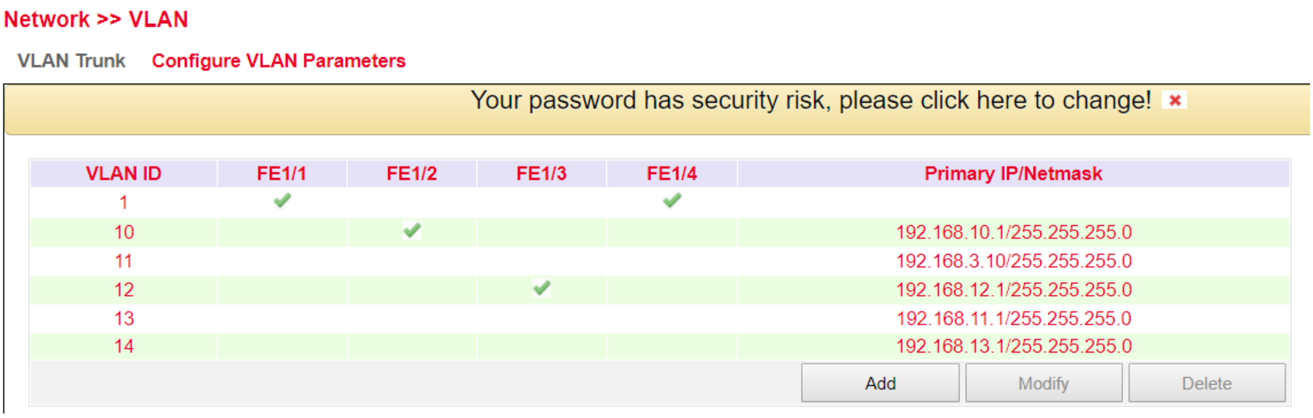
Port	Mode	Native VLAN
FE1/1	Trunk ▼	1
FE1/2	Access ▼	1
FE1/3	Access ▼	1
FE1/4	Trunk ▼	2

NOTE:
Native VLAN is only valid in trunking mode

The options **Access** and **Trunk** are available for the FastEthernet ports.
In access mode, the VLAN 1 is always selected.
In Trunk mode, you can assign VLAN IDs between 1-4000 to FastEthernet ports.

3.2.3.2. Configure VLAN Parameters

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



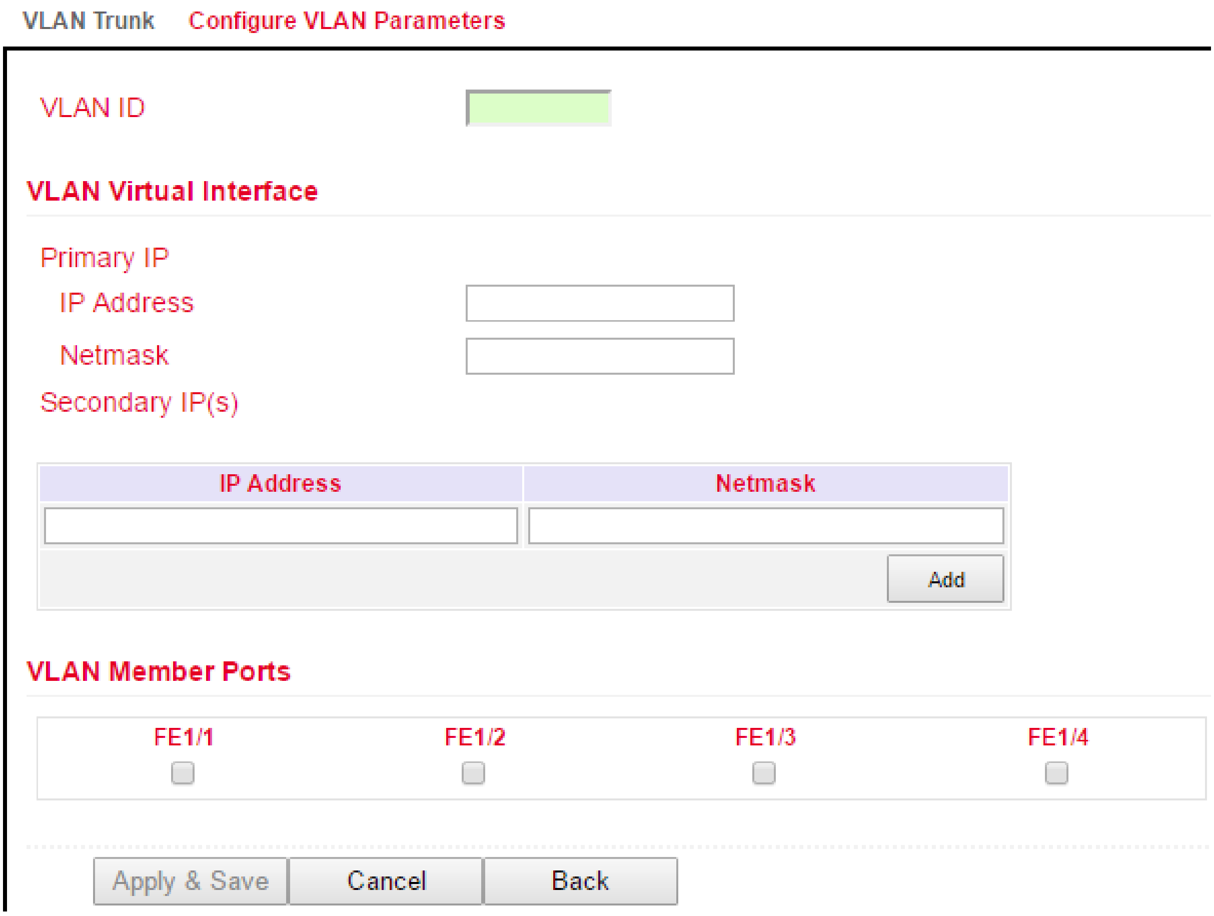
Network >> VLAN

Your password has security risk, please click here to change! ✖

VLAN ID	FE1/1	FE1/2	FE1/3	FE1/4	Primary IP/Netmask
1	✓			✓	
10		✓			192.168.10.1/255.255.255.0
11					192.168.3.10/255.255.255.0
12			✓		192.168.12.1/255.255.255.0
13					192.168.11.1/255.255.255.0
14					192.168.13.1/255.255.255.0

Button	Description
Add	Click the Add button to add a new VLAN.
Modify	The existing VLAN can be edited by selecting and clicking Modify ⚠ **Note** For model TK8x5-EXW, the VLAN with ID1 can not be edited as long as the bridge is active.
Delete	Using Delete you can delete the previously chosen VLAN ⚠ **Note** The VLAN with ID1 can not be deleted!!!

Add a new VLAN:



VLAN Trunk   Configure VLAN Parameters

VLAN ID

VLAN Virtual Interface

Primary IP

IP Address

Netmask

Secondary IP(s)

IP Address	Netmask

Add

VLAN Member Ports

FE1/1	FE1/2	FE1/3	FE1/4
□	□	□	□

Apply & Save   Cancel   Back

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

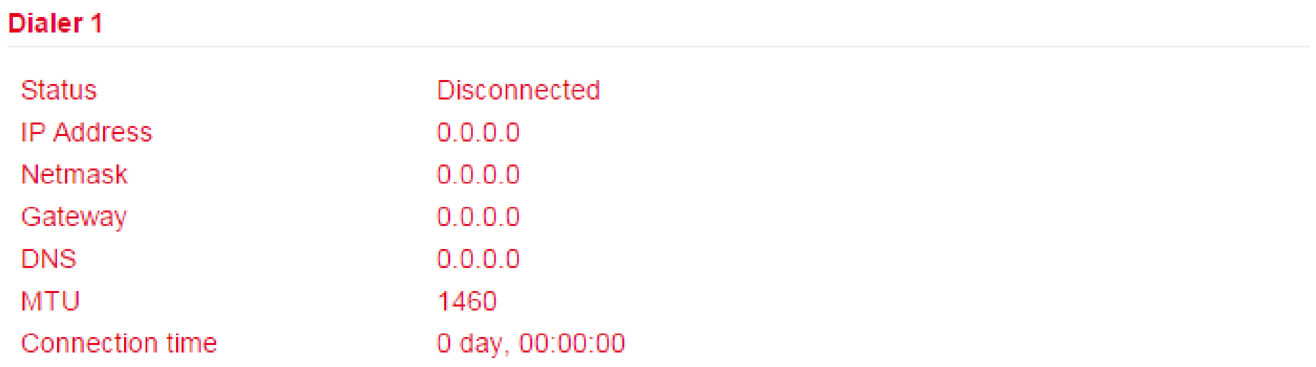
Under **VLAN Member Ports**, setting the checkmark in the checkbox assigns one or more FastEthernet port/s to the VLAN.

⚠ **Note**

The routers of the TK800 series 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. ADSL Dialup (PPPoE)

3.2.4.1. Status



Dialer 1

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

Note

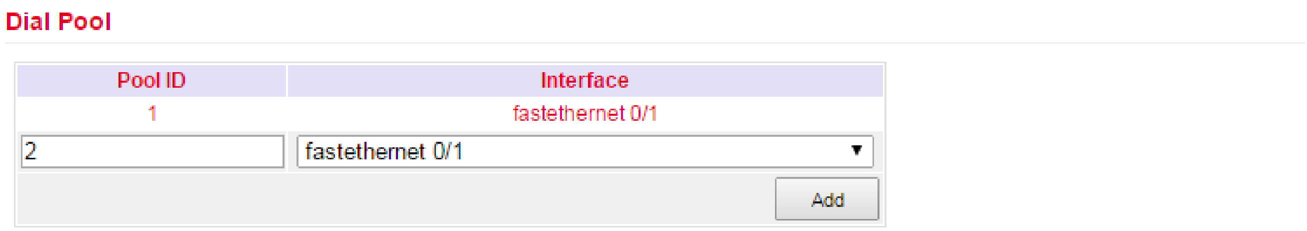
The routers of the TK800 series do not have a built-in ADSL modem. For the use of ADSL
Dialup, an external ADSL modem must be connected to the WAN port. For the digital transmission technology a DSL modem is necessary, which masters the new IP technologies.

3.2.4.2. ADSL Dialup (PPPoE)

Here you can configure dial-up via the DSL modem for PPPoE. The TK800 does not have its own DSL modem, so they cannot dial in independently.
In this case, an appropriate DSL modem is required that can handle the new IP technologies. The modem should meet the following criteria:

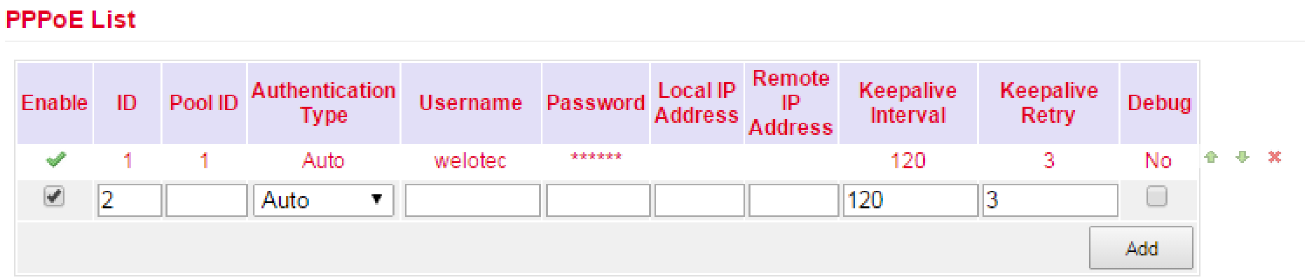
- VDSL2/ADSL2 Ethernet modem
- Annex A/B/M/J compatible
- PPPoE bridge operation
- IPv4 and IPv6 compatible
- DSL standards
  - ANSI T1.413 Issue 2
  - ITU G.992.1 A/B (G.dmt)
  - ITU G.992.2 (G.lite)
  - ITU G.992.3 (VDSL2)
  - ITU G.992.4 (G.HS)
  - ITU G.992.5 (ADSL2+)

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



Dial Pool

Pool ID	Interface
1	fastethernet 0/1
2	fastethernet 0/1 ▼
	Add



PPPoE List

Enable	ID	Pool ID	Authentication Type	Username	Password	Local IP Address	Remote IP Address	Keepalive Interval	Keepalive Retry	Debug	
✓	1	1	Auto	welotec	******			120	3	No	↑ ↓ ×
☑	2		Auto ▼					120	3	□	
										Add	

Dial Pool

The **Pool ID** defines the **Interface** for the PPPoE dial-up.

PPPoE List

Parameter	Description
Enable	Enables or disables the PPPoE entry
ID	Assign any unique ID
Pool ID	The ID previously created via Dial Pool for the interface over which the connection is to be established
Authentication Type	Auto, PAP, CHAP is selectable. In most cases, this parameter can be set to Auto
Username	The username, you got from your provider for log in
Password	The password, you got from your provider for log in
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 the connection check fails
Debug	When activated, detailed logging is performed

⚠ **Note**

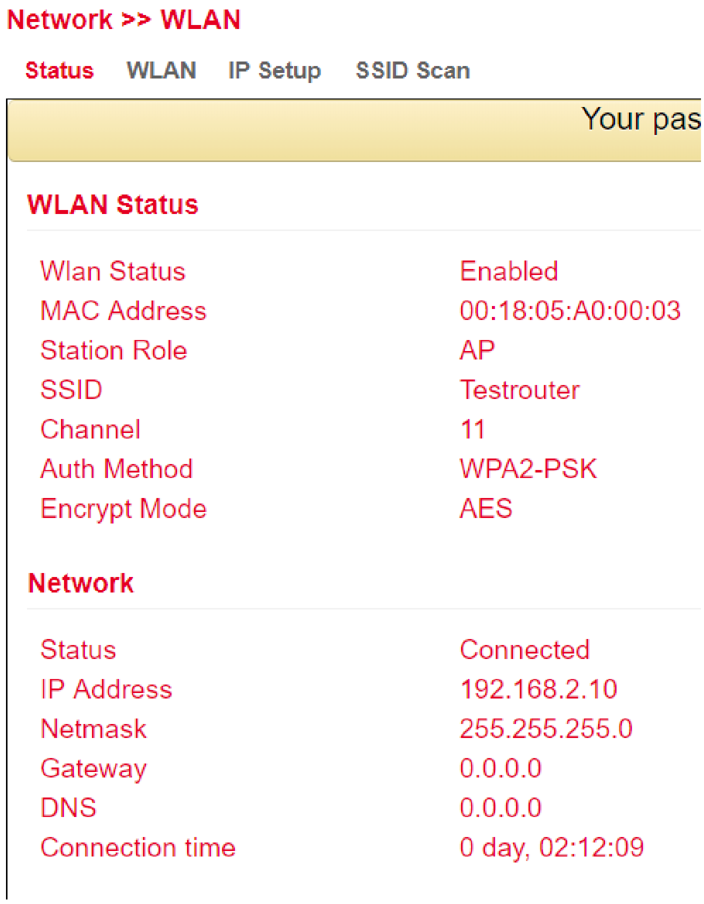
Using the wizard, a PPPoE connection can also be set up via **New WAN**, which is easier than the manual configuration!

3.2.5. WLAN (TK8x5-EXW)

3.2.5.1. WLAN Status

Under **Network > WLAN** the status of the WLAN is displayed

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



Network >> WLAN

Your pas

WLAN Status

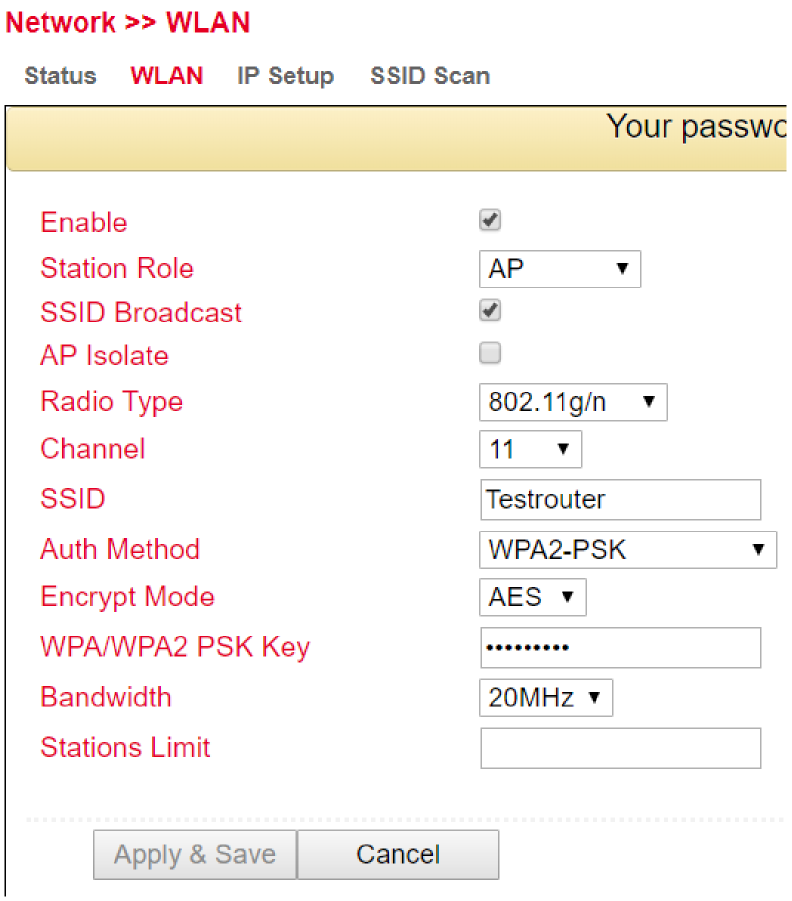
Wlan Status	Enabled
MAC Address	00:18:05:A0:00:03
Station Role	AP
SSID	Testrouter
Channel	11
Auth Method	WPA2-PSK
Encrypt Mode	AES

Network

Status	Connected
IP Address	192.168.2.10
Netmask	255.255.255.0
Gateway	0.0.0.0
DNS	0.0.0.0
Connection time	0 day, 02:12:09

3.2.5.2. WLAN Configuration

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



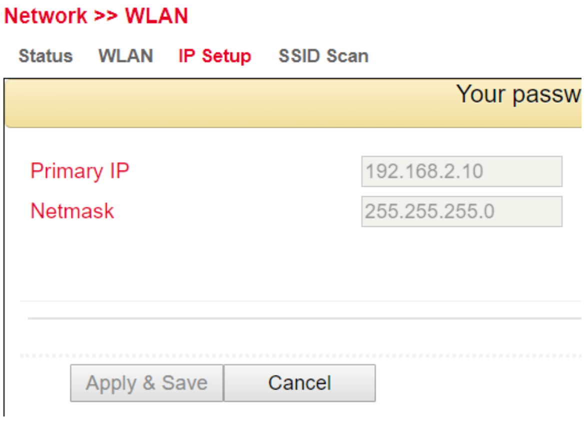
Network >> WLAN

Enable	☑
Station Role	AP ▾
SSID Broadcast	☑
AP Isolate	□
Radio Type	802.11g/n ▾
Channel	11 ▾
SSID	Testrouter
Auth Method	WPA2-PSK ▾
Encrypt Mode	AES ▾
WPA/WPA2 PSK Key	•••••••••
Bandwidth	20MHz ▾
Stations Limit	

Parameter	Description	Factory setting
Enable	Enables or disables the WLAN	Enables
Station Role	AP (Access Point) or Client	AP
SSID Broadcast	Display the SSID when searching for it	Enables
AP Isolate	Enables or disables AP isolation	Disables
Radio Type	Here you can select the wireless standard	802.11/g/n
Channel	Here the radio channel can be selected	11
SSID	The SSID that identifies your WLAN and which is to be displayed when searching for WLAN networks	TK800
Auth Method	The encryption standard to be used. OPEN if the WLAN is not supposed to be protected (not recommended)	OPEN
Encrypt Mode	When choosing Open or Shared: WEP40 or WEP104, both are no longer used today because it is not safe. If you select 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 channels that do not overlap.	20MHz
Stations Limit	Maximal amount of simultaneous connected Clients	empty

3.2.5.3. IP Setup

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



Your passw

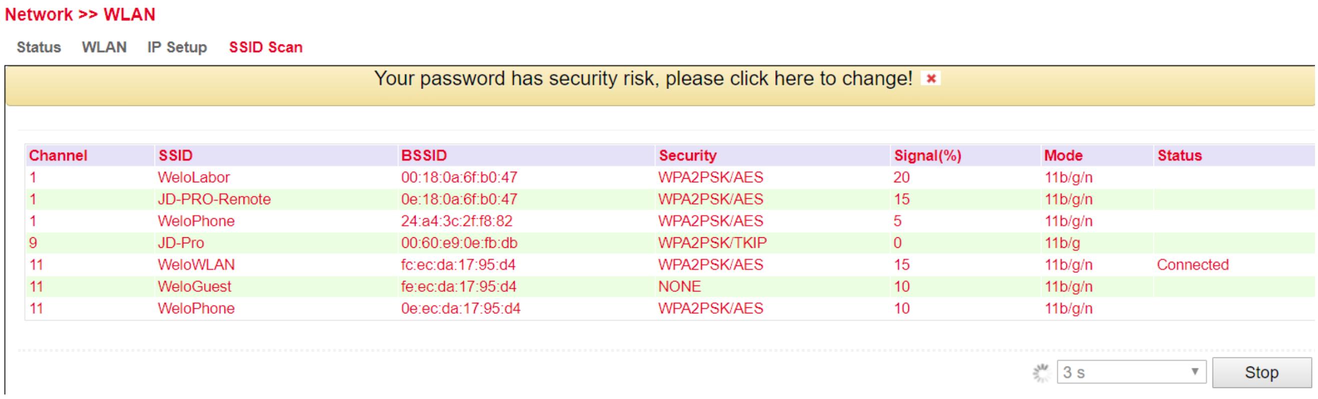
Primary IP	192.168.2.10
Netmask	255.255.255.0

⚠ **Note**

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. In case the TK 800 is connected to a WLAN as a client, this will be displayed in the Connected status.



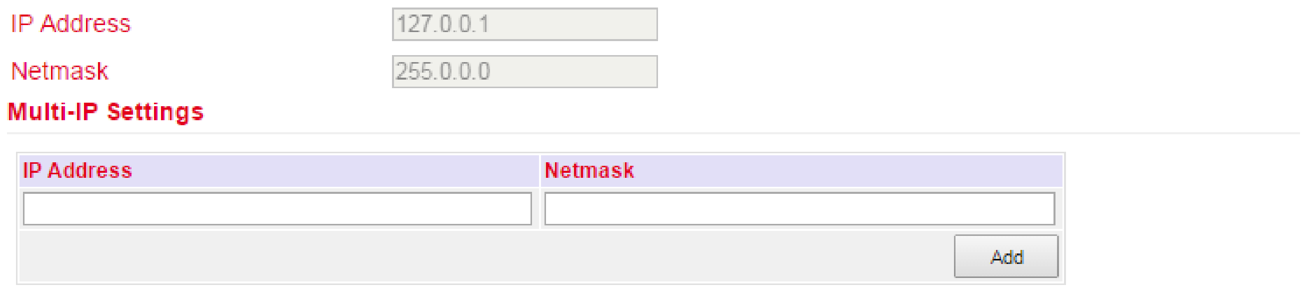
Your password has security risk, please click here to change! ×

Channel	SSID	BSSID	Security	Signal(%)	Mode	Status
1	WeloLabor	00:18:0a:6f:b0:47	WPA2PSK/AES	20	11b/g/n	
1	JD-PRO-Remote	0e:18:0a:6f:b0:47	WPA2PSK/AES	15	11b/g/n	
1	WeloPhone	24:a4:3c:2f:f8:82	WPA2PSK/AES	5	11b/g/n	
9	JD-Pro	00:60:e9:0e:fb:db	WPA2PSK/TKIP	0	11b/g	
11	WeloWLAN	fc:ec:da:17:95:d4	WPA2PSK/AES	15	11b/g/n	Connected
11	WeloGuest	fe:ec:da:17:95:d4	NONE	10	11b/g/n	
11	WeloPhone	0e:ec:da:17:95:d4	WPA2PSK/AES	10	11b/g/n	

3.2.6. Loopback

3.2.6.1. Loopback Configuration

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



IP Address	127.0.0.1
Netmask	255.0.0.0

Multi-IP Settings

IP Address	Netmask

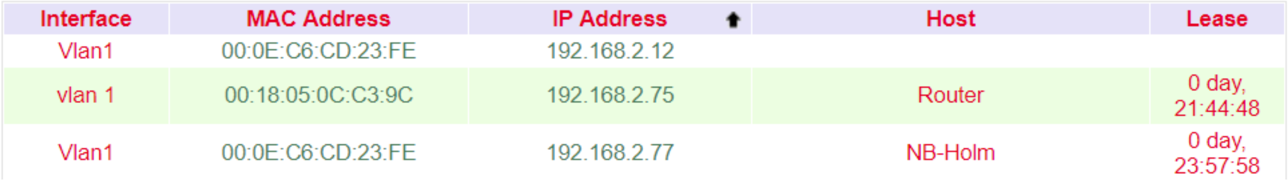
3.3. Services

3.3.1. DHCP

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

3.3.1.1. DHCP Status

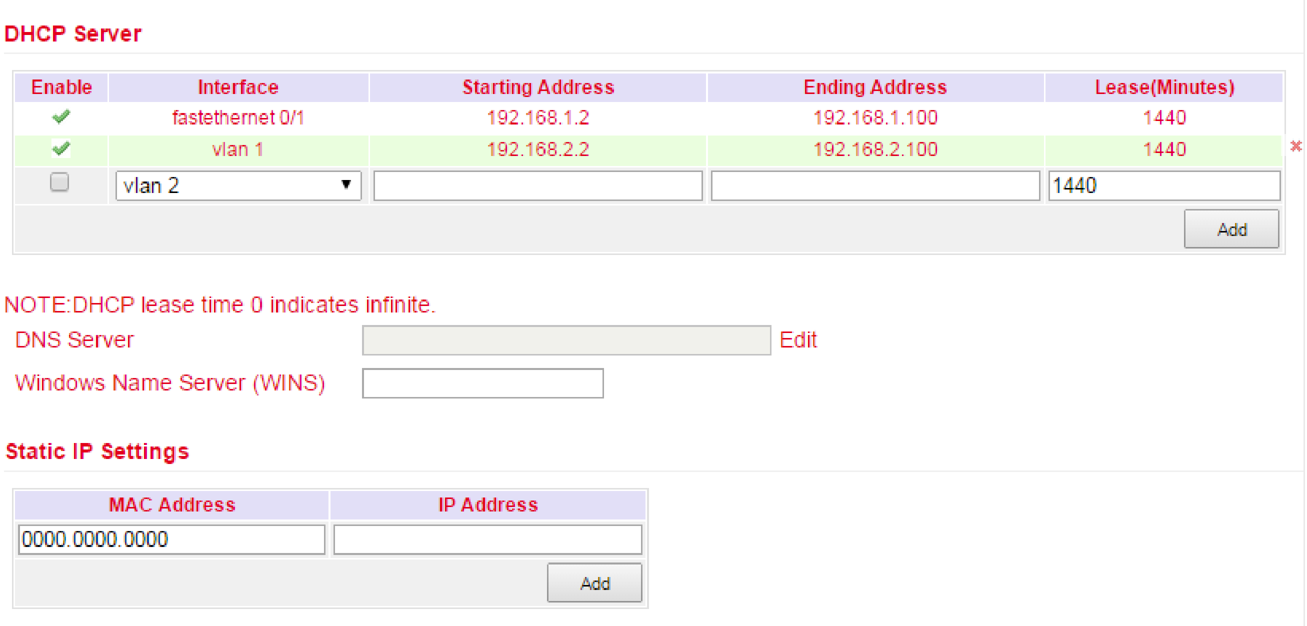
Under **Services > DHCP > Status** you can see who is currently connected to the router via which interface.



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** the settings for the DHCP server can be configured.Select the corresponding interface and enter the start or end IP address, as well as the lease, see example.



DHCP Server

Enable	Interface	Starting Address	Ending Address	Lease(Minutes)
✓	fastethernet 0/1	192.168.1.2	192.168.1.100	1440
✓	vlan 1	192.168.2.2	192.168.2.100	1440
□	vlan 2 ▼			1440

NOTE:DHCP lease time 0 indicates infinite.

DNS Server Edit

Windows Name Server (WINS)

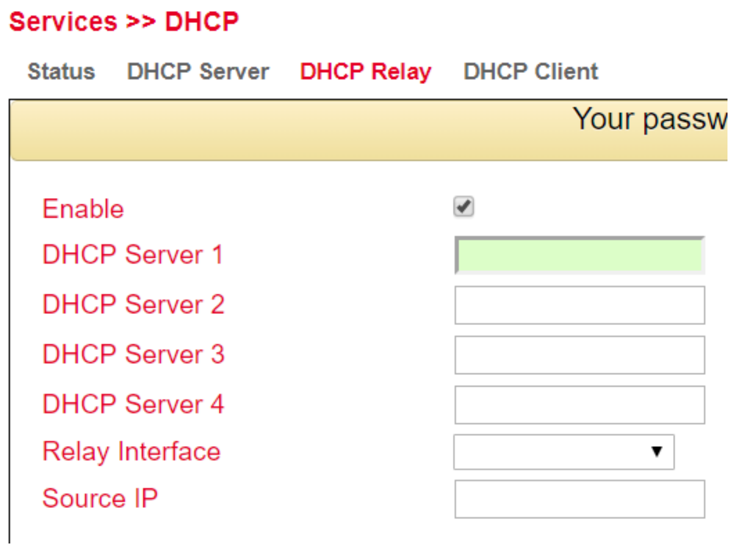
Static IP Settings

MAC Address	IP Address
0000.0000.0000	

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

3.3.1.3. DHCP Relay

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

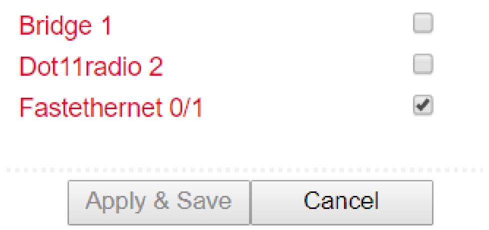


Services >> DHCP

Enable	☑
DHCP Server 1	
DHCP Server 2	
DHCP Server 3	
DHCP Server 4	
Relay Interface	▾
Source IP	

3.3.1.4. DHCP Client

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



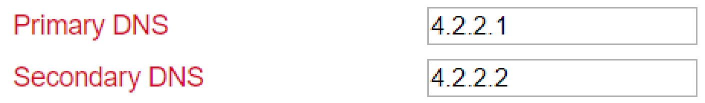
Bridge 1	□
Dot11radio 2	□
Fastethernet 0/1	☑

3.3.2. DNS

The **Domain Name System (DNS)** is one of the most important services in many IP-based networks. It´s main task is to answer questions about name resolution.
The DNS works works much like a phone assistance. The user knows the domain (name of a server on the Internet) e. g. welotec. com and sends it as a request to the Internet. The domain is then converted from the DNS into the corresponding IP address (if you want, the „connection number" on the Internet). For example, an IPv4 address of the form 192.168.2.1 and thus leads to the correct server.

3.3.2.1. DNS Server

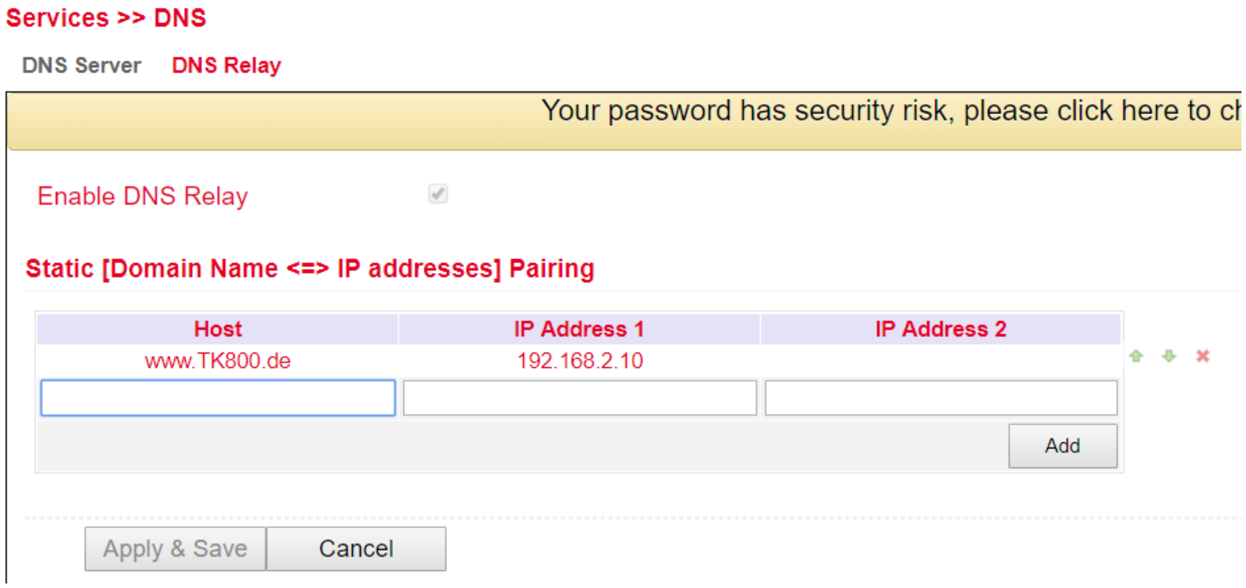
You can enter two DNS servers by choosing **Services > DNS > DNS Server**. These then apply to all interfaces, unless another DNS server was assigned via DHCP.



Primary DNS	4.2.2.1
Secondary DNS	4.2.2.2

3.3.2.2. DNS Relay

You can also manually enter DNS resolutions under **Services > DNS > DNS Relay**. By clicking on Add you add the entry and with Apply & Save you accept it.



Services >> DNS

Your password has security risk, please click here to ch

Enable DNS Relay ☑

Static [Domain Name <=> IP addresses] Pairing

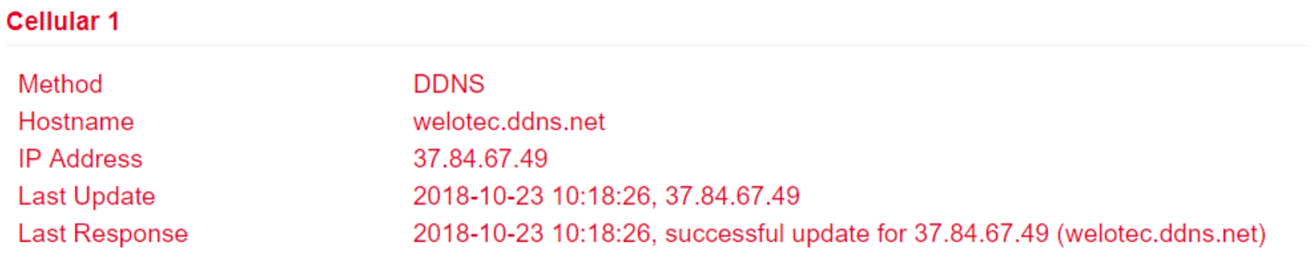
Host	IP Address 1	IP Address 2
www.TK800.de	192.168.2.10	

3.3.3. DDNS

Dynamic DNS or **DDNS** is a technique for dynamically updating domains in the Domain Name System (DNS). The purpose is that a computer (e. g. a PC or router) automatically and quickly changes the corresponding domain entry after changing its IP address. So, the computer is always accessible 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.

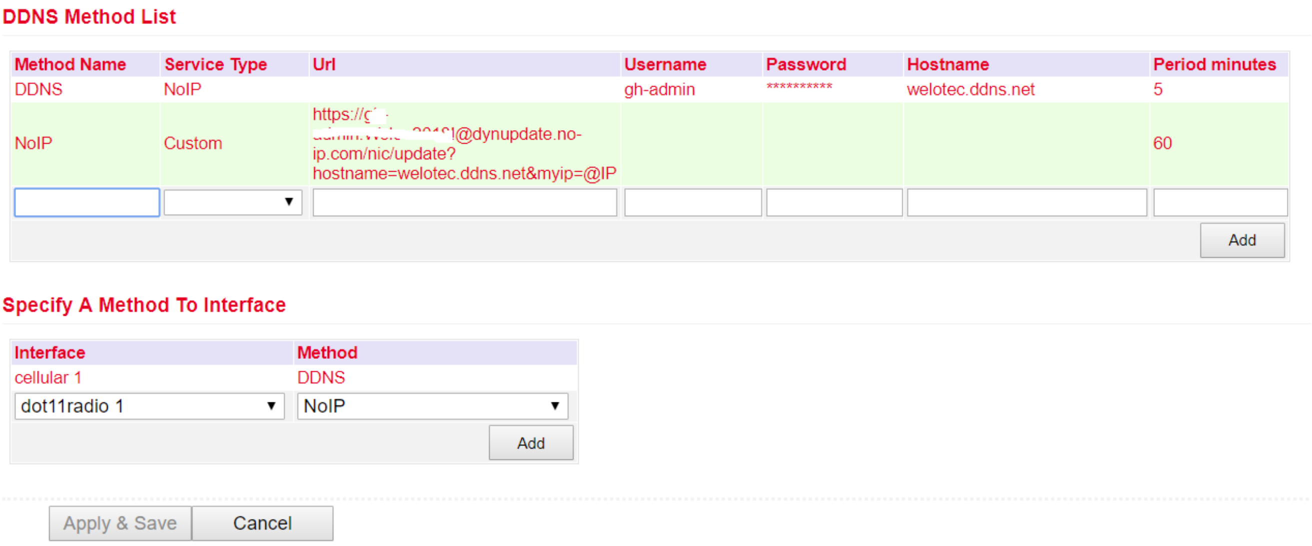


Cellular 1

Method	DDNS
Hostname	welotec.ddns.net
IP Address	37.84.67.49
Last Update	2018-10-23 10:18:26, 37.84.67.49
Last Response	2018-10-23 10:18:26, successful update for 37.84.67.49 (welotec.ddns.net)

3.3.3.2. DDNS

Under **Services > DDNS > DDNS** you can add a new DDNS service. It is important that you first create a new DDNS service under DDNS Method List.
Then you have to assign it to an interface, this is done under **Specify A Method To Interface**.



DDNS Method List

Method Name	Service Type	Url	Username	Password	Hostname	Period minutes
DDNS	NoIP		gh-admin	**********	welotec.ddns.net	5
NoIP	Custom	https://[redacted]@dynupdate.no- ip.com/nic/update? hostname=welotec.ddns.net&myip=@IP				60

Specify A Method To Interface

Interface	Method
cellular 1	DDNS
dot11radio 1	NoIP

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, you can use an individual DDNS service via Custom.
Url	Only used to select Custom for Service Type. The complete url of the DDNS service including username and password is then 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 used domain.
Period minutes	Specifies how often the IP address should be updated. Input values can be entered from 1 to 999999 minutes.

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

⚠ **Note**

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

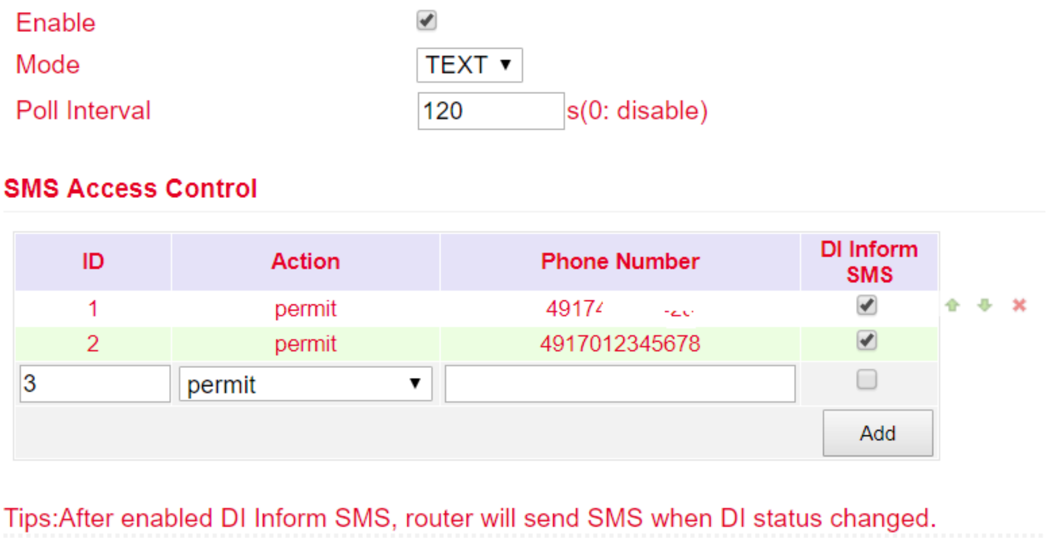
3.3.4. SMS

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

Status request / restart

1. Click on the menu point **Services** and then select the submenu **SMS**

2. Click on the Checkbox **Enable** to enable the function



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

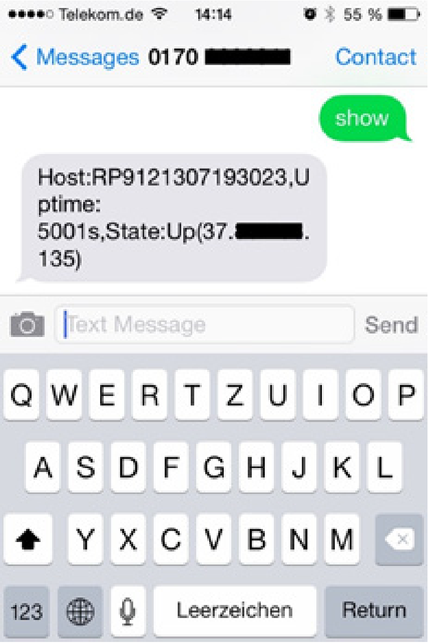
SMS Access Control

ID	Action	Phone Number	DI Inform SMS
1	permit	4917[redacted]	☑
2	permit	4917012345678	☑
3	permit ▾		□
			Add

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

3) In the **SMS Access Control** table, enter the phone numbers that may send SMS messages to the router (format 4917123456789, no 0049 or +49!) and enter the action **permit**.

If an SMS with the content **show** is sent to the router's mobile phone number, the router sends its current status as an answer.

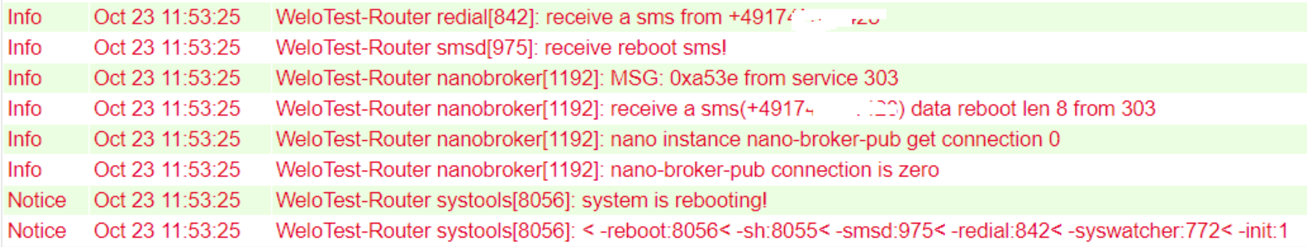


0170 [redacted]

show

Host:RP9121307193023,Uptime:
5001s,State:Up(37.[redacted].
135)

If an SMS containing the content **reboot** is sent to the router, it restarts. You can also trace this process in the log of the router.

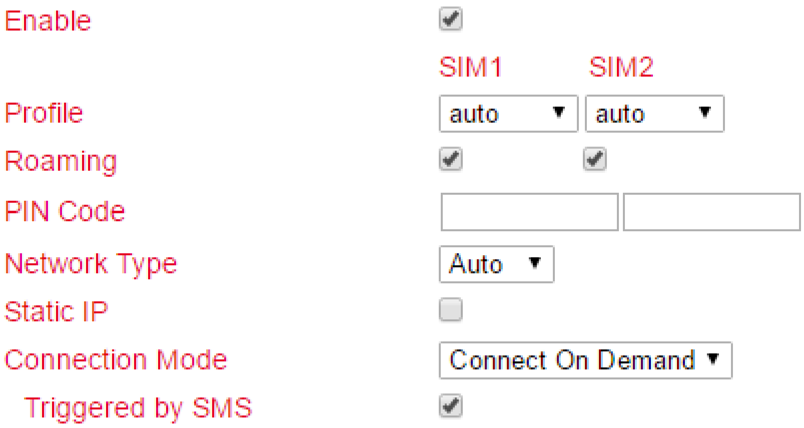


```
Info    Oct 23 11:53:25   WeloTest-Router redial[842]: receive a sms from +4917[redacted]
Info    Oct 23 11:53:25   WeloTest-Router smsd[975]: receive reboot sms!
Info    Oct 23 11:53:25   WeloTest-Router nanobroker[1192]: MSG: 0xa53e from service 303
Info    Oct 23 11:53:25   WeloTest-Router nanobroker[1192]: receive a sms(+4917[redacted]) 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
```

Establishing or disconnecting the Internet connection
After successful configuration, you can also control the router's Internet connection via SMS. For this, however, it is necessary that the router is set to „Connect On Demand"!

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

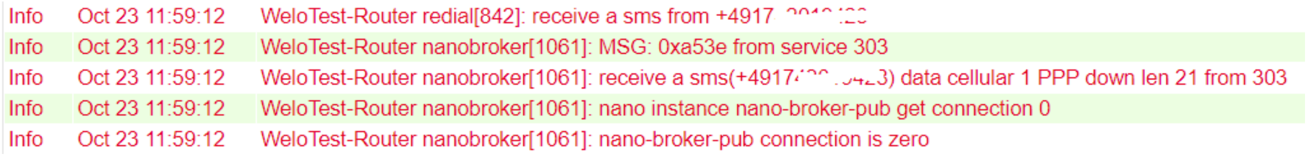
2. Now select the tab **Cellular**



	SIM1	SIM2
Enable	☑	
Profile	auto ▼	auto ▼
Roaming	☑	☑
PIN Code		
Network Type	Auto ▼	
Static IP	☐	
Connection Mode	Connect On Demand ▼	
Triggered by SMS	☑	

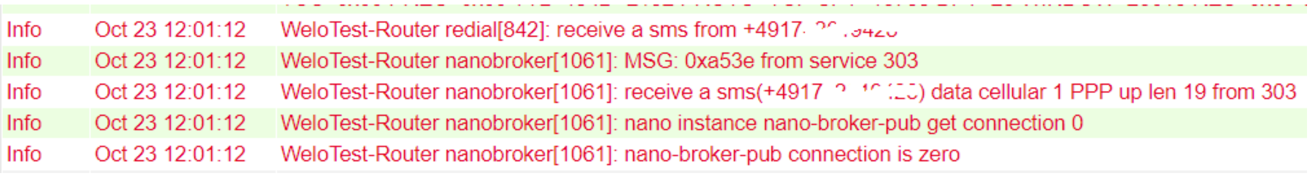
Select the mode **Connect On Demand** in the menu point **Connection Mode** and activate the field **Triggered by SMS**.

3. You can now send the following commands to the router via SMS:
cellular 1 ppp down - disconnects the internet connection (see picture)



```
Info   Oct 23 11:59:12   WeloTest-Router redial[842]: receive a sms from +4917[redacted]
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[redacted]3) 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
```

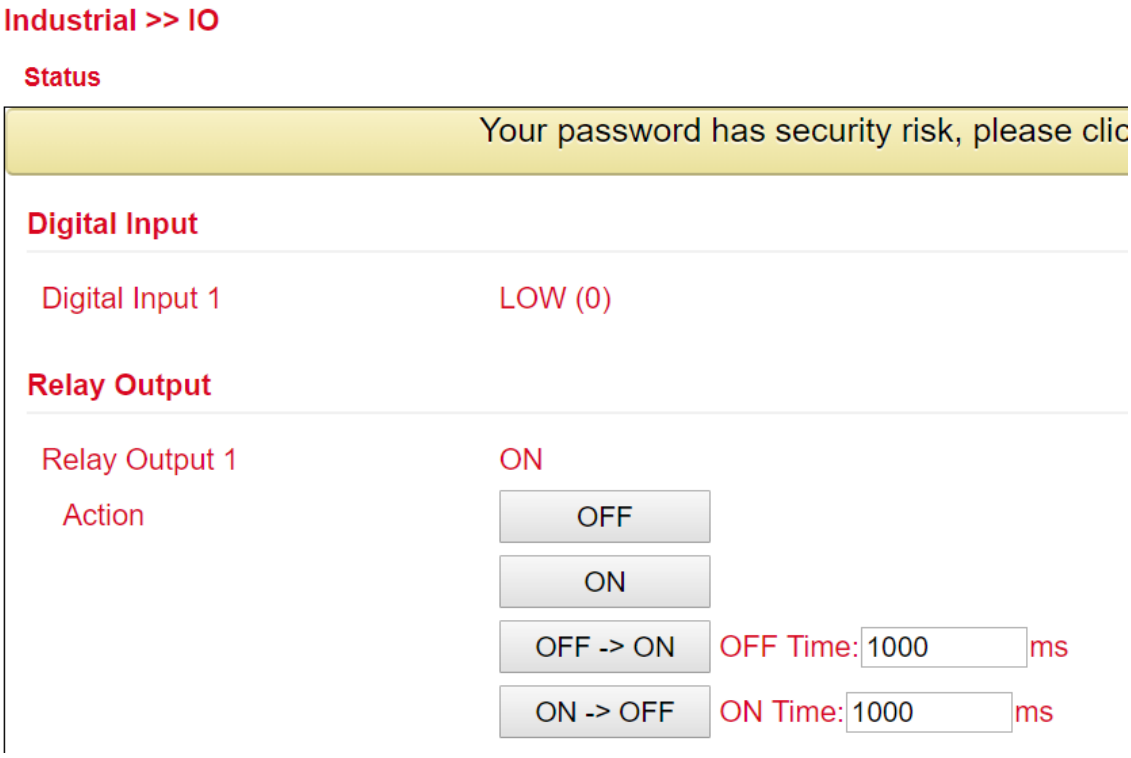
cellular 1 ppp up - restores the internet connection (s. picture)



```
Info   Oct 23 12:01:12   WeloTest-Router redial[842]: receive a sms from +4917[redacted]
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[redacted]) 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
```

Switching digital relay on or off

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



Industrial >> IO

Status

Your password has security risk, please clic

Digital Input

Digital Input 1 LOW (0)

Relay Output

Relay Output 1 ON

Action

OFF Time: 1000 ms

ON Time: 1000 ms

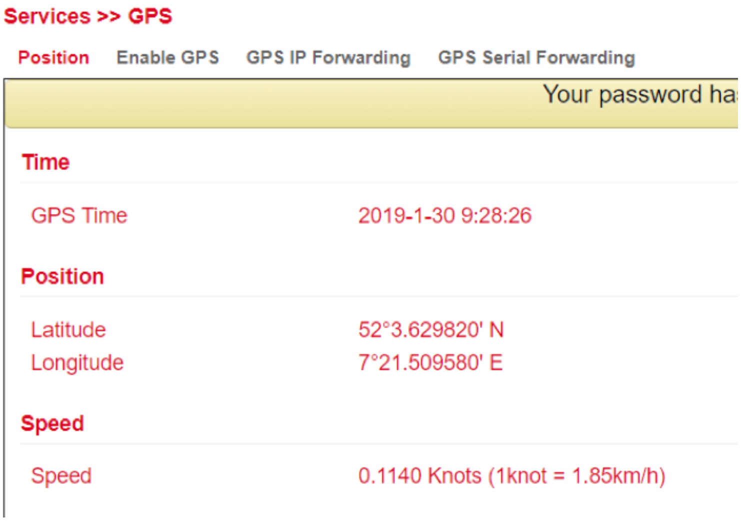
The following SMS commands can be used for this purpose

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

3.3.5. GPS (TK8x5-EGW)

3.3.5.1. Position

In the menu **Services** > **GPS** > **Position** the data for the current position are displayed, if the corresponding antenna is connected to the router.



Services >> GPS

Your password ha

Time

GPS Time 2019-1-30 9:28:26

Position

Latitude 52°3.629820' N

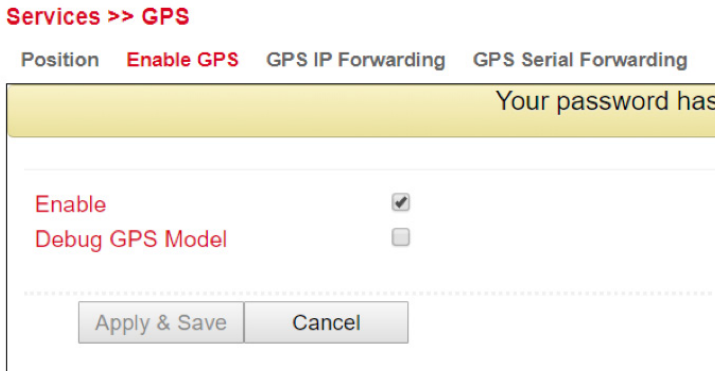
Longitude 7°21.509580' E

Speed

Speed 0.1140 Knots (1knot = 1.85km/h)

3.3.5.2. Enable GPS

To activate the GPS function of the router, open the menu under **Services** > **GPS** > **Enable GPS** and click on the checkbox **Enable** to activate the function. **Apply & Save** saves the settings and activates the GPS.

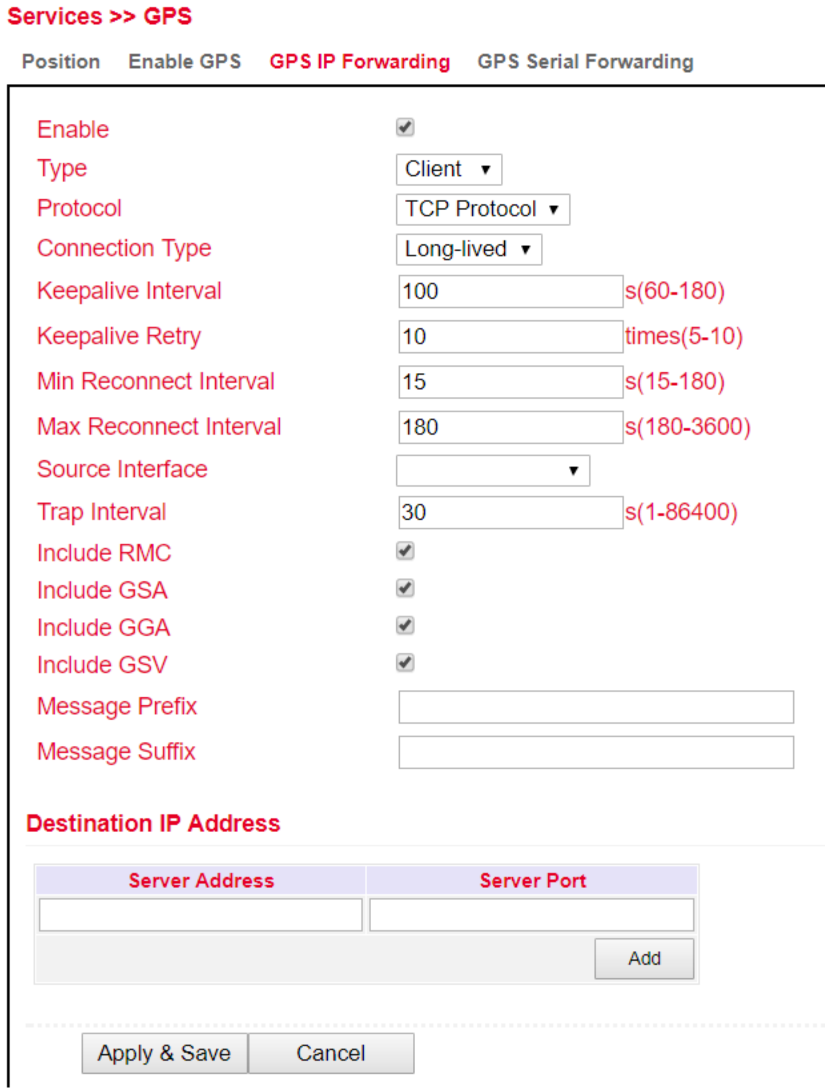


Your password has

Enable	☑
Debug GPS Model	□

3.3.5.3. GPS IP Forwarding

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

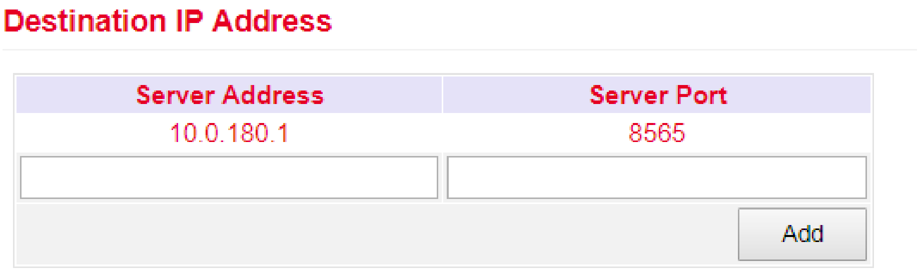


Enable	☑	
Type	Client ▾	
Protocol	TCP Protocol ▾	
Connection Type	Long-lived ▾	
Keepalive Interval	100	s(60-180)
Keepalive Retry	10	times(5-10)
Min Reconnect Interval	15	s(15-180)
Max Reconnect Interval	180	s(180-3600)
Source Interface	▾	
Trap Interval	30	s(1-86400)
Include RMC	☑	
Include GSA	☑	
Include GGA	☑	
Include GSV	☑	
Message Prefix		
Message Suffix		

Destination IP Address

Server Address	Server Port

GPS IP Forwarding List	
Type	Selection between Client and Server
Protocol	Here you can choose between TCP or UDP protocol types
Connection Type	Selection of Long-lived or Short-lived possible. Standard is long-lived
Keepalive Interval	Entry between 60 and 180 possible. Standard 100s
Keepalive Retry	The number of repetitions may be between 5 and 10 times. Standard = 10
Min Reconnect Interval	Min. Interval for Reconnection zw. 15 und 180 Seconds. Standard = 15s.
Max Reconnect Interval	Min. reconnection interval between 180 and 3600 seconds. Standard = 180s.
Source Interface	Selection of the corresponding interface to which you want to transfer data to
Trap Interval	The interval may be between 1 and 86400 seconds. Standard = 30
Include RMC	Recommended minimum data set. If selected, the minimum of the GPS receiver will be displayed.
Include GSA	Active satellites. Here, information about PRN numbers of the satellites whose signal is used for position determination is displayed
Include GGA	Most important dataset with time, position, altitude and quality of the measuremen
Include GSV	Visible satellites. Provides information about satellites that may be received at the moment and information about their position, signal strength, etc. Since only the information from four satellites can be transmitted per set (limited to 82 characters), there can be up to three such data sets.
Message Prefix	Input of a message Prefix possible. Free input
Message Suffix	Input of a message suffix possible. Free input

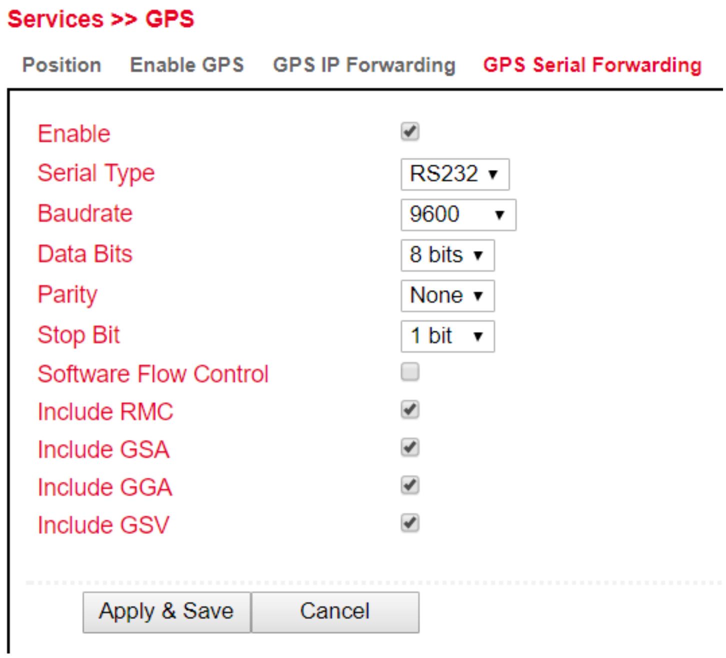

Destination IP Address

Server Address	Server Port
10.0.180.1	8565

You can enter a destination address for a server here.

3.3.5.4. GPS Serial Forwarding

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



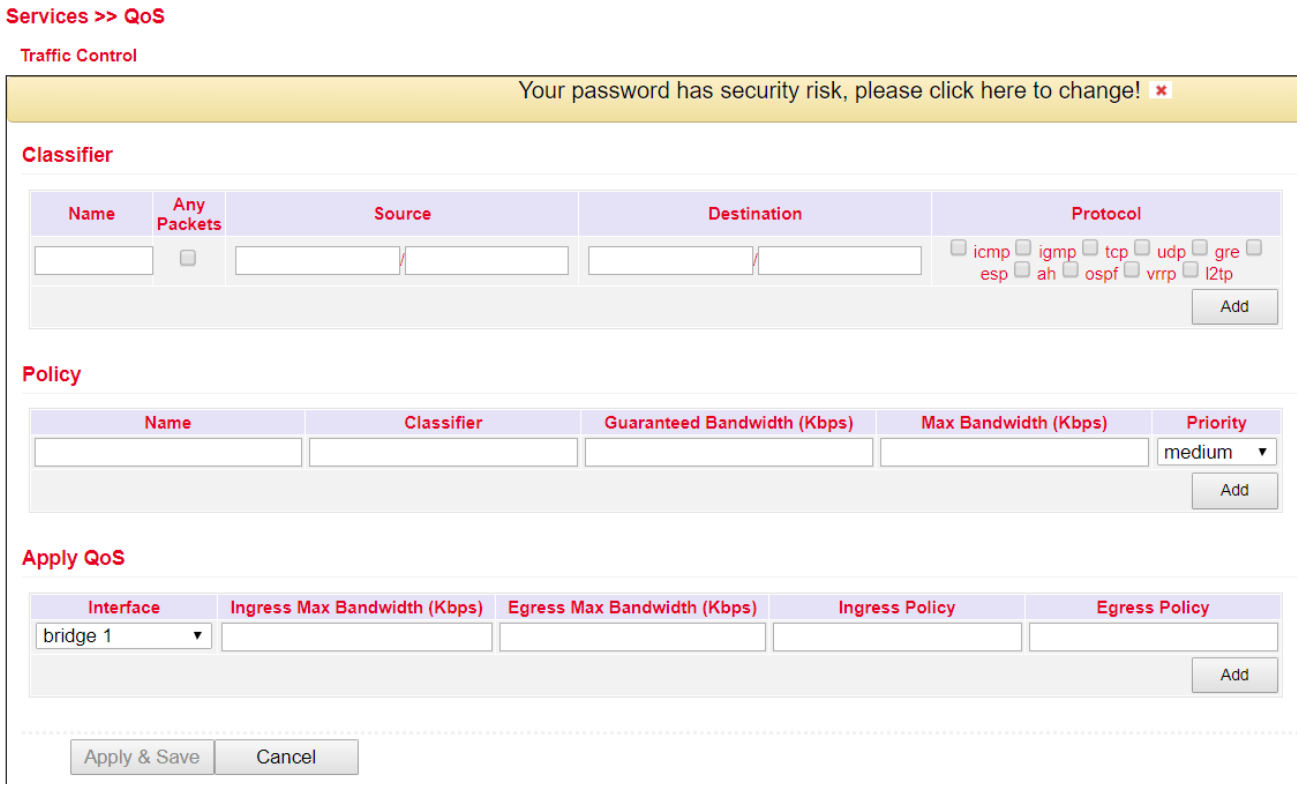
Services >> GPS

Enable	☑
Serial Type	RS232 ▾
Baudrate	9600 ▾
Data Bits	8 bits ▾
Parity	None ▾
Stop Bit	1 bit ▾
Software Flow Control	□
Include RMC	☑
Include GSA	☑
Include GGA	☑
Include GSV	☑

GPS Serial Forwarding List	
Serial Type	Selection of serial interfaces. RS232 or RS485.
Baudrate	Here the transmission rate can be selected. Value between 300 und 230400 is possible. Standard = 9600
Data Bits	Adjustment of data bits. Selection between 7 and 8 bits. Standard = 8 bits
Parity	Here the parity for the interface can be set. Standard = none
Stop Bit	Adjustment of the stop bits. Standard = 1 bit
Software Flow Control	Can be turned on or off. Stndard = Off
Include RMC	Recommended Minimum data set. If selected, the minimum of the GPS receiver will be displayed.
Include GSA	Active satellites. Here, information about PRN numbers of the satellites whose signal is used for position determination is displayed.
Include GGA	Most important dataset with time, position, altitude and quality of the measurement
Include GSV	Visible satellites. Provides information about satellites that may be received at the moment and about their position, signal strength, etc. Since only the information from four satellites can be transmitted per set (limited to 82 characters), there can be up to three such data sets.

3.3.6. QoS

At this point it is possible to define a Quality of Service. Choose **Services** > **QoS**



Services >> QoS

Traffic Control

Your password has security risk, please click here to change! ✖

Classifier

Name	Any Packets	Source	Destination	Protocol
	□	/	/	□ icmp □ igmp □ tcp □ udp □ gre □ esp □ ah □ ospf □ vrrp □ l2tp
				Add

Policy

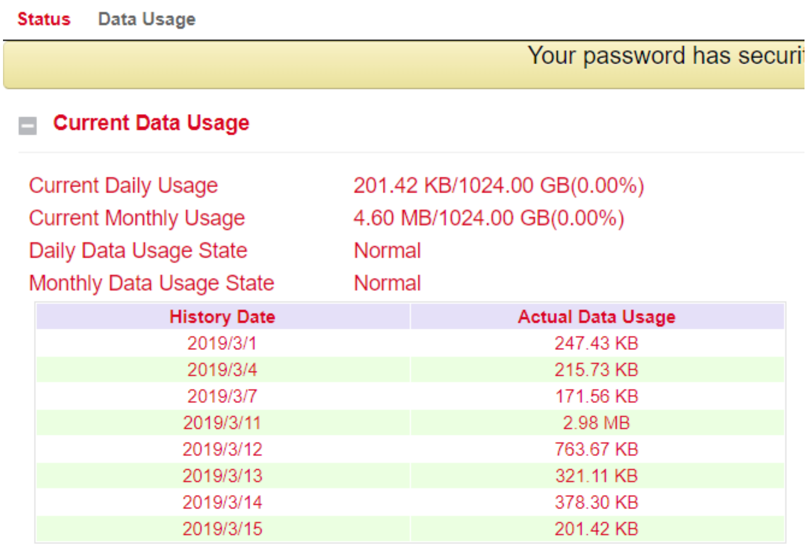
Name	Classifier	Guaranteed Bandwidth (Kbps)	Max Bandwidth (Kbps)	Priority
				medium ▼
				Add

Apply QoS

Interface	Ingress Max Bandwidth (Kbps)	Egress Max Bandwidth (Kbps)	Ingress Policy	Egress Policy
bridge 1 ▼				
				Add

3.3.7. Data Usage

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



Your password has securi

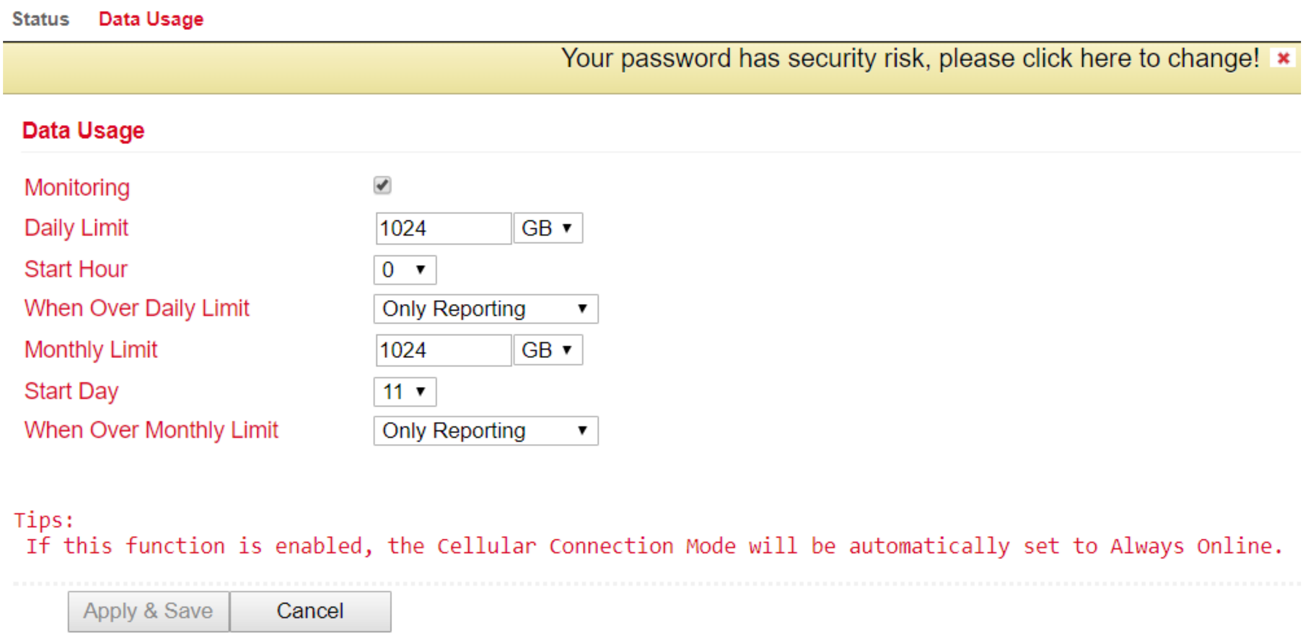
Current Data Usage

Current Daily Usage	201.42 KB/1024.00 GB(0.00%)
Current Monthly Usage	4.60 MB/1024.00 GB(0.00%)
Daily Data Usage State	Normal
Monthly Data Usage State	Normal

History Date	Actual Data Usage
2019/3/1	247.43 KB
2019/3/4	215.73 KB
2019/3/7	171.56 KB
2019/3/11	2.98 MB
2019/3/12	763.67 KB
2019/3/13	321.11 KB
2019/3/14	378.30 KB
2019/3/15	201.42 KB

3.3.7.1. Data Usage

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



Status
Data Usage
Your password has security risk, please click here to change!
Data Usage

Monitoring	☑
Daily Limit	1024 GB
Start Hour	0
When Over Daily Limit	Only Reporting
Monthly Limit	1024 GB
Start Day	11
When Over Monthly Limit	Only Reporting

```
Tips:
 If this function is enabled, the Cellular Connection Mode will be automatically set to Always Online.
```

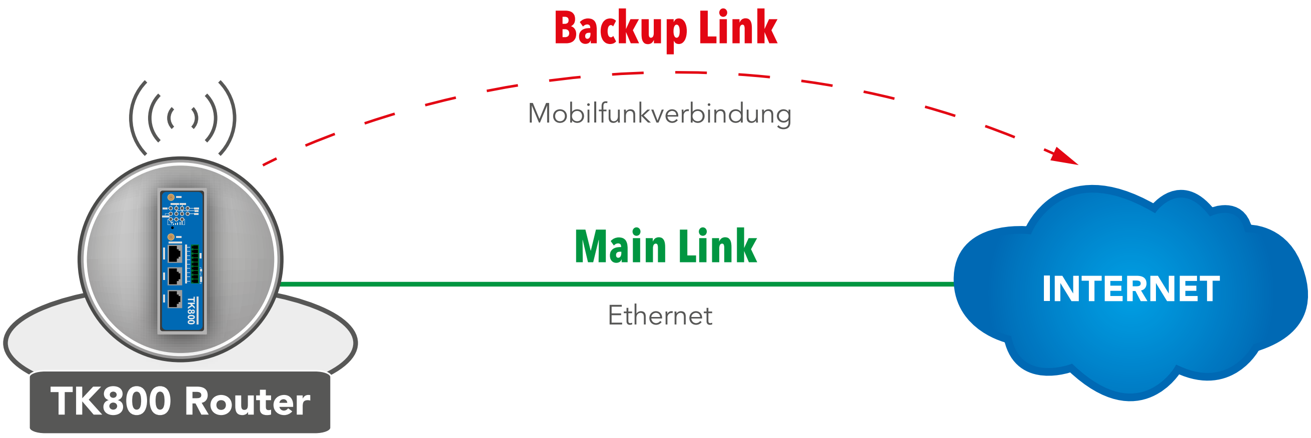
Data Usage	
Monitoring	Activate your data consumption display here
Daily Limit	Enter a guide value for the daily limit here. Information can be entered in KB, MB or GB.
Start Hour	Time at which the measurement is to be started.
When Over Daily Limit	Here you can enter what should happen if the entered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

3.4. Link Backup

With the TK800, it is possible to use two different Internet connections (cable-bound and mobile) to increase availability.

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

In this example, a cable-bound (Ethernet, DHCP) is used as primary and 4G LTE as secondary Internet connection.



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

⚠ **Note**

A prerequisite for Link Backup is Internet access via the mobile network. Therefore, configure the mobile 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.

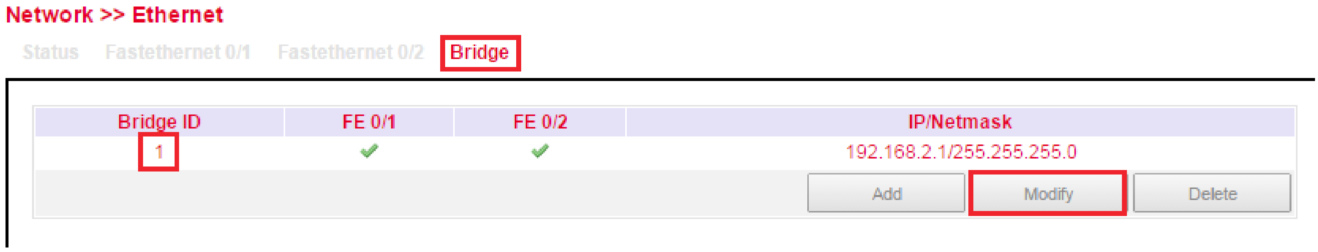
With the TK8X2-X, the two Ethernet ports are connected at the factory via a bridge. To configure one of the ports to the WAN port, the corresponding port must be excluded from the bridge.

To do this, follow the steps below:

1. Select from the menu **Network** and go to **Ethernet**

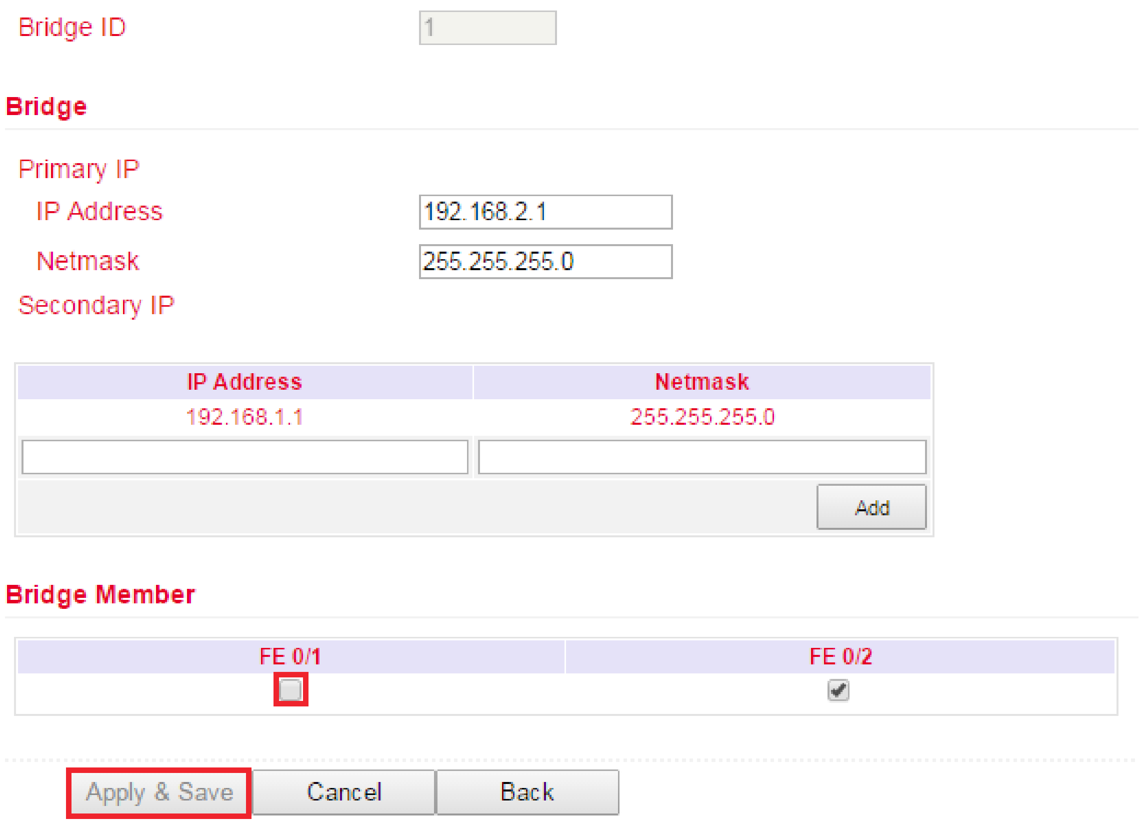
2. Choose the tab **Bridge**

3. Click in the line with the Bridge ID 1 and edit the entry by clicking on **Modify**



Bridge ID	FE 0/1	FE 0/2	IP/Netmask
1	✓	✓	192.168.2.1/255.255.255.0

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



Bridge ID: 1

Bridge

Primary IP

IP Address: 192.168.2.1

Netmask: 255.255.255.0

Secondary IP

IP Address	Netmask
192.168.1.1	255.255.255.0

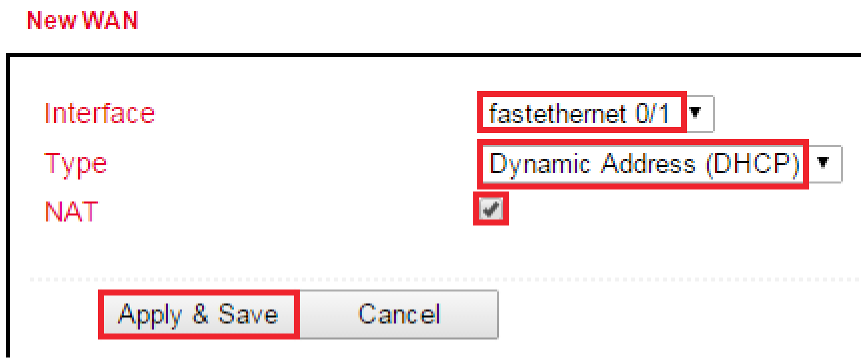
Bridge Member

FE 0/1	FE 0/2
□	☑

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.

- a new WAN port can be configured in the Wizard menu using the submenu New WAN
- the Ethernet port (FE 0/1) that has just been disconnected from the bridge is specified as the interface, DHCP is also used for the port as an example
- NAT must be activated if the connected devices should establish a connection to the Internet



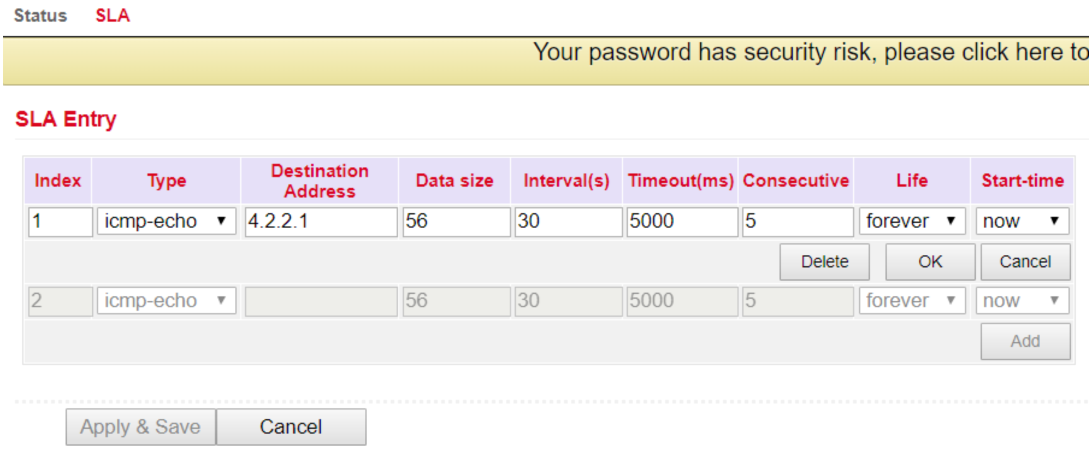
New WAN

Interface: fastethernet 0/1

Type: Dynamic Address (DHCP)

NAT: ☑

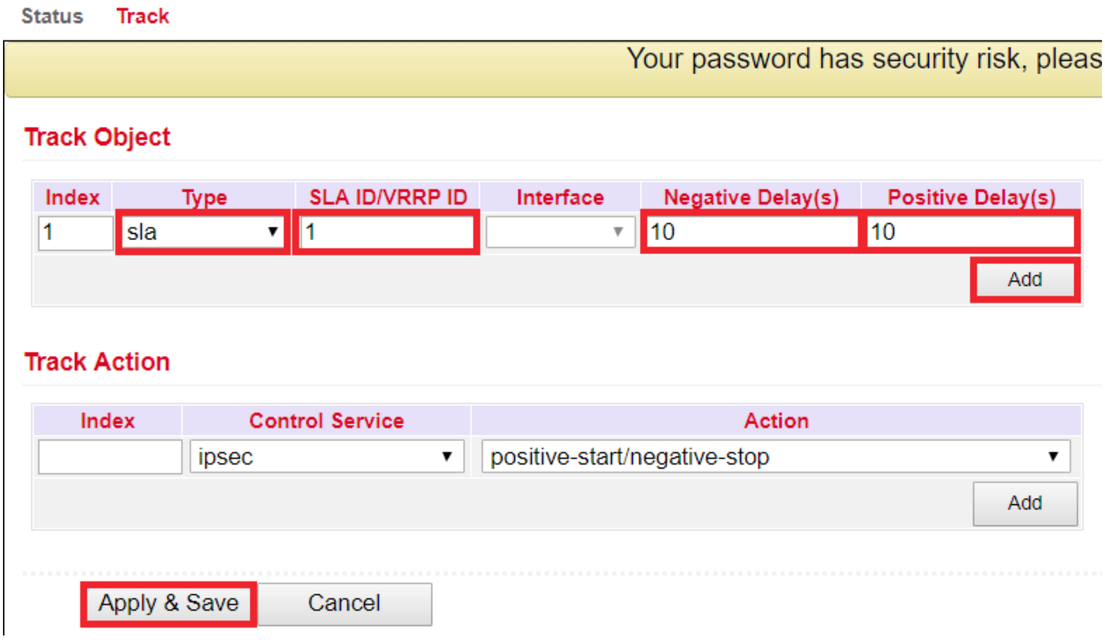
- the next step is to configure the ICMP program (SLA)
- under IP Address (Destination Address) a pingable IP address with high availability should be entered (Note: In this example 4.2.2.1 was entered, because this address has a very high availability).
- all other data can be taken from the example.



SLA Entry

Index	Type	Destination Address	Data size	Interval(s)	Timeout(ms)	Consecutive	Life	Start-time
1	icmp-echo	4.2.2.1	56	30	5000	5	forever	now
						Delete	OK	Cancel
2	icmp-echo		56	30	5000	5	forever	now
								Add

- the SLA program that has just been created is monitored with the help of tracking in order to register an interruption of the main line
- this is configured as in the following example



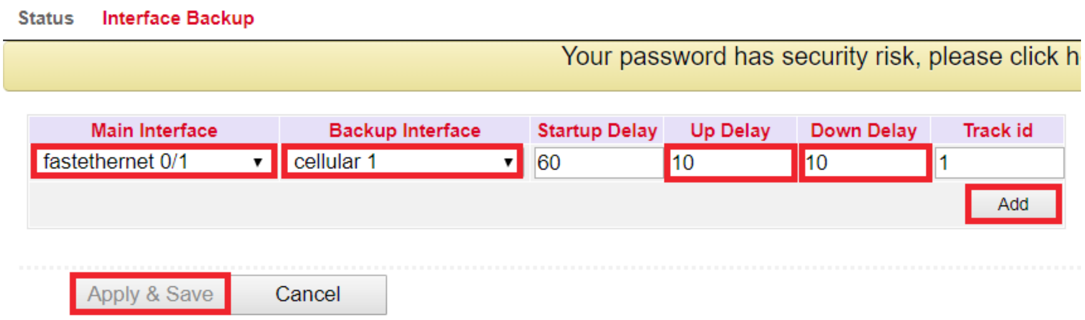
Track Object

Index	Type	SLA ID/VRRP ID	Interface	Negative Delay(s)	Positive Delay(s)
1	sla	1		10	10
					Add

Track Action

Index	Control Service	Action
	ipsec	positive-start/negative-stop
		Add

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



Main Interface	Backup Interface	Startup Delay	Up Delay	Down Delay	Track id
fastethernet 0/1	cellular 1	60	10	10	1
					Add

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 interface monitoring
Up Delay	Switching delay
Down Delay	Switching delay
Track ID	Reference to ICMP monitoring

in the last step, the routing data is created or adjusted as in the following example. It is important that the distance of the main line (here: FE 0/1) is smaller than that of the backup line. The TrackID links the main line to the ICMP monitoring created in the previous step.

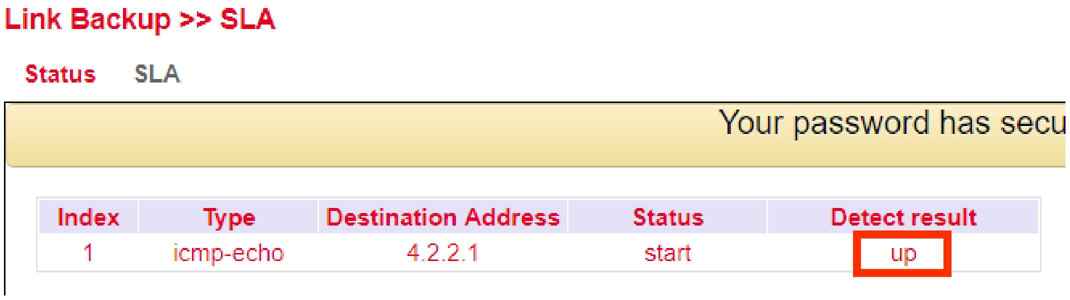
Configuration elements:

Destination	Destination address to be routed to
Netmask	Subnet mask belonging to the target address
Interface	Interface to be used for transmission
Gateway	IP-Address to be used for transmission
Distance	Preference/costs of the route
Track ID	Reference to ICMP supervision

Main line works (Internet connection via WAN)

In case the main line works and an internet connection is established, the following can be traced:

1. SLA-Status

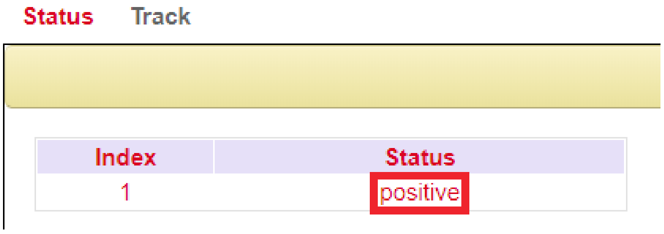


Link Backup >> SLA

Your password has secu

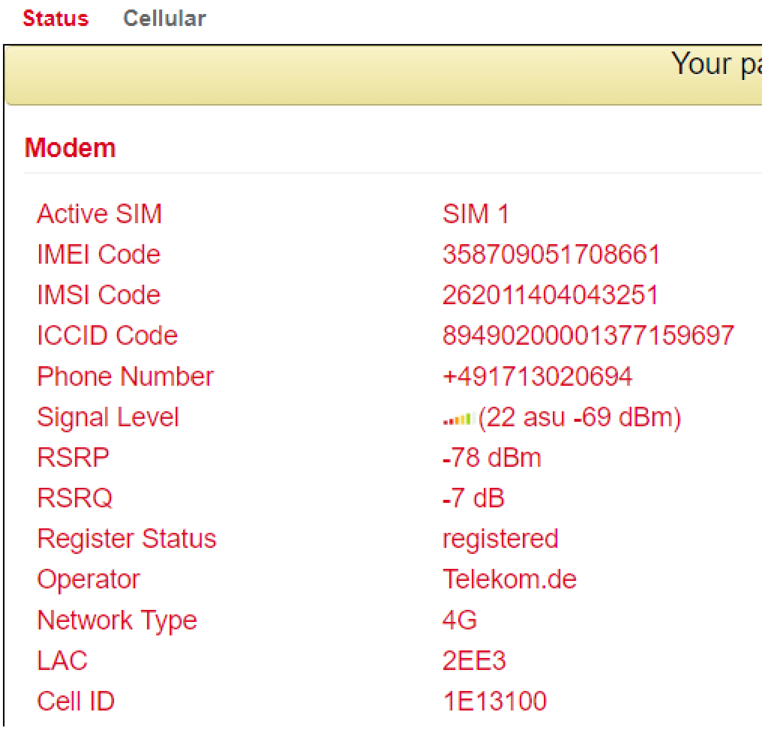
Index	Type	Destination Address	Status	Detect result
1	icmp-echo	4.2.2.1	start	up

2. Track-Status



Index	Status
1	positive

3. Status of mobile connection

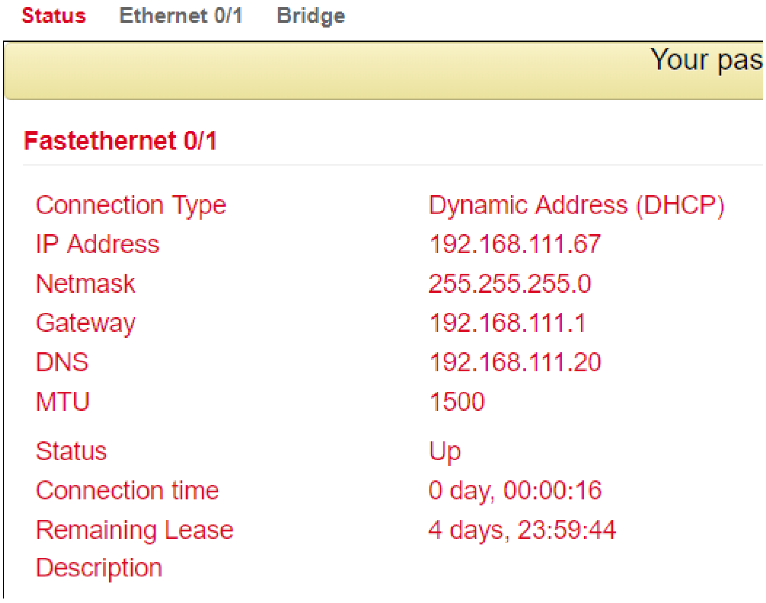


Your pa

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 WAN-Connection (Ethernet)

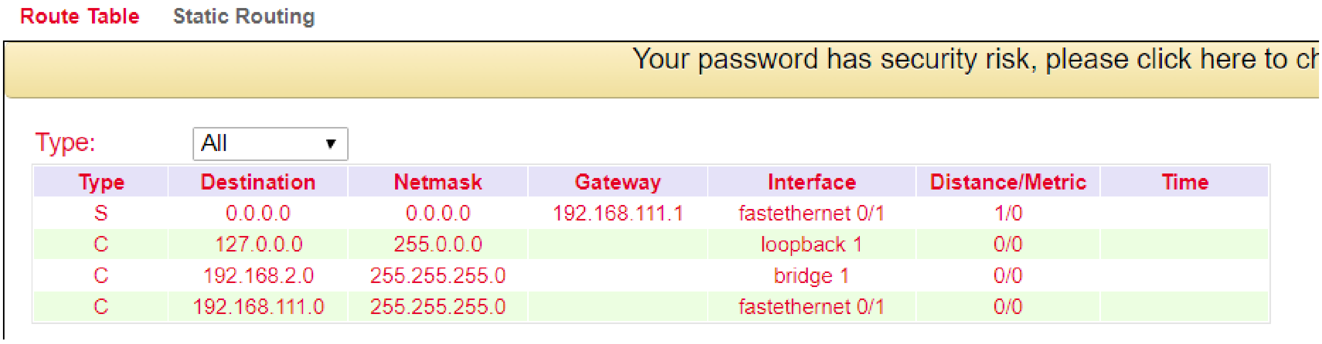


Your pas

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



Your password has security risk, please click here to ch

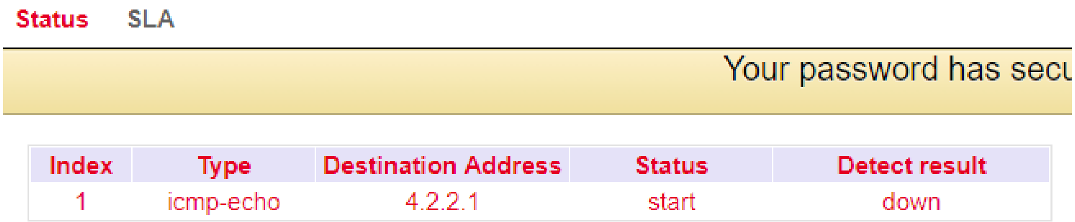
Type: All

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 mobile)

If the main line does not work and an Internet connection is established via the cellular interface, the following can be understood:

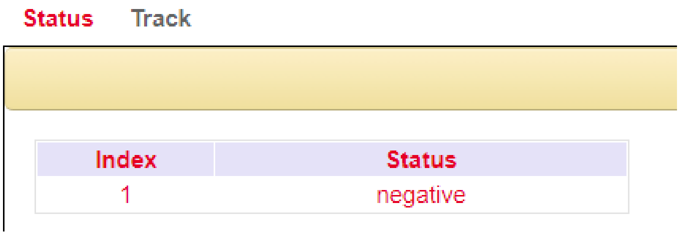
1. SLA-Status



Your password has secu

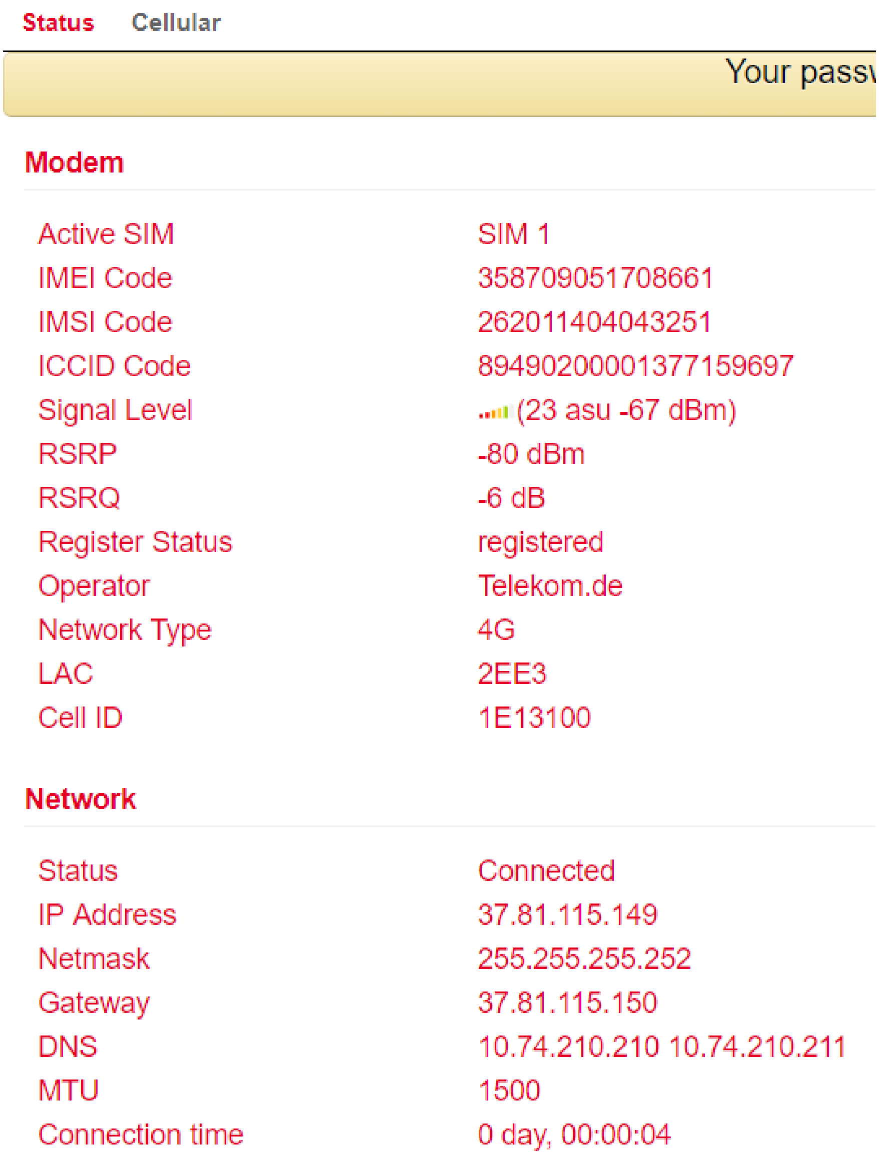
Index	Type	Destination Address	Status	Detect result
1	icmp-echo	4.2.2.1	start	down

2. Track-Status



Index	Status
1	negative

3. Status of mobile connection



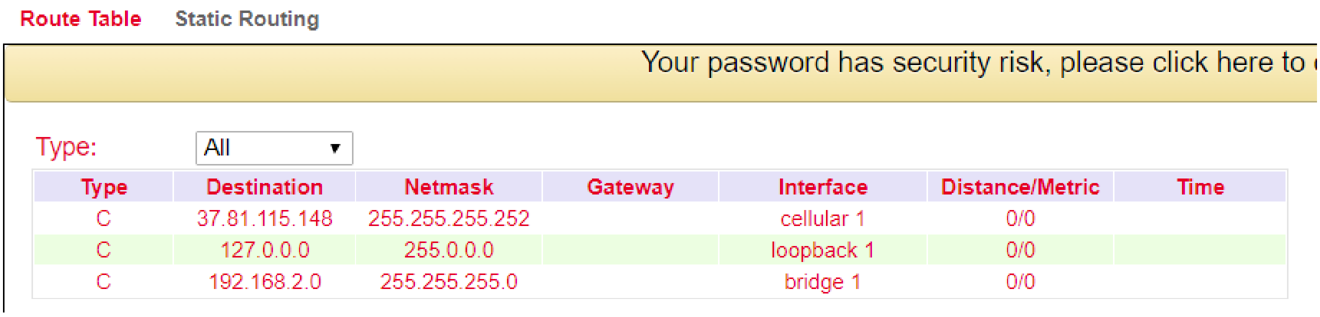
Modem

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



Type: All ▾

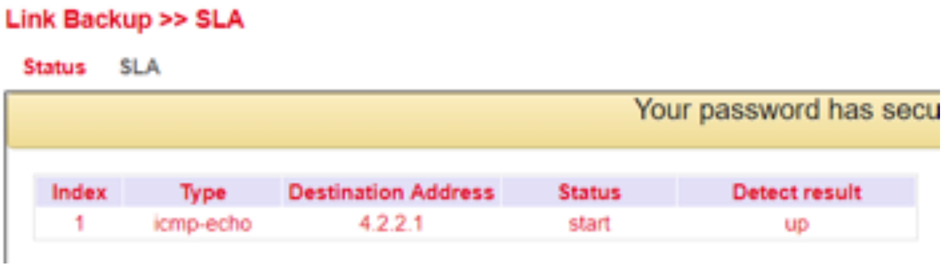
Type	Destination	Netmask	Gateway	Interface	Distance/Metric	Time
C	37.81.115.148	255.255.255.252		cellular 1	0/0	
C	127.0.0.0	255.0.0.0		loopback 1	0/0	
C	192.168.2.0	255.255.255.0		bridge 1	0/0	

3.4.1. SLA

SLA monitoring monitors the connections to remote sites within a network structure. Ping tests for defined targets indicate the availability of the peers and show the status of the line (up or down).

3.4.1.1. Status

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



Link Backup >> SLA

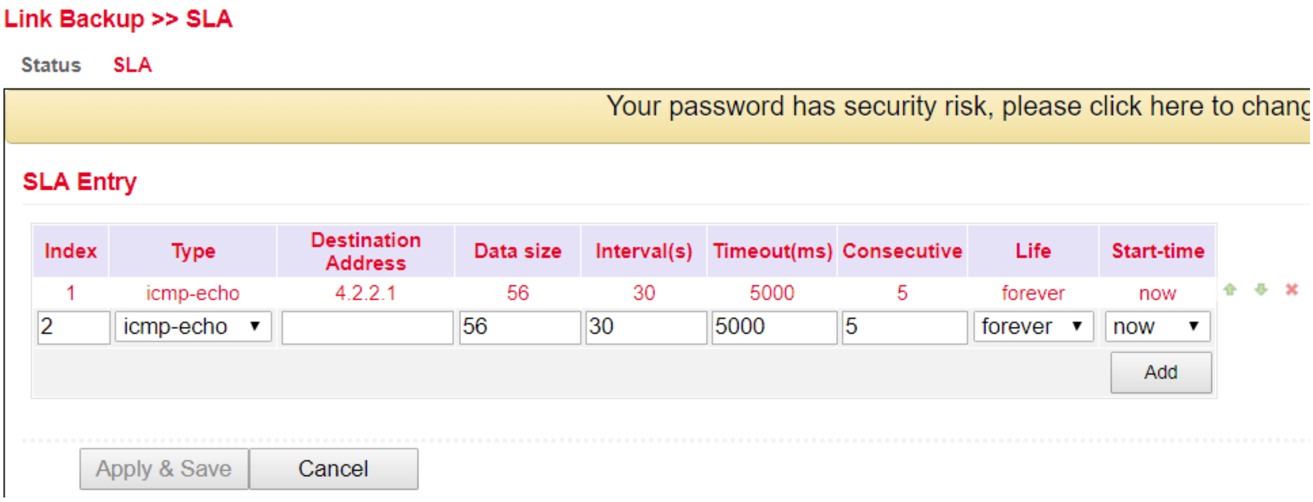
Status SLA

Your password has secu

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

3.4.1.2. SLA Configuration

Under **Link Backup** > **SLA** > **SLA**, enter the required data to monitor the status of the line.



Link Backup >> SLA

Status SLA

Your password has security risk, please click here to chang

SLA Entry

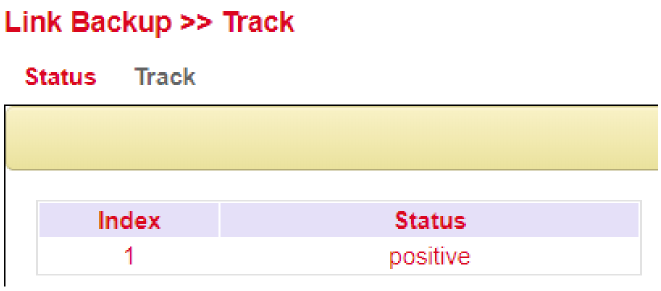
Index	Type	Destination Address	Data size	Interval(s)	Timeout(ms)	Consecutive	Life	Start-time
1	icmp-echo	4.2.2.1	56	30	5000	5	forever	now
2	icmp-echo ▼		56	30	5000	5	forever ▼	now ▼

Parameter	Meaning
Index	Freely selectable, used for the Identification of the listing.
Type	icmp-echo, a simple ping to check the connection.
Destination Address	The address being pinged. If possible, it should be highly available, e. g. a Google DNS server (8.8.8.8.8).
Data size	The packet size of a ping, usually 56 bytes.
Interval(s)	The time interval in seconds in which the ping is executed.
Timeout(ms)	Timeout for a ping.
Consecutive	Number of repetitions, 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. 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 status track via **Link Backup** > **Track** > **Status** if it is configured.

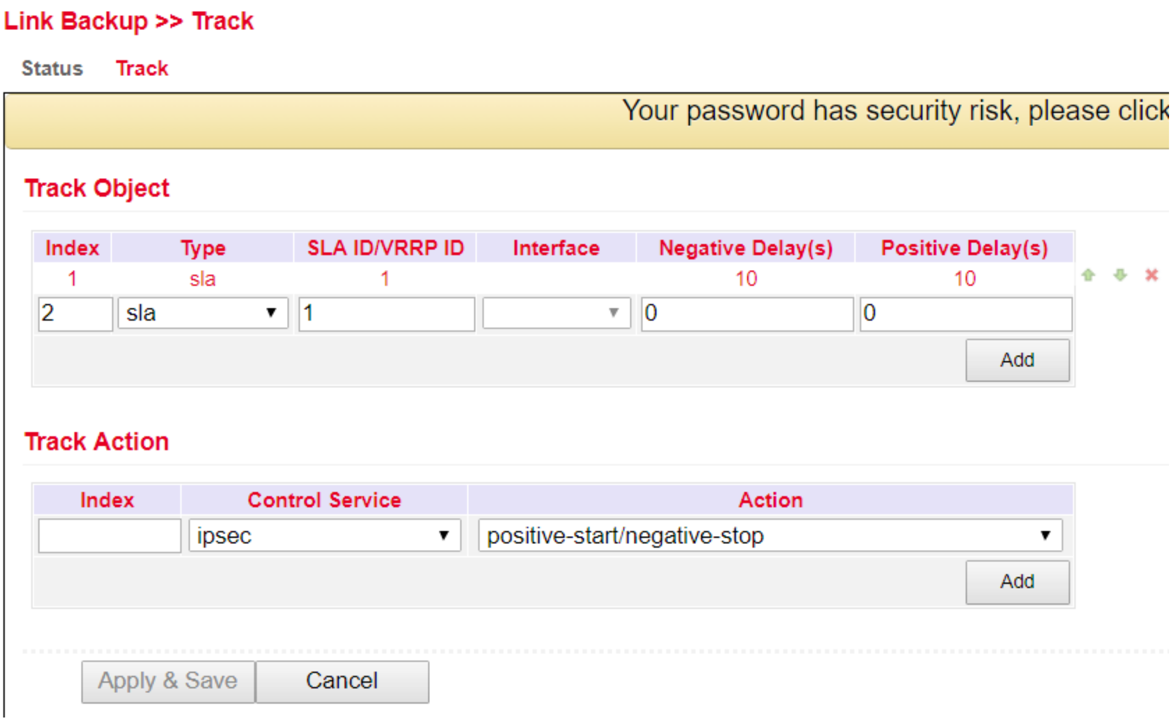


Link Backup >> Track

Index	Status
1	positive

3.4.2.2. Track Configuration

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



Link Backup >> Track

Track Object

Index	Type	SLA ID/VRRP ID	Interface	Negative Delay(s)	Positive Delay(s)
1	sla	1		10	10
2	sla ▼	1	▼	0	0

Track Action

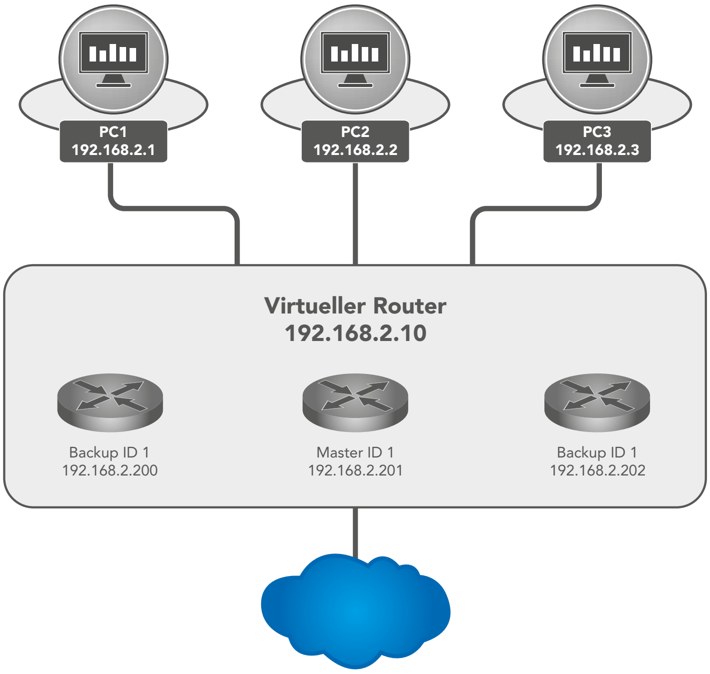
Index	Control Service	Action
	ipsec ▼	positive-start/negative-stop ▼

Parameter	Meaning
Index	Freely selectable. Identifies the entry.
Type	SLA or interface.
SLA ID	Index of the SLA that was previously created.
Interface	Not used for SLA.
Negative Delay(s)	Delay when switching to the backup interface when 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. VRRP

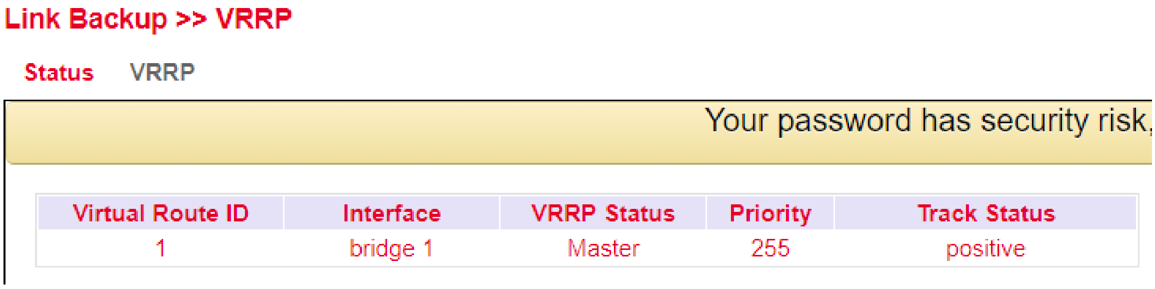
In a network, all subscribers have a common gateway for communication with other networks. If this gateway fails, communication with other networks (and the Internet) is no longer possible.

For this reason, the **Virtual Router Redundancy Protocol (VRRP)** is available. This makes it possible to operate several routers (gateways) in parallel, but only one is always active (master). The other routers serve as backup if the master fails. All routers together represent a virtual router. Within this virtual router, VRRP controls the communication, so that in case of a failure of the master, 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.

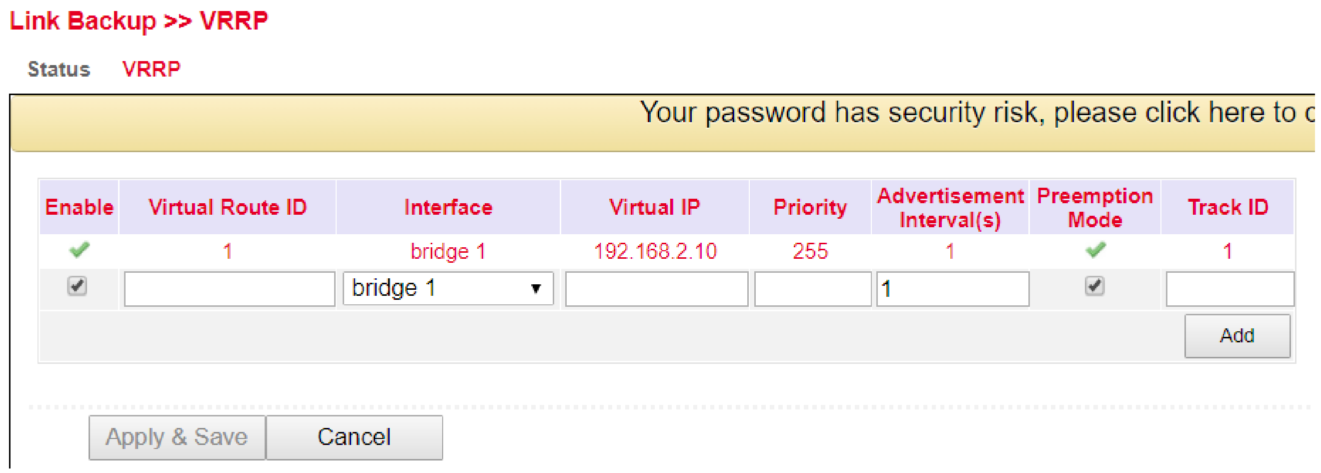


Your password has security risk,

Virtual Route ID	Interface	VRRP Status	Priority	Track Status
1	bridge 1	Master	255	positive

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

3.4.3.2. VRRP Configuration



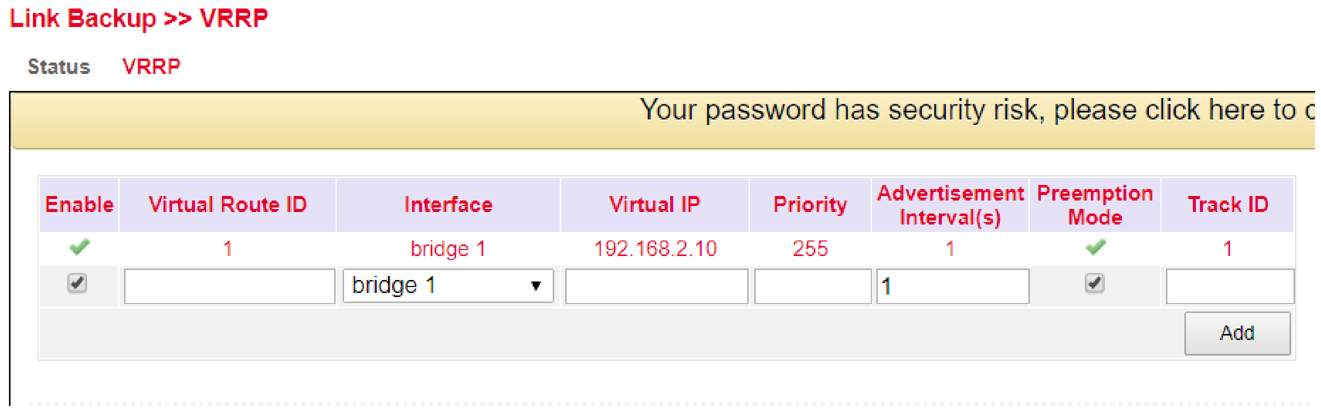
Link Backup >> VRRP

Your password has security risk, please click here to c

Enable	Virtual Route ID	Interface	Virtual IP	Priority	Advertisement Interval(s)	Preemption Mode	Track ID
✓	1	bridge 1	192.168.2.10	255	1	✓	1
☑		bridge 1 ▾			1	☑	

Parameter	Description
Enable	Turns the Configuration on or off
Virtual Route ID	Freely selectable, specifies the Virtual Router Group. Must be identical for all routers within the group
Interface	Das 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.
Advertisement Interval(s)	Check time within the group to find out who the Master is.
Preemption Mode	If switched on, the router will automatically check if the priority is higher than that of the current master. If it´s like that, it causes it to become the master itself 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 set up a track under **Link Backup > Track**. Then configure **Router A** via **Link Backup > VRRP > VRRP** as shown in figure 1.



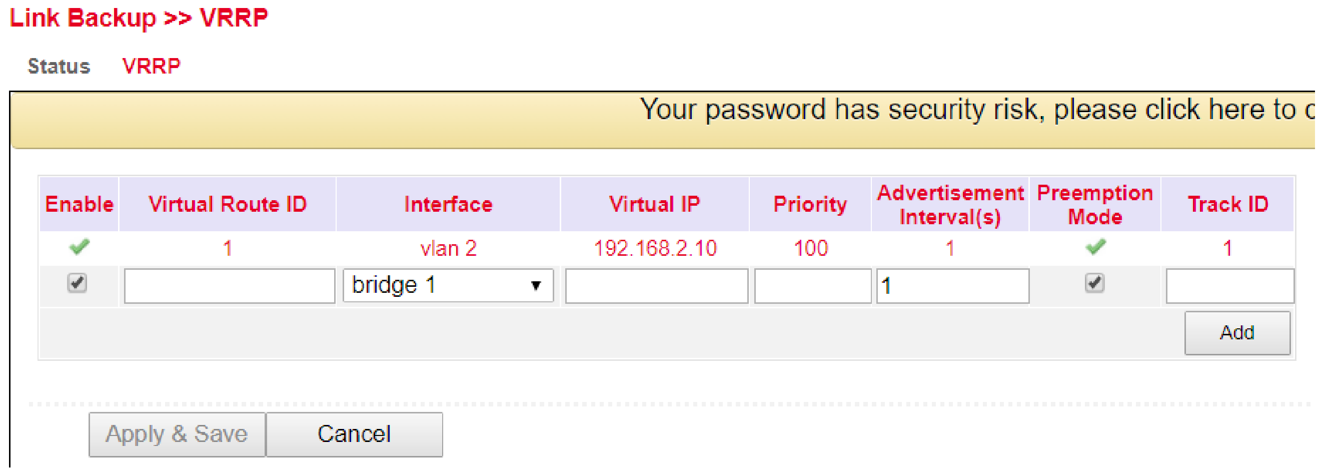
Link Backup >> VRRP

Your password has security risk, please click here to c

Enable	Virtual Route ID	Interface	Virtual IP	Priority	Advertisement Interval(s)	Preemption Mode	Track ID
✓	1	bridge 1	192.168.2.10	255	1	✓	1
☑		bridge 1 ▾			1	☑	

Illustration 1 (Interface may vary depending on router modell)

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



Link Backup >> VRRP

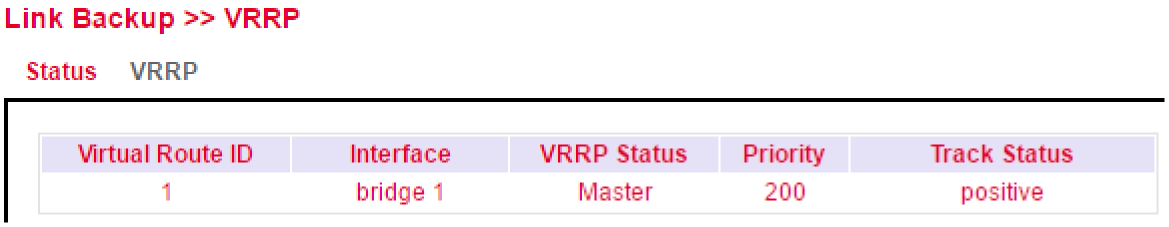
Your password has security risk, please click here to c

Enable	Virtual Route ID	Interface	Virtual IP	Priority	Advertisement Interval(s)	Preemption Mode	Track ID
✓	1	vlan 2	192.168.2.10	100	1	✓	1
☑		bridge 1 ▾			1	☑	

Illustration 2 (interface may vary depending on router model)

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

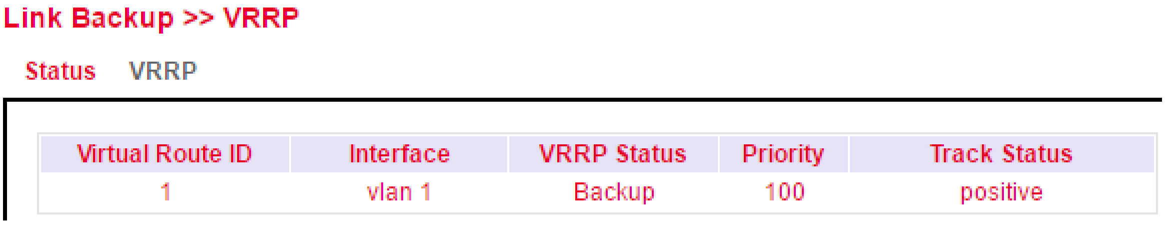
Router A



Link Backup >> VRRP

Virtual Route ID	Interface	VRRP Status	Priority	Track Status
1	bridge 1	Master	200	positive

Router B

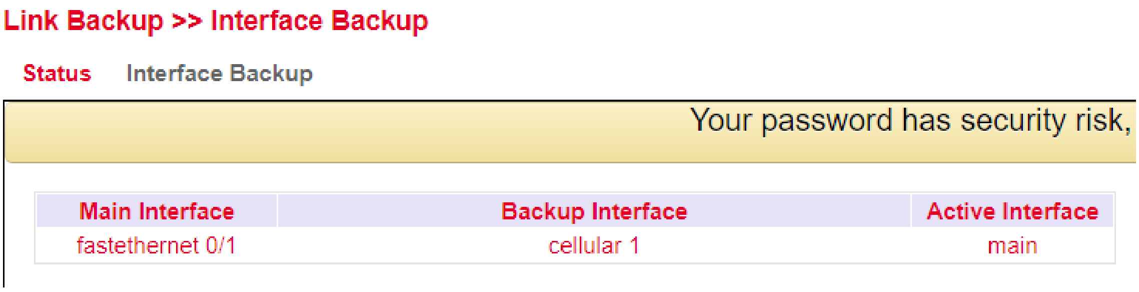


Link Backup >> VRRP

Virtual Route ID	Interface	VRRP Status	Priority	Track Status
1	vlan 1	Backup	100	positive

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 reached under **Link Backup** > **Interface Backup**.



Link Backup >> Interface Backup

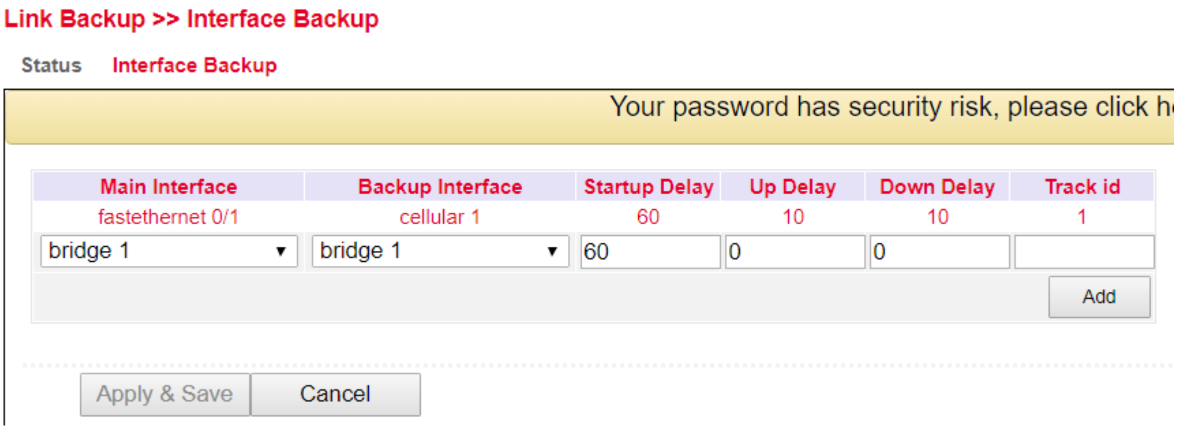
Status Interface Backup

Your password has security risk,

Main Interface	Backup Interface	Active Interface
fastethernet 0/1	cellular 1	main

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 the backup interface.



Link Backup >> Interface Backup

Status Interface Backup

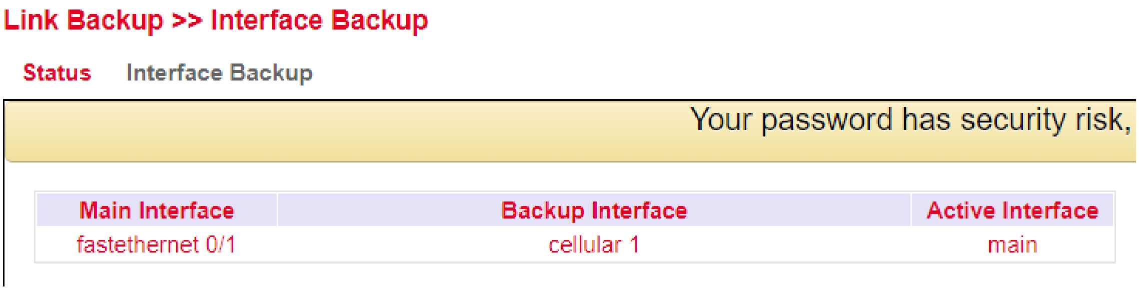
Your password has security risk, please click h

Main Interface	Backup Interface	Startup Delay	Up Delay	Down Delay	Track id
fastethernet 0/1	cellular 1	60	10	10	1
bridge 1 ▾	bridge 1 ▾	60	0	0	

Parameter	Meaning
Main Interface	Here the main interface is defined.
Backup Interface	Here the backup interface is defined.
Startup Delay	Delay in seconds at system startup.
Up Delay	Delay in switching from the backup interface to the main interface.
Down Delay	Delay in switching from the main interface to the backup interface.
Track ID	The track index of 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).



Link Backup >> Interface Backup

Your password has security risk,

Main Interface	Backup Interface	Active Interface
fastethernet 0/1	cellular 1	main

3.5. Routing

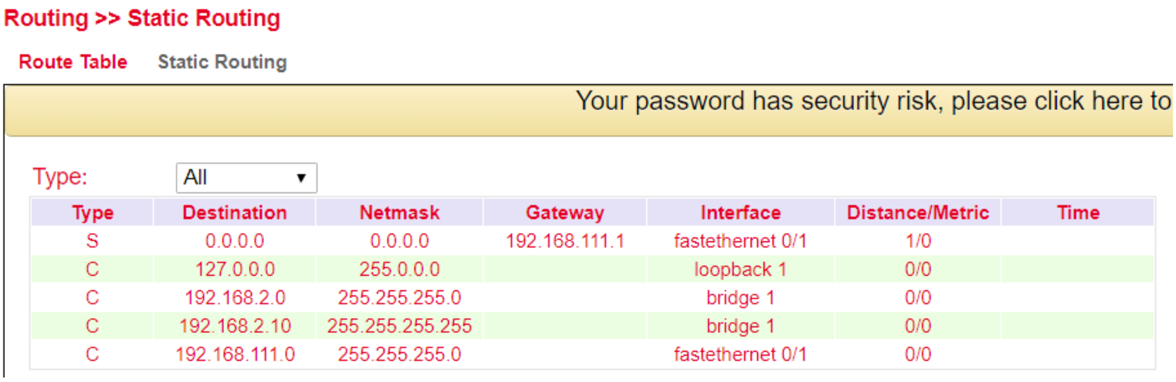
Routing is a generic term for the router-controlled transport of data packets between different networks. On the Internet, the data packets can take completely different paths, since there are no direct connections between computers on the Internet. The destination of the data is contained in the header. Only at the receiver, the data packets are reassembled correctly. Routing makes data traffic very flexible and failsafe.

3.5.1. Static Routing

Static routing is based, as the name indicates, on a fixed specification of the path between two arbitrary end systems. The default is taken during the installation of a network and is usually stored as a fixed routing table in the router. The end devices are each assigned to a router through which they are reachable and can reach other destinations. Accessible 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



Routing >> Static Routing

Route Table Static Routing

Your password has security risk, please click here to

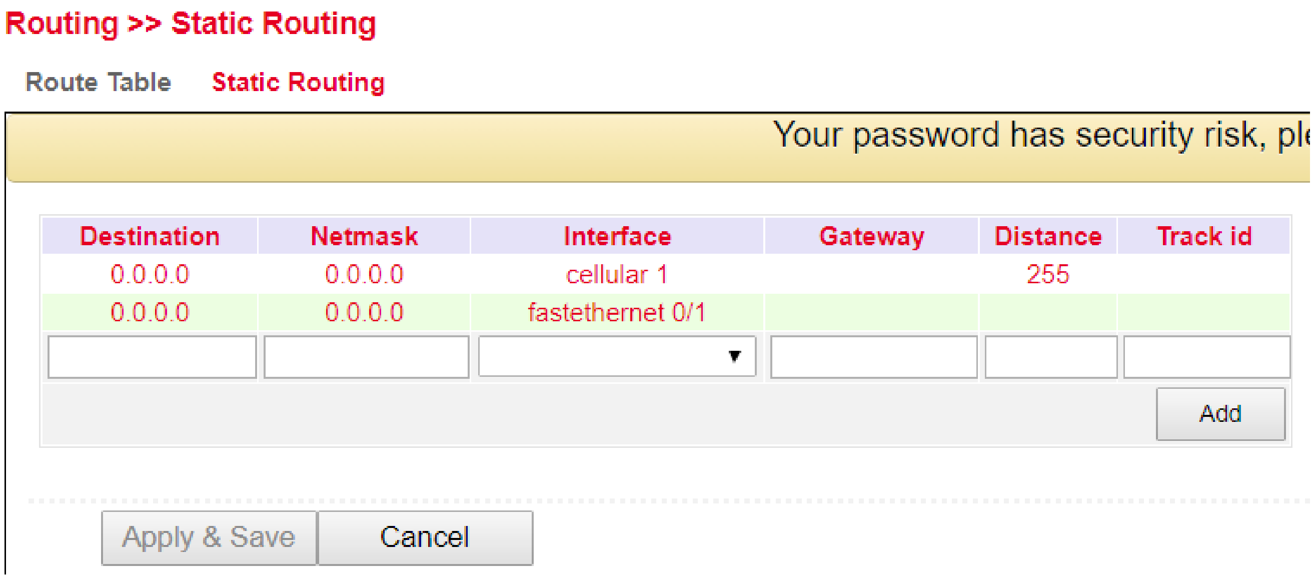
Type: All ▼

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	192.168.2.10	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, they are automatically taken over into a routing table when an interface is configured with an IP address • S = Static route / route entered manually by the administrator • R = RIP (Routing Information Protocol) / dynamic route added through RIP • O = OSPF (Open Shortest Path First) / dynamic route added through OSPF
Destination	The destination is the destination host, subnet address, network address or default route. The target for a default route is 0.0.0.0.
Netmask	The network mask is used together with the destination to determine when a route is used. For example, a host route has the mask 255.255.255.255, a default route has the mask 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 has to be sent.
Interface	The interface is the network interface that should be used to get to the next router. Cellular 1 = GSM radio interface Loopback 1 = internal loopback address (loopback circuit) FastEthernet 0/1 = Network port FastEthernet 0/1 on the router VLAN 1 = Network ports which are assigned to the VLAN 1.
Distance/ Metric	Distance/Metrik is the priority of the route. If multiple routes lead to the same destination, the route with the lowest metric is the best route.
Time	Time

3.5.1.2. Static Routing

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



Routing >> Static Routing

Route Table Static Routing

Your password has security risk, ple

Destination	Netmask	Interface	Gateway	Distance	Track id
0.0.0.0	0.0.0.0	cellular 1		255	
0.0.0.0	0.0.0.0	fastethernet 0/1			

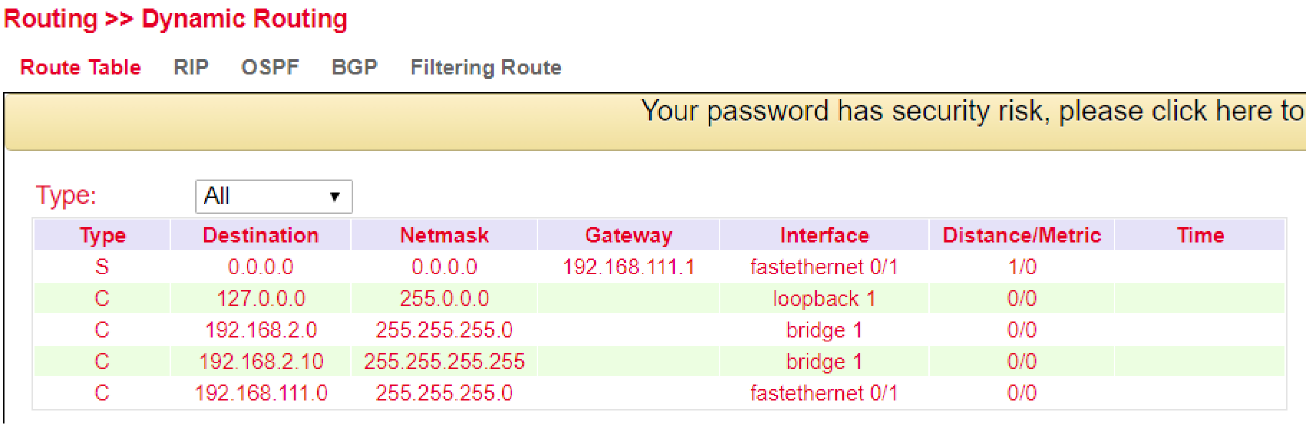
Parameter	Description
Destination	The destination is the destination host, subnet address, network address or default route. The target for a default route is 0.0.0.0.
Netzmask	The network mask is used together with the destination to determine when a route is used. For example, a host route has the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

3.5.2. Dynamic Routing

Dynamic routing is used to automatically route routes from the routing protocol used. The advantage of dynamic routing over static routing is that the route selection takes place dynamically during operation. Routes are learned and set automatically by the routing protocol algorithm.

3.5.2.1. Route Table

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



Routing >> Dynamic Routing

Your password has security risk, please click here to

Type: All

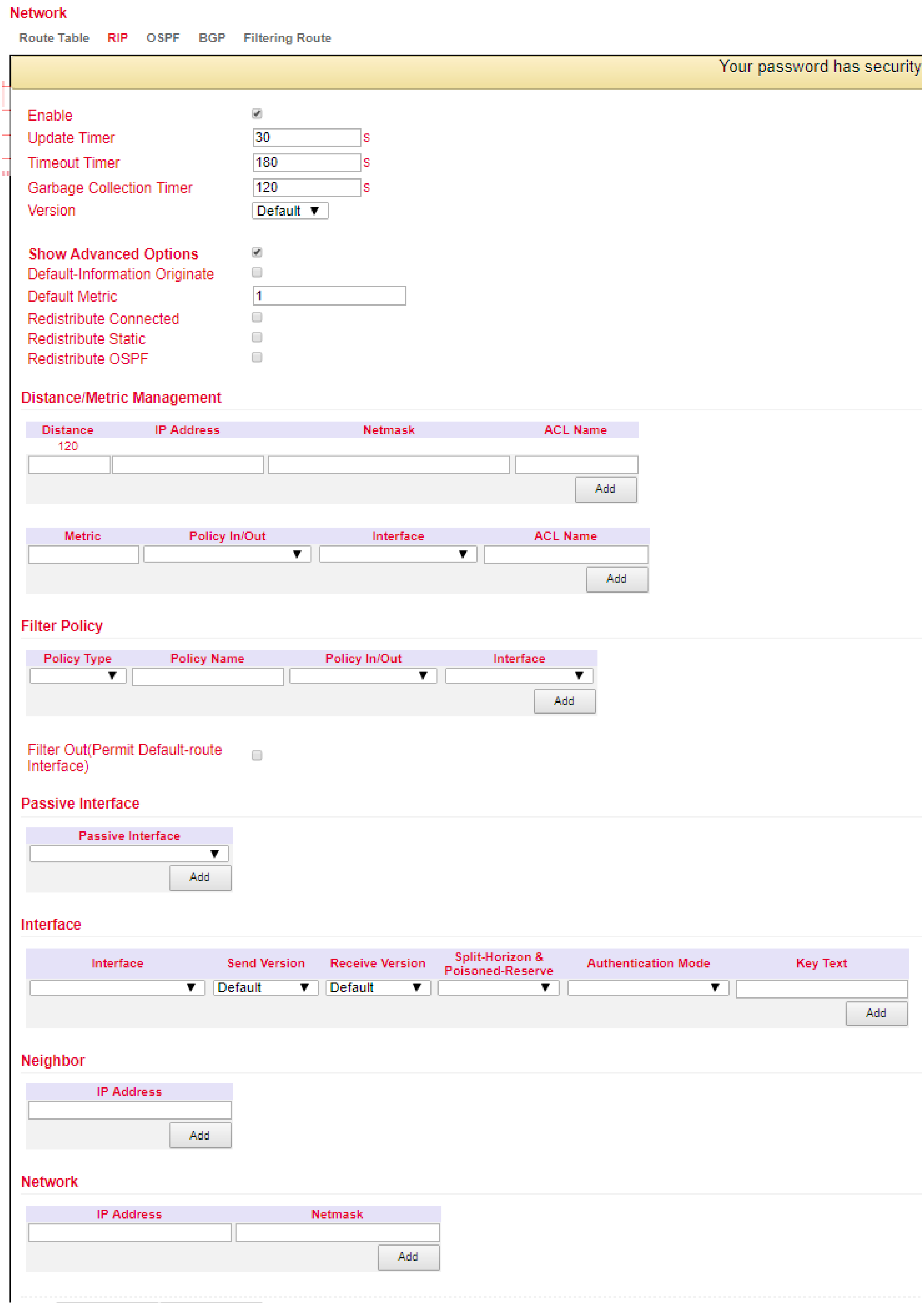
Type	Destination	Netmask	Gateway	Interface	Distance/Metric	Time
S	0.0.0.0	0.0.0.0	192.168.111.1	fastethernet 0/1	1/0	
C	127.0.0.0	255.0.0.0		loopback 1	0/0	
C	192.168.2.0	255.255.255.0		bridge 1	0/0	
C	192.168.2.10	255.255.255.255		bridge 1	0/0	
C	192.168.111.0	255.255.255.0		fastethernet 0/1	0/0	

Parameter Description see 3.5.1.1

3.5.2.2. RIP

RIP (Routing Information Protocol) is a dynamic routing protocol that works with distance vector algorithm. RIP dynamically learns routing addresses from other routers and stores them in its routing tables. The distance and costs are compared to other networks from the router's point of view and the most cost-effective way to the target network is specified in the routing tables. Based on this information, the cheapest and shortest route to the target network can be determined and taken. 15 Hops are the maximum distance that a route to the target network can take from the RIP.

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



Network

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			

Metric	Policy In/Out	Interface	ACL Name
	▼	▼	

Filter Policy

Policy Type	Policy Name	Policy In/Out	Interface
▼		▼	▼

Filter Out(Permit Default-route Interface)	□

Passive Interface

Passive Interface
▼

Interface

Interface	Send Version	Receive Version	Split-Horizon & Poisoned-Reserve	Authentication Mode	Key Text
▼	Default ▼	Default ▼	▼	▼	

Neighbor

IP Address

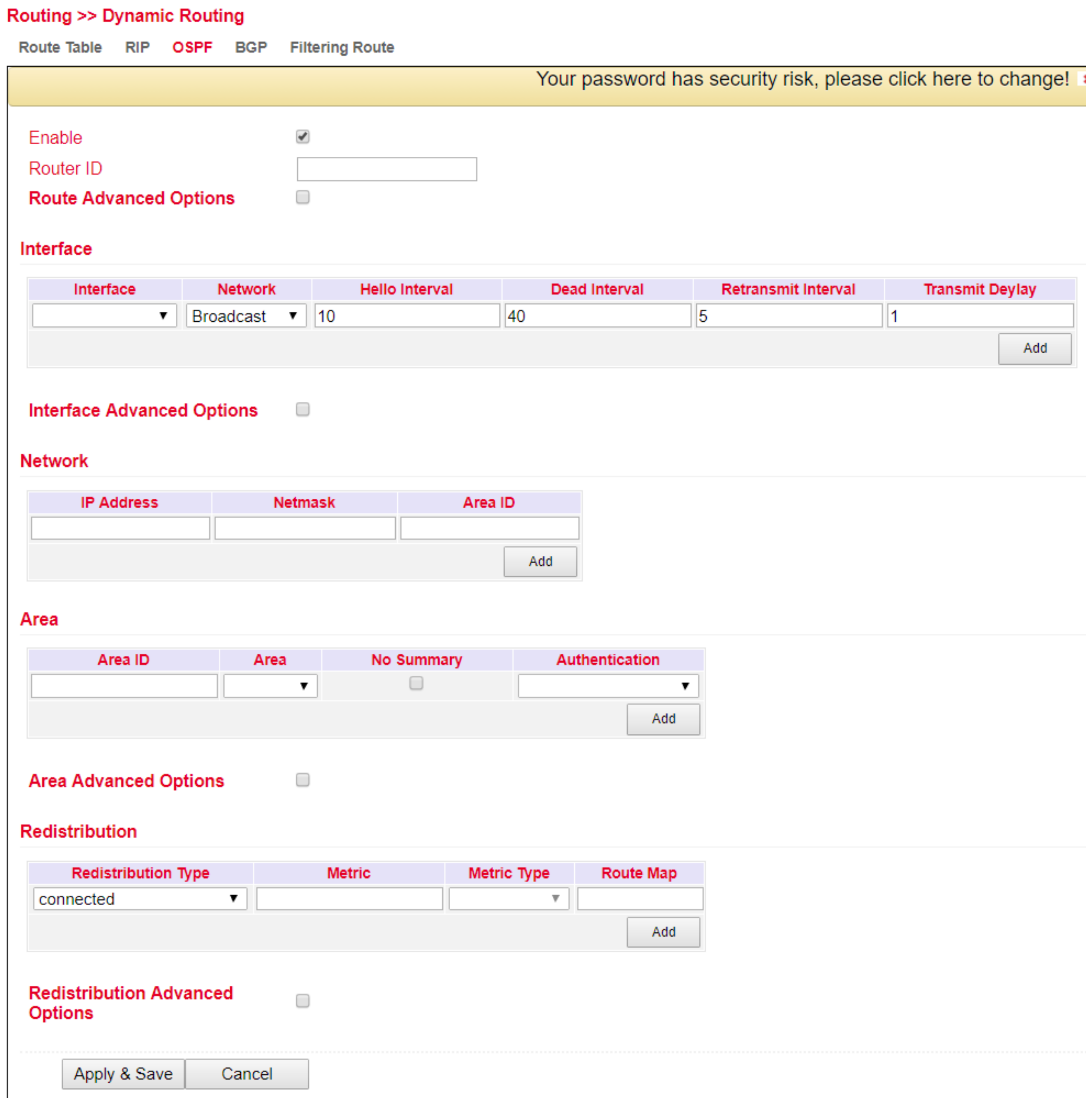
Network

IP Address	Netmask

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, unlike RIP it supports multiple concurrent connection paths of the same cost to a subnet and is able to transmit the occurring data traffic via different connection paths. The OSPF protocol is particularly fast in terms of network topology changes and is characterized by the economical use of bandwidth when creating new routing tables.

The following settings can be made in the menu **Routing** > **Dynamic Routing** > **OSPF**:



Routing >> Dynamic Routing

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

Enable	☑
Router ID	
Route Advanced Options	□

Interface

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

Interface Advanced Options □

Network

IP Address	Netmask	Area ID

Area

Area ID	Area	No Summary	Authentication
	▼	□	▼

Area Advanced Options □

Redistribution

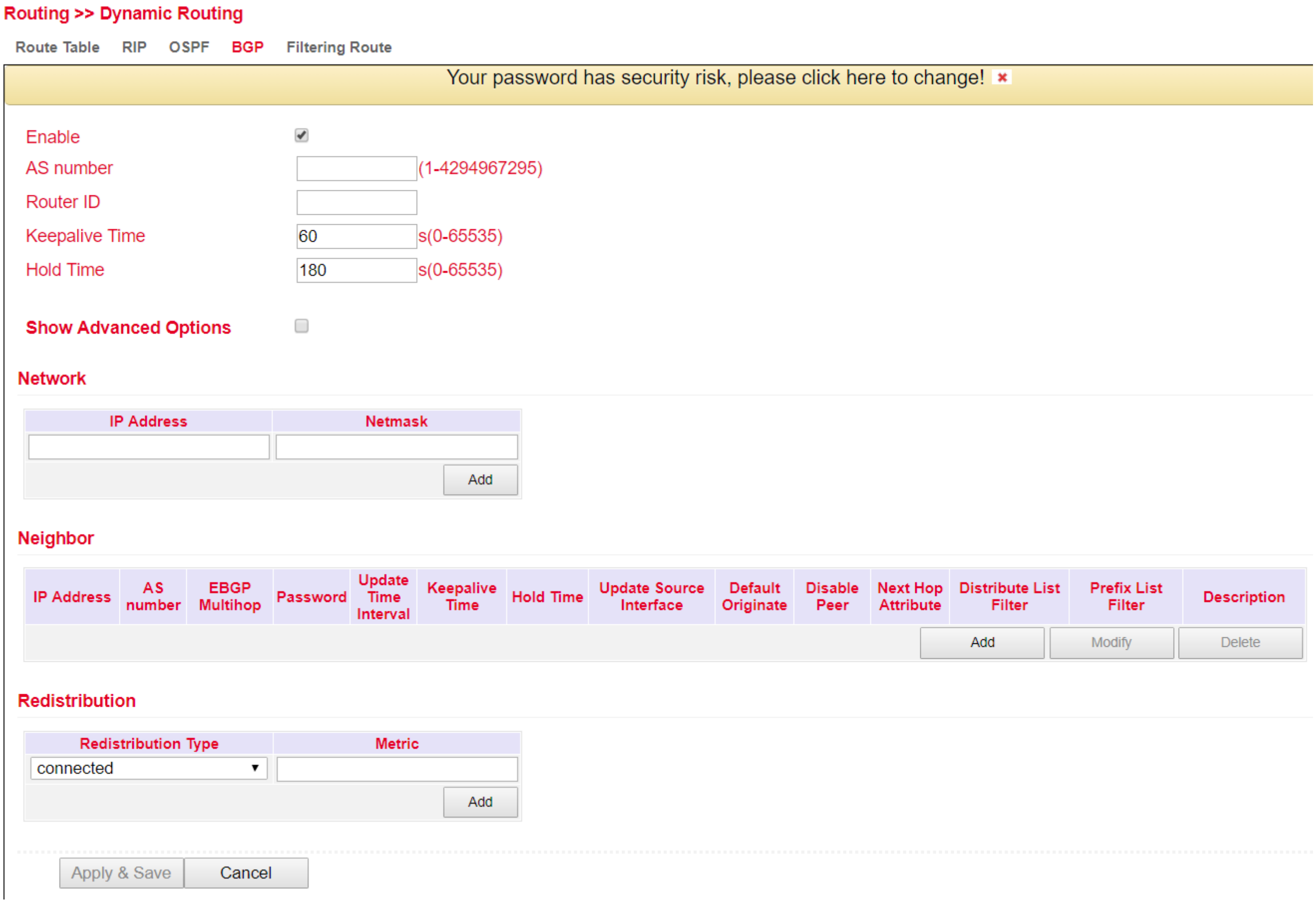
Redistribution Type	Metric	Metric Type	Route Map
connected ▼		▼	

Redistribution Advanced Options □

3.5.2.4. BGP

The Border Gateway Protocol (BGP) is the routing protocol used in the Internet and connects autonomous systems (AS) with each other. These autonomous systems are usually made up of Internet service providers. BGP is commonly referred to as the Exterior Gateway Protocol (EGP) and Path Vector Protocol and uses both strategic and technical-metric criteria for routing decisions, whereby in practice mostly business management aspects are considered. Within autonomous systems, interior gateway protocols (IGP) such as e.g. OSPF are used.

The following settings can be made for BGP in the menu **Routing > Dynamic Routing > BGP**:


Routing >> Dynamic Routing
Route Table
RIP
OSPF
BGP
Filtering Route
Your password has security risk, please click here to change!

Enable	☑
AS number	(1-4294967295)
Router ID	
Keepalive Time	60 s(0-65535)
Hold Time	180 s(0-65535)
Show Advanced Options	□

Network

IP Address	Netmask

Neighbor

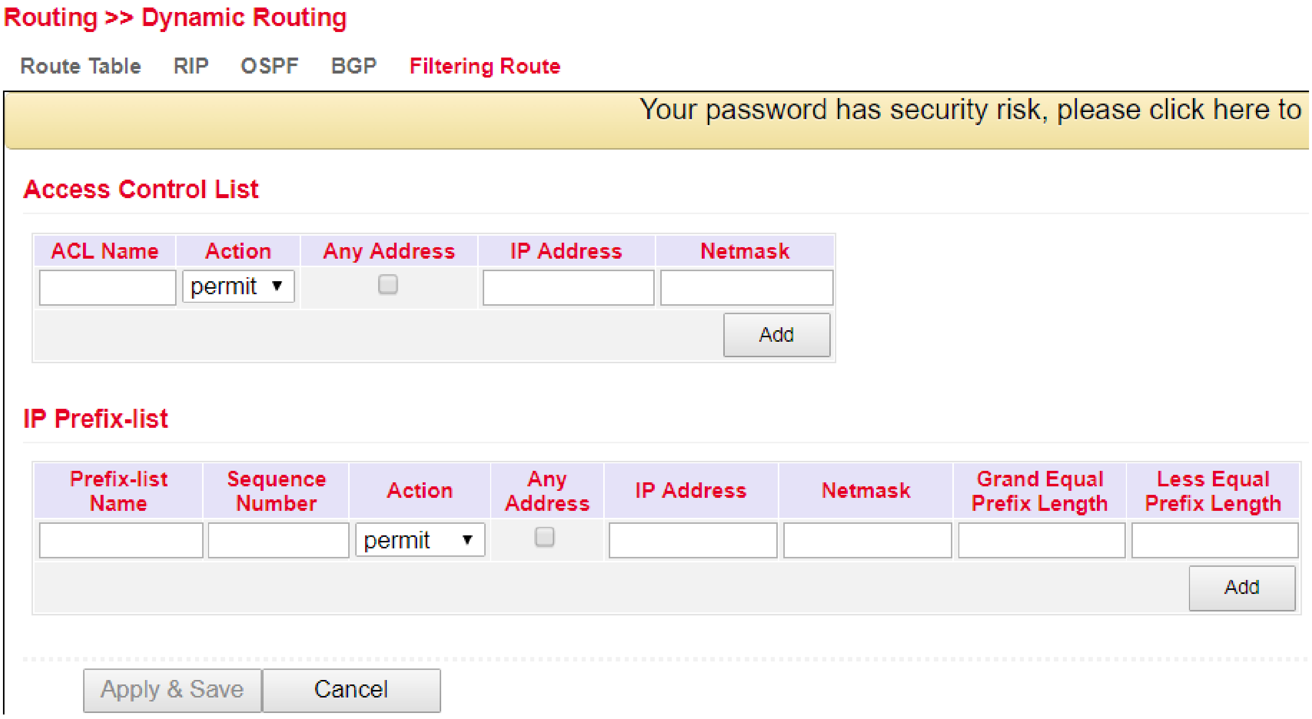
IP Address	AS number	EBGP Multihop	Password	Update Time Interval	Keepalive Time	Hold Time	Update Source Interface	Default Originate	Disable Peer	Next Hop Attribute	Distribute List Filter	Prefix List Filter	Description

Redistribution

Redistribution Type	Metric
connected	

3.5.2.5. Filtering Route

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



Routing >> Dynamic Routing

Access Control List

ACL Name	Action	Any Address	IP Address	Netmask
	permit ▾	□		

IP Prefix-list

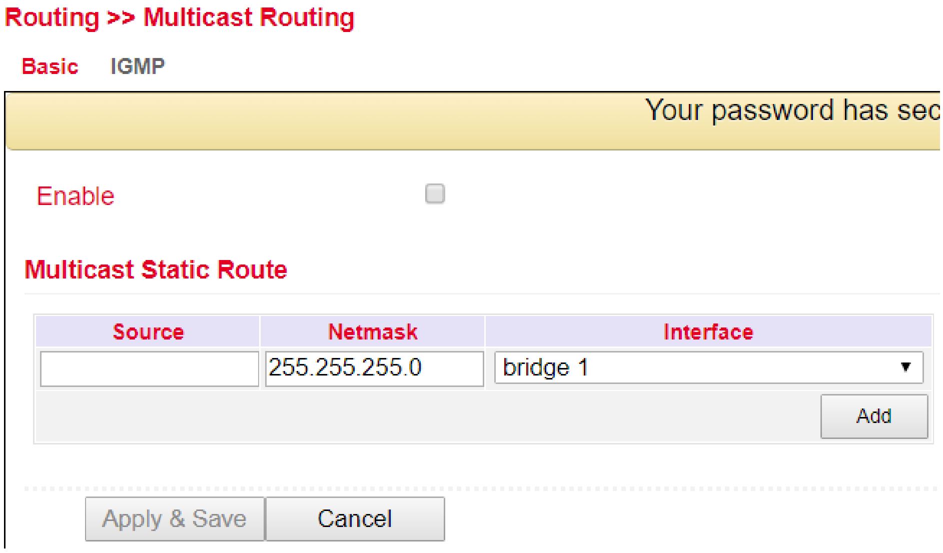
Prefix-list Name	Sequence Number	Action	Any Address	IP Address	Netmask	Grand Equal Prefix Length	Less Equal Prefix Length
		permit ▾	□				

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 an IP address to several stations at the same time.

3.5.3.1. Basic

The following settings can be made in the **Routing** > **Multicast Routing** > **Basic** menu:



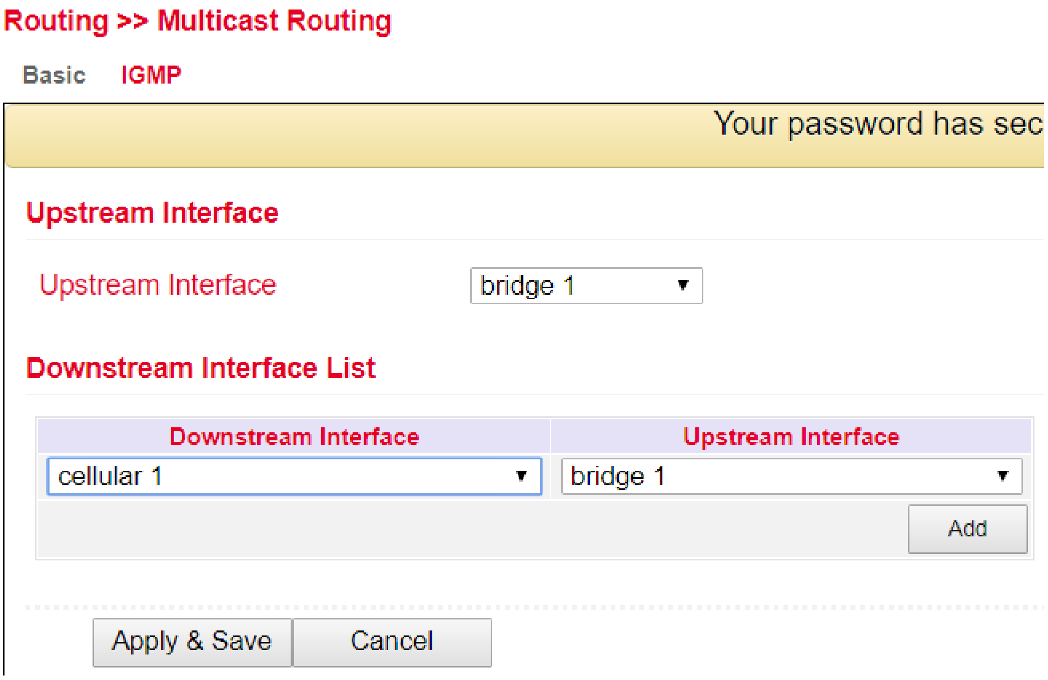
Routing >> Multicast Routing

Enable □

Multicast Static Route

Source	Netmask	Interface
	255.255.255.0	bridge 1 ▾

3.5.3.2. IGMP



Routing >> Multicast Routing

Your password has sec

Upstream Interface

Upstream Interface: bridge 1

Downstream Interface List

Downstream Interface	Upstream Interface
cellular 1	bridge 1

The **Upstream Interface** selects the interface via which the multicast is to be distributed.

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

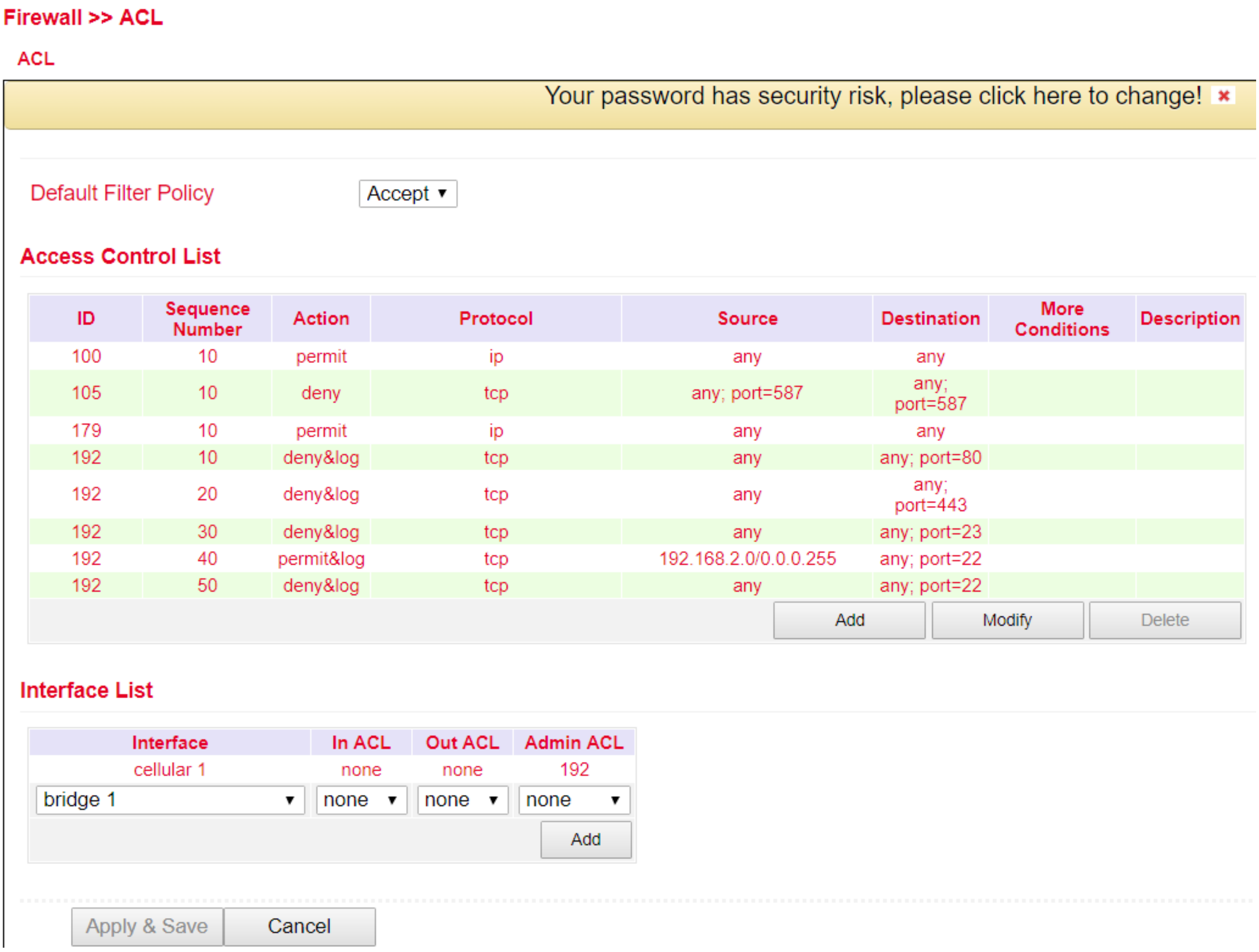
The interfaces can vary depending on the model.

3.6. Firewall

3.6.1. ACL

The ACL (Access Control List) is an access control list to control usage and administration. The ACL determines which computers or networks can access the router or networks behind the router. The ACL analyzes incoming and outgoing data packets and manages them according to the ACL rules.

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



Firewall >> ACL

ACL

Your password has security risk, please click here to change! ✖

Default Filter Policy: Accept ▾

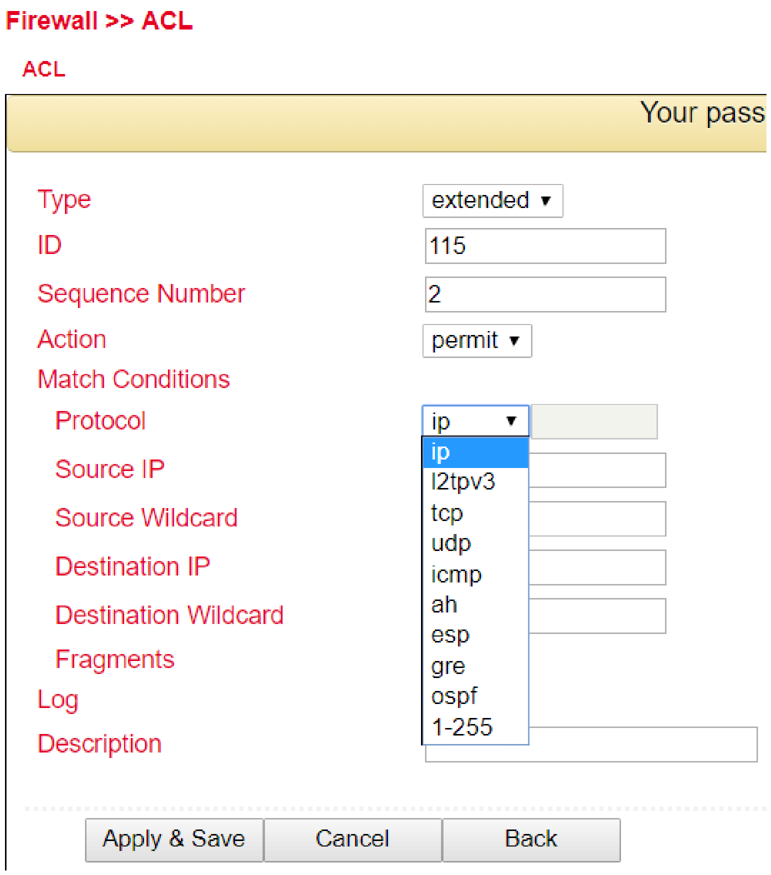
Access Control List

ID	Sequence Number	Action	Protocol	Source	Destination	More Conditions	Description
100	10	permit	ip	any	any		
105	10	deny	tcp	any; port=587	any; port=587		
179	10	permit	ip	any	any		
192	10	deny&log	tcp	any	any; port=80		
192	20	deny&log	tcp	any	any; port=443		
192	30	deny&log	tcp	any	any; port=23		
192	40	permit&log	tcp	192.168.2.0/0.0.0.255	any; port=22		
192	50	deny&log	tcp	any	any; port=22		

Interface List

Interface	In ACL	Out ACL	Admin ACL
cellular 1	none	none	192
bridge 1 ▾	none ▾	none ▾	none ▾

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



Firewall >> ACL

ACL

Your pass

Type	extended ▾
ID	115
Sequence Number	2
Action	permit ▾
Match Conditions	
Protocol	ip ▾
Source IP	
Source Wildcard	
Destination IP	
Destination Wildcard	
Fragments	
Log	
Description	

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

Extended ACL offers extended settings for source and target networks within an ACL. Protocols from different levels can be selected. In this way, it is possible to allow or prohibit individual services such as Web (http), FTP, Telnet etc. in a targeted manner.

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

Destination Wildcard is the wildcard address of the destination subnet, e. g. for the 255.255.0.0 subnet mask, the Wildcard Address 0.0.255.255
Description (text) Description field for the ACL

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 in order with others to connect different networks. They are therefore typically used on routers.

Use of Source NAT
It allows devices with private network addresses to connect to the Internet. Private IP addresses usually cannot 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, there is a relevant security aspect in NAT, since a public IP address cannot be traced back to the associated private IP address. This feature is factory configured on the TK800 router.

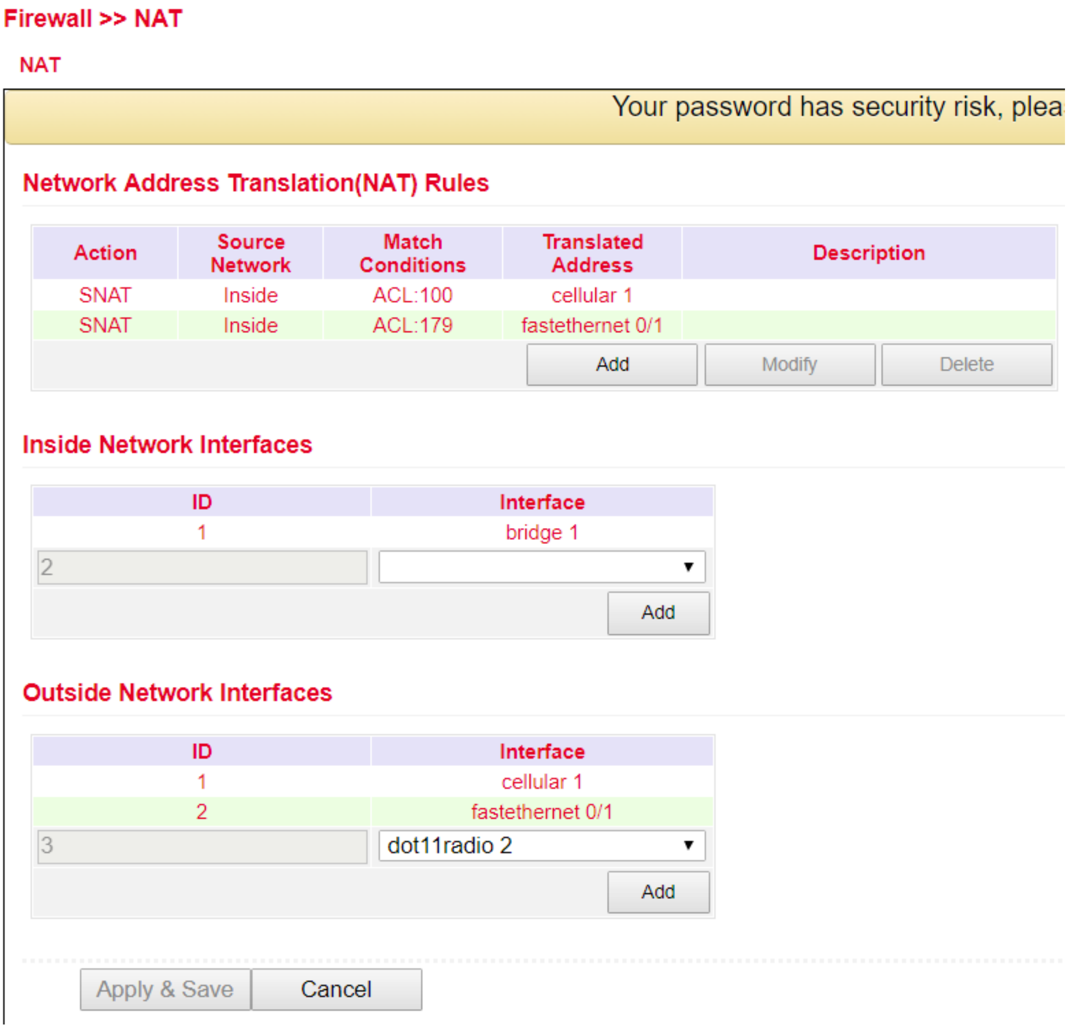
Use of Destination NAT
This is used to provide server services running on computers under a single IP address. It is often referred to as port mapping or port forwarding. This function must be set up explicitly on the TK800.

Use of 1:1-NAT
A special form of Destination-NAT is 1:1-NAT. It is used, for example, when a central office wants to access different locations, which are all configured with the same IP network addresses. This is common in machine nets.

Configuration

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

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



Firewall >> NAT

NAT

Your password has security risk, plea

Network Address Translation(NAT) Rules

Action	Source Network	Match Conditions	Translated Address	Description
SNAT	Inside	ACL:100	cellular 1	
SNAT	Inside	ACL:179	fastethernet 0/1	

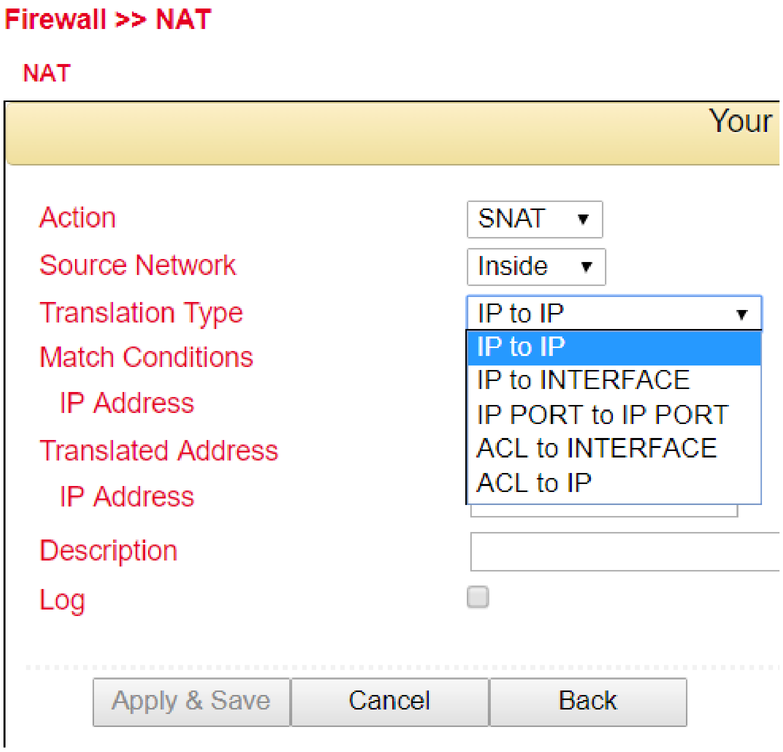
Inside Network Interfaces

ID	Interface
1	bridge 1
2	

Outside Network Interfaces

ID	Interface
1	cellular 1
2	fastethernet 0/1
3	dot11radio 2

- Click **Add** to configure a new NAT rule in the following menu



Firewall >> NAT

NAT

Your

Action	SNAT
Source Network	Inside
Translation Type	IP to IP
Match Conditions	
IP Address	
Translated Address	
IP Address	
Description	
Log	□

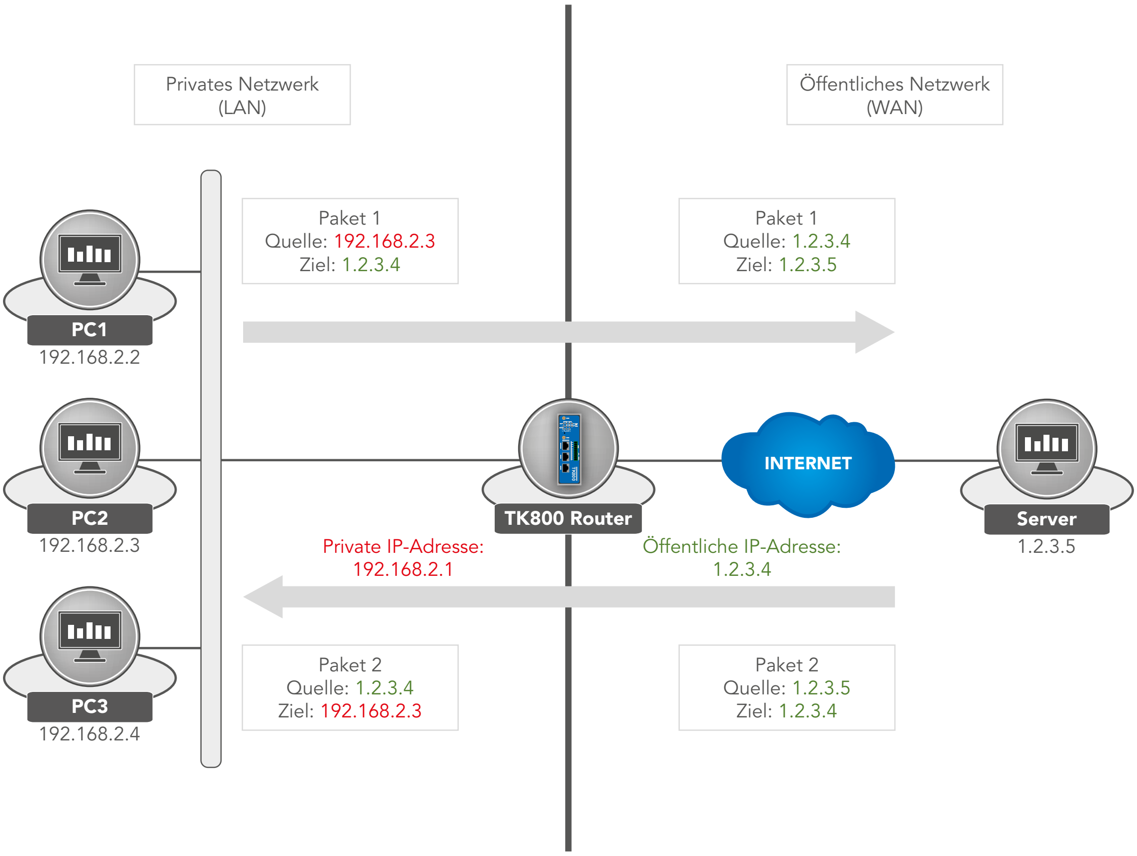
Action	
SNAT	Translate the IP address of the computer setting up the connection
DNAT	Translate the IP address of the target computer
1:1NAT	Translate IP-Address one to one
Source Network	
Inside	Packets come from an internal interface (LAN)
Outside	Packets come from an external interface (WAN)
Translation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

Examples

Case 1: SNAT (TK router as internet gateway)

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

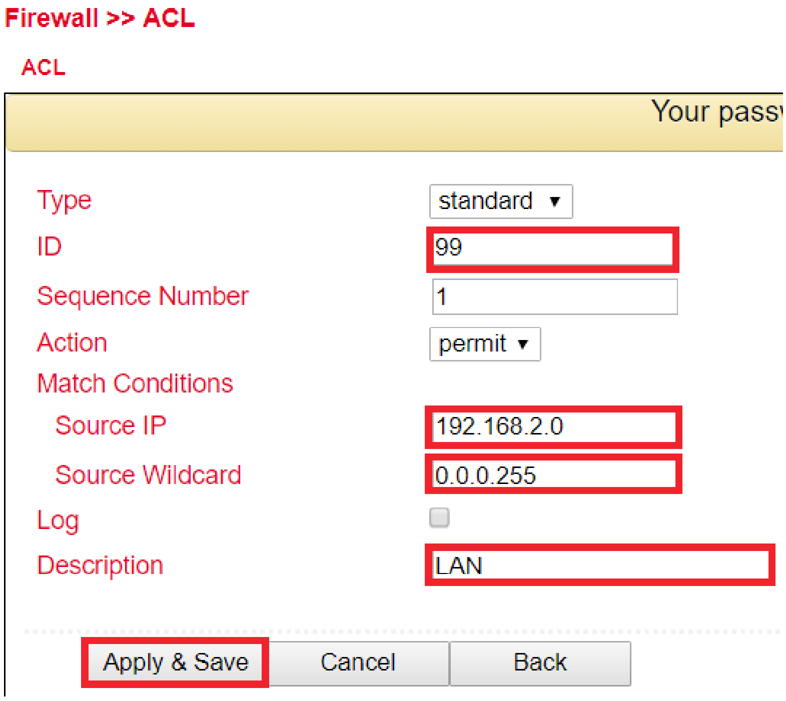
(**Note**: This is the default setting of all Welotec routers.)



1. Configure the ACL rule. In the **Firewall** menu, go to sub-item **ACL**

2. Enter an **ID** for the rule and enter the **IP-Address** and the corresponding **Wildcard-Mask**.

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



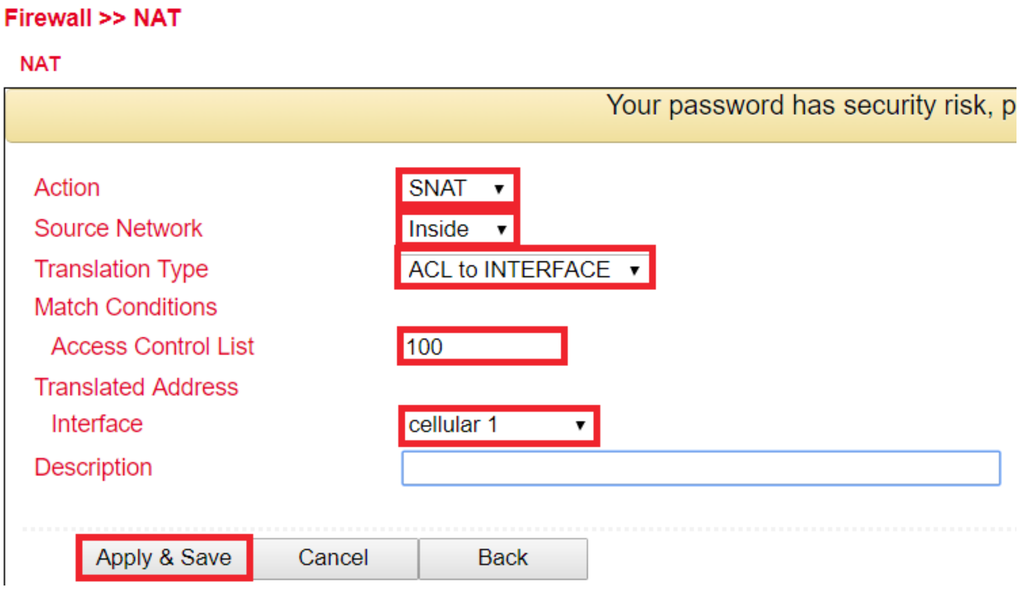
Firewall >> ACL

ACL

Your pass

Type	standard
ID	99
Sequence Number	1
Action	permit
Match Conditions	
Source IP	192.168.2.0
Source Wildcard	0.0.0.255
Log	□
Description	LAN

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



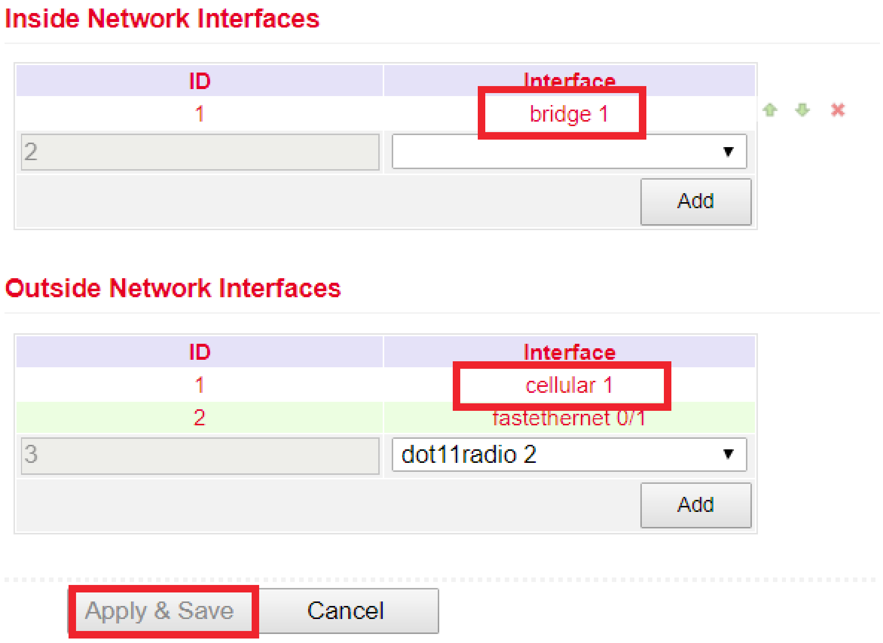
Firewall >> NAT

NAT

Your password has security risk, p

Action	SNAT
Source Network	Inside
Translation Type	ACL to INTERFACE
Match Conditions	
Access Control List	100
Translated Address	
Interface	cellular 1
Description	

4. Now define the **Inside** and **Outside-Interface**



Inside Network Interfaces

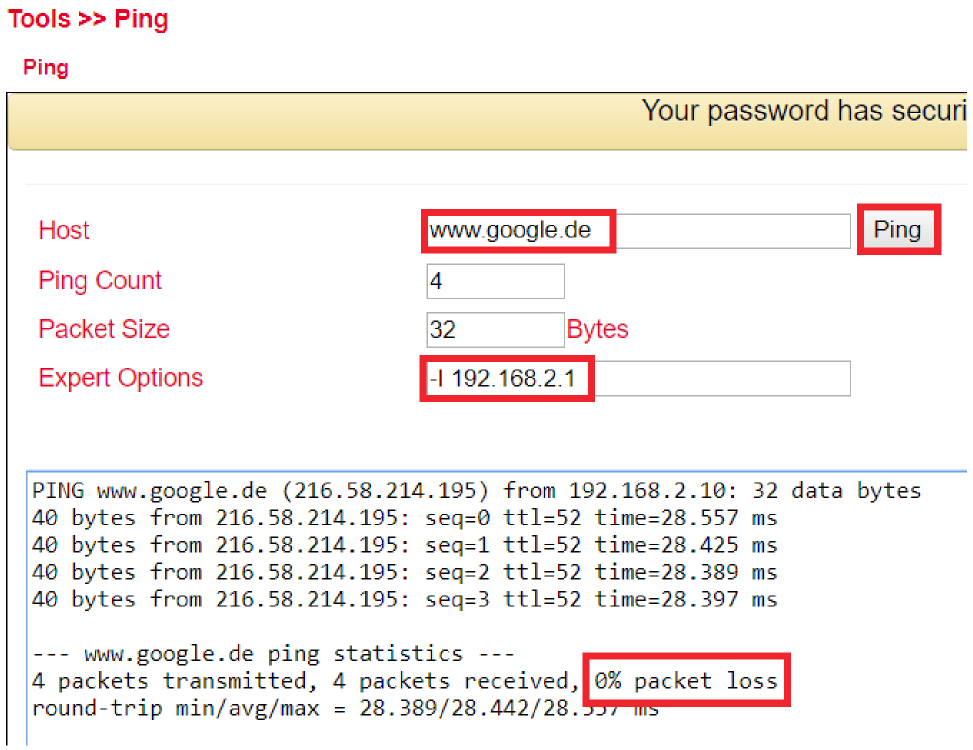
ID	Interface
1	bridge 1
2	

Outside Network Interfaces

ID	Interface
1	cellular 1
2	fastethernet 0/1
3	dot11radio 2

5. Test the access via the **ping** tool. This can be done directly from the router. In the Tools menu, go to the sub-item Ping and enter the values according to the example.

(**Note**: Use the **Expert Option** -I 192.168.2.1 (large i) to get access from the inside (LAN) interface of the TK800 router)



Tools >> Ping

Ping

Your password has securi

Host: www.google.de

Ping Count: 4

Packet Size: 32 Bytes

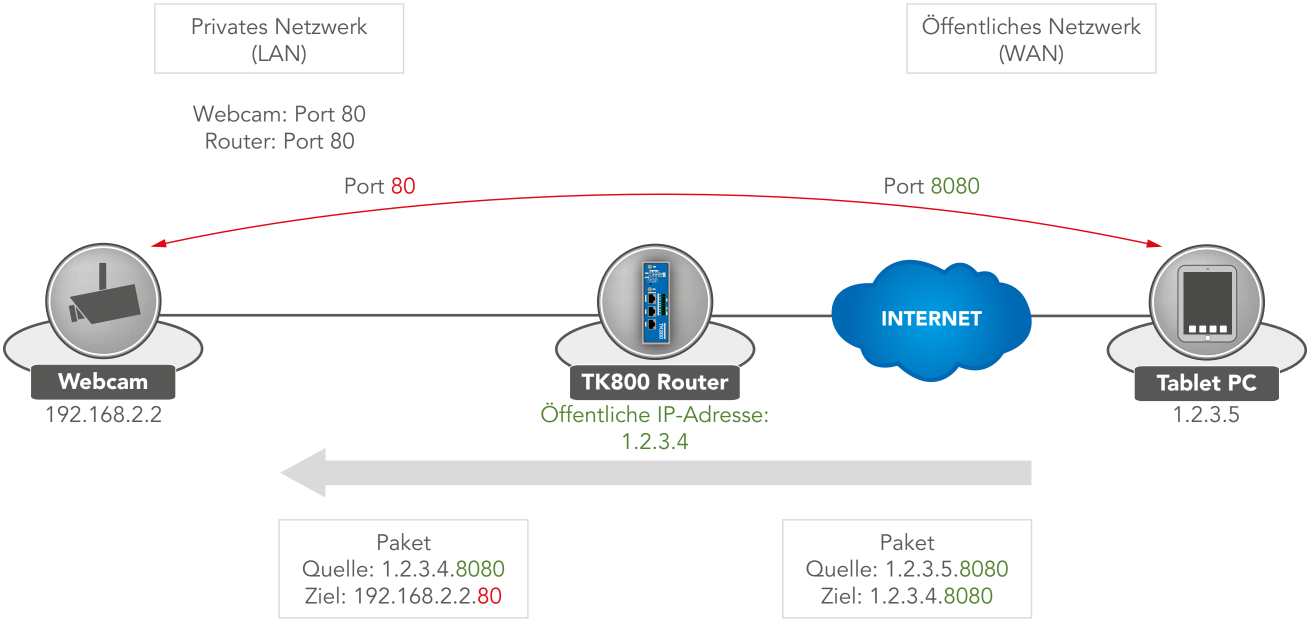
Expert Options: -I 192.168.2.1

```
PING www.google.de (216.58.214.195) from 192.168.2.10: 32 data bytes
40 bytes from 216.58.214.195: seq=0 ttl=52 time=28.557 ms
40 bytes from 216.58.214.195: seq=1 ttl=52 time=28.425 ms
40 bytes from 216.58.214.195: seq=2 ttl=52 time=28.389 ms
40 bytes from 216.58.214.195: seq=3 ttl=52 time=28.397 ms

--- www.google.de ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 28.389/28.442/28.557 ms
```

Case 2: DNAT (port mapping / port forwarding)

Internet access to connected devices

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. It uses so-called port forwarding / port mapping function.



Requirements

- Public IP address in the mobile network (or even with wired Internet connections)

(**Note:** Many mobile operators offer rates for business customers to access mobile devices, including T-Mobile IP VPN or Vodafone CDA. There are also providers who provide you with a public IP address via a conventional mobile phone card.

⚠ Note

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

Notes on port mapping

The following information must be available before port mapping can be set up:

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

Exmaple:

Welotec Router

LAN IP-Address:	192.168.2.1
Subnet mask:	255.255.255.0

Webcam

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)

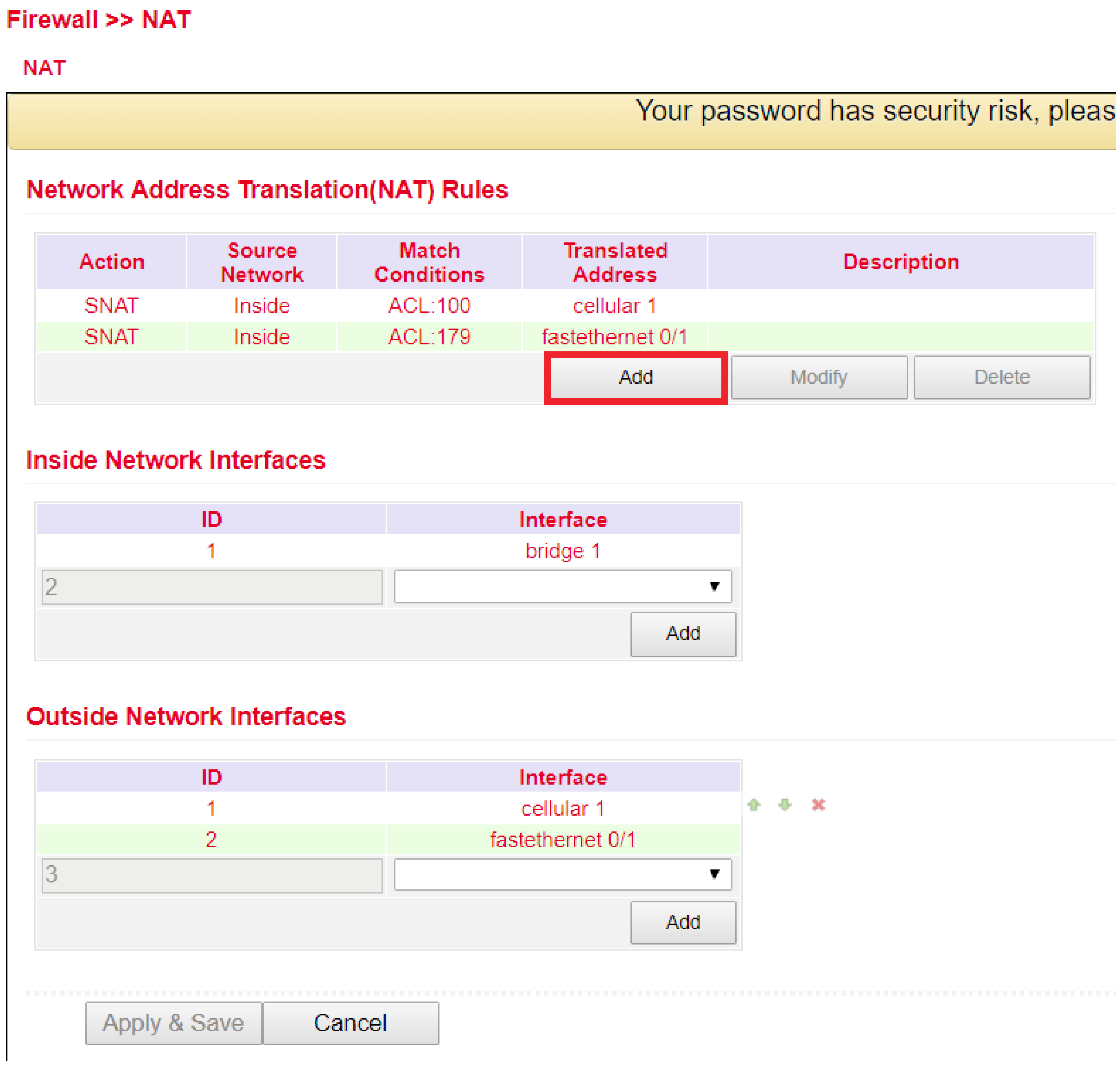
For a working port mapping it is helpful to check the settings of the connected devices beforehand. The following checklist is helpful (according to the above example):

- Does the camera have the IP address 192.168.2.2?
- Does it answer at „ping 192.168.2.2"?
- Is the web interface of the camera accessible via http://192.168.2.2?
- Is the Welotec router registered with the camera as the default gateway (192.168.2.1)?

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

Configuration

1.) Go via the menu item **Firewall** to the submenu **NAT**
2.) Now add a new NAT rule with **Add**



Firewall >> NAT

NAT

Your password has security risk, pleas

Network Address Translation(NAT) Rules

Action	Source Network	Match Conditions	Translated Address	Description
SNAT	Inside	ACL:100	cellular 1	
SNAT	Inside	ACL:179	fastethernet 0/1	

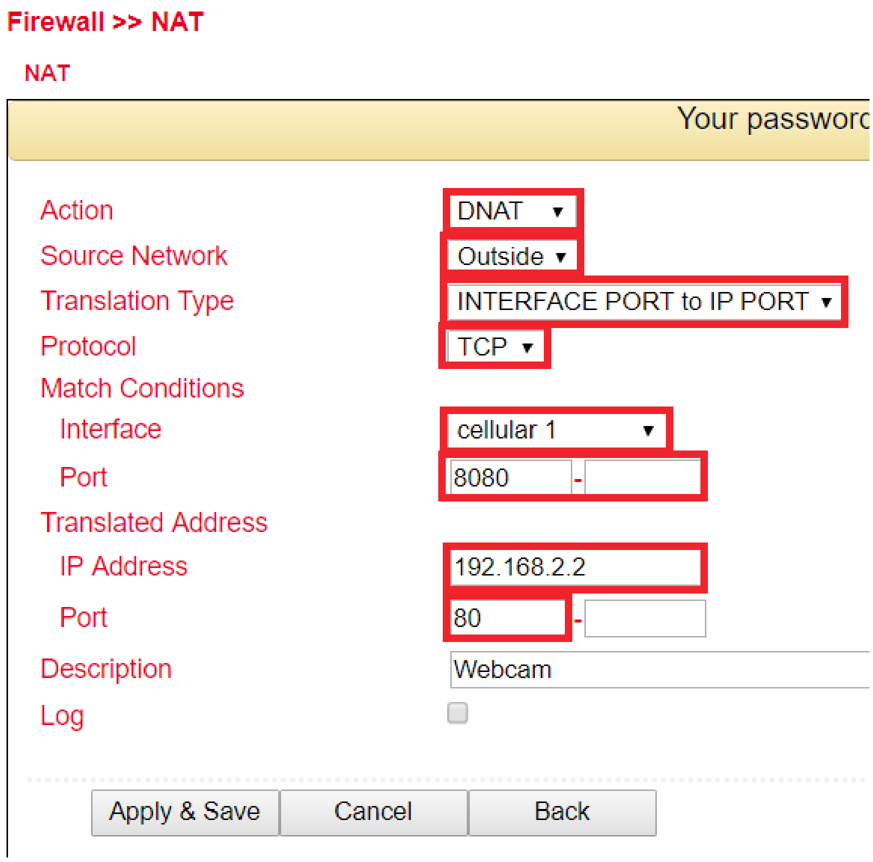
Inside Network Interfaces

ID	Interface
1	bridge 1
2	

Outside Network Interfaces

ID	Interface
1	cellular 1
2	fastethernet 0/1
3	

3.) Enter the data as in the example



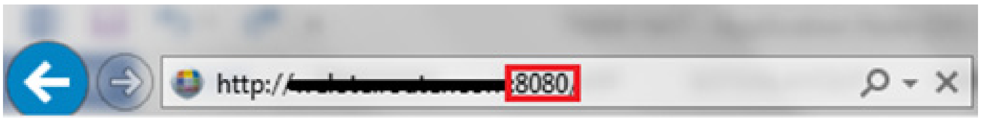
Firewall >> NAT

NAT

Your passworc

Action	DNAT ▾
Source Network	Outside ▾
Translation Type	INTERFACE PORT to IP PORT ▾
Protocol	TCP ▾
Match Conditions	
Interface	cellular 1 ▾
Port	8080 -
Translated Address	
IP Address	192.168.2.2
Port	80 -
Description	Webcam
Log	□

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

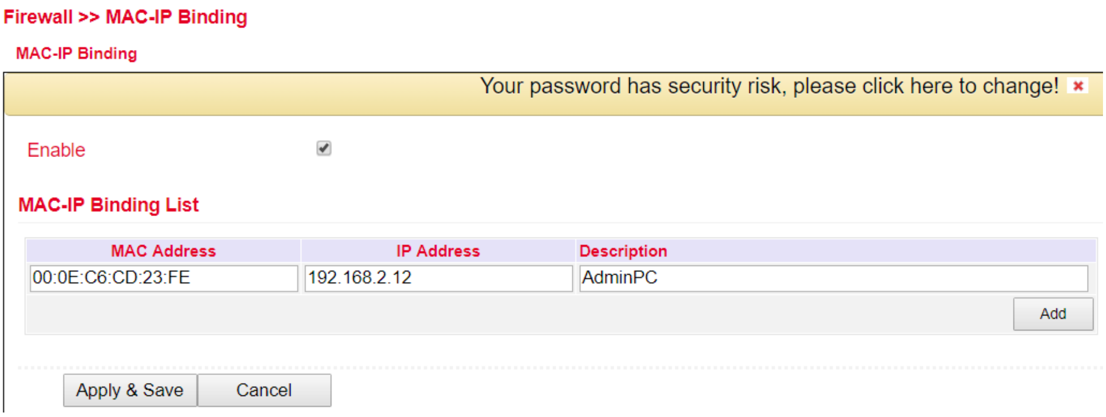


http:/[redacted]:8080/

3.6.3. MAC-IP Binding

You can find MAC-IP Binding in the navigation tree under **Firewall** > **MAC-IP Binding**.

MAC-IP Binding ensures that a device (PC, server, etc.) can only access the router if the MAC and IP address entered here match.



Firewall >> MAC-IP Binding

MAC-IP Binding

Your password has security risk, please click here to change! ✖

Enable ☑

MAC-IP Binding List

MAC Address	IP Address	Description
00:0E:C6:CD:23:FE	192.168.2.12	AdminPC

Parameter	Description
MAC-Address	Enter the MAC-address in this format XX : XX : XX : XX: XX : XX. A typical MAC-address looks like this: 00:FF:4E:85:F1:B5
IP-Address	Type in IP-adress that the device should receive e.g. 192.168.2.150
Description	Text Description field

3.7. VPN

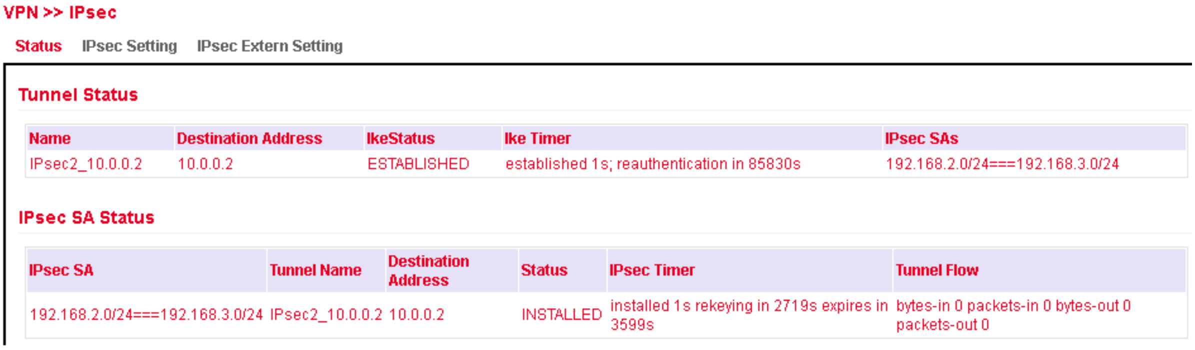
Virtual Private Network, in short VPN. The VPN is used to bind subscribers of the existing communication network to another network.For example, this allows an employee’s computer to gain access to the corporate network from home, just as if he were sitting in the middle of it.

3.7.1. IPsec

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

3.7.1.1. Status

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



Tunnel Status

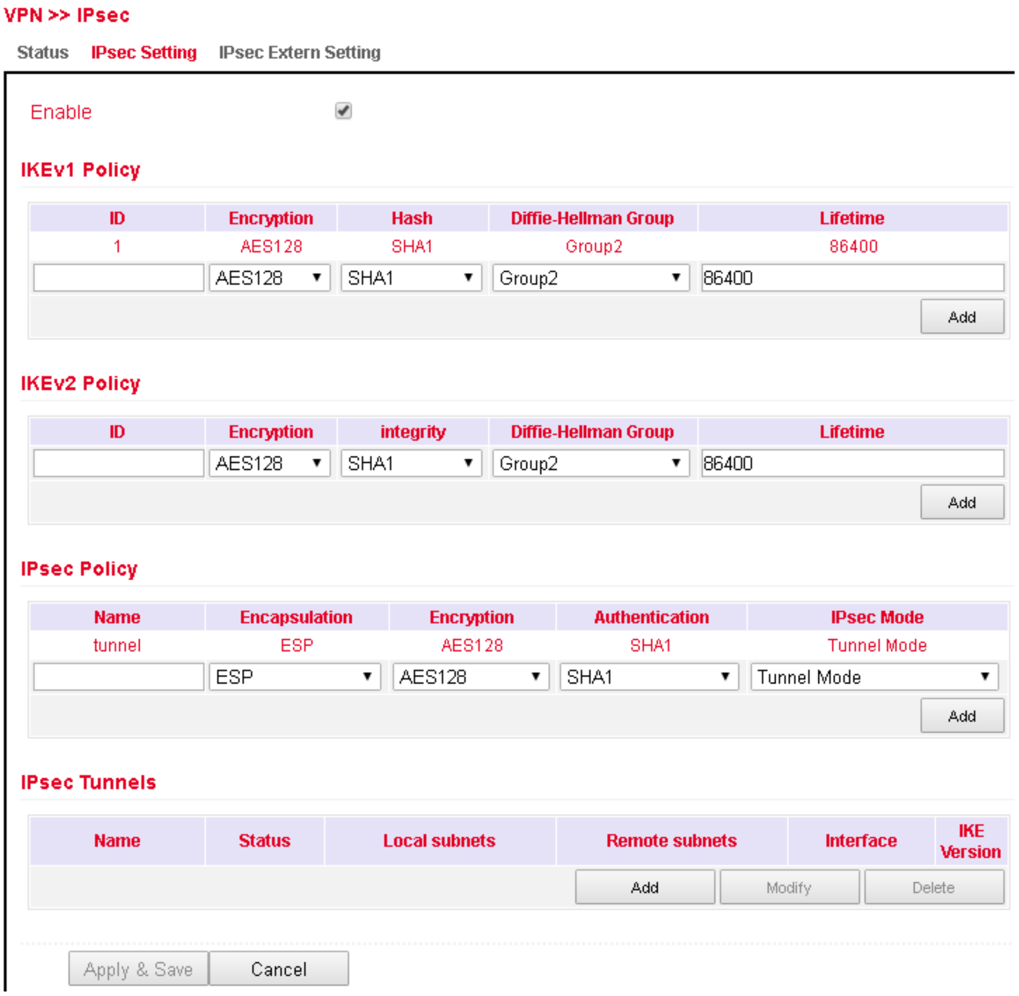
Name	Destination Address	IkeStatus	Ike Timer	IPsec SAs
IPsec2_10.0.0.2	10.0.0.2	ESTABLISHED	established 1s; reauthentication in 85830s	192.168.2.0/24===192.168.3.0/24

IPsec SA Status

IPsec SA	Tunnel Name	Destination Address	Status	IPsec Timer	Tunnel Flow
192.168.2.0/24===192.168.3.0/24	IPsec2_10.0.0.2	10.0.0.2	INSTALLED	installed 1s rekeying in 2719s expires in 3599s	bytes-in 0 packets-in 0 bytes-out 0 packets-out 0

3.7.1.2. IPsec Settings

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



VPN >> IPsec

Status | IPsec Setting | IPsec Extern Setting

Enable ☑

IKEv1 Policy

ID	Encryption	Hash	Diffie-Hellman Group	Lifetime
1	AES128	SHA1	Group2	86400
	AES128 ▾	SHA1 ▾	Group2 ▾	86400

Add

IKEv2 Policy

ID	Encryption	integrity	Diffie-Hellman Group	Lifetime
	AES128 ▾	SHA1 ▾	Group2 ▾	86400

Add

IPsec Policy

Name	Encapsulation	Encryption	Authentication	IPsec Mode
tunnel	ESP	AES128	SHA1	Tunnel Mode
	ESP ▾	AES128 ▾	SHA1 ▾	Tunnel Mode ▾

Add

IPsec Tunnels

Name	Status	Local subnets	Remote subnets	Interface	IKE Version

Add | Modify | Delete

Apply & Save | Cancel

IKEv1 Policy:

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

IKEv2 Policy:

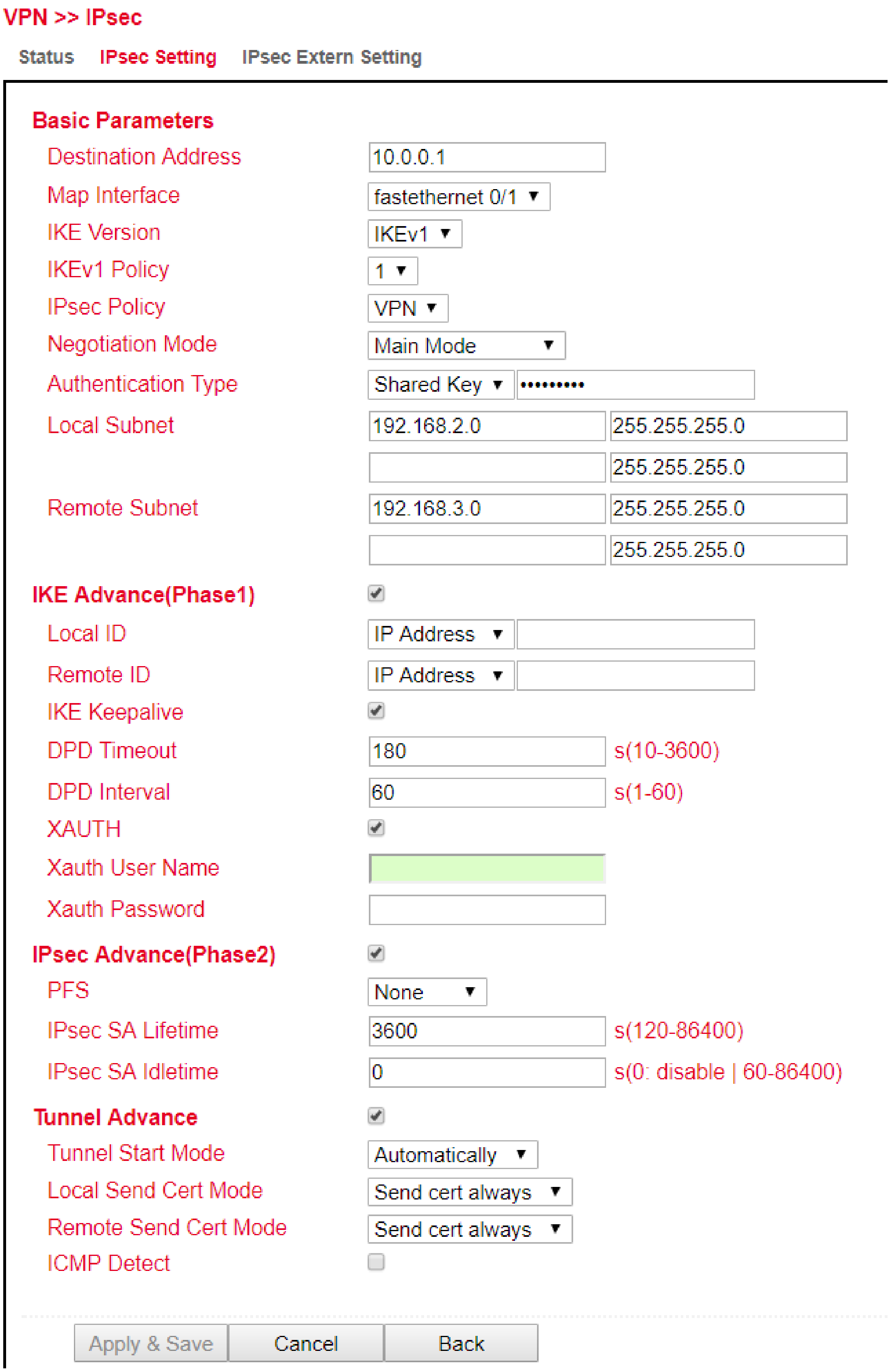
Parameter	Description
ID	Integer, can be freely selected. Identifies the policy in the tunnel configuration
Encryption	Encryption methode
integrity	Secure hash algorithm
Diffie-Hellman Group	DH-Group for key exchange
Lifetime	Period of validity of the IKE before it is renegotiated

IPsec Policy:

Parameter	Description
Name	Freely selectable name of the IPsec policy. Identifies the policy in the tunnel configuration
Encapsulation	ESP or AH
Encryption	Encryption methode
Authentication	Secure hash algorithm
IPsec Mode	Tunnel or Transport Mode

3.7.1.2.1. IPsec Tunnel

Via **VPN > IPsec > IPsec Settings** you can create a new IPsec Tunnel (IKEv1 and IKEv2) with **Add**. The requirement is that an IKEv1 or IKEv2 policy and an IPsec policy have been created.



Basic Parameters

Destination Address	10.0.0.1	
Map Interface	fastethernet 0/1 ▼	
IKE Version	IKEv1 ▼	
IKEv1 Policy	1 ▼	
IPsec Policy	VPN ▼	
Negotiation Mode	Main Mode ▼	
Authentication Type	Shared Key ▼	••••••••••
Local Subnet	192.168.2.0	255.255.255.0
		255.255.255.0
Remote Subnet	192.168.3.0	255.255.255.0
		255.255.255.0

IKE Advance(Phase1) ☑

Local ID	IP Address ▼	
Remote ID	IP Address ▼	
IKE Keepalive	☑	
DPD Timeout	180	s(10-3600)
DPD Interval	60	s(1-60)
XAUTH	☑	
Xauth User Name		
Xauth Password		

IPsec Advance(Phase2) ☑

PFS	None ▼	
IPsec SA Lifetime	3600	s(120-86400)
IPsec SA Idletime	0	s(0: disable | 60-86400)

Tunnel Advance ☑

Tunnel Start Mode	Automatically ▼
Local Send Cert Mode	Send cert always ▼
Remote Send Cert Mode	Send cert always ▼
ICMP Detect	☐

Basic Parameters:

Parameter	Description
Destination Address	IP address of the tunnel remote station
Map Interface	Interface of the router, over which the connection is to be set up
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's subnet
Remote Subnet	The subnet of the remote station

IKE Advance(Phase1):

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

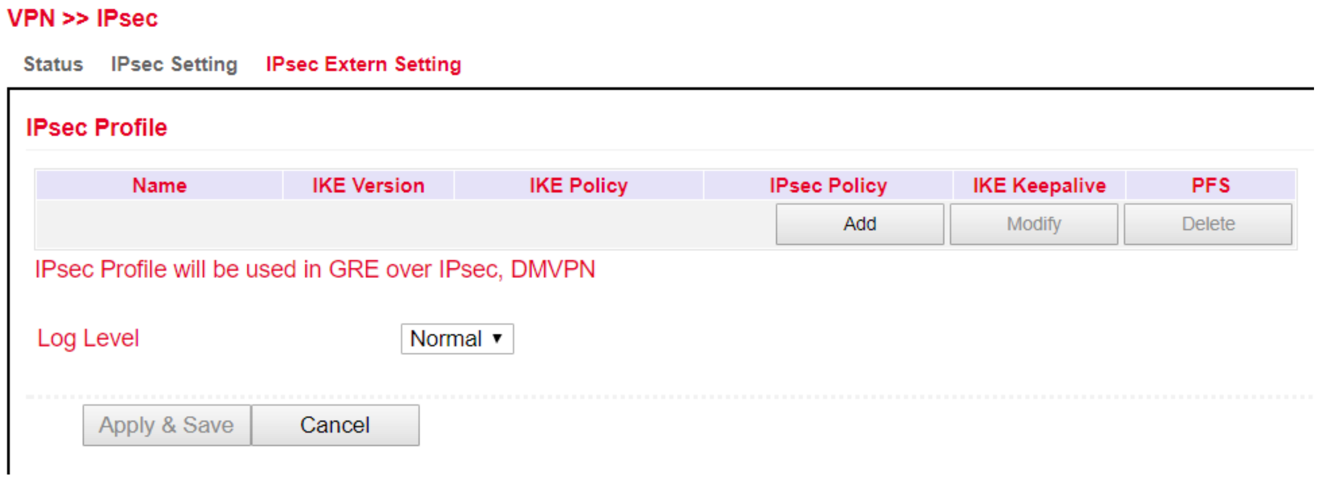
IPsec Advance(Phase2):

Parameter	Description
PFS	Perfect Forward Secrecy Group
IPsec SA Lifetime	Validity period of the SA before it is re-created
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 standard
Local Send Cert Mode	Determines when the certificate should be sent
Remote Send Cert Mode	Determines 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 which can only be reached through the tunnel.
ICMP Detection Local IP	Specifies the router interface IP of the local subnet
ICMP Detection Interval	Intervall in 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

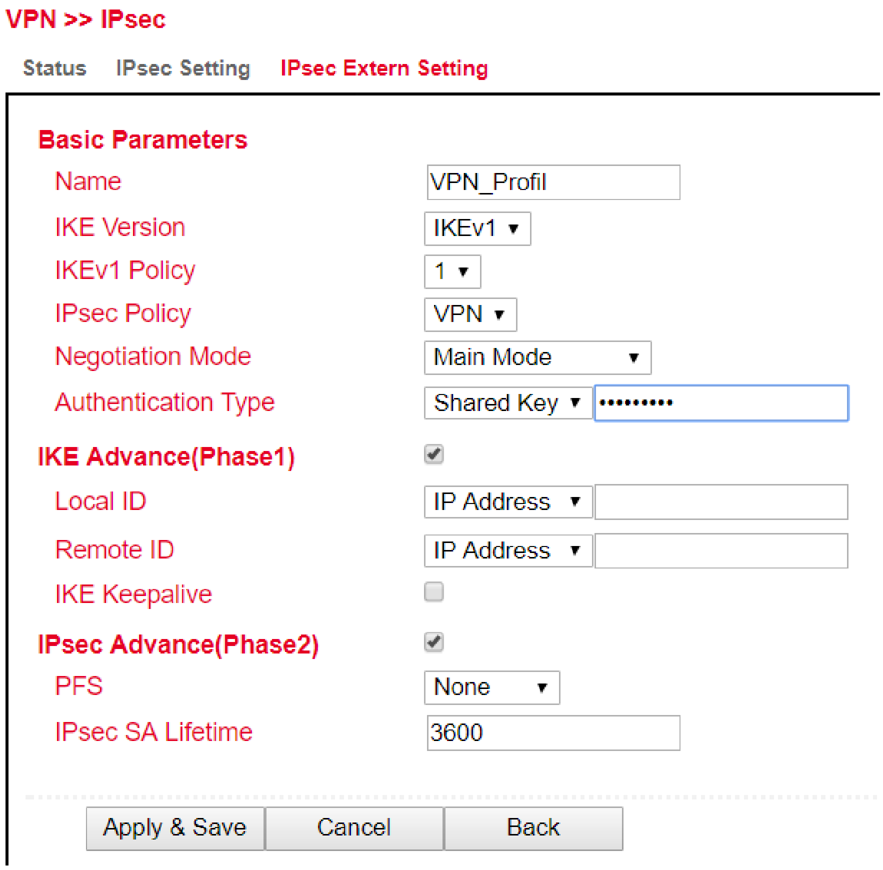


Name	IKE Version	IKE Policy	IPsec Policy	IKE Keepalive	PFS

IPsec Profile will be used in GRE over IPsec, DMVPN

Log Level: Normal

IPsec profiles are used with GRE over IPsec. The profile is created using the **Add** button.



Basic Parameters

Name	VPN_Profil
IKE Version	IKEv1 ▾
IKEv1 Policy	1 ▾
IPsec Policy	VPN ▾
Negotiation Mode	Main Mode ▾
Authentication Type	Shared Key ▾ •••••••••
IKE Advance(Phase1)	☑
Local ID	IP Address ▾
Remote ID	IP Address ▾
IKE Keepalive	□
IPsec Advance(Phase2)	☑
PFS	None ▾
IPsec SA Lifetime	3600

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	Turns IKE Keepalive on or off
DPD Timeout	Timeout for a DPD packets
DPD Interval	Interval of DPD packets

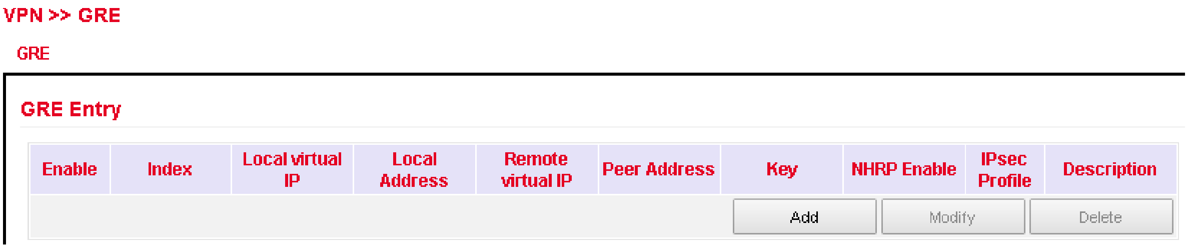
IPsec Advance(Phase2):

Parameter	Description
PFS	Perfect Forward Secrecy Group
IPsec SA Lifetime	Validity period of the SA before it is re-created

3.7.2. GRE

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

GRE is used for dynamic routing via the IPSec tunnel.



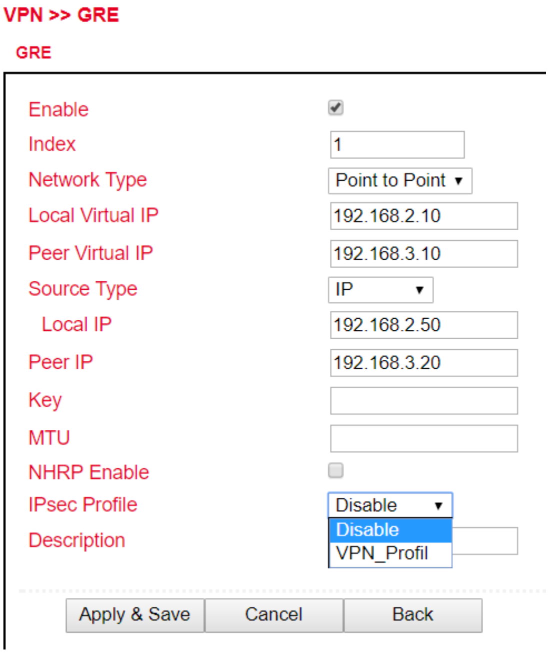
VPN >> GRE

GRE

GRE Entry

Enable	Index	Local virtual IP	Local Address	Remote virtual IP	Peer Address	Key	NHRP Enable	IPsec Profile	Description

Overview page. With **Add** a new GRE entry is added.



VPN >> GRE

GRE

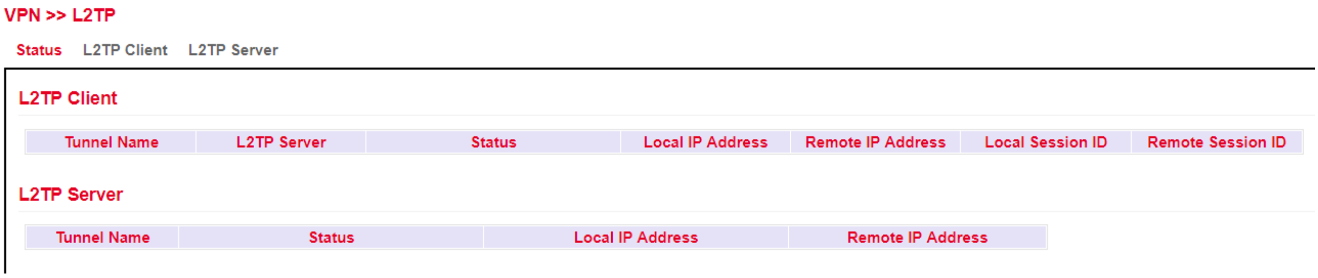
Enable	☑
Index	1
Network Type	Point to Point ▾
Local Virtual IP	192.168.2.10
Peer Virtual IP	192.168.3.10
Source Type	IP ▾
Local IP	192.168.2.50
Peer IP	192.168.3.20
Key	
MTU	
NHRP Enable	□
IPsec Profile	Disable ▾
Description	

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

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



VPN >> L2TP

L2TP Client

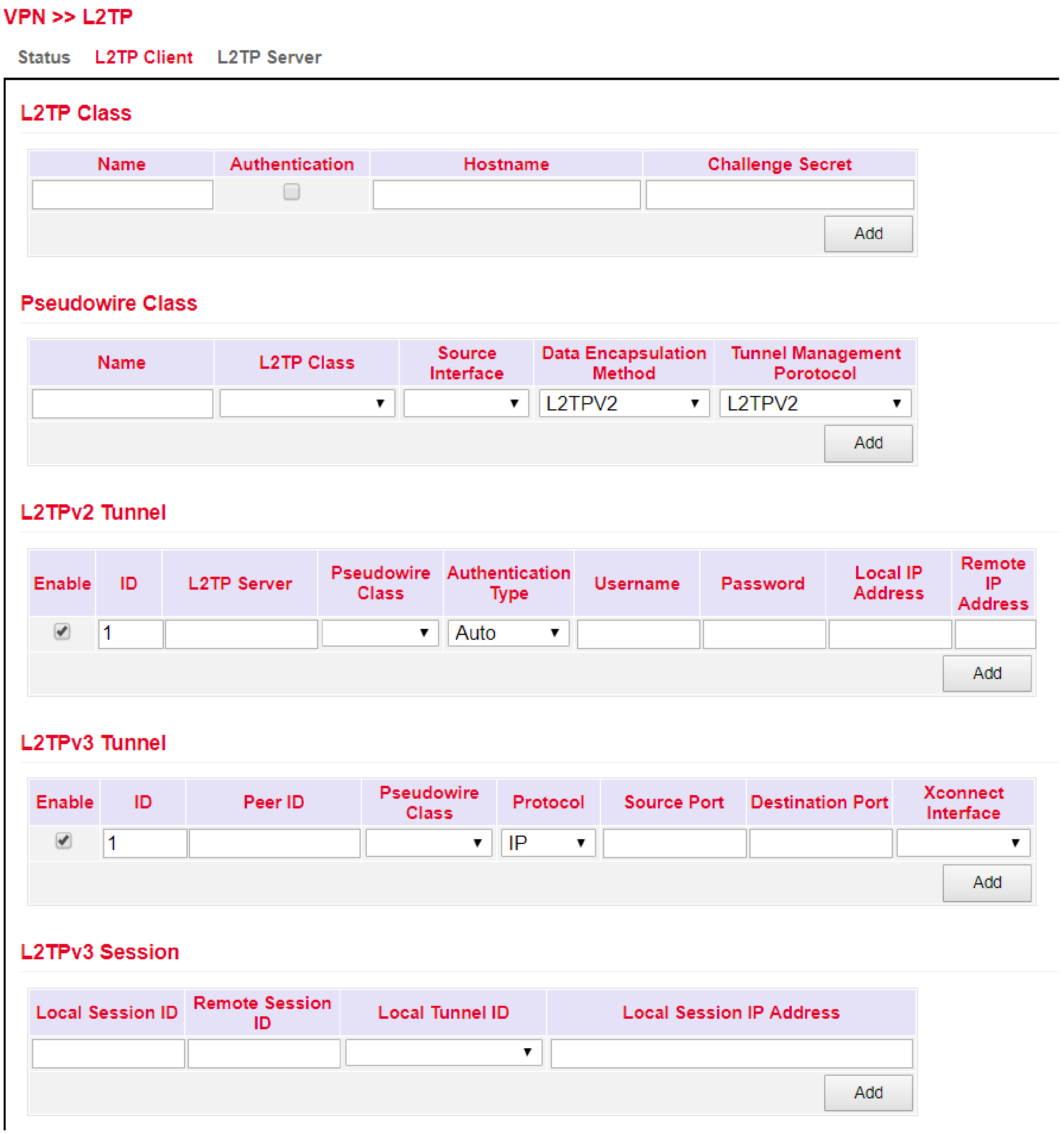
Tunnel Name	L2TP Server	Status	Local IP Address	Remote IP Address	Local Session ID	Remote Session ID

L2TP Server

Tunnel Name	Status	Local IP Address	Remote IP Address

3.7.3.2. L2TP Client

The corresponding client for the tunnel is created here under **VPN** > **L2TP** > **L2TP Client**. The respective entries must be added with the **Add** button and are not completely saved until the **Apply & Save** button is clicked.



VPN >> L2TP

L2TP Class

Name	Authentication	Hostname	Challenge Secret
	☐		
			Add

Pseudowire Class

Name	L2TP Class	Source Interface	Data Encapsulation Method	Tunnel Management Porotocol
	▼	▼	L2TPV2 ▼	L2TPV2 ▼
				Add

L2TPv2 Tunnel

Enable	ID	L2TP Server	Pseudowire Class	Authentication Type	Username	Password	Local IP Address	Remote IP Address
☑	1		▼	Auto ▼				
								Add

L2TPv3 Tunnel

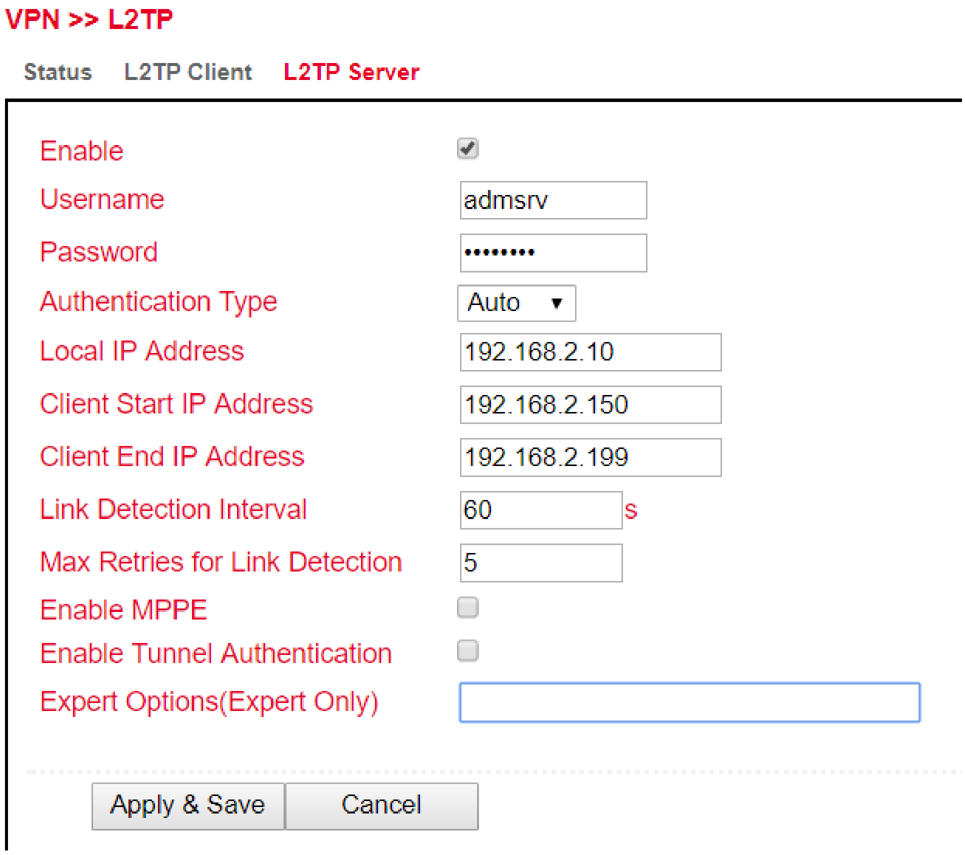
Enable	ID	Peer ID	Pseudowire Class	Protocol	Source Port	Destination Port	Xconnect Interface
☑	1		▼	IP ▼			▼
							Add

L2TPv3 Session

Local Session ID	Remote Session ID	Local Tunnel ID	Local Session IP Address
		▼	
			Add

3.7.3.3. L2TP Server

Here you can create a corresponding L2TP server.



Enable	☑
Username	admsrv
Password	••••••••
Authentication Type	Auto ▾
Local IP Address	192.168.2.10
Client Start IP Address	192.168.2.150
Client End IP Address	192.168.2.199
Link Detection Interval	60 s
Max Retries for Link Detection	5
Enable MPPE	☐
Enable Tunnel Authentication	☐
Expert Options(Expert Only)	

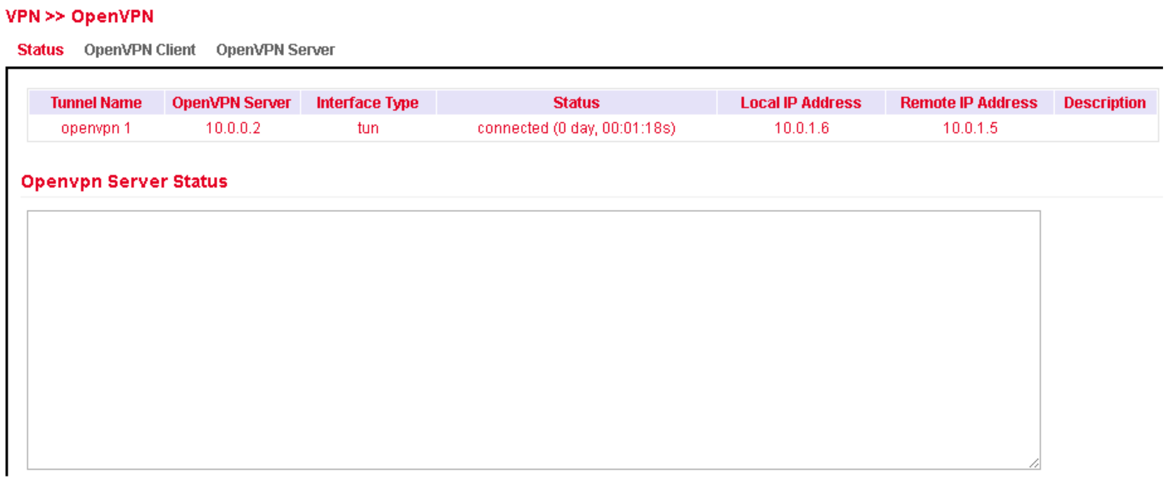
3.7.4. OpenVPN

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

3.7.4.1. OpenVPN Status

Overview of the status of the established OpenVPN.

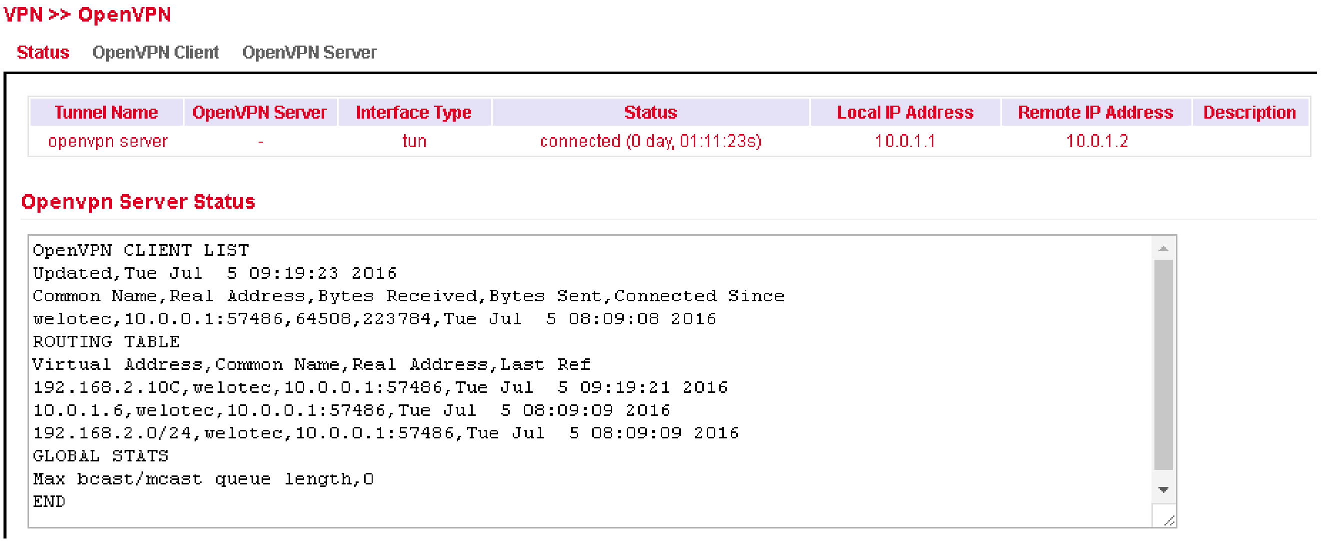
Client Status:



Tunnel Name	OpenVPN Server	Interface Type	Status	Local IP Address	Remote IP Address	Description
openvpn 1	10.0.0.2	tun	connected (0 day, 00:01:18s)	10.0.1.6	10.0.1.5	

Openvpn Server Status

Server Status:



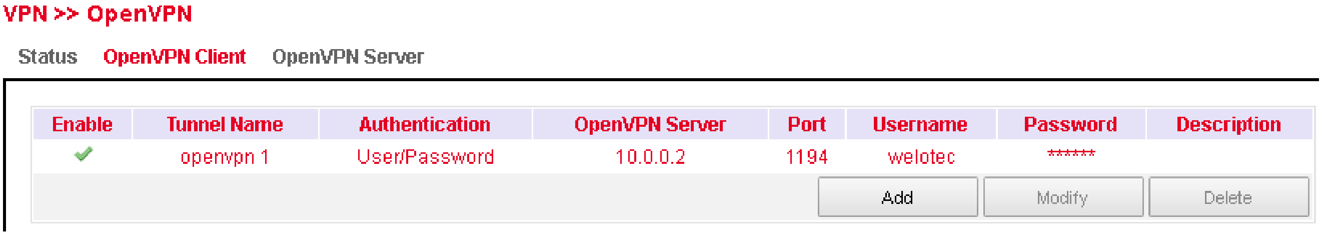
Tunnel Name	OpenVPN Server	Interface Type	Status	Local IP Address	Remote IP Address	Description
openvpn server	-	tun	connected (0 day, 01:11:23s)	10.0.1.1	10.0.1.2	

Openvpn Server Status

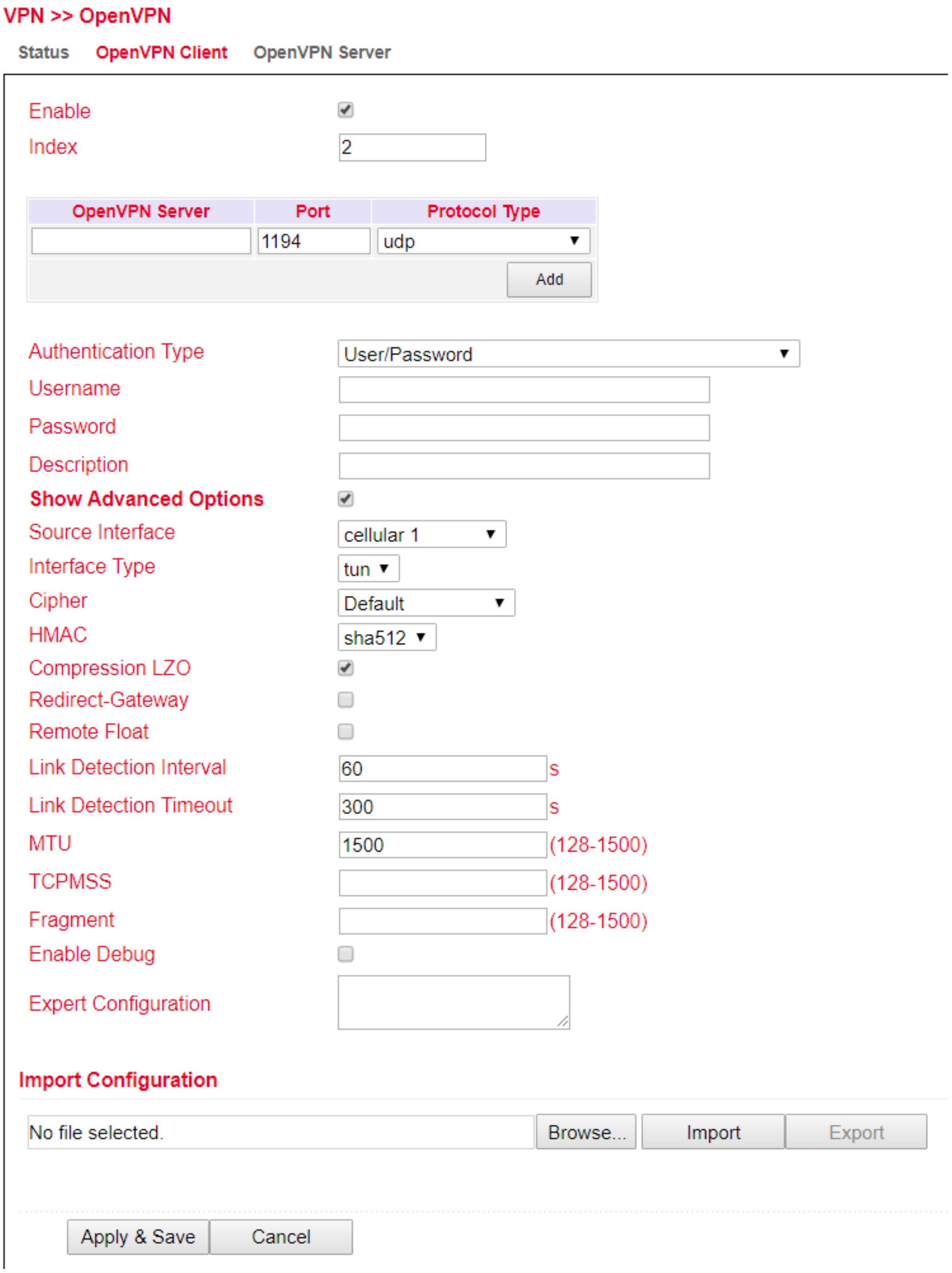
```
OpenVPN CLIENT LIST
Updated,Tue Jul  5 09:19:23 2016
Common Name,Real Address,Bytes Received,Bytes Sent,Connected Since
welotec,10.0.0.1:57486,64508,223784,Tue Jul  5 08:09:08 2016
ROUTING TABLE
Virtual Address,Common Name,Real Address,Last Ref
192.168.2.10C,welotec,10.0.0.1:57486,Tue Jul  5 09:19:21 2016
10.0.1.6,welotec,10.0.0.1:57486,Tue Jul  5 08:09:09 2016
192.168.2.0/24,welotec,10.0.0.1:57486,Tue Jul  5 08:09:09 2016
GLOBAL STATS
Max bcast/mcast queue length,0
END
```

3.7.4.2. OpenVPN Client

Under **VPN > OpenVPN > OpenVPN Client** a new OpenVPN tunnel can be added. The router must be configured as a client. Click on the button „**Add**" to create a new configuration.



Enable	Tunnel Name	Authentication	OpenVPN Server	Port	Username	Password	Description
✓	openvpn 1	User/Password	10.0.0.2	1194	welotec	******	



VPN >> OpenVPN

Enable	☑
Index	2

OpenVPN Server	Port	Protocol Type
	1194	udp ▼

Authentication Type	User/Password ▼
Username	
Password	
Description	
Show Advanced Options	☑
Source Interface	cellular 1 ▼
Interface Type	tun ▼
Cipher	Default ▼
HMAC	sha512 ▼
Compression LZO	☑
Redirect-Gateway	□
Remote Float	□
Link Detection Interval	60 s
Link Detection Timeout	300 s
MTU	1500 (128-1500)
TCPMSS	(128-1500)
Fragment	(128-1500)
Enable Debug	□
Expert Configuration	

Import Configuration

No file selected.

Note

Depending on the chosen authentication, different types of input are possible. This example treats, username/password.

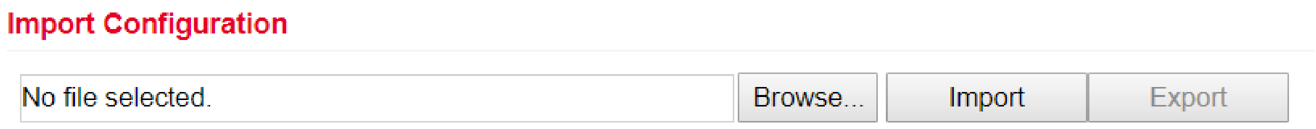
Parameter	Description
Enable	Switches the OpenVPN client on or off
Index	Freely selectable, for identification purposes only
OpenVPN Server	The IP address or FQDN of the OpenVPN server
Authentication Type	Authentication type (x509-cert recommended)
Username	Username
Password	Password
Description	Short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

Show Advanced Options:

Parameter	Description
Source Interface	The interface over which the OpenVPN tunnel
Interface Type	tun or tap (tun commended) should be established
Cipher	encryption method
HMAC	Sign all packages involved in the TLS handshake. Sha1 is standard
Compression LZO	Activate or deactivate compression of data
Redirect-Gateway	If redirect gateway is enabled, all traffic is routed through the tunnel.
Remote Float	If Remote Float is enabled, the client also accepts packets that match 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	Sets the maximum size for TCP packets
Fragment	Maximum packet size for UDP packets
Enable Debug	Turns debug mode on or off
Expert Configuration	Here OpenVPN tunnel options that are not available via the web interface can be entered directly.

⚠ Note

The client always requires the CA certificate of the server, otherwise it cannot authenticate itself.



Import Configuration

No file selected.

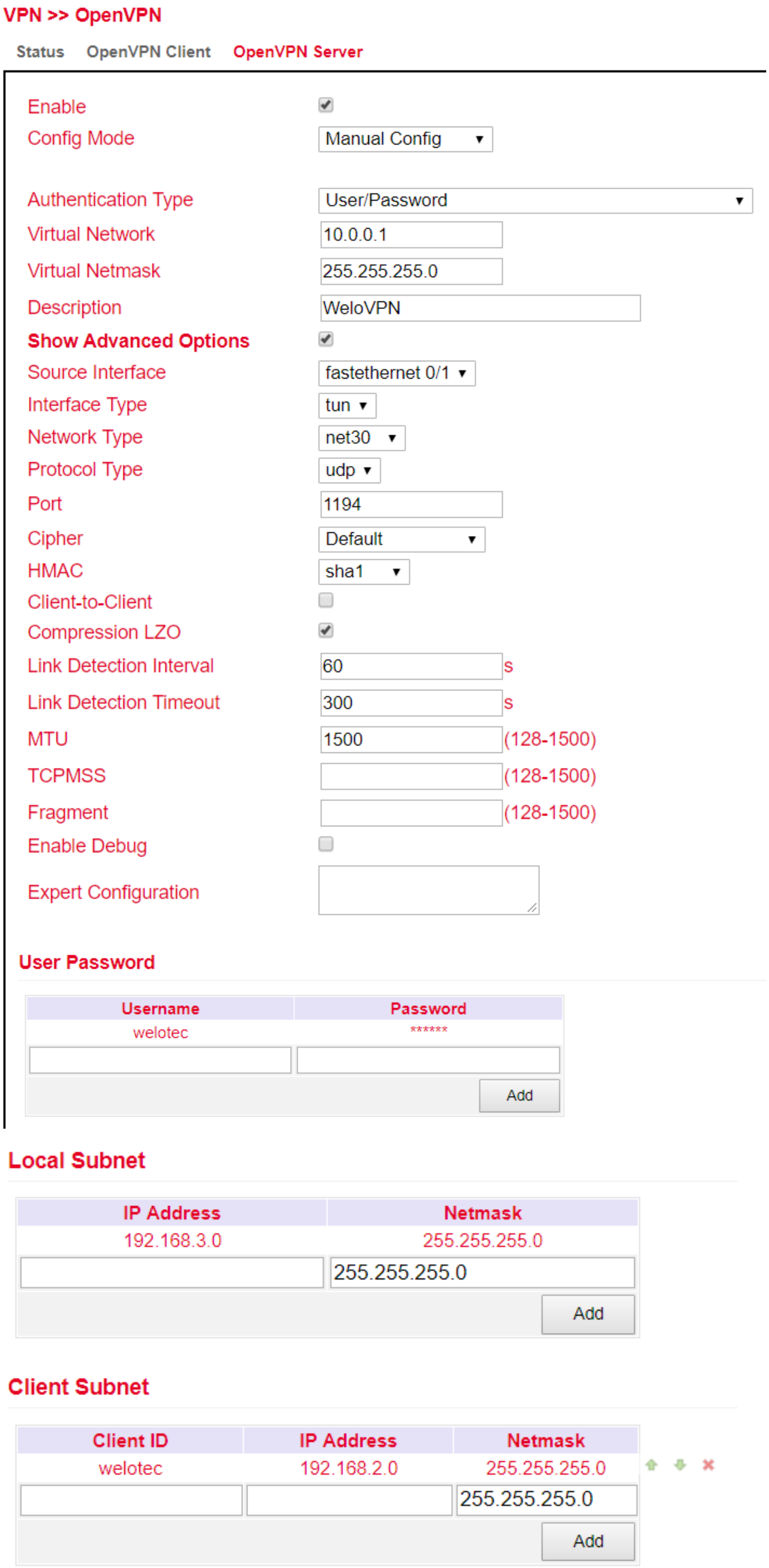
This can be used to import an existing OpenVPN configuration or to export the current configuration. The OpenVPN configuration can be exported from the OpenVPN server. This then has the file extension .ovpn.

⚠ Note

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 Server. A requirement for this is that the router has a **public IP adress**.



VPN >> OpenVPN

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	******

Local Subnet

IP Address	Netmask
192.168.3.0	255.255.255.0
	255.255.255.0

Client Subnet

Client ID	IP Address	Netmask
welotec	192.168.2.0	255.255.255.0
		255.255.255.0

Note

Depending on the chosen authentication, different entries are possible. This example treats, username/password.

Parameter	Description
Enable	Turns 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 Server

Advanced Options:

Parameter	Description
Source Interface	The Interface, over which the OpenVPN Tunnel should be established
Interface Type	tun or tap (tun commended)
Network Type	Connection type (net30 commended)
Protocol Type	UDP or TCP
Port	Port on which the OpenVPN server should 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	Activate or deactivate the compression of data
Link Detection Interval	Interval at which the tunnel connection is checked.
Link Detection Timeout	Timeout for a package for a tunnel connection check.
MTU	Maximum packet size
TCPMSS	Sets the maximum size for TCP packets
Fragment	Maximum packet size for UDP packets
Enable Debug	Turns the Debug-Mode on or off
Expert Configuration	Here you can directly enter OpenVPN tunnel options which are not available via the web interface.

User Password:
Clients can be added here, which can then log in with the username and password.

Local Subnet:
The local subnets of the router that should be accessible to the clients are entered here.

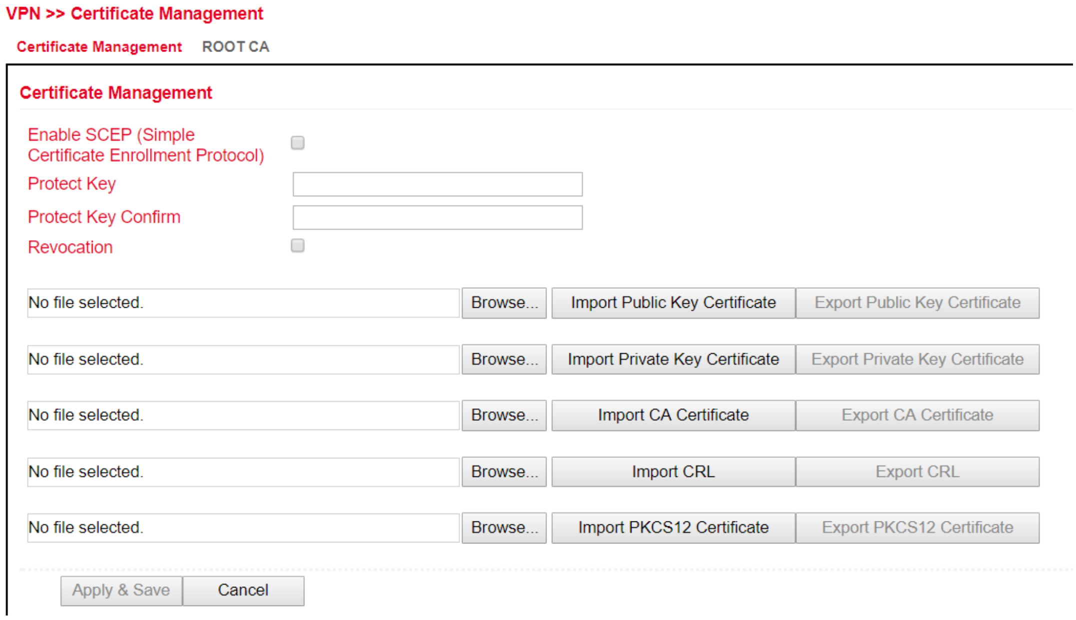
Client Subnet:
The client subnets that are to be accessible from the server side are entered here. The **Client ID** for the authentication method username/password is the username of the client and for certificates the common name.

⚠ Note

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

3.7.5. Certificate Management

Certificates for an IPSec tunnel or an OpenVPN tunnel are stored in Certificate Management unless they are secured via a Pre Shared Key (PSK).



VPN >> Certificate Management

Certificate Management ROOT CA

Certificate Management

Enable SCEP (Simple Certificate Enrollment Protocol) □

Protect Key

Protect Key Confirm

Revocation □

No file selected. Browse... Import Public Key Certificate Export Public Key Certificate

No file selected. Browse... Import Private Key Certificate Export Private Key Certificate

No file selected. Browse... Import CA Certificate Export CA Certificate

No file selected. Browse... Import CRL Export CRL

No file selected. Browse... Import PKCS12 Certificate Export PKCS12 Certificate

Apply & Save Cancel

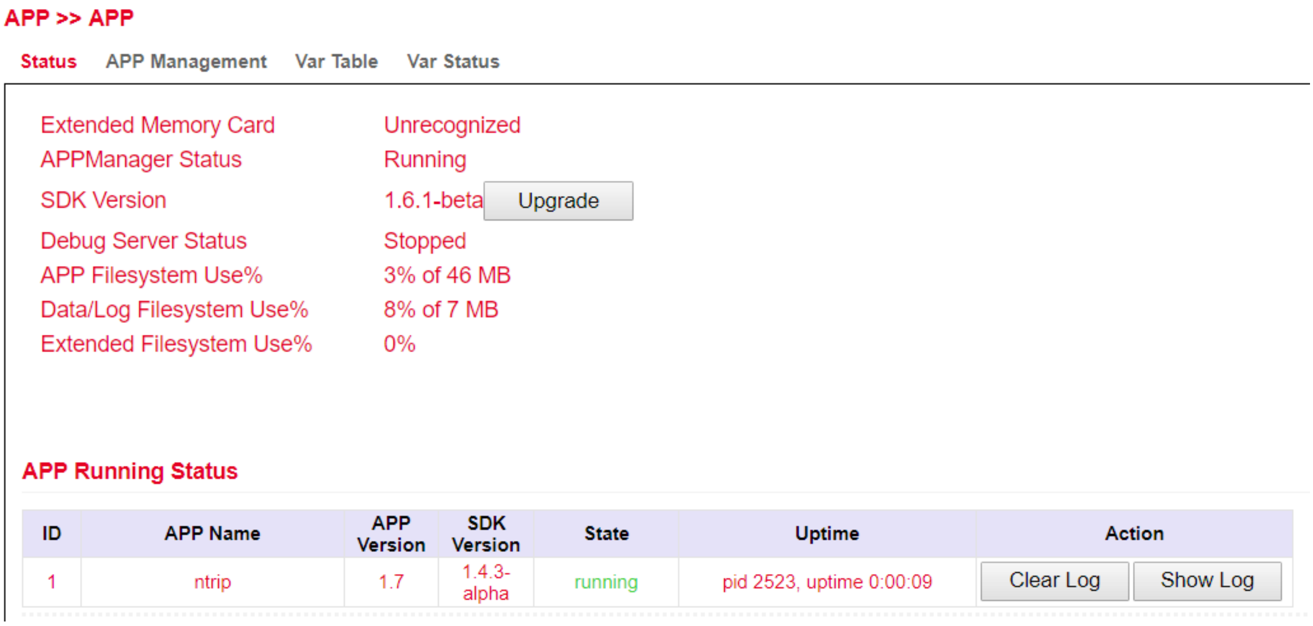
To upload a certificate, click on „**Browse**“, select the locally saved certificate and then click on „**Import**...“.

The „**Export Funktion**“ can be used to check whether the certificates have been properly uploaded. In case the files contain a size of 0-byte, 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 after the import under Protect Key and Protec Key Confirm.
Then click on „**Apply & Save**“ below 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 activate this function.
Protect Key	If the certificate is password-protected, the password for the certificate must be entered in this field, otherwise it cannot be uploaded correctly.
Protec Key Confirm	Enter the certificate password again to confirm the correctness of the entered password.
Revocation	Enable this feature to create a revocation list for invalid certificates.
Import Public Key Certificate	Public Key Certificate
Import Private Key Certivicate	Private Key Certificate.
Import CA Certificate	Certificate Authority (CA).
Import CRL	Certificate Revocation List.
Import PKCS12 Certifikate	PKCS12 Certificate

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). Using the client IDE you can create Python applications, compile them on the router and export them as .tar files. These .tar files can be uploaded via the system's WebUI.



APP >> APP

Status | APP Management | Var Table | Var Status

Extended Memory Card	Unrecognized
APPManager Status	Running
SDK Version	1.6.1-beta Upgrade
Debug Server Status	Stopped
APP Filesystem Use%	3% of 46 MB
Data/Log Filesystem Use%	8% of 7 MB
Extended Filesystem Use%	0%

APP Running Status

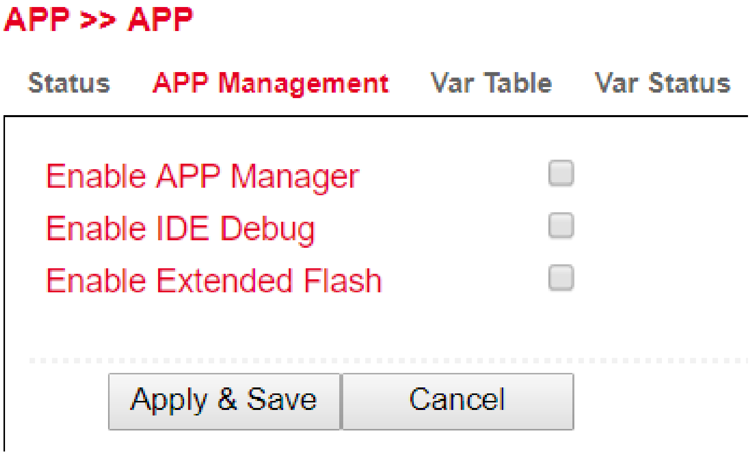
ID	APP Name	APP Version	SDK Version	State	Uptime	Action
1	ntrip	1.7	1.4.3-alpha	running	pid 2523, uptime 0:00:09	Clear Log Show Log

3.8.1. Status

Under the menu item **APP > APP** and **Status** you can see which Python SDK version is installed and which APP runs under Python. You can also use the upgrade button to update your Python SDK version.

3.8.2. AppManager Configuration

To use the client IDE, it is necessary to activate the Enable IDE Debug function on the TK800. For more information about using the client IDE, see the corresponding manual for the client IDE. We also recommend that you activate 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.



APP >> APP

Status | APP Management | Var Table | Var Status

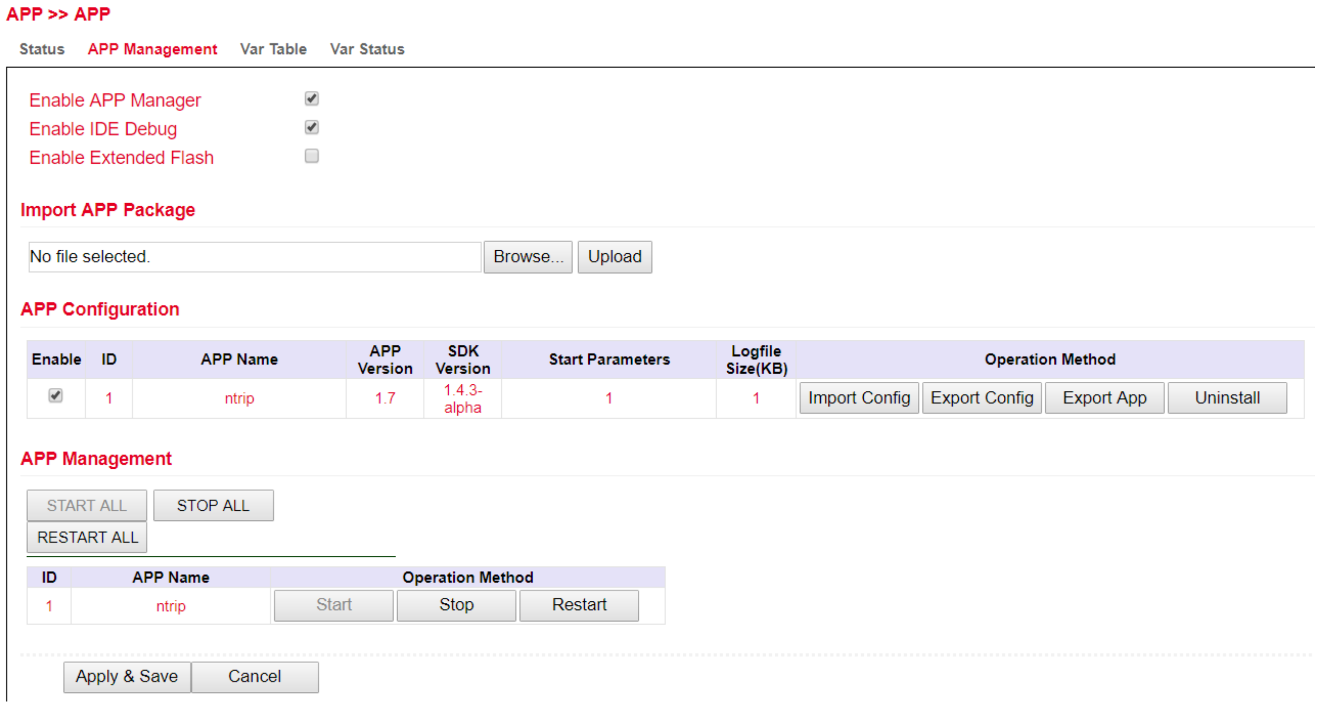
Enable APP Manager □

Enable IDE Debug □

Enable Extended Flash □

Apply & Save | Cancel

Please activate the functions Enable APP Manager and Enable IDE Debug. Then click Apply & Save.



APP >> APP

Status APP Management Var Table Var Status

Enable APP Manager ☑
Enable IDE Debug ☑
Enable Extended Flash □

Import APP Package

No file selected. [Browse...] [Upload]

APP Configuration

Enable	ID	APP Name	APP Version	SDK Version	Start Parameters	Logfile Size(KB)	Operation Method
☑	1	ntrip	1.7	1.4.3-alpha	1	1	Import Config Export Config Export App Uninstall

APP Management

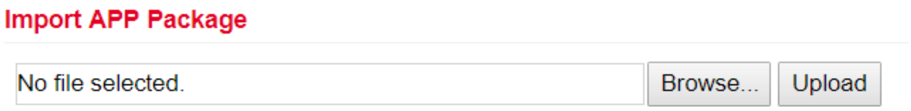
START ALL STOP ALL RESTART ALL

ID	APP Name	Operation Method
1	ntrip	Start Stop Restart

Apply & Save Cancel

Upload application

Once you have created your application, you can import it to other TK800 routers.
You can select „APP -> APP -> APP Management“ and click on „Browse“ at Import APP Package.

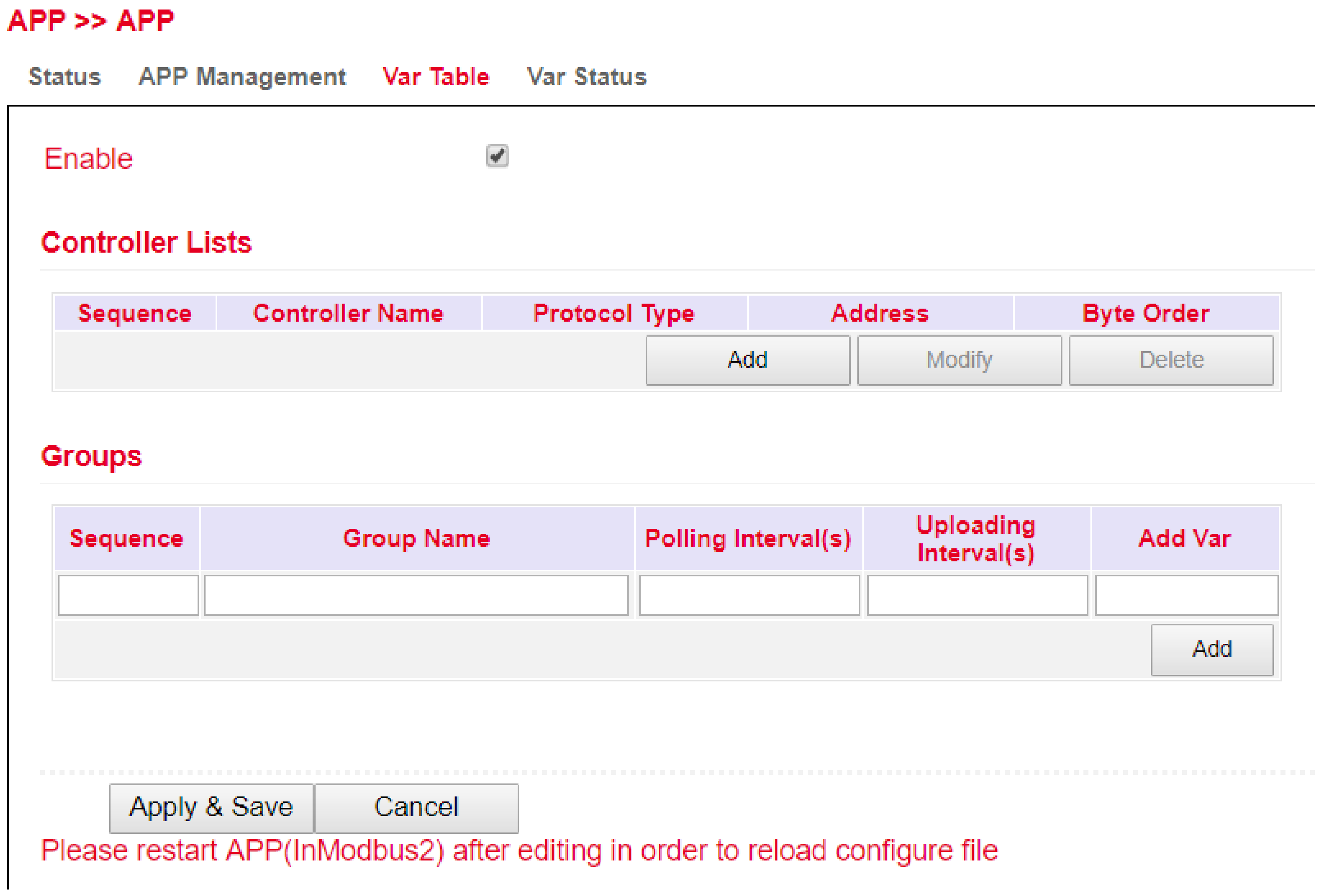


Import APP Package

No file selected. [Browse...] [Upload]

Select your .tar file and click Upload.
After confirming the upload with „OK“, the application will be uploaded to the system.
If necessary, you can then upload your configuration and activate the application by clicking Enable.

3.8.3. Var Table



APP >> APP

Status APP Management Var Table Var Status

Enable ☑

Controller Lists

Sequence	Controller Name	Protocol Type	Address	Byte Order

Groups

Sequence	Group Name	Polling Interval(s)	Uploading Interval(s)	Add Var

Please restart APP(InModbus2) after editing in order to reload configure file

In this area you have the possibility to set variables with the corresponding Modbus App. This APP has not yet been finalized and is therefore not yet available.

3.8.4. Var Status

APP >> APP

Status APP Management Var Table Var Status

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

3.9. Industrial

Note

The Industrial functions are available for all models of the TK800 series with “EX” in the name. Example: TK8x2L-EX0.
The following functions are available:

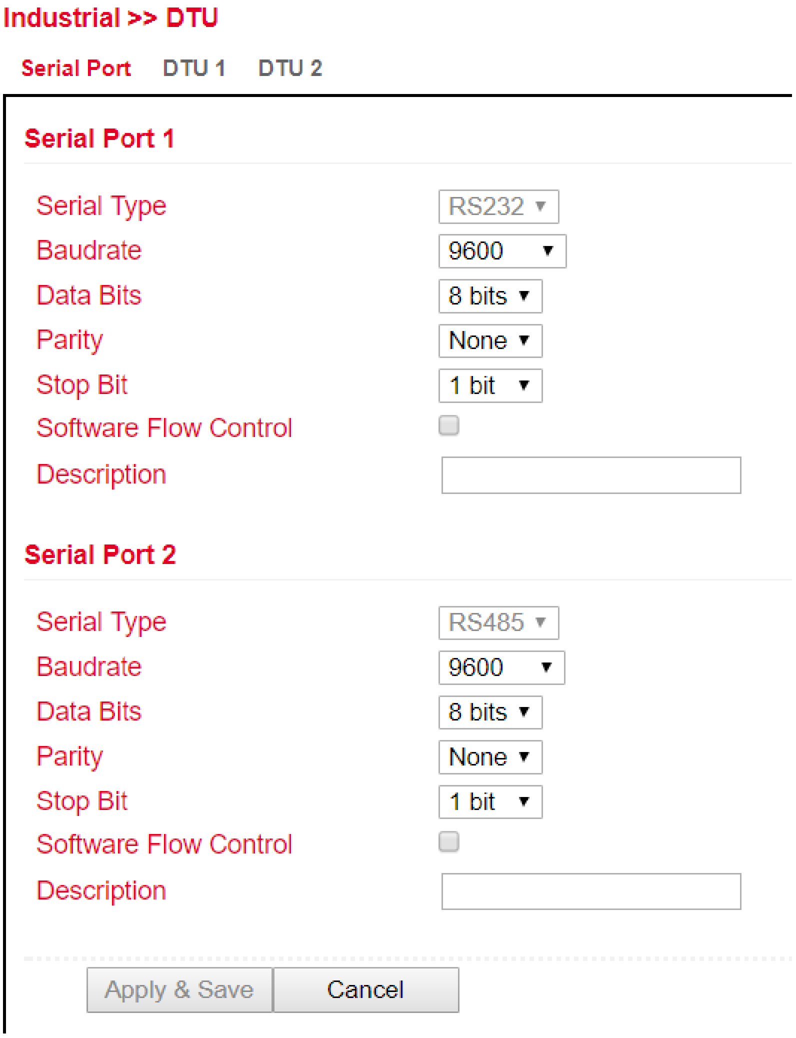
- Digital Input
- Relay Output
- RS-232 Interface
- RS-485 Interface

3.9.1. DTU

DTU stands for Data Terminal Unit and is used to connect devices with a serial interface (RS-232 and RS-485). The configuration of the DTU properties always consists of two parts.
The properties of the interface can be defined under **Serial Port**. Here you can find the parameters for the RS-232 and the RS-485 interface. Under **DTU 1 (RS-232)** and **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.


Industrial >> DTU

Serial Port DTU 1 DTU 2

Serial Port 1

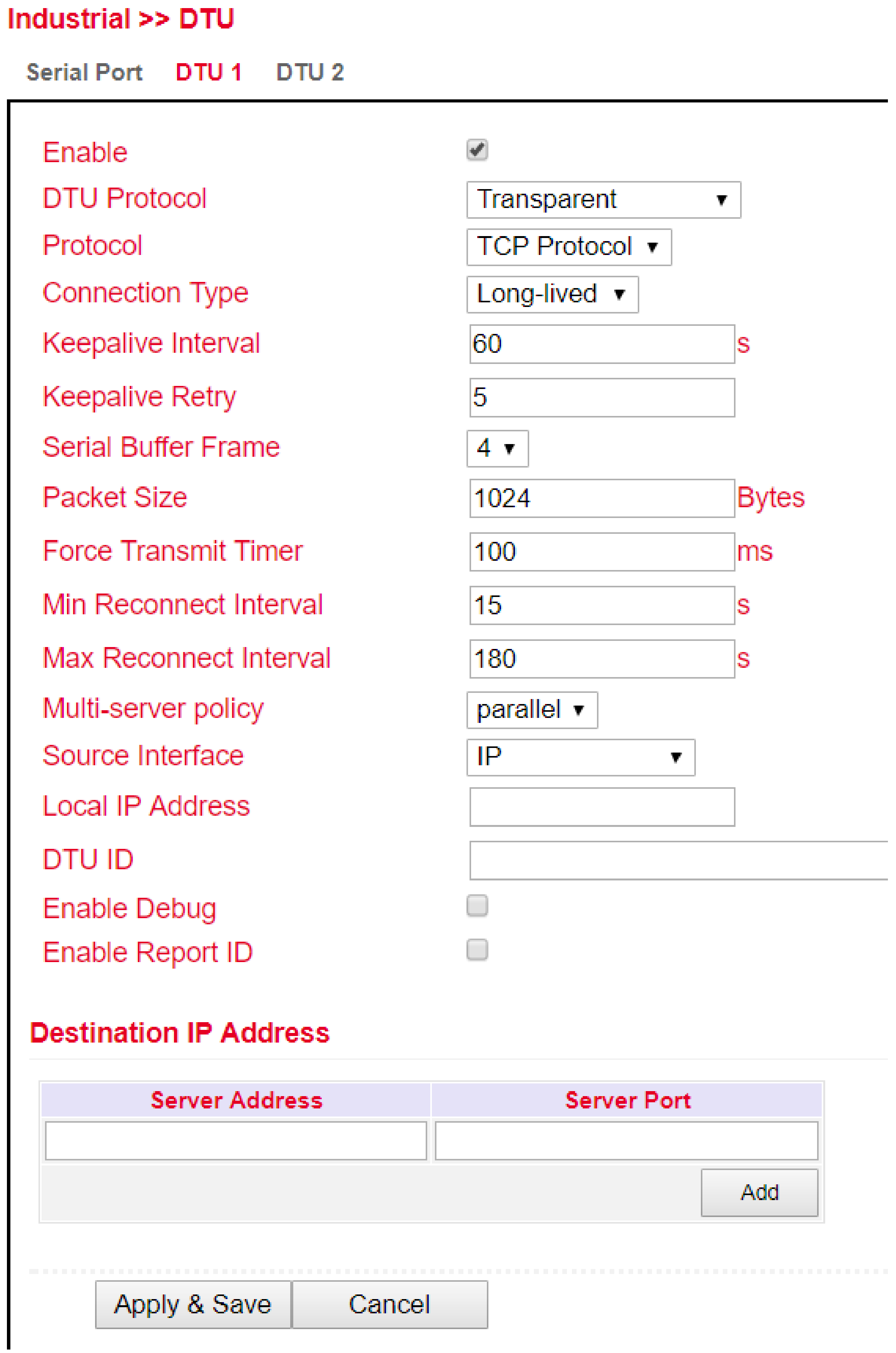
Serial Type	RS232 ▾
Baudrate	9600 ▾
Data Bits	8 bits ▾
Parity	None ▾
Stop Bit	1 bit ▾
Software Flow Control	□
Description	

Serial Port 2

Serial Type	RS485 ▾
Baudrate	9600 ▾
Data Bits	8 bits ▾
Parity	None ▾
Stop Bit	1 bit ▾
Software Flow Control	□
Description	

3.9.1.2. DTU 1 / DTU 2

Transparent



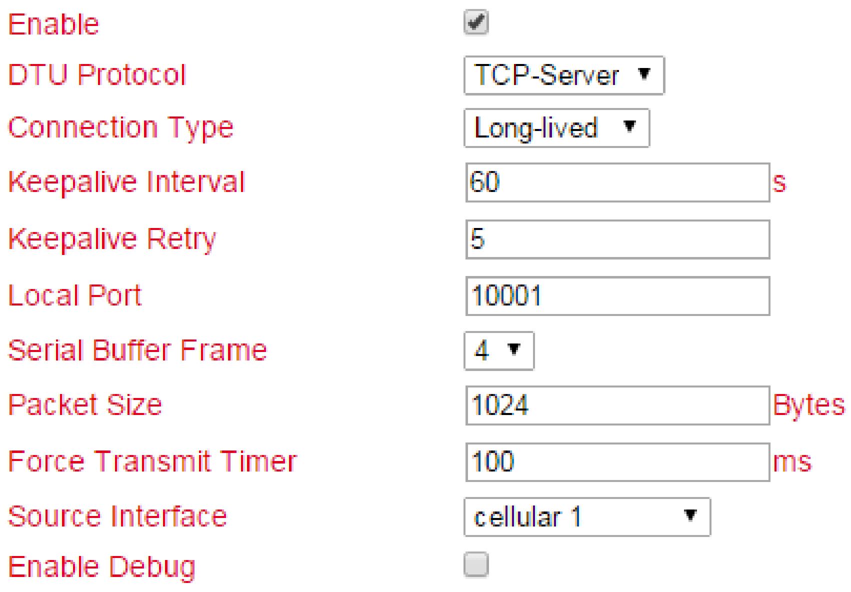
Industrial >> DTU

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

Destination IP Address

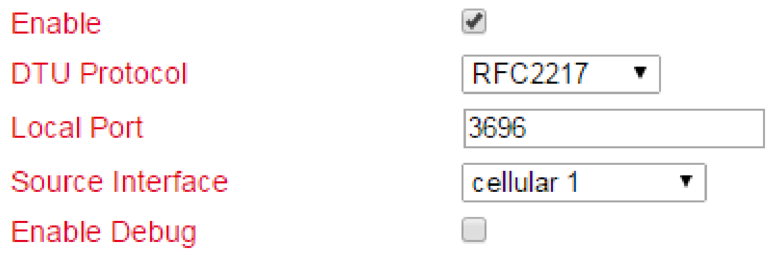
Server Address	Server Port

Select TCP server for DTU Protocol



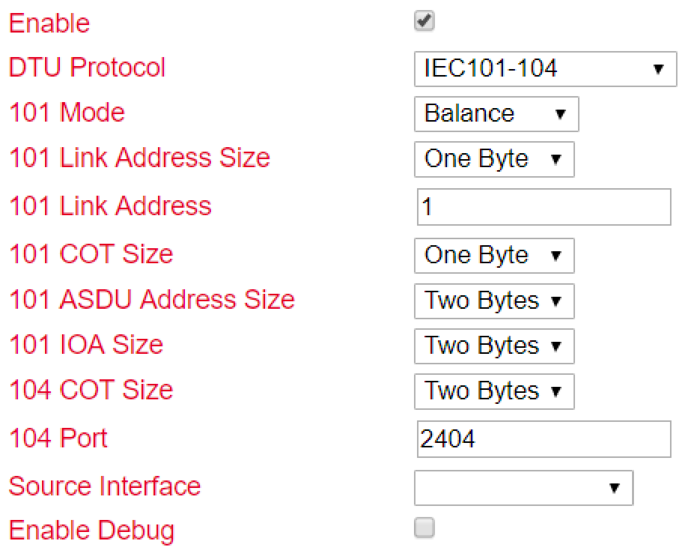
Enable	☑
DTU Protocol	TCP-Server ▼
Connection Type	Long-lived ▼
Keepalive Interval	60 s
Keepalive Retry	5
Local Port	10001
Serial Buffer Frame	4 ▼
Packet Size	1024 Bytes
Force Transmit Timer	100 ms
Source Interface	cellular 1 ▼
Enable Debug	☐

Selection RFC2217 for DTU Protocol



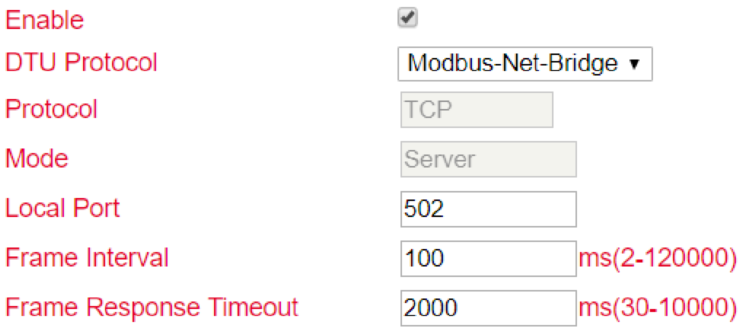
Enable	☑
DTU Protocol	RFC2217 ▼
Local Port	3696
Source Interface	cellular 1 ▼
Enable Debug	☐

Selection IEC60870-5-101/104 for DTU Protocol



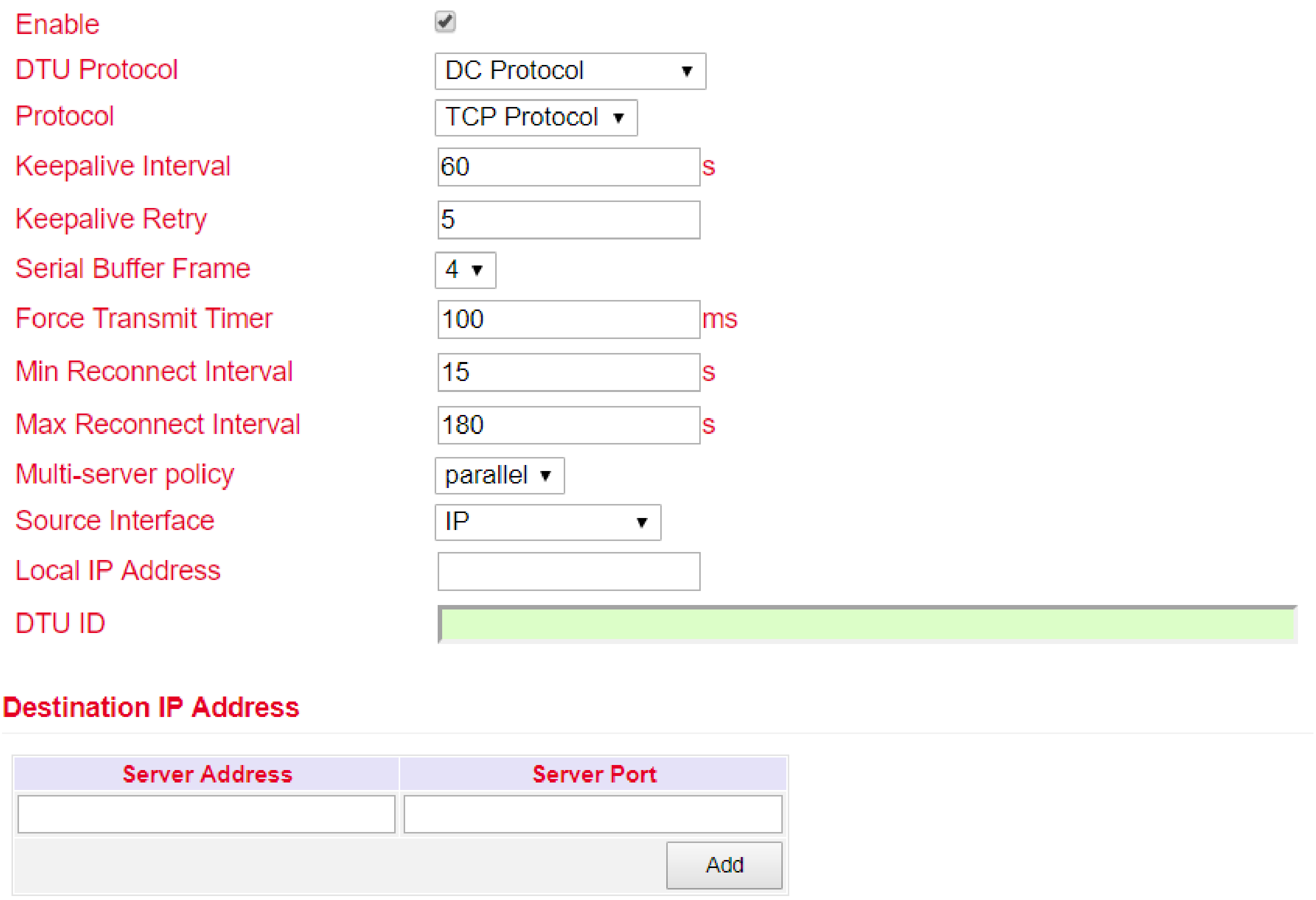
Enable	☑
DTU Protocol	IEC101-104 ▾
101 Mode	Balance ▾
101 Link Address Size	One Byte ▾
101 Link Address	1
101 COT Size	One Byte ▾
101 ASDU Address Size	Two Bytes ▾
101 IOA Size	Two Bytes ▾
104 COT Size	Two Bytes ▾
104 Port	2404
Source Interface	▾
Enable Debug	□

Selection of Modbus-Net-Bridge at DTU Protocol



Enable	☑
DTU Protocol	Modbus-Net-Bridge ▾
Protocol	TCP
Mode	Server
Local Port	502
Frame Interval	100 ms(2-120000)
Frame Response Timeout	2000 ms(30-10000)

Select DC Protocol for DTU Protocol



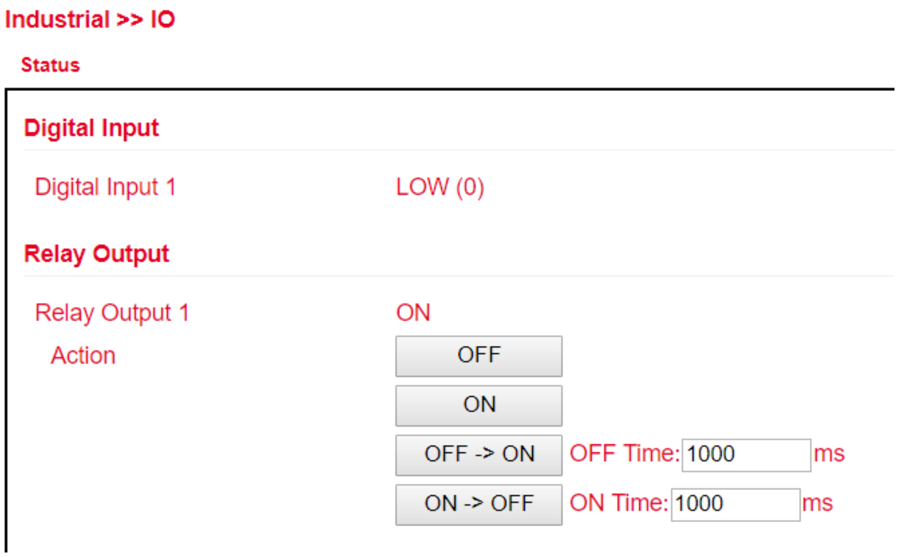
Enable	☑
DTU Protocol	DC Protocol ▾
Protocol	TCP Protocol ▾
Keepalive Interval	60 s
Keepalive Retry	5
Serial Buffer Frame	4 ▾
Force Transmit Timer	100 ms
Min Reconnect Interval	15 s
Max Reconnect Interval	180 s
Multi-server policy	parallel ▾
Source Interface	IP ▾
Local IP Address	
DTU ID	

Destination IP Address

Server Address	Server Port

3.9.2. IO

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



Industrial >> IO

Status

Digital Input

Digital Input 1 LOW (0)

Relay Output

Relay Output 1 ON

Action

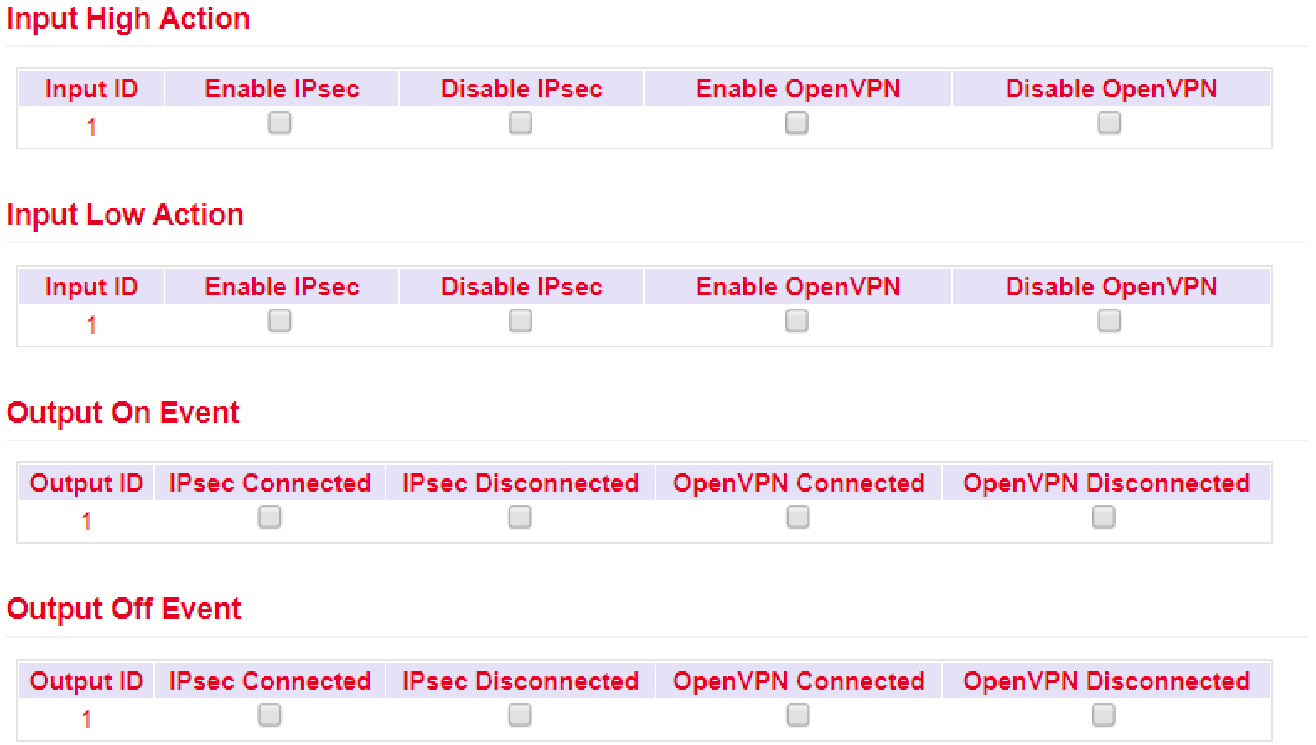
OFF Time: 1000 ms

ON Time: 1000 ms

Digital Input:
Displays the status of the digital input.

Relay Output:

Parameter	Description
Relay Output 1	Status of the Relay Output
Action	Switching on, switching off or defining a cycle



Input High Action

Input ID	Enable IPsec	Disable IPsec	Enable OpenVPN	Disable OpenVPN
1	□	□	□	□

Input Low Action

Input ID	Enable IPsec	Disable IPsec	Enable OpenVPN	Disable OpenVPN
1	□	□	□	□

Output On Event

Output ID	IPsec Connected	IPsec Disconnected	OpenVPN Connected	OpenVPN Disconnected
1	□	□	□	□

Output Off Event

Output ID	IPsec Connected	IPsec Disconnected	OpenVPN Connected	OpenVPN Disconnected
1	□	□	□	□

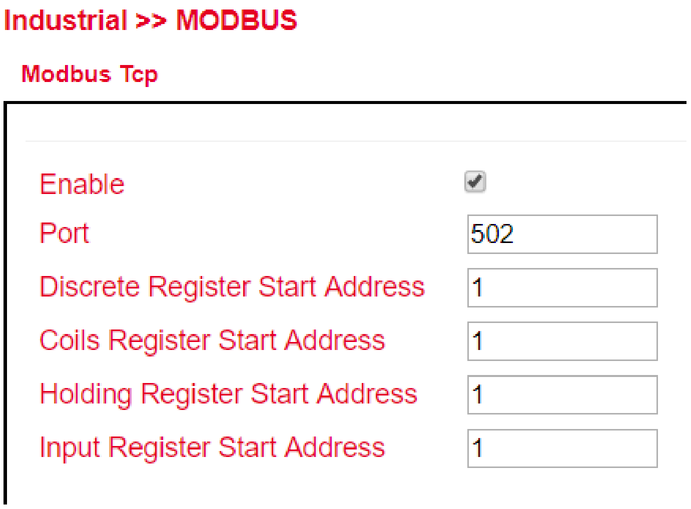
Input High/Low Action:
Description
Default relay settings on or off. This allows the status of the relay output to be turned on or off, or a corresponding cycle to be defined.
Here, an OpenVPN or IPsec tunnel can be started or stopped via the digital input.

Output On/Off Event:
Here the relay output can be used to start or stop IPsec and OpenVPN.

3.9.3. 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 turn the corresponding settings on or off.



Industrial >> MODBUS

Modbus Tcp

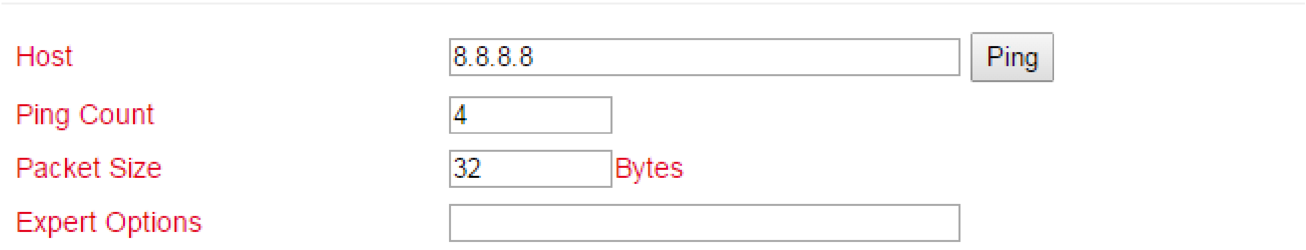
Enable	☑
Port	502
Discrete Register Start Address	1
Coils Register Start Address	1
Holding Register Start Address	1
Input Register Start Address	1

3.10.Tools

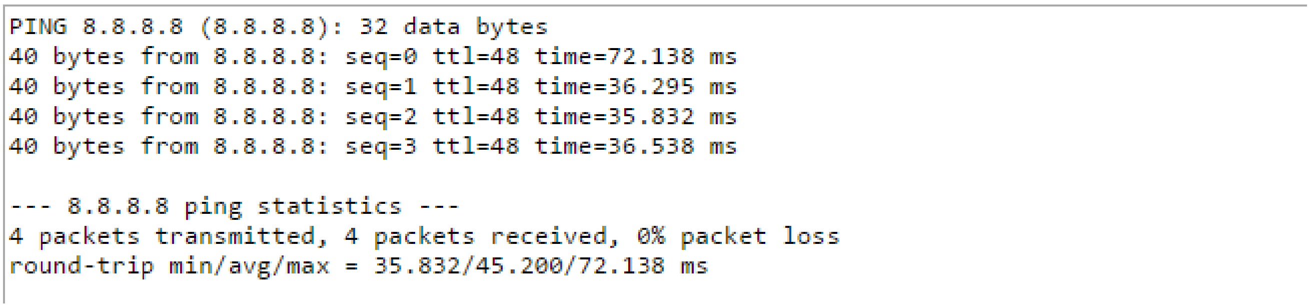
Useful tools that can be used for pinging, tracing etc.

3.10.1. Ping

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



Host	8.8.8.8
Ping Count	4
Packet Size	32 Bytes
Expert Options	

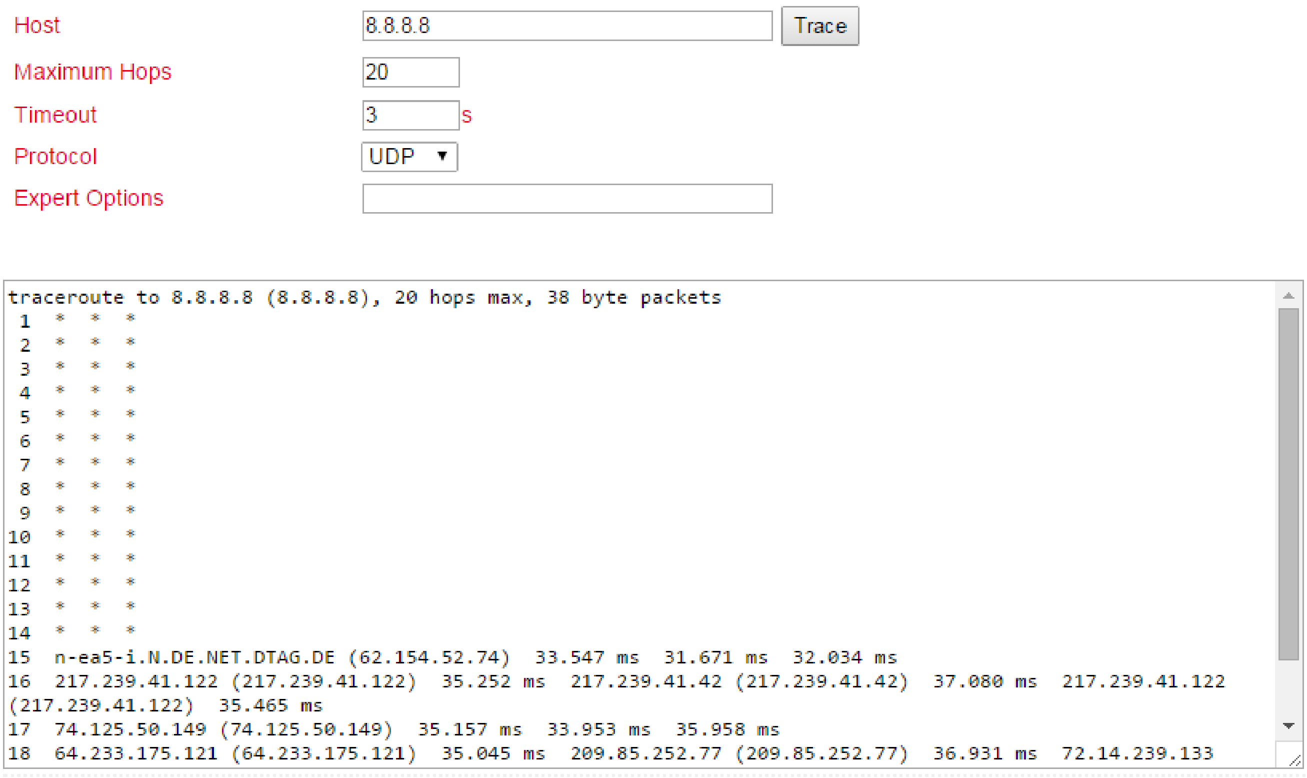


```
PING 8.8.8.8 (8.8.8.8): 32 data bytes
40 bytes from 8.8.8.8: seq=0 ttl=48 time=72.138 ms
40 bytes from 8.8.8.8: seq=1 ttl=48 time=36.295 ms
40 bytes from 8.8.8.8: seq=2 ttl=48 time=35.832 ms
40 bytes from 8.8.8.8: seq=3 ttl=48 time=36.538 ms

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

Parameter	Description
Host	Input of the address to be pinged on
Ping Count	Number of executed pings. Input from 1 to 50 possible. Standard is 4
Packet Size	Size of the package to be sent. Standard is 32 bytes
Expert Options	Advanced functions

3.10.2. Traceroute

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



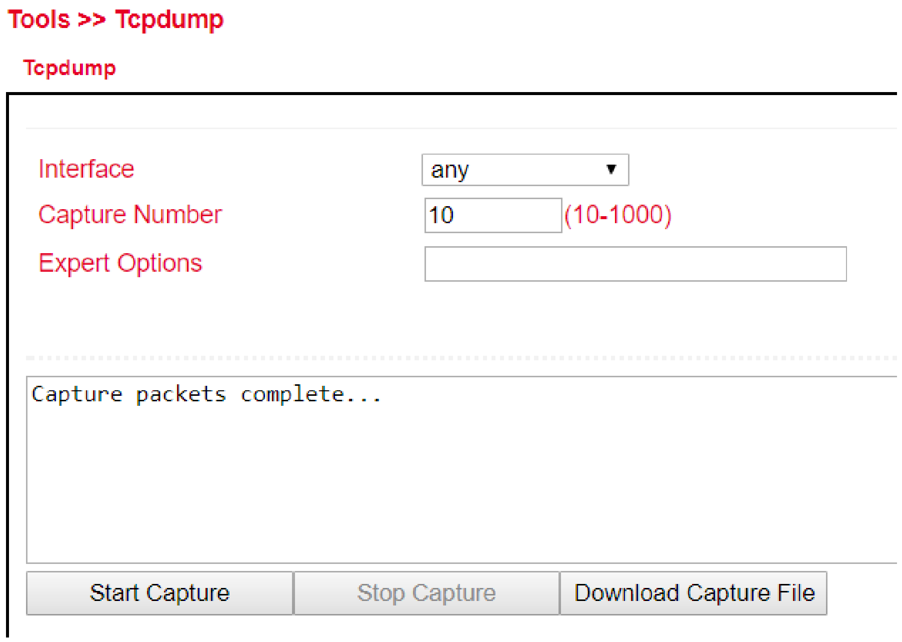
Host	8.8.8.8
Maximum Hops	20
Timeout	3 s
Protocol	UDP
Expert Options	

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

Parameter	Description
Host	Enter the destination host to be discovered.
Maximum Hops	Number of hops executed. Input from 2 to 40 possible. Standard is 20
Timeout	Enter the timeout in seconds. value can be between 2 and 10s.
Protocol	Optional entweder ICMP oder UDP. Standard ist UDP
Expert Options	Advanced functions

3.10.3. Tcpdump

Well-known and widely used packet sniffer. Enables recording of TCP packets.
You can reach this sniffer via **Tools** > **Tcpdump**.



Tools >> Tcpdump

Tcpdump

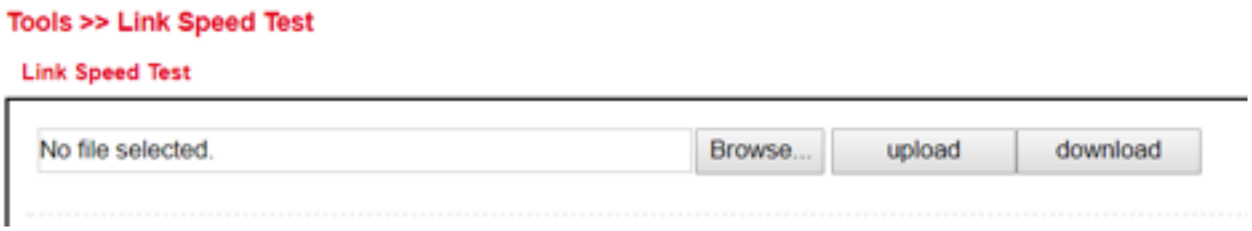
Interface	any
Capture Number	10 (10-1000)
Expert Options	

```
Capture packets complete...
```

Parameter	Description
Interface	Selection of the interface to be recorded
Capture Number	Number of recordings. Standard is 10
Expert Options	Extended functions
Start Capture (Button)	Starts the recording of data packets
Stop Capture (Button)	Stops the recording of data packets
Download Capture File (Button)	Download the recording as tcpdump. pcap file. Readable e. g. with Wireshark

3.10.4. Link Speed Test

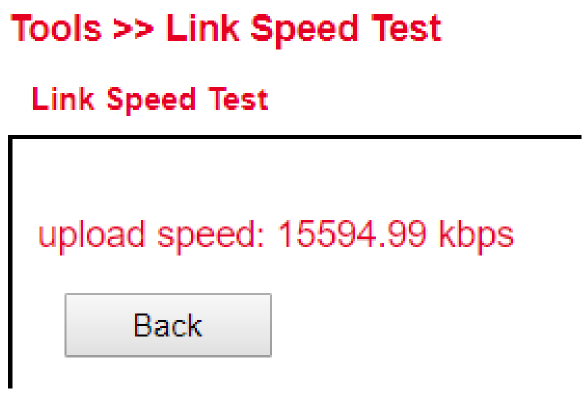
Determine the connection speed by uploading and downloading files.



Tools >> Link Speed Test

Link Speed Test

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



Tools >> Link Speed Test

Link Speed Test

upload speed: 15594.99 kbps

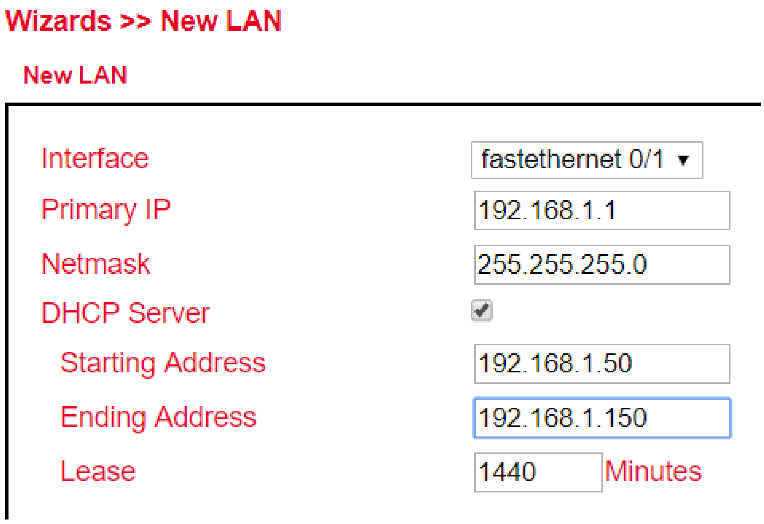
Via the **download** button you can download a 130MB file (test. bin) about which you can see the download speed during the download.

3.11.Wizards

These are assistants (wizards) to facilitate the creation of the following processes.

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 then creates all required data in the background.



Wizards >> New LAN

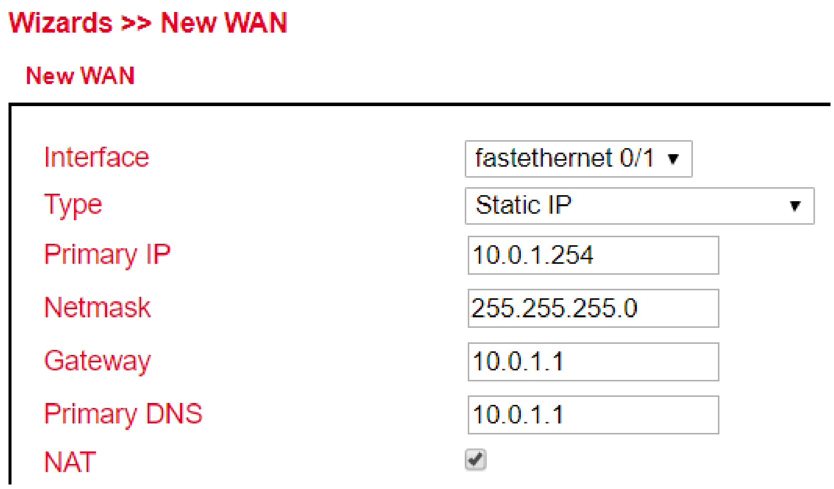
New LAN

Interface	fastethernet 0/1 ▾
Primary IP	192.168.1.1
Netmask	255.255.255.0
DHCP Server	☑
Starting Address	192.168.1.50
Ending Address	192.168.1.150
Lease	1440 Minutes

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

3.11.2. New WAN

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



Wizards >> New WAN

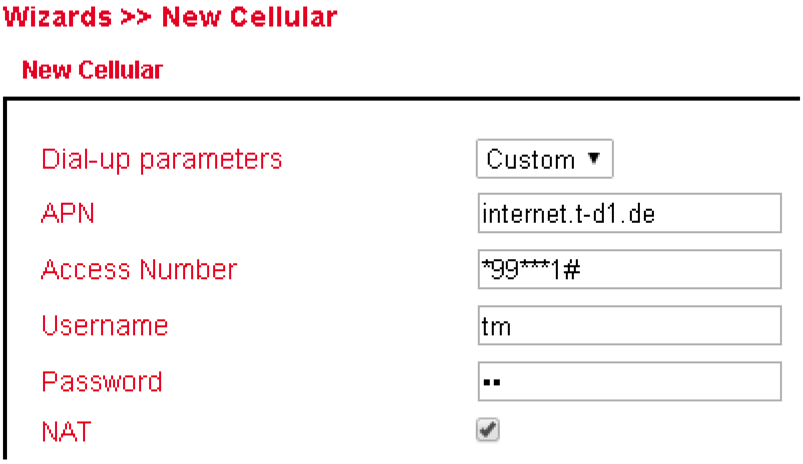
New WAN

Interface	fastethernet 0/1 ▾
Type	Static IP ▾
Primary IP	10.0.1.254
Netmask	255.255.255.0
Gateway	10.0.1.1
Primary DNS	10.0.1.1
NAT	☑

Parameter	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 interfaces
Netmask	The Subnet mask of the interfaces
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: Username of the provider for ADSL access. **Important**: For this purpose a DSL modem is required
Password	If PPPoE is selected under Type: Password of the provider for ADSL access. **Important**: For this purpose a DSL modem is required

3.11.3. New Cellular

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



Wizards >> New Cellular

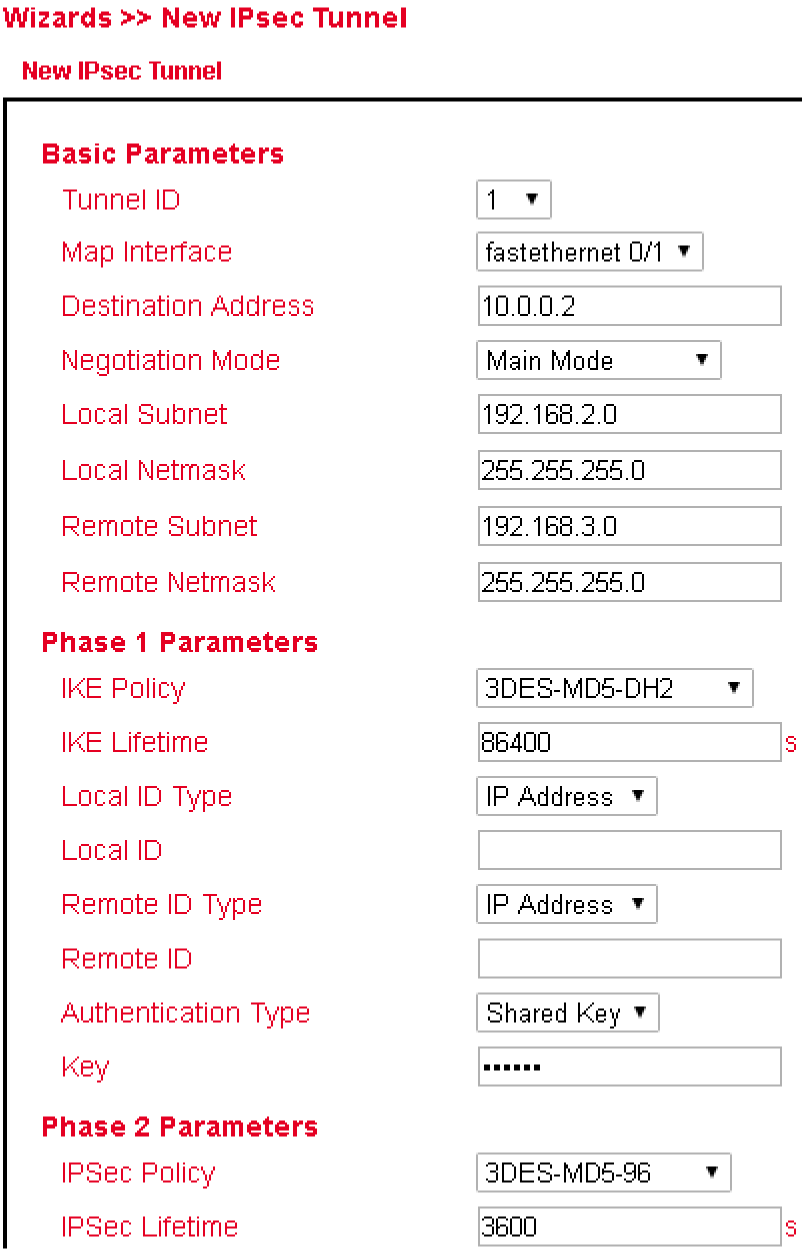
New Cellular

Dial-up parameters	Custom ▼
APN	internet.t-d1.de
Access Number	*99***1#
Username	tm
Password	••
NAT	☑

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 for the APN mentioned above, if this is necessary.
NAT	Activate or deactivate NAT

3.11.4. New IPsec Tunnel

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



Wizards >> New IPsec Tunnel

New IPsec Tunnel

Basic Parameters

Tunnel ID	1 ▼
Map Interface	fastethernet 0/1 ▼
Destination Address	10.0.0.2
Negotiation Mode	Main Mode ▼
Local Subnet	192.168.2.0
Local Netmask	255.255.255.0
Remote Subnet	192.168.3.0
Remote Netmask	255.255.255.0

Phase 1 Parameters

IKE Policy	3DES-MD5-DH2 ▼
IKE Lifetime	86400 s
Local ID Type	IP Address ▼
Local ID	
Remote ID Type	IP Address ▼
Remote ID	
Authentication Type	Shared Key ▼
Key	••••••

Phase 2 Parameters

IPSec Policy	3DES-MD5-96 ▼
IPSec Lifetime	3600 s

Basic Parameters:

Parameter	Description
Tunnel ID	Used to identify 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 to be reached by the remote station
Local Netmask	Subnet mask of the router
Remote Subnet	The subnetwork of the remote station
Remote Netmask	The subnet mask of the remote station

Phase 1 Parameters:

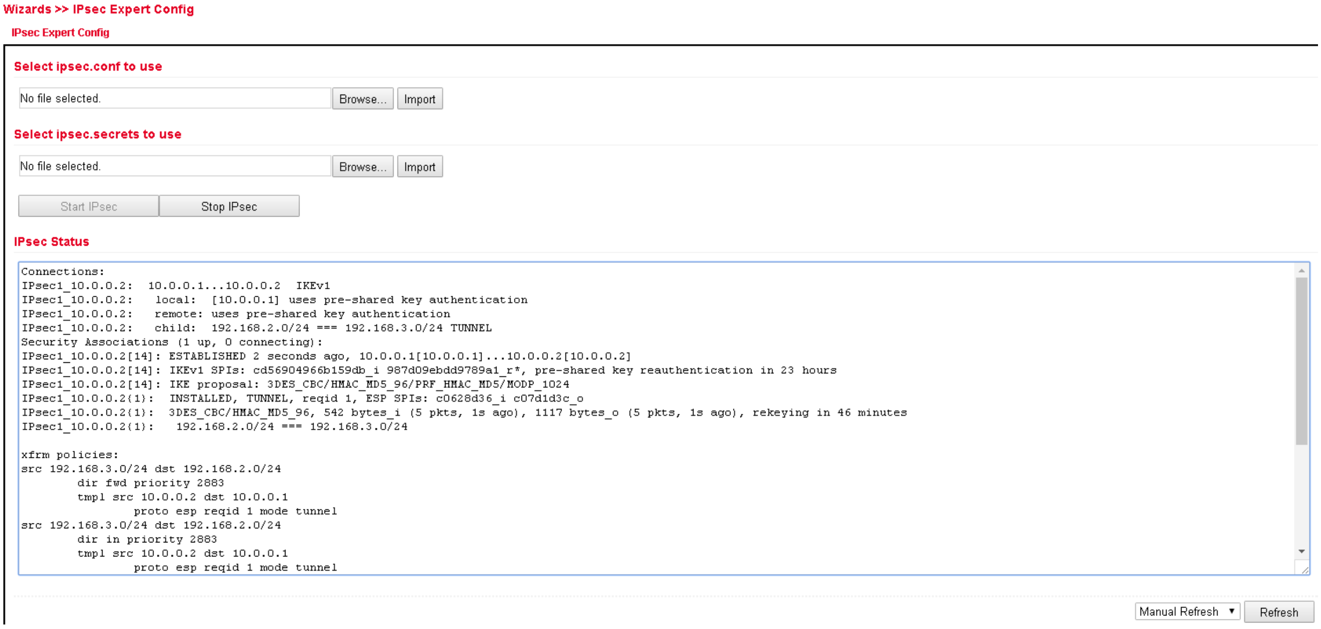
Parameter	Description
IKE Policy	Encryption / Hash / Diffie-Hellman-Group
IKE Lifetime	Validity periode of IKE policy
Local ID Type	IP Address / FQDN / User FQDN
Local ID	IP Address or FQDN
Remote ID Type	IP Address / FQDN / User FQDN
Remote ID	IP Address or FQDN
Authentication Type	Pre-shared key or certificate authentication method
Key	Pre-Shared-Key

Phase 2 Parameters:

Parameter	Description
IPSec Policy	Encryption / Hash
IPSec Lifetime	Validity period of the IPsec policy

3.11.5. IPsec Expert Config

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



Wizards >> IPsec Expert Config

IPsec Expert Config

Select ipsec.conf to use

No file selected.

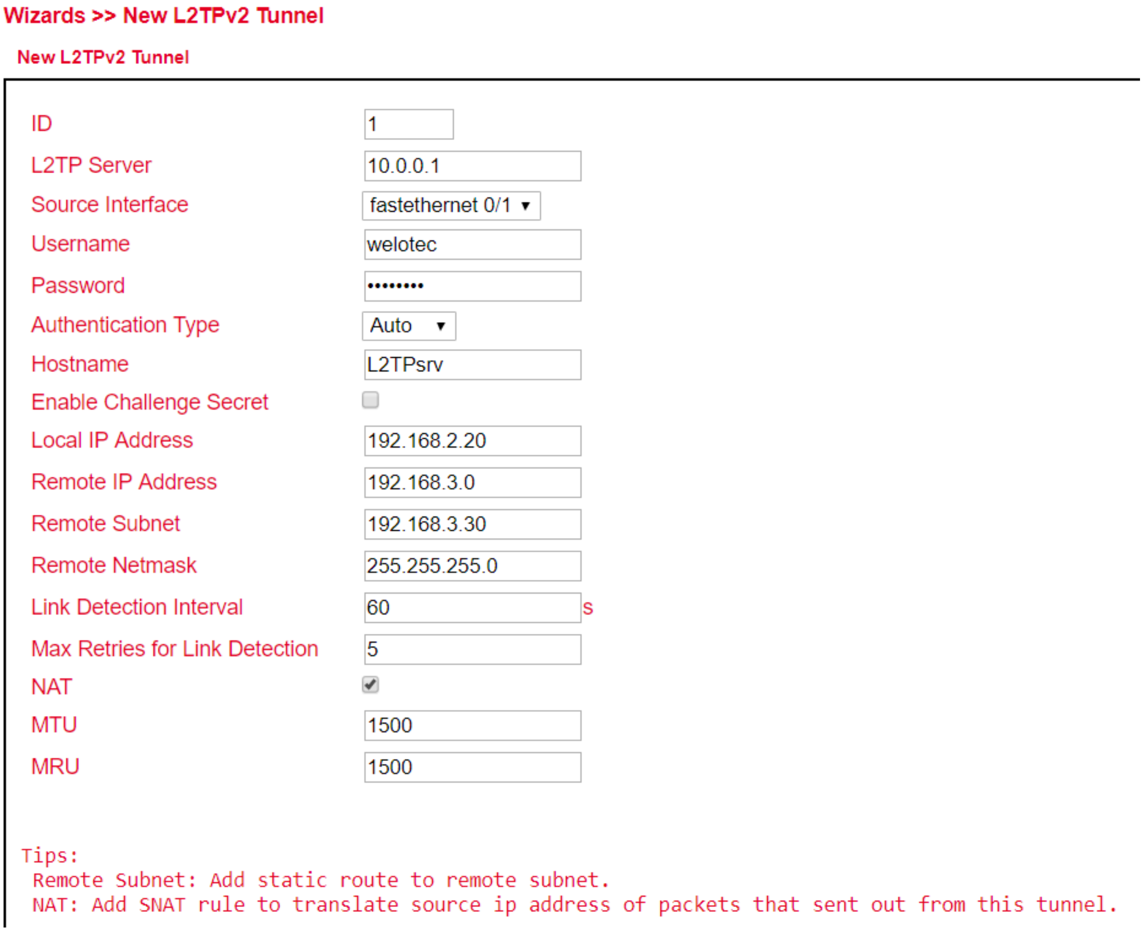
Select ipsec.secrets to use

No file selected.

IPsec Status

```
Connections:
IPsec1_10.0.0.2:  10.0.0.1...10.0.0.2  IKEv1
IPsec1_10.0.0.2:   local:  [10.0.0.1] uses pre-shared key authentication
IPsec1_10.0.0.2:   remote: uses pre-shared key authentication
IPsec1_10.0.0.2:   child:  192.168.2.0/24 === 192.168.3.0/24 TUNNEL
Security Associations (1 up, 0 connecting):
IPsec1_10.0.0.2[14]: ESTABLISHED 2 seconds ago, 10.0.0.1[10.0.0.1]...10.0.0.2[10.0.0.2]
IPsec1_10.0.0.2[14]: IKEv1 SPIs: cd56904966b159db_i 987d09ebdd9789a1_r*, pre-shared key reauthentication in 23 hours
IPsec1_10.0.0.2[14]: IKE proposal: 3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024
IPsec1_10.0.0.2{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c0628d36_i c07d1d3c_o
IPsec1_10.0.0.2{1}:  3DES_CBC/HMAC_MD5_96, 542 bytes_i (5 pkts, 1s ago), 1117 bytes_o (5 pkts, 1s ago), rekeying in 46 minutes
IPsec1_10.0.0.2{1}:   192.168.2.0/24 === 192.168.3.0/24

xfrm policies:
src 192.168.3.0/24 dst 192.168.2.0/24
        dir fwd priority 2883
        tmpl src 10.0.0.2 dst 10.0.0.1
                proto esp reqid 1 mode tunnel
src 192.168.3.0/24 dst 192.168.2.0/24
        dir in priority 2883
        tmpl src 10.0.0.2 dst 10.0.0.1
                proto esp reqid 1 mode tunnel
```

3.11.6. New L2TPv2 Tunnel



Wizards >> New L2TPv2 Tunnel

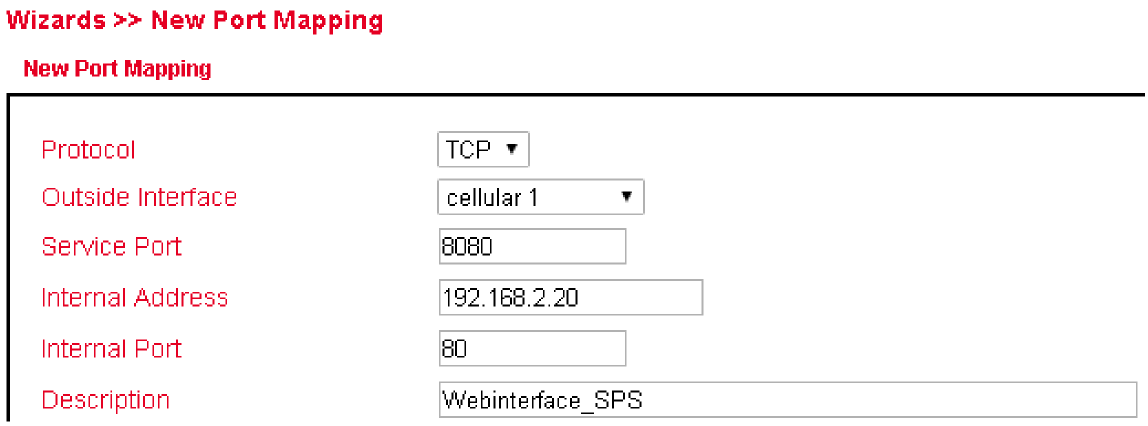
New L2TPv2 Tunnel

ID	1
L2TP Server	10.0.0.1
Source Interface	fastethernet 0/1 ▾
Username	welotec
Password	••••••••
Authentication Type	Auto ▾
Hostname	L2TPsrv
Enable Challenge Secret	□
Local IP Address	192.168.2.20
Remote IP Address	192.168.3.0
Remote Subnet	192.168.3.30
Remote Netmask	255.255.255.0
Link Detection Interval	60 s
Max Retries for Link Detection	5
NAT	☑
MTU	1500
MRU	1500

```
Tips:
 Remote Subnet: Add static route to remote subnet.
 NAT: Add SNAT rule to translate source ip address of packets that sent out from this tunnel.
```

3.11.7. New Port Mapping

A new port mapping can be easily set up under **Wizards > New Port Mapping**.



Wizards >> New Port Mapping

New Port Mapping

Protocol	TCP
Outside Interface	cellular 1
Service Port	8080
Internal Address	192.168.2.20
Internal Port	80
Description	Webinterface_SPS

Parameter	Description
Protocol	TCP or UDP
Outside Interface	The interface from which access should be made
Service Port	The port open to the outside.
Internal Address	The internal IP address you want to reach
Internal Port	The internal port you want to reach
Description	Brief description

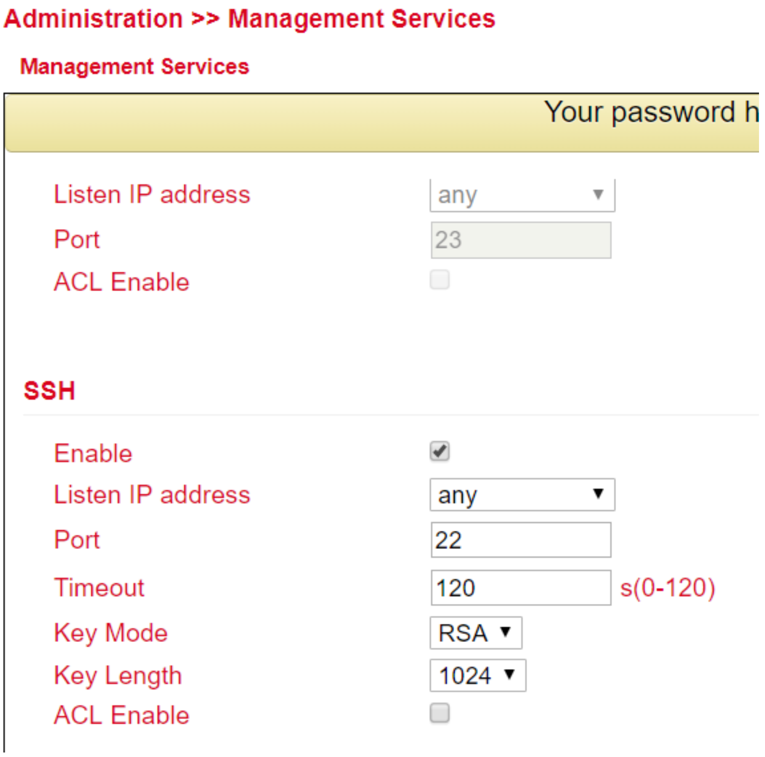
⚠ **Note**

If Cellular 1 is selected as outside Interface, port mapping only works if the mobile interface receives a public IP address!

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. Putty, for example, has proven itself as a tool for this.

One way to connect via the CLI is via SSH. This function must first be activated in the router. This is done via Administration > Management Services. Here the check mark must be set at enable under SSH. The second possibility to connect to the router is via the serial console in connection with a serial console cable. For this, the console cable must be connected to a computer at the router port labeled Console.



Administration >> Management Services

Management Services

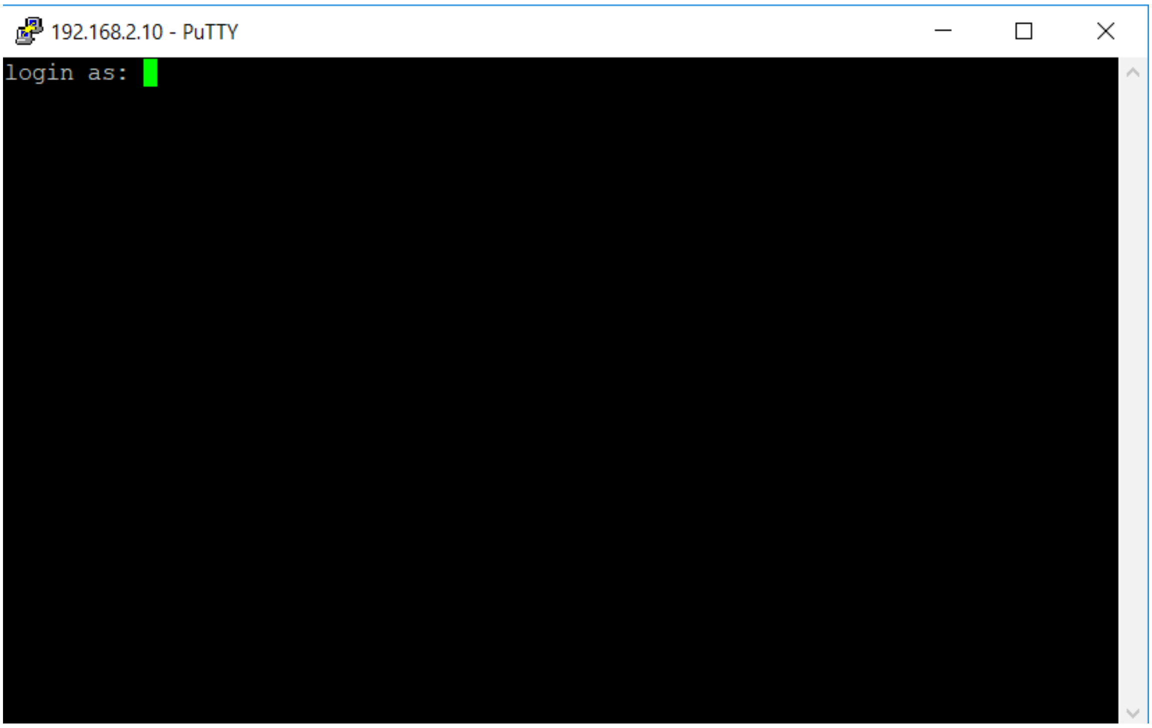
Your password h

Listen IP address	any ▼
Port	23
ACL Enable	□

SSH

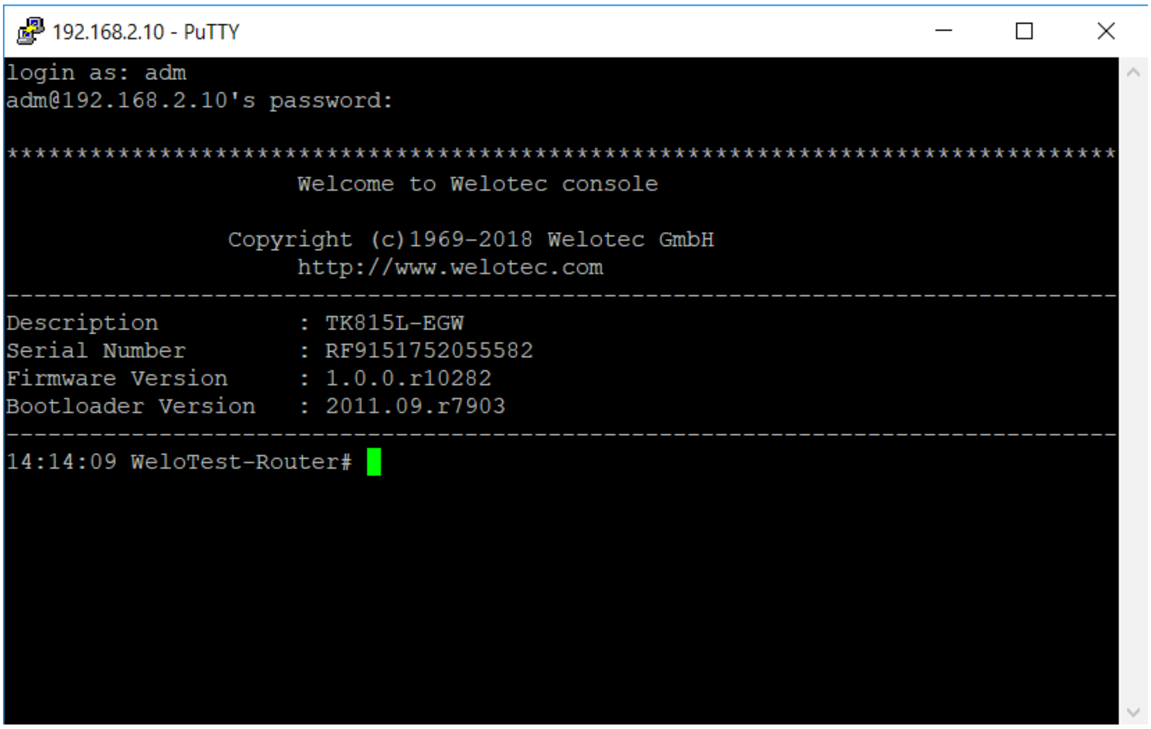
Enable	☑
Listen IP address	any ▼
Port	22
Timeout	120 s(0-120)
Key Mode	RSA ▼
Key Length	1024 ▼
ACL Enable	□

Then start e.g. putty and enter the IP address of your router and select SSH as port or connection type. For the connection via the serial console, select the COM port with the following settings from Baudrate 115200, Data Bits 8, Parity None, Stop Bit 1. Then click on open to establish the connection to the router. If the connection is established successfully, you will receive the CLI window with the login for the router.



```
login as:
```

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

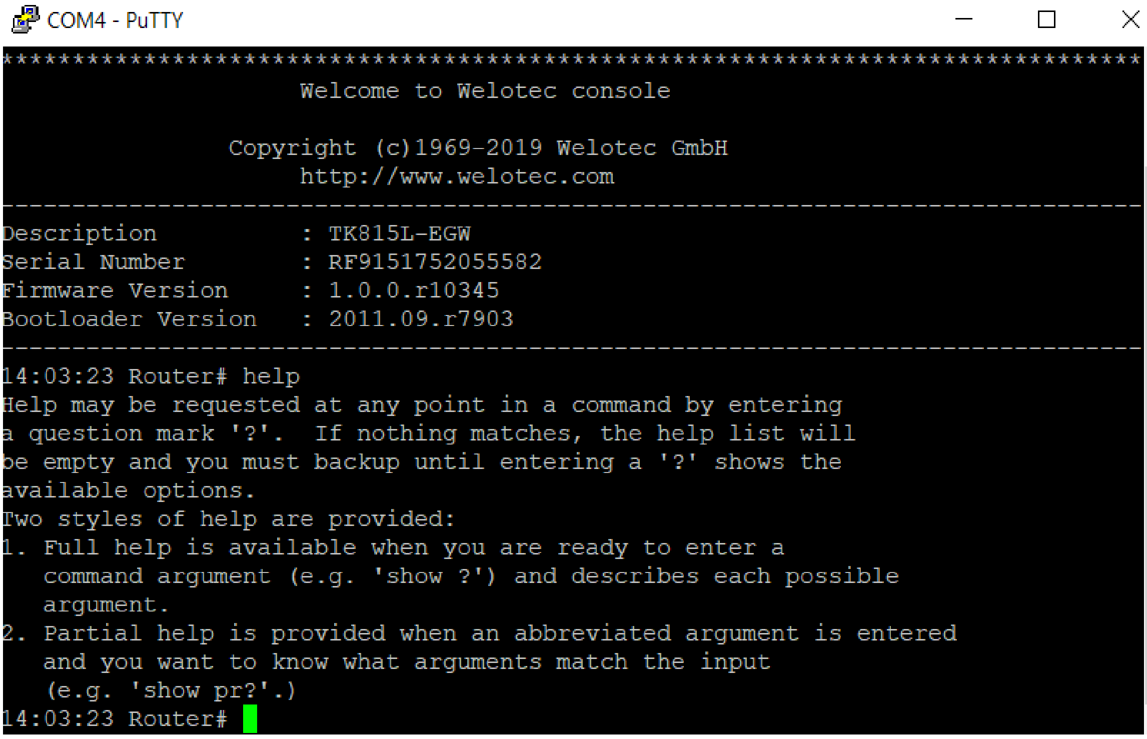


```
login as: adm
adm@192.168.2.10's password:

********************************************************************************
                     Welcome to Welotec console

                Copyright (c)1969-2018 Welotec GmbH
                     http://www.welotec.com
--------------------------------------------------------------------------------
Description           : TK815L-EGW
Serial Number         : RF9151752055582
Firmware Version      : 1.0.0.r10282
Bootloader Version    : 2011.09.r7903
--------------------------------------------------------------------------------
14:14:09 WeloTest-Router#
```

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

3.12.1. Help Command

The help can be retrieved after entering help or „?" in the console, „?" can be entered at any time during command input to get the current command or help from the command parameters, and the command or parameters can be completed automatically if only the command or command parameter exists.



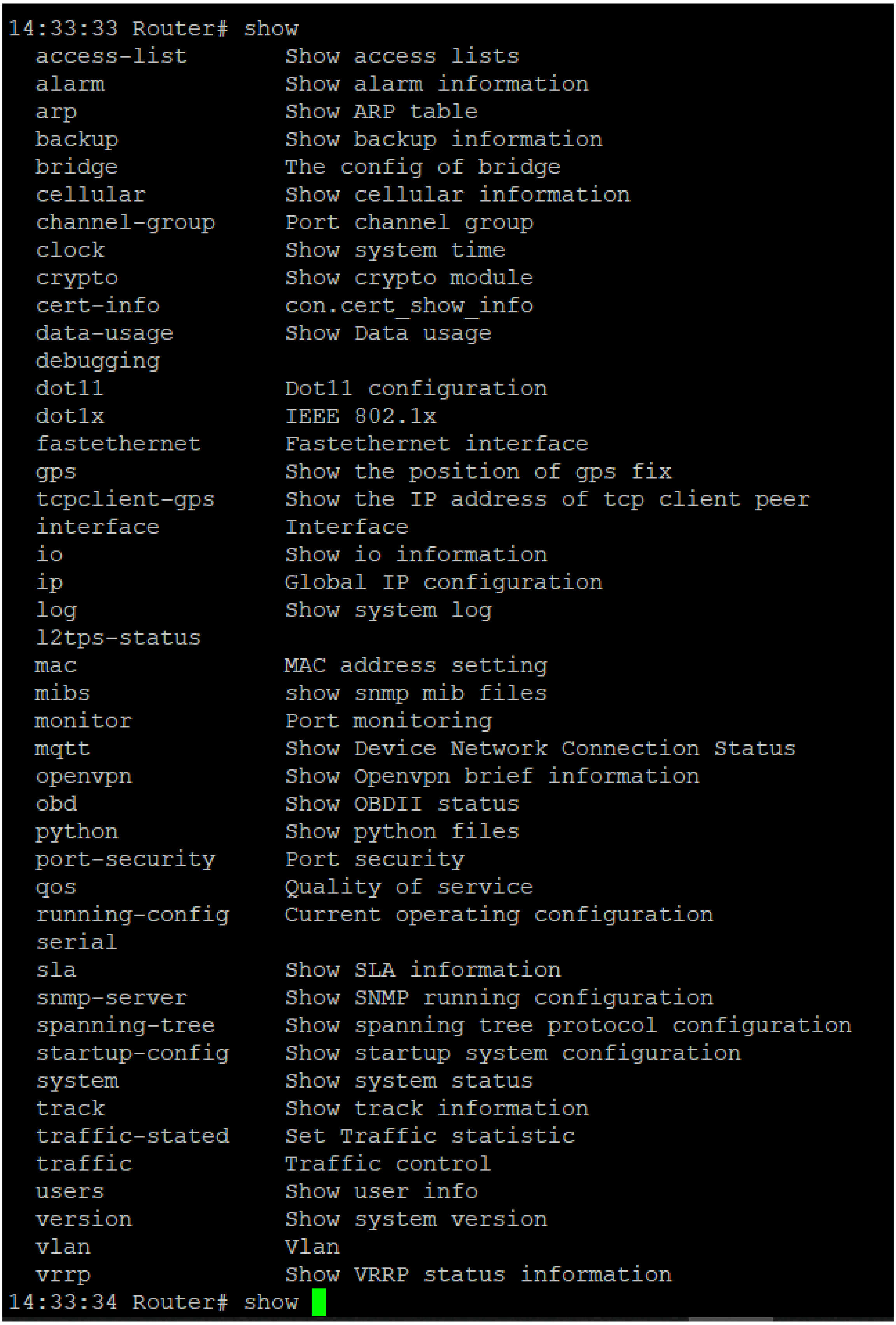
COM4 - PuTTY

```
*******************************************************************************
                     Welcome to Welotec console

                Copyright (c)1969-2019 Welotec GmbH
                     http://www.welotec.com
-------------------------------------------------------------------------------
Description          : TK815L-EGW
Serial Number        : RF9151752055582
Firmware Version     : 1.0.0.r10345
Bootloader Version   : 2011.09.r7903
-------------------------------------------------------------------------------
14:03:23 Router# help
Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)
14:03:23 Router#
```

Entering help at the input prompt outputs a short description of how to use the Help command. If you append the „?" to a command, you are shown the possibilities that can be used in connection with the command. If there is no output, there is no or no further command for this input.

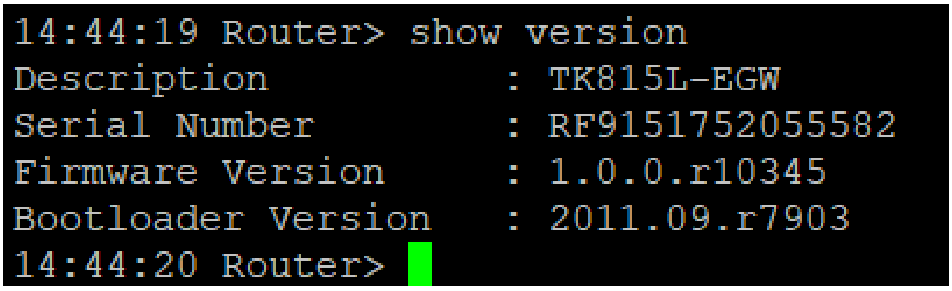
3.12.2. Show Command

With the show command you can display parameters of the router or the configuration of the router. The help command, or the „?“ command, displays the commands that can be used in connection 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
```

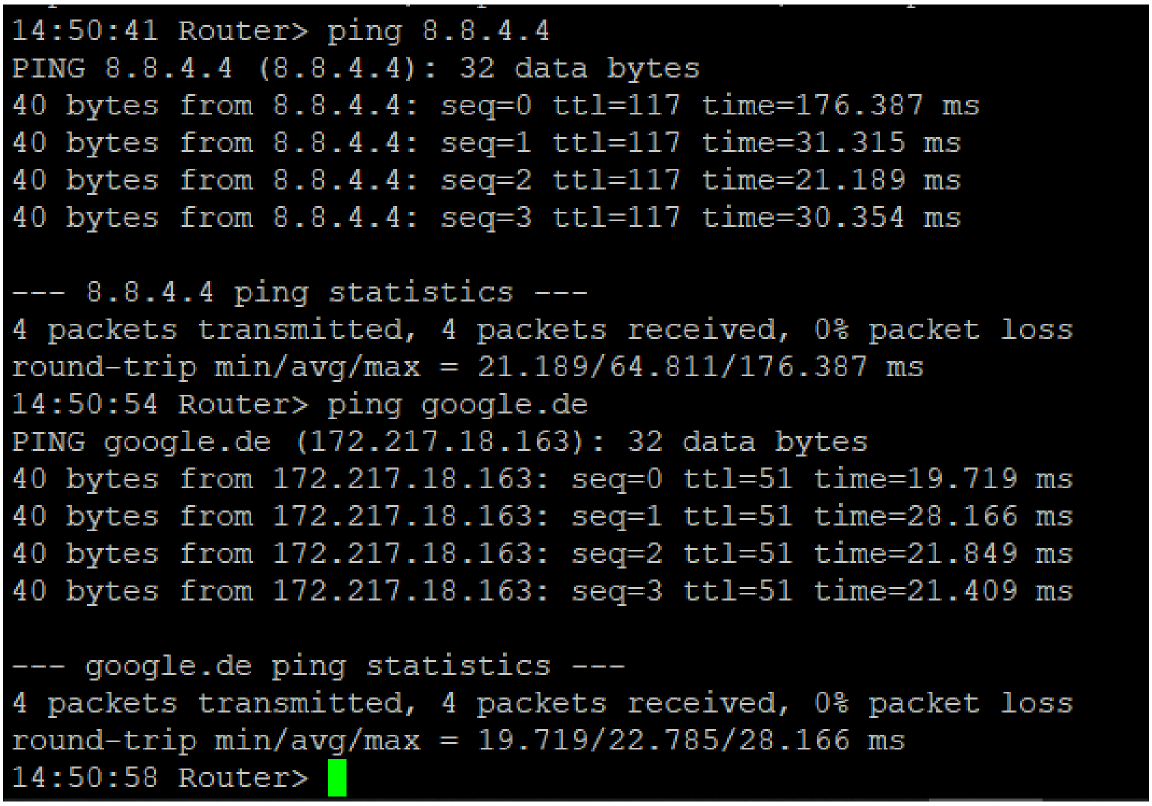
show version, for example, shows you data about the router, such as the description, serial number, firmware and bootloader version.



```
14:44:19 Router> show version
Description           : TK815L-EGW
Serial Number         : RF9151752055582
Firmware Version      : 1.0.0.r10345
Bootloader Version    : 2011.09.r7903
14:44:20 Router>
```

3.12.3. Ping Command

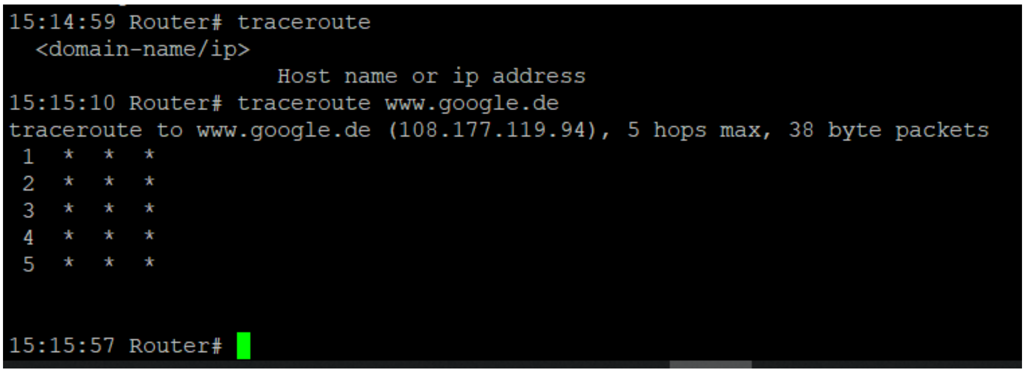
The ping command can be used to check whether the router is connected to the Internet. The input form is, as usual with Windows and Linux, ping hostname or IP address.



```
14:50:41 Router> ping 8.8.4.4
PING 8.8.4.4 (8.8.4.4): 32 data bytes
40 bytes from 8.8.4.4: seq=0 ttl=117 time=176.387 ms
40 bytes from 8.8.4.4: seq=1 ttl=117 time=31.315 ms
40 bytes from 8.8.4.4: seq=2 ttl=117 time=21.189 ms
40 bytes from 8.8.4.4: seq=3 ttl=117 time=30.354 ms

--- 8.8.4.4 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 21.189/64.811/176.387 ms
14:50:54 Router> ping google.de
PING google.de (172.217.18.163): 32 data bytes
40 bytes from 172.217.18.163: seq=0 ttl=51 time=19.719 ms
40 bytes from 172.217.18.163: seq=1 ttl=51 time=28.166 ms
40 bytes from 172.217.18.163: seq=2 ttl=51 time=21.849 ms
40 bytes from 172.217.18.163: seq=3 ttl=51 time=21.409 ms

--- google.de ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 19.719/22.785/28.166 ms
14:50:58 Router>
```

3.12.4. Traceroute Command

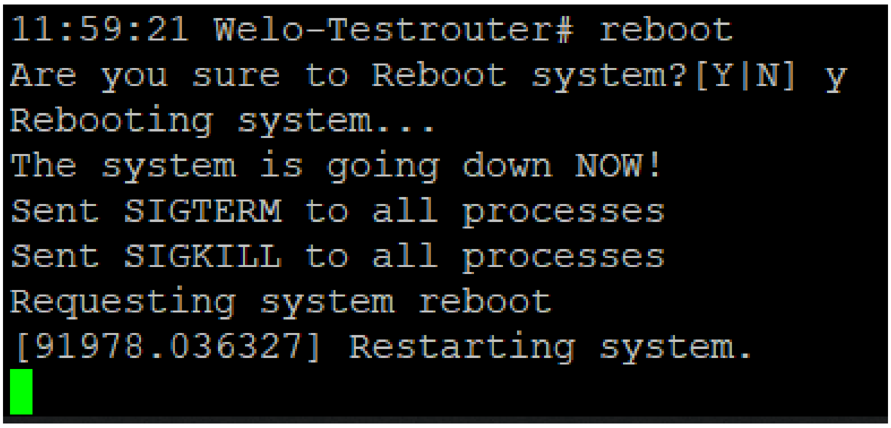
Use Traceroute to test the active routing of the specified destination. Use traceroute hostname or IP address to start the query.



```
15:14:59 Router# traceroute
  <domain-name/ip>
                  Host name or ip address
15:15:10 Router# traceroute www.google.de
traceroute to www.google.de (108.177.119.94), 5 hops max, 38 byte packets
 1  *  *  *
 2  *  *  *
 3  *  *  *
 4  *  *  *
 5  *  *  *


15:15:57 Router#
```

3.12.5. Reboot Command

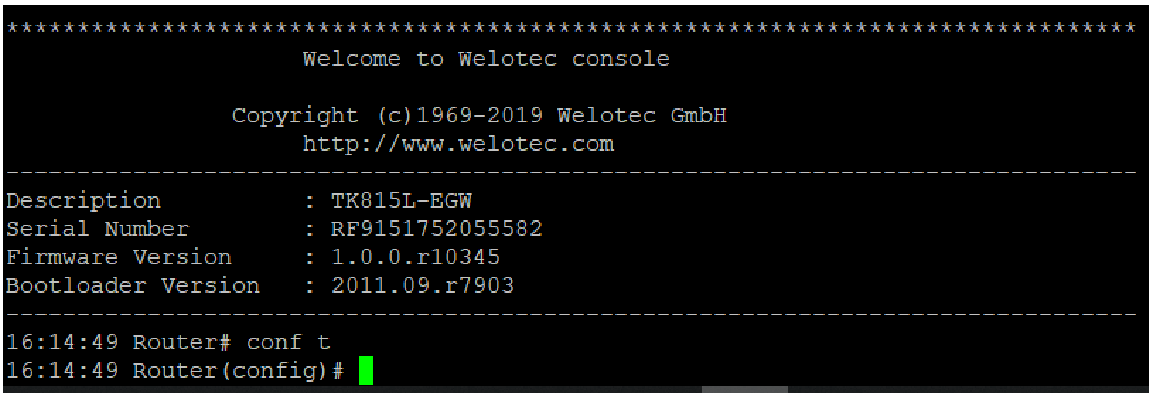
To restart the router, you can use the reboot command. Enter this command in the CLI and the router will be restarted.



```
11:59:21 Welo-Testrouter# reboot
Are you sure to Reboot system?[Y|N] y
Rebooting system...
The system is going down NOW!
Sent SIGTERM to all processes
Sent SIGKILL to all processes
Requesting system reboot
[91978.036327] Restarting system.
```

3.12.6. Configuration Command

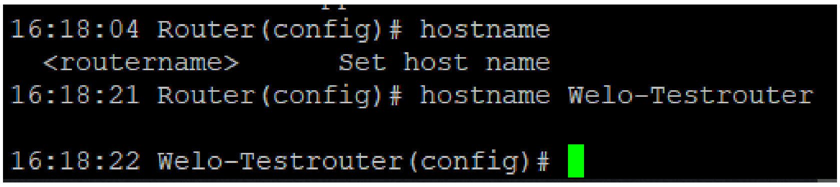
In the superuser view, the router can use the configure command to switch the configuration view to management. A configure command can support no and default, where no is the setting to abort a parameter and default is the setting to restore the default setting of a parameter. The configure terminal (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.



```
********************************************************************************
                     Welcome to Welotec console

                Copyright (c)1969-2019 Welotec GmbH
                     http://www.welotec.com
--------------------------------------------------------------------------------
Description          : TK815L-EGW
Serial Number        : RF9151752055582
Firmware Version     : 1.0.0.r10345
Bootloader Version   : 2011.09.r7903
--------------------------------------------------------------------------------
16:14:49 Router# conf t
16:14:49 Router(config)#
```

3.12.6.1. Hostname Command

The router name can now be changed in configuration mode. This can be done with the command hostname Name-des-Routers. This command converts the router name to the name you entered. If you want to reset the router's default name, use the default hostname command. This resets the router name to the default router name.



```
16:18:04 Router(config)# hostname
  <routername>      Set host name
16:18:21 Router(config)# hostname Welo-Testrouter

16:18:22 Welo-Testrouter(config)#
```

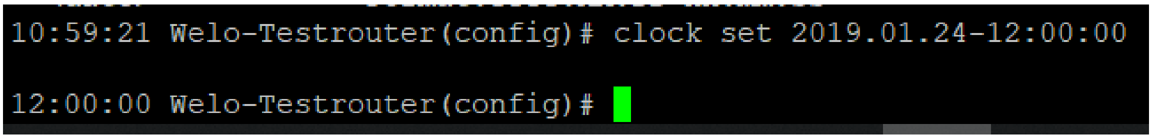
3.12.6.2. Clock set Command

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

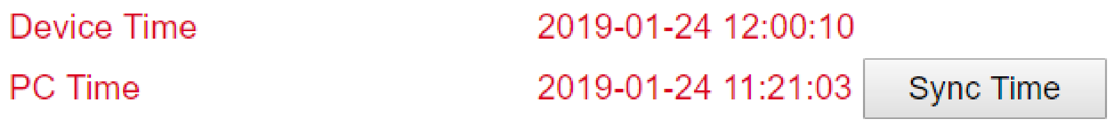
YYYY.MM.DD-HH:MM:SS

Completely the command would look like this

clock set 2019.01.24-12:00:00



```
10:59:21 Welo-Testrouter(config)# clock set 2019.01.24-12:00:00

12:00:00 Welo-Testrouter(config)#
```



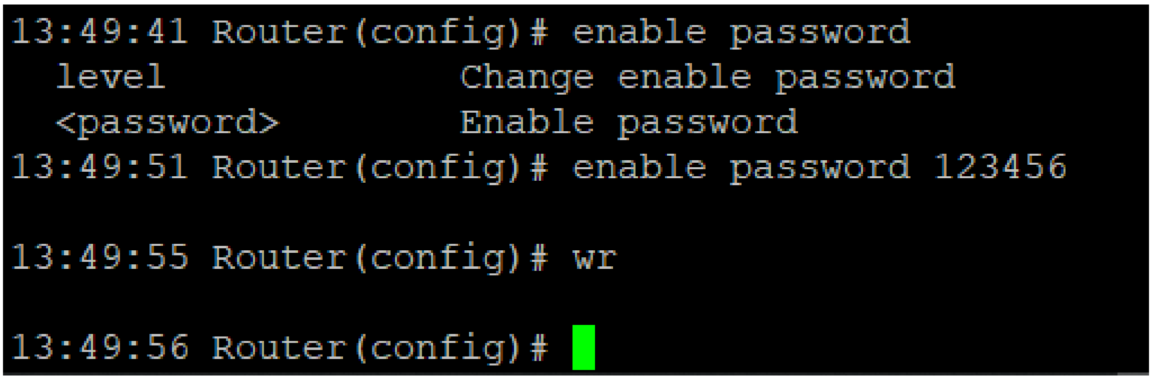
Device Time 2019-01-24 12:00:10

PC Time 2019-01-24 11:21:03

3.12.6.3. Enable password Command

It is possible to change the password of the super user (adm) at any time via the CLI. You can do this with the enable password command. The input form is as follows

Enable password password

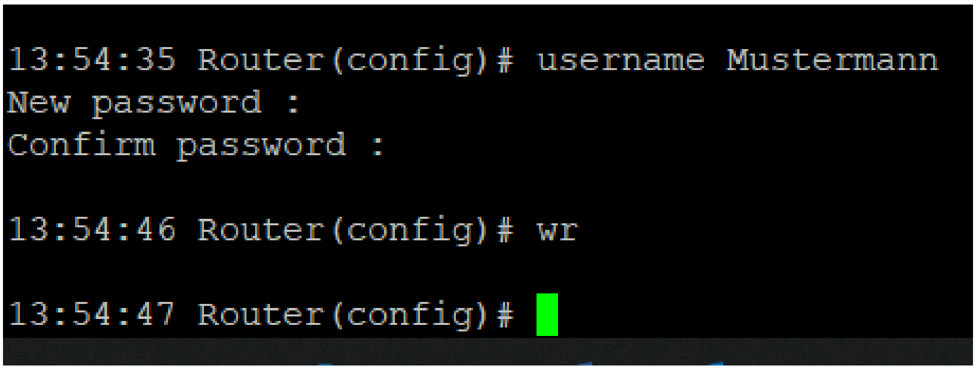


```
13:49:41 Router(config)# enable password
  level                 Change enable password
  <password>            Enable password
13:49:51 Router(config)# enable password 123456

13:49:55 Router(config)# wr

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

3.12.6.4. Username Command

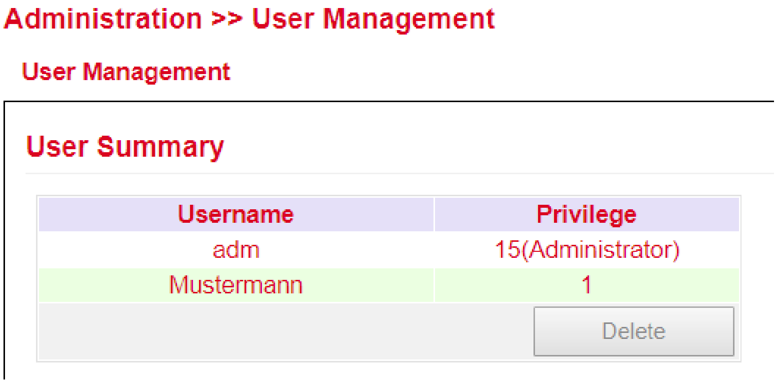
You can use the Username command to create users to access the router. The syntax for the input is as follows

Username NamedesUsers



```
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, which you can assign here. The user that is created is always a standard user.



Administration >> User Management

User Management

User Summary

Username	Privilege
adm	15(Administrator)
Mustermann	1

4. TECHNICAL DATA

4.1. Device characteristics

Characteristic	Value
Dimensions (W x H x D)	45 x 132.6 x 112.8 mm
Operating voltage	230 V AC at 12 V – 48 V DC
Power consumption standby	3.8 W
Power consumption active	5.3 W
Approval	CE-compliant

4.2. Enviromental characteristics

Characteristic	Value
Operating temperature range	-25 to +70 °C
Storage temperature range	-40 to +85 °C
Humidity	5 - 95 %, non-condensing
Shock	IEC 60068-2-27
Free Fall	IEC 60068-2-32
Vibration	IEC 60068-2-6

4.3. Radio frequencies

4.3.1. Radio frequencies 4G LTE Europe

Frequency	Frequency range and transmission power	Router
Band 1	• Frequency range Down: 2110 MHz – 2170 MHz • Frequency range Up: 1920 MHz – 1980 MHz • Max. transmission 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. transmission 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. transmission 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. transmission 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. transmission power: 199 mW	TK812L, TK815L-EX0, TK815L-EXW, TK815L-EGW

4.3.2. Radio frequencies 3G UMTS Europa

Frequency	Frequency range and transmission power	Router
Band 1	• Frequency range Down: 2110 MHz – 2170 MHz • Frequency range Up: 1920 MHz – 1980 MHz • Max. transmission power: 251 mW	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. transmission 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. transmission power: 251 mW	TK802U, TK812L, TK815L-EX0, TK815L-EXW, TK815L-EGW

4.3.3. Radio frequencies 2G GSM Europe

Frequency	Frequency range and transmission power	Router
GSM 900	• Frequency range Down: 925 MHz – 960 MHz • Frequency range Up: 880 MHz – 915 MHz • Max. transmission power: 1995 mW	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. transmission power: 1000 mW	TK802U, TK812L, TK815L-EX0, TK815L-EXW, TK815L-EGW

4.3.4. Radio frequencies 4G LTE Asia

Frequency	Frequency range and transmission power	Router
Band 1	• Frequency range Down: 1920 MHz – 1980 MHz • Frequency range Up: 2110 MHz – 2170 MHz • Max. transmission power: 200 mW	TK822L, TK825L-EXW, TK825L-EX0
Band 2	• Frequency range Down: 1930 MHz – 1990 MHz • Frequency range Up: 1850 MHz – 1910 MHz • Max. transmission 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. transmission 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. transmission 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. transmission power: 200 mW	TK822L, TK825L-EXW, TK825L-EX0
Band 38 China	• Frequency range Down: 2570 MHz – 2620 MHz • Frequency range Up: not known • Max. transmission power: 200 mW	TK822L, TK825L-EXW, TK825L-EX0
Band 39 China	• Frequency range Down: 1880 MHz – 1920 MHz • Frequency range Up: not known • Max. transmission power: 200 mW	TK822L, TK825L-EXW, TK825L-EX0
Band 40 China	• Frequency range Down: 2300 MHz – 2400 MHz • Frequency range Up: not known • Max. transmission power: 200 mW	TK822L, TK825L-EXW, TK825L-EX0
Band 41 China	• Frequency range Down: 2496 MHz – 2690 MHz • Frequency range Up: not known • Max. transmission power: 200 mW	TK822L, TK825L-EXW, TK825L-EX0

4.3.5. Radio frequencies 3G UMTS Asia

Frequency	Frequency range and transmission power	Router
Band 1	• Frequency range Down: 2110 MHz – 2170 MHz • Frequency range Up: 1920 MHz – 1980 MHz • Max. transmission power: 251 mW	TK822L, TK825L-EXW, TK825L-EX0
Band 5	• Frequency range Down: 869 MHz – 894 MHz • Frequency range Up: 824 MHz – 849 MHz • Max. transmission 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. transmission power: 251 mW	TK822L, TK825L-EXW, TK825L-EX0

4.3.6. Radio frequencies 2G GSM Asia

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

4.3.7. Radio frequencies 4G LTE USA

Frequency	Frequency range and transmission power	Router
Band 2	• Frequency range Down: 1930 MHz – 1990 MHz • Frequency range Up: 1850 MHz – 1910 MHz • Max. transmission power: 200 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. transmission power: 200 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. transmission power: 200 mW	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. transmission power: 200 mW	TK832L, TK835L-EXW, TK835L-EX0, TK842L, TK845L-EXW, TK845L-EX0

4.3.8. Radio frequencies 3G UMTS USA

Frequency	Frequency range and transmission power	Router
Band 2	• Frequency range Down: 1930 MHz – 1990 MHz • Frequency range Up: 1850 MHz – 1910 MHz • Max. transmission 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. transmission 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. transmission power: 251 mW	TK832L, TK835L-EXW, TK835L-EX0, TK842L, TK845L-EXW, TK845L-EX0

4.3.9. Radio frequencies 2G GSM USA

Frequency	Frequency range and transmission power	Router
GSM 850	• Frequency range Down: 869 MHz – 894 MHz • Frequency range Up: 824 MHz – 849 MHz • Max. transmission power: 1995 mW	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. transmission power: 1000 mW	TK832L, TK835L-EXW, TK835L-EX0, TK842L, TK845L-EXW, TK845L-EX0

4.3.10. Radio frequencies 4G LTE for further countries world-wide

Frequency	Frequency range and transmission power	Router
Band 1	• Frequency range Down: 2110 MHz – 2170 MHz • Frequency range Up: 1920 MHz – 1980 MHz • Max. transmission power: 199 mW	TK882L, TK885L-EX0, TK885L-EXW
Band 3	• Frequency range Down: 1805 MHz – 1880 MHz • Frequency range Up: 1710 MHz – 1785 MHz • Max. transmission 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. transmission 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. transmission 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. transmission 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. transmission power: 199 mW	TK882L, TK885L-EX0, TK885L-EXW

4.3.11. Radio frequencies 3G UMTS for further countries world-wide

Frequency	Frequency range and transmission power	Router
Band 2	• Frequency range Down: 1930 MHz – 1990 MHz • Frequency range Up: 1850 MHz – 1910 MHz • Max. transmission 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. transmission 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. transmission power: 251 mW	TK882L, TK885L-EX0, TK885L-EXW

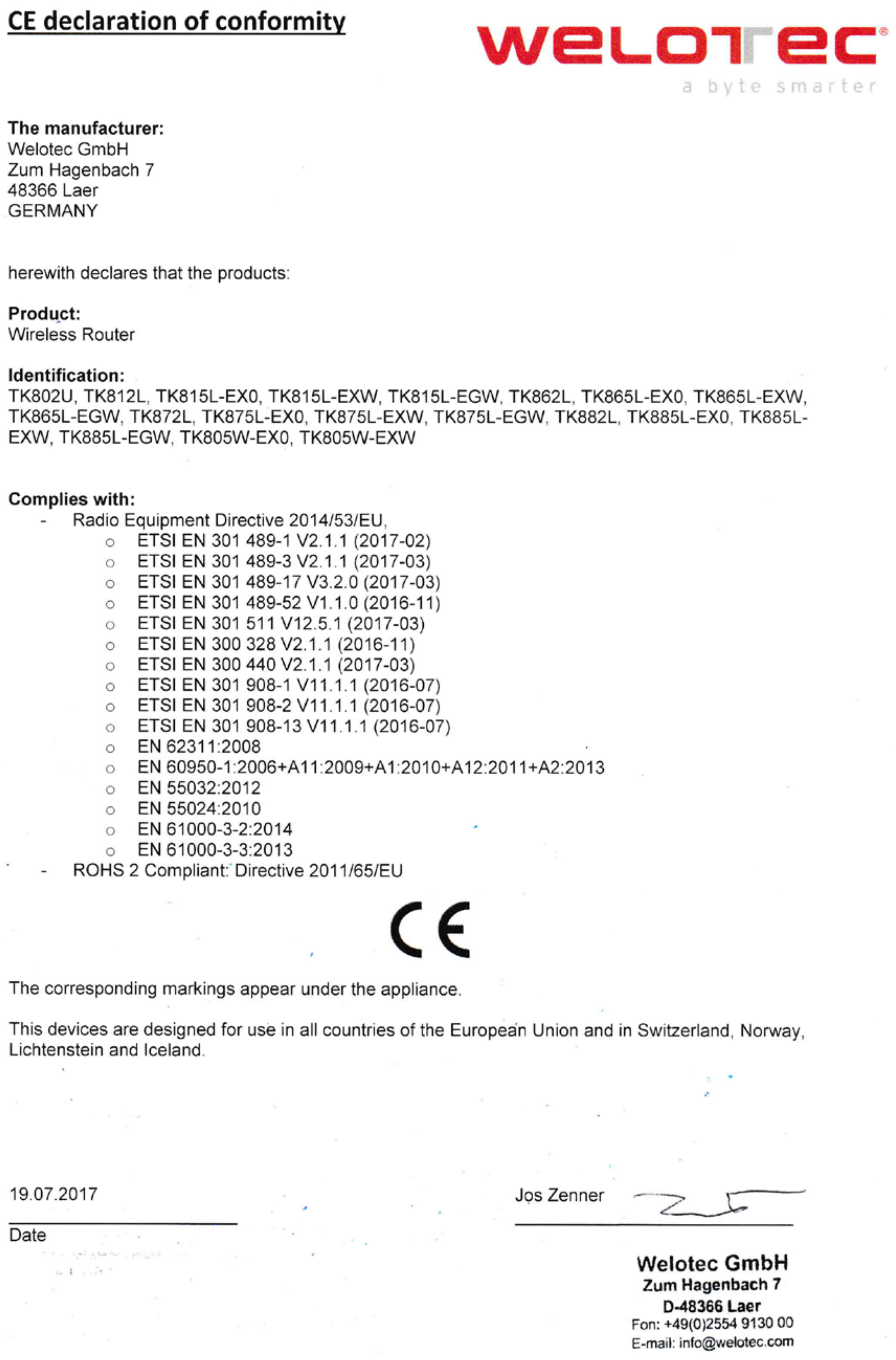
4.3.12. Radio frequencies 2G GSM for further countries world-wide

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

4.3.13. Radio frequencies WLAN

Frequency	Frequency range and transmission power	Router
2.4 GHz	• Frequency range: 2400 MHz – 2483.5 MHz • Max. transmission power: 40 mW	TK805-EXW, TK815L-EXW, TK815L-EGW , TK825L-EXW, TK835L-EXW, TK845L-EXW

5. CE DECLARATION



CE declaration of conformity

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, TK882L, 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.

19.07.2017
Date

Jos Zenner

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