TK804

Version:
v1.2.15

Date:
22.12.2025

welotec
a Westermo company

Contents

1 Introduction

1.1 Copyright Notice

1.2 Trademarks

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

1.3 Legal Notice

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

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

1.4 Technical Support Contact Information

Welotec GmbH

Zum Hagenbach 7

48366 Laer

Tel.: +49 2554 9130 00

Fax.: +49 2554 9130 10

Email: info@welotec.com

1.5 Description

The Welotec TK804L-450, part of the rugged TK804 industrial router series, delivers highly reliable cellular connectivity across 2G, 3G, and 4G LTE networks. Engineered for demanding environments, it offers exceptional performance and versatile deployment options—including DIN-rail installation—making it ideal for mission-critical applications in industries like automation, smart grids, water management, and remote monitoring.

1.6 *Important Safety Notes*:

This product is not suitable for the following areas of application

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

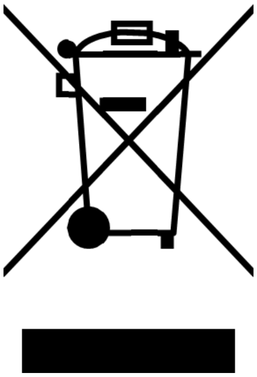
1.7 Warning

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

1.8 WEEE Notice

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

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



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

2 Regulatory Compliances

2.1 Complies with the following EU directives

No	Short Name
2014/35/EU	Low Voltage Directive (LVD)
2014/53/EU	Radio Equipment Directive (RED)
2014/30/EU	Electromagnetic Compatibility (EMC)
2011/65/EU	Restriction of the use of certain hazardous substances in electrical and electronic equipment Directive (RoHS2)
2015/863/EU	Amendment to Annex II in Directive 2011/65/EU regards the list of restricted substances (RoHS3)

2.2 References of standards applied

Standard	Reference	Issue
EN 18031-1	Common security requirements for radio equipment - Part 1: Internet connected radio equipment	2024
EN 55032	Electromagnetic compatibility of multimedia equipment - Emission Requirements	2015+A11:2020+A1:2020
EN 55035	Electromagnetic compatibility of multimedia equipment - Immunity requirements	2017+A11:2020
EN 301 489-1	ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements; Harmonised Standard for ElectroMagnetic Compatibility	V2.2.3
EN 301 489-52	ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 52: Specific conditions for Cellular Communication User Equipment (UE) radio and ancillary equipment; Harmonised Standard for ElectroMagnetic Compatibility	V1.2.1
EN 301 511	Global System for Mobile communications (GSM); Harmonised EN for mobile stations in the GSM 900 and GSM 1800 bands covering essential requirements under article 3.2 of the R&TTE directive (1999/5/EC)	V12.5.1
EN 301 908-1	IMT cellular networks; Harmonised Standard for access to radio spectrum; Part 1: Introduction and common requirements Release 15	V15.2.1
EN 301 908-13	IMT cellular networks; Harmonised Standard for access to radio spectrum; Part 13: Evolved Universal Terrestrial Radio Access (E-UTRA) User Equipment (UE)	V13.2.1
ETSI TS 151 010-1	Digital cellular telecommunications system (Phase 2+) (GSM); Mobile Station (MS) conformance specification; Part 1: Conformance specification	V12.8.0
ETSI TS 136 521-1	LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) conformance specification; Radio transmission and reception; Part 1: Conformance testing	V16.9.0
EN IEC 62311	Assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (0 Hz – 300 GHz)	2020
EN IEC 62368-1	Safety requirements: Audio/video, information and communication technology	2020+A11:2020

3 Safety Instructions

Please read these instructions carefully and retain them for future reference.

1. Disconnect this equipment from the power outlet before cleaning. Do not use liquid or sprayed detergent for cleaning. Use a moist cloth or sheet.
2. Keep this equipment away from humidity.
3. Ensure the power cord is positioned to prevent tripping hazards and do not place anything on top of it.
4. Pay attention to all cautions and warnings on the equipment.
5. If the equipment is not used for an extended period, disconnect it from the main power to avoid damage from transient over-voltage.
6. **Prolonged usage with less than 9V may damage the PSU or destroy the mainboard.**
7. Never pour any liquid into openings as this could cause fire or electrical shock.
8. Have the equipment checked by service personnel if:
   - The power cord or plug is damaged.
   - Liquid has penetrated the equipment.
   - The equipment has been exposed to moisture in a condensation environment.
   - The equipment does not function properly, or you cannot get it to work by following the user manual.
   - The equipment has been dropped and damaged.
9. Do not leave this equipment in an unconditioned environment, with storage temperatures below -40 degrees or above 85 degrees Celsius for extended periods, as this may damage the equipment.
10. Unplug the power cord when performing any service or adding optional kits.
11. Lithium Battery Caution:
    - Risk of explosion if the battery is replaced incorrectly. Replace only with the original or an equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.
    - Do not remove the cover, and ensure no user-serviceable components are inside. Take the unit to a service center for service and repair.

4 Quick Start Guide

Guide to installation and comissioning of the TK804 series. Please ensure that all package contents are present upon delivery. If you need a SIM card, contact your local network operator.

4.1 Package Contents

Each TK804L-450 is supplied in a box with standard accessories. Optional accessories can also be ordered. Check the contents of the box. If something is missing, contact Welotec.

4.1.1 Components Router

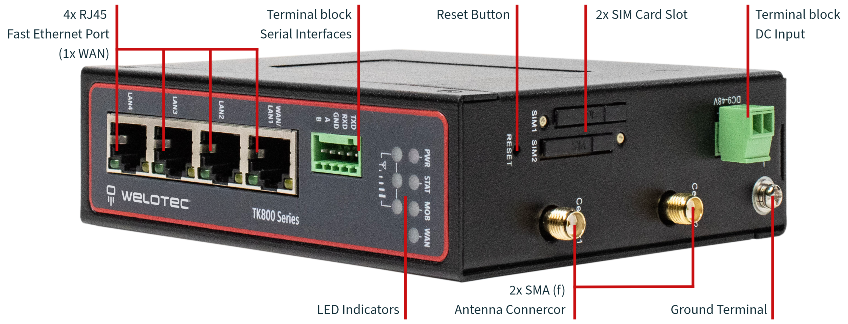
Product	Amount	Description
TK804L-450	1	TK804 series industrial router
Terminal block	1	Terminal block, 2-pin (m)
Terminals Serial and I/O	1	Terminal block, 5-pin (EX0 / EXW variants only)

4.1.2 Components Set

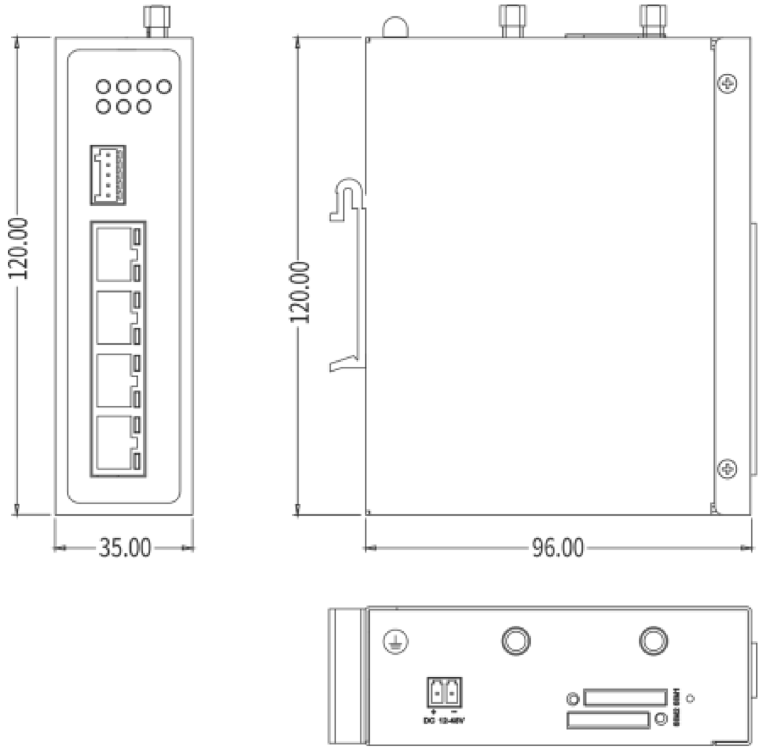
Product	Amount	Description
TK804L-450	1	TK804 series industrial router
Terminal block	1	Terminal block, 2-pin (m)
Network cable	1	1,5 m
Antenna	2 (4)	3G/4G Antenna Wi-fi Antenna (EXW variant only)
Power supply unit	1	230 V AC to 12 V DC
Terminals Serial and I/O	1	Terminal block, 9-pin (EX0 / EXW variants only)

4.2 Information and Control Panel

4.2.1 Control Panel



4.2.2 Dimension Drawings



4.3 Installation Guide

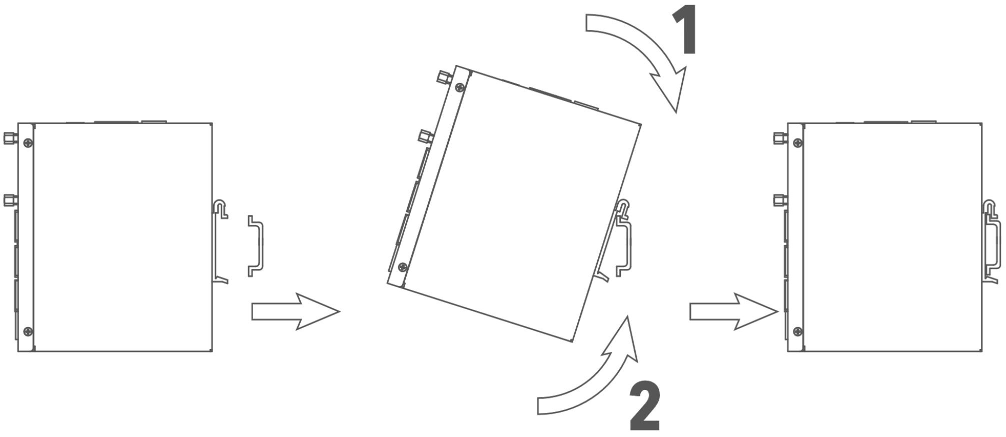
4.3.1 Preparations

Prepare the power supply (9 - 36 V DC). Make sure that the device can operate under the specified environmental conditions (working temperature range -25 - +70 °C, humidity: 5 – 95 % relative humidity). The device should not be exposed to direct sunlight and should be installed away from heat sources and environments with strong electromagnetic interference. The router can be mounted on a DIN rail (top-hat rail) or used at a workstation.

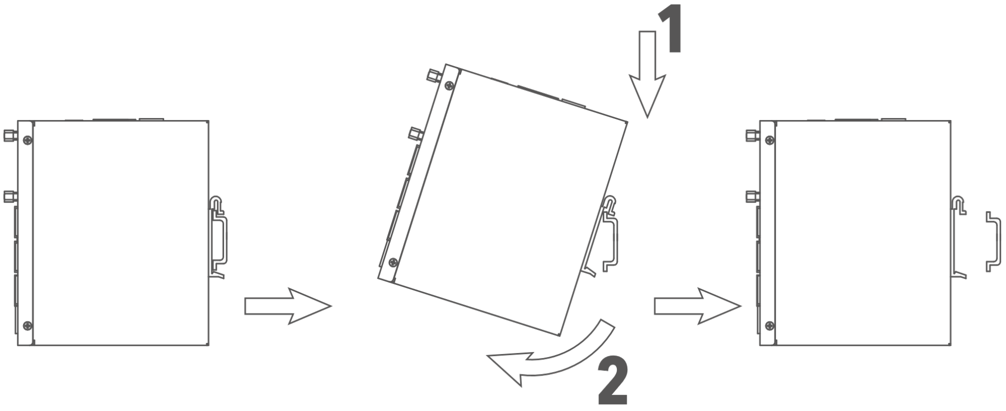
4.3.2 Mounting the Device

DIN rail:

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



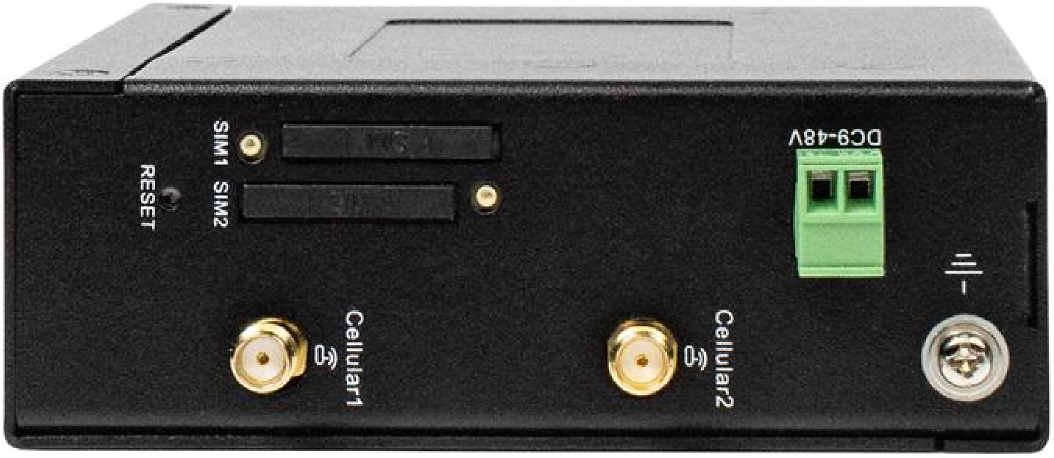
For demounting press the device from top to bottom and then pull the lower side of the device from the DIN rail (see figure).



4.4 Installing the SIM Card

The TK804L-450 supports dual SIM. To insert the cards, press the yellow “Eject” button with a small screwdriver on the top of the device, for example. The respective SIM card slot is pushed out. If the TK804L-450 is not operated in dual SIM mode, use the SIM card slot “SIM1”.

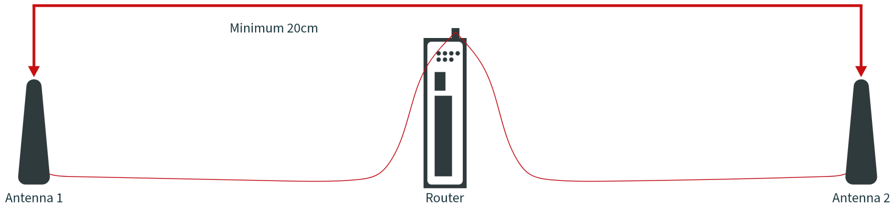
Then insert the SIM card. The SIM card slot is not hot-pluggable. The router must be restarted after inserting the SIM card.



4.5 Antennas Installation

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

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



4.6 Installation of the Power Supply

Remove the terminal block from the top of the router. Loosen the corresponding screws on the terminal block and route the wires to the corresponding terminals. The terminals are marked accordingly on the top of the router. Tighten the screws and then reinsert the connector block into the router. To ground the device, use the grounding screw on the device.

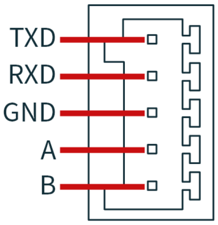
⊠ To prevent interference due to electromagnetic influence, the housing of the router must be grounded via the grounding screw.

4.7 Cable Connections

Connect the router to your PC via a network cable (RJ45).

4.8 Connection of the Serial Interfaces and I/O's

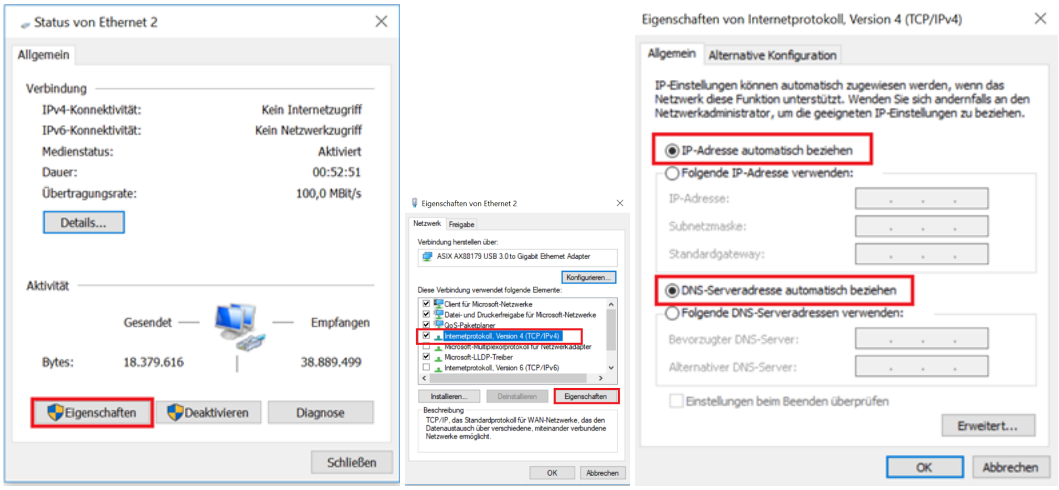
For the connection of the serial interfaces and the I/O's you will find a terminal block on the front of the device. The individual contacts for this are labeled on the front of the device. Connect the lines according to these labels. The "IN" contact here represents the digital input, while the output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



4.9 Startup of the Router

4.9.1 Automatic Configuration (DHCP)

Configure the PC so that it works as a DHCP client (obtain IP address automatically). Connect the PC with a network cable to one of the ethernet interfaces. The PC is then assigned an IP address, standard gateway and DNS server by the router. The following figure shows the configuration process via DHCP on a PC with the Windows 10 operating system. The settings can be accessed via the Network and Sharing Center in Windows 10.


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

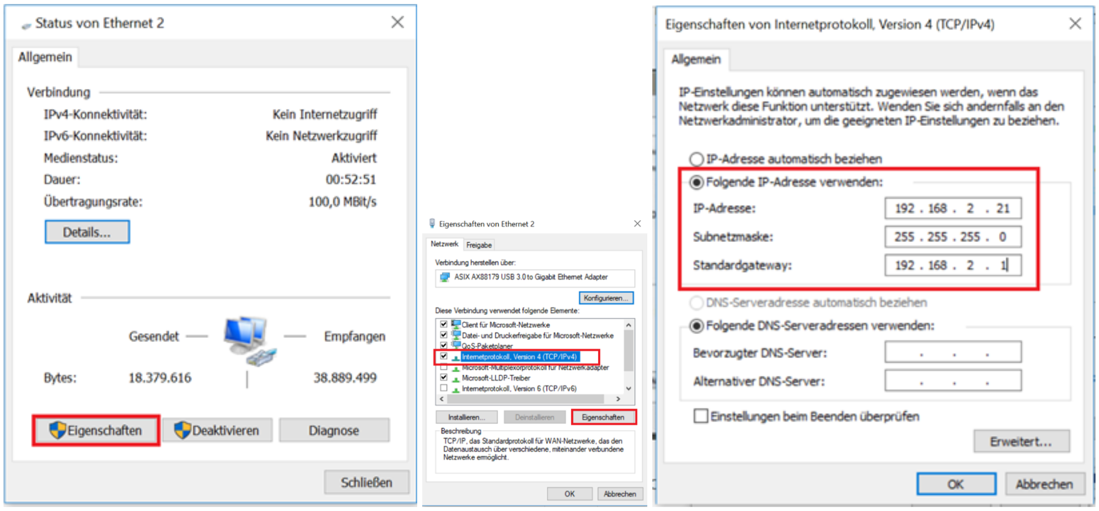
After configuring the IP address of the PC and connecting to the router, open a web browser.

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

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

4.9.2 Manual Configuration

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



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.

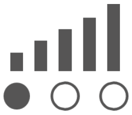
Then enter "**http://192.168.2.1**" in the address line of your browser (e.g. Google Chrome). After confirming with the "Enter" key, a pop-up appears as the login page of the router. Enter the username and password (note: username and password printed on the device label) and confirm with "Enter". Now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

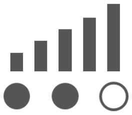
To check if you are connected to the Internet, select ***Network*** > ***Cellular*** > ***Status*** from the navigation panel. Here you can see the data of the cellular unit in the router. Alternatively, simply open a web page in your browser.

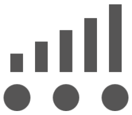
4.10 LED-Indicator Guide for TK804L-450

Power	Status	Mobile	Wide Area Network	Description
(Red)	(Green)	(Green)	(Green)	
Off	Off	Off	Off	Turned off
On	Off	Off	Off	System error
On	On	Off	Off	The module or SIM card is not recognized
On	On	Flashing	Flashing	Dial up
On	On	On	On	Dial up successful
On	Flashing	On	On	System upgrade
On	Flashing->On	On	On	Reset

4.10.1 Signal Strength







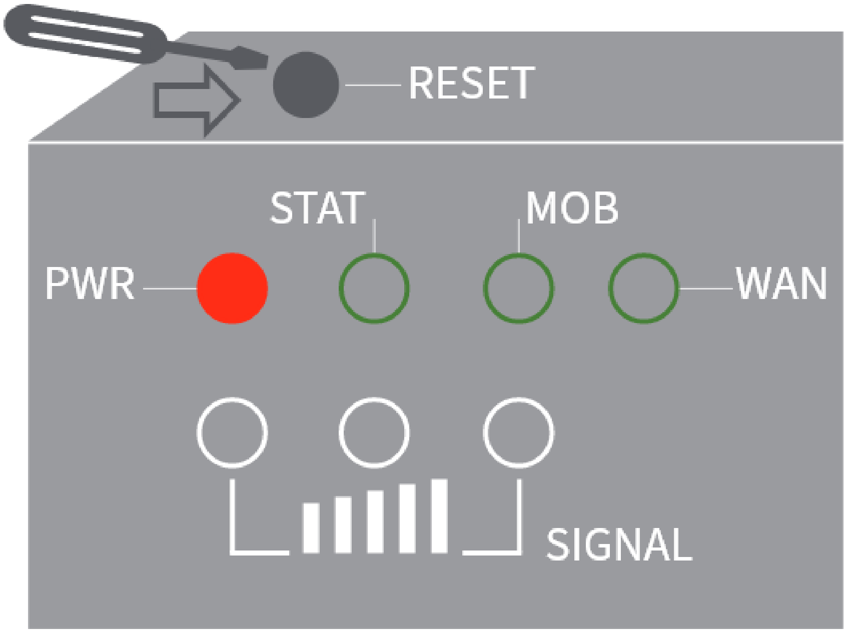
Signal Level	Description
1–9	Poor reception – The router cannot function properly. Please check the antenna connection and network coverage.
10–19	Normal reception – The router is working properly.
20–31	Perfect reception – Optimal signal strength.

4.11 Factory Reset

4.11.1 Hardware Method

1. Turn on the TK804L-450 Router and wait 30 Seconds, then press and hold the Reset button until the STAT LED is steady on.

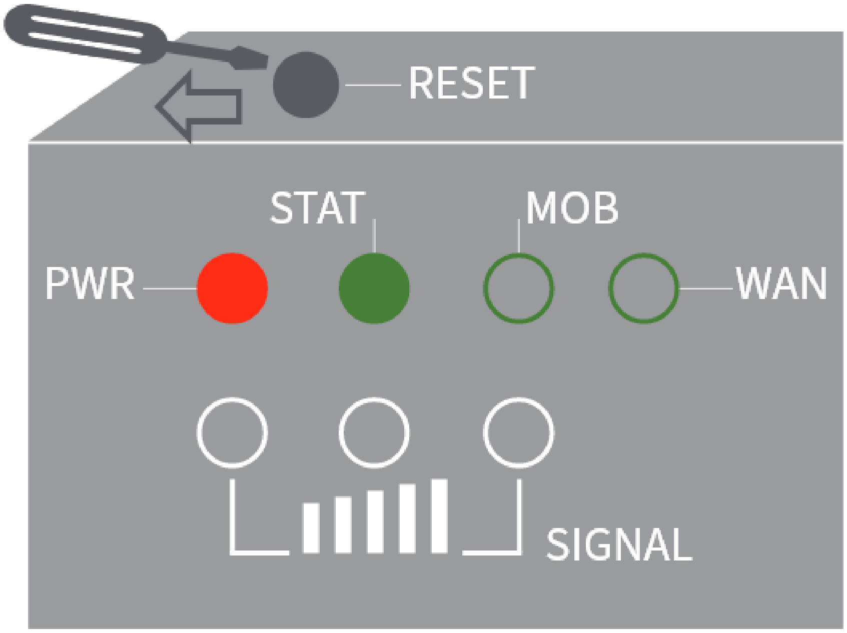
1.



Symbol explanation: ● LED on ○ LED off ⟳ LED flashing

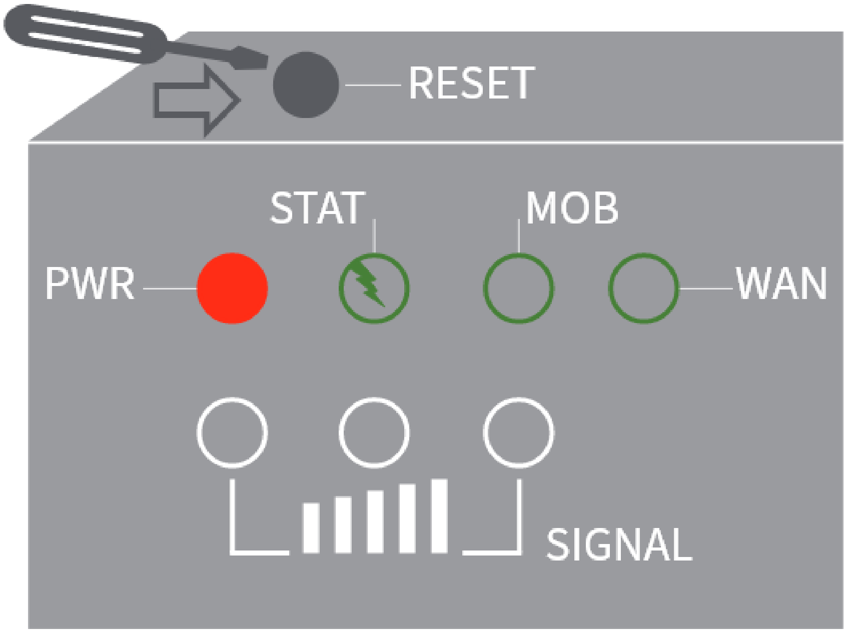
2. When the STAT LED is steady, wait for 2 seconds and Release the Reset button, the STAT LED will go off.

2.



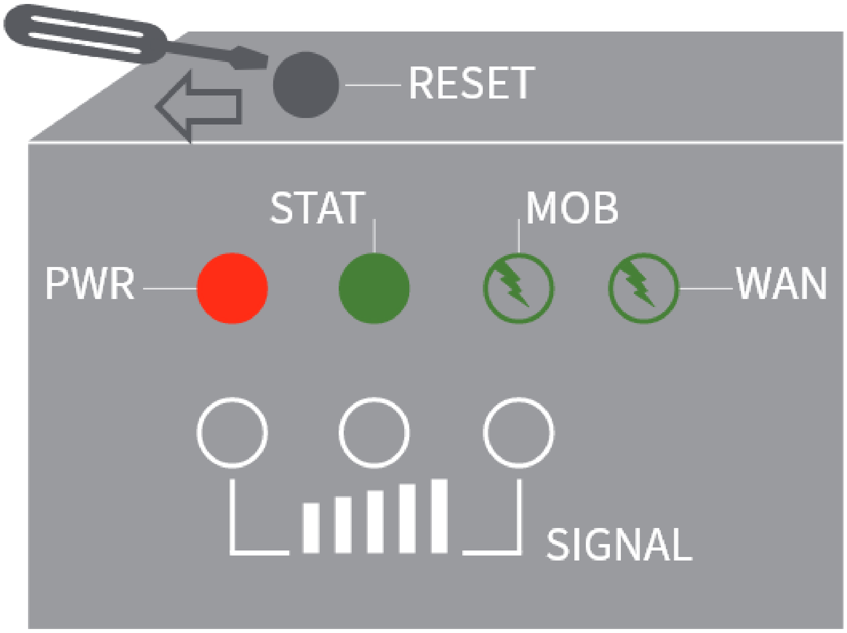
3. After the STAT LED goes off, press the Reset button again, the STAT LED will blink.

3.



4. Release the Reset button then the device will restore to default settings

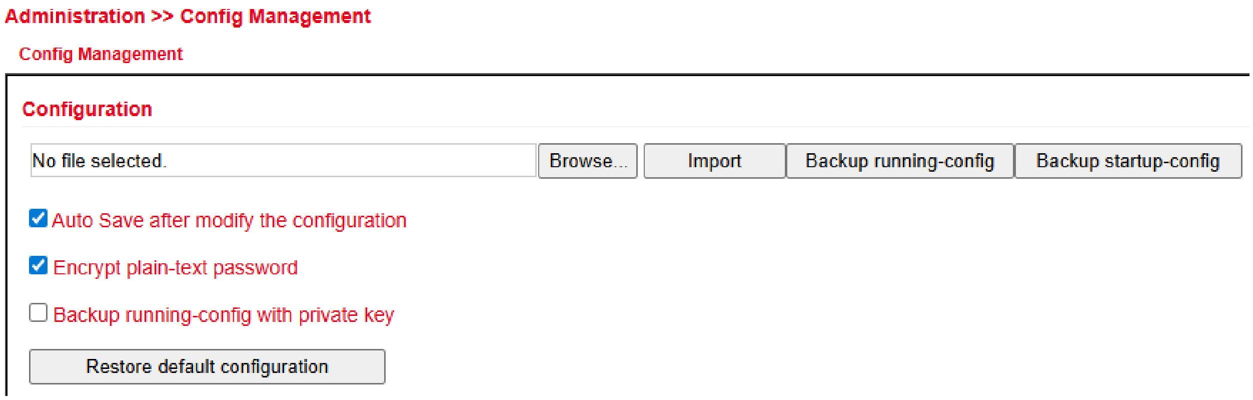
4.



Factory default settings	
IP:	192.168.2.1
Netmask:	255.255.255.0
Username:	adm
Password:	[check label]
Serial parameter:	115200-N-8-1

4.11.2 Web Method

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



Administration >> Config Management

Config Management

Configuration

No file selected.

☑ Auto Save after modify the configuration

☑ Encrypt plain-text password

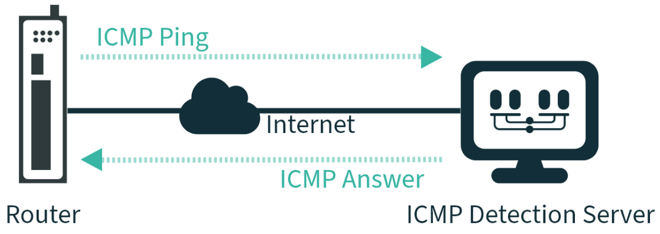
☐ Backup running-config with private key

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

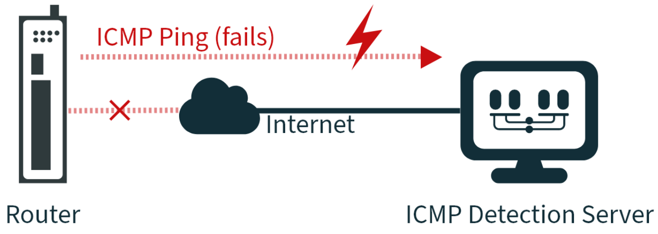
3) After clicking ***reboot*** the router reboots to factory defaults.

4.12 Watchdog

4.12.1 Self Monitoring of the Router



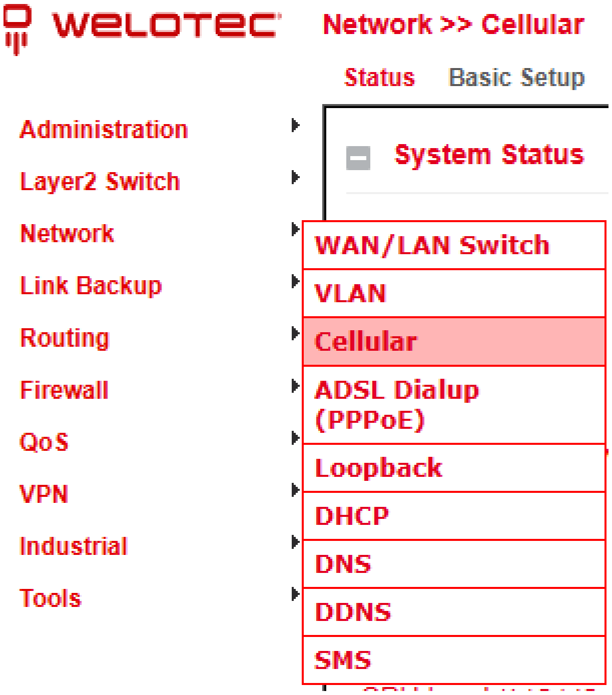
Internet connection active



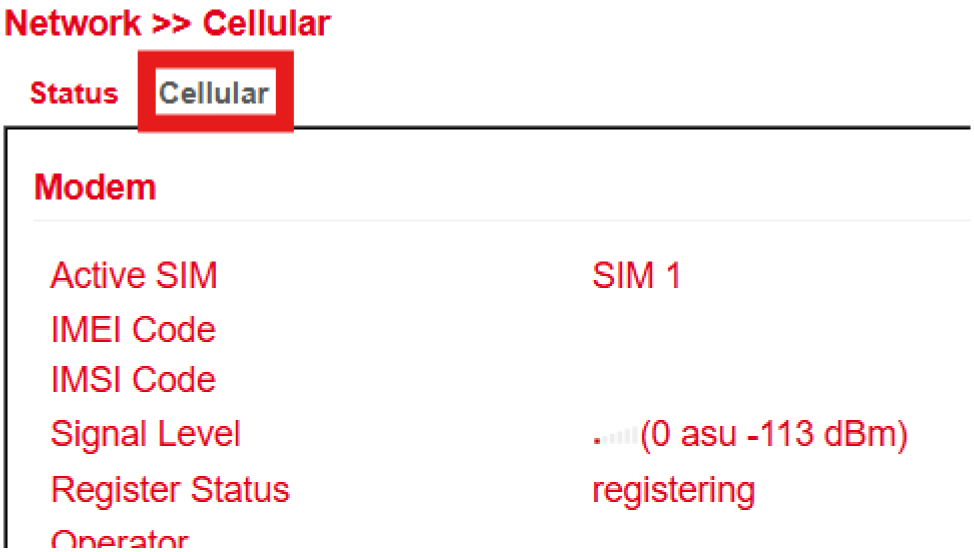
Watchdog active

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

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

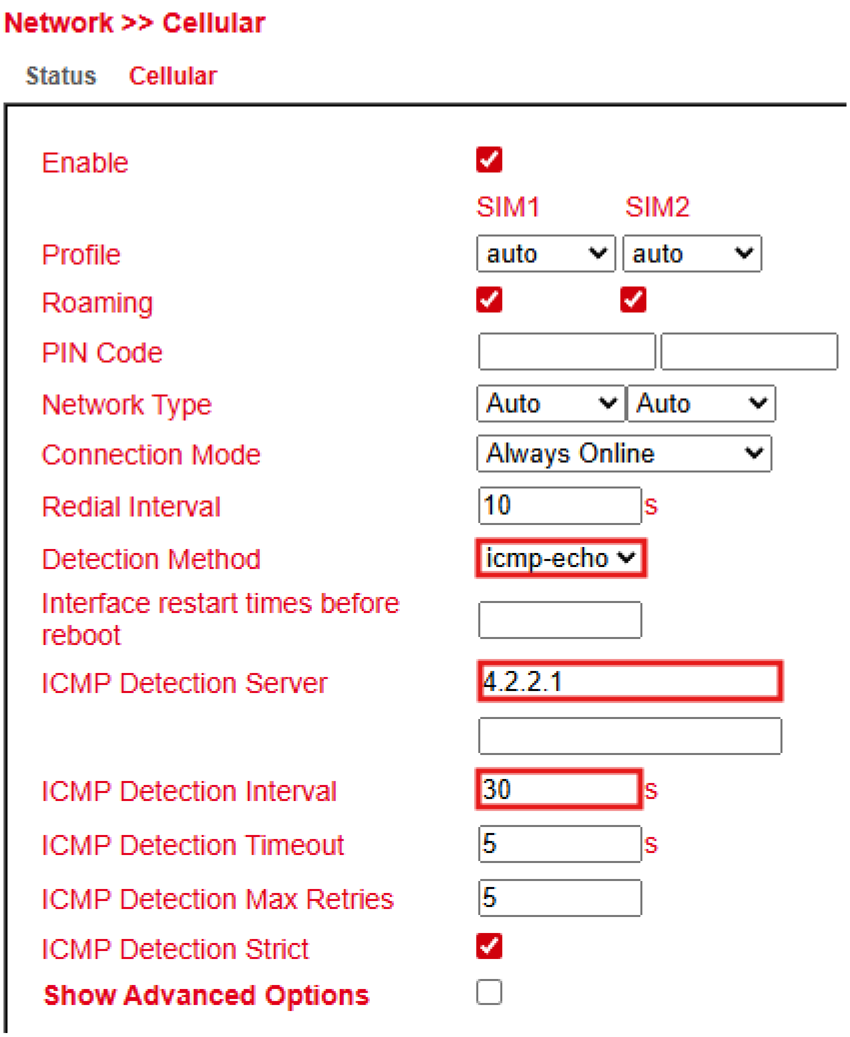


2) Select the ***Cellular*** tab



Active SIM SIM 1
IMEI Code
IMSI Code
Signal Level (0 asu -113 dBm)
Register Status registering
Operator

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



Network >> Cellular

Status Cellular

	SIM1	SIM2
Enable	☑	
Profile	auto	auto
Roaming	☑	☑
PIN Code		
Network Type	Auto	Auto
Connection Mode	Always Online	
Redial Interval	10 s	
Detection Method	icmp-echo	
Interface restart times before reboot		
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	□	

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

4.13 Port Mapping / Port Forwarding

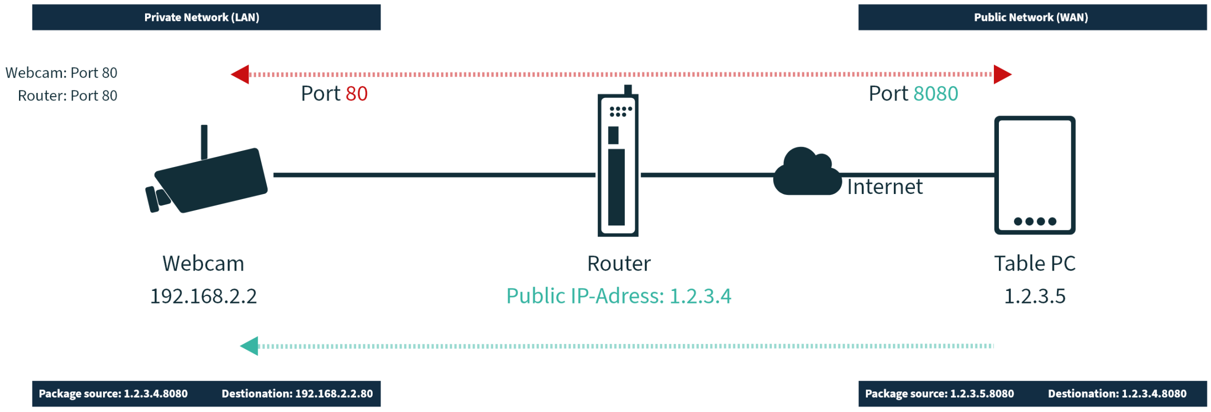
4.13.1 Access to Connected Devices via the Internet

To access devices connected to the Welotec router via the Internet, port mapping or port forwarding can be used. This is configured in the TK804L-450 router via NAT rules.

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

The instructions refer to all TK804L-450 routers with firmware ***Version 1.2.15*** or higher.

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


Private Network (LAN)
Public Network (WAN)
Webcam: Port 80
Router: Port 80
Port 80
Port 8080
Internet
Webcam
192.168.2.2
Router
Public IP-Adress: 1.2.3.4
Table PC
1.2.3.5
Package source: 1.2.3.4.8080
Destionation: 192.168.2.2.80
Package source: 1.2.3.5.8080
Destionation: 1.2.3.4.8080

Explanation:

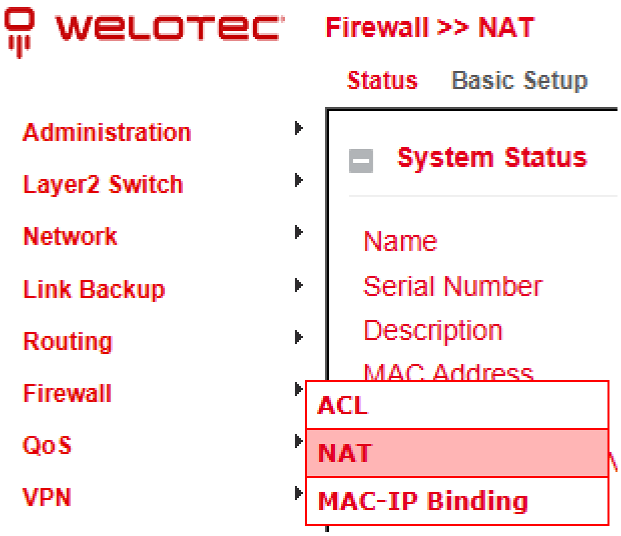
Welotec Router	
LAN IP address:	192.168.2.1
Subnet mask:	255.255.255.0

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

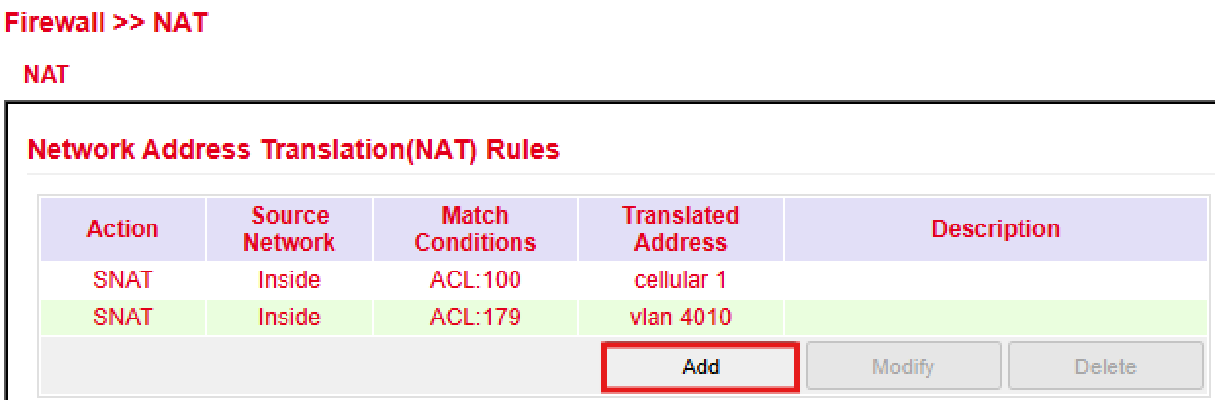
The IP camera has an interface that can be reached with a browser via **http://192.168.2.2** (note: http protocol has TCP port 80).

4.13.2 Port Mapping Guide

1. Go to `Firewall > NAT`



2. Click **Add** to create a new NAT rule



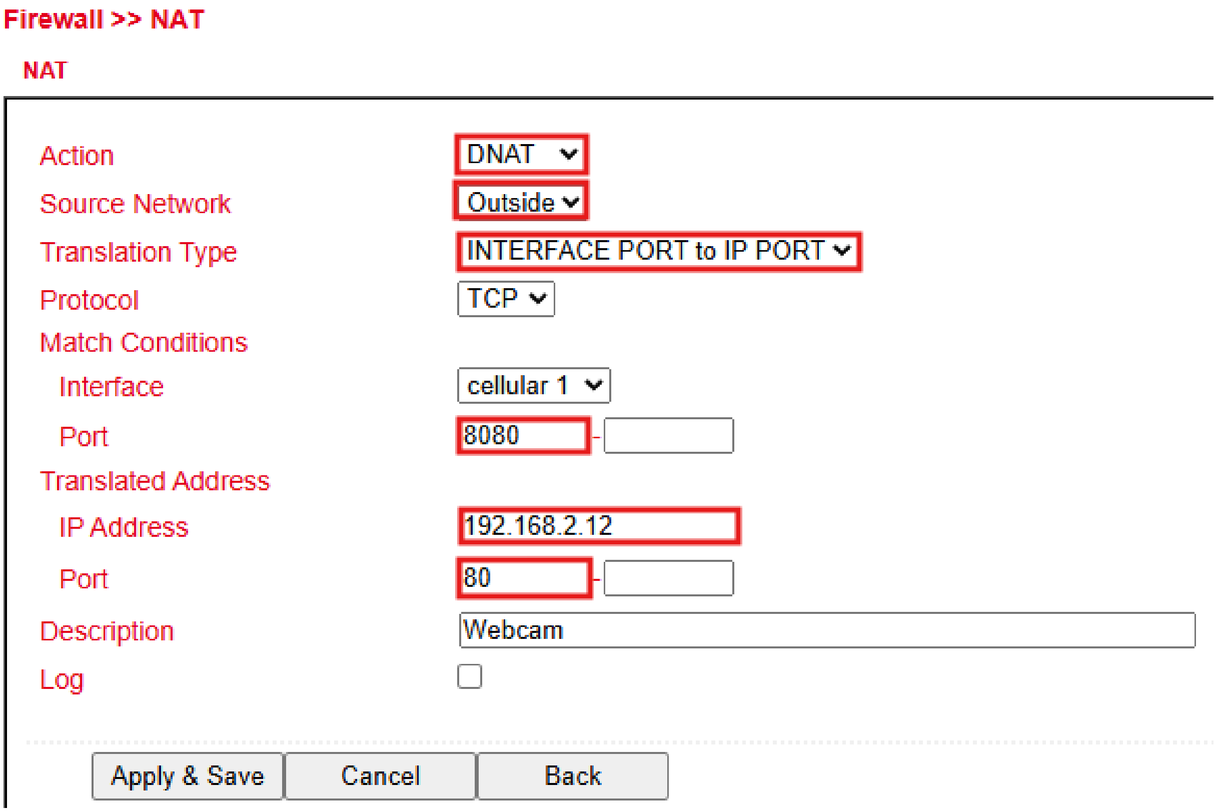
Firewall >> NAT

NAT

Network Address Translation(NAT) Rules

Action	Source Network	Match Conditions	Translated Address	Description
SNAT	Inside	ACL:100	cellular 1	
SNAT	Inside	ACL:179	vlan 4010	

3. Enter rule details (as shown)

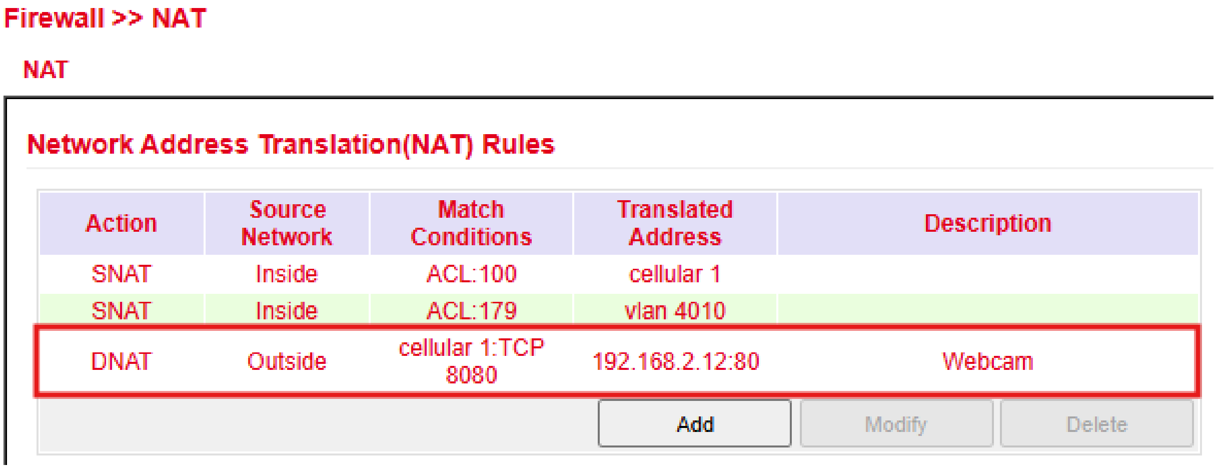


Firewall >> NAT

NAT

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 rule appears in the list



Firewall >> NAT

NAT

Network Address Translation(NAT) Rules

Action	Source Network	Match Conditions	Translated Address	Description
SNAT	Inside	ACL:100	cellular 1	
SNAT	Inside	ACL:179	vlan 4010	
DNAT	Outside	cellular 1:TCP 8080	192.168.2.12:80	Webcam

Checklist for functionality:

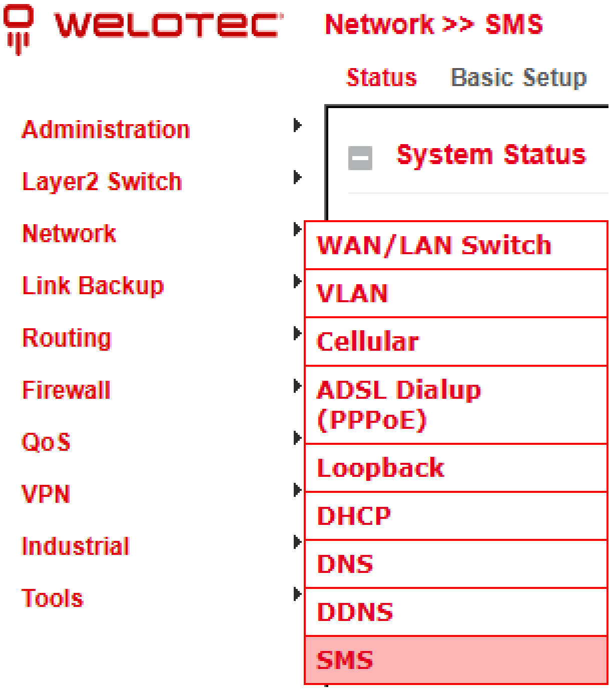
- Correct IP set on the device?
- Responds to `ping`?
- Web interface reachable?
- Gateway set to `192.168.2.1`?

4.14 SMS Functions

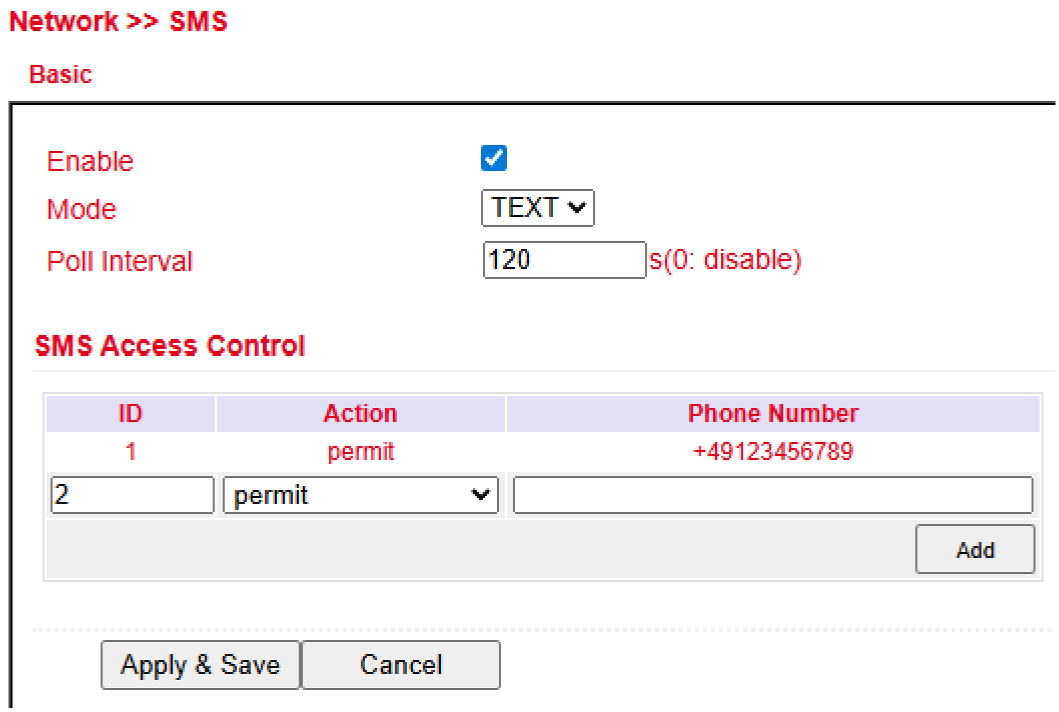
The TK804L-450 can be reached by SMS from the outside and reacts to various commands sent by SMS. One has the possibility to query the status of the device, to start / stop the dial-up or to restart the device.

4.14.1 Status Request / Restart

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



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



Network >> SMS

Basic

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

SMS Access Control

ID	Action	Phone Number
1	permit	+49123456789
2	permit	

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

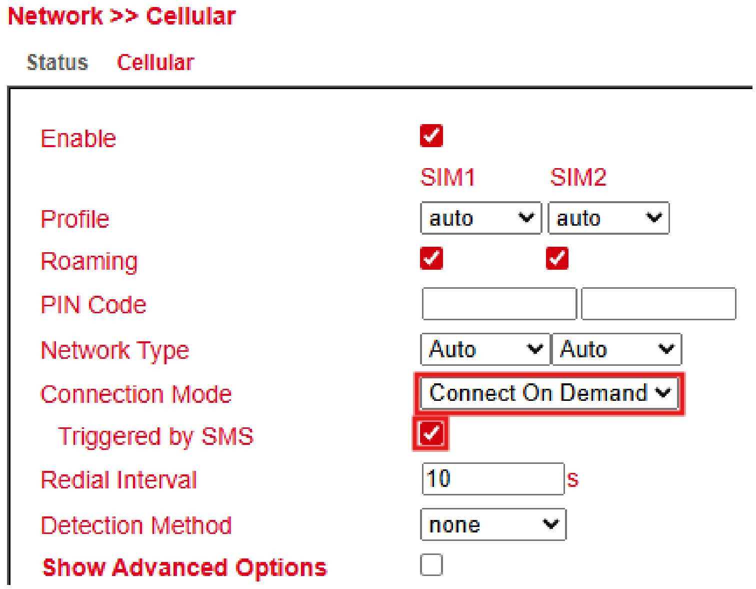
If now an SMS with the content ***show*** is sent to the mobile phone number of the router, the router sends its current status as response

4.14.2 Connecting or Disconnecting from the Internet

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

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

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



Network >> Cellular

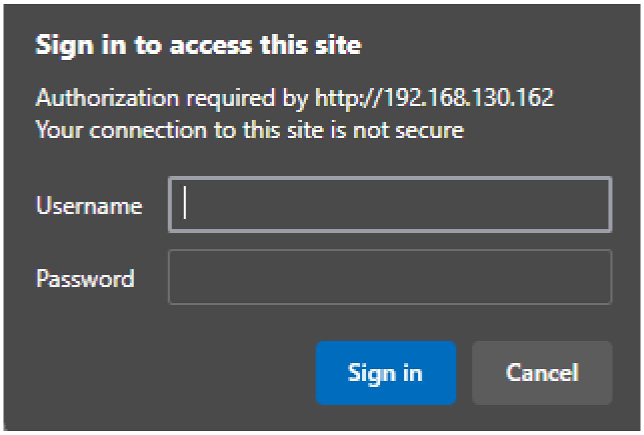
	SIM1	SIM2
Enable	☑	
Profile	auto	auto
Roaming	☑	☑
PIN Code		
Network Type	Auto	Auto
Connection Mode	Connect On Demand	
Triggered by SMS	☑	
Redial Interval	10 s	
Detection Method	none	
Show Advanced Options	□	

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

5 Web Configuration

5.1 Accessing the Web Interface

The **TK804 series routers** have a built-in web server for configuration.
Open `http://192.168.2.1` in your browser.
Enter the user name and password (default values printed on the label) and confirm with **Login**.



Sign in to access this site

Authorization required by http://192.168.130.162
Your connection to this site is not secure

Username

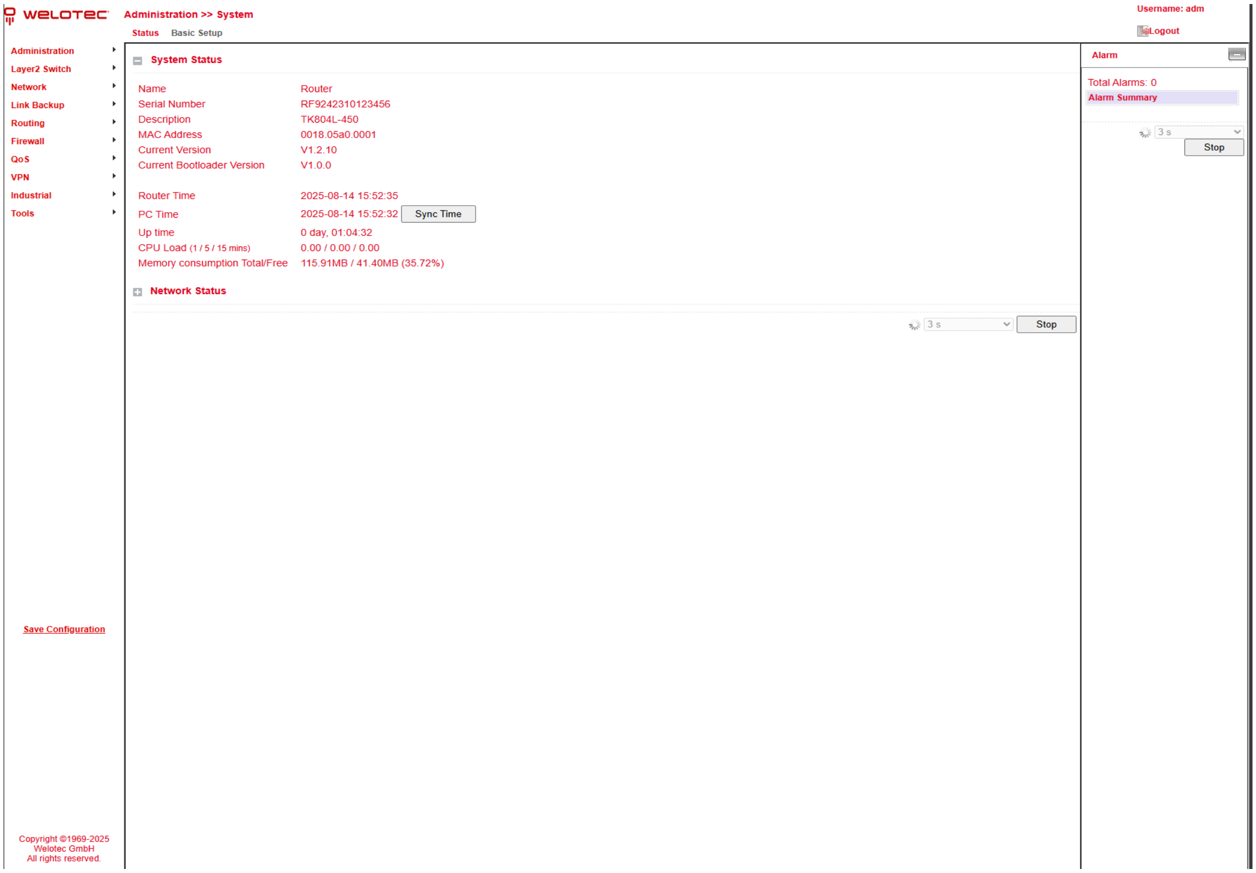
Password

☒ For security reasons, the password should be changed after the first login.
Choose a password with **at least 10 characters**, including:

- uppercase and lowercase letters
- numbers
- special characters

☒The router allows parallel access for up to **four users** via the web interface.
However, simultaneous configuration by multiple users should be avoided.

After successful login, the **router web interface** appears:



Name: Router
Serial Number: RF9242310123456
Description: TK804L-450
MAC Address: 0018.05a0.0001
Current Version: V1.2.10
Current Bootloader Version: V1.0.0

Router Time: 2025-08-14 15:52:35
PC Time: 2025-08-14 15:52:32
Up time: 0 day, 01:04:32
CPU Load (1 / 5 / 15 mins): 0.00 / 0.00 / 0.00
Memory consumption Total/Free: 115.91MB / 41.40MB (35.72%)

Total Alarms: 0

Copyright ©1969-2025
Welotec GmbH
All rights reserved.

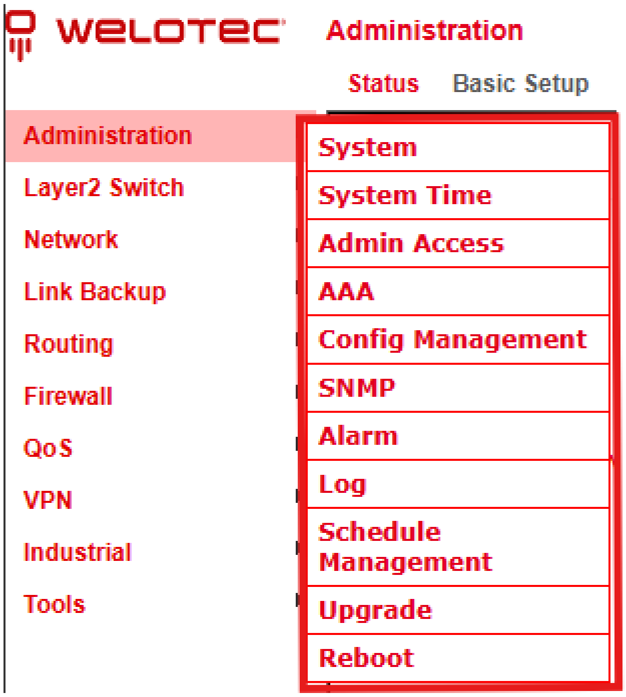
The web interface of the TK804L-450 is divided into **four areas**:

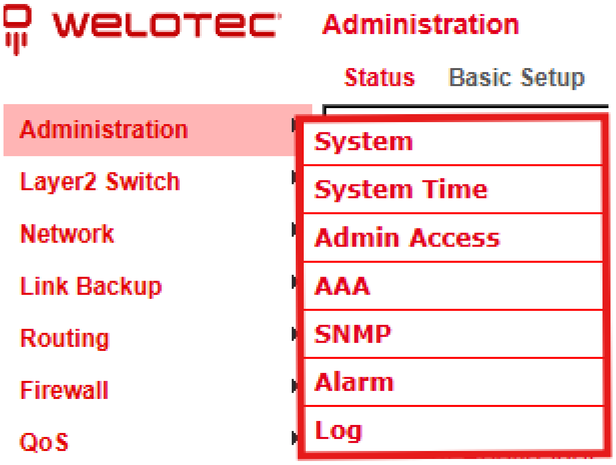
1. **Main navigation** (left) – e.g., Administration, Network.
2. **Detail navigation** (top) – e.g., *Status (active)*, *Basic Setup*.
3. **Main content area** (center) – shows status and configuration options.
4. **Alarm area** (right) – shows active alarms.

5.2 Administration

On the left side you will find the menu item **Administration**.
Clicking it with the mouse opens a submenu.
This area contains the **status overview** and **administration settings** for the router.

 With **restricted user rights** (not administrator), some menu items are missing.
Restricted users cannot configure the router, the **Apply & Save** option is unavailable,
and several configuration options are hidden.



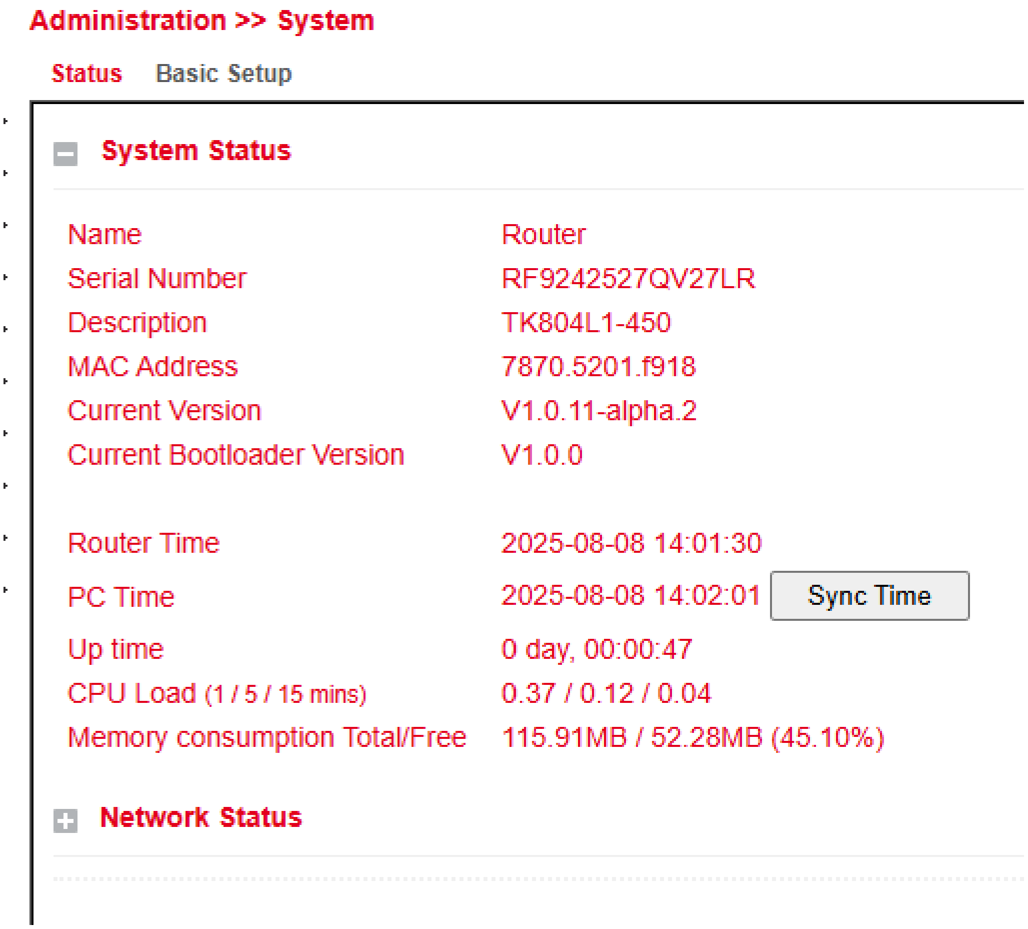


5.2.1 System

Status

Under **Administration > System > Status** you will find the most important **status information** of the router at a glance.

- With the **Sync Time** button, the router time can be synchronized with the time of the connected PC.



Administration >> System

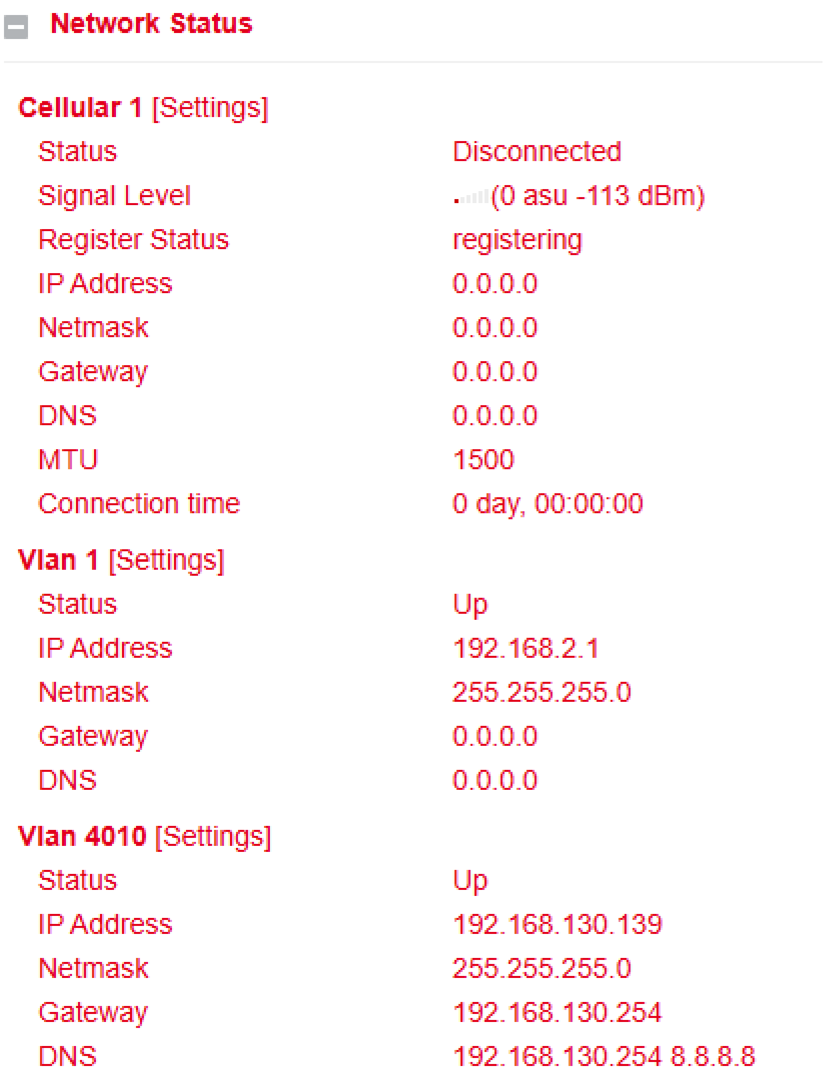
System Status

Name	Router
Serial Number	RF9242527QV27LR
Description	TK804L1-450
MAC Address	7870.5201.f918
Current Version	V1.0.11-alpha.2
Current Bootloader Version	V1.0.0
Router Time	2025-08-08 14:01:30
PC Time	2025-08-08 14:02:01
Up time	0 day, 00:00:47
CPU Load (1 / 5 / 15 mins)	0.37 / 0.12 / 0.04
Memory consumption Total/Free	115.91MB / 52.28MB (45.10%)

Network Status

- Below the system status, you will find the **Network Status** section.
  By clicking on the gray [+] symbol, details of the individual network interfaces will expand.
  Here you can see all relevant information about each interface.

☒ By clicking on [**Settings**] next to an interface (e.g., *Cellular 1*), you can directly access its configuration page.



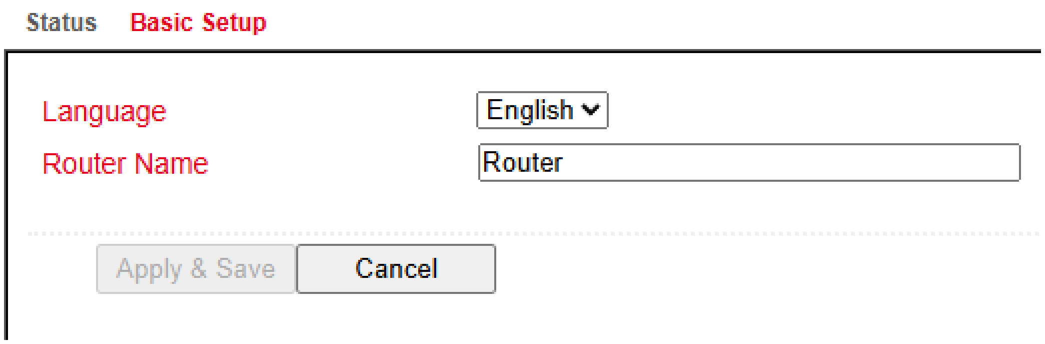
Network Status

Cellular 1 [Settings]	
Status	Disconnected
Signal Level	(0 asu -113 dBm)
Register Status	registering
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	0 day, 00:00:00
Vlan 1 [Settings]	
Status	Up
IP Address	192.168.2.1
Netmask	255.255.255.0
Gateway	0.0.0.0
DNS	0.0.0.0
Vlan 4010 [Settings]	
Status	Up
IP Address	192.168.130.139
Netmask	255.255.255.0
Gateway	192.168.130.254
DNS	192.168.130.254 8.8.8.8

Basic Setup

Under **Administration** > **System** > **Basic Setup** you can configure:

- **Language** – currently only *English* is supported.
- **Router name** – choose a meaningful, unique name for easier identification.



Language	English
Router Name	Router

5.2.2 System Time

To ensure correct coordination between the TK804L-450 router and other devices, the **system time** must be consistent across all components.

Under **Administration > System Time** you can configure:

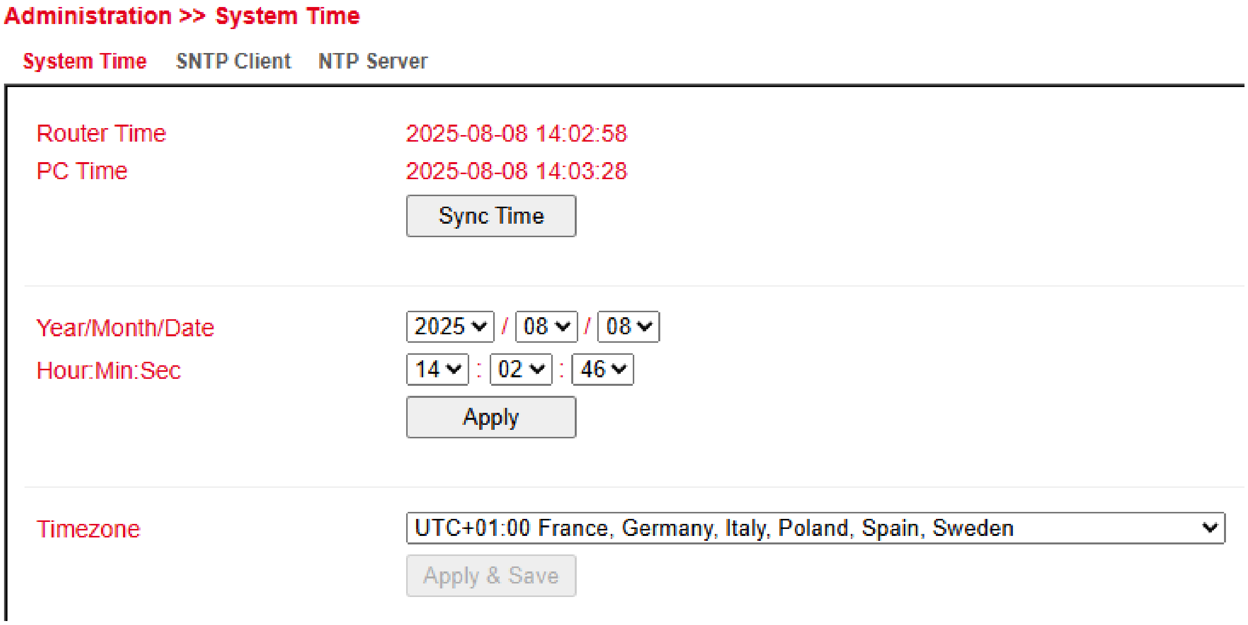
- **Manual time setting**
- **Automatic synchronization** via a time server using the **Simple Network Time Protocol** (SNTP)
- **NTP server function** – allows connected devices to obtain the current time from the router

System Time Configuration

Under **Administration > System Time** you will find an overview and local settings for the system time of the router.

- With **Sync Time**, the router time can be synchronized with the time of the connected PC.
- Time and date can also be set **manually**.
- Under **Timezone**, the current time zone can be selected.

The default is **UTC+1** (Germany, Austria, Switzerland).



Administration >> System Time

System Time | SNTP Client | NTP Server

Router Time: 2025-08-08 14:02:58
PC Time: 2025-08-08 14:03:28

Year/Month/Date: 2025 / 08 / 08
Hour:Min:Sec: 14 : 02 : 46

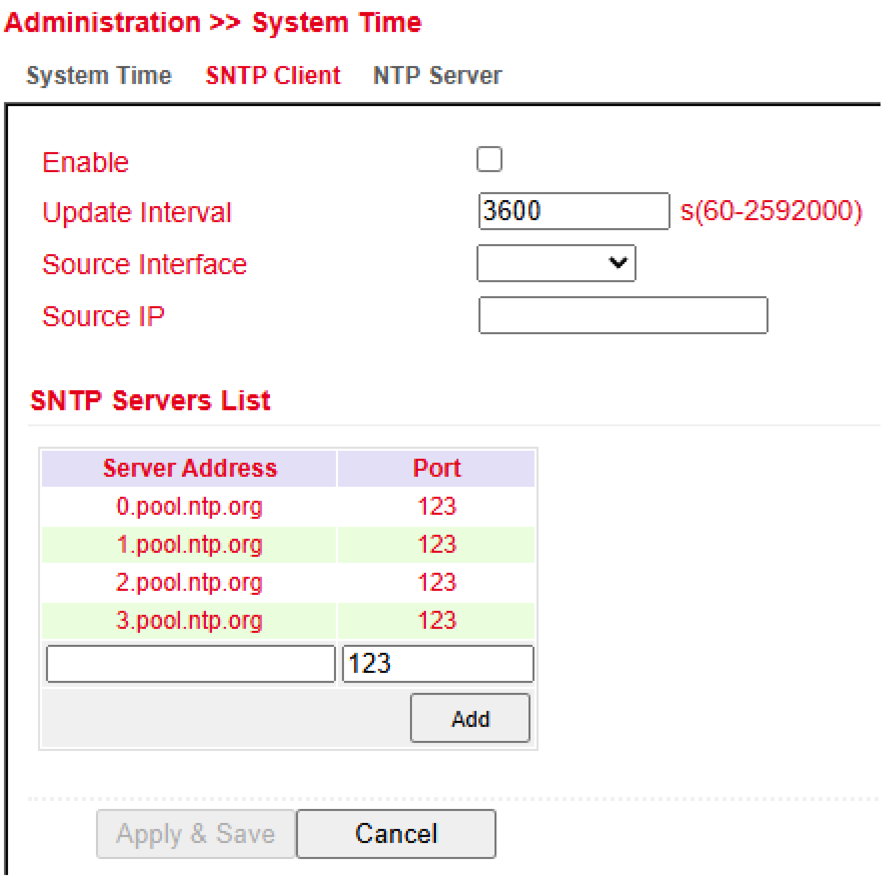
Timezone: UTC+01:00 France, Germany, Italy, Poland, Spain, Sweden

SNTP Client

SNTP (Simple Network Time Protocol) is used to synchronize the clocks of network devices.
It provides mechanisms to synchronize time across a subnet, a network, or the Internet.

- Typical accuracy: **1–50 ms**, depending on the synchronization source and routers.
- Goal: Ensure that all devices in a network share the same clock, so distributed applications run consistently.

Under **Administration > System Time > SNTP Client** you can configure the router to update its time from a **public or private time server**.



Administration >> System Time

Enable	□
Update Interval	3600 s(60-2592000)
Source Interface	
Source IP	

SNTP Servers List

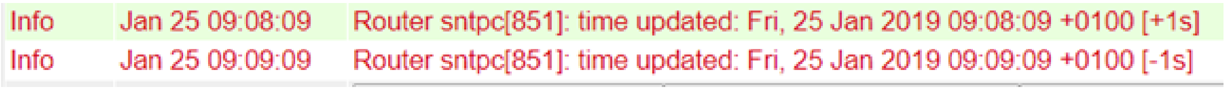
Server Address	Port
0.pool.ntp.org	123
1.pool.ntp.org	123
2.pool.ntp.org	123
3.pool.ntp.org	123
	123

⊠ Before setting up an SNTP client:

- Verify that the selected **SNTP server is reachable**.
- If using a **domain name**, ensure that the DNS server is configured correctly for name resolution.

You can configure either a **Source Interface** or a **Source IP**.

After a successful update, the following entry will appear under **Administration > Log**:



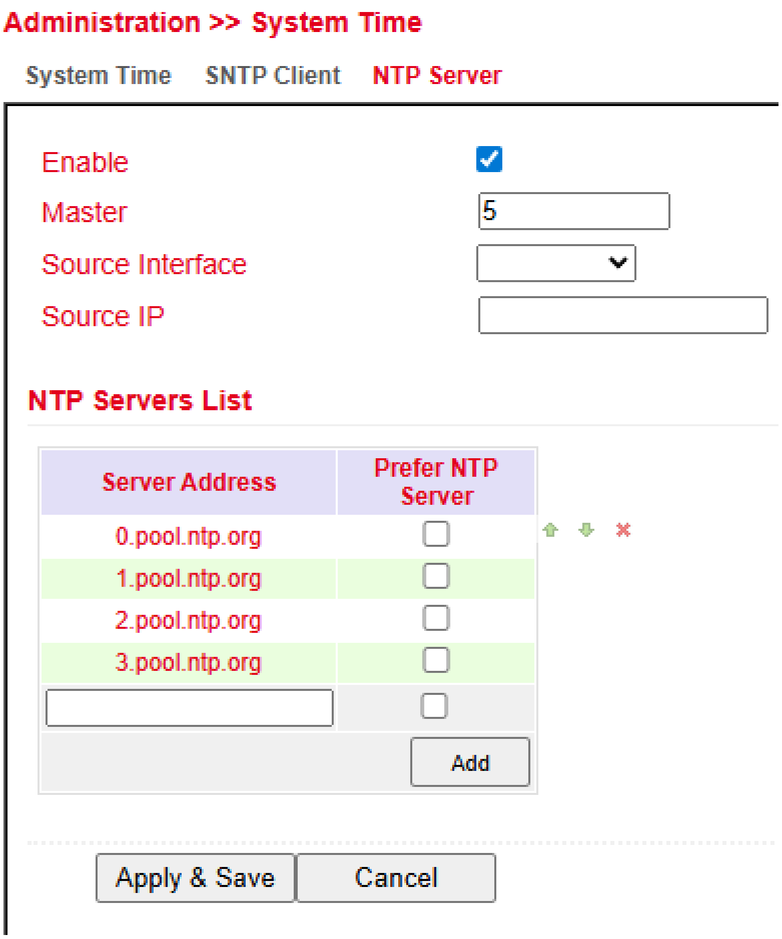
```
Info   Jan 25 09:08:09   Router sntpc[851]: time updated: Fri, 25 Jan 2019 09:08:09 +0100 [+1s]
Info   Jan 25 09:09:09   Router sntpc[851]: time updated: Fri, 25 Jan 2019 09:09:09 +0100 [-1s]
```

NTP Server

The settings for the time server are located under **Administration > System Time > NTP Server**.
In this mode, the TK804L-450 can act as a **time server** for connected devices.

- **Master (Stratum):** Defines the accuracy level of the server.
  - Range: **2–15**
  - Lower values indicate proximity to a highly accurate time source (e.g., atomic or radio clock).
- **Source Interface:** Specifies the interface from which devices can request NTP.
- **Source IP:** Alternative option for providing NTP service.

⊠ **Important:**
NTP **server** and NTP **client** operate independently.
This means both require their own NTP service from the Internet.
To configure this, enter the address under **Server Address** (multiple entries possible).



Administration >> System Time

Enable	☑
Master	5
Source Interface	
Source IP	

NTP Servers List

Server Address	Prefer NTP Server
0.pool.ntp.org	□
1.pool.ntp.org	□
2.pool.ntp.org	□
3.pool.ntp.org	□
	□

5.2.3 Admin Access

Management Services

Under **Administration > Management Services** you can configure access to the router via:

- **HTTP / HTTPS** – web interface
- **Telnet / SSH** – Command Line Interface (CLI)

HTTP

HTTP (Hypertext Transfer Protocol) is used for unencrypted access to the router's web interface.

HTTPS

HTTPS (Hypertext Transfer Protocol Secure) uses **SSL/TLS encryption** to secure HTTP communication.

Telnet

Telnet allows access to the router's **Command Line Interface (CLI)**.
⊠ Since Telnet is unencrypted, it is recommended to use **SSH** instead.

SSH

SSH (Secure Shell) provides encrypted CLI access to the router, comparable to Telnet but secure.

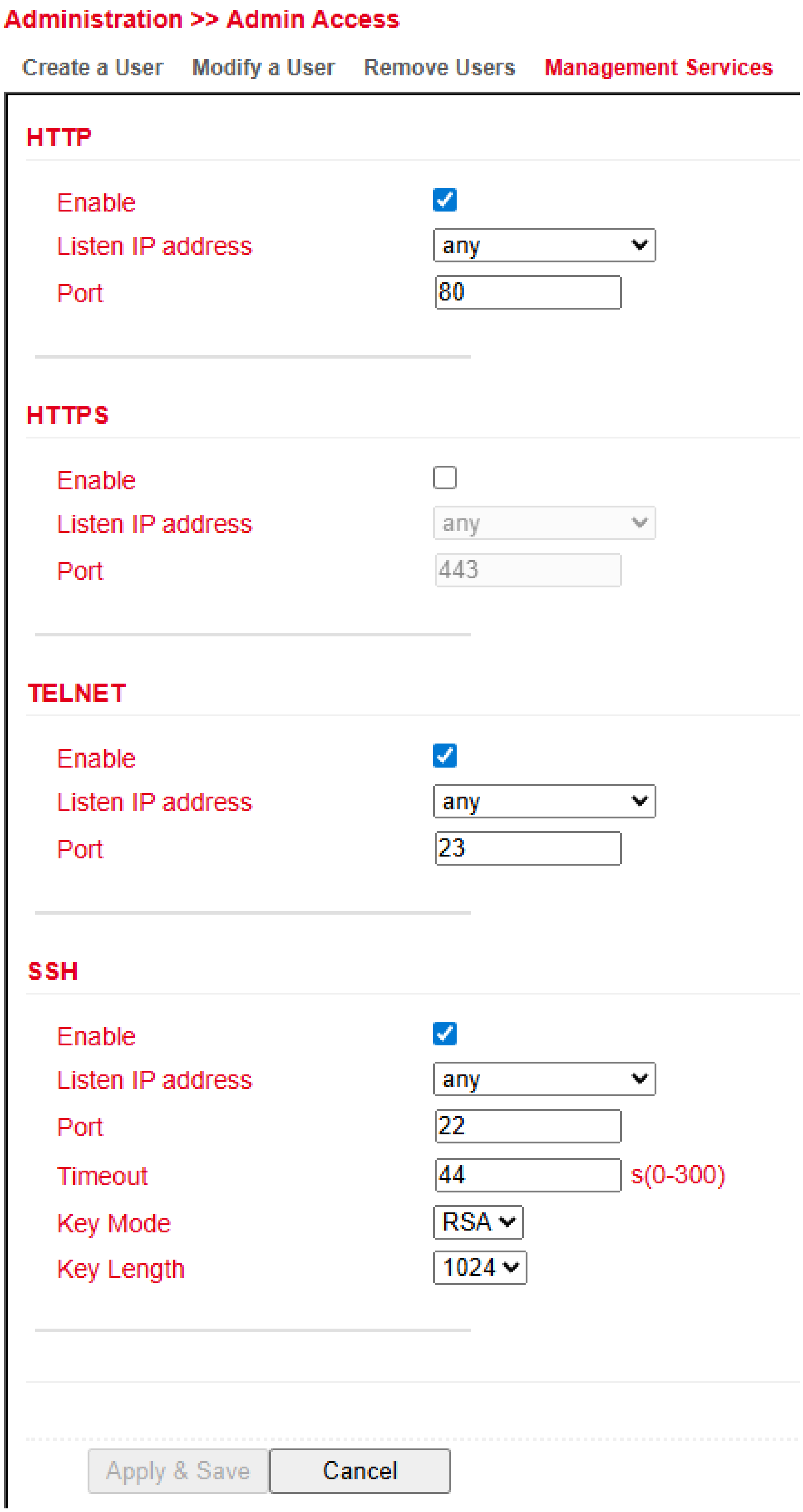
Configuration Options

For each service (HTTP, HTTPS, Telnet, SSH) you can configure:

- **Enable / Disable** the service
- **Port** – select the TCP port for the service
- **ACL Enable** – activate access control:
  - **Source Range** and **IP Wildcard** define which IP addresses or ranges may access the router
- **SSH-specific options:**
  - **Timeout** – inactive sessions are automatically closed after this period
  - **Key Mode / Key Length** – define encryption standard and key size

Other Parameters

- **Web login timeout** – defines how long a web session remains active without input.
  - After the timeout expires, the user is logged out automatically.



Administration >> Admin Access

HTTP

Enable	☑
Listen IP address	any
Port	80

HTTPS

Enable	□
Listen IP address	any
Port	443

TELNET

Enable	☑
Listen IP address	any
Port	23

SSH

Enable	☑
Listen IP address	any
Port	22
Timeout	44 s(0-300)
Key Mode	RSA
Key Length	1024

User Management

Under **Administration > User Management** you can configure the users that have access to the router.
The router distinguishes between **Administrator** and **Standard User**:

- **Administrator (adm)** – created by the system, full rights
- **Standard User** – created by the administrator, limited rights (monitoring only)

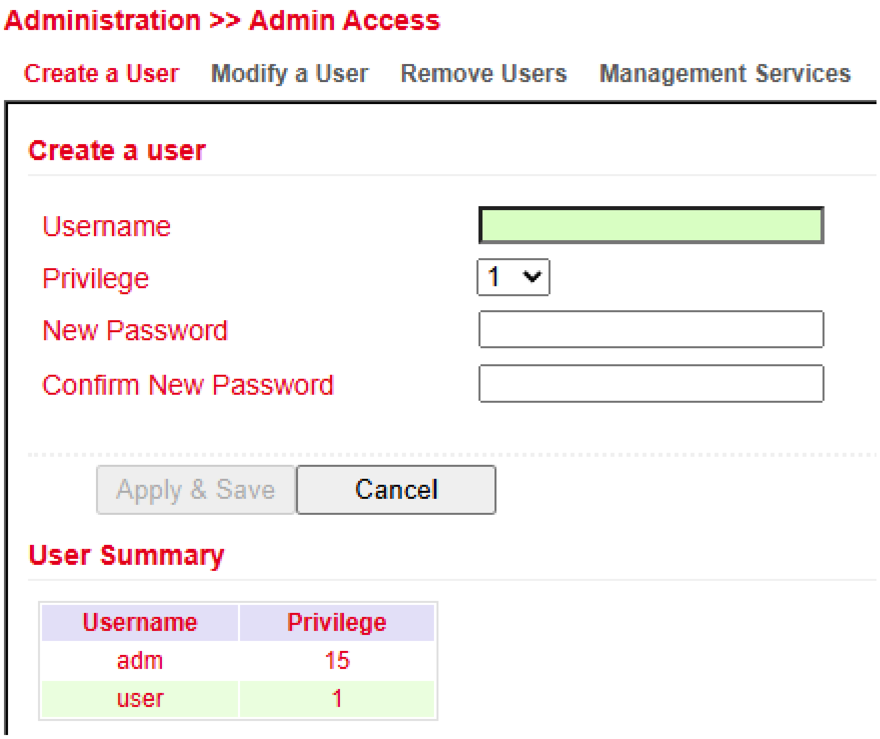
Create a User

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

Required fields:

- **Username**
- **Password**
- **Permission (Privilege):**
  - **1–14** → standard users (*read-only*)
  - **15** → administrators (*full access*)

Under **User Summary** you will find a list of all users and their assigned privileges.



Create a user

Username	
Privilege	1
New Password	
Confirm New Password	

User Summary

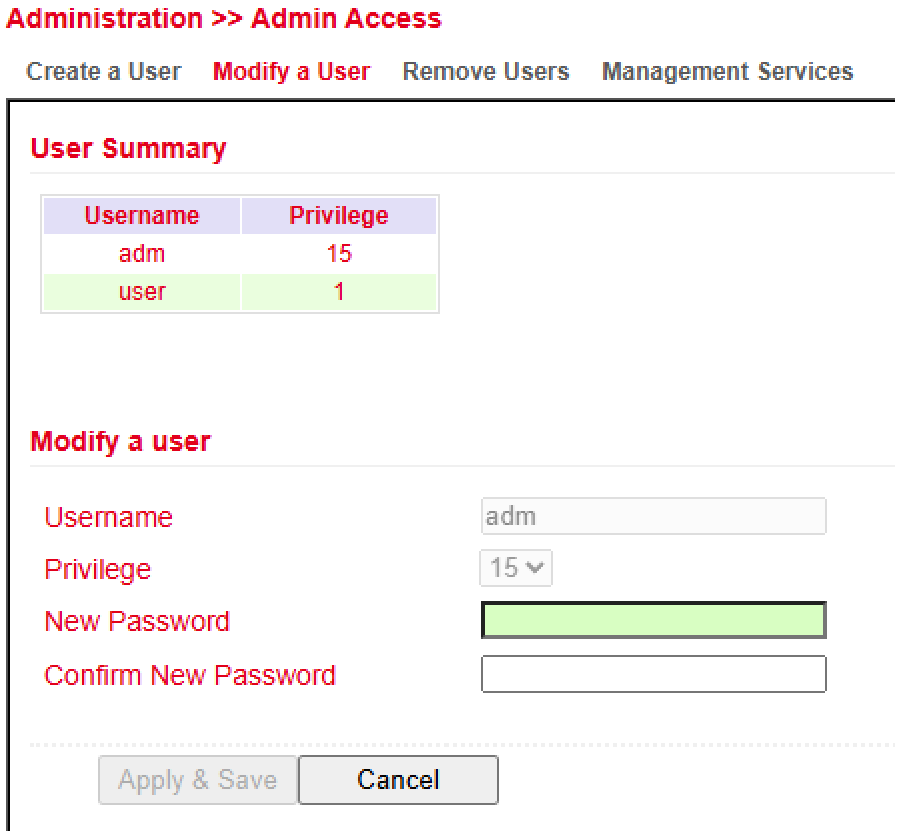
Username	Privilege
adm	15
user	1

⊠ **Password policy:**
Use at least **8 characters**, including uppercase/lowercase letters, numbers, and special characters.
The username **root** is reserved for the operating system.

Modify a User

To change user settings, go to **Administration > User Management > Modify a User**. Here you can update **permissions** and **passwords**.

In **User Summary**, select a user and edit them under **Modify a User**.



Administration >> Admin Access

User Summary

Username	Privilege
adm	15
user	1

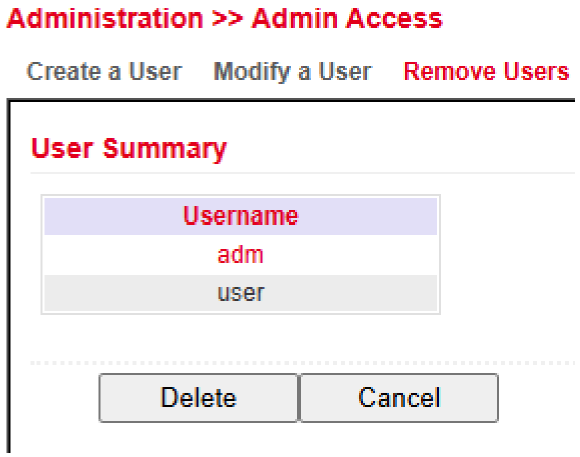
Modify a user

Username	adm
Privilege	15
New Password	
Confirm New Password	

Remove Users

Under **Administration > User Management > Remove Users** you can delete accounts.

1. Select the user in **User Summary**.
2. Click **Delete** to remove the account.



Administration >> Admin Access

User Summary

Username
adm
user

5.2.4 AAA

AAA (Authentication, Authorization, Accounting) is a framework for managing network access:

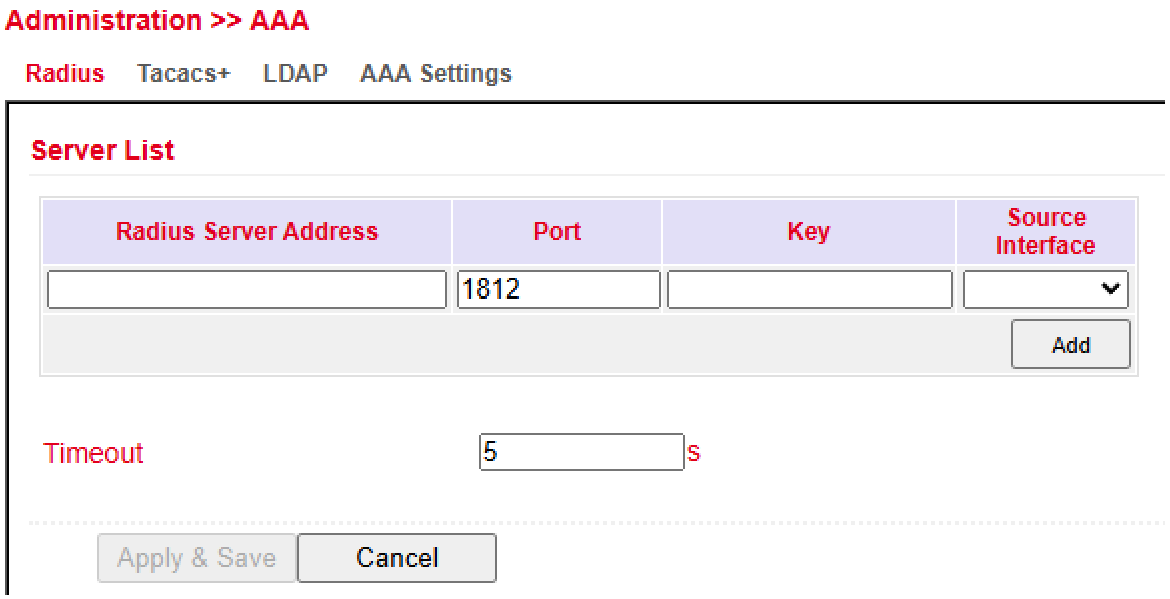
- **Authentication** → controls whether a user may access the device or network
- **Authorization** → defines which services or resources the user may access
- **Accounting** → logs all access events and resource usage

Notes:

- Not all AAA services must be enabled; one or two can be used as needed.
- AAA typically follows a **client–server architecture**.
- The **TK804L-450** acts as an **AAA client** and supports:
  - **RADIUS**
  - **TACACS+**
  - **LDAP**

RADIUS

RADIUS (Remote Authentication Dial-In User Service) is a client–server protocol used for **authentication, authorization, and accounting**.



Radius Server Address	Port	Key	Source Interface
	1812		

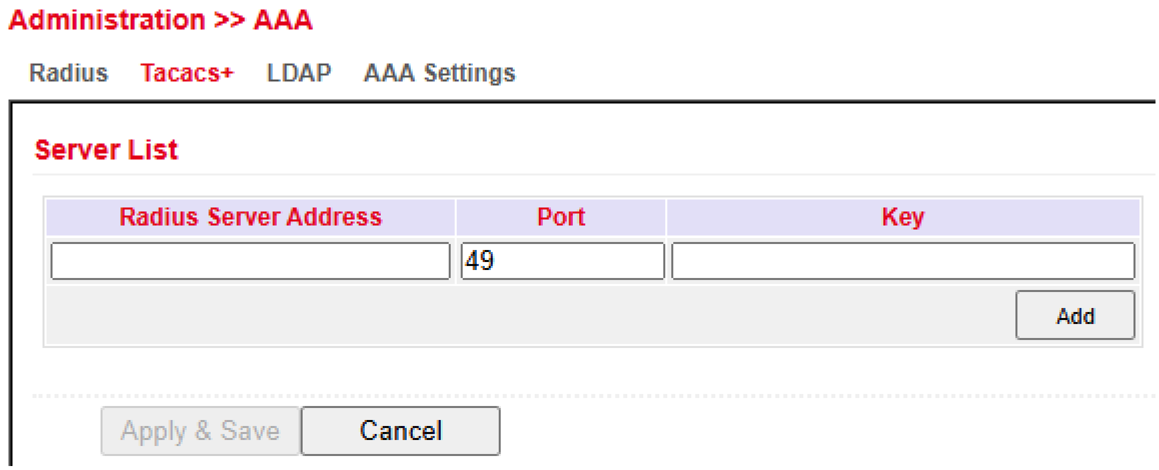
Timeout 5 s

You can configure:

- **FQDN or IP address** of the RADIUS server
- **Port**
- **Shared Key**
- **Source Interface**

TACACS+

TACACS+ (Terminal Access Controller Access Control System) is a client–server protocol used for **authentication, authorization, and accounting**.
It provides communication between **AAA servers** and a **Network Access Server (NAS)**.



Administration >> AAA

Server List

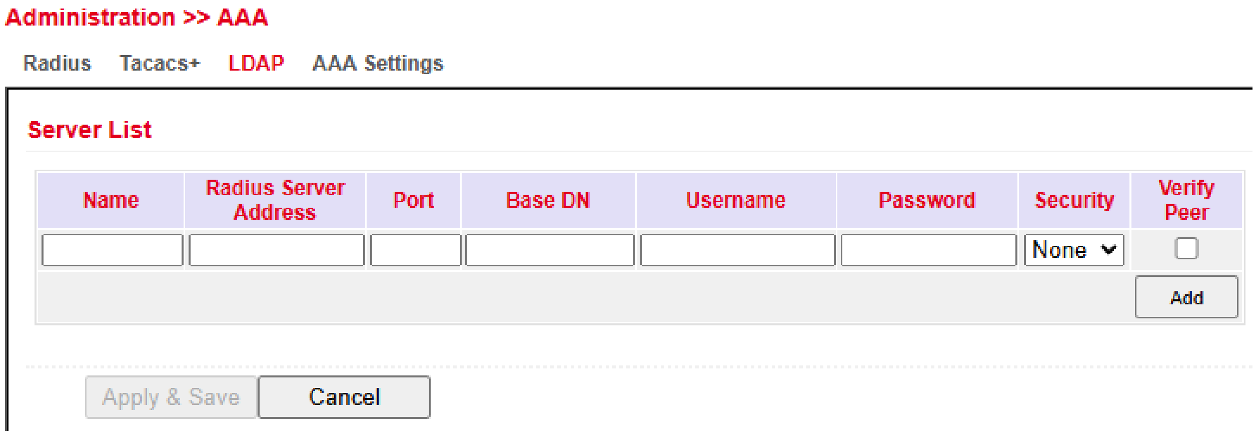
Radius Server Address	Port	Key
	49	

You can configure:

- **Server Address**
- **Port**
- **Shared Key**

LDAP

LDAP (Lightweight Directory Access Protocol) is a protocol based on the client–server model, suitable for querying and modifying information from **directory services**.



Administration >> AAA

Server List

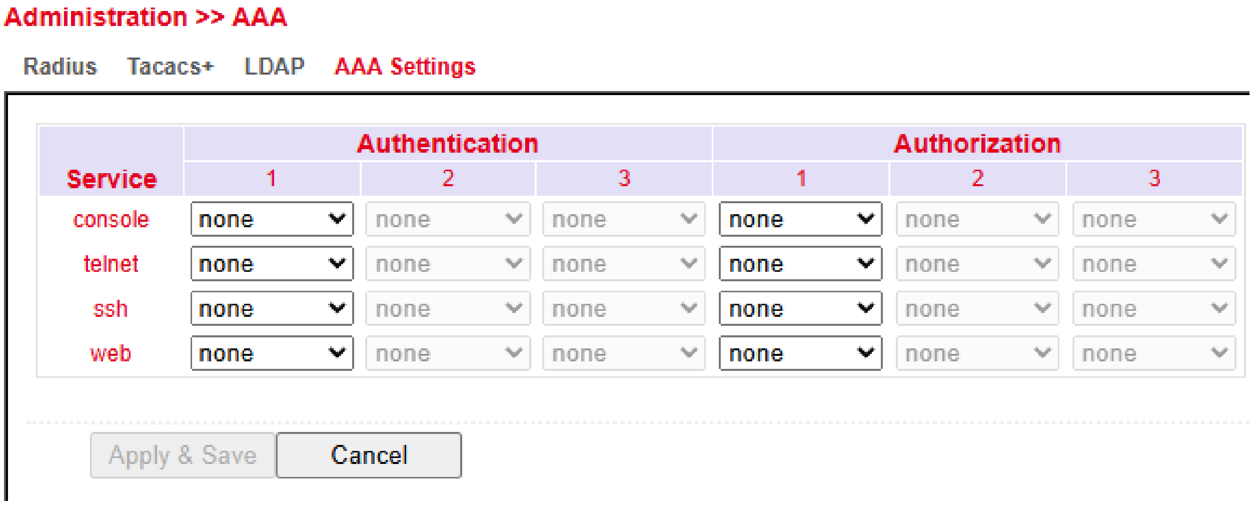
Name	Radius Server Address	Port	Base DN	Username	Password	Security	Verify Peer
						None	□

Enter the required connection details for your LDAP server here.

AAA Settings

The AAA Settings page lets administrators configure Authentication and Authorization for different management services: ***Console, Telnet, SSH, and Web***.

- ***Authentication:*** Verifies user identity. Up to three methods (e.g., Local, RADIUS, TACACS+, LDAP) can be set in order of preference.
- ***Authorization:*** Controls user permissions after authentication. Also supports up to three methods.
- None means no AAA is applied.
- ***Apply & Save*** stores the changes; Cancel discards them.



Administration >> AAA

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

5.2.5 Config Management

Under **Administration > Config Management** you can:

- Save the current configuration
- Import an existing configuration
- Reset the router to factory defaults

Importing an Existing Configuration

1. Click **Browse…** and select a configuration file.
2. Click **Import** to upload it.
3. After successful import, restart the router to activate the configuration.

Saving an Existing Configuration

- **Backup running-config** → saves the current configuration including unconfirmed changes.
- **Backup startup-config** → saves the configuration without unconfirmed changes.

Automatic Saving

If **Auto Save after modify the configuration** is checked:

- All changes are applied immediately and persist after reboot.

If not checked:

- Changes will be lost after reboot unless saved manually via **Save Configuration** (bottom left navigation).

Reset to Factory Defaults

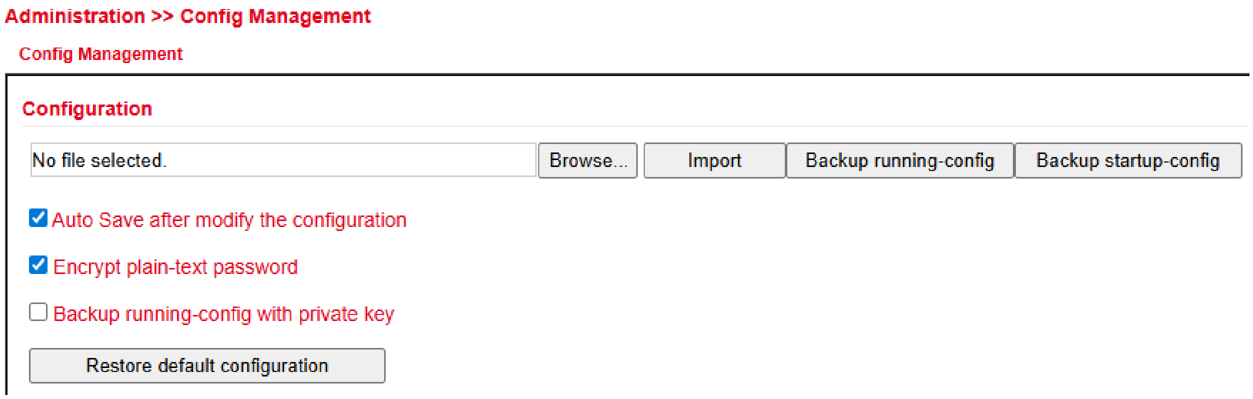
Click **Restore default configuration** to reset the router to its default settings.

Encrypt Passwords in the Configuration File

Enable **Encrypt plain-text password** to prevent passwords from being displayed in clear text.

Back Up Running-Config with Private Key

Enable **Backup running-config with private key** to include imported private keys from certificate management in the backup.



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

5.2.6 SNMP

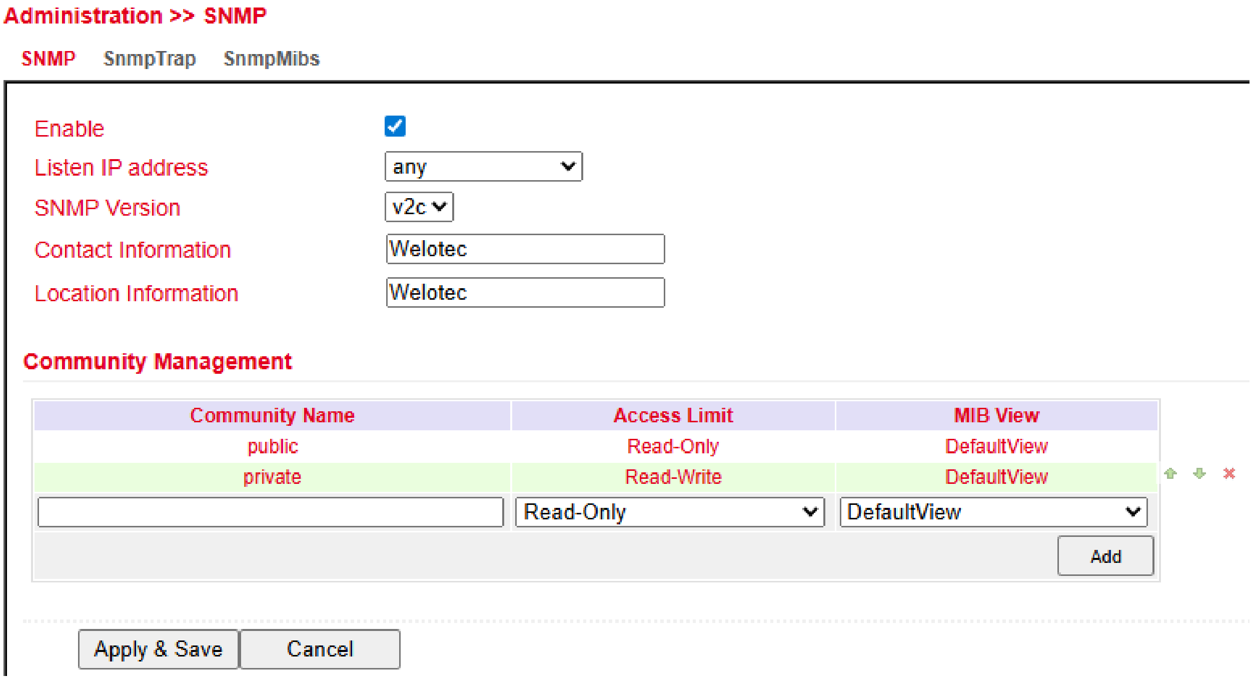
SNMP (Simple Network Management Protocol) is an IETF-standard protocol used to **monitor and control network elements** such as routers, servers, switches, printers, and computers from a central station.

- SNMP defines the structure of the data packets and the communication flow.
- It was designed so that any network-capable device can be integrated into monitoring.
- Communication occurs between **monitored devices (agents)** and the **monitoring station (manager)**.

SNMP Configuration

The TK804L-450 supports **SNMP v1, v2c, and v3**.

- **SNMPv1 / v2c**: use a **community name** for authentication with *read-only* or *read-write* rights.
  The IP address for the SNMP service can be selected under **Listen IP address**.



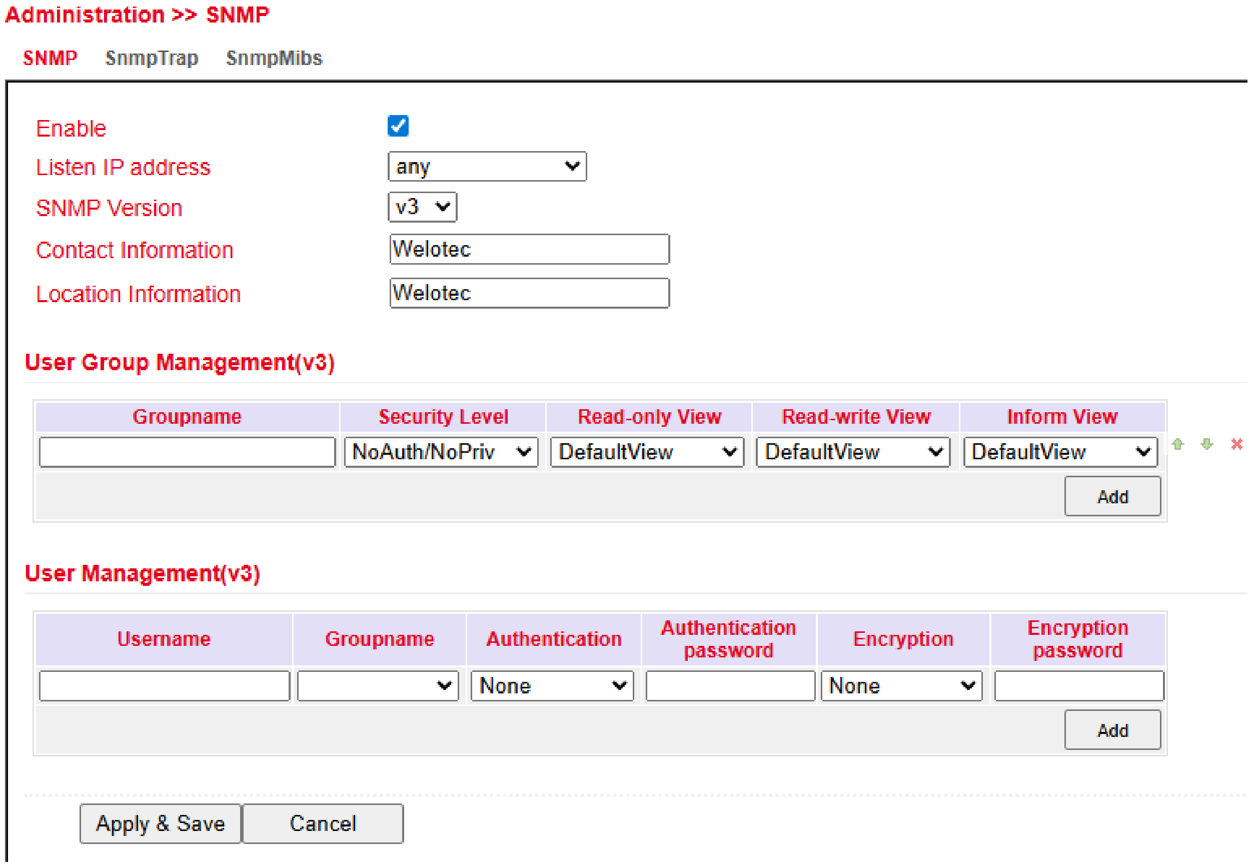
Administration >> SNMP

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**: uses **username/password authentication** and provides **group management**. This allows individual users to be authorized more precisely compared to v1/v2.



Administration >> SNMP

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)

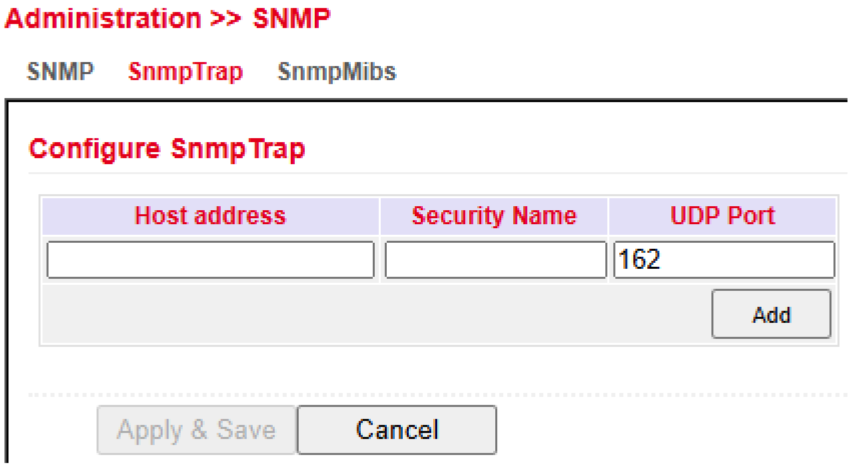
Username	Groupname	Authentication	Authentication password	Encryption	Encryption password
		None		None	

Supported in SNMPv3:

- **Authentication** → SHA or MD5
- **Encryption** → AES or DES

SNMP Trap

An **SNMP Trap server** can be configured.
This allows the router to actively send SNMP messages to the management server instead of waiting for requests.



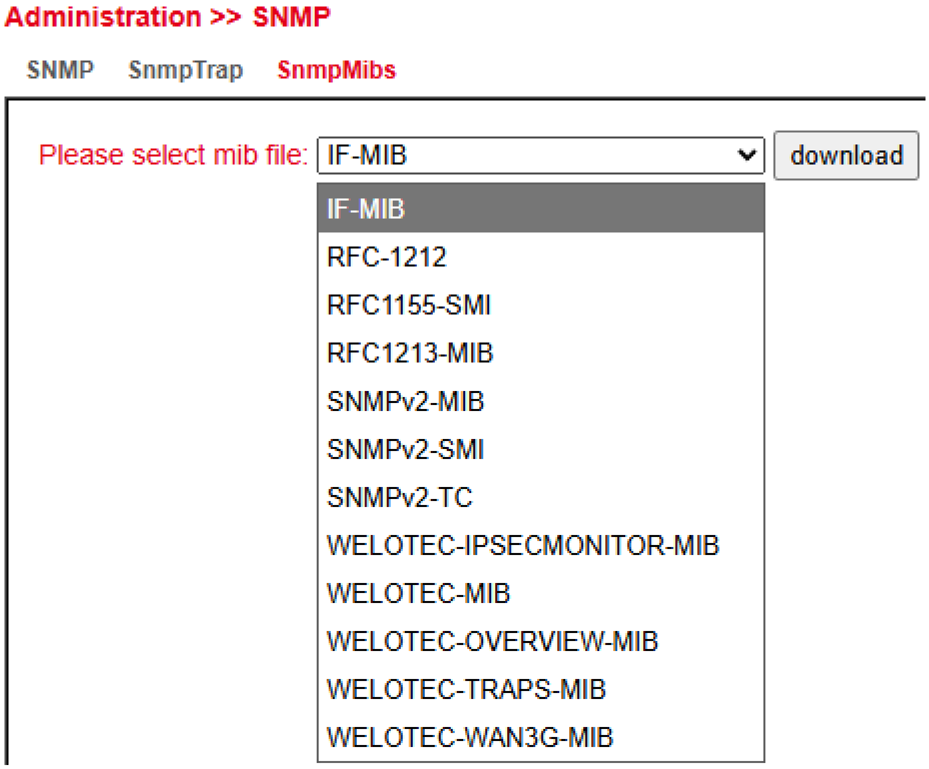
Administration >> SNMP

Configure SnmpTrap

Host address	Security Name	UDP Port
		162

SNMP MIBs

The **SNMP MIB files** for monitoring the router can be downloaded and used for evaluations.
Select the desired MIB file and click the **Download** button.

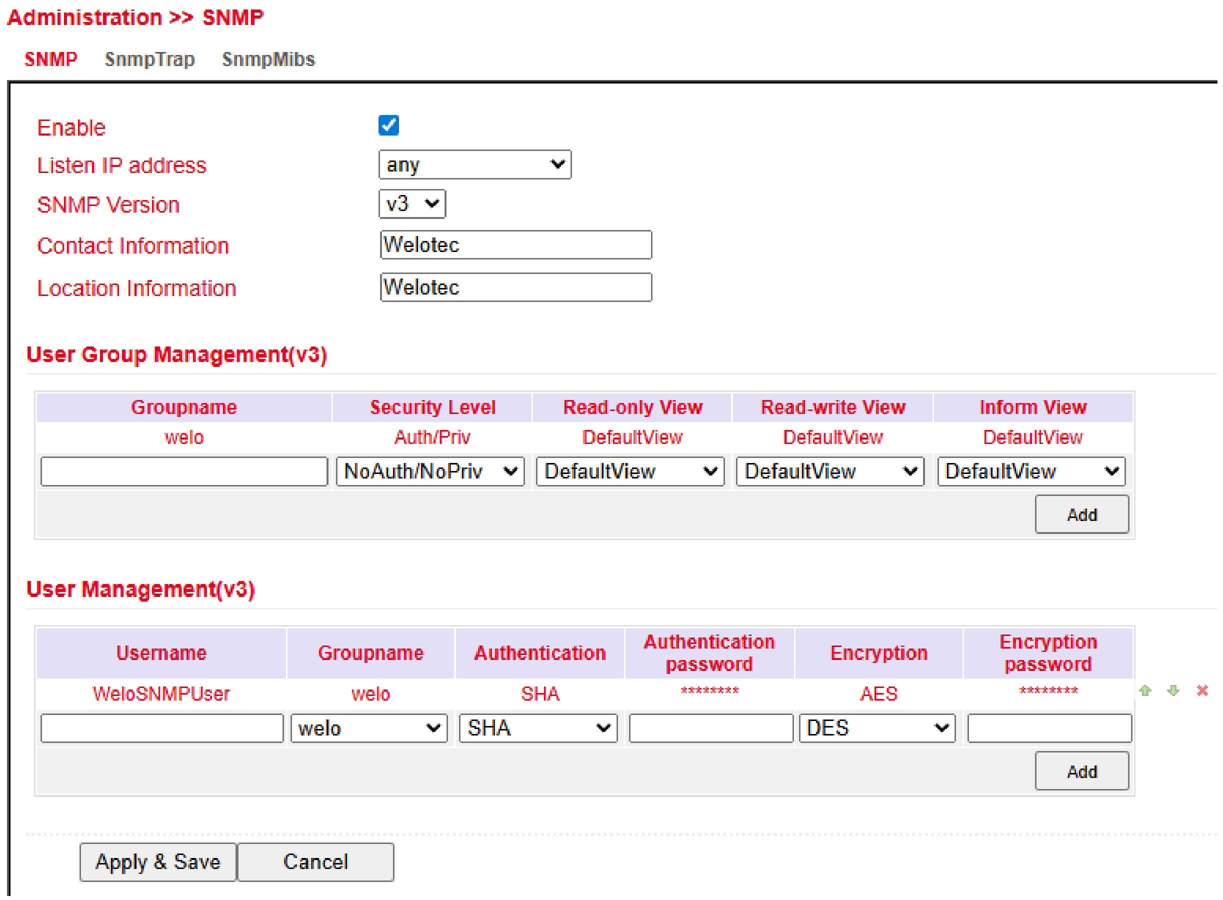


Administration >> SNMP

Please select mib file: IF-MIB

Reading SNMP MIBs with SNMPWALK

1. **Configure SNMP** on the router:



Administration >> SNMP

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

User Management(v3)

Username	Groupname	Authentication	Authentication password	Encryption	Encryption password	
WeloSNMPUser	welo	SHA	********	AES	********	↑ ↓ ✕
	welo	SHA		DES		

2. **Run SNMPWALK** on a Linux computer, for example:

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

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

3. **Download MIBs from TK804L-450**

4. **Install MIBs locally**

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


 Available MIBs:

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

5. **Start SNMPWALK using the MIBs**

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


Example Output

WELOTEC-MIB::ihOverview.1.0 = STRING: "TK804L-450"
WELOTEC-MIB::ihOverview.2.0 = STRING: "RF9151408241109"
WELOTEC-MIB::ihOverview.3.0 = STRING: "2011.09.r7903"
WELOTEC-MIB::ihOverview.4.0 = STRING: "1.0.0.r9919"
WELOTEC-MIB::ihWan3g.1.1.1.0 = INTEGER: 3
```

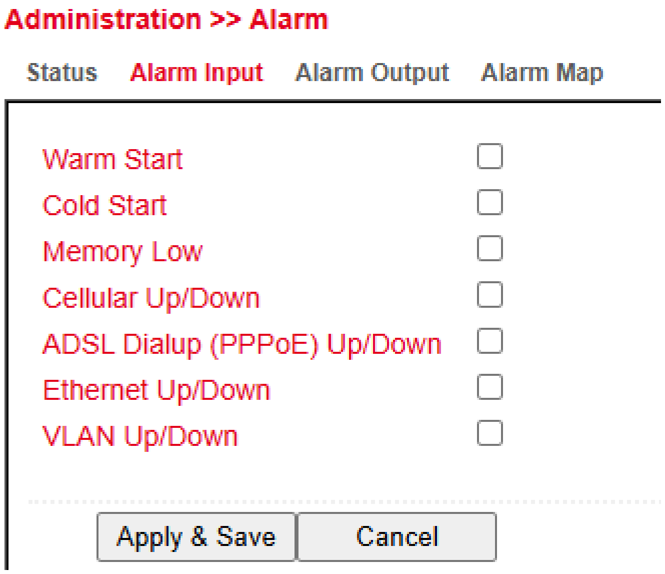
5.2.7 Alarm

Status

The **Alarm Status** page shows an overview of all triggered alarms.

Alarm Input

In the **Alarm Input** menu, you can define which alarm messages the router should output.
By setting or removing checkmarks, each alarm can be enabled or disabled.



Administration >> Alarm

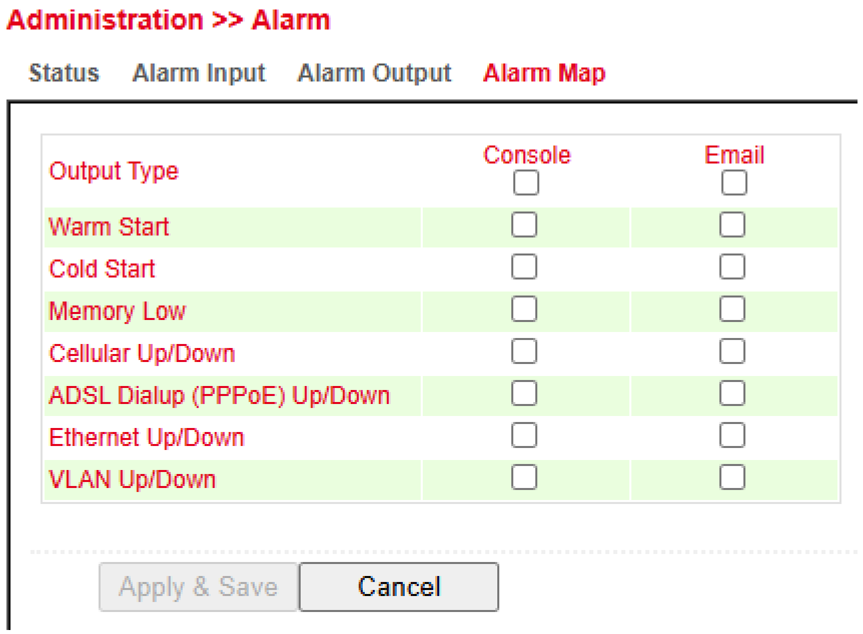
Warm Start ☐
Cold Start ☐
Memory Low ☐
Cellular Up/Down ☐
ADSL Dialup (PPPoE) Up/Down ☐
Ethernet Up/Down ☐
VLAN Up/Down ☐

Available alarm messages:

Parameter	Description
Warm Start	Warm restart/reboot of the router
Cold Start	Cold start = booting the router after power-off
Memory Low	Low memory condition
Cellular Up/Down	Mobile connection (GPRS/UMTS/LTE) connected or disconnected
ADSL Dialup (PPPoE) Up/Down	ADSL dialup connected or disconnected
Ethernet Up/Down	Ethernet interface connected or disconnected
VLAN Up/Down	VLAN connection established or disconnected

Alarm Map

In the **Alarm Map** you can define whether alerts are displayed in the web interface.
Enable or disable the feature by checking the box.



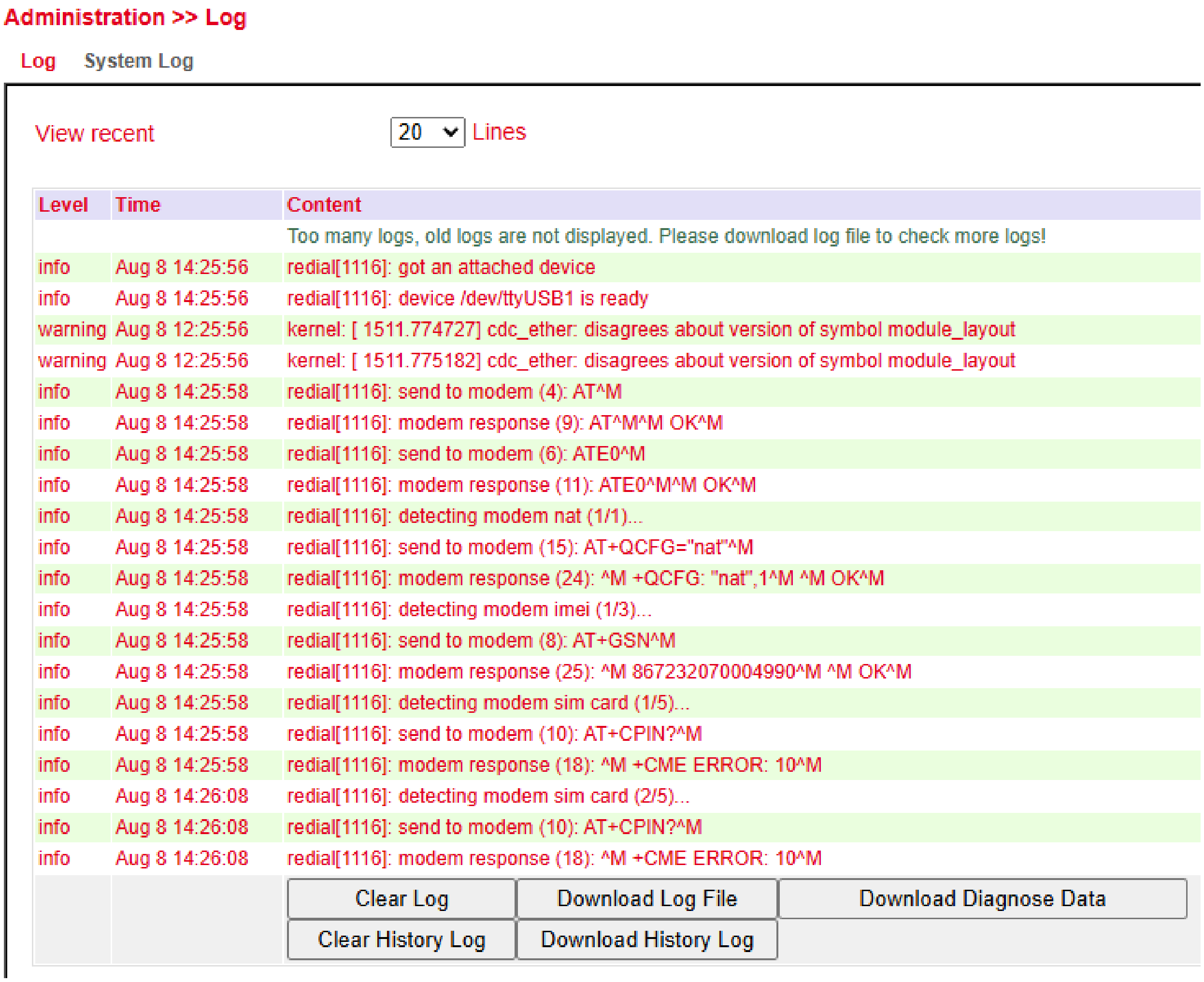
Administration >> Alarm

Output Type	Console □	Email □
Warm Start	□	□
Cold Start	□	□
Memory Low	□	□
Cellular Up/Down	□	□
ADSL Dialup (PPPoE) Up/Down	□	□
Ethernet Up/Down	□	□
VLAN Up/Down	□	□

5.2.8 Log

The **Log** menu displays the current router messages.
It contains information about:

- Network status
- Operational status
- Configuration changes
- ISP connection
- IPSec / OpenVPN status
- And more



Administration >> Log

Log System Log

View recent 20 Lines

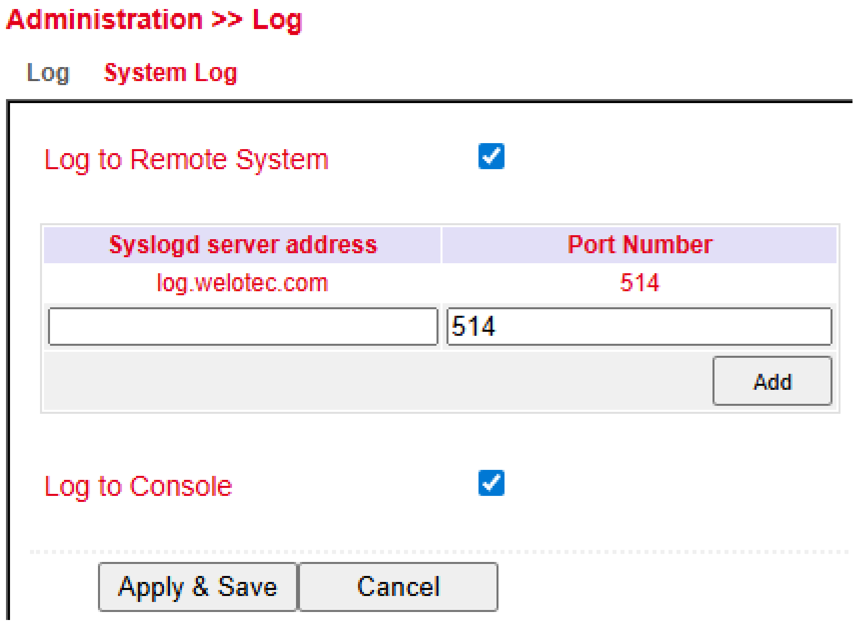
Level	Time	Content
		Too many logs, old logs are not displayed. Please download log file to check more logs!
info	Aug 8 14:25:56	redial[1116]: got an attached device
info	Aug 8 14:25:56	redial[1116]: device /dev/ttyUSB1 is ready
warning	Aug 8 12:25:56	kernel: [1511.774727] cdc_ether: disagrees about version of symbol module_layout
warning	Aug 8 12:25:56	kernel: [1511.775182] cdc_ether: disagrees about version of symbol module_layout
info	Aug 8 14:25:58	redial[1116]: send to modem (4): AT^M
info	Aug 8 14:25:58	redial[1116]: modem response (9): AT^M^M OK^M
info	Aug 8 14:25:58	redial[1116]: send to modem (6): ATE0^M
info	Aug 8 14:25:58	redial[1116]: modem response (11): ATE0^M^M OK^M
info	Aug 8 14:25:58	redial[1116]: detecting modem nat (1/1)...
info	Aug 8 14:25:58	redial[1116]: send to modem (15): AT+QCFG="nat"^M
info	Aug 8 14:25:58	redial[1116]: modem response (24): ^M +QCFG: "nat",1^M ^M OK^M
info	Aug 8 14:25:58	redial[1116]: detecting modem imei (1/3)...
info	Aug 8 14:25:58	redial[1116]: send to modem (8): AT+GSN^M
info	Aug 8 14:25:58	redial[1116]: modem response (25): ^M 867232070004990^M ^M OK^M
info	Aug 8 14:25:58	redial[1116]: detecting modem sim card (1/5)...
info	Aug 8 14:25:58	redial[1116]: send to modem (10): AT+CPIN?^M
info	Aug 8 14:25:58	redial[1116]: modem response (18): ^M +CME ERROR: 10^M
info	Aug 8 14:26:08	redial[1116]: detecting modem sim card (2/5)...
info	Aug 8 14:26:08	redial[1116]: send to modem (10): AT+CPIN?^M
info	Aug 8 14:26:08	redial[1116]: modem response (18): ^M +CME ERROR: 10^M

Available options in the log section:

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

System Log

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



Administration >> Log

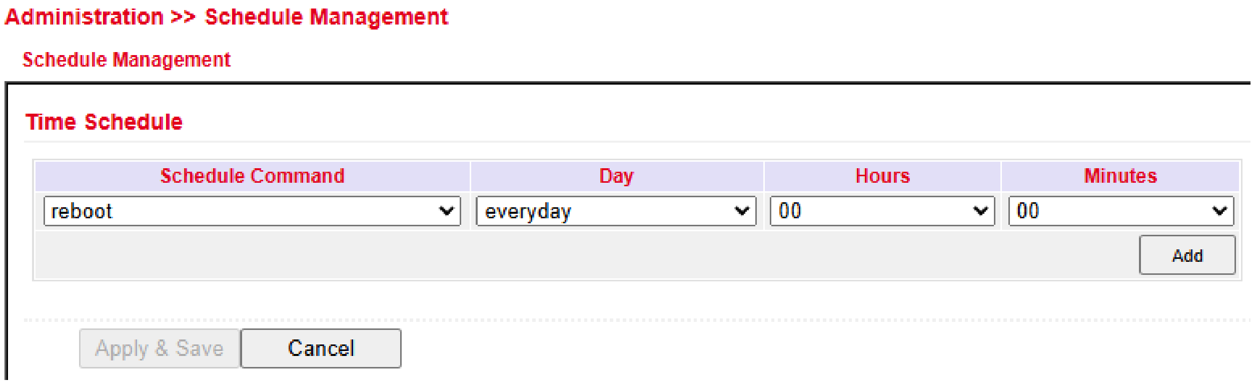
Log to Remote System ☑

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

Log to Console ☑

- **Syslog server address** → Enter the host name (FQDN) or IP address of the syslog server.
- **Port** → Default is **514** (standard syslog port).

5.2.9 Schedule Management



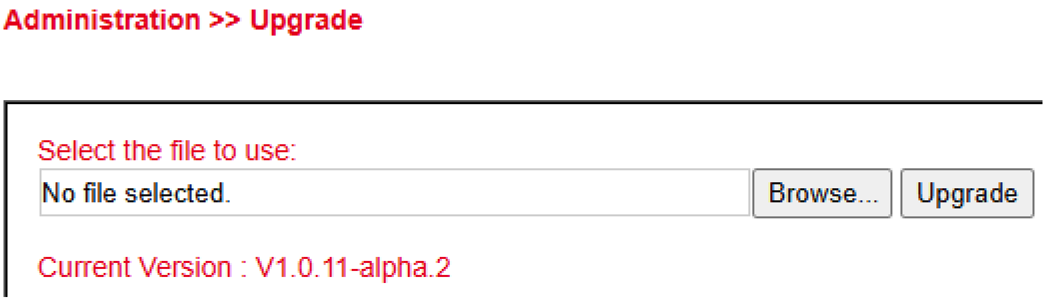
Administration >> Schedule Management

Time Schedule

Schedule Command	Day	Hours	Minutes
reboot	everyday	00	00

5.2.10 Upgrade

Firmware updates can be performed in the **Upgrade** menu.
Firmware updates may include **new features** or **bug fixes**.



Administration >> Upgrade

Select the file to use:

No file selected.

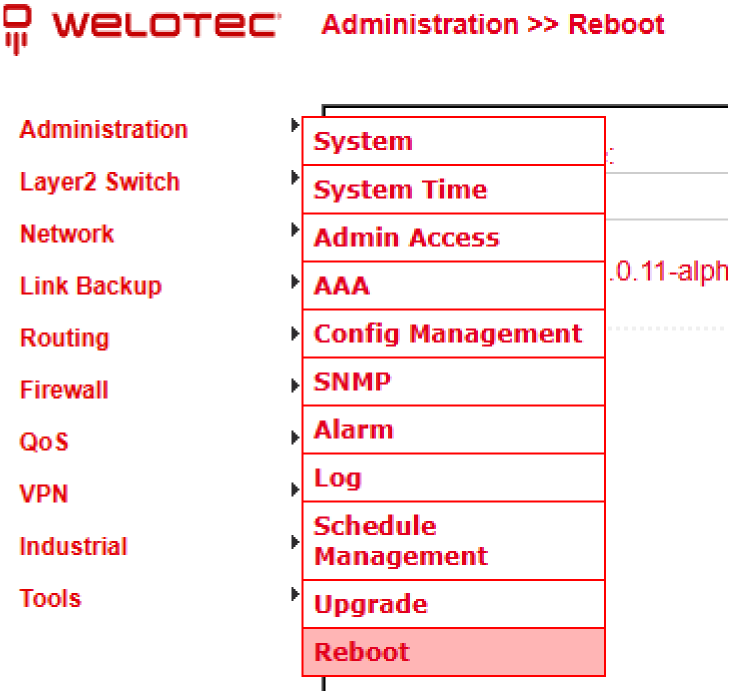
Current Version : V1.0.11-alpha.2

- The currently installed firmware is displayed under **Select the file to use**.
- Click **Browse** and select the firmware file (`.bin` or `.pkg`) previously downloaded.
- Click **Upgrade** to install the firmware.

⊠ **Note:**
If the installed version is significantly older, the **bootloader** and the **I/O board** may need to be updated separately. For details, please contact support.

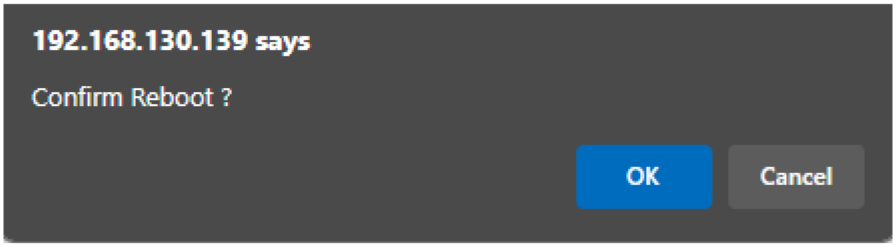
5.2.11 Reboot

The router can be restarted via **Reboot**.



⊠ - Click **OK** to confirm the reboot.

- Always **save the configuration before restarting**. Otherwise, unsaved changes will be lost.


192.168.130.139 says

Confirm Reboot ?

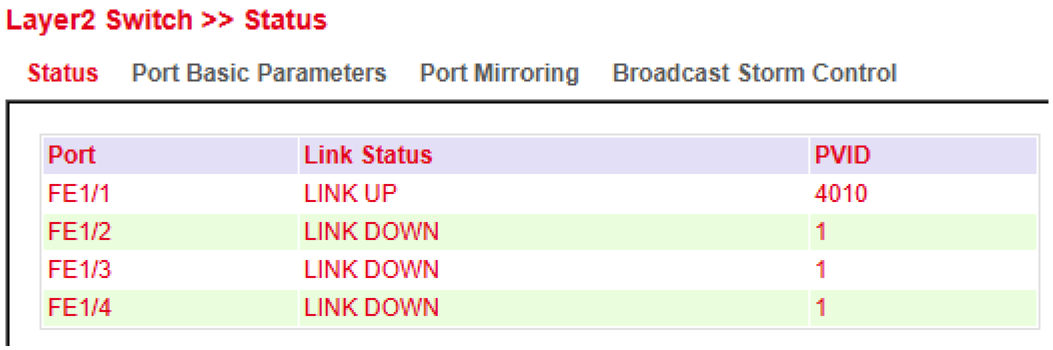
5.3 Layer2 Switch

5.3.1 Status

The **Status** section shows the **link status** and **VLAN assignment (PVID)** for each physical switch port.

- **Link Status** → Displays if a port is *active (LINK UP)* or *inactive (LINK DOWN)*
- **PVID (Port VLAN ID)** → Indicates the VLAN assigned to untagged traffic on the port

This helps to quickly identify active connections and verify VLAN configuration.



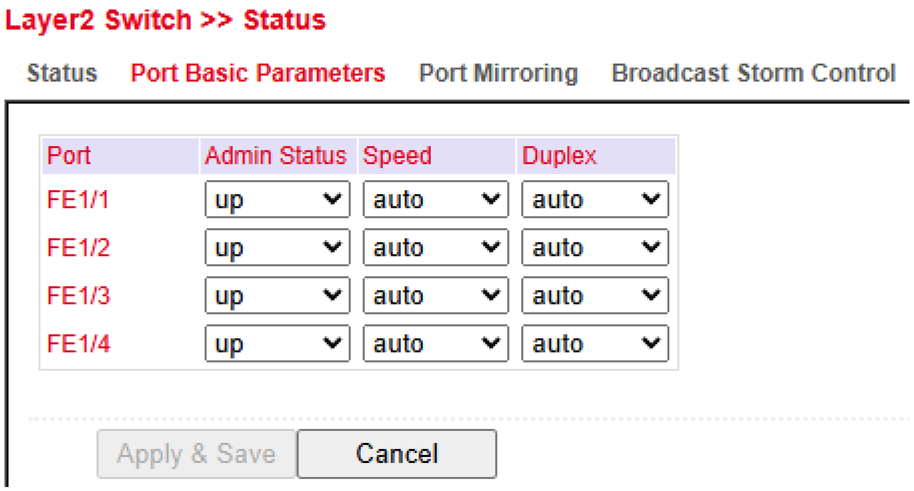
Port	Link Status	PVID
FE1/1	LINK UP	4010
FE1/2	LINK DOWN	1
FE1/3	LINK DOWN	1
FE1/4	LINK DOWN	1

Port Basic Parameters

In **Port Basic Parameters**, you can configure each port with:

- **Admin Status** → Enable/disable the port (up or down)
- **Speed** → Auto-negotiation or fixed speed
- **Duplex** → Auto, Full, or Half duplex

These settings allow performance optimization and device compatibility management.



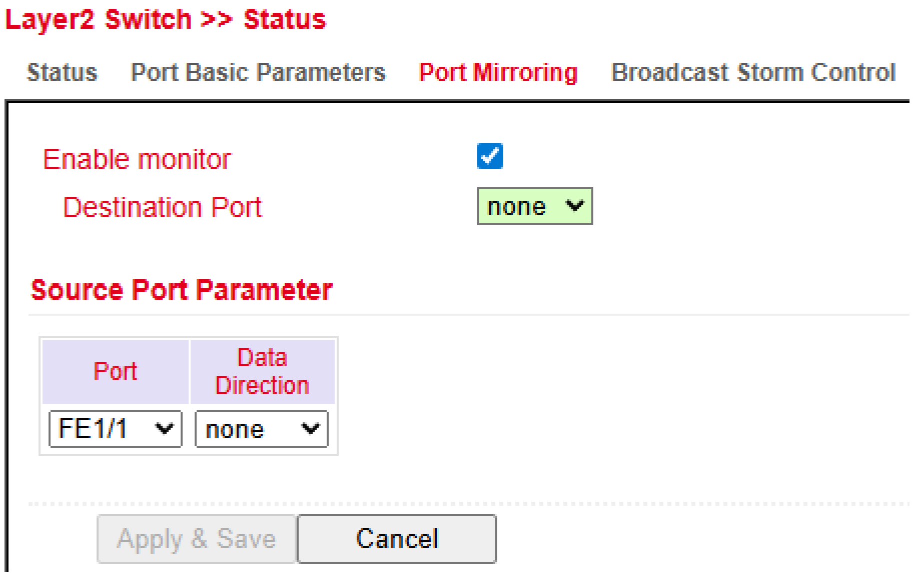
Port	Admin Status	Speed	Duplex
FE1/1	up	auto	auto
FE1/2	up	auto	auto
FE1/3	up	auto	auto
FE1/4	up	auto	auto

Port Mirroring

Port Mirroring allows monitoring of network traffic by copying packets from one or more source ports to a destination port.

- **Enable Monitor** → Activates mirroring
- **Destination Port** → Port to which mirrored traffic is sent (e.g., analysis tool)
- **Source Port Parameters**:
  - **Port** → The monitored port
  - **Data Direction** → Ingress, Egress, or Both

This feature is used for **diagnostics**, **intrusion detection**, or **performance analysis**.



Layer2 Switch >> Status

Enable monitor ☑

Destination Port: none

Source Port Parameter

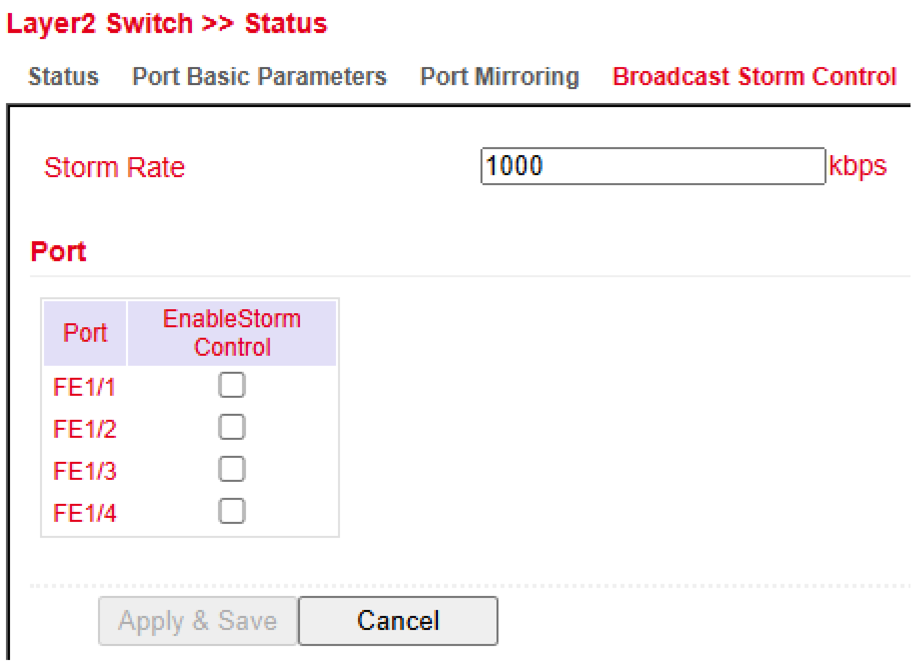
Port	Data Direction
FE1/1	none

Broadcast Storm Control

The **Broadcast Storm Control** feature allows administrators to limit the rate of broadcast traffic per port to prevent network flooding.

- **Storm Rate** → Sets the maximum allowed broadcast traffic rate (in kbps).
- **Enable Storm Control** → Can be enabled individually for each port.

Activating this feature on selected ports helps maintain network stability during broadcast storms caused by misconfigured devices or loops.



Layer2 Switch >> Status

Storm Rate 1000 kbps

Port

Port	EnableStorm Control
FE1/1	□
FE1/2	□
FE1/3	□
FE1/4	□

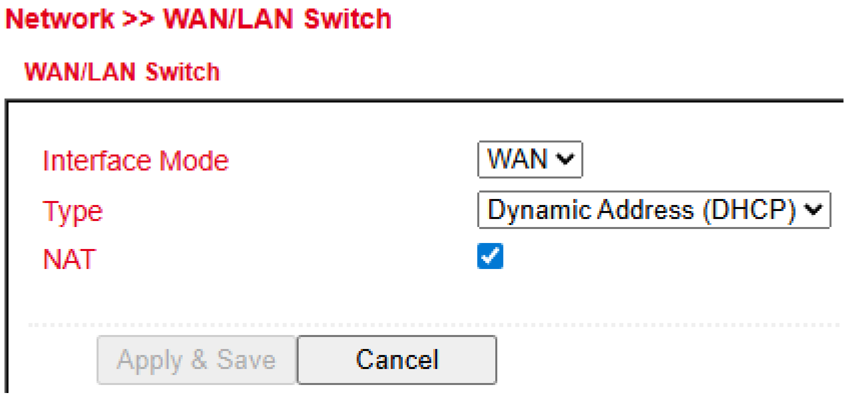
5.4 Network

5.4.1 WAN/LAN Switch

The **WAN/LAN Switch** section defines the role and addressing behavior of the network interface.

- **Interface Mode** → Select whether the interface operates as **WAN** or **LAN**.
- **Type** → Defines the IP configuration mode:
  - **Dynamic Address (DHCP)** → Automatically obtains IP settings from a DHCP server.
  - **Static Address** → Manual configuration (not shown in image but typically supported).
- **NAT (Network Address Translation)** → When enabled, private IP addresses are translated to a public IP for Internet access.

This configuration is essential for defining how the device integrates into the network and whether it routes traffic between private and public networks.



Network >> WAN/LAN Switch

WAN/LAN Switch

Interface Mode: WAN

Type: Dynamic Address (DHCP)

NAT: ☑

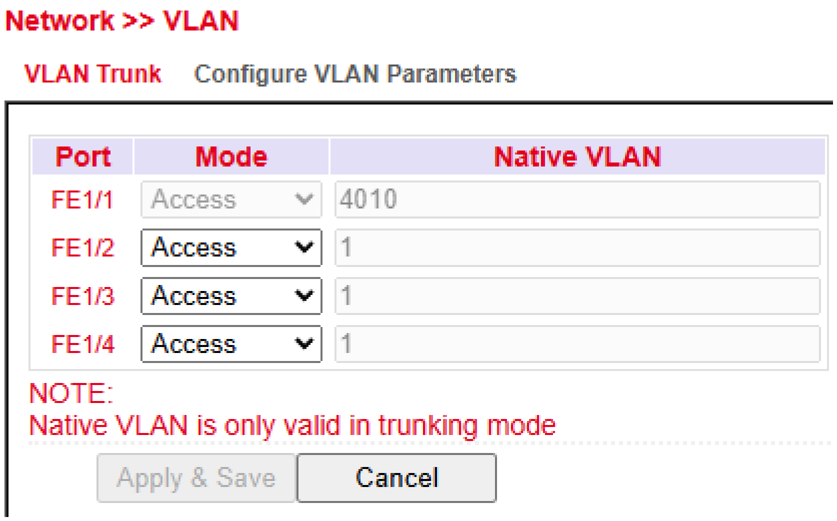
5.4.2 VLAN

VLAN Trunk

The **VLAN Trunk** configuration assigns VLAN modes and native VLANs to individual ports.

- **Port** → The physical Ethernet interface.
- **Mode** →
  - **Access** → Port belongs to a single VLAN.
  - **Trunk** → Port carries traffic for multiple VLANs (not shown in image but typically supported).
- **Native VLAN** → Only valid when the port is in *Trunk* mode; defines the VLAN for untagged traffic.

⊠ **Note:** Native VLAN settings apply only when the port operates in **Trunk mode**.
This setting is critical for managing VLAN tags on networks with VLAN-aware devices.



Network >> VLAN

Port	Mode	Native VLAN
FE1/1	Access	4010
FE1/2	Access	1
FE1/3	Access	1
FE1/4	Access	1

NOTE:
Native VLAN is only valid in trunking mode

Configure VLAN Parameters

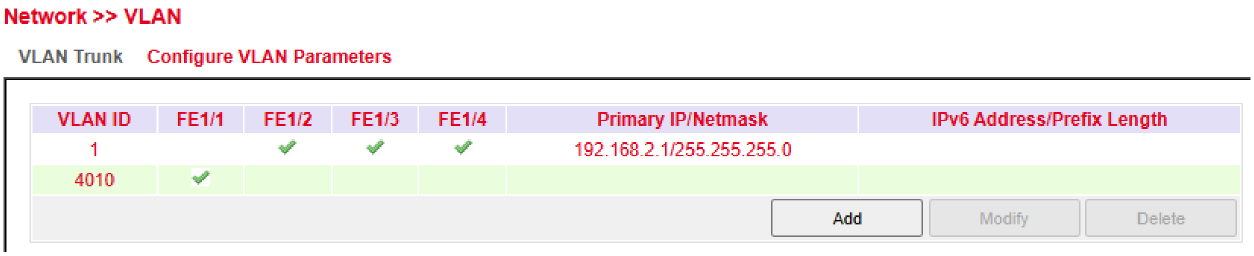
In this section you can define VLAN IDs, assign them to ports, and configure IP addressing for VLAN interfaces.

- **VLAN ID** → Identifier for the VLAN (e.g., 1, 4010).
- **Port Membership** → Assigns ports to the VLAN.
- **Primary IP / Netmask** → Layer3 IP configuration for management or routing.
- **IPv6 Address / Prefix Length** → Optional IPv6 configuration (empty in example).

Available Actions:

- **Add** → Create a new VLAN.
- **Modify** → Change VLAN settings.
- **Delete** → Remove an existing VLAN.

This configuration is essential for **network segmentation**, **traffic isolation**, and improving **security and performance**.



Network >> VLAN

VLAN Trunk   Configure VLAN Parameters

VLAN ID	FE1/1	FE1/2	FE1/3	FE1/4	Primary IP/Netmask	IPv6 Address/Prefix Length
1		✓	✓	✓	192.168.2.1/255.255.255.0	
4010	✓					

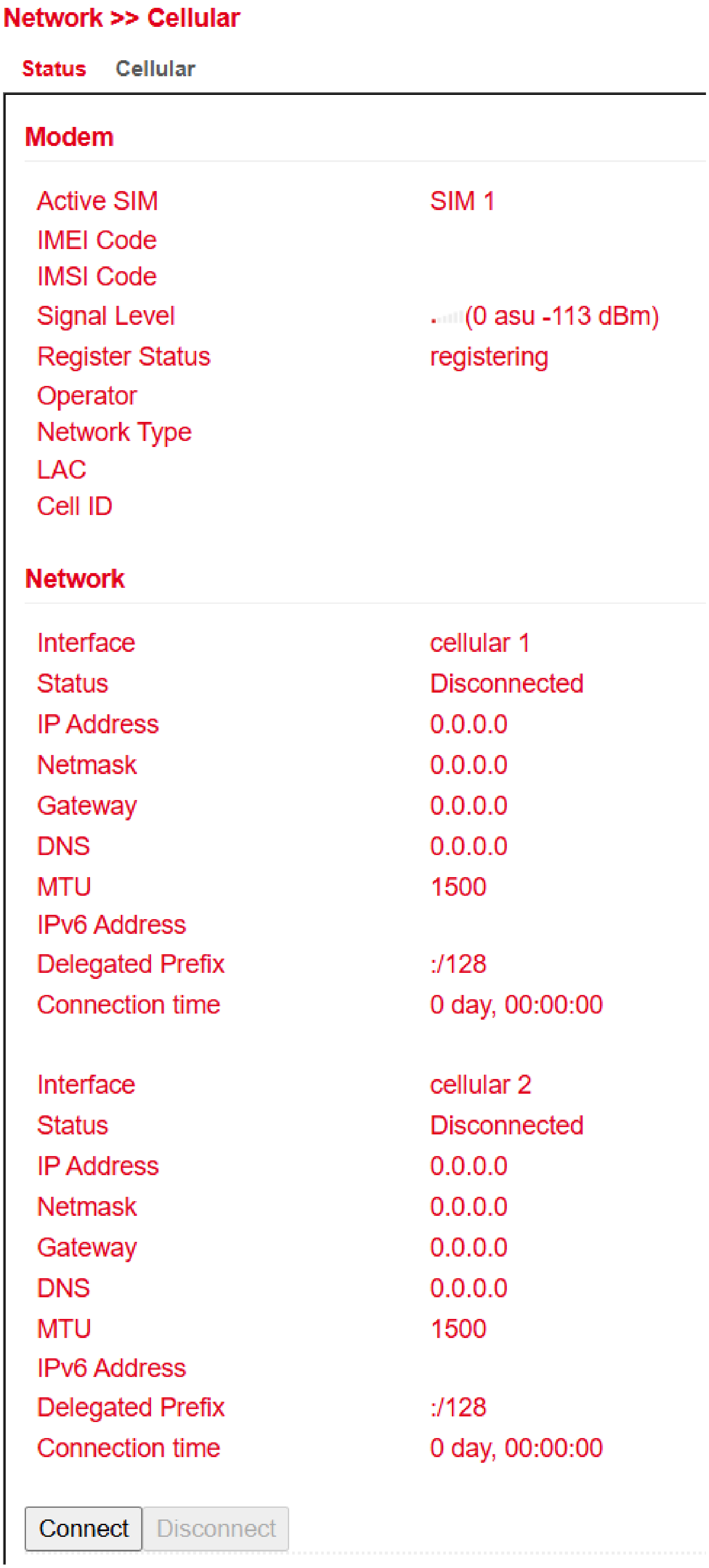
5.4.3 Cellular

The **Cellular** interface provides mobile communication access.
With an inserted SIM card, the router can connect to the Internet via **GPRS, EDGE, UMTS, or LTE**, depending on the model.

Status

Under **Status** you find an overview of the current connection state (**Connected** / **Disconnected**).

- **Network Type** → shown in the Status tab
- **IP Address** → shown in the Network section
- **Modem area** → shows signal level, RSRP, and RSRQ



Network >> Cellular

Modem

Active SIM	SIM 1
IMEI Code	
IMSI Code	
Signal Level	(0 asu -113 dBm)
Register Status	registering
Operator	
Network Type	
LAC	
Cell ID	

Network

Interface	cellular 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	1500
IPv6 Address	
Delegated Prefix	:/128
Connection time	0 day, 00:00:00
Interface	cellular 2
Status	Disconnected
IP Address	0.0.0.0
Netmask	0.0.0.0
Gateway	0.0.0.0
DNS	0.0.0.0
MTU	1500
IPv6 Address	
Delegated Prefix	:/128
Connection time	0 day, 00:00:00

☒ In some cases, the router may not receive a valid DNS server from the provider.
Check the DNS entry:

- If empty → no DNS assigned
- If unusual (e.g., `10.74.210.210` → Telekom internal DNS), adjust settings accordingly.

RSRP (Reference Signal Received Power)

RSRP is one of the most important indicators for assessing LTE reception quality.
It is measured directly by the device and used to determine the strongest cell.

RSRP (dBm)	Grade	Comment
-50 to -65	1 (very good)	Excellent reception – perfect
-65 to -80	2 (good)	Good reception – sufficient
-80 to -95	3 (satisfactory)	Stable, but not optimal
-95 to -105	4 (sufficient)	Acceptable, but speed restrictions / occasional drops possible
-110 to -125	5 (poor)	Very poor – connection barely possible
-125 to -140	6 (insufficient)	Extremely poor – likely no connection

RSRQ (Reference Signal Received Quality)

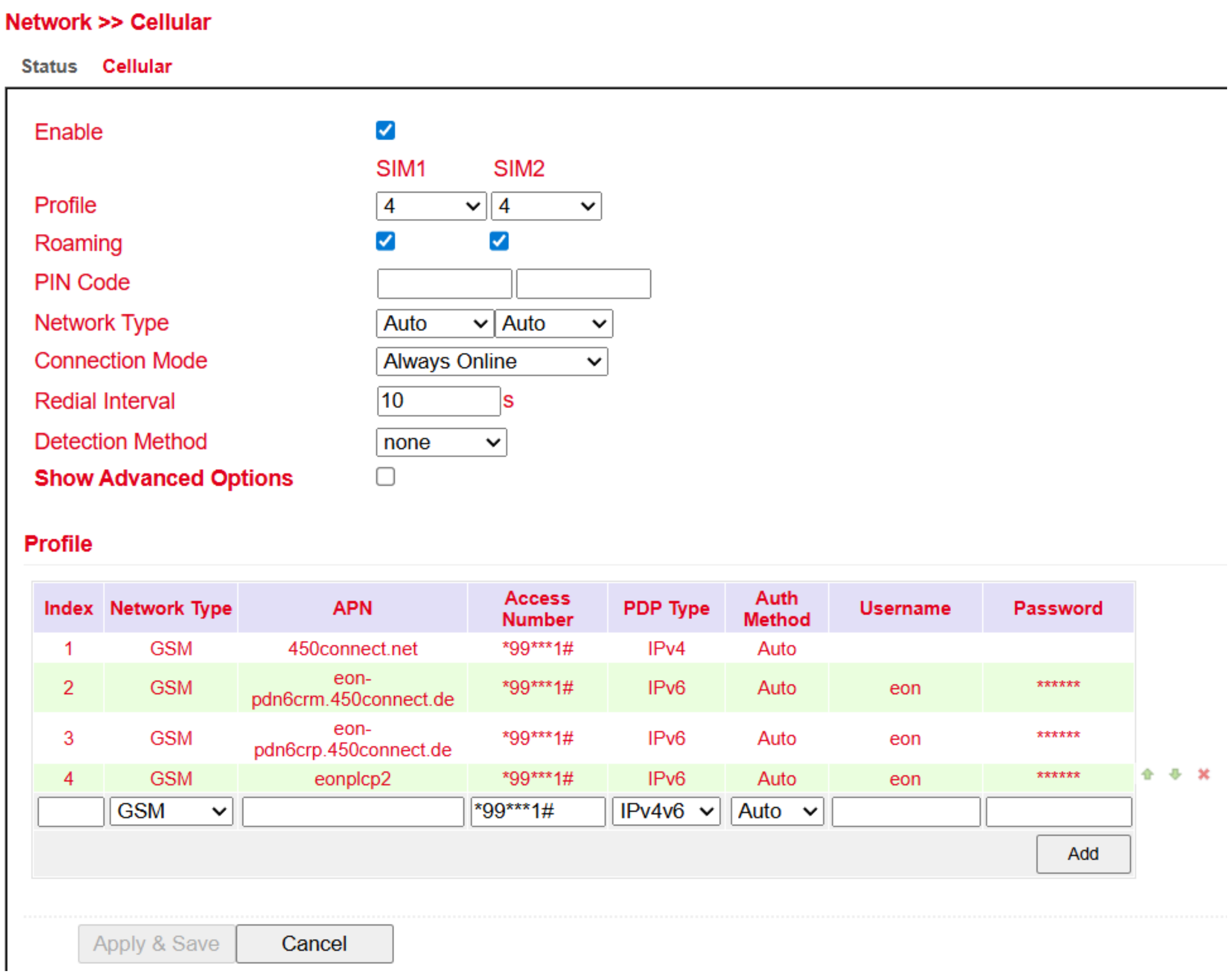
RSRQ is a calculated ratio based on **RSRP** and **RSSI**, and is crucial for evaluating LTE quality.
Together with RSRP, it helps optimize antenna alignment for stationary use.

RSRQ (dB)	Grade	Comment
-3	1 (very good)	Optimal, no interference
-4 … -5	2 (good)	Minor interference, no impact
-6 … -8	3 (satisfactory)	Noticeable influence, but still stable
-9 … -11	4 (sufficient)	Significant interference, connection affected
-12 … -15	5 (poor)	Heavy interference, unstable connection
-16 … -20	6 (insufficient)	Severe interference, no usable connection

☒ Many providers assign **private IP addresses** that are not directly routable from the Internet.
A successful or failed ping does **not** always indicate Internet reachability.

Cellular Configuration

Under **Network > Cellular > Cellular** you can configure mobile network access.



Network >> Cellular

Status Cellular

Enable	☑	
	SIM1	SIM2
Profile	4	4
Roaming	☑	☑
PIN Code		
Network Type	Auto	Auto
Connection Mode	Always Online	
Redial Interval	10 s	
Detection Method	none	
Show Advanced Options	☐	

Profile

Index	Network Type	APN	Access Number	PDP Type	Auth Method	Username	Password
1	GSM	450connect.net	*99***1#	IPv4	Auto		
2	GSM	eon-pdn6crm.450connect.de	*99***1#	IPv6	Auto	eon	******
3	GSM	eon-pdn6crp.450connect.de	*99***1#	IPv6	Auto	eon	******
4	GSM	eonplcp2	*99***1#	IPv6	Auto	eon	******
	GSM		*99***1#	IPv4v6	Auto		

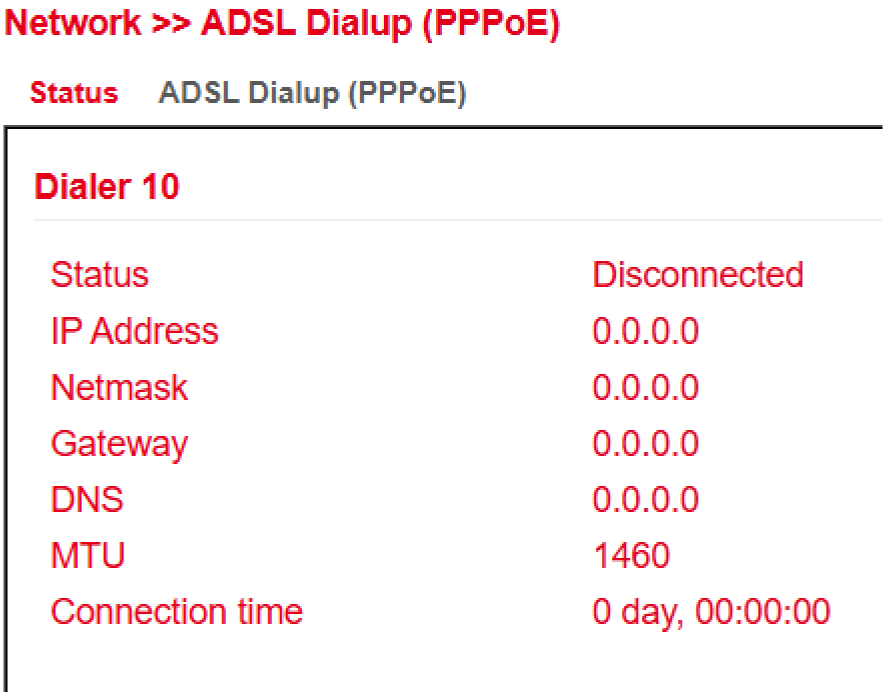
Add

Apply & Save Cancel

Parameter	Description	Default
Enable	Enable or disable the cellular interface	Enabled
Profile	APN profile for SIM 1 and SIM 2	Auto / Auto
Roaming	Enable or disable roaming. Depends on provider – roaming may occur despite being disabled.	Enabled / Enabled
PIN Code	SIM card PIN. Enter before inserting SIM card.	Blank / Blank
Network Type	Auto / 2G (GPRS, EDGE) / 3G (UMTS, HSDPA, HSUPA, HSPA+) / 4G (LTE)	Auto
Connection Mode	Always online or on-demand connection	Always Online
Redial Interval	Interval for redialing	10 seconds
Detection Method	How to check Internet connectivity (e.g., ICMP ping, DNS, HTTP)	ICMP (Ping)
Show Advanced Options	Displays additional settings when enabled	Disabled

5.4.4 ADSL Dialup (PPPoE)

Status



Network >> ADSL Dialup (PPPoE)

Dialer 10

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

The **TK804L-450 routers** do **not** have a built-in ADSL modem.
For ADSL dial-up, connect an **external ADSL modem** to the WAN port.
⊠ Ensure the DSL modem supports **modern IP technologies** for proper operation.

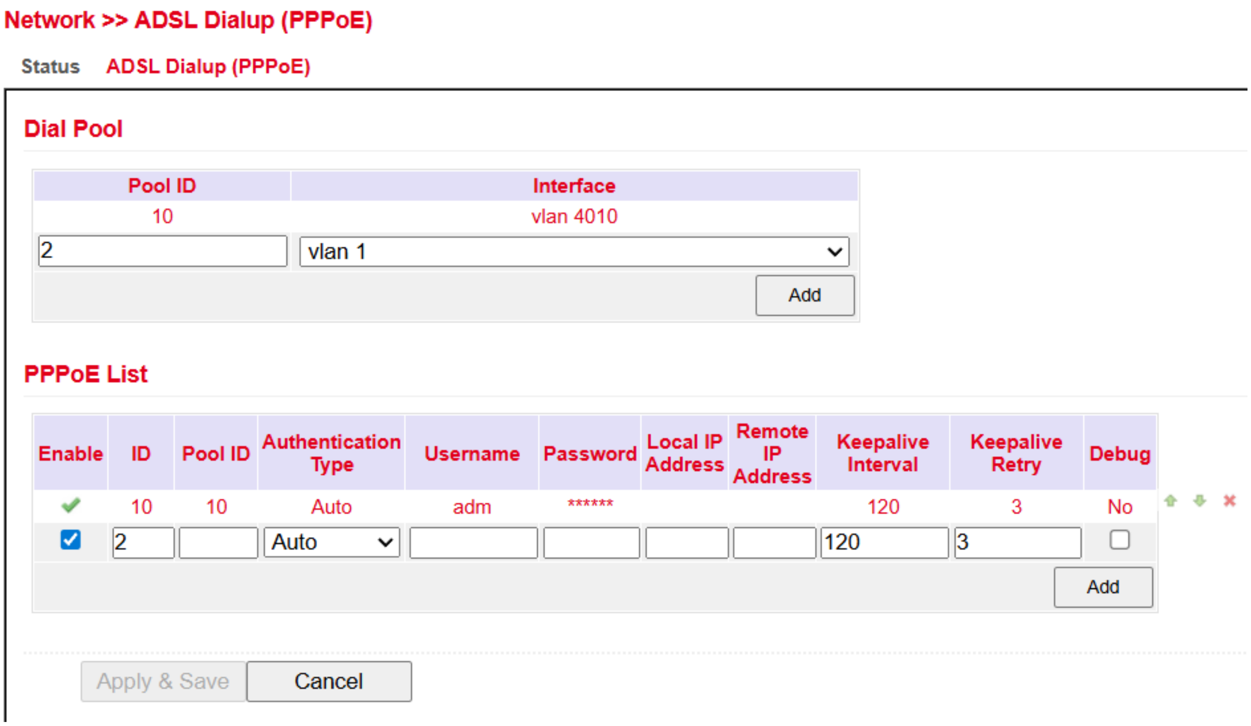
ADSL Dialup (PPPoE)

Here you can configure **DSL dial-in via PPPoE**.
The TK804L-450 does **not** have an integrated DSL modem, so an **external modem** is required.

The DSL 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+)

⊠ Ensure the modem is connected to the router before configuration.
The DSL modem should be attached to **FE 0/1** or a defined **VLAN port**.



Dial Pool

Pool ID	Interface
10	vlan 4010
2	vlan 1

PPPoE List

Enable	ID	Pool ID	Authentication Type	Username	Password	Local IP Address	Remote IP Address	Keepalive Interval	Keepalive Retry	Debug
✓	10	10	Auto	adm	******			120	3	No
☑	2		Auto					120	3	☐

Dial Pool

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

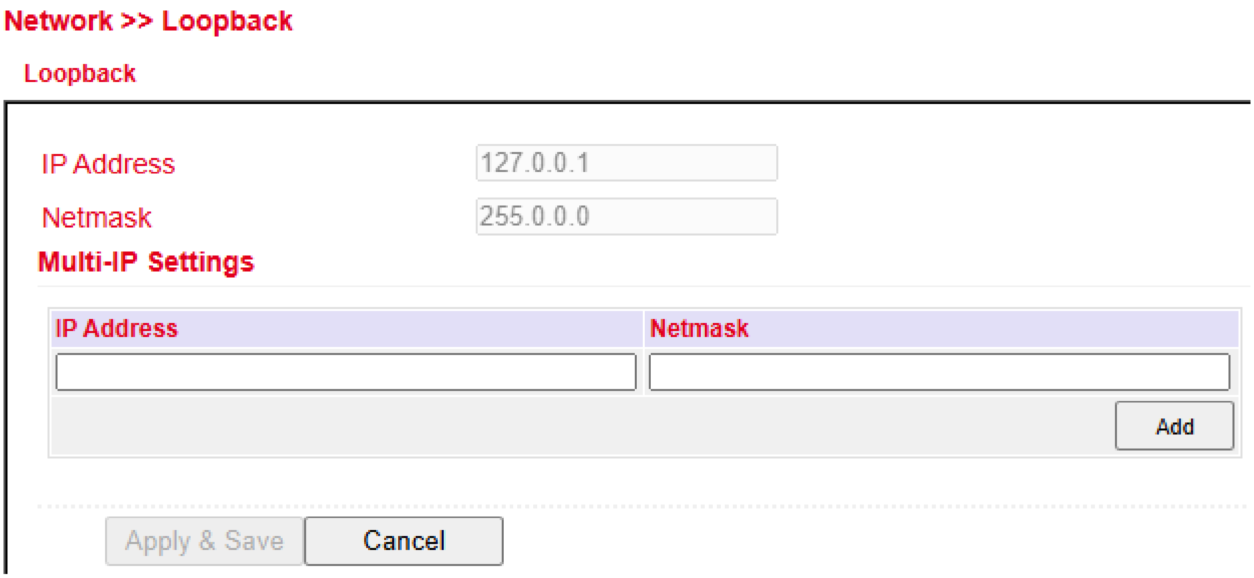
PPPoE List

Parameter	Description
Enable	Enable or disable the PPPoE entry
ID	Unique identifier for the entry
Pool ID	Pool ID created under *Dial Pool* for the interface used for the connection
Authentication Type	Auto, PAP, CHAP (usually set to Auto)
Username	Username provided by your ISP
Password	Password provided by your ISP
Local IP Address	Local IP address
Remote IP Address	IP address of the remote device (modem)
Keepalive Interval	Time interval for connection checks
Keepalive Retry	Number of retries if a connection check fails
Debug	Enables detailed logging

5.4.5 Loopback

Loopback Configuration

Under **Network > Loopback** you can configure additional loopback IP addresses.
⊠ The default address `127.0.0.1` cannot be modified.



Network >> Loopback

Loopback

IP Address: 127.0.0.1
Netmask: 255.0.0.0

Multi-IP Settings

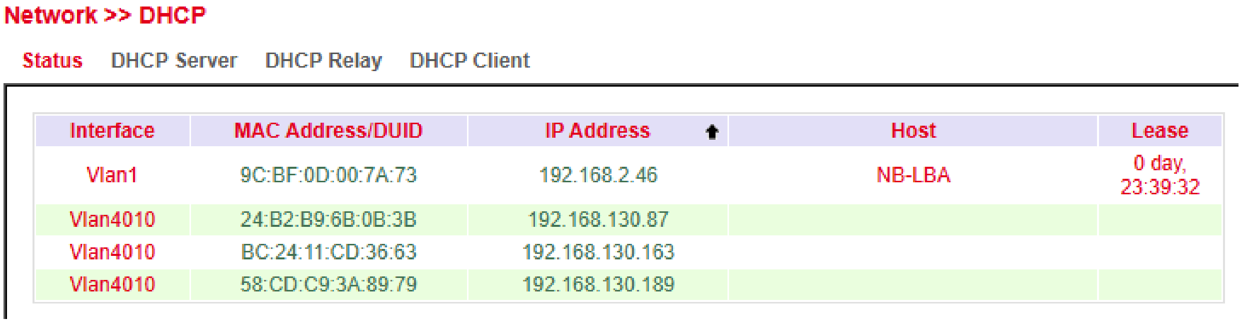
IP Address	Netmask

5.4.6 DHCP

Dynamic Host Configuration Protocol (DHCP) automatically assigns network configuration to clients.

Status

Under **Services > DHCP > Status** you can view which clients are currently connected to the router and on which interface.



Network >> DHCP

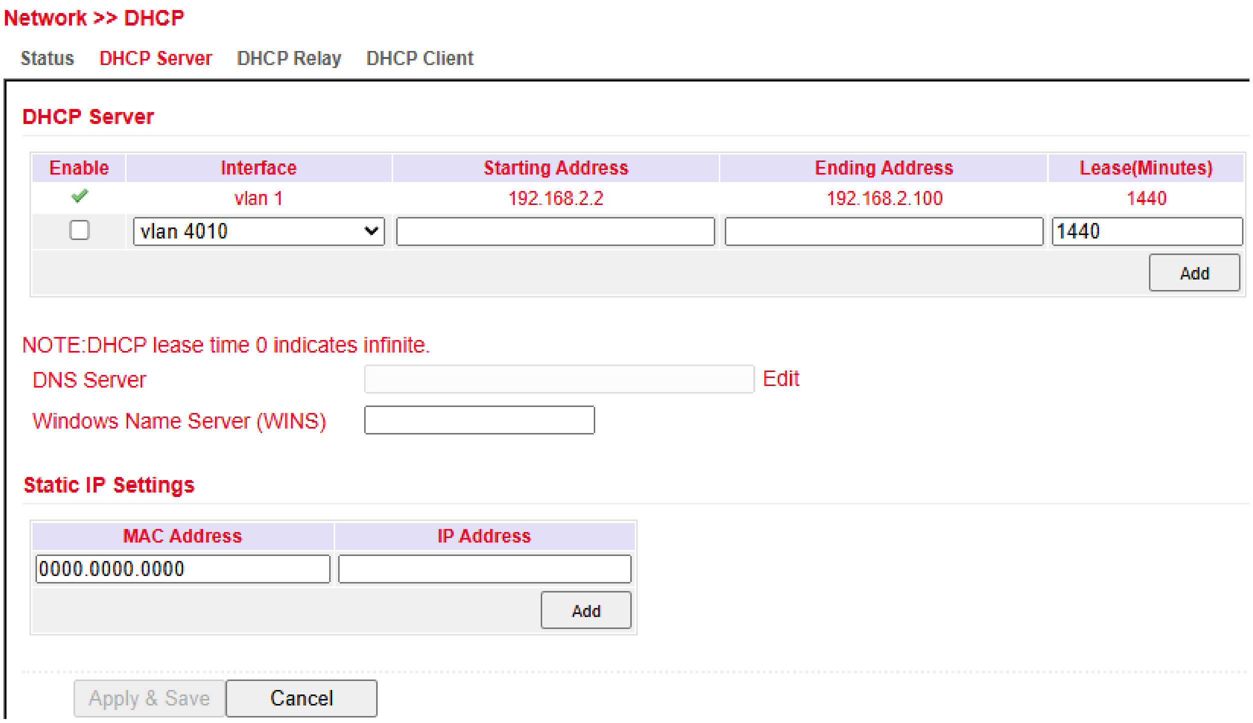
Interface	MAC Address/DUID	IP Address ⬆	Host	Lease
Vlan1	9C:BF:0D:00:7A:73	192.168.2.46	NB-LBA	0 day, 23:39:32
Vlan4010	24:B2:B9:6B:0B:3B	192.168.130.87		
Vlan4010	BC:24:11:CD:36:63	192.168.130.163		
Vlan4010	58:CD:C9:3A:89:79	192.168.130.189		

DHCP Server

Under **Services > DHCP > DHCP Server** you can configure the DHCP server:

- Select the interface
- Define start and end IP address
- Configure lease time

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



Network >> DHCP

DHCP Server

Enable	Interface	Starting Address	Ending Address	Lease(Minutes)
✓	vlan 1	192.168.2.2	192.168.2.100	1440
□	vlan 4010			1440

NOTE:DHCP lease time 0 indicates infinite.

DNS Server Edit

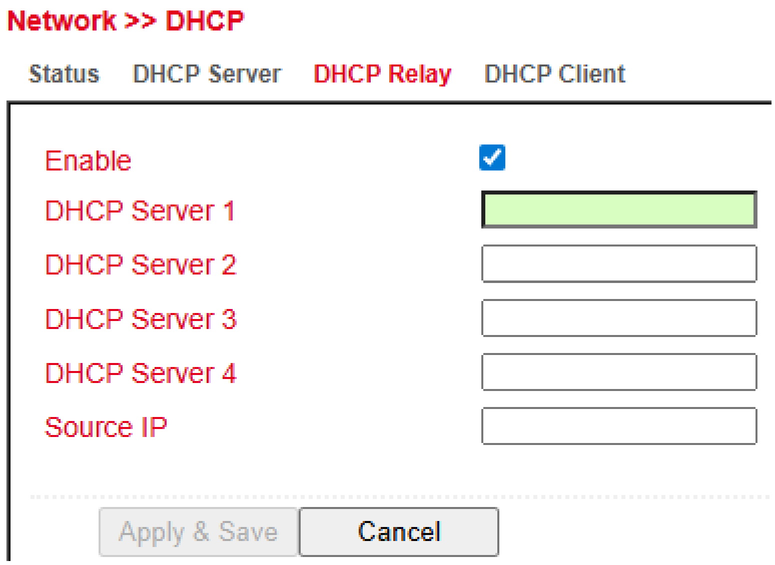
Windows Name Server (WINS)

Static IP Settings

MAC Address	IP Address
0000.0000.0000	

DHCP Relay

Under **Services > DHCP > DHCP Relay** you can specify **remote DHCP servers**, which then provide IP management for connected networks.
Enable this feature with the **Enable** checkbox.



Network >> DHCP

Enable ☑

DHCP Server 1

DHCP Server 2

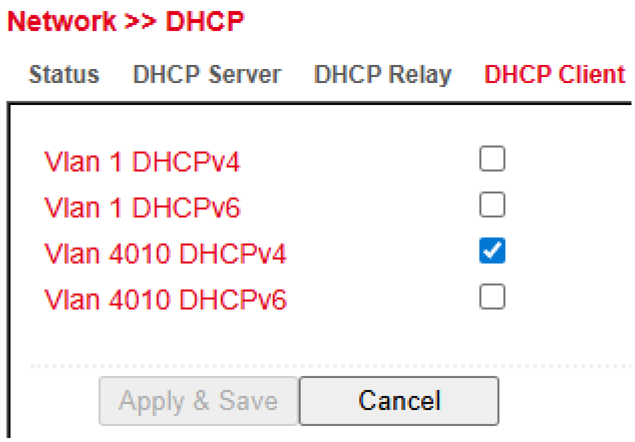
DHCP Server 3

DHCP Server 4

Source IP

DHCP Client

Under **Services > DHCP > DHCP Client**, the router itself can obtain an IP address from a DHCP server.
Select the interface to be configured via DHCP (varies by router model).



Vlan 1 DHCPv4 □
Vlan 1 DHCPv6 □
Vlan 4010 DHCPv4 ☑
Vlan 4010 DHCPv6 □

5.4.7 DNS

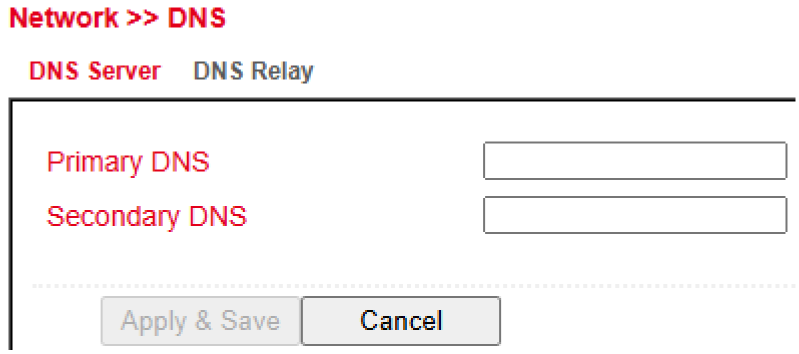
Domain Name System (DNS) is one of the most important services in IP networks.
Its main purpose is **name resolution**:

- A client queries a domain name (e.g., `welotec.com`).
- DNS resolves the domain to the corresponding IP address (e.g., `192.168.2.1`).
- The IP address allows the client to reach the correct server.

This works similar to a **telephone directory**, where a name is resolved into a number.

DNS Server

Under **Services > DNS > DNS Server** you can configure up to **two DNS servers**.
These apply to all interfaces unless a different DNS server is assigned via DHCP.

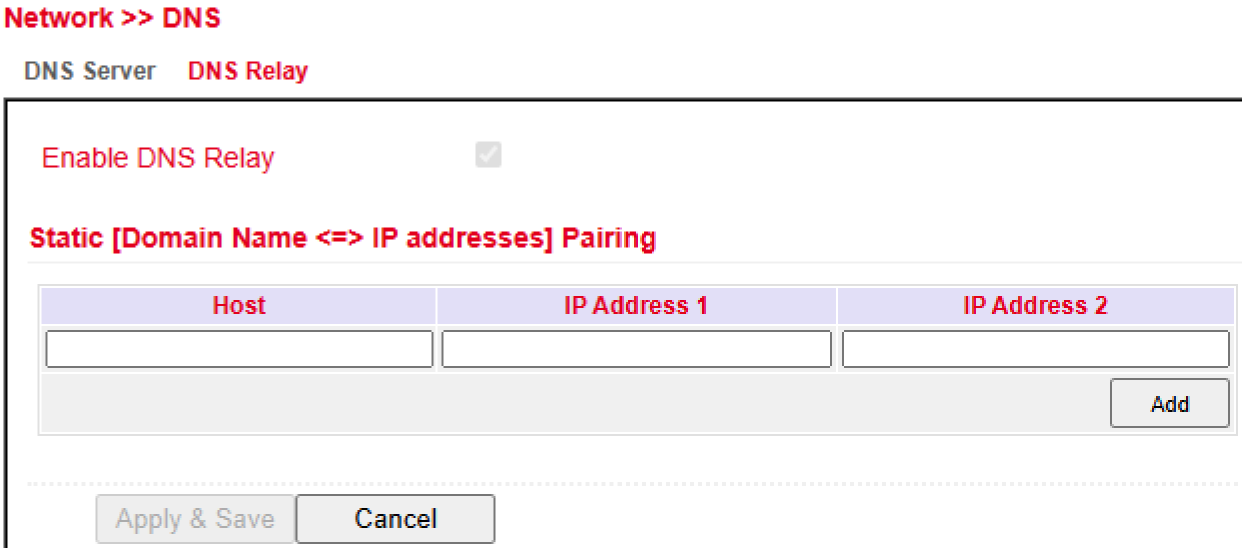


Primary DNS
Secondary DNS

DNS Relay

Under **Services** > **DNS** > **DNS Relay** you can add manual DNS resolutions.

- Click **Add** to create an entry.
- Click **Apply & Save** to confirm changes.



Enable DNS Relay ☑

Static [Domain Name <=> IP addresses] Pairing

Host	IP Address 1	IP Address 2

DDNS (Dynamic DNS)

Dynamic DNS (DDNS) updates domain entries automatically after a public IP address changes.
This ensures the device is always reachable under the same domain name, even if the public IP changes.

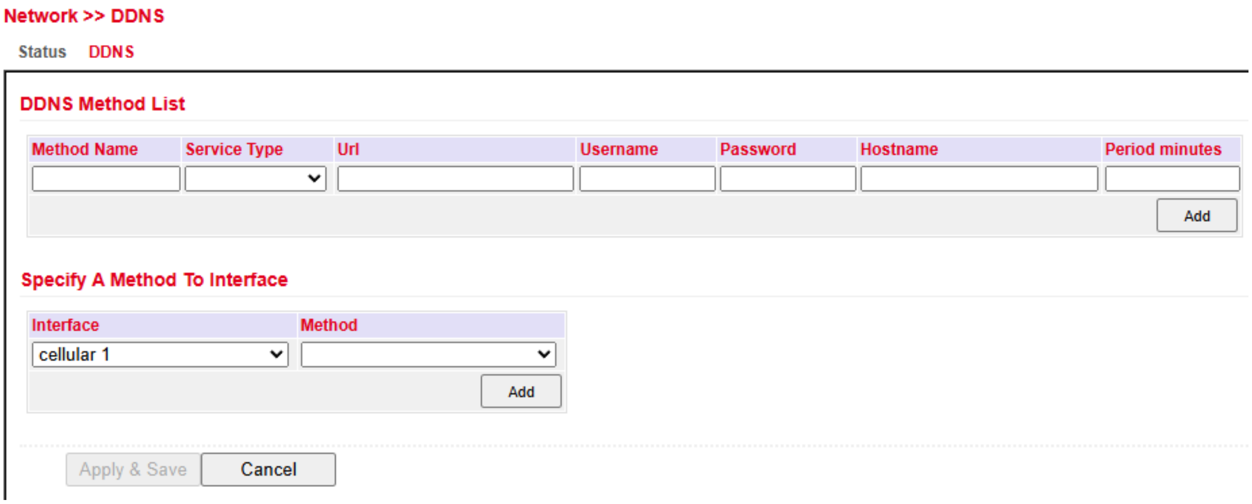
```
Example providers: DynDNS, NoIP
```

DDNS Status

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

DDNS Configuration

Under **Services > DDNS > DDNS** you can configure a new service.
⊠ A DDNS service must first be created in **DDNS Method List**, then assigned to an interface under **Specify A Method To Interface**.



Interface: cellular 1

DDNS Method List

Parameter	Description
Method Name	Freely selectable name for the service
Service Type	Predefined DDNS services available. Use **Custom** if not listed
URL	Required only for **Custom** type. Full service URL including username and password. Example (NoIP):`https://username:password@dynupdate.no-ip.com/nic/update?hostname=welotec.ddns.net&myip=@IP`
Username	Username for the DDNS provider
Password	Password for the DDNS provider
Hostname	Domain name used
Period (minutes)	Update interval, range **1–999999 minutes**

Assign Method to Interface

Parameter	Description
Interface	Router interface whose IP should be updated via DDNS
Method	DDNS service created under *DDNS Method List*

⊠ **Note:** You need an account with a DDNS provider (may be chargeable). Configure this account before use.

5.4.8 SMS

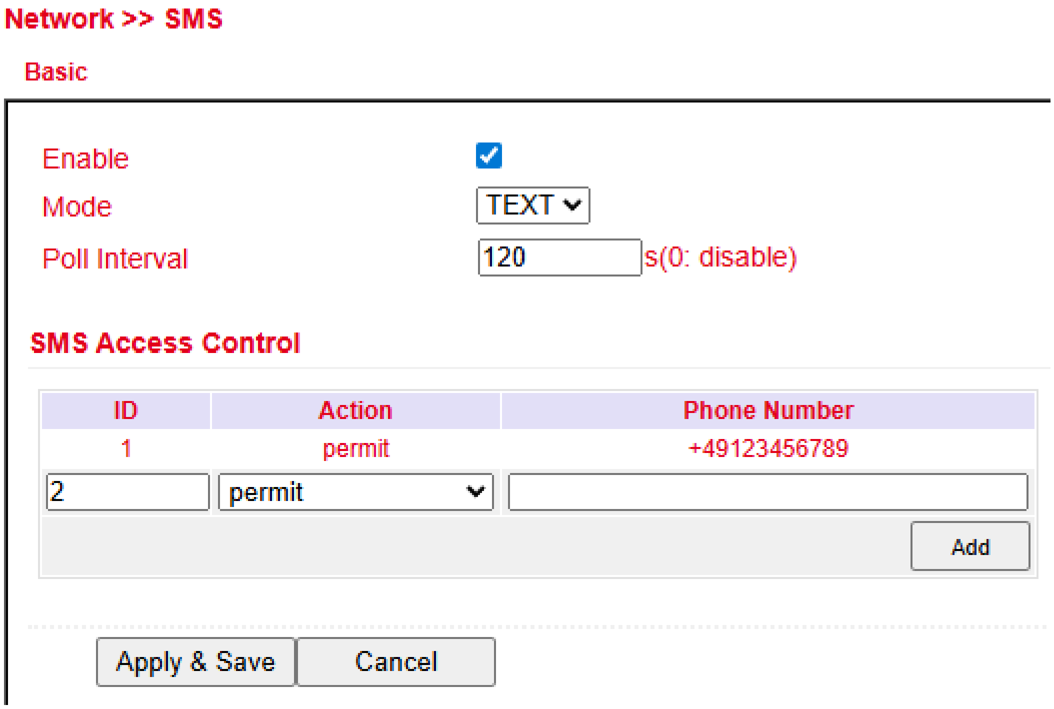
Introduction

The TK804L-450 can be controlled via **SMS commands**.
Supported actions include:

- Querying device status
- Starting/stopping dial-up
- Restarting the router

Status Query / Restart

1. Open the **Services > SMS** menu.
2. Check **Enable** to activate the feature.



Network >> SMS

Basic

Enable ☑

Mode TEXT

Poll Interval 120 s(0: disable)

SMS Access Control

ID	Action	Phone Number
1	permit	+49123456789
2	permit	

3. In **SMS Access Control**, enter phone numbers allowed to send SMS commands.
   - Format: 4917123456789 (no 0049 or +49)
   - Action: **permit**

Example:
Send SMS with text `show` → router replies with its current status.

5.5 Link Backup

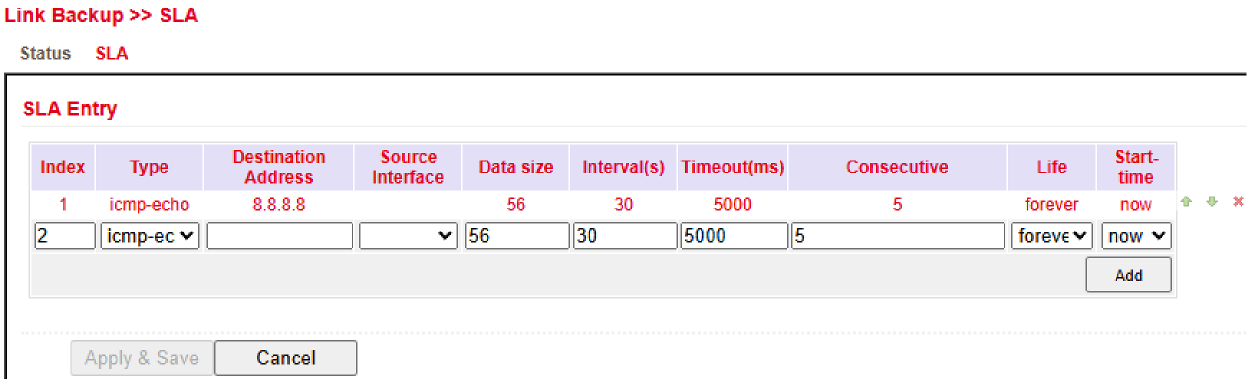
The TK804L-450 supports **dual Internet connectivity** (wired + cellular) to increase availability.

- The router regularly checks the **primary Internet connection**.
- On failure, it switches automatically to the **secondary (cellular) connection**.
- Once the primary connection is restored, the router switches back automatically.

⊠ **Prerequisite:** Cellular Internet access must be configured.
The router is preconfigured for **T-Mobile SIM cards**, so normally no additional steps are required.

5.5.1 SLA

SLA Monitoring checks the availability of peers within the network using ping tests.
Defined destinations are continuously pinged, and the line state is shown as **up** or **down**.



SLA Entry

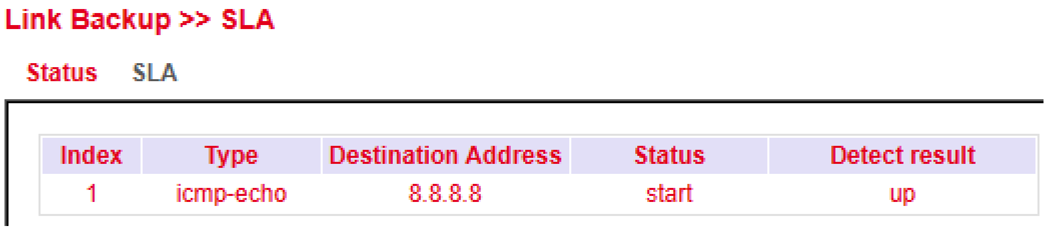
Index	Type	Destination Address	Source Interface	Data size	Interval(s)	Timeout(ms)	Consecutive	Life	Start-time
1	icmp-echo	8.8.8.8		56	30	5000	5	forever	now
2	icmp-ec			56	30	5000	5	foreve	now

Configure SLA under **Link Backup > SLA > SLA**.

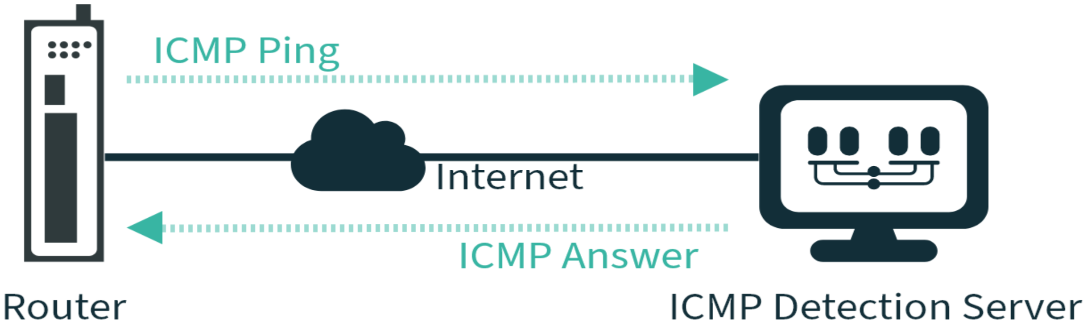
Parameter	Description
Index	Freely selectable, used to identify the entry
Type	`icmp-echo` → simple ping to check connectivity
Destination Address	Address to be pinged (should be highly available, e.g., Google DNS `8.8.8.8`)
Data size	Packet size of a ping (default: 56 bytes)
Interval (s)	Interval in seconds between pings
Timeout (ms)	Timeout for each ping
Consecutive	Number of retries if a ping fails
Life	`forever` → pings are executed continuously
Start-time	`now` → check starts immediately

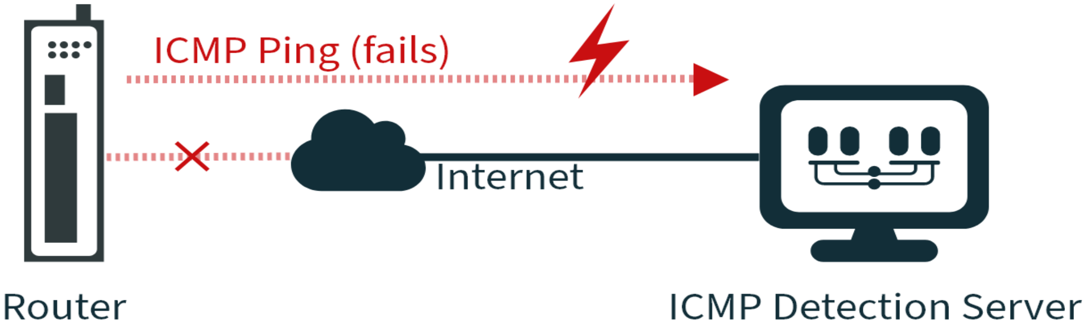
Status

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



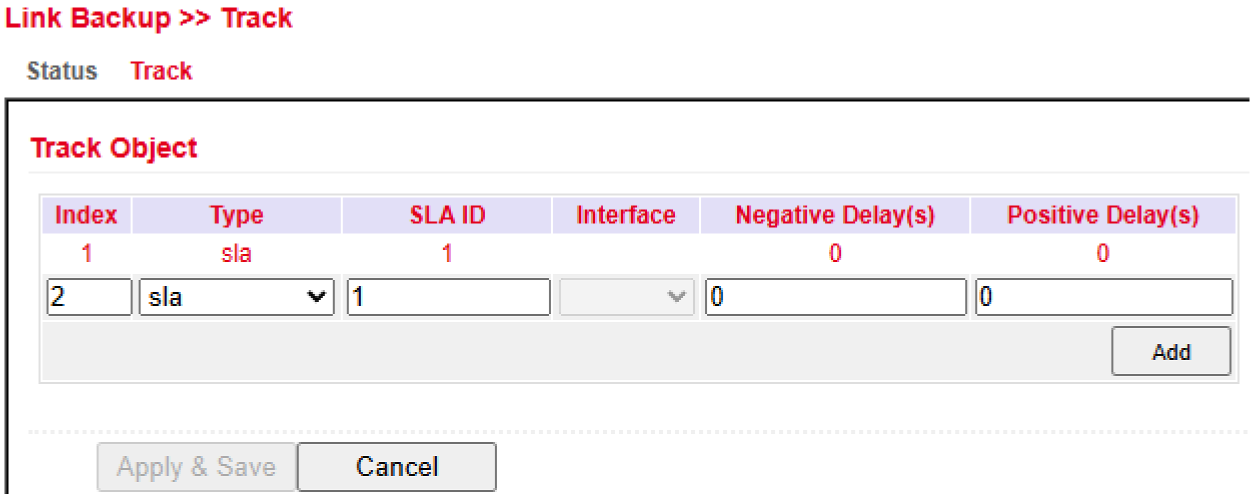
Index	Type	Destination Address	Status	Detect result
1	icmp-echo	8.8.8.8	start	up





5.5.2 Track

Configure a **Track object** under **Link Backup > Track > Track**.



Link Backup >> Track

Status Track

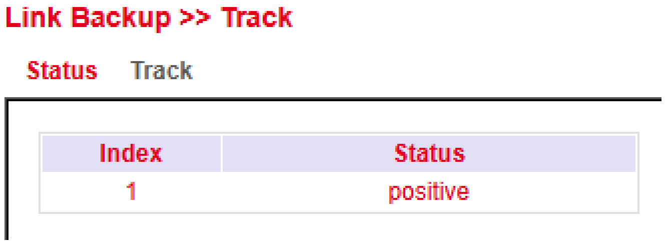
Track Object

Index	Type	SLA ID	Interface	Negative Delay(s)	Positive Delay(s)
1	sla	1		0	0
2	sla	1		0	0

Parameter	Description
Index	Freely selectable, identifies the entry
Type	`SLA` or `interface`
SLA ID	SLA index previously created
Interface	Not used when type = SLA
Negative Delay (s)	Delay before switching to backup if the main connection fails
Positive Delay (s)	Delay before switching back to the main connection once available

Status

The Track status indicates whether the monitored connection is up.
Check status under **Link Backup > Track > Status**.



Link Backup >> Track

Status Track

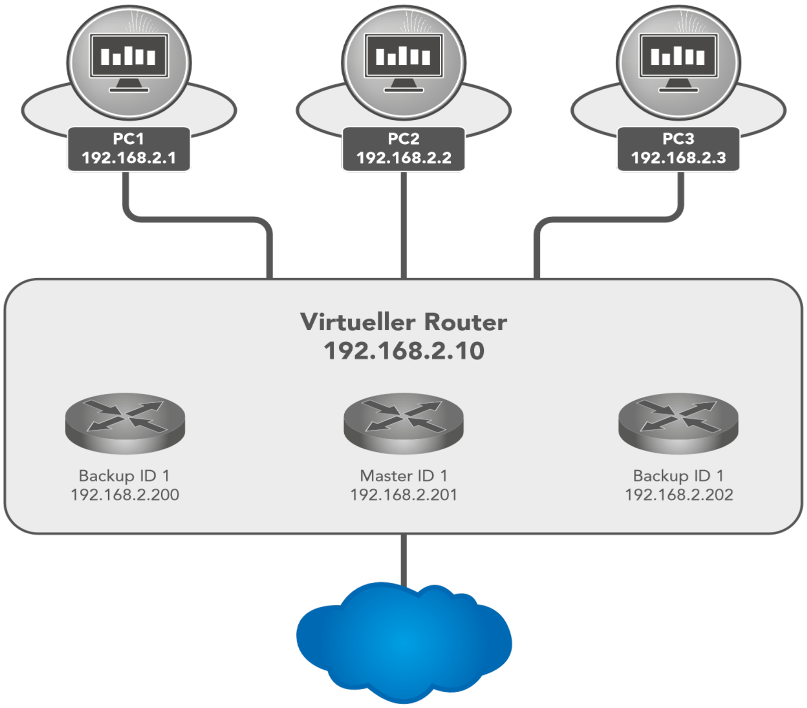
Index	Status
1	positive

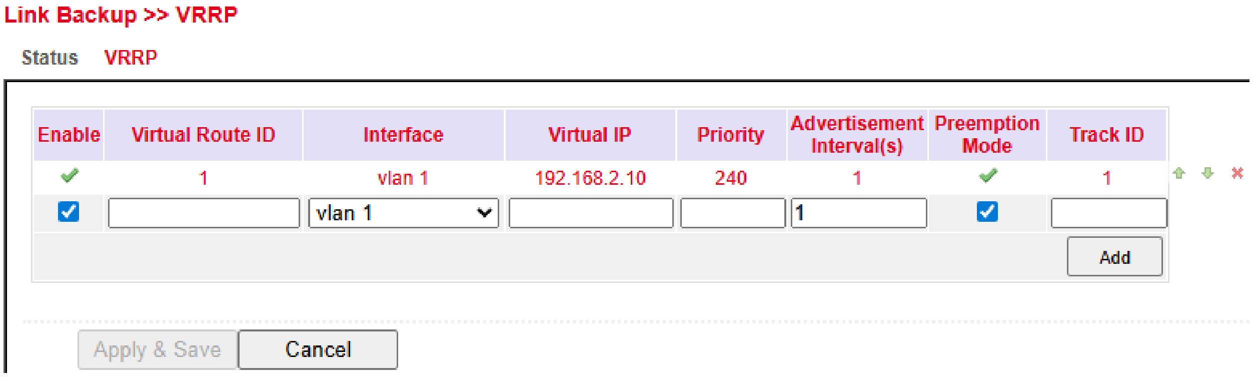
5.5.3 VRRP

In IP networks, all clients rely on a common **gateway**. If this gateway fails, communication to external networks (e.g., the Internet) is interrupted.

VRRP (Virtual Router Redundancy Protocol) solves this by allowing multiple routers to act as one **virtual router**:

- One router is the **master** (active gateway).
- Others remain in **backup** mode.
- If the master fails, a backup automatically takes over.



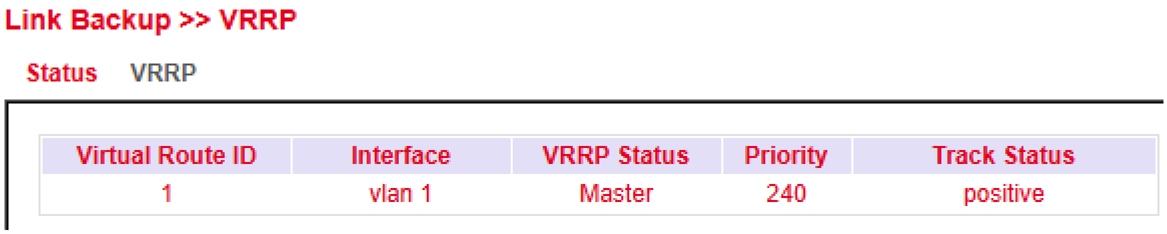


Link Backup >> VRRP

Enable	Virtual Route ID	Interface	Virtual IP	Priority	Advertisement Interval(s)	Preemption Mode	Track ID
✓	1	vlan 1	192.168.2.10	240	1	✓	1
☑		vlan 1			1	☑	

Parameter	Description
Enable	Enable/disable VRRP
Virtual Router ID	Group ID – must match across all routers in the VRRP group
Interface	LAN interface used
Virtual IP	Shared virtual router IP, must match across all routers in the group
Priority	0–254 → higher value = higher priority (highest becomes master)
Advertisement Interval(s)	Interval in seconds for VRRP hello messages
Preemption Mode	If enabled, a router with higher priority takes over as master automatically
Track ID	Track object used to monitor connection health

Status



Link Backup >> VRRP

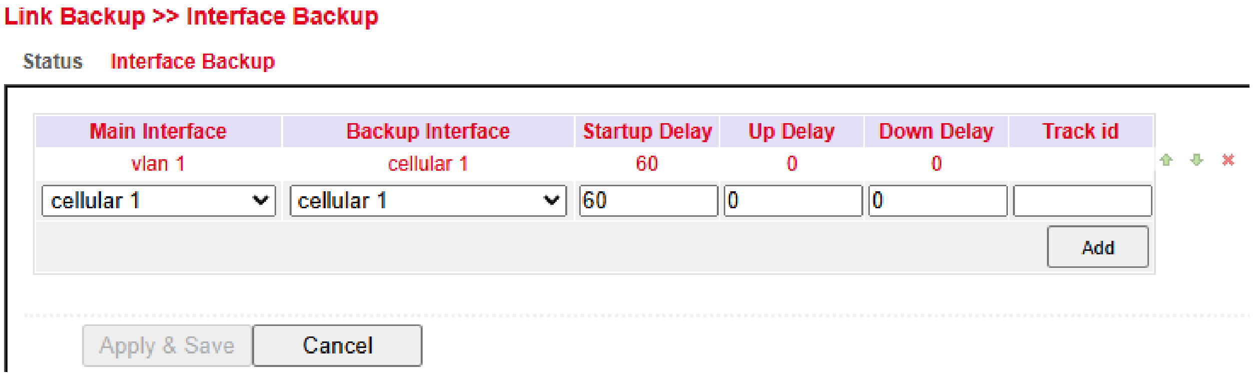
Virtual Route ID	Interface	VRRP Status	Priority	Track Status
1	vlan 1	Master	240	positive

Parameter	Description
Virtual Router ID	Router group identifier
Interface	LAN interface
VRRP Status	Current role → master or backup
Priority	Priority of the router
Track Status	Connection check result

5.5.4 Interface Backup

Interface Backup allows automatic failover between interfaces:
If the main interface fails, traffic switches to a backup interface.

Configure under **Link Backup > Interface Backup > Interface Backup**.



Link Backup >> Interface Backup

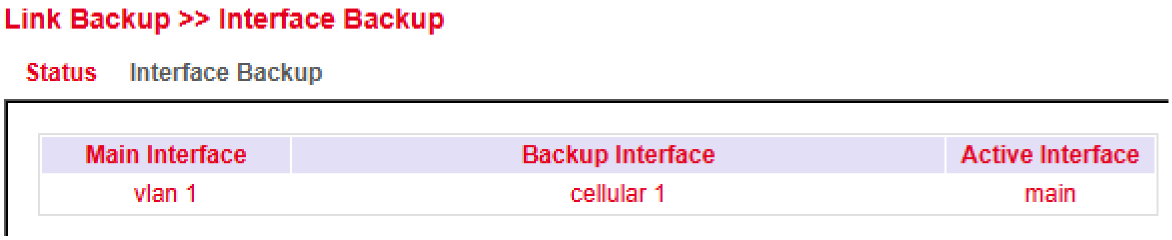
Main Interface	Backup Interface	Startup Delay	Up Delay	Down Delay	Track id
vlan 1	cellular 1	60	0	0	
cellular 1	cellular 1	60	0	0	

Parameter	Description
Main Interface	Defines the main (primary) interface
Backup Interface	Defines the backup interface
Startup Delay	Delay in seconds after system startup before monitoring begins
Up Delay	Delay before switching back to the main interface
Down Delay	Delay before switching to backup interface
Track ID	Track index linked to a previously created Track entry

Status

The status page shows:

- Which interfaces are configured as main/backup
- Which interface is currently active



Link Backup >> Interface Backup

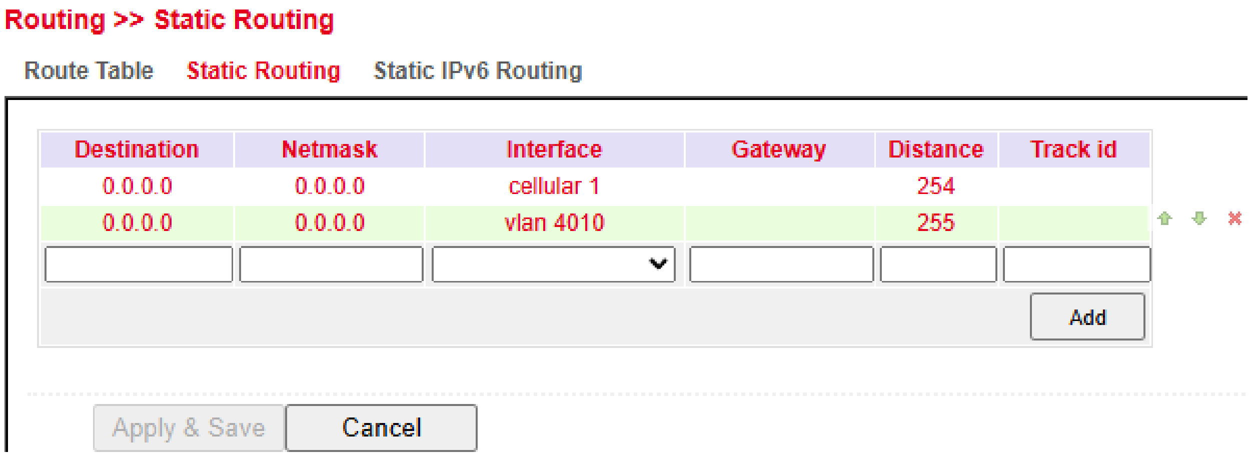
Main Interface	Backup Interface	Active Interface
vlan 1	cellular 1	main

5.6 Routing

Routing determines how data packets are transported between networks.
Routers use routing tables to select the best path.
On the Internet, multiple paths may exist, but data is reassembled correctly at the destination.

5.6.1 Static Routing

Static Routing defines fixed routes to specific networks or hosts.
Configure under **Routing** > **Static Routing** > **Static Routing**.



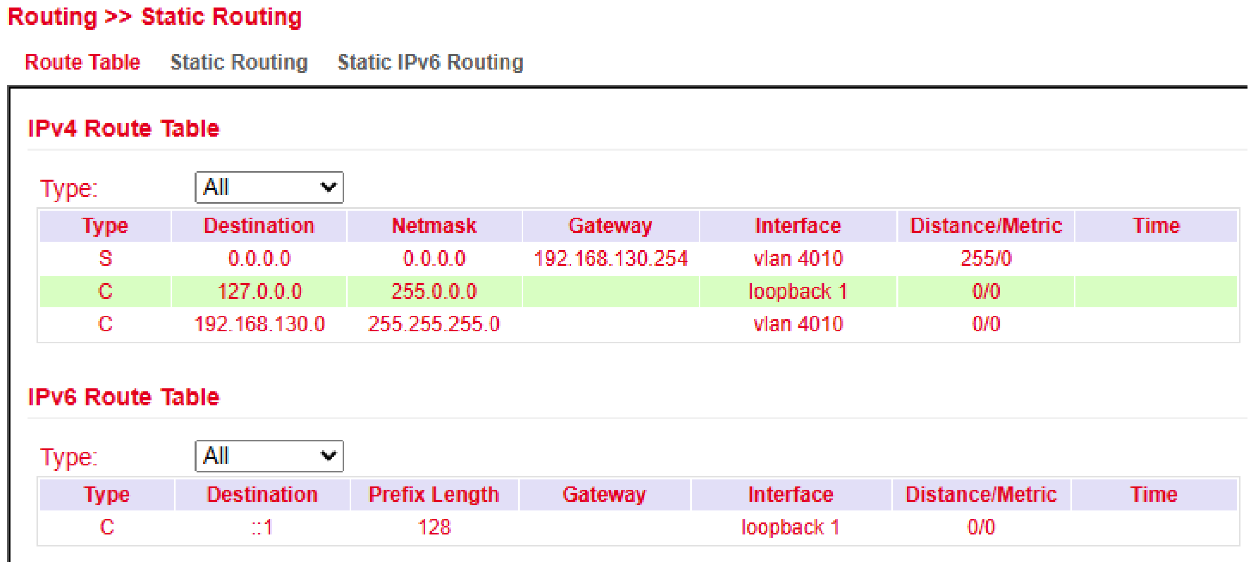
Routing >> Static Routing

Destination	Netmask	Interface	Gateway	Distance	Track id
0.0.0.0	0.0.0.0	cellular 1		254	
0.0.0.0	0.0.0.0	vlan 4010		255	

Parameter	Description
Destination	Destination host, subnet, or network. Default route = `0.0.0.0`
Netmask	Subnet mask used with destination. Example: host = `255.255.255.255`, default route = `0.0.0.0`
Interface	Network interface for the route (e.g., `cellular1`, `fastethernet0/1`, `VLAN1`, `bridge1`)
Gateway	Next-hop IP address
Distance	Priority/metric for the route – lower values take precedence if multiple routes exist
Track ID	Optional link to a Track object for monitoring

Route Table

The routing table can be viewed under:
Routing > Static Routing > Routing Table and
Routing > Dynamic Routing > Routing Table



Routing >> Static Routing

Route Table | Static Routing | Static IPv6 Routing

IPv4 Route Table

Type: All

Type	Destination	Netmask	Gateway	Interface	Distance/Metric	Time
S	0.0.0.0	0.0.0.0	192.168.130.254	vlan 4010	255/0	
C	127.0.0.0	255.0.0.0		loopback 1	0/0	
C	192.168.130.0	255.255.255.0		vlan 4010	0/0	

IPv6 Route Table

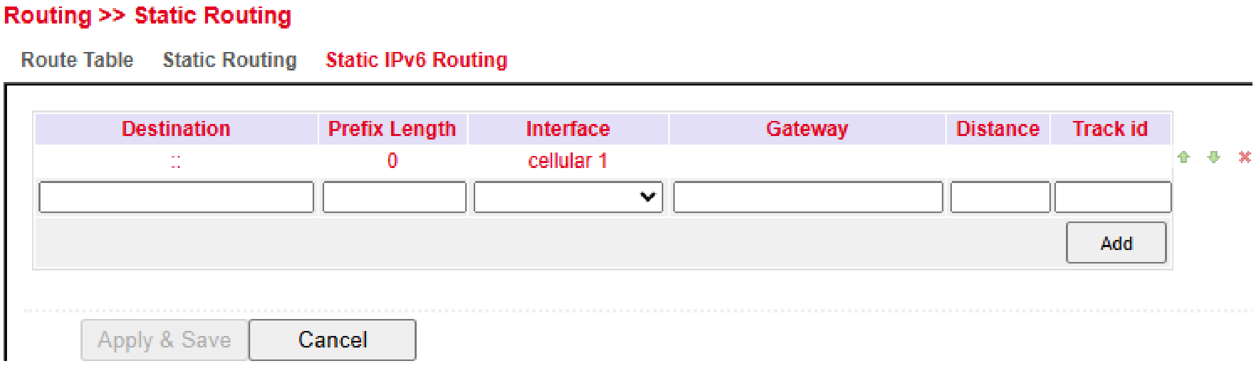
Type: All

Type	Destination	Prefix Length	Gateway	Interface	Distance/Metric	Time
C	::1	128		loopback 1	0/0	

Parameter	Description
Type	C = Connected (added automatically if interface has IP)S = Static (entered manually)R = RIP (dynamic, via RIP)O = OSPF (dynamic, via OSPF)
Destination	Destination host, subnet, network, or default route (0.0.0.0).
Netmask	Used with destination to define route scope. Example:- Host route = 255.255.255.255- Default route = 0.0.0.0.
Gateway	Next-hop IP address.
Interface	Interface used for the route (e.g., cellular1, loopback1, fastethernet0/1, VLAN1).
Distance/Metric	Route priority. Lower = higher priority. If multiple routes exist, the one with the lowest metric is preferred.
Time	Duration the route has been active.

Static IPv6 Routing

Static IPv6 routes can be defined to direct traffic through specific network paths.
This is essential in **multi-interface** or **segmented** networks.



Routing >> Static Routing

Route Table | Static Routing | Static IPv6 Routing

Destination	Prefix Length	Interface	Gateway	Distance	Track id
::	0	cellular 1			

Parameter	Description
Field	Destination IPv6 network or host address.
Prefix Length	Subnet size (e.g., 64 for a /64 subnet).
Interface	Outgoing interface (e.g., `cellular1`).
Gateway	Next-hop IPv6 address.
Distance	Administrative distance (lower = preferred).
Track ID	(Optional) ID for route tracking / failover.

Actions:

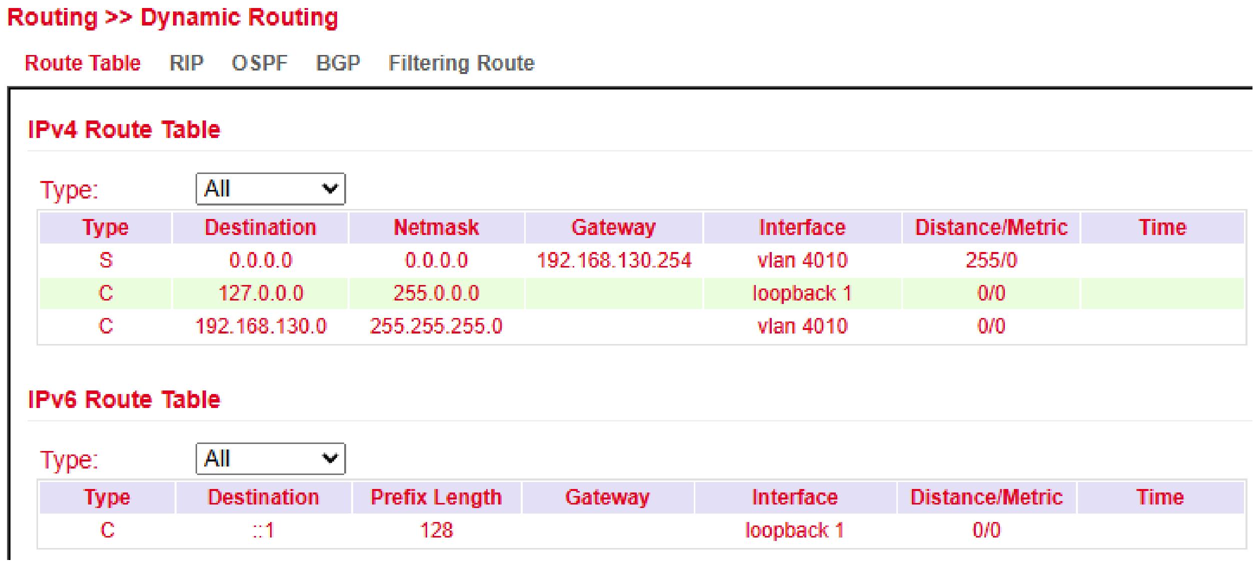
- **Add** → Create new static IPv6 route.
- **Apply & Save** → Save changes.
- **Cancel** → Discard changes.

5.6.2 Dynamic Routing

Dynamic routing allows routes to be learned automatically by routing protocols.
Unlike static routing, paths are updated **dynamically during operation**.

Route Table

Viewable under:
Routing > Dynamic Routing > Routing Table



IPv4 Route Table

Type: All

Type	Destination	Netmask	Gateway	Interface	Distance/Metric	Time
S	0.0.0.0	0.0.0.0	192.168.130.254	vlan 4010	255/0	
C	127.0.0.0	255.0.0.0		loopback 1	0/0	
C	192.168.130.0	255.255.255.0		vlan 4010	0/0	

IPv6 Route Table

Type: All

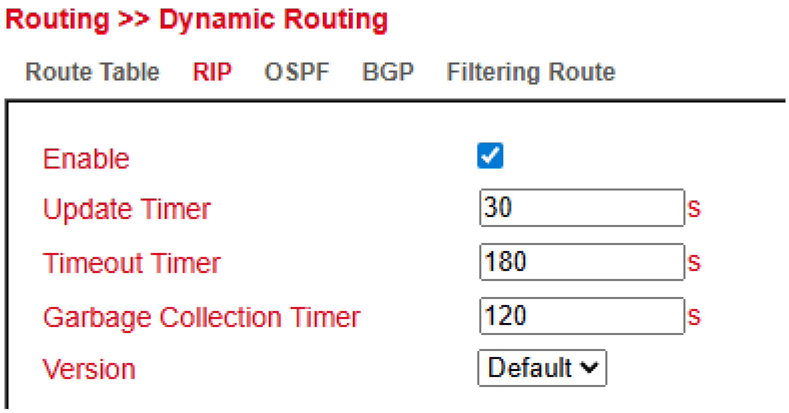
Type	Destination	Prefix Length	Gateway	Interface	Distance/Metric	Time
C	::1	128		loopback 1	0/0	

RIP

RIP (Routing Information Protocol) uses a **distance vector algorithm** to share routes.

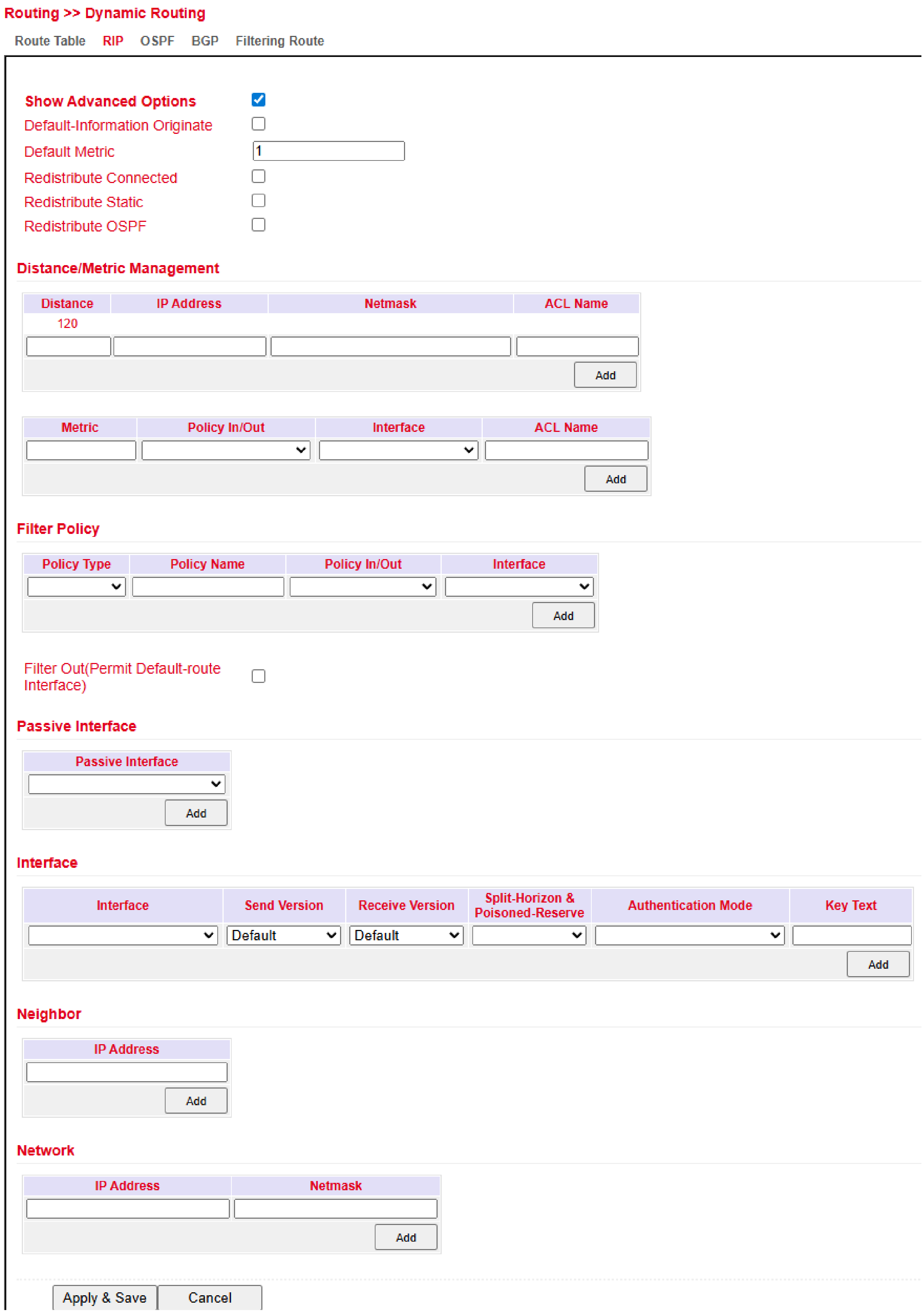
- Each router advertises known routes to its neighbors.
- The best route is chosen based on hop count (max. 15 hops).

Configure under: **Routing > Dynamic Routing > RIP**



Routing >> Dynamic Routing

Enable	☑
Update Timer	30 s
Timeout Timer	180 s
Garbage Collection Timer	120 s
Version	Default



Routing >> Dynamic Routing

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

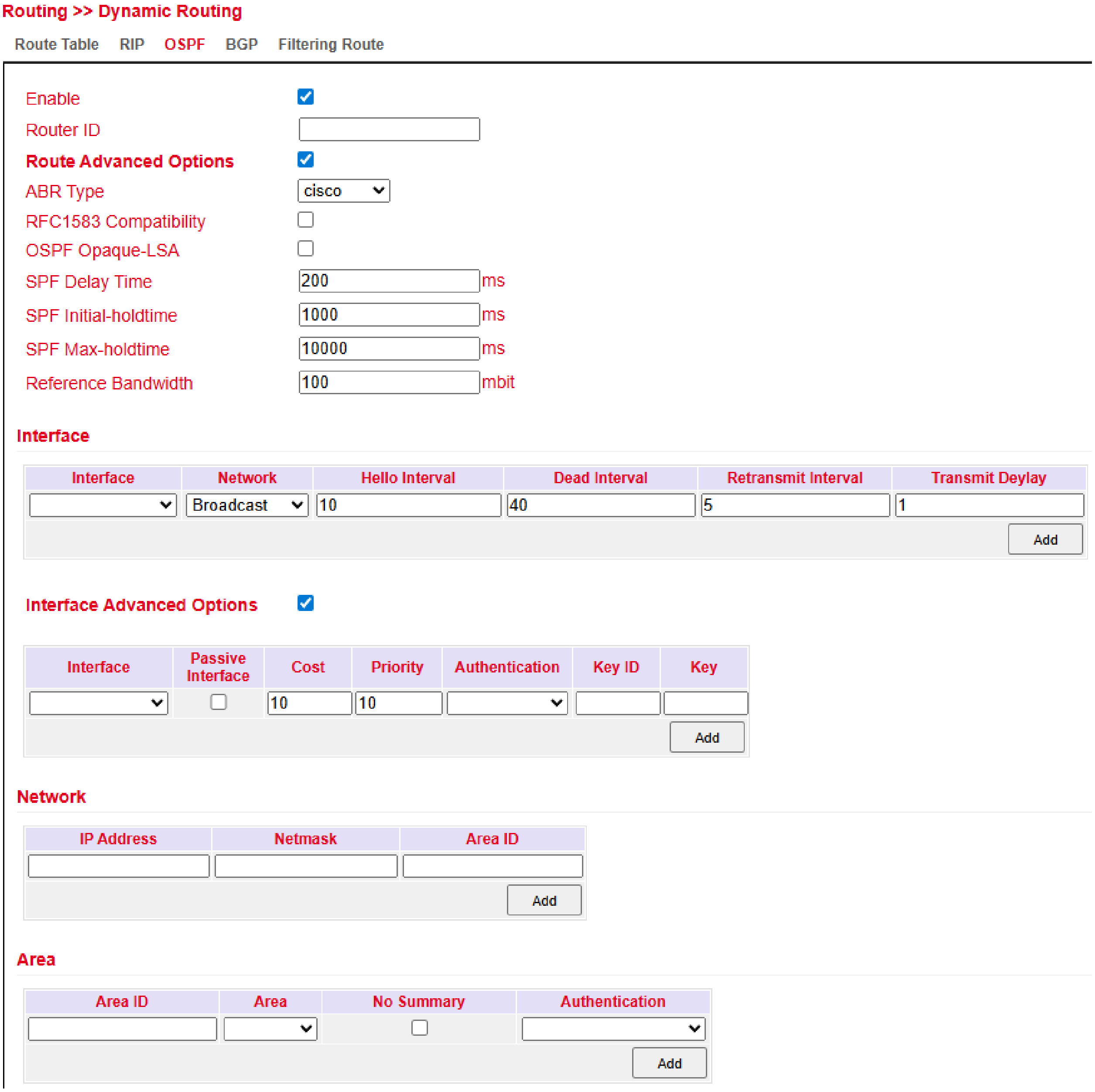
IP Address	Netmask

OSPF

OSPF (Open Shortest Path First) uses a **link-state algorithm**.

- Supports hierarchical networks.
- Allows multiple equal-cost paths simultaneously.
- Reacts quickly to topology changes and uses bandwidth efficiently.

Configure under: **Routing > Dynamic Routing > OSPF**



Routing >> Dynamic Routing

Enable	☑
Router ID	
Route Advanced Options	☑
ABR Type	cisco
RFC1583 Compatibility	□
OSPF Opaque-LSA	□
SPF Delay Time	200 ms
SPF Initial-holdtime	1000 ms
SPF Max-holdtime	10000 ms
Reference Bandwidth	100 mbit

Interface

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

Interface Advanced Options ☑

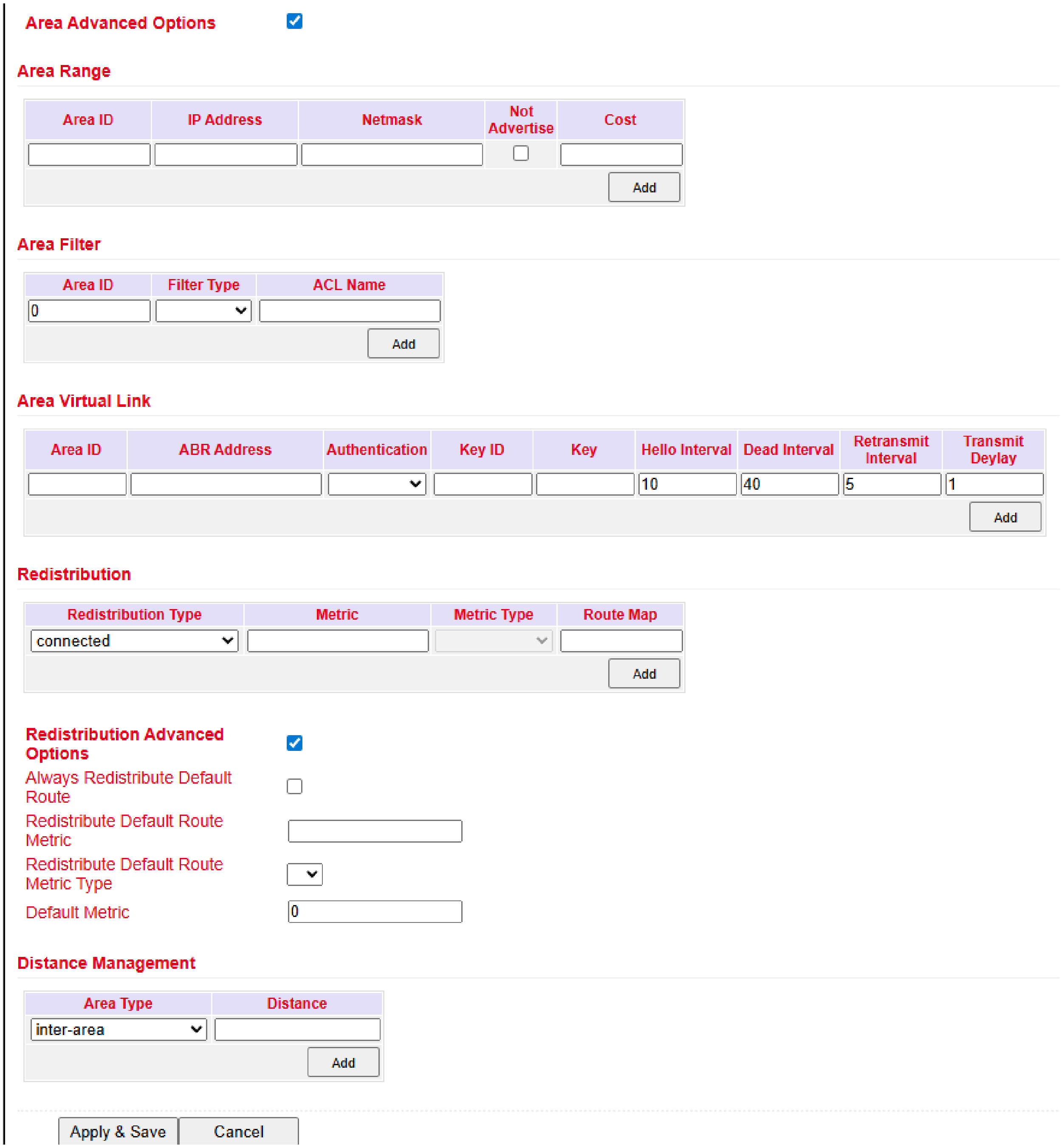
Interface	Passive Interface	Cost	Priority	Authentication	Key ID	Key
	□	10	10			

Network

IP Address	Netmask	Area ID

Area

Area ID	Area	No Summary	Authentication
		□	



Area Advanced Options ☑

Area Range

Area ID	IP Address	Netmask	Not Advertise	Cost
			□	

Area Filter

Area ID	Filter Type	ACL Name
0		

Area Virtual Link

Area ID	ABR Address	Authentication	Key ID	Key	Hello Interval	Dead Interval	Retransmit Interval	Transmit Deylay
					10	40	5	1

Redistribution

Redistribution Type	Metric	Metric Type	Route Map
connected			

Redistribution Advanced Options ☑

Always Redistribute Default Route □

Redistribute Default Route Metric

Redistribute Default Route Metric Type

Default Metric 0

Distance Management

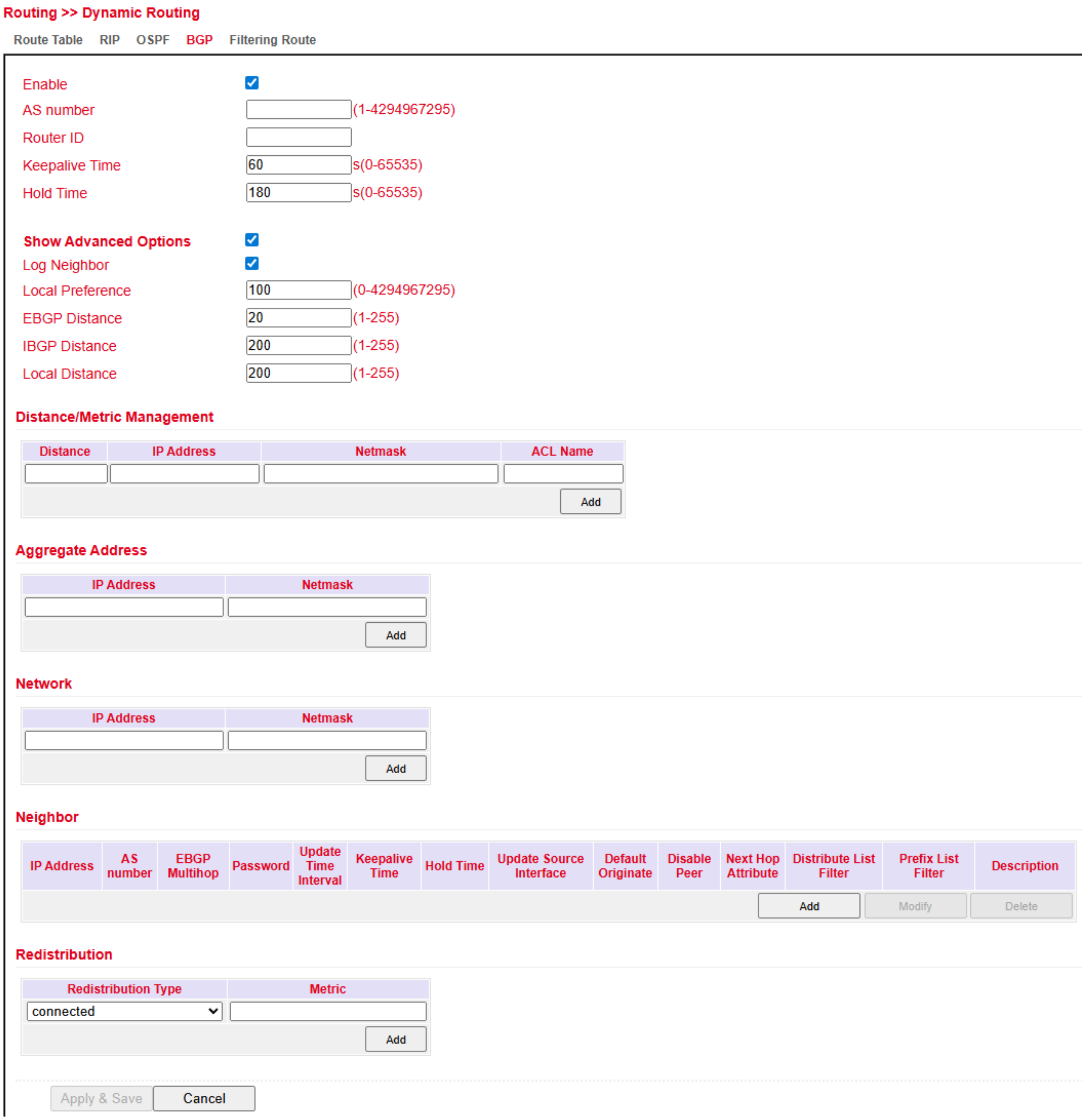
Area Type	Distance
inter-area	

BGP

BGP (Border Gateway Protocol) is the **Internet's main routing protocol**.

- Connects **autonomous systems (AS)**, typically Internet Service Providers.
- Uses **path vector routing**.
- Routing decisions often consider **business policies** in addition to technical metrics.

Configure under: **Routing > Dynamic Routing > BGP**



Routing >> Dynamic Routing

Enable	☑	
AS number		(1-4294967295)
Router ID		
Keepalive Time	60	s(0-65535)
Hold Time	180	s(0-65535)
Show Advanced Options	☑	
Log Neighbor	☑	
Local Preference	100	(0-4294967295)
EBGP Distance	20	(1-255)
IBGP Distance	200	(1-255)
Local Distance	200	(1-255)

Distance/Metric Management

Distance	IP Address	Netmask	ACL Name

Aggregate Address

IP Address	Netmask

Network

IP Address	Netmask

Neighbor

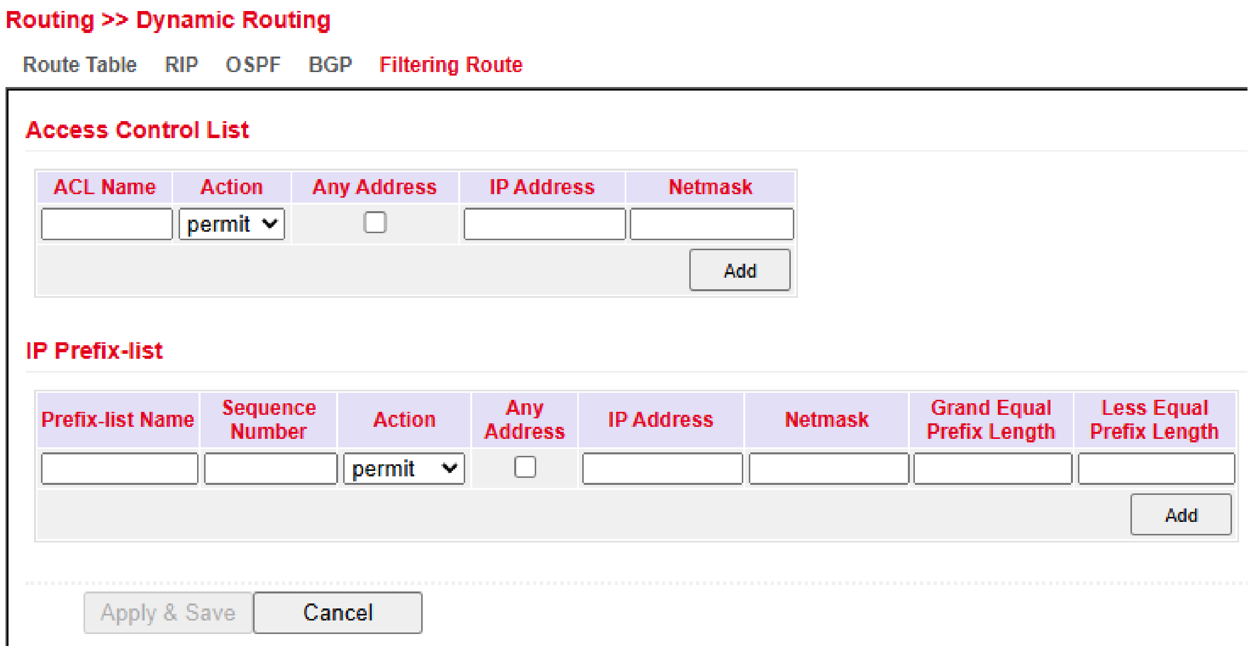
IP Address	AS number	EBGP Multihop	Password	Update Time Interval	Keepalive Time	Hold Time	Update Source Interface	Default Originate	Disable Peer	Next Hop Attribute	Distribute List Filter	Prefix List Filter	Description

Redistribution

Redistribution Type	Metric
connected	

Filtering Route

Under **Routing > Dynamic Routing > Filtering Route** you can configure routing filters.
Filters define which routes are advertised or accepted.



Access Control List

ACL Name	Action	Any Address	IP Address	Netmask
	permit	□		

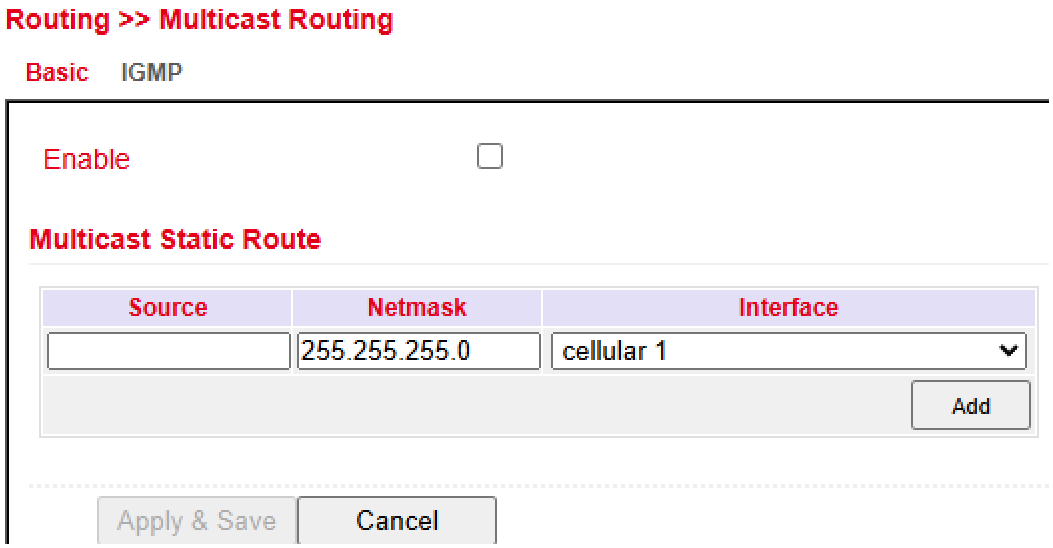
IP Prefix-list

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

5.6.3 Multicast Routing

Basic

Configure under: **Routing** > **Multicast Routing** > **Basic**



Enable □

Multicast Static Route

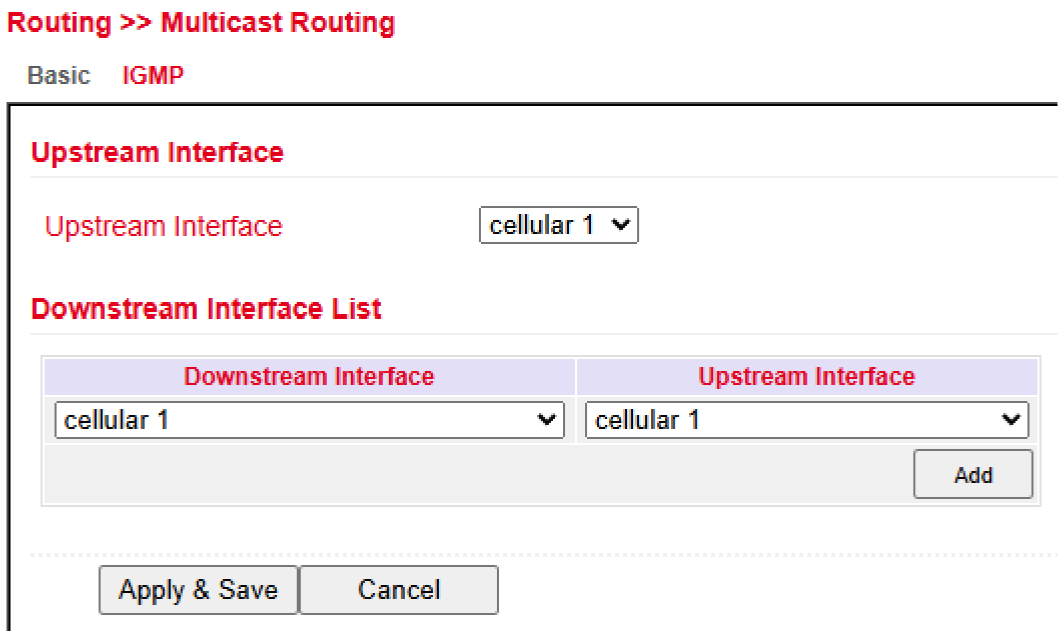
Source	Netmask	Interface
	255.255.255.0	cellular 1

IGMP

IGMP (Internet Group Management Protocol) configuration:

- **Upstream Interface** → Select the interface distributing the multicast.
- **Downstream Interface List** → Select downstream interfaces for multicast traffic.

Interfaces vary depending on the router model.



Routing >> Multicast Routing

Basic IGMP

Upstream Interface

Upstream Interface: cellular 1

Downstream Interface List

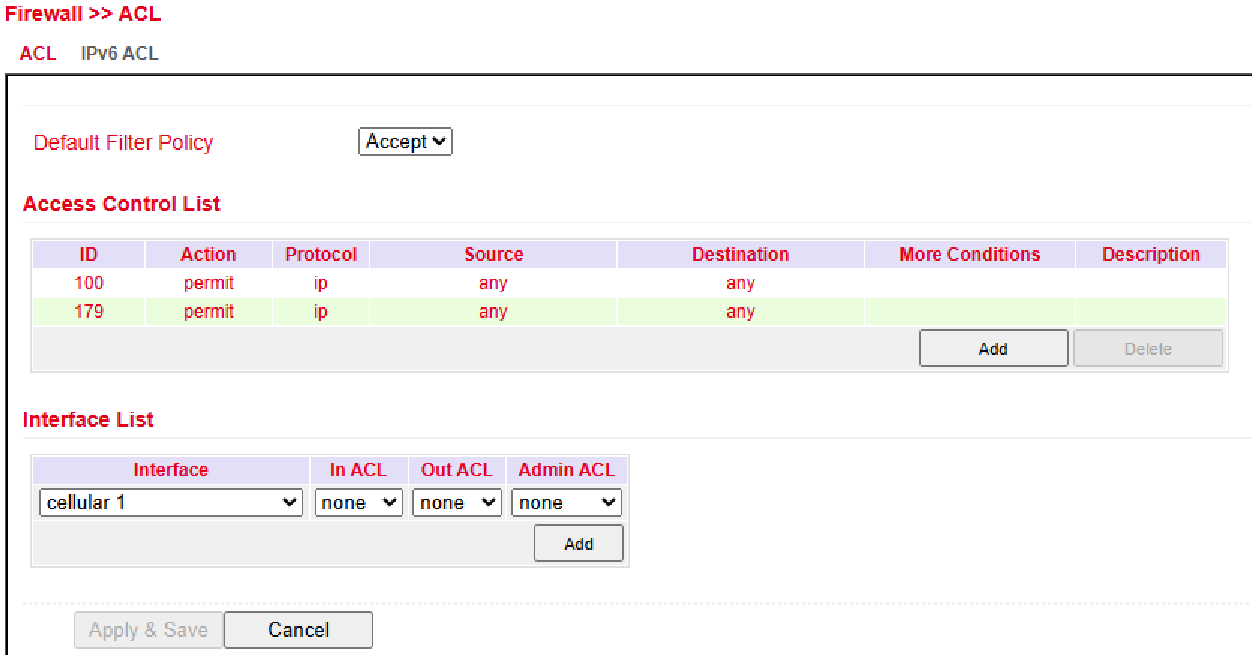
Downstream Interface	Upstream Interface
cellular 1	cellular 1

5.7 Firewall

5.7.1 ACL

The **Access Control List (ACL)** controls usage and administration by defining which computers or networks can access the router or networks behind it.
ACL rules analyze and manage **incoming and outgoing data packets** according to defined rules.

- Rules can be based on **source/destination IP addresses**, **TCP/UDP port numbers**, and more.
- Two types of ACL are supported:
  - **Standard ACL** → Allow/deny communication from/to a network.
  - **Extended ACL** → More granular options (e.g., restrict HTTP, FTP, Telnet).



Firewall >> ACL

ACL IPv6 ACL

Default Filter Policy: Accept

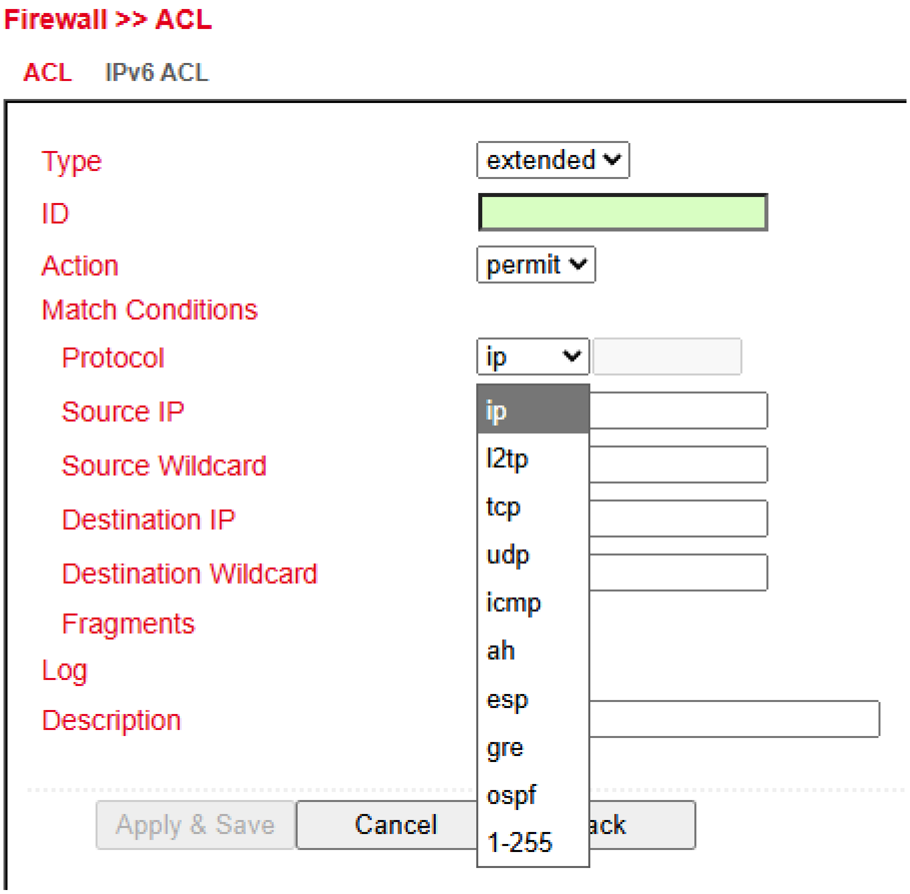
Access Control List

ID	Action	Protocol	Source	Destination	More Conditions	Description
100	permit	ip	any	any		
179	permit	ip	any	any		

Interface List

Interface	In ACL	Out ACL	Admin ACL
cellular 1	none	none	none

- Overview of existing ACL rules.
- Click **Add** to create a new ACL.



Firewall >> ACL

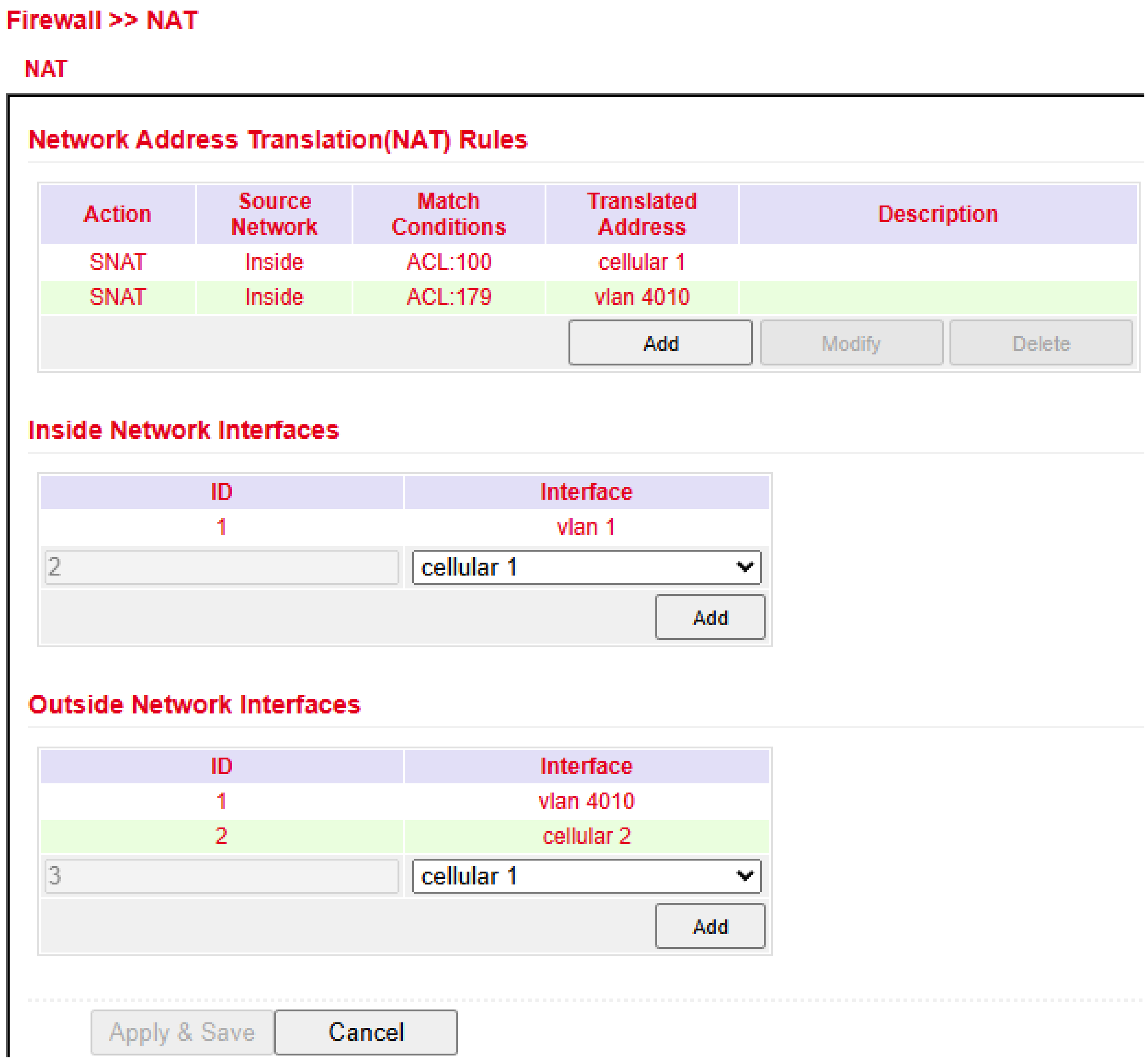
ACL Parameters

Parameter	Description
Type	`standard` or `extended`
ID	Default: 100 (preconfigured). Additional IDs can be freely assigned.
Action	`Permit` or `Deny`
Protocol	Protocol(s) to match
Source IP	Source IP address or network (e.g., `192.168.2.0`)
Source Wildcard	Wildcard of source subnet mask (e.g., `255.255.255.0` → `0.0.0.255`)
Destination IP	Destination IP address or network (e.g., `172.16.0.0`)
Destination Wildcard	Wildcard of destination subnet mask (e.g., `255.255.0.0` → `0.0.255.255`)
Description	Optional text description

5.7.2 NAT

Network Address Translation (NAT)

NAT modifies address information in data packets to connect different networks.
It is configured under **Firewall > NAT**.



Firewall >> NAT

NAT

Network Address Translation(NAT) Rules

Action	Source Network	Match Conditions	Translated Address	Description
SNAT	Inside	ACL:100	cellular 1	
SNAT	Inside	ACL:179	vlan 4010	

Inside Network Interfaces

ID	Interface
1	vlan 1
2	cellular 1

Outside Network Interfaces

ID	Interface
1	vlan 4010
2	cellular 2
3	cellular 1

NAT Types

Type	Action
SNAT	Rewrites the source IP address (LAN → WAN)
DNAT	Rewrites the destination IP address (WAN → LAN)
1:1 NAT	Maps one IP address to another (one-to-one translation)

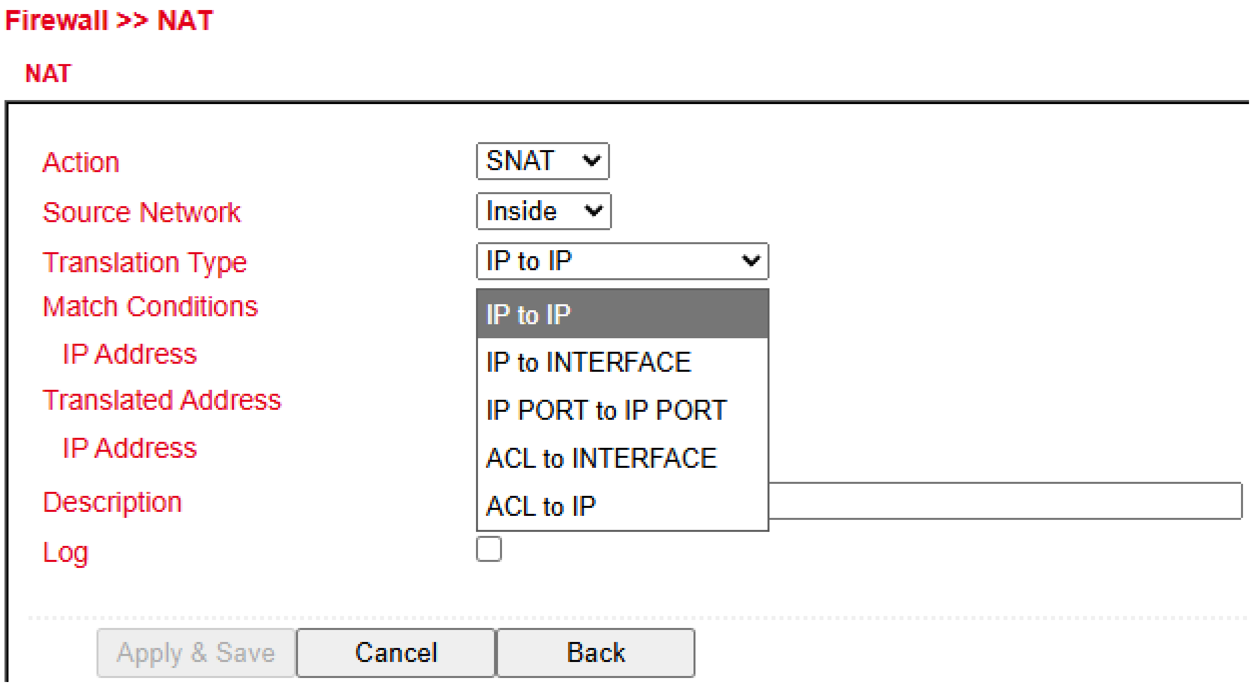
Inside/Outside Interfaces

- **Inside** = LAN interface

- **Outside** = WAN interface

Translation Types

Type	Description
IP to IP	Translate one IP to another
IP to Interface	Translate IP to an interface’s address
IP Port to IP Port	Translate IP:Port combination to another
ACL to Interface	Translate address according to ACL into an interface address
ACL to IP	Translate address according to ACL into another IP



Firewall >> NAT

NAT

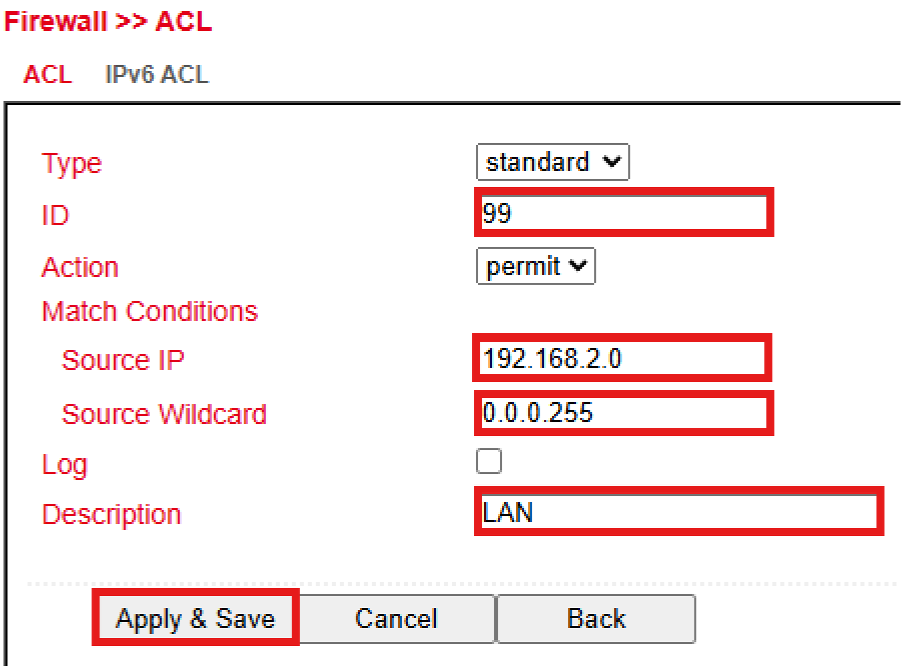
Action	SNAT
Source Network	Inside
Translation Type	IP to IP
Match Conditions	
IP Address	
Translated Address	
IP Address	
Description	
Log	□

Example: Case 1 – SNAT (Router as Internet Gateway)

The TK804L-450 translates **private LAN IPs** into a **public IP** for Internet access.
⊠ This is the **default factory setting**.

Steps:

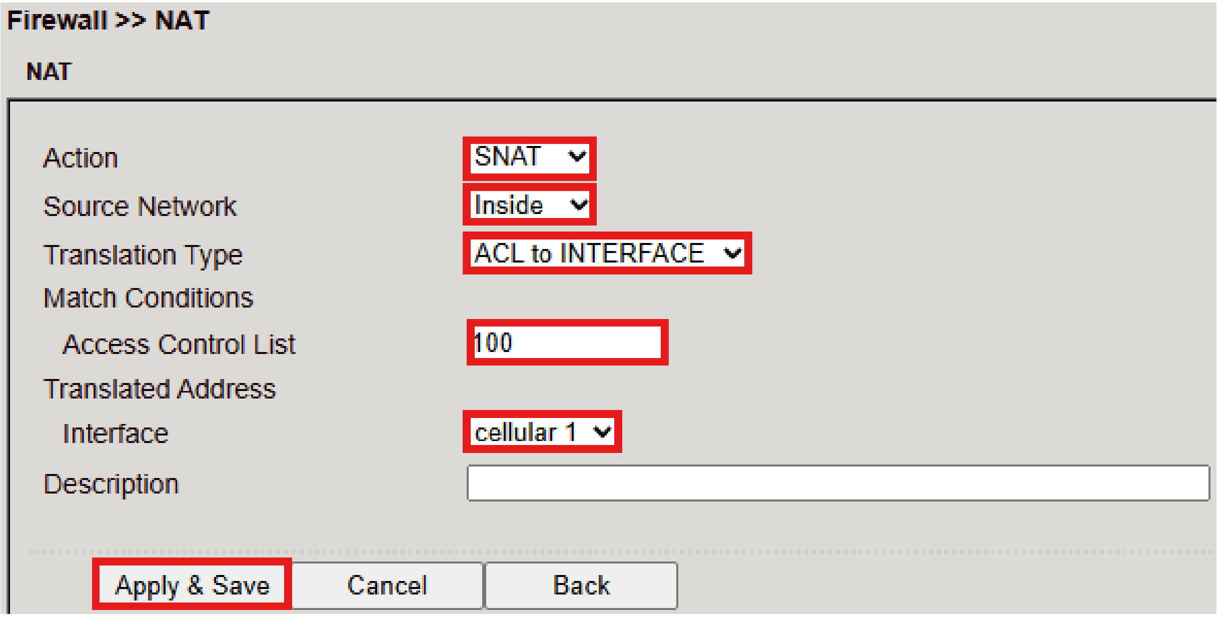
1. Create an **ACL rule** under **Firewall > ACL**:
   - Assign an **ID**.
   - Enter **source IP/network** and **wildcard mask**.



Firewall >> ACL

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

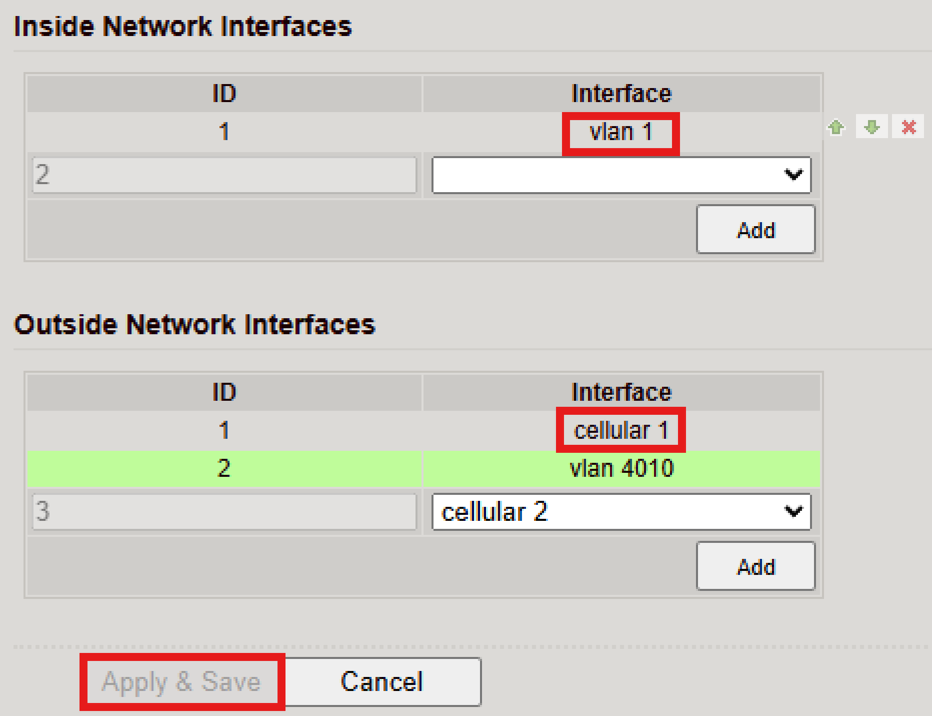
2. Configure the **SNAT rule**.



Firewall >> NAT

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

3. Define the **Inside (LAN)** and **Outside (WAN)** interfaces.



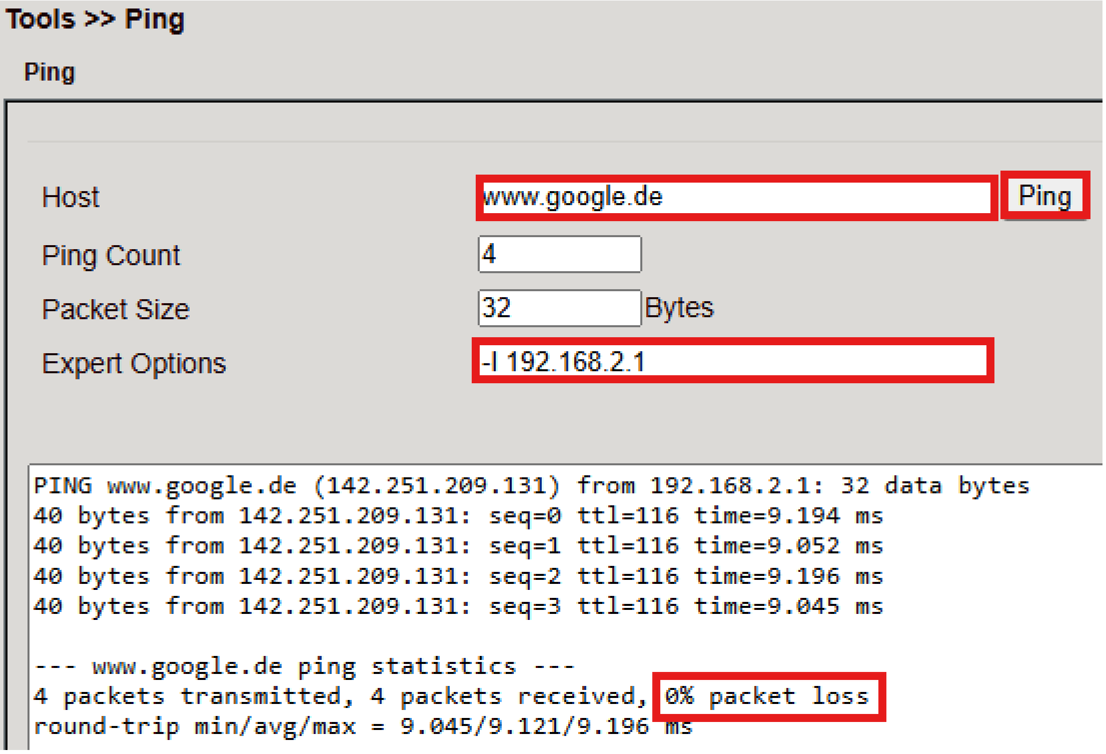
Inside Network Interfaces

ID	Interface
1	vlan 1
2	

Outside Network Interfaces

ID	Interface
1	cellular 1
2	vlan 4010
3	cellular 2

4. Test access with **Ping** under **Tools > Ping**.
   - Use the **Expert option:** `-I 192.168.2.1` (capital i) to ensure ping originates from LAN interface.



Tools >> Ping

Ping

Host: www.google.de

Ping Count: 4

Packet Size: 32 Bytes

Expert Options: -I 192.168.2.1

```
PING www.google.de (142.251.209.131) from 192.168.2.1: 32 data bytes
40 bytes from 142.251.209.131: seq=0 ttl=116 time=9.194 ms
40 bytes from 142.251.209.131: seq=1 ttl=116 time=9.052 ms
40 bytes from 142.251.209.131: seq=2 ttl=116 time=9.196 ms
40 bytes from 142.251.209.131: seq=3 ttl=116 time=9.045 ms

--- www.google.de ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 9.045/9.121/9.196 ms
```

Example: Case 2 – DNAT (Port Mapping / Port Forwarding)

DNAT (also known as Port Mapping/Forwarding) is used to make internal services (e.g., web servers) accessible from the Internet.
Configuration steps follow the same pattern:

1. Define ACL (optional, depending on policy).
2. Configure **DNAT rule** with desired port mapping.
3. Assign interfaces.

Requirements

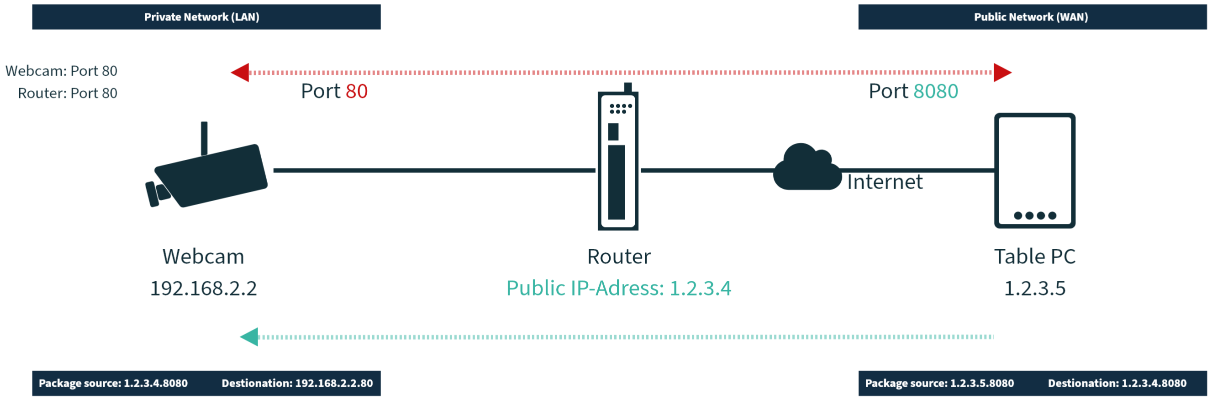
- Public IP address in the mobile network (or also for wired Internet connections).
  (Note: Many mobile operators offer business tariffs with public IPs, e.g. T-Mobile IP VPN or Vodafone CDA. Some providers also supply public IPs via standard SIM cards.)

Port Mapping Notes

To configure port mapping you need:

- **IP address** of the target device
- **Port** to be redirected (e.g., HTTP/80)

Example: Welotec


Private Network (LAN)
Public Network (WAN)
Webcam: Port 80
Router: Port 80
Port 80
Port 8080
Internet
Webcam
192.168.2.2
Router
Public IP-Adress: 1.2.3.4
Table PC
1.2.3.5
Package source: 1.2.3.4.8080
Destionation: 192.168.2.2.80
Package source: 1.2.3.5.8080
Destionation: 1.2.3.4.8080

Parameter	Value
LAN IP (Router)	192.168.2.1
Subnet Mask	255.255.255.0
LAN IP (Webcam)	192.168.2.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1

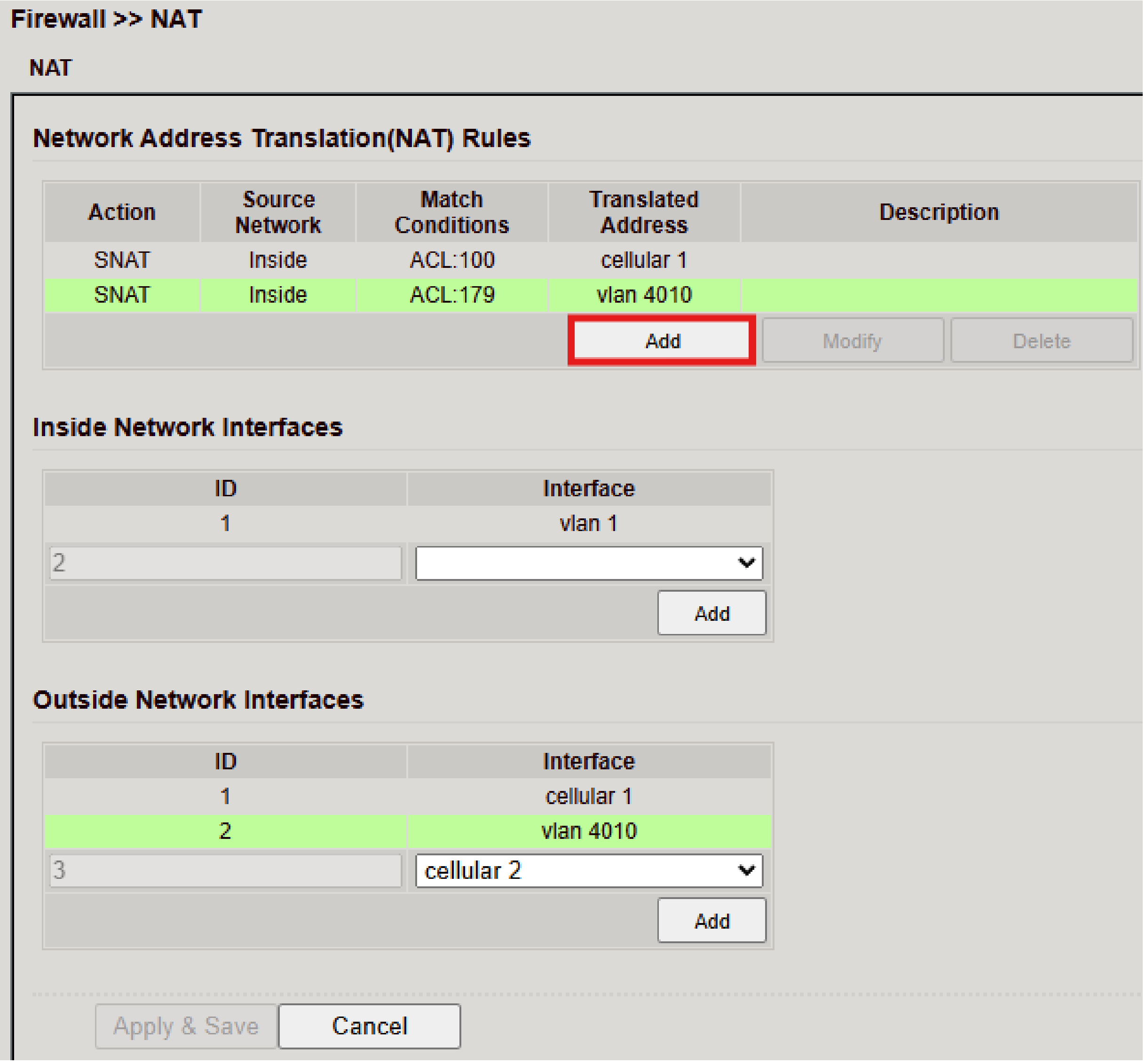
The webcam is reachable via:
http://192.168.2.2 (TCP Port 80).

Checklist before setup:

- Does the camera have IP `192.168.2.2`?
- Does it respond to `ping 192.168.2.2`?
- Is the web interface accessible via `http://192.168.2.2`?
- Is the router (`192.168.2.1`) set as default gateway?

Configuration

1. Open **Firewall > NAT**.
2. Click **Add** to create a new NAT rule.



Firewall >> NAT

NAT

Network Address Translation(NAT) Rules

Action	Source Network	Match Conditions	Translated Address	Description
SNAT	Inside	ACL:100	cellular 1	
SNAT	Inside	ACL:179	vlan 4010	

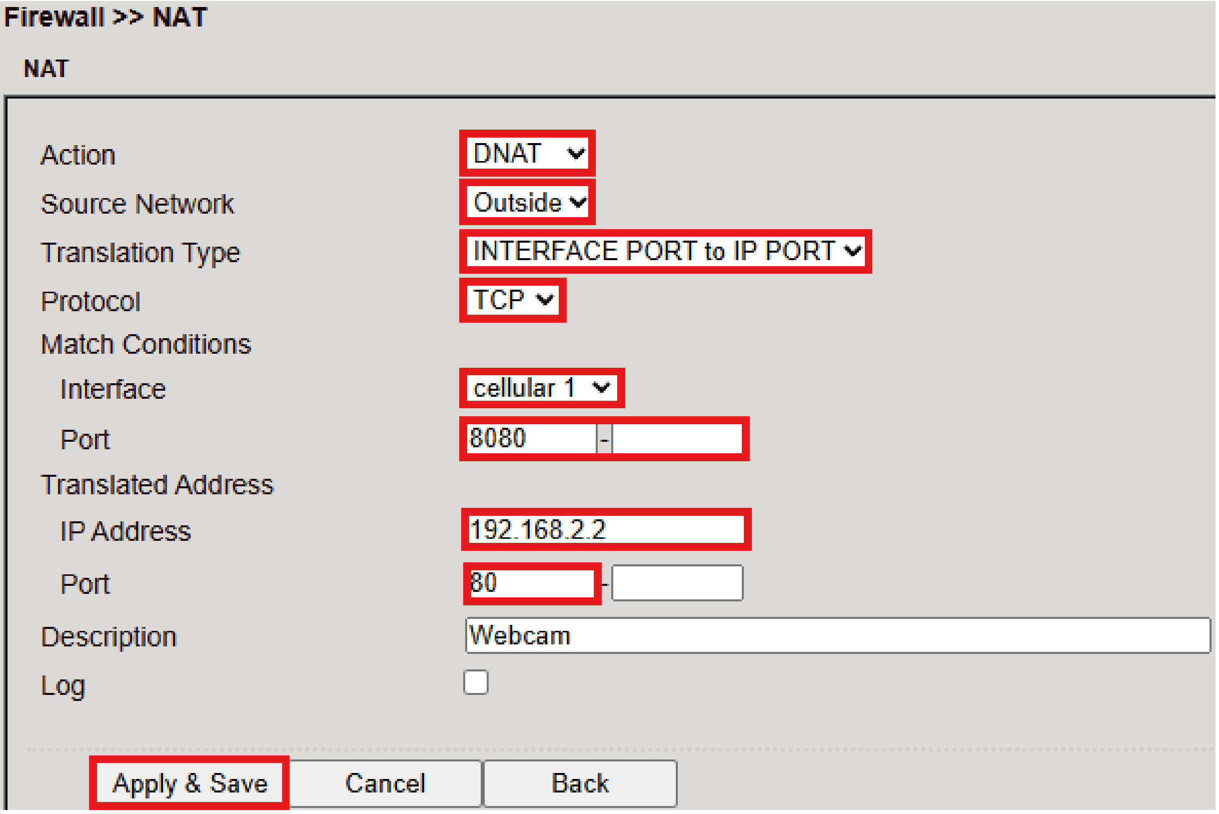
Inside Network Interfaces

ID	Interface
1	vlan 1
2	

Outside Network Interfaces

ID	Interface
1	cellular 1
2	vlan 4010
3	cellular 2

3. Enter the required data (example shown below).

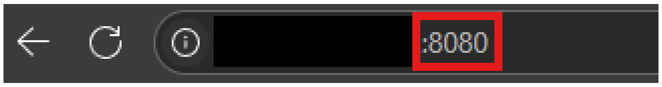


Firewall >> NAT

NAT

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: □

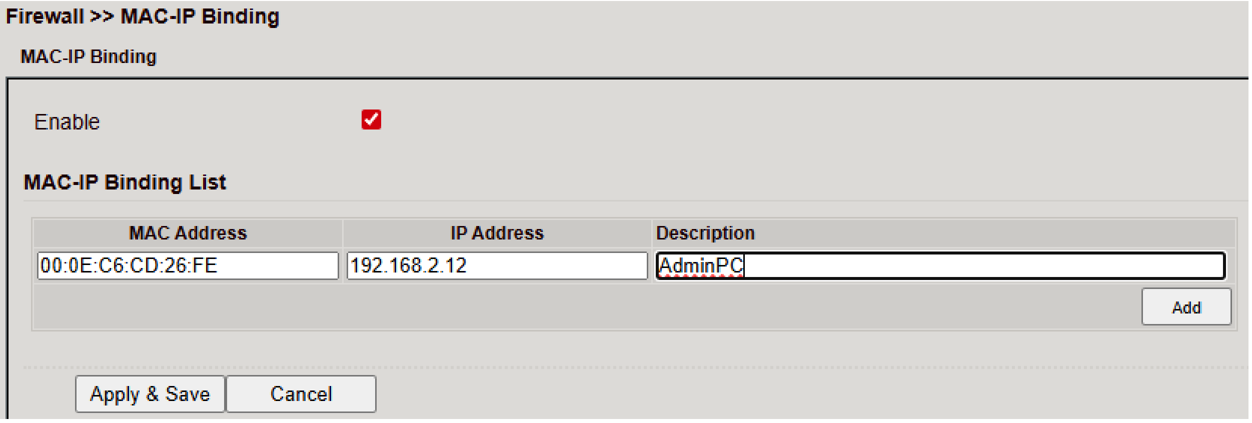
4. The device is now accessible via the router’s **public IP + mapped port**.



[redacted]:8080

5.7.3 MAC-IP Binding

Located under **Firewall > MAC-IP Binding**.
This feature ensures that devices can only access the router if their **MAC and IP address match**.



Firewall >> MAC-IP Binding

MAC-IP Binding

Enable ☑

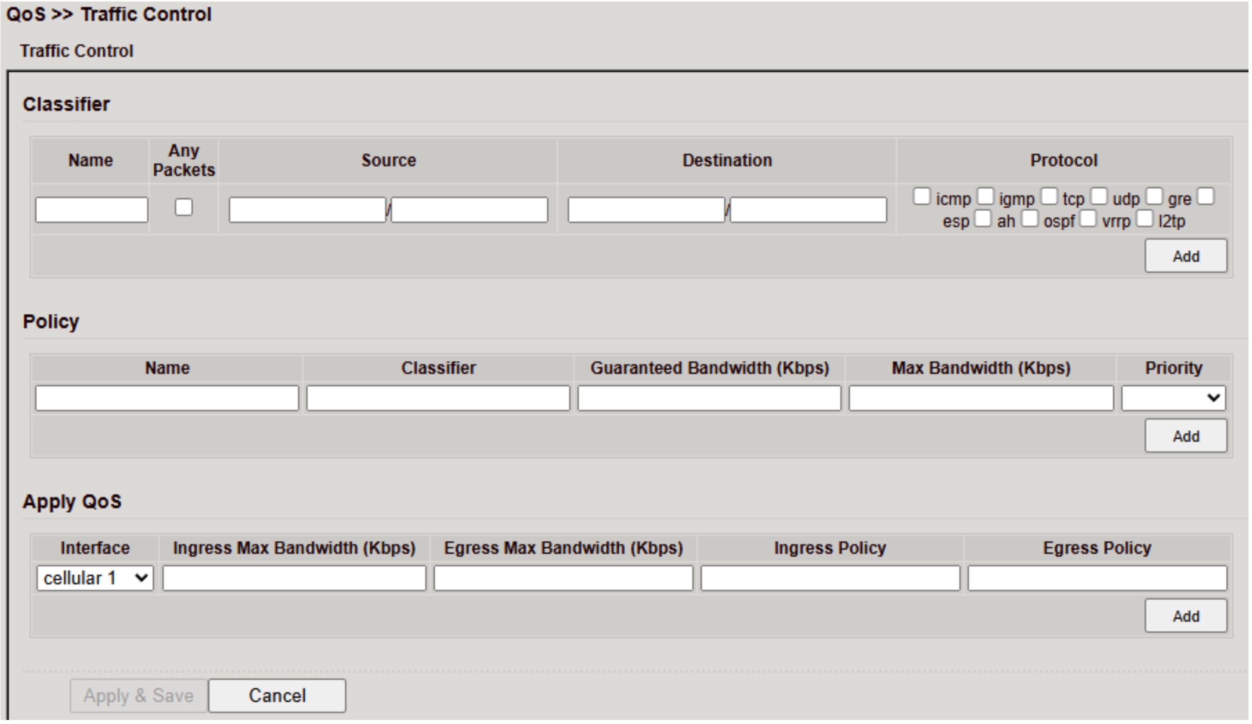
MAC-IP Binding List

MAC Address	IP Address	Description
00:0E:C6:CD:26:FE	192.168.2.12	AdminPC

Parameter	Description
MAC Address	Enter in format `XX:XX:XX:XX:XX:XX`, e.g. `00:FF:4E:85:F1:B5`
IP Address	IP address assigned to the device, e.g. `192.168.2.150`
Description	Optional description text

5.7.4 QoS – Traffic Control

The **Traffic Control** page allows configuration of QoS rules to prioritize traffic.



QoS >> Traffic Control

Traffic Control

Classifier

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

Policy

Name	Classifier	Guaranteed Bandwidth (Kbps)	Max Bandwidth (Kbps)	Priority

Apply QoS

Interface	Ingress Max Bandwidth (Kbps)	Egress Max Bandwidth (Kbps)	Ingress Policy	Egress Policy
cellular 1				

Classifier

Define criteria for traffic matching:

- **Name** → Identifier
- **Source/Destination** → IP or range
- **Protocol** → TCP, UDP, ICMP

Click **Add** to save the classifier.

Policy

Assign bandwidth rules to a classifier:

- **Guaranteed Bandwidth** → Minimum rate (Kbps)
- **Max Bandwidth** → Maximum rate (Kbps)
- **Priority** → Importance of traffic

Click **Add** to apply the policy.

Apply QoS

Assign policies to interfaces:

- **Interface** → e.g., Cellular 1
- **Ingress/Egress Bandwidth** → Max allowed rates
- **Ingress/Egress Policy** → Selected policy

Click **Add**, then **Apply & Save**.

5.8 VPN

VPN (Virtual Private Network) connects devices securely to remote networks.
Example: Remote employees accessing the company LAN from home.

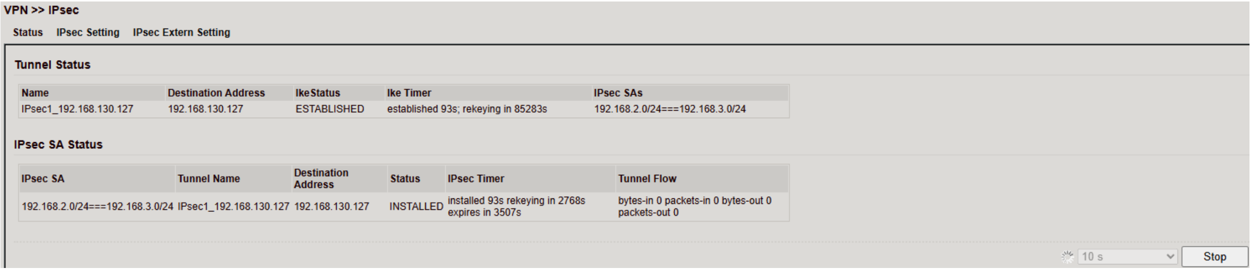
5.8.1 IPsec

IPsec (Internet Protocol Security) is a protocol suite that secures communication at the network level by providing:

- Integrity
- Authentication
- Confidentiality
- Anti-replay protection

Status

If the tunnel is established, status shows active connection(s).



Tunnel Status

Name	Destination Address	IkeStatus	Ike Timer	IPsec SAs
IPsec1_192.168.130.127	192.168.130.127	ESTABLISHED	established 93s; rekeying in 85283s	192.168.2.0/24===192.168.3.0/24

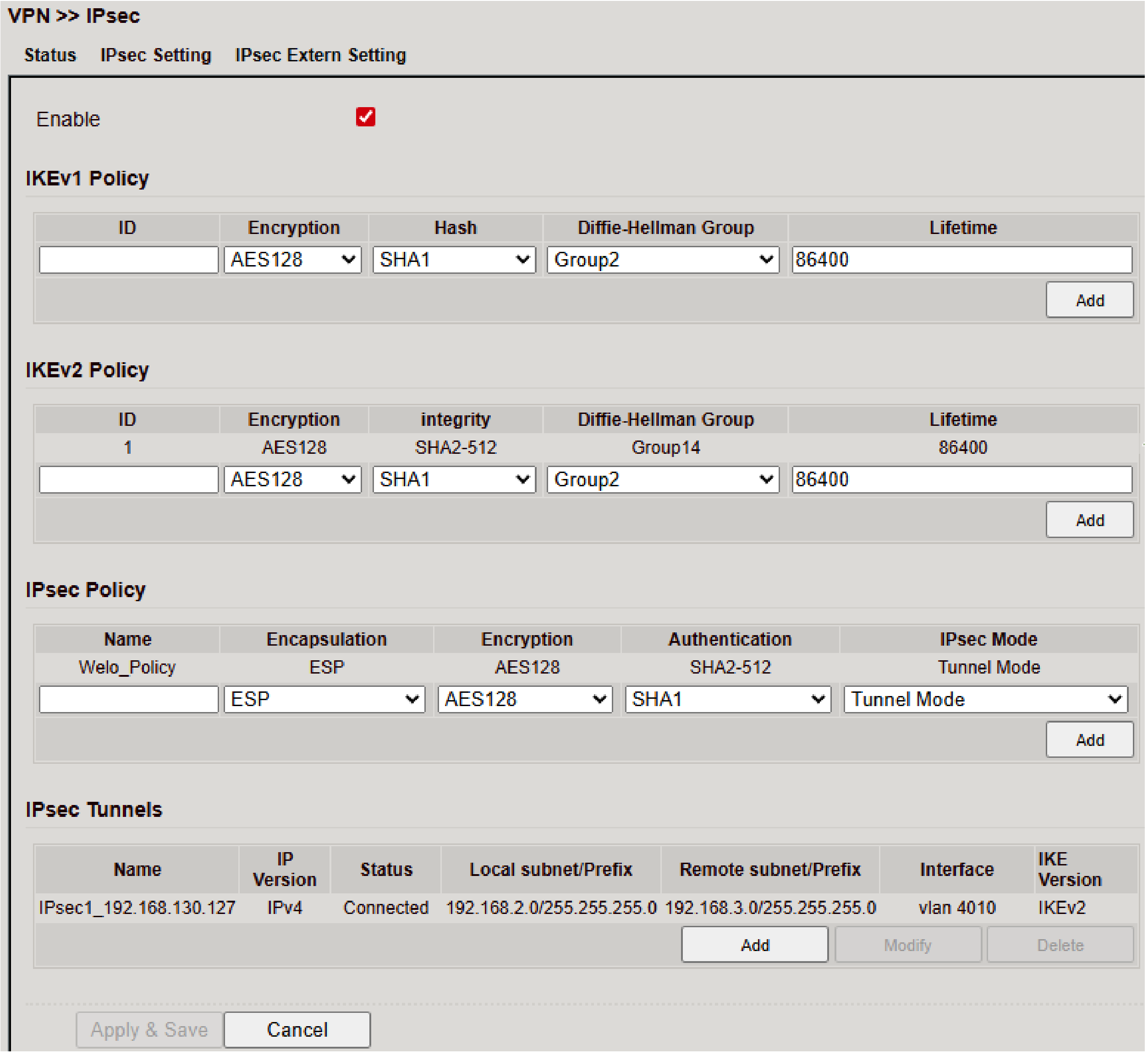
IPsec SA Status

IPsec SA	Tunnel Name	Destination Address	Status	IPsec Timer	Tunnel Flow
192.168.2.0/24===192.168.3.0/24	IPsec1_192.168.130.127	192.168.130.127	INSTALLED	installed 93s rekeying in 2768s expires in 3507s	bytes-in 0 packets-in 0 bytes-out 0 packets-out 0

IPsec Setting

Configure under **VPN > IPsec > IPsec Setting**.
Steps:

1. Create **IKE policy** (v1 or v2).
2. Create **IPsec policy**.
3. Save via **Apply & Save**.
4. Create the actual **IPsec tunnel**.



VPN >> IPsec

Enable ☑

IKEv1 Policy

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

IKEv2 Policy

ID	Encryption	integrity	Diffie-Hellman Group	Lifetime
1	AES128	SHA2-512	Group14	86400
	AES128	SHA1	Group2	86400

IPsec Policy

Name	Encapsulation	Encryption	Authentication	IPsec Mode
Welo_Policy	ESP	AES128	SHA2-512	Tunnel Mode
	ESP	AES128	SHA1	Tunnel Mode

IPsec Tunnels

Name	IP Version	Status	Local subnet/Prefix	Remote subnet/Prefix	Interface	IKE Version
IPsec1_192.168.130.127	IPv4	Connected	192.168.2.0/255.255.255.0	192.168.3.0/255.255.255.0	vlan 4010	IKEv2

IKEv1 Policy

Parameter	Description
ID	Unique identifier (integer)
Encryption	Selected encryption method
Hash	Hash algorithm
Diffie-Hellman Group	DH group for key exchange
Lifetime	Validity period before renegotiation

IKEv2 Policy

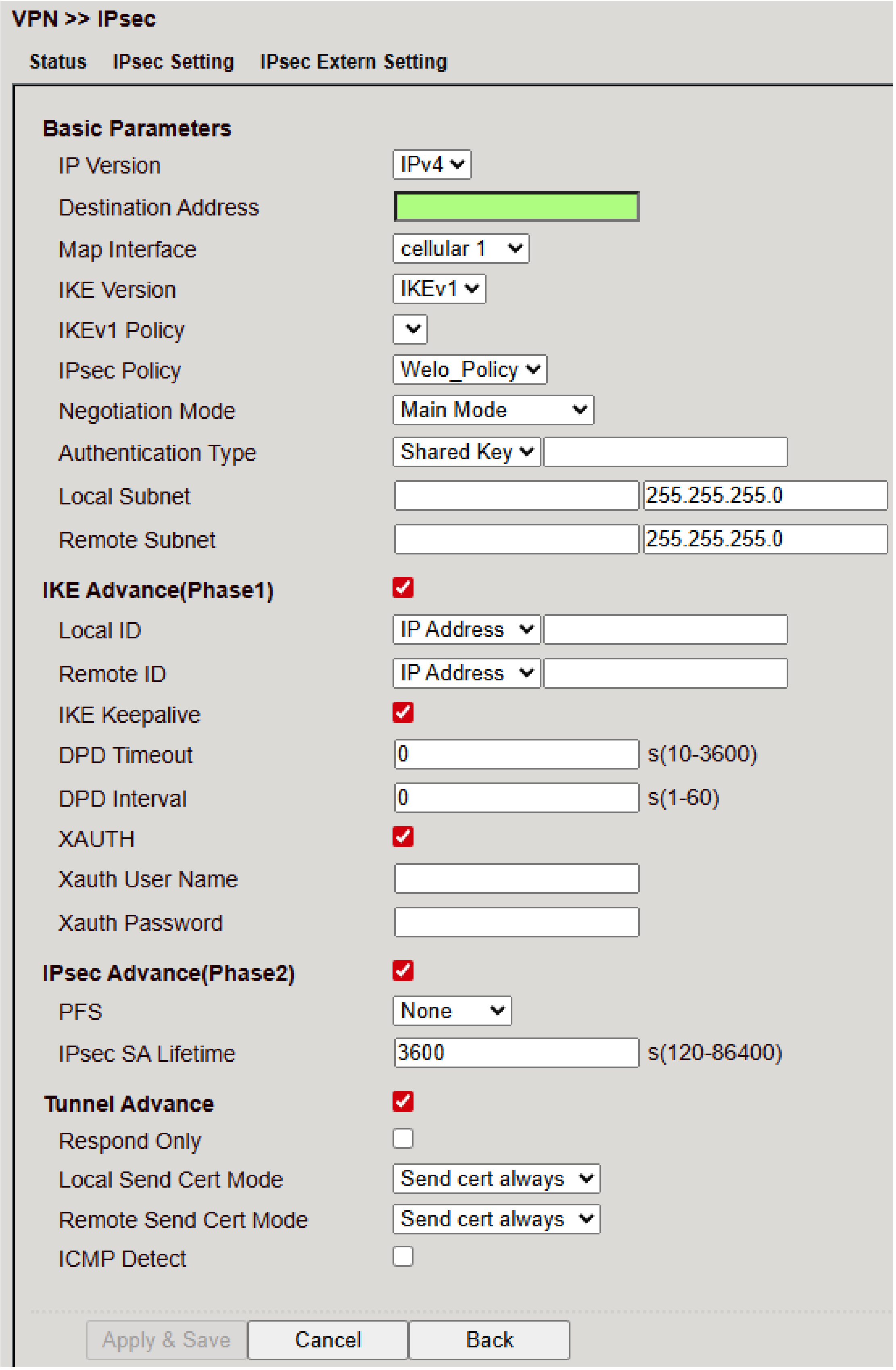
Parameter	Description
ID	Unique identifier (integer)
Encryption	Selected encryption method
Hash	Hash algorithm
Diffie-Hellman Group	DH group for key exchange
Lifetime	Validity period before renegotiation

IPsec Policy

Parameter	Description
Name	Identifier for the policy
Encapsulation	ESP or AH
Encryption	Encryption method
Authentication	Hash algorithm
IPsec Mode	Tunnel or Transport mode

IPsec Tunnel

Create tunnel under **VPN > IPsec > IPsec Setting > IPsec Tunnels**.
☒ Requires existing IKE (v1/v2) and IPsec policy.



VPN >> IPsec

Basic Parameters

IP Version	IPv4
Destination Address	🟩
Map Interface	cellular 1
IKE Version	IKEv1
IKEv1 Policy	
IPsec Policy	Welo_Policy
Negotiation Mode	Main Mode
Authentication Type	Shared Key
Local Subnet	255.255.255.0
Remote Subnet	255.255.255.0
IKE Advance(Phase1)	☑
Local ID	IP Address
Remote ID	IP Address
IKE Keepalive	☑
DPD Timeout	0 s(10-3600)
DPD Interval	0 s(1-60)
XAUTH	☑
Xauth User Name	
Xauth Password	
IPsec Advance(Phase2)	☑
PFS	None
IPsec SA Lifetime	3600 s(120-86400)
Tunnel Advance	☑
Respond Only	□
Local Send Cert Mode	Send cert always
Remote Send Cert Mode	Send cert always
ICMP Detect	□

Basic Parameters

Parameter	Description
Destination Address	Remote peer IP
Map Interface	Local interface used
IKE Version	IKEv1 or IKEv2
IKEv1 Policy	ID of the previously created IKEv1 policy
IPsec Policy	Name of the IPsec policy
Negotiation Mode	Main Mode or Aggressive Mode
Authentication Type	Shared Key or Certificate
Local Subnet	Local LAN subnet
Remote Subnet	Remote LAN subnet

IKE Advanced (Phase 1)

Parameter	Description
Local ID	IP Address, FQDN or User FQDN
Remote ID	IP Address, FQDN or User FQDN
IKE Keepalive	Enable/disable IKE Keepalive
DPD Timeout	Timeout for a Dead Peer Detection packet
DPD Interval	Interval of DPD packets
XAUTH	Enable/disable Extended Authentication
XAUTH Username	Username for XAUTH
XAUTH Password	Password for XAUTH

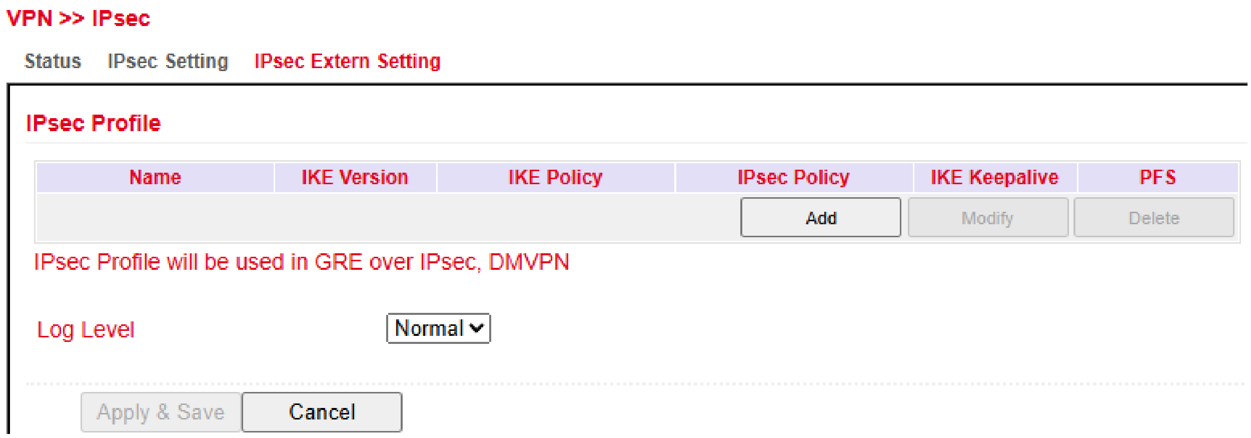
IPsec Advanced (Phase 2)

Parameter	Description
PFS	Perfect Forward Secrecy group
IPsec SA Lifetime	Validity period of Security Association before renewal
IPsec SA Idletime	Time before inactive SAs are deleted (prior to global lifetime)

Tunnel Advanced Parameters

Parameter	Description
Tunnel Start Mode	Default = Automatic
Local Send Cert Mode	Defines when to send the certificate
Remote Send Cert Mode	Defines when the peer must send its certificate
ICMP Detect	Enable/disable ICMP watchdog
ICMP Detection Server	Server used to test tunnel reachability (reachable only via tunnel)
ICMP Detection Local IP	Local router interface IP
ICMP Detection Interval	Interval for ICMP tests
ICMP Detection Timeout	Timeout for ICMP responses
ICMP Detection Max Retries	Maximum retries after failed ICMP pings

IPsec External Setting



VPN >> IPsec

Status IPsec Setting IPsec Extern Setting

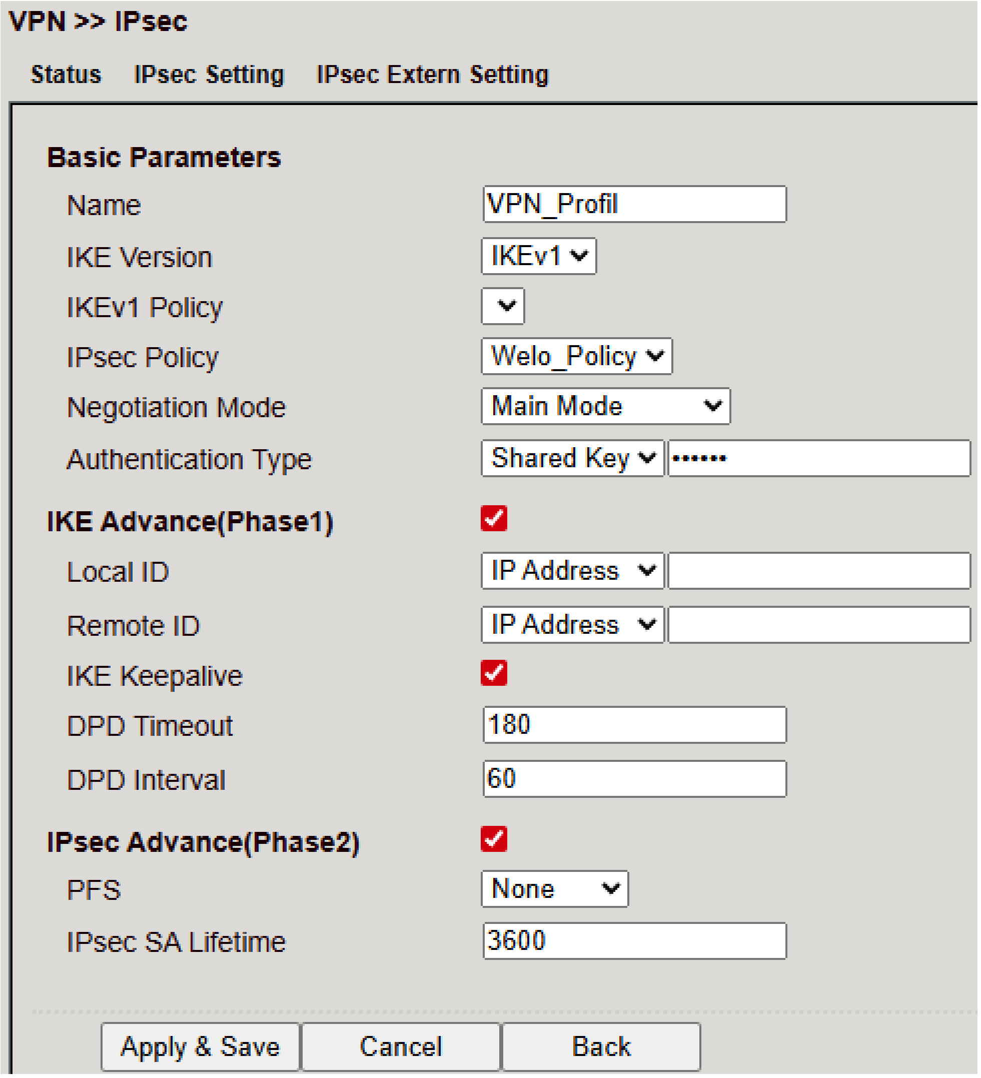
IPsec Profile

Name	IKE Version	IKE Policy	IPsec Policy	IKE Keepalive	PFS

IPsec Profile will be used in GRE over IPsec, DMVPN

Log Level: Normal

Profiles are required for **GRE over IPsec**. Create a profile with **Add**.



VPN >> IPsec

Basic Parameters

Name	VPN_Profil
IKE Version	IKEv1
IKEv1 Policy	
IPsec Policy	Welo_Policy
Negotiation Mode	Main Mode
Authentication Type	Shared Key ●●●●●●
IKE Advance(Phase1)	☑
Local ID	IP Address
Remote ID	IP Address
IKE Keepalive	☑
DPD Timeout	180
DPD Interval	60
IPsec Advance(Phase2)	☑
PFS	None
IPsec SA Lifetime	3600

Parameter	Description
Name	Unique profile name
IKE Version	IKEv1 or IKEv2
IKEv1 Policy	ID of the IKEv1 policy
IPsec Policy	Name of the IPsec policy
Negotiation Mode	Main or Aggressive
Authentication	Shared Key or Certificate

IKE Advanced (Phase 1)

Parameter	Description
Local ID	IP Address, FQDN, or User FQDN
Remote ID	IP Address, FQDN, or User FQDN
IKE Keepalive	Enable/disable Keepalive
DPD Timeout	Timeout for DPD packet
DPD Interval	Interval for DPD packets

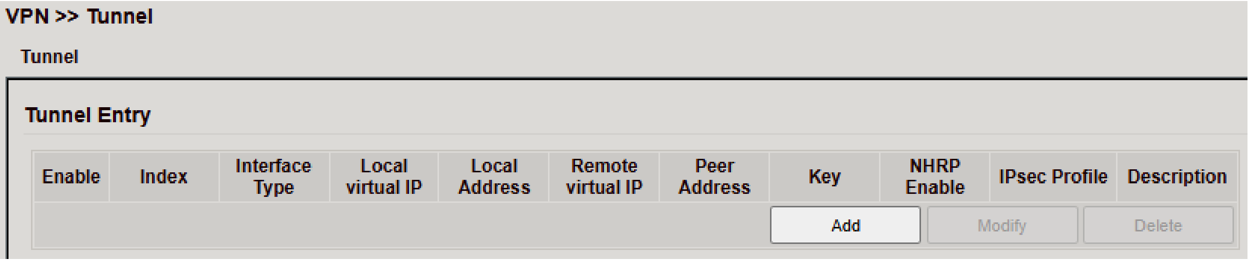
IPsec Advanced (Phase 2)

Parameter	Description
PFS	Perfect Forward Secrecy group
IPsec SA Lifetime	Validity period before SA is recreated
Fail Times to Restart Interface	Failed attempts before restarting interface
Fail Times to Reboot	Failed attempts before router reboot

5.8.2 Tunnel

VPN tunnels enable secure communication between networks or devices.

Tunnel Entry



VPN >> Tunnel

Tunnel

Tunnel Entry

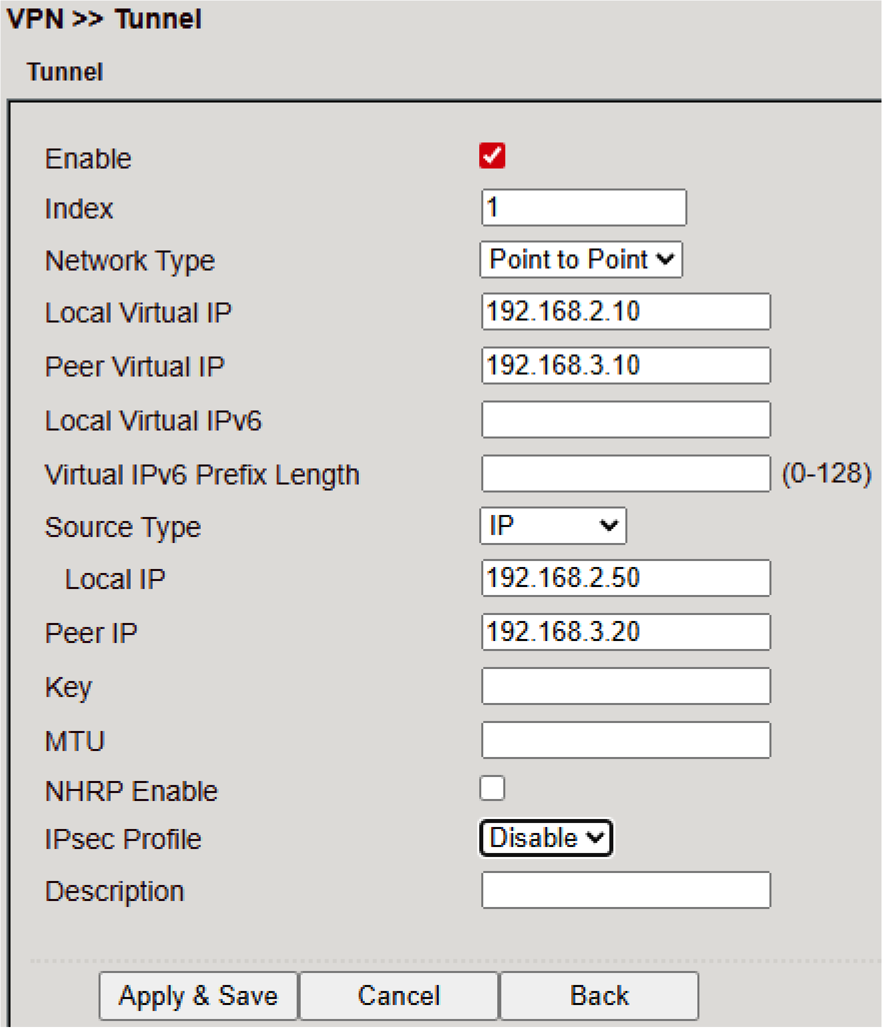
Enable	Index	Interface Type	Local virtual IP	Local Address	Remote virtual IP	Peer Address	Key	NHRP Enable	IPsec Profile	Description

Overview table shows:

- Interface Type
- Local/Remote Virtual IP
- Peer Address
- IPsec Profile
- Description

Use **Add** to create, or **Modify/Delete** to manage.

Tunnel Configuration



VPN >> Tunnel

Tunnel

Enable	☑
Index	1
Network Type	Point to Point
Local Virtual IP	192.168.2.10
Peer Virtual IP	192.168.3.10
Local Virtual IPv6	
Virtual IPv6 Prefix Length	(0-128)
Source Type	IP
Local IP	192.168.2.50
Peer IP	192.168.3.20
Key	
MTU	
NHRP Enable	□
IPsec Profile	Disable
Description	

Options when adding/editing:

- **Enable** – Activate tunnel
- **Index** – Unique identifier
- **Network Type** – e.g. Point-to-Point
- **Local/Peer Virtual IP** – Virtual tunnel endpoints
- **Local/Peer IP** – Physical endpoints
- **Key** – Shared key if required
- **MTU** – Max transmission unit
- **NHRP Enable** – Enable Next Hop Resolution Protocol
- **IPsec Profile** – Select encryption/auth profile
- **Description** – Optional

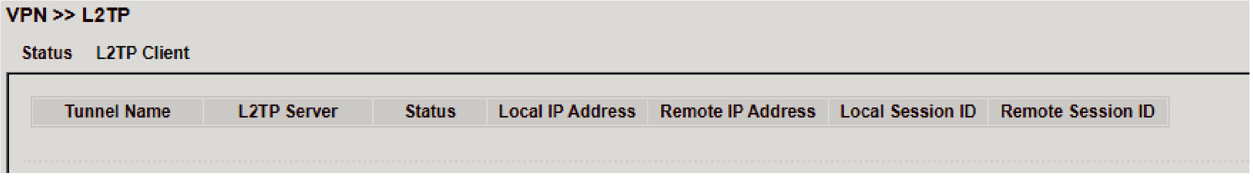
Click **Apply & Save** to activate.

5.8.3 L2TP

L2TP (Layer 2 Tunneling Protocol) combines **PPTP** and **L2F**.

- Provides tunneling, but **no encryption** → must be paired with IPsec.
- Often used for single-user connections (road warrior).

L2TP Status



VPN >> L2TP

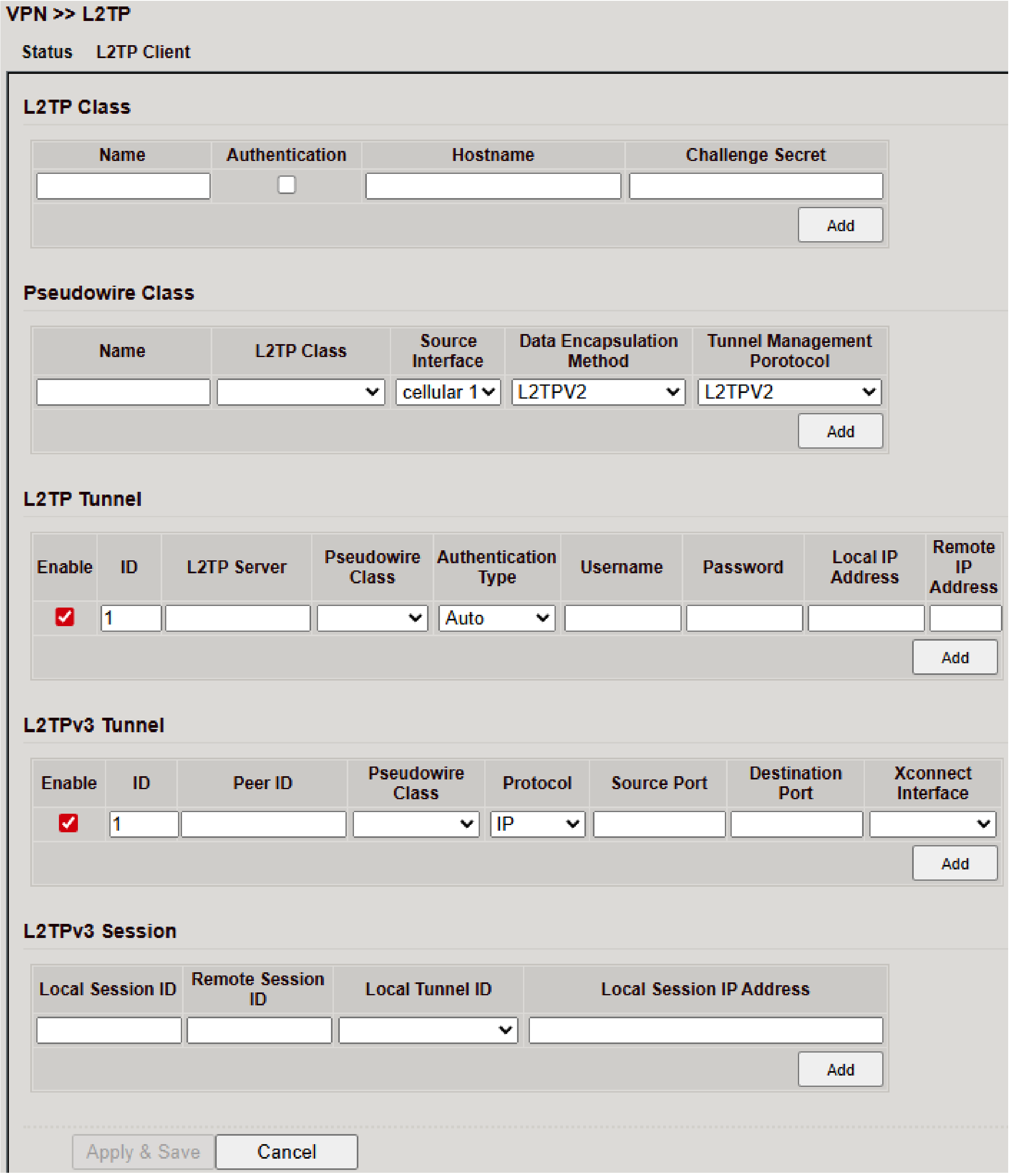
Status   L2TP Client

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

L2TP Client

Configure under **VPN > L2TP > L2TP Client**.

- Add entries via **Add**
- Save with **Apply & Save**



VPN >> L2TP

Status L2TP Client

L2TP Class

Name	Authentication	Hostname	Challenge Secret
	☐		

Add

Pseudowire Class

Name	L2TP Class	Source Interface	Data Encapsulation Method	Tunnel Management Porotocol
		cellular 1	L2TPV2	L2TPV2

Add

L2TP 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

Apply & Save Cancel

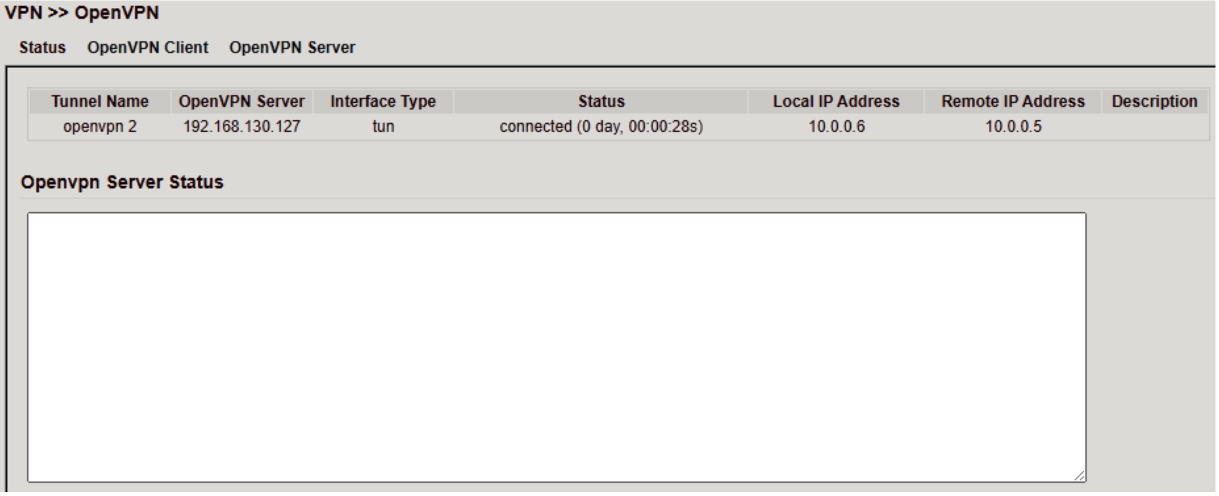
5.8.4 OpenVPN

OpenVPN is open-source VPN software using **TLS/SSL** encryption.

- Transport: UDP or TCP
- Encryption via **OpenSSL**

OpenVPN Status

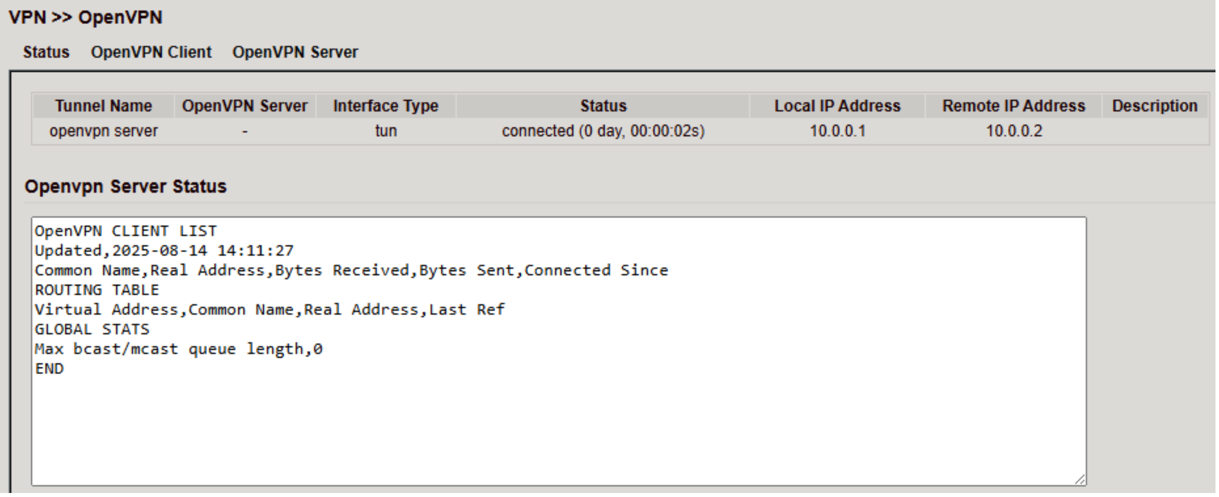
- **Client Status**



Tunnel Name	OpenVPN Server	Interface Type	Status	Local IP Address	Remote IP Address	Description
openvpn 2	192.168.130.127	tun	connected (0 day, 00:00:28s)	10.0.0.6	10.0.0.5	

Openvpn Server Status

- **Server Status**



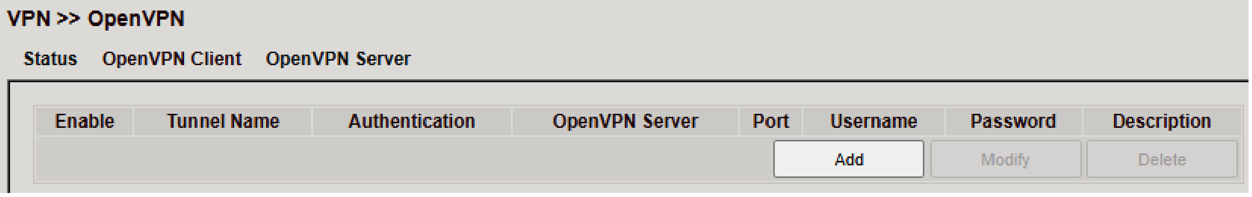
Tunnel Name	OpenVPN Server	Interface Type	Status	Local IP Address	Remote IP Address	Description
openvpn server	-	tun	connected (0 day, 00:00:02s)	10.0.0.1	10.0.0.2	

Openvpn Server Status

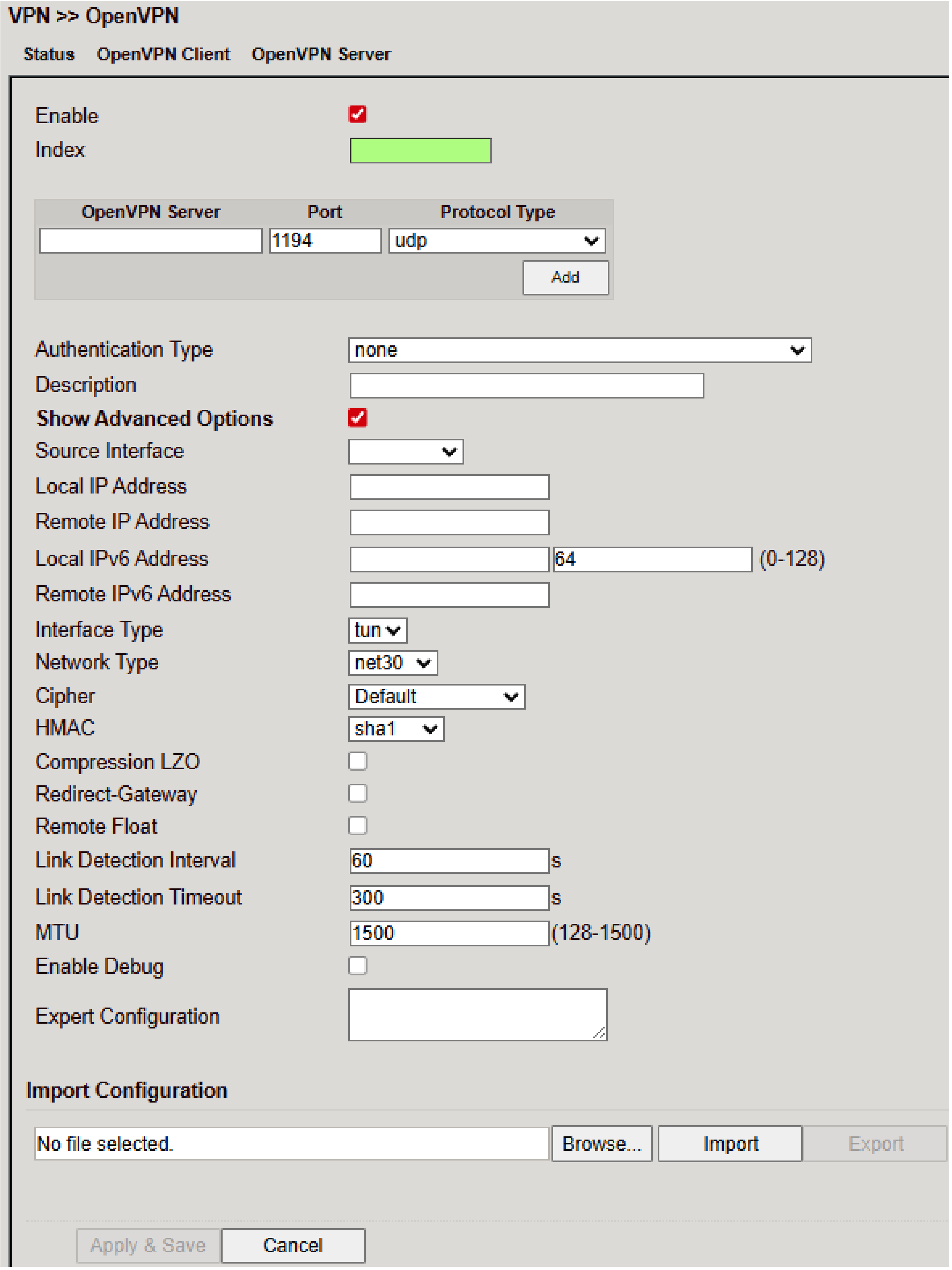
```
OpenVPN CLIENT LIST
Updated,2025-08-14 14:11:27
Common Name,Real Address,Bytes Received,Bytes Sent,Connected Since
ROUTING TABLE
Virtual Address,Common Name,Real Address,Last Ref
GLOBAL STATS
Max bcast/mcast queue length,0
END
```

OpenVPN Client

Configure under **VPN > OpenVPN > OpenVPN Client**.
Create a new tunnel with **Add**.



Enable	Tunnel Name	Authentication	OpenVPN Server	Port	Username	Password	Description



VPN >> OpenVPN

Enable	☑
Index	🟩

OpenVPN Server	Port	Protocol Type
	1194	udp

Authentication Type	none
Description	
Show Advanced Options	☑
Source Interface	
Local IP Address	
Remote IP Address	
Local IPv6 Address	64 (0-128)
Remote IPv6 Address	
Interface Type	tun
Network Type	net30
Cipher	Default
HMAC	sha1
Compression LZO	□
Redirect-Gateway	□
Remote Float	□
Link Detection Interval	60 s
Link Detection Timeout	300 s
MTU	1500 (128-1500)
Enable Debug	□
Expert Configuration	

Import Configuration

No file selected.

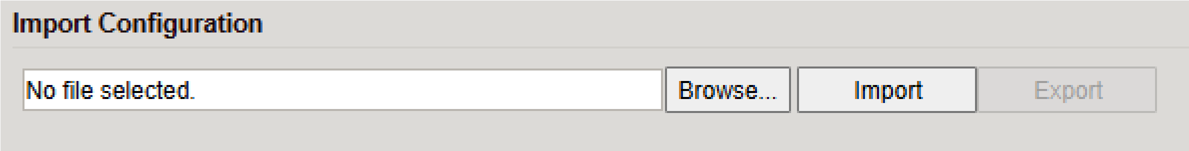
Parameters:

Parameter	Description
Enable	Enable/disable tunnel
Index	Identifier for tunnel
OpenVPN Server	IP/FQDN of OpenVPN server
Authentication Type	Method (recommended: `x509-cert`)
Username	Username
Password	Password
Description	Optional description

Show Advanced Options

Parameter	Description
Source Interface	Interface used for tunnel
Interface Type	`tun` (recommended) or `tap`
Cipher	Encryption method
HMAC	Signs TLS handshake packets (default: SHA1)
Compression LZO	Enable/disable data compression
Redirect-Gateway	Route all traffic via tunnel
Remote Float	Accept packets even if server IP changes (useful for dynamic IP servers)
Link Detection Interval	Interval for connection checks
Link Detection Timeout	Timeout for connection checks
MTU	Maximum packet size
TCPMSS	Maximum size for TCP packets
Fragment	Maximum packet size for UDP
Enable Debug	Enable/disable debug mode
Expert Configuration	Raw OpenVPN options not available via GUI

⊠ The client **always needs the server's CA certificate**.

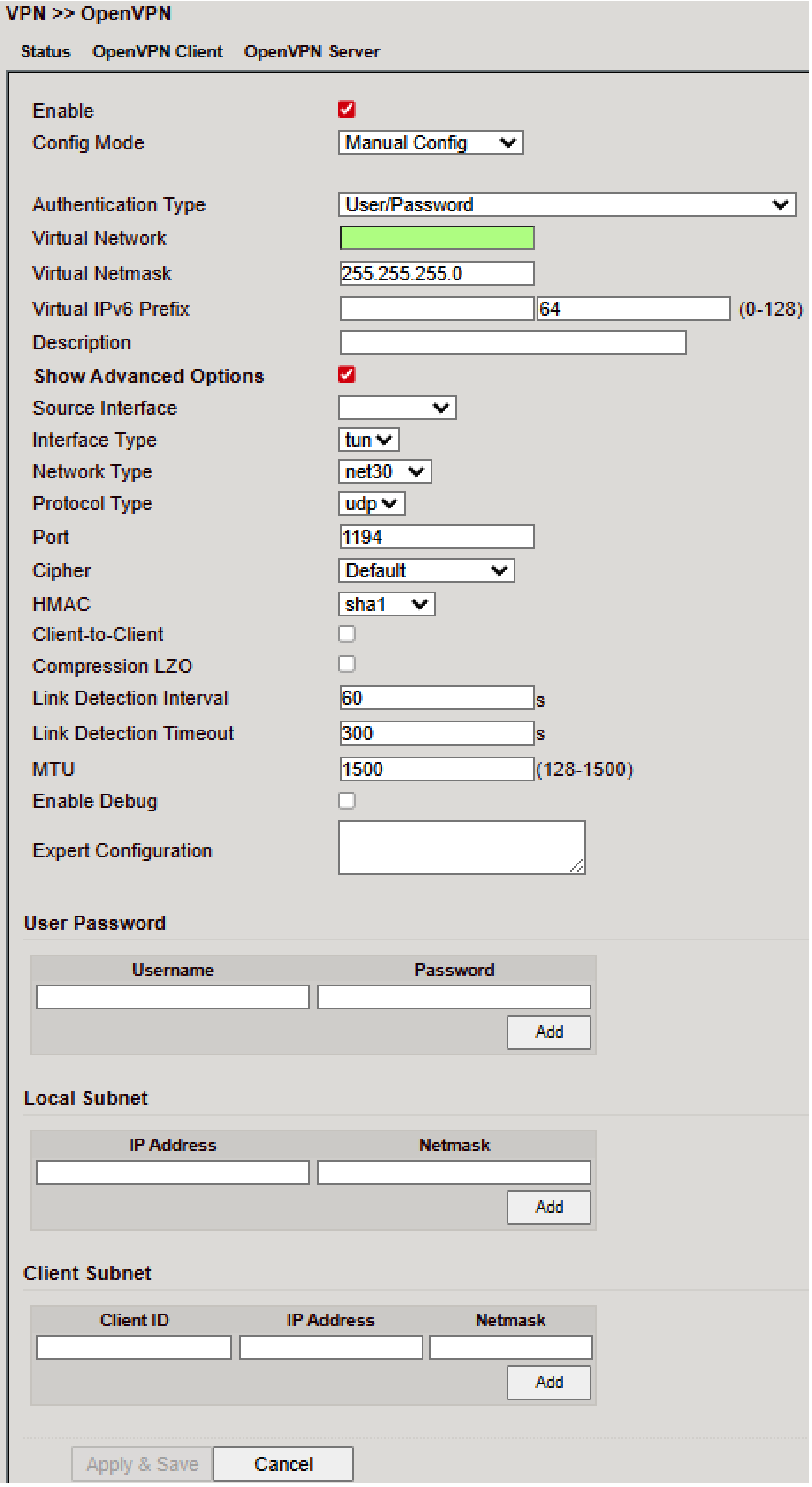

Import Configuration

No file selected.

You can **import/export** OpenVPN configurations (`.ovpn` files).
⊠ Avoid spaces in filenames.

5.8.5 OpenVPN Server

Configure under **VPN > OpenVPN > OpenVPN Server**.
☒ A **public IP** is required.



VPN >> OpenVPN

Enable	☑
Config Mode	Manual Config
Authentication Type	User/Password
Virtual Network	
Virtual Netmask	255.255.255.0
Virtual IPv6 Prefix	64 (0-128)
Description	
Show Advanced Options	☑
Source Interface	
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)
Enable Debug	☐
Expert Configuration	

User Password

Local Subnet

Client Subnet

Parameters:

Parameter	Description
Enable	Enable/disable OpenVPN server
Config Mode	Manual configuration or import of an existing config
Authentication Type	Authentication method
Virtual Network	Virtual subnet for VPN clients
Virtual Netmask	Subnet mask for the VPN network
Description	Optional description

Advanced Options

Parameter	Description
Source Interface	Interface over which the OpenVPN tunnel is established
Interface Type	`tun` or `tap` (recommended: `tun`)
Network Type	Connection type (recommended: `net30`)
Protocol Type	UDP or TCP
Port	Port on which the OpenVPN server listens
Cipher	Encryption method
HMAC	Hash-based Message Authentication Code
Client-to-Client	Enable/disable communication between clients
Compression LZO	Enable/disable compression
Link Detection Interval	Interval for tunnel connection checks
Link Detection Timeout	Timeout for tunnel connection check packets
MTU	Maximum packet size
TCPMSS	Maximum size for TCP packets
Fragment	Maximum packet size for UDP packets
Enable Debug	Enable/disable debug mode
Expert Configuration	Enter custom OpenVPN options not available via web interface

User Password

Clients can be added here. Each client logs in with a **username** and **password**.

Local Subnet

Defines which **local subnets** of the router are accessible for clients.

Client Subnet

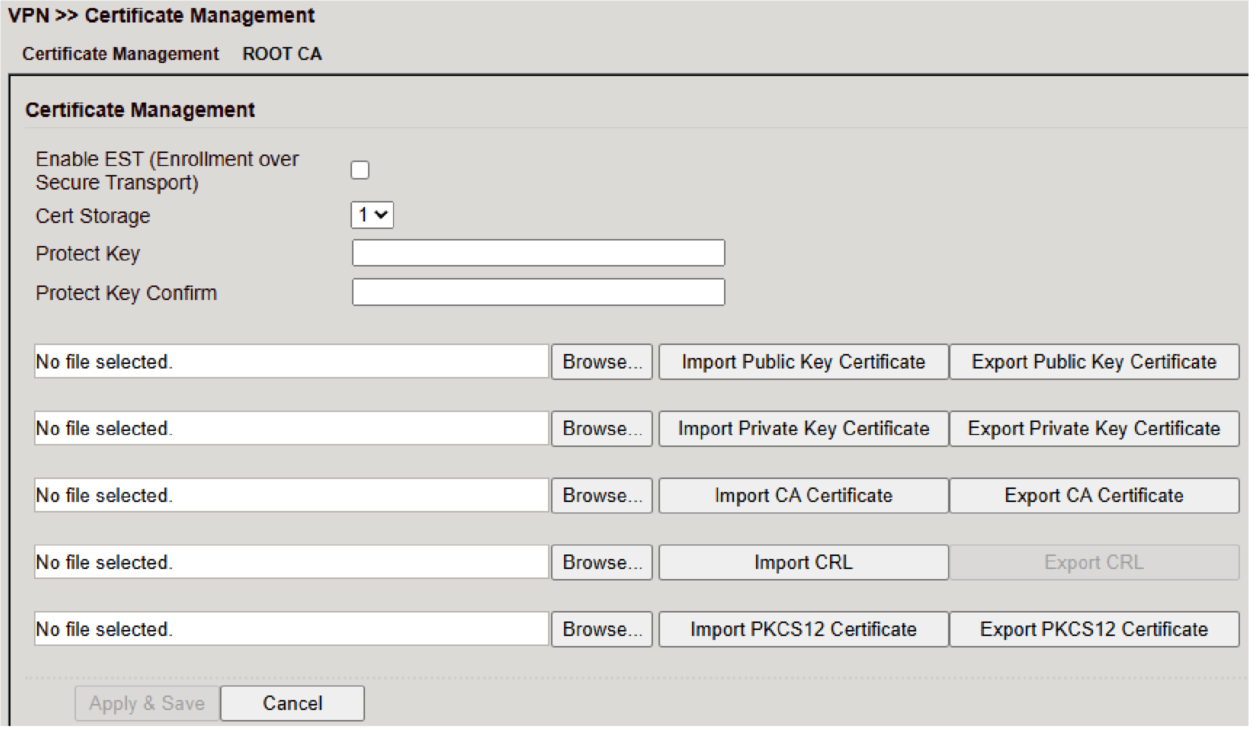
Defines which **client subnets** are accessible from the server.

- **Client ID** = Username (for User/Password auth) or CN (for certificate auth).

⊠ The OpenVPN server **requires a CA certificate, public key and private key** (uploaded under *VPN > Certificate Management*).
If these are missing, the server will not start.

5.8.6 Certificate Management

Used to store certificates for IPsec and OpenVPN (unless using PSK).



VPN >> Certificate Management

Certificate Management   ROOT CA

Certificate Management

Enable EST (Enrollment over Secure Transport) □

Cert Storage: 1

Protect Key:

Protect Key Confirm:

No file selected.

No file selected.

No file selected.

No file selected.

No file selected.

Browse...
Import Public Key Certificate
Export Public Key Certificate
Browse...
Import Private Key Certificate
Export Private Key Certificate
Browse...
Import CA Certificate
Export CA Certificate
Browse...
Import CRL
Export CRL
Browse...
Import PKCS12 Certificate
Export PKCS12 Certificate
Apply & Save
Cancel

1. Click **Browse**, select the certificate file and **Import**.
2. Use **Export** to verify upload (file size > 0 bytes).
   - If upload fails, try another browser/PC.
3. If importing a **PKCS12** set with password → enter password in **Protect Key** + **Protect Key Confirm**.
4. Click **Apply & Save**.

Parameter	Description
Enable SCEP	Enable Simple Certificate Enrollment Protocol for auto-rollout
Protect Key / Confirm	Password for password-protected certificates
Revocation	Enable certificate revocation list (CRL)
Import Public Key Certificate	Upload public key certificate
Import Private Key Certificate	Upload private key certificate
Import CA Certificate	Upload Certificate Authority certificate
Import CRL	Upload Certificate Revocation List
Import PKCS12 Certificate	Upload PKCS12 certificate set

5.9 Industrial

Features:

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

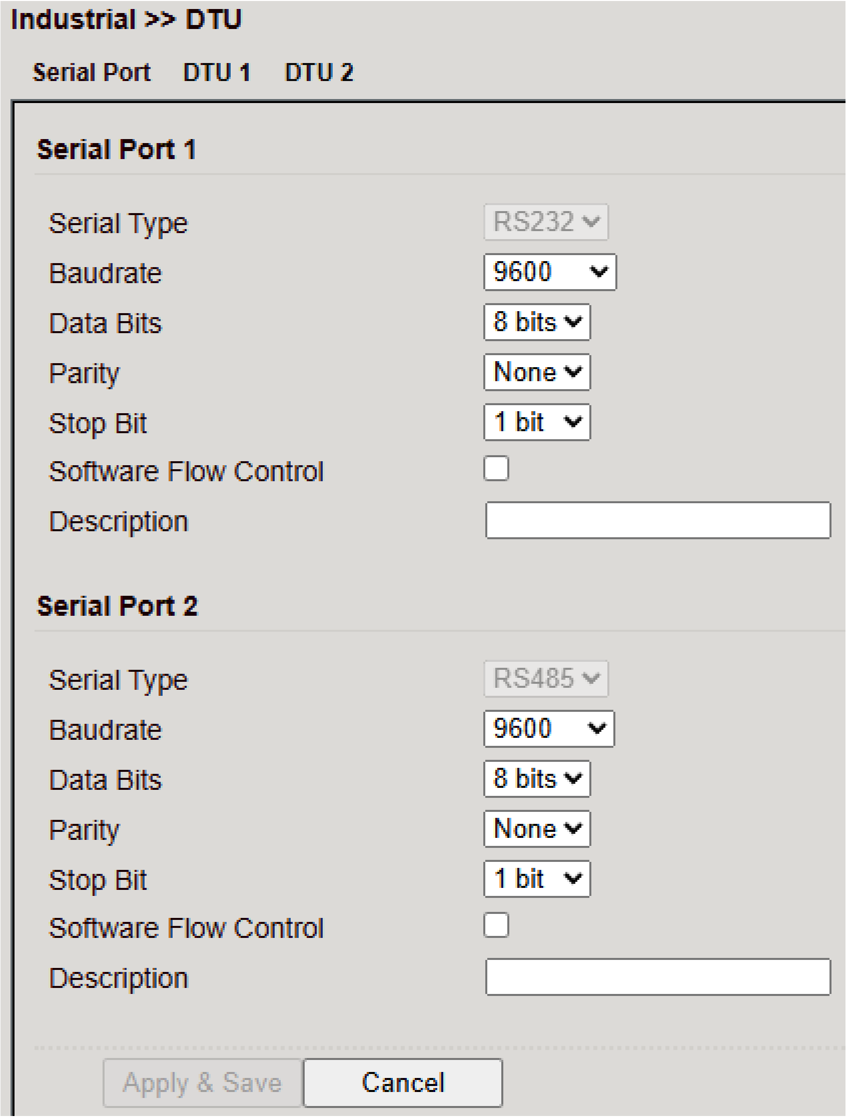
5.9.1 DTU (Data Terminal Unit)

Connects serial devices (RS-232, RS-485).
Configuration consists of two parts:

1. **Serial Port** properties (RS-232 / RS-485).
2. **DTU Protocol Parameters**.

Serial Port

Configure serial ports `1 (RS232)` and `2 (RS485)`.



Serial Port 1

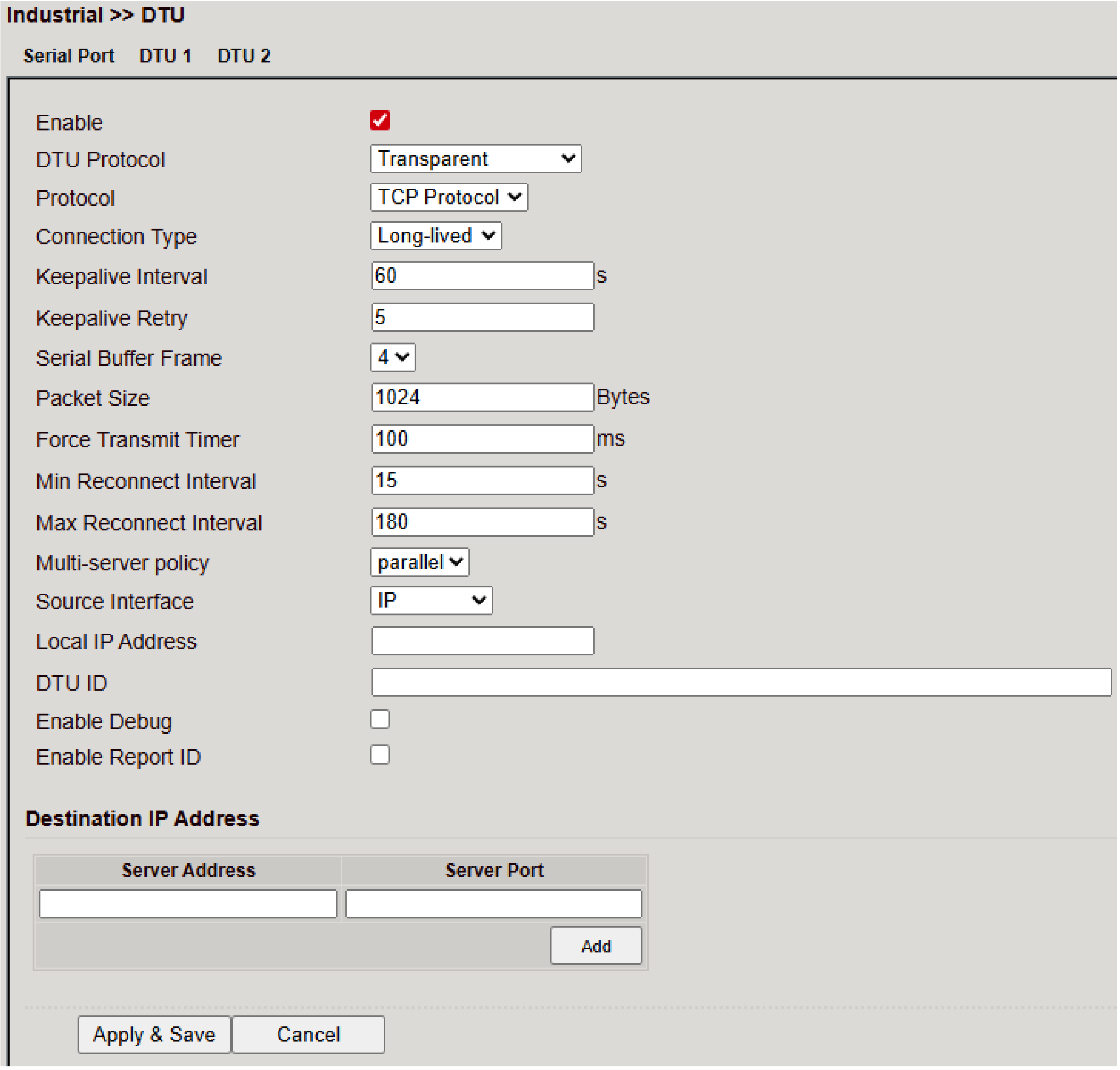
Serial Type	RS232
Baudrate	9600
Data Bits	8 bits
Parity	None
Stop Bit	1 bit
Software Flow Control	□
Description	

Serial Port 2

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

DTU Protocols

- Transparent Mode



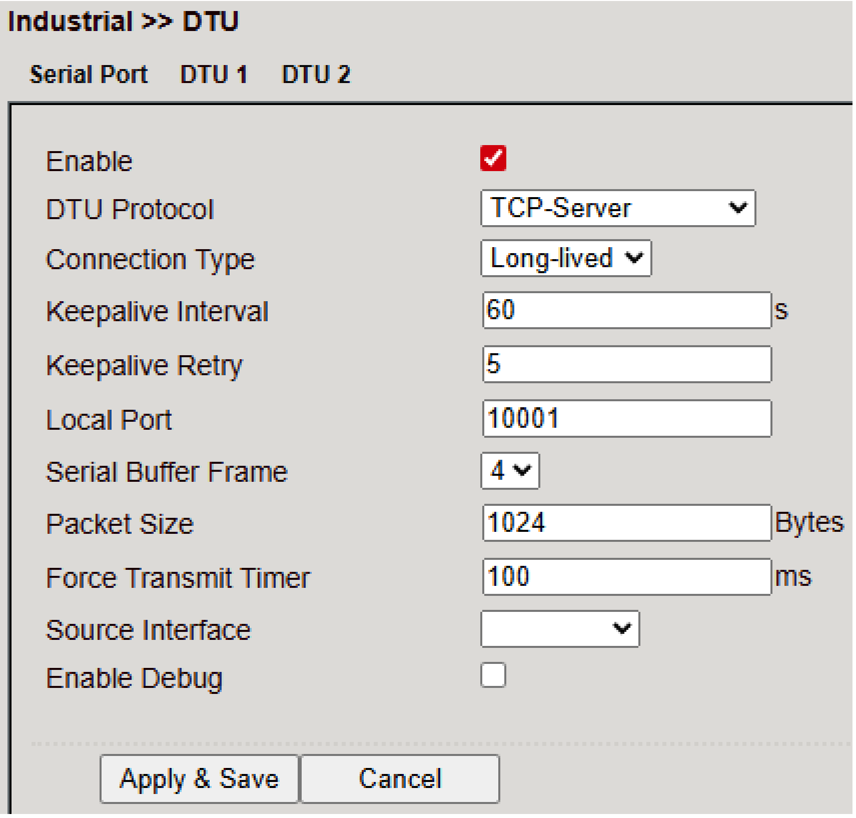
Industrial >> DTU

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

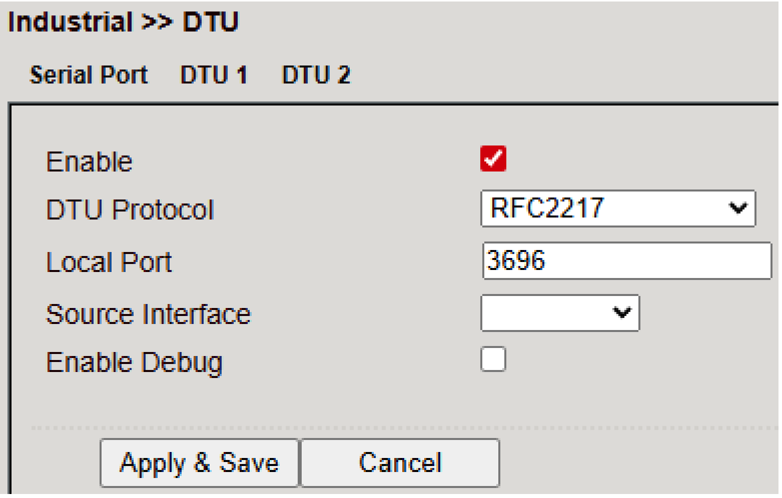
- TCP Server



Industrial >> DTU

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	
Enable Debug	□

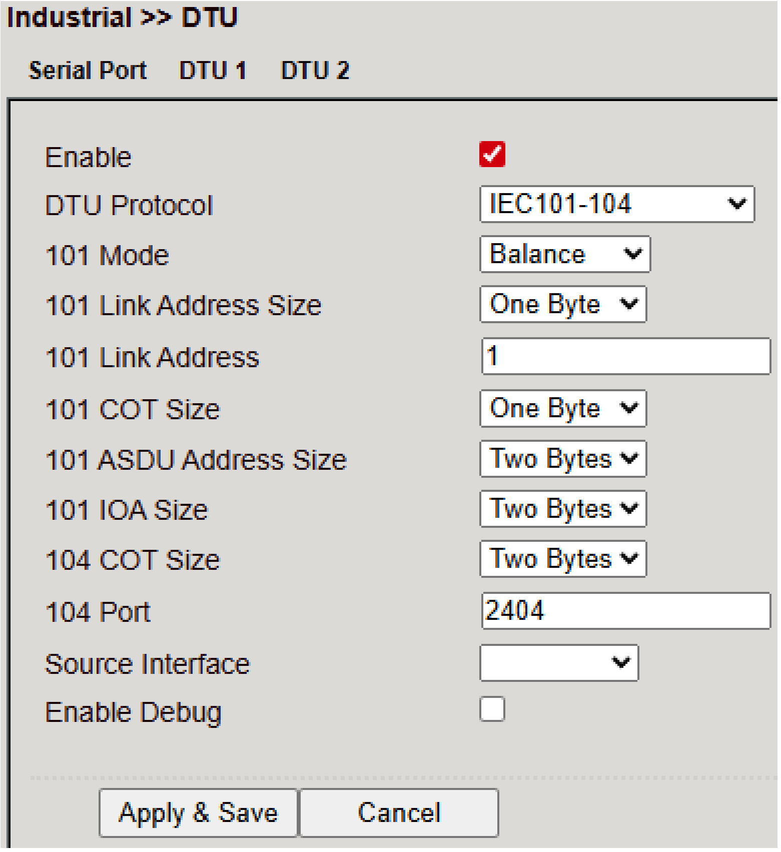
- RFC2217



Industrial >> DTU

Enable	☑
DTU Protocol	RFC2217
Local Port	3696
Source Interface	
Enable Debug	□

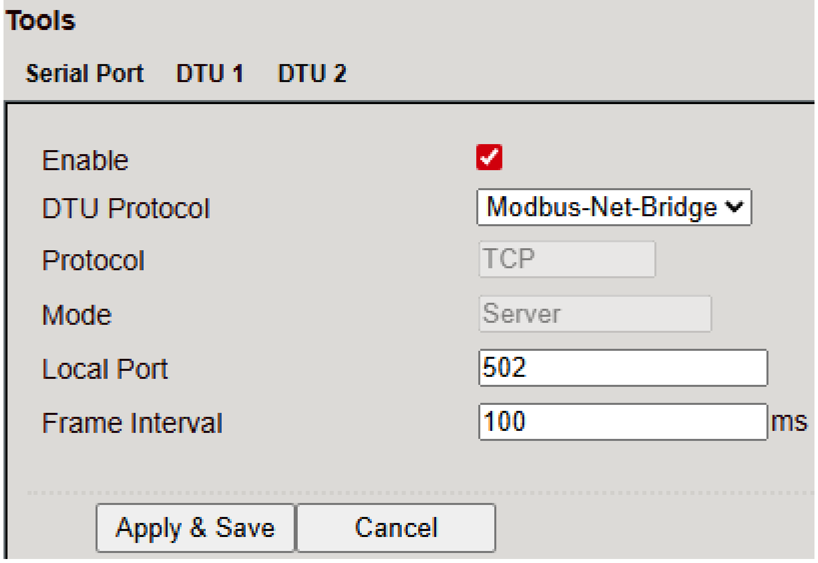
- IEC60870-5-101/104



Industrial >> DTU

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	□

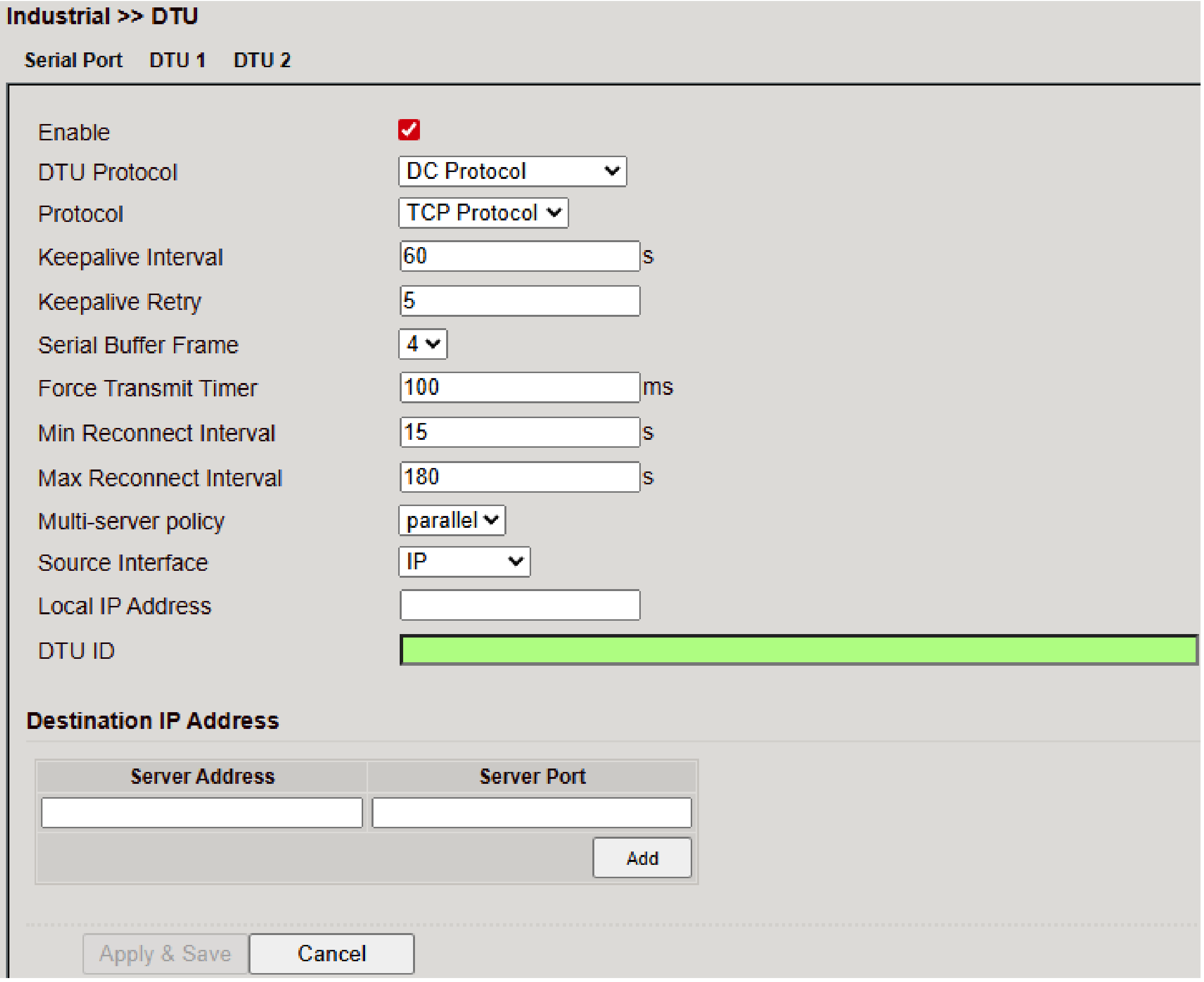
- Modbus-Net-Bridge



Tools

Enable	☑
DTU Protocol	Modbus-Net-Bridge
Protocol	TCP
Mode	Server
Local Port	502
Frame Interval	100 ms

- DC 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

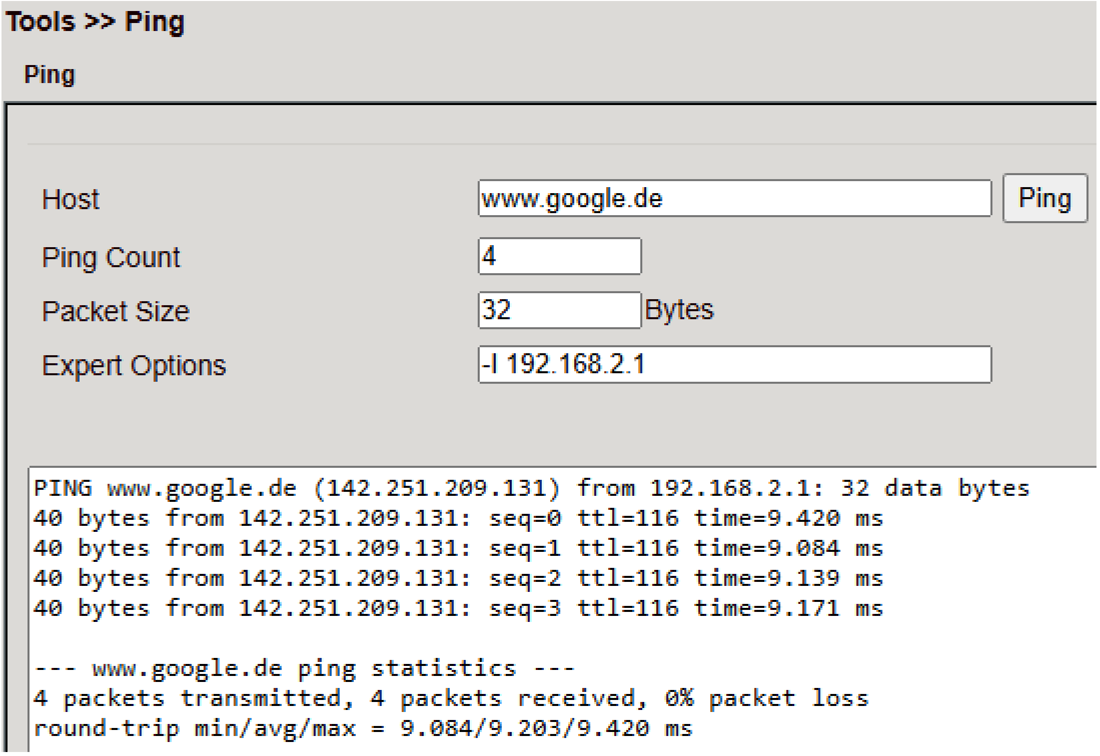
Server Address	Server Port

5.10 Tools

Utilities for diagnostics and network tests.

5.10.1 Ping

Send ICMP echo requests.



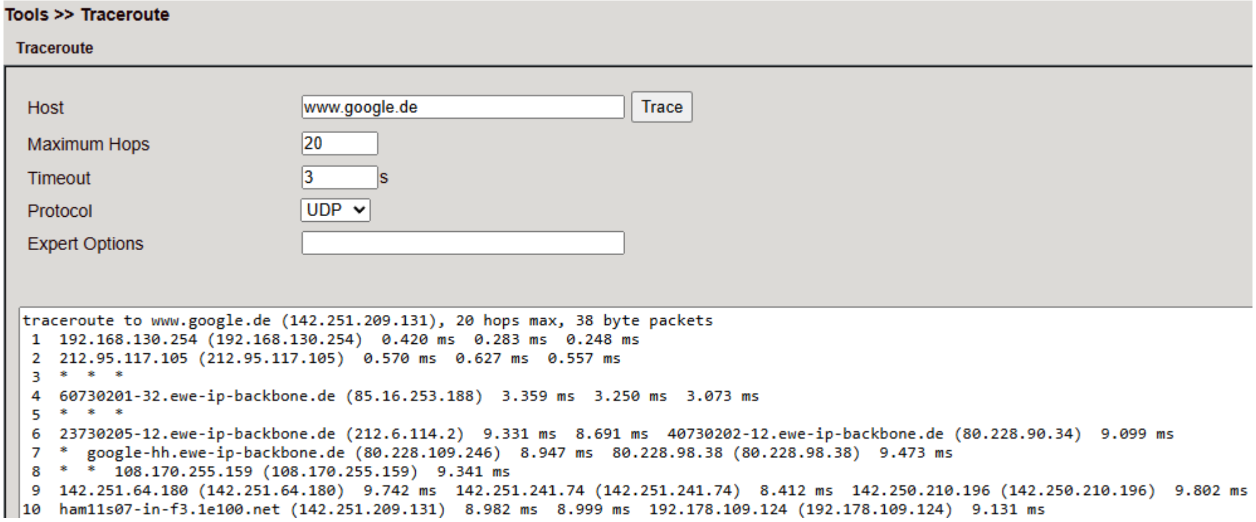
Host: www.google.de
Ping Count: 4
Packet Size: 32 Bytes
Expert Options: -I 192.168.2.1

```
PING www.google.de (142.251.209.131) from 192.168.2.1: 32 data bytes
40 bytes from 142.251.209.131: seq=0 ttl=116 time=9.420 ms
40 bytes from 142.251.209.131: seq=1 ttl=116 time=9.084 ms
40 bytes from 142.251.209.131: seq=2 ttl=116 time=9.139 ms
40 bytes from 142.251.209.131: seq=3 ttl=116 time=9.171 ms

--- www.google.de ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 9.084/9.203/9.420 ms
```

Parameter	Description
Host	Destination IP/hostname
Ping Count	Number of pings (1–50, default: 4)
Packet Size	Packet size (default: 32 bytes)
Expert Options	Additional advanced settings

5.10.2 Traceroute

Displays routing path to a host.



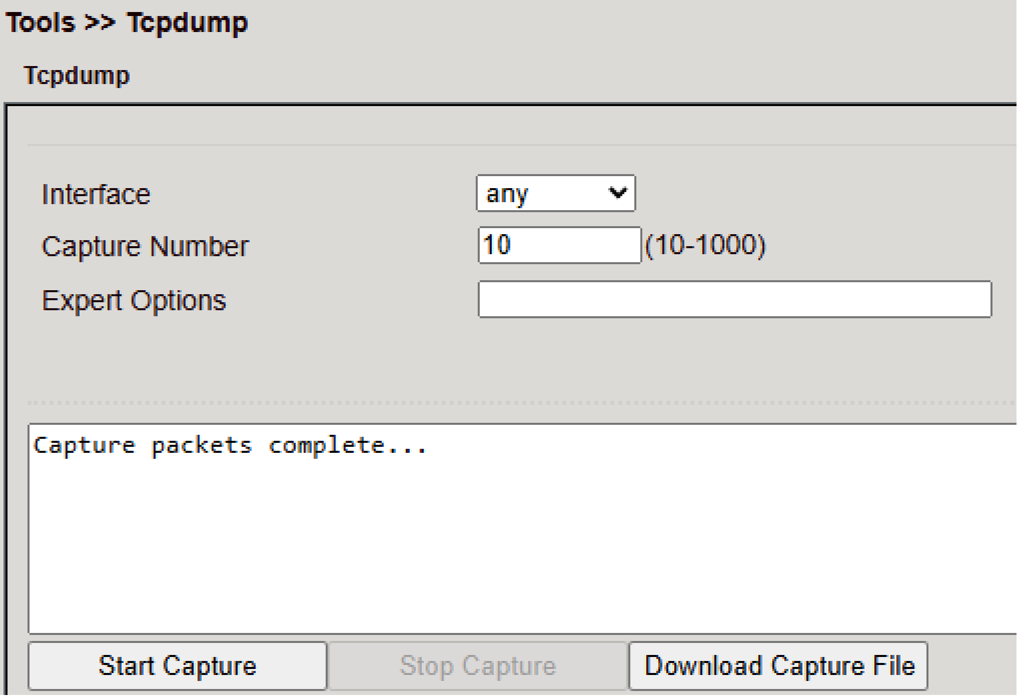
Host: www.google.de
Maximum Hops: 20
Timeout: 3 s
Protocol: UDP
Expert Options:

```
traceroute to www.google.de (142.251.209.131), 20 hops max, 38 byte packets
 1  192.168.130.254 (192.168.130.254)  0.420 ms  0.283 ms  0.248 ms
 2  212.95.117.105 (212.95.117.105)  0.570 ms  0.627 ms  0.557 ms
 3  *  *  *
 4  60730201-32.ewe-ip-backbone.de (85.16.253.188)  3.359 ms  3.250 ms  3.073 ms
 5  *  *  *
 6  23730205-12.ewe-ip-backbone.de (212.6.114.2)  9.331 ms  8.691 ms  40730202-12.ewe-ip-backbone.de (80.228.90.34)  9.099 ms
 7  *  google-hh.ewe-ip-backbone.de (80.228.109.246)  8.947 ms  80.228.98.38 (80.228.98.38)  9.473 ms
 8  *  *  108.170.255.159 (108.170.255.159)  9.341 ms
 9  142.251.64.180 (142.251.64.180)  9.742 ms  142.251.241.74 (142.251.241.74)  8.412 ms  142.250.210.196 (142.250.210.196)  9.802 ms
10  ham11s07-in-f3.1e100.net (142.251.209.131)  8.982 ms  8.999 ms  192.178.109.124 (192.178.109.124)  9.131 ms
```

Parameter	Description
Host	Destination IP/hostname
Maximum Hops	Hop limit (2–40, default: 20)
Timeout	Timeout per hop (2–10s)
Protocol	ICMP or UDP (default: UDP)
Expert Options	Advanced options

5.10.3 Tcpdump

Packet sniffer for TCP/UDP analysis.



Tools >> Tcpdump

Tcpdump

Interface: any

Capture Number: 10 (10-1000)

Expert Options:

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

Parameter	Description
Interface	Interface to capture
Capture Number	Number of packets (default: 10)
Expert Options	Advanced options
Start Capture	Begin packet capture
Stop Capture	Stop packet capture
Download Capture File	Save capture as `.pcap` (analyze with Wireshark)

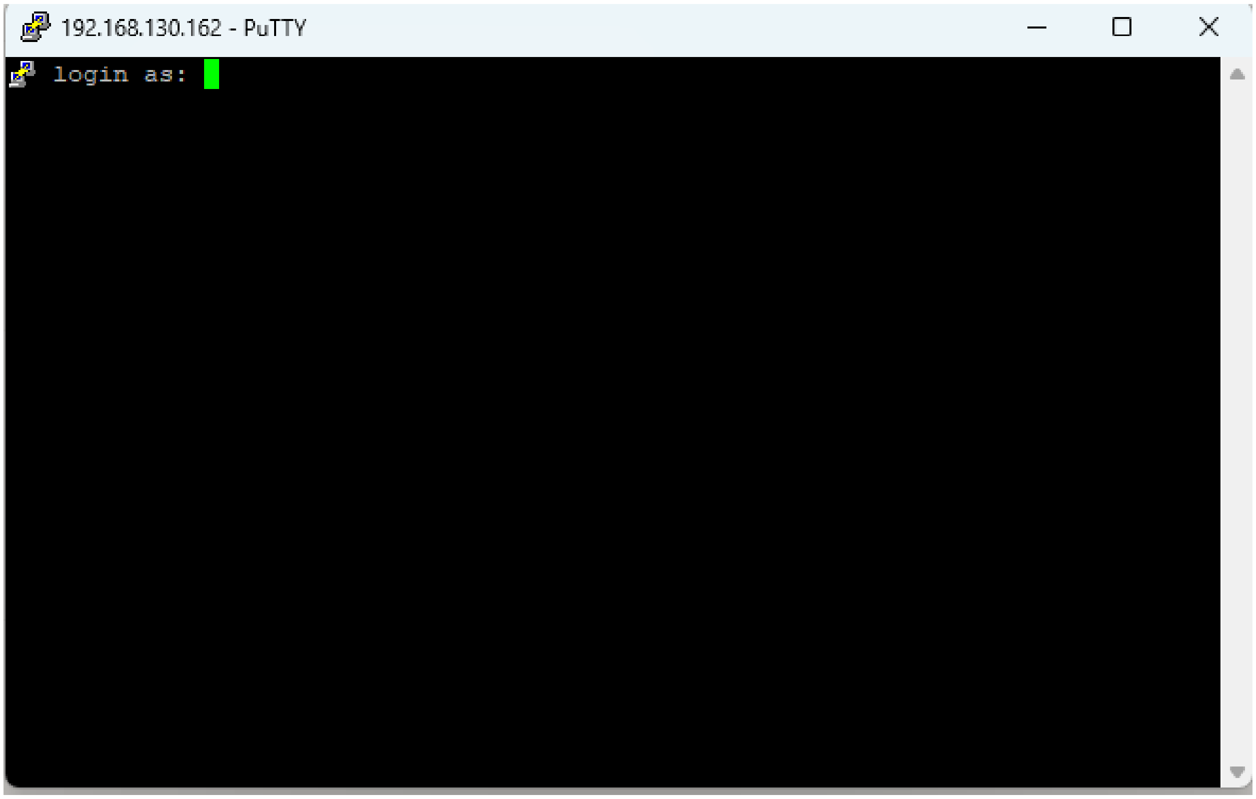
5.11 CLI Commands

The router can also be managed via **CLI (Command Line Interface)** using **SSH** or **Telnet**.

- Enable under **Administration > Management Services**.
- Use a terminal client such as **PuTTY**.

5.11.1 Connection

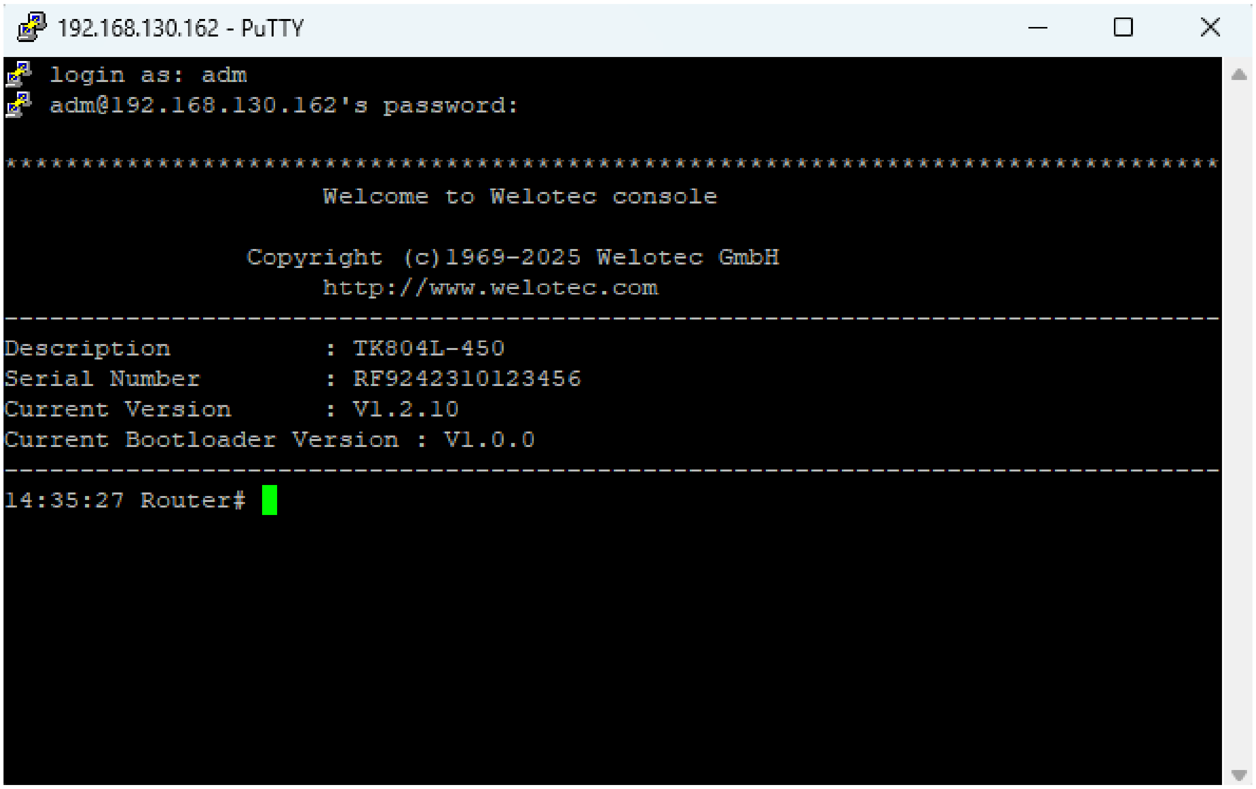
1. Enable SSH/Telnet in the router (**Apply & Save**).
2. Start PuTTY, enter router IP, select SSH/Telnet.
3. Connect.



```
login as:
```

Default login:

- User: `adm`
- Password: `123456`

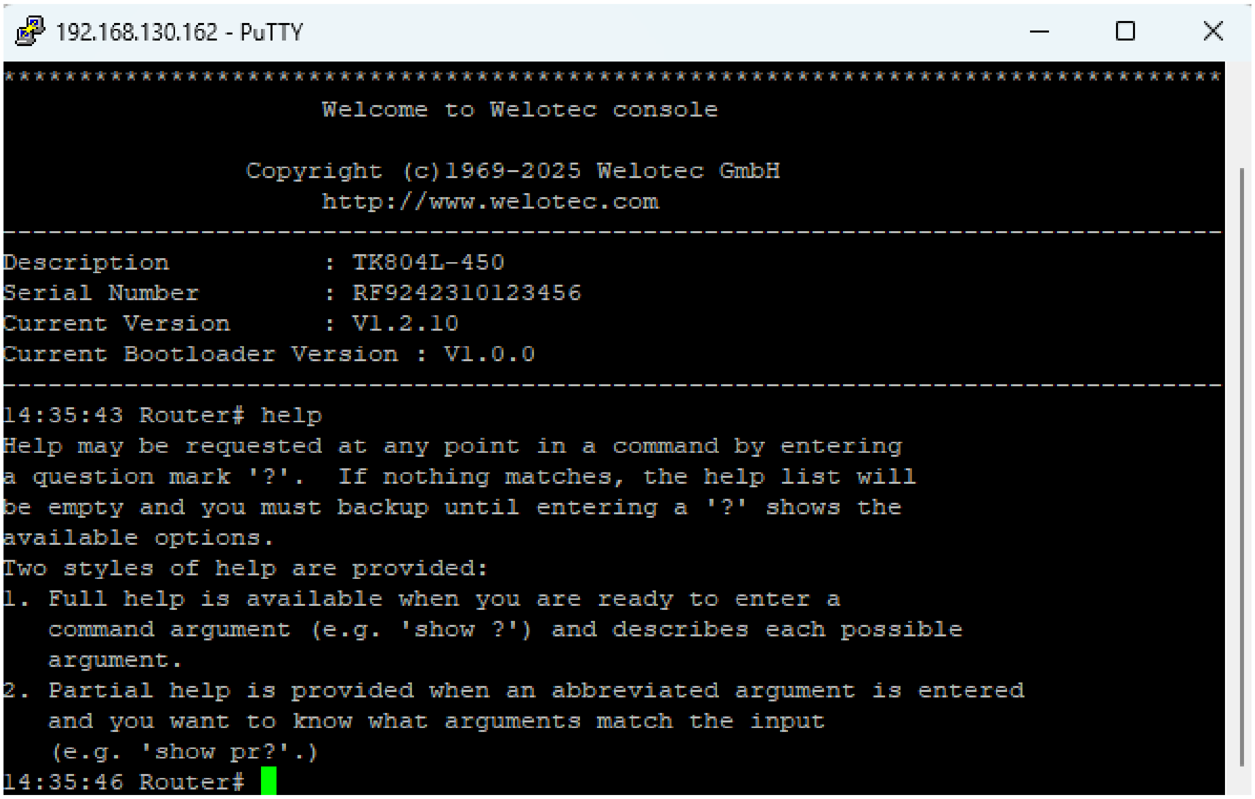


192.168.130.162 - PuTTY

```
login as: adm
adm@192.168.130.162's password:

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

                Copyright (c)1969-2025 Welotec GmbH
                     http://www.welotec.com
--------------------------------------------------------------------------------
Description              : TK804L-450
Serial Number            : RF9242310123456
Current Version          : V1.2.10
Current Bootloader Version : V1.0.0
--------------------------------------------------------------------------------
14:35:27 Router#
```

5.11.2 Help Command

- `help` → Shows help usage
- ? → Context-sensitive help at any point



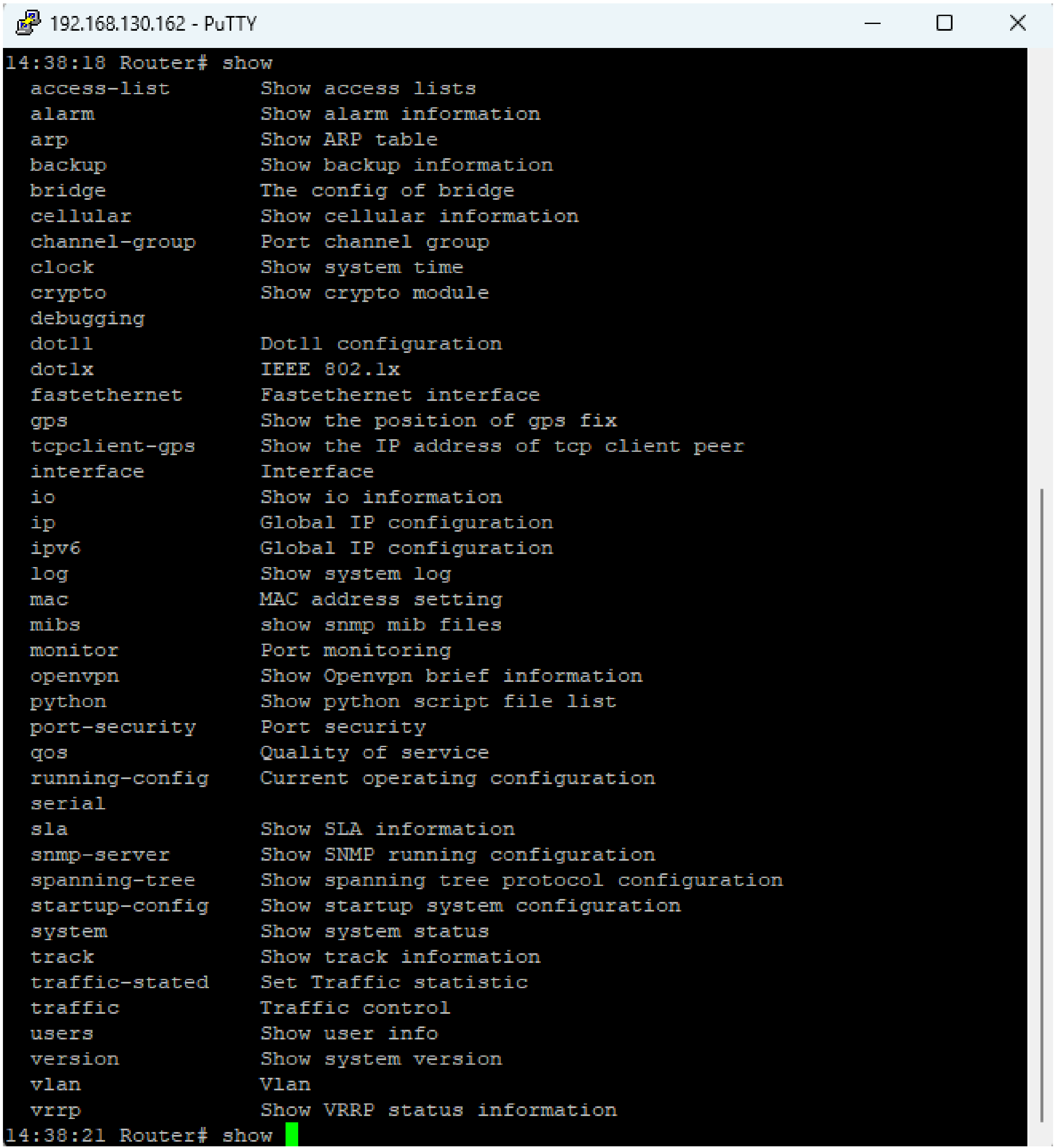
192.168.130.162 - PuTTY

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

                Copyright (c)1969-2025 Welotec GmbH
                     http://www.welotec.com
--------------------------------------------------------------------------------
Description              : TK804L-450
Serial Number            : RF9242310123456
Current Version          : V1.2.10
Current Bootloader Version : V1.0.0
--------------------------------------------------------------------------------
14:35:43 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?'.)
14:35:46 Router#
```

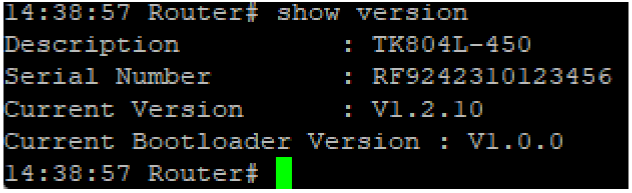
5.11.3 Show Command

Displays router parameters/config.

Example:
`show version` → Device info, serial no., firmware, bootloader.



```
14:38:18 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
  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
  ipv6                Global IP configuration
  log                 Show system log
  mac                 MAC address setting
  mibs                show snmp mib files
  monitor             Port monitoring
  openvpn             Show Openvpn brief information
  python              Show python script file list
  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
14:38:21 Router# show
```

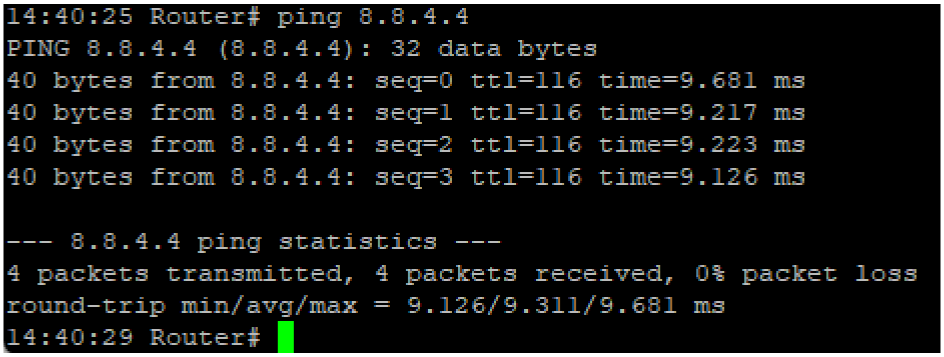


```
14:38:57 Router# show version
Description              : TK804L-450
Serial Number            : RF9242310123456
Current Version          : V1.2.10
Current Bootloader Version : V1.0.0
14:38:57 Router#
```

5.11.4 Ping Command

Check Internet connectivity.

ping <hostname/IP>

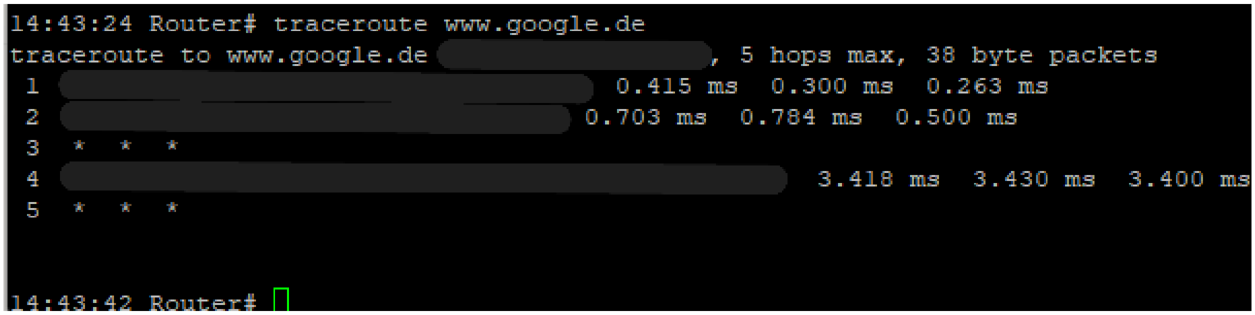


```
14:40:25 Router# ping 8.8.4.4
PING 8.8.4.4 (8.8.4.4): 32 data bytes
40 bytes from 8.8.4.4: seq=0 ttl=116 time=9.681 ms
40 bytes from 8.8.4.4: seq=1 ttl=116 time=9.217 ms
40 bytes from 8.8.4.4: seq=2 ttl=116 time=9.223 ms
40 bytes from 8.8.4.4: seq=3 ttl=116 time=9.126 ms

--- 8.8.4.4 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 9.126/9.311/9.681 ms
14:40:29 Router#
```

5.11.5 Traceroute Command

Test the active routing path to a destination.

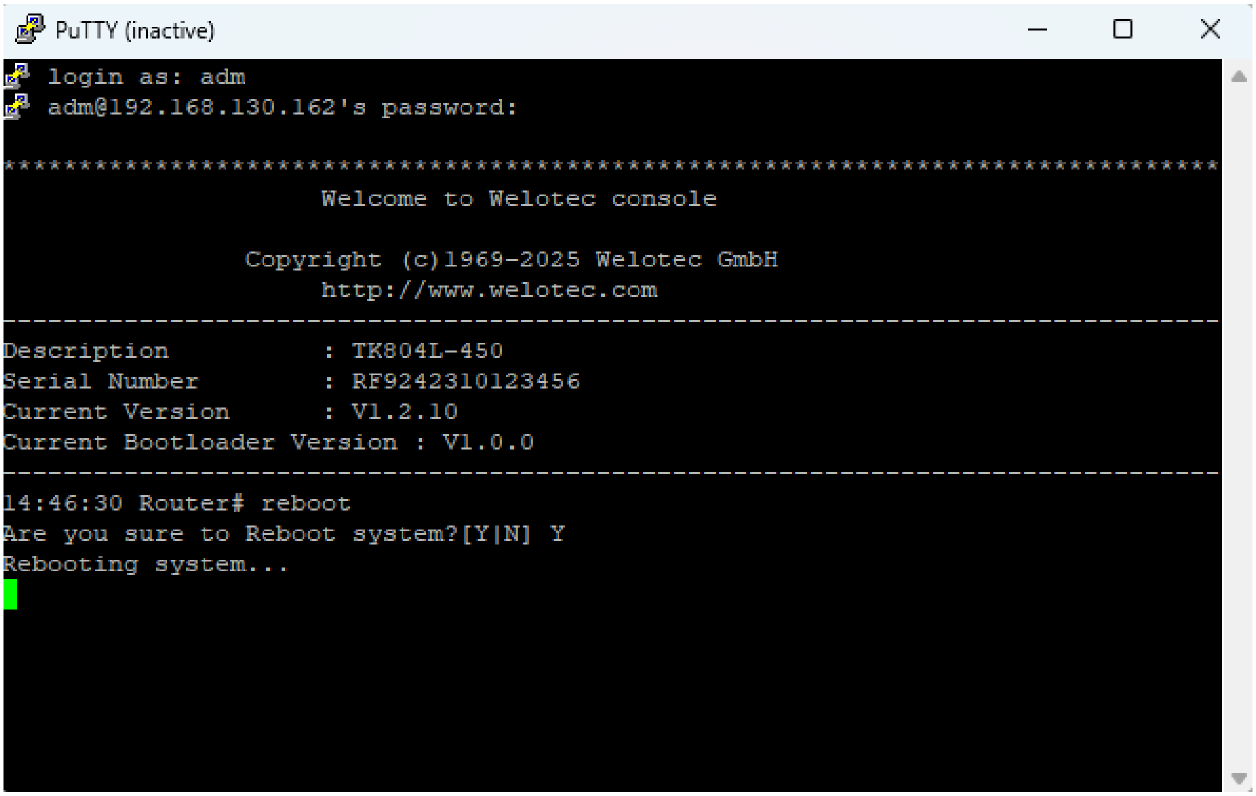
traceroute <hostname/IP>



```
14:43:24 Router# traceroute www.google.de
traceroute to www.google.de [redacted], 5 hops max, 38 byte packets
 1  [redacted]  0.415 ms  0.300 ms  0.263 ms
 2  [redacted]  0.703 ms  0.784 ms  0.500 ms
 3  *  *  *
 4  [redacted]  3.418 ms  3.430 ms  3.400 ms
 5  *  *  *


14:43:42 Router#
```

5.11.6 Reboot Command

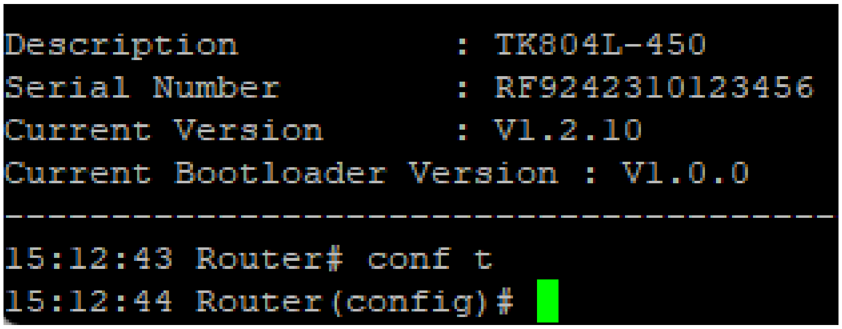
To restart the router, you can use the reboot command. Enter it in the CLI and the router will be restarted.



```
login as: adm
adm@192.168.130.162's password:

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

                Copyright (c)1969-2025 Welotec GmbH
                     http://www.welotec.com
--------------------------------------------------------------------------------
Description             : TK804L-450
Serial Number           : RF9242310123456
Current Version         : V1.2.10
Current Bootloader Version : V1.0.0
--------------------------------------------------------------------------------
14:46:30 Router# reboot
Are you sure to Reboot system?[Y|N] Y
Rebooting system...
```

5.11.7 Configuration Command

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

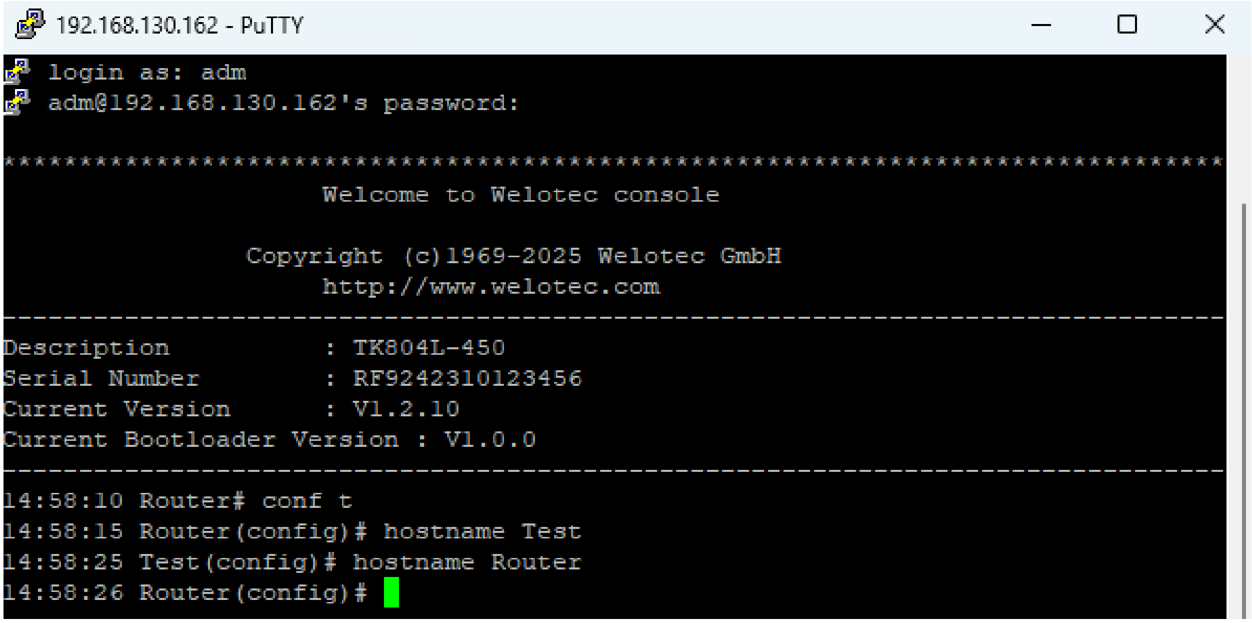


```
Description             : TK804L-450
Serial Number           : RF9242310123456
Current Version         : V1.2.10
Current Bootloader Version : V1.0.0
---------------------------------------
15:12:43 Router# conf t
15:12:44 Router(config)#
```

Hostname Command

In **configuration mode**, you can change the router name using **hostname** .
This sets the router’s name to the value you specify.

To reset the router name back to the factory default, use **default hostname**.

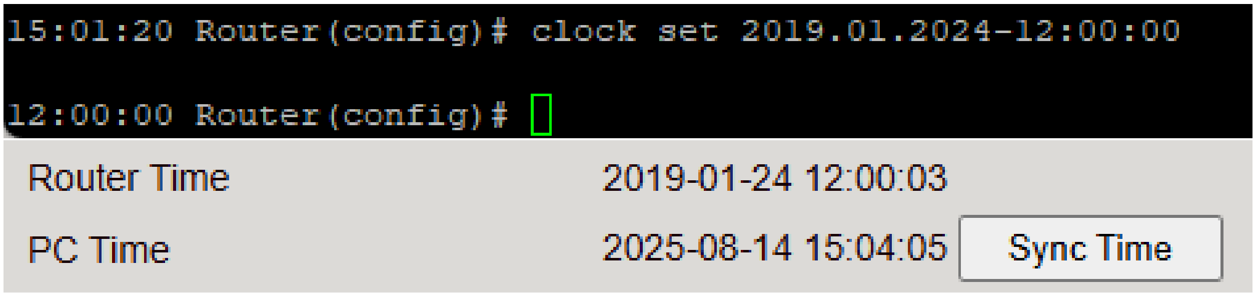


```
login as: adm
adm@192.168.130.162's password:

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

               Copyright (c)1969-2025 Welotec GmbH
                    http://www.welotec.com
--------------------------------------------------------------------------------
Description             : TK804L-450
Serial Number           : RF9242310123456
Current Version         : V1.2.10
Current Bootloader Version : V1.0.0
--------------------------------------------------------------------------------
14:58:10 Router# conf t
14:58:15 Router(config)# hostname Test
14:58:25 Test(config)# hostname Router
14:58:26 Router(config)#
```

Clock Set Command

You can configure the system date and time of the router using the **clock set** command.
The required format is: **YYYY.MM.DD-HH:MM:SS**

Example: **clock set 2019.01.24-12:00:00**



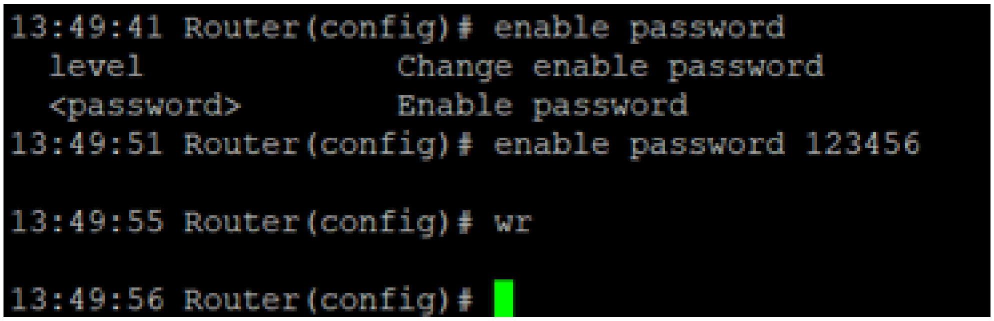
```
15:01:20 Router(config)# clock set 2019.01.2024-12:00:00

12:00:00 Router(config)#
```

Router Time 2019-01-24 12:00:03

PC Time 2025-08-14 15:04:05

Enable Password Command

The password of the superuser (**adm**) can be changed at any time via the CLI.
Use the command: **enable password**

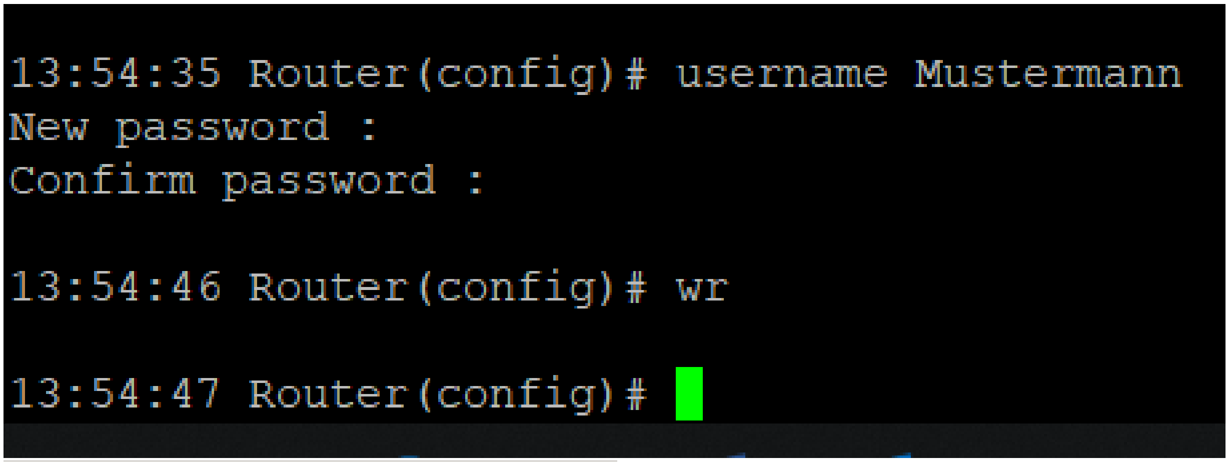


```
13:49:41 Router(config)# enable password
  level                Change enable password
  <password>           Enable password
13:49:51 Router(config)# enable password 123456

13:49:55 Router(config)# wr

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

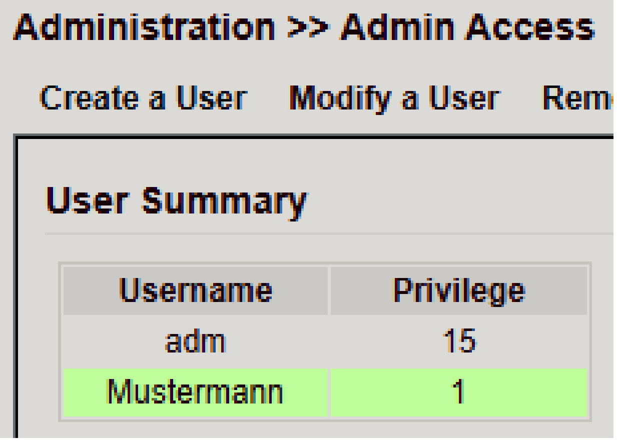
Username Command

The **username** command allows you to create new users for router access.
Syntax: **username**

When creating the user, you will be prompted to set a password.
⊠ New users created this way are always standard users (not administrators).



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

13:54:46 Router(config)# wr

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



Administration >> Admin Access

User Summary

Username	Privilege
adm	15
Mustermann	1

6 Technical Specifications

6.1 Device Properties

Property	Value
Housing material	Metal
Ingress Protection	IP30
Dimensions (W x H x D)	35 x 127 x 108 mm
Weight	457 g
Operating voltage	9 - 36 V DC
Mounting	DIN rail
Approval	CE compliant

6.2 Environmental Conditions

Property	Value
Operating temperature range	-25 to + 70 °C
Storage temperature range	-40 to +85 °C
Air humidity	5 - 95 %, non condensing
Concussions	IEC 60068-2-27
Free fall	IEC 60068-2-32
Vibration	IEC 60068-2-6
EMC	EN 61000-4, Level 3

7 Frequency bands by region

7.1 Radio frequencies LTE Europe

Frequency	Frequency Range Downlink (MHz)	Frequency Range Uplink (MHz)	Max. Transmit Power (mW)	Router
B1	2110 – 2170	1920 – 1980	200	TK804L-450
B3	1805 – 1880	1710 – 1785	200	TK804L-450
B5	869 – 894	824 – 849	200	TK804L-450
B7	2620 – 2690	2500 – 2570	200	TK804L-450
B8	925 – 960	880 – 915	200	TK804L-450
B20	791 – 821	832 – 862	200	TK804L-450
B28	758 – 788	703 – 733	200	TK804L-450
B31	462.5 – 467.5	452.5 – 457.5	200	TK804L-450

7.2 Radio frequencies GSM Europe

Frequency	Frequency Range Downlink (MHz)	Frequency Range Uplink (MHz)	Max. Transmit Power (mW)	Router
GSM 900	925 – 960	880 – 915	2000	TK804L-450
GSM 1800	1805 – 1880	1710 – 1785	1000	TK804L-450

7.3 Radio frequencies LTE USA/Canada

Frequency	Frequency Range Downlink (MHz)	Frequency Range Uplink (MHz)	Max. Transmit Power (mW)	Router
B5	869 – 894	824 – 849	200	TK804L-450
B28	758 – 788	703 – 733	200	TK804L-450
B72	663 – 698	617 – 652	200	TK804L-450

7.4 Radio frequencies GSM USA/Canada

Frequency	Frequency Range Downlink (MHz)	Frequency Range Uplink (MHz)	Max. Transmit Power (mW)	Router
GSM 900	925 – 960	880 – 915	2000	TK804L-450
GSM 1800	1805 – 1880	1710 – 1785	1000	TK804L-450

7.5 Radio frequencies LTE Asia

Frequency	Frequency Range Downlink (MHz)	Frequency Range Uplink (MHz)	Max. Transmit Power (mW)	Router
B1	2110 – 2170	1920 – 1980	200	TK804L-450
B3	1805 – 1880	1710 – 1785	200	TK804L-450
B5	869 – 894	824 – 849	200	TK804L-450
B8	925 – 960	880 – 915	200	TK804L-450
B28	758 – 788	703 – 733	200	TK804L-450
B31	462.5 – 467.5	452.5 – 457.5	200	TK804L-450

7.6 Radio frequencies GSM Asia

Frequency	Frequency Range Downlink (MHz)	Frequency Range Uplink (MHz)	Max. Transmit Power (mW)	Router
GSM 900	925 – 960	880 – 915	2000	TK804L-450
GSM 1800	1805 – 1880	1710 – 1785	1000	TK804L-450

7.7 Radio frequencies LTE Global

Frequency Band	Frequency Range Downlink (MHz)	Frequency Range Uplink (MHz)	Max. Transmit Power (mW)	Router
B1	2110 – 2170	1920 – 1980	200	TK804L-450
B3	1805 – 1880	1710 – 1785	200	TK804L-450
B5	869 – 894	824 – 849	200	TK804L-450
B7	2620 – 2690	2500 – 2570	200	TK804L-450
B8	925 – 960	880 – 915	200	TK804L-450
B20	791 – 821	832 – 862	200	TK804L-450
B28	758 – 788	703 – 733	200	TK804L-450
B31	462.5 – 467.5	452.5 – 457.5	200	TK804L-450
B72	663 – 698	617 – 652	200	TK804L-450

7.8 Radio frequencies GSM Global

Frequency Band	Frequency Range Downlink (MHz)	Frequency Range Uplink (MHz)	Max. Transmit Power (mW)	Router
GSM 900	925 – 960	880 – 915	2000	TK804L-450
GSM 1800	1805 – 1880	1710 – 1785	1000	TK804L-450

8 FAQ: IPsec

8.1 Preface

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

8.1.1 *Components of IPsec-VPNs*

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

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

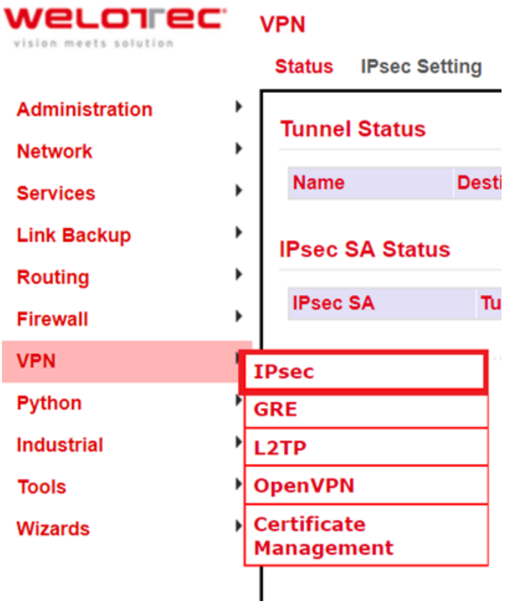
8.1.2 *Deployment scenarios*

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

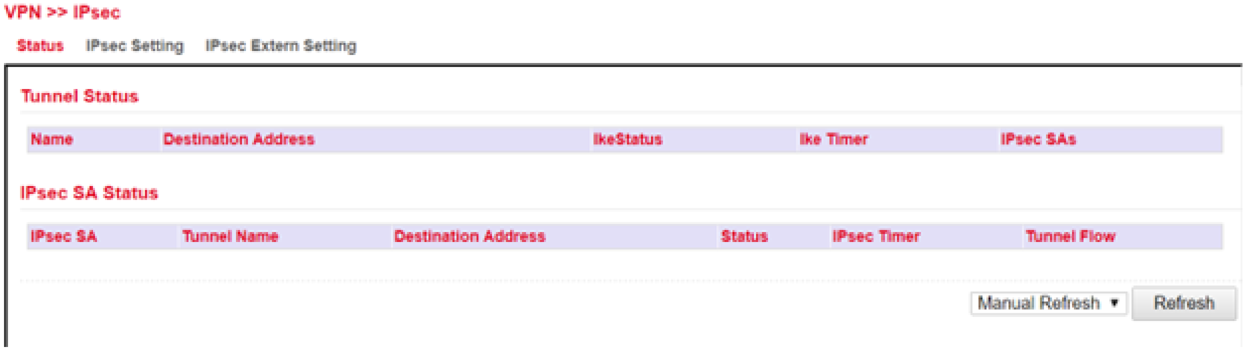
In principle, IPsec is suitable for gateway-to-gateway scenarios. In other words, the connection between networks via a third insecure network.

8.2 IPsec

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



Here the options *“IPsec Setting”* and *“IPsec Extern Setting”* are available.



Tunnel Status

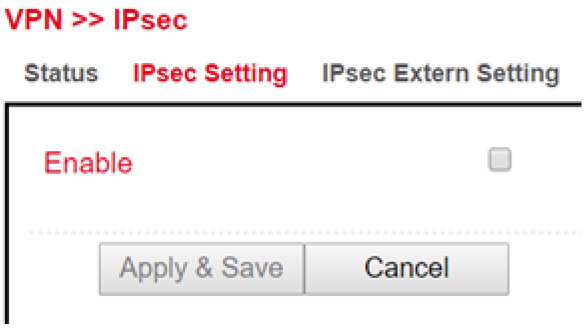
Name	Destination Address	IkeStatus	Ike Timer	IPsec SAs

IPsec SA Status

IPsec SA	Tunnel Name	Destination Address	Status	IPsec Timer	Tunnel Flow

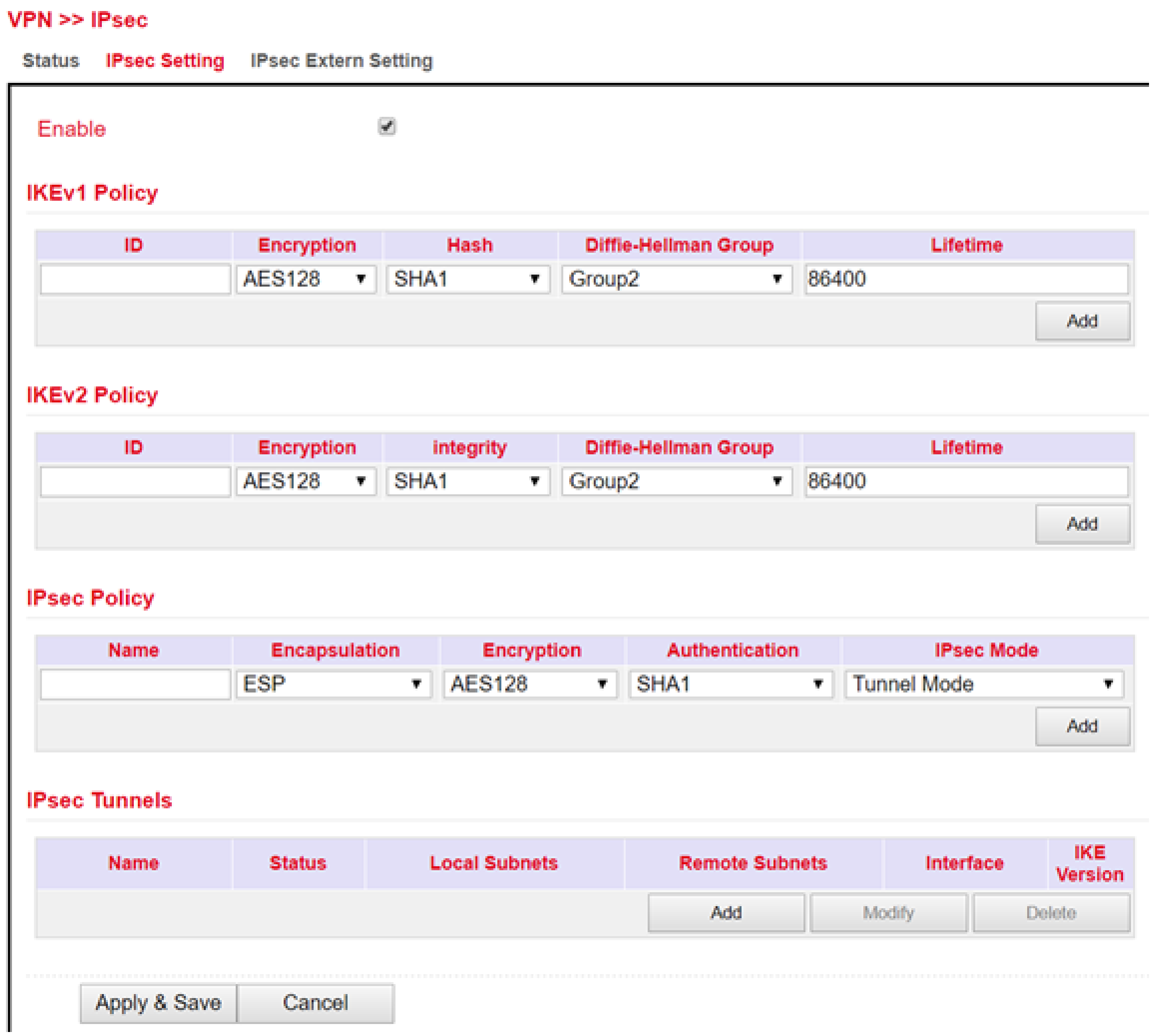
To create a new IPsec tunnel, proceed as follows:

1. Click on **“IPsec Setting”**



Enable □

2. Click on **“Enable”**



VPN >> IPsec

Status | IPsec Setting | IPsec Extern Setting

Enable ☑

IKEv1 Policy

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

IKEv2 Policy

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

IPsec Policy

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

IPsec Tunnels

Name	Status	Local Subnets	Remote Subnets	Interface	IKE Version

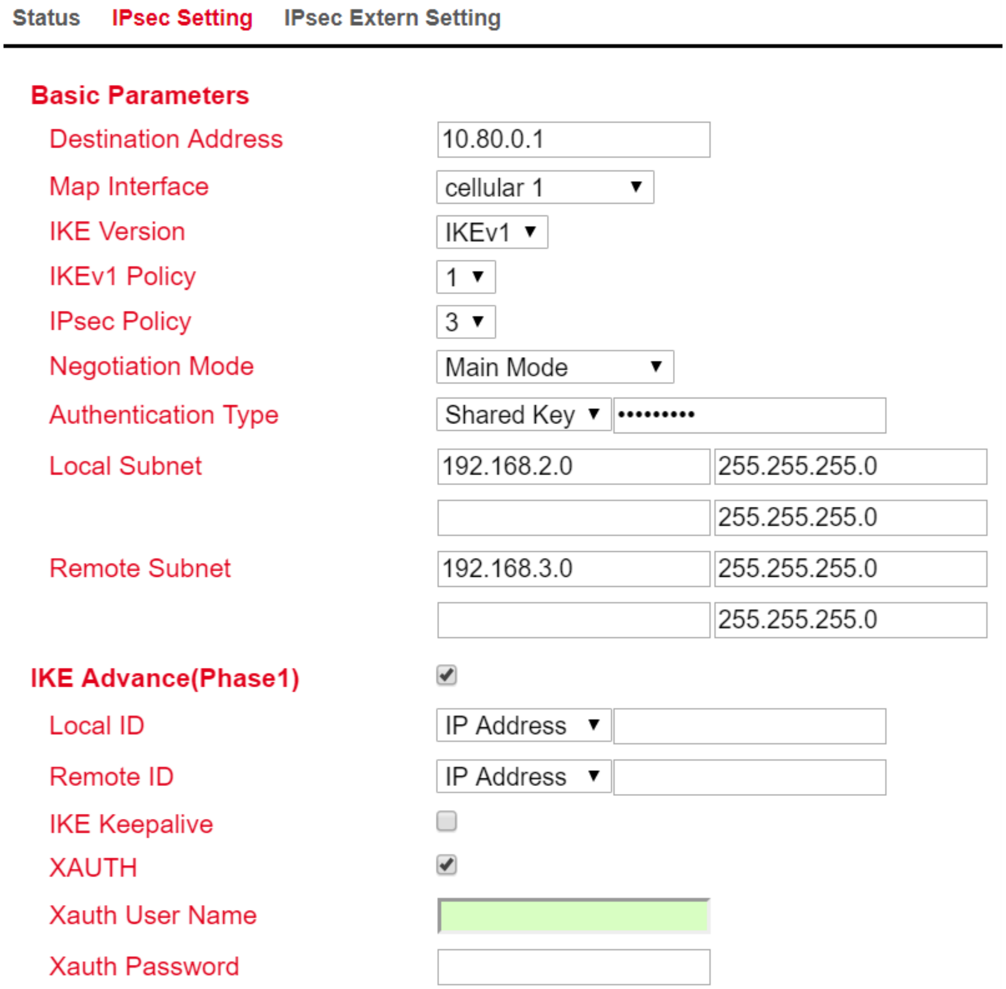
Now you can start with the configuration. Proceed as follows:

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

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

3. *IPsec Tunnels:*

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



Basic Parameters

Destination Address	10.80.0.1	
Map Interface	cellular 1 ▼	
IKE Version	IKEv1 ▼	
IKEv1 Policy	1 ▼	
IPsec Policy	3 ▼	
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	☐	
XAUTH	☑	
Xauth User Name		
Xauth Password		

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

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

- *IKE Advance (Phase 1)*

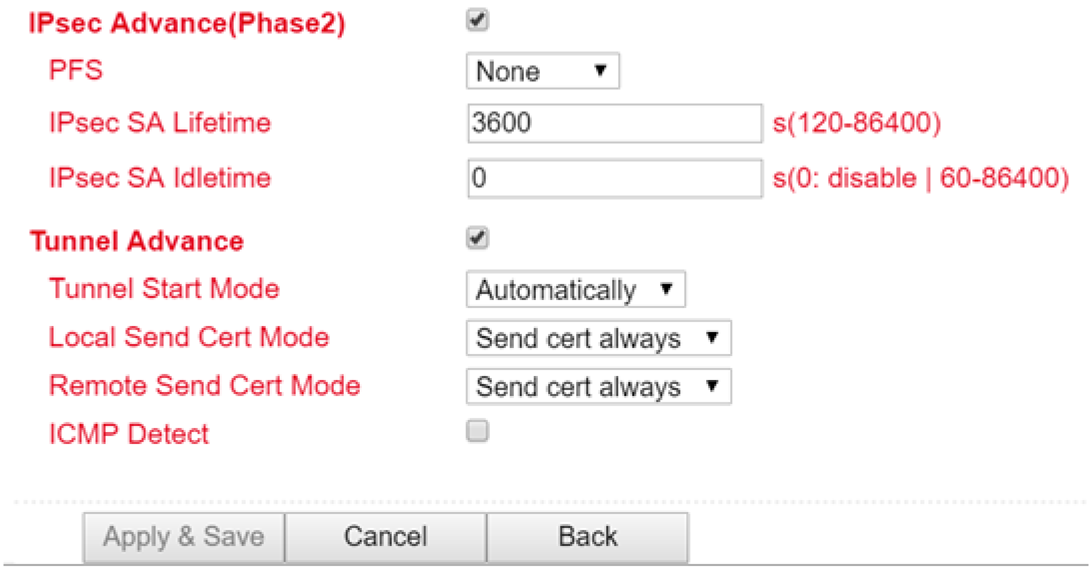
  After activation, the following options are available:

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

- *IPsec Advance (Phase 2)*

  After activation, the following options are available:

  1. **Perfect Forward Secrecy (PFS)** is a characteristic of certain key exchange protocols in cryptography. These use previously exchanged long-term keys to arrange a new secret session key for each session that needs to be encrypted. Perfect Forward Secrecy does not have a log so that the session keys used cannot be reconstructed from the long-term secret keys after the session is closed. This means that a recorded encrypted communication cannot be subsequently decrypted even if the long-term key is known. Here you can choose between several groups that work with Diffie Hellman keys. For example, Group 1 has an encryption of 768 bits, Group2 has 1024 bits and Group 5 uses 1536 bit, etc.
  2. You can enter the validity period of the SA (Security Association) under **"IPsec SA Lifetime"**. A Security Association groups IP packets together based on an SPI (Security Parameter Index), the IP destination address and the Security Protocol Identifier. An SA is only valid for ONE direction at a time, so there are always two SAs in use.
  3. With **"IPsec SA Idletime"** you specify whether SAs associated with inactive peers can be deleted before the global lifetime has expired. The 0 means that the function is disabled.



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	□	

- *Tunnel Advance*

  After activation, the following options are available:

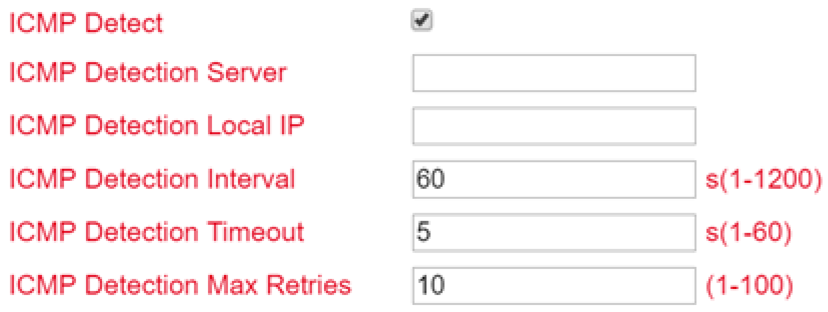
  1. For **"Tunnel Start Mode"**, set how the tunnel should start. The default setting is always automatic.
  2. In the **"Local Send Cert Mode"** field, you specify when a certificate should be sent for the local area. The default setting is that the certificate should always be sent (Send cert always).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

  image

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

8.2.1 IPsec Status

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



ICMP Detect	☑	
ICMP Detection Server		
ICMP Detection Local IP		
ICMP Detection Interval	60	s(1-1200)
ICMP Detection Timeout	5	s(1-60)
ICMP Detection Max Retries	10	(1-100)