



# UCR Routers

## User Guide

V1.0, June 2020



## Table of Contents

<b>Status Section</b> .....	5
Overview .....	5
Summary .....	5
Overview .....	5
<b>System</b> .....	8
Summary .....	8
System, Memory .....	8
<b>Network</b> .....	9
Summary .....	9
Mobile .....	9
WAN .....	12
LAN .....	14
Wireless .....	16
Wireless Information .....	16
OpenVPN .....	18
Topology .....	19
Access .....	19
<b>Device</b> .....	22
Summary .....	22
Device Information .....	22
<b>Services</b> .....	24
Summary .....	24
Services .....	24
<b>Routes</b> .....	25
Summary .....	25
ARP .....	25
Active IP routes .....	26
Active IPv6 routes .....	27
<b>Graphs</b> .....	29
Summary .....	29
Mobile Signal .....	29
Load .....	29
Traffic .....	30
Wireless .....	32
Connections .....	33
<b>Mobile Traffic</b> .....	34
Summary .....	34
Mobile Traffic Usage periods .....	34
Obtaining data usage values from command line .....	35
<b>Events Log</b> .....	37
Summary .....	37
Events Reporting .....	37
Reporting Configuration .....	56

<b>Network Section</b> .....	61
<b>Mobile</b> .....	61
Summary.....	61
General.....	61
SIM Management .....	68
Network Operators .....	70
Mobile Data Limit .....	72
SMS Limit .....	75
SIM Idle Protection.....	76
USB Modem .....	77
<b>WAN</b> .....	79
Summary.....	79
Operation Modes .....	79
Common Configuration .....	79
IP Aliases .....	85
Failover Configuration.....	87
<b>LAN</b> .....	89
Summary.....	89
Configuration .....	89
DHCP Server.....	90
Static Leases.....	93
IP Aliases .....	93
Relayd .....	95
UDP Broadcast Relay .....	95
<b>Wireless</b> .....	97
Summary.....	97
Wireless technology.....	97
Wireless Configuration.....	97
Wireless Access Point .....	97
Wireless Station .....	102
<b>Load Balancing</b> .....	104
Summary.....	104
Policies .....	104
Rules .....	105
<b>Services Section</b> .....	107
<b>MQTT</b> .....	107
Summary.....	107
MQTT Broker .....	107
MQTT Publisher .....	111
<b>NTP</b> .....	112
Summary.....	112
General.....	112
Time Servers.....	113
<b>RS232/RS485</b> .....	114

Summary.....	114
RS232.....	114
RS485.....	116
Modes of different serial types in RS232 and RS485.....	117
<b>VPN</b> .....	123
Summary.....	123
OpenVPN.....	123
IPsec.....	135
PPTP.....	142
L2TP.....	145
<b>Dynamic DNS</b> .....	148
Summary.....	148
Dynamic DNS Overview.....	148
Editing a DDNS instance.....	148
<b>SMS Gateway</b> .....	151
Summary.....	151
Post/Get.....	151
<b>GPS</b> .....	152
Summary.....	152
Map.....	152
General.....	152
NMEA.....	153
GPS Geofencing.....	156
<b>Hotspot</b> .....	159
Summary.....	159
General.....	159
Restricted Internet Access.....	173
Logging.....	174
Landing Page.....	177
Radius Server.....	177
Statistics.....	180
Manage.....	181
<b>Modbus</b> .....	182
Summary.....	182
Modbus TCP.....	182
Modbus TCP Master.....	187
Modbus Serial Master.....	192
Modbus Data to Server.....	199
<b>Input/Output</b> .....	201
Summary.....	201
Status.....	201
Input.....	202
Output.....	204

# Status Section

## Overview

### Summary

This chapter is an overview of the UCR devices.

### Overview

The Overview page contains **widgets** that display the status of various systems related to the device. The figure below is an example of the Overview page:

The screenshot displays the Overview page with the following widgets:

- System**: Shows 4.5% CPU load, Router uptime (0d 2h 9m 4s), Local device time (2018-10-11, 12:41:10), Memory usage (RAM: 40% used, FLASH: 7% used), and Firmware version (RUT9XX\_R\_00.05.02).
- Mobile**: Shows -51 dBm signal strength, Data connection (0d 0h 5m 53s), State (Registered (home); OMNITEL LT; 4G (LTE)), SIM card slot in use (SIM 1 (Ready)), and Bytes received/sent (2.4 KB / 656 B).
- Wireless**: Shows ON status, SSID (RUT955\_696D (AP)), and Mode (1- AP; 1 CH (2.412 GHz)).
- WAN**: Shows Wired connection, IP address (15.15.15.15, Public IP address), and WAN failover status (Failover link is enabled).
- Local Network**: Shows IP / netmask (192.168.1.1 / 255.255.255.0) and Clients connected (1).
- Remote Management System**: Shows ON status, Status (Enabled), and Connection State (Connected to monitoring system).
- Recent System Events**:
  - 2018-10-11 12:38:09 - SMS: SMS recieved from: +37000000000
  - 2018-10-11 12:37:00 - Port: LAN1 cable is plugged in
  - 2018-10-11 12:36:59 - DHCP: Leased 192.168.1.151 IP address fo ...
  - 2018-10-11 12:36:05 - Port: LAN1 cable is unplugged
- Recent Network Events**:
  - 2018-10-11 12:35:38 - Mobile data connected, IP: 15.15.15.15
  - 2018-10-01 16:40:49 - Mobile data disconnected
  - 2018-10-01 16:40:43 - Mobile data connected: N/A
  - 2017-07-18 15:01:30 - Mobile data disconnected

## Mobile widget

The **Mobile** widget displays information related to the mobile connection and the current **signal strength** (📶). Each filled-up bar represents a different RSSI value:

Bars	Signal Strength Value / RSSI (In DBm)
0	≤ -111
1	-110 to -97
2	-96 to -82
3	-81 to -67
4	-66 to -52
5	≥ -51

The same calculation principle applies to the **Signal strength LEDs** located on your device.

## Widget button: Info

The **Info** (i) button is located next to the name of some widgets. Clicking the Info button redirects the user to a status page related to the widget's displayed information. For example, clicking the Info button on the Mobile widget would redirect the user to the **Status** → **System** page:

The screenshot shows the Mobile widget on the left and the Mobile Information page on the right. A red arrow points from the Info button on the widget to the Mobile Information page.

**Mobile widget:**

- Mobile *i* -55 dBm 📶
- Data connection: Detailed information | Connected
- State: Registered (home); OMNITEL LT; 4G (LTE)
- SIM card slot in use: SIM 1 (Ready)
- Bytes received/sent \*: 42.4 KB / 47.5 KB

**Mobile Information page:**

- Mobile 📶 SIM card slot in use: SIM 1
- Data connection state: Connected
- IMEI: 861107030078134
- MSISDN: 24601210192055
- ICCID: 8937001010001920551
- SIM card state: Ready
- Signal strength: -55 dBm
- Cell ID: 4647903
- RSRP: -53 dBm
- RSRQ: -9 dB
- SINR: 19.5 dB
- Operator: OMNITEL LT
- Operator state: Registered (home)
- Connection type: 4G (LTE)
- Connected band: LTE BAND 3
- Bytes received \*: 23.8 KB (2422 bytes)
- Bytes sent \*: 14.9 KB (15207 bytes)
- Buttons: Reboot modem, Restart connection, Re-register, Refresh

## Widget button: Settings

The **Settings** (⚙️) button is located next to the name of some widgets. Clicking the Settings button redirects the user to a configuration page related to the widget's displayed information. For example, clicking the Info button on the Mobile widget would redirect the user to the **Network** → **Mobile** → **Mobile Configuration** page:



## Adding more widgets

There is a default set of widgets displayed in the Overview page, but more can be added from the **System** → **Administration** → **Overview** page.

# System

## Summary

---

The **System** window displays the device's system and memory related information.

## System, Memory

---

The figure below is an example of the System page and the table below provides information on the fields contained in that page:

### Field Name Description

---

<b>Router name</b>	Displays the device's product name
<b>Host name</b>	Displays the device's host name. The hostname can be used instead of the LAN IP address to communicate with the device inside the local network. The hostname can be changed in the <b>System</b> → <b>Administration</b> → <b>General</b> page
<b>Router model</b>	Displays the device's full model name
<b>Firmware version</b>	Displays the firmware version currently used by the device. The firmware can be upgraded from the <b>System</b> → <b>Firmware</b> page.
<b>Kernel version</b>	Displays the device's kernel version. A kernel is a computer program responsible for connecting a device's software to its hardware
<b>Local device time</b>	Displays the current time as perceived by the device. Time settings can be adjusted in the <b>Services</b> → <b>NTP</b> page
<b>Uptime</b>	Displays the amount of time that has passed since the device's last start up
<b>Load average</b>	Displays the device's CPU load average (in %) over the last minute, 5 minutes and 15 minutes
<b>Free</b>	Displays the amount of currently unused random-access memory (RAM)
<b>Cached</b>	Displays the amount of random-access memory (RAM) that is allocated for frequently accessed data storage
<b>Buffered</b>	Displays the amount of random-access memory (RAM) used by temporarily stored data before moving it to another location



# Network


## Summary

The **Network** page contains information related to the device's networking features. This chapter is an overview of the Network page in UCR devices.

## Mobile

The **Mobile** section displays information about the mobile connection and the SIM card in use. The figure below is an example of the Mobile page:

### Mobile Information

Mobile  SIM card slot in use: **SIM 1**

Data connection state	Connected
IMEI	██████████
IMSI	██████████
ICCID	██████████
Sim card state	Ready
Signal strength	-65 dBm
Cell ID	1037089
RSRP	-91 dBm
RSRQ	-9 dB
SINR	21.3 dB
Operator	LT BITE GSM
Operator state	Registered (home)
Connection type	4G (LTE)
Connected band	LTE BAND 7
Bytes received *	70.1 KB (71792 bytes)
Bytes sent *	44.1 KB (45184 bytes)

[Reboot modem](#) [Restart connection](#) [\(Re\)register](#) [Refresh](#)

\*Your carrier's data usage accounting may differ. Teltonika is not liable should any accounting discrepancies occur.

### Field Name

### Description

**Data connection state**

Indicates whether the device has an active mobile data connection

<b>IMEI</b>	The IMEI (International Mobile Equipment Identity) is a unique 15 decimal digit number used to identify cellular modules. GSM network operators use the IMEI to identify devices in their networks
<b>IMSI</b>	The IMSI (international mobile subscriber identity) is a unique 15 decimal digit (or less) number used to identify the user of a cellular network
<b>ICCID</b>	SIM card's ICCID is a unique serial number used to identify the SIM chip
<b>SIM card state</b>	The current SIM card state. Possible values are: <ul style="list-style-type: none"> <li>• <b>Ready</b> - SIM card is inserted and ready to be used</li> <li>• <b>Inserted</b> - SIM card is inserted</li> <li>• <b>Not inserted</b> - SIM card is not inserted</li> <li>• <b>Unknown</b> - unable to obtain SIM card state value. Possible communication issue between the the device and the modem</li> </ul>
<b>Signal strength</b>	Received signal strength indicator ( <b>RSSI</b> ) measured in dBm. Values closer to 0 indicate a better signal strength
<b>Cell ID</b>	The ID of the cell that the modem is currently connected to
<b>Signal level measurements</b>	Overall signal quality is defined by different measurements for different connection types. Short explanations and recommendations are provided below. <ul style="list-style-type: none"> <li>• <b>4G</b> <ul style="list-style-type: none"> <li>• RSRP - reference signal received power, measured in dBm. Values closer to 0 indicate better signal strength</li> <li>• RSRQ - reference signal received quality, measured in dB. Values closer to 0 indicate a better rate of information transfer</li> <li>• SINR - signal-to-interference-plus-noise ratio, measured in dB. Higher values indicate a better rate of information transfer</li> </ul> </li> <li>• <b>3G</b> <ul style="list-style-type: none"> <li>• EC/IO - downlink carrier-to-interference ratio. Values range from -20 to 0 (closer to 0 indicates better signal quality/cleanliness)</li> <li>• RSCP - received signal code power. Values range from -124 to 0 (closer to 0 indicates better signal strength)</li> </ul> </li> <li>• <b>2G</b> <ul style="list-style-type: none"> <li>• RSSI - received signal strength indicator, measured in dBm. Values closer to 0 indicate better signal strength</li> </ul> </li> </ul>

<b>Operator</b>	Network operator's name
<b>Operator state</b>	Shows whether the network has currently indicated the registration of the mobile device. Possible values are: <ul style="list-style-type: none"> <li>• <b>Unregistered</b> - not registered to a network and the device is not currently searching for a new operator to register to</li> <li>• <b>Registered (home)</b> - registered, home network</li> <li>• <b>Searching</b> - not registered to a network, but the device is currently searching for a new operator to register to</li> <li>• <b>Network denied</b> - registration to network denied by operator</li> <li>• <b>Unknown</b> - operator state is currently unknown</li> <li>• <b>Registered (roaming)</b> - registered to network, roaming conditions</li> </ul>
<b>Connection type</b>	Mobile connection type. Possible values are: <ul style="list-style-type: none"> <li>• <b>2G</b>: 2G (GSM), 2G (GPRS), 2G (EDGE)</li> <li>• <b>3G</b>: 3G (WCDMA), 3G (HSDPA), 3G (HSUPA), 3G (HSPA), 3G (HSPA+), 3G (DC-HSPA+), 3G (HSDPA+HSUPA), UMTS</li> <li>• <b>4G</b>: 4G (LTE)</li> <li>• <b>N/A</b> - not possible to determine at the moment</li> </ul>
<b>Connected band</b>	Currently used frequency band.
<b>Bytes received</b>	Amount of data received through the mobile interface
<b>Bytes sent</b>	Amount of data sent through the mobile interface
<b>Restart Modem</b>	Reboots the device's cellular module
<b>Restart Connection</b>	Restarts the mobile connection
<b>(Re)register</b>	Registers to the mobile network
<b>Refresh</b>	Refreshes all information fields in the page

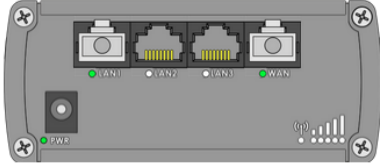
# WAN

The **WAN** section displays information about the Main and Backup WAN connections. The figure below is an example of the Mobile page:

### WAN Information


WAN	
Interface	Wired
Type	Static
IP address	10.21.41.240
WAN MAC	00:1E:42:████████
Netmask	255.255.255.0
Gateway	10.21.41.241
DNS 1	212.59.1.1
DNS 2	8.8.8.8
Connected	0h 1m 23s

### Ports



### WAN Failover Status

WAN: [Wired] IN USE    WAN Failover: [Mobile] READY    WAN Failover: [WiFi] READY

Refresh 

Field	Description
Interface	WAN type. Possible values are: <ul style="list-style-type: none"><li>• Mobile</li><li>• Wired</li><li>• Wireless</li></ul>
Type	Connection type or protocol. The value displayed in this field is dependent on used WAN type. Possible values are: <ul style="list-style-type: none"><li>• <b>Mobile WAN or USB modem</b><ul style="list-style-type: none"><li>• <b>Qmi2</b> - Qualcomm MSM Interface, a proprietary protocol used between Qualcomm cellular processors and their software stacks</li><li>• <b>PPP</b> - Point-to-Point Protocol; uses a dialling number to establish a data connection</li></ul></li></ul>

- **NCM** - Network Control Model, a protocol by which USB hosts and devices can efficiently exchange Ethernet frames (this is the connection type when using a Huawei USB modem)
- **Wired WAN**
  - **DHCP** - Dynamic Host Configuration Protocol; the WAN network interface controller acts as a DHCP client, meaning that it receives a dynamically assigned IP address and other network configuration parameters
  - **Static** - WAN network interface controller configuration parameters are set manually (used when the WAN gateway is not a DHCP server)
  - **PPPoE** - Point-to-Point Protocol over Ethernet; used to establish a Digital Subscriber Line (DSL) Internet service connection
- **WiFi WAN**
  - **DHCP** - Dynamic Host Configuration Protocol; the WAN network interface controller acts as a DHCP client, meaning that it receives a dynamically assigned IP address and other network configuration parameters
  - **Static** - WAN network interface controller configuration parameters are set manually (used when the WAN gateway is not a DHCP server)

IP address	Router's WAN IP address
WAN MAC	MAC address of the WAN network interface controller (WiFi radio or WAN Ethernet port). This field is only visible if main WAN is set to Wired or WiFi
Netmask	A <b>netmask</b> is used to define how "large" a network is by specifying which part of the IP address denotes the network and which part denotes the device
Gateway	Gateway of the default route - an IP address through which the router reaches the Internet
DNS	DNS servers used by the main WAN connection
Connected	Currently used WAN connection uptime
Ports	Displays an image of the router's back panel with highlighted Ethernet ports that are currently in use
WAN Failover Status	Displays the router's current WAN failover status
Refresh	Refreshes all information fields in the page

WAN settings can be customized via the **Network** → **WAN** page.

# LAN

---

The **LAN** section displays information about your Local Area Network and active DHCP leases.

## LAN Information

---

The **LAN Information** section contains data on the router's LAN interface(s). The figure below is an example of the LAN Information section:

LAN Information				
Name	IP address	Netmask	Ethernet MAC address	Connected for
Lan	192.168.1.1	255.255.255.0	00:1E:42:...	5h 53m 4s

Field	Description
Name	LAN interface name
IP address	Router's LAN IP address
Netmask	A <b>netmask</b> is used to define how "large" a network is by specifying which part of the IP address denotes the network and which part denotes the device
Ethernet MAC address	Router's LAN MAC address
Connected for	LAN interface uptime

## DHCP Leases

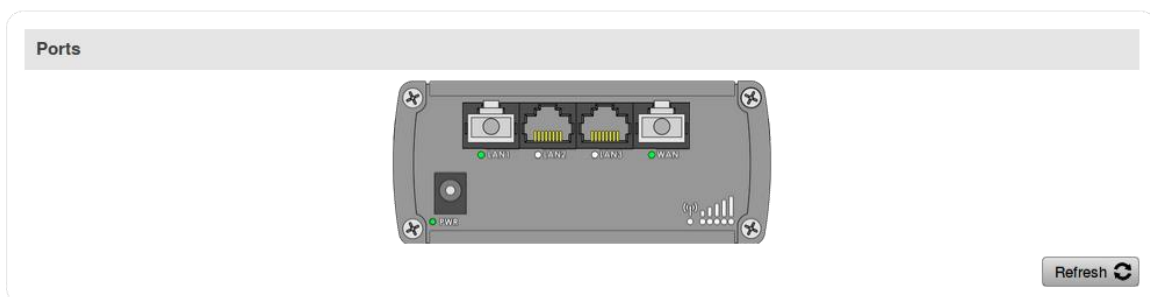
The **DHCP Leases** section contains information on DHCP clients that hold active DHCP lease. The figure below is an example of the DHCP Leases section:

DHCP Leases				
Hostname	IP address	LAN name	MAC address	Lease time remaining
mat	192.168.1.151	Lan	18:D6:C7:FF:FF:FF	11h 59m 50s

Field	Description
Hostname	DHCP client's hostname
IP address	DHCP client's IP address
LAN name	LAN interface name through which the client is connected to the router
MAC address	DHCP client's MAC address
Lease time remaining	Remaining lease time for a DHCP client. Active DHCP lease holders will try to renew their DHCP leases after a half of the lease time passes. DHCP lease settings can be changed in the <b>Network</b> → <b>LAN</b> → <b>DHCP Server</b> section

## Ports

The **Ports** displays an image of the router's front panel with highlighted Ethernet ports that are currently in use. The Refresh button refreshes all information fields in the page. The figure below is an example of the Ports section:

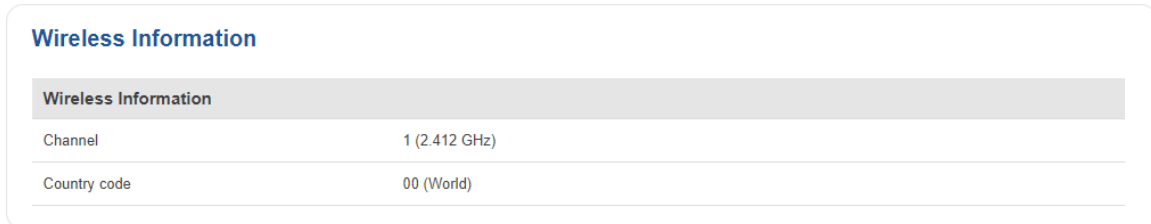


# Wireless

The **Wireless** section displays information about wireless connections and associated WiFi stations.

## Wireless Information

The figure below is an example of the **Wireless Information** section:



Wireless Information	
Channel	1 (2.412 GHz)
Country code	00 (World)

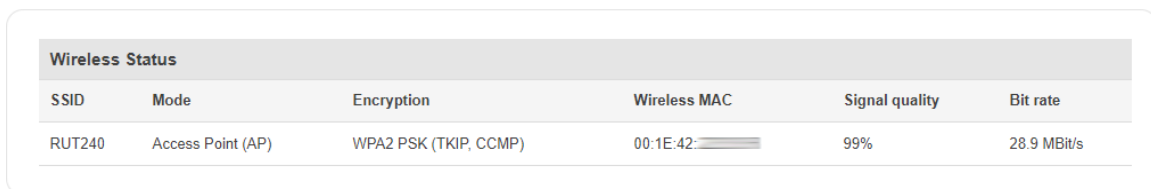
### Field Name Description

**Channel** Currently used channel. In most countries there are 13 WiFi channels on the 2.4 GHz band (14 in Japan) to choose from

**Country Code** Indicates currently used country code (SO/IEC 3166 alpha2 country codes as defined in ISO 3166-1 standard)

## Wireless Status

The **Wireless Status** section contains information about Wireless Access Points. The figure below is an example of the **Wireless Status** section:



Wireless Status					
SSID	Mode	Encryption	Wireless MAC	Signal quality	Bit rate
RUT240	Access Point (AP)	WPA2 PSK (TKIP, CCMP)	00:1E:42:...	99%	28.9 MBit/s

### Field Name Description

**SSID** The broadcasted SSID (Service Set Identifier) of the wireless network

**Mode** Connection mode. Can either be Access Point (AP) or Client. In AP mode others can connect to this router's wireless connection. In client mode router connects to other wireless networks


**Encryption** The type of WiFi encryption used



- Wireless MAC** The MAC (Media Access Control) address of the access point radio
- Signal Quality** The signal quality between router's radio and some other device that is connected to the router
- Bit rate** The maximum possible physical throughput that the router's radio can handle. Bit rate will be shared between router and other possible devices which connect to local Access Point (AP)

## Associated Stations

The **Associated Stations** section contains information about devices that are connected to Wireless Access Point. The figure below is an example of the **Associated Stations** section:

Associated Stations				
MAC address	Device name	Signal	RX rate	TX rate
	Galaxy-S9	-41 dBm	24.0 Mbit/s, MCS 0, 20MHz	28.9 Mbit/s, MCS 3, 20MHz

Field Name	Description
<b>MAC address</b>	Associated station's MAC (Media Access Control) address
<b>Device Name</b>	Currently connected device name
<b>Signal</b>	Received Signal Strength Indicator (RSSI). Signal's strength measured in dBm
<b>RX rate</b>	The rate at which packets are received from associated station
<b>TX rate</b>	The rate at which packets are sent to associated station


# OpenVPN

The OpenVPN section displays information about the OpenVPN connection (either client or server).

## OpenVPN Information

Client\_Client1

OpenVPN	
Enabled	Yes
Status	Connected
Type	Client
IP	10.0.0.6
Mask	255.255.255.255
Time	0h 0m 40s

Refresh 

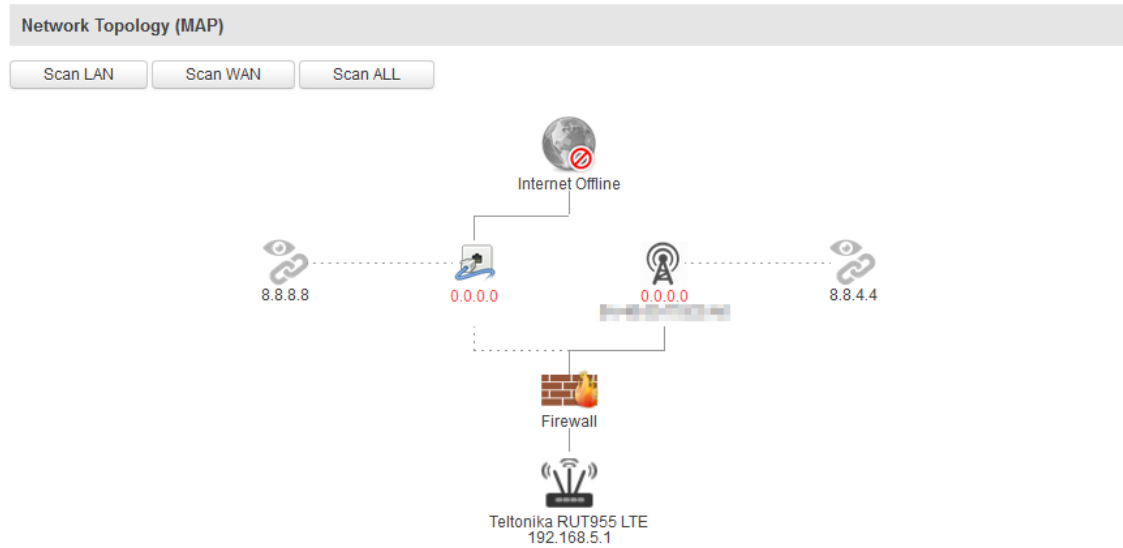
Field Name	Description
<b>Enabled</b>	Indicates whether OpenVPN server/client is enabled or not
<b>Status</b>	Shows connection status
<b>Type</b>	Shows whether the router is a server or client
<b>IP</b>	Router's OpenVPN IP address
<b>Mask</b>	A netmask is used to define how "large" a network is by specifying which part of the IP address denotes the network and which part denotes the device
<b>Time</b>	Shows OpenVPN connection uptime

# Topology

---

The Topology section is a visual representation of your LAN network.

## Network Topology



# Access

---

## Access Information

---

The Access Information section displays the status of both local and remote SSH, HTTP and HTTPS access and shows the number of current connections to your router through each of those protocol.

## Access Status

Access Information

Last Connections

Local Access			
Type	Status	Port	Active connections
SSH	Enabled	22	0 ( 0.00 B )
HTTP	Enabled	80	2 ( 5.12 KB )
HTTPS	Enabled	443	0 ( 0.00 B )

Remote Access			
Type	Status	Port	Active connections
SSH	Disabled	22	0 ( 0.00 B )
HTTP	Enabled	80	0 ( 0.00 B )
HTTPS	Disabled	443	0 ( 0.00 B )

Refresh 

### Field Name

### Description

<b>Type</b>	Shows access type
<b>Status</b>	Indicates whether that access type is enabled or not
<b>Port</b>	Shows which port which type of access uses
<b>Active connections</b>	Currently active connections count and data usage

## Last Connections

The Last Connections section displays three of the last local and remote connections to your router via SSH, HTTP and HTTPS and their status (either failed or successful).

## Access Status

Access Information

Last Connections

Last Local Connections			
Type	Date	IP	Authentications Status
SSH	2017-10-17 13:22:08	192.168.56.124	Succeeded
	2017-10-19 06:48:23	192.168.56.124	Succeeded
HTTP	2017-10-24 05:16:10	192.168.1.174	Failed
	2017-10-24 05:16:14	192.168.1.174	Failed
	2017-10-24 05:16:23	192.168.1.174	Succeeded
HTTPS	<i>There are no records yet.</i>		

Last Remote Connections			
Type	Date	IP	Authentications Status
SSH	<i>There are no records yet.</i>		
HTTP	<i>There are no records yet.</i>		
HTTPS	<i>There are no records yet.</i>		

Refresh 

### Field Name

### Description

<b>Type</b>	Shows access type
<b>Date</b>	Indicates connection date
<b>IP</b>	Shows what IP address connected
<b>Authentication Status</b>	Shows whether authentication was successful or not

# Device

## Summary

The **Device** section displays information related to the device's hardware.

## Device Information

The figure below is an example of the Device section and the table below provides explanations on the fields contained in that section:

Device Information	
Device	
Serial number	0011223344
Product code	RUT955H7V3C0
Batch number	0004
Hardware revision	0505
IMEI	861107030078134
IMSI	246020100944448
Ethernet LAN MAC address	00:1E:42:77:69:6B
Ethernet WAN MAC address	00:1E:42:77:69:6C
Wireless MAC address	00:1E:42:77:69:6D
Modem	
Model	EC25
FW version	EC25EFAR02A08M4G

Field Name	Description
<b>Serial number</b>	A unique 10-digit device identifier
<b>Product code</b>	Ordering code, displays under which product code the device was manufactured. Different product codes indicate different versions of the overall product. For example, devices with different product codes may support different LTE bands, come with different accessories, different firmware, etc.
<b>Batch number</b>	A 4-digit number that indicates the batch of materials
<b>Hardware revision</b>	A 4-digit number representing the router's hardware revision version
<b>IMEI</b>	The IMEI (International Mobile Equipment Identity) is a unique 15 decimal digit number used to identify mobile modules. GSM network operators use the IMEI to identify devices in their networks
<b>IMSI</b>	The IMSI (international mobile subscriber identity) is a unique 15 decimal digit (or less) number used to identify the user of a cellular network

**MAC address** The media access control (MAC) address is a unique identifier used to distinguish a network interface controller for communication in the data link layer (OSI layer2)

- Ethernet LAN MAC address - MAC address of the LAN Ethernet network interface.  
Ethernet WAN MAC address - MAC address of the WAN Ethernet network interface
- Wireless MAC address - MAC address of the wireless radio

**Model** The modem's model number

**FW version** Modem's current firmware version

# Services

## Summary

The **Services** page is used for easy service management. From here you can monitor your device's services states. By click of a button access respective section where it was originally configured.


## Services

The Services table displays the status of most of the device's services. Services that are currently inactive are displayed in a red font, while active ones are highlighted in green.

The figure below is an example of the Services page:

### Services

Services Status		
VRRP LAN	Disabled	<a href="#">Change settings</a>
OpenVPN server	Disabled	<a href="#">Change settings</a>
OpenVPN clients	Disabled	<a href="#">Change settings</a>
SNMP agent	Enabled	<a href="#">Change settings</a>
SNMP trap	Disabled	<a href="#">Change settings</a>
NTP client	Enabled	<a href="#">Change settings</a>
IPsec	Disabled	<a href="#">Change settings</a>
Ping reboot	Disabled	<a href="#">Change settings</a>
Input/Output rules	Disabled	<a href="#">Change settings</a>
DDNS	Disabled	<a href="#">Change settings</a>
Site blocking	Disabled	<a href="#">Change settings</a>
Content blocker	Disabled	<a href="#">Change settings</a>
SMS utilities	Enabled	<a href="#">Change settings</a>
Hotspot logging	Disabled	<a href="#">Change settings</a>
QoS	Disabled	<a href="#">Change settings</a>
GPS	Disabled	<a href="#">Change settings</a>

[Refresh](#) 

Click the zone next to a service where it says "Change settings" and you will be redirected to configuration page.

### Additional notes:

- By default, only [NTP](#) and [SMS Utilities](#) services are enabled



# Routes

## Summary

---

The **Routes** page displays the router's ARP table and active IPv4 and IPv6 routes.

## ARP

---

The **Address Resolution Protocol (ARP)** is a communication protocol used for mapping an Internet Protocol address (IP address) to a physical machine's link layer address (MAC address) belonging to the local network.

The ARP section displays the router's **ARP cache** (also known as ARP table) data. The ARP cache contains information on each known MAC address and its corresponding IP address. When the router receives a packet destined for a local host, the ARP program attempts to find a physical host or MAC address in the ARP cache that matches the IP address. If the ARP cache doesn't contain the needed IP address, ARP broadcasts a request packet to all LAN machines in order to find the device with the IP address in question.

The figure below is an example of the ARP cache section:

ARP		
IP address	MAC address	Interface
192.168.1.103	AC:E2:D3:00:00:00	br-lan
192.168.1.151	18:D6:C7:00:00:00	br-lan

Field Name	Value	Description
<b>IP address</b>	ip; Default: <b>none</b>	IP address of a local host
<b>MAC address</b>	mac; Default: <b>none</b>	MAC address of a local host
<b>Interface</b>	string; Default: <b>none</b>	Interface through which the router is associated with the host

You can also view the ARP cache via shell using the **arp** or **ip neigh** commands, depending on which output your prefer:

```
root@UCR:~# arp
IP address      HW type    Flags      HW address    Mask
Device
192.168.1.103  0x1       0x2       ac:e2:d3:00:00:00  *
br-lan
```

```

192.168.1.151    0x1          0x2          18:d6:c7:00:00:00    *
br-lan
root@UCR:~# ip neigh
192.168.1.103 dev br-lan lladdr ac:e2:d3:00:00:00 REACHABLE
192.168.1.151 dev br-lan lladdr 18:d6:c7:00:00:00 REACHABLE

```

## Active IP routes

The **Active IP routes** section displays the router's **routing table**. A routing table contains a list of routes to network destinations associated with and known by the router.

The figure below is an example of the Active IP routes section:

Active IP Routes			
Network	Target	IP gateway	Metric
ppp	0.0.0.0/0	10.1.179.213	0
ppp	10.1.179.208/29	0.0.0.0	10
ppp	10.1.179.213	0.0.0.0	10
lan	192.168.1.0/24	0.0.0.0	0

Field Name	Value	Description
<b>Network</b>	string; Default: <b>none</b>	Associated network interface name
<b>Target</b>	ip   ip/netmask; Default: <b>none</b>	Destination network address
<b>IP gateway</b>	ip; Default: <b>none</b>	Indicates the IP address of the gateway through which the target network can be reached
<b>Metric</b>	integer [0..4,294,967,295]; Default: <b>none</b>	Metrics help the router choose the best route among multiple feasible routes to a destination. The route will go in the direction of the gateway with the lowest metric value

You can also view the routing table via shell using the **route** or **ip route** commands, depending on which output you prefer:

```

root@UCR:~# route
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref
Use Iface

```

```

default          10.1.179.213    0.0.0.0          UG    0      0
0 wwan0
10.1.179.208    *                255.255.255.248 U     10     0
0 wwan0
10.1.179.213    *                255.255.255.255 UH    10     0
0 wwan0
192.168.1.0     *                255.255.255.0   U     0      0
0 br-lan
root@UCR:~# ip route
default via 10.1.179.213 dev wwan0
10.1.179.208/29 dev wwan0 proto static scope link metric 10
10.1.179.213 dev wwan0 proto static scope link src 10.1.179.212
metric 10
192.168.1.0/24 dev br-lan proto kernel scope link src 192.168.1.1

```

## Active IPv6 routes

The **Active IPv6 routes** section displays the router's IPv6 routing table.

The figure below is an example of the Active IPv6 routes section:

Active IPv6-Routes			
Network	Target	IPv6 gateway	Metric
loopback	0:0:0:0:0:0:0:0	0:0:0:0:0:0:0:0	FFFFFFFF
loopback	0:0:0:0:0:0:0:1	0:0:0:0:0:0:0:0	00000000
ppp	FF00:0:0:0:0:0:0:8	0:0:0:0:0:0:0:0	00000100
loopback	0:0:0:0:0:0:0:0	0:0:0:0:0:0:0:0	FFFFFFFF

Field Name	Value	Description
<b>Network</b>	string; Default: <b>none</b>	Associated network interface name
<b>Target</b>	ip6   ip6/netmask; Default: <b>none</b>	Destination network address
<b>IP gateway</b>	ip6; Default: <b>none</b>	Indicates the IPv6 address of the gateway through which the target network can be reached
<b>Metric</b>	integer [0..4,294,967,295]; Default: <b>none</b>	Metrics help the router choose the best route among multiple feasible routes to a destination. The route will go in the direction of the gateway with the lowest metric value

You can also view the routing table via shell using the **route -A inet6** or **ip -6 route show** commands, depending on which output you prefer:

```
root@UCR:~# ip -6 route
fe80::/64 dev wwan0 proto kernel metric 256
```

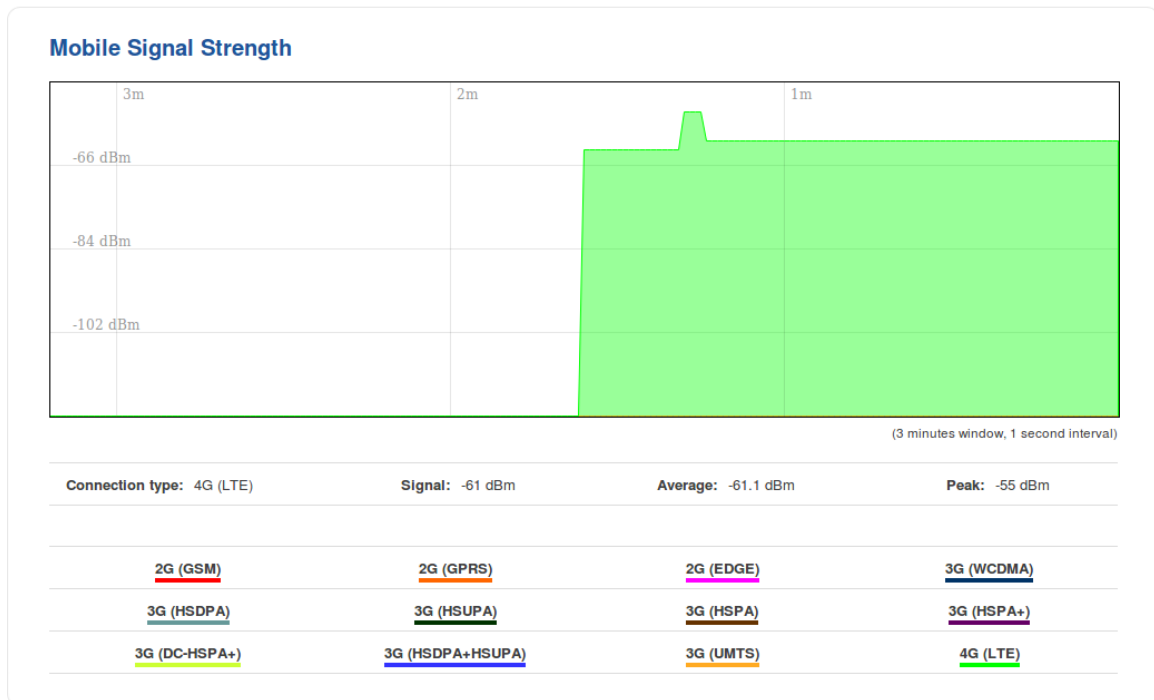
# Graphs

## Summary

The **Graphs** section contains various graphs that display various statistical data changes in real time.

## Mobile Signal

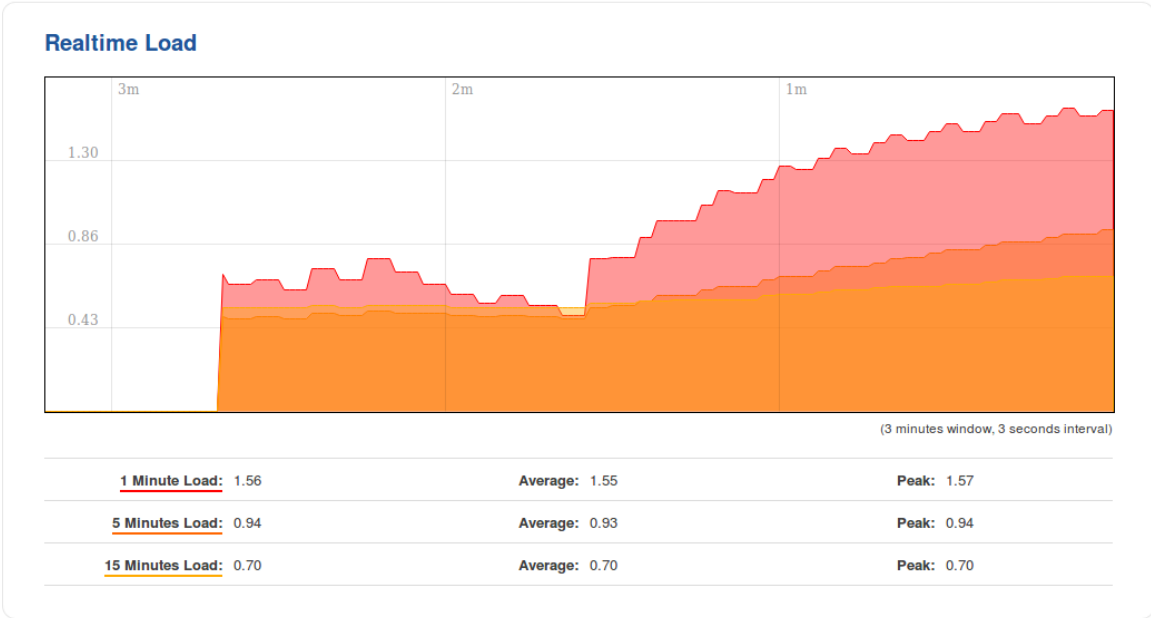
The **Mobile Signal Strength** graph displays mobile signal strength (RSSI, measured in dBm) value changes over a period of 3 minutes. The figure below is an example of the Mobile Signal Strength graph:



## Load

The **Realtime Load** section displays a tri-graph that illustrates average CPU load values in real time. The graph consists out of three color coded graphs, each one corresponding to the average CPU load over 1 (red), 5 (orange) and 15 (yellow) most recent minutes.

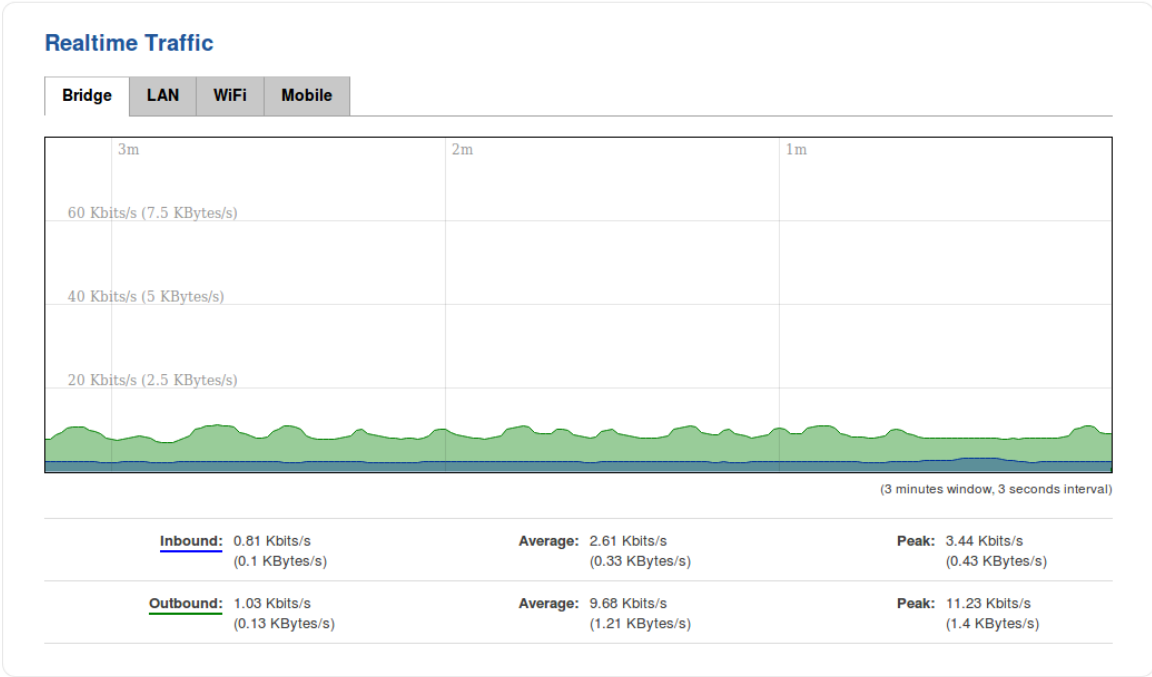
The figure below is an example of the Realtime Load graph:



## Traffic

The **Realtime Traffic** graphs provide users with the possibility to monitor average inbound and outbound traffic over the course of 3 minutes; each new measurement is taken every 3 seconds. The graphs consist out of two color coded graphs: the green graph shows the outbound traffic, the blue graph shows the inbound traffic. Although not graphed, the page also displays peak loads and averages of inbound and outbound traffic.

The figure below is an example of the Realtime traffic graph for the Bridge connection:

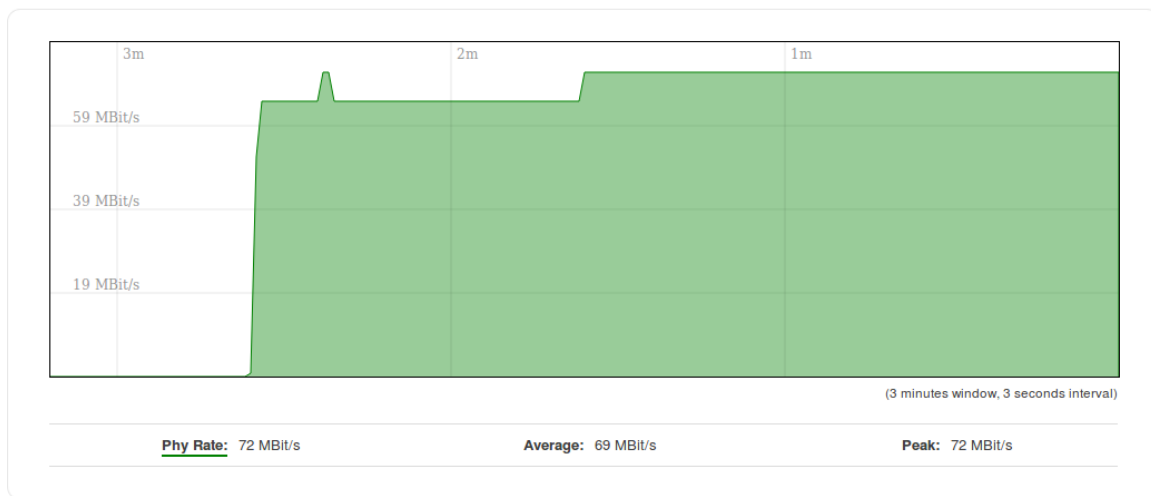
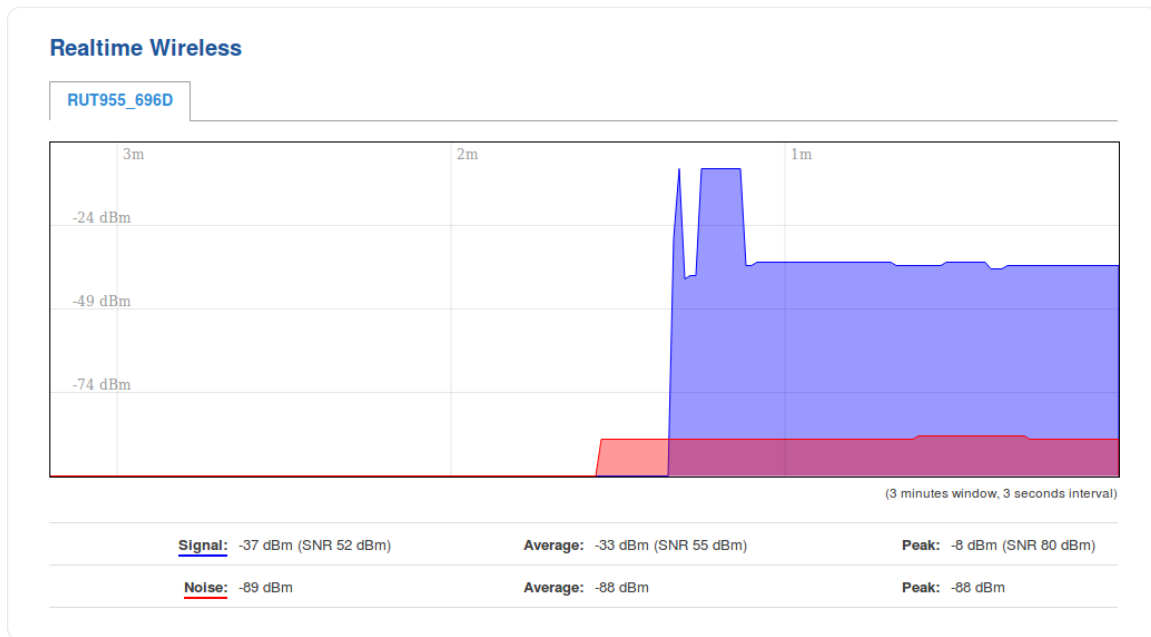


GRAPH	DESCRIPTION
<b>Bridge</b>	Cumulative graph, which encompasses wired Ethernet LAN and the wireless network
<b>LAN</b>	Displays traffic that passes through the LAN network interface(s) in graph form
<b>WiFi</b>	Displays traffic that passes through the WiFi interface in graph form
<b>WAN (Wired)   WAN (WiFi)   Mobile</b>	Displays traffic that passes through the current active WAN connection in graph form

# Wireless

The **Realtime Wireless** graph displays the wireless radio signal strength, signal noise, average and peak signal levels and the theoretical maximum channel permeability. The graph below the WiFi signal graph displays the Phy Rate for the wireless connection.

The figures below are examples of both Wireless graphs:

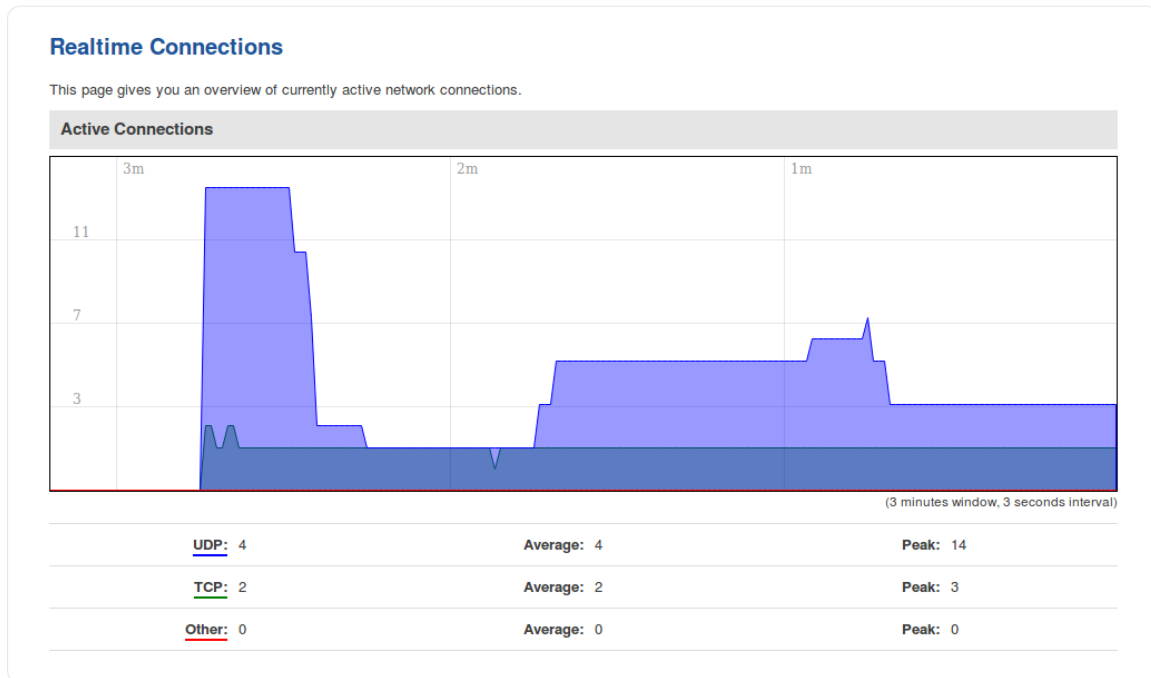




# Connections

The **Realtime Connections** graph displays currently active network connections with the information about network, protocol, source and destination addresses and transfer speed. The table below the graph displays basic information on active connections.

The figures below are examples of both of the Realtime Connections graph and the corresponding table:



# Mobile Traffic

## Summary

---

The **Mobile Traffic** section contains graphs that display mobile data usage values over different periods of time.

## Mobile Traffic Usage periods

---

Different tabs of the Mobile Traffic section display mobile data usage values over different periods of time. This includes:

- **Today** - data usage values for the current day
  - **Current Week** - weekly data usage values
  - **Current Month** - monthly data usage values
  - **Data Limit Period** - data usage values for the current data limit period (as set in the Network → Mobile → Mobile Data Limit page)
  - **Total** - data usage for the entire monitoring period (since Mobile Traffic Usage Logging was enabled)
- 

The figure below is an example of the weekly data usage graph:



Data usage graphs for other periods of time are essentially identical, with the exception that different time units (hours for daily usage, days of the week/month for

weekly/monthly usage, months for total data usage) are displayed at the top of the graphs.

Take note that the **Delete all data** button (located in the bottom right corner of each graph) clears the entire data usage database, meaning that data usage values for **all periods** will be cleared and the **data limit counter** will be reset.

## Obtaining data usage values from command line

Mobile data usage values can be obtained via [command line interface](#) with the help of **mdcollectedctl**. The usage for this command is described below:

```
usage: mdcollectedctl OPTIONS
-cdayrx<SIM> | GET today RX
-cdaytx<SIM> | GET today TX
-clast24hrx<SIM> | GET last 24h
RX
-clast24htx<SIM> | GET last 24h
TX
-cweekrx<SIM> | GET this week
RX
-cweektx<SIM> | GET this week
TX
-pweekrx<SIM> | GET last seven
days RX
-pweektx<SIM> | GET last seven
days TX
-cmonthrx<SIM> | GET this month
RX
-cmonthtx<SIM> | GET this month
TX
-pmonthrx<SIM> | GET last
month(30 days) RX
-pmonthtx<SIM> | GET last
month(30 days) TX
-rx | GET current
sim RX from reset
-tx | GET current
sim TX from reset
-dayrx<SIM> <YEAR> <MONTH> <DAY> | GET entered
day RX
```

```

-daytx<SIM> <YEAR> <MONTH> <DAY> | GET entered
day TX
-monthrx<SIM> <YEAR> <MONTH> | GET entered
month RX
-monthtx<SIM> <YEAR> <MONTH> | GET entered
month TX
-fromtorx<SIM> <FROM_YEAR> <FROM_MONTH> <FROM_DAY> | GET RX from
entered date to today
-fromtotx<SIM> <FROM_YEAR> <FROM_MONTH> <FROM_DAY> | GET TX from
entered date to today
-fromtorx<SIM> <FROM_YEAR> <FROM_MONTH> <FROM_DAY> <TO_YEAR>
<TO_MONTH> <TO_DAY> | GET RX from entered date to entered date
-fromtotx<SIM> <FROM_YEAR> <FROM_MONTH> <FROM_DAY> <TO_YEAR>
<TO_MONTH> <TO_DAY> | GET TX from entered date to entered date
-clear | Reset
collected data
-backup | Backup
database

```

To print the usage helper list, use **mdcollectedctl --help**.

### Examples:

- Get data usage value\* of SIM1 for the current day:

```
root@UCR:~# mdcollectedctl -cdayrx1
```

```
26558
```

- Get data usage value\* of SIM2 for the current month:

```
root@ UCR:~# mdcollectedctl -pmonthrx2
```

```
77701
```

\* All received/sent data usage values are returned in **kibibytes (KiB)**, which is an ISQ standard accepted by most major standard organizations.

1 kibibyte (KiB) =  $2^{10}$  bytes = 1024 bytes

1 mebibyte (MiB) =  $2^{10}$  kibibytes (KiB) =  $2^{20}$  bytes = 1 048 576 bytes

# Events Log

## Summary

The **Events Log** windows display records of such event as logins, reboots, resets, connections, configuration changes and more.

All Events	System Events	Network Events	Events Reporting	Reporting Configuration	
------------	---------------	----------------	------------------	-------------------------	--

### Events Log

Events Log

Events per page  Search

ID	Date	Event type	Event
345823S	2020-02-24 13:44:14	Reboot	Request after FW upgrade

All Events	System Events	Network Events	Events Reporting	Reporting Configuration	
------------	---------------	----------------	------------------	-------------------------	--

### System Log

All	Authentication	Reboot	SMS/Call	Mail	Configuration	DHCP
-----	----------------	--------	----------	------	---------------	------

Events Log

Events per page  Search

ID	Date	Event type	Event
345869	2020-02-21 14:01:59	DHCP	Leased 192.168.1.225 IP address for client - ██████████

All Events	System Events	Network Events	Events Reporting	Reporting Configuration	
------------	---------------	----------------	------------------	-------------------------	--

### Connections Log

All	Wireless	Mobile Data	Network Type	Network Operator
-----	----------	-------------	--------------	------------------

Connections Log











Events per page  Search

ID	Date	Event type	Event
4983	2020-02-21 13:57:58	Mobile Data	Mobile data connected: ██████████

## Events Reporting

The **Events Reporting** section gives you the ability to configure rules that will inform you via SMS or email when certain events occur on your router. These events can be almost anything – configuration changes, reboots, new connections, various status updates, SIM switches, etc.

## Events Reporting

Events Reporting Rules				
Event type	Event subtype	Action	Enable	Sort
FW upgrade	From file	Send SMS	<input checked="" type="checkbox"/>	  <input type="button" value="Edit"/> <input type="button" value="Delete"/>
Reboot	After unexpected shut down	Send email	<input checked="" type="checkbox"/>	  <input type="button" value="Edit"/> <input type="button" value="Delete"/>
SSH	All	Send SMS	<input checked="" type="checkbox"/>	  <input type="button" value="Edit"/> <input type="button" value="Delete"/>
Config change	OpenVPN	Send SMS	<input checked="" type="checkbox"/>	  <input type="button" value="Edit"/> <input type="button" value="Delete"/>
Backup	Switched to backup	Send SMS	<input checked="" type="checkbox"/>	  <input type="button" value="Edit"/> <input type="button" value="Delete"/>

Events Reporting Configuration			
Event type	Event subtype	Action	
<input type="text" value="Config change"/>	<input type="text" value="All"/>	<input type="text" value="Send SMS"/>	<input type="button" value="Add"/>

## Events Reporting Configuration

**Events Reporting Configuration** is used to create and customize Events Reporting Rules. Here you can specify any event type and subtype, chose whether you want to be informed by an SMS message or email, modify what kind of information you want receive should an event occur. To open this window, choose an Event type, Event subtype and Action and click the **Add** button. A new rule should appear in the Events Reporting Rules tab. Click the **Edit** button located next to that rule after which you will be redirected to that rule's configuration window.

## Send SMS

### Event Reporting Configuration

**Modify Event Reporting Rule**

Enable

Event type

Event subtype

Action

Enable delivery retry

Retry interval

Retry count

Message text on Event 

Time stamp - %ts
Router name - %m
WAN MAC address - %wm  
Serial number - %sn
LAN MAC address - %lm
Curren FW version - %fc  
LAN MAC address - %lm
Connection state - %cs
Operator name - %on  
Connection state - %cs
Connection type - %ct
Signal strength - %ss  
Connection type - %ct
SIM slot in use - %su
IMSI - %im  
SIM slot in use - %su
Event type - %et
Event text - %ex  
Event type - %et
FW available on server - %fs
LAN IP - %li  
FW available on server - %fs
Network state - %ns
WAN IP address - %wi  
Network state - %ns
New line - %nl

Get status after reboot

Status message after reboot 

Time stamp - %ts
Router name - %m
WAN MAC address - %wm  
Serial number - %sn
WAN MAC address - %wm
Curren FW version - %fc  
LAN MAC address - %lm
Connection state - %cs
Operator name - %on  
Connection state - %cs
Connection type - %ct
Signal strength - %ss  
Connection type - %ct
SIM slot in use - %su
IMSI - %im  
SIM slot in use - %su
Event type - %et
Event text - %ex  
Event type - %et
FW available on server - %fs
LAN IP - %li  
FW available on server - %fs
Network state - %ns
WAN IP address - %wi  
Network state - %ns
New line - %nl

Recipients

Recipient's phone number

FIELD NAME	VALUE	DESCRIPTION
<b>Enable</b>	yes   no; Default: <b>no</b>	Toggles the rule ON or OFF
<b>Event type</b>	Config change   New DHCP client   Mobile data   SMS   SIM switch   Signal Strength   Reboot   SSH   WebUI   New WiFi client   LAN port state   WAN failover   Restore point   GPS;	The type of event that you wish to receive information about

Default: **Config change**

<b>Event subtype</b>	<b>Sample:</b> After unexpected shut down	Specified event's sub-type. This field changes in accordance with <b>Event type</b>
<b>Action</b>	Send SMS   Send email; Default: <b>Send SMS</b>	Action that is to be taken after the specified event occurs
<b>Enable delivery retry</b>	yes   no; Default: <b>no</b>	Toggles delivery retry On or OFF. If for some reason the message delivery is unsuccessful, the router initiates a retry if this field is enabled
<b>Retry interval</b>	1 min.   5 min.   10 min.   15 min.   30 min.   60 min.; Default <b>5 min.</b>	Specifies when the router should try re-sending the message in case the first attempt was a failure
<b>Retry count</b>	2   3   4   5   6   7   8   9   10; Default: <b>2</b>	Specifies the maximum number of failed attempts after which the router does not try to send the message anymore
<b>Message text on Event</b>	string; Default: <b>Router name - %rn; Event type - %et; Event text - %ex; Time stamp - %ts;</b>	Specifies the text that the message will contain
<b>Get status after reboot</b>	yes   no; Default: <b>no</b>	Specifies whether the router should send an SMS message indicating the router's status after the reboot in addition to the original message
<b>Status message after reboot</b>	string; Default: <b>Router name - %rn; WAN IP - %wi; Data Connection state - %cs; Connection type - %ct; Signal strength - %ss; New FW available - %fs;</b>	Specifies the text that the status message will contain. This field becomes visible only if <b>Get status after reboot</b> is checked
<b>Recipients</b>	Single number   User group; Default: <b>Single number</b>	Specifies the intended recipients. A guide on how to create a User group



can be found in the SMS Utilities chapter, User Groups section

---

<b>Recipient's phone number</b>	phone number; Default: " "	The intended recipient's phone number. To add more than one number, click the green plus symbol located to the right of this field. The phone number must be entered in the international format, but without dash symbols or spaces, e.g., <b>+120161234567</b>
---------------------------------	----------------------------	--

---

## Send Email

### Event Reporting Configuration

**Modify Event Reporting Rule**

Enable

Event type

Event subtype

Action

Enable delivery retry

Retry interval

Retry count

Subject

Message text on Event

Time stamp - %ts  
Serial number - %sn  
LAN MAC address - %lm  
Connection state - %cs  
Connection type - %ct  
SIM slot in use - %su  
Event type - %et  
FW available on server - %fs  
Network state - %ns  
New line - %nl

Router name - %rn  
WAN MAC address - %wm  
Current FW version - %fc  
Operator name - %on  
Signal strength - %ss  
IMSI - %im  
Event text - %ex  
LAN IP - %li  
WAN IP address - %wi

Get status after reboot

SMTP server

SMTP server port

Secure connection

User name

Password

Sender's email address

Recipient's email address

Send test email

FIELD NAME	VALUE	DESCRIPTION
<b>Enable</b>	yes   no; Default: <b>no</b>	Toggles the rule ON or OFF
<b>Event type</b>	Config change   New DHCP client   Mobile data   SMS   SIM switch   Signal Strength   Reboot   SSH   WebUI	The type of event that you wish to receive information about

New WiFi client | LAN port state | WAN failover | Restore point | GPS;

Default: **Config change**

<b>Event subtype</b>	<b>Sample:</b> After unexpected shut down	Specified event's sub-type. This field changes in accordance with <b>Event type</b>
<b>Action</b>	Send SMS   Send email; Default: <b>Send SMS</b>	Action that is to be taken after the specified event occurs
<b>Enable delivery retry</b>	yes   no; Default: <b>no</b>	Toggles delivery retry On or OFF. If for some reason the message delivery is unsuccessful, the router initiates a retry if this field is enabled
<b>Retry interval</b>	1 min.   5 min.   10 min.   15 min.   30 min.   60 min.; Default <b>5 min.</b>	Specifies when the router should try re-sending the message in case the first attempt was a failure
<b>Retry count</b>	2   3   4   5   6   7   8   9   10; Default: <b>2</b>	Specifies the maximum number of failed attempts after which the router does not try to send the message anymore
<b>Subject</b>	string; Default: " "	Specifies the subject of the email message
<b>Message text on Event</b>	string; Default: <b>Router name - %rn; Event type - %et; Event text - %ex; Time stamp - %ts;</b>	Specifies the text that the message will contain
<b>Get status after reboot</b>	yes   no; Default: <b>no</b>	Specifies whether the router should send an SMS message indicating the router's status after the reboot in addition to the original message. If this is checked you will be prompted to enter the text that the status message should contain

<b>SMTP server</b>	ip   host; Default: " "	Sender's email service provider's SMTP server. If you don't know the SMTP server's address, you can easily look it up online since it is public information
<b>SMTP port</b>	integer [0..65535]; Default: " "	Sender's email service provider's SMTP port. If you don't know the SMTP server's port, you can easily look it up online since it is public information
<b>Secure connection</b>	yes   no; Default: <b>no</b>	Toggles secure connection feature ON or OFF (use only if the email service provider's server supports SSL or TLS)
<b>Username</b>	string; Default: " "	Sender's email account's login user name
<b>Password</b>	string; Default: " "	Sender's email account's login password
<b>Sender's email address</b>	email; Default: " "	The email address of the sender, i.e., the report message will be sent from this email. Make sure this is the same email that you provided login information to
<b>Recipient's email address</b>	email; Default: " "	The intended recipient's email address. To add more than one email address, click the green plus symbol located to the right of this field
<b>Send test mail</b>	-	Sends a test mail using the information that you provided. Once you click this button, the router will login to the provided email account and send the specified message to the specified address(-es). You should always send a test mail before

finishing the configuration to make sure that everything is in order

---

### Event Types and Sub-types

---

The examples provided above are both concerning the **Reboot** Event type and **After unexpected shut down** sub-type. This section is an overview of all other Event type and sub-types.

Config change

---

ENEBT SUB-TYPE	DESCRIPTION
----------------	-------------

---

<b>All</b>	Sends a report message when any type of configuration changes are applied
------------	---

---

<b>OpenVPN</b>	Sends a report message when any <b>OpenVPN</b> configuration changes are applied. For example, whenever a new OpenVPN instance is created, an OpenVPN instance gets disabled/enabled, an OpenVPN instance's protocol is changed from UDP to TCP or vice versa, etc.
----------------	---

---

<b>SMS</b>	Sends a report message when any SMS related configuration changes are applied. For example, whenever a new <b>SMS Utilities</b> rule is created or changed, changes are made to <b>Auto Reply</b> or <b>Remote configurations</b> , etc.
------------	--

---

<b>Mobile traffic</b>	Sends a report message when <b>Mobile Traffic</b> Logging is enabled/disabled or logging interval is changed.
-----------------------	---

---

<b>Multiwan</b>	Sends a report message when changes to WAN <b>Backup</b> configuration are applied. For example, whenever a switch from using Wired as main WAN to backup WAN occurs, Wireless is added as a Backup WAN, Health monitor configurations are changed, etc.
-----------------	--

---

**SIM switch** Sends a report message when any **SIM Management** configuration changes are applied. For example, whenever the primary SIM card is changed, a new SIM switch rule is configured, SIM switching is turned ON or OFF, etc.

---

**Mobile** Sends a report message when any **Mobile** configuration changes are applied. For example, whenever Service mode, APN, Connection type is changed, etc.

---

**Data limit** Sends a report message when any **Mobile Data Limit** configuration changes are applied. For example, whenever new data limit is configured, data limit gets disabled/enabled on SIM1/SIM2, data limit period is changed, etc.

---

**GPS** Sends a report message when any configuration changes concerning **GPS** are applied. For example, whenever GPS gets enabled/disabled, Remote host/IP address is changed, new **Geofencing** area is defined, etc.

---

**Events reporting** Sends a report message when any configuration changes to Events Reporting are applied. For example, whenever a new Events Reporting Rule is created, changed, deleted, etc.

---

**Periodic reboot** Sends a report message when any configuration changes to **Periodic Reboot** are applied. For example, whenever Periodic Reboot gets enabled/disabled, Periodic Reboot interval is changed, etc.

---

**SNMP** Sends a report message when any configuration changes to **SNMP** are applied. For example, whenever SNMP service is enabled/disabled, SNMP remote access is enabled/disabled, SNMP port is changed, etc.

---

<b>GRE Tunnel</b>	Sends a report message when any configuration changes to <b>GRE Tunnel</b> are applied. For example, whenever a new GRE Tunnel instance is created, deleted, enabled/disabled, Local tunnel IP is changed, etc.
<b>Ping reboot</b>	Sends a report message when any configuration changes to <b>Ping Reboot</b> are applied. For example, whenever Ping Reboot gets enabled/disabled, host to ping has changed, etc.
<b>Auto update</b>	Sends a report message when any configuration changes to Auto update are applied
<b>Site blocking</b>	Sends a report message when any configuration changes to <b>Site Blocking</b> are applied. For example, whenever Whitelist is changed to Blacklist or vice versa, a new entry is added to Blacklist/Whitelist, etc.
<b>PPTP</b>	Sends a report message when any configuration changes to <b>PPTP</b> are applied. For example, whenever a new PPTP instance was created, deleted, enabled/disabled, PPTP server address was changed, etc.
<b>Hotspot</b>	Sends a report message when any configuration changes to <b>Hotspot</b> are applied. For example, whenever Hotspot SSID was changed, Radius server was changed, Hotspot was enabled/disabled, etc.
<b>Input/Output</b>	Sends a report message when any configuration changes to <b>Input/Output</b> are applied. For example, whenever a new <b>Periodic Output Control</b> Rule was created, changed, deleted, an output was turn ON/OFF, etc.
<b>Content blocker</b>	Sends a report message when any configuration changes to <b>Proxy Based Content Blocker</b> are applied. For example,

whenever Whitelist is changed to Blacklist or vice versa, a new entry is added to Blacklist/Whitelist, etc.

---

<b>Login page</b>	Sends a report message when any <b>Language Settings</b> are changed
<b>Language</b>	Sends a report message when any <b>Language Settings</b> are changed
<b>Profile</b>	Sends a report message when a new <b>Profile</b> is added or deleted
<b>DDNS</b>	Sends a report message when any configuration changes to <b>Dynamic DNS</b> are applied. For example, whenever a new DDNS instance is created, changed, deleted or edited
<b>IPsec</b>	Sends a report message when any configuration changes to <b>IPsec</b> are applied. For example, a new IPsec instance is created, changed, deleted, etc.
<b>Access control</b>	Sends a report message when any configuration changes to Access Control are applied. For example, SSH/HTTP/HTTPS remote or local access is enabled/disabled, changes are made to SSH or WebUI Access Secure, etc.
<b>DHCP</b>	Sends a report message when any configuration changes to <b>DHCP</b> are applied. For example, whenever DHCP Server is enabled/disabled, DHCP address range is changed
<b>RS232/RS485</b>	Sends a report message when any configuration changes to <b>RS232/RS485</b> are applied. For example, whenever RS232 or RS485 configuration is enabled/disabled, baud rate is changed, etc.

---



---

<b>VRRP</b>	Sends a report message when any configuration changes to <b>VRRP</b> are applied. For example, whenever VRRP is enabled/disabled, VRRP IP address is changed, etc.
<b>SSH</b>	Sends a report message when any configuration changes to SSH are applied
<b>Network</b>	Sends a report message when any Network related configuration changes are applied. For example, whenever Main WAN is changed, LAN IP address is changed, a Wi-Fi Access Point is enabled/disabled, etc.
<b>Wireless</b>	Sends a report message when any configuration changes to <b>Wireless</b> are applied. For example, a new Wi-Fi Access point is created, deleted, enabled/disabled, SSID is changed, etc.
<b>Firewall</b>	Sends a report message when any configuration changes to <b>Firewall</b> are applied. For example, a new Traffic rule is added, a new SNAT rule is added, a rule is disabled/enabled, etc.
<b>NTP</b>	Sends a report message when any configuration changes to <b>NTP</b> are applied. For example, whenever NTP is enabled/disabled, Time zone is changed, etc.
<b>L2TP</b>	Sends a report message when any configuration changes to <b>L2TP</b> are applied. For example, whenever a new L2TP instance was created, changed, deleted, etc.
<b>Other</b>	Sends a report message when any configuration changes other than the ones provided above are applied

---

New DHCP client

---

EVENT SUB-TYPE	DESCRIPTION
<b>All</b>	Sends a report message when a new devices is connected to the router either via LAN or Wi-Fi
<b>Connected from WiFi</b>	Sends a report message when a new device is connected to the router via Wi-Fi
<b>Connected from LAN</b>	Sends a report message when a new device is connected to the router via LAN port

Mobile Data

EVENT SUB-TYPE	DESCRIPTION
<b>All</b>	Sends a report message when mobile data connection status changes (from Connected to Disconnected or vice versa)
<b>Connected</b>	Sends a report message when mobile data connection is achieved
<b>Disconnected</b>	Sends a report message when mobile data connection is lost

SMS

EVENT SUB-TYPE	DESCRIPTION
<b>SMS received</b>	Sends a report message when the router receives a new SMS message

## SIM Switch

---

<b>EVENT SUB-TYPE</b>	<b>DESCRIPTION</b>
<b>All</b>	Sends a report message when the router switches the SIM card in use
<b>From SIM1 to SIM2</b>	Sends a report message when the router switches from using SIM1 to SIM2
<b>From SIM2 to SIM1</b>	Sends a report message when the router switches from using SIM2 to SIM1

## Signal Strength

---

<b>EVENT SUB-TYPE</b>	<b>DESCRIPTION</b>
<b>All</b>	Sends a report message when the router's <b>RSSI</b> value leaves any one of the below specified ranges
<b>-121 dBm -113 dBm</b>	Sends a report message when the router's RSSI value leaves the -121 dBm to -113 dBm range
<b>-113 dBm -98 dBm</b>	Sends a report message when the router's RSSI value leaves the -113 dBm to -98 dBm range
<b>-98 dBm -93 dBm</b>	Sends a report message when the router's RSSI value leaves the -98 dBm to -93 dBm range

<b>-93 dBm -75 dBm</b>	Sends a report message when the router's RSSI value leaves the -93 dBm to -75 dBm range
------------------------	---

---

<b>-75 dBm -60 dBm</b>	Sends a report message when the router's RSSI value leaves the -75 dBm to -60 dBm range
------------------------	---

---

<b>-60 dBm -50 dBm</b>	Sends a report message when the router's RSSI value leaves the -60 dBm to -50 dBm range
------------------------	---

---

Reboot

---

<b>EVENT SUB-TYPE</b>	<b>DESCRIPTION</b>
<b>All</b>	Sends a report message when the router starts up after any type of reboot (except factory reset)
<b>After unexpected shutdown</b>	Sends a report message when the router starts up after any type of reboot (except factory reset)
<b>After FW upgrade</b>	Sends a report message when the router starts back up again after FW upgrade
<b>From WebUI</b>	Sends a report message when the router starts up after a reboot command is initiated from the router's WebUI Administration->Reboot section
<b>From SMS</b>	Sends a report message when the router starts up after a reboot command is initiated via SMS
<b>From Input/Output</b>	Sends a report message when the router starts up after a reboot command is initiated via Input/Output

---

**From ping reboot** Sends a report message when the router starts up after a reboot command is initiated by the Ping Reboot function

---

**From periodic reboot** Sends a report message when the router starts up after a reboot command is initiated by the Periodic Reboot function

---

**From button** Sends a report message when the router starts up after being restarted by the press of the physical button located on the router

---

SSH

---

<b>EVENT SUB-TYPE</b>	<b>DESCRIPTION</b>
-----------------------	--------------------

---

<b>All</b>	Sends a report message when someone connects to the router via SSH (either successfully or unsuccessfully)
------------	--

---

<b>Successful authentication</b>	Sends a report message when someone successfully connects to the router via SSH
----------------------------------	---

---

<b>Unsuccessful authentication</b>	Sends a report message when someone unsuccessfully tries to connect to the router via SSH
------------------------------------	---

---

WebUI

---

<b>EVENT SUB-TYPE</b>	<b>DESCRIPTION</b>
-----------------------	--------------------

---

<b>All</b>	Sends a report message when someone connects to the router via HTTP or HTTPS (either successfully or unsuccessfully)
------------	--

---

<b>Successful authentication</b>	Sends a report message when someone successfully connects to the router via HTTP or HTTPS
<b>Unsuccessful authentication</b>	Sends a report message when someone unsuccessfully tries to connect to the router via HTTP or HTTPS

New WiFi client

<b>EVENT SUB-TYPE</b>	<b>DESCRIPTION</b>
<b>All</b>	Sends a report message when a device connects to or disconnects from the router's WLAN (Wireless Network or Wireless LAN)
<b>Connected</b>	Sends a report message when a device connects to the router's WLAN
<b>Disconnected</b>	Sends a report message when a device disconnects from the router's WLAN

LAN Port State

<b>EVENT SUB-TYPE</b>	<b>DESCRIPTION</b>
<b>All</b>	Sends a report message when a device is either plugged in or unplugged from one of the router's LAN ports
<b>Unplugged</b>	Sends a report message when a device is unplugged from one of the router's LAN ports

**Plugged in** Sends a report message when a device is plugged into one of the router's LAN ports

---

WAN failover

---

<b>EVENT SUB-TYPE</b>	<b>DESCRIPTION</b>
-----------------------	--------------------

---

<b>All</b>	Sends a report message when the router switches from using the Main WAN to using the Backup WAN and vice versa
------------	--

---

<b>Switched to main</b>	Sends a report message when the router switches from using the Main WAN to using the Backup WAN
-------------------------	---

---

<b>Switched to backup</b>	Sends a report message when the router stops using the Backup WAN and start using the Main WAN
---------------------------	--

---

Restore Point

---

<b>EVENT SUB-TYPE</b>	<b>DESCRIPTION</b>
-----------------------	--------------------

---

<b>All</b>	Sends a report message when either when a new Restore point is created or a Restore Point is loaded in to the router
------------	--

---

<b>Save</b>	Sends a report message when a new Restore Point is created
-------------	--

---

<b>Load</b>	Sends a report message when a Restore Point is loaded on to the router
-------------	--

---

GPS

---

EVENT SUB-TYPE	DESCRIPTION
<b>All</b>	Sends a report message when the router moves in and out of the GPS Geofence area
<b>Left geofence</b>	Sends a report message when the router leaves the GPS Geofence area
<b>Entered geofence</b>	Sends a report message when the router enter the GPS Geofence area





## Reporting Configuration

The **Reporting Configuration** section lets you create rules that transfer logs to email or FTP.

*FTP*

### Events Log Files Report

Create rules for Events Log reporting.

Events Log Report Rules			
Events log	Transfer type	Enable	Sort
Network	Email	<input checked="" type="checkbox"/>	  <span>Edit</span> <span>Delete</span>
System	FTP	<input checked="" type="checkbox"/>	  <span>Edit</span> <span>Delete</span>

Events Log Reporting Configuration		
Events log	Transfer type	
System ▾	Email ▾	<span>Add</span>

FIELD NAME	VALUE	DESCRIPTION
<b>Enable</b>	yes   no; Default: <b>no</b>	Toggles the log file report rule ON or OFF



<b>Events log</b>	System   Network   All; Default: <b>System</b>	Specifies which log to transfer
<b>Transfer type</b>	Email   FTP   Syslog server; Default: <b>Email</b>	Specifies whether to transfer the log(s) to FTP, Syslog server or Email
<b>Compress file</b>	yes   no; Default: <b>no</b>	Compress events log file using gzip
<b>Enable delivery retry</b>	yes   no; Default: <b>no</b>	Toggles delivery retry On or OFF. If for some reason the message delivery is unsuccessful, the router initiates a retry if this field is enabled
<b>Host</b>	host   ip; Default: " "	FTP server's IP address or hostname
<b>Retry count</b>	2   3   4   5   6   7   8   9   10; Default: <b>2</b>	Specifies the maximum number of failed attempts after which the router does not try to send the message anymore
<b>User name</b>	string; Default: " "	Login user name used for authentication to the FTP server
<b>Password</b>	string; Default: " "	Login password used for authentication to the FTP
<b>Interval between reports</b>	Week   Month   Year; Default: <b>Week</b>	Specifies how often the reports should be sent
<b>Weekday   Month day</b>	weekday   month day; Default: <b>Sunday</b>	Specifies the day of the month/week when the logging should take place. This field

changes in accordance with **Interval between reports**

<b>Hour</b>	integer [1..24]; Default: <b>1</b>	Specifies on the hour of the day when the logging should take place
-------------	---------------------------------------	---

## Email

### Events Log Report Configuration

**Modify events log file report rule**

Enable

Events log Network ▾

Transfer type Email ▾

Compress file

Subject


Message

SMTP server


SMTP server port

Secure connection

User name

Password  

Sender's email address

Recipient's email address  

Interval between reports Week ▾

Weekday Sunday ▾

Hour 1 ▾

FIELD NAME	VALUE	DESCRIPTION
<b>Enable</b>	yes   no; Default: <b>no</b>	Toggles the log file report rule ON or OFF
<b>Events log</b>	System   Network   All; Default: <b>System</b>	Specifies which log to transfer

<b>Transfer type</b>	Email   FTP; Default: <b>Email</b>	Specifies whether to transfer the log(s) to FTP or Email
<b>Compress file</b>	yes   no; Default: <b>no</b>	Compress events log file using gzip
<b>Subject</b>	string; Default: " "	Specifies the subject of the email log message
<b>Message</b>	string; Default: " "	The text contained in the log email. This has nothing to do with the log itself, which will be sent as an attached file
<b>SMTP server</b>	ip   host; Default: " "	Sender's email service provider's SMTP server. If you don't know the SMTP server's address, you can easily look it up online since it is public information
<b>SMTP server port</b>	integer [0..65535]; Default: " "	Sender's email service provider's SMTP server. If you don't know the SMTP server's address, you can easily look it up online since it is public information
<b>Secure connection</b>	yes   no; Default: <b>no</b>	Toggles secure connection feature ON or OFF (use only if the email service provider's server supports SSL or TLS)
<b>Username</b>	string; Default: " "	Sender's email account's login user name
<b>Password</b>	string; Default: " "	Sender's email account's login password
<b>Sender's email address</b>	email; Default: " "	The email address of the sender, i.e., the report message will be sent from this email.

Make sure this is the same email that you provided login information to

---

<b>Recipient's email address</b>	email; Default: " "	The intended recipient's email address. To add more than one email address, click the green plus symbol located to the right of this field
<b>Interval between reports</b>	Week   Month   Year; Default: <b>Week</b>	Specifies how often the reports should be sent
<b>Weekday   Month day</b>	weekday   month day; Default: <b>Sunday</b>	Specifies the day of the month/week when the logging should take place. This field changes in accordance with <b>Interval between reports</b>
<b>Hour</b>	integer [1..24]; Default: <b>1</b>	Specifies on the hour of the day when the logging should take place

---

# Network Section

## Mobile

### Summary

The **Mobile** page is used for setting parameters related to the mobile data connection. All of the examples given below are concerning SIM1. However, SIM2 configuration is identical to SIM1. To configure SIM2 all you need to do is select the SIM2 tab. This is true for all cases in the *Network* → *Mobile* section of the router's WebUI (General, SIM Management, etc.)

### General

The **General** section is used to configure the SIM card parameters that define how the router establishes a cellular connection.

### Mobile Configuration

The **Mobile Configuration** section is used to configure main SIM card parameters. Refer to the figure and table below for information on the fields contained in that section.

The screenshot shows the 'Mobile Configuration' web interface. At the top, there is a title 'Mobile Configuration' and two tabs: 'SIM 1' and 'SIM 2', with 'SIM 2' selected. Below the tabs, the configuration fields are as follows:

- Connection type: QMI (dropdown)
- Mode: NAT (dropdown)
- APN: [text input]  Auto
- PIN number: [text input]
- Dialing number: \*99# (text input)
- MTU: 1500 (text input)
- Authentication method: None (dropdown)
- Service mode: Automatic (dropdown)
- Deny data roaming:
- Use IPv4 only:

A warning message is displayed below the Mode dropdown: 'Passthrough and Bridge modes are disabled when multiwan is enabled'.

Field	Value	Description
<b>Connection type</b>	QMI   PPP; default: <b>QMI</b>	<p>How the router's modem will establish a connection to the carrier.</p> <ul style="list-style-type: none"> <li>• <b>PPP</b> - uses a dialling number to establish a data connection.</li> <li>• <b>QMI</b> - does not use a dialling number to connect and is usually faster than PPP.</li> </ul>
<b>Mode</b>	NAT   Bridge *   Passthrough**; default: <b>NAT</b>	<p>Mobile connection operating mode.</p> <ul style="list-style-type: none"> <li>• <b>NAT</b> - the mobile connection uses NAT (network address translation).</li> <li>• <b>Bridge</b> - bridges the LTE data connection with LAN. In this mode the router relay the IP address received from the ISP to another LAN device (e.g., computer). Using Bridge mode will disable most of the router's capabilities and you will only be able to access your router's WebUI with a <a href="#">static IP configuration</a>.</li> <li>• <b>Passthrough</b> - works in a similar fashion to Bridge mode, except in Passthrough mode the router will have an Internet connection and be reachable from LAN, because the router's DHCP Server is not disabled.</li> </ul>
<b>APN</b>	string; default: <b>none</b>	<p>An Access Point Name (APN) is a gateway between a GSM, GPRS, 3G or 4G mobile network and another computer network. Depending on the contract, some operators may require you to use an APN just to complete the registration on a network. In other cases, APN is used to get special parameters from the operator (e.g., a <a href="#">public IP address</a>) depending on the contract.</p> <p>An APN Network Identifier cannot start with any of the following strings:</p> <ul style="list-style-type: none"> <li>• rac;</li> <li>• lac;</li> <li>• sgsn;</li> <li>• rnc;</li> </ul> <p>it cannot end in:</p>

<b>Auto APN</b>	checkbox; default: <b>enabled</b>	<ul style="list-style-type: none"> <li>• .gprs;</li> </ul> <p>And it cannot contain the asterisk symbol (*).</p> <p>Auto APN scans an internal Android APN database and selects an APN based on the SIM card's operator and country. If the first automatically selected APN doesn't work, it attempts to use the next existing APN from the database.</p>
<b>PIN number</b>	string; default: <b>none</b>	<p>A 4-digit long numeric password used to authenticate the modem to the SIM card. <b>Reminder: Firstboot will not reset the PIN number, it must be changed manually</b></p>
<b>PUK number</b>	string; default: <b>none</b>	<p>A 12-digit long numeric password used to reset a personal identification number (PIN) that has been lost or forgotten.</p>
<b>Dialing number</b>	string; default: <b>none</b>	<p>A <a href="#">dial code</a> used to establish a mobile PPP connection.</p>
<b>MTU</b>	integer [0..1500]; default: <b>1500</b>	<p>Sets the maximum transmission unit (MTU) size. It is the largest size of a protocol data unit (PDU) that can be transmitted in a single network layer transaction.</p>
<b>Authentication method</b>	CHAP   PAP   None; default: <b>None</b>	<p>Authentication method that your GSM carrier uses to authenticate new connections on its network. If you select PAP or CHAP, you will also be required to enter a username and password.</p>
<b>Service mode</b>	2G only   3G only   Automatic; default: <b>Automatic</b>	<p>Your service mode preference. If your local mobile network supports 2G, 3G and 4G (LTE), you can specify to which type of network you wish to connect to. For example, if you choose 2G only, the router will connect to a 2G network, so long as it is available, otherwise it will connect to a network that provides better connectivity. If you select Automatic, then the router will connect to the network that provides the best connectivity.</p>
<b>Deny data roaming</b>	yes   no; default: <b>no</b>	<p>When enabled, this option prevents the device from establishing a mobile data connection while not in your home network (roaming conditions).</p>

**Use IPv4 only**      yes | no; default: **yes**      When enabled, this makes the device only use IPv4 settings for the mobile connection.

## Mobile data on demand

The **mobile data on demand** function keeps the mobile data connection *on* only when it is in use. When the router detects that there is no traffic, it shuts down the mobile data connection and turns it back *on* only when there is a "Demand" (a user trying to reach a website, for example). Refer to the figure and table below for more information.

Field	Value	Description
<b>Enable</b>	yes   no; default: <b>no</b>	Turns mobile data on demand on or off <b>Important:</b> this function is only available with PPP Connection type.
<b>No data timeout (sec)</b>	integer [10..3600]; default: <b>10</b>	Mobile data connection will be terminated if no data is transferred during the timeout period specified in this field.

## Network frequency bands

The **network frequency bands** section provides the possibility to manually choose which frequency band the router's module should use for the cellular connection.

Simply select *Manual* connection method and check the bands that you want the module to use. If all bands are unchecked, the band that provides the best connectivity will be used.



**Network Frequency Bands**

This is band selector option. You can't force specific band usage, you could choose it if module detects more than one band on selected network service. If all bands are unchecked any band will be used.

SIM 1
SIM 2

---

Connection method Manual

- GSM900
- GSM1800
- WCDMA 850
- WCDMA 900
- WCDMA 2100
- LTE B1
- LTE B3
- LTE B5
- LTE B7
- LTE B8

Available network frequency bands may differ based on router modem module. More information about router module supported network frequency bands: <https://www.quectel.com/product/ec25.htm>

Information about router's modem module can be found by going to *Status* → *Device Information* page and checking FW Version field. Usually first 5-7 characters show modem module series code. For example:

**Modem**

Model	EC25
FW version	EC25EUGAR06A03M4G

EC25EU

EC25-EU

## Force LTE network

The **Force LTE network** function makes the router forcefully connect to an LTE network at a specified period of time. Refer to the figure and table below for more information.

**Force LTE network**

Enable

Reregister

Interval (sec)

Field	Value	Description
<b>Enable</b>	yes   no; default: <b>no</b>	Turns force LTE network on or off.
<b>Reregister</b>	yes   no; default: <b>no</b>	When enabled the modem will attempt to reregister to the carrier before trying to connect to an LTE network.
<b>Timeout (sec)</b>	integer [180..3600]; default: <b>300</b>	Time in seconds between forced connection attempts.

## Passthrough mode

In **Passthrough** mode the router assigns its mobile WAN IP address to another device. It is similar to *Bridge* mode, except in Passthrough mode other devices can still connect to the router and get LAN IP addresses and both other clients and the router retain Internet access, while Bridge mode also disables the router's DHCP Server.

To begin configuring Passthrough mode, make sure that WAN failover is turned off and mobile is set as main WAN in the *Network* → *WAN* page. Then in the *Network* → *Mobile* page select *Mode: Passthrough* in the mobile configuration section. You will then see additional configuration fields appear at the bottom of the section.

**Important:** using Passthrough mode will disable most of the router's other capabilities.

DHCP mode

MAC Address

Field	Value	Description
<b>DHCP mode</b>	Static   Dynamic   No DHCP; default: <b>Static</b>	Specifies DHCP mode used with Passthrough. <ul style="list-style-type: none"> <li>• <b>Static</b> - manually binds the WAN IP address to the device with the specified MAC address. This device will get an IP address from your GSM operator. Other devices that are connected to the router will get IP</li> </ul>

addresses from the router's DHCP server, but they will not have internet access.

- **Dynamic** - the GSM operator will connect to the router first and give out an IP address to one of your connected devices. The device will be selected at random. Therefore, you should usually use Dynamic mode when you have only one device (e.g., computer) connected to the router. When using Passthrough in Dynamic mode, the router's LAN DHCP server will be disabled, but it will be enabled again automatically when you switch to a different mode.
- **No DHCP** - IP address, subnet mask, default gateway and DNS information from the GSM operator will have to be entered on your computer manually. When using Passthrough in No DHCP mode, the router's LAN DHCP server will be disabled, but it will become enabled automatically when you switch to a different mode.

**MAC address**      mac; default: **none**      MAC address of a LAN device (e.g., computer).

## Bridge mode

In **Bridge** mode the router assigns its WAN IP address to another device. It is used instead of Network Address Translation (NAT) in order to make the router "transparent" in the communication process. The main difference between Passthrough and Bridge is that in Passthrough, the router's DHCP Server still works and the regular LAN interface is still up, allowing clients to connect to the router's local network as usual, while Bridge mode disables all of these features and simply gives a single specified device its WAN IP address. Since Bridge uses less of the router's features, it is a bit faster than Passthrough.

To begin configuring Bridge mode, make sure that WAN failover is turned off and mobile is set as main WAN in the *Network* → *WAN* page. Then in the *Network* → *Mobile* page select *Mode: Bridge* in the mobile configuration section. You will then see an additional configuration field for entering a MAC address appear *Mode* field.

**Important:** using Bridge mode will disable most of the router's other capabilities.

**Mobile Configuration**

Mobile Configuration

SIM 1 SIM 2

Connection type QMI

Mode Bridge

Bind to MAC

Field	Value	Description
<b>Bind to MAC</b>	mac; default: <b>none</b>	Specifies the MAC address of the device that will work with the router in Bridge mode, i.e., the device whose MAC is specified in this field will be assigned the router's Mobile WAN IP address.

If you have configured Bridge mode and can no longer reach your router, you'll need to set up a Static IP address on your PC in order to do so.

## SIM Management

The **SIM Management** section provides you with the possibility to specify which SIM card slot is the primary one and setup SIM switching rules. SIM switching is used as a failover mechanism when the user has two working SIM cards. For example, if the user has two SIM cards with limited data, you can setup a rule that switches the SIM card in use to the secondary SIM card when the data limit is reached. You can setup similar rules for SMS limit, signal strength and more.

### Primary card

The **Primary card** section is used to select which SIM slot will host the router's primary SIM card. The primary SIM card is the one which is active by default, while the secondary card stays inactive until switched to or set as primary.

**SIM Switching**

Primary Card

Primary SIM card SIM 1

**Note:** both SIM cards cannot be active at the same time.

### SIM Switching

The **SIM switching** section is used to enable automatic SIM switching and to set the SIM switching check interval. Refer to the figure and table below for more information.

**SIM Switching**

Enable automatic switching

Check interval

Field	Value	Description
<b>Enable automatic switching*</b>	yes   no; default: <b>no</b>	Turns automatic SIM Switching on or off.
<b>Check interval</b>	integer; default: <b>30</b>	The frequency at which the router will check for condition changes corresponding to SIM switch rules. If such a condition exists, the router will perform a SIM switch, if not - it will check for the same conditions again after the amount of time specified in this field.

### *SIM switching rules*

Below the SIM switching section you can configure **SIM switching rules**, i.e., set up circumstances under which the router will perform a switch from using one SIM card to the other. Refer to the figure and table below for information.

SIM1 To SIM2

SIM2 To SIM1

On weak signal

On data limit

On SMS limit

On roaming

No network

On network denied

On data connection fail

Field	Value	Description
<b>On weak signal</b>	yes   no; default: <b>no</b>	Performs a SIM switch when signal strength value ( <a href="#">RSSI</a> in dBm) falls below a specified threshold. When this field is checked you will see an additional field for entering the minimum signal strength value appear.
<b>On data limit</b>	yes   no; default: <b>no</b>	Performs a SIM switch when the SIM card reaches the specified data limit for the designated period. Mobile data limit can be

		configured in the Services → Mobile → <a href="#">Mobile Data Limit</a> page.
<b>On SMS limit</b>	yes   no; default: <b>no</b>	Performs a SIM switch when the SIM card reaches the specified sent SMS limit for the designated period. SMS limit can be configured in the Services → Mobile → <a href="#">SMS Limit</a> page.
<b>On roaming</b>	yes   no; default: <b>no</b>	Performs a SIM switch when roaming conditions are detected (i.e., when the SIM card connects to a foreign operator).
<b>No network</b>	yes   no; default: <b>no</b>	Performs a SIM switch when the SIM card cannot find an operator to connect to.
<b>On network denied</b>	yes   no; default: <b>no</b>	Performs a SIM switch when access to a network is denied (usually by an operator).
<b>On data connection fail</b>	yes   no; default: <b>no</b>	Performs a SIM switch when the router does receive an LCP or ICMP echo from a specified host address.

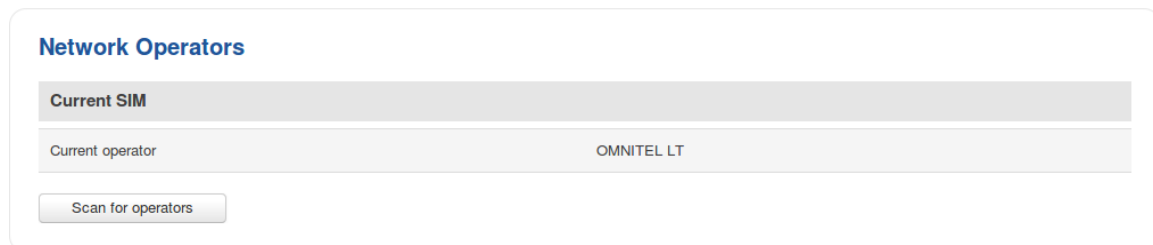
**Note:** remember to check the *Enable automatic switching* field above in order to make you SIM switching rules work.

## Network Operators

The **Network Operators** tab provides you with the possibility to scan for and manually manage mobile network operators to which the router's SIM card can connect to. Operator selection is only available for the primary SIM card. In order to specify an operator for the other SIM card it must first be selected as the primary SIM in the SIM Management section.

### Scan For Network Operators

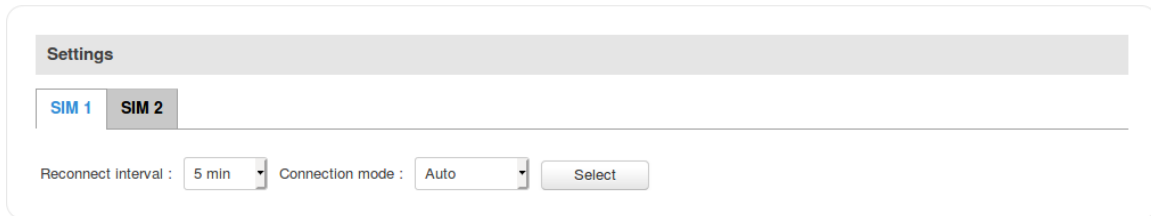
**Scan For Network Operators** is a function that initiates a scan for mobile network operators available in your area. To initiate a scan, press the 'Scan for operators' button. After you do, you will be prompted with a pop-up asking if you wish to proceed. This is because while the scan is in progress you will lose your data connection for approximately 2 minutes.



After the scan is complete you will be presented with a list of operators available in your area. The list provides such information as operator's name, code and network access

type. You can also choose to which operator you would like to connect provided that the operator's status is not *Forbidden*.

Below the list you can select how to the router should connect to network operators:



Settings

SIM 1 SIM 2

Reconnect interval : 5 min Connection mode : Auto Select

The 'Reconnect interval' box specifies how often the device will attempt to reconnect to a network operator, while the 'Connection mode' specifies the logic of how the router will connect operators:

- **Auto** - the router automatically connects to the network operator that provides the best connectivity.
- **Manual** - prompts you to enter an operator's code\*. The router will then only attempt to connect to the operator whose code was specified (even if previous attempts have been unsuccessful).
- **Manual-Auto** - prompts you to enter an operator's code\* but if the router can't complete the connection, it will automatically connect to the next available operator.

\* Most network operators' codes can be found online or you can initiate a scan for operators - if the operator you're looking for can be reached from your current area, the list of available network operators will contain the desired operator's code.

## Operators List

The **Operators List** section is used for creating a blacklist or whitelist for undesired or desired operators. Please note that when using either Whitelist mode or Blacklist mode, you will initially lose your mobile connection for several minutes. Also if you have your SIM card set to switch "On network denied", your SIM card may switch when using Blacklist mode

### Settings



Operators list

Settings

Enable

Mode Whitelist

Field	Value	Description
<b>Enable</b>	yes   no; default: <b>no</b>	Turns operator list on or off.
<b>Mode</b>	Blacklist   Whitelist; default: <b>Whitelist</b>	Defines how operators will be filtered. <ul style="list-style-type: none"> <li>• <b>Blacklist</b> - operators contained in the blacklist are considered forbidden and your router will not attempt to connect to them even if they are available.</li> <li>• <b>Whitelist</b> - operators contained in the whitelist will be the only operators that the router will be trying to connect to. Other operators that are not in the whitelist will be considered forbidden.</li> </ul>

## Operators List

The screenshot shows a web interface for managing an Operators List. At the top, there is a header 'Operators List'. Below it is a table with three columns: 'Name', 'Operator code', and 'Sort'. Under the 'Name' column, there is an empty text input field. Under the 'Operator code' column, there is an empty text input field. Under the 'Sort' column, there is a dropdown menu with up and down arrows, and a 'Delete' button to its right.

Field	Value	Description
<b>Name</b>	string; default: <b>none</b>	Operator's name. Used only for easier management purposes and not in the actual filtering process.
<b>Operator code</b>	integer; default: <b>none</b>	Operator's code used to identify a network operator.

**Important:** be mindful when using the Operators List function as it very easy to block yourself from the right operators and lose your data connection.

## Mobile Data Limit

The **Mobile Data Limit** page provides you with the possibility to set data usage limits for your SIM cards and data usage warnings via SMS message in order to protect yourself from unwanted data charges.

### Data Connection Limit Configuration

The **Data Connection Limit Configuration** section is used to configure custom mobile data limits for your SIM card(s). When the mobile data limit set for the SIM card(s) is reached, the router will no longer use the mobile connection to establish a data connection until the limit period is over or the limit is reset by the user.



**Mobile Data Limit Configuration**

SIM1 SIM2

**Data Connection Limit Configuration**

Enable data connection limit

Data limit\* (MB)

Period

Start day

Field	Value	Description
<b>Enable data connection limit</b>	yes   no; default: <b>no</b>	Turns mobile data limitations on or off.
<b>Data limit* (MB)</b>	integer; default: <b>none</b>	The amount of data that is allowed to be downloaded over the specified period of time. When the limit is reached, the router will no longer be able to establish a data connection until the period is over or the data limit is reset. <b>Note:</b> after the router has reached the data limit it will not switch to using the secondary SIM card. If you wish to configure a SIM switch system based on received data limit, instructions can be found in the SIM Switching rules section of this page.
<b>Period</b>	Month   Week   Day; default: <b>Month</b>	Data limit period after which the data counter is reset on the specified <i>Start day</i> .
<b>Start day   Start hour</b>	day [1..31]   day [Monday..Sunday]   hour [1..24]; default: <b>day 1</b>	Specifies when the period of counting data usage should begin. After the period is over, the limit is reset and the count begins over again.

## SMS Warning Configuration

The **SMS Warning Configuration** section provides you with the possibility to configure a rule that sends you an SMS message after the router's SIM card(s) uses a specified amount of mobile data.

**SMS Warning Configuration**

Enable SMS warning

Data limit\* (MB)

Period Month ▾

Start day 1 ▾

Phone number

Field	Value	Description
<b>Enable SMS warning</b>	yes   no; default: <b>no</b>	Toggles SMS warning On or OFF
<b>Data limit* (MB)</b>	integer; default: <b>none</b>	The received data limit before sending an SMS warning. After reaching using the the amount of data specified in this field, the router will send an SMS warning message to the specified phone number.
<b>Period</b>	Month   Week   Day; default: <b>Month</b>	Period to which the data limit applies to.
<b>Start day   Start hour</b>	day of the month [1..31]   day of the week [Monday..Sunday]   hour of the day [1..24]; default: <b>1</b>	Specifies when the period of counting data usage should begin. After the period is over, the limit is reset and the count begins over again.
<b>Phone number</b>	phone number; default: <b>none</b>	Recipient's phone numbers

## Clear Data Limit

The **Clear Data Limit** section contains only one button - 'Clear data limit'. When clicked, the button resets the data limit counter for the related SIM card. Thus, the count is started over again regardless of the specified period.

**Clear Data Limit**

Data used: N/A

Data limit: Not set

Clear data limit

\* Important: data limit database is not reset when the functionality is disabled and then re-enabled. Automatically the database is reset at a given Period (month, week, day). If you wish to reset it manually you can hit the "Clear" button.

**Important:** remember that the 'Clear data limit' button doesn't clear the actual data usage statistics for the SIM card, only the data counters as calculated by the router.

## SMS Limit

The **SMS Limit** page provides you with the possibility to set up a limit of SMS messages that the router's SIM card(s) can send in a period of one day, week or a month.

### SMS Limit Configuration

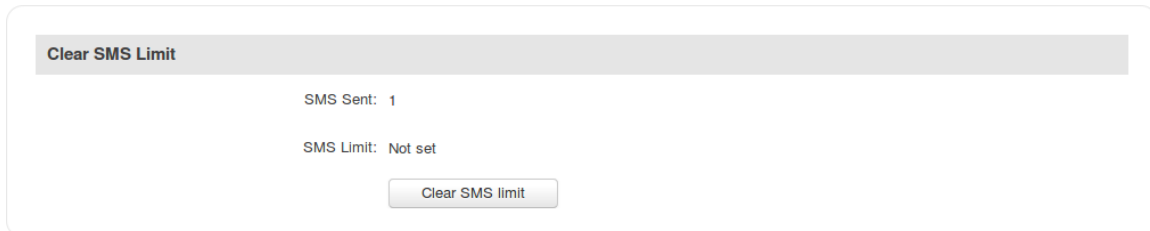
The **SMS Limit Configuration** section is used to configure custom SMS limits for your SIM card(s). In order to limit sent SMS messages, select the SIM card (SIM1 or SIM2), enable SMS limit and configure the limit conditions. For related information, refer to the figure and table below.

Field	Value	Description
<b>Enable SMS limit</b>	yes   no; default: <b>no</b>	Turns SMS limitations on or off.
<b>Period</b>	Month   Week   Day; default: <b>Month</b>	SMS limit period after which the sent SMS counter is reset on the specified <i>Start day</i> .
<b>Start day   Start hour</b>	day of the month [1..31]   day of the week [Monday..Sunday]   hour of the day [1..24]; default: <b>1</b>	Specifies when the period of counting SMS messages should begin. After the period is over, the limit is reset and the count begins over again.
<b>SMS limit*</b>	integer; default: <b>none</b>	Number of SMS messages that the SIM card is allowed to send over the specified period of time. When the limit is reached, the router will no longer be able to send SMS messages until the period is over or the SMS limit is reset. <b>Note:</b> after the router has reached the SMS limit it will not switch to using the secondary SIM card. If you wish to configure a SIM switch system based on sent SMS limit, instructions can be found in the <a href="#">SIM Switching rules</a> section of this page.

\* Your carrier's SMS usage accounting may differ.

## Clear SMS Limit

The **Clear SMS Limit** section displays the amount of sent SMS messages and provides the possibility to reset that counter. When the 'Clear SMS button' is clicked, it clears the SMS limit counter for the related SIM card. Thus, the count is started over again regardless of the specified period.



Clear SMS Limit

SMS Sent: 1

SMS Limit: Not set

Clear SMS limit

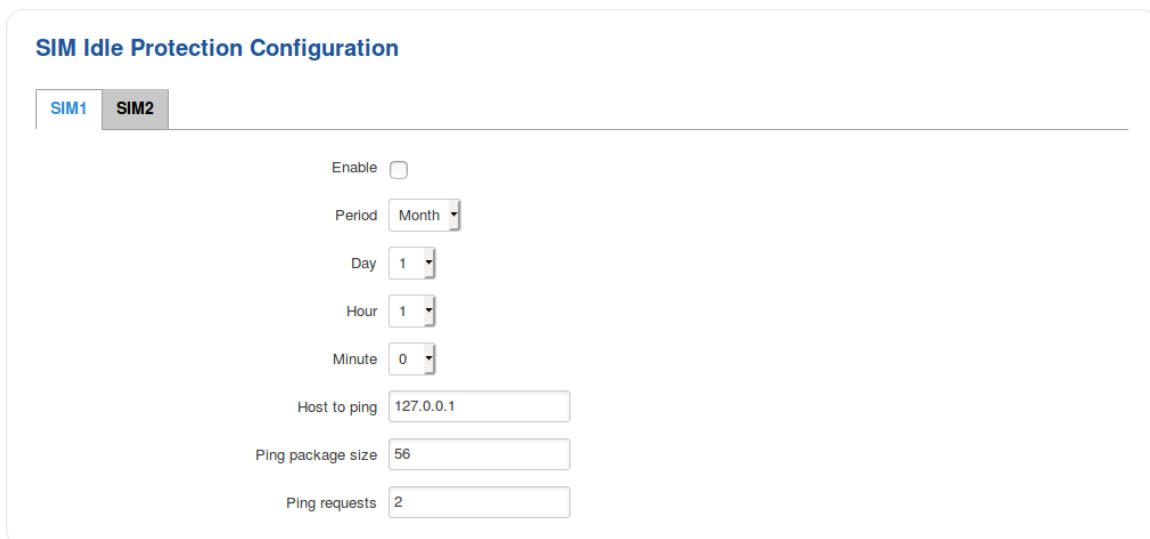
**Important:** remember that the 'Clear SMS limit' button doesn't clear the actual sent SMS statistics for the SIM card, only the SMS counters as calculated by the router.

## SIM Idle Protection

Some operators block user SIM cards after a period of inactivity. The **SIM Idle Protection** tab provides you with the possibility to configure the router to periodically switch to the secondary SIM card and establish a data connection with a mobile network operator in order to break the idleness and prevent the SIM card from being blocked.

### Settings

The **Settings** tab is used to configure the parameters used by the SIM Idle Protection function. Refer to the figure and table below for more information.



SIM Idle Protection Configuration

SIM1 SIM2

Enable

Period Month

Day 1

Hour 1

Minute 0

Host to ping 127.0.0.1

Ping package size 56

Ping requests 2

Field	Value	Description
-------	-------	-------------

<b>Enable</b>	yes   no; default: <b>no</b>	Turns SIM Idle Protection on or off.
<b>Period</b>	Month   Week; default: <b>Month</b>	How often SIM Idle Protection will be performed. Use the three following fields ('Day', 'Hour' and 'Minute') to set the exact time of the action.
<b>Host to ping</b>	ip; default: <b>127.0.0.1</b>	IP address of a host that will be pinged during the SIM Idle Protection action.
<b>Ping package size</b>	integer [1..1000]; default: <b>56</b>	ICMP packet size in bytes.
<b>Ping requests</b>	integer [1..30]; default: <b>2</b>	How many ping requests will be sent.

## Test

Once you have configured the SIM Idle Protection settings, you can use the **Test** section to test these settings to make sure everything works correctly. Once you click the 'Test' button, the SIM Idle Protection test will initiate. The test is designed to simulate SIM Idle Protection according to your current SIM Idle Protection settings.

**SIM Idle Protection Test**

The test takes about 2 minutes, so make sure the router isn't doing anything important before you start the test because during it you will lose connectivity. It is very important to **wait for the test to finish before committing any actions**. Committing actions on the router during test phase you may cause the router to crash.

## USB Modem

The **USB Modem** section is used to configure the connection settings of a USB modem attached to the router's USB connector. This section only becomes visible when a USB modem is connected to the router.

The configuration is a minimalistic version of the regular SIM card settings page:

**USB Modem Configuration**

APN

PIN number

Authentication method

Service mode

Field	Value	Description
<b>APN</b>	string; default: <b>none</b>	<p>An Access Point Name (APN) is a gateway between a GSM, GPRS, 3G or 4G mobile network and another computer network. Depending on the contract, some operators may require you to use an APN just to complete the registration on a network. In other cases, APN is used to get special parameters from the operator (e.g., a <a href="#">public IP address</a>) depending on the contract. The check mark on the right side of the APN field enables the <i>Auto APN</i> feature. Auto APN sets the APN value automatically based on your provider and country. An APN Network Identifier cannot start with any of the following strings:</p> <ul style="list-style-type: none"> <li>• rac;</li> <li>• lac;</li> <li>• sgsn;</li> <li>• rnc;</li> </ul> <p>it cannot end in:</p> <ul style="list-style-type: none"> <li>• .gprs;</li> </ul> <p>and it cannot contain the asterisk symbol (*).</p>
<b>PIN number</b>	string; default: <b>none</b>	A 4-digit long numeric password used to authenticate the modem to the SIM card.
<b>Authentication method</b>	CHAP   PAP   None; default: <b>None</b>	Authentication method that your GSM carrier uses to authenticate new connections on its network. If you select PAP or CHAP, you will also be required to enter a username and password.
<b>Service mode</b>	2G only   2G preferred   3G only   3G preferred   4G (LTE) only   4G (LTE) preferred   Automatic; default: <b>4G (LTE) preferred</b>	Your service mode preference. If your local mobile network supports 2G, 3G and 4G (LTE), you can specify to which type of network you wish to connect to. For example, if you choose 2G only, the router will connect to a 2G network, so long as it is available, otherwise it will connect to a network that provides better connectivity. If you select Automatic, then the router will connect to the network that provides the best connectivity.

To select the USB modem to act as a WAN connection, go to the **Network** → **WAN** page.

# WAN

## Summary

A wide area network (WAN) is a telecommunications network or computer network that extends over a large geographical distance.

## Operation Modes

The Operation Modes window lets you determine how the router will be connecting to the internet. You can choose between three types of WAN – Mobile, Wired and Wi-Fi. You can also setup backup WAN options in case your main connection goes down.

The screenshot shows the WAN configuration page. At the top, it says "WAN" and "Your WAN configuration determines how the router will be connecting to the internet." Below this is a section titled "Operation Mode" which contains a table with columns: Main WAN, WAN Failover, Interface Name, Protocol, IP Address, and Sort. There are three rows representing different WAN interfaces: Wired (WAN1), Mobile (WAN2), and WiFi (WAN3). Each row has a radio button for the Main WAN and a checkbox for the WAN Failover. The Mobile (WAN2) interface is selected as the Main WAN and has a checkmark in the WAN Failover column. Each row also has an "Edit" button.

Main WAN	WAN Failover	Interface Name	Protocol	IP Address	Sort
<input checked="" type="radio"/>	<input type="checkbox"/>	Wired (WAN1)	Static	192.168.50.10	<input type="button" value="Edit"/>
<input type="radio"/>	<input checked="" type="checkbox"/>	Mobile (WAN2)	None	188.69.69.69	<input type="button" value="Edit"/>
<input type="radio"/>	<input type="checkbox"/>	WiFi (WAN3)	DHCP	-	<input type="button" value="Edit"/>

You can choose one main WAN and one or two (or none) backup WAN options. To choose your main WAN just check the desired option (wired, mobile or Wi-Fi) in the **Main WAN** column (first from the left), to choose a backup WAN(s), check the desired option(s) in the Backup WAN column (second from the left). Above is an example of a configuration that uses wired as Main WAN and mobile as Backup WAN. The Operation Modes tab also displays each interfaces name, WAN IP address and Protocol in use. To configure a WAN interface more in depth, click the **Edit** button located to the right of the desired interface. Each interface configures separately, to avoid redundancy this chapter will only overview the configuration of the wired WAN interface, since mobile contains less information and Wi-Fi is basically the same.

## Common Configuration

The Common Configuration section is used to configure different protocols for WAN interfaces.

## Static

The Static protocol is used when the source of your internet doesn't have a DHCP server enabled. Therefore, in order to connect to the internet, you have to make configurations in accordance to that source.

### General

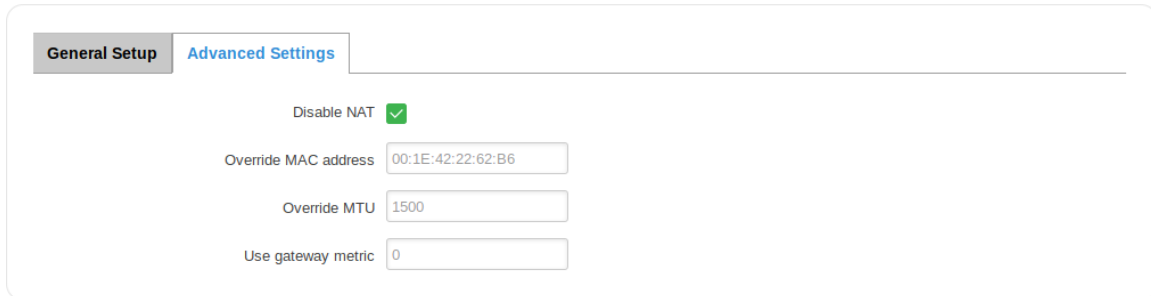
The screenshot shows a configuration window with two tabs: 'General Setup' (selected) and 'Advanced Settings'. Under 'General Setup', the 'Protocol' is set to 'Static'. Below it are input fields for 'IPv4 address' (192.168.50.212), 'IPv4 netmask' (255.255.255.0), 'IPv4 gateway' (192.168.50.254), and 'IPv4 broadcast' (192.168.50.255). At the bottom, there is a section for 'Use custom DNS servers' with two input fields containing '8.8.8.8' and '8.8.4.4', each with a delete icon (X) and an add icon (+).

Field Name	Value	Description
<b>Protocol</b>	Static   DHCP   PPPoE; Default: <b>DHCP</b>	The protocol used by the WAN interface
<b>IPv4 address</b>	ip; Default: " "	Your router's address on the WAN network
<b>IPv4 netmask</b>	ip; Default: <b>255.255.255.0</b>	Netmask defines how "large" a network is
<b>IPv4 gateway</b>	ip; Default: " "	The address where the router will send all the outgoing traffic
<b>IPv4 broadcast</b>	ip; Default: " "	IP broadcasts are used by BOOTP and DHCP clients to find and send requests to their respective servers
<b>Use custom DNS servers</b>	ip; Default: " "	When the router needs to resolve a hostname ("www.google.com", "www.cnn.com", etc.) to an IP address, it will forward all the DNS requests to the gateway. By entering custom DNS servers the router will take care of the host name resolution. You can enter multiple DNS servers to provide redundancy in case one of the servers fails



## Advanced

The Advanced Settings tab will change in accordance to which network protocol is selected. For the Static protocol you can turn NAT on or off, override the router's MAC address, MTU and define the gateway's metric.



General Setup **Advanced Settings**

Disable NAT

Override MAC address

Override MTU

Use gateway metric

Field Name	Value	Description
<b>Disable NAT</b>	yes   no; Default: <b>no</b>	Toggles Network Address Translation (NAT) on or off for the selected network interface
<b>Override MAC address</b>	mac; Default: <b>router's mac</b>	Override MAC address of the WAN interface. For example, your ISP (Internet Service Provider) gives you a static IP address and it might also bind it to your computer's MAC address (i.e., that IP will only work with your computer but not with your router). In this field you can enter your computer's MAC address and fool the gateway in to thinking that it is communicating with your computer
<b>Override MTU</b>	integer [0..1500]; Default: <b>1500</b>	Maximum Transmission Unit (MTU) – specifies the largest possible size of a data packet
<b>Use gateway metric</b>	integer; Default: <b>0</b>	The WAN configuration by default generates a routing table entry. In this field you can alter the metric of that entry. Higher metric means higher priority

## DHCP

The DHCP protocol should be used when the source of your internet has a DHCP server enabled. If that is the case, when you select the DHCP protocol you can use it as is, because most networks will not require any additional advanced configuration.

## General

### WAN

Your WAN configuration determines how the router will be connecting to the internet.

**Common Configuration**

**General Setup** | **Advanced Settings**

Protocol:

Hostname to send when requesting DHCP:

Field Name	Value	Description
<b>Protocol</b>	Static   DHCP   PPPoE; Default: <b>DHCP</b>	The protocol used by the WAN interface
<b>Hostname to send when requesting DHCP</b>	ip   hostname; Default: <b>router's hostname</b>	Host name to which the DHCP request will be sent to

## Advanced

For the DHCP protocol you can turn NAT on or off, specify custom DNS servers, define the gateway metric, override the router's MAC address, set MTU and more.

**Common Configuration**

**General Setup** | **Advanced Settings**

Disable NAT

Use broadcast flag

Use default gateway

Use DNS servers advertised by peer

Use custom DNS servers:

Use gateway metric:

Client ID to send when requesting DHCP:

Vendor class to send when requesting DHCP:

Override MAC address:

Override MTU:

Field Name	Value	Description
<b>Disable NAT</b>	yes   no; Default: <b>no</b>	Toggles Network Address Translation (NAT) on or off for the selected network interface
<b>Use broadcast flag</b>	yes   no; Default: <b>no</b>	Required for certain ISPs (Internet Service Providers), e.g. Charter with DOCSIS 3
<b>Use default gateway</b>	yes   no; Default: <b>yes</b>	Uses the default gateway obtained through DHCP. If left unchecked, no default route is configured
<b>Use DNS servers advertised by peer</b>	yes   no; Default: <b>yes</b>	Uses DNS servers obtained from DHCP. If left unchecked, the advertised DNS server addresses are ignored
<b>Use custom DNS servers</b>	ip; Default: " "	Lets you chose your own preferred DNS servers. This field only becomes visible if <b>Use DNS servers advertised by peer</b> field is unchecked
<b>Use gateway metric</b>	ip; Default: " "	The WAN configuration by default generates a routing table entry. In this field you can alter the metric of that entry. Higher metric means higher priority
<b>Client ID to send when requesting DHCP</b>	string; Default: " "	Client ID which will be sent when requesting a DHCP lease
<b>Vendor class to send when requesting DHCP</b>	string; Default: " "	Vendor class which will be sent when requesting a DHCP lease
<b>Override MAC address</b>	mac; Default: <b>router's mac</b>	Override MAC address of the WAN interface. For example, your ISP (Internet Service Provider) gives you a static IP address and it might also bind it to your computers MAC address (i.e., that IP will only work with your computer but not with your router). In this field you can enter your computer's MAC address and fool the gateway in to thinking that it is communicating with your computer

<b>Override MTU</b>	integer [0..1500]; Default: <b>1500</b>	Maximum Transmission Unit (MTU) – specifies the largest possible size of a data packet
---------------------	--	--

## PPPoE

The PPPoE protocol is mainly used if you have a DSL internet provider.

### General

The General configuration tab for the PPPoE protocol is mainly used to specify your PAP/CHAP login information, but you can also configure some additional, more specific settings.

The screenshot shows a configuration window with two tabs: 'General Setup' (selected) and 'Advanced Settings'. Under 'General Setup', there are five fields:
 

- Protocol: A dropdown menu set to 'PPPoE'.
- PAP/CHAP username: A text input field containing 'user'.
- PAP/CHAP password: A text input field containing 'pass' with a small eye icon to its right.
- Access Concentrator: A text input field containing 'auto'.
- Service Name: A text input field containing 'auto'.

Field Name	Value	Description
<b>Protocol</b>	Static   DHCP   PPPoE; Default: <b>DHCP</b>	The protocol used by the WAN interface
<b>PAP/CHAP username</b>	string; Default: " "	The username that you use to connect to your carrier's network
<b>PAP/CHAP password</b>	string; Default: " "	The password that you use to connect to your carrier's network
<b>Access concentrator</b>	string; Default: " "	The name of the access concentrator. Leave empty to auto detect
<b>Service name</b>	string; Default: " "	The name of the service. Leave empty to auto detect

### Advanced

For the PPPoE protocol you can turn NAT on or off, specify custom DNS servers, define the gateway metric, configure LCP echo settings and more.

General Setup
Advanced Settings

Disable NAT

Use default gateway

Use gateway metric

Use DNS servers advertised by peer

Use custom DNS servers

LCP echo failure threshold

LCP echo interval

Inactivity timeout

Field Name	Value	Description
<b>Disable NAT</b>	yes   no; Default: <b>no</b>	Toggles Network Address Translation (NAT) on or off for the selected network interface
<b>Use default gateway</b>	yes   no; Default: <b>yes</b>	Uses the default gateway obtained through DHCP. If left unchecked, no default route is configured
<b>Use gateway metric</b>	integer; Default: <b>0</b>	The WAN configuration by default generates a routing table entry. In this field you can alter the metric of that entry. Higher metric means higher priority
<b>Use DNS servers advertised by peer</b>	yes   no; Default: <b>yes</b>	Uses DNS servers obtained from DHCP. If left unchecked, the advertised DNS server addresses are ignored
<b>Use custom DNS servers</b>	ip; Default: " "	Lets you chose your own preferred DNS servers. This field only becomes visible if <b>Use DNS servers advertised by peer</b> field is unchecked
<b>LCP echo failure threshold</b>	integer; Default: <b>0</b>	Presumes peer to be dead after given amount of LCP echo failures. Leave it at 0 to ignore failures
<b>LCP echo interval</b>	integer; Default: <b>5</b>	Sends LCP echo requests at the given interval in seconds. This function is only effective in conjunction with failure threshold
<b>Inactivity timeout</b>	integer; Default: <b>0</b>	Close inactive connection after the given amount of seconds. Leave it at 0 to persist connection

## IP Aliases

IP Aliases are a way of defining or reaching a subnet that works in the same space as the regular network. This is useful if you need to reach the router that is located in the same network but in a different subnet. If you have a static IP configuration on your computer and don't want to change it every time you need to reach a router in a different subnet, you can configure an IP alias in order to do so.

## General setup

The screenshot shows a configuration interface with two tabs: 'General Setup' (active) and 'Advanced Settings'. Under 'General Setup', there are three input fields: 'IP Address' with the value '192.168.50.111', 'Netmask' with a dropdown menu showing '255.255.255.0', and 'Gateway' with the value '192.168.1.1'. Below these fields are two buttons: 'Delete' and 'Add'.

Field Name	Value	Description
<b>IP address</b>	ip; Default: " "	An alternate IP address used to reach the router by a device(s) that resides in the router's LAN but has a different subnet
<b>Netmask</b>	ip; Default: <b>255.255.255.0</b>	Netmask defines how "large" a network is
<b>Gateway</b>	ip; Default: " "	A gateway is a network node that connects two networks using different protocols together

As you can see, the configuration is very similar to the static protocol; in the example above an IP address with a 99th subnet is defined. In this case, if some device has an IP in the 99th subnet (e.g., 192.168.99.xxx) and the subnet's gateway metric is "higher" and the device is trying to reach the internet it will reroute it's traffic not to the gateway that is defined in common configurations but through the one that is specified in IP aliases.

## Advanced Settings

You may also define a broadcast address and a custom DNS server for your IP Aliases in the Advanced Settings tab.

General Setup
Advanced Settings

IP Broadcast

DNS Server

Delete
Add

Field Name	Value	Description
<b>IP Broadcast</b>	ip; Default: " "	IP broadcasts are used by BOOTP and DHCP clients to find and send requests to their respective servers
<b>DNS</b>	ip; Default: " "	A separate DNS server to be used by the IP Alias address

## Failover Configuration

Backup WAN is a function that allows you to back up your primary connection in case it goes down. There can be up to two backup connections selected at one time. In that case, when the primary connection fails, the router tries to use the backup with the higher priority and if this one is unavailable or fails too, then the router tries the backup with the lower priority.

**Failover Configuration**

Timing and other parameters will indicate how and when it will be determined that your conventional connection has gone down.

Health monitor interval

Health monitor ICMP host(s)

Health monitor ICMP timeout

Attempts before failover

Attempts before recovery

Execute command

Command

Field Name	Value	Description
<b>Health monitor interval</b>	Disable   5 sec.   10 sec.   20 sec.   30 sec.   60 sec.   120 sec.; Default: <b>10 sec.</b>	The interval at which health checks are performed
<b>Health monitor ICMP host(s)</b>	ip   hostname   8.8.4.4   Disable   DNS	Indicate where to send ping requests for a health check. As there is no definitive way to

	server(s)   WAN gateway   --custom--; Default: <b>8.8.4.4</b>	determine when the connection to internet is down for good, it is best to define a host whose availability is that of the internet as a whole (e.g., 8.8.8.8, 8.8.4.4)
<b>Health monitor ICMP timeout</b>	1 sec.   2 sec.   3 sec.   4 sec.   5 sec.   10 sec.; Default: <b>3 sec.</b>	The frequency at which ICMP requests are to be sent. It is advised to set a higher value if your connection has high latency or high jitter (latency spikes)
<b>Attempts before failover</b>	1   3   5   1   15   20; Default: <b>3</b>	The number of failed ping attempts after which the connection is to be declared as <b>"down"</b>
<b>Attempts before recovery</b>	1   3   5   1   15   20; Default: <b>3</b>	The number of successful ping attempts after which the connection is to be declared as <b>"up"</b>

**Additional notes:**

- Failover configuration field's default values may differ based on WAN type.
- The majority of the options consist of timing and other important parameters that help determine the health of your primary connection. Regular health checks are constantly performed in the form of ICMP packets (Pings) on your primary connection. When the connections state starts to change (READY->NOT READY and vice versa) a necessary amount of failed or passed health checks has to be reached before the state changes completely. This delay is instituted so as to mitigate "spikes" in connection availability, but it also extends the time before the backup link can be brought up or down.



# LAN

## Summary

A **local area network (LAN)** is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building. By contrast, a wide area network (WAN) not only covers a larger geographic distance, but also generally involves leased telecommunication circuits or Internet links. An even greater contrast is the Internet, which is a system of globally connected business and personal computers.

This chapter is an overview of the LAN section.

## Configuration

### General Setup

The General Setup tab provides you with the possibility to set the router's Private IP address, IP netmask and IP broadcast.

The screenshot shows the LAN Configuration interface. Under the 'Configuration' section, the 'General Setup' tab is active. It displays three input fields: 'IP address' with the value '192.168.1.1', 'IP netmask' with a dropdown menu showing '255.255.255.0', and 'IP broadcast' with the value '192.168.1.255'.

Field Name	Value	Description
<b>IP address</b>	ip; Default: <b>192.168.1.1</b>	IP address that the device uses on the LAN network
<b>IP netmask</b>	ip; Default: <b>255.255.255.0</b>	A netmask is used to define how "large" the LAN network is
<b>IP broadcast</b>	ip; Default: " "	IP broadcasts are used by BOOTP and DHCP clients to find and send requests to their respective servers

### Advanced Settings

LAN Configurations Advanced Settings tab contains some less frequently used, more complicated configurations, such as custom MTUs and network interface metric values.

**LAN**

Configuration

General Setup **Advanced Settings**

Accept router advertisements

Override MTU

Use gateway metric

Use WAN port as LAN  WAN Ethernet port selected as LAN

Field Name	Value	Description
<b>Accept router advertisements</b>	yes   no; Default: <b>no</b>	Allows accepting router advertisements
<b>Override MTU</b>	integer [0..1500]; Default: <b>1500</b>	MTU (Maximum Transmission Unit) specifies the largest possible size of a data packet
<b>Use gateway metric</b>	integer; Default: <b>0</b>	The LAN configuration generates an entry in the routing table. In this field you can alter the metric of that entry. Higher metric means higher priority
<b>Use WAN port as LAN</b>	yes   no; Default: <b>no</b>	If this is enabled, the router's WAN port will act as if it were a LAN port. <b>Works only if WAN is not set to wired</b>

## DHCP Server

A **DHCP** server is a service that can automatically configure the TCP/IP settings of any device that requests such a service (i.e., connects to the device with the operational DHCP server). If you connect a device that has been configured to obtain an IP address automatically, the DHCP server will lease out an IP address from the available IP pool and the device will be able to communicate within the private network.

### General

The **General Setup** tab is used to set DHCP server settings. The figure below is an example of the General Setup tab and the table below provides information on the fields contained in that tab:

DHCP Server

General Setup
Advanced Settings

DHCP Enable

Start 100

Limit 150

Lease time 12 Hours

Start IP address: 192.168.1.100

End IP address: 192.168.1.249

Field Name	Value	Description
<b>DHCP</b>	Enable   Disable   DHCP Relay; Default: <b>Enable</b>	Enables or disables DHCP Server. If DHCP Relay is selected, you will be prompted to enter an IP address of another DHCP server in your LAN. In this case, whenever a new device connects to the router, the router will redirect any DHCP requests to the specified DHCP Server
<b>Start</b>	integer [1..253]; Default: <b>100</b>	The starting IP address value. e.g., if your router's LAN IP is 192.168.2.1 and your subnet mask is 255.255.255.0 that means that in your network a valid IP address has to be in the range of [192.168.2.0..192.168.2.254] (192.168.2.255 is a special unavailable address). If the Start value is set to 100 then the DHCP server will only lease out addresses starting from 192.168.2.100
<b>Limit</b>	integer [1..4294967296]; Default: <b>150</b>	How many addresses the DHCP server can lease out. Continuing from the above example: if the start address is 192.168.2.100 and the server can lease out 150 (default limit value), available addresses will be from 192.168.2.100 to 192.168.2.249 (100 + 150 - 1 = 249; this is because the first address is inclusive)
<b>Lease time</b>	time in 'h' (hours) or 'm' (minutes); Default: <b>12h</b>	The duration of an IP lease. Leased out addresses will expire after the amount of time specified in this field and the device that was using the lease will have to request a new DHCP lease. However, if the device stays connected, its lease will be renewed after half of the specified amount of time

passes, e.g., if the lease time is 12 hours, then every 6 hours the device will send a request to the DHCP server asking to renew its lease  
 Lease time can be set in **hours (h)** or **minutes (m)**.  
 The minimal amount of time that can be specified is **2min (2m)**

## Advanced Settings

You may also apply more complicated, less common configurations to your router's DHCP Server in the **Advanced Settings** tab. The figure below is an example of the Advanced Settings tab and the table below provides information on the fields contained in that tab:

Field Name	Value	Description
<b>Dynamic DHCP</b>	yes   no; Default: <b>yes</b>	Enables Dynamic allocation of client addresses. If this is disabled, only clients that have static IP leases will be served
<b>Enable DNS rebind protection</b>	yes   no; Default: <b>yes</b>	Enables DNS rebind attack protection by discarding upstream RFC1918 responses (leave default unless necessary otherwise)
<b>Force</b>	yes   no; Default: <b>no</b>	The DHCP force function ensures that the router will always start the DHCP server, even if there is another DHCP server already running in the router's network. By default the router's DHCP server will not start when it is connected to a network segment that already has a working DHCP server
<b>IP netmask</b>	ip; Default: <b>255.255.255.0</b>	Overrides your LAN netmask, thus making the DHCP server think that it's serving a larger or smaller network than it actually is

**DHCP Options**      DHCP options; Default: " "      Additional options to be added to the DHCP server. For example with '26,1470' or 'option:mtu, 1470' you can assign an MTU value per DHCP.

## Static Leases

Static IP leases are used to reserve specific IP addresses for specific devices by binding them to their MAC address. This is useful when you have a stationary device connected to your network that you need to reach frequently, e.g., printer, IP phone, etc.

The screenshot shows a web interface titled "Static Leases". It features a table with three columns: "Hostname", "MAC address", and "IP address". Below the table, there are three input fields corresponding to these columns, a "Delete" button, and an "Add" button.

Field Name	Value	Description
<b>Hostname</b>	string; Default: " "	A custom name that will be linked with the device
<b>MAC address</b>	mac; Default: " "	Device's MAC address
<b>IP address</b>	ip; Default: " "	The desirable IP address that will be reserved for the specified device

## IP Aliases

IP Aliases are a way of defining or reaching a subnet that works in the same space as the regular network. This is useful if you need to reach the router that is located in the same network but in a different subnet. If you have a static IP configuration on your computer and don't want to change it every time you need to reach a router in a different subnet, you can configure an IP alias in order to do so.

## General setup

### IP Aliases

IP aliasing can be used to provide multiple network addresses on a single interface.

**General Setup** **Advanced Settings**

IP Address

Netmask

Delete

Add

Field Name	Value	Description
<b>IP address</b>	ip; Default: " "	An alternate IP address used to reach the router by a device(s) that resides in the router's LAN but has a different subnet
<b>Netmask</b>	ip; Default: <b>255.255.255.0</b>	Netmask defines how "large" a network is

As you can see, the configuration is very similar to the static protocol; in the example above an IP address with a 99th subnet is defined. In this case, if some device has an IP in the 99th subnet (e.g., 192.168.99.xxx) and the subnet's gateway metric is "higher" and the device is trying to reach the internet it will reroute it's traffic not to the gateway that is defined in common configurations but through the one that is specified in IP aliases.

## Advanced Settings

You may also define a broadcast address, a custom DNS server and Gateway for your IP Aliases in the Advanced Settings tab.

### IP Aliases

IP aliasing can be used to provide multiple network addresses on a single interface.

**General Setup** **Advanced Settings**

IP Broadcast

DNS Server

Gateway

Delete

Add

Field Name	Value	Description
------------	-------	-------------

<b>IP Broadcast</b>	ip; Default: " "	IP broadcasts are used by BOOTP and DHCP clients to find and send requests to their respective servers
<b>DNS</b>	ip; Default: " "	A separate DNS server to be used by the IP Alias address
<b>Gateway</b>	ip; Default: " "	A gateway is a network node that connects two networks using different protocols together

## Relayd

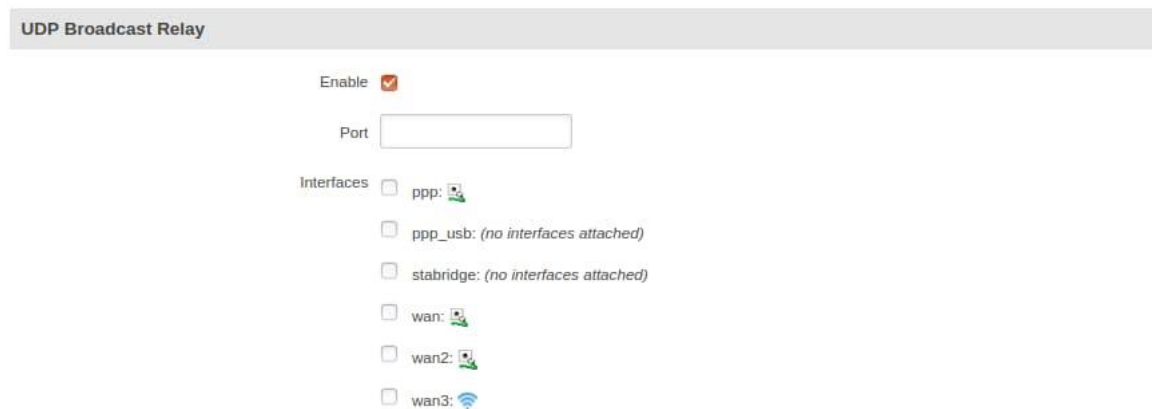
**Relayd** is a daemon to relay and dynamically redirect incoming connections to a target host. Its main purpose in UCR routers is extending the wireless network. For example, when UCR is in STA (Wireless Station) mode, it can be used to bridge WAN and LAN interfaces to create a larger Wireless network.



Field Name	Value	Description
<b>Enable</b>	yes   no; Default: <b>no</b>	Toggles Relayd ON or OFF

## UDP Broadcast Relay

**UDP Broadcast Relay** listens for packets on a specified UDP broadcast port. When a packet is received, it sends that packet to all specified interfaces but the one it came from as though it originated from the original sender. The primary purpose of this is to allow games on machines on separated local networks (Ethernet, WLAN) that use udp broadcasts to find each other to do so.



Field Name	Value	Description
<b>Enable</b>	yes   no; Default: <b>no</b>	Toggles UDP Broadcast Relay ON or OFF
<b>Port</b>	integer [0..65535]; Default: " "	Specifies a port which the UDP broadcast relay will listen on for incoming packets to relay

## Interfaces

ppp | ppp\_usb |  
stabridge | wan |  
wan2 | wan3 ;  
Default: " "

UDP broadcast relay destination interfaces.  
Note: Open port 137 in firewall so LAN could be  
reachable from WAN



# Wireless

## Summary

The **Wireless** section of the Network tab can be used to manage and configure WiFi Access Points (AP) and WiFi Stations (STA).

## Wireless technology

UCR routers support IEEE 802.11b/g/n and 802.11e\_WMM wireless technologies.

## Wireless Configuration

The **Wireless configuration** window provides you with the possibility to configure your wireless access points and wireless stations. The Wireless Station Mode will become active only when WiFi is configured as an active WAN interface (either main or backup).

### Wireless Configuration

The screenshot shows the 'Wireless Configuration' window. It has two main sections. The first section is 'Wireless Access Points', which has an 'Add' button. Below it, there is one entry with SSID: HAL9000 and Encryption: WPA-PSK/WPA2-PSK mixed mode. To the right of this entry are three buttons: 'Disable', 'Edit', and 'Remove'. The second section is 'Wireless Station Mode', which also has an 'Add' button. Below it, there is one entry with SSID: GUEST\_TELTONIKA and Encryption: WPA2-PSK. To the right of this entry are three buttons: 'Disable', 'Edit', and 'Remove'.

Above is the overview of the Wireless Configuration window. It displays active access points and stations. Here you can disable or enable your WiFi interfaces, remove unwanted access points or stations or enter a configuration window for each WiFi interface, where you can configure it more thoroughly.

## Wireless Access Point

The Wireless Access Point configuration window is used to make changes to different access points. It is divided into two main sections – device and interface. One is dedicated to configuring hardware parameters, the other – software. To access this window, simply click the **edit** button next to the WiFi interface that you wish to configure:

This is a close-up screenshot of the 'Wireless Access Points' section. It shows the entry for SSID: HAL9000 and Encryption: WPA-PSK/WPA2-PSK mixed mode. The 'Edit' button is highlighted with a hand cursor, indicating it is the button to click to access the configuration window.

## Device Configuration

---

The **Device Configuration** section is used for configuring WiFi hardware parameters.

### *General Setup*

---

The **General Setup** tab is used to **Enable** or **Disable** an Access Point and to select the wireless channel used by the Access Point.

Choose a WiFi channel according to the busyness of other channels. While UCR devices do not provide a function that lets you monitor the usage of nearby WiFi channels, you can download a free WiFi analyzer app on your phone, laptop or other WiFi device. In most countries there are 13 WiFi channels on the 2.4 GHz band (14 in Japan) to choose from. UCR routers' WiFi works on the 2.4 GHz band. A wireless 2.4 GHz WiFi channel requires a signaling band roughly 22 MHz wide, radio frequencies of neighboring channels numbers significantly overlap each other. Many home networks utilize routers that by default run on channel 6 on the 2.4 GHz band. Neighboring WiFi home networks that run over the same channel generate radio interference that can cause significant network performance slowdowns for users. Reconfiguring a network to run on a different wireless channel helps minimize these slowdowns. Therefore, pick a channel with no other active Access Points and preferably one that has no active Access Point on two adjacent channels on each side as well. If you don't feel like doing this, set the **Channel** field to **Auto** and the router will pick the least busy channel in your location automatically.

### **Wireless Access Point**

Here you can configure your wireless settings like radio frequency, mode, encryption etc...

#### Device Configuration

General Setup

Advanced Settings

Enable wireless

Channel 4 (2.427 GHz) ▼

### *Advanced Setup*

---

The **Advanced Setup** tab is used to configure how the wireless Access Point will work from a hardware perspective.

## Device Configuration

General Setup

Advanced Settings

Mode

HT mode

Country code

Transmit power

Fragmentation threshold

RTS/CTS threshold

Field Name	Value	Description
<b>Mode</b>	Auto   802.11b   802.11g   802.11g+n; Default: <b>802.11g+n</b>	Wireless protocol used. Different modes provide different wireless standard support which directly impacts the radio's throughput performance
<b>HT mode</b>	20 MHz   40 MHz 2nd channel above; Default: <b>20 MHz</b>	HT (High Throughput) mode allows you to specify channel width. 40 MHz bandwidth provides better performance but it overlaps 4 adjacent channels on each side, therefore, it might overlap with many other Access Points working in those channels. If that is the case, the router will switch back to 20 MHz mode automatically to reduce interference. 40 MHz is only available if the selected channel is not <b>Auto</b>
<b>Country code</b>	country code; Default: <b>0 - World</b>	SO/IEC 3166 alpha2 country codes as defined in ISO 3166-1 standard
<b>Transmit power</b>	100 %   80 %   60 %   40 %   20 %; Default: <b>100 %</b>	WiFi signal power. Use lower power to reduce the router's CPU usage
<b>Fragmentation threshold</b>	integer [256..2346]; Default: " "	The smallest packet size that can be fragmented and transmitted by multiple frames. In areas where interference is a problem, setting a lower fragment threshold might help reduce the probability of unsuccessful packet transfers, thus increasing speed

**RTS/CTS threshold** integer [0..2347]; Default: RTS/CTS (Request to Send/Clear to Send) " " are mechanisms, used to reduce frame collisions introduced by the hidden node problem. It can help resolve problems arising when several access points are in the same area, contending

## Interface Configuration

The **Interface Configuration** section is used to configure wireless Access Points from the software perspective.

### General Setup

The **General Setup** tab contains only two options. **SSID** is the name of your WiFi interface. When other WiFi capable computers or devices scan the area for WiFi networks they will see your network with this name. **Hide SSID** is used to make your Access Point invisible to other devices. To use a hidden WiFi Access Point, first un-hide it, connect your device to it, then hide it again.

Interface Configuration

General Setup | Wireless Security | MAC Filter | Advanced Settings

SSID: HAL9000

Hide SSID:

### WPA

Interface Configuration

General Setup | Wireless Security | MAC Filter | Advanced Settings

Encryption: WPA-PSK/WPA2-PSK mixed mode

Cipher: Auto

Key: [masked]

Field Name	Value	Description
<b>Encryption*</b>	No encryption   WPA-PSK   WPA2-PSK   WPA-PSK/WPA2-PSK mixed mode; Default: <b>No encryption</b>	The type of WiFi encryption used.

<b>Cipher</b>	Auto   Force CCMP (AES)   Force TKIP   Force TKIP and CCMP (AES); Default: <b>Auto</b>	An algorithm for performing encryption or decryption
<b>Key</b>	string; Default: " "	A custom passphrase used for authentication (at least 8 characters long)

WPA-Enterprise (WPA-EAP, WPA2-EAP)

The **Enterprise variants** of WPA and WPA2 use a RADIUS server for authentication purposes instead of a password(s).

Interface Configuration

General Setup

Wireless Security

MAC Filter

Advanced Settings

Encryption

Cipher

Radius Server IP

Radius Server Port

Radius Server Secret

Field Name	Value	Description
<b>Encryption*</b>	No encryption   WPA-PSK   WPA2-PSK   WPA-PSK/WPA2-PSK mixed mode; Default: <b>No encryption</b>	The type of WiFi encryption used.
<b>Cipher</b>	Auto   Force CCMP (AES)   Force TKIP   Force TKIP and CCMP (AES); Default: <b>Auto</b>	An algorithm for performing encryption or decryption
<b>Radius Server IP</b>	host   ip; Default: " "	RADIUS server's IP address or host name
<b>Radius Server Port</b>	integer [0..65535]; Default: " "	The port number used for connection to the RADIUS server
<b>Radius Server Secret</b>	string; Default: " "	A case-sensitive shared secret used for authentication on both RADIUS devices

## MAC Filter

The **MAC Filter** tab is used for setting up rules that allow or exclude devices with specified MAC addresses from connecting to your WiFi network.

Interface Configuration

General Setup | Wireless Security | **MAC Filter** | Advanced Settings

MAC address filter: Allow listed only

MAC list: C0:11:73:94:E8:E5

18:66:da:28:6a:34

Field Name	Value	Description
<b>MAC address filter</b>	Disable   Allow listed only   Allow all except listed; Default: <b>Disable</b>	<b>Allow listed only</b> – only allows devices with MAC addresses specified in the MAC list to connect to your WiFi network <b>Allow all except listed</b> - blocks devices with MAC addresses specified in the MAC list from connecting to your WiFi network
<b>MAC</b>	mac; Default: " "	List of MAC addresses to be included or excluded from connecting to your WiFi network
<b>Key</b>	string; Default: " "	A custom passphrase used for authentication (at least 8 characters long)

## Advanced Settings

Interface Configuration

General Setup | Wireless Security | MAC Filter | **Advanced Settings**

Separate clients

Increase TTL packet size

Field Name	Value	Description
<b>Separate clients</b>	yes   no; Default: <b>no</b>	Prevents WiFi clients from communicating with each other on the same subnet
<b>Increase TTL packet size</b>	yes   no; Default: <b>no</b>	Increase TTL packet size for incoming packets

## Wireless Station

UCR can also work as a WiFi client. Configuring client mode is nearly identical to AP, except for the fact that most of the options are dictated by the wireless access point that






the router is connecting to. Changing them can result in an interrupted connection to that AP.

In addition to standard options you can also click the **Scan** button to rescan the surrounding area and attempt to connect to a new wireless access point.

## WAN

Your WAN configuration determines how the router will be connecting to the internet.

**Operation Mode**

Main WAN	Backup WAN	Interface Name	Protocol	IP Address	Sort	
 <input type="radio"/>	<input type="checkbox"/>	WiFi (WAN)	DHCP	-		<input type="button" value="Edit"/> <input type="button" value="Scan"/>
 <input type="radio"/>	<input checked="" type="checkbox"/>	Wired (WAN2)	Static	192.168.90.66		<input type="button" value="Edit"/>
 <input type="radio"/>	<input type="checkbox"/>	Mobile (WAN3)	None	188.69.245.225		<input type="button" value="Edit"/>

After the scan finishes, you will see a list of these Access points. Choose one according to your liking and press the **Join Network** button next to it.



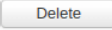
# Load Balancing


## Summary

Load balancing lets users create policies and rules that divide traffic between different interfaces.

## Policies

The **Policies** section contains Load Balancing policies. One default policy named **Balanced** is already in place. You can edit this default policy or create a new custom policy.

Policies			
Policy	Members assigned	Ratio	Sort
balanced	Wired Mobile	3 2	  



To configure a Policy, click the **Edit** button located next to it, after which you will be redirected to the Configuration window.

### WAN Policy Configuration - balanced

Interface	Ratio	Sort
Mobile	<input type="text" value="3"/>	 
Wired	<input type="text" value="2"/>	 



As you can see from the image above, the configuration is very simple. You can assign ratio values to WAN interfaces. The ratio values represent a percentage of load that will go through an interface. For example, in the default configuration 3 parts of traffic will go through the Mobile interface and 2 parts will go through the Wired interface, which means roughly 60% (3/5) of data will be transferred through Mobile, 40% (2/5) through Wired. If the ratios would be different, say Mobile: 5, Wired: 10, then 33% (5/15) of data would be transferred through Mobile, and 66% (10/15) would go through Wired.



# Rules

The **Rules** section contains Load Balancing rules. One default rule named **default\_rule** is already in place. You can edit this default rule or create a new custom rule.

Rules							
Rule	Source address	Source port	Destination address	Destination port	Protocol	Policy assigned	Sort
default_rule	—	—	0.0.0.0/0	—	all	balanced	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="text"/> <input type="button" value="Add"/>							

To configure a rule, click the **Edit** button located next to it, after which you will be redirected to the Configuration window.

## Load Balancing Rule Configuration - default\_rule

Source address

Source port

Destination address

Destination port

Protocol

Policy assigned

Field Name	Value	Description
<b>Source address</b>	ip; Default: <b>none</b>	Source IP address. Can be specified in CIDR notation (eg "192.168.1.0/24" without quotes).
<b>Source port</b>	number; Default: <b>none</b>	Source port number. May be entered as a single or multiple ports (eg "21" or "80,443" without quotes).
<b>Destination address</b>	ip; Default: <b>none</b>	Destination IP address. Can be specified in CIDR notation (eg "192.168.1.0/24" without quotes).
<b>Destination port</b>	number; Default: <b>none</b>	Destination port number. May be entered as a single or multiple ports (eg "21" or "80,443" without quotes).
<b>Protocol</b>	all   ip   #hopopt   icmp   igmp   ggp   ipencap   st   tcp   egp   igp   pup   udp   hmp   xns   rdp   iso   xtp   ddp   idpr   ipv6   ipv6   ipv6   idrp   rsvp   gre   esp   ah   skip   ipv6   ipv6   ipv6	Which protocol to use.

**Policy assigned**      rspf | vmtp | eigrp |  
ospf | ax | ipip | etherip  
| encap | pim | ipcomp  
| vrrp | l2tp | isis | sctp  
| fc; Default: **all**  
policies;                      Policy to use for this rule.  
Default: **balanced**

# Services Section

## MQTT

### Summary

---

**MQTT (MQ Telemetry Transport or Message Queue Telemetry Transport)** is an ISO standard (ISO/IEC PRF 20922) publish-subscribe-based "lightweight" messaging protocol for use on top of the TCP/IP protocol. It is designed to send short messages from one client (**publisher**) to another (**subscriber**) through **brokers**, which are responsible for message delivery to the end point. UCR routers support this functionality via an open source Mosquitto broker. The messages are sent this way: a client (**subscriber**) subscribes to a topic(s); a publisher posts a message to that specific topic(s). The **broker** then checks who is subscribed to that particular topic(s) and transmits data from the publisher to the subscriber.

### MQTT Broker

---

The **Broker** will "listen" for connections on the specified Local port. In order to accept connections from WAN, you also need to check Enable Remote Access.

**MQTT Broker**

Enable

Local Port

Enable Remote Access

Field Name	Value	Description
<b>Enable</b>	yes   no; Default: <b>no</b>	Toggles MQTT Broker ON or OFF
<b>Local Port</b>	integer [0..65535]; Default: "1883"	Specifies the local port that the MQTT broker will listen to
<b>Enable Remote Access</b>	yes   no; Default: <b>no</b>	If enabled, MQTT Broker will be reachable by remote user (from WAN)

### Security

---

The MQTT **Security** tab is used to establish MQTT connection security via TLS/SSL.

Security
Bridge
Miscellaneous

Use TLS/SSL

CA File  No file selected.

CERT File  No file selected.

Key File  No file selected.

TLS version

Field Name	Value	Description
<b>Use TLS/SSL</b>	yes   no; Default: <b>no</b>	Toggles the use of TLS/SSL certificates ON or OFF
<b>CA File</b>	.ca file; Default: " "	<b>Certificate authority</b> is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate
<b>CERT File</b>	.cert file; Default: " "	Certificate file is a type of digital certificate that is used by client systems to make authenticated requests to a remote server. Client certificates play a key role in many mutual authentication designs, providing strong assurances of a requester's identity
<b>Key File</b>	.key file; Default: " "	Private key for client to establish connection
<b>TLS version</b>	tlsv1.1   tlsv1.2   Support all; Default: <b>Support all</b>	Authenticates a client to a server and establishes precisely who they are

## Bridge

The MQTT Broker also supports a functionality called **Bridge**. An MQTT Bridge is used for the communication between two MQTT Brokers. The window of Bridge parameters is presented below. Some of these are mandatory as they are needed to create a connection: Connection Name, Remote Address and Remote Port. For more information on **MQTT Bridge** parameters you can read the official mosquitto.conf manual page.

Security
Bridge
Miscellaneous

Enable

Connection Name

Remote Address

Remote Port

Use Remote TLS/SSL

Use Remote Bridge Login

Try Private

Clean Session

Field Name	Value	Description
<b>Use TLS/SSL</b>	yes   no; Default: <b>no</b>	Toggles MQTT Bridge ON or OFF
<b>Connection Name</b>	string; Default: " "	Name of the Bridge connection. Although this is used for easier management purposes, this field is mandatory
<b>Remote Address</b>	ip; Default: " "	Remote Broker's address
<b>Remote Port</b>	integer [0..65535]; Default: <b>1883</b>	Specifies which port the remote broker uses to listen for connections
<b>Use Remote TLS/SSL</b>	yes   no; Default: <b>no</b>	Enables the use of TSL/SSL certificates of the remote broker. If this is checked, you will be prompted to upload TLS/SSL certificates. More information can be found in the <a href="#">Security</a> section of this chapter
<b>Use Remote Bridge Login</b>	yes   no; Default: <b>no</b>	Enables the use of Remote login data. If this is checked, you will be prompted to enter a remote client ID, username and password
<b>Topic</b>	string; Default: " "	Specifies the names of the Topics that your Broker will subscribe to
<b>Try Private</b>	yes   no; Default: <b>no</b>	Check if the remote Broker is another instance of a daemon
<b>Clean Session</b>	yes   no; Default: <b>no</b>	Check to discard session state after connecting or disconnecting

## Miscellaneous

---

The last section of MQTT Broker parameters is called **Miscellaneous**. It contains parameters that are related to neither Security nor Bridge.

Security Bridge **Miscellaneous**

---

ACL File  No file chosen

Password File  No file chosen

Persistence

Allow Anonymous

Field Name	Value	Description
<b>ACL File</b>	.ACL file; Default: " "	The contents of this file are used to control client access to topics of the broker
<b>Password File</b>	password file; Default: " "	The Password file stores user names and corresponding passwords, used for authentication
<b>Persistence</b>	yes   no; Default: <b>no</b>	If enabled, connection, subscription and message data will be written to the disk. Otherwise, the data is stored in the router's memory only
<b>Allow Anonymous</b>	yes   no; Default: <b>yes</b>	If enabled, the Broker allows anonymous access

# MQTT Publisher

---

An **MQTT Publisher** is a client that sends messages to the Broker, who then forwards these messages to the Subscriber.


## MQTT Publisher

Enable

Hostname

Port

Username

Password  

Field Name	Value	Description
<b>Enable</b>	yes   no; Default: <b>no</b>	Toggles the MQTT Publisher ON or OFF
<b>Hostname</b>	host   ip; Default: " "	Broker's IP address or hostname
<b>Port</b>	integer [0..65535]; Default: " "	Specifies the port used for connecting to the Broker
<b>Username</b>	string; Default: " "	User name used for authentication when connecting to the Broker
<b>Password</b>	string; Default: " "	Password used for authentication when connecting to the Broker

# NTP

## Summary

**Network Time Protocol (NTP)** is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

## General

The **Time Synchronization** section is used to configure general router time settings, like selecting the local time zone, setting a time update interval, synchronizing the time, etc.

The figure below is an example of the Time Synchronization section and the table below provides information about the fields contained in that section:

**Time Synchronization**

General

Current system time 2019-06-13 07:15:36 Sync with GPS Sync with browser

Time zone UTC

Enable NTP

Force servers

Update interval (in seconds) 3660

Save time to flash

Count of time synchronizations

GPS synchronization

GPS time update interval Every 24 hours

**Clock Adjustment**

Offset frequency 0

Field	Value	Description
<b>Current system time</b>	time; default: <b>none</b>	Current local time of the router.
<b>Time zone</b>	time zone; default: <b>UTC</b>	The router will sync time in accordance with the selected time zone.
<b>Enable NTP</b>	yes   no; default: <b>yes</b>	Turns NTP on or off.
<b>Force servers</b>	yes   no; default: <b>no</b>	Forces unreliable NTP servers.



<b>Update interval (in seconds)</b>	integer; default: <b>3660</b>	Defines how often the router will update the time.
<b>Save time to flash</b>	yes   no; default: <b>no</b>	Saves last synchronized time to flash memory.
<b>Count of time synchronizations</b>	integer; default: <b>none</b>	The amount of times that router will perform time synchronizations. Leave empty in order to set to infinite.
<b>GPS synchronization</b>	yes   no; default: <b>no</b>	Enables periodic time synchronization for the system using the GPS module (does not require an Internet connection).
<b>GPS time update interval</b>	5, 30 minutes   1, 6, 12, 24 hours   1 week   1 month; default: <b>Every 24 hours</b>	Defines how often the router will update the time using the GPS module.
<b>Offset frequency</b>	integer; default: <b>0</b>	Adjusts the minor drift of the clock so that it will run more accurately.

## NTP Server

---

The router can also act as an **NTP Server**, providing clock synchronization to other devices in the network. From this section you can turn this feature on or off:

**NTP Server**

General

Enable

## Time Servers

---

The **Time Servers** section displays the NTP servers that the router uses. You are provided with 4 default time servers (as seen in the example below), but you can also add custom time servers by clicking the "Add" button or you can edit the given time servers.

## Time Synchronisation

Time Servers	
Hostname	
0.europe.pool.ntp.org	Delete
1.europe.pool.ntp.org	Delete
2.europe.pool.ntp.org	Delete
3.europe.pool.ntp.org	Delete

# RS232/RS485

## Summary

RS232 and RS485 functions are designed to utilize available serial interfaces of the router. Serial interfaces provide a possibility for legacy devices to gain access to IP networks.

## RS232

### RS232 Configuration

RS232 Serial Configuration	
Enabled	<input type="checkbox"/>
Baud rate	115200
Data bits	8
Parity	None
Stop bits	1
Flow control	None
Serial type	Console
Echo	<input type="checkbox"/>

Field Name	Value	Description
<b>Enabled</b>	yes   no; Default: <b>no</b>	When checked, enables the RS232 service
<b>Baud rate</b>	300   1200   2400   4800   9600   19200   38400	Sets the data rate for serial data transmission (in bits per second)

	57600   115200; Default: <b>115200</b>	
<b>Data bits</b>	5   6   7   8; Default: <b>8</b>	The number of data bits for each character
<b>Parity</b>	None   Odd   Even; Default: <b>None</b>	<p>In serial transmission, parity is a method of detecting errors. An extra data bit is sent with each data character, arranged so that the number of 1 bits in each character, including the parity bit, is always odd or always even. If a byte is received with the wrong number of 1s, then it must have been corrupted. However, an even number of errors can pass the parity check.</p> <p><b>None (N)</b> - no parity method is used  <b>Odd (O)</b> - the parity bit is set so that the number of "logical ones (1s)" has to be odd  <b>Even (E)</b> - the parity bit is set so that the number of "logical ones (1s)" has to be even</p>
<b>Stop bits</b>	1   2; Default: <b>1</b>	Stop bits sent at the end of every character allow the receiving signal hardware to detect the end of a character and to resynchronise with the character stream. Electronic devices usually use one stop bit. Two stop bits are required if slow electromechanical devices are used
<b>Flow control</b>	None   RTS/CTS   Xon/Xoff; Default: <b>None</b>	<p>In many circumstances a transmitter might be able to send data faster than the receiver is able to process it. To cope with this, serial lines often incorporate a "handshaking" method, usually distinguished between hardware and software handshaking.</p> <p><b>RTS/CTS</b> - hardware handshaking. RTS and CTS are turned OFF and ON from alternate ends to control data flow, for instance when a buffer is almost full</p> <p><b>Xon/Xoff</b> - software handshaking. The Xon and Xoff characters are sent by the receiver to the sender to control when the sender will send data, i.e., these characters go in the opposite direction to the data being sent. The circuit starts in the "sending allowed" state. When the receiver's buffers approach</p>

capacity, the receiver sends the Xoff character to tell the sender to stop sending data. Later, after the receiver has emptied its buffers, it sends an Xon character to tell the sender to resume transmission

**Serial type** Console | Over IP | Modem | Modbus gateway | NTRIP client; Default: **Console**

Specifies the serial connection type.

**Echo** yes | no; Default: **no**

Toggles RS232 echo ON or OFF. RS232 echo is a loopback test usually used to check whether the RS232 cable is working properly

## RS485

**RS-485** is a different serial data transmission standard for use in long ranges or noisy environments.

### RS485 Configuration

**RS485 Serial Configuration**

Enabled

Baud rate

Parity

Flow control

Serial type

Interface	Allow IP
LAN	<input style="width: 100px;" type="text" value="192.168.1.124"/> <input style="width: 20px; height: 20px; border: 1px solid #ccc;" type="button" value="+"/> <span style="float: right; margin-right: 20px;"><input type="button" value="Delete"/></span>

Interface name:

Field Name	Value	Description
<b>Enabled</b>	yes   no; Default: <b>no</b>	Toggles the RS485 serial port function ON or OFF
<b>Baud rate</b>	300   1200   2400   4800   9600   19200   38400   57600   115200; Default: <b>115200</b>	The communication speed of the serial interface

<b>Parity</b>	None   Odd   Even; Default: <b>None</b>	The parity bit setting used for error detection during data transfer
<b>Flow control</b>	None   RTS- CTS   Xon- Xoff; Default: <b>None</b>	Specifies how many stop bits will be used to detect the end of character
<b>Serial type</b>	Console   Over IP   Modem   Modbus Gateway   NTRIP Client; Default: <b>Console</b>	Specifies the function of the serial interface
<b>Interface</b>	LAN   WAN   VPN   L2TP   PPTP   GRE   HOTSPOT   SSTP; Default: <b>LAN</b>	Interface used for connection
<b>Allow IP</b>	ip; Default: " "	Allows IP to connect to server

## Modes of different serial types in RS232 and RS485

### Console

In this mode the serial interface set up as a Linux console of the device. It can be used for debugging purposes, to get the status of the device or to control it.

### Over IP

In **Over IP Serial** type the router provides a connection to a TCP/IP network for the devices connected via serial interfaces.

*Mode: Server*

Serial type

Protocol

Mode

No leading zeros

TCP port

Timeout (s)

Field Name	Value	Description
<b>Protocol</b>	TCP; Default: <b>TCP</b>	Specifies the protocol used in the communication process

<b>Mode</b>	Server   Client   Bidirect; Default: <b>Server</b>	Specifies the device's role in the connection: <b>Server</b> - the device waits for incoming connections <b>Client</b> - the device initiates the connection <b>Bidirect</b> - acts as client by default but waits for incoming connections at the same time
<b>No leading zeros</b>	yes   no; Default: <b>no</b>	Specifies that the first hex zeros should be skipped
<b>TCP port</b>	integer [0..65535]; Default: " "	The port number used to connect to the server
<b>Timeout (s)</b>	integer; Default: " "	Disconnects clients after the amount of inactivity time (in seconds) specified in this field

Mode: Client

Serial type

Protocol

Mode

No leading zeros

Server Address

TCP port

Reconnect interval (s)

Field Name	Value	Description
<b>Protocol</b>	TCP; Default: <b>TCP</b>	The protocol used for data transmission
<b>Mode</b>	Server   Client   Bidirect; Default: <b>Server</b>	<b>Server</b> - waits for incoming connection <b>Client</b> - initiates the connection <b>Bidirect</b> - acts as a client by default, but at the same time waits for incoming connections
<b>No leading zeros</b>	yes   no; Default: <b>no</b>	Skips first hex zeros
<b>Server address</b>	host   ip; Default: <b>no</b>	Server address to which the client will connect to
<b>TCP port</b>	integer [0..65535]; Default: " "	The port number used to listen for incoming connections

**Reconnect intervals (s)** integer; Default: " "

Indicates the time period between reconnection attempts

Mode: Bidirect

Mode

No leading zeros

Client settings:

Server Address

TCP port

Reconnect interval (s)

Server settings:

TCP port

Timeout (s)

Output

Output state

Field Name	Value	Description
<b>Mode</b>	Server   Client   Bidirect; Default: <b>Server</b>	<b>Server</b> - waits for incoming connection <b>Client</b> - initiates the connection <b>Bidirect</b> - acts as a client by default, but at the same time waits for incoming connections
<b>No leading zeros</b>	yes   no; Default: <b>no</b>	Skips first hex zeros
<b>Server address</b>	host   ip; Default: <b>no</b>	Server address to which the client will connect to
<b>TCP port</b>	integer [0..65535]; Default: " "	The port number used to listen for incoming connections
<b>Reconnect intervals (s)</b>	integer; Default: " "	Indicates the time period between reconnection attempts
<b>TCP port</b>	integer [0..65535]; Default: " "	The port number used to listen for incoming connections
<b>Timeout (s)</b>	integer; Default: " "	Disconnects client after the specified timeout of inactivity

<b>Output</b>	OC Output   Relay Output; Default: <b>OC Output</b>	Output to indicate that application switched from client (default) to server state
<b>Output state</b>	integer [0..1]; Default: <b>0</b>	Output state value after the application reverts to server mode

## Modem

With Modem Serial type, the router imitates a dial-up modem. Connections to TCP/IP networks can be established using AT commands. The connection can be initiated by the device connected via serial interface with an ATD command: ATD <host>:<port>. If Direct connect settings are specified, the connection to the server is always active. Data mode can be entered by issuing the ATD command. Incoming connections are indicated by sending a RING to the serial interface.

Serial type

Direct connect

TCP port

Initiation string

No extra CR LF in response

Field Name	Value	Description
<b>Direct connect</b>	host:port   ip:port; Default: " "	Maintains a constant connection to specified host. Leave empty to use an ATD command to initiate the connection
<b>TCP port</b>	integer [0..65535]; Default: " "	The port number used to listen for incoming connections. Leave it empty to disable incoming connections
<b>Initiation string</b>	string; Default: " "	A command string that will be sent to the modem to initiate it in some special way
<b>No extra CR LF in response</b>	yes   no; Default: <b>yes</b>	Removes extra CR LF before and LF after response code

This is the AT command set\* used in Modem mode of the serial interfaces:

COMMAND	DESCRIPTION	USAGE
<b>A</b>	Answers incoming call	To answer incoming connection: ATA



<b>D</b>	Dial a number	To initiate data connection: ATD <host>:<port> To enter data mode with Direct connect settings: ATD
<b>E</b>	Local echo	Turn local echo on: ATE1 Turn local echo off: ATE0
<b>H</b>	Hang up current call	To end data connection: ATH
<b>O</b>	Return to data mode	To return to data mode from command mode: ATO
<b>Z</b>	Reset to default configuration	To reset the modem to default configuration: ATZ

\* Only these commands are supported in Modem mode.

## Modbus gateway

The Modbus gateway Serial type allows redirecting TCP data coming to a specified port to RTU specified by the Slave ID. The Slave ID can be specified by the user or be obtained directly from the Modbus header.

Serial type

Listening IP

Port

Slave ID configuration type

Slave ID

Field Name	Value	Description
<b>Listening IP</b>	ip; Default: <b>0.0.0.0</b>	IP address on which the Modbus gateway will wait for incoming connections
<b>Port</b>	integer [0..65535]; Default: " "	The port number used to listen for incoming connections
<b>Slave ID configuration type</b>	User defined   Obtained from TCP; Default: <b>User defined</b>	Specifies whether slave IDs are user defined or automatically obtained from TCP
<b>Slave ID   Permitted slave IDs</b>	integer   range of integers; Default: <b>1</b>	Specifies the slave ID of range of permitted slave IDs. The way this field is named and its function depends on the value of the <i>Slave ID configuration</i> field.

A range of IDs can be specified by placing a **hyphen (-)** between two integer numbers. For example, if you permit slave IDs in the range of 10 to 20, you would specify it as: **10-20**

You can also specify multiple values that are not connected in a range using **commas (,)**. For example, to specify 6, 50 and 100 as permitted slave IDs, you would have to use: **6,50,100**

## NTRIP client

Networked Transport of RTCM via Internet Protocol (Ntrip) is a protocol for streaming differential GPS (DGPS) data over the Internet in accordance with specification published by RTCM.

Serial type

IP address

Port

Mount point

Data format

User name

Password

Default NMEA string

Use device GPS

Field Name	Value	Description
<b>IP address</b>	ip; Default: <b>0.0.0.0</b>	IP address of the NTRIP server
<b>Port</b>	integer [0..65535]; Default: " "	TCP/UDP port used for NTRIP communication
<b>Mount point</b>	string; Default: " "	NTRIP mount point
<b>Data format</b>	NTRIP V2.0 TCP/IP   NTRIP V2.0 RSTP/RTP   NTRIP V1.0   Automatic detection   NTRIP V2.0 UDP; Default: <b>NTRIP V1.0</b>	Specifies the used version of NTRIP
<b>Username</b>	string; Default: " "	User name for NTRIP authentication
<b>Password</b>	string; Default: " "	Password for NTRIP authentication

<b>Default NMEA string</b>	string; Default: " "	Optional NMEA string that will be used as the default value when initiating the connection to the NTRIP server (this value is only sent to the server if there is no NMEA from router's GPS device)
<b>Use device GPS</b>	yes   no; Default: <b>no</b>	Allows to obtain default NMEA string from the router's GPS device. Only works if GPS service is enabled and location fix is obtained at the time of NTRIP service start

## VPN

### Summary

---

**Virtual Private Network (VPN)** is a method of connecting multiple private networks across the Internet. VPNs can serve to achieve many different goals, but some of its main purposes are:

- access between remote private networks;
- data encryption;
- Anonymity when browsing the Internet.

### OpenVPN

---

**OpenVPN** is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It is often regarded as being the most universal VPN protocol because of its flexibility, support of SSL/TLS security, multiple encryption methods, many networking features and compatibility with most OS platforms.

### OpenVPN client

---

An **OpenVPN client** is an entity that initiates a connection to an OpenVPN server. To create a new client instance, go to the **Services** → **VPN** → **OpenVPN** section, select **Role: Client**, enter a custom name and click the 'Add New' button. An OpenVPN client instance with the given name will appear in the "OpenVPN Configuration" list. A maximum of six OpenVPN client instances are allowed to be added.

To begin configuration, click the 'Edit' button next to the client instance. Refer to the figure and table below for information on the OpenVPN client's configuration fields:

## OpenVPN Instance: Client\_Demo

### Main Settings

Enable OpenVPN config from file

Enable

TUN/TAP

Protocol

Port

LZO

Authentication

Encryption

TLS cipher

Remote host/IP address

Resolve retry


Keep alive

Remote network IP address

Remote network IP netmask

HMAC authentication algorithm

Additional HMAC authentication


Extra options  

Use PKCS #12 format

Certificate authority  No file selected.

Client certificate  No file selected.

Client key  No file selected.

Private key decryption password (optional)  

Field	Value	Description
<b>Enable OpenVPN config from file</b>	yes   no; default: <b>no</b>	Enables custom OpenVPN configuration from file.
<b>Enable</b>	yes   no; default: <b>no</b>	Turns the OpenVPN instance on or off.
<b>TUN/TAP</b>	TUN (tunnel)   TAP (bridged); default: <b>TUN (tunnel)</b>	Virtual network device type. <ul style="list-style-type: none"> <li><b>TUN</b> - a virtual point-to-point IP link which operates at the network layer (OSI layer 3), used when routing is required.</li> </ul>

<b>Protocol</b>	UDP   TCP; default: <b>UDP</b>	<ul style="list-style-type: none"> <li>• <b>TAP</b> - a virtual Ethernet adapter (switch), operates at the data link layer (OSI layer 2), used when bridging is required.</li> </ul> <p>Transfer protocol used for the OpenVPN connection.</p>
		<ul style="list-style-type: none"> <li>• <b>Transmission Control Protocol (TCP)</b> - most commonly used protocol in the Internet Protocol (IP) suite. It ensures the recipient will receive packets in the order they were sent by numbering, analysing response messages, checking for errors and resending them if an issue occurs. It should be used when reliability is crucial (for example, in file transfer).</li> <li>• <b>User Datagram Protocol (UDP)</b> - packets are sent to the recipient without error-checking or back-and-forth quality control, meaning that when packets are lost, they are gone forever. This makes it less reliable but faster than TCP; therefore, it should be used when transfer speed is crucial (for example, in video streaming, live calls).</li> </ul>
<b>Port</b>	integer [0..65535]; default: <b>1194</b>	<p>TCP/UDP port number used for the connection. Make sure it matches the port number specified on the server side.</p> <p><b>NOTE:</b> traffic on the selected port will be automatically allowed in the router's firewall rules.</p>
<b>LZO</b>	yes   no; default: <b>no</b>	Turns LZO data compression on or off.
<b>Authentication</b>	TLS   Static Key   Password   TLS/Password; default: <b>TLS</b>	<p>Authentication mode, used to secure data sessions.</p> <ul style="list-style-type: none"> <li>• <b>Static key</b> is a secret key used for server-client authentication.</li> <li>• <b>TLS</b> authentication mode uses X.509 type certificates: <ul style="list-style-type: none"> <li>• Certificate Authority (CA)</li> </ul> </li> </ul>

- Client certificate
- Client key

All mentioned certificates can be generated using OpenVPN or Open SSL utilities on any type of host machine. One of the most popular utilities used for this purpose is called Easy-RSA.

- **Password** is a simple username/password based authentication where the owner of the OpenVPN server provides the login data.
- **TLS/Password** uses both TLS and username/password authentication.

## Encryption

DES-CBC 64 | RC2-CBC 128 | DES-EDE-CBC 128 | DES-EDE3-CBC 192 | DESX-CBC 192 | RC2-40-CBC 40 | CAST5-CBC 128 | RC2-64-CBC 64 | AES-128-CFB 128 | AES-128-CFB1 128 | AES-128-CFB8 128 | AES-128-OFB 128 | AES-128-CBC 128 | AES-128-GCM 128 | AES-192-CFB 192 | AES-192-CFB1 192 | AES-192-CFB8 192 | AES-192-OFB 192 | AES-192-CBC 192 | AES-192-GCM 192 | AES-256-CFB 256 | AES-256-CFB1 256 | AES-256-CFB8 256 | AES-256-OFB 256 | AES-256-CBC 256 | AES-256-GCM 256 |

Algorithm used for packet encryption.

	none ; default: <b>BF-CBC 128</b>	
<b>TLS: TLS cipher</b>	All   DHE+RSA   Custom; default: <b>All</b>	Packet encryption algorithm cipher.
<b>TLS: Allowed TLS ciphers</b>	All   DHE+RSA   Custom; default: <b>All</b>	A list of TLS ciphers accepted for this connection.
<b>Remote host/IP address</b>	ip; default: <b>none</b>	IP address or hostname of an OpenVPN server.
<b>Resolve retry</b>	integer   infinite; default: <b>infinite</b>	In case server hostname resolve fails, this field indicates the amount of time (in seconds) to retry the resolve. Specify <i>infinite</i> to retry indefinitely.
<b>Keep alive</b>	two integers separated by a space; default: <b>none</b>	Defines two time intervals: the first is used to periodically send ICMP requests to the OpenVPN server, the second one defines a time window, which is used to restart the OpenVPN service if no ICMP response is received during the specified time slice. When this value is specified on the OpenVPN server, it overrides the 'keep alive' values set on client instances. <b>Example:</b> <i>10 120</i>
<b>Static key: Local tunnel endpoint IP</b>	ip; default: <b>none</b>	IP address of the local OpenVPN network interface.
<b>Static key: Remote tunnel endpoint IP</b>	ip; default: <b>none</b>	IP address of the remote OpenVPN network (server) interface.
<b>Remote network IP address</b>	ip; default: <b>none</b>	LAN IP address of the remote network (server).
<b>Remote network IP netmask</b>	netmask; default: <b>none</b>	LAN IP subnet mask of the remote network (server).
<b>Password: User name</b>	string; default: <b>none</b>	Username used for authentication to the OpenVPN server.
<b>Password: Password</b>	string; default: <b>none</b>	Password used for authentication to the OpenVPN server.

<b>Extra options</b>	string; default: <b>none</b>	Extra OpenVPN options to be used by the OpenVPN instance.
<b>Use PKCS #12 format</b>	yes   no; default: <b>no</b>	Use PKCS #12 archive file format to bundle all the members of a chain of trust.
<b>PKCS #12 passphrase</b>	string; default: <b>none</b>	Passphrase to decrypt PKCS #12 certificates.
<b>PKCS #12 certificate chain</b>	string; default: <b>none</b>	
<b>TLS/Password: HMAC authentication algorithm</b>	none   SHA1   SHA256   SHA384   SHA512; default: <b>SHA1</b>	HMAC authentication algorithm type.
<b>TLS/Password: Additional HMAC authentication</b>	none   Authentication only (tls-auth)   Authentication and encryption (tls-crypt); default: <b>none</b>	An additional layer of HMAC authentication on top of the TLS control channel to protect against DoS attacks.
<b>TLS/Password: HMAC authentication key</b>	.key file; default: <b>none</b>	Uploads an HMAC authentication key file.
<b>TLS/Password: HMAC key direction</b>	0   1   none; default: <b>1</b>	The value of the key direction parameter should be complementary on either side (client and server) of the connection. If one side uses 0, the other side should use 1, or both sides should omit the parameter altogether.
<b>TLS/Password: Certificate authority</b>	.ca file; default: <b>none</b>	Certificate authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.
<b>TLS: Client certificate</b>	.crt file; default: <b>none</b>	Client certificate is a type of digital certificate that is used by client systems to make authenticated requests to a remote server. Client certificates play a key role in many mutual authentication



designs, providing strong assurances of a requester's identity.

<b>TLS: Client key</b>	.key file; default: <b>none</b>	Authenticates the client to the server and establishes precisely who they are.
<b>TLS: Private key decryption password (optional)</b>	string; default: <b>none</b>	A password used to decrypt the server's private key. Use only if server's .key file is encrypted with a password.
<b>Static key: Static pre-shared key</b>	.key file; default: <b>none</b>	Uploads a secret key file used for server-client authentication.

#### Additional notes:

- Some configuration fields become available only when certain other parameters are selected. The names of the parameters are followed by a prefix that specifies the authentication type under which they become visible. Different color codes are used for different prefixes:
  - Red for **Authentication: TLS**
  - Purple for **Authentication: Static key**
  - Blue for **Authentication: Password**
- After changing any of the parameters, don't forget to click the **Save** button located at the bottom-right side of the page.

## OpenVPN server

---

An **OpenVPN server** is an entity that waits for incoming connections from OpenVPN clients. To create a new server instance, go to the *Services* → *VPN* → *OpenVPN* section, select *Role: Server*, enter a custom name and click the 'Add New' button. An OpenVPN server instance with the given name will appear in the "OpenVPN Configuration" list. Only one OpenVPN server instance is allowed to be added.

A server needs to have a public IP address in order to be available from the public network (the Internet).

To begin configuration, click the 'Edit' button next to the server instance. Refer to the figure and table below for information on the OpenVPN server's configuration fields:

## OpenVPN Instance: Server\_Demo

### Main Settings

Enable OpenVPN config from file

Enable

TUN/TAP

Protocol

Port

LZO

Authentication

Encryption

TLS cipher

Client to client

Keep alive

Virtual network IP address

Virtual network netmask

Push option

Allow duplicate certificates

HMAC authentication algorithm

Additional HMAC authentication

Use PKCS #12 format

Certificate authority  No file selected.

Server certificate  No file selected.

Server key  No file selected.

Diffie Hellman parameters  No file selected.

CRL file (optional)  No file selected.

Enable manual ccd upload

Field	Value	Description
<b>Enable OpenVPN config from file</b>	yes   no; default: <b>no</b>	Enables custom OpenVPN configuration from file.
<b>Enable</b>	yes   no; default: <b>no</b>	Turns the OpenVPN instance on or off.
<b>TUN/TAP</b>	TUN (tunnel)   TAP (bridged); default: <b>TUN (tunnel)</b>	Virtual network device type. <ul style="list-style-type: none"> <li><b>TUN</b> - a virtual point-to-point IP link which operates at the network</li> </ul>

<p><b>Protocol</b></p>	<p>UDP   TCP; default: <b>UDP</b></p>	<p>layer (OSI layer 3), used when routing is required.</p> <ul style="list-style-type: none"> <li>• <b>TAP</b> - a virtual Ethernet adapter (switch), operates at the data link layer (OSI layer 2), used when bridging is required.</li> </ul> <p>Transfer protocol used for the connection.</p>
<p><b>Port</b></p>	<p>integer [0..65535]; default: <b>1194</b></p>	<ul style="list-style-type: none"> <li>• <b>Transmission Control Protocol (TCP)</b> - most commonly used protocol in the Internet Protocol (IP) suite. It ensures the recipient will receive packets in the order they were sent by numbering, analysing response messages, checking for errors and resending them if an issue occurs. It should be used when reliability is crucial (for example, file transfer).</li> <li>• <b>User Datagram Protocol (UDP)</b> - packets are sent to the recipient without error-checking or back-and-forth quality control, meaning that when packets are lost, they are gone forever. This makes it less reliable but faster than TCP; therefore, it should be used when transfer speed is crucial (for example, video streaming, live calls).</li> </ul> <p>TCP/UDP port number used for the connection. Make sure it matches the port number specified on the server side.</p> <p><b>NOTE:</b> traffic on the selected port will be automatically allowed in the router's firewall rules.</p>
<p><b>LZO</b></p>	<p>yes   no; default: <b>no</b></p>	<p>Turns LZO data compression on or off.</p>
<p><b>Authentication</b></p>	<p>TLS   Static Key   TLS/Password; default: <b>TLS</b></p>	<p>Authentication mode, used to secure data sessions.</p> <ul style="list-style-type: none"> <li>• <b>Static key</b> is a secret key used for server-client authentication.</li> </ul>

- **TLS** authentication mode uses X.509 type certificates:
  - Certificate Authority (CA)
  - Client certificate
  - Client key

All mentioned certificates can be generated using OpenVPN or Open SSL utilities on any type of host machine. One of the most popular utilities used for this purpose is called Easy-RSA.

- **TLS/Password** uses both TLS and username/password authentication.

## Encryption

DES-CBC 64 | RC2- Algorithm used for packet encryption.  
 CBC 128 | DES-  
 EDE-CBC 128 |  
 DES-EDE3-CBC 192  
 | DESX-CBC 192 |  
 RC2-40-CBC 40 |  
 CAST5-CBC 128 |  
 RC2-64-CBC 64 |  
 AES-128-CFB 128 |  
 AES-128-CFB1 128  
 | AES-128-CFB8  
 128 | AES-128-OFB  
 128 | AES-128-CBC  
 128 | AES-128-  
 GCM 128 | AES-  
 192-CFB 192 | AES-  
 192-CFB1 192 |  
 AES-192-CFB8 192  
 | AES-192-OFB 192  
 | AES-192-CBC 192  
 | AES-192-GCM  
 192 | AES-256-CFB  
 256 | AES-256-  
 CFB1 256 | AES-  
 256-CFB8 256 |  
 AES-256-OFB 256 |  
 AES-256-CBC 256 |  
 AES-256-GCM 256  
 | none ;

	default: <b>BF-CBC 128</b>	
<b>Static key: Local tunnel endpoint IP</b>	ip; default: <b>none</b>	IP address of the local OpenVPN network interface.
<b>Static key: Remote tunnel endpoint IP</b>	ip; default: <b>none</b>	IP address of the remote OpenVPN network (client) interface.
<b>Static key: Remote network IP address</b>	ip; default: <b>none</b>	LAN IP address of the remote network (client).
<b>Static key: Remote network IP netmask</b>	netmask; default: <b>none</b>	LAN IP subnet mask of the remote network (client).
<b>TLS/TLS/Password: TLS cipher</b>	All   DHE+RSA   Custom; default: <b>All</b>	Packet encryption algorithm cipher.
<b>TLS/Password: Allowed TLS ciphers</b>	All   DHE+RSA   Custom; default: <b>All</b>	A list of TLS ciphers accepted for this connection.
<b>TLS/TLS/Password: Client to client</b>	yes   no; default: <b>no</b>	Allows OpenVPN clients to communicate with each other on the VPN network.
<b>TLS/TLS/Password: Keep alive</b>	two integers separated by a space; default: <b>none</b>	Defines two time intervals: the first is used to periodically send ICMP requests to the OpenVPN server, the second one defines a time window, which is used to restart the OpenVPN service if no ICMP response is received during the specified time slice. When this value is specified on the OpenVPN server, it overrides the 'keep alive' values set on client instances. <b>Example:</b> <i>10 120</i>
<b>TLS/TLS/Password: Virtual network IP address</b>	ip; default: <b>none</b>	IP address of the OpenVPN network.
<b>TLS/TLS/Password: Virtual network netmask</b>	netmask; default: <b>none</b>	Subnet mask of the OpenVPN network.
<b>TLS/TLS/Password: Push option</b>	OpenVPN options; default: <b>none</b>	Push options are a way to "push" routes and other additional OpenVPN options to connecting clients.
<b>TLS/TLS/Password: Allow duplicate certificates</b>	yes   no; default: <b>no</b>	When enabled allows multiple clients to connect using the same certificates.
<b>Use PKCS #12 format</b>	yes   no; default: <b>no</b>	Use PKCS #12 archive file format to bundle all the members of a chain of trust.
<b>PKCS #12 passphrase</b>	string; default: <b>none</b>	Passphrase to decrypt PKCS #12 certificates.

<b>PKCS #12 certificate chain</b>	string; default: <b>none</b>	
<b>TLS/Password: User name</b>	string; default: <b>none</b>	Username used for authentication to this OpenVPN server.
<b>TLS/Password: Password</b>	string; default: <b>none</b>	Password used for authentication to this OpenVPN server.
<b>Static key: Static pre-shared key</b>	.key file; default: <b>none</b>	Uploads a secret key file used for server-client authentication.
<b>TLS/TLS/Password: Certificate authority</b>	.ca file; default: <b>none</b>	Certificate authority is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.
<b>TLS/TLS/Password: Server certificate</b>	.crt file; default: <b>none</b>	A type of digital certificate that is used to identify the OpenVPN server.
<b>TLS/TLS/Password: Server key</b>	.key file; default: <b>none</b>	Authenticates clients to the server.
<b>TLS/TLS/Password: Diffie Hellman parameters</b>	.pem file; default: <b>none</b>	DH parameters define how OpenSSL performs the Diffie-Hellman (DH) key-exchange.
<b>TLS/TLS/Password: CRL file (optional)</b>	.pem file   .crl file; default: <b>none</b>	A certificate revocation list (CRL) file is a list of certificates that have been revoked by the certificate authority (CA). It indicates which certificates are no longer accepted by the CA and therefore cannot be authenticated to the server.
<b>TLS/TLS/Password: Enable manual ccd upload</b>	yes   no; default: <b>no</b>	Enable manual upload of client-config-dir files.

**Additional notes:**

- Some configuration fields become available only when certain other parameters are selected. The names of the parameters are followed by a prefix that specifies the authentication type under which they become visible. Different color codes are used for different prefixes:
  - Red for **Authentication: TLS**
  - Purple for **Authentication: Static key**
  - Blue for **Authentication: TLS/Password**
- After changing any of the parameters, don't forget to click the **Save** button located at the bottom-right side of the page.

# IPsec

To create a new IPsec instance, go to the *Services* → *VPN* → *IPsec* section, enter a custom name and click "Add". An IPsec instance with the given name will appear in the "IPsec Configuration" list.

To begin configuration, click the 'Edit' button located next to the instance.

## IPsec configuration

The **IPsec configuration** section is used to configure the main parameters of an IPsec connection. Refer to the figure and table below for information on the configuration fields located in the general settings section.

The screenshot displays the 'IPsec Configuration' page. At the top left, the word 'IPsec' is written in blue. Below it, a grey header bar contains the text 'IPsec Configuration'. The main area contains the following configuration options:

- Enable:
- IKE version: IKEv1 (dropdown)
- Mode: Main (dropdown)
- Type: Tunnel (dropdown)
- On startup: Start (dropdown)
- My identifier:
- Local IP address/Subnet mask:  (+)
- Left firewall:
- Force encapsulation:
- Dead Peer Detection:
- Remote VPN endpoint:
- Remote identifier:
- Remote IP address/Subnet mask:  (+)
- Right firewall:
- Enable keepalive:
- Host:
- Ping period (sec):
- Allow WebUI access:
- Custom options:  (+)

Field	Value	Description
<b>Enable</b>	yes   no; default: <b>no</b>	Turns the IPsec instance on or off.
<b>IKE version</b>	IKEv1   IKEv2; default: <b>IKEv1</b>	<p>Internet Key Exchange (IKE) version used for key exchange.</p> <ul style="list-style-type: none"> <li>• <b>IKEv1</b> - more commonly used but contains known issues, for example, dealing with NAT.</li> <li>• <b>IKEv2</b> - updated version with increased and improved capabilities, such as integrated NAT support, supported multihosting, deprecated exchange modes (does not use main or aggressive mode; only 4 messages required to establish a connection).</li> </ul>
<b>Mode</b>	Main   Aggressive; default: <b>Main</b>	<p>Internet Security and Key Management Protocol (ISAKMP) phase 1 exchange mode.</p> <ul style="list-style-type: none"> <li>• <b>Main</b> - performs three two-way exchanges between the initiator and the receiver (a total of 9 messages).</li> <li>• <b>Aggressive</b> - performs fewer exchanges than main mode (a total of 6 messages) by storing most data into the first exchange. In aggressive mode, the information is exchanged before there is a secure channel, making it less secure but faster than main mode.</li> </ul>
<b>Type</b>	Tunnel   Transport; default: <b>Tunnel</b>	<p>Type of connection.</p> <ul style="list-style-type: none"> <li>• <b>Tunnel</b> - protects internal routing information by encapsulating the entire IP packet (IP header and payload); commonly used in site-to-site VPN connections; supports NAT traversal.</li> <li>• <b>Transport</b> - only encapsulates IP payload data; used in client-to-site VPN connections; does not support NAT traversal; usually implemented with other tunneling protocols (for example, L2TP).</li> </ul>



<b>On startup</b>	Ignore   Add   Route   Start; default: <b>Start</b>	Defines how the instance should act on router startup. <ul style="list-style-type: none"> <li>• <b>Ignore</b> - does not start the tunnel.</li> <li>• <b>Add</b> - loads a connection without starting it.</li> <li>• <b>Route</b> - starts the tunnel only if there is traffic.</li> <li>• <b>Start</b> - starts the tunnel on router startup.</li> </ul>
<b>My identifier</b>	ip   string; default: <b>none</b>	Defines how the user (IPsec instance) will be identified during authentication.
<b>Tunnel: Local IP address/Subnet mask</b>	ip/netmask   default: <b>none</b>	Local IP address and subnet mask used to determine which part of the network can be accessed in the VPN network. Netmask range [0..32]. If left empty, IP address will be selected automatically.
<b>Left firewall</b>	off   on; default: <b>on</b>	Adds necessary firewall rules to allow traffic of this IPsec instance on this router.
<b>Force encapsulation</b>	yes   no; default: <b>no</b>	Forces UDP encapsulation for ESP packets even if a "no NAT" situation is detected.
<b>Dead Peer Detection</b>	yes   no; default: <b>no</b>	A function used during Internet Key Exchange (IKE) to detect a "dead" peer. It used to reduce traffic by minimizing the number of messages when the opposite peer is unavailable and as failover mechanism.
<b>Dead Peer Detection: Delay (sec)</b>	integer; default: <b>none</b>	The frequency of checking whether a peer is still available or not.
<b>Dead Peer Detection: Timeout (sec)</b>	integer; default: <b>none</b>	Time limit after which the IPsec instance will stop checking the availability of a peer and determine it to be "dead" if no response is received.
<b>Authentication type</b>	Pre-shared key   X.509; default: <b>Pre-shared key</b>	Here you can choose authentication type accordingly to your IPsec configuration
<b>Certificate file</b>	.crt file; default: <b>none</b>	Uploads a certificate file.

<b>Key file</b>	.key file; default: <b>none</b>	Uploads a key file.
<b>CA certificate</b>	.crt file; default: <b>none</b>	Uploads a Certificate authority (CA) file.
<b>Remote participant's certificate</b>	.crt file; default: <b>none</b>	Remote participant's certificate certificate is used to authenticate remote peer
<b>Use additional xauth authentication</b>	yes   no; default: <b>no</b>	Adds additional xauth authentication options.
<b>Xauth: Xauth password</b>	string; default: <b>none</b>	Password for additional peer authentication.
<b>Remote VPN endpoint</b>	host   ip; default: <b>none</b>	IP address or hostname of the remote IPsec instance.
<b>Remote identifier</b>	ip   string; default: <b>none</b>	Defines remote IPsec instance identification.
<b>Tunnel: Remote IP address/subnet mask</b>	ip/netmask; default: <b>none</b>	Remote network IP address and subnet mask used to determine which part of the network can be accessed in the VPN network. Netmask range [0..32]. This value must differ from the device's LAN IP.
<b>Right firewall</b>	yes   no; default: <b>yes</b>	Adds necessary firewall rules to allow traffic of from the opposite IPsec instance on this router.
<b>Transport: Use with DMVPN</b>	yes   no; default: <b>no</b>	Adds several necessary options to make DMVPN work.
<b>Passthrough networks</b>	None   LAN   Wired   WiFi   Mobile   custom; default: <b>none</b>	Select networks which should be passthrough and excluded from routing through tunnel
<b>Enable keepalive</b>	yes   no; default: <b>no</b>	When enabled, the instance sends ICMP packets to the specified host at the specified frequency. If no response is received, the router will attempt to restart the connection.
<b>Host</b>	host   ip; default: <b>none</b>	Hostname or IP address to which keep alive ICMP packets will be sent to.
<b>Ping period (sec)</b>	integer [0..99999999]; default: <b>none</b>	The frequency at which keep alive ICMP packets will be sent to the specified host or IP address.

<b>Allow WebUI access</b>	yes   no; default: <b>no</b>	Allows WebUI access for hosts in the VPN network.
<b>Custom options</b>	ipsec options; default: <b>none</b>	Provides the possibility to further customize the connection by adding extra IPsec options.

**Additional notes:**

- Some configuration fields become available only when certain other parameters are selected. Different color codes are used for different parameters:
  - Orange for **Type: Xauth**
  - Red for **Type: Tunnel**
  - Purple for **Type: Transport**
  - Blue for **Dead Peer Detection: Enabled**
- After changing any of the parameters, don't forget to click the **Save** button located at the bottom-right side of the page.

## Phase settings

IKE (Internet Key Exchange) is a protocol used to set up security associations (SAs) for the IPsec connection. This process is required before the IPsec tunnel can be established. It is done in two phases:

---

<b>Phase</b>	<b>Mode</b>
<b>Phase 1</b>	Main mode (figure 1)      Aggressive mode (figure 2)
<ul style="list-style-type: none"> <li>• Establishes a secure channel between peers</li> <li>• Authenticates peers</li> <li>• Negotiates SA policy</li> <li>• Shares secret keys</li> <li>• Establishes secure tunnel for phase 2</li> </ul>	<ul style="list-style-type: none"> <li>• 6 packets exchanged</li> <li>• Identity protected during exchange</li> <li>• 3 packets exchanged</li> <li>• Identity information exchanged before a secure channel is established</li> </ul>
<b>Phase 2</b>	Quick mode
<ul style="list-style-type: none"> <li>• Sets up matching IPsec SAs</li> <li>• Periodically renegotiates IPsec SAs</li> </ul>	<ul style="list-style-type: none"> <li>• 3 packets exchanged</li> <li>• IPsec SA parameters (ESP/AH, SHA/MD5) established</li> <li>• SA lifetime set</li> </ul>

Figure 1

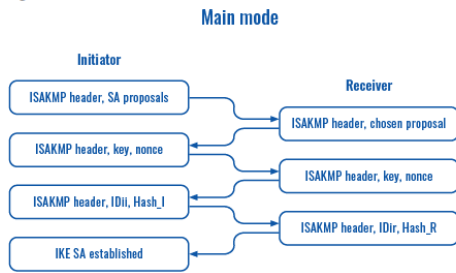
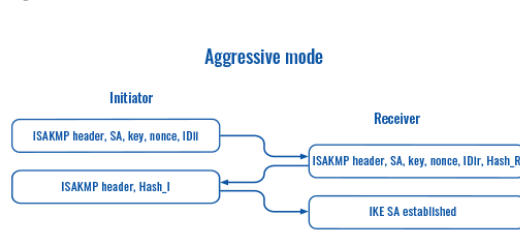


Figure 2



**Phase**

The phase must match with another incoming connection to establish IPsec

Phase 1

Phase 2

Encryption algorithm 3DES ▼

Authentication SHA1 ▼

DH group MODP1536 ▼

Lifetime (h)  Hours ▼

Field	Value	Description
<b>Encryption algorithm</b>	DES   3DES   AES128   AES192   AES256; default: <b>3DES</b>	Algorithm used for data encryption.
<b>Authentication/Hash algorithm</b>	MD5   SHA1   SHA256   SHA384   SHA512; default: <b>SHA1</b>	Algorithm used for exchanging authentication and hash information.
<b>DH group/PFS group</b>	MODP768   MODP1024   MODP1536   MODP2048   MODP3072   MODP4096; default: <b>MODP1536</b>	Diffie-Hellman (DH) group used in the key exchange process. Higher group numbers provide more security, but take longer and use more resources to compute the key.
<b>Lifetime</b>	integer; default: <b>8 hours</b>	Defines a time period after which the phase will re-initiate its exchange of information.

## Pre-shared keys

A **pre-shared key** is a secret password used for authentication between IPsec peers before a secure tunnel is established. To create a new key, click the 'Add' button.

The figure below is an example of the Pre-shared keys section and the table below provides information on configuration fields contained in that section:

The screenshot shows a configuration interface for Pre-shared Keys. At the top is a header 'Pre-shared Keys'. Below it is a table with two columns: 'Pre-shared key' and 'Secret's ID selector'. The 'Pre-shared key' column contains an empty text input field with a copy icon to its right. The 'Secret's ID selector' column contains a text input field with the placeholder text '%any, IP or FQDN' and a plus icon to its right. To the right of the 'Secret's ID selector' input is a 'Delete' button. Below the table is an 'Add' button.

Field	Value	Description
<b>Pre-shared key</b>	string; default: <b>none</b>	A shared password used for authentication between IPsec peers before a secure channel is established.
<b>Secret's ID selector</b>	string; default: <b>none</b>	Each secret can be preceded by a list of optional ID selectors. A selector is an IP address, a Fully Qualified Domain Name, user@FQDN or %any. <b>NOTE:</b> IKEv1 only supports IP address ID selector.

# PPTP

**Point-to-Point Tunneling Protocol (PPTP)** is a type of VPN protocol that uses a TCP control channel and a Generic Routing Encapsulation tunnel to encapsulate PPP packets.

## PPTP client

A **PPTP client** is an entity that initiates a connection to a PPTP server. To create a new client instance, go to the *Services* → *VPN* → *PPTP* section, select *Role: Client*, enter a custom name and click the 'Add New' button. A PPTP client instance with the given name will appear in the "PPTP Configuration" list.

To begin configuration, click the 'Edit' button located next to the client instance. Refer to the figure and table below for information on the PPTP client's configuration fields:

The screenshot shows the configuration page for a PPTP Client Instance named 'Demo'. Under the 'Main Settings' section, there are several fields: 'Enable' (checkbox), 'Use as default gateway' (checkbox), 'Client to client' (checkbox), 'Server' (text input), 'User name' (text input), and 'Password' (password input with an eye icon for visibility toggle).

Field	Value	Description
<b>Enable</b>	yes   no; default: <b>no</b>	Turns the PPTP instance on or off.
<b>Use as default gateway</b>	yes   no; default: <b>no</b>	When turned on, this connection will become the router's default route. This means that all traffic directed to the Internet will go through the PPTP server and the server's IP address will be seen as this device's source IP to other hosts on the Internet. <b>NOTE:</b> this can only be used when <a href="#">WAN Failover</a> is turned off.
<b>Client to client</b>	yes   no; default: <b>no</b>	Adds a route that makes other PPTP clients accessible within the PPTP network.

<b>Server</b>	ip   host; default: <b>none</b>	IP address or hostname of a PPTP server.
<b>Username</b>	string; default: <b>none</b>	Username used for authentication to the PPTP server.
<b>Password</b>	string; default: <b>none</b>	Password used for authentication to the PPTP server.

## PPTP server

A **PPTP server** is an entity that waits for incoming connections from PPTP clients. To create a new server instance, go to the *Services* → *VPN* → *PPTP* section, select *Role: Server*, enter a custom name and click the 'Add New' button. A PPTP server instance with the given name will appear in the "PPTP Configuration" list. Only one PPTP server instance is allowed to be added.

A server needs to have a public IP address in order to be available from the public network (the Internet).

To begin configuration, click the 'Edit' button located next to the server instance. Refer to the figure and table below for information on the PPTP server's configuration fields:

**PPTP Server Instance: Demo**

---

**Main Settings**

Enable

Local IP

Remote IP range start

Remote IP range end

---

User name	Password	PPTP Client's IP	
<input type="text" value="youruser"/>	<input type="password" value="*****"/>	<input type="text"/>	<input type="button" value="Delete"/>

---

Field	Value	Description
<b>Enable</b>	yes   no; default: <b>no</b>	Turns the PPTP instance on or off.
<b>Local IP</b>	ip; default: <b>192.168.0.1</b>	IP address of this PPTP network interface.
<b>Remote IP range start</b>	ip; default: <b>192.168.0.20</b>	PPTP IP address leases will begin from the address specified in this field.

<b>Remote IP range end</b>	ip; default: <b>192.168.0.30</b>	PPTP IP address leases will end with the address specified in this field.
<b>User name</b>	string; default: <b>youruser</b>	Username used for authentication to this PPTP server.
<b>Password</b>	string; default: <b>yourpass</b>	Password used for authentication to this PPTP server.
<b>PPTP Client's IP</b>	ip; default: <b>none</b>	Assigns an IP address to the client that uses the adjacent authentication info. This field is optional and if left empty the client will simply receive an IP address from the IP pool defined above.



# L2TP

In computer networking, **Layer 2 Tunneling Protocol (L2TP)** is a tunneling protocol used to support virtual private networks (VPNs). It is more secure than PPTP but, because it encapsulates the transferred data twice, but it is slower and uses more CPU power.

## L2TP client

An **L2TP client** is an entity that initiates a connection to an L2TP server. To create a new client instance, go to the *Services* → *VPN* → *L2TP* section, select *Role: Client*, enter a custom name and click the 'Add New' button. An L2TP client instance with the given name will appear in the "L2TP Configuration" list.

To begin configuration, click the 'Edit' button located next to the client instance. Refer to the figure and table below for information on the L2TP client's configuration fields:

The screenshot shows the configuration interface for an L2TP Client Instance named 'Demo'. It features a 'Main Settings' section with the following fields:

- Enable:** A checkbox that is currently unchecked.
- Server:** A text input field.
- Username:** A text input field.
- Password:** A text input field with a toggle icon to the right.
- Keep alive:** A text input field.
- Default route:** A checkbox that is currently unchecked.

Below the 'Default route' checkbox, there is a note: "Use this option when multiwan is off".

Field	Value	Description
<b>Enable</b>	yes   no; default: <b>no</b>	Turns the L2TP instance on or off.
<b>Server</b>	ip   host; default: <b>none</b>	IP address or hostname of an L2TP server.
<b>Username</b>	string; default: <b>none</b>	Username used for authentication to the L2TP server.
<b>Password</b>	string; default: <b>none</b>	Password used for authentication to the L2TP server.
<b>Keep alive</b>	integer; default: <b>none</b>	Frequency (in seconds) at which LCP echo requests are sent to the remote instance in

order to determine the health of the connection.

<b>Default route</b>	yes   no; default: <b>no</b>	When turned on, this connection will become the router's default route. This means that all traffic directed to the Internet will go through the L2TP server and the server's IP address will be seen as this device's source IP to other hosts on the Internet. <b>NOTE:</b> this can only be used when WAN Failover is turned off.
----------------------	------------------------------	---

## L2TP server

An **L2TP server** is an entity that waits for incoming connections from L2TP clients. To create a new server instance, go to the *Services* → *VPN* → *L2TP* section, select *Role: Server*, enter a custom name and click the 'Add New' button. An L2TP server instance with the given name will appear in the "L2TP Configuration" list. Only one L2TP server instance is allowed to be added.

A server needs to have a public IP address in order to be available from the public network (the Internet).

To begin configuration, click the 'Edit' button located next to the server instance. Refer to the figure and table below for information on the L2TP server's configuration fields:

User name	Password	L2TP Client's IP
user	****	

Field	Value	Description
<b>Enable</b>	yes   no; default: <b>no</b>	Turns the L2TP instance on or off.
<b>Local IP</b>	ip; default: <b>192.168.0.1</b>	IP address of this L2TP network interface.
<b>Remote IP range begin</b>	ip; default: <b>192.168.0.20</b>	L2TP IP address leases will begin from the address specified in this field.

<b>Remote IP range end</b>	ip; default: <b>192.168.0.30</b>	L2TP IP address leases will end with the address specified in this field.
<b>User name</b>	string; default: <b>user</b>	Username used for authentication to this L2TP server.
<b>Password</b>	string; default: <b>pass</b>	Password used for authentication to this L2TP server.
<b>L2TP Client's IP</b>	ip; default: <b>none</b>	Assigns an IP address to the client that uses the adjacent authentication info. This field is optional and if left empty the client will simply receive an IP address from the IP pool defined above.

# Dynamic DNS

## Summary

---

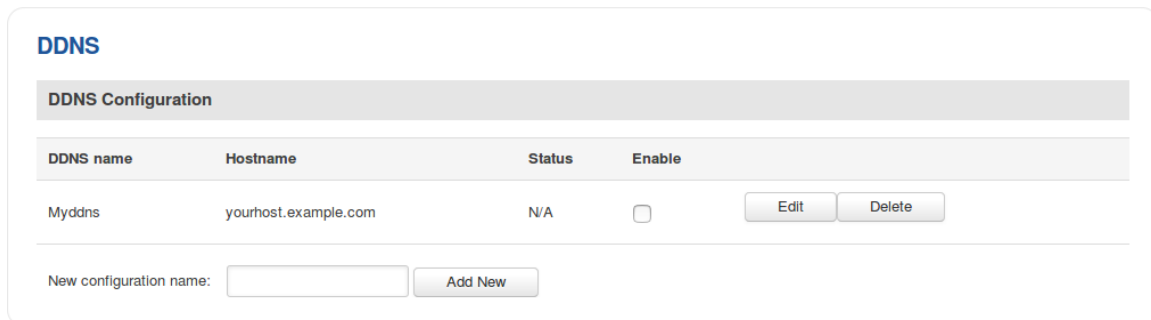
**Dynamic DNS (DDNS or DynDNS)** is a method of automatically updating a name server in the Domain Name System (DNS). This is most often utilized when the end user has a dynamic IP address and wants to bind it to a static hostname.

The router is compatible with many different third party DNS services that provide the possibility to create a custom hostname and bind it to an IP address. The DDNS service periodically updates the IP address information of the hostname, making sure that the device remains reachable via the same hostname even in cases when its IP address has changed.

## Dynamic DNS Overview

---

By default, an unconfigured DDNS instance will be present in the **Dynamic DNS Overview** page (the figure below is an example of this). You can create more DDNS instances by entering a **New configuration name** and clicking the **Add new** button or you can edit the existing instance since it is not operational by default.



The screenshot shows the DDNS Configuration page. At the top, there is a header 'DDNS' and a sub-header 'DDNS Configuration'. Below this is a table with the following columns: 'DDNS name', 'Hostname', 'Status', and 'Enable'. The table contains one row with the following data: 'Myddns', 'yourhost.example.com', 'N/A', and an unchecked checkbox. To the right of the table are 'Edit' and 'Delete' buttons. Below the table is a form with a label 'New configuration name:' followed by an input field and an 'Add New' button.

DDNS name	Hostname	Status	Enable	
Myddns	yourhost.example.com	N/A	<input type="checkbox"/>	<button>Edit</button> <button>Delete</button>

New configuration name:  Add New

## Editing a DDNS instance

---

To configure a DDNS instance, click the **Edit** button located next to it.

The figure below is an example of the edit page of the default DDNS instance called "MyDDNS" (already present in the router by default) and the table below provides information on the configuration fields contained in that page:

## Dynamic DNS

Dynamic DNS allows you to reach your router using a fixed hostname while having a dynamically changing IP address.

**DDNS**

Enable

Use HTTP Secure

Status N/A

Service

Lookup host

Hostname

User name

Password

IP address source

Public, Private, Custom or Script IP source setting, will disable DNS rebinding protection

Network

IP renew interval  IP renew interval unit

Force IP renew  Force IP renew unit

Field Name	Value	Description
<b>Enable</b>	yes   no; Default: <b>no</b>	Turns the DDNS instance ON or OFF
<b>Use HTTP Secure</b>	yes   no; Default: <b>no</b>	Enables SSL data encryption
<b>Status</b>	string; Default: <b>N/A</b>	Data on the last status update of the DDNS instance. When status is shown as "N/A", it means that the router has not been able to establish a connection to the DNS service provider
<b>Service</b>	third party DNS service (chosen from list*)   -- custom --; Default: <b>dyn.com</b>	Third party DNS service provider
<b>Lookup host</b>	host; Default: <b>yourhost.example.com</b>	Fully qualified domain name (FQDN) of your defined host. This is required to verify what the hostname's current IP address at DNS is (using <i>nslookup/host</i> command)
<b>Hostname</b>	host; Default: <b>yourhost.example.com</b>	Hostname that will be linked with the router's IP address
<b>Username</b>	string; Default: <b>your_username</b>	User name required to login to the third party DNS service; used to periodically login to your DNS service account and make necessary updates.
<b>Password</b>	string; Default: <b>your_password</b>	Password required to login to the third party DNS service; used to periodically login to your DNS service account and make necessary updates.
<b>IP address source</b>	Custom   Public   Private   Script; Default: <b>Custom</b>	Defines the source to read the system's IPv4-Address from, that will be sent to the DNS provider. So if, for example, your UCR has a Private IP (i.e., 10.140.56.57) on its WAN

<b>Network</b>	LAN   WAN   WAN2   WAN3   PPP   PPP_USB ; Default: <b>WAN</b>	interface, then you can send this exact IP to DDNS server by selecting <b>Private</b> Specifies which interface's IP address should be bound to the hostname
<b>IP renew interval</b>	integer [5..600000]; Default: <b>10</b>	Frequency at which the device will check whether it's IP address has changed
<b>IP renew interval unit</b>	Minutes   Hours   Days; Default: <b>Minutes</b>	Unit which is used in IP renew interval
<b>Force IP renew</b>	integer [5..600000]; Default: <b>72</b>	Frequency at which IP update requests are sent to the DNS provider
<b>Force IP renew unit</b>	Minutes   Hours   Days; Default: <b>Minutes</b>	Unit which is used in Force IP renew interval

# SMS Gateway

## Summary

---

The **SMS Gateway** service is used to set up various SMS related (mostly automated) functions.

## Post/Get

---

The **Post/Get Configuration** section is used to turn ON and configure SMS related post/get settings. When the function is enabled, it provides you with the possibility to perform SMS related action requests by writing them in the URL field of your web browser.

The figure below is an example of the Post/Get Configuration page and the table below provides information on fields contained in that page:

Field Name	Value	Description
<b>Enable</b>	yes   no; Default: <b>no</b>	Turns SMS post/get ON or OFF
<b>Username</b>	string; Default: <b>user1</b>	User name used for authorization when sending post/get requests
<b>Password</b>	string; Default: <b>user_pass</b>	Password used for authorization when sending post/get requests

# GPS

## Summary

---

The **Global Positioning System (GPS)** is a space-based radio navigation system.

## Map

---

The **Map** page displays the device's current coordinates and position on the map. To see the device's location on the map, make sure to attach the GPS antenna on the router and enable GPS in the General page.

## General

---

The **General** section is used to enable the GPS service and the support for different types satellites. Once you turn on GPS, you can check the Map page in order to see if the router has obtained a GPS fix. It is very important to attach the GPS antenna on the router and place it outside (not inside of a building). The router will not be likely to obtain a GPS fix otherwise.

The figure below is an example of the General page and the table below provides information on the fields contained in that page:

**GPS configuration**

GPS service needs to be enabled to use GPS related functionality. You can micromanage this service using configuration options inside the tabs above.

Enabled

**Satellite configuration**

Changing these options requires modem reboot

Galileo NMEA support

Glonass NMEA support

BeiDou NMEA support

Field	Value	Description
<b>Enabled</b>	yes   no; default: <b>no</b>	Turns the GPS service on or off.
<b>Galileo NMEA support*</b>	yes   no; default: <b>no</b>	Turns support for Galileo satellites on or off.
<b>Glonass NMEA support*</b>	yes   no; default: <b>no</b>	Turns support for Glonass satellites on or off.
<b>BeiDou NMEA support*</b>	yes   no; default: <b>no</b>	Turns support for BeiDou satellites on or off.



\*Changing these options requires a modem reboot. Therefore, if you make changes to these options and save them, the router will lose cellular connectivity for about 30 seconds.

## NMEA

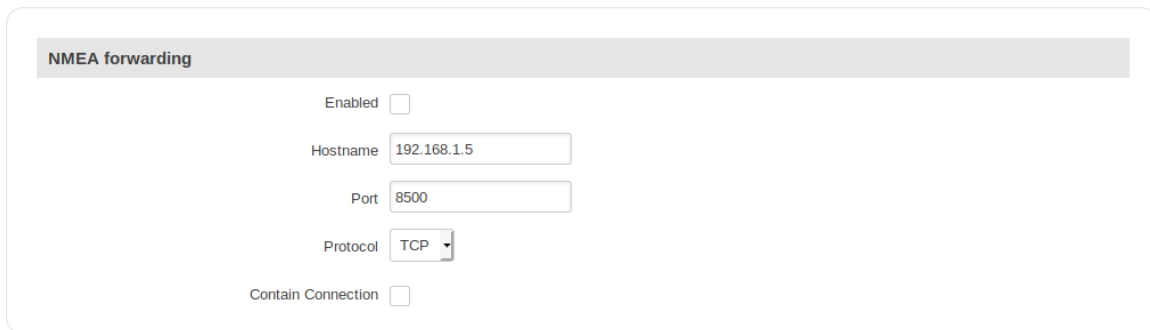
---

The **NMEA** page is used to configure settings related to NMEA sentence collecting and forwarding.

### NMEA forwarding

---

The **NMEA forwarding** section is used to configure and enable NMEA forwarding. The figure below is an example of the NMEA forwarding section and the table below provides information on the fields contained in that section:



Field	Value	Description
<b>Enabled</b>	yes   no; default: <b>no</b>	Turns NMEA forwarding on or off
<b>Hostname</b>	ip   host; default: <b>192.168.1.5</b>	IP address or hostname of the server to which NMEA data will be forwarded
<b>Port</b>	integer [0..65535]; default: <b>8500</b>	Port number off the server to which NMEA data will be forwarded
<b>Protocol</b>	TCP   UDP; default: <b>TCP</b>	Protocol that will be used to send NMEA data
<b>Contain Connection</b>	yes   no; default: <b>no</b>	Contain active session with a remote server

### NMEA forwarding cache

---

The router **caches NMEA forwarding** information if NMEA forwarding is enabled. This section is used to select the memory type where the cache will be stored and the maximum amount of data that will be saved:

Field	Value	Description
<b>Type</b>	ram   flash; default: <b>ram</b>	Selects which type of memory will be used for storing NMEA forwarding cache.
<b>Maximum sentences</b>	integer; default: <b>5000</b>	Maximum amount of NMEA sentences that will be saved in the cache before older entries are deleted and replaced by new ones.
<b>File</b>	filepath; default: <b>none</b>	Location of the file where NMEA forwarding cache information will be stored. This field becomes visible only when the selected memory type is "flash".

## NMEA collecting

The **NMEA collecting** section is used to enable NMEA sentence gathering and storing. The figure below is an example of the NMEA collecting section and the table below provides information on the fields contained in that section:

Field	Value	Description
<b>Enabled</b>	yes   no; default: <b>no</b>	Turns NMEA sentence collecting on or off.
<b>Location</b>	filepath; default: <b>none</b>	Location of the file where NMEA sentences will be stored. This field becomes visible only when NMEA collecting is enabled.

## NMEA sentence settings

The **NMEA sentence settings** section provides the possibility to configure which NMEA sentences will be forwarded or collected and at what frequency. The figure below is an example of the NMEA sentence settings section and the table below provides information on the fields contained in that section:

NMEA sentence settings				
	Forwarding enabled	Forwarding interval	Collecting enabled	Collecting interval
GPGSV	<input type="checkbox"/>	5	<input type="checkbox"/>	5
GPGGA	<input type="checkbox"/>	5	<input type="checkbox"/>	5
GPVTG	<input type="checkbox"/>	5	<input type="checkbox"/>	5
GPRMC	<input type="checkbox"/>	5	<input type="checkbox"/>	5
GPGSA	<input type="checkbox"/>	5	<input type="checkbox"/>	5
GLGSV	<input type="checkbox"/>	5	<input type="checkbox"/>	5
GNGSA	<input type="checkbox"/>	5	<input type="checkbox"/>	5
GNGNS	<input type="checkbox"/>	5	<input type="checkbox"/>	5
GAGSV	<input type="checkbox"/>	5	<input type="checkbox"/>	5
PQGSV	<input type="checkbox"/>	5	<input type="checkbox"/>	5
PQGSA	<input type="checkbox"/>	5	<input type="checkbox"/>	5

Field	Value	Description
<b>Forwarding enabled</b>	yes   no; default: <b>no</b>	Enables forwarding for the adjacent NMEA sentence.
<b>Forwarding interval</b>	integer; default: <b>5</b>	NMEA sentence forwarding frequency in seconds.
<b>Collecting enabled</b>	yes   no; default: <b>no</b>	Enables collecting for the adjacent NMEA sentence.
<b>Collecting interval</b>	integer; default: <b>5</b>	NMEA sentence collecting frequency in seconds.

### NMEA sentence reference table:

NMEA sentence name	Description
<b>GPGSV</b>	Number of GPS satellites in view.
<b>GPGGA</b>	GPS fix data.
<b>GPVTG</b>	Track made good and speed relative to the ground.
<b>GPRMC</b>	Recommended minimum specific GPS/Transit data.
<b>GPGSA</b>	GPS DOP and active satellites.
<b>GLGSA</b>	GLONASS DOP and active satellites.
<b>GLGSV</b>	Number of GLONASS satellites in view.
<b>GNGNS</b>	GNSS position fix from more than one constellation (e.g., GPS + GLONASS).
<b>GAGSV</b>	Number of Galileo satellites in view.
<b>PQGSV</b>	Detailed satellite data (used in BeiDou sentences).
<b>PQGSA</b>	Overall satellite data (used in BeiDou sentences).

## GPS Geofencing

---

A **geofence** is a virtually defined boundary for a real-world geographic area. The GPS Geofencing page provides you with the possibility to set this custom area and apply rules that will inform you when the device leaves or enters the geofence.

**GPS Geofencing**

Geofencing

Name	Status	Longitude (X)	Latitude (Y)	Radius	Generate event on
There are no geofencing configurations yet					

1. Add new geofence

demo Add

2. Configure geofence

Geofencing details

Enable

Longitude (X) 23.964898

Latitude (Y) 54.898095

Radius 200

Generate event on Exit

Get current coordinates Get

3. Manage geofences

demo Disabled 0.000000 0.000000 200 Exit Edit Delete

Add

The figure below is an example of GPS Geofencing configuration and the table below provides information related to that configuration:

**Geofencing details**

Enable

Longitude (X) 23.964898

Latitude (Y) 54.898095

Radius 200

Generate event on Exit

Get current coordinates Get

\* To receive SMS or email when entering or leaving geofence zone, go to Events reporting page and configure GPS event type.  
 \* Geofencing circle shown in map is for a reference and it might not represent real coordinates.

Field	Value	Description
Enable	yes   no; default: <b>no</b>	Turns the Geofence rule on or off

<b>Longitude (X)</b>	degrees [-180.000000..180.000000]; default: <b>0.000000</b>	East-west position of a point on the Earth's surface. Combining this and the Latitude information will produce a point on the world map that will serve as the center of the geofence area.
<b>Latitude (Y)</b>	degrees [-90.000000..90.000000]; default: <b>0.000000</b>	North-south position of a point on the Earth's surface. Combining this and the Longitude information will produce a point on the world map that will serve as the center of the geofence area.
<b>Radius</b>	integer [1..999999]; default: <b>200</b>	Radius (in meters) of the geofence area.
<b>Generate event on</b>	Exit   Enter   Enter/exit; default: <b>Exit</b>	Specifies whether the rule should be triggered when the device enters the geofence area, leaves it or on both events.
<b>Get current coordinates</b>	- (interactive button)	Obtains the device's current coordinates and places them in the Longitude and Latitude fields.

# Hotspot

## Summary

---

Wireless **Hotspots** are essentially Wireless Access Points - they provide network and/or internet access to other Wi-Fi devices. The difference is that Hotspots are a lot more versatile when it comes to managing, monitoring and authenticating the wireless network's users. For example, while Wireless APs can be password protected, with Hotspots you can configure different users with different names, passwords, even data limits and data speeds and more.

## General

---

The **General** tab is where most of the Hotspot configurations take place. This section will be divided into six sub-sections - one for each **Authentication mode**, since the chosen **Authentication mode** will define how the Hotspot will be configured in general.

## External Radius

---

**External Radius** authentication mode uses an external Radius server, to which you have to provide an address to, instead of using the router's internal Radius server.

## Wireless Hotspot Configuration

### General Settings

Configuration profile

Enable

AP IP

Logout address

Authentication mode

Authentication protocol

Terms of Service

RADIUS server #1

RADIUS server #2

Authentication port

Accounting port

Radius secret key

UAM port

UAM UI port

UAM secret

NAS Identifier

Swap octets

Location name

External landing page

Landing page address

Success URL

HTTPS to landing page redirect

SSL key file  No file selected.

SSL certificate file  No file selected.

Use custom DNS

DNS server 1

DNS server 2

### Field Name

### Value

### Description

**Configuration profile**

Custom | Cloud4wi |  
Hotspotsystem;  
Default: **Custom**

If not set to **Custom**, Configuration profile selections will automatically fill all the fields in accordance with the chosen profile. It also automatically adds an



		exception for the chosen service in the <b>Walled Garden</b> section. Used only with <b>External radius</b> Authentication mode.
<b>Enable</b>	yes   no; Default: <b>no</b>	Toggles Wi-Fi Hotspot ON or OFF
<b>AP IP</b>	ip; Default: <b>192.168.2.254/24</b>	Access Point IP address defines the IP address of your Hotspot's network
<b>Logout address</b>	host   ip; Default: <b>1.1.1.1</b>	An address that can be used by users to logout from the Hotspot session
<b>Authentication mode</b>	External radius   Internal radius   Without radius   Advertisement   MAC auth   SMS OTP; Default: <b>Without radius</b>	Authentication mode defines how users will connect to the Hotspot
<b>Authentication protocol</b>	PAP   CHAP; Default: <b>PAP</b>	Authentication protocol used to authenticate new connections on the Hotspot
<b>Terms of service</b>	yes   no; Default: <b>no</b>	If enabled, users have to agree to the Terms of service before logging in. Custom Terms of service can be defined in the <b>Landing Page</b> section
<b>RADIUS server #1   RADIUS server #2</b>	ip; Default: " "	The IP address of the RADIUS server that is to be used for Authenticating your wireless clients
<b>Authentication port</b>	integer [0..65535]; Default: <b>1812</b>	RADIUS server authentication port
<b>Accounting port</b>	integer [0..65535]; Default: <b>1813</b>	RADIUS server accounting port
<b>Radius secret key</b>	string; Default: " "	The secret key is a password used for authentication with the RADIUS server
<b>UAM port</b>	integer [0..65535]; Default: <b>3990</b>	Port to bind for authenticating clients
<b>UAM UI port</b>	integer [0..65535]; Default: <b>4990</b>	UAM User Interface port

<b>UAM secret</b>	string; Default: " "	Shared secret between the UAM server and the Hotspot
<b>NAS identifier</b>	string; Default: " "	NAS-Identifier is one of the basic RADIUS attributes
<b>Swap octets</b>	yes   no; Default: <b>no</b>	Swaps the meaning of input octets and output as it relates to RADIUS attributes
<b>Location name</b>	string; Default: " "	Custom location name for your Hotspot
<b>External landing page</b>	yes   no; Default: <b>no</b>	Enables the use of an external landing page
<b>Landing page address</b>	string; Default: " "	A custom Hotspot's external landing page
<b>Success URL</b>	string; Default: " "	A custom redirect URL after successful Hotspot login
<b>Protocol</b>	HTTP   HTTPS; Default: <b>HTTP</b>	Connection protocol of your Hotspot
<b>HTTPS to landing page redirect</b>	yes   no; Default: <b>no</b>	Redirects HTTP pages to landing page
<b>SSL key file</b>	.key file; Default: " "	SSL key file used for authentication. This field becomes visible only if <b>HTTPS to landing page redirect</b> is enabled
<b>SSL certificate file</b>	.cert file; Default: " "	SSL certificate file used for authentication. This field becomes visible only if <b>HTTPS to landing page redirect</b> is enabled
<b>Use custom DNS</b>	yes   no; Default: <b>no</b>	Enables the use of custom DNS servers instead of your regular DNS
<b>DNS server 1   DNS server 2</b>	ip; Default: " "	Additional DNS servers that are to be used by the Hotspot. These fields become visible only if <b>Use custom DNS</b> is enabled

## Internal Radius

**Internal Radius** is Authentication mode that uses the router's internal RADIUS server for authentication.

## Wireless Hotspot Configuration

### General Settings

Configuration profile:

Enable:

AP IP:

Logout address:

Authentication mode:

Terms of Service:

External landing page:

Landing page address:

Success URL:

HTTPS to landing page redirect:

SSL key file:  No file selected.

SSL certificate file:  No file selected.

Use custom DNS:

DNS server 1:

DNS server 2:

Field Name	Value	Description
<b>Configuration profile</b>	Custom   Cloud4wi   Hotspotsystem; Default: <b>Custom</b>	If not set to <b>Custom</b> , Configuration profile selections will automatically fill all the fields in accordance with the chosen profile. It also automatically adds an exception for the chosen service in the <b>Walled Garden</b> section. Used only with <b>External radius</b> Authentication mode.
<b>Enable</b>	yes   no; Default: <b>no</b>	Toggles Wi-Fi Hotspot ON or OFF
<b>AP IP</b>	ip; Default: <b>192.168.2.254/24</b>	Access Point IP address defines the IP address of your Hotspot's network
<b>Logout address</b>	host   ip; Default: <b>1.1.1.1</b>	An address that can be used by users to logout from the Hotspot session
<b>Authentication mode</b>	External radius   Internal radius   Without radius   Advertisement   MAC auth   SMS OTP; Default: <b>Without radius</b>	Authentication mode defines how users will connect to the Hotspot
<b>Terms of service</b>	yes   no; Default: <b>no</b>	If enabled, users have to agree to the Terms of service before logging in.

<b>External landing page</b>	yes   no; Default: <b>no</b>	Custom Terms of service can be defined in the <b>Landing Page</b> section
<b>Landing page address</b>	string; Default: " "	Enables the use of an external landing page
<b>Success URL</b>	string; Default: " "	A custom Hotspot's external landing page
<b>HTTPS to landing page redirect</b>	yes   no; Default: <b>no</b>	A custom redirect URL after successful Hotspot login
<b>SSL key file</b>	.key file; Default: " "	Redirects HTTP pages to landing page
<b>SSL certificate file</b>	.crt file; Default: " "	SSL key file used for authentication. This field becomes visible only if <b>HTTPS to landing page redirect</b> is enabled
<b>Use custom DNS</b>	yes   no; Default: <b>no</b>	SSL certificate file used for authentication. This field becomes visible only if <b>HTTPS to landing page redirect</b> is enabled
<b>DNS server 1   DNS server 2</b>	ip; Default: " "	Enables the use of custom DNS servers instead of your regular DNS
		Additional DNS servers that are to be used by the Hotspot. These fields become visible only if <b>Use custom DNS</b> is enabled

## Without Radius

---

**Without Radius** Authentication doesn't use a Radius server to authenticate users connecting to the Hotspot, instead it gives you the possibility to configure different users with different password and session parameters.

## Wireless Hotspot Configuration

### General Settings

Configuration profile

Enable

AP IP

Logout address

Authentication mode

Terms of Service

External landing page

Landing page address

Success URL

HTTPS to landing page redirect

SSL key file  No file selected.

SSL certificate file  No file selected.

Use custom DNS

DNS server 1

DNS server 2

Field Name	Value	Description
<b>Configuration profile</b>	Custom   Cloud4wi   Hotspotsystem; Default: <b>Custom</b>	If not set to <b>Custom</b> , Configuration profile selections will automatically fill all the fields in accordance with the chosen profile. It also automatically adds an exception for the chosen service in the <b>Walled Garden</b> section. Used only with <b>External radius</b> Authentication mode.
<b>Enable</b>	yes   no; Default: <b>no</b>	Toggles Wi-Fi Hotspot ON or OFF
<b>AP IP</b>	ip; Default: <b>192.168.2.254/24</b>	Access Point IP address defines the IP address of your Hotspot's network
<b>Logout address</b>	host   ip; Default: <b>1.1.1.1</b>	An address that can be used by users to logout from the Hotspot session
<b>Authentication mode</b>	External radius   Internal radius   Without radius   Advertisement   MAC auth   SMS OTP; Default: <b>Without radius</b>	Authentication mode defines how users will connect to the Hotspot
<b>Terms of service</b>	yes   no; Default: <b>no</b>	If enabled, users have to agree to the Terms of service before logging in.

<b>External landing page</b>	yes   no; Default: <b>no</b>	Custom Terms of service can be defined in the <b>Landing Page</b> section
<b>Landing page address</b>	string; Default: " "	Enables the use of an external landing page
<b>Success URL</b>	string; Default: " "	A custom Hotspot's external landing page
<b>Protocol</b>	HTTP   HTTPS; Default: <b>HTTP</b>	A custom redirect URL after successful Hotspot login
<b>HTTPS to landing page redirect</b>	yes   no; Default: <b>no</b>	Connection protocol of your Hotspot
<b>SSL key file</b>	.key file; Default: " "	Redirects HTTP pages to landing page
<b>SSL certificate file</b>	.cert file; Default: " "	SSL key file used for authentication. This field becomes visible only if <b>HTTPS to landing page redirect</b> is enabled
<b>Use custom DNS</b>	yes   no; Default: <b>no</b>	SSL certificate file used for authentication. This field becomes visible only if <b>HTTPS to landing page redirect</b> is enabled
<b>DNS server 1   DNS server 2</b>	ip; Default: " "	Enables the use of custom DNS servers instead of your regular DNS
		Additional DNS servers that are to be used by the Hotspot. These fields become visible only if <b>Use custom DNS</b> is enabled

## Users Configuration

The **Users Configuration** tab is used to create new, unique users that can connect to the Hotspot.

The screenshot shows the 'Users Configuration' interface. At the top, there is a header 'Users Configuration'. Below it is a table with columns: User name, Password, Idle timeout, Session timeout, Download bandwidth, Upload bandwidth, and Session template. The table contains one row with the following values: User, password, Unlimited, Unlimited, Unlimited, Unlimited, and unlimited. To the right of the table are 'Edit' and 'Delete' buttons. Below the table is a form with three input fields: 'Username', 'Password', and 'Session Template'. The 'Session Template' dropdown is set to 'unlimited'. To the right of the form is an 'Add' button.

Field Name	Value	Description
<b>Username</b>	string; Default: " "	A custom user name used to authenticate clients connecting to the Hotspot

<b>Password</b>	string; Default: " "	A custom password for the specified user name
<b>Session Template</b>	string; Default: <b>unlimited</b>	Session templates define session settings for different users. The <b>unlimited</b> Session Template is a default template with no restrictions. More on Session Template in the next section

## Session Templates

A **Session Template** is a set of rules that can be prescribed to a Hotspot user. A default template named **unlimited** is present in the router, but it has no configured restrictions. You can edit the default template or you can create a custom template and configure it.

### Hotspot Configuration

**Session Configuration Settings**

Idle timeout

Session timeout

Download bandwidth  Mbit/s ▼

Upload bandwidth  Kbit/s ▼

Download limit

Upload limit

Period  ▼

Start day  ▼

Field Name	Value	Description
<b>Idle timeout</b>	integer; Default: " "	A timeout in seconds after which idle users are automatically disconnected from the Hotspot. 0 means unlimited
<b>Session timeout</b>	integer; Default: " "	A timeout in seconds after users are automatically disconnected from the Hotspot. The timeout countdown begins when a user is authenticated to the Hotspot and, after an amount of time specified in this field, the user gets disconnected from the Hotspot. 0 means unlimited
<b>Download bandwidth</b>	integer; Default: " "	Maximum download bandwidth that the users assigned to this template can achieve. Bandwidth can be specified in Kbit/s, Mbit/s, Gbit/s

<b>Upload bandwidth</b>	integer; Default: " "	Maximum upload bandwidth that the users assigned to this template can achieve. Bandwidth can be specified in Kbit/s, Mbit/s or Gbit/s
<b>Download limit</b>	integer; Default: " "	A received data limit that the users assigned to this template can reach. After the data limit is reached, the user will lose data connection. Download limit is specified in MB
<b>Upload limit</b>	integer; Default: " "	A sent data limit that the users assigned to this template can reach. After the data limit is reached, the user will lose data connection. Upload limit is specified in MB
<b>Period</b>	Month   Week   Day; Default: <b>Month</b>	The beginning of the period during which the restriction specified in this section will apply. After the period is over, all specified limits are reset
<b>Start day   Start hour</b>	integer [1..31]   Monday..Sunday   integer [1..24]; Default: <b>day 1</b>	Specifies which day of the month, week or hour of the day the limits will be reset

## Advertisement

The **Advertisement** Authentication mode doesn't use any kind of actual authentication. Instead when a user connects to the Hotspot he first gets redirected to a specified advertisement page. After that the user is free to use the Hotspot.

### Wireless Hotspot Configuration

General Settings

Configuration profile

Enable

AP IP

Authentication mode

Advertisement address

HTTPS to landing page redirect

SSL key file  No file selected.

SSL certificate file  No file selected.

Use custom DNS

DNS server 1

DNS server 2



Field Name	Value	Description
<b>Configuration profile</b>	Custom   Cloud4wi   Hotspotsystem; Default: <b>Custom</b>	If not set to <b>Custom</b> , Configuration profile selections will automatically fill all the fields in accordance with the chosen profile. It also automatically adds an exception for the chosen service in the <b>Walled Garden</b> section. Used only with <b>External radius</b> Authentication mode.
<b>Enable</b>	yes   no; Default: <b>no</b>	Toggles Wi-Fi Hotspot ON or OFF
<b>AP IP</b>	ip; Default: <b>192.168.2.254/24</b>	Access Point IP address defines the IP address of your Hotspot's network
<b>Authentication mode</b>	External radius   Internal radius   Without radius   Advertisement   MAC auth   SMS OTP; Default: <b>Without radius</b>	Authentication mode defines how users will connect to the Hotspot
<b>Advertisement address</b>	host   ip; Default: " "	The address of the advertisement page that newly connected users will be redirected to
<b>HTTPS to landing page redirect</b>	yes   no; Default: <b>no</b>	Redirects HTTP pages to landing page
<b>SSL key file</b>	.key file; Default: " "	SSL key file used for authentication. This field becomes visible only if <b>HTTPS to landing page redirect</b> is enabled
<b>SSL certificate file</b>	.crt file; Default: " "	SSL certificate file used for authentication. This field becomes visible only if <b>HTTPS to landing page redirect</b> is enabled
<b>Use custom DNS</b>	yes   no; Default: <b>no</b>	Enables the use of custom DNS servers instead of your regular DNS
<b>DNS server 1   DNS server 2</b>	ip; Default: " "	Additional DNS servers that are to be used by the Hotspot. These fields become visible only if <b>Use custom DNS</b> is enabled

# MAC auth

**MAC auth** Authentication mode authenticates users by their MAC address. A list of accepted or unaccepted MAC addresses can be configured in the router's WebUI's Wireless section under Interface Configuration->MAC Filter

## Wireless Hotspot Configuration

**General Settings**

Configuration profile

Enable

AP IP

Logout address

Authentication mode

Terms of Service

Password protection

Password

Website access

Protocol

HTTPS redirect

SSL key file  No file chosen

SSL certificate file  No file chosen

Use custom DNS

DNS server 1

DNS server 2

Field Name	Value	Description
<b>Configuration profile</b>	Custom   Cloud4wi   Hotspotsystem; Default: <b>Custom</b>	If not set to <b>Custom</b> , Configuration profile selections will automatically fill all the fields in accordance with the chosen profile. It also automatically adds an exception for the chosen service in the <b>Walled Garden</b> section. Used only with <b>External radius</b> Authentication mode.
<b>Enable</b>	yes   no; Default: <b>no</b>	Toggles Wi-Fi Hotspot ON or OFF

<b>AP IP</b>	ip; Default: <b>192.168.2.254/24</b>	Access Point IP address defines the IP address of your Hotspot's network
<b>Logout address</b>	host   ip; Default: <b>1.1.1.1</b>	An address that can be used by users to logout from the Hotspot session
<b>Authentication mode</b>	External radius   Internal radius   Without radius   Advertisement   MAC auth   SMS OTP; Default: <b>Without radius</b>	Authentication mode defines how users will connect to the Hotspot
<b>Terms of service</b>	yes   no; Default: <b>no</b>	If enabled, users have to agree to the Terms of service before logging in. Custom Terms of service can be defined in the <b>Landing Page</b> section
<b>Password protection</b>	yes   no; Default: <b>no</b>	Enables Hotspot password protection
<b>Password</b>	string; Default: " "	A password used to authenticate connecting clients to the Hotspot
<b>Website access link</b>	Link   Auto redirect   Custom address; Default: <b>Link</b>	Requested website access mode
<b>Protocol</b>	HTTP   HTTPS; Default: <b>HTTP</b>	Connection protocol of your Hotspot
<b>HTTPS to landing page redirect</b>	yes   no; Default: <b>no</b>	Redirects HTTP pages to landing page
<b>SSL key file</b>	.key file; Default: " "	SSL key file used for authentication. This field becomes visible only if <b>HTTPS to landing page redirect</b> is enabled
<b>SSL certificate file</b>	.crt file; Default: " "	SSL certificate file used for authentication. This field becomes visible only if <b>HTTPS to landing page redirect</b> is enabled
<b>Use custom DNS</b>	yes   no; Default: <b>no</b>	Enables the use of custom DNS servers instead of your regular DNS
<b>DNS server 1   DNS server 2</b>	ip; Default: " "	Additional DNS servers that are to be used by the Hotspot. These fields

become visible only if **Use custom DNS** is enabled

## SMS OTP

With **SMS OTP** Authentication mode connecting users are prompted to enter their phone number. After that, the router sends an SMS message containing a code to the specified number. Users then authenticate themselves to the Hotspot using this code.

### Wireless Hotspot Configuration

**General Settings**

Configuration profile: Custom

Enable:

AP IP: 192.168.2.254/24

Logout address: 1.1.1.1

Authentication mode: SMS OTP

Protocol: HTTP

HTTPS redirect:

SSL key file:  No file chosen

SSL certificate file:  No file chosen

Use custom DNS:

DNS server 1: 8.8.8.8

DNS server 2: 8.8.4.4

Field Name	Value	Description
<b>Configuration profile</b>	Custom   Cloud4wi   Hotspotsystem; Default: <b>Custom</b>	If not set to <b>Custom</b> , Configuration profile selections will automatically fill all the fields in accordance with the chosen profile. It also automatically adds an exception for the chosen service in the <b>Walled Garden</b> section. Used only with <b>External radius</b> Authentication mode.
<b>Enable</b>	yes   no; Default: <b>no</b>	Toggles Wi-Fi Hotspot ON or OFF
<b>AP IP</b>	ip; Default: <b>192.168.2.254/24</b>	Access Point IP address defines the IP address of your Hotspot's network

<b>Authentication mode</b>	External radius   Internal radius   Without radius   Advertisement   MAC auth   SMS OTP; Default: <b>Without radius</b>	Authentication mode defines how users will connect to the Hotspot
<b>Protocol</b>	HTTP   HTTPS; Default: <b>HTTP</b>	Connection protocol of your Hotspot
<b>HTTPS to landing page redirect</b>	yes   no; Default: <b>no</b>	Redirects HTTP pages to landing page
<b>SSL key file</b>	.key file; Default: " "	SSL key file used for authentication. This field becomes visible only if <b>HTTPS to landing page redirect</b> is enabled
<b>SSL certificate file</b>	.crt file; Default: " "	SSL certificate file used for authentication. This field becomes visible only if <b>HTTPS to landing page redirect</b> is enabled
<b>Use custom DNS</b>	yes   no; Default: <b>no</b>	Enables the use of custom DNS servers instead of your regular DNS
<b>DNS server 1   DNS server 2</b>	ip; Default: " "	Additional DNS servers that are to be used by the Hotspot. These fields become visible only if <b>Use custom DNS</b> is enabled

## Restricted Internet Access

---

The **Restricted Internet Access** page provides you with the possibility to restrict internet access on Hotspot on specified hours. Blue squares represent restricted access, white squares - allowed access. Below is an example of a configuration that restricts internet access outside of working hours.

## Internet Access Restriction Settings

Select Time To Restrict Access On Hotspot HAL9000

Days/Hours	0-1h	1-2h	2-3h	3-4h	4-5h	5-6h	6-7h	7-8h	8-9h	9-10h	10-11h	11-12h	12-13h	13-14h	14-15h	15-16h	16-17h	17-18h	18-19h	19-20h	20-21h	21-22h	22-23h	23-24h
Monday																								
Tuesday																								
Wednesday																								
Thursday																								
Friday																								
Saturday																								
Sunday																								

Internet access allowed  
 Internet access blocked

## Logging

The Hotspot **Logging** section is used to send Hotspot or Wireless information to an FTP or Syslog server.

### Wireless Hotspot Logging Settings

Logging Settings

Enable

Field Name	Value	Description
<b>Enable</b>	yes   no; Default: <b>no</b>	Enables or disables whole logging section's functionality

Syslog Server Settings

Enable

Server address

Port

Protocol

Prefix text

Protocol filter

Port filter

Field Name	Value	Description
<b>Enable</b>	yes   no; Default: <b>no</b>	Toggles logging to Syslog ON or OFF
<b>Server address</b>	host   ip; Default: " "	Syslog server address
<b>Port</b>	integer [0..65535]; Default: " "	Syslog server port
<b>Protocol</b>	UDP TCP Default: <b>TCP</b>	Protocol of the syslog server
<b>Prefix text</b>	string; Default: " "	Prefix custom text to streamed messages

<b>Protocol filter</b>	UDP TCP Any; Default: <b>Any</b>	Filter log messages depending on protocol
<b>Port filter</b>	integer [0..65535]; Default: " "	Filter log messages depending on port of port range

**FTP Server Settings**

Enable

Server address

User name

Password

Port

File name extras

Field Name	Value	Description
<b>Enable</b>	yes   no; Default: <b>no</b>	Toggles logging to FTP ON or OFF
<b>Server address</b>	host   ip; Default: <b>your.ftp.server</b>	FTP server address.
<b>User name</b>	string; Default: <b>username</b>	User name used for authentication when logging into an FTP server
<b>Password</b>	string; Default: <b>password</b>	Password used for authentication when logging into an FTP server
<b>Port</b>	integer [0..65535]; Default: <b>21</b>	FTP server port
<b>File name extras</b>	No extra information   MAC address   Serial number   Custom string; Default: <b>No extra information</b>	Extra information to be added to the log filename

## FTP Upload Settings

Here you can configure your timing settings for the log upload via FTP feature.

## FTP Upload Settings

You can configure your timing settings for the log upload via FTP feature here.

Mode

Hours

Minutes

Days  Monday  
 Tuesday  
 Wednesday  
 Thursday  
 Friday  
 Saturday  
 Sunday

Field Name	Value	Description
<b>Mode</b>	Fixed   Interval; Default: <b>Fixed</b>	The scheduling mode to be used for uploading to FTP server
<b>Hours</b>	time; Default: <b>8 hours</b>	Time interval when the uploads will take place
<b>Minutes</b>	time;Default: <b>15 minutes</b>	Time interval when the uploads will take place
<b>Days</b>	time;Default: <b>Monday, Tuesday, Wednesday, Thursday, Friday</b>	On which day upload will take place

## Wifi Log/SMS OTP Log

WiFi and SMS OTP logs show information about connections to your WiFi Hotspot. FTP logging has to be enabled.

[Configuration](#) [Log](#) [SMS OTP Log](#)

### Wifi Log

MAC	IP	Port	Date	Time
.....	.....	443	2020-Feb-25	13:15:13
.....	.....	443	2020-Feb-25	13:15:16



## SMS OTP Log

SMS OTP Log	
Events per page	10 <input type="text"/>
Search <input type="text"/>	
Tel. Number <span>⬆</span>	Password <span>⬆</span>
<input type="text"/>	9935

## Landing Page

This section is used to define how your Hotspot's Landing Page will look like.

### Wireless Hotspot Landing Settings

Landing Page Settings	
Page title	<input type="text" value="Teltonika Hotspot"/>
Theme	<input type="text" value="Custom"/>
Upload login page	<input type="button" value="Choose File"/> No file chosen
Login page file	<input type="button" value="Download"/>
<input type="button" value="Demo preview"/>	
<input type="checkbox"/> Terms Of Services	
<input type="checkbox"/> Background Configuration	
<input type="checkbox"/> Logo Image Configuration	
<input type="checkbox"/> Link Configuration	
<input type="checkbox"/> Text Configuration	
<input type="checkbox"/> Button Configuration	
<input type="checkbox"/> Input Configuration	

## Radius Server

This section is used to configure your **Radius Server** for use with **Internal radius** Authentication mode.

### Radius Server Configuration

General Settings	
Enable	<input type="checkbox"/>
Remote access	<input type="checkbox"/>
Accounting port	<input type="text" value="1813"/>
Authentication port	<input type="text" value="1812"/>

Field Name	Value	Description
<b>Enable</b>	yes   no; Default: <b>no</b>	Toggles Radius Server ON or OFF
<b>Remote access</b>	yes   no; Default: <b>no</b>	Toggles remote access to the Radius Server ON or OFF.
<b>Accounting port</b>	integer [0..65535]; Default: <b>1813</b>	Radius server accounting port
<b>Authentication port</b>	integer [0..65535]; Default: <b>1812</b>	Radius server authentication port

## Session Settings

A **Session Template** is a set of rules that can be prescribed to a Hotspot user. A default template named **unlimited** is present in the router, but it has no configured restriction. You can edit the default template or you can create a custom template and configure it.

### Hotspot Configuration

**Session Configuration Settings**

Idle timeout

Session timeout

Download bandwidth  Mbit/s ▼

Upload bandwidth  Kbit/s ▼

Download limit

Upload limit

Period  ▼

Start day  ▼

Field Name	Value	Description
<b>Idle timeout</b>	integer; Default: " "	A timeout in seconds after which idle users are automatically disconnected from the Hotspot. 0 means unlimited
<b>Session timeout</b>	integer; Default: " "	A timeout in seconds after users are automatically disconnected from the Hotspot. The timeout countdown begins when a user is authenticated to the Hotspot and, after an amount of time specified in this

		field, the user gets disconnected from the Hotspot. 0 means unlimited
<b>Download bandwidth</b>	integer; Default: " "	Maximum download bandwidth that the users assigned to this template can achieve. Bandwidth can be specified in Kbit/s, Mbit/s or Gbit/s
<b>Upload bandwidth</b>	integer; Default: " "	Maximum upload bandwidth that the users assigned to this template can achieve. Bandwidth can be specified in Kbit/s, Mbit/s or Gbit/s
<b>Download limit</b>	integer; Default: " "	A received data limit that the users assigned to this template can reach. After the data limit is reached, the user will lose data connection. Download limit is specified in MB
<b>Upload limit</b>	integer; Default: " "	A sent data limit that the users assigned to this template can reach. After the data limit is reached, the user will lose data connection. Upload limit is specified in MB
<b>Period</b>	Month   Week   Day; Default: <b>Month</b>	The beginning of the period during which the restriction specified in this section will apply. After the period is over, all specified limits are reset
<b>Start day   Start hour</b>	integer [1..31]   Monday..Sunday   integer [1..24]; Default: <b>day 1</b>	Specifies which day of the month, week or hour of the day the limits will be reset

## Users Configuration Settings

---

The **Users Configuration** tab is used to create new, unique users that can connect to the Hotspot.

**Users Configuration**

User name	Password	Idle timeout	Session timeout	Download bandwidth	Upload bandwidth	Session template	
User	password	Unlimited	Unlimited	Unlimited	Unlimited	unlimited	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Username	Password	Session Template	
<input type="text"/>	<input type="text"/>	unlimited	<input type="button" value="Add"/>

Field Name	Value	Description
<b>Username</b>	string; Default: " "	A custom user name used to authenticate clients connecting to the Hotspot
<b>Password</b>	string; Default: " "	A custom password for the specified user name
<b>Session Template</b>	string; Default: <b>unlimited</b>	Session templates define session settings for different users. The <b>unlimited</b> Session Template is a default template with no restrictions. More on Session Template in the next section

## Clients Configuration Settings

**Clients Configuration Settings**

Enable	Client name	IP address	Netmask	Radius shared secret	
<input checked="" type="checkbox"/>	<input type="text" value="Client1"/>	<input type="text" value="192.168.56.124"/>	<input type="text" value="24"/>	<input type="text" value="secret_code"/>	<input type="button" value="Delete"/>

Field Name	Value	Description
<b>Enable</b>	yes   no; Default: <b>yes</b>	Toggles Clients Configuration ON or OFF
<b>Client name</b>	string; Default: " "	A custom user name used to authenticate clients connecting to the Hotspot
<b>IP address</b>	ip; Default: " "	The IP address of the client
<b>Netmask</b>	integer [0..32]; Default: " "	The netmask of the client
<b>Radius shared secret</b>	string; Default: " "	Radius shared secret used for communication between the client/NAS and the radius server

## Statistics

The **Statistics** page shows statistics about connections to the hotspot. **Reminder: Statistics page becomes visible only when device is connected to the hotspot.**

## Hotspot Statistics


Hotspot statistics								
Events per page		10	Search					
Username	IP	MAC	Start time	End time	Use time	Download	Upload	Clean
user1	192.168.2.1	D8-C7-71-47-90-E1	2017-10-17 13:49:48	2017-10-17 13:49:55	00:00:09	36.13 KB	19.76 KB	Clean

Showing 1 to 1 of 1 entries

## Manage

With the help of the **Manage** page you manage the users that are connected to your Hotspot. To reach the **Manage** window, go to Services->Hotspot. The **Manage** button will be located next to your Hotspot instance.

### Hotspot Configuration


 **Hotspot Instances**

Enabled: Yes  
Auth Mode: Without RADIUS

SSID: HAL9000  
IP: 192.168.2.254/24

[Disable](#) [Edit](#) [Manage](#)

### Clients Management

 **Hotspot Clients**

Logged in: Yes  
URL: http://h.fb.com/?cid...

IP Address: 192.168.2.1  
MAC Address: D8-C7-71-47-90-E1

Idle / Max: 0/- sec.  
Duration / Max: 6/- sec.

Download: 17.90 KB  
Upload: 9.69 KB

[Logout](#)

### Realtime Traffic



(3 minutes window, 3 seconds interval)

**Inbound:** 16.99 Kbits/s  
(2.12 KBytes/s)

**Average:** 23.64 Kbits/s  
(2.96 KBytes/s)

**Peak:** 71.55 Kbits/s  
(8.94 KBytes/s)

**Outbound:** 58.8 Kbits/s  
(7.35 KBytes/s)

**Average:** 56.37 Kbits/s  
(7.05 KBytes/s)

**Peak:** 738.48 Kbits/s  
(92.31 KBytes/s)

# Modbus

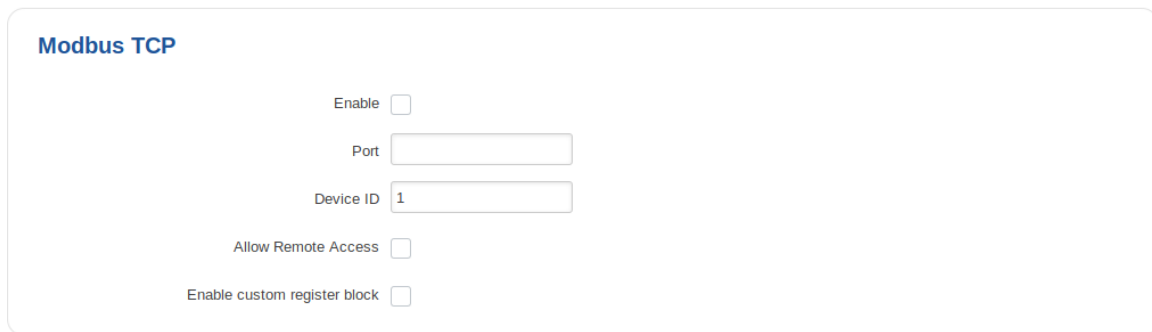
## Summary

**Modbus** is a serial communications protocol. Simple and robust, it has become a de facto standard communication protocol and is now a commonly available means of connecting industrial electronic devices.

## Modbus TCP

**Modbus TCP** provides users with the possibility to set or get system parameters. The Modbus daemon acts as slave device. That means it accepts connections from a master (client) and sends out a response or sets some system related parameter in accordance with the given query.

The figure below is an example of the Modbus TCP window section and the table below provides information on the fields contained in that window:



Modbus TCP

Enable

Port

Device ID

Allow Remote Access

Enable custom register block

Field	Value	Description
<b>Enable</b>	yes   no; default: <b>none</b>	Turns Modbus TCP on or off.
<b>Port</b>	integer [0..65535]; default: <b>502</b>	TCP port used for Modbus communications.
<b>Device ID</b>	integer [0..255]; default: <b>1</b>	The device's Modbus slave ID. When set to 0, it will respond to requests addressed to any ID.
<b>Allow Remote Access</b>	yes   no; default: <b>no</b>	Allows remote Modbus connections by adding an exception to the device's firewall on the port specified in the field above.
<b>Enable custom register block</b>	yes   no; default: <b>no</b>	Allow custom register block

## Get Parameters

---

Modbus parameters are held within **registers**. Each register contains 2 bytes of information. For simplification, the number of registers for storing numbers is 2 (4 bytes), while the number of registers for storing text information is 16 (32 bytes). The register numbers and corresponding system values are described in the table below:

Required Value	Register Address	Register Number	Number Of Registers	Representation
<b>System uptime</b>	1	2	2	32 bit unsigned integer
<b>Mobile signal strength (RSSI in dBm)</b>	3	4	2	32 bit integer
<b>System temperature (in 0.1 °C)</b>	5	6	2	32 bit integer
<b>System hostname</b>	7	8	16	Text
<b>GSM operator name</b>	23	24	16	Text
<b>Router serial number</b>	39	40	16	Text
<b>LAN MAC address</b>	55	56	16	Text
<b>Router name</b>	71	72	16	Text
<b>Currently active SIM card slot</b>	87	88	16	Text
<b>Network registration info</b>	103	104	16	Text
<b>Network type</b>	119	120	16	Text
<b>Digital input (DIN1) state</b>	135	136	2	32 bit integer
<b>Digital galvanically isolated input (DIN2) state</b>	137	138	2	32 bit integer
<b>Current WAN IP address</b>	139	140	2	32 bit unsigned integer
<b>Analog input value</b>	141	142	2	32 bit integer
<b>GPS latitude coordinate</b>	143	144	2	32 bit float
<b>GPS longitude coordinate</b>	145	146	2	32 bit float

<b>GPS fix time</b>	147	148	16	Text (Unix timestamp×1000)
<b>GPS date and time</b>	163	164	16	Text (DDMMYYhhmmss)
<b>GPS speed</b>	179	180	2	32 bit integer
<b>GPS satellite count</b>	181	182	2	32 bit integer
<b>GPS accuracy</b>	183	184	2	32 bit float
<b>Mobile data received today (SIM1)</b>	185	186	2	32 bit unsigned integer
<b>Mobile data sent today (SIM1)</b>	187	188	2	32 bit unsigned integer
<b>Mobile data received this week (SIM1)</b>	189	190	2	32 bit unsigned integer
<b>Mobile data sent this week (SIM1)</b>	191	192	2	32 bit unsigned integer
<b>Mobile data received this month (SIM1)</b>	193	194	2	32 bit unsigned integer
<b>Mobile data sent this month (SIM1)</b>	195	196	2	32 bit unsigned integer
<b>Mobile data received last 24h (SIM1)</b>	197	198	2	32 bit unsigned integer
<b>Mobile data sent last 24h (SIM1)</b>	199	200	2	32 bit unsigned integer
<b>Galvanically isolated open collector output status</b>	201	202	1	32 bit unsigned integer
<b>Relay output status</b>	202	203	1	32 bit unsigned integer
<b>Active SIM card</b>	205	206	1	32 bit unsigned integer
<b>Mobile data received last week (SIM1)</b>	292	293	2	32 bit unsigned integer



<b>Mobile data sent last week (SIM1)</b>	294	295	2	32 bit unsigned integer
<b>Mobile data received last month (SIM1)</b>	296	297	2	32 bit unsigned integer
<b>Mobile data sent last month (SIM1)</b>	298	299	2	32 bit unsigned integer
<b>Mobile data received today (SIM2)</b>	300	301	2	32 bit unsigned integer
<b>Mobile data sent today (SIM2)</b>	302	303	2	32 bit unsigned integer
<b>Mobile data received this week (SIM2)</b>	304	305	2	32 bit unsigned integer
<b>Mobile data sent this week (SIM2)</b>	306	307	2	32 bit unsigned integer
<b>Mobile data received this month (SIM2)</b>	308	309	2	32 bit unsigned integer
<b>Mobile data sent this month (SIM2)</b>	310	311	2	32 bit unsigned integer
<b>Mobile data received last 24h (SIM2)</b>	312	313	2	32 bit unsigned integer
<b>Mobile data sent last 24h (SIM2)</b>	314	315	2	32 bit unsigned integer
<b>Mobile data received last week (SIM2)</b>	316	317	2	32 bit unsigned integer
<b>Mobile data sent last week (SIM2)</b>	318	319	2	32 bit unsigned integer
<b>Mobile data received last month(SIM2)</b>	320	321	2	32 bit unsigned integer
<b>Mobile data sent last month (SIM2)</b>	322	323	2	32 bit unsigned integer
<b>Digital non-isolated input (4 PIN connector)</b>	324	325	1	32 bit unsigned integer

<b>Digital open collector output (4 PIN connector)</b>	325	326	1	32 bit unsigned integer
--	-----	-----	---	-------------------------

## Set Parameters

---

The Modbus daemon can also set some device parameters. These parameters and explanations on how to use them are described in the table below:

Value To Set	Register Address	Register Value	Description
<b>Digital output 1 (DOUT1) (ON/OFF*)</b>	201	1   0	Changes the state of the open collector (OC) output
<b>Digital output 2 (DOUT2) (ON/OFF*)</b>	202	1   0	Changes the state of the relay output
<b>Switch WiFi (ON/OFF*)</b>	203	1   0	Turns WiFi ON or OFF
<b>Switch mobile data connection (ON/OFF*)</b>	204	1   0	Turns mobile data connection ON or OFF
<b>Switch SIM card</b>	205	1   2   0	Changes the active SIM card slot <ul style="list-style-type: none"> <li>• 1 - switch to SIM1</li> <li>• 2 - switch to SIM2</li> <li>• 0 - switch from the the SIM card opposite of the one currently in use (SIM1 → SIM2 or SIM2 → SIM1)</li> </ul>
<b>Reboot</b>	206	1	Reboots the router
<b>Change APN</b>	207	APN code	Changes APN. The number of input registers may vary depending on the length of the APN, but the very first byte of the set APN command denotes the number of the SIM card for which to set the APN. This byte should be set to: <ul style="list-style-type: none"> <li>• 1 - to set APN for SIM1</li> <li>• 2 - to set APN for SIM2</li> </ul>

\* All ON/OFF commands only accept **0** and **1** values, which represent the following:

- 1 - ON
- 0 - OFF

## Modbus TCP Master

A Modbus **master** device can request data from Modbus slaves. The Modbus TCP Master section is used to configure Modbus TCP slaves. To add a new slave, enter a custom name, slave's ID, IP address and port and click the "Add" button:

**Modbus TCP Master**  
Modbus TCP master periodically sends modbus requests to modbus slave devices. Data collected from TCP slaves is stored and periodically sent to remote server

**Modbus TCP slave devices**

Name	ID	IP address	Period	Timeout	Enabled	
slave1	1	192.168.1.101	N/A	N/A	<input type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Alarms"/> <input type="button" value="Clone"/>

**New slave device**

Name	Slave ID	IP address	Port	
<input type="text" value="slave1"/>	<input type="text" value="1"/>	<input type="text" value="192.168.1.101"/>	<input type="text" value="503"/>	<input type="button" value="Add"/>

Button	Description
<b>Edit</b>	Redirects you to the slave's configuration page
<b>Delete</b>	Deletes the slave configuration
<b>Alarms</b>	Redirects you to the slave's alarm configuration page
<b>Clone</b>	Creates an identical slave configuration

You can create a maximum of 10 slave configurations.

## Slave device configuration

The figure below is an example of the **Slave device configuration** and the table below provides information on the fields contained in that section:

## Advanced device settings

Here you can add and configure request parameters and alarms for this TCP slave device

### Slave device configuration

Enabled

Name

Slave ID

IP address

Port

Period

Timeout

Field	Value	Description
<b>Enabled</b>	yes   no; default: <b>no</b>	Turns communication with the slave device on or off.
<b>Name</b>	string; default: <b>none</b>	Slave device's name, used for easier management purposes.
<b>Slave ID</b>	integer [0..255]; default: <b>none</b>	Slave ID. Each slave in a network is assigned a unique identifier ranging from 1 to 255. When the master requests data from a slave, the first byte it sends is the Slave ID. When set to 0, the slave will respond to requests addressed to any ID.
<b>IP address</b>	ip; default: <b>none</b>	Slave device's IP address.
<b>Port</b>	integer [0..65535]; default: <b>none</b>	Slave device's Modbus TCP port.
<b>Period</b>	integer [1..6400]; default: <b>none</b>	Interval at which requests are sent to the slave device.
<b>Timeout</b>	integer [1..30]; default: <b>none</b>	Maximum response wait time.

## Requests configuration

A Modbus **request** is a way of obtaining data from Modbus slaves. The master sends a request to a slave specifying the function code to be performed. The slave then sends the requested data back to the Modbus master. You can create a maximum of 64 request configurations for each slave device.

The figure below is an example of the Requests configuration section and the table below provides information contained in the fields of that section:

Name	Data type	Function	First Register	Number of Registers	Enabled
Unnamed Parameter	16bit INT, high byte first	3	1	1	<input type="checkbox"/>

Add

Field	Value	Description
<b>Name</b>	string; default: <b>Unnamed Parameter</b>	Request name. Used for easier management purposes.
<b>Data type</b>	8bit INT   8bit UINT   16bit INT, high byte first   16bit INT, low byte first   16bit UINT, high byte first   16bit UINT, low byte first   32bit float, Byte order 1,2,3,4   32bit float, Byte order 4,3,2,1   32bit float, Byte order 2,1,4,3   32bit float, Byte order 3,4,1,2; default: <b>16bit INT, high byte first</b>	How read data will be stored.
<b>Function</b>	1   2   3   4   5   6   15   16; default: <b>3</b>	A function code specifies the type of register being addressed by a Modbus request. The codes represent these functions: <ul style="list-style-type: none"> <li>• <b>1</b> - read Coil Status</li> <li>• <b>2</b> - read Input Status</li> <li>• <b>3</b> - read Holding Registers</li> <li>• <b>4</b> - read Input Registers</li> <li>• <b>5</b> - force Single Coil</li> <li>• <b>6</b> - preset Single Register</li> <li>• <b>15</b> - force Multiple Coils</li> <li>• <b>16</b> - force Multiple Registers</li> </ul>
<b>First Register</b>	integer [1..65536]; default: <b>1</b>	First Modbus register number from which data will be read. numbers, which value is +1 higher than address value.

<b>Number of Registers</b>	integer [1..2000]; default: <b>none</b>	Number of Modbus registers that will be read during the request.
<b>Enabled</b>	yes   no; default: <b>no</b>	Turns the request on or off.
<b>Test</b>	- (interactive button)	Generates a Modbus request according to given parameters in order to test the request configuration. You must first save the configuration before you can use the Test button.
<b>Delete</b>	- (interactive button)	Deletes the request.
<b>Add</b>	- (interactive button)	Adds a new request configuration.

## Alarm configuration

**Alarms** are a way of setting up automated actions when some Modbus values meet user specified conditions. The figure below is an example of the Alarm configuration page and the table below provides information on fields that it contains:

### Alarm Configuration

Alarm settings

Enabled

Function Code Read Coil Status (1)

Register

Condition Equal to

Value

Action SMS

Message

Phone number  +

Field	Value	Description
<b>Enabled</b>	yes   no; default: <b>no</b>	Turns the alarm on or off
<b>Function code</b>	Read Coil Status (1)   Read Input Status (2)   Read Holding Registers (3)   Read Input	Modbus function used in Modbus request.

	Registers (4); default: <b>Read Coil Status (1)</b>	
<b>Register</b>	integer [0..65535]; default: <b>none</b>	Number of the Modbus coil/input/holding register/input register that will be read.
<b>Condition</b>	More than   Less than   Equal to   Not Equal to; default: <b>Equal to</b>	When a value is obtained it will be compared against the value specified in the following field. The comparison will be made in accordance with the condition specified in this field.
<b>Value</b>	various; default: <b>none</b>	The value against which the read data will be compared.
<b>Action</b>	SMS   Trigger output   Modbus Request; default: <b>SMS</b>	Action that will be taken if the condition is met. Possible actions: <ul style="list-style-type: none"> <li>• <b>SMS</b> - sends and SMS message to a specified recipient(s).</li> <li>• <b>Trigger output</b> - changes the state of a specified output(s).</li> <li>• <b>Modbus Request</b> - sends a Modbus request to a specified slave.</li> </ul>
<b>SMS: Message</b>	string; default: <b>none</b>	SMS message text.
<b>SMS: Phone number</b>	phone number; default: <b>none</b>	Recipient's phone number.
<b>Trigger output: Output</b>	Open collector output   Relay output   Both; default: <b>Open collector output</b>	Which output(s) will be triggered.
<b>Trigger output: I/O Action</b>	Turn On   Turn Off   Invert; default: <b>Turn On</b>	Action that will taken on the specified output.
<b>Modbus Request: IP address</b>	ip   host; default: <b>none</b>	Modbus slave's IP address.
<b>Modbus Request: Port</b>	integer [0..65535]; default: <b>none</b>	Modbus slave's port.
<b>Modbus Request: Timeout</b>	integer [1..30]; default: <b>5</b>	Maximum time to wait for a response.

<b>Modbus Request ID</b>	integer [1..255]; default: <b>none</b>	Modbus slave ID.
<b>Modbus Request: Modbus function</b>	Read Coil Status (1)   Read Input Status (2)   Read Holding Registers (3)   Read Input Registers (4)   Force Single Coil (5)   Preset Single Register (6)   Force Multiple Coils (15)   Force Multiple Registers (16); default: <b>Force Single Coil (5)</b>	A function code specifies the type of register being addressed by a Modbus request.
<b>Modbus Request: First register</b>	integer [0..65535]; default: <b>none</b>	Begins reading from the register specified in this field.
<b>Modbus Request: Number of registers</b>	integer [0..65535]; default: <b>none</b>	The number of registers that will be read from the first register.

## Modbus Serial Master

---

The **Modbus Serial Master** page is used to configure the router as a Modbus RTU master. Modbus RTU (remote terminal unit) is a serial communication protocol mainly used in communication via RS232 or RS485 serial interfaces.

### RS232

---

This section is used to configure the Modbus RTU master's RS232 serial interface settings. Refer to the figure and table below for information on RS232 configuration.



## RS232

### RS232 configuration

Enabled

Baud rate 19200 ▾

Data bits 8 ▾

Parity Even ▾

Stop bits 1 ▾

Flow control None ▾

Field	Value	Description
<b>Enabled</b>	yes   no; default: <b>no</b>	Turns Modbus RTU via RS232 on or off.
<b>Baud rate</b>	300   1200   2400   4800   9600   19200   38400   57600   115200; default: <b>19200</b>	Serial data transmission rate (in bits per second).
<b>Data bits</b>	5   6   7   8; default: <b>8</b>	Number of data bits for each character.
<b>Parity</b>	None   Even   Odd; default: <b>Even</b>	<p>In serial transmission, parity is a method of detecting errors. An extra data bit is sent with each data character, arranged so that the number of 1 bits in each character, including the parity bit, is always odd or always even. If a byte is received with the wrong number of 1s, then it must have been corrupted. However, an even number of errors can pass the parity check.</p> <ul style="list-style-type: none"><li>• <b>None (N)</b> - no parity method is used.</li><li>• <b>Odd (O)</b> - the parity bit is set so that the number of "logical ones (1s)" has to be odd.</li><li>• <b>Even (E)</b> - the parity bit is set so that the number of "logical ones (1s)" has to be even.</li></ul>
<b>Stop bits</b>	1   2; default: <b>1</b>	Stop bits sent at the end of every character allow the receiving signal hardware to detect the end of a character and to resynchronise with the character stream. Electronic devices usually use one stop bit. Two stop bits are required if slow electromechanical devices are used.

## Flow control

None | RTS/CTS |  
Xon/Xoff;  
default: **None**

In many circumstances a transmitter might be able to send data faster than the receiver is able to process it. To cope with this, serial lines often incorporate a "handshaking" method, usually distinguished between hardware and software handshaking.

- **RTS/CTS** - hardware handshaking. RTS and CTS are turned OFF and ON from alternate ends to control data flow, for instance when a buffer is almost full.
- **Xon/Xoff** - software handshaking. The Xon and Xoff characters are sent by the receiver to the sender to control when the sender will send data, i.e., these characters go in the opposite direction to the data being sent. The circuit starts in the "sending allowed" state. When the receiver's buffers approach capacity, the receiver sends the Xoff character to tell the sender to stop sending data. Later, after the receiver has emptied its buffers, it sends an Xon character to tell the sender to resume transmission.

## RS485

This section is used to configure the Modbus RTU master's RS485 serial interface settings. Refer to the figure and table below for information on RS485 configuration.

### RS485

RS485 configuration

Enabled

Baud rate 19200

Data bits 8

Parity Even

Stop bits 1

Flow control None

Field	Value	Description
Enabled	yes   no; default: <b>no</b>	Turns Modbus RTU via RS485 on or off.

<b>Baud rate</b>	300   1200   2400   4800   9600   19200   38400   57600   115200; default: <b>19200</b>	Serial data transmission rate (in bits per second).
<b>Data bits</b>	5   6   7   8; default: <b>8</b>	Number of data bits for each character.
<b>Parity</b>	None   Even   Odd; default: <b>Even</b>	<p>In serial transmission, parity is a method of detecting errors. An extra data bit is sent with each data character, arranged so that the number of 1 bits in each character, including the parity bit, is always odd or always even. If a byte is received with the wrong number of 1s, then it must have been corrupted. However, an even number of errors can pass the parity check.</p> <ul style="list-style-type: none"> <li>• <b>None (N)</b> - no parity method is used.</li> <li>• <b>Odd (O)</b> - the parity bit is set so that the number of "logical ones (1s)" has to be odd.</li> <li>• <b>Even (E)</b> - the parity bit is set so that the number of "logical ones (1s)" has to be even.</li> </ul>
<b>Stop bits</b>	1   2; default: <b>1</b>	<p>Stop bits sent at the end of every character allow the receiving signal hardware to detect the end of a character and to resynchronise with the character stream. Electronic devices usually use one stop bit. Two stop bits are required if slow electromechanical devices are used.</p>
<b>Flow control</b>	None   RTS/CTS   Xon/Xoff; default: <b>None</b>	<p>In many circumstances a transmitter might be able to send data faster than the receiver is able to process it. To cope with this, serial lines often incorporate a "handshaking" method, usually distinguished between hardware and software handshaking.</p> <ul style="list-style-type: none"> <li>• <b>RTS/CTS</b> - hardware handshaking. RTS and CTS are turned OFF and ON from alternate ends to control data flow, for instance when a buffer is almost full.</li> <li>• <b>Xon/Xoff</b> - software handshaking. The Xon and Xoff characters are sent by the receiver to the sender to control when the sender will send data, i.e., these characters go in the opposite direction to the data being sent. The circuit starts in the "sending</li> </ul>

allowed" state. When the receiver's buffers approach capacity, the receiver sends the Xoff character to tell the sender to stop sending data. Later, after the receiver has emptied its buffers, it sends an Xon character to tell the sender to resume transmission.

## Slaves

---

The **Slaves** section is used to configure new Modbus slave devices. A Modbus slave is an entity that can be called upon by a Modbus master in order to obtain some type of information from it.

To create a new Modbus slave, enter a custom name for it and click the 'Add' button. Then click the 'Edit' button next to the slave in order to enter its configuration window.

### *Slave settings*

---

The **Settings** section is used to configure the main parameters of the Modbus slave. Refer to the figure and table below for additional information.

Slave 'Demo' configuration

Settings

Enabled

Slave ID

Period

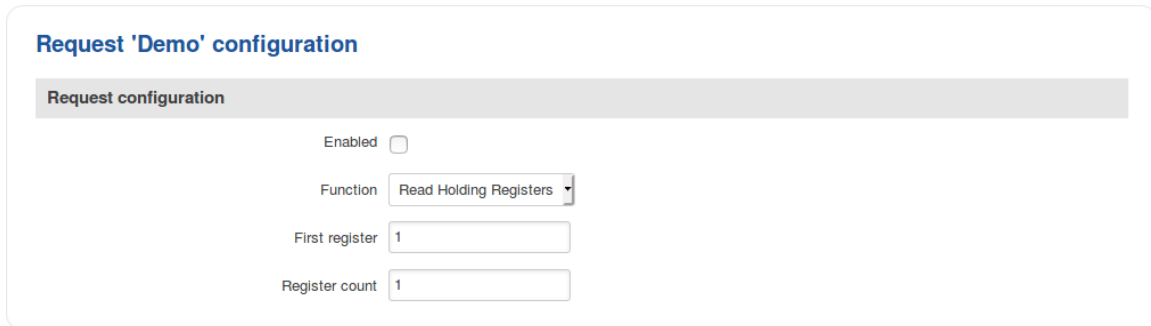
Field	Value	Description
<b>Enabled</b>	yes   no; default: <b>no</b>	Turns the slave on or off.
<b>Slave ID</b>	integer [1..255]; default: <b>1</b>	Slave ID. Each slave in a network is assigned a unique identifier ranging from 1 to 255. When the master requests data from a slave, the first byte it sends is the Slave ID.
<b>Period</b>	integer [1..9999]; default: <b>10</b>	Interval (in minutes) at which requests are sent to the slave device.

### *Slave requests*

---

A Modbus **request** is a way of obtaining data from Modbus slaves. The master sends a request to a slave specifying the function code to be performed. The slave then sends the requested data back to the Modbus master.

The figure below is an example of the Requests configuration section and the table below provides information contained in the fields of that section:



The screenshot shows a configuration form titled "Request 'Demo' configuration". It contains a section labeled "Request configuration" with the following fields:

- Enabled:** A checkbox that is currently unchecked.
- Function:** A dropdown menu with "Read Holding Registers" selected.
- First register:** A text input field containing the value "1".
- Register count:** A text input field containing the value "1".

Field	Value	Description
<b>Enabled</b>	yes   no; default: <b>no</b>	Turns the request on or off.
<b>Function</b>	Read Coil   Read Discrete Input   Read Holding Registers   Read Input Registers; default: <b>Read Holding Registers</b>	Modbus function used in Modbus request.
<b>First Register</b>	integer [1..65536]; default: <b>1</b>	First Modbus register from which data will be read.
<b>Number of Registers</b>	integer [1..2000]; default: <b>none</b>	Number of Modbus registers that will be read during the request/

### *Slave alarms*

**Alarms** are a way of setting up automated actions when some Modbus values meet user specified conditions. The figure below is an example of the Alarm configuration page and the table below provides information on fields that it contains:

## Alarm 'Demo' configuration

Alarm configuration

Enabled

Function Read Holding Registers ▾

Register

Condition More than ▾

Value

Action SMS ▾

Phone number

Message

Field	Value	Description
<b>Enabled</b>	yes   no; default: <b>no</b>	Turns the alarm on or off.
<b>Function</b>	Read Coil   Read Discrete Input   Read Holding Registers   Read Input Registers; default: <b>Read Holding Registers</b>	Modbus function used in Modbus request.
<b>Register</b>	integer [1..65536]; default: <b>1</b>	Number of the Modbus coil/input/holding register/input register that will be read.
<b>Condition</b>	More than   Less than   Equal to   Not equal to; default: <b>More than</b>	When a value is obtained it will be compared against the value specified in the following field. The comparison will be made in accordance with the condition specified in this field.
<b>Value</b>	integer [0..65535]; default: <b>0</b>	The value against which the read data will be compared.
<b>Action</b>	SMS   Trigger output   Modbus request; default: <b>SMS</b>	Action that will be taken if the condition is met. Possible actions: <ul style="list-style-type: none"> <li>• <b>SMS</b> - sends an SMS message to a specified recipient(s).</li> <li>• <b>Trigger output</b> - changes the state of a specified output(s).</li> </ul>

- **Modbus Request** - sends a Modbus request to a specified slave.

## Modbus Data to Server

The Modbus **Data to Server** function provides you with the possibility to set up senders that transfer data collected from Modbus slaves to remote servers. To add a new data sender, enter the server's address, specify the data sending period and click the "Add" button:

**Modbus data sender**

Modbus data to server function allows to send data collected from modbus slaves to remote server

**Modbus data senders**

Name	Protocol	URL	Device	Period	Enabled	
N/A	HTTP(S)	192.168.1.1	All	50	<input type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

**New modbus data sender**

Protocol: HTTP(S) | URL: 192.168.1.1 | Period: 50 |

## Data sender configuration

When you add a new data sender, you will be redirected to its configuration window. The figure below is an example of that window and the table below provides information on the fields that it contains:

## Advanced sender settings

Here you can configure advanced settings for the data sender

**Data sender configuration**

Enabled

Name

Protocol HTTP(S) ▾

JSON format 

Modbus slave ID - %i  
 Modbus slave IP - %p  
 Date (Linux timestamp) - %t  
 Date (Day/Month/Year Hour:Minute:Second) - %d  
 Start register - %s  
 Register data - %a

Segment count 1 ▾

URL

Period

Data filtering All data ▾

Retry on fail

Custom Header  +

Enabled	Yes   No; Default: No	Turns The Data Sender ON Or OFF
<b>Name</b>	string; Default: <b>none</b>	Data sender's name. used for easier management purposes
<b>Protocol</b>	HTTP(S); Default: <b>HTTP(S)</b>	Data sending protocol
<b>JSON format</b>	json string; Default: <b>{"ID": "%i", "TS": "%t", "ST": "%s", "VR": "%a"}</b>	Provides the possibility to fully customize the JSON segment
<b>Segment count</b>	1   2   3   4   5   6   7   8   9   10; Default: <b>1</b>	Max segment count in one JSON string sent to server
<b>URL</b>	host   ip; Default: <b>none</b>	Address of the server to which the data will be sent. . <b>Important note:</b> when using HTTPS, remember to add the <b>https://</b> prefix before the URL
<b>Period</b>	integer [1..6400]; Default: <b>none</b>	Data sending frequency (in seconds)
<b>Data filtering</b>	All data   By slave ID   By slave IP; Default: <b>All data</b>	Which data this sender will transfer to the server
<b>Retry on fail</b>	yes   no; Default: <b>no</b>	Specifies whether the data sender should retry failed attempts
<b>Custom header</b>	string; Default: <b>no</b>	Adds a custom header(s) to HTTP requests



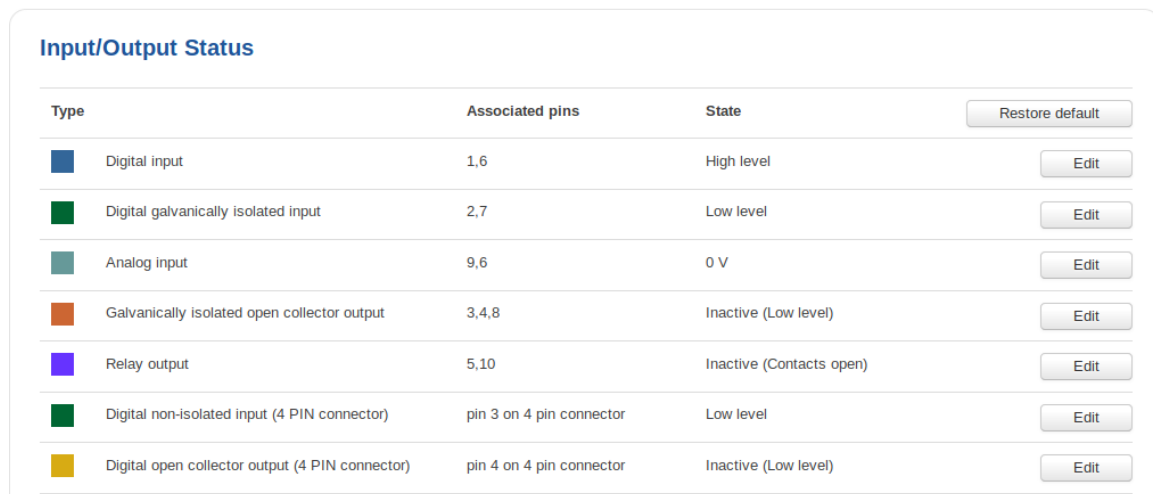
# Input/Output








## Summary

**Inputs and Outputs** are used for the monitoring and controlling of a connected device or receiving signals from that device in order to trigger certain events.

## Status

The **Status** tab displays the current states the router's inputs and outputs:



Type	Associated pins	State	Restore default
 Digital input	1,6	High level	<input type="button" value="Edit"/>
 Digital galvanically isolated input	2,7	Low level	<input type="button" value="Edit"/>
 Analog input	9,6	0 V	<input type="button" value="Edit"/>
 Galvanically isolated open collector output	3,4,8	Inactive (Low level)	<input type="button" value="Edit"/>
 Relay output	5,10	Inactive (Contacts open)	<input type="button" value="Edit"/>
 Digital non-isolated input (4 PIN connector)	pin 3 on 4 pin connector	Low level	<input type="button" value="Edit"/>
 Digital open collector output (4 PIN connector)	pin 4 on 4 pin connector	Inactive (Low level)	<input type="button" value="Edit"/>

## Custom Labels

If the default Input/Output labels do not suit your needs, you can always configure custom ones in the **Custom Labels** section. Click the 'Edit' button next to the desired Input or Output and you will be redirected to a window such as this:



**Custom I/O Status Labels**

Customize Digital input and state fields

Digital Input name

Input shorted state

Input open state

The figure above is an example of custom label configuration for *Digital Input*. You can change an input's/output's name and the names of their states. The changes are purely cosmetic and used for easier management purposes.

In addition to adding custom names, you can also define how the displayed value for Analog Input is calculated and displayed. The figure below represents what the configuration of custom labels for Analog Input looks like.

**Custom I/O Status Labels**

Customize Analog input and value fields

Analog Input name

User defined unit of measurement

Add custom values into fields to calculate formula:

$$DV = \text{Value} \times \left( \frac{A \pm \text{Value}}{\text{Value}} \right) \pm \text{Value}$$

Displayed Value      Sensor slope      Analog Value      Voltage offset      Resistor value      Sensor offset

## Input

The **Input** tab is used to configure the router's input pins.

### Check Analog

The **Check Analog** section is used to set how often the router checks the value of the analog input. This is relevant to input rules related to the analog input. For example, if you have configured an input rule that triggers a certain action when the analog input value is inside a certain range, the frequency at which the router will check this value is set in this section.

**Input/Output**

Create rules for Input/Output configuration.

**Check Analog**

Interval [sec]

### Input Rules

The **Input Rules** section provides you with the possibility to set up rules that execute user specified actions after a certain trigger occurs. To add a new rule, look to the Input Configuration section that is just below. Select the input, the trigger and the action for the rule and click the 'Add' button. A new rule will appear in the Input Rules list:

Type	Trigger	Action	Enable	Sort
Digital	Input open	Send SMS	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

**Input Configuration**

Input type:  Trigger:  Action:

To begin editing an input rule, click the 'Edit' button located next to it. Refer to the figure and table below for information on input rule configuration.

**Input Configuration**

Enable

Input type:

Trigger:

Action:

SMS text:

Time stamp - %ts      Router name - %rn  
 Serial number - %sn    WAN MAC address - %wm  
 LAN MAC address - %lm    Current FW version - %fc  
 Connection state - %cs    Operator name - %on  
 Connection type - %ct    Signal strength - %ss  
 SIM slot in use - %su    IMSI - %im  
 Event type - %et        Event text - %ex  
 FW available on server - %fs    LAN IP - %li  
 Network state - %ns        WAN IP address - %wi  
 New line - %nl            Digital input - %di  
 Digital isolated input - %li    Analog input - %ai  
 Analog min voltage - %an        Analog max voltage - %ax

Recipients:

Recipient's phone number:

Field	Value	Description
<b>Enable</b>	yes   no; default: <b>yes</b>	Turns the input rule on or off.
<b>Input type</b>	Digital   Digital isolated   Analog; default: <b>Digital</b>	Selects to which input pin the rule will apply.
<b>Trigger</b>	Input open   Input shorted   Both; default: <b>Input open</b>	Selects which input state will trigger the rule.
<b>Action</b>	Send SMS   Change SIM card   Send email   Change profile   Turn	The action that will be taken when the rule is triggered.

on WiFi | Turn off WiFi  
 | Reboot | Activate  
 output | HTTP  
 POST/GET;  
 default: **Send SMS**

- **Send SMS** - sends an SMS message to a specified number(s) or user group. The message text is custom.
- **Change SIM card** - switches to using the SIM card that is currently not in use.
- **Send email** - sends an email to the specified address(es). You will be prompted to enter your email account's authentication information.
- **Change profile** - switches to using another configuration profile. Configuration profiles can be created via the *System* → *Profiles* page.
- **Turn on WiFi/Turn off WiFi** - turns WiFi on or off.
- **Reboot** - reboots the router when a specified amount of time passes or instantly after the trigger occurrence.
- **Activate output** - activates the specified router output.
- **HTTP POST/GET** - executes an HTTP POST or HTTP GET action.

## Output

The **Output** tab is used to configure the router's output pins.

### Output Configuration

The **Output Configuration** section is used to change the default states of the router's output pins.

#### Output Configuration

Default output state configuration

Open collector output

Relay output

Digital output 4PIN

Field	Value	Description
<b>Open collector output</b>	Low level   High level; default: <b>Low level</b>	Changes the default* state of the open collector (OC) output pin.

\* Changing the default state of an output means that the changes will be written into the input/output config and saved. This means that unless some other related change occurs the state of the output will remain as set in this section.

## ON/OFF

The **ON/OFF** section is used to turn the router's outputs on or off. This action does not save the state permanently, meaning that after a reboot the states will revert back to their default values.

### Output

---

**Output**

Digital OC output	<input type="button" value="Turn on"/>
Digital relay output	<input type="button" value="Turn on"/>
Digital 4PIN output	<input type="button" value="Turn on"/>

## Periodic control

The **Periodic control** section allows you to set up automatic output control rules that trigger output state changes at the specified period or interval. Refer to the figure and table below for information on configuration fields contained in that section.

### Periodic Output Control

---

**Edit Output Control Rule**

Enable

Output

Action

Action timeout

Mode

Hours

Minutes

Days  Monday  
 Tuesday  
 Wednesday  
 Thursday  
 Friday  
 Saturday  
 Sunday

Field	Value	Description
<b>Enable</b>	yes   no; default: <b>no</b>	Turns the rule on or off.
<b>Output</b>	Digital OC Output   Digital 4PIN   Digital relay output; default: <b>Digital OC Output</b>	The output pin that will be effected by the rule.
<b>Action</b>	On   Off; default: <b>On</b>	The action that will be performed on the output.
<b>Action timeout</b>	yes   no; default: <b>no</b>	Action timeout specifies whether an action should end after some time. For example, if action is set to <i>on</i> and timeout is set to 10, when the trigger occurs the output will turn on for 10 seconds before turning off.
<b>Mode</b>	Fixed   Interval; default: <b>Fixed</b>	When the rule will be triggered. <ul style="list-style-type: none"> <li>• <b>Fixed</b> - triggers the specified action on a specified day(s), hour and minute. For example, every Sunday at 8:30 AM.</li> <li>• <b>Interval</b> - performs the action at an interval. For example, every 1 hour during Mondays.</li> </ul>

## Scheduler

---

With the help of the output **Scheduler** you can configure a timetable of when the outputs should be enabled or disabled based on time.

## Output Scheduler

### Configure Scheduled Outputs

Output Digital OC output

Days/Hours	0-1h	1-2h	2-3h	3-4h	4-5h	5-6h	6-7h	7-8h	8-9h	9-10h	10-11h	11-12h	12-13h	13-14h	14-15h	15-16h	16-17h	17-18h	18-19h	19-20h	20-21h	21-22h	22-23h	23-24h
Monday																								
Tuesday																								
Wednesday																								
Thursday																								
Friday																								
Saturday																								
Sunday																								

- Digital OC output active

---

- Digital relay output active (relay contacts closed)

---

- Digital 4PIN output active

---

- Digital OC and relay output active

---

- Digital OC and 4PIN output active

---

- Digital relay and 4PIN output active

---

- All active