UCR Routers

User Guide

V 1.A, July 2020

UNITRONICS®

Table of Contents

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 bellow is an example of the Overview page:
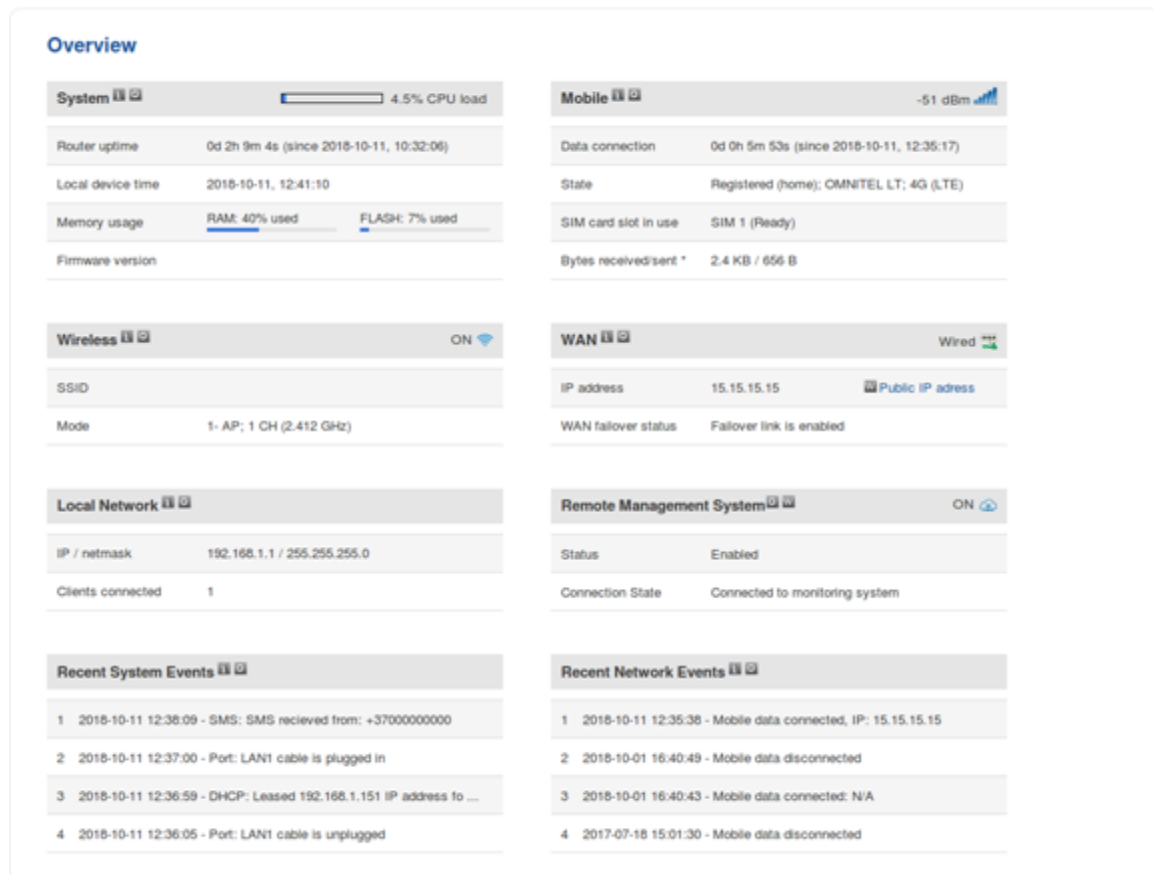
Mobile widget
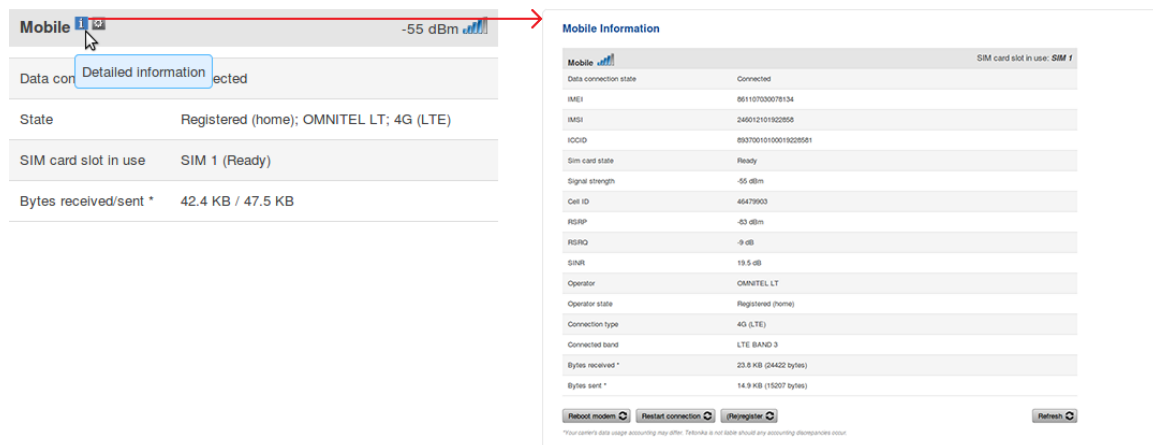
The **Mobile** widget displays information related to the mobile connection and the current **signal strength** (▂▄▆█). Each filled-up bar represents a different RSSI value:

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** (ℹ️) 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:

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:
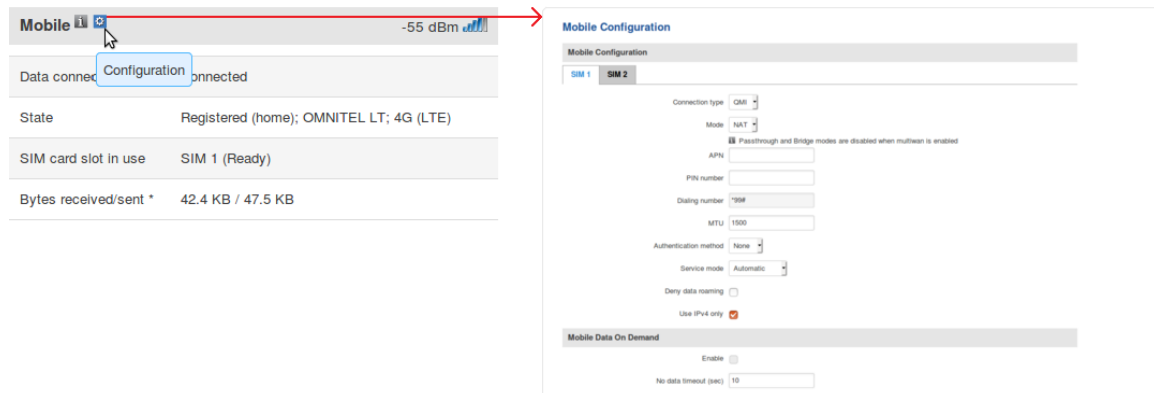
Adding more widgets

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

Field Name	Description
Router name	Displays the device's product name
Host name	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 **System → Administration → General** page
Router model	Displays the device's full model name
Firmware version	Displays the firmware version currently used by the device. The firmware can be upgraded from the **System → Firmware** page.
Kernel version	Displays the device's kernel version. A kernel is a computer program responsible for connecting a device's software to its hardware
Local device time	Displays the current time as perceived by the device. Time settings can be adjusted in the **Services → NTP** page
Uptime	Displays the amount of time that has passed since the device's last start up
Load average	Displays the device's CPU load average (in %) over the last minute, 5 minutes and 15 minutes
Free	Displays the amount of currently unused random-access memory (RAM)
Cached	Displays the amount of random-access memory (RAM) that is allocated for frequently accessed data storage
Buffered	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

IMEI	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
IMSI	The IMSI (international mobile subscriber identity) is a unique 15 decimal digit (or less) number used to identify the user of a cellular network
ICCID	SIM card's ICCID is a unique serial number used to identify the SIM chip
SIM card state	The current SIM card state. Possible values are: • **Ready** - SIM card is inserted and ready to be used • **Inserted** - SIM card is inserted • **Not inserted** - SIM card is not inserted • **Unknown** - unable to obtain SIM card state value. Possible communication issue between the the device and the modem
Signal strength	Received signal strength indicator (**RSSI**) measured in dBm. Values closer to 0 indicate a better signal strength
Cell ID	The ID of the cell that the modem is currently connected to

Signal level measurements	Overall signal quality is defined by different measurements for different connection types. Short explanations and recommendations are provided below.
	
	• **4G**
	    • RSRP - reference signal received power, measured in dBm. Values closer to 0 indicate better signal strength
	    • RSRQ - reference signal received quality, measured in dB. Values closer to 0 indicate a better rate of information transfer
	    • SINR - signal-to-interference-plus-noise ratio, measured in dB. Higher values indicate a better rate of information transfer
	• **3G**
	    • EC/IO - downlink carrier-to-interference ratio. Values range from -20 to 0 (closer to 0 indicates better signal quality/cleanliness)
	    • RSCP - received signal code power. Values range from -124 to 0 (closer to 0 indicates better signal stength)
	• **2G**
	    • RSSI - received signal strength indicator, measured in dBm. Values closer to 0 indicate better signal strength

Operator   Network operator's name

Operator state   Shows whether the network has currently indicated the registration
                            of the mobile device. Possible values are:

- **Unregistered** - not registered to a network and the device is not
  currently searching for a new operator to register to
- **Registered (home)** - registered, home network
- **Searching** - not registered to a network, but the device is
  currently searching for a new operator to register to
- **Network denied** - registration to network denied by operator
- **Unknown** - operator state is currently unknown
- **Registered (roaming)** - registered to network, roaming
  conditions

Connection type   Mobile connection type. Possible values are:

- **2G**: 2G (GSM), 2G (GPRS), 2G (EDGE)
- **3G**: 3G (WCDMA), 3G (HSDPA), 3G (HSUPA), 3G (HSPA), 3G
  (HSPA+), 3G (DC-HSPA+), 3G (HSDPA+HSUPA), UMTS
- **4G**: 4G (LTE)
- **N/A** - not possible to determine at the moment

Connected band   Currently used frequency band.

Bytes received   Amount of data received through the mobile interface

Bytes sent   Amount of data sent through the mobile interface

Restart Modem   Reboots the device's cellular module

Restart Connection   Restarts the mobile connection

(Re)register   Registers to the mobile network

Refresh   Refreshes all information fields in the page
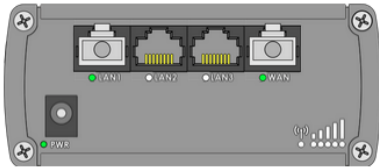
WAN

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

Field	Description
Interface	WAN type. Possible values are: • Mobile • Wired • Wireless

Type	Connection type or protocol. The value displayed in this field is dependent on used WAN type. Possible values are:
	
	• **Mobile WAN or USB modem**
	   • **Qmi2** - Qualcomm MSM Interface, a proprietary protocol used between Qualcomm cellular processors and their software stacks
	   • **PPP** - Point-to-Point Protocol; uses a dialling number to establish a data connection

12

- **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 **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
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

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 **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
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:	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 **Network → LAN → DHCP Server** 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:
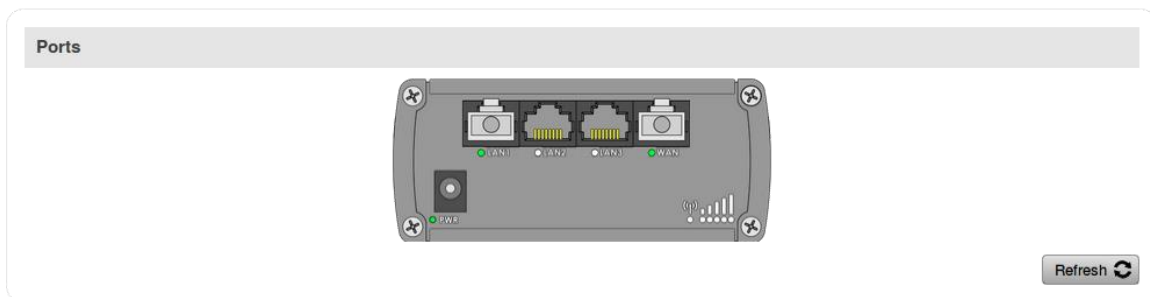
Wireless

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

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

16

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:

Field Name	Description
MAC address	Associated station's MAC (Media Access Control) address
Device Name	Currently connected device name
Signal	Received Signal Strength Indicator (RSSI). Signal's strength measured in dBm
RX rate	The rate at which packets are received from associated station
TX rate	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
Enabled	Indicates whether OpenVPN server/client is enabled or not
Status	Shows connection status
Type	Shows whether the router is a server or client
IP	Router's OpenVPN IP address
Mask	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
Time	Shows OpenVPN connection uptime

Topology

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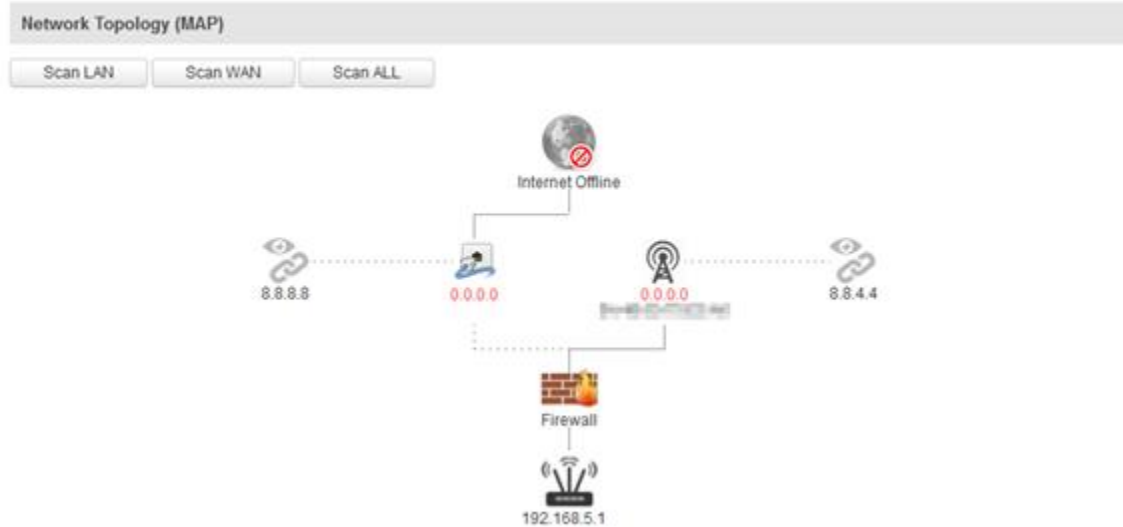
Access

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
Type	Shows access type
Status	Indicates whether that access type is enabled or not
Port	Shows which port which type of access uses
Active connections	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	*There are no records yet.*		

Last Remote Connections

Type	Date	IP	Authentications Status
SSH	*There are no records yet.*		
HTTP	*There are no records yet.*		
HTTPS	*There are no records yet.*		

Refresh ⟳

Field Name	Description
Type	Shows access type
Date	Indicates connection date
IP	Shows what IP address connected
Authentication Status	Shows whether authentication was successful or not

Device

Summary

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

Device Information

The figure bellow 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
Serial number	A unique 10-digit device identifier
Product code	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.
Batch number	A 4-digit number that indicates the batch of materials
Hardware revision	A 4-digit number representing the router's hardware revision version
IMEI	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
IMSI	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:

Click the zone next to a service where it says "Change settings" and you will 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
IP address	ip; Default: **none**	IP address of a local host
MAC address	mac; Default: **none**	MAC address of a local host
Interface	string; Default: **none**	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
Network	string; Default: **none**	Associated network interface name
Target	ip | ip/netmask; Default: **none**	Destination network address
IP gateway	ip; Default: **none**	Indicates the IP address of the gateway through which the target network can be reached
Metric	integer [0..4,294,967,295]; Default: **none**	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 your 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:

Field Name	Value	Description
Network	string; Default: **none**	Associated network interface name
Target	ip6 | ip6/netmask; Default: **none**	Destination network address
IP gateway	ip6; Default: **none**	Indicates the IPv6 address of the gateway through which the target network can be reached
Metric	integer [0..4,294,967,295]; Default: **none**	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 your 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:

Mobile Signal Strength

3m	2m	1m

-66 dBm

-84 dBm

-102 dBm

(3 minutes window, 1 second interval)

Connection type: 4G (LTE)　　　**Signal:** -61 dBm　　　**Average:** -61.1 dBm　　　**Peak:** -55 dBm

2G (GSM)	2G (GPRS)	2G (EDGE)	3G (WCDMA)
3G (HSDPA)	3G (HSUPA)	3G (HSPA)	3G (HSPA+)
3G (DC-HSPA+)	3G (HSDPA+HSUPA)	3G (UMTS)	4G (LTE)
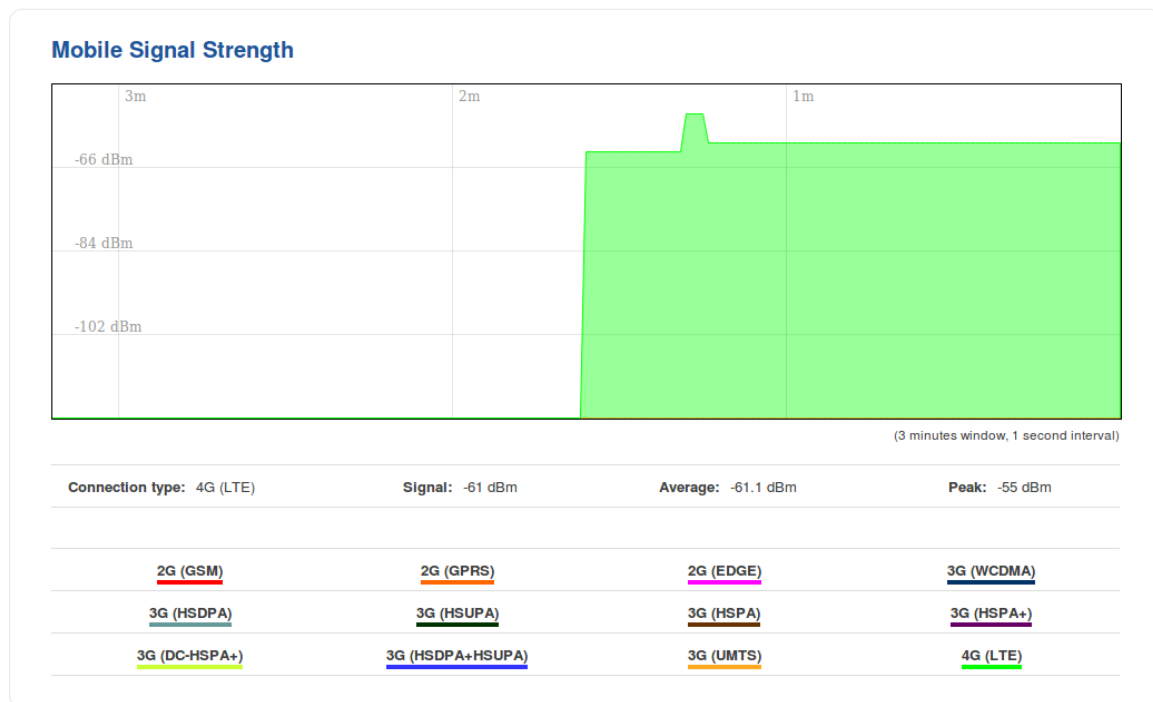
Load

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:

Realtime Load

(3 minutes window, 3 seconds interval)

1 Minute Load: 1.56	Average: 1.55	Peak: 1.57
5 Minutes Load: 0.94	Average: 0.93	Peak: 0.94
15 Minutes Load: 0.70	Average: 0.70	Peak: 0.70
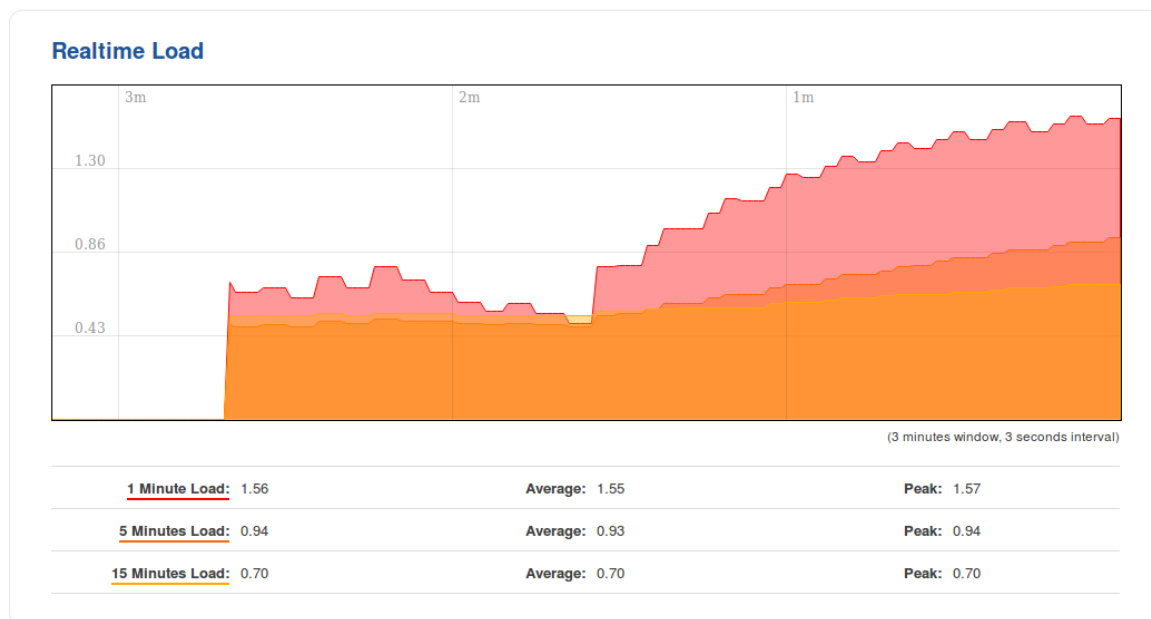
Traffic

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:

Realtime Traffic

| Bridge | LAN | WiFi | Mobile |

(3 minutes window, 3 seconds interval)

Inbound: 0.81 Kbits/s
(0.1 KBytes/s)

Average: 2.61 Kbits/s
(0.33 KBytes/s)

Peak: 3.44 Kbits/s
(0.43 KBytes/s)

Outbound: 1.03 Kbits/s
(0.13 KBytes/s)

Average: 9.68 Kbits/s
(1.21 KBytes/s)

Peak: 11.23 Kbits/s
(1.4 KBytes/s)
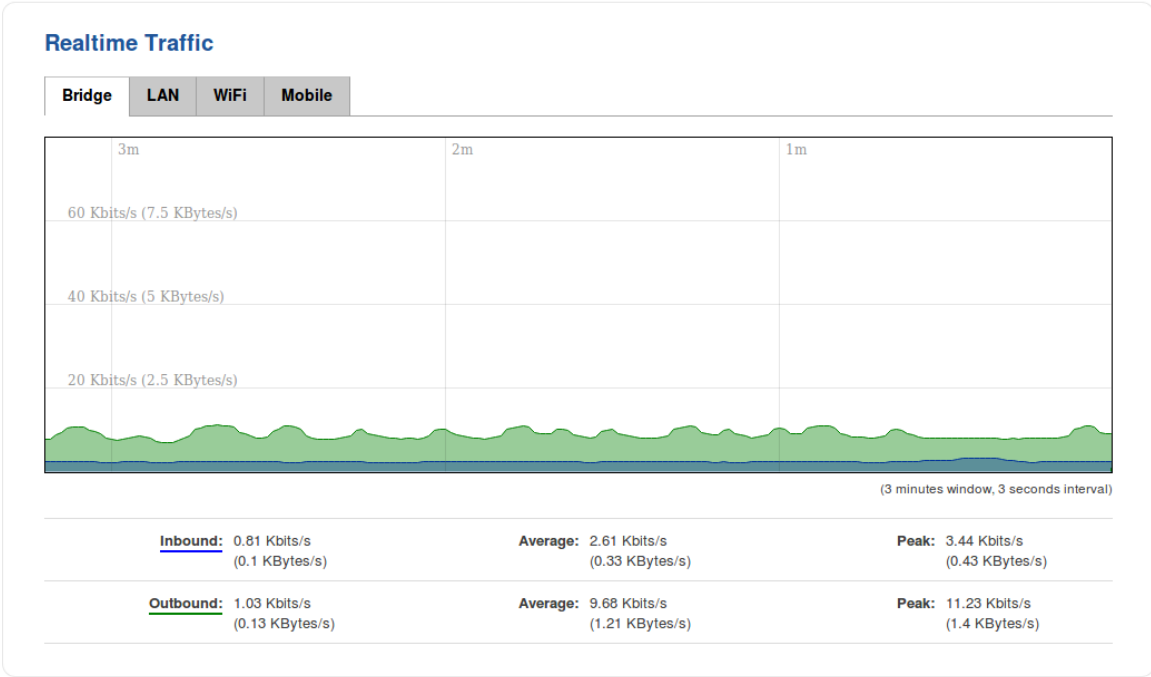
GRAPH	DESCRIPTION
Bridge	Cumulative graph, which encompasses wired Ethernet LAN and the wireless network
LAN	Displays traffic that passes through the LAN network interface(s) in graph form
WiFi	Displays traffic that passes through the WiFi interface in graph form
**WAN (Wired)	WAN (WiFi)	Mobile**	Displays 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:
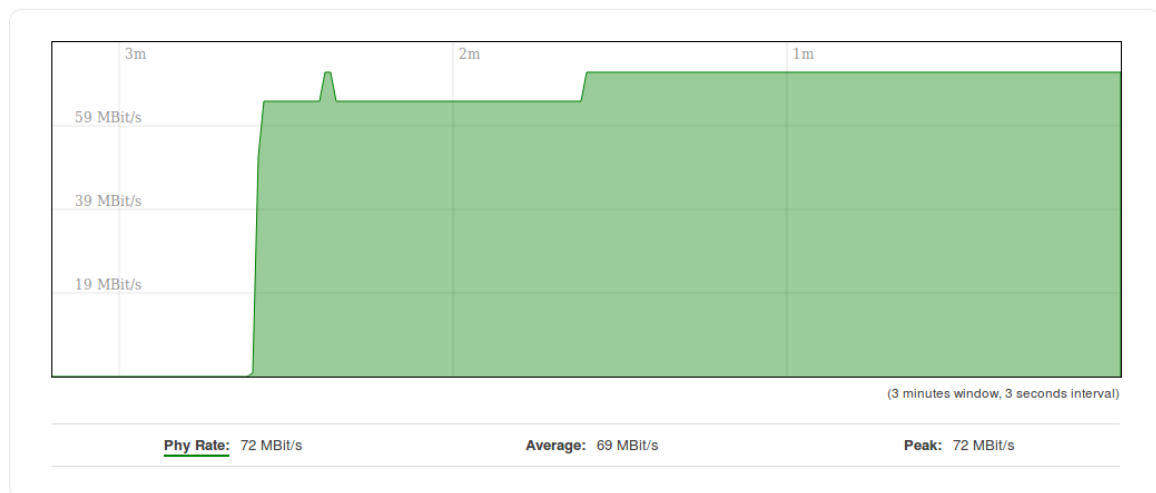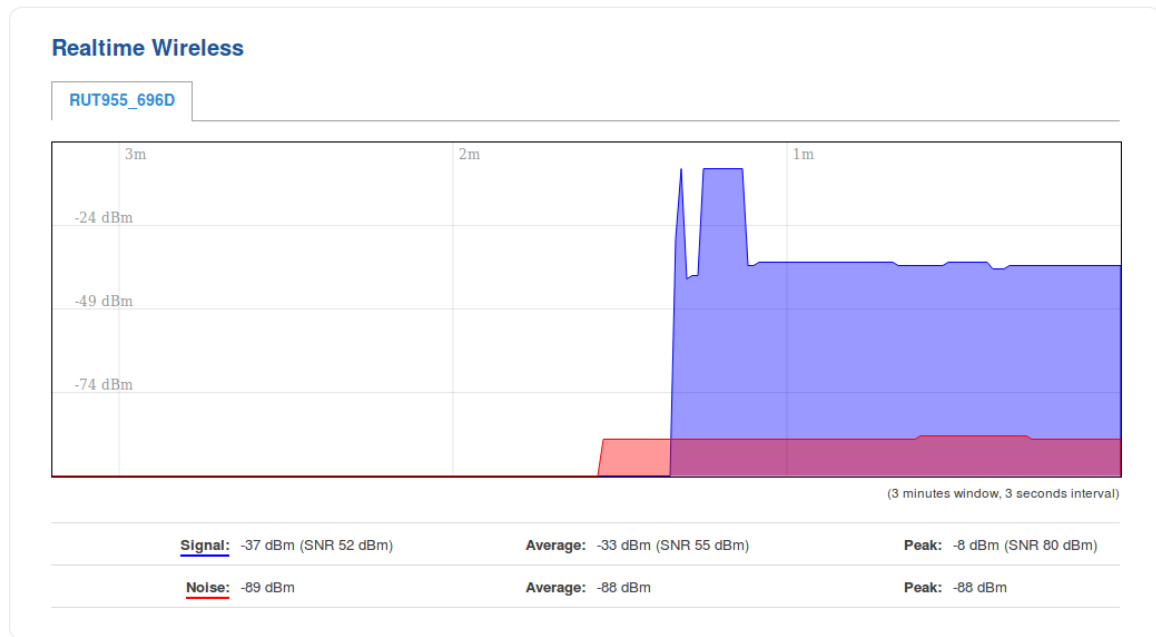
Connections

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:

Realtime Connections

This page gives you an overview of currently active network connections.

Active Connections

	3m	2m	1m
11			
7			
3			

(3 minutes window, 3 seconds interval)

UDP: 4	**Average:** 4	**Peak:** 14
TCP: 2	**Average:** 2	**Peak:** 3
Other: 0	**Average:** 0	**Peak:** 0
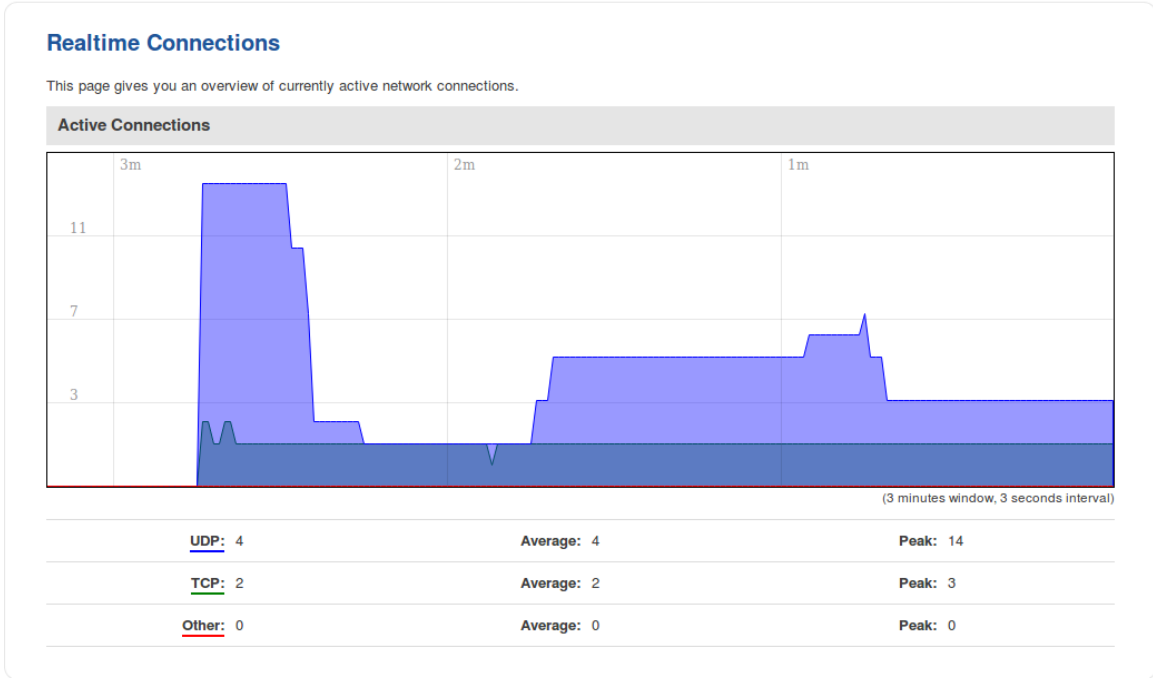
Mobile Traffic

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 **mdcollectdctl**. The usage for this command is described below:

```
usage: mdcollectdctl 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 **mdcollectdctl --help**.

Examples:

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

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

```
26558
```

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

```
root@ UCR:~# mdcollectdctl -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 | 10 | | | 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 | 10 | | | 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 | 10 | | | 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	☑	◆ ◆	Edit	Delete
Reboot	After unexpected shut down	Send email	☑	◆ ◆	Edit	Delete
SSH	All	Send SMS	☑	◆ ◆	Edit	Delete
Config change	OpenVPN	Send SMS	☑	◆ ◆	Edit	Delete
Backup	Switched to backup	Send SMS	☑	◆ ◆	Edit	Delete

Events Reporting Configuration

Event type	Event subtype	Action	
Config change ▾	All ▾	Send SMS ▾	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	Reboot ▼
Event subtype	All ▼
Action	Send SMS ▼
Enable delivery retry	☑
Retry interval	5 min. ▼
Retry count	2 ▼

Message text on Event

```
Router name - %rn;
Event type - %et; Event
text - %ex; Time stamp -
%ts;
```

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
Curren 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 ☑

Status message after reboot

```
Router name - %rn; WAN
IP - %wi; Data
Connection state - %cs;
Connection type - %ct;
Signal strength - %ss;
New FW available - %fs;
```

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
Curren FW version - %fc
Operator name - %on
Signal strength - %ss
IMSI - %im
Event text - %ex
LAN IP - %li
WAN IP address - %wi

Recipients	Single number ▼
Recipient's phone number	[ ] ➕

FIELD NAME	VALUE	DESCRIPTION
Enable	yes | no; Default: **no**	Toggles the rule ON or OFF
Event type	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**

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

		can be found in the SMS Utilities chapter, User Groups section
Recipient's phone number	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., **+120161234567**

Send Email

Event Reporting Configuration

Modify Event Reporting Rule

Enable	☑
Event type	Reboot ▼
Event subtype	After unexpected shut down ▼
Action	Send email ▼
Enable delivery retry	☑
Retry interval	5 min. ▼
Retry count	2 ▼
Subject	Reboot
Message text on Event	Router name - %rn; Event type - %et; Event text - %ex; Time stamp - %ts;

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
Curren 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	mail.hostname.com
SMTP server port	12345
Secure connection	☑
User name	user_name
Password	•••••••••••• 👁
Sender's email address	sender@email.com
Recipient's email address	recipient@email.com ➕
Send test email	Send

FIELD NAME	VALUE	DESCRIPTION
Enable	yes | no; Default: **no**	Toggles the rule ON or OFF
Event type	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**	
Event subtype	**Sample:** After unexpected shut down	Specified event's sub-type. This field changes in accordance with **Event type**
Action	Send SMS | Send email; Default: **Send SMS**	Action that is to be taken after the specified event occurs
Enable delivery retry	yes | no; Default: **no**	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
Retry interval	1 min. | 5 min. | 10 min. | 15 min. | 30 min. | 60 min.; Default **5 min.**	Specifies when the router should try re-sending the message in case the first attempt was a failure
Retry count	2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10; Default: **2**	Specifies the maximum number of failed attempts after which the router does not try to send the message anymore
Subject	string; Default: " "	Specifies the subject of the email message
Message text on Event	string; Default: **Router name - %rn; Event type - %et; Event text - %ex; Time stamp - %ts;**	Specifies the text that the message will contain
Get status after reboot	yes | no; Default: **no**	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

SMTP server	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
SMTP port	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
Secure connection	yes | no; Default: **no**	Toggles secure connection feature ON or OFF (use only if the email service provider's server supports SSL or TLS)
Username	string; Default: " "	Sender's email account's login user name
Password	string; Default: " "	Sender's email account's login password
Sender's email address	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
Recipient's email address	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
Send test mail	-	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
All	Sends a report message when any type of configuration changes are applied
OpenVPN	Sends a report message when any **OpenVPN** 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.
SMS	Sends a report message when any SMS related configuration changes are applied. For example, whenever a new **SMS Utilities** rule is created or changed, changes are made to **Auto Reply** or **Remote configurations**, etc.
Mobile traffic	Sends a report message when **Mobile Traffic** Logging is enabled/disabled or logging interval is changed.
Multiwan	Sends a report message when changes to WAN **Backup** 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.

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

	whenever Whitelist is changed to Blacklist or vice versa, a new entry is added to Blacklist/Whitelist, etc.
Login page	Sends a report message when any **Language Settings** are changed
Language	Sends a report message when any **Language Settings** are changed
Profile	Sends a report message when a new **Profile** is added or deleted
DDNS	Sends a report message when any configuration changes to **Dynamic DNS** are applied. For example, whenever a new DDNS instance is created, changed, deleted or edited
IPsec	Sends a report message when any configuration changes to **IPsec** are applied. For example, a new IPsec instance is created, changed, deleted, etc.
Access control	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.
DHCP	Sends a report message when any configuration changes to **DHCP** are applied. For example, whenever DHCP Server is enabled/disabled, DHCP address range is changed
RS232/RS485	Sends a report message when any configuration changes to **RS232/RS485** are applied. For example, whenever RS232 or RS485 configuration is enabled/disabled, baud rate is changed, etc.

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

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

Mobile Data

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

SMS

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

SIM Switch

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

Signal Strength

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

-93 dBm -75 dBm	Sends a report message when the router's RSSI value leaves the -93 dBm to -75 dBm range
-75 dBm -60 dBm	Sends a report message when the router's RSSI value leaves the -75 dBm to -60 dBm range
-60 dBm -50 dBm	Sends a report message when the router's RSSI value leaves the -60 dBm to -50 dBm range

Reboot

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

EVENT SUB-TYPE	DESCRIPTION
All	Sends a report message when someone connects to the router via SSH (either successfully or unsuccessfully)
Successful authentication	Sends a report message when someone successfully connects to the router via SSH
Unsuccessful authentication	Sends a report message when someone unsuccessfully tries to connect to the router via SSH

WebUI

EVENT SUB-TYPE	DESCRIPTION
All	Sends a report message when someone connects to the router via HTTP or HTTPS (either successfully or unsuccessfully)

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

New WiFi client

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

LAN Port State

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

EVENT SUB-TYPE	DESCRIPTION
All	Sends a report message when the router switches from using the Main WAN to using the Backup WAN and vice versa
Switched to main	Sends a report message when the router switches from using the Main WAN to using the Backup WAN
Switched to backup	Sends a report message when the router stops using the Backup WAN and start using the Main WAN

Restore Point

EVENT SUB-TYPE	DESCRIPTION
All	Sends a report message when either when a new Restore point is created or a Restore Point is loaded in to the router
Save	Sends a report message when a new Restore Point is created
Load	Sends a report message when a Restore Point is loaded on to the router

GPS

EVENT SUB-TYPE	DESCRIPTION
All	Sends a report message when the router moves in and out of the GPS Geofence area
Left geofence	Sends a report message when the router leaves the GPS Geofence area
Entered geofence	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	☑		Edit	Delete
System	FTP	☑		Edit	Delete

Events Log Reporting Configuration

Events log	Transfer type
System ▾	Email ▾	Add

FIELD NAME	VALUE	DESCRIPTION
Enable	yes | no; Default: **no**	Toggles the log file report rule ON or OFF

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

changes in accordance with **Interval between reports**

Hour	integer [1..24]; Default: **1**	Specifies on the hour of the day when the logging should take place

Email

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

Transfer type	Email | FTP; Default: **Email**	Specifies whether to transfer the log(s) to FTP or Email
Compress file	yes | no; Default: **no**	Compress events log file using gzip
Subject	string; Default: " "	Specifies the subject of the email log message
Message	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
SMTP server	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
SMTP server port	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
Secure connection	yes | no; Default: **no**	Toggles secure connection feature ON or OFF (use only if the email service provider's server supports SSL or TLS)
Username	string; Default: " "	Sender's email account's login user name
Password	string; Default: " "	Sender's email account's login password
Sender's email address	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
Recipient's email address	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
Interval between reports	Week | Month | Year; Default: **Week**	Specifies how often the reports should be sent
Weekday | Month day	weekday | month day; Default: **Sunday**	Specifies the day of the month/week when the logging should take place. This field changes in accordance with **Interval between reports**
Hour	integer [1..24]; Default: **1**	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.

Field	Value	Description
Connection type	QMI | PPP; default: **QMI**	How the router's modem will establish a connection to the carrier. • **PPP** - uses a dialling number to establish a data connection. • **QMI** - does not use a dialling number to connect and is usually faster than PPP.
Mode	NAT | Bridge ***** | Passthrough******; default: **NAT**	Mobile connection operating mode. • **NAT** - the mobile connection uses NAT (network address translation). • **Bridge** - 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 static IP configuration. • **Passthrough** - 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.
APN	string; default: **none**	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 public IP address) depending on the contract. An APN Network Identifier cannot start with any of the following strings: • rac; • lac; • sgsn; • rnc; it cannot end in:

		• .gprs; And it cannot contain the asterisk symbol (*****).
Auto APN	checkbox; default: **enabled**	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.
PIN number	string; default: **none**	A 4-digit long numeric password used to authenticate the modem to the SIM card. **Reminder: Firstboot will not reset the PIN number, it must be changed manually**
PUK number	string; default: **none**	A 12-digit long numeric password used to reset a personal identification number (PIN) that has been lost or forgotten.
Dialing number	string; default: **none**	A dial code used to establish a mobile PPP connection.
MTU	integer [0..1500]; default: **1500**	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.
Authentication method	CHAP | PAP | None; default: **None**	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.
Service mode	2G only | 3G only | Automatic; default: **Automatic**	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.
Deny data roaming	yes | no; default: **no**	When enabled, this option prevents the device from establishing a mobile data connection while not in your home network (roaming conditions).

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
Enable	yes | no; default: **no**	Turns mobile data on demand on or off **Important**: this function is only available with PPP Connection type.
No data timeout (sec)	integer [10..3600]; default: **10**	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.

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:

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) 300

Field	Value	Description
Enable	yes | no; default: **no**	Turns force LTE network on or off.
Reregister	yes | no; default: **no**	When enabled the modem will attempt to reregister to the carrier before trying to connect to an LTE network.
Timeout (sec)	integer [180..3600]; default: **300**	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 Static ▾

MAC Address

Field	Value	Description
DHCP mode	Static | Dynamic | No DHCP; default: **Static**	Specifies DHCP mode used with Passthrough. • **Static** - 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

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 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.

Field	Value	Description
Bind to MAC	mac; default: **none**	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.

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.

Field	Value	Description
Enable automatic switching*	yes | no; default: **no**	Turns automatic SIM Switching on or off.
Check interval	integer; default: **30**	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.

Field	Value	Description
On weak signal	yes | no; default: **no**	Performs a SIM switch when signal strength value ([RSSI](#) 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.
On data limit	yes | no; default: **no**	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 → **Mobile Data Limit** page.
On SMS limit	yes | no; default: **no**	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 → **SMS Limit** page.
On roaming	yes | no; default: **no**	Performs a SIM switch when roaming conditions are detected (i.e., when the SIM card connects to a foreign operator).
No network	yes | no; default: **no**	Performs a SIM switch when the SIM card cannot find an operator to connect to.
On network denied	yes | no; default: **no**	Performs a SIM switch when access to a network is denied (usually by an operator).
On data connection fail	yes | no; default: **no**	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 opertors 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
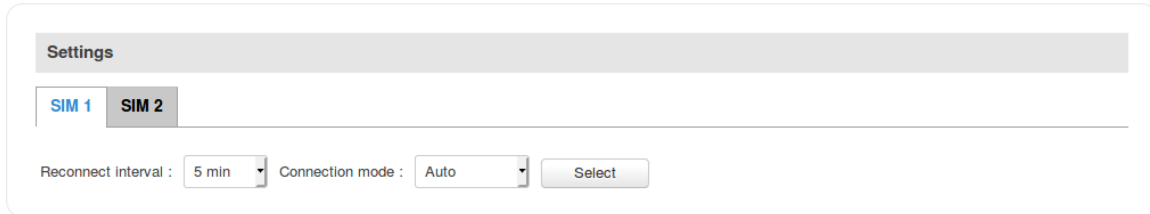
Scan For Network Operators is a function that initiates a scan for mobile network operators available in your area. To initiate a scan, press the 'Scan for operators' button. After you do, you will be prompted with a pop-up asking if you wish to proceed. This is because while the scan is in progress you will lose your data connection for approximately 2 minutes.

Network Operators

Current SIM

Current operator	OMNITEL LT

Scan for operators

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:

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

Field	Value	Description
Enable	yes | no; default: **no**	Turns operator list on or off.
Mode	Blacklist | Whitelist; default: **Whitelist**	Defines how operators will be filtered. • **Blacklist** - operators contained in the blacklist are considered forbidden and your router will not attempt to connect to them even if they are available. • **Whitelist** - 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.

Operators List

Field	Value	Description
Name	string; default: **none**	Operator's name. Used only for easier management purposes and not in the actual filtering process.
Operator code	integer; default: **none**	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 [Month ▾]

Start day [1 ▾]

Field	Value	Description
Enable data connection limit	yes | no; default: **no**	Turns mobile data limitations on or off.
Data limit* (MB)	integer; default: **none**	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. **Note**: 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.
Period	Month | Week | Day; default: **Month**	Data limit period after which the data counter is reset on the specified *Start day*.
Start day | Start hour	day [1..31] | day [Monday..Sunday] | hour [1..24]; default: **day 1**	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.

Field	Value	Description
Enable SMS warning	yes | no; default: **no**	Toggles SMS warning On or OFF
Data limit* (MB)	integer; default: **none**	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.
Period	Month | Week | Day; default: **Month**	Period to which the data limit applies to.
Start day | Start hour	day of the month [1..31] | day of the week [Monday..Sunday] | hour of the day [1..24]; default: **1**	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.
Phone number	phone number; default: **none**	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.

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
Enable SMS limit	yes | no; default: **no**	Turns SMS limitations on or off.
Period	Month | Week | Day; default: **Month**	SMS limit period after which the sent SMS counter is reset on the specified *Start day*.
Start day | Start hour	day of the month [1..31] | day of the week [Monday..Sunday] | hour of the day [1..24]; default: **1**	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.
SMS limit*	integer; default: **none**	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. **Note**: 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 SIM Switching rules 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**

Enable	yes | no; default: **no**	Turns SIM Idle Protection on or off.
Period	Month | Week; default: **Month**	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.
Host to ping	ip; default: **127.0.0.1**	IP address of a host that will be pinged during the SIM Idle Protection action.
Ping package size	integer [1..1000]; default: **56**	ICMP packet size in bytes.
Ping requests	integer [1..30]; default: **2**	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.

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 commiting any actions**. Commiting 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:

Field	Value	Description
APN	string; default: **none**	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 public IP address) depending on the contract. The check mark on the right side of the APN field enables the *Auto APN* 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: • rac; • lac; • sgsn; • rnc; it cannot end in: • .gprs; and it cannot contain the asterisk symbol (*****).
PIN number	string; default: **none**	A 4-digit long numeric password used to authenticate the modem to the SIM card.
Authentication method	CHAP | PAP | None; default: **None**	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.
Service mode	2G only | 2G preferred | 3G only | 3G preferred | 4G (LTE) only | 4G (LTE) preferred | Automatic; default: **4G (LTE) preferred**	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 chose between three types of WAN – Mobile, Wired and Wi-Fi. You can also setup backup WAN options in case your main connection goes down.

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

Field Name	Value	Description
Protocol	Static | DHCP | PPPoE; Default: **DHCP**	The protocol used by the WAN interface
IPv4 address	ip; Default: " "	Your router's address on the WAN network
IPv4 netmask	ip; Default: **255.255.255.0**	Netmask defines how "large" a network is
IPv4 gateway	ip; Default: " "	The address where the router will send all the outgoing traffic
IPv4 broadcast	ip; Default: " "	IP broadcasts are used by BOOTP and DHCP clients to find and send requests to their respective servers
Use custom DNS servers	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 00:1E:42:22:62:B6

Override MTU 1500

Use gateway metric 0

Field Name	Value	Description
Disable NAT	yes | no; Default: **no**	Toggles Network Address Translation (NAT) on or off for the selected network interface
Override MAC address	mac; Default: **router's mac**	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
Override MTU	integer [0..1500]; Default: **1500**	Maximum Transmission Unit (MTU) – specifies the largest possible size of a data packet
Use gateway metric	integer; Default: **0**	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

Field Name	Value	Description
Protocol	Static | DHCP | PPPoE; Default: **DHCP**	The protocol used by the WAN interface
Hostname to send when requesting DHCP	ip | hostname; Default: **router's hostname**	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.

Field Name	Value	Description
Disable NAT	yes | no; Default: **no**	Toggles Network Address Translation (NAT) on or off for the selected network interface
Use broadcast flag	yes | no; Default: **no**	Required for certain ISPs (Internet Service Providers), e.g. Charter with DOCSIS 3
Use default gateway	yes | no; Default: **yes**	Uses the default gateway obtained through DHCP. If left unchecked, no default route is configured
Use DNS servers advertised by peer	yes | no; Default: **yes**	Uses DNS servers obtained from DHCP. If left unchecked, the advertised DNS server addresses are ignored
Use custom DNS servers	ip; Default: " "	Lets you chose your own preferred DNS servers. This field only becomes visible if **Use DNS servers advertised by peer** field is unchecked
Use gateway metric	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
Client ID to send when requesting DHCP	string; Default: " "	Client ID which will be sent when requesting a DHCP lease
Vendor class to send when requesting DHCP	string; Default: " "	Vendor class which will be sent when requesting a DHCP lease
Override MAC address	mac; Default: **router's mac**	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

Override MTU	integer [0..1500]; Default: **1500**	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.

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

Field Name	Value	Description
Disable NAT	yes | no; Default: **no**	Toggles Network Address Translation (NAT) on or off for the selected network interface
Use default gateway	yes | no; Default: **yes**	Uses the default gateway obtained through DHCP. If left unchecked, no default route is configured
Use gateway metric	integer; Default: **0**	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
Use DNS servers advertised by peer	yes | no; Default: **yes**	Uses DNS servers obtained from DHCP. If left unchecked, the advertised DNS server addresses are ignored
Use custom DNS servers	ip; Default: " "	Lets you chose your own preferred DNS servers. This field only becomes visible if **Use DNS servers advertised by peer** field is unchecked
LCP echo failure threshold	integer; Default: **0**	Presumes peer to be dead after given amount of LCP echo failures. Leave it at 0 to ignore failures
LCP echo interval	integer; Default: **5**	Sends LCP echo requests at the given interval in seconds. This function is only effective in conjunction with failure threshold
Inactivity timeout	integer; Default: **0**	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

Field Name	Value	Description
IP address	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
Netmask	ip; Default: **255.255.255.0**	Netmask defines how "large" a network is
Gateway	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.

Field Name	Value	Description
IP Broadcast	ip; Default: " "	IP broadcasts are used by BOOTP and DHCP clients to find and send requests to their respective servers
DNS	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.

Field Name	Value	Description
Health monitor interval	Disable | 5 sec. | 10 sec. | 20 sec. | 30 sec. | 60 sec. | 120 sec.; Default: **10 sec.**	The interval at which health checks are performed
Health monitor ICMP host(s)	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: **8.8.4.4**	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)
Health monitor ICMP timeout	1 sec. | 2 sec. | 3 sec. | 4 sec. | 5 sec. | 10 sec.; Default: **3 sec.**	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)
Attempts before failover	1 | 3 | 5 | 1 | 15 | 20; Default: **3**	The number of failed ping attempts after which the connection is to be declared as "**down**"
Attempts before recovery	1 | 3 | 5 | 1 | 15 | 20; Default: **3**	The number of successful ping attempts after which the connection is to be declared as "**up**"

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.

Field Name	Value	Description
IP address	ip; Default: **192.168.1.1**	IP address that the device uses on the LAN network
IP netmask	ip; Default: **255.255.255.0**	A netmask is used to define how "large" the LAN network is
IP broadcast	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 `1500`

Use gateway metric `10`

Use WAN port as LAN ☐ ⓘ WAN Ethernet port selected as LAN

Field Name	Value	Description
Accept router advertisements	yes | no; Default: **no**	Allows accepting router advertisements
Override MTU	integer [0..1500]; Default: **1500**	MTU (Maximum Transmission Unit) specifies the largest possible size of a data packet
Use gateway metric	integer; Default: **0**	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
Use WAN port as LAN	yes | no; Default: **no**	If this is enabled, the router's WAN port will act as if it were a LAN port. **Works only if WAN is not set to wired**

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:

90

Field Name	Value	Description
DHCP	Enable | Disable | DHCP Relay; Default: **Enable**	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
Start	integer [1..253]; Default: **100**	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
Limit	integer [1..4294967296]; Default: **150**	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)
Lease time	time in 'h' (hours) or 'm' (minutes); Default: **12h**	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
Dynamic DHCP	yes | no; Default: **yes**	Enables Dynamic allocation of client addresses. If this is disabled, only clients that have static IP leases will be served
Enable DNS rebind protection	yes | no; Default: **yes**	Enables DNS rebind attack protection by discarding upstream RFC1918 responses (leave default unless necessary otherwise)
Force	yes | no; Default: **no**	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
IP netmask	ip; Default: **255.255.255.0**	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.

Static Leases

Hostname	MAC address	IP address	
			Delete

Add

Field Name	Value	Description
Hostname	string; Default: " "	A custom name that will be linked with the device
MAC address	mac; Default: " "	Device's MAC address
IP address	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

Field Name	Value	Description
IP address	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
Netmask	ip; Default: **255.255.255.0**	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.

Field Name	Value	Description

IP Broadcast	ip; Default: " "	IP broadcasts are used by BOOTP and DHCP clients to find and send requests to their respective servers
DNS	ip; Default: " "	A separate DNS server to be used by the IP Alias address
Gateway	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
Enable	yes | no; Default: **no**	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
Enable	yes | no; Default: **no**	Toggles UDP Broadcast Relay ON or OFF
Port	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).
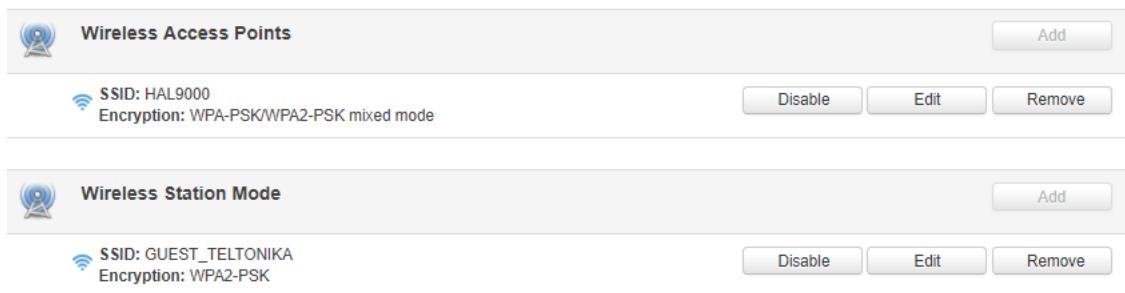
Above is the overview of the Wireless Configuration window. It displays active access points and stations. Here you can disable or enable your WiFi interfaces, remove unwanted access points or stations or enter a configuration window for each WiFi interface, where you can configure it more thoroughly.

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:
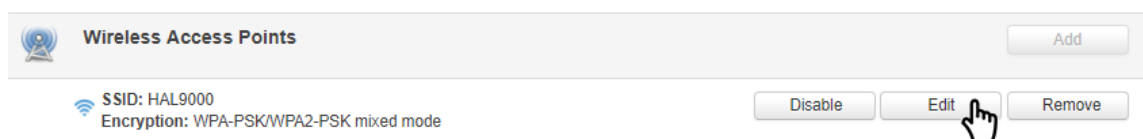
Device Configuration

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.

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	802.11g+n ▾
HT mode	20MHz ▾
Country code	00 - World ▾
Transmit power	100 % ▾
Fragmentation threshold	
RTS/CTS threshold	

Field Name	Value	Description
Mode	Auto | 802.11b | 802.11g | 802.11g+n; Default: **802.11g+n**	Wireless protocol used. Different modes provide different wireless standard support which directly impacts the radio's throughput performance
HT mode	20 MHz | 40 MHz 2nd channel above; Default: **20 MHz**	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 **Auto**
Country code	country code; Default: **0 - World**	SO/IEC 3166 alpha2 country codes as defined in ISO 3166-1 standard
Transmit power	100 % | 80 % | 60 % | 40 % | 20 %; Default: **100 %**	WiFi signal power. Use lower power to reduce the router's CPU usage
Fragmentation threshold	integer [256..2346]; Default: " "	The smallest packet size that can be fragmented and transmitted by multiple frames. In areas were 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 •••••••••••• ⌀

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

Cipher	Auto | Force CCMP (AES) | Force TKIP | Force TKIP and CCMP (AES); Default: **Auto**	An algorithm for performing encryption or decryption
Key	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).

Field Name	Value	Description
Encryption*	No encryption | WPA-PSK | WPA2-PSK | WPA-PSK/WPA2-PSK mixed mode; Default: **No encryption**	The type of WiFi encryption used.
Cipher	Auto | Force CCMP (AES) | Force TKIP | Force TKIP and CCMP (AES); Default: **Auto**	An algorithm for performing encryption or decryption
Radius Server IP	host | ip; Default: " "	RADIUS server's IP address or host name
Radius Server Port	integer [0..65535]; Default: " "	The port number used for connection to the RADIUS server
Radius Server Secret	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
MAC address filter	Disable | Allow listed only | Allow all except listed; Default: **Disable**	**Allow listed only** – only allows devices with MAC addresses specified in the MAC list to connect to your WiFi network **Allow all except listed** - blocks devices with MAC addresses specified in the MAC list from connecting to your WiFi network
MAC	mac; Default: " "	List of MAC addresses to be included or excluded from connecting to your WiFi network
Key	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
Separate clients	yes | no; Default: **no**	Prevents WiFi clients from communicating with each other on the same subnet
Increase TTL packet size	yes | no; Default: **no**	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		
🛜	⦿	☐	WiFi (WAN)	DHCP	-		Edit	Scan
🖧	○	☑	Wired (WAN2)	Static	192.168.90.66	◆ ◆	Edit	
📡	○	☐	Mobile (WAN3)	None	188.69.245.225	◆ ◆	Edit	

Save

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	↑ ↓	Edit	Delete

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	3		↑ ↓	Delete
Wired	2		↑ ↓	Delete

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	⬆⬇ Edit Delete

[ ] 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	[0.0.0.0/0]
Destination port	[ ]
Protocol	[all ▼]
Policy assigned	[balanced ▼]

Field Name	Value	Description
Source address	ip; Default: **none**	Source IP address. Can be specified in CIDR notation (eg "192.168.1.0/24" without quotes).
Source port	number; Default: **none**	Source port number. May be entered as a single or multiple ports (eg "21" or "80,443" without quotes).
Destination address	ip; Default: **none**	Destination IP address. Can be specified in CIDR notation (eg "192.168.1.0/24" without quotes).
Destination port	number; Default: **none**	Destination port number. May be entered as a single or multiple ports (eg "21" or "80,443" without quotes).
Protocol	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.

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

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 1883

Enable Remote Access ☐

Field Name	Value	Description
Enable	yes | no; Default: **no**	Toggles MQTT Broker ON or OFF
Local Port	integer [0..65535]; Default: "1883"	Specifies the local port that the MQTT broker will listen to
Enable Remote Access	yes | no; Default: **no**	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.

Field Name	Value	Description
Use TLS/SSL	yes | no; Default: **no**	Toggles the use of TLS/SSL certificates ON or OFF
CA File	.ca file; Default: " "	**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
CERT File	.crt 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
Key File	.key file; Default: " "	Private key for client to establish connection
TLS version	tlsv1.1 | tlsv1.2 | Support all; Default: **Support all**	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.

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

Field Name	Value	Description
ACL File	.ACL file; Default: " "	The contents of this file are used to control client access to topics of the broker
Password File	password file; Default: " "	The Password file stores user names and corresponding passwords, used for authentication
Persistence	yes | no; Default: **no**	If enabled, connection, subscription and message data will be written to the disk. Otherwise, the data is stored in the router's memory only
Allow Anonymous	yes | no; Default: **yes**	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
Enable	yes | no; Default: **no**	Toggles the MQTT Publisher ON or OFF
Hostname	host | ip; Default: " "	Broker's IP address or hostname
Port	integer [0..65535]; Default: " "	Specifies the port used for connecting to the Broker
Username	string; Default: " "	User name used for authentication when connecting to the Broker
Password	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:

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

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

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.

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

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

	57600 | 115200; Default: **115200**	
Data bits	5 | 6 | 7 | 8; Default: **8**	The number of data bits for each character
Parity	None | Odd | Even; Default: **None**	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. **None** (**N**) - no parity method is used **Odd** (**O**) - the parity bit is set so that the number of "logical ones (1s)" has to be odd **Even** (**E**) - the parity bit is set so that the number of "logical ones (1s)" has to be even
Stop bits	1 | 2; Default: **1**	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
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.

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

Parity	None | Odd | Even; Default: **None**	The parity bit setting used for error detection during data transfer
Flow control	None | RTS- CTS | Xon-Xoff; Default: **None**	Specifies how many stop bits will be used to detect the end of character
Serial type	Console | Over IP | Modem | Modbus Gateway | NTRIP Client; Default: **Console**	Specifies the function of the serial interface
Interface	LAN | WAN | VPN | L2TP | PPTP | GRE | HOTSPOT | SSTP; Default: **LAN**	Interface used for connection
Allow IP	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	Over IP ▼
Protocol	TCP ▼
Mode	Server ▼
No leading zeros	☐
TCP port	
Timeout (s)	

Field Name	**Value**	**Description**
Protocol	TCP; Default: **TCP**	Specifies the protocol used in the communication process

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

Mode: Client

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

118

| **Reconnect intervals (s)** | integer; Default: " " | Indicates the time period between reconnection attempts |

Mode: Bidirect

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

Output	OC Output | Relay Output; Default: **OC Output**	Output to indicate that application switched from client (default) to server state
Output state	integer [0..1]; Default: **0**	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	Modem
Direct connect	
TCP port	
Initiation string	
No extra CR LF in response	☐

Field Name	Value	Description
Direct connect	host:port | ip:port; Default: " "	Maintains a constant connection to specified host. Leave empty to use an ATD command to initiate the connection
TCP port	integer [0..65535]; Default: " "	The port number used to listen for incoming connections. Leave it empty to disable incoming connections
Initiation string	string; Default: " "	A command string that will be sent to the modem to initiate it in some special way
No extra CR LF in response	yes | no; Default: **yes**	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
A	Answers incoming call	To answer incoming connection: ATA

D	Dial a number	To initiate data connection: ATD <host>:<port>
		To enter data mode with Direct connect settings: ATD
E	Local echo	Turn local echo on: ATE1
		Turn local echo off: ATE0
H	Hang up current call	To end data connection: ATH
O	Return to data mode	To return to data mode from command mode: ATO
Z	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	Modbus gateway ▾
Listening IP	0.0.0.0 ▾
Port	502
Slave ID configuration type	User defined ▾
Slave ID	1

Field Name	Value	Description
Listening IP	ip; Default: **0.0.0.0**	IP address on which the Modbus gateway will wait for incoming connections
Port	integer [0..65535]; Default: " "	The port number used to listen for incoming connections
Slave ID configuration type	User defined | Obtained from TCP; Default: **User defined**	Specifies whether slave IDs are user defined or automatically obtained from TCP
Slave ID | Permitted slave IDs	integer | range of integers; Default: **1**	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 *Slave ID configuration* field.

A range of IDs can be specified by placing a **hyphen** (**-**) between two integer numbers. For example, if you permitt 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.

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

| **Default NMEA string** | 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) |
| **Use device GPS** | yes \| no; Default: **no** | 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	TUN (tunnel)
Protocol	UDP
Port	1194
LZO	☐
Authentication	TLS
Encryption	BF-CBC 128 (default)
TLS cipher	All
Remote host/IP address	
Resolve retry	infinite
Keep alive	
Remote network IP address	
Remote network IP netmask	255.255.255.0
HMAC authentication algorithm	SHA1 (default)
Additional HMAC authentication	None
Extra options	
Use PKCS #12 format	☐
Certificate authority	Browse... No file selected.
Client certificate	Browse... No file selected.
Client key	Browse... No file selected.
Private key decryption password (optional)	

Field	Value	Description
Enable OpenVPN config from file	yes | no; default: **no**	Enables custom OpenVPN configuration from file.
Enable	yes | no; default: **no**	Turns the OpenVPN instance on or off.
TUN/TAP	TUN (tunnel) | TAP (bridged); default: **TUN (tunnel)**	Virtual network device type. • **TUN** - a virtual point-to-point IP link which operates at the network layer (OSI layer 3), used when routing is required.

		• **TAP** - a virtual Ethernet adapter (switch), operates at the data link layer (OSI layer 2), used when bridging is required.
Protocol	UDP | TCP; default: **UDP**	Transfer protocol used for the OpenVPN connection. • **Transmission Control Protocol** (**TCP**) - 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). • **User Datagram Protocol** (**UDP**) - 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).
Port	integer [0..65535]; default: **1194**	TCP/UDP port number used for the connection. Make sure it matches the port number specified on the server side. **NOTE**: traffic on the selected port will be automatically allowed in the router's firewall rules.
LZO	yes | no; default: **no**	Turns LZO data compression on or off.
Authentication	TLS | Static Key | Password | TLS/Password; default: **TLS**	Authentication mode, used to secure data sessions. • **Static key** is a secret key used for server–client authentication. • **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.

- **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: **BF-CBC 128**	
TLS: TLS cipher	All | DHE+RSA | Custom; default: **All**	Packet encryption algorithm cipher.
TLS: Allowed TLS ciphers	All | DHE+RSA | Custom; default: **All**	A list of TLS ciphers accepted for this connection.
Remote host/IP address	ip; default: **none**	IP address or hostname of an OpenVPN server.
Resolve retry	integer | infinite; default: **infinite**	In case server hostname resolve fails, this field indicates the amount of time (in seconds) to retry the resolve. Specify *infinite* to retry indefinitely.
Keep alive	two integers separated by a space; default: **none**	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 specfiied on the OpenVPN server, it overrides the 'keep alive' values set on client instances. **Example**: *10 120*
Static key: Local tunnel endpoint IP	ip; default: **none**	IP address of the local OpenVPN network interface.
Static key: Remote tunnel endpoint IP	ip; default: **none**	IP address of the remote OpenVPN network (server) interface.
Remote network IP address	ip; default: **none**	LAN IP address of the remote network (server).
Remote network IP netmask	netmask; default: **none**	LAN IP subnet mask of the remote network (server).
Password: User name	string; default: **none**	Username used for authentication to the OpenVPN server.
Password: Password	string; default: **none**	Password used for authentication to the OpenVPN server.

Extra options	string; default: **none**	Extra OpenVPN options to be used by the OpenVPN instance.
Use PKCS #12 format	yes | no; default: **no**	Use PKCS #12 archive file format to bundle all the members of a chain of trust.
PKCS #12 passphrase	string; default: **none**	Passphrase to decrypt PKCS #12 certificates.
PKCS #12 certificate chain	string; default: **none**	
TLS/**Password: HMAC authentication algorithm**	none | SHA1 | SHA256 | SHA384 | SHA512; default: **SHA1**	HMAC authentication algorithm type.
TLS/**Password: Additional HMAC authentication**	none | Authentication only (tls-auth) | Authentication and encryption (tls-crypt); default: **none**	An additional layer of HMAC authentication on top of the TLS control channel to protect against DoS attacks.
TLS/**Password: HMAC authentication key**	.key file; default: **none**	Uploads an HMAC authentication key file.
TLS/**Password: HMAC key direction**	0 | 1 | none; default: **1**	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.
TLS/**Password: Certificate authority**	.ca file; default: **none**	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.
TLS: Client certificate	.crt file; default: **none**	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.
TLS: Client key	.key file; default: **none**	Authenticates the client to the server and establishes precisely who they are.
TLS: Private key decryption password (optional)	string; default: **none**	A password used to decrypt the server's private key. Use only if server's .key file is encrypted with a password.
Static key: Static pre-shared key	.key file; default: **none**	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	TUN (tunnel)
Protocol	UDP
Port	1194
LZO	☐
Authentication	TLS
Encryption	BF-CBC 128 (default)
TLS cipher	All
Client to client	☐
Keep alive	10 120
Virtual network IP address	172.16.1.0
Virtual network netmask	255.255.255.0
Push option	route 192.168.1.0 255.25 ➕
Allow duplicate certificates	☐
HMAC authentication algorithm	SHA1 (default)
Additional HMAC authentication	None
Use PKCS #12 format	☐
Certificate authority	Browse... No file selected.
Server certificate	Browse... No file selected.
Server key	Browse... No file selected.
Diffie Hellman parameters	Browse... No file selected.
CRL file (optional)	Browse... No file selected.
Enable manual ccd upload	☐

Field	Value	Description
Enable OpenVPN config from file	yes | no; default: **no**	Enables custom OpenVPN configuration from file.
Enable	yes | no; default: **no**	Turns the OpenVPN instance on or off.
TUN/TAP	TUN (tunnel) | TAP (bridged); default: **TUN (tunnel)**	Virtual network device type. • **TUN** - a virtual point-to-point IP link which operates at the network

		layer (OSI layer 3), used when routing is required.
		• **TAP** - a virtual Ethernet adapter (switch), operates at the data link layer (OSI layer 2), used when bridging is required.
Protocol	UDP | TCP; default: **UDP**	Transfer protocol used for the connection. • **Transmission Control Protocol** (**TCP**) - 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). • **User Datagram Protocol** (**UDP**) - 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).
Port	integer [0..65535]; default: **1194**	TCP/UDP port number used for the connection. Make sure it matches the port number specified on the server side. **NOTE**: traffic on the selected port will be automatically allowed in the router's firewall rules.
LZO	yes | no; default: **no**	Turns LZO data compression on or off.
Authentication	TLS | Static Key | TLS/Password; default: **TLS**	Authentication mode, used to secure data sessions. • **Static key** is a secret key used for server–client authentication.

- **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-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 ;	Algorithm used for packet encryption.

	default: **BF-CBC 128**	
Static key: Local tunnel endpoint IP	ip; default: **none**	IP address of the local OpenVPN network interface.
Static key: Remote tunnel endpoint IP	ip; default: **none**	IP address of the remote OpenVPN network (client) interface.
Static key: Remote network IP address	ip; default: **none**	LAN IP address of the remote network (client).
Static key: Remote network IP netmask	netmask; default: **none**	LAN IP subnet mask of the remote network (client).
TLS/**TLS/Password: TLS cipher**	All | DHE+RSA | Custom; default: **All**	Packet encryption algorithm cipher.
TLS/Password: Allowed TLS ciphers	All | DHE+RSA | Custom; default: **All**	A list of TLS ciphers accepted for this connection.
TLS/**TLS/Password: Client to client**	yes | no; default: **no**	Allows OpenVPN clients to communicate with each other on the VPN network.
TLS/**TLS/Password: Keep alive**	two integers separated by a space; default: **none**	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 specifiied on the OpenVPN server, it overrides the 'keep alive' values set on client instances. **Example**: *10 120*
TLS/**TLS/Password: Virtual network IP address**	ip; default: **none**	IP address of the OpenVPN network.
TLS/**TLS/Password: Virtual network netmask**	netmask; default: **none**	Subnet mask of the OpenVPN network.
TLS/**TLS/Password: Push option**	OpenVPN options; default: **none**	Push options are a way to "push" routes and other additional OpenVPN options to connecting clients.
TLS/**TLS/Password: Allow duplicate certificates**	yes | no; default: **no**	When enabled allows multiple clients to connect using the same certificates.
Use PKCS #12 format	yes | no; default: **no**	Use PKCS #12 archive file format to bundle all the members of a chain of trust.
PKCS #12 passphrase	string; default: **none**	Passphrase to decrypt PKCS #12 certificates.

PKCS #12 certificate chain	string; default: **none**	
TLS/Password: User name	string; default: **none**	Username used for authentication to this OpenVPN server.
TLS/Password: Password	string; default: **none**	Password used for authentication to this OpenVPN server.
Static key: Static pre-shared key	.key file; default: **none**	Uploads a secret key file used for server–client authentication.
TLS/TLS/Password: Certificate authority	.ca file; default: **none**	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.
TLS/TLS/Password: Server certificate	.crt file; default: **none**	A type of digital certificate that is used to identify the OpenVPN server.
TLS/TLS/Password: Server key	.key file; default: **none**	Authenticates clients to the server.
TLS/TLS/Password: Diffie Hellman parameters	.pem file; default: **none**	DH parameters define how OpenSSL performs the Diffie-Hellman (DH) key-exchange.
TLS/TLS/Password: CRL file (optional)	.pem file | .crl file; default: **none**	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 acccepted by the CA and therefore cannot be authenticated to the server.
TLS/TLS/Password: Enable manual ccd upload	yes | no; default: **no**	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.

IPsec

IPsec Configuration	
Enable	☐
IKE version	IKEv1 ▾
Mode	Main ▾
Type	Tunnel ▾
On startup	Start ▾
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
Enable	yes | no; default: **no**	Turns the IPsec instance on or off.
IKE version	IKEv1 | IKEv2; default: **IKEv1**	Internet Key Exchange (IKE) version used for key exchange. • **IKEv1** - more commonly used but contains known issues, for example, dealing with NAT. • **IKEv2** - 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).
Mode	Main | Aggressive; default: **Main**	Internet Security and Key Management Protocol (ISAKMP) phase 1 exchange mode. • **Main** - performs three two-way exchanges between the initiator and the receiver (a total of 9 messages). • **Aggressive** - 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.
Type	Tunnel | Transport; default: **Tunnel**	Type of connection. • **Tunnel** - 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. • **Transport** - 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).

On startup	Ignore | Add | Route | Start; default: **Start**	Defines how the instance should act on router startup.
		• **Ignore** - does not start the tunnel. • **Add** - loads a connection without starting it. • **Route** - starts the tunnel only if there is traffic. • **Start** - starts the tunnel on router startup.
My identifier	ip | string; default: **none**	Defines how the user (IPsec instance) will be identified during authentication.
Tunnel: Local IP address/Subnet mask	ip/netmask | default: **none**	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.
Left firewall	off | on; default: **on**	Adds necessary firewall rules to allow traffic of this IPsec instance on this router.
Force encapsulation	yes | no; default: **no**	Forces UDP encapsulation for ESP packets even if a "no NAT" situation is detected.
Dead Peer Detection	yes | no; default: **no**	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 in unavailable and as failover mechanism.
Dead Peer Detection: Delay (sec)	integer; default: **none**	The frequency of checking whether a peer is still available or not.
Dead Peer Detection: Timeout (sec)	integer; default: **none**	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.
Authentication type	Pre-shared key | X.509; default: **Pre-shared key**	Here you can choose authentication type accordingly to your IPSec configuration
Certificate file	.crt file; default: **none**	Uploads a certificate file.

Key file	.key file; default: **none**	Uploads a key file.
CA certificate	.crt file; default: **none**	Uploads a Certificate authority (CA) file.
Remote participant's certificate	.crt file; default: **none**	Remote participant's certificate certificate is used to authenticate remote peer
Use additional xauth authentification	yes | no; default: **no**	Adds additional xauth authentication options.
Xauth: Xauth password	string; default: **none**	Password for additional peer authentication.
Remote VPN endpoint	host | ip; default: **none**	IP address or hostname of the remote IPsec instance.
Remote identifier	ip | string; default: **none**	Defines remote IPsec instance identification.
Tunnel: Remote IP address/subnet mask	ip/netmask; default: **none**	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.
Right firewall	yes | no; default: **yes**	Adds necessary firewall rules to allow traffic of from the opposite IPsec instance on this router.
Transport: Use with DMVPN	yes | no; default: **no**	Adds several necessary options to make DMVPN work.
Passthrough networks	None | LAN | Wired | WiFi | Mobile | custom; default: **none**	Select networks which should be passthrough and excluded from routing through tunnel
Enable keepalive	yes | no; default: **no**	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.
Host	host | ip; default: **none**	Hostname or IP address to which keep alive ICMP packets will be sent to.
Ping period (sec)	integer [0..9999999]; default: **none**	The frequency at which keep alive ICMP packets will be sent to the specified host or IP address.

Allow WebUI access	yes | no; default: **no**	Allows WebUI access for hosts in the VPN network.
Custom options	ipsec options; default: **none**	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:

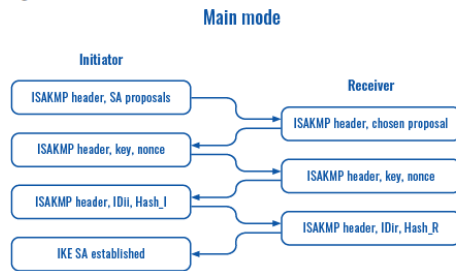| **Phase**	**Mode**	
Phase 1 - Establishes a secure channel between peers - Authenticates peers - Negotiates SA policy - Shares secret keys - Establishes secure tunnel for phase 2	Main mode (figure 1) - 6 packets exchanged - Identity protected during exchange	Aggressive mode (figure 2) - 3 packets exchanged - Identity information exchanged before a secure channel is established
Phase 2 - Sets up matching IPsec SAs - Periodically renegotiates IPsec SAs	Quick mode - 3 packets exchanged - IPsec SA parameters (ESP/AH, SHA/MD5) established - SA lifetime set	

Figure 1

Main mode

Initiator / Receiver

ISAKMP header, SA proposals
ISAKMP header, chosen proposal
ISAKMP header, key, nonce
ISAKMP header, key, nonce
ISAKMP header, IDii, Hash_I
ISAKMP header, IDir, Hash_R
IKE SA established

Figure 2

Aggressive mode

Initiator / Receiver

ISAKMP header, SA, key, nonce, IDii
ISAKMP header, SA, key, nonce, IDir, Hash_R
ISAKMP header, Hash_I
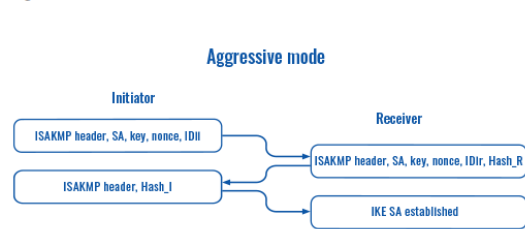IKE SA established

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): 8   Hours

Field	Value	Description
Encryption algorithm	DES | 3DES | AES128 | AES192 | AES256; default: **3DES**	Algorithm used for data encryption.
Authentication/Hash algorithm	MD5 | SHA1 | SHA256 | SHA384 | SHA512; default: **SHA1**	Algorithm used for exchanging authentication and hash information.
DH group/PFS group	MODP768 | MODP1024 | MODP1536 | MODP2048 | MODP3072 | MODP4096; default: **MODP1536**	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.
Lifetime	integer; default: **8 hours**	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:

Field	Value	Description
Pre-shared key	string; default: **none**	A shared password used for authentication between IPsec peers before a secure channel is established.
Secret's ID selector	string; default: **none**	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. **NOTE**: 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:

Field	Value	Description
Enable	yes | no; default: **no**	Turns the PPTP instance on or off.
Use as default gateway	yes | no; default: **no**	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. **NOTE**: this can only be used when WAN Failover is turned off.
Client to client	yes | no; default: **no**	Adds a route that makes other PPTP clients accessible within the PPTP network.

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

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

Remote IP range end	ip; default: **192.168.0.30**	PPTP IP address leases will end with the address specified in this field.
User name	string; default: **youruser**	Username used for authentication to this PPTP server.
Password	string; default: **yourpass**	Password used for authentication to this PPTP server.
PPTP Client's IP	ip; default: **none**	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:

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

		order to determine the health of the connection.
Default route	yes | no; default: **no**	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. **NOTE**: 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:

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

Remote IP range end	ip; default: **192.168.0.30**	L2TP IP address leases will end with the address specified in this field.
User name	string; default: **user**	Username used for authentication to this L2TP server.
Password	string; default: **pass**	Password used for authentication to this L2TP server.
L2TP Client's IP	ip; default: **none**	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.

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	dyn.com ▾
Lookup host	yourhost.example.com
Hostname	yourhost.example.com
User name	your_username
Password	•••••••••••• 👁
IP address source	Custom ▾
	Public, Private, Custom or Script IP source setting, will disable DNS rebinding protection
Network	WAN ▾
IP renew interval	10
Force IP renew	72

IP renew interval unit	Minutes ▾
Force IP renew unit	Minutes ▾

Field Name	Value	Description
Enable	yes | no; Default: **no**	Turns the DDNS instance ON or OFF
Use HTTP Secure	yes | no; Default: **no**	Enables SSL data encryption
Status	string; Default: **N/A**	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
Service	third party DNS service (chosen from list*) | -- custom --; Default: **dyn.com**	Third party DNS service provider
Lookup host	host; Default: **yourhost.example.com**	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 *nslookup/host* command)
Hostname	host; Default: **yourhost.example.com**	Hostname that will be linked with the router's IP address
Username	string; Default: **your_username**	User name required to login to the third party DNS service; used to periodically login to your DNS service account and make necessary updates.
Password	string; Default: **your_password**	Password required to login to the third party DNS service; used to periodically login to your DNS service account and make necessary updates.
IP address source	Custom | Public | Private | Script; Default: **Custom**	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

149

		interface, then you can send this exact IP to DDNS server by selecting **Private**
Network	LAN | WAN | WAN2 | WAN3 | PPP | PPP_USB ; Default: **WAN**	Specifies which interface's IP address should be bound to the hostname
IP renew interval	integer [5..600000]; Default: **10**	Frequency at which the device will check whether it's IP address has changed
IP renew interval unit	Minutes | Hours | Days; Default: **Minutes**	Unit which is used in IP renew interval
Force IP renew	integer [5..600000]; Default: **72**	Frequency at which IP update requests are sent to the DNS provider
Force IP renew unit	Minutes | Hours | Days; Default: **Minutes**	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
Enable	yes | no; Default: **no**	Turns SMS post/get ON or OFF
Username	string; Default: **user1**	User name used for authorization when sending post/get requests
Password	string; Default: **user_pass**	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 functionallity. 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
Enabled	yes | no; default: **no**	Turns the GPS service on or off.
Galileo NMEA support*	yes | no; default: **no**	Turns support for Galileo satellites on or off.
Glonass NMEA support*	yes | no; default: **no**	Turns support for Glonass satellites on or off.
BeiDou NMEA support*	yes | no; default: **no**	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
Enabled	yes | no; default: **no**	Turns NMEA forwarding on or off
Hostname	ip | host; default: **192.168.1.5**	IP address or hostname of the server to which NMEA data will be forwarded
Port	integer [0..65535]; default: **8500**	Port number off the server to which NMEA data will be forwarded
Protocol	TCP | UDP; default: **TCP**	Protocol that will be used to send NMEA data
Contain Connection	yes | no; default: **no**	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
Type	ram | flash; default: **ram**	Selects which type of memory will be used for storing NMEA forwarding cache.
Maximum sentences	integer; default: **5000**	Maximum amount of NMEA sentences that will be saved in the cache before older entries are deleted and replaced by new ones.
File	filepath; default: **none**	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
Enabled	yes | no; default: **no**	Turns NMEA sentence collecting on or off.
Location	filepath; default: **none**	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	☐	5	☐	5
GPGGA	☐	5	☐	5
GPVTG	☐	5	☐	5
GPRMC	☐	5	☐	5
GPGSA	☐	5	☐	5
GLGSV	☐	5	☐	5
GNGSA	☐	5	☐	5
GNGNS	☐	5	☐	5
GAGSV	☐	5	☐	5
PQGSV	☐	5	☐	5
PQGSA	☐	5	☐	5

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

NMEA sentence reference table:

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

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

Field	Value	Description
Enable	yes | no; default: **no**	Turns the Geofence rule on or off

Longitude (X)	degrees [-180.000000..180.000000]; default: **0.000000**	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.
Latitude (Y)	degrees [-90.000000..90.000000]; default: **0.000000**	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.
Radius	integer [1..999999]; default: **200**	Radius (in meters) of the geofence area.
Generate event on	Exit | Enter | Enter/exit; default: **Exit**	Specifies whether the rule should be triggered when the device enters the geofence area, leaves it or on both events.
Get current coordinates	- (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	Custom
Enable	✓
AP IP	192.168.2.254/24
Logout address	1.1.1.1
Authentication mode	External RADIUS
Authentication protocol	PAP
Terms of Service	✓
RADIUS server #1	
RADIUS server #2	
Authentication port	1812
Accounting port	1813
Radius secret key	
UAM port	3990
UAM UI port	4990
UAM secret	
NAS Identifier	
Swap octets	✓
Location name	
External landing page	✓
Landing page address	
Success URL	
HTTPS to landing page redirect	✓
SSL key file	Browse… No file selected.
SSL certificate file	Browse… No file selected.
Use custom DNS	✓
DNS server 1	8.8.8.8
DNS server 2	8.8.4.4

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

UAM secret	string; Default: " "	Shared secret between the UAM server and the Hotspot
NAS identifier	string; Default: " "	NAS-Identifier is one of the basic RADIUS attributes
Swap octets	yes | no; Default: **no**	Swaps the meaning of input octets and output as it relates to RADIUS attributes
Location name	string; Default: " "	Custom location name for your Hotspot
External landing page	yes | no; Default: **no**	Enables the use of an external landing page
Landing page address	string; Default: " "	A custom Hotspot's external landing page
Success URL	string; Default: " "	A custom redirect URL after successful Hotspot login
Protocol	HTTP | HTTPS; Default: **HTTP**	Connection protocol of your Hotspot
HTTPS to landing page redirect	yes | no; Default: **no**	Redirects HTTP pages to landing page
SSL key file	.key file; Default: " "	SSL key file used for authentication. This field becomes visible only if **HTTPS to landing page redirect** is enabled
SSL certificate file	.crt file; Default: " "	SSL certificate file used for authentication. This field becomes visible only if **HTTPS to landing page redirect** is enabled
Use custom DNS	yes | no; Default: **no**	Enables the use of custom DNS servers instead of your regular DNS
DNS server 1 | DNS server 2	ip; Default: " "	Additional DNS servers that are to be used by the Hotspot. These fields become visible only if **Use custom DNS** 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	Custom
Enable	✓
AP IP	192.168.2.254/24
Logout address	1.1.1.1
Authentication mode	Internal RADIUS
Terms of Service	✓
External landing page	✓
Landing page address	
Success URL	
HTTPS to landing page redirect	✓
SSL key file	Browse... No file selected.
SSL certificate file	Browse... No file selected.
Use custom DNS	✓
DNS server 1	8.8.8.8
DNS server 2	8.8.4.4

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 **Walled Garden** section. Used only with **External radius** Authentication mode.
Enable	yes | no; Default: **no**	Toggles Wi-Fi Hotspot ON or OFF
AP IP	ip; Default: **192.168.2.254/24**	Access Point IP address defines the IP address of your Hotspot's network
Logout address	host | ip; Default: **1.1.1.1**	An address that can be used by users to logout from the Hotspot session
Authentication mode	External radius | Internal radius | Without radius | Advertisement | MAC auth | SMS OTP; Default: **Without radius**	Authentication mode defines how users will connect to the Hotspot
Terms of service	yes | no; Default: **no**	If enabled, users have to agree to the Terms of service before logging in.

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

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 **Walled Garden** section. Used only with **External radius** Authentication mode.
Enable	yes | no; Default: **no**	Toggles Wi-Fi Hotspot ON or OFF
AP IP	ip; Default: **192.168.2.254/24**	Access Point IP address defines the IP address of your Hotspot's network
Logout address	host | ip; Default: **1.1.1.1**	An address that can be used by users to logout from the Hotspot session
Authentication mode	External radius | Internal radius | Without radius | Advertisement | MAC auth | SMS OTP; Default: **Without radius**	Authentication mode defines how users will connect to the Hotspot
Terms of service	yes | no; Default: **no**	If enabled, users have to agree to the Terms of service before logging in.

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

Users Configuration

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

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

Password	string; Default: " "	A custom password for the specified user name
Session Template	string; Default: **unlimited**	Session templates define session settings for different users. The **unlimited** 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	600
Session timeout	1800
Download bandwidth	10 Mbit/s ▾
Upload bandwidth	10 Kbit/s ▾
Download limit	250
Upload limit	250
Period	Month ▾
Start day	1 ▾

Field Name	Value	Description
Idle timeout	integer; Default: " "	A timeout in seconds after which idle users are automatically disconnected from the Hotspot. 0 means unlimited
Session timeout	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
Download bandwidth	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

Upload bandwidth	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
Download limit	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
Upload limit	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
Period	Month | Week | Day; Default: **Month**	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
Start day | Start hour	integer [1..31] | Monday..Sunday | integer [1..24]; Default: **day 1**	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	Custom
Enable	☐
AP IP	192.168.2.254/24
Authentication mode	Advertisement
Advertisement address	
HTTPS to landing page redirect	☑
SSL key file	Browse... No file selected.
SSL certificate file	Browse... 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 **Walled Garden** section. Used only with **External radius** Authentication mode.
Enable	yes | no; Default: **no**	Toggles Wi-Fi Hotspot ON or OFF
AP IP	ip; Default: **192.168.2.254/24**	Access Point IP address defines the IP address of your Hotspot's network
Authentication mode	External radius | Internal radius | Without radius | Advertisement | MAC auth | SMS OTP; Default: **Without radius**	Authentication mode defines how users will connect to the Hotspot
Advertisement address	host | ip; Default: " "	The address of the advertisement page that newly connected users will be redirected to
HTTPS to landing page redirect	yes | no; Default: **no**	Redirects HTTP pages to landing page
SSL key file	.key file; Default: " "	SSL key file used for authentication. This field becomes visible only if **HTTPS to landing page redirect** is enabled
SSL certificate file	.crt file; Default: " "	SSL certificate file used for authentication. This field becomes visible only if **HTTPS to landing page redirect** is enabled
Use custom DNS	yes | no; Default: **no**	Enables the use of custom DNS servers instead of your regular DNS
DNS server 1 | DNS server 2	ip; Default: " "	Additional DNS servers that are to be used by the Hotspot. These fields become visible only if **Use custom DNS** 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	Custom
Enable	✔
AP IP	192.168.2.254/24
Logout address	1.1.1.1
Authentication mode	MAC auth
Terms of Service	✔
Password protection	✔
Password	●●●●●●●●●●●●
Website access	Link
Protocol	HTTP
HTTPS redirect	✔
SSL key file	Choose File No file chosen
SSL certificate file	Choose 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
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 **Walled Garden** section. Used only with **External radius** Authentication mode.
Enable	yes | no; Default: **no**	Toggles Wi-Fi Hotspot ON or OFF

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

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

Logging

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

Wireless Hotspot Logging Settings

Field Name	Value	Description
Enable	yes | no; Default: **no**	Enables or disables whole logging section's fuctionality

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

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

FTP Server Settings

Enable	☐
Server address	your.ftp.server
User name	username
Password	••••••••
Port	21
File name extras	No extra information ▾

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

Hours   8

Minutes   15

Days   ☑ Monday
         ☑ Tuesday
         ☑ Wednesday
         ☑ Thursday
         ☑ Friday
         ☐ Saturday
         ☐ Sunday

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

Wifi Log

Events per page   10   Search

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 ▼	Search _____

Tel. Number ↑	Password ↑
▨▨▨▨▨▨▨▨▨	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	Teltonika Hotspot
Theme	Custom ▼
Upload login page	Choose File No file chosen
Login page file	Download
	Demo preview

☑ Terms Of Services
☑ Background Configuration
☑ Logo Image Configuration
☑ Link Configuration
☑ Text Configuration
☑ Button Configuration
☑ 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	☐
Remote access	☐
Accounting port	1813
Authentication port	1812

Field Name	Value	Description
Enable	yes | no; Default: **no**	Toggles Radius Server ON or OFF
Remote access	yes | no; Default: **no**	Toggles remote access to the Radius Server ON or OFF.
Accounting port	integer [0..65535]; Default: **1813**	Radius server accounting port
Authentication port	integer [0..65535]; Default: **1812**	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	600
Session timeout	1800
Download bandwidth	10 Mbit/s ▼
Upload bandwidth	10 Kbit/s ▼
Download limit	250
Upload limit	250
Period	Month ▼
Start day	1 ▼

Field Name	Value	Description
Idle timeout	integer; Default: " "	A timeout in seconds after which idle users are automatically disconnected from the Hotspot. 0 means unlimited
Session timeout	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
Download bandwidth	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
Upload bandwidth	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
Download limit	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
Upload limit	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
Period	Month | Week | Day; Default: **Month**	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
Start day | Start hour	integer [1..31] | Monday..Sunday | integer [1..24]; Default: **day 1**	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.

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

Clients Configuration Settings

Field Name	Value	Description
Enable	yes | no; Default: **yes**	Toggles Clients Configuration ON or OFF
Client name	string; Default: " "	A custom user name used to authenticate clients connecting to the Hotspot
IP address	ip; Default: " "	The IP address of the client
Netmask	integer [0..32]; Default: " "	The netmask of the client
Radius shared secret	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.
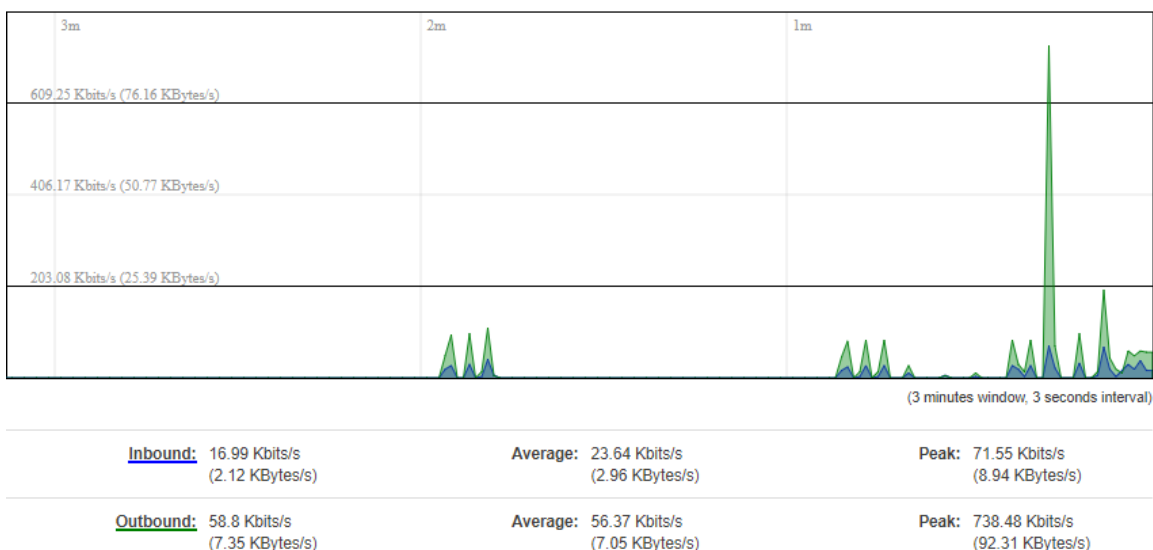
Hotspot Configuration

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

3m	2m	1m

609.25 Kbits/s (76.16 KBytes/s)

406.17 Kbits/s (50.77 KBytes/s)

203.08 Kbits/s (25.39 KBytes/s)

(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)
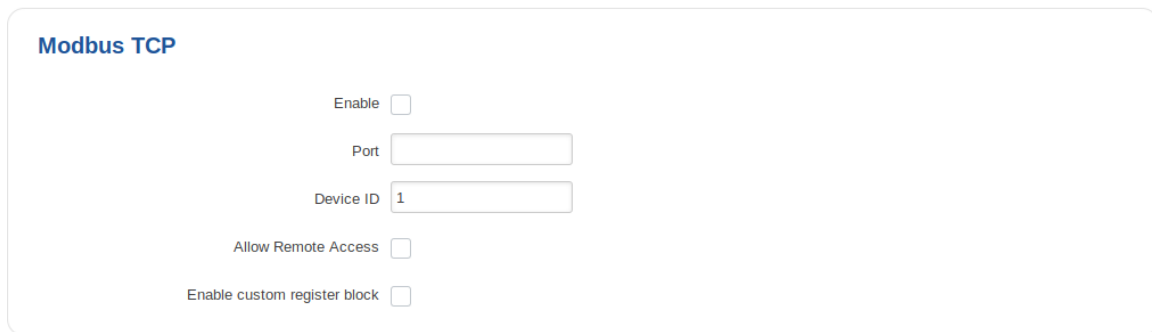
Modbus

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	1
Allow Remote Access	☐
Enable custom register block	☐

Field	Value	Description
Enable	yes | no; default: **none**	Turns Modbus TCP on or off.
Port	integer [0..65535]; default: **502**	TCP port used for Modbus communications.
Device ID	integer [0..255]; default: **1**	The device's Modbus slave ID. When set to 0, it will respond to requests addressed to any ID.
Allow Remote Access	yes | no; default: **no**	Allows remote Modbus connections by adding an exception to the device's firewall on the port specified in the field above.
Enable custom register block	yes | no; default: **no**	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
System uptime	1	2	2	32 bit unsigned integer
Mobile signal strength (RSSI in dBm)	3	4	2	32 bit integer
System temperature (in 0.1 °C)	5	6	2	32 bit integer
System hostname	7	8	16	Text
GSM operator name	23	24	16	Text
Router serial number	39	40	16	Text
LAN MAC address	55	56	16	Text
Router name	71	72	16	Text
Currently active SIM card slot	87	88	16	Text
Network registration info	103	104	16	Text
Network type	119	120	16	Text
Digital input (DIN1) state	135	136	2	32 bit integer
Digital galvanically isolated input (DIN2) state	137	138	2	32 bit integer
Current WAN IP address	139	140	2	32 bit unsigned integer
Analog input value	141	142	2	32 bit integer
GPS latitude coordinate	143	144	2	32 bit float
GPS longitude coordinate	145	146	2	32 bit float

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

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

Digital open collector output (4 PIN connector)	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
Digital output 1 (DOUT1) (ON/OFF*)	201	1 | 0	Changes the state of the open collector (OC) output
Digital output 2 (DOUT2) (ON/OFF*)	202	1 | 0	Changes the state of the relay output
Switch WiFi (ON/OFF*)	203	1 | 0	Turns WiFi ON or OFF
Switch mobile data connection (ON/OFF*)	204	1 | 0	Turns mobile data connection ON or OFF
Switch SIM card	205	1 | 2 | 0	Changes the active SIM card slot • 1 - switch to SIM1 • 2 - switch to SIM2 • 0 - switch from the the SIM card opposite of the one currently in use (SIM1 → SIM2 or SIM2 → SIM1)
Reboot	206	1	Reboots the router
Change APN	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: • 1 - to set APN for SIM1 • 2 - to set APN for SIM2

* 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:

Button	Description
Edit	Redirects you to the slave's configuration page
Delete	Deletes the slave configuration
Alarms	Redirects you to the slave's alarm configuration page
Clone	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	slave1
Slave ID	1
IP address	192.168.1.101
Port	503
Period	
Timeout	

Field	Value	Description
Enabled	yes | no; default: **no**	Turns communication with the slave device on or off.
Name	string; default: **none**	Slave device's name, used for easier management purposes.
Slave ID	integer [0..255]; default: **none**	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.
IP address	ip; default: **none**	Slave device's IP address.
Port	integer [0..65535]; default: **none**	Slave device's Modbus TCP port.
Period	integer [1..6400]; default: **none**	Interval at which requests are sent to the slave device.
Timeout	integer [1..30]; default: **none**	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:

Field	Value	Description
Name	string; default: **Unnamed Parameter**	Request name. Used for easier management purposes.
Data type	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: **16bit INT, high byte first**	How read data will be stored.
Function	1 | 2 | 3 | 4 | 5 | 6 | 15 | 16; default: **3**	A function code specifies the type of register being addressed by a Modbus request. The codes represent these functions: • **1** - read Coil Status • **2** - read Input Status • **3** - read Holding Registers • **4** - read Input Registers • **5** - force Single Coil • **6** - preset Single Register • **15** - force Multiple Coils • **16** - force Multiple Registers
First Register	integer [1..65536]; default: **1**	First Modbus register number from which data will be read. numbers, which value is +1 higher than address value.

Number of Registers	integer [1..2000]; default: **none**	Number of Modbus registers that will be read during the request.
Enabled	yes | no; default: **no**	Turns the request on or off.
Test	- (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.
Delete	- (interactive button)	Deletes the request.
Add	- (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:

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

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

Modbus Request: ID	integer [1..255]; default: **none**	Modbus slave ID.
Modbus Request: Modbus function	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: **Force Single Coil (5)**	A function code specifies the type of register being addressed by a Modbus request.
Modbus Request: First register	integer [0..65535]; default: **none**	Begins reading from the register specified in this field.
Modbus Request: Number of registers	integer [0..65535]; default: **none**	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
Enabled	yes | no; default: **no**	Turns Modbus RTU via RS232 on or off.
Baud rate	300 | 1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200; default: **19200**	Serial data transmission rate (in bits per second).
Data bits	5 | 6 | 7 | 8; default: **8**	Number of data bits for each character.
Parity	None | Even | Odd; default: **Even**	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. • **None** (**N**) - no parity method is used. • **Odd** (**O**) - the parity bit is set so that the number of "logical ones (1s)" has to be odd. • **Even** (**E**) - the parity bit is set so that the number of "logical ones (1s)" has to be even.
Stop bits	1 | 2; default: **1**	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.

Field	Value	Description
Enabled	yes | no; default: **no**	Turns Modbus RTU via RS485 on or off.

Baud rate	300 | 1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200; default: **19200**	Serial data transmission rate (in bits per second).
Data bits	5 | 6 | 7 | 8; default: **8**	Number of data bits for each character.
Parity	None | Even | Odd; default: **Even**	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. • **None** (**N**) - no parity method is used. • **Odd** (**O**) - the parity bit is set so that the number of "logical ones (1s)" has to be odd. • **Even** (**E**) - the parity bit is set so that the number of "logical ones (1s)" has to be even.
Stop bits	1 | 2; default: **1**	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.
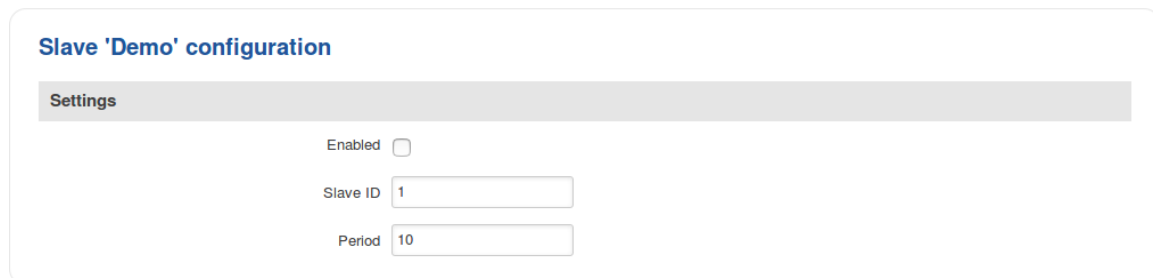
Slaves

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.

Field	Value	Description
Enabled	yes | no; default: **no**	Turns the slave on or off.
Slave ID	integer [1..255]; default: **1**	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.
Period	integer [1..9999]; default: **10**	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:

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

Field	Value	Description
Enabled	yes | no; default: **no**	Turns the alarm on or off.
Function	Read Coil | Read Discrete Input | Read Holding Registers | Read Input Registers; default: **Read Holding Registers**	Modbus function used in Modbus request.
Register	integer [1..65536]; default: **1**	Number of the Modbus coil/input/holding register/input register that will be read.
Condition	More than | Less than | Equal to | Not equal to; default: **More than**	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.
Value	integer [0..65535]; default: **0**	The value against which the read data will be compared.
Action	SMS | Trigger output | Modbus request; default: **SMS**	Action that will be taken if the condition is met. Possible actions: • **SMS** - sends and SMS message to a specified recipient(s). • **Trigger output** - changes the state of a specified output(s).

- **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:

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	{"ID":"%I", "TS":"%t","ST":"%s","VR":"%a"}

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	192.168.1.1
Period	50
Data filtering	All data ▾
Retry on fail	☐
Custom Header	⊞

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

Input/Output Status

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

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 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:

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.

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

203

| 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	Low level
Relay output	Contacts open
Digital output 4PIN	Low level

Field	Value	Description
Open collector output	Low level | High level; default: **Low level**	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	Turn on	
Digital relay output	Turn on	
Digital 4PIN output	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 [Digital OC output ▾]

Action [On ▾]

Action timeout ☐

Mode [Fixed ▾]

Hours [ ]

Minutes [ ]

Days ☐ Monday
☐ Tuesday
☐ Wednesday
☐ Thursday
☐ Friday
☐ Saturday
☐ Sunday

Field	Value	Description
Enable	yes | no; default: **no**	Turns the rule on or off.
Output	Digital OC Output | Digital 4PIN | Digital relay output; default: **Digital OC Output**	The output pin that will be be effected by the rule.
Action	On | Off; default: **On**	The action that will be performed on the output.
Action timeout	yes | no; default: **no**	Action timeout specifies whether an action should end after some time. For example, if action is set to *on* and timeout is set to 10, when the trigger occurs the output will turn on for 10 seconds before turning off.
Mode	Fixed | Interval; default: **Fixed**	When the rule will be triggered. • **Fixed** - triggers the specified action on a specified day(s), hour and minute. For example, every Sunday at 8:30 AM. • **Interval** - performs the action at an interval. For example, every 1 hour during Mondays.

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

System Section

UCR Administration

Summary

This page is an overview of the **Administration** section of UCR routers.

General

The **General** section is used to set up some of the router's managerial parameters, such as password, name, language, etc. For more information on the General section, refer to figure and table below.

Administration Settings

Router Name And Host Name

Router name	
Host name	

Administrator Password

Password requirements: Minimum 8 characters, at least one uppercase letter, one lowercase letter and one number.

Current password	
New password	
Confirm new password	

Language Settings

Language	English

IPv6 Support

Enable	

Login Page

Show mobile info at login page	
Show WAN IP at login page	

LEDs Indication

Enable	✔

Reset button configuration

Enabled	Min time	Max time	Action	
✔	0	5	Reboot	Delete
✔	6	11	User's defaults configuration	Delete
✔	12	20	Factory defaults configuration	Delete

Add

Restore Default Settings

Restore to User's defaults	Restore
Restore to Factory defaults	Restore

Field	Value	Description
Router name	string; default: **UCR**	The router's model name.
Host name	string; default: **UnitronicsUCR**	The router's hostname. This can be used for communication with other LAN hosts.
Current password	string; default: **none**	The router's current password.
New password | Confirm new password	string; default: **none**	A new password for the router. The password must be comprised of 8-32 characters, including at least one upper case letter, one lower case letter and one digit.
Language	English | Deutsch | Français | Turkish; default: **English**	Selects the router's WebUI language.
IPv6 Support	yes | no; default: **no**	Turns IPv6 support on or off.
Show mobile info at login page	yes | no; default: **no**	Shows mobile data connection information (signal strength, state, service mode) at login page.
Show WAN IP at login page	yes | no; default: **no**	Shows the router's WAN IP address at login page.
LEDs Indication	yes | no; default: **yes**	Turns the router's LED indications on or off.
Min time	integer [0..60]; default:**none**	Minimum time 0-60 (in seconds) that the button needs to be held to perform an action.
Max time	integer [0..59]; default:**none**	Maximum time 1-60 (in seconds) that the button can be held to perform an action, after which no action will be performed.
Action	Reboot|User's defaults configuration|Factory defaults configuration; default:**Reboot**	The action to be performed when this rule is met.
Restore to User's default	-(interactive button)	Restores the router to custom configuration set by the user.
Restore to Factory default's	-(interactive button)	Restores the router to manufacturer default settings.

Backup

The **Backup** page is used to generate the user's defaults configuration and download or upload backup files to the router.

User's Defaults Configuration

User's Defaults Configuration is used to create a custom default configuration that will be applied after resetting the device. The corresponding preset is automatically

generated according to the current router's configuration by pressing the 'Create' button.

With the help of this feature, the device can have two different default configuration presets:

- **User defaults** - custom configuration set by the user.
- **Factory defaults** - default configuration set by the manufacturer.

The device can be reset to selected default configuration by pressing and holding the reset button for a specified period of time.

Backup

User's Defaults Configuration

User's defaults configuration let's you create router's backup and then access it using reset button configuration located in System -> Administration -> General tab.

Created -

User's defaults configuration   Create   Remove

Important: the backup file does not contain **User's Defaults Configuration**.

Backup/Restore Configuration

The **Backup/Restore Configuration** sections are used to download or upload configuration backup files to the router. Backup files can be uploaded only from identical devices with identical or older firmware. Once a backup file is uploaded to a router, that router will have identical configuration as the router from which the backup file originated (was downloaded from).

Backup Configuration

Backup archive: Download

Restore Configuration

Restore from backup: Browse...   No file selected.

Upload archive

Only configuration file from identical device with same or lower firmware version (lowest 03.726) can be uploaded

- **Backup Configuration** - generates and downloads the router's backup file based on the current configuration.
- **Restore Configuration** - uploads a configuration backup file to the router. This can be done in two ways:

Important: backup files can be uploaded only when taken from a device with an identical **Product code** (can be checked in **Status → Device)** and identical or older firmware.