


Configuration - General

The basic setup of common settings.


- Protocol HUB
- Status
- Services
- Network
- Logout
- WCC Lite Tags

Protocol HUB

 Full Protocol HUB section is only available on “Cloud gateway” firmware type.
For “RTU” firmware type refer to Sequence of Events and Imported Signals subsections.



Protocol HUB section stores configuration for every connected device. There are three ways to configure these devices:

1. Manual configuration in Manage devices section.
2. Import settings from Excel file.
3. Remote configuration via CloudIndustries.eu.

 Any changes made in this section will take effect only after being applied. A notification with apply button will appear after making any changes.

Manage devices

MANAGE MASTER PROTOCOLS

<input type="checkbox"/>	Name	Description	Protocol	Enabled	
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	
<input type="checkbox"/>	IOMod-8AI		Modbus RTU	Yes	
<input type="checkbox"/>	IOMOD-8DI8DO		Modbus RTU	Yes	

Export selected

Delete selected

Create new device

Page size:

The “Manage Master Protocols” section displays a list of configured devices. Devices can be edited, removed, added and exported from this window.

 This functionality is only available on “Cloud gateway” firmware type.

Further device configuration is described below in “Manual device configuration” section.

Manual device configuration

Manual configuration allows to create fine tuned device configuration that can later be exported as a template.

Create new device: Device creation is performed by selecting it’s working protocol and configuring it’s name, slave address and communication settings. Existing device configuration is performed similary.

CREATE A NEW DEVICE

Fields with * are required.

Select protocol

Next

CREATE A NEW DEVICE

Fields with * are required.

Name *	<input type="text" value="IOMOD-8DI8DO"/>
Description	<input type="text" value="Input - Output module made by Elseta. Consists of 8 inputs and 8 outputs."/>
Alias (unique identifier)	<input type="text"/>
Enable	<input checked="" type="checkbox"/>
Event history size	<input type="text"/>
Modbus ID *	<input type="text" value="1"/>
ASCII mode *	<input type="checkbox"/>
Timeout (us) *	<input type="text" value="500000"/>
Port *	<input type="text" value="PORT1"/>
Baud rate *	<input type="text" value="9600"/>
Data bits *	<input type="text" value="8"/>
Stop bits *	<input type="text" value="1"/>
Parity *	<input type="text" value="None"/>
Flow control *	<input type="text" value="None"/>

Name: Device name to be used further in signals and events

Description: Short device description

Alias: An unique alphanumeric string that identifies this device. If alias is left blank, it will be generated automatically.

Enable: If disabled, configuration for this device will be ignored and it's measurements will not be updated.

Event history size: Number of device measurements to keep in events history. If this field is left blank, history is disabled.

Modbus ID: Modbus slave device unique identifier.

Modbus ASCII mode: Check to use Modbus ASCII mode. If left unchecked, RTU mode is used by default.

Timeout: Time limit to wait for a response from the device.

Port: Select port that device is connected to.

Communication settings: Serial port communication rate; Number of data bits; Number of stop bits; parity mode; flow control.

Manage jobs: A job is a software instruction to communicate with a device and get required data. Further data extraction is done with tags. Job creation and configuration is performed similarly.

NEW JOB

Fields with * are required.

Name	<input type="text"/>
Function	<input type="text" value="01: Read coil status"/>
Data address	<input type="text" value="0"/> bin hex dec
Number of coils/registers	<input type="text" value="0"/> bin hex dec
Retry Count	<input type="text" value="3"/>

Name: Job name

Description: Short device description

Function: A specific instruction to communicate with device. These instruction options are protocol specific.

Retry Count: This number indicates the retry limit when communication has failed.

When job is created and configuration is applied, WCC Lite immediately starts sending data requests to configured port. Tag settings needs to be configured for data extraction from job.

Manage tags: Tag is one measurement for a device. Tags contain information how to obtain required values from job data. Tag configuration is divided into two panes - "Tag settings" and "Advanced", the latter dedicated only for experienced users.

TAG SETTINGS

Fields with * are required.

Name *	<input type="text" value="First Input"/>
Type	<input type="text" value="Normal"/>
Alias (unique identifier)	<input type="text"/>
Enable	<input checked="" type="checkbox"/>
Record logs	<input type="checkbox"/>
Function	<input type="text" value="02: Read input status"/>
Data address	<input type="text" value="0"/> bin hex dec
Number of coils/registers	<input type="text" value="1"/> bin hex dec
Measurement unit	<input type="text" value="State"/>
Multiply value	<input type="text" value="1"/>
Add to value	<input type="text" value="0"/>

Name: Name for one measurement, e.g. "Temperature" or "Energy consumption".

Type: Tag type.

Alias: An unique alphanumeric string that identifies this device. If alias is left blank, it will be generated automatically.

Enable: If disabled, configuration for this tag will be ignored and measurements will not be updated.

Function: A specific instruction to communicate with device. These instruction options are protocol specific.

Measurement unit: Units to show for this measurement, e.g. V, W or kg.

Multiply value: Value to multiply by measurement. Use values below 1 to divide.

Add to value: Adds value to measurement. Use negative values to subtract.

ADVANCED

Integer mask (AND)

Add other tags values

Select tags to add

Source tags

Select tags to link

Source alarms

Select alarms to link

Minimum value

Maximum value

Threshold units

%

Absolute threshold

Integral threshold

Integral threshold interval (ms)

Suppression time (ms)

Suppression values

Data Type

Unsigned 16

Swap bytes (8)

☐

Swap words (16)

☐

Swap double words (32)

☐

Ignore in cloud

☐

Create

Measurement data format and parsing rules can be configured via the "Advanced" pane.

Name: Name for one measurement, e.g. "Temperature" or "Energy consumption"

Integer mask (AND):

Add other tags values:

Source tags:

Source alarms:

Minimum value:

Maximum value:

Threshold units:

Absolute threshold:

Integral threshold:

Integral threshold interval (ms):

Suppression time (ms):

Suppression values:

Data Type: Selects data type e.g. Float, signed / unsigned integer.

Swap bytes (8): changes byte sequence.

Swap words (16): changes word sequence.

Swap double words (32): changes double word sequence.

Ignore in cloud:

Port settings

EDIT PORT

Fields with * are required.

Scan rate (ms)

1000

Pool delay (ms)


200

Port mode

RS-485

Save

These options affect how device data polling is scheduled each port. These settings do not affect IEC 60870-5 protocols.

 This functionality is only available on “Cloud gateway” firmware type.

Scan rate: Time duration in milliseconds when all jobs on current port should be done. This option directly affects measurement update speed on one port. For example, if this value is set to 10 seconds, every measurement will be updated every 10 seconds if possible.

Poll delay: Minimum time delay in milliseconds to wait before sending any data on port. This is useful when devices fail to respond when data is transmitted too fast.

Port mode: Mode selection for port. WCC Lite has first port selectable between RS-232 and RS-485 interfaces.

Import

IMPORT CONFIGURATION FROM EXCEL FILE

Configuration file

Choose File

No file chosen


Insert not existing items

☒

Update existing items

☒

Import


 This functionality is only available on “Cloud gateway” firmware type.

Import new configuration from Excel file (.xls, .xlsx formats). If any errors in the file are found, device will not be imported and importing process will be stopped.

Insert: If this checkbox is selected, items that are not yet present in current configuration will be added. Otherwise new content will not be processed.

Update: If this checkbox is selected, any items that already exist in current configuration replaced with new configuration. Otherwise existing configuration will be left intact.

Signals

TAGS VALUES						
Device name	Name	Value	Status	Time		
I/O-Mod 88						
I/O-Mod 88	DI-1	OFF		2017-04-07 07:34:24		
I/O-Mod 88	DI-2	OFF		2017-04-07 07:34:24		
I/O-Mod 88	DI-3	OFF		2017-04-07 07:34:24		
I/O-Mod 88	DI-4	OFF		2017-04-07 07:34:24		
I/O-Mod 88	DI-5	OFF		2017-04-07 07:34:24		
I/O-Mod 88	DI-6	OFF		2017-04-07 07:34:24		
I/O-Mod 88	DI-7	OFF		2017-04-07 07:34:24		
I/O-Mod 88	DI-8	OFF		2017-04-07 07:34:24		
I/O-Mod 88	DO-1	ON		2017-04-07 07:34:24		
I/O-Mod 88	DO-2	OFF		2017-04-07 07:34:24		
I/O-Mod 88	DO-3	ON		2017-04-07 07:34:24		
I/O-Mod 88	DO-4	OFF		2017-04-07 07:34:24		
I/O-Mod 88	DO-5	OFF		2017-04-07 07:34:24		
I/O-Mod 88	DO-6	OFF		2017-04-07 07:34:24		
I/O-Mod 88	DO-7	OFF		2017-04-07 07:34:24		
I/O-Mod 88	DO-8	OFF		2017-04-07 07:34:24		
Refresh Page size: 20						

The “Tag Values” window displays a measurement list that contains information about tag states. Several columns can be sorted and filtered. By clicking the magnifying glass icon measurement history is shown (if recording is enabled).

 This functionality is only available on “Cloud gateway” firmware type.



Name: Device or tag label. Sorting and filtering can be applied.

Value: Latest measured value. Sorting and filtering can be applied.

Status: Any error flags are listed here.

Time: The time measurement was updated. Sorting can be applied.


Sequence of Events (SOE)

PROTOCOL HUB	STATUS	SYSTEM	SERVICES	NETWORK	USERS	LOGOUT			
CONFIGURATION	IMPORTED SIGNALS	EVENT LOG							
EVENT LOG									
Scada IEC104  Refresh									
Event time	Time	Dir	Type	Originator	Common address	COT	Address	Value	State
		<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
2018-04-09T11:30:15.21	2018-04-09T17:30:13.51	tx	M_DP_TB_1	0	1	Spontaneous data (3)	20801	1	
2018-04-09T11:30:12.19	2018-04-09T17:30:10.38	tx	M_DP_TB_1	0	1	Spontaneous data (3)	20801	2	
2018-04-09T11:28:54.43	2018-04-09T14:28:51.54	tx	M_DP_TB_1	0	1	Spontaneous data (3)	20801	1	
2018-04-09T11:28:08.96	2018-04-09T14:28:06.61	tx	M_DP_TB_1	0	1	Spontaneous data (3)	20801	2	
2018-04-09T11:28:04.95	2018-04-09T14:28:02.24	tx	M_DP_TB_1	0	1	Spontaneous data (3)	20801	1	
2018-04-09T11:27:55.89	2018-04-09T11:27:55.88	tx	C_CS_NA_1	0	1	Command activation ACK (7)	0		
2018-04-09T11:27:55.87	2018-04-09T11:27:55.88	rx	C_CS_NA_1	0	1	Command activation (6)	0		
2018-04-09T11:27:47.91	2018-04-09T14:27:46.59	tx	M_SP_TB_1	0	1	Spontaneous data (3)	20416	1	
2018-04-09T11:27:46.90	2018-04-09T14:27:45.97	tx	M_SP_TB_1	0	1	Spontaneous data (3)	20415	1	
2018-04-09T11:27:46.89	2018-04-09T14:27:45.48	tx	M_SP_TB_1	0	1	Spontaneous data (3)	20414	1	
2018-04-09T11:27:45.88	2018-04-09T14:27:44.86	tx	M_SP_TB_1	0	1	Spontaneous data (3)	20413	1	
2018-04-09T11:27:45.88	2018-04-09T14:27:44.38	tx	M_SP_TB_1	0	1	Spontaneous data (3)	20412	1	
2018-04-09T11:27:44.98	2018-04-09T11:27:44.98	tx	C_CS_NA_1	0	1	Command activation ACK (7)	0		

SOE is the time-stamped status data. SOE allows to review latest events and changes for device's state changes in chronological order. Newest events are shown at the top of the list. WCC Lite will time-stamp the status data with a time resolution of one millisecond.

Initially, all breakers, protection contacts digital status input points in the WCC Lite; events captured from IEDs shall be configured as SOE points. It's possible to assign any digital status input data point in the WCC Lite as SOE point with Excel template during configuration.

Each time a device changes state, the WCC Lite will save it with time-tag in internal storage. WCC Lite will maintain a SOE buffer within the configured history size limitations.

 Events are recorded only for devices that have Event history size field set. When log size exceeds its limit, oldest records are deleted.

Imported signals

Imported signals section shows basic information about applied configuration. This section is view only. For signals and their states refer to “Protocol Hub” section “Signals”

Status

Overview

System

SYSTEM	
Hostname	wcc-lite
Model	Elseta WCC Lite board
Firmware Version	OpenWrt Designated Driver 1.2.13-rtu 50167 / LuCI Master (git-19.190.32138-694c7fd)
Kernel Version	4.4.14
Local Time	Thu Jul 11 08:32:15 2019
Uptime	0h 1m 39s
Load Average	1.05, 0.46, 0.17

System section in status tab shows basic information about current status of the system.

Hostname: The label that is used to identify the device in the network.

Model: Model of the device.

Firmware version: Current firmware version.

Kernel version: Current kernel version.

Local Time: Current local time.

Uptime: The time a device has been working.

Load average: Measure CPU utilization of the last 1, 5, and 15 minute periods. Load of 0.5 means the CPU has been 50% utilized over the last period. Values over 1.0 mean the system was overloaded.

Memory

MEMORY	
Total Available	11652 kB / 60388 kB (19%)
Free	2016 kB / 60388 kB (3%)
Buffered	9636 kB / 60388 kB (15%)

The "Memory" window provides memory usage information on the device.

Total available memory: The amount of available memory that could be used over installed physical memory.

Free: The amount of physical memory that is not currently in use over installed physical memory.

Buffered: The amount of buffered memory that is currently in use for active I/O operations over installed physical memory.

Network

NETWORK	
IPv4 WAN Status	Type: dhcp Address: 192.168.0.108 Netmask: 255.255.255.0 Gateway: 192.168.0.1 DNS 1: 192.168.0.1 Expires: 1h 58m 49s Connected: 0h 1m 11s
IPv6 WAN Status	Not connected
Active Connections	94 / 16384 (0%)

IPv4 WAN, IPv6 WAN status and active connections of the device.

Type: Type of addressing of IPv4 network interface - DHCP or static.

Address: IP address of the device.

Netmask: Netmask of the device.

Gateway: IP address of the Gateway.

DNS: IP address of DNS server.

Expires: DHCP lease expiration time of the connection.

Connected: The time a device has been connected.

Active Connections: The number of the active connections with the device.

DHCP leases

DHCP LEASES			
Hostname	IPv4-Address	MAC-Address	Leasetime remaining
There are no active leases.			

DHCPV6 LEASES			
Host	IPv6-Address	DUID	Leasetime remaining
?	fd74:8536:7bae::33f/128	00046836d59efa382760f3193e5ec5bf4a24	11h 58m 53s

DHCPv4 and DHCPv6 lease expiration time.

Hostname: The label that is used to identify the device in the network.

IPv4-Address: IPv4 address of network interface.

MAC-Address: The media access control address of IPv4 network interface.

DUID: DHCP Unique Identifier of IPv6 network interface.

Lease Time remaining: The amount of time the device will be allowed connection to the Router.

Wireless

WIRELESS	
Generic 802.11bgn Wireless Controller (radio0)	<div><div><div>0%</div><div></div></div><div><div>SSID: WCC Lite</div><div>Mode: Master</div><div>Channel: 11 (2.462 GHz)</div><div>Bitrate: ? Mbit/s</div><div>BSSID: C6:93:00:0E:C4:33</div><div>Encryption: None</div></div></div>
	<div><div><div>60%</div><div></div></div><div><div>SSID: AP5</div><div>Mode: Client</div><div>Channel: 11 (2.462 GHz)</div><div>Bitrate: 6.5 Mbit/s</div><div>BSSID: 02:1A:11:FF:87:09</div><div>Encryption: WPA2 PSK (CCMP)</div></div></div>

WiFi interface information window.

SSID: The sequence of characters that uniquely names a wireless local area network.

Mode: Shows how the device is connected to the wireless network – Master or Client.

Channel: The number of channel and radio frequency for connection to access point.

Bitrate: The number of bits that pass the device in a given amount of time.

BSSID: The MAC address of the wireless access point.

Encryption: Security protocol for the wireless network.

Associated stations

ASSOCIATED STATIONS					
	Network	MAC-Address	Host	Signal / Noise	RX Rate / TX Rate
 wlan0	Client "AP5"	02:1A:11:FF:87:09	192.168.43.1	 -71 / -95 dBm	1.0 Mbit/s, 20MHz 6.5 Mbit/s, 20MHz, MCS 0

List of associated stations (clients).

Network: Mode and SSID of network point.

MAC-Address: The media access control address of IPv4 network interface.

Hostname: The label or IP address that is used to identify the device in the network.

Signal/Noise: Received signal level over the background noise level. -30 dBm is the maximum achievable signal strength, -70 dBm is the minimum signal strength for reliable packet delivery in the wireless network.

RX Rate/TX rate: Used measure data transmission in the wireless network over bandwidth. RX Rate represents the rate at which data packets being received by the device, TX Rate represents the rate at which data packets being sent from the device.

Board information

BOARD INFORMATION	
Hardware version	WCCLite v1.3
Serial number	318040040
SoC ID	c493000bf455

Board information provides the following details:

Hardware version: Current hardware version;
Serial number: Serial number of the board;
SoC ID: Unique identifier of CPU unit;

Firewall

IPv4 Firewall

IPv4 Firewall

IPv6 Firewall

Table: Filter

Chain INPUT (Policy: ACCEPT, Packets: 0, Traffic: 0.00 B)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
576	38.25 KB	ACCEPT	all	lo	*	0.0.0.0/0	0.0.0.0/0	/* !fw3 */
1038	217.50 KB	input_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	/* !fw3: user chain for input */
985	214.56 KB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED /* !fw3 */
42	2.46 KB	syn_flood	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02 /* !fw3 */
53	2.94 KB	zone_lan_input	all	br-lan	*	0.0.0.0/0	0.0.0.0/0	/* !fw3 */
0	0.00 B	zone_wan_input	all	eth1	*	0.0.0.0/0	0.0.0.0/0	/* !fw3 */

Firewall rule list for IPv4 traffic.
Table: The four distinct tables which store rules regulating operations on the packet. Filter concerns filtering rules. NAT concerns translation of source or destination addresses and ports of packages. Mangle table is for specialized packet alteration. The raw table is for configuration exceptions.

Chain: The list of rules. Filter table has the following built-in chains: Input – concerns packets whose destination is the firewall itself, Forward – concerns packets transiting through the firewall, Output – concerns packets emitted by the firewall, Reject – reject the packet, Accept – allow the packet to go on its way. NAT table has the following built-in chains: Prerouting – to modify packets as soon as they arrive, Postrouting – to modify packets when they are ready to go on their way. Mangle table has one built-in chain: Forward for transiting packets through the firewall.

Pkts.: The packets processed by the firewall.

Traffic: The amount of data processed by the firewall.

Target: The chain of the table of the firewall.

Prot.: The transport layer protocol processed by the firewall.

In: The network interface for the input chain processed by the firewall.

Out: The network interface for the output chain processed by the firewall.

Source: IPv4 address of the device that the packet comes from.

Destination: IPv4 address of the device that the packet goes to.

Options: The options for configuring the firewall.

IPv6 Firewall

IPv4 Firewall

IPv6 Firewall

Table: Filter

Chain INPUT (Policy: ACCEPT, Packets: 0, Traffic: 0.00 B)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
0	0.00 B	ACCEPT	all	lo	*	:::0	:::0	/* !fw3 */
8041	684.54 KB	input_rule	all	*	*	:::0	:::0	/* !fw3: user chain for input */
32	3.08 KB	ACCEPT	all	*	*	:::0	:::0	ctstate RELATED,ESTABLISHED /* !fw3 */

Firewall rule list for IPv6 traffic.

Table: The three distinct tables which store rules regulating operations on the packet. Filter concerns filtering rules. Mangle table is for specialized packet alteration. The raw table is for configuration exceptions.

Chain: The list of rules. Filter table has the following built-in chains: Input – concerns packets whose destination is the

firewall itself, Forward – concerns packets transiting through the firewall, Output – concerns packets emitted by the firewall, Reject – reject the packet, Accept – allow the packet to go on its way. Mangle table has one built-in chain: Forward for transiting packets through the firewall.

Pkts.: The packets processed by the firewall.

Traffic: The amount of data processed by the firewall.

Target: The chain of the table of the firewall.

Prot.: The transport layer protocol processed by the firewall.

In: The network interface for the input chain processed by the firewall.

Out: The network interface for the output chain processed by the firewall.

Source: IPv6 address of the device that the packet comes from.

Destination: IPv6 address of the device that the packet goes to.

Options: The options for configuring the firewall.

Routes

ARP				
IPv4-Address	MAC-Address	Interface		
192.168.2.2	f0:76:1c:3b:cb:13	br-lan		

ACTIVE IPV4-ROUTES				
Network	Target	IPv4-Gateway	Metric	Table
lan	192.168.2.0/24		0	main

ACTIVE IPV6-ROUTES				
Network	Target	Source	Metric	Table
lan	fd74:8536:7bae::/64		1024	main
lan	ff00::/8		256	local

IPV6 NEIGHBOURS		
IPv6-Address	MAC-Address	Interface

The routing tables provide information on how datagrams are sent to their destinations.

ARP: An address Resolution Protocol which defines how IP address is converted to a physical hardware address needed to deliver packets to the devices.

Interface: The type of Network interface. br-lan refers to the virtual bridged interface: to make multiple network interfaces act as if they were one network interface.

Network: The type of network through which the traffic will be sent to the destination subnet.

Target: An address of the destination network. The prefix /24 refers the subnet mask 255.255.255.0.

IPv4-Gateway: IP address of the gateway to which traffic intended for the destination subnet will be sent.

Metric: The number of hops required to reach destinations via the gateway.

Table: The type of routing tables: main (default), local (maintained by the kernel).

IPv6 Neighbours: The devices on the same network with IPv6 addresses.

System Log

#	Time	Facility	Process	Priority	Message
1	Sat Mar 30 08:57:04 2019	local0	gsm-pinger	info	network unreachable, resetting modem
2	Sat Mar 30 08:57:04 2019	daemon	pppd[14918]	info	Terminating on signal 15
3	Sat Mar 30 08:57:04 2019	daemon	pppd[14918]	info	Connect time 5.0 minutes.
4	Sat Mar 30 08:57:04 2019	daemon	pppd[14918]	info	Sent 272 bytes, received 3180 bytes.
5	Sat Mar 30 08:57:04 2019	daemon	netifd	notice	Network device 'ublox-gsm' link is down
6	Sat Mar 30 08:57:04 2019	daemon	netifd	notice	Network alias 'ublox-gsm' link is down
7	Sat Mar 30 08:57:04 2019	daemon	netifd	notice	Interface 'gsm_6' has link connectivity loss
8	Sat Mar 30 08:57:04 2019	kern	kernel	info	[154912.796479] usb 1-1.1: USB disconnect, device number 126
9	Sat Mar 30 08:57:04 2019	kern	kernel	err	[154912.800748] cdc_acm 1-1.1:2: failed to set dtr/rts
10	Sat Mar 30 08:57:04 2019	daemon	pppd[14918]	notice	Modem hangup
11	Sat Mar 30 08:57:04 2019	daemon	pppd[14918]	notice	Connection terminated.
12	Sat Mar 30 08:57:04 2019	daemon	netifd	notice	Interface 'gsm_6' is now down
13	Sat Mar 30 08:57:04 2019	daemon	netifd	notice	Interface 'gsm_6' is disabled
14	Sat Mar 30 08:57:04 2019	daemon	dnsmasq[2046]	info	reading /tmp/resolv.conf.auto
15	Sat Mar 30 08:57:04 2019	daemon	dnsmasq[2046]	info	using local addresses only for domain lan
16	Sat Mar 30 08:57:04 2019	daemon	dnsmasq[2046]	info	using nameserver 192.168.67.1#53
17	Sat Mar 30 08:57:04 2019	daemon	dnsmasq[2046]	info	using nameserver fe80::c693:ff:fe0b:ae28%eth1#53
18	Sat Mar 30 08:57:05 2019	daemon	pppd[14918]	info	Exit.
19	Sat Mar 30 08:57:05 2019	daemon	netifd	notice	Interface 'gsm' is now down
20	Sat Mar 30 08:57:05 2019	local0	gsm	info	Modem was reset
21	Sat Mar 30 08:57:06 2019	kern	kernel	info	[154914.314857] usb 1-1.1: new high-speed USB device number 127 using ehci-platform
22	Sat Mar 30 08:57:08 2019	kern	kernel	info	[154916.380202] usb 1-1.1: USB disconnect, device number 127
23	Sat Mar 30 08:57:10 2019	kern	kernel	info	[154918.914874] usb 1-1.1: new high-speed USB device number 3 using ehci-platform
24	Sat Mar 30 08:57:10 2019	kern	kernel	info	[154919.070028] cdc_acm 1-1.1:1.0: ttyACM0: USB ACM device
25	Sat Mar 30 08:57:10 2019	kern	kernel	info	[154919.075447] cdc_acm 1-1.1:1.2: ttyACM1: USB ACM device
26	Sat Mar 30 08:57:10 2019	kern	kernel	info	[154919.084318] cdc_acm 1-1.1:1.4: ttyACM2: USB ACM device
27	Sat Mar 30 08:57:11 2019	kern	kernel	info	[154919.093522] cdc_acm 1-1.1:1.6: ttyACM3: USB ACM device
28	Sat Mar 30 08:57:11 2019	kern	kernel	info	[154919.103248] cdc_acm 1-1.1:1.8: ttyACM4: USB ACM device
29	Sat Mar 30 08:57:11 2019	kern	kernel	info	[154919.109495] cdc_acm 1-1.1:1.10: ttyACM5: USB ACM device
30	Sat Mar 30 08:57:16 2019	daemon	netifd	notice	Interface 'gsm' is setting up now
31	Sat Mar 30 08:57:18 2019	daemon	netifd	notice	gsm (19093): SIM ready
32	Sat Mar 30 08:57:18 2019	daemon	netifd	notice	gsm (19093): pin_check 0
33	Sat Mar 30 08:57:18 2019	daemon	netifd	notice	gsm (19093): pin_status -> 0
34	Sat Mar 30 08:57:19 2019	daemon	netifd	notice	gsm (19093): sending -> AT+COPS=2
35	Sat Mar 30 08:57:20 2019	daemon	pppd[19260]	notice	pppd 2.4.7 started by root, uid 0

System log window shows a table containing the events that are logged by the device. It has the following columns:

- # (sequence number);
- Time (day of the week, month, day of the month, time and year);
- facility;
- process (who generated the message);
- priority level;
- message.

Messages can be sorted and filtered to extract a particular set of messages. This might be useful when debugging kernel or protocol level problems.

Kernel Log

```
[ 0.000000] Linux version 4.4.14 (paulius@paulius-desktop) (gcc version 5.3.0 (OpenWrt GCC 5.3.0 50087) ) #15 Mon Mar 27 14:57:19 UTC 2017
[ 0.000000] MyLoader: sysp=23fff3b3, boardp=137b7fb7, parts=70537976
[ 0.000000] bootconsole [early0] enabled
[ 0.000000] CPU0 revision is: 00019374 (MIPS 24Kc)
[ 0.000000] SoC: Atheros AR9330 rev 1
[ 0.000000] Determined physical RAM map:
[ 0.000000] memory: 04000000 @ 00000000 (usable)
[ 0.000000] Initrd not found or empty - disabling initrd
[ 0.000000] No valid device tree found, continuing without
[ 0.000000] Zone ranges:
[ 0.000000] Normal [mem 0x0000000000000000-0x0000000003ffffff]
[ 0.000000] Movable zone start for each node
[ 0.000000] Early memory node ranges
[ 0.000000] node 0: [mem 0x0000000000000000-0x0000000003ffffff]
[ 0.000000] Initmem setup node 0 [mem 0x0000000000000000-0x0000000003ffffff]
```

Kernel log shows a list of the events that are logged by the kernel of the device. Log format: time in seconds since the kernel started and message.

Processes

PID	Owner	Command	CPU usage (%)	Memory usage (%)	Hang Up	Terminate	Kill
1	root	/sbin/procd	8%	3%	Hang Up	Terminate	Kill
2	root	[kthreadd]	0%	0%	Hang Up	Terminate	Kill
3	root	[ksoftirqd/0]	0%	0%	Hang Up	Terminate	Kill
5	root	[kworker/0:0H]	0%	0%	Hang Up	Terminate	Kill
67	root	[writeback]	0%	0%	Hang Up	Terminate	Kill
68	root	[crypto]	0%	0%	Hang Up	Terminate	Kill
70	root	[bioset]	0%	0%	Hang Up	Terminate	Kill
71	root	[kblockd]	0%	0%	Hang Up	Terminate	Kill
73	root	[kswapd0]	0%	0%	Hang Up	Terminate	Kill
152	root	[fsnotify_mark]	0%	0%	Hang Up	Terminate	Kill
169	root	[spi0]	0%	0%	Hang Up	Terminate	Kill
180	root	[bioset]	0%	0%	Hang Up	Terminate	Kill
185	root	[bioset]	0%	0%	Hang Up	Terminate	Kill

List of processes running on the system.

PID: Process ID.

Owner: User to whom the process belongs.

Command: Process.

CPU usage: It is CPU usage of the individual process. CPU usage above 90 % is an indicator of insufficient processing power.

Memory usage: Memory usage of the individual process.

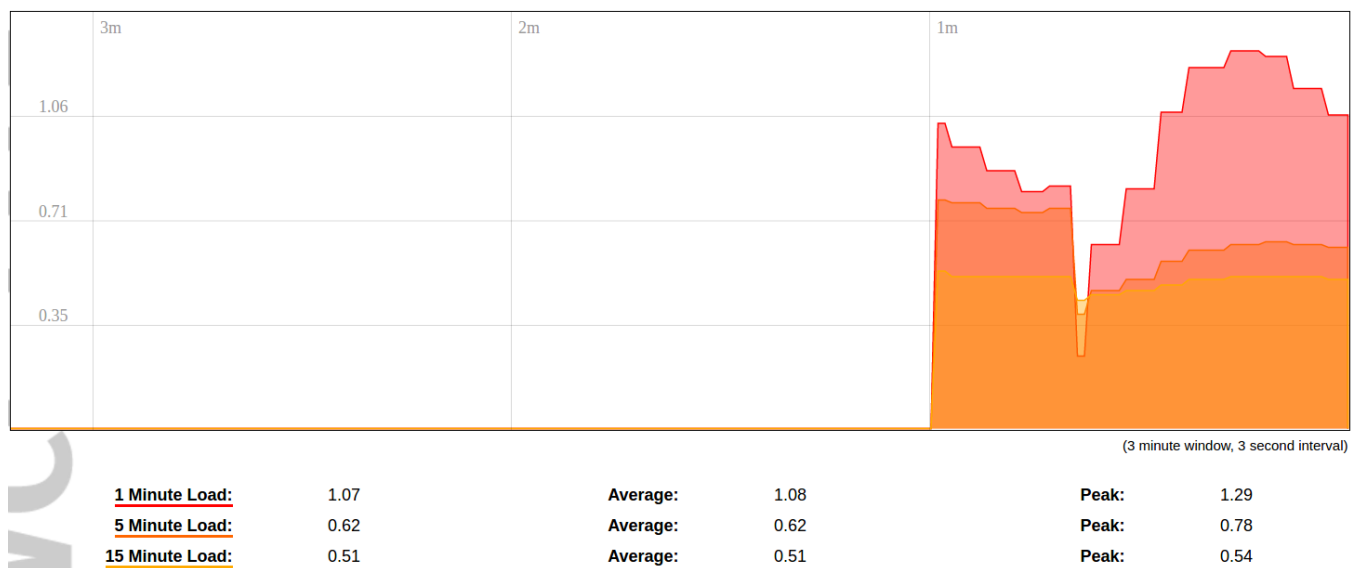
Hang Up: To freeze the process.

Terminate: To end the process cleanly.

Kill: To end the process immediately.

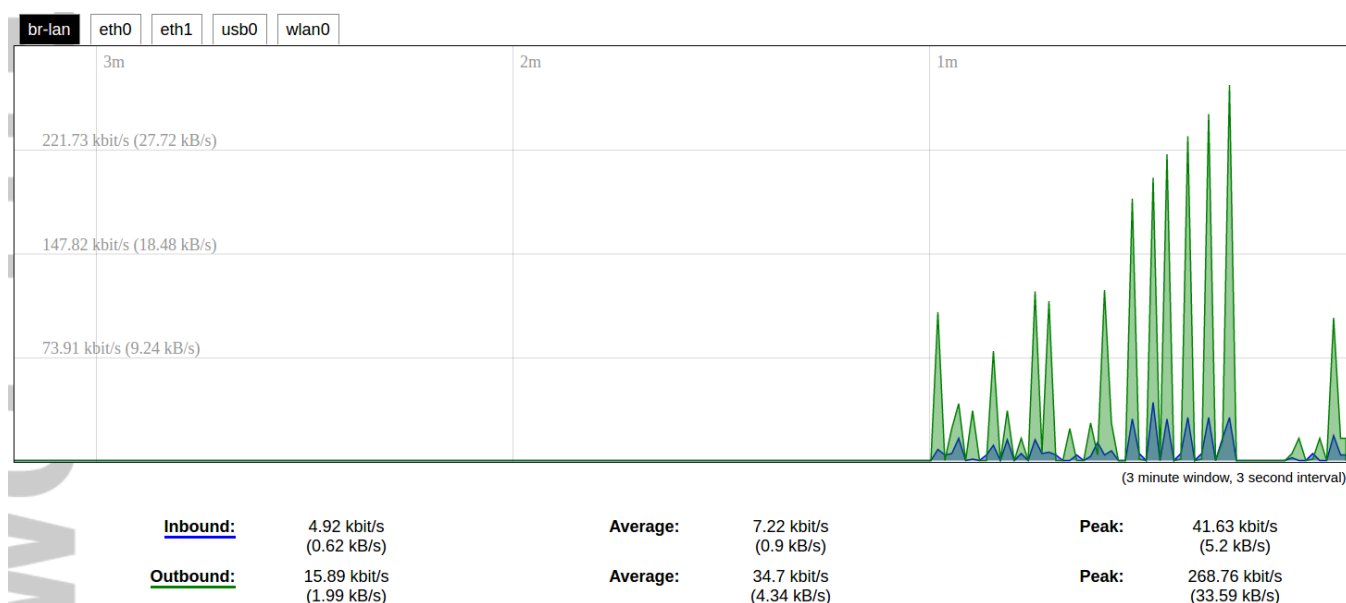
Realtime graph

Realtime Load



CPU utilization graph. Load of 0.5 means the CPU has been 50% utilized over the last period. Values over 1.0 mean the system was overloaded.

Realtime Traffic



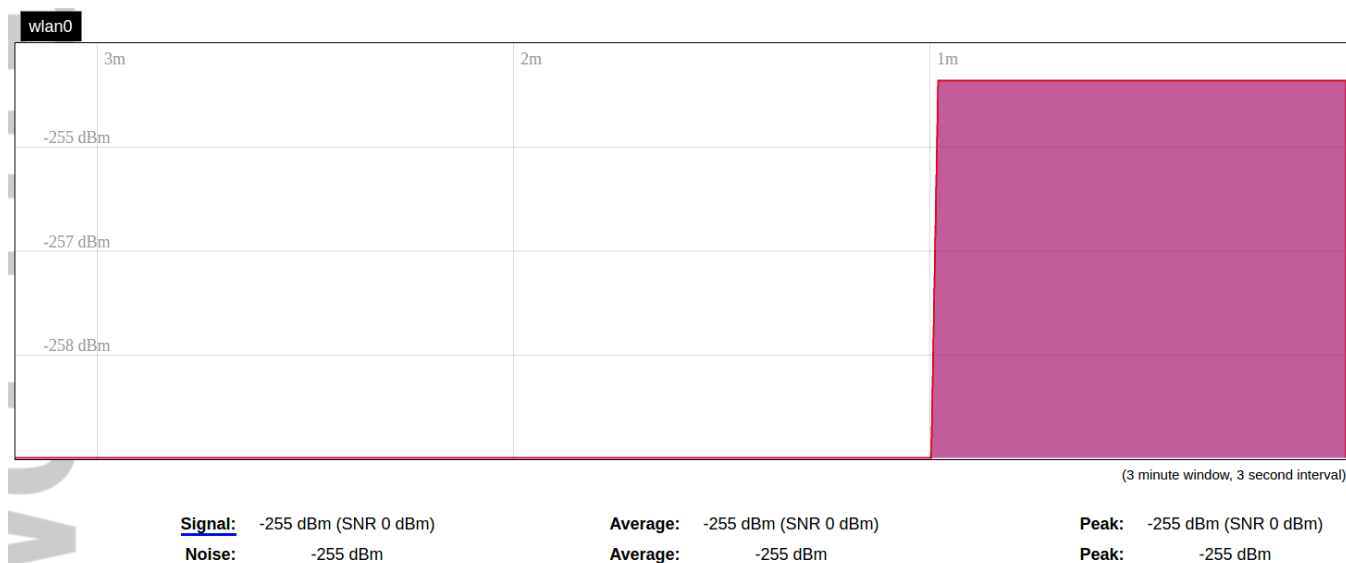
Graphs representing the status of the virtual and physical network interfaces of the device.

Inbound: The speed at which the incoming packets arrive at the device.

Outbound: The speed of the packets which were originated by the device.

Phy. Rate: The speed at which bits can be transmitted over the physical layer.

Realtime Wireless



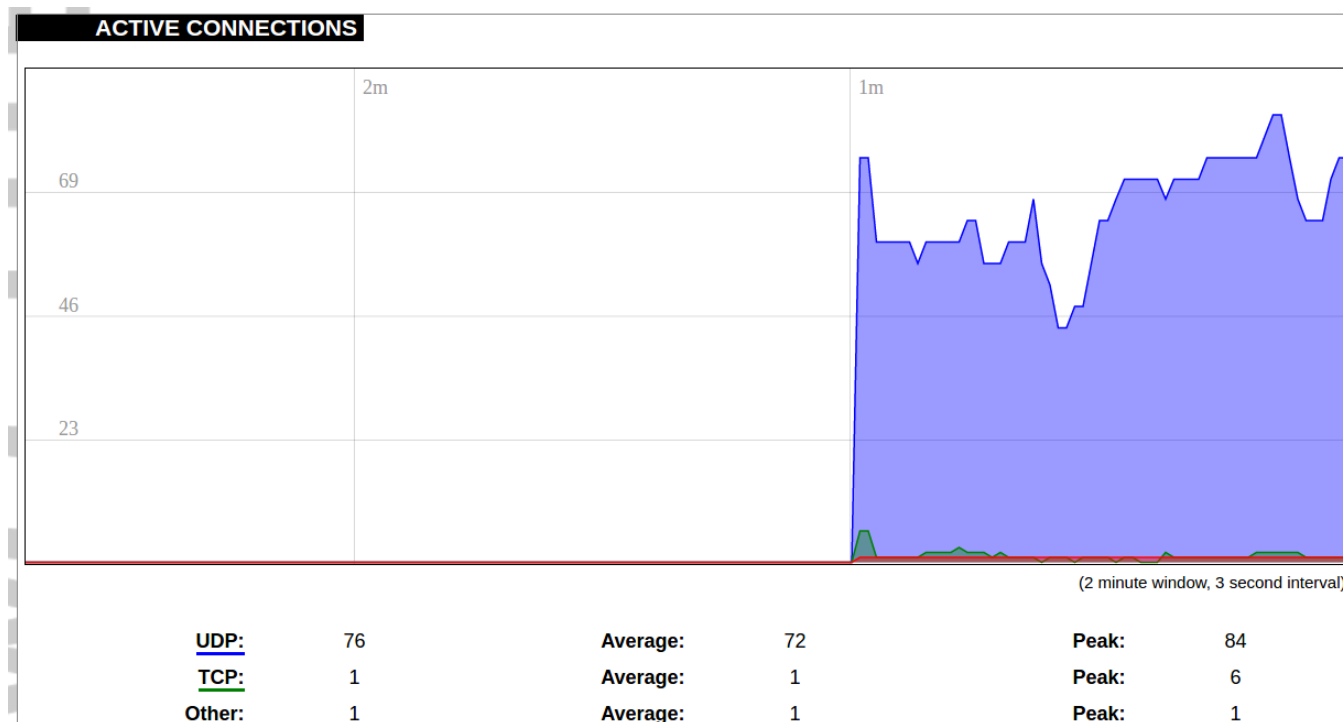
WiFi status graph.

Signal: Signal strength level.

Noise: Noise level.

Phy. Rate: The speed at which bits can be transmitted on the physical layer.

Active connections



Graph representation of active connections with the device.

UDP: Transport layer – User Datagram Protocol.

TCP: Transport layer – Transmission Control Protocol.

Network: Type of the network layer – IPv4 or IPv6.

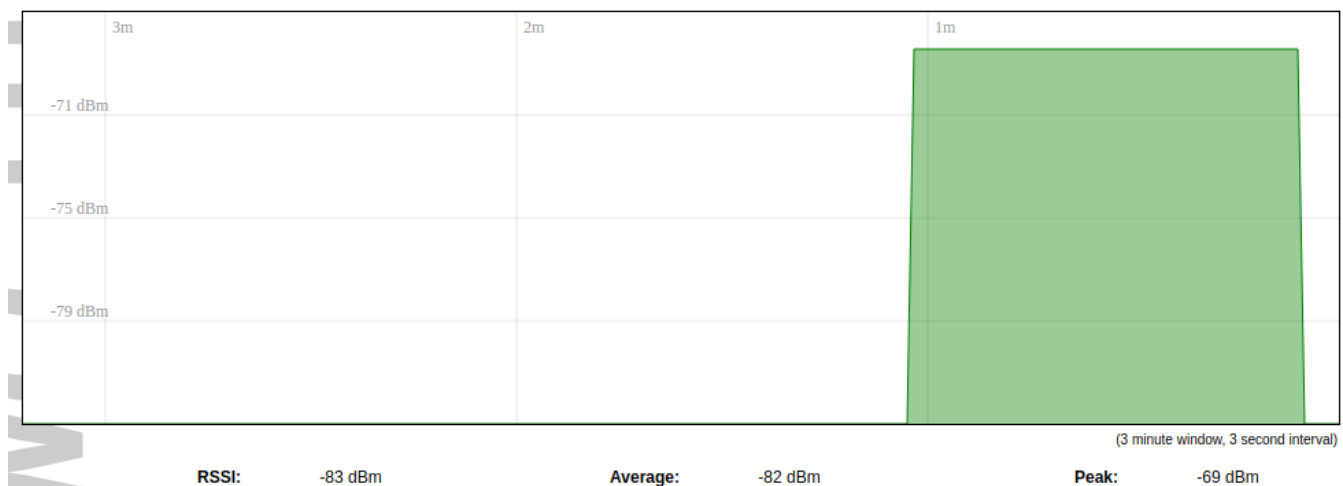
Source, Destination: IP address and the port number.

Transfer: The amount of the transferred data in kB and packets.

GSM signal quality

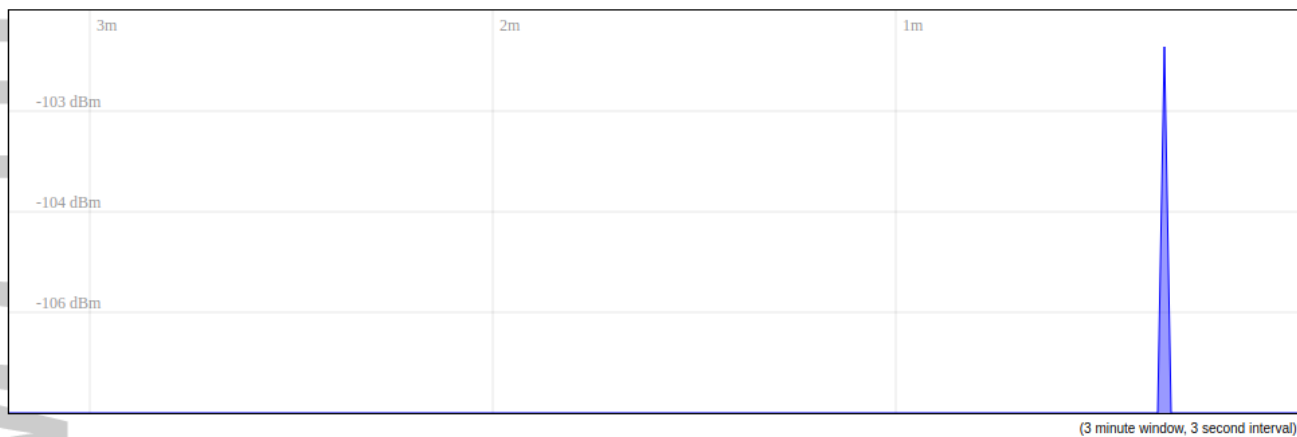
Realtime GSM Signal Quality

This page gives an overview over current RSSI (2G/3G) or RSRP, RSRQ (4G) signal strengths.



Realtime GSM Signal Quality

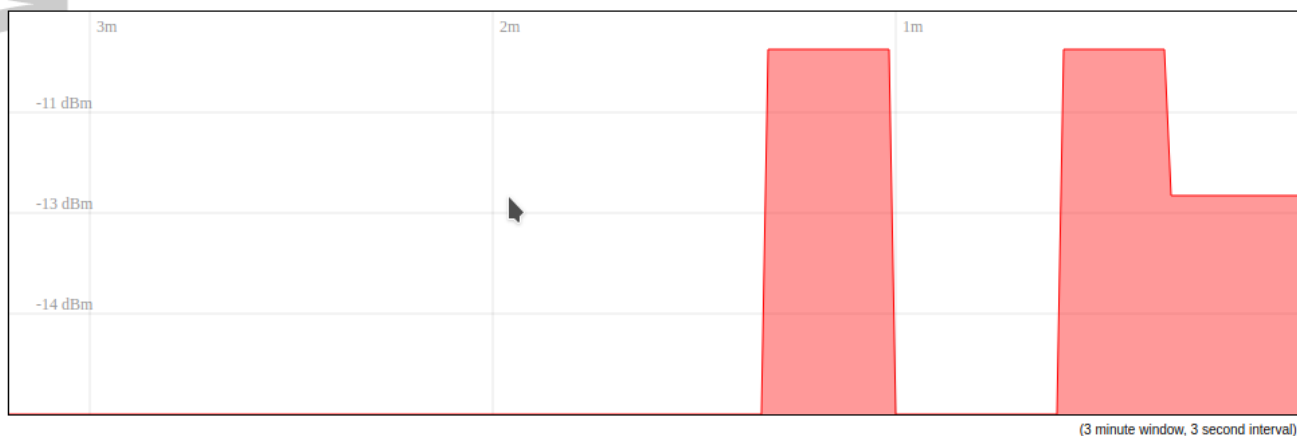
This page gives an overview over current RSSI (2G/3G) or RSRP, RSRQ (4G) signal strengths.



RSRP: -108 dBm

Average: -107 dBm

Peak: -102 dBm



RSRQ: -13 dBm

Average: -12 dBm

Peak: -11 dBm

Graph representation of gsm modem receiving signal quality. RSRP - RSRQ graph is showed, when connected to 4G/LTE network, RSSI - when 2G/3G networks are used.

RSSI: Received Signal Strength Indicator in dBm.

RSRP: Received Signal Reference Power in dBm.

RSRQ: Received Signal Reference Quality in dBm.

GSM status

This page shows all information that is related to GSM modem.

GSM Status


Current hardware and network status of GSM

HARDWARE INFO

Modem model
Modem type
Supported network modes
IMEI

QUECTEL EC25
DUAL SIM
2G 3G 4G 2G/3G/4G

NETWORK INFO

 37%

IMSI:
ICCID:
Registration status: Registered, home network
Internet status: Offline
Operator: Tele2 LT Tele2
Service provider: Tele2
Data interface: Down
SIM state: SIM READY
Signal quality: RSRP: -105 RSRQ: -13
Radio access tech.: 4G, LTE
Active SIM: 1
Roaming status: Off

Reset modem

Switch SIM

Hardware info

All static information on GSM modem.

Modem model: Manufacturer and model of present modem.

Modem type: Single SIM or Double SIM modem.

Supported network modes: Shows which network modes (or their combinations) are supported (e.g. 2G 4G 2G/4G).

IMEI: IMEI (International Mobile Equipment Identity number).

Network info

All dynamic information on GSM modem and connected network.

IMSI: IMSI (International Mobile Subscriber Identity) number related to current SIM card user.

ICCID: ICCID (Integrated Circuit Card Identifier) number related to physical SIM card.

Registration status: Current status of network connection.

Internet status: Status of connection to internet (valid, when gsm-pinger is enabled and can reach provided hosts).

Operator: Operator's name, to which modem is currently connected.

Service provider: IMEI (Service provider for SIM card. Data interface: Shows, whether wcc-lite have a data connection through gsm or not (possible values: "Up", "Down").

SIM state: Shows current status of SIM card (needs PIN, needs PUK, not-inserted and etc.).

Signal quality: Shows current signal strength value in dBms. RSSI value is shown, when connected to 2G/3G networks, RSRP-RSRQ values - when connected to 4G network.

Radio access tech.: Current radio technology used (2G, 3G or 4G).

Active SIM: Shows which SIM card is active (if the modem is Dual SIM).

Roaming status: Current status of roaming ("Off", "On").

Little bars with percentage at the center left shows signal strength. It is calculated with the respect to current radio access technology used (RSSI or RSRP). Two buttons at the bottom can reset (cold-reset) modem or manually switch SIM cards (if it is Dual SIM modem and both cards are enabled).

Reset modem

Switch SIM

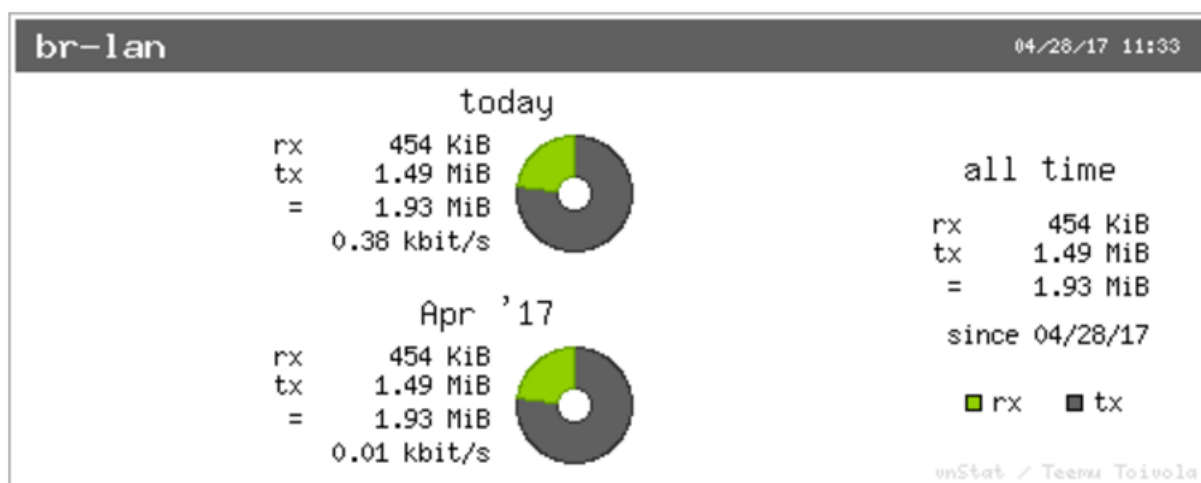
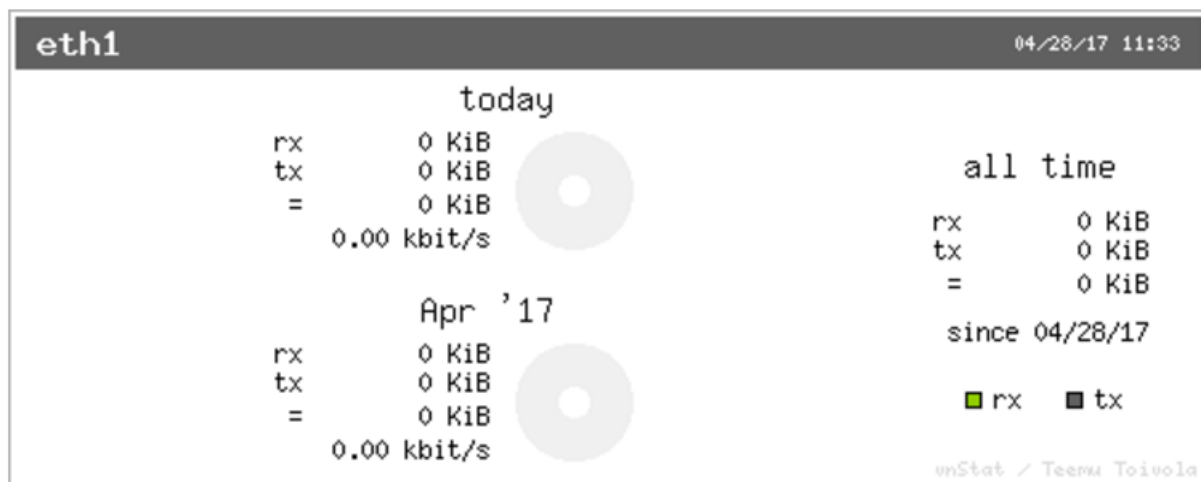
- Signal quality is described in different ways for different type for different mobile services: Received Signal Strength Indication (RSSI) in GSM (2G) and UMTS (3G), the Reference Signal Received Quality (RSRQ) in LTE RAT.

- The Reference Signal Received Power (RSRP) is a LTE specific measure that averages the power received on the subcarriers carrying the reference signal. The RSRP measurement bandwidth is equivalent to a single LTE subcarrier: its value is therefore much lower than the total received power usually referred to as RSSI. In LTE the RSSI depends on the currently allocated bandwidth, which is not pre-determined. Therefore the RSSI is not useful to describe the signal level in the cell.

VNSTAT Traffic monitor

To monitor the traffic of various network interfaces VNSTAT Traffic monitor can be used. Traffic tracking can be useful if user wants to have a precise information on how much data is used because it can have a dependance with data transmission costs, for example, mobile (cellular) data.

Graph



An example graph shows the statistics gathered for two network interfaces. In these graphs:

eth1: Network interface (e.g. Ethernet).

br-lan: Virtual network interface (bridge).

rx: Data packets received by the device.

tx: Data packets sent from the device.

Configuration

Monitor selected interfaces	<input checked="" type="checkbox"/>	 Bridge: "br-lan" (lan)
	<input type="checkbox"/>	 Ethernet Adapter: "eth0"
	<input checked="" type="checkbox"/>	 Ethernet Adapter: "eth1" (wan, wan6)

Save & Apply

Save

Reset

Interfaces to be monitored can be selected in a configuration screen. It includes all the network interfaces configured in a system. To start or stop monitoring user should either select or unselect respective checkbox and save settings by pressing Save & Apply.

Services

Introduction

Services tab shows the services of the device and contains the following subsections:



Services tab shows the services of the device and contains the following subsections:

- TELEMETRY AGENT: device telemetry sending to a remote server;
- IPSEC: encrypted virtual private network (VPN) configuration.
- OPENVPN: shows the open-source software application that implements virtual private network (VPN).
- SER2NET: network-to-serial proxy;

Telemetry agent

Having data about the device helps to easily maintain it. Telemetry agent gathers information in a compact and easily decodable way. It uses UDP packets therefore only small overhead is introduced.

However, UDP does not guarantee the arrival of sent packets therefore not every message might reach the server saving these messages.

To start using Telemetry agent a user should configure and enable it. Four options are available:

- Enable agent;
- Server address;
- Port (UDP);
- Period (s).

Every time timer of period length expires, a message is sent to a server of configured server if service is enabled .

⚠ Telemetry agent doesn't start as a service if Enable agent checkbox is unchecked.

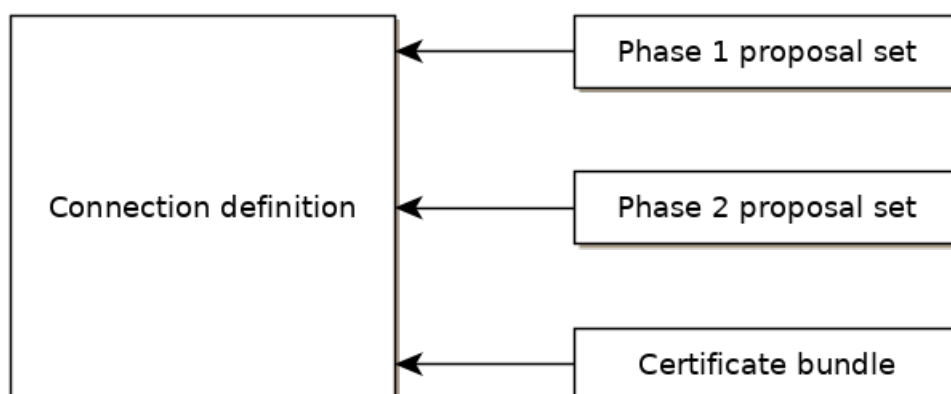
ℹ Enabling agent and saving the configuration automatically starts the process with the new configuration.

IPsec

Background

WCC Lite supports ipsec vpn, thus is able to deliver data securely over encrypted link. To establish ipsec vpn, a connection definition must be created by entering appropriate configuration settings.

For advanced connection description auxiliary settings sets can be defined. They can be joined to the connection and can be reusable several times according to the need. Each configuration record is identified by a unique name, which is assigned in time of creation. The following diagram shows relations between connection and auxiliary sets.



Ipssec settings

Connection description

Options supported by wcclite is described below.

Item	Type	Description
Gateway	string	Host name or IP address of the remote peer.
Type	selector	Tunnel mode: full packet encryption, covers host-to-host, host-to-subnet, subnet-to-subnet situations or transport mode: ip payload encryption, secures host-to-host data only.
Local subnet	string	Specifies local network, in form network/netmask, for example 192.168.11.0/24
Remote subnet	string	Specifies remote network at another side of a tunnel.
Authentication	selector	Pre-shared key or RSA certificate
Pre-shared key	string	Available if Authentication set to Pre-shared key
Certificate set	selector	Available if Authentication set to RSA certificate. Selectable from configured auxiliary set.
Phase 1 proposal (IKE)	selector	Authentication-encryption schema, selectable from configured auxiliary set.
Phase 2 proposal (ESP)	selector	Authentication-encryption schema, selectable from configured auxiliary set.
Local ID	string	Specifies the identity of the local endpoint
Remote ID	string	Specifies the identity of the remote endpoint
Key exchange	selector	Sets method of key exchange IKEv2 or IKEv1. Default IKEv2.

Exchange mode	selector	Main or aggressive. Available if key exchange is set to IKEv1.
Use compression	checkbox	If selected a compression ability will be proposed to the peer.
DPD action	selector	Controls the use of dead peer detection protocol, values: <ul style="list-style-type: none"> • none – default, disables sending of DPD messages. • clear – the connection closed with no action. • hold – keeps description, tries re-negotiate connection on demand. • restart – will try to re-negotiate immediately.
DPD delay	string	Time interval in seconds between peer check. Default 30.
DPD timeout	string	Time in seconds after which peer consider to be unusable. IKEv1 only. Default 150.
Key lifetime	string	Lifetime of data channel in seconds . Default 10800.
IKE lifetime	string	Lifetime of keying channel in seconds. Default 3600.


Auxiliary settings

Phase 1 proposals - IKE/ISAKMP cipher suite components:

Item	Type	Description	Note
Encryption algorithm	selector	Encryption algorithm – 3DES, AES128, AES192, AES256.	required
Hash algorithm	selector	Hash algorithm – MD5, SHA1, SHA256, SHA384 or SHA512.	required
DH exponentiation	selector	Specifies Diffie-Hellman groups – 1,2,5,14,15,16,18	required

Phase 2 proposals - ESP cipher suite components:

Item	Type	Description	Note
Encryption algorithm	selector	Encryption algorithm – 3DES, AES128, AES192, AES256.	required
Hash algorithm	selector	Hash algorithm – MD5, SHA1, SHA256, SHA384 or SHA512.	required
DH exponentiation	selector	Specifies Diffie-Hellman groups – 1,2,5,14,15,16,18	optional

 The following specification and topology map corresponds to settings used in further configuration walk-through example.

Creating a connection description


Site-to-Site VPN scenario



VPN connection details

Tunnel: demoo

```
IPsec peer: ipsec.vpn.net
Pre-shared key: thebigsecret
Mode: tunnel
Remote network: 10.10.10.10/24
Local network: 10.10.12.0/24
Local ID: wcclite
IKE authentication: aes256
IKE hash: sha256
IKE DH group: 5 (modp1536)
ESP authentication: aes128
ESP hash: sha1
```

 If auxiliary data is needed, it is recommended to check or define it first.

Creation of Phase 1 proposal

- Enter section “Phase 1 proposals”.
- Create a new record by assigning new name, for example “aes256-sha256-dh5” and click the button “Add”.
- Choose corresponding values: encryption, hash algorithm and DH exponentiation.
- Push “save” to save the data.

Save

IPsec

PHASE 1 PROPOSALS

Below is a list of configured IPsec phase 1 proposals

	Encryption algorithm	Hash algorithm	DH exponentiation	
aes256_sha256_dh5	<div>aes256</div>	<div>sha256</div>	<div>modp3072 (15)</div>	<div>Delete</div>
<div></div>				<div>Add</div>

Save & Apply

Save

Reset

Creation of Phase 2 proposal

- Enter section “Phase 2 proposals”.
- Create a new record by assign new name for example “aes128-sha1” and click the button “Add”.
- Choose corresponding values: encryption, hash algorithm.
- Push “save” to save the data.

Save

IPsec

PHASE 2 PROPOSALS

Below is a list of configured IPsec phase 2 proposals

	Encryption algorithm	Hash algorithm	DH exponentiation	
aes128_sha1	<div>aes128</div>	<div>sha1</div>	<div></div>	<div>Delete</div>
<div></div>				<div>Add</div>

Save & Apply

Save

Reset

Creation of tunnel definition

Enter section connections

- Create a new record by assigning new name (e.g. “demo0”) and clicking “Add”.
- Call a detail form by pushing the button “edit”.
- Enter peer address into “Gateway”: “ipsec.vpn.net”.
- Ensure “Type” is set to: “Tunnel”.
- Fill local subnet to: 10.10.12.0/24.
- Fill remote subnet to: 10.10.10.0/24.
- Make sure authentication is set to: “Shared secret”.
- Enter Pre-shared key (PSK): thebigsecret.
- “Phase 1 proposal (IKE)”, choose a value: aes256_sha256_dh5.
- “Phase 2 proposal (ESP)”, choose a value: aes128_sha1.

- Locate combo box “additional field”, select “Local ID”, then set value to: wcclite.
- Push “Save”.

Save

» CONNECTION "DEMO0"

Gateway	<input type="text" value="ipsec.vpn.net"/>
Type	<div>Tunnel ▼</div>
Local subnet	<div>10.10.12.0/24 </div>
Remote subnet	<div>10.10.10.0/24 </div>
Authentication	<div>Shared secret ▼</div>
Pre-shared key (PSK)	<div>..... </div>
Phase 1 proposal (IKE)	<div>aes256_sha256 ▼ </div>
Phase 2 proposal (ESP)	<div>aes128_sha1 ▼ </div>
Local ID	<input type="text" value="wcclite"/>
<div>-- Additional Fiel ▼ Add </div>	

Save & Apply
Save
Reset

Activating the tunnel

- Return to the section “connections”.
- Check the checkbox “Enabled”.
- Push the button “save & apply”.
- Examine indicator “configured”, it should be “yes”, if not, review settings just entered.
- The tunnel should be prepared for operation and will be established on demand.
- Optionally, it is possible to establish tunnel operation by pressing button “start”.

Save

IPsec CONNECTIONS

Below is a list of configured IPsec connection instances and their current state

	Enabled	Configured	Established	Gateway	Start/Stop	
demo0	<input checked="" type="checkbox"/>	yes	yes	ipsec.vpn.net	stop	Edit Delete
<input type="text"/> Add						

Save & Apply
Save
Reset

L2TP/IPsec

Because of the lack of confidentiality inherent in the L2TP protocol, it is often implemented along with IPsec. This is referred to as L2TP/IPsec, and is standardized in IETF RFC 3193. The process of setting up an L2TP/IPsec VPN is as follows:

- Negotiation of IPsec security association (SA), typically through Internet key exchange (IKE). This is carried out over UDP port 500, and commonly uses either a shared password (so-called “pre-shared keys”), public keys, or X.509 certificates on both ends, although other keying methods exist.
- Establishment of Encapsulating Security Payload (ESP) communication in transport mode. The IP protocol number for ESP is 50 (compare TCP’s 6 and UDP’s 17). At this point, a secure channel has been established, but no tunneling is taking place.
- Negotiation and establishment of L2TP tunnel between the SA endpoints. The actual negotiation of parameters takes place over the SA’s secure channel, within the IPsec encryption. L2TP uses UDP port 1701.

When the process is complete, L2TP packets between the endpoints are encapsulated by IPsec. Since the L2TP packet itself is wrapped and hidden within the IPsec packet, no information about the internal private network can be gathered from the encrypted packet. Also, it is not necessary to open UDP port 1701 on firewalls between the endpoints, since the inner packets are not acted upon until after IPsec data has been decrypted and stripped, which only takes place at the endpoints. A potential point of confusion in L2TP/IPsec is the use of the terms tunnel and secure channel. The term tunnel refers to a channel which allows untouched packets of one network to be transported over

another network. In the case of L2TP/PPP, it allows L2TP/PPP packets to be transported over IP. A secure channel refers to a connection within which the confidentiality of all data is guaranteed. In L2TP/IPsec, first IPsec provides a secure channel, then L2TP provides a tunnel.

OpenVPN

OpenVPN Instances

The primary goal is to get a working WCC Lite tunnel and establish a basic platform for further customisation. Most users will require further configuration tailored to their individual needs. If you are creating an OpenVPN server (either type), you must create security certificates using the instructions below. If you are using OpenVPN as a client, the required certificates should have been provided with your configuration details. OpenVPN can be configured either by using WCC Lite Web interface or uploading the OVPN file containing necessary parameters. OpenVPN will automatically attempt to load all *.conf files placed in the /etc/openvpn folder. Several OpenVPN recipes are suggested containing most used configurations that may only require minor changes. If a user intends setting up OpenVPN without OVPN file, it is highly advised to use these recipes and tweaking them up to individual needs.

OpenVPN

OPENVPN INSTANCES

Below is a list of configured OpenVPN instances and their current state

	Enabled	Started	Start/Stop	Port	Protocol	
custom_config	<input type="checkbox"/>	no	start	-	-	<div>Edit</div> <div>Delete</div>
sample_server	<input type="checkbox"/>	no	start	1194	udp	<div>Edit</div> <div>Delete</div>
sample_client	<input type="checkbox"/>	no	start	-	udp	<div>Edit</div> <div>Delete</div>

Template based configuration

Simple server configuration for a routed point-to-point VPN

Add

OVPN configuration file upload

Browse...

No file selected.

Upload

OpenVPN instances page contains parameters to be configured.

Enabled: Flag to specify if a particular configuration should be enabled;

Started: Specifies if a particular configuration has been started by OpenVPN;

Start/Stop: Button to manually start or stop any configured tunnels;

Port: Specifies the listening port of this service;

Protocol: A standard that defines how to establish and maintain a network connection: UDP - User Datagram Protocol, TCP - Transmission Control Protocol.

More parameters for every instance can be changed by pressing Edit button, configuration can be removed with Delete button. Pressing Edit takes the user to main configuration screen containing the options usually used in particular OpenVPN recipes. To do more specific changes user should further select Switch to advanced configuration.

OVPN files contain configuration in a textual form therefore changing parameters requires having prior knowledge about different OpenVPN parameters. It is advised to use OVPN files, however, if configuration has been pre-built beforehand and is used without further changes.

The ser2net daemon allows telnet and tcp sessions to be established with a device's serial ports. The program comes up normally as a daemon, opens the TCP ports specified in the configuration file, and waits for connections. Once a connection occurs, the program attempts to set up the connection and open the serial port. If another user is already using the connection or serial port, the connection is refused with an error message.

API

The firmware of the WCC Lite features a built-in API which is accessible via the web interface.



As of version 1.2.11, it does not implement any access restriction features apart from those provided by the firewall functionality.

Individual API endpoints can be enabled or disabled via the web configuration interface at Services->API.



All endpoints are disabled by default.

Available API endpoints are shown in the table below.

Table. Available API endpoints:

Endpoint	Description
/api/version	Version of the API
/api/actions	List of available points
/api/syncVersion	Version of the sync service
/api/sync	Protocol hub configuration sync (name="file")*
/api/syslog	Prints out the syslog
/api/systemInfo	General system info
/api/gsmInfo	GSM modem information
/api/devices	List of configured devices
/api/device/info	Device information (name="device_alias")**
/api/device/tags	List of tags on particular device (name="device_alias")**
/api/device/tag/value	Tag value (name="device_alias", name="signal_alias")**
/api/tags	List of configured tags
/api/sysupgrade	Firmware upgrade (name="file")*

* Endpoints accepting files

** Endpoints accepting field data

The API accepts data and files as POST requests encoded as "multipart/form-data".

SNMP

SNMP (Simple Network Management Protocol) is an internet-standard protocol for managing devices on IP networks. SNMP exposes management data in the form of a hierarchy of variables in a MIB (Management Information Base).

WCC Lite supports SNMP service which is not added to default build of firmware but can be installed as a module. It enables user to collect data on various parameters of system:

- CPU time - time spent for calculations of various processes:

- user - time for user processes;

- system - time for system processes;

- idle - time spent idling;

- interrupts - time spent handling interrupts.

- CPU load average - CPU load average for 1, 5 and 15 minutes respectively;

- Disk usage:

total - total amount of storage in the device (in kB)

available - amount of storage available to store data (in kB)

used - amount of storage used in the device (in KB)

blocks used percentage - blocks (sectors) used to store data in a disk (in kB)

inodes used percentage - the inode (index node) is a data structure in a Unix-style file system that describes a file-system object such as a file or a directory. Each inode stores the attributes and disk block location(s) of the object's data.

- Memory usage - RAM usage statistics:

total - total amount of RAM in the device (in kB);

available - unused amount of RAM in the device (in kB);

shared - shared amount of RAM between multiple processes (in kB);

buffered - refers to an electronic buffer placed between the memory and the memory controller;

cached - a portion of memory made of high-speed static RAM (SRAM) instead of the slower dynamic RAM (DRAM) used for main memory;

- Network interfaces:

MTU - maximum transmission unit to be sent over network;

speed - rate of network transmission;

physical address - unique MAC address assigned to a device;

tx/rx: byte, packet, drop, error count;

- System properties:

uptime - time since the device was turned on;

process uptime - time since the process has been started;

hostname - a label that is assigned to a device connected to a computer network;

name - name of the device (if defined);

location - location of the device (if defined).

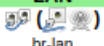
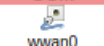
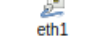

Network

The page shows information about current interface status, its configurations, provides various interface, network properties configuration capabilities and contains the following subsections:

- **INTERFACES:** shows information about current interface status, allows to create new and configure them.
- **WIRELESS:** shows information about wireless radio stations, covers physical settings of the wireless hardware.
- **DHCP AND DNS:** allows management of DHCP and DNS servers.
- **HOSTNAMES:** allows management of host names.
- **STATIC ROUTES:** allows management of IPv4 and IPv6 static routes.
- **FIREWALL:** allows management of firewall zones and various firewall properties.
- **DIAGNOSTICS:** provides network diagnostics utilities.
- **GSM:** allows management of gsm modem and SIM cards.

Interfaces

INTERFACE OVERVIEW

Network	Status	Actions
<div>LAN</div> <div>br-lan</div>	<div>Uptime: 0h 20m 27s</div> <div>MAC-Address: C4:93:00:0B:F4:57</div> <div>RX: 0 B (0 Pkts.)</div> <div>TX: 0 B (0 Pkts.)</div> <div>IPv4: 192.168.1.1/24</div> <div>IPv6: fd94:746:4098::1/60</div>	<div>Connect/Reconnect</div> <div>Stop</div> <div>Edit</div> <div>Delete</div>
<div>GSM</div> <div>wwan0</div>	<div>Uptime: 0h 20m 20s</div> <div>MAC-Address: 00:00:00:00:00:00</div> <div>RX: 256.18 KB (4425 Pkts.)</div> <div>TX: 271.71 KB (4364 Pkts.)</div>	<div>Connect/Reconnect</div> <div>Stop</div> <div>Edit</div> <div>Delete</div>
<div>WAN</div> <div>eth1</div>	<div>Uptime: 0h 20m 22s</div> <div>MAC-Address: C4:93:00:0B:F4:56</div> <div>RX: 497.67 KB (2523 Pkts.)</div> <div>TX: 663.41 KB (1238 Pkts.)</div> <div>IPv4: 192.168.5.131/24</div>	<div>Connect/Reconnect</div> <div>Stop</div> <div>Edit</div> <div>Delete</div>
<div>WAN6</div> <div>eth1</div>	<div>Uptime: 0h 0m 0s</div> <div>MAC-Address: C4:93:00:0B:F4:56</div> <div>RX: 497.67 KB (2523 Pkts.)</div> <div>TX: 663.41 KB (1238 Pkts.)</div>	<div>Connect/Reconnect</div> <div>Stop</div> <div>Edit</div> <div>Delete</div>

Add new interface...

Current information and status of various network interfaces (GSM, LAN, WAN).

Uptime: Current interface uptime in hours, minutes and seconds.

MAC address: Physical interface address.

RX: Received data in bytes (packet count).

TX: Transmitted data in bytes (packet count).

IPv4: Internet protocol version 4 address.

IPv6: Internet protocol version 6 address.

In addition to the network interface status, several actions may be performed:

Connect/Reconnect: Connect to configured interface network if it does not do it automatically. If it already connected to the network it will be trying to reconnect to it.

Stop: Shutdown interface. If you are connected through this interface the connection may be lost.

Edit: Edit interface settings.

Delete: Delete interface.


Add new interface: Adding new Ethernet, GSM or wireless interface with the custom name, protocol and etc.

	eth0	eth1
Type	Static	DHCP
Address	192.168.1.1	
Subnet mask	255.255.255.0	
Gateway		


 Changes will only take effect after device reboots.

Network interfaces can be configured on the common page, which can be accessed through add new interface or edit button.

Name of the new interface

 The allowed characters are: A - Z, a - z, 0 - 9 and _

Note: interface name length

 Maximum length of the name is 15 characters including the automatic protocol/bridge prefix (br-, 6in4-, pppoe- etc.)

Protocol of the new interface

Static address

Create a bridge over multiple interfaces

☐

Cover the following interface

☐
☐
☐
☐
☐
☐

Ethernet Adapter:
"eth0" (lan)

Ethernet Adapter:
"eth1" (wan, wan6)

Ethernet Adapter:
"usb0" (gsm)

Wireless Network:
Master "WCC Lite"
(lan)

Wireless Network:
Client "AP5" (wwan)

Custom Interface:

The following options can be defined in the interface creation panel: name of the interface, protocol, coverage of a particular interface or bridging with other interfaces. After the general setup is done, more detailed settings can be set.


General Setup

Advanced Settings

Physical Settings

Firewall Settings

Status

 **Uptime:** 0h 2m 42s
MAC-Address: CE:0A:91:C9:25:F2
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)

Protocol

Static address

IPv4 address

IPv4 netmask


IPv4 gateway

IPv4 broadcast

Use custom DNS servers

IPv6 assignment length


disabled

 Assign a part of given length of every public IPv6-prefix to this interface

IPv6 address

IPv6 gateway

IPv6 routed prefix

 Public prefix routed to this device for distribution to clients.

General common interface setup panel.

General Setup	Advanced Settings	Physical Settings	Firewall Settings
Bring up on boot		<input checked="" type="checkbox"/>	
Use builtin IPv6-management		<input checked="" type="checkbox"/>	
Override MAC address		<input type="text" value="CE:0A:91:C9:25:F2"/>	
Override MTU		<input type="text" value="1500"/>	
Use gateway metric		<input type="text" value="0"/>	

Advanced common interface setup panel.

General Setup	Advanced Settings	Physical Settings	Firewall Settings
Bridge interfaces		<input type="checkbox"/> creates a bridge over specified interface(s)	
Interface		<div><div><input type="radio"/></div><div><input type="radio"/></div><div><input checked="" type="radio"/></div><div><input type="radio"/></div><div><input type="radio"/></div><div><input type="radio"/></div><div><input type="radio"/></div><div><input type="text"/></div></div> <div><div> Ethernet Adapter: "eth0" (lan)</div><div> Ethernet Adapter: "eth1" (wan, wan6)</div><div> Ethernet Adapter: "usb0" (gsm)</div><div> Wireless Network: Master "WCC Lite" (lan)</div><div> Wireless Network: Client "AP5" (wwan)</div><div> Custom Interface:</div></div>	

Physical common interface setup panel.

General Setup	Advanced Settings	Physical Settings	Firewall Settings
Create / Assign firewall-zone			
<div><input type="radio"/> lan: lan: </div>		Choose the firewall zone you want to assign to this interface. Select unspecified to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.	
<div><input checked="" type="radio"/> wan: wan: wan6: gsm: wwan: </div>			
<div><input type="radio"/> unspecified -or- create: <input type="text"/></div>			

Firewall common interface setup panel.

General Setup
Advanced Settings
IPv6 Settings

Ignore interface
☐
? Disable DHCP for this interface.

Start
100
? Lowest leased address as offset from the network address.

Limit
150
? Maximum number of leased addresses.

Leasetime
12h
? Expiry time of leased addresses, minimum is 2 minutes (2m).

DHCP server general setup panel.

General Setup
Advanced Settings
IPv6 Settings

Dynamic DHCP
☒
? Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.

Force
☐
? Force DHCP on this network even if another server is detected.

IPv4-Netmask
? Override the netmask sent to clients. Normally it is calculated from the subnet that is served.

DHCP-Options
? Define additional DHCP options, for example "6, 192.168.2.1, 192.168.2.2" which advertises different DNS servers to clients.

DHCP server advanced setup panel.

General Setup
Advanced Settings
IPv6 Settings

Router Advertisement-Service
server mode

DHCPv6-Service
hybrid mode

NDP-Proxy
hybrid mode

DHCPv6-Mode
stateless + stateful
? Default is stateless + stateful

Always announce default router
☐
? Announce as default router even if no public prefix is available.

Announced DNS servers

Announced DNS domains

DHCP server IPv6 settings setup panel.

GSM

Interfaces - GSM

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

COMMON CONFIGURATION

General Setup
Advanced Settings
Firewall Settings

Status

wwan0

Uptime: 1h 18m 58s
MAC-Address: 00:00:00:00:00:00
RX: 437.84 KB (7532 Pkts.)
TX: 456.23 KB (7490 Pkts.)

Protocol
wwan

General Settings Information tab. Gives you name of physical GSM interface, lets you choose protocol (not recommended!).

Note: Make sure you won't change GSM interface's protocol, which is set by default to WWAN. Changing this parameter will lead to undefined GSM modem behaviour.

Interfaces - GSM

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

COMMON CONFIGURATION

General Setup

Advanced Settings

Firewall Settings

Bring up on boot

☒

Use builtin IPv6-management

☒

Force link

☐

Set interface properties regardless of the link carrier (If set, carrier sense events do not invoke hotplug handlers).

Enable IPv6 negotiation on the PPP link

☐

Modem init timeout

Maximum amount of seconds to wait for the modem to become ready

Use default gateway

☒

If unchecked, no default route is configured

Prefer PPP connection

☐

If checked, modem will prioritise PPP type connection over other types (if available)

Use gateway metric

Use DNS servers advertised by peer

☒

If unchecked, the advertised DNS server addresses are ignored

LCP echo failure threshold

Presume peer to be dead after given amount of LCP echo failures, use 0 to ignore failures

LCP echo interval

Send LCP echo requests at the given interval in seconds, only effective in conjunction with failure threshold

Inactivity timeout

Close inactive connection after the given amount of seconds, use 0 to persist connection

Override MTU

Advanced Settings tab enables user to configure advanced settings for mobile communication. It includes the following options:

Bring up on boot: Checkbox to start a GSM interface on startup;

Use builtin IPv6-management: Checkbox to select if the device is going to use its own tools to manage IPv6 transport layer messages;

Force link: Specifies whether IP address, route, and gateway are assigned to the interface regardless of the link being active or only after the link has become active; when active, carrier sense events do not invoke hotplug handlers;

IPv6 support: User can select if IPv6 support is handled automatically, manually or disabled altogether;

Modem init timeout: Maximum amount of seconds before the device gives up on finishing initialization;

Use default gateway: Uses the default gateway obtained through DHCP. If left unchecked, no default route is configured;

Prefer PPP connection: If ,the modem, supports PPP and any other communication protocol (e.g. QMI, RNDIS and etc.), prioritise PPP type connection;

Use gateway metric: 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: Uses DNS servers obtained from DHCP. If left unchecked, the advertised DNS server addresses are ignored;

LCP echo failure threshold: LCP (link control protocol) is a part of PPP (Point-to-Point Protocol) and helps to determine the quality of data transmission. If enough failures happen, LCP presumes link to be dead. 0 disables failure count checking;

LCP echo interval: Determines the period of LCP echo requests. Only effective if LCP echo failure threshold is more than zero;

Inactivity timeout: Station inactivity limit in seconds: if a station does not send anything, the connection will be dropped. A value of 0 can be used to persist connection.

Override MTU: Set custom MTU to gsm interface.

Note: If modem uses QMI connection protocol and user haven't defined custom MTU setting, the MTU on interface will be set to operator's defined MTU value.

COMMON CONFIGURATION

General Setup

Advanced Settings

Firewall Settings

Create / Assign firewall-zone



lan:

lan:



wan:

wan:

wan6:

gsm:



unspecified -or- create:



Choose the firewall zone you want to assign to this interface. Select unspecified to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.

GSM configuration ends with firewall settings. A user can assign an already defined firewall zone or create a new one.

Wireless

The wireless network interface parameters and configuration are described in this section.



Generic MAC80211 802.11bgn (radio0)

Channel: 11 (2.462 GHz) | Bitrate: 1 Mbit/s



0%

SSID: WCC Lite | Mode: Master

BSSID: C6:93:00:0E:C4:33 | Encryption: None



50%

SSID: AP5 | Mode: Client

BSSID: 02:1A:11:FF:87:09 | Encryption: WPA2 PSK (CCMP)

Disable

Edit

Remove

Disable

Edit

Remove

Scan
Add

Configured interfaces for the physical radio device.

Channel: Specifies the wireless channel to use.

Bitrate: Specifies transfer rate in Mbit/s.

SSID: The broadcasted service set identifier of the wireless network.

Mode: Selects the operation mode of the wireless network interface controller.

BSSID: The basic service set identification of the network, only applicable in adhoc or STA mode.

Encryption: Wireless encryption method.

	SSID	MAC-Address	Host	Signal / Noise	RX Rate / TX Rate
wlan0	AP5	02:1A:11:FF:87:09	192.168.43.1	-75 / -95 dBm	1.0 Mbit/s, 20MHz 1.0 Mbit/s, 20MHz

List of associated wireless stations.

The Device Configuration section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which are shared among all defined wireless networks (if the radio hardware is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the Interface Configuration.

General Setup

Advanced Settings



47%

Mode: Client | SSID: AP5

BSSID: 02:1A:11:FF:87:09 | Encryption: WPA2 PSK (CCMP)

Channel: 11 (2.462 GHz) | Tx-Power: 20 dBm

Signal: -77 dBm | Noise: -95 dBm

Bitrate: 6.5 Mbit/s | Country: US

Status

Wireless network is enabled

Disable

Operating frequency

Mode
N

Channel
11 (2462 MHz)

Width
20 MHz






Transmit Power

auto ? dBm

General device settings.

General Setup	Advanced Settings
Country Code	<div>US - United States</div> ⓘ Use ISO/IEC 3166 alpha2 country codes.
Distance Optimization	<div></div> ⓘ Distance to farthest network member in meters.
Fragmentation Threshold	<div></div>
RTS/CTS Threshold	<div></div>

Advanced device settings.

INTERFACE CONFIGURATION	
General Setup	Wireless Security
Advanced Settings	
ESSID	<div>AP5</div>
Mode	<div>Client</div>
BSSID	<div>02:1A:11:FF:87:09</div>
Network	ⓘ Choose the network(s) you want to attach to this wireless interface or fill out the create field to define a new network.
<input type="checkbox"/> gsm: 	
<input type="checkbox"/> lan: 	
<input type="checkbox"/> wan: 	
<input type="checkbox"/> wan6: 	
<input checked="" type="checkbox"/> wwan: 	
<input type="checkbox"/> create:	<div></div>

General interface settings.

General Setup	Wireless Security	Advanced Settings
Encryption	<div>WPA2-PSK</div>	
Cipher	<div>auto</div>	
Key	<div>.....</div> ⓘ	

Wireless security interface settings.

INTERFACE CONFIGURATION	
General Setup	Wireless Security
Advanced Settings	
Interface name	<div></div> ⓘ Override default interface name

Advanced interface settings.

DHCP and DNS

DHCP server and DNS forward for NAT firewalls is described in this section.

General Settings	Resolv and Hosts Files	TFTP Settings	Advanced Settings
Domain required <input checked="" type="checkbox"/> ? Don't forward DNS-Requests without DNS-Name			
Authoritative <input checked="" type="checkbox"/> ? This is the only DHCP in the local network			
Local server <input type="text" value="/lan/"/> ? Local domain specification. Names matching this domain are never forwarded and are resolved from DHCP or hosts files only			
Local domain <input type="text" value="lan"/> ? Local domain suffix appended to DHCP names and hosts file entries			
Log queries <input type="checkbox"/> ? Write received DNS requests to syslog			
DNS forwardings <input type="text" value="/example.org/10.1.2.3"/> ? List of DNS servers to forward requests to			
Rebind protection <input checked="" type="checkbox"/> ? Discard upstream RFC1918 responses			
Allow localhost <input checked="" type="checkbox"/> ? Allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services			
Domain whitelist <input type="text" value="ihost.netflix.com"/> ? List of domains to allow RFC1918 responses for			
Local Service Only <input checked="" type="checkbox"/> ? Limit DNS service to subnets interfaces on which we are serving DNS.			
Non-wildcard <input type="checkbox"/> ? Bind only to specific interfaces rather than wildcard address.			

General DHCP settings.

General Settings	Resolv and Hosts Files	TFTP Settings	Advanced Settings
Use /etc/ethers <input checked="" type="checkbox"/> Read /etc/ethers to configure the DHCP-Server			
Leasefile <input type="text" value="/tmp/dhcp.leases"/> file where given DHCP-leases will be stored			
Ignore resolve file <input type="radio"/>			
Resolve file <input type="text" value="/tmp/resolv.conf.auto"/> local DNS file			
Ignore /etc/hosts <input type="radio"/>			
Additional Hosts files <input type="text"/>			

Resolve and hosts files settings.

General Settings	Resolv and Hosts Files	TFTP Settings	Advanced Settings
Enable TFTP server <input checked="" type="checkbox"/>			
TFTP server root <input type="text" value="/"/> Root directory for files served via TFTP			
Network boot image <input type="text" value="pxelinux.0"/> Filename of the boot image advertised to clients			

TFTP server settings.

General Settings
Resolv and Hosts Files
TFTP Settings
Advanced Settings

Suppress logging
☐

? Suppress logging of the routine operation of these protocols

Allocate IP sequentially
☐

? Allocate IP addresses sequentially, starting from the lowest available address

Filter private
☒

? Do not forward reverse lookups for local networks

Filter useless
☐

? Do not forward requests that cannot be answered by public name servers

Localise queries
☒

? Localise hostname depending on the requesting subnet if multiple IPs are available

Expand hosts
☒

? Add local domain suffix to names served from hosts files

No negative cache
☐

? Do not cache negative replies, e.g. for not existing domains

Additional servers file

? This file may contain lines like 'server=/domain/1.2.3.4' or 'server=1.2.3.4' for domain-specific or full upstream DNS servers.

Strict order
☐

? DNS servers will be queried in the order of the resolvfile

Bogus NX Domain Override

? List of hosts that supply bogus NX domain results

DNS server port

? Listening port for inbound DNS queries

DNS query port

? Fixed source port for outbound DNS queries

Max. DHCP leases

? Maximum allowed number of active DHCP leases

Max. EDNS0 packet size

? Maximum allowed size of EDNS.0 UDP packets

Max. concurrent queries

? Maximum allowed number of concurrent DNS queries

Advanced settings.

ACTIVE DHCP LEASES

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
There are no active leases.			

ACTIVE DHCPV6 LEASES

Host	IPv6-Address	DUID	Leasetime remaining
?	fd74:8536:7bae::33f/128	00046836d59efa382760f3193e5ec5bf4a24	11h 54m 16s

STATIC LEASES

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.
Use the Add Button to add a new lease entry. The MAC-Address identifies the host, the IPv4-Address specifies the fixed address to use and the Hostname is assigned as symbolic name to the requesting host. The optional Lease time can be used to set non-standard host-specific lease time, e.g. 12h, 3d or infinite.

Hostname	MAC-Address	IPv4-Address	Lease time	IPv6-Suffix (hex)
<input type="text" value="host2"/>	<input type="text" value="f0:76:1c:3b:cb:13 (192.168.2.2)"/>	<input type="text" value="192.168.2.2"/>	<input type="text" value="10"/>	<input type="text"/>

Add
Delete

List of active DHCP and static leases. It is also possible to assign fixed IP addresses to hosts on the network, based on their MAC (hardware) address.

Hostnames

HOST ENTRIES		
Hostname	IP address	
<input type="text" value="Host1"/>	<input type="text" value="192.168.2.35"/>	<input type="button" value="Delete"/>
<input type="button" value="Add"/>		

List of existing host names. Addition or deletion is allowed for the user.

Static routes

Routes specify over which interface and gateway a certain host or network can be reached.

STATIC IPV4 ROUTES						
Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric	MTU	Route type
	Host-IP or Network	if target is a network				
<input type="text" value="lan"/>	<input type="text" value="192.168.0.254"/>	<input type="text" value="255.255.255.255"/>	<input type="text" value="192.168.0.254"/>	<input type="text" value="0"/>	<input type="text" value="1500"/>	<input type="text" value="unicast"/>
<input type="button" value="Delete"/>						
<input type="button" value="Add"/>						

STATIC IPV6 ROUTES						
Interface	Target	IPv6-Gateway	Metric	MTU	Route type	
	IPv6-Address or Network (CIDR)					
<input type="text" value="lan"/>	<input type="text" value="0:0:0:0:ffff:c0a8:fe"/>	<input type="text" value="0:0:0:0:ffff:c0a8:fe"/>	<input type="text" value="0"/>	<input type="text" value="1500"/>	<input type="text" value="unicast"/>	<input type="button" value="Delete"/>
<input type="text" value="lan"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="1500"/>	<input type="text" value="unicast"/>	<input type="button" value="Delete"/>
<input type="button" value="Add"/>						

Current IPv4 and IPv6 static routes configuration.

Interface: Lets to chose for which interface static route is created.

Target: Defines target host IP or network.

IPv4 Netmask: Defines netmask if the target is a network.

IPv4/IPv6 Gateway: Defines IPv4 or IPv6 gateway.

Metric: Specifies the route metric to use for the route.

MTU: Maximum Transmit/Receive Unit, in bytes.

Route type: All incoming packets can be: accepted, rejected, dropped.

Firewall

This subsection is divided into four categories: general settings, port forwards, traffic rules and custom rules.

General settings

GENERAL SETTINGS	
Enable SYN-flood protection	<input type="checkbox"/>
Drop invalid packets	<input type="checkbox"/>
Input	accept
Output	accept
Forward	reject

General Settings for firewall can be changed in General Settings screen. These settings are defined as follows:
Input: All incoming packets can be: accepted, rejected, dropped.
Output: All outgoing packets can be: accepted, rejected, dropped.
Forward: All packets being sent to another device can be: accepted, rejected, dropped.

ZONES		Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan:	lan: ⇒ wan	accept	accept	accept	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
wan:	wan: ⇒ REJECT	reject	accept	reject	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
wan6:								
gsm:								
wwan:								
<input type="button" value="Add"/>								

Additional zones for firewall can be created, edited or deleted.
Zone => Forwardings: Defines zones and their traffic flow.
Input: All incoming packets can be: accepted, rejected, dropped.
Output: All outgoing packets can be: accepted, rejected, dropped.
Forward: All packets being sent to another device can be: accepted, rejected, dropped.
Masquerading: Allows one or more devices in a zones network without assigned IP addresses to communicate with the Internet.
MSS clamping: Change the maximum segment size (MSS) of all TCP connections passing through this zone with MTU lower than the Ethernet default of 1500.

i Additional actions can be performed with zones: add, edit, delete.

General Settings	Advanced Settings
Name	newzone
Input	accept
Output	accept
Forward	reject
Masquerading	<input type="checkbox"/>
MSS clamping	<input type="checkbox"/>
Covered networks	<input type="checkbox"/> gsm: <input type="checkbox"/> lan: <input type="checkbox"/> wan: <input type="checkbox"/> wan6: <input type="checkbox"/> wwan: <input type="checkbox"/> create: <input type="text"/>

Common properties of newly created or edited zones can be edited in this panel. The input and output options set the

default policies for traffic entering and leaving this zone while the forward option describes the policy for forwarded traffic between different networks within the zone. Covered networks specify which available networks are members of this zone.

General Settings	Advanced Settings
Restrict to address family	IPv4 and IPv6
Restrict Masquerading to given source subnets	0.0.0.0/0
Restrict Masquerading to given destination subnets	0.0.0.0/0
Force connection tracking	<input type="checkbox"/>
Enable logging on this zone	<input type="checkbox"/>

Advanced settings of new created or edited zone. Restrict to address family option defines to what IP families the zone belongs to IPv4, IPv6 or both. Restrict masquerading to given source/destination subnets defines one or more subnets for which the masquerading option is applied to. Connection tracking and logging options enable additional information gathering on the zone.

Allow forward to destination zones:	<input type="checkbox"/> lan: lan:
	<input type="checkbox"/> wan: wan: wan6: gsm: wwan:
Allow forward from source zones:	<input type="checkbox"/> lan: lan:
	<input type="checkbox"/> wan: wan: wan6: gsm: wwan:

Controls of the forwarding policies between new/edited zone and other zones. Destination zones cover forwarded traffic originating from the new/edited zone. Source zones match forwarded traffic from other zones targeted at the new/edited zone. The forwarding rule is unidirectional, e.g. a forward from LAN to WAN does not imply a permission to forward from WAN to LAN as well.

Port forwards

PORT FORWARDS

Name	Match	Forward to	Enable	Sort	
4000	IPv4-tcp From any host in wan Via any router IP at port 4000	IP 192.168.2.1, port 4000 in lan	<input checked="" type="checkbox"/>	▲ ▼	<div>Edit</div> <div>Delete</div>
4001	IPv4-tcp, udp From any host in wan Via any router IP at port 4001	IP 192.168.2.1, port 4001 in lan	<input checked="" type="checkbox"/>	▲ ▼	<div>Edit</div> <div>Delete</div>

New port forward:

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port	
<div>New port forward</div>	<div>TCP+UDP</div>	<div>wan</div>	<div></div>	<div>lan</div>	<div></div>	<div></div>	<div>Add</div>

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN. It is done in a way of routing network packets within a private network created by the device. Settings for the port forwarding of the device are defined as follows:

Name: The name of the port forwarding rule.

Match: Informs what port forward is matched to.

Forward to: Informs where the port is forwarded to.

Enable: Enable (checked) or disable port forward.

Sort: Allows to sort port forwarding.

The user can add, edit or delete port forwarding rules.

Traffic rules

TRAFFIC RULES

Name	Match	Action	Enable	Sort	
Allow-DHCP-Renew	IPv4-udp From any host in wan To any router IP at port 68 on this device	Accept input	<input checked="" type="checkbox"/>	▲ ▼	<div>Edit</div> <div>Delete</div>
Allow-Ping	IPv4-icmp with type echo-request From any host in wan To any router IP on this device	Accept input	<input checked="" type="checkbox"/>	▲ ▼	<div>Edit</div> <div>Delete</div>
Allow-IGMP	IPv4-igmp From any host in wan To any router IP on this device	Accept input	<input checked="" type="checkbox"/>	▲ ▼	<div>Edit</div> <div>Delete</div>
Allow-DHCPv6	IPv6-udp From IP range fc00::/6 in wan To IP range fc00::/6 at port 546 on this device	Accept input	<input checked="" type="checkbox"/>	▲ ▼	<div>Edit</div> <div>Delete</div>

Traffic rules which define policies for packets traveling between different zones.

Name: The name of the traffic rule.

Match: Informs what ICMP types are matched.

Action: Informs what action would be performed.

Enable: Enable (checked) or disable the rule.

Sort: Allows to sort rules.

The user can add, edit or delete traffic rules. For every rule can be defined these options: name, restrict to address family, protocol, match ICMP type, source and destination zones, source MAC, IP addresses and port, destination IP address and port, action and extra arguments, month and weekdays for which rule will apply, start/stop dates and times, time in UTC.

Name	Match	Action	Enable	Sort
This section contains no values yet				
New source NAT:				
Name	Source zone	Destination zone	To source IP	To source port
<div>New SNAT rule</div>	<div>lan</div>	<div>wan</div>	<div>Do not rewrite</div>	<div>Do not rewrite</div>
				<div>Add and edit...</div>

Source NAT, which is a specific form of masquerading which allows fine grained control over the source IP used for

outgoing traffic, for the example to map multiple WAN addresses to internal subnets. The user can add, edit or delete source NAT rules. For every rule can be defined these options: name, protocol, source and destination zones, source, destination, SNAT IP addresses, ports, extra arguments, month and weekdays for which rule will apply, start/stop dates and times, time in UTC.

Custom rules

```
# This file is interpreted as shell script.
# Put your custom iptables rules here, they will
# be executed with each firewall (re-)start.

# Internal uci firewall chains are flushed and recreated on reload, so
# put custom rules into the root chains e.g. INPUT or FORWARD or into the
# special user chains, e.g. input_wan_rule or postrouting_lan_rule.
```

Custom rules allow to executing arbitrary iptables commands which are not otherwise covered by the firewall framework. The commands are executed after each firewall restart, right after the default ruleset has been loaded.

Diagnostics

NETWORK UTILITIES

IPv4 ▼ Ping

IPv4 ▼ Traceroute


Nslookup



Diagnostics tools which can be used to diagnose some of the networking problems: ping, traceroute and nslookup.





GSM

GSM

Configuration page for GSM modem

SIM CARDS PARAMETERS	
<div><div>SIM 1</div><div>SIM 2</div></div>	
Enable	<input checked="" type="checkbox"/>
PIN code	<input type="text"/> 
APN	<input type="text"/>
PAP/CHAP username	<input type="text"/>
PAP/CHAP password	<input type="text"/>

MODEM PARAMETERS	
Enable data connection	<input checked="" type="checkbox"/>
Priority SIM	<div><div>1</div><div>▼</div></div>
 Which SIM will be prioritised when switching cards	
Service Type	<div><div>2G/3G/4G</div><div>▼</div></div>
 Choosing modem service type. For service type to come to effect, you will have restart connection.	

PINGER CONFIGURATION	
Disable	<input type="checkbox"/>
Failed ping count	<div><div>3</div><div>▼</div></div>
 Limit of failed ping requests, before pinger decides, that internet connection is lost	
Reset modem	<input checked="" type="checkbox"/>
 Reset modem after failed pings	
Switch SIM	<input checked="" type="checkbox"/>
 Switch SIM to non-priority after specified retry count	
Priority SIM retry count	<div><div>3</div><div>▼</div></div>
 How much blocks of failed pings will the pinger tolerate, before switching to non-priority SIM	
Ping interval (minutes)	<div><div>2</div><div>▼</div></div>
Primary host	<input type="text" value="google.com"/>
Secondary host	<input type="text" value="8.8.4.4"/>
Network interface	<input type="text" value="gsm"/>

SIM cards parameters

Parameters for SIM card. If single SIM modem is used, there won't be "SIM 1" and "SIM 2" tabs.

Enable: Enable or disable this SIM card.

PIN code: PIN code to use on that SIM card.

APN: APN to use on that SIM card.

PAP/CHAP username: Username (optional).

PAP/CHAP password: Password (optional).

Modem parameters

Enable data connection: Enable or disable data connection through gsm modem.

Priority SIM: Primary SIM card (if Dual SIM modem is used). Mainly used for pinger configuration.

Service Type: Which radio access technology will be used when connecting to the gsm network.

Pinger configuration

Pinger is a service which pings defined hosts to check internet connection. If both of these hosts are unreachable pinger will wait and restart modem (or switch SIM card, if Dual-SIM modem is installed in WCC Lite)

Disable: Disable pinger functionality.

Failed ping count: Limit of failed ping requests, before pinger decides that internet connection is lost.

Reset modem: If checked, pinger resets gsm modem after "Failed ping count".

Switch SIM: If checked, pinger switches SIM to non-priority after "Priority SIM retry count". If internet connection is not available with non-priority SIM as well, pinger switches back to priority SIM after one failed ping attempt.

Priority SIM retry count: How many blocks of failed pings will the pinger tolerate, before switching to non-priority SIM.

Ping interval (minutes): Interval between ping requests.

Primary host: The host that will be pinged first.

Secondary host: The host that will be pinged second, if the primary host fails.

Network interface: GSM network interface name.

1 GSM Pinger is used to detect the status of network connection via cellular network. This status is written to file (/var/run/board/internet-status) and can be configured to be sent to SCADAs. If pinger is disabled, status is always set equal to zero and should not be trusted to represent internet status. Additionally, this status is reflected in the "Status"->"GSM Status" window.

This is Pinger functionality described step by step:

- Pinger will ping the primary host every 2 minutes.
- If the primary host fails, pinger redirects to the secondary host immediately.
- If either primary or secondary host is responding to ping requests, pinger will continue testing connection every "Ping interval (minutes)" parameter and no further action is taken.
- If both primary and secondary hosts are unreachable, pinger will start pinging these hosts every "Ping interval (minutes) / 2" minute for "Failed ping count" times.
- If hosts are still unreachable, pinger will try to switch SIM and restart modem (if corresponding parameters are set) or will restart immediately if single SIM modem is used.
- SIM card is switched to non-priority SIM after "Priority SIM retry count" failed modem restarts with priority SIM. If a non-priority SIM fails, it is switched to priority SIM in the next pinger action.

Dual SIM start procedure

Table below shows, which card is expected on boot, when selection is made between Enable/Disable SIM cards and Primary card.

SIM 1 Enabled	SIM 2 Enabled	Priority SIM	SIM on boot
X		1	1
X		2	1
	X	1	2
	X	2	2
X	X	1	1
X	X	2	2
		1	Undefined
		2	Undefined

Layer 2 Tunneling Protocol

In computer networking, Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy.

Description

The entire L2TP packet, including payload and L2TP header, is sent within a User Datagram Protocol (UDP) datagram. It is common to carry PPP sessions within an L2TP tunnel. L2TP does not provide confidentiality or strong authentication by itself. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination of these two protocols is generally known as L2TP/IPsec (discussed below). The two endpoints of an L2TP tunnel are called the LAC (L2TP Access Concentrator) and the LNS (L2TP Network Server). The LNS waits for new tunnels. Once a tunnel is established, the network traffic between the peers is bidirectional. To be useful for networking, higher-level protocols are then run through the L2TP tunnel. To facilitate this, an L2TP session (or 'call') is established within the tunnel for each higher-level protocol such as PPP. Either the LAC or LNS may initiate sessions. The traffic for each session is isolated by L2TP, so it is possible to set up multiple virtual networks across a single tunnel. MTU should be considered when implementing L2TP. The packets exchanged within an L2TP tunnel are categorized as either control packets or data packets. L2TP provides reliability features for the control packets, but no reliability for data packets. Reliability, if desired, must be provided by the nested protocols running within each session of the L2TP tunnel. L2TP allows the creation of a virtual private dialup network (VPDN) to connect a remote client to its corporate network by using a shared infrastructure, which could be the Internet or a service provider's network.

Setting up L2TP interface

In order to create a L2TP tunnel following steps are required:

1. Go to **Network > Interfaces > Add new interface:**

INTERFACES

WIRELESS

DHCP AND DNS

HOSTNAMES

STATIC ROUTES

FIREWALL

DIAGNOSTICS

LOAD BALANCING

Save

Interfaces

INTERFACE OVERVIEW

Network	Status	Actions			
<div>LAN</div> <div>br-lan</div>	Uptime: 0h 6m 51s MAC-Address: C4:93:00:08:4E:25 RX: 235.56 KB (1340 Pkts.) TX: 786.39 KB (1261 Pkts.) IPv4: 192.168.1.1/24 IPv6: fd15:7d60:daa1::1/60	Connect	Stop	Edit	Delete
<div>GSM</div> <div>ublox-gsm</div>	RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)	Connect	Stop	Edit	Delete
<div>WAN</div> <div>eth1</div>	Uptime: 0h 0m 0s MAC-Address: C4:93:00:08:4E:24 RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)	Connect	Stop	Edit	Delete
<div>WAN6</div> <div>eth1</div>	Uptime: 0h 0m 0s MAC-Address: C4:93:00:08:4E:24 RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)	Connect	Stop	Edit	Delete

Add new inter

2. Enter interface name and select L2TP protocol:

Save

Create Interface

Name of the new interface ⓘ The allowed characters are: A-Z, a-z, 0-9 and _

Note: interface name length
ⓘ Maximum length of the name is 15 characters including the automatic protocol/bridge prefix (br-, 6in4-, pppoe- etc.)

Protocol of the new interface

L2TP ▼

Static address
DHCP client
Unmanaged
DHCPv6 client
PPP
PPPoE
UMTS/GPRS/EV-DO
L2TP
ublox

Back to Overview Submit

3. Enter server name and authorization parameters:

COMMON CONFIGURATION

General Setup

Advanced Settings

Firewall Settings

l2tp-l2tp

RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)

Status

Protocol

L2TP ▼

L2TP Server

servername

PAP/CHAP username

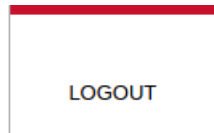
username

PAP/CHAP password

🔑

4. Save and apply the new configuration. A new network interface will appear.

Logout



WCC LITE

To log out of the device graphical user interface a logout button in interface's upper right corner should be pressed. A user is automatically disconnected after ten minutes of inactivity. This ensures that the device would not be suspect to any deliberate damage made by unauthorized access.

WCC Lite Tags

Single point

Commonly used in storing digital states single point values have only one bit of information. The value of such tags can be either one or zero.

On the internal web of WCC Lite states of this type of tags are shown in colored boxes with customisable label.

Value	Representation
0	OFF
1	ON

Double point

Double point signals contain two bits of information that allow four different states, therefore they contain additional information compared to single point ones. INDETERMINATE state might, for example, mean that part of the equipment has been turned off or a mechanical part which does the switching has stuck between states. ERROR state might mean that both contacts are connected and there might be a short circuit in the equipment.

Value	Representation
00	INDETERMINATE
01	OFF
10	ON
11	ERROR