

Cellular and Wired Routers **SPECTRE LTE, 3G, RT**

CONFIGURATION MANUAL



International Headquarters

B+B SmartWorx
707 Dayton Road
Ottawa, IL 61350 USA

Phone (815) 433-5100 – **General Fax** (815) 433-5105

Websites
bb-smartsensing.com
www.bb-smartworx.com
support@bb-smartworx.com

European Headquarters

B+B SmartWorx
Westlink Commercial Park
Oranmore, Co. Galway, Ireland

Phone +353 91-792444 – **Fax** +353 91-792445

Websites
www.bb-europe.com
techsupport@bb-elec.com



Document: SPECTRE_Configuration_Manual
Conel s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
Manual issued in CZ, July 27, 2015

Contents

Document Information	1
1 Access to the Web Conf.	2
1.1 Secured access to web configuration	3
2 Status	4
2.1 General	4
2.1.1 Mobile Connection	4
2.1.2 Primary LAN	5
2.1.3 Peripheral Ports	5
2.1.4 System Information	5
2.2 Mobile WAN Status	6
2.3 WiFi	9
2.4 WiFi Scan	10
2.5 Network status	12
2.6 DHCP status	14
2.7 IPsec status	15
2.8 DynDNS status	15
2.9 System Log	16
3 Configuration	18
3.1 LAN configuration	18
3.2 VRRP configuration	23
3.3 Mobile WAN configuration	26
3.3.1 Connection to mobile network	26
3.3.2 DNS address configuration	27
3.3.3 Check connection to mobile network configuration	27
3.3.4 Data limit configuration	28
3.3.5 Switch between SIM cards configuration	29
3.3.6 Dial-In access configuration	31
3.3.7 PPPoE bridge mode configuration	31
3.4 PPPoE Configuration	34
3.5 WiFi configuration	35
3.6 WLAN configuration	39
3.7 Backup Routes	41
3.8 Firewall configuration	42
3.9 NAT configuration	46
3.10 OpenVPN tunnel configuration	50
3.11 IPsec tunnel configuration	55

3.12 GRE tunnel configuration	60
3.13 L2TP tunnel configuration	63
3.14 PPTP tunnel configuration	65
3.15 DynDNS client configuration	67
3.16 NTP client configuration	68
3.17 SNMP configuration	69
3.18 SMTP Configuration	74
3.19 SMS configuration	75
3.19.1 Send SMS	78
3.20 Expansion port configuration	84
3.21 USB port configuration	88
3.22 Startup script	92
3.23 Up/Down script	93
3.24 Automatic update configuration	94
4 Customization	96
4.1 User Modules	96
5 Administration	98
5.1 Change Profile	98
5.2 Change Password	98
5.3 Set Real Time Clock	99
5.4 Set SMS service center address	99
5.5 Unlock SIM card	100
5.6 Send SMS	100
5.7 Backup Configuration	101
5.8 Restore Configuration	101
5.9 Update Firmware	101
5.10 Reboot	102
6 Configuration over Telnet	103
7 IoT Network Gateway	105
7.1 IoT Network Gateway	105
7.2 Gateway Configuration	105
7.3 SmartMesh IP Configuration	107
7.4 MQTT Broker Configuration	107
7.5 MQTT Bridge Configuration	107
7.6 DUST LINK Configuration	108
7.7 SmartMesh IP Port LEDs	108

List of Figures

1	Web configuration	2
2	Mobile WAN status	8
3	WiFi Status	9
4	WiFi Scan	11
5	Network status	13
6	DHCP status	14
7	IPsec status	15
8	DynDNS status	15
9	System Log	17
10	Example program syslogd start with the parameter -r	17
11	Example 1 – Network Topology for Dynamic DHCP Server	20
12	Example 1 – LAN Configuration Page	20
13	Example 2 – Network Topology with both Static and Dynamic DHCP Servers	21
14	Example 2 – LAN Configuration Page	21
15	Example 3 – Network Topology	22
16	Example 3 – LAN Configuration Page	22
17	Topology of example VRRP configuration	24
18	Example of VRRP configuration – main router	24
19	Example of VRRP configuration – backup router	25
20	Mobile WAN configuration	32
21	Example 1 – Mobile WAN configuration	33
22	Example 2 – Mobile WAN configuration	33
23	Example 3 – Mobile WAN configuration	33
24	PPPoE configuration	34
25	WiFi konfigurace	38
26	WLAN configuration	40
27	Backup Routes	41
28	Firewall configuration	44
29	Topology of sample firewall configuration	45
30	Example of a firewall configuration	45
31	Example 1 – Topology of basic NAT configuration	47
32	Example 1 – Basic NAT configuration	48
33	Example 2 – Topology of NAT configuration	49
34	Example 2 – NAT configuration	49
35	OpenVPN tunnel configuration	50
36	OpenVPN tunnel configuration	53
37	Topology of OpenVPN configuration example	54
38	IPsec tunnel configuration	55
39	IPsec tunnels configuration	59
40	Topology of IPsec configuration example	60

41	GRE tunnel configuration	61
42	GRE tunnel configuration	62
43	Topology of GRE tunnel configuration	62
44	L2TP tunnel configuration	63
45	Topology of L2TP tunnel configuration example	64
46	PPTP tunnel configuration	65
47	Topology of PPTP tunnel configuration example	66
48	Example of DynDNS configuration	67
49	Example of NTP configuration	68
50	Example of SNMP configuration	72
51	Example of the MIB browser	73
52	Example of the SMTP client configuration	74
53	Example of SMS configuration 1	80
54	Example of SMS configuration 2	81
55	Example of SMS configuration 3	82
56	Example of SMS configuration 4	83
57	Expansion port configuration	86
58	Example of Ethernet to serial communication	86
59	Example of serial port extension	87
60	USB configuration	90
61	Example of USB port configuration 1	90
62	Example of USB port configuration 2	91
63	Startup script	92
64	Example of a startup script	92
65	Up/Down script	93
66	Example of Up/Down script	93
67	Example of automatic update 1	95
68	Example of automatic update 2	95
69	User modules	96
70	Added user module	96
71	Change profile	98
72	Change password	98
73	Set Real Time Clock	99
74	Set SMS service center address	99
75	Unlock SIM card	100
76	Send SMS	100
77	Restore Configuration	101
78	Update Firmware	101
79	Reboot	102
80	User Modules	105
81	IoT Gateway	106
82	IoT Gateway Configuration	106

List of Tables

1	Mobile connection	4
2	Peripheral Ports	5
3	System Information	5
4	Mobile Network Information	6
5	Description of period	7
6	Mobile Network Statistics	7
7	Traffic statistics	8
8	State information about access point	9
9	State information about connected clients	9
10	Information about neighbouring WiFi networks	10
11	Interface connection status	12
12	Description of information in network status	13
13	DHCP status description	14
14	Configuration of network interface	18
15	Configuration of dynamic DHCP server	19
16	Configuration of static DHCP server	19
17	VRRP configuration	23
18	Check connection	23
19	Mobile WAN connection configuration	26
20	Check connection to mobile network configuration	28
21	Data limit configuration	28
22	Default and backup SIM configuration	29
23	Switch between SIM card configurations	30
24	Switch between SIM card configurations	30
25	Dial-In access configuration	31
26	PPPoE configuration	34
27	WiFi configuration	38
28	WLAN configuration	39
29	Configuration of DHCP server	40
30	Backup Routes	42
31	Filtering of incoming packets	43
32	Forwarding filtering	44
33	NAT configuration	46
34	Configuration of "send all" incoming packets	46
35	Remote access configuration	47
36	Overview of OpenVPN tunnels	50
37	OpenVPN configuration	53
38	Example of OpenVPN configuration	54
39	Overview of IPsec tunnels	55
40	IPsec configuration	57

41	Example of IPsec configuration	60
42	Overview of GRE tunnels	61
43	GRE tunnel configuration	61
44	Example GRE tunnel configuration	62
45	L2TP tunnel configuration	63
46	Example of L2TP tunnel configuration	64
47	PPTP tunnel configuration	65
48	Example of PPTP tunnel configuration	66
49	DynDNS configuration	67
50	NTP configuration	68
51	SNMP agent configuration	69
52	SNMPv3 configuration	69
53	SNMP configuration (MBUS extension)	70
54	SNMP configuration (R-SeeNet)	70
55	Object identifier for binary input and output	70
56	Object identifier for CNT port	71
57	Object identifier for M-BUS port	71
58	SMTP client configuration	74
59	Send SMS configuration	76
60	Control via SMS configuration	76
61	Control SMS	77
62	Send SMS on serial PORT1 configuration	77
63	Send SMS on serial PORT2 configuration	77
64	Send SMS on Ethernet PORT1 configuration	78
65	List of AT commands	79
66	Expansion port configuration 1	84
67	Expansion port configuration 2	85
68	CD signal description	85
69	DTR signal description	85
70	USB port configuration 1	88
71	USB PORT configuration 2	89
72	CD signal description	89
73	DTR signal description	89
74	Automatic update configuration	94
75	User modules	97
76	Telnet commands	104
77	SmartMesh IP parameters	107
78	MQTT Broker configuration	107
79	MQTT Bridge parameters	108
80	DUST LINK configuration	108
81	SmartMesh IP port LEDs	108

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photography, recording, or any information storage and retrieval system without written consent. Information in this manual is subject to change without notice, and does not represent a commitment on the part of B&B Electronics Mfg. Co. Inc.

B&B Electronics Mfg. Co. Inc. shall not be liable for incidental or consequential damages resulting from the furnishing, performance, or use of this manual.

All brand names used in this manual are the registered trademarks of their respective owners. The use of trademarks or other designations in this publication is for reference purposes only and does not constitute an endorsement by the trademark holder.

Used symbols



Danger – Information regarding user safety or potential damage to the router.



Attention – Problems that can arise in specific situations.



Information, notice – Useful tips or information of special interest.

GPL license

Source codes under GPL license are available free of charge by sending an email to:

support@bbelec.com

Router version

The properties and settings associated with the cellular network connection are not available in non-cellular SPECTRE RT routers.

PPPoE configuration is only available on SPECTRE RT and XR5i v2 routers. It is used to set the PPPoE connection over Ethernet.



1. Access to the Web Configuration



Attention! The cellular router will not operate unless the cellular carrier has been correctly configured and the account activated and provisioned for data communications. For UMTS and LTE carriers, a SIM card must be inserted into the router. Do not insert the SIM card when the router is powered up.

You can monitor the status, configuration and administration of the router via the Web interface. To access the router over the web interface, enter `http://xxx.xxx.xxx.xxx` into the URL for the browser where `xxx.xxx.xxx.xxx` is the router IP address. The modem's default IP address is **192.168.1.1**. The default username is **root** and the default password is **root**.

The left side of the web interface displays the menu. You will find links for the *Status*, *Configuration*, *Customization* and *Administration* of the router.

Name and *Location* displays the router's name, location and SNMP configuration (see 3.17). These fields are user-defined for each router.

For enhanced security, you should change the default password. If the router's default password is set, the menu item **Change password** is highlighted in red.

Status	General Status
General	Mobile Connection
Mobile WAN	SIM Card : Primary
Network	Interface : usb0
DHCP	Flags : Multicast
IPsec	IP Address : Unassigned
DynDNS	State : Offline
System Log	> Less Information <
Configuration	Primary LAN
LAN	Interface : eth0
VRRP	Flags : Up, Running, Multicast
Mobile WAN	IP Address : 192.168.1.2 / 255.255.255.0
Backup Routes	MAC Address : 00:0A:14:81:6E:2A
Firewall	MTU : 1500 B
NAT	Rx Data : 13.2 KB
OpenVPN	Rx Packets : 116
IPsec	Rx Errors : 0
GRE	Rx Dropped : 0
L2TP	Rx Overruns : 0
PPTP	Tx Data : 130.8 KB
DynDNS	Tx Packets : 152
NTP	Tx Errors : 0
SNMP	Tx Dropped : 0
SMTP	Tx Overruns : 0
SMS	> Less Information <
Expansion Port 1	Secondary LAN
USB Port	Interface : eth1
Startup Script	Flags : Multicast
Up/Down Script	IP Address : Unassigned
Automatic Update	MAC Address : 00:0A:14:81:6E:2B
Customization	> Less Information <
User Modules	Peripheral Ports
Administration	Expansion Port 1 : Ethernet
Change Profile	Expansion Port 2 : None
Change Password	Binary Input : Off
Set Real Time Clock	Binary Output : Off
Set SMS Service Center	System Information
Unlock SIM Card	Firmware Version : 3.0.9 (2014-02-14)
Send SMS	Serial Number : 8900091
Backup Configuration	Profile : Standard
Restore Configuration	Supply Voltage : 12.3 V
Update Firmware	Temperature : 37 °C
Reboot	Time : 2014-04-08 15:37:32
	Uptime : 0 days, 0 hours, 1 minute

Figure 1: Web configuration

If the green LED is blinking, you may restore the router to its factory default settings by pressing RST on front panel. The configuration will be restored to the factory defaults and the router will reboot. (The green LED will be on during the reboot.)

1.1 Secured access to web configuration

The Web interface can be accessed through a standard web browser via a secure HTTPS connection.

Access the web interface by entering `https://192.168.1.1` in the web browser. You may receive a message that there is a problem with the website's security certificate. If you do, click on *Continue to this website*. If you wish to prevent this message, you must install a security certificate into the router.

Since the domain name in the certificate is given the MAC address of the router (such addresses use dashes instead of colons as separators), it is necessary to access the router under this domain name. For access to the router via a domain name, a DNS record must be added to the DNS table in the operating system.

There are three methods to add a domain name to the operating system:

- Editing `/etc/hosts` (Linux/Unix)
- Editing `C:\WINDOWS\system32\drivers\etc\hosts` (Windows XP)
- Configuring your own DNS server

To access the router with MAC address `00:11:22:33:44:55` securely, type the address `https://00-11-22-33-44-55` in the web browser. When accessing for the first time, it will be necessary to install a security certificate.



If using self signed certificate, the files `https_cert` and `https_key` has to be uploaded into `/etc/certs` directory of the router.

2. Status

2.1 General

A summary of basic information about the router and its activities can be invoked by selecting the *General* menu item. This page is also displayed when you login to the web interface. Information is divided into a several of separate blocks according to the type of router activity or the properties area – *Mobile Connection*, *Primary LAN*, *Peripherals Ports* and *System Information*. If your router is equipped with WIFI expansion port, there is also *WIFI* section.

2.1.1 Mobile Connection

Item	Description
SIM Card	Identification of the SIM card (<i>Primary</i> or <i>Secondary</i>)
Interface	Defines the interface
Flags	Displays network interface flags
IP Address	IP address of the interface
MTU	Maximum packet size that the equipment is able to transmit
Rx Data	Total number of received bytes
Rx Packets	Received packets
Rx Errors	Erroneous received packets
Rx Dropped	Dropped received packets
Rx Overruns	Lost received packets because of overload
Tx Data	Total number of sent bytes
Tx Packets	Sent packets
Tx Errors	Erroneous sent packets
Tx Dropped	Dropped sent packets
Tx Overruns	Lost sent packets because of overload
Uptime	Time indicating how long the connection to mobile network is established

Table 1: Mobile connection

2.1.2 Primary LAN

Items displayed in this part have the same meaning as items in the previous part. Moreover, there is information about the MAC address of the router (*MAC Address* item).

2.1.3 Peripheral Ports

Item	Description
Expansion Port 1	Expansion port fitted to the position 1 (<i>None</i> indicates that this position is equipped with no port)
Expansion Port 2	Expansion port fitted to the position 2 (<i>None</i> indicates that this position is equipped with no port)
Binary Input	State of binary input
Binary Output	State of binary output

Table 2: Peripheral Ports

2.1.4 System Information

Item	Description
Firmware Version	Information about the firmware version
Serial Number	Serial number of the router (in case of <i>N/A</i> is not available)
Profile	Current profile – standard or alternative profiles (profiles are used for example to switch between different modes of operation)
Supply Voltage	Supply voltage of the router
Temperature	Temperature in the router
Time	Current date and time
Uptime	Time indicating how long the router is used

Table 3: System Information

2.2 Mobile WAN Status



The SPECTRE RT and the XR5i v2 routers do not display the *Mobile WAN* status option.

The *Mobile WAN* menu item contains current information about connections to the mobile network. The first part of this page (*Mobile Network Information*) displays basic information about mobile network in which the router is operated. There is also information about the module, which is mounted in the router.

Item	Description
Registration	State of the network registration
Operator	Specifies the operator in whose network the router is operated
Technology	Transmission technology
PLMN	Code of operator
Cell	Cell to which the router is connected
LAC	Location Area Code – unique number assigned to each location area
Channel	Channel on which the router communicates
Signal Strength	Signal strength of the selected cell
Signal Quality	Signal quality of the selected cell: <ul style="list-style-type: none"> • EC/IO for UMTS and CDMA (it's the ratio of the signal received from the pilot channel – EC – to the overall level of the spectral density, ie the sum of the signals of other cells – IO) • RSRQ for LTE technology (Defined as the ratio $\frac{N \times RSRP}{RSSI}$)
CSQ	Cell Signal Quality, relative value is given by RSSI (dBm). 2–9 range means Marginal, 10–14 range means OK, 15–16 range means Good, 20–30 range means excellent.
Neighbours	Signal strength of neighboring hearing cells
Manufacturer	Module Manufacturer
Model	Type of module
Revision	Revision of module
IMEI	IMEI (International Mobile Equipment Identity) number of module
ESN	ESN (Electronic Serial Number) number of module (for CDMA routers)
MEID	MEID number of module
ICCID	Integrated Circuit Card Identifier is international and unique serial number of the SIM card.

Table 4: Mobile Network Information

If a neighboring cell is highlighted in red, there is a risk that the router may repeatedly switch between the neighboring cell and the primary cell. This can affect the performance of the router. To prevent this, re-orient the antenna or use a directional antenna.

The next section of this window displays historical information about the quality of the cellular WAN connection during each logging period. The router has standard intervals, such as the previous 24 hours and last week, and also includes information one user-defined interval.

Period	Description
Today	Today from 0:00 to 23:59
Yesterday	Yesterday from 0:00 to 23:59
This week	This week from Monday 0:00 to Sunday 23:59
Last week	Last week from Monday 0:00 to Sunday 23:59
This period	This accounting period
Last period	Last accounting period

Table 5: Description of period

Item	Description
Signal Min	Minimal signal strength
Signal Avg	Average signal strength
Signal Max	Maximal signal strength
Cells	Number of switch between cells
Availability	Availability of the router via the mobile network (expressed as a percentage)

Table 6: Mobile Network Statistics



Tips for *Mobile Network Statistics* table:

- Availability of connection to mobile network information is expressed as a percentage that is calculated by the ratio of the time when connection to a mobile network is established to the time when the router is turned on.
- When you place your cursor on the maximum or minimum signal strength, you will be shown the last time the router reached this signal strength. The middle part of this page displays information about transferred data and number of connections for both SIM card (for each period).

In the middle part of this page is displayed information about transferred data and number of connections for both SIM card (for each period).

Item	Description
RX data	Total volume of received data
TX data	Total volume of sent data
Connections	Number of connection to mobile network establish

Table 7: Traffic statistics

The last part (*Mobile Network Connection Log*) displays information about the mobile network connection and any problems that occurred while establishing them.

Mobile WAN Status

Mobile Network Information

Registration : Home Network

Operator : T-Mobile CZ

Technology : EDGE

PLMN : 23001

Cell : 69A6

LAC : 353E

Channel : 30

Signal Strength : -71 dBm

Neighbours : -83 dBm (80), -81 dBm (57), -93 dBm (59)

> More Information <

Mobile Network Statistics

Signal Min : -108 dBm Today Yesterday This Week Last Week This Period Last Period

Signal Avg : -71 dBm -121 dBm -121 dBm -121 dBm -121 dBm -121 dBm

Signal Max : -65 dBm -71 dBm -71 dBm -69 dBm -70 dBm -85 dBm

Signal Max : -65 dBm -65 dBm -65 dBm -63 dBm -63 dBm -58 dBm

Cells : 15 261 525 206 730 962

Availability : 99.7% 99.7% 99.7% 99.7% 99.7% 97.5%

Traffic Statistics for Primary SIM card

Rx Data : 12 KB Today Yesterday This Week Last Week This Period Last Period

Tx Data : 13 KB 21 KB 19402 KB 6366 KB 25768 KB 18868 KB

Connections : 2 19 KB 5167 KB 3382 KB 8549 KB 3726 KB

Connections : 2 7 20 36 56 49

Traffic Statistics for Secondary SIM card

Rx Data : 0 KB Today Yesterday This Week Last Week This Period Last Period

Tx Data : 0 KB 0 KB 0 KB 0 KB 0 KB 0 KB

Connections : 0 0 KB 0 KB 0 KB 0 KB 0 KB

Connections : 0 0 0 0 0 0

Mobile Network Connection Log

2013-07-10 11:52:40 Connection successfully established.

2013-07-10 21:17:21 Terminated by signal.

2013-07-10 21:18:01 Connection successfully established.

2013-07-11 08:39:20 Terminated by signal.

2013-07-11 08:40:01 Connection successfully established.

2013-07-11 09:22:24 Terminated by signal.

2013-07-11 09:23:08 Connection successfully established.

Figure 2: Mobile WAN status

2.3 WiFi



This item is available only if the router is equipped with a Wi-Fi module.

Select the *WiFi* item in the main menu of the web interface to see information about the Wi-Fi access point (AP) and associated stations.

Item	Description
hostapd state dump	Time to which statistical data relates
num_sta	Number of connected stations
num_sta_non_erp	Number of connected stations using 802.11b in 802.11g BSS connection
num_sta_no_short_slot_time	Number of stations not supporting the Short Slot Time
num_sta_no_short_preamble	Number of stations not supporting the Short Preamble

Table 8: State information about access point

Detailed information is displayed for each connected device. Most of them have an internal character. Here are two examples:

Item	Description
STA	MAC address of connected device (station)
AID	Identifier of connected device (1 – 2007). If 0 is displayed, the station is not currently connected.

Table 9: State information about connected clients

```

WiFi Status
WiFi AP Status

hostapd state dump - Mon Apr 7 12:49:50 2014
num_sta=1 num_sta_non_erp=0 num_sta_no_short_slot_time=1
num_sta_no_short_preamble=0

STA=20:02:af:2a:8f:b1
AID=1 flags=0xa3 [AUTH][ASSOC][AUTHORIZED][SHORT_PREAMBLE]
capability=0x21 listen_interval=10
supported_rates=82 84 0b 16
timeout_next=NULLFUNC POLL
  
```

Figure 3: WiFi Status

2.4 WiFi Scan



This item is available only if the router is equipped with a Wi-Fi module.

Selecting the *WiFi Scan* item scans for neighboring Wi-Fi networks and displays the results. **Scanning can only be performed if the access point (WiFi AP) is off.**

item	Description
BSS	MAC address of access point (AP)
TSF	A Timing Synchronization Function (TSF) keeps the timers for all stations in the same Basic Service Set (BSS) synchronized. All stations shall maintain a local TSF timer.
freq	Frequency band of WiFi network [kHz]
beacon interval	Period of time synchronization
capability	List of access point (AP) properties
signal	Signal level of access point (AP)
last seen	Last response time of access point (AP)
SSID	Identifier of access point (AP)
Supported rates	Supported rates of access point (AP)
DS Parameter set	The channel on which access point (AP) broadcasts
ERP	Extended Rate PHY – information element providing backward compatibility
Extended supported rates	Supported rates of access point (AP) that are beyond the scope of eight rates mentioned in <i>Supported rates</i> item
RSN	Robust Secure Network – The protocol for establishing a secure communication through wireless network 802.11

Table 10: Information about neighbouring WiFi networks

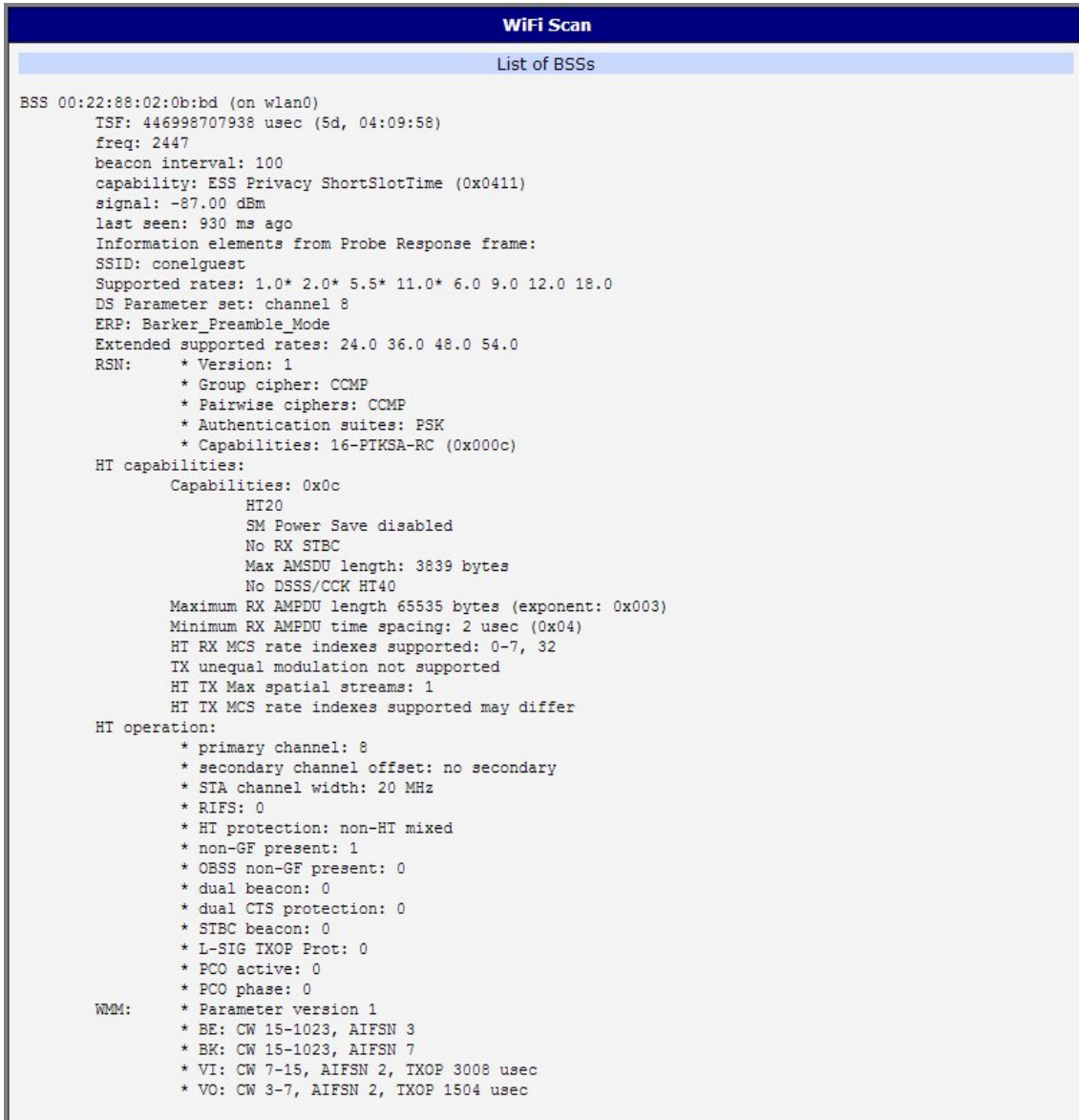


Figure 4: WiFi Scan

2.5 Network status

Select the *Network* menu item to view the current system information for the router. The upper part of the window displays detailed information about the active interfaces.

Interface	Description
eth0, eth1	Network interfaces (ethernet connection)
usb0	Mobile Network interface (active connection to mobile network)
wlan0	WiFi interface
ppp0	PPP interface (e.g. PPPoE tunnel)
tun0	OpenVPN tunnel interface
ipsec0	IPSec tunnel interface
gre1	GRE tunnel interface
lo	Local loopback interface

Table 11: Interface connection status

The following detailed information will be shown for each active connection:

Item	Description
HWaddr	Hardware MAC (unique) address of primary network interface
inet	IP address of primary network interface
P-t-P	IP address second ends connection
Bcast	Broadcast address
Mask	Network Subnet Mask
MTU	Maximum transmittable packet size
Metric	Number of routers that the packet must pass through
RX	<ul style="list-style-type: none"> • packets – number of received packets • errors – number of errors • dropped – number of dropped packets • overruns – number of incoming packets lost because of overload • frame – number of frame errors
TX	<ul style="list-style-type: none"> • packets – number of transmit packets • errors – number of packet errors • dropped – number of dropped packets • overruns – number of outgoing packets lost because of overload • carrier – outgoing packet errors resulting from the physical layer

Continued on next page

Continued from previous page

Item	Description
collisions	Number of collisions on physical layer
txqueuelen	Number of packets in the transmit queue
RX bytes	Total number of received bytes
TX bytes	Total number of transmitted bytes

Table 12: Description of information in network status

You may view the status of the mobile network connection from the *Network* information screen. If the connection to mobile network is active, it will be displayed as ppp0 interface.



For the SPECTRE RT industrial routers and the XR5i v2 routers, interface ppp0 indicates the PPPoE connection.

Network Status						
Interfaces						
eth0	Link encap:Ethernet HWaddr 00:11:22:33:44:55 inet addr:192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:407 errors:0 dropped:0 overruns:0 frame:0 TX packets:461 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:32 RX bytes:51793 (50.5 KB) TX bytes:321807 (314.2 KB) Interrupt:23					
ppp0	Link encap:Point-Point Protocol inet addr:10.169.80.137 P-t-P:10.0.0.1 Mask:255.255.255.255 UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1 RX packets:35 errors:0 dropped:0 overruns:0 frame:0 TX packets:46 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:3 RX bytes:7772 (7.5 KB) TX bytes:8716 (8.5 KB)					
Route Table						
Destination	Gateway	Genmask	Flags	Metric	Ref	Use Iface
10.0.0.1	0.0.0.0	255.255.255.255	UH	0	0	0 ppp0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0 eth0
0.0.0.0	10.0.0.1	0.0.0.0	UG	0	0	0 ppp0

Figure 5: Network status

2.6 DHCP status

Information about the DHCP server can be accessed by selecting the *DHCP status*. The DHCP server provides automatic configuration of the client devices connected to the router. The DHCP server assigns each device an IP address, subnet mask, default gateway (IP address of router) and DNS server (IP address of router).

For each client in the list, the DHCP status window displays the following information.

Item	Description
lease	Assigned IP address
starts	Time that the IP address was assigned
ends	Time that the IP address lease expires
hardware ethernet	Hardware MAC (unique) address
uid	Unique ID
client-hostname	Computer name

Table 13: DHCP status description



The DHCP status may occasionally display two records for one IP address. This may be caused by resetting the client network interface.

DHCP Status	
Active DHCP Leases (Primary LAN)	
lease 192.168.1.2 {	
starts 1 2011/01/17 08:08:37;	
ends 1 2011/01/17 08:18:37;	
hardware ethernet 00:1d:92:25:72:33;	
uid 01:00:1d:92:25:72:33;	
client-hostname "felgr2";	
}	
Active DHCP Leases (WLAN)	
No active dynamic DHCP leases.	

Figure 6: DHCP status

Note: Starting with firmware 4.0.0, records in the *DHCP status* window are divided into two separate parts – *Active DHCP Leases (Primary LAN)* and *Active DHCP Leases (WLAN)*.

2.7 IPsec status

Selecting the *IPsec* option in the status menu of the web page will bring up the information for any IPsec Tunnels that have been established. Up to four IPsec tunnels can be created. If no IPsec tunnels are configured, the status will show that *IPsec is disabled*.

If an IPsec tunnel is established, the router will show *IPsec SA established* (highlighted in red) in the IPsec status information.

IPsec Status	
IPsec Tunnels Information	
<pre> interface eth0/eth0 192.168.2.250 interface ppp0/ppp0 10.0.0.132 !myid = (none) debug none "ipsecl": 192.168.2.0/24===10.0.0.132...10.0.1.228===192.168.1.0/24; erouted; eroute owner: #2 "ipsecl": myip=unset; hisip=unset; myup=/etc/scripts/updown; hisup=/etc/scripts/updown; "ipsecl": ike_life: 3600s; ipsec_life: 3600s; rekey_margin: 540s; rekey_fuzz: 100%; keyingtries: 0 "ipsecl": policy: PSK+ENCRYPT+TUNNEL+UP; prio: 24,24; interface: ppp0; "ipsecl": newest ISAKMP SA: #1; newest IPsec SA: #2; "ipsecl": IKE algorithm newest: AES_CBC_128-SHA1-MODP2048 #2: "ipsecl":500 STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in 2708s; newest IPSEC; erout #2: "ipsecl" esp.d07e3080@10.0.1.228 esp.783be7ee@10.0.0.132 tun.0@10.0.1.228 tun.0@10.0.0.132 ref=0 refhim=4294 #1: "ipsecl":500 STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in 2733s; newest ISAKMP; lastdpd=-1s(se </pre>	

Figure 7: IPsec status

2.8 DynDNS status

The router supports DynamicDNS using a DNS server on www.dyndns.org. If Dynamic DNS is configured, the status can be displayed by selecting menu option *DynDNS*. Refer to www.dyndns.org for more information on how to configure a Dynamic DNS client.

DynDNS Status
Last DynDNS Update Status
DynDNS record successfully updated.

Figure 8: DynDNS status

DynDNS report messages:

- DynDNS client is disabled.
- Invalid username or password.
- Specified hostname doesn't exist.
- Invalid hostname format.
- Hostname exists, but not under specified username.
- No update performed yet.
- DynDNS record is already up to date.
- DynDNS record successfully update.
- DNS error encountered.
- DynDNS server failure.



For Dynamic DNS to function properly, the router's SIM card must have a public IP address assigned.

2.9 System Log

If you are having problems with a GPRS connection, use the *System Log* menu item to view the router system log. The system log contains helpful information about the operation of the router. Only the most recent information is shown on the screen, but older log entries can be viewed by saving the system log to a file and opening it with a text editor. The *Save Log* button allows you to save the system log to a log file whereas the *Save Report* button allows you to save the system log as a text file in report format. The system log is cleared when the unit re-boots.

The Syslog default size is 1000 lines. When the system log reaches the maximum size, a new log file is started. After completion of 1000 lines (maximum size) in the second file, the first file is overwritten with the new one.

The program syslogd can be run on the router to configure the system log. The syslogd option "-s" followed by a decimal number will set the maximum number of lines in the log file. The "-r" option followed by the hostname or IP address will enable logging to a syslog daemon on a remote computer. On remote Linux machines, the syslog daemon is enabled by running syslogd with the parameter "-r". On remote Windows machines, a syslog server such as Syslog Watcher must be installed.

To enable remote logging when the router powers up, modify the script `/etc/init.d/syslog` or insert the commands `"killall syslogd"` and `"syslogd <options>"` into the startup script.

System Log

System Messages

```

2013-07-02 12:46:14 System log daemon started.
2013-07-02 12:46:19 pppsd[426]: pppsd started
2013-07-02 12:46:19 pppsd[426]: module is turned on
2013-07-02 12:46:19 pppsd[426]: selected SIM: 1st
2013-07-02 12:46:19 dnsmasq[453]: started, version 2.59 cachesize 150
2013-07-02 12:46:19 dnsmasq[453]: cleared cache
2013-07-02 12:46:19 bard[455]: bard started
2013-07-02 12:46:19 pppsd[426]: selected APN: conel.agnep.cz
2013-07-02 12:46:19 pppsd[426]: waiting for registration
2013-07-02 12:46:20 pppsd[426]: starting usbd
2013-07-02 12:46:20 usbd[500]: usbd started
2013-07-02 12:46:20 usbd[500]: establishing connection
2013-07-02 12:46:20 sshd[506]: Server listening on 0.0.0.0 port 22.
2013-07-02 12:46:29 usbd[500]: connection established
2013-07-02 12:46:29 usbd[500]: local IP address 10.0.1.229
2013-07-02 12:46:29 usbd[500]: primary   DNS address 10.0.0.1
2013-07-02 12:46:29 bard[455]: backup route selected: "Mobile WAN"
2013-07-02 12:46:29 bard[455]: script /etc/scripts/ip-up started
2013-07-02 12:46:30 bard[455]: script /etc/scripts/ip-up finished, status = 0x0
2013-07-02 12:46:31 dnsmasq[453]: reading /etc/resolv.conf
2013-07-02 12:46:31 dnsmasq[453]: using nameserver 10.0.0.1#53
                
```

Save Log
Save Report

Figure 9: System Log

The following example (figure) shows how to send syslog information to a remote server at 192.168.2.115 on startup.

Startup Script

Startup Script

```

#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here.

killall syslogd
syslogd -R 192.168.2.115
                
```

Figure 10: Example program syslogd start with the parameter -r

3. Configuration

3.1 LAN configuration

Select the *LAN* menu item to enter the network configuration for the Ethernet ports. The main Ethernet port, *ETH*, is setup in the *Primary LAN* section. If the router has additional Ethernet ports (*PORT1* or *PORT2*), they are configured under the *Secondary LAN* section. For routers with two additional Ethernet ports, *PORT1* and *PORT2* are automatically bridged together.

Item	Description
DHCP Client	<ul style="list-style-type: none"> • disabled – The router will not obtain an IP address automatically from a DHCP server on the network. • enabled – The router will attempt to obtain an IP address automatically from a DHCP server on the network.
IP address	Fixed IP address of the network interface.
Subnet Mask	IP address Subnet Mask for the interface.
Bridged	<ul style="list-style-type: none"> • no – router is not used as a bridge (default) • yes – router is used as a bridge
Media type	<ul style="list-style-type: none"> • Auto-negotiation – The router automatically selects the communication speed of the network interface. • 100 Mbps Full Duplex – The router communicates at 100Mbps, in the full duplex mode. • 100 Mbps Half Duplex – The router communicates at 100Mbps, in the half duplex mode. • 10 Mbps Full Duplex – The router communicates at 10Mbps, in the full duplex mode. • 10 Mbps Half Duplex – The router communicates at 10Mbps, in the half duplex mode.
Default Gateway	IP address of Default gateway for the router. When entering the IP address of default gateway, all packets for which the record was not found in the routing table are sent to this address.
DNS server	IP address of the primary DNS server for the router, and the address to which all DNS questions will be forwarded.

Table 14: Configuration of network interface

The *Default Gateway* and *DNS Server* items are only used if the *DHCP Client* item is disabled, and if the Primary or Secondary LAN is selected by the Backup Routes system as a default route. (The backup routes selection algorithm is described in in section 3.7 *Backup Routes*).

There can be only one active bridge on the router at a time. Only the parameters *DHCP Client*, *IP address* and *Subnet Mask* can be used to configure the bridge. The Primary LAN has the higher priority when both interfaces (eth0, eth1) are added to the bridge. Other interfaces (wlan0 – wifi) can be added (or deleted) to (from) an existing bridge at any time. Moreover, the bridge can be created on demand for such interfaces but not configured by their respective parameters.

The DHCP server assigns the IP address, default gateway IP address, and IP address of the DNS server to the connected DHCP clients. If these values are filled-in by the user in the configuration form, they are preferred.


The DHCP server supports both static and dynamic assignment of IP addresses. In *Dynamic IP address* assignment, the DHCP server will assign a client the next available IP address from the allowed IP address pool. *Static DHCP* assigns IP addresses that correspond to the MAC addresses of connected clients.

Item	Description
Enable dynamic DHCP leases	Select this option to enable a dynamic DHCP server.
IP Pool Start	Starting IP address of the range allocated to the DHCP clients.
IP Pool End	Ending IP address of the range allocated to the DHCP clients.
Lease time	Time in seconds that the IP address is reserved before it can be re-used.

Table 15: Configuration of dynamic DHCP server

Item	Description
Enable static DHCP leases	Select this option to enable a static DHCP server.
MAC Address	MAC address of a DHCP client.
IP Address	Assigned IP address.

Table 16: Configuration of static DHCP server

 Do not overlap the static IP addresses with the addresses allocated by the dynamic DHCP address pool. Otherwise, the network may function incorrectly.

Example of the network interface configuration for a dynamic DHCP server:

- The range of dynamically allocated addresses is from 192.168.1.2 to 192.168.1.4.
- The addresses are allocated 600 second (10 minutes).

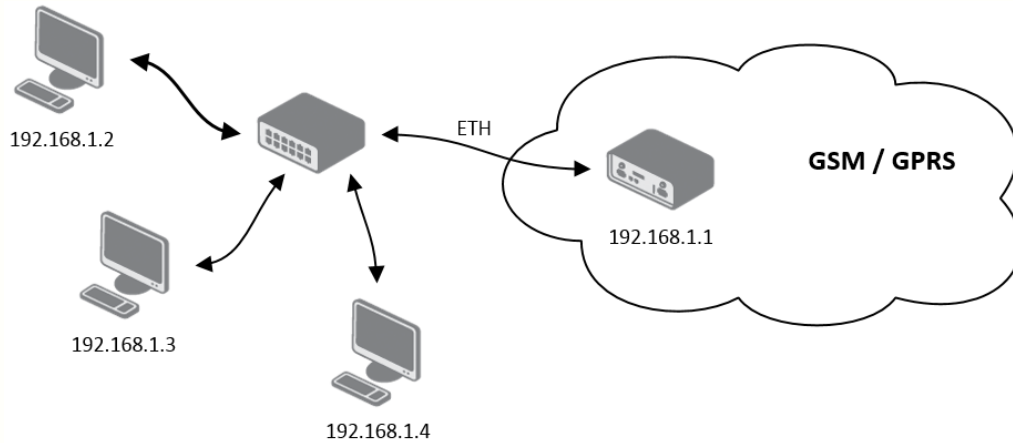


Figure 11: Example 1 – Network Topology for Dynamic DHCP Server

LAN Configuration			
	Primary LAN		Secondary LAN
DHCP Client	disabled		enabled
IP Address	192.168.1.1		
Subnet Mask	255.255.255.0		
Bridged	no		no
Media Type	auto-negotiation		auto-negotiation
Default Gateway			
DNS Server			
<input checked="" type="checkbox"/> Enable dynamic DHCP leases			
IP Pool Start	192.168.1.2		
IP Pool End	192.168.1.4		
Lease Time	600 sec		
<input type="checkbox"/> Enable static DHCP leases			
MAC Address	IP Address		
<input type="button" value="Apply"/>			

Figure 12: Example 1 – LAN Configuration Page

Example of the network interface with dynamic and static DHCP server:

- The allocated address range is from 192.168.1.2 to 192.168.1.4.
- The address is allocated for 10 minutes.
- The client with MAC address 01:23:45:67:89:ab has IP address 192.168.1.10.
- The client with MAC address 01:54:68:18:ba:7e has IP address 192.168.1.11.

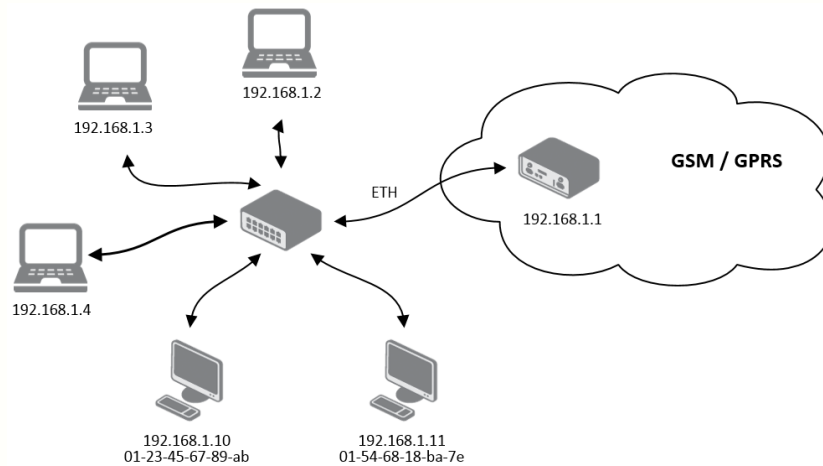


Figure 13: Example 2 – Network Topology with both Static and Dynamic DHCP Servers

LAN Configuration			
	Primary LAN		Secondary LAN
DHCP Client	disabled	enabled	
IP Address	192.168.1.1		
Subnet Mask	255.255.255.0		
Bridged	no	no	
Media Type	auto-negotiation	auto-negotiation	
Default Gateway			
DNS Server			
<input checked="" type="checkbox"/> Enable dynamic DHCP leases			
IP Pool Start	192.168.1.2		
IP Pool End	192.168.1.4		
Lease Time	600 sec		
<input checked="" type="checkbox"/> Enable static DHCP leases			
MAC Address	IP Address		
01:23:45:67:89:ab	192.168.1.10		
01:54:68:18:ba:7e	192.168.1.11		
<input type="button" value="Apply"/>			

Figure 14: Example 2 – LAN Configuration Page

Example of the network interface with default gateway and DNS server:

- Default gateway IP address is 192.168.1.20
- DNS server IP address is 192.168.1.20

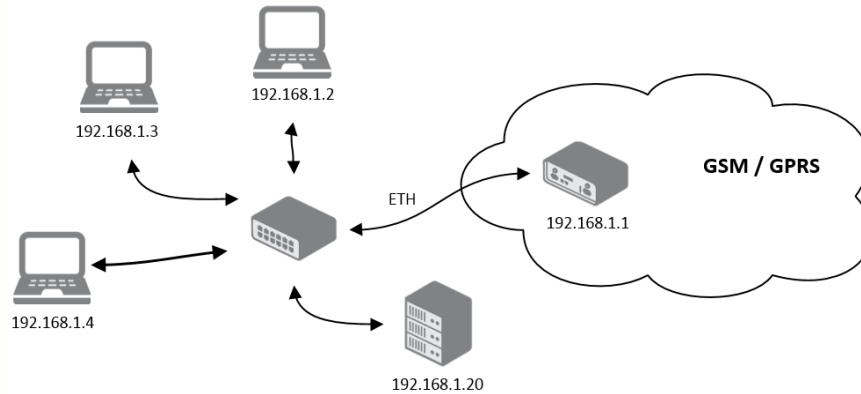


Figure 15: Example 3 – Network Topology

LAN Configuration			
	Primary LAN		Secondary LAN
DHCP Client	<input type="text" value="disabled"/>	<input type="text" value="enabled"/>	
IP Address	<input type="text" value="192.168.1.1"/>	<input type="text"/>	
Subnet Mask	<input type="text" value="255.255.255.0"/>	<input type="text"/>	
Bridged	<input type="text" value="no"/>	<input type="text" value="no"/>	
Media Type	<input type="text" value="auto-negotiation"/>	<input type="text" value="auto-negotiation"/>	
Default Gateway	<input type="text" value="192.168.1.20"/>	<input type="text"/>	
DNS Server	<input type="text" value="192.168.1.20"/>	<input type="text"/>	
<input checked="" type="checkbox"/> Enable dynamic DHCP leases			
IP Pool Start	<input type="text" value="192.168.1.2"/>		
IP Pool End	<input type="text" value="192.168.1.4"/>		
Lease Time	<input type="text" value="600"/>	sec	
<input type="checkbox"/> Enable static DHCP leases			
MAC Address	IP Address		
<input type="text"/>	<input type="text"/>		
<input type="text"/>	<input type="text"/>		
<input type="text"/>	<input type="text"/>		
<input type="text"/>	<input type="text"/>		
<input type="text"/>	<input type="text"/>		
<input type="text"/>	<input type="text"/>		
<input type="button" value="Apply"/>			

Figure 16: Example 3 – LAN Configuration Page

3.2 VRRP configuration

Select the *VRRP* menu item to enter the VRRP configuration. VRRP protocol (Virtual Router Redundancy Protocol) allows you to transfer packet routing from the main router to a backup router in case the main router fails. (This can be used to provide a wireless cellular backup to a primary wired router in critical applications.) If the *Enable VRRP* is checked, you may set the following parameters.

Item	Description
Virtual Server IP Address	This parameter sets the virtual server IP address. This address must be the same for both the primary and backup routers. Devices on the LAN will use this address as their default gateway IP address.
Virtual Server ID	This parameter distinguishes one virtual router on the network from another. The main and backup routers must use the same value for this parameter.
Host Priority	The active router with highest priority set by the parameter Host Priority, is the main router. According to RFC 2338, the main router should have the highest possible priority – 255. The backup router(s) have a priority in the range 1 – 254 (default value is 100). A priority value of 0 is not allowed.

Table 17: VRRP configuration

You may set the *Check connection* flag in the second part of the window to enable automatic test messages for the cellular network. In some cases, the mobile WAN connection could still be active but the router will not be able to send data over the cellular network. This feature is used to verify that data can be sent over the PPP connection and supplements the normal VRRP message handling. The currently active router (main/backup) will send test messages to the defined *Ping IP Address* at periodic time intervals (*Ping Interval*) and wait for a reply (*Ping Timeout*). If the router does not receive a response to the Ping command, it will retry up to the number of times specified by the *Ping Probes* parameter. After that time, it will switch itself to a backup router until the PPP connection is restored.

Item	Description
Ping IP Address	Destinations IP address for the Ping commands. IP Address can not be specified as a domain name.
Ping Interval	Interval in seconds between the outgoing Pings.
Ping Timeout	Time in seconds to wait for a response to the Ping.
Ping Probes	Maximum number of failed ping requests.

Table 18: Check connection



You may use the DNS server of the mobile carrier as the destination IP address for the test messages (Pings).

The *Enable traffic monitoring* option can be used to reduce the number of messages that are sent to test the PPP connection. When this parameter is set, the router will monitor the interface for any packets different from a ping. If a response to the packet is received within the timeout specified by the *Ping Timeout* parameter, then the router knows that the connection is still active. If the router does not receive a response within the timeout period, it will attempt to test the mobile WAN connection using standard Ping commands.

Example of the VRRP protocol:

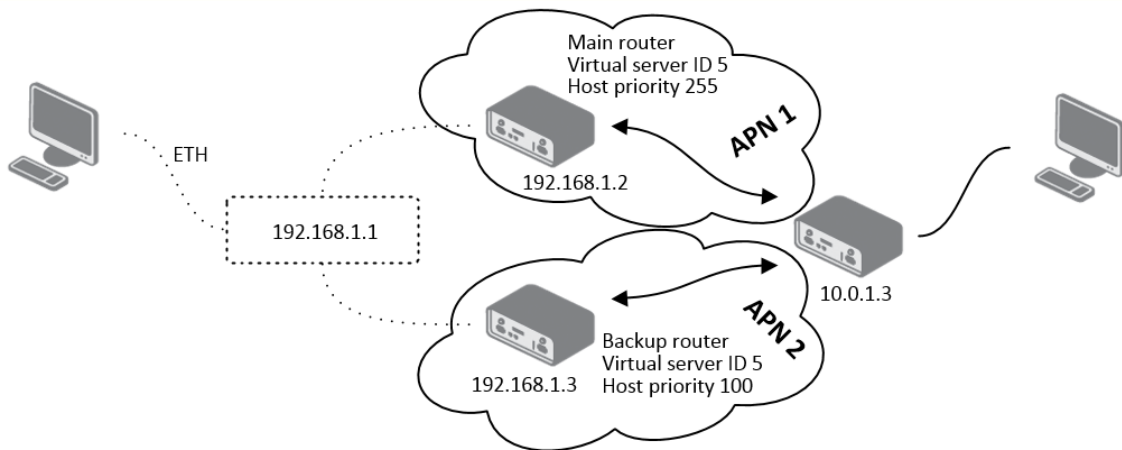


Figure 17: Topology of example VRRP configuration

VRRP Configuration	
<input checked="" type="checkbox"/> Enable VRRP	
Virtual Server IP Address	192.168.1.1
Virtual Server ID	5
Host Priority	255
<input checked="" type="checkbox"/> Check connection	
Ping IP Address	10.0.1.3
Ping Interval	10 sec
Ping Timeout	5 sec
Ping Probes	10
<input type="checkbox"/> Enable traffic monitoring	
<input type="button" value="Apply"/>	

Figure 18: Example of VRRP configuration – main router

VRRP Configuration	
<input checked="" type="checkbox"/> Enable VRRP	
Virtual Server IP Address	<input type="text" value="192.168.1.1"/>
Virtual Server ID	<input type="text" value="5"/>
Host Priority	<input type="text" value="100"/>
<input checked="" type="checkbox"/> Check connection	
Ping IP Address	<input type="text" value="10.0.1.3"/>
Ping Interval	<input type="text" value="10"/> sec
Ping Timeout	<input type="text" value="5"/> sec
Ping Probes	<input type="text" value="10"/>
<input type="checkbox"/> Enable traffic monitoring	
<input type="button" value="Apply"/>	

Figure 19: Example of VRRP configuration – backup router

3.3 Mobile WAN configuration



The SPECTRE RT and the XR5i v2 industrial routers do not display the *Mobile WAN* configuration option.

Select the *Mobile WAN* menu item to enter the cellular network configuration page.

3.3.1 Connection to mobile network

If the *Create connection to mobile network* item is selected, the router automatically tries to establish connection after switching-on.

Item	Description
APN	Network identifier (Access Point Name)
Username	User name to log into the GSM network
Password	Password to log into the GSM network
Authentication	Authentication protocol in GSM network: <ul style="list-style-type: none"> • PAP or CHAP – authentication method is chosen by router • PAP – PAP authentication method • CHAP – CHAP authentication method
IP Address	IP address of SIM card. The user sets the IP address, only if the IP address was assigned by the operator.
Phone Number	Telephone number to dial GPRS or CSD connection. The default telephone number is *99***1 #.
Operator	The defined PLNM preferred carrier code
Network type	<ul style="list-style-type: none"> • Automatic selection – router automatically selects transmission method according to the availability of transmission technology • <i>Furthermore, according to the type of router</i> – it's also possible to select a specific method of data transmission (GPRS, UMTS, ...)
PIN	PIN parameter should be set only if it requires a SIM card router. SIM card is blocked after several bad attempts to enter the PIN.
MRU	Maximum Receiving Unit – Identifier of maximum size of packet which can be received in a given environment. Default value is 1500 B. Other settings may cause incorrect transmission of data.
MTU	Maximum Transmission Unit – Identifier of max. size of packet which can be transferred in a given environment. Default value is 1500 B. Other settings may cause incorrect transmission of data.


Table 19: Mobile WAN connection configuration



Tips for working with the *Mobile WAN* configuration form:

- If the MTU value is set incorrectly, data transfer may fail. If the MTU value is too low it causes more frequent fragmentation of the data. That increases overhead as well as making it more likely that packets may be damaged during defragmentation. If the MTU value is too high, the network might not transfer the packet.
- If the *IP address* field is not filled in, the router automatically assigns the IP address when it is establishing the connection. If an IP address is supplied by the operator, the router accelerates access to the network.
- If the *APN* field is not filled in, the router automatically selects the APN according to the IMSI code of the SIM card. If the PLMN (operator number format) is not in the list of APNs, then the default APN is "internet". The mobile operator defines APN.
- If the word *blank* is entered in the *APN* field, the router interprets APN as blank.

ATTENTION:

- 
- **If only one SIM card is installed in the router (or the router has one only one SIM card slot), the router switches between the APN options. A router with two SIM cards switches between SIM cards.**
 - **The correct PIN must be filled in. SIM cards with two APNs will use the same PIN for both APNs. An incorrect PIN can block the SIM card.**

Items marked with an asterisk only need to be filled in if this information is required by the operator (carrier).

If establishing a connection to the mobile network is unsuccessful, it is recommended to check the accuracy of the entered data. Alternatively, try a different authentication method or network type.

3.3.2 DNS address configuration

The *DNS Settings* item is designed to make configuration easier on the client side. When this item is set to the value *get from operator*, the router will attempt to automatically get the IP addresses of the primary and secondary DNS server from the operator. Alternatively, the *set manually* option allows you to set the IP addresses of Primary DNS servers manually (using the *DNS Server* item).

3.3.3 Check connection to mobile network configuration

If the *Check Connection* item is set to *enabled* or *enabled + bind*, it activates checking the connection to the mobile network. The router will automatically send ping requests to the specified domain or IP address (*Ping IP Address* item) at regular time intervals (*Ping Interval*). In case of unsuccessful ping, a new one will be sent after ten seconds. If it fails to ping the IP

address three times in a row, the router terminates the current connection and tries to establish new ones. Checking can be set separately for two SIM cards or two APNs. Send an ICMP to an IP address that you know is still functional. (The operator's DNS server, for example.)

If the *Check Connection* item is set to the *enabled* option, ping requests are sent on the basis of routing table. Thus, the requests may be sent through any available interface. If you require each ping request to be sent through the network interface, which was created when establishing a connection to the mobile operator, it is necessary to set the *Check Connection* item to *enabled + bind*. The *disabled* option deactivates checking the connection to the mobile network.

Item	Description
Ping IP Address	Destinations IP address or domain name of ping queries.
Ping Interval	Time intervals between the outgoing pings.

Table 20: Check connection to mobile network configuration

If the *Enable Traffic Monitoring* option is selected, the router stops sending ping questions to the Ping IP Address and it will watch traffic on the connection to the mobile network. If this connection is without traffic longer than the *Ping Interval*, the router sends ping questions to the Ping IP Address.



Attention! The feature of check connection to mobile network is necessary for uninterrupted operation.

3.3.4 Data limit configuration

Item	Description
Data limit	With this parameter you can set the maximum expected amount of data transmitted (sent and received) over GPRS in one billing period (month).
Warning Threshold	Parameter <i>Warning Threshold</i> determines percentage of Data Limit in the range of 50% to 99%. If exceeded, the router sends an SMS in the form <i>Router has exceeded (value of Warning Threshold) of data limit</i> .
Accounting Start	Parameter sets the day of the month in which the billing cycle starts SIM card used. Start of the billing period defines the operator, which has provided the SIM card. The router begins to count the transferred data since that day.

Table 21: Data limit configuration




If the parameters *Switch to backup SIM card when data limit is exceeded* and *switch to default SIM card when data limit isn't exceeded* (see next subsection) or *Send SMS when data limit is exceeded* (see SMS configuration) are not selected, the data limit will be ignored.

3.3.5 Switch between SIM cards configuration

You may define rules in the router for switching between two APNs on one SIM card or between two SIM cards or network providers. The router can automatically switch between the network setups when the active connection to mobile network is lost, the data limit is exceeded, or the binary input on the front panel goes active.

Item	Description
Default SIM card	This parameter sets the default APN or SIM card for the connection to mobile network. If this parameter is set to <i>none</i> , the router boots up in off-line mode and it will be necessary to initiate the connection to mobile network by sending an SMS message to the router.
Backup SIM card	Defines the backup APN or SIM card.

Table 22: Default and backup SIM configuration

 If parameter *Backup SIM card* is set to *none*, then parameters *Switch to other SIM card when connection fails*, *Switch to backup SIM card when roaming is detected* and *switch to default SIM card when home network is detected* and *Switch to backup SIM card when data limit is exceeded* and *switch to default SIM card when data limit isn't exceeded* will switch the router to off-line mode.

Item	Description
Switch to other SIM card when connection fails	If the connection to mobile network fails, the router will switch to the secondary SIM card or secondary APN of the SIM card. The router will switch to the backup SIM card if the router is unable to establish a connection to mobile network after 3 attempts or the Check the connection to mobile network option is selected and the router detects that the connection to mobile network has failed.
Switch to backup SIM card when roaming is detected and switch to default SIM card when home network is detected	If roaming is detected, this option forces the router to switch to the secondary SIM card or secondary APN of the SIM card. If the home network is detected, this option enables switching back to the default SIM card. For proper operation, it is necessary to enable roaming on your SIM card!
Switch to backup SIM card when data limit is exceeded and switch to default SIM card when data limit isn't exceeded	This option enables the router to switch to the secondary SIM card or secondary APN of the SIM card when the data limit of default APN is exceeded. This option also enables switching back to default SIM card, when data limit is not exceeded.

Continued on next page

Continued from previous page

Item	Description
Switch to backup SIM card when binary input is active switch to default SIM card when binary input isn't active	This parameter forces the router to switch to the secondary SIM card or secondary APN of the SIM card when binary input 'bin0' is active. If the binary input isn't active, this option enables switching back to the default SIM card.
Switch to default SIM card after timeout	This parameter defines the method the router will use to try to switch back to the default SIM card or default APN.

Table 23: Switch between SIM card configurations

The following parameters define the time after which the router attempts to go back to the default SIM card or APN.

Item	Description
Initial timeout	The first attempt to switch back to the primary SIM card or APN shall be made for the time defined in the parameter <i>Initial Timeout</i> . The range of this parameter is from 1 to 10000 minutes.
Subsequent Timeout	After an unsuccessful attempt to switch to the default SIM card, the router will make a second attempt after the amount of time defined in the parameter <i>Subsequent Timeout</i> . The range is from 1 to 10000 minutes.
Additive constants	Any further attempts to switch back to the primary SIM card or APN shall be made after a timeout computed as the sum of the previous timeout period and the time defined in the parameter <i>Additive constant</i> . The range is from 1 to 10000 minutes.

Table 24: Switch between SIM card configurations

Example:

Option *Switch to primary SIM card after timeout* is checked and the parameters are set as follows: *Initial Timeout* = 60 min, *Subsequent Timeout* = 30 min, *Additive Constant* = 20 min.

The first attempt to switch back to the primary SIM card or APN shall be carried out after 60 minutes. The second attempt will be made 30 minutes later. The third attempt will be made after 50 minutes (30+20). The fourth attempt will be made after 70 minutes (30+20+20).

3.3.6 Dial-In access configuration



Dial-In access configuration is supported for these routers only: ER75i, UR5, ER75i v2 and UR5 v2.

You may define access over CSD connection by selecting the *Enable Dial-In Access* function. Access can be secured by using the *Username* and *Password*. If the router does not have a connection to a mobile network, you may use this function to gain access to the router via dial-up connections. The router waits two minutes to accept connections. If no one logs on during this time the router will make another attempt to establish a GPRS connection.

Item	Description
Username	User name for secured Dial-In access.
Password	Password for secured Dial-In access.

Table 25: Dial-In access configuration

3.3.7 PPPoE bridge mode configuration

If the *Enable PPPoE bridge mode* option is selected, the router will activate the PPPoE bridge protocol. PPPoE (Point-to-Point over Ethernet) is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. This feature allows a device connected to the ETH port of the router to create a PPP connection with the cellular network. The changes in settings will apply after pressing the *Apply* button.

Mobile WAN Configuration			
<input type="checkbox"/> Create connection to mobile network			
	Primary SIM card	Secondary SIM card	
APN *	<input type="text"/>	<input type="text"/>	
Username *	<input type="text"/>	<input type="text"/>	
Password *	<input type="text"/>	<input type="text"/>	
Authentication	PAP or CHAP <input type="button" value="v"/>	PAP or CHAP <input type="button" value="v"/>	
IP Address *	<input type="text"/>	<input type="text"/>	
Phone Number *	<input type="text"/>	<input type="text"/>	
Operator *	<input type="text"/>	<input type="text"/>	
PIN *	<input type="text"/>	<input type="text"/>	
MRU	1500	1500	bytes
MTU	1500	1500	bytes
DNS Settings	get from operator <input type="button" value="v"/>	get from operator <input type="button" value="v"/>	
DNS Server	<input type="text"/>	<input type="text"/>	
<i>(The feature of check connection to mobile network is necessary for uninterrupted operation)</i>			
Check Connection	disabled <input type="button" value="v"/>	disabled <input type="button" value="v"/>	
Ping IP Address	<input type="text"/>	<input type="text"/>	
Ping Interval	<input type="text"/>	<input type="text"/>	sec
<input type="checkbox"/> Enable traffic monitoring			
Data Limit	<input type="text"/>	MB	
Warning Threshold	<input type="text"/>	%	
Accounting Start	1		
Default SIM card	primary <input type="button" value="v"/>		
Backup SIM card	secondary <input type="button" value="v"/>		
<input type="checkbox"/> Switch to other SIM card when connection fails <input type="checkbox"/> Switch to backup SIM card when roaming is detected and switch to default SIM card when home network is detected <input type="checkbox"/> Switch to backup SIM card when data limit is exceeded and switch to default SIM card when data limit isn't exceeded <input type="checkbox"/> Switch to backup SIM card when binary input is active and switch to default SIM card when binary input isn't active <input type="checkbox"/> Switch to default SIM card after timeout			
Initial Timeout	60	min	
Subsequent Timeout *	<input type="text"/>	min	
Additive Constant *	<input type="text"/>	min	
<input type="checkbox"/> Enable Dial-In access			
Username *	<input type="text"/>		
Password *	<input type="text"/>		
<input type="checkbox"/> Enable PPPoE bridge mode			
* can be blank			
<input type="button" value="Apply"/>			

Figure 20: Mobile WAN configuration

Example 1: The figure below describes the situation, when the connection to mobile network is controlled on the address 8.8.8.8 in the time interval of 60 s for primary SIM card and on the address www.google.com in the time interval 80 s for secondary SIM card. In the case of traffic on the router the control pings are not sent, but the traffic is monitored.

(The feature of check connection to mobile network is necessary for uninterrupted operation)

Check Connection	enabled	enabled
Ping IP Address	8.8.8.8	www.google.com
Ping Interval	60	80 sec

☒ Enable traffic monitoring

Figure 21: Example 1 – Mobile WAN configuration

Example 2: The following configuration illustrates the situation in which the router switches to a backup SIM card after exceeding the data limits of 800 MB in the billing period. It will send out a warning SMS message when 400 MB of data have been transmitted. In the example shown, the billing period begins on the 18th day of the month.

Data Limit	800	MB
Warning Threshold	50	%
Accounting Start	18	

Default SIM card	primary
Backup SIM card	secondary

☐ Switch to other SIM card when connection fails
☐ Switch to backup SIM card when roaming is detected and switch to default SIM card when home network is detected
☒ Switch to backup SIM card when data limit is exceeded and switch to default SIM card when data limit isn't exceeded
☐ Switch to backup SIM card when binary input is active and switch to default SIM card when binary input isn't active
☐ Switch to default SIM card after timeout

Initial Timeout	60	min
Subsequent Timeout *		min
Additive Constant *		min

Figure 22: Example 2 – Mobile WAN configuration

Example 3: Configuring the router to switch to offline mode when it detects that it is roaming. The first attempt to switch back to the default SIM card is executed after 60 minutes, the second after 40 minutes, the third after 50 minutes (40+10) etc.

Default SIM card	primary
Backup SIM card	none

☐ Switch to other SIM card when connection fails
☒ Switch to backup SIM card when roaming is detected and switch to default SIM card when home network is detected
☐ Switch to backup SIM card when data limit is exceeded and switch to default SIM card when data limit isn't exceeded
☐ Switch to backup SIM card when binary input is active and switch to default SIM card when binary input isn't active
☒ Switch to default SIM card after timeout

Initial Timeout	60	min
Subsequent Timeout *	40	min
Additive Constant *	10	min

Figure 23: Example 3 – Mobile WAN configuration

3.4 PPPoE Configuration

PPPoE (Point-to-Point over Ethernet) is a network protocol where PPP frames are encapsulated in Ethernet frames. It is used to set the PPPoE connection over Ethernet. The router will connect to a PPPoE server or a PPPoE bridge device such as an ADSL router.

To enter the PPPoE configuration, select the *PPPoE* menu item. If the *Create PPPoE connection* option is selected, the router will attempt to establish a PPPoE connection on power up. After a PPPoE connection is established, the router obtains the IP address of the PPPoE Server device and all communications from the device are forwarded to the industrial router.

Item	Description
Username	Username for secure access to PPPoE
Password	Password for secure access to PPPoE
Authentication	Authentication protocol in GSM network <ul style="list-style-type: none"> • PAP or CHAP – authentication method is chosen by router • PAP – PAP authentication method is used • CHAP – CHAP authentication method is used
MRU	Maximum Receiving Unit – The maximum packet size that can be received in the given environment. Default value is set to 1492 bytes. Other settings may cause incorrect data transmission.
MTU	Maximum Transmission Unit – The maximum packet size that can be transmitted in the given environment. Default value is set to 1492 bytes. Other settings may cause incorrect data transmission.

Table 26: PPPoE configuration

PPPoE Configuration

☐ Create PPPoE connection

Username *

Password *

Authentication PAP or CHAP

MRU bytes

MTU bytes

☒ Get DNS addresses from server

Figure 24: PPPoE configuration

3.5 WiFi configuration



This item is available only if the router is equipped with a WiFi module.

Configure the Wi-Fi network by selecting the Wi-Fi item in the main menu of the router web interface. Activate *WiFi* by selecting *Enable WiFi* at the top of the form. You may also set the following properties:

Item	Description
Operating mode	<p>WiFi operating mode:</p> <ul style="list-style-type: none"> • access point (AP) – router becomes an access point to which other devices in <i>station (STA)</i> mode can be connect • station (STA) – router becomes a client station – it receives data packets from the available access point (AP) and sends data from cable connection via the Wi-Fi network
SSID	Unique identifier of Wi-Fi network
Broadcast SSID	<p>Method of broadcasting the unique identifier of SSID network in beacon frame and type of response to a request for sending the beacon frame.</p> <ul style="list-style-type: none"> • Enabled – SSID is broadcasted in beacon frame • Zero length – Beacon frame does not include SSID. Requests for sending beacon frame are ignored. • Clear – All SSID characters in beacon frame are replaced by 0. Original length is kept. Requests for sending beacon frame are ignored.
Probe Hidden SSID	Probes hidden SSID (only for <i>station (STA)</i> mode)
Country Code	<p>Code of the country where the router is installed. This code must be entered in ISO 3166-1 alpha-2 format. If a <i>country code</i> isn't specified and the router has not implemented a system to determine this code, it will use "US" as the default <i>country code</i>.</p> <p>If no <i>country code</i> is specified or if the wrong country code is entered, then the router may violate country-specific regulations for the use of the Wi-Fi frequency bands.</p>

Continued on next page

Continued from previous page

Item	Description
HW Mode	<p>HW mode of WiFi standard that will be supported by WiFi access point (AP).</p> <ul style="list-style-type: none"> • IEE 802.11b • IEE 802.11b+g • IEE 802.11b+g+n
Channel	The channel where the WiFi AP is transmitting
BW 40 MHz	The option for HW mode 802.11n which allows transmission on two standard 20 MHz channels simultaneously.
WMM	Basic QoS for WI FI networks is enabled by checking this item. This version doesn't guarantee network throughput. It is suitable for simple applications that require QoS.
Authentication	<p>Access control and authorization of users in the Wi-Fi network.</p> <ul style="list-style-type: none"> • Open – Authentication is not required (free access point) • Shared – Base authentication using WEP key • WPA-PSK – Authentication using better authentication method PSK-PSK • WPA2-PSK – WPA-PSK using new encryption AES.
Encryption	<p>Type of data encryption in the Wi-Fi network:</p> <ul style="list-style-type: none"> • None – No data encryption • WEP – Encryption using static WEP keys. This encryption can be used for <i>Shared</i> authentication. • TKIP – Dynamic encryption key management that can be used for <i>WPA-PSK</i> and <i>WPA2-PSK</i> authentication. • AES – Improved encryption used for <i>WPA2-PSK</i> authentication
WEP Key Type	<p>Type of WEP key for WEP encryption:</p> <ul style="list-style-type: none"> • ASCII – WEP key in ASCII format • HEX – WEP key in hexadecimal format
WEP Default Key	This item specifies the default WEP key

Continued on next page

Continued from previous page

Item	Description
WEP Key 1-4	<p>Items for different four WEP keys</p> <ul style="list-style-type: none"> • WEP key in ASCII format must be entered in quotes. This key can be specified in the following lengths: <ul style="list-style-type: none"> – 5 ASCII characters (40b WEP key) – 13 ASCII characters (104b WEP key) – 16 ASCII characters (128b WEP key) • WEP key must be entered in hexadecimal digits. This key can be specified in the following lengths.: <ul style="list-style-type: none"> – 10 hexadecimal digits (40b WEP key) – 26 hexadecimal digits (104b WEP key) – 32 hexadecimal digits (128b WEP key)
WPA PSK Type	<p>Type of key for WPA-PSK authentication:</p> <ul style="list-style-type: none"> • 256-bit secret • ASCII passphrase • PSK File
WPA PSK	<p>Key for WPA-PSK authentication. This key must be entered according to the selected WPA-PSK type as follows:</p> <ul style="list-style-type: none"> • 256-bit secret – 64 hexadecimal digits • ASCII passphrase – 8 to 63 characters which are subsequently converted into PSK • PSK File – absolute path to the file containing the list of pairs (PSK key, MAC address)
Access List	<p>Mode of Access/Deny list:</p> <ul style="list-style-type: none"> • Disabled – Access/Deny list is not used • Accept – Clients in Accept/Deny list can access the network • Deny – Clients in Access/Deny list cannot access the network
Accept/Deny List	<p>Accept or Deny list of client MAC addresses that set network access. Each MAC address is separated by new line.</p>

Continued on next page

Continued from previous page

Item	Description
Syslog Level	<p>Logging level, when system writes to the system log</p> <ul style="list-style-type: none"> • Verbose debugging – The highest level of logging • Debugging • Informational – Default level of logging • Notification • Warning – The lowest level of logging
Extra options	Allows the user to define additional parameters

Table 27: WiFi configuration

WiFi Configuration

☐ Enable WiFi

Operating Mode: access point (AP)

SSID:

Broadcast SSID: enabled

Probe Hidden SSID: ☐

Country Code *:

HW Mode: IEEE 802.11b

Channel: 7

BW 40 MHz: ☐

WMM: ☐

Authentication: WPA2-PSK

Encryption: AES

WEP Key Type: ASCII

WEP Default Key: 1

WEP Key 1:

WEP Key 2:

WEP Key 3:

WEP Key 4:

WPA PSK Type: 256-bit secret

WPA PSK:

Access List: disabled

Accept/Deny List:

Syslog Level: informational

Extra options *:

* can be blank

Apply

Figure 25: WiFi konfigurace

3.6 WLAN configuration



This item is available only if the router is equipped with a WiFi module.

The Wi-Fi LAN and DHCP server page is displayed by selecting **WLAN** in the configuration section. You will then be able to set the following properties:

Item	description
Operating Mode	<p>Wi-Fi operating mode:</p> <ul style="list-style-type: none"> • access point (AP) – Router becomes an access point to which other devices in <i>station (STA)</i> mode can be connected. • station (STA) – Router becomes a client station. It will receive data packets from the available access point (AP) and send data from cable connection via the Wi-Fi network.
DHCP Client	Activates/deactivates DHCP client
IP Address	Fixed set IP address of Wi-Fi network interface
Subnet Mask	Subnet mask of Wi-Fi network interface
Bridged	<p>Activates bridge mode:</p> <ul style="list-style-type: none"> • no – Bridged mode is not allowed (default value). WLAN network is not connected with LAN network of the router. • yes – Bridged mode is allowed. WLAN network is connected with one or more LAN networks of the router. In this case, the setting of most items in this table are ignored. Instead, the router uses the settings of the selected network interface (LAN).
Default Gateway	IP address of the default gateway. When entering the IP address of the default gateway, all packets for which the record was not found in the routing table will be sent to this address.
DNS Server	Address to which all DNS queries are forwarded.

Table 28: WLAN configuration

Use *Enable dynamic DHCP leases* item at the bottom of this form to enable dynamic allocation of IP addresses using the DHCP server. You may also specify these values:

Item	Description
IP Pool Start	Beginning of the range of IP addresses which will be assigned to DHCP clients
IP Pool End	End of the range of IP addresses which will be assigned to DHCP clients
Lease Time	Time in seconds for which the client may use the IP address

Table 29: Configuration of DHCP server

All changes in settings will apply after pressing the *Apply* button.

WLAN Configuration	
<input type="checkbox"/> Enable WLAN interface	
Operating Mode	access point (AP) ▼
DHCP Client	disabled ▼
IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Bridged	no ▼
Default Gateway	<input type="text"/>
DNS Server	<input type="text"/>
<input checked="" type="checkbox"/> Enable dynamic DHCP leases	
IP Pool Start	192.168.3.2
IP Pool End	192.168.3.254
Lease Time	600 sec
<input type="button" value="Apply"/>	

Figure 26: WLAN configuration

3.7 Backup Routes

By using the configuration form on the *Backup Routes* page, you can back up the primary connection with alternative connections to the Internet/mobile network. Each backup connection can be assigned a priority. Switching between connections is done based upon set priorities and the state of the connections (for *Primary LAN* and *Secondary LAN*).

If *Enable backup routes switching* option is checked, the default route is selected according to the settings in the chart below. (Options include *Enable backup routes switching for Mobile WAN*, *Enable backup routes switching for PPPoE*, *Enable backup routes switching for Wi-Fi STA*, *Enable backup routes switching for Primary LAN*, and *Enable backup routes switching for Secondary LAN*.)

Network interfaces belonging to individual backup routes should display a flag that says they are **RUNNING**. This check fixes, for example, the disconnection of an Ethernet cable.



Attention! If you want to use connection to mobile WAN as one of the backup routes, it is necessary to enable *Check Connection* at *Mobile WAN* configuration to *enable + bind* option, see chapter 3.3.3.

Backup Routes Configuration	
<input type="checkbox"/>	Enable backup routes switching
<input type="checkbox"/>	Enable backup routes switching for Mobile WAN
Priority	1st ▼
<input type="checkbox"/>	Enable backup routes switching for PPPoE
Priority	1st ▼
Ping IP Address	<input type="text"/>
Ping Interval	<input type="text"/> sec
<input type="checkbox"/>	Enable backup routes switching for WiFi STA
Priority	1st ▼
Ping IP Address	<input type="text"/>
Ping Interval	<input type="text"/> sec
<input type="checkbox"/>	Enable backup routes switching for Primary LAN
Priority	1st ▼
Ping IP Address	<input type="text"/>
Ping Interval	<input type="text"/> sec
<input type="checkbox"/>	Enable backup routes switching for Secondary LAN
Priority	1st ▼
Ping IP Address	<input type="text"/>
Ping Interval	<input type="text"/> sec
<input type="button" value="Apply"/>	

Figure 27: Backup Routes

If the *Enable backup routes switching* option is not checked, the *Backup routes* system operates in the so-called backward compatibility mode. The default route is selected based on implicit priorities according to the status of each enabled network interface. The names of backup routes and corresponding network interfaces, in order of implicit priorities, are:

- Mobile WAN (pppX, usbX)
- PPPoE (ppp0)
- Secondary LAN (eth1)
- Primary LAN (eth0)

Example:

Secondary LAN is selected as the default route only if *Create connection to mobile network* option is not checked on the *Mobile WAN* page, or if the *Create PPPoE connection* option is not checked on the *PPPoE* page. To select the Primary LAN it is also necessary that the *IP address* for Secondary LAN is not entered, and that *DHCP Client* for Secondary LAN is not enabled.

Item	Description
Priority	Priority for the type of connection
Ping IP Address	Destination IP address of ping queries to check the connection (address can not be specified as a domain name)
Ping Interval	The time intervals between sent ping queries

Table 30: Backup Routes

All changes in settings will be applied after pressing the *Apply* button.

3.8 Firewall configuration

Incoming packets must first pass a check of enabled source IP address and destination ports. You may specify the IP address from which you will remotely access the router and the internal network behind the router. If the *Enable filtering of incoming packets* item is checked (located at the beginning of the *Firewall* configuration form), this element is enabled and accessibility is checked against the table of IP addresses. This means that access is only permitted to the addresses specified in the table. You can define the rules for up to eight remote accesses.

Item	Description
Source	IP address from which access to the router is allowed
Protocol	Specifies protocol for remote access: <ul style="list-style-type: none"> • all – access is enabled for all protocols • TCP – access is enabled for TCP protocol • UDP – access is enabled for UDP protocol • ICMP – access is enabled for ICMP protocol
Target Port	The port number on which access to the router is allowed
Action	Type of action: <ul style="list-style-type: none"> • allow – access is allowed • deny – access is denied

Table 31: Filtering of incoming packets

The next part of the configuration form defines the forwarding policy. If *Enabled filtering of forwarded packets* is not checked, packets will be accepted automatically. If *Enabled filtering of forwarded packets* is checked and the incoming packet is addressed to another network interface, it will forward the packet according the rules defined in this second table. If the packet is allowed according to the table, it will be sent out according to the routing table. If the forwarding rule does not exist, the packet will be dropped.

You can choose to allow all traffic within the selected protocol (the rule specifies only a protocol). Or you can create strict rules by specifying source and destination IP addresses and ports.

Item	Description
Source	IP address of source device
Destination	IP address of destination device
Protocol	Specifies protocol for remote access: <ul style="list-style-type: none"> • all – access is enabled for all protocols • TCP – access is enabled for TCP protocol • UDP – access is enabled for UDP protocol • ICMP – access is enabled for ICMP protocol
Target Port	The port number on which access to the router is allowed

Continued on next page

Continued from previous page

Item	Description
Action	<p>Type of action:</p> <ul style="list-style-type: none"> • allow – access is allowed • deny – access is denied

Table 32: Forwarding filtering

Select *Enable filtering of locally destined packets* to drop a packet whenever a request for service which is not in the router comes in. The packet will be dropped automatically, without any information. As a protection against DoS attacks (Attacks during which the target system is flooded with large quantities of meaningless requirements) select *Enable protection against DoS attacks*. This limits the number of connections to five per second.

Firewall Configuration

☐ Enable filtering of incoming packets

Source *	Protocol	Target Port *	Action
<input type="checkbox"/>	all ▼	<input type="text"/>	allow ▼
<input type="checkbox"/>	all ▼	<input type="text"/>	allow ▼
<input type="checkbox"/>	all ▼	<input type="text"/>	allow ▼
<input type="checkbox"/>	all ▼	<input type="text"/>	allow ▼
<input type="checkbox"/>	all ▼	<input type="text"/>	allow ▼
<input type="checkbox"/>	all ▼	<input type="text"/>	allow ▼
<input type="checkbox"/>	all ▼	<input type="text"/>	allow ▼
<input type="checkbox"/>	all ▼	<input type="text"/>	allow ▼

☐ Enabled filtering of forwarded packets

Source *	Destination *	Protocol	Target Port *	Action
<input type="checkbox"/>	<input type="text"/>	all ▼	<input type="text"/>	allow ▼
<input type="checkbox"/>	<input type="text"/>	all ▼	<input type="text"/>	allow ▼
<input type="checkbox"/>	<input type="text"/>	all ▼	<input type="text"/>	allow ▼
<input type="checkbox"/>	<input type="text"/>	all ▼	<input type="text"/>	allow ▼
<input type="checkbox"/>	<input type="text"/>	all ▼	<input type="text"/>	allow ▼
<input type="checkbox"/>	<input type="text"/>	all ▼	<input type="text"/>	allow ▼
<input type="checkbox"/>	<input type="text"/>	all ▼	<input type="text"/>	allow ▼
<input type="checkbox"/>	<input type="text"/>	all ▼	<input type="text"/>	allow ▼

☐ Enable filtering of locally destined packets

☐ Enable protection against DoS attacks

* can be blank

Figure 28: Firewall configuration

Example of the firewall configuration:

The router has allowed the following access:

- from address 171.92.5.45 using any protocol
- from address 10.0.2.123 using TCP protocol on port 1000
- from address 142.2.26.54 using ICMP protocol

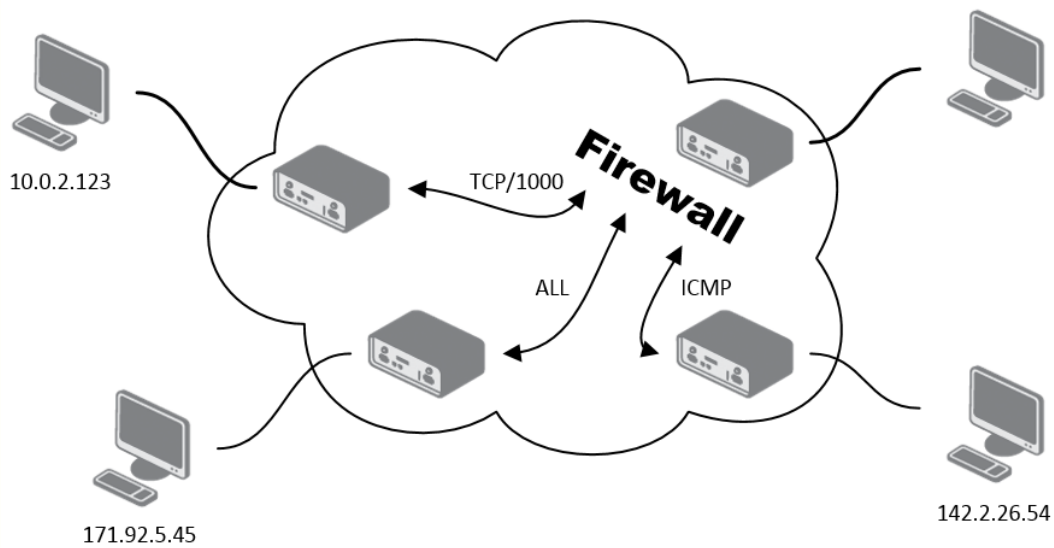


Figure 29: Topology of sample firewall configuration

Firewall Configuration				
<input checked="" type="checkbox"/> Enable filtering of incoming packets				
Source *	Protocol	Target Port *	Action	
<input checked="" type="checkbox"/> 171.92.5.45	all		allow	
<input checked="" type="checkbox"/> 10.0.2.123	TCP	1000	allow	
<input checked="" type="checkbox"/> 142.2.26.54	ICMP		allow	
<input type="checkbox"/>	all		allow	
<input type="checkbox"/>	all		allow	
<input type="checkbox"/>	all		allow	
<input type="checkbox"/>	all		allow	
<input type="checkbox"/>	all		allow	

Figure 30: Example of a firewall configuration

3.9 NAT configuration

NAT (Network Address Translation / Port Address Translation – PAT) is a method of sharing a single external IP address among many internal hosts. It also helps prevent unauthorized access to the internal network. To enter the Network Address Translation configuration, select the *NAT* menu item. Up to sixteen NAT rules may be defined.

Item	Description
Public Port	Public port
Private Port	Private port
Type	Protocol selection
Server IP address	IP address to which incoming data will be forwarded

Table 33: NAT configuration

If you need to set up more than sixteen NAT rules, insert the following statement into the startup script:

```
iptables -t nat -A napt -p tcp --dport [PORT\_PUBLIC] -j DNAT --to-destination [IPADDR] : [PORT1\_PRIVATE]
```

The IP address parameter [IPADDR] and port parameters [PORT_PUBLIC] and [PORT_PRIVATE] must be filled in with the desired information.

The following option can be used to route all incoming traffic from the PPP to a single internal host address.

Item	Description
Send all remaining incoming packets to default server	Select this item to route all incoming data from GPRS to a single IP address on the internal network.
Default Server IP Address	Send all incoming packets to this IP address.

Table 34: Configuration of "send all" incoming packets

Enable the following options and enter the port number to allow remote access to the router from the Internet.

Item	Description
Enable remote HTTP access on port	If field and port number are filled in, configuration of the router over web interface is allowed (disabled in default configuration).
Enable remote HTTPS access on port	If field and port number are filled in, configuration of the router over web interface is allowed (disabled in default configuration).
Enable remote FTP access on port	Select this option to allow the router using FTP.
Enable remote SSH access on port	Select this option to allow access to the router using SSH (disabled in default configuration).
Enable remote Telnet access on port	Select this option to allow the router using Telnet.
Enable remote SNMP access on port	Select this option to allow access to the router using SNMP (disabled in default configuration).
Masquerade outgoing packets	Select this option to turn on NAT.

Table 35: Remote access configuration

Example 1: NAT configuration with one host connected to the router:

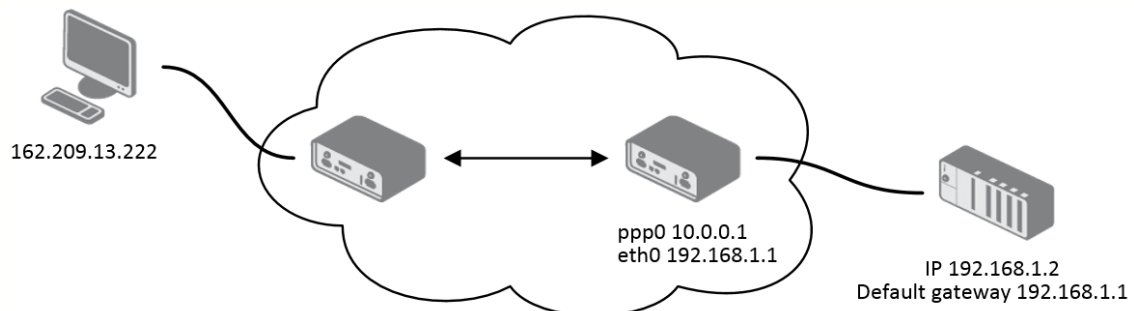


Figure 31: Example 1 – Topology of basic NAT configuration

NAT Configuration			
Public Port	Private Port	Type	Server IP Address
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	

<input checked="" type="checkbox"/> Enable remote HTTP access on port	80
<input type="checkbox"/> Enable remote HTTPS access on port	443
<input checked="" type="checkbox"/> Enable remote FTP access on port	21
<input type="checkbox"/> Enable remote SSH access on port	22
<input checked="" type="checkbox"/> Enable remote Telnet access on port	23
<input checked="" type="checkbox"/> Enable remote SNMP access on port	161
<input checked="" type="checkbox"/> Send all remaining incoming packets to default server	
Default Server IP Address 198.162.1.2	
<input checked="" type="checkbox"/> Masquerade outgoing packets	
<input type="button" value="Apply"/>	

Figure 32: Example 1 – Basic NAT configuration

In this configuration, it is important to select *Send all remaining incoming packets to default server*. In this case, the IP address is the address of the device behind the router. The router must be set as the *Default Gateway* for connected equipment behind the router. If you send ping message to the IP address of the SIM card, connected device behind the router sends response.

Example 2: Configuration with more connected equipment:

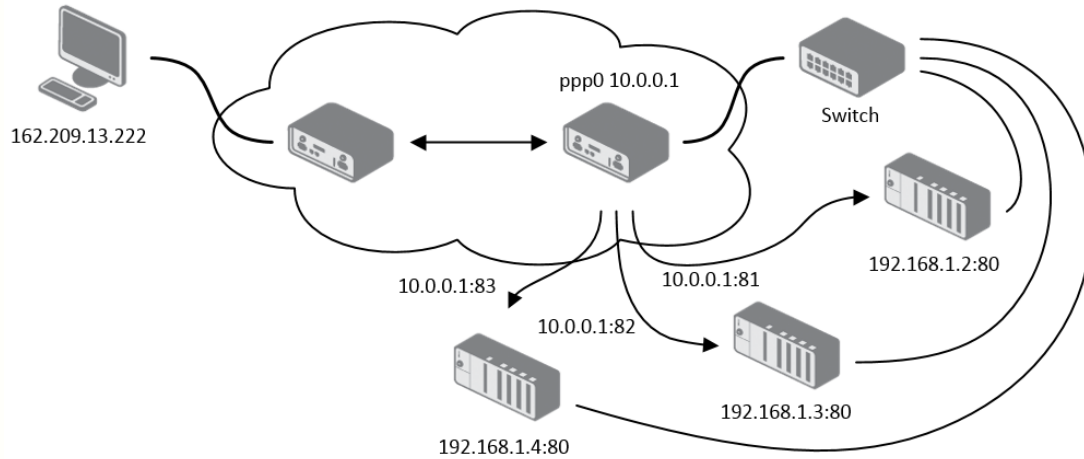


Figure 33: Example 2 – Topology of NAT configuration

NAT Configuration

Public Port	Private Port	Type	Server IP Address
81	80	TCP	198.162.1.2
82	80	TCP	198.162.1.3
83	80	TCP	198.162.1.4
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	

☒ Enable remote HTTP access on port
☐ Enable remote HTTPS access on port
☒ Enable remote FTP access on port
☐ Enable remote SSH access on port
☒ Enable remote Telnet access on port
☒ Enable remote SNMP access on port

☐ Send all remaining incoming packets to default server
 Default Server IP Address

☒ Masquerade outgoing packets

Figure 34: Example 2 – NAT configuration

In this example there is additional equipment connected behind the router, using a Switch. Every device connected behind the router has its own IP address. This is the address to enter in the *Server IP Address* field in the NAT configuration. All of these devices will be communicating on port 80, but you can configure the Port Forwarding in the NAT configuration *Public Port* and *Private Port* fields. It is now configured to access 192.168.1.2:80 socket behind the router when accessing 10.0.0.1:81 from the Internet, and so on. If you send the ping request to the public IP address of the router (10.0.0.1), the router will respond as usual (not forwarding). If you access the IP address 10.0.0.1 in the browser (it is port 80), nothing will happen – Port 80 in the Public Port list is not defined, and you have not checked the *Enable remote HTTP access on port 80*. And since the *Send all remaining incoming packets to default server* is not enabled, the attempt to connect will fail.

3.10 OpenVPN tunnel configuration

Select the *OpenVPN* item to configure an OpenVPN tunnel. OpenVPN is a protocol which is used to create a secure connection between two LANs. Up to two OpenVPN tunnels may be created.

Item	Description
Create	Enables the individual tunnels
Description	Displays the name of the tunnel specified in the configuration form of the tunnel
Edit	Select to configure an OpenVPN tunnel

Table 36: Overview of OpenVPN tunnels

OpenVPN Tunnels Configuration		
	Create	Description
1st	no	<input type="text"/> Edit
2nd	no	<input type="text"/> Edit
<input type="button" value="Apply"/>		

Figure 35: OpenVPN tunnel configuration

Item	Description
Description	Description (or name) of tunnel
Protocol	Protocol by which the tunnel will communicate. <ul style="list-style-type: none"> • UDP – OpenVPN will communicate using UDP • TCP server – OpenVPN will communicate using TCP in server mode • TCP client – OpenVPN will communicate using TCP in client mode
UDP/TCP port	Port by which the tunnel will communicate.
Remote IP Address	IP address of opposite tunnel side (domain name can be used).
Remote Subnet	Network IP address of the opposite side of the tunnel.
Remote Subnet Mask	Subnet mask of the opposite side of the tunnel.
Redirect Gateway	Allows to redirect all traffic on Ethernet
Local Interface IP Address	IP address of the local side of tunnel.
Remote Interface IP Address	IP address of interface local side of tunnel.
Ping Interval	Parameter (in seconds) defines how often the router will send a message to the remote end to verify that the tunnel is still connected.
Ping Timeout	Parameter which defines how long the router will wait for a response to the ping (in seconds). <i>Ping Timeout</i> must be larger than <i>Ping Interval</i> .
Renegotiate Interval	Sets renegotiate period (reauthorization) of the OpenVPN tunnel. This parameter can be set only when <i>Authenticate Mode</i> is set to <i>username/password</i> or <i>X.509 certificate</i> . After this time period, the router changes the tunnel encryption to ensure the continued safety of the tunnel.
Max Fragment Size	Defines maximum packet size
Compression	Data compression: <ul style="list-style-type: none"> • none – No compression is used. • LZO – Lossless LZO compression. Compression has to be selected on both tunnel ends.

Continued on next page

Continued from previous page

Item	Description
NAT Rules	<p>Applies NAT rules to the OpenVPN tunnel:</p> <ul style="list-style-type: none"> • not applied – NAT rules are not applied to the OpenVPN tunnel. • applied – NAT rules are applied to the OpenVPN tunnel.
Authenticate Mode	<p>Sets authentication mode:</p> <ul style="list-style-type: none"> • none – no authentication is set • Pre-shared secret – sets the shared key for both sides of the tunnel • Username/password – enables authentication using <i>CA Certificate</i>, <i>Username</i> and <i>Password</i> • X.509 Certificate (multiclient) – enables X.509 authentication in multiclient mode • X.509 Certificate (client) – enables X.509 authentication in client mode • X.509 Certificate (server) – enables X.509 authentication in server mode
Pre-shared Secret	Authentication using pre-shared secret can be used for all offered authentication mode.
CA Certificate	Auth. using CA Certificate can be used for username/password and X.509 Certificate modes.
DH Parameters	Protocol for exchange key DH parameters can be used for X.509 Certificate authentication in server mode.
Local Certificate	This authentication certificate can be used for X.509 Certificate authentication mode.
Local Private Key	Local private key can be used for X.509 certificate auth. mode.
Username	Authentication using a login name and password authentication can be used for username/password mode.
Password	Authentication using a login name and password authentication can be used for username/password mode.

Continued on next page

Continued from previous page

Item	Description
Extra Options	Defines additional parameters of OpenVPN tunnel such as DHCP options etc. Parameters are introduced by two dashes. For possible parameters see the <i>Help</i> in the router via SSH – run the <code>openvpn --help</code> command.

Table 37: OpenVPN configuration

OpenVPN Tunnel Configuration

☐ Create 1st OpenVPN tunnel

Description *

ProtocolUDP

UDP port1194

Remote IP Address *

Remote Subnet *

Remote Subnet Mask *

Redirect Gatewayno

Local Interface IP Address

Remote Interface IP Address

Ping Interval *sec

Ping Timeout *sec

Renegotiate Interval *sec

Max Fragment Size *bytes

CompressionLZO

NAT Rulesnot applied

Authenticate Modenone

Pre-shared Secret

CA Certificate

DH Parameters

Local Certificate

Local Private Key

Username

Password

Extra Options *

* can be blank

Apply

Figure 36: OpenVPN tunnel configuration

Example of the OpenVPN tunnel configuration:

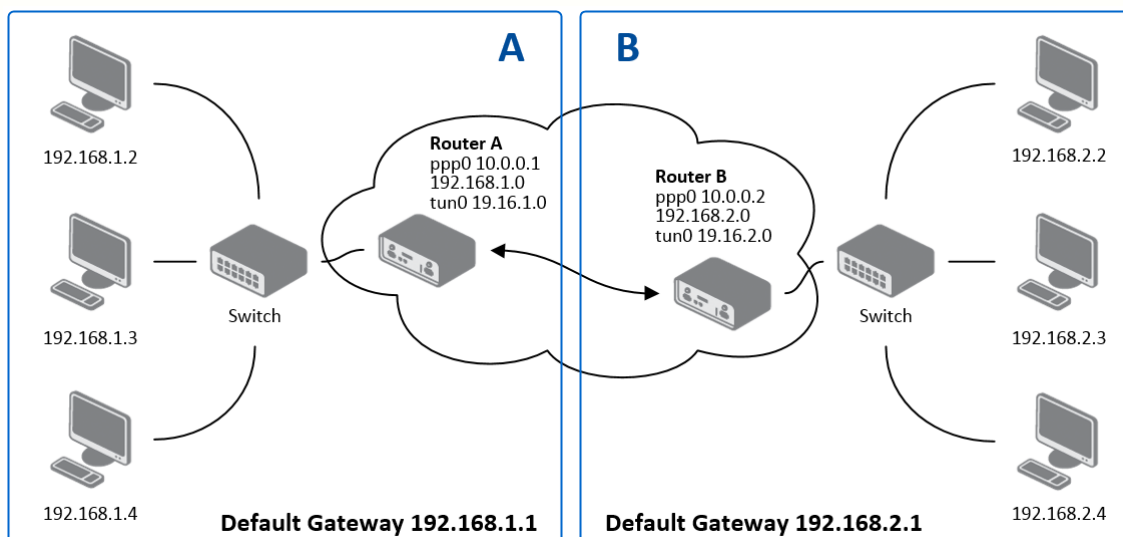


Figure 37: Topology of OpenVPN configuration example

OpenVPN tunnel configuration:

Configuration	A	B
Protocol	UDP	UDP
UDP Port	1194	1194
Remote IP Address	10.0.0.2	10.0.0.1
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Local Interface IP Address	19.16.1.0	19.16.2.0
Remote Interface IP Address	19.16.2.0	19.18.1.0
Compression	LZO	LZO
Authenticate mode	none	none

Table 38: Example of OpenVPN configuration



Examples of different options for configuration and authentication of OpenVPN tunnel can be found in the application note *OpenVPN*.

3.11 IPsec tunnel configuration

Select the IPsec menu item to configure an *IPsec* tunnel. IPsec is a protocol which is used to create a secure, encrypted connection between two LANs. Up to four IPsec tunnels may be created.

Item	Description
Create	Enables the individual tunnels.
Description	Displays the name of the tunnel specified in the configuration of the tunnel.
Edit	Select to configure an IPsec tunnel.

Table 39: Overview of IPsec tunnels

Figure 38: IPsec tunnel configuration

Item	Description
Description	Name (description) of the tunnel
Remote IP Address	IP address or domain name of the remote host.
Remote ID	Identification of remote host. The ID contains two parts: a <i>host-name</i> and a <i>domain-name</i> (more information can be found under this table).
Remote Subnet	Remote Subnet address
Remote Subnet Mask	Remote Subnet mask
Remote Protocol/Port	Specifies the Protocol/Port of the remote side of the tunnel. The general form is <i>protocol/port</i> , for example 17/1701 for UDP (protocol 17) and port 1701. It is also possible to enter only the number of the protocol, however, the above mentioned format is preferred.
Local ID	Identification of local host. The ID contains two parts: a <i>host-name</i> and a <i>domain-name</i> (more information can be found under the table).

Continued on next page

Continued from previous page

Item	Description
Local Subnet	Local subnet address
Local Subnet Mask	Local subnet mask
Local Protocol/Port	Specifies the Protocol/Port of a local network. The general form is <i>protocol/port</i> , for example 17/1701 for UDP (protocol 17) and port 1701. It is also possible to enter only the number of protocol, however, the above mentioned format is preferred.
Encapsulation Mode	IPsec mode (according to the method of encapsulation) – You can choose <i>tunnel</i> (entire IP datagram is encapsulated) or <i>transport</i> (only IP header).
NAT traversal	If address translation between two end points of the IPsec tunnel is used, it needs to allow <i>NAT Traversal</i> .
IKE Mode	Defines the mode for establishing connection (<i>main</i> or <i>aggressive</i>). If the aggressive mode is selected, establishing of IPsec tunnel will be faster, but encryption will set permanently on 3DES-MD5. We recommend avoiding the use of aggressive mode, as it is less secure!
IKE Algorithm	Way of algorithm selection: <ul style="list-style-type: none"> • auto – encryption and hash alg. are selected automatically • manual – encryption and hash alg. are defined by the user
IKE Encryption	Encryption algorithm – 3DES, AES128, AES192, AES256
IKE Hash	Hash algorithm – MD5, SHA1, SHA256, SHA384 or SHA512
IKE DH Group	Diffie-Hellman groups determine the strength of the key used in the key exchange process. Higher group numbers are more secure, but require additional time to compute the key. Group with higher number provides more security, but requires more processing time.
ESP Algorithm	Way of algorithm selection: <ul style="list-style-type: none"> • auto – encryption and hash alg. are selected automatically • manual – encryption and hash alg. are defined by the user
ESP Encryption	Encryption algorithm – DES, 3DES, AES128, AES192, AES256
ESP Hash	Hash algorithm – MD5, SHA1, SHA256, SHA384 or SHA512
PFS	Ensures that derived session keys are not compromised if one of the private keys is compromised in the future

Continued on next page

Continued from previous page

Item	Description
PFS DH Group	Diffie-Hellman group number (see <i>IKE DH Group</i>)
Key Lifetime	Lifetime key data part of tunnel. The minimum value of this parameter is 60 s. The maximum value is 86400 s.
IKE Lifetime	Lifetime key service part of tunnel. The minimum value of this parameter is 60 s. The maximum value is 86400 s.
Rekey Margin	Specifies how long before connection expiry an attempt to negotiate a replacement should begin. The maximum value must be less than half the parameters IKE and Key Lifetime.
Rekey Fuzz	Percentage extension of Rekey Margin time
DPD Delay	Time after which the IPsec tunnel functionality is tested
DPD Timeout	The period during which device waits for a response
Authenticate Mode	This parameter sets authentication: <ul style="list-style-type: none"> • Pre-shared key – shared key for both sides of the tunnel • X.509 Certificate – allows X.509 authentication in multi-client mode
Pre-shared Key	Shared key for both sides for Pre-shared key authentication
CA Certificate	Certificate for X.509 authentication
Remote Certificate	Certificate for X.509 authentication
Local Certificate	Certificate for X.509 authentication
Local Private Key	Private key for X.509 authentication
Local Passphrase	Passphrase for X.509 authentication
Extra Options	Use this parameter to define additional parameters of the IPsec tunnel, secure parameters, for example.

Table 40: IPsec configuration

IPsec supports the following types of identifiers (ID) of both tunnel sides (*Remote ID* and *Local ID* items):

- IP address (e.g. 192.168.1.1)
- DN (e.g. C=CZ,O=Conel,OU=TP,CN=A)
- FQDN (e.g. @director.conel.cz) – **in front of FQDN must always be @**
- User FQDN (e.g. director@conel.cz)



The certificates and private keys have to be in PEM format. You may only use a certificate that has start and stop tag certificate.



The random time, after which it will exchange new keys, is defined as follows:

*Lifetime - (Rekey margin + random value in range (from 0 to Rekey margin * Rekey Fuzz/100))*

By default, the time for the exchange of keys is between:

- Minimal time: 1h - (9m + 9m) = 42m
- Maximal time: 1h - (9m + 0m) = 51m

In most cases, the settings should be left at their default values. Setting higher time gives the tunnel has smaller operating costs less safety. Conversely, reducing the time gives the tunnel higher operating costs and higher safety.

The changes in settings will apply after pressing the *Apply* button.

IPsec Tunnel Configuration	
<input type="checkbox"/> Create 1st IPsec tunnel	
Description *	<input type="text"/>
Remote IP Address *	<input type="text"/>
Remote ID *	<input type="text"/>
Remote Subnet *	<input type="text"/>
Remote Subnet Mask *	<input type="text"/>
Remote Protocol/Port *	<input type="text"/>
Local ID *	<input type="text"/>
Local Subnet *	<input type="text"/>
Local Subnet Mask *	<input type="text"/>
Local Protocol/Port *	<input type="text"/>
Encapsulation Mode	tunnel ▼
NAT Traversal	disabled ▼
IKE Mode	main ▼
IKE Algorithm	auto ▼
IKE Encryption	3DES ▼
IKE Hash	MD5 ▼
IKE DH Group	2 ▼
ESP Algorithm	auto ▼
ESP Encryption	DES ▼
ESP Hash	MD5 ▼
PFS	disabled ▼
PFS DH Group	2 ▼
Key Lifetime	3600 sec
IKE Lifetime	3600 sec
Rekey Margin	540 sec
Rekey Fuzz	100 %
DPD Delay *	<input type="text"/> sec
DPD Timeout *	<input type="text"/> sec
Authenticate Mode	pre-shared key ▼
Pre-shared Key	<input type="text"/>
CA Certificate	<input type="text"/>
Remote Certificate	<input type="text"/>
Local Certificate	<input type="text"/>
Local Private Key	<input type="text"/>
Local Passphrase *	<input type="text"/>
Extra Options *	<input type="text"/>
* can be blank	
<input type="button" value="Apply"/>	

Figure 39: IPsec tunnels configuration

Example of the IPsec Tunnel configuration:

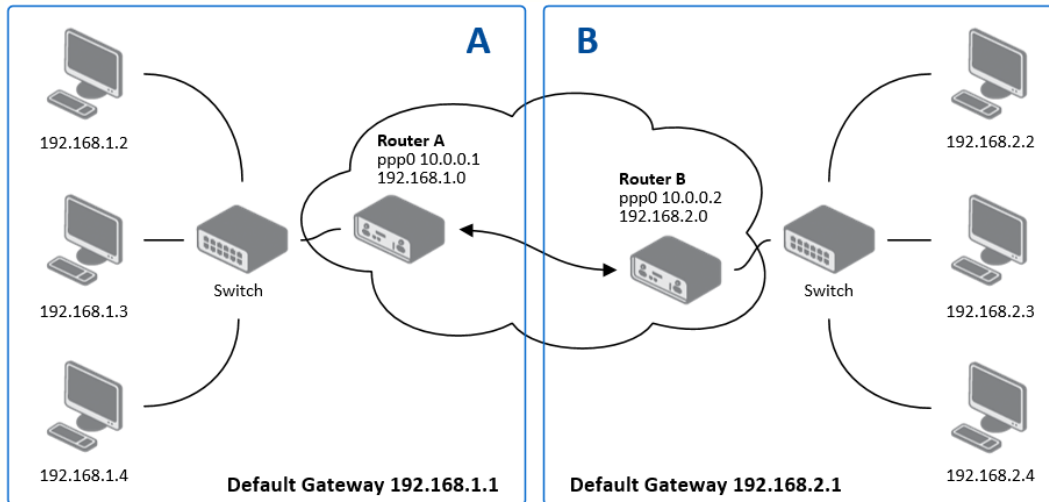


Figure 40: Topology of IPsec configuration example

IPsec tunnel configuration:

Configuration	A	B
Remote IP Address	10.0.0.2	10.0.0.1
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Local Subnet	192.168.1.0	192.168.2.0
Local Subnet Mas:	255.255.255.0	255.255.255.0
Authenticate mode	pre-shared key	pre-shared key
Pre-shared key	test	test

Table 41: Example of IPsec configuration



Examples of different options for configuration and authentication of IPsec tunnel can be found in the application note *IPsec Tunnel*.

3.12 GRE tunnel configuration



GRE is an unencrypted protocol.

Select the *GRE* item in the menu to configure a GRE tunnel. GRE is a protocol which is used to create an unencrypted connection between two LANs. Up to four GRE tunnels may be created.

Item	Description
Create	Enables the individual tunnels
Description	Displays the name of the tunnel specified in the configuration form
Edit	Configuration of GRE tunnel

Table 42: Overview of GRE tunnels

Figure 41: GRE tunnel configuration

Item	Description
Description	Description of the tunnel.
Remote IP Address	IP address of the remote side of the tunnel
Remote Subnet	IP address of the network behind the remote side of the tunnel
Remote Subnet Mask	Mask of the network behind the remote side of the tunnel
Local Interface IP Address	IP address of the local side of the tunnel
Remote Interface IP Address	IP address of the remote side of the tunnel
Multicasts	Enables/disables multicast: <ul style="list-style-type: none"> • disabled – multicast disabled • enabled – multicast enabled
Pre-shared Key	An optional value that defines the 32 bit shared key in numeric format. This key must be defined the same way on both routers, otherwise the router will drop received packets.

Table 43: GRE tunnel configuration



Attention, GRE tunnel doesn't connect itself via NAT.

GRE Tunnel Configuration

☐ Create 1st GRE tunnel

Description *

Remote IP Address

Remote Subnet *

Remote Subnet Mask *

Local Interface IP Address *

Remote Interface IP Address *

Multicasts disabled

Pre-shared Key *

* can be blank

Figure 42: GRE tunnel configuration

Example of the GRE Tunnel configuration:

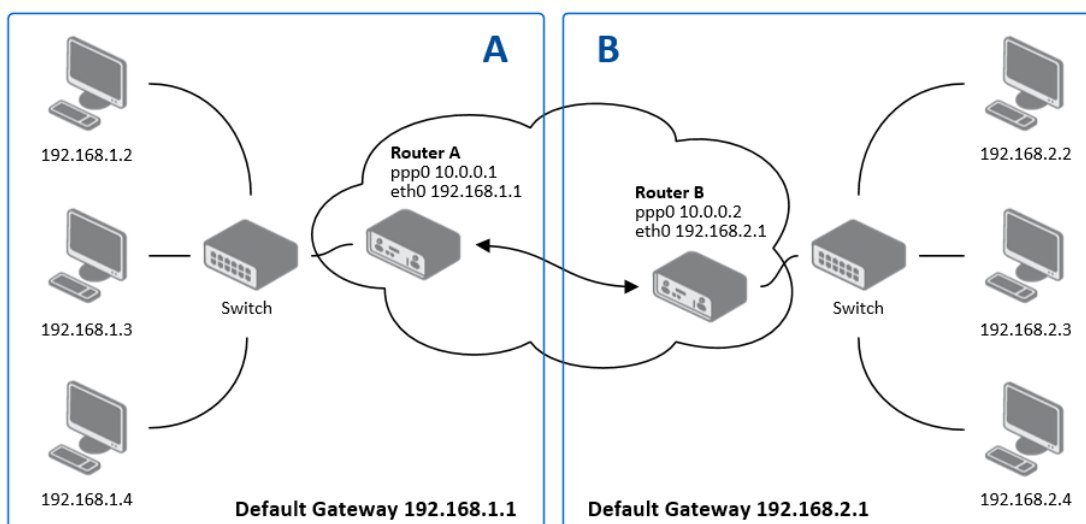


Figure 43: Topology of GRE tunnel configuration

GRE tunnel Configuration:

Configuration	A	B
Remote IP Address	10.0.0.2	10.0.0.1
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0

Table 44: Example GRE tunnel configuration

Examples of different options for configuration of GRE tunnel can be found in the application note *GRE Tunnel*.

3.13 L2TP tunnel configuration



L2TP is an unencrypted protocol.

Select the *L2TP* item in the menu to configure an L2TP tunnel. L2TP is a protocol which is used to create a password-protected connection between two LANs. The tunnels are active after selecting *Create L2TP tunnel*.

Item	Description
Mode	L2TP tunnel mode on the router side: <ul style="list-style-type: none"> • L2TP server – For a server, you must define the start and end IP address range offered by the server. • L2TP client – For a client, you must enter the IP address of the server.
Server IP Address	IP address of server.
Client Start IP Address	Start IP address in range, which is offered by server to clients.
Client End IP Address	End IP address in range, which is offered by server to clients.
Local IP Address	IP address of the local side of the tunnel.
Remote IP Address	IP address of the remote side of the tunnel.
Remote Subnet	Address of the network behind the remote side of the tunnel.
Remote Subnet Mask	The mask of the network behind the remote side of the tunnel.
Username	Username for login to L2TP tunnel.
Password	Password for login to L2TP tunnel.

Table 45: L2TP tunnel configuration

The changes in settings will apply after pressing the *Apply* button.

L2TP Tunnel Configuration

☐ Create L2TP tunnel

Mode

L2TP client

Server IP Address

Client Start IP Address

Client End IP Address

Local IP Address *

Remote IP Address *

Remote Subnet *

Remote Subnet Mask *

Username

Password

* can be blank

Apply

Figure 44: L2TP tunnel configuration

Example of the L2TP Tunnel configuration:

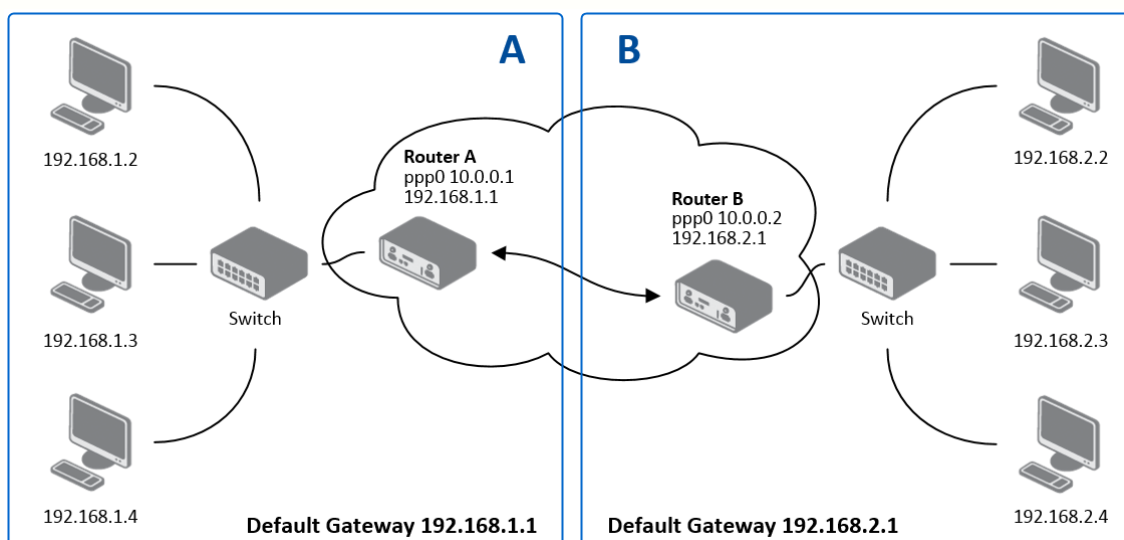


Figure 45: Topology of L2TP tunnel configuration example

Configuration of the L2TP tunnel:

Configuration	A	B
Mode	L2TP Server	L2TP Client
Server IP Address	—	10.0.0.1
Client Start IP Address	192.168.1.2	—
Client End IP Address	192.168.1.254	—
Local IP Address	192.168.1.1	—
Remote IP Address	—	—
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Username	username	username
Password	password	password

Table 46: Example of L2TP tunnel configuration

3.14 PPTP tunnel configuration



PPTP is an unencrypted protocol.

Select the *PPTP* item in the menu to configure a PPTP tunnel. PPTP tunnel allows password protected connections between two LANs. It is similar to L2TP. The tunnels are active after selecting *Create PPTP tunnel*.

Item	Description
Mode	PPTP tunnel mode on the router side: <ul style="list-style-type: none"> • PPTP server – For a server, you must define the start and end IP address range offered by the server. • PPTP client – For a client, you must enter the IP address of the server.
Server IP Address	IP address of the server.
Local IP Address	IP address of the local side of the tunnel.
Remote IP Address	IP address of the remote side of the tunnel.
Remote Subnet	Address of the network behind the remote side of the tunnel.
Remote Subnet Mask	The mask of the network behind the remote side of the tunnel.
Username	Username for logging into PPTP tunnel.
Password	Password for logging into PPTP tunnel.

Table 47: PPTP tunnel configuration

Figure 46: PPTP tunnel configuration



Starting with firmware version 3.0.9, PPTP passthrough is supported, which means that it is possible to create a tunnel through the router.

Example of the PPTP Tunnel configuration:

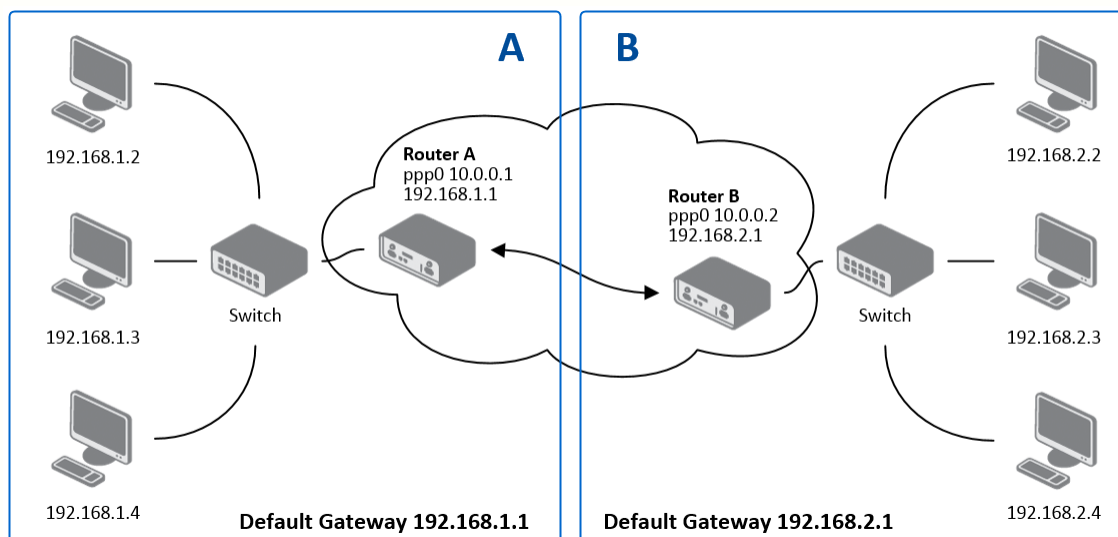


Figure 47: Topology of PPTP tunnel configuration example

Configuration of the PPTP tunnel:

Configuration	A	B
Mode	PPTP Server	PPTP Client
Server IP Address	—	10.0.0.1
Local IP Address	192.168.1.1	—
Remote IP Address	—	—
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Username	username	username
Password	password	password

Table 48: Example of PPTP tunnel configuration

3.15 DynDNS client configuration

DynDNS service lets you access the router remotely using an easy to remember custom hostname. This client monitors the router's IP address and updates it whenever it changes. To use DynDNS you must have a public IP address (static or dynamic) and an active account at www.dyndns.org (Remote Access service).

DynDNS client Configuration can be called up by selecting option *DynDNS* item in the menu. A registered custom domain (third-level) and account information must be defined in the configuration form.

Item	Description
Hostname	Third order domain registered on server www.dyndns.org .
Username	Username for logging into DynDNS server.
Password	Password for logging into DynDNS server.
Server	If you wish to use a DynDNS service other than www.dyndns.org , enter that update server service. If this item is left blank, the router uses the default server: members.dyndns.org .

Table 49: DynDNS configuration

Example of the DynDNS client configuration with domain conel.dyndns.org:

DynDNS Configuration

☒ Enable DynDNS client

Hostname:

Username:

Password:

Server *:

* can be blank

Figure 48: Example of DynDNS configuration

3.16 NTP client configuration

NTP (Network Time Protocol) allows the router to set its internal clock using a network time server. The NTP client Configuration can be called up by selecting option *NTP* item in the menu.

- If option *Enable local NTP service* is selected, the router will function as an NTP server for other devices on the LAN.
- If option *Synchronize clock with NTP server* is selected, the router acts as a NTP client. This means that the router automatically adjusts the internal clock every 24 hours.

Item	Description
Primary NTP Server Address	IP address or domain name of the primary NTP server.
Secondary NTP Server Address	IP address or domain name of the secondary NTP server.
Timezone	Sets the time zone of the router.
Daylight Saving Time	Defines time shift: <ul style="list-style-type: none"> • No – time shift is disabled • Yes – time shift is allowed

Table 50: NTP configuration

Example of the NTP conf. with set primary (ntp.cesnet.cz) and secondary (tik.cesnet.cz) NTP server and with daylight saving time:

NTP Configuration	
<input type="checkbox"/>	Enable local NTP service
<input checked="" type="checkbox"/>	Synchronize clock with NTP server
Primary NTP Server	<input type="text" value="ntp.cesnet.cz"/>
Secondary NTP Server	<input type="text" value="tik.cesnet.cz"/>
Timezone	<input type="text" value="GMT+01:00"/> ▼
Daylight Saving Time	<input type="text" value="yes"/> ▼
<input type="button" value="Apply"/>	

Figure 49: Example of NTP configuration

3.17 SNMP configuration

SNMP (Simple Network Management Protocol) provides status information about network elements such as routers or end computers.

To enter the SNMP Configuration, select the *SNMP* item from the configuration menu. The router supports SNMP agent v1, v2 or v3, which are just different versions of SNMP. The SNMP agent sends information about the router and its expansion ports. In SNMP version v3 the communication is secured (encrypted), except for the notification messages (such as notifications of events – Traps). To enable SNMP service, select Enable SNMP agent.

Item	Description
Name	Designation of the router.
Location	Placing of the router.
Contact	Person who manages the router, together with contact information for this person.

Table 51: SNMP agent configuration

Enable SNMPv1/v2 with the *Enable SNMPv1/v2 access* item. You will need to define a password for access to the SNMP agent (Community). *Public* is commonly used.



At SNMPv1/v2 it is possible to define a different password for *Read* community (read only) and *Write* community (read and write). At SNMPv3 you can define two SNMP users. One can read only (*Read*), the second can read and write (*Write*). The items in the following table can be set up for every user separately. These are not router's Web interface users, just the SNMP access users.

The *Enable SNMPv3 access* option allows you to enable SNMPv3. Then you must define the following parameters:


Item	Description
Username	User name
Authentication	Encryption algorithm on the Authentication Protocol that is used to ensure the identity of users.
Authentication Password	Password used to generate the key used for authentication.
Privacy	Encryption algorithm on the Privacy Protocol that is used to ensure confidentiality of data.
Privacy Password	Password for encryption on the Privacy Protocol.

Table 52: SNMPv3 configuration

- Selecting the *Enable I/O extension* lets you monitor binary inputs I/O on the router.
- Selecting the *Enable XC-CNT extension* lets you monitor the expansion port CNT inputs and outputs status.
- Selecting the *Enable M-BUS extension* and entering the Baudrate, Parity and Stop Bits lets you monitor the meter status connected to the expansion port MBUS status.

Item	Description
Baudrate	Communication speed
Parity	Control parity bit: <ul style="list-style-type: none"> • none – data will be sent without parity • even – data will be sent with even parity • odd – data will be sent with odd parity
Stop Bits	Number of stop bits

Table 53: SNMP configuration (MBUS extension)

 Parameters *Enable XC-CNT extension* and *Enable M-BUS extension* cannot be checked at the same time.

Selecting *Enable reporting to supervisory system* and entering the *IP Address* and *Period* lets you send statistical information to the monitoring system, R-SeeNet.

Item	Description
IP Address	IP address
Period	Period of sending statistical information (in minutes)

Table 54: SNMP configuration (R-SeeNet)

Every monitor value is uniquely identified a number identifier *OID* – *Object Identifier*. For binary input and output the following range of OIDs is used:

OID	Description
.1.3.6.1.4.1.30140.2.3.1.0	Binary input BIN0 (values 0,1)
.1.3.6.1.4.1.30140.2.3.2.0	Binary output OUT0 (values 0,1)

Table 55: Object identifier for binary input and output

For the expansion port CNT the following range of OID is used:

OID	Description
.1.3.6.1.4.1.30140.2.1.1.0	Analogy input AN1 (range 0-4095)
.1.3.6.1.4.1.30140.2.1.2.0	Analogy input AN2 (range 0-4095)
.1.3.6.1.4.1.30140.2.1.3.0	Counter input CNT1 (range 0-4294967295)
.1.3.6.1.4.1.30140.2.1.4.0	Counter input CNT2 (range 0-4294967295)
.1.3.6.1.4.1.30140.2.1.5.0	Binary input BIN1 (values 0,1)
.1.3.6.1.4.1.30140.2.1.6.0	Binary input BIN2 (values 0,1)
.1.3.6.1.4.1.30140.2.1.7.0	Binary input BIN3 (values 0,1)
.1.3.6.1.4.1.30140.2.1.8.0	Binary input BIN4 (values 0,1)
.1.3.6.1.4.1.30140.2.1.9.0	Binary output OUT1 (values 0,1)

Table 56: Object identifier for CNT port

For the expansion port M-BUS the following range of OID is used:

OID	Description
.1.3.6.1.4.1.30140.2.2.<address>.1.0	IdNumber – meter number
.1.3.6.1.4.1.30140.2.2.<address>.2.0	Manufacturer
.1.3.6.1.4.1.30140.2.2.<address>.3.0	Version – specified meter version
.1.3.6.1.4.1.30140.2.2.<address>.4.0	Medium – type of metered medium
.1.3.6.1.4.1.30140.2.2.<address>.5.0	Status – errors report
.1.3.6.1.4.1.30140.2.2.<address>.6.0	0. VIF – value information field
.1.3.6.1.4.1.30140.2.2.<address>.7.0	0. measured value
.1.3.6.1.4.1.30140.2.2.<address>.8.0	1. VIF – value information field
.1.3.6.1.4.1.30140.2.2.<address>.9.0	1. measured value
.1.3.6.1.4.1.30140.2.2.<address>.10.0	2. VIF – value information field
.1.3.6.1.4.1.30140.2.2.<address>.11.0	2. measured value
.1.3.6.1.4.1.30140.2.2.<address>.12.0	3. VIF – value information field
.1.3.6.1.4.1.30140.2.2.<address>.13.0	3. measured value
⋮	⋮
.1.3.6.1.4.1.30140.2.2.<address>.100.0	47. VIF – value information field
.1.3.6.1.4.1.30140.2.2.<address>.101.0	47. measured value

Table 57: Object identifier for M-BUS port

The meter address can be from range 0..254 when 254 is broadcast.

Starting with firmware version 3.0.4, all v2 routers with board RB-v2-6 and newer provide information About the internal temperature of the device (OID 1.3.6.1.4.1.30140.3.3) and power voltage (OID 1.3.6.1.4.1.30140.3.4).

Example of SNMP settings and readout:

SNMP Configuration		
<input checked="" type="checkbox"/> Enable SNMP agent		
Name *	<input type="text" value="Conel"/>	
Location *	<input type="text" value="Usti nad Orlici"/>	
Contact *	<input type="text" value="Jack Roghul +420 732 123 4"/>	
<i>(Configuration via SNMP is not possible.)</i>		
<input checked="" type="checkbox"/> Enable SNMPv1/v2 access		
Community	Read <input type="text" value="public"/>	Write <input type="text" value="public"/>
<input type="checkbox"/> Enable SNMPv3 access		
Username	Read <input type="text"/>	Write <input type="text"/>
Authentication	MD5 ▼	MD5 ▼
Authentication Password	<input type="text"/>	<input type="text"/>
Privacy	DES ▼	DES ▼
Privacy Password	<input type="text"/>	<input type="text"/>
<input checked="" type="checkbox"/> Enable I/O extension		
<input type="checkbox"/> Enable XC-CNT extension		
<input checked="" type="checkbox"/> Enable M-BUS extension		
Baudrate	300 ▼	
Parity	even ▼	
Stop Bits	1 ▼	
<input type="checkbox"/> Enable reporting to supervisory system		
IP Address	<input type="text"/>	
Period	<input type="text"/>	min
<i>* can be blank</i>		
<input type="button" value="Apply"/>		

Figure 50: Example of SNMP configuration

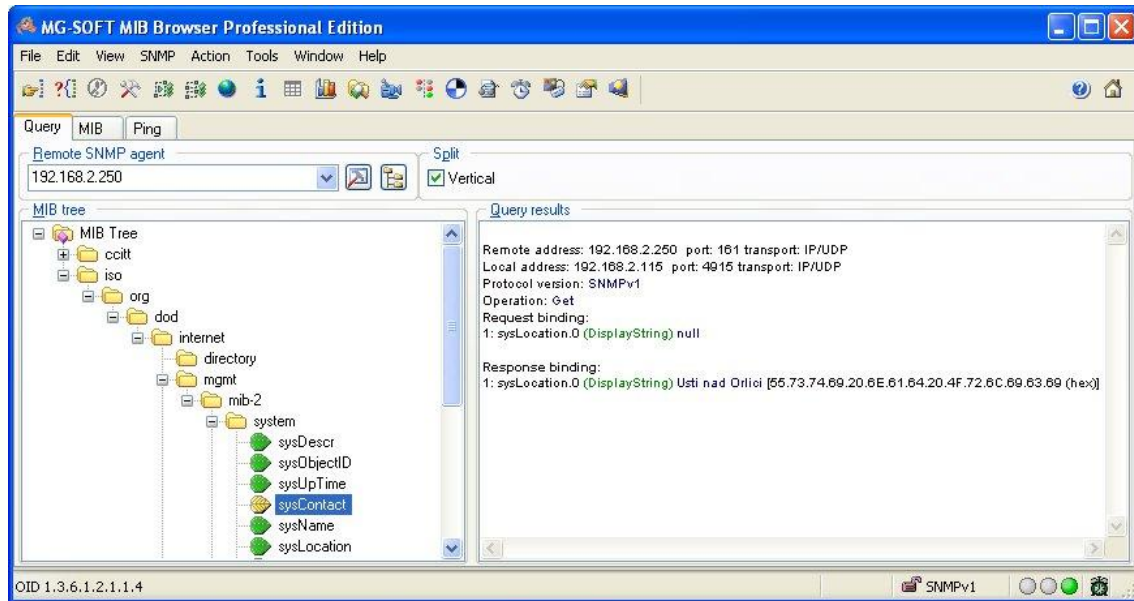


Figure 51: Example of the MIB browser

It is important to set the IP address of the SNMP agent (router) in field *Remote SNMP agent*. After entering the IP address in a MIB tree part it becomes possible to show the object identifier.

The path to objects is:

iso → org → dod → internet → private → enterprises → conel → protocols

The path to information about the router is:

iso → org → dod → internet → mgmt → mib-2 → system

3.18 SMTP Configuration

The SMTP (Simple Mail Transfer Protocol) client is used to send emails.

Item	Description
SMTP Server Address	IP address or domain name of the mail server.
SMTP Port	Port the SMTP server is listening on.
Secure Method	none, SSL/TLS, or STARTTLS. Secure method has to be supported by the SMTP server.
Username	Name to e-mail account.
Password	Password to e-mail account. Can contain special characters * + , - . / : = ? ! # % [] _ { } ~ and cannot contain special characters " \$ & ' () ; < >
Own E-mail Address	Address of the sender.

Table 58: SMTP client configuration



The mobile operator may block other SMTP servers. If this occurs, then you must use the SMTP server of the operator.

SMTP Configuration	
SMTP Server Address	<input type="text" value="smtp.domain.com"/>
SMTP Port	<input type="text" value="465"/>
Secure Method	<input type="text" value="SSL/TLS"/>
Username	<input type="text" value="name"/>
Password	<input type="password" value="pass"/>
Own Email Address	<input type="text" value="name@domain.com"/>
<input type="button" value="Apply"/>	

Figure 52: Example of the SMTP client configuration

E-mail can be sent from the Startup script (*Startup Script* item in the *Configuration* section) or via telnet and SSH connection. The command *email* can be used with the following parameters:

- t receiver's E-mail address
- s subject (has to be in quotation marks)
- m message (has to be in quotation marks)
- a attachment file
- r number of attempts to send email (default 2 attempts set)



Commands and parameters can be entered only in lowercase.

Example of sending an e-mail:

```
email -t name@domain.com -s "subject" -m "message" -a c:\directory\abc.doc -r 5
```

This command sends e-mail to address *name@domain.com* with the subject "*subject*", body message "*message*" and attachment "*abc.doc*" right from the directory *c:\directory* and attempts to send 5 times.

3.19 SMS configuration



The *SMS Configuration* item is not available for the Spectre RT industrial router and the XR5i v2 router.

The router can automatically send SMS messages to a cell phone or SMS message server when certain events occur. The *SMS Configuration* page allows the user to select which events will generate an SMS message.

Item	Description
Send SMS on power up	Send an SMS message when the router powers up.
Send SMS on connect to mobile network	Send an SMS message when the mobile network connection is active.
Send SMS on disconnect to mobile network	Send an SMS message on mobile network disconnection.
Send SMS when datalimit exceeded	Send an SMS message when the data limit is exceeded.
Send SMS when binary input on I/O port (BIN0) is active	Send an SMS message when the binary input on the I/O port (BIN0) goes active. The text of the message is set using parameter BIN0.
Send SMS when binary input on expansion port (BIN1 – BIN4) is active	Send an SMS message after binary input on expansion port (BIN1 – BIN4) is active. Text of message is intended parameter BIN1 – BIN4.
Add timestamp to SMS	Adds time stamp to sent SMS messages. This stamp has a fixed format YYYY-MM-DD hh:mm:ss.
Phone Number 1	Telephone numbers for sending automatically generated SMS.
Phone Number 2	Telephone numbers for sending automatically generated SMS.
Phone Number 3	Telephone numbers for sending automatically generated SMS.
Unit ID	The name of the router that sends the SMS.

Continued on next page

Continued from previous page

Item	Description
BIN0 – SMS	SMS text messages when the binary input on the router is activated.
BIN1 – SMS	SMS text messages when the binary input on the router is activated.
BIN2 – SMS	SMS text messages when the binary input on the router is activated.
BIN3 – SMS	SMS text messages when the binary input on the router is activated.
BIN4 – SMS	SMS text messages when the binary input on the router is activated.

Table 59: Send SMS configuration

You can also control the function of the router by sending SMS messages to the device. The *Enable remote control via SMS* option must be selected to enable this feature. Up to three numbers can be configured for incoming SMS messages.

Item	Description
Phone Number 1	This control can be configured for up to three numbers. If <i>Enable remote control via SMS</i> is set, all incoming SMS messages are processed and deleted. The default setting is ON.
Phone Number 2	This control can be configured for up to three numbers. If <i>Enable remote control via SMS</i> is set, all incoming SMS messages are processed and deleted. The default setting is ON.
Phone Number 3	This control can be configured for up to three numbers. If <i>Enable remote control via SMS</i> is set, all incoming SMS messages are processed and deleted. The default setting is ON.

Table 60: Control via SMS configuration

Note: If no phone number is filled in, or if "*" is entered, the router will accept incoming SMS messages from all phone numbers. If any phone numbers are entered into the list, the router will only accept SMS messages which originate from those numbers. You may use SMS messages to reboot the router.

Control SMS messages cannot change the router configuration. Any changes made to the router by an SMS message will only remain in effect until the router is restarted. After a reboot, the router configuration will return to the settings in non-volatile memory. For example, if the router is switched offline by an SMS message, the router will remain offline until the next time it is power cycled or re-booted.

To control the router using SMS, the message text must contain the control command. Supported SMS control messages are:

SMS	Description
go online sim 1	Switch to SIM1 card
go online sim 2	Switch to SIM2 card
go online	Switch the router in online mode
go offline	Connection termination
set out0=0	Set output I/O connector on 0
set out0=1	Set output I/O connector on 1
set out1=0	Set output expansion port XC-CNT on 0
set out1=1	Set output expansion port XC-CNT on 1
set profile std	Set standard profile
set profile alt1	Set alternative profile 1
set profile alt2	Set alternative profile 2
set profile alt3	Set alternative profile 3
reboot	Router reboot
get ip	Router send answer with IP address SIM card

Table 61: Control SMS

Choosing *Enable AT-SMS protocol on expansion port 1* and *Baudrate* makes it possible to send/receive an SMS on the serial Port 1.

Item	Description
Baudrate	Communication speed on expansion port 1

Table 62: Send SMS on serial PORT1 configuration

Choosing *Enable AT-SMS protocol on expansion port 2* and *Baudrate* makes it possible to send/receive an SMS on the serial Port 2.

Item	Description
Baudrate	Communication speed on expansion port 2

Table 63: Send SMS on serial PORT2 configuration

It is also possible to send and receive SMS messages over a TCP/IP connection by choosing *Enable AT-SMS protocol on TCP port*. The *TCP port* used for sending and receiving SMS messages must be entered into the configuration field. SMS messages are sent with the help of standard AT commands.

Item	Description
TCP Port	TCP port on which will be allowed to send/receive SMS messages.

Table 64: Send SMS on Ethernet PORT1 configuration

3.19.1 Send SMS

The following table lists the commands that are supported by the router. For other AT commands, the *OK* response is always sent. There is no support for complex AT commands. If they are sent, the router responds with an *ERROR* message.

AT Command	Description
AT+CGMI	Returns the manufacturer specific identity
AT+CGMM	Returns the manufacturer specific model identity
AT+CGMR	Returns the manufacturer specific model revision identity
AT+CGPADDR	Displays the IP address of the ppp0 interface
AT+CGSN	Returns the product serial number
AT+CIMI	Returns the International Mobile Subscriber Identity number (IMSI)
AT+CMGD	Deletes a message from the location
AT+CMGF	Sets the presentation format of short messages
AT+CMGL	Lists messages of a certain status from a message storage area
AT+CMGR	Reads a message from a message storage area
AT+CMGS	Sends a short message from the device to entered tel. number
AT+CMGW	Writes a short message to SIM storage
AT+CMSS	Sends a message from SIM storage location value
AT+COPS?	Identifies the available mobile networks
AT+CPIN	Is used to query and enter a PIN code
AT+CPMS	Selects SMS memory storage types, to be used for short message operations
AT+CREG	Displays network registration status
AT+CSCA	Sets the short message service centre (SMSC) number
AT+CSCS	Selects the character set
AT+CSQ	Returns the signal strength of the registered network

Continued on next page

Continued from previous page

AT Command	Description
AT+GMI	Returns the manufacturer specific identity
AT+GMM	Returns the manufacturer specific model identity
AT+GMR	Returns the manufacturer specific model revision identity
AT+GSN	Returns the product serial number
ATE	Determines whether or not the device echoes characters
ATI	Transmits the manufacturer specific information about the device

Table 65: List of AT commands



A detailed description and examples of these AT commands can be found in the application note *AT commands*.

Example 1: SMS sending configuration:

After powering up the router sends this SMS:

Router (Unit ID) has been powered up. Signal strength –xx dBm.

After connection to the mobile network the router sends this SMS:

Router (Unit ID) has established connection to mobile network. IP address xxx.xxx.xxx.xxx

After disconnection to mobile network the router sends this SMS:

Router (Unit ID) has lost connection to mobile network. IP address xxx.xxx.xxx.xxx

Example of SMS configuration 1:

SMS Configuration	
<input checked="" type="checkbox"/>	Send SMS on power up
<input checked="" type="checkbox"/>	Send SMS on connect to mobile network
<input checked="" type="checkbox"/>	Send SMS on disconnect from mobile network
<input checked="" type="checkbox"/>	Send SMS when datalimit is exceeded
<input checked="" type="checkbox"/>	Send SMS when binary input on I/O port (BIN0) is active
<input checked="" type="checkbox"/>	Send SMS when binary input on expansion port 1 (BIN1-BIN4) is active
<input checked="" type="checkbox"/>	Add timestamp to SMS
Phone Number 1	<input type="text" value="723123456"/>
Phone Number 2	<input type="text" value="756858635"/>
Phone Number 3	<input type="text" value="603854758"/>
Unit ID *	<input type="text" value="Router"/>
BIN0 - SMS *	<input type="text" value="BIN0"/>
BIN1 - SMS *	<input type="text" value="BIN1"/>
BIN2 - SMS *	<input type="text" value="BIN2"/>
BIN3 - SMS *	<input type="text" value="BIN3"/>
BIN4 - SMS *	<input type="text" value="BIN4"/>
<input checked="" type="checkbox"/>	Enable remote control via SMS
Phone Number 1	<input type="text"/>
Phone Number 2	<input type="text"/>
Phone Number 3	<input type="text"/>
<input type="checkbox"/>	Enable AT-SMS protocol on expansion port 1
Baudrate	<input type="text" value="9600"/>
<input type="checkbox"/>	Enable AT-SMS protocol on expansion port 2
Baudrate	<input type="text" value="9600"/>
<input type="checkbox"/>	Enable AT-SMS protocol over TCP
TCP Port	<input type="text"/>
* can be blank	
<input type="button" value="Apply"/>	

Figure 53: Example of SMS configuration 1

Example of SMS configuration for sending via serial interface on PORT1:

SMS Configuration	
<input type="checkbox"/>	Send SMS on power up
<input type="checkbox"/>	Send SMS on connect to mobile network
<input type="checkbox"/>	Send SMS on disconnect from mobile network
<input type="checkbox"/>	Send SMS when datalimit is exceeded
<input type="checkbox"/>	Send SMS when binary input on I/O port (BIN0) is active
<input type="checkbox"/>	Send SMS when binary input on expansion port 1 (BIN1-BIN4) is active
<input type="checkbox"/>	Add timestamp to SMS
Phone Number 1	<input type="text"/>
Phone Number 2	<input type="text"/>
Phone Number 3	<input type="text"/>
Unit ID *	<input type="text"/>
BIN0 - SMS *	<input type="text"/>
BIN1 - SMS *	<input type="text"/>
BIN2 - SMS *	<input type="text"/>
BIN3 - SMS *	<input type="text"/>
BIN4 - SMS *	<input type="text"/>
<hr/>	
<input type="checkbox"/>	Enable remote control via SMS
Phone Number 1	<input type="text"/>
Phone Number 2	<input type="text"/>
Phone Number 3	<input type="text"/>
<hr/>	
<input checked="" type="checkbox"/>	Enable AT-SMS protocol on expansion port 1
Baudrate	<input type="text" value="9600"/>
<hr/>	
<input type="checkbox"/>	Enable AT-SMS protocol on expansion port 2
Baudrate	<input type="text" value="9600"/>
<hr/>	
<input type="checkbox"/>	Enable AT-SMS protocol over TCP
TCP Port	<input type="text"/>
* can be blank	
<input type="button" value="Apply"/>	

Figure 54: Example of SMS configuration 2

Example of SMS configuration for controlling the router from any phone number:

SMS Configuration	
<input type="checkbox"/>	Send SMS on power up
<input type="checkbox"/>	Send SMS on connect to mobile network
<input type="checkbox"/>	Send SMS on disconnect from mobile network
<input type="checkbox"/>	Send SMS when datalimit is exceeded
<input type="checkbox"/>	Send SMS when binary input on I/O port (BIN0) is active
<input type="checkbox"/>	Send SMS when binary input on expansion port 1 (BIN1-BIN4) is active
<input type="checkbox"/>	Add timestamp to SMS
Phone Number 1	<input type="text"/>
Phone Number 2	<input type="text"/>
Phone Number 3	<input type="text"/>
Unit ID *	<input type="text"/>
BIN0 - SMS *	<input type="text"/>
BIN1 - SMS *	<input type="text"/>
BIN2 - SMS *	<input type="text"/>
BIN3 - SMS *	<input type="text"/>
BIN4 - SMS *	<input type="text"/>
<input checked="" type="checkbox"/>	Enable remote control via SMS
Phone Number 1	<input type="text" value="*"/>
Phone Number 2	<input type="text"/>
Phone Number 3	<input type="text"/>
<input type="checkbox"/>	Enable AT-SMS protocol on expansion port 1
Baudrate	<input type="text" value="9600"/>
<input type="checkbox"/>	Enable AT-SMS protocol on expansion port 2
Baudrate	<input type="text" value="9600"/>
<input type="checkbox"/>	Enable AT-SMS protocol over TCP
TCP Port	<input type="text"/>
* can be blank	
<input type="button" value="Apply"/>	

Figure 55: Example of SMS configuration 3

Example of SMS configuration for controlling the router via SMS from two specified phone numbers:

SMS Configuration	
<input type="checkbox"/>	Send SMS on power up
<input type="checkbox"/>	Send SMS on connect to mobile network
<input type="checkbox"/>	Send SMS on disconnect from mobile network
<input type="checkbox"/>	Send SMS when datalimit is exceeded
<input type="checkbox"/>	Send SMS when binary input on I/O port (BIN0) is active
<input type="checkbox"/>	Send SMS when binary input on expansion port 1 (BIN1-BIN4) is active
<input type="checkbox"/>	Add timestamp to SMS
Phone Number 1	<input type="text"/>
Phone Number 2	<input type="text"/>
Phone Number 3	<input type="text"/>
Unit ID *	<input type="text"/>
BIN0 - SMS *	<input type="text"/>
BIN1 - SMS *	<input type="text"/>
BIN2 - SMS *	<input type="text"/>
BIN3 - SMS *	<input type="text"/>
BIN4 - SMS *	<input type="text"/>
<input checked="" type="checkbox"/>	Enable remote control via SMS
Phone Number 1	<input type="text" value="728123456"/>
Phone Number 2	<input type="text" value="766254864"/>
Phone Number 3	<input type="text"/>
<input type="checkbox"/>	Enable AT-SMS protocol on expansion port 1
Baudrate	<input type="text" value="9600"/>
<input type="checkbox"/>	Enable AT-SMS protocol on expansion port 2
Baudrate	<input type="text" value="9600"/>
<input type="checkbox"/>	Enable AT-SMS protocol over TCP
TCP Port	<input type="text"/>
* can be blank	
<input type="button" value="Apply"/>	

Figure 56: Example of SMS configuration 4

3.20 Expansion port configuration

Select *Expansion Port 1* or *Expansion Port 2* option to configure expansion ports PORT1 and PORT2.

Item	Description
Baudrate	Communication speed
Data Bits	Number of data bits
Parity	Control parity bit <ul style="list-style-type: none"> • none – data will be sent without parity • even – data will be sent with even parity • odd – data will be sent with odd parity
Stop Bits	Number of stop bits
Split Timeout	Time to rupture reports. If the gap between two characters exceeds the parameter in milliseconds, any buffered characters will be sent over the Ethernet port.
Protocol	Protocol: <ul style="list-style-type: none"> • TCP • UDP
Mode	Mode of connection: <ul style="list-style-type: none"> • TCP server – The router will listen for incoming TCP connection requests. • TCP client – The router will connect to a TCP server on the specified IP address and TCP port.
Server Address	When set to <i>TCP client</i> above, it is necessary to enter the <i>Server address</i> and <i>TCP port</i> .
TCP Port	The TCP port for connections.
Inactivity Timeout	Time period after which the TCP/UDP connection is interrupted in case of inactivity.

Table 66: Expansion port configuration 1

If the *Reject new connections* item is ticked, all other connections are rejected. This means that it is not possible to establish multiple connections.

If the *Check TCP connection* is selected, the router will automatically send TCP keep-alive messages to verify that the connection is still valid.

Item	Description
Keepalive Time	Time between sending keep-alive packets
Keepalive Interval	Keep-alive Response Timeout
Keepalive Probes	Number of attempts before connection is down

Table 67: Expansion port configuration 2

If the option *Use CD as indicator of the TCP connection* is selected, the router will activate the DTR output when a TCP connection is active.

CD	Description
Active	TCP connection is on
Nonactive	TCP connection is off

Table 68: CD signal description

Select *Use DTR as control of TCP connection* to use DTR to control when TCP connections are allowed. (CD on the router).

DTR	Description server	Description client
Active	The router will accept a TCP connection	Router creates a TCP connection
Nonactive	The router does not accept incoming TCP connection	Router ends the TCP connection

Table 69: DTR signal description

The changes in settings will apply after pressing the *Apply* button.

Expansion Port 1 Configuration

☒ Enable expansion port 1 access over TCP/UDP
HW flow control not supported

Port Type:

Baudrate:

Data Bits:

Parity:

Stop Bits:

Split Timeout: msec

Protocol:

Mode:

Server Address:

TCP Port:

Inactivity Timeout *: sec

☐ Reject new connections

☐ Check TCP connection

Keepalive Time: sec

Keepalive Interval: sec

Keepalive Probes:

☐ Use CD as indicator of TCP connection

☐ Use DTR as control of TCP connection

** can be blank*

Figure 57: Expansion port configuration

Example of external port configuration:

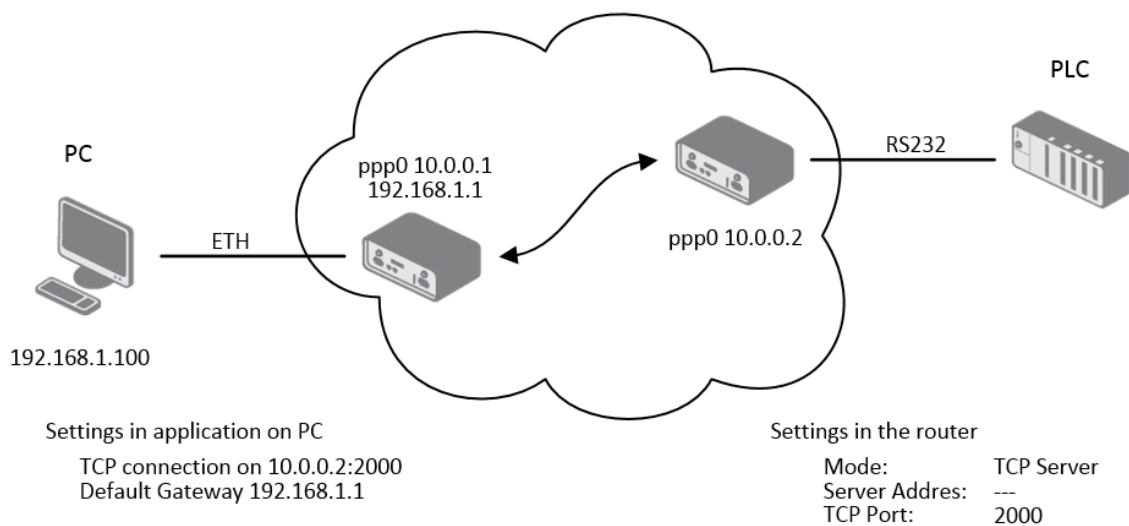


Figure 58: Example of Ethernet to serial communication

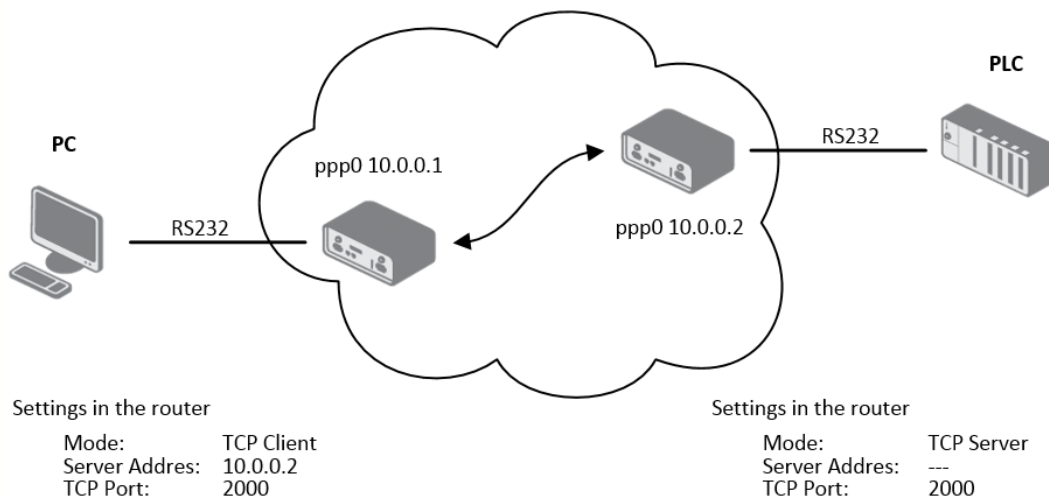


Figure 59: Example of serial port extension



Since firmware 3.0.9, all v2 routers provide a program called *getty* which allows user to connect to the router via the serial line (the router must be fitted with an RS232 expansion port!). *Getty* displays the prompt, and the username has been entered, *getty* passes it on to the *login* program. The login program asks for a password, verifies it and runs the shell. After logging in, you may manage the system, as well as a user who is connected via telnet.

3.21 USB port configuration

Select the *USB Port* item in the configuration menu to bring up the USB configuration page. A USB to RS-232 converter can be used to send data out of the serial port from the Ethernet network in the same manner as the RS-232 expansion port options.

Item	Description
Baudrate	Communication speed
Data Bits	Number of data bits
Parity	Control parity bit: <ul style="list-style-type: none"> • none – data will be sent without parity • even – data will be sent with even parity • odd – data will be sent with odd parity
Stop Bits	Number of stop bits
Split Timeout	Time to rupture reports. If the gap between two characters exceeds the parameter in milliseconds, any buffered characters will be sent over the Ethernet port.
Protocol	Communication protocol: <ul style="list-style-type: none"> • TCP • UDP
Mode	Mode of connection: <ul style="list-style-type: none"> • TCP server – The router will listen for incoming TCP connection requests. • TCP client – The router will connect to a TCP server on the specified IP address and TCP port.
Server Address	When set to <i>TCP client</i> above, it is necessary to enter the <i>Server address</i> and <i>TCP port</i> .
TCP Port	The TCP port for connections.
Inactivity Timeout	Time period after which the TCP/UDP connection is interrupted in case of inactivity.

Table 70: USB port configuration 1

If the *Reject new connections* item is selected, all other connections are rejected. This means that it is not possible to establish multiple connections.

If the *Check TCP connection* option is selected, the router will automatically send TCP keep-alive messages to verify that the connection is still valid.

Item	Description
Keepalive Time	Time between sending keep-alive packets
Keepalive Interval	Keep-alive Response Timeout
Keepalive Probes	Number of attempts before connection is down

Table 71: USB PORT configuration 2

If the option *Use CD as indicator of the TCP connection* is selected, the router will activate the DTR output when a TCP connection is active.

CD	Description
Active	TCP connection is on
Nonactive	TCP connection is off

Table 72: CD signal description

Select *Use DTR as control of TCP connection* to use DTR to control when TCP connections are allowed. (CD on the router).

DTR	Description server	Description client
Active	The router will accept a TCP connection	Router creates a TCP connection
Nonactive	The router does not accept incoming TCP connection	Router ends the TCP connection

Table 73: DTR signal description



Supported USB/RS232 converters:

- FTDI
- Prolific PL2303
- Silicon Laboratories CP210×(supported from firmware version 3.0.1)

The changes in settings will apply after pressing the *Apply* button.

USB Port Configuration

☐ Enable USB serial converter access over TCP/UDP

Baudrate	9600	▼	
Data Bits	8	▼	
Parity	none	▼	
Stop Bits	1	▼	
Split Timeout	20		msec
Protocol	TCP	▼	
Mode	server	▼	
Server Address			
TCP Port			
Inactivity Timeout *			sec

☐ Reject new connections

☐ Check TCP connection

Keepalive Time	3600	sec	
Keepalive Interval	10	sec	
Keepalive Probes	5		

☐ Use CD as indicator of TCP connection
☐ Use DTR as control of TCP connection

Figure 60: USB configuration

Example of USB port configuration:

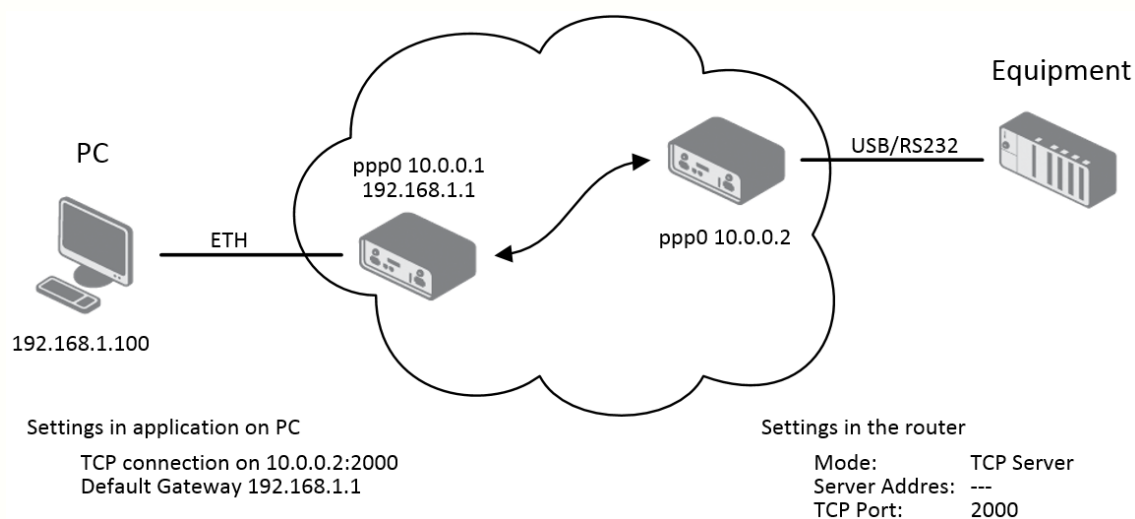


Figure 61: Example of USB port configuration 1

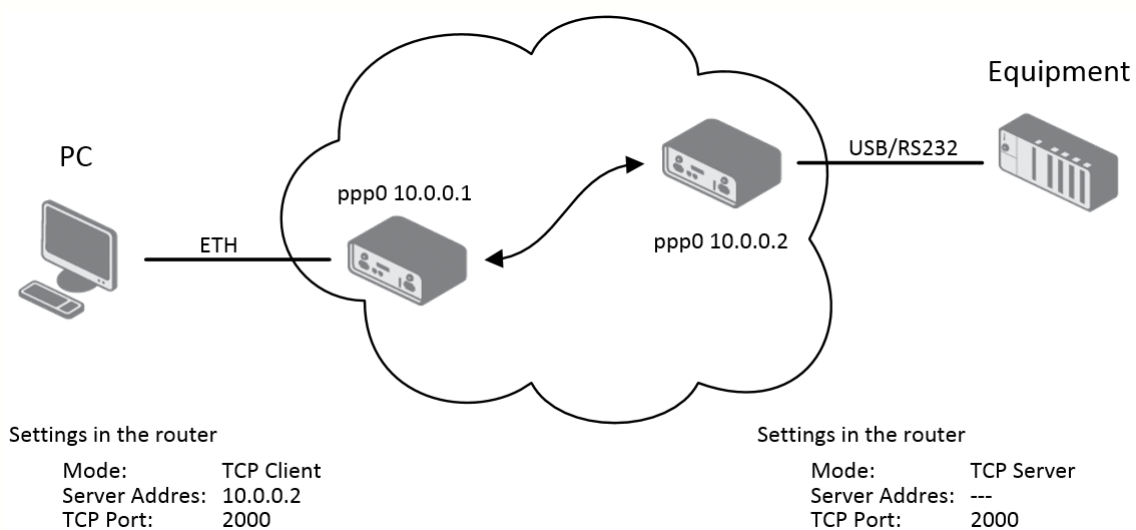
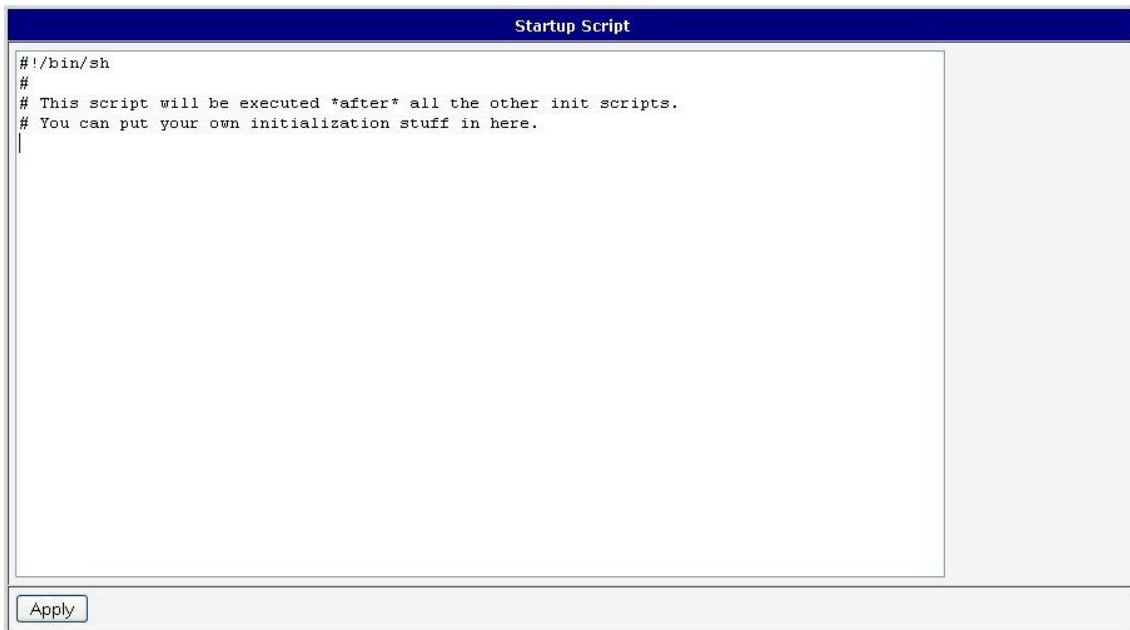


Figure 62: Example of USB port configuration 2

3.22 Startup script

Use the *Startup Script* window to create your own scripts which will be executed after all of the initialization scripts are run.

The changes in settings will apply after pressing the *Apply* button.



```
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here.
```

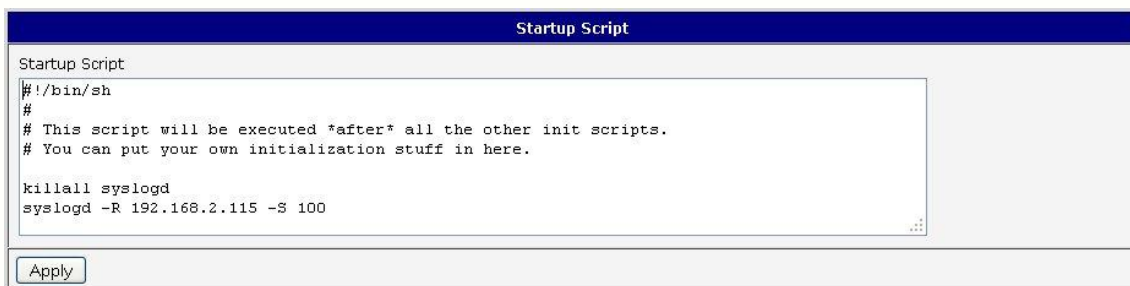
Apply

Figure 63: Startup script



Any changes to the startup scripts will take effect the next time the router is power cycled or rebooted. This can be done with the Reboot button in the web administration, or by SMS message.

Example of Startup script: When the router starts up, stop syslogd program and start syslogd with remote logging on address 192.168.2.115 and limited to 100 entries.



```
Startup Script
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here.

killall syslogd
syslogd -R 192.168.2.115 -S 100
```

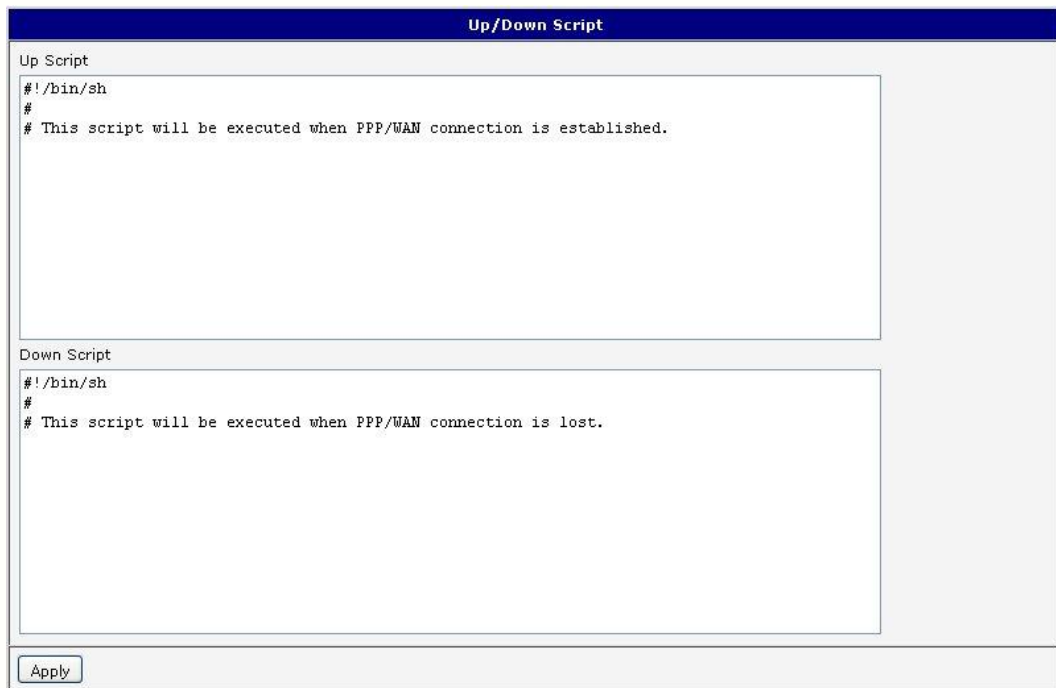
Apply

Figure 64: Example of a startup script

3.23 Up/Down script

Use the *Up/Down Script* window to create scripts which will run when the PPP connection is started or goes down. Any scripts entered into the *Up Script* window will run after a PPP/WAN connection is established. Script commands entered into the *Down Script* window will run when the PPP/WAN connection is lost.

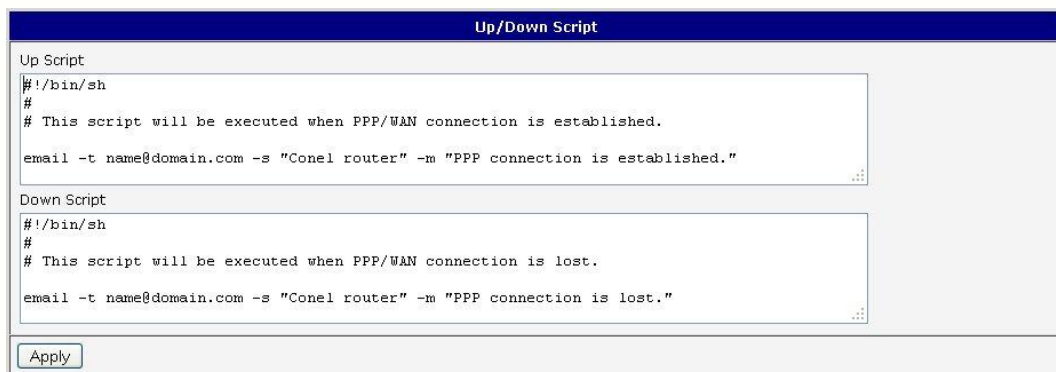
The changes in settings will apply after pressing the *Apply* button.



The screenshot shows the 'Up/Down Script' configuration window. It has two text areas: 'Up Script' and 'Down Script'. Both areas contain the following text: `#!/bin/sh`, `#`, and `# This script will be executed when PPP/WAN connection is established.` (for Up Script) or `# This script will be executed when PPP/WAN connection is lost.` (for Down Script). An 'Apply' button is at the bottom.

Figure 65: Up/Down script

Example of UP/Down script: After establishing or losing a PPP connection (connection to mobile network), the router sends an email with information about the PPP connection.



The screenshot shows the 'Up/Down Script' configuration window with example email commands. The 'Up Script' field contains: `#!/bin/sh`, `#`, `# This script will be executed when PPP/WAN connection is established.`, and `email -t name@domain.com -s "Conel router" -m "PPP connection is established."`. The 'Down Script' field contains: `#!/bin/sh`, `#`, `# This script will be executed when PPP/WAN connection is lost.`, and `email -t name@domain.com -s "Conel router" -m "PPP connection is lost."`. An 'Apply' button is at the bottom.

Figure 66: Example of Up/Down script

3.24 Automatic update configuration

The router can be configured to automatically check for firmware updates from an FTP site or a web server and update its firmware or configuration information. Use the *Automatic update* menu to configure the automatic update settings. It is also possible to update the configuration and firmware through the USB host connector of the router. To prevent possible unwanted manipulation of the files, downloaded file (tar.gz format) is checked. At first, the format of the downloaded file is checked. Then the type of architecture and each file in the archive (tar.gz file) is checked.

If the *Enable automatic update of configuration* option is selected, the router will check if there is a configuration file on the remote server, and if the configuration in the file is different than its current configuration, it will update its configuration to the new settings and reboot.

If the *Enable automatic update of firmware* option is checked, the router will look for a new firmware file and update its firmware if necessary.

Item	Description
Source	<p>Select the location of the update files:</p> <ul style="list-style-type: none"> • HTTP(S)/FTP(S) server – Remote file server. • USB flash drive – Router will check for firmware or configuration files in the root directory of the connected USB device. • Both – Router will check for new firmware or configuration files in both places.
Base URL	Base URL or IP address from which the configuration file will be downloaded. This option also specifies the communication protocol (HTTP, HTTPS, FTP or FTPS), see examples below.
Unit ID	Name of configuration (name of the file without the extension). If the <i>Unit ID</i> of the router is not filled in, then the MAC address of the router will be used as the default file name. (The delimiter in a MAC address is a colon instead of a dot.)
Update Hour	You may select the update hour (Range 1 – 24). If no time is specified, automatic configuration update starts 5 minutes after turning on the router and then every 24 hours at the <i>Update Hour</i> . If the detected configuration file is different from the installed file, the router will download and install the new file.

Table 74: Automatic update configuration

The configuration file name is from parameter *Base URL*, hardware MAC address of ETH0 interface and *cfg* extension. Hardware MAC address and *cfg* extension are added to the file name automatically and it isn't necessary to enter them. When using parameter *Unit ID*, the hardware MAC address in the name will not be used.

The firmware file name is named parameter *Base URL*, type of router and bin extension.



It is necessary to load both files (.bin and .ver) to the HTTP/FTP server. If only the .bin file is uploaded and the HTTP server sends the incorrect answer of *200 OK* (instead of expected *404 Not Found*) when the device tries to download the nonexistent .ver file, then there is a risk that the router will download the .bin file over and over again.

The following examples check for new firmware or configurations each day at 1:00 a.m. An example is given for the SPECTRE LTE router.

- Firmware: <http://example.com/SPECTRE-LTE.bin>
- Configuration file: <http://example.com/test.cfg>

Figure 67: Example of automatic update 1

The following examples check for new firmware or configurations each day at 1:00 a.m. An example is given for the SPECTRE LTE router with MAC address 00:11:22:33:44:55.

- Firmware: <http://example.com/SPECTRE-LTE.bin>
- Configuration file: <http://example.com/00.11.22.33.44.55.cfg>

Figure 68: Example of automatic update 2



Firmware update can cause incompatibility with the user modules. It is recommended to update user modules to the most recent version. Information about the user module and the firmware compatibility is at the beginning of the user module's Application Note.

4. Customization

4.1 User Modules

You may run custom software programs in the router to enhance the features of the router. Use the *User Modules* menu item to add new software modules to the router, to remove them, or to change their configuration. Use the *Browse* button to select the user module (compiled module has tgz extension). Use the *Add* button to add a user module.



The screenshot shows a web interface titled "User Modules". Below the title, it says "No user modules installed." At the bottom, there is a "New Module" label followed by a text input field, a "Procházet..." button, and an "Add" button.

Figure 69: User modules

When a module is added it will appear in the list of modules on the same page. If the module contains an *index.html* or *index.cgi* page, the module name serves as a link to this page. The module can be deleted using the *Delete* button.

Updating a module works the same way. The module with a higher (newer) version will replace the existing module. The current module configuration is kept in same state.



Programming and compiling of modules are described in the programming guide.



The screenshot shows the "User Modules" interface with one module listed: "Example 1.0.0 (2011-05-30)". To the right of the module name is a "Delete" button. At the bottom, there is a "New Module" label followed by a text input field, a "Procházet..." button, and an "Add" button.

Figure 70: Added user module

These are some of the available user modules:

Module name	Description
MODBUS TCP2RTU	Provides a conversion of MODBUS TCP/IP protocol to MDBUS RTU protocol, which can be operated on the serial line.
Easy VPN client	Provides secure connection of LAN network behind our router with LAN network behind CISCO router.
NMAP	Allows the v2 router to do TCP and UDP scan.
Daily Reboot	Allows the v2 router to perform daily reboot of the router at the specified time.

Continued on next page

Continued from previous page

Module name	Description
HTTP Authentication	Adds the process of authentication to a server that doesn't provide this service.
BGP, RIP, OSPF	Add support of dynamic protocols.
PIM SM	Adds support of multicast routing protocol PIM-SM.
WMBUS Concentrator	Allows the v2 router to receive messages from WMBUS meters and saves contents of these messages to an XML file.
pduSMS	Sends short messages (SMS) to specified number.
GPS	Allows the v2 router to provide location and time information in all weather, anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites.
Pinger	Allows you to manually or automatically verify the functionality of the connection between two network interfaces (ping).
IS-IS	Adds support of IS-IS protocol.

Table 75: User modules



Attention: In some cases the firmware update can cause incompatibility with used user modules. Some of them are dependent on the version of the Linux kernel (e.g. *SmsBE* and *PoS Configuration*). It is recommended that you update user modules to the most recent version.

Information about the user module and the firmware compatibility is at the beginning of the user module's Application Note.

5. Administration

5.1 Change Profile

Up to three alternate router configurations or profiles can be stored in router non-volatile memory. You can save the current configuration to a router profile through the *Change Profile* menu item. Select the alternate profile to store the settings to and ensure that the *Copy settings from current profile to selected profile* box is checked. The current settings will be stored in the alternate profile after the *Apply* button is pressed. Any changes will take effect after restarting router through the *Reboot* menu in the web administrator or using an SMS message.

Example of usage profiles: Profiles can be used to switch between different modes of operation of the router such as PPP connection, VPN tunnels, etc. It is then possible to switch between these settings using the front panel binary input, an SMS message, or Web interface of the router.



Figure 71: Change profile

5.2 Change Password

You may change the router password using the *Change Password* menu item. Type the new password twice. The new password will be saved after pressing the *Apply* button.



The default password is **root**. It is strongly recommended that you change the password during initial setup for higher security.

Only the first 8 characters of the password are used for the authentication. Longer passwords are meaningless. This is the standard Unix Crypt mechanism. It won't be possible to enable the remote access to the router (in NAT) until the change of the password is done.



Figure 72: Change password

5.3 Set Real Time Clock

The internal clock of the router can be altered by selecting the *Set Real Time Clock* menu item. Date and time can be manually set by changing the *Date* and *Time* items. The clock can also be adjusted by using a NTP server. This would require you to enter the IP address or domain name of the NTP Server and click *Apply* to set the clock.

Set Real Time Clock	
Date	<input type="text" value="2013 - 07 - 08"/>
Time	<input type="text" value="12 : 50 : 17"/>
NTP Server Address	<input type="text"/>
<input type="button" value="Apply"/>	

Figure 73: Set Real Time Clock

5.4 Set SMS service center address



The SPECTRE RT industrial router and the XR5i v2 do not support the *Set SMS service center address* option.

The SMS service center phone number is normally programmed into the SIM card by the carrier and does not need to be manually entered. However, in some cases, it may be necessary to set the phone number of the SMS service center in order to send SMS messages. This parameter cannot be set if the SIM card already contains the SMSC information. The phone number can be entered with or without an international prefix. For example: +420 xxx xxx xxx. If you are unable to send or receive SMS messages, contact your carrier to find out if this parameter is required. This parameter is provisioned automatically by the carrier on CDMA networks and does not need to be manually entered.

Set SMS Service Center Address	
Service Center Address	<input type="text"/>
<input type="button" value="Apply"/>	

Figure 74: Set SMS service center address

5.5 Unlock SIM card



The SPECTRE RT industrial router and the XR5i v2 do not support the *Unlock SIM card* option.

You may lock the SIM card with a 4-8 digit PIN (Personal Identification Number) code to prevent unauthorized use of the SIM card. The PIN code must be entered each time that the SIM card is powered up. The SPECTRE cellular router supports the use of a SIM card with a PIN number. Enter the PIN number into the SIM PIN field on the configuration page and select *Apply*.



Access to the SIM card is blocked if the PIN code is incorrectly entered 3 times. Contact your SIM card provider if it has been blocked.

Figure 75: Unlock SIM card

5.6 Send SMS



The SPECTRE RT industrial router and the XR5i v2 do not support the *Send SMS* option.

You can send an SMS message from the router to test the cellular network. To send an SMS message, select *Send SMS* from the configuration menu. Enter the phone number and text of the message into the text boxes and click the *Send* button. It may take a few seconds to send the message.

The maximum length of the SMS is 160 characters. (To send longer messages, install the pduSMS user module).

Figure 76: Send SMS

It is also possible to send an SMS message using an HTTP request in the form:

```
GET/send_exec.cgi?phone=%2B420712345678&message=Test HTTP/1.1
Authorization: Basic cm9vdDpyb290
```

The HTTP request will be sent to TCP connection on router port 80. Router sends an SMS message with text "Test". SMS is sent to phone number "420712345678". Authorization is in the format "user:password" coded by BASE64.

5.7 Backup Configuration

You may save the current router configuration to a file using the *Backup Configuration* menu item (*Administration* section). It is recommended that you save the current configuration before a firmware update.

5.8 Restore Configuration

You may restore the router configuration from a file using the *Restore Configuration* menu item (*Administration* section).



Figure 77: Restore Configuration

5.9 Update Firmware

Select the *Update Firmware* menu item to view the current router firmware version and load new firmware into the router. To load new firmware, browse to the new firmware file and press the *Update* button to begin the update.



Do not turn off the router during the firmware update.



Figure 78: Update Firmware

During the firmware update, the router will show the following messages:

```
Uploading firmware to RAM... ok
Programming FLASH..... ok

Reboot in progress

Continue here after reboot.
```

After the firmware update, the router will automatically reboot.



Upload Uploading firmware intended for a different device can cause damage to the router.

Starting with FW 5.1.0, mechanism to prevent multiple startup of firmware update is added. Firmware update can cause incompatibility with the user modules. It is recommended that you update user modules to the most recent version. Information about the user module and the firmware compatibility is at the beginning of the user module's Application Note.

5.10 Reboot

The router can be rebooted remotely through the web interface. To reboot the router, select the *Reboot* menu item and then press the *Reboot* button.



Figure 79: Reboot

6. Configuration over Telnet



Attention! The router cannot operate unless an activated SIM card has been inserted.

Monitoring of status, configuration and administration of the router can be performed over the Telnet interface. The default IP address of the modem is 192.168.1.1. Configuration may be performed only by the user "root" with initial password "root".

The following commands may be used to configure the router over Telnet:

Command	Description
cat	file contain write
cp	copy of file
date	show/change of system time
df	displaying of informations about file system
dmesg	displaying of kernel diagnostics messages
echo	string write
email	Email send
free	displaying of informations about memory
gsmat	sends AT commands (<i>cdmaat</i> for routers with CDMA module)
gsminfo	displaying of informations about signal quality
gsmsms	SMS send
hwclock	displaying/change of time in RTC
ifconfig	displaying/change of interface configuration
io	reading/writing input/output pins
ip	displaying/change of route table
iptables	displaying/modification of NetFilter rules
kill	process kill
killall	processes kill
ln	link create
ls	dump of directory contain
mkdir	file create
mv	file move
ntpdate	synchronization of system time with NTP server
passwd	password change

Continued on next page

Continued from previous page

Command	Description
ping	ICMP ping
ps	displaying of processes information
pwd	dump of actual directory
reboot	reboot
rm	file delete
rmdir	directory delete
route	displaying/change of route table
service	start/stop of service
sleep	pause on set seconds number
slog	displaying of system log
tail	displaying of file end
tcpdump	monitoring of network
touch	file create/actualization of file time stamp
vi	text editor

Table 76: Telnet commands

7. IoT Network Gateway Configuration

7.1 IoT Network Gateway

The SPECTRE Network Gateway routers can provide access to the Wzzard sensor network using a built-in SmartMesh IP module. Support for the Wzzard sensor network is provided by a User Software module which is pre-loaded into the SPECTRE Network Gateway router at the factory. The Wzzard sensor network uses MQTT-SN 93 protocol to communicate between the sensor edge nodes and the gateway. The gateway and the sensor edge nodes must be configured with the same Network ID and Join Key in order for them to communicate with each other. The gateway functions as an MQTT bridge and forwards MQTT-SN data from the sensor nodes to a remote MQTT broker. The Network Gateway also has an internal MQTT v3.1 Broker that allows external MQTT clients to access the sensor node data.

7.2 Gateway Configuration

Select the *User Modules* item under the *Customization* section of the main menu to view the *IoT Gateway* user module.

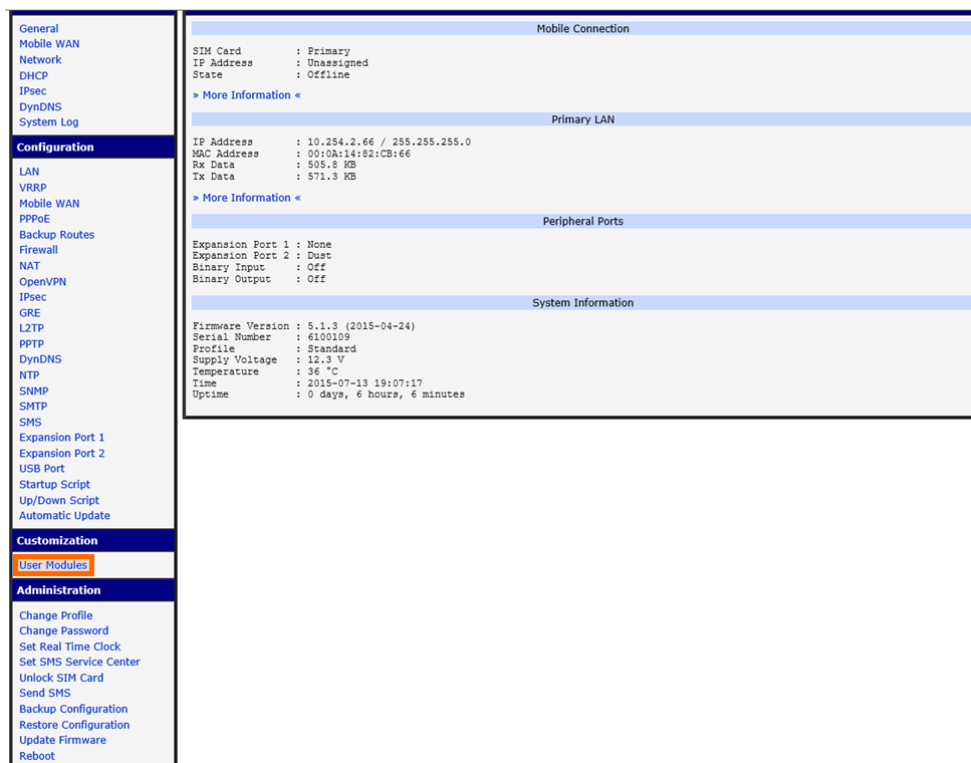


Figure 80: User Modules

This web page shows the user modules that have been loaded into the router and the version number of each module. Click on the *IoT Gateway User Module* to bring up the configuration screen.

The screenshot shows a web interface titled "User Modules". It contains a table with one row: "IoT Gateway 1.1 (20150608T160912Z)" with a "Delete" button next to it. Below the table, there are three input fields: "New Module", "Browse...", and "Add or Update".

Figure 81: IoT Gateway

The IoT Gateway configuration screen contains sections for configuring the sensor network, the internal MQTT broker, and the MQTT Bridge to an external cloud partner. Once the parameters have been configured, click on the *Save* button to store the settings in the gateway. The *Restore* button can be used to reset the text boxes to the stored values.

The screenshot shows the "IoT Gateway Settings" configuration page. It is divided into several sections:

- SmartMesh IP**
 - Network ID**: A text box containing "1981" with a description: "The SmartMesh IP network identifier (1 - 65534)."
 - Join Key**: A text box with a description: "Enter a value only if the SmartMesh IP common join key (32 hexadecimal digits) is to be changed; otherwise, leave this blank to keep the current common join key."
- MQTT Broker**
 - MQTT Broker Enable**: A dropdown menu set to "Off" with a description: "Enable the local MQTT broker."
 - MQTT Broker Port**: A text box containing "1883" with a description: "The local MQTT broker TCP port number (1 - 65535)."
- MQTT Bridge**
 - MQTT Bridge Enable**: A dropdown menu set to "Off" with a description: "Enable bridging to a remote MQTT broker."
 - MQTT Bridge Port**: A text box containing "1883" with a description: "The remote MQTT broker TCP port number (1 - 65535)."
 - MQTT Bridge Address**: A text box with a description: "The remote MQTT broker address."
 - MQTT Bridge User**: A text box with a description: "The user name for the remote MQTT broker."
 - MQTT Bridge Password**: A text box with a description: "The password for the remote MQTT broker."
 - MQTT Bridge Client Identifier**: A text box with a description: "The client identifier for the remote MQTT broker."
- Dust Link**
 - Dust Link Enable**: A dropdown menu set to "Off" with a description: "Enable Dust Link installation tool for initial site survey. During the site survey, no SmartMesh IP data will be sent to the MQTT Broker or MQTT Bridge."
 - Dust Link Port**: A text box containing "8001" with a description: "The TCP port number used to listen for Dust Link (1 - 65535)."

At the bottom of the page, there are three buttons: "Save", "Restore", and "Return".

Figure 82: IoT Gateway Configuration

7.3 SmartMesh IP Configuration

Each SmartMesh Sensor Network gateway must have a unique network ID to prevent interference from other SmartMesh networks. Each sensor node must be programmed with the network ID of the gateway that it should communicate with. In addition, each sensor node on the network must also have the same join key defined. This is a 128-bit value that is used to encrypt the data between the nodes and the gateway. If the join key on the sensor edge node does not match the key programmed into the gateway, the sensor edge node will not be able to communicate with the gateway.

Item	Description
Network ID	Identifies the gateway to other devices on the network
Join Key	128-bit value that is used to encrypt the communication between the node and the gateway

Table 77: SmartMesh IP parameters

7.4 MQTT Broker Configuration

Each SmartMesh Sensor Network gateway has an internal MQTT Broker for connecting with external MQTT clients. The default IP port for the broker is 1883.

Item	Description
MQTT Broker Enable	Enables/Disables the internal MQTT Broker
MQTT Broker Port	IP Port used to access the internal broker

Table 78: MQTT Broker configuration

7.5 MQTT Bridge Configuration

Each SmartMesh Sensor Network gateway has an internal MQTT Bridge for connecting with an external MQTT broker or pubic platform provider. For a public platform provider, the specific configuration settings will be provided by the individual provider.

Item	Description
MQTT Bridge Enable	Enables/Disables the internal MQTT Bridge function
MQTT Bridge Port	IP Port of the external MQTT broker
MQTT Bridge Address	IP Address of the external MQTT broker
MQTT Bridge User	User name for the external MQTT broker

Continued on next page

Continued from previous page

Item	Description
MQTT Bridge Password	Password for the external MQTT broker
MQTT Bridge Client Identifier	The unique client ID for the external MQTT broker

Table 79: MQTT Bridge parameters

7.6 DUST LINK Configuration

The Dust Link program is used to do a site survey. The Dust Link program and setup instructions can be obtained from the B+B website:

<https://bb-smartsensing.com/technical-documentation>

Item	Description
On/Off	Enables or disables DustLink installation tool for initial site survey
Dust Link Port	The TCP port number used to listen for Dust Link (1 – 65535)

Table 80: DUST LINK configuration

During the site survey, no SmartMesh IP data will be sent to the MQTT Broker or MQTT Bridge and changes to the SmartMesh IP network identifier and join key will not take effect until Dust Link is disabled. If changes to the network identifier or join key are required, it is recommended to make the changes prior to enabling Dust Link. When the site survey is complete, Dust Link must be turned off in order for SmartMesh IP data to be sent to the MQTT Broker and MQTT Bridge.

The Dust Link Port is the TCP port number used to listen for communication from a serial port redirector used with the Dust Link program. This port must not conflict with other TCP ports of the router listening for incoming TCP connections.

7.7 SmartMesh IP Port LEDs

LED	Description
Green LED	SmartMesh IP module is powered on
Yellow LED	Permanently off

Table 81: SmartMesh IP port LEDs