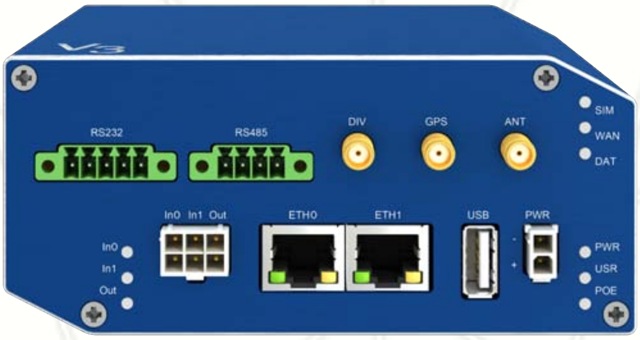
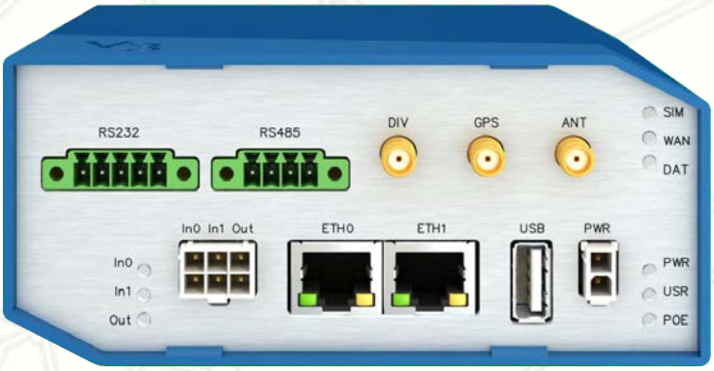
B+B SMARTWORX®

ENABLING CONNECTED INTELLIGENCE

Configuration Manual

for v3 Routers





ENABLING CONNECTED INTELLIGENCE

Used symbols

⚠ *Danger* – important notice, which may have an influence on the user's safety or the function of the device.

❗ *Attention* – notice on possible problems, which can arise in specific cases.

ℹ *Information, notice* – information, which contains useful advice or special interest.

Firmware version

Actual version of firmware is 5.1.0 (March 17, 2015).

GPL licence

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

info@conel.cz.

CE

TÜVRheinland®
COTI
ISO 9001

Conel s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
Manual Rev. 1 released in CZ, June 3, 2015

Contents

List of Figures

List of Tables

1. Basic Information

Cellular routers SPECTRE v3 LTE are designed for communication in mobile networks using LTE, HSPA+, UMTS, EDGE or GPRS technology. Data transfer speed is up to 100 Mbit/s (download) and up to 50 Mbit/s (upload). The router is an ideal solution for wireless connection of traffic and security camera systems, individual computers, LANs, automatic teller machines (ATM), other self-service terminals, etc.

Standard equipment of the router: Two Ethernet 10/100 ports, one USB 2.0 Host port, two binary inputs and one output (I/O connector). Two readers for 3 V and 1.8 V SIM cards, memory card reader for microSD cards – maximum capacity of inserted card can be 64 GB (32 GB in case of SDHC cards).

Optional equipment of the router: The router can be equipped with WiFi module on customer's request (it is not possible to add it to the router later in the future). Other possible interfaces are: Three ports SWITCH, serial line RS232, combined serial line RS232-RS485/422. Router is supplied either in a plastic or metal casing, based on the requirements of the customer. For details see the router's Technical manual.

Configuration possibilities: Statistics about the router activities, signal strength, detailed system log, etc. Creation of VPN tunnels using technologies IPSec, OpenVPN and L2TP for secure communications. Functions such as DHCP, NAT, NAT-T, DynDNS, NTP, VRRP, control by SMS, backup primary connection and many other. Automatic check of PPP connection offering an automatic restart feature in case of connection fail, hardware watchdog monitoring the status of the router. It's possible to insert Linux scripts for various actions. Several different configurations for one LTE wireless router and the option to switch between them (e.g. via SMS, binary input status, etc.). Automatic upgrade configuration and firmware update from server. This allows mass reconfiguration of many routers at one time.

Ways of configuration: Routers can be configured via web browser or Secure Shell (SSH). Configuration via Web Browser is described in this Configuration Manual. Commands and scripts applicable in configuration via SSH are described in Commands and Scripts for v2 and v3 Routers – Application Note [1]. The standard and optional equipment and technical parameters of your router can be found in User's Manual of your router. You can use additional software – communication VPN server SmartCluster [2] and software for router monitoring R-SeeNet [3, 4].

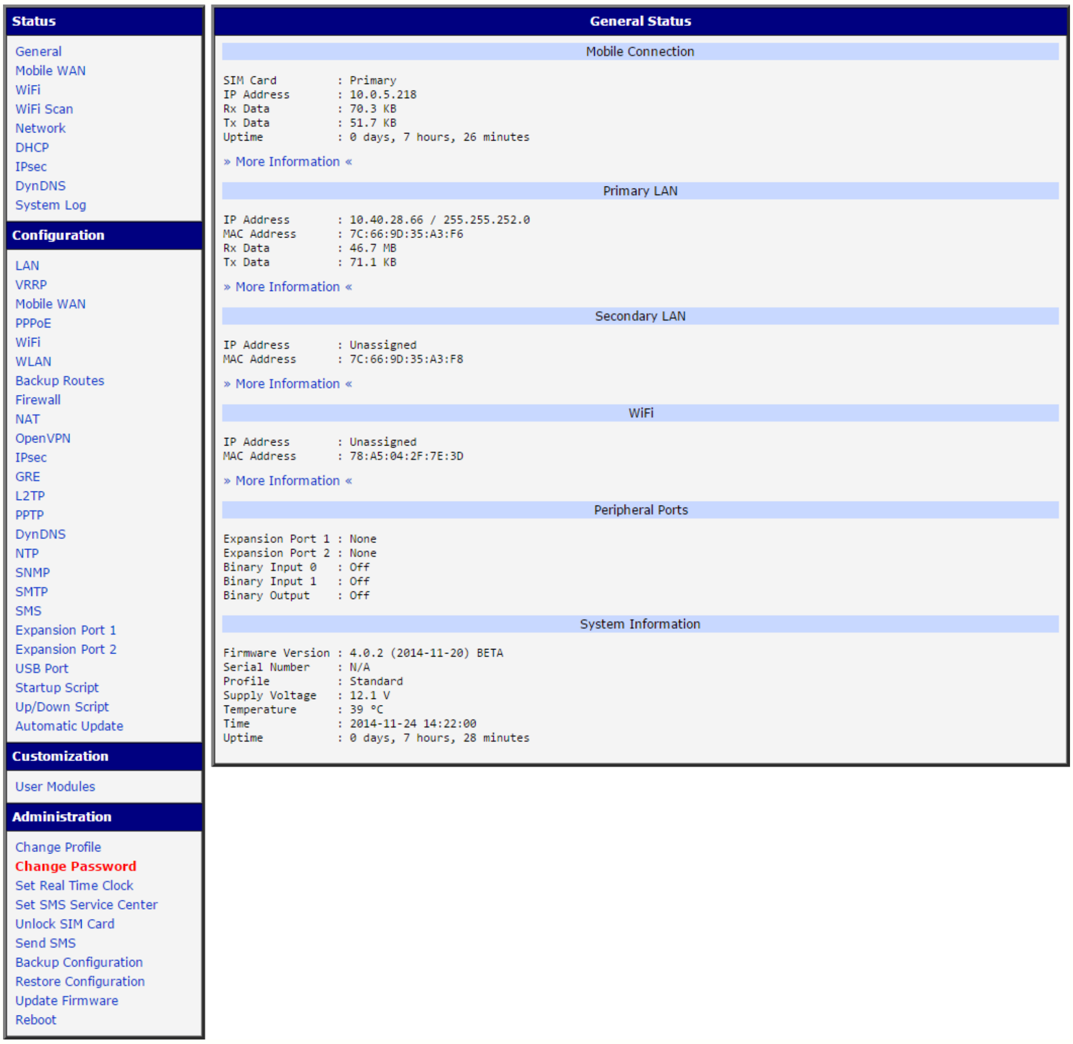
This Configuration Manual describes:

- Configuration of the router item by item according to the web interface (chapters 3 to 6).
- Examples of these typical configurations of the router (chapter 7):
  - Access to the Internet from LAN (Local Area Network) via mobile network
  - Backed up access to the Internet (from LAN)
  - Secure networks interconnection or using VPN (Virtal Private Network)
  - Serial Gateway (connection of serial devices to the Internet)

2. Access to the Web Configuration

Attention! If the SIM card with activated data traffic is not inserted in the router, wireless transmissions will not work. Insert the SIM card when the router is switched-off.

For monitoring, configuring and managing the router, use the web interface which can be invoked by entering the IP address of the router into your browser. The default IP address of the router is 192.168.1.1. and only access via secured **HTTPS** protocol is available. That implies the adress of the router has to be in https://192.168.1.1 syntax. When accessing for the first time, it will be necessary to install a security certificate. To prevent the domain disagreement message of your browser, follow the procedure described in the following subchapter. Configuration may be performed only by the user "***root***" with initial password "***root***".



```
Mobile Connection

SIM Card         : Primary
IP Address       : 10.0.5.218
Rx Data          : 70.3 KB
Tx Data          : 51.7 KB
Uptime           : 0 days, 7 hours, 26 minutes

Primary LAN

IP Address       : 10.40.28.66 / 255.255.252.0
MAC Address      : 7C:66:9D:35:A3:F6
Rx Data          : 46.7 MB
Tx Data          : 71.1 KB

Secondary LAN

IP Address       : Unassigned
MAC Address      : 7C:66:9D:35:A3:F8

WiFi

IP Address       : Unassigned
MAC Address      : 78:A5:04:2F:7E:3D

Peripheral Ports

Expansion Port 1 : None
Expansion Port 2 : None
Binary Input 0   : Off
Binary Input 1   : Off
Binary Output    : Off

System Information

Firmware Version : 4.0.2 (2014-11-20) BETA
Serial Number    : N/A
Profile          : Standard
Supply Voltage   : 12.1 V
Temperature      : 39 °C
Time             : 2014-11-24 14:22:00
Uptime           : 0 days, 7 hours, 28 minutes
```

Figure 1: Example of the web configuration

The left part of the web interface contains the menu with sections for monitoring (*Status*), *Configuration*, *Customization* and *Administration* of the router.

Name and *Location* items in the right upper corner displays the name and location of the router filled in the SNMP configuration (see SNMP Configuration).

For increased safety of the network managed by the router, the default router password must be changed. If the router's default password is set, the ***Change password*** item is highlighted in red.

After green LED starts to blink it is possible to restore initial settings of the router by pressing button RST on back panel. If RST button pressed, configuration would restore to default and the router would reboot (green LED would be on).

2.1 Preventing the domain disagreement message

Since the domain name in the certificate is the given MAC address of the router, it is necessary to access the router via this domain name (use dash separators instead of colons). To enable this, add a DNS record in your DNS system:

- Edit /etc/hosts (Linux/Unix OS)
- Edit C:\WINDOWS\system32\drivers\etc\hosts (Windows OS)
- Configure 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.

3. Status

3.1 General Status

A summary of basic information about the router and its activities can be invoked by selecting the *General* 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*, *Secondary LAN*, *Peripherals Ports* and *System Information*. If the router is SWITCH version, there will be *Tertiary LAN* block displayed. If the router is WiFi equipped, there will be *WiFi* block displayed, too.

3.1.1 Mobile Connection

Item	Description
SIM Card	Identification of the SIM card (*Primary* or *Secondary*)
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	Indicates how long the connection to mob. network is established

Table 1: Mobile Connection

3.1.2 Primary LAN, Secondary LAN, Tertiary LAN, WiFi

Items displayed in this part have the same meaning as items in the previous part. Moreover, the *MAC Address* item shows the MAC address of the corresponding router's interface (*Primary LAN – eth0, Secondary LAN – eth1, Tertiary LAN – eth2, WiFi – wlan0*). Visible information depends on configuration (see 4.1 or 4.4).

3.1.3 Peripheral Ports

Item	Description
Expansion Port 1	Expansion port fitted to the position 1 (*None* indicates that this position is equipped with no port)
Expansion Port 2	Expansion port fitted to the position 2 (*None* 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

3.1.4 System Information

Item	Description
Firmware Version	Information about the firmware version
Serial Number	Serial number of the router (in case of *N/A* 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	Indicates how long the router is used

Table 3: System Information

3.2 Mobile WAN Status

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 the router operates in. 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's network the router operates in
Technology	Transmission technology
PLMN	Code of operator
Cell	Cell the router is connected to
LAC	Location Area Code – unique number assigned to each location area

Continued on next page

Continued from previous page

Item	Description
Channel	Channel the router communicates on
Signal Strength	Signal strength of the selected cell
Signal Quality	Signal quality of the selected cell: • 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 $\frac{N \times RSRP}{RSSI}$) • The value is not available for the EDGE technology
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

Highlighted in red adjacent cells have a close signal quality, which means that there is imminence of frequent switching between the current and the highlighted cell.

The next section of this window displays information about the quality of the connection in each period.

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 Periods

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:

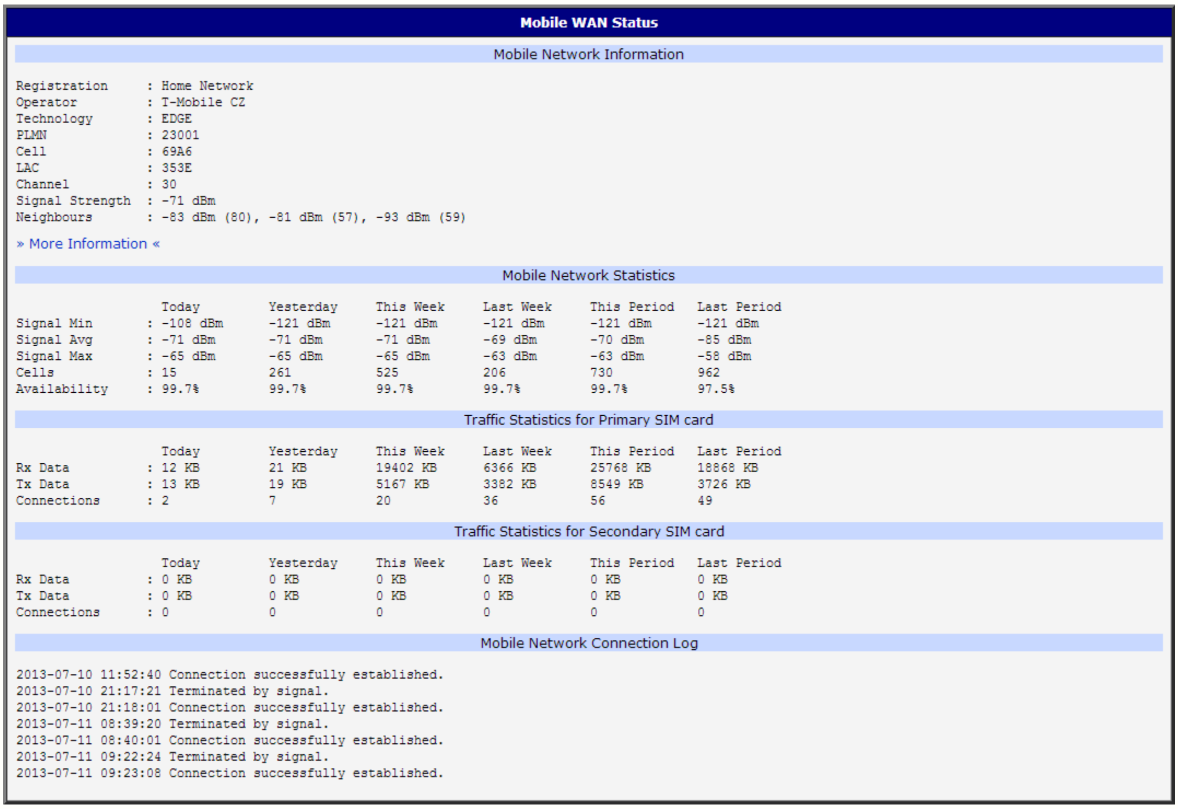
- Availability of connection to mobile network is information expressed as a percentage that is calculated by the ratio of time when connection to mobile network is established to the time when the router is turned on.
- After you place your cursor on the maximum or minimum signal strength, the last time when the router reached this signal strength is displayed.

In the middle part of this page is displayed information about transferred data and number of connections for both SIM cards (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 establishment

Table 7: Traffic Statistics

The last part (*Mobile Network Connection Log*) informs about the mobile network connection and problems in establishment.



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

```
                   Today         Yesterday     This Week     Last Week     This Period   Last Period
Signal Min       : -108 dBm      -121 dBm      -121 dBm      -121 dBm      -121 dBm      -121 dBm
Signal Avg       : -71 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

```
                   Today         Yesterday     This Week     Last Week     This Period   Last Period
Rx Data          : 12 KB         21 KB         19402 KB      6366 KB       25768 KB      18868 KB
Tx Data          : 13 KB         19 KB         5167 KB       3382 KB       8549 KB       3726 KB
Connections      : 2             7             20            36            56            49
```

Traffic Statistics for Secondary SIM card

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

3.3 WiFi

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

After selecting the *WiFi* item in the main menu of the web interface, information about WiFi access point (AP) and associated stations is displayed.

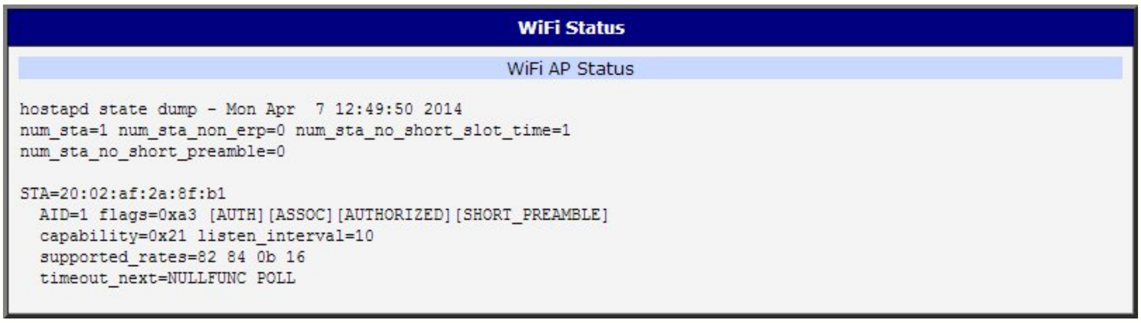
Item	Description
hostapd state dump	Time the statistical data relates to
num_sta	Number of connected stations
num_sta_non_erp	Number of connected stations using 802.11b in 802.11g BSS connection
num_sta_no_short_slot_time	Number of stations not supporting the Short Slot Time
num_sta_no_short_preamble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

Table 8: State Information about Access Point

More detailed information is displayed for each connected client. Most of them has an internal character, let us mention only the following:

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

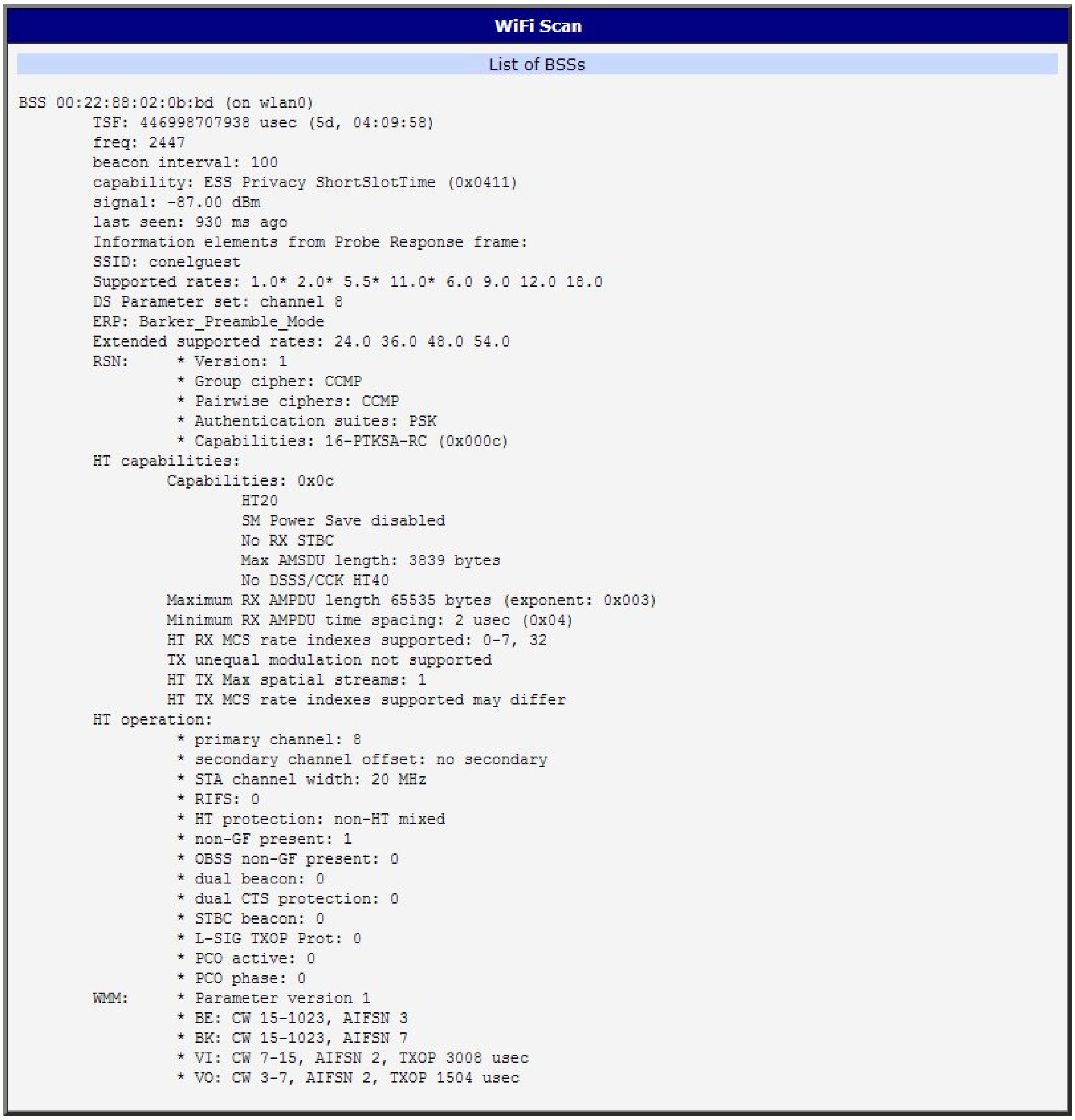
3.4 WiFi Scan

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

After selecting the *WiFi Scan* item in the menu of the web interface, scanning of neighbouring WiFi networks and subsequent printing of results are invoked. **Scanning can be performed only 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 *Supported rates* item
RSN	Robust Secure Network – The protocol for establishing a secure communication through wireless network 802.11

Table 10: Information about Neighbouring WiFi Networks



```
BSS 00:22:88:02:0b:bd (on wlan0)
        TSF: 446998707938 usec (5d, 04:09:58)
        freq: 2447
        beacon interval: 100
        capability: ESS Privacy ShortSlotTime (0x0411)
        signal: -87.00 dBm
        last seen: 930 ms ago
        Information elements from Probe Response frame:
        SSID: conelguest
        Supported rates: 1.0* 2.0* 5.5* 11.0* 6.0 9.0 12.0 18.0
        DS Parameter set: channel 8
        ERP: Barker_Preamble_Mode
        Extended supported rates: 24.0 36.0 48.0 54.0
        RSN:     * Version: 1
                 * Group cipher: CCMP
                 * Pairwise ciphers: CCMP
                 * Authentication suites: PSK
                 * Capabilities: 16-PTKSA-RC (0x000c)
        HT capabilities:
                Capabilities: 0x0c
                        HT20
                        SM Power Save disabled
                        No RX STBC
                        Max AMSDU length: 3839 bytes
                        No DSSS/CCK HT40
                Maximum RX AMPDU length 65535 bytes (exponent: 0x003)
                Minimum RX AMPDU time spacing: 2 usec (0x04)
                HT RX MCS rate indexes supported: 0-7, 32
                TX unequal modulation not supported
                HT TX Max spatial streams: 1
                HT TX MCS rate indexes supported may differ
        HT operation:
                 * primary channel: 8
                 * secondary channel offset: no secondary
                 * STA channel width: 20 MHz
                 * RIFS: 0
                 * HT protection: non-HT mixed
                 * non-GF present: 1
                 * OBSS non-GF present: 0
                 * dual beacon: 0
                 * dual CTS protection: 0
                 * STBC beacon: 0
                 * L-SIG TXOP Prot: 0
                 * PCO active: 0
                 * PCO phase: 0
        WMM:     * Parameter version 1
                 * BE: CW 15-1023, AIFSN 3
                 * BK: CW 15-1023, AIFSN 7
                 * VI: CW 7-15, AIFSN 2, TXOP 3008 usec
                 * VO: CW 3-7, AIFSN 2, TXOP 1504 usec
```

Figure 4: WiFi Scan

3.5 Network Status

To view system information about the router operation, select the *Network* item in the *Status* menu. The upper part of the window displays detailed information about active interfaces:

Interface	Description
eth0, eth1, eth2	Network interfaces (ethernet connection)
usb0	Active PPP connection to the mobile network – wireless module is connected via USB interface
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: Description of interface in network status

Each of the interfaces shows the following information:

Item	Description
HWaddr	Hardware (unique) address of networks interface
inet	IP address of interface
P-t-P	IP address second ends connection
Bcast	Broadcast address
Mask	Mask of network
MTU	Maximum packet size that the equipment is able to transmit
Metric	Number of routers, over which packet must go trought
RX	• **packets** – received packets • **errors** – number of errors • **dropped** – dropped packets • **overruns** – incoming packets lost because of overload • **frame** – wrong incoming packets because of incorrect packet size

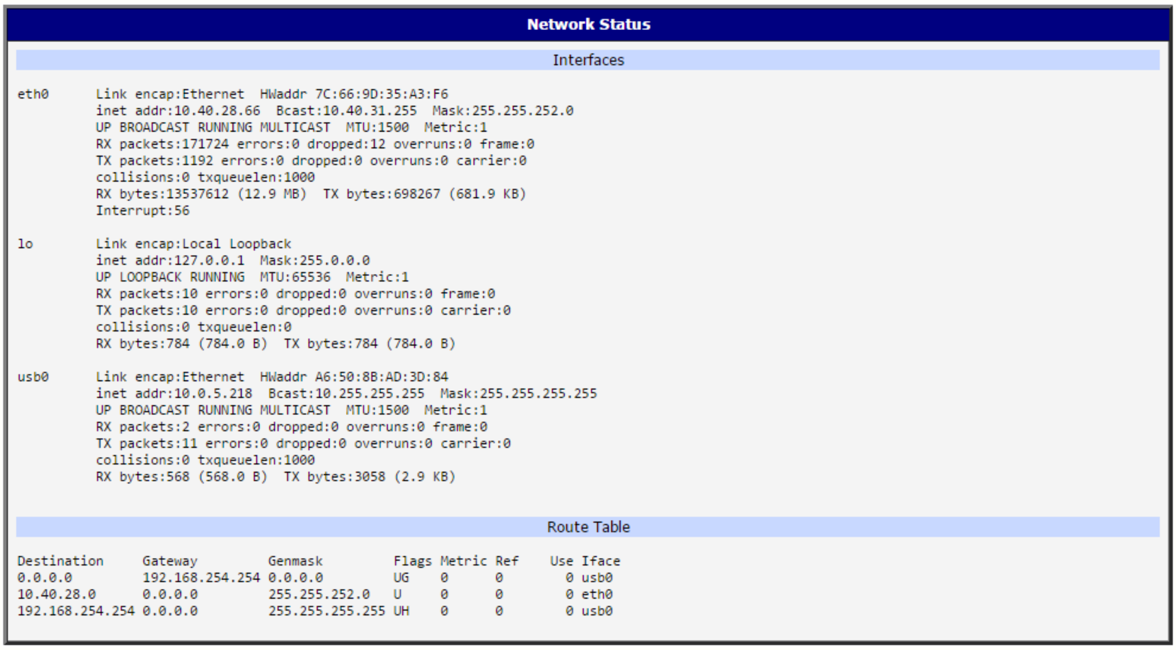
Continued on next page

Continued from previous page

Item	Description
TX	• **packets** – transmit packets • **errors** – number of errors • **dropped** – dropped packets • **overruns** – outgoing packets lost because of overload • **carrier** – wrong outgoing packets with errors resulting from the physical layer
collisions	Number of collisions on physical layer
txqueuelen	Length of front network device
RX bytes	Total number of received bytes
TX bytes	Total number of transmitted bytes

Table 12: Description of Information in Network Status

It is possible to read status of connection to mobile network from the network information. If the connection to the mobile network is active, it will be shown in the system information as an usb0 interface. At the bottom, there is the Route Table displayed.



```
eth0      Link encap:Ethernet  HWaddr 7C:66:9D:35:A3:F6
          inet addr:10.40.28.66  Bcast:10.40.31.255  Mask:255.255.252.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:171724 errors:0 dropped:12 overruns:0 frame:0
          TX packets:1192 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13537612 (12.9 MB)  TX bytes:698267 (681.9 KB)
          Interrupt:56

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:10 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:784 (784.0 B)  TX bytes:784 (784.0 B)

usb0      Link encap:Ethernet  HWaddr A6:50:8B:AD:3D:84
          inet addr:10.0.5.218  Bcast:10.255.255.255  Mask:255.255.255.255
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:568 (568.0 B)  TX bytes:3058 (2.9 KB)
```

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.254.254 0.0.0.0         UG    0      0        0 usb0
10.40.28.0      0.0.0.0         255.255.252.0   U     0      0        0 eth0
192.168.254.254 0.0.0.0         255.255.255.255 UH    0      0        0 usb0
```

Figure 5: Network Status

3.6 DHCP Status

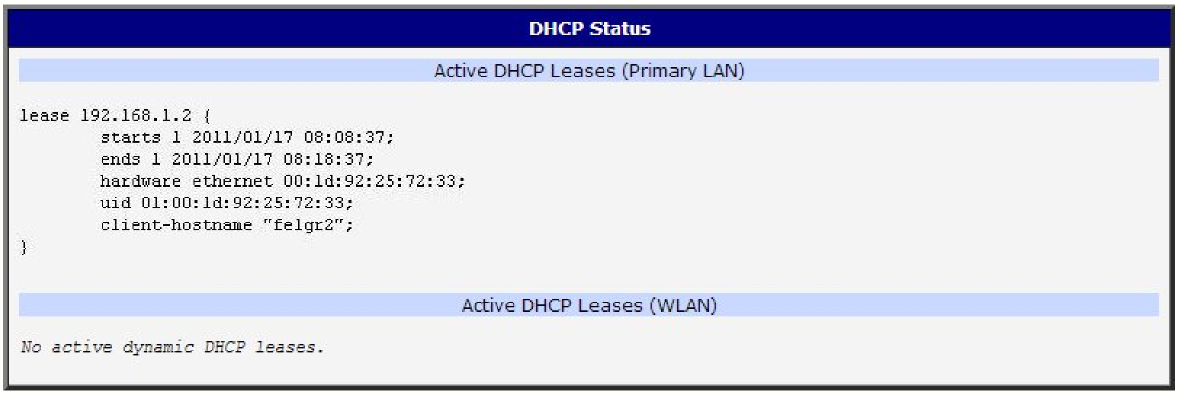
Information about the DHCP server activity is accessible via *DHCP* item. The DHCP server provides automatic configuration of devices connected to the network managed router. DHCP server assigns IP address, netmask, default gateway (IP address of router) and DNS server (IP address of router) to each device.

The DHCP status window displays the following information for each configuration:

Item	Description
lease	Assigned IP address
starts	Time of assignation of IP address
ends	Time of termination IP address validity
hardware ethernet	Hardware MAC (unique) address
uid	Unique ID
client-hostname	Computer name

Table 13: DHCP status description

In the extreme case, the DHCP status can display two records for one IP address. That could have been caused by resetting of network cards.


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.

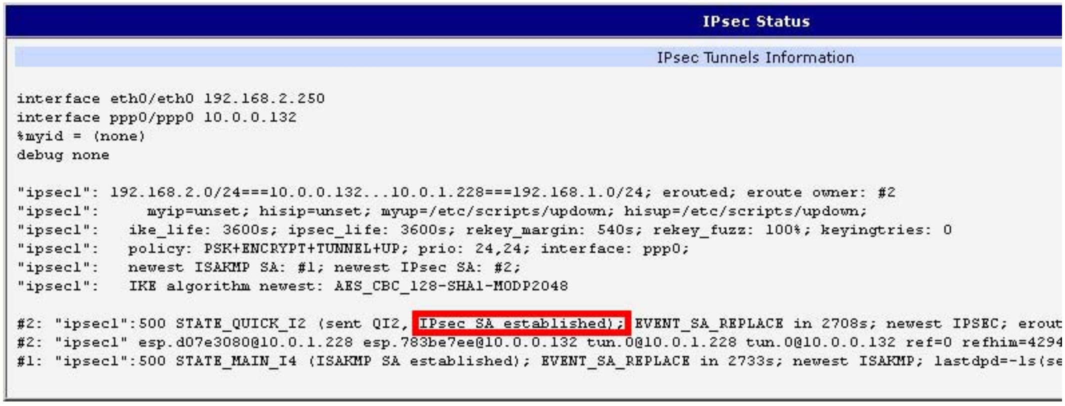
Figure 6: DHCP status

Note: Records in the *DHCP status* window are divided into two separate parts – *Active DHCP Leases (Primary LAN)* and *Active DHCP Leases (WLAN)*.

3.7 IPsec Status

Information on actual IPsec tunnel state can be called up in option *IPsec* in the menu.

After correct build the IPsec tunnel, status display *IPsec SA established* (highlighted in red) in IPsec status information. Other information has only internal character.

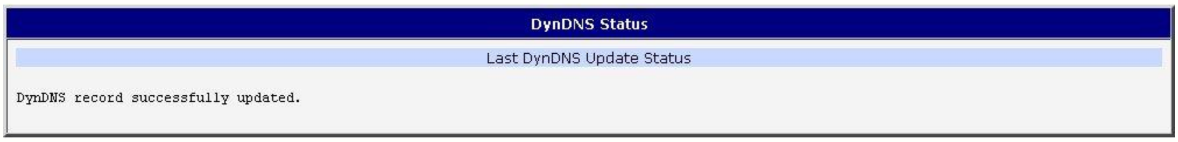


```
interface eth0/eth0 192.168.2.250
interface ppp0/ppp0 10.0.0.132
%myid = (none)
debug none

"ipsec1": 192.168.2.0/24===10.0.0.132...10.0.1.228===192.168.1.0/24; erouted; eroute owner: #2
"ipsec1":     myip=unset; hisip=unset; myup=/etc/scripts/updown; hisup=/etc/scripts/updown;
"ipsec1":   ike_life: 3600s; ipsec_life: 3600s; rekey_margin: 540s; rekey_fuzz: 100%; keyingtries: 0
"ipsec1":   policy: PSK+ENCRYPT+TUNNEL+UP; prio: 24,24; interface: ppp0;
"ipsec1":   newest ISAKMP SA: #1; newest IPsec SA: #2;
"ipsec1":   IKE algorithm newest: AES_CBC_128-SHA1-MODP2048

#2: "ipsec1":500 STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in 2708s; newest IPSEC; erout
#2: "ipsec1" 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: "ipsec1":500 STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in 2733s; newest ISAKMP; lastdpd=-1s(se
```

Figure 7: IPsec Status

3.8 DynDNS status

The result of DynDNS record update (from the server www.dyndns.org) can be invoked pressing the *DynDNS* item in the *Status* menu.



```
DynDNS record successfully updated.
```

Figure 8: DynDNS status

Following messages are possible when detecting the status of DynDNS record update:

- 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.

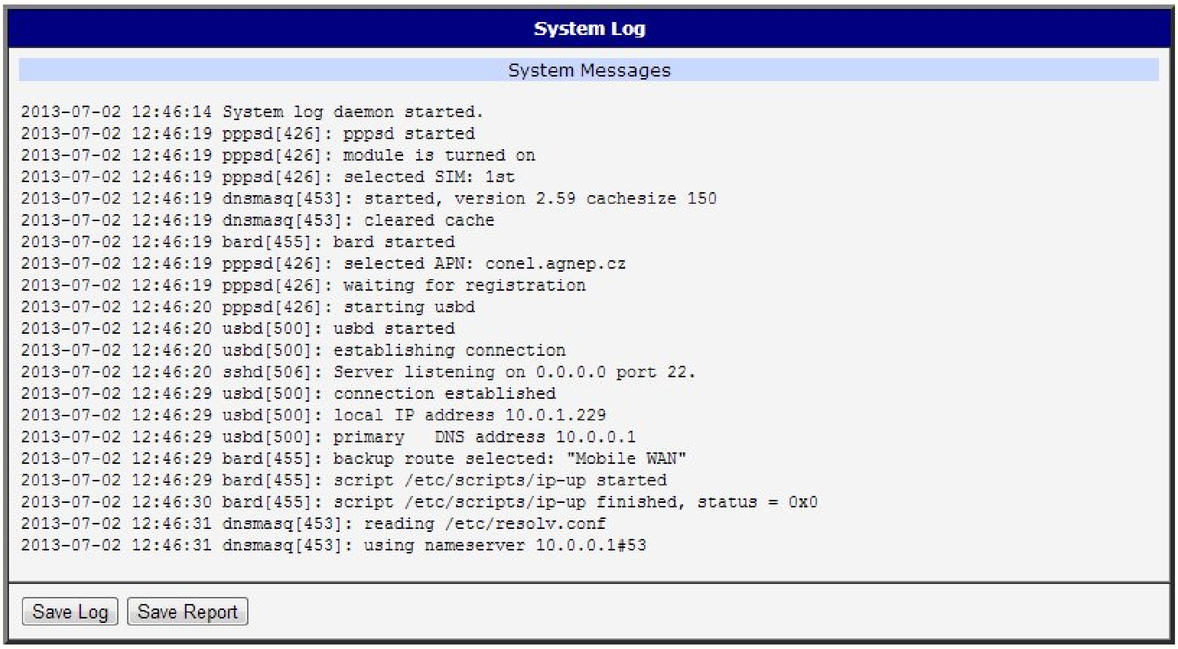
For correct function of DynDNS, SIM card of router must have public IP address assigned.

3.9 System Log

In case of any connection problems it is possible to view the system log by pressing the *System Log* menu item. Detailed reports from individual applications running in the router are displayed. Use the *Save Log* button to save the system log to a connected computer (the text file with the .log extension will be saved). The second button – *Save Report* – is used for creating detailed report (generates all information needed by support in one text file in the .txt format – statistical data, routing and process tables, system log, configuration).

The default length of the system log is 1000 lines. After reaching 1000 lines the new file is created for storing the system log. After completion of 1000 lines in the second file, the first file is overwritten with the new one.

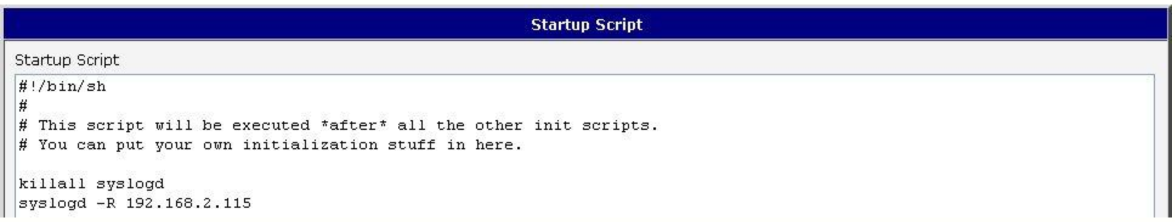
Output of the system log is done by the *Syslogd* program. It can be started with two options to modify its behavior. Option "*-S*" followed by decimal number sets the maximal number of lines in one log file. Option "*-R*" followed by hostname or IP address enables logging to a remote syslog daemon. (If the remote syslog deamon is Linux OS, there has to be remote logging enabled (typically running "*syslogd -R*"). If it's the Windows OS, there has to be syslog server installed, e.g. *Syslog Watcher*). To start *syslogd* with these options, the "*/etc/init.d/syslog*" script can be modified via SSH or lines can be added into *Startup Script* (accessible in *Configuration* section) according to figure 10.



```
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
```

Figure 9: System Log

Example of logging into the remote daemon at 192.168.2.115:



```
#!/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

4. Configuration

4.1 LAN Configuration

To enter the Local Area Network configuration, select the *LAN* menu item in the *Configuration* section. *Primary LAN* is for the first ETH router's interface (ETH0), *Secondary LAN* is for the second ETH router's interface (ETH1). *Tertiary LAN* is for the SWITCH (3x Ethernet) Expansion Port if installed, it is the ETH2 interface.

Item	Description
DHCP Client	• **disabled** – The router does not allow automatic allocation IP address from a DHCP server in LAN network. • **enabled** – The router allows automatic allocation IP address from a DHCP server in LAN network.
IP address	Fixed set IP address of network interface ETH.
Subnet Mask	IP address of Subnet Mask.
Bridged	• **no** – router is not used as a bridge (default) • **yes** – router is used as a bridge
Media type	• **Auto-negation** – The router automatically sets the best speed and duplex mode of communication according to the network's possibilities. • **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 router default gateway. If filled in, all packets not fitting the route table rules would have been sent to this adress.
DNS server	IP address of DNS server of the router. All the DNS queries are forwarded to this address.

Table 14: Configuration of the Network Interface

Default Gateway and *DNS Server* items are used only if the *DHCP Client* item is set to *disabled* and if the Primary or Secondary LAN is selected by Backup routes system as a default route (selection algorithm is described in section *4.6 Backup Routes*).

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

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

DHCP server supports static and dynamic assignment of IP addresses. Dynamic DHCP server assigns clients IP addresses from a defined address space. Static DHCP assigns IP addresses that correspond to the MAC addresses of connected clients.

Item	Description
Enable dynamic DHCP leases	If checked, dynamic DHCP server enabled.
IP Pool Start	Start of IP addresses allocated to the DHCP clients.
IP Pool End	End of IP addresses allocated to the DHCP clients.
Lease time	Client can use the IP address for this amount of time in seconds.

Table 15: Configuration of Dynamic DHCP Server

Item	Description
Enable static DHCP leases	If checked, static DHCP server enabled.
MAC Address	MAC address of a DHCP client.
IP Address	Assigned IP address.

Table 16: Configuration of Static DHCP Server

It is important not to overlap ranges of static allocated IP addresses with addresses allocated by the dynamic DHCP. Collision of IP addresses and incorrect function of network may occur if ranges overlaped.

Example 1: The network interface with dynamic DHCP server

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

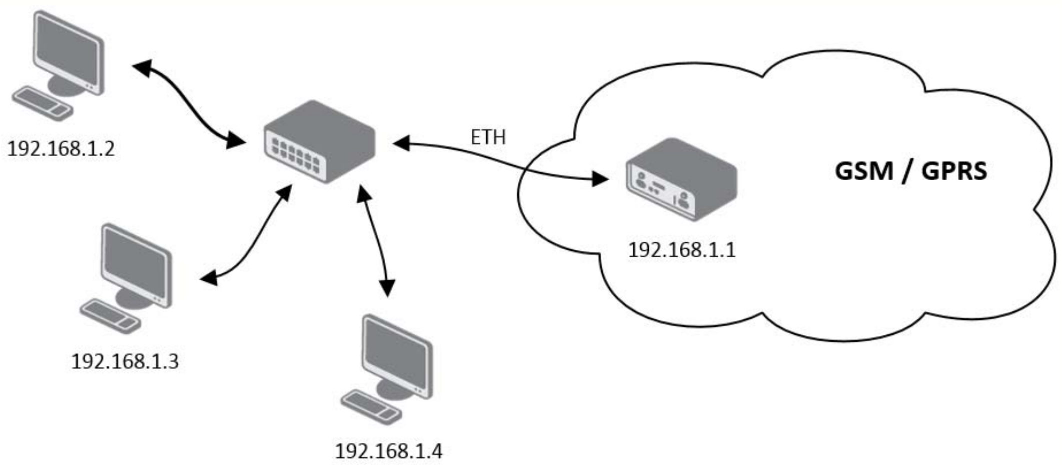
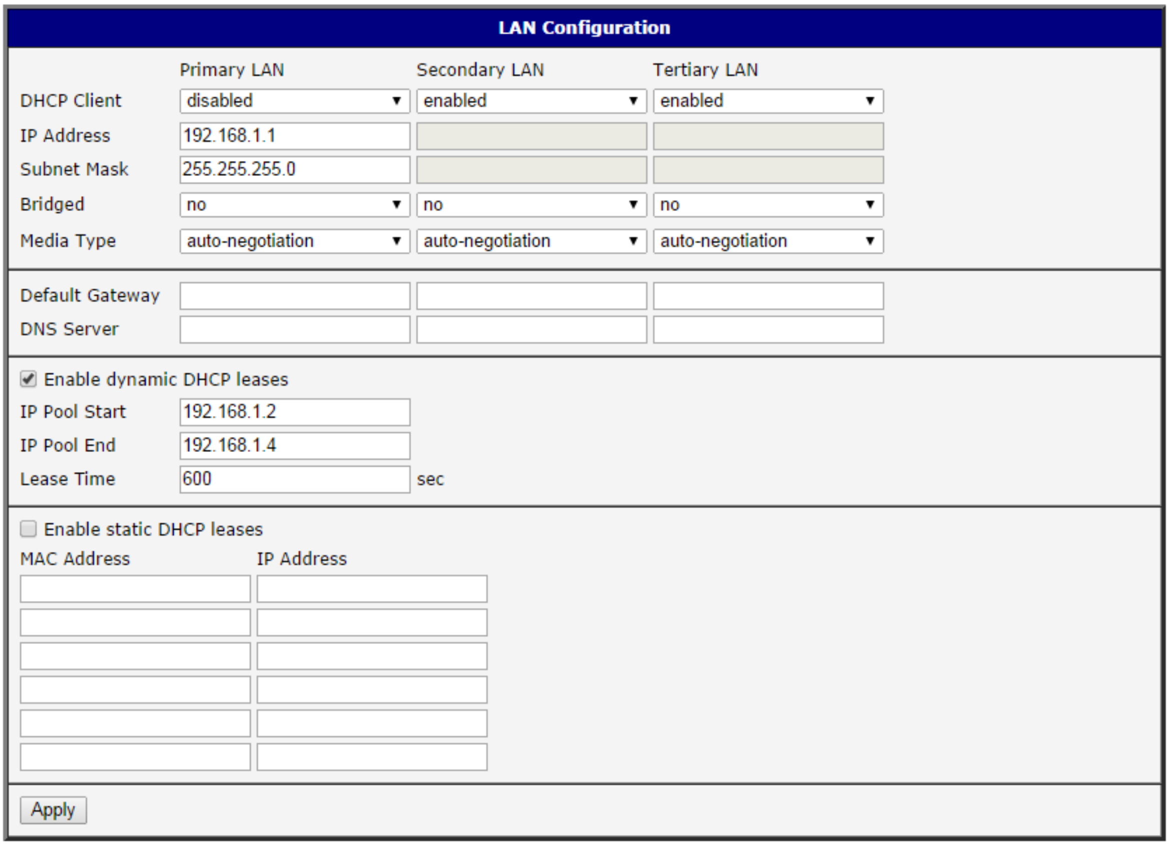


Figure 11: Example 1 Topology of LAN Configuration



LAN Configuration

	Primary LAN	Secondary LAN	Tertiary LAN
DHCP Client	disabled	enabled	enabled
IP Address	192.168.1.1		
Subnet Mask	255.255.255.0		
Bridged	no	no	no
Media Type	auto-negotiation	auto-negotiation	auto-negotiation
Default Gateway			
DNS Server			

☑ Enable dynamic DHCP leases

IP Pool Start	192.168.1.2
IP Pool End	192.168.1.4
Lease Time	600 sec

☐ Enable static DHCP leases

MAC Address	IP Address

Figure 12: Example 1 LAN Configuration

Example 2: The network interface with dynamic and static DHCP server

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

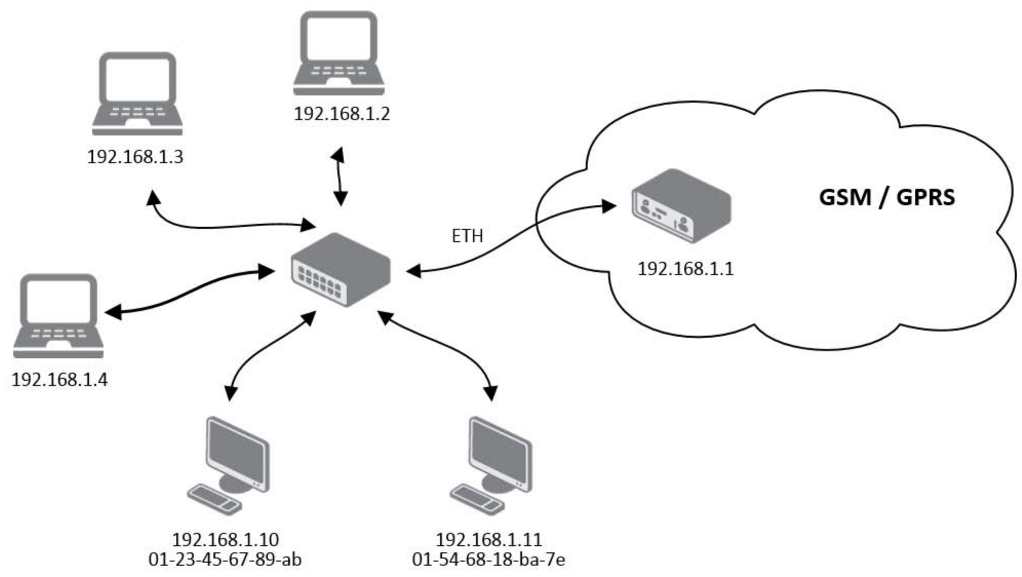
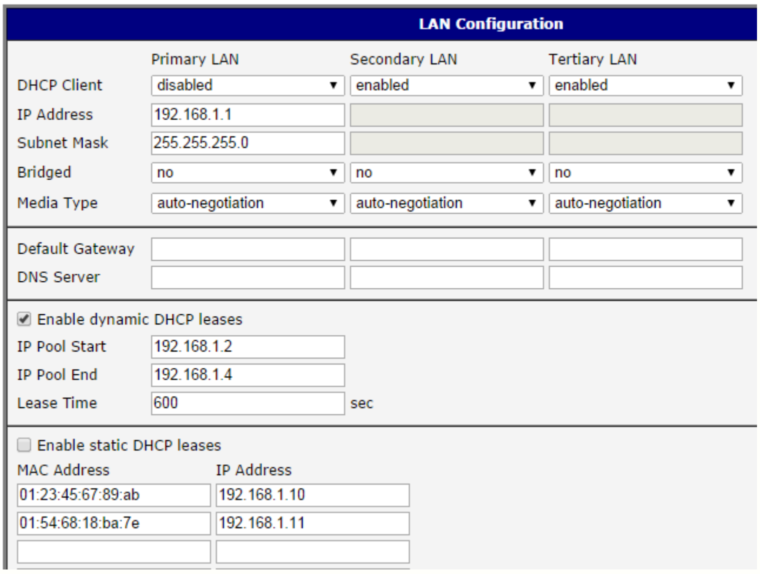


Figure 13: Example 2 Topology of LAN Configuration



LAN Configuration

	Primary LAN	Secondary LAN	Tertiary LAN
DHCP Client	disabled	enabled	enabled
IP Address	192.168.1.1		
Subnet Mask	255.255.255.0		
Bridged	no	no	no
Media Type	auto-negotiation	auto-negotiation	auto-negotiation
Default Gateway			
DNS Server			

☑ Enable dynamic DHCP leases

IP Pool Start	192.168.1.2	
IP Pool End	192.168.1.4	
Lease Time	600	sec

☐ 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

Figure 14: Example 2 LAN Configuration

Example 3: 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

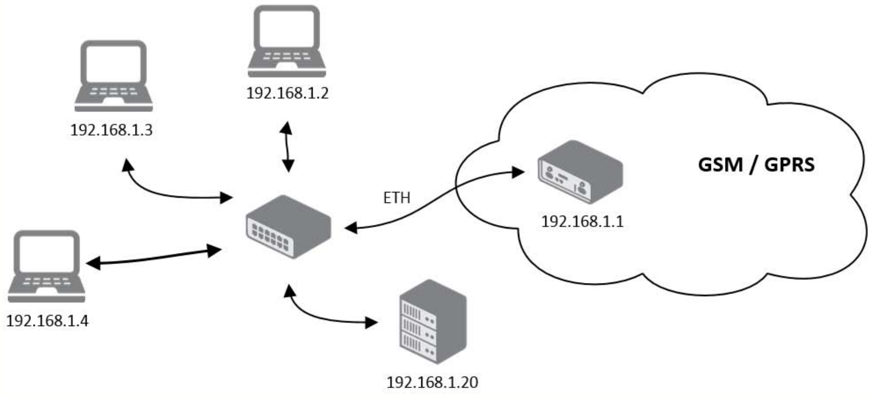
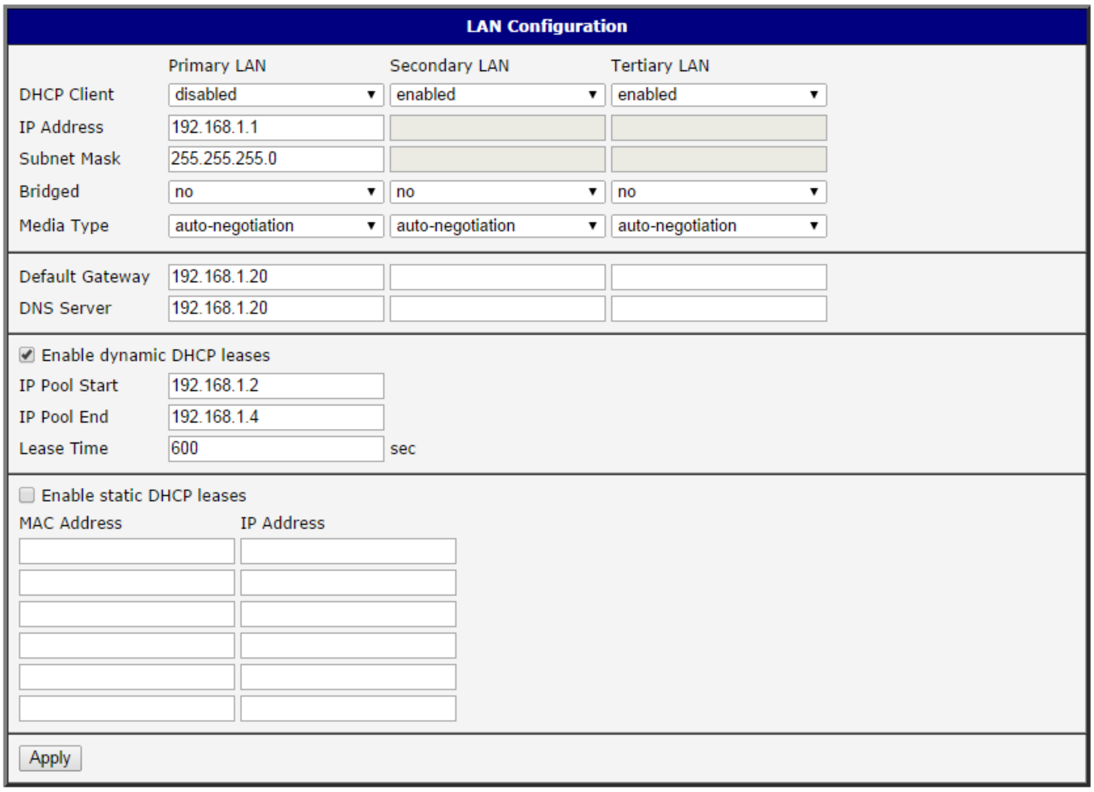


Figure 15: Example 3 Topology of LAN Configuration



LAN Configuration

	Primary LAN	Secondary LAN	Tertiary LAN
DHCP Client	disabled	enabled	enabled
IP Address	192.168.1.1		
Subnet Mask	255.255.255.0		
Bridged	no	no	no
Media Type	auto-negotiation	auto-negotiation	auto-negotiation
Default Gateway	192.168.1.20		
DNS Server	192.168.1.20		

☑ Enable dynamic DHCP leases

IP Pool Start	192.168.1.2
IP Pool End	192.168.1.4
Lease Time	600 sec

☐ Enable static DHCP leases

MAC Address	IP Address

Figure 16: Example 3 LAN Configuration

4.2 Mobile WAN Configuration

Configuration of a connection to the mobile network can be invoked by selecting the *Mobile WAN* item in the *Configuration* menu section.

4.2.1 Connection to Mobile Network

If the *Create connection to mobile network* item is selected, the router automatically tries to establish connection after switching-on. Following items can be set up for every SIM card separately or as two separate APNs to switch one SIM card between.

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: • **PAP or CHAP** – authentication method is chosen by router • **PAP** – it is used PAP authentication method • **CHAP** – it is used CHAP authentication method
IP Address	IP address of SIM card. The user sets the IP address, only in the case IP address was assigned of the operator.
Phone Number	Telephone number to dial GPRS or CSD connection. Router as a default telephone number used *99***1 #.
Operator	This item can be defined PLNM preferred carrier code
Network type	• **Automatic selection** – router automatically selects transmission method according to the availability of transmission technology • *Furthermore, according to the type of router* – 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 in case of several bad attempts to enter the PIN.
MRU	Maximum Receiving Unit – It's an identifier of maximum size of packet, which is possible to receive in a given environment. Default value is 1500 B. Other settings may cause incorrect transmission of data.
MTU	Maximum Transmission Unit – It's an identifier of max. size of packet, which is possible to transfer in a given environment. Default value is 1500 B. Other settings may cause incorrect transmission of data.

Table 17: Mobile WAN connection configuration

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

- If the size is set incorrectly, data transfer may not be succeeded. By setting a lower MTU it occurs to more frequent fragmentation of data, which means higher overhead and also the possibility of damage of packet during defragmentation. On the contrary, the higher value of MTU can cause that the network does not transfer the packet.
- If the *IP address* field is not filled in, the operator automatically assigns the IP address when it is establishing the connection. If filled IP address supplied by the operator, router accelerate access to the network.
- If the *APN* field is not filled in, the router automatically selects the APN by the IMSI code of the SIM card. If the PLMN (operator number format) is not in the list of APN, then default APN is "internet". The mobile operator defines APN.
- If the word *blank* is filled in the *APN* field, router interprets APN as blank.

ATTENTION:

- **If only one SIM card is plugged in the router (router has one slot for a SIM card), router switches between the APN. Router with two SIM cards switches between SIM cards.**
- **Correct PIN must be filled. For SIM cards with two APN's there will be the same PIN for both APN‘s. Otherwise the SIM card can be blocked by false SIM PIN.**

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

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

4.2.2 DNS Address Configuration

The *DNS Settings* item is designed for easier configuration on the client side. When this item is set to the value *get from opertor* router makes an attempt to automatically get an IP address of the primary and secondary DNS server from the operator. By way of contrast, *set manually* option allows you to set IP addresses of Primary DNS servers manually (using the *DNS Server* item).

4.2.3 Check Connection to Mobile Network Configuration

If the *Check Connection* item is set to *enabled* or *enabled + bind*, checking the connection to mobile network is activated. Router will automatically send ping requests to the specified domain or IP address (*Ping IP Address* item) in regular time interval (*Ping Interval*). In case of unsuccessful ping, a new one will be sent after ten seconds. If it fails to ping the IP address of 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. As a ping address can be used an IP address for which it is certain that it is still functional and is possible to send ICMP ping (e.g. DNS server of operator).

In the case of 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 on the occasion of establishing a connection to the mobile operator, it is necessary to set the *Check Connection* item to *enabled + bind*. The *disabled* variant deactivates checking the connection to 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 18: Check connection to mobile network configuration

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

Attention! The enabling of *Check connection* to mobile network is necessary for uninterrupted and lasting operation of the router.

4.2.4 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 *Warning Threshold* determine per cent of Data Limit in the range of 50% to 99%, which if is exceeded, then the router sends SMS in the form *Router has exceeded (value of Warning Threshold) of data limit*.
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 gives the SIM card. The router begin to count the transferred data since that day.

Table 19: Data limit configuration

If 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 datalimit is exceeded* (see SMS configuration) are not selected, the data limit will not count using the oldest versions of Conel routers.

4.2.5 Switch Between SIM Cards Configuration

At the bottom of configuration it is possible to set rules for switching between two APN's on the SIM card, in the event that one SIM card is inserted or between two SIM cards, in the event that two SIM cards are inserted.

Item	Description
Default SIM card	This parameter sets default APN or SIM card, from which it will try to establish the connection to mobile network. If this parameter is set to none, the router launches in offline mode and it is necessary to establish connection to mobile network via SMS message.
Backup SIM card	Defines backup APN or SIM card, that the router will switch the defining one of the following rules.

Table 20: 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* switch the router to off-line mode.

Item	Description
Switch to other SIM card when connection fails	If connection to mobile network fails, then this parameter ensures switch to secondary SIM card or secondary APN of the SIM card. Failure of the connection to mobile network can occur in two ways. When I start the router, when three fails to establish a connection to mobile network. Or if it is checked Check the connection to mobile network, and is indicated by the loss of a connection to mobile network.
Switch to backup SIM card when roaming is detected and switch to default SIM card when home network is detected	In case that the roaming is detected this parameter enables switching to secondary SIM card or secondary APN of the SIM. If home network is detected, this parameter enables switching back to default SIM card. **For proper operation, it is necessary to have enabled 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 parameter enables switching to secondary SIM card or secondary APN of the SIM card, when the data limit of default APN is exceeded. This parameter 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 enables switching to secondary SIM card or secondary APN of the SIM card, when binary input 'bin0' is active. If binary input isn't active, this parameter enables switching back to default SIM card.
Switch to default SIM card after timeout	This parameter defines the method, how the router will try to switch back to default SIM card or default APN.

Table 21: 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 Initial Timeout, range of this parameter is from 1 to 10000 minutes.
Subsequent Timeout	In an unsuccessful attempt to switch to default SIM card, the router on the second attempt to try for the time defined in the parameter Subsequent Timeout, range is from 1 to 10000 min.
Additive constants	Any further attempt to switch back to the primary SIM card or APN shall be made in time computed as the sum of the previous time trial and time defined in the parameter Additive constants range is 1-10000 minutes.

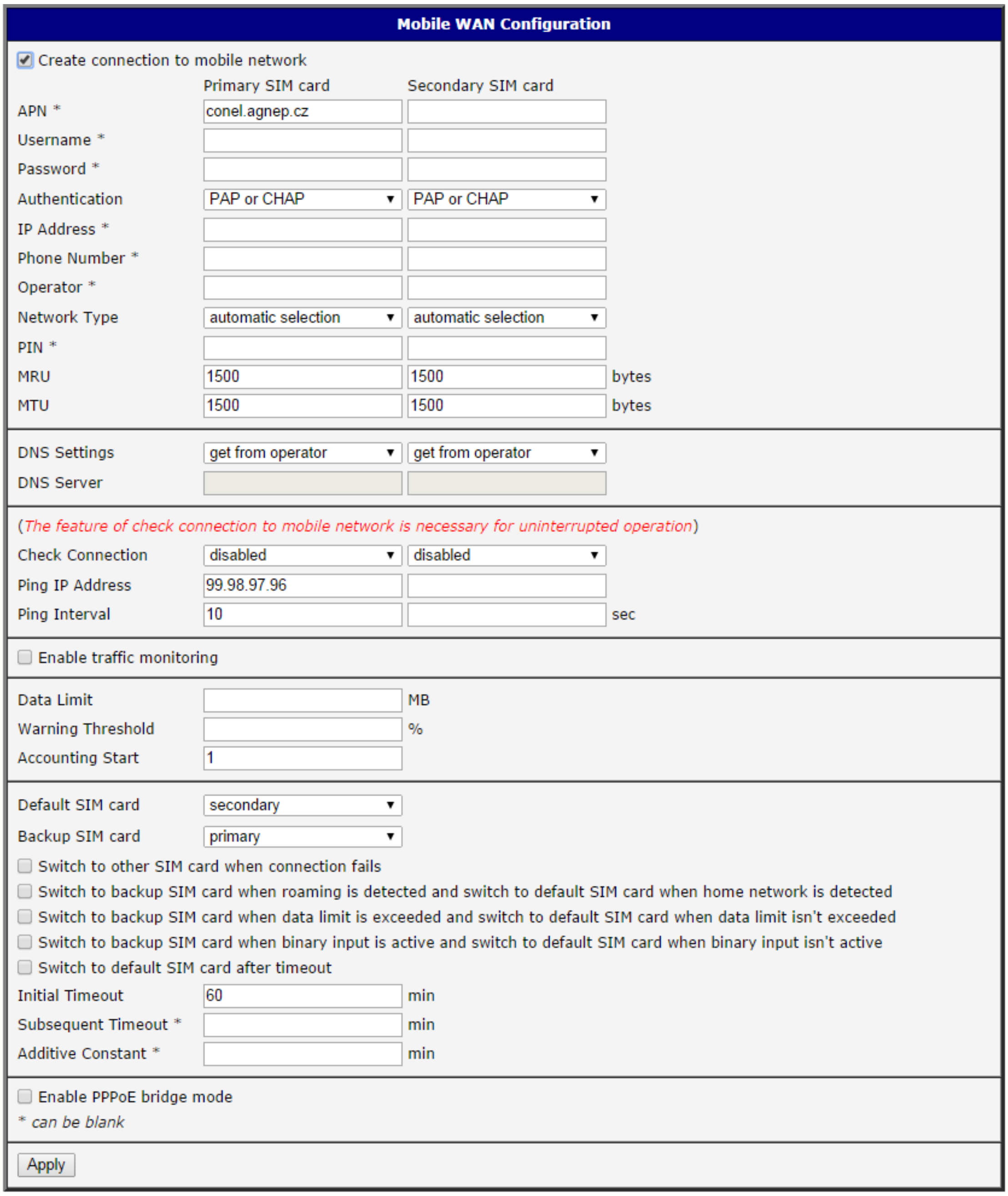
Table 22: Switch between SIM card configurations

Example:
If parameter *Switch to default SIM card after timeout* is checked and parameters are set as follows: *Initial Timeout* – 60 min, *Subsequent Timeout* 30 min and *Additive Timeout* – 20 min, the first attempt to switch the primary SIM card or APN shall be carried out after 60 minutes. Switched to a failed second attempt made after 30 minutes. Third after 50 minutes (30+20). Fourth after 70 minutes (30+20+20).

4.2.6 PPPoE Bridge Mode Configuration

If the *Enable PPPoE bridge mode* option selected, it 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. Allows you to create a PPPoE connection from the device behind router. For example from PC which is connected to ETH port router. The IP address of the SIM card will be alloted to PC.

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



Mobile WAN Configuration

☑ Create connection to mobile network

	Primary SIM card	Secondary SIM card	
APN *	conel.agnep.cz		
Username *			
Password *			
Authentication	PAP or CHAP ▾	PAP or CHAP ▾	
IP Address *			
Phone Number *			
Operator *			
Network Type	automatic selection ▾	automatic selection ▾	
PIN *			
MRU	1500	1500	bytes
MTU	1500	1500	bytes
DNS Settings	get from operator ▾	get from operator ▾	
DNS Server			

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

Check Connection	disabled ▾	disabled ▾	
Ping IP Address	99.98.97.96		
Ping Interval	10		sec

□ Enable traffic monitoring

Data Limit		MB
Warning Threshold		%
Accounting Start	1	
Default SIM card	secondary ▾	
Backup SIM card	primary ▾	

□ 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

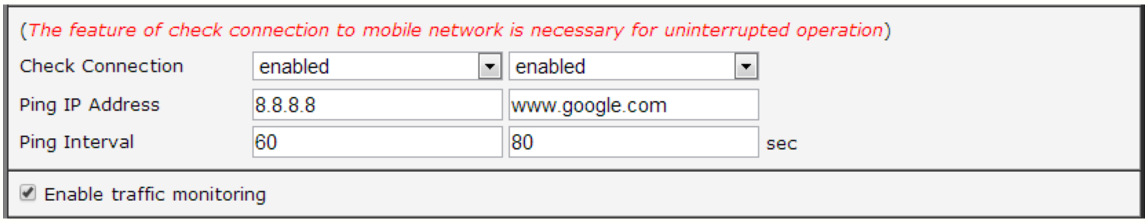
Initial Timeout	60	min
Subsequent Timeout *		min
Additive Constant *		min

□ Enable PPPoE bridge mode

* *can be blank*

Figure 17: 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.



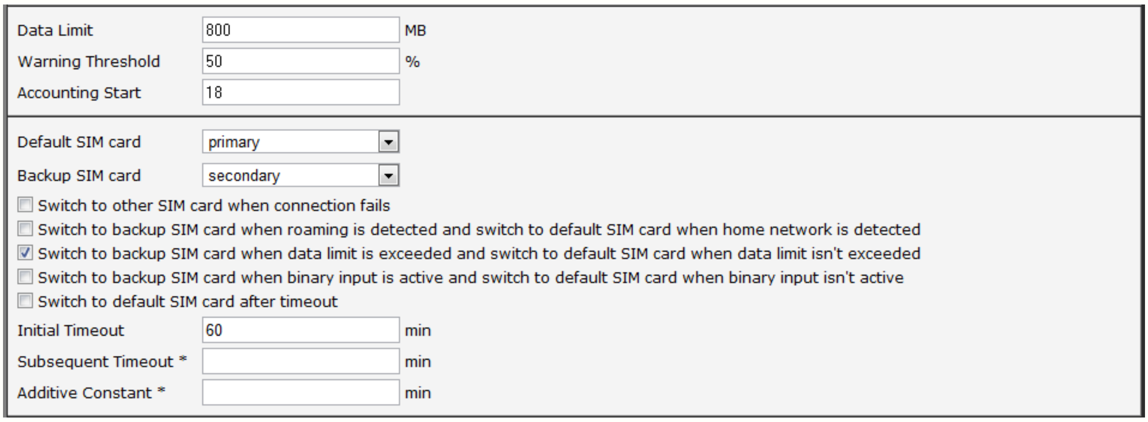
(The feature of check connection to mobile network is necessary for uninterrupted operation)

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

☑ Enable traffic monitoring

Figure 18: 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. Warning SMS is sent upon reaching 400 MB. The start of accounting period is set to the 18th day of the month.



Data Limit	800	MB
Warning Threshold	50	%
Accounting Start	18	

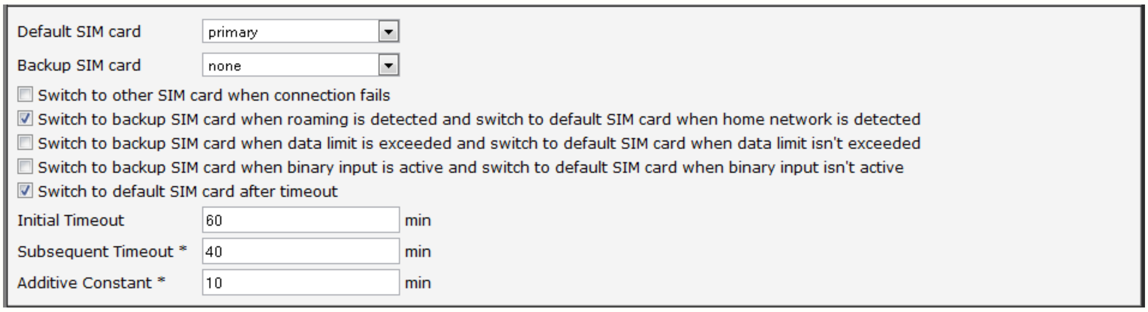
Default SIM card	primary
Backup SIM card	secondary

☐ 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 19: Example 2 – Mobile WAN configuration

Example 3: Primary SIM card is switched to the offline mode after the router detects 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

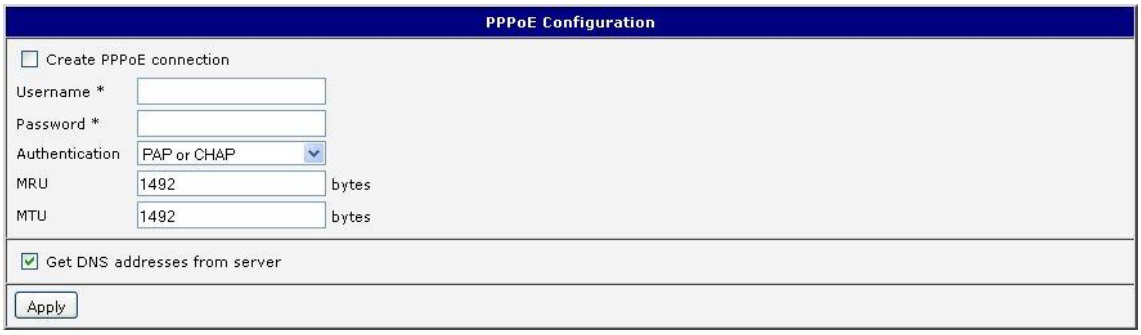
☐ Switch to other SIM card when connection fails
☑ Switch to backup SIM card when roaming is detected and switch to default SIM card when home network is detected
☐ Switch to backup SIM card when data limit is exceeded and switch to default SIM card when data limit isn't exceeded
☐ Switch to backup SIM 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 20: Example 3 – Mobile WAN configuration

4.3 PPPoE Configuration

To enter the PPPoE configuration select the *PPPoE* menu item. If the *Create PPPoE connection* option is selected, the router tries to establish PPPoE connection after switching-on. PPPoE (Point-to-Point over Ethernet) is a network protocol, which PPP frames encapsulating to the Ethernet frames. PPPoE client to connect devices that support PPPoE bridge or a server (typically ADSL router). After connecting the router obtains the IP address of the device to which it is connected. All communications from the device behind the PPPoE server is forwarded to industrial router.



PPPoE Configuration

☐ Create PPPoE connection

Username *		
Password *		
Authentication	PAP or CHAP	
MRU	1492	bytes
MTU	1492	bytes

☑ Get DNS addresses from server

Figure 21: PPPoE configuration

Item	Description
Username	Username for secure access to PPPoE
Password	Password for secure access to PPPoE
Authentication	Authentication protocol in GSM network • **PAP or CHAP** – authentication method is chosen by router • **PAP** – it is used PAP authentication method • **CHAP** – it is used CHAP authentication method
MRU	Maximum Receiving Unit – It is the identifier of the maximum size of packet, which is possible to recese in given environment. Default value is set to 1492 bytes. Other settings may cause incorrect data transmission.
MTU	Maximum Transmission Unit – It is the identifier of the maximum size of packet, which is possible to transfer in given environment. Default value is set to 1492 bytes. Other settings may cause incorrect data transmission.

Table 23: PPPoE configuration

If setting bad packet size value (MRU, MTU), the transmission can be unsuccessful.

4.4 WiFi Configuration

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

The form for configuration of WiFi network can be invoked by pressing the *WiFi* item in the main menu of the router web interface. *Enable WiFi* check box at the top of this form is used to activate WiFi. It is also possible to set the following properties:

Item	Description
Operating mode	WiFi operating mode: • **access point (AP)** – router becomes an access point to which other devices in *station (STA)* mode can be connected • **station (STA)** – router becomes a client station, it means that receives data packets from the available access point (AP) and sends data from cable connection via wifi network
SSID	Unique identifier of WiFi network
Broadcast SSID	Method of broadcasting the unique identifier of SSID network in beacon frame and type of response to a request for sending the beacon frame. • **Enabled** – SSID is broadcasted in beacon frame • **Zero length** – Beacon frame does not include SSID. Requests for sending beacon frame are ignored. • **Clear** – Each SSID character in beacon frame is replaced by 0. However, original length is kept. Requests for sending beacon frame are ignored.
Probe Hidden SSID	Probes hidden SSID (only for *station (STA)* mode)
Country Code	Code of the country, where the router is used with WiFi. This code must be entered in format ISO 3166-1 alpha-2. If *country code* isn't specified and the router has implemented no system to determine this code, it is used "US" as default *country code*. If no *country code* is specified or is entered the wrong country code, then it may come a pass a breach of regulatory rules for the using of frequency bands in the particular country.

Continued on next page

Continued from previous page

Item	Description
HW Mode	HW mode of WiFi standard the access point (AP) will support. • IEE 802.11b • IEE 802.11b+g • IEE 802.11b+g+n
Channel	Channel where the WiFi AP is transmitting
BW 40 MHz	Option for HW mode 802.11n that allows using of two standard 20 MHz channels simultaneously. Option is available in the STA mode also and it has to be enabled in both – the AP and STA mode if using the high throughput mode.
WMM	Enables basic QoS for WiFi networks. This version doesn't guarantee network throughput. It is suitable for simple applications requiring QoS.
Authentication	Provides access control of authorized users in WiFi network: • **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** – authentication using AES encryption
Encryption	Type of data encryption in WiFi network: • **None** – No data encryption • **WEP** – Encryption using static WEP keys. This encryption can be used for *Shared* authentication. • **TKIP** – Dynamic management of encryption keys which can be used for *WPA-PSK* and *WPA2-PSK* authentication. • **AES** – Improved encryption used for *WPA2-PSK* authentication
WEP Key Type	Type of WEP key for WEP encryption: • **ASCII** – WEP key is entered in ASCII format • **HEX** – WEP key is entered in hexadecimal format
WEP Default Key	Specifies default WEP key

Continued on next page

Continued from previous page

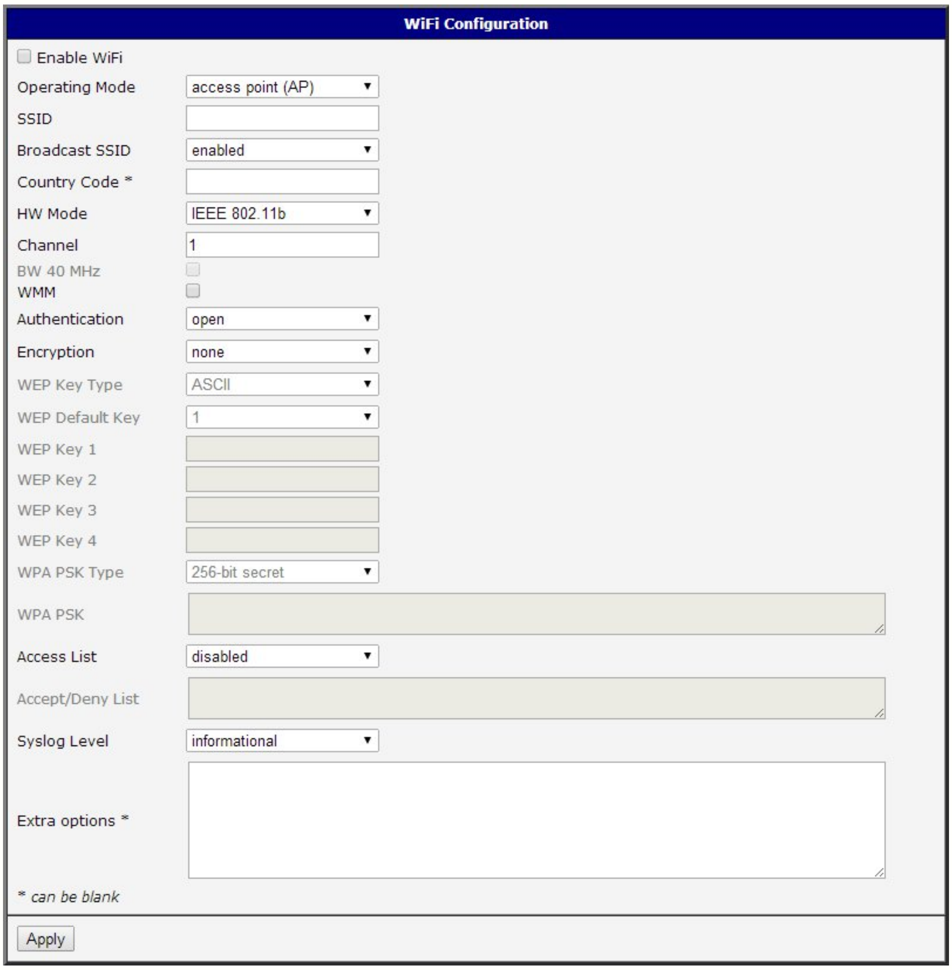
Item	Description
WEP Key 1-4	Items for different four WEP keys • WEP key in ASCII format must be entered in quotes and must have the following lengths: – 5 ASCII characters (40b WEP key) – 13 ASCII characters (104b WEP key) – 16 ASCII characters (128b WEP key) • WEP key in hexadecimal format must be entered using only hexadecimal digits and must the following lengths: – 10 hexadecimal digits (40b WEP key) – 26 hexadecimal digits (104b WEP key) – 32 hexadecimal digits (128b WEP key)
WPA PSK Type	The type of encryption when WPA-PSK authenticating: • 256-bit secret • ASCII passphrase • PSK File
WPA PSK	Key for WPA-PSK authentication. This key must be entered according to the selected WPA-PSK type as follows: • **256-bit secret** – 64 hexadecimal digits • **ASCII passphrase** – from 8 to 63 characterswhich are subsequently converted into PSK • **PSK File** – absolute path to the file containing the list of pairs (PSK key, MAC address)
Access List	Determines a manner of Access/Deny list application: • **Disabled** – Access/Deny list is not used • **Accept** – Only items mentioned in the Access/Deny list have access to the network • **Deny** – Items mentioned in the Access/Deny list do not have access to the network
Accept/Deny List	Accept or Denny list of client MAC addresses that set network access. Each MAC address is separated by new line.

Continued on next page

Continued from previous page

Item	Description
Syslog Level	Communicativeness level when system writes to the system log - **Verbose debugging** – the highest level of communicativeness - **Debugging** - **Informational** – default level of communicativeness which is used for writing standard events - **Notification** - **Warning** – the lowest level of communicativeness
Extra options	Allows user to define additional parameters

Table 24: WiFi configuration



WiFi Configuration

□ Enable WiFi

Operating Mode	access point (AP)
SSID	
Broadcast SSID	enabled
Country Code *	
HW Mode	IEEE 802.11b
Channel	1
BW 40 MHz	□
WMM	□
Authentication	open
Encryption	none
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*

Figure 22: WiFi configuration

4.5 WLAN Configuration

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

The form for configuration of WiFi network and DHCP server functioning on this network can be invoked by pressing the *WLAN* item in the main menu of the router web interface. *Enable WLAN interface* check box at the top of this form is used to activate WIFi LAN interface. It is also possible to set the following properties:

Item	description
Operating Mode	WiFi operating mode: • **access point (AP)** – router becomes an access point to which other devices in *station (STA)* mode can be connected • **station (STA)** – router becomes a client station, it means that receives data packets from the available access point (AP) and sends data from cable connection via wifi network
DHCP Client	Activates/deactivates DHCP client
IP Address	Fixed set IP address of WiFi network interface
Subnet Mask	Subnet mask of WiFi network interface
Bridged	Activates bridge mode: • **no** – Bridged mode is not allowed (it's 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 network of the router. In this case, the setting of most items in this table is ignored. Instead, it takes setting of selected network interface (LAN).
Default Gateway	IP address of default gateway. When entering 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	Address to which all DNS queries are forwarded

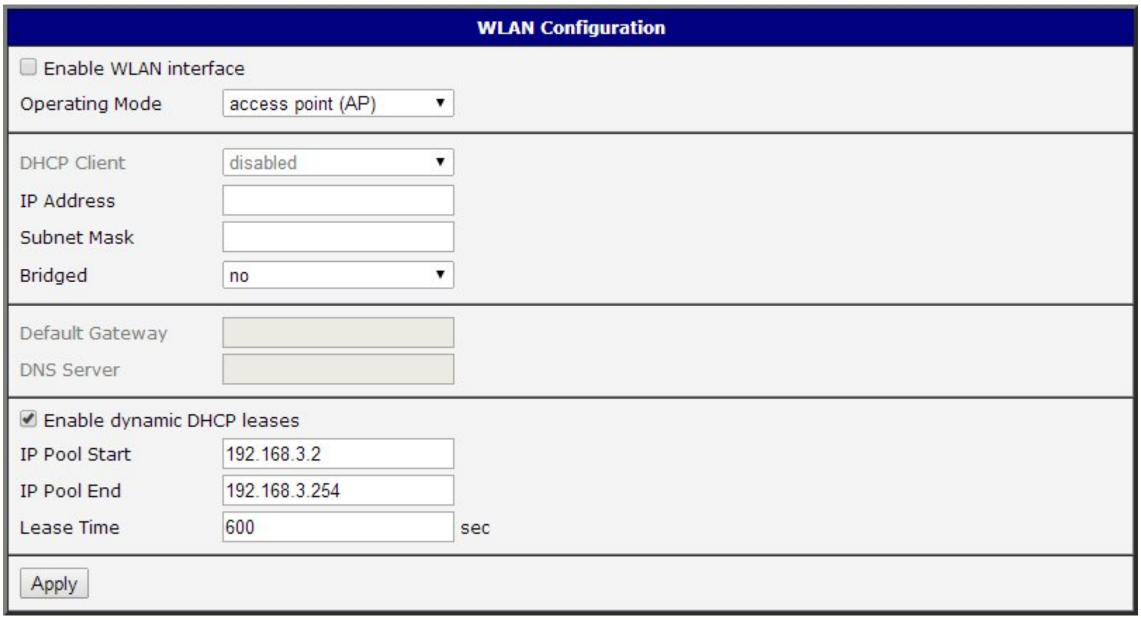
Table 25: WLAN configuration

Use *Enable dynamic DHCP leases* item at the bottom of this form to enable dynamic allocation of IP addresses using DHCP server. It is also possible to 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 26: Configuration of DHCP server

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



WLAN Configuration

☐ Enable WLAN interface

Operating Mode	access point (AP)
DHCP Client	disabled
IP Address	
Subnet Mask	
Bridged	no
Default Gateway	
DNS Server	

☑ Enable dynamic DHCP leases

IP Pool Start	192.168.3.2
IP Pool End	192.168.3.254
Lease Time	600 sec

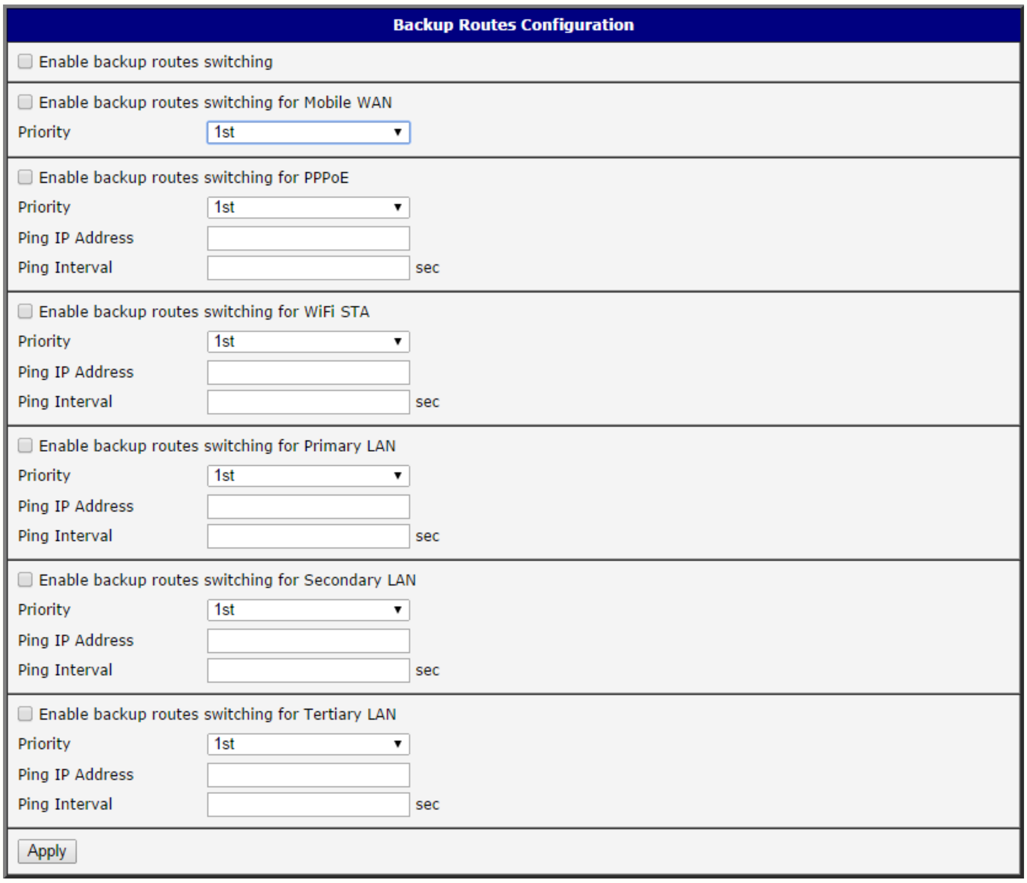
Figure 23: WLAN configuration

4.6 Backup Routes

Using the configuration form on the *Backup Routes* page can be set backing up primary connection by other connections to internet/mobile network. For each back up connection can be defined a priority. Own switching is done based on set priorities and state of the connection (for *Primary LAN* and *Secondary LAN*).

If *Enable backup routes switching* option is checked, the default route is selected according to the settings below. Namely according to status of enabling each of backup route (i.e. *Enable backup routes switching for Mobile WAN*, *Enable backup routes switching for PPPoE*, *Enable backup routes switching for WiFi STA*, *Enable backup routes switching for Primary LAN* or *Enable backup routes switching for Secondary LAN*), according to explicitly set priorities and according to status of connection check (if it is enabled). In addition, network interfaces belonging to individual backup routes have checked a flag RUNNING. This check fixes for example disconnecting 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 4.2.1.



Backup Routes Configuration

□ Enable backup routes switching

□ Enable backup routes switching for Mobile WAN

Priority	1st ▾

□ Enable backup routes switching for PPPoE

Priority	1st ▾
Ping IP Address	
Ping Interval	sec

□ Enable backup routes switching for WiFi STA

Priority	1st ▾
Ping IP Address	
Ping Interval	sec

□ Enable backup routes switching for Primary LAN

Priority	1st ▾
Ping IP Address	
Ping Interval	sec

□ Enable backup routes switching for Secondary LAN

Priority	1st ▾
Ping IP Address	
Ping Interval	sec

□ Enable backup routes switching for Tertiary LAN

Priority	1st ▾
Ping IP Address	
Ping Interval	sec

Figure 24: Backup Routes

If *Enable backup routes switching* option is not checked, 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 enabling settings for each of network interface, as the case may be enabling services that set these network interfaces. Names of backup routes and corresponding network interfaces in order of implicit priorities:

- Mobile WAN (pppX, usbX)
- PPPoE (ppp0)
- WiFi STA (wlan0)
- Secondary LAN (eth1)
- Tertiary LAN (eth2)
- 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, alternatively if *Create PPPoE connection* option is not checked on the *PPPoE* page. To select the Primary LAN it is also necessary not to be entered *IP address* for Secondary LAN and must not be enabled *DHCP Client* for Secondary LAN.

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 27: Backup Routes

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

4.7 Firewall Configuration

The first security element which incoming packets must pass is check of enabled source IP addresses and destination ports. It can be specified IP addresses from which you can remotely access the router and the internal network connected behind a router. If the *Enable filtering of incoming packets* item is checked (located at the beginning of the configuration form *Firewall*), this element is enabled and all incoming packets are checked against the table with IP addresses. This means that incoming packets will be treated according rules specified in the table. It is possible to define up to eight rules for incoming packets. There are the following parameters:

Item	Description
Source	IP address from which access to the router is allowed
Protocol	Specifies protocol for remote access: • **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: • **allow** – access is allowed • **deny** – access is denied

Table 28: Filtering of incoming packets

The following part of the configuration form defines the forwarding policy. If *Enabled filtering of forwarded packets* item is not checked, packets will be accepted automatically. If this item is checked and 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 alowed according to the table, it will be sent out according to the routing table. If the forwarding rule does not exist, packet will be dropped.

In tables with rules it is possible 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: • **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

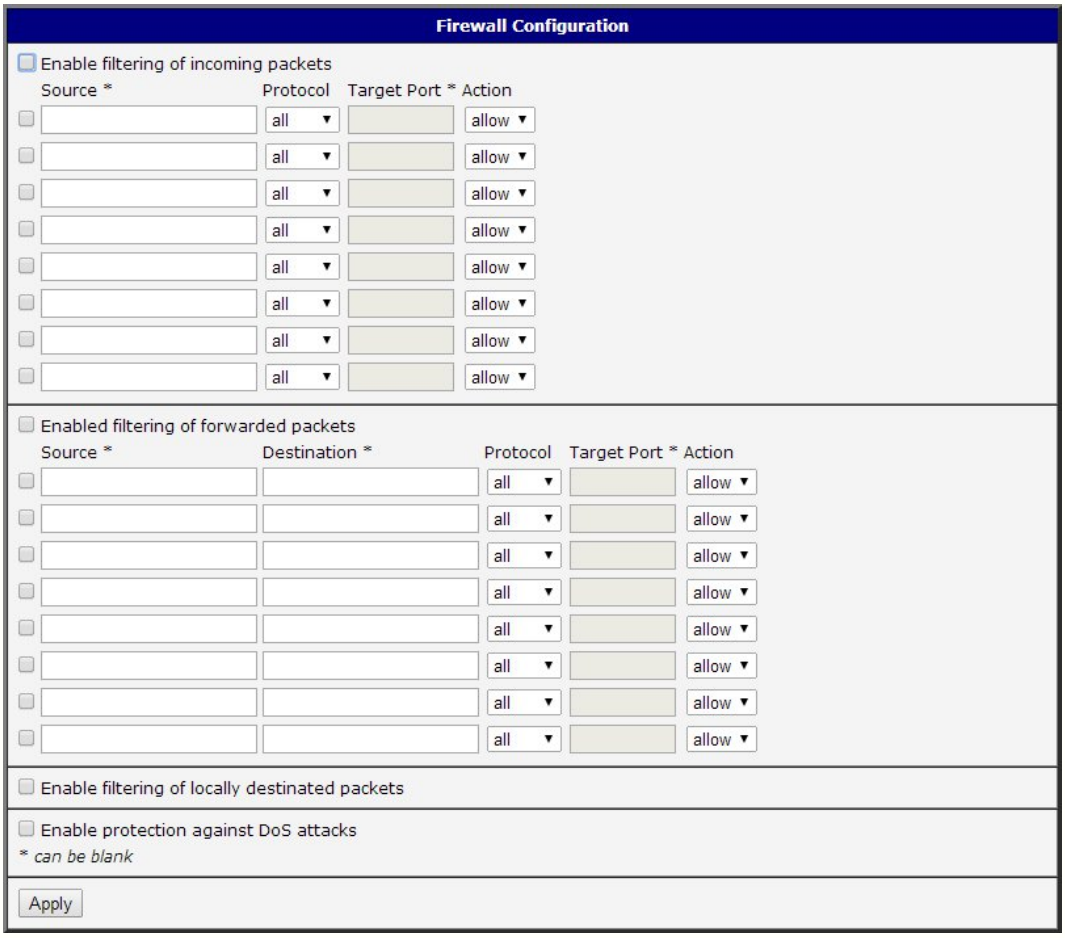
Continued from previous page

Item	Description
Action	Type of action: • **allow** – access is allowed • **deny** – access is denied

Table 29: Forwarding filtering

There is also the possibility to drop a packet whenever request for service which is not in the router comes (check box named *Enable filtering of locally destinated packets*). The packet is dropped automatically without any information.

As a protection against DoS attacks (this means attacks during which the target system is flooded with plenty of meaningless requirements) is used option named *Enable protection against DoS attacks* which limits the number of connections to five per second.



Firewall Configuration

□ Enable filtering of incoming packets

	Source *	Protocol	Target Port *	Action
□		all ▼		allow ▼
□		all ▼		allow ▼
□		all ▼		allow ▼
□		all ▼		allow ▼
□		all ▼		allow ▼
□		all ▼		allow ▼
□		all ▼		allow ▼
□		all ▼		allow ▼

□ Enabled filtering of forwarded packets

	Source *	Destination *	Protocol	Target Port *	Action
□			all ▼		allow ▼
□			all ▼		allow ▼
□			all ▼		allow ▼
□			all ▼		allow ▼
□			all ▼		allow ▼
□			all ▼		allow ▼
□			all ▼		allow ▼
□			all ▼		allow ▼

□ Enable filtering of locally destinated packets

□ Enable protection against DoS attacks

* *can be blank*

Figure 25: 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

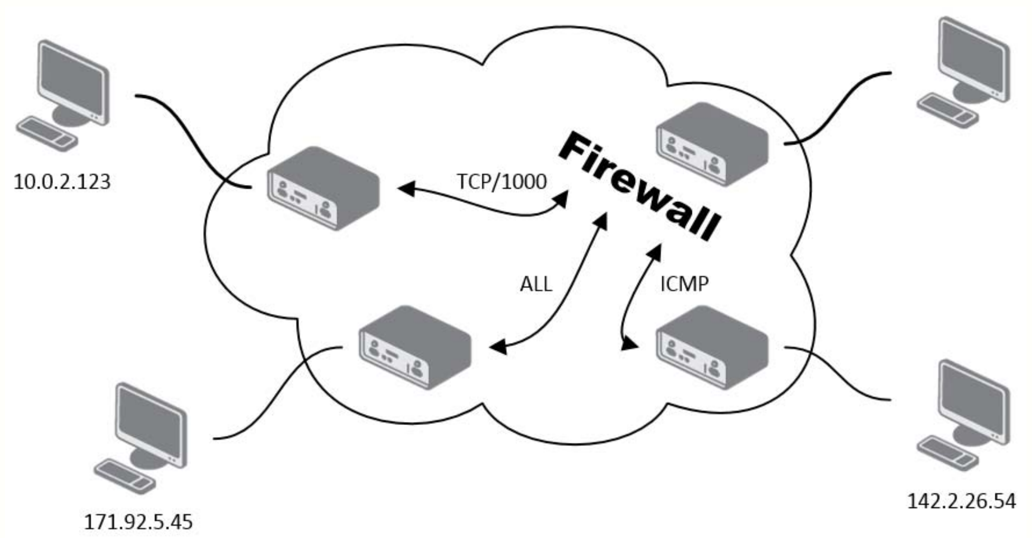
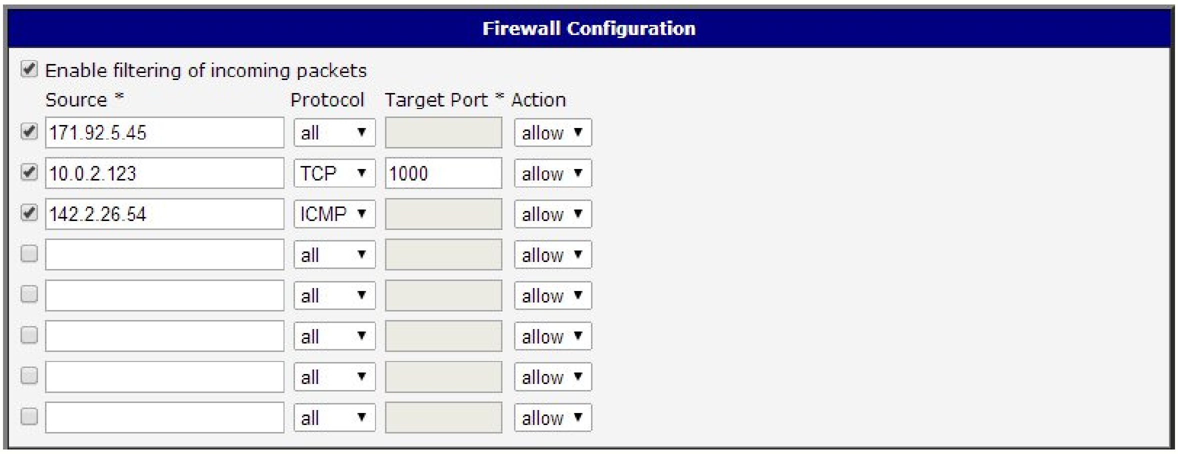


Figure 26: Topology of example firewall configuration



Firewall Configuration

☑ Enable filtering of incoming packets

	Source *	Protocol	Target Port *	Action
☑	171.92.5.45	all		allow
☑	10.0.2.123	TCP	1000	allow
☑	142.2.26.54	ICMP		allow
□		all		allow
□		all		allow
□		all		allow
□		all		allow
□		all		allow

Figure 27: Example firewall configuration

4.8 NAT Configuration

To enter the Network Address Translation configuration, select the *NAT* menu item. NAT (Network address Translation / Port address Translation - PAT) is a method of adjusting the network traffic through the router default transcript and/or destination IP addresses often change the number of TCP/UDP port for walk-through IP packets. The window contains sixteen entries for the definition of NAT rules.

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

Table 30: NAT configuration

If necessary, you can set more than sixteen NAT rules – insert them into start up script (*Startup Script* item in the *Configuration* section) by typing the following:

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

Concrete IP address [IPADDR] and ports numbers [PORT_PUBLIC] and [PORT_PRIVATE] are filled up into square bracket.

The following items are used to set the routing of all incoming traffic from the PPP to the connected computer.

Item	Description
Send all remaining incoming packets to default server	By checking this item and setting the Default Server item it is possible to put the router into the mode in which all incoming data from GPRS will be routed to the computer with the defined IP address.
Default Server IP Address	Send all incoming packets to this IP addresses.

Table 31: Configuration of send all incoming packets

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

⚠ Attention! *Enable remote HTTP access on port* activates **the redirect from HTTP to HTTPS protocol only**. Router doesn't allow unsecured HTTP protocol to access the web configuration. To access the web configuration, always check the *Enable remote HTTPS access on port* item. Never enable the HTTP item only to access the web configuration from the Internet (configuration would not be accessible from the internet). Always check the HTTPS item or HTTPS and HTTP items together (to set the redirect from HTTP).

Item	Description
Enable remote HTTP access on port	This option **sets the redirect** from HTTP to HTTPS **only** (disabled in default configuration).
Enable remote HTTPS access on port	If this item field and port number is filled in, then configuration of the router over web interface is possible (disabled in default configuration).
Enable remote SSH access on port	Choice this item and port number makes it possible to access over SSH (disabled in default configuration).
Enable remote SNMP access on port	Choice this item and port number makes it possible to access to SNMP agent (disabled in default configuration).
Masquerade outgoing packets	Choice Masquerade (alternative name for the NAT system) item option turns the system address translation NAT.

Table 32: Remote access configuration

Example 1: Configuration with one connection equipment on the router.

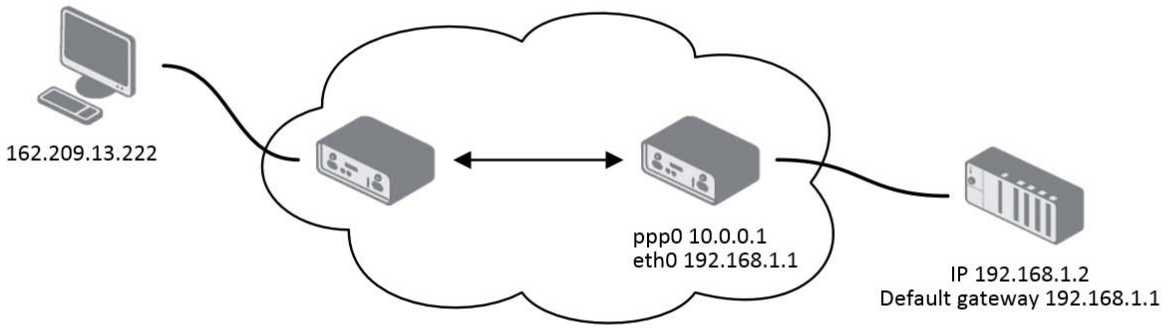
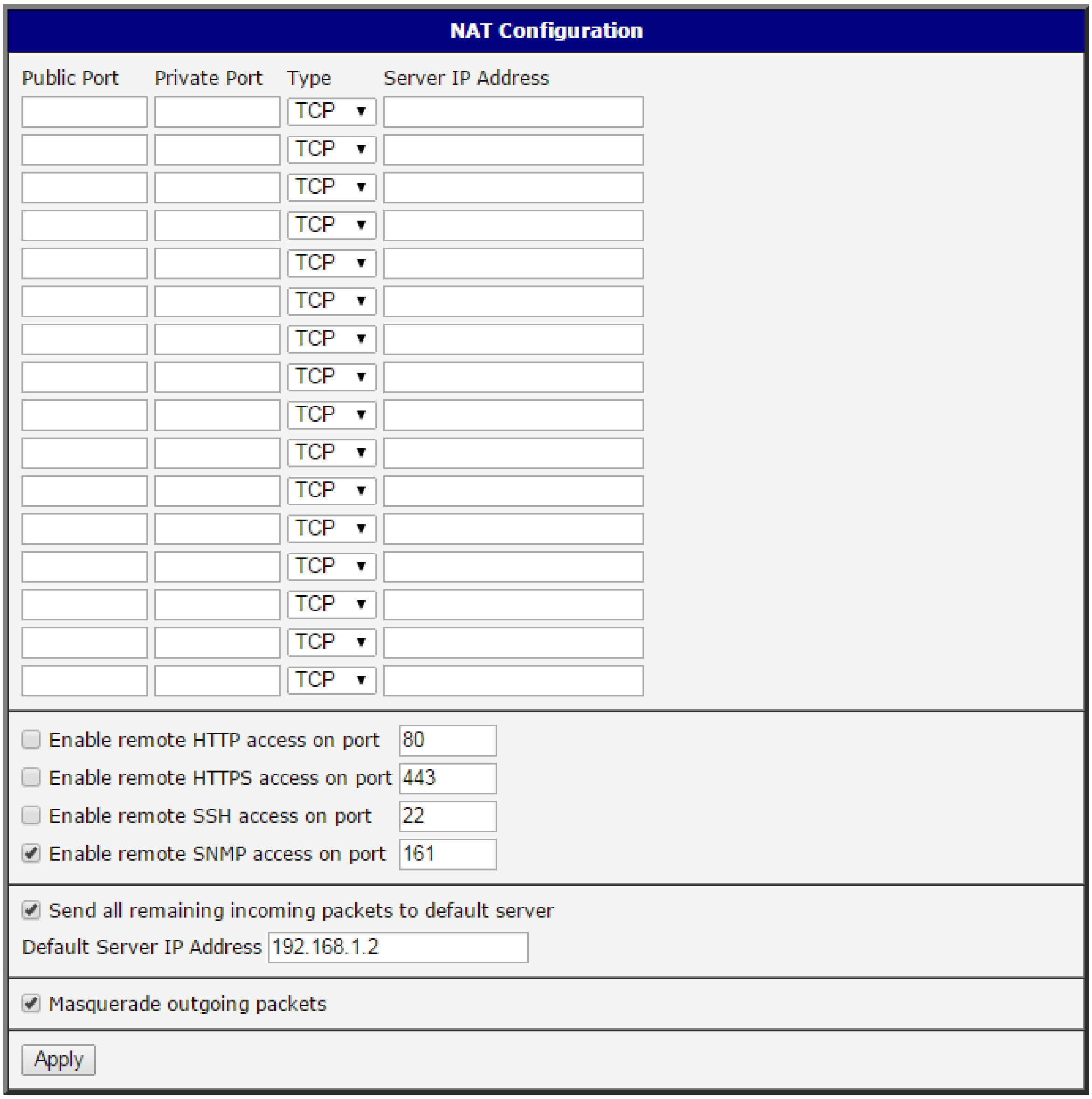


Figure 28: Example 1 – Topology of NAT configuration



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 ▾	

☐ Enable remote HTTP access on port 80

☐ Enable remote HTTPS access on port 443

☐ Enable remote SSH access on port 22

☑ Enable remote SNMP access on port 161

☑ Send all remaining incoming packets to default server

Default Server IP Address 192.168.1.2

☑ Masquerade outgoing packets

Figure 29: Example 1 – NAT configuration

In these configurations it is important to have marked choice of *Send all remaining incoming packets it default server*, IP address in this case is the address of the device behind the router. Connected equipment behind the router must have set *Default Gateway* on the router. Connected device replies, while PING on IP address of SIM card.

Example 2: Configuration with more connected equipment.

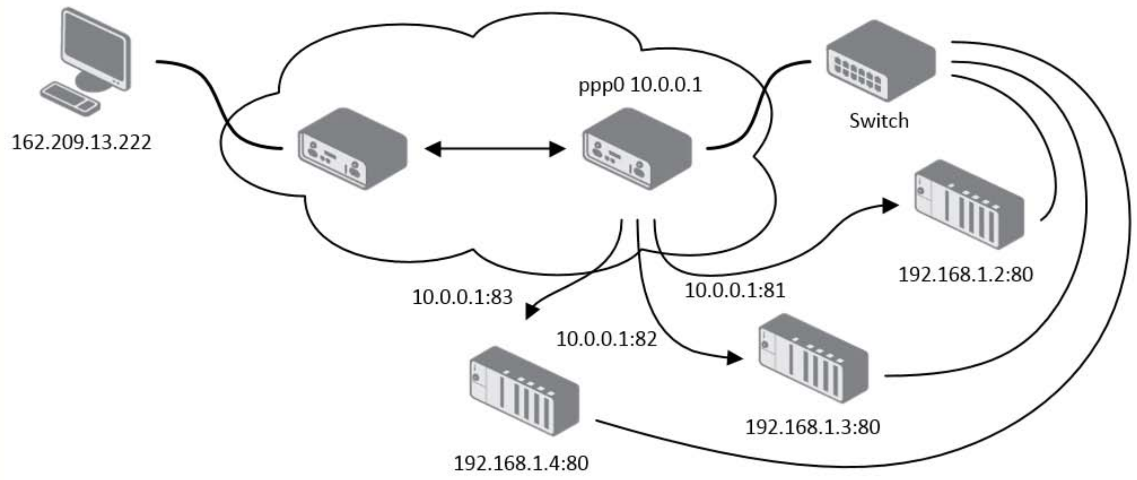
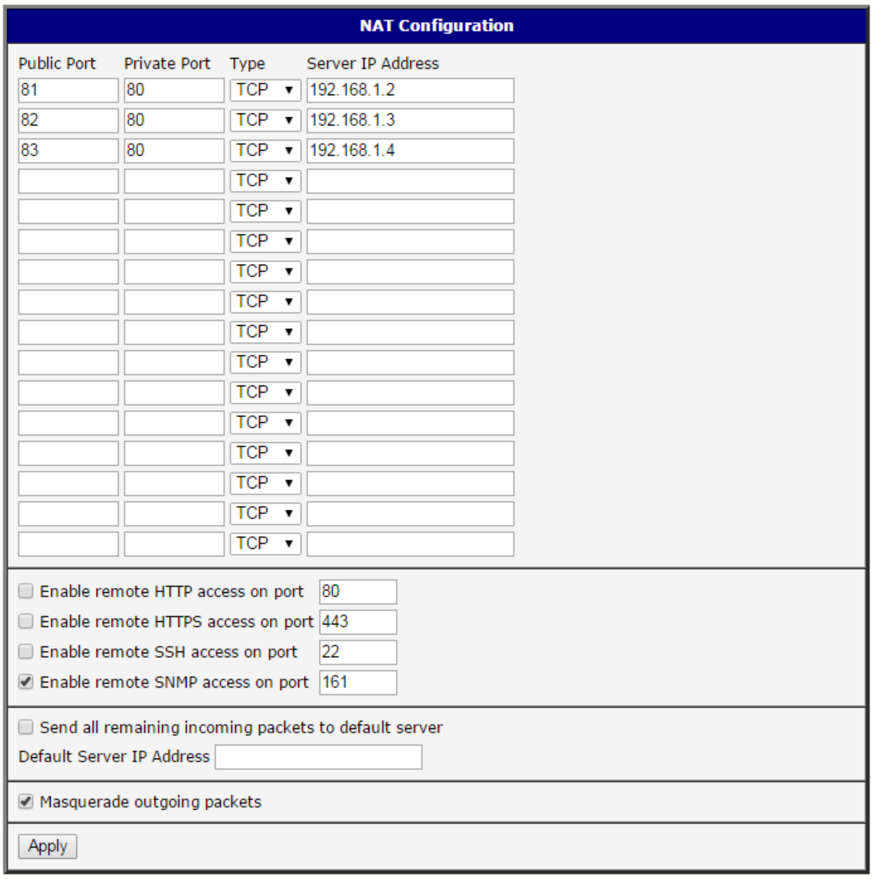


Figure 30: Example 2 – topology of NAT configuration



NAT Configuration

Public Port	Private Port	Type	Server IP Address
81	80	TCP ▾	192.168.1.2
82	80	TCP ▾	192.168.1.3
83	80	TCP ▾	192.168.1.4
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	

☐ Enable remote HTTP access on port 80
☐ Enable remote HTTPS access on port 443
☐ Enable remote SSH access on port 22
☑ Enable remote SNMP access on port 161

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

☑ Masquerade outgoing packets

Figure 31: Example 2 – NAT configuration

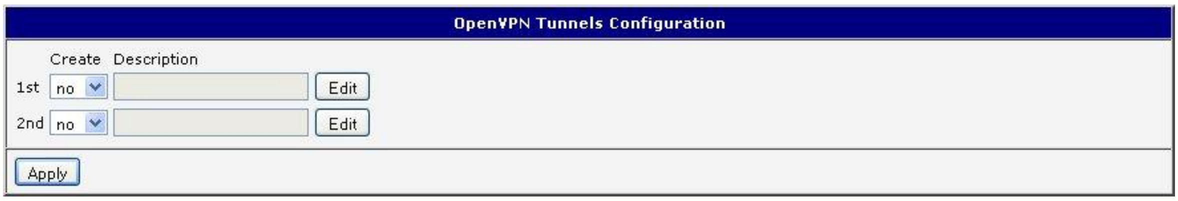
In this example there is more equipment connected behind the router, using a Switch. Every device connected behind the router has its own IP address and this is the address to fill in the *Server IP Address* field in the NAT configuration. These devices are all communicating on the port 80, but you can set the Port Forwarding in the NAT configuration – see Figure 31 – *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 – there is neither 80 port in Public Port list defined nor you have 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 of connection will lead to failure.

4.9 OpenVPN Tunnel Configuration

OpenVPN tunnel configuration can be called up by option *OpenVPN* item in the menu. OpenVPN tunnel allows protected connection of two networks LAN to the one which looks like one homogenous. In the *OpenVPN Tunnels Configuration* window are two rows, each row for one configured OpenVPN tunnel.

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

Table 33: Overview OpenVPN tunnels



OpenVPN Tunnels Configuration

	Create	Description	
1st	no		Edit
2nd	no		Edit

Apply

Figure 32: OpenVPN tunnels configuration

Item	Description
Description	Description (or name) of tunnel
Protocol	Communication protocol: • **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

Continued on next page

Continued from previous page

Item	Description
UDP/TCP port	Port of the relevant protocol (UDP or TCP)
Remote IP Address	IP address of opposite tunnel side (domain name can be used)
Remote Subnet	IP address of a network behind opposite tunnel side
Remote Subnet Mask	Subnet mask of a network behind opposite tunnel side
Redirect Gateway	Allows to redirect all traffic on Ethernet
Local Interface IP Address	Defines the IP address of a local interface
Remote Interface IP Address	Defines the IP address of the interface of opposite tunnel side
Ping Interval	Defines the time interval after which sends a message to opposite side of tunnel for checking the existence of the tunnel.
Ping Timeout	Defines the time interval during which the router waits for a message sent by the opposite side. For proper verification of OpenVPN tunnel, *Ping Timeout* must be greater than *Ping Interval*.
Renegotiate Interval	Sets renegotiate period (reauthorization) of the OpenVPN tunnel. This parameter can be set only when *Authenticate Mode* is set to *username/password* or *X.509 certificate*. After this time period, router changes the tunnel encryption to ensure the continues safety of the tunnel.
Max Fragment Size	Defines the maximum size of a sent packet
Compression	Sent data can be compressed: • **none** – no compression is used • **LZO** – a lossless compression is used (must be set on both sides of the tunnel!)
NAT Rules	Applies NAT rules to the OpenVPN tunnel: • **not applied** – NAT rules are not applied to the OpenVPN tunnel • **applied** – NAT rules are applied to the OpenVPN tunnel

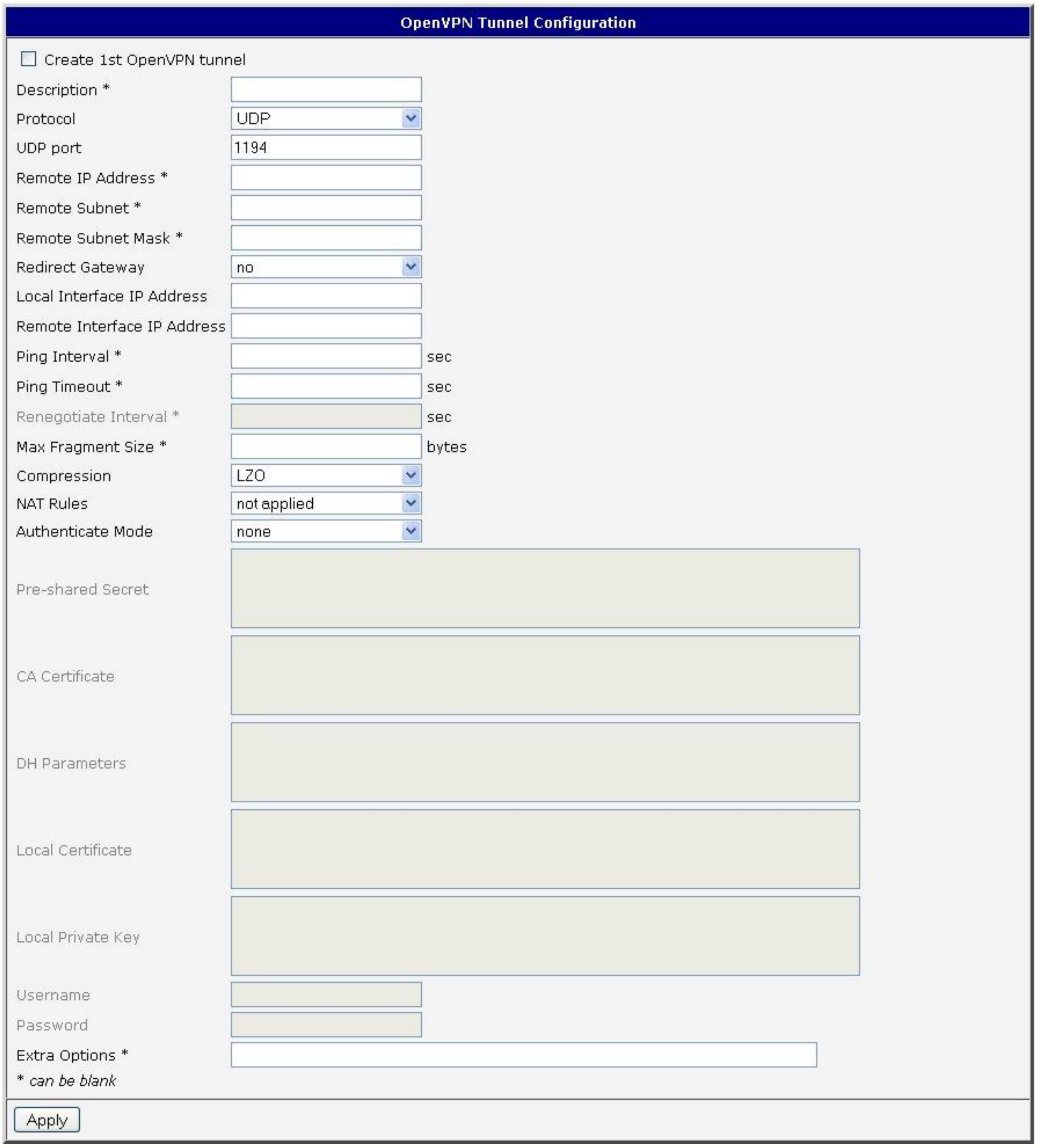
Continued on next page

Continued from previous page

Item	Description
Authenticate Mode	Sets authentication mode: • **none** – no authentication is set • **Pre-shared secret** – sets the shared key for both sides of the tunnel • **Username/password** – enables authentication using *CA Certificate*, *Username* and *Password* • **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	It can be used for X.509 Certificate authentication 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.
Extra Options	Allows to define additional parameters of OpenVPN tunnel such as DHCP options etc. Parameters are introduced by two dashes. For possible parameters see the help in the router via SSH – run the `openvpnd --help` command.

Table 34: OpenVPN tunnels configuration

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



OpenVPN Tunnel Configuration

☐ Create 1st OpenVPN tunnel		
Description *		
Protocol	UDP	
UDP port	1194	
Remote IP Address *		
Remote Subnet *		
Remote Subnet Mask *		
Redirect Gateway	no	
Local Interface IP Address		
Remote Interface IP Address		
Ping Interval *		sec
Ping Timeout *		sec
Renegotiate Interval *		sec
Max Fragment Size *		bytes
Compression	LZO	
NAT Rules	not applied	
Authenticate Mode	none	
Pre-shared Secret		
CA Certificate		
DH Parameters		
Local Certificate		
Local Private Key		
Username		
Password		
Extra Options *		

* *can be blank*

Figure 33: OpenVPN tunnel configuration

Example of the OpenVPN tunnel configuration:

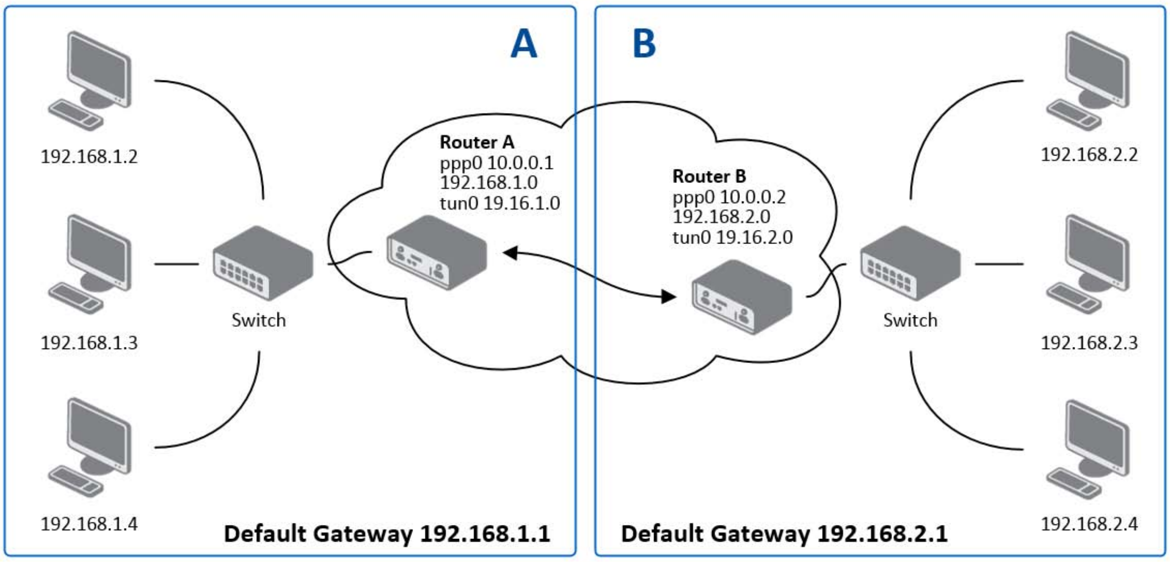


Figure 34: Topology of example OpenVPN configuration

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 35: Example OpenVPN configuration

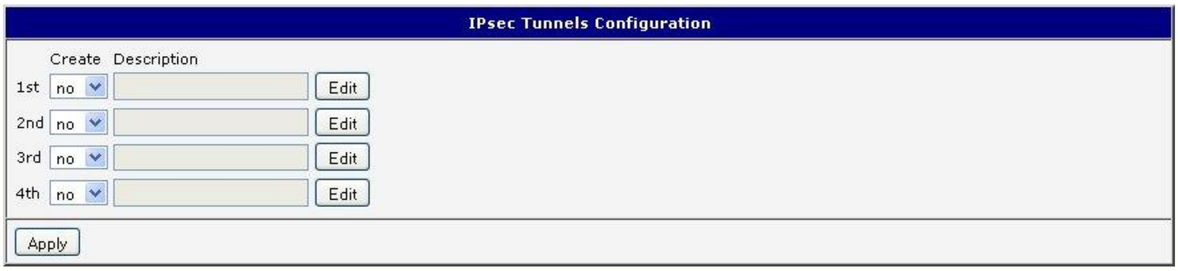
Examples of different options for configuration and authentication of OpenVPN tunnel can be found in the application note *OpenVPN Tunnel* [5].

4.10 IPsec Tunnel Configuration

IPsec tunnel configuration can be called up by option *IPsec* item in the menu. IPsec tunnel allows protected (encrypted) connection of two networks LAN to the one which looks like one homogenous. In the *IPsec Tunnels Configuration* window are four rows, each row for one configured one IPsec tunnel.

Item	Description
Create	This item enables the individual tunnels.
Description	The name of the tunnel specified in the configuration of the tunnel.
Edit	Configuration IPsec tunnel.

Table 36: Overview IPsec tunnels


IPsec Tunnels Configuration

	Create	Description	
1st	no		Edit
2nd	no		Edit
3rd	no		Edit
4th	no		Edit

Figure 35: IPsec tunnels configuration

Item	Description
Description	Name (description) of the tunnel
Remote IP Address	IP address of remote side of the tunnel. Domain name possible.
Remote ID	Identifier (ID) of remote side of the tunnel. It consists of two parts: *hostname* and *domain-name* (more information under the table).
Remote Subnet	IP address of a network behind remote side of the tunnel
Remote Subnet Mask	Subnet mask of a network behind remote side of the tunnel
Remote Protocol/Port	Specifies Protocol/Port of remote side of the tunnel. The general form is *protocol/port*, 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.
Local ID	Identifier (ID) of local side of the tunnel. It consists of two parts: *hostname* and *domain-name* (more information under the table).
Local Subnet	IP address of a local network
Local Subnet Mask	Subnet mask of a local network

Continued on next page

Continued from previous page

Item	Description
Local Protocol/Port	Specifies Procokol/Port of a local network. The general form is *protocol*/*port*, 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 (the method of encapsulation) – choose *tunnel* (entire IP datagram is encapsulated) or *transport* (only IP header).
NAT traversal	If address translation is used between two end points of the tunnel, it needs to enable *NAT Traversal*.
IKE Mode	Defines mode for establishing connection (*main* or *aggressive*). If the aggressive mode is selected, establishing of IPsec tunnel will be faster, but encryption will set permanently on 3DES-MD5. **We recommend not to use *aggressive* mode due to a lower security!**
IKE Algorithm	Way of algorithm selection: • **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: • **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
PFS DH Group	Diffie-Hellman group number (see *IKE DH Group*)
Key Lifetime	Lifetime key data part of tunnel. The minimum value of this parameter is 60 s. The maximum value is 86400 s.

Continued on next page

Continued from previous page

Item	Description
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 should attempt to negotiate a replacement begin. Maximum value must be less than half of IKE and Key Lifetime parameters.
Rekey Fuzz	Percentage extension of Rekay 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	Using this parameter can be set authentication: • **Pre-shared key** – sets the 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, for example secure parameters etc.

Table 37: IPsec tunnel 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. As certificate it is possible to use only certificate which has start and stop tag certificate.

Random time, the new keys are re-exchanged after, is defined this way:

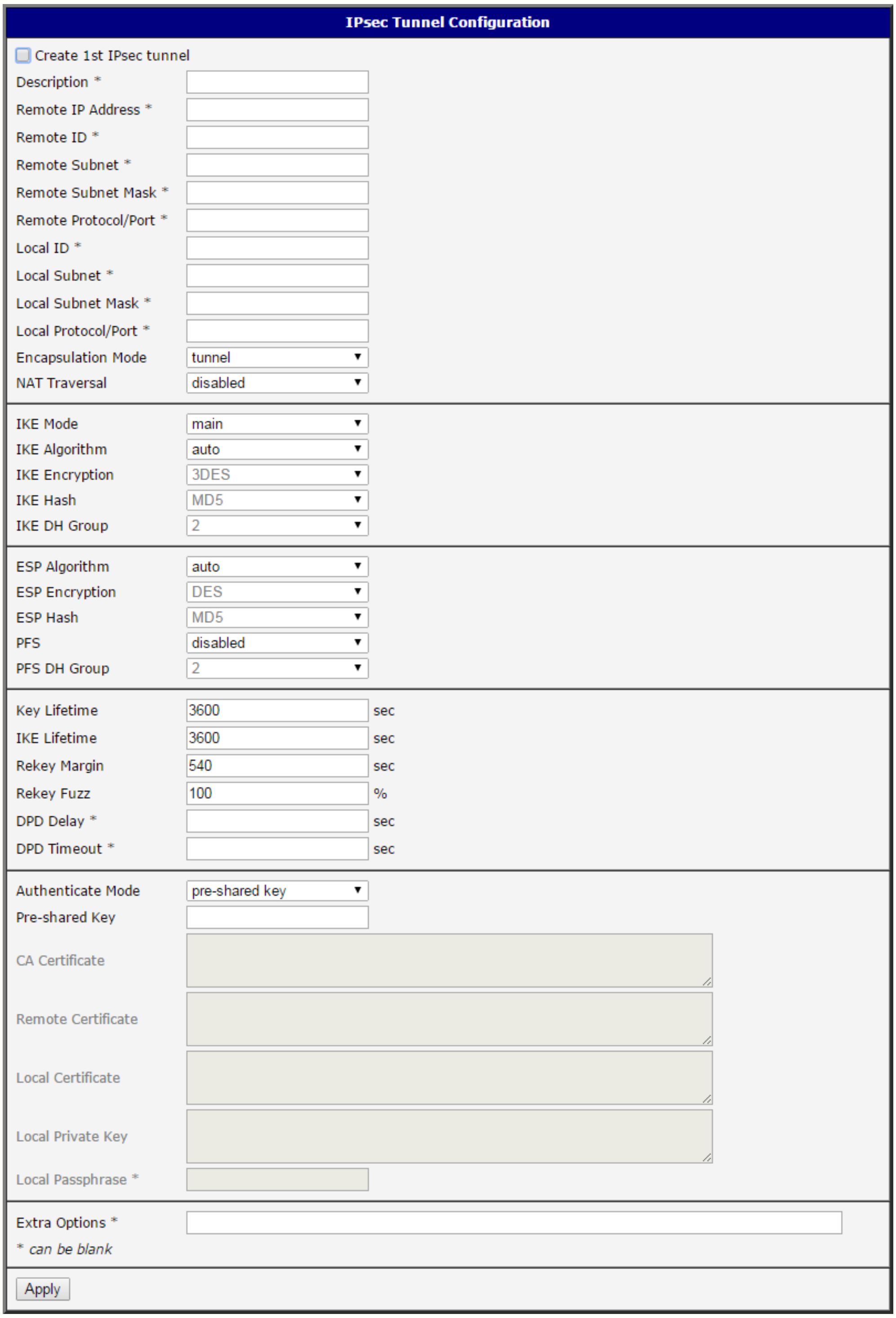
*Lifetime - (Rekey margin + random value in range (from 0 to Rekey margin * Rekey Fuzz/100))*

By default, the repeated exchange of keys held in the time range:

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

When setting the times for key exchange is recommended to leave the default setting in which tunnel has guaranteed security. When set higher time, tunnel has smaller operating costs and smaller the safety. Conversely, reducing the time, tunnel has higher operating costs and higher safety of the tunnel.

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



IPsec Tunnel Configuration

□ Create 1st IPsec tunnel

Description *		
Remote IP Address *		
Remote ID *		
Remote Subnet *		
Remote Subnet Mask *		
Remote Protocol/Port *		
Local ID *		
Local Subnet *		
Local Subnet Mask *		
Local Protocol/Port *		
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 *		sec
DPD Timeout *		sec
Authenticate Mode	pre-shared key	
Pre-shared Key		
CA Certificate		
Remote Certificate		
Local Certificate		
Local Private Key		
Local Passphrase *		
Extra Options *		

** can be blank*

Figure 36: IPsec tunnels configuration

Example of the IPSec Tunnel configuration:

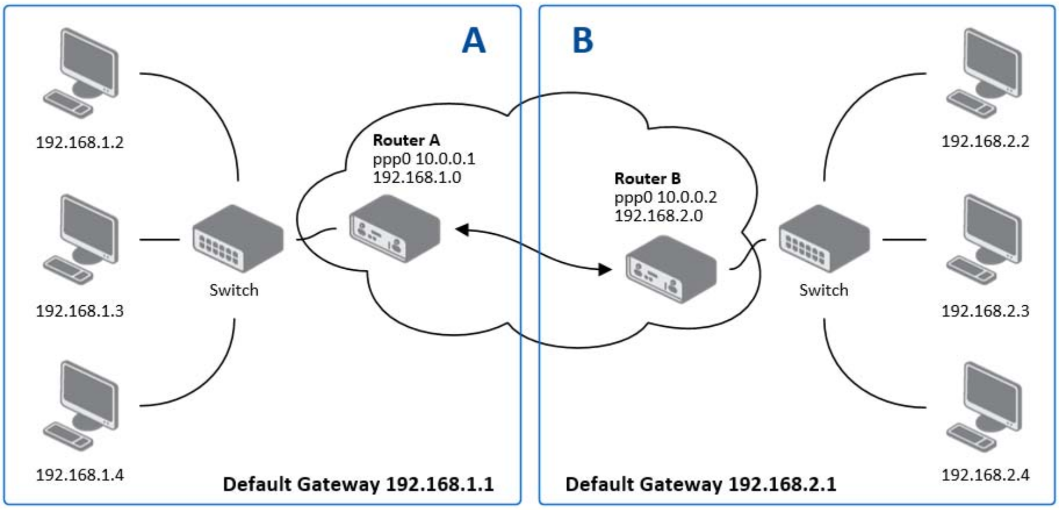


Figure 37: Topology of example IPsec configuration

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 38: Example IPsec configuration

Examples of different options for configuration and authentication of IPsec tunnel can be found in the application note *IPsec Tunnel* [6].

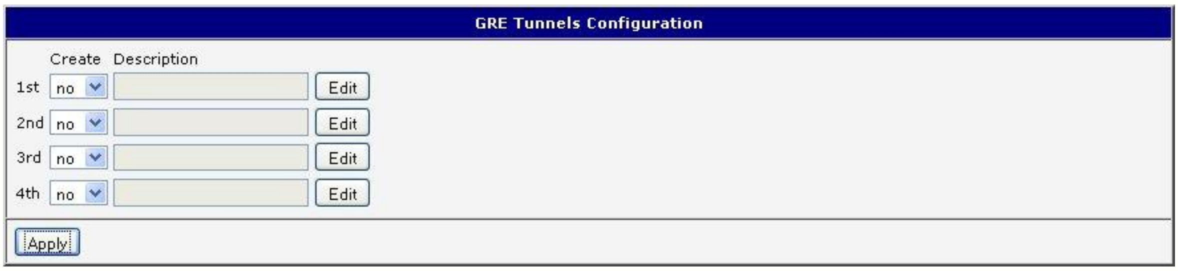
4.11 GRE Tunnels Configuration

GRE is an unencrypted protocol.

To enter the GRE tunnels configuration, select the *GRE* menu item. The GRE tunnel is used for connection of two networks to one that appears as one homogenous. It is possible to configure up to four GRE tunnels. In the *GRE Tunnels Configuration* window are four rows, each row for one configured GRE tunnel.

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 39: Overview GRE tunnels



GRE Tunnels Configuration

	Create	Description	
1st	no		Edit
2nd	no		Edit
3rd	no		Edit
4th	no		Edit

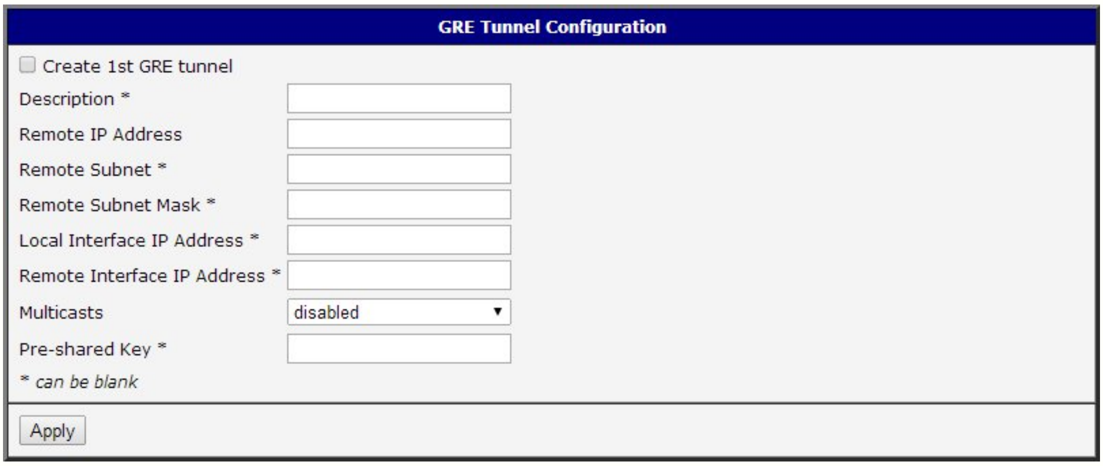
Figure 38: GRE tunnels configuration

Item	Description
Description	Description of tunnel.
Remote IP Address	IP address of 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
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
Multicasts	Enables/disables multicast: • **disabled** – multicast disabled • **enabled** – multicast enabled
Pre-shared Key	An optional value that defines the 32 bit shared key in numeric format, through which the filtered data through the tunnel. This key must be defined on both routers as same, otherwise the router will drop received packets. Using this key, the data do not provide a tunnel through.

Table 40: GRE tunnel configuration

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

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



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 39: GRE tunnel configuration

Example of the GRE Tunnel configuration:

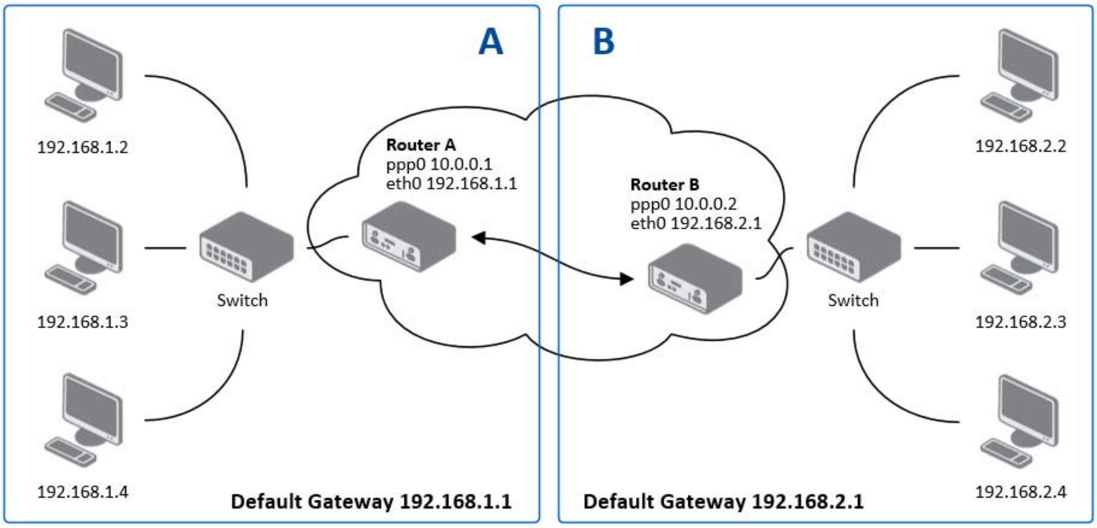


Figure 40: Topology of GRE tunnel configuration

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 41: Example GRE tunnel configuration

Examples of different options for configuration of GRE tunnel can be found in the application note *GRE Tunnel* [7].

4.12 L2TP Tunnel Configuration

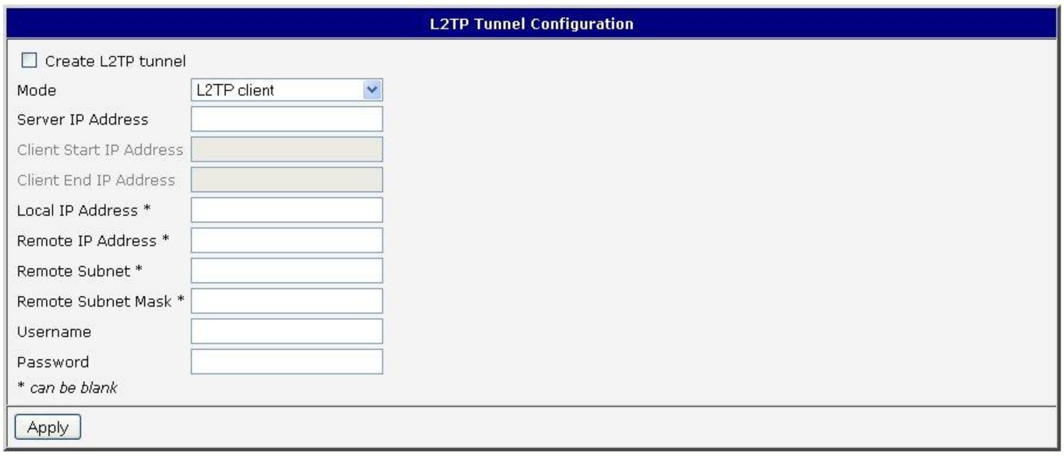
L2TP is an unencrypted protocol.

To enter the L2TP tunnels configuration, select the L2TP menu item. L2TP tunnel allows protected connection by password of two networks LAN to the one which it looks like one homogenous. The tunnels are active after selecting Create L2TP tunnel.

Item	Description
Mode	L2TP tunnel mode on the router side: • **L2TP server –** in the case of a server must be defined IP address range offered by the server • **L2TP client** – in case of client must be defined 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 42: 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*

Figure 41: L2TP tunnel configuration

Example of the L2TP Tunnel configuration:

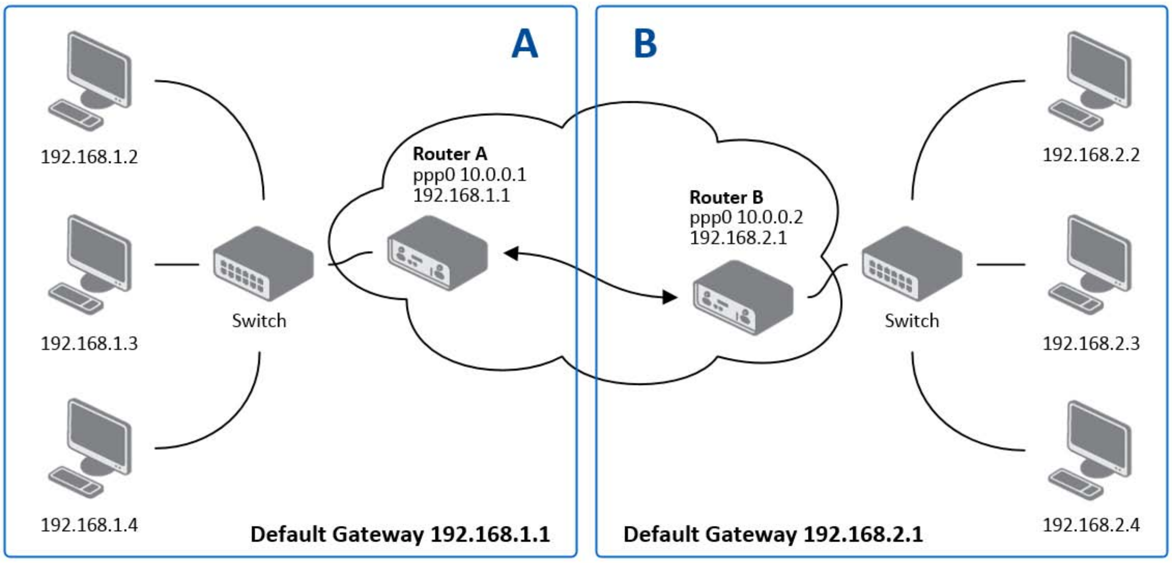


Figure 42: Topology of example L2TP tunnel configuration

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 43: Example L2TP tunel configuration

4.13 PPTP Tunnel Configuration

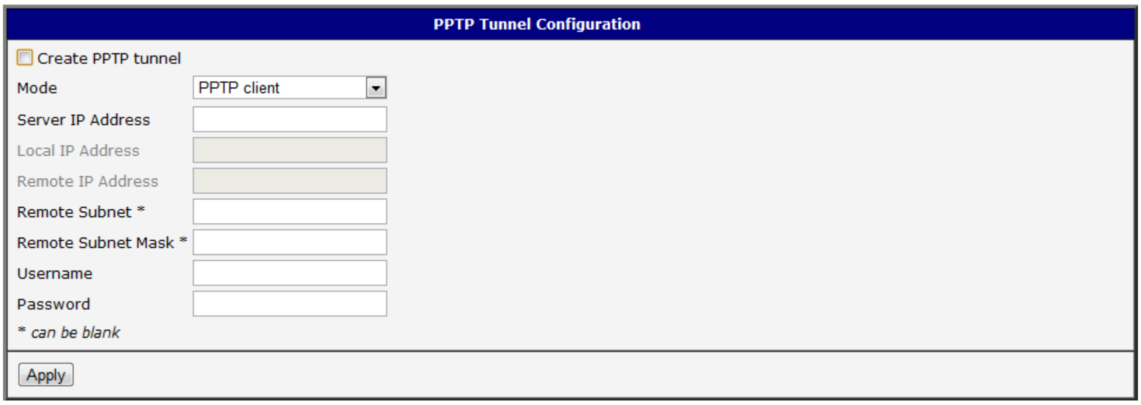
PPTP is an unencrypted protocol.

To enter the PPTP tunnels configuration, select the *PPTP* menu item. PPTP tunnel allows protected connection by password of two networks LAN to the one which it looks like one homogenous. It is a similar method of VPN execution as L2TP. The tunnels are active after selecting *Create PPTP tunnel*.

Item	Description
Mode	PPTP tunnel mode on the router side: • **PPTP server** – in the case of a server must be defined IP address range offered by the server • **PPTP client** – in case of client must be defined the IP address of the server
Server IP Address	IP address of 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 login to PPTP tunnel
Password	Password for login to PPTP tunnel

Table 44: PPTP tunnel configuration

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



PPTP Tunnel Configuration

☐ Create PPTP tunnel

Mode	PPTP client
Server IP Address	
Local IP Address	
Remote IP Address	
Remote Subnet *	
Remote Subnet Mask *	
Username	
Password	

* can be blank

Figure 43: PPTP tunnel configuration

Firmware also supports PPTP passthrough, which means that it is possible to create a tunnel through router.

Example of the PPTP Tunnel configuration:

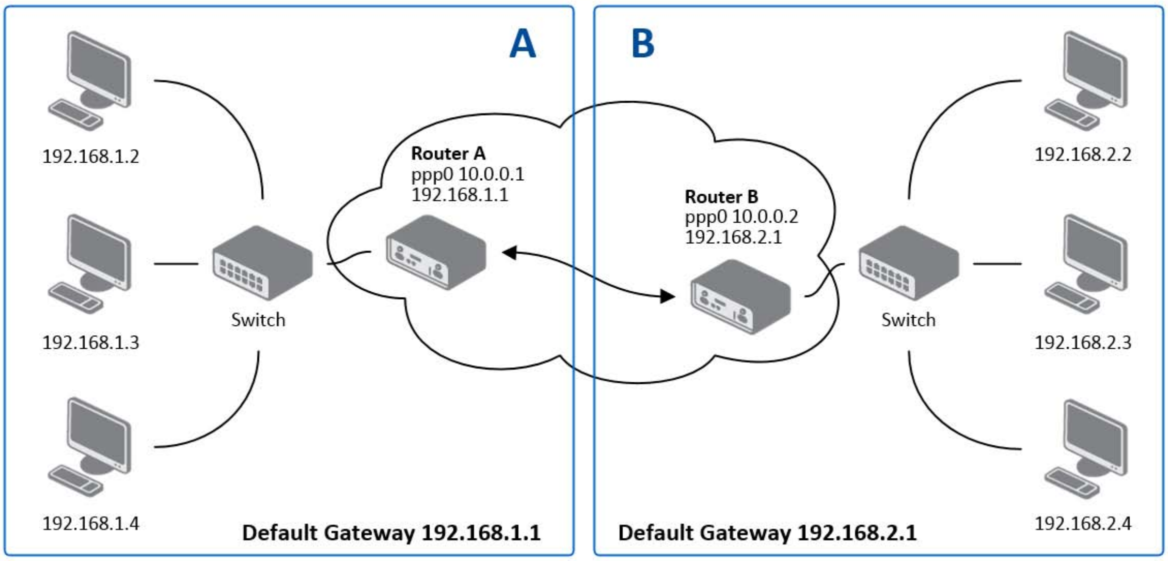


Figure 44: Topology of example PPTP tunnel configuration

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 45: Example PPTP tunel configuration

4.14 DynDNS Client Configuration

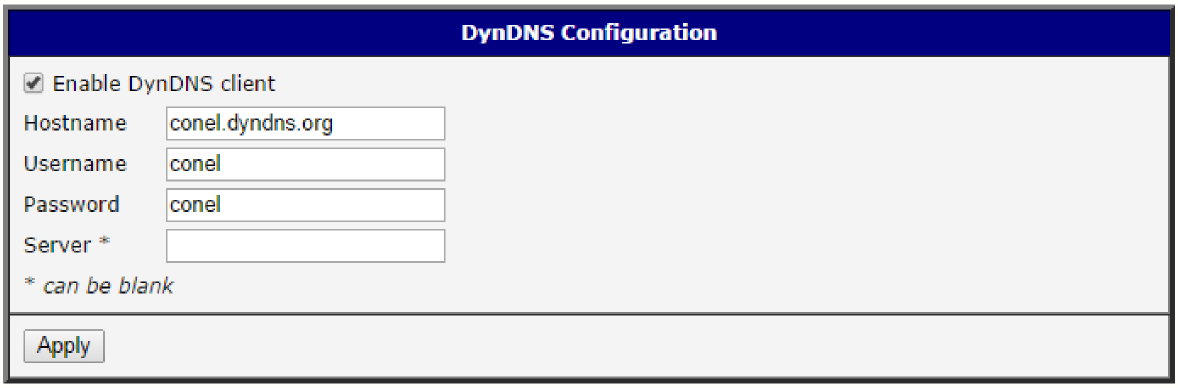
With the DynDNS service you can access the router remotely using an easy to remember custom hostname. This client monitors the router's IP address and update it whenever it changes. To make DynDNS work it is necessary to have a public IP address (static or dynamic) and an active account at www.dyndns.org (Remote Access service).

DynDNS client Configuration is accessible in the *DynDNS* item in the menu. There has to be registered custom domain (third-level) and account information defined in the configuration form.

Item	Description
Hostname	Third order domain registered on server www.dyndns.org
Username	Username for login to DynDNS server
Password	Password for login to DynDNS server
Server	If you want to use another DynDNS service than www.dyndns.org, then enter the update server service to this item. If this item is left blank, it uses the default server members.dyndns.org.

Table 46: DynDNS configuration

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



DynDNS Configuration

☑ Enable DynDNS client

Hostname	conel.dyndns.org
Username	conel
Password	conel
Server *	

* can be blank

Figure 45: Example of DynDNS configuration

To access the router's configuration remotely it is neccessary to enable this in the NAT configuration (bottom part of the form), see chapter 4.8.

4.15 NTP Client Configuration

NTP client Configuration can be called up by option *NTP* item in the menu. NTP (Network Time Protocol) allows set the exact time to the router from the servers, which provide the exact time on the network.

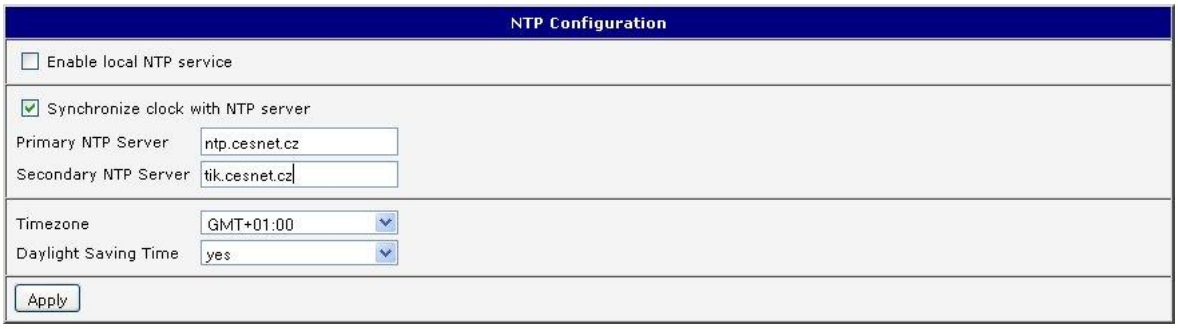
By parameter *Enable local NTP service* router is set to a mode in which it operates as an NTP server for other devices in the LAN behind the router.

By parameter *Enable local NTP service* it is possible to set the router in mode, that it can serve as NTP server for other devices.

Item	Description
Primary NTP Server Address	IP or domain address primary NTP server.
Secondary NTP Server Address	IP or domain address secondary NTP server.
Timezone	By this parameter it is possible to set the time zone of the router
Daylight Saving Time	Using this parameter can be defined time shift: • **No** – time shift is disabled • **Yes** – time shift is allowed

Table 47: 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

□ Enable local NTP service

☑ Synchronize clock with NTP server

Primary NTP Server: ntp.cesnet.cz

Secondary NTP Server: tik.cesnet.cz

Timezone: GMT+01:00

Daylight Saving Time: yes

Figure 46: Example of NTP configuration

4.16 SNMP Configuration

To enter the *SNMP configuration* it is possible with SNMP agent v1/v2 or v3 configuration which sends information about the router, eventually about the I/O inputs.

SNMP (Simple Network Management Protocol) provides status information about network elements such as routers or end computers. v1, v2 and v3 are just different versions of the SNMP. In the version v3 the communication is secured (encrypted), except of the notification messages (such as notifications of events – Traps). To enable using of SNMP service, check the *Enable SNMP agent* item.

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

Table 48: SNMP agent configuration

Enabling SNMPv1/v2 is performed using the *Enable SNMPv1/v2 access* item. It is also necessary to define a password for access to the SNMP agent (*Community*). Standard *public* is predefined.

The *Enable SNMPv3 access* item 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 49: SNMPv3 configuration

By choosing *Enable I/O extension* it is possible to monitor binary inputs I/O on the router.

Enabling *Enable M-BUS extension* has no meaning at this time, since v3 routers doesn't allow the installation of the M-BUS port yet.

By choosing *Enable reporting to supervisory system* and enter the *IP Address* and *Period* it is possible to send statistical information to the monitoring system R-SeeNet.

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

Table 50: SNMP configuration (R-SeeNet)

Every monitor value is uniquely identified by the help of number identifier *OID – Object Identifier*. For binary input and output the following range of OID 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)
.1.3.6.1.4.1.30140.2.3.3.0	Binary input BIN1 (values 0,1)

Table 51: Object identifier for binary input and output

All SPECTRE v3 routers also provide information about 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).

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

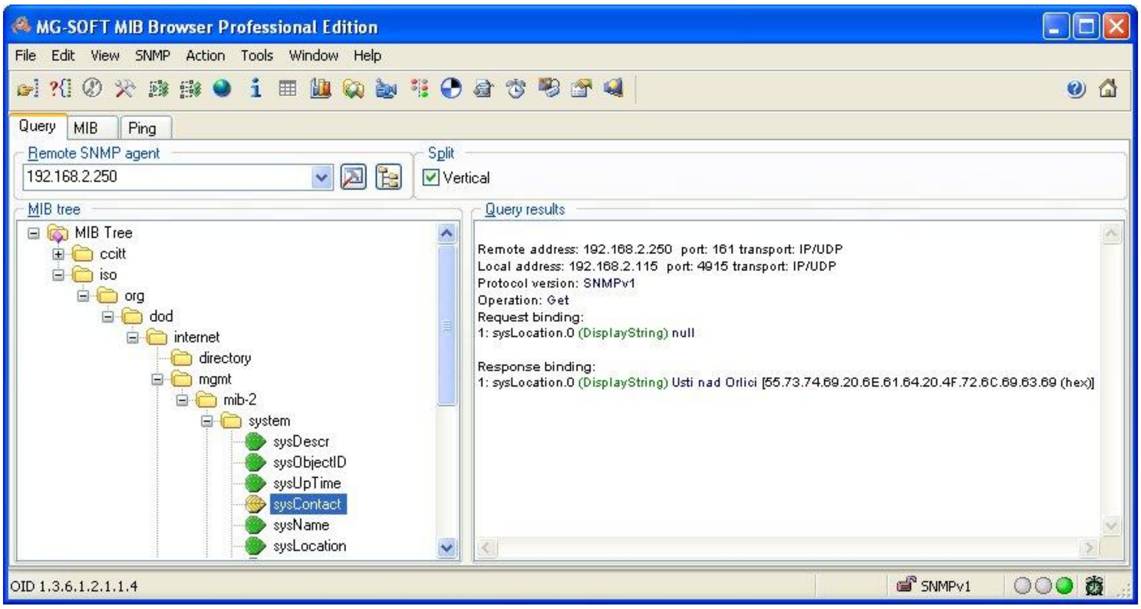
The path to objects is:

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

The path to information about router is:

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

The list of available and supported OIDs and other details can be found in the application note *SNMP Object Identifier* [8].



Remote SNMP agent: 192.168.2.250

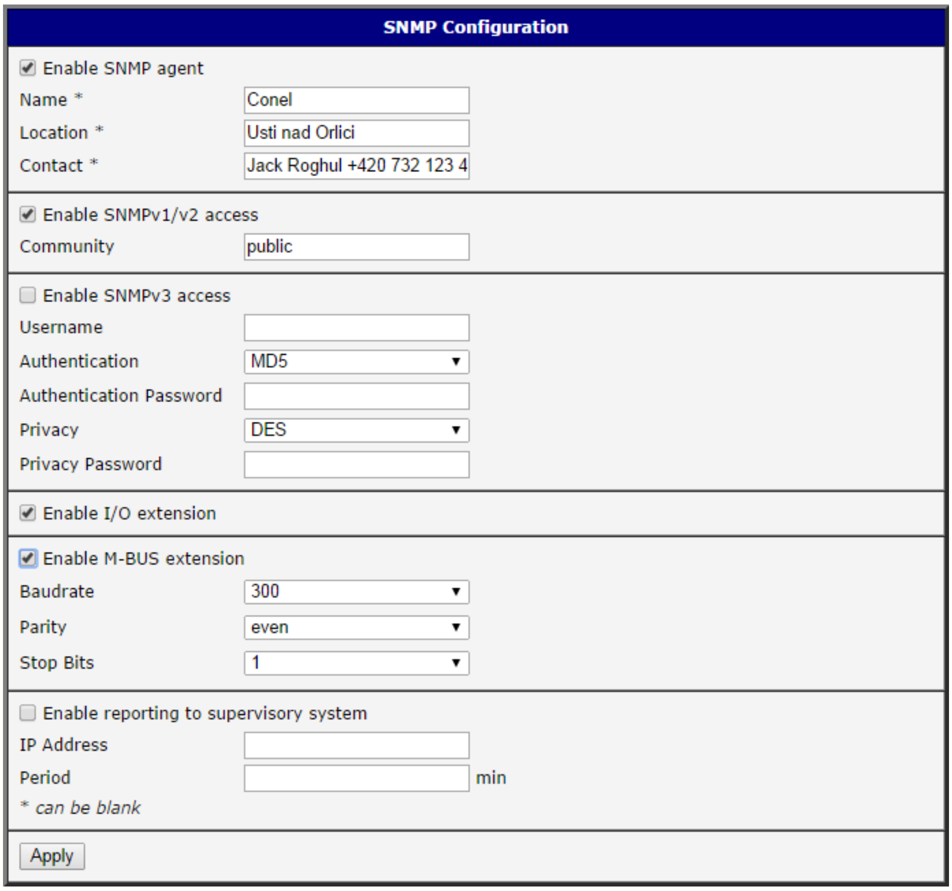
☑ Vertical

MIB Tree
- ccitt
- iso
  - org
    - dod
      - internet
        - directory
        - mgmt
          - mib-2
            - system
              - sysDescr
              - sysObjectID
              - sysUpTime
              - sysContact
              - sysName
              - sysLocation

```
Remote address: 192.168.2.250  port: 161 transport: IP/UDP
Local address: 192.168.2.115  port: 4915 transport: IP/UDP
Protocol version: SNMPv1
Operation: Get
Request binding:
1: sysLocation.0 (DisplayString) null

Response binding:
1: sysLocation.0 (DisplayString) Usti nad Orlici [55.73.74.69.20.6E.61.64.20.4F.72.6C.69.63.69 (hex)]
```

OID 1.3.6.1.2.1.1.4

Figure 47: Example of the MIB browser



SNMP Configuration

☑ Enable SNMP agent	
Name *	Conel
Location *	Usti nad Orlici
Contact *	Jack Roghul +420 732 123 4
☑ Enable SNMPv1/v2 access	
Community	public
☐ Enable SNMPv3 access	
Username	
Authentication	MD5
Authentication Password	
Privacy	DES
Privacy Password	
☑ Enable I/O extension	
☑ Enable M-BUS extension	
Baudrate	300
Parity	even
Stop Bits	1
☐ Enable reporting to supervisory system	
IP Address	
Period	min

* *can be blank*

Figure 48: Example of SNMP configuration

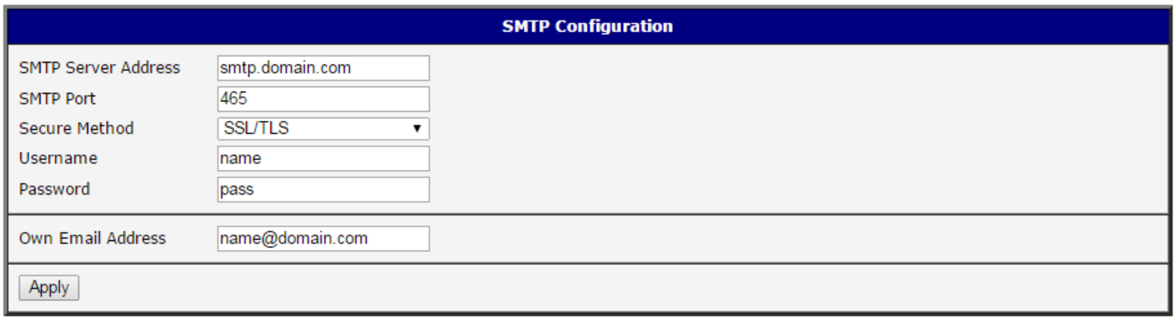
4.17 SMTP Configuration

The item *SMTP* is used for configuring SMTP (Simple Mail Transfer Protocol) client for sending e-mails.

Item	Description
SMTP Server Address	IP or domain address 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 can not contain special characters “ $ & ’ ( ) ; < >
Own E-mail Address	Address of the sender.

Table 52: SMTP client configuration

Mobile operator can block other SMTP servers, then you can use only the SMTP server of operator.



SMTP Configuration

SMTP Server Address	smtp.domain.com
SMTP Port	465
Secure Method	SSL/TLS
Username	name
Password	pass
Own Email Address	name@domain.com

Figure 49: Example of the SMTP client configuration

E-mail can be sent from the Startup script (*Startup Script* item in the *Configuration* section) or via SSH connection. The command *email* is 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.

4.18 SMS Configuration

SMS configuration can be invoked by *SMS* item in the *Configuration* section. Sending of SMS can be defined in various events and states of the router. Sending od SMS can be configured in the first part of the window:

Item	Description
Send SMS on power up	Automatic sending of SMS messages after power up.
Send SMS on connect to mobile network	Automatic sending SMS message after connection to mobile network.
Send SMS on disconnect to mobile network	Automatic sending SMS message after disconnection to mobile network.
Send SMS when datalimit exceeded	Automatic sending SMS message after datalimit exceeded.
Send SMS when binary input on I/O port (BIN0) is active	Automatic sending SMS message after binary input on I/O port (BIN0) is active. Text of message is intended parameter BIN0.
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 will be sent in an SMS.
BIN0 – SMS	SMS text messages when activate the first binary input on the router.

Table 53: Send SMS configuration

In the second part of the window it is possible to set function *Enable remote control via SMS*. After enabling it is possible to control the router by SMS message.

Item	Description
Phone Number 1	This control can be configured for up to three numbers. If is set *Enable remote control via SMS*, all incoming SMS are processed and deleted. In the default settings this parameter is turned on.
Phone Number 2	This control can be configured for up to three numbers. If is set *Enable remote control via SMS*, all incoming SMS are processed and deleted. In the default settings this parameter is turned on.
Phone Number 3	This control can be configured for up to three numbers. If is set *Enable remote control via SMS*, all incoming SMS are processed and deleted. In the default settings this parameter is turned on.

Table 54: Control via SMS configuration

If no phone number is filled in, then it is possible to restart the router with the help of SMS in the form of *reboot* from any phone number. While filling up one, two or three numbers it is possible to control the router with the help of an SMS sent only from these numbers. While filling up sign ∗ it is possible to control the router with the help of an SMS sent from any number.

Control SMS message doesn't change the router's configuration. If the router is switched to offline mode by the SMS message the router will be in this mode up to next restart. This behavior is the same for all control SMS messages.

It is possible to send controls SMS in the form:

SMS	Description
go online sim 1	Switch to SIM1 card
go online sim 2	Switch to SIM2 card
go online	Switch 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 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 55: Control SMS

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

Item	Description
Baudrate	Communication speed on expansion port 1

Table 56: Send SMS on serial PORT1 configuration

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

Item	Description
Baudrate	Communication speed on expansion port 2

Table 57: Send SMS on serial PORT2 configuration

Choosing *Enable AT-SMS protocol on TCP port* and enter the *TCP port* it is possible to send/receive an SMS on the TCP port. SMS messages are sent with the help of standard AT commands.

Item	Description
TCP Port	TCP port the sending/receiving SMS messages will be allowed on.

Table 58: Send SMS on ethernet PORT1 configuration

4.18.1 Sending SMS

After establishing connection with the router via serial interface or Ethernet, it is possible to use AT commands for work with SMS messages.

The following table lists the commands that are supported by Conel routers. For other AT commands *OK* response is always sent. There is no support for complex AT commands, in such a case *ERROR* response is sent by router.

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

Continued on next page

Continued from previous page

AT Command	Description
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
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 59: List of AT commands

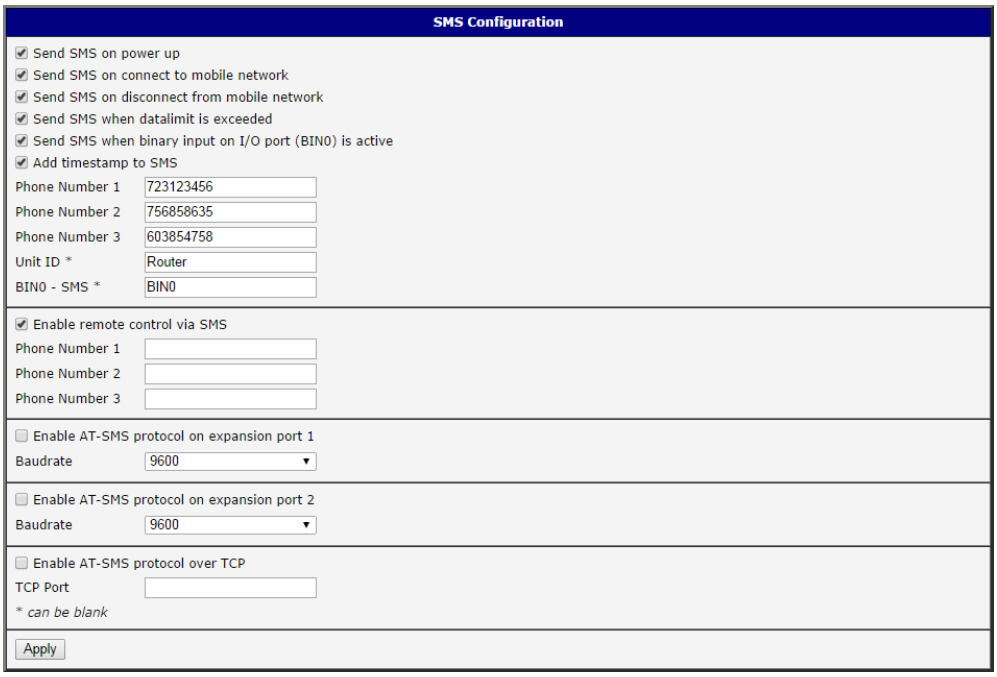
A detailed description and examples of these AT commands can be found in the application note *AT commands* [9].

Example 1: SMS sending configuration.

After powering up the router, at the mentioned the phone number comes SMS in this form:
Router (Unit ID) has been powered up. Signal strength –xx dBm.

After connect to mobile network, at the mentioned phone number comes SMS in this form:
Router (Unit ID) has established connection to mobile network. IP address xxx.xxx.xxx.xxx

After disconnect to mobile network, at the mentioned phone number comes SMS in this form:
Router (Unit ID) has lost connection to mobile network. IP address xxx.xxx.xxx.xxx



SMS Configuration

☑ Send SMS on power up
☑ Send SMS on connect to mobile network
☑ Send SMS on disconnect from mobile network
☑ Send SMS when datalimit is exceeded
☑ Send SMS when binary input on I/O port (BIN0) is active
☑ Add timestamp to SMS

Phone Number 1	723123456
Phone Number 2	756858635
Phone Number 3	603854758
Unit ID *	Router
BIN0 - SMS *	BIN0

☑ Enable remote control via SMS

Phone Number 1	
Phone Number 2	
Phone Number 3	

☐ Enable AT-SMS protocol on expansion port 1
Baudrate 9600 ▾

☐ Enable AT-SMS protocol on expansion port 2
Baudrate 9600 ▾

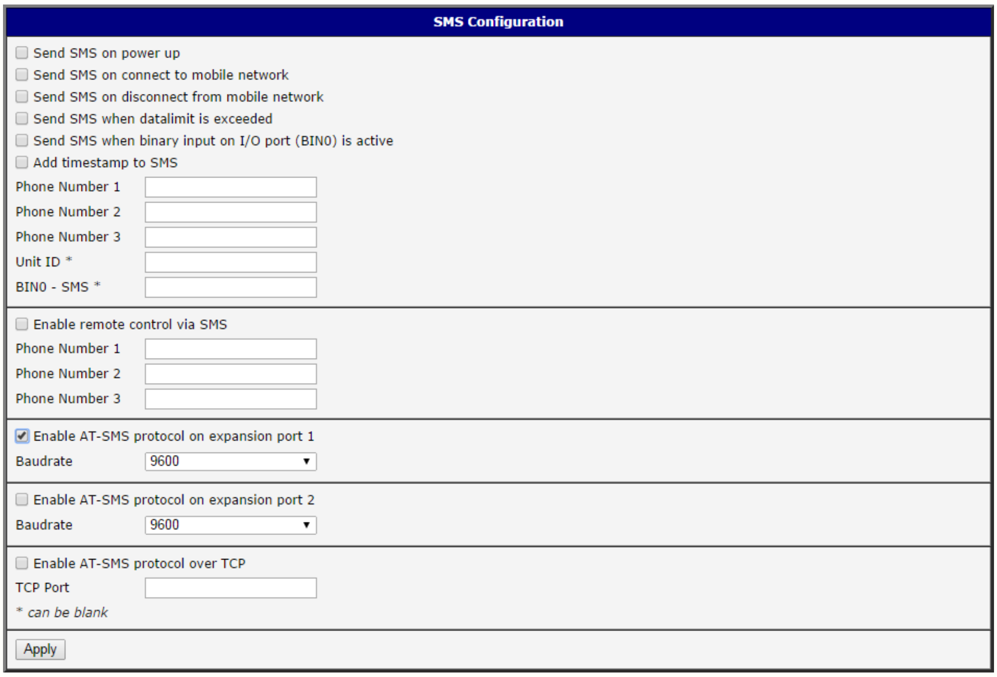
☐ Enable AT-SMS protocol over TCP
TCP Port

** can be blank*

Apply

Figure 50: Example 1 – SMS configuration

Example 2: Configuration of sending SMS via serial interface on the PORT1.



SMS Configuration

☐ Send SMS on power up
☐ Send SMS on connect to mobile network
☐ Send SMS on disconnect from mobile network
☐ Send SMS when datalimit is exceeded
☐ Send SMS when binary input on I/O port (BIN0) is active
☐ Add timestamp to SMS

Phone Number 1	
Phone Number 2	
Phone Number 3	
Unit ID *	
BIN0 - SMS *	

☐ Enable remote control via SMS

Phone Number 1	
Phone Number 2	
Phone Number 3	

☑ Enable AT-SMS protocol on expansion port 1
Baudrate 9600 ▾

☐ Enable AT-SMS protocol on expansion port 2
Baudrate 9600 ▾

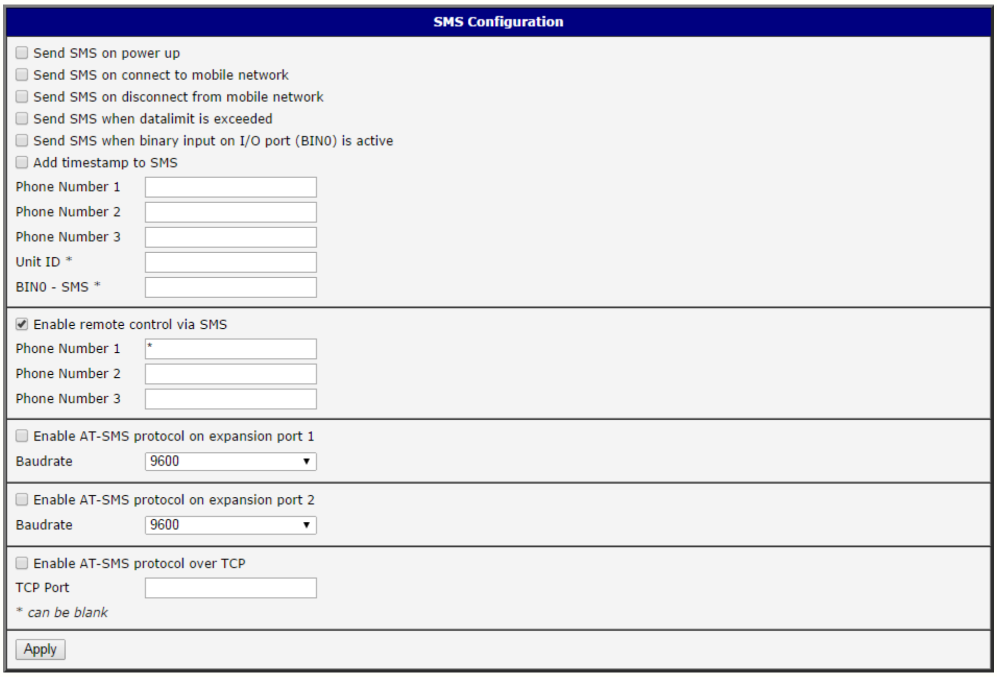
☐ Enable AT-SMS protocol over TCP
TCP Port

** can be blank*

Apply

Figure 51: Example 2 – SMS configuration

Example 3: Configuration of controlling the router via SMS from any phone number.



SMS Configuration

☐ Send SMS on power up
☐ Send SMS on connect to mobile network
☐ Send SMS on disconnect from mobile network
☐ Send SMS when datalimit is exceeded
☐ Send SMS when binary input on I/O port (BIN0) is active
☐ Add timestamp to SMS

Phone Number 1	
Phone Number 2	
Phone Number 3	
Unit ID *	
BIN0 - SMS *	

☑ Enable remote control via SMS

Phone Number 1	*
Phone Number 2	
Phone Number 3	

☐ Enable AT-SMS protocol on expansion port 1

Baudrate: 9600

☐ Enable AT-SMS protocol on expansion port 2

Baudrate: 9600

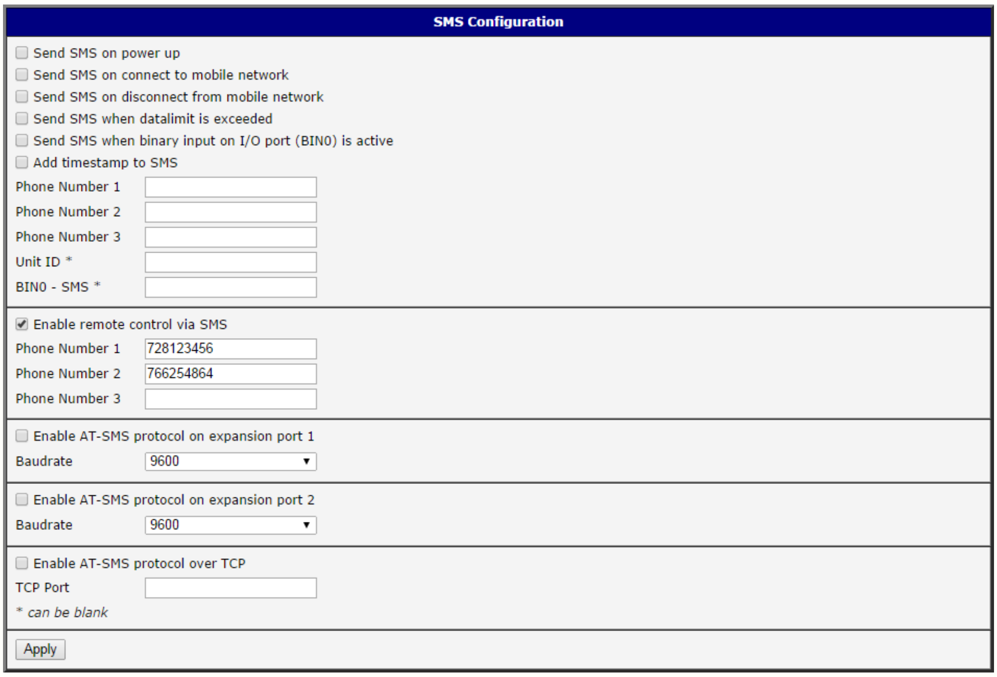
☐ Enable AT-SMS protocol over TCP

TCP Port:

** can be blank*

Figure 52: Example 3 – SMS configuration

Example 4: Configuration of controlling the router via SMS from the two phone numbers.



SMS Configuration

☐ Send SMS on power up
☐ Send SMS on connect to mobile network
☐ Send SMS on disconnect from mobile network
☐ Send SMS when datalimit is exceeded
☐ Send SMS when binary input on I/O port (BIN0) is active
☐ Add timestamp to SMS

Phone Number 1	
Phone Number 2	
Phone Number 3	
Unit ID *	
BIN0 - SMS *	

☑ Enable remote control via SMS

Phone Number 1	728123456
Phone Number 2	766254864
Phone Number 3	

☐ Enable AT-SMS protocol on expansion port 1

Baudrate: 9600

☐ Enable AT-SMS protocol on expansion port 2

Baudrate: 9600

☐ Enable AT-SMS protocol over TCP

TCP Port:

** can be blank*

Figure 53: Example 4 – SMS configuration

4.19 Expansion Port Configuration

Configuration of the expansion port can be done via *Expansion Port 1* or *Expansion Port 2* items in the menu.

- If the version of router is with the **RS232** interface, configuration of the *Expansion Port 1* only is needed (*Expansion Port 2* item is not used).
- With the **RS232-RS485/422** interface present, configuration of RS232 interface is accessible via *Expansion Port 1* item and configuration of RS485 or RS422 via *Expansion Port 2* item.
- In case of **SWITCH** version of router (3x Ethernet, ETH2 interface of the router), the port can be configured in the *LAN* item, *Tertiary LAN* column – see chapter 4.1.

In the upper part of the configuration window, the port can be enabled and type of the connected port is shown in the *Port Type* item. Other items are described in the table:

Item	Description
Baudrate	Applied communication speed.
Data Bits	Number of data bits.
Parity	Control parity bit • **none** – will be sent without parity • **even** – will be sent with even parity • **odd** – will be sent with odd parity
Stop Bits	Number of stop bit.
Split Timeout	Time to rupture reports. If you receive will identify the gap between two characters, which is longer than the parameter value in milliseconds. Then all of the received data compiled and sent the message.
Protocol	Protocol: • **TCP** – communication using a linked protocol TCP • **UDP** – communication using a unlinked protocol UDP

Continued on next page

Continued from previous page

Item	Description
Mode	Mode of connection: • **TCP server** – router will listen to incoming requests about TCP connection • **TCP client** – router will connect to a TCP server on the specified IP address and TCP port
Server Address	In mode TCP client it is necessary to enter the Server IP address.
TCP Port	TCP/UDP port the communication is running on (for both modes).
Inactivity Timeout	Time period after which the TCP/UDP connection is interrupted in case of inactivity

Table 60: Expansion Port configuration – serial interface

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 *Check TCP connection* checked, the check of the connection would be activated.

Item	Description
Keepalive Time	Time, after which it will carry out verification of the connection
Keepalive Interval	Waiting time on answer
Keepalive Probes	Number of tests

Table 61: Expansion Port configuration – *Check TCP connection*

When item *Use CD as indicator of the TCP connection* selected, indication of the TCP connection state using signal CD (DTR on the router) would be activated.

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

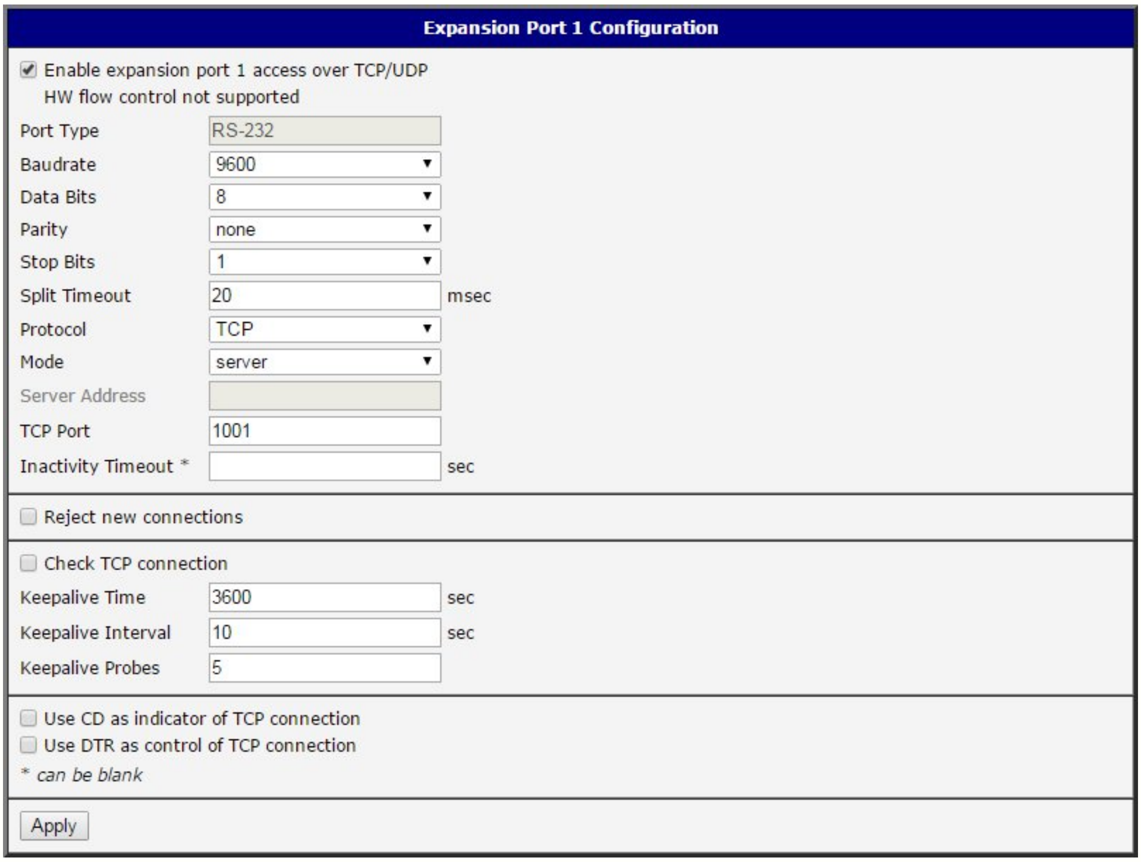
Table 62: CD signal description

When item *Use DTR as control of TCP connection* selected, control of the TCP connection using signal CD (DTR on the router) would be activated.

DTR	Description server	Description client
Active	Router allows TCP connect. establishm.	Router starts TCP connection
Nonactive	Router does not permit TCP con. estab.	Router stops TCP connection

Table 63: 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	RS-232	
Baudrate	9600 ▼	
Data Bits	8 ▼	
Parity	none ▼	
Stop Bits	1 ▼	
Split Timeout	20	msec
Protocol	TCP ▼	
Mode	server ▼	
Server Address		
TCP Port	1001	
Inactivity Timeout *		sec

□ Reject new connections

□ Check TCP connection

Keepalive Time	3600	sec
Keepalive Interval	10	sec
Keepalive Probes	5	

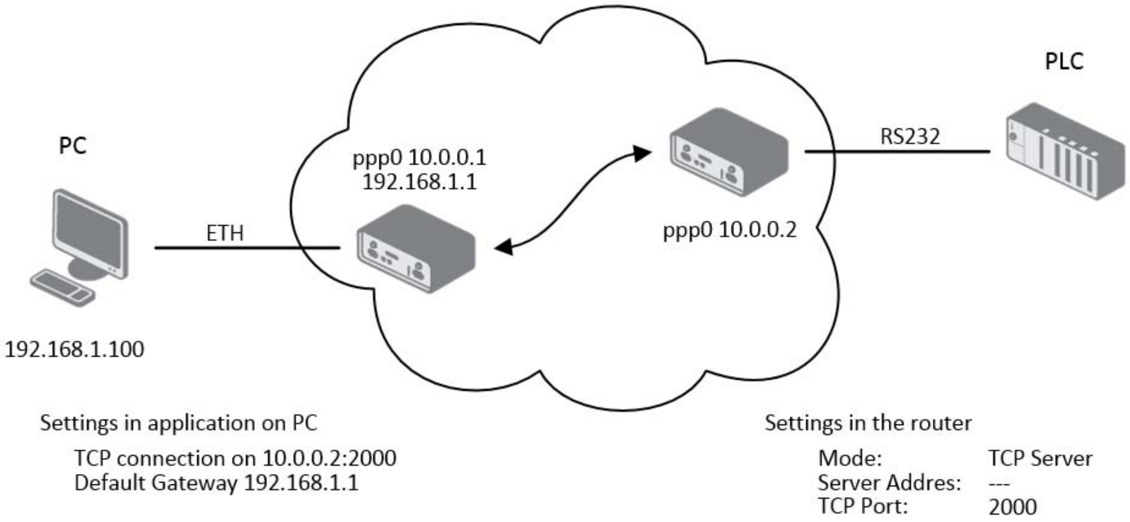
□ Use CD as indicator of TCP connection

□ Use DTR as control of TCP connection

** can be blank*

Figure 54: Expansion port configuration

Examples of the expansion port configuration:



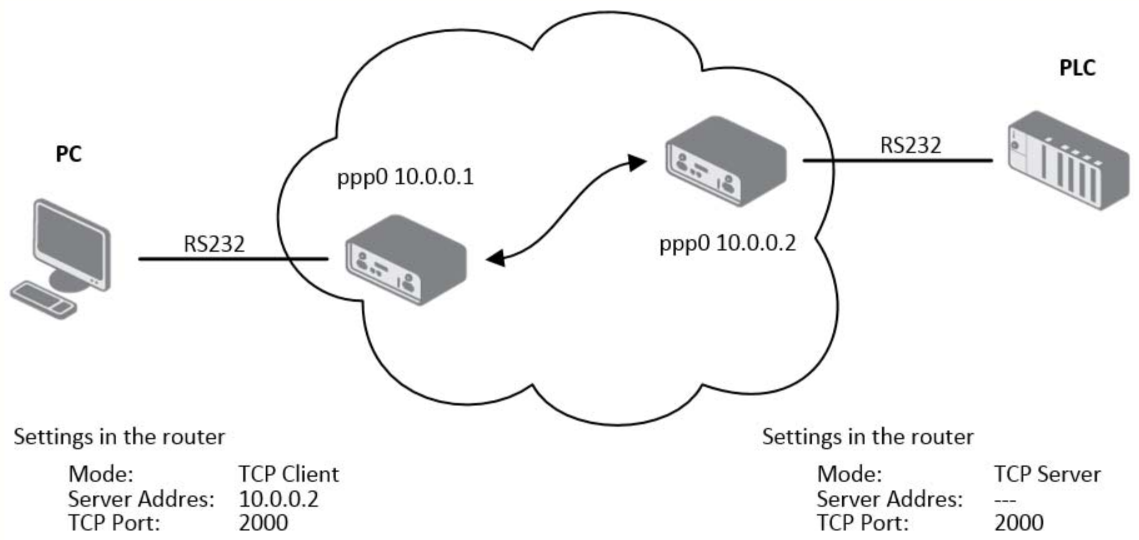
Settings in application on PC

TCP connection on 10.0.0.2:2000
Default Gateway 192.168.1.1

Settings in the router

Mode:	TCP Server
Server Addres:	---
TCP Port:	2000

Figure 55: Example 1 – expansion port configuration



Settings in the router

Mode:	TCP Client
Server Addres:	10.0.0.2
TCP Port:	2000

Settings in the router

Mode:	TCP Server
Server Addres:	---
TCP Port:	2000

Figure 56: Example 2 – expansion port configuration

All v3 routers provide a program called *getty* which allows user to connect to the router via the serial line (router must be fitted with an expansion port RS232!). Getty displays the prompt and after entering the username passes it on *login* program, which asks for a password, verifies it and runs the shell. After logging in, it is possible to manage the system as well as a user is connected via SSH.

4.20 USB Port Configuration

The USB port configuration can be made choosing *USB Port* option in the menu. Configuration can be done, if USB/RS232 converter connected.

Item	Description
Baudrate	Applied communication speed.
Data Bits	Number of data bits.
Parity	Control parity bit: • **none** – will be sent without parity • **even** – will be sent with even parity • **odd** – will be sent with odd parity
Stop Bits	Number of stop bit.
Split Timeout	Time to rupture reports. If you receive will identify the gap between two characters, which is longer than the parameter value in milliseconds. Then all of the received data compiled and sent the message.
Protocol	Communication protocol: • **TCP** – communication using a linked protocol TCP • **UDP** – communication using a unlinked protocol UDP
Mode	Mode of connection: • **TCP server** – router will listen to incoming requests about TCP connection • **TCP client** – router will connect to a TCP server on the specified IP address and TCP port
Server Address	In mode TCP client it is necessary to enter the Server IP address.
TCP Port	In both modes of connection it is necessary to specify the TCP port the router will communicate on.
Inactivity Timeout	Time period after which the TCP/UDP connection is interrupted in case of inactivity

Table 64: USB 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* item is ticked, check of the established TCP connection is activated.

Item	Description
Keepalive Time	Time, after which it will carry out verification of the connection
Keepalive Interval	Waiting time on answer
Keepalive Probes	Number of tests

Table 65: USB PORT configuration 2

When item *Use CD as indicator of the TCP connection* selected, indication of the TCP connection state using signal CD (DTR on the router) would be activated.

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

Table 66: CD signal description

When item *Use DTR as control of TCP connection* selected, control of the TCP connection using signal CD (DTR on the router) would be activated.

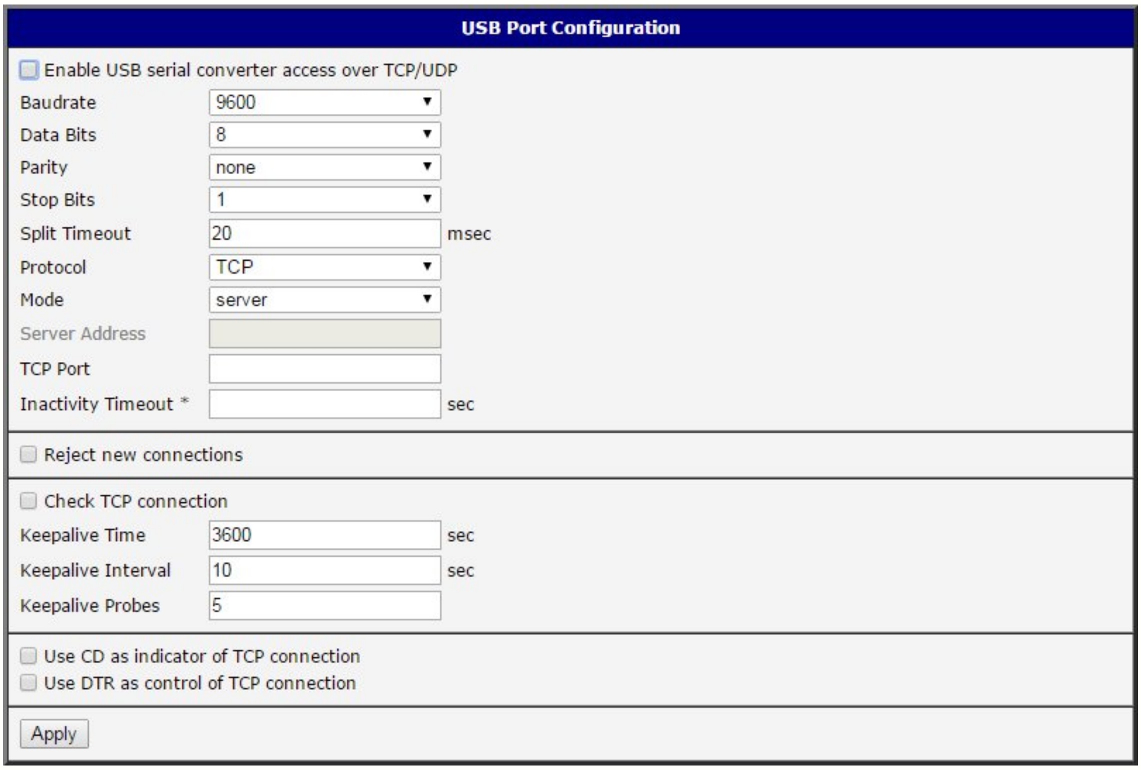
DTR	Description server	Description client
Active	The router allows a TCP connection	Router starts TCP connection
Nonactive	The router doesn’t allow a TCP conn.	Router stops TCP connection

Table 67: DTR signal description

Supported USB/RS232 converters:

- FTDI
- Prolific PL2303
- Silicon Laboratories CP210×

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

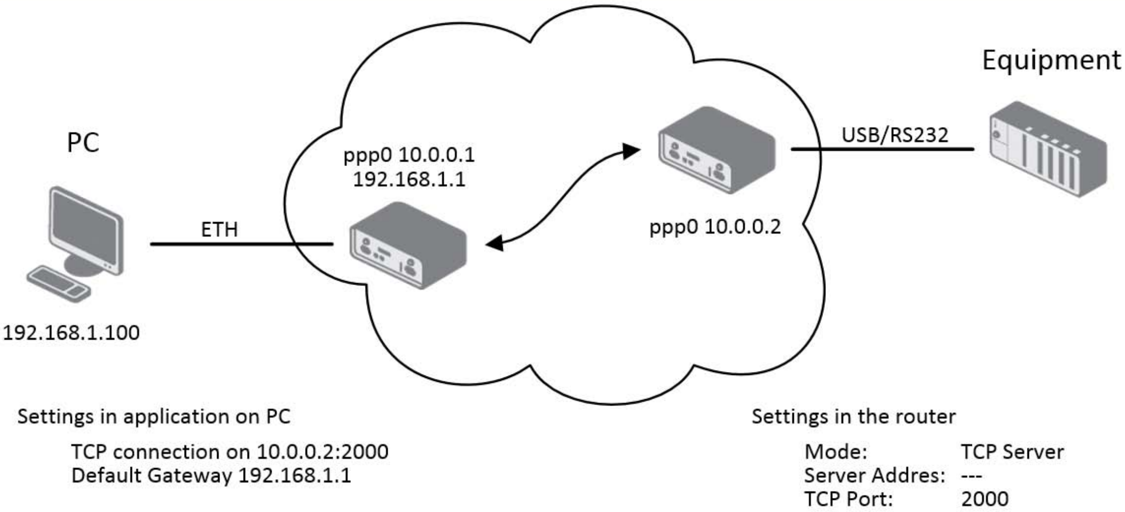
Keepalive Time	3600	sec
Keepalive Interval	10	sec
Keepalive Probes	5	

☐ Use CD as indicator of TCP connection

☐ Use DTR as control of TCP connection

Figure 57: USB configuration

Examples of USB port configuration:



Settings in application on PC

TCP connection on 10.0.0.2:2000
Default Gateway 192.168.1.1

Settings in the router

Mode:	TCP Server
Server Addres:	---
TCP Port:	2000

Figure 58: Example 1 – USB port configuration

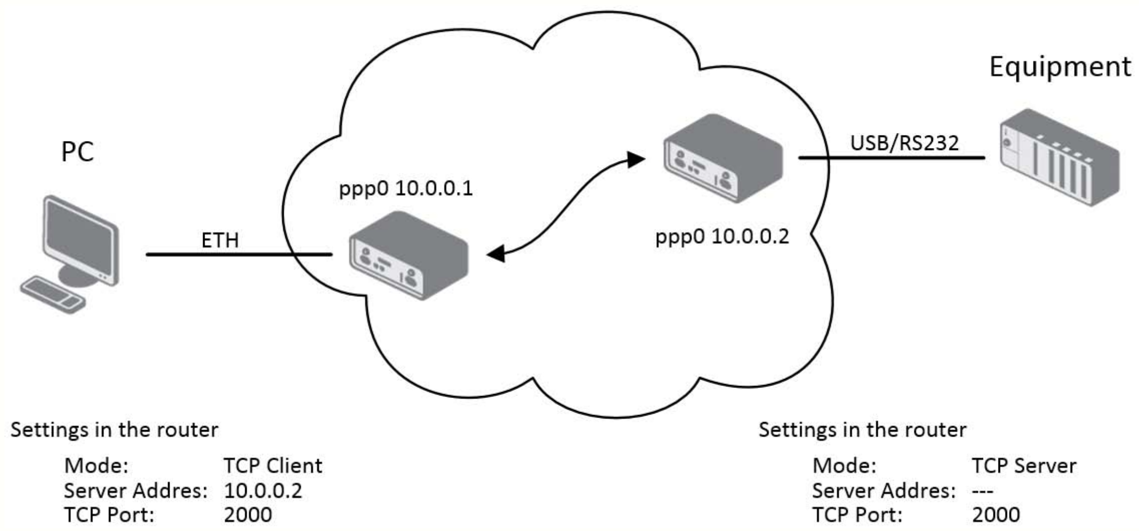
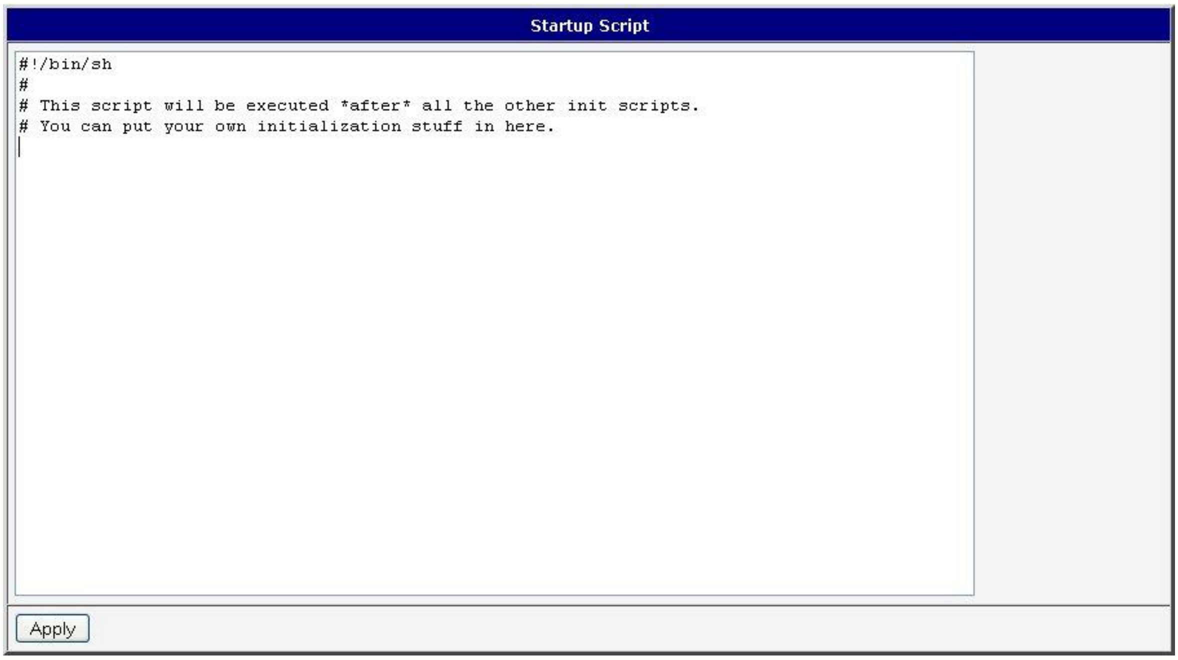


Figure 59: Example 2 – USB port configuration

4.21 Startup Script

In the window *Startup Script* it is possible to create own scripts which will be executed after all initial scripts.

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

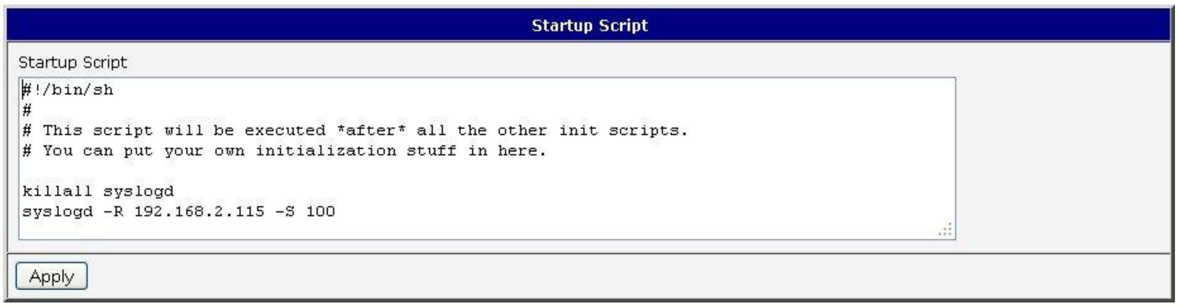


```
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here.
```

Figure 60: Startup script

Change will take effect after shut down and turn on the router. This can be done in the *Reboot* item in the *Administration* section or by SMS message (see *SMS Configuration*).

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



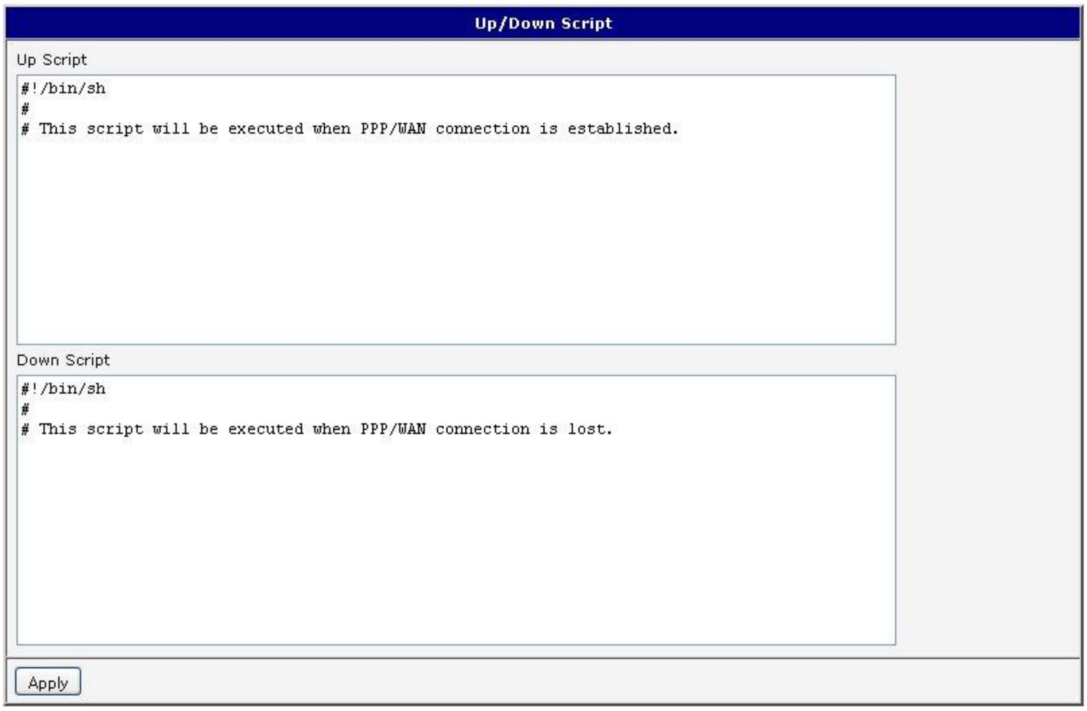
```
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here.

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

Figure 61: Example of Startup script

4.22 Up/Down Script

In the window *Up/Down Script* it is possible to create own scripts. In the item *Up script* is defined a script, which begins after establishing a PPP/WAN connection. In the item *Down Script* is defined script, which begins after lost a PPP/WAN connection.

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

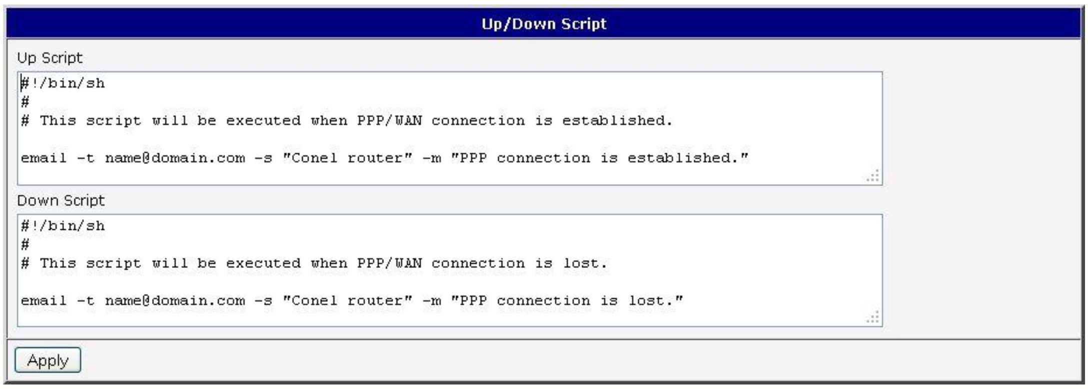


```
#!/bin/sh
#
# This script will be executed when PPP/WAN connection is established.
```

```
#!/bin/sh
#
# This script will be executed when PPP/WAN connection is lost.
```

Figure 62: Up/Down script

Example of UP/Down script: After establishing or lost a connection, the router sends an email with information about establishing or loss a connection.



```
#!/bin/sh
#
# This script will be executed when PPP/WAN connection is established.

email -t name@domain.com -s "Conel router" -m "PPP connection is established."
```

```
#!/bin/sh
#
# This script will be executed when PPP/WAN connection is lost.

email -t name@domain.com -s "Conel router" -m "PPP connection is lost."
```

Figure 63: Example of Up/Down script

4.23 Automatic Update Configuration

In the *Automatic update* item it is possible to set the automatic configuration update. This choice enables the router to download the configuration and the newest firmware from the server automatically. The configuration and firmware files are stored on the server. To prevent possible unwanted manipulation of the files, downloaded file (tar.gz format) is controlled. 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 controlled.

By *Enable automatic update of configuration* it is possible to enable automatic configuration update.

By *Enable automatic update of firmware* it is possible to enable firmware update.

Item	Description
Source	Where the router will download the firmware and configuration from: • **HTTP(S)/FTP(S) server** – updates are downloaded from the *Base URL* address below. Used protocol is specified by that address: HTTP, HTTPS, FTP or FTPS. • **USB flash drive** – Router finds current firmware or configuration in the root directory of the connected USB device. • **Both** – looking for the current firmware or configuration from both sources.
Base URL	Enter the base part of the domain or IP address to download the updates from. Specify the communication protocol by the address (HTTP, HTTPS, FTP or FTPS).
Unit ID	Name of configuration (name of the file without extension). If the Unit ID is not filled, the MAC address of the router is used as the filename (the delimiter colon is used instead of a dot.)
Update Hour	Use this item to set the hour (range 1-24) when the automatic update will be performed every day. If the time is not specified, automatic update is performed five minutes after turning on the router and then every 24 hours. If the detected configuration file is different from the running one, it is downloaded and the router is restarted automatically to make it run.

Table 68: Automatic update configuration

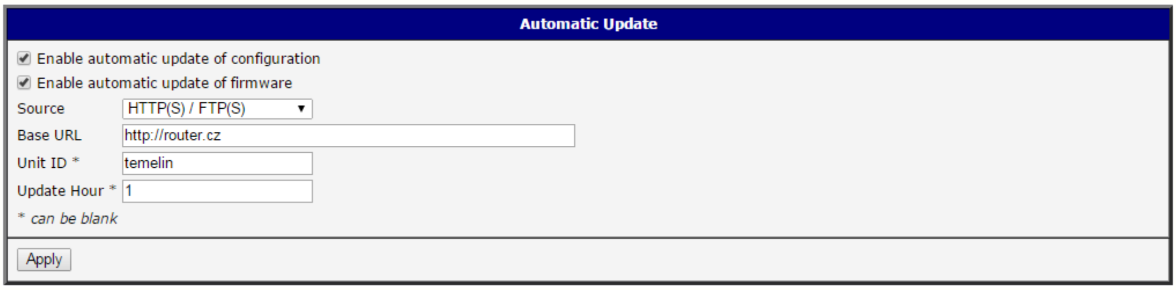
The *configuration file* name consists of *Base URL*, hardware MAC address of ETH0 interface and *cfg* extension. Hardware MAC address and *cfg* extension is connected automatically and it isn't needed to enter this. By parameter *Unit ID* enabled it defines the concrete configuration name which will be download to the router. When using parameter *Unit ID*, hardware MAC address in configuration name will not be used.

The *firmware file* name consists of *Base URL*, type of router and bin extension.

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

The following examples find if there is a new firmware or configuration each day at 1:00 in the morning. An example is for the SPECTRE v3 LTE type of router.

- Firmware: http://router.cz/SPECTRE-v3-LTE.bin
- Configuration file: http://router.cz/temelin.cfg



Automatic Update

☑ Enable automatic update of configuration
☑ Enable automatic update of firmware

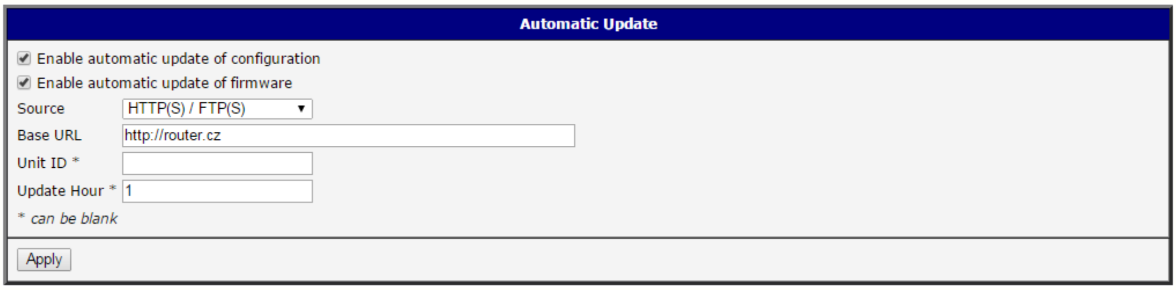
Source	HTTP(S) / FTP(S) ▾
Base URL	http://router.cz
Unit ID *	temelin
Update Hour *	1

* can be blank

Figure 64: Example of automatic update 1

The following examples find if there is a new firmware or configuration each day at 1:00 in the morning. An example is for the SPECTRE v3 LTE type of router with MAC address 00:11:22:33:44:55.

- Firmware: http://router.cz/SPECTRE-v3-LTE.bin
- Configuration file: http://router.cz/00.11.22.33.44.55.cfg



Automatic Update

☑ Enable automatic update of configuration
☑ Enable automatic update of firmware

Source	HTTP(S) / FTP(S) ▾
Base URL	http://router.cz
Unit ID *	
Update Hour *	1

* can be blank

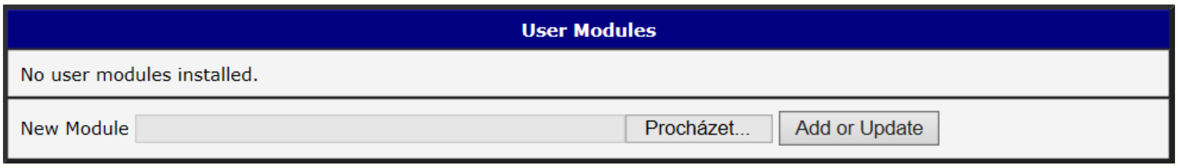
Figure 65: Example of automatic update 2

Firmware update can cause incompatibility of 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.

5. Customization

5.1 User Modules

Configuration of user modules can be accessed by selecting the *User Modules* item. It is possible to add new modules, delete them or switch to their configuration. Use the *Browse* button to select the user module (compiled module has tgz extension). The module is added using the *Add* button.



User Modules

No user modules installed.

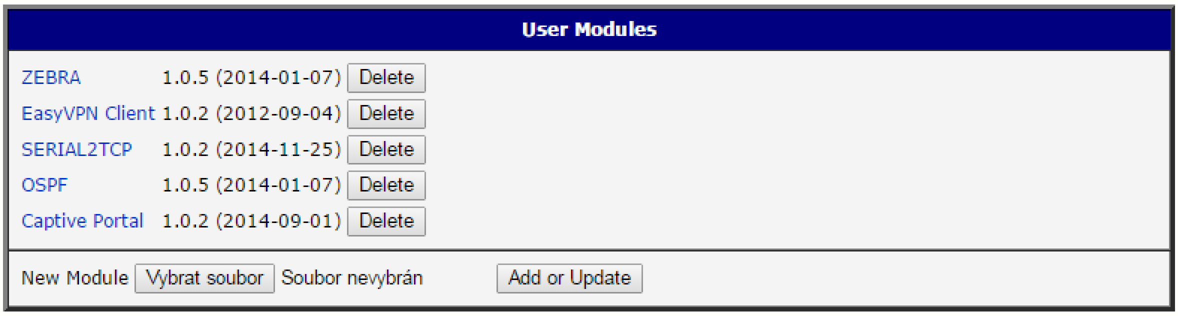
New Module

Figure 66: User modules

Added module appears in the list of modules on the same page. If the module contains index.html or index.cgi page, module name serves as a link to this page. The module can be deleted using the *Delete* button.

Updating of the module can be done in the same way like adding a new module. 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.



User Modules

ZEBRA	1.0.5 (2014-01-07)	Delete
EasyVPN Client	1.0.2 (2012-09-04)	Delete
SERIAL2TCP	1.0.2 (2014-11-25)	Delete
OSPF	1.0.5 (2014-01-07)	Delete
Captive Portal	1.0.2 (2014-09-01)	Delete

New Module Soubor nevybrán

Figure 67: Added user module

There are for example these user's modules available. User modules can be downloaded from web pages www.conel.cz or can be custom-programmed.

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 to do TCP and UDP scan.
Daily Reboot	Allows to perform daily reboot of the router at the specified time.
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 to receive messages from WMBUS meters and saves contents of these messages to XML file.
pduSMS	Sends short messages (SMS) to specified number.
GPS	Allows 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 to manually or automatically verify the functionallity of the connection between two network interfaces (ping).
IS-IS	Add support of IS-IS protocol.

Table 69: User modules

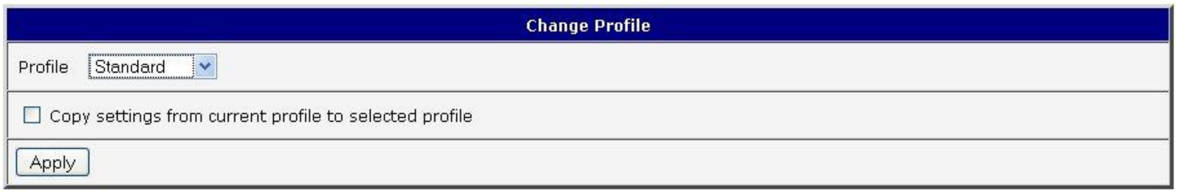
! Attention, in some cases the firmware update can cause the incompatibility of used user modules. Some of them are are dependent on the version of linux kernel (e.g. *SmsBE* and *PoS Configuration*). It is recommended to update user modules to the most recent version. Information about the user module and the firmware compatibility is at the beginning of the user module's Application Note.

6. Administration

6.1 Change Profile

Using profiles it is possible to switch between different configurations of the router. It can be used for example to switch between different modes of operation of the router (router has established connection, the router has not established connection and the router creates a tunnel to the service center). Change of the profile can be done using a binary input, SMS or Web interface of the router.

To open the dialog box for changing the profile select the *Change Profile* menu item. Profile switch is making by press the button *Apply*. Change take effect after restarting router by the help of button *Reboot* in web administration or by SMS message. It is possible to select the standard profile or up to three alternative profiles. It is possible to copy actual configuration to selected configuration by selecting *Copy settings from current profile to selected profile*.


Change Profile

Profile: Standard

☐ Copy settings from current profile to selected profile

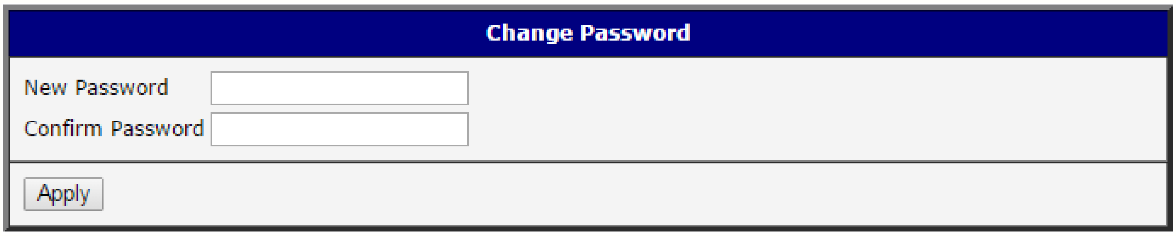
Figure 68: Change profile

6.2 Change Password

To change the access password, select the *Change Password* menu item. Type the new password twice and save it by pressing the the *Apply* button.

In basic settings of the router the password is set on *root* in default. **It is necessary to change this default password for the security of your network**.

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.


Change Password

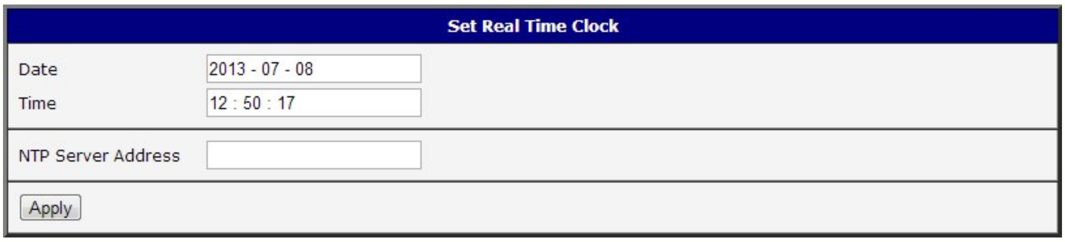
New Password:

Confirm Password:

Figure 69: Change password

6.3 Set Real Time Clock

Disposable setting of the router internal clock can be invoked by pressing the *Set Real Time Clock* item in the main menu of the web interface. Date and time can be set manually through the *Date* and *Time* items. Always enter data in a format that is illustrated in the figure below. The clock can be also adjusted according to the specified NTP server. Finally, it is necessary to press the *Apply* button.



Set Real Time Clock

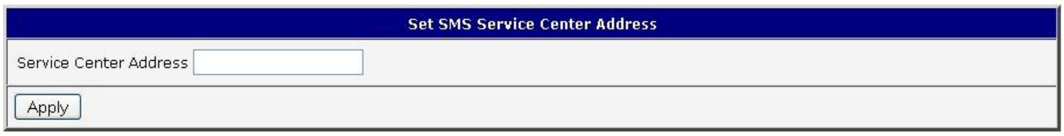
Date	2013 - 07 - 08
Time	12 : 50 : 17
NTP Server Address	

Figure 70: Set real time clock

6.4 Set SMS Service Center Address

This option is not available in cable routers.

In some cases it is needed to set the phone number of the SMS service centre because of SMS sending. This parameter can not be set when the SIM card has set phone number of the SMS service centre. The phone number can be formed without international prefix xxx xxx xxx or with international prefix for example +420 xxx xxx xxx.



Set SMS Service Center Address

Service Center Address	

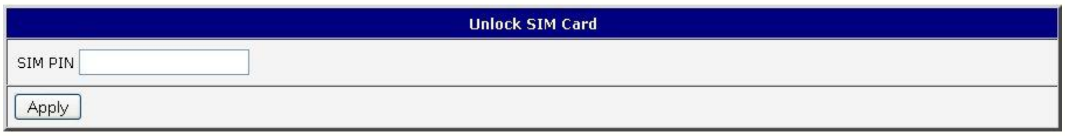
Figure 71: Set SMS service center address

6.5 Unlock SIM Card

This option is not available in cable routers.

Possibility to unlock SIM PIN is under *Unlock SIM Card* item. If the inserted SIM card is secured by a PIN number, enter the PIN to field *SIM PIN* and click the *Apply* button.

SIM card is blocked after three failed attempts to enter the PIN code.



Unlock SIM Card

SIM PIN	

Figure 72: Unlock SIM card

6.6 Send SMS

This option is not available in cable routers.

Sending SMS messages is possible in menu *Send SMS*. The SMS message will be sent after entering the *Phone number* and text SMS (*Message*) and by pushing button *Send*. Messages of the standard length 160 characters can be sent. (For sending long SMS messages the user module pduSMS can be used.)

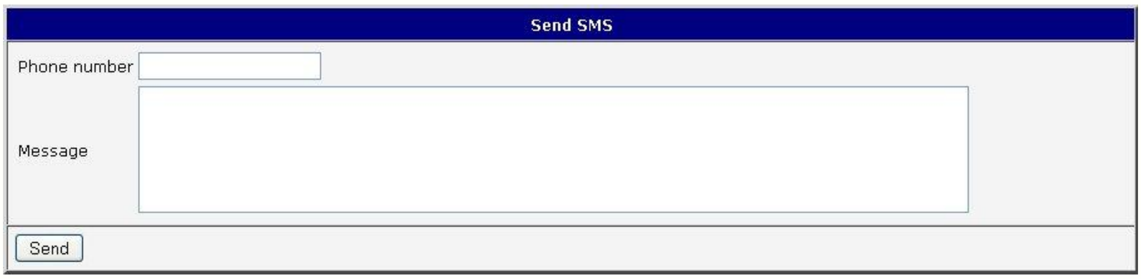


Figure 73: Send SMS

SMS message sending via HTTPS request is in the form:

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

HTTPS request will be sent to TCP connection on router port 443. 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. In the example is used for root:root.

6.7 Backup Configuration

The router's configuration can be saved in the *Backup Configuration* menu item. Clicking on this item it is possible to choose a destination directory of the configuration file in your PC.

6.8 Restore Configuration

If you need to restore the router's configuration, click the *Restore Configuration* menu item. Clicking on the *Browse* button you can choose the configuration file (.cfg) from your PC.

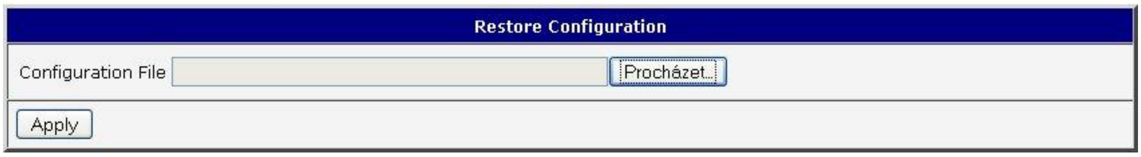
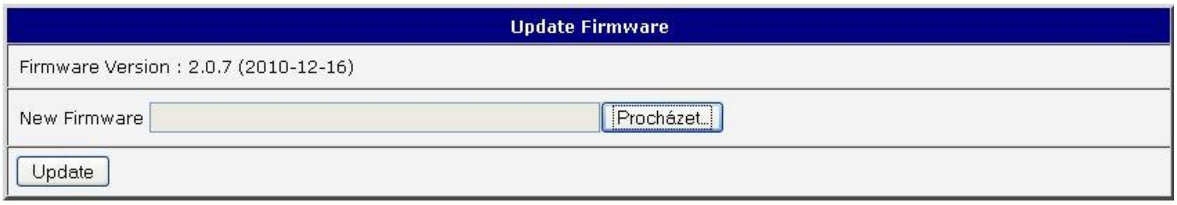


Figure 74: Restore configuration

6.9 Update Firmware

To view the information about the firmware version and instructions for its update select the *Update Firmware* menu item. New firmware is selected via *Browse* button form your PC (it is necessary to have the firmware file on your computer) and update is run pressing the *Update* button. It takes about three and half minutes to complete the update.



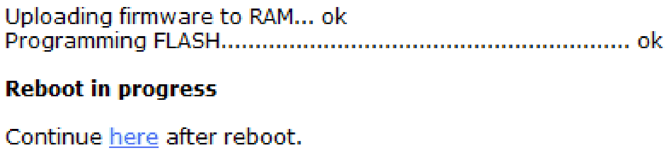
Update Firmware

Firmware Version : 2.0.7 (2010-12-16)

New Firmware

Figure 75: Update firmware

After successful firmware update the following statement is listed (informs about update of the FLASH memory):



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

Reboot in progress

Continue here after reboot.

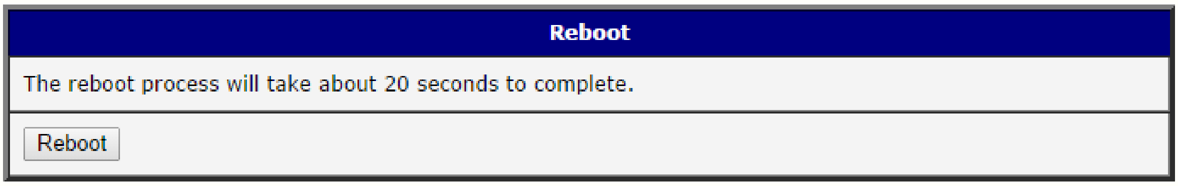
Upload firmware of different device can cause damage of the router!
During the update of the firmware the permanent power supply has to be maintained.

Starting with FW 5.1.0 mechanism to prevent multiple startup of firmware update is added.

Firmware update can cause incompatibility of 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.

6.10 Reboot

To reboot the router select the *Reboot* menu item and then press the *Reboot* button.



Reboot

The reboot process will take about 20 seconds to complete.

Figure 76: Reboot

7. Configuration in Typ. Situations

Although Conel routers have wide variety of usage, they are used in these typical situations mostly. In this chapter, there are four examples of router's configuration in the typical situations. Examples include the configuration of all items needed for router to work properly in that situation.

7.1 Access to the Internet from LAN

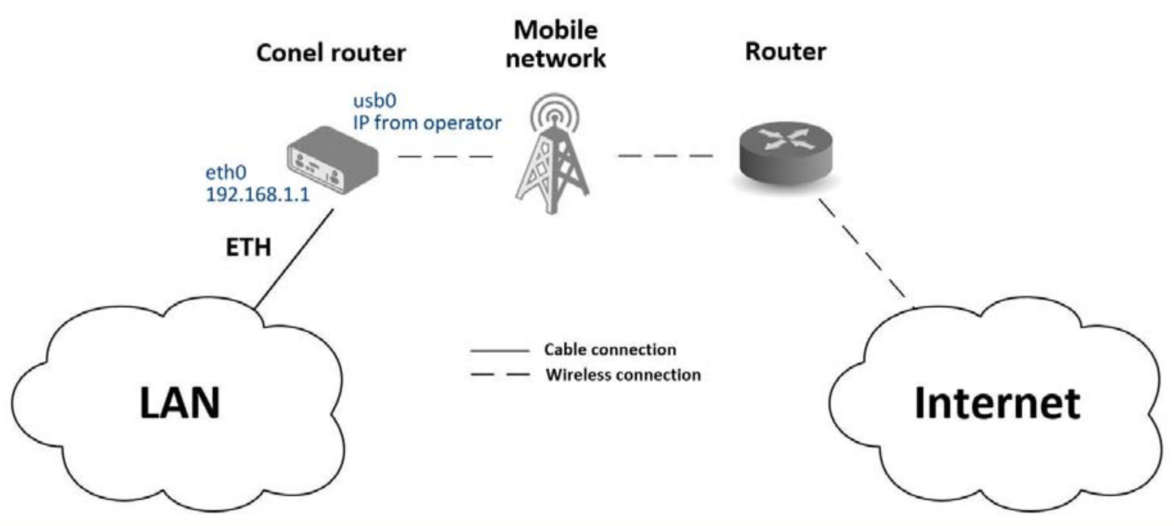
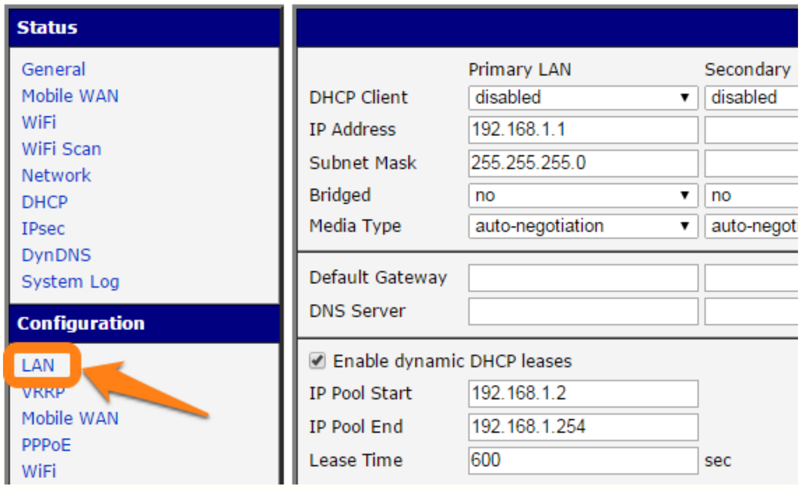


Figure 77: Access to the Internet from LAN – topology of the example

There is topology of this easy example shown on the fig. 77. To connect to the Internet via mobile network the SIM card with the data tariff has to be available from the operator. This basic router's function **does not need any configuration** in this case. It is sufficient to put the SIM card into the SIM1 slot (Primary SIM card), attach the antenna to the ANT connector and connect the computer (or switch and computers) to the router's ETH0 interface (LAN). Wait a moment after turning on the router. It will connect to the mobile network and the Internet signalized by LEDs on the front panel of the router (WAN and DAT). Additional configuration can be done in the *LAN* and *Mobile WAN* items in the *Configuration* section of the web interface.

***LAN* configuration** The factory default IP adress of the eth0 router's interface is in the form of 192.168.1.1. This can be changed (after login to the router) in the *LAN* item in the *Configuration* section, see figure 78. In this case there is no need of any additional configuration, DHCP server is also enabled by factory default (so the first connected computer will get the 192.168.1.2 IP address etc.). Other configuration possibilities are described in the chapter 4.1.



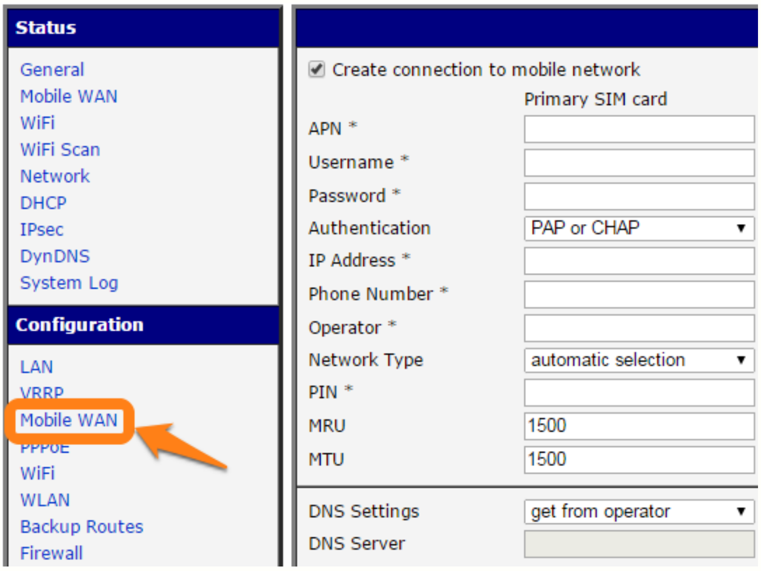
	Primary LAN	Secondary
DHCP Client	disabled ▾	disabled
IP Address	192.168.1.1	
Subnet Mask	255.255.255.0	
Bridged	no ▾	no
Media Type	auto-negotiation ▾	auto-negot
Default Gateway		
DNS Server		

☑ Enable dynamic DHCP leases

IP Pool Start	192.168.1.2	
IP Pool End	192.168.1.254	
Lease Time	600	sec

Figure 78: Access to the Internet from LAN – *LAN* configuration

***Mobile WAN* Configuration** Connection to the mobile network can be configured in the Mobile WAN item in the Configuration section, see fig. 79. In this case (depending on the SIM card) the configuration form can be blank, just make sure that *Create connection to mobile network* on the top is checked (factory default). For more details, see chapter 4.2.1.



☑ Create connection to mobile network

	Primary SIM card
APN *	
Username *	
Password *	
Authentication	PAP or CHAP ▾
IP Address *	
Phone Number *	
Operator *	
Network Type	automatic selection ▾
PIN *	
MRU	1500
MTU	1500
DNS Settings	get from operator ▾
DNS Server	

Figure 79: Access to the Internet from LAN – *Mobile WAN* configuration

To check whether the connection is working properly, go to *Mobile WAN* item in the *Status* section. Information about operator, signal strength etc. is available. At the bottom, the message *Connection successfully established* will be written out. In the *Network* item there is information about a newly created network interface usb0 (mobile connection). IP address from operator, route table etc. can be found here. Internet is accessible from LAN now.

7.2 Backed Up Access to the Internet from LAN

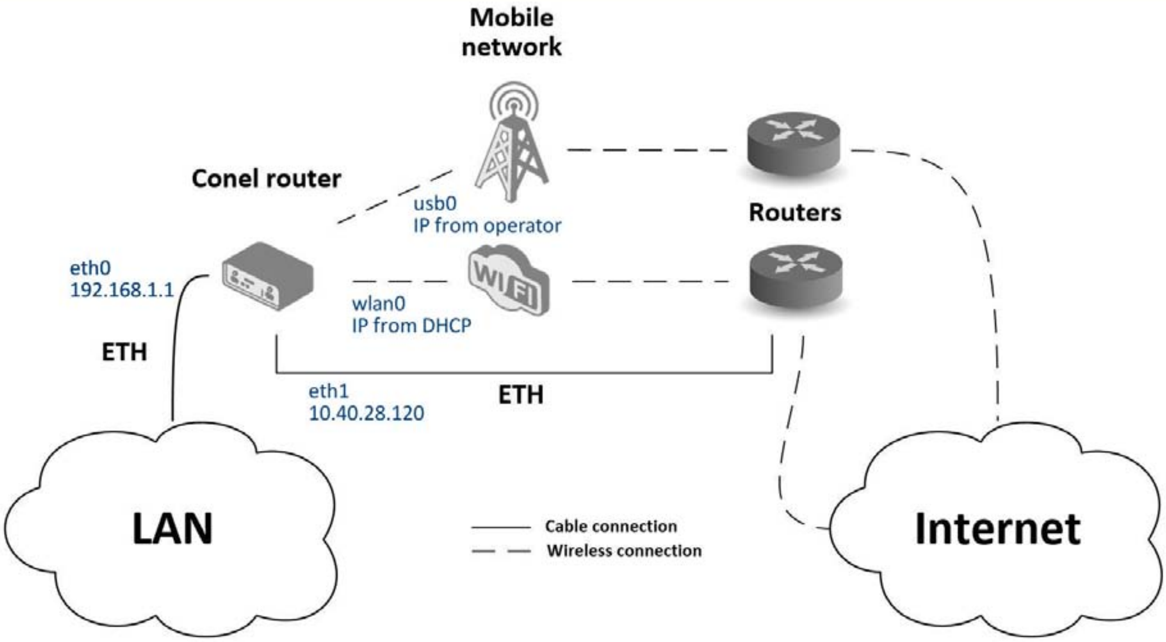
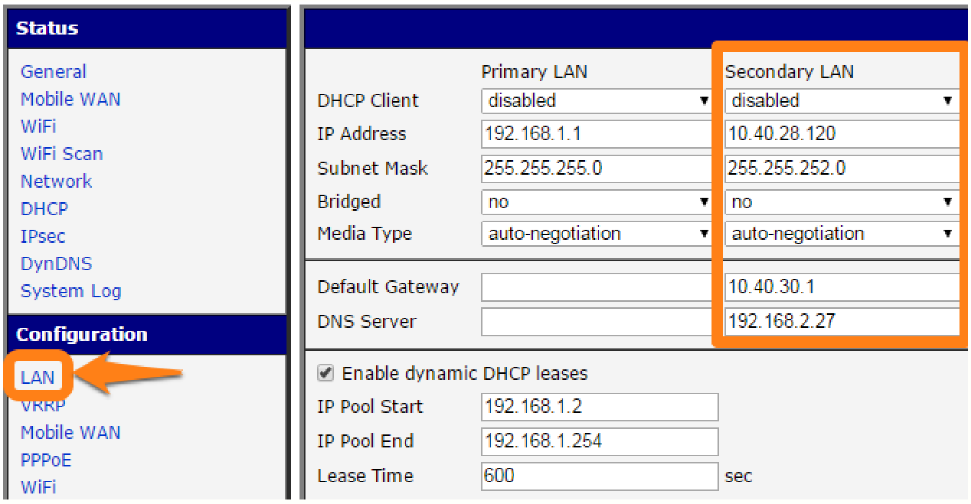


Figure 80: Backed up access to the Internet – topology of the example

In the situation on the fig. 80 it's necessary to configure all the connections to the Internet in items *LAN* for Ethernet, *WLAN* and *WiFi* for WiFi connection and *Mobile WAN* for mobile connection. Then it is possible to configure the priorities of backup routes in the *Backup Routes* item.



	Primary LAN	Secondary LAN
DHCP Client	disabled	disabled
IP Address	192.168.1.1	10.40.28.120
Subnet Mask	255.255.255.0	255.255.252.0
Bridged	no	no
Media Type	auto-negotiation	auto-negotiation
Default Gateway		10.40.30.1
DNS Server		192.168.2.27

☑ Enable dynamic DHCP leases

IP Pool Start	192.168.1.2
IP Pool End	192.168.1.254
Lease Time	600 sec

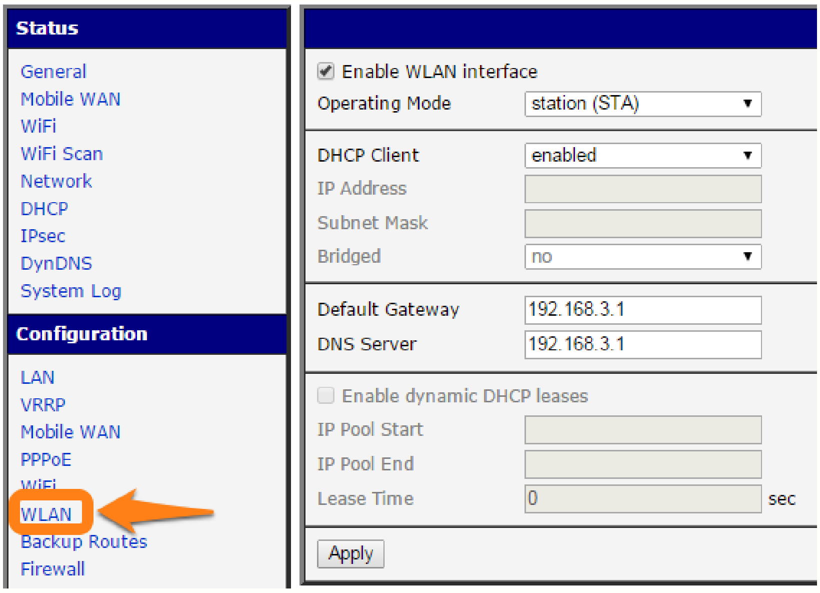
Figure 81: Backed up access to the Internet – *LAN* configuration

***LAN* configuration** In the *LAN* item – *Primary LAN* – you can leave the factory default configuration as in the previous situation. The ETH1 interface on the front panel of the router is used for connection to the Internet. It can be configured in *Secondary LAN*. Connect the cable to the router and set appropriate values as in the fig. 81 – here static IP address, default gateway and DNS server are configured. Changes will take effect clicking on the *Apply* button. Detailed configuration of *LAN* is described in the 4.1 chapter.

***WLAN* and *WiFi* configuration** It's necessary to enable wlan0 network interface in the *WLAN* item, see fig. 82. Check the *Enable WLAN interface*, set the *Operating Mode* to *station (STA)*, enable the DHCP client and fill in the default gateway and DNS server for accessing the Internet. Click the *Apply* button to confirm the changes. For details see chapter 4.5.

Configure connection to a WiFi network in the WiFi item, see fig. 83. Here check the *Enable WiFi* and fill in the data for connection (*SSID*, security, password) and confirm clicking the *Apply* button. For detailed configuration see 4.4 chapter.

To verify successful WiFi connection, see *Status* section, *WiFi* item. There will be `wpa_state=COMPLETED` written out if connected successfully.



☑ Enable WLAN interface

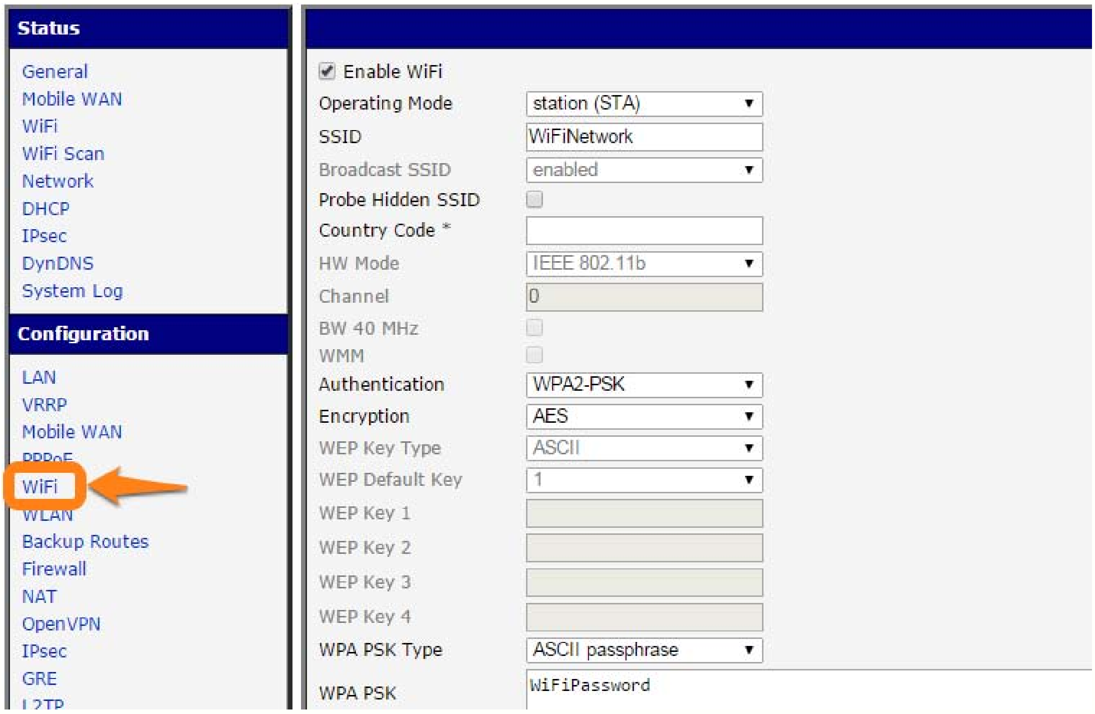
Operating Mode	station (STA)
DHCP Client	enabled
IP Address	
Subnet Mask	
Bridged	no
Default Gateway	192.168.3.1
DNS Server	192.168.3.1

□ Enable dynamic DHCP leases

IP Pool Start	
IP Pool End	
Lease Time	0 sec

Figure 82: Backed up access to the Internet – *WLAN* configuration

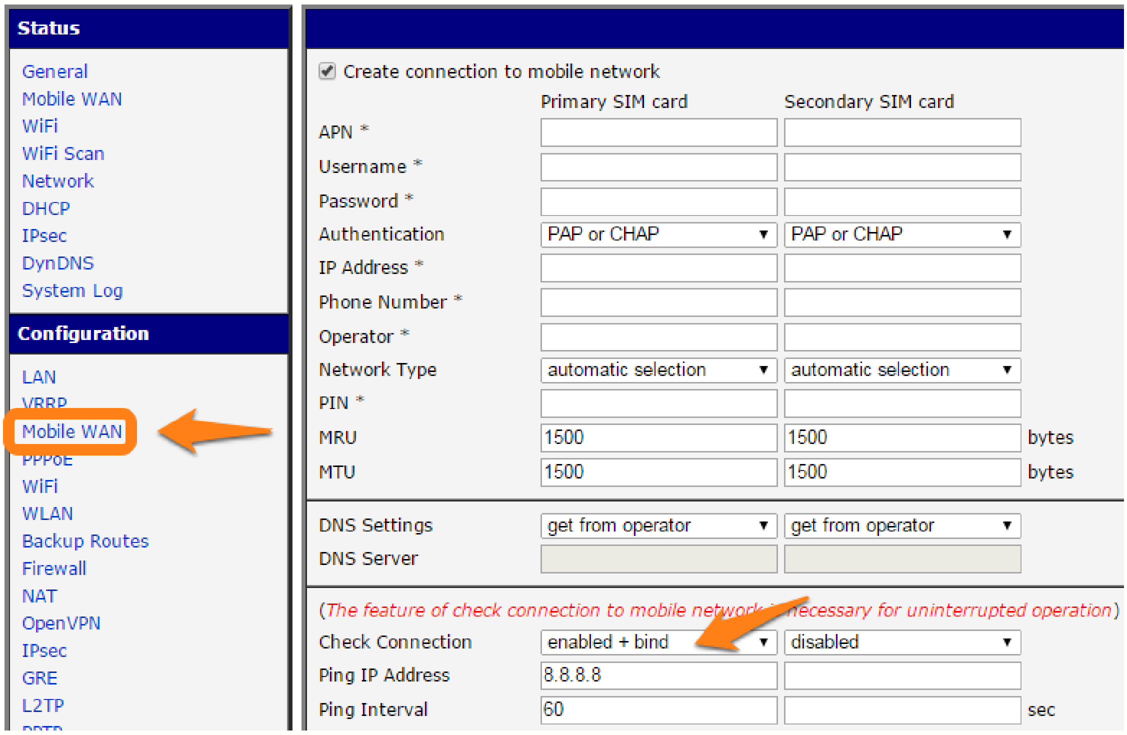
***Mobile WAN* configuration** To configure the mobile connection it is sufficient to insert the SIM card into the SIM1 slot and attach the antenna to the ANT connector as in previous situation (depending on used SIM card). For using the system of backup routes it's necessary to enable check of connection in the *Mobile WAN* item, see fig. 84. Set the *Check connection* option to *enabled + bind* and fill in an IP adress of e.g. operator's DNS server or any other surely available server and time interval of the check. For detailed configuration see chapter 4.2.1.



☑ Enable WiFi

Operating Mode	station (STA) ▾
SSID	WiFiNetwork
Broadcast SSID	enabled ▾
Probe Hidden SSID	□
Country Code *	
HW Mode	IEEE 802.11b ▾
Channel	0
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	ASCII passphrase ▾
WPA PSK	WiFiPassword

Figure 83: Backed up access to the Internet – *WiFi* configuration



☑ Create connection to mobile network

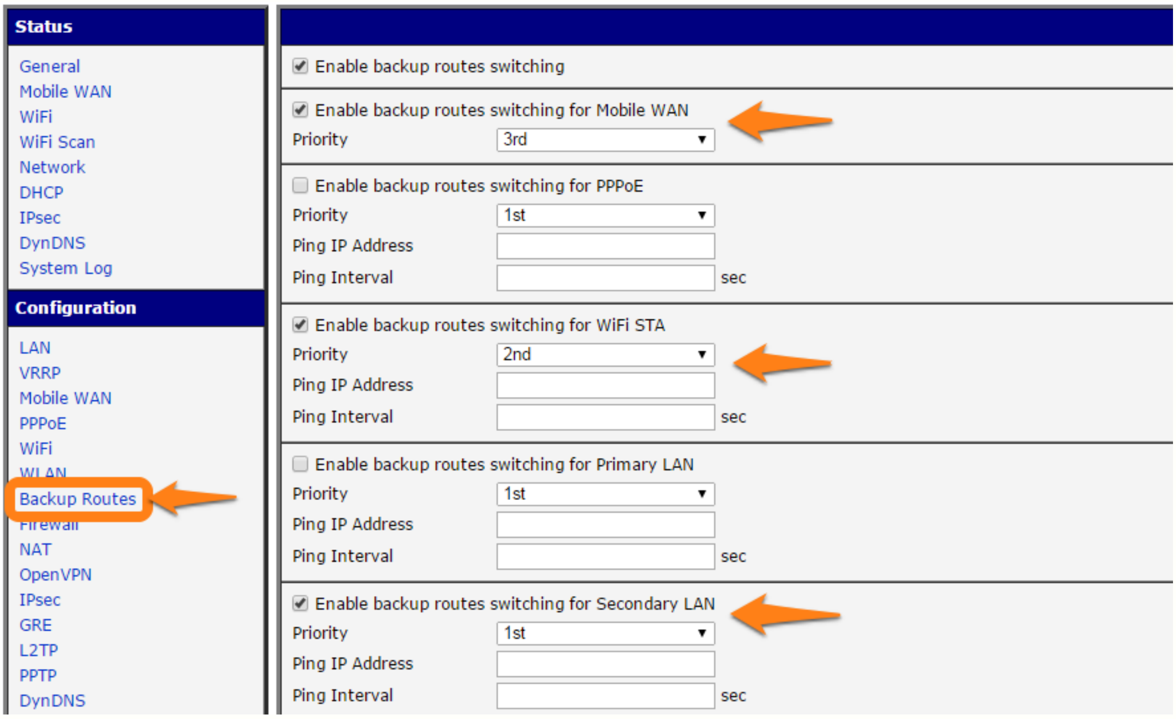
	Primary SIM card	Secondary SIM card	
APN *			
Username *			
Password *			
Authentication	PAP or CHAP ▾	PAP or CHAP ▾	
IP Address *			
Phone Number *			
Operator *			
Network Type	automatic selection ▾	automatic selection ▾	
PIN *			
MRU	1500	1500	bytes
MTU	1500	1500	bytes
DNS Settings	get from operator ▾	get from operator ▾	
DNS Server			

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

Check Connection	enabled + bind ▾	disabled ▾	
Ping IP Address	8.8.8.8		
Ping Interval	60		sec

Figure 84: Backed up access to the Internet – *Mobile WAN* configuration

***Backup Routes* configuration** Finally configure the priorities of the backup routes. The eth1 wired connection has the highest priority in this situation. In case of failure, the second priority has WiFi wlan0 network interface, and then the mobile connection – usb0 network interface. See fig. 85 for corresponding settings of the *Backup Routes* item. System of backup routes has to be activated by checking the *Enable backup routes switching* item. Then enable backup routes switching at every backup route used and set up the priorities. Click the *Apply* button to confirm the changes. For detailed configuration see chapter 4.6.



☑ Enable backup routes switching

☑ Enable backup routes switching for Mobile WAN
Priority 3rd

□ Enable backup routes switching for PPPoE
Priority 1st
Ping IP Address
Ping Interval sec

☑ Enable backup routes switching for WiFi STA
Priority 2nd
Ping IP Address
Ping Interval sec

□ Enable backup routes switching for Primary LAN
Priority 1st
Ping IP Address
Ping Interval sec

☑ Enable backup routes switching for Secondary LAN
Priority 1st
Ping IP Address
Ping Interval sec

Figure 85: Backed up access to the Internet – *Backup Routes* configuration

The router configured this way now serves to computers in LAN for backed up access to the Internet. You can verify the configured network interfaces in the *Status* section in the *Network* item. There you should see active network interfaces eth0 (connection to LAN), eth1 (wired connection to the Internet), wlan0 (WiFi connection to the Internet) and usb0 (mobile connection to the Internet). IP adresses and other data are included. At the bottom you can see the *Route Table* and corresponding changes of it when e.g. wired connection fails or cable disconnected (default route changes to wlan0). And the same – if WiFi is not available, the mobile connection will be used.

Backup routes are working even if not activated in the *Backup Routes* item, but with implicit priorities of network interfaces set as factory default. These priorities are different from the ones desired in this situation, see chapter 4.6.

7.3 Secure Networks Interconnection or Using VPN

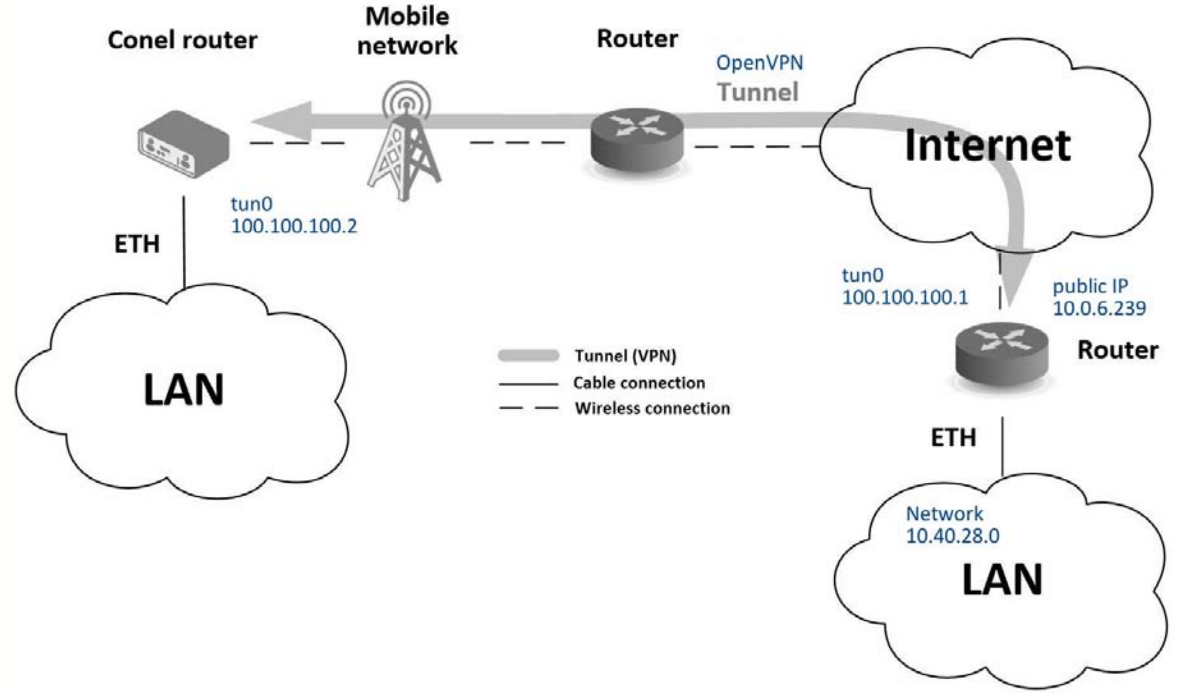


Figure 86: Secure networks interconnection – topology of the example

VPN (Virtual Private Network) is a secured (encrypted) and authenticated (verified) connection of two LANs into one, so it performs as one homogenous LAN. LANs are connected over public untrusted network (Internet), see fig. 86. In Conel routers you can use more ways (protocols) for this reason:

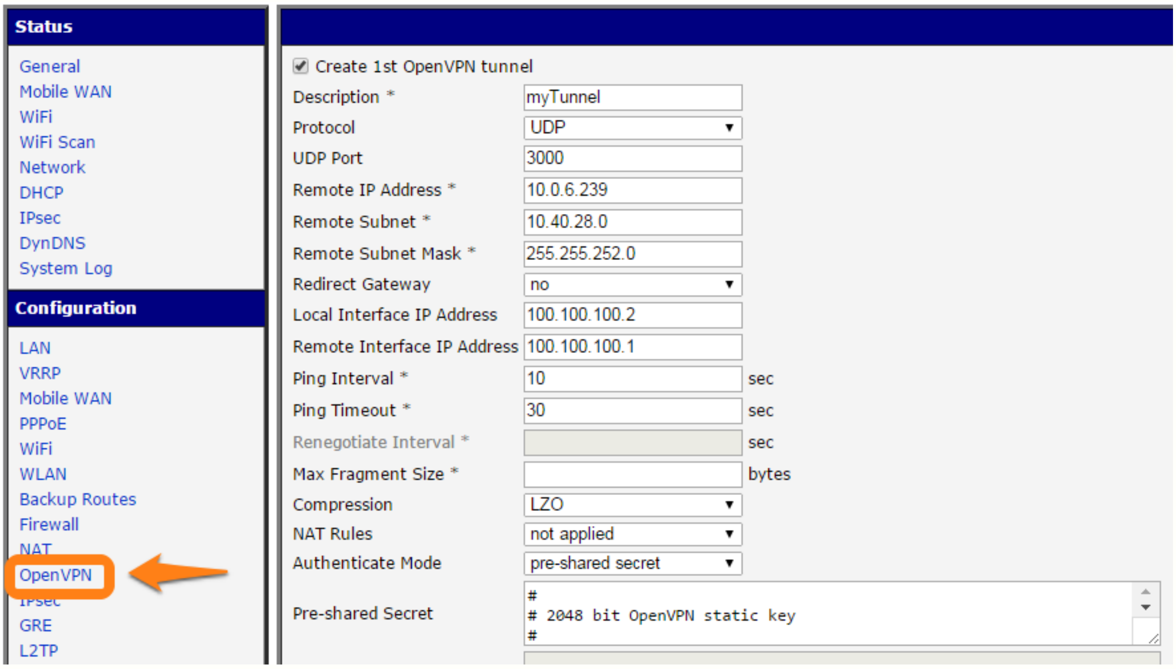
- *OpenVPN* (it is also configuration item in the web interface of the router), see chapter 4.9 or Application Note [5],
- *IPsec* (it is also configuration item in the web interface of the router), see chapter 4.10 or Application Note [6].

You can create also non-encrypted tunnels: *GRE*, *PPTP* and *L2TP* with Conel router. In combination with IPsec you can use GRE or L2TP tunnel to create VPN.

There is an example of OpenVPN tunnel in the fig. 86. These are the prerequisites for this example: knowledge of the opposite router IP address, knowledge of the opposite network IP address (not necessary) and knowledge of the pre-shared secret (key). To create the OpenVPN tunnel it is necessary to configure the *Mobile WAN* and *OpenVPN* items in the *Configuration* section.

***Mobile WAN* configuration** The mobile connection can be configured the same way as in the previous situations (router connects itself after inserting the SIM card into SIM1 slot and attaching the antenna to the ANT connector), configuration is accessible in the *Configuration* section, the *Mobile WAN* item (see chapter 4.2.1), where mobile connection has to be enabled.

***OpenVPN* configuration** is accessible in the *Configuration* section in the *OpenVPN* item. Choose one of two possible tunnels and enable it checking the *Create 1st OpenVPN tunnel*, see fig. 87. It's necessary to fill in the protocol and port (according to the data about opposite side of the tunnel or Open VPN server). Fill in the public IP address of the opposite side of the tunnel including the remote subnet and mask (not necessary). Important items are *Local* and *Remote Interface IP Address* where the interfaces of the tunnel's ends has to be filled in. In this situation the *pre-shared secret* was know, so choose this option in the *Authentication Mode* item and insert the secret (key) into the field. Confirm the configuration clicking the *Apply* button. For detailed configuration see chapter 4.9 or Application Note [5].



☑ Create 1st OpenVPN tunnel

Description *	myTunnel	
Protocol	UDP ▾	
UDP Port	3000	
Remote IP Address *	10.0.6.239	
Remote Subnet *	10.40.28.0	
Remote Subnet Mask *	255.255.252.0	
Redirect Gateway	no ▾	
Local Interface IP Address	100.100.100.2	
Remote Interface IP Address	100.100.100.1	
Ping Interval *	10	sec
Ping Timeout *	30	sec
Renegotiate Interval *		sec
Max Fragment Size *		bytes
Compression	LZO ▾	
NAT Rules	not applied ▾	
Authenticate Mode	pre-shared secret ▾	
Pre-shared Secret	# # 2048 bit OpenVPN static key #	

Figure 87: Secure networks interconnection – *OpenVPN* configuration

In the *Status* section, *Network* item, you can verify the activated network interface tun0 for the tunnel with the IP addresses of the tunnel's ends set. Successful connection can be verified in the *System Log* where `Initialization Sequence Completed` should be written out. Networks are now interconnected – it can be verified by the `ping` program also (ping between tunnel's endpoints IP addresses from one of the routers, console is accessible via SSH).

7.4 Serial Gateway

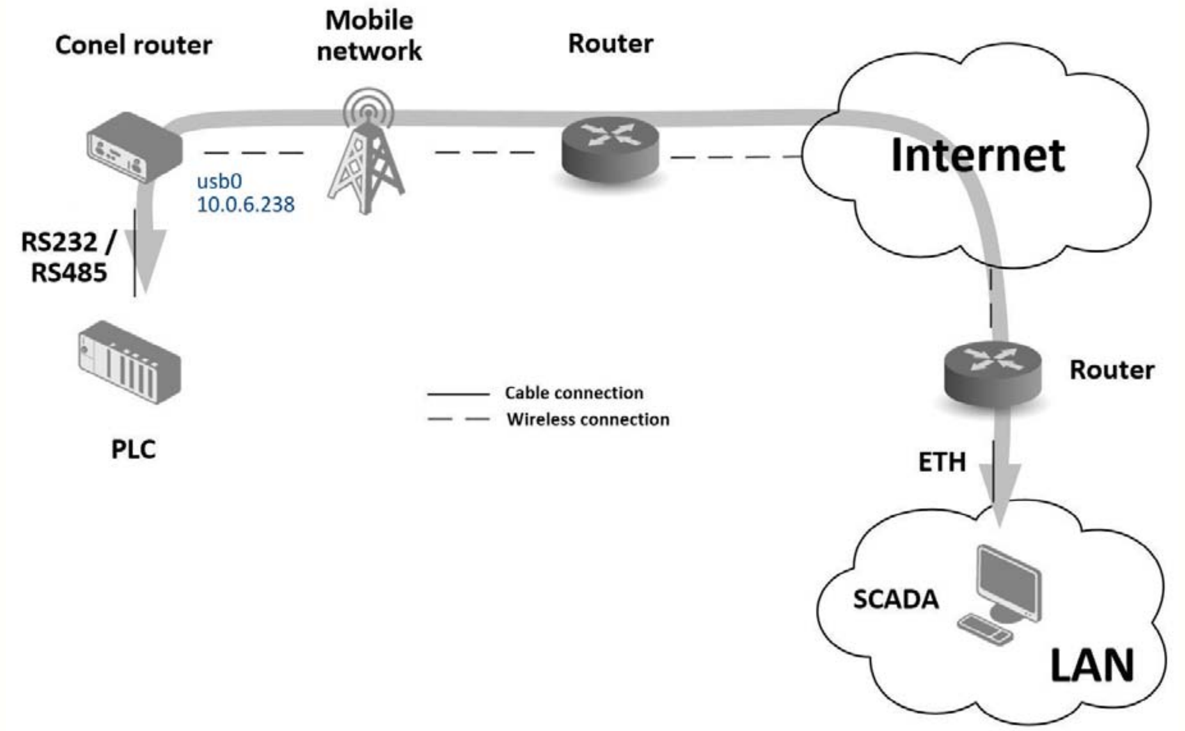
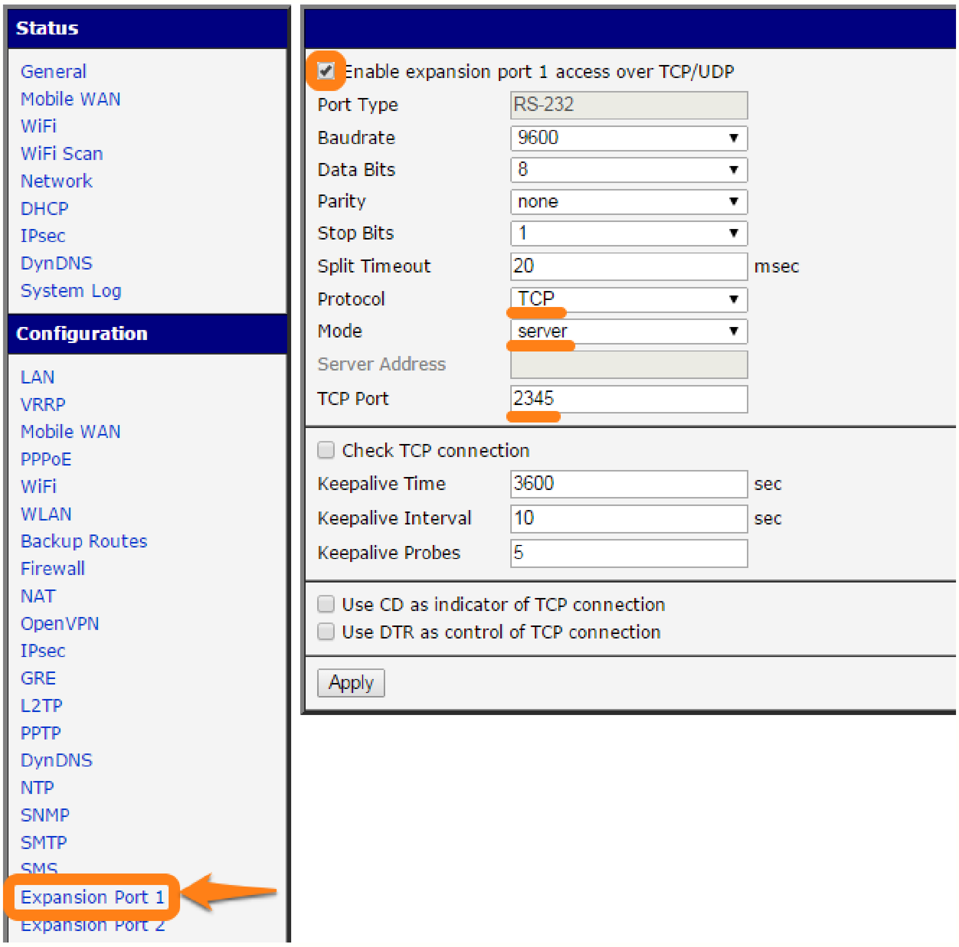


Figure 88: Serial Gateway – topology of the example

With the serial gateway you can enable the serial line communicating devices to access the internet or another network. These devices (meters, PLC, etc.) can upload and download the useful data then. The situation is depicted in the fig. 88. The Conel router has to have serial interface (port) RS232 or RS232-RS485/422 installed to serve as a serial gateway. Configuration is done in the *Mobile WAN* and *Expansion Port 1* items (or *Expansion Port 2* for RS422 and RS485) in the *Configuration* section of the web interface. In this situation the router is equipped with the RS232 interface (port).

***Mobile WAN* configuration** is the same as in the previous situations. Just insert the SIM card into the SIM1 slot at the back of the router and attach the antenna to the ANT connector at the front. No extra configuration is needed (depending on the SIM card used), for more details see chapter 4.2.1.

***Expansion Port 1* configuration** The interface RS232 (port) can be configured in the *Configuration* section, *Expansion Port 1* item – see fig. 89. It's necessary to enable the RS232 port checking the *Enable expansion port 1 access over TCP/UDP*. It is possible to edit the serial communication parameters (not needed in this situation). Important are *Protocol*, *Mode* and *Port* items where parameters of communication out to the network and internet can be configured. The TCP protocol is chosen in this situation and the router will work as the server listening on the 2345 TCP port. Confirm the configuration clicking the Apply button.



☑ Enable expansion port 1 access over TCP/UDP

Port Type	RS-232	
Baudrate	9600	
Data Bits	8	
Parity	none	
Stop Bits	1	
Split Timeout	20	msec
Protocol	TCP	
Mode	server	
Server Address		
TCP Port	2345	

☐ 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 89: Serial Gateway – konfigurace *Expansion Port 1*

To communicate with the serial device (PLC), connect from the PC (in fig. 88 labeled as SCADA) as a TCP client to the IP address 10.0.6.238, port 2345 (public IP address of the SIM card used in the Conel router, corresponding to the usb0 network interface). Devices can now communicate. To check the connection, go to *System Log* (*Status* section) and look for the *TCP connection established* message.

8. Recommended Literature

[1] Conel: **Commands and Scripts for v2 and v3 Routers**, Application Note

[2] Conel: **SmartCluster**, Application Note

[3] Conel: **R-SeeNet**, Application Note

[4] Conel: **R-SeeNet Admin**, Application Note

[5] Conel: **OpenVPN Tunnel**, Application Note

[6] Conel: **IPsec Tunnel**, Application Note

[7] Conel: **GRE Tunnel**, Application Note

[8] Conel: **SNMP Object Identifier**, Application Note

[9] Conel: **AT Commands**, Application Note