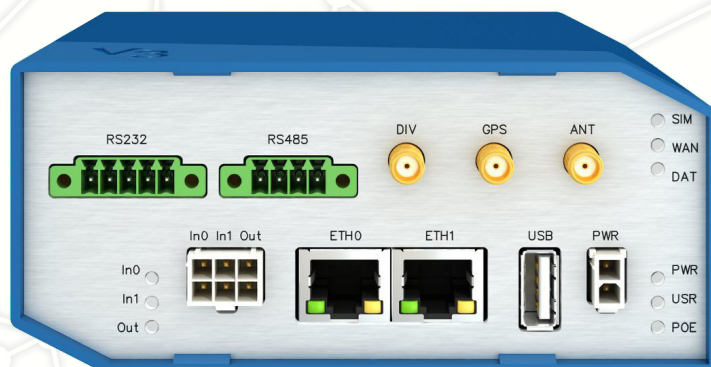
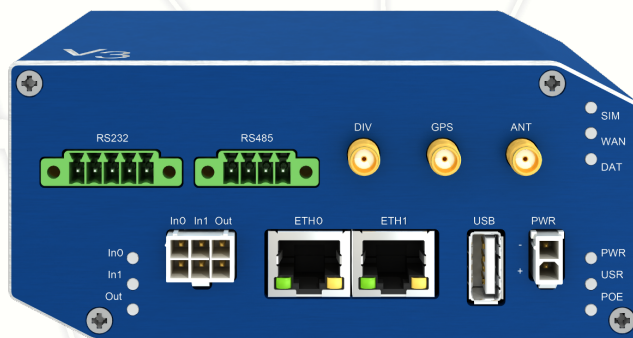


Configuration Manual

for v3 Routers



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.



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

Firmware version

Current version of firmware is 5.3.0 (October 9, 2015).

GPL licence

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

info@conel.cz.



Contents

1 Basic Information	1
2 Access to the Web Conf.	2
2.1 Preventing the domain disagreement message	3
3 Status	4
3.1 General Status	4
3.1.1 Mobile Connection	4
3.1.2 Primary LAN, Secondary LAN, Tertiary LAN, WiFi	5
3.1.3 Peripheral Ports	5
3.1.4 System Information	6
3.2 Mobile WAN Status	6
3.3 WiFi	9
3.4 WiFi Scan	10
3.5 Network Status	12
3.6 DHCP Status	14
3.7 IPsec Status	15
3.8 DynDNS status	15
3.9 System Log	16
4 Configuration	18
4.1 LAN Configuration	18
4.2 VRRP Configuration	23
4.3 Mobile WAN Configuration	26
4.3.1 Connection to Mobile Network	26
4.3.2 DNS Address Configuration	27
4.3.3 Check Connection to Mobile Network Configuration	27
4.3.4 Data Limit Configuration	28
4.3.5 Switch Between SIM Cards Configuration	29
4.3.6 PPPoE Bridge Mode Configuration	30
4.4 PPPoE Configuration	33
4.5 WiFi Configuration	34
4.6 WLAN Configuration	39
4.7 Backup Routes	41
4.8 Firewall Configuration	42
4.9 NAT Configuration	46
4.10 OpenVPN Tunnel Configuration	50
4.11 IPsec Tunnel Configuration	55
4.12 GRE Tunnels Configuration	60

4.13 L2TP Tunnel Configuration	63
4.14 PPTP Tunnel Configuration	65
4.15 DynDNS Client Configuration	67
4.16 NTP Client Configuration	68
4.17 SNMP Configuration	69
4.18 SMTP Configuration	73
4.19 SMS Configuration	74
4.19.1 Sending SMS	76
4.20 Expansion Port Configuration	80
4.21 USB Port Configuration	84
4.22 Startup Script	88
4.23 Up/Down Script	89
4.24 Automatic Update Configuration	90
5 Customization	92
5.1 User Modules	92
6 Administration	94
6.1 Users	94
6.2 Change Profile	95
6.3 Change Password	95
6.4 Set Real Time Clock	96
6.5 Set SMS Service Center Address	96
6.6 Unlock SIM Card	97
6.7 Send SMS	97
6.8 Backup Configuration	98
6.9 Restore Configuration	98
6.10 Update Firmware	98
6.11 Reboot	99
7 Configuration in Typ. Situations	100
7.1 Access to the Internet from LAN	100
7.2 Backed Up Access to the Internet from LAN	102
7.3 Secure Networks Interconnection or Using VPN	106
7.4 Serial Gateway	108
8 Recommended Literature	110

List of Figures

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

41	GRE tunnels configuration	61
42	GRE tunnel configuration	62
43	Topology of GRE tunnel configuration	62
44	L2TP tunnel configuration	63
45	Topology of example L2TP tunnel configuration	64
46	PPTP tunnel configuration	65
47	Topology of example PPTP tunnel configuration	66
48	Example of DynDNS configuration	67
49	Example of NTP configuration	68
50	Example of SNMP configuration	71
51	Example of the MIB browser	72
52	Example of the SMTP client configuration	73
53	Example 1 – SMS configuration	78
54	Example 2 – SMS configuration	78
55	Example 3 – SMS configuration	79
56	Example 4 – SMS configuration	79
57	Expansion port configuration	82
58	Example 1 – expansion port configuration	82
59	Example 2 – expansion port configuration	83
60	USB configuration	86
61	Example 1 – USB port configuration	86
62	Example 2 – USB port configuration	87
63	Startup script	88
64	Example of Startup script	88
65	Up/Down script	89
66	Example of Up/Down script	89
67	Example of automatic update 1	91
68	Example of automatic update 2	91
69	User modules	92
70	Added user module	92
71	Users	95
72	Change profile	95
73	Change password	96
74	Set real time clock	96
75	Set SMS service center address	96
76	Unlock SIM card	97
77	Send SMS	97
78	Restore configuration	98
79	Update Firmware	98
80	Reboot	99
81	Access to the Internet from LAN – topology of the example	100
82	Access to the Internet from LAN – LAN configuration	101
83	Access to the Internet from LAN – Mobile WAN configuration	101
84	Backed up access to the Internet – topology of the example	102

85	Backed up access to the Internet – <i>LAN</i> configuration	102
86	Backed up access to the Internet – <i>WLAN</i> configuration	103
87	Backed up access to the Internet – <i>WiFi</i> configuration	104
88	Backed up access to the Internet – <i>Mobile WAN</i> configuration	104
89	Backed up access to the Internet – <i>Backup Routes</i> configuration	105
90	Secure networks interconnection – topology of the example	106
91	Secure networks interconnection – <i>OpenVPN</i> configuration	107
92	Serial Gateway – topology of the example	108
93	Serial Gateway – konfigurace <i>Expansion Port 1</i>	109

List of Tables

1	Mobile Connection	4
2	PoE PSE information	5
3	Peripheral Ports	5
4	System Information	6
5	Mobile Network Information	7
6	Description of Periods	7
7	Mobile Network Statistics	7
8	Traffic Statistics	8
9	State Information about Access Point	9
10	State Information about Connected Clients	9
11	Information about Neighbouring WiFi Networks	10
12	Description of interface in network status	12
13	Description of Information in Network Status	13
14	DHCP status description	14
15	Configuration of the Network Interface	19
16	Configuration of Dynamic DHCP Server	19
17	Configuration of Static DHCP Server	19
18	VRRP configuration	23
19	Check connection	23
20	Mobile WAN connection configuration	26
21	Check connection to mobile network configuration	28
22	Data limit configuration	28
23	Default and backup SIM configuration	29
24	Switch between SIM card configurations	30
25	Switch between SIM card configurations	30
26	PPPoE configuration	33
27	WiFi configuration	37
28	WLAN configuration	39
29	Configuration of DHCP server	40
30	Backup Routes	42
31	Filtering of incoming packets	43
32	Forwarding filtering	44
33	NAT configuration	46
34	Configuration of send all incoming packets	46
35	Remote access configuration	47
36	Overview of OpenVPN tunnels	50
37	OpenVPN configuration	52
38	Example of OpenVPN configuration	54
39	Overview IPsec tunnels	55
40	IPsec tunnel configuration	57

41	Example IPsec configuration	60
42	Overview GRE tunnels	61
43	GRE tunnel configuration	61
44	Example GRE tunnel configuration	62
45	L2TP tunnel configuration	63
46	Example L2TP tunnel configuration	64
47	PPTP tunnel configuration	65
48	Example PPTP tunnel configuration	66
49	DynDNS configuration	67
50	NTP configuration	68
51	SNMP agent configuration	69
52	SNMPv3 configuration	69
53	SNMP configuration (R-SeeNet)	70
54	Object identifier for binary input and output	70
55	SMTP client configuration	73
56	Send SMS configuration	74
57	Control via SMS configuration	75
58	Control SMS	75
59	Send SMS on serial PORT1 configuration	76
60	Send SMS on serial PORT2 configuration	76
61	Send SMS on ethernet PORT1 configuration	76
62	List of AT commands	77
63	Expansion Port configuration – serial interface	81
64	Expansion Port configuration – <i>Check TCP connection</i>	81
65	CD signal description	81
66	DTR signal description	81
67	USB port configuration 1	84
68	USB PORT configuration 2	85
69	CD signal description	85
70	DTR signal description	85
71	Automatic update configuration	90
72	User modules	93
73	Users overview	94
74	Add User	94

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, combined Ethernet and serial lines with stronger insulation RS232-RS485-ETH. 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 (Virtual Private Network)
 - Serial Gateway (connection of serial devices to the Internet)

2. Access to the Web Configuration



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

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

SPECTRE v3 LTE Router

Status	General Status
General	Mobile Connection
Mobile WAN	SIM Card : Primary
WiFi	IP Address : Unassigned
WiFi Scan	State : Offline
Network	> More Information <
DHCP	Primary LAN
IPsec	IP Address : 10.40.28.66 / 255.255.252.0
DynDNS	MAC Address : 7C:66:9D:38:30:F0
System Log	Rx Data : 4.2 MB
	Tx Data : 140.8 KB
	Bridged : Yes
	> More Information <
	Secondary LAN
	IP Address : 10.40.28.66 / 255.255.252.0
	MAC Address : 7C:66:9D:38:30:F0
	Rx Data : 0 B
	Tx Data : 0 B
	Bridged : Yes
	> More Information <
	WiFi
	IP Address : Unassigned
	MAC Address : 78:A5:04:22:2A:67
	> More Information <
	Peripheral Ports
	Expansion Port 1 : RS-232
	Expansion Port 2 : RS-485
	Binary Input 0 : Off
	Binary Input 1 : Off
	Binary Output : Off
	System Information
	Firmware Version : 5.3.0 (2015-10-01) BETA #120
	Serial Number : N/A
	Profile : Standard
	Supply Voltage : 12.0 V
	Temperature : 38 °C
	Time : 2000-05-16 00:57:08
	Uptime : 0 days, 0 hours, 39 minutes

Figure 1: Example of the web configuration

When you successfully enter login information on the login page, web interface will be displayed. The left side of the web interface displays the menu. You will find links for the *Status*, *Configuration*, *Customization* and *Administration* of the router.

Name and *Location* displays the router's name, location and SNMP configuration (see 4.17). These fields are user-defined for each router.



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

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

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 or RS232-RS485-ETH 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 (<i>Primary</i> or <i>Secondary</i>)
Interface	Defines the interface
Flags	Displays network interface flags
IP Address	IP address of the interface
MTU	Maximum packet size that the equipment is able to transmit
Rx Data	Total number of received bytes
Rx Packets	Received packets
Rx Errors	Erroneous received packets
Rx Dropped	Dropped received packets
Rx Overruns	Lost received packets because of overload
Tx Data	Total number of sent bytes
Tx Packets	Sent packets
Tx Errors	Erroneous sent packets
Tx Dropped	Dropped sent packets
Tx Overruns	Lost sent packets because of overload
Uptime	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 4.5). If the router is equipped with PoE PSE board, there are also information about it in the *Primary LAN* or *Secondary LAN* section (see table below for description).

Item	Description
PoE PSE Status	<ul style="list-style-type: none"> • Disabled – PoE PSE is disabled in the <i>Primary LAN</i> or <i>Secondary LAN</i> configuration form. • Undervoltage – Undervoltage, i.e. a lower voltage than the nominal operating voltage. • Overcurrent – Overcurrent, i.e. a higher current than the permissible positive difference of the nominal current. • Idle – PoE PSE is enabled, but currently not used. • Class 0 – Power level (classification unimplemented) • Class 1 – Power level (very low power) • Class 2 – Power level (low power) • Class 3 – Power level (mid power) • Class 4 – Power level (high power)
PoE PSE Power	Power of PoE PSE [W]
PoE PSE Voltage	Voltage of PoE PSE [V]
PoE PSE Current	Current of PoE PSE [mA]

Table 2: PoE PSE information

3.1.3 Peripheral Ports

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

Table 3: 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 4: 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
Channel	Channel the router communicates on
Signal Strength	Signal strength of the selected cell
Signal Quality	Signal quality of the selected cell: <ul style="list-style-type: none"> • EC/IO for UMTS and CDMA (it's the ratio of the signal received from the pilot channel – EC – to the overall level of the spectral density, ie the sum of the signals of other cells – IO) • RSRQ for LTE technology (Defined as the ratio $\frac{N \times RSRP}{RSSI}$) • The value is not available for the EDGE technology

Continued on next page

Continued from previous page

Item	Description
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 5: 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 6: 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 7: 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 8: 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

Signal Min : -108 dBm

Signal Avg : -71 dBm

Signal Max : -65 dBm

Cells : 15

Availability : 99.7%

Yesterday -121 dBm

Yesterday -71 dBm

Yesterday -65 dBm

Yesterday 261

Yesterday 99.7%

This Week -121 dBm

This Week -71 dBm

This Week -65 dBm

This Week 525

This Week 99.7%

Last Week -121 dBm

Last Week -69 dBm

Last Week -63 dBm

Last Week 206

Last Week 99.7%

This Period -121 dBm

This Period -70 dBm

This Period -63 dBm

This Period 730

This Period 99.7%

Last Period -121 dBm

Last Period -85 dBm

Last Period -58 dBm

Last Period 962

Last Period 97.5%

Traffic Statistics for Primary SIM card

Rx Data : 12 KB

Tx Data : 13 KB

Connections : 2

Yesterday 21 KB

Yesterday 19 KB

Yesterday 7

This Week 19402 KB

This Week 5167 KB

This Week 20

Last Week 6366 KB

Last Week 3382 KB

Last Week 36

This Period 25768 KB

This Period 8549 KB

This Period 56

Last Period 18868 KB

Last Period 3726 KB

Last Period 49

Traffic Statistics for Secondary SIM card

Rx Data : 0 KB

Tx Data : 0 KB

Connections : 0

Yesterday 0 KB

Yesterday 0 KB

Yesterday 0

This Week 0 KB

This Week 0 KB

This Week 0

Last Week 0 KB

Last Week 0 KB

Last Week 0

This Period 0 KB

This Period 0 KB

This Period 0

Last Period 0 KB

Last Period 0 KB

Last Period 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 9: 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 10: 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 <i>Supported rates</i> item
RSN	Robust Secure Network – The protocol for establishing a secure communication through wireless network 802.11

Table 11: Information about Neighbouring WiFi Networks

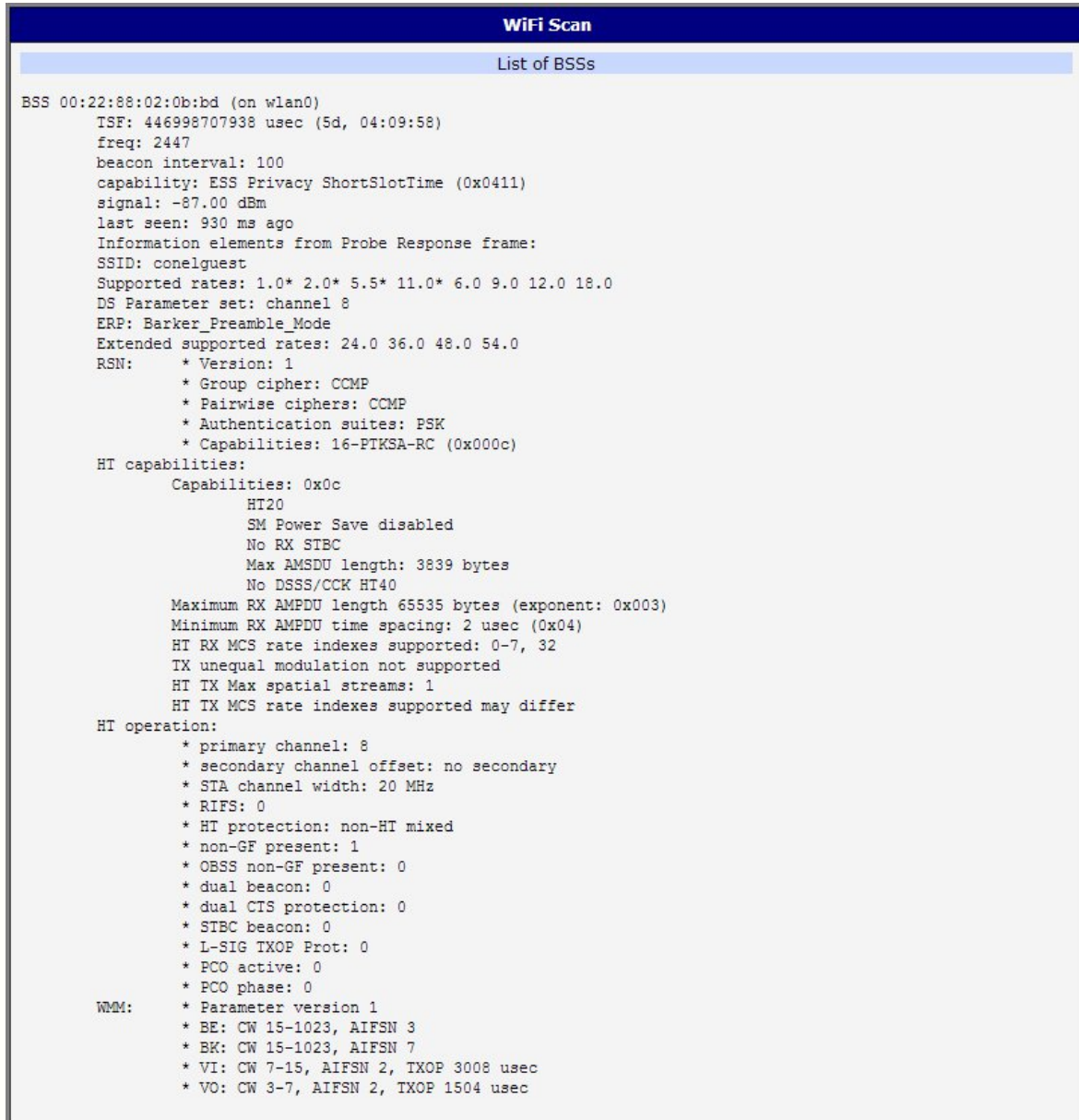


Figure 4: WiFi Scan

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 12: 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 through
RX	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 13: 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.

Network Status

Interfaces

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)

Route Table

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 14: 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.

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

Figure 7: IPsec Status

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 Status	
Last DynDNS Update Status	
<pre> DynDNS record successfully updated. </pre>	

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 daemon 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.

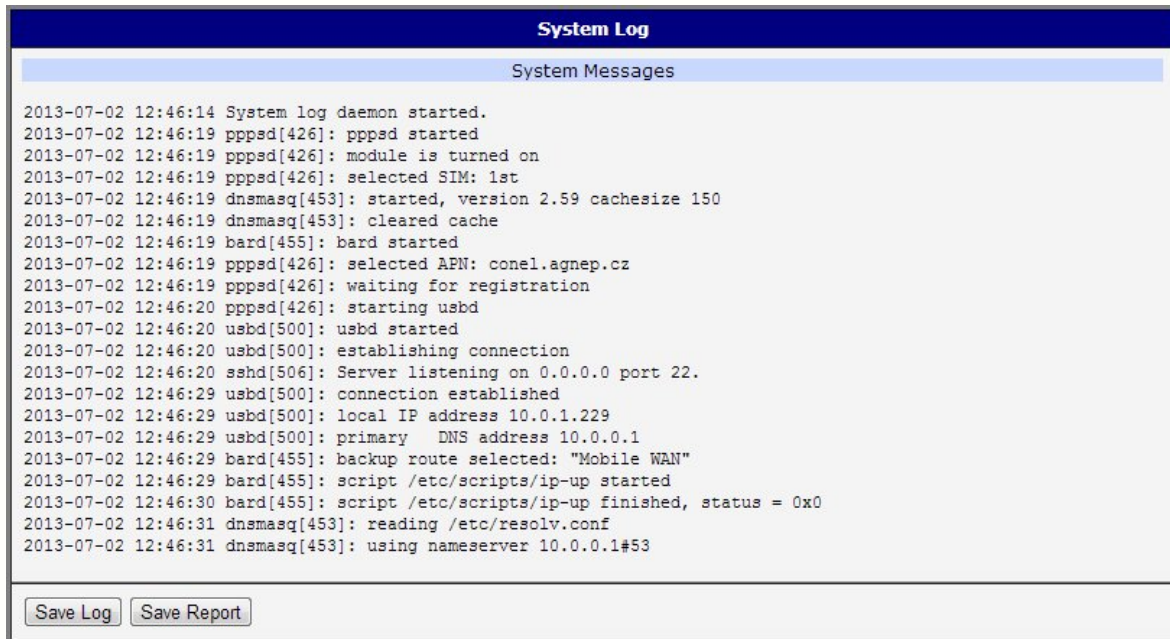


Figure 9: System Log

Example of logging into the remote daemon at 192.168.2.115:

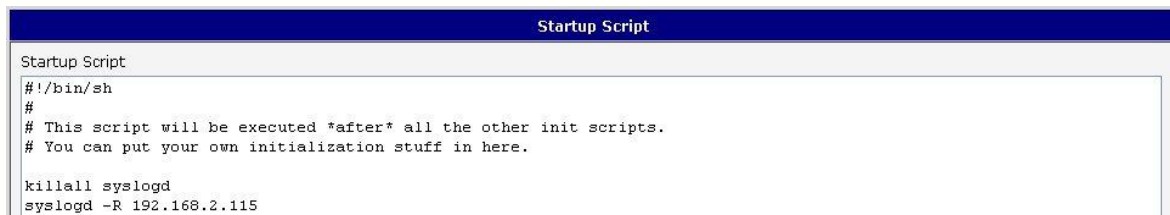


Figure 10: Example program syslogd start with the parameter -r

4. Configuration

4.1 LAN Configuration

Select the *LAN* menu item to enter the network configuration for the Ethernet ports. *Primary* subitem is intended for the first ETH router's interface (ETH0), *Secondary* is for the second ETH router's interface (ETH1). *Tertiary LAN* is for the SWITCH (3x Ethernet) or RS232-RS485-ETH expansion port if installed, it is the ETH2 interface.

Item	Description
DHCP Client	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • no – router is not used as a bridge (default) • yes – router is used as a bridge
Media type	<ul style="list-style-type: none"> • Auto-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.
PoE PSE	<ul style="list-style-type: none"> • enabled – The router provides power on the Ethernet cable • disabled – The router does not provide power on the Ethernet cable (default)

Continued on next page

Continued from previous page

Item	Description
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 address.
DNS server	IP address of DNS server of the router. All the DNS queries are forwarded to this address.

Table 15: Configuration of the Network Interface

The *Default Gateway* and *DNS Server* items are only used if the *DHCP Client* item is disabled, and if the Primary or Secondary LAN is selected by the Backup Routes system as a default route. (The backup routes selection algorithm is described in in section 4.7 *Backup Routes*). Since FW 5.3.0, *Default Gateway* and *DNS Server* are also supported on bridged interfaces (e.g. eth0 + eth1).

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

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

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

Item	Description
Enable dynamic DHCP leases	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 16: 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 17: Configuration of Static DHCP Server



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

Example 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).

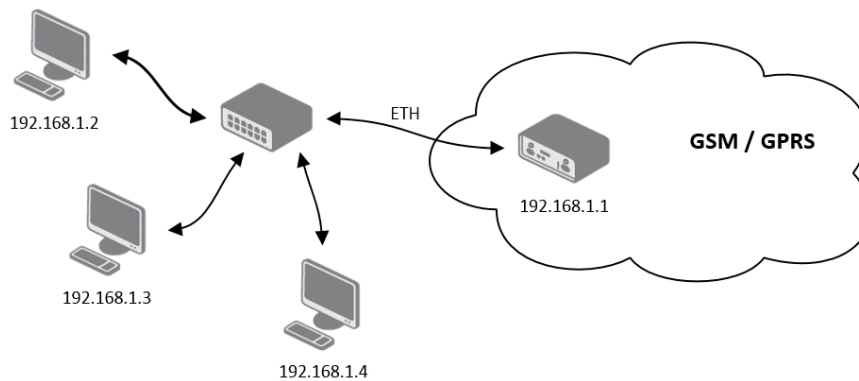


Figure 11: Example 1 – Network Topology for Dynamic DHCP Server

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

Figure 12: Example 1 – LAN Configuration Page

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.

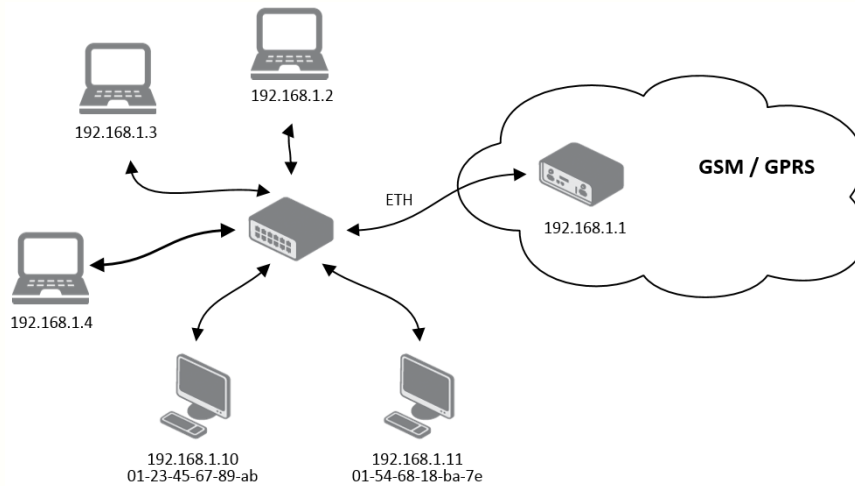


Figure 13: Example 2 – Network Topology with both Static and Dynamic DHCP Servers

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

Figure 14: Example 2 – LAN Configuration Page

Example 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

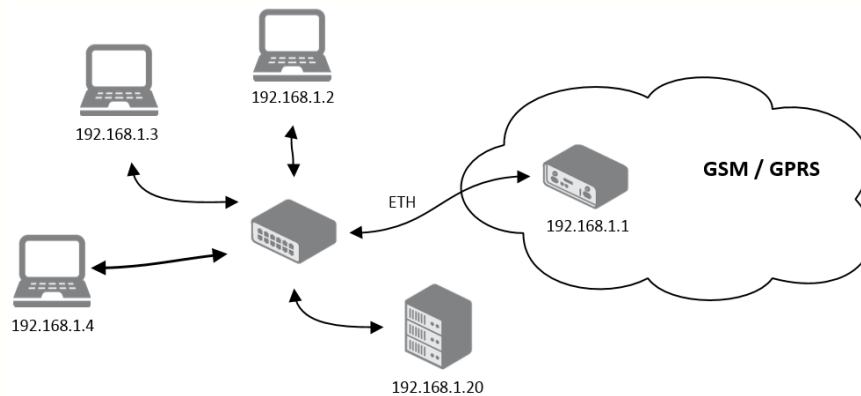


Figure 15: Example 3 – Network Topology

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

Figure 16: Example 3 – LAN Configuration Page

4.2 VRRP Configuration

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


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

Table 18: VRRP configuration

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

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

Table 19: Check connection

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

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

Example of the VRRP protocol:

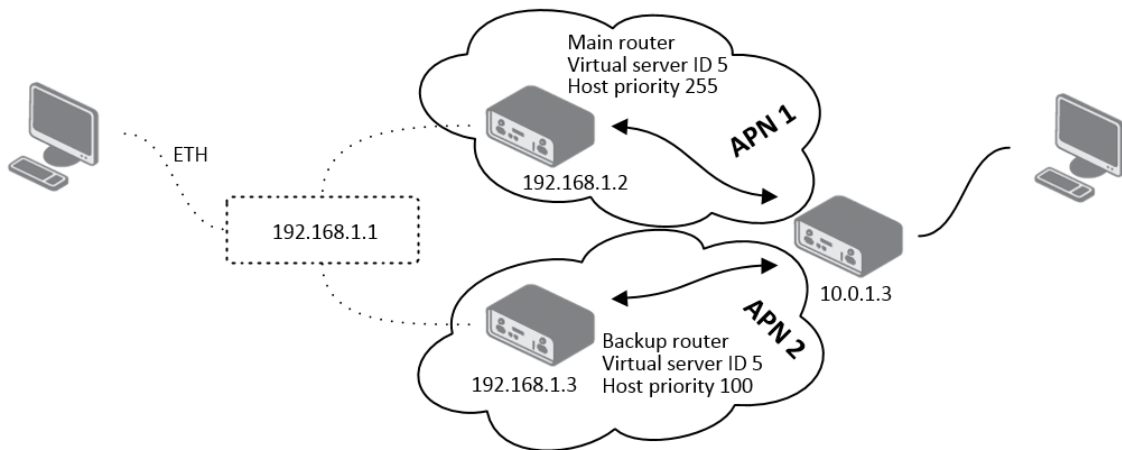


Figure 17: Topology of example VRRP configuration

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

Figure 18: Example of VRRP configuration – main router

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

Figure 19: Example of VRRP configuration – backup router

4.3 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.

4.3.1 Connection to Mobile Network

If the *Create connection to mobile network* item is selected, the router automatically tries to establish connection after switching-on. 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: <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Automatic selection – router automatically selects transmission method according to the availability of transmission technology • <i>Furthermore, according to the type of router</i> – it's also possible to select a specific method of data transmission (GPRS, UMTS, ...)
PIN	PIN parameter should be set only if it requires a SIM card router. SIM card is blocked 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 20: 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.

4.3.2 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 operator* 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).

4.3.3 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 21: 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.

4.3.4 Data Limit Configuration

Item	Description
Data limit	With this parameter you can set the maximum expected amount of data transmitted (sent and received) over GPRS in one billing period (month).
Warning Threshold	Parameter <i>Warning Threshold</i> 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 <i>Router has exceeded (value of Warning Threshold) of data limit</i> .
Accounting Start	Parameter sets the day of the month in which the billing cycle starts SIM card used. Start of the billing period defines the operator, which gives the SIM card. The router begin to count the transferred data since that day.

Table 22: 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.

4.3.5 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 23: 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 24: 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 25: 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).

4.3.6 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 allotted to PC.

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

Mobile WAN Configuration			
<input checked="" type="checkbox"/> Create connection to mobile network			
	Primary SIM card	Secondary SIM card	
APN *	<input type="text" value="conel.agnep.cz"/>	<input type="text"/>	
Username *	<input type="text"/>	<input type="text"/>	
Password *	<input type="text"/>	<input type="text"/>	
Authentication	<input type="text" value="PAP or CHAP"/>	<input type="text" value="PAP or CHAP"/>	
IP Address *	<input type="text"/>	<input type="text"/>	
Phone Number *	<input type="text"/>	<input type="text"/>	
Operator *	<input type="text"/>	<input type="text"/>	
Network Type	<input type="text" value="automatic selection"/>	<input type="text" value="automatic selection"/>	
PIN *	<input type="text"/>	<input type="text"/>	
MRU	<input type="text" value="1500"/>	<input type="text" value="1500"/>	bytes
MTU	<input type="text" value="1500"/>	<input type="text" value="1500"/>	bytes
DNS Settings	<input type="text" value="get from operator"/>	<input type="text" value="get from operator"/>	
DNS Server	<input type="text"/>	<input type="text"/>	
<i>(The feature of check connection to mobile network is necessary for uninterrupted operation)</i>			
Check Connection	<input type="text" value="disabled"/>	<input type="text" value="disabled"/>	
Ping IP Address	<input type="text" value="99.98.97.96"/>	<input type="text"/>	
Ping Interval	<input type="text" value="10"/>	<input type="text"/> sec	
<input type="checkbox"/> Enable traffic monitoring			
Data Limit	<input type="text"/>	MB	
Warning Threshold	<input type="text"/>	%	
Accounting Start	<input type="text" value="1"/>		
Default SIM card	<input type="text" value="secondary"/>		
Backup SIM card	<input type="text" value="primary"/>		
<input type="checkbox"/> Switch to other SIM card when connection fails <input type="checkbox"/> Switch to backup SIM card when roaming is detected and switch to default SIM card when home network is detected <input type="checkbox"/> Switch to backup SIM card when data limit is exceeded and switch to default SIM card when data limit isn't exceeded <input type="checkbox"/> Switch to backup SIM card when binary input is active and switch to default SIM card when binary input isn't active <input type="checkbox"/> Switch to default SIM card after timeout			
Initial Timeout	<input type="text" value="60"/>	min	
Subsequent Timeout *	<input type="text"/>	min	
Additive Constant *	<input type="text"/>	min	
<input type="checkbox"/> Enable PPPoE bridge mode			
* can be blank			
<input type="button" value="Apply"/>			

Figure 20: Mobile WAN configuration

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

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

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

☒ Enable traffic monitoring

Figure 21: Example 1 – Mobile WAN configuration

Example 2: The following configuration illustrates the situation in which the router switches to a backup SIM card after exceeding the data limits of 800 MB. 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 22: 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 23: Example 3 – Mobile WAN configuration

4.4 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.

Figure 24: PPPoE configuration

Item	Description
Username	Username for secure access to PPPoE
Password	Password for secure access to PPPoE
Authentication	Authentication protocol in GSM network <ul style="list-style-type: none"> • PAP or CHAP – authentication method is chosen by router • PAP – 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 receive 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 26: PPPoE configuration



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

4.5 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	<p>WiFi operating mode:</p> <ul style="list-style-type: none"> • access point (AP) – router becomes an access point to which other devices in <i>station (STA)</i> mode can be 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	<p>Method of broadcasting the unique identifier of SSID network in beacon frame and type of response to a request for sending the beacon frame.</p> <ul style="list-style-type: none"> • Enabled – SSID is broadcasted in beacon frame • Zero length – Beacon frame does not include SSID. Requests for sending beacon frame are ignored. • Clear – 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 <i>station (STA)</i> mode)
Country Code	<p>Code of the country, where the router is used with WiFi. This code must be entered in format ISO 3166-1 alpha-2. If <i>country code</i> isn't specified and the router has implemented no system to determine this code, it is used "US" as default <i>country code</i>.</p> <p>If no <i>country code</i> 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.</p>

Continued on next page

Continued from previous page

Item	Description
HW Mode	<p>HW mode of WiFi standard the access point (AP) will support.</p> <ul style="list-style-type: none"> • IEE 802.11b • IEE 802.11b+g • IEE 802.11b+g+n • IEE 802.11a • IEE 802.11a+n
Channel	<p>Channel where the WiFi AP is transmitting. Channels 12, 13 and 14 can be selected only in countries where they are allowed on the basis of country code.</p>
BW 40 MHz	<p>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.</p>
WMM	<p>Enables basic QoS for WiFi networks. This version doesn't guarantee network throughput. It is suitable for simple applications requiring QoS.</p>
Authentication	<p>Provides access control of authorized users in WiFi network:</p> <ul style="list-style-type: none"> • Open – authentication is not required (free access point) • Shared – base authentication using WEP key • WPA-PSK – authentication using better authentication method PSK-PSK • WPA2-PSK – authentication using AES encryption
Encryption	<p>Type of data encryption in WiFi network:</p> <ul style="list-style-type: none"> • None – No data encryption • WEP – Encryption using static WEP keys. This encryption can be used for <i>Shared</i> authentication. • TKIP – Dynamic management of encryption keys which can be used for <i>WPA-PSK</i> and <i>WPA2-PSK</i> authentication. • AES – Improved encryption used for <i>WPA2-PSK</i> authentication

Continued on next page

Continued from previous page

Item	Description
WEP Key Type	Type of WEP key for WEP encryption: <ul style="list-style-type: none"> • ASCII – WEP key is entered in ASCII format • HEX – WEP key is entered in hexadecimal format
WEP Default Key	Specifies default WEP key
WEP Key 1-4	Items for different four WEP keys <ul style="list-style-type: none"> • WEP key in ASCII format must be entered in quotes and must have the following lengths: <ul style="list-style-type: none"> – 5 ASCII characters (40b WEP key) – 13 ASCII characters (104b WEP key) – 16 ASCII characters (128b WEP key) • WEP key in hexadecimal format must be entered using only hexadecimal digits and must the following lengths: <ul style="list-style-type: none"> – 10 hexadecimal digits (40b WEP key) – 26 hexadecimal digits (104b WEP key) – 32 hexadecimal digits (128b WEP key)
WPA PSK Type	The type of encryption when WPA-PSK authenticating: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 256-bit secret – 64 hexadecimal digits • ASCII passphrase – from 8 to 63 characters which are subsequently converted into PSK • PSK File – absolute path to the file containing the list of pairs (PSK key, MAC address)

Continued on next page

Continued from previous page

Item	Description
Access List	<p>Determines a manner of Access/Deny list application:</p> <ul style="list-style-type: none"> • 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	<p>Accept or Deny list of client MAC addresses that set network access. Each MAC address is separated by new line.</p>
Syslog Level	<p>Communicativeness level when system writes to the system log</p> <ul style="list-style-type: none"> • 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	<p>Allows user to define additional parameters</p>

Table 27: 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 25: WiFi configuration

4.6 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	<p>WiFi operating mode:</p> <ul style="list-style-type: none"> • access point (AP) – router becomes an access point to which other devices in <i>station (STA)</i> mode can be 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	<p>Activates bridge mode:</p> <ul style="list-style-type: none"> • 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 28: 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 29: Configuration of DHCP server

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

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

Figure 26: WLAN configuration

4.7 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 4.3.1.

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

Figure 27: Backup Routes

If *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 30: Backup Routes

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

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

Table 31: Filtering of incoming packets

The 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 allowed 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: <ul style="list-style-type: none"> • all – access is enabled for all protocols • TCP – access is enabled for TCP protocol • UDP – access is enabled for UDP protocol • ICMP – access is enabled for ICMP protocol
Target Port	The port number on which access to the router is allowed

Continued on next page

Continued from previous page

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

Table 32: Forwarding filtering

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 destined 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
<input type="text"/>	all ▼	<input type="text"/>	allow ▼
<input type="text"/>	all ▼	<input type="text"/>	allow ▼
<input type="text"/>	all ▼	<input type="text"/>	allow ▼
<input type="text"/>	all ▼	<input type="text"/>	allow ▼
<input type="text"/>	all ▼	<input type="text"/>	allow ▼
<input type="text"/>	all ▼	<input type="text"/>	allow ▼
<input type="text"/>	all ▼	<input type="text"/>	allow ▼
<input type="text"/>	all ▼	<input type="text"/>	allow ▼
<input type="text"/>	all ▼	<input type="text"/>	allow ▼

☐ Enabled filtering of forwarded packets

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

☐ Enable filtering of locally destined packets

☐ Enable protection against DoS attacks

* can be blank

Apply

Figure 28: Firewall configuration

Example of the firewall configuration:

The router has allowed the following access:

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

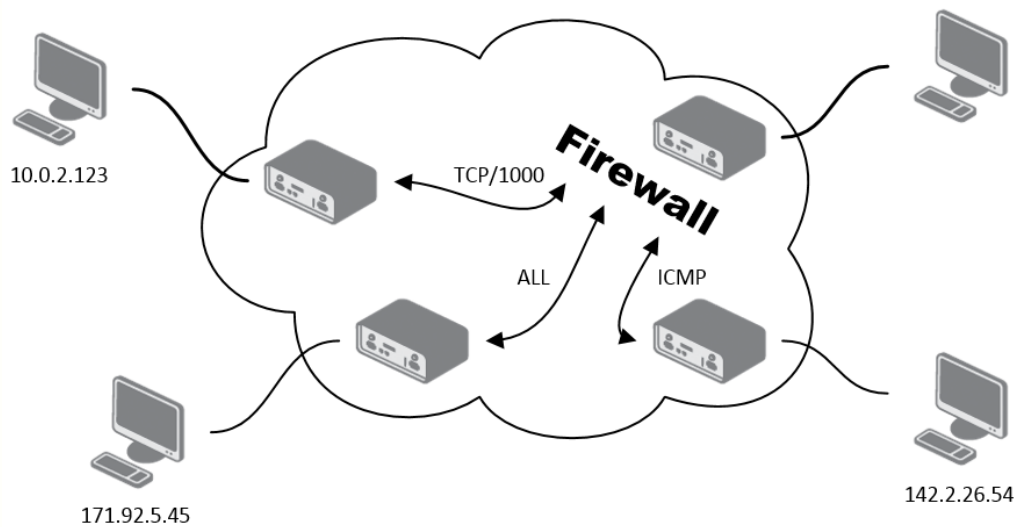


Figure 29: Topology of example firewall configuration

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

Figure 30: Example firewall configuration

4.9 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 33: 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 34: 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 35: Remote access configuration

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

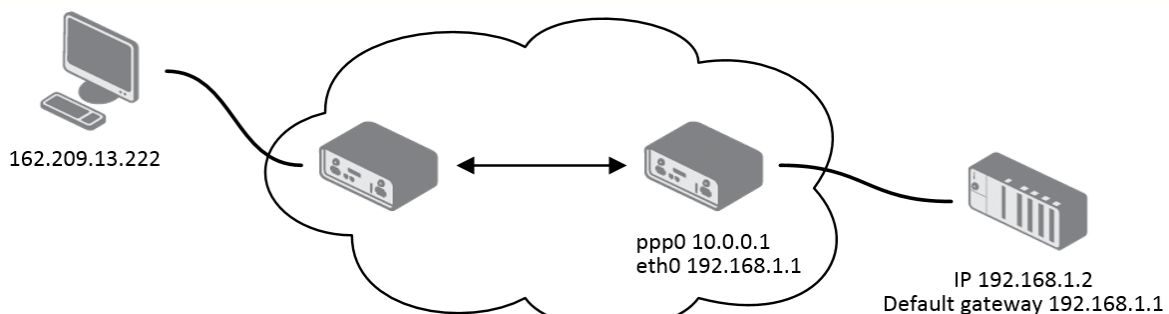


Figure 31: Example 1 – Topology of NAT configuration

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 ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	

☐ Enable remote HTTP access on port

☐ Enable remote HTTPS access on port

☐ Enable remote SSH access on port

☒ Enable remote SNMP access on port

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

☒ Masquerade outgoing packets

Figure 32: Example 1 – NAT configuration

In these configurations it is important to have marked choice of *Send all remaining incoming packets to 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.

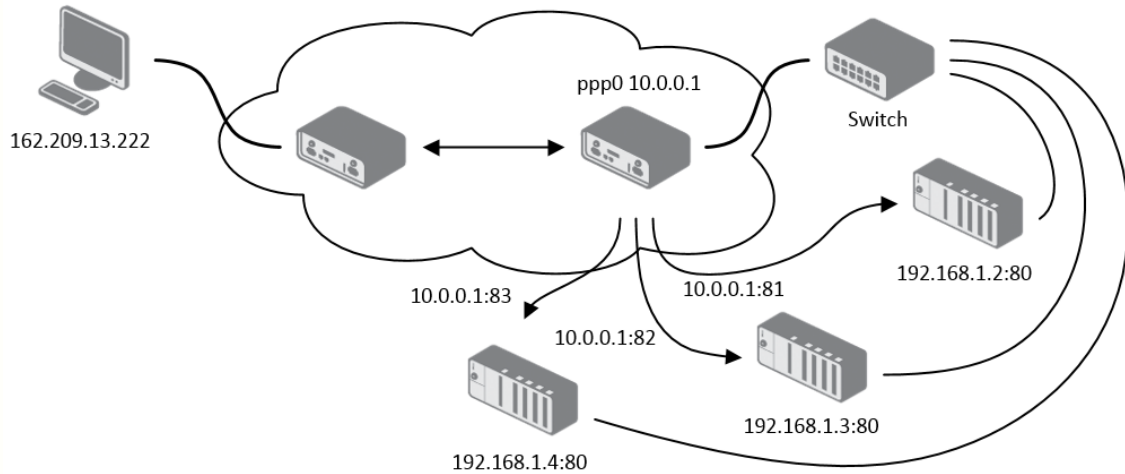


Figure 33: Example 2 – topology of NAT configuration

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 ▼	
		TCP ▼	

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

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

☒ Masquerade outgoing packets

Figure 34: Example 2 – NAT configuration

In this example there is 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.

4.10 OpenVPN Tunnel Configuration

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

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

Table 36: Overview of OpenVPN tunnels

Figure 35: OpenVPN tunnels configuration

Item	Description
Description	Description (or name) of tunnel
Protocol	<p>Protocol by which the tunnel will communicate.</p> <ul style="list-style-type: none"> • UDP – OpenVPN will communicate using UDP • TCP server – OpenVPN will communicate using TCP in server mode • TCP client – OpenVPN will communicate using TCP in client mode

Continued on next page

Continued from previous page

Item	Description
UDP/TCP port	Port by which the tunnel will communicate.
Remote IP Address	IP address of opposite tunnel side (domain name can be used).
Remote Subnet	Network IP address of the opposite side of the tunnel.
Remote Subnet Mask	Subnet mask of the opposite side of the tunnel.
Redirect Gateway	Allows to redirect all traffic on Ethernet
Local Interface IP Address	IP address of the local side of tunnel.
Remote Interface IP Address	IP address of interface local side of tunnel.
Ping Interval	Parameter (in seconds) defines how often the router will send a message to the remote end to verify that the tunnel is still connected.
Ping Timeout	Parameter which defines how long the router will wait for a response to the ping (in seconds). <i>Ping Timeout</i> must be larger than <i>Ping Interval</i> .
Renegotiate Interval	Sets renegotiate period (reauthorization) of the OpenVPN tunnel. This parameter can be set only when <i>Authenticate Mode</i> is set to <i>username/password</i> or <i>X.509 certificate</i> . After this time period, the router changes the tunnel encryption to ensure the continued safety of the tunnel.
Max Fragment Size	Defines maximum packet size
Compression	Data compression: <ul style="list-style-type: none"> • none – No compression is used. • LZO – Lossless LZO compression. Compression has to be selected on both tunnel ends.
NAT Rules	Applies NAT rules to the OpenVPN tunnel: <ul style="list-style-type: none"> • not applied – NAT rules are not applied to the OpenVPN tunnel. • applied – NAT rules are applied to the OpenVPN tunnel.

Continued on next page

Continued from previous page

Item	Description
Authenticate Mode	<p>Sets authentication mode:</p> <ul style="list-style-type: none"> • none – no authentication is set • Pre-shared secret – sets the shared key for both sides of the tunnel • Username/password – enables authentication using <i>CA Certificate</i>, <i>Username</i> and <i>Password</i> • X.509 Certificate (multiclient) – enables X.509 authentication in multiclient mode • X.509 Certificate (client) – enables X.509 authentication in client mode • X.509 Certificate (server) – enables X.509 authentication in server mode
Pre-shared Secret	Authentication using pre-shared secret can be used for all offered authentication mode.
CA Certificate	Auth. using CA Certificate can be used for username/password and X.509 Certificate modes.
DH Parameters	Protocol for exchange key DH parameters can be used for X.509 Certificate authentication in server mode.
Local Certificate	This authentication certificate can be used for X.509 Certificate authentication mode.
Local Private Key	Local private key can be used for X.509 certificate auth. mode.
Username	Authentication using a login name and password authentication can be used for username/password mode.
Password	Authentication using a login name and password authentication can be used for username/password mode.
Extra Options	Defines additional parameters of OpenVPN tunnel such as DHCP options etc. Parameters are introduced by two dashes. For possible parameters see the <i>Help</i> in the router via SSH – run the <code>openvpnd --help</code> command.

Table 37: OpenVPN configuration

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

OpenVPN Tunnel Configuration

☐ Create 1st OpenVPN tunnel

Description *
 Protocol
 UDP port
 Remote IP Address *
 Remote Subnet *
 Remote Subnet Mask *
 Redirect Gateway
 Local Interface IP Address
 Remote Interface IP Address
 Ping Interval *
 Ping Timeout *
 Renegotiate Interval *
 Max Fragment Size *
 Compression
 NAT Rules
 Authenticate Mode

UDP

1194

no

sec

sec

sec

bytes

LZO

not applied

none

Pre-shared Secret

 CA Certificate

 DH Parameters

 Local Certificate

 Local Private Key

 Username
 Password
 Extra Options *
* can be blank

Apply

Figure 36: OpenVPN tunnel configuration

Example of the OpenVPN tunnel configuration:

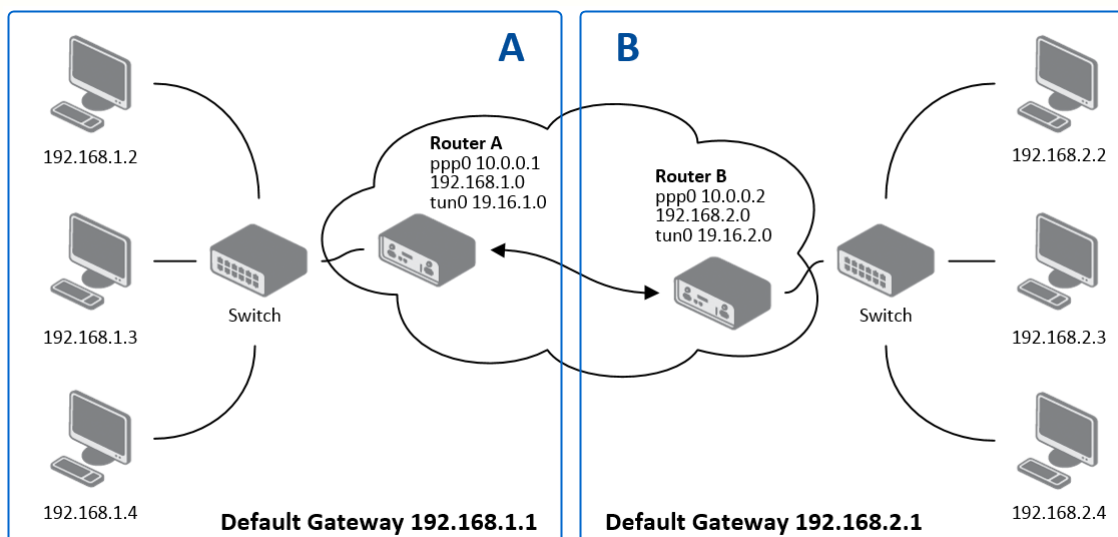


Figure 37: Topology of OpenVPN configuration example

OpenVPN tunnel configuration:

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

Table 38: Example of OpenVPN configuration

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

4.11 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 39: Overview IPsec tunnels

Figure 38: 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: <i>hostname</i> and <i>domain-name</i> (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 <i>protocol/port</i> , for example 17/1701 for UDP (protocol 17) and port 1701. It is also possible to enter only the number of protocol, however, the above mentioned format is preferred.
Local ID	Identifier (ID) of local side of the tunnel. It consists of two parts: <i>hostname</i> and <i>domain-name</i> (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 Protocol/Port of a local network. The general form is <i>protocol/port</i> , for example 17/1701 for UDP (protocol 17) and port 1701. It is also possible to enter only the number of protocol, however, the above mentioned format is preferred.
Encapsulation Mode	IPsec mode (the method of encapsulation) – choose <i>tunnel</i> (entire IP datagram is encapsulated) or <i>transport</i> (only IP header).
NAT traversal	If address translation is used between two end points of the tunnel, it needs to enable <i>NAT Traversal</i> .
IKE Mode	Defines mode for establishing connection (<i>main</i> or <i>aggressive</i>). If the aggressive mode is selected, establishing of IPsec tunnel will be faster, but encryption will set permanently on 3DES-MD5. We recommend not to use aggressive mode due to a lower security!
IKE Algorithm	Way of algorithm selection: <ul style="list-style-type: none"> • auto – encryption and hash alg. are selected automatically • manual – encryption and hash alg. are defined by the user
IKE Encryption	Encryption algorithm – 3DES, AES128, AES192, AES256
IKE Hash	Hash algorithm – MD5, SHA1, SHA256, SHA384 or SHA512
IKE DH Group	Diffie-Hellman groups determine the strength of the key used in the key exchange process. Higher group numbers are more secure, but require additional time to compute the key. Group with higher number provides more security, but requires more processing time.
ESP Algorithm	Way of algorithm selection: <ul style="list-style-type: none"> • auto – encryption and hash alg. are selected automatically • manual – encryption and hash alg. are defined by the user
ESP Encryption	Encryption algorithm – DES, 3DES, AES128, AES192, AES256
ESP Hash	Hash algorithm – MD5, SHA1, SHA256, SHA384 or SHA512
PFS	Ensures that derived session keys are not compromised if one of the private keys is compromised in the future
PFS DH Group	Diffie-Hellman group number (see <i>IKE DH Group</i>)
Key Lifetime	Lifetime key data part of tunnel. The minimum value of this parameter is 60 s. The maximum value is 86400 s.

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 Rekey Margin time
DPD Delay	Time after which the IPsec tunnel functionality is tested
DPD Timeout	The period during which device waits for a response
Authenticate Mode	Using this parameter can be set authentication: <ul style="list-style-type: none"> • 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 40: 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	
<input type="checkbox"/> Create 1st IPsec tunnel	
Description *	<input type="text"/>
Remote IP Address *	<input type="text"/>
Remote ID *	<input type="text"/>
Remote Subnet *	<input type="text"/>
Remote Subnet Mask *	<input type="text"/>
Remote Protocol/Port *	<input type="text"/>
Local ID *	<input type="text"/>
Local Subnet *	<input type="text"/>
Local Subnet Mask *	<input type="text"/>
Local Protocol/Port *	<input type="text"/>
Encapsulation Mode	tunnel ▼
NAT Traversal	disabled ▼
IKE Mode	main ▼
IKE Algorithm	auto ▼
IKE Encryption	3DES ▼
IKE Hash	MD5 ▼
IKE DH Group	2 ▼
ESP Algorithm	auto ▼
ESP Encryption	DES ▼
ESP Hash	MD5 ▼
PFS	disabled ▼
PFS DH Group	2 ▼
Key Lifetime	3600 sec
IKE Lifetime	3600 sec
Rekey Margin	540 sec
Rekey Fuzz	100 %
DPD Delay *	<input type="text"/> sec
DPD Timeout *	<input type="text"/> sec
Authenticate Mode	pre-shared key ▼
Pre-shared Key	<input type="text"/>
CA Certificate	<input type="text"/>
Remote Certificate	<input type="text"/>
Local Certificate	<input type="text"/>
Local Private Key	<input type="text"/>
Local Passphrase *	<input type="text"/>
Extra Options *	<input type="text"/>
* can be blank	
<input type="button" value="Apply"/>	

Figure 39: IPsec tunnels configuration

Example of the IPsec Tunnel configuration:

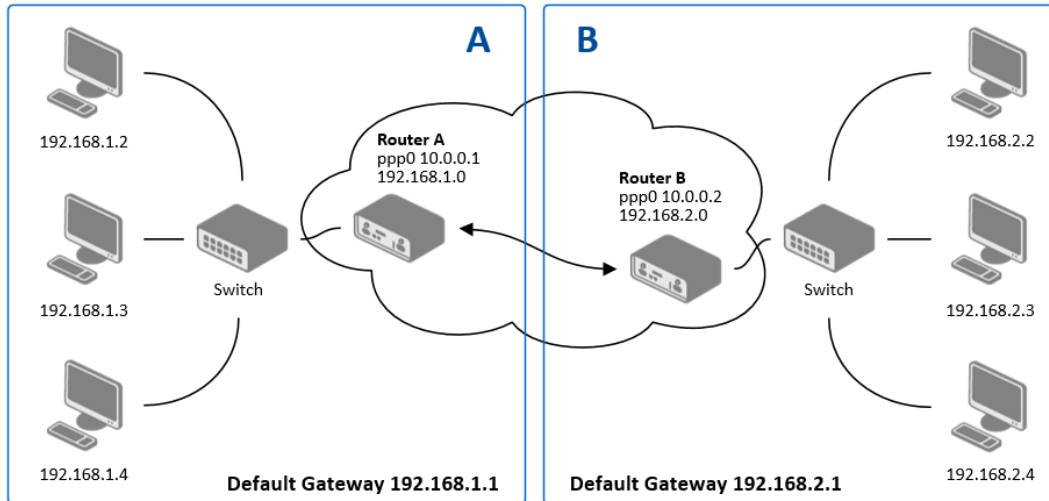


Figure 40: Topology of example IPsec configuration

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 41: Example IPsec configuration



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

4.12 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 42: Overview GRE tunnels

Figure 41: 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: <ul style="list-style-type: none"> • disabled – multicast disabled • enabled – multicast enabled
Pre-shared Key	An optional value that defines the 32 bit shared key in numeric format, 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 43: 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 ▼

Pre-shared Key *

* can be blank

Figure 42: GRE tunnel configuration

Example of the GRE Tunnel configuration:

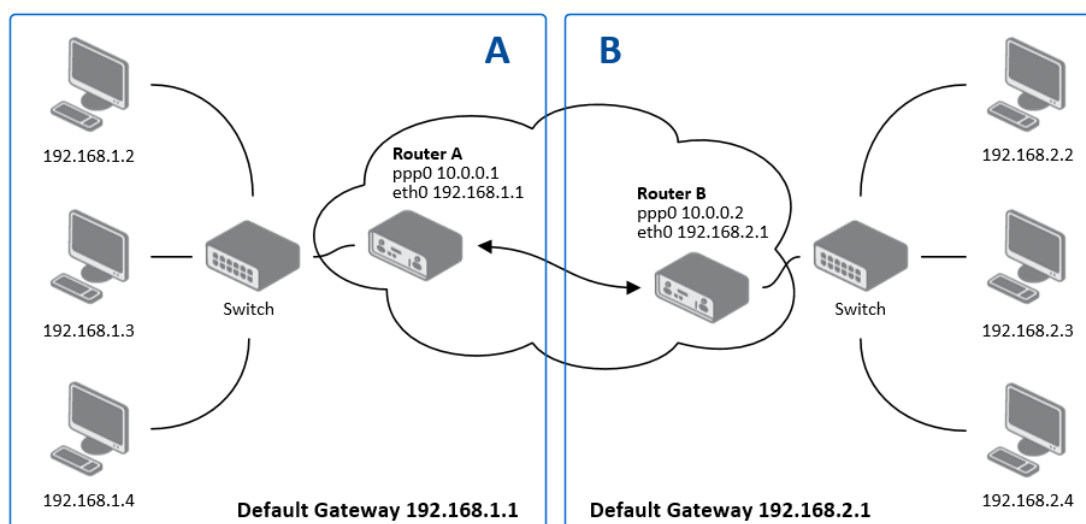


Figure 43: Topology of GRE tunnel configuration

GRE tunnel configuration:

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

Table 44: Example GRE tunnel configuration

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

4.13 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: <ul style="list-style-type: none"> • 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 45: L2TP tunnel configuration

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

Figure 44: L2TP tunnel configuration

Example of the L2TP Tunnel configuration:

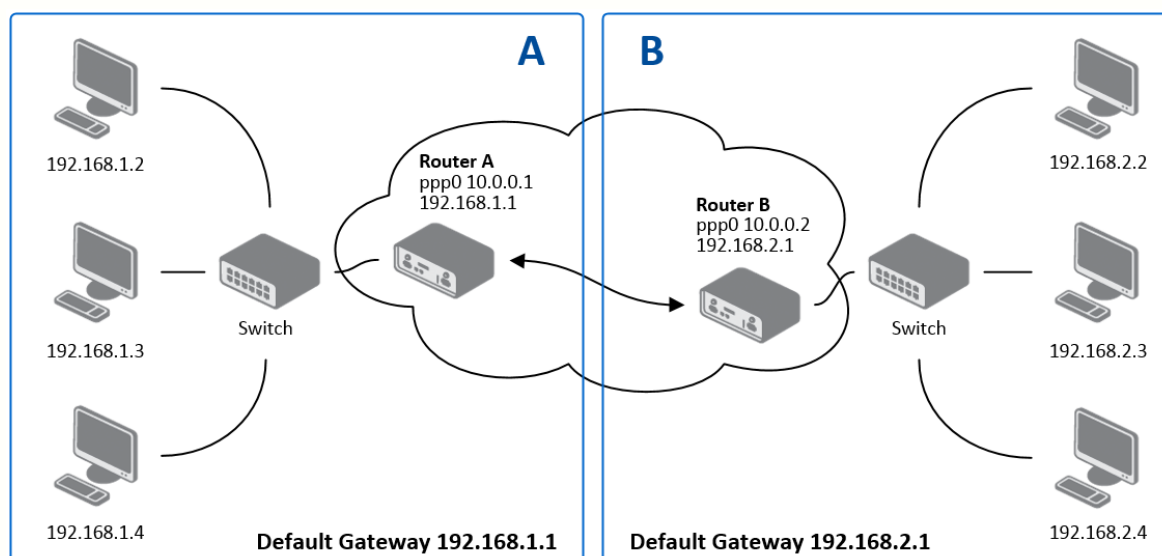


Figure 45: Topology of example L2TP tunnel configuration

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 46: Example L2TP tunnel configuration

4.14 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: <ul style="list-style-type: none"> • 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 47: PPTP tunnel configuration

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

Figure 46: 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:

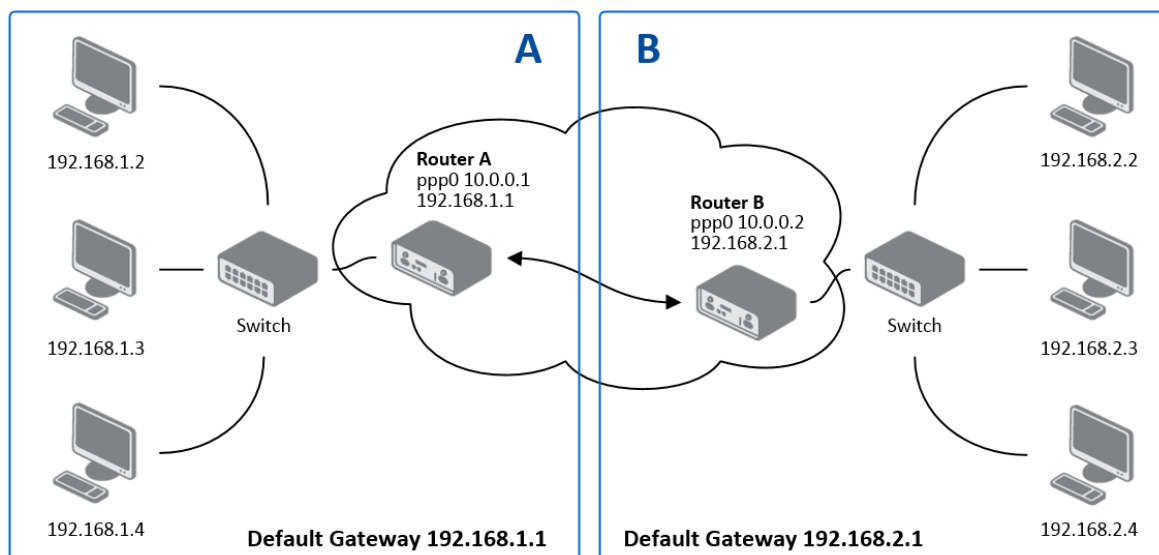


Figure 47: Topology of example PPTP tunnel configuration

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 48: Example PPTP tunnel configuration

4.15 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 49: DynDNS configuration

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

Figure 48: Example of DynDNS configuration



To access the router's configuration remotely it is necessary to enable this in the NAT configuration (bottom part of the form), see chapter 4.9.

4.16 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: <ul style="list-style-type: none"> • No – time shift is disabled • Yes – time shift is allowed

Table 50: NTP configuration

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

NTP Configuration

☐ Enable local NTP service

☒ Synchronize clock with NTP server

Primary NTP Server:

Secondary NTP Server:

Timezone:

Daylight Saving Time:

Figure 49: Example of NTP configuration

4.17 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 51: 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.



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

The *Enable SNMPv3 access* 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 52: 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 53: 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 54: 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).

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

SNMP Configuration	
<input checked="" type="checkbox"/> Enable SNMP agent	
Name *	<input type="text" value="Conel"/>
Location *	<input type="text" value="Usti nad Orlici"/>
Contact *	<input type="text" value="Jack Roghul +420 732 123 4"/>
<input checked="" type="checkbox"/> Enable SNMPv1/v2 access	
Community	<input type="text" value="public"/>
<input type="checkbox"/> Enable SNMPv3 access	
Username	<input type="text"/>
Authentication	<input type="text" value="MD5"/>
Authentication Password	<input type="text"/>
Privacy	<input type="text" value="DES"/>
Privacy Password	<input type="text"/>
<input checked="" type="checkbox"/> Enable I/O extension	
<input checked="" type="checkbox"/> Enable M-BUS extension	
Baudrate	<input type="text" value="300"/>
Parity	<input type="text" value="even"/>
Stop Bits	<input type="text" value="1"/>
<input type="checkbox"/> Enable reporting to supervisory system	
IP Address	<input type="text"/>
Period	<input type="text"/> min
* can be blank	
<input type="button" value="Apply"/>	

Figure 50: Example of SNMP configuration

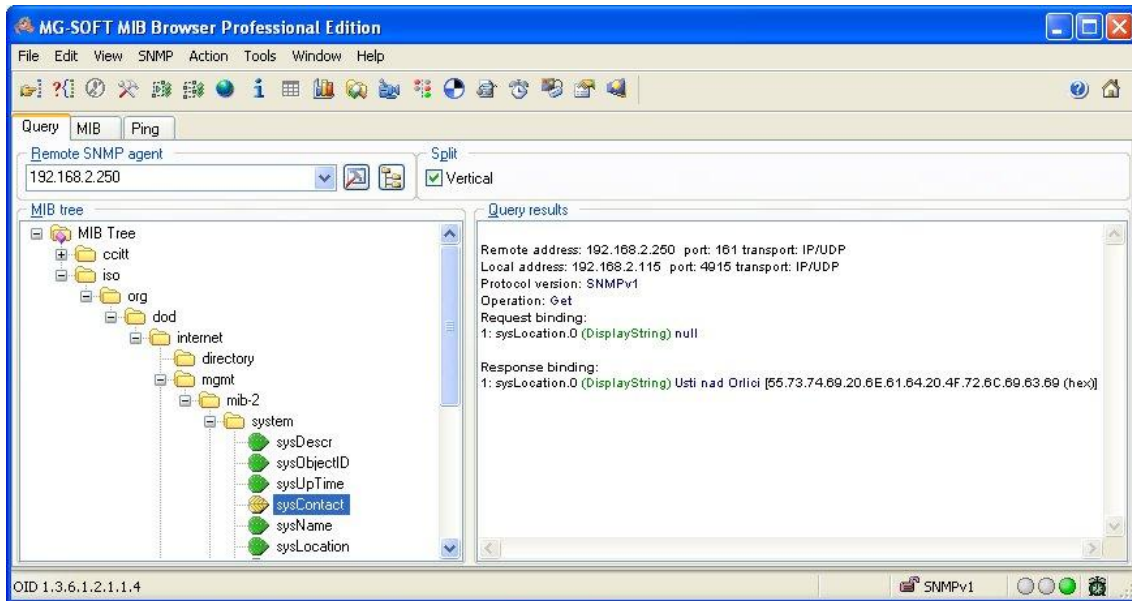


Figure 51: Example of the MIB browser

It is important to set the IP address of the SNMP agent (router) in field *Remote SNMP agent*. After 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

4.18 SMTP Configuration

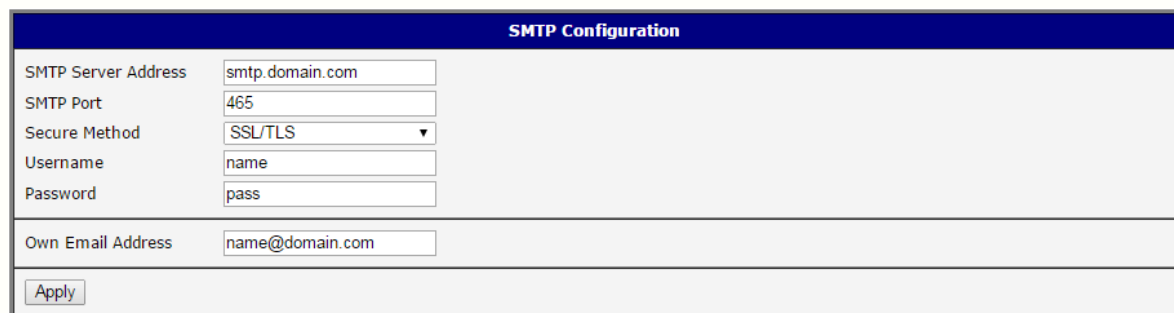
The item *SMTP* is used for configuring SMTP (Simple Mail Transfer Protocol) client for sending e-mails.

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 55: SMTP client configuration



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



The screenshot shows a web form titled "SMTP Configuration". It contains the following fields and values:

- SMTP Server Address: smtp.domain.com
- SMTP Port: 465
- Secure Method: SSL/TLS (selected from a dropdown menu)
- Username: name
- Password: pass
- Own Email Address: name@domain.com

At the bottom of the form is an "Apply" button.

Figure 52: Example of the SMTP client configuration

E-mail can be sent from the Startup script (*Startup Script* item in the *Configuration* section) or via 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.

4.19 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 of 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 56: 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 <i>Enable remote control via SMS</i> , 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 <i>Enable remote control via SMS</i> , 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 <i>Enable remote control via SMS</i> , all incoming SMS are processed and deleted. In the default settings this parameter is turned on.

Table 57: 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 58: 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 59: 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 60: 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 61: Send SMS on ethernet PORT1 configuration

4.19.1 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 62: 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	
<input checked="" type="checkbox"/>	Send SMS on power up
<input checked="" type="checkbox"/>	Send SMS on connect to mobile network
<input checked="" type="checkbox"/>	Send SMS on disconnect from mobile network
<input checked="" type="checkbox"/>	Send SMS when datalimit is exceeded
<input checked="" type="checkbox"/>	Send SMS when binary input on I/O port (BIN0) is active
<input checked="" type="checkbox"/>	Add timestamp to SMS
Phone Number 1	<input type="text" value="723123456"/>
Phone Number 2	<input type="text" value="756858635"/>
Phone Number 3	<input type="text" value="603854758"/>
Unit ID *	<input type="text" value="Router"/>
BIN0 - SMS *	<input type="text" value="BIN0"/>
<input checked="" type="checkbox"/>	Enable remote control via SMS
Phone Number 1	<input type="text"/>
Phone Number 2	<input type="text"/>
Phone Number 3	<input type="text"/>
<input type="checkbox"/>	Enable AT-SMS protocol on expansion port 1
Baudrate	<input type="text" value="9600"/>
<input type="checkbox"/>	Enable AT-SMS protocol on expansion port 2
Baudrate	<input type="text" value="9600"/>
<input type="checkbox"/>	Enable AT-SMS protocol over TCP
TCP Port	<input type="text"/>
* can be blank	
<input type="button" value="Apply"/>	

Figure 53: Example 1 – SMS configuration

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

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

Figure 54: Example 2 – SMS configuration

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

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

Figure 55: Example 3 – SMS configuration

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

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

Figure 56: Example 4 – SMS configuration

4.20 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.
- If the version of router is with the **RS232-RS485-ETH** interface, configuration of RS232 interface is accessible via *Expansion Port 1* item, configuration of RS485 via *Expansion Port 2* item and configuration of ETH (ETH2 interface of the router) via *LAN* item, the *Tertiary LAN* column.
- 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 <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 63: 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 64: 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 65: 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 66: 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 *	

☐ 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 57: Expansion port configuration

Examples of the expansion port configuration:

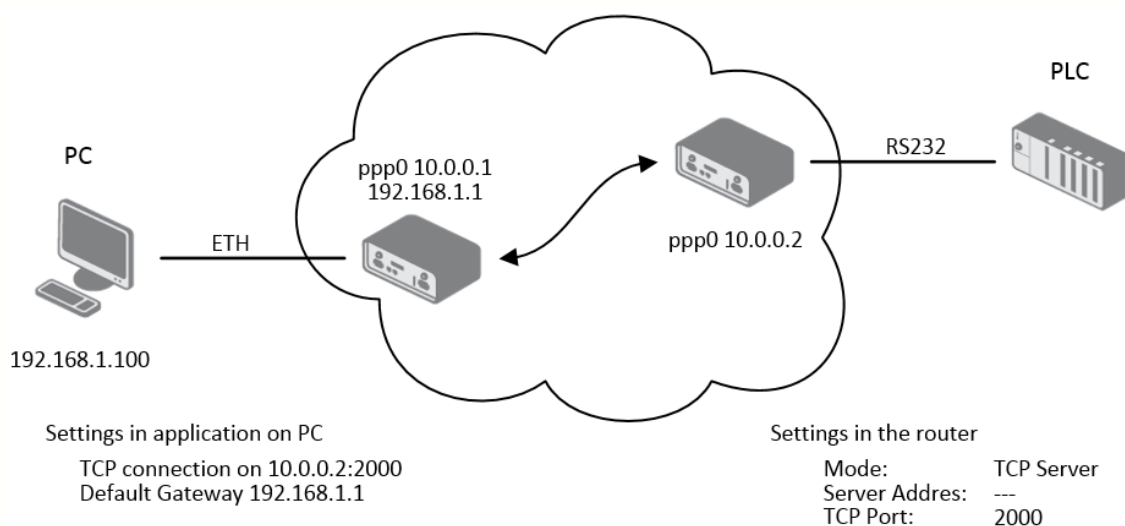


Figure 58: Example 1 – expansion port configuration

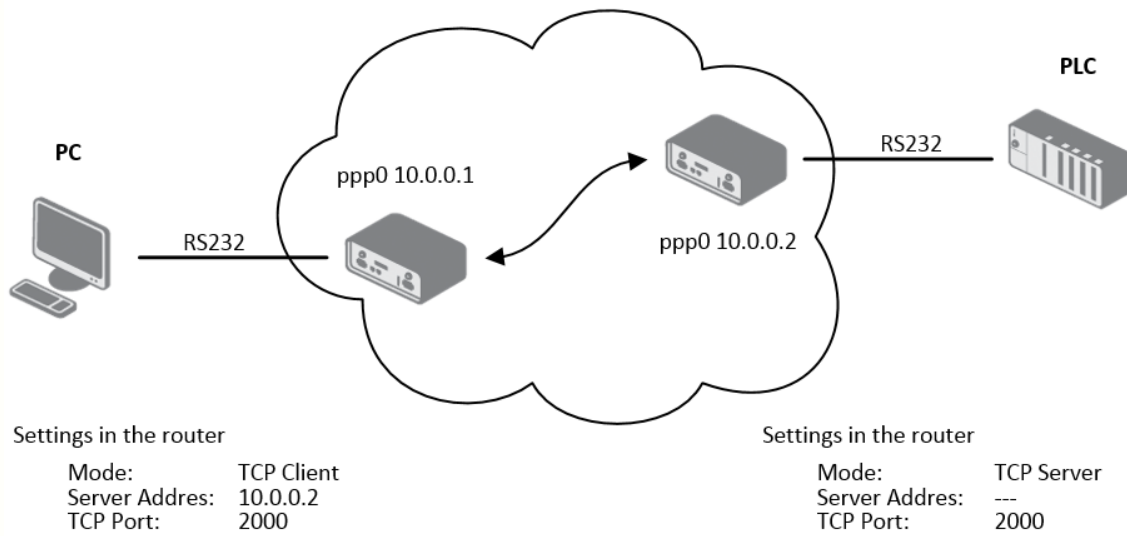


Figure 59: Example 2 – expansion port configuration



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.

4.21 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • TCP – communication using a linked protocol TCP • UDP – communication using a unlinked protocol UDP
Mode	Mode of connection: <ul style="list-style-type: none"> • 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 67: 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 68: 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 69: 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 70: DTR signal description



Supported USB/RS232 converters:

- FTDI
- Prolific PL2303
- Silicon Laboratories CP210x

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

USB Port Configuration

☐ Enable USB serial converter access over TCP/UDP

Baudrate:

Data Bits:

Parity:

Stop Bits:

Split Timeout: msec

Protocol:

Mode:

Server Address:

TCP Port:

Inactivity Timeout *: sec

☐ Reject new connections

☐ Check TCP connection

Keepalive Time: sec

Keepalive Interval: sec

Keepalive Probes:

☐ Use CD as indicator of TCP connection

☐ Use DTR as control of TCP connection

Figure 60: USB configuration

Examples of USB port configuration:

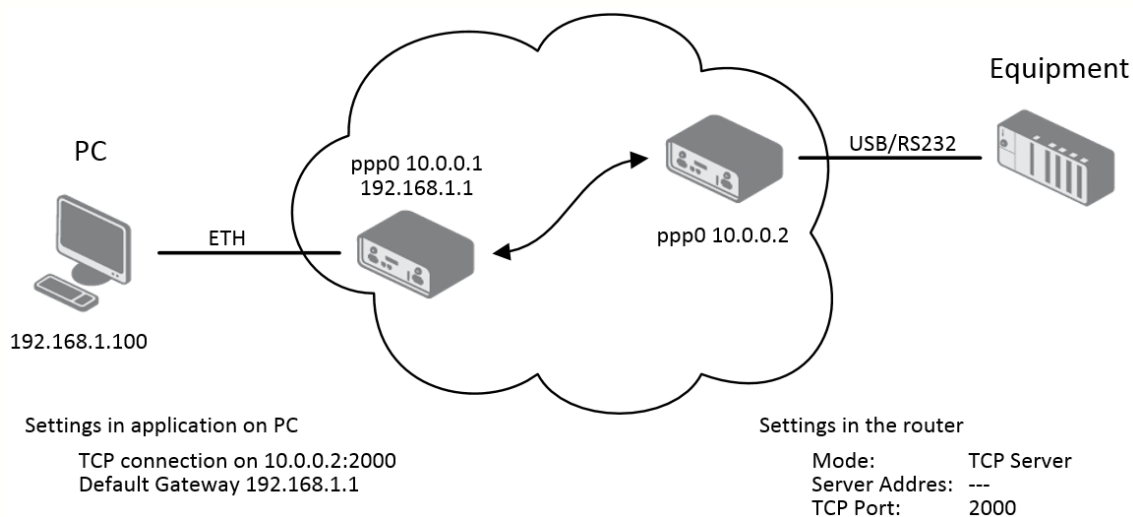


Figure 61: Example 1 – USB port configuration

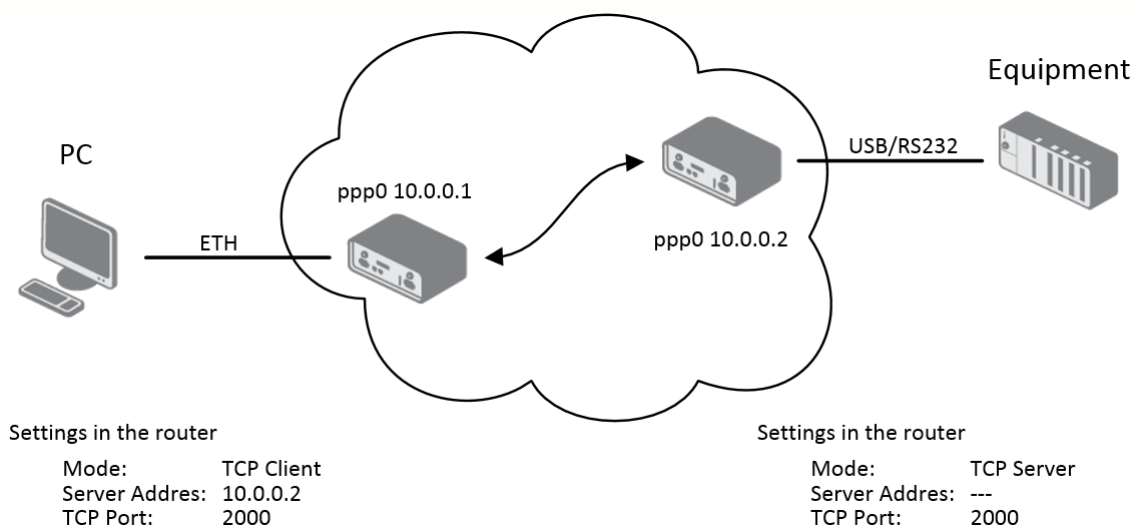


Figure 62: Example 2 – USB port configuration

4.22 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.

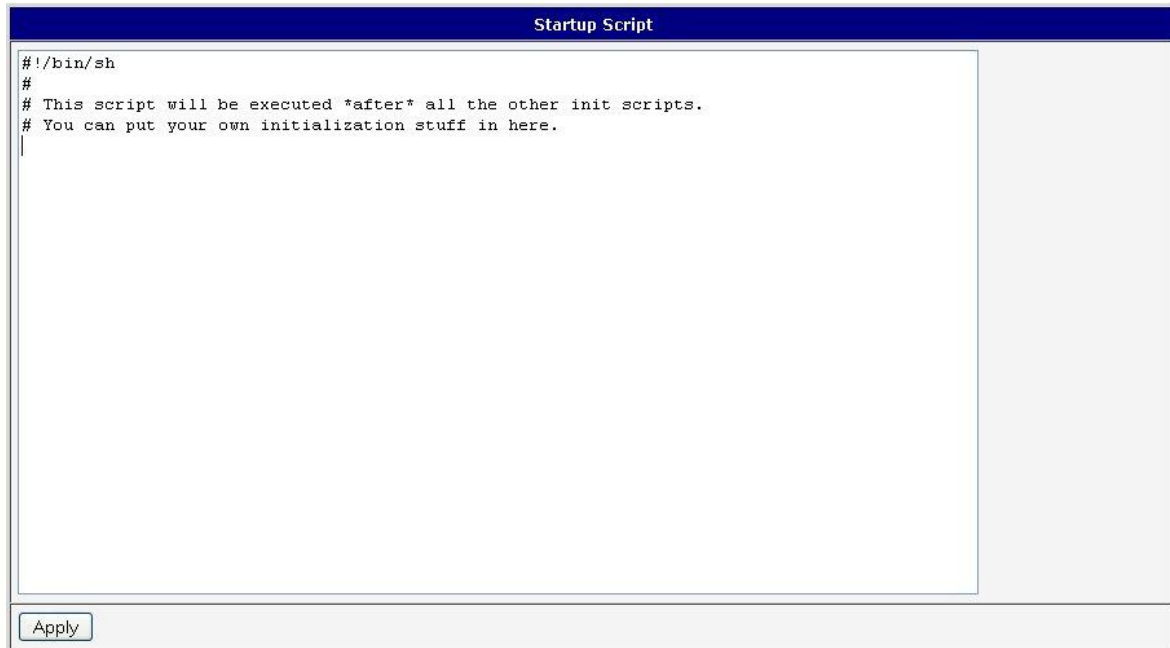


Figure 63: Startup script



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.

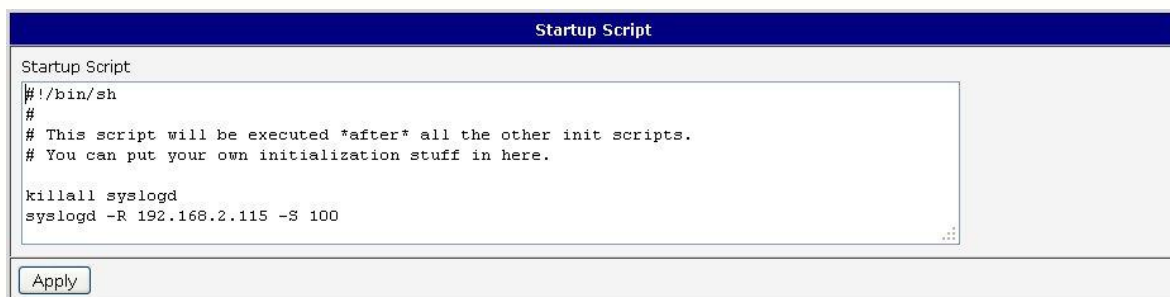
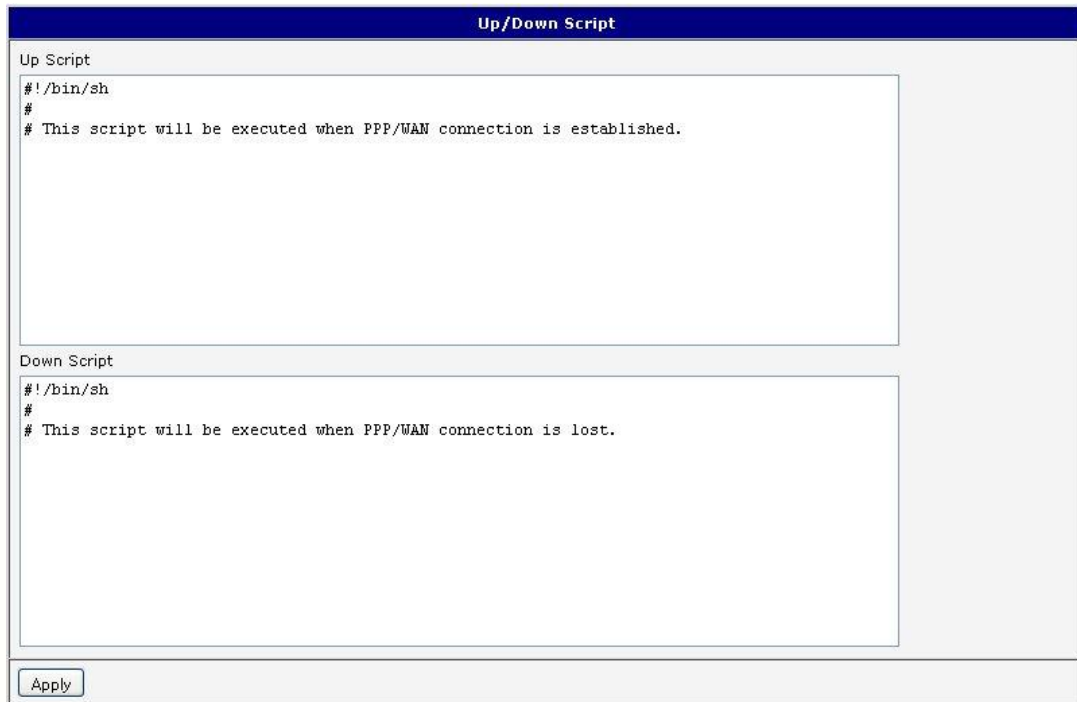


Figure 64: Example of Startup script

4.23 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.

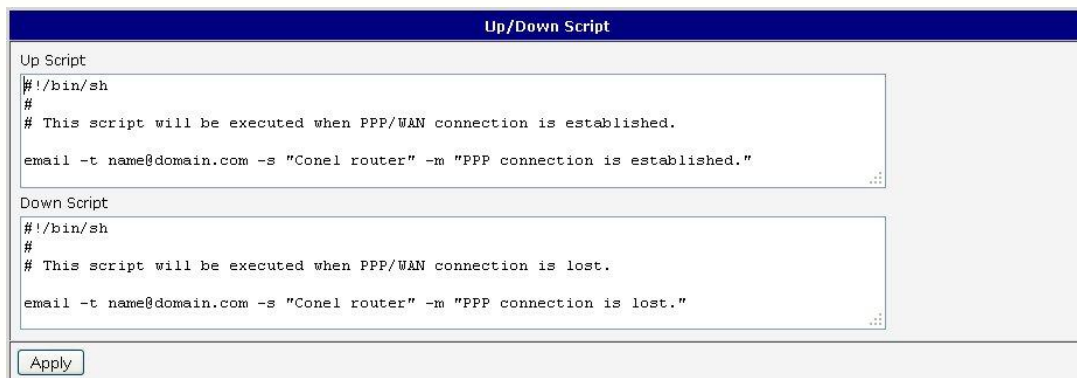
The changes in settings will apply after pressing the *Apply* button.



The screenshot shows the 'Up/Down Script' configuration window. It has two text areas for scripts. The 'Up Script' area contains the following text: `#!/bin/sh`, `#`, and `# This script will be executed when PPP/WAN connection is established.`. The 'Down Script' area contains the following text: `#!/bin/sh`, `#`, and `# This script will be executed when PPP/WAN connection is lost.`. At the bottom of the window is an 'Apply' button.

Figure 65: 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.



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

Figure 66: Example of Up/Down script

4.24 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: <ul style="list-style-type: none"> • HTTP(S)/FTP(S) server – updates are downloaded from the <i>Base URL</i> 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 71: 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 both files (.bin and .ver) to the HTTP(S)/FTP(S) server. If only the .bin file is uploaded and the HTTP server sends the incorrect answer of *200 OK* (instead of expected *404 Not Found*) when the device tries to download the nonexistent .ver file, then there is a risk that the router will download the .bin file over and over again.

The following examples 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>

Figure 67: 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>

Figure 68: Example of automatic update 2

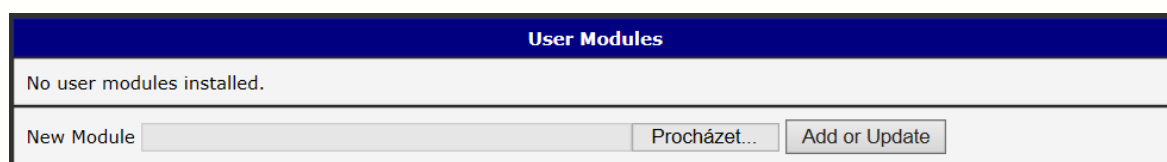


Firmware update can cause incompatibility with the user modules. It is recommended to update user modules to the most recent version. Information about the user module and the firmware compatibility is at the beginning of the user module's Application Note.

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.



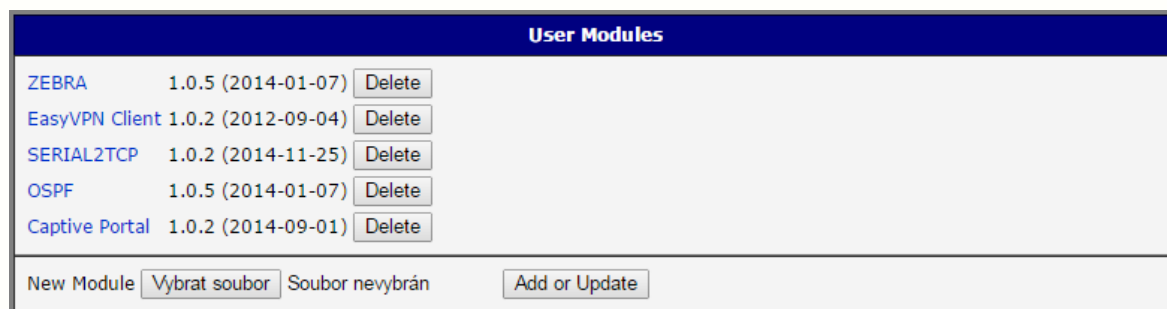
User Modules	
No user modules installed.	
New Module	<input type="text"/> <input type="button" value="Procházet..."/> <input type="button" value="Add or Update"/>

Figure 69: 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) <input type="button" value="Delete"/>
EasyVPN Client	1.0.2 (2012-09-04) <input type="button" value="Delete"/>
SERIAL2TCP	1.0.2 (2014-11-25) <input type="button" value="Delete"/>
OSPF	1.0.5 (2014-01-07) <input type="button" value="Delete"/>
Captive Portal	1.0.2 (2014-09-01) <input type="button" value="Delete"/>
New Module <input type="button" value="Vybrat soubor"/> <input type="button" value="Soubor nevybrán"/> <input type="button" value="Add or Update"/>	

Figure 70: 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 functionality of the connection between two network interfaces (ping).
IS-IS	Add support of IS-IS protocol.

Table 72: User modules



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

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

6. Administration

6.1 Users



This configuration form is not available for users with role *User*!

Use *Users* item in the *Administration* part of the main menu for managing user accounts. The first block of this form contains overview of added users. The table below describes meaning of all buttons in this block.

Button	Description
Lock	Locks user account. This user is not allowed to log in to the router (neither web interface nor SSH)
Change Password	Allows to change password for corresponding user
Delete	Deletes corresponding user account

Table 73: Users overview



Be careful! If you lock all accounts with permissions (role) *Admin*, it will not be possible to unlock these accounts! This also means that the *Users* item will be unavailable for all users, because all "admins" are locked and "users" don't have sufficient permissions.

The second block contains configuration form which allows you to add new user. All items are described in the table below.

Item	Description
Role	Defines type of user account <ul style="list-style-type: none"> • User – user with basic permissions • Admin – user with full permissions
Username	Username for logging into the web interface
Password	Password for logging into the web interface
Confirm Password	Confirms the password you specified above

Table 74: Add User



Ordinary users are not able to access router via Telnet, SSH or SFTP. Read only FTP access is allowed for these users.

Figure 71: Users

6.2 Change Profile

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

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

Figure 72: Change profile

6.3 Change Password

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



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

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

Change Password	
New Password	<input type="text"/>
Confirm Password	<input type="text"/>
<input type="button" value="Apply"/>	

Figure 73: Change password

6.4 Set Real Time Clock

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

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

Figure 74: Set real time clock

6.5 Set SMS Service Center Address



The SPECTRE v3 ERT routers do not support the *Set SMS service center address* option.

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

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

Figure 75: Set SMS service center address

6.6 Unlock SIM Card



The SPECTRE v3 ERT routers do not support the *Unlock SIM Card* option.

You may lock the SIM card with a 4-8 digit PIN (Personal Identification Number) code to prevent unauthorized use of the SIM card. The PIN code must be entered each time that the SIM card is powered up. The SPECTRE v3 cellular router supports the use of a SIM card with a PIN number. Enter the PIN number into the SIM PIN field on the configuration page and select *Apply*.



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

Figure 76: Unlock SIM card

6.7 Send SMS



The SPECTRE v3 ERT routers do not support the *Send SMS* option.

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

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

Figure 77: Send SMS

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

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

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

6.8 Backup Configuration

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

6.9 Restore Configuration

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



Figure 78: Restore configuration

6.10 Update Firmware

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



Do not turn off the router during the firmware update. The firmware update can take up to five minutes to complete.



Figure 79: Update Firmware

During the firmware update, the router will show the following messages. The progress is shown in the form of adding dots ('.').

Firmware Update

**Do not turn off the router during the firmware update.
The firmware update can take up to 5 minutes to complete.**

Uploading firmware to RAM... ok
Checking firmware validity... ok
Backing up configuration... ok
Programming FLASH..... ok

Reboot in progress

Continue [here](#) after reboot.

After the firmware update, the router will automatically reboot.



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

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

6.11 Reboot

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

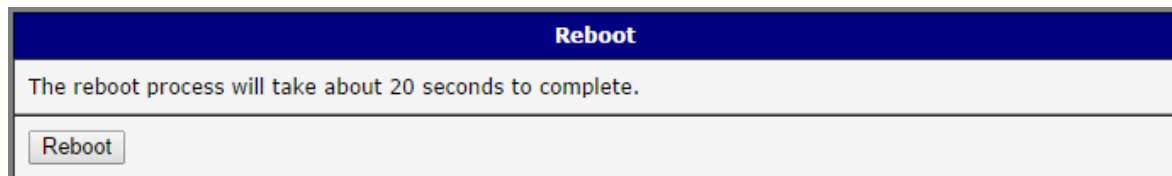


Figure 80: Reboot

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

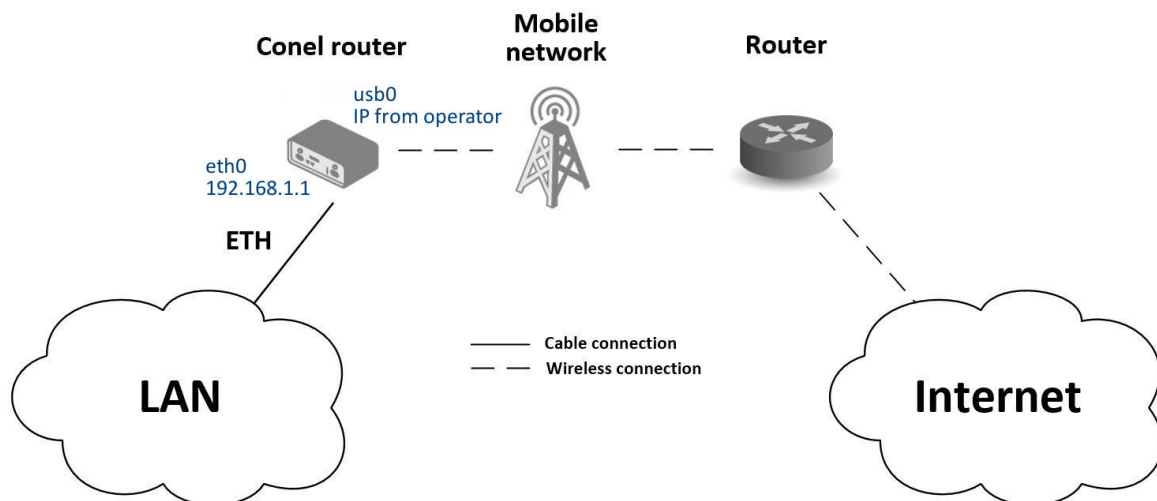


Figure 81: Access to the Internet from LAN – topology of the example

There is topology of this easy example shown on the fig. 81. 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 signaled 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 address 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 82. 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		
<input checked="" type="checkbox"/> Enable dynamic DHCP leases		
IP Pool Start	192.168.1.2	
IP Pool End	192.168.1.254	
Lease Time	600	sec

Figure 82: 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. 83. 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 4.3.1.

<input checked="" type="checkbox"/> 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 83: 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

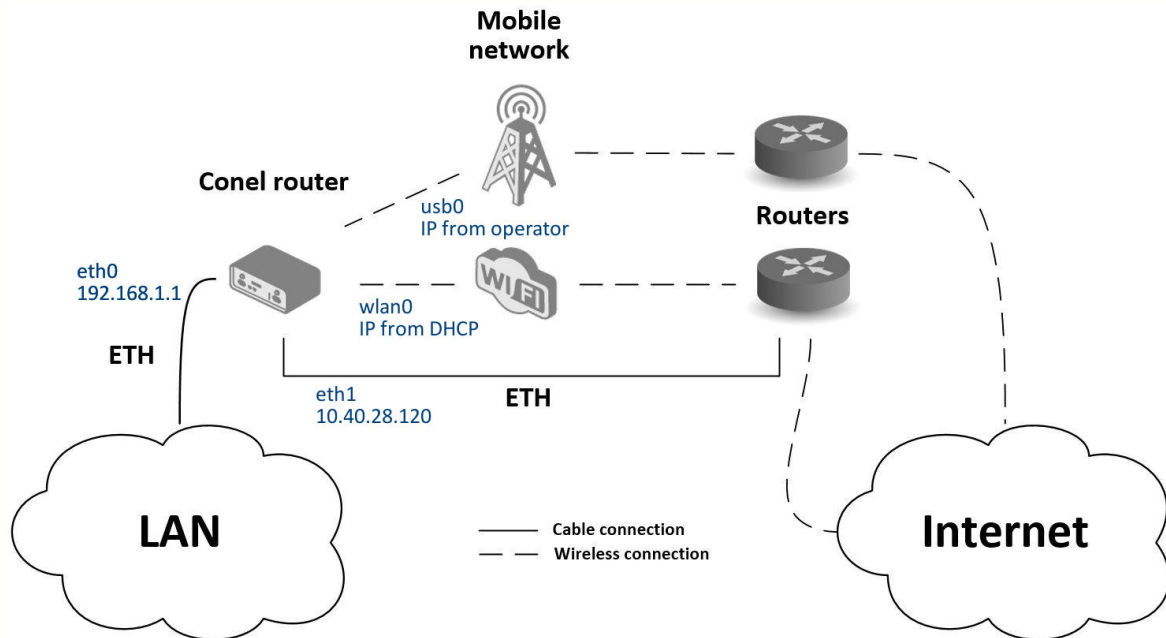


Figure 84: Backed up access to the Internet – topology of the example

In the situation on the fig. 84 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.

Status	
General	
Mobile WAN	
WiFi	
WiFi Scan	
Network	
DHCP	
IPsec	
DynDNS	
System Log	
Configuration	
LAN	
VRRP	
Mobile WAN	
PPPoE	
WiFi	

	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
<input checked="" type="checkbox"/> Enable dynamic DHCP leases		
IP Pool Start	192.168.1.2	
IP Pool End	192.168.1.254	
Lease Time	600 sec	

Figure 85: 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. 85 – 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. 86. 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 4.6.

Configure connection to a WiFi network in the *WiFi* item, see fig. 87. 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 4.5 chapter.

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

Status	
General	
Mobile WAN	
WiFi	
WiFi Scan	
Network	
DHCP	
IPsec	
DynDNS	
System Log	

Configuration	
LAN	
VRRP	
Mobile WAN	
PPPoE	
WiFi	
WLAN	
Backup Routes	
Firewall	

<input checked="" type="checkbox"/> 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
<input type="checkbox"/> Enable dynamic DHCP leases	
IP Pool Start	
IP Pool End	
Lease Time	0 sec
<input type="button" value="Apply"/>	

Figure 86: 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. 88. 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 4.3.1.

Status	Configuration
General	<input checked="" type="checkbox"/> Enable WiFi Operating Mode: station (STA) SSID: WiFiNetwork Broadcast SSID: enabled Probe Hidden SSID: <input type="checkbox"/> Country Code *: HW Mode: IEEE 802.11b Channel: 0 BW 40 MHz: <input type="checkbox"/> WMM: <input type="checkbox"/> 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 87: Backed up access to the Internet – *WiFi* configuration

Status	Configuration																																				
General	<input checked="" type="checkbox"/> Create connection to mobile network																																				
Mobile WAN	<table border="1"> <thead> <tr> <th></th> <th>Primary SIM card</th> <th>Secondary SIM card</th> </tr> </thead> <tbody> <tr> <td>APN *</td> <td></td> <td></td> </tr> <tr> <td>Username *</td> <td></td> <td></td> </tr> <tr> <td>Password *</td> <td></td> <td></td> </tr> <tr> <td>Authentication</td> <td>PAP or CHAP</td> <td>PAP or CHAP</td> </tr> <tr> <td>IP Address *</td> <td></td> <td></td> </tr> <tr> <td>Phone Number *</td> <td></td> <td></td> </tr> <tr> <td>Operator *</td> <td></td> <td></td> </tr> <tr> <td>Network Type</td> <td>automatic selection</td> <td>automatic selection</td> </tr> <tr> <td>PIN *</td> <td></td> <td></td> </tr> <tr> <td>MRU</td> <td>1500</td> <td>1500 bytes</td> </tr> <tr> <td>MTU</td> <td>1500</td> <td>1500 bytes</td> </tr> </tbody> </table> DNS Settings: get from operator DNS Server: (The feature of check connection to mobile network is necessary for uninterrupted operation) Check Connection: enabled + bind Ping IP Address: 8.8.8.8 Ping Interval: 60 sec		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
	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																																			

Figure 88: 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. 89 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 4.7.

Status	
General	
Mobile WAN	
WiFi	
WiFi Scan	
Network	
DHCP	
IPsec	
DynDNS	
System Log	

Configuration	
LAN	
VRRP	
Mobile WAN	
PPPoE	
WiFi	
WiFi LAN	
Backup Routes	
Firewall	
NAT	
OpenVPN	
IPsec	
GRE	
L2TP	
PPTP	
DynDNS	

<input checked="" type="checkbox"/> Enable backup routes switching	
<input checked="" type="checkbox"/> Enable backup routes switching for Mobile WAN	Priority: 3rd
<input type="checkbox"/> Enable backup routes switching for PPPoE	Priority: 1st
	Ping IP Address:
	Ping Interval: sec
<input checked="" type="checkbox"/> Enable backup routes switching for WiFi STA	Priority: 2nd
	Ping IP Address:
	Ping Interval: sec
<input type="checkbox"/> Enable backup routes switching for Primary LAN	Priority: 1st
	Ping IP Address:
	Ping Interval: sec
<input checked="" type="checkbox"/> Enable backup routes switching for Secondary LAN	Priority: 1st
	Ping IP Address:
	Ping Interval: sec

Figure 89: 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 addresses 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 4.7.

7.3 Secure Networks Interconnection or Using VPN

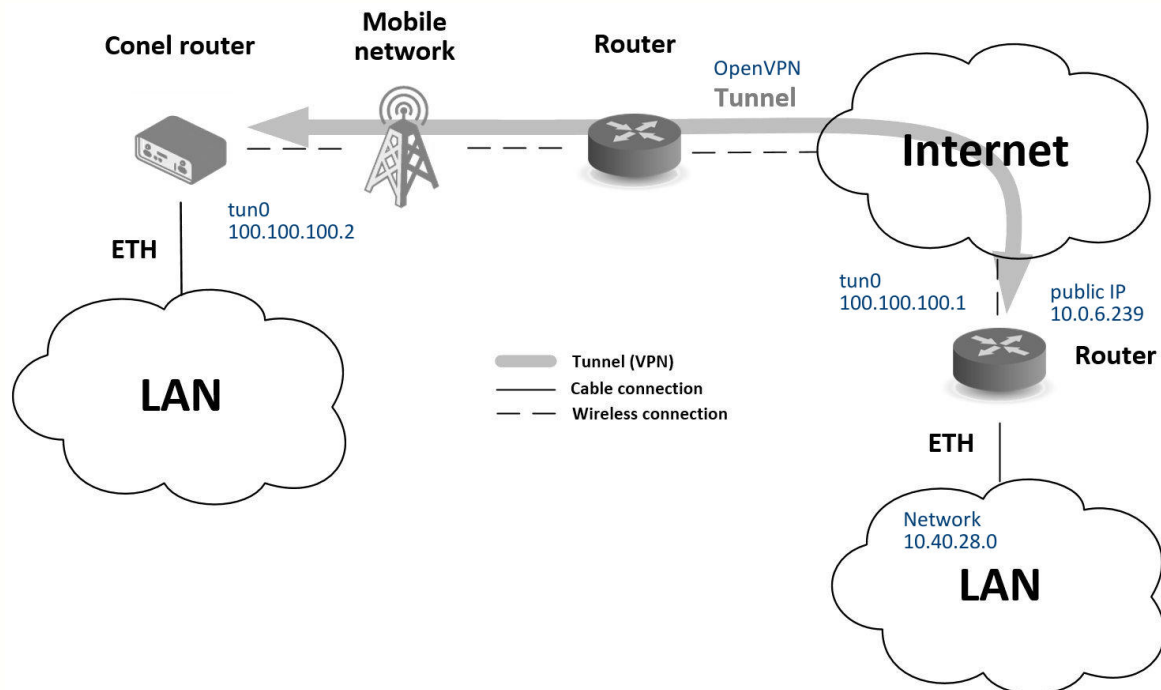


Figure 90: Secure networks interconnection – topology of the example

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. 90. In Conel routers you can use more ways (protocols) for this reason:

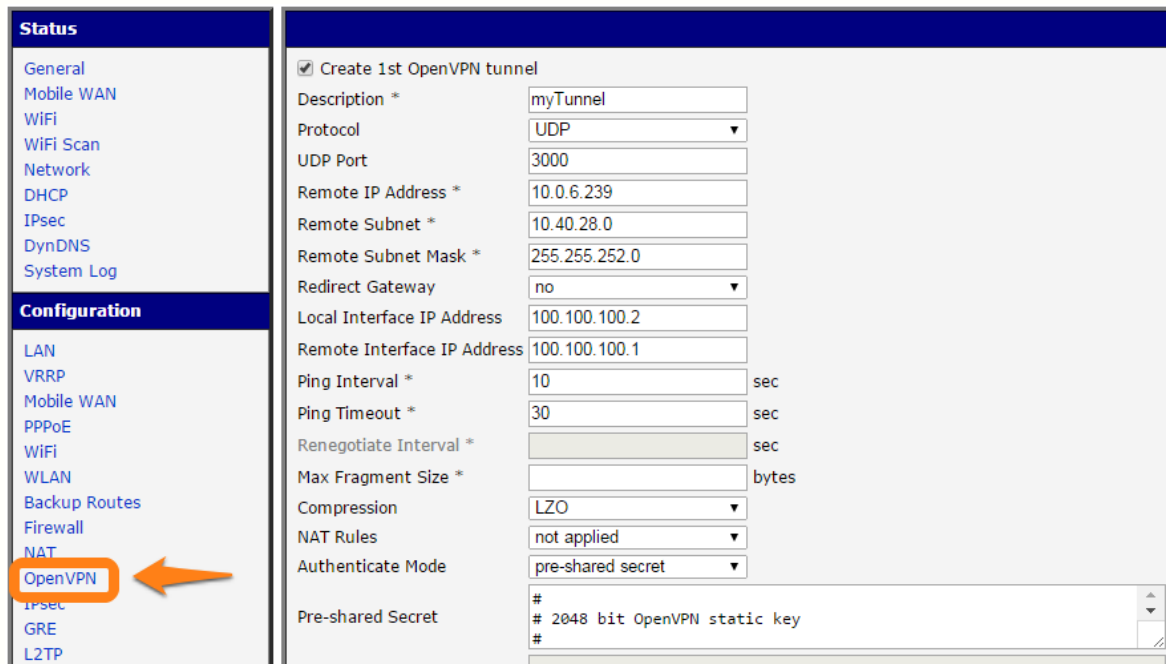
- *OpenVPN* (it is also configuration item in the web interface of the router), see chapter 4.10 or Application Note [5],
- *IPsec* (it is also configuration item in the web interface of the router), see chapter 4.11 or Application Note [6].

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. 90. 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 4.3.1), 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. 91. 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 4.10 or Application Note [5].



Status	
General	
Mobile WAN	
WiFi	
WiFi Scan	
Network	
DHCP	
IPsec	
DynDNS	
System Log	

Configuration	
LAN	
VRRP	
Mobile WAN	
PPPoE	
WiFi	
WLAN	
Backup Routes	
Firewall	
NAT	
OpenVPN	
IPsec	
GRE	
L2TP	

Configuration	
<input checked="" type="checkbox"/> 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 91: 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

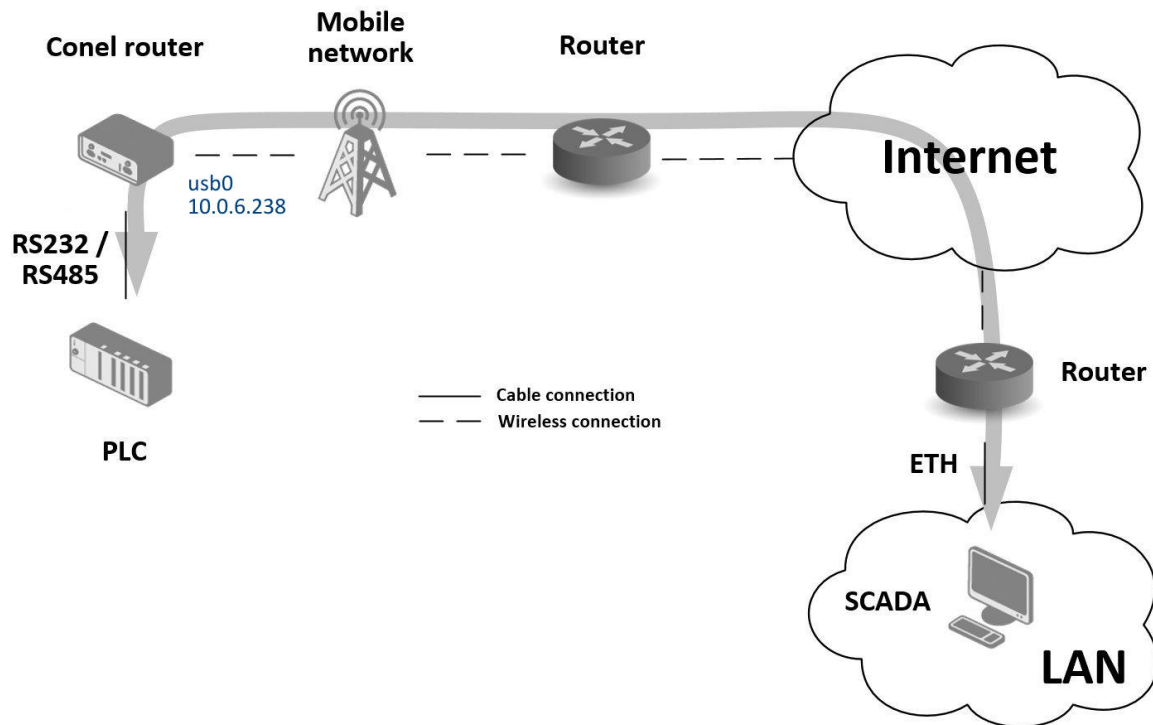


Figure 92: Serial Gateway – topology of the example

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. 92. The Conel router has to have serial interface (port) RS232 or RS232-RS485/422 or RS232-RS485-ETH 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 4.3.1.

Expansion Port 1 configuration The interface RS232 (port) can be configured in the *Configuration* section, *Expansion Port 1* item – see fig. 93. 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.

Status

- General
- Mobile WAN
- WiFi
- WiFi Scan
- Network
- DHCP
- IPsec
- DynDNS
- System Log

Configuration

- LAN
- VRRP
- Mobile WAN
- PPPoE
- WiFi
- WLAN
- Backup Routes
- Firewall
- NAT
- OpenVPN
- IPsec
- GRE
- L2TP
- PPTP
- DynDNS
- NTP
- SNMP
- SMTP
- SMS
- Expansion Port 1**
- Expansion Port 2

☒ 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

Apply

Figure 93: Serial Gateway – konfigurace *Expansion Port 1*

To communicate with the serial device (PLC), connect from the PC (in fig. 92 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