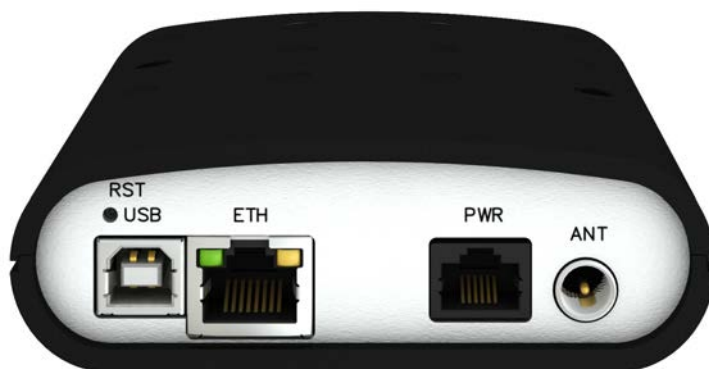


EDGE router

ER75s

USER MANUAL



ADVANTECH

Used symbols



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



Attention – Problems that can arise in specific situations.



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

GPL licence

Source codes under GPL licence are available free of charge by sending an email to:
cellularsales@advantech-bb.com.



Advantech B+B SmartWorx s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
Document No. MAN-0033-EN, revision from January 17, 2019. Released in the Czech Republic.

Contents

1	Safety Instructions	2
2	WEEE directive	3
3	Description of the router	4
4	Contents of package	5
5	Router design	6
5.1	Delivery identification	6
5.2	Ordering codes	6
5.3	Basic dimensions	7
5.4	Mechanical dimensions and mounting recommendations	7
5.5	Description of individual components of the router	10
5.5.1	GSM/GPRS/EDGE module	10
5.5.2	Control microcomputer	10
5.6	Description of the front and rear panel	11
5.6.1	Status indication	12
5.6.2	Power connector PWR	12
5.6.3	Antenna connector ANT	13
5.6.4	SIM card reader	13
5.6.5	ETH port	14
5.6.6	USB Port	15
5.6.7	Reset	16
6	First use	17
6.1	Connecting the router before first use	17
6.2	Start	17
6.3	Configuration	18
6.3.1	Configuration over web browser	18
6.3.2	Configuration over Telnet	18
7	Technical parameters	19
7.1	Technical parameters of router	19
7.2	Technical parameters of module	19
8	Configuration via web browser	20
8.1	General	21

8.1.1	Mobile Connection	21
8.1.2	Primary LAN	21
8.1.3	Peripheral Ports	22
8.1.4	System Information	22
8.2	Mobile WAN status	22
8.3	Network status	25
8.4	DHCP status	27
8.5	IPsec status	28
8.6	DynDNS status	28
8.7	System log	29
8.8	LAN configuration	30
8.9	VRRP configuration	36
8.10	Mobile WAN configuration	37
8.10.1	Mobile WAN	37
8.10.2	DNS address configuration	40
8.10.3	Check connection to mobile network configuration	40
8.10.4	Data limit configuration	41
8.10.5	Configuration of switching between APNs	42
8.10.6	Dial-In access configuration	44
8.10.7	PPPoE bridge mode configuration	44
8.11	Backup Routes	48
8.12	Firewall configuration	48
8.13	NAT configuration	53
8.14	OpenVPN tunnel configuration	57
8.15	IPSec tunnel configuration	62
8.16	GRE tunnels configuration	65
8.17	L2TP tunnel configuration	71
8.18	DynDNS client configuration	74
8.19	NTP client configuration	74
8.20	SNMP configuration	75
8.21	SMTP configuration	78
8.22	SMS configuration	79
8.22.1	Send SMS	80
8.23	Startup Script	85
8.24	Up/Down Script	86
8.25	Automatic update configuration	87
8.26	Change profile	89
8.27	Change password	89
8.28	Set real time clock	90
8.29	Set SMS service center address	90
8.30	Unlock SIM card	90
8.31	Send SMS	91
8.32	Backup configuration	91
8.33	Restore configuration	91

8.34 Update firmware	92
8.35 Reboot	92
9 Configuration setting over Telnet	93
10 Recommended literature	95
11 Possible problems	96
12 FAQ	97
13 Customers Support	99
13.1 Customer Support for NAM	99
13.2 Customer Support for Europe	99
13.3 Customer Support for Asia	99

List of Figures

1	ER75s router	5
2	Label for ER75s	6
3	Basic dimensions	7
4	Space around antennas	8
5	Cable routing	9
6	Space in front of connectors	9
7	Front panel	11
8	Rear panel	11
9	Connection of power supply connector	12
10	External antenna	13
11	Ethernet connector	14
12	ETH – Example of router connection	14
13	USB connector	15
14	USB – Example of router connection	15
15	Router reset	16
16	Router connection	17
16	Web configuration	20
17	Mobile WAN status	24
18	Network status	26
19	DHCP status	27
20	IPsec status	28
21	DynDNS status	28
22	System log	29
23	Example program syslogd start with the parameter -r	30
24	Topology of example LAN configuration 1	32
25	Example LAN configuration 1	33
26	Topology of example LAN configuration 2	34
27	Example LAN configuration 2	34
28	Topology of example LAN configuration 3	35
29	Example LAN configuration 3	35
30	Topology of example VRRP configuration	37
31	Example VRRP configuration — main router	37
32	Example VRRP configuration — backup router	38
33	Mobile WAN configuration	46
34	Example of Mobile WAN configuration 1	47
35	Example of Mobile WAN configuration 2	47
36	Example of Mobile WAN configuration 3	47
37	Backup Routes	49
38	Firewall configuration	51
39	Topology of example firewall configuration	52

40	Example firewall configuration	52
41	Topology of example NAT configuration 1	54
42	Example NAT configuration 1	55
43	Topology of example NAT configuration 2	56
44	Example NAT configuration 2	56
45	OpenVPN tunnels configuration	57
46	OpenVPN tunnel configuration	60
47	Topology of example OpenVPN configuration	61
48	IPsec tunnels configuration	62
49	IPsec tunnels configuration	68
50	Topology of example IPsec configuration	69
51	GRE tunnels configuration	69
52	GRE tunnel configuration	69
53	Topology of GRE tunnel configuration	70
54	L2TP tunnel configuration	72
55	Topology of example L2TP tunnel configuration	72
56	Example of DynDNS configuration	74
57	Example of NTP configuration	75
58	Example of SNMP configuration	76
59	Example of the MIB browser	77
60	SMTP configuration	78
61	Example of SMS configuration 1	82
62	Example of SMS configuration 2	83
63	Example of SMS configuration 3	84
64	Startup script	85
65	Example of Startup script	85
66	Up/Down script	86
67	Example of Up/Down script	86
68	Example of automatic update 1	88
69	Example of automatic update 2	88
70	Change profile	89
71	Change password	89
72	Set real time clock	90
73	Set SMS service center address	90
74	Unlock SIM card	90
75	Send SMS	91
76	Restore configuration	91
77	Update firmware	92
78	Reboot	92

List of Tables

1	Delivery identification	6
2	Description of the rear panel	11
3	Status indication	12
4	Connection of the PWR supply connector	12
5	Connection of Ethernet connector	14
6	Connection of USB connector	15
7	Description of reset and restart router	16
8	Technical parameters of router	19
9	Technical parameters of module	19
10	Mobile connection	21
11	System Information	22
12	Mobile Network Information	23
13	Description of period	23
14	Mobile Network Statistics	23
15	Traffic statistics	24
16	Description of interface in network status	25
17	Description of information in network status	26
18	DHCP status description	27
19	Configuration of network interface	30
20	Configuration of dynamic DHCP server	31
21	Configuration of static DHCP server	31
22	VRRP configuration	36
23	Check connection	36
24	Mobile WAN connection configuration	39
25	Check connection to mobile network configuration	41
26	Data limit configuration	41
27	Default and backup APN configuration	42
28	Configuration of switching between APNs I	43
29	Configuration of switching between APNs II	44
30	Dial-In access configuration	44
31	Backup Routes	48
32	Filtering of incoming packets	49
33	Forwarding filtering	50
34	NAT configuration	53
35	Configuration of send all incoming packets	53
36	Remote access configuration	54
37	Overview OpenVPN tunnels	57
38	OpenVPN tunnels configuration	59
39	Example OpenVPN configuration	61
40	Overview IPsec tunnels	62

41	OpenVPN tunnels configuration	64
42	Example IPsec configuration	65
43	Overview GRE tunnels	66
44	GRE tunnel configuration	66
45	Example GRE tunnel configuration	67
46	L2TP tunnel configuration	71
47	Example L2TP tunnel configuration	73
48	DynDNS configuration	74
49	NTP configuration	75
50	SNMP agent configuration	75
51	SMTP client configuration	78
52	Send SMS configuration	79
53	Control via SMS configuration	79
54	Control SMS	80
55	Send SMS on ethernet PORT1 configuration	80
56	List of AT commands	81
57	Automatic update configuration	87
58	Telnet commands	94

1. Safety Instructions



Please, observe the following instructions:

- The router must be used in compliance with all applicable international and national laws and in compliance with any special restrictions regulating the utilization of the router in prescribed applications and environments.
- To prevent possible injury and damage to appliances and to ensure compliance with all relevant provisions, use only the original accessories. Unauthorized modifications or the use of unapproved accessories may result in damage to the router and/or a breach of applicable regulations. Unauthorized modifications or use of unapproved accessories may void the warranty.
- The router can not be opened.
- Turn off the router and disconnect it from power supply before handling the SIM card.
- **Caution!** The SIM card could be swallowed by small children.
- Input voltage must not exceed 36 V DC max.
- Do not expose the router to extreme ambient conditions. Protect the router against dust, moisture and high temperature.
- Only routers with appropriate certification and labelling should be used in locations where flammable and explosive materials are present, including gas stations, chemical plants, or locations in which explosives are used. We remind users of the duty to observe the restrictions concerning the utilization of radio devices at such places.
- Switch off the router when traveling by plane. Utilization of the router on a plane may endanger the operation of the plane or interfere with the mobile telephone network, and may be unlawful. Failure to observe these instructions may result in the suspension or cancellation of telephone services for the respective client and/or may result in legal sanctions.
- When using the router in close proximity to personal medical devices, such as cardiac pacemakers or hearing aids, you must proceed with heightened caution.
- The router may cause interference when used in close proximity to TV sets, radio receivers or personal computers.
- It is recommended that you create an appropriate copy or backup of all important settings that are stored in the memory of the device.



2. Product Disposal Instructions

The WEEE (Waste Electrical and Electronic Equipment: 2012/19/EU) directive was introduced to ensure that electrical/electronic products are recycled using the best available recovery techniques in order to minimize impact on the environment. This product contains high quality materials and components which can be recycled. At the end of its life this product **MUST NOT** be mixed with other commercial waste for disposal. The device contains the battery. Remove the battery from the device before disposal. The battery in the device needs to be disposed apart accordingly. Check the terms and conditions of your supplier for disposal information.

3. Description of the router

EDGE router is a compact electronic device based on the module which enables data transfers using GSM, GPRS and EDGE technologies. Primarily, the router expands the capabilities of the module by the option of connecting more PCs by means of the built-in Ethernet interface. In addition, the firmware of the router provides automatic establishment and maintenance of GPRS connection. By means of integration of a DHCP server it provides the users with simple installation and Internet access. In addition, the router is equipped with a USB 2.0 Full Speed interface which is designed only for connection to a PC with Windows 2000, Windows XP, Windows Vista or Windows Seven operating system. EDGE router is only available in one basic version called ER75s. Allows user to use one SIM card to connect to the GSM network and is embedded in a plastic box.

Configuration is done via web interface protected by password. The GPRS/EDGE router supports creation of VPN tunnels using technologies IPsec, OpenVPN and L2TP to ensure safe communication. Web interface provides detail statistics about the wireless router activities, signal strength, detailed log, etc. Router supports functions: DHCP, NAT, NAT-T, DynDNS, NTP, VRRP, control by SMS and many other functions.

Other diagnostic functions ensuring continuous communication include automatic inspection of PPP connection offering an automatic restart feature – in case of connection losses, or hardware watchdog which monitors the status of the router. With the help of a special window (start up script window) you may insert Linux scripts for various actions. For some applications the key option to create several different configurations for one wireless GPRS/EDGE router, the so-called profiles (maximum of 4), and the option to switch between them (for example via SMS, binary input status, etc.) is essential. Cellular wireless routers may automatically upgrade configuration and firmware from server. This allows mass reconfiguration of many routers in one time.



Examples of possible applications:

- mobile office
- image transmission
- security systems
- telematics
- telemetry
- remote monitoring
- monitoring of traffic information
- vending and dispatcher machines

4. Contents of package



Basic delivered set of the router includes:

- router,
- power supply,
- crossover UTP cable,
- external antenna,
- clip for the DIN rail,
- paper start guide.



Figure 1: ER75s router

5. Router design

5.1 Delivery identification

Trade name	Type name	Other
ER75s	ER-75s	Router with one SIM card in plastic box

Table 1: Delivery identification



Figure 2: Label for ER75s

5.2 Ordering codes

Router is supplied in a single version, which can be ordered using this code: **ER75s set**.

5.3 Basic dimensions

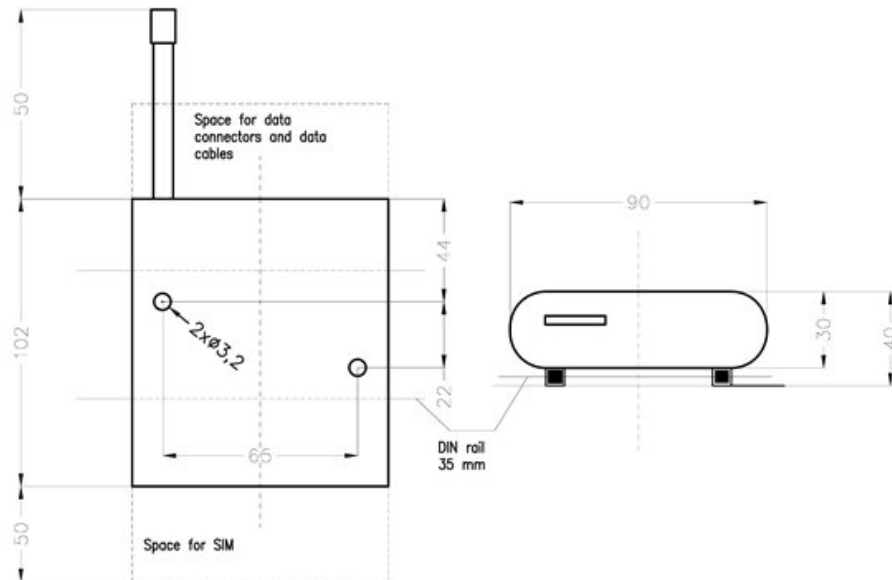


Figure 3: Basic dimensions

5.4 Mechanical dimensions and mounting recommendations



Router is standardly designed for:

- mounting to a panel using through holes,
- possibility to be put on a work surface,
- mounting onto the DIN rail by the plastic clips, which are included.

For the most of applications with a built-in router in a switch board it is possible to recognize two kinds of environments:

- no public and industry environment of low voltage with high interference,
- public environment of low voltage without high interference.

For both of these environments it is possible to mount router to a switch board, the following there is no need to have examination immunity or issues in connection with EMC according to EN 60439-1 ed.2:00 + A1:04 + Opr.1:08 + Z1:10.

For compliance of EN 60439-1 ed.2:00 + A1:04 specification it is necessary to observe next assembly of the router to the switch – board:



- for whip antennas we recommend to observe a distance of 6 cm from cables and metal surfaces on every side according to the next picture due to the elimination of interference, while using an external antenna except for the switch-board it is necessary to fit a lightning conductor,



- before mounting a router on sheet-steel we recommend using an external antenna,

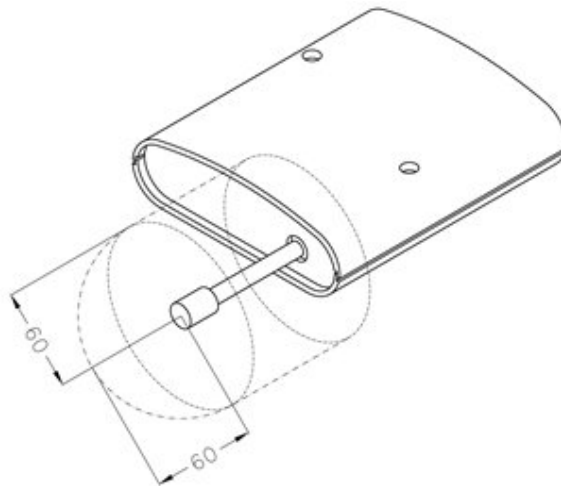


Figure 4: Space around antennas



- For every cables we recommend to bind the bunch according to the following picture, we recommend for this use:
 - Length of the bunch (combination of power supply and data cables) can be maximum 1,5 m. If the length of data cables exceeds 1,5 m or in the event of, the cable leads towards the switch – board. We recommend installing over – voltage protectors (surge suppressors).
 - With data cables they mustn't carry cables with reticular tension $\sim 230 \text{ V}/50 \text{ Hz}$.
 - All signals to sensors must be twisted pairs.

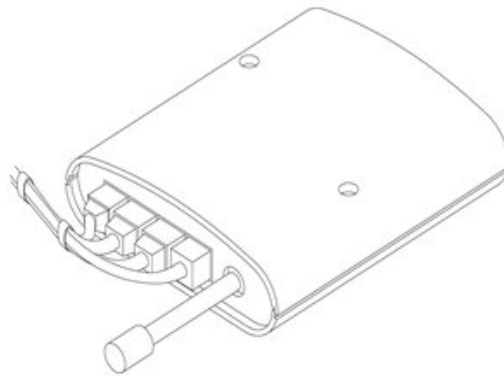


Figure 5: Cable routing



- Sufficient space must be left before individual connectors for handling of cables,

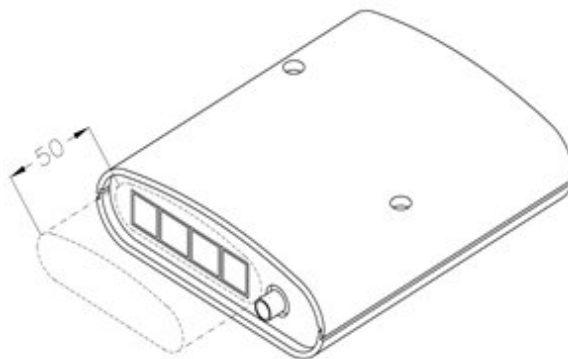


Figure 6: Space in front of connectors



- For correct function of the router we recommend to use in the switch-board earth-bonding distribution frame for grounding of power supply of router, data cables and antenna.

5.5 Description of individual components of the router

5.5.1 GSM/GPRS/EDGE module

Cinterion module is used for GSM network wireless communication. It is integrated into the printed circuit board. The slide-out SIM card reader is accessible from the front panel. The FME antenna connector is accessible from the rear panel.

GSM/GPRS/EDGE module is equipped with a USB 2.0 Full Speed interface which is brought to the USB-B connector marked USB. The module is connected to the control microcomputer via the high-speed serial interface RS232.

GSM/GPRS/EDGE module

- Communicates in four GSM bands (850 MHz, 900 MHz, 1800 MHz a 1900 MHz).
- In the GPRS mode it is able to transmit in three "Time Slots" and receive in two (GPRS multi-slot class 10 – the maximum bit rate of reception is 42.8 kb/s) or transmit in one "Time Slot" and receive in four (GPRS multi-slot class 12 – the maximum bit rate of reception is 85.6 kb/s).
- In the EDGE mode it is able to transmit in three "Time Slots" and receive in two (EDGE multi-slot class 10 – the maximum bit rate of reception is 118.4 kb/s) or transmit in one "Time Slot" and receive in four (GPRS multi-slot class 12 – the maximum bit rate of reception is 236.8 kb/s).
- Supports coding schemes CS1 to CS4 and MCS1 to MCS9.



Attention! The transmitting and receiving in timeslots depends on the operator networks possibilities.

5.5.2 Control microcomputer

The core of the ER75s router is a 32-bit microprocessor with 16 MB RAM, 4 MB FLASH EEPROM, serial interface RS232 and an Ethernet interface 10/100 Mbit/s. The microcomputer is connected to the MC75i OEM module through the serial interface and controls the communication via GSM/GPRS. Towards to the user it is connected on the Ethernet interface.

- The software is built on the uClinux operating system.
- The router supports services such as DHCP, NAT, GRE, IPSec tunnels, etc.
- The router settings are saved in the FLASH EEPROM memory. All configuration of the modem can be done through a web interface (HTTP) which is security password controlled.

5.6 Description of the front and rear panel

On the front panel is located holder for the SIM card. On the rear panel of the router are located the following connectors:

Caption	Connector	Description
PWR	RJ12	Connector for the power supply adapter
ETH	RJ45	Connector for connection into the local computer network
ANT	FME	Connector for main antenna
USB	USB-B	Connector for connection of the router to the PC

Table 2: Description of the rear panel



Figure 7: Front panel

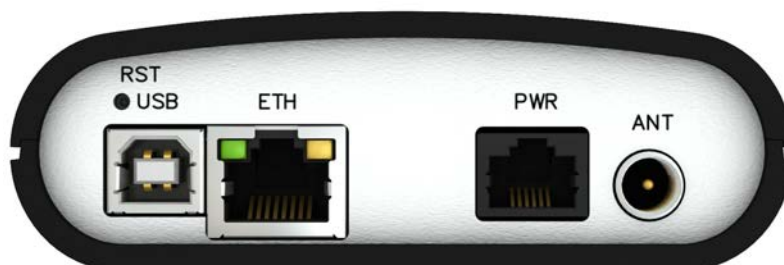


Figure 8: Rear panel

5.6.1 Status indication

Na předním a zadním panelu routeru jsou dohromady tři kontrolky (LED diody), které informují o stavu routeru. Na Ethernetovém portu pak jsou dvě kontrolky informující o stavu nebo aktivitě tohoto portu.

Caption	Color	State	Description
PWR	Green	Blinking (1:9) Fast blinking (9:1) On	Router is ready (connection established) Establishing connection Starting of the router
GSM	Red	Blinking	Communication in progress on radio channel
ETH	Green	On Off	Selected 100 Mbit/s Selected 10 Mbit/s
ETH	Yellow	On Blinking Off	The network cable is connected Data transmission The network cable is not connected
SIM	Yellow	On	SIM card is active

Table 3: Status indication

5.6.2 Power connector PWR

Panel socket RJ12.

Pin number	Signal mark	Description
1	+UN	Positive pole of DC supply voltage (+10 to +30 VDC)
2	NC	Signal not connected
3	NC	Signal not connected
4	+UN	Positive pole of DC supply voltage (+10 to +30 VDC)
5	GND	Negative pole of DC supply voltage
6	GND	Negative pole of DC supply voltage

Table 4: Connection of the PWR supply connector

Power supply for router is required between +10 V to +30 V DC supply. Protection against reversed polarity without signaling is built into the router.

The power consumption during receiving is 1 W. The peak power consumption during data sending is 5.5 W. For correct operation it is necessary that the power source is able to supply a peak current of 1 A.



Circuit example:

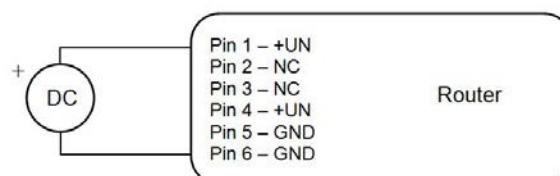


Figure 9: Connection of power supply connector

5.6.3 Antenna connector ANT

Main antenna is connected to the router using the FME connector on the rear panel of the router. The connector is marked with ANT.



The router can not operate without the connected main antenna.

Example of antenna:



Figure 10: External antenna

5.6.4 SIM card reader

The SIM card reader for 3 V and 1.8 V SIM cards is located on the front panel of the router. To initiate the router into operation it is necessary to insert an activated SIM card with unblocked PIN in the reader. The SIM cards might be of different adjusted APN.

Changing the SIM card on the front panel:



1. Before handling of the SIM card turn off the router and disconnect it from power supply.
2. Press the small yellow button to eject the reader holder.
3. Insert the SIM card into the reader holder and slide it in the reader.

5.6.5 ETH port

Panel socket RJ45.

Pin	Signal mark	Description	Data flow direction
1	TXD+	Transmit Data – positive pole	Input/Output
2	TXD-	Transmit Data – negative pole	Input/Output
3	RXD+	Receive Data – positive pole	Input/Output
4	—	—	
5	—	—	
6	RXD-	Receive Data – negative pole	Input/Output
7	—	—	
8	—	—	

Table 5: Connection of Ethernet connector

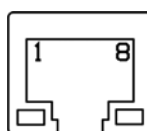


Figure 11: Ethernet connector



ATTENTION! Port ETH is not POE (Power Over Ethernet) compatible!



Example of the ETH router connection:

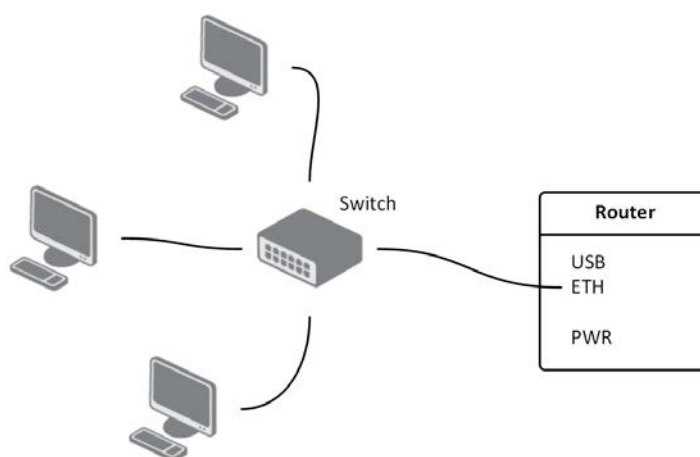


Figure 12: ETH – Example of router connection

5.6.6 USB Port

Panel socket USB-B.

Pin	Signal mark	Description	Data flow direction
1	+5 V	Positive pole of 5 V DC supply voltage	
2	USB data -	USB data signal – negative pole	Input/Output
3	USB data +	USB data signal – positive pole	Input/Output
4	GND	Negative pole of DC supply voltage	

Table 6: Connection of USB connector



Figure 13: USB connector



Example of the USB router connection:

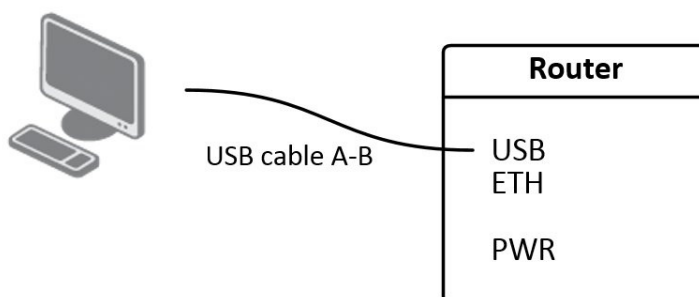


Figure 14: USB – Example of router connection

5.6.7 Reset



It is important to distinguish between reset and reboot the router.

Action	Router behavior	Invoking events
Reboot	Turn off and then turn on router	Disconnect and connect the power, Press the <i>Reboot</i> button in the web configuration
Reset	Restore default configuration and reboot the router	Press RST button

Table 7: Description of reset and restart router

After green LED starts to blink it is possible to restore initial settings of the router by pressing button RST on front panel. After pressing RST button it is restoration of default configuration and reboot (green LED will be on). For pressing the RST button could be used a narrow screwdriver.

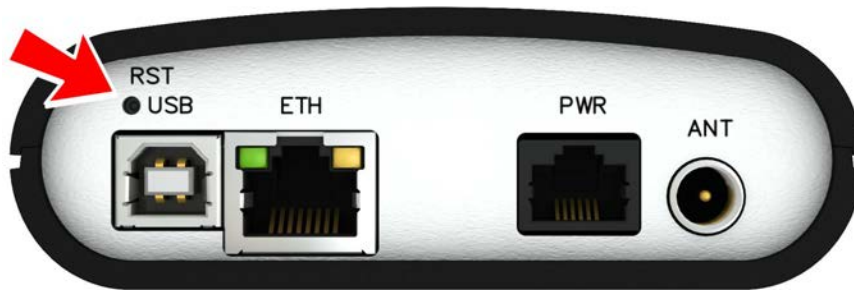


Figure 15: Router reset



We recommend to backup your router configuration (see chapter [8 Configuration via web browser](#)), because after reset router set configuration to the initial state.

6. First use

6.1 Connecting the router before first use

Before you give up the router, it is necessary to connect all components needed for the operation of your applications and the SIM card must be inserted (see figure below).



The router can not operate without connected antenna, SIM card and power supply. If the antenna is not connected, router can be damaged.

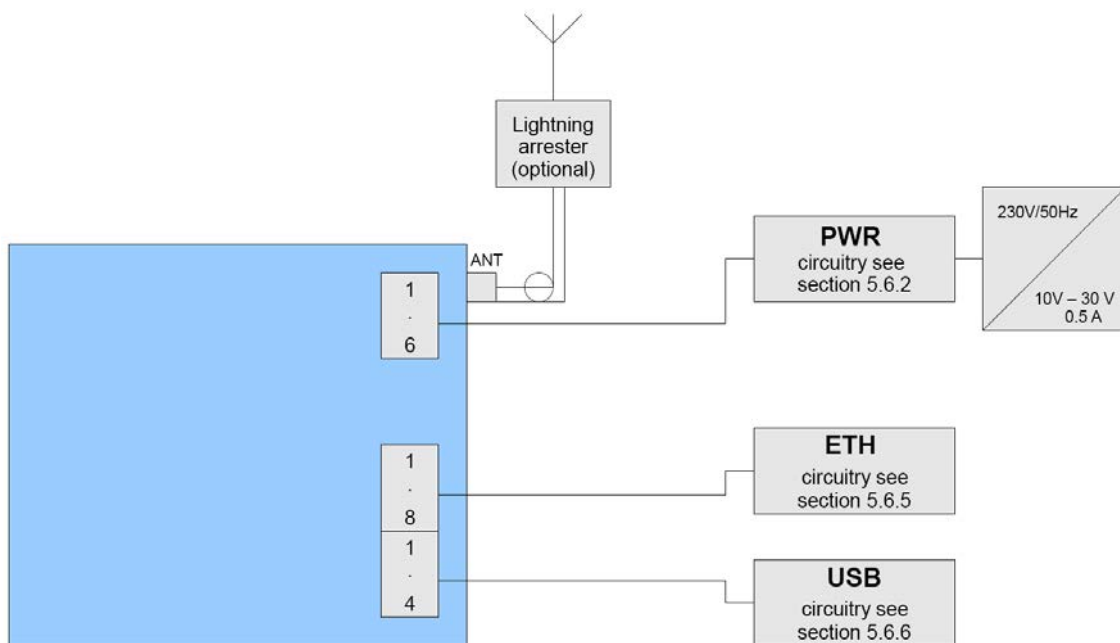


Figure 16: Router connection

6.2 Start

The router is set up connecting the power supply to the router. In the default setting the router starts to login automatically to the preset APN. Device on the Ethernet port DHCP server will assign addresses. The behavior of the router can be modified by means of the web or Telnet interface, which is described in chapter [8 Configuration via web browser](#).

The power consumption during receiving is 1 W. The peak power consumption during data sending is 5,5 W. For correct operation it is necessary that the power source is able to supply a peak current of 1 A.

6.3 Configuration



Attention! If the SIM card is not inserted in the router, then it is impossible to operate. The inserted SIM card must have activated EDGE/GPRS.

6.3.1 Configuration over web browser

Monitoring of the status, configuration and administration of the router can be performed by means of the web interface, which is available after insertion of IP address of the router into the web browser. The default IP address of the router is 192.168.1.1. Configuration may be performed only by the user "root" with initial password "root".



A detailed description of the router settings via the Web interface can be found in chapter [8 Configuration via web browser](#).

6.3.2 Configuration over Telnet

Monitoring of status, configuration and administration of the router can be performed by means of the Telnet interface. After IP address entry to the Telnet interface it is possible to configure the router by the help of commands. The default IP address of the router is 192.168.1.1. Configuration may be performed only by the user "root" with initial password "root".



A detailed description of the router settings via the Telnet interface can be found in chapter [9 Configuration setting over Telnet](#).

7. Technical parameters

7.1 Technical parameters of router

ER75s		
Complies with standards		ETSI EN 301 511 V12.5.1 ETSI EN 301 489-1 V2.1.1 EN 55032:2015 Class A EN 60950-1:06 ed.2 + A11:09 + A1:10
Temperature range	Function Storage	-30 °C to +60 °C -40 °C to +85 °C
Protection		IP20
Supply voltage		10 to 30 V DC
Consumption	Reception Transmission	1 W 5,5 W
Dimensions	Plastic box	30 x 90 x 102 mm (DIN rail 35 mm)
Weight		140 g
Antenna connector		FME – 50 Ohm
User interfaces	ETH USB	Ethernet (10/100 Mbit/s) USB 2.0

Table 8: Technical parameters of router

7.2 Technical parameters of module

EDGE modul	
Frequency bands	EGSM850, EGSM900, GSM1800 and GSM1900
Transmit power	Class 4 (2 W) for EGSM850 Class 4 (2 W) for EGSM900 Class 1 (1 W) for GSM1800 Class 1 (1 W) for GSM1900

Table 9: Technical parameters of module

Attention! If the SIM card is not inserted in the router, then wireless transmissions will not work. The inserted SIM card must have activated GPRS. Insert the SIM card when the router is switched-off.

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

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



Figure 16: Web configuration



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

8.1 General

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*, *Peripherals Ports* and *System Information*.

8.1.1 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 10: Mobile connection

8.1.2 Primary LAN

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

8.1.3 Peripheral Ports

ER75s can be equipped with no expansion port, so in this section is always displayed this information: *Expansion Port: None*.

8.1.4 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 11: System Information

8.2 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 in which the router is operated. There is also information about the module, which is mounted in the router.

Item	Description
Registration	State of the network registration
Operator	Specifies the operator in whose network the router is operated
Technology	Transmission technology
PLMN	Code of operator
Cell	Cell to which the router is connected
LAC	Location Area Code – unique number assigned to each location area
Channel	Channel on which the router communicates
Signal Strength	Signal strength of the selected cell
Neighbours	Signal strength of neighboring hearing cells
Manufacturer	Module manufacturer
Model	Type of module
Revision	Revision of module

Continued on next page

Continued from previous page

Item	Description
IMEI	IMEI (International Mobile Equipment Identity) number of module

Table 12: 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 13: Description of period

Item	Description
Signal Min	Minimal signal strength
Signal Avg	Average signal strength
Signal Max	Maximal signal strength
Cells	Number of switch between cells
Availability	Availability of ER75s via the mobile network (expressed as a percentage)

Table 14: 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 card (for each period).

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

Table 15: Traffic statistics

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

Mobile WAN Status

Mobile Network Information

Registration : Home Network

Operator : T-Mobile CZ

Technology : EDGE

PLMN : 23001

Cell : 69A6

LAC : 353E

Channel : 30

Signal Strength : -71 dBm

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

> More Information <

Mobile Network Statistics

	Today	Yesterday	This Week	Last Week	This Period	Last Period
Signal Min	: -108 dBm	-121 dBm	-121 dBm	-121 dBm	-121 dBm	-121 dBm
Signal Avg	: -71 dBm	-71 dBm	-71 dBm	-69 dBm	-70 dBm	-85 dBm
Signal Max	: -65 dBm	-65 dBm	-65 dBm	-63 dBm	-63 dBm	-58 dBm
Cells	: 15	261	525	206	730	962
Availability	: 99.7%	99.7%	99.7%	99.7%	99.7%	97.5%

Traffic Statistics for Primary SIM card

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

Traffic Statistics for Secondary SIM card

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

Mobile Network Connection Log

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

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

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

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

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

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

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

Figure 17: Mobile WAN status

8.3 Network status

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

Interface	Description
eth0, eth1	Network interfaces (ethernet connection)
ppp0	Interface (active connection to GPRS/EDGE)
tun0	OpenVPN tunnel interface
ipsec0	IPSec tunnel interface
gre1	GRE tunnel interface
usb0	USB interface

Table 16: Description of interface in network status

U každého rozhraní jsou pak zobrazeny následující informace:

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
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

Continued on next page

Continued from previous page

Item	Description
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 17: 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 mobile network is active, then it is in the system information shown as a ppp0 interface.

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

Figure 18: Network status

8.4 DHCP status

Information on the activities of the DHCP server can be accessed by selecting the *DHCP status* item. The DHCP server provides automatic configuration of devices connected to the network managed router. DHCP server assigns to each device's IP address, netmask, default gateway (IP address of router) and DNS server (IP address of router).

For each configuration, the *DHCP status* window displays the following information:

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 18: 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 19: DHCP status

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

8.5 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 is only internal character.

```

IPsec Status
IPsec Tunnels Information

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+ENC+CRYPT+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@10.0.1.132 tun.0@10.0.1.228 tun.0@10.0.1.132 ref=0 refhim=4294
#1: "ipsecl":500 STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in 2733s; newest ISAKMP; lastdpd=-1s(se

```

Figure 20: IPsec status

8.6 DynDNS status

The result of updating DynDNS record on the server www.dyndns.org can be invoked by pressing the *DynDNS* item in the menu.

```

DynDNS Status
Last DynDNS Update Status

DynDNS record successfully updated.

```

Figure 21: DynDNS status

In detecting the status of updates DynDNS record are possible following message:

- 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 DynDNS, SIM card of router must have assigned public IP address.

8.7 System log

In case of any problems with connection to GPRS it is possible to view the system log by pressing the *System Log* menu item. In the window, are displayed detailed reports from individual applications running in the router. Use the *Save Log* button to save the system log to a connected computer. The second button – *Save Report* – is used for creating detailed report (generates all support needed information in one file).

The Syslog default size is 1000 lines. After reaching 1000 lines create a new file for storing system log. After completion of the 1000 lines in the second file, the first file is deleted and creates a new one.

Program syslogd can be started with two options that modifies its behavior. Option "-s" followed by decimal number set maximal number of lines in one log file. Option "-r" followed by hostname or IP address enable logging to remote syslog daemon. In the Linux must be enabled remote logging on the target computer. Typically running syslogd with the parameter "-r". On Windows must be installed the syslog server (for example Syslog Watcher). For starting syslogd with these options you could modify script "/etc/init.d/syslog" or add lines "killall syslogd" and "syslogd <options> &" into Startup Script.

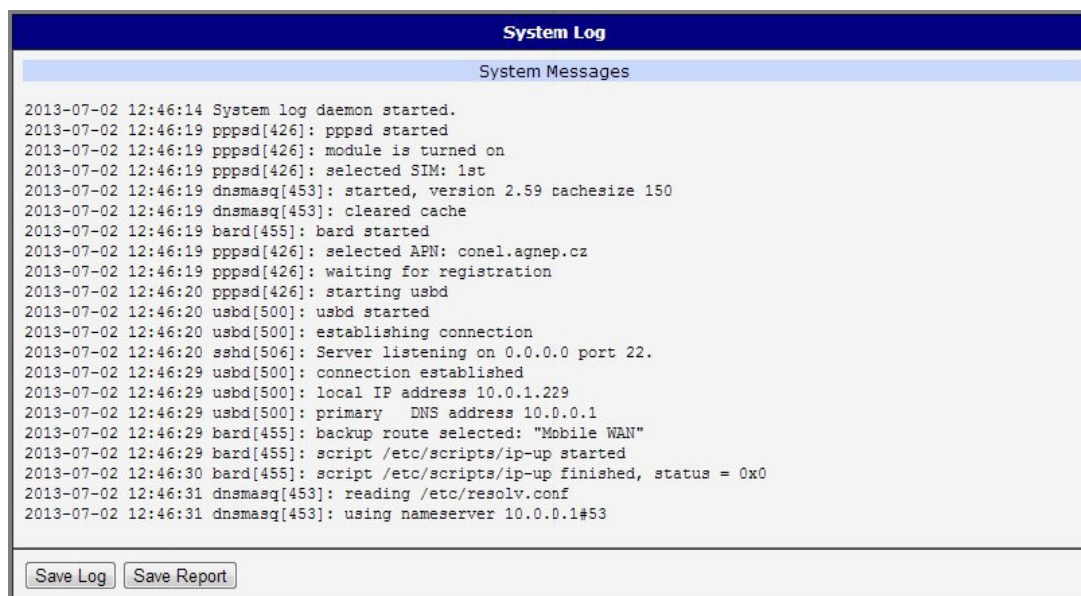


Figure 22: System log

Example of logging into the remote daemon at 192.168.2.115:

```

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

killall syslogd
syslogd -R 192.168.2.115
    
```

Figure 23: Example program syslogd start with the parameter -r

8.8 LAN configuration

To enter the network configuration, select the *LAN* menu item.

Item	Description
IP address	Fixed set IP address of network interface ETH.
Subnet Mask	IP address of Subnet Mask.
Media type	<ul style="list-style-type: none"> • Auto-negation – The router selects the speed of communication of network options. • 100 Mbps Full Duplex – The router communicates at 100Mbps, in the full duplex mode. • 100 Mbps Half Duplex – The router communicates at 100Mbps, in the half duplex mode. • 10 Mbps Full Duplex – The router communicates at 10Mbps, in the full duplex mode. • 10 Mbps Half Duplex – The router communicates at 10Mbps, in the half duplex mode.
Default Gateway	IP address of router default gateway. When entering IP address of default gateway, all packets for which the record was not found in the routing table, sent to this address.
DNS server	IP address of DNS server of router. Address where they are forwarded to all DNS questions on the router.

Table 19: Configuration of network interface

Default Gateway and *DNS Server* items are used only if LAN is selected by Backup routes system as a default route (selection algorithm is described in section [8.11 Backup Routes](#)).

DHCP server assigns IP address, gateway IP address (IP address of the router) and IP address of the DNS server (IP address of the router) to the connected clients. If these values

are filled-in by the user in the configuration form, they are preferred.

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

Item	Description
Enable dynamic DHCP leases	If this option is checked, dynamic DHCP server is enable.
IP Pool Start	Start IP addresses space to be allocated to the DHCP clients.
IP Pool End	End IP addresses space to be allocated to the DHCP clients.
Lease time	Time in seconds, after which the client can use IP address.

Table 20: Configuration of dynamic DHCP server

Item	Description
Enable static DHCP leases	If this option is checked, static DHCP server is enable.
MAC Address	MAC address of a DHCP client.
IP Address	Assigned IP address.

Table 21: Configuration of static DHCP server



It is important not to overlap ranges of static allocated IP address with address allocated by the dynamic DHCP. Then risk collision of IP addresses and incorrect function of network.

Example of 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).

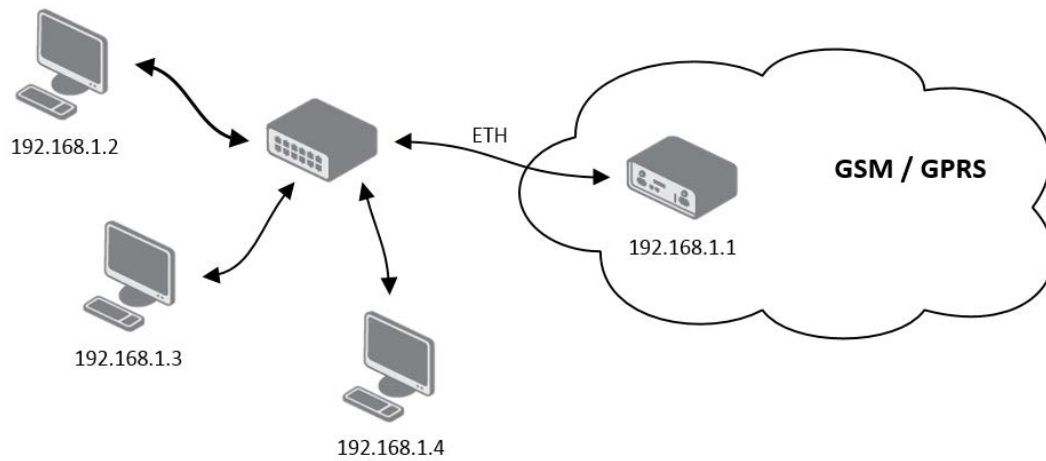


Figure 24: Topology of example LAN configuration 1

LAN Configuration	
IP Address	<input type="text" value="192.168.1.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Media Type	<input type="text" value="auto-negotiation"/>
Default Gateway	<input type="text"/>
DNS Server	<input type="text"/>
<input checked="" type="checkbox"/> Enable dynamic DHCP leases	
IP Pool Start	<input type="text" value="192.168.1.2"/>
IP Pool End	<input type="text" value="192.168.1.4"/>
Lease Time	<input type="text" value="600"/> sec
<input type="checkbox"/> Enable static DHCP leases	
MAC Address	IP Address
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="button" value="Apply"/>	

Figure 25: Example LAN configuration 1

Example of 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's with MAC address 01:23:45:67:89:ab has IP address 192.168.1.10.
- Client's with MAC address 01:54:68:18:ba:7e has IP address 192.168.1.11.

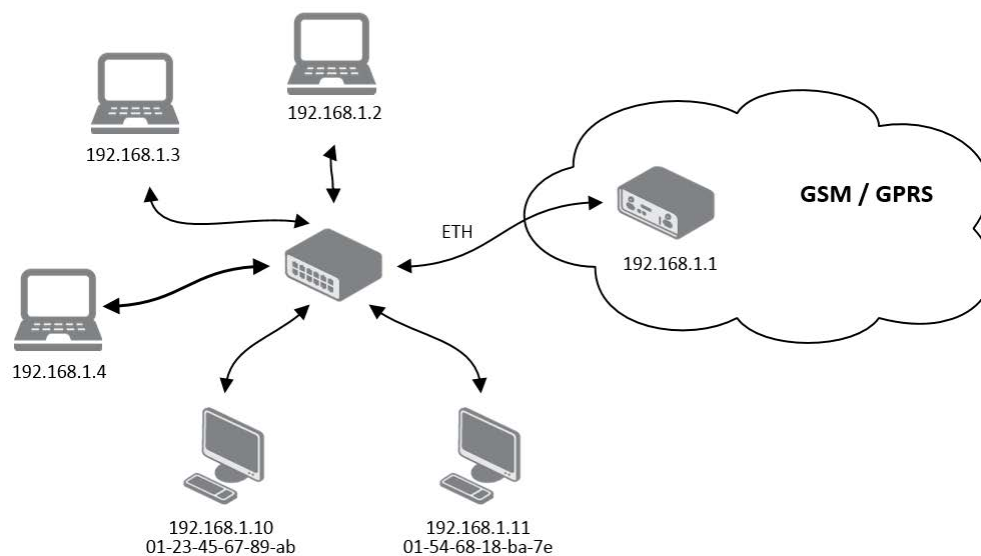


Figure 26: Topology of example LAN configuration 2

LAN Configuration	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Media Type	auto-negotiation
Default Gateway	
DNS Server	
<input checked="" type="checkbox"/> Enable dynamic DHCP leases	
IP Pool Start	192.168.1.2
IP Pool End	192.168.1.4
Lease Time	600 sec
<input type="checkbox"/> Enable static DHCP leases	
MAC Address	IP Address
01:23:45:67:89:ab	192.168.1.10
01:54:68:18:ba:7e	192.168.1.11
Apply	

Figure 27: Example LAN configuration 2

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

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

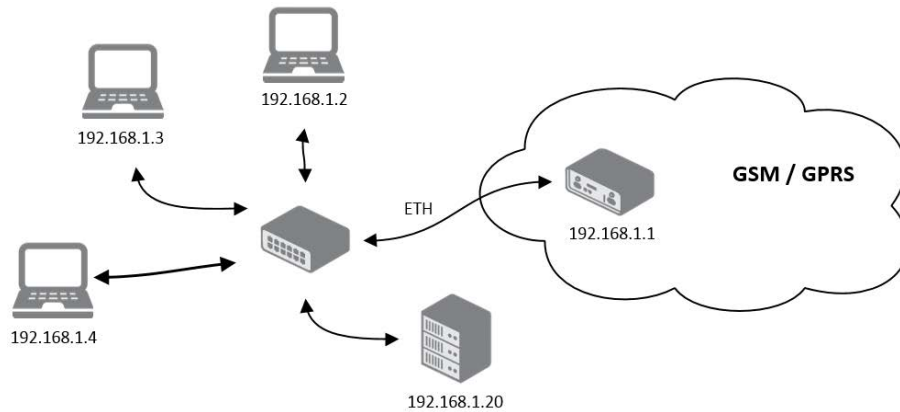


Figure 28: Topology of example LAN configuration 3

LAN Configuration	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Media Type	auto-negotiation
Default Gateway	192.168.1.20
DNS Server	192.168.1.20
<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 29: Example LAN configuration 3

8.9 VRRP configuration

To enter the VRRP configuration select the *VRRP* menu item. VRRP protocol (Virtual Router Redundancy Protocol) is a technique, by which it is possible to forward routing from main router to backup router in the case of the main router failure. If the *Enable VRRP* is checked, then it is possible to set the following parameters.

Item	Description
Virtual Server IP Address	This parameter sets virtual server IP address. This address should be the same for both routers. A connected device sends its data via this virtual address.
Virtual Server ID	Parameter Virtual Server ID distinguishes one virtual router on the network from others. Main and backup routers must use the same value for this parameter.
Host Priority	The router, with higher priority set by the parameter Host Priority, is the main router. According to RFC 2338 the main router has the highest possible priority - 255. The backup router has priority in range 1 – 254 (init value is 100). The priority value equals 0 is not allowed.

Table 22: VRRP configuration

It is possible to set *Check connection* flag in the second part of the window. The currently active router (main/backup) will send testing messages to defined *Ping IP Address* at periodic time intervals (*Ping Interval*) with setting time of waiting for answer (*Ping Timeout*). The function check connection is used as a supplement of VRRP standard with the same final result. If there are no answers from remote devices (*Ping IP Address*) for a defined number of probes (*Ping Probes*), then connection is switched to the other line.

Item	Description
Ping IP Address	Destination IP address of ping queries. Address can not be specified as domain name.
Ping Interval	Time intervals between the outgoing pings.
Ping Timeout	Time to wait to answer.
Ping Probes	Number of failed ping requests, after which the route is considered to be impassable.

Table 23: Check connection



Ping IP address is possible to use for example a DNS server of mobile operator as a test message (ping) IP address.

There's an additional way for evaluating the state of the active line. It is activated by selecting *Enable traffic monitoring* parameter. If this parameter is set and any packet different from ping is sent to the monitored line, then any answer to this packet is expected for *Ping Timeout*. If *Ping Timeout* expires with no answer received then process of testing the active line contin-

ues the same way like in the case of standard testing process after first test message answer drops out.

Example of the VRRP protocol:

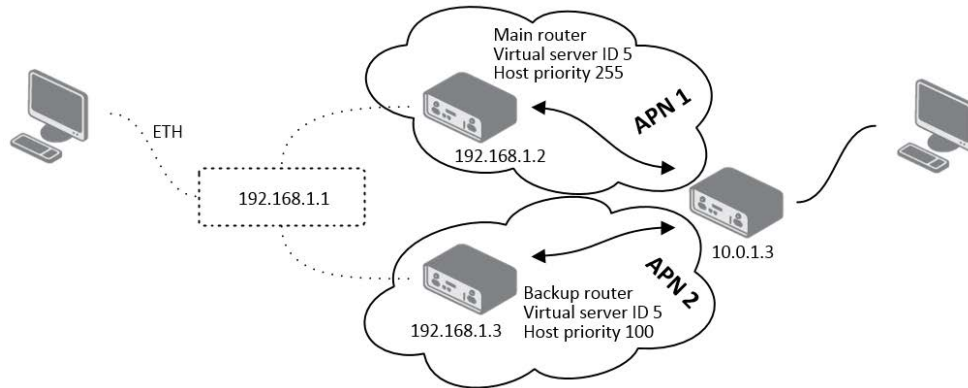


Figure 30: Topology of example VRRP configuration

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 31: Example VRRP configuration — main router

8.10 Mobile WAN configuration

The form for configuration of a connection to the mobile network can be invoked by selecting the *Mobile WAN* item in the main menu of the router web interface.

8.10.1 Mobile WAN

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

VRRP Configuration

☒ Enable VRRP

Virtual Server IP Address

Virtual Server ID

Host Priority

☒ Check connection

Ping IP Address

Ping Interval

sec

Ping Timeout

sec

Ping Probes

☐ Enable traffic monitoring

Figure 32: Example VRRP configuration -- backup router

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.

Continued on next page

Continued from previous page

Item	Description
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 24: 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.**
- **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.

8.10.2 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).

8.10.3 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 25: 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 feature of check connection to mobile network is necessary for uninterrupted operation.

8.10.4 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 26: 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.

8.10.5 Configuration of switching between APNs

At the bottom of configuration it is possible to set rules for switching between two APN's on one SIM card.

Item	Description
Default SIM card	This parameter sets default APN, 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, that the router will switch the defining one of the following rules.

Table 27: Default and backup APN 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 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 APN of the SIM card. If home network is detected, this parameter enables switching back to default APN. 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 APN of the SIM card, when the data limit of default APN is exceeded. This parameter also enables switching back to default APN, when data limit is not exceeded.
Switch to default SIM card after timeout	This parameter defines the method, how the router will try to switch back to default APN.

Continued on next page

Continued from previous page

Item	Description
------	-------------

Table 28: Configuration of switching between APNs I

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

Item	Description
Initial timeout	The first attempt to switch back to the primary 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 APN, 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 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 29: Configuration of switching between APNs II

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 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).

8.10.6 Dial-In access configuration

In the bottom part of the window it is possible to define access over CSD connection by *Enable Dial-In Access* function. Access can be secured by used the *Username* and *Password*. In the event that this function is enabled and the router does not have a connection to mobile network is granted access to the router via dial-up connections CSD. The router waits 2 minutes to accept connections. If the router during this time nobody logs on, the router will try again to establish a GPRS connection.

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

Table 30: Dial-In access configuration

8.10.7 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. There will be allot Ip address of SIM card to PC.

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

Mobile WAN Configuration			
<input type="checkbox"/> Create connection to mobile network			
	Primary SIM card	Secondary SIM card	
APN *	<input type="text"/>	<input type="text"/>	
Username *	<input type="text"/>	<input type="text"/>	
Password *	<input type="text"/>	<input type="text"/>	
Authentication	PAP or CHAP ▼	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"/>	
PIN *	<input type="text"/>	<input type="text"/>	
MRU	1500	1500	bytes
MTU	1500	1500	bytes
DNS Settings	get from operator ▼	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	disabled ▼	disabled ▼	
Ping IP Address	<input type="text"/>	<input type="text"/>	
Ping Interval	<input type="text"/>	<input type="text"/>	sec
<input type="checkbox"/> Enable traffic monitoring			
Data Limit	<input type="text"/>	MB	
Warning Threshold	<input type="text"/>	%	
Accounting Start	1		
Default SIM card	primary ▼		
Backup SIM card	secondary ▼		
<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 default SIM card after timeout			
Initial Timeout	60	min	
Subsequent Timeout *	<input type="text"/>	min	
Additive Constant *	<input type="text"/>	min	
<input type="checkbox"/> Enable Dial-In access			
Username *	<input type="text"/>		
Password *	<input type="text"/>		
<input type="checkbox"/> Enable PPPoE bridge mode			
* can be blank			
<input type="button" value="Apply"/>			

Figure 33: Mobile WAN configuration

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 APN and on the address www.google.com in the time interval 80 s for secondary APN. 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 34: Example of Mobile WAN configuration 1

The following configuration illustrates the situation in which the router switches to a backup APN 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 default SIM card after timeout

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

Figure 35: Example of Mobile WAN configuration 2

Primary APN is switched to the offline mode after the router detects roaming. The first attempt to switch back to the default APN 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 default SIM card after timeout

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

Figure 36: Example of Mobile WAN configuration 3

8.11 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*).

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 Primary 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.

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)
- Primary LAN (eth0)

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 31: Backup Routes

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

8.12 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 accessibility is checked against the table with IP addresses. This means that access is permitted only addresses specified in the table. It is possible to define up to eight remote accesses. There are the following parameters:

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 Primary LAN
Priority	1st
Ping IP Address	
Ping Interval	sec
<input type="button" value="Apply"/>	

Figure 37: Backup Routes

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 32: 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 are automatically accepted. If this item is checked and incoming packet is addressed to another network interface, it will go to the FORWARD chain. In case that the FORWARD chain accepted this packet (there is a rule for its forwarding), it will be sent out. If the forwarding rule does not exist, packet will be dropped.

Then there is a table for defining the rules. It is possible to allow all traffic within the selected protocol (rule specifies only protocol) or create stricter rules by specifying items for source IP address, destination IP address and port.

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

Table 33: 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 per second for five.

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 ▼

☐ 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 ▼

☐ Enable filtering of locally destined packets

☐ Enable protection against DoS attacks
** can be blank*

Figure 38: 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 any ports
- from address 142.2.26.54 using ICMP protocol

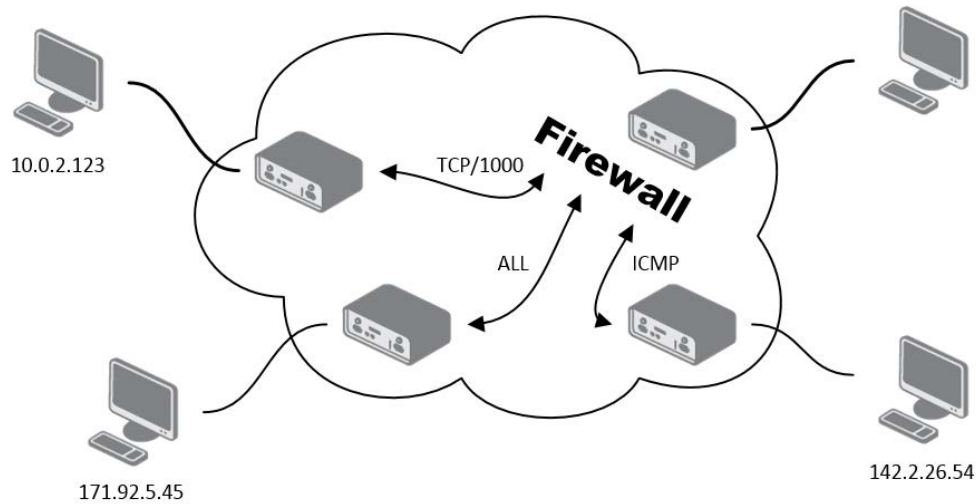


Figure 39: Topology of example firewall configuration

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 40: Example firewall configuration

8.13 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 34: NAT configuration

If necessary set more than sixteen rules for NAT rules, then is possible insert into start up script following script:

```
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 35: Configuration of send all incoming packets

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

Item	Description
Enable remote HTTP 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 FTP access on port	Choice this item and port number makes it possible to access over FTP (disabled in default configuration).
Enable remote Telnet access on port	Choice this item and port number makes it possible to access over Telnet (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 36: Remote access configuration

Example of the configuration with one connection equipment on the router:

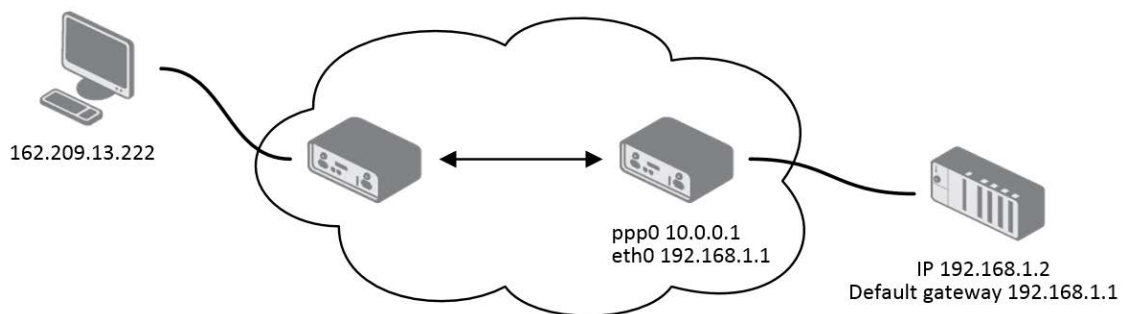


Figure 41: Topology of example NAT configuration 1

[illegible]

Figure 42: Example NAT configuration 1

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 of the configuration with more connected equipment:

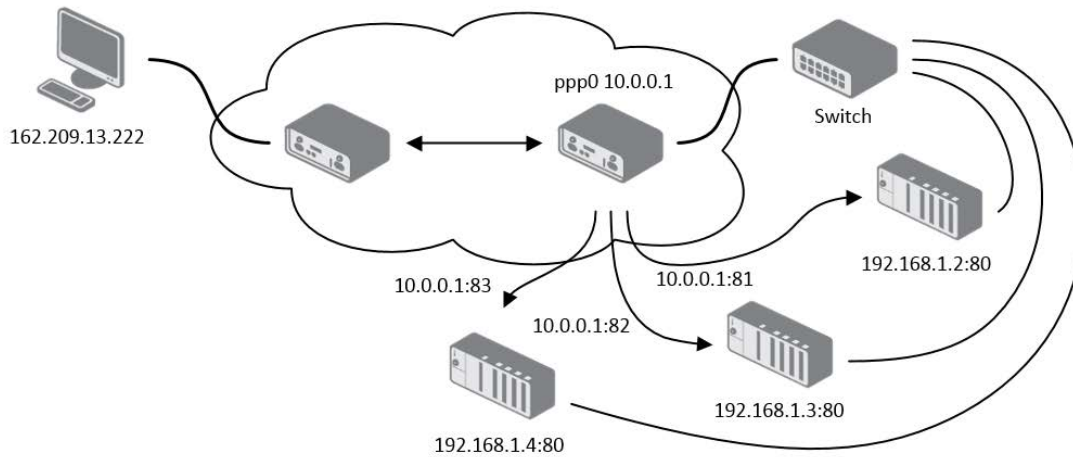


Figure 43: Topology of example NAT configuration 2

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

☒ Enable remote HTTP access on port

☒ Enable remote FTP access on port

☒ Enable remote Telnet access on port

☒ Enable remote SNMP access on port

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

☒ Masquerade outgoing packets

Figure 44: Example NAT configuration 2

In this configuration equipment wired behind the router defines the address *Server IP Address*. The router replies, while PING on address of SIM card. Access on web interface of the equipment behind the router is possible by the help of Port Forwarding, when behind IP address of SIM is indicating public port of equipment on which we want to come up. At demand on port 80 it is surveyed singles outer ports (Public port), there this port isn't defined, therefore at check selection Enable remote http access it automatically opens the web interface router. If this choice isn't selected and is selected volition Send all remaining incoming packets to the default server fulfill oneself connection on induction IP address. If it is not selected selection *Send all remaining incoming packets to default server* and *Default server IP address* then connection requests a failure.

8.14 OpenVPN tunnel configuration

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

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

Table 37: Overview OpenVPN tunnels

Figure 45: OpenVPN tunnels configuration

Item	Description
Description	Description (or name) of tunnel

Continued on next page

Continued from previous page

Item	Description
Protocol	<p>Communication protocol:</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
UDP/TCP port	Port of the relevant protocol (UDP or TCP)
Remote IP Address	IP address of opposite tunnel side (domain name can be used)
Remote Subnet	IP address of a network behind opposite tunnel side
Remote Subnet Mask	Subnet mask of a network behind opposite tunnel side
Redirect Gateway	Allows to redirect all traffic on Ethernet
Local Interface IP Address	Defines the IP address of a local interface
Remote Interface IP Address	Defines the IP address of the interface of opposite tunnel side
Ping Interval	Defines the time interval after which sends a message to opposite side of tunnel for checking the existence of the tunnel.
Ping Timeout	Defines the time interval during which the router waits for a message sent by the opposite side. For proper verification of OpenVPN tunnel, <i>Ping Timeout</i> must be greater 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, router changes the tunnel encryption to ensure the continues safety of the tunnel.
Max Fragment Size	Defines the maximum size of a sent packet
Compression	<p>Sent data can be compressed:</p> <ul style="list-style-type: none"> • none – no compression is used • LZO – a lossless compression is used (must be set on both sides of the tunnel!)

Continued on next page

Continued from previous page

Item	Description
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
Authenticate Mode	Sets authentication mode: <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	It can be used for X.509 Certificate authentication mode.
Username	Authentication using a login name and password authentication can be used for username/password mode.
Password	Authentication using a login name and password authentication can be used for username/password mode.
Extra Options	Allows to define additional parameters of OpenVPN tunnel such as DHCP options etc.

Table 38: OpenVPN tunnels configuration

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

OpenVPN Tunnel Configuration

☐ Create 1st OpenVPN tunnel

Description *

ProtocolUDP

UDP port1194

Remote IP Address *

Remote Subnet *

Remote Subnet Mask *

Redirect Gatewayno

Local Interface IP Address

Remote Interface IP Address

Ping Interval *sec

Ping Timeout *sec

Renegotiate Interval *sec

Max Fragment Size *bytes

CompressionLZO

NAT Rulesnot applied

Authenticate Modenone

Pre-shared Secret

CA Certificate

DH Parameters

Local Certificate

Local Private Key

Username

Password

Extra Options *

* can be blank

Apply

Figure 46: OpenVPN tunnel configuration

Example of the OpenVPN tunnel configuration:

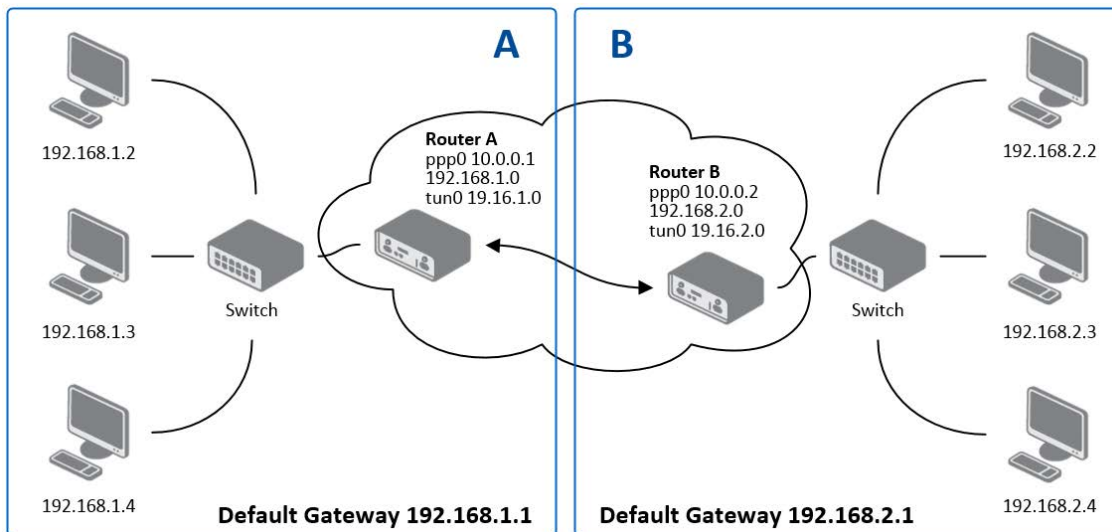


Figure 47: Topology of example OpenVPN configuration

OpenVPN tunnel configuration:

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

Table 39: Example OpenVPN configuration

Examples of different options for configuration and authentication of OpenVPN can be found in the application note *OpenVPN tunnel* (see [3]).

8.15 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	This item displays the name of the tunnel specified in the configuration of the tunnel.
Edit	Configuration IPsec tunnel.

Table 40: Overview IPsec tunnels

Figure 48: IPsec tunnels configuration

Item	Description
Description	Description of tunnel.
Remote IP Address	IP address of opposite side tunnel. Can be used domain main.
Remote ID	Identification of opposite side tunnel. Parameters ID contain two parts: hostname and domain-name.
Remote Subnet	Address nets behind off – side tunnel
Remote Subnet Mask	Subnet mask behind off – side tunnel
Local ID	Identification of local side. Parameters ID contain two parts: hostname and domain-name.
Local Subnet	Local subnet address
Local subnet mask	Local subnet mask
Encapsulation Mode	IPsec mode – you can choose tunnel or transport
NAT traversal	If address translation between two end points of the IPsec tunnel is used, it needs to allow NAT Traversal

Continued on next page

Continued from previous page

Item	Description
IKE Mode	Defines mode for establishing connection (<i>main</i> or <i>aggressive</i>). If the <i>aggressive</i> mode is selected, establishing of IPsec tunnel will be faster, but encryption will set permanently on 3DES-MD5.
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 or SHA1
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 or SHA1
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 60s. The maximum value is 86400 s.
IKE Lifetime	Lifetime key service part of tunnel. The minimum value of this parameter is 60s. The maximum value is 86400 s.
Rekey Margin	Specifies how long before connection expiry should attempt to negotiate a replacement begin. The maximum value must be less than half the parameters IKE and Key Lifetime.
Rekey Fuzz	Specifies the maximum percentage by which should be randomly increased to randomize re-keying intervals
DPD Delay	Defines time after which is made IPsec tunnel verification
DPD Timeout	By parameter DPD Timeout is set timeout of the answer

Continued on next page

Continued from previous page

Item	Description
Authenticate Mode	By this parameter can be set authentication: <ul style="list-style-type: none"> • Pre-shared key – shared key for both off-side tunnel • X.509 Certificate – allows X.509 certification in multiclient mode
Pre-shared Key	Sharable key for both parties tunnel.
CA Certificate	This certificate is necessary to insert Authentication mode x.509.
Remote Certificate	This certificate is necessary to insert Authentication mode x.509.
Local Certificate	This certificate is necessary to insert Authentication mode x.509.
Local Private Key	This private key is necessary to insert Authentication mode x.509.
Local Passphrase	This Local Passphrase is necessary to insert Authentication mode x.509.
Extra Options	Use this parameter to define additional parameters of the IPsec tunnel, for example secure parameters etc.

Table 41: OpenVPN tunnels configuration



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, after which it will re-exchange of new keys are defined:

*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.

Example of the IPSec Tunnel 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 42: Example IPsec configuration

Examples of different options for configuration and authentication of IPsec can be found in the application note *IPsec tunnel* (see [4]).

8.16 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 43: Overview GRE tunnels

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, 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 44: GRE tunnel configuration



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

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

Example of the 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 45: Example GRE tunnel configuration

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"/>
Local ID *	<input type="text"/>
Local Subnet *	<input type="text"/>
Local Subnet Mask *	<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 *	sec
DPD Timeout *	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 49: IPsec tunnels configuration

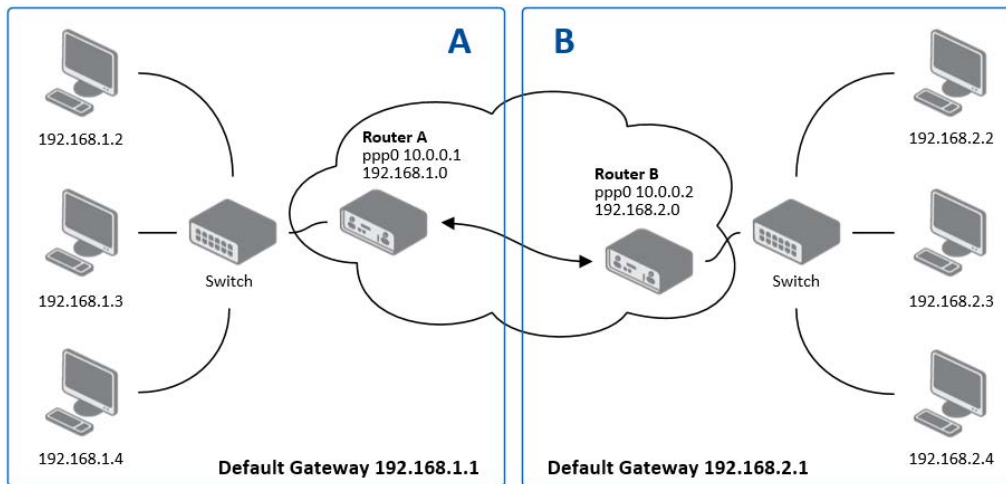


Figure 50: Topology of example IPsec configuration

GRE Tunnels Configuration		
Create	Description	
1st	<input type="text" value="no"/>	<input type="button" value="Edit"/>
2nd	<input type="text" value="no"/>	<input type="button" value="Edit"/>
3rd	<input type="text" value="no"/>	<input type="button" value="Edit"/>
4th	<input type="text" value="no"/>	<input type="button" value="Edit"/>
<input type="button" value="Apply"/>		

Figure 51: GRE tunnels configuration

GRE Tunnel Configuration	
<input type="checkbox"/>	Create 1st GRE tunnel
Description *	<input type="text"/>
Remote IP Address	<input type="text"/>
Remote Subnet *	<input type="text"/>
Remote Subnet Mask *	<input type="text"/>
Local Interface IP Address *	<input type="text"/>
Remote Interface IP Address *	<input type="text"/>
Multicasts	<input type="text" value="disabled"/>
Pre-shared Key *	<input type="text"/>
* can be blank	
<input type="button" value="Apply"/>	

Figure 52: GRE tunnel configuration

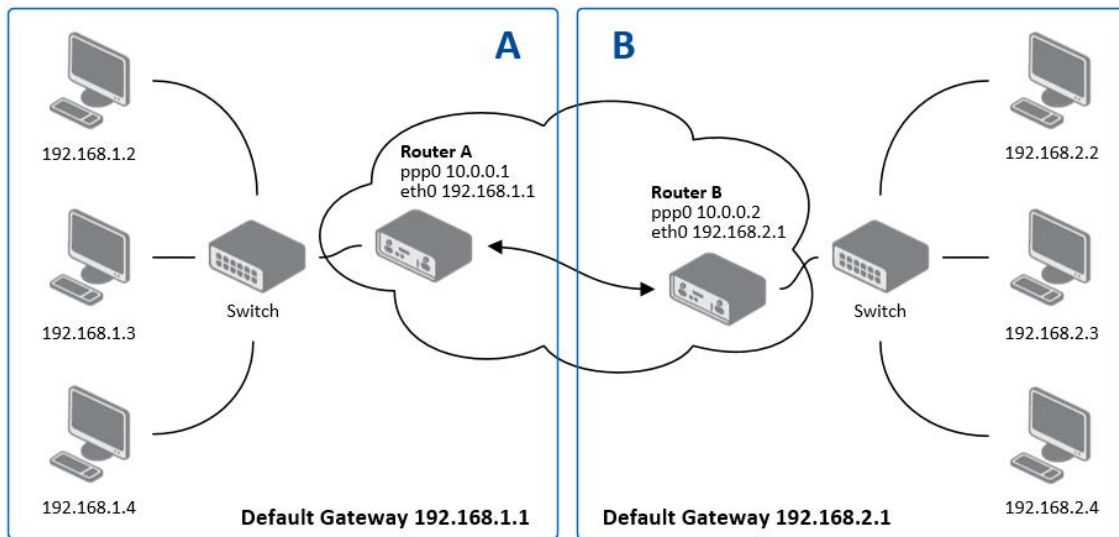


Figure 53: Topology of GRE tunnel configuration

8.17 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 46: L2TP tunnel configuration

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

L2TP Tunnel Configuration

☐ Create L2TP tunnel
Mode: L2TP client
Server IP Address:
Client Start IP Address:
Client End IP Address:
Local IP Address *:
Remote IP Address *:
Remote Subnet *:
Remote Subnet Mask *:
Username:
Password:
** can be blank*

Figure 54: L2TP tunnel configuration

Example of the L2TP Tunnel configuration:

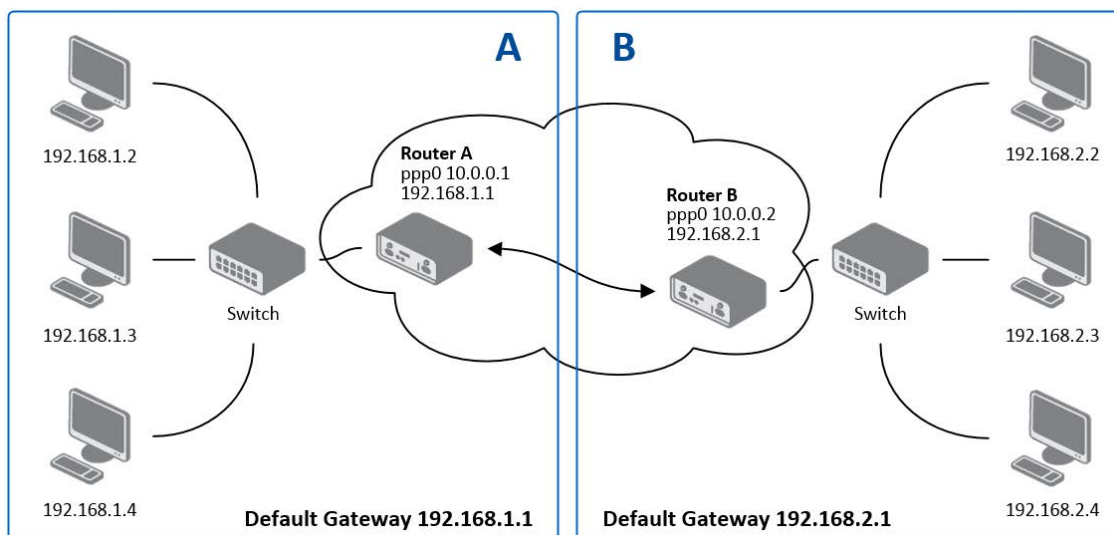


Figure 55: Topology of example L2TP tunnel configuration

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 47: Example L2TP tunnel configuration

8.18 DynDNS client configuration

DynDNS client Configuration can be called up by option *DynDNS* item in the menu. In the window can be defined a third order domain registered on server www.dyndns.org.

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 48: DynDNS configuration

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

Figure 56: Example of DynDNS configuration

8.19 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 49: 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:

Figure 57: Example of NTP configuration

8.20 SNMP configuration

It is possible to configure SNMP agent sending information about the router by invoking the *SNMP configuration* page. SNMP (Simple Network Management Protocol) provides status information about network elements such as routers or end computers.

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 50: SNMP agent configuration

Enabling SNMP is performed using the *Enable SNMP agent* item. It is also necessary to define a password for access to the SNMP agent (*Community*). Standardly is used *public* that is predefined.

Example of SNMP settings and readout:

SNMP Configuration	
<input checked="" type="checkbox"/> Enable SNMP agent	
Community	<input type="text" value="public"/>
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 type="checkbox"/> Enable XC-CNT extension	
<input 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 58: Example of SNMP configuration

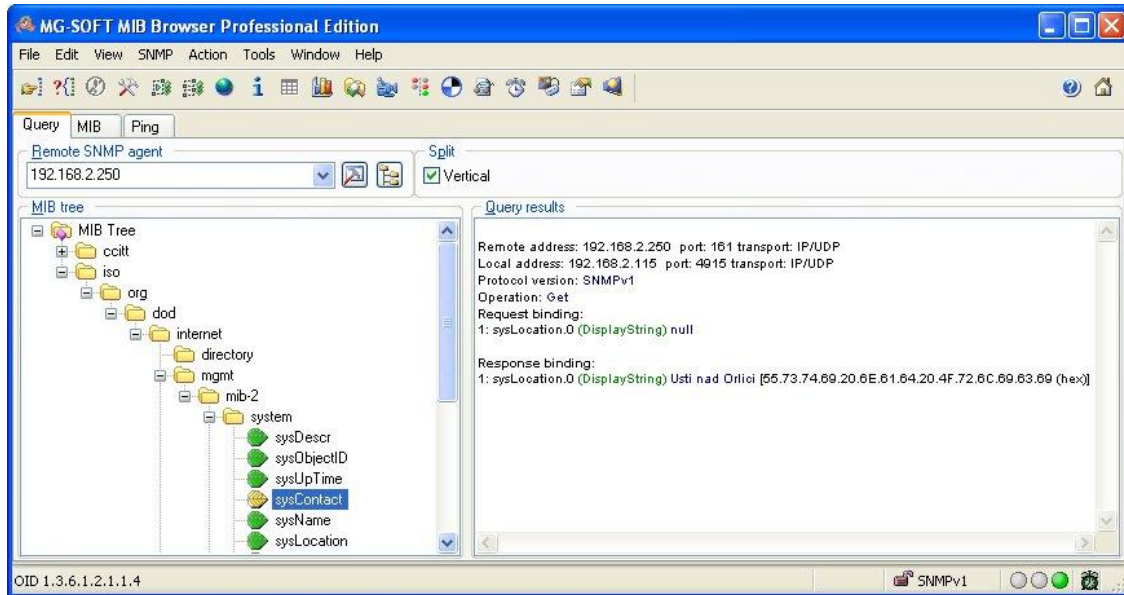


Figure 59: Example of the MIB browser

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

8.21 SMTP configuration

It's possible to configure SMTP (Simple Mail Transfer Protocol) client by invoking the *SMTP* page. This client is used to set sending emails.

Item	Description
SMTP Server Address	IP or domain address of the mail server.
Username	Name to email account.
Password	Password to email account.
Own Email Address	Address of the sender.

Table 51: SMTP client configuration



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

Example settings SMTP client:

SMTP Configuration	
SMTP Server Address	<input type="text" value="smtp.domain.com"/>
Username	<input type="text" value="name@domain.com"/>
Password	<input type="text" value="pass"/>
Own Email Address	<input type="text" value="name@domain.com"/>
<input type="button" value="Apply"/>	

Figure 60: SMTP configuration

E-mail can be send from the Startup script. This command is used to email with following parameters.

- -t receiver Email address
- -s subject
- -m message
- -a appendix
- -r number of attempts to send email (default set 2 attempts)



Commands and parameters can be entered only in lowercase.

Example to send email:

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

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

8.22 SMS configuration

SMS Configuration can be called up by option *SMS* item in the menu. SMS configuration defines the options for sending SMS messages from the router at different defined events and states of the router. In the first part of window it configuration send SMS.

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 expansion port (BIN1 – BIN4) is active	Automatic sending SMS message after binary input on expansion port (BIN1 – BIN4) is active. Text of message is intended parameter BIN1 – BIN4.
Add timestamp to SMS	Adds time stamp to sent SMS messages. This stamp has a fixed format YYYY-MM-DD hh:mm:ss.
Phone Number 1	Telephone numbers for sending automatically generated SMS.
Phone Number 2	Telephone numbers for sending automatically generated SMS.
Phone Number 3	Telephone numbers for sending automatically generated SMS.
Unit ID	The name of the router that will be sent in an SMS.

Table 52: Send SMS configuration

In the second part of the window it is possible to set function *Enable remote control via SMS*. After this it is possible to establish and close connection by SMS message.

Item	Description
Phone Number 1, Phone Number 2, 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 53: 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 of 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 of sign "" it is possible control the router with the help of an SMS sent from every numbers.



Control SMS message doesn't change the router 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 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 54: Control SMS

By 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 by the help of a standard AT commands.

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

Table 55: Send SMS on ethernet PORT1 configuration

8.22.1 Send 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 only lists the commands that are supported by Advantech B+B Smart-Worx routers. For other AT commands is always sent *OK* response. There is no support for treatment of complex AT commands, so in such a case router sends *ERROR* response.

AT Command	Description
AT+CGMI	Returns the manufacturer specific identity

Continued on next page

Continued from previous page

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



A detailed description and examples of these AT commands can be found in the application note *AT commands* (see [5]).

Example of sending SMS:

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

Configuration of sending this SMS is following:

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 expansion port (BIN1-BIN4) is active
<input checked="" type="checkbox"/>	Add timestamp to SMS
Phone Number 1	<input type="text" value="723123456"/>
Phone Number 2	<input type="text" value="756858635"/>
Phone Number 3	<input type="text" value="603854758"/>
Unit ID *	<input type="text" value="Router"/>
BIN0 - SMS *	<input type="text" value="BIN0"/>
BIN1 - SMS *	<input type="text" value="BIN1"/>
BIN2 - SMS *	<input type="text" value="BIN2"/>
BIN3 - SMS *	<input type="text" value="BIN3"/>
BIN4 - SMS *	<input type="text" value="BIN4"/>
<input checked="" type="checkbox"/>	Enable remote control via SMS
Phone Number 1	<input type="text"/>
Phone Number 2	<input type="text"/>
Phone Number 3	<input type="text"/>
<input type="checkbox"/>	Enable AT-SMS protocol on expansion port
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 61: Example of SMS configuration 1

Example of the router configuration for controlling via SMS from every 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 expansion port (BIN1-BIN4) is active
<input type="checkbox"/>	Add timestamp to SMS
Phone Number 1	<input type="text"/>
Phone Number 2	<input type="text"/>
Phone Number 3	<input type="text"/>
Unit ID *	<input type="text"/>
BIN0 - SMS *	<input type="text"/>
BIN1 - SMS *	<input type="text"/>
BIN2 - SMS *	<input type="text"/>
BIN3 - SMS *	<input type="text"/>
BIN4 - SMS *	<input type="text"/>
<input checked="" type="checkbox"/>	Enable remote control via SMS
Phone Number 1	<input type="text" value="*"/>
Phone Number 2	<input type="text"/>
Phone Number 3	<input type="text"/>
<input type="checkbox"/>	Enable AT-SMS protocol on expansion port
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 62: Example of SMS configuration 2

Example of the router configuration for controlling via SMS from 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 expansion port (BIN1-BIN4) is active
<input type="checkbox"/>	Add timestamp to SMS
Phone Number 1	<input type="text"/>
Phone Number 2	<input type="text"/>
Phone Number 3	<input type="text"/>
Unit ID *	<input type="text"/>
BIN0 - SMS *	<input type="text"/>
BIN1 - SMS *	<input type="text"/>
BIN2 - SMS *	<input type="text"/>
BIN3 - SMS *	<input type="text"/>
BIN4 - SMS *	<input type="text"/>
<input checked="" type="checkbox"/>	Enable remote control via SMS
Phone Number 1	<input type="text" value="728123456"/>
Phone Number 2	<input type="text" value="766254864"/>
Phone Number 3	<input type="text"/>
<input type="checkbox"/>	Enable AT-SMS protocol on expansion port
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 63: Example of SMS configuration 3

8.23 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.

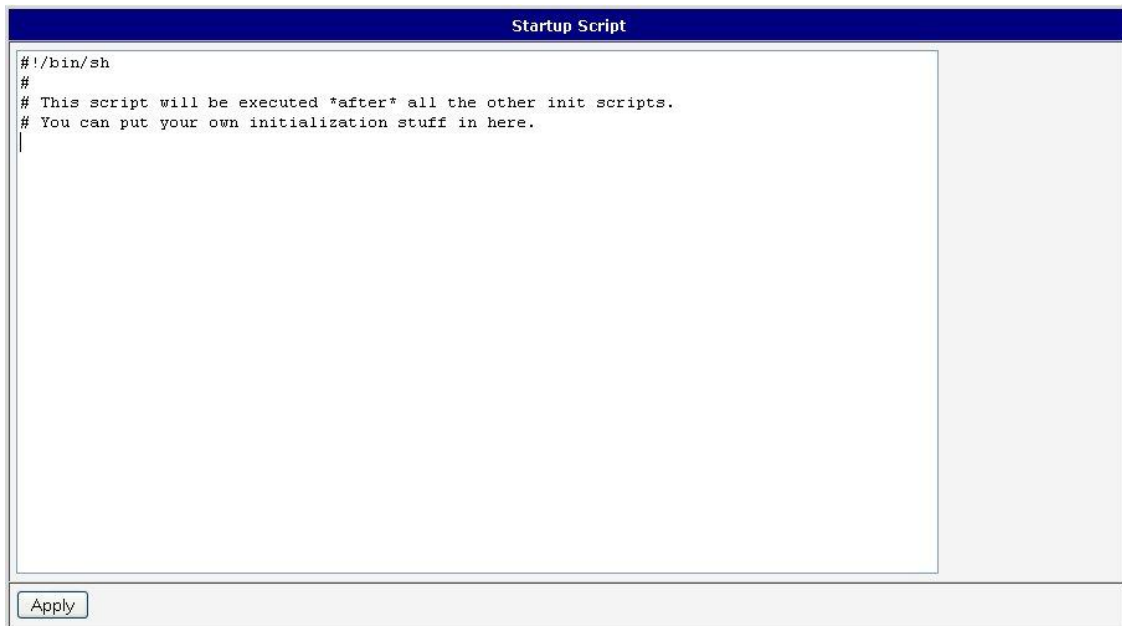


Figure 64: Startup script



Changes take effect after shut down and witch on router by the help of button Reboot in web administration or by SMS message.

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.

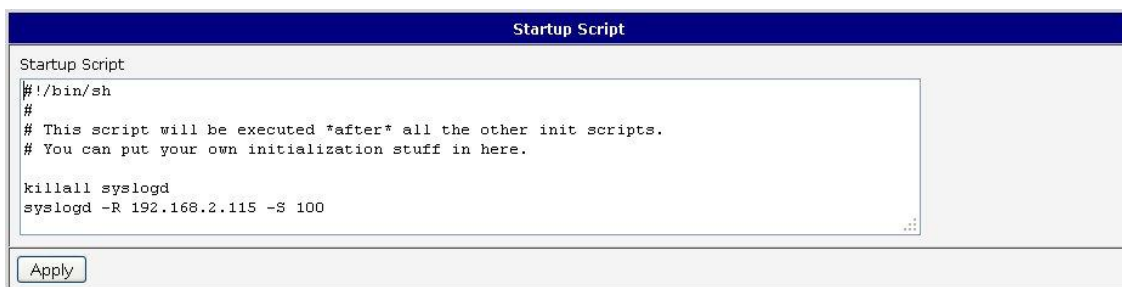
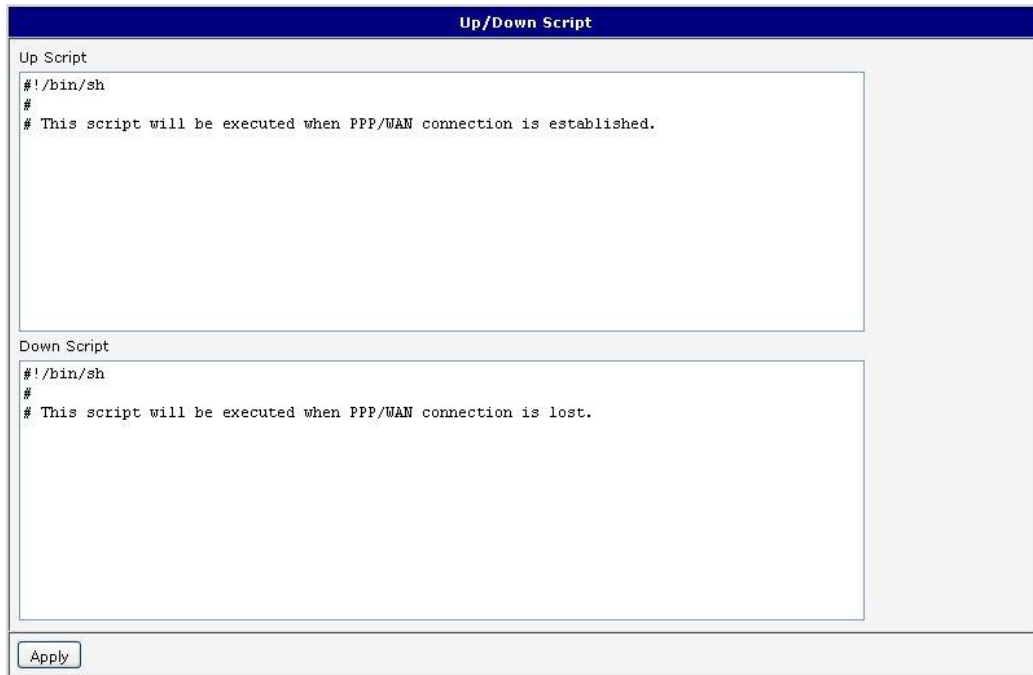


Figure 65: Example of Startup script

8.24 Up/Down Script

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

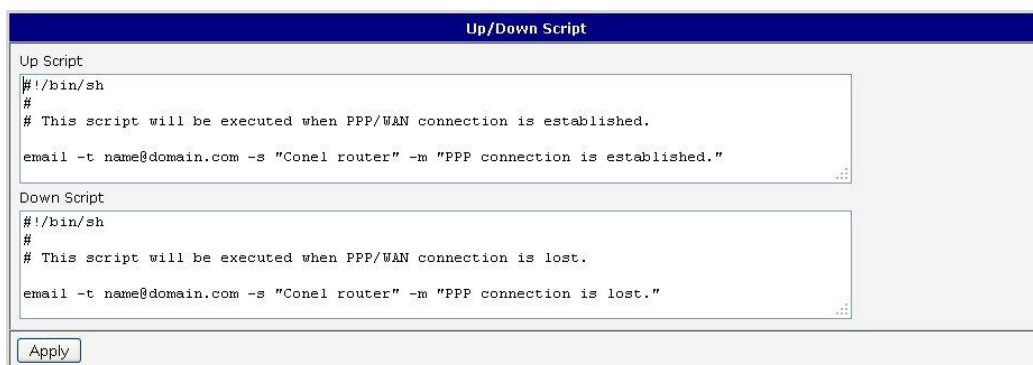
The changes in settings will apply after pressing the *Apply* button.



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 66: 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 email commands. 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 67: Example of Up/Down script

8.25 Automatic update configuration

In the window *Automatic update* it is possible to set automatic configuration update. This choice enables that the router automatically downloads the configuration and the newest firmware from the server itself. The configuration and firmware are stores on the server. To prevent possible manipulation of the update, downloaded file (tar.gz format) is controlled. At first, format of the downloaded file is checked. Then there is controlled type of architecture and each file in the archive (tar.gz file).

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

Item	Description
Base URL	By parameter Base URL it is possible to enter base part of the domain or IP address, from which the configuration file will be downloaded.
Unit ID	Name of configuration. If the Unit ID is not filled, then as the file name used the MAC address of the router. (The delimiter is a colon is used instead of a dot.)
Update Hour	Use this item to set the hour (range 1-24) in which 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. In the event of a different configuration at the specified URL router downloads this configuration and restarts itself.

Table 57: Automatic update configuration



The *configuration file* name is from parameter *Base URL*, hardware MAC address of ETH0 interface and *cfg* extension. Hardware MAC address and *cfg* extension 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 is from parameter *Base URL*, type of router and bin extension.



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

The following examples find if there is a new firmware or configuration each day at 1:00 in the morning.

- Firmware: <http://router.cz/er75s.bin>
- Configuration file: <http://router.cz/temelin.cfg>

The screenshot shows the 'Automatic Update' configuration page. It has a dark blue header with the title 'Automatic Update'. Below the header, there are two checked checkboxes: 'Enable automatic update of configuration' and 'Enable automatic update of firmware'. There are three input fields: 'Base URL' with the value 'router.cz', 'Unit ID *' with the value 'temelin', and 'Update Hour *' with the value '1'. Below these fields is a note '* can be blank'. At the bottom left is an 'Apply' button.

Figure 68: Example of automatic update 1

The following example find if there is a new firmware or configuration each day at 1:00 in the morning. There was used ER75s router with MAC address 00:11:22:33:44:55.

- Firmware: <http://router.cz/er75s.bin>
- Configuration file: <http://router.cz/00.11.22.33.44.55.cfg>

The screenshot shows the 'Automatic Update' configuration page. It has a dark blue header with the title 'Automatic Update'. Below the header, there are two checked checkboxes: 'Enable automatic update of configuration' and 'Enable automatic update of firmware'. There are three input fields: 'Base URL' with the value 'router.cz', 'Unit ID *' which is empty, and 'Update Hour *' with the value '1'. Below these fields is a note '* can be blank'. At the bottom left is an 'Apply' button.

Figure 69: Example of automatic update 2

8.26 Change profile

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

Example of usage profiles: Profiles can be used for example to switch between different modes of operation of the router (router has compiled a connection, the router has not compiled a connection and the router creates a tunnel to the service center). Change the profile can then be done using a binary input, SMS or Web interface of the router.

Figure 70: Change profile

8.27 Change password

To open the dialog box for changing the access password select the *Change Password* menu item. The new password will be saved after pressing the *Apply* button.

In basic settings of the router the password is set on default form *root*. For higher security of your network we recommend changing this password.

Figure 71: Change password

8.28 Set real time clock

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

Set Real Time Clock	
Date	<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 72: Set real time clock

8.29 Set SMS service center address

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

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

Figure 73: Set SMS service center address

8.30 Unlock SIM card

Possibility to unlock SIM PIN is under *Unlock SIM Card* item. If the inserted SIM card is secured by a PIN number, enter the PIN to field *SIM PIN* and push-button *Apply*. SIM card is blocked after three failed attempts to enter the PIN code.



Unlock SIM Card	
SIM PIN	<input type="text"/>
<input type="button" value="Apply"/>	

Figure 74: Unlock SIM card

8.31 Send SMS

Sending SMS messages is possible in menu *Send SMS*. The SMS message will be sent after entering the *Phone number* and text SMS (*Message*) and by pushing button *Send*.



Figure 75: Send SMS

SMS message sending via HTTP request is in the form:

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

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. In the example is used for root:root.

8.32 Backup configuration

The router configuration is possible to save by help of the *Backup Configuration* menu item. After clicking on this menu it is possible to check a destination directory, where it will save the router configuration.

8.33 Restore configuration

In case it is needed to restore the router configuration, it is possible in *Restore Configuration* menu item to check configuration by help *Browse* button.



Figure 76: Restore configuration

8.34 Update firmware

To view the information about the firmware version and instructions for its update select the *Update Firmware* menu item. New firmware is selected via Browse button and update the following pressing the Update button.

Update Firmware	
Firmware Version : 2.0.7 (2010-12-16)	
New Firmware	<input type="text"/> <input type="button" value="Browse"/>
<input type="button" value="Update"/>	

Figure 77: Update firmware

After successful firmware updating the following statement is listed:

```

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

Reboot in progress
Continue here after reboot.
    
```

There is information about updating of the FLASH memory.



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

8.35 Reboot

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

Reboot	
The reboot process will take about 15 seconds to complete.	
<input type="button" value="Reboot"/>	

Figure 78: Reboot

9. Configuration setting over Telnet



Attention! If the SIM card isn't inserted in the router, it is impossible for the router to operate. The Included SIM card must be activated for GPRS transmissions.

Monitoring of status, configuration and administration of the router can be performed by means of the Telnet interface. After IP address entry to the Telnet it is possible to configure the router by the help of commands. The default IP address of the modem is 192.168.1.1. Configuration may be performed only by the user "root" with initial password "root".

For Telnet exists the following commands:

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

Continued on next page

Continued from previous page

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

Table 58: Telnet commands

10. Recommended literature

- [1] Advantech B+B SmartWorx: **Start guide,**
- [2] Advantech B+B SmartWorx: **Application note – Programmer guide,**
- [3] Advantech B+B SmartWorx: **Application note – OpenVPN tunnel,**
- [4] Advantech B+B SmartWorx: **Application note – IPsec tunnel,**
- [5] Advantech B+B SmartWorx: **Application note – AT commands.**


11. Possible problems




Some network cards are able to be set in situation, when it is not possible to connect the router. It is possible to solve this problem in the following steps:

- hand by selection communication rates 10 MB/s in property network cards,
- connect router over switch,
- start computer only after finalizing the start of the router.


12. FAQ

 I can't get from internet on equipment, which is connected to router and I have NAT enabled.

- *The device's gateway has to be configured as the router.*

 Router resets itself, connection on Ethernet fails.


- *It is necessary to use an antenna, which will be situated far from power supply.*

 I don't get on web server at NAT.


- *The remote http access of the router has to be disabled, default server address has to be your web server and the gateway of the web server has to be the IP of router.*

 GPRS connection fails.


- *Check signal power. If signal power is weak, you will have to use a better antenna. If the environmental cells have a similar signal it will be necessary to use a directive antenna. Signal levels have to be in the range -50 dBm and -90 dBm.*
- *It is necessary to set ping, which will check the connection and, in the case of fail ping, restart connection.*

 GPRS connection won't be established.

- *Recheck GPRS settings – APN, name, password and IP address.*
- *Try to enter PIN – verification if the SIM card hasn't set PIN code.*
- *In private APN it is appropriate to switch the DNS server send off.*
- *Switch log system on and observe where the error turns up.*

 Connection fails on Ethernet or connection isn't establishing.

- *On ethernet interface of the router it is possible to switch auto negotiation off and set a rate and duplex by hand.*


 How is it possible to enter AT commands?

- *It is necessary to use a USB connection, but it is impossible to connect to GPRS from the router together.*

 DynDNS not function.

- *In private APN not functional.*
- *If the same IP address is recorded in your canonic name as dynamically assign address, it means that the operator is using NAT or firewall.*


- *NAT is possible to verify by the help of the ping on address of your server with static IP address and by the help of the router address verify and address in ping.*
- *Firewall is possible to verify, for example by remote access on web interface.*
- *The operator doesn't give out address DNS servers and without DNS server's it is impossible to connect to server dyndns.org. In log system will be this message:*
 - *DynDNS daemon started*
 - *Error resolving hostname: no such file or directory*
 - *Connect to DynDNS server failed*

 IPsec tunnel is establishing but communication doesn't function.


- *Probably it is badly set up route conditionals of connected equipment or it is bad set up GW.*

 FTP doesn't function.


- *Router doesn't support the active FTP mode, supports the passive mode only.*

 L2TP or IPsec isn't establishing.

- *Verify the reason in the log system.*

 How do I get to know that EDGE is functional?

- *If download is higher than 85.6 kb/s then EDGE is functioning.*

 I switched the router to offline mode by the SMS message, but the router is in online mode after restart.

- *Control SMS messages don't change the router configuration. For example, if the router is switched to offline mode by SMS message the router will be in this mode up to next restart. This behaviour is the same for next all control SMS messages.*

13. Customers Support

13.1 Customer Support for NAM

E-mail: support@advantech-bb.com
 Web: www.advantech-bb.com

13.2 Customer Support for Europe

E-mail: iiotcustomerservice@advantech.eu
 Web: www.advantech-bb.com

13.3 Customer Support for Asia

E-mail: icg.support@advantech.com.tw
 Web: www.advantech.com



Upkeep – Advices:

- The SIM-card must be handled carefully as with a credit card. Don't bend, don't scratch on this and do not expose to static electricity.
- During cleaning of the router do not use aggressive chemicals, solvents and abrasive cleaners!



Hereby, Advantech B+B SmartWorx s.r.o. company declares that the radio equipment narrated in this user's guide is in compliance with EU Directive **2014/53/EU**.

The full text of the EU Declaration of Conformity is available at the following internet address:
www.advantech-bb.cz/eudoc