



UMTS/HSDPA router UR5

USER'S GUIDE



ISO 9001:2001



Contents

1. Safety instruction	4
2. Description of the UR5 router	5
2.1. Introduction	5
2.2. UMTS technology	5
2.3. HSDPA technology (High Speed Download Packet Access)	6
2.4. Delivery Identification	6
2.5. Antenna Connection	7
2.6. SIM Card Reader	8
2.7. Power Supply	8
2.8. Technical parameters	9
2.9. Description of the individual components of the UR5	10
2.9.1. UMTS module	10
2.9.2. Control microcomputer	10
2.10. User interfaces (Connectors)	11
2.10.1. Connection of the PWR Supply Connector	12
2.10.2. Connection of the Port1 Connector – RS232	12
2.10.3. Connection of the Port1 Connector – RS485G	13
2.10.4. Connection of the Port1 Connector – MBUS	14
2.10.5. Connection of the Port1 Connector – CNT	15
2.10.6. Connection of the ETH Connector	16
2.10.7. Connection of the Connector USB	16
2.11. Technical specification of optional PORT1	17
2.12. Modem status indication	19
2.13. Putting into operation	19
2.14. Mechanical external dimensions and mounting recommendations	19
3. Expansion port mounting	22
4. Change of the SIM cards	24
5. Configuration setting over web browser	27
5.1. Network Status	27
5.2. DHCP Status	29
5.3. IPsec status	29
5.4. UMTS/GPRS Status	29
5.5. DynDNS status	30
5.6. System Log	30
5.7. Network Configuration	30
5.8. UMTS/GPRS Configuration	31
5.9. Firewall Configuration	33
5.10. NAT Configuration	33
5.11. IPSec Tunnel Configuration	36
5.12. GRE Tunnels Configuration	37
5.13. L2TP Configuration	39
5.14. DynDNS Client Configuration	40
5.15. NTP Client Configuration	41
5.16. SNMP Configuration	41
5.17. SMS Configuration	43
5.18. External Port Configuration	46
5.19. USB Port Configuration	48
5.20. Startup Script	49

5.21.	Change password	49
5.22.	Setting inner o'clock	50
5.23.	Unlock SIM card	50
5.24.	Backup Configuration	50
5.25.	Restore Configuration	50
5.26.	Update firmware	50
5.27.	Reboot	51
5.28.	Default settings	52
5.28.1.	LAN Configuration	52
5.28.2.	UMTS/GPRS Configuration	52
5.28.3.	Firewall Configuration	52
5.28.4.	NAT Configuration	53
5.28.5.	IPsec Tunnel Configuration	53
5.28.6.	GRE Tunnels Configuration	54
5.28.7.	L2TP Tunnel Configuration	54
5.28.8.	DynDNS Configuration	55
5.28.9.	NTP Configuration	55
5.28.10.	SNMP Configuration	55
5.28.11.	SMS Configuration	56
5.28.12.	External Port Configuration	56
5.28.13.	USB Port Configuration	57
5.28.14.	Startup script	57
6.	Configuration setting over Telnet	58
7.	Possible problems	59
8.	Reference	59
9.	FAQ	59
10.	Customers support	60
11.	Guarantee Claim Guidelines	61
12.	Guarantee certificate	64

Symbols used



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



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



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

GPL licence

Source codes under GPL licence are available free of charge by sending email on info@conel.cz.



1. Safety instruction

Please, observe the following instructions:

- The UR5 communication module must be used in compliance with all applicable international and national laws and in compliance with any special restrictions regulating the utilization of the communication module in prescribed applications and environments.
- To prevent possible injury to health and damage to appliances and to ensure that all the relevant provisions have been complied with, use only the original accessories. Unauthorised modifications or utilization of accessories that have not been approved may result in damage to the communication module and in a breach of applicable regulations. Unauthorized modifications or utilization of accessories that have not been approved may result in the termination of the validity of the guarantee.
- The communication module UR5 must not be opened. Only the replacement of the SIM card is permitted.



- **Caution!** The SIM card could be swallowed by small children.
- Voltage at the feed connector of the communication module must not be exceeded.
- Do not expose the communication module to extreme ambient conditions. Protect the communication module against dust, moisture and high temperature.
- It is recommended that the communication module should not be used at petrol stations. We remind the users of the duty to observe the restrictions concerning the utilization of radio devices at petrol stations, in chemical plants, or in the course of blasting works in which explosives are used.
- Switch off the communication module when travelling by airplane. Utilization of the communication module in a airplane may endanger the operation of the airplane 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, or, it may result in legal sanctions; it may also result in both eventualities.
- When using the communication module in the close proximity of personal medical devices, such as cardiac pacemakers or hearing aids, you must proceed with heightened caution.
- If it is in the proximity of TV sets, radio receivers and personal computers, the telephone may cause interference.
- It is recommended that you should create an appropriate copy or backup of all the important settings that are stored in the memory of the device.

2. Description of the UR5 router

2.1. Introduction

The UR5 is a compact electronic device based on the HC15 module of SIEMENS which enables data transfers using HSDPA/UMTS/EDGE/GPRS GSM, GPRS and UMTS technologies.

Primarily, the UR5 router expands the capabilities of the HC15 module by the option of connecting more PC's by means of the built-in Ethernet interface. In addition, the firmware of the UR5 router provides automatic establishment and maintenance of HSDPA/UMTS/EDGE/GPRS PPP connection. By means of the integration of a DHCP server it provides the user with simple installation and Internet access.

In addition, the UR5 router is equipped with a USB 2.0 Host interface which is designed only for connection to a USB device.

By customer request it is possible to equip the UR5 router with the PORT1 module and extend the function of the UR5 UMTS router.



Examples of Possible Applications

- mobile office
- fleet management
- security system
- telematic
- telemetric
- remote monitoring
- vending and dispatcher machines

2.2. UMTS technology

For radio terrestrial part UMTS (Universal Mobile Telecommunication System), which is marked as UTRA (UMTS Terrestrial Radio Access), is warranted 155 MHz band in frequency band about the 2 GHz. It is bands 1900–1980 MHz, 2010–2025 MHz and 2110–2170 MHz.

The UMTS system is based on code solution of carried channels – use the access method WCDMA (Wideband Code Division Multiple Access). WCDMA exploit direct spread spectrum DS (Direct Spread). For transmission the UMTS network exploits two duplex techniques – transmission modes FDD (Frequency Division Duplex), which is based on separate frequency channels (i.e. uplink and downlink uses different channels) and TDD (Time Division Duplex), which is based on separate time (i.e. uplink and downlink uses one channel, in which both direction are changes in time).

UMTS network consists of three basic entities:

- Basic network CN (Core Network) – own core of network UMTS,
- network UTRAN (UMTS Terrestrial Radio Access Network) – the radio access network,
- users part UE (User Equipment) – entity, which allows the user to access the UMTS network.

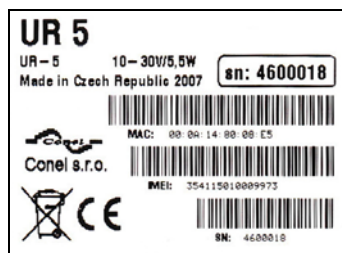
2.3. HSDPA technology (High Speed Download Packet Access)

HSDPA is an improved and extended version of the UMTS-TDD. HSDPA is available for both UMTS FDD and for UMTS TDD. HSDPA raises essential bit rate for downlink. It is attained on the programmer level. It doubles capacity on BTS stations, the basic radio stations that allows the process of data and signals from more users at one time. HSDPA is based on a few innovations of network architecture; because of wheeze it gets lower latency, faster reaction on channel change quality and processing of H-ARQ (Hybrid automatic repeat request) on transmission repeat. Transport channel for HSDPA effectively uses available frequencies, on which transmits data packets together. Afterwards these packets help define the algorithms within individual users.

2.4. Delivery Identification

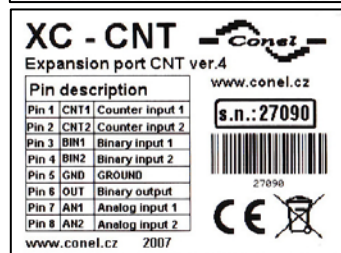
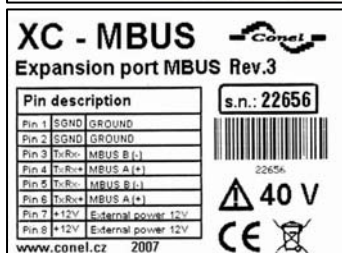
Specimen Label:

Trade name	Type name
UR 5	UR-5



Example of expansion port PORT1:

Trade name	Type name	Power supply
Expansion port RS232	XC-232	Internal power supply
Expansion port RS485	XC-485G	Internal/external power supply
Expansion port MBUS	XC-MBUS	External power supply
Expansion port CNT	XC-CNT	Internal power supply





Basic delivered set of UR5 includes:

- UMTS router UR5
- power supply
- crossover UTP cable
- external antenna
- plastic clips for the DIN rail with fixing screws
- installation CD containing instructions



In addition to the basics it is possible to deliver:

- PORT1 module
- adapter for use of a second SIM card



Router UR5 standard designed for

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

2.5. Antenna Connection

The antenna is connected to the UR5 using an the FME connector on the back panel.

External antennas:



2.6. SIM Card Reader

The SIM card reader for 3 V and 1.8 V SIM cards is located on the front panel of the modem, possibility inside the modem in case of adapter for the second SIM card. To initiate the modem 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 (Access Point Name).

2.7. Power Supply

The UR5 requires +10 V DC to +30 V DC supply. Protection against reversed polarity without signaling is built into the modem.

The power consumption during receiving is 1W. The peak power consumption during data sending is 3.5W. For correct operation it is necessary that the power source is able to supply a peak current of 500mA.

2.8. Technical parameters

HSDPA/UMTS/EDGE/GPRS module		SIEMENS HC15
Complies with standards		EN 301 511, v9.0.2, EN 301 908-1&2, v2.2.1, ETSI EN 301 489-1 V1.6.1, EN 60950-1:06 ed.2
HSDPA parameters		3GPP rel. 5 standard bitrate 3.6 Mbps/384 kbps UE CAT. 1 to 6, 11, 12 Data compress 3GPP TS25.212
UMTS parameters		W-CDMA FDD standard PS bitrate – 384/384 kbps CS bitrate – 64/64 kbps
GPRS parameters		GPRS multislot class 10, CS 1 to 4 EGPRS multislot class 10, CS 1 to 4, MCS 1 to 9
Transmit power		Class 3 (+23dBm) for UMTS 2100MHz
Temperature range	Function Storage	-20 °C to +55 °C -40 °C to +85 °C
Supply voltage		10 to 30 V DC
Consumption	Reception GPRS UMTS/HSDPA	300 mW to 3,5 W (GPRS transmission) to 5,5 W (UMTS/HSDPA transmission)
Dimensions		30x90x102 mm (DIN 35mm)
Weight		150 g
Antenna connector		FME – 50 Ohm
User interface	ETH USB PORT1	Ethernet (10/100 Mbit/s) USB 2.0 type A host Optional RS232/RS485/MBUS or inputs/outputs (I/O)

2.9. Description of the individual components of the UR5

2.9.1. UMTS module

The Siemens HC15 module is used for HSDPA/UMTS/EDGE/GPRS UMTS network wireless communication. It is integrated in the printed circuit board. The slide-out SIM card reader is accessible from the front panel. The FME antenna connector is accessible from the back panel.

Module HC15

- Communicates in UMTS band 2100MHz
- CS bitrate – 64/64 kbps
- PS bitrate – 384/384 kbps
- Supports W-CDMA FDD (Wideband - Code Division Multiple Access Frequency Division Duplex) standard

2.9.2. Control microcomputer

The core of the UR5 router is a 32-bit microprocessor with 16 MB RAM, 4 MB FLASH EEPROM, serial interface RS-232 and an Ethernet interface 10/100 Mbit/s. The microcomputer is connected to the HC15 OEM module through the USB interface and controls the communication via HSDPA/UMTS/EDGE/GPRS. Towards to the user it is connected on the Ethernet interface.

The software is built on the uClinux operating system.

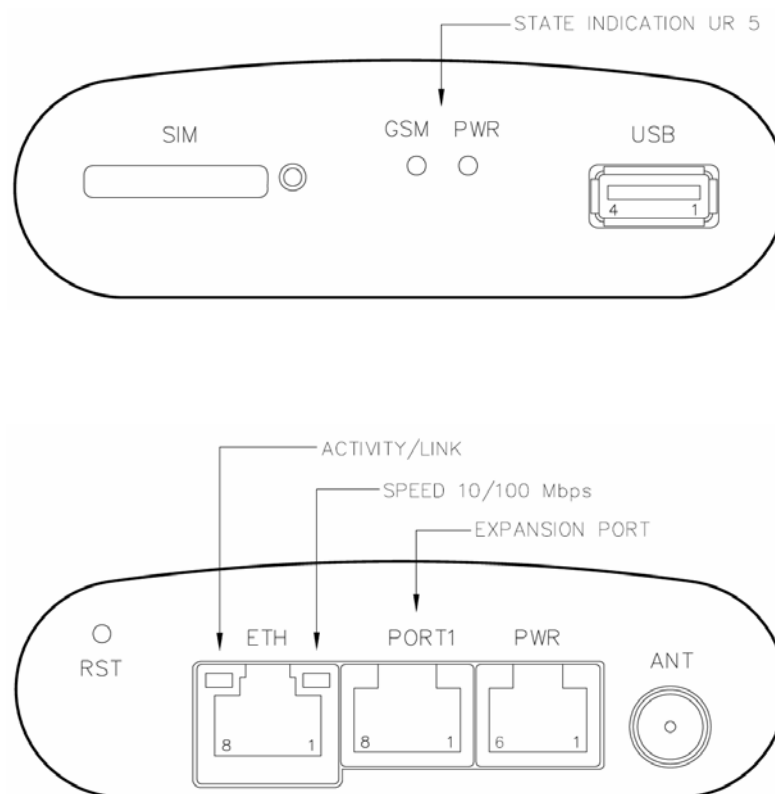
The router UR5 support services as like DHCP, NAT, GRE, IPsec tunnels, etc.

The modem settings are saved in the FLASH EEPROM memory. All modem configurations can be done through a web interface (HTTP), which is protected by security password.

2.10. User interfaces (Connectors)

On the back panel of UR5 the following connectors are located:

- one RJ12 connector (PWR) – for connection of the power supply adapter,
- one RJ45 connector (ETH) – for connection into the local equipment,
- one RJ45 connector (optional PORT1) – for connection of the local any arrangement,
- one FME or SMA connector (ANT) – for connection of the antenna,
- one USB-A Host connector (USB) – for connection of the devices to the router, USB supports equipments with PL-2303 and FTDI USB/RS232 converter.



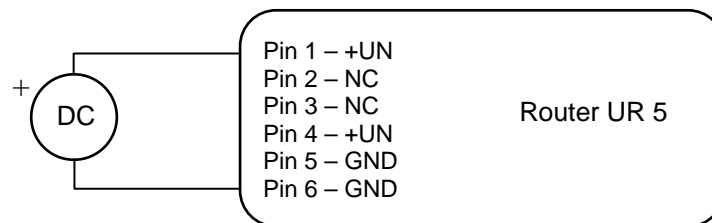
2.10.1. Connection of the PWR Supply Connector

Panel socket RJ12.

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



Circuit example:



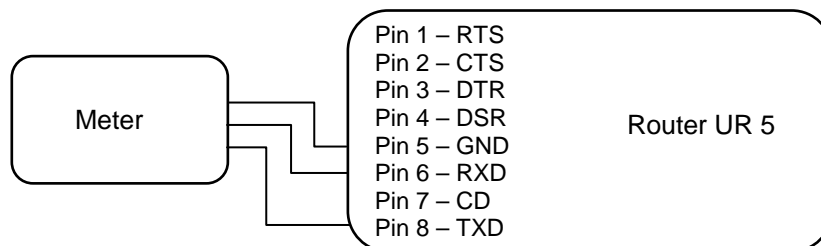
2.10.2. Connection of the Port1 Connector – RS232

Panel socket RJ45 (RS232 – DCE – Data Communication Equipment).

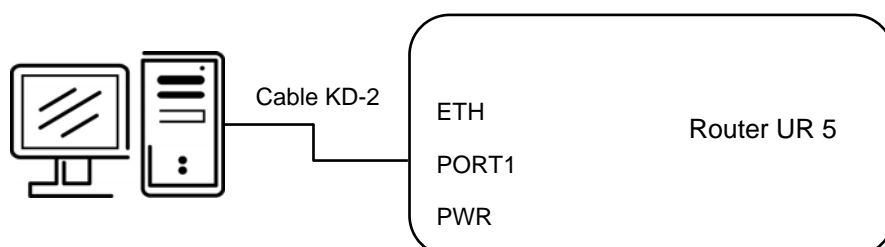
Pin number	Signal mark	Description	Data flow direction
1	RTS	Request To Send	Input
2	CTS	Clear To Send	Output
3	DTR	Data Terminal Ready	Input
4	DSR	Data Set Ready – connected to +4 V through 330 Ohm	Output
5	GND	GROUND – signal ground	
6	RXD	Receive Data	Output
7	CD	Carrier Detect	Output
8	TXD	Transmit Data	Input



Circuit example:

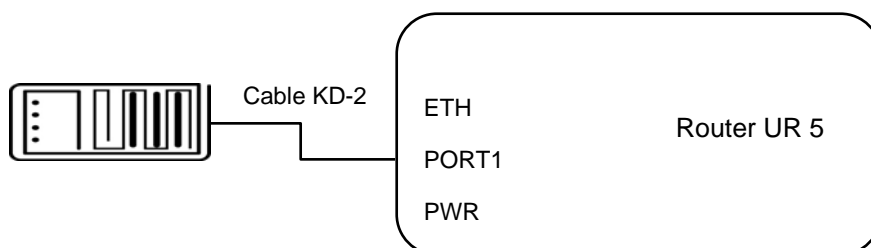


i The UR 5 connection to the PC:



- cable KD2 is connected to serial port PC (example COM1)

i The UR 5 connection to equipment with full-value RS232 interface:



2.10.3. Connection of the Port1 Connector – RS485G

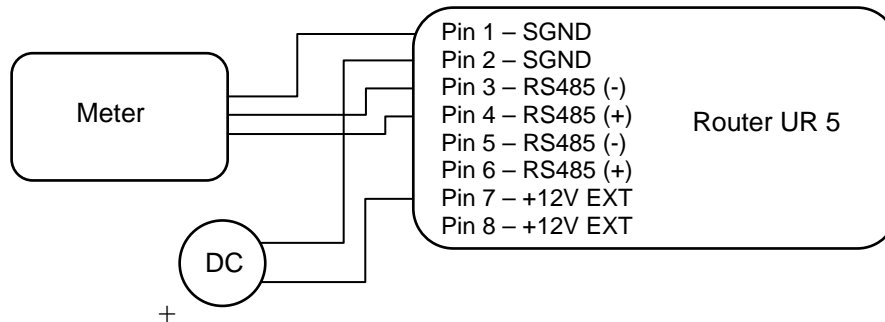
Panel socket RJ45.

Pin number	Signal mark	Description	Data flow direction
1	GND	Signal and supply ground	
2	GND	Signal and supply ground	
3	TxRx-	RS485 B (-)	Input/Output
4	TxRx+	RS485 A (+)	Input/Output
5	TxRx-	RS485 B (-)	Input/Output
6	TxRx+	RS485 A (+)	Input/Output
7	+12 V EXT	External power supply +10,8 ÷ +15,6V	
8	+12 V EXT	External power supply +10,8 ÷ +15,6V	

! **ATTENTION!** External power supply is for converter RS485G. Power supply is selected on module PORT2-RS485 by help of jumper, ref. 2.11.



Circuit example:



2.10.4. Connection of the Port1 Connector – MBUS

Panel socket RJ45.

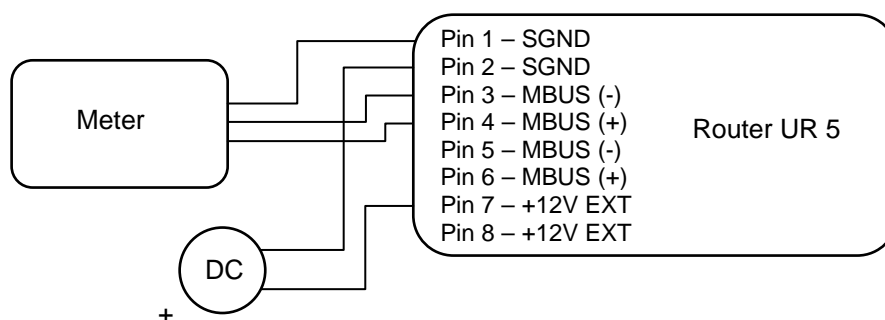
Pin number	Signal mark	Description	Data flow direction
1	GND	Signal and supply ground	
2	GND	Signal and supply ground	
3	TxRx-	MBUS B (-)	Input/Output
4	TxRx+	MBUS A (+)	Input/Output
5	TxRx-	MBUS B (-)	Input/Output
6	TxRx+	MBUS A (+)	Input/Output
7	+12 V EXT	External power supply +10,8 ÷ +15,6V	
8	+12 V EXT	External power supply +10,8 ÷ +15,6V	



ATTENTION! External power supply is for converter MBUS.



Circuit example:



2.10.5. Connection of the Port1 Connector – CNT

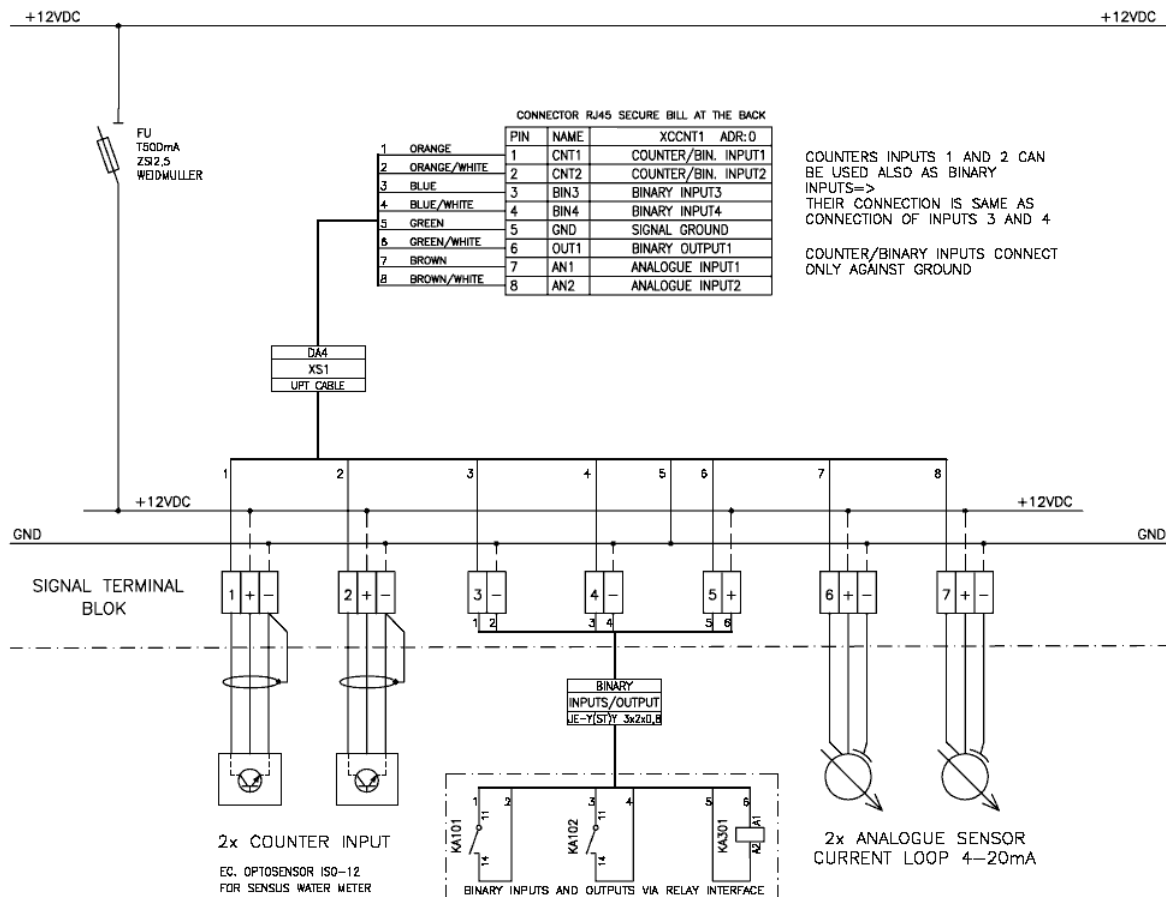
Panel socket RJ45.

Pin number	Signal mark	Description	Data flow direction
1	BIN1/CNT1	Binary input/counter input	Input
2	BIN2/CNT2	Binary input/counter input	Input
3	BIN3	Binary input	Input
4	BIN4	Binary input	Input
5	GND	Signal ground	
6	OUT1	Binary output (open collector)	Output
7	AN1	Analogy input	Input
8	AN2	Analogy input	Input

The user interface CNT is for monitoring and processing of analogy and binary signals and to control (settings) of binary signal. To disposition are 2 counter and 2 binary inputs or 4 binary inputs, 2 analogy inputs a 1 binary output. The settings of binaries and counters inputs by the help of firmware in which it is defined the singles inputs and output.



Typical connection of UR5 measuring circuits:



2.10.6. Connection of the ETH Connector

Panel socket RJ45.

Pin number	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	DNC	---	
5	DNC	---	
6	RXD-	Receive Data – negative pole	Input/Output
7	DNC	---	
8	DNC	---	



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

2.10.7. Connection of the Connector USB

Panel socket USB-A.

Pin number	Signal mark	Description	Data flow direction
1	VCC	Positive pole of 5V 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	

2.11. Technical specification of optional PORT1

- Expansion port RS232

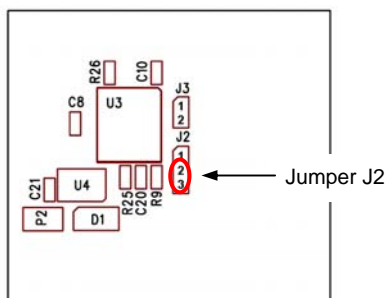
Name of product	Expansion port RS232	
Power supply	Internal
Environment	Operating temperature	-20 .. +55 C
	Storage temperature	-20 .. +85 C
Standards	Emission	EN 55022/B
	Immunity	ETS 300 342
	Safety	EN 60950
RS232 specifications (EN 1434)	Max. operating bus current	15 mA
	Max. bit rate	230400 bps
	Max. overvoltage	±30 V
	Max. total cable length (300Bd, 200nF/km)	20 m

- Expansion port RS485

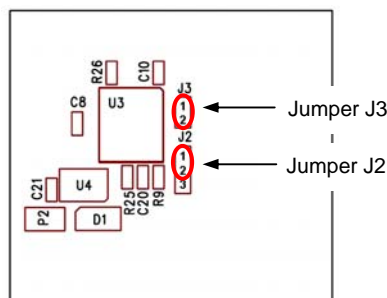
Name of product	Expansion port RS485	
Power supply	External	10,8 .. 15,6 V
	Internal
	Supply power	Max. 30 W
	Supply current	Max. 250 mA
Environment	Operating temperature	-20 .. +55 C
	Storage temperature	-20 .. +85 C
Standards	Emission	EN 55022/B
	Immunity	ETS 300 342
	Safety	EN 60950
RS485 specifications (EN 1434)	Max. devices (each 1,5 mA)	256
	Max. bit rate	38400 bps
	Overload detection	250 mA
	Short circuit strength	Permanent
	Max. total cable length (300Bd, 200nF/km)	1200 m



External or internal power supply of expansion port RS485 can be made by wiring jumpers J2 and J3 on this module. If external power supply of the module is required, jumper J2 must be connected to pins 2 - 3 and jumper J3 must be disconnection. Internal power supply is made by connecting jumper J2 to pins 1 - 2 and connecting jumper J3. Jumpers placement can be seen in the picture below (expansion port RS485 from TOP side). We recommend that internal power supply be only used in the event where it is not possible to ensure an external power supply. If internal power supply is chosen, converter RS485G is not galvanic separated.



The jumper circuitry for external supply



The jumper circuitry for internal supply

- Expansion port MBUS

Name of product	Expansion port MBUS	
Power supply	Voltage	10,8 .. 15,6 V
	Supply power	Max. 30 W
Environment	Operating temperature	-20 .. +55 C
	Storage temperature	-20 .. +85 C
Standards	Emission	EN 55022/B
	Immunity	ETS 300 342
	Safety	EN 60950
M-Bus specifications (EN 1434)	Max. devices (each 1,5 mA)	30
	Max. operating bus current	60 mA
	Overload detection	100 mA
	Short circuit strength	Permanent
	Bus voltage mark	36 .. 43 V
	Bus voltage space	24 .. 31 V
	Max. total cable length (300Bd, 200nF/km)	1000 m

- Expansion port CNT

Name of product	Expansion port CNT	
Power supply	Voltage	Internal 10 .. 30V
	Sleep	100 μ A (counter is functional)
	Operation	2 mA
Environment	Operating temperature	-20 .. +55 C
	Storage temperature	-20 .. +85 C
Standards	Emission	EN 55022/B
	Immunity	ETS 300 342
	Safety	EN 60950
	Isolation	EN 60747
Inputs/Outputs	2x counter	Max. 100 Hz, ratio max. 1:10
	2x analogy inputs	0 .. 20 mA, R_{in} 100 Ohms
	2x binary inputs	reed contact
	1x output (open collector)	100 mA
Others	Voltage resistance	Permanent
	Sleeping mode	Controlled

2.12. Modem status indication

On the front and back panel of the modem there are altogether four LED indicators, which inform on the modem status.

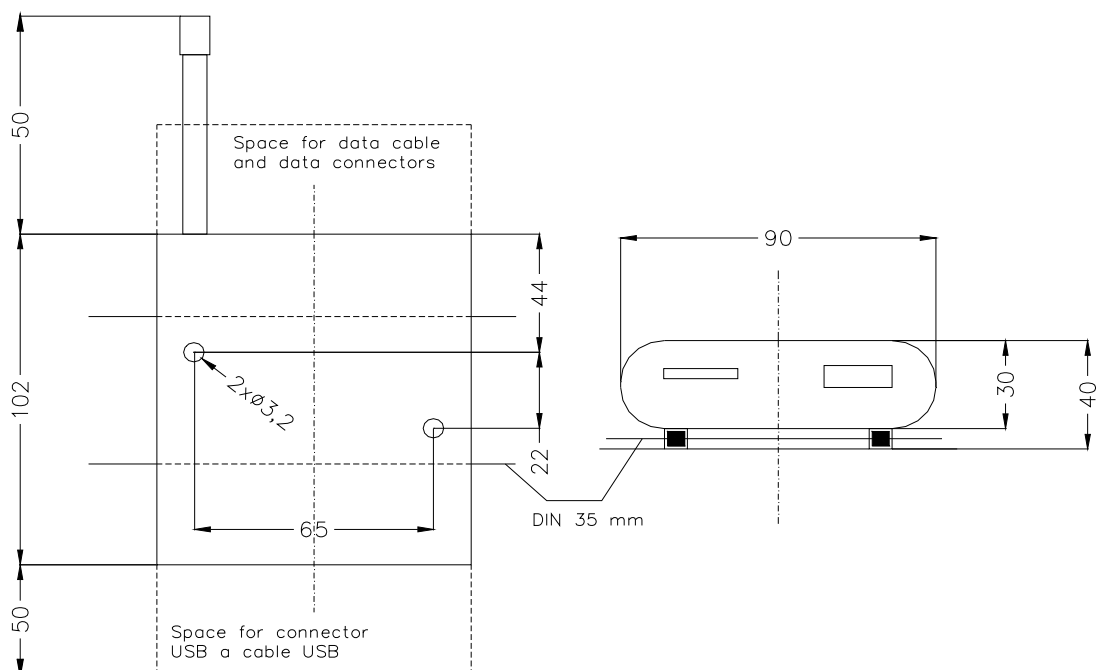
Panel	Color	Description	Description
Front	Green	PWR	Blinking 1:9 join connection Blinking 9:1 establishing of connection Permanently on starting of the UR5
Front	Red	GSM	Blinking communication in progress
Back	Green	–	On selected 100 Mbit/s Off selected 10 Mbit/s
Back	Green	–	On..... the network cable is connected Blinking data transmission Off the network cable is not connected

2.13. Putting into operation

Before putting the UR5 router into operation it is necessary to connect all components needed for the operation of your applications and the SIM card must be inserted (the modem is off).

The modem is put into operation by connection of the power supply to the modem. In the default setting the modem starts to login automatically to the preset APN. The behavior of the modem can be modified by means of the web interface which is described in the following chapter.

2.14. Mechanical external dimensions and mounting recommendations



For the majority of applications with a built-in modem in a switch board it is possible to recognize two sorts 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 modems to switch board, the following it is not need have no examination immunity or issues in connection with EMC according to EN 60439-1+A1.

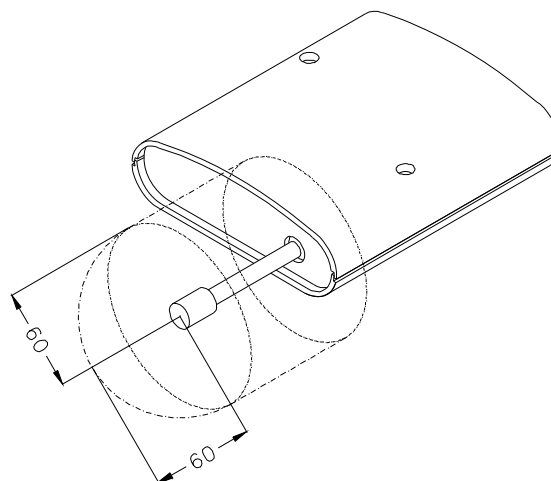
For compliance of EN 60439 - 1 + A1 specification it is necessary observe next assembly of the modem to the switch - board:



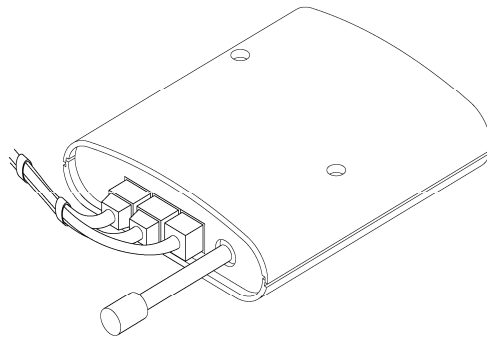
- round antenna we recommend to observe a distance of 6 cm from cables and metal surfaces on every side according to the next picture due to the elimination of interference, while using an external antenna except for the switch-board it is necessary to fit a lightening conductor,



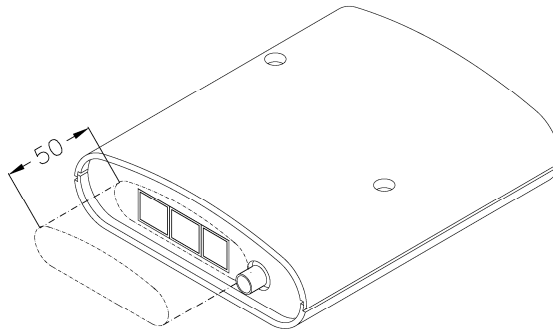
- before mounting a modem on sheet-steel we recommend using an external antenna,



- for single cables we recommend to bind the bunch according to the following picture, for this use we recommend:
 - length of the bunch (combination of power supply and data cables) can be maximum 1,5 m, if length of data cables exceeds 1,5 m or in the event of, the cable leads towards the switch - board, we recommend to use fit over - voltage protectors (surge suppressors),
 - with data cables they mustn't carry cables with reticular tension ~ 230 V/50 Hz,
 - all signals to sensors must be twisted pairs.



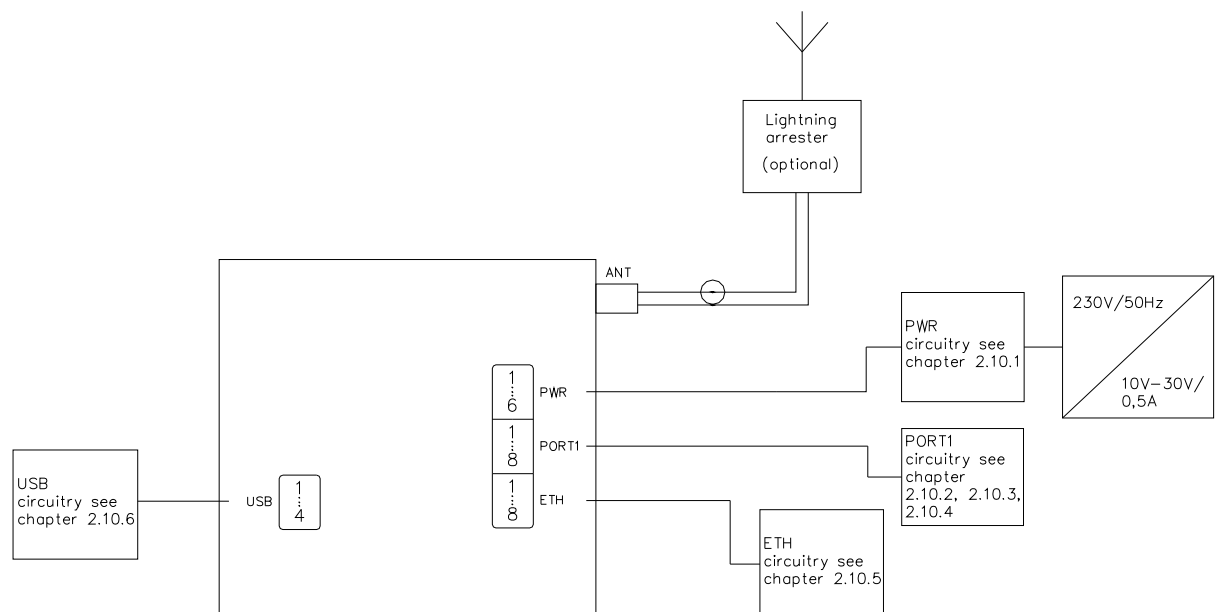
- sufficient space must be left before individual connectors for handling of cables,



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



- the circuit diagram of the modem is on the following pictures.

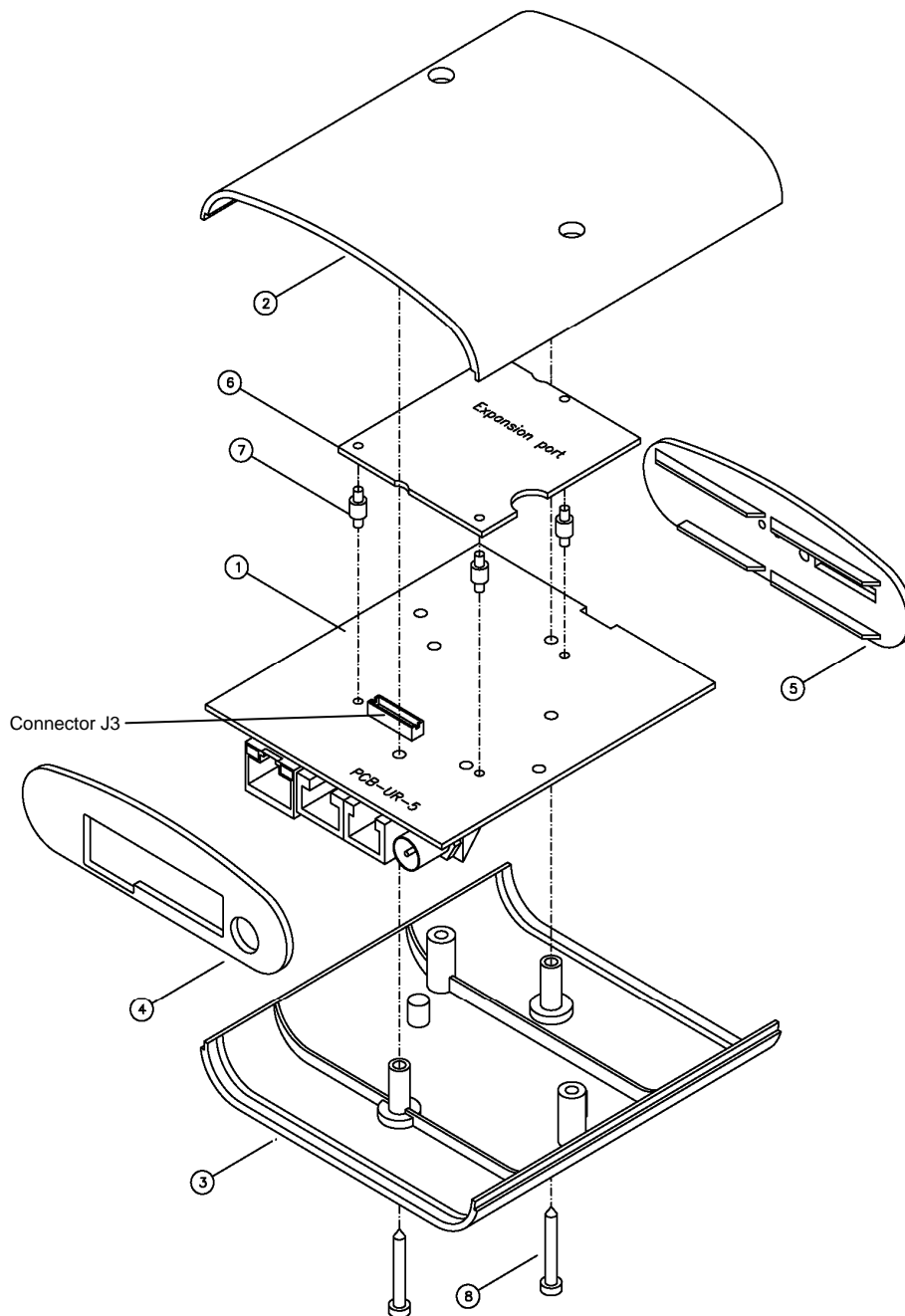


3. Expansion port mounting



Attention! Expansion port PORT1 include when the router UR 5 is switch off.

After unscrewed two screws (position 8) on box bottom part (position 3) and carried out box top part (position 2) the expansion port PORT1 (position 6) connect to connector J3 (see below) of the router B-UR-5 motherboard (position 1) from TOP side. Expansion port is mounted to motherboard by the help of three distant columns (position 7). After expansion port mounting the box is screwed by the help three screws (position 8).



Parts list and description

Part	Description	Number
1	UMTS router UR 5 motherboard	1
2	UR 5 box top part	1
3	UR 5 box bottom part	1
4	UR 5 rear head	1
5	UR 5 front head	1
6	Expansion port	1
7	Distant columns for expansion port PORT1 mounting to motherboard	3
8	Screw for box completion	2

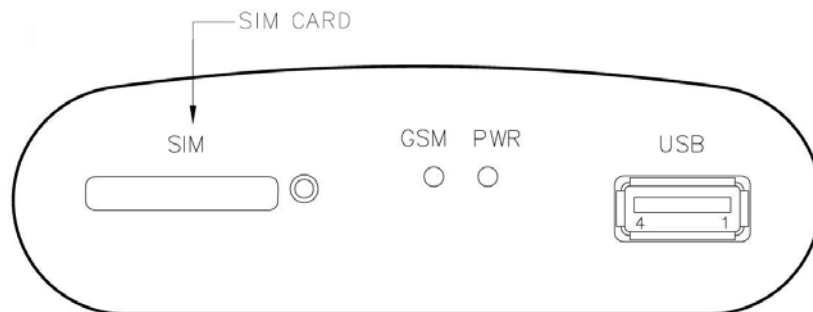
4. Change of the SIM cards



Attention! SIM card include when the router UR 5 is switch off.

First SIM card change:

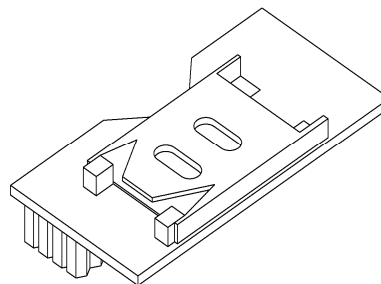
Ensure that the modem is disconnected from the power supply. Press the small yellow button next to the reader to eject the reader holder. Insert the SIM card into the reader holder and slide it in the reader.



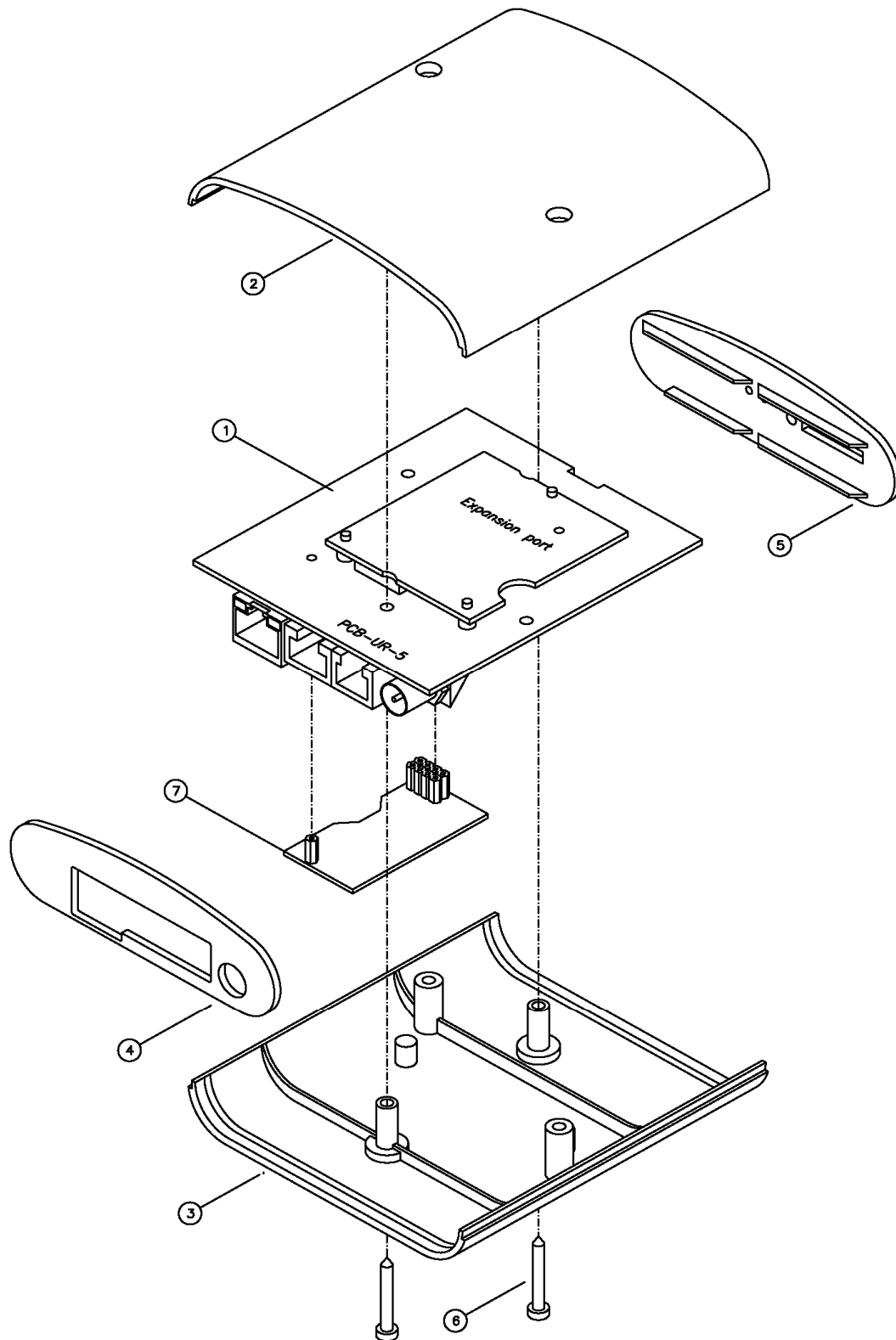
Second SIM card change:

After unscrewed two screws (position 6) on box bottom part (position 3) and carried out box top part (position 2) the second SIM card (position 7) is on the router B-UR-5 motherboard (position 1) from TOP side (see below). After the second SIM card mounting the box is screwed by the help two screws (position 6).

Adapter for the second SIM card:



The second SIM socket mounting:



Parts list and description

Part	Description	Number
1	UMTS router UR 5 motherboard	1
2	UR 5 box top part	1
3	UR 5 box bottom part	1
4	UR 5 rear head	1
5	UR 5 front head	1
6	Screw for box completion	2
7	Adapter for the second SIM card	1

5. Configuration setting over web browser



Attention! If the SIM card isn't included in the UR5 router, it is impossible for the UR5 router to operate. The Included SIM card must be activated for HSDPA/UMTS/EDGE/GPRS UMTS transmissions. Insert the SIM card when the UR5 router is switched off.

Monitoring of status, configuration and administration of the UR5 router can be performed by means of the web interface which is available after entering the IP address of the modem in the web browser. The default IP address of the modem is 192.168.1.1. Configuration may be performed only by the user "root" with initial password "root".

The left part of the web interface contains the menu with pages for monitoring of the Status, Configuration and Administration of the UR5 router.

UMTS router UR5

Status

Network

DHCP

UMTS/GPRS

IPsec

DynDNS

System Log

Configuration

LAN

UMTS/GPRS

Firewall

NAT

IPsec

GRE

L2TP

DynDNS

NTP

SMS

External Port

USB Port

Administration

Change Password

Set Real Time Clock

Unlock SIM Card

Backup Configuration

Restore Configuration

Update Firmware

Reboot

Network Status

Interfaces

eth0Link encap:Ethernet HWaddr 00:CF:53:29:CF:01
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:98 errors:0 dropped:0 overruns:0 frame:0
TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:10037 (9.8 KB) TX bytes:5274 (5.1 KB)

Route Table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0

After the green LED diode starts blinking it is possible to restore initial setting of the router by pressing buttons RST, thereby leading to a reset (green LED will be on).

5.1. Network Status

To view the system information about the modem operation, select the *System Information's* menu item. The bottom part of the window contains information about the system memory usage. The upper part of the window displays detailed information about active interfaces:

- eth0 – parameters of networks interface
 - HWaddr – hardware (unique) address of networks interface
 - inet – own IP address, Bcast – broadcast address, Mask – mask of network
 - MTU – maximal size of packet, which is equipment able transmit, Metric – number of routers, over which packet must pass

- RX packets – received packets, errors – number of errors, dropped – dropped packets
- TX packets – transmit packets, errors – number of errors, dropped – dropped packets
- collisions – number of collisions
- RX bytes – total number of received bytes, TX bytes – total number of transmit bytes
- ppp0 – PPP interface (active connection to UMTS)
 - inet – own IP address for PPP, P-t-P – address of second end, Mask – mask of network
 - MTU – maximal size of packet, which is equipment able transmit, Metric – number of routers, over which packet must pass
 - RX packets – received packets, errors – number of errors, dropped – dropped packets
 - TX packets – transmit packets, errors – number of errors, dropped – dropped packets
 - collisions – number of collisions
 - RX bytes – total number of received bytes, TX bytes – total number of transmit bytes
- gre1 – interface of the GRE tunnel
 - inet – own IP address for GRE, P-t-P – address of second end, Mask – mask of network
 - MTU – maximal size of packet, which is equipment able transmit, Metric – number of routers, over which packet must pass
 - RX packets – received packets, errors – number of errors, dropped – dropped packets
 - TX packets – transmit packets, errors – number of errors, dropped – dropped packets
 - collisions – number of collisions
 - RX bytes – total number of received bytes, TX bytes – total number of transmit bytes

By active UMTS connection it is in the *Network status* display ppp0 connection.

Network Status

Interfaces

eth0

Link encap:Ethernet HWaddr 00:0A:14:80:09:D3
inet addr:192.168.2.254 Bcast:192.168.2.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:2004 errors:0 dropped:0 overruns:0 frame:0
TX packets:721 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:215537 (210.4 KB) TX bytes:390840 (381.6 KB)

ppp0

Link encap:Point-Point Protocol
inet addr:10.0.1.228 P-t-P:192.168.254.254 Mask:255.255.255.255
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
RX packets:31 errors:0 dropped:0 overruns:0 frame:0
TX packets:31 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:3
RX bytes:1879 (1.8 KB) TX bytes:2381 (2.3 KB)

Route Table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.254.254	0.0.0.0	255.255.255.255	UH	0	0	0	ppp0
192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
0.0.0.0	192.168.254.254	0.0.0.0	UG	0	0	0	ppp0

5.2. DHCP Status

Information about the IP address which was allotted by DHCP server to UR5; it is possible to find in menu in sum *DHCP*:

- lease 192.168.1.2 (generally IP address) – assigned IP address
- starts – information about time of assigned IP address
- ends – information about time of termination IP address
- hardware ethernet – hardware MAC (unique) address
- uid – unique ID

DHCP Status	
Active DHCP Leases	
lease 192.168.1.2 {	
starts 4 1970/01/01 00:00:18;	
ends 4 1970/01/01 00:10:18;	
hardware ethernet 00:40:f4:8a:5c:76;	
uid 01:00:40:f4:8a:5c:76;	
}	

In the extreme the DHCP status can display to one's IP address two DHCP status, causes of that it can be reset of network cards.

5.3. IPsec status

Information on actual IPsec tunnel state can be called up in option entries NTP in the menu. Detailed information description here as shown can be found on the following link <http://www.freeswan.org/doc.html>.

IPsec Status	
IPsec Tunnel Info	
000 interface eth0/eth0 192.168.2.254	
000 interface ppp0/ppp0 10.0.1.229	
000 tmyid = (none)	
000 debug none	
000	
000 algorithm ESP encrypt: id=64, name=(null), ivlen=231, keysize=58844, keysize=0	
000	
000 algorithm IKE encrypt: id=5, name=OAKLEY_3DES_CBC, blocksize=8, keydeflen=192	
000 algorithm IKE encrypt: id=7, name=OAKLEY_AES_CBC, blocksize=16, keydeflen=128	
000 algorithm IKE hash: id=1, name=OAKLEY_MD5, hashsize=16	
000 algorithm IKE hash: id=2, name=OAKLEY_SHA1, hashsize=20	
000 algorithm IKE dh group: id=2, name=OAKLEY_GROUP_MODP1024, bits=1024	
000 algorithm IKE dh group: id=5, name=OAKLEY_GROUP_MODP1536, bits=1536	
000 algorithm IKE dh group: id=14, name=OAKLEY_GROUP_MODP2048, bits=2048	
000 algorithm IKE dh group: id=15, name=OAKLEY_GROUP_MODP3072, bits=3072	
000 algorithm IKE dh group: id=16, name=OAKLEY_GROUP_MODP4096, bits=4096	
000 algorithm IKE dh group: id=17, name=OAKLEY_GROUP_MODP6144, bits=6144	
000 algorithm IKE dh group: id=18, name=OAKLEY_GROUP_MODP8192, bits=8192	
000	
000 stats dh_ops.c: {curr_cnt, total_cnt, maxsz} :context={0,0,0} trans={0,0,0} attrs={0,0,0}	
000	
000 "ipsec": 192.168.2.0/24==10.0.1.229[Src]...10.0.2.38[Src]==192.168.1.0/24; unrouted; eroute owner: #0	
000 "ipsec": srcip=unset; dstip=unset; srcup=bin/_updown; dstup=bin/_updown;	
000 "ipsec": ike_life: 3600s; ipsec_life: 3600s; rekey_margin: 540s; rekey_fuzz: 100%; keyingtries: 0	
000 "ipsec": policy: PSK+ENCRYPT+TUNNEL+UP; prio: 24,24; interface: ppp0;	
000 "ipsec": newest ISAKMP SA: #1; newest IPsec SA: #0;	
000 "ipsec": IKE algorithm newest: 3DES_CBC_192-MD5-MODP1536	
000	
000 #23: "ipsec":500 STATE_QUICK_I1 (sent QI1, expecting QR1); EVENT_RETRANSMIT in 10s; lastdpd=-1s(seq in:0 out:0)	
000 #1: "ipsec":500 STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in 1514s; newest ISAKMP; lastdpd=-1s(seq in:0 out:0)	
000	

5.4. UMTS/GPRS Status

The item *UMTS* in the menu contains information about the signal strength. At the bottom of this window is the PPP Connection Log, where you will find information about PPP connection establishment and pertinent problems on this establishment.

UMTS/GPRS Status
Actual GSM Info
GSM signal strength : -73 dBm
PPP Connection Log
2007-11-30 06:00:05 Connection successfully established.

5.5. DynDNS status

DynDNS up - data entry result on server www.dyndns.org can be called - up in option DynDNS item in the menu.

DynDNS Status
Last DynDNS Update Status
DynDNS client is disabled.

5.6. System Log

In case of any problems with PPP connection it is possible to view the system log by pressing the *System Log* menu item. The upper part of the window displays possible errors during PPP connection establishment. To update the contents of the window press the *Refresh* button. By the help of the *Save* button it is possible to save the system log.

System Log
System Messages
<pre> 2007-08-06 10:06:27 pppd[208]: rcvd [LCP EchoRep id=0x13 magic=0x30e28cf5 0a 0b 0c 0e] 2007-08-06 10:06:57 pppd[208]: sent [LCP EchoReq id=0x14 magic=0x2593a852] 2007-08-06 10:06:57 pppd[208]: rcvd [LCP EchoRep id=0x14 magic=0x30e28cf5 0a 0b 0c 0e] 2007-08-06 10:07:27 pppd[208]: sent [LCP EchoReq id=0x15 magic=0x2593a852] 2007-08-06 10:07:27 pppd[208]: rcvd [LCP EchoRep id=0x15 magic=0x30e28cf5 0a 0b 0c 0e] 2007-08-06 10:07:57 pppd[208]: sent [LCP EchoReq id=0x16 magic=0x2593a852] 2007-08-06 10:07:57 pppd[208]: rcvd [LCP EchoRep id=0x16 magic=0x30e28cf5 0a 0b 0c 0e] 2007-08-06 10:08:27 pppd[208]: sent [LCP EchoReq id=0x17 magic=0x2593a852] 2007-08-06 10:08:27 pppd[208]: rcvd [LCP EchoRep id=0x17 magic=0x30e28cf5 0a 0b 0c 0e] 2007-08-06 10:08:57 pppd[208]: sent [LCP EchoReq id=0x18 magic=0x2593a852] 2007-08-06 10:08:57 pppd[208]: rcvd [LCP EchoRep id=0x18 magic=0x30e28cf5 0a 0b 0c 0e] 2007-08-06 10:09:27 pppd[208]: sent [LCP EchoReq id=0x19 magic=0x2593a852] 2007-08-06 10:09:27 pppd[208]: rcvd [LCP EchoRep id=0x19 magic=0x30e28cf5 0a 0b 0c 0e] 2007-08-06 10:09:57 pppd[208]: sent [LCP EchoReq id=0x1a magic=0x2593a852] 2007-08-06 10:09:57 pppd[208]: rcvd [LCP EchoRep id=0x1a magic=0x30e28cf5 0a 0b 0c 0e] 2007-08-06 10:10:27 pppd[208]: sent [LCP EchoReq id=0x1b magic=0x2593a852] 2007-08-06 10:10:27 pppd[208]: rcvd [LCP EchoRep id=0x1b magic=0x30e28cf5 0a 0b 0c 0e] 2007-08-06 10:10:57 pppd[208]: sent [LCP EchoReq id=0x1c magic=0x2593a852] 2007-08-06 10:10:57 pppd[208]: rcvd [LCP EchoRep id=0x1c magic=0x30e28cf5 0a 0b 0c 0e] 2007-08-06 10:11:27 pppd[208]: sent [LCP EchoReq id=0x1d magic=0x2593a852] 2007-08-06 10:11:27 pppd[208]: rcvd [LCP EchoRep id=0x1d magic=0x30e28cf5 0a 0b 0c 0e] 2007-08-06 10:11:57 pppd[208]: sent [LCP EchoReq id=0x1e magic=0x2593a852] 2007-08-06 10:11:57 pppd[208]: rcvd [LCP EchoRep id=0x1e magic=0x30e28cf5 0a 0b 0c 0e] 2007-08-06 10:12:27 pppd[208]: sent [LCP EchoReq id=0x1f magic=0x2593a852] 2007-08-06 10:12:27 pppd[208]: rcvd [LCP EchoRep id=0x1f magic=0x30e28cf5 0a 0b 0c 0e] </pre>
<input type="button" value="Stop"/> <input type="button" value="Refresh"/> <input type="button" value="Save"/>

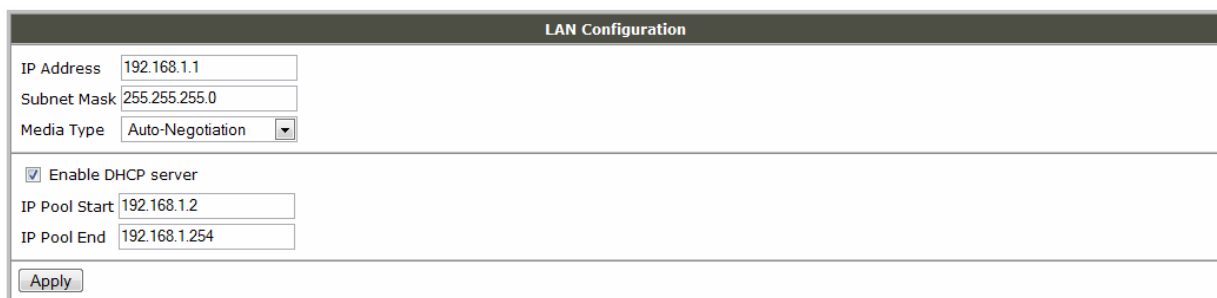
5.7. Network Configuration

To enter the network configuration, select the *Network* menu item. In the first part of the window it is possible to define the network interface IP address (*IP address*), the network mask (*Subnet Mask*) and media type (*Media Type*).

In the second part of window, it is possible to define the DHCP server by checking the *Enable DHCP server* option. In the window it is possible to define the beginning (*IP Pool Start*) and end (*IP Pool End*) of the pool of IP addresses that will be assigned to DHCP clients.

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

The DHCP server assigns to the connected clients IP addresses from the defined address pool, IP address of the gate and IP address of the primary DNS server. It is important not to overlap the ranges of the static engaged IP address with the address allotted by the help of DHCP, or else it is able to achieve a collision of addresses and thereby to create a false function of the network.



5.8. UMTS/GPRS Configuration

To enter the PPP connection configuration select the *PPP* menu item. If the *Create PPP connection* option is checked, the modem itself automatically tries to establish PPP connection after switch on. In the window it is possible to define *APN*, *Username*, *Password* and *IP address* for both SIM cards, eventually if the first SIM card has set two difference APN's.



Attention! If in the UR5 is include the main SIM card which has set two difference APN's, second socket for SIM card have not to be in the UR5, otherwise switch to secondary APN according to rules in web fail.

If the *APN* field is not filled in, the APN will be automatically assigned by the IMSI code of the SIM card. If the PLMN (operator number format) is not in the book of APN, then default APN is "internet". The mobile operator defines APN. The PLMN parameter is possible to define in *Operator* item. *Network Type* item defines way of data transmission, respectively *Automatic selection* according to network availability or *UMTS/HSDPA* or *GPRS/EDGE* technology.

If the *IP address* field is not filled in, the operator when establishing the connection will automatically assign the IP address.

The choice *Get DNS address from operator* is given for easier configuration on client side; by this choice it is possible to use the web browser. If this field is not filled, the client's station has no access to the Internet and it is possible to send data to a known IP address.

If the *Check PPP connection* option is checked, it has active control of connection over PPP. The modem will automatically send the ping question to the selected IP address (Ping IP Address) in periodic time intervals (Ping Interval). It is possible to use as ping IP address for example DNS server of mobile operator.

At the bottom of configuration it is possible set rules for switching between two SIM cards, eventually between two APN on one SIM card. Parameter *Default SIM card* sets default SIM card from which will try the PPP connection. If this parameter is set to *none* the UMTS router UR5 is launch in offline mode and it is need establish PPP connection by SMS message. If PPP connection fail the parameter *Switch to other SIM card when connection fails* ensure switch to secondary SIM card, if it is included and set, or to secondary APN of the first SIM card. In case that the roaming is detect the parameter *Switch to secondary SIM card when roaming is detected* enable switching to secondary SIM card, or to secondary APN of the default SIM card. Parameter *Switch to primary SIM card after timeout* defines conditions, how to switch back to the default SIM card.

Parameter *Initial Timeout* set time after which UR5 try to make connection with default SIM card, range of this parameter is 1 up to 10000 minutes. Parameter *Subsequent Timeout* set time period for every other next attempt to make connection with default SIM card, range is 1 up to 10000 minutes. Parameter *Additive Constant* set amount of time which is added to every attempt at main connection establishment after unsuccessful defined attempt (for example: after second unsuccessful attempt at main connection establishment time of next attempt is extended about 30 minutes etc.). Range is 1 up to 1000 minutes.

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

UMTS/GPRS Configuration			
<input checked="" type="checkbox"/> Create PPP connection			
	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"/>	
IP Address *	<input type="text"/>	<input type="text"/>	
MRU	<input type="text" value="1500"/>	<input type="text" value="1500"/>	bytes
MTU	<input type="text" value="1500"/>	<input type="text" value="1500"/>	bytes
Operator *	<input type="text"/>	<input type="text"/>	
Network Type	<input type="text" value="automatic selection"/>	<input type="text" value="automatic selection"/>	
<input checked="" type="checkbox"/> Get DNS addresses from operator			
<input type="checkbox"/> Check PPP connection			
Ping IP Address	<input type="text"/>		
Ping Interval	<input type="text"/>	min	
Default SIM card	<input type="text" value="primary"/>		
<input type="checkbox"/> Switch to other SIM card when connection fails			
<input type="checkbox"/> Switch to secondary SIM card when roaming is detected			
<input type="checkbox"/> Switch to primary SIM card after timeout			
Initial Timeout	<input type="text" value="60"/>	min	
Subsequent Timeout *	<input type="text"/>	min	
Additive Constant *	<input type="text"/>	min	
* can be blank			
<input type="button" value="Apply"/>			

 **Attention! Check PPP connection we recommended in case of uninterrupted running.**

Note:

- MTU (Maximum Transmission Unit) – it identifies the maximal size of packet that it is possible to transfer in the given environment.
- MRU (Maximum Receiving Unit) – it identifies the maximal size of packet that it is possible to receive in the given environment.

Default value is 1500 bytes. Other settings may cause incorrect transmission of data.

5.9. Firewall Configuration

By the help of a firewall are possible set IP addresses from which is possible remote access on UR 5. The choice *Allow remote access only from specified hosts* is given for easier configuration of hosts. In this firewall configuration is possible set up to four remote accesses by the help of *Source IP Address*, *Protocol* and *Target Port*.

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

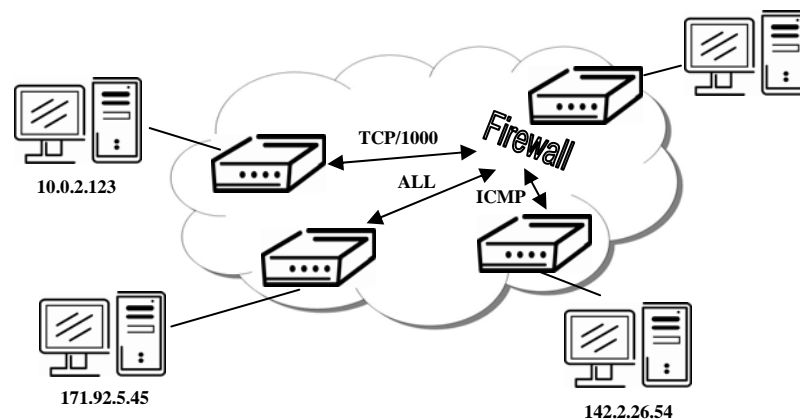
Firewall Configuration

☐ Allow remote access only from specified hosts

Source IP Address	Protocol	Target Port *
<input type="text"/>	All	<input type="text"/>
<input type="text"/>	All	<input type="text"/>
<input type="text"/>	All	<input type="text"/>
<input type="text"/>	All	<input type="text"/>

* can be blank

Example of the firewall configuration:



Firewall Configuration

☒ Allow remote access only from specified hosts

Source IP Address	Protocol	Target Port *
171.92.5.45	All	<input type="text"/>
10.0.2.123	TCP	1000
142.2.26.54	ICMP	<input type="text"/>
<input type="text"/>	All	<input type="text"/>

* can be blank

5.10. NAT Configuration

To enter the Network Address Translation configuration, select the *NAT* menu item. By checking off the *Send all incoming packets to default server* item and setting of the *Default Server* item it is possible to put the UR5 router into the mode in which all incoming data from UMTS will be routed to the computer with the defined IP address.

If the *Enable remote HTTP access* and port number field is filled in, it is possible to configure the router over the web interface.

Choosing *Enable remote Telnet access* and port number enter makes it possible to access via Telnet.

Choice *Enable remote SNMP access* and port number makes it possible access to SNMP agent.

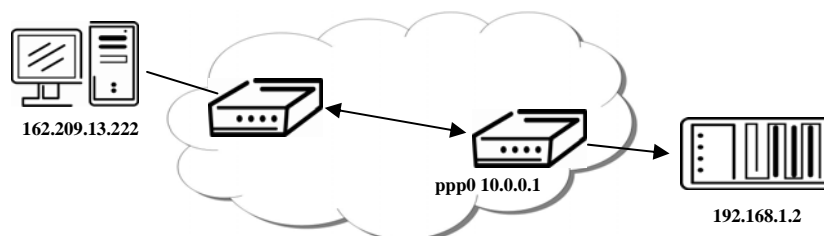
The changes in settings will apply after pressing the *Apply* button.

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

☒ Enable remote HTTP 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

Configuration example with connected equipment on UR5:



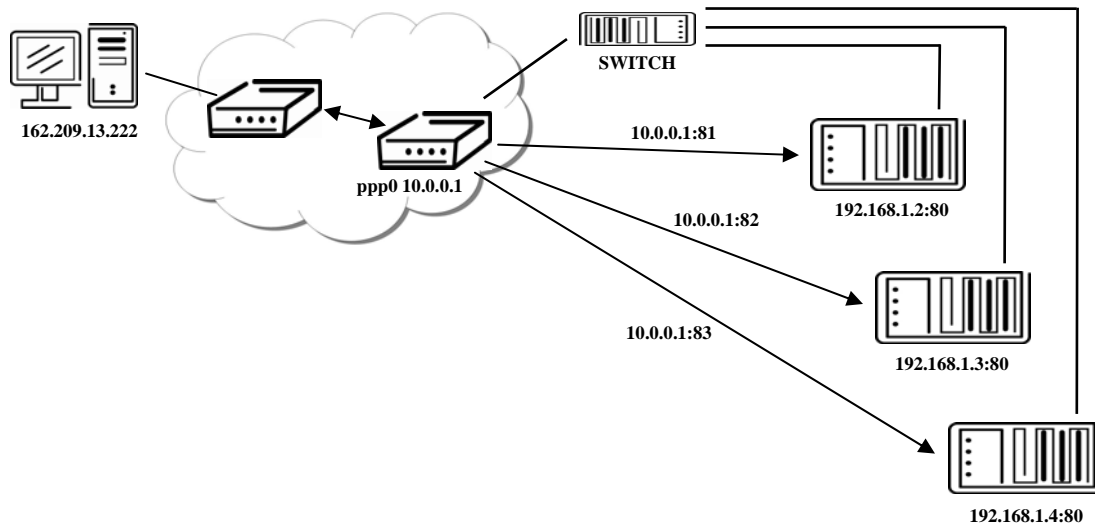
NAT Configuration			
Public Port	Private Port	Type	Server IP Address
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	

☒ Enable remote HTTP 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

In this configuration it is important to have marked *Send all remaining incoming packets to default server*, The IP address in this case is the device address behind the UR5. Equipment connected behind the UR5 must have the setting Default Gateway on the UR5. For PING on IP address of the SIM card matches connected equipment.

Example of the configuration with more connected equipment:



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

☒ Enable remote HTTP 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

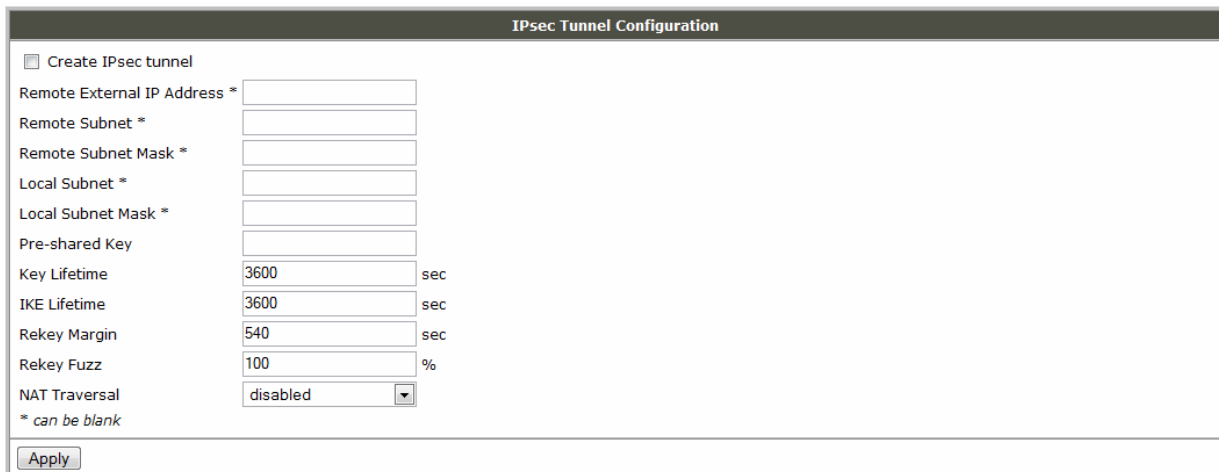
In this configuration the address defines *Server IP Address* equipment wired behind the UR5. For PING on IP address of the SIM card matches UR5. Access to the web interface of equipment behind UR5 is possible by the help of Port Forwarding, when after the IP address of SIM is given the external port of the equipment on which we want to join. If required on port 80 it is checked the individual external ports (Public port), there this port isn't defined, therefore at check off choose *Enable remote http access* it automatically opens the web interface on the UR5. If this choice isn't checked and is checked option *Send all remaining incoming packets to default server* created oneself connection on induction IP address. If it is not checked options web interface and *Default server IP address* it is request failure.

5.11. IPsec Tunnel Configuration

IPsec tunnel configuration it can be call - up option IPsec item in menu. In window it can be define off - side tunnel IP address (*Remote External IP Address*), address nets behind off - side tunnel (*Remote Subnet*), mask nets behind off - side tunnel (*Remote Subnet Mask*), address LAN (*Remote Subnet*), mask LAN (*Remote Subnet Mask*), sharable key for both parties tunnel (*Pre shared Key*), service life keys (*Key Lifetime*) and service life IKA SA (*IKE Lifetime*). *Rekey Margin* specifies how long before connection expiry should attempts to negotiate a replacement begin. *Rekey Fuzz* specifies the maximum percentage by which *Rekey Margin* should be randomly increased to randomize re-keying intervals. If it is used address translation between two end points of the IPsec tunnel it is need permit NAT Traversal (*Enabled*).

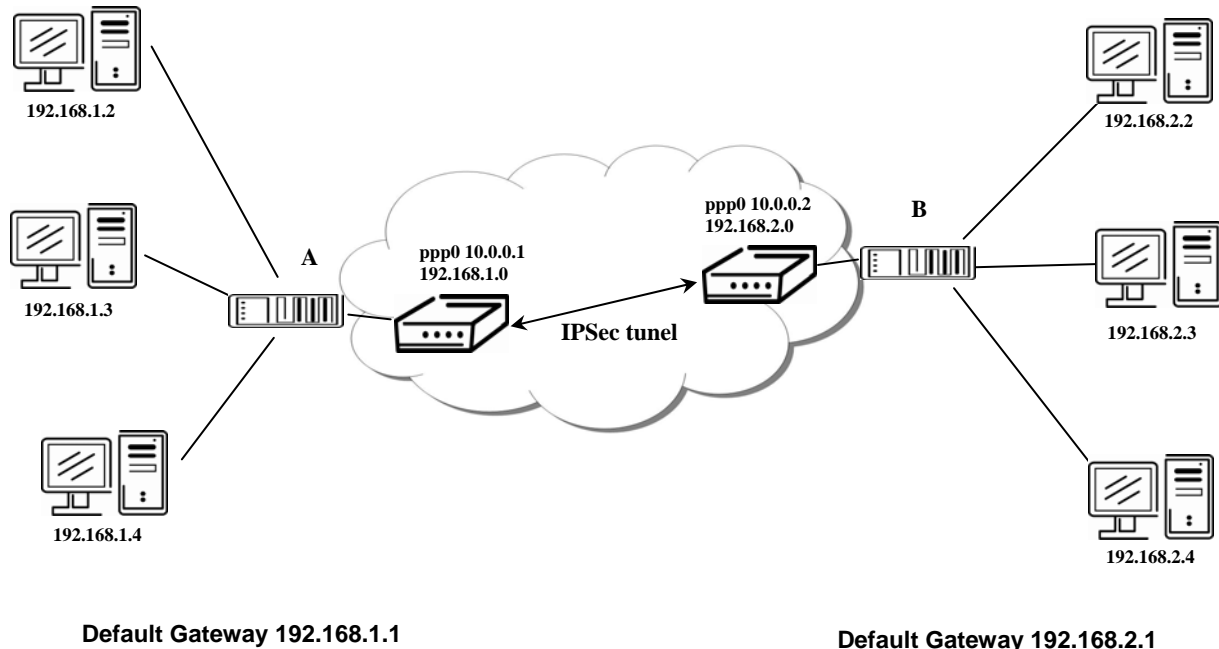
IPsec tunnel allows protected connection of two networks LAN to the one which it is cheek as one homogenous.

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



The image shows a screenshot of the 'IPsec Tunnel Configuration' window. At the top, there is a title bar with the text 'IPsec Tunnel Configuration'. Below the title bar, there is a checkbox labeled 'Create IPsec tunnel'. Underneath, there are several input fields and labels: 'Remote External IP Address *', 'Remote Subnet *', 'Remote Subnet Mask *', 'Local Subnet *', 'Local Subnet Mask *', 'Pre-shared Key', 'Key Lifetime' (with a value of 3600 and unit 'sec'), 'IKE Lifetime' (with a value of 3600 and unit 'sec'), 'Rekey Margin' (with a value of 540 and unit 'sec'), 'Rekey Fuzz' (with a value of 100 and unit '%'), and 'NAT Traversal' (with a dropdown menu showing 'disabled'). At the bottom left, there is a small text '* can be blank'. At the bottom center, there is an 'Apply' button.

Example of the IPsec Tunnel configuration



IPsec tunnel configuration:

	A	B
Remote External 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 Mask:	255.255.255.0	255.255.255.0
Pre-shared Key:	test	test

5.12. GRE Tunnels Configuration

To enter the GRE tunnels configuration, select the *GRE* menu item. It is possible to configure up to four GRE tunnels. The single tunnels are active after entering the choice *Create x GRE tunnel*. In the single window it is possible to define the IP address of the remote side of the tunnel (*Remote External IP Address*), internal IP address of the local side of the tunnel (*Local Internal IP Address*), internal IP address of the remote side of the tunnel (*Remote Internal IP Address*), address of the network behind the remote side of the tunnel (*Remote Subnet*) and the mask of the network behind the remote side of the tunnel (*Remote Subnet Mask*). The GRE tunnel is used for connection of two networks to one that appears as one homogenous.

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

GRE Tunnels Configuration

☐ Create 1st GRE tunnel

Remote External IP Address
 Remote Subnet
 Remote Subnet Mask
 Local Internal IP Address *
 Remote Internal IP Address *

☐ Create 2nd GRE tunnel

Remote External IP Address
 Remote Subnet
 Remote Subnet Mask
 Local Internal IP Address *
 Remote Internal IP Address *

☐ Create 3rd GRE tunnel

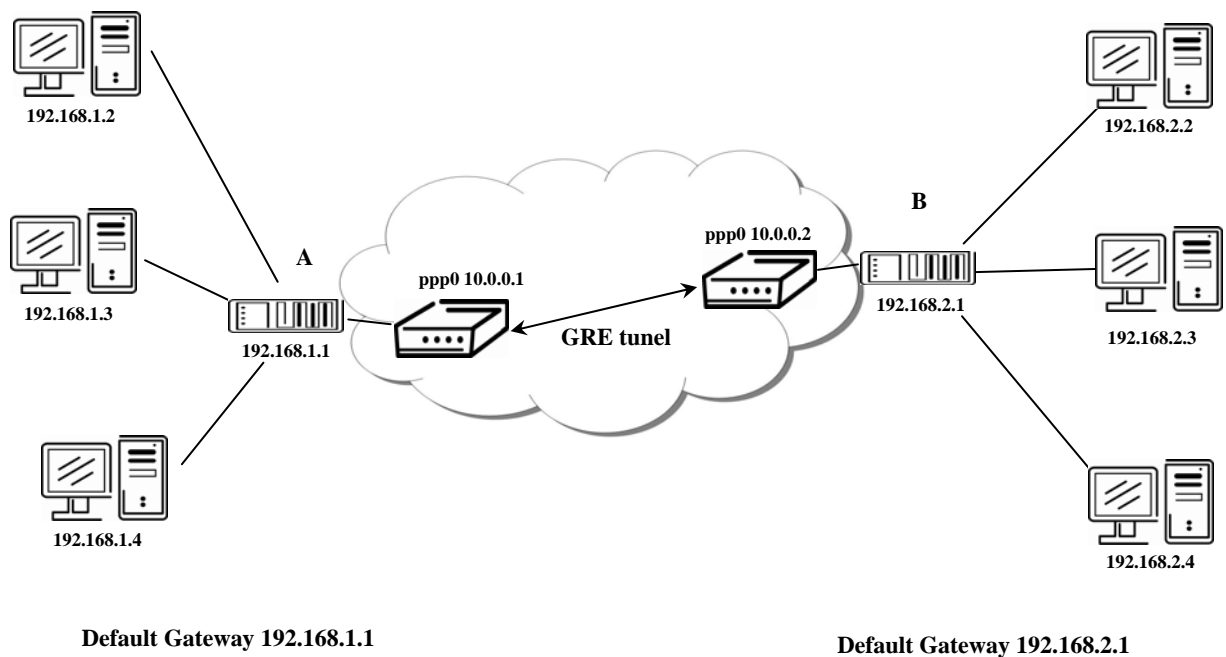
Remote External IP Address
 Remote Subnet
 Remote Subnet Mask
 Local Internal IP Address *
 Remote Internal IP Address *

☐ Create 4th GRE tunnel

Remote External IP Address
 Remote Subnet
 Remote Subnet Mask
 Local Internal IP Address *
 Remote Internal IP Address *

* can be blank

Example of the GRE Tunnel configuration:



GRE tunnel Configuration:

	A	B
Remote External IP Address:	10.0.0.2	10.0.0.1
Local Internal IP Address:	192.168.1.254	192.168.2.254
Remote Subnet:	192.168.2.0	192.168.1.0
Remote Subnet Mask:	255.255.255.0	255.255.255.0

5.13. L2TP Configuration

To enter the L2TP tunnel configuration, select the L2TP menu item. In the window it is possible to define L2TP tunnel mode (Mode) on UR5 side, in case of client IP address of server (Server IP Address), start IP address in range, which is offered by server to clients (Client Start IP Address), end IP address in range, which is offered by server to clients (Client End IP Address), IP address of the local side of the tunnel (Local IP Address), IP address of the remote side of the tunnel (Remote IP Address), address of the network behind the remote side of the tunnel (Remote Subnet), the mask of the network behind the remote side of the tunnel (Remote Subnet Mask), username for login to L2TP tunnel (Username) and password (Password).

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

L2TP Tunnel Configuration

☐ Create L2TP tunnel

Mode

L2TP server

Server IP Address

Client Start IP Address

Client End IP Address

Local IP Address *

Remote IP Address *

Remote Subnet *

Remote Subnet Mask *

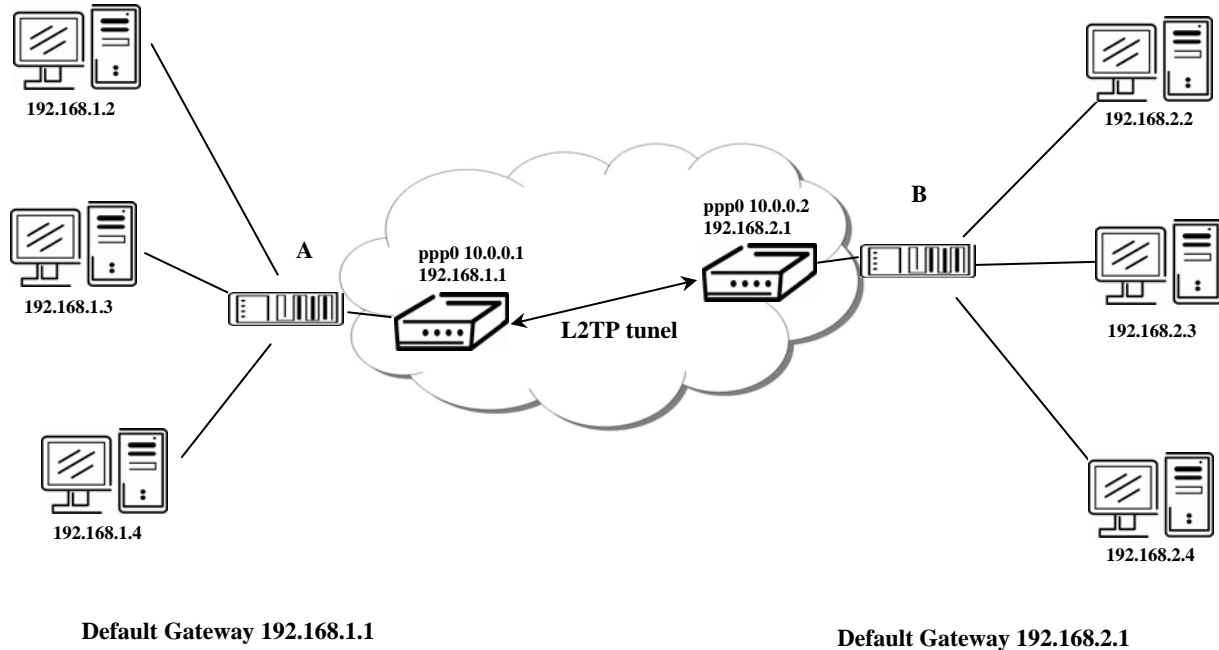
Username

Password

* can be blank

Apply

Example of the L2TP configuration:



Configuration of the L2TP tunnel:

	A	B
Mode	L2TP Server	L2TP Client
Server IP Address	---	10.0.0.1
Client Start IP Address:	192.168.3.2	---
Client End IP Address:	192.168.3.254	---
Local IP Address:	192.168.3.1	---
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

5.14. DynDNS Client Configuration

DynDNS client Configuration is possible by call - up option DynDNS item in menu. In the window can be defined the domain of third order registered on server www.dyndns.org (*Hostname*), user name (*Username*) and password (*Password*).

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

DynDNS Configuration

☐ Enable DynDNS client

Hostname

Username

Password

Example of the DynDNS client configuration with domain conel.dyndns.org, username conel and password conel:

DynDNS Configuration	
<input checked="" type="checkbox"/>	Enable DynDNS client
Hostname	<input type="text" value="conel.dyndns.org"/>
Username	<input type="text" value="conel"/>
Password	<input type="text" value="conel"/>
<input type="button" value="Apply"/>	

5.15. NTP Client Configuration

NTP client Configuration is possible by call - up option NTP item in the menu. In the window can be defined the address prime (Primary NTP server Address) and secondary NTP server (Secondary NTP server Address), by the help of which router after initial connection to the GPRS from connecting power supply will adjust the internal clock.

Example of NTP server address can be found at ntp.isc.org/bin/view/Servers/StratumOneTimeServers.

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

NTP Configuration	
<input type="checkbox"/>	Synchronize clock with NTP server on power up
Primary NTP Server Address	<input type="text"/>
Secondary NTP Server Address	<input type="text"/>
<input type="button" value="Apply"/>	

Example of the NTP configuration with set primary and secondary NTP server:

NTP Configuration	
<input checked="" type="checkbox"/>	Synchronize clock with NTP server on power up
Primary NTP Server Address	<input type="text" value="ntp.cesnet.cz"/>
Secondary NTP Server Address	<input type="text" value="tik.cesnet.cz"/>
<input type="button" value="Apply"/>	

5.16. SNMP Configuration

To enter the SNMP Configuration it is possible SNMP agent ver.1 configuration which sends information about the UR5, eventually about status of the expansion port CNT or MBUS.

The *Community* item defines password for access to the SNMP agent. Item *Contact* identify a person which manage the UR5 together with informations how contact this person, item *Name* is designation of the UR5 and item *Location* describe physical placing of the UR5.

By the choice *Enable XC-CNT extension* is possible monitor the expansion port CNT inputs status or by the choice *Enable M-BUS extension* and enter the *Baudrate*, *Parity* and *Stop Bits* is possible monitor meter status connected to the expansion port MBUS status.

SNMP Configuration

☒ Enable SNMP agent
 Community
 Contact *
 Name *
 Location *
* can be blank

☐ Enable XC-CNT extension

☐ Enable M-BUS extension
 Baudrate
 Parity
 Stop Bits

Every monitor value is uniquely identified by the help of number identifier **OID** - *Object Identifier*.

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

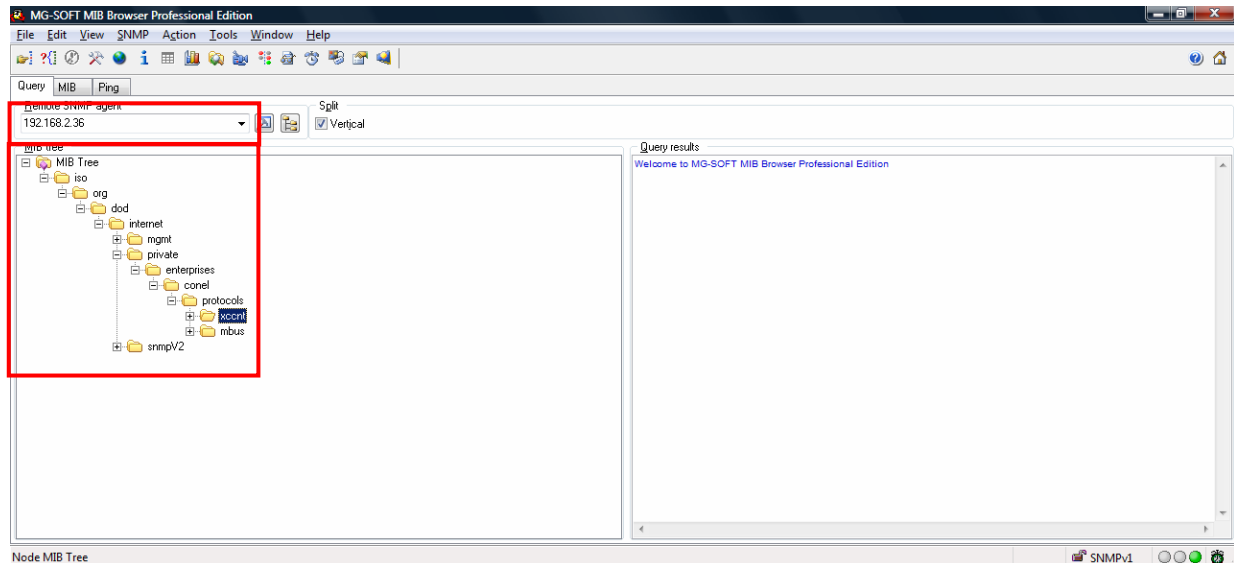
OID	Description
.1.3.6.1.4.1.30140.2.1.1.0	Analogy input AN1 (range 0-4095)
.1.3.6.1.4.1.30140.2.1.2.0	Analogy input AN2 (range 0-4095)
.1.3.6.1.4.1.30140.2.1.3.0	Counter input CNT1 (range 0-4294967295)
.1.3.6.1.4.1.30140.2.1.4.0	Counter input CNT2 (range 0-4294967295)
.1.3.6.1.4.1.30140.2.1.5.0	Binary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

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

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

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

Example of the MIB browser:



It is important to set the IP address of the SNMP agent (UR5) 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.

5.17. SMS Configuration

To enter the SMS Configuration it is possible *Enable remote control via SMS*. After this is possible establish and close PPP connection by SMS message.

SMS	Description
go online sim 1	PPP connection establishment from first SIM card
go online sim 2	PPP connection establishment from second SIM card
go offline	PPP connection termination

Next it is possible to select automatic sending of SMS messages following power up and at the start or the loss of the PPP connection. Info is possible to send to five telephone numbers. Unit ID is the name of the UR5 that it will send a SMS message to. Unit ID may have a random form.

By the choice *Enable AT-SMS protocol on external port* and *Baudrate* is possible send/receive a SMS on serial port.

By the choice *Enable AT-SMS protocol on TCP port* and enter the *TCP port* is possible send/receive a SMS on TCP port. SMS messages send by the help of a standard AT commands. More about the AT commands in reference [1].

SMS Configuration	
<input type="checkbox"/>	Enable remote control via SMS
<input type="checkbox"/>	Send SMS on power up
<input type="checkbox"/>	Send SMS on PPP connect
<input type="checkbox"/>	Send SMS on PPP disconnect
Phone Number 1	<input type="text"/>
Phone Number 2	<input type="text"/>
Phone Number 3	<input type="text"/>
Phone Number 4	<input type="text"/>
Phone Number 5	<input type="text"/>
Unit ID *	<input type="text"/>
<hr/>	
<input type="checkbox"/>	Enable AT-SMS protocol on external port
Baudrate	<input type="text" value="9600"/>
<hr/>	
<input type="checkbox"/>	Enable AT-SMS protocol over TCP
TCP port	<input type="text"/>
* can be blank	
<input type="button" value="Apply"/>	

After powering up the UR5, the initial telephone number receives a SMS in the form of:

UR5 (Unit ID) has been powered up. GSM signal strength: -xxdBm,
where is GSM signal strength – level signal

After PPP establishment (PPP connect) comes a SMS in the form:

UR5 (Unit ID) has established PPP connection

After PPP disconnect at the initial telephone number comes a SMS in the form:

UR5 (Unit ID) has lost UMTS connection.

Configuration of sending this SMS is following:

SMS Configuration	
<input type="checkbox"/>	Enable remote control via SMS
<input checked="" type="checkbox"/>	Send SMS on power up
<input checked="" type="checkbox"/>	Send SMS on PPP connect
<input checked="" type="checkbox"/>	Send SMS on PPP disconnect
Phone Number 1	<input type="text" value="723123456"/>
Phone Number 2	<input type="text" value="712123456"/>
Phone Number 3	<input type="text" value="713123456"/>
Phone Number 4	<input type="text"/>
Phone Number 5	<input type="text"/>
Unit ID *	<input type="text" value="UR5"/>
<hr/>	
<input type="checkbox"/>	Enable AT-SMS protocol on external port
Baudrate	<input type="text" value="9600"/>
<hr/>	
<input type="checkbox"/>	Enable AT-SMS protocol over TCP
TCP port	<input type="text"/>
* can be blank	
<input type="button" value="Apply"/>	

Example of the UR5 onfiguration for SMS sending via serial interface or via Ethernet:

SMS Configuration

☐ Enable remote control via SMS
☐ Send SMS on power up
☐ Send SMS on PPP connect
☐ Send SMS on PPP disconnect

Phone Number 1
 Phone Number 2
 Phone Number 3
 Phone Number 4
 Phone Number 5
 Unit ID *

☒ Enable AT-SMS protocol on external port
 Baudrate

☒ Enable AT-SMS protocol over TCP
 TCP port
* can be blank

The SMS is possible to do for example in HyperTerminal program. After establish of the connection with the UR5 via serial interface or Ethernet, is possible do with SMS by the help of the next AT commands (more about AT commands see reference [1]):

AT commands	Description
AT+CMGF=1	Set the text mode for SMS writing
AT+CMGS=<tel. number>	Commands enables to send SMS on entered tel. number
AT+CMGL=ALL	List of all SMS messages
AT+CMGR=<index>	Read of the definite SMS (all SMS has our index)
AT+CMGD=<index>	SMS delete according to index

For the text mode for SMS writing is used command *AT+CMGF=1*.

AT+CMGF=1 Enter
OK

The SMS message is create by the help of command *AT+CMGS=<tel. number>*. After *Enter* button press is display mark *>*, behind this mark it is possible to write own SMS message. The SMS message is send by the help of *CTRL+Z* (SMS sending take about few minutes). The SMS writing is possible cancel by *Esc*.

AT+CMGS=712123456 Enter
>Hello World! CTRL+Z
OK

The new SMS is possible find out by the help of command *AT+CMGL=ALL*. This command reproaches all SMS messages.

AT+CMGL=ALL Enter
+CMGL: <index>, <status>,<sender number>, ,<date>,<time>
SMS text.
+CMGL: 1,"REC UNREAD", "+420721123456", , "08/02/02, 10:33:26+04"

Hello World!

where <index> is ordinal number of the SMS,

<status> is SMS status:

REC UNREAD – SMS unread

REC READ – SMS read

STO UNSENT – stored unsent SMS

STO SENT – stored sent SMS

ALL – all SMS messages

<sender number> is tel. number from which the SMS was receive,

<date> is date of SMS receive,

<time> is time of SMS receive.

The new SMS message is possible read by command AT+CMGR=<index>.

AT+CMGR=1 Enter

+CMGL: <index>, <status>, <sender number>, , <date>, <time>
SMS text.

**+CMGL: 1, "REC READ", "+420721123456", , "08/01/12, 9:48:04+04"
Hello World!**

Received SMS is possible delete by command AT+CMGD=<index>.

AT+CMGD=1 Enter

OK

5.18. External Port Configuration

The external port configuration can be selected by option External Port in menu. Inside the window can be defined baudrate, number of data bits, parity, number of stop bits and mode. Split timeout is for messages.

In mode TCP server it is necessary to enter the TCP port, on which the router will listen to incoming requests about TCP connection. In mode TCP client it is necessary to enter the server address and final TCP port.

After checking TCP connection it activates verification of coupled TCP connection. Inside the window can be define time, after which it will carry out verification of the connection (Keepalive Time), waiting time on answer (Keepalive Interval) and number of tests (Keepalive Probes).

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

External Port Configuration

☐ Enable external port access over TCP

Port Type: RS-232

Baudrate: 9600

Data Bits: 8

Parity: none

Stop Bits: 1

Split Timeout: 20 msec

Mode: TCP server

Server Address:

TCP Port:

☐ Check TCP connection

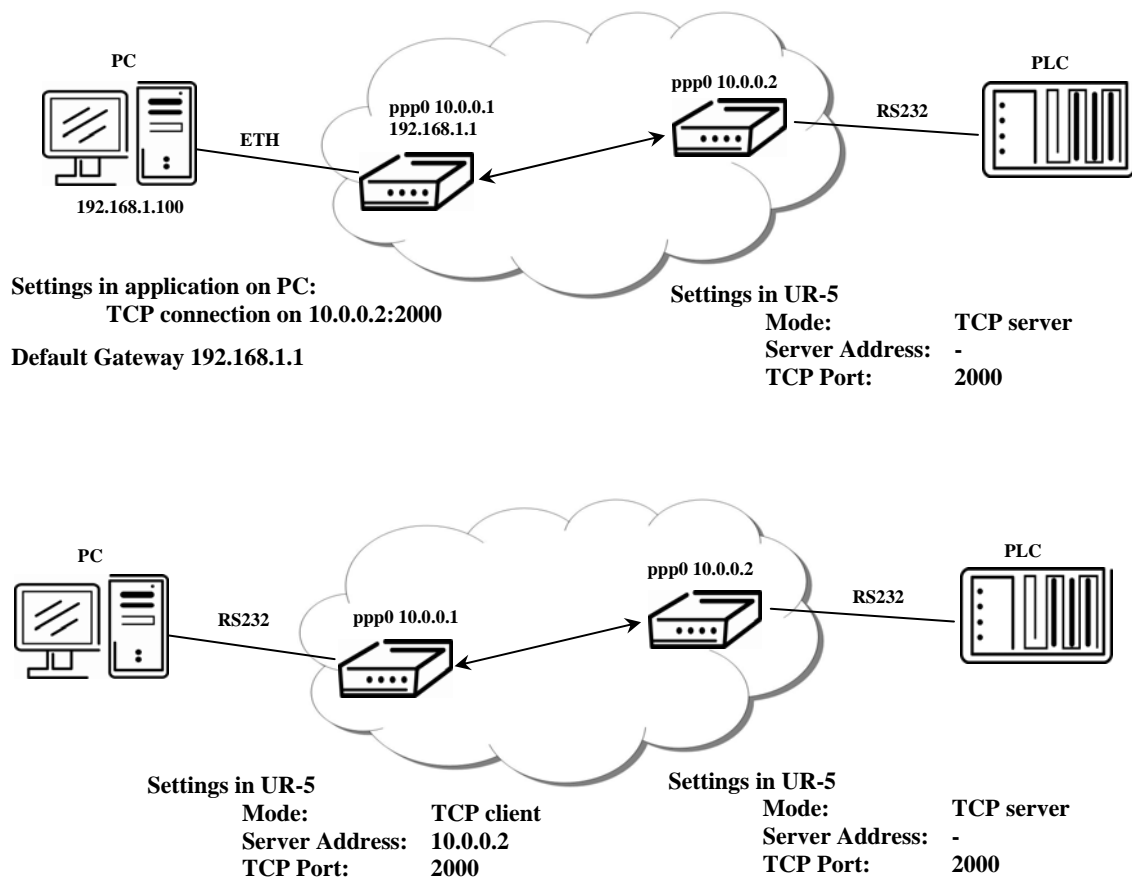
Keepalive Time: 3600 sec

Keepalive Interval: 10 sec

Keepalive Probes: 5

Apply

Example of external port configuration:



5.19. USB Port Configuration

The USB port configuration can be selected by option *USB Port* in menu. Inside the window can be defined baudrate, number of data bits, parity, number of stop bits and mode. Split timeout is for messages.

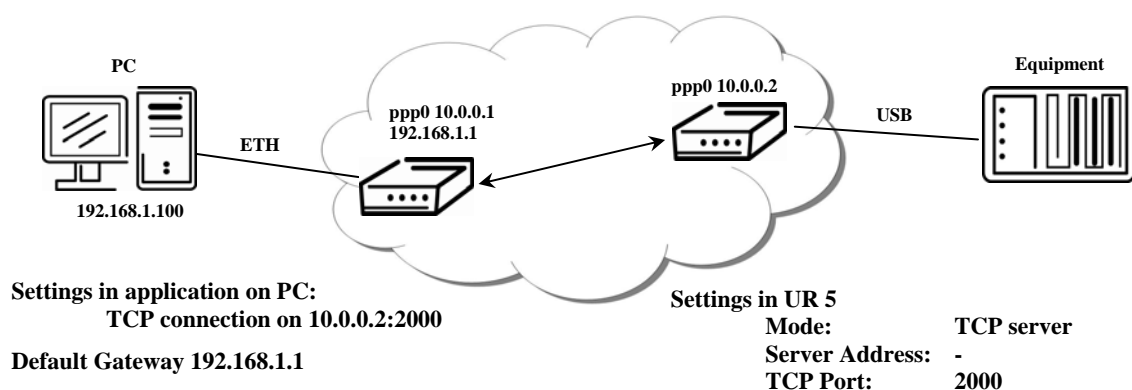
In mode TCP server it is necessary to enter the TCP port, on which the router will listen to incoming requests about TCP connection. In mode TCP client it is necessary to enter the server address and final TCP port.

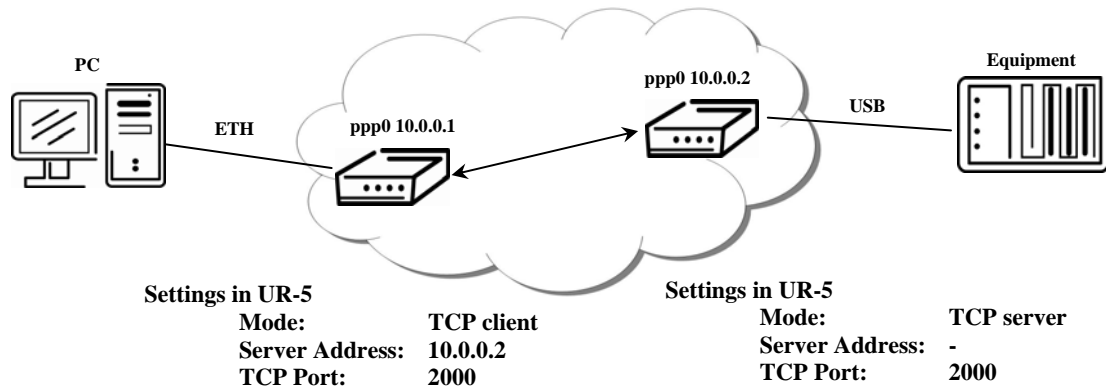
After checking TCP connection it activates verification of coupled TCP connection. Inside the window can be define time, after which it will carry out verification of the connection (*Keepalive Time*), waiting time on answer (*Keepalive Interval*) and number of tests (*Keepalive Probes*).

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

USB Port Configuration	
<input type="checkbox"/> Enable USB serial converter access over TCP	
Baudrate	9600
Data Bits	8
Parity	none
Stop Bits	1
Split Timeout	20 msec
Mode	TCP server
Server Address	
TCP Port	
<input type="checkbox"/> Check TCP connection	
Keepalive Time	3600 sec
Keepalive Interval	10 sec
Keepalive Probes	5
<input type="button" value="Apply"/>	

Example of USB port configuration:





5.20. Startup Script

In the window *Startup Script* it is possible create own scripts which will be executed after all init scripts. This scrip is not stored or restored when using web interface backup or restore option.

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

Startup Script

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

5.21. 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 the basic setting of the UR5 router, the password is set on default form *root*. For higher security of our network we recommend to change this password.

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

5.22. Setting inner o'clock

One - shot setting of the internal clock of the router can done in the call - up option *Set Real Time Clock* item in menu. The clock is set according to the engaged NTP server after pressing the *Apply* button.

Set Real Time Clock	
NTP Server Address	<input type="text"/>
<input type="button" value="Apply"/>	

5.23. Unlock SIM card

Unlocking of the SIM card is possible in the *Unlock SIM Card* item. Unlock is finished after pressing the *Apply* button.

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

5.24. Backup Configuration

The UR 5 configuration is possible to save by help *Backup Configuration* menu item. After clicking on this menu it is possible to check a destination directory, where it will save the UR 5 configuration.

5.25. Restore Configuration

In case, that a restore of the UR 5 configuration is needed, it is possible in *Restore Configuration* menu item to check configuration by help of the *Browse* button.

Restore Configuration	
Configuration File	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Apply"/>	

5.26. Update firmware

To view the information about the firmware version and instructions for its update select the *Update Firmware* menu item. The new firmware will be checked after pressing *Browse* button and update the following pressing the *Update* button.

Update Firmware	
Firmware Version : 1.0.0 (2007-08-03)	
New Firmware <input type="text"/>	<input type="button" value="Browse..."/>
<input type="button" value="Update"/>	

After successful firmware updating the following statement is displayed:

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

Reboot in progress

UR5 with default settings will be available at 192.168.1.1 after reboot.

where it is information about updating of FLASH memory.

After updating firmware it will set the IP address on 192.168.1.1 and all values are in the default state. Total update time lasts for 3 - 4 minutes. During updating of the firmware power supply has to remain permanent. We strongly recommend not to remotely update due to PPP connection, it could damage the router.

5.27. Reboot

To reboot the UR5 router select the *Reboot* menu item and then press the *Reboot* button.

Reboot
The reboot process will take about 10 seconds to complete.
<input type="button" value="Reboot"/>



5.28. Default settings

5.28.1. LAN Configuration

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"/>
<input checked="" type="checkbox"/> Enable DHCP server	
IP Pool Start	<input type="text" value="192.168.1.2"/>
IP Pool End	<input type="text" value="192.168.1.254"/>
<input type="button" value="Apply"/>	

5.28.2. UMTS/GPRS Configuration

UMTS/GPRS Configuration			
<input checked="" type="checkbox"/> Create PPP connection			
	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"/>	
IP Address *	<input type="text"/>	<input type="text"/>	
MRU	<input type="text" value="1500"/>	<input type="text" value="1500"/>	bytes
MTU	<input type="text" value="1500"/>	<input type="text" value="1500"/>	bytes
Operator *	<input type="text"/>	<input type="text"/>	
Network Type	<input type="text" value="automatic selection"/>	<input type="text" value="automatic selection"/>	
<input checked="" type="checkbox"/> Get DNS addresses from operator			
<input type="checkbox"/> Check PPP connection			
Ping IP Address	<input type="text"/>		
Ping Interval	<input type="text"/>		min
Default SIM card	<input type="text" value="primary"/>		
<input type="checkbox"/> Switch to other SIM card when connection fails			
<input type="checkbox"/> Switch to secondary SIM card when roaming is detected			
<input type="checkbox"/> Switch to primary SIM card after timeout			
Initial Timeout	<input type="text" value="60"/>		min
Subsequent Timeout *	<input type="text"/>		min
Additive Constant *	<input type="text"/>		min
* can be blank			
<input type="button" value="Apply"/>			

5.28.3. Firewall Configuration

Firewall Configuration		
<input type="checkbox"/> Allow remote access only from specified hosts		
Source IP Address	Protocol	Target Port *
<input type="text"/>	All	<input type="text"/>
<input type="text"/>	All	<input type="text"/>
<input type="text"/>	All	<input type="text"/>
<input type="text"/>	All	<input type="text"/>
* can be blank		
<input type="button" value="Apply"/>		

5.28.4. NAT Configuration

NAT Configuration			
Public Port	Private Port	Type	Server IP Address
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>

☒ Enable remote HTTP 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

5.28.5. IPsec Tunnel Configuration

IPsec Tunnel Configuration	
<input type="checkbox"/> Create IPsec tunnel	
Remote External IP Address *	<input type="text"/>
Remote Subnet *	<input type="text"/>
Remote Subnet Mask *	<input type="text"/>
Local Subnet *	<input type="text"/>
Local Subnet Mask *	<input type="text"/>
Pre-shared Key	<input type="text"/>
Key Lifetime	<input type="text" value="3600"/> sec
IKE Lifetime	<input type="text" value="3600"/> sec
Rekey Margin	<input type="text" value="540"/> sec
Rekey Fuzz	<input type="text" value="100"/> %
NAT Traversal	<input type="text" value="disabled"/> ▼
* can be blank	

5.28.6. GRE Tunnels Configuration

GRE Tunnels Configuration	
<input type="checkbox"/> Create 1st GRE tunnel	
Remote External IP Address	<input type="text"/>
Remote Subnet	<input type="text"/>
Remote Subnet Mask	<input type="text"/>
Local Internal IP Address *	<input type="text"/>
Remote Internal IP Address *	<input type="text"/>
<input type="checkbox"/> Create 2nd GRE tunnel	
Remote External IP Address	<input type="text"/>
Remote Subnet	<input type="text"/>
Remote Subnet Mask	<input type="text"/>
Local Internal IP Address *	<input type="text"/>
Remote Internal IP Address *	<input type="text"/>
<input type="checkbox"/> Create 3rd GRE tunnel	
Remote External IP Address	<input type="text"/>
Remote Subnet	<input type="text"/>
Remote Subnet Mask	<input type="text"/>
Local Internal IP Address *	<input type="text"/>
Remote Internal IP Address *	<input type="text"/>
<input type="checkbox"/> Create 4th GRE tunnel	
Remote External IP Address	<input type="text"/>
Remote Subnet	<input type="text"/>
Remote Subnet Mask	<input type="text"/>
Local Internal IP Address *	<input type="text"/>
Remote Internal IP Address *	<input type="text"/>
* can be blank	
<input type="button" value="Apply"/>	

5.28.7. L2TP Tunnel Configuration

L2TP Tunnel Configuration	
<input type="checkbox"/> Create L2TP tunnel	
Mode	<input type="text" value="L2TP client"/>
Server IP Address	<input type="text"/>
Client Start IP Address	<input type="text"/>
Client End IP Address	<input type="text"/>
Local IP Address *	<input type="text"/>
Remote IP Address *	<input type="text"/>
Remote Subnet *	<input type="text"/>
Remote Subnet Mask *	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
* can be blank	
<input type="button" value="Apply"/>	

5.28.8. DynDNS Configuration

DynDNS Configuration	
<input type="checkbox"/> Enable DynDNS client	
Hostname	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
<input type="button" value="Apply"/>	

5.28.9. NTP Configuration

NTP Configuration	
<input type="checkbox"/> Synchronize clock with NTP server on power up	
Primary NTP Server Address	<input type="text"/>
Secondary NTP Server Address	<input type="text"/>
<input type="button" value="Apply"/>	

5.28.10. SNMP Configuration

SNMP Configuration	
<input checked="" type="checkbox"/> Enable SNMP agent	
Community	<input type="text" value="public"/>
Contact *	<input type="text"/>
Name *	<input type="text"/>
Location *	<input type="text"/>
* can be blank	
<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="button" value="Apply"/>	

5.28.11. SMS Configuration

SMS Configuration	
<input type="checkbox"/>	Enable remote control via SMS
<input type="checkbox"/>	Send SMS on power up
<input type="checkbox"/>	Send SMS on PPP connect
<input type="checkbox"/>	Send SMS on PPP disconnect
Phone Number 1	<input type="text"/>
Phone Number 2	<input type="text"/>
Phone Number 3	<input type="text"/>
Phone Number 4	<input type="text"/>
Phone Number 5	<input type="text"/>
Unit ID *	<input type="text"/>
<input type="checkbox"/> Enable AT-SMS protocol on external 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"/>	

5.28.12. External Port Configuration

External Port Configuration	
<input type="checkbox"/> Enable external port access over TCP	
Port Type	<input type="text" value="RS-232"/>
Baudrate	<input type="text" value="9600"/>
Data Bits	<input type="text" value="8"/>
Parity	<input type="text" value="none"/>
Stop Bits	<input type="text" value="1"/>
Split Timeout	<input type="text" value="20"/> msec
Mode	<input type="text" value="TCP server"/>
Server Address	<input type="text"/>
TCP Port	<input type="text"/>
<input type="checkbox"/> Check TCP connection	
Keepalive Time	<input type="text" value="3600"/> sec
Keepalive Interval	<input type="text" value="10"/> sec
Keepalive Probes	<input type="text" value="5"/>
<input type="button" value="Apply"/>	

5.28.13. USB Port Configuration

USB Port Configuration	
<input type="checkbox"/> Enable USB serial converter access over TCP	
Baudrate	9600
Data Bits	8
Parity	none
Stop Bits	1
Split Timeout	20 msec
Mode	TCP server
Server Address	
TCP Port	
<input type="checkbox"/> Check TCP connection	
Keepalive Time	3600 sec
Keepalive Interval	10 sec
Keepalive Probes	5
<input type="button" value="Apply"/>	

5.28.14. Startup script

Startup Script
<pre>#!/bin/sh # # This script will be executed *after* all the other init scripts. # You can put your own initialization stuff in here.</pre>
<input type="button" value="Apply"/>

6. Configuration setting over Telnet

Attention! If the SIM card isn't included in the UR 5 router, it is impossible for the UR 5 router to operate. The Included SIM card must be activated for HSDPA/UMTS/EDGE/GPRS transmissions. Insert the SIM card when the UR 5 router is switched off.

Monitoring of status, configuration and administration of the UR 5 router can be performed by means of the Telnet interface. After IP address enters to Telnet interface is possible configure router UR 5 by the help of AT 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 AT 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
free	displaying of informations about memory
gsmat	AT commend send
gsminfo	displaying of informations about signal quality
gsmsms	SMS send
hwclock	displaying/change of time in RTC
ifconfig	displaying/change of interface configuration
ip	displaying/change of route table
iptables	displaying/modification of NetFilter rules
kill	process kill
killall	processes kill
ln	link create
ls	dump of directory contain
mkdir	file create
mv	file move
ntpdate	synchronization of system time with NTP server
passwd	password change
ping	ICMP ping
ps	displaying of processes information
pwd	dump of actual directory
reboot	restart
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



7. Possible problems

On some network cards it is possible to find the situation when it is not possible to connect to the UR5. This problem is possible to solve using the following steps:

- hand by selection communication rates 10 MB/s in property network cards,
- connect UR5 over switch,
- start computer till after finalization start UR5.



8. Reference

[1] Siemens: **HC15_ATC_V01.101 – AT command Set, 2007**



9. FAQ

- I can't get from the internet on equipment, which is connected to the router and I have NAT enabled.
 - *The device's gateway has to be configured as the router UR5.*
- Router resets itself, connection on Ethernet fails.
 - *It is necessary to use an antenna, which needs to be far from the 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 UR5.*
- PPP connection fails.
 - *Check signal power. If signal power is weak, you need to use a better antenna. If the environmental cells have similar signal it will be necessary to use a directive antenna.*
 - *It is necessary to set ping, which checks the connection and in the case of fail ping restart the connection.*
- PPP connection won't be established.
 - *Recheck PPP 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 UR5 it is possible to switch auto negotiation off and set a rate and duplex by hand.*
- DynDNS does not function.
 - *In private APN not functional.*
 - *If there is recorded the same IP address as your canonic name and dynamically assigned address, means that the operator is using NAT or firewall.*
 - *NAT is possible to verify by the help of ping to a random address of your server with a fixed IP address and by the help of the UR5 control address and address in ping.*
 - *Firewall is possible to verify for example by remote access on the web interface.*

- *The operator doesn't give out address DNS servers and without DNS server's is impossible to connect to the server dyndns.org. In log system this message will be displayed:*
 - 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 bad set up routes conditionals of connected equipments or it is bad set up GW.*
- FTP connection.
 - *UR5 doesn't support the active FTP regime, only passive.*
- RS232 don't function.
 - *It is necessary to verify the presence of the RS232 expansion port.*
 - *Verify the presence of the RS232 expansion port in the UR5 configuration in menu „external port“, or verify connection locally by the help Telnet-Hyper terminal.*
- L2TP or IPsec isn't establishing.
 - *Verify the reason in log system.*

10. Customers support

Up to date information about our products is on website:

<http://www.conel.cz/>



Maintenance advice:

It is advisable to handle the SIM-card as is maybe with a credit card. Do not bend, do not scratch it and do not expose it to static electricity.

During cleaning of the modem do not use aggressive chemicals, solvents and abrasive cleaners!

Siemens Company declared that the modem narrated in this user's guide fit all basic demands of directive 1999/5/EC (R&TTE).

Modem fits values of coefficient SAR defined by association ICNIRP and values of "About protection of health before non-ionized radiation".



Declaration about consistency was issue and is possible get it on website <http://www.conel.cz>



11. Guarantee Claim Guidelines

Dear customer,

The product that you have purchased was tested by the manufacturer and, before it was sold, the product's functions were checked once more by our company's technician. However if, in spite of the above-mentioned measures, a breakdown of this product occurs during the guarantee period, which makes proper utilization of the product impossible, we ask you to observe the Guarantee Claim Guidelines when asserting a guarantee claim.

To facilitate the possible guarantee claim procedure, please, when taking over the product, make sure that the seller, who is selling you the product, has properly filled in the relevant parts of the guarantee certificate, including the date of sale, stamp and signature.

This guarantee claim procedure applies to the products that have been purchased. This guarantee claim procedure does not apply to the services that have been provided.

Guarantee periods of products

A guarantee of the purchased device, power supply unit, antenna, data cable, and possible accessories is provided, with a guarantee period of 24 months from the date of sale. The date of sale is at the same time the date of acceptance of the product by the customer.

Lodging a guarantee claim

The guarantee claim must be lodged at the seller from whom the relevant object of the guarantee claim has been purchased. When lodging the guarantee claim, the customer is to submit the properly filled-in guarantee certificate and the complete object of the guarantee claim. The object of the guarantee claim should be submitted in a state corresponding to the state at the sale.

Caution!

The seller does not guarantee that individual settings or data stored in the object of the guarantee claim will be retained.

When lodging the guarantee claim, the customer is obligated to specify the particular defect of the guarantee claim object, possibly its symptoms and, furthermore, the particular right resulting from the liability for defects that he is asserting.

Settling a guarantee claim

Depending on the circumstances, the seller shall ensure the defect removal free of charge; possibly, the seller shall exchange the object of the guarantee claim for a new product or, possibly, settle the guarantee claim in a different way which is in compliance with the Civil Code and with the Consumer Protection Act.

At the moment when the customer has lodged the guarantee claim and the object of the guarantee claim has been accepted by the seller, running of the guarantee period is interrupted. Running of the guarantee period shall continue from the date of acceptance of the repaired object of the guarantee claim or of the exchanged faultless product by the customer or, in the event that neither of the two has been accepted by the customer, from the date when the customer was obligated to accept the repaired object of the guarantee claim or the exchanged product. In the event that a guarantee claim resulting from a defect covered by the guarantee has been lodged and the defective object of the guarantee claim has been exchanged by the seller for a new product (including

the exchange of the IMEI), the ownership of the original object of the guarantee claim is passed hereupon onto the seller, and the ownership of the new product, onto the buyer. A new guarantee period starts running from the date of acceptance of the new product. In the event that the seller, upon agreement with the customer, has settled the guarantee claim by exchanging the object of the guarantee claim for a faultless product, the new guarantee of the product shall expire as follows:

1. After the expiration of a period of 12 months from the date of acceptance of the exchanged product by the customer.
2. On the date when the guarantee period of the original product (the object of the guarantee claim) would have expired if the original product had not been exchanged, whichever is later.
3. The guarantee claim is not justified if the defect being claimed has not been detected by the seller within the framework of the guarantee claim settlement, or if the guarantee does not apply to the defect of the product pursuant to Article 4 of the Guarantee Claim Guidelines.
4. If the defect being claimed has not been detected, and the functional state of the guarantee claim object has been demonstrated to the customer, the customer is obligated to refund the provable expenses incurred in connection with expert assessment of the defect being claimed.
5. If, during the process of assessment of justifiability of the guarantee claim, a defect of the product is detected which is not covered by the guarantee (a repair not covered by the guarantee), the seller shall notify of this fact the customer, and the customer shall notify the seller whether he wants to have this defect removed at a price quoted by the seller. Precise conditions of the repair not covered by the guarantee will be specified in a drawn-up report signed by the customer and seller. If the customer does not require the defect removal by a repair not covered by the guarantee under the conditions communicated by the seller, the device will be returned to the customer, after he has refunded the provable expenses incurred in connection with the expert assessment of the claimed defect.

The guarantee does not apply to the defects caused by the following:

1. Mechanical damage (e.g. by a fall, etc.).
2. Utilization of power supply units and other accessories that are not suitable, possibly, are not recommended for the particular product.
3. Interconnecting the product with non-standard accessories.
4. Installation or utilization of the product in contradiction to the operating instructions, or utilization of the product for purposes that are not usual for this type.
5. Incompetent handling, possibly intervention into the product by an unauthorized person or by a repair shop that has not been authorized by the manufacturer;
6. Damage caused by the natural elements (flooding, fire, etc.) or by other local effects (storm, mains over voltage, etc.).
7. Storage under conditions outside the temperature range.
8. Operation in a chemically aggressive environment.

Other guarantee claim conditions

The fact that the object of the guarantee claim does not correspond to parameters that have been set for other similar types of products can not be considered to be a defect.



GUARANTEE

For the assessment whether a defect has occurred, the product parameters included in the technical documentation of the product are decisive.

The guarantee shall be terminated in the event of any modification of the object of the guarantee claim or in the event that the serial number of the object of the guarantee claim has been damaged or is illegible due to other reasons.

12. Guarantee certificate

Type of the device	
Serial number	
Guarantee period (in months)	
Seller	
Date of sale	
Stamp of the seller	

	1	2	3	4	5
Date of reception of the guarantee claim by the seller					
Number of the guarantee claim report					
Date of reception of the device into the repair shop					
Date of completion of the repair by the repair shop					
Number of the receipt form of the repair shop					
Guarantee repair	YES – NO	YES – NO	YES – NO	YES – NO	YES – NO
New serial number of the device (IMEI)					
Comments					
Stamp of the repair shop					