



HIRSCHMANN

A **BELDEN** BRAND

User Manual

Configuration

Industrial Cellular Router

OWL 3G

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

© 2020 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at:
<https://www.doc.hirschmann.com>

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany

Open Source Information

Open Source Software used in the product

The product contains, among other things, Open Source Software files, as defined below, developed by third parties and licensed under an Open Source Software license. These Open Source Software files are protected by copyright. Your right to use the Open Source Software is governed by the relevant applicable Open Source Software license conditions.

Your compliance with those license conditions will entitle you to use the Open Source Software as foreseen in the relevant license. In the event of conflicts between other Hirschmann Automation and Control GmbH license conditions applicable to the product and the Open Source Software license conditions, the Open Source Software conditions shall prevail. The Open Source Software is provided royalty-free (i.e. no fees are charged for exercising the licensed rights). Open Source Software contained in this product and the respective Open Source Software licenses are stated in the graphical user interface of the software under `Status > General > System Information > Licenses`.

If Open Source Software contained in this product is licensed under GNU General Public License (GPL), GNU Lesser General Public License (LGPL), Mozilla Public License (MPL) or any other Open Source Software license, which requires that source code is to be made available and such source code is not already delivered together with the product, you can order the corresponding source code of the Open Source Software from Hirschmann Automation and Control GmbH - against payment of the shipping and handling charges - for a period of at least 3 years since purchase of the product. Please send your specific request, within 3 years of the purchase date of this product, together with the name and ID number of the product to be found at the label of the product to:

Hirschmann Automation and Control GmbH
Head of R&D
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany

Warranty regarding further use of the Open Source Software

Hirschmann Automation and Control GmbH provides no warranty for the Open Source Software contained in this product, if such Open Source Software is used in any manner other than intended by Hirschmann Automation and Control GmbH. The licenses listed below define the warranty, if any, from the authors or licensors of the Open Source Software. Hirschmann Automation and Control GmbH specifically disclaims any warranty for defects caused by altering any Open Source Software or the product's configuration. Any warranty claims against Hirschmann Automation and Control GmbH in the event that the Open Source Software contained in this product infringes the intellectual property rights of a third party are excluded.

The following disclaimer applies to the GPL and LGPL components in relation to the rights holders:

"This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License and the GNU Lesser General Public License for more details."

For the remaining open source components, the liability exclusions of the rights holders in the respective license texts apply. Technical support, if any, will only be provided for unmodified software.

Used Symbols



Danger – Information regarding user safety.



Note – Problems that can arise in specific situations.



Information – Useful tips or information of special interest.



Example – Example of function, command or script.

Safety Instructions

WARNING

UNCONTROLLED MACHINE ACTIONS

To avoid uncontrolled machine actions caused by data loss, configure all the data transmission devices individually.

Before you start any machine which is controlled via data transmission, be sure to complete the configuration of all the data transmission devices.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Contents

About this Manual	11
1 Basic Information	1
2 Access to the Web Conf.	2
2.1 Certificates and Preventing the Security Message	3
3 Status	4
3.1 General Status	4
3.1.1 Mobile Connection	4
3.1.2 Primary LAN, Secondary LAN	4
3.1.3 System Information	5
3.2 Mobile WAN Status	6
3.3 Network Status	9
3.4 DHCP Status	11
3.5 IPsec Status	12
3.6 DynDNS Status	13
3.7 System Log	14
4 Configuration	16
4.1 LAN Configuration	16
4.1.1 DHCP Server	18
4.1.2 802.1X Authentication to RADIUS Server	19
4.2 VRRP Configuration	25
4.3 Mobile WAN Configuration	28
4.3.1 Connection to Mobile Network	28
4.3.2 DNS Address Configuration	29
4.3.3 Check Connection to Mobile Network Configuration	30
4.3.4 Data Limit Configuration	31
4.3.5 Switch between SIM Cards Configuration	31
4.3.6 PPPoE Bridge Mode Configuration	34
4.4 PPPoE Configuration	37
4.5 Backup Routes	39
4.6 Static Routes	42
4.7 Firewall Configuration	43
4.8 NAT Configuration	47
4.9 OpenVPN Tunnel Configuration	52
4.10 IPsec Tunnel Configuration	57
4.11 GRE Tunnels Configuration	64
4.11.1 Example of the GRE Tunnel Configuration	65
4.12 L2TP Tunnel Configuration	67
4.12.1 Example of the L2TP Tunnel Configuration	68
4.13 PPTP Tunnel Configuration	69
4.13.1 Example of the PPTP Tunnel Configuration	70
4.14 Services	71

4.14.1 DynDNS	71
4.14.2 FTP	72
4.14.3 HTTP	73
4.14.4 NTP	74
4.14.5 PAM	75
4.14.6 SNMP	78
4.14.7 SMTP	82
4.14.8 SMS	84
4.14.9 SSH	92
4.14.10 Syslog	93
4.14.11 Telnet	94
4.15 Scripts	95
4.15.1 Startup Script	95
4.15.2 Up/Down Script	95
4.16 Automatic Update Configuration	97
5 Customization	99
5.1 User Modules	99
6 Administration	101
6.1 Users	101
6.2 Change Profile	102
6.3 Change Password	103
6.4 Set Real Time Clock	103
6.5 Set SMS Service Center Address	104
6.6 Unlock SIM Card	104
6.7 Unblock SIM Card	105
6.8 Send SMS	106
6.9 Backup Configuration	107
6.10 Restore Configuration	108
6.11 Update Firmware	109
6.12 Reboot	111
6.13 Logout	111
A Maintenance	112
B Glossary and Acronyms	113
C Index	117
D Recommended Literature	119
E Further support	120

List of Figures

1	Example of the Web Configuration	2
2	Mobile WAN status	8
3	Network Status	10
4	DHCP Status	11
5	IPsec Status	12
6	DynDNS Status	13
7	System Log	14
8	Example program syslogd start with the parameter -R	15
9	Example 1 – Network Topology for Dynamic DHCP Server	19
10	Example 1 – LAN Configuration Page	20
11	Example 2 – Network Topology with both Static and Dynamic DHCP Servers	21
12	Example 2 – LAN Configuration Page	22
13	Example 3 – Network Topology	23
14	Example 3 – LAN Configuration Page	24
15	Topology of VRRP configuration example	26
16	Example of VRRP configuration – main router	26
17	Example of VRRP configuration – backup router	27
18	Mobile WAN Configuration	35
19	Example 1 – Mobile WAN Configuration	36
20	Example 2 – Mobile WAN Configuration	36
21	PPPoE configuration	37
22	Backup Routes Configuration	39
23	Static Routes Configuration	42
24	Firewall Configuration	45
25	Topology for the Firewall Configuration Example	46
26	Firewall Configuration Example	46
27	Example 1 – Topology of NAT Configuration	48
28	Example 1 – NAT Configuration	49
29	Example 2 – Topology of NAT Configuration	50
30	Example 2 – NAT Configuration	51
31	OpenVPN tunnel configuration	55
32	Topology of OpenVPN Configuration Example	56
33	IPsec Tunnels Configuration	62
34	Topology of IPsec Configuration Example	63
35	GRE Tunnel Configuration	65
36	Topology of GRE Tunnel Configuration Example	65
37	L2TP Tunnel Configuration	67
38	Topology of L2TP Tunnel Configuration Example	68
39	PPTP Tunnel Configuration	69
40	Topology of PPTP Tunnel Configuration Example	70
41	Enabling of FTP server	72
42	Configuration of HTTP and HTTPS services	73
43	Example of NTP Configuration	74
44	Configuration of RADIUS	75
45	Configuration of TACACS+	76
46	OID Basic Structure	79
47	SNMP Configuration Example	80

48	MIB Browser Example	81
49	SMTP Client Configuration Example	82
50	Example 1 – SMS Configuration	89
51	Example 2 – SMS Configuration	90
52	Example 3 – SMS Configuration	91
53	Configuration of HTTP service	92
54	Syslog configuration	93
55	Enabling of Telnet service	94
56	Example of a Startup Script	95
57	Example of Up/Down Script	96
58	User modules	99
59	Added user module	99
60	Users	102
61	Change Profile	102
62	Change Password	103
63	Set Real Time Clock	103
64	Set SMS Service Center Address	104
65	Unlock SIM Card	104
66	Unblock SIM Card	105
67	Send SMS	106
68	Backup Configuration	107
69	Restore Configuration	108
70	Update Firmware Administration Page	109
71	Process of Firmware Update	110
72	Reboot	111

List of Tables

1	Mobile Connection	4
2	System Information	5
3	Mobile Network Information	6
4	Value ranges of signal strength for different technologies.	7
5	Description of Periods	7
6	Mobile Network Statistics	7
7	Description of Interfaces in Network Status	9
8	Description of Information in Network Status	9
9	DHCP Status Description	11
10	Configuration of the Network Interface	17
11	Configuration of Dynamic DHCP Server	18
12	Configuration of Static DHCP Server	18
13	Configuration of 802.1X Authentication	19
14	VRRP configuration	25
15	Check connection	26
16	Mobile WAN Connection Configuration	29
17	Check Connection to Mobile Network Configuration	30
18	Data Limit Configuration	31
19	Switch between SIM cards configuration	32
20	Parameters for SIM card switching	33
21	PPPoE configuration	38
22	Backup Routes Configuration	40
23	Backup Routes	40
24	Static Routes configuration	42
25	Filtering of Incoming Packets	43
26	Forwarding filtering	44
27	NAT Configuration	47
28	Configuration of send all incoming packets	47
29	Remote Access Configuration	48
30	OpenVPN Configuration	54
31	OpenVPN Configuration Example	56
32	IPsec Tunnel Configuration	60
33	Example IPsec configuration	63
34	GRE Tunnel Configuration	64
35	GRE Tunnel Configuration Example	66
36	L2TP Tunnel Configuration	67
37	L2TP Tunnel Configuration Example	68
38	PPTP Tunnel Configuration	69
39	PPTP Tunnel Configuration Example	70
40	DynDNS Configuration	71
41	Parameters for HTTP and HTTPS services configuration	73
42	NTP Configuration	74
43	Available Modes of PAM	75
44	Configuration of RADIUS	76
45	Configuration of TACACS+	77
46	SNMP Agent Configuration	78
47	SNMPv3 Configuration	78

48	SNMP Configuration (R-SeeNet)	79
49	SMTP client configuration	82
50	SMS Configuration	84
51	Control via SMS	85
52	Control SMS	86
53	Send SMS on ethernet PORT1 configuration	86
54	List of AT Commands	88
55	Parameters for SSH service configuration	92
56	Syslog configuration	93
57	Automatic Update Configuration	97
58	User modules	100
59	Users Overview	101
60	Add User	101

About this Manual

This "Configuration" user manual contains the information you need to start operating the device. It takes you step by step from the first startup operation through to the basic settings for operation in your environment.

1 Basic Information

The OWL 3G Industrial Cellular Router is designed for wireless communication in mobile networks using HSPA+, UMTS, EDGE or GPRS technology. Due to the high speed of data transfer up to 14.4 Mbit/s (download) and up to 5.76 Mbit/s (upload). The router is an ideal wireless solution for connecting the data stream of security camera systems, individual computers, LANs, automatic teller machines (ATM), and other self-service terminals.

You can configure the router using either a web browser or Secure Shell (SSH). The Hirschmann Automation and Control GmbH Technical Support also uses the Secure Shell to help you locate problems with your device. Configuring the functions in the router using a web browser is described in this Configuration Manual. You can find the technical parameters of your router in UM-Installation Manual.

The graphical user interface (GUI) is password protected. After logging in, the GUI provides detailed statistics about the router activities, signal strength, and a detailed system log. You can also create VPN tunnels using IPSec, OpenVPN and L2TP for secure communications.

The router also supports the following functions.

- DHCP
- NAT
- DynDNS
- NTP
- VRRP
- Control using SMS
- primary/backup connection

Diagnostic functions, which provide for continuous communication, include an automatic inspection of a PPP connection, offering an automatic restart feature in case of an unexpected termination of the connection. Another diagnostic function is the hardware watchdog, which monitors the status of the router.

Diagnostic functions, which provide for continuous communication, include an automatic inspection of a PPP connection, offering an automatic restart feature in case of an unexpected termination of the connection. Another diagnostic function is the hardware watchdog, which monitors the status of the router.

2 Access to the Web Configuration

Wireless transmissions work only when you activate the SIM card for data traffic and insert it into the router. Remove the power source before inserting the SIM card.



You may use the web interface to monitor, configure and manage the router. To do so, enter the router's IP address in your browser. The default address is 192.168.1.1. Only access via secured **HTTPS** protocol is permitted. So the syntax for the IP address must be `https://192.168.1.1`. When accessing the router for the first time you will need to install a security certificate if you don't want the browser to show you a domain disagreement message. To avoid receiving domain disagreement messages, follow the procedure described in the following subchapter.

The default username is **admin**. The default password is printed on the router's label.

For increased security of the network connected to the router, change the default router password. When the default password of the router is still active, the **Change password** title is highlighted in red.



After three unsuccessful login attempts, any HTTP(S) access from an IP address is blocked for one minute.



Status	General Status
General	Mobile Connection
Mobile WAN	SIM Card : 1st
Network	IP Address : 10.80.0.48
DHCP	IPv6 Address : Unassigned
IPsec	Rx Data : 580 B
DynDNS	Tx Data : 843 B
System Log	Uptime : 0 days, 15 hours, 0 minutes
Configuration	Primary LAN
LAN	IP Address : 10.64.0.54 / 255.255.252.0
VRRP	IPv6 Address : fd00:a40:54 / 56
Mobile WAN	MAC Address : 02:AD:FF:00:00:54
PPPoE	Rx Data : 75.5 KB
Backup Routes	Tx Data : 252.9 KB
Static Routes	Secondary LAN
Firewall	IP Address : 10.65.0.54 / 255.255.252.0
NAT	IPv6 Address : fd00:a41:54 / 56
OpenVPN	MAC Address : 02:AD:FF:01:00:54
IPsec	Rx Data : 30.9 KB
GRE	Tx Data : 680 B
L2TP	Peripheral Ports
PPTP	Expansion Port 1 : RS-232
Services	Expansion Port 2 : RS-485
Expansion Port 1	Binary Input 0 : Off
Expansion Port 2	Binary Input 1 : Off
USB Port	Binary Output : On
Scripts	System Information
Automatic Update	Firmware Version : XXX(YYYY-MM-DD)
Customization	Serial Number : AC21199000000546
User Modules	Profile : Standard
Administration	RTC Battery : Ok
Users	Supply Voltage : 24.0 V
Change Profile	Temperature : 42.0 C
Change Password	Time : 2019-08-20 14:23:18
Set Real Time Clock	Uptime : 0 days, 15 hours, 0 minutes
Set SMS Service Center	Licenses
Unlock SIM Card	
Unlock SIM Card	
Send SMS	
Backup Configuration	
Restore Configuration	
Update Firmware	
Reboot	
Logout	

Figure 1: Example of the Web Configuration

When you successfully enter login information on the login page, web interface will be displayed. The left side of the web interface contains a menu tree with sections for monitoring (*Status*), configuration (*Configuration*), customization (*Customization*) and administration (Administration) of the router.

Name and *Location* items in the right upper corner display the name and location of the router in the SNMP configuration (see 4.14.6). These fields are user-defined for each router.

After the green LED starts to blink you may restore the initial router settings by pressing the reset (*RST*) button on the back panel. If the reset button is pressed, all configuration will revert to factory defaults and the router will reboot (the green LED will be on during the reboot).

2.1 Certificates and Preventing the Security Message

There is the self-signed HTTPS certificate in the router. Because the identity of this certificate cannot be validated, a message can appear in the web browser. To solve this, upload your own certificate, signed by Certification Authority, to the router. If you want to use your own certificate (e.g. in combination with the dynamic DNS service), you need to replace the `/etc/certs/https_cert` and `/etc/certs/https_key` files in the router. This can be done easily in the GUI on *HTTP* configuration page, see chapter 4.14.3.



HTTPS certificate creation in the router was updated since FW 5.3.5 to be more secure. Existing HTTPS certificates on already manufactured routers will not be automatically upgraded with the firmware upgrade! You can upgrade HTTPS certificate or upload your own certificate, for more information see chapter 4.14.3.

If you decide to use the self-signed certificate in the router to prevent the security message (domain disagreement) from pop up every time you log into the router, you can take the following steps:

Note: You will have to use the domain name based on the MAC address of the router and it is not guaranteed to work with every combination of an operating system and a browser.

- Add the DNS record to your [DNS](#) system: Edit `/etc/hosts` (Linux/Unix OS) or `C:\WINDOWS\system32\drivers\etc\hosts` (Windows OS) or configure your own DNS server. Add a new record with the IP address of your router and the domain name based of the MAC address of the router (MAC address of the first network interface seen in *Network Status* in the Web interface of the router.) Use dash separators instead of colons. Example: A router with the MAC address 00:11:22:33:44:55 will have a domain name 00-11-22-33-44-55.
- Access the router via the new domain name address (E.g. `https://00-11-22-33-44-55`). If you see the security message, add an exception so the next time the message will not pop up (E.g. in Firefox Web browser). If there is no possibility to add an exception, export the certificate to the file and import it to your browser or operating system.

3 Status

3.1 General Status

You can access a summary of basic router information and its activities by opening the *General* page. This page is the default dialog displayed when you login to the device. Information is divided into several sections, based upon the type of router activity or the properties area: *Mobile Connection*, *Primary LAN*, *Secondary LAN* and *System Information*.

3.1.1 Mobile Connection

Item	Description
SIM Card	Identification of the SIM card
Interface	Defines the interface
Flags	Displays network interface flags
IP Address	IP address of the interface
MTU	Maximum packet size that the equipment is able to transmit
Rx Data	Total number of received bytes
Rx Packets	Received packets
Rx Errors	Erroneous received packets
Rx Dropped	Dropped received packets
Rx Overruns	Lost received packets because of overload
Tx Data	Total number of sent bytes
Tx Packets	Sent packets
Tx Errors	Erroneous sent packets
Tx Dropped	Dropped sent packets
Tx Overruns	Lost sent packets because of overload
Uptime	Indicates how long the connection to the cellular network has been established

Table 1: Mobile Connection

3.1.2 Primary LAN, Secondary LAN

Items displayed in this part have the same meaning as items in the previous part. Moreover, the *MAC Address* item shows the MAC address of the corresponding router's interface (*Primary LAN – eth0*, *Secondary LAN – eth1*).

3.1.3 System Information

Item	Description
Firmware Version	Information about the firmware version
Serial Number	Serial number of the router (in case of <i>N/A</i> is not available)
Profile	Current profile – standard or alternative profiles (profiles are used for example to switch between different modes of operation)
Supply Voltage	Supply voltage of the router
Temperature	Temperature in the router
Time	Current date and time
Uptime	Indicates how long the router is used
Licenses	Link to the list of open source software components of the firmware together with their complete license texts (GPL versions 2 and 3, LGPL version 2, BSD-style licenses, MIT-style licenses).

Table 2: System Information

3.2 Mobile WAN Status

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

Item	Description
Registration	State of the network registration.
Operator	Specifies the operator's network the router operates in.
Technology	Transmission technology.
PLMN	Code of operator
Cell	Cell the router is connected to.
LAC	Location Area Code – unique number assigned to each location area.
Channel	Channel the router communicates on. <ul style="list-style-type: none"> • ARFCN in case of GPRS/EDGE technology, • UARFCN in case of UMTS/HSPA technology, • EARFCN in case of LTE technology.
Signal Strength	Signal strength of the selected cell, for details see the Table 4.
Signal Quality	Signal quality of the selected cell: <ul style="list-style-type: none"> • EC/IO for UMTS and CDMA (it's the ratio of the signal received from the pilot channel – EC – to the overall level of the spectral density, ie the sum of the signals of other cells – IO). • RSRQ for LTE technology (Defined as the ratio $\frac{N \times RSRP}{RSSI}$). • The value is not available for the EDGE technology.
CSQ	Cell Signal Quality, relative value is given by RSSI (dBm). 2–9 range means Marginal, 10–14 range means OK, 15–16 range means Good, 20–30 range means excellent.
Manufacturer	Module manufacturer
Model	Type of module
Revision	Revision of module
IMEI	IMEI (International Mobile Equipment Identity) number of module
ICCID	Integrated Circuit Card Identifier is international and unique serial number of the SIM card.

Table 3: Mobile Network Information

The value of signal strength is displayed in different color: in black for good, in orange for fair and in red for poor signal strength.

Signal strength	GPRS/EDGE/CDMA (RSSI)	UMTS/HSPA (RSCP)	LTE (RSRP)
good	> -70 dBm	> -75 dBm	> -90 dBm
fair	-70 dBm to -89 dBm	-75 dBm to -94 dBm	-90 dBm to -109 dBm
poor	< -89 dBm	< -94 dBm	< -109 dBm

Table 4: Value ranges of signal strength for different technologies.

The middle part of this page displays information about mobile signal quality, transferred data and number of connections for all the SIM cards (for each period). The router has standard intervals, such as the previous 24 hours and last week, and also period starting with *Accounting Start* defined for the MWAN module.

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

Table 5: Description of Periods

Item	Description
RX data	Total volume of received data
TX data	Total volume of sent data
Connections	Number of connection to mobile network establishment
Signal Min	Minimal signal strength
Signal Avg	Average signal strength
Signal Max	Maximal signal strength
Cells	Number of switch between cells
Availability	Availability of the router via the mobile network (expressed as a percentage)

Table 6: Mobile Network Statistics



Tips for *Mobile Network Statistics* table:

- *Availability* is expressed as a percentage. It is the ratio of time connection to the mobile network has been established to the time that router has been is turned on.
- Placing your cursor over the maximum or minimum signal strength will display the last time the router reached that signal strength.

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

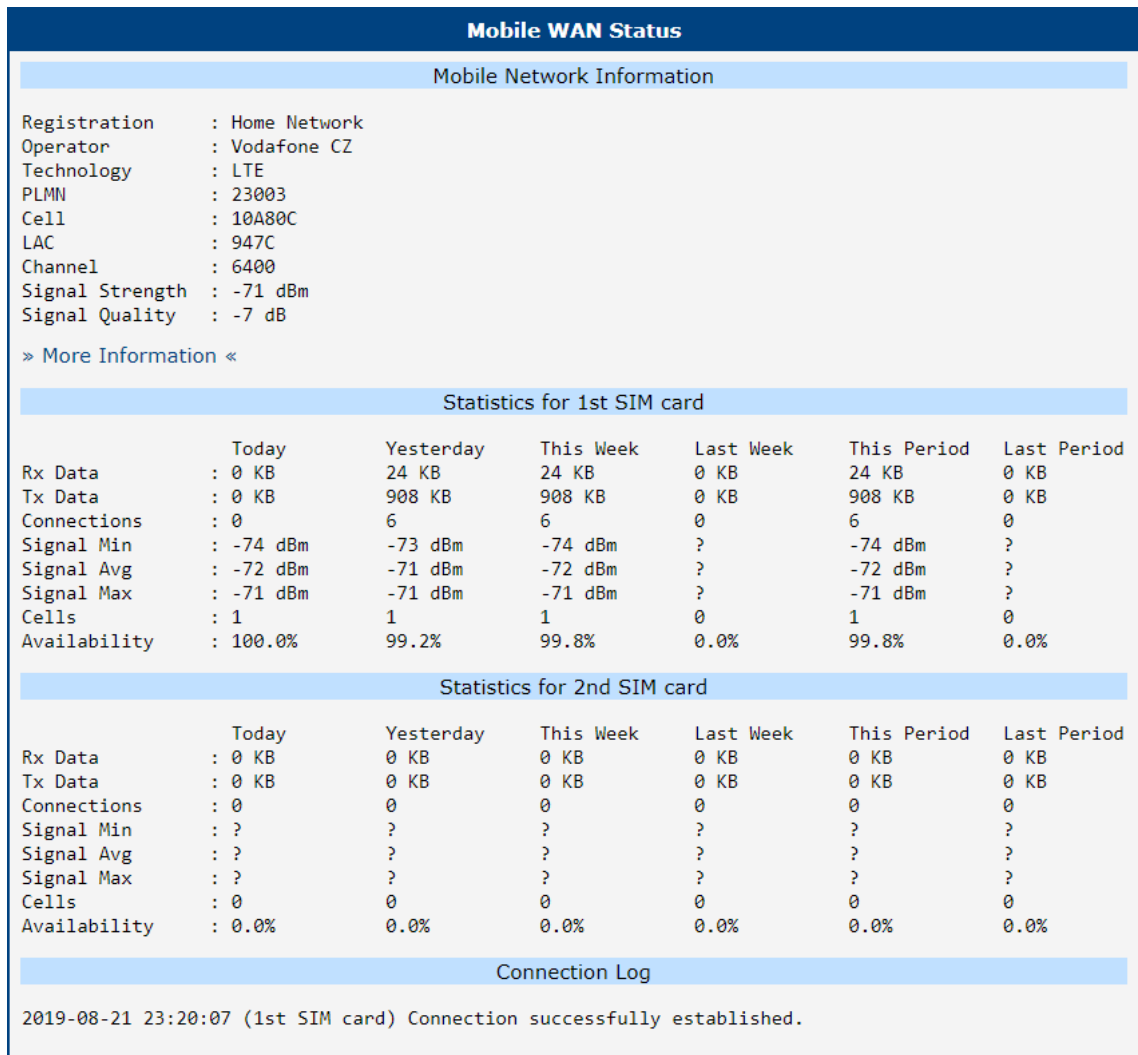


Figure 2: Mobile WAN status

3.3 Network Status

To view information about the interfaces and the routing table, open the *Network* item in the *Status* menu. The upper part of the window displays detailed information about the active interfaces only:

Interface	Description
eth0, eth1	Network interfaces (Ethernet connection)
lo	Local loopback interface
ppp0	Active PPP connection to the mobile network – wireless module is connected via USB interface

Table 7: Description of Interfaces in Network Status

Each of the interfaces displays the following information:

Item	Description
HWaddr	Hardware (unique) address of networks interface
inet	IP address of interface
P-t-P	IP address second ends connection
Bcast	Broadcast address
Mask	Mask of network
MTU	Maximum packet size that the equipment is able to transmit
Metric	Number of routers, over which packet must go trough
RX	packets – received packets errors – number of errors dropped – dropped packets overruns – incoming packets lost because of overload frame – wrong incoming packets because of incorrect packet size
TX	packets – transmit packets errors – number of errors dropped – dropped packets overruns – outgoing packets lost because of overload carrier – wrong outgoing packets with errors resulting from the physical layer
collisions	Number of collisions on physical layer
txqueuelen	Length of front network device
RX bytes	Total number of received bytes
TX bytes	Total number of transmitted bytes

Table 8: Description of Information in Network Status

You may view the status of the mobile network connection on the network status screen. If the connection to the mobile network is active, it will appear in the system information as an usb0 interface. The Route Table is displayed at the bottom.

Network Status							
Interfaces							
eth0	Link encap:Ethernet HWaddr 02:AD:FF:00:00:80 inet addr:10.64.0.80 Bcast:10.64.3.255 Mask:255.255.252.0 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:1868 errors:0 dropped:0 overruns:0 frame:0 TX packets:1290 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:251284 (245.3 KB) TX bytes:438023 (427.7 KB) Interrupt:39 Base address:0x8000						
eth1	Link encap:Ethernet HWaddr 02:AD:FF:01:00:80 inet addr:10.65.0.80 Bcast:10.65.3.255 Mask:255.255.252.0 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:429 errors:0 dropped:0 overruns:0 frame:0 TX packets:3 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:113418 (110.7 KB) TX bytes:182 (182.0 B) Interrupt:66						
lo	Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 UP LOOPBACK RUNNING MTU:65536 Metric:1 RX packets:0 errors:0 dropped:0 overruns:0 frame:0 TX packets:0 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)						
ppp0	Link encap:Point-to-Point Protocol inet addr:10.185.214.91 P-t-P:192.168.254.254 Mask:255.255.255.255 UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1 RX packets:7 errors:0 dropped:0 overruns:0 frame:0 TX packets:7 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:3 RX bytes:232 (232.0 B) TX bytes:240 (240.0 B)						
Route Table							
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.254.254	0.0.0.0	UG	0	0	0	ppp0
10.64.0.0	0.0.0.0	255.255.252.0	U	0	0	0	eth0
10.65.0.0	0.0.0.0	255.255.252.0	U	0	0	0	eth1
192.168.254.254	0.0.0.0	255.255.255.255	UH	0	0	0	ppp0

Figure 3: Network Status

3.4 DHCP Status

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

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

Item	Description
lease	Assigned IP address
starts	Time that the IP address was assigned
ends	Time that the IP address lease expires
hardware ethernet	Unique hardware MAC address
uid	Unique ID
client-hostname	Host computer name

Table 9: DHCP Status Description



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

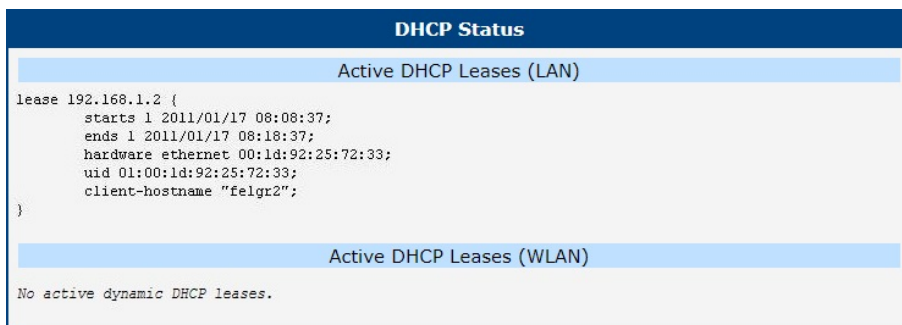
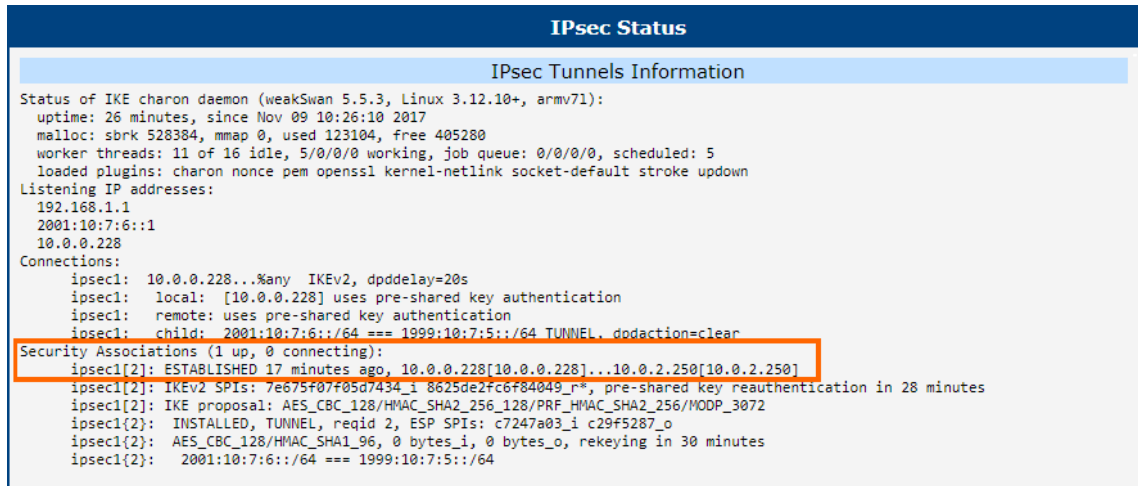


Figure 4: DHCP Status

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

3.5 IPsec Status

Selecting the *IPsec* option in the *Status* menu of the web page will bring up the information for any IPsec Tunnels that have been established. If the tunnel has been built correctly, the screen will display **ESTABLISHED** and the number of running IPsec connections **1 up** (orange highlighted in the figure below.) If there is no such text in log (e.g. "0 up"), the tunnel was not created!



```
IPsec Status
IPsec Tunnels Information
Status of IKE charon daemon (weakSwan 5.5.3, Linux 3.12.10+, armv7l):
  uptime: 26 minutes, since Nov 09 10:26:10 2017
  malloc: sbrk 528384, mmap 0, used 123104, free 405280
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 5
  loaded plugins: charon nonce pem openssl kernel-netlink socket-default stroke updown
Listening IP addresses:
  192.168.1.1
  2001:10:7:6::1
  10.0.0.228
Connections:
  ipsec1: 10.0.0.228...%any IKEv2, dpddelay=20s
  ipsec1: local: [10.0.0.228] uses pre-shared key authentication
  ipsec1: remote: uses pre-shared key authentication
  ipsec1: child: 2001:10:7:6::/64 === 1999:10:7:5::/64 TUNNEL, dpdaction=clear
Security Associations (1 up, 0 connecting):
ipsec1[2]: ESTABLISHED 17 minutes ago, 10.0.0.228[10.0.0.228]...10.0.2.250[10.0.2.250]
ipsec1[2]: IKEv2 SPIs: 7e675f07f05d7434_i 8625de2fc6f84049_r*, pre-shared key reauthentication in 28 minutes
ipsec1[2]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MDP_3072
ipsec1[2]: INSTALLED, TUNNEL, reqid 2, ESP SPIs: c7247a03_i c29f5287_o
ipsec1{2}: AES_CBC_128/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 30 minutes
ipsec1{2}: 2001:10:7:6::/64 === 1999:10:7:5::/64
```

Figure 5: IPsec Status

3.6 DynDNS Status

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

 You can use the following servers for the Dynamic DNS service:

- www.dyndns.org
- www.spdns.de
- www.dnsdynamic.org
- www.noip.com



Figure 6: DynDNS Status

When the router detects a DynDNS record update, the dialog displays one or more of the following messages:

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



The router's SIM card must have public IP address assigned or DynDNS will not function correctly.

3.7 System Log

If there are any connection problems you may view the system log by selecting the *System Log* menu item. Detailed reports from individual applications running in the router will be displayed. Use the *Save Log* button to save the system log to a connected computer. (It will be saved as a text file with the .log extension.) The *Save Report* button is used for creating detailed reports. (It will be saved as a text file with the .txt extension. The file will include statistical data, routing and process tables, system log, and configuration.)

Sensitive data from the report are filtered out for security reasons.



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

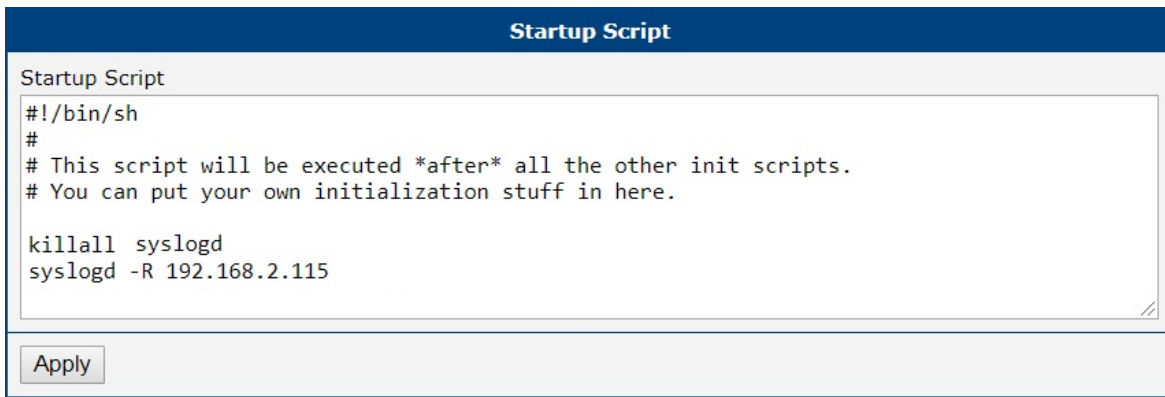
The *Syslogd* program will output the system log. It can be started with two options to modify its behavior. Option "-S" followed by decimal number sets the maximal number of lines in one log file. Option "-R" followed by hostname or IP address enables logging to a remote syslog daemon. (If the remote syslog daemon is Linux OS, there has to be remote logging enabled (typically running "*syslogd -R*"). If it's the Windows OS, there has to be syslog server installed, e.g. *Syslog Watcher*). To start *syslogd* with these options, the `"/etc/init.d/syslog"` script can be modified via SSH or lines can be added into *Startup Script* (accessible in *Configuration* section) according to figure 8.

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

Save Log Save Report

Figure 7: System Log

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



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

killall syslogd
syslogd -R 192.168.2.115
```

Figure 8: Example program syslogd start with the parameter -R

4 Configuration

4.1 LAN Configuration

To enter the Local Area Network configuration, select the *LAN* menu item in the *Configuration* section. The *Primary LAN* subitem is for the router's main Ethernet interface (ETH). If the router has additional Ethernet ports (*PORT1* or *PORT2*), they are configured using the *Secondary LAN* subitem. For routers with two additional Ethernet ports, *PORT1* and *PORT2* are automatically bridged together.

Item	Description
DHCP Client	Enables/disables the DHCP client function. <ul style="list-style-type: none"> • disabled – The router does not allow automatic allocation IP address from a DHCP server in LAN network. • enabled – The router allows automatic allocation IP address from a DHCP server in LAN network.
IP address	Specifies a fixed set of IP addresses for the network interfaces ETH.
Subnet Mask	Specifies a Subnet Mask for the IP address.
Default Gateway	Specifies the IP address of default gateway. When entering the IP address of default gateway, every packet for which the destination IP address was not found in the routing table, is sent to this IP address.
DNS server	Specifies the IP address of the DNS server. When the IP address is not found the Routing Table, the router forwards an IP address requests to the DNS server.
Bridged	Activates/deactivates the bridging function on the router. <ul style="list-style-type: none"> • no – The bridging function is inactive (default). • yes – The bridging function is active.

Continued on next page

Continued from previous page

Item	Description
Media type	<p>Specifies the type of duplex and speed used in the network.</p> <ul style="list-style-type: none"> ● Auto-negotiation – The router automatically sets the best speed and duplex mode of communication according to the network's possibilities. ● 100 Mbps Full Duplex – The router communicates at 100Mbps, in the full duplex mode. ● 100 Mbps Half Duplex – The router communicates at 100Mbps, in the half duplex mode. ● 10 Mbps Full Duplex – The router communicates at 10Mbps, in the full duplex mode. ● 10 Mbps Half Duplex – The router communicates at 10Mbps, in the half duplex mode.

Table 10: Configuration of the Network Interface



The router considers the last address in the network range to be broadcast address, regardless of the address is set as a broadcast or not. Connection (ping) to the broadcast address does not work.

The *Default Gateway* and *DNS Server* items are only used if the *DHCP Client* item is set to *disabled* and if the Primary or Secondary LAN is selected by the Backup Routes system as the default route. (The selection algorithm is described in section 4.5). Since FW 5.3.0, *Default Gateway* and *DNS Server* are also supported on bridged interfaces (e.g. eth0 + eth1).

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

4.1.1 DHCP Server

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

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

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

Table 11: Configuration of Dynamic DHCP Server

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

Table 12: Configuration of Static DHCP Server

Do not to overlap ranges of static allocated IP addresses with addresses allocated by the dynamic DHCP server. IP address conflicts and incorrect network function can occur if you overlap the ranges.



4.1.2 802.1X Authentication to RADIUS Server

Authentication (802.1X) to RADIUS server can be enabled in next configuration section. The router can be RADIUS client only (not the server). This functionality requires additional setting of identity and certificates as described in the following table.

Item	Description
Enable IEEE 802.1X Authentication	Select this option to enable 802.1X Authentication.
Authentication Method	Select authentication method (EAP-PEAPMSCHAPv2 or EAP-TLS).
CA Certificate	Definition of CA certificate for EAP-TLS authentication protocol.
Local Certificate	Definition of local certificate for EAP-TLS authentication protocol.
Local Private Key	Definition of local private key for EAP-TLS authentication protocol.
Identity	User name – identity.
Password	Access password. This item is available for EAP-PEAPMSCHAPv2 protocol only. Enter valid characters only.
Local Private Key Password	Definition of password for private key of EAP-TLS protocol. This item is available for EAP-TLS protocol only. Enter valid characters only.

Table 13: Configuration of 802.1X Authentication

Example 1: Configure the network interface to connect to a dynamic DHCP server:

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

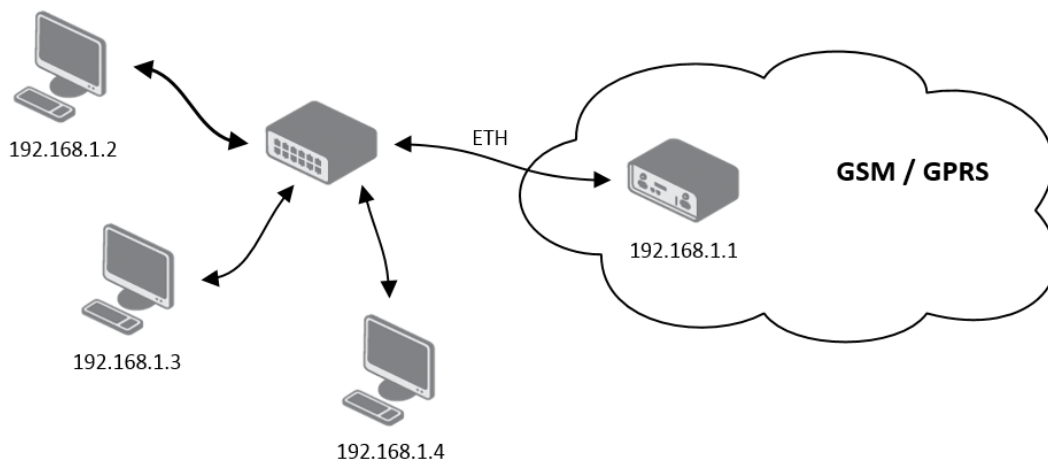


Figure 9: Example 1 – Network Topology for Dynamic DHCP Server

Primary LAN Configuration	
DHCP Client	<input type="text" value="disabled"/>
IP Address	<input type="text" value="192.168.1.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text"/>
DNS Server	<input type="text"/>
Bridged	<input type="text" value="no"/>
Media Type	<input type="text" value="auto-negotiation"/>
<input checked="" type="checkbox"/> Enable dynamic DHCP leases	
IP Pool Start	<input type="text" value="192.168.1.2"/>
IP Pool End	<input type="text" value="192.168.1.4"/>
Lease Time	<input type="text" value="600"/> sec
<input type="checkbox"/> Enable static DHCP leases	
MAC Address	IP Address
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="checkbox"/> Enable IEEE 802.1X Authentication	
Authentication Method	<input type="text" value="EAP-PEAP/MSCHAPv2"/>
CA Certificate	<input type="text"/>
	<input type="button" value="Choose File"/> No file chosen
Local Certificate	<input type="text"/>
	<input type="button" value="Choose File"/> No file chosen
Local Private Key	<input type="text"/>
	<input type="button" value="Choose File"/> No file chosen
Identity	<input type="text"/>
Password	<input type="text"/>
<input type="button" value="Apply"/>	

Figure 10: Example 1 – LAN Configuration Page

Example 2: Configure the network interface to connect to a dynamic and static DHCP server:

- The range of allocated addresses is from 192.168.1.2 to 192.168.1.4.
- The address is allocated for 600 seconds (10 minutes).
- The client with the MAC address 01:23:45:67:89:ab has the IP address 192.168.1.10.
- The client with the MAC address 01:54:68:18:ba:7e has the IP address 192.168.1.11.

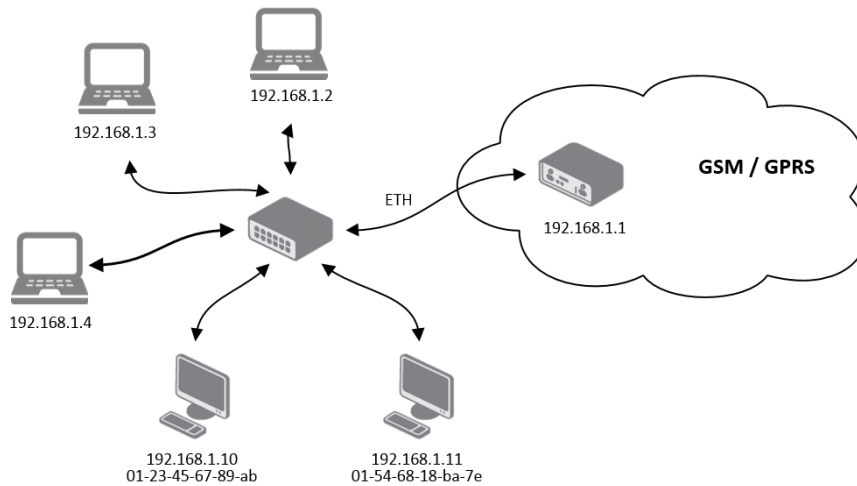


Figure 11: Example 2 – Network Topology with both Static and Dynamic DHCP Servers

Primary LAN Configuration	
DHCP Client	disabled
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	
DNS Server	
Bridged	no
Media Type	auto-negotiation
<input checked="" type="checkbox"/> Enable dynamic DHCP leases	
IP Pool Start	192.168.1.2
IP Pool End	192.168.1.4
Lease Time	600 sec
<input checked="" type="checkbox"/> Enable static DHCP leases	
MAC Address	IP Address
01:23:45:67:89:ab	192.168.1.10
01:54:68:18:ba:7e	192.168.1.11
<input type="checkbox"/> Enable IEEE 802.1X Authentication	
Authentication Method	EAP-TLS
CA Certificate	<input type="text"/>
	<input type="button" value="Choose File"/> No file chosen
Local Certificate	<input type="text"/>
	<input type="button" value="Choose File"/> No file chosen
Local Private Key	<input type="text"/>
	<input type="button" value="Choose File"/> No file chosen
Identity	<input type="text"/>
Password	<input type="text"/>
<input type="button" value="Apply"/>	

Figure 12: Example 2 – LAN Configuration Page

Example 3: Configure the network interface to connect to a default gateway and DNS server:

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

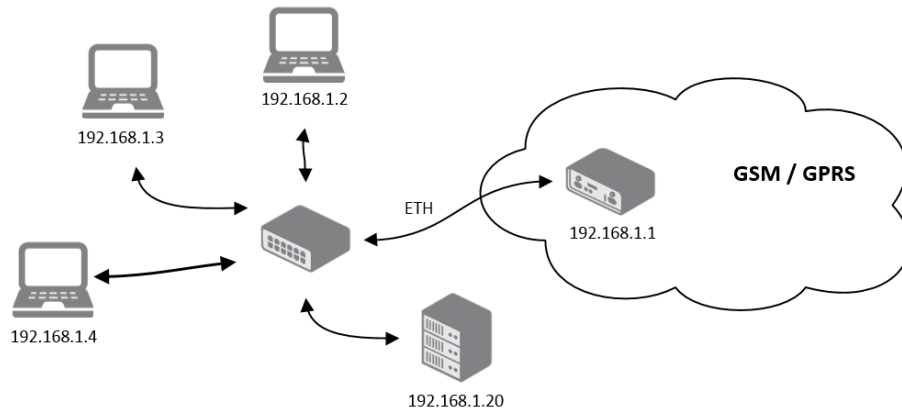


Figure 13: Example 3 – Network Topology

Primary LAN Configuration	
DHCP Client	disabled ▼
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.20
DNS Server	192.168.1.20
Bridged	no ▼
Media Type	auto-negotiation ▼
<input checked="" type="checkbox"/> Enable dynamic DHCP leases	
IP Pool Start	192.168.1.2
IP Pool End	192.168.1.4
Lease Time	600 sec
<input type="checkbox"/> Enable static DHCP leases	
MAC Address	IP Address
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="checkbox"/> Enable IEEE 802.1X Authentication	
Authentication Method	EAP-PEAP/MSCHAPv2 ▼
CA Certificate	<input type="text"/>
	Choose File No file chosen
Local Certificate	<input type="text"/>
	Choose File No file chosen
Local Private Key	<input type="text"/>
	Choose File No file chosen
Identity	<input type="text"/>
Password	<input type="text"/>
<input type="button" value="Apply"/>	

Figure 14: Example 3 – LAN Configuration Page

4.2 VRRP Configuration

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

Item	Description
Protocol Version	Choose version of the VRRP (VRRPv2 or VRRPv3).
Virtual Server IP Address	This parameter sets the virtual server IP address. This address must be the same for both the primary and backup routers. Devices on the LAN will use this address as their default gateway IP address.
Virtual Server ID	This parameter distinguishes one virtual router on the network from another. The main and backup routers must use the same value for this parameter.
Host Priority	The active router with highest priority set by the parameter Host Priority, is the main router. According to RFC 2338, the main router should have the highest possible priority – 255. The backup router(s) have a priority in the range 1 – 254 (default value is 100). A priority value of 0 is not allowed.

Table 14: VRRP configuration

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



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

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

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

Table 15: Check connection

Example of the VRRP protocol:

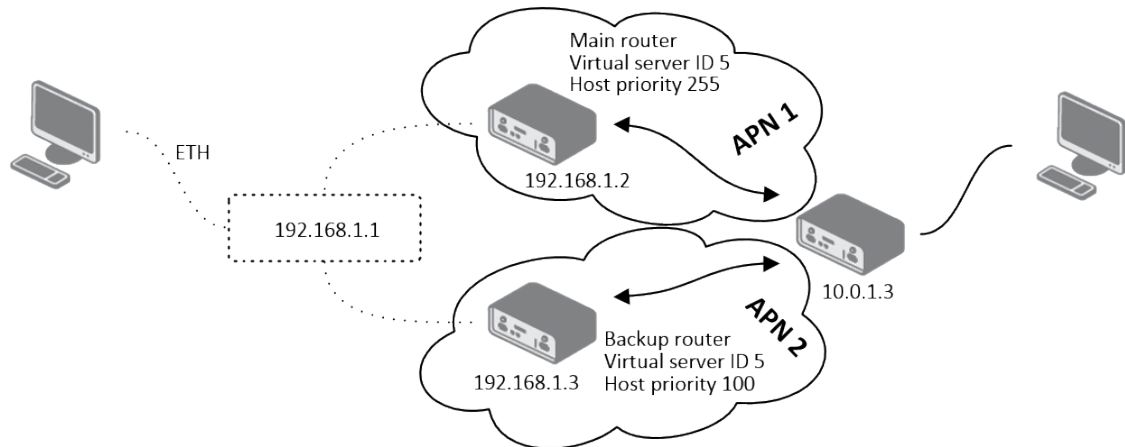


Figure 15: Topology of VRRP configuration example

1st VRRP Instance Configuration	
<input checked="" type="checkbox"/> Enable 1st VRRP Instance	
Protocol Version	VRRPv2
Virtual Server IP Address	192.168.1.1
Virtual Server ID	5
Host Priority	255
<input checked="" type="checkbox"/> Check connection	
Ping IP Address	10.0.1.3
Ping Interval	10 sec
Ping Timeout	5 sec
Ping Probes	10
<input type="checkbox"/> Enable traffic monitoring	
Apply	

Figure 16: Example of VRRP configuration – main router

1st VRRP Instance Configuration	
<input checked="" type="checkbox"/> Enable 1st VRRP Instance	
Protocol Version	VRRPv2
Virtual Server IP Address	192.168.1.1
Virtual Server ID	5
Host Priority	100
<input checked="" type="checkbox"/> Check connection	
Ping IP Address	10.0.1.3
Ping Interval	10 sec
Ping Timeout	5 sec
Ping Probes	10
<input type="checkbox"/> Enable traffic monitoring	
<input type="button" value="Apply"/>	

Figure 17: Example of VRRP configuration – backup router

4.3 Mobile WAN Configuration

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

4.3.1 Connection to Mobile Network

If you mark the *Create connection to mobile network* checkbox, then the router automatically attempts to establish a connection after booting up. You can specify the following parameters for each SIM card separately (on FULL version of the router with two SIM card slots), or to toggle between the APNs on single SIM card, specify two different APNs (BASIC version of the router with single SIM card slot).

Item	Description
APN	Network identifier (Access Point Name)
Username	User name for logging into the GSM network
Password	Password for logging into the GSM network Enter valid characters only.
Authentication	Authentication protocol in the GSM network: <ul style="list-style-type: none"> • PAP or CHAP – The router selects the authentication method. • PAP – The router uses the PAP authentication method. • CHAP – The router uses the CHAP authentication method.
IP Address	Specifies the IP address of SIM card. You manually enter the IP address, only when mobile network carrier assigned the IP address.
Dial Number	Specifies the telephone number the router dials for a GPRS or CSD connection. The router uses a default telephone number *99***1 #.
Operator	Specifies the carrier code. You can specify the parameter as the PLMN preferred carrier code.
Network type	Specifies the type of protocol used in the mobile network. <ul style="list-style-type: none"> • Automatic selection – The router automatically selects the transmission method according to the availability of transmission technology. • <i>Furthermore, according to the type of router</i> – It's also possible to select a specific method of data transmission (GPRS, UMTS, ...)
PIN	Specifies the PIN used to unlock the SIM card. Use a PIN parameter only if the network requires a SIM card router. The SIM card is blocked after several failed attempts to enter the PIN.
MRU	Specifies the Maximum Receive Unit which is the maximum size of a packet that the router can receive in a given environment. The default value is 1500 B. Other settings can cause the router to incorrectly transmit data. Minimal value is 128 B.

Continued on next page

Continued from previous page

Item	Description
MTU	Specifies the Maximum Transmission Unit which is the maximum size of a packet that the router can transmit in a given environment. The default value is 1500 B. Other settings can cause the router to incorrectly transmit data. Minimal value is 128 B.

Table 16: Mobile WAN Connection Configuration



The following list contains tips for working with the *Mobile WAN* configuration form:

- If the MTU size is set incorrectly, then the router does not exceed the data transfer. When you set the MTU value low, more frequent fragmentation of data occurs. More frequent fragmentation means a higher overhead and also the possibility of packet damage during defragmentation. On the contrary, a higher MTU value can cause the network to drop the packet.
- If the *IP address* field is left blank, when the router establishes a connection, then the mobile network carrier automatically assigns an IP address. If you assign an IP address, then the router accesses the network quicker.
- If the *APN* field is left blank, then the router automatically selects the APN using the IMSI code of the SIM card. If the PLMN (operator number format) is not in the APN list, then the router uses the default APN "internet". If AT&T carrier network is detected, "**phone**" is used as default APN. The mobile network carrier defines the APN.
- If you enter the word `blank` in the *APN* field, then the router interprets the APN as blank.



ATTENTION:

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

Parameters identified with an asterisk require you to enter the appropriate information only if this information is required by the mobile network carrier.

When the router is unsuccessful in establishing a connection to mobile network, verify accuracy of the entered data. Alternatively, you can try a different authentication method or network type.

4.3.2 DNS Address Configuration

The *DNS Settings* parameter is designed for easier configuration on the client side. When you set the value to *get from operator* the router attempts to automatically obtain an IP address from the primary and secondary DNS server of the mobile network carrier. To specify the IP addresses of the Primary DNS servers manually, from the *DNS Server* pull down list, select the value *set manually*.

4.3.3 Check Connection to Mobile Network Configuration

If the *Check Connection* item is set to *enabled* or *enabled + bind*, it activates checking the connection to the mobile network. The router will automatically send ping requests to the specified domain or IP address (*Ping IP Address* item) at regular time intervals (*Ping Interval*). In case of unsuccessful ping, a new one will be sent after ten seconds. If it fails to ping the IP address three times in a row, the router terminates the current connection and tries to establish new ones. Checking can be set separately for two SIM cards or two APNs. Send an ICMP to an IP address that you know is still functional. (The operator's DNS server, for example.)

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

Item	Description
Ping IP Address	Specifies the destination IP address or domain name for ping queries.
Ping Interval	Specifies the time intervals between the outgoing pings.
Ping Timeout	Time in seconds to wait for a Ping response.

Table 17: Check Connection to Mobile Network Configuration

If you mark the *Enable Traffic Monitoring* checkbox, then the router stops sending ping request to the *Ping IP Address* and it monitors the data stream on the connection to mobile network. If this connection is without data longer than the *Ping Interval*, then the router sends a ping request to the *Ping IP Address*.


Enabling the *Check Connection* function for mobile networks is necessary for uninterrupted and lasting operation of the router.



4.3.4 Data Limit Configuration


Item	Description
Data Limit	Specifies the maximum expected amount of data transmitted (sent and received) over GPRS in one billing period (month). Maximum value is 2 TB (2097152 MB).
Warning Threshold	Specifies the percentage of the "Data Limit" in the range of 50 % to 99 %. If the data limit is exceeded, the router sends an SMS in the following form <i>Router has exceeded (value of Warning Threshold) of data limit.</i>
Accounting Start	Specifies the day of the month in which the billing cycle starts for the SIM card used. When the service provider that issued the SIM card specifies the start billing period, the router begins to count the amount of transferred data starting on this day.

Table 18: Data Limit Configuration

 If the parameter *Data Limit State* (see below) is set to *not applicable* or *Send SMS when data limit is exceeded* in *SMS Configuration* is not selected, the *Data Limit* set here will be ignored.

4.3.5 Switch between SIM Cards Configuration

In the lower part of the configuration form you can specify the rules for toggling between the two SIM cards.

 The router will automatically toggle between the SIM cards and their individual setups depending on the configuration settings specified here (manual permission, roaming, data limit). Note that the SIM card selected for connection establishment is the result of the logical product (AND) of the configuration here (table below).

Item	Description
SIM Card	<p>Enable or disable the use of a SIM card. If you set all the SIM cards to <i>disabled</i>, this means that the entire cellular module is disabled.</p> <ul style="list-style-type: none"> ● enabled – It is possible to use the SIM card. ● disabled – Never use the SIM card, the usage of this SIM is forbidden.
Roaming State	<p>Configure the use of SIM cards based on roaming. This roaming feature has to be activated for the SIM card on which it is enabled!</p> <ul style="list-style-type: none"> ● not applicable – It is possible to use the SIM card everywhere. ● home network only – Only use the SIM card if roaming is not detected.

Continued on next page

Continued from previous page

Item	Description
Data Limit State	<p>Configure the use of SIM cards based on the Data Limit set above:</p> <ul style="list-style-type: none"> • not applicable – It is possible to use the SIM regardless of the limit. • not exceeded – Use the SIM card only if the Data Limit (set above) has not been exceeded.

Table 19: Switch between SIM cards configuration

Use the following parameters to specify the decision making of SIM card switching in the cellular module.

Item	Description
Default SIM Card	<p>Specifies the modules' default SIM card. The router will attempt to establish a connection to mobile network using this default.</p> <ul style="list-style-type: none"> • 1st – The 1st SIM card is the default one. • 2nd – The 2nd SIM card is the default one.
Initial State	<p>Specifies the action of the cellular module after the SIM card has been selected.</p> <ul style="list-style-type: none"> • online – establish connection to the mobile network after the SIM card has been selected (default). • offline – go to the off-line mode after the SIM card has been selected. <p>Note: If offline, you can change this initial state by SMS message only – see <i>SMS Configuration</i>. The cellular module will also go into off-line mode if none of the SIM cards are not selected.</p>
Switch to other SIM card when connection fails	<p>Applicable only when connection is established on the default SIM card and then fails. If the connection failure is detected by <i>Check Connection</i> feature above, the router will switch to the backup SIM card.</p>
Switch to default SIM card after timeout	<p>If enabled, after timeout, the router will attempt to switch back to the default SIM card. This applies only when there is default SIM card defined and the backup SIM is selected because of a failure of the default one or if roaming settings cause the switch. This feature is available only when <i>Switch to other SIM card when connection fails</i> is enabled.</p>
Initial Timeout	<p>Specifies the length of time that the router waits before the first attempt to revert to the default SIM card, the range of this parameter is from 1 to 10000 minutes.</p>
Subsequent Timeout	<p>Specifies the length of time that the router waits after an unsuccessful attempt to revert to the default SIM card, the range is from 1 to 10000 min.</p>

Continued on next page

Continued from previous page

Item	Description
Additive Constant	Specifies the length of time that the router waits for any further attempts to revert to the default SIM card. This length time is the sum of the time specified in the "Subsequent Timeout" parameter and the time specified in this parameter. The range in this parameter is from 1 to 10000 minutes.

Table 20: Parameters for SIM card switching

Example:

If you mark the *Switch to default SIM card after timeout* check box, and you enter the following values:

- *Initial Timeout* – 60 min,
- *Subsequent Timeout* – 30 min,
- *Additional Timeout* – 20 min.

The first attempt to change to the primary SIM card or APN is carried out after 60 minutes. When the first attempt fails, a second attempt is made after 30 minutes. A third attempt is made after 50 minutes (30+20). A fourth attempt is made after 70 minutes (30+20+20).

4.3.6 PPPoE Bridge Mode Configuration

If you mark the *Enable PPPoE bridge mode* check box on the configuration page for the first MWAN module, the router activates the PPPoE bridge protocol. PPPoE (point-to-point over ethernet) is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. The bridge mode allows you to create a PPPoE connection from a device behind the router. For example, a PC connected to the ETH port of the router. You assign the IP address of the SIM card to the PC.

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

1st Mobile WAN Configuration			
<input checked="" type="checkbox"/> Create connection to mobile network			
	1st SIM card	2nd SIM card	
APN *	<input type="text" value="gprsa.agnep"/>	<input type="text" value="conel.agnep.cz"/>	
Username *	<input type="text"/>	<input type="text"/>	
Password *	<input type="text"/>	<input type="text"/>	
Authentication	<input type="text" value="PAP or CHAP"/>	<input type="text" value="PAP or CHAP"/>	
IP Address *	<input type="text"/>	<input type="text"/>	
Dial Number *	<input type="text"/>	<input type="text"/>	
Operator *	<input type="text"/>	<input type="text"/>	
Network Type	<input type="text" value="automatic selection"/>	<input type="text" value="automatic selection"/>	
PIN *	<input type="text"/>	<input type="text"/>	
MRU	<input type="text" value="1500"/>	<input type="text" value="1500"/>	bytes
MTU	<input type="text" value="1500"/>	<input type="text" value="1500"/>	bytes
DNS Settings	<input type="text" value="get from operator"/>	<input type="text" value="get from operator"/>	
DNS IP Address	<input type="text"/>	<input type="text"/>	
<i>(The feature of check connection to mobile network is necessary for uninterrupted operation)</i>			
Check Connection	<input type="text" value="disabled"/>	<input type="text" value="disabled"/>	
Ping IP Address	<input type="text"/>	<input type="text"/>	
Ping Interval	<input type="text"/>	<input type="text"/>	sec
Ping Timeout	<input type="text" value="10"/>	<input type="text" value="10"/>	sec
<input type="checkbox"/> Enable traffic monitoring			
Data Limit	<input type="text"/>	<input type="text"/>	MB
Warning Threshold	<input type="text"/>	<input type="text"/>	%
Accounting Start	<input type="text" value="1"/>	<input type="text" value="1"/>	
SIM Card	<input type="text" value="enabled"/>	<input type="text" value="enabled"/>	
Roaming State	<input type="text" value="not applicable"/>	<input type="text" value="not applicable"/>	
Data Limit State	<input type="text" value="not applicable"/>	<input type="text" value="not applicable"/>	
BINO State	<input type="text" value="not applicable"/>	<input type="text" value="not applicable"/>	
Default SIM Card	<input type="text" value="1st"/>		
Initial State	<input type="text" value="online"/>		
<input type="checkbox"/> Switch to other SIM card when connection fails			
<input type="checkbox"/> Switch to default SIM card after timeout			
Initial Timeout	<input type="text" value="60"/>		min
Subsequent Timeout *	<input type="text"/>		min
Additive Constant *	<input type="text"/>		min
<input type="checkbox"/> Enable PPPoE bridge mode			
* can be blank			
<input type="button" value="Apply"/>			

Figure 18: Mobile WAN Configuration

Example 1: The figure below displays the following scenario: the connection to the mobile network is controlled on the address 8.8.8.8 with the time interval of 60 seconds for the primary SIM card and on the address www.google.com with the time interval 80 seconds for the secondary SIM card. In the case of data stream on the router, the control pings are not sent, but the data stream is monitored.

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

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

Figure 19: Example 1 – Mobile WAN Configuration

Example 2: The following configuration illustrates a scenario in which the router changes to a backup SIM card after exceeding the data limits of 800MB. The router sends SMS upon reaching 400MB. The accounting period starts on the 18th day of the month.

Data Limit	800		MB
Warning Threshold	50		%
Accounting Start	18	1	
SIM Card	enabled ▼	enabled ▼	
Roaming State	not applicable ▼	not applicable ▼	
Data Limit State	not applicable ▼	not applicable ▼	
BIN0 State	not applicable ▼	not applicable ▼	
Default SIM Card	1st ▼		
Initial State	online ▼		
<input type="checkbox"/> Switch to other SIM card when connection fails <input type="checkbox"/> Switch to default SIM card after timeout			
Initial Timeout			min
Subsequent Timeout *			min
Additive Constant *			min

Figure 20: Example 2 – Mobile WAN Configuration

4.4 PPPoE Configuration

PPPoE (Point-to-Point over Ethernet) is a network protocol which encapsulates PPP frames into Ethernet frames. The router uses the PPPoE client to connect to devices supporting a PPPoE bridge or server. The bridge or server is typically an ADSL router.

To open the *PPPoE Configuration* page, select the *PPPoE* menu item. If you mark the *Create PPPoE connection* check box, then the router attempts to establish a PPPoE connection after boot up. After connecting, the router obtains the IP address of the device to which it is connected. The communications from a device behind the PPPoE server is forwarded to the router.

Figure 21: PPPoE configuration

Item	Description
Username	Username for secure access to PPPoE.
Password	Password for secure access to PPPoE. Enter valid characters only.
Authentication	Authentication protocol in GSM network. <ul style="list-style-type: none"> ● PAP or CHAP – The router selects the authentication method. ● PAP – The router uses the PAP authentication method. ● CHAP – The router uses the CHAP authentication method.

Continued on the next page

Continued from previous page

Item	Description
MRU	Specifies the Maximum Receiving Unit. The MRU identifies the maximum packet size, that the router can receive in a given environment. The default value is 1492 bytes. Other settings can cause incorrect data transmission.
MTU	Specifies the Maximum Transmission Unit. The MTU identifies the maximum packet size, that the router can transfer in a given environment. The default value is 1492 bytes. Other settings can cause incorrect data transmission.
DNS Settings	Can be set to obtain the DNS address from the server or to set it manually.
DNS IP Address	Manual setting of DNS address.
Interface	Select an Ethernet interface.
VLAN Tagging	Select yes to turn on the VLAN tagging.
VLAN ID	Set the ID for VLAN tagging. The range is from 1 to 1000.

Table 21: PPPoE configuration

Setting an incorrect packet size value (MRU, MTU) can cause unsuccessful transmission.



4.5 Backup Routes

Using the configuration form on the *Backup Routes* page, you can back up the primary connection with alternative connections to the Internet (mobile network) or enable *Multiple WANs* mode. It is also possible to prioritize each backup connection option. Switching between connections is carried out according to order of priority and the state of the connections.

Backup Routes Configuration

Enable backup routes switching

Mode

Enable backup routes switching for Mobile WAN

Priority

Weight

Enable backup routes switching for PPPoE

Priority

Ping IP Address

Ping Interval sec

Ping Timeout sec

Weight

Enable backup routes switching for Primary LAN

Priority

Ping IP Address

Ping Interval sec

Ping Timeout sec

Weight

Enable backup routes switching for Secondary LAN

Priority

Ping IP Address

Ping Interval sec

Ping Timeout sec

Weight

Figure 22: Backup Routes Configuration

Item	Description
Enable backup routes switching	The default route is selected according to the settings below. If disabled (unchecked), the backup routes system operates in the backward compatibility mode based on the default priorities of the network interfaces (listed below).
Mode	<ul style="list-style-type: none"> • Single WAN – The default mode. Only one interface is used for WAN communication at a time. Other interfaces are used for WAN when the preferred interface fails, based on the priorities set. • Multiple WANs – Multiple interfaces can be used for WAN connection. When WAN communication via multiple interfaces is received, the same interface is used in reply, therefore; the traffic will stay on the given interface. The set priorities are used when transmitting data from the router or from the network behind the router. The highest priority interface is used for these transmissions. • Load Balancing – In this mode, the weight for every interface can be set. This setting determines the relative number of data streams going through the interfaces. Please note that this may not exactly match the amount of data, it very depends on the number of streams and the structure of the data.

Table 22: Backup Routes Configuration

To add the network interfaces to the backup routes system, mark the checkbox(s) of the following interface options: *Enable backup routes switching for Mobile WAN*, *Enable backup routes switching for PPPoE*, *Enable backup routes switching for Primary LAN* or *Enable backup routes switching for Secondary LAN*. Enabled interfaces are then used for WAN access either in *Single WAN* mode (only one interface at a time) or in *Multiple WANs* mode (multiple interfaces at a time), based on priorities set:

Item	Description
Priority	Priority for the type of connection (network interface).
Ping IP Address	Destination IP address or domain name of ping queries to check the connection.
Ping Interval	The time interval between consecutive ping queries.
Ping Timeout	Time in seconds to wait for a response to the Ping.
Weight	Weight for the Load Balancing mode only. The number from 1 to 256 determines the ratio for load balancing of the interface. For example, if two interfaces have set up the weight to 1, the ratio is 50% to 50%. If they have set up the weight to 1 and 4, the ratio is 20% to 80%.

Table 23: Backup Routes



If you want to use a mobile WAN connection as a backup route, you must choose the *enable + bind* option in the *Check Connection* item on the *Mobile WAN* page and fill in the ping address.

Network interfaces belonging to individual backup routes are also checked before use for flags which indicate the state of the interface. (E.g. RUNNING on the *Network Status* page.) This prevents, for example, the disconnection of an Ethernet cable. Any changes made to settings will be applied after pressing the *Apply* button.

Default Priorities for Backup Routes: If the *Enable backup routes switching* check box is unchecked, the backup routes system will operate in the backward compatibility mode. The router selects the route based on the default priorities of the enabled settings for each of the network interfaces, enabling appropriate services that comply with these network interfaces. The following list contains the names of backup routes and corresponding network interfaces in order of default priorities:

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



Note: Consider there is a concept of variable WAN and LAN interfaces even if the *Backup Routes* are not enabled. The situation may occur, that LAN intended interface becomes WAN interface (because of specified or default priorities). Communication from WAN interface to LAN interface can then be blocked depending on the *NAT* and *Firewall* Configuration.

4.6 Static Routes

Static routes can be specified on the *Static Routes* configuration page. A static route provide fixed routing path through the network. It is manually configured on the router and must be updated if the network topology was changed recently. Static routes are private routers unless they are redistributed by a routing protocol. Static routes configuration form is shown on Figure 23.

Static Routes Configuration

Enable static routes

Destination Network	Mask or Prefix Length	Gateway *	Metric *	Interface
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Primary LAN ▾
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Primary LAN ▾
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Primary LAN ▾
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Primary LAN ▾
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Primary LAN ▾
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Primary LAN ▾
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Primary LAN ▾
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Primary LAN ▾

* can be blank

Figure 23: Static Routes Configuration

The description of all items is listed in Table 24.

Item	Description
Enable static routes	If checked, static routing functionality is enabled. Active are only routes enabled by the checkbox in the first column of the table.
Destination Network	The destination IP address of the remote network or host to which you want to assign a static route.
Mask or Prefix Length	The subnet mask of the remote network or host IP address.
Gateway	IP address of the gateway device that allows for contact between the router and the remote network or host.
Metric	Metric definition, means number rating of the priority for the route in the routing table. Routes with lower metrics have higher priority.
Interface	Select an interface the remote network or host is on.

Table 24: Static Routes configuration

4.7 Firewall Configuration

The first security element which incoming packets pass is a check of the enabled source IP addresses and destination ports. You can specify the IP addresses as an IP address from which you can remotely access the router and the internal network connected behind a router. To enable this function, marking the *Enable filtering of incoming packets* check box located at the top of the *Firewall Configuration* page. Accessibility is checked against the IP address table. This means that access is permitted only to addresses specified in the table. It is possible to specify up to eight remote IP addresses for access. You can specify the following parameters:

Item	Description
Source	IP address from which access to the router is allowed.
Protocol	Specifies the protocol used for remote access: <ul style="list-style-type: none"> • all – Access for all protocols is active. • TCP – Access for the TCP protocol is active. • UDP – Access for the UDP protocol is active. • GRE – Access for the GRE protocol is active. • ESP – Access for the ESP protocol is active. • ICMP – Access for the ICMP protocol is active.
Target Port(s)	The port numbers range allowing access to the router. Enter the initial and final port numbers separated by the hyphen mark. One static port is allowed as well.
Action	Specifies the type of action the router performs: <ul style="list-style-type: none"> • allow – The router allows the packets to enter the network. • deny – The router denies the packets from entering the network

Table 25: Filtering of Incoming Packets

The next section of the configuration form specifies the forwarding policy. If you unmark the *Enabled filtering of forwarded packets* check box, then packets are automatically accepted. If you activate this function, and a packet is addressed to another network interface, then the router sends the packet to the FORWARD chain. When the FORWARD chain accepts the packet and there is a rule for forwarding it, the router sends the packet. If a forwarding rule is unavailable, then the router drops the packet.

This configuration form also contains a table for specifying the filter rules. It is possible to create a rule to allow data with the selected protocol by specifying only the protocol, or to create stricter rules by specifying values for source IP addresses, destination IP addresses, and ports.

Item	Description
Source	IP address from which access to the router is allowed.
Destination	IP address of destination device.

Continued on next page

Continued from previous page

Item	Description
Protocol	Specifies the protocol used for remote access: <ul style="list-style-type: none"> • all – Access for all protocols is active. • TCP – Access for the TCP protocol is active. • UDP – Access for the UDP protocol is active. • GRE – Access for the GRE protocol is active. • ESP – Access for the ESP protocol is active. • ICMP – Access for the ICMP protocol is active.
Target Port(s)	The target port numbers. Enter the initial and final port numbers separated by the hyphen mark. One static port is allowed as well.
Action	Specifies the type of action the router performs: <ul style="list-style-type: none"> • allow – The router allows the packets to enter the network. • deny – The router denies the packets from entering the network.

Table 26: Forwarding filtering

When you enable the *Enable filtering of locally destined packets* function, the router drops receives packets requesting an unsupported service. The packet is dropped automatically without any information.

As a protection against DoS attacks, the *Enable protection against DoS attacks* limits the number of allowed connections per second to five. The DoS attack floods the target system with meaningless requirements.

IPv4 Firewall Configuration

Enable filtering of incoming packets

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

Enabled filtering of forwarded packets

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

Enable filtering of locally destined packets

Enable protection against DoS attacks

* can be blank

Figure 24: Firewall Configuration

Example of the firewall configuration:

The router allows the following access:

- from IP address 171.92.5.45 using any protocol
- from IP address 10.0.2.123 using the TCP protocol on target port 1000
- from IP address 142.2.26.54 using the ICMP protocol
- from IP address 142.2.26.54 using the TCMP protocol on target ports from 1020 to 1040

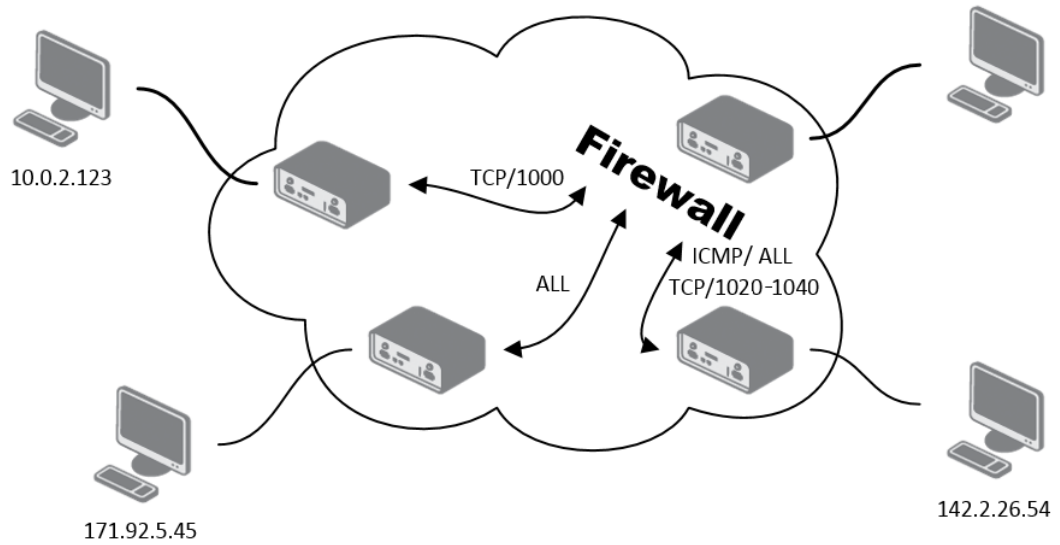


Figure 25: Topology for the Firewall Configuration Example

Firewall Configuration				
<input checked="" type="checkbox"/> Enable filtering of incoming packets				
<input checked="" type="checkbox"/>	Source *	Protocol	Target Port(s) *	Action
<input checked="" type="checkbox"/>	171.92.5.45	all ▼		allow ▼
<input checked="" type="checkbox"/>	10.0.2.123	TCP ▼	1000	allow ▼
<input checked="" type="checkbox"/>	142.2.26.54	ICMP ▼		allow ▼
<input checked="" type="checkbox"/>	142.2.26.54	TCP ▼	1020-1040	allow ▼
<input type="checkbox"/>		all ▼		allow ▼
<input type="checkbox"/>		all ▼		allow ▼
<input type="checkbox"/>		all ▼		allow ▼
<input type="checkbox"/>		all ▼		allow ▼

Figure 26: Firewall Configuration Example

4.8 NAT Configuration

To configure the address translation function, open the *NAT Configuration* page, click on *NAT* in the *Configuration* section of the main menu. The router actually uses Port Address Translation (PAT), which is a method of mapping a TCP/UDP port to another TCP/UDP port. The router modifies the information in the packet header as the packets traverse a router. This configuration form allows you to specify up to 16 PAT rules.

Item	Description
Public Port(s)	The public port numbers range for NAT. Enter the initial and final port numbers separated by the hyphen mark. One static port is allowed as well.
Private Port(s)	The private port numbers range for NAT. Enter the initial and final port numbers separated by the hyphen mark. One static port is allowed as well.
Type	Protocol type
Server IP address	IP address where the router forwards incoming data.

Table 27: NAT Configuration

If you require more than sixteen NAT rules, then insert the remaining rules into the start up script. The *Startup Script* dialog is located in the *Configuration* section of the main menu. When creating your rules in the start up script, use the following format:

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

Enter the IP address [IPADDR], the public ports numbers [PORT_PUBLIC], and private [PORT_PRIVATE] in square bracket.

You use the following parameters to set the routing of incoming data from the PPP to a connected computer.

Item	Description
Send all remaining incoming packets to default server	Activates/deactivates forwarding unmatched incoming packets to the default server. The prerequisite for the function is that you specify a default server in the <i>Default Server IP Address</i> field. The router can forward incoming data from a GPRS to a computer with the assigned IP address.
Default Server IP Address	Specified the IP address for the default server.

Table 28: Configuration of send all incoming packets

If you enable the following options and enter the port number, the router allows you to remotely access to the router from a PPP interface.

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

Table 29: Remote Access Configuration

Example 1: NAT configuration with one connection to the router:

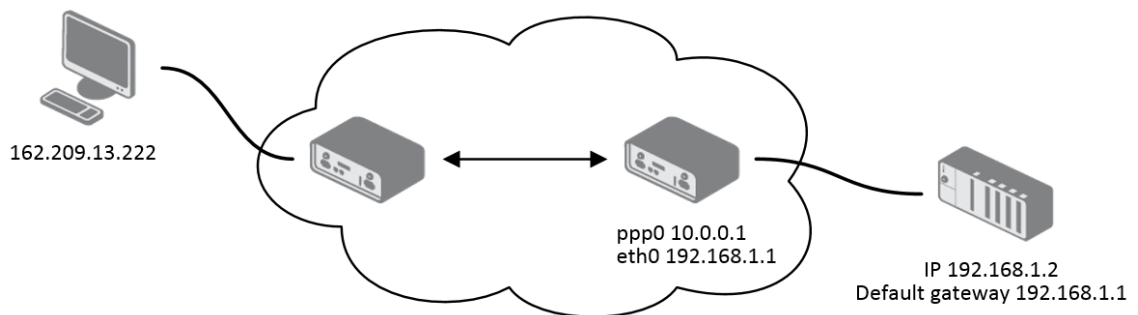


Figure 27: Example 1 – Topology of NAT Configuration

IPv4 NAT Configuration			
Public Port(s)	Private Port(s)	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"/>
<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"/>
<input checked="" type="checkbox"/> Enable remote HTTP access on port	<input type="text"/>	80	
<input type="checkbox"/> Enable remote HTTPS access on port	<input type="text"/>	443	
<input checked="" type="checkbox"/> Enable remote FTP access on port	<input type="text"/>	21	
<input type="checkbox"/> Enable remote SSH access on port	<input type="text"/>	22	
<input checked="" type="checkbox"/> Enable remote Telnet access on port	<input type="text"/>	23	
<input checked="" type="checkbox"/> Enable remote SNMP access on port	<input type="text"/>	161	
<input checked="" type="checkbox"/> Send all remaining incoming packets to default server			
Default Server IP Address <input type="text" value="192.168.1.2"/>			
<input checked="" type="checkbox"/> Masquerade outgoing packets			
<input type="button" value="Apply"/>			

Figure 28: Example 1 – NAT Configuration

It is important to mark the *Send all remaining incoming packets to default server* check box for this configuration. The IP address in this example is the address of the device behind the router. The default gateway of the devices in the subnetwork connected to router is the same IP address as displayed in the *Default Server IP Address* field. The connected device replies if a PING is sent to the IP address of the SIM card.

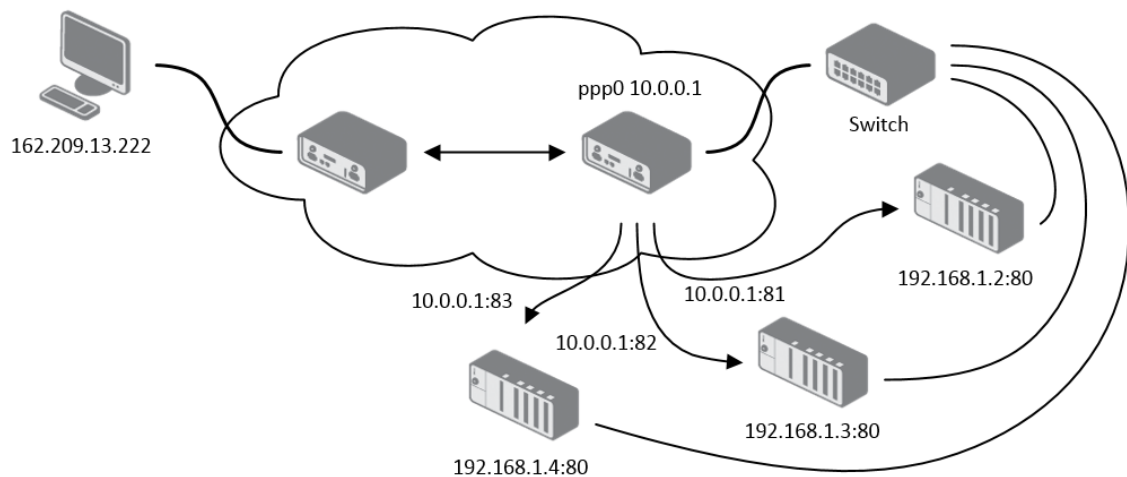
Example 2: Configuration with more equipment connected.

Figure 29: Example 2 – Topology of NAT Configuration

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

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

Enable remote HTTP access on port

Enable remote HTTPS access on port

Enable remote FTP access on port

Enable remote SSH access on port

Enable remote Telnet access on port

Enable remote SNMP access on port

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

Masquerade outgoing packets

Figure 30: Example 2 – NAT Configuration

4.9 OpenVPN Tunnel Configuration

Select the *OpenVPN* item to configure an OpenVPN tunnel. The menu item will expand and you will see four separate configuration pages: *1st Tunnel*, *2nd Tunnel*, *3rd Tunnel* and *4th Tunnel*. The OpenVPN tunnel function allows you to create a secure connection between two separate LAN networks. The router allows you to create up to four OpenVPN tunnels.

Item	Description
Description	Specifies the description or name of tunnel.
Protocol	Specifies the communication protocol. <ul style="list-style-type: none"> • UDP – The OpenVPN communicates using UDP. • TCP server – The OpenVPN communicates using TCP in server mode. • TCP client – The OpenVPN communicates using TCP in client mode.
UDP/TCP port	Specifies the port of the relevant protocol (UDP or TCP).
Remote IP Address	Specifies the IP address of opposite tunnel side. You can also use the domain name.
Remote Subnet	Specifies the IP address of a network behind opposite side of the tunnel.
Remote Subnet Mask	Specifies the subnet mask of a network behind opposite side of the tunnel.
Redirect Gateway	Adds (rewrites) the default gateway. All the packets are then sent to this gateway via tunnel, if there is no other specified default gateway inside them.
Local Interface IP Address	Specifies the IP address of a local interface.
Remote Interface IP Address	Specifies the IP address of the interface of opposite side of the tunnel.
Ping Interval	Specifies the time interval after which the router sends a message to opposite side of tunnel to verify the existence of the tunnel.
Ping Timeout	Specifies the time interval during which the router waits for a message sent by the opposite side. For proper verification of the OpenVPN tunnel, set the <i>Ping Timeout</i> to greater than the <i>Ping Interval</i> .
Renegotiate Interval	Specifies the renegotiate period (reauthorization) of the OpenVPN tunnel. You can only set this parameter when the <i>Authenticate Mode</i> is set to <i>username/password</i> or <i>X.509 certificate</i> . After this time period, the router changes the tunnel encryption to help provide the continues safety of the tunnel.
Max Fragment Size	Maximum size of a sent packet.

Continued on next page

Continued from previous page

Item	Description
Compression	Compression of the data sent: <ul style="list-style-type: none"> • none – No compression is used. • LZO – A lossless compression is used, use the same setting on both sides of the tunnel.
NAT Rules	Activates/deactivates the NAT rules for the OpenVPN tunnel: <ul style="list-style-type: none"> • not applied – NAT rules are not applied to the OpenVPN tunnel. • applied – NAT rules are applied to the OpenVPN tunnel.
Authenticate Mode	Specifies the authentication mode: <ul style="list-style-type: none"> • none – No authentication is set. • Pre-shared secret – Specifies the shared key function for both sides of the tunnel. • Username/password – Specifies authentication using a CA Certificate, Username and Password. • X.509 Certificate (multiclient) – Activates the X.509 authentication in multi-client mode. • X.509 Certificate (client) – Activates the X.509 authentication in client mode. • X.509 Certificate (server) – Activates the X.509 authentication in server mode.
Pre-shared Secret	Specifies the pre-shared secret which you can use for every authentication mode.
CA Certificate	Specifies the CA Certificate which you can use for the username/password and X.509 Certificate authentication modes.
DH Parameters	Specifies the protocol for the DH parameters key exchange which you can use for X.509 Certificate authentication in the server mode.
Local Certificate	Specifies the certificate used in the local device. You can use this authentication certificate for the X.509 Certificate authentication mode.
Local Private Key	Specifies the key used in the local device. You can use the key for the X.509 Certificate authentication mode.
Username	Specifies a login name which you can use for authentication in the username/password mode.
Password	Specifies a password which you can use for authentication in the username/password mode. Enter valid characters only.

Continued on next page

Continued from previous page

Item	Description
Extra Options	Specifies additional parameters for the OpenVPN tunnel, such as DHCP options. The parameters are preceded by two dashes. For possible parameters see the help text in the router using SSH – run the <code>openvpn --help</code> command.

Table 30: OpenVPN Configuration

There is a condition for tunnel to be established: WAN route has to be active (for example mobile connection established) even if the tunnel does not go through the WAN.



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

1st OpenVPN Tunnel Configuration	
<input type="checkbox"/> Create 1st OpenVPN tunnel	
Description *	<input type="text"/>
Protocol	UDP ▼
UDP Port	1194
Remote IP Address *	<input type="text"/>
Remote Subnet *	<input type="text"/>
Remote Subnet Mask *	<input type="text"/>
Redirect Gateway	no ▼
Local Interface IP Address	<input type="text"/>
Remote Interface IP Address	<input type="text"/>
Ping Interval *	<input type="text"/> sec
Ping Timeout *	<input type="text"/> sec
Renegotiate Interval *	<input type="text"/> sec
Max Fragment Size *	<input type="text"/> bytes
Compression	LZO ▼
NAT Rules	not applied ▼
Authenticate Mode	none ▼
Pre-shared Secret	<input type="text"/>
CA Certificate	<input type="text"/> Choose File No file chosen
DH Parameters	<input type="text"/> Choose File No file chosen
Local Certificate	<input type="text"/> Choose File No file chosen
Local Private Key	<input type="text"/> Choose File No file chosen
Username	<input type="text"/>
Password	<input type="text"/>
Extra Options *	<input type="text"/>
* can be blank	
<input type="button" value="Apply"/>	

Figure 31: OpenVPN tunnel configuration

Example of the OpenVPN tunnel configuration:

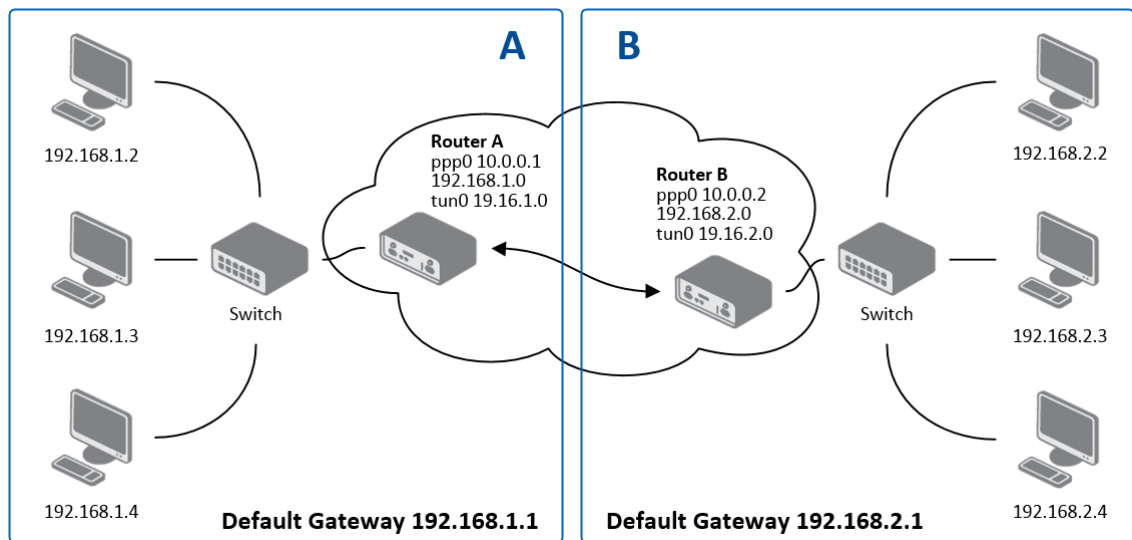


Figure 32: Topology of OpenVPN Configuration Example

OpenVPN tunnel configuration:

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

Table 31: OpenVPN Configuration Example

Examples of different options for configuration and authentication of OpenVPN tunnel can be found in the application note *OpenVPN Tunnel* [4].



4.10 IPsec Tunnel Configuration

To open the *IPsec Tunnel Configuration* page, click *IPsec* in the *Configuration* section of the main menu. The menu item will expand and you will see four separate configuration pages: *1st Tunnel*, *2nd Tunnel*, *3rd Tunnel* and *4th Tunnel*. The IPsec tunnel function allows you to create a secured connection between two separate LAN networks. The router allows you to create up to four IPsec tunnels.



To encrypt data between the local and remote subnets, specify the appropriate values in the subnet fields on both routers. To encrypt the data stream between the routers only, leave the local and remote subnets fields blank.



If you specify the protocol and port information in the *Local Protocol/Port* field, then the router encapsulates only the packets matching the settings.



For optimal setup, we recommend to follow instructions on the web page: <https://wiki.strongswan.org/projects/strongswan/wiki/SecurityRecommendations>.

Item	Description
Description	Name or description of the tunnel.
Remote IP Address	IP address of remote side of the tunnel. It is also possible to enter the domain name.
Remote ID	Identifier (ID) of remote side of the tunnel. It consists of two parts: a <i>hostname</i> and a <i>domain-name</i> .
First Remote Subnet	IP address of a network behind remote side of the tunnel.
First Remote Subnet Mask	Subnet mask of a network behind remote side of the tunnel.
Second Remote Subnet	IP address of the second network behind remote side of the tunnel. For <i>IKE Protocol = IKEv2</i> only.
Second Remote Subnet Mask	Subnet mask of the second network behind remote side of the tunnel. For <i>IKE Protocol = IKEv2</i> only.
Remote Protocol/Port	Specifies Protocol/Port of remote side of the tunnel. The general form is <i>protocol/port</i> , for example 17/1701 for UDP (protocol 17) and port 1701. It is also possible to enter only the number of protocol, however, the above mentioned format is preferred.
Local ID	Identifier (ID) of local side of the tunnel. It consists of two parts: a <i>hostname</i> and a <i>domain-name</i> .
First Local Subnet	IP address of a local network.
First Local Subnet Mask	Subnet mask of a local network.

Continued on next page

Continued from previous page

Item	Description
Second Local Subnet	IP address of the second local network. For <i>IKE Protocol</i> = IKEv2 only.
Second Local Subnet Mask	Subnet mask of the second local network. For <i>IKE Protocol</i> = IKEv2 only.
Local Protocol/Port	Specifies Protocol/Port of a local network. The general form is <i>protocol/port</i> , for example 17/1701 for UDP (protocol 17) and port 1701. It is also possible to enter only the number of protocol, however, the above mentioned format is preferred.
Encapsulation Mode	Specifies the IPsec mode, according to the method of encapsulation. You can select the <i>tunnel</i> mode in which the entire IP datagram is encapsulated or the <i>transport</i> mode in which only IP header is encapsulated.
Force NAT Traversal	Enable NAT traversal enforcement (UDP encapsulation of ESP packets). (<i>Enabled</i>).
IKE Protocol	Specifies the version of IKE (IKEv1/IKEv2, IKEv1 or IKEv2).
IKE Mode	Specifies the mode for establishing a connection (<i>main</i> or <i>aggressive</i>). If you select the aggressive mode, then the router establishes the IPsec tunnel faster, but the encryption is permanently set to 3DES-MD5. We recommend that you not use the aggressive mode due to lower security!
IKE Algorithm	Specifies the means by which the router selects the algorithm: <ul style="list-style-type: none"> • auto – The encryption and hash algorithm are selected automatically. • manual – The encryption and hash algorithm are defined by the user.
IKE Encryption	Encryption algorithm – 3DES, AES128, AES192, AES256, AES128GCM128, AES192GCM128, AES256GCM128.
IKE Hash	Hash algorithm – MD5, SHA1, SHA256 or SHA512.
IKE DH Group	Specifies the Diffie-Hellman groups which determine the strength of the key used in the key exchange process. Higher group numbers are more secure, but require additional time to compute the key.
IKE Reauthentication	Enable or disable IKE reauthentication (IKEv2 only).
XAUTH Enabled	Enable extended authentication (for IKEv1 only).
XAUTH Mode	Select XAUTH mode (client or server).
XAUTH Username	XAUTH username.
XAUTH Password	XAUTH password.

Continued on next page

Continued from previous page

Item	Description
ESP Algorithm	Specifies the means by which the router selects the algorithm: <ul style="list-style-type: none"> • auto – The encryption and hash algorithm are selected automatically. • manual – The encryption and hash algorithm are defined by the user.
ESP Encryption	Encryption algorithm – DES, 3DES, AES128, AES192, AES256, AES128GCM128, AES192GCM128, AES256GCM128.
ESP Hash	Hash algorithm – MD5, SHA1, SHA256 or SHA512.
PFS	Enables/disables the Perfect Forward Secrecy function. The function ensures that derived session keys are not compromised if one of the private keys is compromised in the future.
PFS DH Group	Specifies the Diffie-Hellman group number (see <i>IKE DH Group</i>).
Key Lifetime	Lifetime key data part of tunnel. The minimum value of this parameter is 60 s. The maximum value is 86400 s.
IKE Lifetime	Lifetime key service part of tunnel. The minimum value of this parameter is 60 s. The maximum value is 86400 s.
Rekey Margin	Specifies how long before a connection expires that the router attempts to negotiate a replacement. Specify a maximum value that is less than half of IKE and Key Lifetime parameters.
Rekey Fuzz	Percentage of time for the Rekey Margin extension.
DPD Delay	Time after which the IPsec tunnel functionality is tested.
DPD Timeout	The period during which device waits for a response.
Authenticate Mode	Specifies the means by which the router authenticates: <ul style="list-style-type: none"> • Pre-shared key – Sets the shared key for both sides of the tunnel. • X.509 Certificate – Allows X.509 authentication in multi-client mode.
Pre-shared Key	Specifies the shared key for both sides of the tunnel. The prerequisite for entering a key is that you select pre-shared key as the authentication mode.
CA Certificate	Certificate for X.509 authentication.
Remote Certificate \ PubKey	Certificate for X.509 authentication or PubKey for public key signature authentication.
Local Certificate \ PubKey	Certificate for X.509 authentication or PubKey for public key signature authentication.
Local Private Key	Private key for X.509 authentication.
Local Passphrase	Passphrase used during private key generation.

Continued on next page

Continued from previous page

Item	Description
Debug	Choose the level of verbosity to System Log. Silent (default), audit, control, control-more, raw, private (most verbose including the private keys).

Table 32: IPsec Tunnel Configuration

Do not miss:

- If local and remote subnets are not configured then only packets between local and remote IP address are encapsulated, so only communication between two routers is encrypted.
- If protocol/port fields are configured then only packets matching these settings are encapsulated.



The following procedure describes how to generate certificates and keys without a password phrase:

```

***** certification authority *****
openssl rand -out private/.rand 1024
openssl genrsa -des3 -out private/ca.key 2048
openssl req -new -key private/ca.key -out tmp/myrootca.req
openssl x509 -req -days 7305 -sha1 -extensions v3_ca -signkey
private/ca.key -in tmp/myrootca.req -out ca.crt

***** server cert *****
openssl genrsa -out private/server.key 2048
openssl req -new -key private/server.key -out tmp/server.req
openssl x509 -req -days 7305 -sha1 -extensions v3_req -CA ca.crt -CAkey
private/ca.key -in tmp/server.req -CAserial ca.srl -CAcreateserial
-out server.crt

***** client cert *****
openssl genrsa -out private/client.key 2048
openssl req -new -key private/client.key -out tmp/client.req
openssl x509 -req -days 7305 -sha1 -extensions v3_req -CA ca.crt -CAkey
private/ca.key -in tmp/client.req -CAserial ca.srl -CAcreateserial
-out client.crt

```



Listed below are the certificates with password phrase "router" (certification authority remains unchanged):

```

***** server cert *****
openssl genrsa -des3 -passout pass:router -out private/server.pem 2048
openssl req -new -key private/server.pem -out tmp/server.req
openssl x509 -req -days 7305 -sha1 -extensions v3_req -CA ca.crt -CAkey
private/ca.key -in tmp/server.req -CAserial ca.srl -CAcreateserial
-out server.crt

***** client cert *****
openssl genrsa -des3 -passout pass:router -out private/client.pem 2048
openssl req -new -key private/client.pem -out tmp/client.req
openssl x509 -req -days 7305 -sha1 -extensions v3_req -CA ca.crt -CAkey
private/ca.key -in tmp/client.req -CAserial ca.srl -CAcreateserial
-out client.crt

```

The IPsec function supports the following types of identifiers (ID) for both sides of the tunnel, *Remote ID* and *Local ID* parameters:

- IP address (for example, 192.168.1.1)
- DN (for example, C=CZ,O=CompanyName,OU=TP,CN=A)
- FQDN (for example, @director.companyname.cz) – **the @ symbol precedes the FQDN. FQDN resolving is not supported.**
- User FQDN (for example, director@companyname.cz)



The certificates and private keys have to be in the PEM format. Use only certificates containing start and stop tags.

The random time, after which the router re-exchanges new keys is defined as follows:

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

The default exchange of keys is in the following time range:

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

We recommend that you maintain the default settings. When you set key exchange times higher, the tunnel produces lower operating costs, but the setting also provides less security. Conversely, when you reducing the time, the tunnel produces higher operating costs, but provides for higher security.

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

1st IPsec Tunnel Configuration		
<input type="checkbox"/> Create 1st IPsec tunnel		
Description *	<input type="text"/>	
Remote IP Address *	<input type="text"/>	
Remote ID *	<input type="text"/>	
First Remote Subnet *	<input type="text"/>	
First Remote Subnet Mask *	<input type="text"/>	
Second Remote Subnet *	<input type="text"/>	
Second Remote Subnet Mask *	<input type="text"/>	
Remote Protocol/Port *	<input type="text"/>	
Local ID *	<input type="text"/>	
First Local Subnet *	<input type="text"/>	
First Local Subnet Mask *	<input type="text"/>	
Second Local Subnet *	<input type="text"/>	
Second Local Subnet Mask *	<input type="text"/>	
Local Protocol/Port *	<input type="text"/>	
Encapsulation Mode	tunnel	▼
Force NAT Traversal	no	▼
IKE Protocol	IKEv1	▼
IKE Mode	main	▼
IKE Algorithm	auto	▼
IKE Encryption	3DES	▼
IKE Hash	MD5	▼
IKE DH Group	2	▼
IKE Reauthentication	yes	▼
XAUTH Enabled	no	▼
XAUTH Mode	client	▼
XAUTH Username	<input type="text"/>	
XAUTH Password	<input type="text"/>	
ESP Algorithm	auto	▼
ESP Encryption	DES	▼
ESP Hash	MD5	▼
PFS	disabled	▼
PFS DH Group	2	▼
Key Lifetime	3600	sec
IKE Lifetime	3600	sec
Rekey Margin	540	sec
Rekey Fuzz	100	%
DPD Delay *	<input type="text"/>	sec
DPD Timeout *	<input type="text"/>	sec
Authenticate Mode	pre-shared key	▼
Pre-shared Key	<input type="text"/>	
CA Certificate	<input type="text"/>	
Remote Certificate / PubKey	<input type="text"/>	
Local Certificate / PubKey	<input type="text"/>	
Local Private Key	<input type="text"/>	
Local Passphrase *	<input type="text"/>	
Debug	control	▼
* can be blank		

Figure 33: IPsec Tunnels Configuration

Example of the IPsec tunnel configuration:

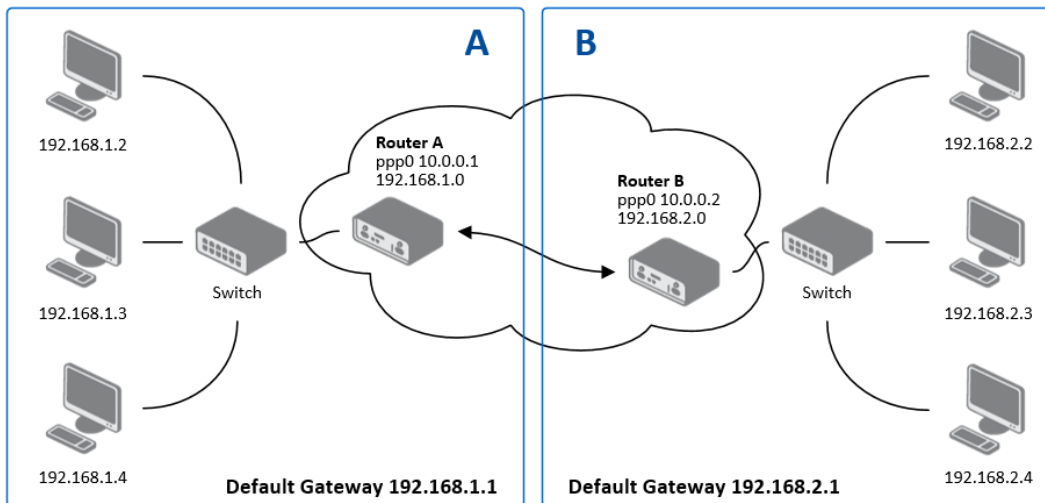



Figure 34: Topology of IPsec Configuration Example

IPsec tunnel configuration:

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

Table 33: Example IPsec configuration

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

4.11 GRE Tunnels Configuration

GRE is an unencrypted protocol.



To open the *GRE Tunnel Configuration* page, click *GRE* in the *Configuration* section of the main menu. The menu item will expand and you will see four separate configuration pages: *1st Tunnel*, *2nd Tunnel*, *3rd Tunnel* and *4th Tunnel*. The GRE tunnel function allows you to create an unencrypted connection between two separate LAN networks. The router allows you to create four GRE tunnels.

Item	Description
Description	Description of the GRE tunnel.
Remote IP Address	IP address of the remote side of the tunnel.
Remote Subnet	IP address of the network behind the remote side of the tunnel.
Remote Subnet Mask	Specifies the mask of the network behind the remote side of the tunnel.
Local Interface IP Address	IP address of the local side of the tunnel.
Remote Interface IP Address	IP address of the remote side of the tunnel.
Multicasts	Activates/deactivates sending multicast into the GRE tunnel: <ul style="list-style-type: none"> • disabled – Sending multicast into the tunnel is inactive. • enabled – Sending multicast into the tunnel is active.
Pre-shared Key	Specifies an optional value for the 32 bit shared key in numeric format, with this key the router sends the filtered data through the tunnel. Specify the same key on both routers, otherwise the router drops received packets.

Table 34: GRE Tunnel Configuration

The GRE tunnel cannot pass through the NAT.



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

1st GRE Tunnel Configuration

Create 1st GRE tunnel

Description *

Remote IP Address

Remote Subnet *

Remote Subnet Mask *

Local Interface IP Address *

Remote Interface IP Address *

Multicasts disabled ▼

Pre-shared Key *

* can be blank

Figure 35: GRE Tunnel Configuration

4.11.1 Example of the GRE Tunnel Configuration

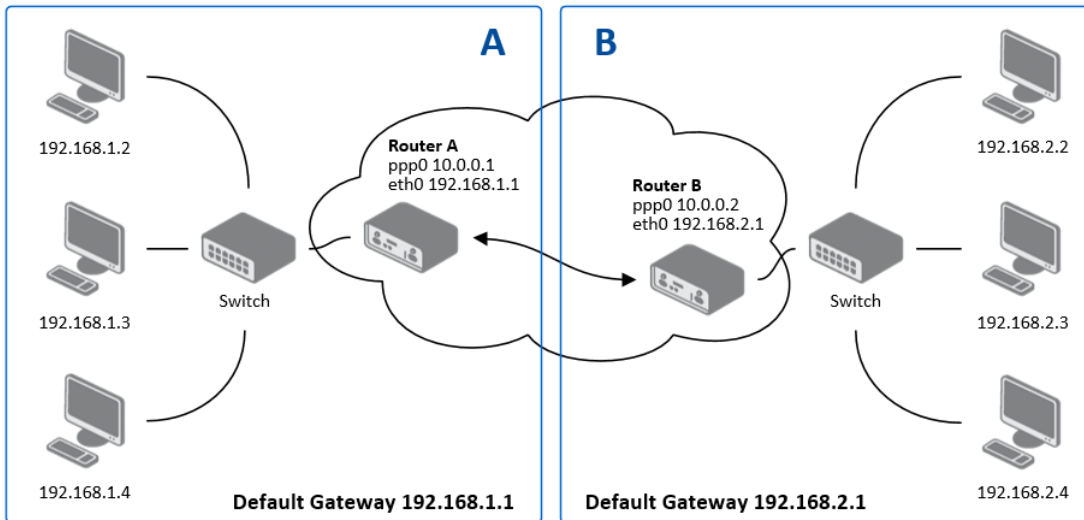


Figure 36: Topology of GRE Tunnel Configuration Example

GRE tunnel configuration:

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

Table 35: GRE Tunnel Configuration Example

Examples of different options for configuration of GRE tunnel can be found in the "GRE Tunnel" application note. You can download the PDF on the Internet at: <https://www.doc.hirschmann.com>.



4.12 L2TP Tunnel Configuration



L2TP is an unencrypted protocol.

To open the *L2TP Tunnel Configuration* page, click *L2TP* in the *Configuration* section of the main menu. The L2TP tunnel function allows you to create a password protected connection between 2 LAN networks. Enable the *Create L2TP tunnel* checkbox to activate the tunnel.

Item	Description
Mode	Specifies the L2TP tunnel mode on the router side: <ul style="list-style-type: none"> ● L2TP server – Specify an IP address range offered by the server. ● L2TP client – Specify the IP address of the server.
Server IP Address	IP address of the server.
Client Start IP Address	IP address to start with in the address range. The range is offered by the server to the clients.
Client End IP Address	The last IP address in the address range. The range is offered by the server to the clients.
Local IP Address	IP address of the local side of the tunnel.
Remote IP Address	IP address of the remote side of the tunnel.
Remote Subnet	Address of the network behind the remote side of the tunnel.
Remote Subnet Mask	The mask of the network behind the remote side of the tunnel.
Username	Username for the L2TP tunnel login.
Password	Password for the L2TP tunnel login. Enter valid characters only.

Table 36: L2TP Tunnel Configuration

L2TP Tunnel Configuration

Create L2TP tunnel

Mode: L2TP client

Server IP Address:

Client Start IP Address:

Client End IP Address:

Local IP Address *:

Remote IP Address *:

Remote Subnet *:

Remote Subnet Mask *:

Username:

Password:

* can be blank

Figure 37: L2TP Tunnel Configuration

4.12.1 Example of the L2TP Tunnel Configuration

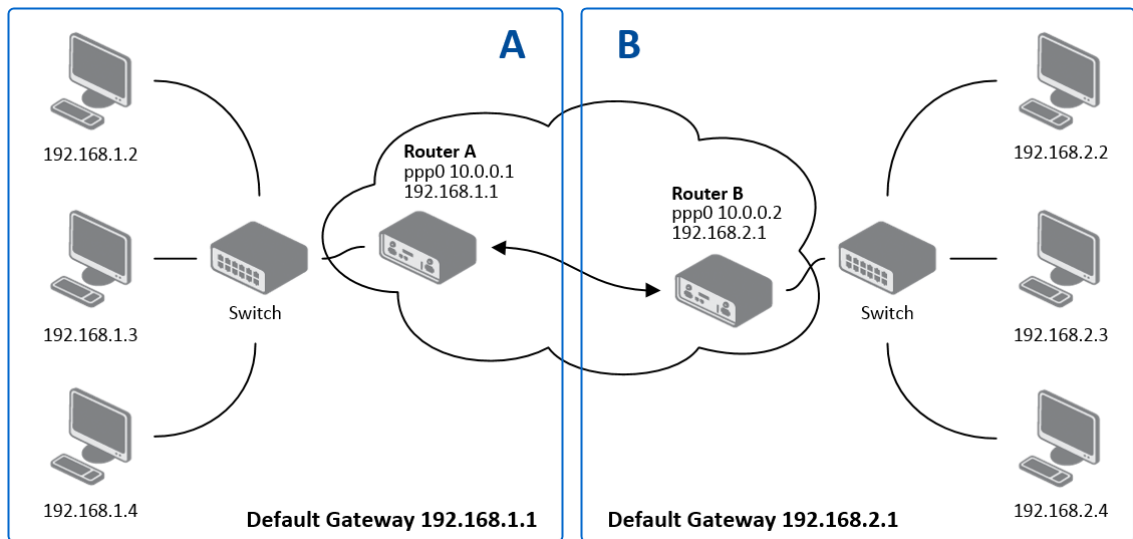


Figure 38: Topology of L2TP Tunnel Configuration Example

Configuration of the L2TP tunnel:

Configuration	A	B
Mode	L2TP Server	L2TP Client
Server IP Address	—	10.0.0.1
Client Start IP Address	192.168.2.5	—
Client End IP Address	192.168.2.254	—
Local IP Address	192.168.1.1	—
Remote IP Address	—	—
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Username	username	username
Password	password	password

Table 37: L2TP Tunnel Configuration Example

4.13 PPTP Tunnel Configuration



PPTP is an unencrypted protocol.

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

Item	Description
Mode	Specifies the L2TP tunnel mode on the router side: <ul style="list-style-type: none"> • PPTP server – Specify an IP address range offered by the server. • PPTP client – Specify the IP address of the server.
Server IP Address	IP address of the server.
Local IP Address	IP address of the local side of the tunnel.
Remote IP Address	IP address of the remote side of the tunnel.
Remote Subnet	Address of the network behind the remote side of the tunnel.
Remote Subnet Mask	The mask of the network behind the remote side of the tunnel
Username	Username for the PPTP tunnel login.
Password	Password for the PPTP tunnel login. Enter valid characters only.

Table 38: PPTP Tunnel Configuration

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

Figure 39: PPTP Tunnel Configuration



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

4.13.1 Example of the PPTP Tunnel Configuration

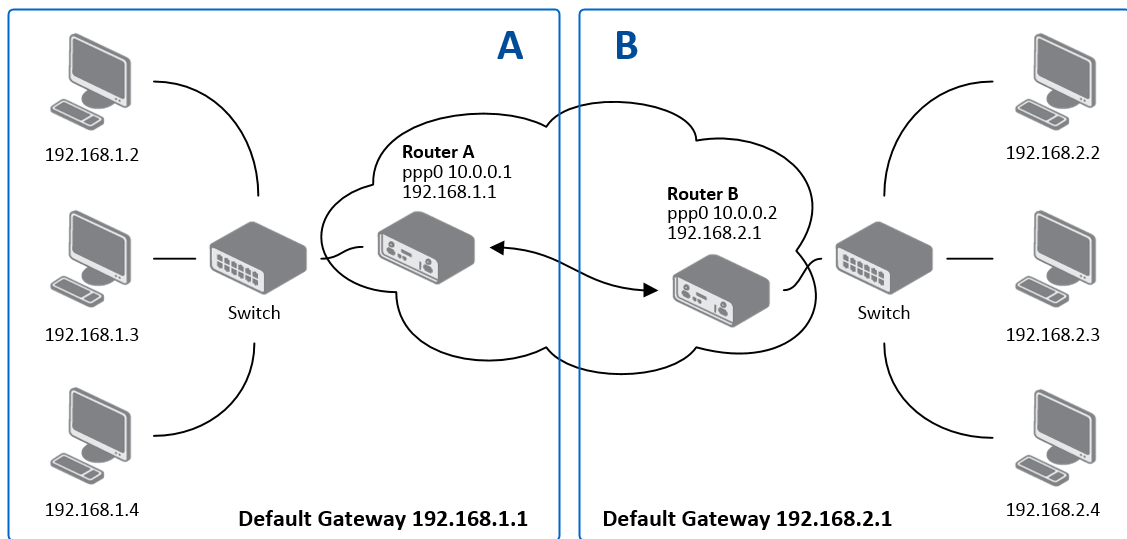


Figure 40: Topology of PPTP Tunnel Configuration Example

Configuration of the PPTP tunnel:

Configuration	A	B
Mode	PPTP Server	PPTP Client
Server IP Address	—	10.0.0.1
Local IP Address	192.168.1.1	—
Remote IP Address	192.168.2.1	—
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Username	username	username
Password	password	password

Table 39: PPTP Tunnel Configuration Example

4.14 Services

4.14.1 DynDNS

The DynDNS function allows you to access the router remotely using an easy to remember custom hostname. This DynDNS client monitors the IP address of the router and updates the address whenever it changes. In order for DynDNS to function, you require a public IP address, either static or dynamic, and an active Remote Access service account at www.dyndns.org. Register the custom domain (third-level) and account information specified in the configuration form. You can use other services, too – see the table below, Server item. To open the *DynDNS Configuration* page, click *DynDNS* in the main menu.

Item	Description
Hostname	The third order domain registered on the www.dyndns.org server.
Username	Username for logging into the DynDNS server.
Password	Password for logging into the DynDNS server. Enter valid characters only.
Server	Specifies a DynDNS service other than the www.dyndns.org . Possible other services: www.spdns.de www.dnsdynamic.org www.noip.com Enter the update server service information in this field. If you leave this field blank, the default server members.dyndns.org will be used.

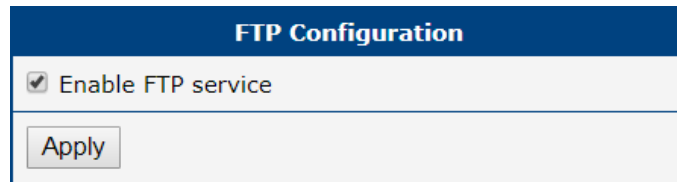
Table 40: DynDNS Configuration



To access the router's configuration remotely, you will need to have enabled this option in the NAT configuration (bottom part of the form), see chapter 4.8.

4.14.2 FTP

FTP protocol (File Transfer Protocol) can be used to transfer files between the router and another device on the computer network. Configuration form of TP server can be done in *FTP* configuration page under *Services* menu item. By ticking *Enable FTP service* item the FTP server on the router is enabled.



FTP Configuration	
<input checked="" type="checkbox"/>	Enable FTP service
<input type="button" value="Apply"/>	

Figure 41: Enabling of FTP server

4.14.3 HTTP

HTTP protocol (Hypertext Transfer Protocol) is internet protocol used for exchange of hyper-text documents in HTML format. This protocol is used for accessing the web server used for user’s configuration of the router. Recommended usage however is of HTTPS protocol, which used encryption for secure exchange of transferred data. Configuration form of HTTP and HTTPS service can be done in *HTTP* configuration page under *Services* menu item. By default, HTTP service is disabled and preferred is using of HTTPS service. For this default setting, a request for communication with HTTP protocol is redirected to HTTPS protocol automatically.

Item	Description
Enable HTTP service	Enabling of HTTP service.
Enable HTTPS service	Enabling of HTTPS service.
Session Timeout	Inactivity timeout when the session is closed.
Keep the current certificate	Left the current one certificate in the router.
Generate a new certificate	Generate a new self-signed certificate to the router.
Upload a new certificate	Upload custom PEM certificate, which can be signed by Certificate Authority.
Certificate	Choose a file with the PEM certificate.
Private Key	Choose a file with the certificate private key.

Table 41: Parameters for HTTP and HTTPS services configuration

HTTP Configuration

Enable HTTP service

Enable HTTPS service

Session Timeout sec

Keep the current certificate

Generate a new certificate

Upload a new certificate

Certificate No file chosen

Private Key No file chosen

Figure 42: Configuration of HTTP and HTTPS services

4.14.4 NTP

The *NTP* configuration form allows you to configure the NTP client. To open the *NTP* page, click *NTP* in the *Configuration* section of the main menu. NTP (Network Time Protocol) allows you to periodically set the internal clock of the router. The time is set from servers that provide the exact time to network devices.

- If you mark the *Enable local NTP service* check box, then the router acts as a NTP server for other devices in the local network (LAN).
- If you mark the *Synchronize clock with NTP server* check box, then the router acts as a NTP client. This means that the router automatically adjusts the internal clock every 24 hours.

Item	Description
Primary NTP Server Address	IP or domain address of primary NTP server.
Secondary NTP Server Address	IP or domain address of secondary NTP server.
Timezone	Specifies the time zone where you installed the router.
Daylight Saving Time	Activates/deactivates the DST shift. <ul style="list-style-type: none"> • No – The time shift is inactive. • Yes – The time shift is active.

Table 42: NTP Configuration

The figure below displays an example of a NTP configuration with the primary server set to `ntp.cesnet.cz` and the secondary server set to `tik.cesnet.cz` and with the automatic change for daylight saving time enabled.

NTP Configuration

Enable local NTP service
 Synchronize clock with NTP server
 Primary NTP Server
 Secondary NTP Server
 Timezone
 Daylight Saving Time

Figure 43: Example of NTP Configuration

4.14.5 PAM

A pluggable authentication module (PAM) is a mechanism to integrate multiple low-level authentication schemes into a high-level application programming interface (API). The configuration made on this configuration page will affect all the router’s authentication mechanisms. The modes available for PAM authentication are listed in the table below.

Item	Description
PAM Mode	<p>local user database – Authenticate against the local user database only.</p> <p>RADIUS with fallback – Authenticate against the RADIUS server and then against the local database in case the RADIUS server is not accessible.</p> <p>RADIUS only – Authenticate only against the RADIUS server. Note that you will not be able to authenticate to the router in case the RADIUS server is not accessible!</p> <p>TACACS+ with fallback – Authenticate against the TACACS+ server and then against the local database in case the TACACS+ server is not accessible.</p> <p>TACACS+ only – Authenticate only against the TACACS+ server. Note that you will not be able to authenticate to the router in case the TACACS+ server is not accessible!</p>

Table 43: Available Modes of PAM

To configure the authentication against a RADIUS server, choose *RADIUS with fallback* or *RADIUS only* as of the PAM mode and set up all required items.

PAM Configuration

Mode RADIUS with fallback ▼

RADIUS Server(s)

	Server	Port *	Secret	Timeout *
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/> sec
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/> sec

Take Over Server Users Disabled ▼

Default User Role Admin ▼

Debug Disabled ▼

* can be blank

Figure 44: Configuration of RADIUS

Item	Description
Server	Address of the RADIUS server. Up to two servers can be configured.
Port	Port of the RADIUS server.
Secret	The secret to verify the user's identity.
Timeout	Timeout for authentication to the RADIUS server.
Take Over Server Users	If enabled, a new user account is created during the login, in case the RADIUS authentication is successful and appropriate local account does not exist. New accounts are created without the password. An existing user account with a password is never modified by this feature.
Default User Role	Choose the default user role (<i>Admin</i> or <i>User</i>).
Debug	Enables or disables the logging of the RADIUS debug information into the System Log.

Table 44: Configuration of RADIUS

To configure the authentication against a TACACS+ server, choose *TACACS+ with fallback* or *TACACS+ only* as of the PAM mode and set up all required items.

PAM Configuration

Mode	<input type="text" value="TACACS+ with fallback"/>		
TACACS+ Server(s)			
Authentication Type	<input type="text" value="ASCII"/>		
Timeout *	<input type="text"/> sec		
	Server	Port *	Secret
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Take Over Server Users	<input type="text" value="Disabled"/>		
Default User Role	<input type="text" value="Admin"/>		
Debug	<input type="text" value="Disabled"/>		
* can be blank			
<input type="button" value="Apply"/>			

Figure 45: Configuration of TACACS+

Item	Description
Authentication Type	Choose ASCII, PAP or CHAP as authentication type.
Timeout	Timeout for authentication to the TACACS+ server.
Server	Address of the TACACS+ server. Up to two servers can be configured.
Port	Port of the TACACS+ server.
Secret	The secret to verify the user's identity.
Take Over Server Users	If enabled, a new user account is created during the login, in case the RADIUS authentication is successful and appropriate local account does not exist. New accounts are created without the password. An existing user account with a password is never modified by this feature.
Default User Role	Choose the default user role (<i>Admin</i> or <i>User</i>).
Debug	Enables or disables the logging of the TACACS+ debug information into the System Log.

Table 45: Configuration of TACACS+

4.14.6 SNMP

The *SNMP* page allows you to configure the SNMP v1/v2 or v3 agent which sends information about the router to a management station. To open the *SNMP* page, click *SNMP* in the *Configuration* section of the main menu. SNMP (Simple Network Management Protocol) provides status information about the network elements such as routers or endpoint computers. In the version v3, the communication is secured (encrypted). To enable the SNMP service, mark the *Enable the SNMP agent* check box. Sending SNMP traps to IPv6 address is supported.

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

Table 46: SNMP Agent Configuration

To enable the SNMPv1/v2 function, mark the *Enable SNMPv1/v2 access* check box. It is also necessary to specify a password for access to the *Community* SNMP agent. The default setting is *public*.

You can define a different password for the *Read* community (read only) and the *Write* community (read and write) for SNMPv1/v2. You can also define 2 SNMP users for SNMPv3. You can define a user as read only (*Read*), and another as read and write (*Write*). The router allows you to configure the parameters in the following table for every user separately. The router uses the parameters for SNMP access only.

To enable the SNMPv3 function, mark the *Enable SNMPv3 access* check box, then specify the following parameters:

Item	Description
Username	User name
Authentication	Encryption algorithm on the Authentication Protocol that is used to verify the identity of the users.
Authentication Password	Password used to generate the key used for authentication. Enter valid characters only, see chap. ??!
Privacy	Encryption algorithm on the Privacy Protocol that is used to ensure confidentiality of data.
Privacy Password	Password for encryption on the Privacy Protocol. Enter valid characters only, see chap. ??!

Table 47: SNMPv3 Configuration

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

Item	Description
IP Address	IPv4 or IPv6 address.
Period	Period of sending statistical information (in minutes).

Table 48: SNMP Configuration (R-SeeNet)

Each monitored value is uniquely identified using a numerical identifier *OID* – *Object Identifier*. This identifier consists of a progression of numbers separated by a point. The shape of each OID is determined by the identifier value of the parent element and then this value is complemented by a point and current number. So it is obvious that there is a tree structure. The following figure displays the basic tree structure that is used for creating the OIDs.

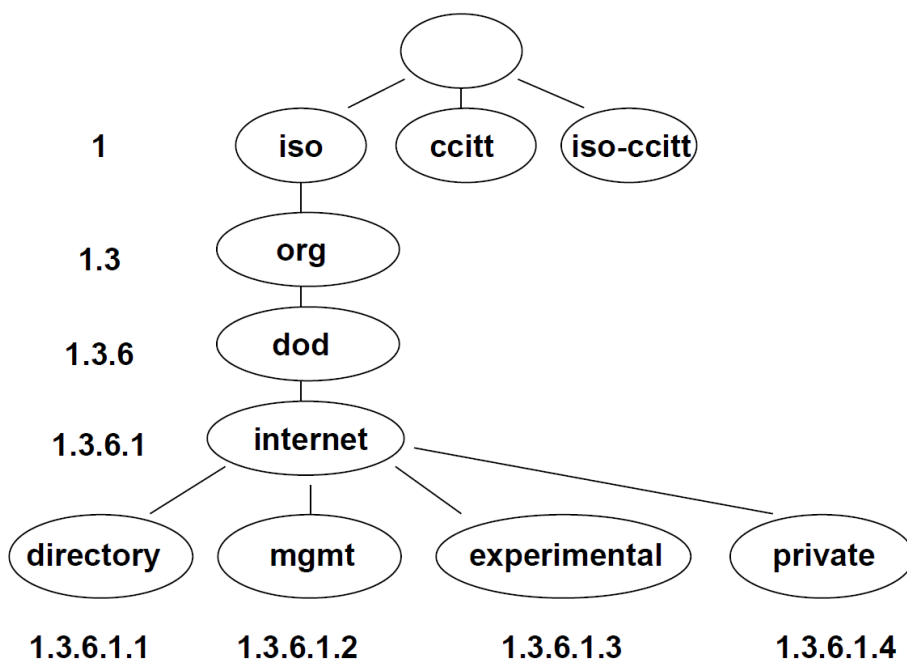


Figure 46: OID Basic Structure

The SNMP values that are specific for Hirschmann routers create the tree starting at $OID = .1.3.6.1.4.1.248$. You interpret the OID in the following manner:

iso.org.dod.internet.private.enterprises.hirschmann



The list of available and supported OIDs and other details can be found in the "SNMP Object Identifier" application note. You can download the PDF on the Internet at: <https://www.doc.hirschmann.com>.

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

Figure 47: SNMP Configuration Example

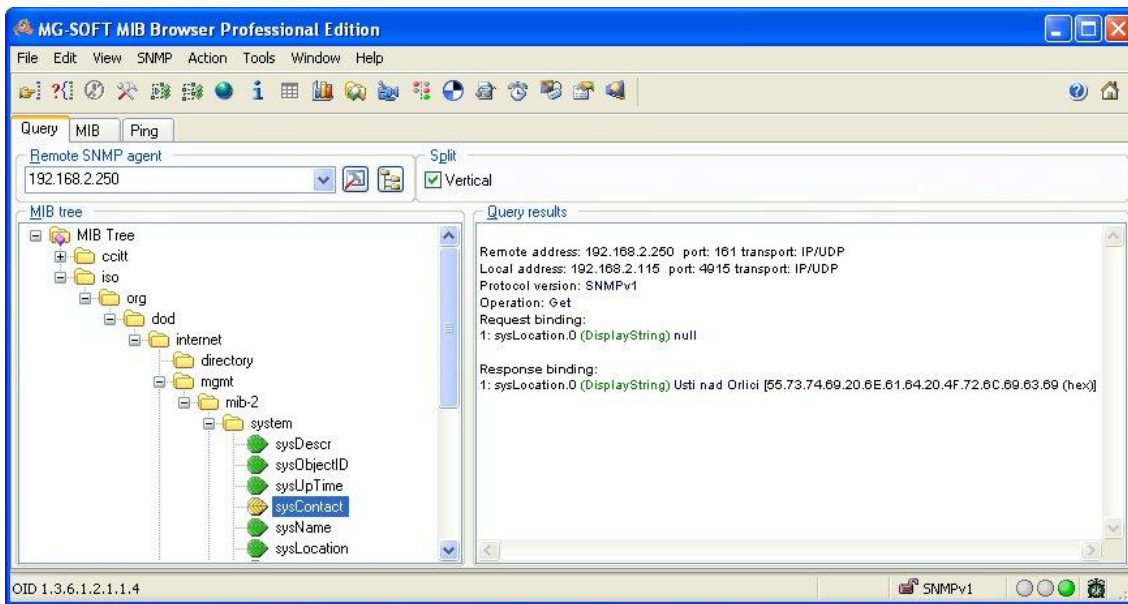


Figure 48: MIB Browser Example

In order to access a particular device enter the IP address of the SNMP agent which is the router, in the *Remote SNMP agent* field. The dialog displayed the internal variables in the MIB tree after entering the IP address. Furthermore, you can find the status of the internal variables by entering their OID.

The path to the objects is:

iso → org → dod → internet → private → enterprises → hirschmann → hmWanMib → hmWanMgmt

The path to information about the router is:


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

4.14.7 SMTP

You use the *SMTP* form to configure the Simple Mail Transfer Protocol client (SMTP) for sending e-mails.

Item	Description
SMTP Server Address	IP or domain address of the mail server.
SMTP Port	Port the SMTP server is listening on.
Secure Method	none, SSL/TLS, or STARTTLS. Secure method has to be supported by the SMTP server.
Username	Name for the e-mail account.
Password	Password for the e-mail account. Enter valid characters only.
Own E-mail Address	Address of the sender.

Table 49: SMTP client configuration

The mobile service provider can block other SMTP servers, then you can only use the SMTP server of the service provider. 

SMTP Configuration

SMTP Server Address	<input style="width: 90%;" type="text" value="smtp.domain.com"/>
SMTP Port	<input style="width: 90%;" type="text" value="465"/>
Secure Method	<input style="border-bottom: 1px solid #ccc;" type="text" value="SSL/TLS"/>
Username	<input style="width: 90%;" type="text" value="username"/>
Password	<input style="width: 90%;" type="password" value="....."/>
Own Email Address	<input style="width: 90%;" type="text" value="name@domain.com"/>

Figure 49: SMTP Client Configuration Example

You send e-mails from the Startup script. The *Startup Script* dialog is located in the *Configuration* section of the main menu. The router also allows you to send e-mails using an SSH connection. Use the email command with the following parameters:

- t e-mail address of the receiver
- s subject, enter the subject in quotation marks
- m message, enter the subject in quotation marks
- a attachment file
- r number of attempts to send e-mail (default setting: 2)



Commands and parameters can be entered only in lowercase.

Example of sending an e-mail:

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

The command above sends an e-mail address to *name@domain.com* with the subject "*subject*", body message "*message*" and attachment "*abc.doc*" directly from the directory *c:\directory*. The router attempts to send the message five times.

4.14.8 SMS

Open the *SMS Configuration* page, click *SMS* in the *Configuration* section of the main menu. The router can automatically send SMS messages to a cell phone or SMS message server when certain events occur. The form allows you to select which events generate an SMS message.

Item	Description
Send SMS on power up	Activates/deactivates the sending of an SMS message automatically on power up.
Send SMS on connect to mobile network	Activates/deactivates the sending of an SMS message automatically when the router is connected to a mobile network.
Send SMS on disconnect to mobile network	Activates/deactivates the sending of an SMS message automatically when the router is disconnection from a mobile network.
Send SMS when datalimit exceeded	Activates/deactivates the sending of an SMS message automatically when the data limit exceeded.
Add timestamp to SMS	Activates/deactivates the adding a time stamp to the SMS messages. This time stamp has a fixed format YYYY-MM-DD hh:mm:ss.
Phone Number 1	Specifies the phone number to which the router sends the generated SMS.
Phone Number 2	Specifies the phone number to which the router sends the generated SMS.
Phone Number 3	Specifies the phone number to which the router sends the generated SMS.
Unit ID	The name of the router. The router sends the name in the SMS.

Table 50: SMS Configuration

Remote Control via SMS

After you enter a phone number in the *Phone Number 1* field, the router allows you to configure the control of the device using an SMS message. You can configure up to three numbers for incoming SMS messages. To enable the function, mark the *Enable remote control via SMS* check box. The default setting of the remote control function is active.

Item	Description
Phone Number 1	Specifies the first phone number allowed to access the router using an SMS.
Phone Number 2	Specifies the second phone number allowed to access the router using an SMS.
Phone Number 3	Specifies the third phone number allowed to access the router using an SMS.

Table 51: Control via SMS



- If you enter one or more phone numbers, then you can control the router using SMS messages sent only from the specified phone numbers.
- If you enter the wild card character *, then you can control the router using SMS messages sent from any phone number.

Most of the control SMS messages do not change the router configuration. For example, if the router is changed to the off line mode using an SMS message, the router remains in this mode, but it will return back to the on-line mode after reboot. The only exception is *set profile* command that changes the configuration permanently, see the table below.

To control the router using an SMS, send only message text containing the control command. You can send control SMS messages in the following form:

SMS	Description
go online sim 1	The router changes to SIM1 (APN1)
go online sim 2	The router changes to SIM2 (APN2)
go online	Changes the router to the online mode
go offline	Changes the router to the off line mode
set profile std	Sets the standard profile. This change is permanent.
set profile alt1	Sets the alternative profile 1. This change is permanent.
set profile alt2	Sets the alternative profile 2. This change is permanent.
set profile alt3	Sets the alternative profile 3. This change is permanent.
reboot	The router reboots
get ip	The router responds with the IP address of the SIM card

Table 52: Control SMS

Note: Every received control SMS is processed and then **deleted** from the router! This may cause a confusion when you want to use AT-SMS protocol for reading received SMS (see section below).

Advanced SMS control: If there is unknown command in received SMS and remote control via SMS is enabled, the script located in "/var/scripts/sms" is run before the SMS is deleted. It is possible to define your own additional SMS commands using this script. Maximum of 7 words can be used in such SMS. Since the script file is located in RAM of the router, it is possible to add creation of such file to Startup Script.

AT-SMS Protocol

AT-SMS protocol is a private set of AT commands supported by the routers. It can be used to access the cellular module in the router directly via commonly used AT commands, work with short messages (send SMS) and cellular module state information and settings.

Setting the parameters in the *Enable AT-SMS protocol over TCP* frame, you can enable the router to use AT-SMS protocol on a TCP port. This function requires you to specify a TCP port number. The router sends SMS messages using a standard AT command.

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

Table 53: Send SMS on ethernet PORT1 configuration

If you establish a connection to the router using a serial interface or Ethernet (TCP), then you can use AT commands to manage SMS messages.

Only the commands supported by the routers are listed in the following table. For other AT commands the OK response is always sent. There is no support for treatment of complex AT commands, so in such a case the router sends ERROR response.

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

Continued on next page

Continued from previous page

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

Table 54: List of AT Commands

Sending SMS from Router

There are more ways how to send your own SMS from the router:

- Using AT-SMS protocol described above – if you establish a connection to the router using a serial interface or Ethernet (TCP), then you can use AT commands to send and manage SMS messages.
- Using HTTP POST method for a remote execution, calling CGI scripts in the router.
- From Web interface of the router, in *Administration* section, *Send SMS* item, see 6.8 Chapter.
- Using `gsmsms` command e.g. in terminal when connected to the router via SSH.

Examples of SMS Configuration

Example 1: SMS sending configuration.

After powering up the router, the phone with the number entered in the dialog receives an SMS in the following form:

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

After connecting to mobile network, the phone with the number entered in the dialog receives an SMS in the following form:

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

After disconnecting from the mobile network, the phone with the number entered in the dialog receives an SMS in the following form:

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

SMS Configuration

- Send SMS on power up
- Send SMS on connect to mobile network
- Send SMS on disconnect from mobile network
- Send SMS when datalimit is exceeded
- Add timestamp to SMS

Phone Number 1

Phone Number 2

Phone Number 3

Unit ID *

- Enable remote control via SMS

Phone Number 1

Phone Number 2

Phone Number 3

- Enable AT-SMS protocol over TCP

TCP Port

** can be blank*

Figure 50: Example 1 – SMS Configuration

Example 2: Control the router using an SMS from any phone number.

SMS Configuration

- Send SMS on power up
- Send SMS on connect to mobile network
- Send SMS on disconnect from mobile network
- Send SMS when datalimit is exceeded
- Add timestamp to SMS

Phone Number 1

Phone Number 2

Phone Number 3

Unit ID *

- Enable remote control via SMS

Phone Number 1

Phone Number 2

Phone Number 3

- Enable AT-SMS protocol over TCP

TCP Port

** can be blank*

Figure 51: Example 2 – SMS Configuration

Example 3: Control the router using an SMS from two phone numbers.

SMS Configuration

- Send SMS on power up
- Send SMS on connect to mobile network
- Send SMS on disconnect from mobile network
- Send SMS when datalimit is exceeded
- Add timestamp to SMS

Phone Number 1

Phone Number 2

Phone Number 3

Unit ID *

- Enable remote control via SMS

Phone Number 1

Phone Number 2

Phone Number 3

- Enable AT-SMS protocol over TCP

TCP Port

** can be blank*

Figure 52: Example 3 – SMS Configuration

4.14.9 SSH

SSH protocol (Secure Shell) allows to carry out a secure remote login to the router. Configuration form of SSH service can be done in *SSH* configuration page under *Services* menu item. By ticking *Enable SSH service* item the SSH server on the router is enabled.

Item	Description
Enable SSH service	Enabling of SSH service.
Session Timeout	Inactivity timeout when the session is closed.

Table 55: Parameters for SSH service configuration

SSH Configuration

Enable SSH service

Session Timeout sec

Figure 53: Configuration of HTTP service

4.14.10 Syslog

Configuration of system log, called syslog, can be done on this configuration page. Size of this log can be restricted by maximal number of its rows. Optionally, the IP address and UDP port can be configured for the real-time log distribution.

Položka	Popis
Log Size	Log size restriction by maximal number of its rows.
Remote IP Address	Optional settings of IP address for real-time log distribution.
Remote UDP Port	Optional settings of UDP port for real-time log distribution.

Table 56: Syslog configuration

Syslog Configuration	
Log Size	<input type="text" value="1000"/> lines
Remote IP Address	<input type="text"/>
Remote UDP Port	<input type="text" value="514"/>
<input type="button" value="Apply"/>	

Figure 54: Syslog configuration

4.14.11 Telnet

Telnet is a protocol used to provide a bidirectional interactive text-oriented communication facility with the router. Configuration form of Telnet service can be done in *Telnet* configuration page under *Services* menu item. By ticking *Enable Telnet service* item the Telnet server on the router is enabled.



Telnet Configuration	
<input checked="" type="checkbox"/>	Enable Telnet service
<input type="button" value="Apply"/>	

Figure 55: Enabling of Telnet service

4.15 Scripts

There is possibility to create your own shell scripts executed in the specific situations. Go to the *Scripts* page in the *Configuration* section in the menu. The menu item will expand and there are *Startup Script* and *Up/Down* scripts you can use.

4.15.1 Startup Script

Use the *Startup Script* window to create your own scripts which will be executed after all of the initialization scripts are run – right after the router is turned on or rebooted. The changes in settings will apply after pressing the *Apply* button.



Any changes to the *Startup Script* will take effect the next time the router is power cycled or rebooted. This can be done with the *Reboot* button in the *Administration* section, or by SMS message.

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

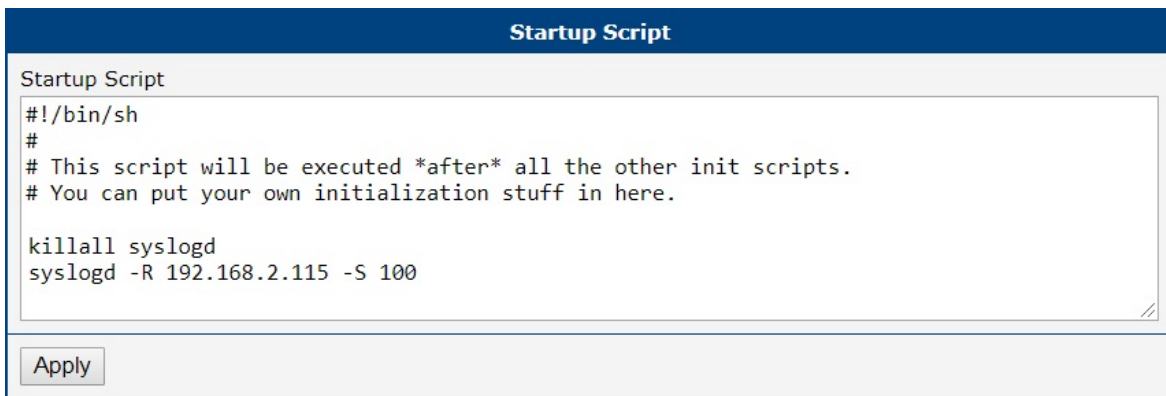


Figure 56: Example of a Startup Script

4.15.2 Up/Down Script

Use the *Up/Down* page to create scripts executed when the Mobile WAN connection is established (up) or lost (down). *Up/Down Script* runs only on the WAN connection established or lost. Any scripts entered into the *Up Script* window will run after a WAN connection is established. Script commands entered into the *Down Script* window will run when the WAN connection is lost.

The changes in settings will apply after pressing the *Apply* button. Also you need to reboot the router to make Up/Down Script work.

Example of Up/Down Script: After establishing or losing the WAN connection (connection to mobile network), the router sends an email with information about the connection state. It is necessary to configure *SMTP* before.

Up/Down Script

Up Script

```
#!/bin/sh
#
# This script will be executed when PPP/WAN IPv6 connection is established.

email -t name@domain.com -s "Router Notification" -m "Connection is established."
```

Down Script

```
#!/bin/sh
#
# This script will be executed when PPP/WAN IPv6 connection is lost.

email -t name@domain.com -s "Router Notification" -m "Connection is lost."
```

Figure 57: Example of Up/Down Script

4.16 Automatic Update Configuration

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

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

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

Item	Description
Source	Select the location of the update files: <ul style="list-style-type: none"> • HTTP(S)/FTP(S) server – Updates are downloaded from the Base URL address below. Used protocol is specified by that address: HTTP, HTTPS, FTP or FTPS (only implicit mode is supported). • USB flash drive – The router finds the current firmware or configuration in the root directory of the connected USB device. • Both – Looking for the current firmware or configuration from both sources.
Base URL	Base URL or IP address from which the configuration file will be downloaded. This option also specifies the communication protocol (HTTP, HTTPS, FTP or FTPS), see examples below.
Unit ID	Name of configuration (name of the file without extension). If the <i>Unit ID</i> is not filled, the MAC address of the router is used as the filename (the delimiter colon is used instead of a dot.)
Decryption Password	Password for decryption of crypted configuration file. This is required only in case the configuration is encrypted.
Update Window Start	Choose an hour (range from 1 to 24) when the automatic update will be performed on a daily basis. If the time is not specified (set to <i>dynamic</i>), the automatic update is performed five minutes after router boots up and then regularly every 24 hours.
Update Window Length	This value defines the period within the update will be done. This period starts at the time set in the <i>Update Window Start</i> field. The exact time, when the update will be done, is generated randomly.

Table 57: Automatic Update Configuration

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

The **firmware file** name consists of *Base URL*, type of router and *bin* extension. For the proper firmware filename, see the *Update Firmware* page in *Administration* section – it is written out there. See Chapter 6.11.

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



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



The automatic update feature is also executed five minutes after the firmware upgrade, regardless of the scheduled time.



5 Customization

5.1 User Modules

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

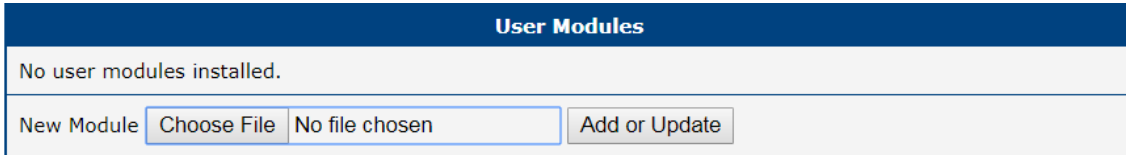


Figure 58: User modules

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

Updating a module is done the same way. Click the *Add* button and the module with the higher (newer) version will replace the existing module. The current module configuration is left in the same state.



Programming and compiling of modules is described in the "Programming of User Modules" application note. You can get the PDF at: <https://hirschmann-support.belden.com>.

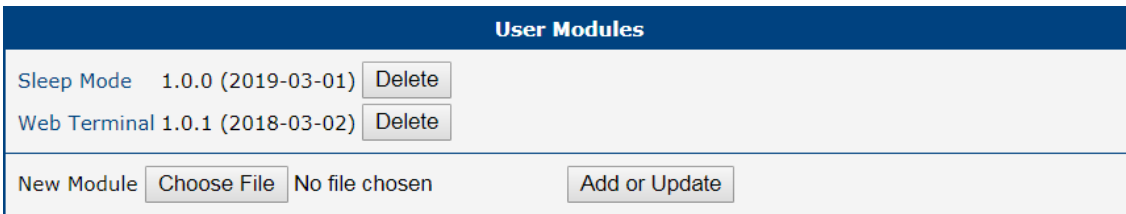


Figure 59: Added user module

User modules can be custom-programmed. Some typical user modules are prepared by the manufacturer and are available on the web site for the download. Here are a few examples of the user modules that are available on the web site.

Module name	Description
MODBUS TCP2RTU	Provides a conversion of MODBUS TCP/IP protocol to MODBUS RTU protocol, which can be operated on the serial line.
Easy VPN client	Provides secure connection of LAN network behind our router with LAN network behind CISCO router.
NMAP	Enables TCP and UDP scan.
Daily Reboot	Enables daily reboot of the router at the specified time.
HTTP Authentication	Adds the process of authentication to a server that doesn't provide this service.
BGP, RIP, OSPF	Adds support of dynamic protocols.
PIM SM	Adds support of multicast routing protocol PIM-SM.
WMBUS Concentrator	Enable the reception of messages from WMBUS meters and saves contents of these messages to an XML file.
pduSMS	Sends short messages (SMS) to specified number.
GPS	Allows the router to provide location and time information in all weather, anywhere on or near the Earth, where there is an unobstructed line of sight to four or more GPS satellites.
Pinger	Allows you to manually or automatically verify the functionality of the connection between two network interfaces (ping).
IS-IS	Adds support of IS-IS protocol.

Table 58: User modules

In some cases the firmware update can cause incompatibility with installed user modules. Some of them are dependent on the version of the Linux kernel (for example *SmsBE* and *PoS Configuration*). It is best to update user modules to the most recent version.



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



6 Administration

6.1 Users



This configuration menu is only available for users with the *admin* role!

For the management of the users, open the *Users* form in the *Administration* section of the main menu. The first part of this configuration form contains an overview of all existing users. The table below describes the meaning of the buttons.

Button	Description
Lock	Locks the user account. This user is not allowed to log in to the router, neither to the web interface or to SSH .
Change Password	Allows you to change the password for the corresponding user. Valid characters are not restricted.
Delete	Deletes the user account.

Table 59: Users Overview



Be careful to not lock all users of the *Admin* role. In this state, any user has access rights to configure the users!

The second part of configuration form allows to add a new user. All items are described in the table below.

Item	Description
Role	Specifies the type of user account: <ul style="list-style-type: none"> • User – user with basic permissions. • Admin – user with enhanced permissions – has full access to the web GUI, access to the router via Telnet, SSH or SFTP. This user has no the same rights as the superuser on Linux-based systems.
Username	Specifies the name of the user having access to log in to the device.
Password	Specifies the password for the user. Valid characters are not restricted.
Confirm Password	Confirms the password.

Table 60: Add User

A user with the *User* role cannot access the router via Telnet, SSH or SFTP. Read-only access to the FTP server is allowed.



User Administration			
root	Admin	Lock	Change Password
test	User	Lock	Change Password Delete
Role	User ▼		
Username	<input type="text"/>		
Password	<input type="password"/>		
Confirm Password	<input type="password"/>		
<input type="button" value="Add User"/>			

Figure 60: Users

6.2 Change Profile

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

Change Profile	
Profile	Standard ▼
<input type="checkbox"/> Copy settings from current profile to selected profile	
<input type="button" value="Apply"/>	

Figure 61: Change Profile

6.3 Change Password

Use the *Change Password* configuration form in the *Administration* section of the main menu for changing your password used to log on the device. Enter the new password in the *New Password* field, confirm the password using the *Confirm Password* field, and press the *Apply* button. Characters for the password are not restricted.



The default password for the **admin** user is printed out on the router's label. To maintain the security of your network change the default password. You can not enable remote access to the router for example, in NAT, until you change the password.

Change Password	
Username	admin
New Password	
Confirm Password	
Apply	

Figure 62: Change Password

6.4 Set Real Time Clock

You can set the internal clock directly using the *Set Real Time Clock* dialog in the *Administration* section of in the main menu. You can set the *Date* and *Time* manually. When entering the values manually use the format yyyy-mm-dd as seen in the figure below. You can also adjust the clock using the specified NTP server. After you enter the appropriate values, click the *Apply* button.

Set Real Time Clock	
Date	2019 - 08 - 20
Time	14 : 45 : 44
NTP Server Address	
Apply	

Figure 63: Set Real Time Clock

6.5 Set SMS Service Center Address

The function requires you to enter the phone number of the SMS service center to send SMS messages. To specify the SMS service center phone number use the *Set SMS Service Center* configuration form in the *Administration* section of the main menu. You can leave the field blank if your SIM card contains the phone number of the SMS service center by default. This phone number can have a value without an international prefix (xxx-xxx-xxx) or with an international prefix (+420-xxx-xxx-xxx). If you are unable to send or receive SMS messages, contact your carrier to find out if this parameter is required.

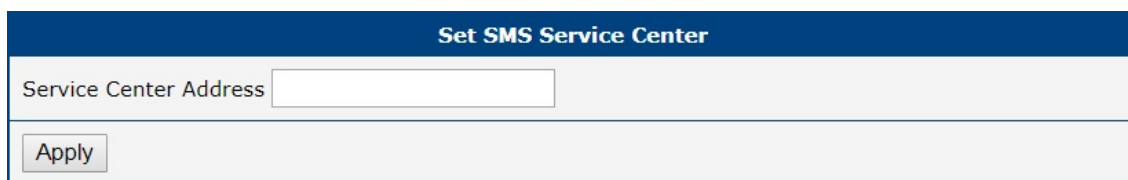


Figure 64: Set SMS Service Center Address

6.6 Unlock SIM Card

It is possible to use the SIM card protected by PIN number in the router – just fill in the PIN on the *Mobile WAN Configuration* page. Here you can remove the PIN protection (4–8 digit Personal Identification Number) from the SIM card, if your SIM card is protected by one. Open the *Unlock SIM Card* form in the *Administration* section of the main menu and enter the PIN number in the *SIM PIN* field, then click the *Apply* button. It is applied on the currently enabled SIM card, or on the first SIM card if there is no SIM card enabled at the moment.

The SIM card is blocked after three failed attempts to enter the PIN code. Unlocking of SIM card by PUK number is described in next chapter.

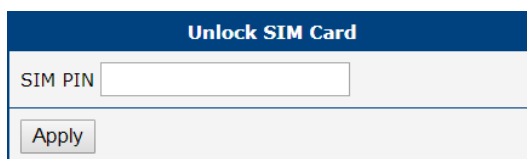


Figure 65: Unlock SIM Card

6.7 Unblock SIM Card

On this page you can unblock the SIM card after 3 wrong PIN attempts or change the PIN code of the SIM card. To unblock the SIM card, go to *Unblock SIM Card* administration page. In both cases enter the PUK code into *SIM PUK* field and new SIM PIN code into *New SIM PIN* field. To proceed click on *Apply* button. It is applied on the currently enabled SIM card, or on the first SIM card if there is no SIM card enabled at the moment.



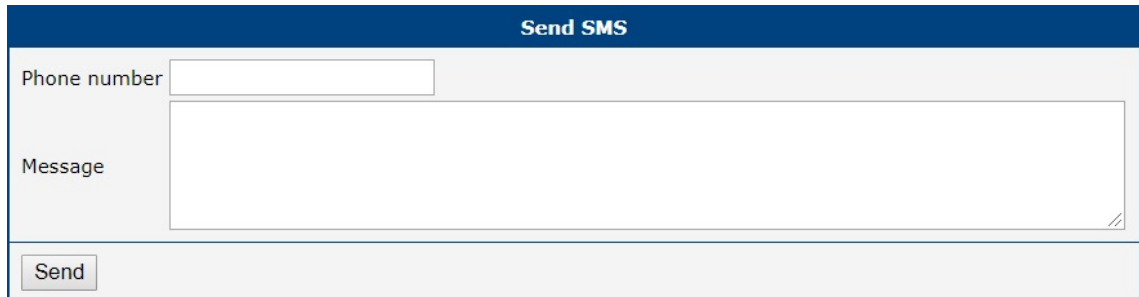
The SIM card will be permanently blocked after the three unsuccessful attempts of the PUK code entering.

Unblock SIM Card	
SIM PUK	<input type="text"/>
New SIM PIN	<input type="text"/>
<input type="button" value="Apply"/>	

Figure 66: Unblock SIM Card

6.8 Send SMS

You can send an SMS message from the router to test the cellular network. Use the *Send SMS* dialog in the *Administration* section of the main menu to send SMS messages. Enter the *Phone number* and text of your message in the *Message* field, then click the *Send* button. The router limits the maximum length of an SMS to 160 characters. (To send longer messages, install the pduSMS user module).



The image shows a web-based dialog box titled "Send SMS". It features a dark blue header with the title in white. Below the header, there are two input fields: "Phone number" (a single-line text box) and "Message" (a multi-line text area). At the bottom left of the dialog, there is a "Send" button. The dialog is set against a light gray background.

Figure 67: Send SMS

6.9 Backup Configuration



Keep in mind potential security issues when creating backup, especially for user accounts. Encrypted configuration or secured connection to the router should be used.

You can save actual configuration of the router using the *Backup Configuration* item in the *Administration* menu section. If you click on this item a configuration pane will open, see Figure 68. Here you can choose what will be backed up. You can back up configuration of the router (item *Configuration*) or configuration of all user accounts (item *Users*). Both types of the configuration can be backed up separately or at once into one configuration file.



It is recommended to save the configuration into an encrypted file. If the encryption password is not configured, the configuration is stored into an unencrypted file.

Click on *Apply* button and the configuration will be stored into configuration file (file with *cfg* extension) into a directory according the settings of the web browser. Stored configuration can be later used for its restoration, see chapter 6.10 for more information.

Backup Configuration	
<input checked="" type="checkbox"/>	Backup configuration
<input type="checkbox"/>	Backup users
Encryption Password *	<input type="text"/>
* can be blank	
<input type="button" value="Save Backup"/>	

Figure 68: Backup Configuration

6.10 Restore Configuration

Due to the different format it is not possible to import user accounts backed up on a router of v1 product line (and older) to a router of v2 product line (and newer). The same limitation is for opposite direction.



You can restore a configuration of the router stored into a file using the *Restore Configuration* form. Click on *Browse* button to navigate to the directory containing the configuration file you wish to load to the router. If the configuration was stored into an encrypted file, the decryption password must be set to decrypt the file successfully. To start the restoration process click on *Apply* button.

Restore Configuration	
Configuration File	<input type="button" value="Choose File"/> No file chosen
Decryption Password *	<input type="text"/>
* can be blank	
<input type="button" value="Apply"/>	

Figure 69: Restore Configuration

6.11 Update Firmware



For security reasons, it is highly recommended to update the firmware of the router to the latest version regularly. Downgrading the firmware to an older version than the production version or uploading a firmware intended for a different device may cause the malfunction of the device.



The firmware update can cause an incompatibility issue with a user module. It is recommended to update all user modules to the most recent version together with the firmware of the router. Information about the user's module compatibility is available at the beginning of the module's Application Note.

Update Firmware administration page shows the current router's firmware version and current firmware name, see Figure 70. On this page, the firmware of the router can be updated as well.

Update Firmware	
Firmware Version :	x.x.x (yyyy-mm-dd)
Firmware Name :	xxx.bin
New Firmware	<input type="button" value="Choose File"/> No file chosen
<input type="button" value="Update"/>	

Figure 70: Update Firmware Administration Page

To load new firmware to the router, click on *Choose File* button, choose the firmware file and press the *Update* button to start the firmware update.

During the firmware update, the router will display messages, as shown in Figure 71. When done, the router will reboot automatically. When rebooted, click the *here* link to re-open the web interface.

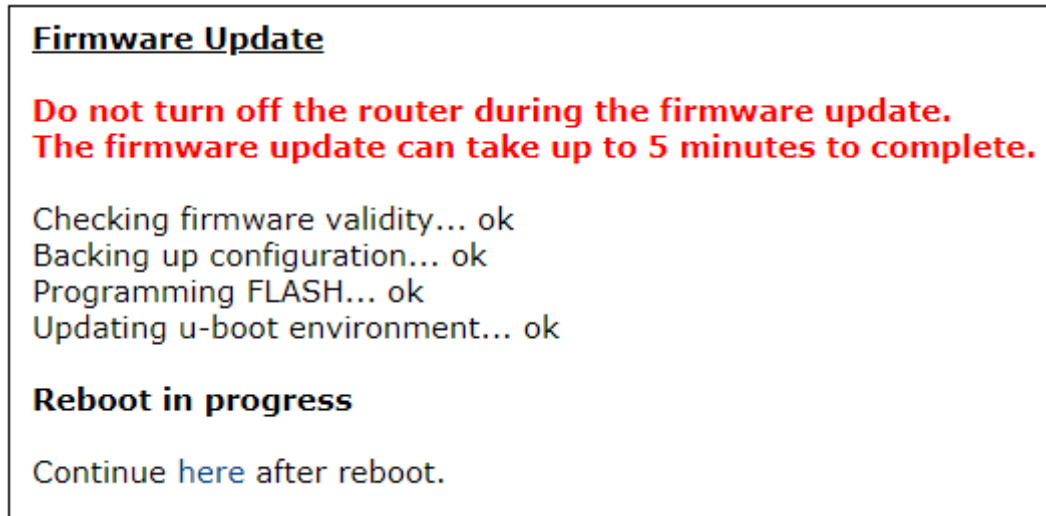


Figure 71: Process of Firmware Update

6.12 Reboot

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

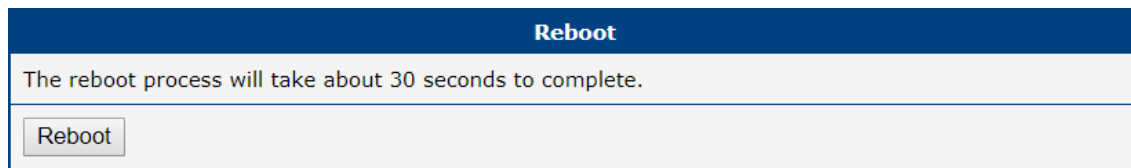


Figure 72: Reboot

6.13 Logout

By clicking the *Logout* menu item, the user is logged out from the web interface.

A Maintenance

Hirschmann is continually working on improving and developing their software. Check regularly whether there is an updated version of the software that provides you with additional benefits. You find information and software downloads on the Hirschmann product pages on the Internet (<http://www.hirschmann.com>).

B Glossary and Acronyms

Backup Routes Allows user to back up the primary connection with alternative connections to the Internet/mobile network. Each backup connection can have assigned a priority. Switching between connections is done based upon set priorities and the state of the connections.

DHCP The Dynamic Host Configuration Protocol (DHCP) is a network protocol used to configure devices that are connected to a network so they can communicate on that network using the Internet Protocol (IP). The protocol is implemented in a client-server model, in which DHCP clients request configuration data, such as an IP address, a default route, and one or more DNS server addresses from a DHCP server.

DHCP client Requests network configuration from [DHCP server](#).

DHCP server Answers configuration request by [DHCP clients](#) and sends network configuration details.

DNS The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for the purpose of locating computer services and devices worldwide. By providing a worldwide, distributed keyword-based redirection service, the Domain Name System is an essential component of the functionality of the Internet.

DynDNS client DynDNS service lets you access the router remotely using an easy to remember custom hostname. This client monitors the router's [IP address](#) and updates it whenever it changes.

GRE Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network. It is possible to create four different tunnels.

HTTP The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.

Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text. HTTP is the protocol to exchange or transfer hypertext.

HTTPS The Hypertext Transfer Protocol Secure (HTTPS) is a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet. Technically, it is not a protocol in and of itself; rather, it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications.

IP address An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterized as follows: *A name indicates what we seek. An address indicates where it is. A route indicates how to get there*

The designers of the Internet Protocol defined an IP address as a 32-bit number and this system, known as Internet Protocol Version 4 ([IPv4](#)), is still in use today. However, due to the enormous growth of the Internet and the predicted depletion of available addresses, a new version of IP ([IPv6](#)), using 128 bits for the address, was developed in 1995.

IP masquerade Kind of [NAT](#).

IP masquerading see [NAT](#).

IPsec Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. The router allows user to select encapsulation mode (tunnel or transport), IKE mode (main or aggressive), IKE Algorithm, IKE Encryp-

tion, ESP Algorithm, ESP Encryption and much more. It is possible to create four different tunnels.

IPv4 The Internet Protocol version 4 (IPv4) is the fourth version in the development of the Internet Protocol (IP) and the first version of the protocol to be widely deployed. It is one of the core protocols of standards-based internetworking methods of the Internet, and routes most traffic in the Internet. However, a successor protocol, [IPv6](#), has been defined and is in various stages of production deployment. IPv4 is described in IETF publication RFC 791 (September 1981), replacing an earlier definition (RFC 760, January 1980).

IPv6 The Internet Protocol version 6 (IPv6) is the latest revision of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace [IPv4](#), which still carries the vast majority of Internet traffic as of 2013. As of late November 2012, IPv6 traffic share was reported to be approaching 1%. IPv6 addresses are represented as eight groups of four hexadecimal digits separated by colons (2001:0db8:85a3:0042:1000:8a2e:0370:7334), but methods of abbreviation of this full notation exist.

L2TP Layer 2 Tunnelling Protocol (L2TP) is a tunnelling protocol used to support virtual private networks ([VPNs](#)) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy.

LAN A local area network (LAN) is a computer network that interconnects computers in a limited area such as a home, school, computer laboratory, or office building using network media. The defining characteristics of LANs, in contrast to wide area networks ([WANs](#)), include their usually higher data-transfer rates, smaller geographic area, and lack of a need for leased telecommunication lines.

NAT In computer networking, Network Address Translation (NAT) is the process of modifying IP

address information in IPv4 headers while in transit across a traffic routing device.

The simplest type of NAT provides a one-to-one translation of IP addresses. RFC 2663 refers to this type of NAT as basic NAT, which is often also called a one-to-one NAT. In this type of NAT only the IP addresses, IP header checksum and any higher level checksums that include the IP address are changed. The rest of the packet is left untouched (at least for basic TCP/UDP functionality; some higher level protocols may need further translation). Basic NATs can be used to interconnect two IP networks that have incompatible addressing.

NAT-T NAT traversal (NAT-T) is a computer networking methodology with the goal to establish and maintain Internet protocol connections across gateways that implement network address translation ([NAT](#)).

NTP Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

OpenVPN OpenVPN implements virtual private network ([VPN](#)) techniques for creating secure point-to-point or site-to-site connections. It is possible to create four different tunnels.

PAT Port and Address Translation (PAT) or Network Address Port Translation (NAPT) see [NAT](#).

Port In computer networking, a Port is an application-specific or process-specific software construct serving as a communications endpoint in a computer's host operating system. A port is associated with an IP address of the host, as well as the type of protocol used for communication. The purpose of ports is to uniquely identify different applications or processes running on a single computer and thereby enable them to share a single physical connection to a packet-switched network like the Internet.

PPTP The Point-to-Point Tunneling Protocol (PPTP) is a tunneling protocol that operates at the Data Link Layer (Layer 2) of the OSI Reference Model. PPTP is a proprietary technique that encapsulates Point-to-Point Protocol (PPP) frames in Internet Protocol (IP) packets using the Generic Routing Encapsulation ([GRE](#)) protocol. Packet filters provide access control, end-to-

end and server-to-server.

RADIUS Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service. Because of the broad support and the ubiquitous nature of the RADIUS protocol, it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services.

Root certificate In cryptography and computer security, a root certificate is either an unsigned public key certificate or a self-signed certificate that identifies the Root Certificate Authority (CA). A root certificate is part of a public key infrastructure scheme. The most common commercial variety is based on the ITU-T X.509 standard, which normally includes a digital signature from a certificate authority (CA).

Digital certificates are verified using a chain of trust. The trust anchor for the digital certificate is the Root Certificate Authority (CA). See [X.509](#).

Router A router is a device that forwards data packets between computer networks, creating an overlay internetwork. A router is connected to two or more data lines from different networks. When a data packet comes in one of the lines, the router reads the address information in the packet to determine its ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey. Routers perform the *traffic directing* functions on the Internet. A data packet is typically forwarded from one router to another through the networks that constitute the internetwork until it reaches its destination node.

SFTP Secure File Transfer Protocol (SFTP) is a secure version of File Transfer Protocol (FTP), which facilitates data access and data transfer over a Secure Shell (SSH) data stream. It is part of the [SSH](#) Protocol. This term is also known as SSH File Transfer Protocol.

SMTP The SMTP (Simple Mail Transfer Protocol) is a standard e-mail protocol on the Internet and part of the TCP/IP protocol suite, as defined by IETF RFC 2821. SMTP defines the message format and the message transfer agent (MTA), which stores and forwards the mail. SMTP by de-

fault uses TCP port 25. The protocol for mail submission is the same, but uses port 587. SMTP connections secured by SSL, known as [SMTPS](#), default to port 465.

SMTPS SMTPS (Simple Mail Transfer Protocol Secure) refers to a method for securing SMTP with transport layer security. For more information about SMTP, see description of the [SMTP](#).

SNMP The Simple Network Management Protocol (SNMP) is an *Internet-standard protocol for managing devices on IP networks*. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

SSH Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities – `slogin`, `ssh`, and `scp` – that are secure versions of the earlier UNIX utilities, `rlogin`, `rsh`, and `rcp`. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

TCP The Transmission Control Protocol (TCP) is one of the core protocols of the Internet protocol suite (IP), and is so common that the entire suite is often called TCP/IP. TCP provides reliable, ordered, error-checked delivery of a stream of octets between programs running on computers connected to a local area network, intranet or the public Internet. It resides at the transport layer.

Web browsers use TCP when they connect to servers on the World Wide Web, and it is used to deliver email and transfer files from one location to another.

UDP The User Datagram Protocol (UDP) is one

of the core members of the Internet protocol suite (the set of network protocols used for the Internet). With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without prior communications to set up special transmission channels or data paths. The protocol was designed by David P. Reed in 1980 and formally defined in RFC 768.

URL A uniform resource locator, abbreviated URL, also known as web address, is a specific character string that constitutes a reference to a resource. In most web browsers, the URL of a web page is displayed on top inside an address bar. An example of a typical URL would be <http://www.example.com/index.html>, which indicates a protocol (http), a hostname (www.example.com), and a file name (index.html). A URL is technically a type of uniform resource identifier (URI), but in many technical documents and verbal discussions, URL is often used as a synonym for URI, and this is not considered a problem.

VPN A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.

A VPN connection across the Internet is similar

to a wide area network (**WAN**) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from the private network.

VPN server see **VPN**.

VPN tunnel see **VPN**.

VRRP VRRP protocol (Virtual Router Redundancy Protocol) allows you to transfer packet routing from the main router to a backup router in case the main router fails. (This can be used to provide a wireless cellular backup to a primary wired router in critical applications).

WAN A wide area network (WAN) is a network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, or national boundaries) using private or public network transports. Business and government entities utilize WANs to relay data among employees, clients, buyers, and suppliers from various geographical locations. In essence, this mode of telecommunication allows a business to effectively carry out its daily function regardless of location. The Internet can be considered a WAN as well, and is used by businesses, governments, organizations, and individuals for almost any purpose imaginable.

X.509 In cryptography, X.509 is an ITU-T standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI). X.509 specifies, amongst other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.

C Index

A

Accessing the router	2
Add User	101
APN	28
AT commands	87

B

Backup Configuration	107
Backup Routes	39
Bridge	16

C

Change Password	103
Change Profile	102
Clock synchronization	74
Configuration update	97
Control SMS messages	86

D

Data limit	31
Default Gateway	16
Default IP address	2
Default password	3
Default SIM card	32
Default username	3
DHCP	16, 113
Dynamic	18
Static	18
DNS	113
DNS server	16, 29
Domain Name System	see DNS
DoS attacks	44
Dynamic Host Configuration Protocol	see DHCP
DynDNS	71

F

Firewall	43
----------------	----

Filtering of Forwarded Packets	43
Filtering of Incoming Packets	43
Protection against DoS attacks	44
Firmware update	97, 109
Firmware version	5
FTP	72

G

GRE	64, 113
-----------	---------

H

HTTP	73
------------	----

I

IPsec	57, 113
Authenticate Mode	59
Encapsulation Mode	58
IKE Mode	58
IPv4	114

L

L2TP	67, 114
LAN	
Primary LAN	16
Secondary LAN	16
Location Area Code	6
Logout	111

M

Mobile network	28
Multiple WANs	40, 42

N

NAT	47, 114
Network Address Translation	see NAT
NTP	74, 114
NTP server	103

O

Object Identifier	79
OpenVPN	52, 114
Authenticate Mode	53

P

PAM	75
Password	103
PAT	47
PIN number	104
PLMN	6
Port	114
PPPoE	37
PPPoE Bridge Mode	34
PPTP	69, 114
PUK number	105

R

RADIUS	19
Reboot	111
Remote access	48
Restore Configuration	108
Router	1
Accessing	2

S

Save Log	14
Save Report	14
Security certificate	3
Send SMS	106
Serial number	5
Set internal clock	103
Signal Quality	6
Simple Network Management Protocol	see SNMP
SMS	84

SMS Service Center	104
SMTP	82, 115
SNMP	78, 115
SSH	92
Startup Script	95
Static Routes	42
Switch between SIM Cards	31
Syslog	93
System Log	14

T

TCP	115
Telnet	94
Transmission Control Protocol	see TCP

U

UDP	115
Unblock SIM card	105
Uniform resource locator	see URL
Unlock SIM card	104
Up/Down script	95
URL	116
Usage Profiles	102
User Datagram Protocol	see UDP
User Module	99
Users	101

V

Virtual private network	see VPN
VPN	116
VRRP	25, 116

W

Web interface	3
---------------------	---

D Recommended Literature

Application Notes, the “Installation” user manual, and documentation of several OWL user modules can be found as PDF files for downloading on the Internet at:

<https://www.doc.hirschmann.com/>

E Further support

Technical questions

For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly.

You find the addresses of our partners on the Internet at <http://www.hirschmann.com>

A list of local telephone numbers and email addresses for technical support directly from Hirschmann is available at <https://hirschmann-support.belden.com>

This site also includes a free of charge knowledge base and a software download section.

Customer Innovation Center

The Customer Innovation Center is ahead of its competitors on three counts with its complete range of innovative services:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- Training offers you an introduction to the basics, product briefing and user training with certification. You find the training courses on technology and products currently available at <https://www.belden.com/solutions/customer-innovation-center>
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Customer Innovation Center, you decide against making any compromises in any case. Our client-customized package leaves you free to choose the service components you want to use.

Internet:

<https://www.belden.com/solutions/customer-innovation-center>



HIRSCHMANN

A **BELDEN** BRAND