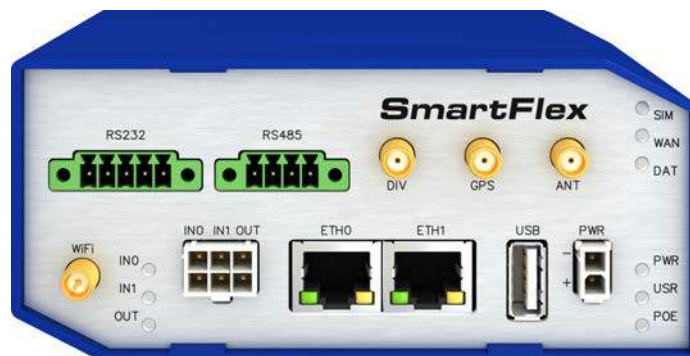


LTE Industrial Router

SmartFlex

CONFIGURATION MANUAL



ADVANTECH

Used Symbols



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



Attention – Problems that can arise in specific situations.



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



Example – example of function, command or script.

Firmware Version

Current version of firmware is 6.2.0 (August 16, 2019).

Open Source Software License

The software in this device uses various pieces of open source software governed by following licenses: GPL versions 2 and 3, LGPL version 2, BSD-style licenses, MIT-style licenses. The list of components together with complete license texts can be found on the device itself: See *Licenses* link at the bottom of the router's main Web page (*General Status*) or point your browser to address `DEVICE_IP/licenses.cgi`. If you are interested in obtaining the source, please contact us at:

techSupport@advantech-bb.com.

Modifications and debugging of LGPL-linked executables:

The manufacturer of the device hereby grants the right to use debugging techniques (e.g. decompilation) and making customer modifications of any executable linked with a LGPL library for own purposes. Note these rights are limited to the customer's own usage. No further distribution of such modified executables and no transmission of the information obtained during these actions may be done.



Advantech B+B SmartWorx s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
Document No. MAN-0023-EN, revision from August 23, 2019. Released in the Czech Republic.

Contents

1	Basic Information	1
1.1	Standard Equipment	1
1.2	Optional Features	1
1.3	Advantages in Relation to v2 Concept Routers	2
1.4	Configuration	2
1.5	Configuration Options	2
1.5.1	Valid characters for web interface	3
1.6	IPv6 Support	3
1.7	This Configuration Manual Describes	3
2	Access to the Web Conf.	4
2.1	Certificates and Preventing the Security Message	5
3	Status	7
3.1	General Status	7
3.1.1	Mobile Connection	7
3.1.2	Primary LAN, Secondary LAN, Tertiary LAN, WiFi	8
3.1.3	Peripheral Ports	9
3.1.4	System Information	9
3.2	Mobile WAN Status	10
3.3	WiFi Status	13
3.4	WiFi Scan	14
3.5	Network Status	16
3.6	DHCP Status	19
3.7	IPsec Status	21
3.8	DynDNS Status	22
3.9	System Log	23
4	Configuration	25
4.1	LAN Configuration	25
4.1.1	DHCP Server	27
4.1.2	IPv6 Prefix Delegation	28
4.1.3	802.1X Authentication to RADIUS Server	29
4.1.4	LAN Configuration Examples	30
4.2	VRRP Configuration	36
4.3	Mobile WAN Configuration	39
4.3.1	Connection to Mobile Network	39
4.3.2	DNS Address Configuration	41
4.3.3	Check Connection to Mobile Network Configuration	41

4.3.4	Example of Check Connection Configuration	42
4.3.5	Data Limit Configuration	43
4.3.6	Switch between SIM Cards Configuration	43
4.3.7	Examples of SIM Card Switching Configuration	47
4.3.8	PPPoE Bridge Mode Configuration	49
4.4	PPPoE Configuration	50
4.5	WiFi Access Point Configuration	52
4.6	WiFi Station Configuration	59
4.7	Backup Routes	64
4.7.1	Default Priorities for Backup Routes	66
4.8	Static Routes	67
4.9	Firewall Configuration	68
4.9.1	Example of the IPv4 Firewall Configuration	71
4.10	NAT Configuration	73
4.10.1	Examples of NAT Configuration	76
4.11	OpenVPN Tunnel Configuration	79
4.11.1	Example of the OpenVPN Tunnel Configuration in IPv4 Network	83
4.12	IPsec Tunnel Configuration	84
4.12.1	Example of the IPsec Tunnel Configuration in IPv4 Network	91
4.13	GRE Tunnels Configuration	92
4.13.1	Example of the GRE Tunnel Configuration	93
4.14	L2TP Tunnel Configuration	95
4.14.1	Example of the L2TP Tunnel Configuration	96
4.15	PPTP Tunnel Configuration	97
4.15.1	Example of the PPTP Tunnel Configuration	98
4.16	Services	99
4.16.1	DynDNS	99
4.16.2	FTP	100
4.16.3	HTTP	101
4.16.4	NTP	102
4.16.5	PAM	103
4.16.6	SNMP	104
4.16.7	SMTP	108
4.16.8	SMS	110
4.16.9	SSH	119
4.16.10	Syslog	120
4.16.11	Telnet	121
4.17	Expansion Port Configuration	122
4.17.1	Examples of the Expansion Port Configuration	125
4.18	USB Port Configuration	126
4.18.1	Examples of USB Port Configuration	129
4.19	Scripts	130
4.19.1	Startup Script	130
4.19.2	Example of Startup Script	130

4.19.3 Up/Down Scripts	131
4.19.4 Example of IPv6 Up/Down Script	131
4.20 Automatic Update Configuration	132
4.20.1 Example of Automatic Update	134
4.20.2 Example of Automatic Update Based on MAC	135
5 Customization	136
5.1 User Modules	136
6 Administration	138
6.1 Users	138
6.2 Change Profile	139
6.3 Change Password	140
6.4 Set Real Time Clock	140
6.5 Set SMS Service Center Address	141
6.6 Unlock SIM Card	141
6.7 Unblock SIM Card	142
6.8 Send SMS	142
6.9 Backup Configuration	143
6.10 Restore Configuration	144
6.11 Update Firmware	145
6.12 Reboot	146
6.13 Logout	146
7 Typical Situations	147
7.1 Access to the Internet from LAN	147
7.2 Backup Access to the Internet from LAN	149
7.3 Secure Networks Interconnection or Using VPN	153
7.4 Serial Gateway	156
8 Glossary and Acronyms	158
9 Index	163
10 Recommended Literature	166

List of Figures

1	Example of the Web Configuration	4
2	Mobile WAN status	12
3	WiFi Status	13
4	WiFi Scan	15
5	Network Status	18
6	DHCP Status	19
7	IPsec Status	21
8	DynDNS Status	22
9	System Log	23
10	Example program syslogd start with the parameter -R	24
11	LAN Configuration page	25
12	IPv6 Address with Prefix Example	28
13	Network Topology for Example 1	30
14	LAN Configuration for Example 1	31
15	Network Topology for Example 2	32
16	LAN Configuration for Example 2	33
17	Network Topology for Example 3	34
18	LAN Configuration for Example 3	35
19	Topology of VRRP configuration example	37
20	Example of VRRP configuration – main router	37
21	Example of VRRP configuration – backup router	38
22	Example of Check Connection Configuration	42
23	Mobile WAN Configuration	46
24	Configuration for SIM card switching Example 1	47
25	Configuration for SIM card switching Example 2	48
26	PPPoE Configuration	50
27	WiFi Access Point Configuration	58
28	WiFi Station Configuration	63
29	Backup Routes Configuration	64
30	Static Routes Configuration	67
31	Firewall Configuration – IPv6 Firewall	69
32	Topology for the IPv4 Firewall Configuration Example	71
33	IPv4 Firewall Configuration Example	72
34	NAT – IPv6 NAT Configuration	74
35	Topology for NAT Configuration Example 1	76
36	NAT Configuration for Example 1	76
37	Topology for NAT Configuration Example 2	77
38	NAT Configuration for Example 2	78
39	OpenVPN tunnel configuration	82
40	Topology of OpenVPN Configuration Example	83

41	IPsec Tunnels Configuration	90
42	Topology of IPsec Configuration Example	91
43	GRE Tunnel Configuration	93
44	Topology of GRE Tunnel Configuration Example	93
45	L2TP Tunnel Configuration	95
46	Topology of L2TP Tunnel Configuration Example	96
47	PPTP Tunnel Configuration	97
48	Topology of PPTP Tunnel Configuration Example	98
49	DynDNS Configuration Example	99
50	Enabling of FTP server	100
51	Configuration of HTTP and HTTPS services	101
52	Example of NTP Configuration	102
53	Configuration of PAM	103
54	OID Basic Structure	105
55	SNMP Configuration Example	106
56	MIB Browser Example	107
57	SMTP Client Configuration Example	108
58	SMS Configuration for Example 1	115
59	SMS Configuration for Example 2	116
60	SMS Configuration for Example 3	117
61	SMS Configuration for Example 4	118
62	Configuration of HTTP service	119
63	Syslog configuration	120
64	Enabling of Telnet service	121
65	Expansion Port Configuration	124
66	Example of Ethernet to serial communication configuration	125
67	Example of serial interface configuration	125
68	USB configuration	128
69	Example 1 – USB port configuration	129
70	Example 2 – USB port configuration	129
71	Example of a Startup Script	130
72	Example of IPv6 Up/Down Script	131
73	Example of Automatic Update 1	134
74	Example of Automatic Update 2	135
75	User modules	136
76	Added user module	136
77	Users	139
78	Change Profile	139
79	Change Password	140
80	Set Real Time Clock	140
81	Set SMS Service Center Address	141
82	Unlock SIM Card	141
83	Unblock SIM Card	142
84	Send SMS	142

85	Backup Configuration	143
86	Restore Configuration	144
87	Update Firmware	145
88	Reboot	146
89	Access to the Internet from LAN – sample topology	147
90	Access to the Internet from LAN – LAN configuration	148
91	Access to the Internet from LAN – Mobile WAN configuration	148
92	Backup access to the Internet – sample topology	149
93	Backup access to the Internet – LAN configuration	149
94	Backup access to the Internet – WiFi configuration	150
95	Backup access to the Internet – Mobile WAN configuration	151
96	Backup access to the Internet – Backup Routes configuration	152
97	Secure networks interconnection – sample topology	153
98	Secure networks interconnection – OpenVPN configuration	154
99	Serial Gateway – sample topology	156
100	Serial Gateway – konfigurace <i>Expansion Port 1</i>	157

List of Tables

1	Mobile Connection	8
2	PoE PSE information	8
3	Peripheral Ports	9
4	System Information	9
5	Mobile Network Information	11
6	Value ranges of signal strength for different technologies.	11
7	Description of Periods	11
8	Mobile Network Statistics	12
9	Information about Neighbouring WiFi Networks	14
10	Description of Interfaces in Network Status	16
11	Description of Information in Network Status	17
12	DHCP Status Description for IPv4 and IPv6 leases	20
13	Configuration of the Network Interface – IPv4 and IPv6	26
14	Configuration of the Network Interface – global items	27
15	Configuration of Dynamic DHCP Server	28
16	Configuration of Static DHCP Server	28
17	IPv6 prefix delegation configuration	29
18	Configuration of 802.1X Authentication	29
19	VRRP configuration	36
20	Check connection	37
21	Mobile WAN Connection Configuration	40
22	Check Connection to Mobile Network Configuration	42
23	Data Limit Configuration	43
24	Switch between SIM cards configuration	44
25	Parameters for SIM card switching	45
26	PPPoE configuration	51
27	WiFi Configuration	57
28	WLAN Configuration	62
29	Backup Routes Configuration	65
30	Backup Routes	66
31	Static Routes configuration	67
32	Filtering of Incoming Packets	68
33	Forwarding filtering	70
34	NAT Configuration	73
35	Remote Access Configuration	75
36	Configuration of Send all incoming packets to server	75
37	OpenVPN Configuration	81
38	OpenVPN Configuration Example	83
39	IPsec Tunnel Configuration	87
40	Example IPsec configuration	91

41	GRE Tunnel Configuration	92
42	GRE Tunnel Configuration Example	94
43	L2TP Tunnel Configuration	95
44	L2TP Tunnel Configuration Example	96
45	PPTP Tunnel Configuration	97
46	PPTP Tunnel Configuration Example	98
47	DynDNS Configuration	99
48	Parameters for HTTP and HTTPS services configuration	101
49	NTP Configuration	102
50	Configuration of PAM	103
51	SNMP Agent Configuration	104
52	SNMPv3 Configuration	104
53	SNMP Configuration (R-SeeNet)	105
54	Object identifier for binary inputs and output	106
55	SMTP client configuration	108
56	SMS Configuration	110
57	Control via SMS	111
58	Control SMS	112
59	Send SMS on the serial Port 1	112
60	Send SMS on the serial Port 2	113
61	Sending/receiving of SMS on TCP port specified	113
62	List of AT Commands	114
63	Parameters for SSH service configuration	119
64	Syslog configuration	120
65	Expansion Port Configuration – serial interface	123
66	Expansion Port Configuration – <i>Check TCP connection</i>	123
67	CD Signal Description	123
68	DTR Signal Description	124
69	USB Port Configuration 1	126
70	USB Port Configuration 2	127
71	CD Signal description	127
72	DTR Signal Description	127
73	Automatic Update Configuration	133
74	User modules	137
75	Users Overview	138
76	Add User	138

1. Basic Information

SmartFlex is LTE cellular router designed for communication across cellular networks using LTE, HSPA+, UMTS, EDGE or GPRS technology. Data transfer speed is up to 100 Mbps (download) and up to 50 Mbps (upload). The router is an ideal solution for the wireless connection of traffic and security camera systems, individual computers, LANs, automatic teller machines (ATM), other self-service terminals, and many other devices.

SmartFlex SR300 version of the router (LAN) is an ideal device for the realization of a secure connection of two local area networks (LANs). Interconnection is carried out using two ETHERNET 10/100 interfaces and secure tunnel ([IPsec](#), [OpenVPN](#), [L2TP](#)). The other equally important ways to use this router is to connect any device with RS232, RS485 or RS422 serial interface to the local network (LAN). For this purpose, SmartFlex SR300 router is equipped with two ETHERNET 10/100 ports and other interfaces based on the version of the router chosen by the user.

1.1 Standard Equipment

Standard features include the LTE cellular module (with three antenna connectors – for main, diversity and GPS antenna), two Ethernet 10/100 ports, one USB 2.0 Host port, two binary inputs, one output (I/O connector), and two SIM card readers for 3 V and 1.8 V SIM cards. The router also has microSD memory card reader that increases the router's storage space by up to 64 GB when using SDXC card or up to 32 GB when using SDHC cards.

1.2 Optional Features

If desired, the router can be configured with these optional interfaces. Note that routers cannot be retrofitted with these interfaces feature at some point in the future. See the router's technical manual for details on versions and possible combinations of interfaces.

- Version with the WiFi module. WiFi antenna connector is on the front panel.
- Version with three more Ethernet ports (switched).
- Version with RS232 interface.
- Version with combination of galvanically separated RS232 and RS485 interfaces.
- Version with combination of galvanically separated RS232, RS485 and Ethernet with stronger isolation.
- Version with SmartMesh IP wireless interface (DUST technology) – the router can serve as SmartMesh IP gateway for DUST nodes (motors).
- The router can be provided in either plastic or metal casing, depending upon the customer's requirements.

1.3 Advantages in Relation to v2 Concept Routers

The most considerable improvement in this new generation of routers is that they contain a CPU that is four times more powerful than the previous generation, providing significantly higher throughput and much faster encryption speeds. The router can also boast a substantially larger memory (512 MB RAM and 256 MB flash). As previously mentioned, the storage space can be further increased using a memory card. The fact that the router supports POE (Power over Ethernet) is also significant. This means that it is possible to power the device over a data network cable without the use of a dedicated power cable. The customer can choose a setup to best meet their requirements, from either "v3" router supporting PSE mode (Power Source Equipment), PD mode (Powered Device) or a router which does not support POE.

1.4 Configuration

Configuring SmartFlex routers is made easy by name and password protected web interface. The interface provides detailed statistics about router activities, signal strength, system logs and more. The router supports both [IPv4](#) and [IPv6](#) protocols, the creation of secure VPN tunnels using technologies that include [IPsec](#), [OpenVPN](#) and [L2TP](#). The router also supports [DHCP](#), [NAT](#), [NAT-T](#), [DynDNS client](#), [NTP](#), [VRRP](#), control by SMS, backup of primary connection, multiple WANs, [RADIUS](#) authentication over WiFi and many other functions.

Additional diagnostic features designed to ensure continuous communication include automatic inspection of PPP connections, an automatic restart feature in case a connection is lost, and a hardware watchdog that monitors the status of the router. Using a start up script window, users can insert Linux scripts for various actions. Users may insert multiple scripts and the router can switch between configurations as needed. Examples would include using SMS or checking the status of the binary input. SmartFlex routers can automatically update their configurations and firmware from a central server, allowing for mass reconfiguration of multiple routers at the same time.

1.5 Configuration Options

Routers can be configured via web browser or Secure Shell ([SSH](#)). Configuration via Web Browser is described in this Configuration Manual. Commands and scripts applicable in configuration using [SSH](#) are described in Commands and Scripts for v2 and v3 Routers – Application Note [\[1\]](#). Technical parameters and a full description of the router can be found in the User Manual of your router. You can also use additional software – communication [VPN server](#) SmartCluster [\[2\]](#) and software for router monitoring R-SeeNet [\[3, 4\]](#).

1.5.1 Valid characters for web interface

If the router is configured through the web interface, avoid entering of forbidden characters into any of input form (not just for password). Forbidden characters can be written into a form, but they will be deleted during data storing.

Valid characters are: 0-9 a-z A-Z * , + - . / : = ? ! # % @ [] _ { } ~

Forbidden characters are: “ \$ & ’ () ; < > \ ^ ‘ | "space"

1.6 IPv6 Support

There is independent IPv4 and IPv6 dual stack configuration implemented in the router's firmware. This means that you can configure traffic through both IP protocols independently and both are supported. Additional EUI-64 IPv6 addresses of network interfaces are generated automatically by standard methods. There is a NAT64 internal gateway network interface for automatic translation between IPv6 and IPv4 (see Chapter 3.5 for more information). This gateway works together with DNS64 seamlessly (for domain names translation).

For cellular IPv6 connection see *Mobile WAN Configuration* in Chapter 4.3.1. For IPv6 LAN configuration see *LAN Configuration* in Chapter 4.1, DHCPv6 server/client is also supported. IPv4 is the default, but IPv6 can be enabled or used with all features and protocols in the router, except for non-secured tunnels GRE, L2TP and PPTP, and VRRP. Using the secured tunnels OpenVPN and IPsec it is possible to run IPv6 traffic through an IPv4 tunnel and vice versa. The configuration forms for *NAT*, *Firewall* and *Up/Down Scripts* are completely separate for the IPv4 and IPv6 stacks. ICMPv6 protocol is also supported. IPv6 configuration is covered in each following Chapter when possible.

1.7 This Configuration Manual Describes

- Configuration of the router item by item according to the web interface (chapters 3 to 6).
- Configuration in typical situations examples (chapter 7):
 - Access to the Internet from LAN (Local Area Network) via mobile network, Ch. 7.1.
 - Backed up access to the Internet (from LAN), Ch. 7.2.
 - Secure networks interconnection or using VPN (Virtual Private Network), Ch. 7.3.
 - Serial Gateway (connection of serial devices to the Internet), Ch. 7.4

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 "**root**". The default password is "**root**". Change the default password as soon as possible!

Status	General Status
General	Mobile Connection
Mobile WAN	SIM Card : 1st
Network	IP Address : 10.00.0.40
DHCP	IPv6 Address : Unassigned
IPsec	Rx Data : 500 B
DynDNS	Tx Data : 843 B
System Log	Uptime : 0 days, 15 hours, 0 minutes
Configuration	> More Information <
LAN	Primary LAN
VRRP	IP Address : 10.64.0.54 / 255.255.252.0
Mobile WAN	IPv6 Address : fd00:a40::54 / 56
PPPoE	MAC Address : 02:AD:FF:00:00:54
Backup Routes	Rx Data : 75.5 KB
Static Routes	Tx Data : 252.9 KB
Firewall	> More Information <
NAT	Secondary LAN
OpenVPN	IP Address : 10.65.0.54 / 255.255.252.0
IPsec	IPv6 Address : fd00:a41::54 / 56
GRE	MAC Address : 02:AD:FF:01:00:54
L2TP	Rx Data : 30.9 KB
PPTP	Tx Data : 600 B
Services	> More Information <
Expansion Port 1	Peripheral Ports
Expansion Port 2	Expansion Port 1 : RS-232
USB Port	Expansion Port 2 : RS-485
Scripts	Binary Input 0 : Off
Automatic Update	Binary Input 1 : Off
Customization	Binary Output : On
User Modules	System Information
Administration	Firmware Version : XXX(YYYY-MM-DD)
Users	Serial Number : ACZ1199000000546
Change Profile	Profile : Standard
Change Password	RTC Battery : 0k
Set Real Time Clock	Supply Voltage : 24.0 V
Set SMS Service Center	Temperature : 42 °C
Unlock SIM Card	Time : 2019-08-20 14:23:18
Unlock SIM Card	Uptime : 0 days, 15 hours, 0 minutes
Send SMS	> Licenses <
Backup Configuration	
Restore Configuration	
Update Firmware	
Reboot	
Logout	

Figure 1: Example of the Web Configuration



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.

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 4.16.6). 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 4.16.3.



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 4.16.3.

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

Selecting the *General* item will open a screen displaying a summary of basic information about the router and its activities. This page is also displayed when you login to the web interface. Information is divided into several sections, based upon the type of router activity or the properties area: *Mobile Connection*, *Primary LAN*, *Secondary LAN*, *Peripheral Ports* and *System Information*. If the router is in the Ethernet switch or RS232-RS485-ETH version, there will be a *Tertiary LAN* section. If the router is WiFi equipped, there will be a *WiFi* section.

IPv6 Address item can show multiple different addresses for one network interface. This is standard behavior since an IPv6 interface uses more addresses. The second IPv6 Address showed after pressing *More Information* is automatically generated EUI-64 format link local IPv6 address derived from MAC address of the interface. It is generated and assigned the first time the interface is used (e.g. cable is connected, Mobile WAN connecting, etc.).



3.1.1 Mobile Connection

Item	Description
SIM Card	Identification of the SIM card (<i>Primary</i> or <i>Secondary</i>).
Interface	Defines the network interface.
Flags	Displays network interface flags.
IP Address	IPv4 address of the network interface.
IPv6 Address	IPv6 address or addresses of the network interface – there can be more IPv6 addresses assigned to one network 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

Continued on next page

Continued from previous page

Item	Description
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, Tertiary LAN, WiFi

Items displayed in this part have the same meaning as items in the previous part. Moreover, the *MAC Address* item shows the MAC address of the corresponding router's interface (*Primary LAN – eth0*, *Secondary LAN – eth1*, *Tertiary LAN – eth2*, *WiFi – wlan0*). Visible information depends on configuration (see 4.5 or 4.6).

If the router is equipped with PoE PSE board, there is also information about it in the *Primary LAN* or *Secondary LAN* section (see table below for description).

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

Table 2: PoE PSE information

3.1.3 Peripheral Ports

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

Table 3: Peripheral Ports

3.1.4 System Information

Item	Description
Firmware Version	Information about the firmware version
Serial Number	Serial number of the router (in case of <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)
Power Board	If the power board is installed in the router, shows the type of power board: PoE PD or PoE PSE.
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 4: System Information

3.2 Mobile WAN Status



The SmartFlex SR300 (LAN version) does not display the Mobile WAN status option.

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 6.
Signal Quality	Signal quality of the selected cell: <ul style="list-style-type: none"> • EC/IO for UMTS (it's the ratio of the signal received from the pilot channel – EC – to the overall level of the spectral density, ie the sum of the signals of other cells – IO). • RSRQ for LTE technology (Defined as the ratio $\frac{N \times RSRP}{RSSI}$). • The value is not available for the EDGE technology.
CSQ	Cell Signal Quality, relative value is given by RSSI (dBm). 2–9 range means Marginal, 10–14 range means OK, 15–16 range means Good, 20–30 range means excellent.
Neighbours	Signal strength of neighboring hearing cells (GPRS only) ¹ .
Manufacturer	Module manufacturer
Model	Type of module
Revision	Revision of module

Continued on next page

¹If a neighboring cell for GPRS is highlighted in red, router may repeatedly switch between the neighboring and the primary cell affecting the router's performance. To prevent this, re-orient the antenna or use a directional antenna.

Continued from previous page

Item	Description
IMEI	IMEI (International Mobile Equipment Identity) number of module
MEID	MEID number of module
ICCID	Integrated Circuit Card Identifier is international and unique serial number of the SIM card.

Table 5: Mobile Network Information

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 6: 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 7: Description of Periods



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.

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 8: Mobile Network Statistics

Mobile WAN Status						
Mobile Network Information						
Registration	:	Home Network				
Operator	:	Vodafone CZ				
Technology	:	LTE				
PLMN	:	23003				
Cell	:	10A80C				
LAC	:	947C				
Channel	:	6400				
Signal Strength	:	-71 dBm				
Signal Quality	:	-7 dB				
» More Information «						
Statistics for 1st SIM card						
	Today	Yesterday	This Week	Last Week	This Period	Last Period
Rx Data	: 0 KB	24 KB	24 KB	0 KB	24 KB	0 KB
Tx Data	: 0 KB	908 KB	908 KB	0 KB	908 KB	0 KB
Connections	: 0	6	6	0	6	0
Signal Min	: -74 dBm	-73 dBm	-74 dBm	?	-74 dBm	?
Signal Avg	: -72 dBm	-71 dBm	-72 dBm	?	-72 dBm	?
Signal Max	: -71 dBm	-71 dBm	-71 dBm	?	-71 dBm	?
Cells	: 1	1	1	0	1	0
Availability	: 100.0%	99.2%	99.8%	0.0%	99.8%	0.0%
Statistics for 2nd SIM card						
	Today	Yesterday	This Week	Last Week	This Period	Last Period
Rx Data	: 0 KB	0 KB	0 KB	0 KB	0 KB	0 KB
Tx Data	: 0 KB	0 KB	0 KB	0 KB	0 KB	0 KB
Connections	: 0	0	0	0	0	0
Signal Min	: ?	?	?	?	?	?
Signal Avg	: ?	?	?	?	?	?
Signal Max	: ?	?	?	?	?	?
Cells	: 0	0	0	0	0	0
Availability	: 0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Connection Log						
2019-08-21 23:20:07 (1st SIM card) Connection successfully established.						

Figure 2: Mobile WAN status

3.3 WiFi Status



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

Selecting the *Status -> WiFi -> Status* item in the main menu of the web interface will display information about the WiFi access point (AP) and the WiFi station (STA). Information about all stations connected to the AP are listed as well. Example of the output for the Wifi status is shown on the following figure.



Figure 3: WiFi Status

3.4 WiFi Scan



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

Selecting the *Status -> WiFi -> Scan* item scans for neighboring WiFi networks and displays the results. In the table below is the description of some items in the output of the WiFi scanning.

Item	Description
BSS	MAC address of access point (AP)
TSF	A Timing Synchronization Function (TSF) keeps the timers for all stations in the same Basic Service Set (BSS) synchronized. All stations shall maintain a local TSF timer.
freq	Frequency band of WiFi network [kHz]
beacon interval	Period of time synchronization
capability	List of access point (AP) properties
signal	Signal level of access point (AP)
last seen	Last response time of access point (AP)
SSID	Identifier of access point (AP)
Supported rates	Supported rates of access point (AP)
DS Parameter set	The channel on which access point (AP) broadcasts
ERP	Extended Rate PHY – information element providing backward compatibility
Extended supported rates	Supported rates of access point (AP) that are beyond the scope of eight rates mentioned in <i>Supported rates</i> item
RSN	Robust Secure Network – The protocol for establishing a secure communication through wireless network 802.11

Table 9: Information about Neighbouring WiFi Networks

WiFi Scan output may look like this:

```

WiFi Scan
List of BSSs
BSS 1c:49:7b:c6:48:98(on wlan1)
  last seen: 38860.637s [boottime]
  TSF: 464854144110 usec (5d, 09:07:34)
  freq: 2412
  beacon interval: 100 TUs
  capability: ESS Privacy ShortPreamble ShortSlotTime (0x0431)
  signal: -86.00 dBm
  last seen: 6760 ms ago
  Information elements from Probe Response frame:
  SSID: WLAN11_2G
  Supported rates: 1.0* 2.0* 5.5* 11.0* 9.0 18.0 36.0 54.0
  DS Parameter set: channel 1
  ERP: Use_Protection
  Extended supported rates: 6.0 12.0 24.0 48.0
  HT capabilities:
    Capabilities: 0x11ec
      HT20
      SM Power Save disabled
      RX HT20 SGI
      RX HT40 SGI
      TX STBC
      RX STBC 1-stream
      Max AMSDU length: 3839 bytes
      DSSS/CCK HT40
    Maximum RX AMPDU length 65535 bytes (exponent: 0x003)
    Minimum RX AMPDU time spacing: 4 usec (0x05)
    HT RX MCS rate indexes supported: 0-15, 32
    HT TX MCS rate indexes are undefined
  HT operation:
    * primary channel: 1
    * secondary channel offset: no secondary
    * STA channel width: 20 MHz
    * RIFS: 0
    * HT protection: nonmember
    * non-GF present: 0
    * OBSS non-GF present: 0
    * dual beacon: 0
    * dual CTS protection: 0
    * STBC beacon: 0
    * L-SIG TXOP Prot: 0
    * PCO active: 0
    * PCO phase: 0
  RSN:
    * Version: 1
    * Group cipher: CCMP
    .....
  WPS:
    * Version: 1.0
    * Wi-Fi Protected Setup State: 2 (Configured)
    * Response Type: 3 (AP)
    * UUID: 00010203-0405-0607-0809-0a0b0c0d0e0f
    * Manufacturer: TP-LINK
    * Model: TL-WR841N
    * Model Number: 12.0
    * Serial Number: 1.0
    * Primary Device Type: 6-0050f204-1
    * Device name: Wireless Router TL-WR841N
    * Config methods: Ethernet, Label, PBC
    * RF Bands: 0x1
    * Unknown TLV (0x1049, 20 bytes): 00 24 e2 60 02 00 01 01 60 00 00 02 00 01 60 01 00 02 00 01

```

Figure 4: WiFi Scan

3.5 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, eth2	Network interfaces (Ethernet connection)
usb0	Active PPP connection to the mobile network – wireless module is connected via USB interface.
wlan0	WiFi interface
ppp0	PPP interface (e.g. PPPoE tunnel)
tun0	OpenVPN tunnel interface
ipsec0	IPSec tunnel interface
gre1	GRE tunnel interface
lo	Local loopback interface
nat64	Network interface of internal translator gateway between IPv6 and IPv4 addresses.

Table 10: Description of Interfaces in Network Status

The following information can be displayed at every network interface:

Item	Description
HWaddr	Hardware (unique, MAC) address of a network interface.
inet addr	IPv4 address of interface
inet6 addr	IPv6 address of interface. There can be more of them for single network interface.
P-t-P	IP address of the opposite end (in case of point-to-point connection).
Bcast	Broadcast address
Mask	Mask of network
MTU	Maximum packet size that the equipment is able to transmit.
Metric	Number of routers the packet must go through.

Continued on next page

Continued from previous page

Item	Description
RX	<ul style="list-style-type: none"> • packets – received packets • errors – number of errors • dropped – dropped packets • overruns – incoming packets lost because of overload. • frame – wrong incoming packets because of incorrect packet size.
TX	<ul style="list-style-type: none"> • packets – transmit packets • errors – number of errors • dropped – dropped packets • overruns – outgoing packets lost because of overload. • carrier – wrong outgoing packets with errors resulting from the physical layer.
collisions	Number of collisions on physical layer.
txqueuelen	Length of buffer (queue) of the network interface.
RX bytes	Total number of received bytes.
TX bytes	Total number of transmitted bytes.

Table 11: 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 of the *Network Status* page. There is IPv4 *Route Table* and IPv6 *Route Table* below.

If the router is connected to the Internet (a default route is defined), the *nat64* network interface is created automatically. This is the NAT64 internal gateway for translating the IPv6 and IPv4 communication. It is used automatically when connected via IPv6 and communicating with IPv4 device or network. It works together with DNS64 running in the router automatically (translation of domain names to IP addresses). The default NAT64 prefix 64:ff9b::/96 is used as you can see in Figure 5 below in the *IPv6 Route Table* section.



Network Status

Interfaces

eth0

Link encap:Ethernet HWaddr 02:AD:FF:00:00:54
inet addr:10.64.0.54 Bcast:10.64.3.255 Mask:255.255.252.0
inet6 addr: fe80::ad:ffff:fe00:54/64 Scope:Link
inet6 addr: fd00:a40::54/56 Scope:Global
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:3361 errors:0 dropped:0 overruns:0 frame:0
TX packets:314 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1232118 (1.1 MB) TX bytes:184879 (180.5 KB)
Interrupt:48

lo

Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
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)

nat64

Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
inet6 addr: fe80::b0bd:dcde:a38a:6302/64 Scope:Link
inet6 addr: 64:ff9b::/96 Scope:Global
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:4 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)

usb0

Link encap:Ethernet HWaddr B6:DF:5F:30:B5:FE
inet addr:10.80.0.48 Bcast:0.0.0.0 Mask:255.255.255.255
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:2 errors:0 dropped:0 overruns:0 frame:0
TX packets:3 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:580 (580.0 B) TX bytes:843 (843.0 B)

Route Table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.253.254	0.0.0.0	UG	0	0	0	usb0
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
192.168.253.254	0.0.0.0	255.255.255.255	UH	0	0	0	usb0

IPv6 Route Table

Destination	Next Hop	Flags	Metric	Ref	Use	Iface
64:ff9b::/96	::	U	256	1	0	nat64
fd00:a40::/56	::	U	256	1	0	eth0
fe80::/64	::	U	256	1	0	eth0
fe80::/64	::	U	256	1	0	nat64
::/0	::	In	-1	1	31	lo
::1/128	::	Un	0	3	2	lo
64:ff9b::/128	::	Un	0	2	0	nat64
fd00:a40::/128	::	Un	0	2	0	eth0
fd00:a40::54/128	::	Un	0	2	0	eth0
fe80::/128	::	Un	0	2	0	eth0
fe80::/128	::	Un	0	2	0	nat64
fe80::ad:ffff:fe00:54/128	::	Un	0	2	0	eth0
fe80::b0bd:dcde:a38a:6302/128	::	Un	0	2	0	nat64
ff00::/8	::	U	256	2	120	eth0
ff00::/8	::	U	256	1	0	nat64
::/0	::	In	-1	1	31	lo

Figure 5: Network Status

3.6 DHCP Status

Information about the DHCP server activity is accessible via *DHCP* item. The DHCP server provides automatic configuration of 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). DHCPv6 server is supported.

DHCP Status
Active DHCP Leases (LAN)
<pre>lease 192.168.10.20 { starts epoch 946708441; # Sat Jan 01 06:34:01 2000 ends epoch 946708501; # Sat Jan 01 06:35:01 2000 tstp epoch 946708501; # Sat Jan 01 06:35:01 2000 cltt epoch 946708441; # Sat Jan 01 06:34:01 2000 binding state free; hardware ethernet 00:0a:14:82:df:f9; }</pre>
Active DHCPv6 Leases (LAN)
<pre>ia-na "\001\000\000\000\000\003\000\001\000\012\024\202\337\371" { cltt epoch 946713997; # Sat Jan 01 08:06:37 2000 iaaddr fd00:1233::2a { binding state active; preferred-life 375; max-life 600; ends epoch 946714597; # Sat Jan 01 08:16:37 2000 } }</pre>
Active DHCP Leases (WLAN)
<pre>lease 192.168.100.10 { starts epoch 946711376; # Sat Jan 01 07:22:56 2000 ends epoch 946711976; # Sat Jan 01 07:32:56 2000 tstp epoch 946711976; # Sat Jan 01 07:32:56 2000 cltt epoch 946711376; # Sat Jan 01 07:22:56 2000 binding state active; next binding state free; hardware ethernet 78:a5:04:2f:7c:2b; }</pre>
Active DHCPv6 Leases (WLAN)
<pre>ia-na "\001\000\000\000\000\003\000\001x\245\004/ +" { cltt epoch 946711437; # Sat Jan 01 07:23:57 2000 iaaddr fd00:1235::1 { binding state active; preferred-life 375; max-life 600; ends epoch 946712037; # Sat Jan 01 07:33:57 2000 } } ia-na "\001\000\000\000\000\003\000\001x\245\004/ +" { cltt epoch 946711513; # Sat Jan 01 07:25:13 2000 iaaddr fd00:1235::1 { binding state released; preferred-life 375; max-life 600; ends epoch 946712037; # Sat Jan 01 07:33:57 2000 } }</pre>

Figure 6: DHCP Status



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

Records in the *DHCP Status* window are divided into separate parts according to LAN and WLAN interface and IPv4 (DHCP) and IPv6 (DHCPv6) – there are parts *Active DHCP Leases (LAN)*, *Active DHCPv6 Leases (LAN)*, *Active DHCP Leases (WLAN)* and *Active DHCPv6*

Leases (WLAN) if the router has WiFi and WLAN network interface is enabled. In Figure 6 above there are both DHCP (IPv4) and DHCPv6 (IPv6) servers enabled LAN interface and WLAN interface. The table below explains information from the client list:

Item	Description
lease	Assigned IPv4 address.
iaaddr	(IPv6) Assigned IPv6 address.
starts epoch	Time that the IP address was assigned.
ends epoch	Time that the IP address lease expires.
tstp epoch	What time the peer has been told the lease expires.
cltt epoch	Client last transaction time.
binding state	The lease's binding state.
next binding state	What state the lease will move to when the current state expires.
hardware ethernet	Unique hardware MAC address.
uid	Unique ID.
client-hostname	Host computer name.
preferred-life	(IPv6) Length of time the address can be used without any restrictions. When the preferred-life expires, the address should not be used for new communications, but might continue to be used for existing communications in certain cases.
max-life	(IPv6) Maximum time for which the DHCPv6 server can grant a lease.

Table 12: DHCP Status Description for IPv4 and IPv6 leases

3.7 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!

The screenshot shows the 'IPsec Status' web page. The title is 'IPsec Status'. Below it is a section titled 'IPsec Tunnels Information'. The content displays the status of the IKE charon daemon (weakSwan 5.5.3, Linux 3.12.10+, armv7l):

```

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/MODP_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
  
```

The line 'ipsec1[2]: ESTABLISHED 17 minutes ago, 10.0.0.228[10.0.0.228]...10.0.2.250[10.0.2.250]' is highlighted with an orange box, indicating the tunnel is established.

Figure 7: IPsec Status

3.8 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 listed servers for the Dynamic DNS service. It is possible to use the DynDNSv6 service with *IP Mode* switched to IPv6 on *DynDNS Configuration* page.

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

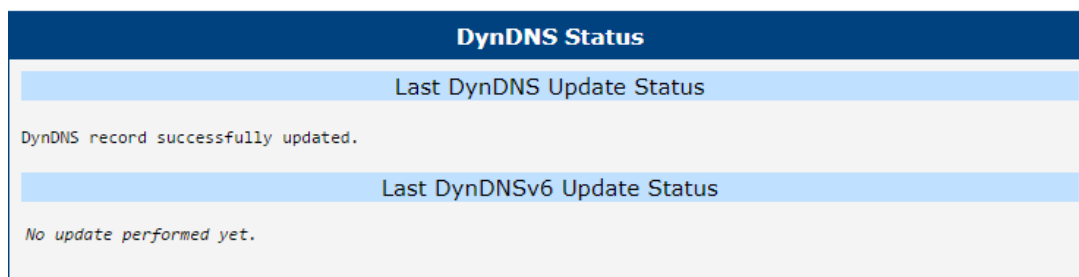


Figure 8: DynDNS Status

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.

3.9 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 10.

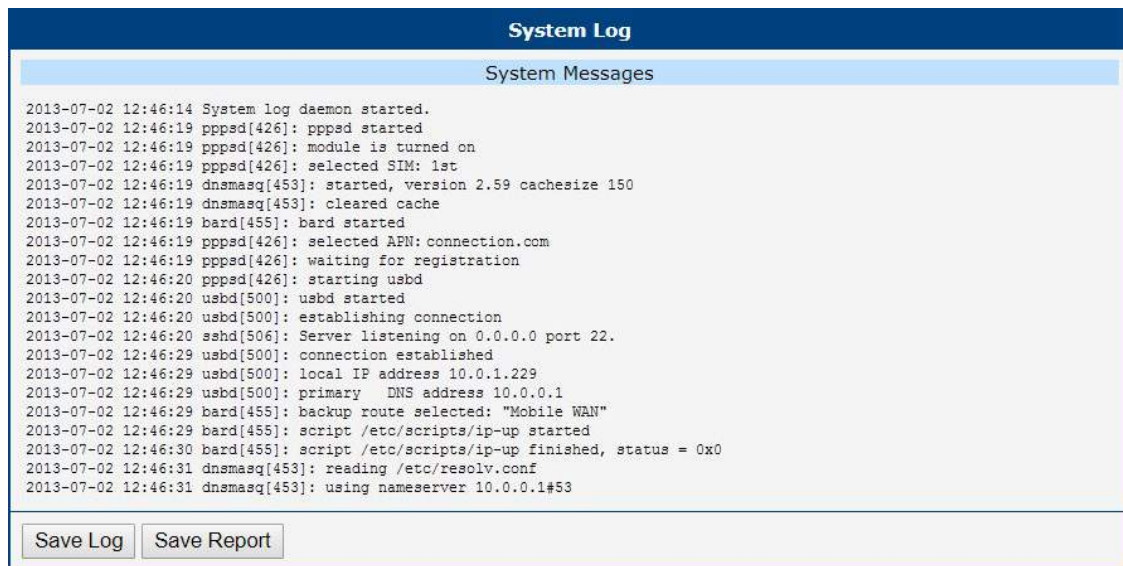


Figure 9: System Log

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

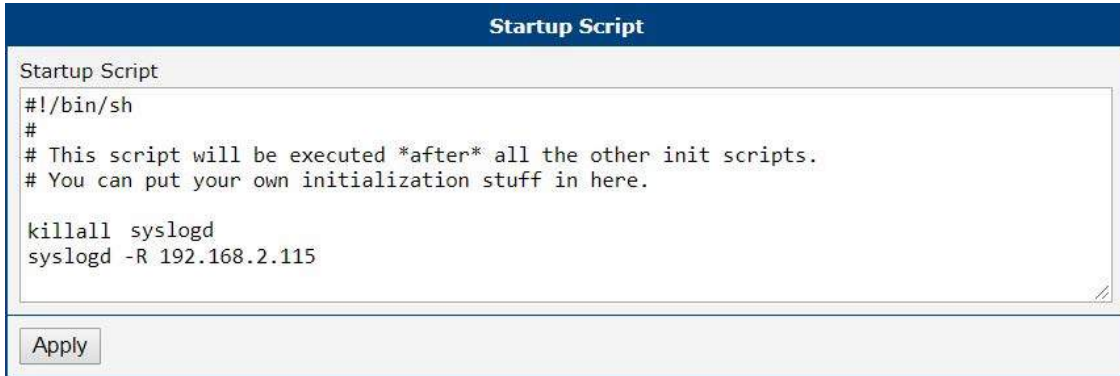


Figure 10: Example program syslogd start with the parameter -R

4. Configuration

4.1 LAN Configuration

To enter the Local Area Network configuration, select the *LAN* menu item in the *Configuration* section. The *LAN* item will expand in the menu on the left, so you can choose the proper Ethernet interface to configure: *Primary LAN* for the router's first Ethernet interface (ETH0), *Secondary LAN* for the router's second Ethernet interface (ETH1) and *Tertiary LAN* for the third Ethernet interface if the router has 3-port Ethernet SWITCH or RS232-RS485-ETH interface.

LAN Configuration page is divided into IPv4 and IPv6 columns, see Figure 11. There is dual stack support of IPv4 and IPv6 protocols – they can run alongside, you can configure either one of them or both. If you configure both IPv4 and IPv6, other network devices will choose the communication protocol. Configuration items and IPv6 to IPv4 differences are described in the tables below.

Primary LAN Configuration		
DHCP Client	IPv4 disabled	IPv6 disabled
IP Address	10.64.0.37	fc00:a40:37
Subnet Mask / Prefix	255.255.252.0	118
Default Gateway		
DNS Server		
Bridged	no	
Media Type	auto-negotiation	
<input type="checkbox"/> Enable dynamic DHCP leases		
	IPv4	IPv6
IP Pool Start		
IP Pool End		
Lease Time		sec
<input type="checkbox"/> Enable static DHCP leases		
MAC Address	IP Address	IPv6 Address
<input type="checkbox"/> Enable IPv6 prefix delegation		
Subnet ID *		
Subnet ID Width *	bits	
<input type="checkbox"/> Enable IEEE 802.1X Authentication		
Authentication Method	EAP-PEAP/MSCHAPv2	
CA Certificate		
Local Certificate		
Local Private Key		
Identity		
Password		
* can be blank		
<input type="button" value="Apply"/>		

Figure 11: LAN Configuration page

Item	Description
DHCP Client	<p>Enables/disables the DHCP client function. If in IPv6 column, the DHCPv6 client is enabled. DHCPv6 client supports all three methods of getting an IPv6 address – SLAAC, stateless DHCPv6 and statefull DHCPv6.</p> <ul style="list-style-type: none"> • disabled – The router does not allow automatic allocation of an IP address from a DHCP server in LAN network. • enabled – The router allows automatic allocation of an IP address from a DHCP server in LAN network.
IP Address	A fixed IP address of the Ethernet interface. Use IPv4 notation in IPv4 column and IPv6 notation in IPv6 column. Shortened IPv6 notation is supported.
Subnet Mask / Prefix	Specifies a Subnet Mask for the IPv4 address. In the IPv6 column, fill in the Prefix for the IPv6 address – number in range 0 to 128.
Default Gateway	Specifies the IP address of a default gateway. If filled-in, every packet with the destination not found in the routing table is sent to this IP address. Use proper IP address notation in IPv4 and IPv6 column.
DNS Server	Specifies the IP address of the DNS server. When the IP address is not found in the Routing Table, the router forwards the request to DNS server specified here. Use proper IP address notation in IPv4 and IPv6 column.

Table 13: Configuration of the Network Interface – IPv4 and IPv6

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 4.7). Since FW 5.3.0, *Default Gateway* and *DNS Server* are also supported on bridged interfaces (e.g. eth0 + eth1).

The following three items (in the table below) are global for the configured Ethernet interface. Only one bridge can be active on the router at a time. The *DHCP Client*, *IP Address* and *Subnet Mask / Prefix* parameters of the only one of the interfaces are used to for 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.

Item	Description
Bridged	<p>Activates/deactivates the bridging function on the router.</p> <ul style="list-style-type: none"> • no – The bridging function is inactive (default). • yes – The bridging function is active.
Media Type	<p>Specifies the type of duplex and speed used in the network.</p> <ul style="list-style-type: none"> • Auto-negation – The router automatically sets the best speed and duplex mode of communication according to the network's possibilities. • 100 Mbps Full Duplex – The router communicates at 100 Mbps, in the full duplex mode. • 100 Mbps Half Duplex – The router communicates at 100 Mbps, in the half duplex mode. • 10 Mbps Full Duplex – The router communicates at 10 Mbps, in the full duplex mode. • 10 Mbps Half Duplex – The router communicates at 10 Mbps, in the half duplex mode.
PoE PSE	<ul style="list-style-type: none"> • enabled – The router provides power on the Ethernet cable. • disabled – The router does not provide power on the Ethernet cable (default).

Table 14: Configuration of the Network Interface – global items

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.



If IPv6 column is filled in, the DHCPv6 server is used. DHCPv6 server offers stateful address configuration to connected clients. Only when the *Subnet Prefix* above is set to 64, the DHCPv6 server offers both – the stateful address configuration and SLAAC (Stateless Address Autoconfiguration).



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.

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. Use proper notation in IPv4 and IPv6 column.
IP Pool End	End of IP addresses allocated to the DHCP clients. Use proper IP address notation in IPv4 and IPv6 column.
Lease time	Time in seconds that the IP address is reserved before it can be re-used.

Table 15: 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.
IPv4 Address	Assigned IPv4 address. Use proper notation.
IPv6 Address	Assigned IPv6 address. Use proper notation.

Table 16: Configuration of Static DHCP Server

4.1.2 IPv6 Prefix Delegation



This is an advanced configuration option. IPv6 prefix delegation works automatically with DHCPv6 – use only if different configuration is desired and if you know the consequences.

If you want to override the automatic IPv6 prefix delegation, you can configure it in this form. You have to know your Subnet ID Width (part of IPv6 address), see Figure below for the calculation help – it is an example: 48 bits is Site Prefix, 16 bits is Subnet ID (*Subnet ID Width*) and 64 bits is Interface ID.

2001:0db8:85a3:08d3:1319:8a2e:0370:7344

└──────────┘	└──┘	└──────────┘
Site Prefix	Subnet ID	Interface ID

Figure 12: IPv6 Address with Prefix Example

Item	Description
Enable IPv6 prefix delegation	Enables prefix delegation configuration filled-in below.
Subnet ID	The decimal value of the Subnet ID of the Ethernet interface. Maximum value depends on the <i>Subnet ID Width</i> .
Subnet ID Width	The maximum <i>Subnet ID Width</i> depends on your Site Prefix – it is the remainder to 64 bits.

Table 17: IPv6 prefix delegation configuration

4.1.3 802.1X 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, see chap. 1.5.1!
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, see chap. 1.5.1!

Table 18: Configuration of 802.1X Authentication

4.1.4 LAN Configuration Examples

Example 1: IPv4 Dynamic DHCP Server, Default Gateway and DNS Server

- The range of dynamic allocated IPv4 addresses is from 192.168.1.2 to 192.168.1.4.
- The address is allocated for 600 second (10 minutes).
- Default gateway IP address is 192.168.1.20
- DNS server IP address is 192.168.1.20

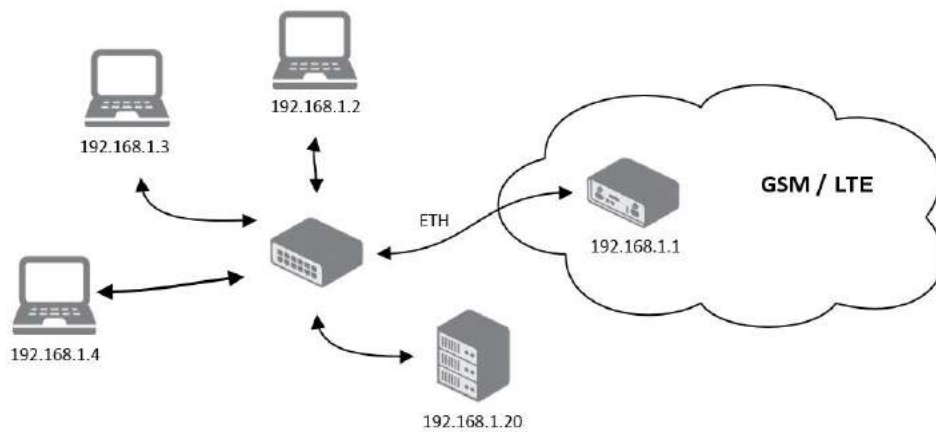


Figure 13: Network Topology for Example 1

Primary LAN Configuration			
DHCP Client	IPv4	IPv6	
	disabled ▼	disabled ▼	
IP Address	192.168.1.1		
Subnet Mask / Prefix	255.255.255.0		
Default Gateway	129.168.1.20		
DNS Server	192.168.1.20		
Bridged	no ▼		
Media Type	auto-negotiation ▼		
<input checked="" type="checkbox"/> Enable dynamic DHCP leases			
	IPv4	IPv6	
IP Pool Start	192.168.1.2		
IP Pool End	192.168.1.4		
Lease Time	600	600	sec
<input type="checkbox"/> Enable static DHCP leases			
MAC Address	IP Address	IPv6 Address	
<input type="checkbox"/> Enable IPv6 prefix delegation			
Subnet ID *			
Subnet ID Width *		bits	
<input type="checkbox"/> Enable IEEE 802.1X Authentication			
Authentication Method	EAP-PEAP/MSCHAPv2 ▼		
CA Certificate	<div>Choose File No file chosen</div>		
Local Certificate	<div>Choose File No file chosen</div>		
Local Private Key	<div>Choose File No file chosen</div>		
Identity			
Password			
* can be blank			
<div>Apply</div>			

Figure 14: LAN Configuration for Example 1

Example 2: IPv4 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.

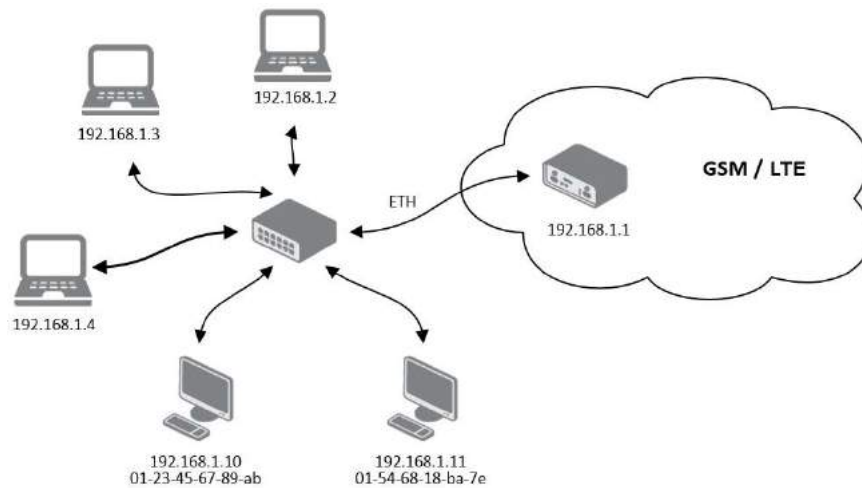


Figure 15: Network Topology for Example 2

Primary LAN Configuration			
DHCP Client	IPv4	IPv6	
	disabled ▼	disabled ▼	
IP Address	192.168.1.1		
Subnet Mask / Prefix	255.255.255.0		
Default Gateway			
DNS Server			
Bridged	no ▼		
Media Type	auto-negotiation ▼		
<input checked="" type="checkbox"/> Enable dynamic DHCP leases			
	IPv4	IPv6	
IP Pool Start	192.168.1.2		
IP Pool End	192.168.1.4		
Lease Time	600	600	sec
<input checked="" type="checkbox"/> Enable static DHCP leases			
MAC Address	IP Address	IPv6 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 IPv6 prefix delegation			
Subnet ID *			
Subnet ID Width *		bits	
<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"/>		
Local Private Key Password	<input type="text"/>		
* can be blank			
<input type="button" value="Apply"/>			

Figure 16: LAN Configuration for Example 2

Example 3: IPv6 Dynamic DHCP Server

- The range of dynamic allocated IPv6 addresses is from 2001:db8::1 to 2001:db8::ffff.
- The address is allocated for 600 second (10 minutes).
- The router is still accessible via IPv4 (192.168.1.1).

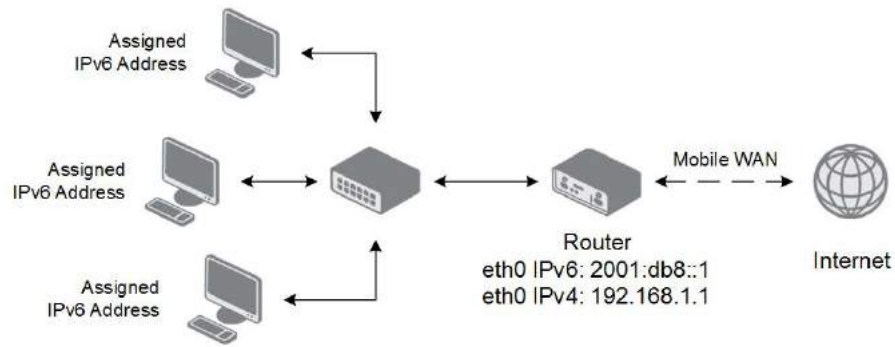


Figure 17: Network Topology for Example 3

Primary LAN Configuration		
DHCP Client	IPv4 disabled ▼	IPv6 disabled ▼
IP Address	192.168.1.1	2001:db8::1
Subnet Mask / Prefix	255.255.255.0	64
Default Gateway		
DNS Server		
Bridged	no ▼	
Media Type	auto-negotiation ▼	
<input checked="" type="checkbox"/> Enable dynamic DHCP leases		
IP Pool Start	IPv4 	IPv6 2001:db8::2
IP Pool End		2001:db8::ffff
Lease Time		600 sec
<input type="checkbox"/> Enable static DHCP leases		
MAC Address	IP Address	IPv6 Address
<input type="checkbox"/> Enable IPv6 prefix delegation		
Subnet ID *		
Subnet ID Width *		bits
<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"/>	
Local Private Key Password	<input type="text"/>	
* can be blank		
<input type="button" value="Apply"/>		

Figure 18: LAN Configuration for Example 3

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 19: 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 20: Check connection

Example of the VRRP protocol:

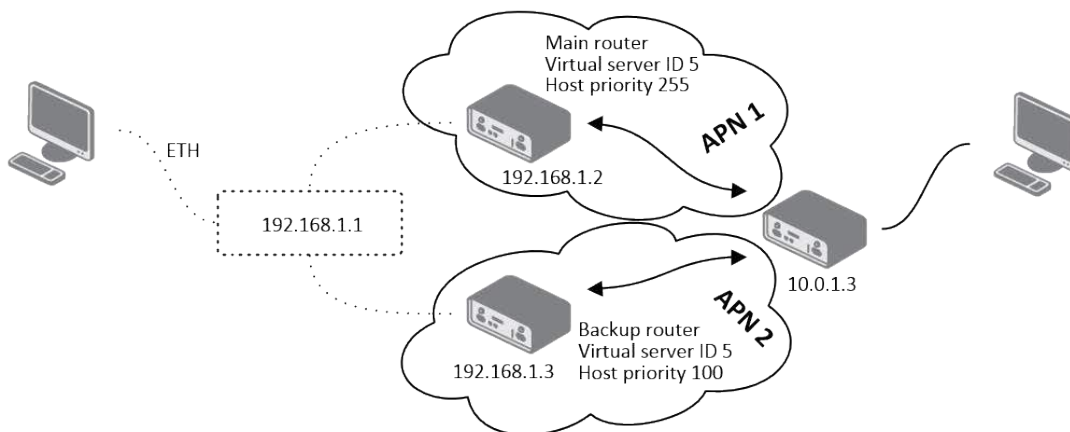


Figure 19: Topology of VRRP configuration example

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	
<input type="button" value="Apply"/>	

Figure 20: 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 21: Example of VRRP configuration – backup router

4.3 Mobile WAN Configuration



The SmartFlex SR300 (LAN version) does not display the Mobile WAN configuration option.

Select the *Mobile WAN* item in the *Configuration* menu section to enter the cellular network configuration page. See *Mobile WAN Configuration* page in Figure 23.

4.3.1 Connection to Mobile Network

If the *Create connection to mobile network* checkbox is checked, then the router will automatically attempt to establish a connection after booting up. You can specify the following parameters for each SIM card separately.

Item	Description
Carrier	Network carrier selection (for SmartStart SR305 router only).
APN	Network identifier (Access Point Name).
Username	The user name used for logging on to the GSM network.
Password	The password used for logging on to the GSM network. Enter valid characters only, see chap. 1.5.1!
Authentication	Authentication protocol used 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 Mode	Specifies the version of IP protocol used: <ul style="list-style-type: none"> • IPv4 – IPv4 protocol is used only (default). • IPv6 – IPv6 protocol is used only. • IPv4/IPv6 – IPv4 and IPv6 independent dual stack is enabled.
IP Address	For use in IPv4 and IPv4/IPv6 mode only. Specifies the IPv4 address of the SIM card. You manually enter the IP address only when mobile network carrier has assigned the IP address.
Dial Number	Specifies the telephone number which the router dials for a GPRS or CSD connection. The router uses the default telephone number *99***1 #.
Operator	Specifies the carrier code. You can specify this parameter as the PLMN preferred carrier code.

Continued on next page

Continued from previous page

Item	Description
Network type	<p>Specifies the type of protocol used in the mobile network.</p> <ul style="list-style-type: none"> • Automatic selection – The router automatically selects a transmission method according to the availability of transmission technologies. • It is also possible to select one of the following specific methods of data transmission: LTE, UMTS/HSPA, GPRS/EDGE.
PIN	Specifies the PIN used to unlock the SIM card. Use only if this is required by a given SIM card. The SIM card will be blocked after several failed attempts to enter the PIN.
MRU	Maximum Receive Unit – maximum size of packet that the router can receive via Mobile WAN. The default value is 1500 B. Other settings may cause the router to receive data incorrectly. Minimal value in IPv4 and IPv4/IPv6 mode: 128 B. Minimal value in IPv6 mode: 1280 B.
MTU	Maximum Transmission Unit – maximum size of packet that the router can transmit via Mobile WAN. The default value is 1500 B. Other settings may cause the router to transmit data incorrectly. Minimal value in IPv4 and IPv4/IPv6 mode: 128 B. Minimal value in IPv6 mode: 1280 B.

Table 21: 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 will not exceed the data transfer. If the MTU value is set too low, more frequent fragmentation of data will occur. More frequent fragmentation will mean a higher overhead and also the possibility of packet damage during defragmentation. In contrast, 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, the mobile network carrier will automatically assign an IP address. If you assign an IP address manually, then the router will access 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.



The correct PIN must be filled in. An incorrect PIN may 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, you should verify accuracy of the entered data. Alternatively, you could 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's side. When this value is set to *get from operator* the router will attempt 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, on the *DNS Server* pull down list select the value *set manually*. You can also fill-in the IPv4 or IPv6 address of the DNS server (or both) based on the IP Mode option.

4.3.3 Check Connection to Mobile Network Configuration



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

If the *Check Connection* item is set to *enabled* or *enabled + bind*, this activates checking of the connection to the mobile network. The router will automatically send ping requests to the specified domain or IP address (*Ping IP Address* or *Ping IPv6 Address* item) at regular time intervals (*Ping Interval*). In the case of an unsuccessful ping, a new one will be sent after ten seconds. If this ping a given IP address three times in a row, the router will terminate the connection and attempt to establish new ones. This checking can be set separate for two SIM cards. Send an ICMP (ICMPv6) ping 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 the routing table. Therefore, 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 of the connection to the mobile network.



For **SmartFlex SR305** routers connected to **Verizon** carrier (autodetected by the router): The retry interval for connecting to the mobile network prolongs with more retries. First two retries are done after 1 minute. Then the interval prolongs to 2, 8 and 15 minutes. The ninth and every other retry is done in 90 minutes interval.

Item	Description
Ping IP Address	Specifies the ping queries destination IPv4 address or domain name. Available in IPv4 and IPv4/IPv6 <i>IP Mode</i> .
Ping IPv6 Address	Specifies the ping queries destination IPv6 address or domain name. Available in IPv6 and IPv4/IPv6 <i>IP Mode</i> .
Ping Interval	Specifies the time interval between outgoing pings.
Ping Timeout	Time in seconds to wait for a Ping response.

Table 22: Check Connection to Mobile Network Configuration

4.3.4 Example of Check Connection Configuration

The figure below displays the following scenario: the connection to the mobile network in IPv4 *IP Mode* is controlled on the address 8.8.8.8 with a time interval of 60 seconds for the first SIM card and on the address www.google.com with the time interval 80 seconds for the second SIM card. In the case of an active 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 IPv6 Address		
Ping Interval	60	80 sec
Ping Timeout	60	80 sec

☒ Enable traffic monitoring

Figure 22: Example of Check Connection Configuration

4.3.5 Data Limit Configuration

Item	Description
Data Limit	Specifies the maximum expected amount of data transmitted (sent and received) over GPRS in one billing period (one month). Maximum value is 2 TB (2097152 MB).
Warning Threshold	Specifies a percentage of the "Data Limit" in the range of 50 % to 99 %. If the given percentage data limit is exceeded, the router will send 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 a given SIM card. When the service provider that issued the SIM card specifies the start of the billing period, the router will begin to count the amount of data transferred starting on this day.

Table 23: 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.

4.3.6 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, binary inputs state). 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.

Continued on next page

Continued from previous page

Item	Description
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.
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.
BIN0 State	<p>Configure the use of SIM cards based on binary input 0 state:</p> <ul style="list-style-type: none"> • not applicable – It is possible to use the SIM regardless of BIN0 state. • on – Only use the SIM card if the BIN0 state is logical 0 – voltage present. • off – Only use the SIM card if the BIN0 state is logical 1 – no voltage.
BIN1 State	<p>Configure the use of SIM cards based on binary input 1 state:</p> <ul style="list-style-type: none"> • not applicable – It is possible to use the SIM regardless of BIN1 state. • on – Only use the SIM card if the BIN1 state is logical 0 – voltage present. • off – Only use the SIM card if the BIN1 state is logical 1 – no voltage.

Table 24: 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>
Additive Constant	<p>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.</p>

Table 25: Parameters for SIM card switching



Specific behavior of **SmartFlex SR305** routers connected to **Verizon** carrier described in Chapter 4.3.3 applies on SIM cards switching, too. (It is single cellular module.)

1st Mobile WAN Configuration			
<input checked="" type="checkbox"/> Create connection to mobile network			
	1st SIM card	2nd SIM card	
APN *	advantech.agnep.cz		
Username *			
Password *			
Authentication	PAP or CHAP ▼	PAP or CHAP ▼	
IP Mode	IPv4 ▼	IPv4 ▼	
IP Address *			
Dial Number *			
Operator *			
Network Type	automatic selection ▼	automatic selection ▼	
PIN *			
MRU	1500	1500	bytes
MTU	1500	1500	bytes
DNS Settings	get from operator ▼	get from operator ▼	
DNS IP Address			
DNS IPv6 Address			
<i>(The feature of check connection to mobile network is necessary for uninterrupted operation)</i>			
Check Connection	disabled ▼	disabled ▼	
Ping IP Address			
Ping IPv6 Address			
Ping Interval			sec
Ping Timeout	10	10	sec
<input type="checkbox"/> Enable traffic monitoring			
Data Limit			MB
Warning Threshold			%
Accounting Start	1	1	
SIM Card	enabled ▼	enabled ▼	
Roaming State	not applicable ▼	not applicable ▼	
Data Limit State	not applicable ▼	not applicable ▼	
BIN0 State	not applicable ▼	not applicable ▼	
BIN1 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	60		min
Subsequent Timeout *			min
Additive Constant *			min
<input type="checkbox"/> Enable PPPoE bridge mode			
* can be blank			
<input type="button" value="Apply"/>			

Figure 23: Mobile WAN Configuration

4.3.7 Examples of SIM Card Switching Configuration

Example 1: Timeout Configuration

Mark the *Switch to default SIM card after timeout* check box, and fill-in the following values:

<input checked="" type="checkbox"/>	Switch to other SIM card when connection fails
<input checked="" type="checkbox"/>	Switch to default SIM card after timeout
Initial Timeout	<input type="text" value="60"/> min
Subsequent Timeout *	<input type="text" value="30"/> min
Additive Constant *	<input type="text" value="20"/> min

Figure 24: Configuration for SIM card switching Example 1

The first attempt to change to the default SIM card 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).

Example 2: Data Limit Switching

The following configuration illustrates a scenario in which the router changes to the second SIM card after exceeding the data limit of 800 MB on the first (default) SIM card. The router sends SMS upon reaching 400 MB (this settings has to be enabled on the *SMS Configuration* page). The accounting period starts on the 18th day of the month.

Data Limit	800		MB
Warning Threshold	50		%
Accounting Start	18		
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 25: Configuration for SIM card switching Example 2

4.3.8 PPPoE Bridge Mode Configuration

If you mark the *Enable PPPoE bridge mode* check box, 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.



For **SmartFlex SR306** and **SmartFlex SR307** routers: If you enable *PPPoE bridge mode*, it is not possible to use *SMS Configuration* features – the router will not send SMS and you can not control the router via SMS! *Send SMS* feature in *Administration* section will not work. Also in *Mobile WAN Status* there will be no signal strength data displayed. This is caused by using the same channel for sending AT commands in the cellular module in this version of the router. If the channel is occupied by AT commands for PPPoE bridge, there is no place for SMS AT commands.

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

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 26: PPPoE Configuration

Item	Description
Username	Username for secure access to PPPoE.
Password	Password for secure access to PPPoE. Enter valid characters only, see chap. 1.5.1!

Continued on next page

Continued from previous page

Item	Description
Authentication	<p>Authentication protocol in GSM network.</p> <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 Mode	<p>Specifies the version of IP protocol:</p> <ul style="list-style-type: none"> • IPv4 – IPv4 protocol is used only (default). • IPv6 – IPv6 protocol is used only. • IPv4/IPv6 – IPv4 and IPv6 dual stack is enabled.
MRU	<p>Specifies the Maximum Receiving Unit. The MRU identifies the maximum packet size, that the router can receive via PPPoE. The default value is 1492 B (bytes). Other settings can cause incorrect data transmission. Minimal value in IPv4 and IPv4/IPv6 mode is 128 B. Minimal value in IPv6 mode is 1280 B.</p>
MTU	<p>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 B (bytes). Other settings can cause incorrect data transmission. Minimal value in IPv4 and IPv4/IPv6 mode is 128 B. Minimal value in IPv6 mode is 1280 B.</p>
DNS Settings	<p>Can be set to obtain the DNS address from the server or to set it manually.</p>
DNS IP Address	<p>Manual setting of DNS address.</p>
DNS IP Address	<p>Manual setting of IPv6 DNS address.</p>
Interface	<p>Select an Ethernet interface.</p>
VLAN Tagging	<p>Select yes to turn on the VLAN tagging.</p>
VLAN ID	<p>Set the ID for VLAN tagging. The range is from 1 to 1000.</p>

Table 26: PPPoE configuration



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

4.5 WiFi Access Point Configuration



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



The WiFi module supports multi-role mode which allows to operate as access point (AP) and station (STA) simultaneously. The multichannel mode is supported as well, so the AP and the STA can operate on different channels.

Activate WiFi access point mode by selecting *Enable WiFi AP* at the top of the form. In this mode the router becomes an access point to which other devices in *station (STA)* mode can connect. You may set the following properties listed in the table below.



RADIUS (Remote Authentication Dial-In User Service) networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users is supported on WiFi. The router can be RADIUS client only (not the server) – typically as a WiFi AP (Access Point) negotiating with the RADIUS server.

Item	Description
Enable WiFi AP	Enable WiFi access point (AP).
IP Address	A fixed IP address of the WiFi interface. Use IPv4 notation in IPv4 column and IPv6 notation in IPv6 column. Shortened IPv6 notation is supported.
Subnet Mask / Prefix	Specifies a Subnet Mask for the IPv4 address. In the IPv6 column, fill in the Prefix for the IPv6 address – number in range 0 to 128.
Bridged	<p>Activates bridge mode:</p> <ul style="list-style-type: none"> • no – Bridged mode is not allowed (default value). WLAN network is not connected with LAN network of the router. • yes – Bridged mode is allowed. WLAN network is connected with one or more LAN networks of the router. In this case, the setting of most items in this table are ignored. Instead, the router uses the settings of the selected network interface (LAN).
Enable dynamic DHCP leases	Enable dynamic allocation of IP addresses using the DHCP (DHCPv6) server.
IP Pool Start	Beginning of the range of IP addresses which will be assigned to DHCP clients. Use proper notation in IPv4 and IPv6 column.
IP Pool End	End of the range of IP addresses which will be assigned to DHCP clients. Use proper notation in IPv4 and IPv6 column.
Lease Time	Time in seconds for which the client may use the IP address.

Continued on next page

Continued from previous page

Item	Description
Enable IPv6 prefix delegation	Enables prefix delegation configuration filled-in below.
Subnet ID	The decimal value of the Subnet ID of the Ethernet inter face. Maximum value depends on the Subnet ID Width.
Subnet ID Width	The maximum Subnet ID Width depends on your Site. Prefix – it is the remainder to 64 bits.
SSID	The unique identifier of WiFi network.
Broadcast SSID	<p>Method of broadcasting the unique identifier of SSID network in beacon frame and type of response to a request for sending the beacon frame.</p> <ul style="list-style-type: none"> • Enabled – SSID is broadcasted in beacon frame • Zero length – Beacon frame does not include SSID. Requests for sending beacon frame are ignored. • Clear – All SSID characters in beacon frames are replaced by 0. Original length is kept. Requests for sending beacon frames are ignored.
Client Isolation	If checked, the access point will isolate every connected client so they do not see each other (they are in different networks, they cannot PING between each other). If unchecked, the access point behavior is like a switch, but wireless – the clients are in the same LAN and can see each other.
Country Code	<p>Code of the country where the router is installed. This code must be entered in ISO 3166-1 alpha-2 format. If a <i>country code</i> isn't specified and the router has not implemented a system to determine this code, it will use "US" as the default <i>country code</i>.</p> <p>If no <i>country code</i> is specified or if the wrong country code is entered, the router may violate country-specific regulations for the use of WiFi frequency bands.</p> <p>This option is not available on SmartFlex SR305 routers – the "US" country code is set by default on these versions of router.</p>

Continued on next page

Continued from previous page

Item	Description
HW Mode	<p>HW mode of WiFi standard that will be supported by WiFi access point.</p> <ul style="list-style-type: none"> • IEEE 802.11b (2.4 GHz) • IEEE 802.11b+g (2.4 GHz) • IEEE 802.11b+g+n (2.4 GHz) • IEEE 802.11a (5 GHz) • IEEE 802.11a+n (5 GHz)
Channel	<p>The channel, where the WiFi AP is transmitting.</p> <p>Supported 2.4 GHz channels: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13.</p> <p>On SmartFlex SR305 routers only channels 1 to 11 are supported!</p> <p>Supported 5 GHz channels: 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165.</p>
BW 40 MHz	<p>The option for HW mode 802.11n which allows transmission on two standard 20 MHz channels simultaneously.</p> <p>If this channel is occupied, the BW 20 MHz channel is used instead.</p>
WMM	<p>Basic QoS for WiFi networks is enabled by checking this item. This version doesn't guarantee network throughput. It is suitable for simple applications that require QoS.</p>
Authentication	<p>Access control and authorization of users in the WiFi network.</p> <ul style="list-style-type: none"> • Open – Authentication is not required (free access point). • Shared – Basic authentication using WEP key. • WPA-PSK – Authentication using higher authentication methods PSK-PSK. • WPA2-PSK – WPA-PSK using newer AES encryption. • WPA-Enterprise – RADIUS authentication done by external server via username and password. • WPA2-Enterprise – RADIUS authentication with better encryption. • 802.1X – RADIUS authentication with port-based Network Access Control (PNAC) using encapsulation of the Extensible Authentication Protocol (EAP) over LAN – EAPOL.

Continued on next page

Continued from previous page

Item	Description
Encryption	<p>Type of data encryption in the WiFi network:</p> <ul style="list-style-type: none"> • None – No data encryption. • WEP – Encryption using static WEP keys. This encryption can be used for <i>Shared</i> authentication. • TKIP – Dynamic encryption key management that can be used for <i>WPA-PSK</i> and <i>WPA2-PSK</i> authentication. • AES – Improved encryption used for <i>WPA2-PSK</i> authentication.
WEP Key Type	<p>Type of WEP key for WEP encryption:</p> <ul style="list-style-type: none"> • ASCII – WEP key in ASCII format. • HEX – WEP key in hexadecimal format.
WEP Default Key	This specifies the default WEP key.
WEP Key 1–4	<p>Allows entry of four different WEP keys:</p> <ul style="list-style-type: none"> • WEP key in ASCII format must be entered in quotes. This key can be specified in the following lengths. <ul style="list-style-type: none"> – 5 ASCII characters (40b WEP key) – 13 ASCII characters (104b WEP key) – 16 ASCII characters (128b WEP key) • WEP key in hexadecimal format must be entered in hexadecimal digits. This key can be specified in the following lengths. <ul style="list-style-type: none"> – 10 hexadecimal digits (40b WEP key) – 26 hexadecimal digits (104b WEP key) – 32 hexadecimal digits (128b WEP key)
WPA PSK Type	<p>The possible key options for WPA-PSK authentication.</p> <ul style="list-style-type: none"> • 256-bit secret • ASCII passphrase • PSK File

Continued on next page

Continued from previous page

Item	Description
WPA PSK	Key for WPA-PSK authentication. This key must be entered according to the selected WPA PSK type as follows: <ul style="list-style-type: none"> • 256-bit secret – 64 hexadecimal digits • ASCII passphrase – 8 to 63 characters • PSK File – absolute path to the file containing the list of pairs (PSK key, MAC address)
RADIUS Auth Server IP	IPv4 or IPv6 address of the RADIUS server. Only with one of RADIUS authentications selected.
RADIUS Auth Password	RADIUS server access password. Only with one of RADIUS authentications selected.
RADIUS Auth Port	RADIUS server port. The default is 1812. Only with one of RADIUS authentications selected.
RADIUS Acct Server IP	IPv4 or IPv6 address of the RADIUS accounting server. Define only if different from the authentication and authorization server. Only with one of RADIUS authentications selected.
RADIUS Acct Password	Access password of RADIUS accounting server. Define only if different from the authentication and authorization server. Only with one of RADIUS authentications selected.
RADIUS Acct Port	RADIUS accounting server port. The default is 1813. Define only if different from the authentication and authorization server. Only with one of RADIUS authentications selected.
Access List	Mode of Access/Deny list. <ul style="list-style-type: none"> • Disabled – Access/Deny list is not used. • Accept – Clients in Accept/Deny list can access the network. • Deny – Clients in Access/Deny list cannot access the network.
Accept/Deny List	Accept or Deny list of client MAC addresses that set network access. Each MAC address is separated by new line.

Continued on next page

Continued from previous page

Item	Description
Syslog Level	Logging level, when system writes to the system log. <ul style="list-style-type: none">• Verbose debugging – The highest level of logging.• Debugging• Informational – Default level of logging.• Notification• Warning – The lowest level of system communication.
Extra options	Allows the user to define additional parameters.

Table 27: WiFi Configuration

WiFi AP Configuration			
<input type="checkbox"/> Enable WiFi AP			
IP Address	IPv4	IPv6	
Subnet Mask / Prefix			
Bridged	no		
<input checked="" type="checkbox"/> Enable dynamic DHCP leases			
IP Pool Start	IPv4	IPv6	
IP Pool End	192.168.3.254		
Lease Time	600	600	sec
<input type="checkbox"/> Enable IPv6 prefix delegation			
Subnet ID *			
Subnet ID Width *		bits	
SSID			
Broadcast SSID	enabled		
Client Isolation	disabled		
Country Code *			
HW Mode	IEEE 802.11b		
Channel	1		
BW 40 MHz	disabled		
WMM	disabled		
Authentication	open		
Encryption	none		
WEP Key Type	ASCII		
WEP Default Key	1		
WEP Key 1			
WEP Key 2			
WEP Key 3			
WEP Key 4			
WPA PSK Type	256-bit secret		
WPA PSK			
RADIUS Auth Server IP			
RADIUS Auth Password			
RADIUS Auth Port *	1812		
RADIUS Acct Server IP *			
RADIUS Acct Password *			
RADIUS Acct Port *	1813		
Access List	disabled		
Accept/Deny List			
Syslog Level	informational		
Extra options *			
* can be blank			
<input type="button" value="Apply"/>			

Figure 27: WiFi Access Point Configuration

4.6 WiFi Station Configuration



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



The WiFi module supports multi-role mode which allows to operate as access point (AP) and station (STA) simultaneously. The multichannel mode is supported as well, so the AP and the STA can operate on different channels.

Activate WiFi station mode by selecting *Enable WiFi STA* at the top of the form. In this mode the router becomes a client station. It will receive data packets from the available access point (AP) and send data from cable connection via the WiFi network. You may set the following properties listed in the table below.



In WiFi STA mode, only the authentication method EAP-PEAP/MSCHAPv2 (both PEAPv0 and PEAPv1) and EAP-TLS are supported.

Item	Description
Enable WiFi STA	Enable WiFi station (STA).
DHCP Client	Activates/deactivates DHCP client. If in IPv6 column, the DHCPv6 client is enabled.
IP Address	A fixed IP address of the WiFi interface. Use IPv4 notation in IPv4 column and IPv6 notation in IPv6 column. Shortened IPv6 notation is supported.
Subnet Mask / Prefix	Specifies a Subnet Mask for the IPv4 address. In the IPv6 column, fill in the Prefix for the IPv6 address – number in range 0 to 128.
Default Gateway	Specifies the IP address of a default gateway. If filled-in, every packet with the destination not found in the routing table is sent there. Use proper IP address notation in IPv4 and IPv6 column.
DNS Server	Specifies the IP address of the DNS server. When the IP address is not found in the Routing Table, the this DNS server is requested. Use proper IP address notation in IPv4 and IPv6 column.
SSID	The unique identifier of WiFi network.
Probe Hidden SSID	Probes hidden SSID
Country Code	Code of the country where the router is installed. This code must be entered in ISO 3166-1 alpha-2 format. If a <i>country code</i> isn't specified and the router has not implemented a system to determine this code, it will use "US" as the default <i>country code</i> . If no <i>country code</i> is specified or if the wrong country code is entered, the router may violate country-specific regulations for the use of WiFi frequency bands. This option is not available on SmartFlex SR305 routers – the "US" country code is set by default on these versions of router.

Continued on next page

Continued from previous page

Item	Description
Authentication	<p>Access control and authorization of users in the WiFi network.</p> <ul style="list-style-type: none"> • Open – Authentication is not required (free access point). • Shared – Basic authentication using WEP key. • WPA-PSK – Authentication using higher authentication methods PSK-PSK. • WPA2-PSK – WPA-PSK using newer AES encryption. • WPA-Enterprise – RADIUS authentication done by external server via username and password. • WPA2-Enterprise – RADIUS authentication with better encryption. • 802.1X – RADIUS authentication with port-based Network Access Control (PNAC) using encapsulation of the Extensible Authentication Protocol (EAP) over LAN – EAPOL.
Encryption	<p>Type of data encryption in the WiFi network:</p> <ul style="list-style-type: none"> • None – No data encryption. • WEP – Encryption using static WEP keys. This encryption can be used for <i>Shared</i> authentication. • TKIP – Dynamic encryption key management that can be used for <i>WPA-PSK</i> and <i>WPA2-PSK</i> authentication. • AES – Improved encryption used for <i>WPA2-PSK</i> authentication.
WEP Key Type	<p>Type of WEP key for WEP encryption:</p> <ul style="list-style-type: none"> • ASCII – WEP key in ASCII format. • HEX – WEP key in hexadecimal format.
WEP Default Key	This specifies the default WEP key.

Continued on next page

Continued from previous page

Item	Description
WEP Key 1–4	<p>Allows entry of four different WEP keys:</p> <ul style="list-style-type: none"> • WEP key in ASCII format must be entered in quotes. This key can be specified in the following lengths. <ul style="list-style-type: none"> – 5 ASCII characters (40b WEP key) – 13 ASCII characters (104b WEP key) – 16 ASCII characters (128b WEP key) • WEP key in hexadecimal format must be entered in hexadecimal digits. This key can be specified in the following lengths. <ul style="list-style-type: none"> – 10 hexadecimal digits (40b WEP key) – 26 hexadecimal digits (104b WEP key) – 32 hexadecimal digits (128b WEP key)
WPA PSK Type	<p>The possible key options for WPA-PSK authentication.</p> <ul style="list-style-type: none"> • 256-bit secret • ASCII passphrase • PSK File
WPA PSK	<p>Key for WPA-PSK authentication. This key must be entered according to the selected WPA PSK type as follows:</p> <ul style="list-style-type: none"> • 256-bit secret – 64 hexadecimal digits • ASCII passphrase – 8 to 63 characters • PSK File – absolute path to the file containing the list of pairs (PSK key, MAC address)
RADIUS EAP Authentication	Type of authentication protocol (EAP-PEAP/MSCHAPv2 or EAP-TLS).
RADIUS CA Certificate	Definition of CA certificate for EAP-TLS authentication protocol.
RADIUS Local Certificate	Definition of local certificate for EAP-TLS authentication protocol.
RADIUS Local Private Key	Definition of local private key for EAP-TLS authentication protocol.

Continued on next page

Continued from previous page

Item	Description
RADIUS Identity	RADIUS user name – identity. Only with one of RADIUS authentications selected.
RADIUS Password	RADIUS access password. Only with one of RADIUS authentications selected.
Syslog Level	Logging level, when system writes to the system log. <ul style="list-style-type: none"> • Verbose debugging – The highest level of logging. • Debugging • Informational – Default level of logging. • Notification • Warning – The lowest level of system communication.
Extra options	Allows the user to define additional parameters.

Table 28: WLAN Configuration

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

WiFi STA Configuration		
<input type="checkbox"/> Enable WiFi STA		
	IPv4	IPv6
DHCP Client	<input type="text" value="enabled"/>	<input type="text" value="enabled"/>
IP Address	<input type="text"/>	<input type="text"/>
Subnet Mask / Prefix	<input type="text"/>	<input type="text"/>
Default Gateway	<input type="text"/>	<input type="text"/>
DNS Server	<input type="text"/>	<input type="text"/>
SSID		
Probe Hidden SSID	<input type="text" value="disabled"/>	
Country Code *	<input type="text"/>	
Authentication	<input type="text" value="open"/>	
Encryption	<input type="text" value="none"/>	
WEP Key Type	<input type="text" value="ASCII"/>	
WEP Default Key	<input type="text" value="1"/>	
WEP Key 1	<input type="text"/>	
WEP Key 2	<input type="text"/>	
WEP Key 3	<input type="text"/>	
WEP Key 4	<input type="text"/>	
WPA PSK Type	<input type="text" value="256-bit secret"/>	
WPA PSK	<input type="text"/>	
RADIUS EAP Authentication	<input type="text" value="EAP-PEAP/MSCHAPv2"/>	
RADIUS CA Certificate	<input type="text"/>	
	<input type="button" value="Choose File"/> No file chosen	
RADIUS Local Certificate	<input type="text"/>	
	<input type="button" value="Choose File"/> No file chosen	
RADIUS Local Private Key	<input type="text"/>	
	<input type="button" value="Choose File"/> No file chosen	
RADIUS Identity	<input type="text"/>	
RADIUS Password	<input type="text"/>	
Syslog Level	<input type="text" value="informational"/>	
Extra options *	<input type="text"/>	
* can be blank		
<input type="button" value="Apply"/>		

Figure 28: WiFi Station Configuration

4.7 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	
<input type="checkbox"/> Enable backup routes switching	
Mode	Single WAN
<input type="checkbox"/> Enable backup routes switching for Mobile WAN	
Priority	1st
Weight	
<input type="checkbox"/> Enable backup routes switching for PPPoE	
Priority	1st
Ping IP Address	
Ping IPv6 Address	
Ping Interval	sec
Ping Timeout	10 sec
Weight	
<input type="checkbox"/> Enable backup routes switching for WiFi STA	
Priority	1st
Ping IP Address	
Ping IPv6 Address	
Ping Interval	sec
Ping Timeout	10 sec
Weight	
<input type="checkbox"/> Enable backup routes switching for Primary LAN	
Priority	1st
Ping IP Address	
Ping IPv6 Address	
Ping Interval	sec
Ping Timeout	10 sec
Weight	
<input type="checkbox"/> Enable backup routes switching for Secondary LAN	
Priority	1st
Ping IP Address	
Ping IPv6 Address	
Ping Interval	sec
Ping Timeout	10 sec
Weight	
<input type="button" value="Apply"/>	

Figure 29: 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 29: 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 WiFi STA*, *Enable backup routes switching for Primary LAN*, *Enable backup routes switching for Secondary LAN* or *Enable backup routes switching for Tertiary 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:



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. See chapter 4.3.1.

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. You can fill-in one or both Ping IP Addresses (IPv4 and IPv6) – based on IP protocol used on particular network interface and WAN connection settings. IPv4 and IPv6 are dual stack implemented in the router. Any changes made to settings will be applied after pressing the *Apply* button.

Item	Description
Priority	Priority for the type of connection (network interface).
Ping IP Address	Destination IPv4 address or domain name of ping queries to check the connection.
Ping IPv6 Address	Destination IPv6 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 30: Backup Routes

4.7.1 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 (usbX)
- PPPoE (ppp0)
- WiFi STA (wlan0)
- Secondary LAN (eth1)
- Tertiary LAN (eth2)
- Primary LAN (eth0)

Example of default priorities: *Backup Routes* are disabled. The router selects the *Secondary LAN* as the default route only if you unmark the *Create connection to mobile network* check box on the *Mobile WAN* page, unmark the *Create PPPoE connection* check box on the *PPPoE* page and unmark the *Enable WiFi* on the *WiFi* page (or use WiFi in AP mode). To select the *Primary LAN*, delete the IP address from the *Secondary LAN* page and disable the *DHCP Client* for the *Secondary LAN*.



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.

4.8 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 30.

IPv4 Static Routes Configuration

☐ Enable IPv4 static routes

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

* can be blank

Apply

Figure 30: Static Routes Configuration

The description of all items is listed in Table 31.

Item	Description
Enable IPv4 (IPv6) 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 31: Static Routes configuration

4.9 Firewall Configuration

The first security element for incoming packets is a check of the enabled source IP addresses and destination ports. There is independent IPv4 and IPv6 firewall since there is dual stack IPv4 and IPv6 implemented in the router. If you click the *Firewall* item in the *Configuration* menu on the left, it will expand to *IPv4* and *IPv6* options and you can click *IPv6* to enable and configure the IPv6 firewall – see Figure below. The configuration fields have the same meaning in the *IPv4 Firewall Configuration* and *IPv6 Firewall Configuration* forms.

You can specify the rules for IP addresses, protocols and ports to allow or deny the access to the router and internal network connected behind the router. To enable this function, tick the *Enable filtering of incoming packets* check box located at the top of the *IPv4 (IPv6) Firewall Configuration* page. Accessibility is checked against the IP address table. This means that access is permitted only to addresses allowed in the table. It is possible to specify up to eight remote IP addresses for access/denial. You can specify the following parameters:

Item	Description
Source	IP address the rule applies to. Use IPv4 address in <i>IPv4 Firewall Configuration</i> and IPv6 address in <i>IPv6 Firewall Configuration</i> .
Protocol	Specifies the protocol the rule applies to: <ul style="list-style-type: none"> • all – The rule applies to all protocols. • TCP – The rule applies to TCP protocol. • UDP – The rule applies to UDP protocol. • GRE – The rule applies to GRE protocol. • ESP – The rule applies to ESP protocol. • ICMP/ICMPv6 – The rule applies to ICMP protocol. In <i>IPv6 Firewall Configuration</i> there is the ICMPv6 option.
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 rule – 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 32: 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.

IPv6 Firewall Configuration				
<input type="checkbox"/> Enable filtering of incoming packets				
Source *	Protocol	Target Port(s) *	Action	
<input type="checkbox"/> <input type="text"/>	all ▼	<input type="text"/>	allow ▼	
<input type="checkbox"/> <input type="text"/>	all ▼	<input type="text"/>	allow ▼	
<input type="checkbox"/> <input type="text"/>	all ▼	<input type="text"/>	allow ▼	
<input type="checkbox"/> <input type="text"/>	all ▼	<input type="text"/>	allow ▼	
<input type="checkbox"/> <input type="text"/>	all ▼	<input type="text"/>	allow ▼	
<input type="checkbox"/> <input type="text"/>	all ▼	<input type="text"/>	allow ▼	
<input type="checkbox"/> <input type="text"/>	all ▼	<input type="text"/>	allow ▼	
<input type="checkbox"/> <input type="text"/>	all ▼	<input type="text"/>	allow ▼	
<input type="checkbox"/> Enabled filtering of forwarded packets				
Source *	Destination *	Protocol	Target Port(s) *	Action
<input type="checkbox"/> <input type="text"/>	<input type="text"/>	all ▼	<input type="text"/>	allow ▼
<input type="checkbox"/> <input type="text"/>	<input type="text"/>	all ▼	<input type="text"/>	allow ▼
<input type="checkbox"/> <input type="text"/>	<input type="text"/>	all ▼	<input type="text"/>	allow ▼
<input type="checkbox"/> <input type="text"/>	<input type="text"/>	all ▼	<input type="text"/>	allow ▼
<input type="checkbox"/> <input type="text"/>	<input type="text"/>	all ▼	<input type="text"/>	allow ▼
<input type="checkbox"/> <input type="text"/>	<input type="text"/>	all ▼	<input type="text"/>	allow ▼
<input type="checkbox"/> <input type="text"/>	<input type="text"/>	all ▼	<input type="text"/>	allow ▼
<input type="checkbox"/> <input type="text"/>	<input type="text"/>	all ▼	<input type="text"/>	allow ▼
<input type="checkbox"/> Enable filtering of locally destined packets				
<input type="checkbox"/> Enable protection against DoS attacks				
* can be blank				
<input type="button" value="Apply"/>				

Figure 31: Firewall Configuration – IPv6 Firewall

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 the rule applies to. Use IPv4 address in <i>IPv4 Firewall Configuration</i> and IPv6 address in <i>IPv6 Firewall Configuration</i> .
Destination	Destination IP address the rule applies to. Use IPv4 address in <i>IPv4 Firewall Configuration</i> and IPv6 address in <i>IPv6 Firewall Configuration</i> .
Protocol	Specifies the protocol the rule applies to: <ul style="list-style-type: none"> • all – The rule applies to all protocols. • TCP – The rule applies to TCP protocol. • UDP – The rule applies to UDP protocol. • GRE – The rule applies to GRE protocol. • ESP – The rule applies to ESP protocol. • ICMP/ICMPv6 – The rule applies to ICMP protocol. In <i>IPv6 Firewall Configuration</i> there is the ICMPv6 option.
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 rule – 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 33: Forwarding filtering

When you enable the *Enable filtering of locally destined packets* function, the router drops the 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.

4.9.1 Example of the IPv4 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 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

See the network topology and configuration form in the figures below.

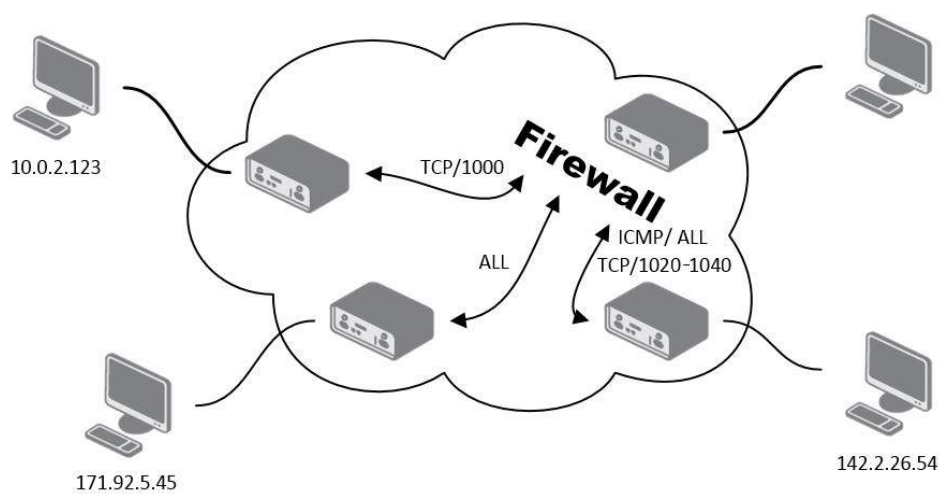


Figure 32: Topology for the IPv4 Firewall Configuration Example

Firewall Configuration

☒ Enable filtering of incoming packets

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 ▼

☐ Enabled filtering of forwarded packets

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

☐ Enable filtering of locally destined packets

☐ Enable protection against DoS attacks

** can be blank*

Figure 33: IPv4 Firewall Configuration Example

4.10 NAT Configuration

To configure the address translation function, click on *NAT* in the *Configuration* section of the main menu. There is independent IPv4 and IPv6 NAT configuration since there is dual stack IPv4 and IPv6 implemented in the router. The *NAT* item in the menu on the left will expand to *IPv4* and *IPv6* options and you can click *IPv6* to enable and configure the IPv6 NAT – see Figure below. The configuration fields have the same meaning in the *IPv4 NAT Configuration* and *IPv6 NAT Configuration* forms.

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 – TCP or UDP.
Server IPv4 address	In <i>IPv4 NAT Configuration</i> only. IPv4 address where the router forwards incoming data.
Server IPv6 address	In <i>IPv6 NAT Configuration</i> only. IPv6 address where the router forwards incoming data.

Table 34: NAT Configuration

If you require more than sixteen NAT rules, insert the remaining rules into the Startup Script. The *Startup Script* dialog is located on *Scripts* page in the *Configuration* section of the menu. When creating your rules in the Startup Script, use this command for IPv4 NAT:



```
iptables -t nat -A pre_nat -p tcp --dport [PORT_PUBLIC] -j DNAT
--to-destination [IPADDR] : [PORT_PRIVATE]
```

Enter the IP address [IPADDR], the public ports numbers [PORT_PUBLIC], and private [PORT_PRIVATE] in place of square brackets. For IPv6 NAT use *ip6tables* command with same options.:



```
ip6tables -t nat -A napt -p tcp --dport [PORT_PUBLIC] -j DNAT
--to-destination [IP6ADDR] : [PORT_PRIVATE]
```

If you enable the following options and enter the port number, the router allows you to remotely access to the router from WAN (Mobile WAN) interface.

NAT Configuration			
Public Port(s)	Private Port(s)	Type	Server IP Address
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	

☐ Enable remote HTTP access on port

☐ Enable remote HTTPS access on port

☐ Enable remote 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 34: NAT – IPv6 NAT Configuration

Item	Description
Enable remote HTTP access on port	This option sets the redirect from HTTP to HTTPS only (disabled in default configuration).
Enable remote HTTPS access on port	If 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 access to the router using FTP (disabled in default configuration).
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 access to the router using Telnet (disabled in default configuration).
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 35: Remote Access Configuration

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

Use the following parameters to set the routing of incoming data from the WAN (Mobile WAN) 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 IPv4/IPv6 Address</i> field. The router can forward incoming data from a GPRS to a computer with the assigned IP address.
Default Server IP Address	In <i>IPv4 NAT Configuration</i> only. The IPv4 address.
Default Server IPv6 Address	In <i>IPv6 NAT Configuration</i> only. The IPv6 address.

Table 36: Configuration of Send all incoming packets to server

Example 2: IPv4 NAT Configuration with More Equipment Connected

In this example, using the switch you can connect more devices behind the router. Every device connected behind the router has its own IP address. Enter the address in the *Server IPv Address* field in the NAT dialog. The devices are communicating on port 80, but you can set port forwarding using the *Public Port* and *Private Port* fields in the NAT dialog. You have now configured the router to access the 192.168.1.2:80 socket behind the router when accessing the IP address 10.0.0.1:81 from the Internet. If you send a ping request to the public IP address of the router (10.0.0.1), the router responds as usual (not forwarding). And since the *Send all remaining incoming packets to default server* is inactive, the router denies connection attempts.

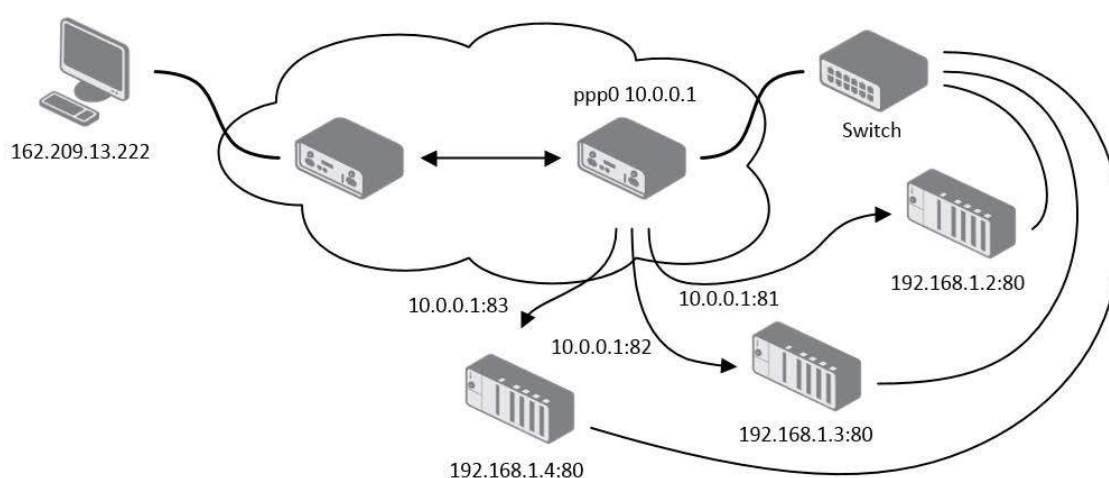


Figure 37: Topology for NAT Configuration Example 2

www.lucom.de

78

4.11 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. IPv4 and IPv6 dual stack is supported.

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. • UDIPv6 – The OpenVPN communicates using UDP over IPv6. • TCPv6 server – The OpenVPN communicates using TCP over IPv6 in server mode. • TCPv6 client – The OpenVPN communicates using TCP over IPv6 in client mode.
UDP/TCP port	Specifies the port of the relevant protocol (UDP or TCP).
Remote IP Address	Specifies the IPv4, IPv6 address or domain name of the opposite side of the tunnel.
Remote Subnet	IPv4 address of a network behind opposite side of the tunnel.
Remote Subnet Mask	IPv4 subnet mask of a network behind opposite tunnel's side.
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 IPv4 address of a local interface. For proper routing it is recommended to fill-in any IPv4 address from local range even if you are using IPv6 tunnel only.
Remote Interface IP Address	Specifies the IPv4 address of the interface of opposite side of the tunnel. For proper routing it is recommended to fill-in any IPv4 address from local range even if you are using IPv6 tunnel only.

Continued on next page

Continued from previous page

Item	Description
Remote IPv6 Subnet	IPv6 address of the remote IPv6 network. Equivalent of the <i>Remote Subnet</i> in IPv4 section.
Remote IPv6 Prefix	IPv6 prefix of the remote IPv6 network. Equivalent of the <i>Remote Subnet Mask</i> in IPv4 section.
Local Interface IPv6 Address	Specifies the IPv6 address of a local interface.
Remote Interface IPv6 Address	Specifies the IPv6 address of the interface of opposite side of the tunnel.
Ping Interval	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 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 keep the tunnel secure.
Max Fragment Size	Maximum size of a sent packet.
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 tunnel. • applied – NAT rules are applied to the OpenVPN tunnel.

Continued on next page

Continued from previous page

Item	Description
Authenticate Mode	<p>Specifies the authentication mode:</p> <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, see chap. 1.5.1!
Extra Options	Specifies additional parameters for the OpenVPN tunnel, such as DHCP options. The parameters are proceeded by two dashes. For possible parameters see the help text in the router using SSH – run the <code>openvpnd --help</code> command.

Table 37: 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"/>
Remote IPv6 Subnet *	<input type="text"/>
Remote IPv6 Subnet Prefix Length *	<input type="text"/>
Local Interface IPv6 Address *	<input type="text"/>
Remote Interface IPv6 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"/>
DH Parameters	<input type="text"/>
Local Certificate	<input type="text"/>
Local Private Key	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Extra Options *	<input type="text"/>
* can be blank	
<input type="button" value="Apply"/>	

Figure 39: OpenVPN tunnel configuration

4.11.1 Example of the OpenVPN Tunnel Configuration in IPv4 Network

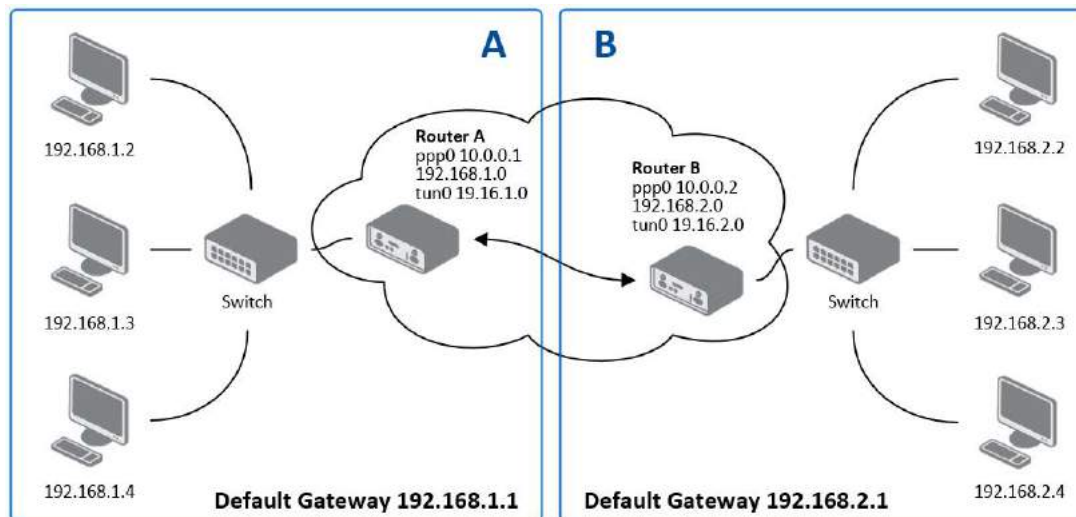


Figure 40: Topology of OpenVPN Configuration Example

OpenVPN tunnel configuration:

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

Table 38: OpenVPN Configuration Example



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

4.12 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. IPv4 and IPv6 tunnels are supported (dual stack), you can transport IPv6 traffic through IPv4 tunnel and vice versa.



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.
Host IP Mode	<ul style="list-style-type: none"> • IPv4 – The router communicates via IPv4 with the opposite side of the tunnel. • IPv6 – The router communicates via IPv4 with the opposite side of the tunnel.
Remote IP Address	IPv4, IPv6 address or domain name of the remote side of the tunnel, based in the <i>Host IP Mode</i> above.
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> .
Tunnel IP Mode	<ul style="list-style-type: none"> • IPv4 – The IPv4 communication runs inside the tunnel. • IPv6 – The IPv6 communication runs inside the tunnel.
First Remote Subnet	IPv4 or IPv6 address of a network behind remote side of the tunnel, based on <i>Tunnel IP Mode</i> above.
First Remote Subnet Mask/Prefix	IPv4 subnet mask of a network behind remote side of the tunnel, or IPv6 prefix (single number 0 to 128).

Continued on next page

Continued from previous page

Item	Description
Second Remote Subnet	IPv4 or IPv6 address of the second network behind remote side of the tunnel, based on <i>Tunnel IP Mode</i> above. For <i>IKE Protocol</i> = IKEv2 only.
Second Remote Subnet Mask/Prefix	IPv4 subnet mask of the second network behind remote side of the tunnel, or IPv6 prefix (single number 0 to 128). For <i>IKE Protocol</i> = IKEv2 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	IPv4 or IPv6 address of a local network, based on <i>Tunnel IP Mode</i> above.
First Local Subnet Mask/Prefix	IPv4 subnet mask of a local network, or IPv6 prefix (single number 0 to 128).
Second Local Subnet	IPv4 or IPv6 address of the second local network, based on <i>Tunnel IP Mode</i> above. For <i>IKE Protocol</i> = IKEv2 only.
Second Local Subnet Mask/Prefix	IPv4 subnet mask of the second local network, or IPv6 prefix (single number 0 to 128). 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!

Continued on next page

Continued from previous page

Item	Description
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 more 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.
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.

Continued on next page

Continued from previous page

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

Table 39: 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 proceeds 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

1st IPsec Tunnel Configuration		
<input type="checkbox"/> Create 1st IPsec tunnel		
Description *	<input type="text"/>	
Host IP Mode	IPv4 ▼	
Remote IP Address *	<input type="text"/>	
Tunnel IP Mode	IPv4 ▼	
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	<input type="text" value="3600"/>	sec
IKE Lifetime	<input type="text" value="3600"/>	sec
Rekey Margin	<input type="text" value="540"/>	sec
Rekey Fuzz	<input type="text" value="100"/>	%
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 41: IPsec Tunnels Configuration

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.

4.12.1 Example of the IPsec Tunnel Configuration in IPv4 Network

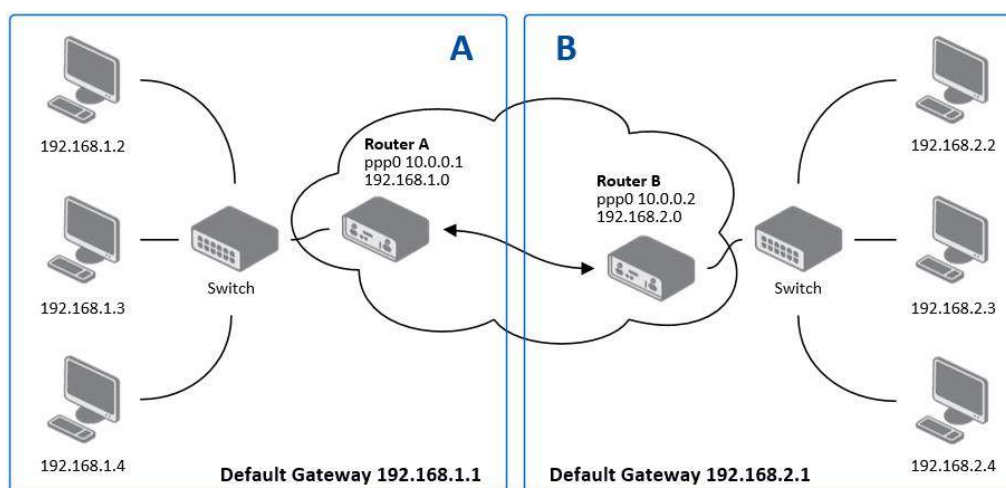


Figure 42: Topology of IPsec Configuration Example

IPsec tunnel configuration:

Configuration	A	B
Host IP Mode	IPv4	IPv4
Remote IP Address	10.0.0.2	10.0.0.1
Tunnel IP Mode	IPv4	IPv4
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 40: Example IPsec configuration



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

4.13 GRE Tunnels Configuration



GRE is an unencrypted protocol. GRE via IPv6 is not supported.

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 41: 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 43: GRE Tunnel Configuration

4.13.1 Example of the GRE Tunnel Configuration

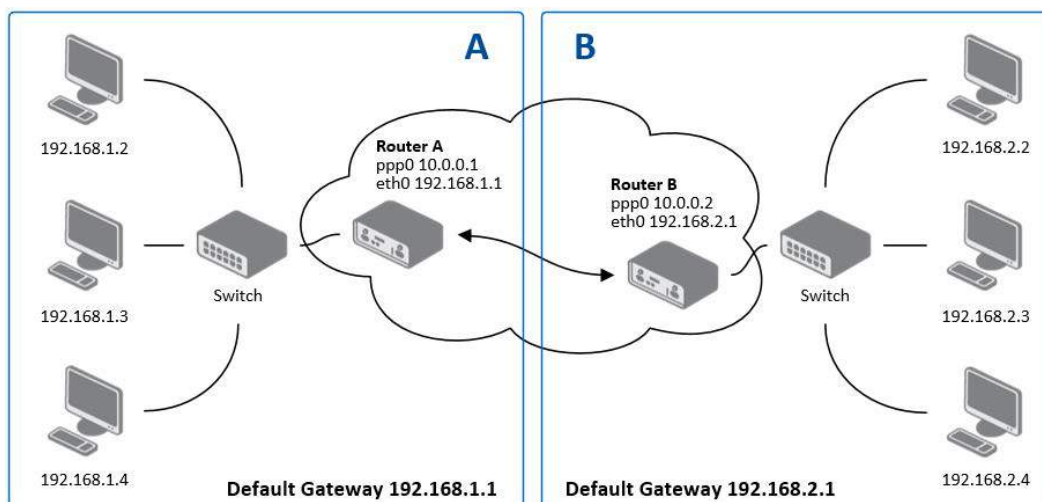


Figure 44: Topology of GRE Tunnel Configuration Example

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 42: GRE Tunnel Configuration Example



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

4.14 L2TP Tunnel Configuration



L2TP is an unencrypted protocol. L2TP via IPv6 is not supported.

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, see chap. 1.5.1.

Table 43: L2TP Tunnel Configuration

Figure 45: L2TP Tunnel Configuration

4.14.1 Example of the L2TP Tunnel Configuration

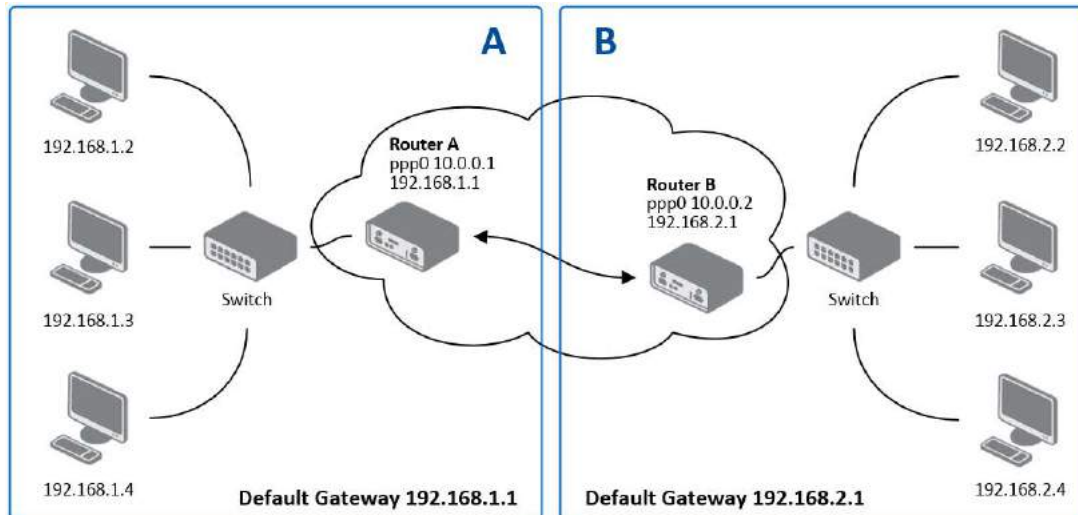


Figure 46: Topology of L2TP Tunnel Configuration Example

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 44: L2TP Tunnel Configuration Example

4.15 PPTP Tunnel Configuration



PPTP is an unencrypted protocol. PPTP via IPv6 is not supported.

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, see chap. 1.5.1!

Table 45: PPTP Tunnel Configuration

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

Figure 47: PPTP Tunnel Configuration



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

4.15.1 Example of the PPTP Tunnel Configuration

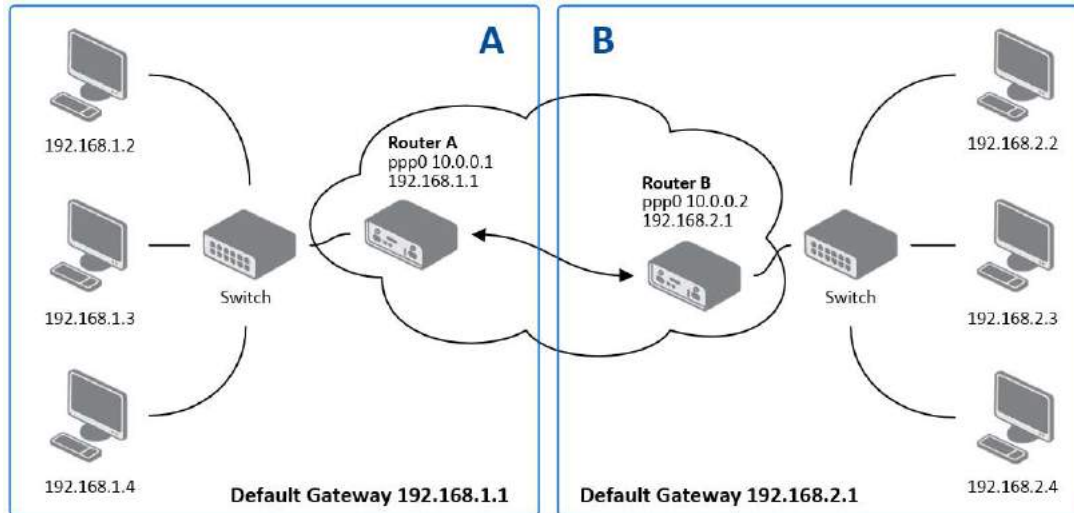


Figure 48: Topology of PPTP Tunnel Configuration Example

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 46: PPTP Tunnel Configuration Example

4.16 Services

4.16.1 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, see chap. 1.5.1!
IP Mode	Specifies the version of IP protocol: <ul style="list-style-type: none"> • IPv4 – IPv4 protocol is used only (default). • IPv6 – IPv6 protocol is used only. • IPv4/IPv6 – IPv4 and IPv6 dual stack is enabled.
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 47: DynDNS Configuration

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

Figure 49: DynDNS Configuration Example



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 4.10.

4.16.2 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 50: Enabling of FTP server

4.16.3 HTTP

HTTP protocol (Hypertext Transfer Protocol) is internet protocol used for exchange of hypertext 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 48: 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 51: Configuration of HTTP and HTTPS services

4.16.4 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. IPv6 Time Servers are supported.

- 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	IPv4 address, IPv6 address or domain name of primary NTP server.
Secondary NTP Server Address	IPv4 address, IPv6 address or domain name 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 49: 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 52: Example of NTP Configuration

4.16.5 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 mode for PAM authentication can be set up together with the configuration of connection to the RADIUS server. You can configure up to two connections to the RADIUS server.

Item	Description
Mode	<p>Choose one of these modes:</p> <ul style="list-style-type: none"> • local user database – Authenticate against the local user database only. • RADIUS with fallback – Authenticate against the RADIUS server and then against the local database in case the RADIUS server is not accessible. • 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!
Server	Address of the RADIUS server.
Port	Port of the RADIUS server.
Secret	Secret to verify the user's identity.
Timeout	Timeout for authentication to the RADIUS server.

Table 50: Configuration of PAM

PAM Configuration				
Mode local user database ▼				
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
* can be blank				
<input type="button" value="Apply"/>				

Figure 53: Configuration of PAM

4.16.6 SNMP

The *SNMP* page allows you to configure the SNMP v1/v2 or v3 agent which sends information about the router (and its expansion ports) 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 51: 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. 1.5.1!
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. 1.5.1!

Table 52: SNMPv3 Configuration

Activating the *Enable I/O extension* function allows you monitor the binary I/O inputs on the router.



Selecting *Enable M-BUS extension* and entering the *Baudrate*, *Parity* and *Stop Bits* lets you monitor the meter status connected via MBUS interface. MBUS expansion port is not currently supported, but it is possible to use an external RS232/MBUS converter.

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 53: 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.

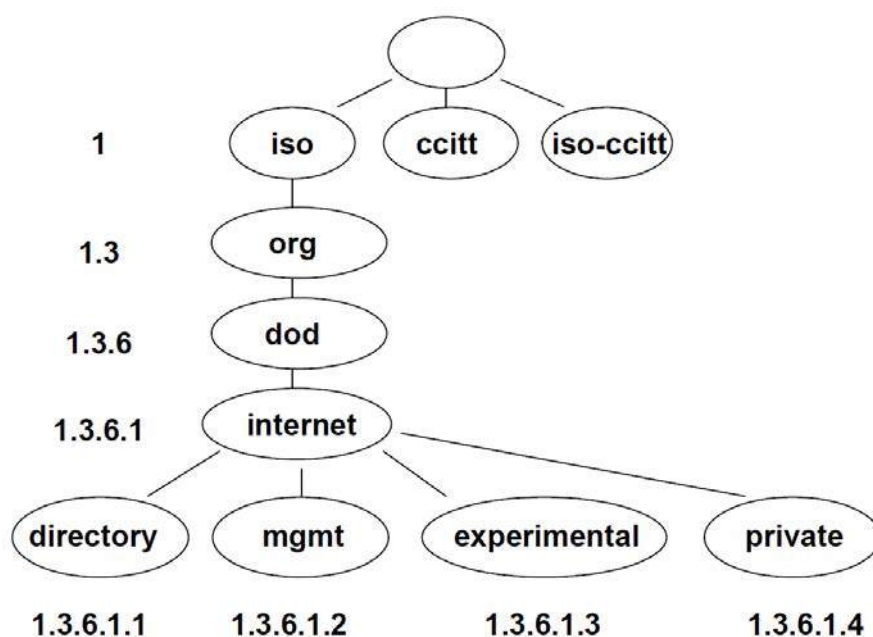


Figure 54: OID Basic Structure

The SNMP values that are specific for Conel routers create the tree starting at OID = .1.3.6.1.4.1.30140. You interpret the OID in the following manner:

iso.org.dod.internet.private.enterprises.conel

This means that the router provides for example, information about the internal temperature (OID 1.3.6.1.4.1.248.40.1.3.3) or about the power voltage (OID 1.3.6.1.4.1.248.40.1.3.4). For binary inputs and output, the following range of OID is used:

OID	Description
.1.3.6.1.4.1.30140.2.3.1.0	Binary input BIN0 (values 0,1)
.1.3.6.1.4.1.30140.2.3.2.0	Binary output OUT0 (values 0,1)
.1.3.6.1.4.1.30140.2.3.3.0	Binary input BIN1 (values 0,1)

Table 54: Object identifier for binary inputs and output



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

SNMP Configuration

☒ Enable SNMP agent

Name *

Company

Location *

City, Street ##

Contact *

Jack Roghul +420 732 123

(Configuration via SNMP is not possible.)

☒ Enable SNMPv1/v2 access

Community

Read

public

Write

private

☐ Enable SNMPv3 access

Username

Authentication

MD5

Authentication Password

Privacy

DES

Privacy Password

☐ Enable I/O extension

☐ Enable XC-CNT extension

☐ Enable M-BUS extension

Baudrate

300

Parity

even

Stop Bits

1

☐ Enable reporting to supervisory system

IP Address

Period

min

* can be blank

Apply

Figure 55: SNMP Configuration Example

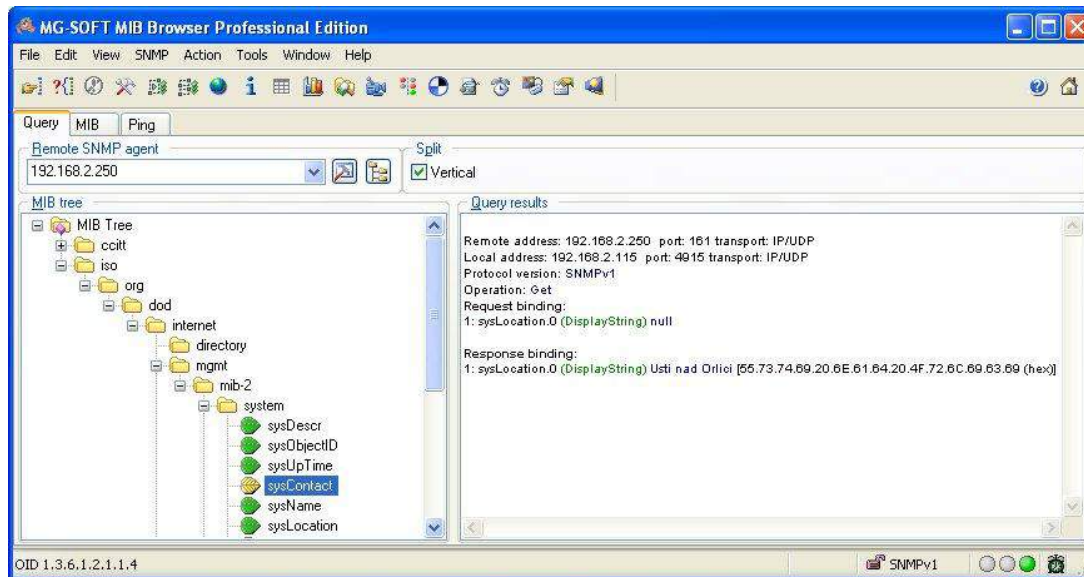


Figure 56: MIB Browser Example

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 → conel → protocols

The path to information about the router is:

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

4.16.7 SMTP

Use the *SMTP* form to configure the Simple Mail Transfer Protocol client (SMTP) for sending e-mails. IPv6 e-mail servers are supported.

Item	Description
SMTP Server Address	IPv4 address, IPv6 address or domain name 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, see chap. 1.5.1!
Own E-mail Address	Address of the sender.

Table 55: 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

smtp.domain.com

SMTP Port

465

Secure Method

SSL/TLS ▼

Username

username

Password

.....

Own Email Address

name@domain.com

Apply

Figure 57: SMTP Client Configuration Example

You can send e-mails from the Startup script. The *Startup Script* dialog is located in *Scripts* 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 john@doe.com -s "System Log" -m "Attached" -a /var/log/messages
```

The command above sends an e-mail to address *john@doe.com* with the subject "*System Log*", body message "*Attached*" and attachment *messages* file with *System Log* of the router directly from the directory */var/log/*.

4.16.8 SMS



The *SMS Configuration* page is not available for the SmartFlex SR300 routers (LAN version).

Open the *SMS* page in the *Services* submenu of 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.
Send SMS when binary input on I/O port (BIN0) is active	Automatic sending SMS message after binary input on I/O port (BIN0) is active. Text of message is intended parameter BIN0.
Add timestamp to SMS	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.
BIN0 – SMS	Text of the SMS message the binary input is activated.


Table 56: 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 57: Control via SMS

- 
- If you leave the phone number field blank, then you can still restart the router using an SMS Reboot message from any phone number.
 - 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
go online sim 2	The router changes to SIM2
go online	Changes the router to the online mode
go offline	Changes the router to the off line mode
set out0=0	Sets the binary output to 0

Continued on next page

Continued from previous page

SMS	Description
set out0=1	Sets the binary output to 1
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 58: 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. See example in *Commands and Scripts* Application Note [1].

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.

Choosing *Enable AT-SMS protocol on expansion port 1* and *Baudrate* makes it possible to use AT-SMS protocol on the serial Port 1.

Item	Description
Baudrate	Communication speed on the expansion port 1

Table 59: Send SMS on the serial Port 1

Choosing *Enable AT-SMS protocol on expansion port 2* and *Baudrate* makes it possible to use AT-SMS protocol on the serial Port 2.

Item	Description
Baudrate	Communication speed on the expansion port 2

Table 60: Send SMS on the serial Port 2

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.

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

Table 61: Sending/receiving of SMS on TCP port specified

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

Continued on next page

Continued from previous page

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

Table 62: List of AT Commands



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

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. See application note *AT Commands (AT-SMS)* [9].
- Using HTTP POST method for a remote execution, calling CGI scripts in the router. See *Commands and Scripts Application Note* [1] for more details and example.
- From Web interface of the router, in *Administration* section, *Send SMS* item, see Chapter 6.8.
- Using `gsmsms` command e.g. in terminal when connected to the router via SSH, see *Commands and Scripts Application Note* [1].

Examples of SMS Configuration

Example 1 Sending SMS 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	
<input checked="" type="checkbox"/>	Send SMS on power up
<input checked="" type="checkbox"/>	Send SMS on connect to mobile network
<input checked="" type="checkbox"/>	Send SMS on disconnect from mobile network
<input checked="" type="checkbox"/>	Send SMS when datalimit is exceeded
<input checked="" type="checkbox"/>	Send SMS when binary input on I/O port (BIN0) is active
<input checked="" type="checkbox"/>	Send SMS when binary input on expansion port 1 (BIN1-BIN4) is active
<input checked="" type="checkbox"/>	Add timestamp to SMS
Phone Number 1	<input type="text" value="723123456"/>
Phone Number 2	<input type="text" value="756858635"/>
Phone Number 3	<input type="text" value="603854758"/>
Unit ID *	<input type="text" value="Router"/>
BIN0 - SMS *	<input type="text" value="BIN0"/>
<input checked="" type="checkbox"/>	Enable remote control via SMS
Phone Number 1	<input type="text"/>
Phone Number 2	<input type="text"/>
Phone Number 3	<input type="text"/>
<input type="checkbox"/>	Enable AT-SMS protocol on expansion port 1
Baudrate	<input type="text" value="9600"/>
<input type="checkbox"/>	Enable AT-SMS protocol on expansion port 2
Baudrate	<input type="text" value="9600"/>
<input type="checkbox"/>	Enable AT-SMS protocol over TCP
TCP Port	<input type="text"/>
* can be blank	
<input type="button" value="Apply"/>	

Figure 58: SMS Configuration for Example 1

Example 2 Sending SMS via Serial Interface on the Port 1

SMS Configuration	
<input type="checkbox"/>	Send SMS on power up
<input type="checkbox"/>	Send SMS on connect to mobile network
<input type="checkbox"/>	Send SMS on disconnect from mobile network
<input type="checkbox"/>	Send SMS when datalimit is exceeded
<input type="checkbox"/>	Send SMS when binary input on I/O port (BIN0) is active
<input type="checkbox"/>	Send SMS when binary input on expansion port 1 (BIN1-BIN4) is active
<input type="checkbox"/>	Add timestamp to SMS
Phone Number 1	<input type="text"/>
Phone Number 2	<input type="text"/>
Phone Number 3	<input type="text"/>
Unit ID *	<input type="text"/>
BIN0 - SMS *	<input type="text"/>
<input type="checkbox"/>	Enable remote control via SMS
Phone Number 1	<input type="text"/>
Phone Number 2	<input type="text"/>
Phone Number 3	<input type="text"/>
<input checked="" type="checkbox"/>	Enable AT-SMS protocol on expansion port 1
Baudrate	<input type="text" value="9600"/>
<input type="checkbox"/>	Enable AT-SMS protocol on expansion port 2
Baudrate	<input type="text" value="9600"/>
<input type="checkbox"/>	Enable AT-SMS protocol over TCP
TCP Port	<input type="text"/>
* can be blank	
<input type="button" value="Apply"/>	

Figure 59: SMS Configuration for Example 2

Example 3 Control the Router Sending SMS from any Phone Number

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

Figure 60: SMS Configuration for Example 3

Example 4 Control the Router Sending SMS from Two Phone Numbers

SMS Configuration	
<input type="checkbox"/>	Send SMS on power up
<input type="checkbox"/>	Send SMS on connect to mobile network
<input type="checkbox"/>	Send SMS on disconnect from mobile network
<input type="checkbox"/>	Send SMS when datalimit is exceeded
<input type="checkbox"/>	Send SMS when binary input on I/O port (BIN0) is active
<input type="checkbox"/>	Send SMS when binary input on expansion port 1 (BIN1-BIN4) is active
<input type="checkbox"/>	Add timestamp to SMS
<input type="checkbox"/>	Enable remote control via SMS
Phone Number 1	<input type="text"/>
Phone Number 2	<input type="text"/>
Phone Number 3	<input type="text"/>
Unit ID *	<input type="text"/>
BIN0 - SMS *	<input type="text"/>
<input checked="" type="checkbox"/>	Enable remote control via SMS
Phone Number 1	<input type="text" value="728123456"/>
Phone Number 2	<input type="text" value="766254864"/>
Phone Number 3	<input type="text"/>
<input type="checkbox"/>	Enable AT-SMS protocol on expansion port 1
Baudrate	<input type="text" value="9600"/>
<input type="checkbox"/>	Enable AT-SMS protocol on expansion port 2
Baudrate	<input type="text" value="9600"/>
<input type="checkbox"/>	Enable AT-SMS protocol over TCP
TCP Port	<input type="text"/>
* can be blank	
<input type="button" value="Apply"/>	

Figure 61: SMS Configuration for Example 4

4.16.9 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 63: Parameters for SSH service configuration

SSH Configuration	
<input checked="" type="checkbox"/>	Enable SSH service
Session Timeout	<input type="text" value="600"/> sec
<input type="button" value="Apply"/>	

Figure 62: Configuration of HTTP service

4.16.10 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 64: 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 63: Syslog configuration

4.16.11 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 64: Enabling of Telnet service

4.17 Expansion Port Configuration

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

- If the router has the **RS232** interface, you configure it with the *Expansion Port 1* selection. (*Expansion Port 2* is not used).
- If the router has the **RS485/422-232** interface, you will configure the RS232 interface with the *Expansion Port 1* selection, and the RS485/422 interface with the *Expansion Port 2* selection.
- If the router has the **RS232-485-ETH** interface, you will configure the RS232 interface with the *Expansion Port 1* selection, the RS485/422 interface with the *Expansion Port 2* selection and the ETH interface with the *LAN* selection (the *Tertiary LAN* subpage).
- If you have the **SWITCH** version of the router (3x Ethernet, ETH2 interface), the port can be configured in the *LAN* item on the *Tertiary LAN* subpage – see Chapter 4.1.

In the upper part of the configuration window, the port can be enabled and the type of the connected port is shown in the *Port Type* item. Other items are described in the table below. IPv6 TCP/UDP client/server are supported.

Item	Description
Baudrate	Applied communication speed.
Data Bits	Number of data bits.
Parity	Control parity bit: <ul style="list-style-type: none"> • none – data will be sent without parity. • even – data will be sent with even parity. • odd – data will be sent with odd parity.
Stop Bits	Number of stop bits.
Flow Control	Set the flow control to none or hardware .
Split Timeout	Time to rupture reports. If the gap between two characters exceeds the parameter in milliseconds, any buffered characters will be sent over the Ethernet port.
Protocol	Protocol: <ul style="list-style-type: none"> • TCP – communication using a linked protocol TCP. • UDP – communication using a unlinked protocol UDP.

Continued on next page

Continued from previous page

Item	Description
Mode	Mode of connection: <ul style="list-style-type: none"> • TCP server – The router will listen for incoming TCP connection requests. • TCP client – The router will connect to a TCP server on the specified IP address and TCP port.
Server Address	When set to <i>TCP client</i> above, it is necessary to enter the <i>Server address</i> and <i>TCP port</i> . IPv4 and IPv6 addresses are allowed.
TCP Port	TCP/UDP port used for communications. The router uses the value for both the server and client modes.
Inactivity Timeout	Time period after which the TCP/UDP connection is interrupted in case of inactivity.

Table 65: Expansion Port Configuration – serial interface

If you mark the *Reject new connections* check box, then the router rejects any other connection attempt. This means that the router no longer supports multiple connections.

If you mark the *Check TCP connection* check box, the router verifies the TCP connection.

Item	Description
Keepalive Time	Time after which the router verifies the connection.
Keepalive Interval	Length of time that the router waits on an answer.
Keepalive Probes	Number of tests that the router performs.

Table 66: Expansion Port Configuration – *Check TCP connection*

When you mark the *Use CD as indicator of the TCP connection* check box, the router uses the carrier detection (CD) signal to verify the status of the TCP connection. The CD signal verifies that another device is connected to the other side of the cable.

CD	Description
Active	TCP connection is enabled
Nonactive	TCP connection is disabled

Table 67: CD Signal Description

When you mark the *Use DTR as control of TCP connection* check box, the router uses the data terminal ready (DTR) single to control the TCP connection. The remote device sends a DTR single to the router indicating that the remote device is ready for communications.

DTR	Description server	Description client
Active	The router allows the establishment of TCP connections.	The router initiates a TCP connection.
Nonactive	The router denies the establishment of TCP connections.	The router terminates the TCP connection.

Table 68: DTR Signal Description

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

Expansion Port 1 Configuration

☒ Enable expansion port 1 access over TCP/UDP

Port Type

RS-232

Baudrate

9600

Data Bits

8

Parity

none

Stop Bits

1

Flow Control

none

Split Timeout

20

msec

Protocol

TCP

Mode

server

Server Address

TCP Port

Inactivity Timeout *

sec

☐ Reject new connections

☐ Check TCP connection

Keepalive Time

3600

sec

Keepalive Interval

10

sec

Keepalive Probes

5

☐ Use CD as indicator of TCP connection

☐ Use DTR as control of TCP connection

* can be blank

Apply

Figure 65: Expansion Port Configuration

4.17.1 Examples of the Expansion Port Configuration

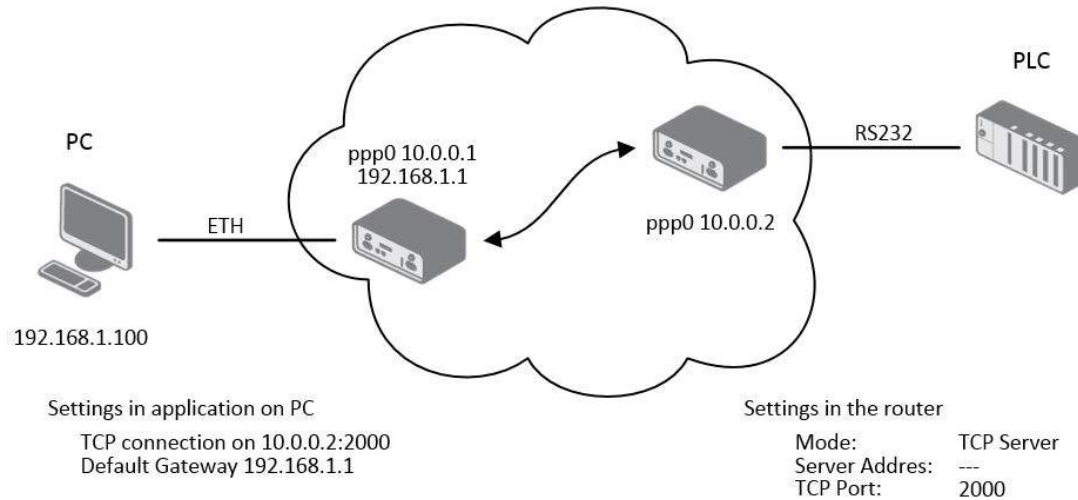


Figure 66: Example of Ethernet to serial communication configuration

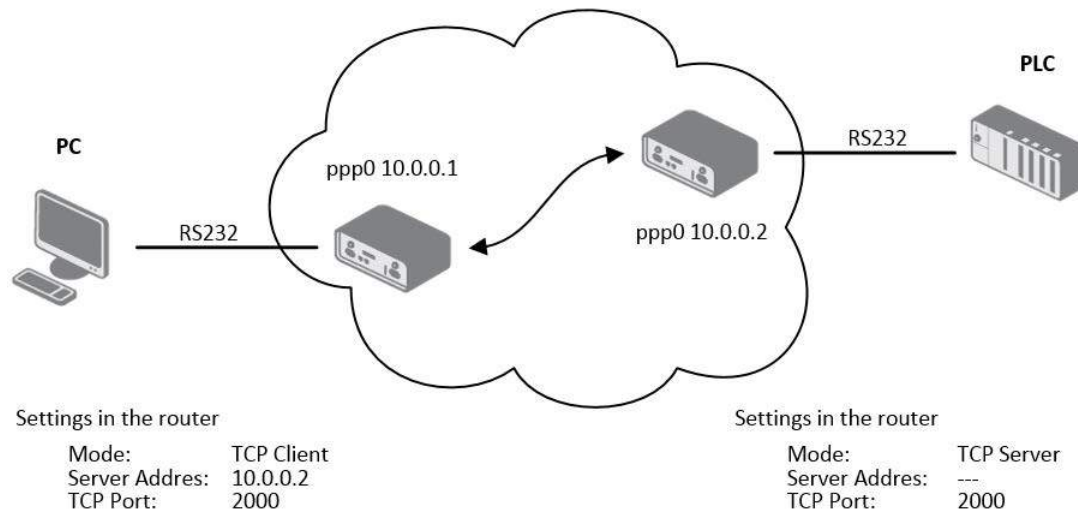


Figure 67: Example of serial interface configuration

4.18 USB Port Configuration

You can use a USB to RS232 converter to send data out of the serial port from the Ethernet network in the same manner as the RS232 expansion port function. To specify the values for the USB port parameters, click *USB Port* in the *Configuration* section of the main menu. The following tables describe the parameters available in the configuration form. IPv6 TCP/UDP client/server are supported.

Item	Description
Baudrate	Applied communication speed.
Data Bits	Number of data bits.
Parity	Control parity bit: <ul style="list-style-type: none"> • none – data will be sent without parity. • even – data will be sent with even parity. • odd – data will be sent with odd parity.
Stop Bits	Number of stop bit.
Flow Control	Set the flow control to none or hardware .
Split Timeout	Time to rupture reports. If the gap between two characters exceeds the parameter in milliseconds, any buffered characters will be sent over the Ethernet port.
Protocol	Communication protocol: <ul style="list-style-type: none"> • TCP – communication using a linked protocol TCP. • UDP – communication using a unlinked protocol UDP.
Mode	Mode of connection: <ul style="list-style-type: none"> • TCP server – The router will listen for incoming TCP connection requests. • TCP client – The router will connect to a TCP server on the specified IP address and TCP port.
Server Address	When set to <i>TCP client</i> above, it is necessary to enter the <i>Server address</i> and <i>TCP port</i> . IPv4 and IPv6 addresses are allowed.
TCP Port	TCP/UDP port used for communications. The router uses the value for both the server and client modes.
Inactivity Timeout	Time period after which the TCP/UDP connection is interrupted in case of inactivity.

Table 69: USB Port Configuration 1

If you mark the *Reject new connections* check box, then the router rejects any other connection attempt. This means that the router no longer supports multiple connections.

If you mark the *Check TCP connection* check box, the router verifies the TCP connection.

Item	Description
Keepalive Time	Time after which the router verifies the connection.
Keepalive Interval	Length of time that the router waits on an answer.
Keepalive Probes	Number of tests that the router performs.

Table 70: USB Port Configuration 2

When you mark the *Use CD as indicator of the TCP connection* check box, the router uses the carrier detection (CD) signal to verify the status of the TCP connection. The CD signal verifies that another device is connected to the other side of the cable.

CD	Description
Active	TCP connection is enabled
Nonactive	TCP connection is disabled

Table 71: CD Signal description

When you mark the *Use DTR as control of TCP connection* check box, the router uses the data terminal ready (DTR) signal to control the TCP connection. The remote device sends a DTR signal to the router indicating that the remote device is ready for communications.

DTR	Description server	Description client
Active	The router allows the establishment of TCP connections.	The router initiates a TCP connection.
Nonactive	The router denies the establishment of TCP connections.	The router terminates the TCP connection.

Table 72: DTR Signal Description



The router supports the following USB/RS232 converters:

- FTDI
- Prolific PL2303
- Silicon Laboratories CP210x

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

USB Port Configuration

☒ Enable USB serial converter access over TCP/UDP

Baudrate

9600

Data Bits

8

Parity

none

Stop Bits

1

Flow Control

none

Split Timeout

20

msec

Protocol

TCP

Mode

server

Server Address

TCP Port

Inactivity Timeout *

sec

☐ Reject new connections

☐ Check TCP connection

Keepalive Time

3600

sec

Keepalive Interval

10

sec

Keepalive Probes

5

☐ Use CD as indicator of TCP connection

☐ Use DTR as control of TCP connection

Apply

Figure 68: USB configuration

4.18.1 Examples of USB Port Configuration

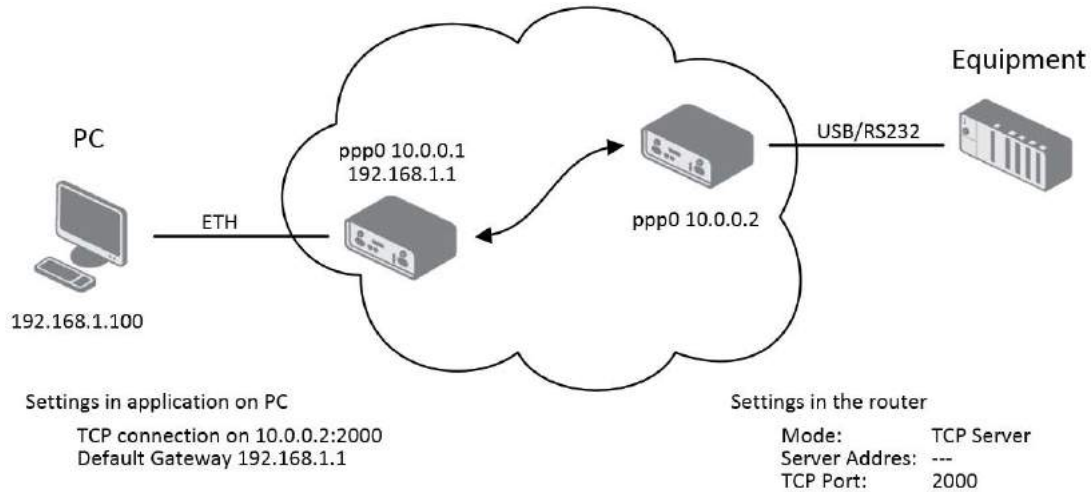


Figure 69: Example 1 – USB port configuration

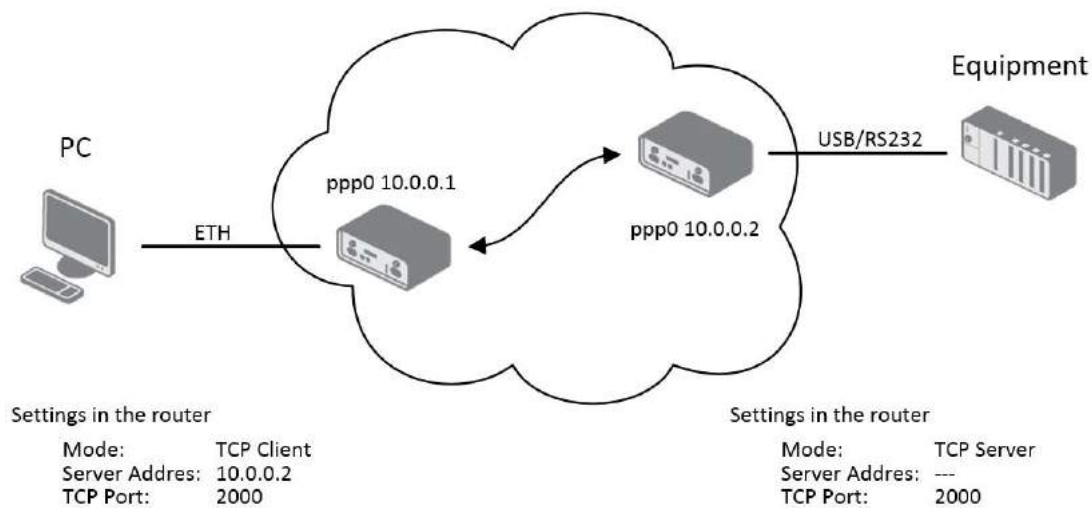


Figure 70: Example 2 – USB port configuration

4.19 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*, *Up/Down IPv4* and *Up/Down IPv6* scripts you can use – there is IPv4 and IPv6 independent dual stack. For more examples of Scripts and possible commands see the Application Note *Commands and Scripts* [1].

4.19.1 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.

4.19.2 Example of Startup Script

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

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

Apply

Figure 71: Example of a 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. Add these lines to the *Startup Script*:



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

4.19.3 Up/Down Scripts

Use the *Up/Down IPv4* and *Up/Down IPv6* page to create scripts executed when the Mobile WAN connection is established (up) or lost (down). There is independent IPv4 and IPv6 dual stack implemented in the router, so there is independent IPv4 and IPv6 Up/Down script. *IPv4 Up/Down Script* runs only on the IPv4 WAN connection established/lost, *IPv6 Up/Down Script* runs only on the IPv6 WAN connection established/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.

4.19.4 Example of IPv6 Up/Down Script

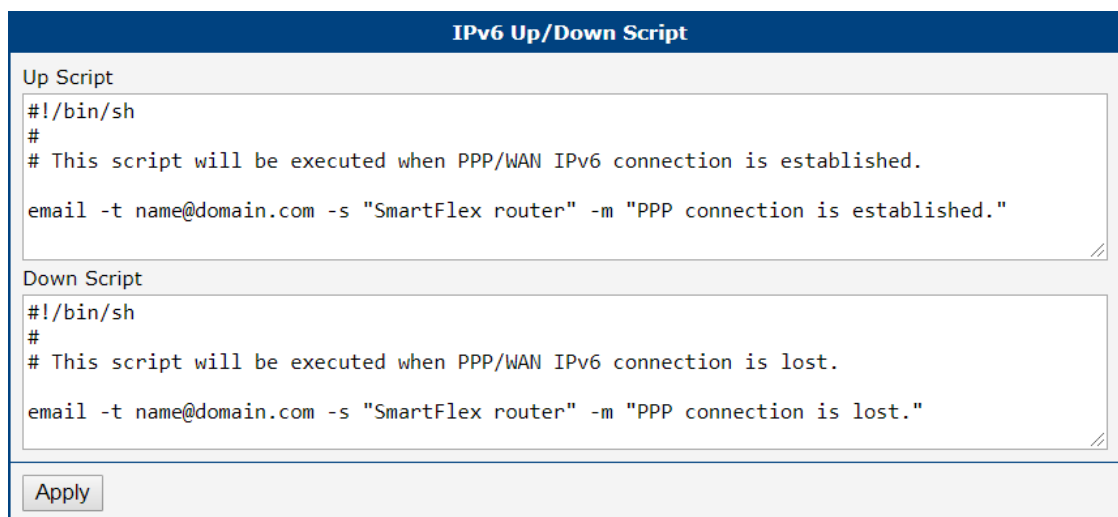


Figure 72: Example of IPv6 Up/Down Script

After establishing or losing an IPv6 WAN connection (connection to mobile network), the router sends an email with information about the connection state. It is necessary to configure *SMTP* before.

Add this line to the *Up Script* field:



```
email -t name@domain.com -s "Router" -m "Connection up."
```

Add this line to the *Down Script* field:



```
email -t name@domain.com -s "Router" -m "Connection down."
```

4.20 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. IPv6 sites/servers are supported. 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.

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.

Item	Description
Source	<p>Select the location of the update files:</p> <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, IPv4 or IPv6 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	<p>Choose an hour (range from 1 to 24) when the automatic update will be performed on a daily basis.</p> <p>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.</p>
Update Window Length	<p>This value defines the period within the update will be done.</p> <p>This period starts at the time set in the <i>Update Window Start</i> field.</p> <p>The exact time, when the update will be done, is generated randomly.</p>

Table 73: Automatic Update Configuration

4.20.1 Example of Automatic Update

The following example the router checks for new firmware or configuration file each day at 1:00 a.m. This example is given for the SmartFlex router.

- Firmware file: <https://example.com/SPECTRE-v3-LTE.bin>
- Configuration file: <https://example.com/test.cfg>

Automatic Update

☒ Enable automatic update of configuration

☒ Enable automatic update of firmware

Source HTTP(S) / FTP(S) ▼

Base URL

Unit ID *

Decryption Password *

Update Window Start 1:00 ▼

Update Window Length * min

* can be blank

Figure 73: Example of Automatic Update 1

4.20.2 Example of Automatic Update Based on MAC

The following example checks for new firmware or configurations each day between 1:00 a.m. and 3:00 a.m. The configuration file is encrypted, therefore the decryption password was configured. This example is given for the SmartFlex router with MAC address 00:11:22:33:44:55.

- Firmware file: <https://example.com/SPECTRE-v3-LTE.bin>
- Configuration file: <https://example.com/00.11.22.33.44.55.cfg>

Automatic Update

☒ Enable automatic update of configuration
☒ Enable automatic update of firmware

Source

HTTP(S) / FTP(S)

Base URL

<https://example.com>

Unit ID *

Decryption Password *

.....

Update Window Start

1:00

Update Window Length *

120

min

* can be blank

Apply

Figure 74: Example of Automatic Update 2

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.

User Modules			
No user modules installed.			
New Module	Choose File	No file chosen	Add or Update

Figure 75: 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 Application Note *Programming of User Modules* [10].

User Modules			
Sleep Mode	1.0.0 (2019-03-01)	Delete	
Web Terminal	1.0.1 (2018-03-02)	Delete	
New Module	Choose File	No file chosen	Add or Update

Figure 76: 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 74: 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 function is only available for users assigned the admin role!

To assign roles and manage user accounts open the *Users* form in the *Administration* section of the main menu. The first frame of this configuration form contains an overview of available users. The table below describes the meaning of the buttons in this frame.

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

Table 75: Users Overview



If you lock every account with the permission role *Admin*, you can not unlock these accounts. This also means that the *Users* dialog is unavailable for every user, because every *admin* account is locked and the *users* do not have sufficient permissions.

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

Item	Description
Role	Specifies the type of user account: <ul style="list-style-type: none"> • User – User with basic permissions. • Admin – User with full permissions.
Username	Specifies the name of the user allowed to log in the device.
Password	Specifies the password for the corresponding user. Characters are not restricted.
Confirm Password	Confirms the password you specified above.

Table 76: Add User



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

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

Figure 77: 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.

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

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

Figure 78: 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 of the router is **root** for the **root** user. 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	<input type="text" value="root"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>
<input type="button" value="Apply"/>	

Figure 79: 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. IPv4, IPv6 address or domain name is supported. After you enter the appropriate values, click the *Apply* button.

Set Real Time Clock	
Date	<input type="text" value="2019 - 08 - 20"/>
Time	<input type="text" value="14 : 45 : 44"/>
NTP Server Address	<input type="text"/>
<input type="button" value="Apply"/>	

Figure 80: Set Real Time Clock

6.5 Set SMS Service Center Address



The SmartFlex SR300 router does not support the *Set SMS Service Center Address* option.

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.

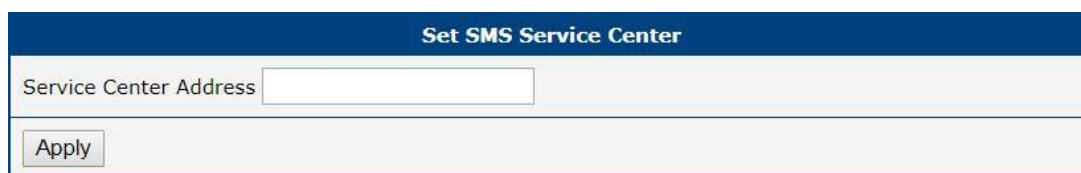


Figure 81: Set SMS Service Center Address

6.6 Unlock SIM Card



The SmartFlex SR300 router does not support the *Unlock SIM Card* option.

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.

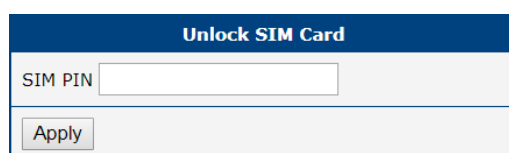


Figure 82: Unlock SIM Card

6.7 Unblock SIM Card



The SmartFlex SR300 router does not support the *Unblock SIM Card* option.

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.

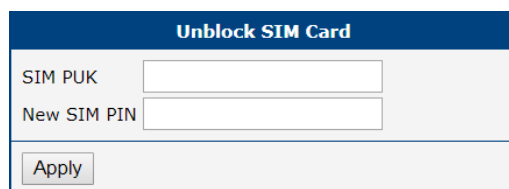


Figure 83: Unblock SIM Card

6.8 Send SMS



The SmartFlex SR300 router does not support the *Send SMS* option.

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).

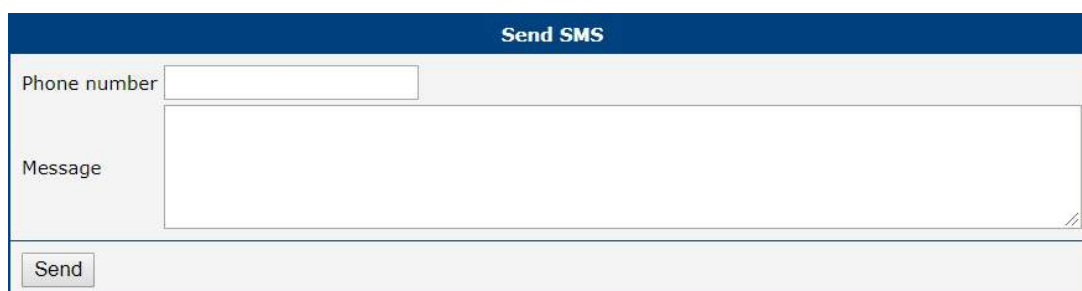


Figure 84: Send SMS

It is also possible to send an SMS message using CGI script. For details of this method, see the application note *Commands and Scripts* [1].

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 85. 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 85: 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 86: Restore Configuration

6.11 Update Firmware

Select the *Update Firmware* menu item to view the current router firmware version and load new firmware into the router. There is current firmware version and firmware filename written out. When loading the new firmware, it has to have this name. To load new firmware, browse to the new firmware file and press the *Update* button to begin the update.



Do not turn off the router during the firmware update. The firmware update can take up to five minutes to complete. Always use the filename written out as *Firmware Name* when updating the firmware.

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 87: Update Firmware



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

During the firmware update, the router will show the following messages. The progress of programming flash memory is shown in the form of increasing percentage number:

Firmware Update

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

Uploading firmware to RAM... ok
Checking firmware validity... ok
Backing up configuration... ok
Programming FLASH... 3 %

After the firmware update, the router will automatically reboot:

Firmware Update

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

Uploading firmware to RAM... ok
Checking firmware validity... ok
Backing up configuration... ok
Programming FLASH... ok
Updating u-boot environment... ok

Reboot in progress

Continue [here](#) after reboot.

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



It is highly recommended to always **update to latest firmware** for security reasons. Downgrading the firmware to a lower version than version uploaded during production may cause malfunction of the device.

6.12 Reboot

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

Reboot
The reboot process will take about 30 seconds to complete.
<input type="button" value="Reboot"/>

Figure 88: Reboot

6.13 Logout

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

7. Configuration in Typical Situations

Although Advantech B+B SmartWorx routers have wide variety of uses, they are commonly used in the following ways. All the examples below are for IPv4 networks.



These examples are not suitable for SmartFlex SR300 router (no cellular module).

7.1 Access to the Internet from LAN

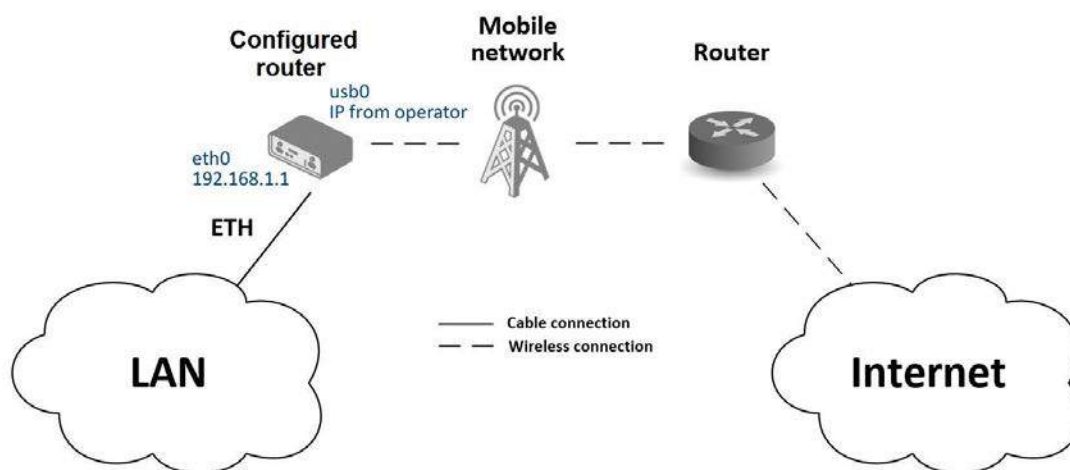


Figure 89: Access to the Internet from LAN – sample topology

In this example, a LAN connecting to the Internet via a mobile network, the SIM card with a data tariff has to be provided by the mobile network operator. This requires no initial configuration. You only need to place the SIM card in the *SIM1* slot (Primary SIM card), attach the antenna to the *ANT* connector and connect the computer (or switch and computers) to the router's eth0 interface (LAN). Wait a moment after turning on the router. The router will connect to the mobile network and the Internet. This will be indicated by the LEDs on the front panel (*WAN* and *DAT*).

Additional configuration can be done in the *LAN* and *Mobile WAN* items in the *Configuration* section of the web interface.

LAN configuration The factory default IP address of the router's eth0 interface is in the form of 192.168.1.1. This can be changed (after login to the router) in the *LAN* item in the *Configuration* section. (See Figure 90.) In this case there is no need of any additional configuration. The **DHCP server** is also enabled by factory default (so the first connected computer will get the 192.168.1.2 IP address etc.). Other configuration options are described in the Chapter 4.1.

Status	Primary LAN Configuration	
General	IPv4	IPv6
Mobile WAN	disabled	disabled
Network	IP Address	192.168.1.1
DHCP	Subnet Mask / Prefix	255.255.255.0
IPsec	Default Gateway	
DynDNS	DNS Server	
System Log		
Configuration		
LAN	Bridged	no
• Primary	Media Type	auto-negotiation
• Secondary		
VRRP	<input checked="" type="checkbox"/> Enable dynamic DHCP leases	
Mobile WAN	IPv4	IPv6
PPPoE	IP Pool Start	192.168.1.2
Backup Routes	IP Pool End	192.168.1.254
Static Routes	Lease Time	600
Firewall		600 sec
NAT		

Figure 90: Access to the Internet from LAN – LAN configuration

Mobile WAN Configuration Use the *Mobile WAN* item in the *Configuration* section to configure the connection to the mobile network. (Fig. 91.) In this case (depending on the SIM card) the configuration form can be blank. But make sure that *Create connection to mobile network* is checked (this is the factory default). For more details, see Chapter 4.3.1.

Status	1st Mobile WAN Configuration	
General	<input checked="" type="checkbox"/> Create connection to mobile network	
Mobile WAN	1st SIM card	2nd SIM card
Network	APN *	
DHCP	Username *	
IPsec	Password *	
DynDNS	Authentication	PAP or CHAP
System Log	IP Mode	IPv4
Configuration	IP Address *	
LAN	Dial Number *	
VRRP	Operator *	
Mobile WAN	Network Type	automatic selection
PPPoE	PIN *	
Backup Routes	MRU	1500 bytes
Static Routes	MTU	1500 bytes
Firewall	DNS Settings	get from operator
NAT		
OpenVPN		
IPsec		
GRE		
L2TP		

Figure 91: Access to the Internet from LAN – Mobile WAN configuration

To check whether the connection is working properly, go to the *Mobile WAN* item in the *Status* section. You will see information about operator, signal strength etc. At the bottom, you should see the message: *Connection successfully established*. The *Network* item should display information about the newly created network interface, usb0 (mobile connection). You should also see the IP address provided by the network operator, as well as the route table etc. The LAN now has Internet access.

7.2 Backup Access to the Internet from LAN

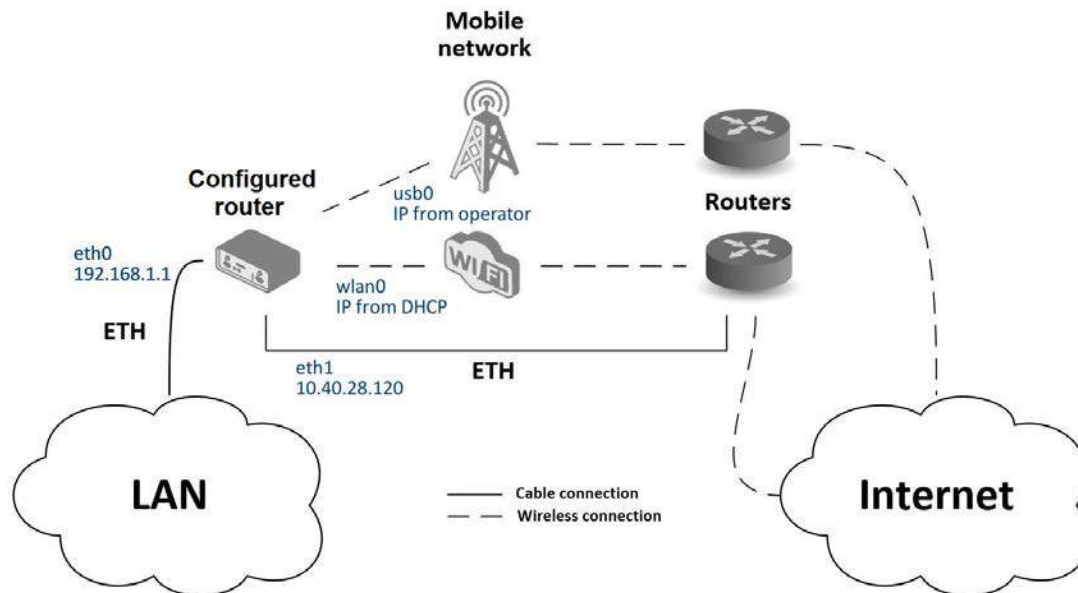


Figure 92: Backup access to the Internet – sample topology

The configuration form on the *Backup Routes* page lets you back up the primary connection with alternative connections to the Internet/mobile network. Each backup connection can be assigned a priority.

Status	Secondary LAN Configuration		
General			
Mobile WAN			
Network			
DHCP			
IPsec			
DynDNS			
System Log			
Configuration			
LAN			
• Primary			
• Secondary			
VRRP			
Mobile WAN			
PPPoE			
Backup Routes			
Static Routes			
Firewall			
NAT			
	DHCP Client	IPv4 disabled	IPv6 disabled
	IP Address	10.40.28.120	
	Subnet Mask / Prefix	255.255.252.0	
	Default Gateway	10.40.30.1	
	DNS Server	192.168.2.27	
	Bridged	no	
	Media Type	auto-negotiation	
	<input type="checkbox"/> Enable dynamic DHCP leases		
	IP Pool Start		
	IP Pool End		
	Lease Time	600	600 sec

Figure 93: Backup access to the Internet – LAN configuration

LAN configuration In the *LAN* item, *Primary LAN*, you can use the factory default configuration as in the previous situation. The *ETH1* interface on the front panel of the router is used for connection to the Internet. It can be configured in *Secondary LAN*. Connect the cable to the router and set the appropriate values as in Figure 93. You may configure the static IP address, default gateway and DNS server. Changes will take effect after you click on the *Apply* button. Detailed LAN configuration is described in Chapter 4.1.

WLAN configuration To use the WLAN you will need to configure the WiFi station in the *WiFi - > Station* item, as shown in Figure 94. Check the *Enable WiFi STA*, enable the DHCP client and fill in the addresses of the default gateway and DNS server. Next, fill in the data for the connection (SSID, authentication, encryption, WPA PSK Type and password). For details see Chapter 4.6. Click the *Apply* button to confirm the changes.

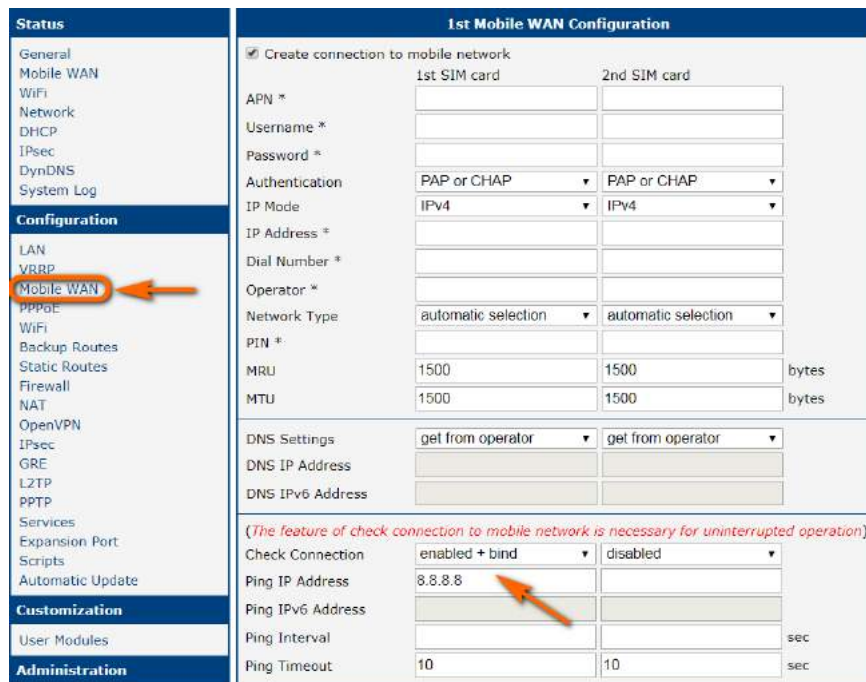
To verify that the WiFi connection is successful, check the *WiFi* item in the *Status* section. If the connection is successful you should see the following message: `wpa_state=COMPLETED`.

Status	WiFi STA Configuration	
General	<input checked="" type="checkbox"/> Enable WiFi STA	
Mobile WAN	IPv4	IPv6
WiFi	DHCP Client	enabled
Network	IP Address	
DHCP	Subnet Mask / Prefix	
IPsec	Default Gateway	192.168.3.1
DynDNS	DNS Server	192.168.3.1
System Log	SSID	WiFiNetwork
	Probe Hidden SSID	enabled
	Country Code *	
	Authentication	WPA2-PSK
	Encryption	AES
	WEP Key Type	ASCII
	WEP Default Key	1
	WEP Key 1	
	WEP Key 2	
	WEP Key 3	
	WEP Key 4	
	WPA PSK Type	ASCII passphrase
	WPA PSK	WiFiPassword

Figure 94: Backup access to the Internet – WiFi configuration

Mobile WAN configuration To configure the mobile connection it should be sufficient to insert the SIM card into the *SIM1* slot and attach the antenna to the *ANT* connector. (Depending on the SIM card you are using).

To set up backup routes you will need to enable Check Connection in the *Mobile WAN* item. (See Figure 95.) Set the *Check connection* option to *enabled + bind* and fill in an IP address of the mobile operator's DNS server or any other reliably available server and enter the time interval of the check. For detailed configuration, see Chapter 4.3.1.



1st Mobile WAN Configuration		
	1st SIM card	2nd SIM card
<input checked="" type="checkbox"/> Create connection to mobile network		
APN *		
Username *		
Password *		
Authentication	PAP or CHAP	PAP or CHAP
IP Mode	IPv4	IPv4
IP Address *		
Dial Number *		
Operator *		
Network Type	automatic selection	automatic selection
PIN *		
MRU	1500	1500
		bytes
MTU	1500	1500
		bytes
DNS Settings	get from operator	get from operator
DNS IP Address		
DNS IPv6 Address		
(The feature of check connection to mobile network is necessary for uninterrupted operation)		
Check Connection	enabled + bind	disabled
Ping IP Address	8.8.8.8	
Ping IPv6 Address		
Ping Interval		sec
Ping Timeout	10	10
		sec

Figure 95: Backup access to the Internet – Mobile WAN configuration

Backup Routes configuration After setting up the backup routes you will need to set their priorities. In Figure 96 the eth1 wired connection has the highest priority. If that connection fails, the second choice will be the WiFi wlan0 network interface. The third choice will be the mobile connection – usb0 network interface.

The backup routes system must be activated by checking the *Enable backup routes switching* item for each of the routes. Click the *Apply* button to confirm the changes. For detailed configuration see Chapter 4.7.

You can verify the configured network interfaces in the *Status* section in the *Network* item. You will see the active network interfaces: eth0 (connection to LAN), eth1 (wired connection to the Internet), wlan0 (WiFi connection to the Internet) and usb0 (mobile connection to the Internet). IP addresses and other data are included.

At the bottom of the page you will see the *Route Table* and corresponding changes if a wired connection fails or a cable is disconnected (the default route changes to wlan0). Similarly, if a WiFi connection is not available, the mobile connection will be used.

Status	Backup Routes Configuration
General	<input checked="" type="checkbox"/> Enable backup routes switching
Mobile WAN	Mode: Single WAN
WiFi	<input checked="" type="checkbox"/> Enable backup routes switching for Mobile WAN
Network	Priority: 3rd
DHCP	Weight:
IPsec	<input type="checkbox"/> Enable backup routes switching for PPPoE
DynDNS	Priority: 1st
System Log	Ping IP Address:
	Ping IPv6 Address:
	Ping Interval: sec
	Ping Timeout: 10 sec
	Weight:
	<input checked="" type="checkbox"/> Enable backup routes switching for WiFi STA
	Priority: 2nd
	Ping IP Address:
	Ping IPv6 Address:
	Ping Interval: sec
	Ping Timeout: 10 sec
	Weight:
	<input type="checkbox"/> Enable backup routes switching for Primary LAN
	Priority: 1st
	Ping IP Address:
	Ping IPv6 Address:
	Ping Interval: sec
	Ping Timeout: 10 sec
	Weight:
	<input checked="" type="checkbox"/> Enable backup routes switching for Secondary LAN
	Priority: 1st
	Ping IP Address:
	Ping IPv6 Address:
	Ping Interval: sec
	Ping Timeout: 10 sec
	Weight:
	Apply

Figure 96: Backup access to the Internet – Backup Routes configuration

Backup routes work even if they are not activated in the *Backup Routes* item, but the router will use the factory defaults.

7.3 Secure Networks Interconnection or Using VPN

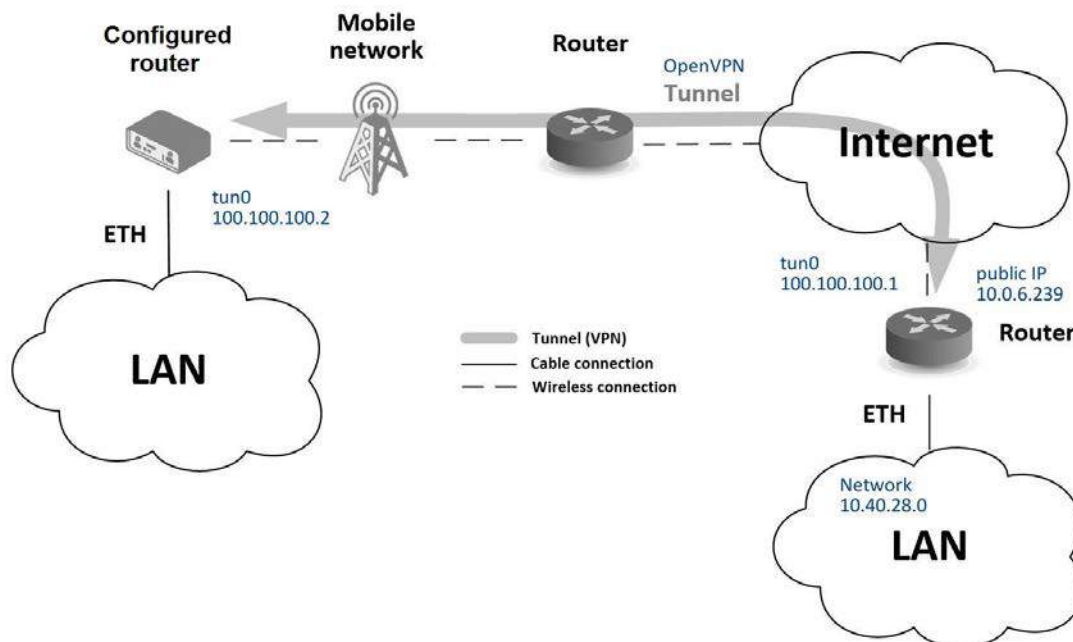


Figure 97: Secure networks interconnection – sample topology

VPN (Virtual Private Network) is a protocol used to create a secure connection between two LANs, allowing them to function as a single network. The connection is secured (encrypted) and authenticated (verified). It is used over public, untrusted networks. (See fig. 97.) You may use several different secure protocols.

- *OpenVPN* (it is a configuration item in the web interface of the router), see chapter 4.11 or Application Note [5],
- *IPsec* (it is also configuration item in the web interface of the router), see chapter 4.12 or Application Note [6].

You can also create non-encrypted tunnels: *GRE*, *PPTP* and *L2TP*. You can use GRE or L2TP tunnel in combination with IPsec to create VPNs.

There is an example of an OpenVPN tunnel in Fig. 97. To establish this tunnel you will need the opposite router's IP address, the opposite router's network IP address (not necessary) and the pre-shared secret (key). Create the OpenVPN tunnel by configuring the *Mobile WAN* and *OpenVPN* items in the *Configuration* section.

Mobile WAN configuration The mobile connection can be configured as described in the previous situations. (The router connects itself after a SIM card is inserted into *SIM1* slot and an antenna is attached to the *ANT* connector.)

Configuration is accessible via the *Mobile WAN* item the *Configuration* section. (See Chapter 4.3.1). The mobile connection has to be enabled.

OpenVPN configuration OpenVPN configuration is done with the *OpenVPN* item in the *Configuration* section. Choose one of the two possible tunnels and enable it by checking the *Create 1st OpenVPN tunnel*. You will need to fill in the protocol and the port (according to the settings on the opposite side of the tunnel or Open VPN server). You may fill in the public IP address of the opposite side of the tunnel including the remote subnet and mask (not necessary). The important items are *Local* and *Remote Interface IP Address* where the information regarding the interfaces of the tunnel's end must be filled in. In the example shown, the *pre-shared secret* is known, so you would choose this option in the *Authentication Mode* item and insert the secret (key) into the field. Confirm the configuration clicking the *Apply* button. For detailed configuration see Chapter 4.11 or Application Note [5].

Status	1st OpenVPN Tunnel Configuration	
General	<input checked="" type="checkbox"/> Create 1st OpenVPN tunnel	
Mobile WAN	Description *	myTunnel
WiFi	Protocol	UDP
Network	UDP Port	3000
DHCP	Remote IP Address *	10.0.6.239
IPsec	Remote Subnet *	10.40.28.0
DynDNS	Remote Subnet Mask *	255.255.252.0
System Log	Redirect Gateway	no
Configuration	Local Interface IP Address	100.100.100.2
LAN	Remote Interface IP Address	100.100.100.1
VRRP	Remote IPv6 Subnet *	
Mobile WAN	Remote IPv6 Subnet Prefix Length *	
PPPoE	Local Interface IPv6 Address *	
WiFi	Remote Interface IPv6 Address *	
Backup Routes	Ping Interval *	10 sec
Static Routes	Ping Timeout *	30 sec
Firewall	Renegotiate Interval *	sec
NAT	Max Fragment Size *	bytes
OpenVPN	Compression	LZO
• 1st Tunnel	NAT Rules	not applied
• 2nd Tunnel	Authenticate Mode	pre-shared secret
• 3rd Tunnel	Pre-shared Secret	# # 2048 OpenVPN static key #
• 4th Tunnel		
IPsec		
GRE		
L2TP		
PPTP		
Services		
Expansion Port		
Scripts		
Automatic Update		
Customization		
User Modules		

Figure 98: Secure networks interconnection – OpenVPN configuration

The *Network* item in the *Status* section will let you verify the activated network interface tun0 for the tunnel with the IP addresses of the tunnel's ends set. Successful connection can be verified in the *System Log* where you should see the message: Initialization Sequence

Completed. The networks are now interconnected. This can also be verified by using the `ping` program. (Ping between tunnel's endpoint IP addresses from one of the routers. The console is accessible via SSH).

7.4 Serial Gateway

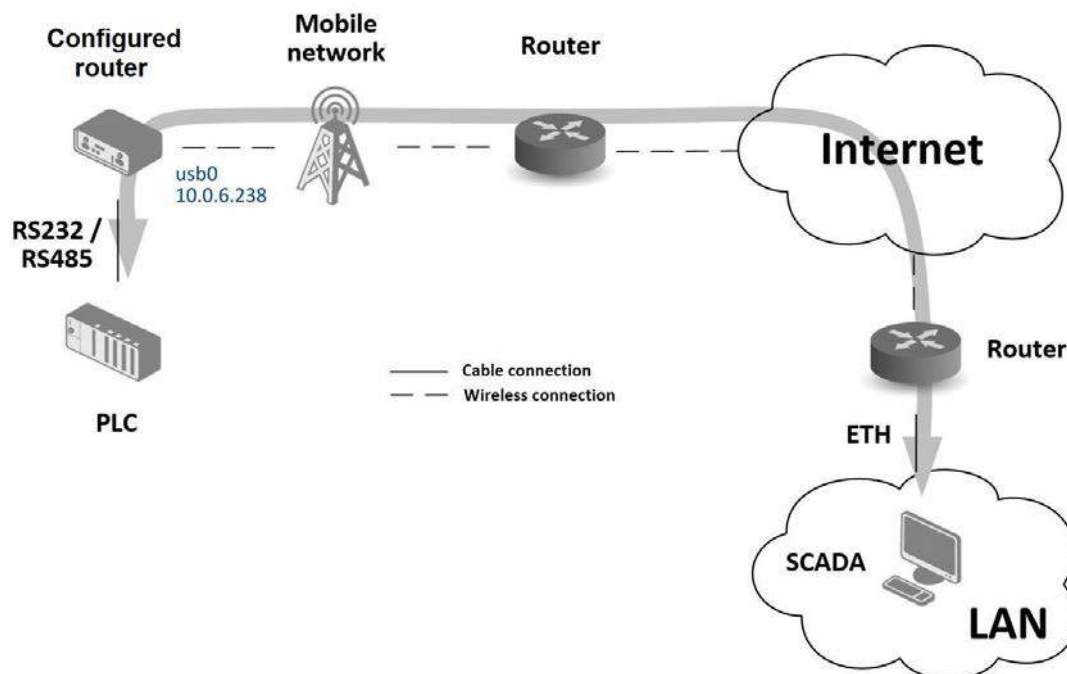


Figure 99: Serial Gateway – sample topology

The router's serial gateway function lets you establish serial connectivity across the Internet or with another network. Serial devices (meters, PLC, etc.) can then upload and download data. (See Fig. 99.) To use this function the router model must have a serial interface (port). Options include RS232, RS485-232 or RS232-485-ETH.

Configuration is done in the *Configuration* section, *Mobile WAN*, with the *Expansion Port 1* item (or *Expansion Port 2*, for RS422 and RS485). In this example, the router is equipped with an RS232 interface (port).

Mobile WAN configuration Mobile WAN configuration is the same as in the previous examples. Just insert the SIM card into the *SIM1* slot at the back of the router and attach the antenna to the *ANT* connector at the front. No extra configuration is needed (depending on the SIM card used). For more details see Chapter 4.3.1.

Expansion Port 1 configuration The RS232 interface (port) can be configured in the *Configuration* section, via the *Expansion Port 1* item. (See fig. 100.) You will need to enable the RS232 port by checking *Enable expansion port 1 access over TCP/UDP*. You may edit the serial communication parameters (not needed in this example). The important items are *Protocol*, *Mode* and *Port*. These set the parameters of communication out to the network and the Internet. In this example the TCP protocol is chosen, and the router will work as a server listening on the 2345 TCP port. Confirm the configuration clicking the *Apply* button.

Status	Expansion Port Configuration
General	<input checked="" type="checkbox"/> Enable expansion port access over TCP/UDP
Mobile WAN	Port Type: RS-232
Network	Baudrate: 9600
DHCP	Data Bits: 8
IPsec	Parity: none
DynDNS	Stop Bits: 1
System Log	Flow Control: none
	Split Timeout: 20 msec
	Protocol: TCP
	Mode: server
	Server Address:
	TCP Port: 2345
	Inactivity Timeout *: sec
	<input type="checkbox"/> Reject new connections
	<input type="checkbox"/> Check TCP connection
	Keepalive Time: 3600 sec
	Keepalive Interval: 10 sec
	Keepalive Probes: 5
	<input type="checkbox"/> Use CD as indicator of TCP connection
	<input type="checkbox"/> Use DTR as control of TCP connection
	* can be blank
	Apply

Figure 100: Serial Gateway – konfigurace *Expansion Port 1*

To communicate with the serial device (PLC), connect from the PC (Labeled as SCADA in Fig. 99) as a TCP client to the IP address 10.0.6.238, port 2345 (the public IP address of the SIM card used in the router, corresponding to the usb0 network interface). The devices can now communicate. To check the connection, go to *System Log* (*Status* section) and look for the *TCP connection established* message.

8. 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 Encryption, 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 be-

tween 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 Author-

ity (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 default 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 regard-

less 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.

9. Index

A

Access Point	
Configuration	52
Information	13
Accessing the router	4
Add User	138
APN	39
AT commands	113

B

Backup Configuration	143
Backup Routes	64
Bridge	27

C

Change Password	140
Change Profile	139
Clock synchronization	102
Configuration update	132
Control SMS messages	111

D

Data limit	43
Default Gateway	26, 59
Default IP address	4
Default password	5
Default SIM card	45
Default username	5
DHCP	19, 26, 59, 158
DHCPv6	27
Dynamic	28
Static	28
DHCPv6	19, 26, 59
DNS	158
DNS server	26, 41, 59

DNS64	17
Domain Name System	see DNS
DoS attacks	70
Dynamic Host Configuration Protocol	see DHCP
DynDNS	22, 99
DynDNSv6	22, 99

E

Expansion Port	
RS232	122
RS232-485-ETH	122
RS485/422-232	122
SWITCH	122

F

Firewall	68
Filtering of Forwarded Packets	69
Filtering of Incoming Packets	68
Protection against DoS attacks	70
Firmware update	132, 145
Firmware version	9
FTP	100

G

GRE	92, 158
-----------	---------

H

HTTP	101
------------	-----

I

ICMPv6	41
--------------	----

IPsec	84, 159
Authenticate Mode	87
Encapsulation Mode	85
IKE Mode	85
IPv4	159
IPv6 .. 7, 17, 25, 28, 39, 41, 68, 73, 79, 84, 99,	131

L

L2TP	95, 159
LAN	
IPv6	25
PoE PSE	27
Primary LAN	25
Secondary LAN	25
Tertiary LAN	25
Location Area Code	10
Logout	146

M

Mobile network	39
Multiple WANs	64, 65, 67

N

NAT	73, 159
NAT64	17
Neighbouring WiFi Networks	14
Network Address Translation	see NAT
NTP	102, 159
NTP server	140

O

Object Identifier	105
OpenVPN	79, 160
Authenticate Mode	81

P

PAM	103
-----------	-----

Password	140
PAT	73
PIN number	141
PLMN	10
PoE PSE	8, 27
Port	160
PPPoE	50
PPPoE Bridge Mode	49
PPTP	97, 160
Prefix delegation	28
PUK number	142

R

RADIUS	29, 52, 56
Reboot	146
Remote access	74
Restore Configuration	144
Router	1
Accessing	4
Advantages	2
Equipment	1
Optional Features	1

S

Save Log	23
Save Report	23
Security certificate	5
Send SMS	142
Serial line	
RS232	122
RS422	122
RS485	122
Serial number	9
Set internal clock	140
Signal Quality	10
Simple Network Management Protocol	see SNMP
SMS	110
SMS Service Center	141
SMTP	108, 160
SNMP	104, 161
SSH	119
Startup Script	130

Static Routes	67
Switch between SIM Cards	43
Syslog	120
System Log	23

T

TCP	161
Telnet	121
Transfer speed	1
Transmission Control Protocol	see TCP

U

UDP	161
Unblock SIM card	142
Uniform resource locator	see URL
Unlock SIM card	141
Up/Down script	131
URL	161
Usage Profiles	139
USB	

USB/RS232 converters	127
USB Port	126
User Datagram Protocol	see UDP
User Module	136
Users	138

V

Virtual private network	see VPN
VPN	161
VRRP	36, 161

W

Web interface	5
WiFi	
Authentication	54, 60
HW Mode	54
WiFi AP	52
WiFi STA	59
WiFi Station	
Configuration	59

10. Recommended Literature

- [1] Advantech B+B SmartWorx: **Commands and Scripts for v2 and v3 Routers**, Application Note
- [2] Advantech B+B SmartWorx: **SmartCluster**, Application Note
- [3] Advantech B+B SmartWorx: **R-SeeNet**, Application Note
- [4] Advantech B+B SmartWorx: **R-SeeNet Admin**, Application Note
- [5] Advantech B+B SmartWorx: **OpenVPN Tunnel**, Application Note
- [6] Advantech B+B SmartWorx: **IPsec Tunnel**, Application Note
- [7] Advantech B+B SmartWorx: **GRE Tunnel**, Application Note
- [8] Advantech B+B SmartWorx: **SNMP Object Identifier**, Application Note
- [9] Advantech B+B SmartWorx: **AT Commands**, Application Note
- [10] Advantech B+B SmartWorx: **Programming of User Modules**, Application Note