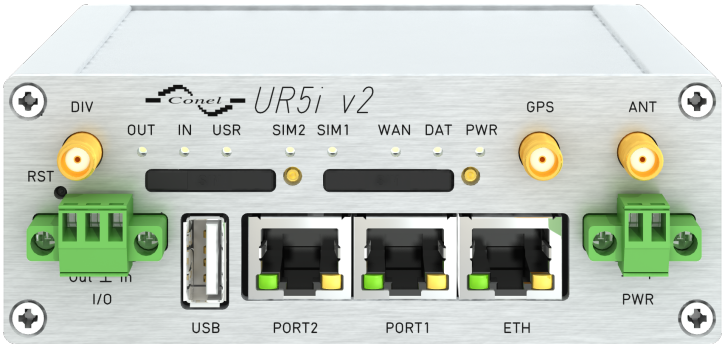
Cellular Industrial

v2 Routers

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 – Useful tips or information of special interest.

Example – Example of function, command or script.

Firmware Version

Current version of firmware is 6.3.12 (March 27, 2024).

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 the *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 get in touch with us at:

iiotcustomerservice@advantech.eu

Modifications and debugging of LGPL-linked executables:

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

Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
Document No. MAN-0021-EN, revision from March 27, 2024. Released in the Czech Republic.

Contents

1 Basic Information **1**

1.1 Document Content . . . 1
1.2 Web Configuration GUI . . . 1
1.3 WebAccess/DMP Configuration . . . 2
1.4 Router Configuration Options . . . 2
1.5 Supported Certificate File Types . . . 2
1.6 IEEE 802.1X Support . . . 3

2 Configuration Introduction **5**

2.1 Web Configuration . . . 5
2.1.1 Managing HTTPS Certificates . . . 8
2.1.2 Allowed and Restricted Input Characters . . . 8
2.1.3 Supported Certificate Formats . . . 8
2.2 Remote Management Platform . . . 9

3 Status **10**

3.1 General Status . . . 10
3.1.1 Mobile Connection . . . 10
3.1.2 Ethernet Status . . . 11
3.1.3 WiFi Status . . . 12
3.1.4 Peripheral Ports . . . 12
3.1.5 System Information . . . 12
3.2 Mobile WAN Status . . . 13
3.3 WiFi Status . . . 16
3.4 WiFi Scan . . . 17
3.5 Network Status . . . 19
3.6 DHCP Status . . . 21
3.7 IPsec Status . . . 22
3.8 DynDNS Status . . . 23
3.9 System Log . . . 24

4 Configuration **26**

4.1 Ethernet Configuration . . . 26
4.1.1 DHCP Server . . . 28
4.1.2 802.1X Authentication to RADIUS Server . . . 29
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 . . . 41
4.3.4 Data Limit Configuration . . . 42
4.3.5 Switch between SIM Cards Configuration . . . 42
4.3.6 PPPoE Bridge Mode Configuration . . . 45
4.4 PPPoE Configuration . . . 48
4.5 WiFi Access Point Configuration . . . 50
4.6 WiFi Station Configuration . . . 56
4.7 Backup Routes . . . 61
4.7.1 Default Priorities for Backup Routes . . . 61
4.7.2 User Customized Backup Routes . . . 62
4.7.3 Backup Routes Examples . . . 65
4.8 Static Routes . . . 71
4.9 Firewall Configuration . . . 72
4.10 NAT Configuration . . . 76
4.11 OpenVPN Tunnel Configuration . . . 81
4.12 IPsec Tunnel Configuration . . . 87
4.12.1 Route-based Configuration Scenarios . . . 87
4.12.2 IPsec Authentication Scenarios . . . 88
4.12.3 Configuration Items Description . . . 89
4.12.4 Basic IPSec Tunnel Configuration . . . 95
4.13 GRE Tunnels Configuration . . . 96
4.13.1 Example of the GRE Tunnel Configuration . . . 97
4.14 L2TP Tunnel Configuration . . . 99
4.14.1 Example of the L2TP Tunnel Configuration . . . 101
4.15 PPTP Tunnel Configuration . . . 102
4.15.1 Example of the PPTP Tunnel Configuration . . . 104
4.16 Services . . . 105
4.16.1 DynDNS . . . 105
4.16.2 FTP . . . 106
4.16.3 HTTP . . . 107
4.16.4 NTP . . . 108
4.16.5 PAM . . . 109
4.16.6 SNMP . . . 112
4.16.7 SMTP . . . 119
4.16.8 SMS . . . 121
4.16.9 SSH . . . 130
4.16.10 Syslog . . . 131
4.16.11 Telnet . . . 132
4.17 Expansion Port Configuration . . . 133
4.18 USB Port Configuration . . . 137
4.19 Scripts . . . 142
4.19.1 Startup Script . . . 142
4.19.2 Up/Down Script . . . 143
4.20 Automatic Update Configuration . . . 144

4.20.1 Example of Automatic Update . . . 146
4.20.2 Example of Automatic Update Based on MAC . . . 147

5 Administration 148

5.1 Users . . . 148
5.2 Change Profile . . . 150
5.3 Change Password . . . 151
5.4 Set Real Time Clock . . . 151
5.5 Set SMS Service Center Address . . . 153
5.6 Unlock SIM Card . . . 153
5.7 Unblock SIM Card . . . 154
5.8 Send SMS . . . 155
5.9 Backup Configuration . . . 156
5.10 Restore Configuration . . . 157
5.11 Update Firmware . . . 158
5.12 Reboot . . . 159
5.13 Logout . . . 159

6 Typical Situations 160

6.1 Access to the Internet from LAN . . . 160
6.2 Backup Access to the Internet from LAN . . . 162
6.3 Secure Networks Interconnection or Using VPN . . . 166
6.4 Serial Gateway . . . 168

7 Customization 170

7.1 Router Apps . . . 170

8 Glossary and Acronyms 171

Index 177

9 Related Documents 180

List of Figures

1 IEEE 802.1X Functional Diagram . . . 3
2 Web Configuration GUI . . . 7
3 Mobile WAN status . . . 15
4 WiFi Status . . . 16
5 WiFi Scan Output Example . . . 17
6 Network Status . . . 20
7 DHCP Status . . . 21
8 IPsec Status . . . 22
9 DynDNS Status . . . 23
10 System Log . . . 24
11 Example program syslogd start with the parameter -R . . . 25
12 Example 1 – Network Topology for Dynamic DHCP Server . . . 30
13 Example 1 – LAN Configuration Page . . . 31
14 Example 2 – Network Topology with both Static and Dynamic DHCP Servers . . . 32
15 Example 2 – LAN Configuration Page . . . 33
16 Example 3 – Network Topology . . . 34
17 Example 3 – LAN Configuration Page . . . 35
18 Topology of VRRP configuration example . . . 37
19 Example of VRRP configuration – main router . . . 37
20 Example of VRRP configuration – backup router . . . 38
21 Mobile WAN Configuration . . . 46
22 Example 1 – Mobile WAN Configuration . . . 47
23 Example 2 – Mobile WAN Configuration . . . 47
24 PPPoE configuration . . . 48
25 WiFi Access Point Configuration . . . 55
26 WiFi Station Configuration . . . 60
27 Backup Routes Configuration GUI . . . 64
28 Example #1: GUI Configuration . . . 65
29 Example #1: Topology . . . 65
30 Example #2: GUI Configuration . . . 66
31 Example #2: Topology . . . 66
32 Example #3: GUI Configuration . . . 67
33 Example #3: Topology for *Single WAN* mode . . . 68
34 Example #3: Topology for *Multiple WAN* mode . . . 68
35 Example #4: GUI Configuration . . . 69
36 Example #4: Topology . . . 69
37 Example #5: GUI Configuration . . . 70
38 Example #5: Topology . . . 70
39 Static Routes Configuration . . . 71
40 Firewall Configuration . . . 74

41 Topology for the Firewall Configuration Example . . . 75
42 Firewall Configuration Example . . . 75
43 Example 1 – Topology of NAT Configuration . . . 77
44 Example 1 – NAT Configuration . . . 78
45 Example 2 – Topology of NAT Configuration . . . 79
46 Example 2 – NAT Configuration . . . 80
47 OpenVPN tunnel configuration . . . 85
48 Topology of OpenVPN Configuration Example . . . 86
49 IPsec Tunnels Configuration . . . 89
50 Topology of IPsec Configuration Example . . . 95
51 GRE Tunnel Configuration . . . 97
52 Topology of GRE Tunnel Configuration Example . . . 97
53 L2TP Tunnel Configuration . . . 99
54 Topology of L2TP Tunnel Configuration Example . . . 101
55 PPTP Tunnel Configuration . . . 102
56 Topology of PPTP Tunnel Configuration Example . . . 104
57 DynDNS Configuration Example . . . 105
58 Configuration of FTP server . . . 106
59 Configuration of HTTP and HTTPS services . . . 107
60 Example of NTP Configuration . . . 108
61 Configuration of Local User Database . . . 109
62 Configuration of RADIUS . . . 110
63 Configuration of TACACS+ . . . 111
64 OID Basic Structure . . . 115
65 SNMP Configuration Example . . . 117
66 MIB Browser Example . . . 118
67 SMTP Client Configuration Example . . . 119
68 Example 1 – SMS Configuration . . . 126
69 Example 2 – SMS Configuration . . . 127
70 Example 3 – SMS Configuration . . . 128
71 Example 4 – SMS Configuration . . . 129
72 Configuration of HTTP service . . . 130
73 Syslog configuration . . . 131
74 Configuration of Telnet service . . . 132
75 Expansion Port Configuration . . . 135
76 Example of Ethernet to serial communication . . . 136
77 Example of serial port extension . . . 136
78 USB configuration . . . 140
79 Example 1 – USB port configuration . . . 140
80 Example 2 – USB port configuration . . . 141
81 Example of a Startup Script . . . 142
82 Example of Up/Down Script . . . 143
83 Example of Automatic Update 1 . . . 146
84 Example of Automatic Update 2 . . . 147

85 Users Administration Form . . . 148
86 Change Profile . . . 150
87 Change Password . . . 151
88 Set Real Time Clock . . . 152
89 Set SMS Service Center Address . . . 153
90 Unlock SIM Card . . . 153
91 Unblock SIM Card . . . 154
92 Send SMS . . . 155
93 Backup Configuration . . . 156
94 Restore Configuration . . . 157
95 Update Firmware Administration Page . . . 158
96 Process of Firmware Update . . . 159
97 Reboot . . . 159
98 Access to the Internet from LAN – sample topology . . . 160
99 Access to the Internet from LAN – *Ethernet* configuration . . . 161
100 Access to the Internet from LAN – *Mobile WAN* configuration . . . 161
101 Backup access to the Internet – sample topology . . . 162
102 Backup access to the Internet – Ethernet configuration . . . 162
103 Backup access to the Internet – WiFi configuration . . . 163
104 Backup access to the Internet – Mobile WAN configuration . . . 164
105 Backup access to the Internet – Backup Routes configuration . . . 165
106 Secure networks interconnection – sample topology . . . 166
107 Secure networks interconnection – OpenVPN configuration . . . 167
108 Serial Gateway – sample topology . . . 168
109 Serial Gateway – konfigurace *Expansion Port 1* . . . 169
110 Router Apps GUI . . . 170
111 Router Apps Added . . . 170

List of Tables

1 Supported Roles of the IEEE 802.1X Authentication . . . 4
2 Mobile Connection . . . 10
3 Peripheral Ports . . . 12
4 System Information . . . 12
5 Mobile Network Information . . . 14
6 Value ranges of signal strength for different technologies. . . . 14
7 Description of Periods . . . 14
8 Mobile Network Statistics . . . 14
9 Detailed Information about WiFi Networks . . . 18
10 Description of Interfaces in Network Status . . . 19
11 Description of Information in Network Status . . . 20
12 DHCP Status Description . . . 21
13 Configuration of the Network Interface . . . 27
14 Configuration of Dynamic DHCP Server . . . 28
15 Configuration of Static DHCP Server . . . 28
16 Configuration of 802.1X Authentication . . . 29
17 VRRP configuration . . . 36
18 Check connection . . . 37
19 Mobile WAN Connection Configuration . . . 40
20 Check Connection to Mobile Network Configuration . . . 41
21 Data Limit Configuration . . . 42
22 Switch between SIM cards configuration . . . 43
23 Parameters for SIM card switching . . . 44
24 PPPoE configuration . . . 49
25 WiFi Configuration . . . 54
26 WLAN Configuration . . . 59
27 Backup Routes Modes . . . 62
28 Backup Routes Configuration . . . 63
29 Static Routes Configuration . . . 71
30 Filtering of Incoming Packets . . . 72
31 Forwarding filtering . . . 73
32 NAT Configuration . . . 76
33 Configuration of send all incoming packets . . . 76
34 Remote Access Configuration . . . 77
35 OpenVPN Configuration . . . 84
36 OpenVPN Configuration Example . . . 86
37 IPsec Tunnel Configuration . . . 93
38 Simple IPSec Tunnel Configuration . . . 95
39 GRE Tunnel Configuration . . . 96
40 GRE Tunnel Configuration Example . . . 98

41 L2TP Tunnel Configuration . . . 100
42 L2TP Tunnel Configuration Example . . . 101
43 PPTP Tunnel Configuration . . . 103
44 PPTP Tunnel Configuration Example . . . 104
45 DynDNS Configuration . . . 105
46 Parameters for FTP service configuration . . . 106
47 Parameters for HTTP and HTTPS services configuration . . . 107
48 NTP Configuration . . . 108
49 Available Modes of PAM . . . 109
50 Configuration of RADIUS . . . 110
51 Configuration of TACACS+ . . . 111
52 SNMP Agent Configuration . . . 112
53 SNMPv3 Configuration . . . 113
54 SNMP configuration – MBUS extension . . . 114
55 SNMP Configuration – R-SeeNet . . . 114
56 Object identifier for binary input and output . . . 115
57 Object identifier for CNT port . . . 116
58 Object identifier for M-BUS port . . . 116
59 SMTP client configuration . . . 119
60 SMS Configuration . . . 122
61 Control via SMS . . . 122
62 Control SMS . . . 123
63 Send SMS on the serial Port 1 . . . 124
64 Send SMS on the serial Port 2 . . . 124
65 Send SMS on ethernet PORT1 configuration . . . 124
66 List of AT Commands . . . 125
67 Parameters for SSH service configuration . . . 130
68 Syslog configuration . . . 131
69 Parameters for Telnet service configuration . . . 132
70 Expansion Port Configuration 1 . . . 133
71 Expansion Port Configuration 2 . . . 134
72 CD Signal Description . . . 134
73 DTR Signal Description . . . 134
74 USB Port Configuration 1 . . . 138
75 USB Port Configuration 2 . . . 139
76 CD Signal description . . . 139
77 DTR Signal Description . . . 139
78 Automatic Update Configuration . . . 145
79 Button Description . . . 148
80 User Parameters . . . 149

1. Basic Information

1.1 Document Content

This configuration manual contains the following information:

- Configuration of the router item by item according to the web interface (Chapters 3 to 5).
- Configuration in typical situations examples (Chapter 6):
  - Access to the Internet from LAN (Local Area Network) via mobile network.
  - Backed up access to the Internet (from LAN).
  - Secure networks interconnection or using VPN (Virtual Private Network).
  - Serial Gateway (connection of serial devices to the Internet).

1.2 Web Configuration GUI

Configuring 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 IPsec, OpenVPN and L2TP. The router also supports DHCP, NAT, NAT-T, DynDNS client, NTP, VRRP, control by SMS, backup of the primary connection, multiple WANs, RADIUS authentication on Ethernet and WiFi, and many other functions.

Additional diagnostic features designed to ensure continuous communication include automatic inspection of Mobile WAN connections, an automatic restart feature in case a connection is lost, and a hardware watchdog that monitors the status of the router. Using a startup 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. The routers can automatically update their configurations and firmware from a central server, allowing for mass reconfiguration of multiple routers simultaneously.

If you are not 100% sure whether your configuration is correct or if it could have an impact on product longevity, please contact our technical support for consultation.

1.3 WebAccess/DMP Configuration

WebAccess/DMP is an advanced enterprise-grade platform solution for provisioning, monitoring, managing, and configuring Advantech's routers and IoT gateways. See the application note [2] for more information of visit the WebAccess/DMP webpage.

New routers have been pre-installed with the *WebAccess/DMP* client. For its activation, enable it in the router's web interface (*Customization* → *Router Apps* → *WebAccess/DMP Client*).

The activated client periodically uploads router identifiers, configuration, and cellular network statistics to the *WebAccess/DMP* server. If you have purchased a part number ending with "-SWH", the DMP client is activated by default.

With the *WebAccess/DMP* client activated, you may configure the router from *WebAccess/DMP* portal. Navigate your browser to `https://www.wadmp.com`.

If this is your first time, please self-sign-up with the site. If not, please log in with your username and password. Once logged in, further assistance can be found at `https://docs.wadmp.com`.

1.4 Router Configuration Options

Routers can be configured via a web browser or Secure Shell (SSH). Configuration via Web Browser is described in this Configuration Manual. Commands and scripts applicable in the configuration using SSH are described in *Commands and Scripts* 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 – WebAccess/VPN [2] and software for router monitoring R-SeeNet [3].

1.5 Supported Certificate File Types

All the GUI forms supporting the uploading of a certificate file support these file types:

- CA, Local/Remote Certificate: **.pem*; **.crt*; **.p12*
- Private Key: **.pem*; **.key*; **.p12*

1.6 IEEE 802.1X Support

IEEE 802.1X is an **IEEE Standard** for **port-based Network Access Control** (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an **authentication mechanism** to devices wishing to attach to a LAN or WLAN. IEEE 802.1X defines the encapsulation of the **Extensible Authentication Protocol** (EAP) over IEEE 802, which is known as "EAP over LAN" or **EAPoL**.

802.1X authentication involves three parties: **a supplicant**, **an authenticator**, and **an authentication server** (see Figure 1).

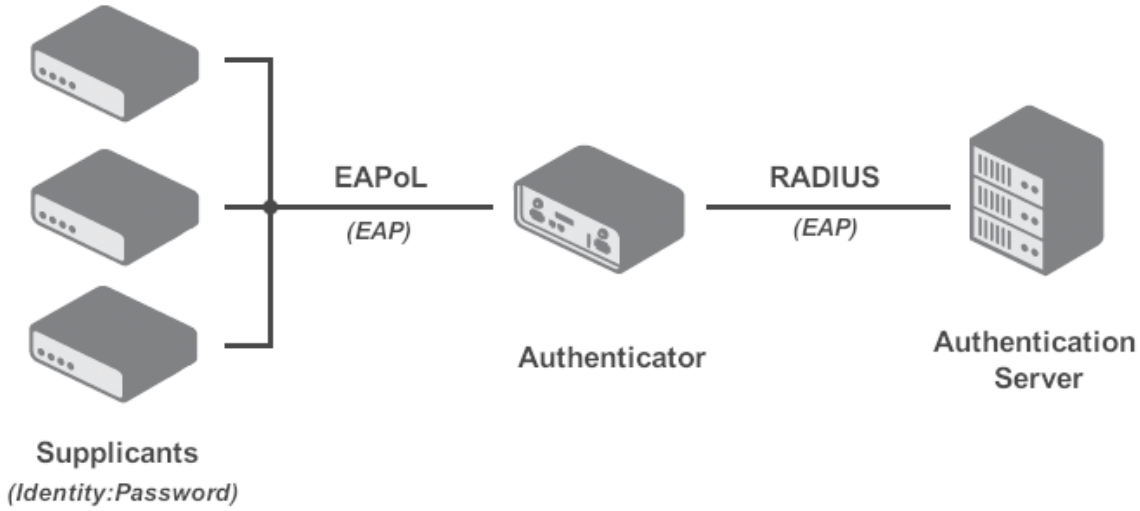


Figure 1: IEEE 802.1X Functional Diagram

- The **supplicant** is a client device (such as a laptop) that wishes to attach to the LAN/WLAN. The term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator.
- The **authenticator** is a network device which provides a data link between the client (supplicant) and the network (LAN/WAN) and can allow or block network traffic between the two, such as an Ethernet switch or wireless access point. The authtenticator communicates with the authentication server to determine if the network access for a supplicant will be granted or not.
- The **authentication server** is typically a trusted server that can receive and respond to requests for network access, and can tell the authenticator if the connection is to be allowed, and various settings that should apply to that client's connection or setting. Authentication servers typically run software supporting the **RADIUS** and **EAP protocols**.

Table 1 summarizes all the supported cases and roles when the IEEE 802.1X authentication can be used on Advantech routers.

Please note that the role of the authentication server is not supported by Advantech routers.

Interface	Supplicant Role	Authenticator Role
LAN	Built-in feature, just configure the LAN with 802.1X authentication, see Chapter 4.1.2.	Not built-in feature, but can be implemented by the UM *802.1X Authenticator*. For more information about this module see [RA].
WiFi	Supported for the Station (STA) mode, see Chapter 4.6.	Supported for the Access Point (AP) mode, see Chapter 4.5.

Table 1: Supported Roles of the IEEE 802.1X Authentication

2. Configuration Introduction

If unsure about the correctness of your configuration or its potential impact on the router's longevity, consult our technical support for guidance.

The router supports configuration via a **web browser** or **Secure Shell** (SSH). This manual primarily covers web browser configuration. For SSH configuration commands, refer to the *Commands and Scripts* Application Note.

Advantech's **remote device management** platform, *WebAccess/DMP*, provides extensive management and monitoring capabilities to ensure devices remain secure and up-to-date. For more information, refer to Chapter 2.2.

2.1 Web Configuration

Configuring routers is made efficient via a name and password-protected web interface. This interface offers a comprehensive configuration GUI, detailed statistics on router activities, signal strength, system logs, and more (see Figure 2).

To access the web interface on a new router with default settings and establish the router connection, refer to the *Hardware Manual*, specifically the *First Use* chapter.

For cellular routers, it's essential to correctly configure the carrier settings and activate the account. Ensure you insert the appropriate SIM card. For detailed guidance, refer to the *Hardware Manual*.

To access the web interface, type the router's default IP address *192.168.1.1* into your browser, beginning with *https://* to ensure secure access. The first time you access it, you'll need to install a security certificate to prevent domain disagreement warnings. For detailed instructions, see Chapter 2.1.1.

The default login username is **root**. The default password is indicated on the router's label.[1] Changing the default password as soon as possible is essential for security.

Changing the default router password is crucial for network security. The ***Change password*** title appears in red until updated.

Three unsuccessful login attempts block HTTP(S) access from the IP address for one minute.

[1] If the router's label does not specify a unique password, use "root" as the default password.

After a successful login, the web interface presents a menu, providing access to the *Status*, *Configuration*, *Customization*, and *Administration* sections.

Configure the router's *Name* and *Location* in the SNMP settings for display in the web interface's upper right corner (see 4.16.6).

Figure 2: Web Configuration GUI

2.1.1 Managing HTTPS Certificates

The router includes a self-signed HTTPS certificate. Due to the inability to validate this certificate's identity, web browsers may display a warning message. To address this, you can upload your own certificate, signed by a Certification Authority, to the router. If you wish to use your own certificate (for example, in combination with a dynamic DNS service), you should replace the */etc/certs/https_cert* and */etc/certs/https_key* files on the router. This replacement can be easily performed via the GUI on the *HTTP* configuration page, as detailed in Chapter 4.16.3.

To utilize the router's self-signed certificate without encountering the security message (due to domain disagreement) each time you log in, follow these steps:

- Add a DNS record to your DNS system: For Linux/Unix OS, edit /etc/hosts, or for Windows OS, navigate to C:\WINDOWS\system32\drivers\etc\hosts, or configure your own DNS server. Insert a new record pairing the router's IP address with a domain name derived from its MAC address (the MAC address of the first network interface, as seen in the *Network Status* on the router's web interface), using dashes instead of colons for separation. For instance, a router with the MAC address 00:11:22:33:44:55 would use the domain name 00-11-22-33-44-55.
- Access the router via this new domain name address (e.g., https://00-11-22-33-44-55). Should the security warning appear, proceed to add an exception so the message will not recur (e.g., in the Firefox Web browser). If the option to add an exception is unavailable, export the certificate to a file and import it to your browser or operating system.

Note: Utilizing a domain name based on the router's MAC address may not be compatible with all combinations of operating systems and browsers.

2.1.2 Allowed and Restricted Input Characters

When configuring the router via the web interface, it is crucial to avoid using forbidden characters in any input field, not solely the password fields. Below are the specified valid and forbidden characters. Note that for certain fields, the "space" character might also be disallowed.

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

Forbidden characters comprise: `‘‘ $ & ’ ( ) ; < > \ ^ ‘ |`

Please pay special attention to these guidelines during configuration, as entering invalid characters can lead to errors or unintended behavior.

2.1.3 Supported Certificate Formats

All GUI forms that allow the uploading of certificate files support the following file types:

- CA, Local/Remote Certificate: **.pem*; **.crt*; **.p12*
- Private Key: **.pem*; **.key*; **.p12*

2.2 Remote Management Platform

WebAccess/DMP is an advanced, enterprise-grade platform for provisioning, monitoring, managing, and configuring Advantech's routers and IoT gateways, offering zero-touch enablement for each remote device. For more information, refer to the application note [3] or visit the *WebAccess/DMP* webpage.

New routers come pre-installed with the *WebAccess/DMP* client, which by default activates the connection to the *WebAccess/DMP* server. This connection can be disabled on the *Welcome* page upon initial web interface login or under (*Customization* → *Router Apps* → *WebAccess/DMP Client*).

The activated client periodically uploads router identifiers and configurations to the *WebAccess/DMP* server.

3. Status

All status pages can display live data. To enable this feature, click on the *refresh* button in the top right corner on the status page. To stop the data update and to limit the amount of data transferred, disable automatic data updates by clicking the *pause* button again.

3.1 General Status

You can reach a summary of basic router information and its activities by opening the *General* status page. This page is displayed when you log in to the device by default. The information displayed on this page is divided into several sections, based upon the type of the router and its hardware configuration. Typically, there are sections for the mobile connection, LAN, system information, system information, and eventually for the WiFi and peripheral ports, if the device is equipped with.

3.1.1 Mobile Connection

Item	Description
SIM Card	Identification of the SIM card
Interface	Defines the interface
Flags	Displays network interface flags: None - no flags Up - the interface is administratively enabled Running - the interface is in operational state (cable detected) Multicast - the interface is capable of multicast transmission
IP Address	IP address of the interface
MTU	Maximum packet size that the equipment is able to transmit
Rx Data	Total number of received bytes
Rx Packets	Received packets
Rx Errors	Erroneous received packets
Rx Dropped	Dropped received packets
Rx Overruns	Lost received packets because of overload
Tx Data	Total number of sent bytes
Tx Packets	Sent packets
Tx Errors	Erroneous sent packets
Tx Dropped	Dropped sent packets
Tx Overruns	Lost sent packets because of overload
Uptime	Indicates how long the connection to the cellular network has been established

Table 2: Mobile Connection

3.1.2 Ethernet Status

Every Ethernet interface has its separate section on the *General* status page. Items displayed here 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. Visible information depends on the Ethernet configuration, see Chapter 4.1.

3.1.3 WiFi Status

Items displayed in this part have the same meaning as items in the previous part. *WiFi AP* part displays information for the WiFi interface (wlan0) working in access point mode, for the configuration see Chapter 4.5. *WiFi STA* part displays information for the WiFi interface (wlan1) working in station mode, for the configuration description see Chapter 4.6.

3.1.4 Peripheral Ports

Information about available peripheral ports is displayed in the *Peripheral Ports* section.

Item	Description
Expansion Port 1	Expansion port fitted to the position 1 (*None* indicates that this position is equipped with no port)
Expansion Port 2	Expansion port fitted to the position 2 (*None* 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

3.1.5 System Information

System information about the device is displayed in the *System Information* section.

Item	Description
Product Name	Name of the product (may not match with the P/N or order code).
Product Type	Type of the product (may be N/A or the same as the Product Name).
Firmware Version	Information about the firmware version.
Serial Number	Serial number of the router (in case of *N/A* is not available).
Hardware UUID[1]	Unique HW identifier for the device.
Product Revision[1]	Manufactured product revision number.
Profile	Current profile – standard or alternative profiles (profiles are used for example to switch between different modes of operation).
CPU Usage	CPU usage value (turn on the refresh in the top right corner).
Memory Usage	Memory usage value (turn on the refresh in the top right corner).
RTC Battery	RTC battery state.
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 license type. Click on the license type to see the license text.

Table 4: System Information

[1] It may not be available for some models.
[2] Only for models with PoE. The router's power supply voltage must meet the required voltage.

3.2 Mobile WAN Status

The XR5i v2 routers do 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 (in hexadecimal format).
LAC/TAC	Unique number (in hexadecimal format) assigned to each location area. LAC (Location Area Code) for 2G/3G networks and TAC (Tracking Area Code) for 4G networks.
Channel	Channel the router communicates on. • ARFCN in case of GPRS/EDGE technology, • UARFCN in case of UMTS/HSPA technology, • EARFCN in case of LTE technology.
Band	Cellular band abbreviation.
Signal Strength	Signal strength (in dBm) of the selected cell, for details see Table 6.
Signal Quality	Signal quality of the selected cell: • EC/IO for UMTS and CDMA (it's the ratio of the signal received from the pilot channel – EC – to the overall level of the spectral density, ie the sum of the signals of other cells – IO). • RSRQ for LTE technology (defined as the ratio $\frac{N \times RSRP}{RSSI}$). • The value is not available for the EDGE technology.
RSSI, RSRP, RSRQ, SINR, RSCP or Ec/Io	Other parameters reporting signal strength or quality. Please note, that some of them may not be available, depending on the cellular module or cellular technology.
CSQ	Cell signal strength with following value ranges: • 2–9 = Marginal, • 10–14 = OK, • 15–19 = Good, • 20–30 = Excelent.
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

[1] If 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
ESN	ESN (Electronic Serial Number) number of module (for CDMA routers)
MEID	MEID number of module
ICCID	Integrated Circuit Card Identifier is international and unique serial number of the SIM card.

Table 5: Mobile Network Information

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, called *Statistics*, 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

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

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.

Mobile WAN Status refresh

Mobile Network Information

Registration	: Home Network
Operator	: Vodafone
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 3: Mobile WAN status

3.3 WiFi Status

This feature is accessible only on routers equipped with a WiFi module.

Selecting the *Status* → *WiFi* → *Status* option in the web interface's main menu displays details about the WiFi access point (AP) and the WiFi station (STA), including a list of all stations connected to the AP.

An example output for WiFi status is illustrated in the figure below. It includes information on the WiFi chip, its firmware version, and the supported modes for the module. For instance, the notation "Supports 1 station and 2 access points" indicates that it is possible to use one station configuration alongside two distinct Access Point configurations simultaneously.

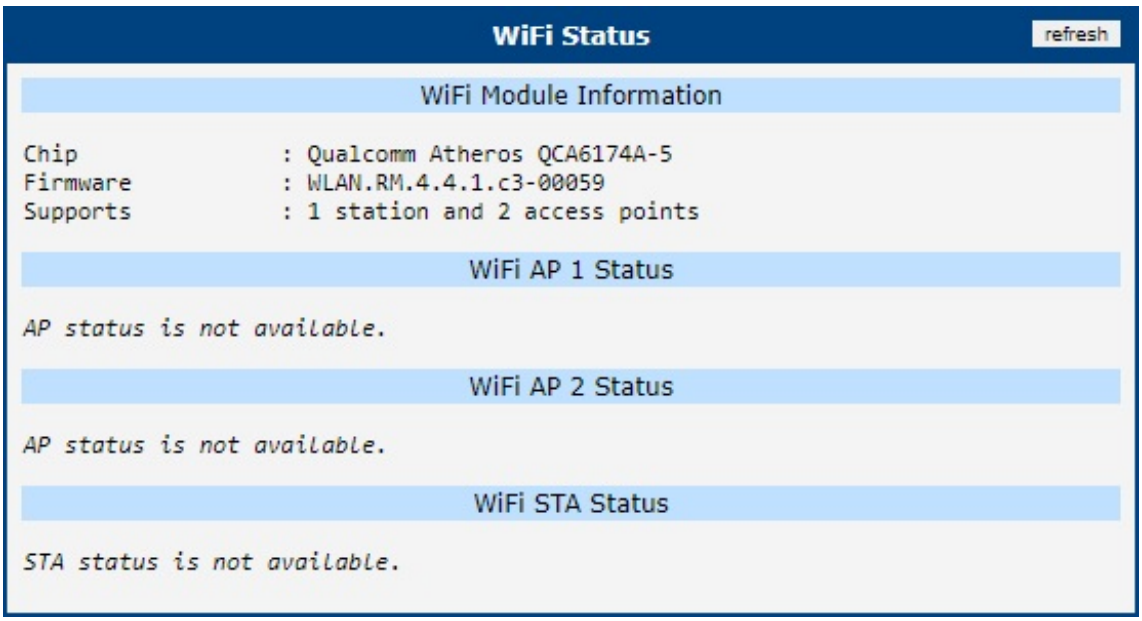


Figure 4: WiFi Status

3.4 WiFi Scan

This feature is accessible only on routers equipped with a WiFi module.

Selecting *Status* → *WiFi* → *Scan* initiates a scan for nearby WiFi networks, with the results displayed as shown in Figure 5.

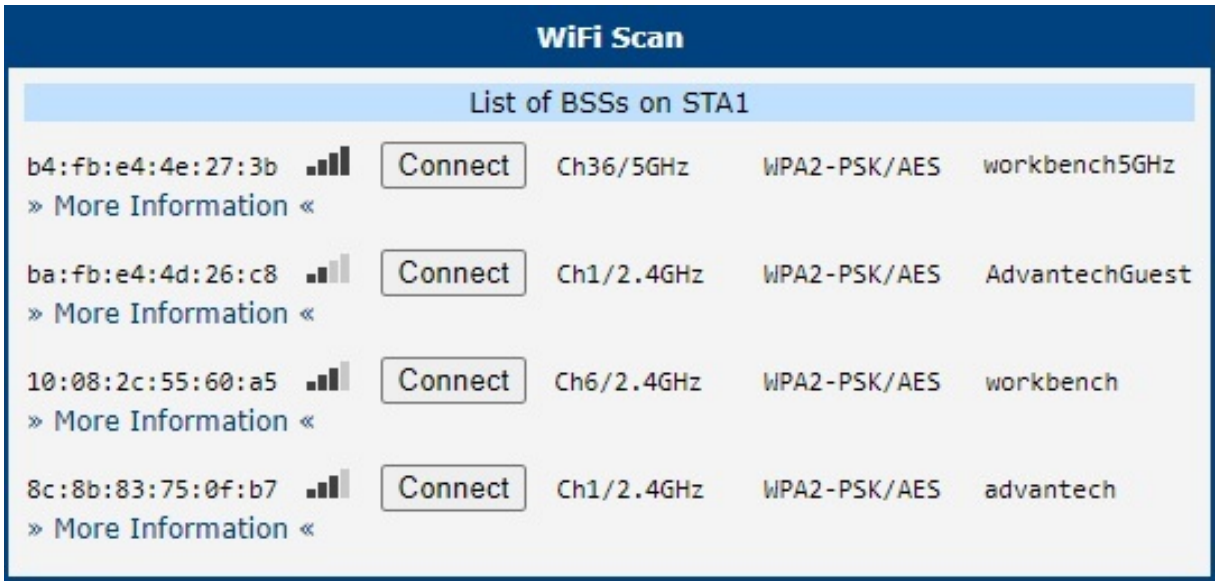


Figure 5: WiFi Scan Output Example

If you click on the *Connect* button next to the respective WiFi network, you will be redirected to the *Configuration* → *WiFi* → *Station* page, where the available fields will be pre-filled and you will be able to connect to the network by entering authentication details.

For each network, you can view details by clicking on the *More Information* button. Below is the description of some items from the WiFi scanning output.

Item	Description
BSS	MAC address of the access point (AP).
TSF	Synchronizes timers across all stations in a Basic Service Set (BSS).
freq	Frequency band of the WiFi network in MHz.
beacon interval	Time between synchronization beacons.
capability	Properties list of the access point (AP).
signal	Signal strength of the access point (AP).

Continued on next page

Continued from previous page

Item	Description
last seen [boottime]	Timestamp of the last time the access point (AP) was detected, relative to the scanning device's boot time.
last seen [ms ago]	Timestamp of the last response from the access point (AP).
SSID	Name identifier of the access point (AP).
Supported rates	Data rates supported by the access point (AP).
DS Parameter set	Broadcasting channel of the access point (AP).
ERP	Provides backward compatibility for PHY rates.
RSN	Protocol ensuring secure wireless communication.
Extended supported rates	Additional supported rates beyond the basic eight.
Country	Regulatory domain for the AP, dictating operational parameters.
BSS Load	Current load information on the Basic Service Set (BSS).
RM enabled capabilities	AP's ability to report radio spectrum measurements.
(V)HT capabilities	Features enhancing data rates for 802.11ac/n networks.
(V)HT operation	Utilization of (V)HT capabilities in the current setup.
Overlapping BSS scan params	Guides scanning for overlapping BSS to minimize interference.
Extended capabilities	Additional AP features improving network functions.
WMM	Prioritizes network traffic to ensure quality for voice and video.

Table 9: Detailed Information about WiFi Networks

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	Network interfaces (Ethernet connection)
ppp0	Active connection to the mobile network – wireless module is connected via USB interface
wlan0	WiFi interface – if configured
tune*x*	OpenVPN tunnel interface – if configured
ipsec*x*	IPSec tunnel interface – if configured
gre1	GRE tunnel interface – if configured
usb*x*	USB interface

Table 10: Description of Interfaces in Network Status

Each of the interfaces displays the following information:

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

Continued on next page

Continued from previous page

Item	Description
collisions	Number of collisions on physical layer
txqueuelen	Length of front network device
RX bytes	Total number of received bytes
TX bytes	Total number of transmitted bytes

Table 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.

For the XR5i v2 routers, interface ppp0 indicates the PPPoE connection.

Network Status refresh

Interfaces

```
eth0      Link encap:Ethernet  HWaddr 02:AD:FF:00:00:26
          inet addr:10.64.0.26  Bcast:10.64.3.255  Mask:255.255.252.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9286 errors:0 dropped:0 overruns:0 frame:0
          TX packets:479 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1696809 (1.6 MB)  TX bytes:208130 (203.2 KB)
          Interrupt:39 Base address:0x8000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

usb0      Link encap:Ethernet  HWaddr BA:0B:30:C2:01:07
          inet addr:10.80.0.30  Bcast:0.0.0.0  Mask:255.255.255.255
          UP BROADCAST RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:656 (656.0 B)  TX bytes:574 (574.0 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
192.168.253.254 0.0.0.0         255.255.255.255 UH    0      0        0 usb0
```

Figure 6: Network Status

3.6 DHCP Status

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

See Figure 7 for the DHCP Status example. Records in the *DHCP Status* window are divided into two parts based on the interface.

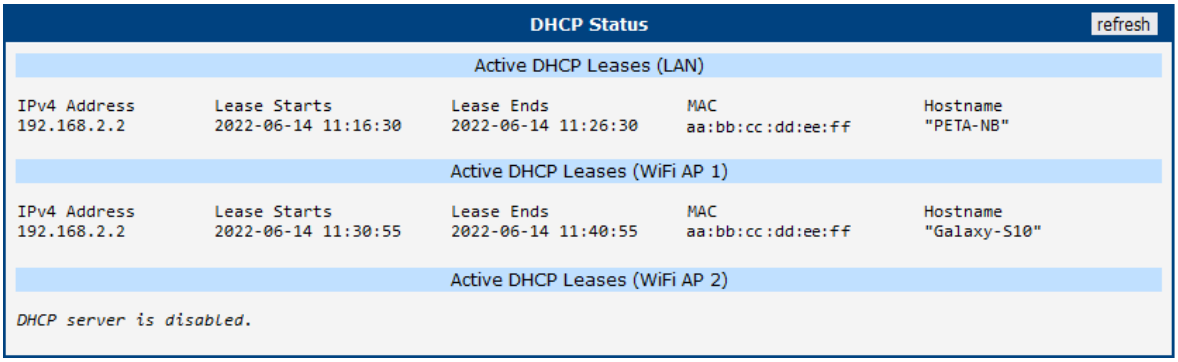


Figure 7: DHCP Status

The DHCP status window displays the following information on a row for each client in the list. All items are described in Table 12.

Item	Description
IPv4 Address	IPv4 address assigned to a client.
Lease Starts	The time the IP address lease started.
Lease Ends	The time the IP address lease expires.
MAC	MAC address of the client.
Hostname	Client hostname.

Table 12: DHCP Status Description

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

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!

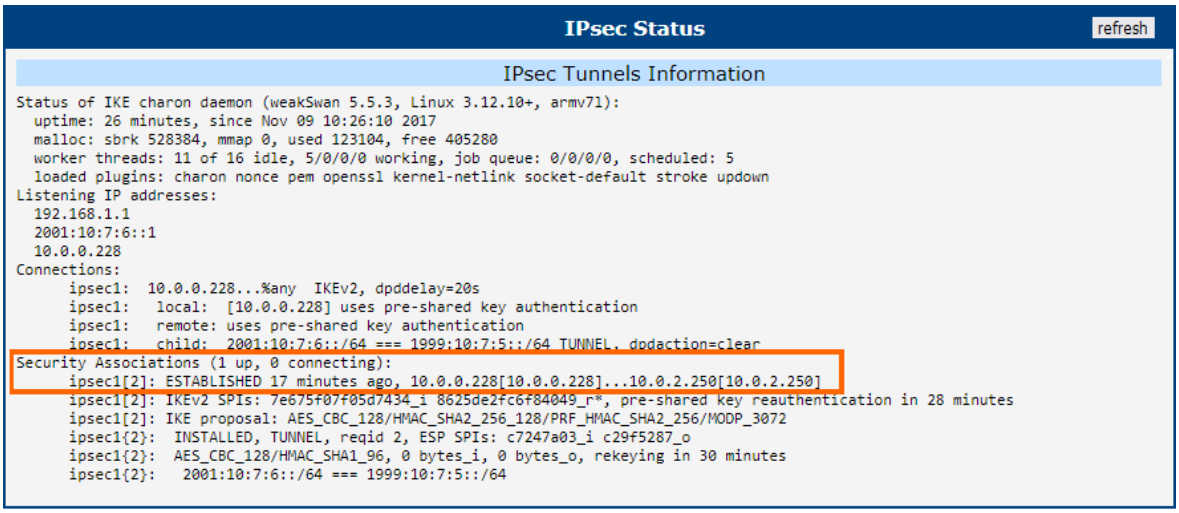


Figure 8: IPsec Status

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 servers for the Dynamic DNS service:

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

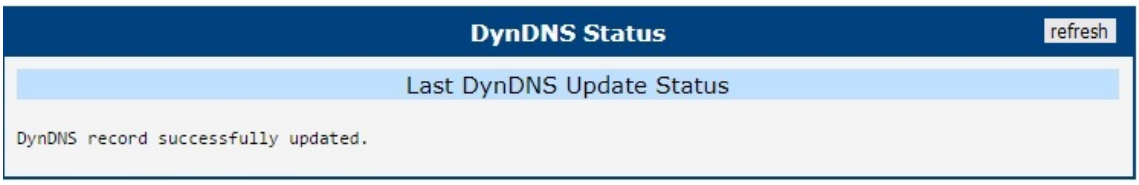


Figure 9: DynDNS Status

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 deamon 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 11.

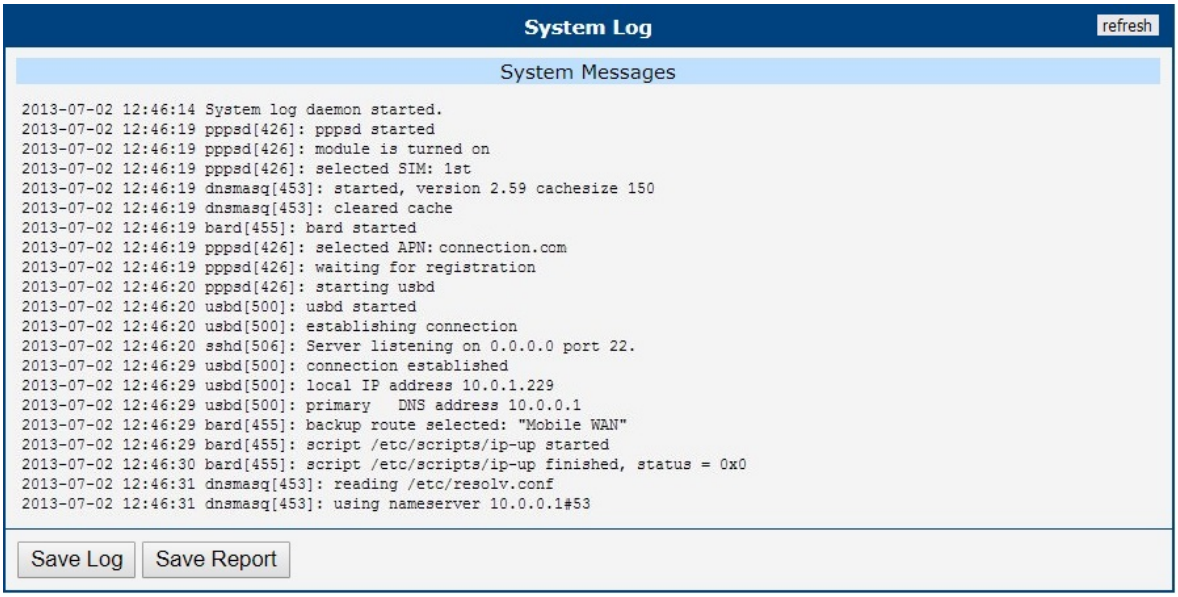


Figure 10: System Log

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

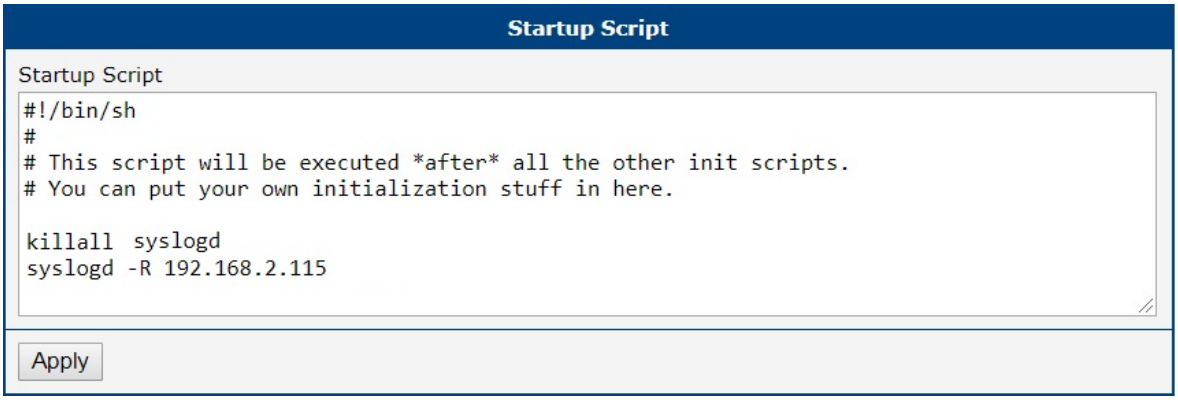


Figure 11: Example program syslogd start with the parameter `-R`

4. Configuration

4.1 Ethernet Configuration

To enter the Local Area Network configuration, select the *Ethernet* menu item in the *Configuration* section. The *ETH0* subitem is for the router's main Ethernet interface. If the router has additional Ethernet ports (*PORT1* or *PORT2*), they are configured using the *ETH1* subitem. For routers with two additional Ethernet ports, *PORT1* and *PORT2* are automatically bridged together.

Item	Description
DHCP Client	Enables/disables the DHCP client function. • **disabled** – The router does not allow automatic allocation IP address from a DHCP server in LAN network. • **enabled** – The router allows automatic allocation IP address from a DHCP server in LAN network.
IP address	Specifies a fixed set of IP addresses for the network interfaces ETH.
Subnet Mask	Specifies a Subnet Mask for the IP address.
Default Gateway	Specifies the IP address of default gateway. When entering the IP address of default gateway, every packet for which the destination IP address was not found in the routing table, is sent to this IP address.
DNS server	Specifies the IP address of the DNS server. When the IP address is not found the Routing Table, the router forwards an IP address requests to the DNS server.
Bridged	Activates/deactivates the bridging function on the router. • **no** – The bridging function is inactive (default). • **yes** – The bridging function is active.

Continued on next page

Continued from previous page

Item	Description
Media type	Specifies the type of duplex and speed used in the network. • **Auto-negation** – The router automatically sets the best speed and duplex mode of communication according to the network's possibilities. • **100 Mbps Full Duplex** – The router communicates at 100Mbps, in the full duplex mode. • **100 Mbps Half Duplex** – The router communicates at 100Mbps, in the half duplex mode. • **10 Mbps Full Duplex** – The router communicates at 10Mbps, in the full duplex mode. • **10 Mbps Half Duplex** – The router communicates at 10Mbps, in the half duplex mode.
MTU	Maximum Transmission Unit value. Default value is 1500 bytes.

Table 13: Configuration of the Network Interface

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

The *Default Gateway* and *DNS Server* items are only used if the *DHCP Client* item is set to *disabled* and if the ETH0 or ETH1 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).

Only one bridge can be active on the router. The Only *DHCP Client*, *IP Address* and *Subnet Mask* parameters are used to configure the bridge. ETH0 LAN has higher priority when both interfaces (ETH0, ETH1) are added to the bridge. Other interfaces can be added to or deleted from an existing bridge at any time. The bridge can be created on demand for such interfaces, but not if it is configured by their respective parameters.

4.1.1 DHCP Server

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

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

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

Table 14: Configuration of Dynamic DHCP Server

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

Table 15: Configuration of Static DHCP Server

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

4.1.2 802.1X Authentication to RADIUS Server

Authentication (802.1X) to RADIUS server can be enabled in next configuration section. The router can be RADIUS user or 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. 2.1.2!
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. 2.1.2!

Table 16: Configuration of 802.1X Authentication

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

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

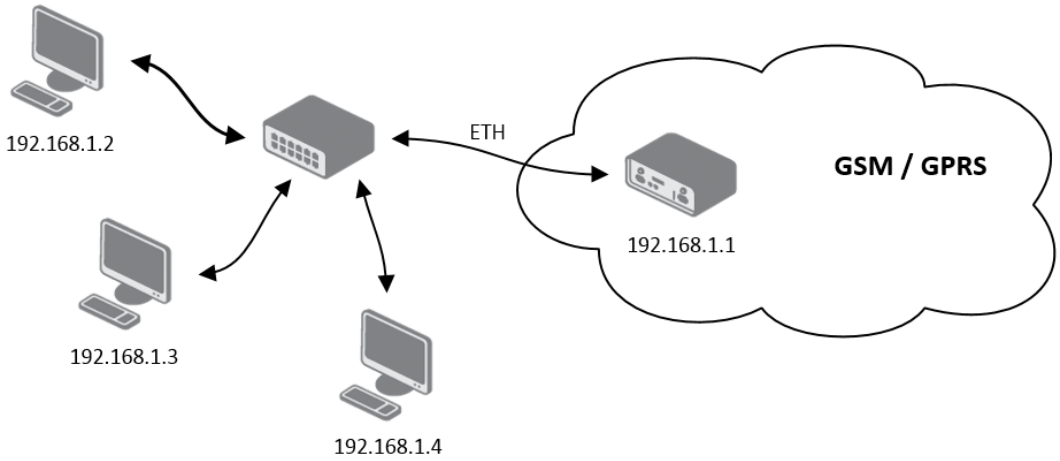


Figure 12: Example 1 – Network Topology for Dynamic DHCP Server

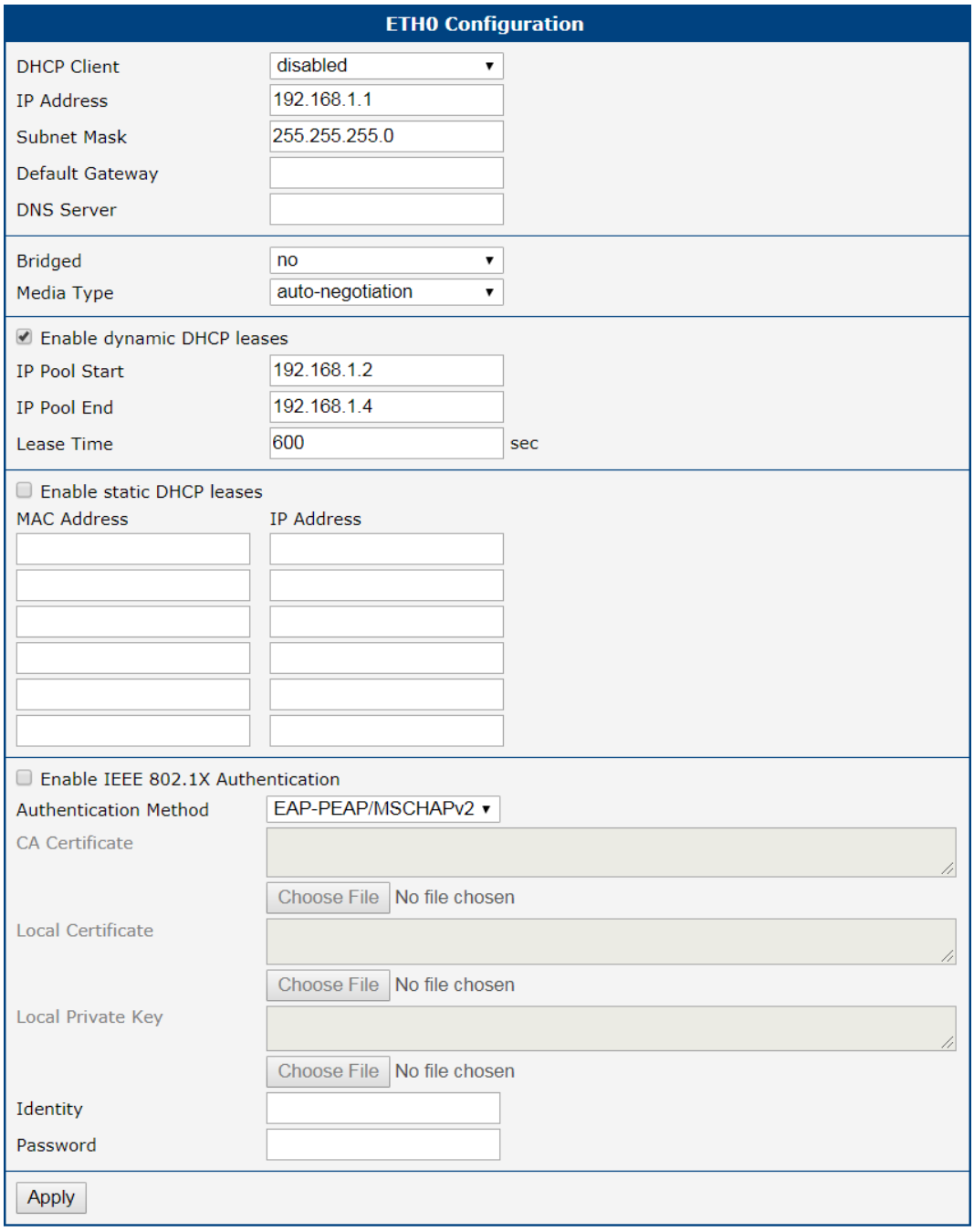


Figure 13: Example 1 – LAN Configuration Page

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

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

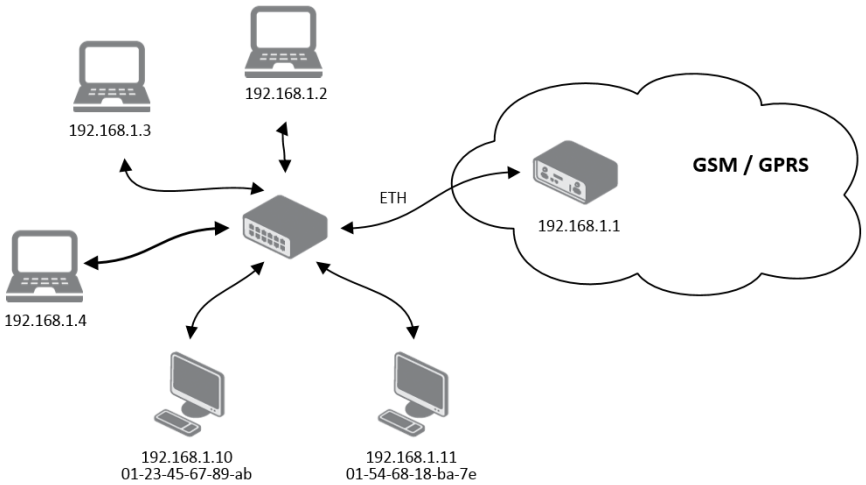


Figure 14: Example 2 – Network Topology with both Static and Dynamic DHCP Servers

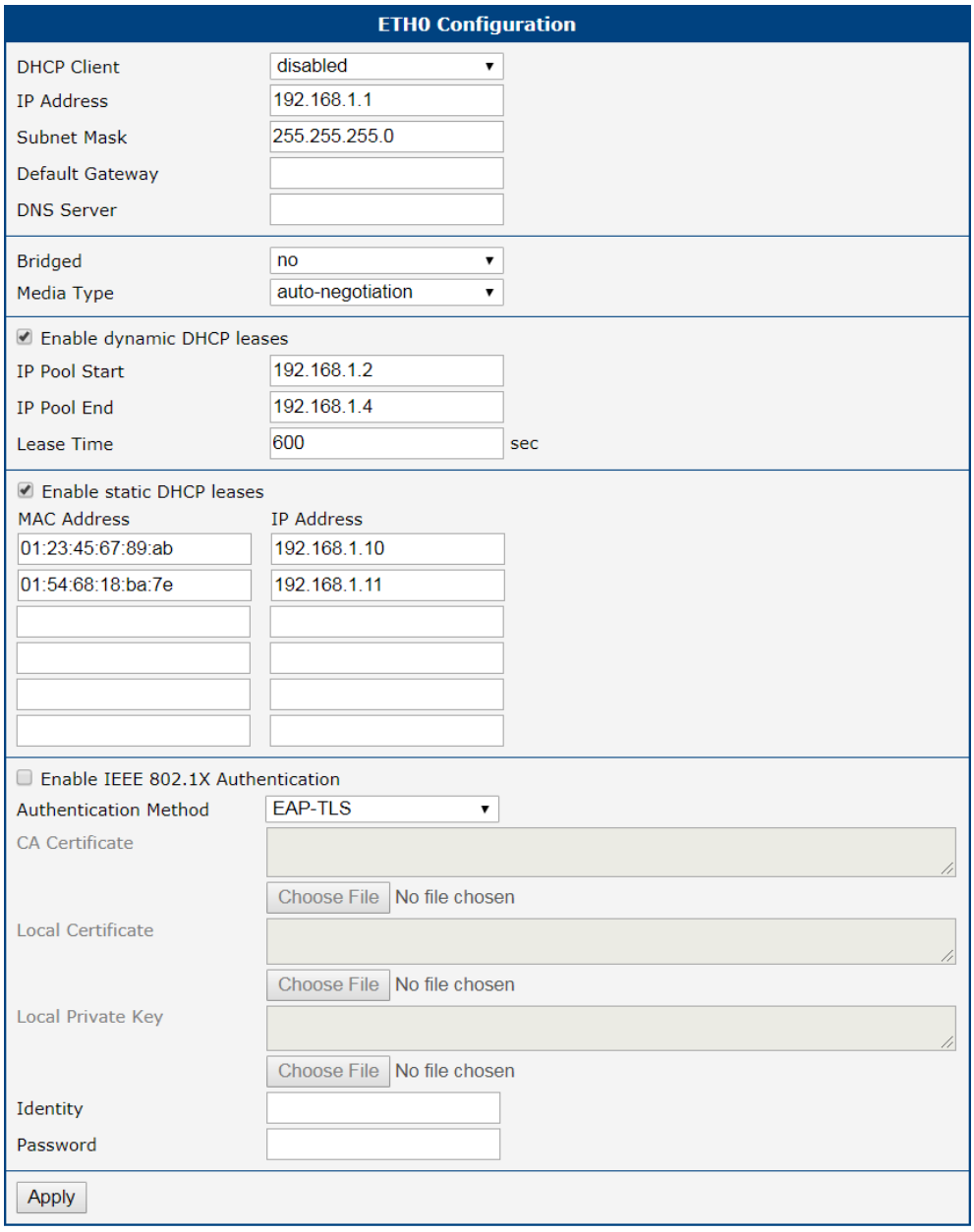


Figure 15: Example 2 – LAN Configuration Page

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

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

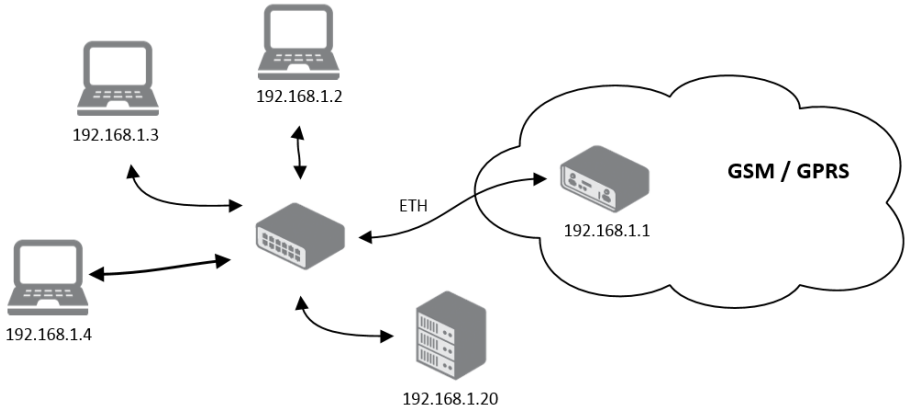


Figure 16: Example 3 – Network Topology

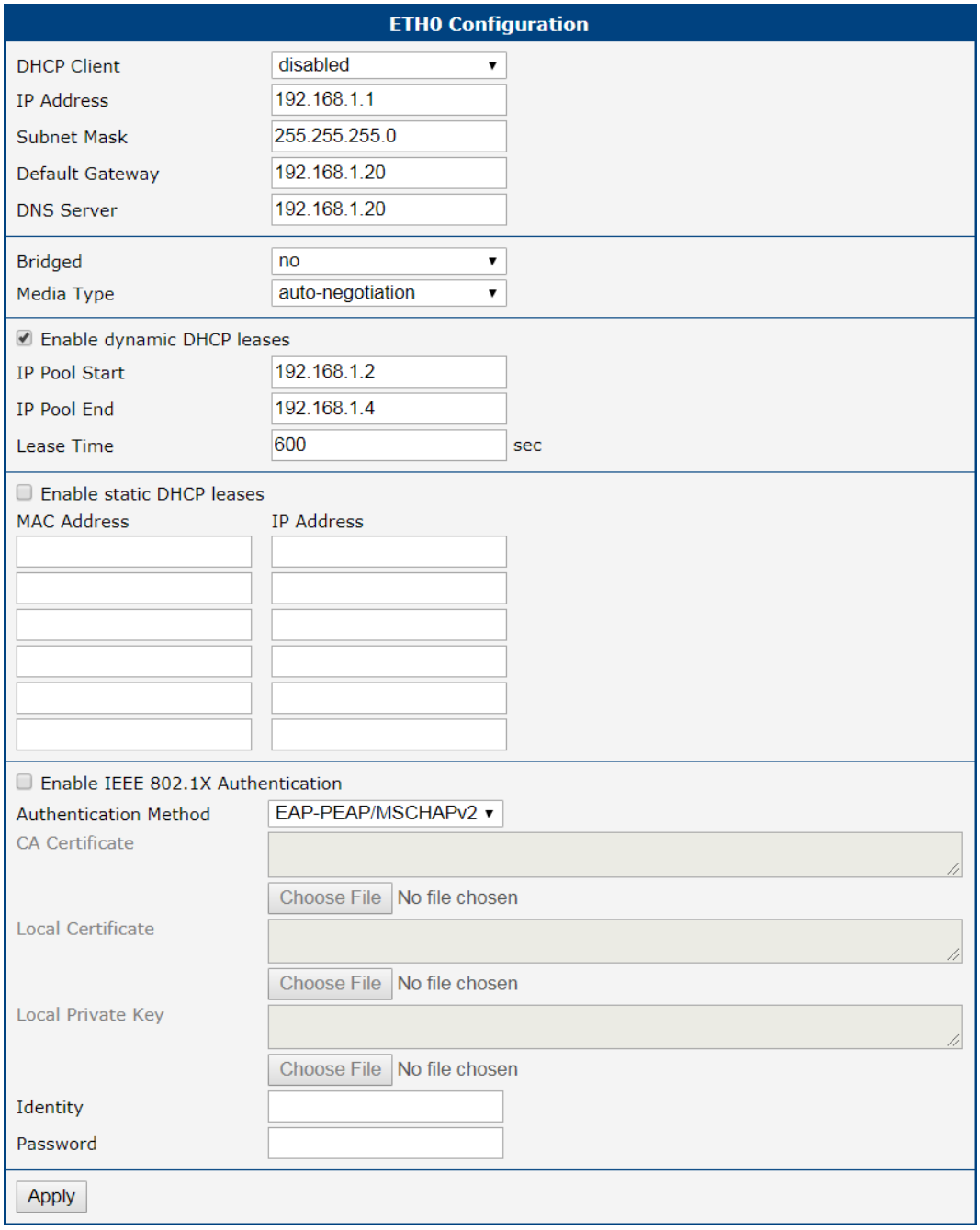


Figure 17: Example 3 – LAN Configuration Page

4.2 VRRP Configuration

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

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

Table 17: 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 18: Check connection

Example of the VRRP protocol:

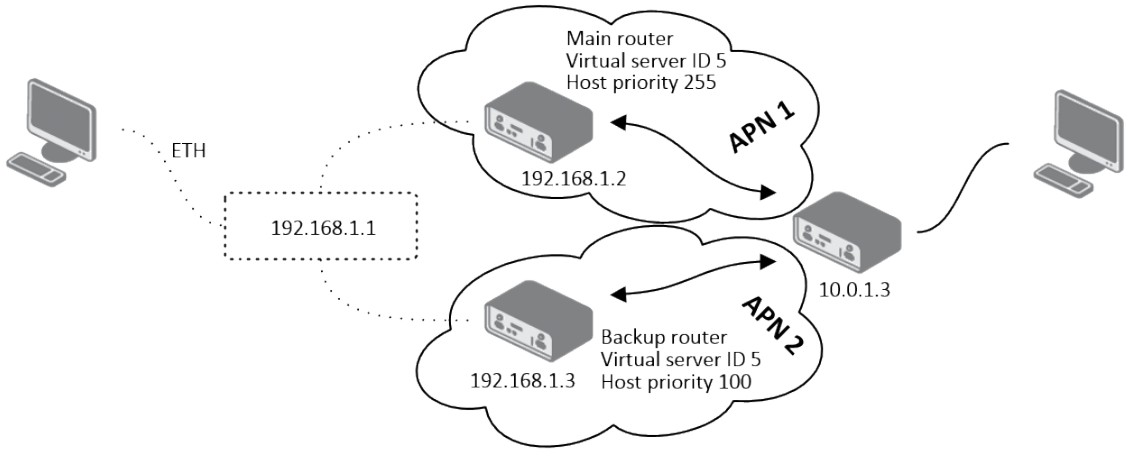


Figure 18: Topology of VRRP configuration example

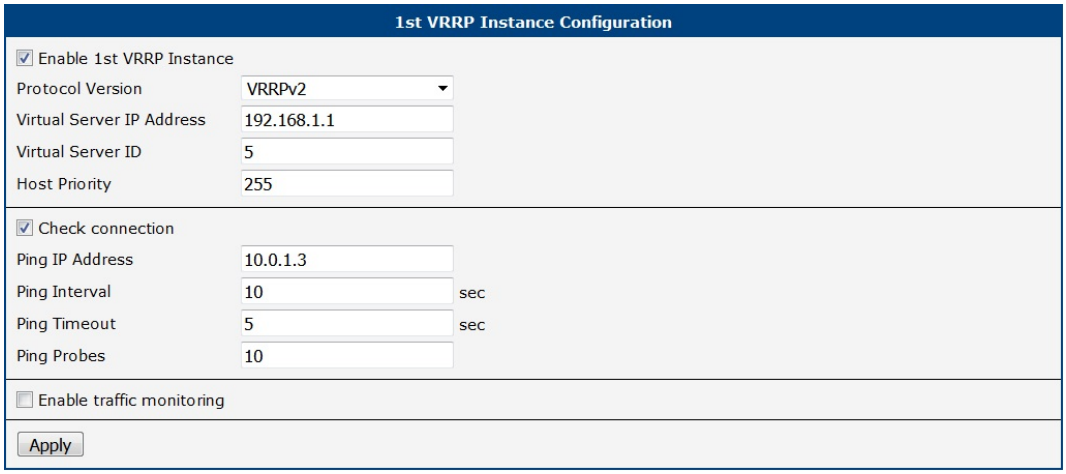


Figure 19: Example of VRRP configuration – main router

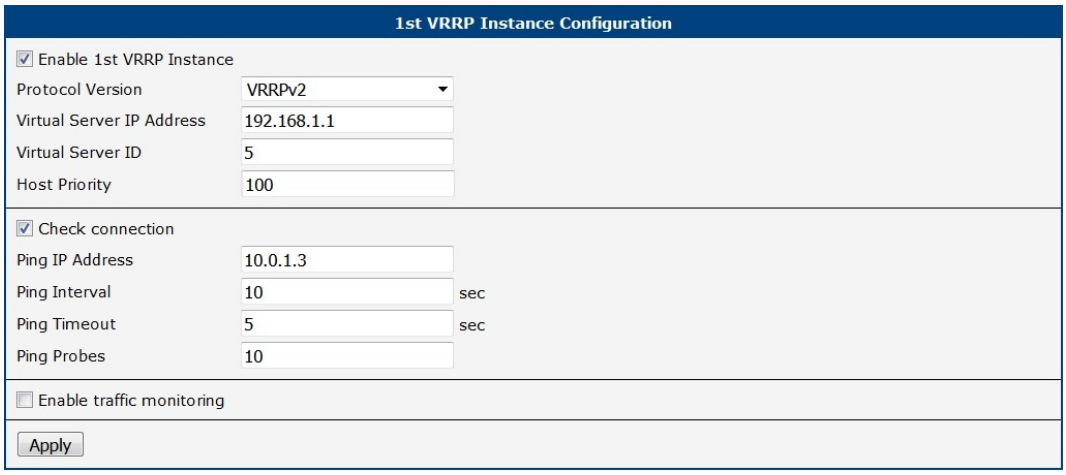


Figure 20: Example of VRRP configuration – backup router

4.3 Mobile WAN Configuration

The XR5i v2 routers do not display the *Mobile WAN* configuration option.

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

4.3.1 Connection to Mobile Network

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

Item	Description
APN	Network identifier (Access Point Name)
Username	User name for logging into the GSM network
Password	Password for logging into the GSM network Enter valid characters only, see chap. 2.1.2!
Authentication	Authentication protocol in the GSM network: • **PAP or CHAP** – The router selects the authentication method. • **PAP** – The router uses the PAP authentication method. • **CHAP** – The router uses the CHAP authentication method.
IP Address	Specifies the IP address of SIM card. You manually enter the IP address, only when mobile network carrier assigned the IP address.
Dial Number	Specifies the telephone number the router dials for a GPRS or CSD connection. The router uses a default telephone number *99***1 #.
Operator	Specifies the carrier code. You can specify the parameter as the PLNM preferred carrier code.
Network type	Specifies the type of protocol used in the mobile network. • **Automatic selection** – The router automatically selects the transmission method according to the availability of transmission technology. • *Furthermore, according to the type of router* – It's also possible to select a specific method of data transmission (GPRS, UMTS, . . .)

Continued on next page

Continued from previous page

Item	Description
PIN	Specifies the PIN used to unlock the SIM card. Use a PIN parameter only if the network requires a SIM card router. The SIM card is blocked after several failed attempts to enter the PIN.
MRU	Specifies the Maximum Receive Unit which is the maximum size of a packet that the router can receive in a given environment. The default value is 1500 B. Other settings can cause the router to incorrectly transmit data. Minimal value is 128 B.
MTU	Specifies the Maximum Transmission Unit which is the maximum size of a packet that the router can transmit in a given environment. The default value is 1500 B. Other settings can cause the router to incorrectly transmit data. Minimal value is 128 B.

Table 19: Mobile WAN Connection Configuration

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

- If the MTU size is set incorrectly, then the router does not exceed the data transfer. When you set the MTU value low, more frequent fragmentation of data occurs. More frequent fragmentation means a higher overhead and also the possibility of packet damage during defragmentation. On the contrary, a higher MTU value can cause the network to drop the packet.
- If the *IP address* field is left blank, when the router establishes a connection, then the mobile network carrier automatically assigns an IP address. If you assign an IP address, then the router accesses the network quicker.
- If the ***APN*** field is left blank, the router automatically selects the APN using the IMSI code of the SIM card. The name of the chosen APN can be found in the System Log.
- If you enter the word `blank` in the *APN* field, then the router interprets the APN as blank.

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

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

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

4.3.2 DNS Address Configuration

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

4.3.3 Check Connection to Mobile Network

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*, the router will be sending the ping requests to the specified domain or IP address configured in *Ping IP Address* or *Ping IPv6 Address* at regular time intervals set up in the *Ping Interval*.

In case of an unsuccessful ping, a new ping will be sent after the *Ping Timeout*. If the ping is unsuccessful three times in a row, the router will terminate the cellular connection and will attempt to establish a new one.

This monitoring function can be set for both SIM cards separately, but running on the active SIM at given time only. Be sure, you configure a functional address as the destination for the ping, for example an IP address of the operator's DNS server.

If the *Check Connection* item is set to the *enabled*, the ping requests are being 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* to *enabled + bind*. The *disabled* option deactivates checking of the connection to the mobile network.

A note for routers connected to the **Verizon** carrier (detected 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.

If *Enable Traffic Monitoring* item is checked, the router will monitor the Mobile WAN traffic without sending the ping requests. If there is no traffic, the router will start sending the ping requests.

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

Table 20: Check Connection to Mobile Network Configuration

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

4.3.4 Data Limit Configuration

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

Table 21: Data Limit Configuration

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

4.3.5 Switch between SIM Cards Configuration

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

The router will automatically toggle between the SIM cards and their individual setups depending on the configuration settings specified here (manual permission, roaming, data limit, binary input 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	Enable or disable the use of a SIM card. If you set all the SIM cards to *disabled*, this means that the entire cellular module is disabled. • **enabled** – It is possible to use the SIM card. • **disabled** – Never use the SIM card, the usage of this SIM is forbidden.
Roaming State	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! • **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	Configure the use of SIM cards based on the Data Limit set above: • **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	Configure the use of SIM cards based on binary input 0 state. This option is not available on Libratum versions of the routers. • **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 1 – voltage present. • **off** – Only use the SIM card if the BIN0 state is logical 0 – no voltage.

Table 22: 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	Specifies the modules' default SIM card. The router will attempt to establish a connection to mobile network using this default. • **1st** – The 1st SIM card is the default one. • **2nd** – The 2nd SIM card is the default one.

Continued on next page

Continued from previous page

Item	Description
Initial State	Specifies the action of the cellular module after the SIM card has been selected. • **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. Note: If offline, you can change this initial state by SMS message only – see *SMS Configuration*. The cellular module will also go into off-line mode if none of the SIM cards are not selected.
Switch to other SIM card when connection fails	Applicable only when connection is established on the default SIM card and then fails. If the connection failure is detected by *Check Connection* feature above, the router will switch to the backup SIM card.
Switch to default SIM card after timeout	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 beacuse of a **failure** of the default one or if **roaming** settings cause the switch. This feature is available only when *Switch to other SIM card when connection fails* is enabled.
Initial Timeout	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.
Subsequent Timeout	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.
Additive Constant	Specifies the length of time that the router waits for any further attempts to revert to the default SIM card. This length time is the sum of the time specified in the "Subsequent Timeout" parameter and the time specified in this parameter. The range in this parameter is from 1 to 10000 minutes.

Table 23: Parameters for SIM card switching

Example:

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

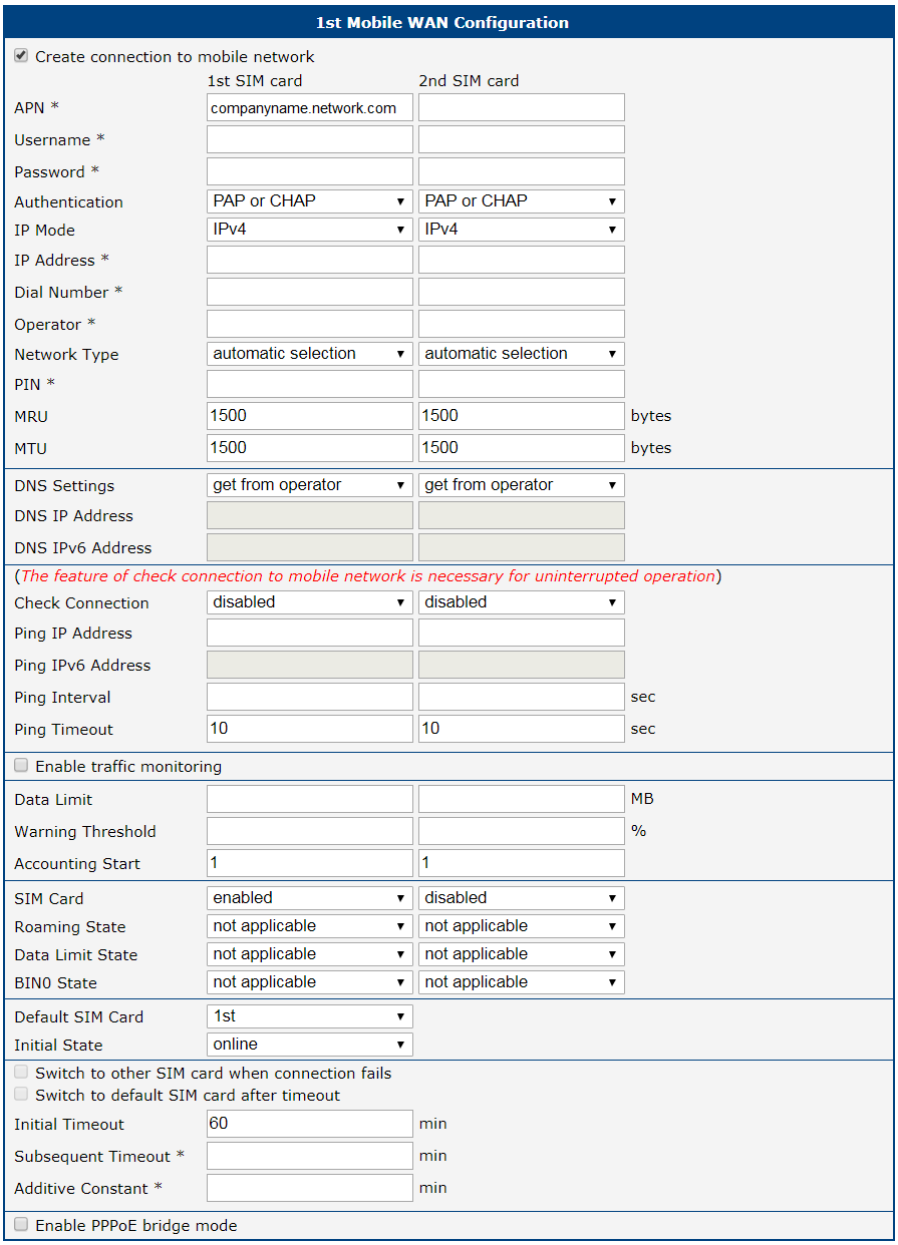
- *Initial Timeout* – 60 min,
- *Subsequent Timeout* – 30 min,
- *Additional Timeout* – 20 min.

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

4.3.6 PPPoE Bridge Mode Configuration

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

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



1st Mobile WAN Configuration

☑ Create connection to mobile network

	1st SIM card	2nd SIM card	
APN *	companyname.network.com		
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	disabled	disabled	
Ping IP Address			
Ping IPv6 Address			
Ping Interval			sec
Ping Timeout	10	10	sec

☐ Enable traffic monitoring

Data Limit			MB
Warning Threshold			%
Accounting Start	1	1	
SIM Card	enabled	disabled	
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

☐ Switch to other SIM card when connection fails
☐ Switch to default SIM card after timeout

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

☐ Enable PPPoE bridge mode

Figure 21: Mobile WAN Configuration

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

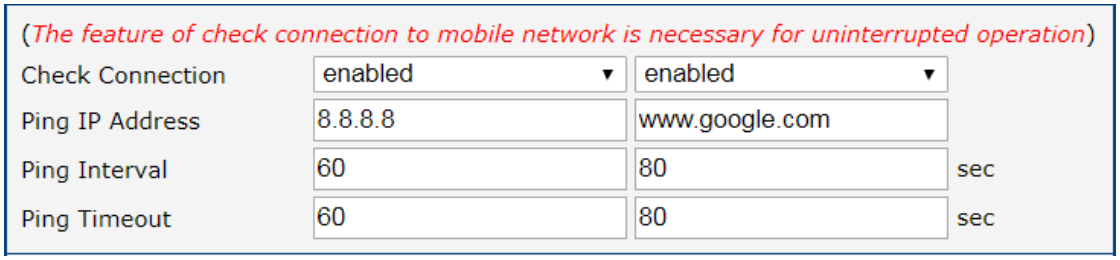


Figure 22: Example 1 – Mobile WAN Configuration

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

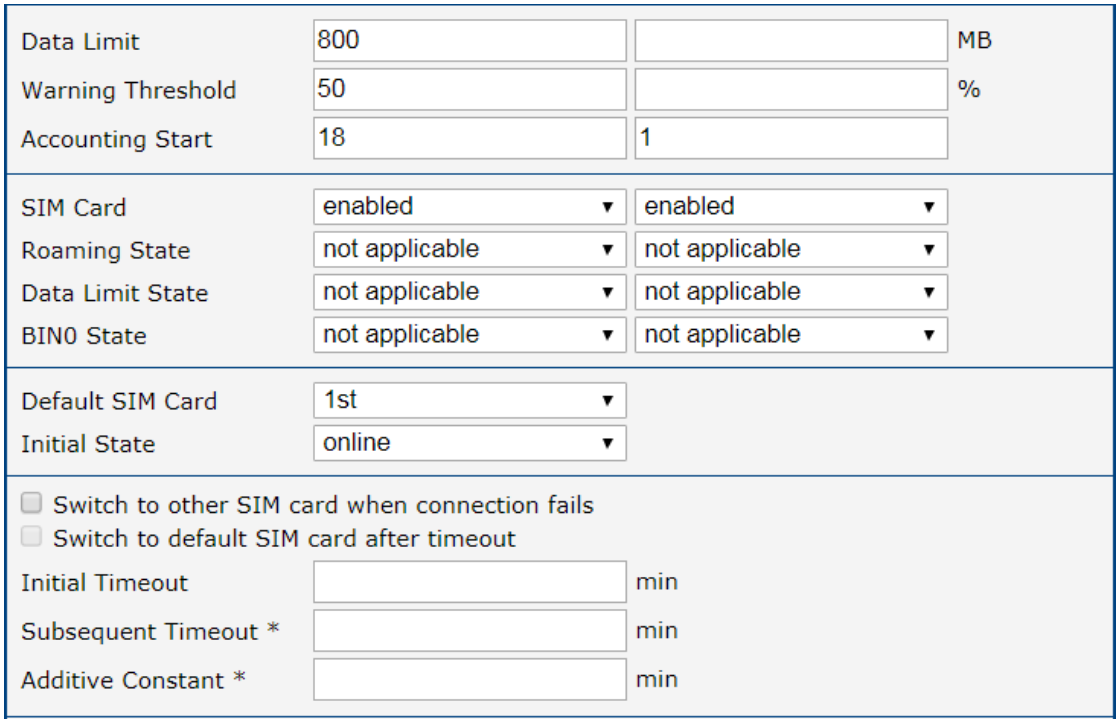


Figure 23: Example 2 – Mobile WAN Configuration

4.4 PPPoE Configuration

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

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

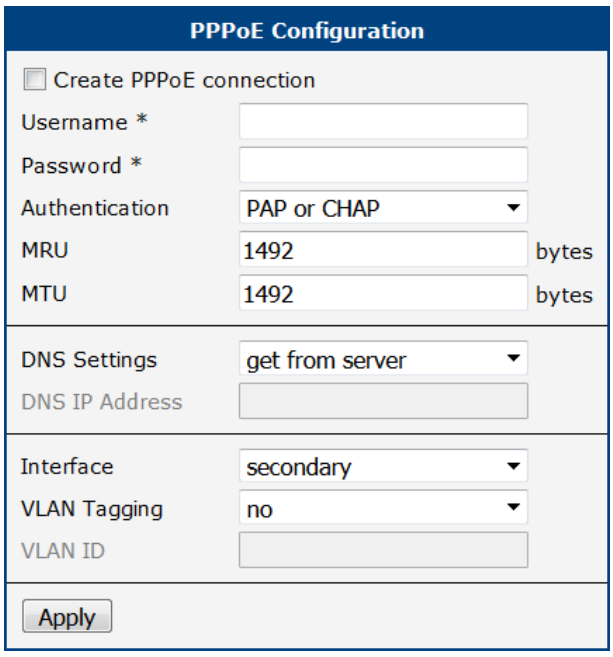


Figure 24: PPPoE configuration

Item	Description
Username	Username for secure access to PPPoE.
Password	Password for secure access to PPPoE. Enter valid characters only.

Continued on the next page

Continued from previous page

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

Table 24: PPPoE configuration

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

4.5 WiFi Access Point Configuration

AttentionBoxThis feature is accessible only on routers equipped with a WiFi module.

Configuration of two separated WLANs (**Multiple SSIDs**) is supported.

Multi-role mode, which allows to operate as access point (AP) and station (STA) simultaneously, is supported. The multichannel mode is not supported, so the AP and the STA must operate on the same channel only.

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.

Activate WiFi access point mode by checking *Enable WiFi AP* box at the top of the *Configuration* → *WiFi* → *Access Point 1* or *Access Point 2* configuration pages. 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.

Item	Description
Enable WiFi AP	Enable WiFi access point (AP).
IP Address	A fixed IP address of the WiFi interface.
Subnet Mask	Subnet mask of WiFi network interface..
Bridged	Activates bridge mode: • **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 server.
IP Pool Start	Beginning of the range of IP addresses which will be assigned to DHCP clients.
IP Pool End	End of the range of IP addresses which will be assigned to DHCP clients.
Lease Time	Time in seconds for which the client may use the IP address.
SSID	The unique identifier of WiFi network.

Continued on next page

Continued from previous page

Item	Description
Broadcast SSID	Method of broadcasting the unique identifier of SSID network in beacon frame and type of response to a request for sending the beacon frame. • **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	Code of the country where the router is installed. This code must be entered in ISO 3166-1 alpha-2 format. If a *country code* isn't specified and the router has not implemented a system to determine this code, it will use "US" as the default *country code*. If no *country code* is specified or if the wrong country code is entered, the router may violate country-specific regulations for the use of WiFi frequency bands.
Follow STA radio settings	When enabled and the STA is connected to a foreign AP, the AP's radio settings will be reconfigured based on the settings of the foreign AP that the STA is currently connected to.
HW Mode	HW mode of WiFi standard that will be supported by WiFi access point. • IEEE 802.11b (2.4 GHz) • IEEE 802.11b+g (2.4 GHz) • IEEE 802.11b+g+n (2.4 GHz)
Channel	The channel, where the WiFi AP is transmitting. Supported 2.4 GHz channels: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13.
Bandwidth	The option for HW mode 802.11n which allows to choose the bandwidth. If the 40 MHz channel is occupied, for 802.11bgn mode, the 20 MHz channel is used instead.

Continued on next page

Continued from previous page

Item	Description
Short GI	The option for HW mode 802.11n which allows to enable the short guard interval (GI) of 400 ns instead of 800 ns.
WMM	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.
Authentication	Access control and authorization of users in the WiFi network. • **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** – WPA2-PSK using newer AES encryption. • **WPA3-PSK** – WPA3-PSK using newer AES encryption. • **WPA-Enterprise** – RADIUS authentication done by external server via username and password. • **WPA2-Enterprise** – RADIUS authentication with better encryption. • **WPA3-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	Type of data encryption in the WiFi network: • **None** – No data encryption. • **WEP** – Encryption using static WEP keys. This encryption can be used for *Shared* authentication. • **TKIP** – Dynamic encryption key management that can be used for *WPA-PSK* and *WPA2-PSK* authentication. • **AES** – Improved encryption used for *WPA2-PSK* authentication.

Continued on next page

Continued from previous page

Item	Description
WEP Key Type	Type of WEP key for WEP encryption: • **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	Allows entry of four different WEP keys: • WEP key in ASCII format must be entered in quotes. This key can be specified in the following lengths. – 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. – 10 hexadecimal digits (40b WEP key) – 26 hexadecimal digits (104b WEP key) – 32 hexadecimal digits (128b WEP key)
WPA PSK Type	The possible key options for WPA-PSK authentication. • 256-bit secret • ASCII passphrase • PSK File
WPA PSK	Key for WPA-PSK authentication. This key must be entered according to the selected WPA PSK type as follows: • **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	IP 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.

Continued on next page

Continued from previous page

Item	Description
RADIUS Auth Port	RADIUS server port. The default is 1812. Only with one of RADIUS authentications selected.
RADIUS Acct Server IP	IP 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. • **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 Denny list of client MAC addresses that set network access. Each MAC address is separated by new line.
Syslog Level	Logging level, when system writes to the system log. • **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 25: WiFi Configuration

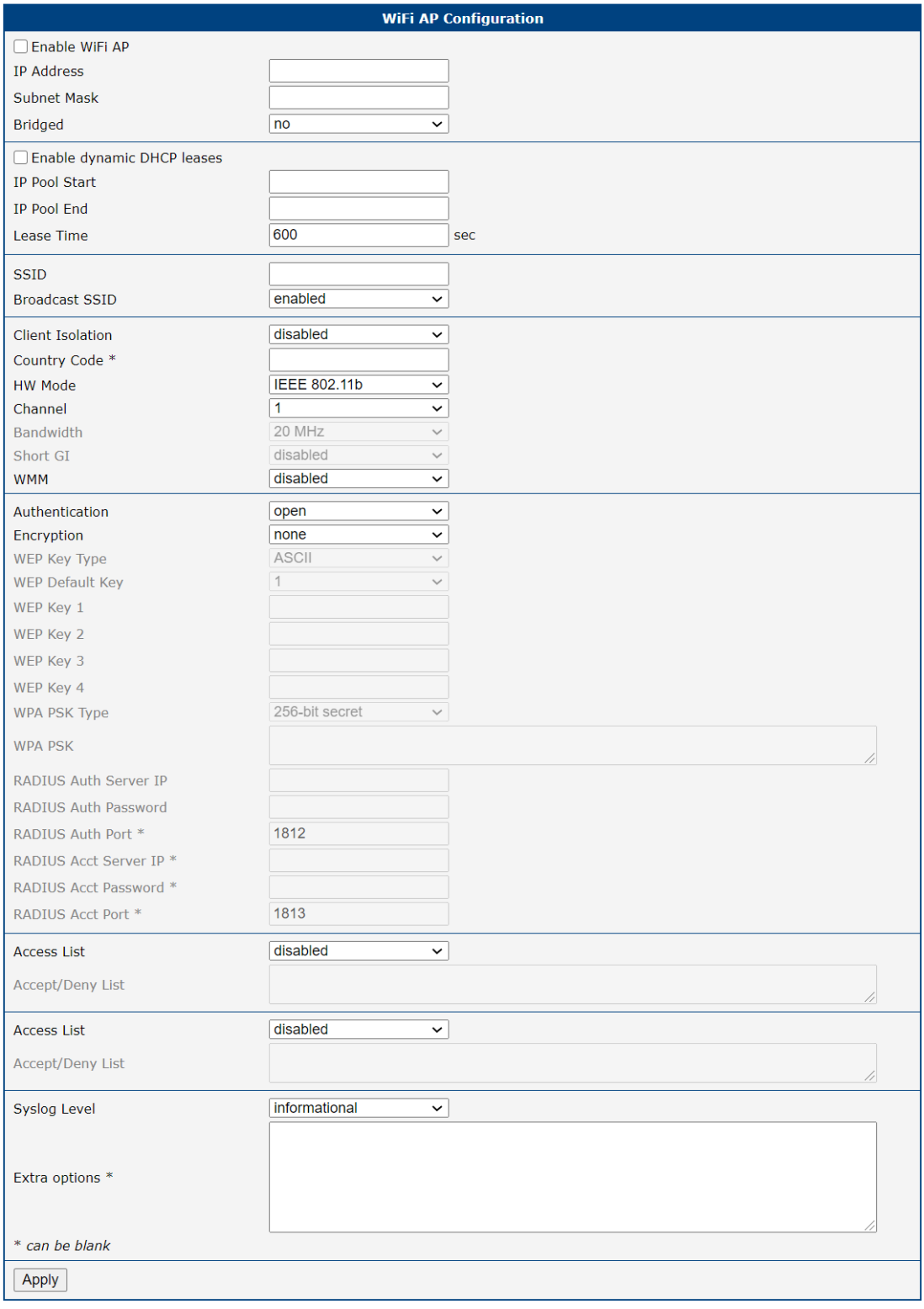


Figure 25: WiFi Access Point Configuration

4.6 WiFi Station Configuration

This feature is accessible only on routers equipped with a WiFi module.

Activate WiFi station mode by checking *Enable WiFi STA* box at the top of the *Configuration* → *WiFi* → *Station* configuration page. 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.
IP Address	A fixed IP address of the WiFi interface.
Subnet Mask / Prefix	Specifies a Subnet Mask for the IP address.
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.
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.
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 *country code* isn't specified and the router has not implemented a system to determine this code, it will use "US" as the default *country code*. If no *country code* is specified or if the wrong country code is entered, the router may violate country-specific regulations for the use of WiFi frequency bands.

Continued on next page

Continued from previous page

Item	Description
Authentication	Access control and authorization of users in the WiFi network. • **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** – WPA2-PSK using newer AES encryption. • **WPA3-PSK** – WPA3-PSK using newer AES encryption. • **WPA-Enterprise** – RADIUS authentication done by external server via username and password. • **WPA2-Enterprise** – RADIUS authentication with better encryption. • **WPA3-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	Type of data encryption in the WiFi network: • **None** – No data encryption. • **WEP** – Encryption using static WEP keys. This encryption can be used for *Shared* authentication. • **TKIP** – Dynamic encryption key management that can be used for *WPA-PSK* and *WPA2-PSK* authentication. • **AES** – Improved encryption used for *WPA2-PSK* authentication.
WEP Key Type	Type of WEP key for WEP encryption: • **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	Allows entry of four different WEP keys: • WEP key in ASCII format must be entered in quotes. This key can be specified in the following lengths. – 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. – 10 hexadecimal digits (40b WEP key) – 26 hexadecimal digits (104b WEP key) – 32 hexadecimal digits (128b WEP key)
WPA PSK Type	The possible key options for WPA-PSK authentication. • 256-bit secret • ASCII passphrase • PSK File
WPA PSK	Key for WPA-PSK authentication. This key must be entered according to the selected WPA PSK type as follows: • **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. • **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 26: WLAN Configuration

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

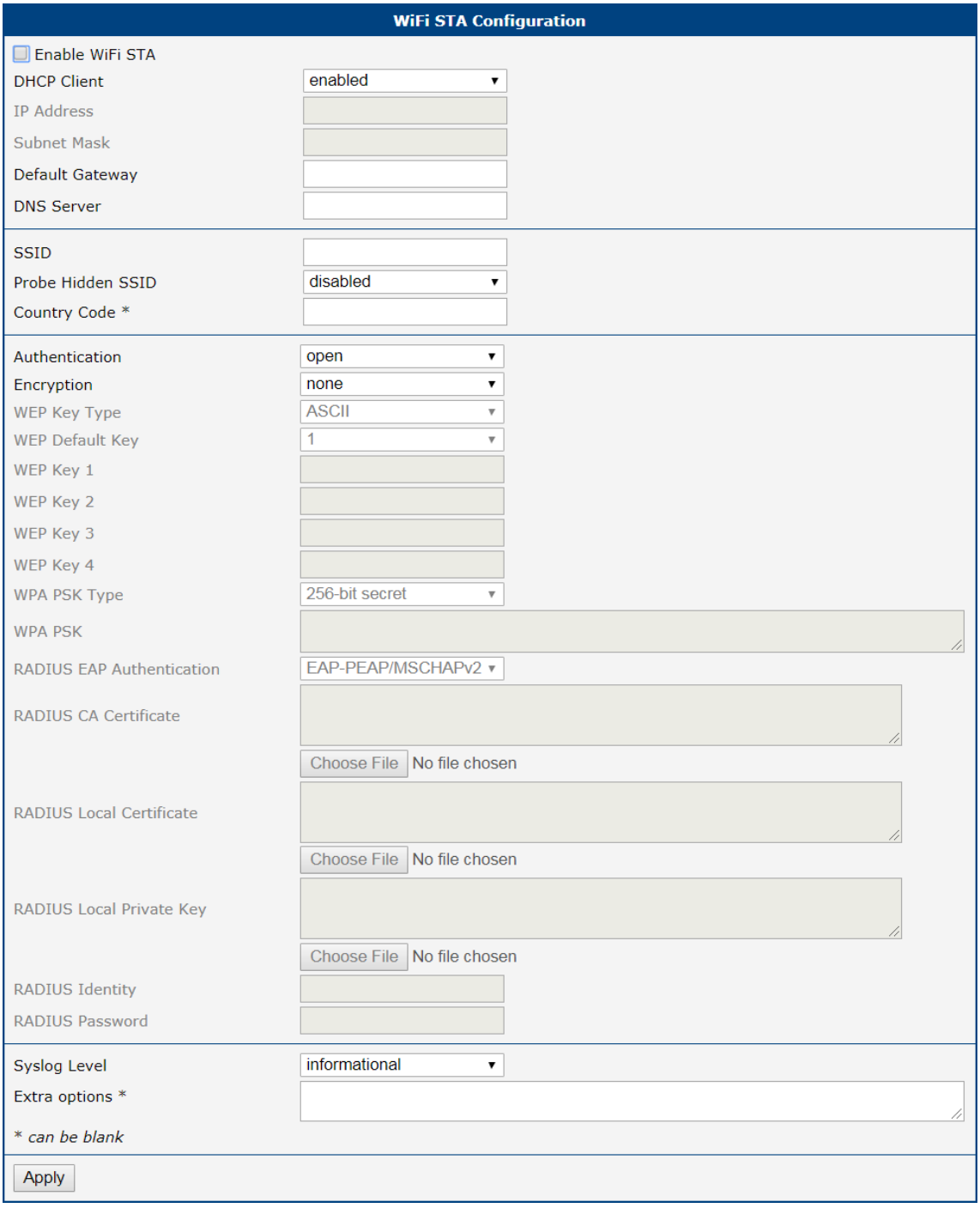


Figure 26: WiFi Station Configuration

4.7 Backup Routes

Note that some interfaces, typically WiFi, ETH2, or ETH1, may not be available for some router product lines or for the model you are currently using.

Typically, you want the router to direct traffic from the whole LAN (Local Area Network) behind the router to an external WAN (Wide Area Network) outside, such as the Internet.

Backup Routes is a mechanism that enables customizing which router's interfaces will be used for communication to the WAN outside the router. The *Backup Routes* configuration page is shown in Figure 27.

You may not care about this configuration and leave this process on the default router mechanism. In this case, leave the *Backup Routes* configuration page as it is, unconfigured, and the router will proceed as described in Chapter 4.7.1.

If you want to set up this feature your way, see Chapter 4.7.2 for more information.

4.7.1 Default Priorities for Backup Routes

By default, when the first checkbox, *Enable backup routes switching*, is unchecked, the backup routes system is not user customized and operates with the default mechanism. Instead, the router selects a route to the WAN based on the default priorities.

The following is the list of the network interfaces in descending order from the highest priority to the lowest priority interface for use as a WAN interface.

1. **Mobile WAN** (pppX, usbX)
2. **PPPoE** (ppp0)
3. **WiFi STA** (wlan0)
4. **ETH1** (eth1)
5. **ETH2** (eth2)
6. **ETH0** (eth0)

For example, based on the list above, we can say that the ETH1 interface will only be used as the WAN interface if Mobile WAN, PPPoE, and WiFI STA interfaces are down or disabled.

It is clear from the above that an interface connected to a LAN network can take over the role of a WAN interface under certain circumstances. Possible communication from the LAN to the WAN can be blocked or forwarded rules configured on the *NAT* and *Firewall* configuration pages.

Note that an ETH interface won't be used as WAN for the default backup route priorities if it has no IP address configured or the DHCP client is disabled for this ETH interface. Also, unplugging the Ethernet cable does not switch the route to the next one (true just for the *Default Priorities* mode).

4.7.2 User Customized Backup Routes

You can choose preferred router interfaces acting as the WAN, including their priorities, on the *Backup Routes* configuration page; see Figure 27. Switching between the WAN is then carried out according to the order of priority and the state of all the affected interfaces.

There are three different modes you can choose for the connection backup as described in Table 27.

Item	Description
Enable backup routes switching	Enables the customized backup routes setting made **on the whole configuration page**. If disabled (unchecked), the backup routes system operates in the default mechanism, as described in Chapter 4.7.1.
Mode	**Single WAN** • Just **one interface** is used for the WAN communication **at a time**. • Other interfaces (if enabled) are used as the backup routes for the WAN communication when the active interface fails (based on the priorities set). • Just one interface, currently active, is allowed to access the router from a network outside the router. **Multiple WANs** • Just **one interface** is used for the WAN communication **at a time**. • Other interfaces (if enabled) are used as the backup routes for the WAN communication when the active interface fails (based on the priorities set). • The router is accessible from networks outside on all enabled interfaces. This is the **only difference** from the *Single WAN* mode. **Load Balancing** • In this mode, it is possible to split the volume of data passing through individual WAN interfaces. • If the mode was chosen, the weight for every interface is enabled in the GUI and can be set. • This setting determines the relative number of data streams passing through the interfaces.

Table 27: Backup Routes Modes

You have now selected a backup route mode. To add a network interface to the backup routes system, mark the enable checkbox of that interface. Enabled interfaces are used for WAN access based on their priorities.

Note for Load Balancing mode: The weight setting for load balancing may not precisely match the amount of balanced data. It depends on the number of data flows and the data structure. The best result of the balancing is achieved for a high amount of data flows.

Note for Mobile WAN: If you want to use a mobile WAN connection as a backup route, 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.

Note for an ETH interface: Unlike the default backup route mode, disconnecting the Ethernet cable from an ETH interface switches the route to the next in the sequence.

Settings, which can be made for each interface, are described in the table below. 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 IP address or domain name of ping queries to check the connection.
Ping Interval	The time interval between consecutive ping queries.
Ping Timeout	Time in seconds to wait for a response to the ping.
Weight	Weight for the Load Balancing mode only. The number from 1 to 256 determines the ratio for load balancing of the interface. For example, if two interfaces set the weight to 1, the ratio is 50% to 50%. If they set the weight up to 1 and 4, the ratio is 20% to 80%.

Table 28: Backup Routes Configuration

Other notes:

- The system checks the status state of an interface. For example, unlike the *Default Priorities* mode, unplugging the Ethernet cable triggers a switchover to the next WAN interface in the sequence.
-

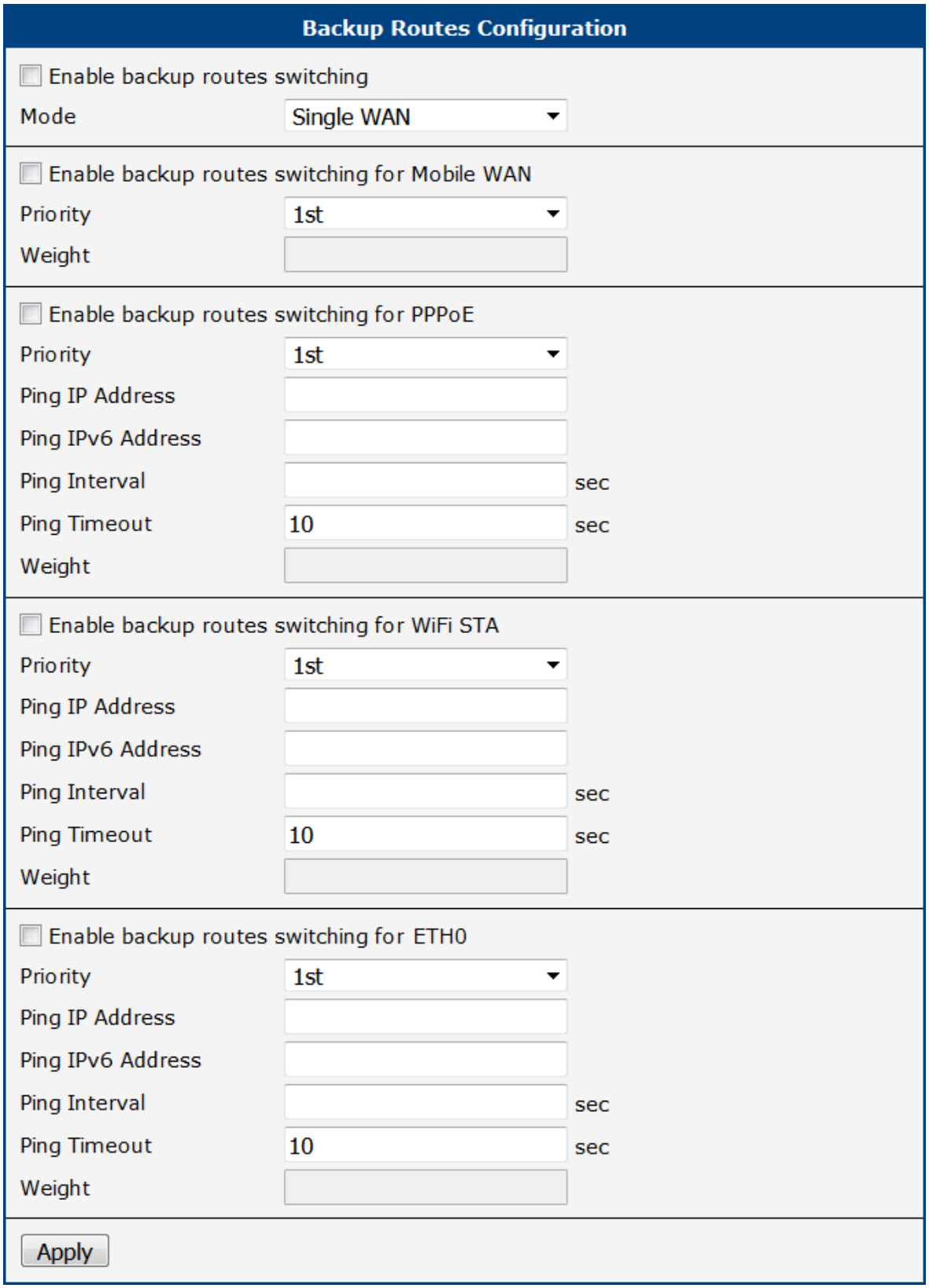


Figure 27: Backup Routes Configuration GUI

4.7.3 Backup Routes Examples

Example #1: Default Settings

As already described above, by default, if the *Backup Routes* are unconfigured, the system operates with the default priorities as described in Chapter 4.7.1. Figure 28 shows the GUI configuration.

Note: Assume all the affected interfaces are correctly configured and activated on their configuration pages.

Figure 28: Example #1: GUI Configuration

Figure 29 illustrates the example topology.

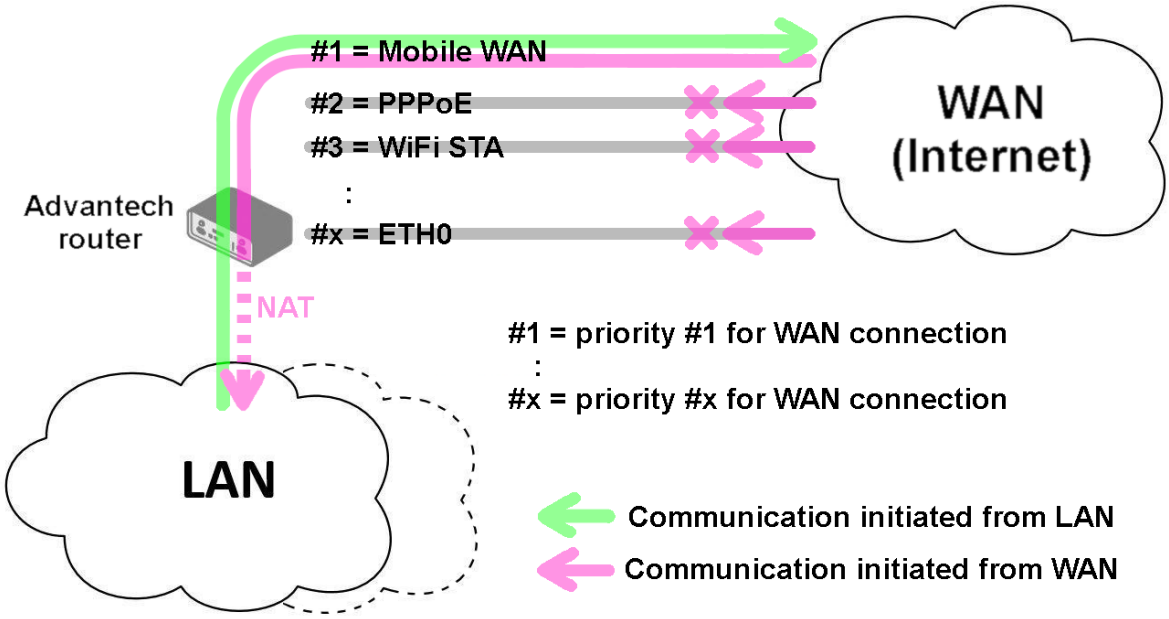


Figure 29: Example #1: Topology

Example #2: Default Routes Switching

This example illustrates when the interface, primarily used for the WAN connection, is down. Its role is taken over by the interface with the second highest priority. Since the *Backup Routes* configuration is still unconfigured, the system operates with the default system priorities described in Chapter 4.7.1. Figure 30 shows the GUI configuration.

Note: Assume all the affected interfaces are correctly configured and activated on their configuration pages.

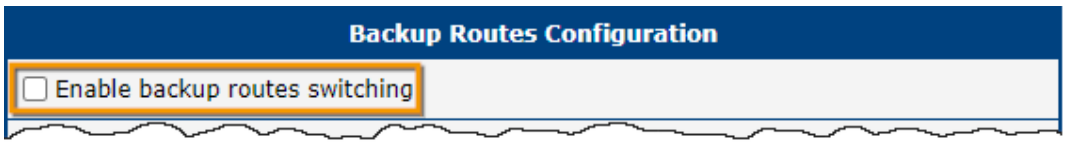


Figure 30: Example #2: GUI Configuration

Figure 31 illustrates the example topology.

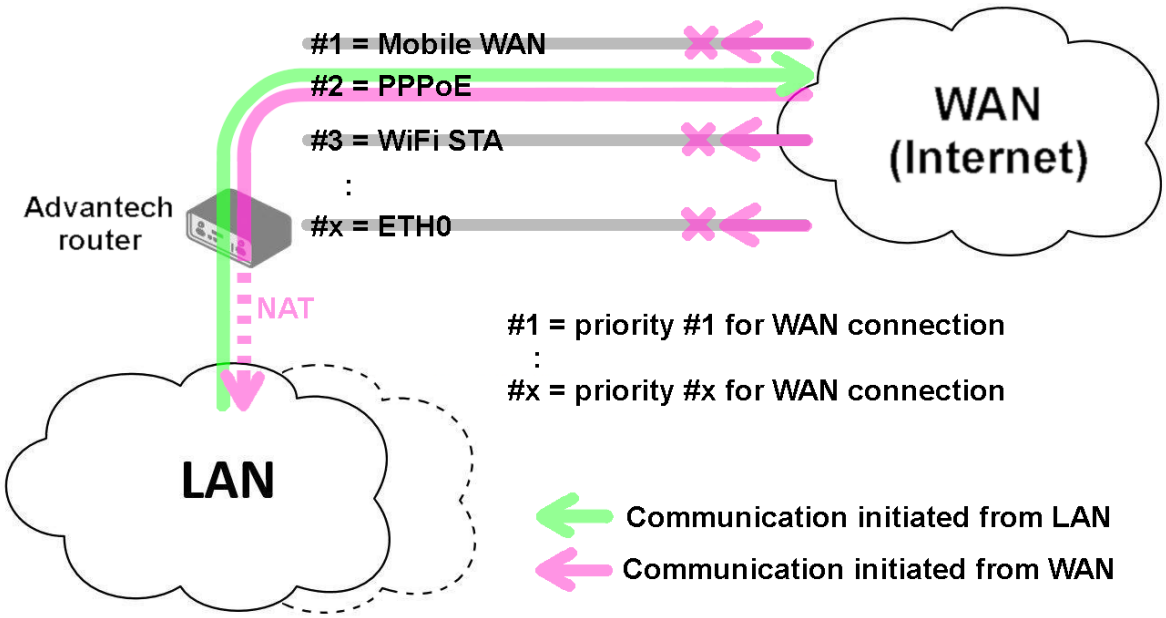


Figure 31: Example #2: Topology

Example #3: Custom Backup Routes

This example illustrates the configuration of custom backup routes for the Mobile WAN, PPPoE, and ETH1 interfaces. The Mobile WAN interface has the highest priority, and the ETH1 interface has the lowest priority. Figure 32 shows the GUI configuration.

Note: Assume all the affected interfaces are correctly configured and activated on their configuration pages.

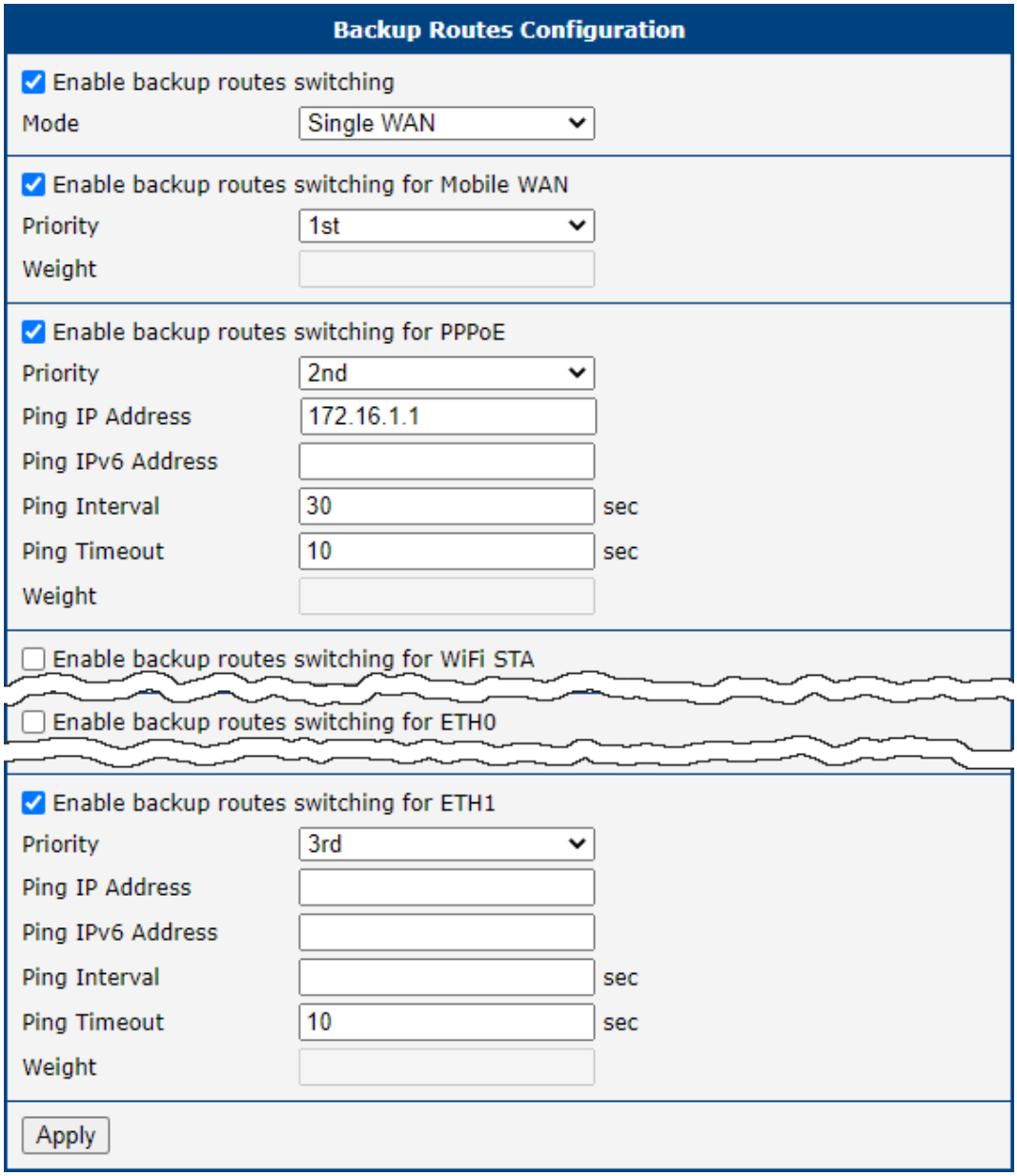


Figure 32: Example #3: GUI Configuration

Figure 33 illustrates the example topology for *Single WAN* mode. If the Mobile WAN connection goes down, the PPPoE tunnel takes its role, and so on. The ping to the 172.16.1.1 address, tested every 30 seconds with a timeout of 10 seconds, checks the status of the PPPoE tunnel.

Figure 34 illustrates the example topology for *Multiple WAN* mode. As you can see, the only difference between these two modes is that in the *Multiple WAN* mode, the router is accessible on all interfaces from the WAN simultaneously.

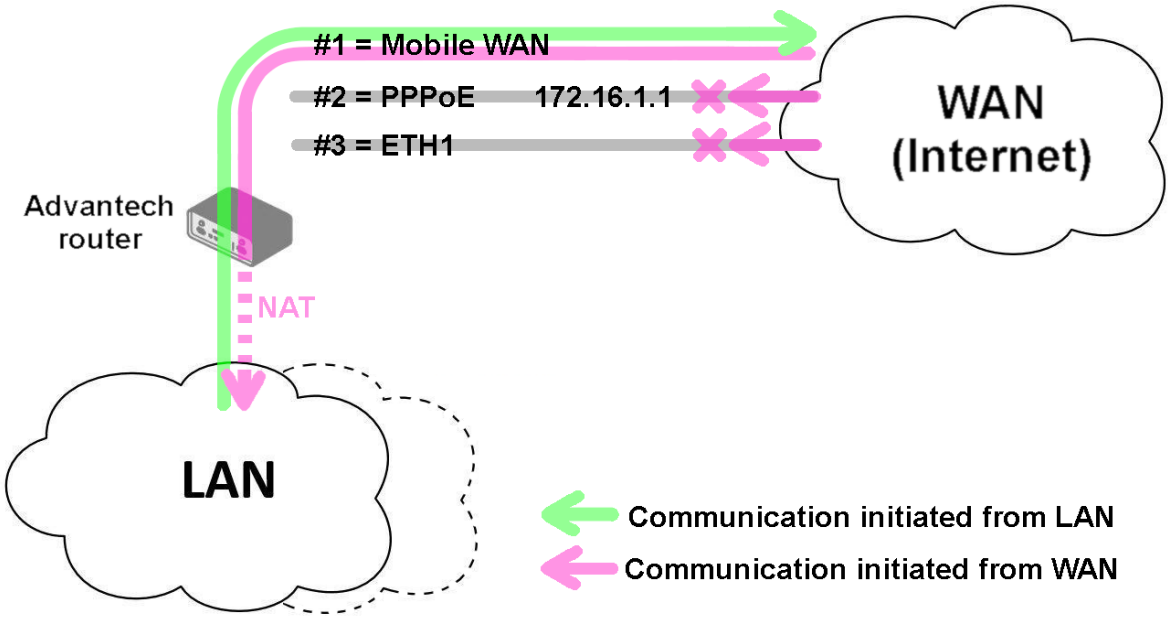


Figure 33: Example #3: Topology for *Single WAN* mode

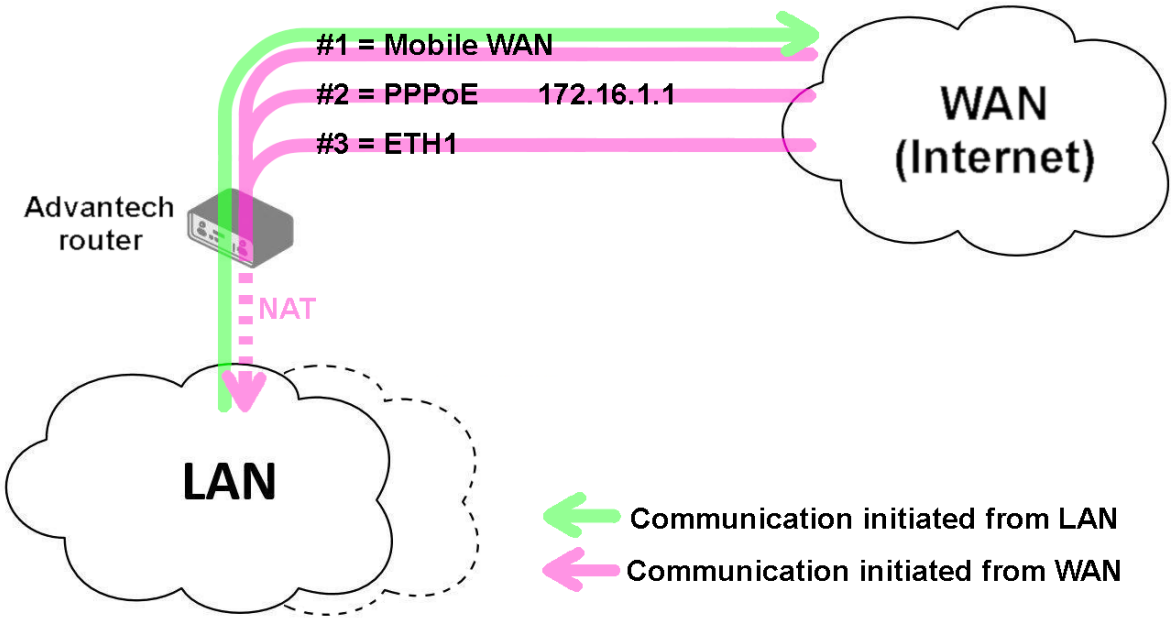


Figure 34: Example #3: Topology for *Multiple WAN* mode

Example #4: Load Ballancing Mode

This example illustrates the *Load Balancing* mode configuration. There are just two interfaces configured, the Mobile WAN and PPPoE. The weight is set to 4 and 1, so the traffic data volume is approximately 80 and 20 percent. Figure 35 shows the GUI configuration.

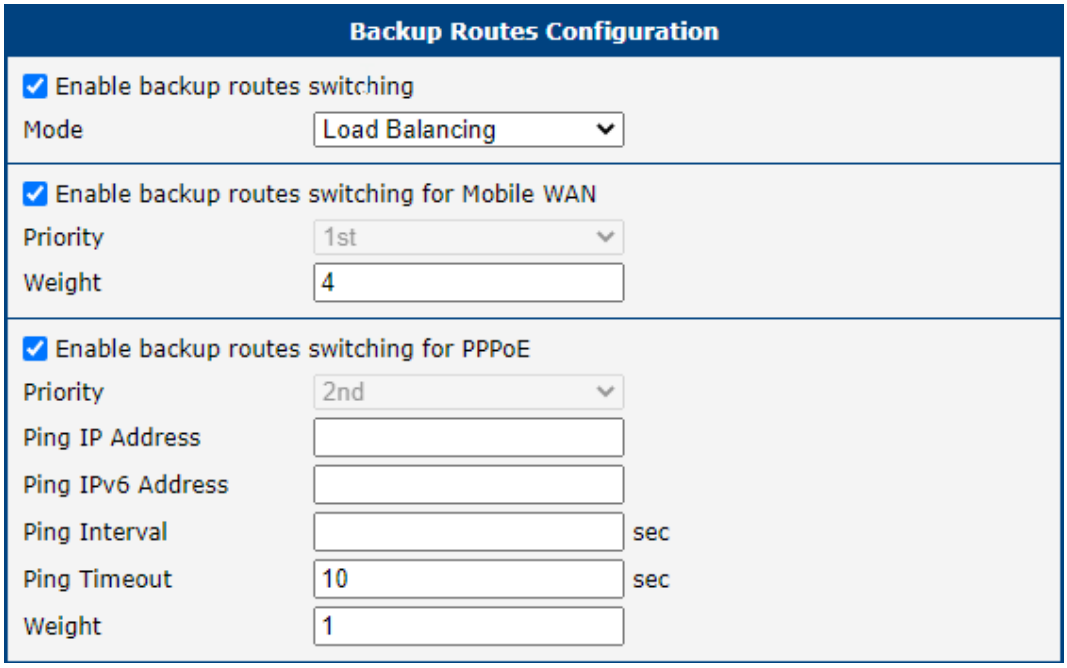


Figure 35: Example #4: GUI Configuration

Figure 36 illustrates the example topology.

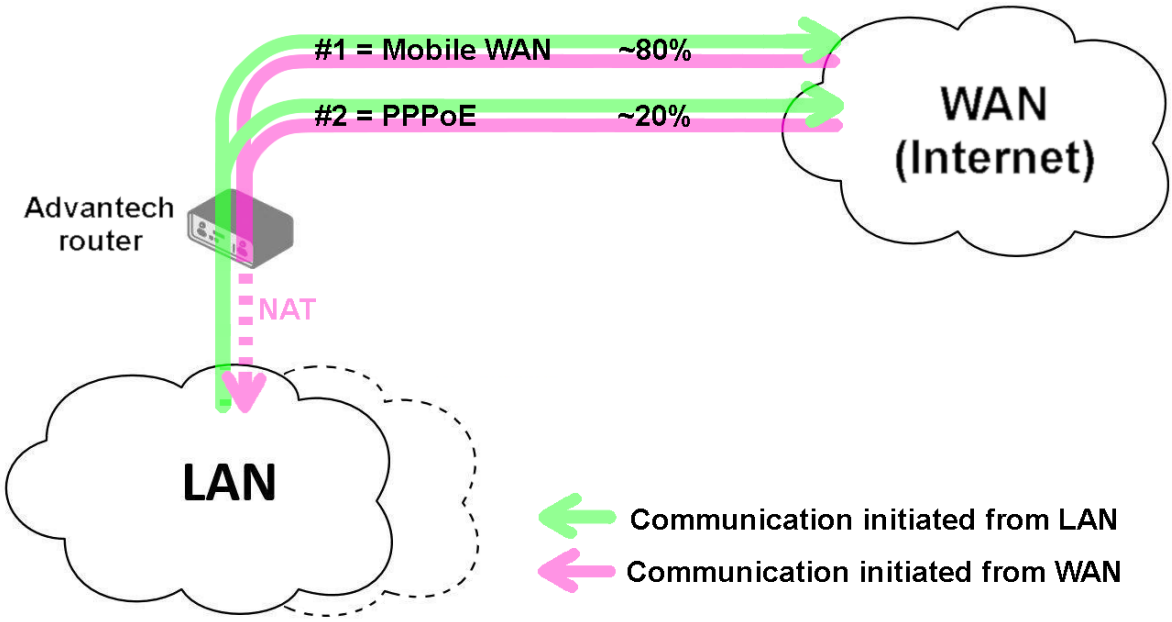


Figure 36: Example #4: Topology

Example #5: No WAN Routes

This example illustrates when *Router Backup* is enabled but no specific interface is selected for the WAN route. In this case, the router has no dedicated WAN interface and routes the traffic within the LANs. Figure 37 shows the GUI configuration.

Note: The Mobile WAN interface is not accessible, even if configured and connected to a cellular network.

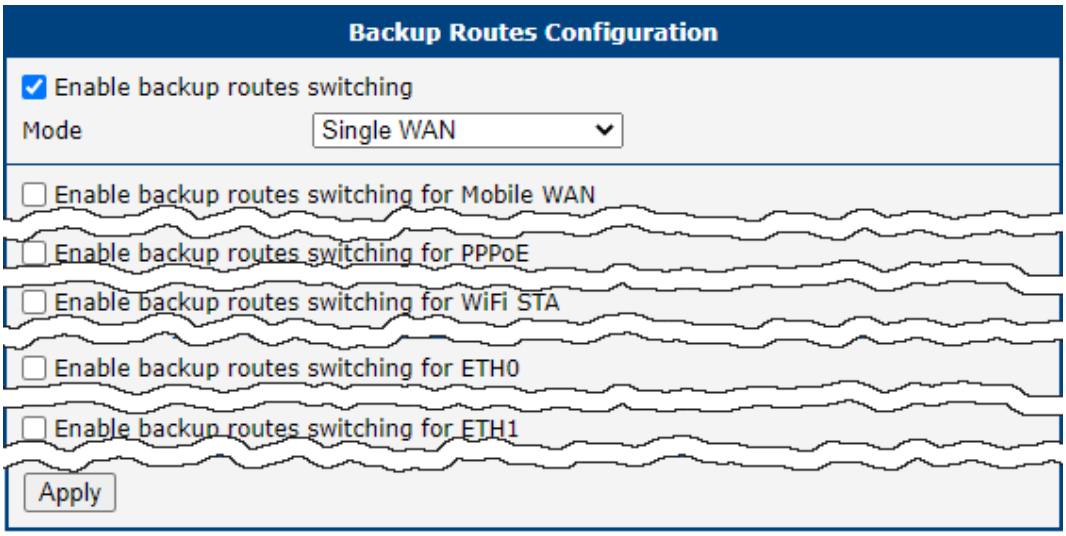


Figure 37: Example #5: GUI Configuration

Figure 38 illustrates the example topology.

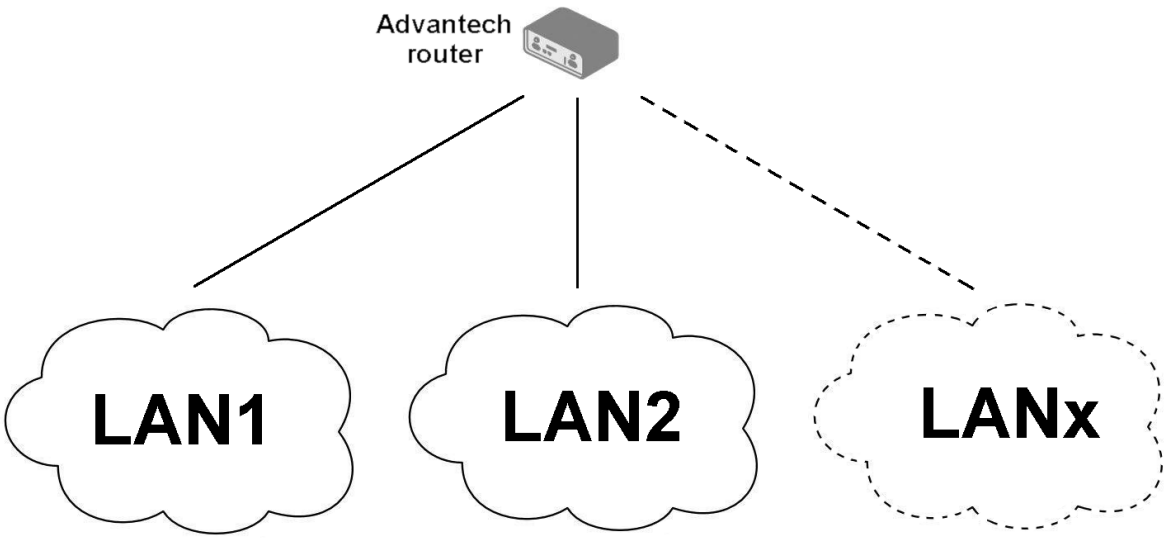


Figure 38: Example #5: Topology

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 39.

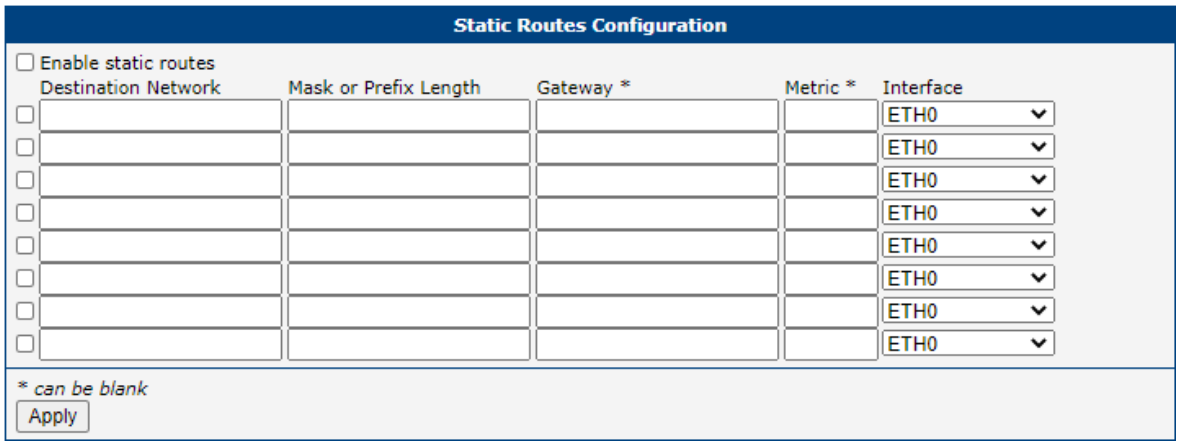


Figure 39: Static Routes Configuration

The description of all items is listed in Table 29.

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

Table 29: Static Routes Configuration

4.9 Firewall Configuration

The first section of the configuration form specifies the incoming firewall policy. If the *Enable filtering of incoming packets* check box is unchecked, all incoming packets are accepted. If checked, and a packet comes from the WAN interface, then the router forwards this packet to the INPUT iptable chain. When the INPUT chain accepts the packet, and there is a rule matching this packet with the *Action* set to *allow*, the router accepts the packet. The packet is dropped if an INPUT rule is unavailable or the *Action* is set to *deny*. You can specify the rules for IP addresses, protocols, and ports to allow or deny access to the router and internal network behind the router. It is possible to specify up to sixteen rules when each rule can be enabled/disabled by ticking the checkbox on the left of the rule row. Please note that the incoming rules are **applied to the WAN interface only**. See Chapter 4.7.1 to see the priority rules for the WAN interfaces. See Table 30 for the incoming definition table description.

Item	Description
Source	IP address from which access to the router is allowed.
Protocol	Specifies the protocol used for remote access: • **all** – Access for all protocols is active. • **TCP** – Access for the TCP protocol is active. • **UDP** – Access for the UDP protocol is active. • **GRE** – Access for the GRE protocol is active. • **ESP** – Access for the ESP protocol is active. • **ICMP** – Access for the ICMP protocol is active.
Target Port(s)	The port numbers range allowing access to the router. Enter the initial and final port numbers separated by the hyphen mark. One static port is allowed as well.
Action	Specifies the type of action the router performs: • **allow** – The router allows the packets to enter the network. • **deny** – The router denies the packets from entering the network
Description	Description of the rule.

Table 30: Filtering of Incoming Packets

The next section of the configuration form specifies the forwarding firewall policy. If the *Enabled filtering of forwarded packets* check box is unchecked, all incoming packets are accepted. If checked, and a packet is addressed to another network interface, then the router forwards this packet to the FORWARD iptable chain. When the FORWARD chain accepts the packet, and there is a rule for forwarding it, the router forwards the packet. If a forwarding rule

is unavailable, then the packet is dropped. It is possible to specify up to sixteen rules when each rule can be enabled/disabled by ticking the checkbox on the left of the rule row. The forwarding setting is applied to all interfaces, regardless of whether it is the WAN interface. The 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 specifying only the protocol or to create stricter rules by specifying values for source IP addresses, destination IP addresses, and ports. See Table 31 for the forwarding definition table description.

Item	Description
Source	IP address from which access to the router is allowed.
Destination	IP address of destination device.
Protocol	Specifies the protocol used for remote access: • **all** – Access for all protocols is active. • **TCP** – Access for the TCP protocol is active. • **UDP** – Access for the UDP protocol is active. • **GRE** – Access for the GRE protocol is active. • **ESP** – Access for the ESP protocol is active. • **ICMP** – Access for the ICMP protocol is active.
Target Port(s)	The target port numbers. Enter the initial and final port numbers separated by the hyphen mark. One static port is allowed as well.
Action	Specifies the type of action the router performs: • **allow** – The router allows the packets to enter the network. • **deny** – The router denies the packets from entering the network.
Description	Description of the rule.

Table 31: Forwarding filtering

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

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

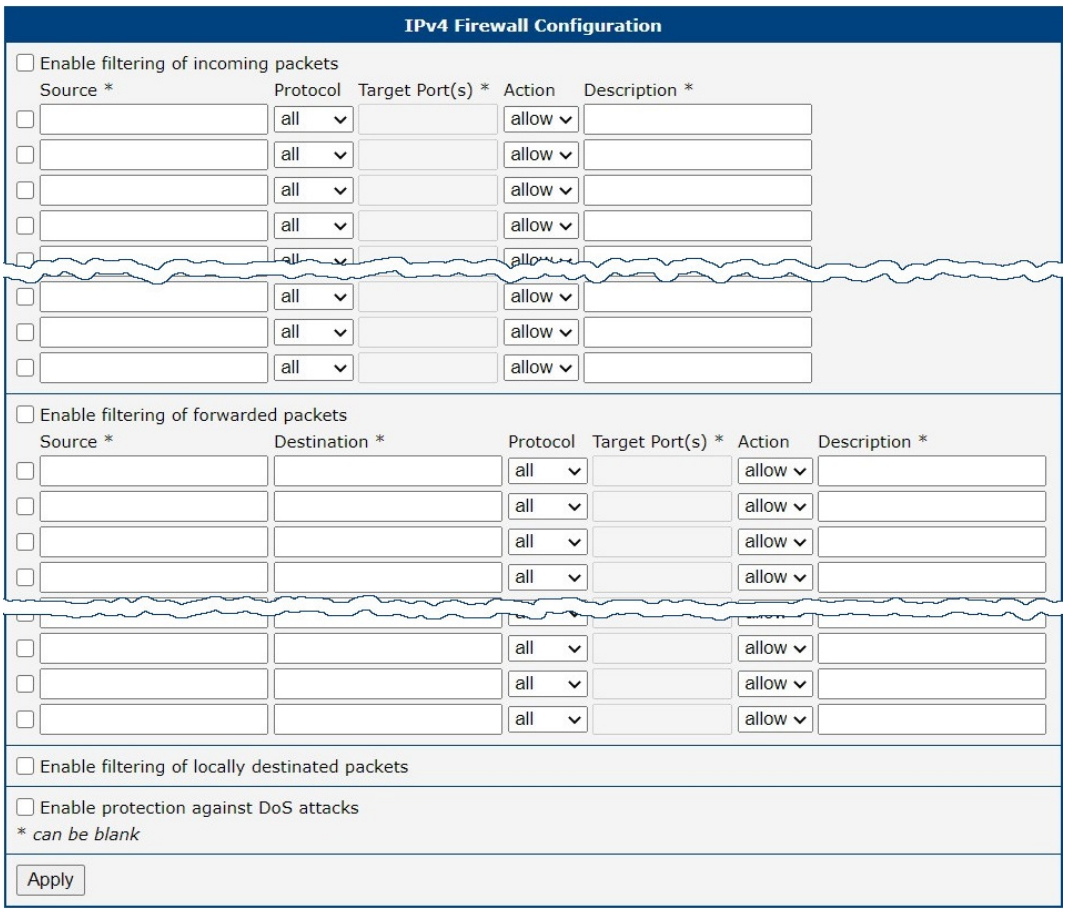


Figure 40: Firewall Configuration

Example of the firewall configuration:

The router allows the following access:

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

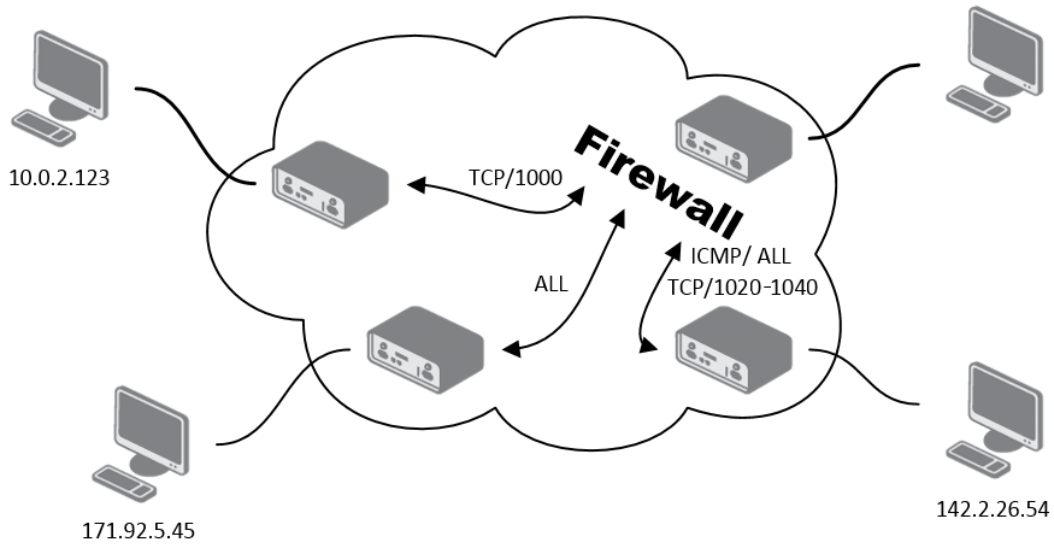


Figure 41: Topology for the Firewall Configuration Example

Firewall Configuration

☑ Enable filtering of incoming packets

	Source *	Protocol	Target Port(s) *	Action	Description *
☑	171.92.5.45	all		allow	
☑	10.0.2.123	TCP	1000	allow	
☑	142.2.26.54	ICMP		allow	
☑	142.2.26.54	TCP	1020-1040	allow	
☐		all		allow	
☐		all		allow	
☐		all		allow	
☐		all		allow	

Figure 42: Firewall Configuration Example

4.10 NAT Configuration

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

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

Table 32: NAT Configuration

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

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

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

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

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

Table 33: Configuration of send all incoming packets

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

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

Table 34: Remote Access Configuration

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

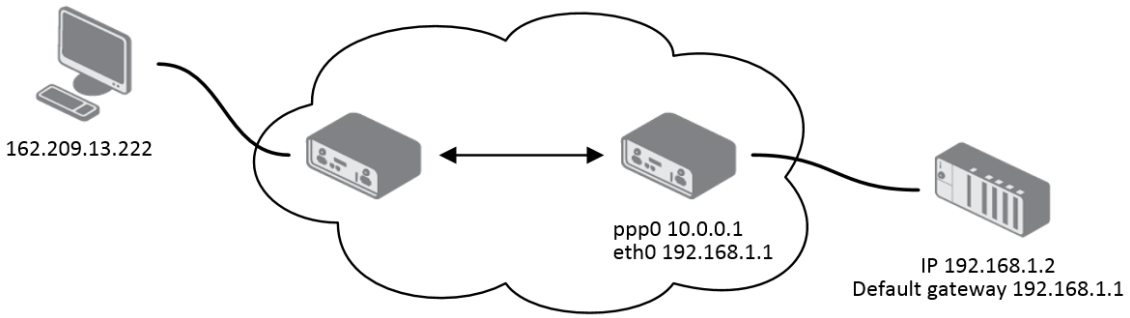


Figure 43: Example 1 – Topology of NAT Configuration

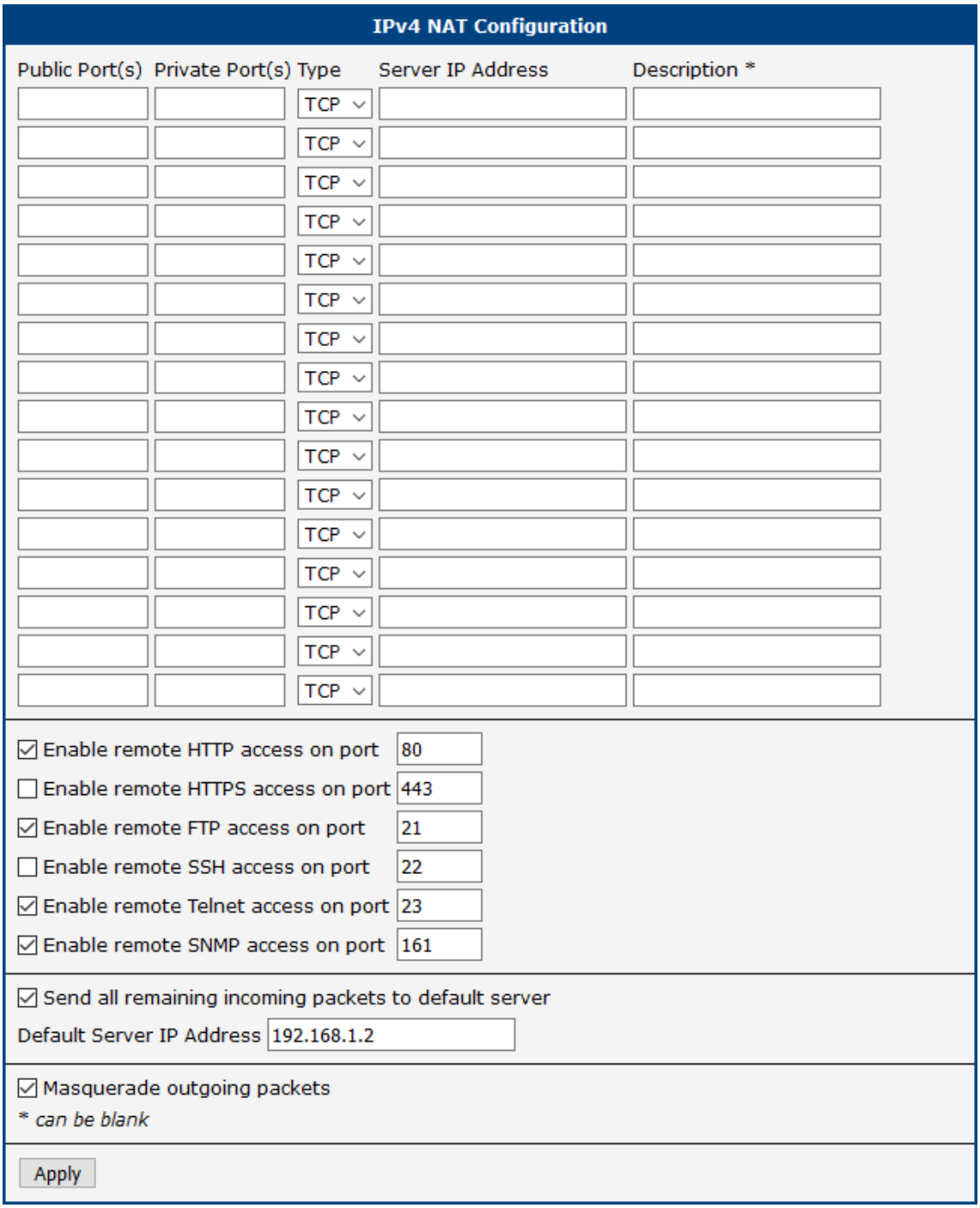


Figure 44: Example 1 – NAT Configuration

It is important to mark the *Send all remaining incoming packets to default server* check box for this configuration. The IP address in this example is the address of the device behind the router. The default gateway of the devices in the subnetwork connected to router is the same

IP address as displayed in the *Default Server IP Address* field. The connected device replies if a PING is sent to the IP address of the SIM card.

Example 2: Configuration with more equipment connected.

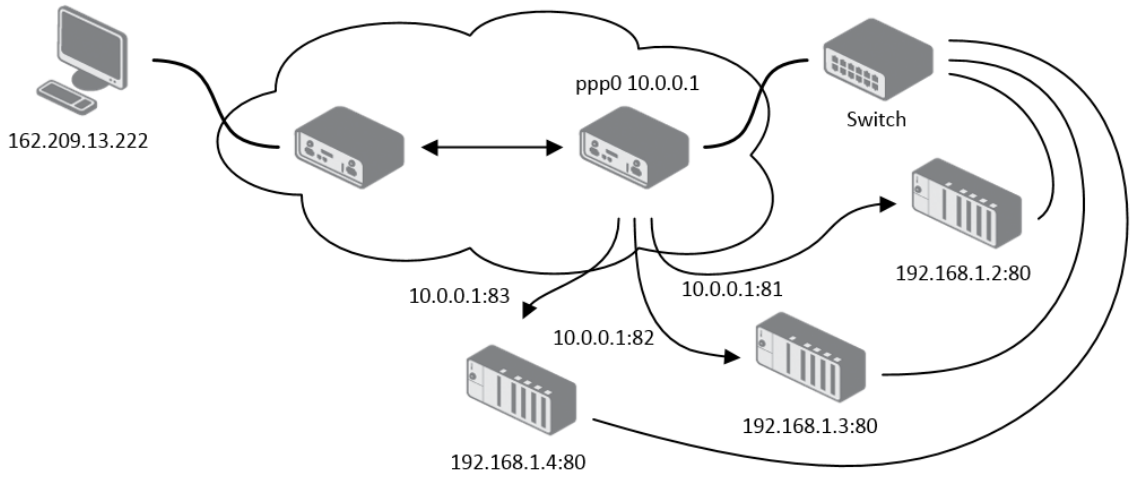


Figure 45: Example 2 – Topology of NAT Configuration

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

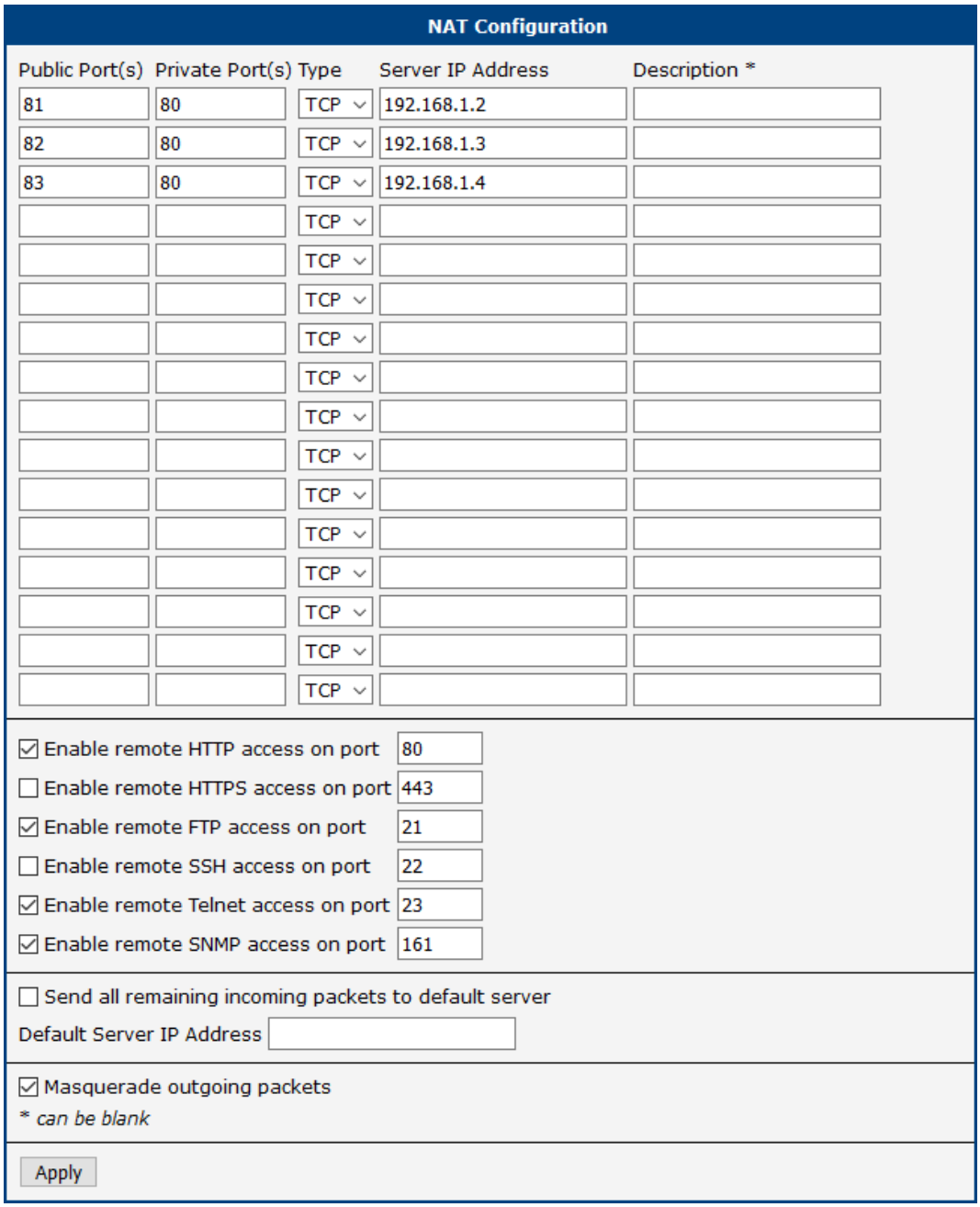


Figure 46: Example 2 – NAT Configuration

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.

Item	Description
Description	Specifies the description or name of tunnel.
Interface Type	TAP is basically at the Ethernet level (layer 2) and acts as a switch, whereas TUN works at the network level (layer 3) and routes packets on the VPN. TAP is bridging, whereas TUN is routing. • **TUN** – Choose the TUN mode. • **TAP** – Choose the TAP mode, but remember first to **configure the bridge** on the ethernet interface.
Protocol	Specifies the communication protocol. • **UDP** – The OpenVPN communicates using UDP. • **TCP server** – The OpenVPN communicates using TCP in server mode. • **TCP client** – The OpenVPN communicates using TCP in client mode.
UDP/TCP port	Specifies the port of the relevant protocol (UDP or TCP).
1st Remote IP Address	Specifies the first IPv4, IPv6 address or domain name of the opposite side of the tunnel.
2nd Remote IP Address	Specifies the second IPv4, IPv6 address or domain name of the opposite side of the tunnel.
Remote Subnet	Specifies the IP address of a network behind opposite side of the tunnel.
Remote Subnet Mask	Specifies the subnet mask of a network behind opposite side of the tunnel.
Redirect Gateway	Adds (rewrites) the default gateway. All the packets are then sent to this gateway via tunnel, if there is no other specified default gateway inside them.
Local Interface IP Address	Specifies the IP address of a local interface.

Continued on next page

Continued from previous page

Item	Description
Remote Interface IP Address	Specifies the IP address of the interface of opposite side of the tunnel.
Ping Interval	Specifies the time interval after which the router sends a message to opposite side of tunnel to verify the existence of the tunnel.
Ping Timeout	Specifies the time interval during which the router waits for a message sent by the opposite side. For proper verification of the OpenVPN tunnel, set the *Ping Timeout* to greater than the *Ping Interval*.
Renegotiate Interval	Specifies the renegotiate period (reauthorization) of the OpenVPN tunnel. You can only set this parameter when the *Authenticate Mode* is set to *username/password* or *X.509 certificate*. After this time period, the router changes the tunnel encryption to help provide the continues safety of the tunnel.
Max Fragment Size	Maximum size of a sent packet.
Compression	Compression of the data sent: • **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: • **not applied** – NAT rules are not applied to the OpenVPN tunnel. • **applied** – NAT rules are applied to the OpenVPN tunnel.

Continued on next page

Continued from previous page

Item	Description
Authenticate Mode	Specifies the authentication mode: • **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.
Security Mode	Choose the security mode, *tls-auth* or *tls-crypt*. We recommend to use the *tls-crypt* mode for the security reasons. In this mode, all the data is encrypted with a pre-shared key. Moreover, this mode is more robust against the TLS denial of service attacks.
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.
Local Passphrase	Passphrase used during private key generation.
Username	Specifies a login name which you can use for authentication in the username/password mode.
Password	Specifies a password which you can use for authentication in the username/password mode. Enter valid characters only.

Continued on next page

Continued from previous page

Item	Description
User's Up Script[1]	Custom script, executed when the OpenVPN tunnel is established.
User's Down Script[1]	Custom script, executed when the OpenVPN tunnel is closed.
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 `openvpnd --help` command.

Table 35: 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.

[1] Parameters passed to the script are `cmd tun_dev tun_mtu link_mtu ifconfig_local_ip ifconfig_remote_ip [ init | restart ]`, see Reference manual for OpenVPN, option `-up cmd`.

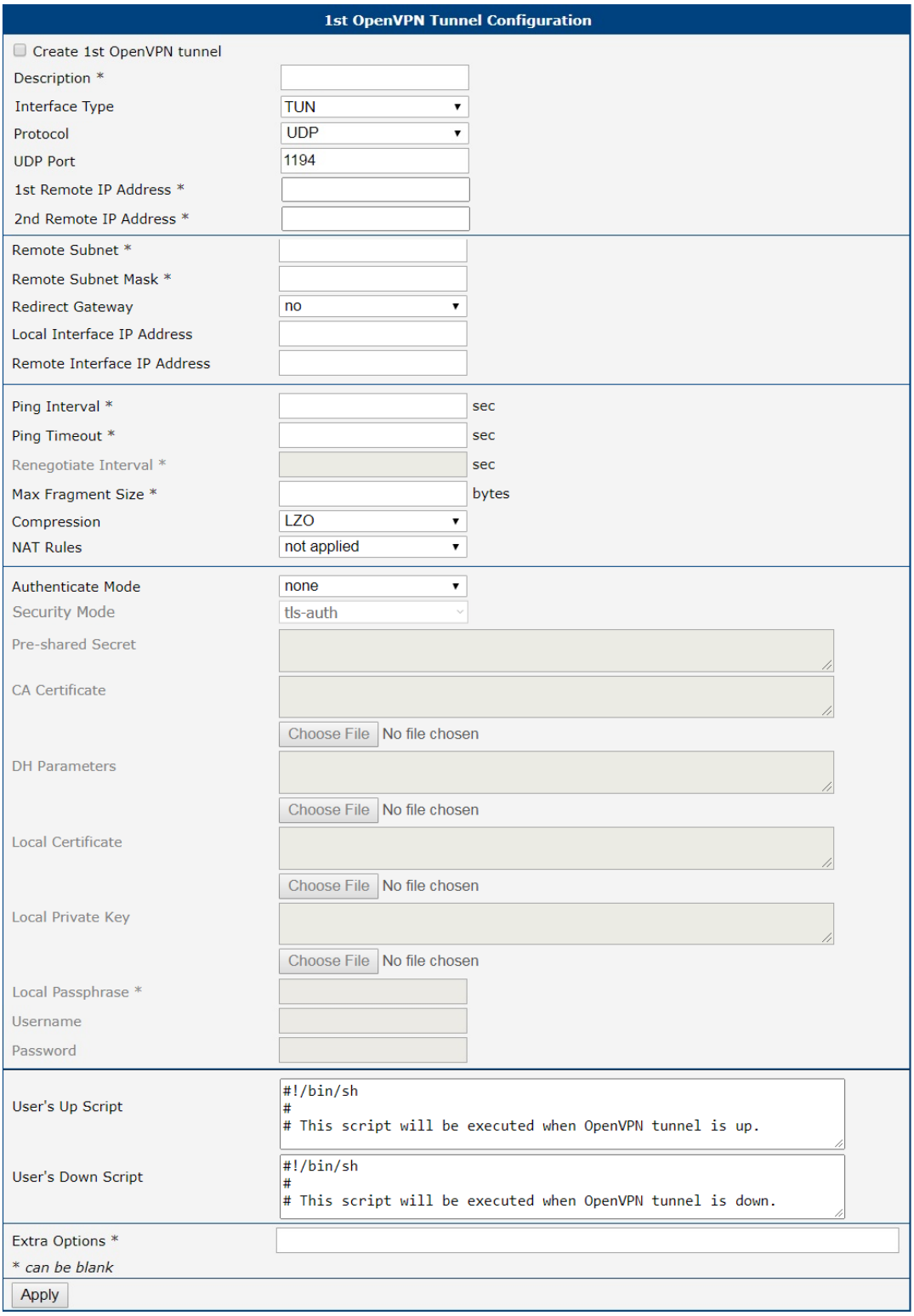


Figure 47: OpenVPN tunnel configuration

Example of the OpenVPN tunnel configuration:

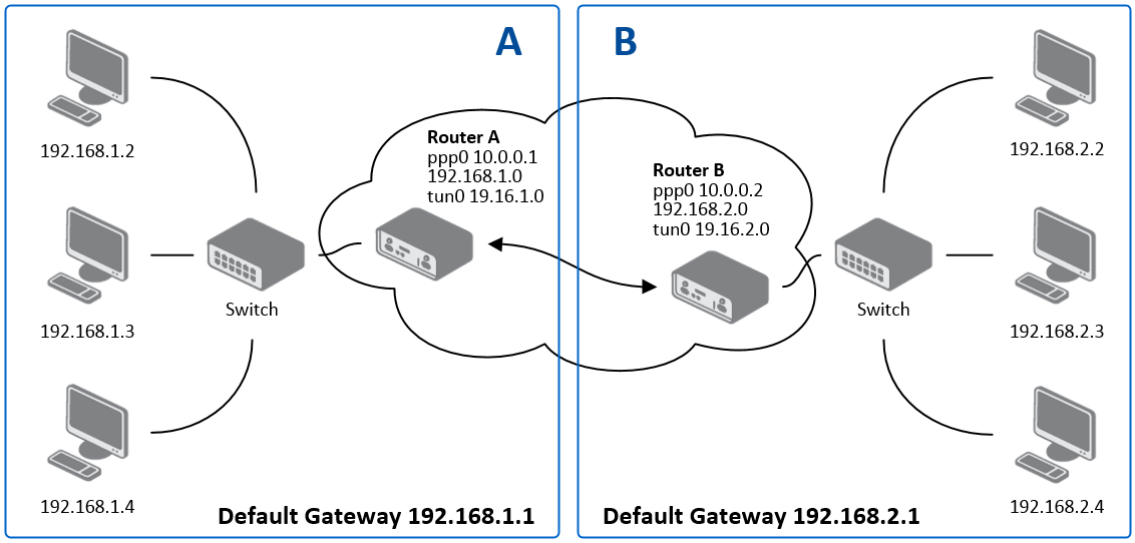


Figure 48: Topology of OpenVPN Configuration Example

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	19.16.1.0
Compression	LZO	LZO
Authenticate mode	none	none

Table 36: 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

The IPsec tunnel function allows you to create a secured connection between two separate LAN networks. Advantech routers allows you to create **up to four IPsec tunnels**.

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*. Supported are both, **policy-based** and **route-based** VPN approaches, see the different configuration scenarios in Chapter 4.12.1.

For different IPsec authentication scenarios, see Chapter 4.12.2.

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 an secure setup, we recommend to follow instructions on the Security Recommendations *strongSwan* web page.

Detailed information and more examples of IPsec tunnel configuration and authentication can be found in the application note IPsec Tunnel [5].

FRRouting (FRR) user module is an Internet routing protocol suite for Advantech routers. This UM includes protocol daemons for BGP, IS-IS, LDP, OSPF, PIM, and RIP.

4.12.1 Route-based Configuration Scenarios

There are more different route-based configuration options which can be configured and used in routers. Below are listed the most common cases which can be used (for more details see Route-based VPNs *strongSwan* web page):

1. **Enabled Installing Routes**
   - Remote (local) subnets are used as traffic selectors (routes).
   - It results to the same outcome as a policy-based VPN.
   - One benefit of this approach is the possibility to verify non-encrypted traffic passed through an IPsec tunnel number X by tcdump tool: `tcpdump -i ipsecX`.
   - Set up the *Install Routes* to *yes* option.
2. **Static Routes**
   - Routes are installed statically by an application as soon as the IPsec tunnel is up.
   - As an application for static routes installation can be used for example FRR/STATICD application.
   - Set up the *Install Routes* to *no* option.

3. **Dynamic Routing**
   • Routes are installed dynamically while running by an application using a dynamic protocol.
   • As an application for dynamic routes installation can be used for example FRR/BGP or FRR/OSPF application. This application gains the routes dynamically from an (BGP, OSPF) server.
   • Set up the *Install Routes* to *no* option.

4. **Multiple Clients**
   • Allows to create VPN network with multiple clients. One router acts as the server and assigns IP address to all the clients on the network.
   • The server has *Remote Virtual Network* and *Remote Virtual Mask* items configured and the client has *Local Virtual Address* item configured.
   • Set up the *Install Routes* to *yes* option.

4.12.2 IPsec Authentication Scenarios

There are four basic authentication options which can be configured and used in routers:

1. **Pre-shared Key**
   • Set *Authenticate Mode* to *pre-shared key* option.
   • Enter the shared key to the *Pre-shared key* field.

2. **Public Key**
   • Set *Authenticate Mode* to *X.509 certificate* option.
   • Enter the public key to the *Local Certificate / PubKey* field.
   • CA certificate is not required.

3. **Peer Certificate**
   • Set *Authenticate Mode* to *X.509 certificate* option.
   • Enter the remote key to the *Remote Certificate / PubKey* field. Users with this certificate will be allowed.
   • CA certificate is not required.

4. **CA Certificate**
   • Set *Authenticate Mode* to *X.509 certificate* option.
   • Enter the CA certificate or a list of CA certificates to the *CA Certificate* field. Any certificate signed by the CA will be accepted.
   • Remote certificate is not required.

Notes:

- The Peer and CA Certificate (options 3 and 4) can be configured and used simultaneously – authentication can be done by one of this method.
- The Local ID is significant. When using certificate authentication, the IKE identity must be contained in the certificate, either as subject or as `subjectAltName`.

4.12.3 Configuration Items Description

The configuration GUI for IPsec is shown in Figure 49 and the description of all items, which can be configured for an IPsec tunnel, are described in Table 37.

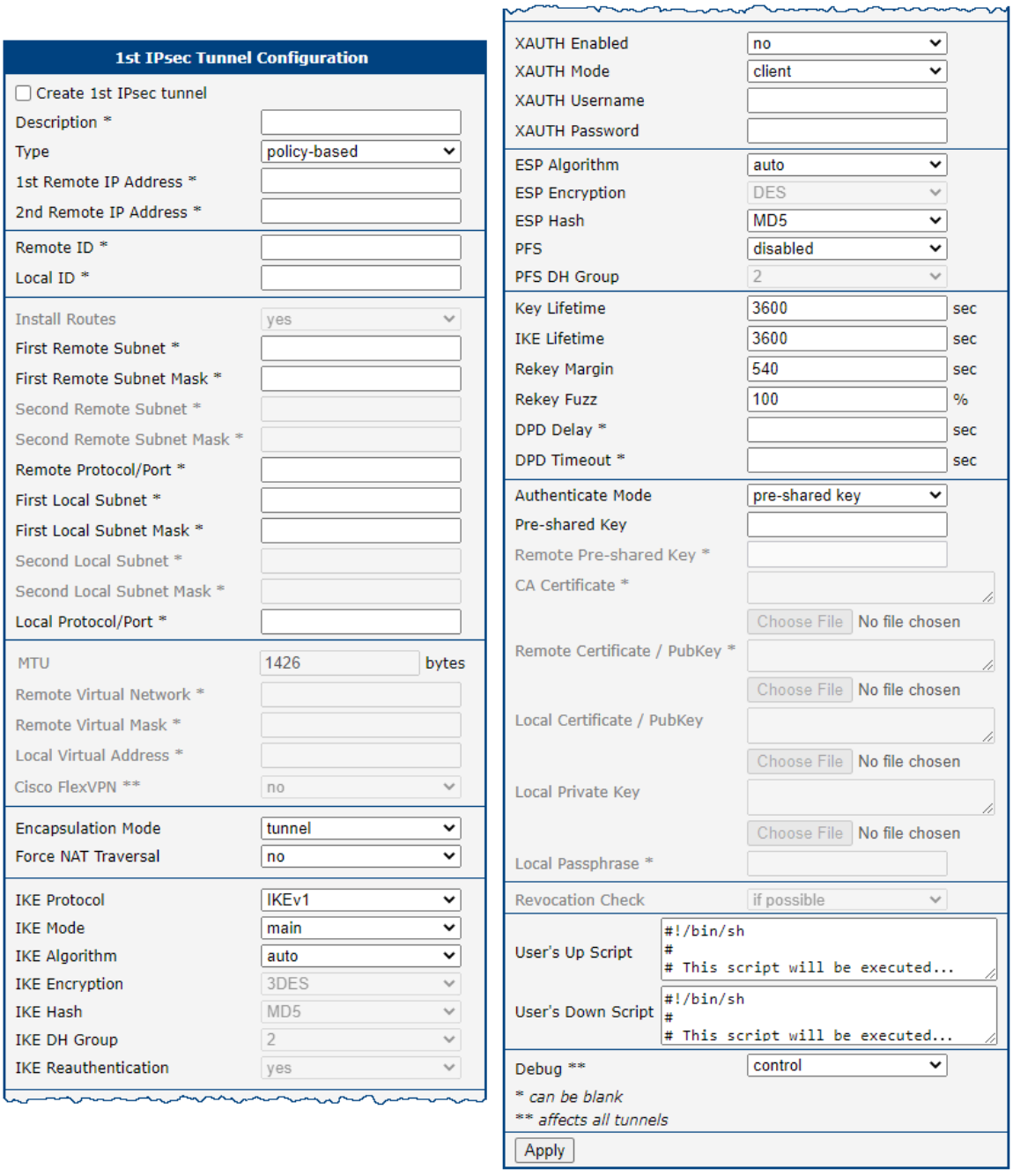


Figure 49: IPsec Tunnels Configuration

Item	Description
Description	Name or description of the tunnel.
Type	• **policy-based** – Choose for the policy-based VPN approach. • **route-based** – Choose for the route-based VPN approach. Note: Data throughput via route-based VPN is slightly lower in comparison with policy-based VPN.
1st Remote IP Address	First IPv4, IPv6 address or domain name of the remote side of the tunnel, based on selected *Host IP Mode* above.
2nd Remote IP Address	Second IPv4, IPv6 address or domain name of the remote side of the tunnel, based on selected *Host IP Mode* above.
Remote ID	Identifier (ID) of remote side of the tunnel. It consists of two parts: a *hostname* and a *domain-name*.
Local ID	Identifier (ID) of local side of the tunnel. It consists of two parts: a *hostname* and a *domain-name*.
Install Routers	For route-based type only. Choose **yes** to use traffic selectors as route(s).
First Remote Subnet	IP address of a network behind remote side of the tunnel, based on *Tunnel IP Mode* above.
First Remote Subnet Mask/Prefix	IP subnet mask of a network behind remote side of the tunnel, or IPv6 prefix (single number 0 to 128).
Second Remote Subnet	IP address of the second network behind remote side of the tunnel, based on *Tunnel IP Mode* above. For *IKE Protocol* = IKEv2 only.
Second Remote Subnet Mask/Prefix	IP subnet mask of the second network behind remote side of the tunnel, or IPv6 prefix (single number 0 to 128). For *IKE Protocol* = IKEv2 only.
Remote Protocol/Port	Specifies Protocol/Port of remote side of the tunnel. The general form is *protocol*/*port*, 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.
First Local Subnet	IP address of a local network, based on *Tunnel IP Mode* above.
First Local Subnet Mask/Prefix	IP subnet mask of a local network, or IPv6 prefix (single number 0 to 128).
Second Local Subnet	IP address of the second local network, based on *Tunnel IP Mode* above. For *IKE Protocol* = IKEv2 only.
Second Local Subnet Mask/Prefix	IP subnet mask of the second local network, or IPv6 prefix (single number 0 to 128). For *IKE Protocol* = IKEv2 only.
Local Protocol/Port	Specifies Protocol/Port of a local network. The general form is *protocol*/*port*, 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.

Continued on next page

Continued from previous page

Item	Description
MTU	Maximum Transmission Unit value (for route-based mode only). Default value is 1426 bytes.
Remote Virtual Network	Specifies virtual remote network for server (responder).
Remote Virtual Mask	Specifies virtual remote network mask for server (responder).
Local Virtual Address	Specifies virtual local network address for client. To get address from server set up the address to 0.0.0.0.
Cisco FlexVPN	Enable to support the Cisco FlexVPN functionality. The *route-based* type must be chossen. For more information, see strongswan.conf page.
Encapsulation Mode	Specifies the IPsec mode, according to the method of encapsulation. • **tunnel** – entire IP datagram is encapsulated. • **transport** – only IP header is encapsulated. Not supported by route-based VPN. • **beet** – the ESP packet is formatted as a transport mode packet, but the semantics of the connection are the same as for tunnel mode.
Force NAT Traversal	Enable NAT traversal enforcement (UDP encapsulation of ESP packets).
IKE Protocol	Specifies the version of IKE (**IKEv1**/**IKEv2**, **IKEv1** or **IKEv2**).
IKE Mode	Specifies the mode for establishing a connection (*main* or *aggressive*). If you select the aggressive mode, then the router establishes the IPsec tunnel faster, but the encryption is permanently set to 3DES-MD5. **We recommend that you not use the *aggressive* mode due to lower security!**
IKE Algorithm	Specifies the means by which the router selects the algorithm: • **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**, **SHA384** 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.

Continued on next page

Continued from previous page

Item	Description
IKE Reauthentication	Enable or disable IKE reauthentication (for 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: • **auto** – The encryption and hash algorithm are selected automatically. • **manual** – The encryption and hash algorithm are defined by the user.
ESP Encryption	Encryption algorithm – **3DES**, **AES128**, **AES192**, **AES256**, **AES128GCM128**, **AES192GCM128**, **AES256GCM128**.
ESP Hash	Hash algorithm – **MD5**, **SHA1**, **SHA256**, **SHA384** 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 *IKE DH Group*).
Key Lifetime	Lifetime key data part of tunnel. The minimum value of this parameter is 60 s. The maximum value is 86400 s.
IKE Lifetime	Lifetime key service part of tunnel. The minimum value of this parameter is 60 s. The maximum value is 86400 s.
Rekey Margin	Specifies how long before a connection expires that the router attempts to negotiate a replacement. Specify a maximum value that is less than half of IKE and Key Lifetime parameters.
Rekey Fuzz	Percentage of time for the Rekey Margin extension.
DPD Delay	Time after which the IPsec tunnel functionality is tested.
DPD Timeout	The period during which device waits for a response.
Authenticate Mode	Specifies the means by which the router authenticates: • **Pre-shared key** – Sets the shared key for both sides of the tunnel. • **X.509 Certificate** – Allows X.509 authentication in multiclient mode.
(Local) Pre-shared Key	Specifies the shared key (local for IKEv2) for both sides of the tunnel. The prerequisite for entering a key is that you select pre-shared key as the authentication mode.

Continued on next page

Continued from previous page

Item	Description
Remote Pre-shared Key	Specifies the remote shared key (for IKEv2) 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.
Revocation Check	Certificate revocation policy: • **if possible** – Fails only if a certificate is revoked, i.e. it is explicitly known that it is bad. • **if URI defined** – Fails only if a CRL/OCSP URI is available, but certificate revocation checking fails, i.e. there should be revocation information available, but it could not be obtained. • **always** – Fails if no revocation information is available, i.e. the certificate is not known to be unrevoked.
User's Up Script[1]	Custom script, executed when the IPSec tunnel is established.
User's Down Script[1]	Custom script, executed when the IPSec tunnel is closed.
Debug	Choose the level of logging verbosity from: **silent**, **audit**, **control** (default), **control-more**, **raw**, **private** (most verbose including the private keys). See Logger Configuration in *strongSwan* web page for more details.

Table 37: IPsec Tunnel Configuration

[1] Parameters passed to the script:
for policy-based type: one parameter: *connection name*, returns e.g. `ipsec1-1`,
for route-based type: two parameters: *connection name* and *interface name*, returns e.g. `ipsec1-1` and `ipsec0`.

We recommend that you keep up 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.

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.

4.12.4 Basic IPSec Tunnel Configuration

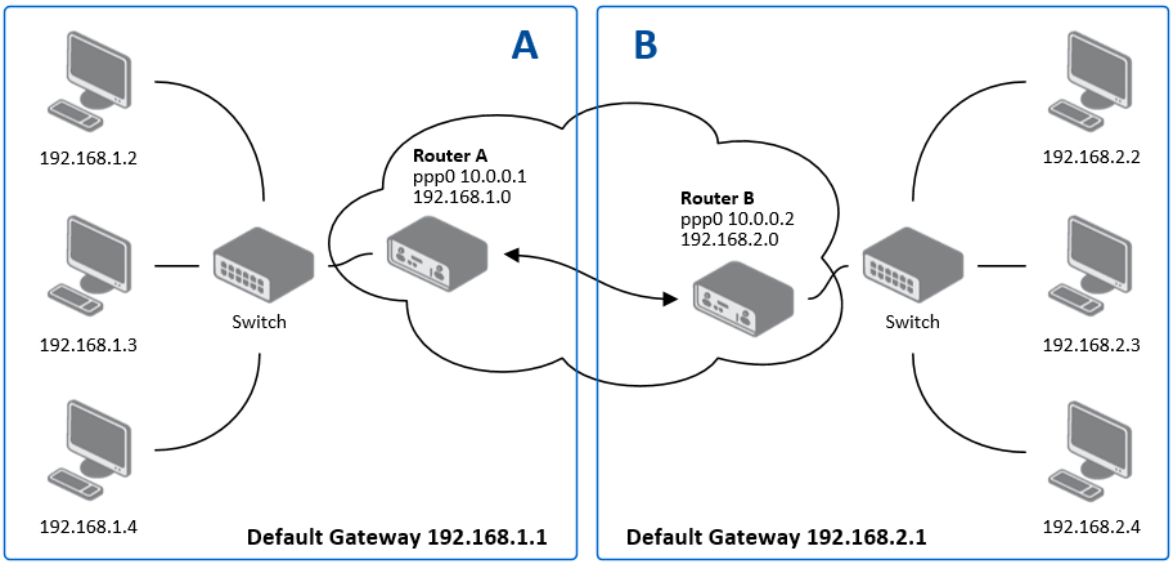


Figure 50: Topology of IPsec Configuration Example

Configuration of *Router A* and *Router B* is as follows:

Configuration	A	B
1st Remote IP Address	10.0.0.2	10.0.0.1
First Remote Subnet	192.168.2.0	192.168.1.0
First Remote Subnet Mask	255.255.255.0	255.255.255.0
First Local Subnet	192.168.1.0	192.168.2.0
First Local Subnet Mask	255.255.255.0	255.255.255.0
Authenticate mode	pre-shared key	pre-shared key
Pre-shared key	test	test

Table 38: Simple IPSec Tunnel Configuration

4.13 GRE Tunnels Configuration

GRE is an unencrypted protocol.

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

Item	Description
Description	Description of the GRE tunnel.
Remote IP Address	IP address of the remote side of the tunnel.
Local IP Address	IP address of the local 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: • **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 39: GRE Tunnel Configuration

The GRE tunnel cannot pass through the NAT.

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

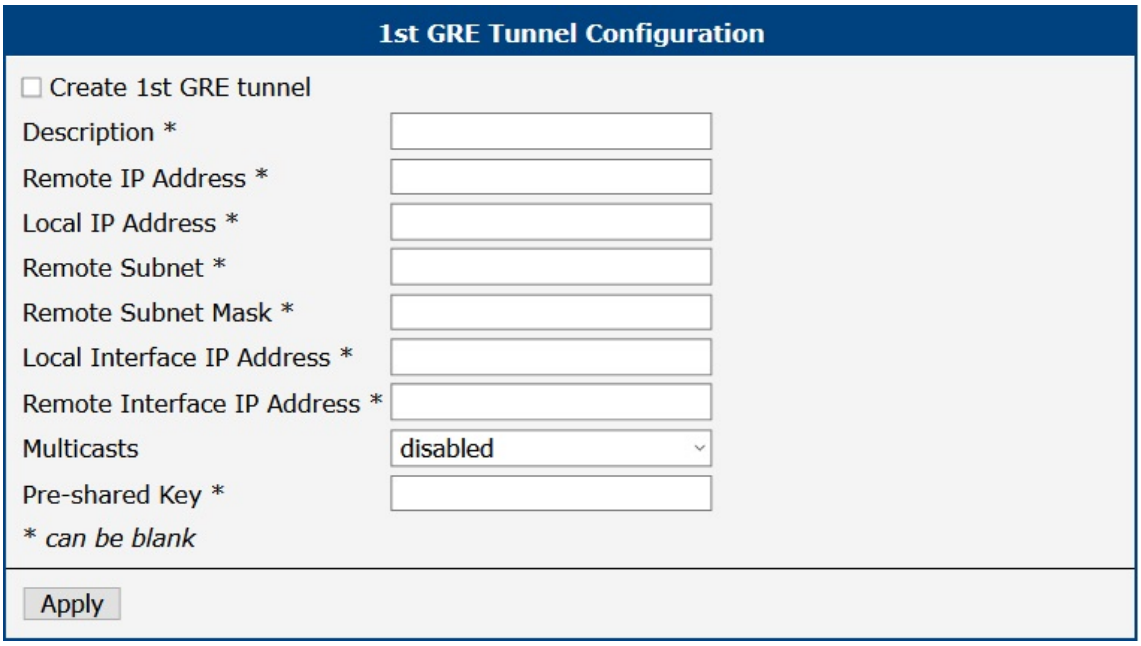


Figure 51: GRE Tunnel Configuration

4.13.1 Example of the GRE Tunnel Configuration

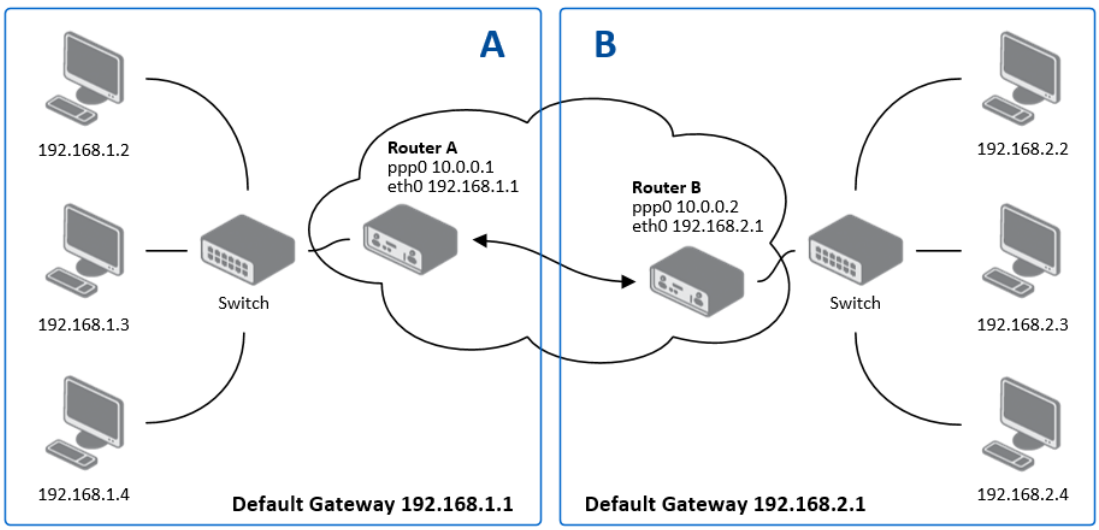


Figure 52: Topology of GRE Tunnel Configuration Example

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 40: 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.

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 two different LAN networks. Enable the *Create L2TP tunnel* checkbox to activate the tunnel.

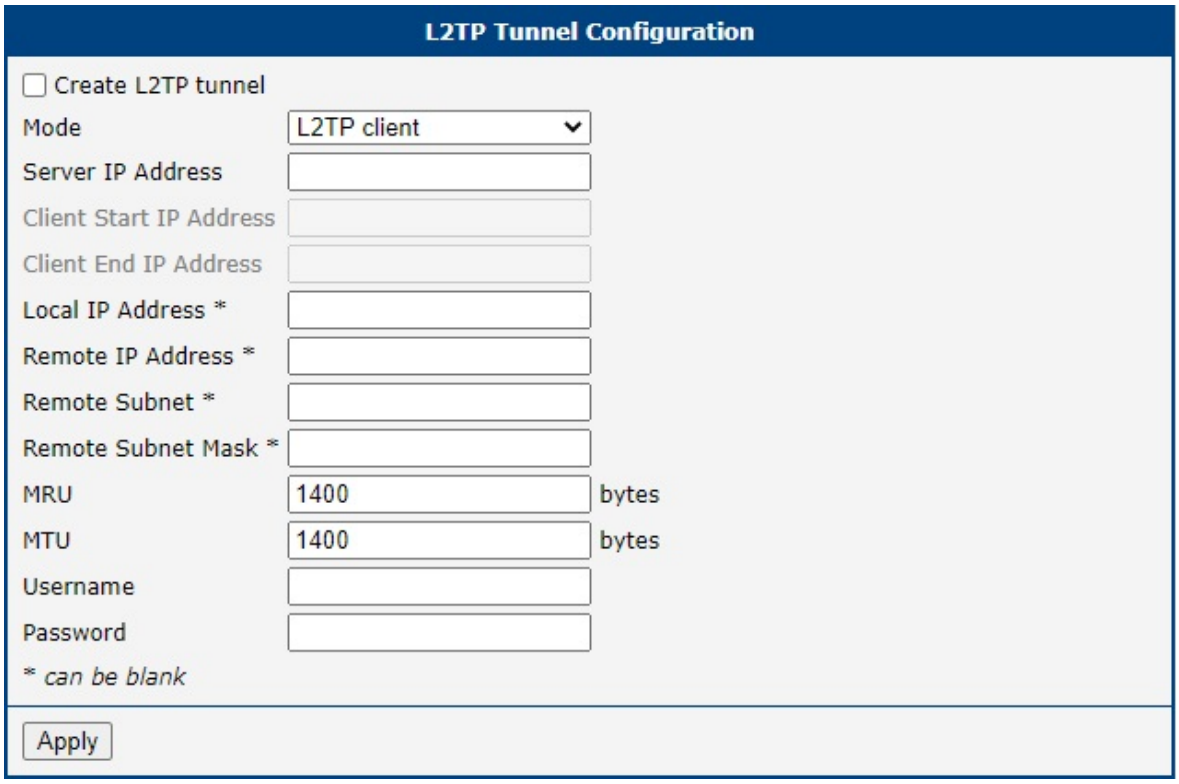


Figure 53: L2TP Tunnel Configuration

Item	Description
Mode	Specifies the L2TP tunnel mode on the router side: • **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.

Continued on next page

Continued from previous page

Item	Description
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.
MRU	Maximum Receive Unit value. Default value is 1400 bytes.
MTU	Maximum Transmission Unit value. Default value is 1400 bytes.
Username	Username for the L2TP tunnel login.
Password	Password for the L2TP tunnel login. Enter valid characters only.

Table 41: L2TP Tunnel Configuration

4.14.1 Example of the L2TP Tunnel Configuration

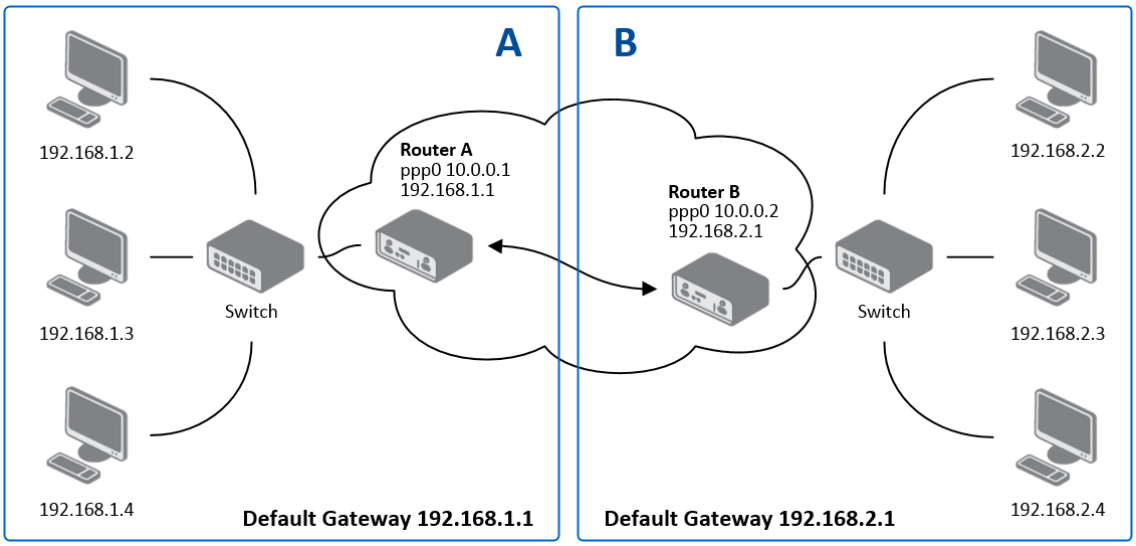


Figure 54: Topology of L2TP Tunnel Configuration Example

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 42: L2TP Tunnel Configuration Example

4.15 PPTP Tunnel Configuration

PPTP is an unencrypted protocol.

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

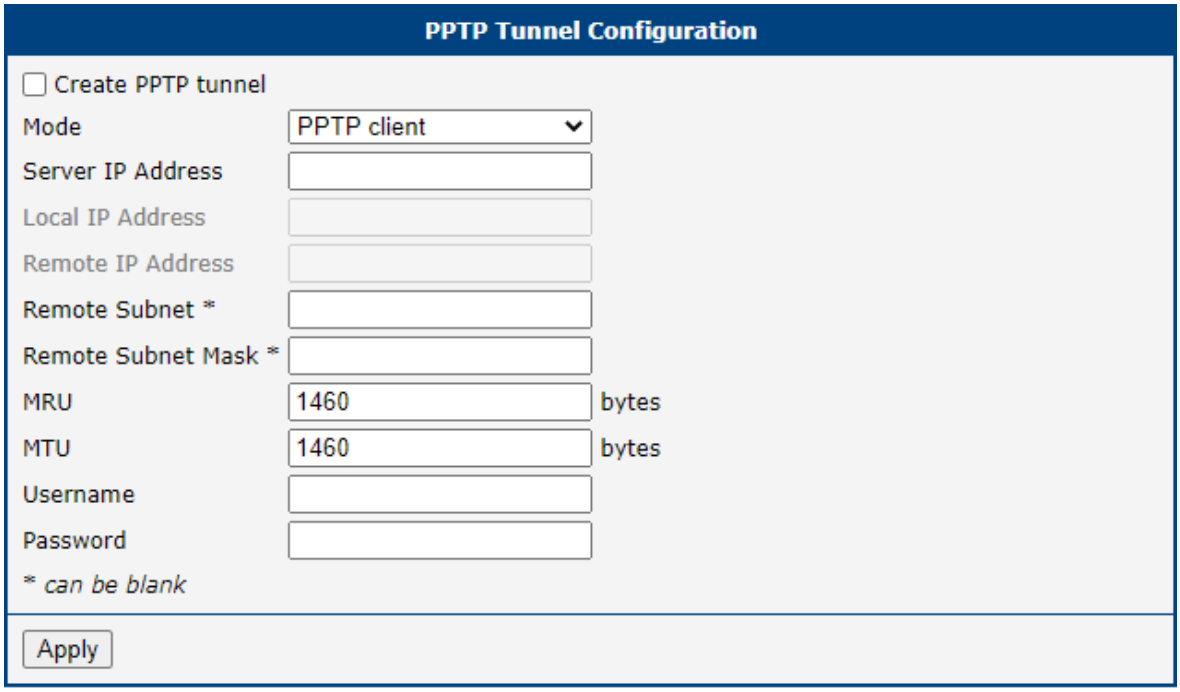


Figure 55: PPTP Tunnel Configuration

Item	Description
Mode	Specifies the L2TP tunnel mode on the router side: • **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.

Continued on next page

Continued from previous page

Item	Description
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
MRU	Maximum Receive Unit value. Default value is 1460 bytes to avoid fragmented packets.
MTU	Maximum Transmission Unit value. Default value is 1460 bytes to avoid fragmented packets.
Username	Username for the PPTP tunnel login.
Password	Password for the PPTP tunnel login. Enter valid characters only.

Table 43: PPTP Tunnel Configuration

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

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

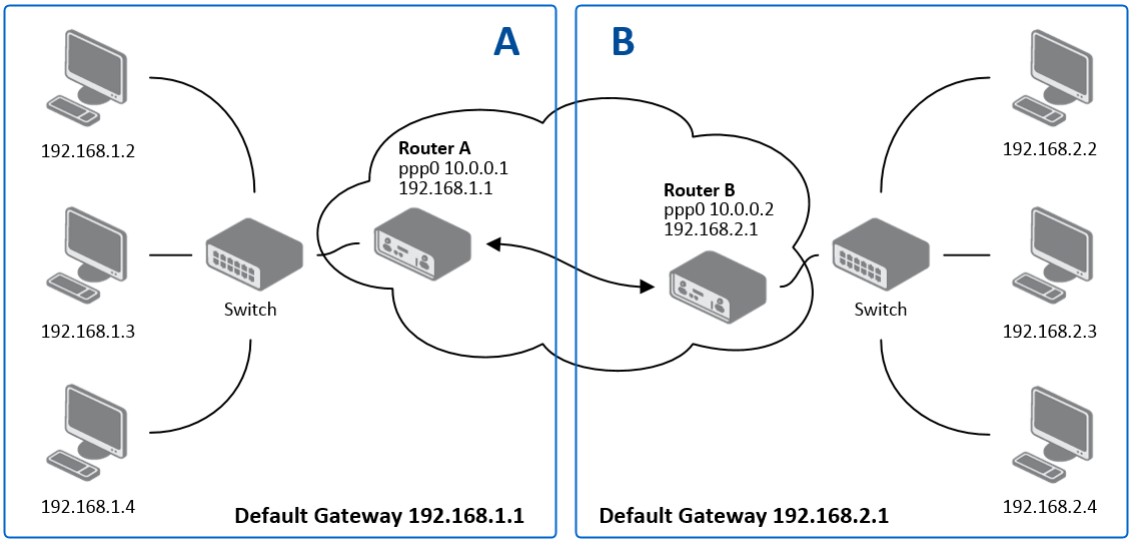


Figure 56: Topology of PPTP Tunnel Configuration Example

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 44: 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.
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 45: DynDNS Configuration

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

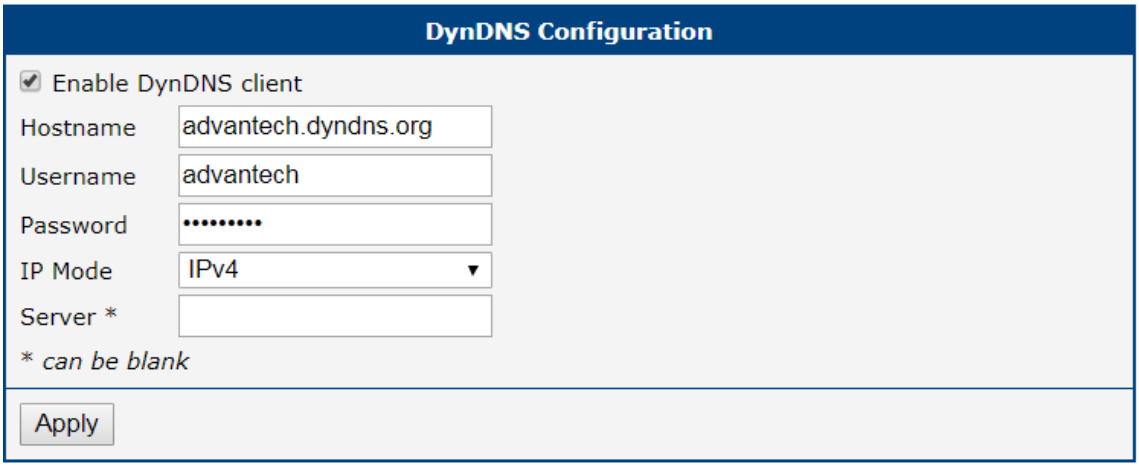


Figure 57: DynDNS Configuration Example

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.

Item	Description
Enable FTP service	Enabling of FTP server.
Maximum Sessions	Indicates how many concurrent connections shall the FTP server accept. Once the maximum is reached, additional connections will be rejected until some of the existing connections are terminated. The range is from 1 to 500.
Session Timeout	Is used to close inactive sessions. The server will terminate a FTP session after it has not been used for the given amount of seconds. The range is from 60 to 7200.

Table 46: Parameters for FTP service configuration

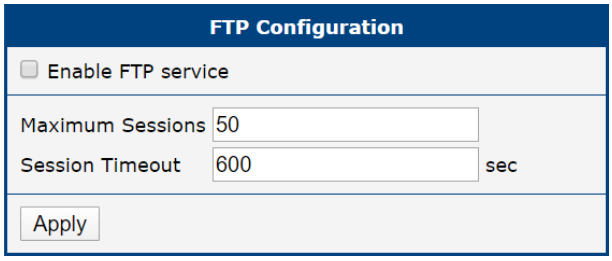


Figure 58: Configuration of FTP server

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.
Minimum TLS Version	If specified, the router will disable TLS versions lower than the specified minimum. For better security choose the highest version of TLS protocol, unless you need to use an older web browser.
Session Timeout	Inactivity timeout when the session is closed.
Login Banner	The text specified in this field will be displayed on the login page just above the credentials fields.
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 47: Parameters for HTTP and HTTPS services configuration

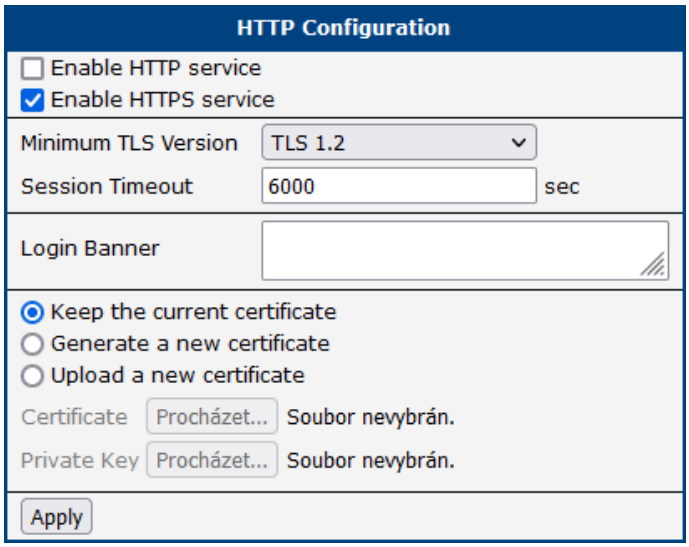


Figure 59: Configuration of HTTP and HTTPS services

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.

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

Item	Description
Primary NTP Server Address	IP or domain address of primary NTP server.
Secondary NTP Server Address	IP or domain address of secondary NTP server.
Timezone	Specifies the time zone where you installed the router.
Daylight Saving Time	Activates/deactivates the DST shift. • **No** – The time shift is inactive. • **Yes** – The time shift is active.

Table 48: 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.

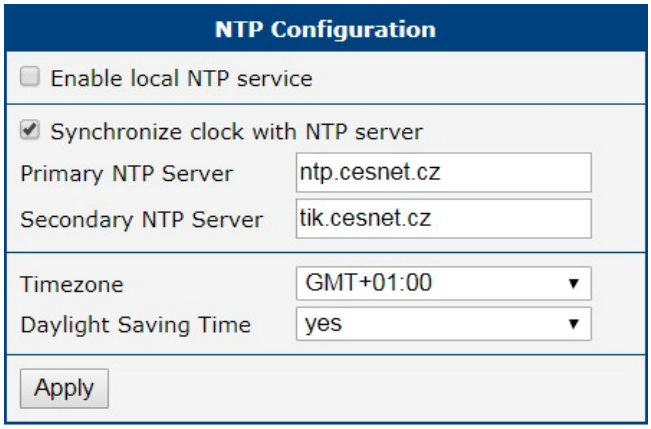


Figure 60: Example of NTP Configuration

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. As the first option, choose the *PAM Mode*.

PAM Modes

The PAM modes available and their description are listed in Table 49.

Item	Description
PAM Mode	• **local user database** – Authenticate against the local user database only, see Chapter 5.1. • **RADIUS with fallback** – Authenticate against the RADIUS server first 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! • **TACACS+ with fallback** – Authenticate against the TACACS+ server first and then against the local database in case the TACACS+ server is not accessible. • **TACACS+ only** – Authenticate only against the TACACS+ server. Note that you will not be able to authenticate to the router in case the TACACS+ server is not accessible!

Table 49: Available Modes of PAM

Local User Database

To configure the authentication against the local user database, choose local user database and enable the debug mode eventually, see Figure 61.

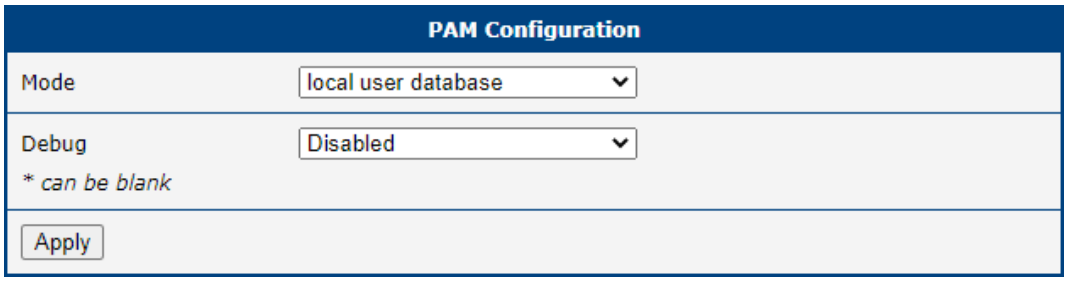


Figure 61: Configuration of Local User Database

RADIUS Mode

When authenticate against the RADIUS server, user with the same name must exist locally. It can be created manually (see Chapter 5.1) or can be created automatically based on data from RADIUS server, if the *Take Over Server Users* option is enabled as described hereunder.

To configure the authentication against a RADIUS server, choose *RADIUS with fallback* or *RADIUS only* as the *PAM mode* and set up all required items, see Figure 62. Table 50 describes all the configuration options for the RADIUS PAM modes.

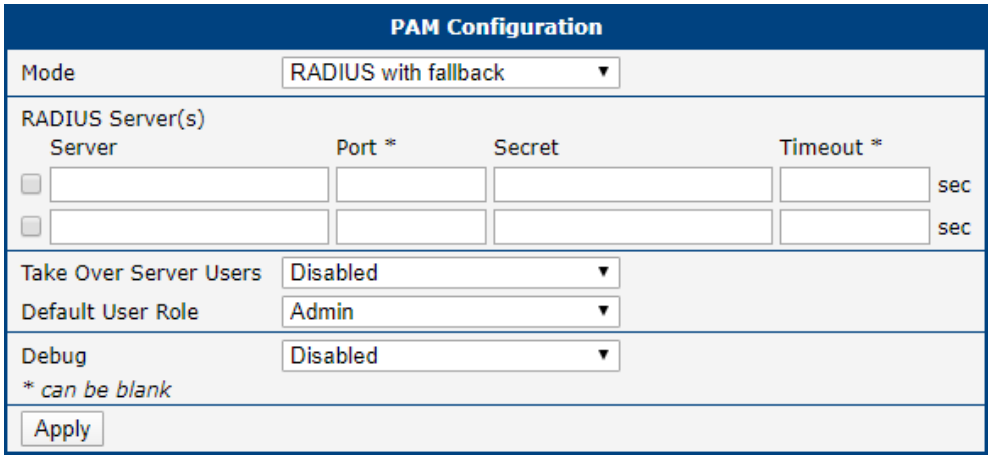


Figure 62: Configuration of RADIUS

Item	Description
Server	Address of the RADIUS server. Up to two servers can be configured.
Port	Port of the RADIUS server.
Secret	The secret For authentication to the RADIUS server.
Timeout	Timeout for authentication to the RADIUS server.
Take Over Server Users	If enabled, a new user account is created during the login, in case the RADIUS authentication is successful and appropriate local account does not exist. New accounts are created without the password. An existing user account with a password is never modified by this feature.
Default User Role	Choose the user role (*Admin* or *User*). This role corresponds with router's user roles, see Chapter 5.1. Selected role will be used for a user in case the option *Take Over Server Users* is enabled and if the user's *Service-Type* set on the RADIUS server is missing or is not set up to *NAS-Prompt-User* or *Administrative-User*. When *Service-Type* is set to *NAS-Prompt-User*, the *User* role will be used. When *Service-Type* is set to *Administrative-User*, the *Admin* role is used.

Table 50: Configuration of RADIUS

TACACS+ Mode

When authenticate against the TACACS+ server, user with the same name must exist locally. It can be created manually (see Chapter 5.1) or can be created automatically based on data from TACACS+ server, if the *Take Over Server Users* option is enabled as described hereunder.

To configure the authentication against a TACACS+ server, choose *TACACS+ with fallback* or *TACACS+ only* as the *PAM mode* and set up all required items, see Figure 63. Table 51 describes all the configuration options for the TACACS PAM modes.

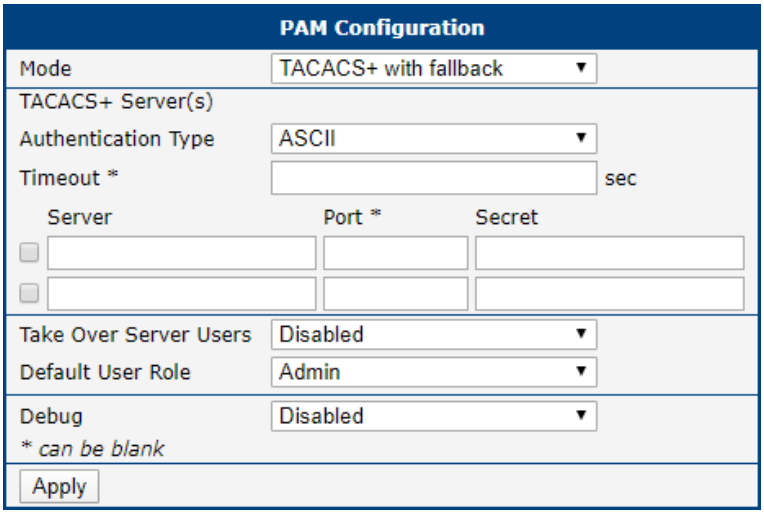


Figure 63: Configuration of TACACS+

Item	Description
Authentication Type	Choose ASCII, PAP or CHAP as authentication type.
Timeout	Timeout for authentication to the TACACS+ server.
Server	Address of the TACACS+ server. Up to two servers can be configured.
Port	Port of the TACACS+ server.
Secret	The secret For authentication to the TACACS+ server.
Take Over Server Users	If enabled, a new user account is created during the login, in case the TACACS+ authentication is successful and appropriate local account does not exist. New accounts are created without the password. An existing user account with a password is never modified by this feature.
Default User Role	Choose the user role (*Admin* or *User*). This role corresponds with router's user roles, see Chapter 5.1. Selected role will be used for a new user when *Take Over Server Users* is used.

Table 51: Configuration of TACACS+

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 about its expansion ports eventually) 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.

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.
Custom	You can use this input field to enter specific information tailored to your requirements.

Table 52: 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.
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.

Table 53: SNMPv3 Configuration

In addition, you can continue with this configuration:

- Activating the *Enable I/O extension* function allows you monitor the binary I/O inputs on the router.
- Selecting the *Enable XC-CNT extension* lets you monitor the expansion port CNT inputs and outputs status.
- Selecting *Enable M-BUS extension* and entering the *Baudrate*, *Parity* and *Stop Bits* lets you monitor the meter status connected to the expansion port MBUS status.

Item	Description
Baudrate	Communication speed
Parity	Control parity bit: • **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.

Table 54: SNMP configuration – MBUS extension

Parameters *Enable XC-CNT extension* and *Enable M-BUS extension* cannot be checked at the same time.

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	IP address
Period	Period of sending statistical information (in minutes).

Table 55: 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.

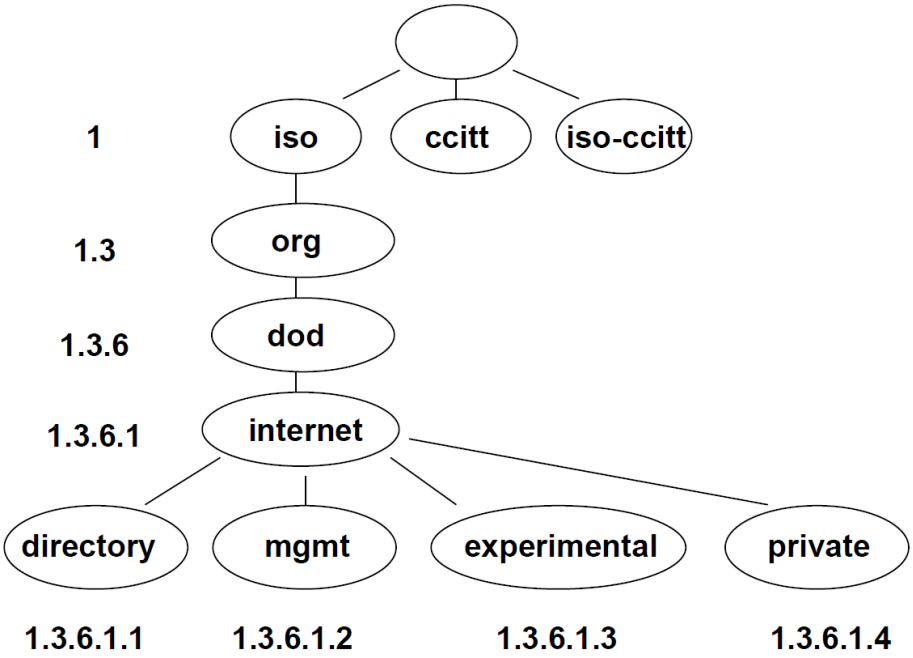


Figure 64: OID Basic Structure

The SNMP values that are specific for Advantech 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 binary input and output. The following table shows the range of used OID values:

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)

Table 56: Object identifier for binary input and output

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

OID	Description
.1.3.6.1.4.1.30140.2.1.1.0	Analogy input AN1 (range 0-4095)
.1.3.6.1.4.1.30140.2.1.2.0	Analogy input AN2 (range 0-4095)
.1.3.6.1.4.1.30140.2.1.3.0	Counter input CNT1 (range 0-4294967295)
.1.3.6.1.4.1.30140.2.1.4.0	Counter input CNT2 (range 0-4294967295)
.1.3.6.1.4.1.30140.2.1.5.0	Binary input BIN1 (values 0,1)
.1.3.6.1.4.1.30140.2.1.6.0	Binary input BIN2 (values 0,1)
.1.3.6.1.4.1.30140.2.1.7.0	Binary input BIN3 (values 0,1)
.1.3.6.1.4.1.30140.2.1.8.0	Binary input BIN4 (values 0,1)
.1.3.6.1.4.1.30140.2.1.9.0	Binary output OUT1 (values 0,1)

Table 57: Object identifier for CNT port

For the expansion port M-BUS, the following range of OID is used:

OID	Description
.1.3.6.1.4.1.30140.2.2.<address>.1.0	IdNumber – meter number
.1.3.6.1.4.1.30140.2.2.<address>.2.0	Manufacturer
.1.3.6.1.4.1.30140.2.2.<address>.3.0	Version – specified meter version
.1.3.6.1.4.1.30140.2.2.<address>.4.0	Medium – type of metered medium
.1.3.6.1.4.1.30140.2.2.<address>.5.0	Status – errors report
.1.3.6.1.4.1.30140.2.2.<address>.6.0	0. VIF – value information field
.1.3.6.1.4.1.30140.2.2.<address>.7.0	0. measured value
.1.3.6.1.4.1.30140.2.2.<address>.8.0	1. VIF – value information field
.1.3.6.1.4.1.30140.2.2.<address>.9.0	1. measured value
.1.3.6.1.4.1.30140.2.2.<address>.10.0	2. VIF – value information field
.1.3.6.1.4.1.30140.2.2.<address>.11.0	2. measured value
.1.3.6.1.4.1.30140.2.2.<address>.12.0	3. VIF – value information field
.1.3.6.1.4.1.30140.2.2.<address>.13.0	3. measured value
⋮	⋮
.1.3.6.1.4.1.30140.2.2.<address>.100.0	47. VIF – value information field
.1.3.6.1.4.1.30140.2.2.<address>.101.0	47. measured value

Table 58: Object identifier for M-BUS port

The meter address can be from range 0 – 254, where the number 254 is broadcast.

Starting with firmware version 3.0.4, all v2 routers with board RB-v2-6 and newer provide information About the internal temperature of the device (OID 1.3.6.1.4.1.30140.3.3) and power voltage (OID 1.3.6.1.4.1.30140.3.4).

The list of available and supported OIDs and other details can be found in the application note *SNMP Object Identifiers* [11].

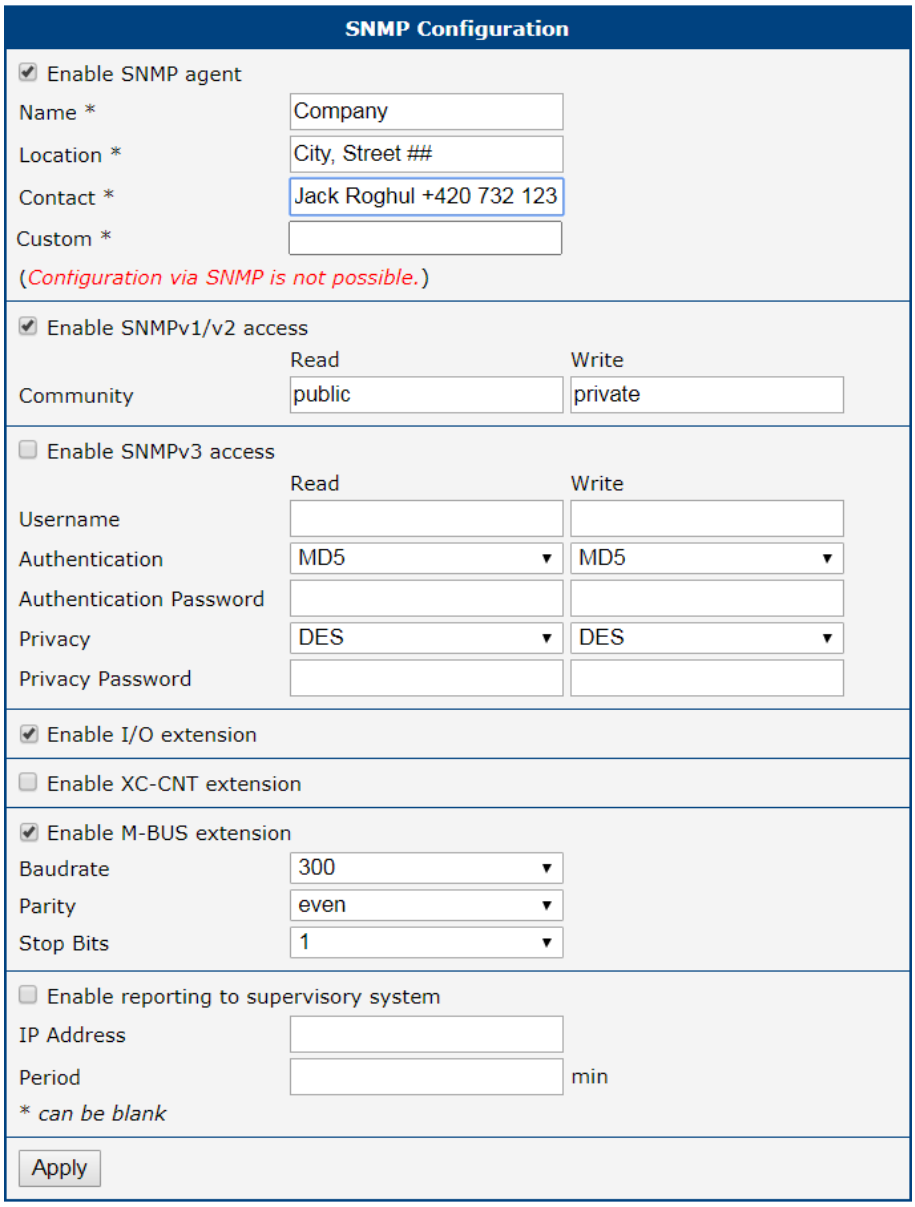


Figure 65: SNMP Configuration Example

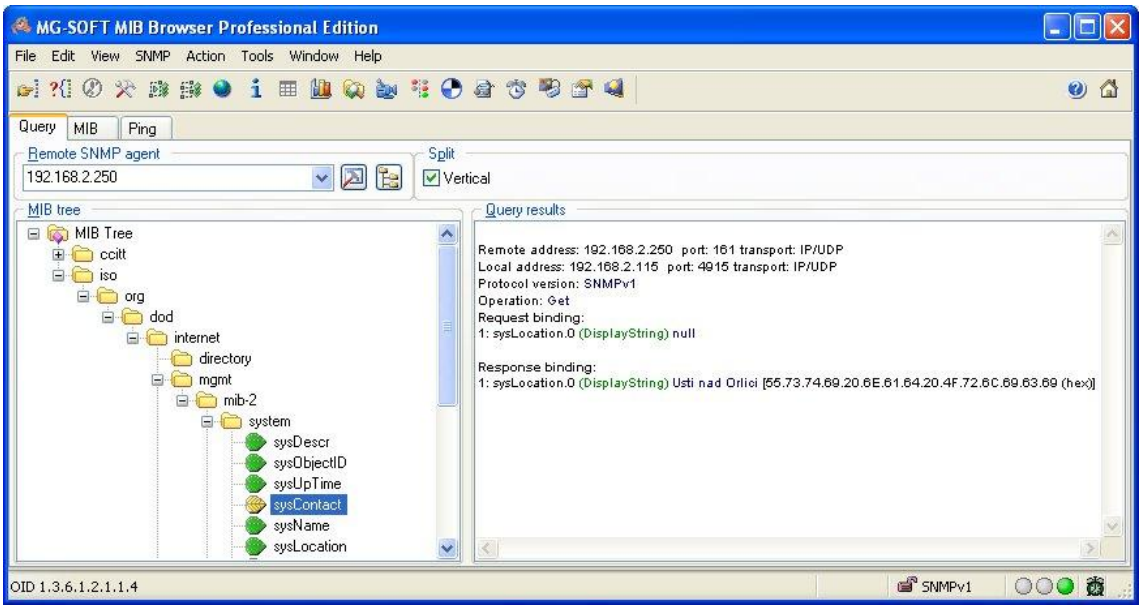


Figure 66: MIB Browser Example

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

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

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

Table 59: SMTP client configuration

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

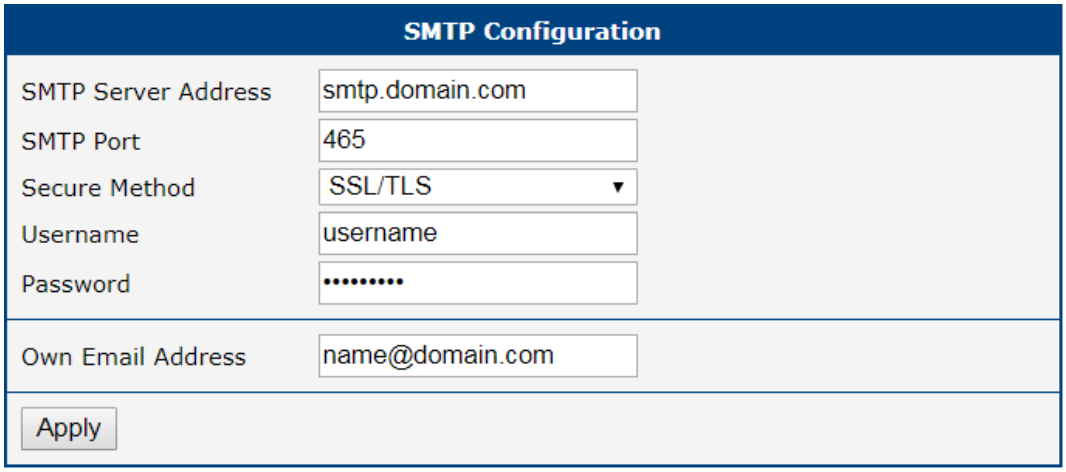


Figure 67: SMTP Client Configuration Example

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

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

Commands and parameters can be entered only in lowercase.

Example of sending an e-mail:

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

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

4.16.8 SMS

The *SMS Configuration* page is not available for the XR5i v2 routers.

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

Item	Description
Send SMS on power up	Activates/deactivates the sending of an SMS message automatically on power up.
Send SMS on connect to mobile network	Activates/deactivates the sending of an SMS message automatically when the router is connected to a mobile network.
Send SMS on disconnect to mobile network	Activates/deactivates the sending of an SMS message automatically when the router is disconnection from a mobile network.
Send SMS when datalimit exceeded	Activates/deactivates the sending of an SMS message automatically when the data limit exceeded.
Send SMS when binary input on I/O port (BIN0) is active	Send an SMS message when the binary input on the I/O port (BIN0) goes active. The text of the message is set using parameter BIN0.
Send SMS when binary input on expansion port (BIN1 – BIN4) is active	Automatic sending SMS message after binary input on expansion port (BIN1 – BIN4) is active. Text of message is intended parameter BIN1 – BIN4.
Add timestamp to SMS	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	SMS text messages when activate the first binary input on the router.

Continued on next page

Continued from previous page

Item	Description
BIN1 – SMS	SMS text messages when activate the binary input on the expansion port.
BIN2 – SMS	SMS text messages when activate the binary input on the expansion port.
BIN3 – SMS	SMS text messages when activate the binary input on the expansion port.
BIN4 – SMS	SMS text messages when activate the binary input on the expansion port.

Table 60: 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 61: Control via SMS

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

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

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

SMS	Description
go online sim 1	The router changes to SIM1 (APN1)
go online sim 2	The router changes to SIM2 (APN2)
go online	Changes the router to the online mode
go offline	Changes the router to the off line mode
set out0=0	Sets the binary output to 0
set out0=1	Sets the binary output to 1
set out1=0	Sets the binary output of XC-CNT to 0
set out1=1	Sets the binary output of XC-CNT 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 62: 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 63: 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 64: 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. The router sends SMS messages using a standard AT command.

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

Table 65: Send SMS on ethernet PORT1 configuration

If you establish a connection to the router through a serial interface or interface using the TCP protocol, 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

Continued on next page

Continued from previous page

AT Command	Description
AT+CMGS	Sends a short message from the device to entered tel. number
AT+CMGW	Writes a short message to SIM storage
AT+CMSS	Sends a message from SIM storage location value
AT+CNUM	Returns the phone number, if available (stored on SIM card)
AT+COPS?	Identifies the available mobile networks
AT+CPIN	Is used to find out the SIM card state and enter a PIN code
AT+CPMS	Selects SMS memory storage types, to be used for short message operations
AT+CREG	Displays network registration status
AT+CSCA	Sets the short message service centre (SMSC) number
AT+CSCS	Selects the character set
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 66: List of AT Commands

A detailed description and examples of these AT commands can be found in the application note *AT commands* [12].

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 through a serial interface or interface using the TCP protocol, then you can use AT commands to manage SMS messages. See application note *AT Commands (AT-SMS)* [12].
- 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 5.8 Chapter.

- 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: SMS sending configuration.

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

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

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

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

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

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

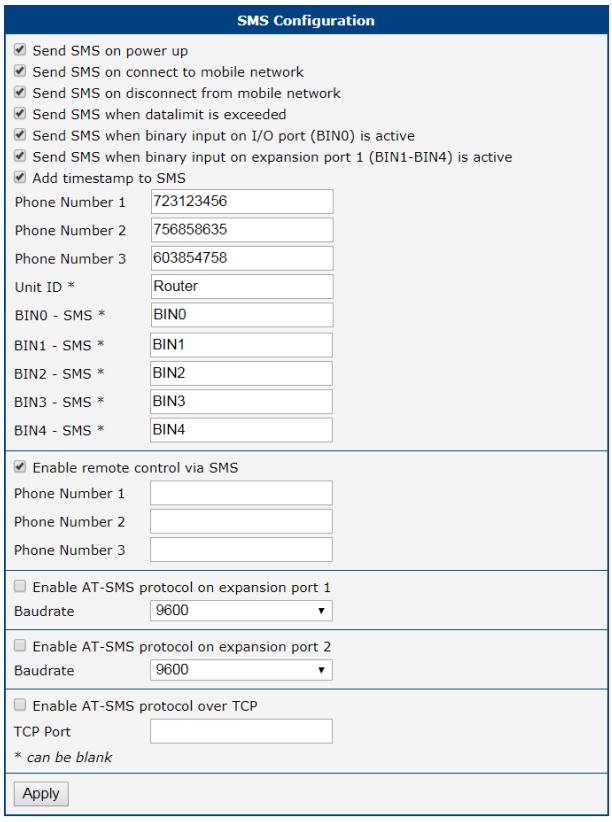


Figure 68: Example 1 – SMS Configuration

Example 2: Configuration for sending SMS via serial interface on the Port 1.

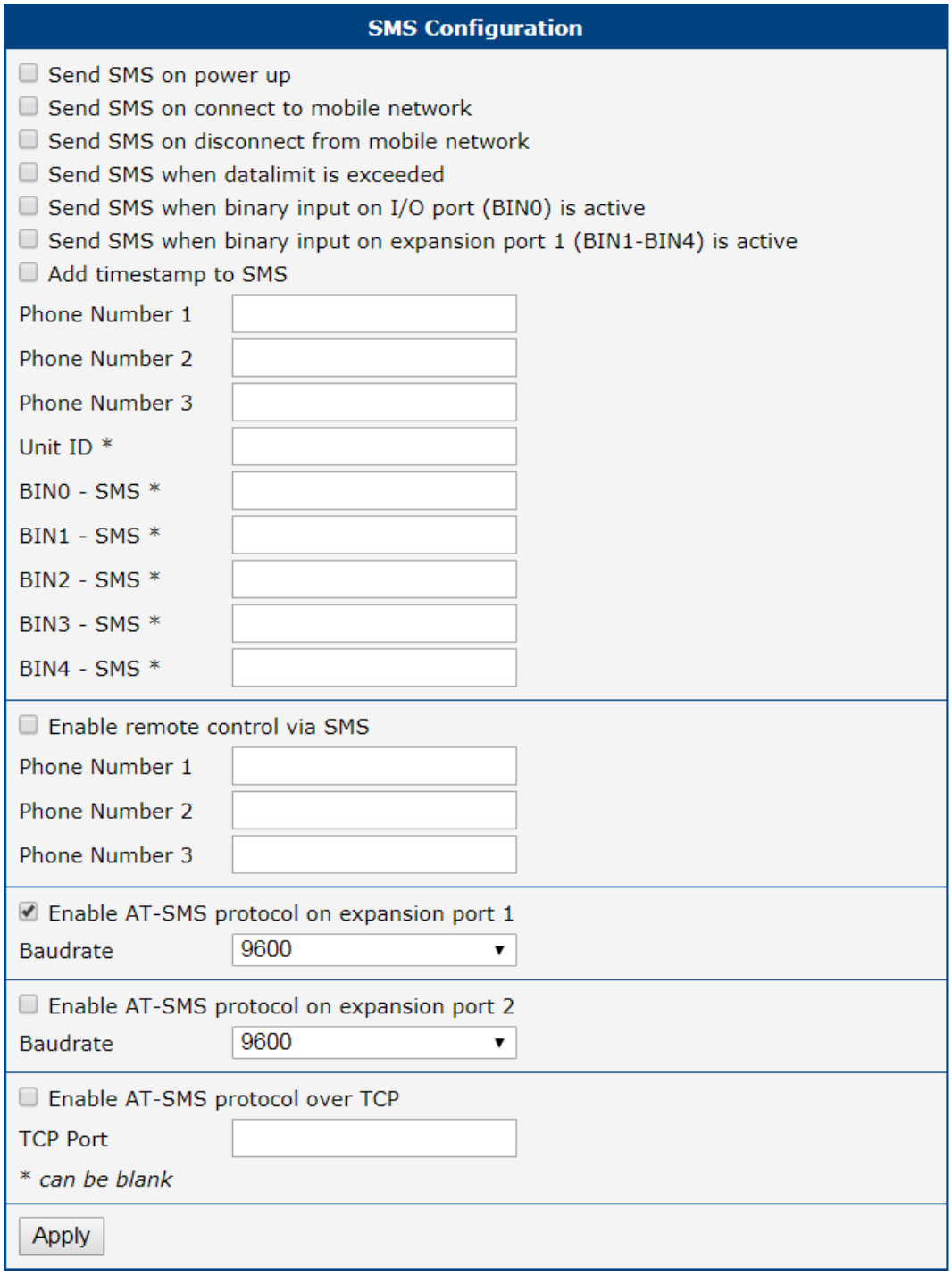


Figure 69: Example 2 – SMS Configuration

Example 3: Control the router using an SMS from any phone number.

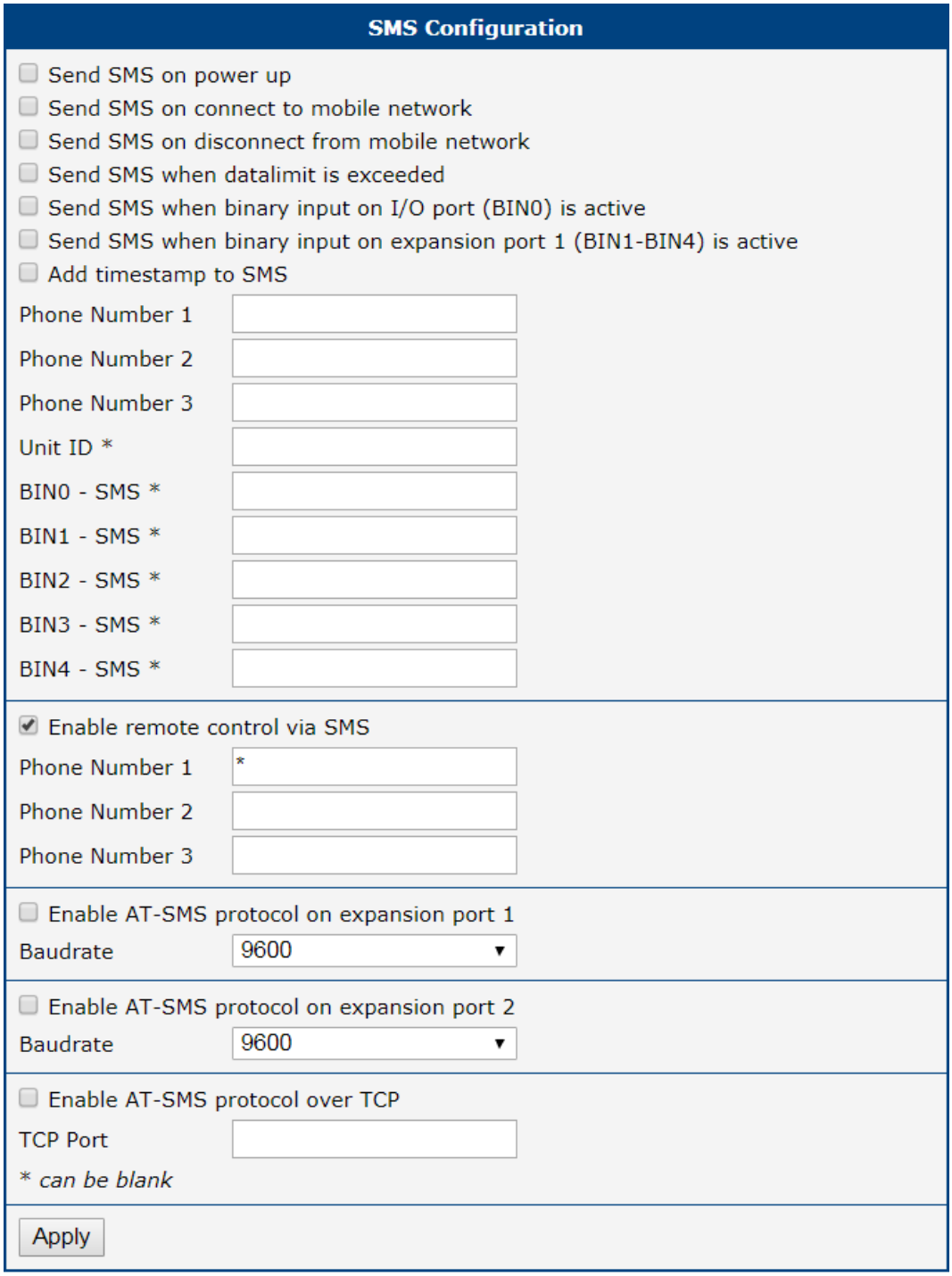


Figure 70: Example 3 – SMS Configuration

Example 4: Control the router using an SMS from two phone numbers.

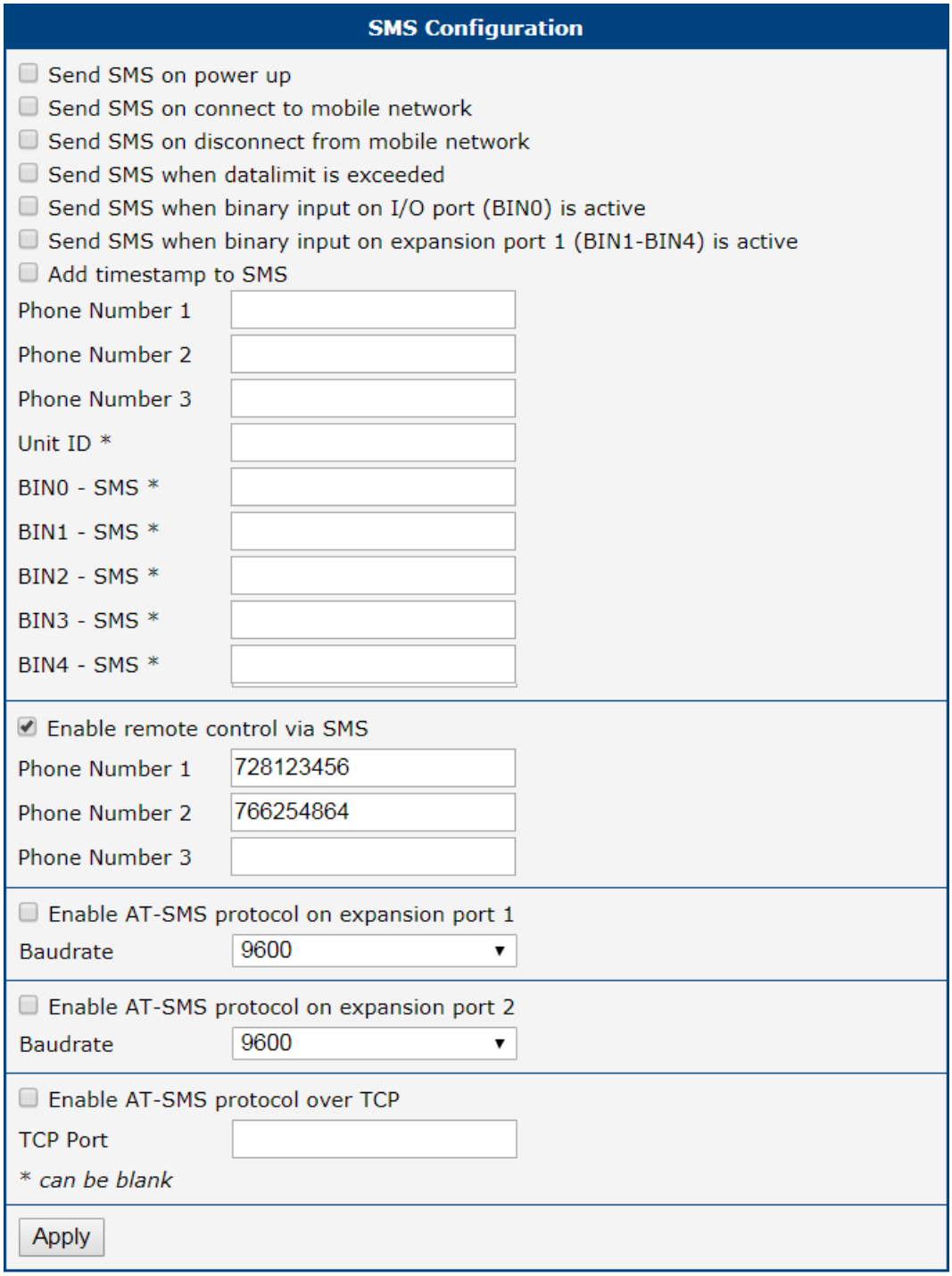


Figure 71: Example 4 – SMS Configuration

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.
Login Banner	The text specified in this field will be displayed in the console during the SSH login just after the login name entry.
Keep the current SSH key	Choose to keep current key.
Generate a new SSH key	Choose to generate new key.
Key Length	Choose the key length to be generated.

Table 67: Parameters for SSH service configuration

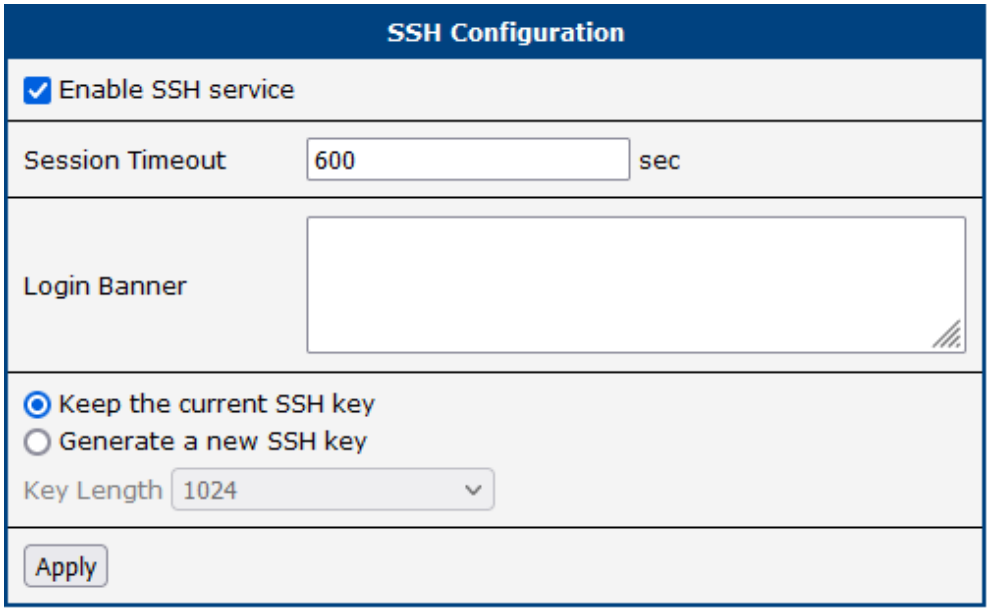


Figure 72: Configuration of HTTP service

4.16.10 Syslog

Configuration of the system log, known as *syslog*, is accessible from this configuration page. It is possible to limit the log size by specifying the maximum number of entries (rows). Additionally, users have the option to set an address and UDP port for distributing the log in real time.

To view this log, navigate to the router's GUI via *Status* → *System Log*, or access it through the console with the `slog` command.

Položka	Popis
Log Size	Restriction of log size by the maximum number of rows.
Log Persistent	Set to *yes* to enable logging to a file saved in non-volatile memory, ensuring that logs are preserved even after the router is powered down. **This feature is exclusive to routers equipped with eMMC memory.**
Remote Host	Remote host address for real-time log distribution. Hostnames are supported[1].
Remote UDP Port	UDP port for real-time log distribution.
Device ID	A unique identification string for remote logging purposes. If left blank, the default string *Router* is utilized.

Table 68: Syslog configuration

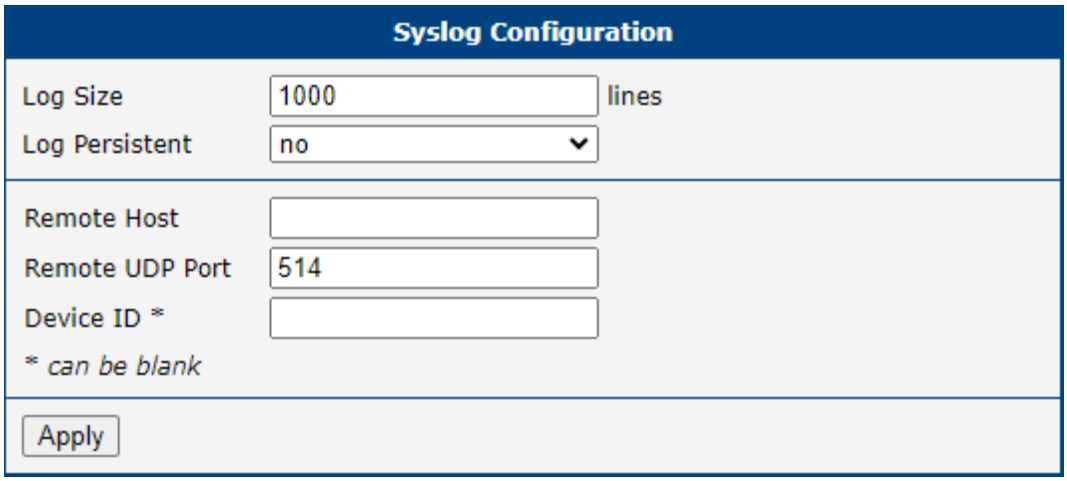


Figure 73: Syslog configuration

[1] DNS translation is refreshed every 60 minutes.

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.

Item	Description
Enable Telnet service	Enabling of Telnet service.
Maximum Sessions	Is used to close inactive sessions. The server will terminate a Telnet session after it has not been used for the given amount of seconds. The range is from 1 to 500.

Table 69: Parameters for Telnet service configuration

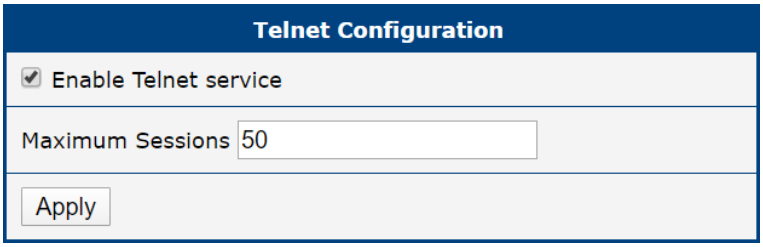


Figure 74: Configuration of Telnet service

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.

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:

Item	Description
Baudrate	Applied communication speed: **300**, **600**, **1200**, **2400**, **4800**, **9600** (default), **19200**, **38400**, **57600**, **115200**, **230400**.
Data Bits	Number of data bits: **5**, **6**, **7**, **8** (default).
Parity	Control parity bit: • **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: **1** (default), **2**.
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: • **TCP** – communication using a linked protocol TCP. • **UDP** – communication using a unlinked protocol UDP.
Mode	Mode of connection: • **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 *TCP client* above, it is necessary to enter the *Server address* and *TCP port*.
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 70: Expansion 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 71: Expansion 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 72: 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 73: DTR Signal Description

Since firmware 3.0.9, all v2 routers provide a program called *getty* which allows user to connect to the router via the serial line (router must be fitted with an expansion port RS232!). Getty displays the prompt and after entering the username passes it on *login* program, which asks for a password, verifies it and runs the shell. After logging in, it is possible to manage the system as well as a user is connected via telnet.

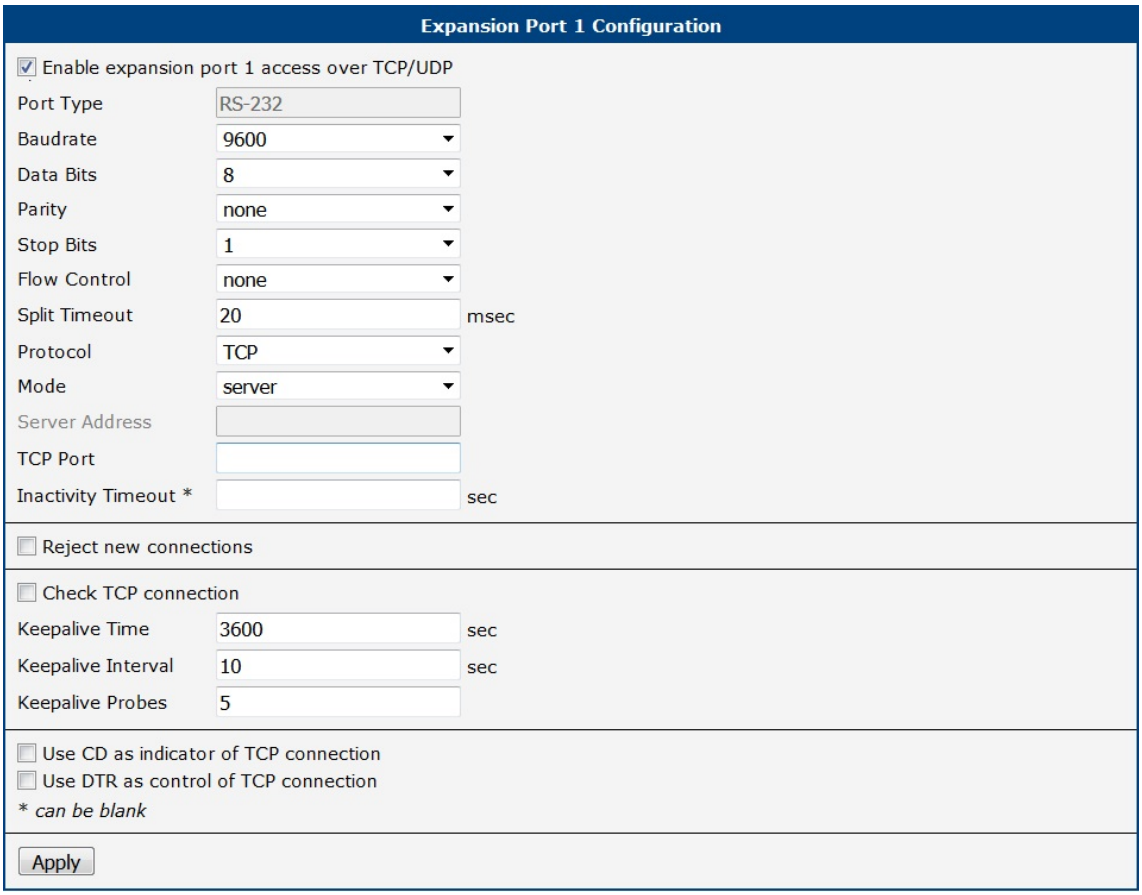


Figure 75: Expansion Port Configuration

Examples of the expansion port configuration:

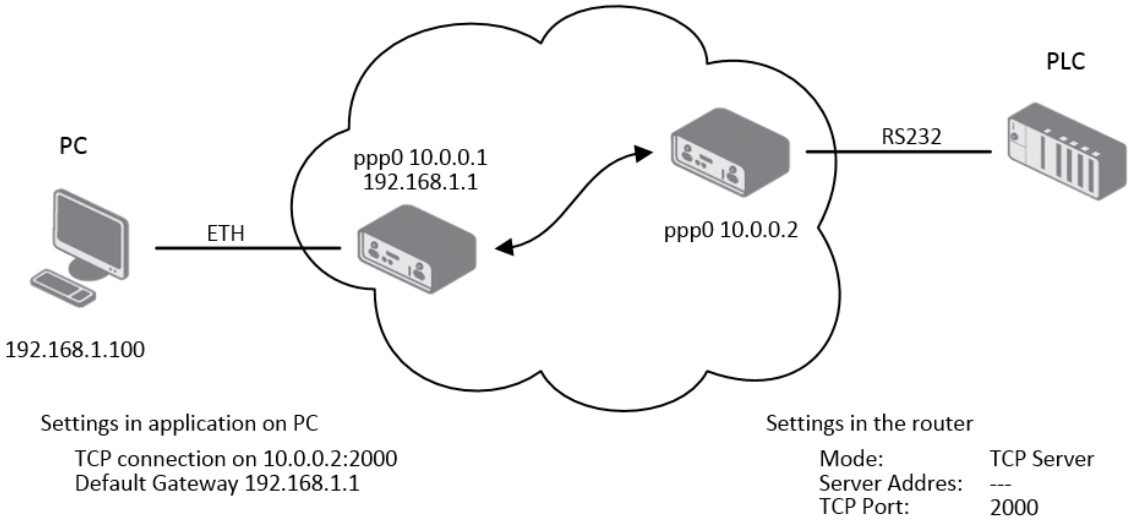


Figure 76: Example of Ethernet to serial communication

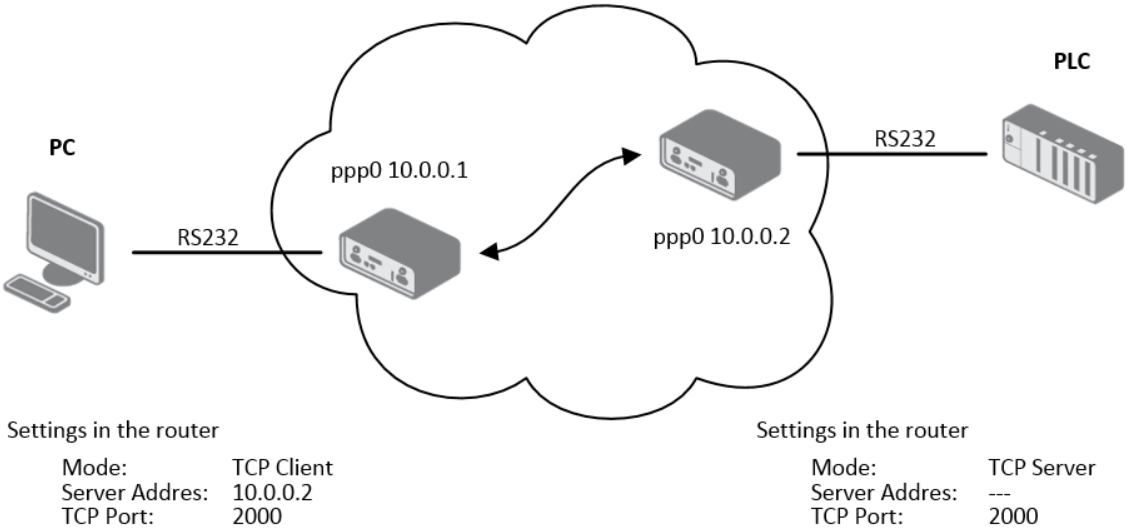


Figure 77: Example of serial port extension

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.

The USB port can be disabled by clearing the *Enable external USB port* checkbox. Ensure that all filesystems attached to storage are unmounted before disabling the USB port.

Item	Description
Baudrate	Applied communication speed.
Data Bits	Number of data bits.
Parity	Control parity bit: • **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: • **TCP** – communication using a linked protocol TCP. • **UDP** – communication using a unlinked protocol UDP.
Mode	Mode of connection: • **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 *TCP client* above, it is necessary to enter the *Server address* and *TCP port*.
TCP Port	TCP/UDP port used for communications. The router uses the value for both the server and client modes.

Continued on next page

Continued from previous page

Item	Description
Inactivity Timeout	Time period after which the TCP/UDP connection is interrupted in case of inactivity.

Table 74: 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 75: 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 76: 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 77: DTR Signal Description

The router supports the following USB/RS232 converters:

- FTDI
- Prolific PL2303
- Silicon Laboratories CP210×

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

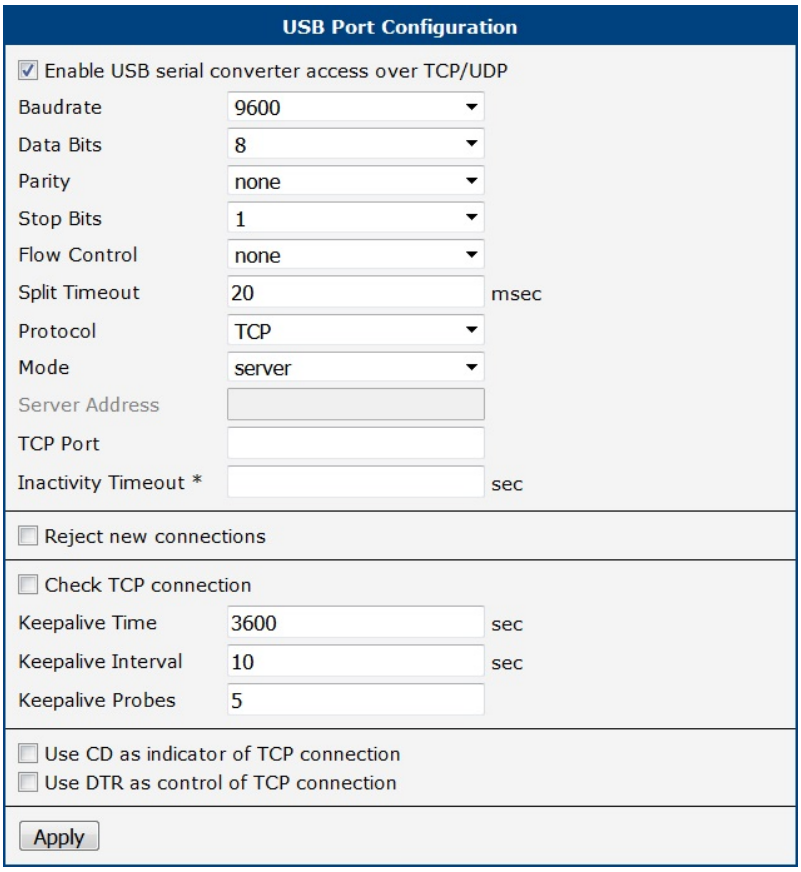


Figure 78: USB configuration

Examples of USB port configuration:

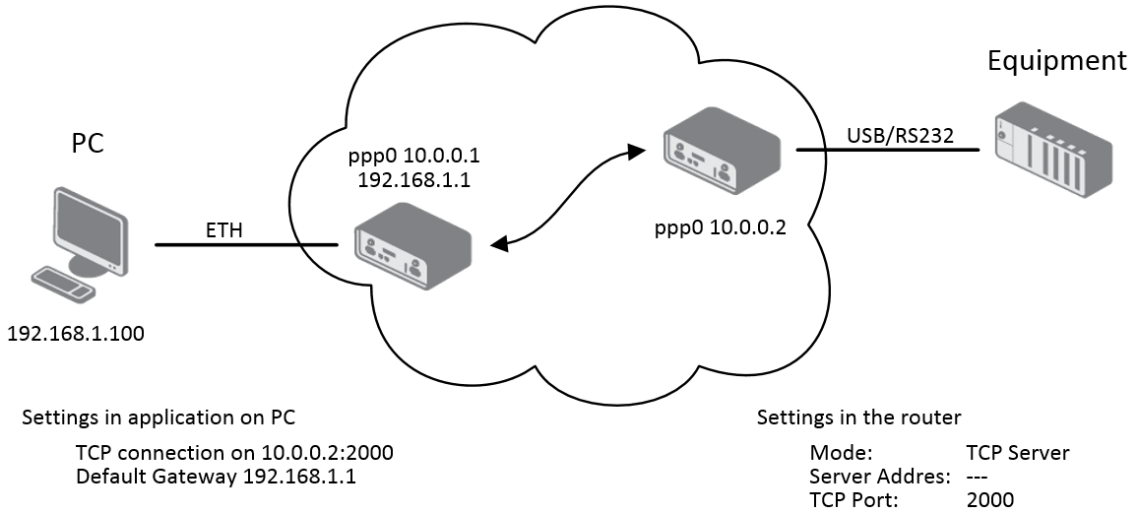
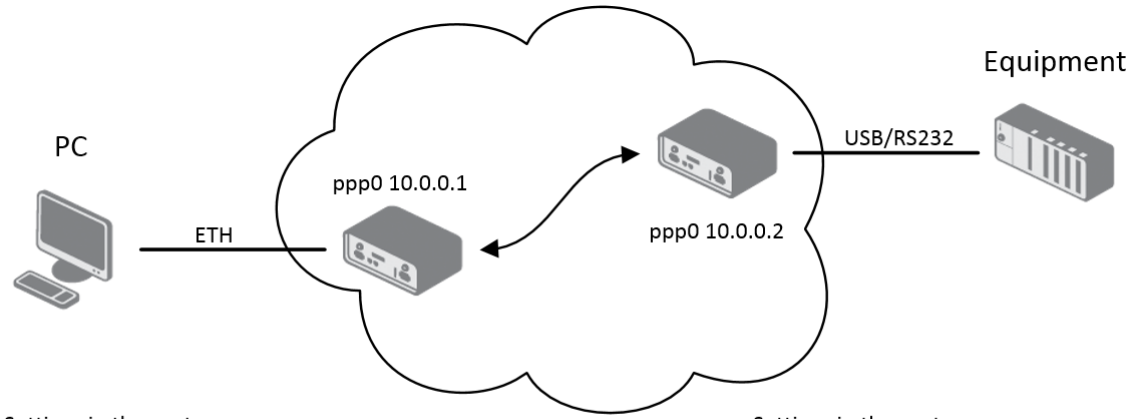


Figure 79: Example 1 – USB port configuration



Settings in the router

Mode:	TCP Client
Server Addres:	10.0.0.2
TCP Port:	2000

Settings in the router

Mode:	TCP Server
Server Addres:	---
TCP Port:	2000

Figure 80: 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* and *Up/Down* scripts you can use. 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.

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

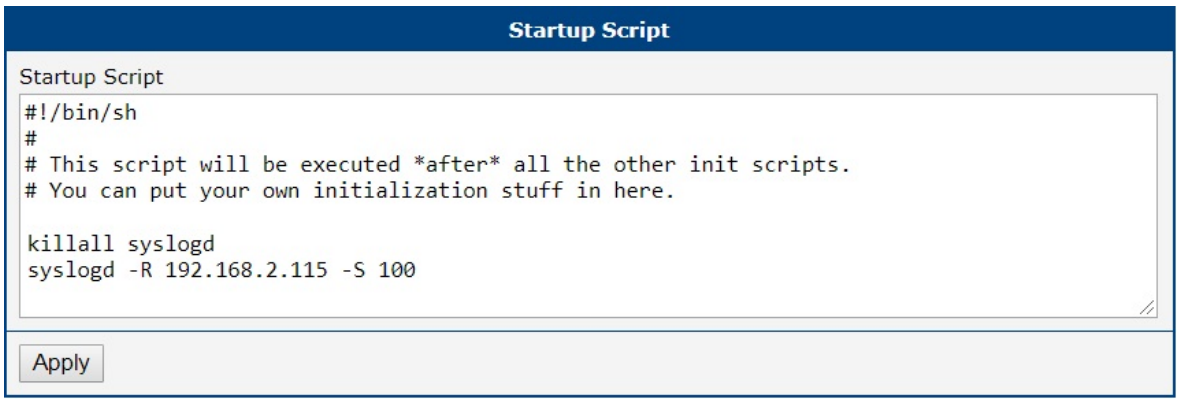


Figure 81: Example of a Startup Script

4.19.2 Up/Down Script

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

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

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

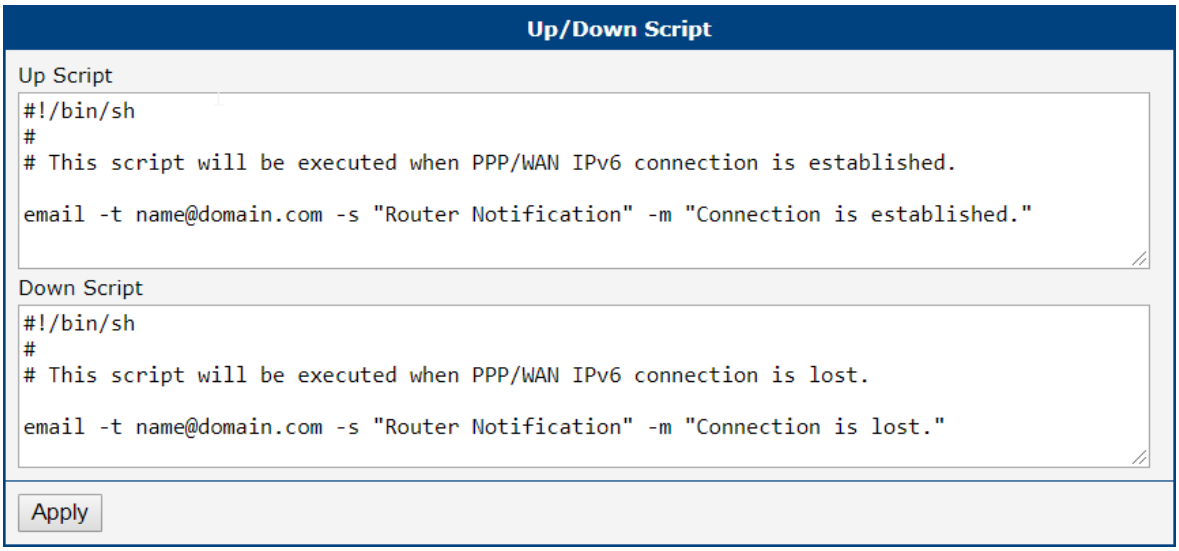


Figure 82: Example of Up/Down Script

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. 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 us written out there, see Chapter 5.11.

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 router apps. It is recommended that you update router apps to the most recent version. Information about the router apps and the firmware compatibility is at the beginning of the router app's Application Note.

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

Item	Description
Source	Select the location of the update files: • **HTTP(S)/FTP(S) server** – Updates are downloaded from the Base URL address below. Used protocol is specified by that address: HTTP, HTTPS, FTP or FTPS (only implicit mode is supported). • **USB flash drive** – The router finds the current firmware or configuration in the root directory of the connected USB device. • **Both** – Looking for the current firmware or configuration from both sources.
Base URL	Base URL or IP address from which the configuration file will be downloaded. This option also specifies the communication protocol (HTTP, HTTPS, FTP or FTPS), see examples below.
Unit ID	Name of configuration (name of the file without extension). If the *Unit ID* is not filled, the MAC address of the router is used as the filename (the delimiter colon is used instead of a dot.)
Decryption Password	Password for decryption of crypted configuration file. This is required only in case the configuration is encrypted.
Update Window Start	Choose an hour (range from 1 to 24) when the automatic update will be performed on a daily basis. If the time is not specified (set to *dynamic*), the automatic update is performed five minutes after router boots up and then regularly every 24 hours.
Update Window Length	This value defines the period within the update will be done. This period starts at the time set in the *Update Window Start* field. The exact time, when the update will be done, is generated randomly.

Table 78: Automatic Update Configuration

4.20.1 Example of Automatic Update

The following example checks for new firmware or configurations each day at 1:00 a.m. This example is given for the LR77 v2 router.

- Firmware: https://example.com/LR77-v2.bin
- Configuration file: https://example.com/test.cfg

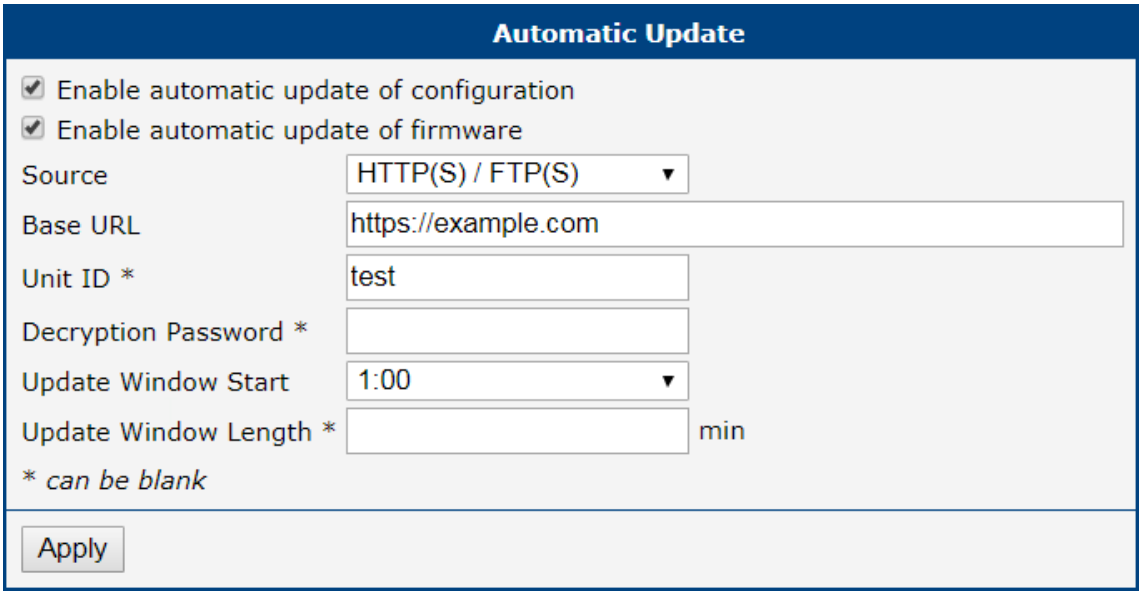


Figure 83: Example of Automatic Update 1

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 configuratin file is encrypted, therefore the decryption password was configured. This example is given for the LR77 v2 router with MAC address 00:11:22:33:44:55.

- Firmware: https://example.com/LR77-v2.bin
- Configuration file: https://example.com/00.11.22.33.44.55.cfg

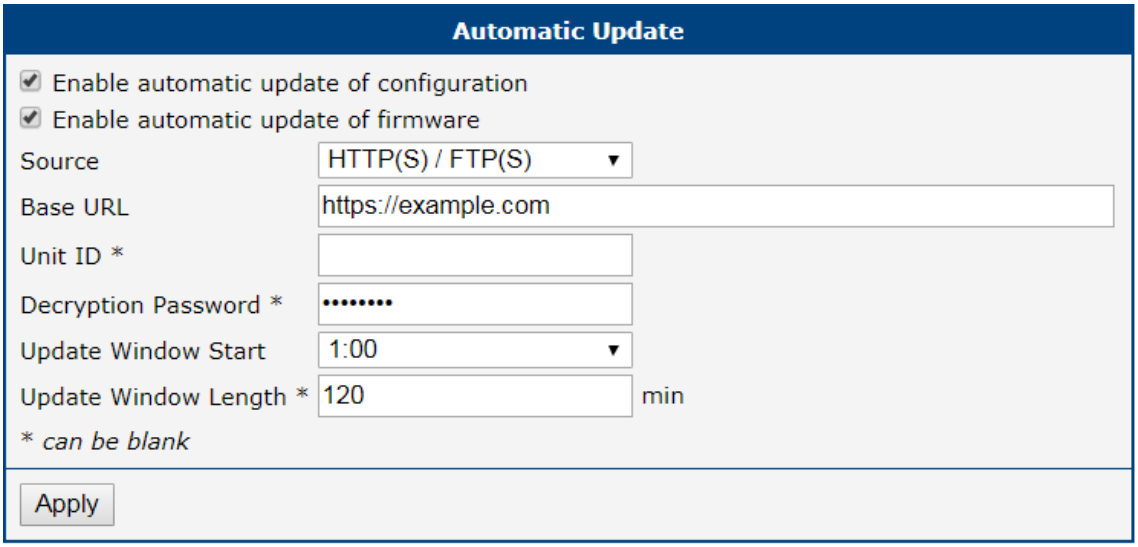


Figure 84: Example of Automatic Update 2

5. Administration

5.1 Users

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

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

To manage the users, open the *Users* form in the *Administration* section of the main menu, see Figure 85.

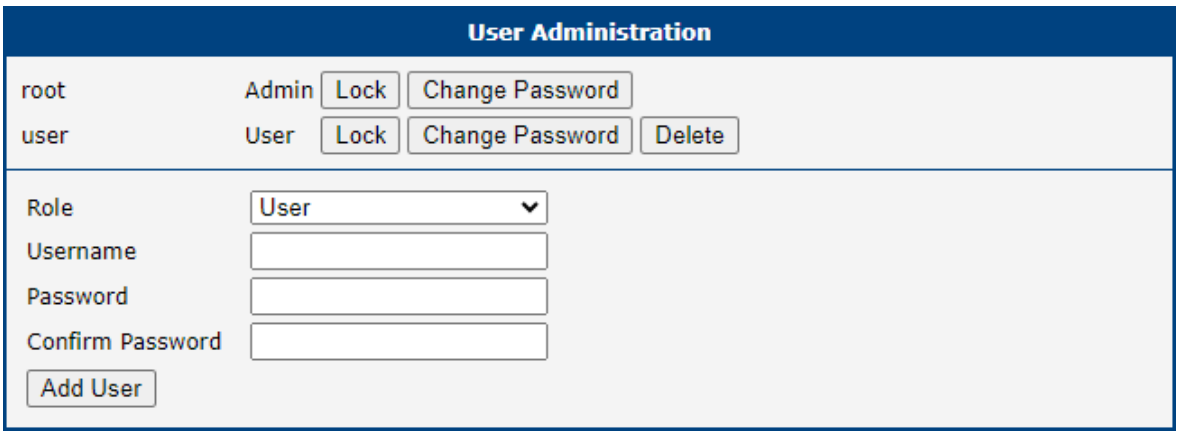


Figure 85: Users Administration Form

The first part of this configuration form contains an overview of all existing users. Table 79 describes the meaning of the buttons on every user's right.

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

Table 79: Button Description

The second part of the configuration form allows adding a new user. All items are described in Table 80.

Item	Description
Role	• **User** ◦ User with **basic permissions**. ◦ Read-only access to the web GUI. ◦ Some menu items are hidden in the web GUI. ◦ Full access to Router Apps GUI. ◦ No access to the router via Telnet, SSH or SFTP. ◦ Read-only access to the FTP server. • **Admin** ◦ User with **enhanced permissions**. ◦ Full access to all items in the web GUI. ◦ Access to the router via Telnet, SSH or SFTP. ◦ Not the same rights as the superuser on a Linux-based system.
Username	Specifies the name of the user having access to log in to the device.
Password	Specifies the password for the user. Valid characters are not restricted.
Confirm Password	Confirms the password.

Table 80: User Parameters

5.2 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.

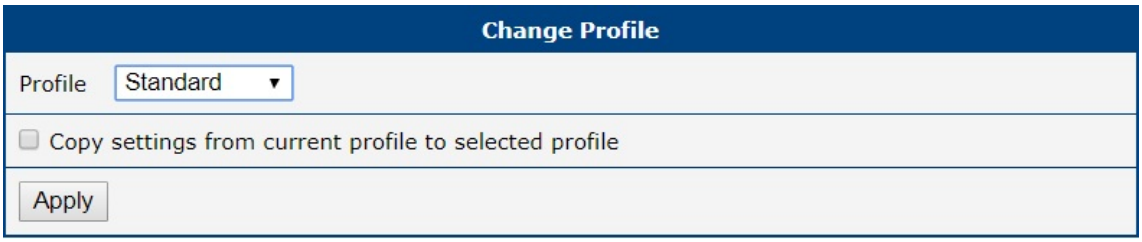


Figure 86: Change Profile

5.3 Change Password

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

The default password for the **root** user is printed out on the router's label.[1] 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.

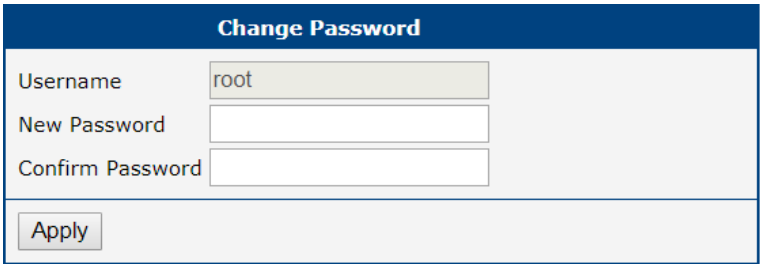


Figure 87: Change Password

5.4 Set Real Time Clock

Manual Configuration:

1. **Date and Time Setting:** You have the option to manually input the date and time. Ensure you adhere to the **yyyy-mm-dd** format for the date, as exemplified in the figure below. For time, use the **HH:MM:SS** format.
2. **Browser Time Sync:** Alternatively, utilize the *Apply Browser Time* button. This option synchronizes the device's clock with the time displayed on your web browser.

Network Time Protocol (NTP) Configuration:

1. **NTP Server Address:** To enable automatic time synchronization, input the address of an NTP server. The system supports both IPv4 and IPv6 addresses, as well as domain names.
2. **Applying Settings:** After configuring the date and time settings manually or specifying an NTP server, finalize the setup by clicking the *Apply* button. This action updates the device's internal clock with the chosen settings.

[1] If the router's label does not contain a unique password, use the password "root".

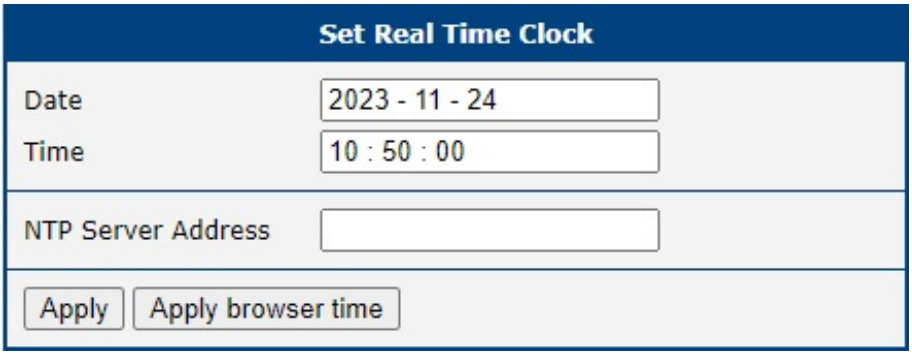


Figure 88: Set Real Time Clock

5.5 Set SMS Service Center Address

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

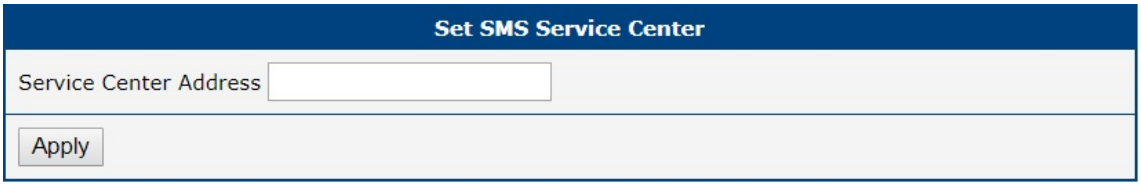


Figure 89: Set SMS Service Center Address

5.6 Unlock SIM Card

The XR5i v2 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. Unblocking of SIM card by PUK number is described in next chapter.

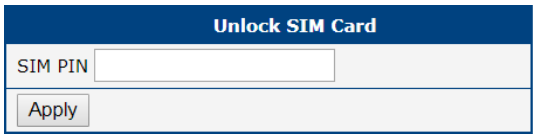


Figure 90: Unlock SIM Card

5.7 Unblock SIM Card

The XR5i v2 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.

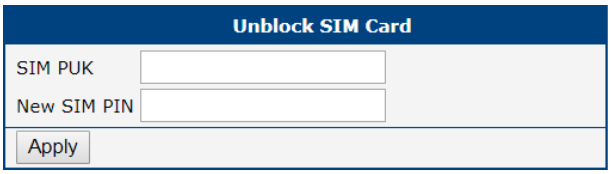


Figure 91: Unblock SIM Card

5.8 Send SMS

The XR5i v2 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* router app).

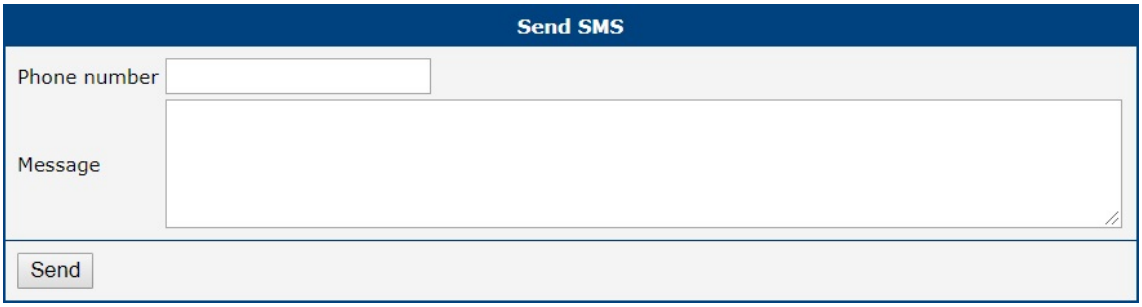


Figure 92: Send SMS

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].

5.9 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 93. 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 5.10 for more information.

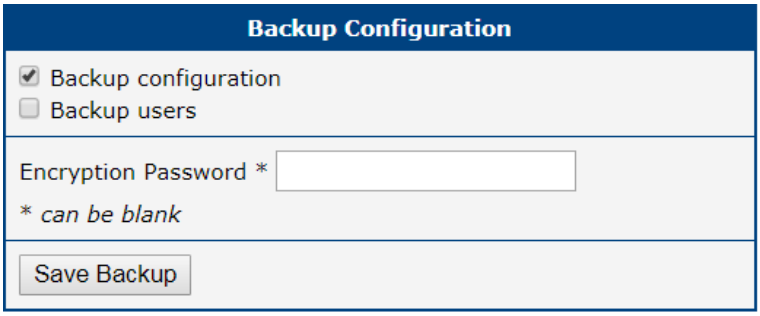


Figure 93: Backup Configuration

5.10 Restore Configuration

You can restore a router configuration stored in a file. You have created the file as shown in the previous chapter.

To restore the configuration from this file, use the *Restore Configuration* form. Next, click the *Browse* button to navigate the directory containing the configuration file you wish to load to the router. If the configuration was stored in an encrypted file, the decryption password must be set to decrypt the file successfully. To start the restoration process, click on *Apply* button.

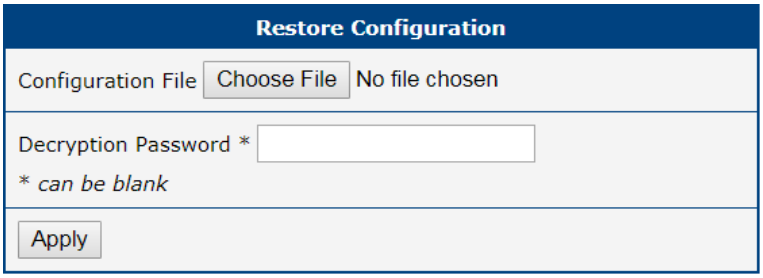


Figure 94: Restore Configuration

5.11 Update Firmware

For security reasons, we highly recommend updating the router's firmware to the latest version regularly. Downgrading the firmware to an older version than the production version or uploading firmware intended for a different device may cause the device's malfunction.

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

Firmware for the routers can be obtained on the product page on *Engineering Portal*, which is available at https://icr.advantech.com/support/router-models.

Update Firmware administration page shows the current router's firmware version and current firmware name, see Figure 95. On this page, the firmware of the router can be updated as well.

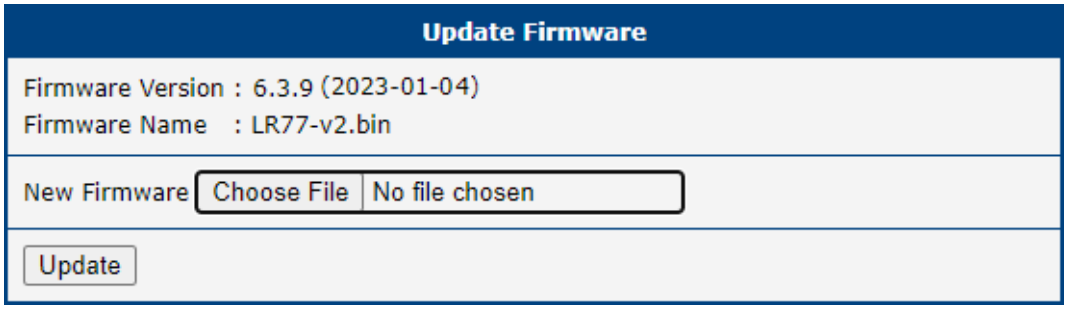


Figure 95: Update Firmware Administration Page

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

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

During the firmware update, the router will display messages, as shown in Figure 96. When done, the router will reboot automatically. When rebooted, click the *here* link to re-open the web interface.

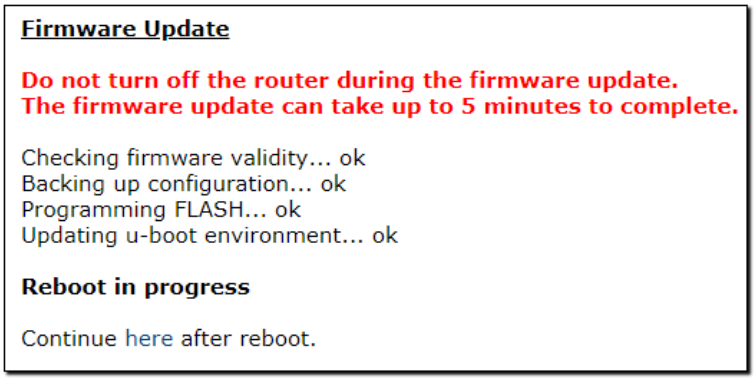


Figure 96: Process of Firmware Update

5.12 Reboot

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

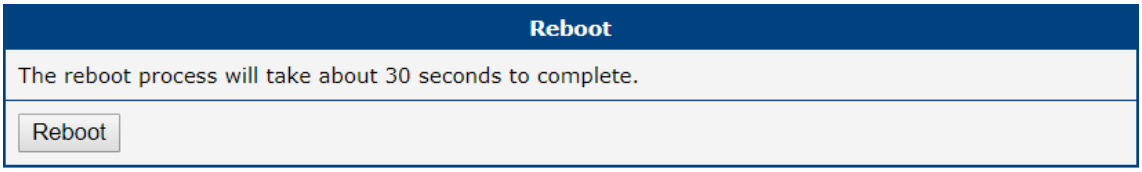


Figure 97: Reboot

5.13 Logout

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

6. Configuration in Typical Situations

Although Advantech 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 routers withouth the cellular module.

6.1 Access to the Internet from LAN

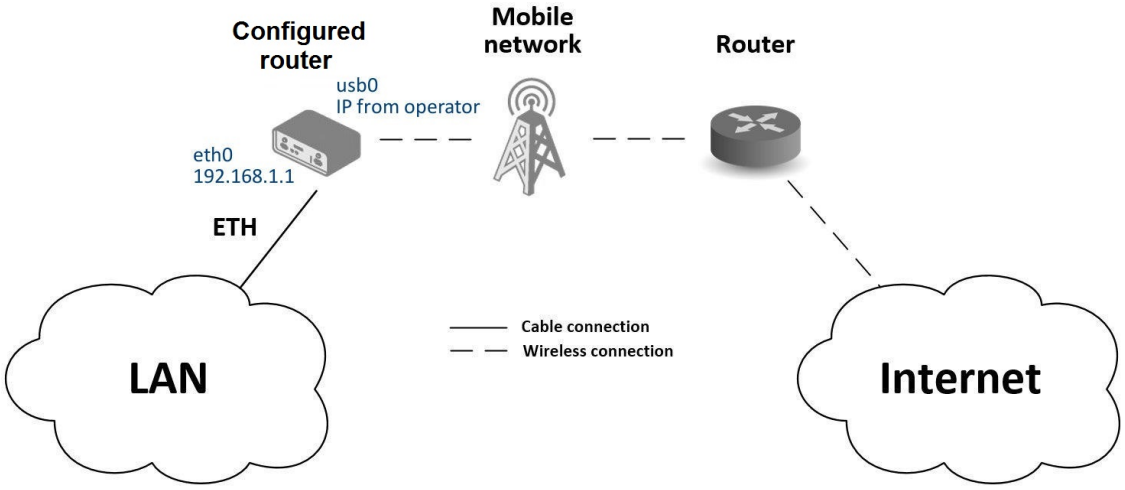


Figure 98: Access to the Internet from LAN – sample topology

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 of the router (*WAN* and *DAT*).

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

Ethernet 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 *Ethernet* item in the *Configuration* section, see Figure 99. 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 Chapter 4.1.

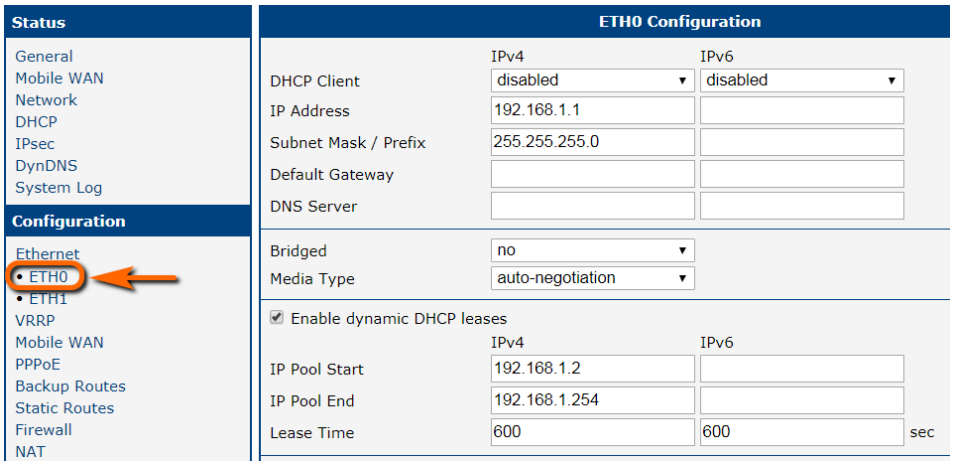


Figure 99: Access to the Internet from LAN – *Ethernet* configuration

Mobile WAN Configuration: Use the *Mobile WAN* item in the *Configuration* section to configure the connection to the mobile network, see Figure 100. 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.

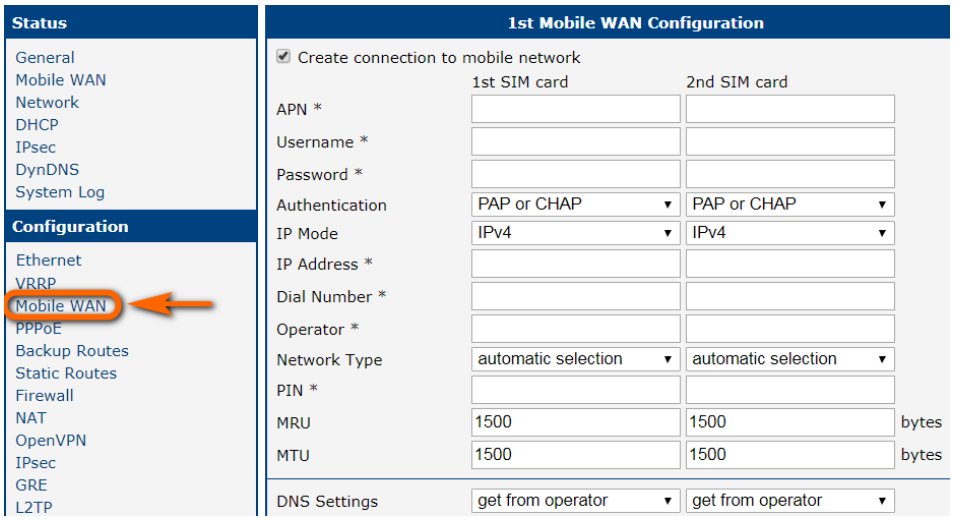


Figure 100: Access to the Internet from LAN – *Mobile WAN* configuration

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.

6.2 Backup Access to the Internet from LAN

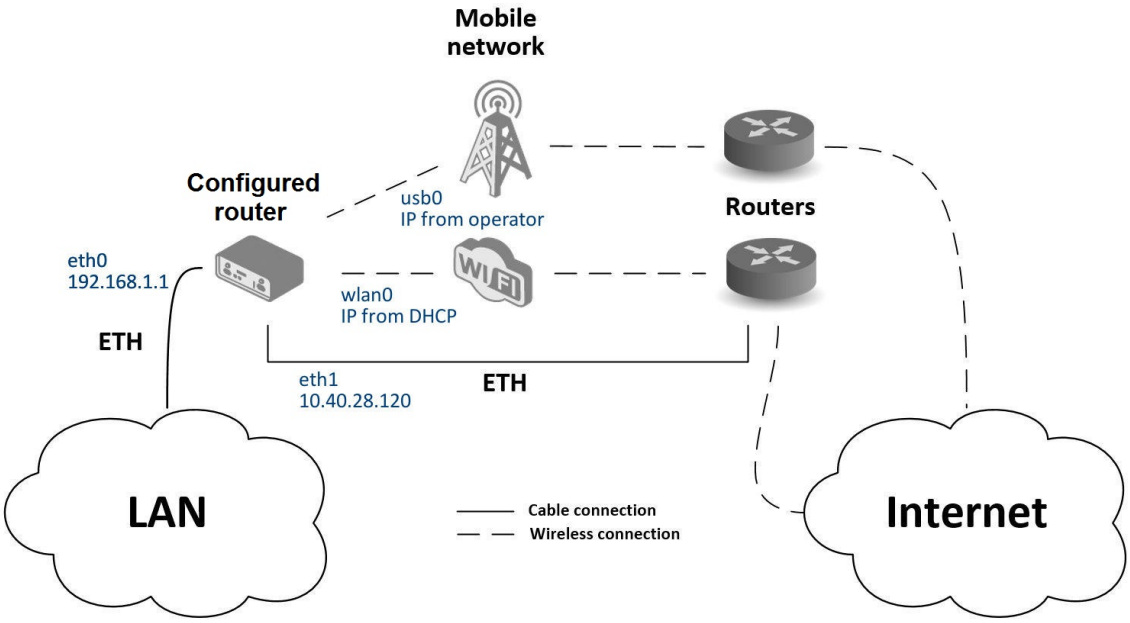


Figure 101: Backup access to the Internet – sample topology

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.

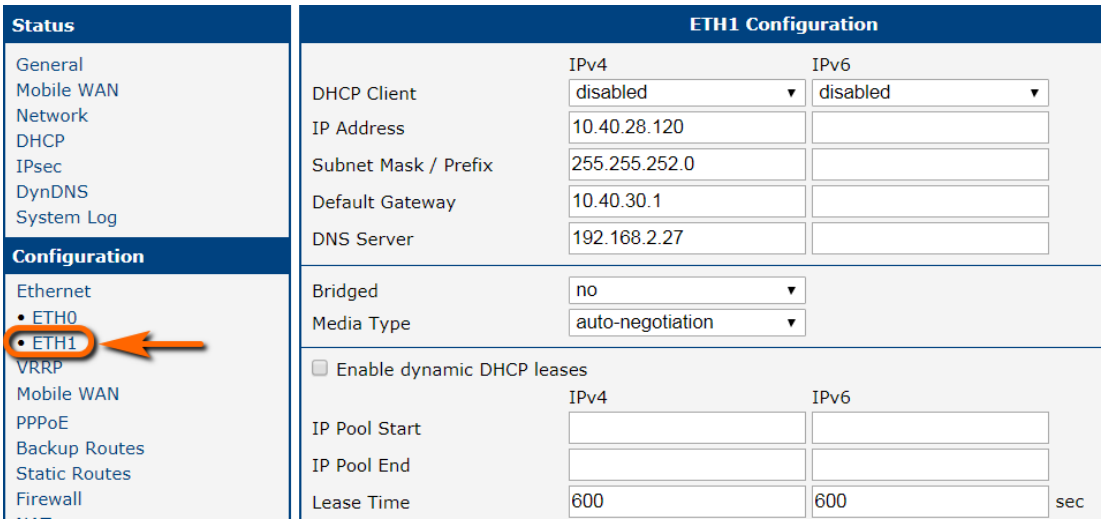


Figure 102: Backup access to the Internet – Ethernet configuration

Ethernet configuration: In the *Ethernet* → *ETH0* item, 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 *ETH1* menu item. Connect the cable to the router and set the appropriate values as in Figure 102. You may configure the static IP address, default gateway and DNS server. Changes will take effect after you click on the *Apply* button. Detailed Ethernet 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 103. Check the *Enable WiFi STA*, enable the DHCP client and fill in the adresses 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`.

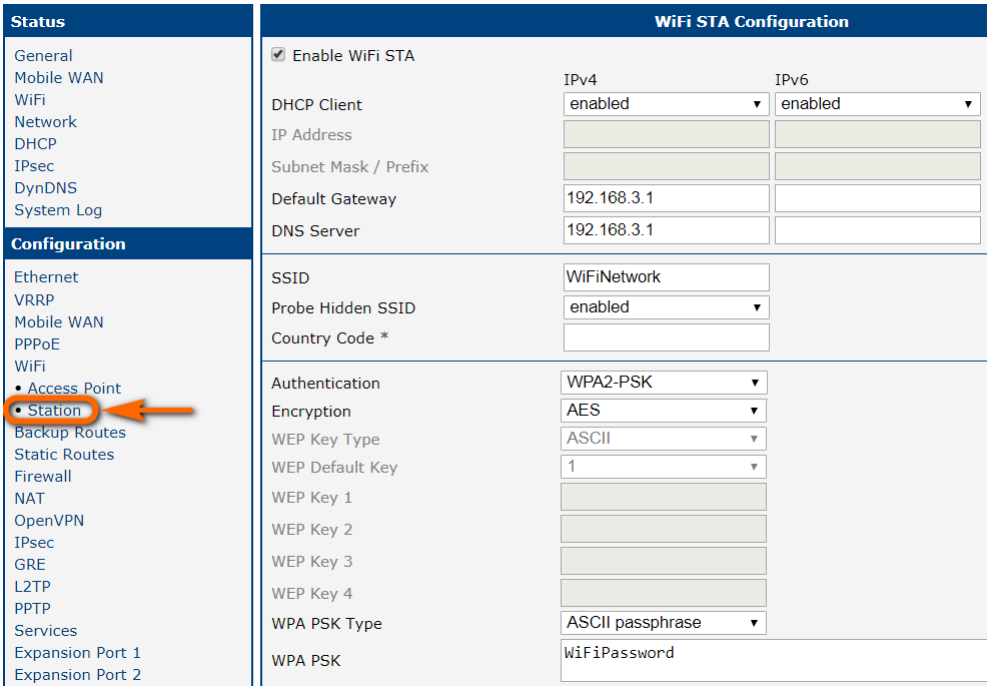


Figure 103: Backup access to the Internet – WiFi configuration

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 104.) 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.

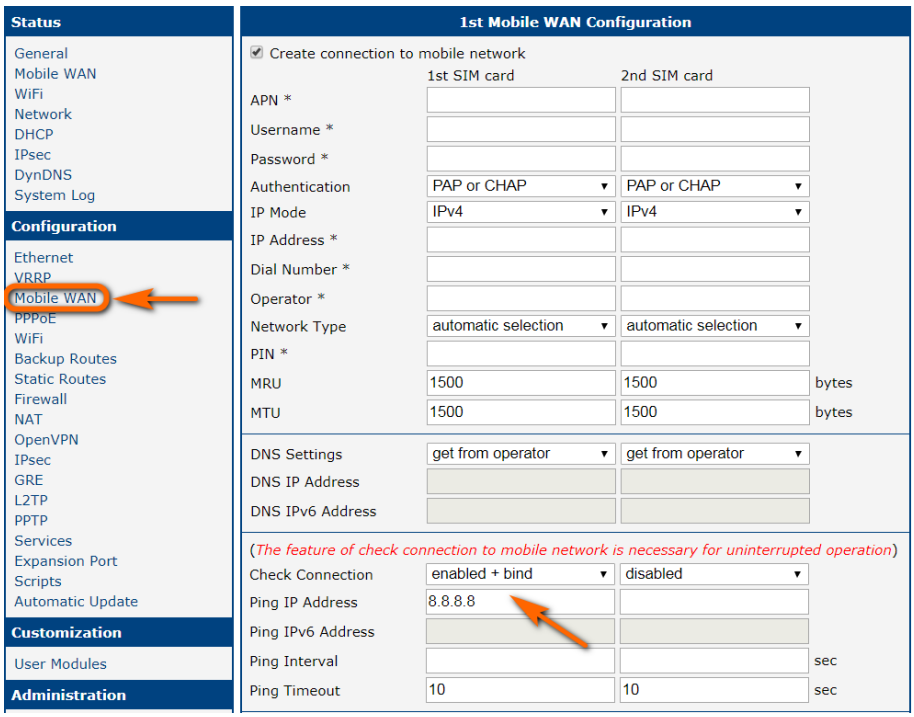


Figure 104: Backup access to the Internet – Mobile WAN configuration

Backup Routes configuration: After setting up the backup routes you will need to set their priorities. In Figure 105, 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.

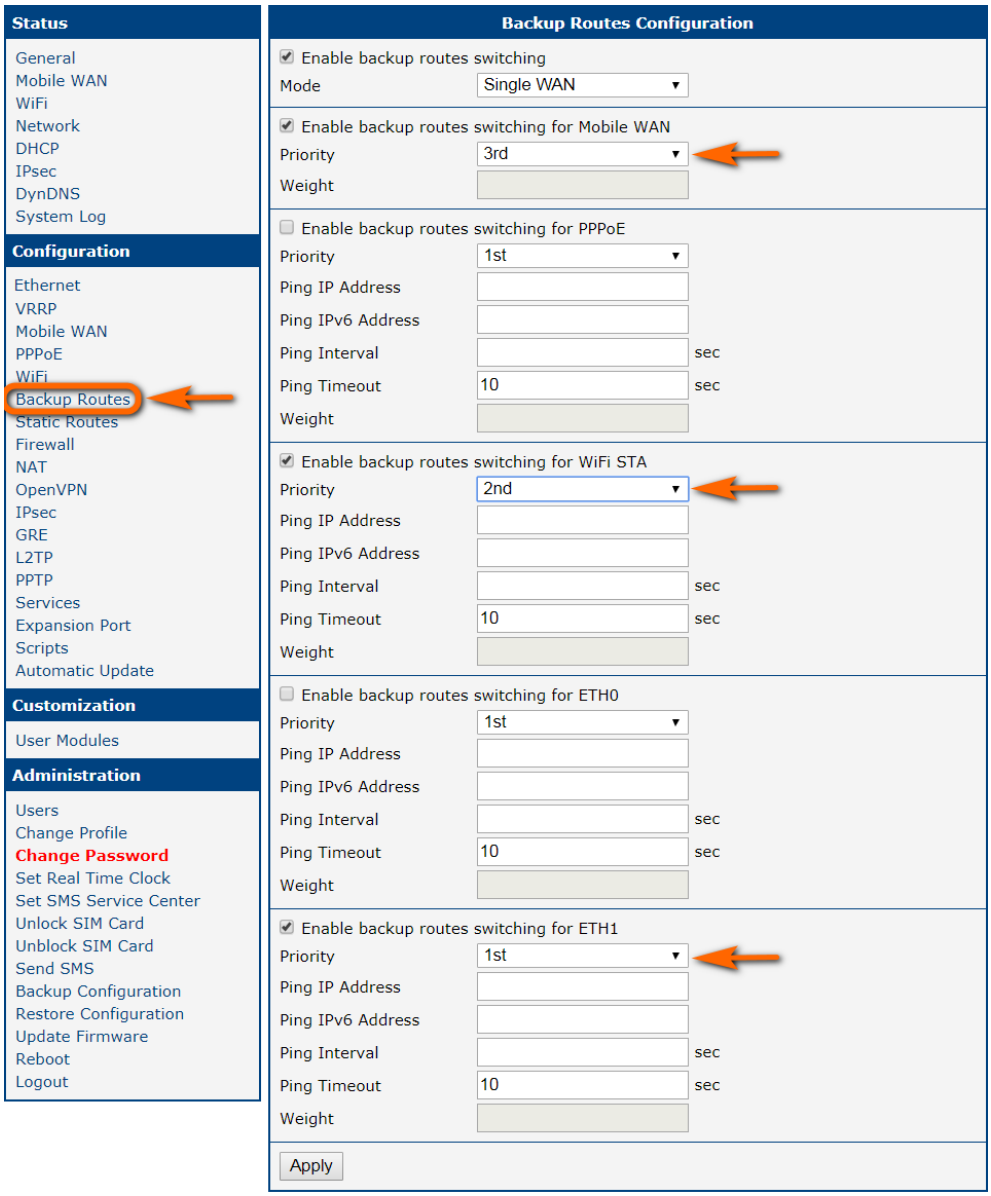


Figure 105: Backup access to the Internet – Backup Routes configuration

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

6.3 Secure Networks Interconnection or Using VPN

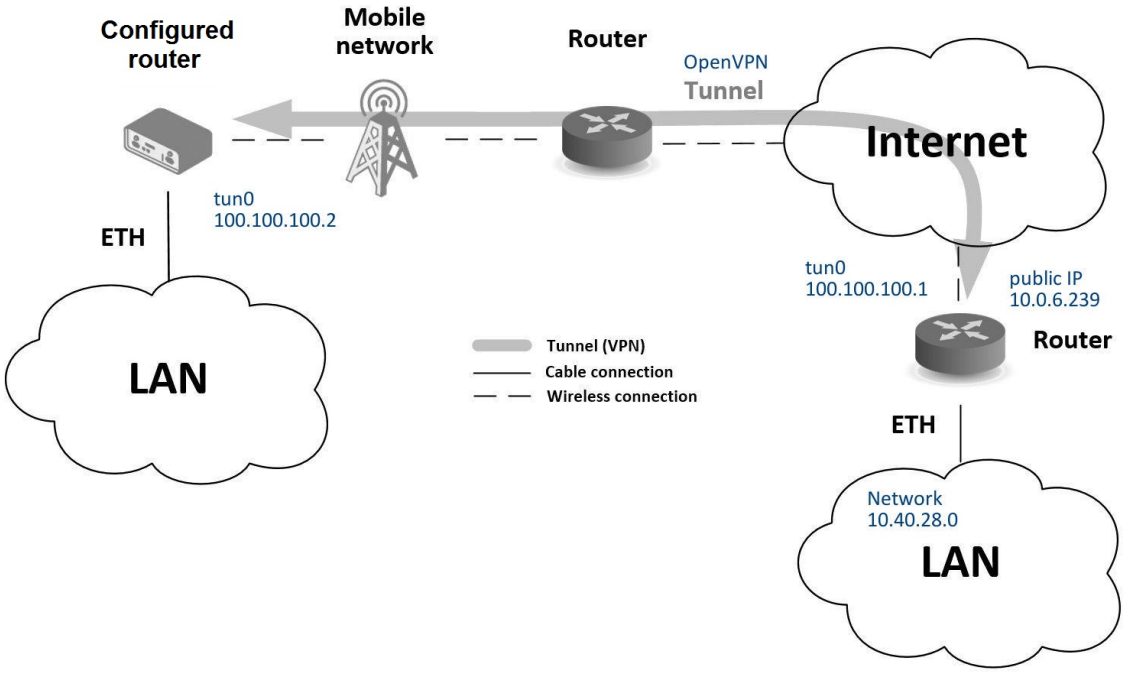


Figure 106: Secure networks interconnection – sample topology

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. 106. 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 Figure 106. 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].

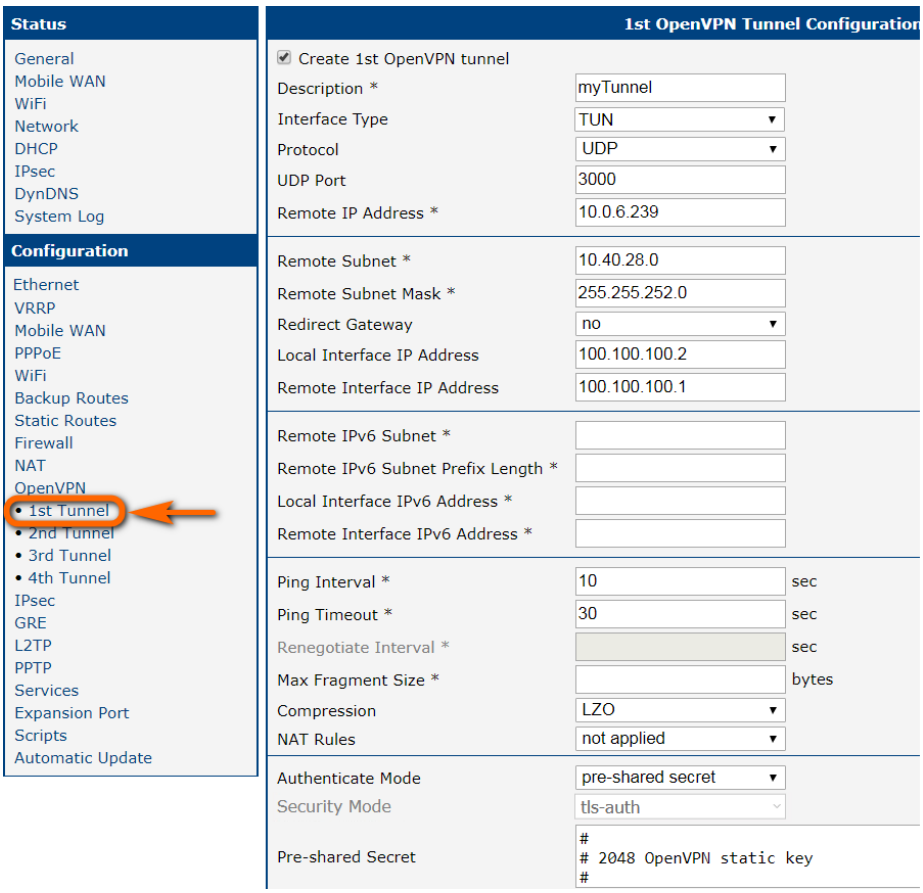


Figure 107: Secure networks interconnection – OpenVPN configuration

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).

6.4 Serial Gateway

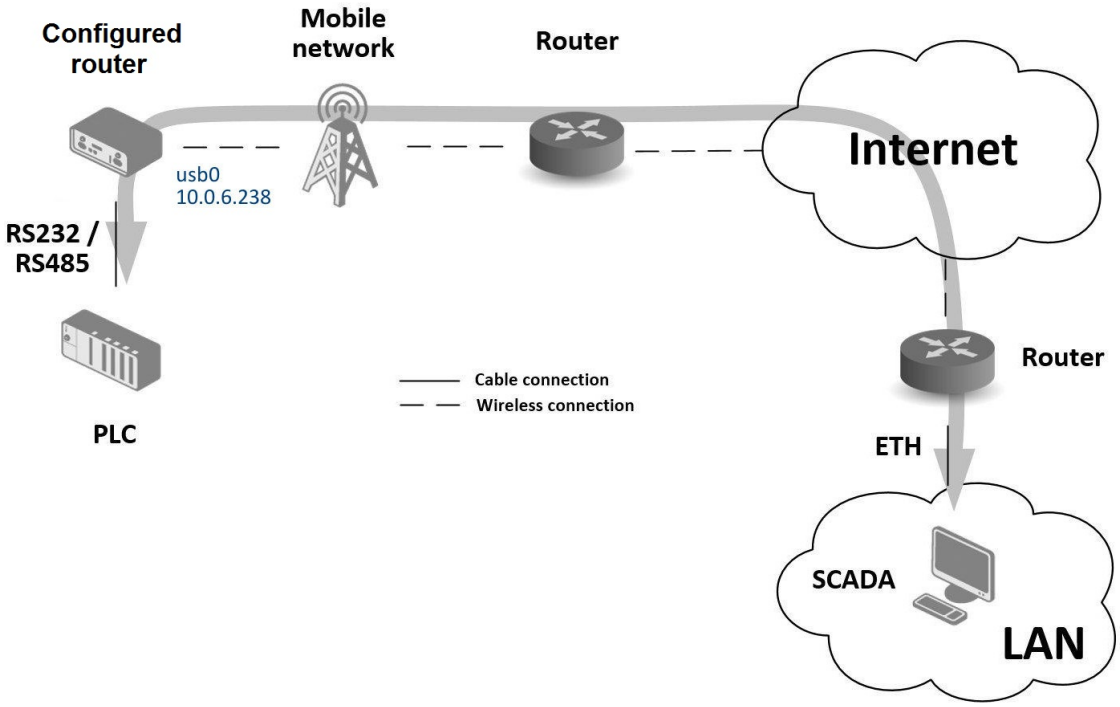


Figure 108: Serial Gateway – sample topology

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. 108.) 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. 109.) 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.

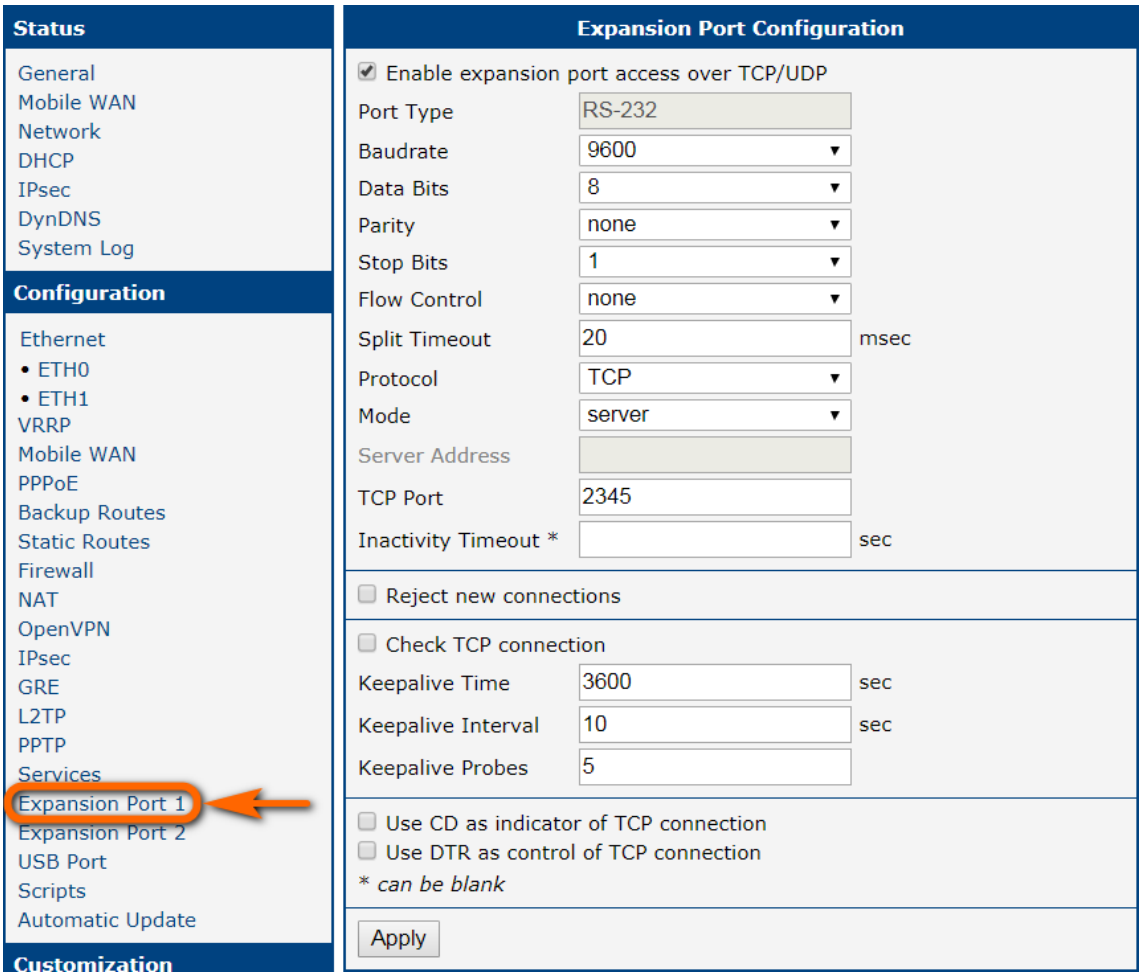


Figure 109: Serial Gateway – konfigurace *Expansion Port 1*

To communicate with the serial device (PLC), connect from the PC (Labeled as SCADA in Fig. 108) 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.

7. Customization

7.1 Router Apps

You may run custom software programs, called *Router Apps* (formerly *User Modules*), in the router to enhance the router's features. Use the *Router Apps* menu item, see Figure 110, to add a new application to the router, remove them, or change its configuration. First, use the *Choose File* button to select the app (compiled application has `*.tgz` extension). Next, use the *Add or Update* button to add an application to the router.

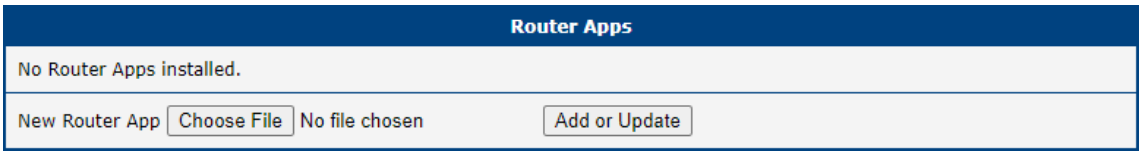


Figure 110: Router Apps GUI

The new application appears in the list of router apps on the same page; see Figure 111. If the application contains an `index.html` or `index.cgi` page, the router app name serves as a link to this page. The router app can be deleted using the *Delete* button.

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

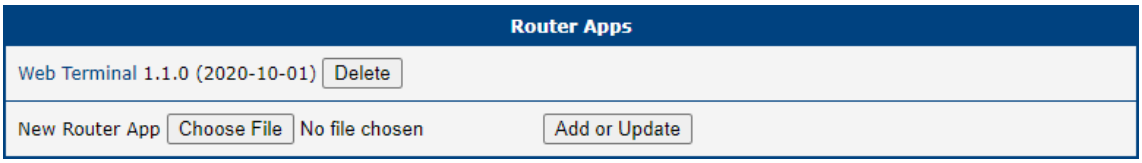


Figure 111: Router Apps Added

Advantech has prepared many Router Apps in *Connectivity*, *Routing*, *Services*, *Administration*, *Protocol Conversion*, *Node-RED*, *Integration*, and *Development* categories. These programs are available for free on the *Router Apps* webpage.

The programming and compiling of router applications is described in the Application Note *Programming of Router Apps* [14].

8. Glossary and Acronyms

B | D | G | H | I | L | N | O | P | R | S | T | U | V | W | X

B

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.

D

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.

G

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.

H

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.

I

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.

L

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.

N

NAT In computer networking, Network Address Translation (NAT) is the process of modifying IP address information in IPv4 headers while in transit across a traffic routing device.

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

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

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

O

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.

P

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.

R

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

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

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

S

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 se-

curely 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.

T

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.

U

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.

V

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).

W

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

WebAccess/DMP WebAccess/DMP is an advanced Enterprise-Grade platform solution for provisioning, monitoring, managing and configuring Advantech's routers and IoT gateways. It provides a zero-touch enablement platform for each remote device.

WebAccess/VPN WebAccess/VPN is an advanced VPN management solution for safe interconnection of Advantech routers and LAN networks in public Internet. Connection among devices and networks can be regional or global and can combine different technology platforms and various wireless, LTE, fixed and satellite connectivities.

X

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.

Index

A

Access Point
- Configuration 50
- Information 16

Accessing the router 5
Add User 148
APN 39
AT commands 124

B

Backup Configuration 156
Backup Routes 61
Bridge 26

C

Change Password 151
Change Profile 150
Clock synchronization 108
Configuration update 144
Control SMS messages 123

D

Data limit 42
Default Gateway 26, 56
Default IP address 5
Default password 6
Default SIM card 43
Default username 6
DHCP 21, 26, 56, 171
- Dynamic 28
- Static 28

DHCPv6 21
DNS 171
DNS server 26, 41, 56
Domain Name System . . . . . *see* DNS
DoS attacks 73
Dynamic Host Configuration Protocol . . . . . *see* DHCP
DynDNS 105

E

Expansion Port
- CNT 133
- MBUS 133
- RS232 133
- RS485/422 133

F

Firewall 72
- Filtering of Forwarded Packets 72
- Filtering of Incoming Packets 72
- Protection against DoS attacks 73

Firmware update 144, 158
Firmware version 12
FTP 106

G

GRE 96, 171

H

HTTP 107

I

ICMPv6 41
IPsec 87, 172
- Authenticate Mode 92
- Encapsulation Mode 91
- IKE Mode 91

IPv4 172
IPv6 41

L

L2TP 99, 172
LAN
ETH0 26
ETH1 26
Location Area Code 13
Logout 159

M

Mobile network 39
Multiple WANs 61, 63, 71

N

NAT 76, 173
Neighbouring WiFi Networks 17
Network Address Translation ..... *see* NAT
NTP 108, 173
NTP server 151

O

Object Identifier 115
OpenVPN 81, 173
Authenticate Mode 83

P

PAM 109
Password 151
PAT 76
PIN number 153
PLMN 13
Port 173
PPPoE 48
PPPoE Bridge Mode 45
PPTP 102, 173
PUK number 154

R

RADIUS 29, 50, 53
Reboot 159
Remote access 77
Restore Configuration 157
Router 1
Accessing 5
Router Apps 170

S

Save Log 24
Save Report 24
Send SMS 155
Serial line
RS232 133
RS422 133
RS485 133
Serial number 12
Set internal clock 151
Signal Quality 13
Simple Network Management Protocol ..... *see* SNMP
SMS 121
SMS Service Center 153
SMTP 119, 174
SNMP 112, 174
SSH 130
Startup Script 142
Static Routes 71
Switch between SIM Cards 42
Syslog 131
System Log 24

T

TCP 175
Telnet 132
Transmission Control Protocol ..... *see* TCP

U

UDP 175

Unblock SIM card 154
Uniform resource locator ..... *see* URL
Unlock SIM card 153
Up/Down script 143
URL 175
Usage Profiles 150
USB
    USB/RS232 converters 139
USB Port 137
User Datagram Protocol ..... *see* UDP
Users 148

V

Virtual private network ..... *see* VPN
VPN 175
VRRP 36, 176

W

Web interface 6
WiFi
    Authentication 52, 57
    HW Mode 51
WiFi AP 50
WiFi STA 56
WiFi Station
    Configuration 56

9. Related Documents

[1] Commands and Scripts
[2] Remote Monitoring
[3] WebAccess/VPN
[4] R-SeeNet
[5] OpenVPN Tunnel
[6] IPsec Tunnel
[7] GRE Tunnel
[8] FlexVPN
[9] VLAN
[10] SNMP Object Identifiers
[11] AT Commands (AT-SMS)
[12] Quality of Service (QoS)
[13] Programming of Router Apps
[14] Security Guidelines

[EP] Product-related documents and applications can be obtained on **Engineering Portal** at `https://icr.advantech.com/download` address.

[RA] **Router Apps** (formerly *User modules*) and related documents can be obtained on *Engineering Portal* at `https://icr.advantech.com/products/router-apps` address.