

Configuration Manual

ICR-4400 Family



© 2024 Advantech Czech s.r.o. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photography, recording, or any information storage and retrieval system without written consent. Information in this manual is subject to change without notice, and it does not represent a commitment on the part of Advantech.

Advantech Czech s.r.o. shall not be liable for incidental or consequential damages resulting from the furnishing, performance, or use of this manual.

All brand names used in this manual are the registered trademarks of their respective owners. The use of trademarks or other designations in this publication is for reference purposes only and does not constitute an endorsement by the trademark holder.

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.

Firmware Version

This manual is compatible with firmware version 6.5.0 (October 8, 2024).



Contents

1. Introduction	1
1.1 Document Content	1
1.2 Device	2
1.2.1 Persistent Storage	2
1.2.2 Reset	2
1.3 Web Configuration	3
1.3.1 Managing HTTPS Certificates	5
1.3.2 Allowed and Restricted Input Characters	5
1.3.3 Supported Certificate Formats	5
1.4 Remote Management Platform	6
2. Status	7
2.1 General	7
2.1.1 Mobile Connection	7
2.1.2 Ethernet Status	8
2.1.3 WiFi	8
2.1.4 Peripheral Ports	9
2.1.5 Security Information	9
2.1.6 System Information	9
2.2 Mobile WAN	10
2.3 WiFi	13
2.4 WiFi Scan	14
2.5 Network	16
2.5.1 Connections	19
2.6 DHCP	20
2.7 IPsec	21
2.8 WireGuard	22
2.9 DynDNS	23
2.10 System Log	24
3. Configuration	26
3.1 Ethernet	26
3.1.1 DHCP Server	29
3.1.2 IPv6 Prefix Delegation	30
3.1.3 802.1X Authentication to RADIUS Server	31
3.1.4 LAN Configuration Examples	33
3.2 VLAN	39
3.3 VRRP	41
3.4 Mobile WAN	44
3.4.1 Connection to Mobile Network	45
3.4.2 DNS Address Configuration	46
3.4.3 Check Connection to Mobile Network	46
3.4.4 Check Connection Example	47
3.4.5 Data Limit Configuration	48
3.4.6 Switch between SIM Cards Configuration	48

3.4.7	Examples of SIM Card Switching Configuration	50
3.4.8	PPPoE Bridge Mode Configuration	51
3.5	PPPoE	52
3.6	WiFi Access Point	54
3.7	WiFi Station	60
3.8	Bluetooth Support	65
3.9	Backup Routes	66
3.9.1	Default Priorities for Backup Routes	66
3.9.2	User Customized Backup Routes	67
3.9.3	Backup Routes Examples	70
3.10	Static Routes	76
3.11	Firewall	77
3.11.1	Sites	79
3.11.2	Example of the IPv4 Firewall Configuration	80
3.12	NAT	82
3.12.1	Examples of NAT Configuration	85
3.13	OpenVPN Tunnel	87
3.13.1	Example of the OpenVPN Tunnel Configuration in IPv4 Network	91
3.14	IPsec	92
3.14.1	Route-based Configuration Scenarios	92
3.14.2	IPsec Authentication Scenarios	93
3.14.3	Configuration Items Description	94
3.14.4	Basic IPv4 IPsec Tunnel Configuration	99
3.14.5	TPM-based Authentication	100
3.15	WireGuard	101
3.15.1	WireGuard IPv4 Tunnel Configuration Example	103
3.16	GRE Tunnels	105
3.16.1	Example of the GRE Tunnel Configuration	106
3.17	L2TP Tunnel	108
3.17.1	Example of the L2TP Tunnel Configuration	110
3.18	PPTP	111
3.18.1	Example of the PPTP Tunnel Configuration	113
3.19	Services	114
3.19.1	Authentication	114
3.19.2	DynDNS	118
3.19.3	FTP	119
3.19.4	HTTP	120
3.19.5	NTP	121
3.19.6	SNMP	122
3.19.7	SMTP	126
3.19.8	SMS	127
3.19.9	SSH	135
3.19.10	Syslog	136
3.19.11	Telnet	138
3.20	Expansion Port 1 & 2, USB Port	139
3.20.1	Examples of the Expansion Port Configuration	142
3.21	Scripts	143
3.21.1	Startup Script	143
3.21.2	Example of Startup Script	143
3.21.3	Up/Down Scripts	143

3.21.4 Example of IPv6 Up/Down Script	144
3.22 Automatic Update	145
3.22.1 Example of Automatic Update	147
3.22.2 Example of Automatic Update Based on MAC	148
4. Customization	149
4.1 Router Apps	149
4.2 Settings	151
4.3 FirstNet Router App	152
5. Administration	153
5.1 Manage Users	153
5.2 Modify User	155
5.2.1 Two-Factor Authentication	156
5.2.2 Passwordless Console Login	159
5.2.3 Expired Password	161
5.3 Change Profile	162
5.4 Set Date and Time	163
5.5 Set SMS Service Center	164
5.6 Unlock SIM Card	164
5.7 Unblock SIM Card	165
5.8 Send SMS	165
5.9 Backup Configuration	166
5.10 Restore Configuration	167
5.11 Update Firmware	168
5.12 Reboot	169
5.13 Logout	169
6. Typical Situations	170
6.1 Access to the Internet from LAN	170
6.2 Backup Access to the Internet from LAN	172
6.3 Secure Networks Interconnection or Using VPN	176
6.4 Serial Gateway	178
Appendix A: Open Source Software License	180
Appendix B: Glossary and Acronyms	181
Appendix C: Index	182
Appendix D: Related Documents	184

List of Figures

1	Web Configuration GUI	4
2	Mobile WAN Status	11
3	WiFi Status	13
4	WiFi Scan Output Example	14
5	Network Status	18
6	Connection List	19
7	DHCP Status	20
8	IPsec Status	21
9	WireGuard Status Page	22
10	DynDNS Status	23
11	System Log	24
12	Example program syslogd start with the parameter -R	25
13	LAN Configuration Page	26
14	IPv6 Address with Prefix Example	30
15	IEEE 802.1X Functional Diagram	31
16	Network Topology for Example 1	33
17	LAN Configuration for Example 1	34
18	Network Topology for Example 2	35
19	LAN Configuration for Example 2	36
20	Network Topology for Example 3	37
21	LAN Configuration for Example 3	38
22	VLAN Configuration Form	39
23	Topology of VRRP Configuration Example	42
24	Example of VRRP Configuration – Main Router	42
25	Example of VRRP Configuration – Backup Router	43
26	Mobile WAN Configuration	44
27	Check Connection Example	47
28	Configuration for SIM card switching Example 1	50
29	Configuration for SIM card switching Example 2	51
30	PPPoE Configuration	52
31	WiFi Access Point Configuration Page	59
32	WiFi Station Configuration Page	60
33	Backup Routes Configuration Page	69
34	Example #1: GUI Configuration	70
35	Example #1: Topology	70
36	Example #2: GUI Configuration	71
37	Example #2: Topology	71
38	Example #3: GUI Configuration	72
39	Example #3: Topology for <i>Single WAN</i> mode	73
40	Example #3: Topology for <i>Multiple WAN</i> mode	73
41	Example #4: GUI Configuration	74
42	Example #4: Topology	74
43	Example #5: GUI Configuration	75
44	Example #5: Topology	75
45	Static Routes Configuration Page	76
46	Firewall Configuration – IPv6 Firewall	77
47	Firewall Sites Configuration GUI	79

48	Topology for the IPv4 Firewall Configuration Example	80
49	IPv4 Firewall Configuration Example	81
50	NAT Configuration Page	83
51	Topology for NAT Configuration Example 1	85
52	NAT Configuration for Example 1	85
53	Topology for NAT Configuration Example 2	86
54	NAT Configuration for Example 2	86
55	OpenVPN tunnel configuration Page	90
56	Topology of OpenVPN Configuration Example	91
57	IPsec Tunnels Configuration Page	94
58	Topology of IPsec Configuration Example	99
59	WireGuard Tunnels Configuration Page	102
60	Topology of WireGuard Configuration Example	103
61	Router A – WireGuard Status Page and Route Table	104
62	Router B – WireGuard Status Page and Route Table	104
63	GRE Tunnel Configuration Page	106
64	Topology of GRE Tunnel Configuration Example	106
65	L2TP Tunnel Configuration Page	108
66	Topology of L2TP Tunnel Configuration Example	110
67	PPTP Tunnel Configuration Page	111
68	Topology of PPTP Tunnel Configuration Example	113
69	Common Configuration Items	114
70	Configuration of RADIUS	116
71	Configuration of TACACS+	117
72	DynDNS Configuration Example	118
73	Configuration of FTP server	119
74	HTTP Configuration Page	120
75	NTP Configuration Page	121
76	OID Basic Structure	123
77	SNMP Configuration Example	124
78	MIB Browser Example	125
79	SMTP Client Configuration Example	126
80	SMS Configuration for Example 1	131
81	SMS Configuration for Example 2	132
82	SMS Configuration for Example 3	133
83	SMS Configuration for Example 4	134
84	SSH Configuration Page	135
85	Syslog Configuration Page	136
86	Telnet Configuration Page	138
87	Expansion Port Configuration	139
88	Example of Ethernet to serial communication configuration	142
89	Example of serial interface configuration	142
90	Example of a Startup Script	143
91	Example of IPv6 Up/Down Script	144
92	Automatic Update	145
93	Example of Automatic Update 1	147
94	Example of Automatic Update 2	148
95	Default Router Apps GUI	149
96	Router Apps GUI with Available Online Apps	150
97	Router Apps Settings	151

98	FirstNet Router App – Global Status	152
99	Modify User Page	153
100	Users Administration Form	155
101	Links for Google Authenticator Application	157
102	Links for Authenticator-Extension	157
103	Standard Login	158
104	Verification Code	158
105	SSH Login	158
106	Key Generation	159
107	Expired Password Prompt	161
108	Change Profile	162
109	Set Real Time Clock	163
110	Set SMS Service Center Address	164
111	Unlock SIM Card	164
112	Unblock SIM Card	165
113	Send SMS	165
114	Backup Configuration	166
115	Restore Configuration	167
116	Update Firmware Administration Page	168
117	Process of Firmware Update	169
118	Reboot	169
119	Access to the Internet from LAN – sample topology	170
120	Access to the Internet from LAN – <i>Ethernet</i> configuration	171
121	Access to the Internet from LAN – <i>Mobile WAN</i> configuration	171
122	Backup access to the Internet – sample topology	172
123	Backup access to the Internet – Ethernet configuration	172
124	Backup access to the Internet – WiFi configuration	173
125	Backup access to the Internet – Mobile WAN configuration	174
126	Backup access to the Internet – Backup Routes configuration	175
127	Secure networks interconnection – sample topology	176
128	Secure networks interconnection – OpenVPN configuration	177
129	Serial Gateway – sample topology	178
130	Serial Gateway – konfigurace <i>Expansion Port 1</i>	179

List of Tables

1	Reset Storage Actions	2
2	Mobile Connection	8
3	PoE PSE Status	8
4	Peripheral Ports	9
5	System Information	9
6	Mobile Network Information	10
7	Signal Strength Value Ranges	11
8	Description of Periods	12
9	Mobile Network Statistics	12
10	Detailed Information about WiFi Networks	15
11	Description of Interfaces in Network Status	16
12	Description of Information in Network Status	17
13	DHCP Status Description	20
14	Configuration of the Network Interface – IPv4 and IPv6	27
15	Configuration of the Network Interface – Global Items	28
16	Configuration of Dynamic DHCP Server	29
17	Configuration of Static DHCP Server	29
18	IPv6 Prefix Delegation Configuration	30
19	Supported Roles for IEEE 802.1X Authentication	32
20	Configuration of 802.1X Authentication	32
21	VLAN Configuration Options	40
22	VRRP Configuration Items Description	41
23	Check Connection	42
24	Mobile WAN Configuration Items Description	45
25	Check Connection to Mobile Network Configuration	47
26	Data Limit Configuration	48
27	Switch between SIM cards configuration	49
28	Parameters for SIM card switching	50
29	PPPoE Configuration	53
30	WiFi Configuration Items Description	58
31	WLAN Configuration Items Description	64
32	Backup Routes Modes Items Description	67
33	Backup Routes Configuration Items Description	68
34	Static Routes Configuration for IPv4	76
35	Filtering of Incoming Packets	78
36	Forwarding filtering	79
37	NAT Configuration Items Description	82
38	Remote Access Configuration	83
39	Incoming Packets Configuration	84
40	Masquerade Configuration	84
41	OpenVPN Configuration Items Description	89
42	OpenVPN Configuration Example	91
43	IPsec Tunnel Configuration Items Description	98
44	Simple IPv4 IPsec Tunnel Configuration	99
45	WireGuard Tunnel Configuration Items Description	102
46	WireGuard IPv4 Tunnel Configuration Example	103
47	GRE Tunnel Configuration Items Description	105

48	GRE Tunnel Configuration Example	107
49	L2TP Tunnel Configuration Items Description	109
50	L2TP Tunnel Configuration Example	110
51	PPTP Tunnel Configuration Items Description	112
52	PPTP Tunnel Configuration Example	113
53	Enter Caption	115
54	Configuration of RADIUS	116
55	Configuration of TACACS+	117
56	DynDNS Configuration Items Description	118
57	FTP Configuration Items Description	119
58	HTTP Configuration Items Description	120
59	NTP Configuration Items Description	121
60	SNMP Agent Configuration	122
61	SNMPv3 Configuration	122
62	SNMP Configuration (R-SeeNet)	123
63	Object identifier for binary inputs and output	124
64	SMTP Client Configuration	126
65	SMS Configuration	127
66	Control via SMS	128
67	Control SMS	128
68	Send SMS on the serial Port 1	129
69	Send SMS on the serial Port 2	129
70	Sending/receiving of SMS on TCP port specified	129
71	List of AT Commands	130
72	SSH Configuration Items Description	135
73	Syslog Configuration Items Description	137
74	Telnet Configuration Items Description	138
75	Expansion Port Configuration – serial interface	140
76	Expansion Port Configuration – <i>Check TCP connection</i>	140
77	CD Signal Description	140
78	DTR Signal Description	141
79	Automatic Update Options	146
80	Router Apps Settings	151
81	Action Button Description	154
82	User Parameters	154

1. Introduction

1.1 Document Content

This manual provides detailed setup procedures for Advantech ICR-4400 family routers, offering comprehensive guidance on the following topics:

- Web configuration interface for the routers – detailed in Chapter 1.3.
- Overview of available remote management system – see Chapter 1.4.
- Detailed configuration instructions, item by item, following the web interface's structure:
 - Status – discussed in Chapter 2.
 - Configuration – outlined in Chapter 3.
 - Customization – covered in Chapter 4.
 - Administration – explained in Chapter 5.
- Configuration examples for typical scenarios – presented in Chapter 6.



For detailed information on topics such as ordering, hardware features, initial setup, and technical specifications, refer to the **Hardware Manual** available on the [Engineering Portal](#).

1.2 Device

1.2.1 Persistent Storage

The persistent storage of the device has three partitions that are combined into a single directory structure:

- **Firmware data:** Permanent system data distributed with firmware upgrades.
- **User/RA data:** Separate storage for user data, visible as `/var/data` and for Router Apps, visible as `/opt`.

1.2.2 Reset



Before initiating a factory reset on the router, consider creating a backup of its configuration.

The *RST* button serves three different purposes:

- **Reset:** Hold the *RST* button for **less than 4 seconds**; the router will reboot, applying its customized configuration. You can also trigger the router reset by selecting the *Reboot* menu option in the router web GUI.
- **Configuration Reset:** To restore the router to its default factory configuration, press and hold the *RST* button for **more than 4 seconds**. The *PWR* LED will turn off and then back on. It's recommended to hold the *RST* button for an additional 1 second after the *PWR* LED comes on.
- **Factory Reset**¹: If the router fails to boot due to incorrect configuration or filesystem error, power off the router by disconnecting its power supply. Then, while holding the *RST* button, power on the router and continue holding the *RST* button for **at least 10 seconds**.

The following table summarizes what storage areas will be retained (kept) and what will be deleted during a Reset.

Storage	Reset	Conf. Reset	Fact. Reset
Configuration	Keep	Keep	Keep
User data	Keep	Keep	Delete

Table 1: Reset Storage Actions

¹Available on some product platforms only.

1.3 Web Configuration



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



Please note that if you are logged in to the router GUI with the *User* role, you will have read-only access to the GUI, except for *Modify User*, and some menu items may be unavailable.

The router supports configuration via a **web browser** or **Secure Shell** (SSH). This manual primarily covers web browser configuration. For console configuration commands, refer to the *Command Line Interface* Application Note. For more information on enhancing the router's basic functionality, refer to the *Extending Router Functionality* 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 1.4.

Configuration of routers is efficiently performed through 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 1).

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 1.3.1.

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



It is highly recommended to have JavaScript enabled in the browser; otherwise, field validation and some functions will be disabled.



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

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 3.19.6).

Status	General Status refresh
General	
Mobile WAN	
WiFi	
Network	
DHCP	
IPsec	
WireGuard	
DynDNS	
System Log	
Configuration	
Ethernet	
VLAN	
VRRP	
Mobile WAN	
PPPoE	
WiFi	
Backup Routes	
Static Routes	
Firewall	
NAT	
OpenVPN	
IPsec	
WireGuard	
GRE	
L2TP	
PPTP	
Services	
Expansion Port 1	
Expansion Port 2	
USB Port	
Scripts	
Automatic Update	
Customization	
Router Apps	
Settings	
Administration	
Manage Users	
Change Profile	
Set Date and Time	
Set SMS Service Center	
Unlock SIM Card	
Unblock SIM Card	
Send SMS	
Backup Configuration	
Restore Configuration	
Update Firmware	
Reboot	
Logout	
	General Status refresh
	Mobile Connection
	SIM Card : 1st IP Address : 10.80.0.46 IPv6 Address : Unassigned Rx Data : 908 B Tx Data : 1.4 KB Uptime : 0 days, 16 hours, 36 minutes » More Information «
	ETH0
	IP Address : 10.64.0.94 / 255.255.252.0 IPv6 Address : fd00:a40::94 / 56 MAC Address : 02:AD:FF:00:00:94 Rx Data : 7.1 MB Tx Data : 341.4 KB » More Information «
	ETH1
	IP Address : 10.65.0.94 / 255.255.252.0 IPv6 Address : fd00:a41::94 / 56 MAC Address : 02:AD:FF:01:00:94 Rx Data : 130.3 KB Tx Data : 25.6 KB » More Information «
	ETH2
	IP Address : 10.66.0.94 / 255.255.252.0 IPv6 Address : fd00:a42::94 / 56 MAC Address : 02:AD:FF:02:00:94 Rx Data : 125.6 KB Tx Data : 25.6 KB » More Information «
	WiFi AP 1
	IP Address : Unassigned IPv6 Address : Unassigned MAC Address : 04:F0:21:67:3C:B7 » More Information «
	WiFi STA
	IP Address : Unassigned IPv6 Address : Unassigned MAC Address : 04:F0:21:68:3C:B7 » More Information «
	Peripheral Ports
	Expansion Port 1 : RS-232 Expansion Port 2 : RS-485 Binary Input 0 : On Binary Input 1 : On Binary Output 0 : On Binary Output 1 : Off
	Security Information
	User : root Last login : 2024-09-22 18:50:55 from 10.64.0.1 (ssh, 04:d9:f5:15:33:58) Failed logins : 0
	System Information
	Firmware Version : 6.5.0-alpha (2024-09-22) TEST #2766 Serial Number : ACZ119900000942 Hardware UUID : N/A Product Revision : N/A Profile : Standard Free space : 708 MB for apps, 473 MB for data Supply Voltage : 23.9 V Temperature : 51 °C Time : 2024-09-23 11:28:02 Uptime : 0 days, 16 hours, 37 minutes » More Information « » Licenses «

Figure 1: Web Configuration GUI

1.3.1 Managing HTTPS Certificates

The router includes a self-signed HTTPS certificate. Since the identity of this certificate cannot be validated, web browsers may display a warning message. To avoid 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), replace the `/etc/certs/https_cert` and `/etc/certs/https_key` files on the router. This can easily be done via the GUI on the *HTTP* configuration page, as detailed in Chapter 3.19.4.

To use the router's self-signed certificate without encountering the security warning (due to domain name mismatch) 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 example, 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 (e.g., `https://00-11-22-33-44-55`). If the security warning appears, add an exception to prevent it from recurring (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: Using a domain name based on the router's MAC address may not be compatible with all operating system and browser combinations.

1.3.2 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 just password fields. Below are the valid and forbidden characters for input. Note that in some cases, the "space" character may also be disallowed.

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

Forbidden characters include: `" $ & ' () ; < > \ ^ ` |`

It is important to follow these guidelines during configuration, as entering invalid characters can lead to errors or unintended behavior.

1.3.3 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`

1.4 Remote Management Platform

WebAccess/DMP is an advanced, enterprise-grade platform for provisioning, monitoring, managing, and configuring Advantech's routers and IoT gateways. It offers 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.

2. 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.

2.1 General

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.



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

2.1.1 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

Continued on next page

Continued from previous page

Item	Description
Uptime	Indicates how long the connection to the cellular network has been established

Table 2: Mobile Connection

2.1.2 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 3.1.

PoE PSE Status

If the router is equipped with the PoE PSE board, there is information about it in the appropriate Ethernet section; see the table below for a description.

Item	Description
LAN1 PoE PSE LAN2 PoE PSE LAN3 PoE PSE LAN4 PoE PSE	<ul style="list-style-type: none"> • Disabled – PoE PSE is disabled in an <i>Ethernet</i> configuration page. • Undervoltage – Undervoltage, router power supply does not meet the PoE required voltage. • Overcurrent / incompatible device – Overcurrent, a higher current than the permissible positive difference of the nominal current or a PoE incompatible device connected. • Idle – PoE PSE is enabled but currently not used (any device powered). • Class 0 – Power level (classification unimplemented) • Class 1 – Power level (very low power) • Class 2 – Power level (low power) • Class 3 – Power level (mid power) • Class 4¹ – Power level (high power)
PoE PSE Power ²	Power of PoE PSE [W]
PoE PSE Voltage ²	Voltage of PoE PSE [V]
PoE PSE Current ²	Current of PoE PSE [mA]

Table 3: PoE PSE Status

2.1.3 WiFi

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 3.6. *WiFi STA* part displays information for the WiFi interface (wlan1) working in station mode, for the configuration description see Chapter 3.7.

¹Valid for *IEEE 802.3at/PoE+ Type 2* devices, not allowed for *IEEE 802.3at/PoE Type 1* devices.

²Visible only when the PoE is enabled, and an external device is powered.

2.1.4 Peripheral Ports

Item	Description
Expansion Port 1	An interface detected on the first expansion port.
Expansion Port 2	An interface detected on the second expansion port.
Binary Input 0	State of the first binary input.
Binary Input 1	State of the second binary input.
Binary Output 0	State of the first binary output.
Binary Output 1	State of the second binary output.

Table 4: Peripheral Ports

2.1.5 Security Information

This section provides information about the logged-in user, their last login time, IP address, and the number of failed login attempts.

2.1.6 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).
Free space	Free space available for Router Apps and user data.
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).
Power Board ²	Detected type of the PoE extension board.
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 5: System Information

¹It may not be available for some models.

²Only for models with PoE. The router's power supply voltage must meet the required voltage.

2.2 Mobile WAN



The ICR-4401 (LAN version) has no the *Mobile WAN* status menu 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) is for 2G/3G networks and TAC (Tracking Area Code) is for 4G networks.
Channel	Channel the router communicates on <ul style="list-style-type: none"> • 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 7.
Signal Quality	Signal quality of the selected cell: <ul style="list-style-type: none"> • EC/IO for UMTS (it's the ratio of the signal received from the pilot channel – EC – to the overall level of the spectral density, ie the sum of the signals of other cells – IO). • RSRQ for LTE technology (Defined as the ratio $\frac{N \times RSRP}{RSSI}$). • The value is not available for the EDGE technology.
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: <ul style="list-style-type: none"> • 2 – 9 = Marginal, • 10 – 14 = OK, • 15 – 19 = Good, • 20 – 30 = Excelent.
Manufacturer	Module manufacturer
Model	Type of module
Revision	Revision of module
IMEI	IMEI (International Mobile Equipment Identity) number of module
ICCID	Integrated Circuit Card Identifier is international and unique serial number of the SIM card.

Table 6: Mobile Network Information

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 2: Mobile WAN Status

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	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 7: Signal Strength Value Ranges

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 8: 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 9: 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.

2.3 WiFi



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.

```
WiFi Status refresh  
  
WiFi Module Information  
Chip : Qualcomm Atheros QCA6174A-5  
Firmware : WLAN.RM.4.4.1.c3-00059  
Supports : 1 station and 2 access points  
  
WiFi AP 1 Status  
AP status is not available.  
  
WiFi AP 2 Status  
AP status is not available.  
  
WiFi STA Status  
STA status is not available.
```

Figure 3: WiFi Status

2.4 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 4.

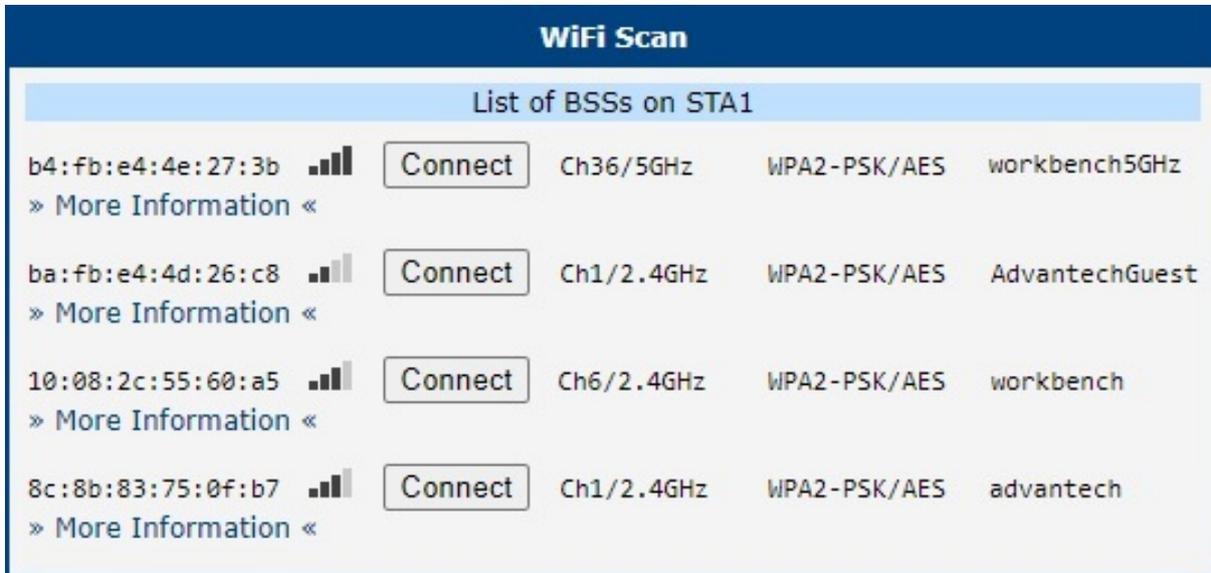


Figure 4: WiFi Scan Output Example

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).
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.

Continued on next page

Continued from previous page

Item	Description
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 10: Detailed Information about WiFi Networks

2.5 Network

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:

Note: Some interfaces may not be available on your router.

Interface	Description
ethx	Ethernet interfaces
lanx	LAN interfaces
lo	Local loopback interface
nat64	Network interface of internal translator gateway between IPv6 and IPv4 addresses.
switch0	SWITCH interface
usbx	Active connection to the mobile network – wireless module is connected via USB interface.
wlanx	WiFi interfaces – if configured
pppx	PPP interfaces (e.g. PPPoE tunnel – if configured)
tunx	OpenVPN tunnel interfaces – if configured
ipsecx	IPSec tunnel interfaces – if configured
grex	GRE tunnel interfaces – if configured
wgx	WireGuard tunnel interfaces – if configured

Table 11: Description of Interfaces in Network Status

The following information can be displayed for network interfaces:

Item	Description
HWaddr	Hardware (unique, MAC) address of a network interface.
inet addr	IPv4 address of interface
inet6 addr	IPv6 address of interface. There can be more of them for single network interface.
P-t-P	IP address of the opposite end (in case of point-to-point connection).
Bcast	Broadcast address
Mask	Mask of network
MTU	Maximum packet size that the equipment is able to transmit.
Metric	Number of routers the packet must go through.
RX	<ul style="list-style-type: none"> • packets – received packets • errors – number of errors • dropped – dropped packets • overruns – incoming packets lost because of overload. • frame – wrong incoming packets because of incorrect packet size.

Continued on next page

Continued from previous page

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

Table 12: Description of Information in Network Status

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

The *Route Table* is displayed at the bottom of the *Network Status* page. There is *IPv4 Route Table* and *IPv6 Route Table* below.

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

refresh

Network Status

Interfaces

```

eth0    Link encap:Ethernet HWaddr 02:AD:FF:00:00:91
        inet addr:10.64.0.91 Bcast:10.64.3.255 Mask:255.255.252.0
        inet6 addr: fe80::ad:ffff:fe00:91/64 Scope:Link
        inet6 addr: fd00:a40:91/56 Scope:Global
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:954 errors:0 dropped:0 overruns:0 frame:0
        TX packets:749 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:82340 (80.4 KB) TX bytes:969616 (946.8 KB)

eth1    Link encap:Ethernet HWaddr 02:AD:FF:01:00:91
        inet addr:10.65.0.91 Bcast:10.65.3.255 Mask:255.255.252.0
        inet6 addr: fd00:a41:91/56 Scope:Global
        inet6 addr: fe80::ad:ffff:fe01:91/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:263 errors:0 dropped:9 overruns:0 frame:0
        TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:14419 (14.0 KB) TX bytes:680 (680.0 B)

eth2    Link encap:Ethernet HWaddr 02:AD:FF:02:00:91
        inet addr:10.66.0.91 Bcast:10.66.3.255 Mask:255.255.252.0
        inet6 addr: fe80::ad:ffff:fe02:91/64 Scope:Link
        inet6 addr: fd00:a42:91/56 Scope:Global
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:15 errors:0 dropped:0 overruns:0 frame:0
        TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1024
        RX bytes:2234 (2.1 KB) TX bytes:1008 (1008.0 B)

lan1    Link encap:Ethernet HWaddr 02:AD:FF:00:00:91
        inet6 addr: fe80::ad:ffff:fe00:91/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:967 errors:0 dropped:9 overruns:0 frame:0
        TX packets:753 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:84227 (82.2 KB) TX bytes:970216 (947.4 KB)

switch0 Link encap:Ethernet HWaddr 02:AD:FF:00:00:91
        inet6 addr: fe80::ad:ffff:fe00:91/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:1230 errors:0 dropped:0 overruns:0 frame:0
        TX packets:764 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1024
        RX bytes:125706 (122.7 KB) TX bytes:977642 (954.7 KB)
            
```

Route Table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.253.254	0.0.0.0	UG	0	0	0	usb0
10.64.0.0	0.0.0.0	255.255.252.0	U	0	0	0	eth0
10.65.0.0	0.0.0.0	255.255.252.0	U	0	0	0	eth1
10.66.0.0	0.0.0.0	255.255.252.0	U	0	0	0	eth2
10.70.0.0	0.0.0.0	255.255.252.0	U	0	0	0	wlan0
10.72.0.0	0.0.0.0	255.255.252.0	U	0	0	0	wlan02
192.168.253.254	0.0.0.0	255.255.255.255	UH	0	0	0	usb0

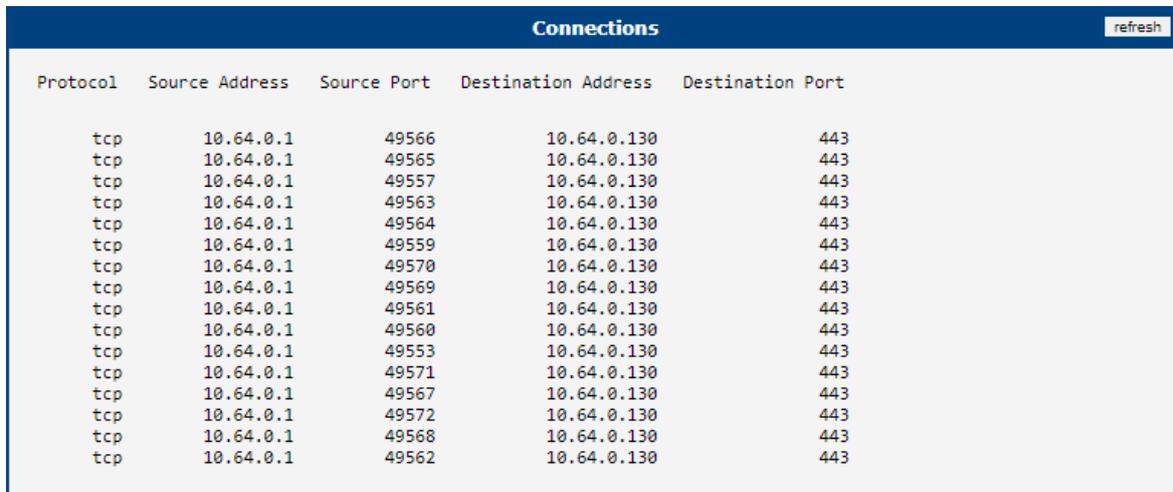
IPv6 Route Table

Destination	Next Hop	Flags	Metric	Ref	Use	Iface
64:ff9b::/96	::	U	256	1	0	nat64
ff00::/8	::	U	256	1	0	nat64
::/0	::	!n	-1	1	1	lo

Figure 5: Network Status

2.5.1 Connections

On the *Network Status* page, scroll down and click the »Connections« link. A new window listing all active router connections will display, see Figure 6.



The screenshot shows a window titled "Connections" with a "refresh" button in the top right corner. The window contains a table with five columns: Protocol, Source Address, Source Port, Destination Address, and Destination Port. The table lists 18 active TCP connections, all originating from 10.64.0.1 and destined for 10.64.0.130 on port 443. The source ports range from 49552 to 49568.

Protocol	Source Address	Source Port	Destination Address	Destination Port
tcp	10.64.0.1	49566	10.64.0.130	443
tcp	10.64.0.1	49565	10.64.0.130	443
tcp	10.64.0.1	49557	10.64.0.130	443
tcp	10.64.0.1	49563	10.64.0.130	443
tcp	10.64.0.1	49564	10.64.0.130	443
tcp	10.64.0.1	49559	10.64.0.130	443
tcp	10.64.0.1	49570	10.64.0.130	443
tcp	10.64.0.1	49569	10.64.0.130	443
tcp	10.64.0.1	49561	10.64.0.130	443
tcp	10.64.0.1	49560	10.64.0.130	443
tcp	10.64.0.1	49553	10.64.0.130	443
tcp	10.64.0.1	49571	10.64.0.130	443
tcp	10.64.0.1	49567	10.64.0.130	443
tcp	10.64.0.1	49572	10.64.0.130	443
tcp	10.64.0.1	49568	10.64.0.130	443
tcp	10.64.0.1	49562	10.64.0.130	443

Figure 6: Connection List

2.6 DHCP

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). DHCPv6 server is supported.

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

DHCP Status					refresh
Active DHCP Leases (LAN)					
IPv4 Address	Lease Starts	Lease Ends	MAC	Hostname	
192.168.2.2	2022-06-14 11:16:30	2022-06-14 11:26:30	aa:bb:cc:dd:ee:ff	"PETA-NB"	
IPv6 Address	Lease Starts	Lease Ends	IA-NA		
2001:db8::10	2022-06-14 11:20:27	2022-06-14 11:30:27	\235{P\006\000\001\000\001%y\030DP{\235\246SK		
Active DHCP Leases (WiFi AP 1)					
IPv4 Address	Lease Starts	Lease Ends	MAC	Hostname	
192.168.2.2	2022-06-14 11:30:55	2022-06-14 11:40:55	aa:bb:cc:dd:ee:ff	"Galaxy-S10"	
No active dynamic DHCPv6 Leases.					
Active DHCP Leases (WiFi AP 2)					
DHCP server is disabled.					

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 13.

Item	Description
IPv4 Address	IPv4 address assigned to a client.
IPv6 Address	IPv6 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.
IA-NA	IPv6 unique identifier.

Table 13: 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.

2.7 IPsec

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

The screenshot shows the 'IPsec Status' page with a 'refresh' button in the top right. The main content area is titled 'IPsec Tunnels Information' and displays the following text:

```
Status of IKE charon daemon (weakSwan 5.5.3, Linux 3.12.10+, armv7l):
uptime: 26 minutes, since Nov 09 10:26:10 2017
malloc: sbrk 528384, mmap 0, used 123104, free 405280
worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 5
loaded plugins: charon nonce pem openssl kernel-netlink socket-default stroke updown
Listening IP addresses:
192.168.1.1
2001:10:7:6::1
10.0.0.228
Connections:
ipsecl: 10.0.0.228...%any IKEv2, dpddelay=20s
ipsecl: local: [10.0.0.228] uses pre-shared key authentication
ipsecl: remote: uses pre-shared key authentication
ipsecl: child: 2001:10:7:6::/64 === 1999:10:7:5::/64 TUNNEL, dpdaction=clear
Security Associations (1 up, 0 connecting):
ipsecl[2]: ESTABLISHED 17 minutes ago, 10.0.0.228[10.0.0.228]...10.0.2.250[10.0.2.250]
ipsecl[2]: IKEv2 SPIs: 7e675f07f05d7434_i 8625de2fc6f84049_r*, pre-shared key reauthentication in 28 minutes
ipsecl[2]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_3072
ipsecl{2}: INSTALLED, TUNNEL, reqid 2, ESP SPIs: c7247a03_i c29f5287_o
ipsecl{2}: AES_CBC_128/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 30 minutes
ipsecl{2}: 2001:10:7:6::/64 === 1999:10:7:5::/64
```

The line 'ipsecl[2]: ESTABLISHED 17 minutes ago, 10.0.0.228[10.0.0.228]...10.0.2.250[10.0.2.250]' is highlighted with an orange box.

Figure 8: IPsec Status

2.8 WireGuard

Selecting the *WireGuard* option in the *Status* menu of the web page will bring up the information for any WireGuard Tunnels established. In the figure below is an example of the first WireGuard tunnel running.

WireGuard Tunnel Status
refresh

1st WireGuard Tunnel Information

```
interface: wg1
  public key: Zu5pZz4h05xUDGvcFN9ULr2W0oxzcL6V4Hi+WkyE63E=
  private key: (hidden)
  listening port: 51820

peer: sHvm8R8HLQM7hRtmD+/VA8c5aIuDpGfnwq371+0gMVM=
  endpoint: 192.168.7.231:51820
  allowed ips: 10.0.0.0/30, 192.168.133.0/24
  latest handshake: 1 minute, 55 seconds ago
  transfer: 1.44 KiB received, 5.28 KiB sent
  persistent keepalive: every 25 seconds
```

2nd WireGuard Tunnel Information

WireGuard is disabled.

3rd WireGuard Tunnel Information

WireGuard is disabled.

4th WireGuard Tunnel Information

WireGuard is disabled.

Figure 9: WireGuard Status Page



The *Latest handshake* time is the time left from the latest successful communication with the opposite tunnel side. This item will not be shown here until there is a tunnel communication (data sent by the client-side or the keepalive data sent when *NAT/Firewall Traversal* is set to *yes*).

2.9 DynDNS

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



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

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

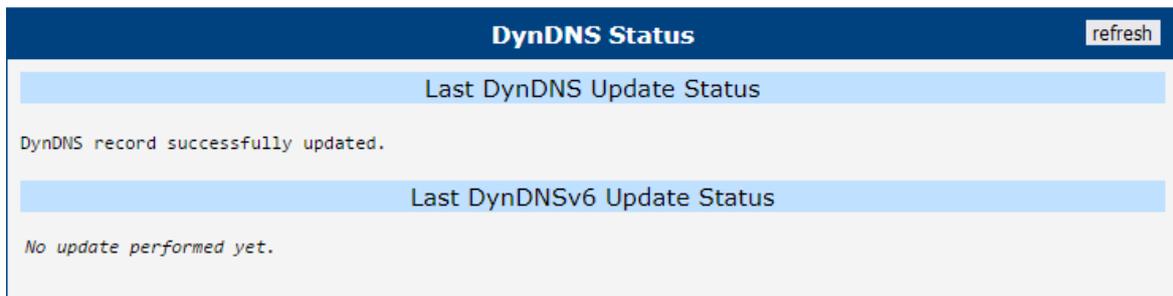


Figure 10: DynDNS Status

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.

2.10 System Log

If there are any connection problems, you can view the system log by selecting the *System Log* menu item. Detailed reports from individual applications running on 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 to create detailed reports (it will be saved as a text file with the .txt extension). The report will include statistical data, routing and process tables, the system log, and configuration.



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

The default length of the system log is 1000 KiB. Once this size is reached, a new file is created for storing the system log. When the second file is full, the first file is overwritten with a new log.

The *Syslogd* program outputs the system log. It can be started with two options to modify its behavior. The option *"-S"* followed by a decimal number sets the maximum number of lines in one log file. The option *"-R"* followed by a hostname or IP address enables logging to a remote syslog daemon. (If the remote syslog daemon is on a Linux OS, remote logging must be enabled, typically by running *"syslogd -R"*. If it's on a Windows OS, a syslog server must be installed, such as *Syslog Watcher*). To start *syslogd* with these options, the *"/etc/init.d/syslog"* script can be modified via SSH, or lines can be added to the *Startup Script* (accessible in the *Configuration* section), as shown in figure 12.

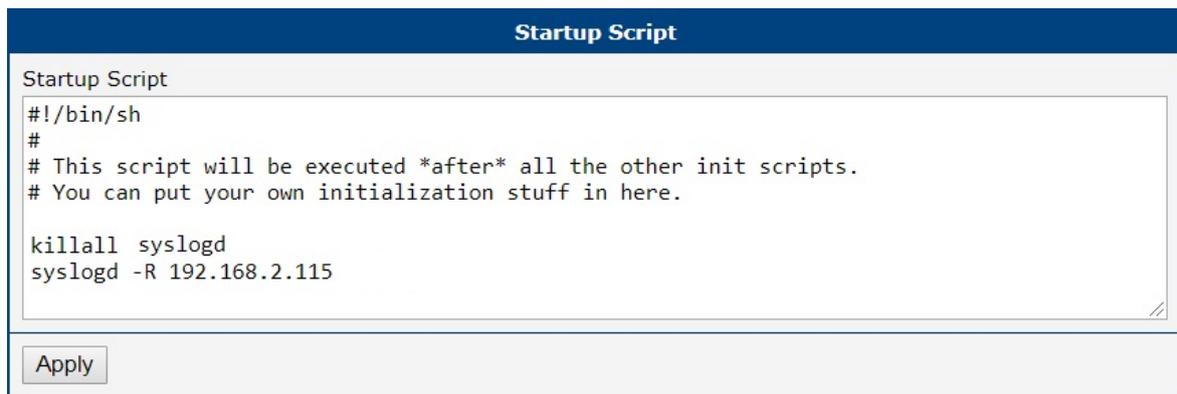
```

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

```

Figure 11: System Log

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



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

killall syslogd
syslogd -R 192.168.2.115
```

Apply

Figure 12: Example program syslogd start with the parameter -R

3. Configuration

3.1 Ethernet

To enter the Local Area Network configuration, select the *Ethernet* menu item in the *Configuration* section. The *Ethernet* item will expand in the menu on the left, allowing you to choose the appropriate Ethernet interface to configure: *ETH0* for the first Ethernet interface, *ETH1* for the second Ethernet interface, and *ETH2* for the third Ethernet interface.

The LAN Configuration page is divided into IPv4 and IPv6 columns, as shown in Figure 13. There is dual stack support for IPv4 and IPv6 protocols, meaning they can run concurrently. You can configure either one of them or both. If both IPv4 and IPv6 are configured, network devices will automatically select the communication protocol. The configuration items and differences between IPv6 and IPv4 are described in the tables below.

ETH0 Configuration		
	IPv4	IPv6
DHCP Client	<input type="text" value="disabled"/>	<input type="text" value="disabled"/>
IP Address	<input type="text" value="10.64.0.37"/>	<input type="text" value="fd00:a40::99"/>
Subnet Mask / Prefix	<input type="text" value="255.255.252.0"/>	<input type="text" value="56"/>
Default Gateway	<input type="text" value="10.64.0.1"/>	<input type="text" value="fd00:a40::1"/>
Primary DNS Server	<input type="text"/>	<input type="text"/>
Secondary DNS Server	<input type="text"/>	<input type="text"/>
Bridged	<input type="text" value="no"/>	
Media Type	<input type="text" value="auto-negotiation"/>	
MTU	<input type="text" value="1500"/>	bytes
<input type="checkbox"/> Enable dynamic DHCP leases		
IP Pool Start	<input type="text" value="192.168.1.2"/>	<input type="text"/>
IP Pool End	<input type="text" value="192.168.1.254"/>	<input type="text"/>
Lease Time	<input type="text" value="600"/>	<input type="text" value="600"/> sec
<input type="checkbox"/> Enable static DHCP leases		
MAC Address	IP Address	IPv6 Address
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> Enable IPv6 prefix delegation		
Subnet ID *	<input type="text"/>	
Subnet ID Width *	<input type="text"/>	bits
<input type="checkbox"/> Enable IEEE 802.1X Authentication		
Authentication Method	<input type="text" value="EAP-PEAP/MSCHAPv2"/>	
CA Certificate	<input type="text"/>	
	<input type="button" value="Choose File"/> No file chosen	
Local Certificate	<input type="text"/>	
	<input type="button" value="Choose File"/> No file chosen	
Local Private Key	<input type="text"/>	
	<input type="button" value="Choose File"/> No file chosen	
Identity	<input type="text"/>	
Password	<input type="text"/>	
* can be blank		
<input type="button" value="Apply"/>		

Figure 13: LAN Configuration Page

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

Table 14: Configuration of the Network Interface – IPv4 and IPv6

The *Default Gateway* and *DNS Server* items are only used if the *DHCP Client* is set to *disabled* and if the ETH0, ETH1 or ETH2 LAN is selected by the *Backup Routes* system as the default route. (The selection algorithm is described in section 3.9). Since FW 5.3.0, *Default Gateway* and *DNS Server* are also supported on bridged interfaces (e.g., eth0 + eth1).

The following three items (in the table below) are global for the configured Ethernet interface. Only one bridge can be active on the router at a time. The *DHCP Client*, *IP Address*, and *Subnet Mask / Prefix* parameters of only one of the interfaces are used for the bridge. The ETH0 LAN has higher priority when both interfaces (ETH0 and ETH1) are added to the bridge. Other interfaces can be added to or removed 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.



Under certain conditions, the ETH interface may operate as a WAN interface, and the rules defined in the Firewall settings will be applied to it. Details are described in Chapter *Backup Routes* and are demonstrated with examples provided in that chapter.

Item	Description
Bridged	<p>Activates/deactivates the bridging function on the router.</p> <ul style="list-style-type: none"> • no – The bridging function is inactive (default). • yes – The bridging function is active.
Media Type	<p>Specifies the type of duplex and speed used in the network.</p> <ul style="list-style-type: none"> • Auto-negotiation – The router automatically sets the best speed and duplex mode of communication according to the network's possibilities. • 1000 Mbps Full Duplex – The router communicates at 1000 Mbps, in the full duplex mode. • 100 Mbps Full Duplex – The router communicates at 100 Mbps, in the full duplex mode. • 100 Mbps Half Duplex – The router communicates at 100 Mbps, in the half duplex mode. • 10 Mbps Full Duplex – The router communicates at 10 Mbps, in the full duplex mode. • 10 Mbps Half Duplex – The router communicates at 10 Mbps, in the half duplex mode.
MTU	<p>Maximum Transmission Unit value. Default value is 1500 bytes.</p>
LAN1 PoE PSE ¹ LAN2 PoE PSE ¹ LAN3 PoE PSE ¹ LAN4 PoE PSE ¹	<ul style="list-style-type: none"> • enabled – The PoE PSE feature is enabled for port LANx of an ETH0 interface. • disabled – The PoE PSE feature is disabled for port LANx of an ETH0 interface (default).

Table 15: Configuration of the Network Interface – Global Items

¹Available only on models equipped with the PoE PSE functionality.

3.1.1 DHCP Server

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

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



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



For DHCPv6 static address assignment to work, DHCPv6 client must use DUID-LL or DUID-LLT types that are derived from its MAC address.



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

Item	Description
Enable dynamic DHCP leases	Select this option to enable a dynamic DHCP server.
IP Pool Start	Starting IP addresses allocated to the DHCP clients. Use proper notation in IPv4 and IPv6 column.
IP Pool End	End of IP addresses allocated to the DHCP clients. Use proper IP address notation in IPv4 and IPv6 column.
Lease time	Time in seconds that the IP address is reserved before it can be re-used.

Table 16: Configuration of Dynamic DHCP Server

Item	Description
Enable static DHCP leases	Select this option to enable a static DHCP server.
MAC Address	MAC address of a DHCP client.
IPv4 Address	Assigned IPv4 address. Use proper notation.
IPv6 Address	Assigned IPv6 address. Use proper notation.

Table 17: Configuration of Static DHCP Server

3.1.3 802.1X Authentication to RADIUS Server

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

IEEE 802.1X authentication involves three parties: **a supplicant, an authenticator, and an authentication server**, illustrated in Figure 15.

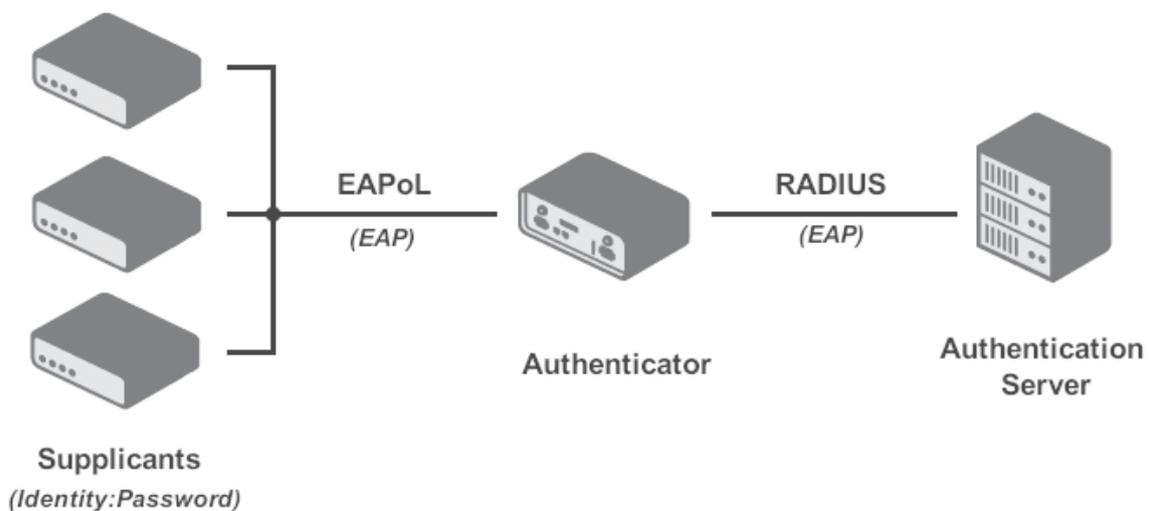


Figure 15: IEEE 802.1X Functional Diagram

- The **supplicant** is a client device (e.g., a laptop) wishing to attach to the LAN/WLAN, also referring to the client software providing credentials to the authenticator.
- The **authenticator** is a network device facilitating the data link between the supplicant and the network, capable of permitting or denying network traffic. This device communicates with the authentication server to decide on network access authorization for a supplicant.
- The **authentication server**, usually a trusted server, handles requests for network access, informing the authenticator about connection permissions and the settings applicable to the client's connection. It commonly runs software supporting the **RADIUS** and **EAP protocols**.

Table 19 summarizes the supported roles and cases for IEEE 802.1X authentication on Advantech routers.



Advantech routers support the roles of supplicant and authenticator only. The authentication server role is not supported.

Interface	Supplicant Role	Authenticator Role
LAN	As a built-in feature, configure LAN with 802.1X authentication, see Chapter 3.1.3.	While not a built-in feature, it can be facilitated by the <i>802.1X Authenticator</i> Router App.
WiFi	In Station (STA) mode, see Chapter 3.7.	In Access Point (AP) mode, see Chapter 3.6.

Table 19: Supported Roles for IEEE 802.1X Authentication

Authentication (802.1X) to RADIUS server can be enabled in next configuration section. This functionality requires additional setting of identity and certificates as described in the following table.

Item	Description
Enable IEEE 802.1X Authentication	Select this option to enable 802.1X Authentication.
Authentication Method	Select authentication method (EAP-PEAPMSCHAPv2 or EAP-TLS).
CA Certificate	Definition of CA certificate for EAP-TLS authentication protocol.
Local Certificate	Definition of local certificate for EAP-TLS authentication protocol.
Local Private Key	Definition of local private key for EAP-TLS authentication protocol.
Identity	User name – identity.
Password	Access password. This item is available for EAP-PEAPMSCHAPv2 protocol only. Enter valid characters only, see chap. 1.3.2!
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. 1.3.2!

Table 20: Configuration of 802.1X Authentication

3.1.4 LAN Configuration Examples

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

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

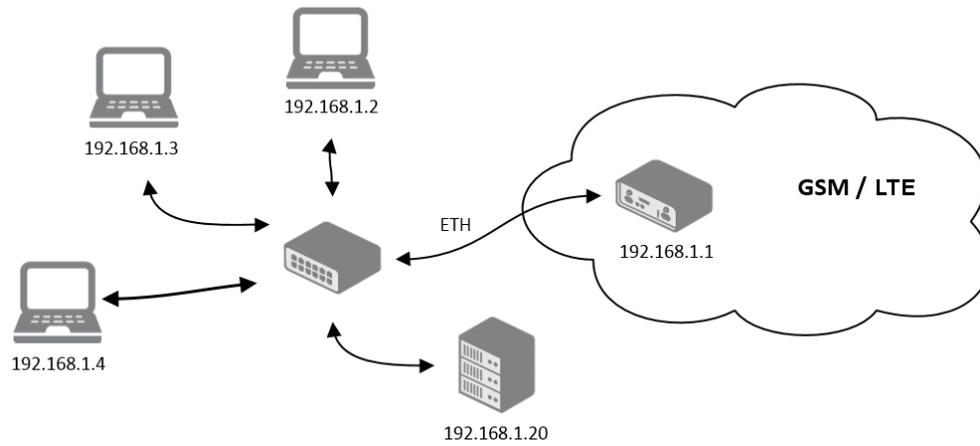


Figure 16: Network Topology for Example 1

ETH0 Configuration		
	IPv4	IPv6
DHCP Client	disabled ▼	disabled ▼
IP Address	192.168.1.1	
Subnet Mask / Prefix	255.255.255.0	
Default Gateway	129.168.1.20	
Primary DNS Server	192.168.1.20	
Secondary DNS Server		
Bridged	no ▼	
Media Type	auto-negotiation ▼	
<input checked="" type="checkbox"/> Enable dynamic DHCP leases		
	IPv4	IPv6
IP Pool Start	192.168.1.2	
IP Pool End	192.168.1.4	
Lease Time	600	600 sec
<input type="checkbox"/> Enable static DHCP leases		
MAC Address	IP Address	IPv6 Address
<input type="checkbox"/> Enable IPv6 prefix delegation		
Subnet ID *		
Subnet ID Width *		bits
<input type="checkbox"/> Enable IEEE 802.1X Authentication		
Authentication Method	EAP-PEAP/MSCHAPv2 ▼	
CA Certificate	<input type="text"/> <input type="button" value="Choose File"/> No file chosen	
Local Certificate	<input type="text"/> <input type="button" value="Choose File"/> No file chosen	
Local Private Key	<input type="text"/> <input type="button" value="Choose File"/> No file chosen	
Identity	<input type="text"/>	
Password	<input type="password"/>	
* can be blank		
<input type="button" value="Apply"/>		

Figure 17: LAN Configuration for Example 1

Example 2: IPv4 Dynamic and Static DHCP server

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

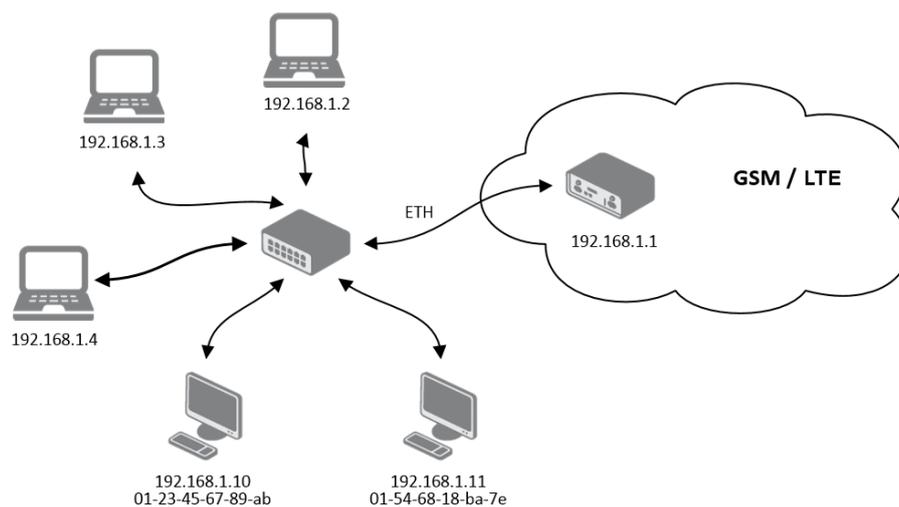


Figure 18: Network Topology for Example 2

ETH0 Configuration		
	IPv4	IPv6
DHCP Client	disabled ▼	disabled ▼
IP Address	192.168.1.1	
Subnet Mask / Prefix	255.255.255.0	
Default Gateway		
Primary DNS Server		
Secondary DNS Server		
Bridged	no ▼	
Media Type	auto-negotiation ▼	
<input checked="" type="checkbox"/> Enable dynamic DHCP leases		
	IPv4	IPv6
IP Pool Start	192.168.1.2	
IP Pool End	192.168.1.4	
Lease Time	600	600 sec
<input checked="" type="checkbox"/> Enable static DHCP leases		
MAC Address	IP Address	IPv6 Address
01:23:45:67:89:ab	192.168.1.10	
01:54:68:18:ba:7e	192.168.1.11	
<input type="checkbox"/> Enable IPv6 prefix delegation		
Subnet ID *		
Subnet ID Width *		bits
<input type="checkbox"/> Enable IEEE 802.1X Authentication		
Authentication Method	EAP-TLS ▼	
CA Certificate	<input type="text"/> <input type="button" value="Choose File"/> No file chosen	
Local Certificate	<input type="text"/> <input type="button" value="Choose File"/> No file chosen	
Local Private Key	<input type="text"/> <input type="button" value="Choose File"/> No file chosen	
Identity	<input type="text"/>	
Local Private Key Password	<input type="password"/>	
* can be blank		
<input type="button" value="Apply"/>		

Figure 19: LAN Configuration for Example 2

Example 3: IPv6 Dynamic DHCP Server

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

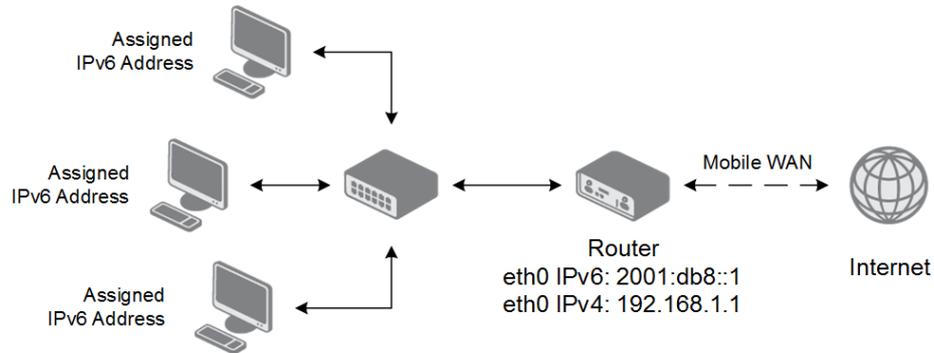


Figure 20: Network Topology for Example 3

ETH0 Configuration		
DHCP Client	IPv4 disabled	IPv6 disabled
IP Address	192.168.1.1	2001:db8::1
Subnet Mask / Prefix	255.255.255.0	64
Default Gateway		
Primary DNS Server		
Secondary DNS Server		
Bridged	no	
Media Type	auto-negotiation	
<input checked="" type="checkbox"/> Enable dynamic DHCP leases		
IP Pool Start	IPv4	IPv6 2001:db8::2
IP Pool End		2001:db8::ffff
Lease Time		600 sec
<input type="checkbox"/> Enable static DHCP leases		
MAC Address	IP Address	IPv6 Address
<input type="checkbox"/> Enable IPv6 prefix delegation		
Subnet ID *		
Subnet ID Width *		bits
<input type="checkbox"/> Enable IEEE 802.1X Authentication		
Authentication Method	EAP-TLS	
CA Certificate	<input type="text"/> <input type="button" value="Choose File"/> No file chosen	
Local Certificate	<input type="text"/> <input type="button" value="Choose File"/> No file chosen	
Local Private Key	<input type="text"/> <input type="button" value="Choose File"/> No file chosen	
Identity	<input type="text"/>	
Local Private Key Password	<input type="password"/>	
* can be blank		
<input type="button" value="Apply"/>		

Figure 21: LAN Configuration for Example 3

3.2 VLAN

This section allows for the configuration of VLAN on the device. You can configure up to three VLANs. The configuration form consists of multiple sections that enable the user to configure VLAN interfaces, DHCP leases, and IPv6 delegation, see Figure 22 and Table 21.

1st VLAN Configuration

Create 1st VLAN connection

	IPv4	IPv6
DHCP Client	disabled ▼	disabled ▼
IP Address	<input type="text"/>	<input type="text"/>
Subnet Mask / Prefix	<input type="text"/>	<input type="text"/>

Interface	ETH0 ▼	
VLAN ID	<input type="text"/>	
MTU *	<input type="text"/>	bytes

Enable dynamic DHCP leases

	IPv4	IPv6
IP Pool Start	<input type="text"/>	<input type="text"/>
IP Pool End	<input type="text"/>	<input type="text"/>
Lease Time	600	600 sec

Enable static DHCP leases

MAC Address	IP Address	IPv6 Address
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>

Enable IPv6 prefix delegation

Subnet ID *	<input type="text"/>
Subnet ID Width *	<input type="text"/> bits

* can be blank

Figure 22: VLAN Configuration Form

Item	Description
Create VLAN connection	Enables the creation of the VLAN connection.
DHCP Client (IPv4/IPv6)	Enables or disables the DHCP client for IPv4 and IPv6: <ul style="list-style-type: none"> • disabled — Disables the DHCP client. • enabled — Enables the DHCP client for the respective protocol.
IP Address	Manually specify the IP address for the VLAN interface.
Subnet Mask / Prefix	Defines the subnet mask for IPv4 or the prefix for IPv6.
Interface	Select the Ethernet interface associated with the VLAN.
VLAN ID	Specifies the VLAN ID for the virtual LAN interface.
MTU	The Maximum Transmission Unit (MTU) size in bytes.

Continued on the next page

Continued from previous page

Item	Description
Enable dynamic DHCP leases	Enables dynamic DHCP leases configuration for IPv4 and IPv6: <ul style="list-style-type: none"> • IP Pool Start: Start of the DHCP pool for IPv4 and IPv6. • IP Pool End: End of the DHCP pool for IPv4 and IPv6. • Lease Time: Lease time in seconds, default is 600 seconds for both IPv4 and IPv6.
Enable static DHCP leases	Enables configuration of static DHCP leases for specific MAC addresses: <ul style="list-style-type: none"> • MAC Address: MAC address of the client. • IP Address: Fixed IPv4 address for the client. • IPv6 Address: Fixed IPv6 address for the client.
Enable IPv6 prefix delegation	Enables configuration of IPv6 prefix delegation: <ul style="list-style-type: none"> • Subnet ID: The subnet ID for prefix delegation. • Subnet ID Width: The width of the subnet ID in bits.

Table 21: VLAN Configuration Options

Once all the desired settings are configured, click the *Apply* button to save the configuration.

3.3 VRRP

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 22: VRRP Configuration Items Description

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 23: Check Connection

Example of the VRRP protocol:

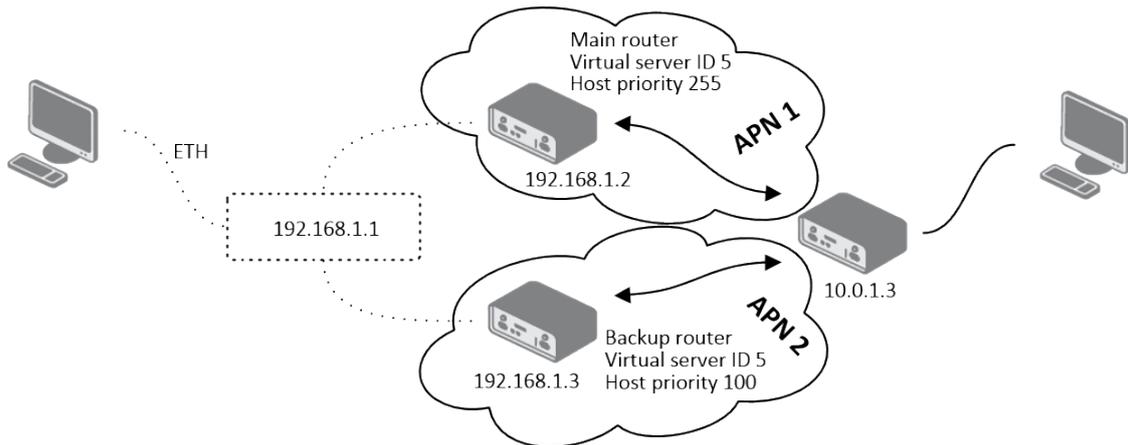


Figure 23: Topology of VRRP Configuration Example

1st VRRP Instance Configuration

Enable 1st VRRP Instance

Protocol Version: VRRPv2

Virtual Server IP Address: 192.168.1.1

Virtual Server ID: 5

Host Priority: 255

Check connection

Ping IP Address: 10.0.1.3

Ping Interval: 10 sec

Ping Timeout: 5 sec

Ping Probes: 10

Enable traffic monitoring

Apply

Figure 24: Example of VRRP Configuration – Main Router

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

Figure 25: Example of VRRP Configuration – Backup Router

3.4 Mobile WAN



The ICR-4401 (LAN version) has no the *Mobile WAN* configuration menu option.

Select the *Mobile WAN* item in the *Configuration* menu section to enter the cellular network configuration page. See *Mobile WAN Configuration* page in Figure 26.

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

Figure 26: Mobile WAN Configuration

3.4.1 Connection to Mobile Network

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

Item	Description
Carrier	Available For NAM routers only. Network carrier selection. Provides either <i>automatic detection</i> option, or manual selection of <i>AT&T</i> , <i>Rogers</i> or <i>Verizon</i> .
APN	Network identifier (Access Point Name).
Username	The user name used for logging on to the GSM network.
Password	The password used for logging on to the GSM network. Enter valid characters only, see chap. 1.3.2!
Authentication	Authentication protocol used in the GSM network: <ul style="list-style-type: none"> • PAP or CHAP – The router selects the authentication method. • PAP – The router uses the PAP authentication method. • CHAP – The router uses the CHAP authentication method.
IP Mode	Specifies the version of IP protocol used: <ul style="list-style-type: none"> • IPv4 – IPv4 protocol is used only (default). • IPv6 – IPv6 protocol is used only. • IPv4/IPv6 – IPv4 and IPv6 independent dual stack is enabled.
IP Address	For use in IPv4 and IPv4/IPv6 mode only. Specifies the IPv4 address of the SIM card. You manually enter the IP address only when mobile network carrier has assigned the IP address.
Dial Number	Specifies the telephone number which the router dials for a CSD connection. The router uses the default telephone number *99***1 #.
Operator	Specifies the carrier code. You can specify this 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 technologies. Automatic selection never selects NB-IoT networks. Use NB-IoT in the selection for NB-IoT networks.
PIN	Specifies the PIN used to unlock the SIM card. Use only if this is required by a given SIM card. The SIM card will be blocked after several failed attempts to enter the PIN.
MRU	Maximum Receive Unit – maximum size of packet that the router can receive via Mobile WAN. The default value is 1500 B. Other settings may cause the router to receive data incorrectly. Minimal value in IPv4 and IPv4/IPv6 mode: 128 B. Minimal value in IPv6 mode: 1280 B.
MTU	Maximum Transmission Unit – maximum size of packet that the router can transmit via Mobile WAN. The default value is 1500 B. Other settings may cause the router to transmit data incorrectly. Minimal value in IPv4 and IPv4/IPv6 mode: 128 B. Minimal value in IPv6 mode: 1280 B.

Table 24: Mobile WAN Configuration Items Description



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

- If the MTU size is set incorrectly, then the router will not exceed the data transfer. If the MTU value is set too low, more frequent fragmentation of data will occur. More frequent fragmentation will mean a higher overhead and also the possibility of packet damage during defragmentation. In contrast, a higher MTU value can cause the network to drop the packet.
- If the *IP address* field is left blank, when the router establishes a connection, the mobile network carrier will automatically assign an IP address. If you assign an IP address manually, then the router will access the network quicker.
- If the **APN** field is left blank, 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.



The correct PIN must be filled in. An incorrect PIN may block the SIM card.

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

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

3.4.2 DNS Address Configuration

The *DNS Settings* parameter is designed to simplify configuration on the client side. When this value is set to *get from operator*, the router will attempt to automatically obtain IP addresses from the primary and secondary DNS servers of the mobile network carrier. To manually specify the IP addresses of the primary or secondary DNS servers, select *set manually* from the *DNS Setting* drop-down list. You can then enter the IPv4 or IPv6 address of the DNS server (or both), depending on the selected IP Mode.

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

Table 25: Check Connection to Mobile Network Configuration

3.4.4 Check Connection Example

The figure below displays the following scenario: the connection to the mobile network in IPv4 *IP Mode* is controlled on the address 8.8.8.8 with a time interval of 60 seconds for the first SIM card and on the address www.google.com with the time interval 80 seconds for the second SIM card (for an active SIM only). Because the *Enable traffic monitoring* option is enabled, the control pings are not sent, but the data stream is monitored. The ping will be sent, if the data stream is interrupted.

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

Check Connection	<input type="text" value="enabled"/>	<input type="text" value="enabled"/>
Ping IP Address	<input type="text" value="8.8.8.8"/>	<input type="text" value="www.google.com"/>
Ping IPv6 Address	<input type="text" value=""/>	<input type="text" value=""/>
Ping Interval	<input type="text" value="60"/>	<input type="text" value="80"/> sec
Ping Timeout	<input type="text" value="60"/>	<input type="text" value="80"/> sec

Enable traffic monitoring

Figure 27: Check Connection Example

3.4.5 Data Limit Configuration

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

Table 26: 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.

3.4.6 Switch between SIM Cards Configuration

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



The router will automatically toggle between the SIM cards and their individual setups depending on the configuration settings specified here (manual permission, roaming, data limit, binary 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 <i>disabled</i> , this means that the entire cellular module is disabled. <ul style="list-style-type: none"> • enabled – It is possible to use the SIM card. • disabled – Never use the SIM card, the usage of this SIM is forbidden.
Roaming State	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! <ul style="list-style-type: none"> • not applicable – It is possible to use the SIM card everywhere. • home network only – Only use the SIM card if roaming is not detected.

Continued on next page

Continued from previous page

Item	Description
Data Limit State	Configure the use of SIM cards based on the Data Limit set above: <ul style="list-style-type: none"> • not applicable – It is possible to use the SIM regardless of the limit. • not exceeded – Use the SIM card only if the Data Limit (set above) has not been exceeded.
BINx State	Configure the use of SIM cards based on binary input x state, where x is the input number: <ul style="list-style-type: none"> • not applicable – It is possible to use the SIM regardless of BINx state. • on – Only use the SIM card if the BINx state is logical 0 – voltage present. • off – Only use the SIM card if the BINx state is logical 1 – no voltage.

Table 27: 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. <ul style="list-style-type: none"> • 1st – The 1st SIM card is the default one. • 2nd – The 2nd SIM card is the default one.
Initial State	Specifies the action of the cellular module after the SIM card has been selected. <ul style="list-style-type: none"> • online – establish connection to the mobile network after the SIM card has been selected (default). • offline – go to the off-line mode after the SIM card has been selected. <p>Note: If offline, you can change this initial state by SMS message only – see <i>SMS Configuration</i>. The cellular module will also go into off-line mode if none of the SIM cards are not selected.</p>
Switch to other SIM card when connection fails	Applicable only when connection is established on the default SIM card and then fails. If the connection failure is detected by <i>Check Connection</i> feature above, the router will switch to the backup SIM card.
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 because of a failure of the default one or if roaming settings cause the switch. This feature is available only when <i>Switch to other SIM card when connection fails</i> is enabled.
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.

Continued on next page

Continued from previous page

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

Table 28: Parameters for SIM card switching

3.4.7 Examples of SIM Card Switching Configuration

Example 1: Timeout Configuration

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

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

Figure 28: Configuration for SIM card switching Example 1

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

Example 2: Data Limit Switching

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

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

Figure 29: Configuration for SIM card switching Example 2

3.4.8 PPPoE Bridge Mode Configuration

If you mark the *Enable PPPoE bridge mode* check box, the router activates the PPPoE bridge protocol. PPPoE (point-to-point over ethernet) is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. The bridge mode allows you to create a PPPoE connection from a device behind the router. For example, a PC connected to the ETH port of the router. You assign the IP address of the SIM card to the PC. The changes in settings will apply after clicking the *Apply* button.

3.5 PPPoE

PPPoE (Point-to-Point over Ethernet) is a network protocol that 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 check the *Create PPPoE connection* box, the router will attempt to establish a PPPoE connection after boot-up. Once connected, the router obtains the IP address of the device to which it is connected. Communication from devices behind the PPPoE server is then forwarded to the router, enabling full network access.

PPPoE Configuration

Create PPPoE connection

Interface ▼

Username *

Password * 👁

Authentication ▼

IP Mode ▼

MRU bytes

MTU bytes

Clamp Max. Segment Size

DNS Settings ▼

Primary DNS Server

Primary IPv6 DNS Server

Secondary DNS Server

Secondary IPv6 DNS Server

* can be blank

Figure 30: PPPoE Configuration

Item	Description
Create PPPoE connection	Enable PPPoE on the selected interface.
Interface	Select an Ethernet interface for the PPPoE connection.
Username	Username for secure access to PPPoE.
Password	Password for secure access to PPPoE. Enter valid characters only, see chap. 1.3.2!

Continued on next page

Continued from previous page

Item	Description
Authentication	Authentication protocol in the GSM network. <ul style="list-style-type: none"> • PAP or CHAP – The router selects the authentication method. • PAP – The router uses the PAP authentication method. • CHAP – The router uses the CHAP authentication method.
IP Mode	Specifies the version of the IP protocol: <ul style="list-style-type: none"> • IPv4 – Only the IPv4 protocol is used (default). • IPv6 – Only the IPv6 protocol is used. • IPv4/IPv6 – Dual stack for both IPv4 and IPv6 is enabled.
MRU	Specifies the Maximum Receive Unit. The MRU identifies the maximum packet size that the router can receive via PPPoE. The default value is 1492 B (bytes). Other settings may result in incorrect data transmission. The minimum value for IPv4 and IPv4/IPv6 mode is 128 B, and for IPv6 mode is 1280 B.
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 B (bytes). Other settings may result in incorrect data transmission. The minimum value for IPv4 and IPv4/IPv6 mode is 128 B, and for IPv6 mode is 1280 B.
Clamp Max. Segment Size	Enhances network performance and stability by adjusting the Maximum Segment Size (MSS) of TCP packets to align with the network connection's Path Maximum Transmission Unit (PMTU). It is enabled by default.
DNS Settings	Can be set to obtain the DNS address from the server or to configure it manually.
Primary DNS Server	Primary IPv4 address of the DNS server.
Primary IPv6 DNS Server	Primary IPv6 address of the DNS server.
Secondary DNS Server	Secondary IPv4 address of the DNS server.
Secondary IPv6 DNS Server	Secondary IPv6 address of the DNS server.

Table 29: PPPoE Configuration



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

3.6 WiFi Access Point



This 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. Use IPv4 notation in IPv4 column and IPv6 notation in IPv6 column. Shortened IPv6 notation is supported.
Subnet Mask / Prefix	Specifies a Subnet Mask for the IPv4 address. In the IPv6 column, fill in the Prefix for the IPv6 address – number in range 0 to 128.
Bridged	Activates bridge mode: <ul style="list-style-type: none"> • no – Bridged mode is not allowed (default value). WLAN network is not connected with LAN network of the router. • yes – Bridged mode is allowed. WLAN network is connected with one or more LAN networks of the router. In this case, the setting of most items in this table are ignored. Instead, the router uses the settings of the selected network interface (LAN).
Enable dynamic DHCP leases	Enable dynamic allocation of IP addresses using the DHCP (DHCPv6) server.
IP Pool Start	Beginning of the range of IP addresses which will be assigned to DHCP clients. Use proper notation in IPv4 and IPv6 column.
IP Pool End	End of the range of IP addresses which will be assigned to DHCP clients. Use proper notation in IPv4 and IPv6 column.
Lease Time	Time in seconds for which the client may use the IP address.
Enable IPv6 prefix delegation	Enables prefix delegation configuration filled-in below.
Subnet ID	The decimal value of the Subnet ID of the Ethernet inter face. Maximum value depends on the Subnet ID Width.

Continued on next page

Continued from previous page

Item	Description
Subnet ID Width	The maximum Subnet ID Width depends on your Site. Prefix – it is the remainder to 64 bits.
SSID	The unique identifier of WiFi network.
Broadcast SSID	Method of broadcasting the unique identifier of SSID network in beacon frame and type of response to a request for sending the beacon frame. <ul style="list-style-type: none"> • Enabled – SSID is broadcasted in beacon frame • Zero length – Beacon frame does not include SSID. Requests for sending beacon frame are ignored. • Clear – All SSID characters in beacon frames are replaced by 0. Original length is kept. Requests for sending beacon frames are ignored.
SSID Isolation	When enabled, by choosing a zone, a WiFi client connected to this Access Point is not able to communicate with another WiFi client connected to another Access Point, having another zone selected. This client still can communicate with a client connected to the same Access Point, unless the Client Isolation is not enabled.
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.
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.
Country Code	This option is not available for NAM routers – the "US" country code is set by default on these versions of router. Code of the country where the router is installed. This code must be entered in ISO 3166-1 alpha-2 format. If a <i>country code</i> isn't specified and the router has not implemented a system to determine this code, it will use "US" as the default <i>country code</i> . If no <i>country code</i> is specified or if the wrong country code is entered, the router may violate country-specific regulations for the use of WiFi frequency bands.
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. <ul style="list-style-type: none"> • IEEE 802.11b (2.4 GHz) • IEEE 802.11b+g (2.4 GHz) • IEEE 802.11b+g+n (2.4 GHz) • IEEE 802.11a (5 GHz) • IEEE 802.11a+n (5 GHz) • IEEE 802.11ac (5 GHz)

Continued on next page

Continued from previous page

Item	Description
Channel	The channel on which the WiFi AP is transmitting. The available channels are based on the selected <i>Country Code</i> . You can choose <i>auto</i> to let the system select the channel automatically. To see channels available for a different country code, change the country code, click <i>Apply</i> , and the channel list will be updated. On NAM routers only channels 1 to 11 are supported!
Bandwidth	Allows you to choose the transfer bandwidth. Note that it may be disabled for some hardware modes, and a lower bandwidth may be used if some is occupied.
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.
Authentication	Access control and authorization of users in the WiFi network. <ul style="list-style-type: none"> • Open – Authentication is not required (free access point). • Shared – Basic authentication using WEP key. • WPA-PSK – Authentication using higher authentication methods PSK-PSK. • WPA2-PSK – WPA2-PSK using newer AES encryption. • WPA3-PSK – WPA3-PSK using newer AES encryption. • WPA-Enterprise – RADIUS authentication done by external server via user-name 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: <ul style="list-style-type: none"> • None – No data encryption. • WEP – Encryption using static WEP keys. This encryption method can be used for <i>Shared</i> authentication. However, it is not secure and may be unavailable for some models. • TKIP – Dynamic encryption key management that can be used for <i>WPA-PSK</i> and <i>WPA2-PSK</i> authentication. • AES – Improved encryption used for <i>WPA2-PSK</i> authentication.
WEP Key Type	Type of WEP key for WEP encryption: <ul style="list-style-type: none"> • ASCII – WEP key in ASCII format. • HEX – WEP key in hexadecimal format.
WEP Default Key	This specifies the default WEP key.

Continued on next page

Continued from previous page

Item	Description
WEP Key 1–4	<p>Allows entry of four different WEP keys:</p> <ul style="list-style-type: none"> • WEP key in ASCII format must be entered in quotes. This key can be specified in the following lengths. <ul style="list-style-type: none"> – 5 ASCII characters (40b WEP key) – 13 ASCII characters (104b WEP key) – 16 ASCII characters (128b WEP key) • WEP key in hexadecimal format must be entered in hexadecimal digits. This key can be specified in the following lengths. <ul style="list-style-type: none"> – 10 hexadecimal digits (40b WEP key) – 26 hexadecimal digits (104b WEP key) – 32 hexadecimal digits (128b WEP key)
WPA PSK Type	<p>The possible key options for WPA-PSK authentication.</p> <ul style="list-style-type: none"> • 256-bit secret • ASCII passphrase • PSK File
WPA PSK	<p>Key for WPA-PSK authentication. This key must be entered according to the selected WPA PSK type as follows:</p> <ul style="list-style-type: none"> • 256-bit secret – 64 hexadecimal digits • ASCII passphrase – 8 to 63 characters • PSK File – absolute path to the file containing the list of pairs (PSK key, MAC address)
RADIUS Auth Server IP	<p>IPv4 or IPv6 address of the RADIUS server. Only with one of RADIUS authentications selected.</p>
RADIUS Auth Password	<p>RADIUS server access password. Only with one of RADIUS authentications selected.</p>
RADIUS Auth Port	<p>RADIUS server port. The default is 1812. Only with one of RADIUS authentications selected.</p>
RADIUS Acct Server IP	<p>IPv4 or IPv6 address of the RADIUS accounting server. Define only if different from the authentication and authorization server. Only with one of RADIUS authentications selected.</p>
RADIUS Acct Password	<p>Access password of RADIUS accounting server. Define only if different from the authentication and authorization server. Only with one of RADIUS authentications selected.</p>
RADIUS Acct Port	<p>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.</p>

Continued on next page

Continued from previous page

Item	Description
Access List	Mode of Access/Deny list. <ul style="list-style-type: none"> • Disabled – Access/Deny list is not used. • Accept – Clients in Accept/Deny list can access the network. • Deny – Clients in Access/Deny list cannot access the network.
Accept/Deny List	Accept or Deny list of client MAC addresses that set network access. Each MAC address is separated by new line.
Syslog Level	Logging level, when system writes to the system log. <ul style="list-style-type: none"> • Verbose debugging – The highest level of logging. • Debugging • Informational – Default level of logging. • Notification • Warning – The lowest level of system communication.
Extra options	Allows the user to define additional parameters for the hostapd. Options are added as is to the end of a configuration file. For more information, see hostapd.conf Linux man page. Use only if you know what you are doing.

Table 30: WiFi Configuration Items Description

WiFi AP 1 Configuration		
<input type="checkbox"/> Enable WiFi AP 1		
IP Address	IPv4	IPv6
Subnet Mask / Prefix		
Bridged	no	
<input type="checkbox"/> Enable dynamic DHCP leases		
IP Pool Start	IPv4	IPv6
IP Pool End		
Lease Time	600	600 sec
<input type="checkbox"/> Enable IPv6 prefix delegation		
Subnet ID *		
Subnet ID Width *		
SSID		
Broadcast SSID	enabled	
SSID Isolation	disabled	
Client Isolation	disabled	
WMM	disabled	
<i>The following radio settings are common for all Access Points on WiFi module 1</i>		
Country Code *		
HW Mode	IEEE 802.11b	
Channel	1	
Bandwidth	20 MHz	
Short GI	disabled	
Authentication	open	
Encryption	none	
WEP Key Type	ASCII	
WEP Default Key	1	
WEP Key 1		
WEP Key 2		
WEP Key 3		
WEP Key 4		
WPA PSK Type	256-bit secret	
WPA PSK		
RADIUS Auth Server IP		
RADIUS Auth Password		
RADIUS Auth Port *	1812	
RADIUS Acct Server IP *		
RADIUS Acct Password *		
RADIUS Acct Port *	1813	
Access List	disabled	
Accept/Deny List		
Syslog Level	informational	
Extra options *		
* can be blank		
<input type="button" value="Apply"/>		

Figure 31: WiFi Access Point Configuration Page

3.7 WiFi Station

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

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

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.

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

WiFi STA Configuration

Enable WiFi STA

	IPv4	IPv6
DHCP Client	enabled	enabled
IP Address	<input type="text"/>	<input type="text"/>
Subnet Mask / Prefix	<input type="text"/>	<input type="text"/>
Default Gateway	<input type="text"/>	<input type="text"/>
Primary DNS Server	<input type="text"/>	<input type="text"/>
Secondary DNS Server	<input type="text"/>	<input type="text"/>

SSID

Probe Hidden SSID disabled

Country Code *

Authentication open

Encryption none

WEP Key Type ASCII

WEP Default Key 1

WEP Key 1

WEP Key 2

WEP Key 3

WEP Key 4

WPA PSK Type 256-bit secret

WPA PSK

RADIUS EAP Authentication EAP-PEAP/MSCHAPv2

RADIUS CA Certificate

No file chosen

RADIUS Local Certificate

No file chosen

RADIUS Local Private Key

No file chosen

RADIUS Identity

RADIUS Password

Syslog Level informational

Extra options *

* can be blank

Figure 32: WiFi Station Configuration Page

Item	Description
Enable WiFi STA	Enable WiFi station (STA).
DHCP Client	Activates/deactivates DHCP client. If in IPv6 column, the DHCPv6 client is enabled.
IP Address	A fixed IP address of the WiFi interface. Use IPv4 notation in IPv4 column and IPv6 notation in IPv6 column. Shortened IPv6 notation is supported.
Subnet Mask / Prefix	Specifies a Subnet Mask for the IPv4 address. In the IPv6 column, fill in the Prefix for the IPv6 address – number in range 0 to 128.
Default Gateway	Specifies the IP address of a default gateway. If filled-in, every packet with the destination not found in the routing table is sent there. Use proper IP address notation in IPv4 and IPv6 column.
Primary DNS Server	Specifies the primary IP address of the DNS server. When the IP address is not found in the Routing Table, the this DNS server is requested. Use proper IP address notation in IPv4 and IPv6 column.
Secondary DNS Server	Specifies the secondary IP address of the DNS server.
SSID	The unique identifier of WiFi network.
Probe Hidden SSID	AP with a hidden SSID (see Broadcast SSID option in the AP configuration) doesn't respond to broadcast probe requests, so the station doesn't have necessary info to connect. Enable this option to force the station probe a specific SSID. It's better to disable it if you don't expect a hidden SSID to avoid messing the radio with useless transmission.
Country Code	<p>This option is not available for NAM routers – the "US" country code is set by default on these versions of router.</p> <p>Code of the country where the router is installed. This code must be entered in ISO 3166-1 alpha-2 format. If a <i>country code</i> is not specified and the router has not implemented a system to determine this code, it will use "US" as the default <i>country code</i>.</p> <p>If no <i>country code</i> is specified or if the wrong country code is entered, the router may violate country-specific regulations for the use of WiFi frequency bands.</p>

Continued on the next page

Continued from previous page

Item	Description
Authentication	<p>Access control and authorization of users in the WiFi network.</p> <ul style="list-style-type: none"> • Open – Authentication is not required (free access point). • Shared – Authentication based on PreShared-Keys using WEP protocol (insecure today). • WPA-PSK – Authentication based on PreShared-Keys using original WPA protocol (insecure today). • WPA2-PSK – Authentication based on PreShared-Keys using standard WPA2 protocol. • WPA3-PSK – Authentication based on PreShared-Keys using newest WPA3 protocol. • WPA-Enterprise – Authentication based on RADIUS using original WPA protocol (insecure today). • WPA2-Enterprise – Authentication based on RADIUS using standard WPA2 protocol. • WPA3-Enterprise – Authentication based on RADIUS using newest WPA3 protocol. • 802.1X – Authentication using RADIUS (802.1X standard) using WEP protocol (insecure today).
Encryption	<p>Type of data encryption in the WiFi network:</p> <ul style="list-style-type: none"> • None – No data encryption. • WEP – Encryption using static WEP keys. This encryption can be used together with Shared authentication. However, it is not secure and may be unavailable for some models. • TKIP – Older dynamic encryption key management that can be used together with WPA and WPA2 authentication. • AES – Newer dynamic encryption can be used together with WPA2 and WPA3 authentication.
WEP Key Type	<p>Type of WEP key for WEP encryption:</p> <ul style="list-style-type: none"> • ASCII – WEP key in ASCII format. • HEX – WEP key in hexadecimal format.
WEP Default Key	<p>This specifies the default WEP key.</p>

Continued on the next page

Continued from previous page

Item	Description
WEP Key 1–4	<p>Allows entry of four different WEP keys:</p> <ul style="list-style-type: none"> • WEP key in ASCII format must be entered in quotes. This key can be specified in the following lengths. <ul style="list-style-type: none"> – 5 ASCII characters (40b WEP key) – 13 ASCII characters (104b WEP key) – 16 ASCII characters (128b WEP key) • WEP key in hexadecimal format must be entered in hexadecimal digits. This key can be specified in the following lengths. <ul style="list-style-type: none"> – 10 hexadecimal digits (40b WEP key) – 26 hexadecimal digits (104b WEP key) – 32 hexadecimal digits (128b WEP key)
WPA PSK Type	<p>The possible key option for WPA-PSK authentication.</p> <ul style="list-style-type: none"> • 256-bit secret • ASCII passphrase
WPA PSK	<p>Key for WPA-PSK authentication. This key must be entered according to the selected WPA PSK type as follows.</p> <ul style="list-style-type: none"> • 256-bit secret – 64 hexadecimal digits • ASCII passphrase – 8 to 63 characters
RADIUS EAP Authentication	<p>EAP protocol used to protect authentication.</p> <ul style="list-style-type: none"> • EAP-PEAP/MSCHAPv2 – use TLS only to protect legacy EAP authentication. • EAP-TLS – use TLS to mutual authentication of client to server and server to client with TLS.
RADIUS CA Certificate	Certification Authority Certificate to verify a server certificate when EAP-TLS is selected.
RADIUS Local Certificate	Client certificate when EAP-TLS is selected.
RADIUS Local Private Key	Client Private Key when EAP-TLS is selected.
RADIUS Identity	Identity for connecting to RADIUS server.
RADIUS Password	Password to authenticate RADIUS Identity when EAP-PEAP/MSCHAPv2 is selected.
RADIUS Local Private Key Password	Password to access RADIUS Local Private Key when EAP-TLS is selected.

Continued on the next page

Continued from previous page

Item	Description
Syslog Level	Logging level, when system writes to the system log. <ul style="list-style-type: none">• Verbose debugging – The highest level of logging.• Debugging• Informational – Default level of logging.• Notification• Warning – The lowest level of system communication.
Extra options	Allows the user to define additional parameters for the hostapd. Options are added as is to the end of a configuration file. For more information, see hostapd.conf Linux man page. Use only if you know what you are doing.

Table 31: WLAN Configuration Items Description

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

3.8 Bluetooth Support

Certain WiFi router models, as detailed in the *Hardware Manual*, come with the capability to support Bluetooth functionality; however, this feature is not activated by default within the firmware. To enable Bluetooth capabilities, the *Bluetooth Router App* needs to be installed on the router. For comprehensive guidelines on the installation process and Bluetooth parameters, refer to the router's *Hardware Manual*.

3.9 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 33.

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 3.9.1.

If you want to set up this feature your way, see Chapter 3.9.2 for more information.

3.9.1 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 neither an IP address is configured nor the DHCP client is enabled for this ETH interface.



Just for the default priorities mode: Unplugging the Ethernet cable does not switch the WAN interface to the next one in order.

3.9.2 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 33. 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 32.

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 3.9.1.
Mode	<p>Single WAN</p> <ul style="list-style-type: none"> • 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. <p>Multiple WANs</p> <ul style="list-style-type: none"> • 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 <i>Single WAN</i> mode. <p>Load Balancing</p> <ul style="list-style-type: none"> • 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 32: Backup Routes Modes Items Description

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 3.4.1.



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 IPv4 address or domain name of ping queries to check the connection.
Ping IPv6 Address	Destination IPv6 address or domain name of ping queries to check the connection.
Ping Interval	The time interval between consecutive ping queries.
Ping Timeout	Time in seconds to wait for a response to the ping.
Weight	Weight for the Load Balancing mode only. The number from 1 to 256 determines the ratio for load balancing of the interface. For example, if two interfaces 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 33: Backup Routes Configuration Items Description

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.
- To monitor the interface availability, you can use one or both Ping IP Addresses (IPv4 and IPv6) based on the IP protocol used on a particular network interface and WAN connection settings.

Backup Routes Configuration	
<input type="checkbox"/> Enable backup routes switching	
Mode	Single WAN
<input type="checkbox"/> Enable backup routes switching for Mobile WAN	
Priority	1st
Weight	
<input type="checkbox"/> Enable backup routes switching for PPPoE	
Priority	1st
Ping IP Address	
Ping IPv6 Address	
Ping Interval	
	sec
Ping Timeout	10
	sec
Weight	
<input type="checkbox"/> Enable backup routes switching for WiFi STA	
Priority	1st
Ping IP Address	
Ping IPv6 Address	
Ping Interval	
	sec
Ping Timeout	10
	sec
Weight	
<input type="checkbox"/> Enable backup routes switching for ETH0	
Priority	1st
Ping IP Address	
Ping IPv6 Address	
Ping Interval	
	sec
Ping Timeout	10
	sec
Weight	
<input type="checkbox"/> Enable backup routes switching for ETH1	
Priority	1st
Ping IP Address	
Ping IPv6 Address	
Ping Interval	
	sec
Ping Timeout	10
	sec
Weight	
<input type="button" value="Apply"/>	

Figure 33: Backup Routes Configuration Page

3.9.3 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 3.9.1. Figure 34 shows the GUI configuration.

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



Figure 34: Example #1: GUI Configuration

Figure 35 illustrates the example topology.

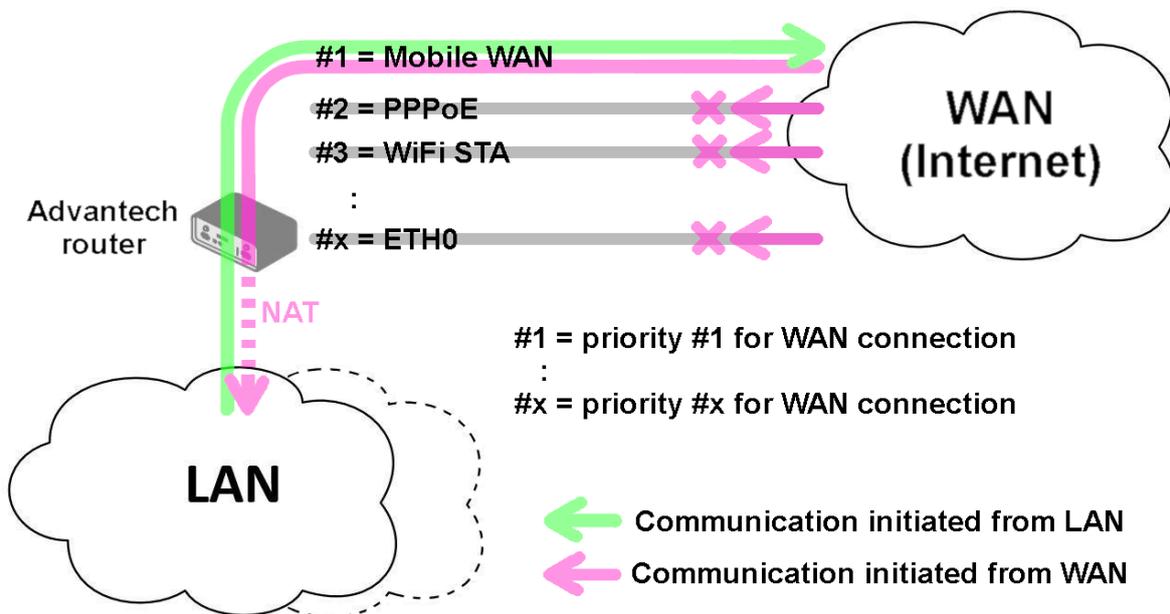


Figure 35: Example #1: Topology

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 3.9.1. Figure 36 shows the GUI configuration.

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

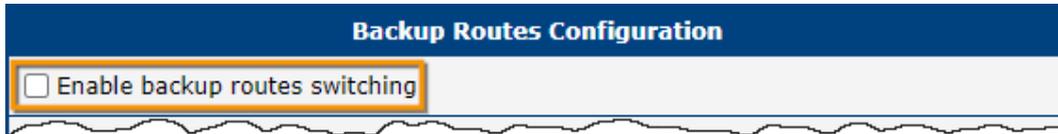


Figure 36: Example #2: GUI Configuration

Figure 37 illustrates the example topology.

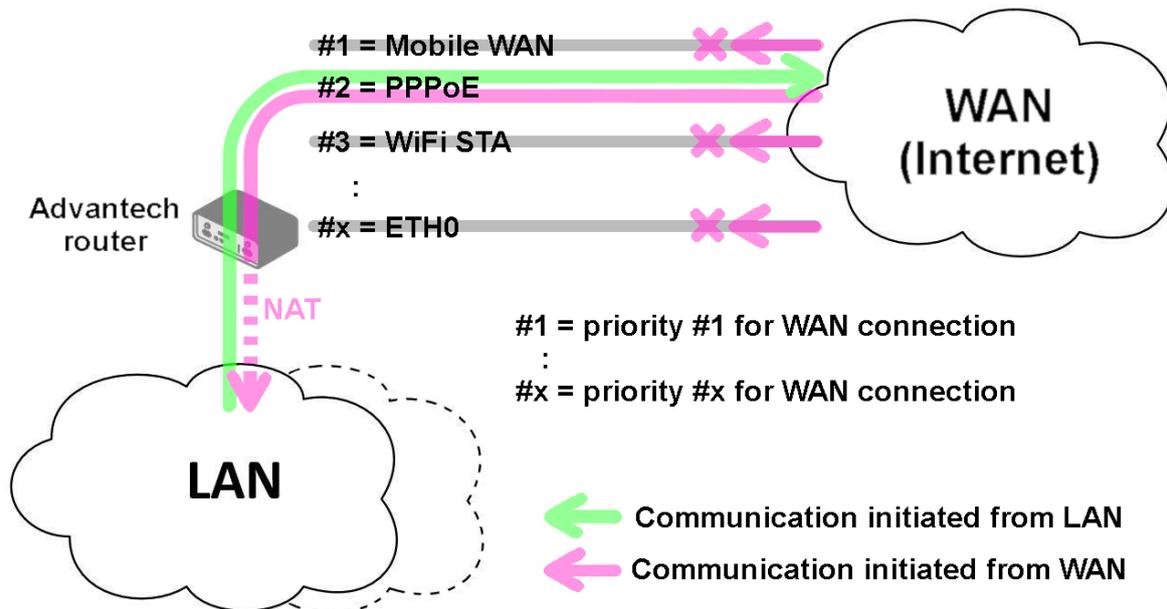


Figure 37: Example #2: Topology

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 38 shows the GUI configuration.

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

Backup Routes Configuration

Enable backup routes switching
Mode Single WAN

Enable backup routes switching for Mobile WAN
Priority 1st
Weight

Enable backup routes switching for PPPoE
Priority 2nd
Ping IP Address 172.16.1.1
Ping IPv6 Address
Ping Interval 30 sec
Ping Timeout 10 sec
Weight

Enable backup routes switching for WiFi STA

Enable backup routes switching for ETH0

Enable backup routes switching for ETH1
Priority 3rd
Ping IP Address
Ping IPv6 Address
Ping Interval sec
Ping Timeout 10 sec
Weight

Apply

Figure 38: Example #3: GUI Configuration

Figure 39 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 40 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.

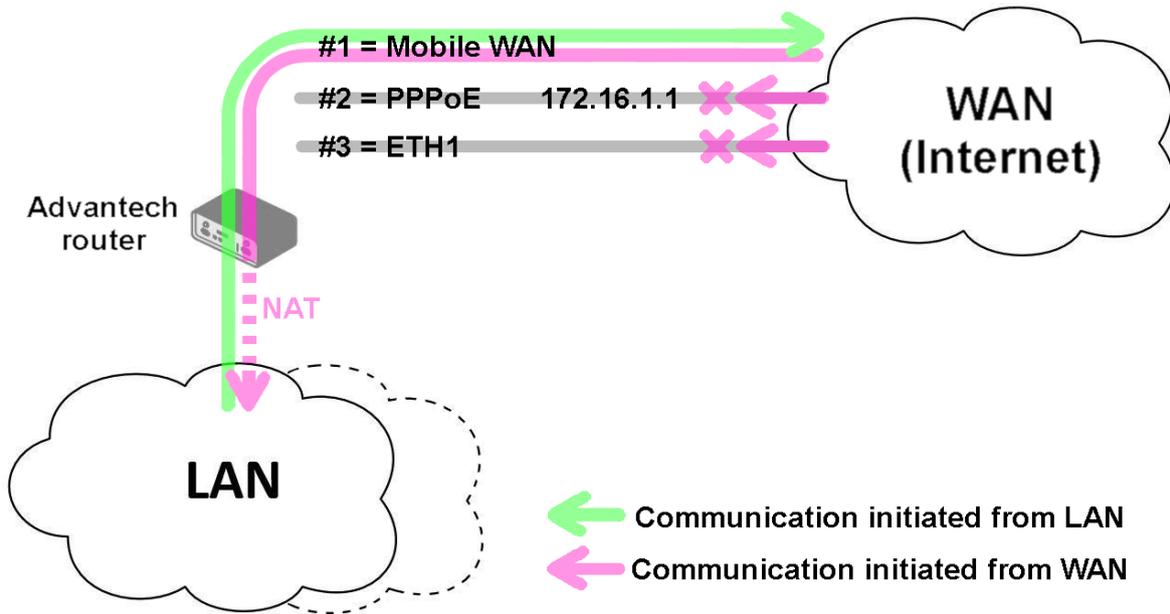


Figure 39: Example #3: Topology for *Single WAN* mode

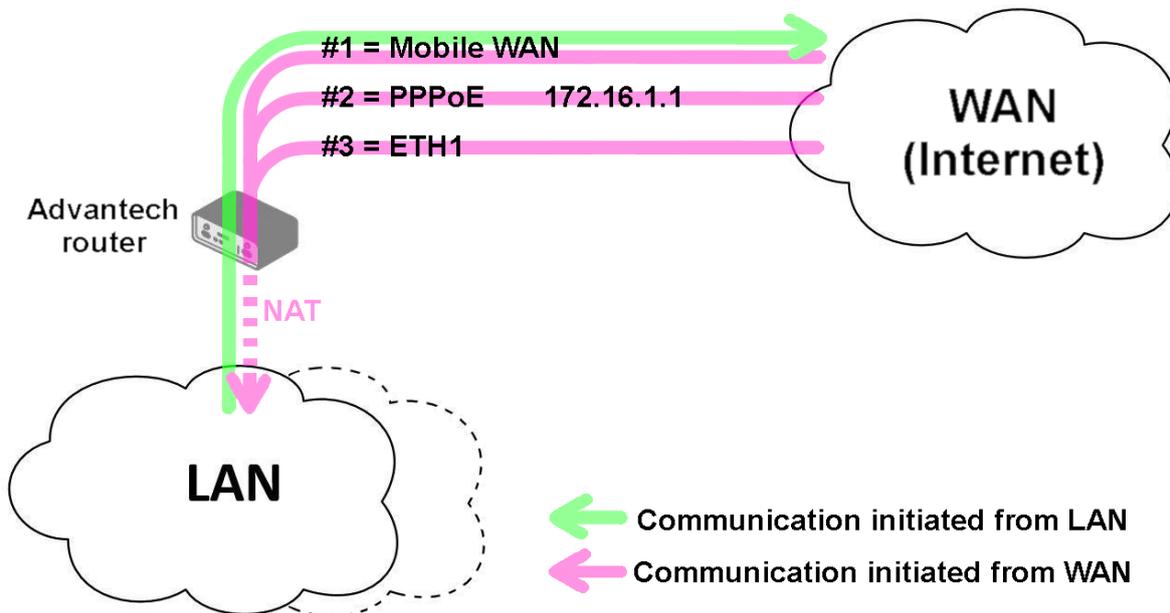


Figure 40: Example #3: Topology for *Multiple WAN* mode

Example #4: Load Balancing 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 41 shows the GUI configuration.

Backup Routes Configuration	
<input checked="" type="checkbox"/> Enable backup routes switching	
Mode	Load Balancing
<input checked="" type="checkbox"/> Enable backup routes switching for Mobile WAN	
Priority	1st
Weight	4
<input checked="" type="checkbox"/> Enable backup routes switching for PPPoE	
Priority	2nd
Ping IP Address	
Ping IPv6 Address	
Ping Interval	
Ping Timeout	10
Weight	1

Figure 41: Example #4: GUI Configuration

Figure 42 illustrates the example topology.

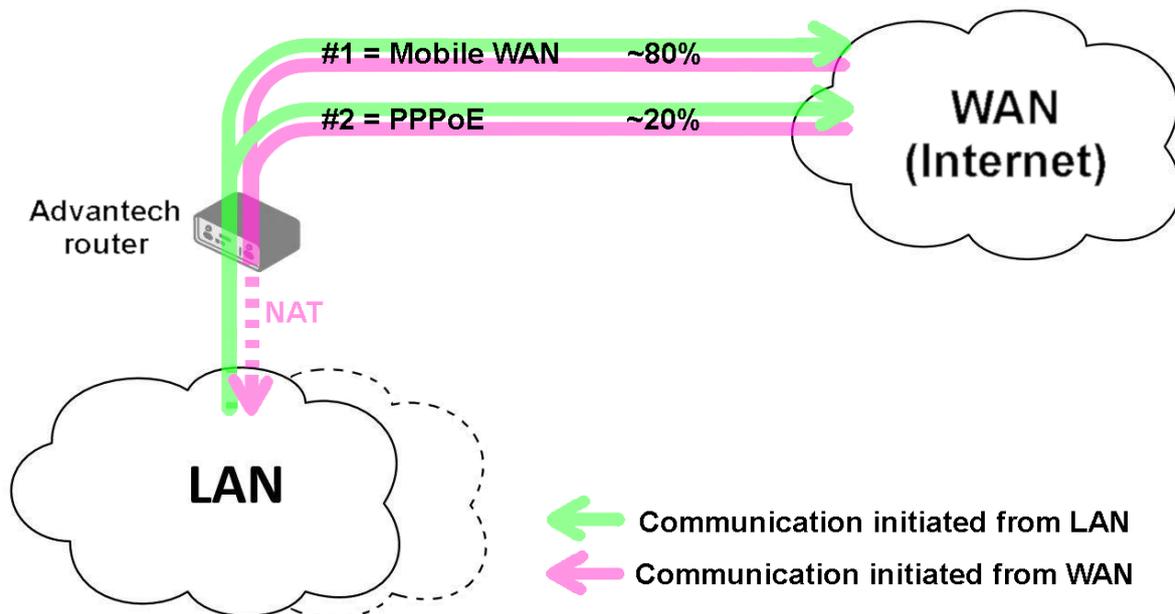


Figure 42: Example #4: Topology

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 43 shows the GUI configuration.

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

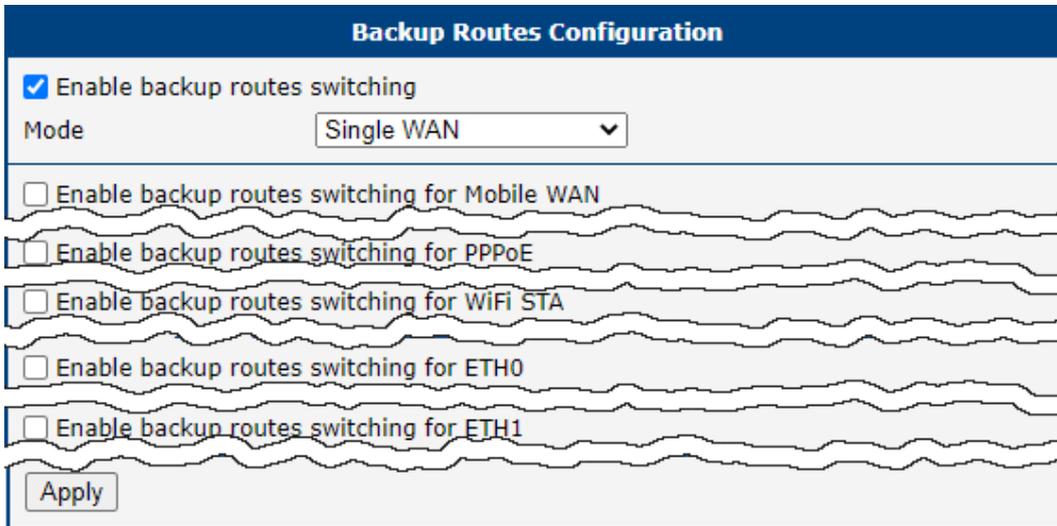


Figure 43: Example #5: GUI Configuration

Figure 44 illustrates the example topology.

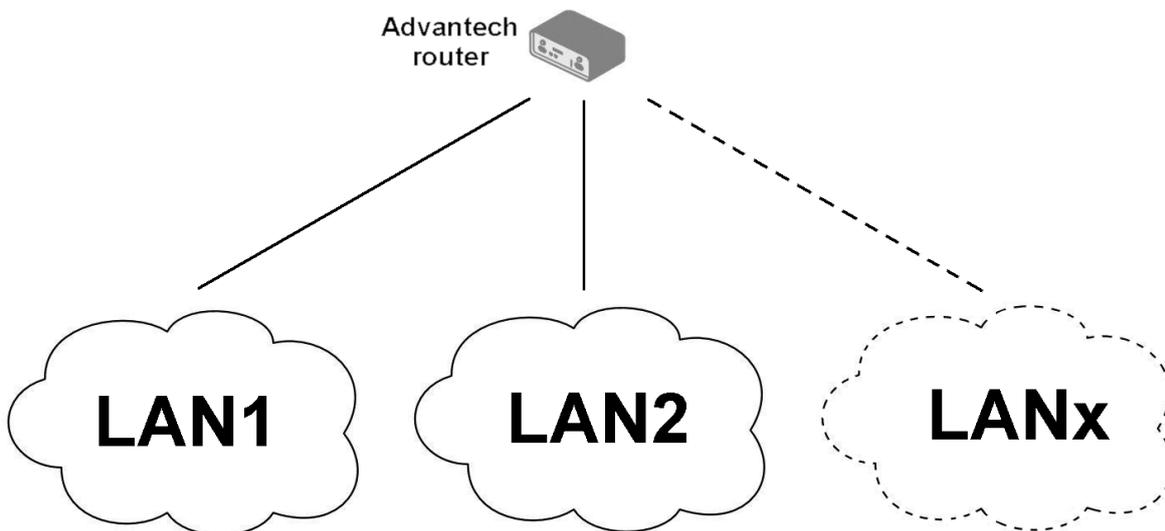


Figure 44: Example #5: Topology

3.10 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. There are two forms, one for IPv4 and the second for IPv6 configuration. Static routes configuration form for IPv4 is shown on Figure 45.

IPv4 Static Routes Configuration					
<input type="checkbox"/>	Enable IPv4 static routes				
	Destination Network	Mask or Prefix Length	Gateway *	Metric *	Interface
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	ETH0 ▼
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	ETH0 ▼
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	ETH0 ▼
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	ETH0 ▼
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	ETH0 ▼
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	ETH0 ▼
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	ETH0 ▼
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	ETH0 ▼

* can be blank

Apply

Figure 45: Static Routes Configuration Page

The description of all items is listed in Table 34.

Item	Description
Enable IPv4 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 34: Static Routes Configuration for IPv4

3.11 Firewall

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

The screenshot shows the 'IPv6 Firewall Configuration' form. It is divided into several sections:

- Enable filtering of incoming packets:** A checkbox at the top left. Below it is a table with columns: Source *, Protocol, Target Port(s) *, Action, and Description *. There are four rows, each with a checkbox on the left, a text input for Source, a dropdown for Protocol (all), a text input for Target Port(s), a dropdown for Action (allow), and a text input for Description.
- Enable filtering of forwarded packets:** A checkbox. Below it is a table with columns: Source *, Destination *, Protocol, Target Port(s) *, Action, and Description *. There are three rows, each with a checkbox on the left, text inputs for Source and Destination, a dropdown for Protocol (all), a text input for Target Port(s), a dropdown for Action (allow), and a text input for Description.
- Enable filtering of locally destined packets:** A checkbox.
- Enable protection against DoS attacks:** A checkbox.

At the bottom, there is a note: '* can be blank' and an 'Apply' button.

Figure 46: Firewall Configuration – IPv6 Firewall

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 3.9.1 to see the priority rules for the WAN interfaces. See Table 35 for the incoming definition table description.

Item	Description
Source	IP address the rule applies to. Use IPv4 address in <i>IPv4 Firewall Configuration</i> and IPv6 address in <i>IPv6 Firewall Configuration</i> .
Protocol	Specifies the protocol the rule applies to: <ul style="list-style-type: none"> • all – The rule applies to all protocols. • TCP – The rule applies to TCP protocol. • UDP – The rule applies to UDP protocol. • GRE – The rule applies to GRE protocol. • ESP – The rule applies to ESP protocol. • ICMP/ICMPv6 – The rule applies to ICMP protocol. In <i>IPv6 Firewall Configuration</i> there is the ICMPv6 option.
Target Port(s)	The port numbers range allowing access to the router. Enter the initial and final port numbers separated by the hyphen mark. One static port is allowed as well.
Action	Specifies the rule – the type of action the router performs: <ul style="list-style-type: none"> • allow – The router allows the packets to enter the network. • deny – The router denies the packets from entering the network.
Description	Description of the rule.

Table 35: 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 36 for the forwarding definition table description.

Item	Description
Source	IP address the rule applies to. Use IPv4 address in <i>IPv4 Firewall Configuration</i> and IPv6 address in <i>IPv6 Firewall Configuration</i> .
Destination	Destination IP address the rule applies to. Use IPv4 address in <i>IPv4 Firewall Configuration</i> and IPv6 address in <i>IPv6 Firewall Configuration</i> .

Continued on next page

Continued from previous page

Item	Description
Protocol	Specifies the protocol the rule applies to: <ul style="list-style-type: none"> • all – The rule applies to all protocols. • TCP – The rule applies to TCP protocol. • UDP – The rule applies to UDP protocol. • GRE – The rule applies to GRE protocol. • ESP – The rule applies to ESP protocol. • ICMP/ICMPv6 – The rule applies to ICMP protocol. In <i>IPv6 Firewall Configuration</i> there is the ICMPv6 option.
Target Port(s)	The target port numbers. Enter the initial and final port numbers separated by the hyphen mark. One static port is allowed as well.
Action	Specifies the rule – the type of action the router performs: <ul style="list-style-type: none"> • allow – The router allows the packets to enter the network. • deny – The router denies the packets from entering the network.
Description	Description of the rule.

Table 36: Forwarding filtering

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

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

3.11.1 Sites

On the *Sites* configuration page, you can configure URL addresses that will be blocked by the firewall, see Figure 47. Tick the *Enable sites blocking* checkbox and define URL addresses in the *Block list* box, each address on a separate line. You can use the *Load From File...* button to load addresses stored in a plain text file.



Figure 47: Firewall Sites Configuration GUI

3.11.2 Example of the IPv4 Firewall Configuration

The router allows the following access:

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

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

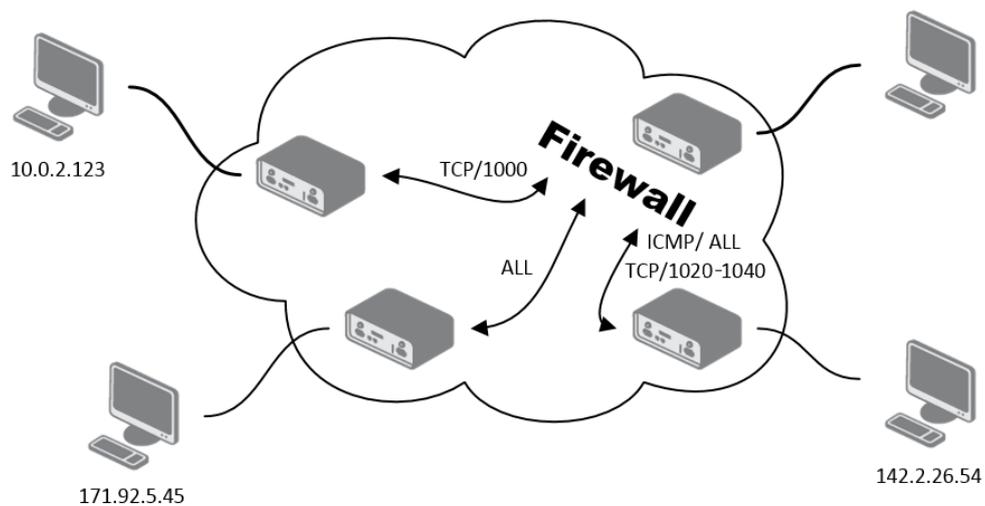


Figure 48: Topology for the IPv4 Firewall Configuration Example

IPv4 Firewall Configuration

Enable filtering of incoming packets

Source *	Protocol	Target Port(s) *	Action	Description *
<input checked="" type="checkbox"/> 171.92.5.45	all		allow	
<input checked="" type="checkbox"/> 10.0.2.123	TCP	1000	allow	
<input checked="" type="checkbox"/> 142.2.26.54	ICMP		allow	
<input checked="" type="checkbox"/> 142.2.26.54	TCP	1020-1040	allow	
<input type="checkbox"/>	all		allow	
<input type="checkbox"/>	all		allow	
<input type="checkbox"/>	all		allow	
<input type="checkbox"/>	all		allow	

Enable filtering of forwarded packets

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

Enable filtering of locally destined packets

Enable protection against DoS attacks
* can be blank

Figure 49: IPv4 Firewall Configuration Example

3.12 NAT

To configure the address translation function, click on *NAT* in the *Configuration* section of the main menu, see Figure 50. There are independent IPv4 and IPv6 NAT configurations available since the router supports dual-stack IPv4 and IPv6. The configuration fields have the same meaning for both the IPv4 and IPv6 configuration pages.

The router 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 pass through the router. This configuration form allows you to specify up to 16 PAT rules. Table 37 provides a description of the first part of the rule definition.

Item	Description
Public Port(s)	The public port numbers range for NAT. Enter the initial and final port numbers separated by the hyphen mark. One static port is allowed as well.
Private Port(s)	The private port numbers range for NAT. Enter the initial and final port numbers separated by the hyphen mark. One static port is allowed as well.
Type	Protocol type – TCP or UDP.
Server IPv4 address	In <i>IPv4 NAT Configuration</i> only. IPv4 address where the router forwards incoming data.
Server IPv6 address	In <i>IPv6 NAT Configuration</i> only. IPv6 address where the router forwards incoming data.
Description	Description of the rule.

Table 37: NAT Configuration Items Description

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



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

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

For IPv6 NAT use `ip6tables` command with same options.:



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

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



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

Parameters for routing of incoming data from the WAN (Mobile WAN) to a connected computer are described in Table 39.

Item	Description
Send all remaining incoming packets to default server	Activates/deactivates forwarding unmatched incoming packets to the default server. The prerequisite for this function is that you specify a default server in the <i>Default Server IPv4/IPv6 Address</i> field. The router can forward incoming data from the mobile WAN to a computer with the assigned IP address.
Default Server IPv4/IPv6 Address	The IPv4/IPv6 address of the default server.

Table 39: Incoming Packets Configuration

The description of the configuration options for NAT helpers, which assist with the proper handling of certain protocols, is shown in Table 40. These options allow for more efficient handling of specific protocols when NAT is in use, ensuring proper packet forwarding and connection stability for FTP and VPN traffic.

Item	Description
Masquerade outgoing packets	When enabled, this option activates Network Address Translation (NAT) for outgoing packets. This ensures that all outgoing traffic appears to come from the router's external IP address, hiding the internal network structure.
Enable SIP ALG	(NAT IPv4 only) This option enables the SIP Application Layer Gateway (ALG). When enabled, the router modifies SIP packets to allow for proper traversal of NAT, which is commonly needed for VoIP traffic.
Enable FTP Helper on public port(s)	When this option is enabled, the router assists in handling FTP traffic on the specified public port (default: 21). The FTP Helper helps with the traversal of FTP traffic through NAT, especially for active FTP sessions.
Enable PPTP Helper on public port(s)	(NAT IPv4 only) This option enables the PPTP (Point-to-Point Tunneling Protocol) Helper for VPN traffic on the specified public port (default: 1723). The PPTP Helper ensures proper handling of PPTP traffic through NAT.

Table 40: Masquerade Configuration

3.12.1 Examples of NAT Configuration

Example 1: IPv4 NAT Configuration with Single Device Connected

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

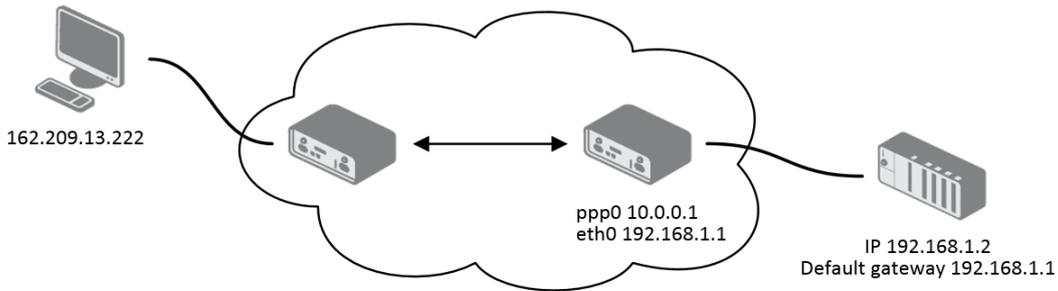


Figure 51: Topology for NAT Configuration Example 1

IPv4 NAT Configuration				
Public Port(s)	Private Port(s)	Type	Server IP Address	Description *
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> Enable remote HTTP access on port <input type="text" value="80"/>				
<input type="checkbox"/> Enable remote HTTPS access on port <input type="text" value="443"/>				
<input type="checkbox"/> Enable remote FTP access on port <input type="text" value="21"/>				
<input type="checkbox"/> Enable remote SSH access on port <input type="text" value="22"/>				
<input type="checkbox"/> Enable remote Telnet access on port <input type="text" value="23"/>				
<input checked="" type="checkbox"/> Enable remote SNMP access on port <input type="text" value="161"/>				
<input checked="" type="checkbox"/> Send all remaining incoming packets to default server Default Server IP Address <input type="text" value="192.168.1.2"/>				
<input checked="" type="checkbox"/> Masquerade outgoing packets				
<input type="checkbox"/> Enable SIP ALG				
<input checked="" type="checkbox"/> Enable FTP Helper on public port(s) <input type="text" value="21"/>				
<input type="checkbox"/> Enable PPTP Helper on public port(s) <input type="text" value="1723"/>				
* can be blank				
<input type="button" value="Apply"/>				

Figure 52: NAT Configuration for Example 1

Example 2: IPv4 NAT Configuration with Multiple Devices Connected

In this example, a switch is used to connect multiple devices behind the router. Each device connected behind the router has its own IP address. Enter the address in the *Server IP Address* field in the NAT dialog. The devices are communicating on port 80, but you can configure port forwarding using the *Public Port* and *Private Port* fields in the NAT dialog. This setup allows you to access the 192.168.1.2:80 socket behind the router by accessing the IP address 10.0.0.1:81 from the Internet. If you send a ping request to the public IP address of the router (10.0.0.1), the router responds as usual (without forwarding). Since the *Send all remaining incoming packets to default server* option is inactive, the router denies connection attempts.

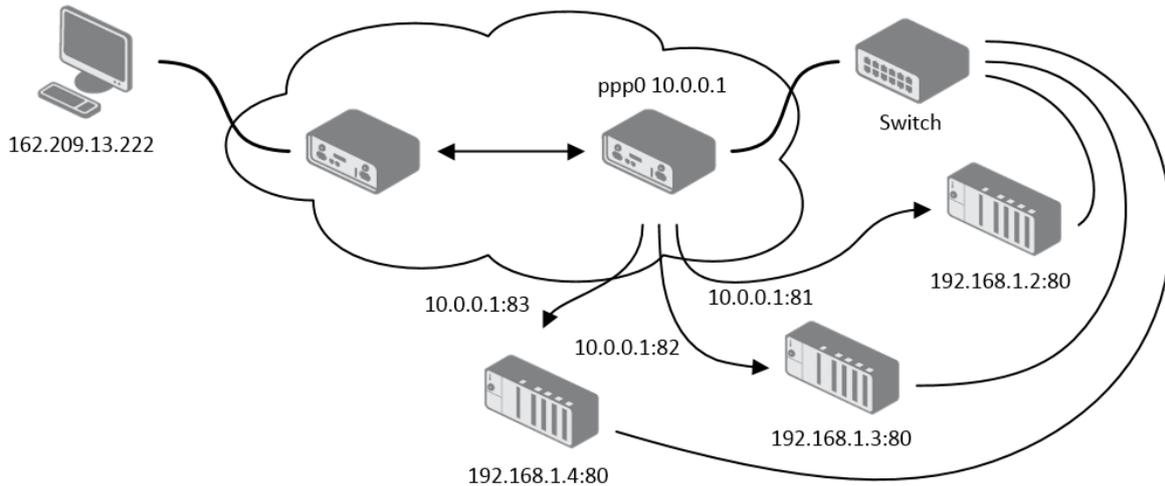


Figure 53: Topology for NAT Configuration Example 2

IPv4 NAT Configuration				
Public Port(s)	Private Port(s)	Type	Server IP Address	Description *
81	80	TCP	192.168.1.2	
82	80	TCP	192.168.1.3	
83	80	TCP	192.168.1.4	
		TCP		

Enable remote HTTP access on port

Enable remote SNMP access on port

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

Masquerade outgoing packets
 Enable SIP ALG
 Enable FTP Helper on public port(s)
 Enable PPTP Helper on public port(s)

* can be blank

Figure 54: NAT Configuration for Example 2

3.13 OpenVPN Tunnel

Select the *OpenVPN* item to configure an OpenVPN tunnel. The menu item will expand and you will see separate configuration pages: *1st Tunnel*, *2nd Tunnel*, *3rd Tunnel* and *4th Tunnel*. The OpenVPN tunnel function allows you to create a secure connection between two separate LAN networks. The router allows you to create up to **four OpenVPN tunnels**. IPv4 and IPv6 dual stack is supported.

Item	Description
Description	Specifies the description or name of tunnel.
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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • UDP – The OpenVPN communicates using UDP. • TCP server – The OpenVPN communicates using TCP in server mode. • TCP client – The OpenVPN communicates using TCP in client mode. • UDPv6 – The OpenVPN communicates using UDP over IPv6. • TCPv6 server – The OpenVPN communicates using TCP over IPv6 in server mode. • TCPv6 client – The OpenVPN communicates using TCP over IPv6 in client mode.
UDP/TCP port	Specifies the port of the relevant protocol (UDP or TCP).
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	IPv4 address of a network behind opposite side of the tunnel.
Remote Subnet Mask	IPv4 subnet mask of a network behind opposite tunnel's side.
Redirect Gateway	Adds (rewrites) the default gateway. All the packets are then sent to this gateway via tunnel, if there is no other specified default gateway inside them.
Local Interface IP Address	Specifies the IPv4 address of a local interface. For proper routing it is recommended to fill-in any IPv4 address from local range even if you are using IPv6 tunnel only.
Remote Interface IP Address	Specifies the IPv4 address of the interface of opposite side of the tunnel. For proper routing it is recommended to fill-in any IPv4 address from local range even if you are using IPv6 tunnel only.
Remote IPv6 Subnet	IPv6 address of the remote IPv6 network. Equivalent of the <i>Remote Subnet</i> in IPv4 section.

Continued on next page

Continued from previous page

Item	Description
Remote IPv6 Prefix	IPv6 prefix of the remote IPv6 network. Equivalent of the <i>Remote Subnet Mask</i> in IPv4 section.
Local Interface IPv6 Address	Specifies the IPv6 address of a local interface.
Remote Interface IPv6 Address	Specifies the IPv6 address of the interface of opposite side of the tunnel.
Ping Interval	Time interval after which the router sends a message to opposite side of tunnel to verify the existence of the tunnel.
Ping Timeout	Specifies the time interval the router waits for a message sent by the opposite side. For proper verification of the OpenVPN tunnel, set the <i>Ping Timeout</i> to greater than the <i>Ping Interval</i> .
Renegotiate Interval	Specifies the renegotiate period (reauthorization) of the OpenVPN tunnel. You can only set this parameter when the <i>Authenticate Mode</i> is set to <i>username/password</i> or <i>X.509 certificate</i> . After this time period, the router changes the tunnel encryption to keep the tunnel secure.
Max Fragment Size	Maximum size of a sent packet.
Compression	Compression of the data sent: <ul style="list-style-type: none"> • none – No compression is used. • LZO – A lossless compression is used, use the same setting on both sides of the tunnel.
NAT Rules	Activates/deactivates the NAT rules for the OpenVPN tunnel: <ul style="list-style-type: none"> • not applied – NAT rules are not applied to the tunnel. • applied – NAT rules are applied to the OpenVPN tunnel.
Authenticate Mode	Specifies the authentication mode: <ul style="list-style-type: none"> • none – No authentication is set. • Pre-shared secret – Specifies the shared key function for both sides of the tunnel. • Username/password – Specifies authentication using a CA Certificate, Username and Password. • X.509 Certificate (multiclient) – Activates the X.509 authentication in multi-client mode. • X.509 Certificate (client) – Activates the X.509 authentication in client mode. • X.509 Certificate (server) – Activates the X.509 authentication in server mode.

Continued on next page

Continued from previous page

Item	Description
Security Mode	Choose the security mode, <i>tls-auth</i> or <i>tls-crypt</i> . We recommend to use the <i>tls-crypt</i> 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, see chap. 1.3.2!
Security Level	Set the Security Level ¹ : <ul style="list-style-type: none"> • 0 - Weak – [Default] Everything is permitted. This setting is not recommended; it is advisable to set a higher security level! • 1 - Low – 80 bits of security. • 2 - Medium – 112 bits of security. • 3 - High – 128 bits of security. • 4 - Very High – 192 bits of security.
User's Up Script	Custom script, executed when the OpenVPN tunnel is established.
User's Down Script	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 <code>openvpn --help</code> command.

Table 41: OpenVPN Configuration Items Description



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.

¹For detailed explanation see the *Security Guidelines* [15], specifically the chapter on *Cryptographic algorithms*.

²Parameters 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.

1st OpenVPN Tunnel Configuration	
<input type="checkbox"/> Create 1st OpenVPN tunnel	
Description *	<input type="text"/>
Interface Type	TUN ▼
Protocol	UDP ▼
UDP Port	1194
1st Remote IP Address *	<input type="text"/>
2nd Remote IP Address *	<input type="text"/>
Remote Subnet *	<input type="text"/>
Remote Subnet Mask *	<input type="text"/>
Redirect Gateway	no ▼
Local Interface IP Address	<input type="text"/>
Remote Interface IP Address	<input type="text"/>
Remote IPv6 Subnet *	<input type="text"/>
Remote IPv6 Subnet Prefix Length *	<input type="text"/>
Local Interface IPv6 Address *	<input type="text"/>
Remote Interface IPv6 Address *	<input type="text"/>
Ping Interval *	<input type="text"/> sec
Ping Timeout *	<input type="text"/> sec
Renegotiate Interval *	<input type="text"/> sec
Max Fragment Size *	<input type="text"/> bytes
Compression	LZO ▼
NAT Rules	not applied ▼
Authenticate Mode	none ▼
Security Mode	tls-auth ▼
Pre-shared Secret	<input type="text"/>
CA Certificate	<input type="text"/>
DH Parameters	<input type="text"/>
Local Certificate	<input type="text"/>
Local Private Key	<input type="text"/>
Local Passphrase *	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Security Level	0 - Weak ▼
User's Up Script	<pre>#!/bin/sh # # This script will be executed when OpenVPN tunnel is up.</pre>
User's Down Script	<pre>#!/bin/sh # # This script will be executed when OpenVPN tunnel is down.</pre>
Extra Options *	<input type="text"/>
<i>* can be blank</i>	
<input type="button" value="Apply"/>	

Figure 55: OpenVPN tunnel configuration Page

3.13.1 Example of the OpenVPN Tunnel Configuration in IPv4 Network

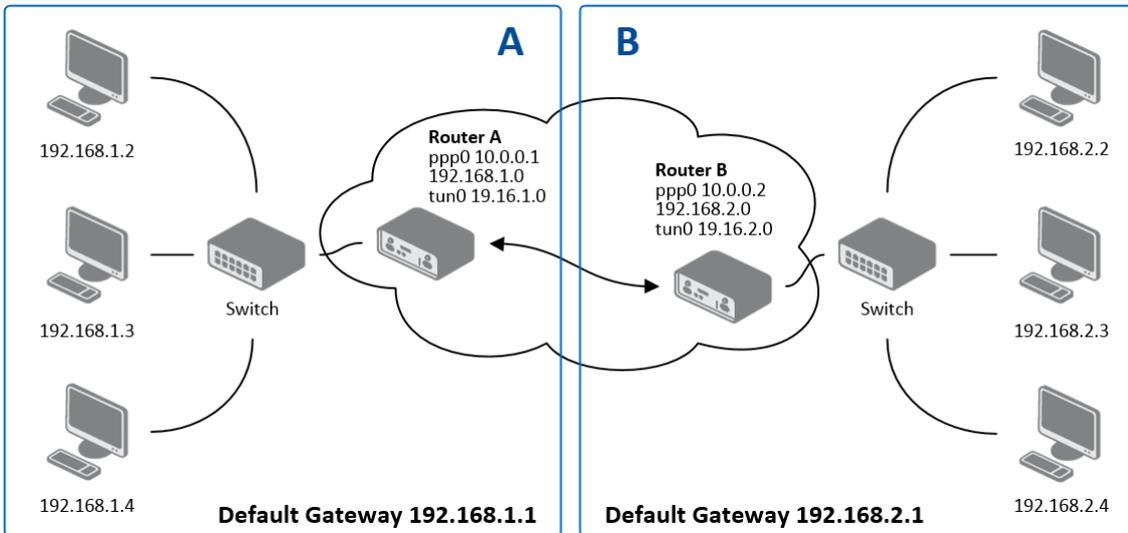


Figure 56: Topology of OpenVPN Configuration Example

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 42: OpenVPN Configuration Example



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

3.14 IPsec

The IPsec tunnel function allows you to create a secured connection between two separate LAN networks. These router family 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 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 3.14.1.

IPv4 and IPv6 tunnels are supported (**dual stack**), you can transport IPv6 traffic through IPv4 tunnel and vice versa. For different IPsec authentication scenarios, see Chapter 3.14.2.



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* [6].



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

3.14.1 Route-based Configuration Scenarios

There are more different route-based configuration options which can be configured and used in Advantech 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: `tcdump -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 Advantech 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.

3.14.2 IPsec Authentication Scenarios

There are four basic authentication options which can be configured and used in Advantech 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.

3.14.3 Configuration Items Description

The configuration GUI for IPsec is shown in Figure 57 and the description of all items, which can be configured for an IPsec tunnel, are described in Table 43.

1st IPsec Tunnel Configuration	
<input type="checkbox"/> Create 1st IPsec tunnel	
Description *	<input type="text"/>
Type	policy-based
Host IP Mode	IPv4
1st Remote IP Address *	<input type="text"/>
2nd Remote IP Address *	<input type="text"/>
Tunnel IP Mode	IPv4
Remote ID *	<input type="text"/>
Local ID *	<input type="text"/>
Install Routes	yes
First Remote Subnet *	<input type="text"/>
First Remote Subnet Mask *	<input type="text"/>
Second Remote Subnet *	<input type="text"/>
Second Remote Subnet Mask *	<input type="text"/>
Remote Protocol/Port *	<input type="text"/>
First Local Subnet *	<input type="text"/>
First Local Subnet Mask *	<input type="text"/>
Second Local Subnet *	<input type="text"/>
Second Local Subnet Mask *	<input type="text"/>
Local Protocol/Port *	<input type="text"/>
MTU	1426 bytes
Remote Virtual Network *	<input type="text"/>
Remote Virtual Mask *	<input type="text"/>
Local Virtual Address *	<input type="text"/>
Cisco FlexVPN **	no
Encapsulation Mode	tunnel
Force NAT Traversal	no
IKE Protocol	IKEv1
IKE Mode	main
IKE Algorithm	auto
IKE Encryption	3DES
IKE Hash	MD5
IKE DH Group	2
IKE Reauthentication	yes
XAUTH Enabled	no
XAUTH Mode	client
XAUTH Username	<input type="text"/>
XAUTH Password	<input type="password"/>
ESP Algorithm	auto
ESP Encryption	DES
ESP Hash	MD5
PFS	disabled
PFS DH Group	2
Key Lifetime	3600 sec
IKE Lifetime	3600 sec
Rekey Margin	540 sec
Rekey Fuzz	100 %
DPD Delay *	<input type="text"/> sec
DPD Timeout *	<input type="text"/> sec
Authenticate Mode	pre-shared key
Pre-shared Key	<input type="password"/>
Remote Pre-shared Key *	<input type="text"/>
CA Certificate *	<input type="text"/> Choose File No file chosen
Remote Certificate / PubKey *	<input type="text"/> Choose File No file chosen
Local Certificate / PubKey	<input type="text"/> Choose File No file chosen
Local Private Key	<input type="text"/> Choose File No file chosen
Local Passphrase *	<input type="text"/>
Revocation Check	if possible
User's Up Script	<pre>#!/bin/sh # # This script will be executed...</pre>
User's Down Script	<pre>#!/bin/sh # # This script will be executed...</pre>
Debug **	control
* can be blank ** affects all tunnels	
Apply	

Figure 57: IPsec Tunnels Configuration Page

Item	Description
Description	Name or description of the tunnel.
Type	<ul style="list-style-type: none"> • 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.
Host IP Mode	<ul style="list-style-type: none"> • IPv4 – The router communicates via IPv4 with the opposite side of the tunnel. • IPv6 – The router communicates via IPv6 with the opposite side of the tunnel.
1st Remote IP Address	First IPv4, IPv6 address or domain name of the remote side of the tunnel, based on selected <i>Host IP Mode</i> above.
2nd Remote IP Address	Second IPv4, IPv6 address or domain name of the remote side of the tunnel, based on selected <i>Host IP Mode</i> above.
Tunnel IP Mode	<ul style="list-style-type: none"> • IPv4 – The IPv4 communication runs inside the tunnel. • IPv6 – The IPv6 communication runs inside the tunnel.
Remote ID	Identifier (ID) of remote side of the tunnel. It consists of two parts: a <i>hostname</i> and a <i>domain-name</i> .
Local ID	Identifier (ID) of local side of the tunnel. It consists of two parts: a <i>hostname</i> and a <i>domain-name</i> .
Install Routers	For route-based type only. Choose yes to use traffic selectors as route(s).
First Remote Subnet	IPv4 or IPv6 address of a network behind remote side of the tunnel, based on <i>Tunnel IP Mode</i> above.
First Remote Subnet Mask/Prefix	IPv4 subnet mask of a network behind remote side of the tunnel, or IPv6 prefix (single number 0 to 128).
Second Remote Subnet	IPv4 or IPv6 address of the second network behind remote side of the tunnel, based on <i>Tunnel IP Mode</i> above. For <i>IKE Protocol</i> = IKEv2 only.
Second Remote Subnet Mask/Prefix	IPv4 subnet mask of the second network behind remote side of the tunnel, or IPv6 prefix (single number 0 to 128). For <i>IKE Protocol</i> = IKEv2 only.
Remote Protocol/Port	Specifies Protocol/Port of remote side of the tunnel. The general form is <i>protocol/port</i> , for example 17/1701 for UDP (protocol 17) and port 1701. It is also possible to enter only the number of protocol, however, the above mentioned format is preferred.
First Local Subnet	IPv4 or IPv6 address of a local network, based on <i>Tunnel IP Mode</i> above.
First Local Subnet Mask/Prefix	IPv4 subnet mask of a local network, or IPv6 prefix (single number 0 to 128).
Second Local Subnet	IPv4 or IPv6 address of the second local network, based on <i>Tunnel IP Mode</i> above. For <i>IKE Protocol</i> = IKEv2 only.
Second Local Subnet Mask/Prefix	IPv4 subnet mask of the second local network, or IPv6 prefix (single number 0 to 128). For <i>IKE Protocol</i> = IKEv2 only.

Continued on next page

Continued from previous page

Item	Description
Local Protocol/Port	Specifies Protocol/Port of a local network. The general form is <i>protocol/port</i> , for example 17/1701 for UDP (protocol 17) and port 1701. It is also possible to enter only the number of protocol, however, the above mentioned format is preferred.
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 <i>route-based</i> type must be chosen. For more information, see strongswan.conf page.
Encapsulation Mode	Specifies the IPsec mode, according to the method of encapsulation. <ul style="list-style-type: none"> • 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 (<i>main</i> or <i>aggressive</i>). If you select the aggressive mode, then the router establishes the IPsec tunnel faster, but the encryption is permanently set to 3DES-MD5. We recommend that you not use the aggressive mode due to lower security!
IKE Algorithm	Specifies the means by which the router selects the algorithm: <ul style="list-style-type: none"> • auto – The encryption and hash algorithm are selected automatically. • manual – The encryption and hash algorithm are defined by the user.
IKE Encryption	Encryption algorithm – 3DES , AES128 , AES192 , AES256 , AES128GCM128 , AES192GCM128 , AES256GCM128 .
IKE Hash	Hash algorithm – MD5 , SHA1 , SHA256 , 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.
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.

Continued on next page

Continued from previous page

Item	Description
ESP Algorithm	Specifies the means by which the router selects the algorithm: <ul style="list-style-type: none"> • auto – The encryption and hash algorithm are selected automatically. • manual – The encryption and hash algorithm are defined by the user.
ESP Encryption	Encryption algorithm – 3DES, AES128, AES192, AES256, AES128GCM128, AES192GCM128, AES256GCM128.
ESP Hash	Hash algorithm – MD5, SHA1, SHA256, SHA384 or SHA512.
PFS	Enables/disables the <i>Perfect Forward Secrecy</i> function. The function ensures that derived session keys are not compromised if one of the private keys is compromised in the future.
PFS DH Group	Specifies the Diffie-Hellman group number (see <i>IKE DH Group</i>).
Key Lifetime	Lifetime key data part of tunnel. The minimum value of this parameter is 60 s. The maximum value is 86400 s.
IKE Lifetime	Lifetime key service part of tunnel. The minimum value of this parameter is 60 s. The maximum value is 86400 s.
Rekey Margin	Specifies how long before a connection expires that the router attempts to negotiate a replacement. Specify a maximum value that is less than half of IKE and Key Lifetime parameters.
Rekey Fuzz	Percentage of time for the Rekey Margin extension.
DPD Delay	Time after which the IPsec tunnel functionality is tested.
DPD Timeout	The period during which device waits for a response.
Authenticate Mode	Specifies the means by which the router authenticates: <ul style="list-style-type: none"> • Pre-shared key – Sets the shared key for both sides of the tunnel. • X.509 Certificate – Allows X.509 authentication in 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.
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.

Continued on next page

Continued from previous page

Item	Description
Revocation Check	Certificate revocation policy: <ul style="list-style-type: none"> • 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 <i>strongSwan</i> web page for more details.

Table 43: IPsec Tunnel Configuration Items Description

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.

¹Parameters 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.

3.14.4 Basic IPv4 IPsec Tunnel Configuration

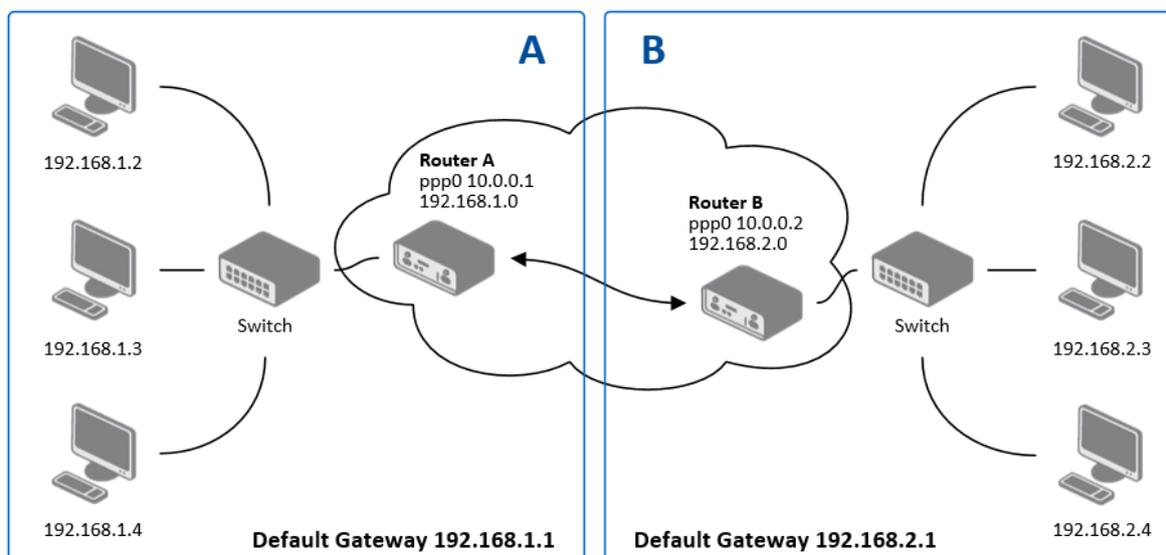


Figure 58: Topology of IPsec Configuration Example

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

Configuration	A	B
Host IP Mode	IPv4	IPv4
1st Remote IP Address	10.0.0.2	10.0.0.1
Tunnel IP Mode	IPv4	IPv4
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 44: Simple IPv4 IPsec Tunnel Configuration

3.14.5 TPM-based Authentication

This chapter describes the process of creating the TPM keys usable for an IPsec tunnel configuration. This feature uses the TPM 2.0 (Trusted Platform Module) chip mounted directly onto the router's mainboard. For details about the TPM commands, see the `tpm2` command description [1] or go to <https://github.com/tpm2-software/tpm2-tools/tree/5.1.X/man>.

To generate the key, connect to the "TPM-equipped" router's console and execute the following commands:

```
$ tpm2 createek -c ek.ctx -G rsa
```

```
$ tpm2 createak -C ek.ctx -G rsa -g sha256 -s rsassa -c ak_rsa.ctx -u ak_rsa.pub -loaded-key:
```

```
name: 000b0a688495f33b96ecfe242807e5b183a41bc5f24f7a4f18716866d084378a6cd2
```

```
qualified name: 000bfffac43e487a8658606636a9640e02151ec0603bec90073dd2bc2e8b82f0
```

```
$ tpm2 evictcontrol -c ak_rsa.ctx
persistent-handle: 0x81010001
action: persisted
```

After this, store the `ak_rsa.pub`, which is the public key in a standard PEM format, and remember the `persistent-handle` such as `0x81010001` that got printed. This is the location (handle) of the private key. The temporary `*.ctx` files can be removed at this point.

To list all existing handles, execute the following command:

```
$ tpm2 getcap handles-persistent
- 0x81010001
```

To configure the key for an IPsec tunnel in the GUI:

- Set *Authentication Mode* to **X509 Certificate** on both routers.
- Place content of `ak_rsa.pub` as local pubkey (item *Local Certificate / PubKey*) to the router and as a remote pubkey (item *Remote Certificate / PubKey*) to the peer router.
- Put the `persistent-handle` number printed by `tpm2 evictcontrol` command above (such as `0x81010001`) as a private key (item *Local Private Key*) to the router.

To remove a persisted key, execute the following command:

```
$ tpm2 evictcontrol -c 0x81010001
persistent-handle: 0x81010001
action: evicted
```

3.15 WireGuard

WireGuard is a communication protocol and free open-source software that implements encrypted virtual private networks (VPNs), and was designed with the goals of ease of use, high speed performance, and low attack surface. It aims for better performance and more power than IPsec and OpenVPN, two common tunneling protocols. The WireGuard protocol passes traffic over UDP. Advantech routers allows you to create **up to four WireGuard tunnels**.

To open the WireGuard tunnel configuration page, click *WireGuard* in the *Configuration* section of the main menu. The menu item will expand and you will see separate configuration pages: *1st Tunnel*, *2nd Tunnel*, *3rd Tunnel* and *4th Tunnel*.

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



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



Detailed information and more examples of WireGuard tunnel configuration and authentication can be found in the application note *WireGuard Tunnel* [8].

The configuration GUI for WireGuard is shown in Figure 59 and the description of all items, which can be configured for an WireGuard tunnel, are described in Table 45.

Item	Description
Description	Name or description of the tunnel.
Host IP Mode	<ul style="list-style-type: none"> ● IPv4 – The router communicates via IPv4 with the opposite side of the tunnel. ● IPv6 – The router communicates via IPv6 with the opposite side of the tunnel.
Remote IP Address	IPv4, IPv6 address or domain name of the remote side of the tunnel to connect to. The address must match with the selected <i>Host IP Mode</i> above.
Remote Port	Port of the remote side of the tunnel.
Local Port	Port of the local side of the tunnel (default port is 51820).
NAT/Firewall Traversal	If set up to <i>yes</i> , keepalive communication (every 25 seconds) is running to preserve the tunnel established. It is useful when a client is running behind the NAT.
Interface IPv4 Address	Local IPv4 tunnel interface address.
Interface IPv4 Prefix Length	Local IPv4 tunnel interface prefix.
Interface IPv6 Address	Local IPv6 tunnel interface address.
Interface IPv6 Prefix Length	Local IPv6 tunnel interface prefix.
Install Routes	<ul style="list-style-type: none"> ● no – Do not install routes. Use when a dynamic routing protocol is configured. ● yes – Install routes.
Traffic Selector	<ul style="list-style-type: none"> ● all traffic – Proceed all the packets to the WireGuard tunnel. ● subnets – Route based on the subnets listed below.

Continued on next page

Continued from previous page

Item	Description
Remote Subnets	If the <i>Traffic Selector</i> is set to <i>subnets</i> , then other subnets (routes) can be routed through the wire tunnel.
Pre-shared Key	The optional key for additional encryption layer and security strengthening. You can use the <i>Generate</i> button to generate a random key.
Local Private Key	The private key of the local side. You can use the <i>Generate</i> button to generate a random key.
Local Public Key	The public key of the local tunnel side.
Remote Public Key	The public key of the remote tunnel side.

Table 45: WireGuard Tunnel Configuration Items Description

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

1st WireGuard Tunnel Configuration

Create 1st WireGuard tunnel

Description *

Host IP Mode IPv4 ▾

Remote IP Address *

Remote Port *

Local Port 51820

NAT/Firewall Traversal no ▾

Interface IPv4 Address *

Interface IPv4 Prefix Length *

Interface IPv6 Address *

Interface IPv6 Prefix Length *

Install Routes yes ▾

Traffic Selector subnets ▾

Remote Subnets *

Pre-shared Key * Generate

Local Private Key Generate

Local Public Key *

Remote Public Key

* can be blank

Apply

Figure 59: WireGuard Tunnels Configuration Page

3.15.1 WireGuard IPv4 Tunnel Configuration Example

There is an example of WireGuard IPv4 tunnel configuration between *Router A* and *Router B*.

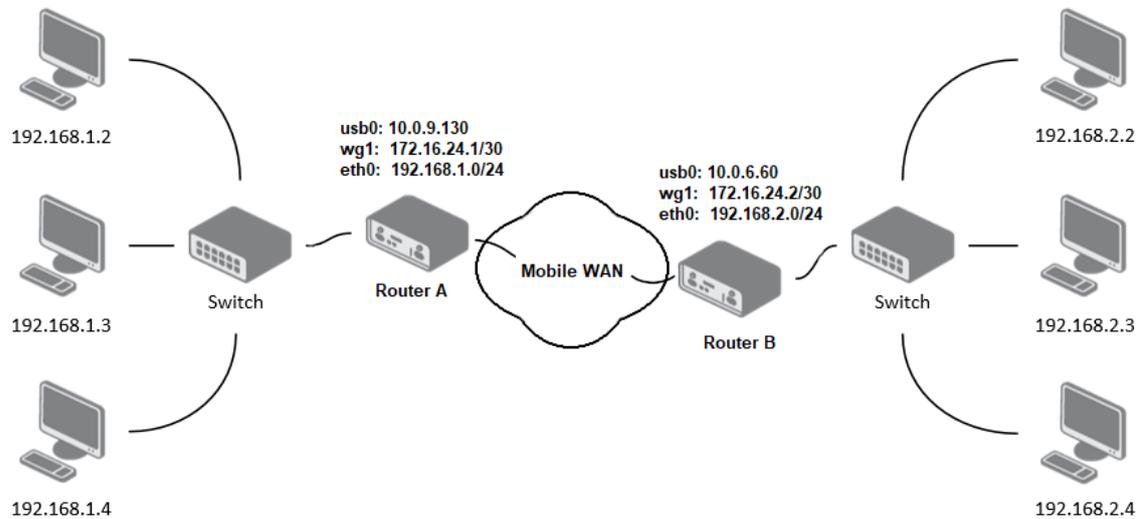


Figure 60: Topology of WireGuard Configuration Example

Router B is configured to listen, and *Router A* is the side initiating the tunnel connection. Configuration of *Router A* and *Router B* from the topology above is as follows:

Configuration	Router A	Router B
Host IP Mode	IPv4	IPv4
Remote IP Address	10.0.6.60	–
Remote Port	51820	–
Local Port	51820	51820
NAT/Firewall Traversal	yes	no
Interface IPv4 Address	172.16.24.1	172.16.24.2
Interface IPv4 Prefix Length	30	30
Install Routes	yes	yes
Traffic Selector	subnets	subnets
Remote Subnets	192.168.2.0/24	192.168.1.0/24
Local Private Key	<i>a local private key</i>	<i>a local private key</i>
Local Public Key	<i>a local public key</i>	<i>a local public key</i>
Remote Public Key	<i>a public key of the opposite side</i>	<i>a public key of the opposite side</i>

Table 46: WireGuard IPv4 Tunnel Configuration Example

In the figure below is the WireGuard status page of *Router A*. If the tunnel connection is established successfully, the *Latest handshake* time is shown here. This value is the time left from the latest successful communication with the opposite tunnel side. This item will not be shown here until there is a tunnel communication (data sent by the *Router A* or the keepalive data sent when *NAT/Firewall Traversal* is set to *yes*).

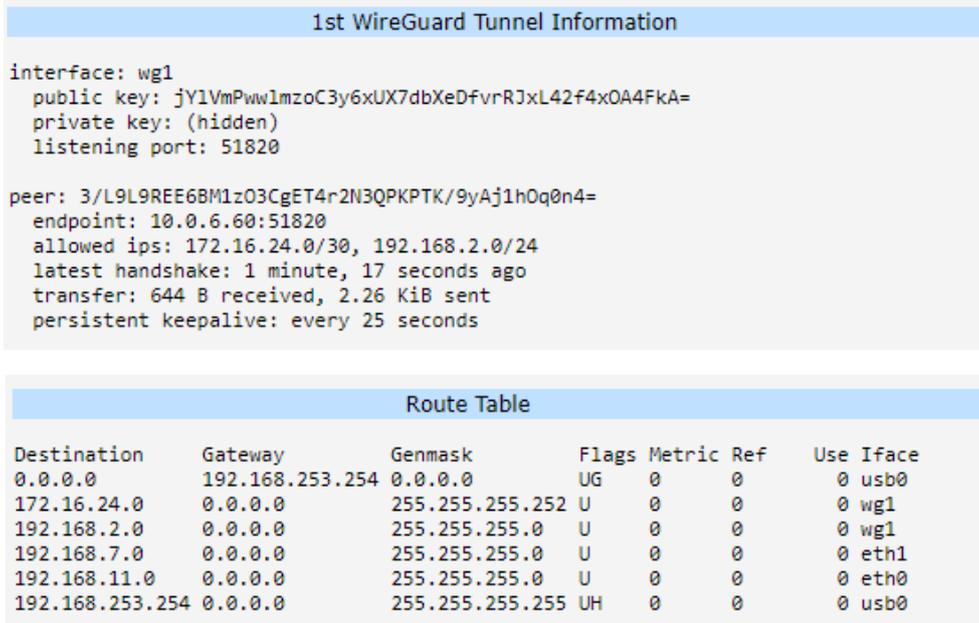


Figure 61: Router A – WireGuard Status Page and Route Table

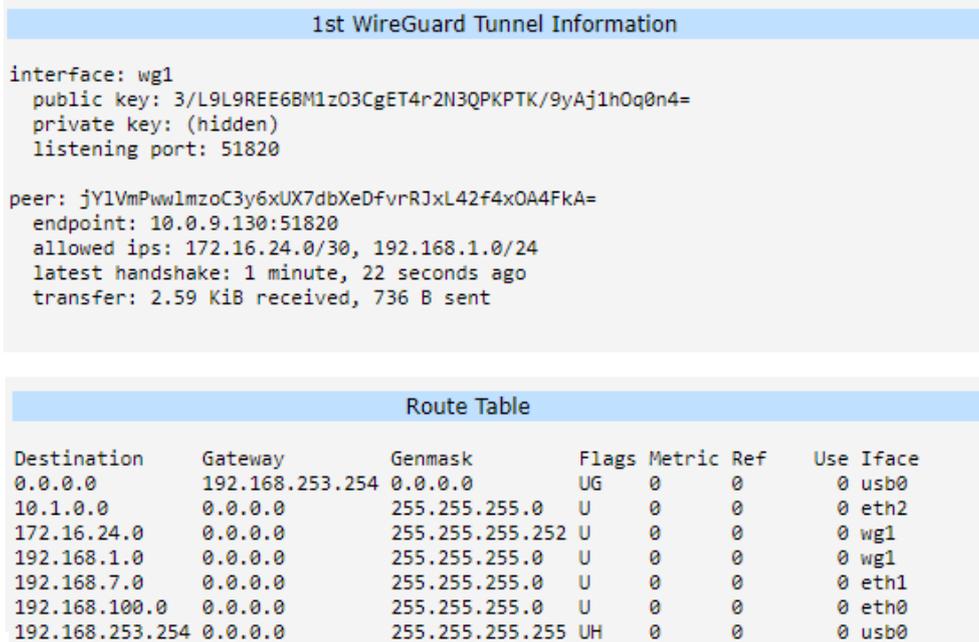


Figure 62: Router B – WireGuard Status Page and Route Table

3.16 GRE Tunnels



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

To open the *GRE Tunnel Configuration* page, click *GRE* in the *Configuration* section of the main menu. The menu item will expand and you will see 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: <ul style="list-style-type: none"> • disabled – Sending multicast into the tunnel is inactive. • enabled – Sending multicast into the tunnel is active.
Pre-shared Key	Specifies an optional value for the 32 bit shared key in numeric format, with this key the router sends the filtered data through the tunnel. Specify the same key on both routers, otherwise the router drops received packets.

Table 47: GRE Tunnel Configuration Items Description



The GRE tunnel cannot pass through the NAT.

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

1st GRE Tunnel Configuration

Create 1st GRE tunnel

Description *

Remote IP Address *

Local IP Address *

Remote Subnet *

Remote Subnet Mask *

Local Interface IP Address *

Remote Interface IP Address *

Multicasts disabled ▼

Pre-shared Key * 👁

* can be blank

Figure 63: GRE Tunnel Configuration Page

3.16.1 Example of the GRE Tunnel Configuration

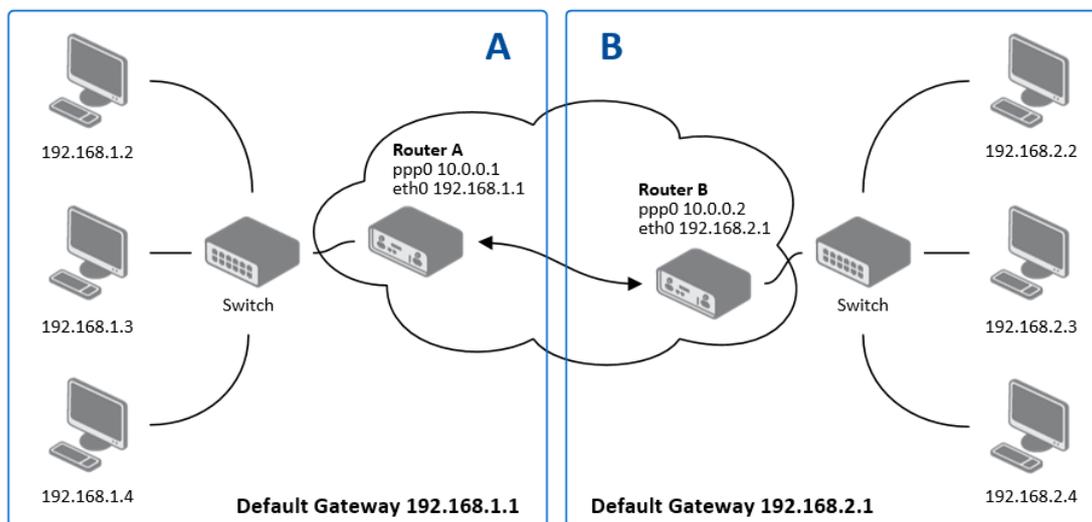


Figure 64: Topology of GRE Tunnel Configuration Example

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 48: GRE Tunnel Configuration Example



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

3.17 L2TP Tunnel



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

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

L2TP Tunnel Configuration

Create L2TP tunnel

Mode ▼

Server IP Address

Client Start IP Address

Client End IP Address

Local IP Address *

Remote IP Address *

Remote Subnet *

Remote Subnet Mask *

MRU bytes

MTU bytes

Username

Password 👁

** can be blank*

Figure 65: L2TP Tunnel Configuration Page

Item	Description
Mode	Specifies the L2TP tunnel mode on the router side: <ul style="list-style-type: none"> L2TP server – Specify an IP address range offered by the server. L2TP client – Specify the IP address of the server.
Server IP Address	IP address of the server.
Client Start IP Address	IP address to start with in the address range. The range is offered by the server to the clients.
Client End IP Address	The last IP address in the address range. The range is offered by the server to the clients.
Local IP Address	IP address of the local side of the tunnel.

Continued on next page

Continued from previous page

Item	Description
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 49: L2TP Tunnel Configuration Items Description

3.17.1 Example of the L2TP Tunnel Configuration

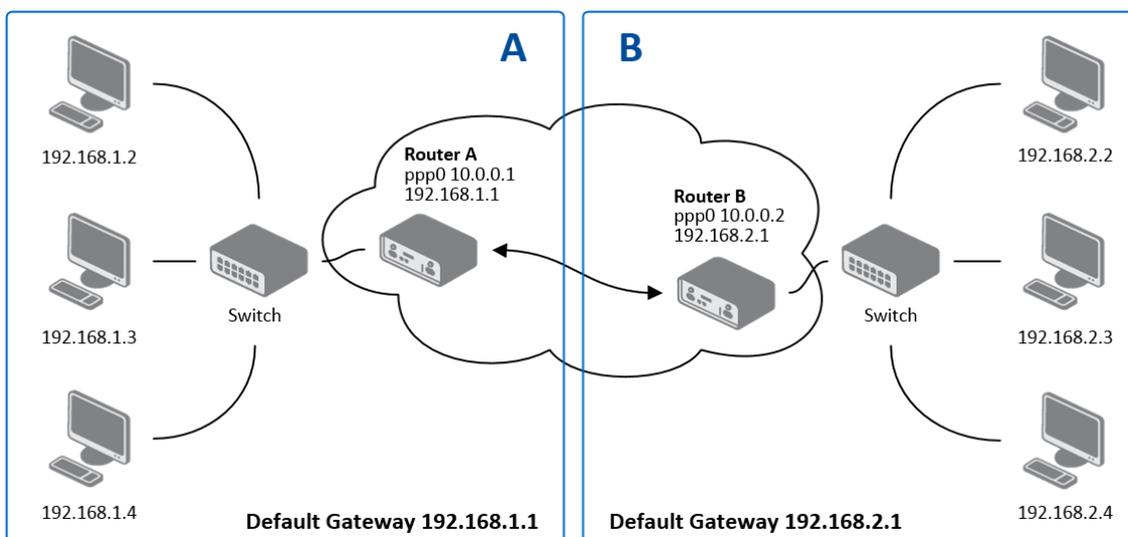


Figure 66: Topology of L2TP Tunnel Configuration Example

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 50: L2TP Tunnel Configuration Example

3.18 PPTP



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

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

PPTP Tunnel Configuration

Create PPTP tunnel

Mode ▼ PPTP client

Server IP Address

Local IP Address

Remote IP Address

Remote Subnet *

Remote Subnet Mask *

MRU 1460 bytes

MTU 1460 bytes

Username

Password 👁

** can be blank*

Apply

Figure 67: PPTP Tunnel Configuration Page

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

Continued on next page

Continued from previous page

Item	Description
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 51: PPTP Tunnel Configuration Items Description

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.

3.18.1 Example of the PPTP Tunnel Configuration

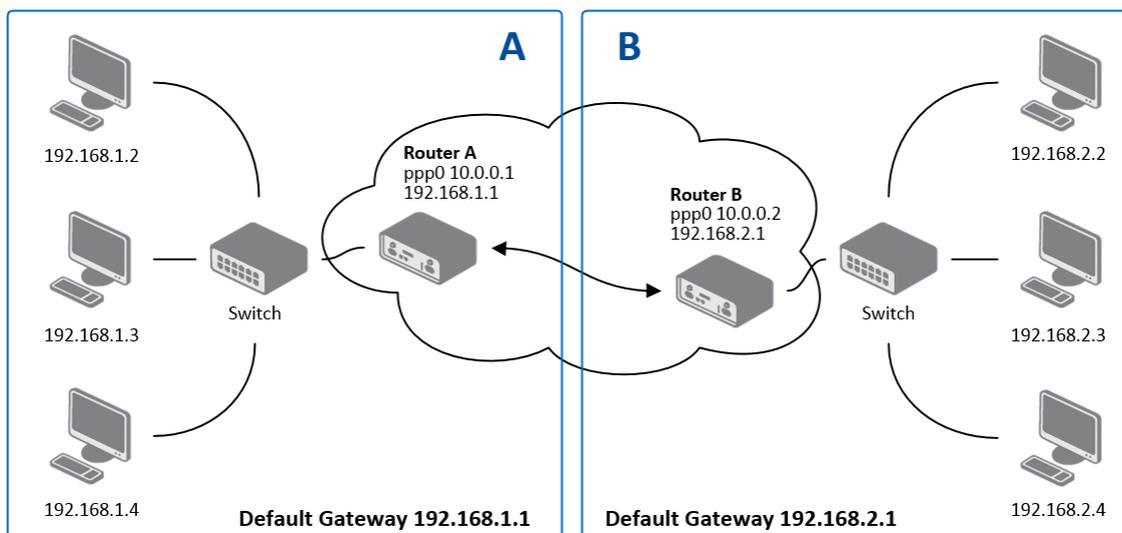


Figure 68: Topology of PPTP Tunnel Configuration Example

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 52: PPTP Tunnel Configuration Example

3.19 Services

3.19.1 Authentication

User authentication options can be configured on the *Configuration* → *Authentication* page. Figure 69 shows the configuration for *local user database* mode. Table 53 describes configuration items for *local user database* mode that are common to all other modes as well.

Authentication Configuration	
Two-Factor Authentication	disabled
Mode	local user database
Lock Account After	3 fail(s)
Count Fails For	3600 sec
Unlock After	60 sec
Force Password Complexity	good
Expire Password After *	days
Delay After Fail *	1 sec
Debug	disabled
* can be blank	
Apply	

Figure 69: Common Configuration Items

Item	Description
Two-Factor Authentication	To enable the two-factor authentication service, choose the service type you want to use from <i>Google Authenticator</i> or <i>OATH Toolkit</i> . For more details refer to Chapter 5.2.1 <i>Two-Factor Authentication</i> .
Mode	<ul style="list-style-type: none"> • 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 if 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 if the RADIUS server is not accessible! • TACACS+ with fallback – Authenticate against the TACACS+ server first, and then against the local database if 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 if the TACACS+ server is not accessible!

Continued on the next page

Continued from previous page

Item	Description
Lock Account After	Number of failed login attempts after which the account will be locked.
Count Fails For	The time window for which unsuccessful login attempts will be counted.
Unlock After	The time after which logging will be unlocked if it was previously locked.
Force Password Complexity	Specify the level of password complexity: <ul style="list-style-type: none"> • very weak – Not secure and not recommended. Requires 6 characters. Time to crack: Seconds to minutes. • weak – Not secure and not recommended. Requires 8 characters from two sets (numbers, letters) [NIST SP 800-63B compliant]. Time to crack: Hours to days. • good – Reasonably secure. Requires 12 characters from three sets (uppercase letters, lowercase letters, and numbers), with a maximum of 3 same characters in sequence [FirstNet compliant]. Time to crack: Months to years. • strong – For the best security level. Requires 16 characters from four sets (uppercase and lowercase letters, digits, and special characters). Time to crack: Centuries.
Expire Password After	Number of days after which the password will expire and the user will be prompted to change it; see Chapter 5.2.3.
Delay After Fail	The time after which the login screen will appear again in case of a previous unsuccessful attempt.
Debug	Enable or disable debugging in the Syslog.

Table 53: Enter Caption

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 70. Table 54 describes all the configuration options for the RADIUS PAM modes.

Authentication Configuration

Two-Factor Authentication disabled ▼

Mode RADIUS only ▼

RADIUS Server(s)

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

Take Over Server Users disabled ▼

Default User Role admin ▼

Delay After Fail * 1 sec

Debug disabled ▼

* can be blank

Figure 70: 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 (<i>Admin</i> or <i>User</i>). This role corresponds with router’s user roles, see Chapter 5.1. Selected role will be used for a user in case the option <i>Take Over Server Users</i> is enabled and if the user’s <i>Service-Type</i> set on the RADIUS server is missing or is not set up to <i>NAS-Prompt-User</i> or <i>Administrative-User</i> . When <i>Service-Type</i> is set to <i>NAS-Prompt-User</i> , the <i>User</i> role will be used. When <i>Service-Type</i> is set to <i>Administrative-User</i> , the <i>Admin</i> role is used.

Table 54: 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 71. Table 55 describes all the configuration options for the TACACS PAM modes.

Authentication Configuration

Two-Factor Authentication disabled ▼

Mode TACACS+ only ▼

TACACS+ Server(s)

Authentication Type ASCII ▼

Timeout * [] sec

	Server	Port *	Secret
<input type="checkbox"/>	[]	[]	[]
<input type="checkbox"/>	[]	[]	[]

Take Over Server Users disabled ▼

Default User Role admin ▼

Delay After Fail * 1 [] sec

Debug disabled ▼

* can be blank

Figure 71: Configuration of TACACS+

Item	Description
Authentication Type	Choose ASCII, PAP or CHAP as authentication type. To configure the two-factor authentication for a user, see Chapter 5.2.1 Two-Factor Authentication .
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 (<i>Admin</i> or <i>User</i>). This role corresponds with router’s user roles, see Chapter 5.1. Selected role will be used for a new user when <i>Take Over Server Users</i> is used.

Table 55: Configuration of TACACS+

3.19.2 DynDNS

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

Item	Description
Hostname	The third order domain registered on the www.dyndns.org server.
Username	Username for logging into the DynDNS server.
Password	Password for logging into the DynDNS server. Enter valid characters only, see chap. 1.3.2!
IP Mode	Specifies the version of IP protocol: <ul style="list-style-type: none"> • IPv4 – IPv4 protocol is used only (default). • IPv6 – IPv6 protocol is used only. • IPv4/IPv6 – IPv4 and IPv6 dual stack is enabled.
Server	Specifies a DynDNS service other than the www.dyndns.org . Possible other services: www.spdns.de , www.dnsdynamic.org , www.noip.com Enter the update server service information in this field. If you leave this field blank, the default server members.dyndns.org will be used.

Table 56: DynDNS Configuration Items Description

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

DynDNS Configuration

Enable DynDNS client

Hostname

Username

Password

IP Mode ▼

Server *

* can be blank

Figure 72: 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 3.12.

3.19.3 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 57: FTP Configuration Items Description

FTP Configuration

Enable FTP service

Maximum Sessions

Session Timeout sec

Figure 73: Configuration of FTP server

3.19.4 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 58: HTTP Configuration Items Description

HTTP Configuration

Enable HTTP service

Enable HTTPS service

Minimum TLS Version TLS 1.2 v

Session Timeout 6000 sec

Login Banner

Keep the current certificate

Generate a new certificate

Upload a new certificate

Certificate Procházet... Soubor nevybrán.

Private Key Procházet... Soubor nevybrán.

Apply

Figure 74: HTTP Configuration Page

3.19.5 NTP

The *NTP* (Network Time Protocol) configuration form allows you to configure the NTP client or NTP server. To open the *NTP* configuration page, click *NTP* in the *Configuration* section of the main menu.

! Using the router as an NTP server without synchronization to another reliable NTP server is not a good idea, as there is a risk that incorrect time will be synchronized with other devices on the network.

i When running the NTP service for the first time, there is an approximate 15-minute delay before it begins working in continuous mode due to Hardware Clock adjustment. The message `TIME_ERROR: Clock Unsynchronized` in the syslog is normal during NTP startup. The time will be synchronized shortly thereafter.

Item	Description
Enable local NTP server	Enables a local NTP server running on the device.
Synchronize clock with remote NTP server	Enables the NTP client for clock synchronization with a remote NTP server.
Primary NTP Server	IP address or domain name of the primary NTP server.
Secondary NTP Server	IP address or domain name of the secondary NTP server.
Tertiary NTP Server	IP address or domain name of the tertiary NTP server.
Maximal Pooling Interval	Select the maximum pooling interval for synchronization.
Enable fast initial synchronization	Allows for quick and immediate time synchronization, even in cases of significant differences between the system time and the time on the NTP server. This function is useful when the time difference between the system and the NTP server is large and needs to be corrected quickly.
Timezone	Specifies the time zone where the router is installed.
Daylight Saving Time	Activates or deactivates the DST shift.

Table 59: NTP Configuration Items Description

NTP Configuration

Enable local NTP server

Synchronize clock with remote NTP server

Primary NTP Server

Secondary NTP Server

Tertiary NTP Server

Maximal Polling Interval

Enable fast initial synchronization

Timezone

Daylight Saving Time

Figure 75: NTP Configuration Page

3.19.6 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. Sending SNMP traps to IPv6 address is supported.

Item	Description
Name	Designation of the router.
Location	Location of where you installed the router.
Contact	Person who manages the router together with information how to contact this person.
Custom	You can use this input field to enter specific information tailored to your requirements.

Table 60: SNMP Agent Configuration

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

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

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

Item	Description
Username	User name
Authentication	Encryption algorithm on the Authentication Protocol that is used to verify the identity of the users.
Authentication Password	Password used to generate the key used for authentication. Enter valid characters only, see chap. 1.3.2!
Privacy	Encryption algorithm on the Privacy Protocol that is used to ensure confidentiality of data.
Privacy Password	Password for encryption on the Privacy Protocol. Enter valid characters only, see chap. 1.3.2!

Table 61: SNMPv3 Configuration

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



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

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

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

Table 62: 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.

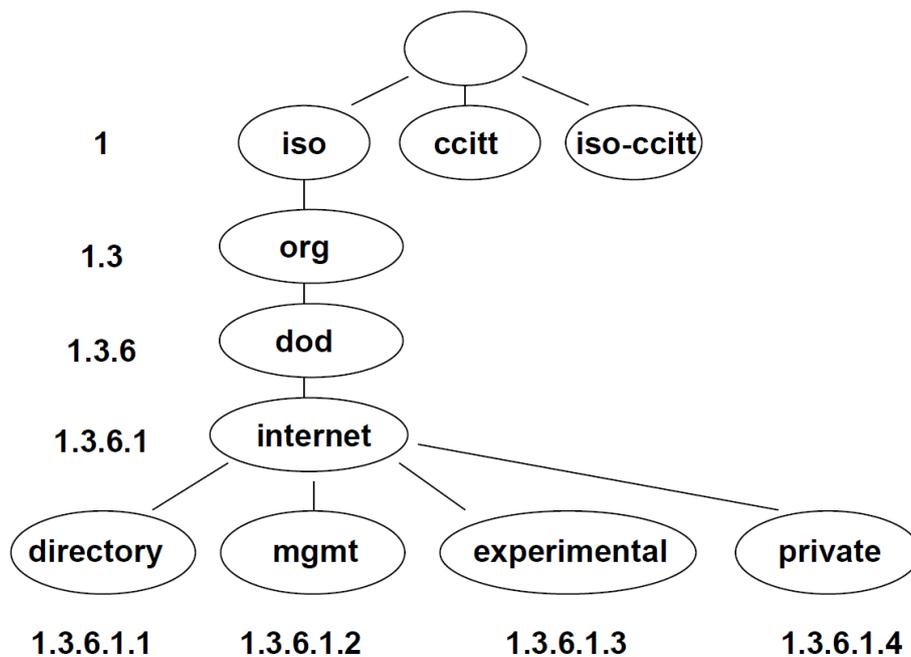


Figure 76: OID Basic Structure

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 internal temperature (OID 1.3.6.1.4.1.30140.3.3) or about the power voltage (OID 1.3.6.1.4.1.30140.3.4). For binary inputs and output, the following range of OID is used:



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

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

Table 63: Object identifier for binary inputs and output

SNMP Configuration

Enable SNMP agent

Name *

Location *

Contact *

Custom *

(Configuration via SNMP is not possible.)

Enable SNMPv1/v2 access

	Read	Write
Community	<input type="text" value="public"/>	<input type="text" value="private"/>

Enable SNMPv3 access

	Read	Write
Username	<input type="text"/>	<input type="text"/>
Authentication	<input style="border: none; border-bottom: 1px solid #ccc;" type="text" value="MD5"/> ▼	<input style="border: none; border-bottom: 1px solid #ccc;" type="text" value="MD5"/> ▼
Authentication Password	<input style="border: none; border-bottom: 1px solid #ccc;" type="text"/> <input type="checkbox"/>	<input style="border: none; border-bottom: 1px solid #ccc;" type="text"/> <input type="checkbox"/>
Privacy	<input style="border: none; border-bottom: 1px solid #ccc;" type="text" value="DES"/> ▼	<input style="border: none; border-bottom: 1px solid #ccc;" type="text" value="DES"/> ▼
Privacy Password	<input style="border: none; border-bottom: 1px solid #ccc;" type="text"/> <input type="checkbox"/>	<input style="border: none; border-bottom: 1px solid #ccc;" type="text"/> <input type="checkbox"/>

Enable I/O extension

Enable XC-CNT extension

Enable M-BUS extension

Baudrate ▼

Parity ▼

Stop Bits ▼

Enable reporting to supervisory system

IP Address

Period min

* can be blank

Figure 77: SNMP Configuration Example

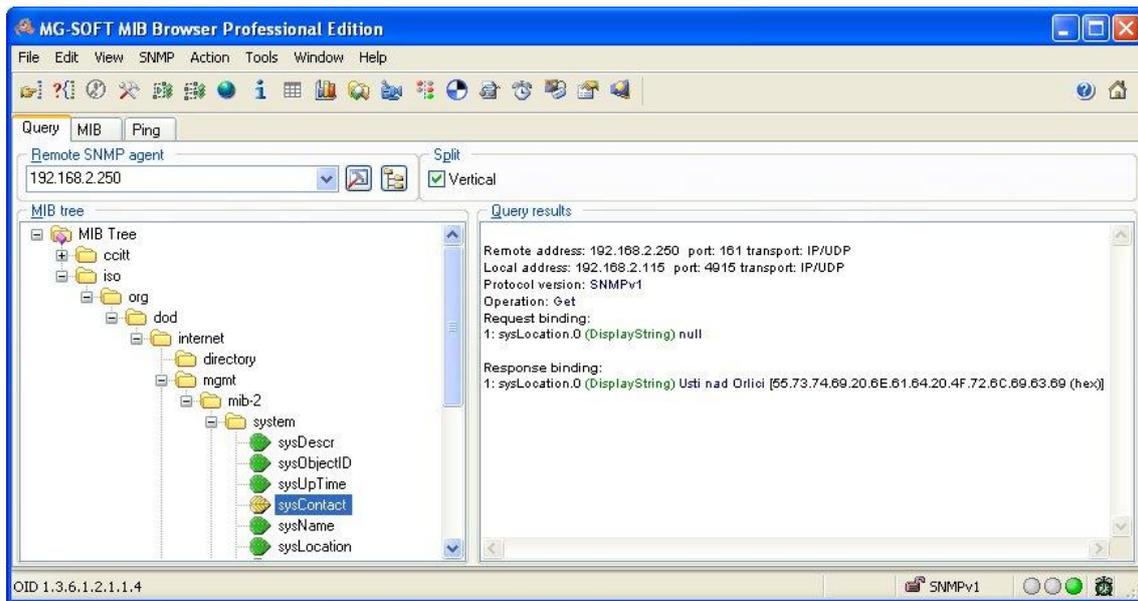


Figure 78: MIB Browser Example

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

3.19.7 SMTP

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

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. The secure method must be supported by the SMTP server.
Username	Name for the email account.
Password	Password for the email account. Enter valid characters only.
Own Email Address	Address of the sender.

Table 64: SMTP Client Configuration



The mobile service provider may block other SMTP servers, so you might only be able to use the SMTP server of the service provider.

SMTP Configuration

SMTP Server Address	<input style="width: 90%;" type="text" value="smtp.domain.com"/>
SMTP Port	<input style="width: 90%;" type="text" value="465"/>
Secure Method	<input style="border-bottom: 1px solid #ccc;" type="text" value="SSL/TLS"/>
Username	<input style="width: 90%;" type="text" value="username"/>
Password	<input style="border-bottom: 1px solid #ccc;" type="password" value="....."/>
Own Email Address	<input style="width: 90%;" type="text" value="name@domain.com"/>
<input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="Apply"/>	

Figure 79: SMTP Client Configuration Example

You can send emails from the startup script. The *Startup Script* dialog is located in *Scripts* in the *Configuration* section of the main menu.

The router also allows you to send emails using an SSH connection. Use the `email` command, see *Command Line Interface* [1] Application Note for details.

3.19.8 SMS

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

Item	Description
Send SMS on power up	Activates/deactivates the sending of an SMS message automatically on power up.
Send SMS on connect to mobile network	Activates/deactivates the sending of an SMS message automatically when the router is connected to a mobile network.
Send SMS on disconnect to mobile network	Activates/deactivates the sending of an SMS message automatically when the router is disconnection from a mobile network.
Send SMS when datalimit exceeded	Activates/deactivates the sending of an SMS message automatically when the data limit exceeded.
Send SMS when binary input on I/O port (BIN0) is active	Automatic sending SMS message after binary input on I/O port (BIN0) is active. Text of message is intended parameter BIN0.
Add timestamp to SMS	Activates/deactivates the adding a time stamp to the SMS messages. This time stamp has a fixed format YYYY-MM-DD hh:mm:ss.
Phone Number 1	Specifies the phone number to which the router sends the generated SMS.
Phone Number 2	Specifies the phone number to which the router sends the generated SMS.
Phone Number 3	Specifies the phone number to which the router sends the generated SMS.
Unit ID	The name of the router. The router sends the name in the SMS.
BIN0 – SMS	Text of the SMS message when the first binary input is activated.
BIN1 – SMS	Text of the SMS message when the second binary input is activated.

Table 65: 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 66: 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 format:

SMS	Description
go online sim 1	Switch the mobile WAN to the SIM1.
go online sim 2	Switch the mobile WAN to the SIM2.
go online	Switch the router to the online mode.
go offline	Switch the router to the off line mode.
set out0=0	Set the binary output to 0.
set out0=1	Set the binary output to 1.
set profile std	Set the standard profile. This change is permanent.
set profile alt1	Set the alternative profile 1. This change is permanent.
set profile alt2	Set the alternative profile 2. This change is permanent.
set profile alt3	Set the alternative profile 3. This change is permanent.
reboot	Reboot the router.
get ip	Respond with the IP address of the SIM card.

Table 67: 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 *Command Line Interface 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 68: 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 69: Send SMS on the serial Port 2

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

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

Table 70: Sending/receiving of SMS on TCP port specified

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

Continued on next page

Continued from previous page

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



A detailed description and examples of these AT commands can be found in the application note *AT Commands (AT-SMS)* [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 *Command Line Interface Application Note* [1] for more details and example.
- From Web interface of the router, in *Administration* section, *Send SMS* item, see Chapter 5.8.
- Using `gsmsms` command e.g. in terminal when connected to the router via SSH. See *Command Line Interface Application Note* [1].

Examples of SMS Configuration

Example 1 Sending SMS Configuration

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

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 format:

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 format:

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

SMS Configuration

- Send SMS on power up
- Send SMS on connect to mobile network
- Send SMS on disconnect from mobile network
- Send SMS when datalimit is exceeded
- Send SMS when binary input on I/O port (BIN0) is active
- Send SMS when binary input on expansion port 1 (BIN1-BIN4) is active
- Add timestamp to SMS

Phone Number 1	<input type="text" value="723123456"/>
Phone Number 2	<input type="text" value="756858635"/>
Phone Number 3	<input type="text" value="603854758"/>
Unit ID *	<input type="text" value="Router"/>
BIN0 - SMS *	<input type="text" value="BIN0"/>

- Enable remote control via SMS

Phone Number 1	<input type="text"/>
Phone Number 2	<input type="text"/>
Phone Number 3	<input type="text"/>

- Enable AT-SMS protocol on expansion port 1

Baudrate	<input type="text" value="9600"/>
----------	-----------------------------------

- Enable AT-SMS protocol on expansion port 2

Baudrate	<input type="text" value="9600"/>
----------	-----------------------------------

- Enable AT-SMS protocol over TCP

TCP Port	<input type="text"/>
----------	----------------------

* can be blank

Figure 80: SMS Configuration for Example 1

Example 2 Sending SMS via Serial Interface on the Port 1

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

Figure 81: SMS Configuration for Example 2

Example 3 Control the Router Sending SMS from any Phone Number

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

Figure 82: SMS Configuration for Example 3

Example 4 Control the Router Sending SMS from Two Phone Numbers

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

Figure 83: SMS Configuration for Example 4

3.19.9 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.
Port	Listening port.
Session Timeout	Inactivity timeout when the session is closed. The maximum allowed value may vary based on security requirements for the specific model.
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 Type	Choose the key type to be generated. The minimum allowed value may vary based on security requirements for the specific model. There are two types of keys: the RSA (Rivest-Shamir-Adleman) key and the ED25519 key. The ED25519 key is based on elliptic curve cryptography and is considered more secure than RSA.

Table 72: SSH Configuration Items Description

SSH Configuration

Enable SSH service

Port

Session Timeout sec

Login Banner

Keep the current SSH key
 Generate a new SSH key

Key Type

Figure 84: SSH Configuration Page

3.19.10 Syslog

Configuration of the system log, known as *syslog*, is accessible from this configuration page.

To view this log, navigate to the router's GUI via *Status* → *System Log*. Remember, you can enable auto-refreshing of this page by clicking the *refresh* button in the top-right corner. You can also access the syslog through the console with the `slog` command.

Figure 85: Syslog Configuration Page

Item	Description
Log Size Limit	Restriction of log size by the maximum number of rows. The default size is 1000 KiB.
Mark Message Period	This defines the time period during which the <code>-- MARK --</code> string will be printed into the syslog. It can function as a keepalive message.
Read Kernel Log	Retrieve new log messages from <code>/dev/kmsg</code> . Check this option if you want to forward kernel messages, such as information about device mounting or messages from the firewall's LOG target. After a service (re)start, all existing kernel log entries will be sent to the remote server, which may result in duplicate messages. After that, the system will wait for new messages.

Continued on the next page

Continued from previous page

Item	Description
Enable Forwarding	Enables the forwarding of messages to another host capable of processing forwarded messages.
Protocol	Choose the forwarding protocol from: <ul style="list-style-type: none"> • UDP • TCP • SSL/TLS
Remote Host	Hostname (IP address) of the remote host for real-time syslog forwarding.
Remote Port	Port for forwarding.
Device ID	A unique identification string for remote logging purposes. If left blank, the default string <i>Router</i> is used.
Authentication	Defines how to authenticate the syslog server when using the SSL/TLS protocol. Allowed values are: <ul style="list-style-type: none"> • None (encryption only) – Skips transport receiver authentication. The communication will still be encrypted. • Certificate fingerprint – Checks the fingerprint of the received certificate against the Acceptable Peers. • Certificate validity – Accepts any server with a valid certificate signed by the specified CA. • Certified peer name – Checks certificate validity and matches the certified DNS names in the <i>subjectAltName</i> extension or the entire certified Common Name against the Acceptable Peers. <p>Note that the server may (depending on its configuration) implement its own transport sender authentication, which is independent of this setting.</p>
Acceptable Peers	The accepted certificate fingerprint (SHA1) or DNS/Common Name of the remote peer. The DNS name may use wildcards, e.g., "*.example.net". Required when Authentication is set to Certificate fingerprint or Certified peer name.
CA Certificates	The entire certificate chain (sequence of CA certificates in PEM format) that can validate remote certificates. Not required when Authentication is set to None.
Local Certificate	A certificate in PEM format. The extended key usage must permit use for TLS client authentication.
Local Private Key	The local key and certificate do not need to be configured if the server does not enforce transport sender authentication.

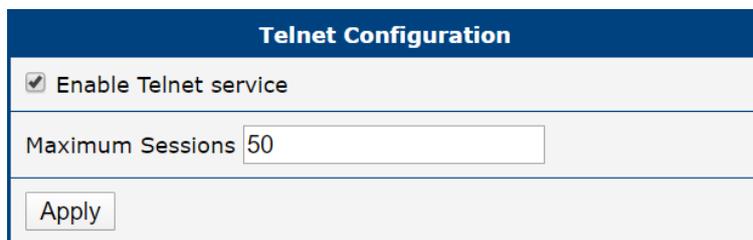
Table 73: Syslog Configuration Items Description

3.19.11 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 74: Telnet Configuration Items Description



The screenshot shows a configuration window titled "Telnet Configuration". It contains a checked checkbox labeled "Enable Telnet service". Below this is a text input field labeled "Maximum Sessions" with the value "50" entered. At the bottom of the window is an "Apply" button.

Figure 86: Telnet Configuration Page

3.20 Expansion Port 1 & 2, USB Port

Configuration of the RS232 and RS485 interfaces can be done via *Expansion Port 1* resp. *Expansion Port 2* menu items. Configuration of the USB port can be done via *USB Port* menu item.

At the top of the configuration window, the port can be activated, and the connected port's type is displayed under the *Port Type* item. Additional settings are outlined in the table below. Support for IPv6 TCP/UDP client/server configurations is available.

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

Figure 87: Expansion Port Configuration

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: <ul style="list-style-type: none"> • none – data will be sent without parity. • even – data will be sent with even parity. • odd – data will be sent with odd parity.

Continued on next page

Continued from previous page

Item	Description
Stop Bits	Number of stop bits: 1 (default), 2 .
Flow Control	Set the flow control to none or hardware .
Split Timeout	Time to rupture reports. If the gap between two characters exceeds the parameter in milliseconds, any buffered characters will be sent over the Ethernet port.
Protocol	Protocol: <ul style="list-style-type: none"> • TCP – communication using a linked protocol TCP. • UDP – communication using a unlinked protocol UDP.
Mode	Mode of connection: <ul style="list-style-type: none"> • TCP server – The router will listen for incoming TCP connection requests. • TCP client – The router will connect to a TCP server on the specified IP address and TCP port.
Server Address	When set to <i>TCP client</i> above, it is necessary to enter the <i>Server address</i> and <i>TCP port</i> . IPv4 and IPv6 addresses are allowed.
TCP Port	TCP/UDP port used for communications. The router uses the value for both the server and client modes.
Inactivity Timeout	Time period after which the TCP/UDP connection is interrupted in case of inactivity.

Table 75: Expansion Port Configuration – serial interface

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

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

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

Table 76: Expansion Port Configuration – *Check TCP connection*

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

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

Table 77: CD Signal Description

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

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

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 78: DTR Signal Description

3.20.1 Examples of the Expansion Port Configuration

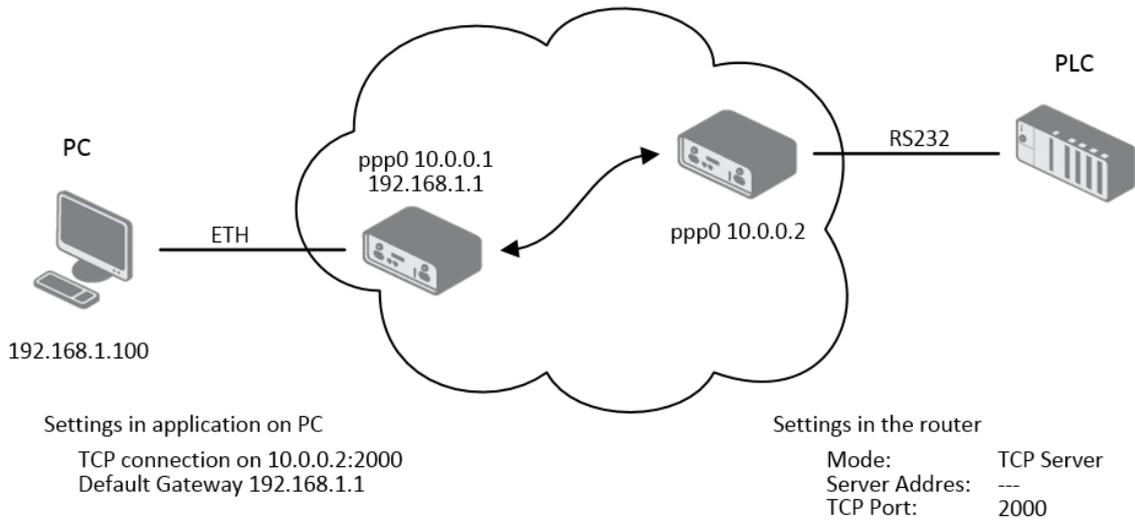


Figure 88: Example of Ethernet to serial communication configuration

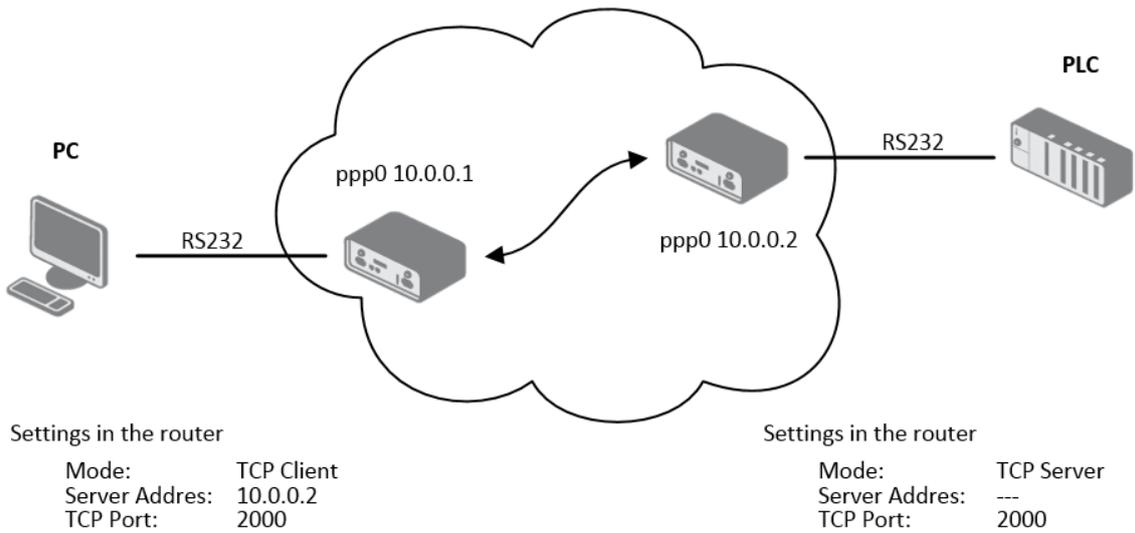


Figure 89: Example of serial interface configuration

3.21 Scripts

There is an option to create your own shell scripts that are executed in specific situations. There are three subpages under the *Scripts* page in the *Configuration* section: *Startup*, *Up/Down IPv4*, and *Up/Down IPv6*.

- The script defined on the *Startup* page is executed after the router starts up, either from powering on or resetting.
- The *Up/Down* script is executed when the WAN connection is either established (up) or lost (down).

For more details, see the following subchapters. For console configuration commands, refer to the [Command Line Interface](#) Application Note. For more information on enhancing the router's basic functionality, refer to the [Extending Router Functionality](#) Application Note.

3.21.1 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. To save the script press the *Apply* button.



Any changes made to a startup script will take effect 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.

3.21.2 Example of Startup Script

```

Startup Script

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

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

Figure 90: Example of a Startup Script

When the router starts up, stop `syslogd` program and start `syslogd` with remote logging on address 192.168.2.115 and limited to 100 entries. Add these lines to the startup script:

```
killall syslogd
```

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

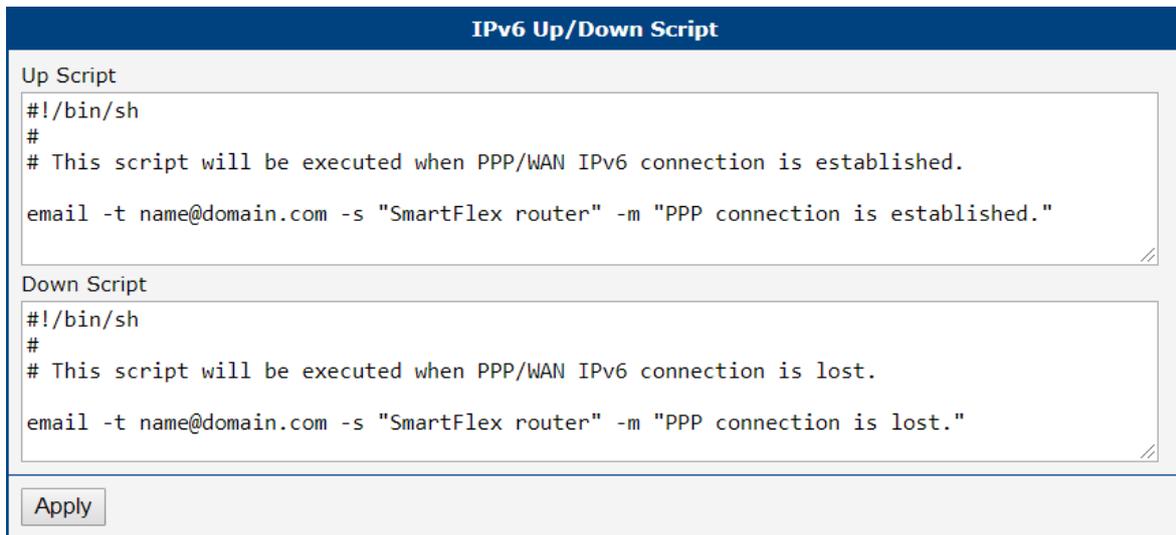
3.21.3 Up/Down Scripts

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

IPv4 WAN connection established/lost, *IPv6 Up/Down Script* runs only on the IPv6 WAN connection established/lost. Any scripts entered into the *Up Script* window will run after a WAN connection is established. Script commands entered into the *Down Script* window will run when the WAN connection is lost.

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

3.21.4 Example of IPv6 Up/Down Script



```
IPv6 Up/Down Script

Up Script
#!/bin/sh
#
# This script will be executed when PPP/WAN IPv6 connection is established.
email -t name@domain.com -s "SmartFlex router" -m "PPP connection is established."

Down Script
#!/bin/sh
#
# This script will be executed when PPP/WAN IPv6 connection is lost.
email -t name@domain.com -s "SmartFlex router" -m "PPP connection is lost."

Apply
```

Figure 91: Example of IPv6 Up/Down Script

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

Add this line to the *Up Script* field:

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

Add this line to the *Down Script* field:

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

3.22 Automatic Update

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; see Figure 92 and Table 79.

Automatic Update

Enable automatic update of configuration

Enable automatic update of firmware

Source HTTP(S) / FTP(S) ▼

Base URL

Unit ID *

Decryption Password *

Update Window Start dynamic ▼

Update Window Length * min

Skip Certificate Verification

Use Custom CA Certificate

CA Certificate *

* can be blank

Figure 92: Automatic Update

Item	Description
Enable automatic update of configuration	If enabled and if there is a new configuration file, it will update it and reboot.
Enable automatic update of firmware	If enabled and if there is a new firmware, it will update it and reboot.
Source	Select the location of the update files: <ul style="list-style-type: none"> HTTP(S)/FTP(S) server – Updates are downloaded from the Base URL address below. The used protocol is specified by that address: HTTP, HTTPS, FTP, or FTPS (only implicit mode is supported). USB flash drive – The router finds the current firmware or configuration in the root directory of the connected USB device. Both – Looking for the current firmware or configuration from both sources.
Base URL	Base URL, IPv4, or IPv6 address from which the configuration file will be downloaded. This option also specifies the communication protocol (HTTP, HTTPS, FTP, or FTPS), see examples below.

Continued on the next page

Continued from previous page

Item	Description
Unit ID	Name of configuration (name of the file without extension). If the <i>Unit ID</i> is not filled, the MAC address of the router is used as the filename (the delimiter colon is used instead of a dot).
Decryption Password	Password for decryption of the encrypted configuration file. This is required only if the configuration is encrypted.
Update Window Start	Choose an hour (range from 1 to 24) when the automatic update will be performed on a daily basis. If the time is not specified (set to <i>dynamic</i>), the automatic update is performed five minutes after the router boots up and then regularly every 24 hours.
Update Window Length	This value defines the period within which the update will be done. This period starts at the time set in the <i>Update Window Start</i> field. The exact time, when the update will be done, is generated randomly.
Skip Certificate Verification	If enabled, the server certificate validation is not executed.
Use Custom CA Certificate	If enabled, the server certificate validation is executed to verify server identity.
CA Certificate	CA certificate to validate on the server.

Table 79: Automatic Update Options

To prevent possible unwanted manipulation of the files, the router verifies that the downloaded file is in the `tar.gz` format. 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.

The **configuration file** name consists of the *Base URL*, the hardware MAC address of the ETH0 interface, and the `cfg` extension. The hardware MAC address and `cfg` extension are added to the file name automatically, so it is not necessary to enter them. When the parameter *Unit ID* is enabled, it defines the specific configuration name that 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 the *Base URL*, the type of router, and the `bin` extension. For the proper firmware filename, see the *Update Firmware* page in the *Administration* section; it is written there, see Chapter 5.11.



It is necessary to load two files (`*.bin` and `*.ver`) to the server. If only the `*.bin` file is uploaded and the HTTP(S) server sends an incorrect `200 OK` response (instead of the expected `404 Not Found`) when the device tries to download the nonexistent `*.ver` file, the router may download the `.bin` file repeatedly.



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 firmware compatibility is provided at the beginning of the router app's Application Note.

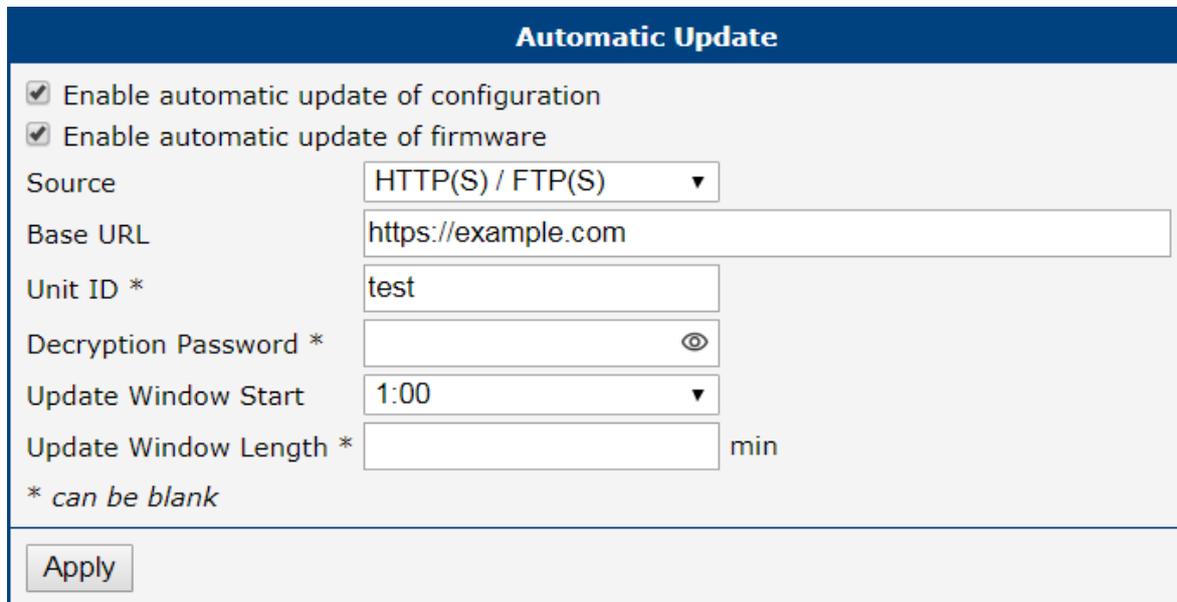


The automatic update feature is also executed five minutes after the firmware upgrade, regardless of the scheduled time.

3.22.1 Example of Automatic Update

In the following example, the router is configured to check for new firmware or a configuration file daily at 1:00 a.m. This scenario is specifically tailored for the SmartFlex router.

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



The screenshot shows a configuration page titled "Automatic Update". It contains the following fields and options:

- Enable automatic update of configuration
- Enable automatic update of firmware
- Source: HTTP(S) / FTP(S) (dropdown menu)
- Base URL: `https://example.com` (text input)
- Unit ID *: `test` (text input)
- Decryption Password *: (password input field with an eye icon)
- Update Window Start: `1:00` (time dropdown menu)
- Update Window Length *: (text input field) min

* can be blank

Apply (button)

Figure 93: Example of Automatic Update 1

3.22.2 Example of Automatic Update Based on MAC

The example provided demonstrates how to check for new firmware or configurations daily between 1:00 a.m. and 3:00 a.m. The configuration file is encrypted, necessitating the setup of a decryption password. This specific example is applicable to the SmartFlex router with the MAC address 00:11:22:33:44:55.

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

Automatic Update

Enable automatic update of configuration

Enable automatic update of firmware

Source

Base URL

Unit ID *

Decryption Password *

Update Window Start

Update Window Length * min

** can be blank*

Figure 94: Example of Automatic Update 2

4. Customization

4.1 Router Apps

Router Apps (RA), formerly known as *User Modules*, enhance router functionality through custom software programs. These apps extend the router's capabilities in areas such as security and advanced networking, offering a flexible and customizable experience.

For Advantech routers, a diverse array of Router Apps is offered, encompassing categories such as connectivity, routing, services, among others. These applications are freely accessible on the Advantech [Router Apps](#) webpage, providing users with a wide range of options to enhance the functionality of their devices.

Figure 95 illustrates the default layout of the *Router Apps* configuration interface. The initial segment, titled *Installed Apps*, presents a comprehensive list of Router Apps currently installed on the device. The subsequent section, *Manual Installation*, provides the functionality for manually adding Router Apps to the system. The *Free Space* row indicates the available space. Lastly, the third section facilitates the online acquisition and installation of Router Apps accessible from a public server.

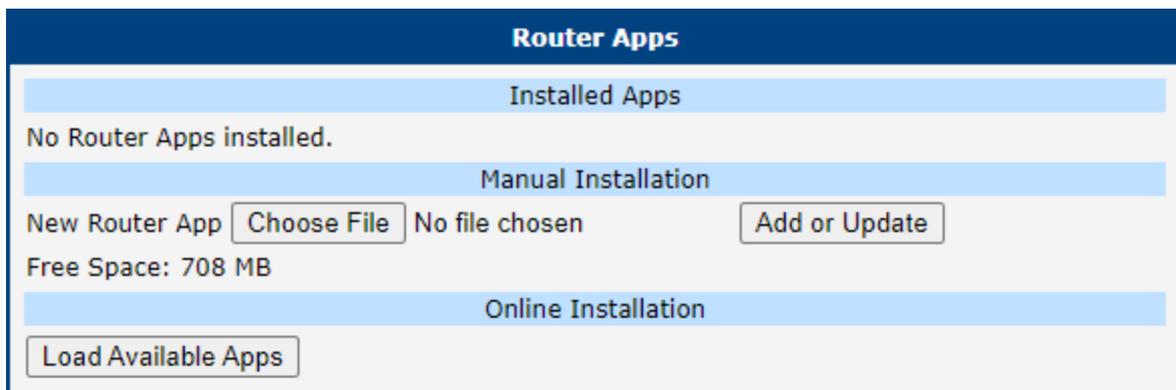


Figure 95: Default Router Apps GUI

Manual RA Installation and Update

For the manual installation of a RA, prepare the application package with a `*.tgz` extension. In the router interface, use the *Choose File* button to select your file and the *Add or Update* button to start the installation.

Online RA Installation and Update

To install Router Apps from the public server, it is imperative to first ensure that the router is correctly configured and connected as outlined in Chapter 4.2. By default, routers are set to automatically connect to the public Advantech server. To proceed with the installation, click on the *Load Available Apps* button, which initiates the loading of a comprehensive list of RA that are available on the server for installation.

Keep these notes in mind:

- The online RA installation functionality starts with firmware version 6.4.0 and is not available for the v2 production platform.
- Note that an Internet connection is required to access the public server. Without it, you will encounter an error: "Cannot get auth header: Couldn't resolve host name".
- The list of online applications is updated only when the *Reload Available Apps* button is pressed. The last loading timestamp is visible next to this button.

- If the router is rebooted, the list of applications is cleared and needs to be reloaded.
- The *Load Available Apps* button is deactivated if the connection to the server is disabled.

Figure 96 displays an instance where the assortment of online applications accessible for installation has been successfully loaded. This figure further demonstrates that only the *Customer Logo* application, version v1.0.0, is installed on the local device, as indicated by its solitary listing in the *Installed Apps* section.

Within the *Online Installation* section, it is highlighted that an updated version of the *Customer Logo* application, version v1.1.0, is available for download from the server, showcasing the potential for upgrading existing applications directly through the router’s interface.

The screenshot shows the 'Router Apps' interface. It is divided into three main sections: 'Installed Apps', 'Manual Installation', and 'Online Installation'.
 - **Installed Apps:** Shows 'Customer Logo v1.0.0 (2020-01-31)' with a 'Delete' button.
 - **Manual Installation:** Includes a 'New Router App' section with a 'Choose File' button (showing 'No file chosen') and an 'Add or Update' button.
 - **Online Installation:** Features a 'Reload Available Apps' button and a 'Last check' timestamp of '2024-01-15 10:39:55'. Below this is a list of available apps, each with a version dropdown and an 'Install' button:
 - 802.1X Authenticator (1.1.0): 802.1X network authentication standard for devices on LAN/WLAN.
 - Azure IoT SDK Python (1.0.0): Add Microsoft Azure IoT Hub Device SDK for Python to router [Obsolete version].
 - Customer Logo (v1.0.0, 1.1.0): Allow users to change the logo displayed in the header of the web interface.
 - Unique Password (1.0.2): unique. From January 2020, this is required by California Senate Bill No. 327. The format used is 'Ph'.
 - WebAccess/VPN Client (1.1.3): This user module allows the router to be part of WebAccess/VPN.
 - WiFi STA Relay (1.3.0): Set the router to transparent mode (WiFi interface in client mode bridged to ETH). [Limited to specific router models]
 - Zabbix Agent (5.0.3-1): Agent for Zabbix network monitoring platform.

Figure 96: Router Apps GUI with Available Online Apps

RA Management

Installed Router Apps, regardless of whether they were installed manually or from the server, appear in the *Installed Apps* section.

Apps with an `index.html` or `index.cgi` page have a clickable link in their name. Clicking on this link opens the GUI of the respective application.

To remove an app, click the *Delete* button, which is located next to the respective application in the *Installed Apps* section.



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

4.2 Settings

To configure the connection settings for the online application hosting server, navigate to the *Customization* → *Settings* menu option. Figure 97 and Table 80 offer comprehensive details regarding the configuration parameters for the server, ensuring users can effectively customize their router to connect to the online application hosting server.

Figure 97: Router Apps Settings

Item	Description
Disable server communication	Connection to the server is disabled, preventing any data exchange with the online application hosting server.
Use public server	Opt to utilize the public server, managed by Advantech, as the primary source for Router Apps. This is the default configuration. An active internet connection is mandatory for accessing the server.
Use custom server ¹	Select this option to establish a connection with a self-hosted server that adheres to the Advantech specifications for Router Apps.
API URL	Enter the URL for the self-hosted server, ensuring the inclusion of the 'https://' prefix to denote a secure connection.
CA certificate	Provide the certificate for the self-hosted server, especially if it utilizes a Certificate Authority (CA) that is not widely recognized or standard.

Table 80: Router Apps Settings

¹Operating your own self-hosted server is feasible exclusively with an on-premises installation of the *WebAccess/DMP* product by Advantech.

4.3 FirstNet Router App

 The *FirstNet* router app is preinstalled for FirstNet models only.



Installing other than the *FirstNet* Router App may invalidate the *FirstNet* certification.

The *FirstNet* router app, which can be located in the *Customization* → *Router Apps* → *FirstNet*, display the global security status as shown in the picture below.

FirstNet

Status	Global Status
Global	
Customization	
Return	Password Policy Set : OK Unique Password Set : OK DoS Protection (IPv4) Enabled : OK DoS Protection (IPv6) Enabled : OK Automatic Update Enabled : OK HTTP Access Disabled : OK SNMP Access Disabled : OK SSH Access Disabled : OK

Figure 98: FirstNet Router App – Global Status

5. Administration

5.1 Manage Users



Be careful not to lock all users with the *Admin* role. In this state, no user will have access rights to configure the users!



This configuration menu is only available for users with the *Admin* role.



If a user with the *Admin* role creates a new user or changes the password for another user, that user is required to change their password after the first login.



For user authentication configuration settings, such as two-factor authentication and account locking rules, refer to Chapter 3.19.1.

To manage users, open the *Manage Users* form in the *Administration* section of the main menu, as shown in Figure 99. In this figure, you can see that there are two users defined on the router: `root` with the *Admin* role, and the user `Alice` with the *User* role. By clicking the *Add User* button, the user `John` (whose data is filled in the form) will be added to the router.

The screenshot shows the 'User Administration' interface. At the top, there is a table listing existing users:

User	Role	Actions
root	Admin	Lock, Modify
Alice	User	Lock, Modify, Delete

Below the table is a form for adding a new user. The form fields are:

- Role: Admin (dropdown)
- Username: John
- New Password: [masked] (with eye icon and validation rules: Must be at least 6 characters long, Must not be palindrome, Must not contain username)
- Confirm Password: [masked] (with eye icon)
- SSH Public Key *: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCMNgYZU504EkVocFQZJJDbmUwe4WbcCIe3aXaEtzlEz30c0/iNTJSNZt10QcY8RmX09nUew0G9H/kC+vP3Px0jRdQAAnJMVtmTlVsdJNeShzkI7oMfBcVDMn3aAcx1T8PQp7YyIPSMURHDTEFa3tUCpGna/QbtXAa397vKRAw765uLiC7ENwBH0axsX6v4xU1qF3Awz7ImUw+PVEe09zjpkpJ3YzJzdzIz (with 'Load From File...' button)
- Phone Number *: +15551234567
- Email Address *: address@email.com

An 'Add User' button is located at the bottom left of the form.

Figure 99: Modify User Page

The first part of this configuration form contains a list of all existing users. Table 81 describes the meaning of the buttons located to the right of each user.

Button	Description
Lock	Locks the user account. This user is not allowed to log in to the router, either to the web interface or via SSH.
Modify	Allows you to change the password or key for the corresponding user, see Chapter 5.2.
Delete	Deletes the user account.

Table 81: Action Button Description

The second part of the configuration form allows adding a new user. All items are described in Table 82. To create a new user, configure all required items and click the *Add User* button.

Item	Description
Role	<ul style="list-style-type: none"> • User <ul style="list-style-type: none"> ○ User with basic permissions. ○ Read-only access to the web GUI, except for <i>Modify User</i>. ○ Some menu items are hidden in the web GUI. ○ Full access to the Router Apps GUI for already installed Router Apps. ○ No access to the router via Telnet, SSH or SFTP. ○ Read-only access to the FTP server. • Admin <ul style="list-style-type: none"> ○ 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.
New Password	Specifies the password for the user. It must match the rules stated in the GUI, which depend on the <i>Force Password Complexity</i> level set in <i>Configuration</i> → <i>Services</i> → <i>Authentication</i> , as described in Chapter 3.19.1.
Confirm Password	Confirms the password.
Public key	Enter the SSH Public Key to enable passwordless SSH login. Refer to Chapter 5.2.2 for details.
Phone Number	User's phone number. If configured, an SMS is sent to the user when their password is changed. A functional SIM card is required.
Email Address	User's email address. If configured, an email is sent to the user when their password is changed. SMTP must be configured.
Add User	Click this button to create a new user based on the entries in the fields above.

Table 82: User Parameters

5.2 Modify User

-  This configuration menu is only available for users with the *User* role. Such users can only modify their own account.
-  To view the current user authentication configuration settings, such as two-factor authentication and account locking rules, refer to Chapter 3.19.1.

If a user with a *User* role is logged in, they can manage only their user account. This can be done on the *Administration* → *Modify User* page. You will get the same configuration page if you have the *Admin* role when modifying another user account on the *Manage Users* page.

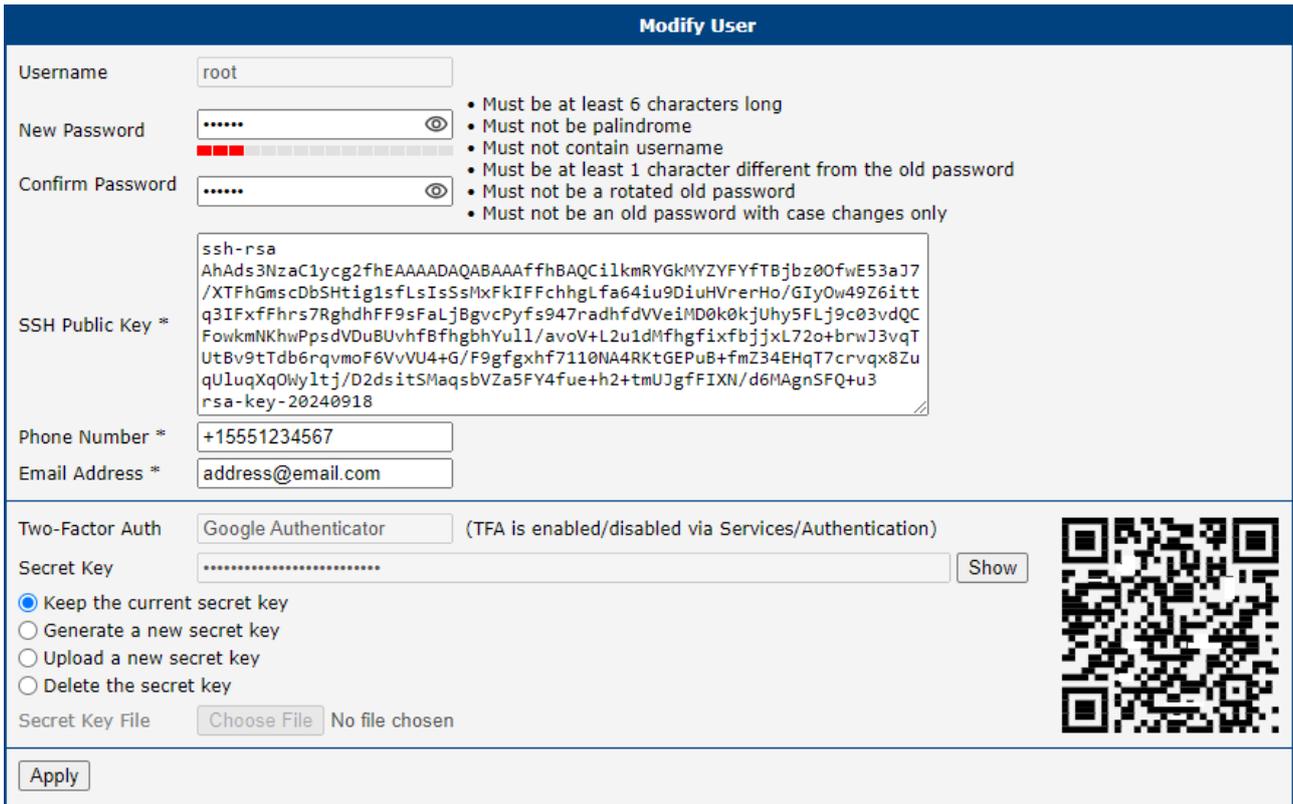


Figure 100: Users Administration Form

The meaning of the items in the first part of this window is clear or described in more detail in Chapter 5.1. If you want to change your own password, you will need to enter the current password as well. In the second part, you can configure two-factor authentication for a user, including its secret key.

5.2.1 Two-Factor Authentication



If the configuration of two-factor authentication fails or does not complete properly, you will be unable to log in to the router using that user account. It is recommended to set up a backup account to log in to the router in case issues arise during the configuration process. You can delete this backup account after successfully configuring two-factor authentication.



To successfully log in using two-factor authentication, the correct system time must be set on the router. Therefore, it is strongly recommended to enable the *Synchronize clock with remote NTP server* option. For more details, refer to Chapter [3.19.5 NTP](#).

If you have enabled one of the two-factor authentication services, as mentioned above, you should see the chosen service name in the *Two-Factor Auth* field, as shown in Figure [100](#).

A secret key is required to activate the two-factor authentication. You can generate this key by choosing the *Generate a new secret key* option. You can upload the user's secret key from a file using *Upload a new secret key*. Clicking the *Apply* button the secret key will be saved. Next, click the *Show* button, located to the right of the secret key, the secret key will be shown. If the secret key is defined, a QR code will appear on the right, allowing you to easily add this key to the chosen authentication application by scanning it, see section [Authenticator](#)



Without the secret key, a user will not be able to finish two-factor configuration and log in to the router.



A user with the *Admin* role cannot generate or upload the secret key for another user; they can only delete the key.

Implementation Notes

- Two different two-factor implementations are supported:
 - [Google Authenticator](#),
 - [OATH Toolkit](#).
- Implemented for the following services only:
 - the router's web server login,
 - SSH login,
 - TELNET login.
- Two-factor authentication is disabled by default.
- Two-factor authentication data are backed up/restored during user backup/restore.
- All private two-factor authentication data are removed when the corresponding user is deleted.
- No internet or mobile connection is required to use two-factor authentication, but keep in mind the need to synchronize the system time.

Configuration Steps

1. Enable the two-factor authentication service as described in Chapter 3.19.1.
2. Enable the two-factor authentication for a user as described in Chapter 5.2.
3. Use an application or service to perform the two-factor authentication to the router as described in following *Authenticator* Chapter.

Authenticator

To log in with two-factor authentication, you need an Authenticator application. Both *Google Authenticator* and *OATH* use TOTP (Time-based One-Time Password, RFC 6238) mode by default. You can use any compatible authenticator. For information about authenticator usage, see the corresponding manual.

You can use the [Google Authenticator](#) application; see Figure 101 for the download links.

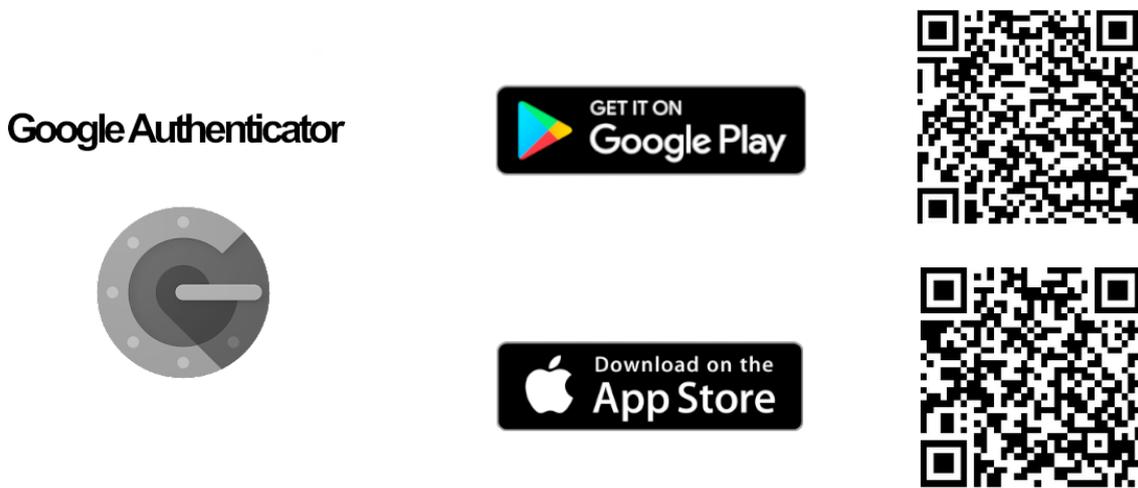


Figure 101: Links for Google Authenticator Application

[Authenticator-Extension](#) is available as an extension for all popular browsers; see Figure 102 for the download links.

Authenticator-Extension / Authenticator



Figure 102: Links for Authenticator-Extension

In an Authenticator application, you can create a new entry by entering the secret key you have noted down or by scanning the QR code shown for the user on the *Modify User* configuration page.

Router Web Login

When logging into the router's web interface, enter the *Username* and *Password* as you would for a standard login; see Figure 103.

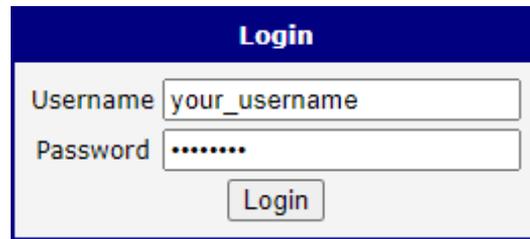


Figure 103: Standard Login

Next, you will be prompted to enter the Verification Code; see Figure 104. This code is obtained from your Authenticator. Note that there is a **limited time** for code usage, typically within five minutes, assuming the system time is correct.

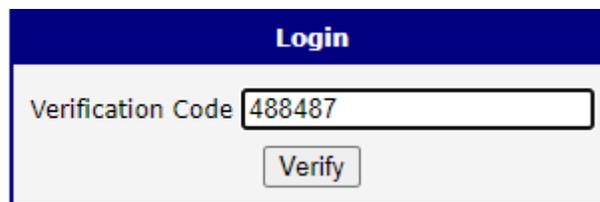


Figure 104: Verification Code

After entering the correct code, you will be successfully logged in to the router's web interface.

SSH and Telnet Login

Logging into SSH and Telnet with two-factor authentication is similar. Enter your username, password, and the generated verification code. For an example of SSH login, see Figure 105.

```
login as: your_username
Using keyboard-interactive authentication.
Password:
Using keyboard-interactive authentication.
Verification code:
$ █
```

Figure 105: SSH Login

5.2.2 Passwordless Console Login

You can log in to SSH without a password using the SSH Public Key. The process of key generation and connection will be demonstrated in this chapter using *PuTTY*, a free terminal emulator for Windows OS.

Installation Notes

- For simplicity and clarity, we will perform a manual installation of PuTTY to the directory C:\bin, instead of using an .msi installation package.
- From the PuTTY application [download page](#), under the section *Alternative binary files*, download the individual files named putty.exe, puttygen.exe, and pageant.exe. You will likely want the 64-bit x86 version. We use *PuTTY* version 0.80. Save these files to the C:\bin directory.

Generate Keys

- Run the downloaded puttygen.exe application to create your SSH key, see Figure 106.
- Ensure the RSA option is selected.
- Click the *Generate* button. Move your mouse within the window to generate the keys.
- Once complete, the key data appears.

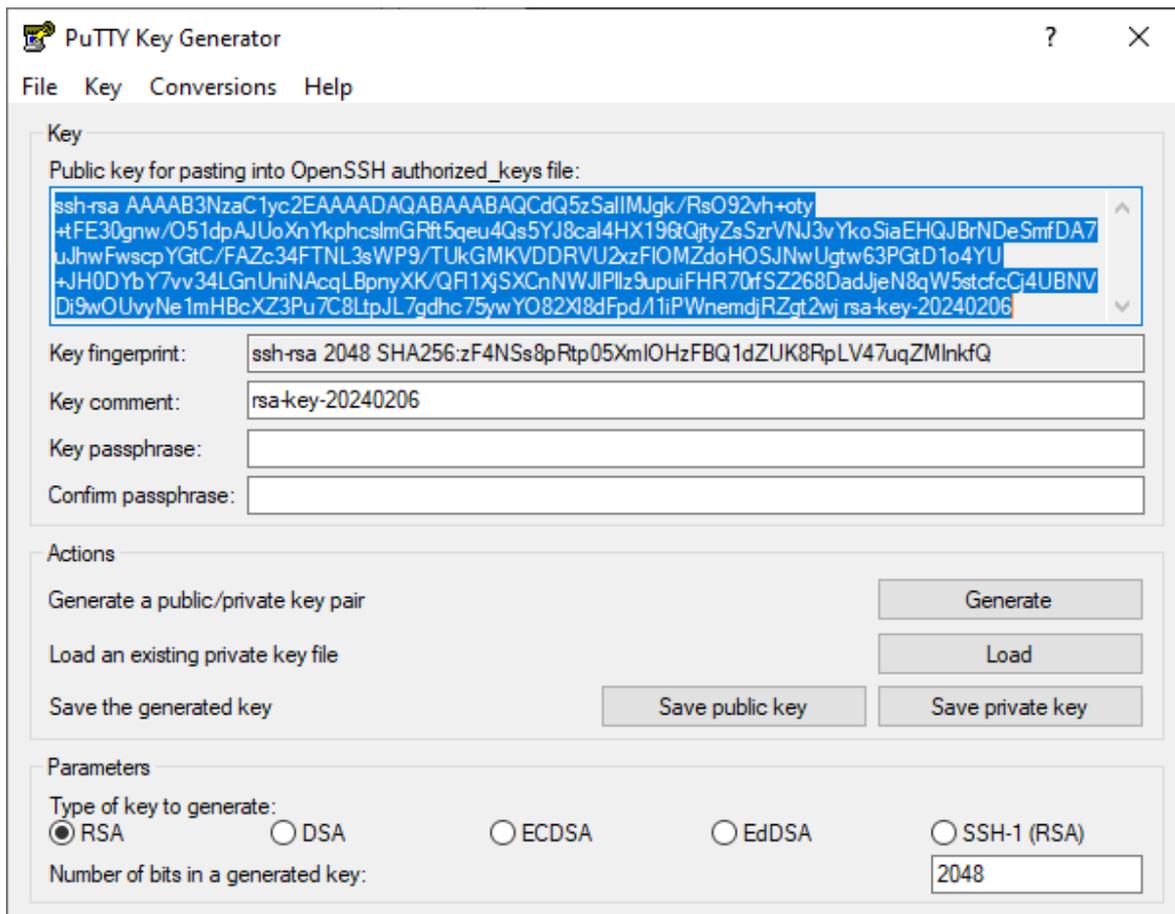


Figure 106: Key Generation

- Click both *Save public key* and *Save private key* buttons to save these keys on your computer:
 - Name the public key something like *hostpublickey* and the private key something like *hostprivatekey*, without manually adding extensions.
 - If prompted about a passphrase, click *Yes* to save without a passphrase.
- Leave the *PuTTY Key Generator* application open.

Uploading Public Key to the Router:

- In the router GUI (*Administration* → *Manage Users*), click the *Modify* button for the user to whom you want to add the public key. Ensure the user has the *Admin* role, since a user with the *User* role is not permitted for SSH login.
- Enter the generated public key for the user:
 - In the *PuTTY Key Generator*, select the entire public key as demonstrated in Figure 106 with the key data selected (in blue), and copy it to the clipboard.
 - In the router GUI, paste the key into the *SSH Public Key* field.
 - It is important that the key **starts with "ssh-rsa "** followed by the key itself.
- Save the user settings by clicking the *Apply* button.
- Now, you can close the *PuTTY Key Generator* application.

PuTTY Session Configuration

- Open the `c:\bin\putty.exe` application.
- In the configuration window, navigate to *Connection* → *Data* and enter the username (the router's user to whom the public key was saved) in the *Auto-login username* field.
- Under *Connection* → *SSH* → *Auth* → *Credentials*, click the *Browse* button near the *Private key file for authentication* field, and select your *hostprivatekey* file generated according to the steps above.
- In the configuration window, navigate to the *Session* menu item and configure the following:
 - *Host Name*: IP address of your router.
 - *Port*: 22.
 - *Connection Type*: SSH.
 - *Saved Session*: Enter a name for this session.
 - Click *Save* to store these session settings.

Connecting to the Router

- Open the `c:\bin\putty.exe` application.
- Select and load your session with the *Load* button.
- Click *Open* to establish the connection.
- If everything is configured correctly, an SSH console prompt will open with the user logged in.

5.2.3 Expired Password

If the password expires after the number of days defined in *Expire Password After* has passed, the user will be prompted to enter a new password as shown in Image 107. The new password must match the rules stated in the GUI, which depend on the *Force Password Complexity* level set in *Configuration* → *Services* → *Authentication*, as described in Chapter 3.19.1.



New Password

Password for user Alice has expired.
You cannot continue until you set a new one.

New Password

Confirm Password

- Must be at least 6 characters long
- Must not be palindrome
- Must not contain username
- Must be at least 1 character different from the old password
- Must not be a rotated old password
- Must not be an old password with case changes only

Apply

Figure 107: Expired Password Prompt



The user will be prompted to change their password when logging into the new router for the first time or if their password was changed by a user with an admin role.

5.3 Change Profile

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

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

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

Figure 108: Change Profile

5.4 Set Date and Time



This administration page is not for configuring the NTP client, but only for one-time date and time settings. For permanent NTP client configuration, please go to the *Configuration* → *Services* → *NTP* page.

There are three ways to set the system date and time on a one-time basis, as shown in the figure below:

1. **Set current browser time:** This option sets the device's clock to match the time displayed on your web browser.
2. **Set specific date/time:** You can manually input the date and time. Ensure you adhere to the **yyyy-mm-dd** format for the date. For the time, use the **HH:MM:SS** format. **Note:** The time preloaded is the browser time, not the router time.
3. **Query NTP server:** To query the date and time from an NTP server, input the address of the NTP server. The system supports both IPv4 and IPv6 addresses, as well as domain names.

Set Date and Time	
<input checked="" type="radio"/> Set current browser time	
<input type="radio"/> Set specific date / time	
Date	2024 - 05 - 23
Time	12 : 34 : 28
<input type="radio"/> Query NTP server	
NTP Server Address	pool.ntp.org
<input type="button" value="Apply"/>	

Figure 109: Set Real Time Clock

5.5 Set SMS Service Center

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.

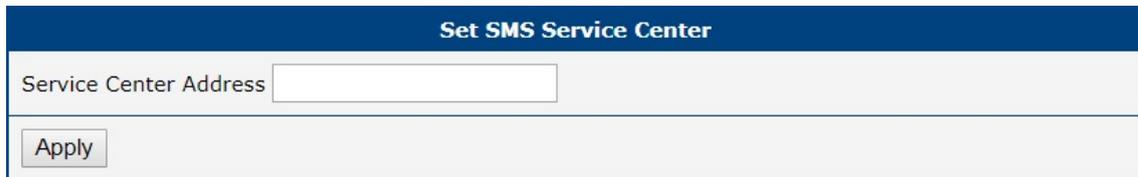


Figure 110: Set SMS Service Center Address

5.6 Unlock SIM Card

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



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



Figure 111: Unlock SIM Card

5.7 Unblock SIM Card

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



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

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

Figure 112: Unblock SIM Card

5.8 Send SMS

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

Send SMS	
Phone number	<input type="text"/>
Message	<input type="text"/>
<input type="button" value="Send"/>	

Figure 113: Send SMS

It is also possible to send an SMS message using CGI script. For details of this method. See the application note *Command Line Interface* [1].

5.9 Backup Configuration



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

You can save the current 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 114. Here you can choose what will be backed up. You can back up the configuration of the router (item *Configuration*) or the configuration of all user accounts (item *Users*). Both types of configurations can be backed up separately or together 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 in an unencrypted file.

Click on the *Apply* button and the configuration will be stored into a configuration file (file with *cfg* extension) in a directory according to the settings of the web browser. The stored configuration can be used later for restoration, see Chapter 5.10 for more information.

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

Figure 114: Backup Configuration

5.10 Restore Configuration

You can restore a router configuration stored in a file. You 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 to 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 the *Apply* button.

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

Figure 115: Restore Configuration

5.11 Update Firmware



For enhanced security, it is strongly recommended to regularly update your router's firmware to the latest version. Avoid downgrading the firmware to a version older than the production release, and refrain from uploading firmware meant for different models, as these actions can lead to device malfunction.



Be aware that firmware updates may cause compatibility issues with Router Apps. To minimize such issues, it is advisable to update all Router Apps to their latest versions concurrently with the router's firmware. Detailed compatibility information for each app is provided at the beginning of its Application Note.



The latest firmware for our routers is available on the Engineering Portal's product page. For downloading the appropriate firmware for your router model, please visit <https://icr.advantech.com/support/router-models>.

The *Update Firmware* administration page showcases the current firmware version and the name of the router's firmware, as illustrated in Figure 116. This page also offers the capability to update the router's firmware, accommodating both manual updates and online updates from the public server.

Update Firmware	
Firmware Version :	6.3.9 (2023-01-04)
Firmware Name :	ICR-445x.bin
New Firmware	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Update"/>
<input type="button" value="Check for updates"/>	Last check 2024-01-18 12:06:55
Newest FW online 6.3.10	<input type="button" value="Download and Update"/>

Figure 116: Update Firmware Administration Page

Manual Firmware Update

To manually update the router's firmware, click on the *Choose File* button and select the firmware file. Then, press the *Update* button to initiate the firmware update process.

Online Firmware Update

Starting with firmware version 6.4.0, the firmware can be updated from a public server. Ensure that your router is properly configured as described in Chapter 4.2.

To verify the availability of a newer firmware version on the server, click the *Check for updates* button. If a new version is available, the version information and a *Download and Update* button will appear. Clicking this button initiates the firmware update process.

During the firmware update, the router will display status messages as depicted in Figure 117. Upon completion, the router will automatically reboot. After rebooting, click the *here* link in the web interface to reopen it.

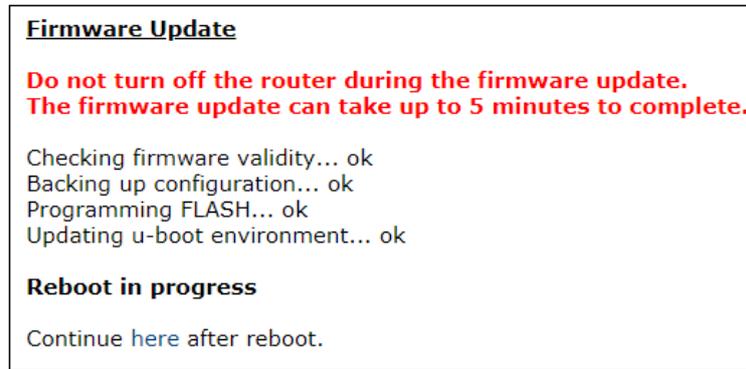


Figure 117: Process of Firmware Update

5.12 Reboot

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

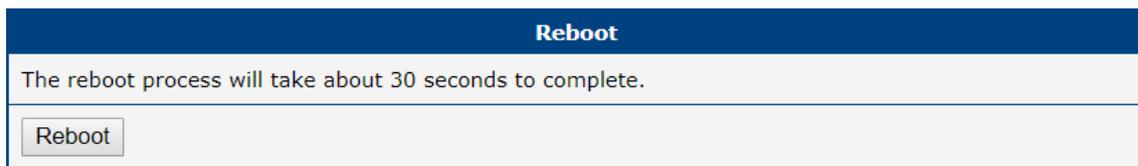


Figure 118: Reboot

5.13 Logout

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

6. 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.

6.1 Access to the Internet from LAN

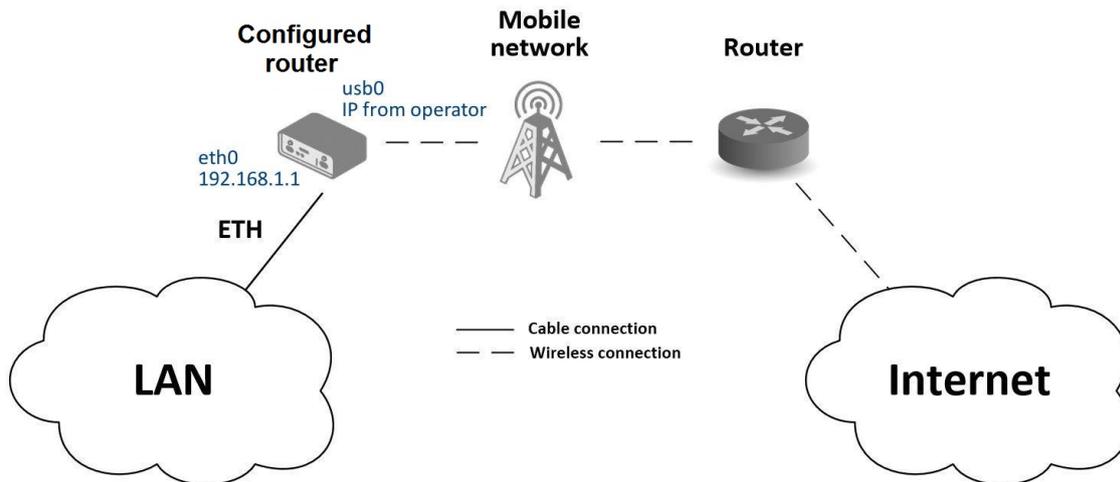


Figure 119: Access to the Internet from LAN – sample topology

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 120. 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 3.1.

Mobile WAN Configuration: Use the *Mobile WAN* item in the *Configuration* section to configure the connection to the mobile network, see Figure 121. 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 3.4.1.

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.

Status	ETH0 Configuration	
General		
Mobile WAN		
Network		
DHCP		
IPsec		
DynDNS		
System Log		
Configuration		
Ethernet		
• ETH0 ←		
• ETH1		
VRRP		
Mobile WAN		
PPPoE		
Backup Routes		
Static Routes		
Firewall		
NAT		
	DHCP Client	IPv4 disabled IPv6 disabled
	IP Address	192.168.1.1
	Subnet Mask / Prefix	255.255.255.0
	Default Gateway	
	DNS Server	
	Bridged	no
	Media Type	auto-negotiation
	<input checked="" type="checkbox"/> Enable dynamic DHCP leases	
	IP Pool Start	IPv4 192.168.1.2 IPv6
	IP Pool End	192.168.1.254
	Lease Time	600 600 sec

Figure 120: Access to the Internet from LAN – *Ethernet* configuration

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

Figure 121: Access to the Internet from LAN – *Mobile WAN* configuration

6.2 Backup Access to the Internet from LAN

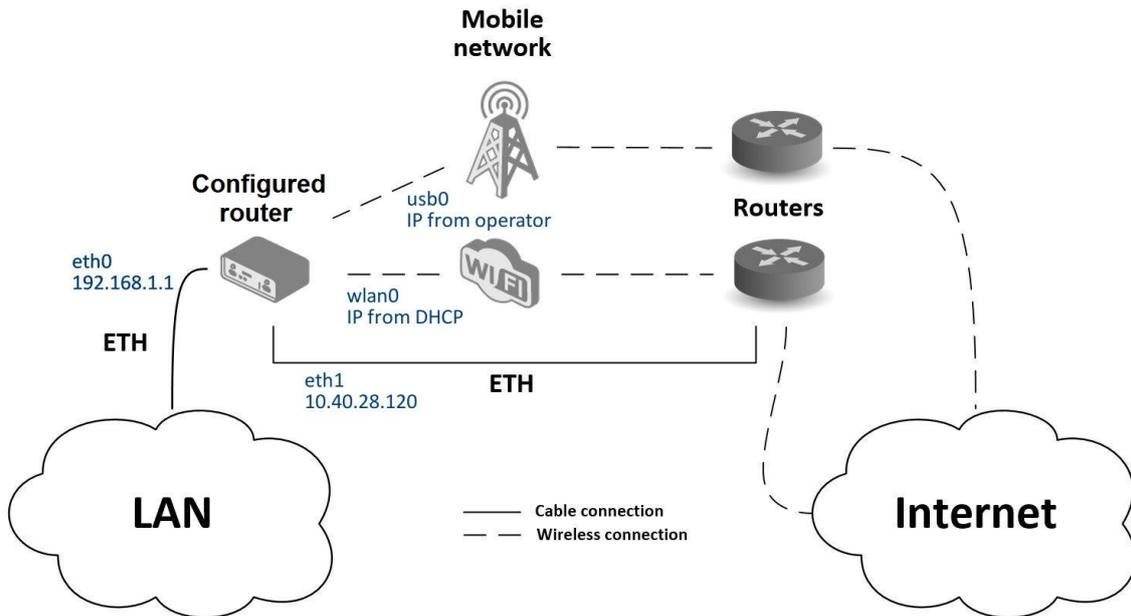


Figure 122: Backup access to the Internet – sample topology

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

Status	ETH1 Configuration	
General	IPv4	
Mobile WAN	IPv6	
Network	DHCP Client	disabled
DHCP	IP Address	10.40.28.120
IPsec	Subnet Mask / Prefix	255.255.252.0
DynDNS	Default Gateway	10.40.30.1
System Log	DNS Server	192.168.2.27
Configuration	Bridged	no
Ethernet	Media Type	auto-negotiation
• ETH0	<input type="checkbox"/> Enable dynamic DHCP leases	
• ETH1	IP Pool Start	
VRRP	IP Pool End	
Mobile WAN	Lease Time	600 sec
PPPoE		
Backup Routes		
Static Routes		
Firewall		

Figure 123: 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 123. 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 3.1.

WLAN configuration: To use the WLAN you will need to configure the WiFi station in the *WiFi* → *Station* item, as shown in Figure 124. Check the *Enable WiFi STA*, enable the DHCP client and fill in the addresses of the default gateway and DNS server. Next, fill in the data for the connection (SSID, authentication, encryption, WPA PSK Type and password). For details see Chapter 3.7. Click the *Apply* button to confirm the changes.

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

Status	WiFi STA Configuration	
General	<input checked="" type="checkbox"/> Enable WiFi STA	
Mobile WAN	DHCP Client	IPv4: enabled IPv6: enabled
WiFi	IP Address	
Network	Subnet Mask / Prefix	
DHCP	Default Gateway	192.168.3.1
IPsec	DNS Server	192.168.3.1
DynDNS	SSID	WiFiNetwork
System Log	Probe Hidden SSID	enabled
	Country Code *	
Configuration	Authentication	WPA2-PSK
Ethernet	Encryption	AES
VRRP	WEP Key Type	ASCII
Mobile WAN	WEP Default Key	1
PPPoE	WEP Key 1	
WiFi	WEP Key 2	
• Access Point	WEP Key 3	
• Station	WEP Key 4	
Backup Routes	WPA PSK Type	ASCII passphrase
Static Routes	WPA PSK	WiFiPassword
Firewall		
NAT		
OpenVPN		
IPsec		
GRE		
L2TP		
PPTP		
Services		
Expansion Port 1		
Expansion Port 2		

Figure 124: 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 125.) 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 3.4.1.

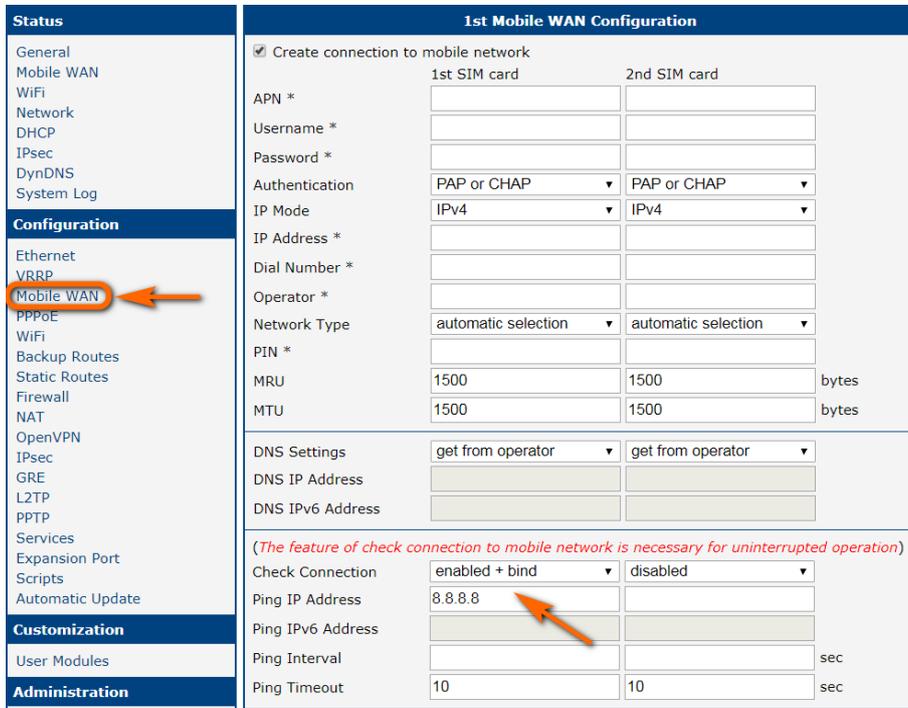


Figure 125: Backup access to the Internet – Mobile WAN configuration

Backup Routes configuration: After setting up the backup routes you will need to set their priorities. In Figure 126, 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 3.9.

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.

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

Status	Backup Routes Configuration
General	<input checked="" type="checkbox"/> Enable backup routes switching
Mobile WAN	Mode: <input type="text" value="Single WAN"/>
WiFi	<input checked="" type="checkbox"/> Enable backup routes switching for Mobile WAN
Network	Priority: <input type="text" value="3rd"/> 
DHCP	Weight: <input type="text"/>
IPsec	<input type="checkbox"/> Enable backup routes switching for PPPoE
DynDNS	Priority: <input type="text" value="1st"/>
System Log	Ping IP Address: <input type="text"/>
Configuration	Ping IPv6 Address: <input type="text"/>
Ethernet	Ping Interval: <input type="text"/> sec
VRRP	Ping Timeout: <input type="text" value="10"/> sec
Mobile WAN	Weight: <input type="text"/>
PPPoE	<input checked="" type="checkbox"/> Enable backup routes switching for WiFi STA
WiFi	Priority: <input type="text" value="2nd"/> 
Backup Routes 	Ping IP Address: <input type="text"/>
Static Routes	Ping IPv6 Address: <input type="text"/>
Firewall	Ping Interval: <input type="text"/> sec
NAT	Ping Timeout: <input type="text" value="10"/> sec
OpenVPN	Weight: <input type="text"/>
IPsec	<input type="checkbox"/> Enable backup routes switching for ETH0
GRE	Priority: <input type="text" value="1st"/>
L2TP	Ping IP Address: <input type="text"/>
PPTP	Ping IPv6 Address: <input type="text"/>
Services	Ping Interval: <input type="text"/> sec
Expansion Port	Ping Timeout: <input type="text" value="10"/> sec
Scripts	Weight: <input type="text"/>
Automatic Update	<input checked="" type="checkbox"/> Enable backup routes switching for ETH1
Customization	Priority: <input type="text" value="1st"/> 
User Modules	Ping IP Address: <input type="text"/>
Administration	Ping IPv6 Address: <input type="text"/>
Users	Ping Interval: <input type="text"/> sec
Change Profile	Ping Timeout: <input type="text" value="10"/> sec
Change Password	Weight: <input type="text"/>
Set Real Time Clock	<input type="text" value="1st"/> 
Set SMS Service Center	Ping IP Address: <input type="text"/>
Unlock SIM Card	Ping IPv6 Address: <input type="text"/>
Unblock SIM Card	Ping Interval: <input type="text"/> sec
Send SMS	Ping Timeout: <input type="text" value="10"/> sec
Backup Configuration	Weight: <input type="text"/>
Restore Configuration	<input type="text" value="1st"/> 
Update Firmware	Ping IP Address: <input type="text"/>
Reboot	Ping IPv6 Address: <input type="text"/>
Logout	Ping Interval: <input type="text"/> sec
	Ping Timeout: <input type="text" value="10"/> sec
	Weight: <input type="text"/>
	<input type="button" value="Apply"/>

Figure 126: Backup access to the Internet – Backup Routes configuration

6.3 Secure Networks Interconnection or Using VPN

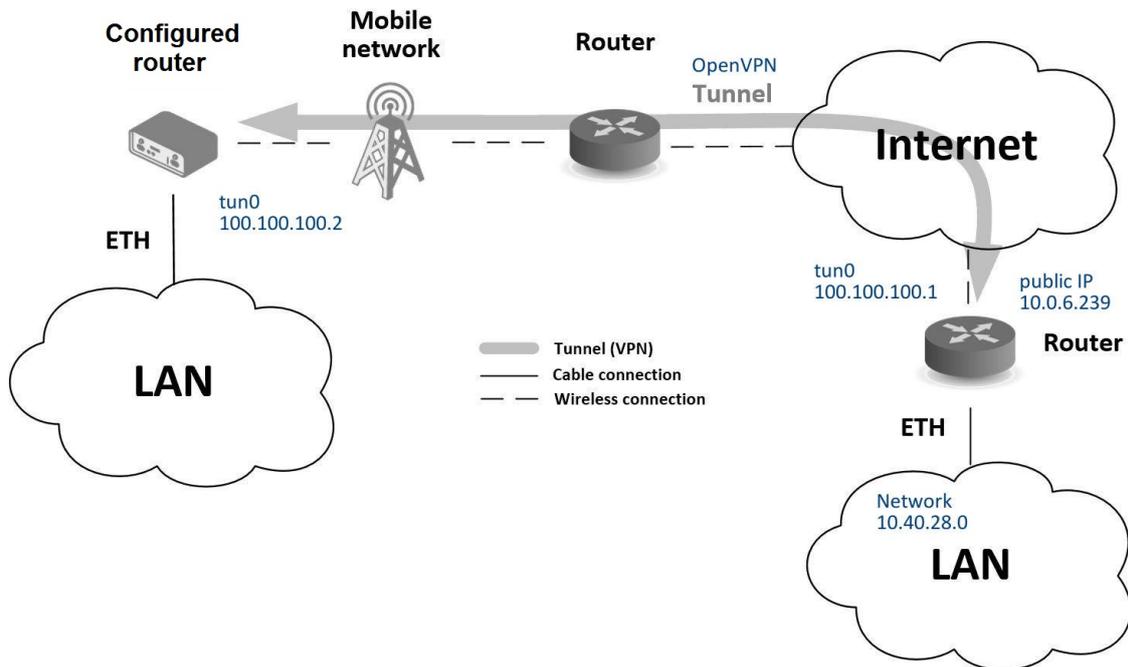


Figure 127: Secure networks interconnection – sample topology

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. 127. You may use several different secure protocols.

- *OpenVPN* (it is a configuration item in the web interface of the router), see Chapter 3.13 or Application Note [5],
- *IPsec* (it is also configuration item in the web interface of the router), see Chapter 3.14 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 127. 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 3.4.1). 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 3.13 or Application Note [5].

Status	1st OpenVPN Tunnel Configuration	
General	<input checked="" type="checkbox"/> Create 1st OpenVPN tunnel	
Mobile WAN	Description *	myTunnel
WiFi	Interface Type	TUN
Network	Protocol	UDP
DHCP	UDP Port	3000
IPsec	Remote IP Address *	10.0.6.239
DynDNS	Remote Subnet *	10.40.28.0
System Log	Remote Subnet Mask *	255.255.252.0
	Redirect Gateway	no
	Local Interface IP Address	100.100.100.2
	Remote Interface IP Address	100.100.100.1
	Remote IPv6 Subnet *	
	Remote IPv6 Subnet Prefix Length *	
	Local Interface IPv6 Address *	
	Remote Interface IPv6 Address *	
	Ping Interval *	10 sec
	Ping Timeout *	30 sec
	Renegotiate Interval *	sec
	Max Fragment Size *	bytes
	Compression	LZO
	NAT Rules	not applied
	Authenticate Mode	pre-shared secret
	Security Mode	tls-auth
	Pre-shared Secret	# # 2048 OpenVPN static key #

Figure 128: 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

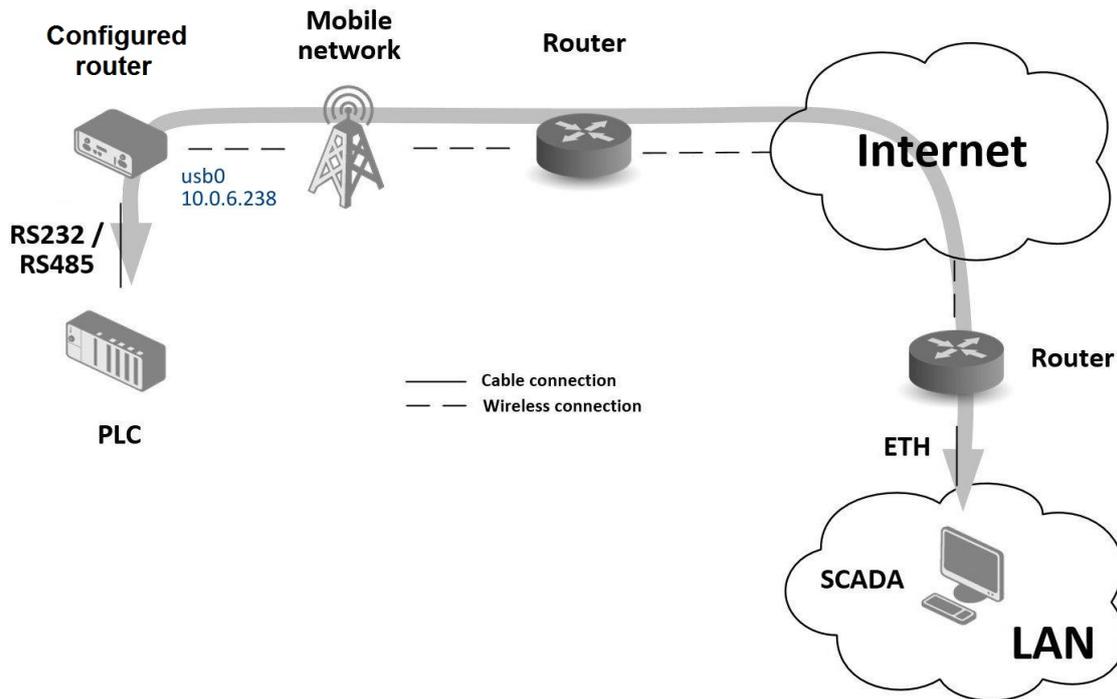


Figure 129: Serial Gateway – sample topology

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 Figure 129.

Configuration is done in the *Configuration* section, *Mobile WAN*, with the *Expansion Port 1* item for RS232, or *Expansion Port 2* for RS485. In this example, the RS232 interface of the router is used.

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 3.4.1.

Expansion Port 1 configuration: The RS232 interface (port) can be configured in the *Configuration* section, via the *Expansion Port 1* item, see Figure 130.) You will need to enable the RS232 port by checking *Enable expansion port 1 access over TCP/UDP*. You may edit the serial communication parameters (not needed in this example). The important items are *Protocol*, *Mode* and *Port*. These set the parameters of communication out to the network and the Internet. In this example the TCP protocol is chosen, and the router will work as a server listening on the 2345 TCP port. Confirm the configuration clicking the *Apply* button.

Status	Expansion Port Configuration
General	<input checked="" type="checkbox"/> Enable expansion port access over TCP/UDP
Mobile WAN	Port Type: RS-232
Network	Baudrate: 9600
DHCP	Data Bits: 8
IPsec	Parity: none
DynDNS	Stop Bits: 1
System Log	Flow Control: none
Configuration	
Ethernet	Split Timeout: 20 msec
• ETH0	Protocol: TCP
• ETH1	Mode: server
VRRP	Server Address:
Mobile WAN	TCP Port: 2345
PPPoE	Inactivity Timeout *: sec
Backup Routes	<input type="checkbox"/> Reject new connections
Static Routes	<input type="checkbox"/> Check TCP connection
Firewall	Keepalive Time: 3600 sec
NAT	Keepalive Interval: 10 sec
OpenVPN	Keepalive Probes: 5
IPsec	<input type="checkbox"/> Use CD as indicator of TCP connection
GRE	<input type="checkbox"/> Use DTR as control of TCP connection
L2TP	* can be blank
PPTP	<input type="button" value="Apply"/>
Services	
Expansion Port 1	
Expansion Port 2	
USB Port	
Scripts	
Automatic Update	
Customization	

Figure 130: Serial Gateway – konfigurace *Expansion Port 1*

To communicate with the serial device (PLC), connect from the PC (Labeled as SCADA in Figure 129) 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.

Appendix A: Open Source Software License

The software in this device uses various pieces of open-source software governed by the following licenses:

- GPL versions 2 and 3
- LGPL version 2
- BSD-style licenses
- MIT-style licenses

The list of components and 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 this address (replace the DEVICE_IP string with the actual router's IP address):

https://DEVICE_IP/licenses.cgi

This is a written offer valid for three years since the device purchase, offering any third party for a charge no more than the cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code on a flash drive medium. 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 an LGPL library for its 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.

Source codes under the GPL license are available at the following address:

<https://icr.advantech.com/source-code>

Appendix B: Glossary and Acronyms

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 Tunneling 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 commer-

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

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 telecommuni-

cations 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.

Appendix C: Index

A

Access Point	
Configuration.....	54
Information.....	13
Accessing the router.....	3
Add User.....	153
APN.....	45
AT commands.....	129
Authentication.....	114

B

Backup Configuration.....	166
Backup Routes.....	66
Bridge.....	28

C

Change Profile.....	162
Configuration update.....	145
Control SMS messages.....	128

D

Data limit.....	48
Default Gateway.....	27, 61
Default IP address.....	3
Default password.....	3
Default SIM card.....	49
Default username.....	3
DHCP.....	20, 27, 61, 181
DHCPv6.....	29
Dynamic.....	29
Static.....	29
DHCPv6.....	20, 27, 61
DNS.....	181
DNS server.....	27, 46, 61
DNS64.....	17
Domain Name System.....	<i>see</i> DNS
DoS attacks.....	79
Dynamic Host Configuration Protocol.....	<i>see</i> DHCP
DynDNS.....	23, 118
DynDNSv6.....	23, 118

E

Expansion Port	
RS232.....	139
RS485.....	139

F

Firewall.....	77
Filtering of Forwarded Packets.....	78
Filtering of Incoming Packets.....	77
Protection against DoS attacks.....	79
Firmware update.....	145, 168
Firmware version.....	9
FTP.....	119

G

GRE.....	105, 181
----------	----------

H

HTTP.....	120
-----------	-----

I

ICMPv6.....	46
IPsec.....	92, 182
Authenticate Mode.....	97
Encapsulation Mode.....	96
IKE Mode.....	96
IPv4.....	182
IPv6... 7, 17, 26, 30, 45, 46, 77, 82, 87, 92, 118, 143	

L

L2TP.....	108, 182
LAN	
ETH0.....	26
ETH1.....	26
ETH2.....	26
IPv6.....	26
PoE PSE.....	28
Location Area Code.....	10
Logout.....	169

M

Mobile network	45
Modify User	155
Multiple WANs	66, 68, 76

N

NAT	82, 182
NAT64	17
Neighbouring WiFi Networks	14
Network Address Translation	see NAT
NTP	121, 182
NTP server	163

O

Object Identifier	123
OpenVPN	87, 183
Authenticate Mode	88

P

PAT	82
PIN number	164
PLMN	10
PoE PSE	8, 28
Port	183
PPPoE	52
PPPoE Bridge Mode	51
PPTP	111, 183
Prefix delegation	30
PUK number	165

R

RADIUS	32, 54, 57
Reboot	169
Remote access	83
Restore Configuration	167
Router	1
Accessing	3
Router Apps	149

S

Save Log	24
Save Report	24

Send SMS	165
Serial line	
RS232	139
RS485	139
Serial number	9
Set internal clock	163
Signal Quality	10
Simple Network Management Protocol	see SNMP
SMS	127
SMS Service Center	164
SMTP	126, 183
SNMP	122, 183
SSH	135
Startup Script	143
Static Routes	76
Switch between SIM Cards	48
Syslog	136
System Log	24

T

TCP	184
Telnet	138
Transmission Control Protocol	see TCP
Two-Factor Authentication	156

U

UDP	184
Unblock SIM card	165
Uniform resource locator	see URL
Unlock SIM card	164
Up/Down script	143
URL	184
Usage Profiles	162
User Datagram Protocol	see UDP
Users	153

V

Virtual private network	see VPN
VLAN	39
VPN	184
VRRP	41, 184

W

Web interface	3
WiFi	

Authentication	56, 62
HW Mode	55
WiFi AP	54
WiFi STA	60

WiFi Station	
Configuration	60
WireGuard	101

Appendix D: Related Documents

- [1] Command Line Interface
- [2] Remote Monitoring
- [3] WebAccess/DMP
- [4] R-SeeNet
- [5] OpenVPN Tunnel
- [6] IPsec Tunnel
- [7] GRE Tunnel
- [8] WireGuard Tunnel
- [9] FlexVPN
- [10] VLAN
- [11] SNMP Object Identifiers
- [12] AT Commands (AT-SMS)
- [13] Quality of Service (QoS)
- [14] Programming of Router Apps
- [15] 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.