

# SPECTRE Router

## CONFIGURATION MANUAL





#### International Headquarters

B&B Electronics Mfg. Co. Inc.  
707 Dayton Road  
Ottawa, IL 61350 USA  
**Phone** (815) 433-5100 -- **General Fax** (815) 433-5105  
Website: [www.bb-elec.com](http://www.bb-elec.com)

#### European Headquarters

B&B Electronics Ltd.  
Westlink Commercial Park  
Oranmore, Co. Galway, Ireland  
**Phone** +353 91-792444 -- **Fax** +353 91-792445  
Website: [www.bb-europe.com](http://www.bb-europe.com)

**Doc: 710-10001-02 Rev 3.0 – July 2013**

©2013 B&B Electronics Mfg. Co. Inc. 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 does not represent a commitment on the part of B&B Electronics Mfg. Co. Inc.

B&B Electronics Mfg. Co. Inc. 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.



Useful tips or information of special interest.

## GPL license

Source codes under GPL license are available free of charge by sending an email to [support@bb-elec.com](mailto:support@bb-elec.com).

## Router version

The properties and settings associated with the cellular network connection are not available in non-cellular SPECTRE RT routers.

PPPoE configuration is only available on SPECTRE RT routers. It is used to set the PPPoE connection over Ethernet.



**Declared quality system  
ISO 9001**

B&B Electronics



## Contents

<b>1. Router Configuration Using a Web Browser</b>	<b>10</b>
1.1. Secured access to web configuration	11
1.2. Network status	12
1.3. DHCP status	13
1.4. Mobile WAN status	14
1.5. IPsec status	16
1.6. DynDNS status	16
1.7. System log	17
1.8. LAN configuration	18
1.9. VRRP configuration	23
1.10. Mobile WAN configuration	26
1.10.1. Cellular Carrier Selection	27
1.10.2. GSM/UMTS connection	27
1.10.3. Sprint CDMA network connection	29
1.10.4. DNS address configuration	30
1.10.5. Check PPP connection configuration	30
1.10.6. Data limit configuration	30
1.10.7. Switching between SIM cards or networks	31
1.10.8. Dial-in Access	32
1.10.9. PPPoE bridge mode configuration	32
1.11. PPPoE configuration	34
1.12. Firewall configuration	35
1.13. NAT configuration	37
1.14. OpenVPN tunnel configuration	40
1.15. IPSec tunnel configuration	44
1.16. GRE tunnels configuration	48
1.17. L2TP tunnel configuration	50
1.18. PPTP tunnel configuration	52
1.19. DynDNS client configuration	54
1.20. NTP client configuration	55
1.21. SNMP configuration	56
1.22. SMTP configuration	59
1.23. SMS configuration	60
1.23.1. Send SMS	62
1.24. Expansion Port Configuration	68
1.25. USB port configuration	71
1.26. Startup script	74
1.27. Up/Down script	75
1.28. Automatic update configuration	76
1.29. User modules	77
1.30. Change profile	78
1.31. Change password	78
1.32. Set real time clock	79
1.33. Set SMS service center address	79
1.34. Unlock SIM card	79
1.35. Send SMS	80
1.36. Backup configuration	80
1.37. Restore configuration	80

---

1.38. Update firmware	81
1.39. Reboot	81
2. Router Configuration over Telnet	82
3. Wi-Fi Configuration	83
3.1. Wi-Fi Access Point	83
3.2. WLAN DHCP	84
3.3. Wireless Network Scanning	85
3.4. Wi-Fi Start Log	86
3.5. System Log	86
3.6. Wi-Fi Access Point Configuration	87
3.7. WLAN Configuration	90
3.8. Wi-Fi Port LEDs	90

## Figure List

Fig. 1: Web Configuration .....	10
Fig. 2: Network Status .....	13
Fig. 3: DHCP Status .....	13
Fig. 4: Mobile WAN Status .....	15
Fig. 5: IPsec status .....	16
Fig. 6: DynDNS status .....	16
Fig. 7: System log .....	17
Fig. 8: Example <i>syslogd</i> startup script with the parameter <i>-r</i> .....	17
Fig. 9: Example 1 - Network Topology for Dynamic DHCP Server .....	19
Fig. 10: Example 1 - LAN Configuration Page .....	20
Fig. 11: Example 2 - Network Topology with both Static and Dynamic DHCP Servers .....	21
Fig. 12: Example 2 - LAN Configuration Page .....	21
Fig. 13: Example 3 - Network Topology .....	22
Fig. 14: Example 3 - LAN Configuration Page .....	22
Fig. 15: Example 4 - Network Topology for VRRP configuration .....	24
Fig. 16: Example 4 - VRRP configuration of main router .....	24
Fig. 17: Example 4 - VRRP configuration of backup router .....	25
Fig. 18: Cellular WAN configuration .....	26
Fig. 19: Advanced CDMA Administration .....	29
Fig. 20: Example of GPRS configuration 1 .....	33
Fig. 21: Example of GPRS configuration 2 .....	33
Fig. 22: Example of GPRS configuration 3 .....	33
Fig. 23: PPPoE configuration .....	34
Fig. 24: Example 5 - Network Topology for Firewall Application .....	36
Fig. 25: Example 5 - Firewall configuration .....	36
Fig. 26: Example 6 – Network Topology for Basic NAT .....	38
Fig. 27: Example 6 – Basic NAT Configuration .....	38
Fig. 28: Example 7 – Network Topology for Advanced NAT .....	39
Fig. 29: Example 7 – Advanced NAT Configuration .....	39
Fig. 30: OpenVPN tunnel configuration .....	40
Fig. 31: OpenVPN tunnel configuration .....	42
Fig. 32: Topology of example OpenVPN configuration .....	43
Fig. 33: IPsec tunnels configuration .....	44
Fig. 34: IPsec tunnel configuration .....	46
Fig. 35: Example 8 – Network Topology for IPsec Tunneling .....	47
Fig. 36: GRE tunnels configuration .....	48
Fig. 37: GRE tunnel configuration .....	49
Fig. 38: Example 9 – Network Topology for GRE Tunneling .....	49
Fig. 39: L2TP tunnel configuration .....	50
Fig. 40: Example 10 – Network Topology for L2TP Tunneling .....	51
Fig. 41: PPTP tunnel configuration .....	52
Fig. 42: Example 11 – Network Topology for PPTP Tunneling configuration .....	53
Fig. 43: Example of DynDNS configuration .....	54
Fig. 44: Example of NTP configuration .....	55
Fig. 45: Example of SNMP configuration .....	58
Fig. 46: Example of the MIB browser .....	58
Fig. 47: SMTP client configuration .....	59

<b>Fig. 48: SMTP configuration</b> .....	59
<b>Fig. 49: Example of SMS configuration 1</b> .....	64
<b>Fig. 50: Example of SMS configuration 2</b> .....	65
<b>Fig. 51: Example of SMS configuration 3</b> .....	66
<b>Fig. 52: Example of SMS configuration 4</b> .....	67
<b>Fig. 53: Expansion port configuration</b> .....	69
<b>Fig. 54: Example of Ethernet to Serial Communication</b> .....	70
<b>Fig. 55: Example of Serial Port Extension</b> .....	70
<b>Fig. 56: USB configuration</b> .....	72
<b>Fig. 57: Example of Ethernet to Serial using USB Port</b> .....	73
<b>Fig. 58: Example of Serial Extension using USB port</b> .....	73
<b>Fig. 59: Startup script</b> .....	74
<b>Fig. 60: Example of Startup script</b> .....	74
<b>Fig. 61: Up/Down script</b> .....	75
<b>Fig. 62: Example of Up/Down script</b> .....	75
<b>Fig. 63: Example of automatic update 1</b> .....	77
<b>Fig. 64: Example of automatic update 2</b> .....	77
<b>Fig. 65: User modules</b> .....	77
<b>Fig. 66: Change profile</b> .....	78
<b>Fig. 67: Change password</b> .....	78
<b>Fig. 68: Set real time clock</b> .....	79
<b>Fig. 69: Set SMS service center address</b> .....	79
<b>Fig. 70: Unlock SIM card</b> .....	79
<b>Fig. 71: Send SMS</b> .....	80
<b>Fig. 72: Restore configuration</b> .....	80
<b>Fig. 73: Update firmware</b> .....	81
<b>Fig. 74: Reboot</b> .....	81
<b>Fig. 75: Wi-Fi AP Status</b> .....	83
<b>Fig. 76: Wi-Fi DHCP Status</b> .....	84
<b>Fig. 77: Wi-Fi Scan</b> .....	85
<b>Fig. 78: Wi-Fi AP Start Log</b> .....	86
<b>Fig. 79: System Log</b> .....	86
<b>Fig. 80: Wi-Fi AP Configuration Page</b> .....	89
<b>Fig. 81: WLAN Configuration</b> .....	90

## Table List

Table 1: Interface connection status.....	12
Table 2: Description of information in network status .....	12
Table 3: DHCP status description .....	13
Table 4: Description of cellular network information.....	14
Table 5: Description of Time Periods.....	14
Table 6: Description of Cellular statistics.....	14
Table 7: Description of Cellular traffic statistics.....	15
Table 8: DynDNS report .....	16
Table 9: Configuration of network interface .....	18
Table 10: Configuration of a dynamic DHCP server .....	18
Table 11: Configuration of static DHCP server .....	19
Table 12: VRRP configuration .....	23
Table 13: Check PPP connection .....	23
Table 14: GPRS connection configuration .....	28
Table 15: Check PPP connection configuration.....	30
Table 16: Data limit configuration .....	30
Table 17: Default and backup SIM configuration .....	31
Table 18: Switch between SIM card configurations.....	31
Table 19: Switch between SIM card configurations.....	32
Table 20: Dial-In access configuration.....	32
Table 21: PPPoE configuration .....	34
Table 22: Firewall configuration.....	35
Table 23: NAT configuration.....	37
Table 24: Configuration of send all incoming packets .....	37
Table 25: Remote access configuration .....	37
Table 26: Overview of OpenVPN tunnels.....	40
Table 27: OpenVPN configuration.....	41
Table 28: Example OpenVPN configuration .....	43
Table 29: Overview IPsec tunnels .....	44
Table 30: IPsec tunnel configuration .....	45
Table 31: Example 8 – IPsec Configuration.....	47
Table 32: Overview GRE tunnels.....	48
Table 33: GRE tunnel configuration.....	48
Table 34: Example 9 - GRE Tunnel Configuration.....	49
Table 35: L2TP tunnel configuration.....	50
Table 36: Example 10 – L2TP Tunnel Configuration.....	51
Table 37: PPTP tunnel configuration .....	52
Table 38: Example 11 – PPTP Tunnel Configuration .....	53
Table 39: DynDNS configuration.....	54
Table 40: NTP configuration .....	55
Table 41: SNMP configuration.....	56
Table 42: SNMP configuration.....	56
Table 43: Object identifier for binary input and output.....	57
Table 44: Object identifier for CNT port.....	57
Table 45: Send SMS configuration.....	60
Table 46: Control via SMS configuration .....	60
Table 47: SMS Control Commands .....	61



---

Table 48: Send SMS on serial PORT1 configuration.....	61
Table 49: Send SMS on serial PORT2 configuration.....	61
Table 50: Send SMS on Ethernet Port configuration .....	62
Table 51: AT commands to send and receive SMS messages.....	62
Table 52: Expansion PORT configuration .....	68
Table 53: TCP Keep-Alive Configuration .....	68
Table 54: CD signal description .....	69
Table 55: DTR signal description .....	69
Table 56: USB port configuration 1.....	71
Table 57: USB PORT configuration 2.....	71
Table 58: CD signal description .....	71
Table 59: DTR signal description .....	72
Table 60: Automatic update configuration .....	76
Table 61: Telnet commands.....	82
Table 62: Wi-Fi AP State .....	83
Table 63: Wi-Fi Client State.....	83
Table 64: Lease Address .....	84
Table 65: Neighboring Wi-Fi networks.....	85
Table 66: Wi-Fi AP Parameters.....	88
Table 67: WLAN Parameter.....	90
Table 68: Wi-Fi LED State Indication.....	90

# 1. Router Configuration Using a Web Browser

**Attention!** The SPECTRE cellular router will not operate unless the cellular carrier has been correctly configured and the account activated and provisioned for data communications. For UMTS and LTE carriers, a SIM card must be inserted into the router. Do not insert the SIM card when the router is powered up.

You can monitor the status, configuration and administration of the router via the Web interface. To access the router over the web interface, enter `http://xxx.xxx.xxx.xxx` into the URL for the browser where `xxx.xxx.xxx.xxx` is the router IP address. The modem's default IP address is **192.168.1.1**. The default username is "**root**" and the default password is "**root**".

The left side of the web interface displays the menu. You will find links for the Status, Configuration and Administration of the router.

Name and Location displays the router's name, location and SNMP configuration (See SNMP configuration). These fields are user-defined for each router.

For enhanced security, you should change the default password. If the router's default password is set, the menu item "**Change password**" is highlighted in red.

Status	Network Status																																
<ul style="list-style-type: none"> <li>Network</li> <li>DHCP</li> <li>GPRS</li> <li>IPsec</li> <li>DynDNS</li> <li>System Log</li> </ul>	<p><b>Interfaces</b></p> <pre> eth0   Link encap:Ethernet  HWaddr 00:11:22:33:44:55        inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1        RX packets:291 errors:0 dropped:0 overruns:0 frame:0        TX packets:359 errors:0 dropped:0 overruns:0 carrier:0        collisions:0 txqueuelen:32        RX bytes:33455 (32.6 KB)  TX bytes:263711 (257.5 KB)        Interrupt:23  ppp0   Link encap:Point-Point Protocol        inet addr:10.169.80.137  P-t-P:10.0.0.1  Mask:255.255.255.255        UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1        RX packets:4 errors:0 dropped:0 overruns:0 frame:0        TX packets:5 errors:0 dropped:0 overruns:0 carrier:0        collisions:0 txqueuelen:3        RX bytes:102 (102.0 B)  TX bytes:142 (142.0 B) </pre> <p><b>Route Table</b></p> <table border="1"> <thead> <tr> <th>Destination</th> <th>Gateway</th> <th>Genmask</th> <th>Flags</th> <th>Metric</th> <th>Ref</th> <th>Use</th> <th>Iface</th> </tr> </thead> <tbody> <tr> <td>10.0.0.1</td> <td>0.0.0.0</td> <td>255.255.255.255</td> <td>UH</td> <td>0</td> <td>0</td> <td>0</td> <td>ppp0</td> </tr> <tr> <td>192.168.1.0</td> <td>0.0.0.0</td> <td>255.255.255.0</td> <td>U</td> <td>0</td> <td>0</td> <td>0</td> <td>eth0</td> </tr> <tr> <td>0.0.0.0</td> <td>10.0.0.1</td> <td>0.0.0.0</td> <td>UG</td> <td>0</td> <td>0</td> <td>0</td> <td>ppp0</td> </tr> </tbody> </table>	Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface	10.0.0.1	0.0.0.0	255.255.255.255	UH	0	0	0	ppp0	192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0	0.0.0.0	10.0.0.1	0.0.0.0	UG	0	0	0	ppp0
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface																										
10.0.0.1	0.0.0.0	255.255.255.255	UH	0	0	0	ppp0																										
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0																										
0.0.0.0	10.0.0.1	0.0.0.0	UG	0	0	0	ppp0																										
<ul style="list-style-type: none"> <li>Configuration</li> <li>LAN</li> <li>VRRP</li> <li>GPRS</li> <li>Firewall</li> <li>NAT</li> <li>OpenVPN</li> <li>IPsec</li> <li>GRE</li> <li>L2TP</li> <li>DynDNS</li> <li>NTP</li> <li>SNMP</li> <li>SMTP</li> <li>SMS</li> <li>Expansion Port 1</li> <li>Expansion Port 2</li> <li>USB Port</li> <li>Startup Script</li> <li>Up/Down Script</li> <li>Automatic Update</li> </ul>																																	
<ul style="list-style-type: none"> <li>Customization</li> <li>User Modules</li> </ul>																																	
<ul style="list-style-type: none"> <li>Administration</li> <li>Change Profile</li> <li><b>Change Password</b></li> <li>Set Real Time Clock</li> <li>Set SMS Service Center</li> <li>Unlock SIM Card</li> <li>Send SMS</li> <li>Backup Configuration</li> <li>Restore Configuration</li> <li>Update Firmware</li> <li>Reboot</li> </ul>																																	

Fig. 1: Web Configuration

If the green LED is blinking, you may restore the router to its factory default settings by pressing RST on front panel. The configuration will be restored to the factory defaults and the router will reboot. (The green LED will be on during the reboot.)

### **1.1. Secured access to web configuration**

The Web interface can be accessed through a standard web browser via a secure HTTPS connection.

Access the web interface by entering `https://192.168.1.1` in the web browser. You may receive a message that there is a problem with the website's security certificate. If you do, click on "Continue to this website". If you wish to prevent this message, you must install a security certificate into the router.

Since the domain name in the certificate is given the MAC address of the router (such addresses use dashes instead of colons as separators), it is necessary to access the router under this domain name. For access to the router via a domain name, a DNS record must be added to the DNS table in the operating system.

There are three methods to add a domain name to the operating system:

- Editing `/etc/hosts` (Linux/Unix)
- Editing `C:\WINDOWS\system32\drivers\etc\hosts` (Windows XP)
- Configuring your own DNS server

You must then add a security certificate to the web server on the router. When using a self-signed certificate, you must upload your files to the certs directory `/etc/certs` in the router.

## 1.2. Network status

To view the current system information for the router, select the **Network** menu item. The upper part of the window displays detailed information about the active interfaces.

Interface	Description
eth0	Primary Ethernet interface
ppp0	PPP Interface (active connection to GPRS/EDGE/CDMA)
tun0	OpenVPN tunnel interface
ipsec0	IPSec tunnel interface
gre1	GRE tunnel interface

**Table 1: Interface connection status**

The following detailed information will be shown for each active connection.

Item	Description
HWaddr	Hardware MAC (unique) address of primary network interface
inet	IP address of primary network interface
P-t-P	IP address second ends connection
Bcast	Broadcast address
Mask	Network Subnet Mask
MTU	Maximum transmittable packet size
Metric	Number of routers that the packet must pass through
RX	<ul style="list-style-type: none"> <li>• packets – number of received packets</li> <li>• errors - number of errors</li> <li>• dropped - number of dropped packets</li> <li>• overruns – incoming packets lost because of overload</li> <li>• frame – number of frame errors</li> </ul>
TX	<ul style="list-style-type: none"> <li>• packets – number of transmitted packets</li> <li>• errors - number of packet errors</li> <li>• dropped - number of dropped packets</li> <li>• overruns – number of outgoing packets lost because of overload</li> <li>• carrier - outgoing packet errors resulting from the physical layer</li> </ul>
collisions	Number of collisions on physical layer
txqueuelen	Number of packets in the transmit queue
RX bytes	Total number of received bytes
TX bytes	Total number of transmitted bytes

**Table 2: Description of information in network status**

If the PPP connection is active, the system information will appear on the ppp0 interface. For the SPECTRE RT industrial router, interface ppp0 indicates the PPPoE connection.

Network Status						
Interfaces						
eth0	Link encap:Ethernet HWaddr 00:11:22:33:44:55 inet addr:192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:407 errors:0 dropped:0 overruns:0 frame:0 TX packets:461 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:32 RX bytes:51793 (50.5 KB) TX bytes:321807 (314.2 KB) Interrupt:23					
ppp0	Link encap:Point-Point Protocol inet addr:10.169.80.137 P-t-P:10.0.0.1 Mask:255.255.255.255 UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1 RX packets:35 errors:0 dropped:0 overruns:0 frame:0 TX packets:46 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:3 RX bytes:7772 (7.5 KB) TX bytes:8716 (8.5 KB)					
Route Table						
Destination	Gateway	Genmask	Flags	Metric	Ref	Use Iface
10.0.0.1	0.0.0.0	255.255.255.255	UH	0	0	0 ppp0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0 eth0
0.0.0.0	10.0.0.1	0.0.0.0	UG	0	0	0 ppp0

Fig. 2: Network Status

### 1.3. DHCP status

Information about the DHCP server can be accessed by selecting the **DHCP status**. The DHCP server provides automatic configuration of the client devices connected to the router. The DHCP server assigns each device an IP address, subnet mask, default gateway (IP address of router) and DNS server (IP address of router).

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

Item	Description
lease	Assigned IP address
starts	Time that the IP address was assigned
ends	Time that the IP address lease expires
hardware ethernet	Hardware MAC (unique) address
uid	Unique ID
client-hostname	Computer name

Table 3: DHCP status description

DHCP Status	
Active DHCP Leases	
lease 192.168.1.2 {	
starts 1 2011/01/17 08:08:37;	
ends 1 2011/01/17 08:18:37;	
hardware ethernet 00:1d:92:25:72:33;	
uid 01:00:1d:92:25:72:33;	
client-hostname "felgr2";	
}	

Fig. 3: DHCP Status

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

## 1.4. Mobile WAN status



The SPECTRE RT industrial router does not display the **Mobile WAN** status option. The router displays information about the current cellular WAN connection.

Item	Description
PLMN	Code of cellular operator
Cell	The primary cell to which the router is connected
Channel	The channel on which the router is communicating
Level	The signal quality of the primary cell
Neighbors	The signal quality of neighboring cells
Uptime	Current PPP connection time

**Table 4: Description of cellular network information**

If a neighboring cell is highlighted in red, there is a risk that the router may repeatedly switch between the neighboring cell and the primary cell. This can affect the performance of the router. To prevent this, re-orient the antenna or use a directional antenna.

The next section of this window displays historical information about the quality of the cellular WAN connection during each logging period. The router has standard intervals such as the previous 24 hours and last week and also includes information one user-defined interval.

Period	Definition of the period
Today	Today from 0:00 to 23:59
Yesterday	Yesterday from 0:00 to 23:59
This week	This week from 0:00 on Monday to 23:59 on Sunday
Last week	Last week from 0:00 on Monday to 23:59 on Sunday
This period	This accounting period. The interval must be set in the Cellular WAN Configuration
Last period	Last accounting period. The interval must be set in the Cellular WAN Configuration

**Table 5: Description of Time Periods**

Item	Description
Level Min.	Minimum signal strength
Level Avg.	Average signal strength
Level Max.	Maximum signal strength
Cells	Number of times that the router switched between cells
Availability	Availability of the PPP connection in %

**Table 6: Description of Cellular statistics**

Connection Availability is displayed as a percentage and is calculated as the ratio of the time that the PPP connection was active to the router power on time during the interval.

Placing your cursor on the maximum or minimum signal strength will display the most recent signal strength reading.

The middle part of window displays information about the amount of data transferred and the number of times that a PPP connection was established for each SIM card during the period.

Item	Description
RX data	Total volume of received data
TX data	The total volume of data sent
Connections	Number of times that a PPP connection was established

**Table 7: Description of Cellular traffic statistics**

The bottom of the window displays the PPP Connection Log. Check here for information about the status of the PPP connection and any problems with the connection.

GPRS Status						
GSM Information						
PLMN	: 23001					
Cell	: 69A6 (EDGE attached)					
Channel	: 30					
Level	: -77 dBm					
Neighbours	: -79 dBm (80), -84 dBm (57), -92 dBm (59), -93 dBm (58), -98 dBm (108)					
Uptime	: 0 days, 0 hours, 29 minutes					
GSM Statistics						
	Today	Yesterday	This Week	Last Week	This Period	Last Period
Level Min	: -89 dBm	--- dBm	-89 dBm	-91 dBm	-91 dBm	-91 dBm
Level Avg	: -74 dBm	--- dBm	-74 dBm	-74 dBm	-74 dBm	-76 dBm
Level Max	: -67 dBm	2011-05-09 11:15:37	-67 dBm	-67 dBm	-67 dBm	-70 dBm
Cells	: 79	0	79	394	472	506
Availability	: 97.9%	0.0%	97.9%	99.2%	99.1%	99.7%
Traffic Statistics for Primary SIM card						
	Today	Yesterday	This Week	Last Week	This Period	Last Period
Rx Data	: 269 KB	0 KB	269 KB	423 KB	692 KB	206 KB
Tx Data	: 61 KB	0 KB	61 KB	499 KB	560 KB	180 KB
Connections	: 5	0	5	80	85	36
Traffic Statistics for Secondary 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
PPP Connection Log						
2011-05-09 11:49:55 Connection successfully established.						

**Fig. 4: Mobile WAN Status**



### 1.5. IPsec status

Selecting the **IPsec** option in the status menu of the web page will bring up the information for any IPsec Tunnels that have been established. Up to 4 IPsec tunnels can be created. If no IPsec tunnels are configured, the status will show that **“IPsec is disabled”**.

If an IPsec tunnel is established, the router will show **“IPsec SA established”** (highlighted in red) in the IPsec status information.

```

IPsec Status
IPsec Tunnels Information

interface eth0/eth0 192.168.2.250
interface ppp0/ppp0 10.0.0.132
%myid = (none)
debug none

"ipsecl": 192.168.2.0/24===10.0.0.132...10.0.1.228===192.168.1.0/24; erouted; eroute owner: #2
"ipsecl":   myip=unset; hisip=unset; myup=/etc/scripts/updown; hisup=/etc/scripts/updown;
"ipsecl":   ike_life: 3600s; ipsec_life: 3600s; rekey_margin: 540s; rekey_fuzz: 100%; keyingtries: 0
"ipsecl":   policy: PSK+ENCRYPT+TUNNEL+UP; prio: 24,24; interface: ppp0;
"ipsecl":   newest ISAKMP SA: #1; newest IPsec SA: #2;
"ipsecl":   IKE algorithm newest: AES_CBC_128-SHA1-MODP2048

#2: "ipsecl":500 STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in 2708s; newest IPSEC; erout
#2: "ipsecl" esp.d07e3080@10.0.1.228 esp.783...@10.0.1.228 tun.0@10.0.0.132 ref=0 refhim=4294
#1: "ipsecl":500 STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in 2733s; newest ISAKMP; lastdpd=-1s(se
    
```

Fig. 5: IPsec status

### 1.6. DynDNS status

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

```


DynDNS Status
Last DynDNS Update Status

DynDNS record successfully updated.
    
```

Fig. 6: DynDNS status

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 updated.
DNS error encountered.
DynDNS server failure.

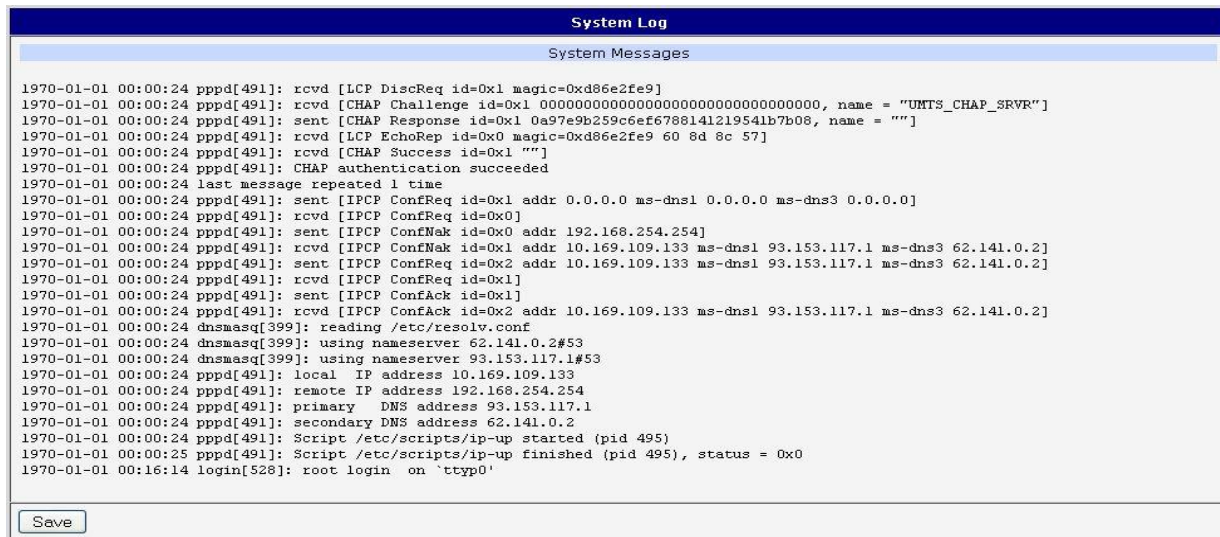
Table 8: DynDNS report

 For Dynamic DNS to function properly, the router's SIM card must have a public IP address assigned.



## 1.7. System log

Use the **System Log** menu item to view the router system log. The system log contains helpful information on the operation of the router. Only the most recent information is shown on the screen but older log entries can be viewed by saving the system log to a file and opening it with a text editor. The **Save** button allows you to save the system log to a file. The system log is cleared when the unit re-boots.



```

System Log
System Messages
1970-01-01 00:00:24 pppd[491]: rcvd [LCP DiscReq id=0x1 magic=0xd86e2fe9]
1970-01-01 00:00:24 pppd[491]: rcvd [CHAP Challenge id=0x1 00000000000000000000000000000000, name = "UMTS_CHAP_SRVR"]
1970-01-01 00:00:24 pppd[491]: sent [CHAP Response id=0x1 0a97e9b259c6e6788141219541b7b08, name = "" ]
1970-01-01 00:00:24 pppd[491]: rcvd [LCP EchoRep id=0x0 magic=0xd86e2fe9 60 8d 8c 57]
1970-01-01 00:00:24 pppd[491]: rcvd [CHAP Success id=0x1 "" ]
1970-01-01 00:00:24 pppd[491]: CHAP authentication succeeded
1970-01-01 00:00:24 last message repeated 1 time
1970-01-01 00:00:24 pppd[491]: sent [IPCP ConfReq id=0x1 addr 0.0.0.0 ms-dns1 0.0.0.0 ms-dns3 0.0.0.0]
1970-01-01 00:00:24 pppd[491]: rcvd [IPCP ConfReq id=0x0]
1970-01-01 00:00:24 pppd[491]: sent [IPCP ConfNak id=0x0 addr 192.168.254.254]
1970-01-01 00:00:24 pppd[491]: rcvd [IPCP ConfNak id=0x1 addr 10.169.109.133 ms-dns1 93.153.117.1 ms-dns3 62.141.0.2]
1970-01-01 00:00:24 pppd[491]: sent [IPCP ConfReq id=0x2 addr 10.169.109.133 ms-dns1 93.153.117.1 ms-dns3 62.141.0.2]
1970-01-01 00:00:24 pppd[491]: rcvd [IPCP ConfReq id=0x1]
1970-01-01 00:00:24 pppd[491]: sent [IPCP ConfAck id=0x1]
1970-01-01 00:00:24 pppd[491]: rcvd [IPCP ConfAck id=0x2 addr 10.169.109.133 ms-dns1 93.153.117.1 ms-dns3 62.141.0.2]
1970-01-01 00:00:24 dnsmasq[399]: reading /etc/resolv.conf
1970-01-01 00:00:24 dnsmasq[399]: using nameserver 62.141.0.2#53
1970-01-01 00:00:24 dnsmasq[399]: using nameserver 93.153.117.1#53
1970-01-01 00:00:24 pppd[491]: local IP address 10.169.109.133
1970-01-01 00:00:24 pppd[491]: remote IP address 192.168.254.254
1970-01-01 00:00:24 pppd[491]: primary DNS address 93.153.117.1
1970-01-01 00:00:24 pppd[491]: secondary DNS address 62.141.0.2
1970-01-01 00:00:24 pppd[491]: Script /etc/scripts/ip-up started (pid 495)
1970-01-01 00:00:25 pppd[491]: Script /etc/scripts/ip-up finished (pid 495), status = 0x0
1970-01-01 00:16:14 login[528]: root login on `tty0'
Save

```

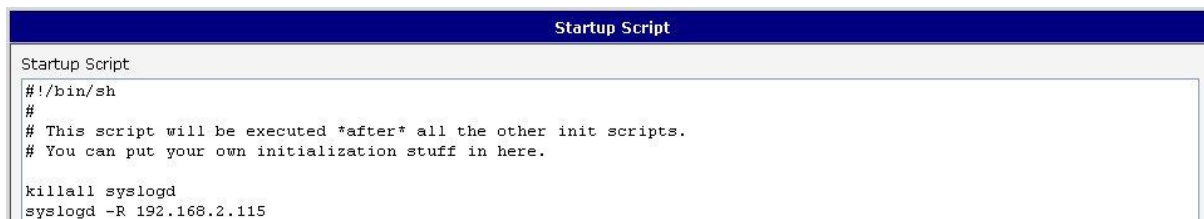
Fig. 7: System log

The Syslog default size is 1000 lines. When the system log reaches the maximum size, it is deleted and a new log file is started.

The program **syslogd** can be run on the router to configure the system log. The **syslogd** option **"-s"** followed by decimal number will set the maximum number of lines in the log file. The **"-r"** option followed by the hostname or IP address will enable logging to a syslog daemon on a remote computer. On remote Linux machines, the syslog daemon is enabled by running **syslogd** with the parameter **"-r"**. On remote Windows machines, a syslog server such as Syslog Watcher must be installed.

To enable remote logging when the router powers up, modify the script **"/etc/init.d/syslog"** or add the commands **"killall syslogd"** and **"syslogd <options>"** into the startup script.

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



```

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

```

Fig. 8: Example **syslogd** startup script with the parameter **-r**

## 1.8. LAN configuration

Select the **LAN** menu item to enter the network configuration for the Ethernet ports. The main Ethernet port, **ETH**, is setup in the **Primary LAN** section. If the router has additional Ethernet ports (**PORT1** or **PORT2**), they are configured under the **Secondary LAN** section. For routers with 2 additional Ethernet ports, **PORT1** and **PORT2** are automatically bridged together.

Item	Description
DHCP Client	<ul style="list-style-type: none"> <li>disabled – The router will not obtain an IP address automatically from a DHCP server on the network.</li> <li>enabled – The router will attempt to obtain an IP address automatically from a DHCP server on the network.</li> </ul>
IP address	Fixed IP address of the network interface.
Subnet Mask	IP address Subnet Mask for the interface.
Media type	<ul style="list-style-type: none"> <li>Auto-negotiation – The router automatically selects the communication speed of the network interface.</li> <li>100 Mbps Full Duplex – The router communicates at 100Mbps, in full-duplex mode.</li> <li>100 Mbps Half Duplex - The router communicates at 100Mbps, in half-duplex mode.</li> <li>10 Mbps Full Duplex - The router communicates at 10Mbps, in full-duplex mode.</li> <li>10 Mbps Half Duplex - The router communicates at 10Mbps, in half-duplex mode.</li> </ul>
Default Gateway	IP address of Default gateway for the router. When entering IP address of default gateway, all packets for which the record was not found in the routing table are sent to this address.
DNS server	IP address of the primary DNS server for the router.

**Table 9: Configuration of network interface**

The DHCP server assigns the IP address, default gateway IP address, and IP address of the DNS server to the connected DHCP clients.

The DHCP server supports both static and dynamic assignment of IP addresses. In Dynamic IP address assignment, the DHCP server will assign a client the next available IP address from the allowed IP address pool. Once the lease time on an IP address has expired, the DHCP server is free to re-assign that IP to another client.

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

**Table 10: Configuration of a dynamic DHCP server**

The DHCP server can also assign a Static IP address to a client. The MAC address of the client must be configured in the MAC address table along with the desired IP address. Up to 6 static IP addresses are supported. Do not overlap the static IP addresses with the addresses

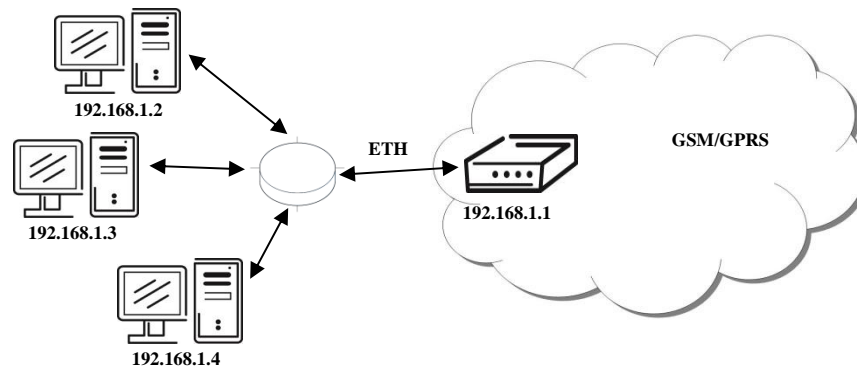
allocated by the dynamic DHCP address pool. Otherwise, incorrect network functioning may occur.

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

**Table 11: Configuration of static DHCP server**

Example of the network interface configuration for a dynamic DHCP server:

- The range of dynamically allocated addresses is from 192.168.1.2 to 192.168.1.4.
- The addresses are allocated for 600 seconds (10 minutes).



**Fig. 9: Example 1 - Network Topology for Dynamic DHCP Server**

LAN Configuration		
	Primary LAN	Secondary LAN
DHCP client	<input type="text" value="disabled"/>	<input type="text" value="disabled"/>
IP Address	<input type="text" value="192.168.1.1"/>	<input type="text"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>	<input type="text"/>
Media Type	<input type="text" value="auto-negotiation"/>	<input type="text" value="auto-negotiation"/>
Default Gateway	<input type="text"/>	
DNS Server	<input type="text"/>	
<input checked="" type="checkbox"/> Enable dynamic DHCP leases		
IP Pool Start	<input type="text" value="192.168.1.2"/>	
IP Pool End	<input type="text" value="192.168.1.4"/>	
Lease Time	<input type="text" value="600"/> sec	
<input type="checkbox"/> Enable static DHCP leases		
MAC Address	IP Address	
<input type="text"/>	<input type="text"/>	
<input type="text"/>	<input type="text"/>	
<input type="text"/>	<input type="text"/>	
<input type="text"/>	<input type="text"/>	
<input type="text"/>	<input type="text"/>	
<input type="text"/>	<input type="text"/>	
<input type="button" value="Apply"/>		

Fig. 10: Example 1 - LAN Configuration Page

Example of the network interface configuration with both dynamic and static DHCP servers:

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

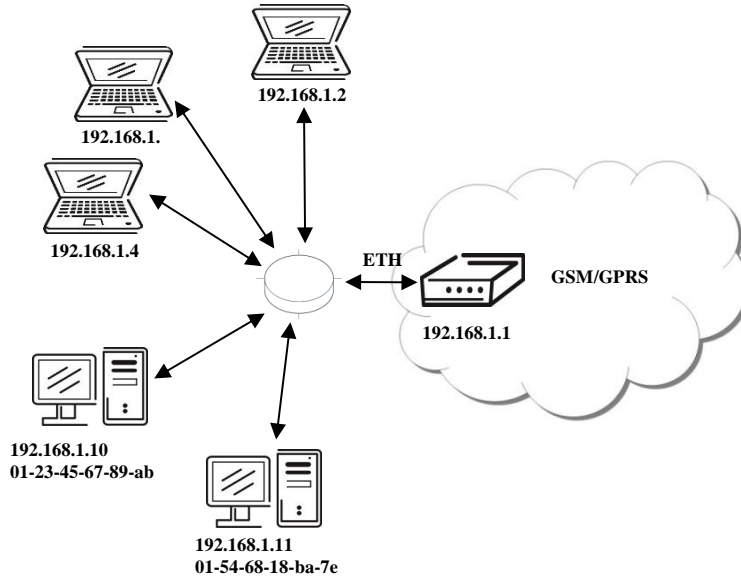


Fig. 11: Example 2 - Network Topology with both Static and Dynamic DHCP Servers

LAN Configuration	
DHCP client	Primary LAN: disabled   Secondary LAN: disabled
IP Address	Primary LAN: 192.168.1.1   Secondary LAN:
Subnet Mask	Primary LAN: 255.255.255.0   Secondary LAN:
Media Type	Primary LAN: auto-negotiation   Secondary LAN: auto-negotiation
Default Gateway	
DNS Server	
<input checked="" type="checkbox"/> Enable dynamic DHCP leases	
IP Pool Start	192.168.1.2
IP Pool End	192.168.1.4
Lease Time	600 sec
<input checked="" type="checkbox"/> Enable static DHCP leases	
MAC Address	IP Address
01:23:45:67:89:ab	192.168.1.10
01:54:68:18:ba:7e	192.168.1.11
<input type="button" value="Apply"/>	

Fig. 12: Example 2 - LAN Configuration Page

Example of the network interface configuration with default gateway and DNS server:

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

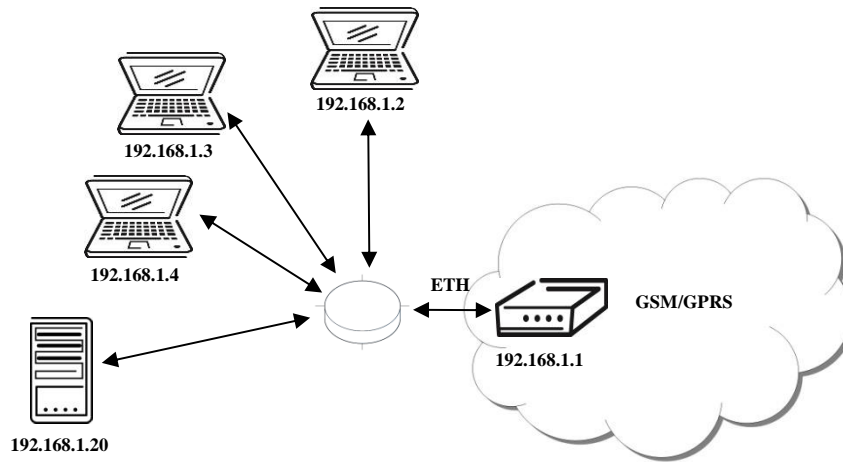


Fig. 13: Example 3 - Network Topology

LAN Configuration		
DHCP client	Primary LAN disabled	Secondary LAN disabled
IP Address	192.168.1.1	
Subnet Mask	255.255.255.0	
Media Type	auto-negotiation	auto-negotiation
Default Gateway	192.168.1.20	
DNS Server	192.168.1.20	
<input checked="" type="checkbox"/> Enable dynamic DHCP leases		
IP Pool Start	192.168.1.2	
IP Pool End	192.168.1.4	
Lease Time	600 sec	
<input type="checkbox"/> Enable static DHCP leases		
MAC Address	IP Address	
Apply		

Fig. 14: Example 3 - LAN Configuration Page

## 1.9. VRRP configuration

Select the **VRRP** menu item to enter the VRRP configuration. 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 application. If the **Enable VRRP** is checked, you may set the following parameters.

Item	Description
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 <i>Host Priority</i> , 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 12: VRRP configuration

You may set the **Check PPP connection** flag in the second part of the window to enable automatic test messages for the cellular network. In some cases, the PPP 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.

Item	Description
Ping IP Address	Destination IP address for the Ping commands.
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 13: Check PPP connection

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 PPP connection using standard Ping commands.

Example of the VRRP protocol:

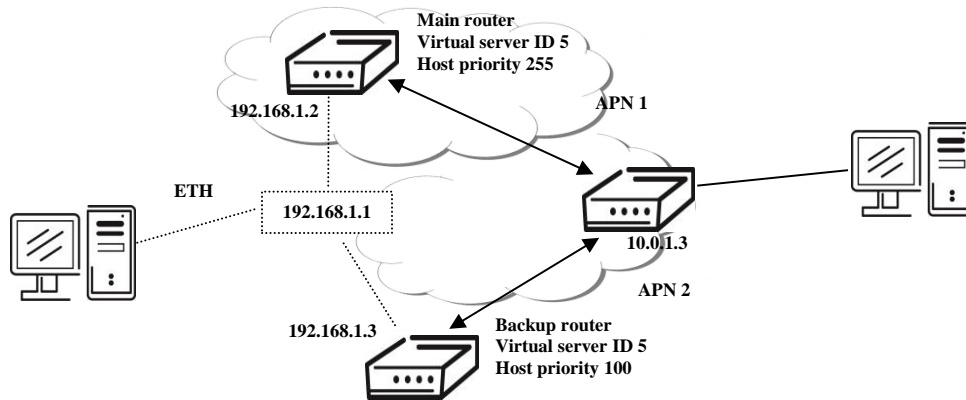


Fig. 15: Example 4 - Network Topology for VRRP configuration

VRRP Configuration	
<input checked="" type="checkbox"/> Enable VRRP	
Virtual Server IP Address	<input type="text" value="192.168.1.1"/>
Virtual Server ID	<input type="text" value="5"/>
Host Priority	<input type="text" value="255"/>
<hr/>	
<input checked="" type="checkbox"/> Check PPP connection	
Ping IP Address	<input type="text" value="10.0.1.3"/>
Ping Interval	<input type="text" value="10"/> sec
Ping Timeout	<input type="text" value="5"/> sec
Ping Probes	<input type="text" value="10"/>
<hr/>	
<input type="checkbox"/> Enable traffic monitoring	
<input type="button" value="Apply"/>	

Fig. 16: Example 4 - VRRP configuration of main router



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

**Fig. 17: Example 4 - VRRP configuration of backup router**

### 1.10. Mobile WAN configuration



The SPECTRE RT industrial router does not display the **Mobile WAN** Configuration option.

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

UMTS/GPRS Configuration			
<input checked="" type="checkbox"/> Create PPP connection			
	Primary SIM card	Secondary SIM card	
APN *	<input type="text"/>	<input type="text"/>	
Username *	<input type="text"/>	<input type="text"/>	
Password *	<input type="text"/>	<input type="text"/>	
Authentication	<input type="text" value="PAP or CHAP"/> ▼	<input type="text" value="PAP or CHAP"/> ▼	
IP Address *	<input type="text"/>	<input type="text"/>	
Phone 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
<input checked="" type="checkbox"/> Get DNS addresses from operator			
<input type="checkbox"/> Check PPP connection ( <i>necessary for uninterrupted operation</i> )			
Ping IP Address	<input type="text"/>	<input type="text"/>	
Ping Interval	<input type="text"/>	<input type="text"/>	sec
<input type="checkbox"/> Enable traffic monitoring			
Data Limit	<input type="text"/>		MB
Warning Threshold	<input type="text"/>		%
Accounting Start	<input type="text" value="1"/>		
Default SIM card	<input type="text" value="primary"/> ▼		
Backup SIM card	<input type="text" value="secondary"/> ▼		
<input type="checkbox"/> Switch to other SIM card when connection fails			
<input type="checkbox"/> Switch to backup SIM card when roaming is detected			
<input type="checkbox"/> Switch to backup SIM card when data limit is exceeded			
<input type="checkbox"/> Switch to backup SIM card when binary input is active			
<input type="checkbox"/> Switch to primary SIM card after timeout			
Initial Timeout	<input type="text" value="60"/>		min
Subsequent Timeout *	<input type="text"/>		min
Additive Constant *	<input type="text"/>		min
<input type="checkbox"/> Enable Dial-In access			
Username *	<input type="text"/>		
Password *	<input type="text"/>		
<input type="checkbox"/> Enable PPPoE bridge mode			
* can be blank			
<input type="button" value="Apply"/>			

Fig. 18: Cellular WAN configuration

### 1.10.1. Cellular Carrier Selection

The SPECTRE 3G Cellular Router can be configured to communicate on up to 2 UMTS or CDMA cellular networks. This allows the router to switch to a second carrier network if there is a problem with the primary network. The router can only communicate on one cellular network at a time and if redundancy is not required, then only one account needs to be activated. For GSM/UMTS networks, the account information will be on the SIM card provided by the carrier. For CDMA networks, the account is provisioned over-the-air by the network provider and a SIM card is not required. The Mobile Equipment Identifier (MEID) of the router must be provided to the CDMA network cellular carrier when the account is set up.

The primary and secondary cellular carriers are selected using the drop-down lists on the Cellular WAN configuration page under the Primary and Secondary SIM card headings. The router supports AT&T, Verizon, Sprint, T-Mobile, and Rogers Cellular networks. Verizon and Sprint have CDMA networks and the others are GSM networks. The default carrier is set to a generic UMTS provider. Refer to Section 1.10.3 for activating the router on the Sprint CDMA network.



**The carrier selection drop-down list is not available on LTE devices. For LTE devices, the carrier must be specified when ordering the router and the account settings will be on the SIM card provided by the network operator.**

### 1.10.2. GSM/UMTS connection

If the **Create PPP connection** option is selected, the router will automatically try to establish a PPP connection after power up. If the attempt is unsuccessful, the router will re-boot and try again. For GSM/UMTS networks, the following network information can be configured. In most cases, the necessary information will be included on the SIM card provided by the carrier and these fields can be left empty or at their default values. Please contact your cellular network provider for more information.

Item	Description
APN	Network identifier (Access Point Name)
Username	User name to log into the GSM network.
Password	Password to log into the GSM network.
Authentication	Authentication protocol in GSM network <ul style="list-style-type: none"> <li>• PAP or CHAP – Router is chose either authentication method.</li> <li>• PAP – Router will use PAP authentication.</li> <li>• CHAP – Router will use CHAP authentication.</li> </ul>
IP Address	IP address of SIM card. (Required if a static IP address was assigned by the cellular carrier.)
Phone Number	Telephone number to dial a GPRS or CSD connection. Router uses *99***1 # as the default telephone number.

Operator	PLNM code for the network operator
Network type	<ul style="list-style-type: none"> <li>• Automatic selection – The router will automatically select the network type</li> <li>• Depending upon the type of router, it is also possible to select a specific method of data transmission (GPRS, EDGE, UMTS ...).</li> </ul>
PIN	PIN code for the SIM card. (Only required if the SIM card has been locked with a PIN to prevent unauthorized access)
MRU	(Maximum Receiving Unit) – The maximum packet size that can be received in a given environment. Default value is 1500 bytes. Other settings may cause incorrect transmission of data.
MTU	(Maximum Transmission Unit) – The maximum packet size that can be transmitted in a given environment. Default value is 1500 bytes. Other settings may cause incorrect transmission of data.

**Table 14: GPRS connection configuration**

If the **IP address** field is not filled in, the network operator will automatically assign an IP address when the connection is established. If a static IP address is supplied by the operator, the time required to connect to the network will be reduced.

If the **APN** field is not filled in, the router will automatically select the APN based on the IMSI code of the SIM card. If the PLMN of the cellular carrier is not in the APN list, then default APN is "internet". Contact your mobile operator to determine if the APN information must be entered.



**Access to the SIM card may be blocked if the PIN code for a locked SIM is entered incorrectly. Contact technical support if your SIM card becomes blocked.**



**If only one SIM card is installed in the router, the router switches between the APNs on the SIM card. A router with two SIM cards switches between SIM cards.**



**The items marked with an "\*" should only be entered if they are required by the cellular network operator. If the router is unable to establish a PPP connection, verify that the network settings have been entered correctly. You may also try a different authentication method or network type.**

### 1.10.3. Sprint CDMA network connection

The SPECTRE 3G router must be manually activated on the Sprint network using the web interface after the account has been set up by Sprint.

To activate the router on the Sprint network:

1. Ensure that a data account has been set up by Sprint. You will need to provide the **MEID** of the router to the Sprint account rep. This number can be found on the label on the bottom of the router and on the outside of the router package. It can also be found on the **Mobile WAN** status web page when Sprint is selected as the primary carrier.
2. Connect the antennas and Ethernet cable to the router and power up the device.
3. Select Sprint as the primary carrier on the **Mobile WAN** configuration web page. This will enable the **CDMA Administration** menu item.
4. Bring up the Advanced CDMA Administration web page by clicking on the **CDMA** menu item under **Administration**.
5. Click on the **Activate Device** button to perform the over-the-air device activation. When it is complete, you can view the Mobile Device Number (MDN) on the **Mobile WAN** status page.
6. If the activation fails, verify that the antenna connections are tight and that the correct MEID has been set up on the Sprint network.

The screenshot displays the web interface for a SPECTRE 3G UMTS/CDMA Router. The main content area is titled "Advanced CDMA Administration" and contains the following sections:

- One-Touch OTA Provisioning:** Includes an "Activate Device" button.
- Client-Initiated Device Configuration (CIDC):** Includes an "Update Profile" button.
- Client-Initiated Preferred Roaming List (CIPRL):** Includes an "Update PRL" button.
- Reset Cellular Module to Factory Defaults:** Includes a "Reset Module" button.

The left sidebar menu is organized into several categories:

- Status:** Network, DHCP, Mobile WAN, IPsec, DynDNS, System Log.
- Configuration:** LAN, VRRP, Mobile WAN, Firewall, NAT, OpenVPN, IPsec, GRE, LZTP, PPTP, DynDNS, NTP, SNMP, SMTP, SMS, Expansion Port 1, Expansion Port 2, USB Port, Startup Script, Up/Down Script, Automatic Update.
- Customization:** User Modules.
- Administration:** Change Profile, Change Password, CDMA, Set Real Time Clock, Set SMS Service Center, Unlock SIM Card, Send SMS, Backup Configuration, Restore Configuration, Update Firmware, Reboot.

Fig. 19: Advanced CDMA Administration

#### 1.10.4. DNS address configuration

If **Get DNS address from operator** option is selected, the router will automatically attempt to get the IP addresses for the primary and secondary DNS servers from the cellular network operator.

#### 1.10.5. Check PPP connection configuration

You may set the **Check PPP connection** flag to enable automatic test messages for the cellular network. In some cases, the PPP connection may still be active but the router will not be able to send data over the cellular network. The router will send a Ping command to the **Ping IP Address** at periodic time intervals (**Ping Interval**) 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.

Item	Description
<i>Ping IP Address</i>	Destination IP address or domain name for the ping queries.
<i>Ping Interval</i>	Time intervals between the outgoing pings.

Table 15: Check PPP connection configuration

If the **Enable Traffic Monitoring** option is selected, the router stops sending ping questions to the *Ping IP Address* and it will watch traffic in PPP connection. If PPP connection is without traffic longer than the *Ping Interval*, then the router sends ping questions to the *Ping IP Address*.



**Note:** It is recommended that you enable **Check PPP Connection** to ensure reliable data communication.

#### 1.10.6. Data limit configuration

The router can be configured to automatically send an SMS message or switch to a backup SIM card if the amount of data sent or received exceeds a given threshold for the monthly billing period.

Item	Description
Data limit	With this parameter, you can set the maximum expected amount of data transmitted (sent and received) over the cellular network in one billing period (month).
Warning Threshold	Percentage of <b>Data Limit</b> (50% to 99%). The router will send an SMS message with <b>Router has exceeded (value of Warning Threshold) of data limit</b> in the message text when this threshold is exceeded.
Accounting Start	Sets the day of the month in which the billing cycle starts for the SIM card being used. The start of the billing period is determined by the network operator.

Table 16: Data limit configuration

If neither one of the options **Switch to backup SIM card when data limit is exceeded** (see next) or **Send SMS when data limit is exceeded** (see SMS configuration) is selected, the data limit will be ignored.

### 1.10.7. Switching between SIM cards or networks

You may define rules in the router for switching between two APNs on one SIM card or between two SIM cards or network providers. The router can automatically switch between the network setups when the active PPP connection is lost, the data limit is exceeded, or the binary input on the front panel goes active.

Item	Description
Default SIM card	This parameter sets the default APN or SIM card for the PPP connection. If this parameter is set to <i>none</i> , the router boots up in off-line mode and it will be necessary to initiate the PPP connection by sending an SMS message to the router.
Backup SIM card	Defines the backup APN or SIM card.

**Table 17: Default and backup SIM configuration**

If parameter Backup SIM card is set to *none*, then the parameters ***Switch to other SIM card when connection fails***, ***Switch to backup SIM card when roaming is detected*** and ***Switch to backup SIM card when data limit is exceeded*** will switch the router to off-line mode.

Item	Description
Switch to other SIM card when connection fails	If the PPP connection fails, the router will switch to the secondary SIM card or secondary APN of the SIM card. The router will switch to the backup SIM card if the router is unable to establish a PPP connection after 3 attempts or the <b><i>Check the PPP connection</i></b> option is selected and the router detects that the PPP connection has failed.
Switch to backup SIM card when roaming is detected	If roaming is detected, this option forces the router to switch to the secondary SIM card or secondary APN of the SIM card.
Switch to backup SIM card when data limit is exceeded	This option enables the router to switch to the secondary SIM card or secondary APN of the SIM card when the data limit of default APN is exceeded.
Switch to backup SIM card when binary input is active	This parameter forces the router to switch to the secondary SIM card or secondary APN of the SIM card when binary input ' <i>bin0</i> ' is active.
Switch to primary SIM card after timeout	This parameter defines the method the router will use to try to switch back to the default SIM card or default APN.

**Table 18: Switch between SIM card configurations**

The following parameters define the amount of time that must elapse before the router will attempt to go back to the default SIM card or APN.

Item	Description
Initial timeout	The first attempt to switch back to the primary SIM card or APN shall be made after the time defined in the parameter Initial Timeout. The range of this parameter is from 1 to 10000 minutes.
Subsequent Timeout	After an unsuccessful attempt to switch to the default SIM card, the router will make a second attempt after the amount of time defined in the parameter Subsequent Timeout. The range is from 1 to 10000 minutes.
Additive constant	Any further attempts to switch back to the primary SIM card or APN shall be made after a timeout computed as the sum of the previous timeout period and the time defined in the parameter <i>Additive constants</i> . The range is from 1 to 10000 minutes.

**Table 19: Switch between SIM card configurations**

**Example:** Option **Switch to primary SIM card after timeout** is checked and the parameters are set as follows: **Initial Timeout** = 60 min. **Subsequent Timeout** = 30 min. **Additive Constant** = 20 min.

The first attempt to switch back to the primary SIM card or APN shall be carried out after 60 minutes. The second attempt will be made 30 minutes later. The third attempt will be made after 50 minutes (30+20). The fourth attempt will be made after 70 minutes (30+20+20).

### 1.10.8. Dial-in Access

The router can be accessed over a CSD connection by using the **Enable Dial-In Access** feature. The router will require a **Username** and **Password** if the fields are not blank. If this feature is enabled, the router will wait 2 minutes for an incoming CSD connection after a PPP connection attempt fails. If there are no connection attempts after this time, the router will try again to establish a PPP connection.

Item	Description
Username	User name for secured Dial-In access.
Password	Password for secured Dial-In access.

**Table 20: Dial-In access configuration**

### 1.10.9. PPPoE bridge mode configuration

If the **Enable PPPoE bridge mode** option is selected, the router will activate 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. This feature allows a device connected to the ETH port of the router to create a PPP connection with the cellular network.



A configuration example for checking the PPP connection is shown in Figure 19. The router will monitor the traffic over the PPP connection. When the router is using SIM card 1, it will ping address 8.8.8.8 if there is no receive traffic on the PPP connection for 60s. If the router is using the secondary SIM card, it will ping [www.google.com](http://www.google.com) after 80 seconds of inactivity on the PPP link.

<input checked="" type="checkbox"/> Check PPP connection ( <i>necessary for uninterrupted operation</i> )		
Ping IP Address	<input type="text" value="8.8.8.8"/>	<input type="text" value="www.google.com"/>
Ping Interval	<input type="text" value="60"/>	<input type="text" value="80"/> sec
<input checked="" type="checkbox"/> Enable traffic monitoring		

**Fig. 20: Example of GPRS configuration 1**

Figure 20 shows an example of how to configure the router to automatically switch to the backup SIM card when it exceeds the data limit of 800MB in the billing period. It will send out a warning SMS message when 400MB of data have been transmitted. The billing period begins on the 18th day of the month.

Data Limit	<input type="text" value="800"/>	MB
Warning Threshold	<input type="text" value="50"/>	%
Accounting Start	<input type="text" value="18"/>	
Default SIM card	<input type="text" value="primary"/>	
Backup SIM card	<input type="text" value="secondary"/>	
<input type="checkbox"/> Switch to other SIM card when connection fails		
<input type="checkbox"/> Switch to backup SIM card when roaming is detected		
<input checked="" type="checkbox"/> Switch to backup SIM card when data limit is exceeded		
<input type="checkbox"/> Switch to backup SIM card when binary input is active		
<input type="checkbox"/> Switch to primary SIM card after timeout		
Initial Timeout	<input type="text" value="60"/>	min
Subsequent Timeout *	<input type="text"/>	min
Additive Constant *	<input type="text"/>	min

**Fig. 21: Example of GPRS configuration 2**

Example: Configuring the router to switch to offline mode when it detects that it is roaming. The first attempt to switch back to the default SIM card is made after 60 minutes, the second after 40 minutes, the third after 50 minutes (40 +10)...

Default SIM card	<input type="text" value="primary"/>	
Backup SIM card	<input type="text" value="none"/>	
<input type="checkbox"/> Switch to other SIM card when connection fails		
<input checked="" type="checkbox"/> Switch to backup SIM card when roaming is detected		
<input type="checkbox"/> Switch to backup SIM card when data limit is exceeded		
<input type="checkbox"/> Switch to backup SIM card when binary input is active		
<input checked="" type="checkbox"/> Switch to primary SIM card after timeout		
Initial Timeout	<input type="text" value="60"/>	min
Subsequent Timeout *	<input type="text" value="40"/>	min
Additive Constant *	<input type="text" value="10"/>	min

**Fig. 22: Example of GPRS configuration 3**

## 1.11. PPPoE configuration



The SPECTRE cellular router does not support the PPPoE configuration option.

PPPoE (Point-to-Point over Ethernet) is a network protocol where PPP frames are encapsulated in Ethernet frames. The PPPoE feature in the SPECTRE RT industrial router operates in client mode. The router will connect to a PPPoE server or a PPPoE bridge device such as an ADSL modem.

To enter the PPPoE configuration, select the **PPPoE** menu item. If the **Create PPPoE connection** option is selected, the router will attempt to establish a PPPoE connection on power up. The PPPoE client will connect to devices that support either a PPPoE bridge or a PPPoE server. After a PPPoE connection is established, the router obtains the IP address of the PPPoE Server device and all communications from the device are forwarded to the industrial router.

Item	Description
Username	Username for secure access to PPPoE
Password	Password for secure access to PPPoE
Authentication	Authentication protocol in GSM network <ul style="list-style-type: none"> <li>• PAP or CHAP – Router is chosen one of the authentication methods.</li> <li>• PAP – It is used PAP authentication method.</li> <li>• CHAP – It is used CHAP authentication method.</li> </ul>
MRU	(Maximum Receiving Unit) – The maximum packet size that can be received in the given environment. Default value is set to 1492 bytes. Other settings may cause incorrect data transmission.
MTU	(Maximum Transmission Unit) – The maximum packet size that can be transmitted in the given environment. Default value is set to 1492 bytes. Other settings may cause incorrect data transmission

Table 21: PPPoE configuration

Fig. 23: PPPoE configuration

## 1.12. Firewall configuration

The router firewall can be configured to only allow certain hosts to access the router and internal LAN network or it can only allow traffic on a certain IP port to pass through to the internal network. Up to 8 filters can be defined when the **Allow remote access only from specified hosts** option is selected. The following parameters can be defined for each filter: *Source*, *Source IP Address*, *Protocol* and *Target Port*.

Item	Description
Source	<ul style="list-style-type: none"> <li>single address – allows access to only the specific IP address defined in the Source IP Address</li> <li>any address – allowed access to any IP address</li> </ul>
Source IP address	Host IP address that is allowed to access the router.
Protocol	Protocols allowed for remote access <ul style="list-style-type: none"> <li>all – access is allowed by all</li> <li>TCP – access is allowed by TCP</li> <li>UDP - access is allowed by UDP</li> <li>ICMP access is allowed by ICMP</li> </ul>
Target Port	The port number for forwarding to the internal network.

**Table 22: Firewall configuration**

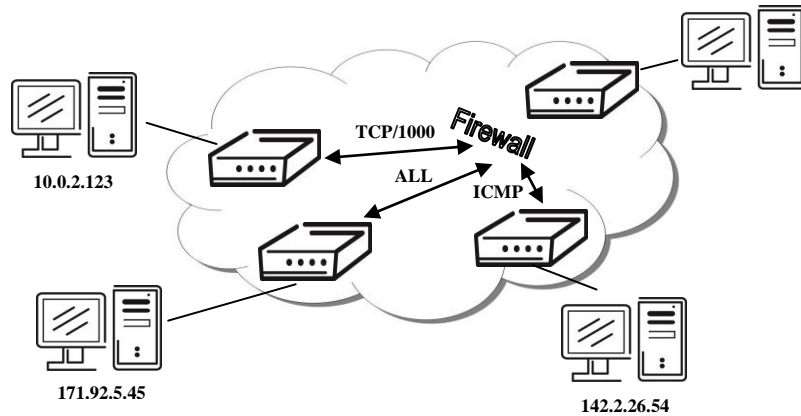


**Caution! The firewall does not filter traffic received over the Ethernet ports.**

**Example firewall configuration:**

The router has allowed the following access:

- from host address 171.92.5.45 using any protocol
- from host address 10.0.2.123 using TCP protocol on any ports
- from host address 142.2.26.54 using ICMP protocol



**Fig. 24: Example 5 - Network Topology for Firewall Application**

Firewall Configuration			
<input checked="" type="checkbox"/> Allow remote access only from specified hosts			
Source	Source IP Address *	Protocol	Target Port *
single address	171.92.5.45	all	
single address	10.0.2.123	TCP	1000
single address	142.2.26.54	ICMP	
single address		all	
single address		all	
single address		all	
single address		all	
single address		all	
* can be blank			
<input type="button" value="Apply"/>			

**Fig. 25: Example 5 - Firewall configuration**

### 1.13. NAT configuration

NAT (Network address Translation / Port address Translation - PAT) is a method of sharing a single external IP address among many internal hosts. It also helps prevent unauthorized access to the internal network. To enter the Network Address Translation configuration, select the **NAT** menu item. Up to sixteen NAT rules may be defined.

Item	Description
Public Port	Public port
Private Port	Private port
Type	Protocol selection
Server IP address	IP address which will be forwarded incoming data.

**Table 23: NAT configuration**

If you need to setup more than 16 NAT rules, insert the following statement into the startup script:

```
iptables -t nat -A napt -p tcp --dport [PORT_PUBLIC] -j DNAT --to-destination [IPADDR]:[PORT1_PRIVATE]
```

The IP address parameter [IPADDR] and port parameters [PORT\_PUBLIC] and [PORT1\_PRIVATE] must be filled in with the desired information.

The following option can be used to route all incoming traffic from the PPP to a single internal host address.

Item	Description
Send all incoming packets to default server	Select this item to route all traffic received over the PPP connection to a single IP address on the internal network.
Default Server	Send all incoming packets to this IP address.

**Table 24: Configuration of send all incoming packets**

You can also specify which ports to use for access to the router using common protocols. In most cases, the default port for each protocol should not be changed.

Item	Description
Enable remote HTTP access on port	Select this option to allow access to the router using HTTP.
Enable remote HTTPS access on port	Select this option to allow access to the router using HTTPS.
Enable remote FTP access on port	Select this option to allow access to the router using FTP.
Enable remote SSH access on port	Select this option to allow access to the router using SSH.
Enable remote Telnet access on port	Select this option to allow access to the router using Telnet.
Enable remote SNMP access on port	Select this option to allow access to the router using SNMP.
Masquerade outgoing packets	Select this option to turn on NAT.

**Table 25: Remote access configuration**





## 1.14. OpenVPN tunnel configuration

Select the **OpenVPN** item in the menu to configure an OpenVPN tunnel. OpenVPN is a protocol which is used to create a secure connection between two LANs. Up to 2 OpenVPN tunnels may be created.

Item	Description
Create	Enables the individual tunnels.
Description	Displays the name of the tunnel specified in the configuration of the tunnel.
Edit	Select to configure an OpenVPN tunnel.

**Table 26: Overview of OpenVPN tunnels**

**Fig. 30: OpenVPN tunnel configuration**

Item	Description
Description	Description of tunnel.
Protocol	Protocol by which the tunnel will communicate. <ul style="list-style-type: none"> <li>• <b>UDP</b> – OpenVPN will communicate using UDP.</li> <li>• <b>TCP server</b> – OpenVPN will communicate using TCP in server mode.</li> <li>• <b>TCP client</b> – OpenVPN will communicate using TCP in client mode.</li> </ul>
UDP/TCP port	Port by which the tunnel will communicate.
Remote IP Address	IP address of the opposite side of the tunnel. Can be used domain name.
Remote Subnet	Network IP address of the opposite side of the tunnel.
Remote Subnet Mask	Subnet mask of the opposite side of the tunnel.
Redirect Gateway	It is possible to redirect all traffic on Ethernet.
Local Interface IP Address	IP address of the local side of tunnel.
Remote Interface IP Address	IP address of interface local side of tunnel.
Ping Interval	Parameter (in seconds) defines how often the router will send a message to the remote end to verify that the tunnel is still connected.
Ping Timeout	Parameter which defines how long the router will wait for a response to the ping (in seconds). <b>Ping Timeout</b> must be larger than <b>Ping Interval</b> .



Renegotiate Interval	Parameter sets the renegotiation period (reauthorization) for the OpenVPN tunnel. After this time period, the router will re-establish the tunnel to ensure the continued security of the tunnel.
Max Fragment Size	Defines maximum packet size.
Compression	<ul style="list-style-type: none"> <li>• <b>none</b> – No compression is used.</li> <li>• <b>LZO</b> – Lossless LZO compression. Compression has to be selected on both tunnel ends.</li> </ul>
NAT Rules	<ul style="list-style-type: none"> <li>• <b>not applied</b> – NAT rules are not applied to OpenVPN tunnel.</li> <li>• <b>applied</b> – NAT rules are not applied to OpenVPN tunnel.</li> </ul>
Authenticate Mode	<ul style="list-style-type: none"> <li>• <b>none</b> – is used any authentication mode</li> <li>• <b>Pre-shared secret</b> – enables authentication using pre-shared secret keys. Both sides of the tunnel must use the same key</li> <li>• <b>Username/password</b> – enables authentication using CA Certificate, Username and Password</li> <li>• <b>X.509 Certificate (multiclient)</b> – enables authentication by CA Certificate, Local Certificate and Local Private Key</li> <li>• <b>X.509 Certificate (client)</b> – enables authentication by CA Certificate, Local Certificate and Local Private Key</li> <li>• <b>X.509 Certificate (server)</b> - enables authentication by CA Certificate, Local Certificate and Local Private Key</li> </ul>
Pre-shared Secret	Authentication using Pre-shared secret keys can be used in all authentication modes.
CA Certificate	This authentication certificate can be used in authentication mode Username/password and X.509 certificate.
DH Parameters	DH parameters can be used in authentication mode X.509 server.
Local Certificate	This authentication certificate can be used in authentication mode X.509 certificate.
Local Private Key	Local private key can be used in authentication mode X.509 certificate.
Username	Authentication using a login name and password authentication can be used in the Authenticate Mode Username/Password.
Password	
Extra Options	Use parameter <i>Extra Options</i> to define additional parameters of the OpenVPN tunnel, for example DHCP options etc.

**Table 27: OpenVPN configuration**

Press the **Apply** button to apply the changes.

OpenVPN Tunnel Configuration

Create 1st OpenVPN tunnel

Description \*

Protocol

UDP port

Remote IP Address \*

Remote Subnet \*

Remote Subnet Mask \*

Redirect Gateway

Local Interface IP Address

Remote Interface IP Address

Ping Interval \*  sec

Ping Timeout \*  sec

Renegotiate Interval \*  sec

Max Fragment Size \*  bytes

Compression

NAT Rules

Authenticate Mode

Pre-shared Secret

CA Certificate

DH Parameters

Local Certificate

Local Private Key

Username

Password

Extra Options \*

*\* can be blank*

**Fig. 31: OpenVPN tunnel configuration**

Example of the OpenVPN tunnel configuration:

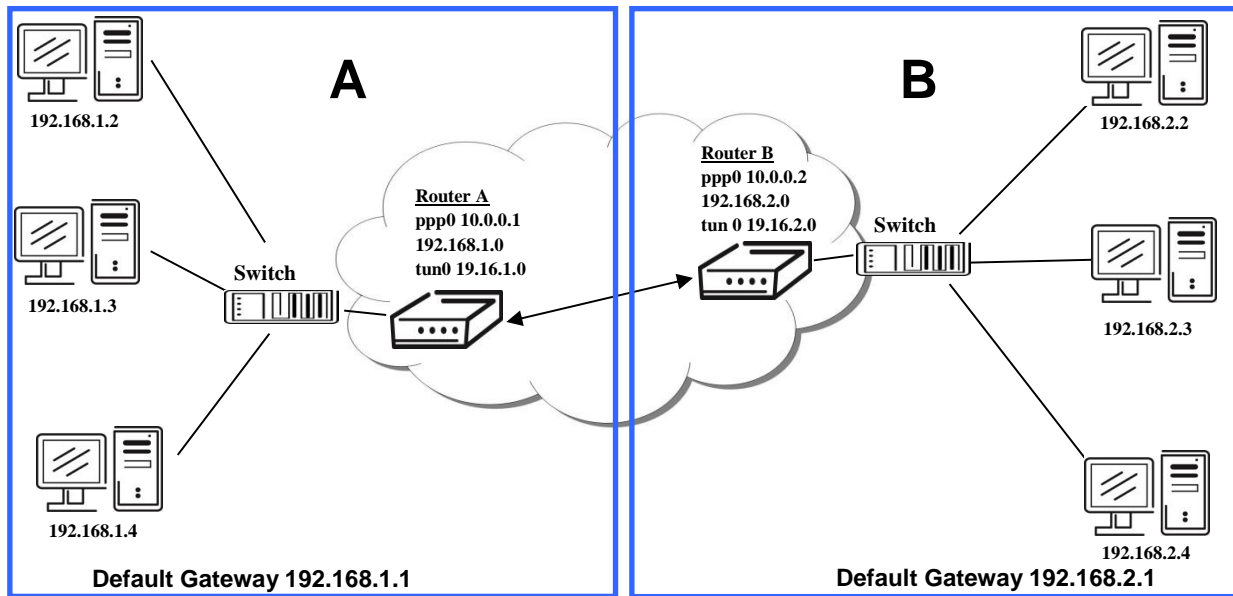


Fig. 32: Topology of example OpenVPN configuration

OpenVPN tunnel configuration:

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

Table 28: Example OpenVPN configuration

Examples of different options for configuration and authentication of OpenVPN can be found in the OpenVPN tunnel configuration manual.

## 1.15. IPsec tunnel configuration

Select the **IPsec** item in the menu to configure an IPsec tunnel. IPsec is a protocol which is used to create a secure connection between two LANs. Up to 4 **IPsec** tunnels may be created.

Item	Description
Create	This item enables the individual tunnels.
Description	This item displays the name of the tunnel specified in the configuration of the tunnel.
Edit	Select to configure an IPsec tunnel.

Table 29: Overview IPsec tunnels

IPsec Tunnels Configuration	
Create	Description
1st no	<input type="text"/> Edit
2nd no	<input type="text"/> Edit
3rd no	<input type="text"/> Edit
4th no	<input type="text"/> Edit

Apply

Fig. 33: IPsec tunnels configuration

Item	Description
Description	Description of tunnel.
Remote IP Address	IP address or domain name of the remote host.
Remote ID	Identification of remote host. The ID contains two parts: a <i>hostname</i> and a <i>domain-name</i> .
Remote Subnet	Remote Subnet address
Remote Subnet Mask	Remote Subnet mask
Local ID	Identification of local host. The ID contains two parts: a <i>hostname</i> and a <i>domain-name</i> .
Local Subnet	Local subnet address
Local subnet mask	Local subnet mask
Key Lifetime	Lifetime key data part of tunnel. The minimum value of this parameter is 60s. The maximum value is 86400 s.
IKE Lifetime	Lifetime key service part of tunnel. The minimum value of this parameter is 60s. The maximum value is 86400 s.
Rekey Margin	Specifies the amount of time before the connection will be re-established. The maximum value must be less than half of the parameters IKE and Key Lifetime.
Rekey Fuzz	Specifies the maximum percentage by which the Rekey Margin should be randomly increased to randomize re-keying intervals
DPD Delay	Defines time after which IPsec tunnel verification occurs
DPD Timeout	Defines the timeout (in seconds) for a DPD response.
NAT traversal	If address translation between two end points of the IPsec tunnel is used, it needs to allow NAT Traversal
Aggressive mode	If this parameter is enabled, the IPsec tunnel will be connected faster, but encryption will set permanently on 3DES-MD5.
Authenticate Mode	Defines the authentication mode: <ul style="list-style-type: none"> <li>• <b>Pre-shared key</b> - shared key for both sides.</li> <li>• <b>X.509 Certificate</b> -</li> </ul>
Pre-shared Key	Shared key for both sides of the tunnel
CA Certificate	This certificate is necessary for Authentication mode x.509.
Remote Certificate	This certificate is necessary for Authentication mode x.509.
Local Certificate	This certificate is necessary for Authentication mode x.509.
Local Private Key	This private key is necessary for Authentication mode x.509.
Local Passphrase	This Local Passphrase is necessary for Authentication mode x.509.
Extra Options	Use this parameter to define additional parameters of the IPsec tunnel, for example security parameters etc.

**Table 30: IPsec tunnel configuration**

The certificates and private keys have to be in PEM format.

The random time, after which it will exchange new keys, is defined as follows:

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

By default, the time for the exchange of keys is between:

- Minimum time: 1h - (9m + 9m) = 42m
- Maximum time: 1h - (9m + 0m) = 51m

In most cases, the settings should be left at their default values.

**IPsec Tunnel Configuration**

Create 1st IPsec tunnel  
 Description \*   
 Remote IP Address \*   
 Remote ID \*   
 Remote Subnet \*   
 Remote Subnet Mask \*   
 Local ID \*   
 Local Subnet \*   
 Local Subnet Mask \*   
 Key Lifetime  sec  
 IKE Lifetime  sec  
 Rekey Margin  sec  
 Rekey Fuzz  %  
 DPD Delay \*  sec  
 DPD Timeout \*  sec  
 NAT Traversal    
 Aggressive Mode    
 Authenticate Mode    
 Pre-shared Key   
 CA Certificate   
 Remote Certificate   
 Local Certificate   
 Local Private Key   
 Local Passphrase \*   
 Extra Options \*   
*\* can be blank*

**Fig. 34: IPsec tunnel configuration**

Example of IPsec Tunnel configuration:

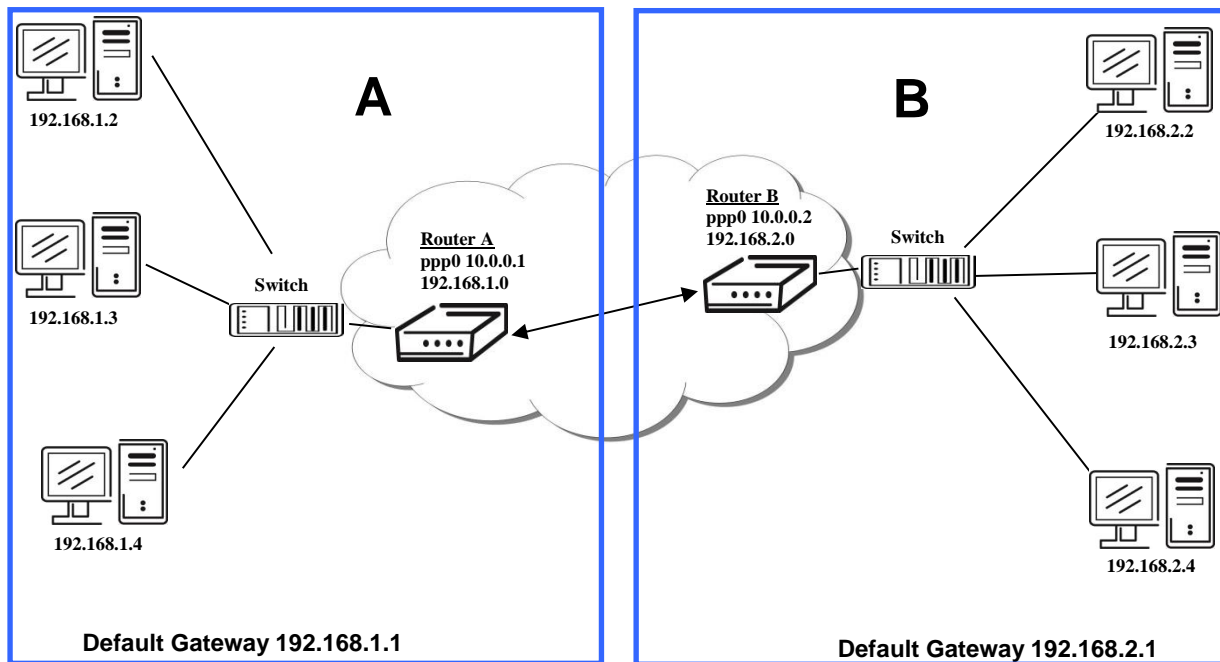


Fig. 35: Example 8 – Network Topology for IPsec Tunneling

IPsec tunnel configuration:

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

Table 31: Example 8 – IPsec Configuration

Examples of the different options for configuration and authentication of IPsec can be found in the IPsec tunnel configuration manual.

## 1.16. GRE tunnels configuration

Select the **GRE** item in the menu to configure a GRE tunnel. GRE is a protocol which is used to create a secure connection between two LANs. Up to 4 **GRE** tunnels may be created.

Item	Description
Create	This item enables the individual tunnels.
Description	This item displays the name of the tunnel specified in the configuration of the tunnel.
Edit	Configure the GRE tunnel.

**Table 32: Overview GRE tunnels**

GRE Tunnels Configuration		
Create	Description	
1st no		Edit
2nd no		Edit
3rd no		Edit
4th no		Edit

Apply

**Fig. 36: GRE tunnels configuration**

Item	Description
Description	Description of tunnel.
Remote IP Address	IP address of 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
Remote Subnet	IP address of the network behind the remote side of the tunnel
Remote Subnet Mask	Subnet Mask of the network behind the remote side of the tunnel
Pre-shared Key	An optional value that defines a 32 bit shared key for data encryption. This key must be the same on both routers.

**Table 33: GRE tunnel configuration**



**GRE Tunnel Configuration**

Create 1st GRE tunnel

Description \*

Remote IP Address

Remote Subnet \*

Remote Subnet Mask \*

Local Interface IP Address \*

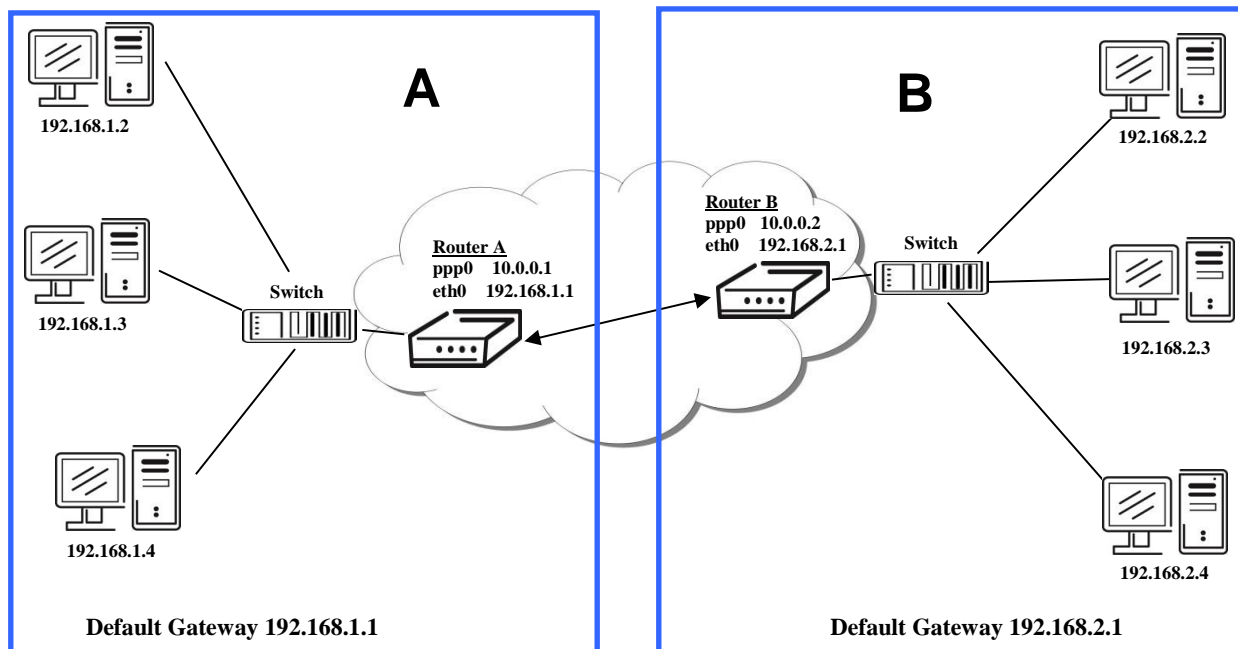
Remote Interface IP Address \*

Pre-shared Key \*

\* can be blank

**Fig. 37: GRE tunnel configuration**

Example of the GRE Tunnel configuration:



**Fig. 38: Example 9 – Network Topology for GRE Tunneling**

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 34: Example 9 - GRE Tunnel Configuration**

## 1.17. L2TP tunnel configuration

Select the **L2TP** item in the menu to configure an L2TP tunnel. L2TP is a protocol which is used to create a secure connection between two LANs. Only one **L2TP** tunnel may be created.

Item	Description
Mode	L2TP tunnel mode on the router side <ul style="list-style-type: none"> <li>• <b>L2TP server</b> - For a server, you must define the start and end IP address range offered by the server</li> <li>• <b>L2TP client</b> – For a client, you must enter the IP address of the server</li> </ul>
Server IP Address	IP address of server
Client Start IP Address	Start IP address in range, which is offered by server to clients
Client End IP Address	End IP address in range, which is offered by server to clients
Local IP Address	IP address of the local side of the tunnel
Remote IP Address	IP address of the remote side of the tunnel
Remote Subnet	Address of the network behind the remote side of the tunnel
Remote Subnet Mask	The mask of the network behind the remote side of the tunnel
Username	Username for login to L2TP tunnel
Password	Password for login to L2TP tunnel

Table 35: L2TP tunnel configuration

Press the Apply button to apply changes.

**L2TP Tunnel Configuration**

Create L2TP tunnel  
 Mode: L2TP client ▼  
 Server IP Address:   
 Client Start IP Address:   
 Client End IP Address:   
 Local IP Address \*:   
 Remote IP Address \*:   
 Remote Subnet \*:   
 Remote Subnet Mask \*:   
 Username:   
 Password:   
\* can be blank

Fig. 39: L2TP tunnel configuration

Example of the L2TP Tunnel configuration:

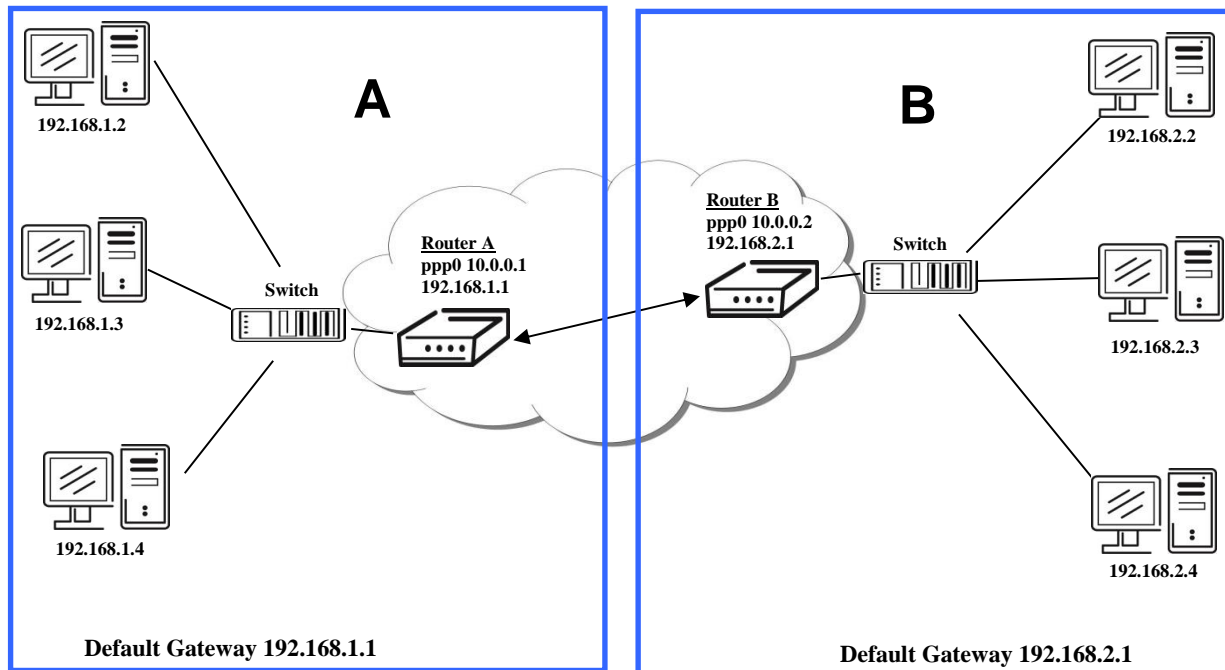


Fig. 40: Example 10 – Network Topology for L2TP Tunneling

Configuration of the L2TP tunnel:

Configuration	A	B
Mode	L2TP Server	L2TP Client
Server IP Address	---	10.0.0.1
Client Start IP Address	192.168.1.2	---
Client End IP Address	192.168.1.254	---
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 36: Example 10 – L2TP Tunnel Configuration

## 1.18. PPTP tunnel configuration

Select the **PPTP** item in the menu to configure a PPTP tunnel. PPTP is a protocol which is used to create a secure connection between two LANs. Only one PPTP tunnel may be created.

Item	Description
Mode	PPTP tunnel mode on the router side <ul style="list-style-type: none"> <li>• <b>PPTP server</b> - For a server, you must define the start and end IP address range offered by the server</li> <li>• <b>PPTP client</b> – For a client, you must enter the IP address of the server</li> </ul>
Server IP Address	IP address of server
Local IP Address	IP address of the local side of the tunnel
Remote IP Address	IP address of the remote side of the tunnel
Remote Subnet	Address of the network behind the remote side of the tunnel
Remote Subnet Mask	The mask of the network behind the remote side of the tunnel
Username	Username for login to PPTP tunnel
Password	Password for login to PPTP tunnel

Table 37: PPTP tunnel configuration

Press the Apply button to apply changes.

Fig. 41: PPTP tunnel configuration

Example of the PPTP Tunnel configuration:

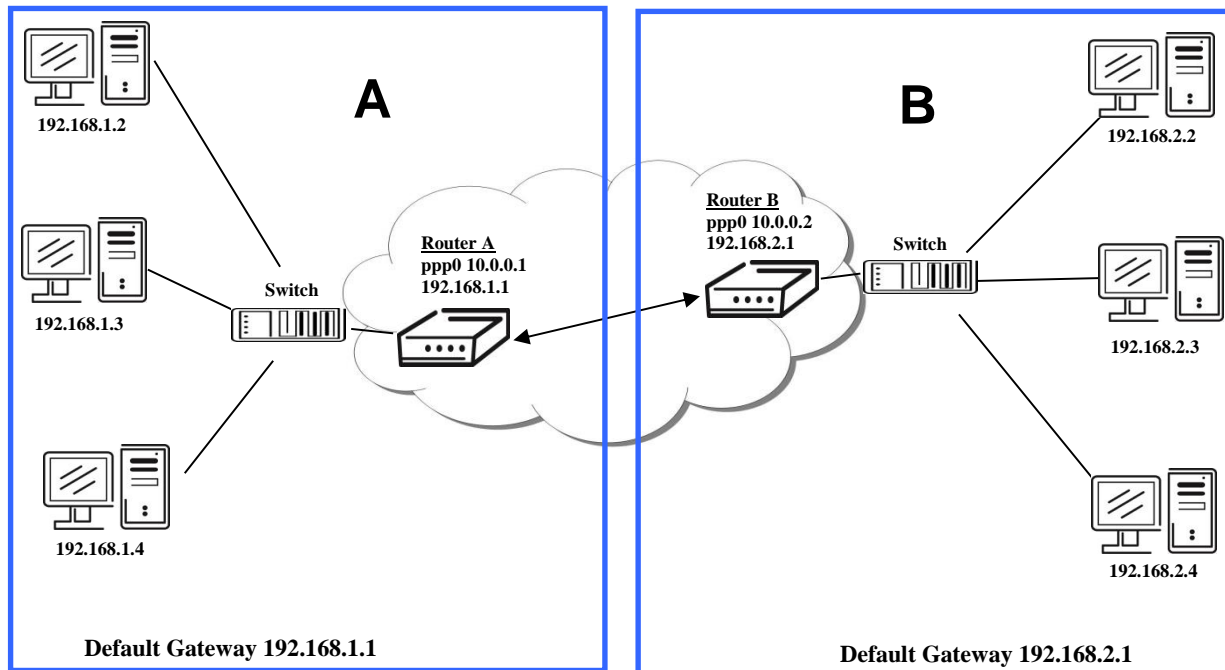


Fig. 42: Example 11 – Network Topology for PPTP Tunneling configuration

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	---	---
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 38: Example 11 – PPTP Tunnel Configuration

### 1.19. DynDNS client configuration

The router supports DynamicDNS using a DNS server on [www.dyndns.org](http://www.dyndns.org). DynDNS client Configuration can be called up by selecting option **DynDNS** item in the menu.

Item	Description
Hostname	Third order domain registered on server <a href="http://www.dyndns.org">www.dyndns.org</a>
Username	Username for login to DynDNS server
Password	Password for login to DynDNS server
Server	If you want to use a different DynDNS service than <a href="http://www.dyndns.org">www.dyndns.org</a> , enter the update server service in this parameter. If this item is left blank, the router uses the default server <b>members.dyndns.org</b> .

**Table 39: DynDNS configuration**

Example of the DynDNS client configuration with domain [conel.dyndns.org](http://conel.dyndns.org):

**DynDNS Configuration**

Enable DynDNS client

Hostname:

Username:

Password:

Server \*:

*\* can be blank*

**Fig. 43: Example of DynDNS configuration**

## 1.20. NTP client configuration

NTP (Network Time Protocol) allows the router to set its internal clock using a network time server. The NTP client Configuration can be called up by selecting option **NTP** item in the menu.

If option **Enable local NTP service** is selected, the router will function as an NTP server for other devices on the LAN.

Item	Description
Primary NTP Server Address	IP or domain address primary NTP server.
Secondary NTP Server Address	IP or domain address secondary NTP server.
Timezone	Sets the time zone of the router
Daylight Saving Time	Define time shift: <ul style="list-style-type: none"> <li>• No - time shift is disabled</li> <li>• Yes - time shift is allowed</li> </ul>

**Table 40: NTP configuration**

Example of the NTP configuration with primary (ntp.cesnet.cz) and secondary (tik.cesnet.cz) NTP servers and with daylight saving time:

The screenshot shows the NTP Configuration page with the following settings:

- Enable local NTP service
- Synchronize clock with NTP server
- Primary NTP Server: ntp.cesnet.cz
- Secondary NTP Server: tik.cesnet.cz
- Timezone: GMT+01:00
- Daylight Saving Time: yes

An **Apply** button is located at the bottom left of the configuration area.

**Fig. 44: Example of NTP configuration**

## 1.21. SNMP configuration

SNMP (Simple Network Management Protocol) provides status information about network elements such as routers or end computers. The router supports SNMP agent Version 1. To enter the **SNMP** Configuration, select the **SNMP** item from the configuration menu.

Item	Description
Community	Password for access to the SNMP agent.
Contact	How to contact the person who manages the router.
Name	Designation of the router.
Location	Location of the router.

**Table 41: SNMP configuration**

Select the **Enable I/O extension** option to monitor the binary input (I/O) on the router.

Select the **Enable XC-CNT extension** to monitor the status of the expansion port CNT inputs and outputs.

Item	Description
<i>Baud rate</i>	Communication speed.
<i>Parity</i>	Control parity bit: <ul style="list-style-type: none"> <li>• none – Data will be sent without parity.</li> <li>• even – Data will be sent with even parity.</li> <li>• odd - Data will be sent with odd parity.</li> </ul>
<i>Stop Bits</i>	Number of stop bits.

**Table 42: SNMP configuration**



Every monitor value is uniquely identified by a number identifier **OID** (*Object Identifier*). For the binary input and output the following range of OIDs is used:

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

**Table 43: Object identifier for binary input and output**

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

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

**Table 44: Object identifier for CNT port**

Example of SNMP settings and readout:



The image shows a 'SNMP Configuration' dialog box with the following settings:

- Enable SNMP agent
- Community: public
- Contact \*: Jack Roghul +420 732 123
- Name \*: Conel
- Location \*: Usti nad Orlici
- Enable I/O extension
- Enable XC-CNT extension
- Enable M-BUS extension
- Baudrate: 300
- Parity: even
- Stop Bits: 1
- \* can be blank
- Apply button

Fig. 45: Example of SNMP configuration

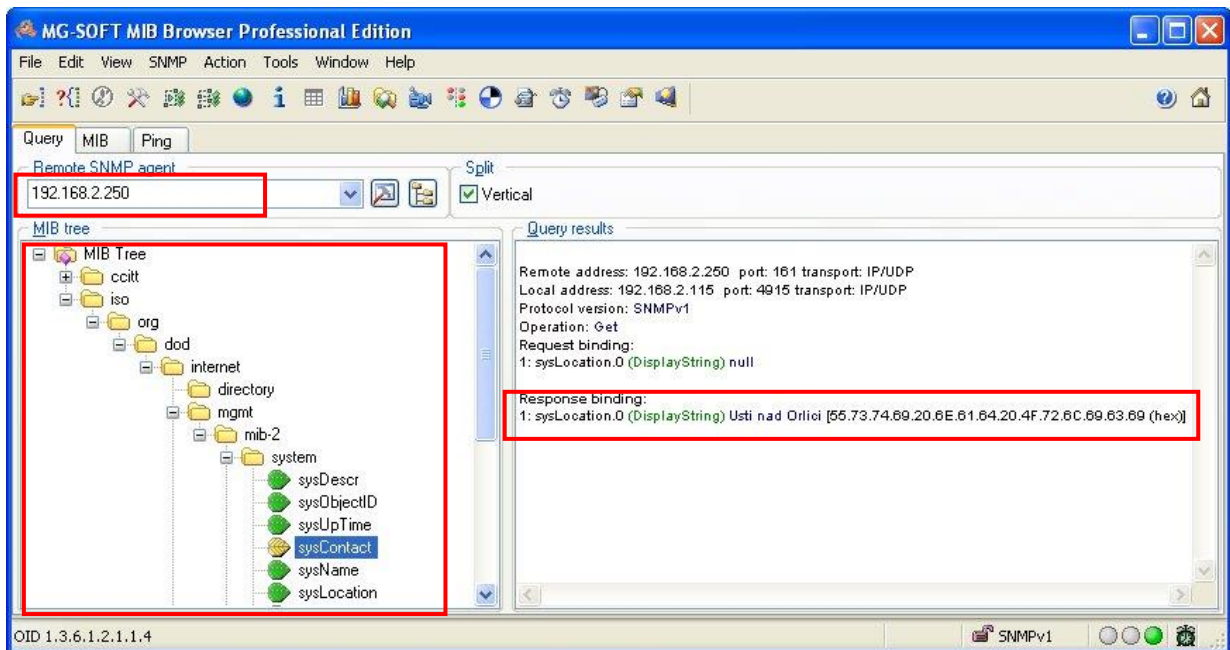


Fig. 46: Example of the MIB browser

It is important to set the IP address of the SNMP agent (router) in the field **Remote SNMP agent**. After entering the IP address, it is possible to show object identifiers.

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*

## 1.22. SMTP configuration

The SMTP (Simple Mail Transfer Protocol) client is used to send emails.

Item	Description
SMTP Server Address	IP or domain address of the mail server.
Username	Name to email account.
Password	Password to email account.
Own Email Address	Address of the sender.

Fig. 47: SMTP client configuration

The mobile operator may block other SMTP servers. If this occurs, then you must use the SMTP server of the operator.

Example settings for the SMTP client:

SMTP Configuration	
SMTP Server Address	<input type="text" value="smtp.domain.com"/>
Username	<input type="text" value="name@domain.com"/>
Password	<input type="text" value="pass"/>
Own Email Address	<input type="text" value="name@domain.com"/>
<input type="button" value="Apply"/>	

Fig. 48: SMTP configuration

An E-mail can be sent from the Startup script. The following command is used to send emails with following parameters.

- -t receiver Email address
- -s subject
- -m message
- -a appendix
- -r number of attempts to send email (default set 2 attempts)



Commands and parameters can be entered only in lowercase.

Example to send email:

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

This command sends an e-mail message to address *jack@google.com* with the subject "subject", body message "message" and annex "abc.doc" right from the directory *c:\directory\* and will attempt 5 times to send the message.

### 1.23. SMS configuration



**Note:** The SPECTRE RT industrial router does not support SMS messaging configuration.

The SPECTRE cellular router can automatically send SMS messages to a cell phone or SMS message server when certain events occur. The SMS Configuration page allows the user to select which events will generate an SMS message.

Item	Description
Send SMS on power up	Send an SMS message when the router powers up
Send SMS on PPP connect	Send an SMS message when the PPP connection is active.
Send SMS on PPP disconnect	Send an SMS message on PPP disconnection.
Send SMS when datalimit exceeded	Send an SMS message when the data limit is exceeded.
Send SMS when binary input on I/O port (BIN0) is active	Send an SMS message when the binary input on the I/O port (BIN0) goes active. The text of the message is set using parameter BIN0.
Send SMS when binary input on expansion port (BIN1-BIN4) is active	Send an SMS message when a binary input on the I/O expansion port (BIN1-BIN4) is active. The text of the message is set using parameters BIN1 - BIN4.
Add timestamp to SMS	Adds a time stamp to the sent SMS messages. The timestamp has the format YYYY-MM-DD hh:mm:ss.
Phone Number 1	The telephone numbers that the SMS messages will be sent to.
Phone Number 2	
Phone Number 3	
Unit ID	The name of the router that is included in the SMS messages.
BIN0 - SMS	User-defined Text field 0 for the SMS messages.
BIN1 - SMS	User-defined Text field 1 for the SMS messages.
BIN2 - SMS	User-defined Text field 2 for the SMS messages.
BIN3 - SMS	User-defined Text field 3 for the SMS messages.
BIN4 - SMS	User-defined Text field 4 for the SMS messages.

**Table 45: Send SMS configuration**

You can also control the function of the router by sending SMS messages to the device. The router can be commanded to go online or offline via an SMS message or to switch to the alternate SIM card or provider. The binary outputs can also be set or reset using SMS. The **Enable remote control via SMS** option must be selected to enable this feature. Up to three numbers can be configured for incoming SMS messages. If the **Enable remote control via SMS** option is set, all incoming SMS messages are processed by the router and deleted.

Item	Description
Phone Number 1	Allowed phone numbers for incoming SMS messages.
Phone Number 2	
Phone Number 3	

**Table 46: Control via SMS configuration**



**Note:** If no phone number is filled in, the router will accept incoming messages from all phone numbers. If any phone numbers are entered into the list, the router will only accept SMS messages which originate from those numbers.

Control SMS messages cannot change the router configuration. Any changes made to the router by an SMS message will only remain in effect until the router is restarted. After a reboot, the router configuration will return to the settings in non-volatile memory. For example, if the router is switched offline by an SMS message, the router will remain offline until the next time it is power cycled or re-booted.

To control the router using SMS, the message text must contain the control command. Table 48 lists the SMS control messages that are supported.

SMS Control Message	Description
go online sim 1	Switch to SIM1 card
go online sim 2	Switch to SIM2 card
go online	Switch router in online mode
go offline	PPP connection termination
set out0=0	Set binary I/O output to 0
set out0=1	Set binary I/O output to 1
set out1=0	Set binary output on port 1 to a 0
set out1=1	Set binary output on port 1 to a 1
set profile std	Set standard profile
set profile alt1	Set alternative profile 1
set profile alt2	Set alternative profile 2
set profile alt3	Set alternative profile 3
reboot	Router reboot
get ip	Router will send an SMS message back with the IP address from the SIM card.

**Table 47: SMS Control Commands**

You may send and receive SMS messages using either the serial expansion ports or a TCP connection over the Ethernet network. For serial communication, the baud rate must be set to match the attached host. Select option **Enable AT-SMS protocol on expansion port 1** to allow messages to be sent and received using serial port 1.

Item	Description
Baud rate	Communication speed expansion port 1

**Table 48: Send SMS on serial PORT1 configuration**

Select option **Enable AT-SMS protocol on expansion port 2** to allow messages to be sent and received using serial port 2.

Item	Description
Baud rate	Communication speed expansion port 2

**Table 49: Send SMS on serial PORT2 configuration**

It is also possible to send and receive SMS messages over a TCP/IP connection by choosing **Enable AT-SMS protocol on TCP port**. The TCP port used for sending and receiving SMS messages must be entered into the configuration field.

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

Table 50: Send SMS on Ethernet Port configuration

### 1.23.1. Send SMS

Standard AT commands are used to send and receive SMS messages over the serial ports or a TCP connection. They can be sent to the router using a terminal program such as Hyper Terminal. After establishing a connection with the router via the serial interface or Ethernet, AT commands are used to read and delete incoming messages and send outgoing messages. Table 52 lists the AT commands that are used for sending and receiving SMS messages.

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

Table 51: AT commands to send and receive SMS messages

In order to send an SMS message, text mode must first be selected by sending the command **AT+CMGF=1** to the router.

Command: **AT+CMGF=1**

Response: **OK**

The SMS message is created and sent using the command **AT+CMGS="tel. number"** where **tel. number** is the telephone number to send the message to. After pressing the **Enter** button, the router will respond with a '>' prompt and the text of the SMS message can be entered. After entering the text, press **CTRL+Z** to send the message. It may take a few minutes for the SMS message to be sent depending on the network. You may cancel SMS text input by pressing **Esc**.

**Example:** To send "Hello World" to telephone number **712-123-4567**

Command: **AT+CMGS="7121234567"**      Press Enter

Response: >

Enter SMS Text: **Hello World!**      Press CTRL+Z (keys combination)

Response: OK

To see a list of all incoming messages, type:

Command: **AT+CMGL="ALL"** Press Enter

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

where <index> is ordinal number of the message,

<status> is SMS status:

REC UNREAD – SMS unread  
REC READ – SMS read  
STO UNSENT – stored unsent SMS  
STO SENT – stored sent SMS  
ALL – all SMS messages

<sender number> tel. number from which the SMS was received.

<date> date SMS message received,

<time> time SMS message received.

Example:

**+CMGL: 1,"REC UNREAD", "+420721123456", "08/02/02, 10:33:26+04"  
Hello World!**

To read a single SMS message, use **AT+CMGR=<index>** where index is the number of the SMS message.

Example:

Command: **AT+CMGR=1** Press Enter

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

To delete a received SMS message, use **AT+CMGD=<index>** where index is the number of the message to delete.

To delete message 1:

Command: **AT+CMGD=1** Press Enter

Response: OK

The format of the Router Power-On SMS message is as follows:

**Router (Unit ID) has been powered up. GSM signal strength –xx dBm.**

The format of the Router PPP connection SMS message is as follows:

**Router (Unit ID) has established PPP connection. IP address xxx.xxx.xxx.xxx**

After a PPP disconnect, the router will send an SMS message in the form:

**Router (Unit ID) has lost PPP connection. IP address xxx.xxx.xxx.xxx**

SMS Configuration Example:

SMS Configuration	
<input checked="" type="checkbox"/>	Send SMS on power up
<input checked="" type="checkbox"/>	Send SMS on PPP connect
<input checked="" type="checkbox"/>	Send SMS on PPP disconnect
<input checked="" type="checkbox"/>	Send SMS when datalimit is exceeded
<input checked="" type="checkbox"/>	Send SMS when binary input on I/O port (BIN0) is active
<input checked="" type="checkbox"/>	Send SMS when binary input on expansion port 1 (BIN1-BIN4) is active
<input checked="" type="checkbox"/>	Add timestamp to SMS
Phone Number 1	<input type="text" value="723123456"/>
Phone Number 2	<input type="text" value="756858635"/>
Phone Number 3	<input type="text" value="603854758"/>
Unit ID *	<input type="text" value="Router"/>
BIN0 - SMS *	<input type="text" value="BIN0"/>
BIN1 - SMS *	<input type="text" value="BIN1"/>
BIN2 - SMS *	<input type="text" value="BIN2"/>
BIN3 - SMS *	<input type="text" value="BIN3"/>
BIN4 - SMS *	<input type="text" value="BIN4"/>
<input checked="" type="checkbox"/>	Enable remote control via SMS
Phone Number 1	<input type="text"/>
Phone Number 2	<input type="text"/>
Phone Number 3	<input type="text"/>
<input type="checkbox"/>	Enable AT-SMS protocol on expansion port 1
Baudrate	<input type="text" value="9600"/>
<input type="checkbox"/>	Enable AT-SMS protocol on expansion port 2
Baudrate	<input type="text" value="9600"/>
<input type="checkbox"/>	Enable AT-SMS protocol over TCP
TCP Port	<input type="text"/>
* can be blank	
<input type="button" value="Apply"/>	

Fig. 49: Example of SMS configuration 1



Router configuration for sending SMS messages via the serial interface on PORT1:

SMS Configuration	
<input type="checkbox"/>	Send SMS on power up
<input type="checkbox"/>	Send SMS on PPP connect
<input type="checkbox"/>	Send SMS on PPP disconnect
<input type="checkbox"/>	Send SMS when datalimit is exceeded
<input type="checkbox"/>	Send SMS when binary input on I/O port (BIN0) is active
<input type="checkbox"/>	Send SMS when binary input on expansion port 1 (BIN1-BIN4) is active
<input type="checkbox"/>	Add timestamp to SMS
Phone Number 1	<input type="text"/>
Phone Number 2	<input type="text"/>
Phone Number 3	<input type="text"/>
Unit ID *	<input type="text"/>
BIN0 - SMS *	<input type="text"/>
BIN1 - SMS *	<input type="text"/>
BIN2 - SMS *	<input type="text"/>
BIN3 - SMS *	<input type="text"/>
BIN4 - 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"/>	

Fig. 50: Example of SMS configuration 2

Example of the router configuration for accepting SMS messages from every phone number:

SMS Configuration	
<input type="checkbox"/>	Send SMS on power up
<input type="checkbox"/>	Send SMS on PPP connect
<input type="checkbox"/>	Send SMS on PPP disconnect
<input type="checkbox"/>	Send SMS when datalimit is exceeded
<input type="checkbox"/>	Send SMS when binary input on I/O port (BIN0) is active
<input type="checkbox"/>	Send SMS when binary input on expansion port 1 (BIN1-BIN4) is active
<input type="checkbox"/>	Add timestamp to SMS
Phone Number 1	<input type="text"/>
Phone Number 2	<input type="text"/>
Phone Number 3	<input type="text"/>
Unit ID *	<input type="text"/>
BIN0 - SMS *	<input type="text"/>
BIN1 - SMS *	<input type="text"/>
BIN2 - SMS *	<input type="text"/>
BIN3 - SMS *	<input type="text"/>
BIN4 - 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"/>	

**Fig. 51: Example of SMS configuration 3**

Example of the router configuration for accepting SMS messages from two phone numbers:

SMS Configuration	
<input type="checkbox"/>	Send SMS on power up
<input type="checkbox"/>	Send SMS on PPP connect
<input type="checkbox"/>	Send SMS on PPP disconnect
<input type="checkbox"/>	Send SMS when datalimit is exceeded
<input type="checkbox"/>	Send SMS when binary input on I/O port (BIN0) is active
<input type="checkbox"/>	Send SMS when binary input on expansion port 1 (BIN1-BIN4) is active
<input type="checkbox"/>	Add timestamp to SMS
Phone Number 1	<input type="text"/>
Phone Number 2	<input type="text"/>
Phone Number 3	<input type="text"/>
Unit ID *	<input type="text"/>
BIN0 - SMS *	<input type="text"/>
BIN1 - SMS *	<input type="text"/>
BIN2 - SMS *	<input type="text"/>
BIN3 - SMS *	<input type="text"/>
BIN4 - 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"/>	

Fig. 52: Example of SMS configuration 4

## 1.24. Expansion Port Configuration

You may send and receive data from a serial port on Auxiliary Port 1 or 2 using UDP or TCP protocol on the Ethernet network. This feature allows a computer on the network to send data to a serial device as if it was physically connected to the computer. You can also configure 2 routers to act as a serial port extender where they transmit data transparently across the Ethernet network between 2 serial devices as if the serial devices were cabled together.

You must be using a router which has the RS-232 or RS-485 option on Port 1 or 2.

Item	Description
Baud rate	Communication speed.
Data Bits	Number of data bits.
Parity	Control parity bit <ul style="list-style-type: none"> <li>• none</li> <li>• even</li> <li>• odd</li> </ul>
Stop Bits	Number of stop bits.
Split Timeout	Inter-character Timeout. If no characters are received within this amount of time, any buffered characters will be sent over the Ethernet port.
Protocol	Protocol: <ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> </ul>
Mode	Mode of connection: <ul style="list-style-type: none"> <li>• TCP server - The router will listen for incoming TCP connection requests.</li> <li>• TCP client - The router will connect to a TCP server on the specified IP address and TCP port.</li> </ul>
Server Address	When set to <b>TCP client</b> above, it is necessary to enter the <b>Server address</b> and <b>TCP port</b> .
TCP Port	The TCP port for connections.

Table 52: Expansion PORT configuration

If the **Check TCP connection** is selected, the router will automatically send TCP keep-alive messages to verify that the connection is still valid.

Item	Description
Keepalive Time	Time between sending keep-alive packets
Keepalive Interval	Keep-alive Response Timeout
Keepalive Probes	Number of attempts before connection is down

Table 53: TCP Keep-Alive Configuration

If the option **Use CD as indicator of the TCP connection** is selected, the router will activate the DTR output when a TCP connection is active.

CD	Description
Active	TCP connection is on
Nonactive	TCP connection is off

**Table 54: CD signal description**

Select **Use DTR as control of TCP connection** to use DTR to control when TCP connections are allowed. (**CD on the router**).

DTR	Description server	Description client
Active	The router will accept a TCP connection.	Router creates a TCP connection.
Nonactive	The router does not accept incoming TCP connections.	Router ends the TCP connection.

**Table 55: DTR signal description**

Press the **Apply** button to apply changes.

**Expansion Port 1 Configuration**

Enable expansion port 1 access over TCP/UDP

Port Type:

Baudrate:  ▼

Data Bits:  ▼

Parity:  ▼

Stop Bits:  ▼

Split Timeout:  msec

Protocol:  ▼

Mode:  ▼

Server Address:

TCP Port:

---

Check TCP connection

Keepalive Time:  sec

Keepalive Interval:  sec

Keepalive Probes:

**Fig. 53: Expansion port configuration**

Example of external port configuration:

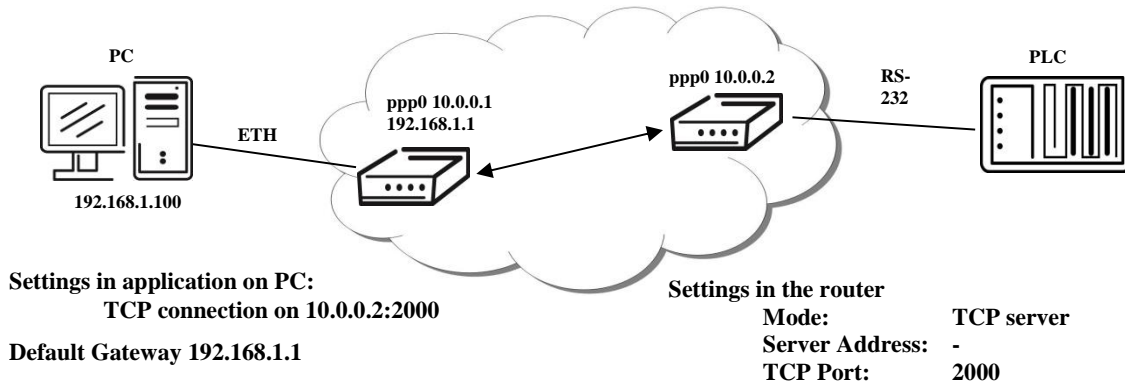


Fig. 54: Example of Ethernet to Serial Communication

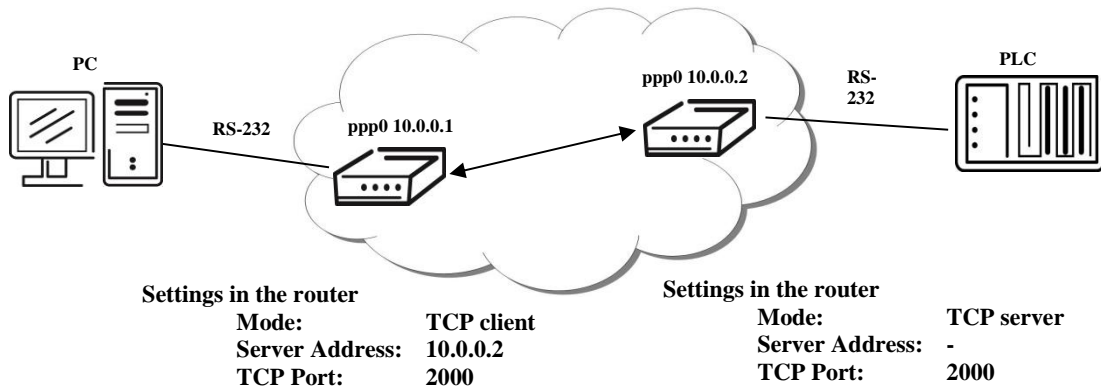


Fig. 55: Example of Serial Port Extension

## 1.25. USB port configuration

Select the **USB Port** item in the configuration menu to bring up the USB configuration page. A USB to RS-232 converter can be used to send data out of the serial port from the Ethernet network in the same manner as the RS-232 expansion port options.

Item	Description
Baud rate	Applied communication speed.
Data Bits	Number of data bits.
Parity	Control parity bit <ul style="list-style-type: none"> <li>• none</li> <li>• even</li> <li>• odd</li> </ul>
Stop Bits	Number of stop bit.
Split Timeout	Inter-character Timeout (ms). If no characters are received within this amount of time, any buffered characters will be sent out of the USB port.
Protocol	Communication protocol: <ul style="list-style-type: none"> <li>• TCP - communication using a linked protocol TCP</li> <li>• UDP - communication using a unlinked protocol UDP</li> </ul>
Mode	Mode of connection: <ul style="list-style-type: none"> <li>• TCP server - The router will listen to incoming requests regarding the TCP connection.</li> <li>• TCP client - The router will connect to a TCP server on the specified IP address and TCP port.</li> </ul>
Server Address	In mode <i>TCP client</i> it is necessary to enter the <i>Server address</i> and final <i>TCP port</i> .
TCP Port	In both modes of connection it is necessary to specify the TCP port on which the router will communicate TCP connections.

**Table 56: USB port configuration 1**

If the **Check TCP connection** is selected, the router will automatically send TCP keep-alive messages to verify that the connection is still valid.

Item	Description
Keepalive Time	Time between sending keep-alive packets
Keepalive Interval	Keep-alive Response Timeout
Keepalive Probes	Number of attempts before connection is down

**Table 57: USB PORT configuration 2**

If the option **Use CD as indicator of the TCP connection** is selected, the router will activate the DTR output when a TCP connection is active.

CD	Description
Active	TCP connection is on
Nonactive	TCP connection is off

**Table 58: CD signal description**

Select **Use DTR as control of TCP connection** to use DTR to control when TCP connections are allowed. (CD on the router).

DTR	Description server	Description client
Active	The router will accept a TCP connection.	Router creates a TCP connection.
Nonactive	The router does not accept incoming TCP connections.	Router ends the TCP connection.

Table 59: DTR signal description

Supported USB/RS-232 converters:

- FTDI
- Prolific PL2303
- Silicon Laboratories CP210x

**USB Port Configuration**

Enable USB serial converter access over TCP/UDP
   
 Baudrate: 
  
 Data Bits: 
  
 Parity: 
  
 Stop Bits: 
  
 Split Timeout:  msec
   
 Protocol: 
  
 Mode: 
  
 Server Address: 
  
 TCP port:

---

Check TCP connection
   
 Keepalive Time:  sec
   
 Keepalive Interval:  sec
   
 Keepalive Probes:

Fig. 56: USB configuration



Example of USB port configuration:

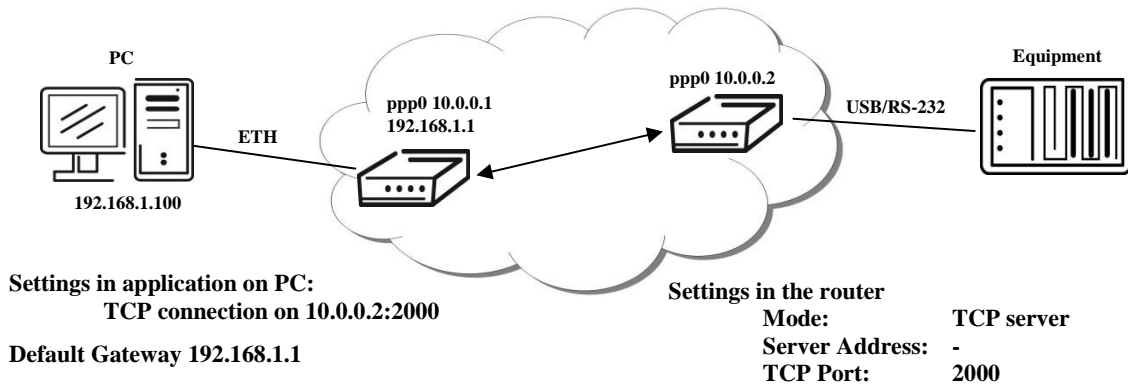


Fig. 57: Example of Ethernet to Serial using USB Port

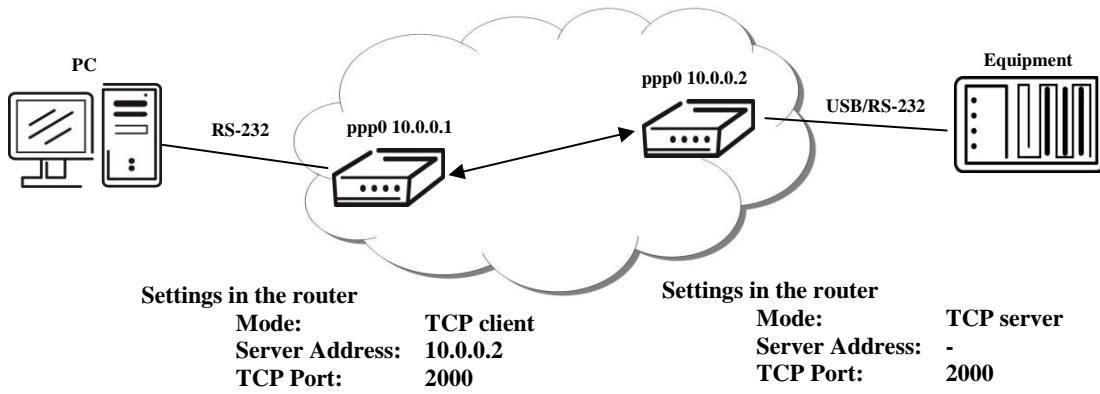


Fig. 58: Example of Serial Extension using USB port

## 1.26. Startup script

Use the **Startup Script** window to create your own scripts which will be executed after all of the initialization scripts are run.

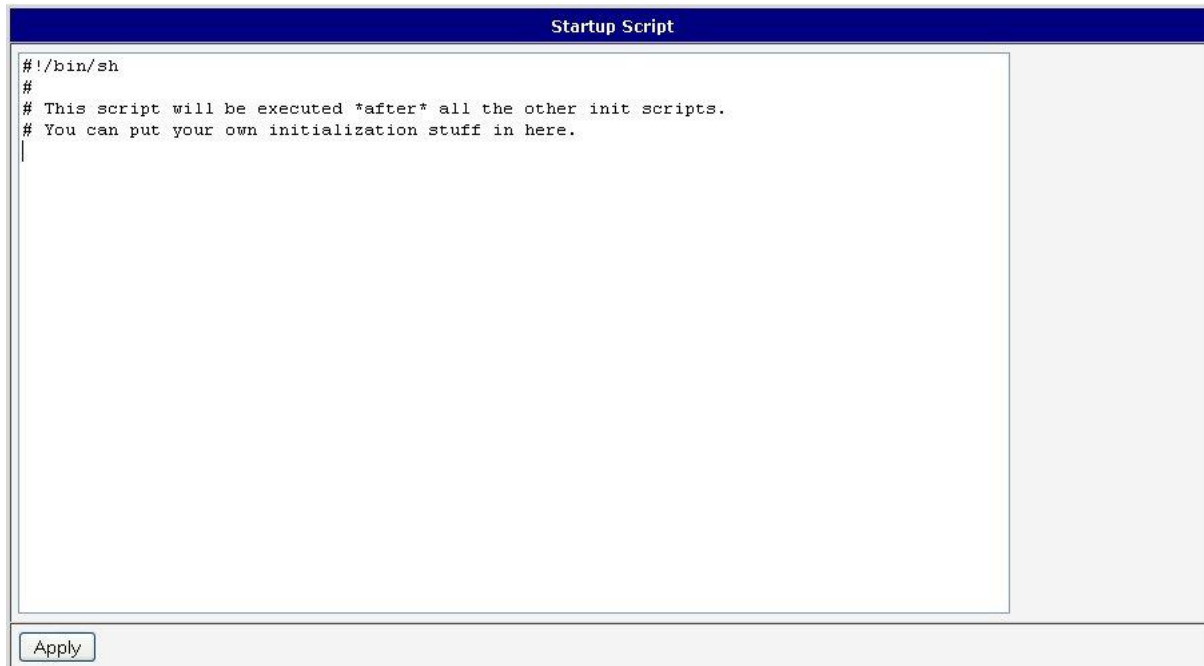


Fig. 59: Startup script

Any changes to the startup scripts will take effect the next time the router is power cycled or rebooted.

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

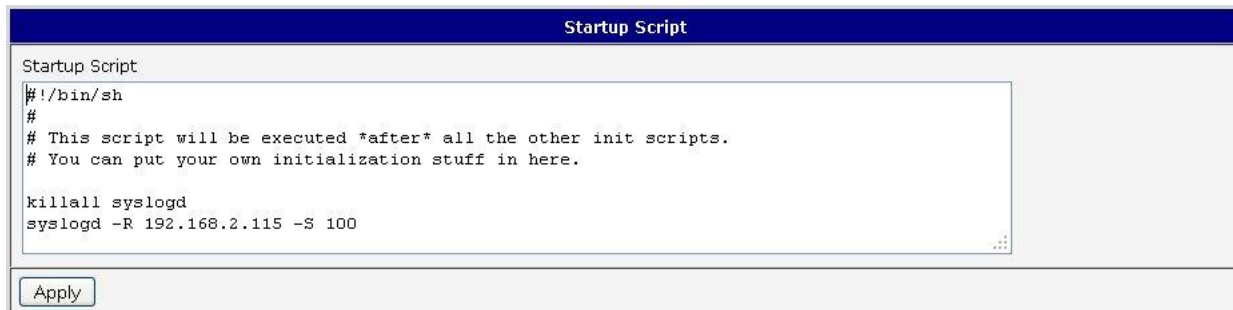


Fig. 60: Example of Startup script

## 1.27. Up/Down script

Use the **Up/Down Script** window to create scripts which will run when the PPP connection is started or goes down. Any scripts entered into the **Up script** window will run after a PPP/WAN connection is established. Script commands entered into the **Down Script** window will run when the PPP/WAN connection is lost.

The screenshot shows a window titled "Up/Down Script" with two text input areas. The top area is labeled "Up Script" and contains the following text: `#!/bin/sh`, `#`, and `# This script will be executed when PPP/WAN connection is established.`. The bottom area is labeled "Down Script" and contains the following text: `#!/bin/sh`, `#`, and `# This script will be executed when PPP/WAN connection is lost.`. An "Apply" button is located at the bottom left of the window.

Fig. 61: Up/Down script

Example of UP/Down script: After establishing or losing a PPP connection, the router sends an email with information about the PPP connection.

The screenshot shows the same "Up/Down Script" window, but with example scripts. The "Up Script" area contains: `#!/bin/sh`, `#`, `# This script will be executed when PPP/WAN connection is established.`, and `email -t name@domain.com -s "Conel router" -m "PPP connection is established."`. The "Down Script" area contains: `#!/bin/sh`, `#`, `# This script will be executed when PPP/WAN connection is lost.`, and `email -t name@domain.com -s "Conel router" -m "PPP connection is lost."`. An "Apply" button is at the bottom left.

Fig. 62: Example of Up/Down script

## 1.28. Automatic update configuration

The SPECTRE router can be configured to automatically check for firmware updates from an FTP site or a web server and update its firmware or configuration information. Use the **Automatic update** menu to configure the automatic update settings. It is also possible to update the configuration and firmware through the USB host connector of the router.

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

Item	Description
Source	Select the location of the update files: <ul style="list-style-type: none"> <li>• <b>HTTP/FTP server</b> – Remote file server.</li> <li>• <b>USB flash drive</b> - Router will check for firmware or configuration files in the root directory of the connected USB device.</li> <li>• <b>Both</b> – Router will check for new firmware or configuration files in both places.</li> </ul>
Base URL	<i>Base URL</i> or IP address from which the configuration file will be downloaded.
Unit ID	Name of configuration. If the Unit ID of the router is not filled in, then the MAC address of the router will be used as the default file name. (The delimiter in a MAC address is a colon instead of a dot.)
Update Hour	Automatic configuration update starts 5 minutes after turning on the router and then every 24 hours at the <i>Update Hour</i> .

**Table 60: Automatic update configuration**

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

The **firmware file** name is named parameter *Base URL*, type of router and bin extension.

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



The following examples check for new firmware or configurations each day at 1:00 a.m. An example is given for the SPECTRE 3G router.

- Firmware: `http://router.cz/spectre3g.bin`
- Configuration file: `http://router.cz/temelin.cfg`

**Fig. 63: Example of automatic update 1**

The following examples check for new firmware or configurations each day at 1:00 a.m. An example is given for the SPECTRE 3G router with MAC address 00:11:22:33:44:55.

- Firmware: `http://router.cz/spectre3g.bin`
- Configuration file: `http://router.cz/00.11.22.33.44.55.cfg`

**Fig. 64: Example of automatic update 2**

## 1.29. User modules

You may run custom software programs in the router to enhance the features of the router. Use the **User Modules** menu item to add new software modules to the router, to remove them, or to change their configuration. Programming, compiling, and uploading user software modules are described in the application programming guide.

**Fig. 65: User modules**

### 1.30. Change profile

Up to three alternate router configurations or profiles can be stored in router 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 usage 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.



The screenshot shows a web interface titled "Change Profile". It features a dropdown menu for "Profile" currently set to "Standard". Below this is a checkbox labeled "Copy settings from current profile to selected profile", which is currently unchecked. At the bottom of the form is an "Apply" button.

Fig. 66: Change profile

### 1.31. Change password

You may change the router password using the **Change Password** menu item. The new password will be saved after pressing the **Apply** button.

The default password is "root". It is recommended that you change the password during initial setup for higher security.



The screenshot shows a web interface titled "Change Password". It contains two input fields: "New Password" and "Confirm Password". Below these fields is an "Apply" button.


Fig. 67: Change password

### 1.32. Set real time clock

You may update the router's internal clock at any time using a NTP server by selecting the **Set Real Time Clock** menu item. Enter the IP address or domain name of the NTP Server and click **Apply** to set the clock.

Fig. 68: Set real time clock


### 1.33. Set SMS service center address

 The SPECTRE RT industrial router does not support the **Set SMS service center address option**.

The SMS service center phone number is normally programmed into the SIM card by the carrier and does not need to be manually entered. However, in some cases, it may be necessary to set the phone number of the SMS service center in order to send SMS messages. This parameter cannot be set if the SIM card already contains the SMSC information. The phone number can be entered with or without an international prefix. For example: +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. This parameter is provisioned automatically by the carrier on CDMA networks and does not need to be manually entered.

Fig. 69: Set SMS service center address

### 1.34. Unlock SIM card

 The SPECTRE RT industrial router does not support the **Unlock SIM card** option.

You may lock the SIM card with a 4-8 digit PIN (Personal Identification Number) code to prevent unauthorized use of the SIM card. The PIN code must be entered each time that the SIM card is powered up. The SPECTRE cellular router supports the use of a SIM card with a PIN number. Enter the PIN number into the SIM PIN field on the configuration page and select **Apply**.


 Access to the SIM card is blocked if the PIN code is incorrectly entered 3 times. Contact technical support if the SIM card has been blocked.

Fig. 70: Unlock SIM card

### 1.35. Send SMS



The SPECTRE RT industrial router does not support the **Send SMS** option.

You can send an SMS message from the router to test the cellular network. To send an SMS message, select **Send SMS** from the configuration menu. Enter the phone number and text of the message into the text boxes and click the **Send** button. It may take a few seconds to send the message.

Fig. 71: Send SMS

It is also possible to send an SMS message using an HTTP request in the form:

```
GET /send_exec.cgi?phone=%2B420712345678&message=Test HTTP/1.1
Authorization: Basic cm9vdDpyb290
```

The HTTP request will be sent to TCP connection on router port 80. Router sends an SMS message with text "Test". SMS is sent to phone number "420712345678". Authorization is in the format "user:password" coded by BASE64. In the example is used for root:root.

### 1.36. Backup configuration

You may save the current router configuration to a file using the **Backup Configuration** menu item. It is recommended that you save the current configuration before a firmware update.

### 1.37. Restore configuration

You may restore the router configuration from a file using the **Restore Configuration** menu item.

Fig. 72: Restore configuration



### 1.38. Update firmware

Select the **Update Firmware** menu item to view the current router firmware version and load new firmware into the router. To load new firmware, browse to the new firmware file and press the **Update** button to begin the update. **Do not turn off the router during the firmware update.**

Update Firmware	
Firmware Version : 2.0.7 (2010-12-16)	
New Firmware	<input type="text"/> <input type="button" value="Browse"/>
<input type="button" value="Update"/>	

Fig. 73: Update firmware

During the firmware update, the router will show the following messages:

```

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

Reboot in progress

Continue here after reboot.

```

After the firmware update, the router will automatically reboot.



**Note:** Do not turn off the router during the firmware update.

### 1.39. Reboot

The router can be rebooted remotely through the web interface. To reboot the router, select the **Reboot** menu item and then press the **Reboot** button.

Reboot
The reboot process will take about 15 seconds to complete.
<input type="button" value="Reboot"/>

Fig. 74: Reboot

## 2. Router Configuration over Telnet

Monitoring of status, configuration and administration of the router can be performed over the Telnet interface. The default IP address of the modem is 192.168.1.1. Configuration may be performed only by the user "root" with initial password "root".

The following commands may be used to configure the router over Telnet:

Command	Description
cat	display file
cp	copy a file
date	show/change system time
df	Display information about file system
dmesg	kernel diagnostic messages
echo	string write
email	Email send
free	Display information about available memory
gsmat	Send an AT commend
gsminfo	Display information about signal quality
gsmsms	SMS send
hwclock	display/change time in RTC
ifconfig	display/change interface configuration
io	reading/writing input/output pins
ip	display/change route table
iptables	display/change NetFilter rules
kill	Kill a process
killall	Kill all processes
ln	link create
ls	dump directory contents
mkdir	create directory
mv	Move file
ntpdate	synchronize system time with NTP server
passwd	password change
ping	ICMP ping
ps	display process information
pwd	display directory contents
reboot	Reboot
rm	file delete
rmdir	directory delete
route	display/change route table
service	start/stop a service
sleep	pause number of seconds
slog	display system log
tail	display file end
tcpdump	monitoring of network
touch	file create/change time stamp
vi	text editor

Table 61: Telnet commands

## 3. Wi-Fi Configuration

### 3.1. Wi-Fi Access Point

The SPECTRE 3G-W and LTE-W routers can provide wireless access to the network using a built-in 802.11bgn Wi-Fi module. Support for the Wi-Fi module is provided by a User Software module which is pre-loaded into the SPECTRE Wi-Fi router at the factory. Only access point functionality is provided by the router.

Select the **WiFi** user module to view the **Wi-Fi AP** status and configuration. This link is located on the **User Modules** customization web page. The link to **"Wi-Fi AP"** information is in the **"Status"** section.

Item	Description
hostapd state dump	Time stamp of actual WiFi status.
num_sta	Number of associated stations.
num_sta_non_erp	Number of associated Non-ERP stations (i.e., stations using 802.11b in 802.11g BSS)
num_sta_no_short_slot_time	Number of associated stations, that do not support Short Slot Time
num_sta_no_short_preamble	Number of associated stations, that do not support Short Preamble.

Table 62: Wi-Fi AP State

Data about connected clients is displayed as well.

Item	Description
STA	MAC address of associated station.
AID	STA's unique AID (1 .. 2007) or 0 if not yet assigned.

Table 63: Wi-Fi Client State

```

WiFi AP Status
-----
WiFi AP Status

hostapd state dump - Thu Apr 12 11:23:58 2012
num_sta=1 num_sta_non_erp=0 num_sta_no_short_slot_time=0
num_sta_no_short_preamble=1

STA=00:b0:8c:01:0d:81
  AID=1 flags=0xa23 [AUTH][ASSOC][AUTHORIZED][WMM]
  capability=0x401 listen_interval=3
  supported_rates=82 84 8b 96 0c 12 18 24 30 48 60 6c
  timeout_next=NULLFUNC POLL

```

Fig. 75: Wi-Fi AP Status

### 3.2. WLAN DHCP

The DHCP server provides automatic configuration of devices connected to the network managed by the router. The DHCP server assigns IP address, netmask, default gateway (IP address of router) and DNS server (IP address of router) to each device.

The following table lists the information that is displayed in the DHCP status window for each attached client.

Item	Description
lease	Assigned IP address
starts	Time of assignation of IP address
ends	Time of termination IP address validity
hardware ethernet	Hardware MAC (unique) address
uid	Unique ID
client-hostname	Computer name

**Table 64: Lease Address**

DHCP Status	
Active DHCP Leases	
lease 192.168.3.2 {	
starts 4 2012/04/12 11:26:21;	
ends 4 2012/04/12 11:36:21;	
hardware ethernet 00:b0:8c:01:0d:81;	
uid 01:00:b0:8c:01:0d:81;	
client-hostname "felgr2";	
}	

**Fig. 76: Wi-Fi DHCP Status**

### 3.3. Wireless Network Scanning

Press **“Scan”** to scan neighboring Wi-Fi networks. Scanning can only be performed if the access point (Wi-Fi AP) is OFF.

Item	Description
BSS	MAC address of access point (AP).
TSF	A Timing Synchronization Function (TSF) keeps the timers for all stations in the same Basic Service Set (BSS) synchronized. All stations shall maintain a local TSF timer.
freq	Frequency band of access point (AP).
beacon interval	Period of time synchronization [kus] (1,024ms).
capability	List of access point (AP) characteristic.
signal	Signal level of access point (AP).
last seen	Last response time of access point (AP).
SSID	Identifier for access point (AP).
Supported rates	Supported rates of access point (AP).
DS Parameter set	The channel on which broadcast access point (AP).

**Table 65: Neighboring Wi-Fi networks**

```

WiFi Scan
-----
List of BSSs

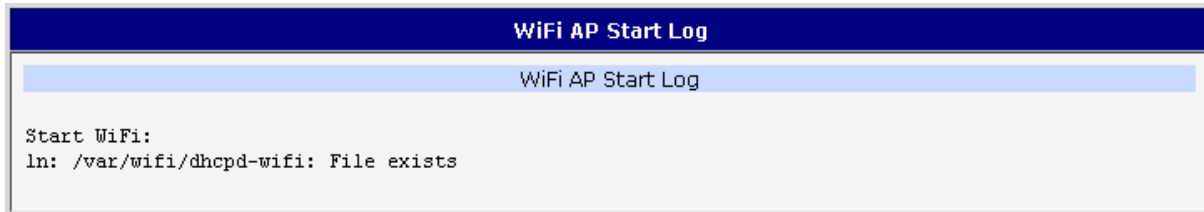
BSS 00:3a:98:eb:5a:30 (on wlan0)
  TSF: 25078863769996 usec (290d, 06:21:03)
  freq: 2467
  beacon interval: 100
  capability: ESS Privacy ShortPreamble ShortSlotTime (0x0431)
  signal: -61.00 dBm
  last seen: 230 ms ago
  Information elements from Probe Response frame:
  SSID: conel
  Supported rates: 1.0* 2.0* 5.5* 6.0 9.0 11.0* 12.0 18.0
  DS Parameter set: channel 12
  ERP:
  RSN:
    * Version: 1
    * Group cipher: TKIP
    * Pairwise ciphers: CCMP TKIP
    * Authentication suites: PSK
    * Capabilities: 4-PTKSA-RC 4-GTKSA-RC (0x0028)
  Extended supported rates: 24.0 36.0 48.0 54.0
  VHM:
    * Parameter version 1
    * u-APSD
    * BE: CW 15-1023, AIFSN 3
    * BK: CW 15-1023, AIFSN 7
    * VI: CW 7-15, AIFSN 2, TXOP 6016 usec
    * VO: CW 3-7, AIFSN 2, TXOP 3264 usec

```

**Fig. 77: Wi-Fi Scan**

### 3.4. Wi-Fi Start Log

If there is some problem starting Wi-Fi connections, check the **“Start Log”** in the **“Status “** section. It will display error reports that correspond to one or more components of the Wi-Fi AP. The basic component Wi-Fi AP (hostapd) is the exception. This component writes its log entries to the System Log.



```

WiFi AP Start Log

WiFi AP Start Log

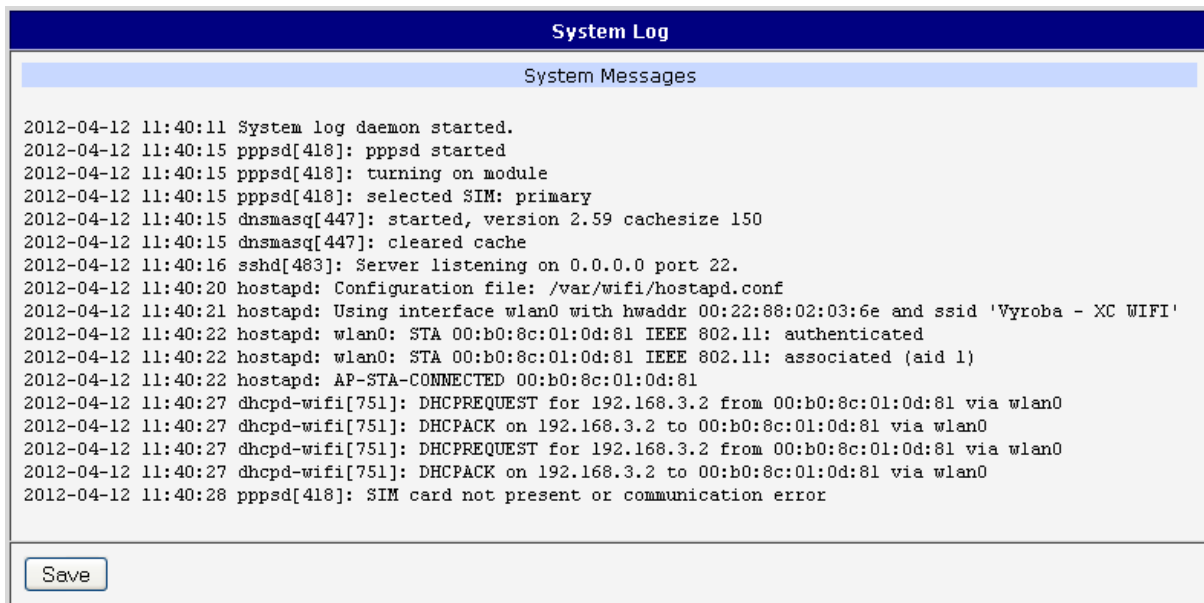
Start WiFi:
ln: /var/wifi/dhcpd-wifi: File exists

```

Fig. 78: Wi-Fi AP Start Log

### 3.5. System Log

If there are problems with Wi-Fi connections you can view the system log by pressing the **“System Log”** menu item. You will see detailed reports from individual applications running in the router. Wi-Fi AP activity is indicated in rows starting “hostapd” or “dhcpd-wifi”. Press the “Save” button to save the system log to the computer.



```

System Log

System Messages

2012-04-12 11:40:11 System log daemon started.
2012-04-12 11:40:15 pppsd[418]: pppsd started
2012-04-12 11:40:15 pppsd[418]: turning on module
2012-04-12 11:40:15 pppsd[418]: selected SIM: primary
2012-04-12 11:40:15 dnsmasq[447]: started, version 2.59 cachesize 150
2012-04-12 11:40:15 dnsmasq[447]: cleared cache
2012-04-12 11:40:16 sshd[483]: Server listening on 0.0.0.0 port 22.
2012-04-12 11:40:20 hostapd: Configuration file: /var/wifi/hostapd.conf
2012-04-12 11:40:21 hostapd: Using interface wlan0 with hwaddr 00:22:88:02:03:6e and ssid 'Vyroba - XC WIFI'
2012-04-12 11:40:22 hostapd: wlan0: STA 00:b0:8c:01:0d:81 IEEE 802.11: authenticated
2012-04-12 11:40:22 hostapd: wlan0: STA 00:b0:8c:01:0d:81 IEEE 802.11: associated (aid 1)
2012-04-12 11:40:22 hostapd: AP-STA-CONNECTED 00:b0:8c:01:0d:81
2012-04-12 11:40:27 dhcpd-wifi[751]: DHCPREQUEST for 192.168.3.2 from 00:b0:8c:01:0d:81 via wlan0
2012-04-12 11:40:27 dhcpd-wifi[751]: DHCPACK on 192.168.3.2 to 00:b0:8c:01:0d:81 via wlan0
2012-04-12 11:40:27 dhcpd-wifi[751]: DHCPREQUEST for 192.168.3.2 from 00:b0:8c:01:0d:81 via wlan0
2012-04-12 11:40:27 dhcpd-wifi[751]: DHCPACK on 192.168.3.2 to 00:b0:8c:01:0d:81 via wlan0
2012-04-12 11:40:28 pppsd[418]: SIM card not present or communication error

Save

```

Fig. 79: System Log

### 3.6. Wi-Fi Access Point Configuration

The configuration page for the Wi-Fi access point is displayed by selecting **Wi-Fi AP** item in **Configuration** section.

Item	Description
Enable Wi-Fi AP	If this item is checked, Wi-Fi AP is enabled.
SSID	Identifier of Wi-Fi network.
Broadcast SSID	Method of broadcasting the SSID in beacon frames and response to a request for sending the beacon frame. <ul style="list-style-type: none"> <li>• Enabled – SSID is broadcast in beacon frames.</li> <li>• Zero length – Beacon frame does not include SSID. Requests for sending beacon frame are ignored.</li> <li>• Clear – All SSID characters in beacon frames are replaced by 0. Original length is kept. Requests for sending beacon frames are ignored.</li> </ul>
Country Code	Code of the country where the router is installed. This code must be entered in <b>ISO 3166-1 alpha-2 format</b> . If a country code isn't specified and the router has not implemented a system to determine this code, it will use "US" as the default country code .  If no country code is specified or if the wrong country code is entered, then the router may violate country-specific regulations for the use of the Wi-Fi frequency bands.
HW Mode	HW mode of Wi-Fi standard that will be supported by Wi-Fi access point. <ul style="list-style-type: none"> <li>• IEE 802.11b</li> <li>• IEE 802.11b+g</li> <li>• IEE 802.11b+g+n</li> </ul>
Channel	The channel, where the Wi-Fi AP is transmitting.
BW 40 MHz	The option for HW mode 802.11n which allows transmission on two standard 20MHz channels simultaneously.
WMM	Basic QoS for Wi-Fi networks is enabled by checking this item. This version doesn't guarantee network throughput. It is suitable for simple applications that require QoS.
Authentication	Access control and authorization of users in the Wi-Fi network. <ol style="list-style-type: none"> <li>1. Open - Authentication is not required. Free access point.</li> <li>2. Shared – Base authentication using WEP key.</li> <li>3. WPA-PSK - Authentication using better authentication methods PSK-PSK.</li> <li>4. WPA2-PSK - WPA-PSK using new encryption AES.</li> </ol>
Encryption	Type of data encryption in the Wi-Fi network <ul style="list-style-type: none"> <li>• None – No data encryption.</li> <li>• WEP – Encryption using static WEP keys. This encryption can be used for Shared authentication.</li> <li>• TKIP – Dynamic encryption key management that can be used</li> </ul>



	for WPA-PSK and WPA2-PSK authentication.
	<ul style="list-style-type: none"> <li>• AES - Improved encryption used for WPA2-PSK authentication.</li> </ul>
WEP Key Type	Type of WEP key for WEP encryption. <ul style="list-style-type: none"> <li>• ASCII – WEP key in ASCII format</li> <li>• HEX – WEP key in hexadecimal format</li> </ul>
WEP Default Key	This item specifies default WEP key.
WEP Key X	Items for different 4 WEP keys. <ul style="list-style-type: none"> <li>• 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"> <li>• 5 ASCII characters (40b WEP key)</li> <li>• 13 ASCII characters ( 104b WEP key)</li> <li>• 16 ASCII characters (128b WEP key)</li> </ul> </li> <li>• WEP key must be entered in hexadecimal digits. This key can be specified in the following lengths. <ul style="list-style-type: none"> <li>• 10 hexadecimal digits (40b WEP key)</li> <li>• 26 hexadecimal digits ( 104b WEP key)</li> <li>• 32 hexadecimal digits (128b WEP key)</li> </ul> </li> </ul>
WPA PSK Type	Type of key for WPA-PSK authentication. <ul style="list-style-type: none"> <li>• 256-bit secret</li> <li>• ASCII passphrase</li> <li>• PSK File</li> </ul>
WPA PSK	Key for WPA-PSK authentication. This key must be entered according to the selected WPA PSK type as follows. <ul style="list-style-type: none"> <li>• 256-bit secret - 64 hexadecimal digits</li> <li>• ASCII passphrase – 8 to 63 characters</li> <li>• PSK File – absolute path to the file containing the list of pairs (PSK key, MAC address)</li> </ul>
Access List	Mode of Access/Deny list. <ul style="list-style-type: none"> <li>• Disabled – Accept/Deny list is not used.</li> <li>• Accept – Clients in Accept/Deny list can access the network.</li> <li>• Deny – Clients in Access/Deny list cannot access the network.</li> </ul>
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"> <li>• Verbose debugging – The highest level of logging.</li> <li>• Debugging</li> <li>• Informational – Default level of logging</li> <li>• Notification</li> <li>• Warning – The lowest level of communicativeness.</li> </ul>

**Table 66: Wi-Fi AP Parameters**



WiFi Configuration

Enable WiFi AP

SSID

Broadcast SSID Enabled

Country Code \*

HW Mode IEEE 802.11b

Channel

BW 40 MHz

WMM

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

Access List Disabled

Accept/Deny List

Syslog Level Informational

Extra options \*

**Fig. 80: Wi-Fi AP Configuration Page**

### 3.7. WLAN Configuration

The Wi-Fi LAN and DHCP server page is displayed by selecting “**WLAN**” in the configuration section.

Item	Description
Enable WLAN interface	If this item is checked, Wi-Fi LAN is enabled.
IP Address	Fixed IP address of Wi-Fi network interface.
Subnet mask	Subnet Mask of Wi-Fi network interface.
Bridged	<ul style="list-style-type: none"> <li>No - Bridged mode is not allowed. WLAN network is not connected with LAN router.</li> <li>Yes - Bridged mode is allowed. WLAN network is connected with one or more LAN network in router. In this case, the setting of most items in this table is ignored. Instead, it takes setting of selected network interface (LAN).</li> </ul>
Enable dynamic DHCP leases	If this option is checked, dynamic DHCP server is enabled.
IP Pool Start	Start IP addresses space.
IP Pool End	End IP addresses space
Lease Time	Time in seconds that the IP Address is available to the client

**Table 67: WLAN Parameter**

**Fig. 81: WLAN Configuration**

### 3.8. Wi-Fi Port LEDs

LED port indicator	
Green LED	Wi-Fi port is powered on.
Yellow LED	Permanently off.

**Table 68: Wi-Fi LED State Indication**