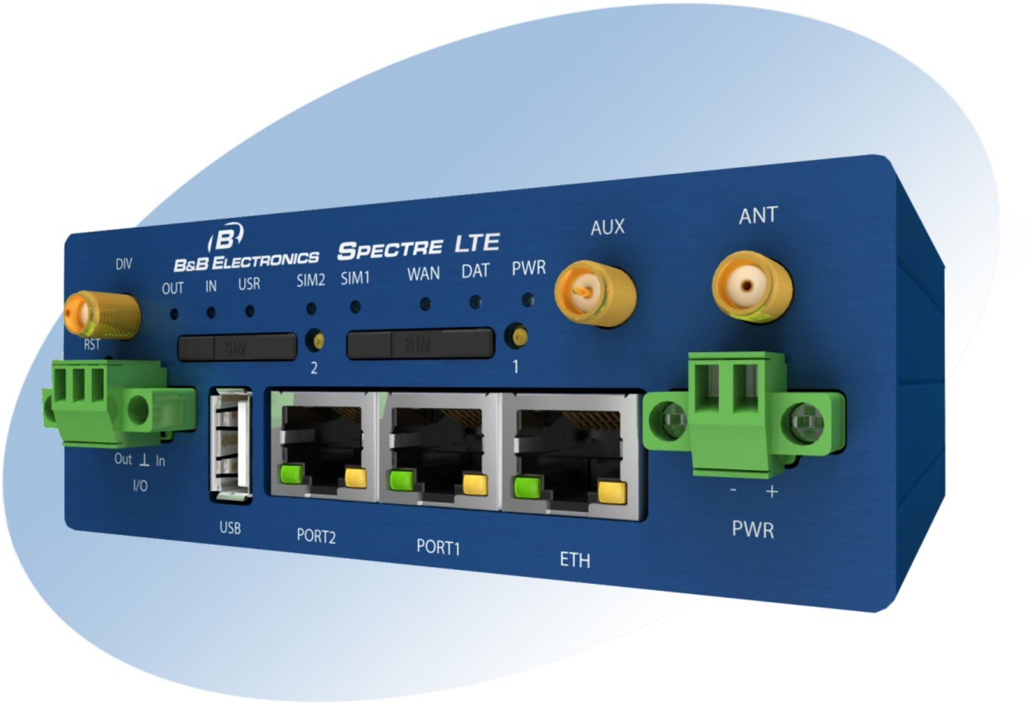
SPECTRE Router

CONFIGURATION MANUAL



B+B SMARTWORX®

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- smartworx.com**
support@bb-smartworx.com

European Headquarters

B&B Electronics
Westlink Commercial Park
Oranmore, Co. Galway, Ireland

Phone +353 91-792444 -- **Fax** +353 91-792445
Website: http://www.bb-elec.com
techsupport@bb- smartworx.com

Document: SPECTRE_Configuration_Manual_R5_4314m

CONTENTS

TABLE LIST

FIGURE LIST

DOCUMENT INFORMATION

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.

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

1. ROUTER CONFIGURATION USING A WEB BROWSER

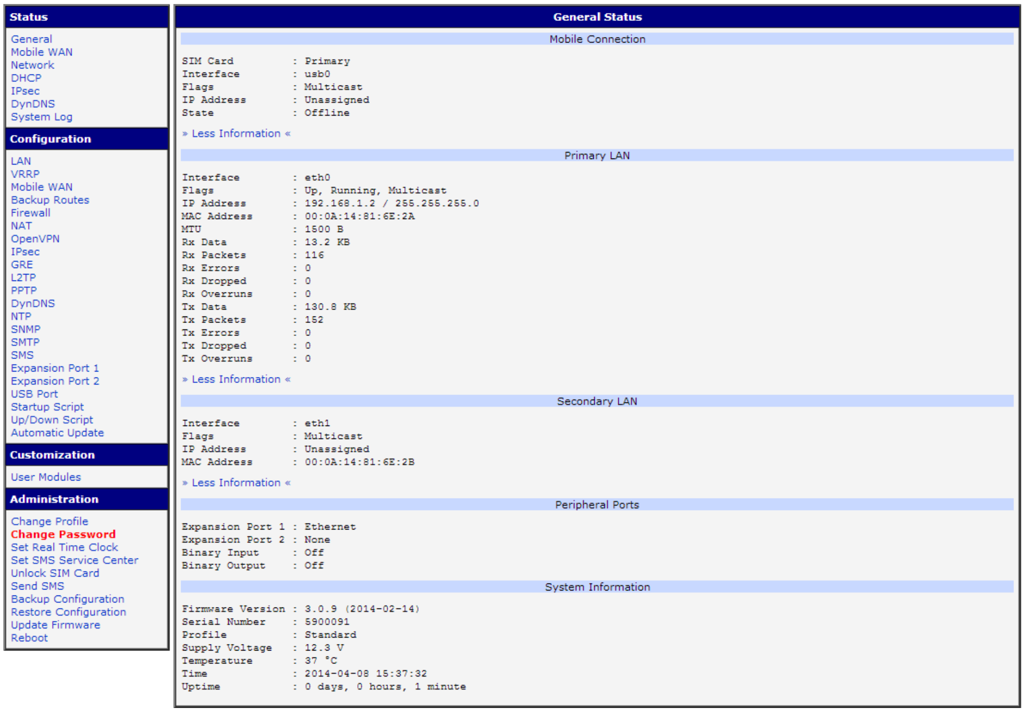
Attention! The SPECTRE cellular router will not operate unless the cellular carrier has been correctly configured and the account activated and provisioned for data communications. For UMTS and LTE carriers, a SIM card must be inserted into the router. Do not insert the SIM card when the router is powered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



General Status

Mobile Connection

```
SIM Card          : Primary
Interface         : usb0
Flags             : Multicast
IP Address        : Unassigned
State             : Offline
```

Primary LAN

```
Interface         : eth0
Flags             : Up, Running, Multicast
IP Address        : 192.168.1.2 / 255.255.255.0
MAC Address       : 00:0A:14:81:6E:2A
MTU               : 1500 B
Rx Data           : 13.2 KB
Rx Packets        : 116
Rx Errors         : 0
Rx Dropped        : 0
Rx Overruns       : 0
Tx Data           : 130.8 KB
Tx Packets        : 152
Tx Errors         : 0
Tx Dropped        : 0
Tx Overruns       : 0
```

Secondary LAN

```
Interface         : eth1
Flags             : Multicast
IP Address        : Unassigned
MAC Address       : 00:0A:14:81:6E:2B
```

Peripheral Ports

```
Expansion Port 1 : Ethernet
Expansion Port 2 : None
Binary Input     : Off
Binary Output    : Off
```

System Information

```
Firmware Version : 3.0.9 (2014-02-14)
Serial Number    : 5900091
Profile          : Standard
Supply Voltage   : 12.3 V
Temperature      : 37 °C
Time             : 2014-04-08 15:37:32
Uptime           : 0 days, 0 hours, 1 minute
```

Figure 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.)

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.

GENERAL

A summary of basic information about the router and its activities can be invoked by selecting the ***General*** menu item. This page is also displayed when you login to the web interface. Information is divided into several of separate blocks according to the type of router activity or the properties area – Mobile Connection, Primary LAN, Peripherals Ports and System Information. If your router is equipped with a WI-FI expansion port, there is also a WI-FI section.

MOBILE CONNECTION

Table 1: Mobile Connection

Item	Description
SIM Card	Identification of the SIM card (Primary or Secondary)
Interface	Defines the interface
Flags	Defines the flags (Example: Up, Running, Multicast)
IP address	IP address of the interface
MTU	Maximum packet size that the equipment is able to transmit
Rx Data	Total number of received bytes
Rx Packets	Received packets
Rx Errors	Erroneous received packets
Rx Dropped	Dropped received packets
Rx Overruns	Lost received packets because of overload
Tx Data	Total number of sent bytes
Tx Packets	Sent packet
Tx Errors	Erroneous sent packets
Tx Dropped	Dropped sent packets
Tx Overruns	Lost sent packets because of overload
Uptime	Time indicating how long the connection to mobile network is established

PRIMARY LAN

Items displayed in this part have the same meaning as items in the previous part. Moreover, there is information about the MAC address of the router (MAC Address item).

WIFI

Items displayed in this part have the same meaning as items in the previous part. (This is displayed if your model has a WI-FI.)

PERIPHERAL PORTS

Table 2: Peripheral ports

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

SYSTEM INFORMATION

Table 3: System information

Item	Description
Firmware Version	Information about the firmware Version
Serial Number	Serial number of the router (in case of N/A is not available)
Profile	Current profile – standard or alternative profiles (profiles are used for example to switch between different modes of operation)
Supply Voltage	Supply voltage of the router
Temperature	Temperature in the router
Time	Current date and time
Uptime	Time indicating how long the router is used

MOBILE WAN STATUS

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

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

Table 4: Cellular network information

Item	Description
Registration	State of the network registration
Operator	Specifies the operator in whose network the router is operated
Technology	Transmission technology
PLMN	Code of operator
Cell	Cell to which the router is connected
LAC	Located Area Code – unique number assigned to each location area
Channel	Channel on which the router communicates
Signal Strength	Signal strength of the selected cell
Signal Quality	Signal quality of the selected cell: • EC/IO for UMTS and CDMA technologies (It is the ratio of the signal received from the pilot channel – EC – to the overall level of the spectral density, i.e. the sum of the signals of other cells – IO.) • RSRQ for LTE technology (Defined as the ratio (N x RSRP) / RSSI)
Neighbors	Signal quality of neighboring hearing cells
Manufacturer	Module Manufacturer
Model	Type of module
Revision	Revision of module
IMEI	IMEI (International Mobile Equipment Identity) number of module
ESN	ESN (Electronic Serial Number) number of module (for CDMA routers)
MEID	MEID (Mobile Equipment Identifier) number of module

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.

Table 5: Description of period

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

Table 6: Mobile network statistics

Item	Description
Signal Min	Minimal signal strength
Signal Avg	Average signal strength
Signal Max	Maximal signal strength
Cells	Number of switch between cells
Availability	Availability of the router via the mobile network (expressed as a percent-age)

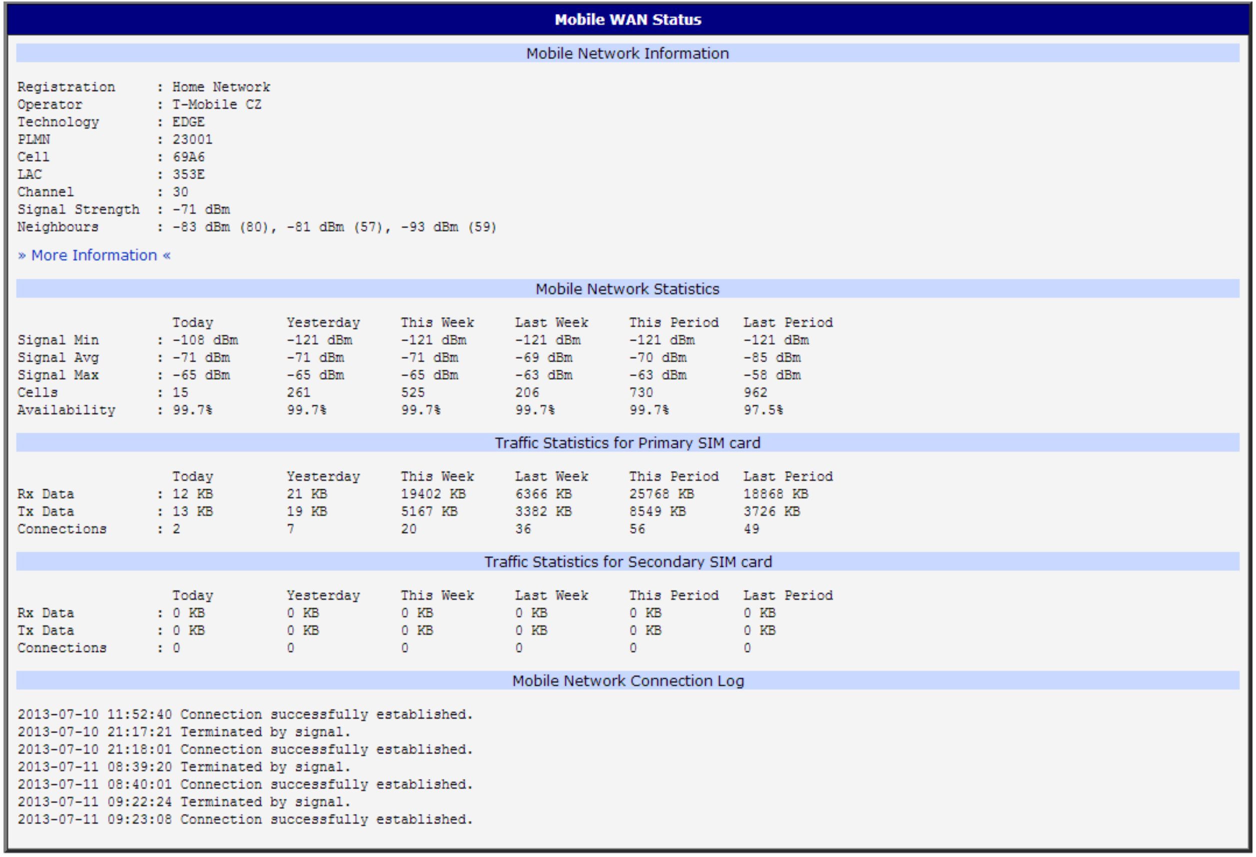
Tips for Mobile Network Statistics table:

- Availability of connection to mobile network information is expressed as a percentage that is calculated by the ratio of the time when connection to a mobile network is established to the time when the router is turned on.
- When you place your cursor on the maximum or minimum signal strength, you will be shown the last time the router reached this signal strength. The middle part of this page displays information about transferred data and number of connections for both SIM card (for each period).

Table 7: Traffic statistics

Item	Description
RX data	Total volume of received data
TX data	Total volume of sent data
Connections	Number of connection to mobile network establish

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



Mobile WAN Status

Mobile Network Information

```
Registration     : Home Network
Operator         : T-Mobile CZ
Technology       : EDGE
PLMN             : 23001
Cell             : 69A6
LAC              : 353E
Channel          : 30
Signal Strength  : -71 dBm
Neighbours       : -83 dBm (80), -81 dBm (57), -93 dBm (59)
```

» More Information «

Mobile Network Statistics

```
                   Today         Yesterday     This Week     Last Week     This Period   Last Period
Signal Min       : -108 dBm      -121 dBm      -121 dBm      -121 dBm      -121 dBm      -121 dBm
Signal Avg       : -71 dBm       -71 dBm       -71 dBm       -69 dBm       -70 dBm       -85 dBm
Signal Max       : -65 dBm       -65 dBm       -65 dBm       -63 dBm       -63 dBm       -58 dBm
Cells            : 15            261           525           206           730           962
Availability     : 99.7%         99.7%         99.7%         99.7%         99.7%         97.5%
```

Traffic Statistics for Primary SIM card

```
                   Today         Yesterday     This Week     Last Week     This Period   Last Period
Rx Data          : 12 KB         21 KB         19402 KB      6366 KB       25768 KB      18868 KB
Tx Data          : 13 KB         19 KB         5167 KB       3382 KB       8549 KB       3726 KB
Connections      : 2             7             20            36            56            49
```

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
```

Mobile Network Connection Log

```
2013-07-10 11:52:40 Connection successfully established.
2013-07-10 21:17:21 Terminated by signal.
2013-07-10 21:18:01 Connection successfully established.
2013-07-11 08:39:20 Terminated by signal.
2013-07-11 08:40:01 Connection successfully established.
2013-07-11 09:22:24 Terminated by signal.
2013-07-11 09:23:08 Connection successfully established.
```

Figure 2: Mobile WAN Status

NETWORK STATUS

Select the Network menu item to view the current system information for the router. The upper part of the window displays detailed information about the active interfaces.

Table 8: Interface connection status

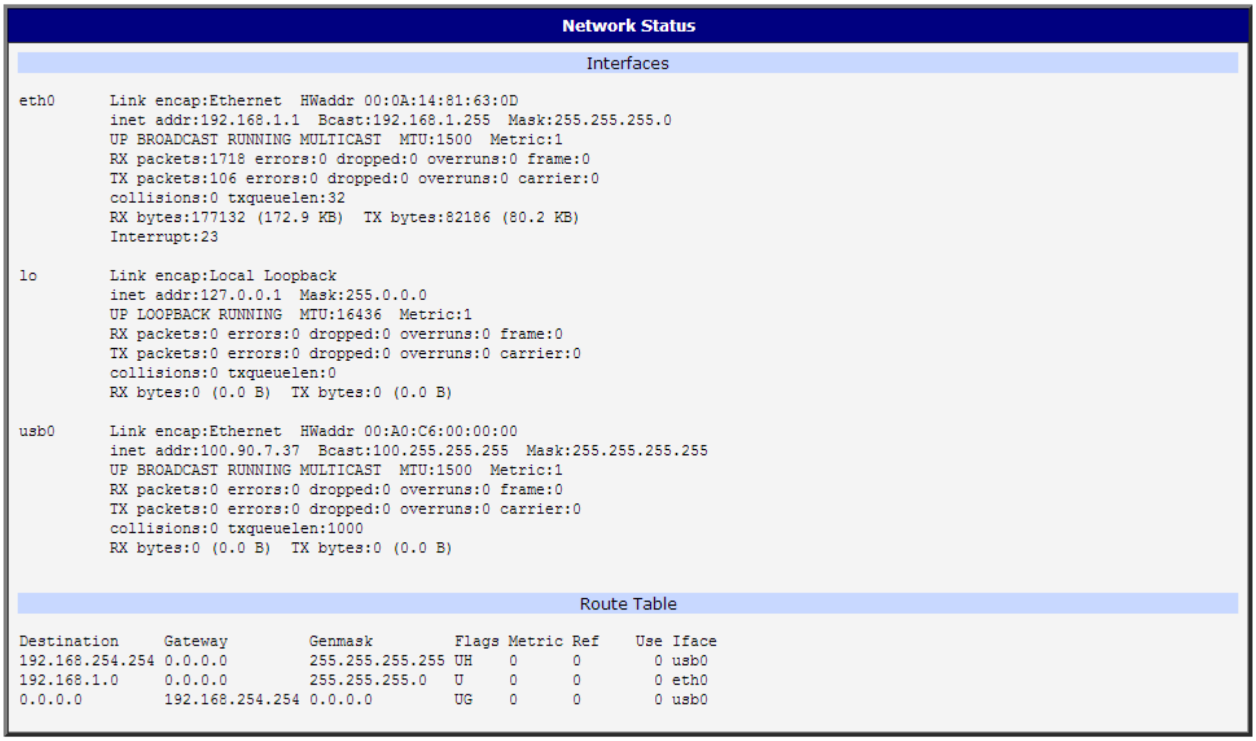
Interface	Description
eth0, eth1	Network interfaces

usb0	Mobile Network interface (active connection to GPRS/EDGE/CDMA/LTE)
tun0	OpenVPN tunnel interface
ipsec0	IPSec tunnel interface
gre1	GRE tunnel interface
ppp0	PPPoE interface (Industrial RT Router only)
lo	Local loopback interface

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

Table 9: Description of information in network status

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	• packets – number of received packets • errors – number of errors • dropped – number of dropped packets • overruns – incoming packets lost because of overload • frame – number of frame errors
TX	• packets – number of transmitted packets • errors – number of packet errors • dropped – number of dropped packets • overruns – number of outgoing packets lost because of overload • carrier - outgoing packet errors resulting from the physical layer
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



```
eth0      Link encap:Ethernet  HWaddr 00:0A:14:81:63:0D
          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:1718 errors:0 dropped:0 overruns:0 frame:0
          TX packets:106 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:32
          RX bytes:177132 (172.9 KB)  TX bytes:82186 (80.2 KB)
          Interrupt:23

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

usb0      Link encap:Ethernet  HWaddr 00:A0:C6:00:00:00
          inet addr:100.90.7.37  Bcast:100.255.255.255  Mask:255.255.255.255
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.254.254 0.0.0.0         255.255.255.255 UH    0      0        0 usb0
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
0.0.0.0         192.168.254.254 0.0.0.0         UG    0      0        0 usb0
```

Figure 3: Network Status

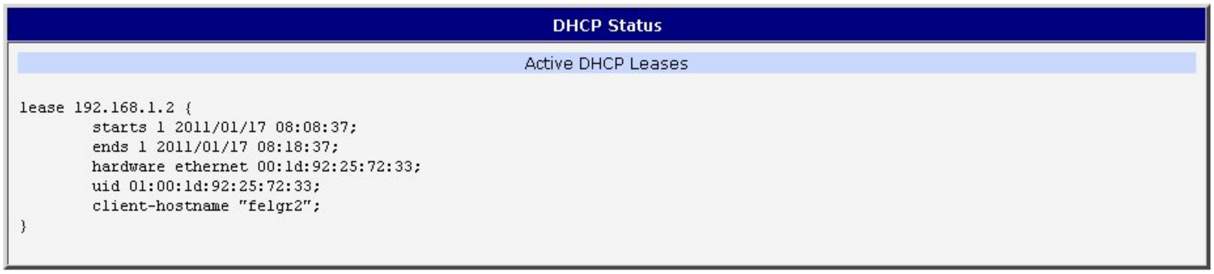
DHCP STATUS

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.

Table 10: DHCP status description

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



```
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";
}
```

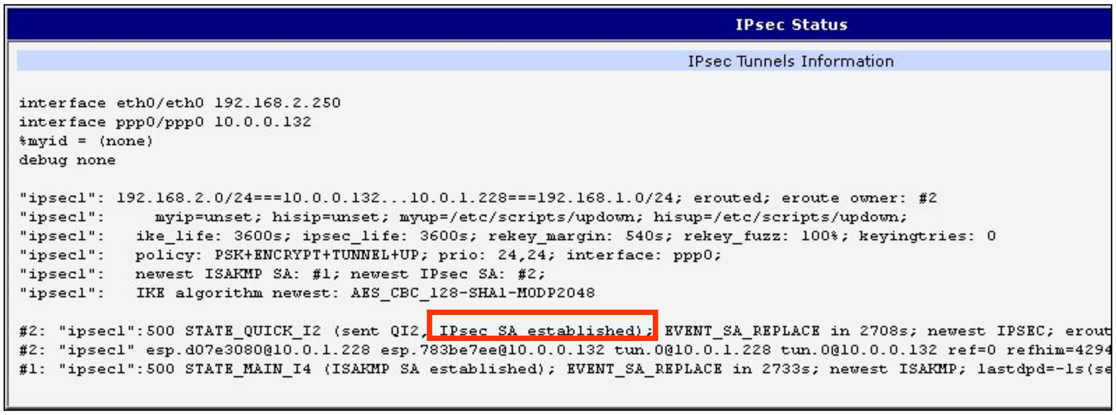
Figure 4: DHCP Status

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

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.

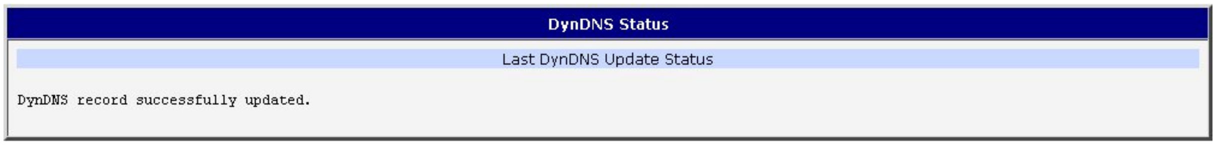


```
interface eth0/eth0 192.168.2.250
interface ppp0/ppp0 10.0.0.132
%myid = (none)
debug none

"ipsec1": 192.168.2.0/24===10.0.0.132...10.0.1.228===192.168.1.0/24; erouted; eroute owner: #2
"ipsec1":     myip=unset; hisip=unset; myup=/etc/scripts/updown; hisup=/etc/scripts/updown;
"ipsec1":   ike_life: 3600s; ipsec_life: 3600s; rekey_margin: 540s; rekey_fuzz: 100%; keyingtries: 0
"ipsec1":   policy: PSK+ENCRYPT+TUNNEL+UP; prio: 24,24; interface: ppp0;
"ipsec1":   newest ISAKMP SA: #1; newest IPsec SA: #2;
"ipsec1":   IKE algorithm newest: AES_CBC_128-SHA1-MODP2048

#2: "ipsec1":500 STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in 2708s; newest IPSEC; erout
#2: "ipsec1" esp.d07e3080@10.0.1.228 esp.783be7ee@10.0.0.132 tun.0@10.0.1.228 tun.0@10.0.0.132 ref=0 refhim=4294
#1: "ipsec1":500 STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in 2733s; newest ISAKMP; lastdpd=-1s(se
```

Figure 5: IPsec Status

DYNDNS STATUS

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



```
DynDNS record successfully updated.
```

Figure 6: DynDNS status

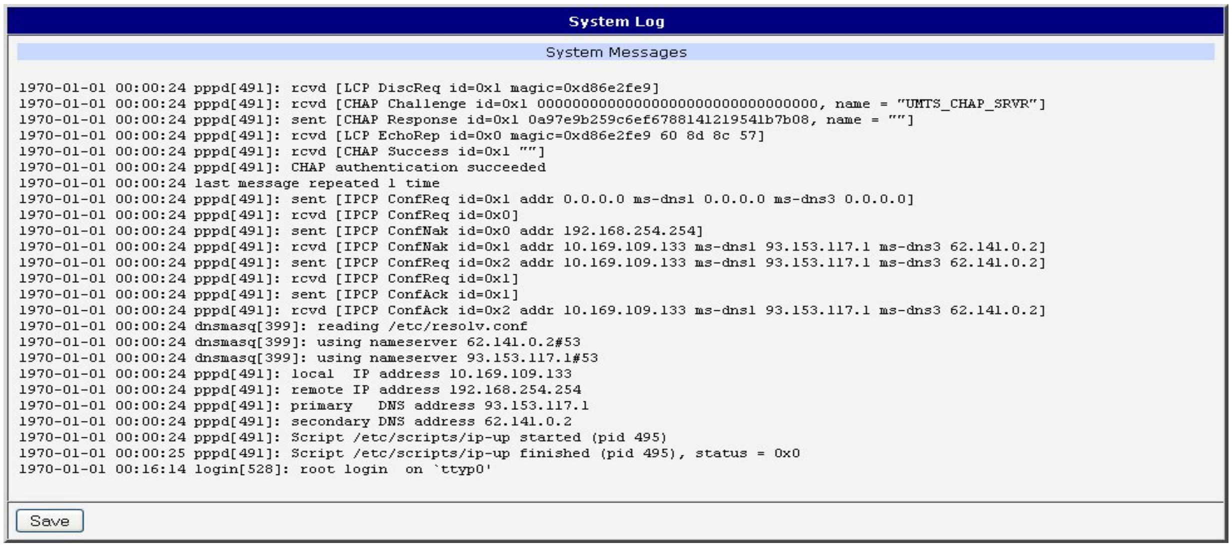
Table 11: DynDNS report

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.

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

SYSTEM LOG

Use the ***System Log*** menu item to view the router system log. The system log contains helpful information about 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.



```
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 0a97e9b259c6ef6788141219541b7b08, 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 `ttyp0'
```

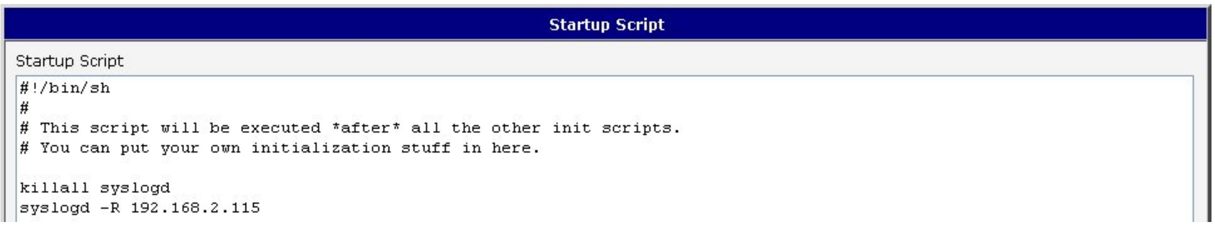
Figure 7: System log

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 a 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 insert 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

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

killall syslogd
syslogd -R 192.168.2.115
```

Figure 8: Example syslogd startup script with the parameter -r

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.

Table 12: Configuration of network interface

Item	Description
DHCP Client	• disabled – The router will not obtain an IP address automatically from a DHCP server on the network. • enabled – The router will attempt to obtain an IP address automatically from a DHCP server on the network.
IP address	Fixed IP address of the network interface.
Subnet Mask	IP address Subnet Mask for the interface.
Media type	• Auto-negotiation – The router automatically selects the communication speed of the network interface. • 100 Mbps Full Duplex – The router communicates at 100Mbps, in full-duplex mode. • 100 Mbps Half Duplex - The router communicates at 100Mbps, in half-duplex mode. • 10 Mbps Full Duplex - The router communicates at 10Mbps, in full-duplex mode. • 10 Mbps Half Duplex - The router communicates at 10Mbps, in half-duplex mode.
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.

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.

Table 13: Configuration of a dynamic DHCP server

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.

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, the network may function incorrectly.

Table 14: Configuration of static DHCP server

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

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).

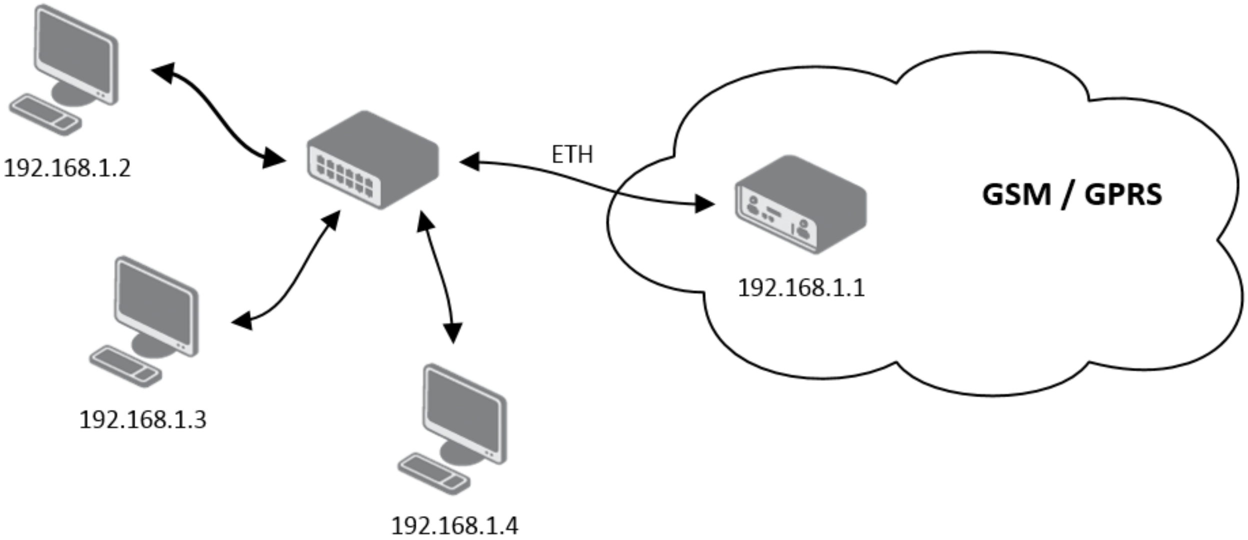
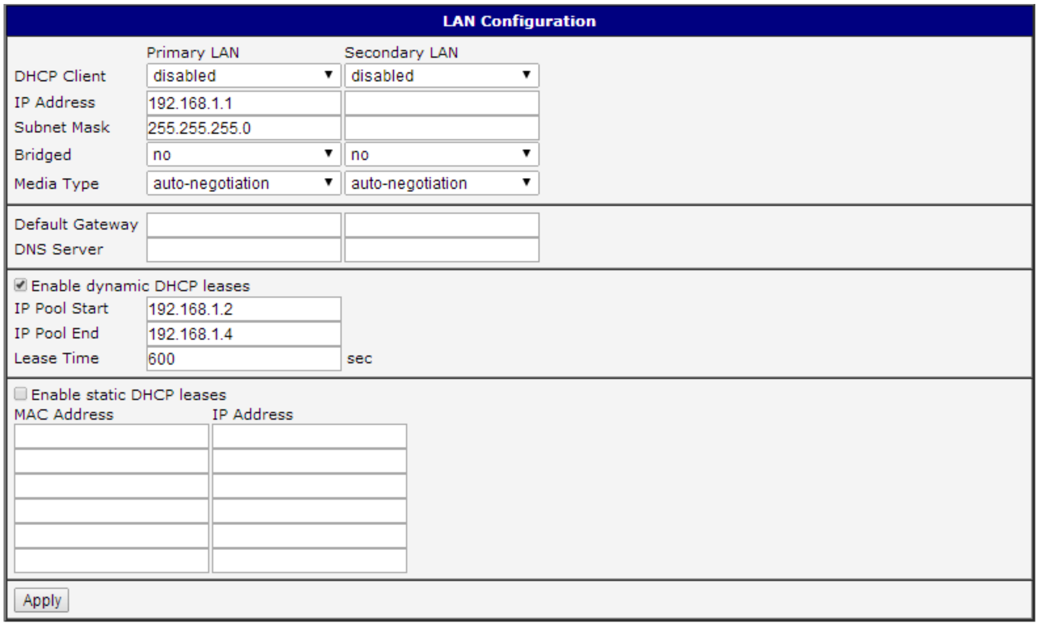


Figure 9: Example 1 - Network Topology for Dynamic DHCP Server



LAN Configuration

	Primary LAN	Secondary LAN
DHCP Client	disabled	disabled
IP Address	192.168.1.1	
Subnet Mask	255.255.255.0	
Bridged	no	no
Media Type	auto-negotiation	auto-negotiation
Default Gateway		
DNS Server		

☑ Enable dynamic DHCP leases

IP Pool Start	192.168.1.2	
IP Pool End	192.168.1.4	
Lease Time	600	sec

□ Enable static DHCP leases

MAC Address	IP Address

Figure 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.

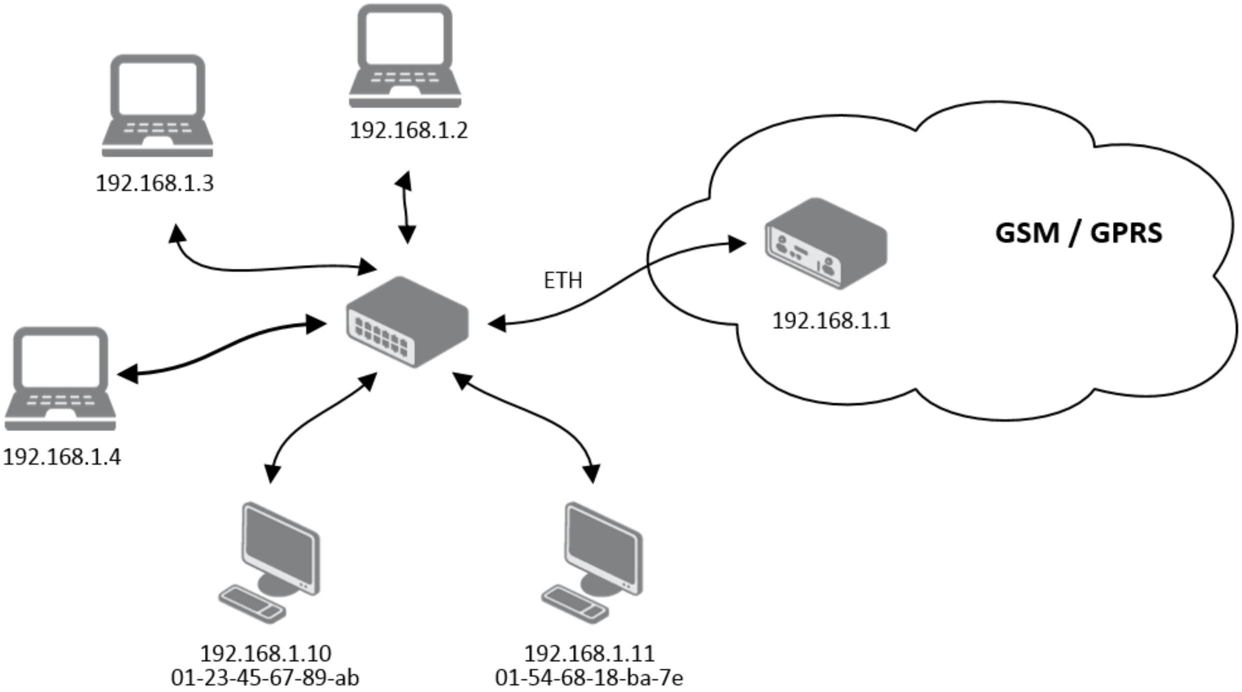
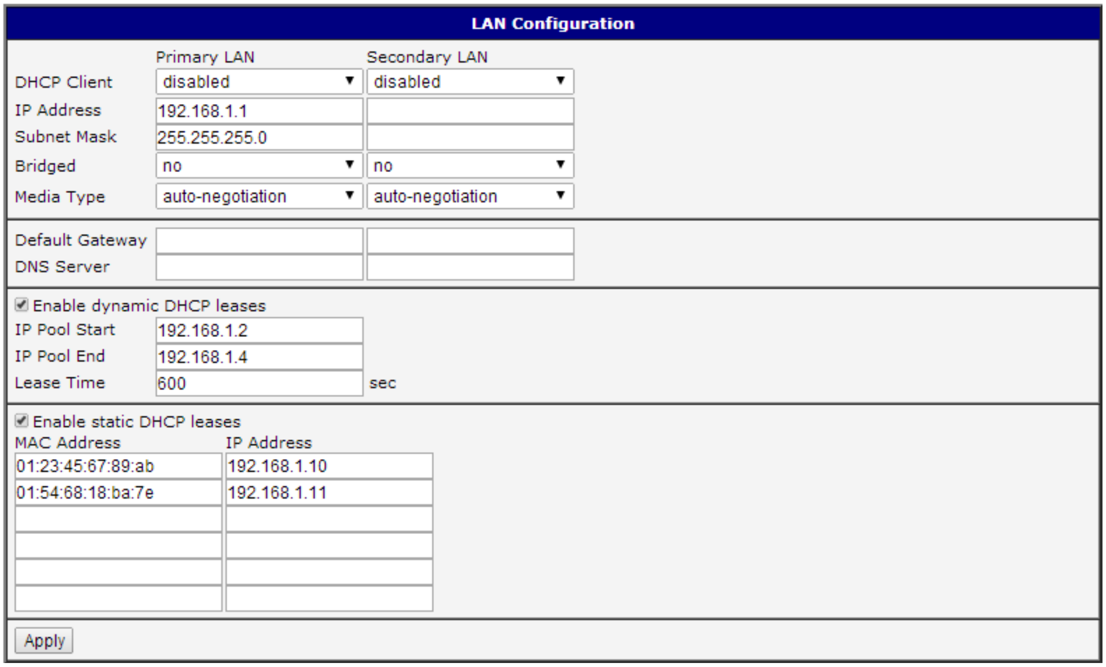


Figure 11: Example 2 - Network Topology with both Static and Dynamic DHCP Servers



LAN Configuration

	Primary LAN	Secondary LAN
DHCP Client	disabled ▼	disabled ▼
IP Address	192.168.1.1	
Subnet Mask	255.255.255.0	
Bridged	no ▼	no ▼
Media Type	auto-negotiation ▼	auto-negotiation ▼
Default Gateway		
DNS Server		

☑ Enable dynamic DHCP leases

IP Pool Start	192.168.1.2	
IP Pool End	192.168.1.4	
Lease Time	600	sec

☑ 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

Figure 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

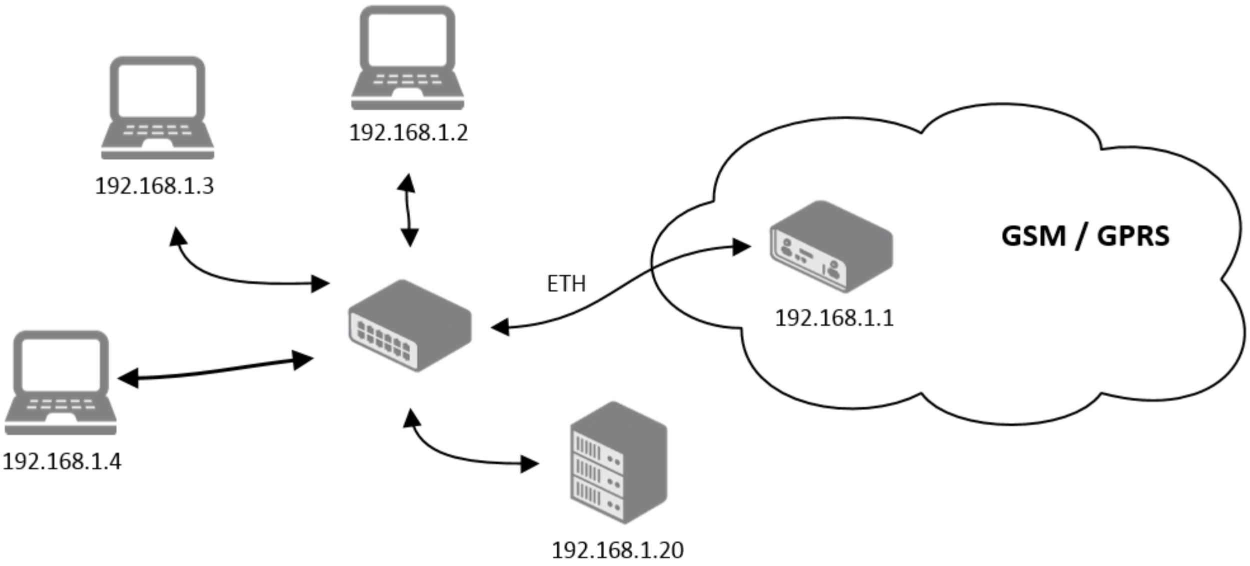
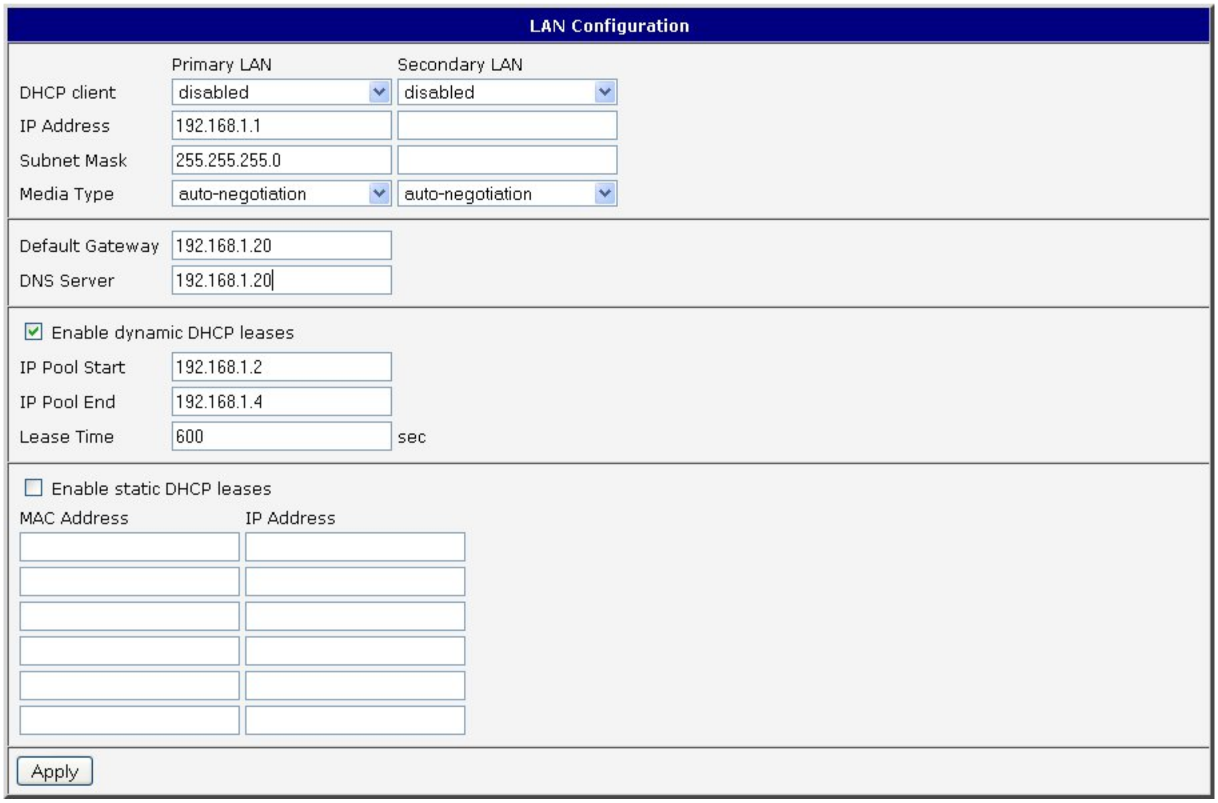


Figure 13: Example 3 - Network Topology



LAN Configuration

	Primary LAN	Secondary LAN
DHCP client	disabled	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

☑ Enable dynamic DHCP leases

IP Pool Start	192.168.1.2	
IP Pool End	192.168.1.4	
Lease Time	600	sec

☐ Enable static DHCP leases

MAC Address	IP Address

Figure 14: Example 3 - LAN Configuration Page

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 applications. If the ***Enable VRRP*** is checked, you may set the following parameters.

Table 15: VRRP configuration

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 *Host Priority*, is the main router. According to RFC 2338, the main router should have the highest possible priority - 255. The backup router(s) have a priority in the range 1 – 254 (default value is 100). A priority value of 0 is not allowed.

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

Table 16: Check connection

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

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

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

Example of the VRRP protocol:

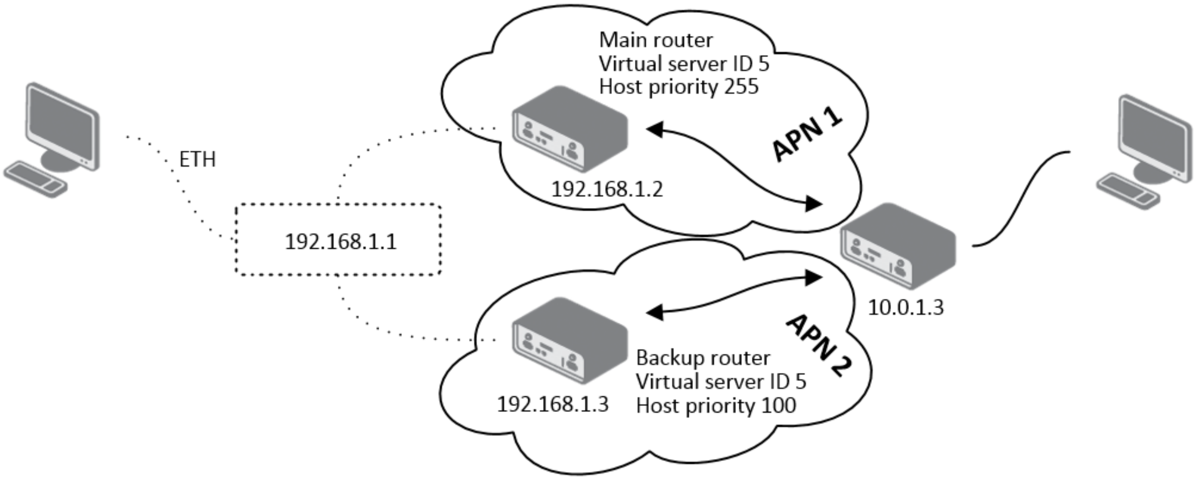
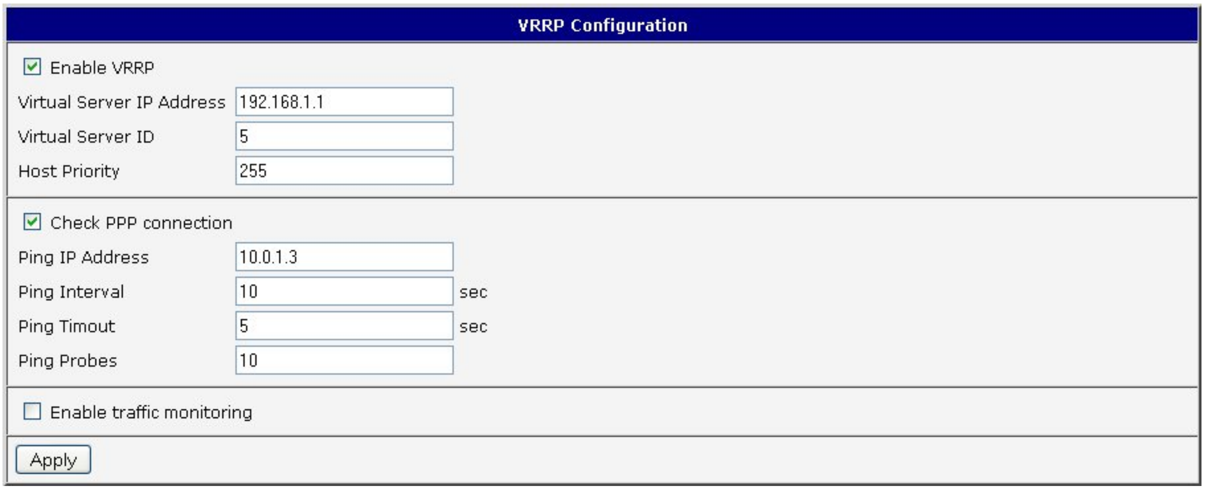


Figure 15: Example 4 - Network Topology for VRRP configuration



VRRP Configuration

☑ Enable VRRP

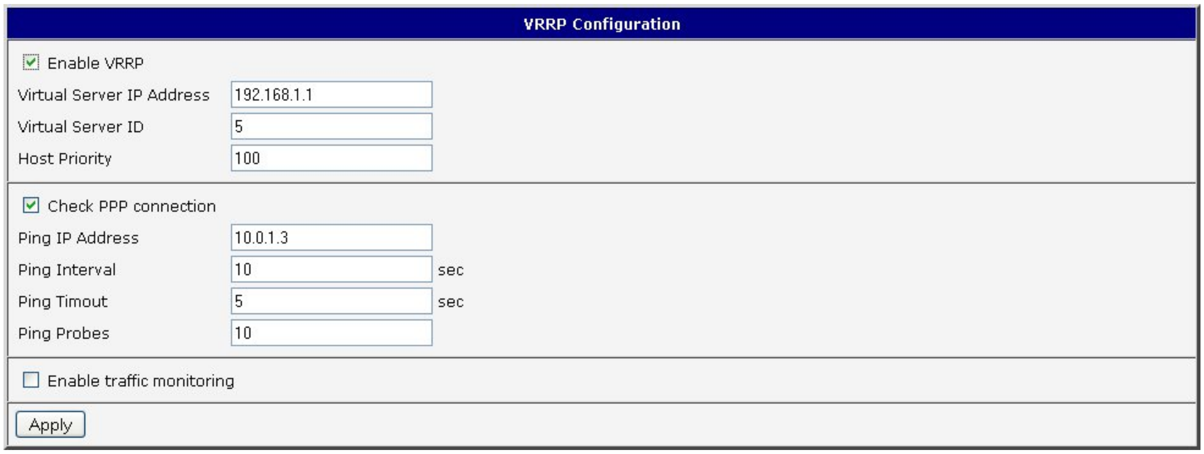
Virtual Server IP Address	192.168.1.1	
Virtual Server ID	5	
Host Priority	255	

☑ Check PPP connection

Ping IP Address	10.0.1.3	
Ping Interval	10	sec
Ping Timout	5	sec
Ping Probes	10	

☐ Enable traffic monitoring

Figure 16: Example 4 - VRRP configuration of main router



VRRP Configuration

☑ Enable VRRP

Virtual Server IP Address	192.168.1.1	
Virtual Server ID	5	
Host Priority	100	

☑ Check PPP connection

Ping IP Address	10.0.1.3	
Ping Interval	10	sec
Ping Timout	5	sec
Ping Probes	10	

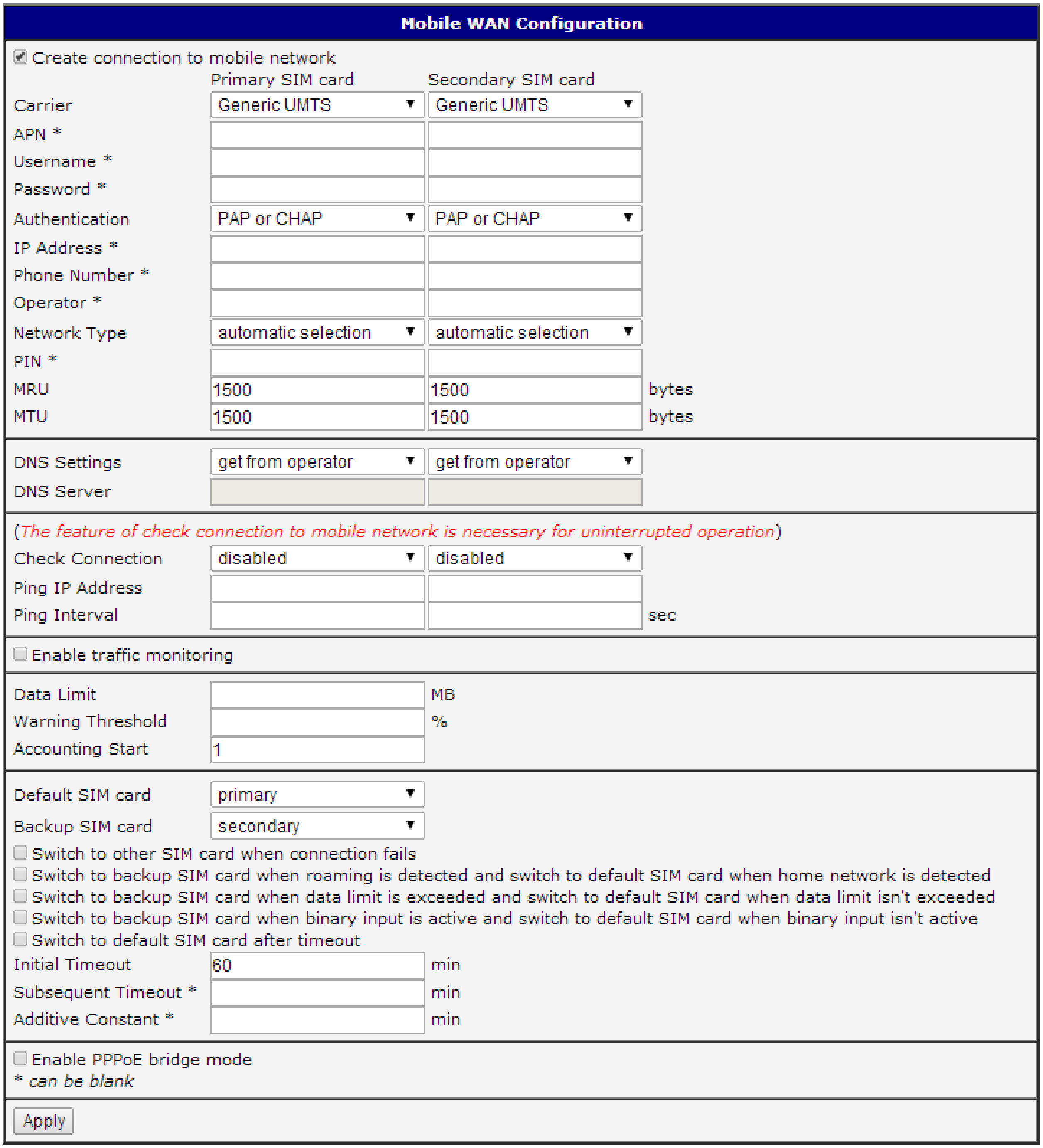
☐ Enable traffic monitoring

Figure 17. Example 4 - VRRP configuration of backup router

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.



Mobile WAN Configuration

☑ Create connection to mobile network

	Primary SIM card	Secondary SIM card	
Carrier	Generic UMTS ▼	Generic UMTS ▼	
APN *			
Username *			
Password *			
Authentication	PAP or CHAP ▼	PAP or CHAP ▼	
IP Address *			
Phone Number *			
Operator *			
Network Type	automatic selection ▼	automatic selection ▼	
PIN *			
MRU	1500	1500	bytes
MTU	1500	1500	bytes
DNS Settings	get from operator ▼	get from operator ▼	
DNS Server			

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

Check Connection	disabled ▼	disabled ▼	
Ping IP Address			
Ping Interval			sec

☐ Enable traffic monitoring

Data Limit		MB
Warning Threshold		%
Accounting Start	1	

Default SIM card	primary ▼
Backup SIM card	secondary ▼

☐ Switch to other SIM card when connection fails

☐ Switch to backup SIM card when roaming is detected and switch to default SIM card when home network is detected

☐ Switch to backup SIM card when data limit is exceeded and switch to default SIM card when data limit isn't exceeded

☐ Switch to backup SIM card when binary input is active and switch to default SIM card when binary input isn't active

☐ Switch to default SIM card after timeout

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

☐ Enable PPPoE bridge mode

* *can be blank*

Figure 18: Cellular WAN configuration

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 3G 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 Sprint CDMA network connection section below 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.

CONNECTION TO MOBILE NETWORK CONNECTION

If the **Create connection to mobile network** option is selected, the router will automatically try to establish a connection after power up. If the attempt is unsuccessful, the router will re-boot and try again. For GSM/UMTS and LTE 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.

Table 17: GPRS connection configuration

Item	Description
Carrier	Generic, AT&T, T-Mobile, Sprint, Verizon (These are commonly used options on the drop-down list only available on the 3G Models)
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 • PAP or CHAP – Router is chose either authentication method. • PAP – Router will use PAP authentication. • CHAP – Router will use CHAP authentication.
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	• Automatic selection – The router will automatically select the network type • Depending upon the type of router, it is also possible to select a specific method of data transmission (GPRS, EDGE, UMTS …).

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.

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 Mobile Network connection, verify that the network settings have been entered correctly. You may also try a different authentication method or network type.

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.

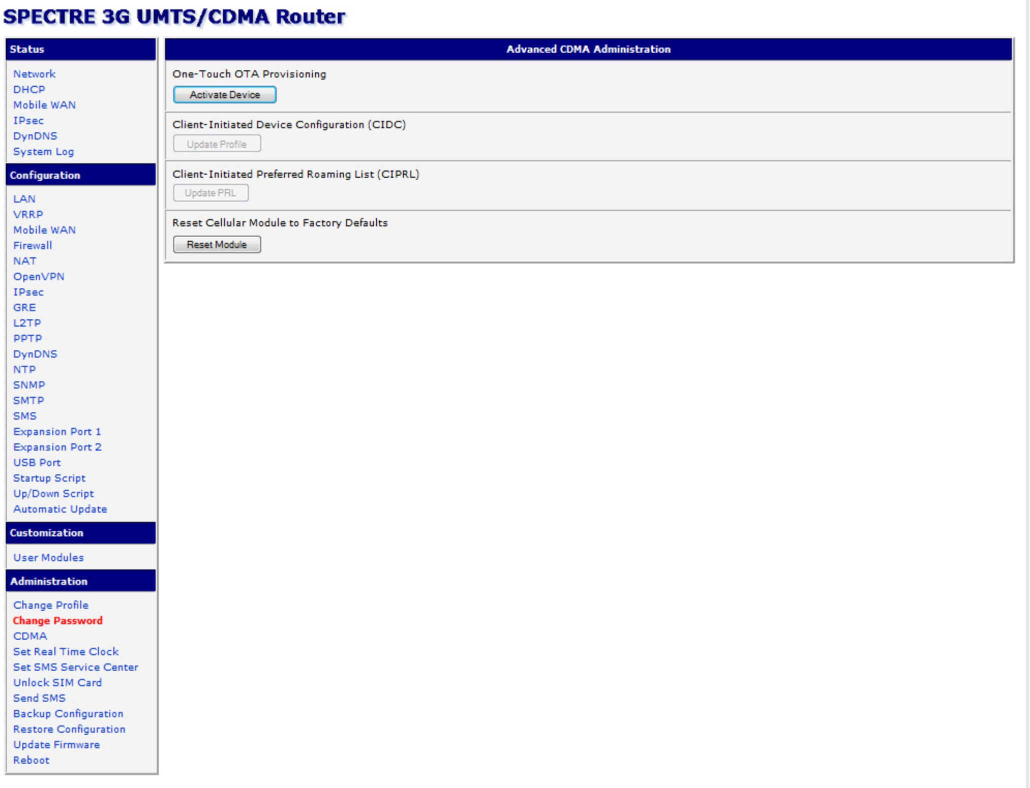


Figure 19: Advanced CDMA administration

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.

CHECK CONNECTION TO MOBILE NETWORK CONFIGURATION

You may set the ***Check 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 mobile network connection is restored.

Table 18: Check connection to mobile network configuration

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

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 mobile network connection. If mobile network 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 Connection*** to ensure reliable data communication.

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.

Table 19: Data limit configuration

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 ***Data Limit*** (50% to 99%). The router will send an SMS message with ***Router has exceeded (value of Warning Threshold) of data limit*** 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.

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.

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.

Table 20: Default and backup SIM configuration

Item	Description
Default SIM card	This parameter sets the default APN or SIM card for the PPP connection. If this parameter is set to ***none,*** 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.

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

Table 21: Switch between SIM card configurations

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 ***Check the PPP connection*** 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 '***bin0***' 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.

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.

Table 22: Switch between SIM card configurations

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 *Additive constants*. The range is from 1 to 10000 minutes.

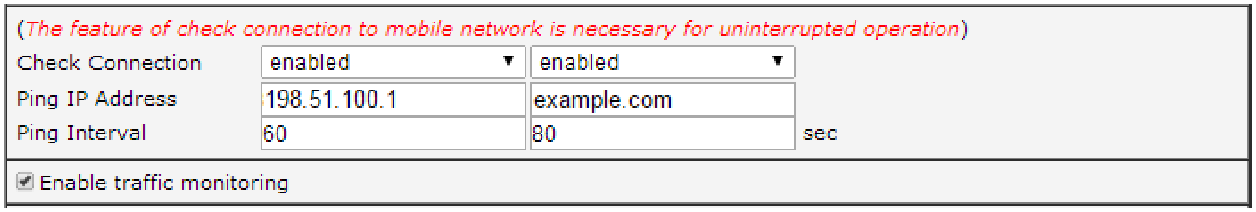
Example: Option ***Switch to primary SIM card after timeout*** is checked and the parameters are set as follows: ***Initial Timeout*** = 60 min. ***Subsequent Timeout*** = 30 min. ***Additive Constant*** = 20 min.

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).

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.

The figure below describes the situation, when the connection to mobile network is controlled on the address 198.51.100.1 in the time interval of 60 s for primary SIM card and on the address example.com in the time interval 80 s for secondary SIM card. In the case of traffic on the router the control pings are not sent, but the traffic is monitored.



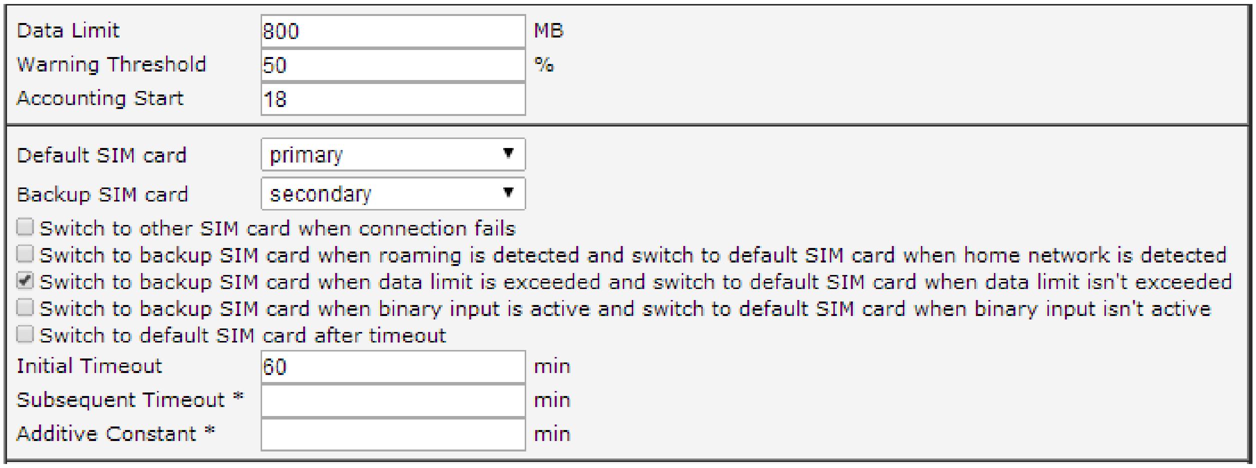
(*The feature of check connection to mobile network is necessary for uninterrupted operation*)

Check Connection	enabled ▼	enabled ▼	
Ping IP Address	198.51.100.1	example.com	
Ping Interval	60	80	sec

☑ Enable traffic monitoring

Figure 20: Example of Mobile WAN configuration 1

Figure 21 shows an example of how to configure the router to automatically switch to the backup SIM card when it exceeds the data limit of 800 MB in the billing period. It will send out a warning SMS message when 400 MB of data have been transmitted. In the example shown, the billing period begins on the 18th day of the month.



Data Limit	800	MB
Warning Threshold	50	%
Accounting Start	18	

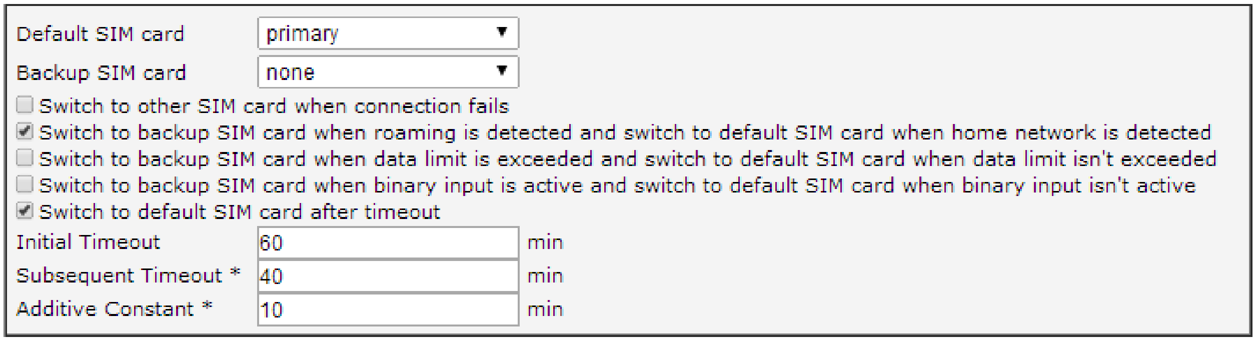
Default SIM card	primary ▼
Backup SIM card	secondary ▼

☐ Switch to other SIM card when connection fails
☐ Switch to backup SIM card when roaming is detected and switch to default SIM card when home network is detected
☑ Switch to backup SIM card when data limit is exceeded and switch to default SIM card when data limit isn't exceeded
☐ Switch to backup SIM card when binary input is active and switch to default SIM card when binary input isn't active
☐ Switch to default SIM card after timeout

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

Figure 21: Example of Mobile WAN 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: primary
Backup SIM card: none
□ Switch to other SIM card when connection fails
☑ Switch to backup SIM card when roaming is detected and switch to default SIM card when home network is detected
□ Switch to backup SIM card when data limit is exceeded and switch to default SIM card when data limit isn't exceeded
□ Switch to backup SIM card when binary input is active and switch to default SIM card when binary input isn't active
☑ Switch to default SIM card after timeout
Initial Timeout: 60 min
Subsequent Timeout *: 40 min
Additive Constant *: 10 min

Figure 22: Example of Mobile WAN configuration 3

BACKUP ROUTES

By using the configuration form on the ***Backup Routes*** page, you can back up the primary connection with alternative connections to the Internet/mobile network. Each back up connection can be assigned a priority. Switching between connections is done based on set priorities and the state of the connections (for Primary LAN and Secondary LAN).

If the ***Enable backup routes*** switching option is checked, the default route is selected according to the settings below.

You can set the parameters for enabling each of backup route

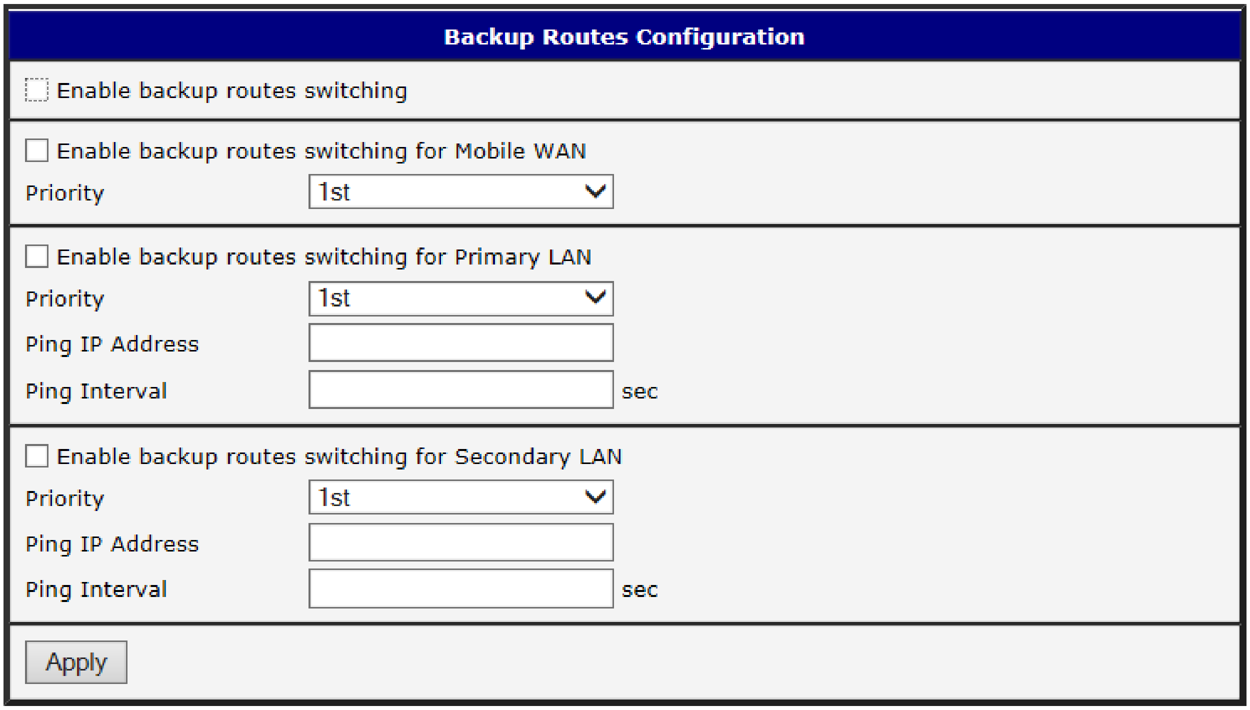
If the ***Enable backup routes*** switching option is not checked, the ***Backup routes*** system operates in the so-called backward compatibility mode. The default route is selected based on implicit priorities according to the status of each enabled network interface. The names of backup routes and corresponding network interfaces, in order of implicit priorities, are:

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

Example:
Secondary LAN is selected as the default route only if Create connection to mobile network option is not checked on the Mobile WAN page, alternatively if Create PPPoE connection option is not checked on the PPPoE page. To select the Primary LAN it is also necessary not to be entered IP address for Secondary LAN and must not be enabled DHCP Client for Secondary LAN.

Table 23: Backup routes

Item	Description
Priority	Priority for the type of connection
Ping IP Address	Destination IP address of ping queries to check the connection (address cannot be specified as a domain name)
Ping Interval	Time intervals between sent ping queries



Backup Routes Configuration

□ Enable backup routes switching

□ Enable backup routes switching for Mobile WAN

Priority: 1st

□ Enable backup routes switching for Primary LAN

Priority: 1st

Ping IP Address:

Ping Interval: sec

□ Enable backup routes switching for Secondary LAN

Priority: 1st

Ping IP Address:

Ping Interval: sec

Figure 23: Backup Routes

PPPOE CONFIGURATION

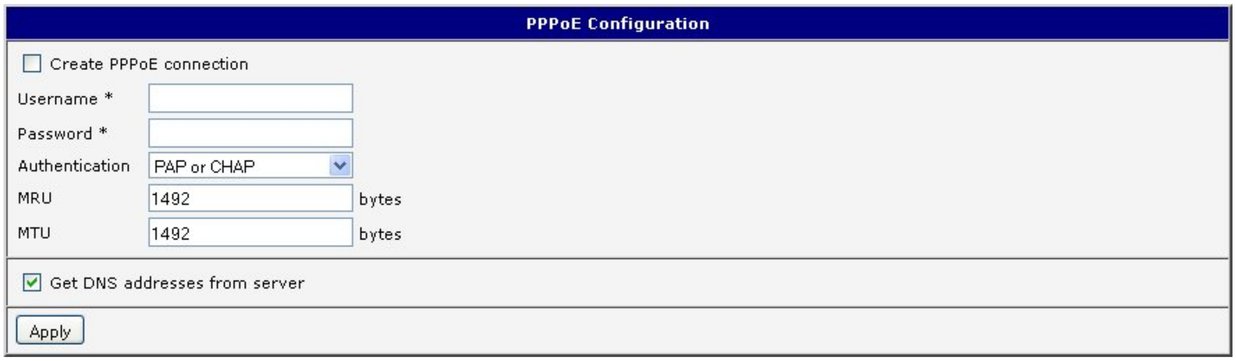
The SPECTRE cellular router does not support the PPPoE configuration option. PPPoE configuration is only available on SPECTRE RT routers. It is used to set the PPPoE connection over Ethernet.

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.

Table 24: PPoE configuration

Item	Description
Username	Username for secure access to PPPoE
Password	Password for secure access to PPPoE
Authentication	Authentication protocol in GSM network • PAP or CHAP – Router is chosen one of the authentication methods. • PAP – It is used PAP authentication method. • CHAP – It is used CHAP authentication method.
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



PPPoE Configuration

☐ Create PPPoE connection

Username *		
Password *		
Authentication	PAP or CHAP	
MRU	1492	bytes
MTU	1492	bytes

☑ Get DNS addresses from server

Figure 24: PPPoE configuration

LTE FIREWALL CONFIGURATION

The first security element which incoming packets must pass is check of enabled source IP address and destination ports. The IP address can be specified from which you can remotely access the router and the internal network connected behind a router. If the Enable filtering of incoming packets items is checked (located at the beginning of the configuration form Firewall), this element is enabled and accessibility is checked against the table with IP addresses. This means that access is permitted only to the address specified in the table. It is possible to define up to eight remote accesses. There are the following parameters:

Table 25: LTE Firewall configuration

Item	Description
Source	IP address from which access to the router is allowed
Protocol	Specifies protocol for remote access • all – access is allowed by all • TCP – access is allowed by TCP • UDP – access is allowed by UDP • ICMP – access is allowed by ICMP
Target Port	The port number on which access to the router is allowed
Action	Type of action: • allow – access is allowed • deny – access is denied

Caution! The firewalls on the 3G and LTE models do not filter traffic received over the Ethernet ports.

The following part of the configuration form defines the forwarding policy. If enabled filtering of forwarded packets item is not checked, packets are automatically accepted. If this item is checked and incoming packet is addressed to another network interface, it will go to the FORWARD chain. In case that the FORWARD chain accepted this packet (there is a rule for its forwarding), it will be sent out. If the forwarding rule does not exist, packet will be dropped.

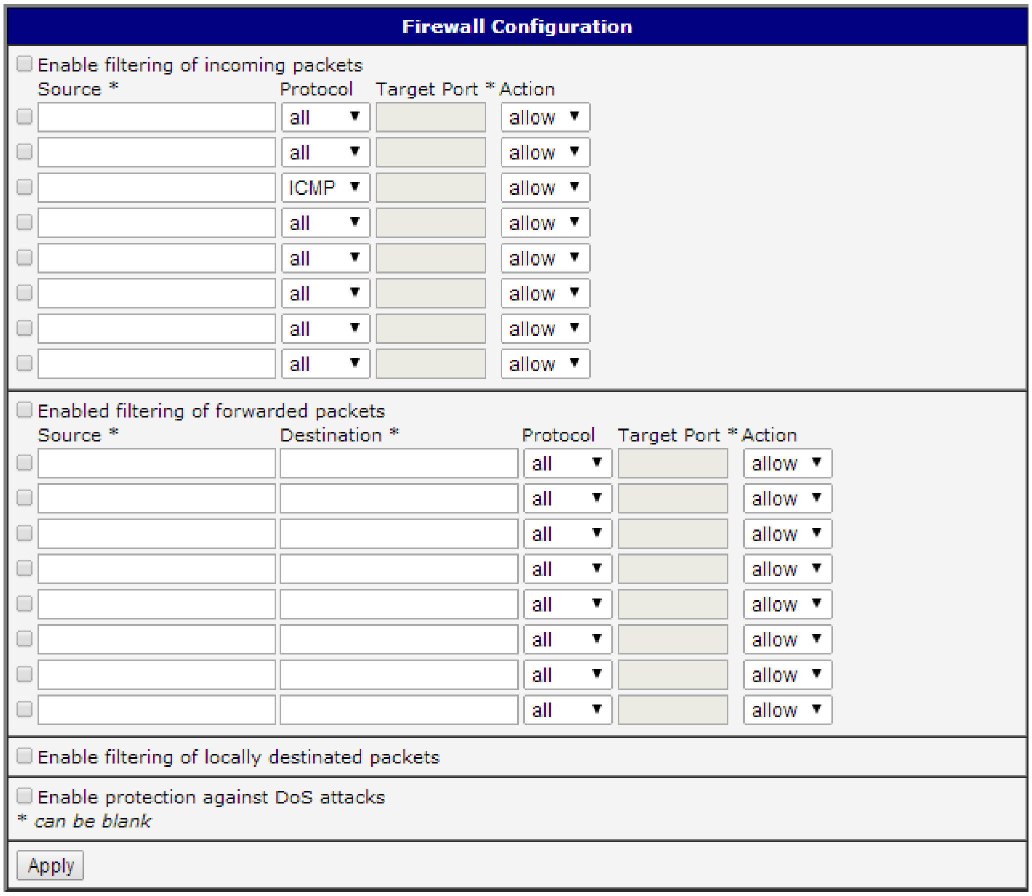
Then there is a table for defining the rules. It is possible to allow all traffic within the selected protocol (rule specifies only protocol) or create stricter rules by specifiying items for source IP address, destination IP address and port.

Table 266: LTE Firewall configuration

Item	Description
Source	IP address of source device
Destination	IP address of destination device
Protocol	Specifies protocol for remote access • all – access is allowed by all • TCP – access is allowed by TCP • UDP – access is allowed by UDP • ICMP – access is allowed by ICMP
Target Port	The port number on which access to the router is allowed
Action	Type of action: • allow – access is allowed • deny – access is denied

There is also the possibility to drop a packet whenever request for service which is not in the router comes (check box named Enable filtering of locally destinated packets). The packet is dropped automatically without any information.

As a protection against DoS attacks (this means attacks during which the target system is flooded with plenty of meaningless requirements) is used option named Enable protected against DoS attacks which limits the number of connections per second for five.



Firewall Configuration

□ Enable filtering of incoming packets

	Source *	Protocol	Target Port *	Action
□		all		allow
□		all		allow
□		ICMP		allow
□		all		allow
□		all		allow
□		all		allow
□		all		allow
□		all		allow

□ Enabled filtering of forwarded packets

	Source *	Destination *	Protocol	Target Port *	Action
□			all		allow
□			all		allow
□			all		allow
□			all		allow
□			all		allow
□			all		allow
□			all		allow
□			all		allow

□ Enable filtering of locally destinated packets

□ Enable protection against DoS attacks

** can be blank*

Apply

Figure 25: LTE Firewall configuration

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

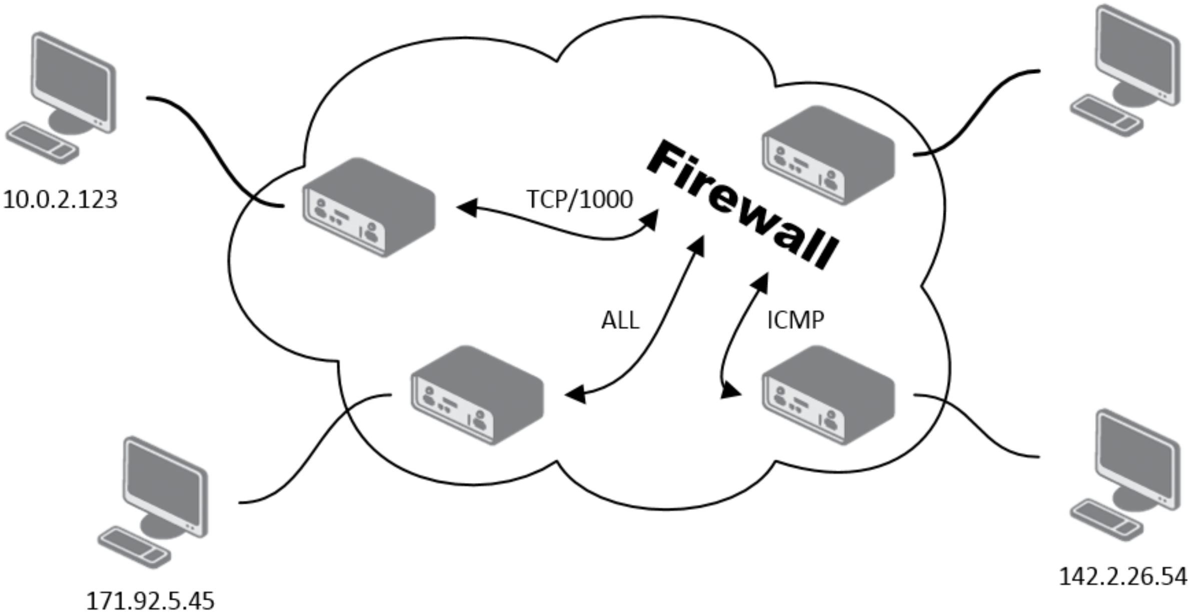
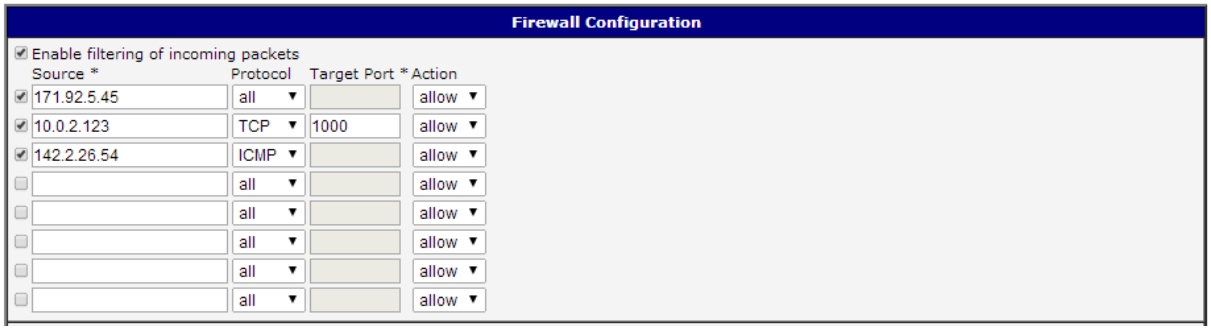


Figure 266: Example 5 - Network Topology for Firewall Application



Firewall Configuration

☑ Enable filtering of incoming packets

	Source *	Protocol	Target Port *	Action
☑	171.92.5.45	all		allow
☑	10.0.2.123	TCP	1000	allow
☑	142.2.26.54	ICMP		allow
□		all		allow
□		all		allow
□		all		allow
□		all		allow
□		all		allow

Figure 277: Example 5 – LTE Firewall configuration

3G and RT FIREWALL CONFIGURATION

The 3G and RT 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*.

Table 277: 3G and RT Firewall configuration

Item	Description
Source	IP address of source device
Destination	IP address of destination device
Protocol	Specifies protocol for remote access • all – access is allowed by all • TCP – access is allowed by TCP • UDP – access is allowed by UDP • ICMP – access is allowed by ICMP
Target Port	The port number on which access to the router is allowed
Action	Type of action: • allow – access is allowed • deny – access is denied

Caution! The firewalls on the 3G and LTE models do 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

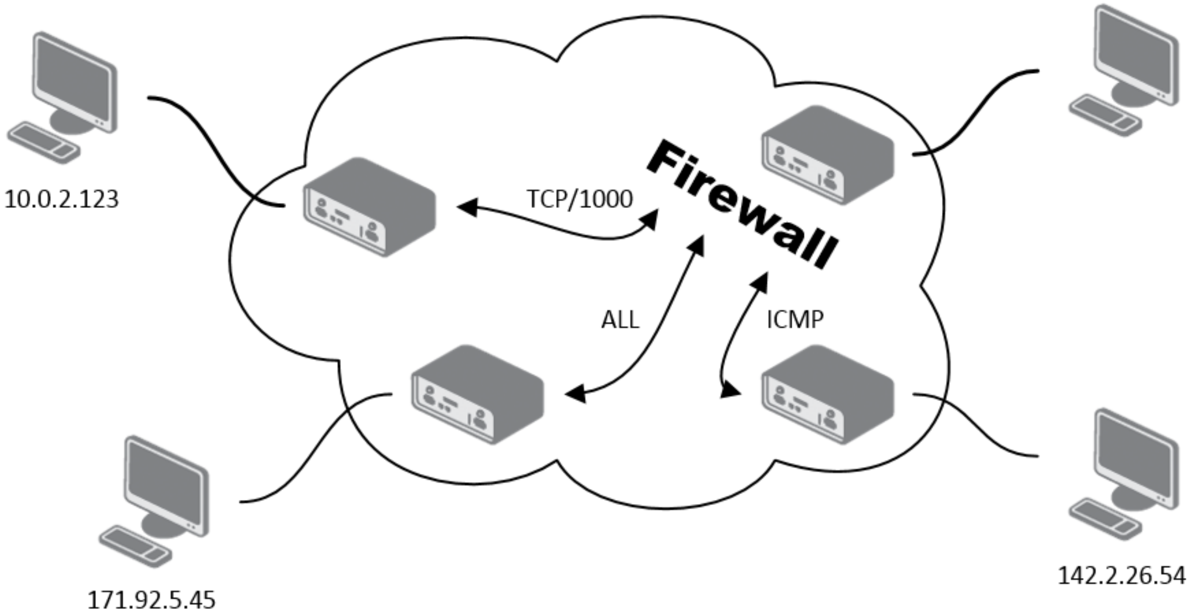
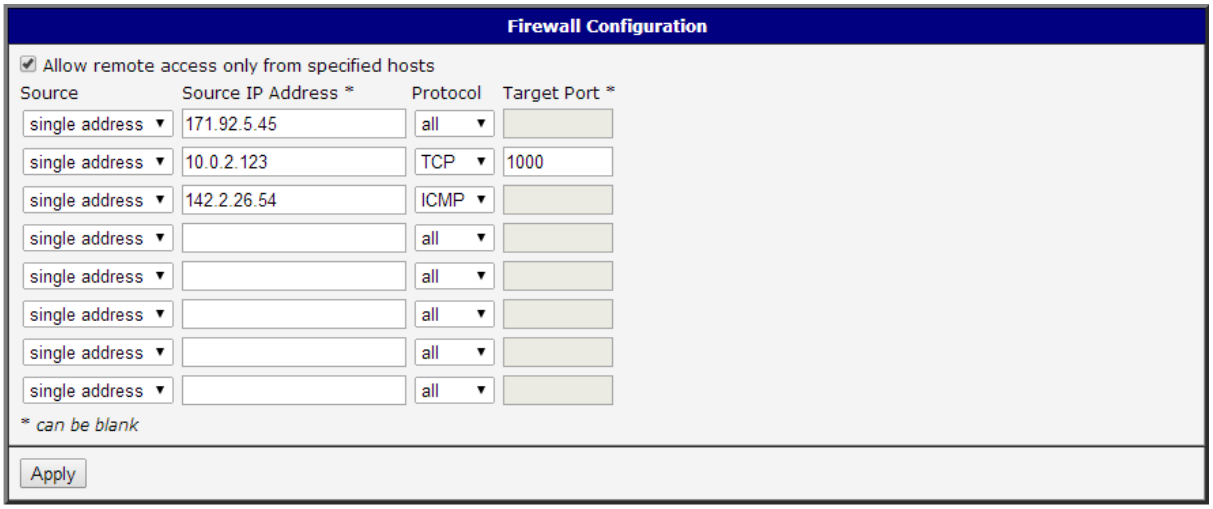


Figure 288: Example 5 - Network Topology for Firewall Application



Firewall Configuration

☑ 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

Apply

Figure 299: Example 5 – 3G and RT Firewall configuration

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.

Table 288: NAT configuration

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

If you need to set up 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.

Table 299: Configuration of send all incoming packets

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.

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

Table 30: Remote access configuration

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.

Example NAT configuration with one host connected to the router:

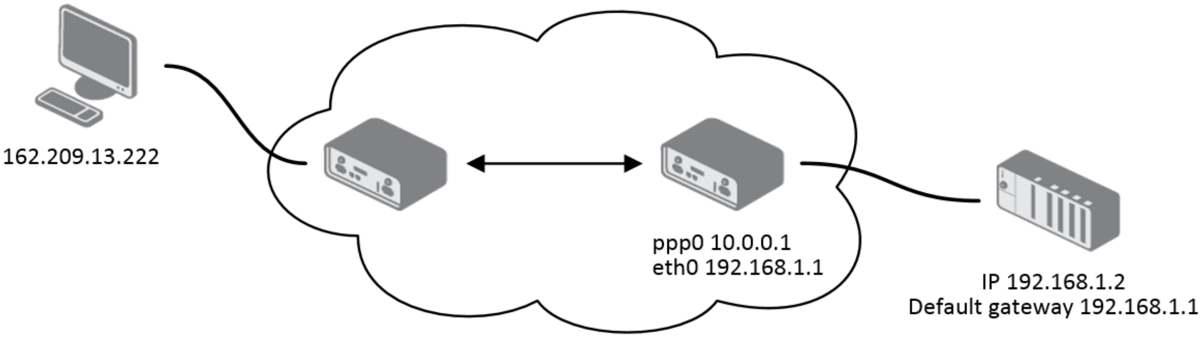
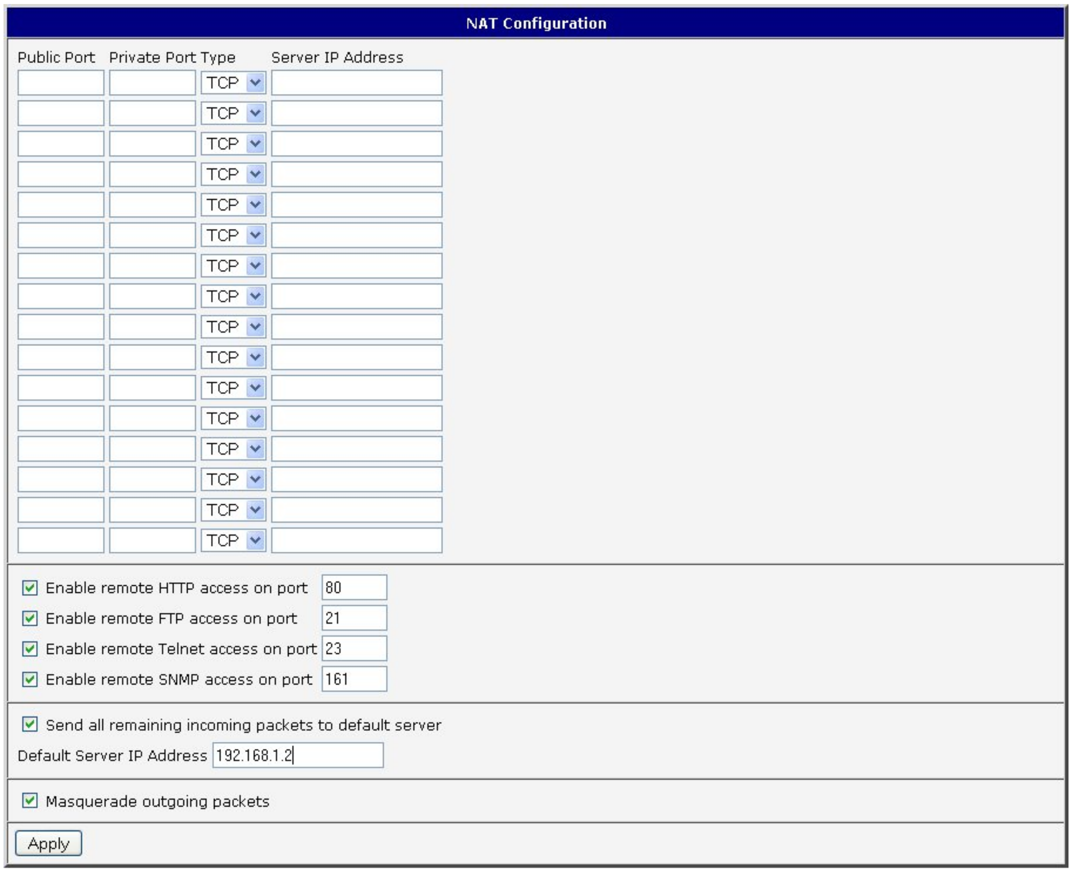


Figure 300: Example 6 - Network Topology for basic NAT



NAT Configuration

Public Port	Private Port	Type	Server IP Address
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	

☑ Enable remote HTTP access on port 80

☑ Enable remote FTP access on port 21

☑ Enable remote Telnet access on port 23

☑ Enable remote SNMP access on port 161

☑ Send all remaining incoming packets to default server

Default Server IP Address 192.168.1.2

☑ Masquerade outgoing packets

Figure 311: Example 6 - Basic NAT configuration

In this configuration, it is important to select ***Send all remaining incoming packets to default server***.

Example NAT configuration with additional connected equipment:

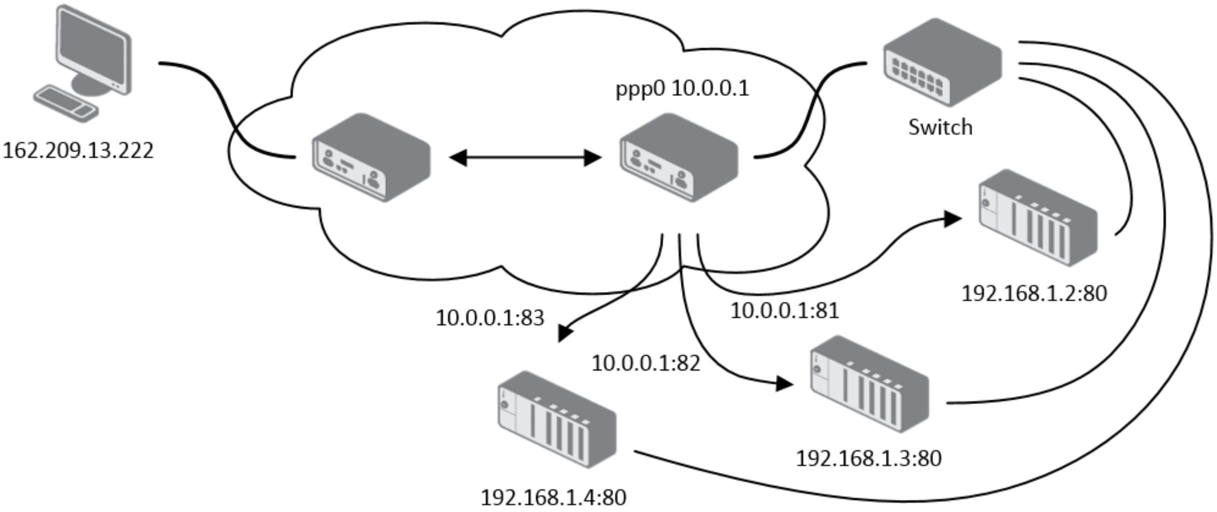
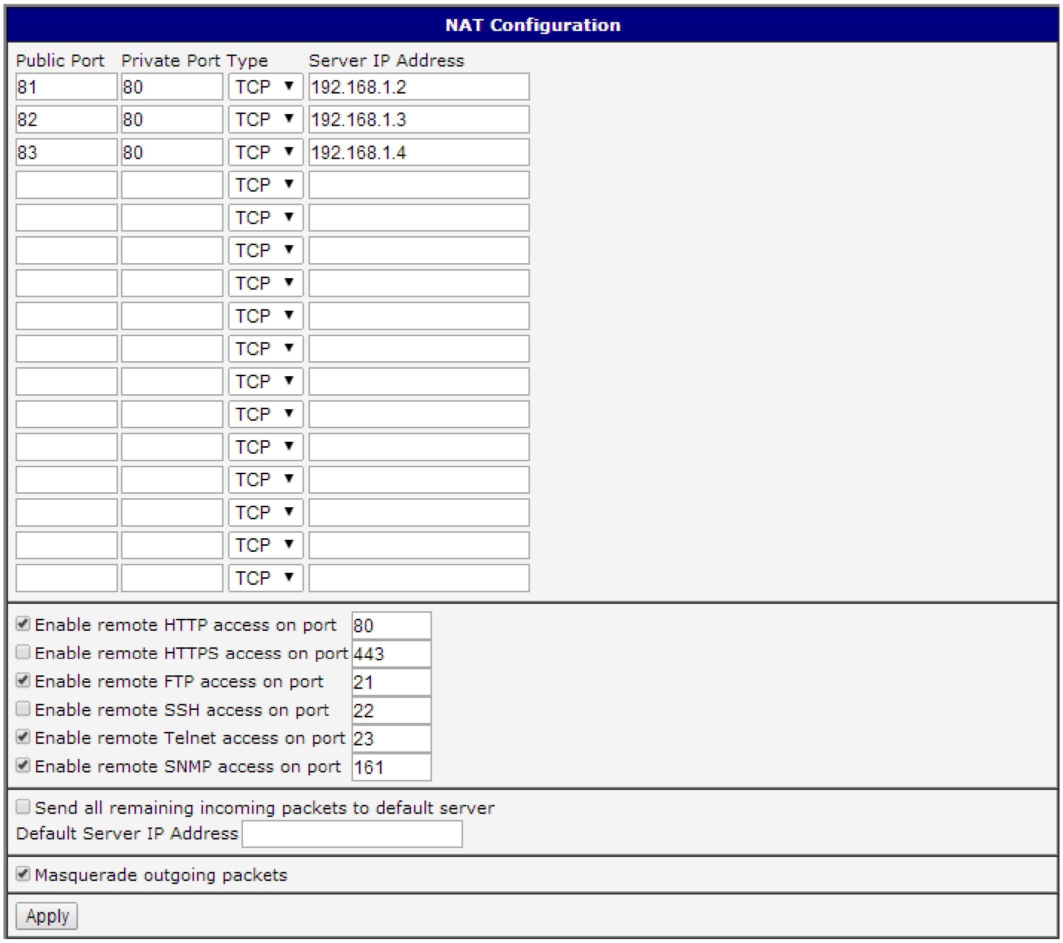


Figure 322: Example 7 - Network topology for advanced NAT



NAT Configuration

Public Port	Private Port	Type	Server IP Address
81	80	TCP ▼	192.168.1.2
82	80	TCP ▼	192.168.1.3
83	80	TCP ▼	192.168.1.4
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	
		TCP ▼	

☑ Enable remote HTTP access on port 80

☐ Enable remote HTTPS access on port 443

☑ Enable remote FTP access on port 21

☐ Enable remote SSH access on port 22

☑ Enable remote Telnet access on port 23

☑ Enable remote SNMP access on port 161

☐ Send all remaining incoming packets to default server

Default Server IP Address

☑ Masquerade outgoing packets

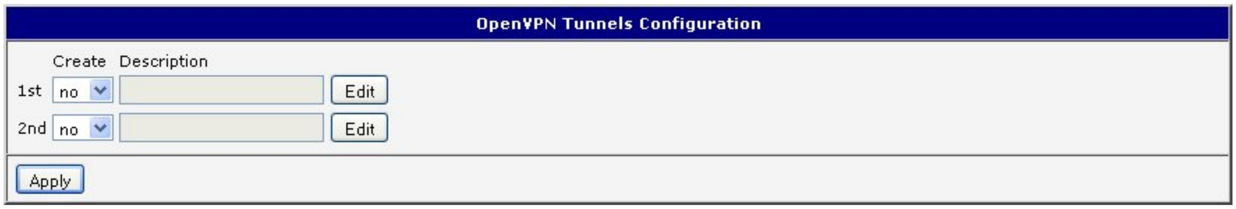
Figure 333: Example 7 - Advanced NAT configuration

OPENVPN TUNNEL CONFIGURATION

Select the ***OpenVPN*** item 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.

Table 31: Overview of OpenVPN tunnels

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.



OpenVPN Tunnels Configuration

	Create	Description	
1st	no		Edit
2nd	no		Edit

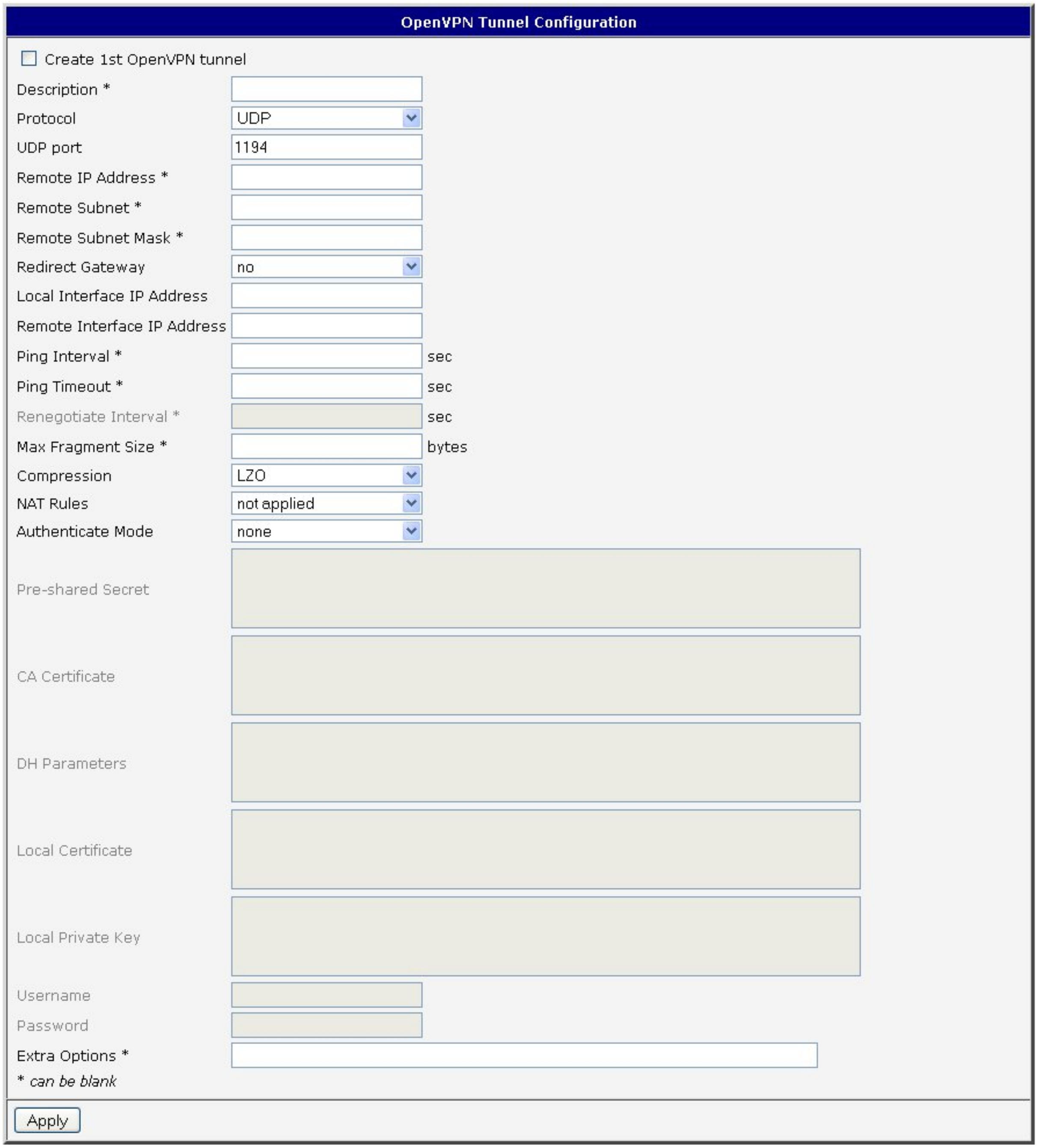
Figure 344: OpenVPN tunnel configuration

Table 312: OpenVPN configuration

Item	Description
Description	Description of tunnel.
Protocol	Protocol by which the tunnel will communicate. • **UDP** – OpenVPN will communicate using UDP. • **TCP server** – OpenVPN will communicate using TCP in server mode. • **TCP client** – OpenVPN will communicate using TCP in client mode.
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). ***Ping Timeout*** must be larger than ***Ping Interval***.
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	• **none** – No compression is used. • **LZO** – Lossless LZO compression. Compression has to be selected on both tunnel ends.
NAT Rules	• **not applied** – NAT rules are not applied to OpenVPN tunnel. • **applied** – NAT rules are not applied to OpenVPN tunnel.

Authenticate Mode	• **none** – is used any authentication mode • **Pre-shared secret** – enables authentication using pre-shared secret keys. Both sides of the tunnel must use the same key • **Username/password** – enables authentication using CA Certificate, Username and Password • **X.509 Certificate (multiclient)** – enables authentication by *CA Certificate*, *Local Certificate* and *Local Private Key* • **X.509 Certificate (client)** – enables authentication by *CA Certificate*, *Local Certificate* and *Local Private Key* • **X.509 Certificate (server)** - enables authentication by *CA Certificate*, *Local Certificate* and *Local Private Key*
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 *Extra Options* to define additional parameters of the OpenVPN tunnel, for example DHCP options etc.

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



OpenVPN Tunnel Configuration

☐ Create 1st OpenVPN tunnel

Description *		
Protocol	UDP	
UDP port	1194	
Remote IP Address *		
Remote Subnet *		
Remote Subnet Mask *		
Redirect Gateway	no	
Local Interface IP Address		
Remote Interface IP Address		
Ping Interval *		sec
Ping Timeout *		sec
Renegotiate Interval *		sec
Max Fragment Size *		bytes
Compression	LZO	
NAT Rules	not applied	
Authenticate Mode	none	
Pre-shared Secret		
CA Certificate		
DH Parameters		
Local Certificate		
Local Private Key		
Username		
Password		
Extra Options *		

* *can be blank*

Figure 355: OpenVPN tunnel configuration

Example of the OpenVPN tunnel configuration:

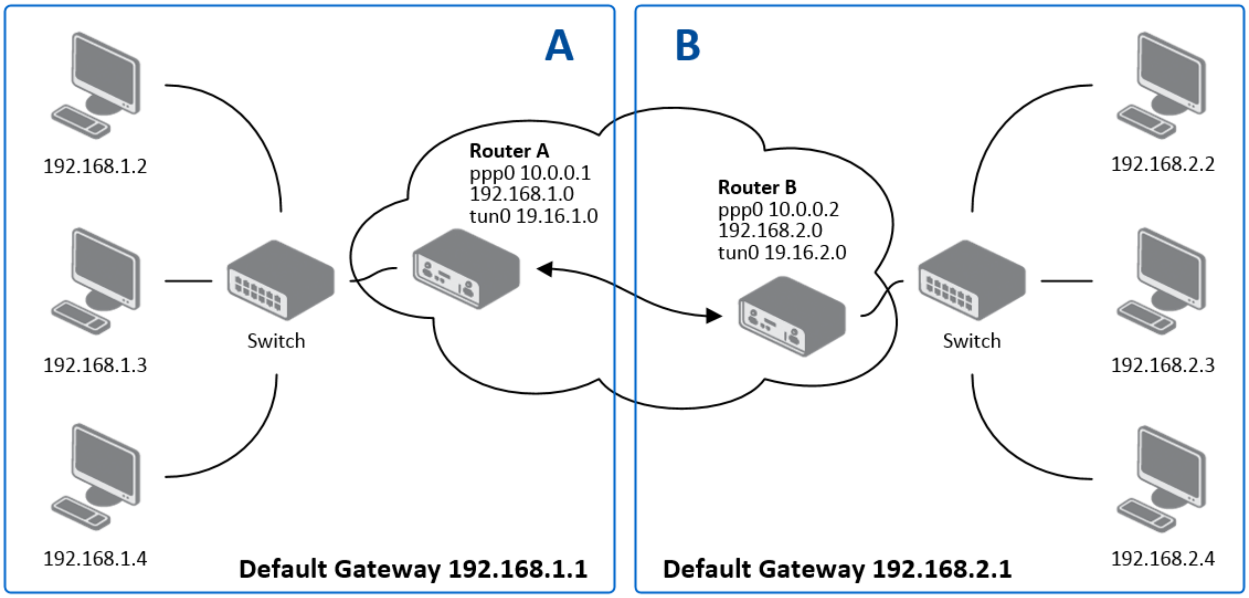


Figure 366: Topology of example OpenVPN configuration

OpenVPN tunnel configuration:

Table 323: Example of OpenVPN 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

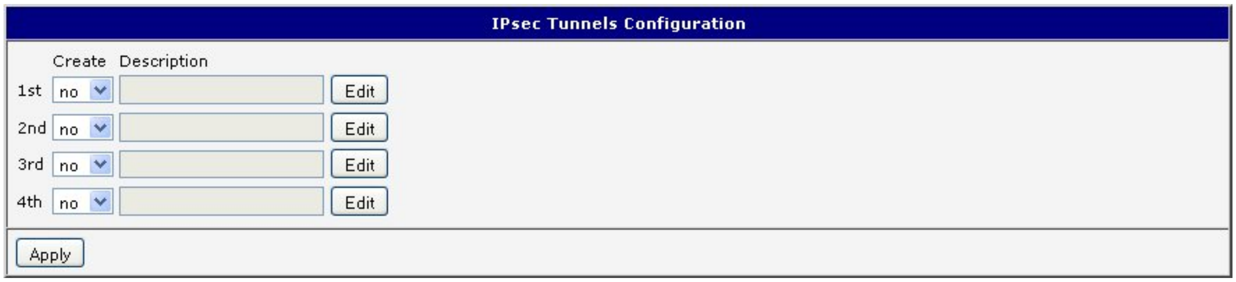
Examples of different options for configuration and authentication of OpenVPN can be found in OpenVPN’s tunnel configuration manuals.

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.

Table 334: Overview IPsec tunnels

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.



IPsec Tunnels Configuration

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

Figure 377: IPsec tunnels configuration

Table 345: IPsec tunnel 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 *hostname* and a *domain-name*.
Remote Subnet	Remote Subnet address
Remote Subnet Mask	Remote Subnet mask
Local ID	Identification of local host. The ID contains two parts: a *hostname* and a *domain-name*.
Local Subnet	Local subnet address
Local subnet mask	Local subnet mask
Encapsulation	IPsec mode – you can choose tunnel or transport
NAT Traversal	If address translation between two end points of the IPsec tunnel is used, it needs to allow NAT Traversal
IKE Mode	Defines mode for establishing connection (main or aggressive). If the aggressive mode is selected, establishing of IPsec tunnel will be faster, but encryption will set permanently on 3DES-MD5.
IKE Algorithm	Way of algorithm selection: • Auto – encryption and hash alg. Are selected automatically • Manual – encryption and hash alg. Are defined by the user
IKE Encryption	Encryption algorithm – 3DES, AES128, AES192, AES256
IKE Hash	Hash algorithm – MD5 or SHA1
IKE DH Group	Diffie-Hellman groups determine the strength of the key used in the key exchange process. Higher group numbers are more secure, but require additional time to compute the key. Group with higher number provides more security, but requires more processing time.
ESP Algorithm	Way of algorithm selection: • auto – encryption and hash alg. are selected automatically • manual – encryption and hash alg. are defined by the user

ESP Encryption	Encryption algorithm – DES, 3DES, AES128, AES192, AES256
ESP Hash	Hash algorithm – MD5 or SHA1
PFS	Ensures that derived session keys are not compromised if one of the private keys is compromised in the future
PFS DH Group	Diffie-Hellman group number (see IKE DH Group)
Key Lifetime	Lifetime key data part of tunnel. The minimum value of this parameter is 60s. The maximum value is 86400s.
IKE Lifetime	Lifetime key service part of tunnel. The minimum value of this parameter is 60s. The maximum value is 86400s.
Rekey Margin	Specifies how long before connection expiry should attempt to negotiate a replacement begin. The maximum value must be less than half the parameters IKE and Key Lifetime.
Rekey Fuzz	Specifies the maximum percentage by which should be randomly increased to randomize re-keying intervals
DPD Delay	Defines time after which is made IPsec tunnel verification
DPD Timeout	By parameter DPD Timeout is set timeout of the answer
Authenticate Mode	By this parameter can be set authentication: • Pre-shared key – shared key for both off-side tunnel. • X.509 Certificate – allows X.509 certification in multiclient mode
Pre-shared Key	Sharable key for both parties tunnel.
CA Certificate	This certificate is necessary to insert Authentication mode x.509.
Remote Certificate	This certificate is necessary to insert Authentication mode x.509.
Local Certificate	This certificate is necessary to insert Authentication mode x.509.
Local Private Key	This private key is necessary to insert Authentication mode x.509.
Local Passphrase	This Local Passphrase is necessary to insert Authentication mode x.509.
Extra Options	Use this parameter to define additional parameters of the IPsec tunnel, for example secure parameters etc.

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

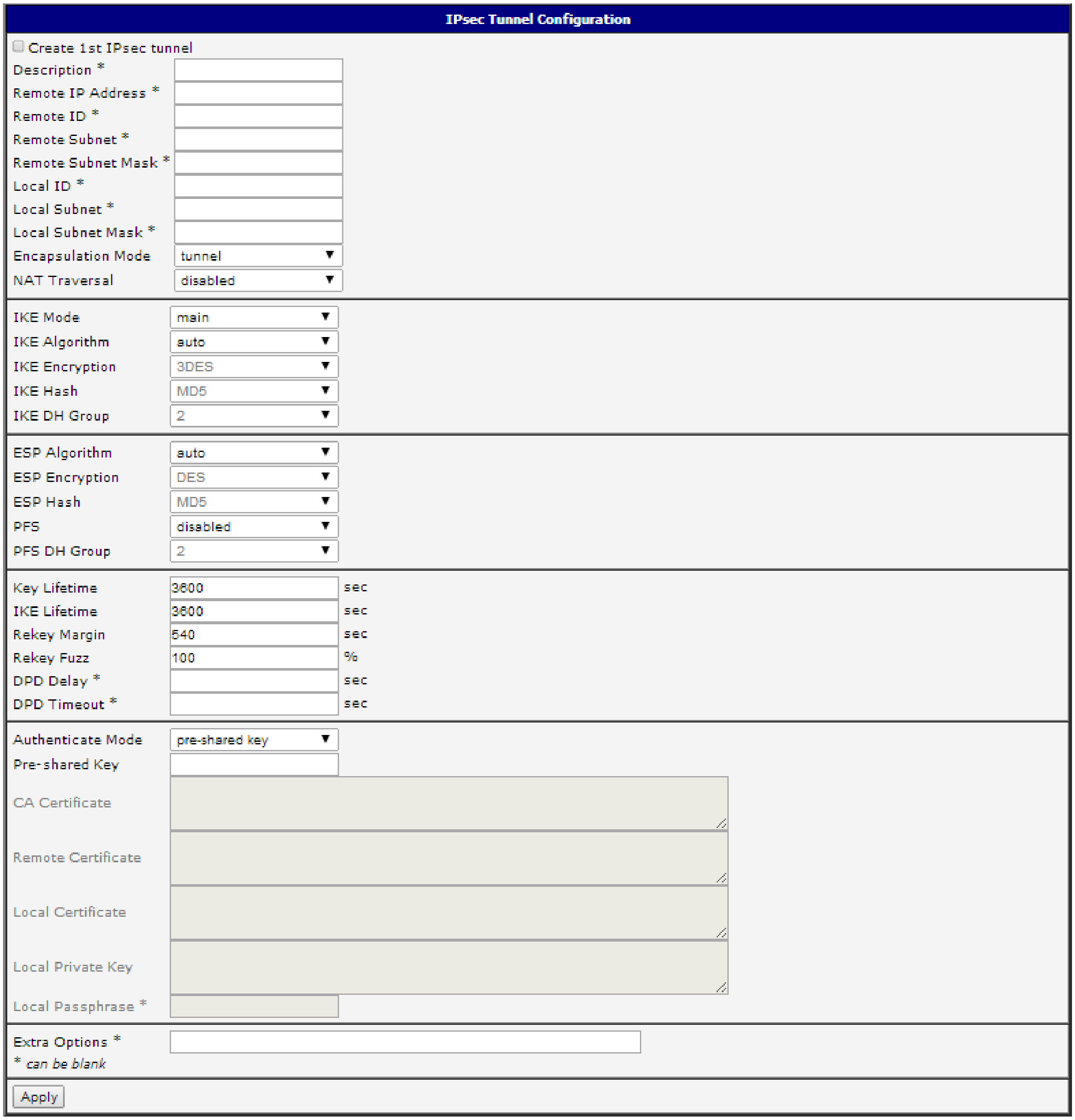
The random time, after which it will exchange new keys, is defined as follows:

*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 *		
Encapsulation Mode	tunnel ▼	
NAT Traversal	disabled ▼	
IKE Mode	main ▼	
IKE Algorithm	auto ▼	
IKE Encryption	3DES ▼	
IKE Hash	MD5 ▼	
IKE DH Group	2 ▼	
ESP Algorithm	auto ▼	
ESP Encryption	DES ▼	
ESP Hash	MD5 ▼	
PFS	disabled ▼	
PFS DH Group	2 ▼	
Key Lifetime	3600	sec
IKE Lifetime	3600	sec
Rekey Margin	540	sec
Rekey Fuzz	100	%
DPD Delay *		sec
DPD Timeout *		sec
Authenticate Mode	pre-shared key ▼	
Pre-shared Key		
CA Certificate		
Remote Certificate		
Local Certificate		
Local Private Key		
Local Passphrase *		
Extra Options *		

* *can be blank*

Figure 388: IPsec tunnel configuration

Example of IPSec Tunnel configuration:

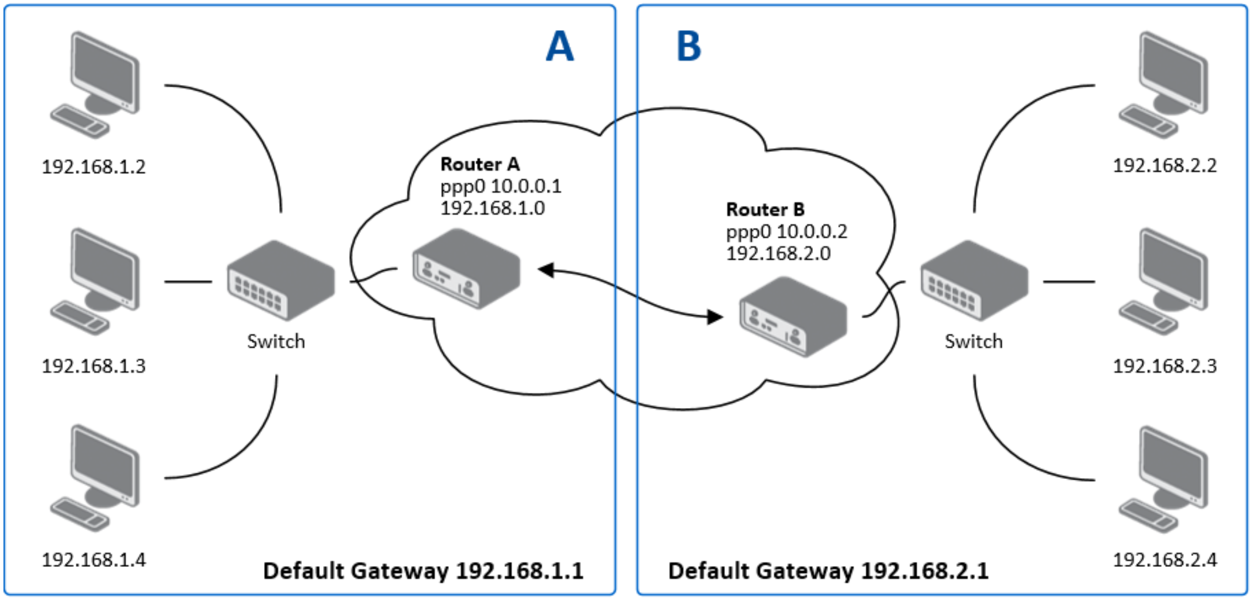


Figure 399: Example 8 - Network topology for IPsec tunneling

IPsec tunnel configuration:

Table 356: Example 8 - IPsec 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 Mask:	255.255.255.0	255.255.255.0
Authenticate mode	pre-shared key	pre-shared key
Pre-shared key	test	test

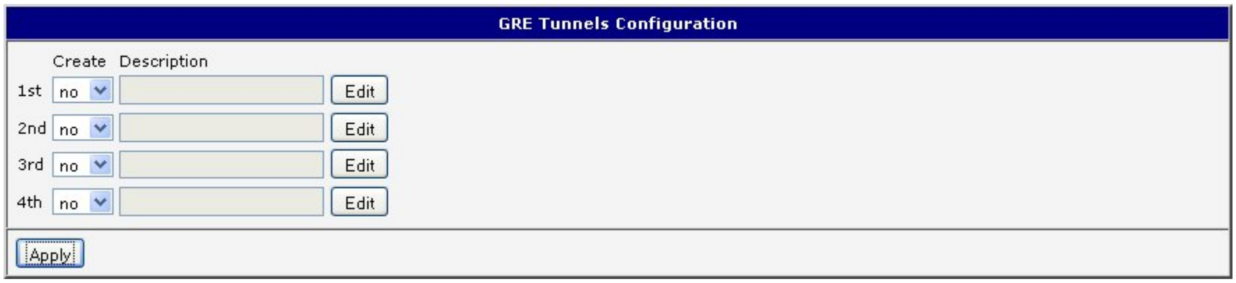
Examples of the different options for configuration and authentication of IPsec can be found in the IPsec tunnel configuration manual.

GRE TUNNELS CONFIGURATION

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

Table 367: Overview GRE tunnels

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.



GRE Tunnels Configuration

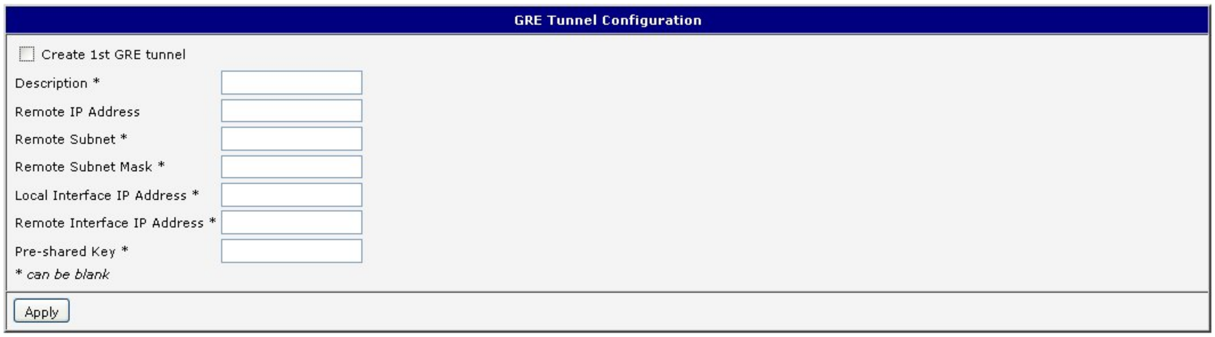
	Create	Description	
1st	no		Edit
2nd	no		Edit
3rd	no		Edit
4th	no		Edit

Apply

Figure 400: GRE tunnels configuration

Table 378: GRE tunnel 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.



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*

Apply

Figure 411: GRE tunnel configuration

Example of the GRE Tunnel configuration:

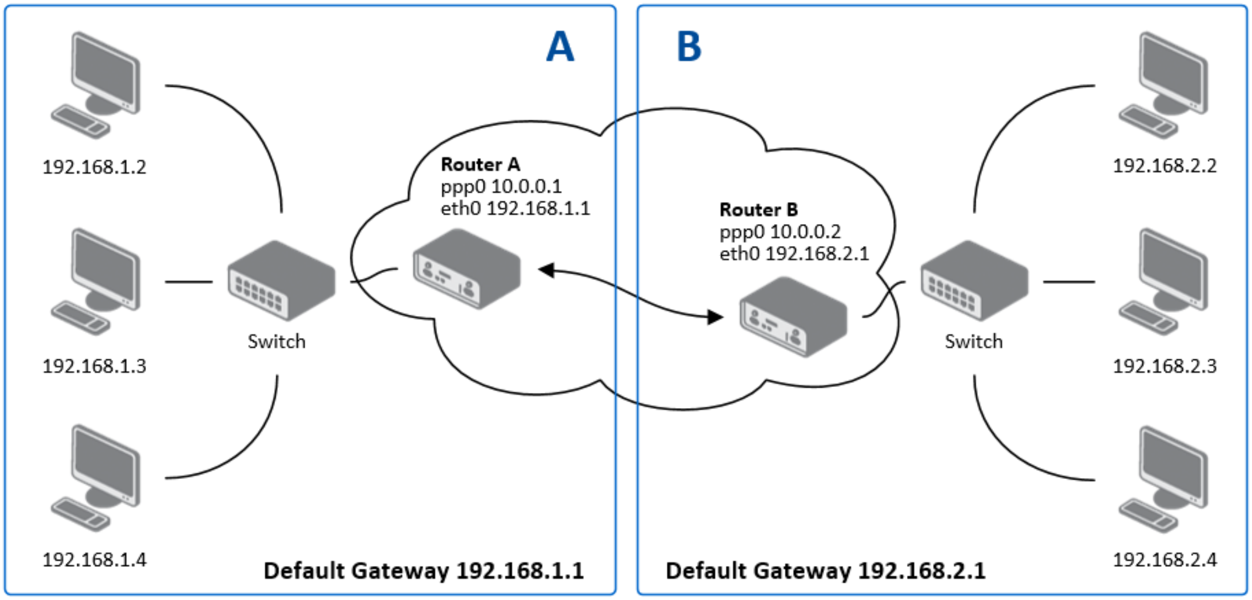


Figure 422: Network topology for GRE tunneling

GRE tunnel Configuration:

Table 389: Example 9 - 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

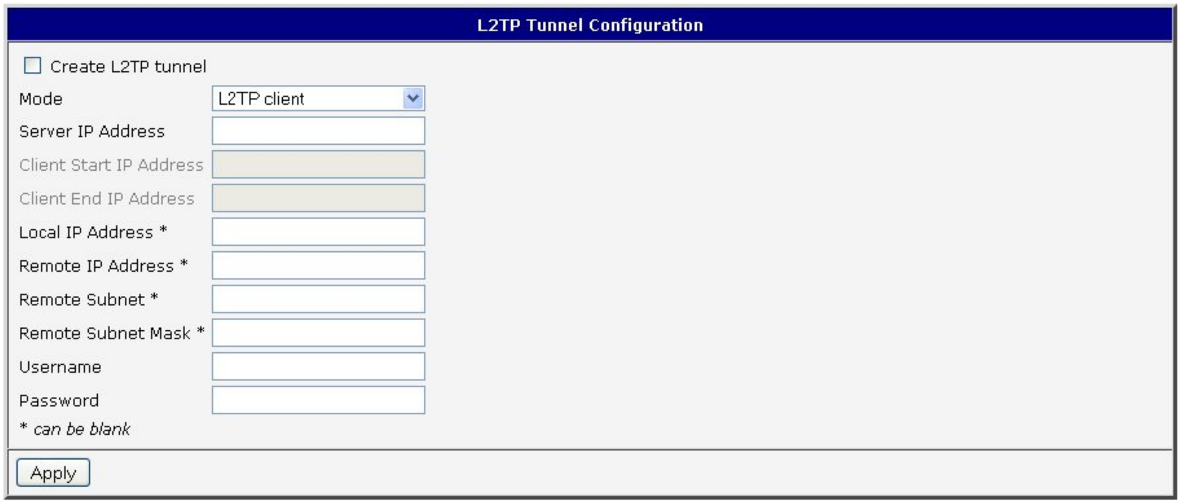
L2TP TUNNEL CONFIGURATION

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

Table 4039: L2TP tunnel configuration

Item	Description
Mode	L2TP tunnel mode on the router side • **L2TP server -** For a server, you must define the start and end IP address range offered by the server • **L2TP client –** For a client, you must enter the IP address of the server
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

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*

Figure 433: L2TP tunnel configuration

Example of the L2TP Tunnel configuration:

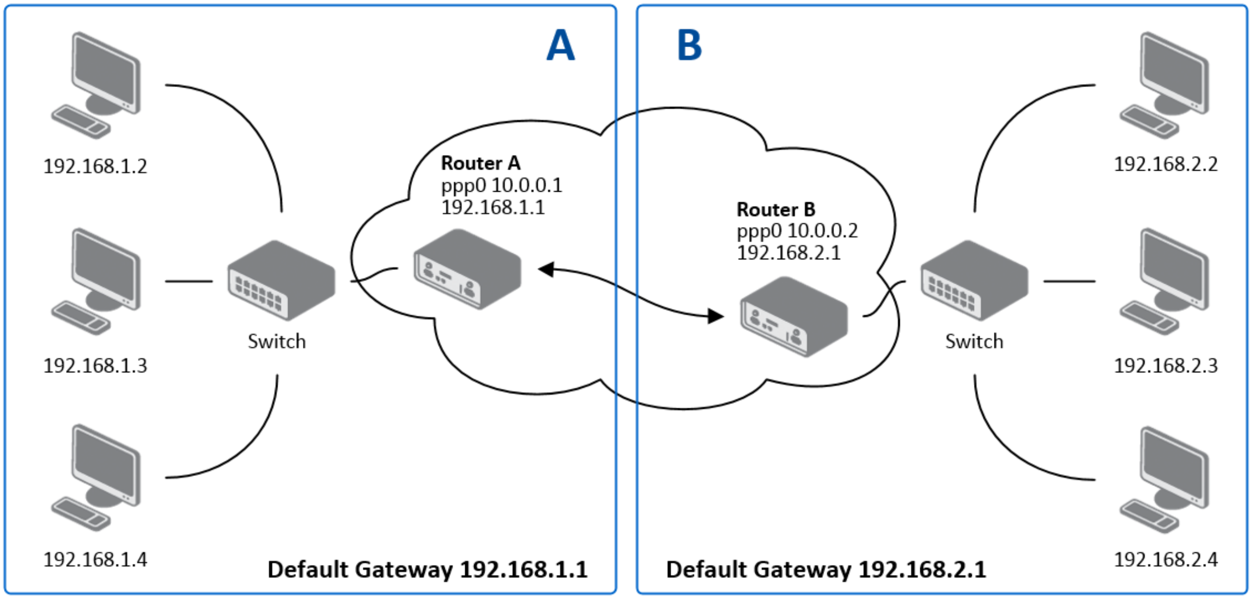


Figure 444: Example 10 - Network topology for L2TP tunneling

Configuration of the L2TP tunnel:

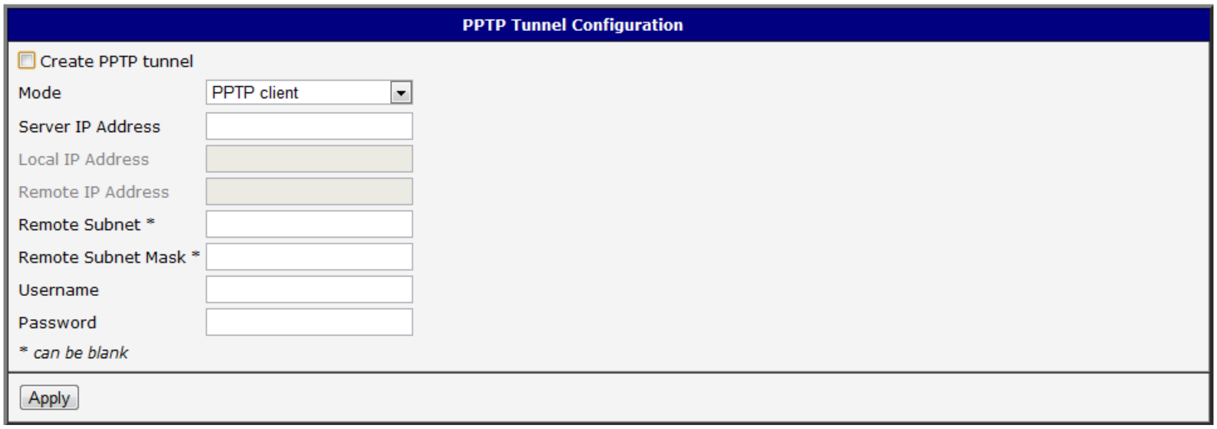
Table 4140: Example 10 - L2TP tunnel configuration

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

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.



PPTP Tunnel Configuration

□ Create PPTP tunnel

Mode	PPTP client
Server IP Address	
Local IP Address	
Remote IP Address	
Remote Subnet *	
Remote Subnet Mask *	
Username	
Password	

** can be blank*

Figure 455: PPTP tunnel configuration

Table 412: PPTP tunnel configuration

Item	Description
Mode	PPTP tunnel mode on the router side • **PPTP server –** For a server, you must define the start and end IP address range offered by the server • **PPTP client –** For a client, you must enter the IP address of the server
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

Press the Apply button to apply changes.

Example of the PPTP Tunnel configuration:

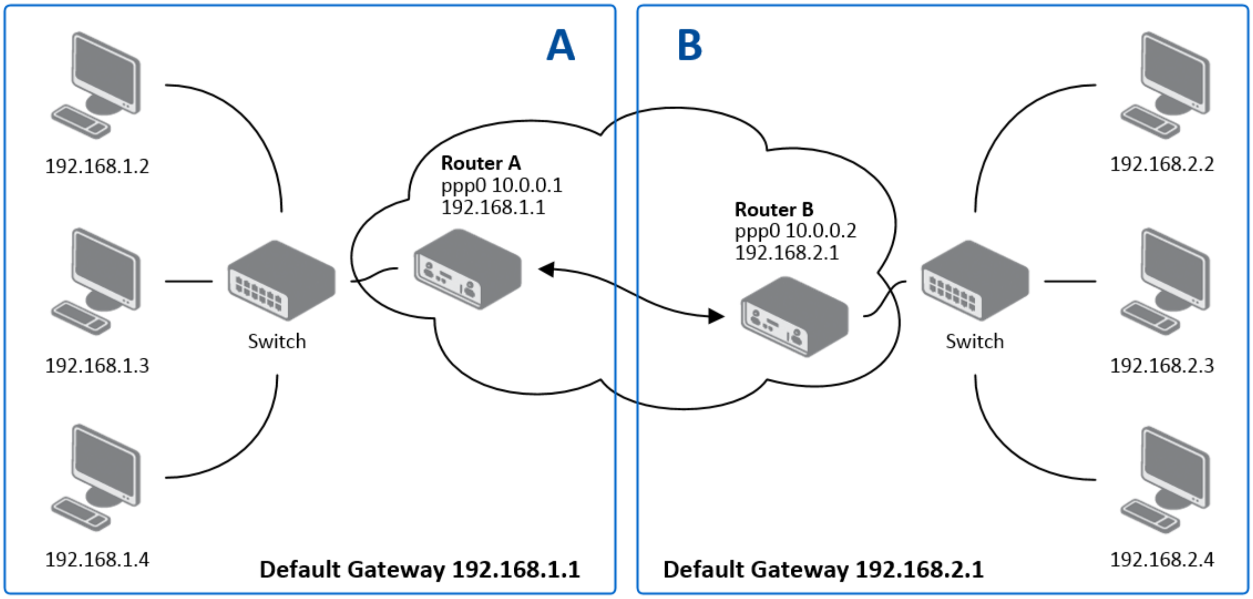


Figure 466: Example 11 - Network topology for PPTP tunneling configuration

Configuration of the PPTP tunnel:

Table 423: Example 11 - PPTP tunnel configuration

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

DYNDNS CLIENT CONFIGURATION

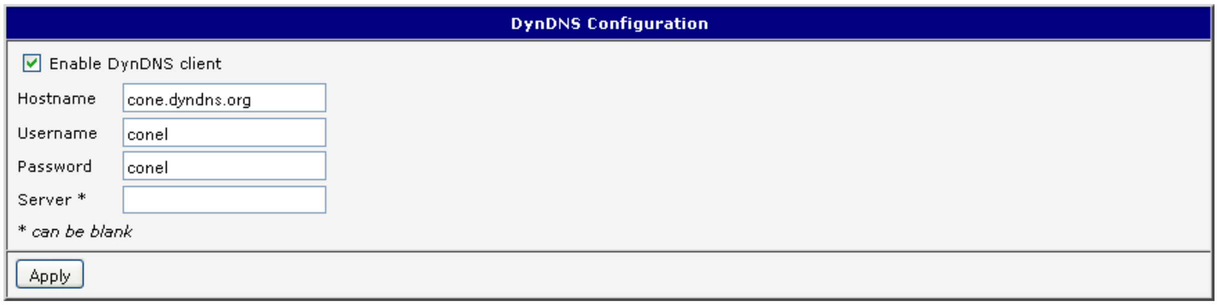
For Dynamic DNS to function properly, the router's SIM card must have a public IP address assigned.

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

Table 434: DynDNS configuration

Item	Description
Hostname	Third order domain registered on server www.dyndns.org
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 www.dyndns.org, enter the update server service in this parameter. If this item is left blank, the router uses the default server ***members.dyndns.org***.

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



DynDNS Configuration

☑ Enable DynDNS client

Hostname	cone.dyndns.org
Username	conel
Password	conel
Server *	

** can be blank*

Figure 477: Example of DynDNS configuration

NTP CLIENT CONFIGURATION

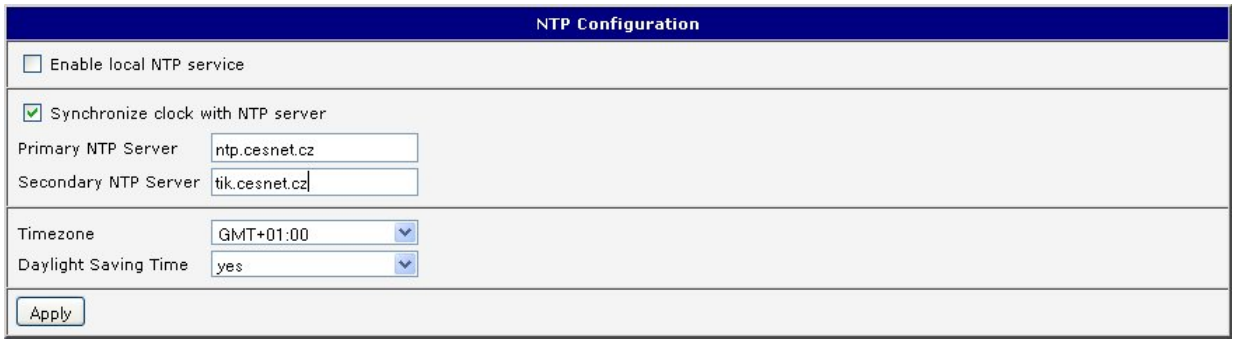
NTP (Network Time Protocol) allows the router to set its internal clock using a network time server. The NTP client Configuration can be called up by selecting option **NTP** item in the menu.

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

Table 445: NTP configuration

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: • No - time shift is disabled • Yes - time shift is allowed

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



NTP Configuration

□ 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

Figure 488: Example of NTP configuration

SNMP CONFIGURATION

SNMP (Simple Network Management Protocol) provides status information about network elements such as routers or end computers. The router supports SNMP agent v1/v2 or v3 which sends information about the router and its expansion ports. To enter the **SNMP** Configuration, select the **SNMP** item from the configuration menu.

Table 456: SNMP agent configuration

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

Enable SNMPv1/v2 with the ***Enable SNMPv1/v2*** access item. You will need to define a password for access to the SNMP agent (Community). “Public” is commonly used.

The ***Enable SNMPv3*** access item allows you to enable SNMPv3. Then you must define the following parameters:

Table 467: SNMPv3 configuration

Item	Description
Username	User Name
Authentication	Encryption algorithm on the Authentication Protocol that is used to ensure the identity of users.
Authentication Password	Password used to generate the key used for authentication.
Privacy	Encryption algorithm on the Privacy Protocol that is used to ensure confidentiality of data.
Privacy Password	Password for encryption on the Privacy Protocol.

In addition, you can continue with this configuration:

- By choosing Enable I/O extension option to monitor the binary input (I/O) on the router.
- By choosing Enable XC-CNT extension to monitor the status of the expansion port CNT inputs and outputs.
- By choosing Enable M-BUS extension and enter the Baud Rate, Parity and Stop Bits it is possible to monitor the meter status connected to the expansion port MBUS status.

Table 478: SNMP configuration (MBUS extension)

Item	Description
Baud rate	Communication speed.
Parity	Control parity bit: • none – Data will be sent without parity. • even – Data will be sent with even parity. • odd - Data will be sent with odd parity.
Stop Bits	Number of stop bits.

Parameters Enable XC-CNT extension and Enable M-BUS extension cannot be checked together.

By choosing ***Enable reporting to supervisor system*** and entering the IP Address and Period it is possible to send statistical information to the monitoring system, R-SeeNet.

Table 489: SNMP configuration (R-SeeNet)

Item	Description
IP Address	IP address
Period	Period of sending statistical information (in minutes)

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:

Table 490: Object identifier for binary input and output

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)

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

Table 501: Object identifier for CNT port

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)

The following range of OID is used for the expansion port M-BUS

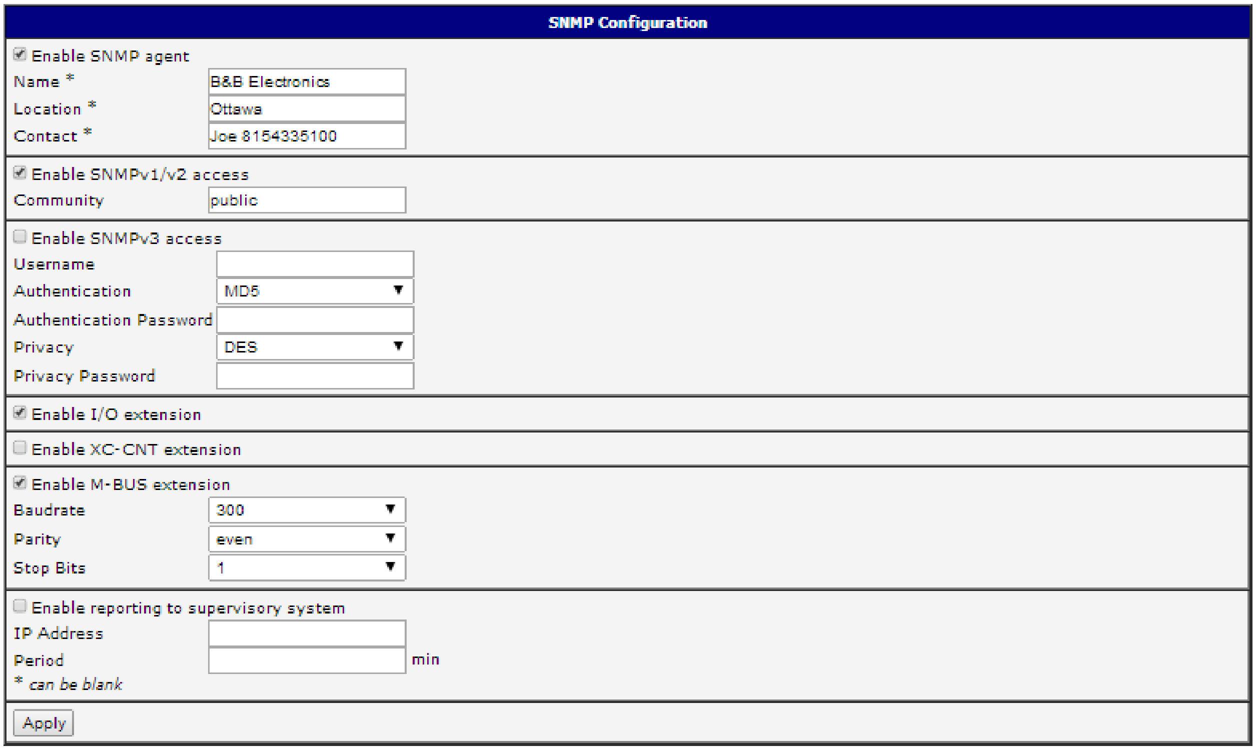
Table 512: Object identifier for M-BUS port

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

The meter address can be from range 0..254 when 254 is broadcast.

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

Example of SNMP settings and readout:



SNMP Configuration

☑ Enable SNMP agent

Name *	B&B Electronics
Location *	Ottawa
Contact *	Joe 8154335100

☑ Enable SNMPv1/v2 access

Community	public

☐ Enable SNMPv3 access

Username	
Authentication	MD5 ▼
Authentication Password	
Privacy	DES ▼
Privacy Password	

☑ Enable I/O extension

☐ Enable XC-CNT extension

☑ Enable M-BUS extension

Baudrate	300 ▼
Parity	even ▼
Stop Bits	1 ▼

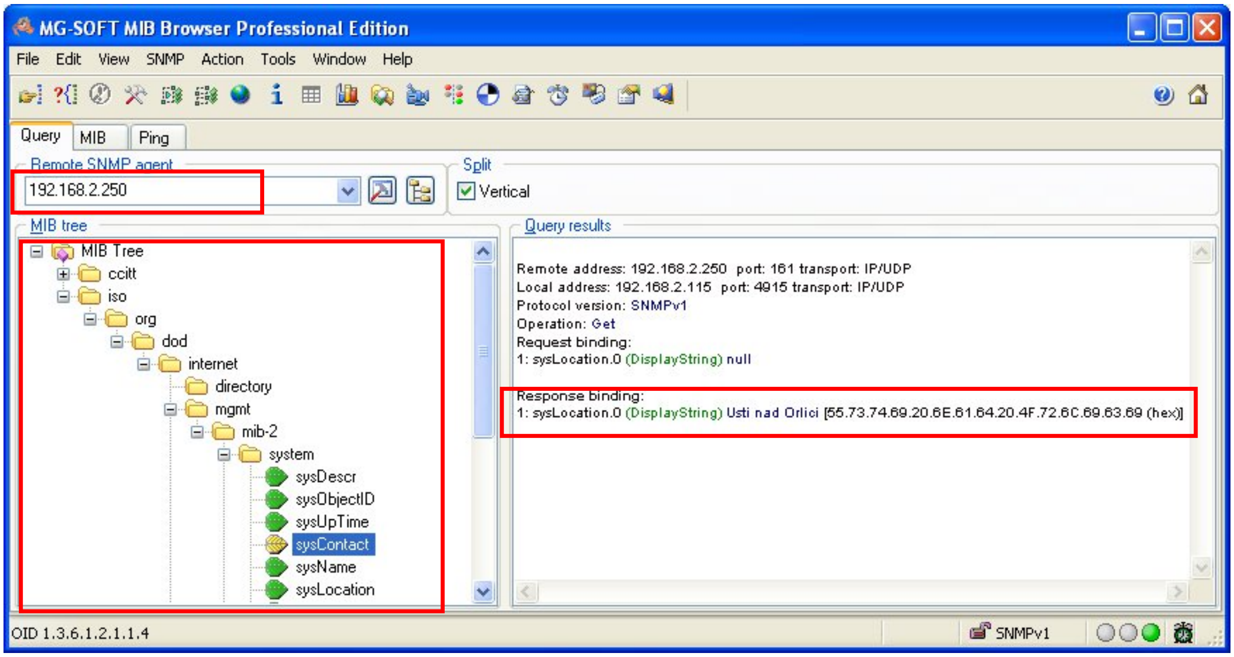
☐ Enable reporting to supervisory system

IP Address	
Period	min

* *can be blank*

Apply

Figure 499. Example of SNMP configuration



Remote SNMP agent: 192.168.2.250

☑ Vertical

```
Remote address: 192.168.2.250  port: 161 transport: IP/UDP
Local address: 192.168.2.115  port: 4915 transport: IP/UDP
Protocol version: SNMPv1
Operation: Get
Request binding:
1: sysLocation.0 (DisplayString) null

Response binding:
1: sysLocation.0 (DisplayString) Usti nad Orlici [55.73.74.69.20.6E.61.64.20.4F.72.6C.69.63.69 (hex)]
```

OID 1.3.6.1.2.1.1.4

Figure 500. 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 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

SMTP CONFIGURATION

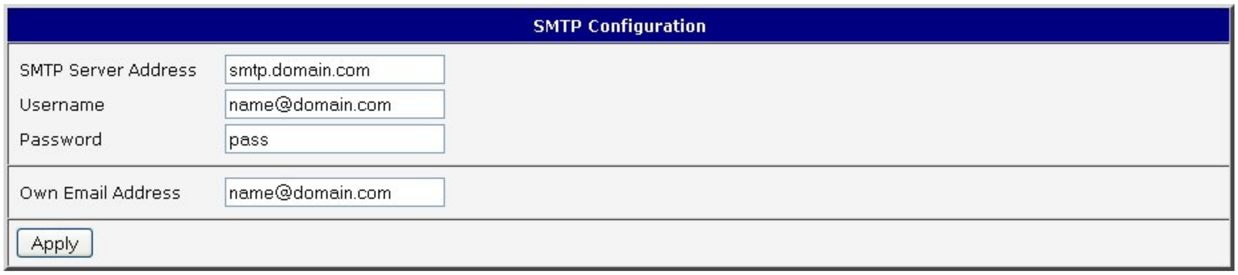
The SMTP (Simple Mail Transfer Protocol) client is used to send emails.

Table 523: SMTP client configuration

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.

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	smtp.domain.com
Username	name@domain.com
Password	pass
Own Email Address	name@domain.com

Figure 511. 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.

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.

Table 534: Send SMS configuration

Item	Description
Send SMS on power up	Send an SMS message when the router powers up
Send SMS on mobile network connect	Send an SMS message when the mobile network connection is active.
Send SMS on mobile network disconnect	Send an SMS message on mobile network 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.

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.

Table 545: Control via SMS configuration

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

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.

Table 556: SMS control commands

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	Mobile network 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.

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.

Table 567: Send SMS on serial PORT1 configuration

Item	Description
Baud rate	Communication speed expansion port 1

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

Table 578: Send SMS on serial PORT2 configuration

Item	Description
Baud rate	Communication speed expansion port 2

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.

Table 589: Send SMS on Ethernet Port configuration

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

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.

Table 6059: AT commands to send and receive SMS messages

AT commands	Description
AT+CGMI	Returns the manufacturer specific identity
AT+CGMM	Returns the manufacturer specific model identity
AT+CGMR	Returns the manufacturer specific model revision identity
AT+CGPADDR	Displays the IP address of the ppp0 interface
AT+CGSN	Returns the product serial number
AT+CIMI	Returns the International Mobile Subscriber Identity number (IMSI)
AT+CMGD	Deletes a message from the location
AT+CMGF	Sets the presentation format of short messages
AT+CMGL	Lists messages of a certain status from a message storage area
AT+CMGR	Reads a message from a message storage area
AT+CMGS	Sends a short message from the device to entered tel. Number
AT+CMGW	Writes a short message to SIM storage
AT+CMSS	Sends a message from SIM storage location value
AT+COPS?	Identifies the available mobile networks
AT+CPIN	Is used to query and enter a PIN code
AT+CPMS	Selects SMS memory storage types, to be used for short message operations
AT+CREG	Displays network registration status
AT+CSCA	Sets the short message service center (SMSC) number
AT+CSCS	Selects the character set
AT+CSQ	Returns the signal strength of the registered network
AT+GMI	Returns the manufacturer specific identity
AT+GMM	Returns the manufacturer specific model identity
AT+GMR	Returns the manufacturer specific model revision identity
AT+GSN	Returns the product serial number
ATE	Determines whether or not the device echoes characters

ATI	Transmits the manufacturer specific information about the device

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. Signal strength –xx dBm.

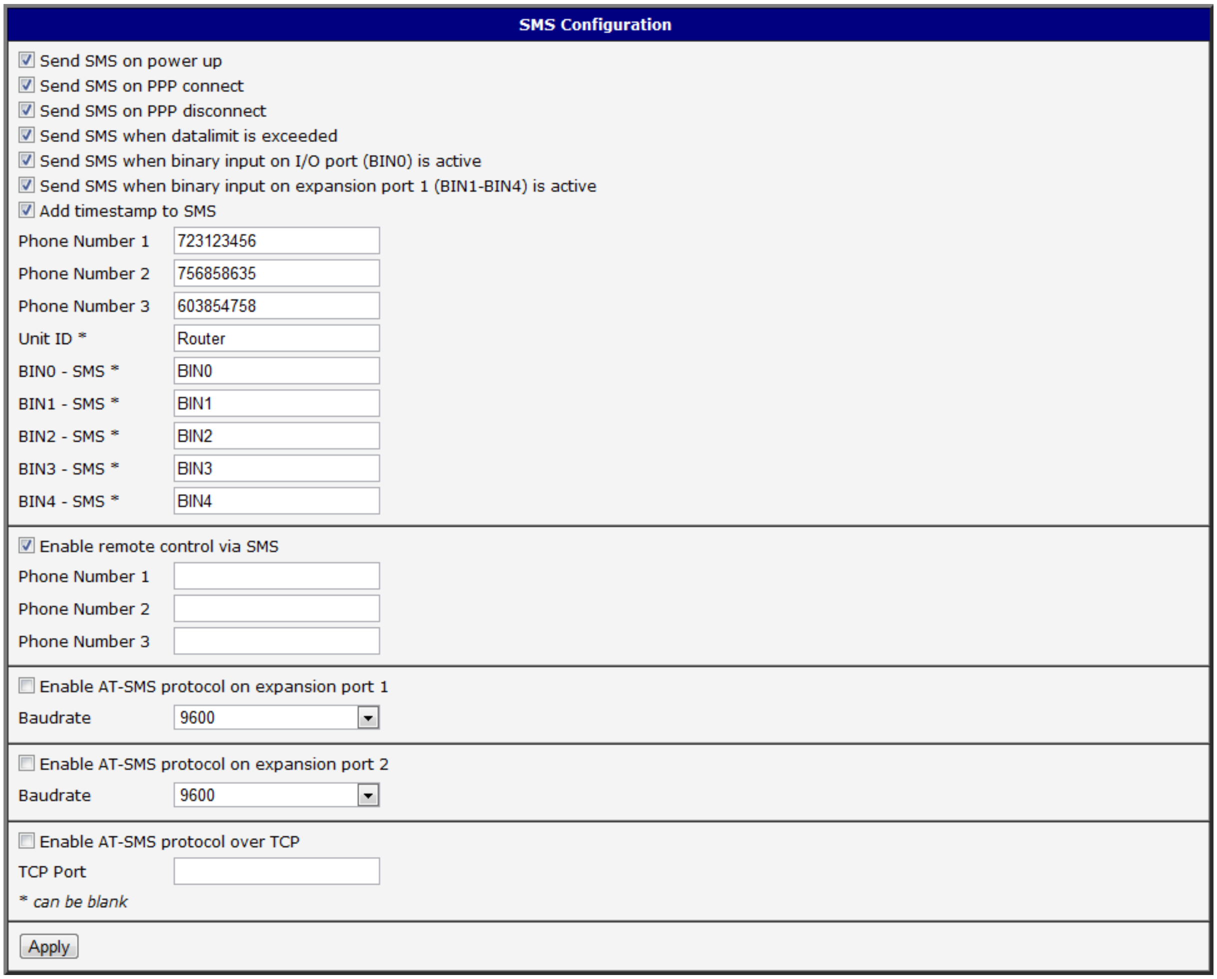
The format of the Router mobile network connection SMS message is as follows:

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

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

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

SMS Configuration Example:



SMS Configuration

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

Phone Number 1	723123456
Phone Number 2	756858635
Phone Number 3	603854758
Unit ID *	Router
BIN0 - SMS *	BIN0
BIN1 - SMS *	BIN1
BIN2 - SMS *	BIN2
BIN3 - SMS *	BIN3
BIN4 - SMS *	BIN4

☑ Enable remote control via SMS

Phone Number 1	
Phone Number 2	
Phone Number 3	

□ Enable AT-SMS protocol on expansion port 1

Baudrate 9600

□ Enable AT-SMS protocol on expansion port 2

Baudrate 9600

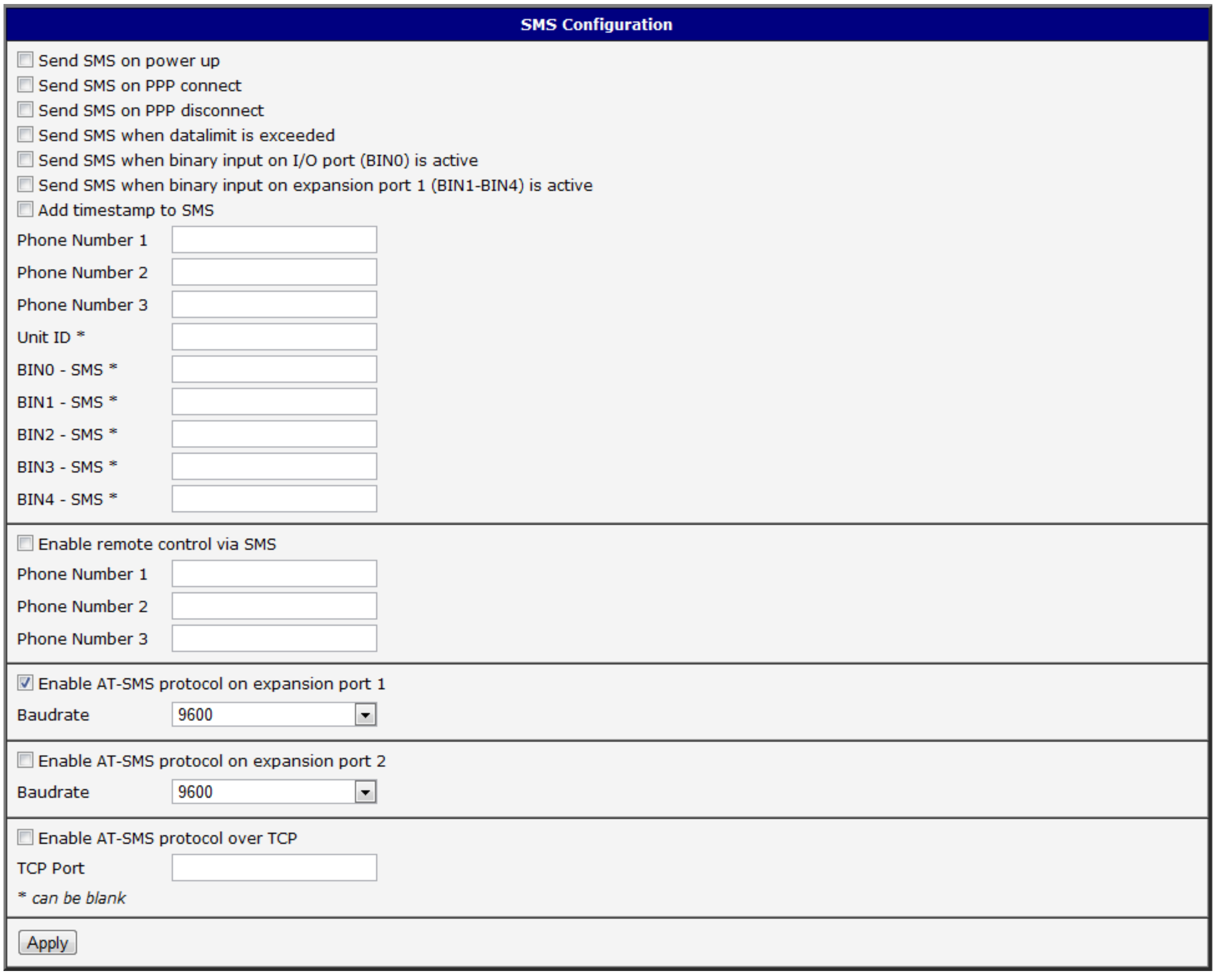
□ Enable AT-SMS protocol over TCP

TCP Port

** can be blank*

Figure 522. Example of SMS configuration 1

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



SMS Configuration

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

Phone Number 1	
Phone Number 2	
Phone Number 3	
Unit ID *	
BIN0 - SMS *	
BIN1 - SMS *	
BIN2 - SMS *	
BIN3 - SMS *	
BIN4 - SMS *	

☐ Enable remote control via SMS

Phone Number 1	
Phone Number 2	
Phone Number 3	

☑ Enable AT-SMS protocol on expansion port 1

Baudrate	9600

☐ Enable AT-SMS protocol on expansion port 2

Baudrate	9600

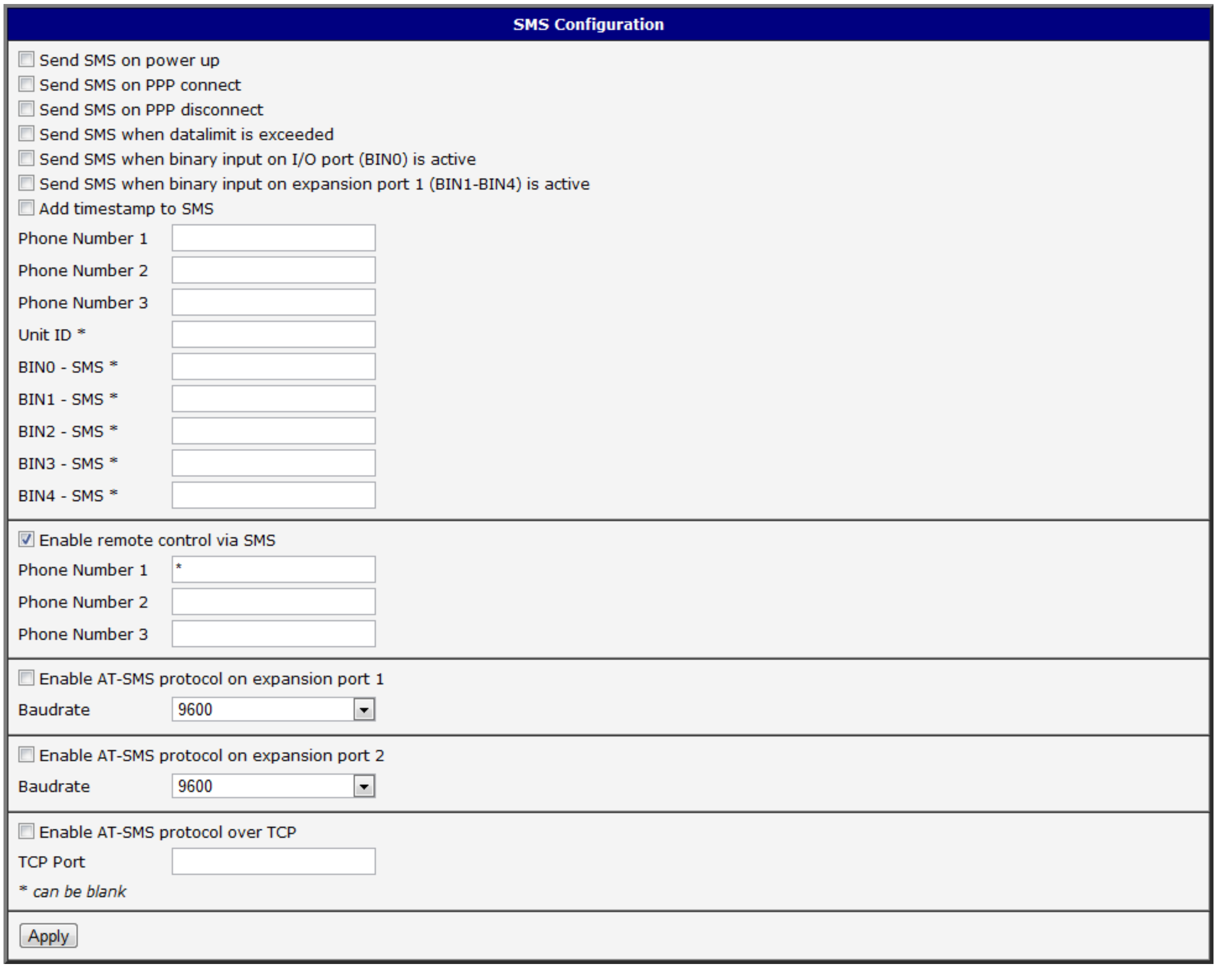
☐ Enable AT-SMS protocol over TCP

TCP Port	

** can be blank*

Figure 533. Example of SMS configuration 2

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



SMS Configuration

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

Phone Number 1	
Phone Number 2	
Phone Number 3	
Unit ID *	
BIN0 - SMS *	
BIN1 - SMS *	
BIN2 - SMS *	
BIN3 - SMS *	
BIN4 - SMS *	

☑ Enable remote control via SMS

Phone Number 1	*
Phone Number 2	
Phone Number 3	

□ Enable AT-SMS protocol on expansion port 1

Baudrate 9600

□ Enable AT-SMS protocol on expansion port 2

Baudrate 9600

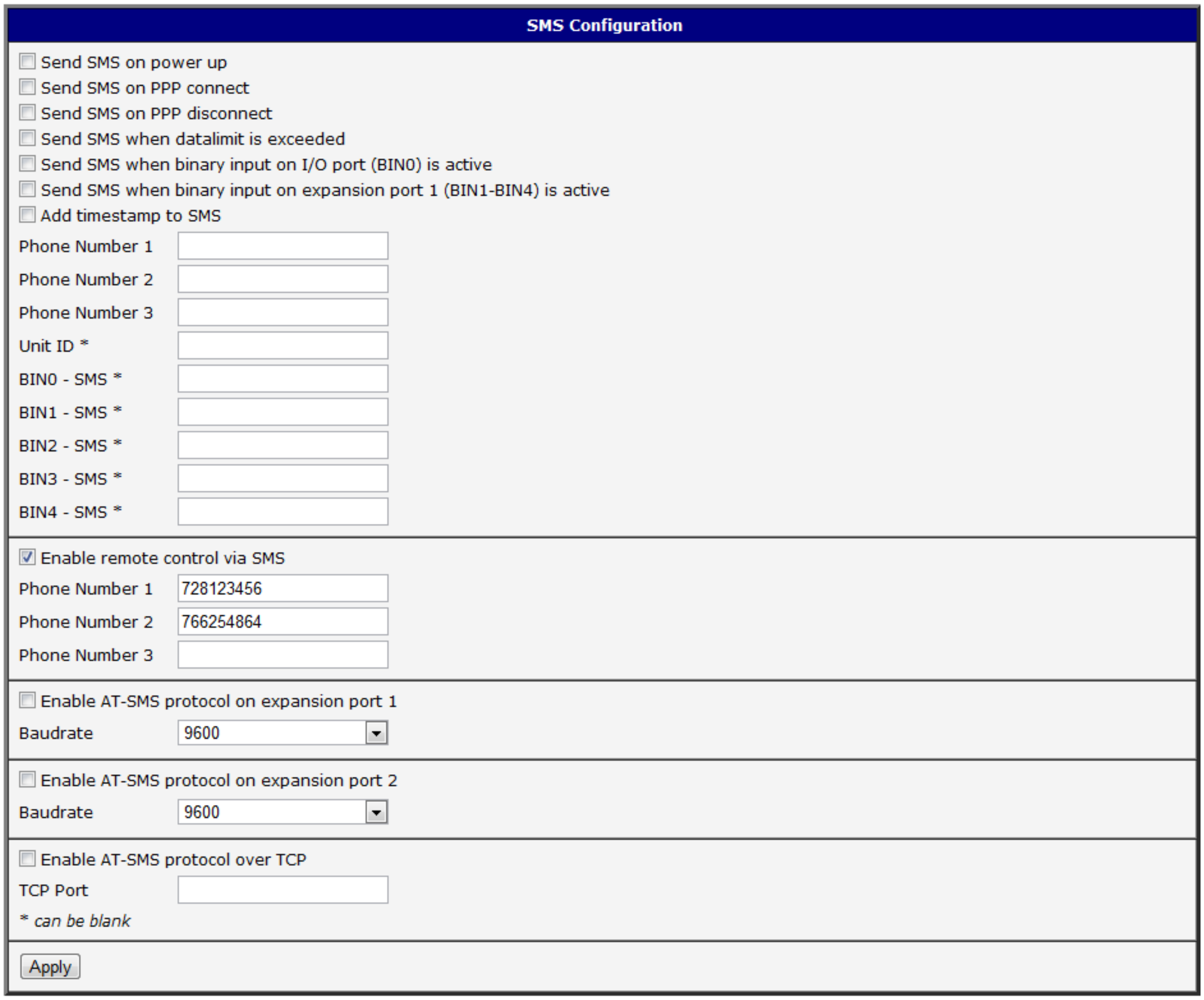
□ Enable AT-SMS protocol over TCP

TCP Port

** can be blank*

Figure 544. Example of SMS configuration 3

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



SMS Configuration

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

Phone Number 1	
Phone Number 2	
Phone Number 3	
Unit ID *	
BIN0 - SMS *	
BIN1 - SMS *	
BIN2 - SMS *	
BIN3 - SMS *	
BIN4 - SMS *	

☑ Enable remote control via SMS

Phone Number 1	728123456
Phone Number 2	766254864
Phone Number 3	

□ Enable AT-SMS protocol on expansion port 1

Baudrate 9600

□ Enable AT-SMS protocol on expansion port 2

Baudrate 9600

□ Enable AT-SMS protocol over TCP

TCP Port

** can be blank*

Figure 555. Example of SMS configuration 4

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.

Table 61: Expansion PORT configuration

Item	Description
Baud rate	Communication speed.
Data Bits	Number of data bits.

Parity	Control parity bit • none • even • odd
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: • TCP • UDP
Mode	Mode of connection: • TCP server - The router will listen for incoming TCP connection requests. • TCP client - The router will connect to a TCP server on the specified IP address and TCP port.
Server Address	When set to ***TCP client*** above, it is necessary to enter the ***Server address*** and ***TCP port***.
TCP Port	The TCP port for connections.

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

Table 602: TCP Keep-Alive configuration

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

It 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.

Table 613: CD signal description

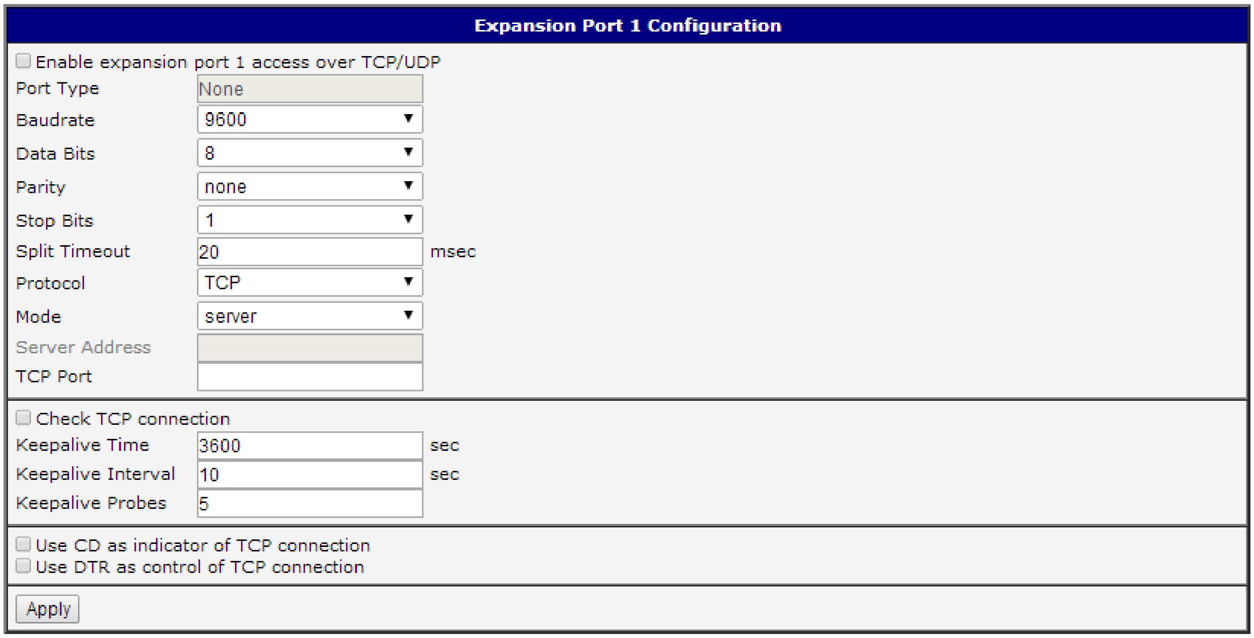
CD	Description
Active	TCP connection is on
Nonactive	TCP connection is off

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

Table 624: DTR signal description

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.

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



Expansion Port 1 Configuration

☐ Enable expansion port 1 access over TCP/UDP

Port Type	None	
Baudrate	9600 ▾	
Data Bits	8 ▾	
Parity	none ▾	
Stop Bits	1 ▾	
Split Timeout	20	msec
Protocol	TCP ▾	
Mode	server ▾	
Server Address		
TCP Port		

☐ Check TCP connection

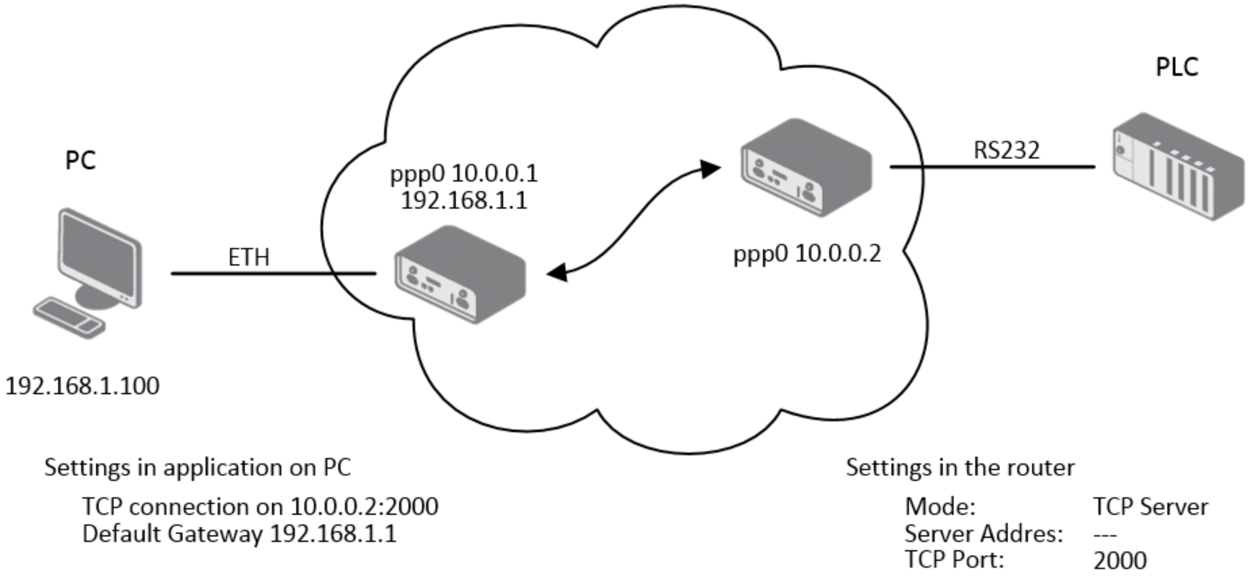
Keepalive Time	3600	sec
Keepalive Interval	10	sec
Keepalive Probes	5	

☐ Use CD as indicator of TCP connection

☐ Use DTR as control of TCP connection

Figure 56. Expansion port configuration

Example of external port configuration:



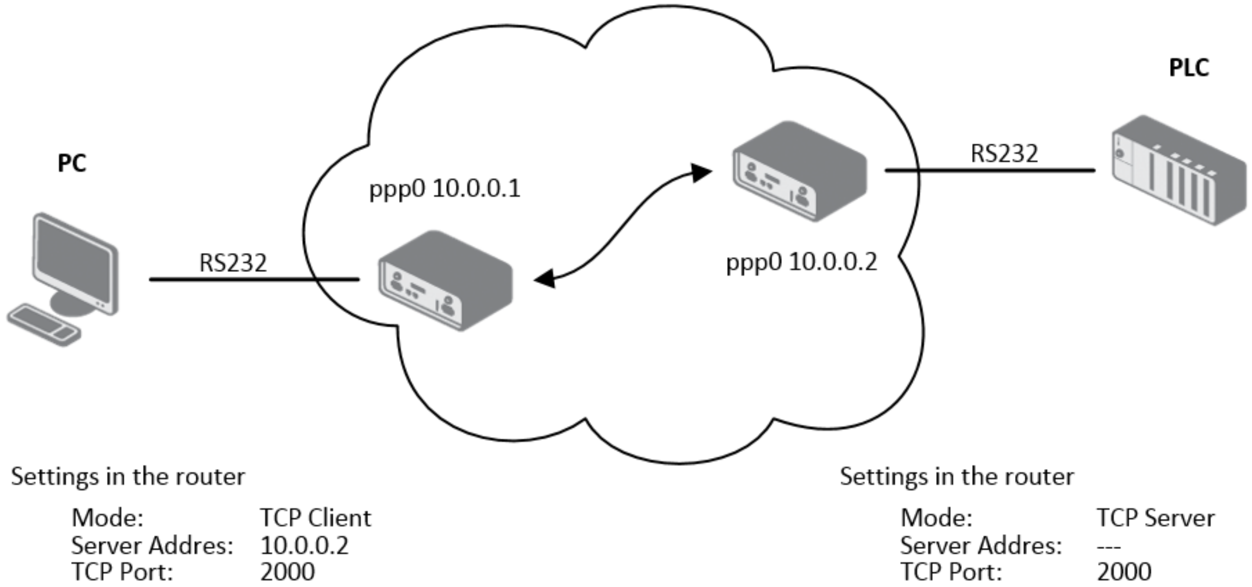
Settings in application on PC

TCP connection on 10.0.0.2:2000
Default Gateway 192.168.1.1

Settings in the router

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

Figure 577. example of Ethernet to serial communication



Settings in the router

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

Settings in the router

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

Figure 588. Example of serial port extension

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.

Table 635: USB port configuration 1

Item	Description
Baud rate	Applied communication speed.
Data Bits	Number of data bits.
Parity	Control parity bit • none • even • odd
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: • TCP - communication using a linked protocol TCP • UDP - communication using a unlinked protocol UDP
Mode	Mode of connection: • TCP server - The router will listen to incoming requests regarding the TCP connection. • TCP client - The router will connect to a TCP server on the specified IP address and TCP port.
Server Address	In mode *TCP client* it is necessary to enter the *Server address* and final *TCP port*.
TCP Port	In both modes of connection it is necessary to specify the TCP port on which the router will communicate TCP connections.

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

Table 646: USB port configuration 2

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

It 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.

Table 657: CD signal description

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

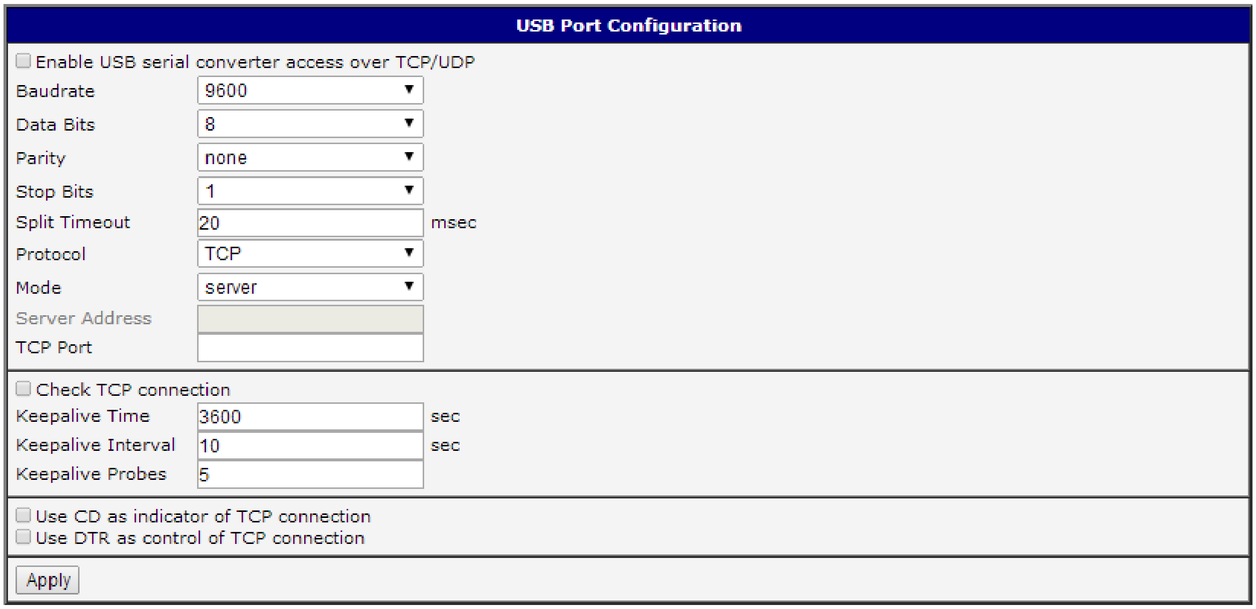
Select ***Use DTR as control of TCP connection*** to use DTR to control when TCP connections are allowed. (CD on the router).

Table 668: DTR signal description

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.

Supported USB/RS-232 converters:

- FTDI
- Prolific PL2303
- Silicon Laboratories CP210×



USB Port Configuration

☐ Enable USB serial converter access over TCP/UDP

Baudrate	9600 ▼	
Data Bits	8 ▼	
Parity	none ▼	
Stop Bits	1 ▼	
Split Timeout	20	msec
Protocol	TCP ▼	
Mode	server ▼	
Server Address		
TCP Port		

☐ Check TCP connection

Keepalive Time	3600	sec
Keepalive Interval	10	sec
Keepalive Probes	5	

☐ Use CD as indicator of TCP connection
☐ Use DTR as control of TCP connection

Figure 599. USB configuration

Example of USB port configuration:

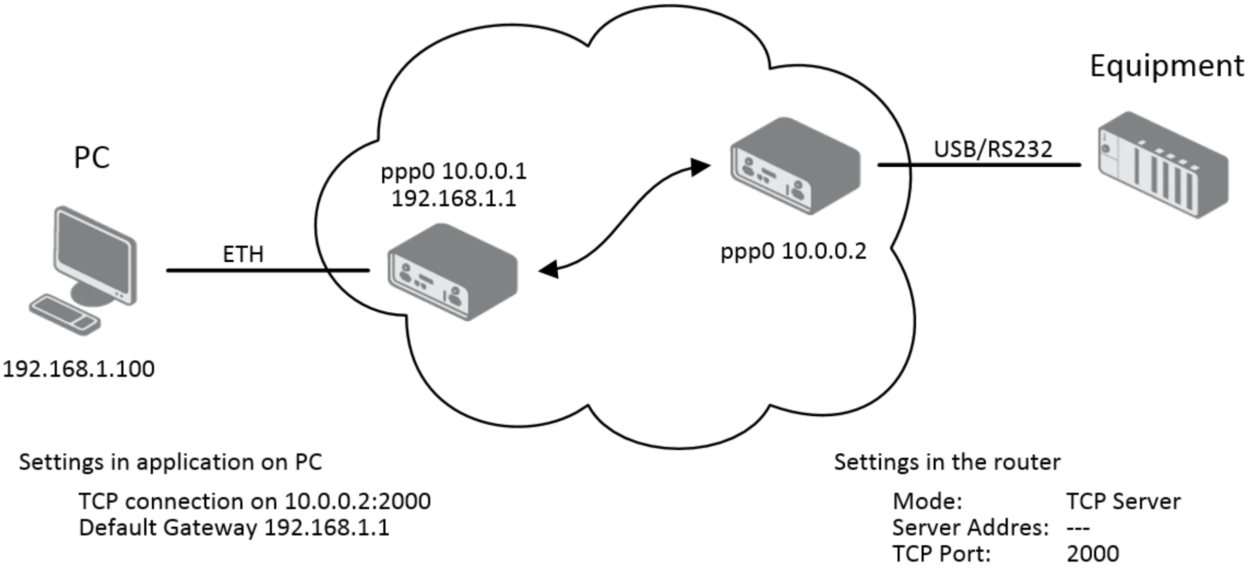


Figure 600. Example of Ethernet to serial using USB port

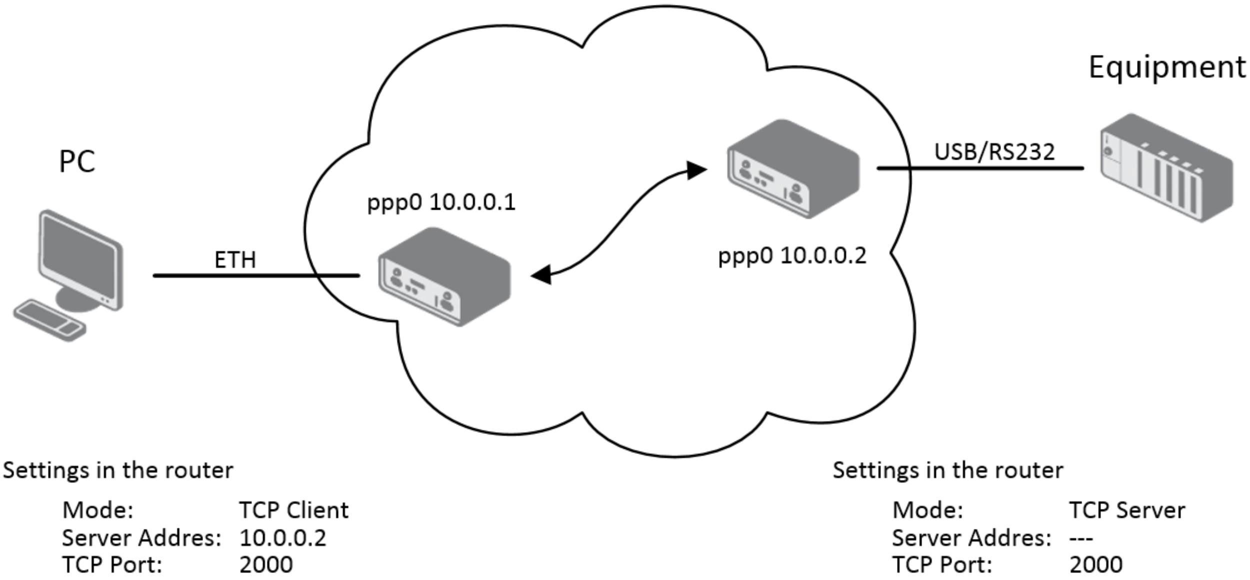
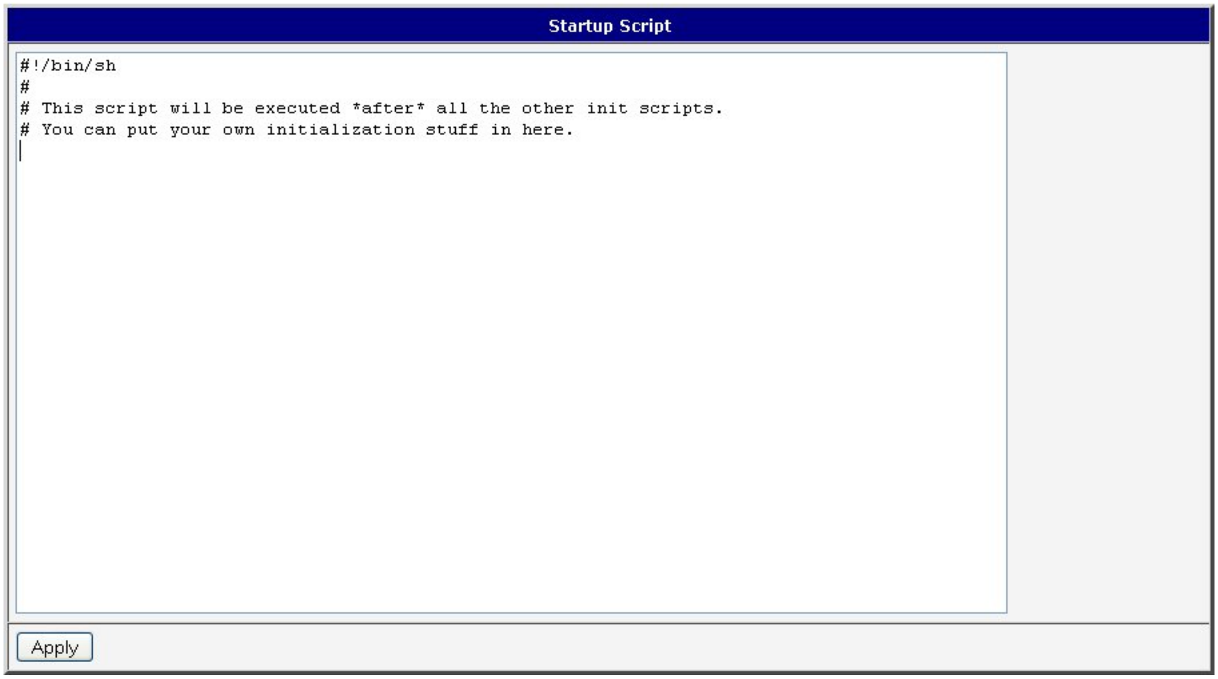


Figure 611. Example of serial extension using USB port

STARTUP SCRIPT

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

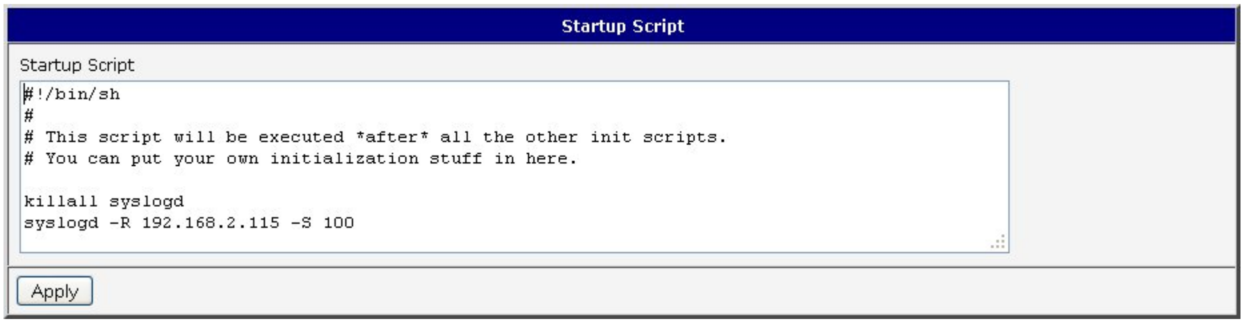


```
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here.
```

Figure 622. 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.

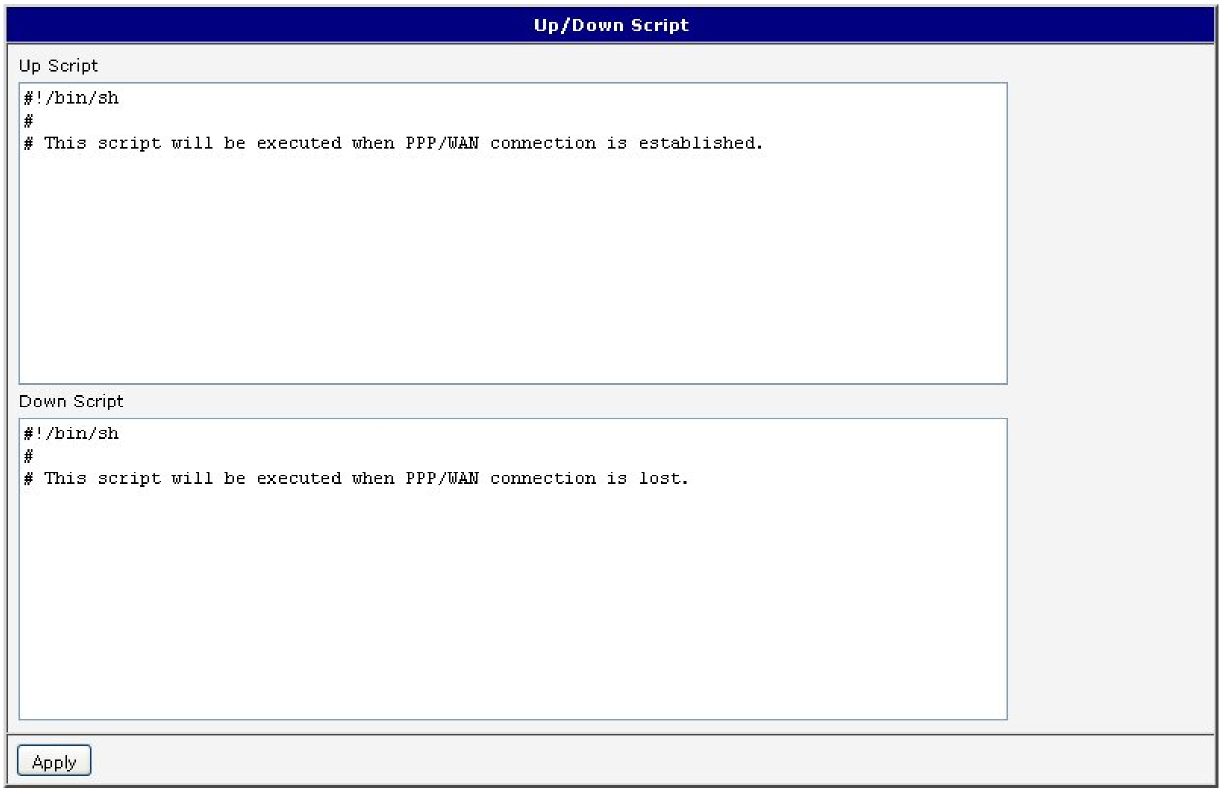


```
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here.

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

Figure 633. Example of startup script

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.

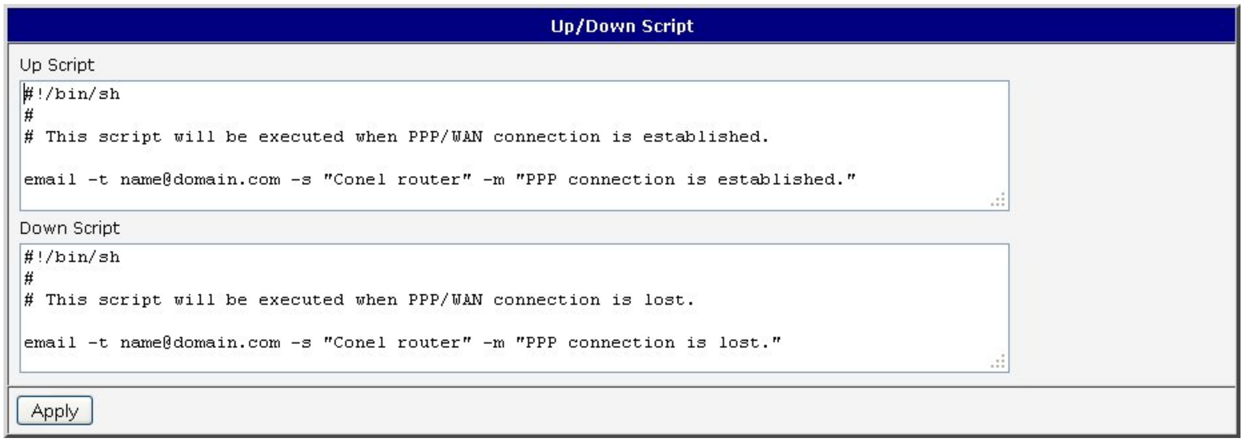


```
#!/bin/sh
#
# This script will be executed when PPP/WAN connection is established.
```

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

Figure 644. 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.



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

email -t name@domain.com -s "Conel router" -m "PPP connection is established."
```

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

email -t name@domain.com -s "Conel router" -m "PPP connection is lost."
```

Figure 655. Example of Up/Down script

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.

Table 679: Automatic update configuration

Item	Description
Source	Select the location of the update files: • ***HTTP/FTP server*** – Remote file server. • ***USB flash drive*** - Router will check for firmware or configuration files in the root directory of the connected USB device. • ***Both*** – Router will check for new firmware or configuration files in • both places.
Base URL	*Base URL* 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 *Update Hour.*

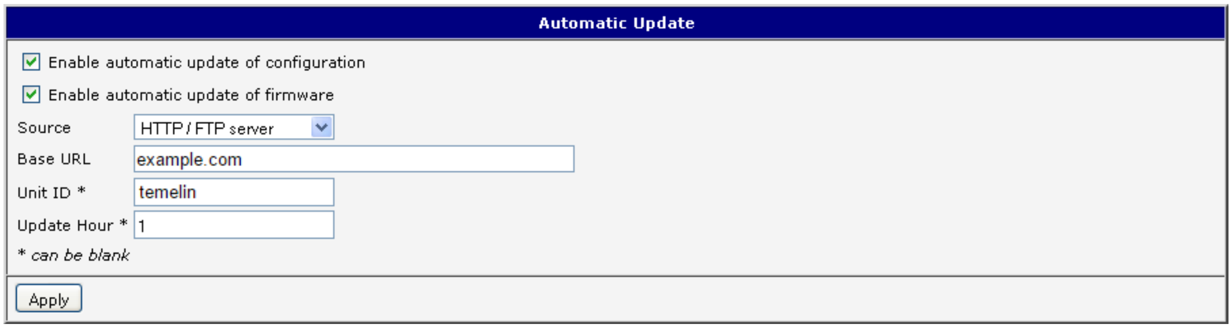
The **configuration file** name is from parameter *Base URL*, hardware MAC address of ETH0 interface and *cfg* extension. Hardware MAC address and *cfg* extension are added to the file name automatically and it isn’t necessary to enter them. When using parameter *Unit ID*, the hardware MAC address in 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://example.com/spectre3g.bin
- Configuration file: http://example.com/temelin.cfg


Automatic Update

☑ Enable automatic update of configuration

☑ Enable automatic update of firmware

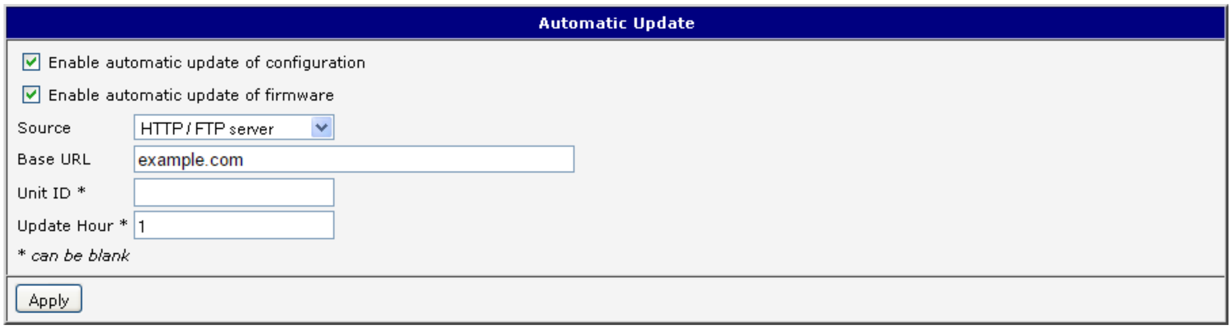
Source	HTTP / FTP server
Base URL	example.com
Unit ID *	temelin
Update Hour *	1

* *can be blank*

Figure 666. 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://example.com/spectre3g.bin
•	Configuration file:	http://example.com/00.11.22.33.44.55.cfg



Automatic Update

☑ Enable automatic update of configuration

☑ Enable automatic update of firmware

Source: HTTP / FTP server

Base URL: example.com

Unit ID *:

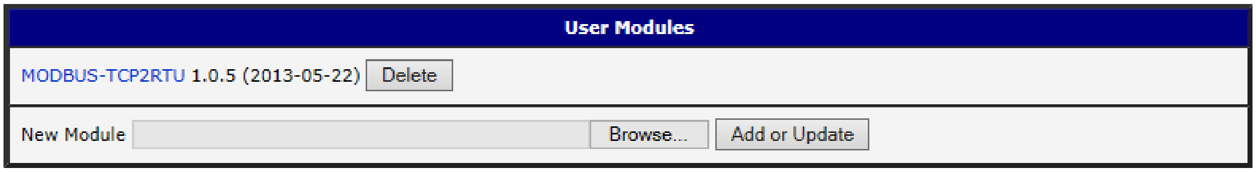
Update Hour *: 1

* *can be blank*

Figure 677. Example of automatic update 2

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.



User Modules

MODBUS-TCP2RTU 1.0.5 (2013-05-22)

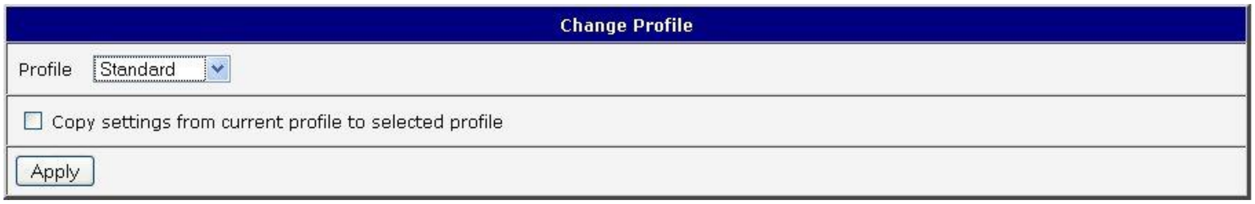
New Module:

Figure 688. User modules

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.



Change Profile

Profile: Standard

☐ Copy settings from current profile to selected profile

Figure 699. Change profile

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.

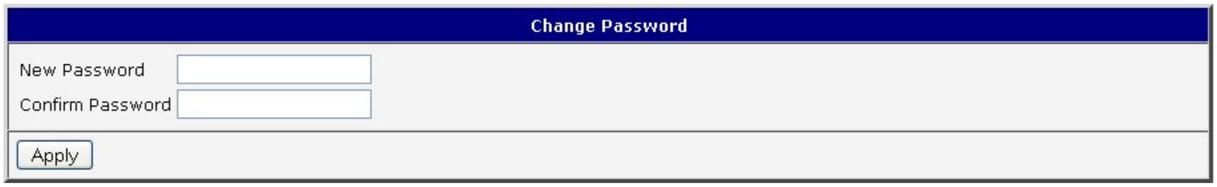


Figure 700. Change password

SET REAL TIME CLOCK

The internal clock of the router can be altered by selecting the ***Set Real Time Clock*** menu item. Date and time can be manually set by changing the ***Date*** and ***Time*** items. The clock can also be adjusted by using a NTP server. This would require you to enter the IP address or domain name of the NTP Server and click ***Apply*** to set the clock.

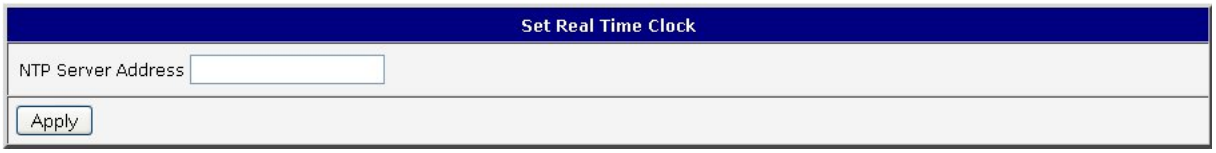


Figure 711. Set real time clock

SET SMS SERVICE CENTER ADDRESS

Note: *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.

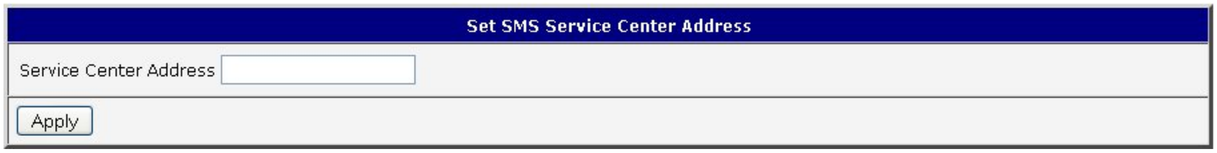


Figure 722. Set SMS service center address

UNLOCK SIM CARD

Note: *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 your SIM card provider if it has been blocked.

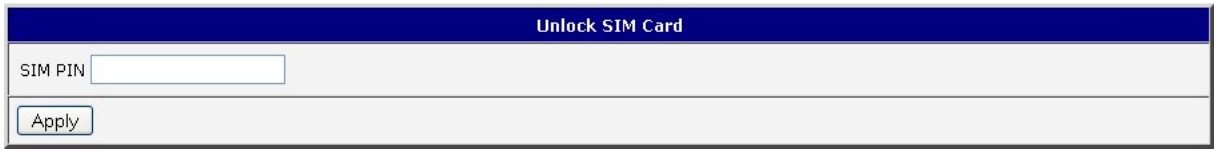


Figure 733. Unlock SIM card

SEND SMS

Note: *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.

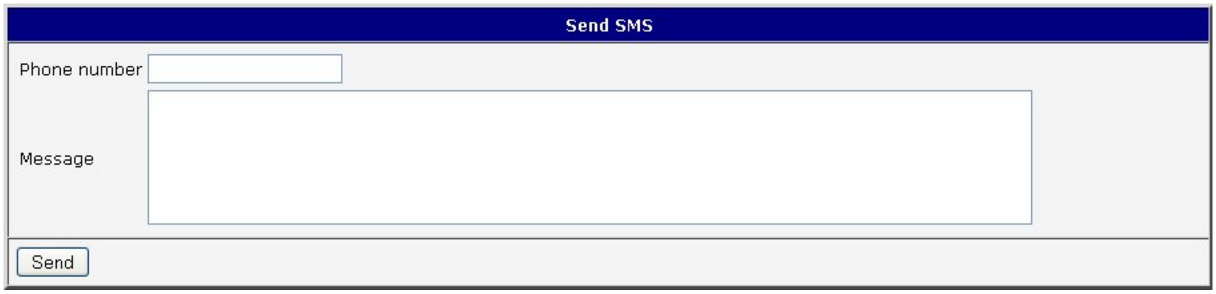


Figure 744. Send SMS

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

> *GET /send_exec.cgi?phone=%2B**420712345678**&message=**Test** HTTP/1.1*
> *Authorization: Basic cm9vdDpyb290*

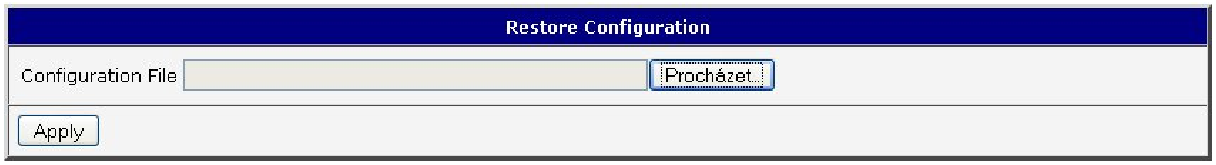
The HTTP request will be sent to TCP connection on router port 80. Router sends an SMS message with text "*Test*". SMS is sent to phone number ""*420712345678*". Authorization is in the format "user:password" coded by BASE64. In the example is used for root:root.

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.

RESTORE CONFIGURATION

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

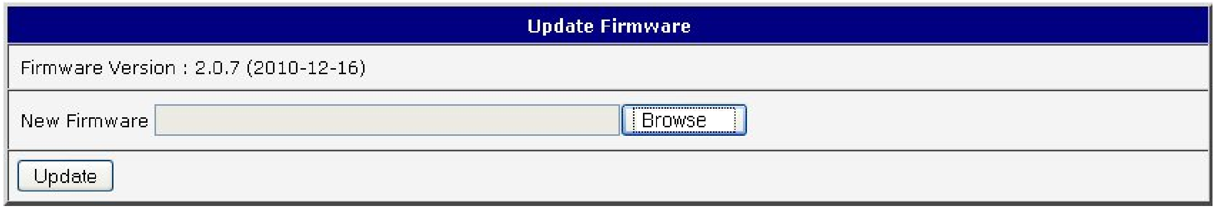

Restore Configuration

Configuration File

Figure 755. Restore configuration

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.**

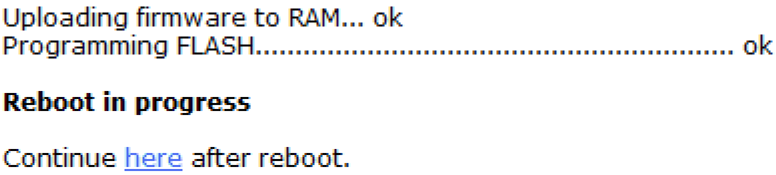

Update Firmware

Firmware Version : 2.0.7 (2010-12-16)

New Firmware

Figure 766. Update firmware

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


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

Reboot in progress

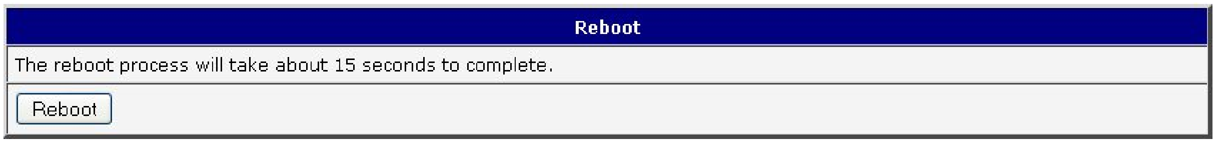
Continue here after reboot.

After the firmware update, the router will automatically reboot.

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

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.

Figure 777: 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:

Table 70: Telnet commands

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

3. WI-FI CONFIGURATION

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 **WI-FI** 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.

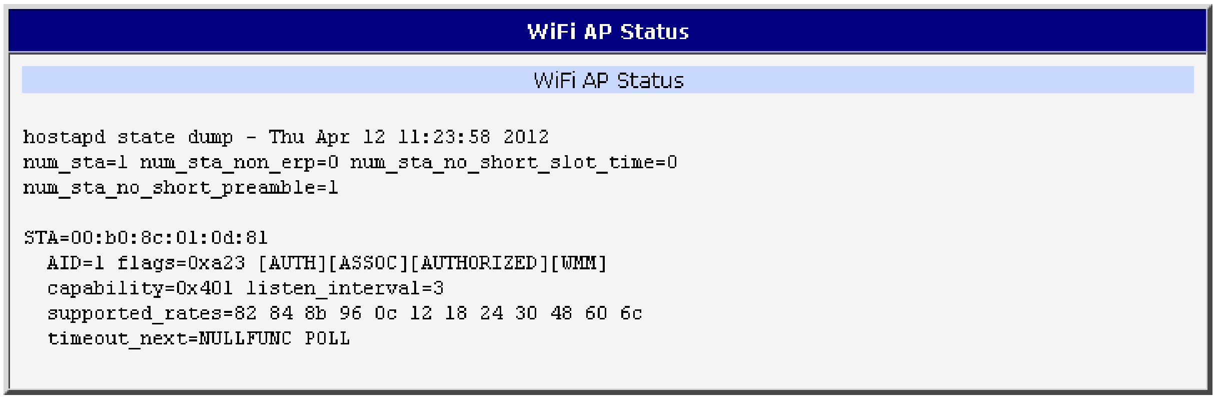
Table 7168: WI-FI AP state

Item	Description
hostapd state dump	Time stamp of actual WI-FI 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.

Data about connected clients is displayed as well.

Table 692: WI-FI client state

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



```
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
```

Figure 788: WI-FI AP status

Fig. 75: WI-FI AP Status

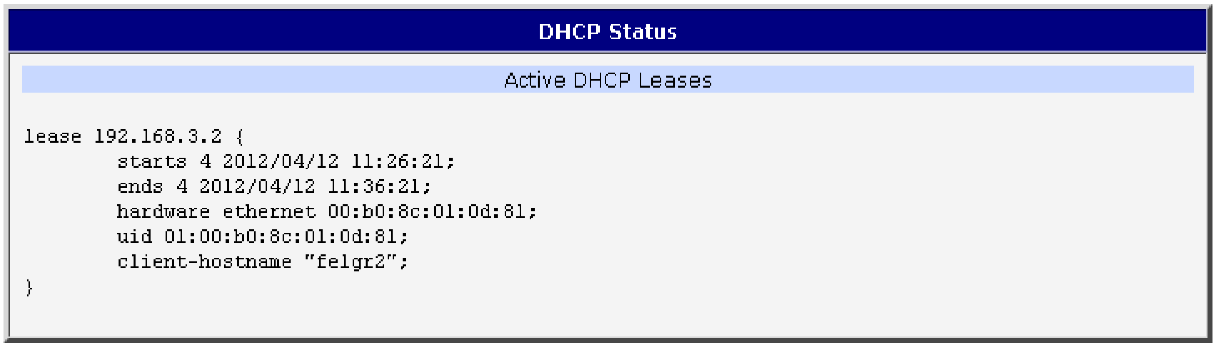
WLAN DHCP

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.

Table 703: Lease address

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



```
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";
}
```

Figure 799. WI-FI DHCP status

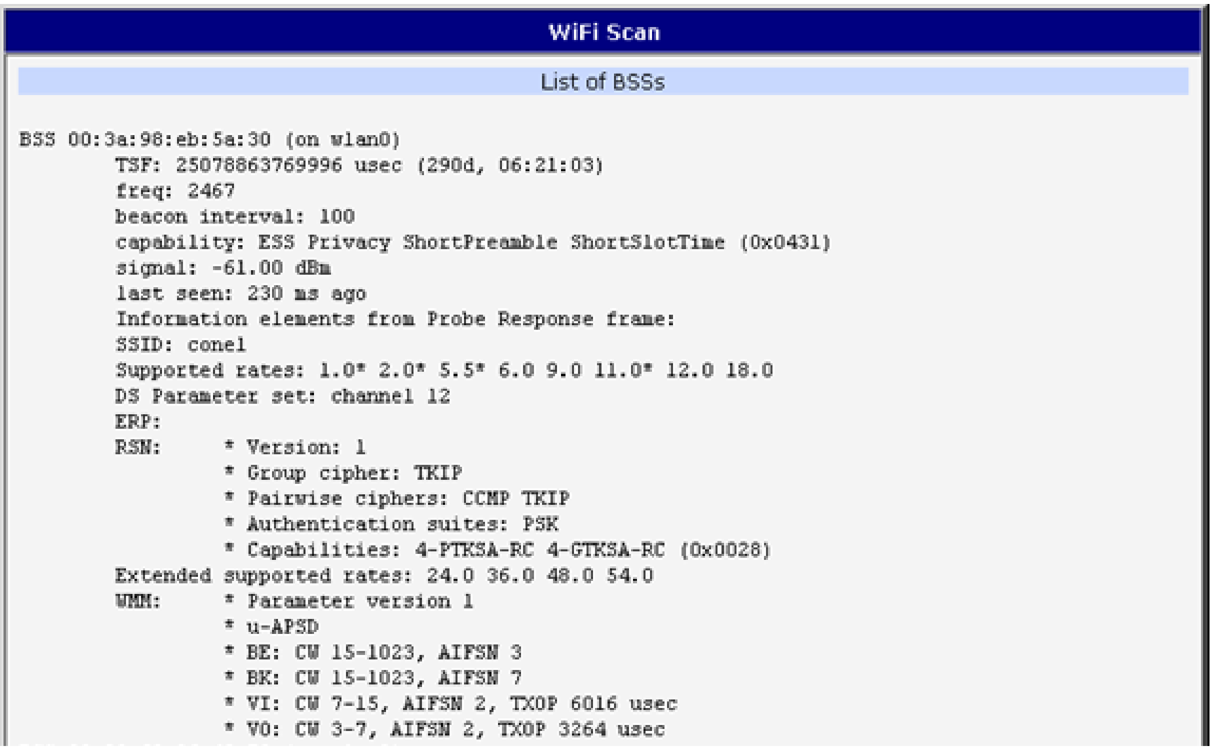
WIRELESS NETWORK SCANNING

Press ***Scan*** to scan neighboring WI-FI networks. Scanning can only be performed if the access point (WI-FI AP) is OFF.

.

Table 714: Neighboring WI-FI networks

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).

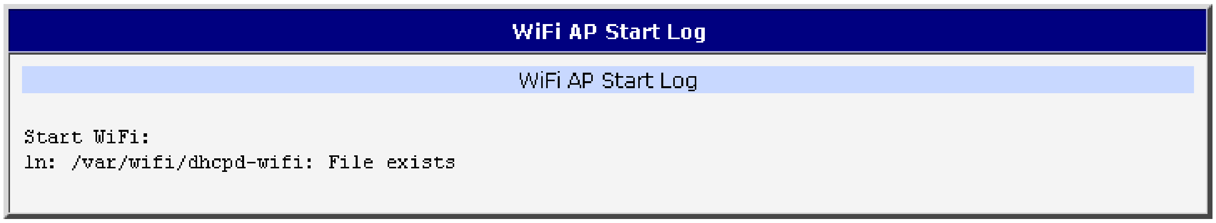


```
BSS 00:3a:98:eb:5a:30 (on wlan0)
        TSF: 25078863769996 usec (290d, 06:21:03)
        freq: 2467
        beacon interval: 100
        capability: ESS Privacy ShortPreamble ShortSlotTime (0x0431)
        signal: -61.00 dBm
        last seen: 230 ms ago
        Information elements from Probe 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
        WMM:     * 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
```

Figure 800. WI-FI Scan

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.

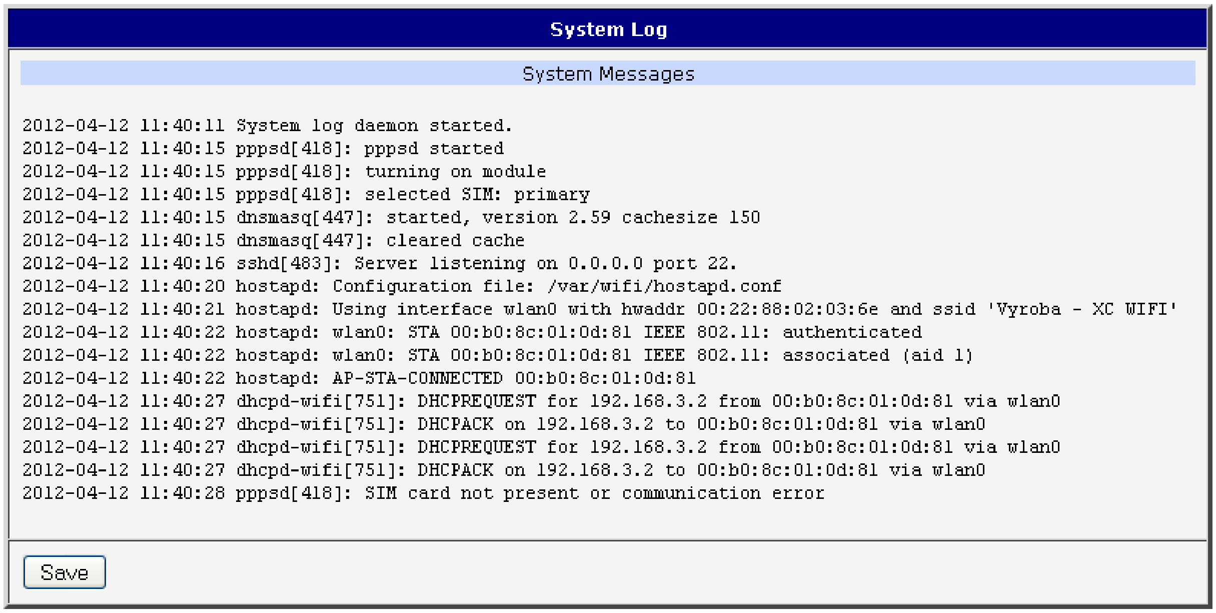


```
Start WiFi:
ln: /var/wifi/dhcpd-wifi: File exists
```

Figure 811. WI-FI AP start log

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.



```
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
```

Figure 822. System log

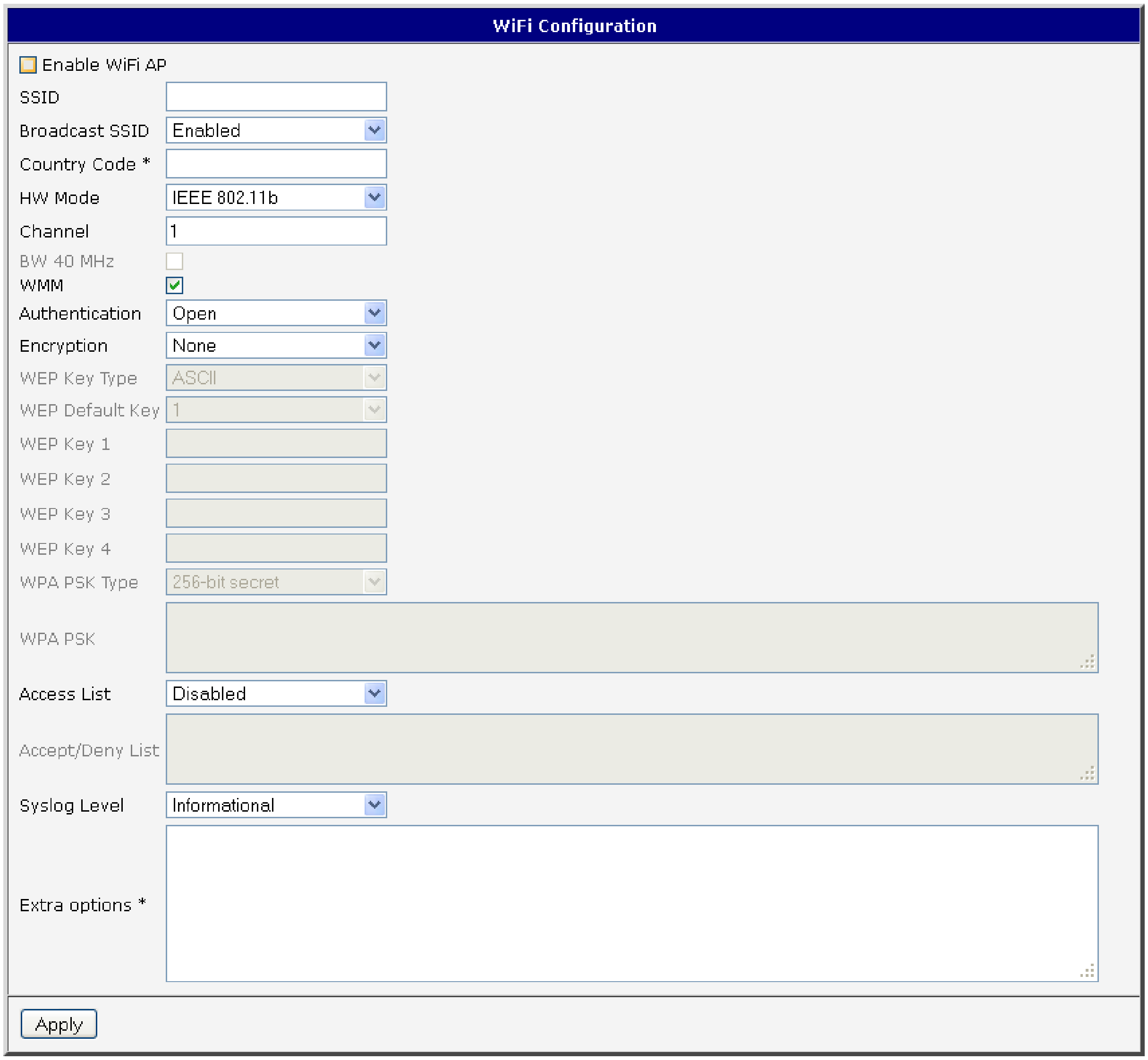
WI-FI ACCESS POINT CONFIGURATION

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

Table 725: WI-FI AP parameters

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. • Enabled – SSID is broadcast in beacon frames. • Zero length – Beacon frame does not include SSID. Requests for sending beacon frame are ignored. • Clear – All SSID characters in beacon frames are replaced by 0. Original length is kept. Requests for sending beacon frames are ignored.
Country Code	Code of the country where the router is installed. This code must be entered in **ISO 3166-1 alpha-2 format**. If a country code isn't specified and the router has not implemented a system to determine this code, it will use "US" as the default country code . If no country code is specified or if the wrong country code is entered, 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. • IEE 802.11b • IEE 802.11b+g • IEE 802.11b+g+n
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. 1. Open - Authentication is not required. Free access point. 2. Shared – Base authentication using WEP key. 3. WPA-PSK - Authentication using better authentication methods PSK-PSK. 4. WPA2-PSK - WPA-PSK using new encryption AES.
Encryption	Type of data encryption in the WI-FI network • None – No data encryption. • WEP – Encryption using static WEP keys. This encryption can be used for Shared authentication. • TKIP – Dynamic encryption key management that can be used for WPA-PSK and WPA2-PSK authentication.
	• AES - Improved encryption used for WPA2-PSK authentication.
WEP Key Type	Type of WEP key for WEP encryption. • ASCII – WEP key in ASCII format • HEX – WEP key in hexadecimal format
WEP Default Key	This item specifies default WEP key.

WEP Key X	Items for different 4 WEP keys. • WEP key in ASCII format must be entered in quotes. This key can be specified in the following lengths. • 5 ASCII characters (40b WEP key) • 13 ASCII characters (104b WEP key) • 16 ASCII characters (128b WEP key) • WEP key must be entered in hexadecimal digits. This key can be specified in the following lengths. • 10 hexadecimal digits (40b WEP key) • 26 hexadecimal digits (104b WEP key) • 32 hexadecimal digits (128b WEP key)
WPA PSK Type	Type of key for WPA-PSK authentication. • 256-bit secret • ASCII passphrase • PSK File
WPA PSK	Key for WPA-PSK authentication. This key must be entered according to the selected WPA PSK type as follows. • 256-bit secret - 64 hexadecimal digits • ASCII passphrase – 8 to 63 characters • PSK File – absolute path to the file containing the list of pairs (PSK key, MAC address)
Access List	Mode of Access/Deny list. • Disabled – Accept/Deny list is not used. • Accept – Clients in Accept/Deny list can access the network. • Deny – Clients in Access/Deny list cannot access the network.
Accept/Deny List	Accept or Deny list of client MAC addresses that set network access. Each MAC address is separated by new line.
Syslog Level	Logging level, when system writes to the system log. • Verbose debugging – The highest level of logging. • Debugging • Informational – Default level of logging • Notification • Warning – The lowest level of communicativeness.



WiFi Configuration

☐ Enable WiFi AP

SSID	
Broadcast SSID	Enabled
Country Code *	
HW Mode	IEEE 802.11b
Channel	1
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 *	

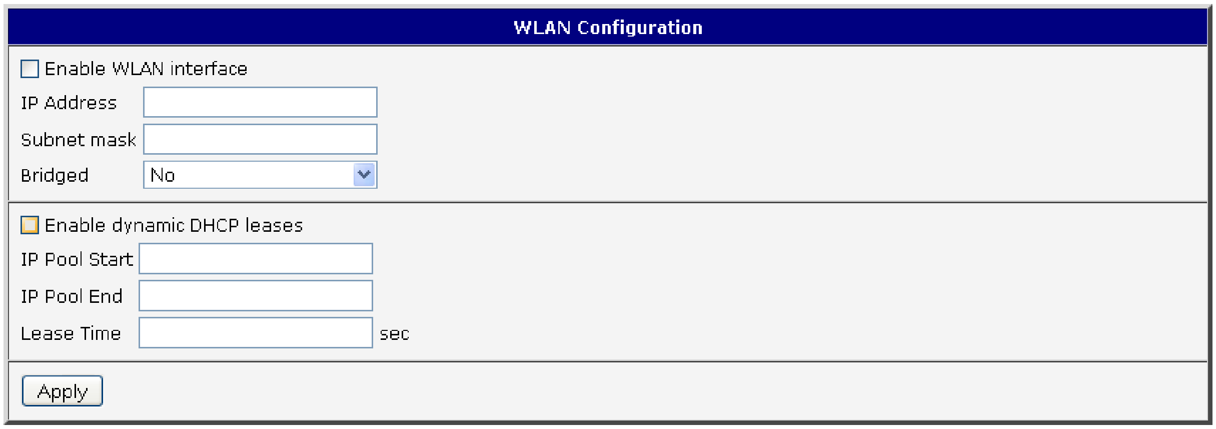
Figure 833. WI-FI AP configuration page

WLAN CONFIGURATION

The WI-FI LAN and DHCP server page is displayed by selecting ***"WLAN"*** in the configuration section.

Table 73: WLAN parameter

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	• No - Bridged mode is not allowed. WLAN network is not connected with LAN router. • 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).
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



WLAN Configuration

□ Enable WLAN interface

IP Address

Subnet mask

Bridged: No

□ Enable dynamic DHCP leases

IP Pool Start

IP Pool End

Lease Time sec

Apply

Figure 844. WLAN configuration

WI-FI PORT LEDS

Table 747: WI-FI LED state indication

LED port indicator	
Green LED	WI-FI port is powered on.
Yellow LED	Permanently off.

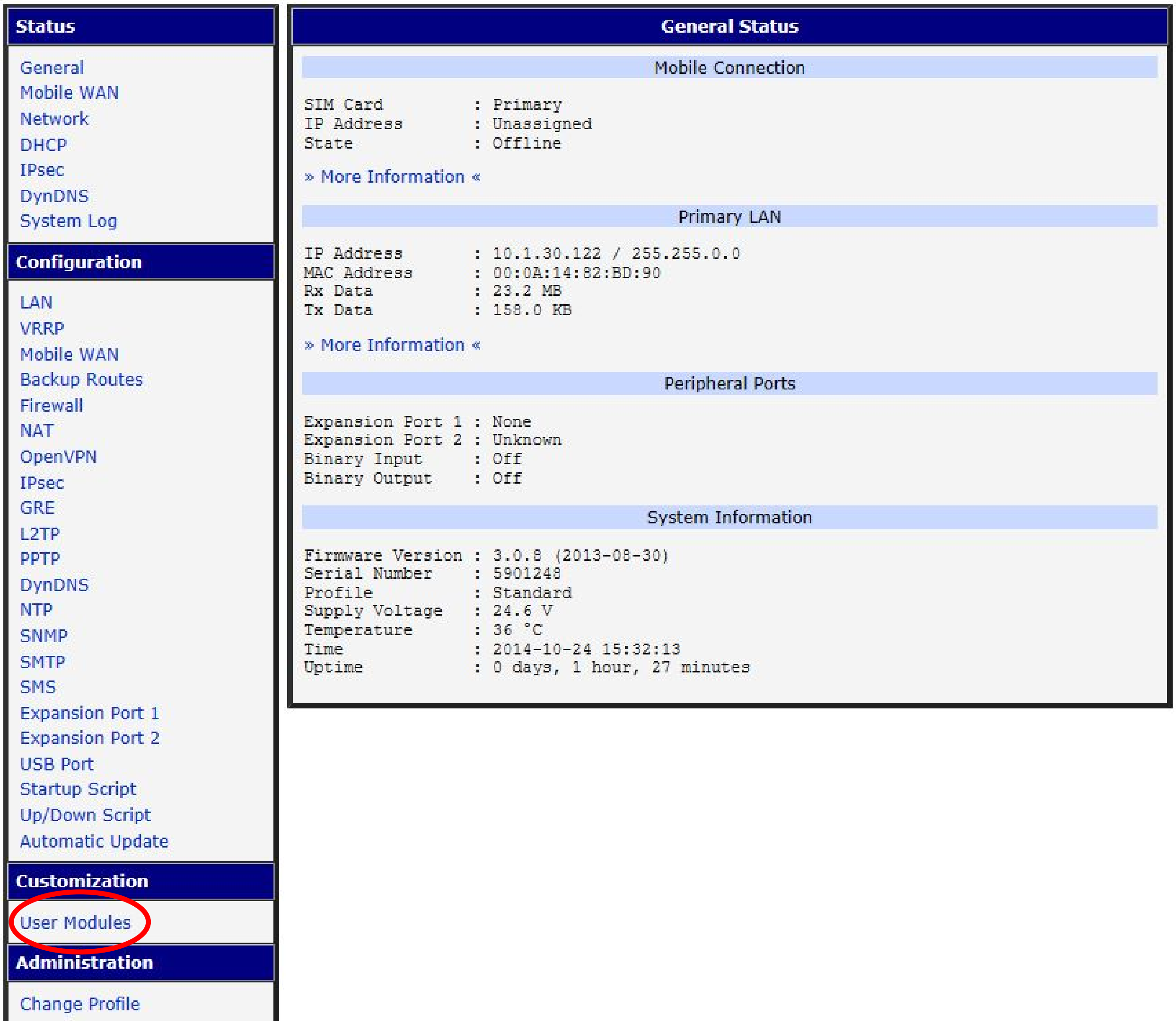
4. IoT NETWORK GATEWAY CONFIGURATION

IoT NETWORK GATEWAY

The SPECTRE Network Gateway routers can provide access to the Wzzard sensor network using a built-in SmartMesh IP module. Support for the Wzzard sensor network is provided by a User Software module which is pre-loaded into the SPECTRE Network Gateway router at the factory. The Wzzard sensor network uses MQTT-SN protocol to communicate between the sensor edge nodes and the gateway. The gateway and the sensor edge nodes must be configured with the same Network ID and Join Key in order for them to communicate with each other. The gateway functions as an MQTT bridge and forwards MQTT-SN data from the sensor nodes to a remote MQTT broker. The Network Gateway also has an internal MQTT v3.1 Broker that allows external MQTT clients to access the sensor node data.

GATEWAY CONFIGURATION

Select the **User Modules** item under the Customization section of the main menu to view the **IoT Gateway** user module.



```
SIM Card         : Primary
IP Address       : Unassigned
State            : Offline
```

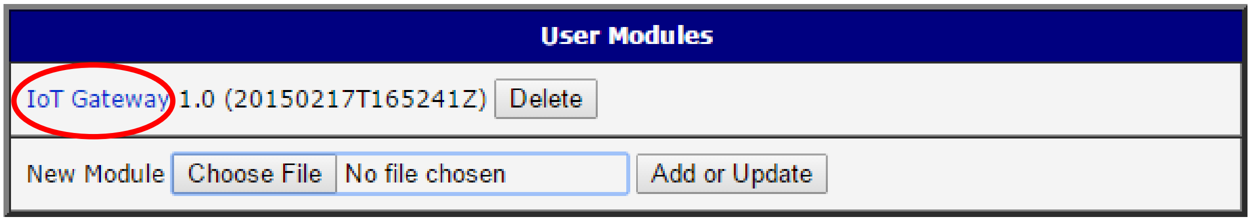
```
IP Address       : 10.1.30.122 / 255.255.0.0
MAC Address      : 00:0A:14:82:BD:90
Rx Data          : 23.2 MB
Tx Data          : 158.0 KB
```

```
Expansion Port 1 : None
Expansion Port 2 : Unknown
Binary Input     : Off
Binary Output    : Off
```

```
Firmware Version : 3.0.8 (2013-08-30)
Serial Number    : 5901248
Profile          : Standard
Supply Voltage   : 24.6 V
Temperature      : 36 °C
Time             : 2014-10-24 15:32:13
Uptime           : 0 days, 1 hour, 27 minutes
```

Figure 85. WLAN configuration

This web page shows the user modules that have been loaded into the router and the version number of each module. Click on the IoT Gateway user module to bring up the configuration screen.



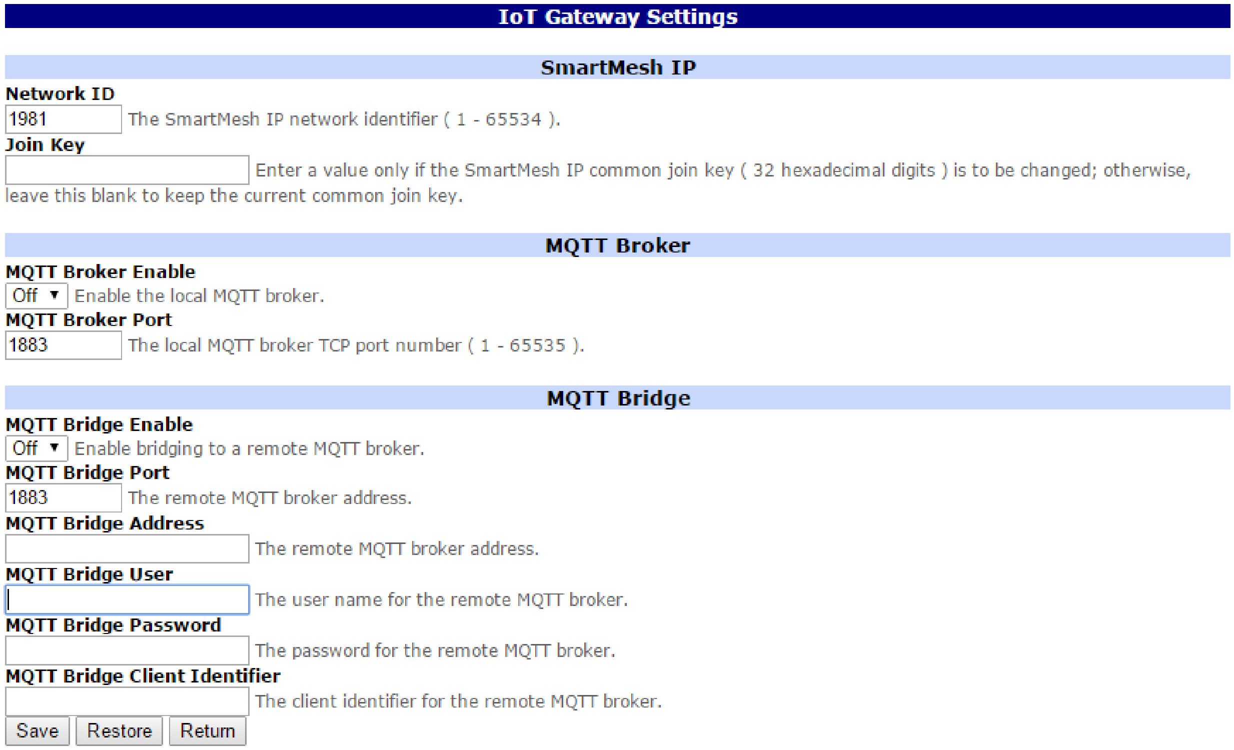
User Modules

IoT Gateway 1.0 (20150217T165241Z) Delete

New Module Choose File No file chosen Add or Update

Figure 86. WLAN configuration

The IoT Gateway configuration screen contains sections for configuring the sensor network, the internal MQTT broker, and the MQTT Bridge to an external cloud partner. Once the parameters have been configured, click on the Save button to store the settings in the gateway. The Restore button can be used to reset the text boxes to the stored values.



IoT Gateway Settings

SmartMesh IP

Network ID
1981 The SmartMesh IP network identifier (1 - 65534).

Join Key
Enter a value only if the SmartMesh IP common join key (32 hexadecimal digits) is to be changed; otherwise, leave this blank to keep the current common join key.

MQTT Broker

MQTT Broker Enable
Off ▾ Enable the local MQTT broker.

MQTT Broker Port
1883 The local MQTT broker TCP port number (1 - 65535).

MQTT Bridge

MQTT Bridge Enable
Off ▾ Enable bridging to a remote MQTT broker.

MQTT Bridge Port
1883 The remote MQTT broker address.

MQTT Bridge Address
The remote MQTT broker address.

MQTT Bridge User
The user name for the remote MQTT broker.

MQTT Bridge Password
The password for the remote MQTT broker.

MQTT Bridge Client Identifier
The client identifier for the remote MQTT broker.

SMARTMESH IP CONFIGURATION

Each SmartMesh Sensor Network gateway must have a unique network ID to prevent interference from other SmartMesh networks. Each sensor node must be programmed with the network ID of the gateway that it should communicate with. In addition, each sensor node on the network must also have the same join key defined. This is a 128-bit value that is used to encrypt the data between the nodes and the gateway. If the join key on the sensor edge node does not match the key programmed into the gateway, the sensor edge node will not be able to communicate with the gateway.

Table 75: SmartMesh IP parameters

Item	Description
Network ID	Identifies the gateway to other devices on the network

Join Key	128-bit value that is used to encrypt the communication between the node and the gateway.

MQTT BROKER CONFIGURATION

Each SmartMesh Sensor Network gateway has an internal MQTT Broker for connecting with external MQTT clients. The default IP port for the broker is 1883.

Table 76: MQTT Broker parameters

Item	Description
On/Off	Enables the internal MQTT Broker
MQTT Broker Port	IP Port used to access the internal broker

MQTT BRIDGE CONFIGURATION

Each SmartMesh Sensor Network gateway has an internal MQTT Bridge for connecting with an external MQTT broker or pubic platform provider. For a public platform provider, the specific configuration settings will be provided by the individual provider.

Table 77: MQTT Bridge parameters

Item	Description
On/Off	Enables the internal MQTT Bridge function
MQTT Bridge Port	IP Port of the external MQTT broker
MQTT Bridge Address	IP Address of the external MQTT broker
MQTT Bridge User	User name for the external MQTT broker
MQTT Bridge Password	Password for the external MQTT broker
MQTT Bridge Client Identifier	The unique client ID for the external MQTT broker

SMARTMESH IP PORT LEDS

Table 78: SmartMesh IP Port 2 LEDs

LED port indicator	
Green LED	SmartMesh IP module is powered on.
Yellow LED	Permanently off.