HIRSCHMANN

A BELDEN BRAND

User Manual

Configuration
Industrial Cellular Router
OWL LTE

UM Configuration OWL LTE
Release 1.0 Rev. 03 - 06/2018

Technical support
https://hirschmann-support.belden.com

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at the Hirschmann product site (http://www.hirschmann.com).

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany

Contents

About this Manual

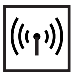
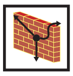
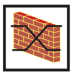
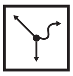
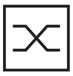
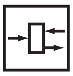
This "Configuration" user manual contains the information you need to start operating the device. It takes you step by step from the first startup operation through to the basic settings for operation in your environment.

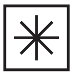
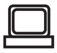
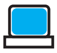
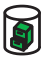
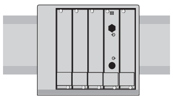
Key

The designations used in this manual have the following meanings:

▶	List
□	Work step
■	Subheading
Link	Cross-reference with link
Note:	A note emphasizes an important fact or draws your attention to a dependency.
`Courier`	ASCII representation in the graphical user interface

Symbols used:

	WLAN access point
	Router with firewall
	Switch with firewall
	Router
	Switch
	Bridge

	Hub
	A random computer
	Configuration Computer
	Server
	PLC - Programmable logic controller
	I/O - Robot

Safety Instructions

⚠ **WARNING**
UNCONTROLLED MACHINE ACTIONS To avoid uncontrolled machine actions caused by data loss, configure all the data transmission devices individually. Before you start any machine which is controlled via data transmission, be sure to complete the configuration of all the data transmission devices. **Failure to follow these instructions can result in death, serious injury, or equipment damage.**

1 Basic Information

The OWL Industrial Cellular Router is designed for wireless communication in mobile networks using LTE, HSPA+, UMTS, EDGE or GPRS technology. Due to the high speed of data transfer up to 100 Mbit/s (download) and up to 50 Mbit/s (upload). The router is an ideal wireless solution for connecting the data stream of security camera systems, individual computers, LANs, automatic teller machines (ATM), and other self-service terminals.

The graphical user interface (GUI) is password protected. After logging in, the GUI provides detailed statistics about the router activities, signal strength, and a detailed system log. You can also create VPN tunnels using IPSec, OpenVPN and L2TP for secure communications.

The router also supports the following functions.

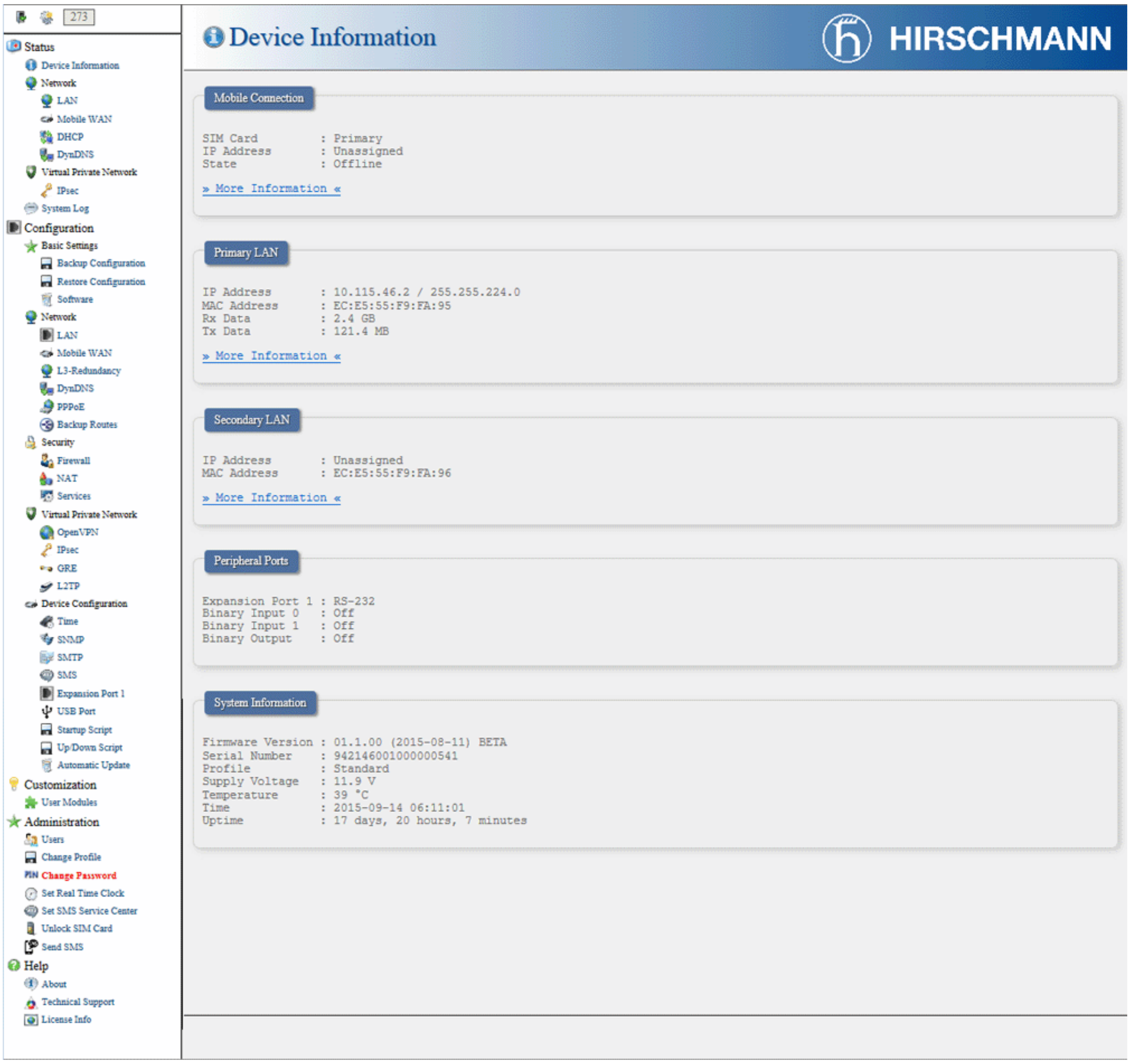
- DHCP
- NAT
- DynDNS
- NTP
- VRRP
- Control using SMS
- primary/backup connection

Using a special window, the start up script window, you can insert Linux scripts for various actions. The device also allows you to create several different configurations for a router. You can exchange these configurations as necessary using an SMS for example. The router can automatically upgrade a configuration and firmware from a server. This allows you to configure several routers at a time.

1.1 Access to the GUI Configuration

For monitoring, configuring and managing the router, use the GUI interface. You can access the GUI interface using the secure HTTPS protocol and the IP address of the router. The default IP address of the router is 192.168.1.1. Initially, only the user `admin` with the password `private` can configure the router.

Note: Wireless transmissions only functions when you activate the SIM card for data traffic and insert it into the router. Remove the power source before inserting the SIM card.



Mobile Connection

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

» More Information «
```

Primary LAN

```
IP Address        : 10.115.46.2 / 255.255.224.0
MAC Address       : EC:E5:55:F9:FA:95
Rx Data           : 2.4 GB
Tx Data           : 121.4 MB

» More Information «
```

Secondary LAN

```
IP Address        : Unassigned
MAC Address       : EC:E5:55:F9:FA:96

» More Information «
```

Peripheral Ports

```
Expansion Port 1 : RS-232
Binary Input 0   : Off
Binary Input 1   : Off
Binary Output    : Off
```

System Information

```
Firmware Version : 01.1.00 (2015-08-11) BETA
Serial Number    : 942146001000000541
Profile          : Standard
Supply Voltage   : 11.9 V
Temperature      : 39 °C
Time             : 2015-09-14 06:11:01
Uptime           : 17 days, 20 hours, 7 minutes
```

Figure 1: Example of the Web Configuration

The "Device Information" dialog is the first dialog that the router displays after logging in. The left side of the dialog contains a menu tree with sections for monitoring (Status), configuration (Configuration), and administration (Administration) of the router.

Note: For increased security of the network connected to the router, change the default router password. When the default password of the router is still active, the "Change password" title is highlighted in red.

After the green LED illuminates, it is possible to restore the initial settings of the router by pressing the "Reset" button on the rear panel. If you press the "Reset" button, the configuration returns to the default settings and the router reboots (the green LED is on).

1.1.1 Secured access to web configuration

It is possible to access to the GUI interface using the HTTPS protocol. If your router still has the default IP address configured, enter https://192.168.1.1 into your web browser. When you access the router for the first time, the router requires you to accept the security certificate. The browser reports a disagreement in the domain, and an unverified certificate.

To prevent this message, upload a new certificate and key to the router using the following steps:

□ Create a new certificate.
□ Generate an new key.
□ Enable the SSH function on the router.
□ Connect to the router using SSH.
□ Replace the file, /etc/certs/https_cert, on the router with your newly created certificate.
□ Replace the file /etc/certs/https_key with your newly generated key.

1.2 Status

1.2.1 Device Information

You can access a summary of basic router information and its activities by opening the "Device Information" dialog. The "Device Information" dialog is the default dialog displayed when you login to the device. Information is divided into the following frames according to the type of router activity or the properties area:

- Mobile Connection
- Primary LAN
- Secondary LAN
- Peripherals Ports
- System Information

Mobile Connection

Parameter	Description
SIM Card	Displays the identification of the SIM card (Primary or Secondary).
Interface	Displays which interface is used.
Flags	Displays the network interface flags.
IP Address	Displays the IP address of the interface.
MTU	Displays the maximum packet size that the equipment is able to transmit.
Rx Data	Displays the total number of received bytes.
Rx Packets	Displays the total number of received packets.
Rx Errors	Displays the total number of erroneous received packets.
Rx Dropped	Displays the total number of dropped received packets.
Rx Overruns	Displays the total number of lost received packets because of overload.
Tx Data	Displays the total number of sent bytes.
Tx Packets	Displays the total number of sent packets.
Tx Errors	Displays the total number of erroneous sent packets.
Tx Dropped	Displays the total number of dropped sent packets.

Table 1: Mobile Connection

Parameter	Description
Tx Overruns	Displays the total number of lost sent packets because of overload.
Uptime	Displays how long the connection to mobile network is established.

Table 1: Mobile Connection

1.2.2 LAN and Peripheral Information

Parameters displayed in these frames have the same meaning as parameters described in the previous chapter. Moreover, the "MAC Address" parameter displays the MAC address assigned to the interface of the remote router. The dialog displays information divided into the following frames:

- The "Mobile Connection" frame displays information about the connection to the mobile network.
- The "Primary LAN" frame displays information about the eth0 interface.
- The "Secondary LAN" frame displays information about the eth1 interface.
- The "Peripheral Ports" frame displays information about the Extension and Binary ports.
- The "System Information" frame displays information about the hardware and firmware of the router.

The dialog displays information depending on the router configuration. See “LAN” on page 32.

Peripheral Ports

Parameter	Description
Expansion Port 1	Displays the type of expansion port fitted on the router.
Binary Input	Displays the state of binary input.
Binary Output	Displays the state of binary output.

Table 2: System Information

System Information

Parameter	Description
Firmware Version	Displays the information about the firmware version.
Serial Number	Displays the serial number of the router.
Profile	Displays the current profile. You use profiles to switch between different modes of operation. Possible value: ▶ `Standard` ▶ `Alternative`
Supply Voltage	Displays the voltage being supply to the router.
Temperature	Displays the temperature in the router.
Time	Displays the current date and time set in the router.
Uptime	Displays the how long the router has been in use.

Table 3: System Information

1.2.3 Network

LAN

To view information about the interfaces and the routing table, open the "LAN" dialog. The upper part of the dialog displays detailed information about the active interfaces only:

Parameter	Description
eth0, eth1	Displays status of the Network interfaces (Ethernet connection).
usb0	Displays the active PPP connection status to the mobile network. The wireless module is connected using a USB interface.
tun0	Displays the OpenVPN tunnel interface status.
gre1	Displays the GRE tunnel interface status.
lo	Displays the Local loopback interface status.

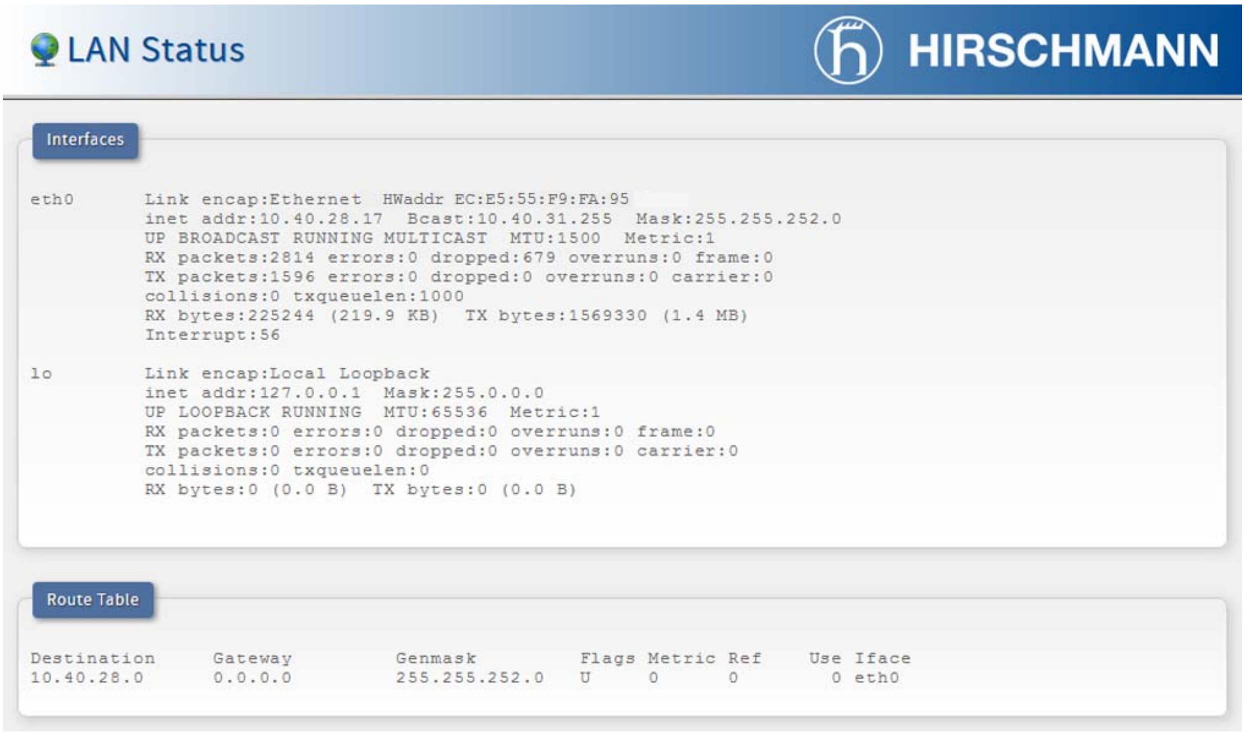
Table 4: Description of Interfaces in LAN Status

The dialog displays the following detailed information for each active connection:

Parameter	Description
HWaddr	Displays the unique address of networks interface.
inet	Displays the IP address of interface.
Bcast	Displays the broadcast address of the network connected to the device.
Mask	Displays the mask of network connected to the device.
MTU	Displays the maximum packet size that the router is able to transmit.
Metric	Displays the number of routers, that the packet traverses until it reaches the remote interface.
RX	Displays the number of packets received. Possible values: ▶ `errors` Displays the number of ingress packets with errors. ▶ `overruns` Displays the ingress packets lost because of an overload. ▶ `frame` Displays the number of ingress packets with incorrect packet size.
TX	Displays the number of packets transmitted. Possible values: ▶ `errors` Displays the number of packets egress with errors. ▶ `overruns` Displays the egress packets lost because of an overload. ▶ `frame` Displays the number of egress packets with incorrect packet size. ▶ `carrier` Displays the number of egress packets with detected errors resulting from the physical layer.
collisions	Displays the number of collisions on physical layer.
txqueuelen	Displays the Transmit Queue Length. The parameter displays the number of packets in the buffer of the router waiting for transmission.
RX bytes	Displays the total number of received bytes.
TX bytes	Displays the total number of transmitted bytes.

Table 5: Description of Information in LAN Status

You can view the status of the connection to mobile network in the "LAN Status" dialog. If the connection to a mobile network is active, it is displayed in the "Interfaces" frame as a `usb0` interface. At the bottom of the dialog, the router displays a "Route Table".



```
eth0      Link encap:Ethernet  HWaddr EC:E5:55:F9:FA:95
          inet addr:10.40.28.17  Bcast:10.40.31.255  Mask:255.255.252.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2814 errors:0 dropped:679 overruns:0 frame:0
          TX packets:1596 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:225244 (219.9 KB)  TX bytes:1569330 (1.4 MB)
          Interrupt:56

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

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.40.28.0      0.0.0.0         255.255.252.0   U     0      0        0 eth0
```

Figure 2: LAN Status

Mobile WAN

The "Mobile WAN" dialog contains current information about the mobile network connections.

The first part of the dialog, the "Mobile Network Information" frame, displays basic information about the mobile network in which the router is operating. There is also information about the module, which is installed in the router.

Parameter	Description
Registration	Displays the state of the network registration.
Operator	Displays the mobile network carrier in whose network the router is installed.
Technology	Displays the transmission technology used in the network.
PLMN	Displays the mobile network carrier code.
Cell	Displays the cell to which the router is connected.
LAC	Displays the Location Area Code. The LAS is a unique number assigned to each location area.
Channel	Displays the channel on which the router is communicating.

Table 6: Mobile Network Information

Parameter	Description
Signal Strength	Displays the signal strength of the selected cell.
Signal Quality	Displays the signal quality of the selected cell: Possible values: ▶ EC/IO for UMTS and CDMA The ratio of the signal received from the pilot channel (EC), to the overall level of the spectral density for example, the sum of the signals of other cells (IO). ▶ RSRQ for LTE technology The value is defined as the ratio of N×RSRP/RSSI. A value is not available for the EDGE technology.
CSQ	Displays the Cell Signal Quality. The value is a relative value given by RSSI (dBm). Possible values: ▶ `2-9` A value in this range means that the signal is marginal. ▶ `10-14` A value in this range means that the signal is OK. ▶ `15-16` A value in this range means that the signal is good. ▶ `20-30` A value in this range means that the signal is excellent.
Neighbors	Displays the signal strength of the neighboring listening cells.
Manufacturer	Displays the manufacturer of the module.
Model	Displays the type of module.
Revision	Displays the module revision.
IMEI	Displays the International Mobile Equipment Identity number of module.
ESN	Displays the Electronic Serial Number of module.
MEID	Displays the Mobile Equipment ID number of module.
ICCID	Displays the Integrated Circuit Card Identifier of the module. The ICCID is the international and unique serial number of the SIM card.

Table 6: Mobile Network Information

If a neighboring cell is highlighted in red, this indicates that the router is in jeopardy of repeatedly toggling between the neighboring cell and the primary cell. Toggling between the cells can affect the performance of the router. To prevent toggling, re-orient the antenna or use a directional antenna.

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

Period	Description
Today	Displays information about the signal quality for today from 0:00 to 23:59.
Yesterday	Displays information about the signal quality for yesterday from 0:00 to 23:59.
This week	Displays information about the signal quality for this week from Monday 0:00 to Sunday 23:59.
Last week	Displays information about the signal quality for last week from Monday 0:00 to Sunday 23:59.
This period	Displays information about the signal quality for this accounting period.
Last period	Displays information about the signal quality for last accounting period.

Table 7: Description of Period

Parameter	Description
Signal Min	Displays the minimal signal strength.
Signal Avg	Displays the average signal strength.
Signal Max	Displays the maximal signal strength.
Cells	Displays the number of times that the router toggled between cells.
Availability	Displays the availability of the router through the mobile network. The router displays the value as a percentage.

Table 8: Mobile Network Statistics

The following list contains tips for the "Mobile Network Statistics" frame:

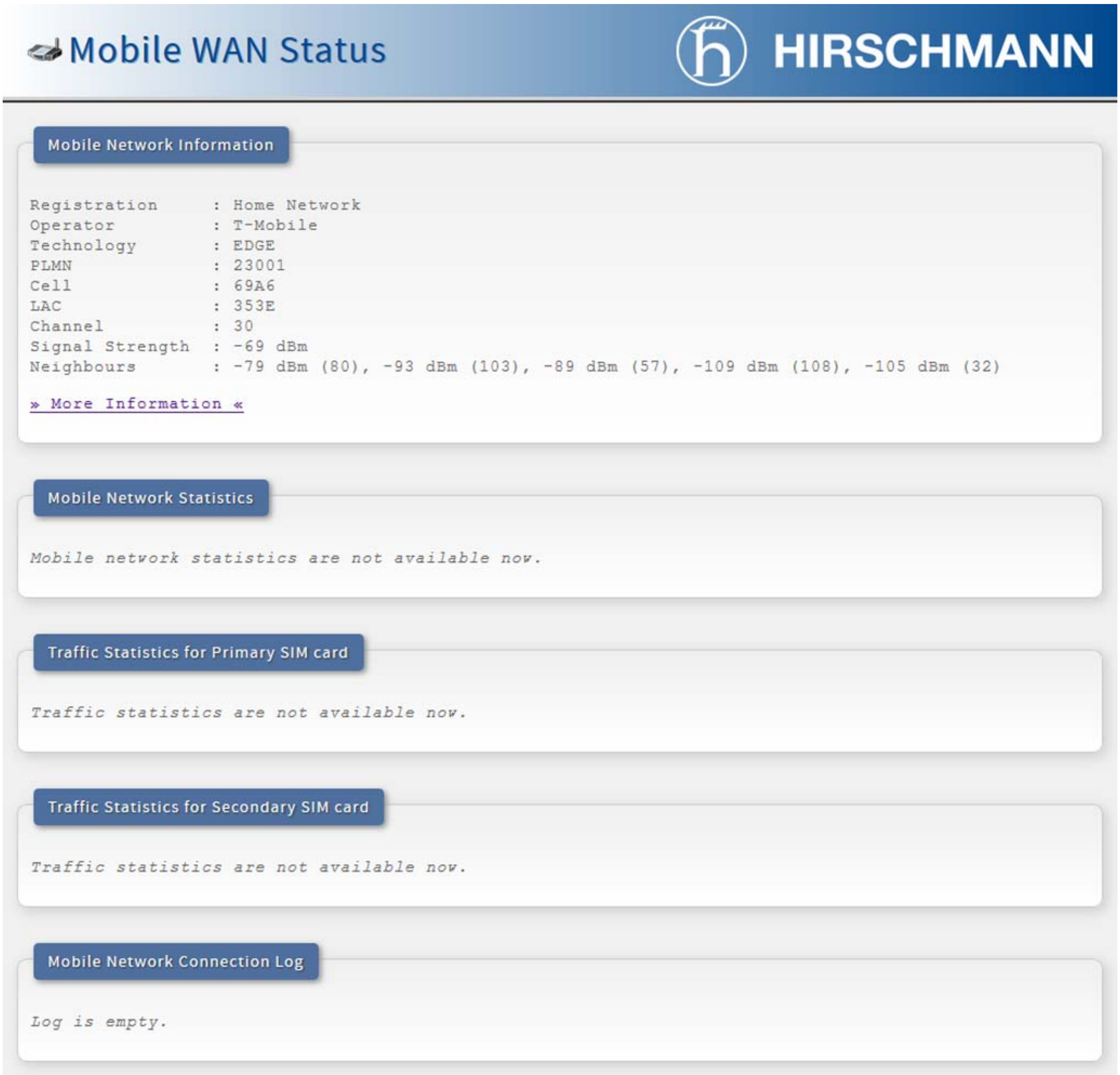
- Availability of the connection to the mobile network is information expressed as a percentage that is calculated using the following ratio: time from when connection to mobile network was established: time that the router is turned on
- After you place your cursor on the maximum or minimum signal strength, the router displays the last time that it reached this signal strength.

In the "Traffic Statics for Primary SIM card" and the "Traffic Statics for Secondary SIM card" frames, the device displays information about the data transferred, and the number of connections for both SIM cards.

Parameter	Description
RX data	Displays the total volume of received data.
TX data	Displays the total volume of sent data.
Connections	Displays the number of connections established to the mobile network.

Table 9: Traffic Statistics

The last frame of the dialog, the "Mobile Network Connection Log", displays information about the mobile network connection and detected connection problems that occurred while establishing the connections.



Mobile Network Information

```
Registration    : Home Network
Operator        : T-Mobile
Technology      : EDGE
PLMN            : 23001
Cell            : 69A6
LAC             : 353E
Channel         : 30
Signal Strength : -69 dBm
Neighbours      : -79 dBm (80), -93 dBm (103), -89 dBm (57), -109 dBm (108), -105 dBm (32)
```

» More Information «

Mobile Network Statistics

Mobile network statistics are not available now.

Traffic Statistics for Primary SIM card

Traffic statistics are not available now.

Traffic Statistics for Secondary SIM card

Traffic statistics are not available now.

Mobile Network Connection Log

Log is empty.

Figure 3: Mobile WAN Status

■ DHCP

Information about the DHCP server activity is accessible in the "DHCP" dialog. The DHCP server provides automatic configuration of devices connected to the network management router. The DHCP server assigns each device its IP address and netmask, the IP address of the default gateway, and the IP address of the DNS server.

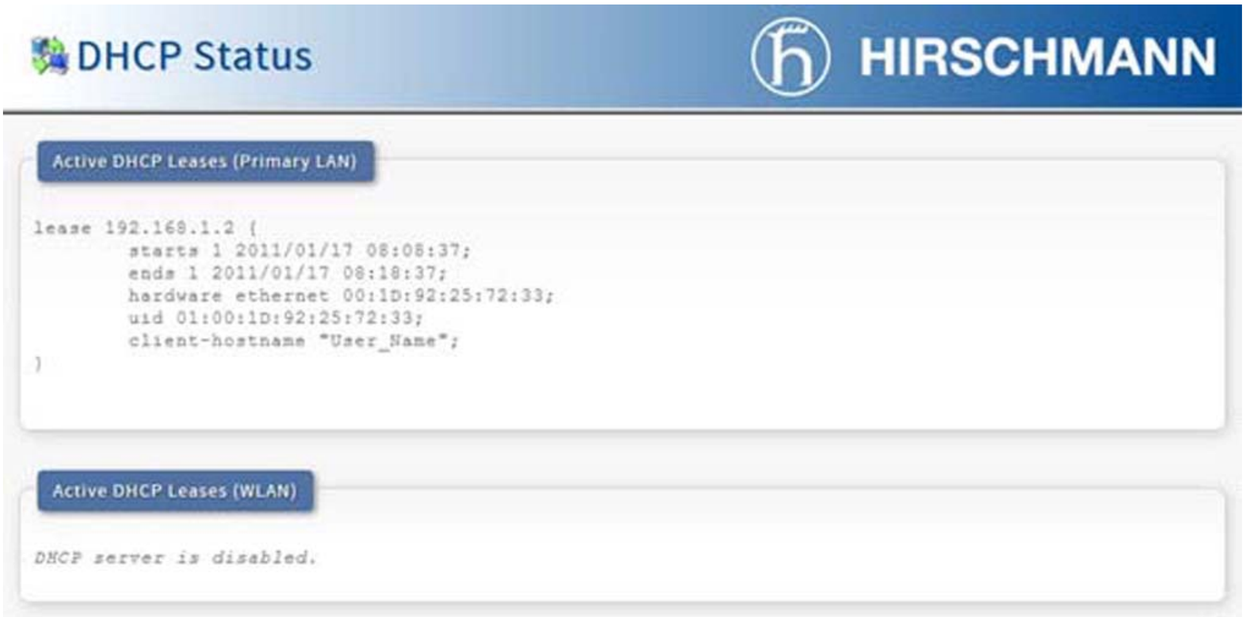
The "DHCP" dialog displays the following information for each configuration:

Parameter	Description
lease	Displays the assigned IP address.
starts	Displays the time that the DHSP server assigned the IP address.
ends	Displays the time that the DHSP server terminates the validity of the IP address.
hardware ethernet	Displays the unique hardware MAC address.
uid	Displays the unique ID.
client-hostname	Displays the host computer name.

Table 10: DHCP Status Description

After resetting the network cards, the DHCP status can display 2 records for 1 IP address.

Note: The records in the "DHCP" dialog are divided into 2 separate parts the "Active DHCP Leases (Primary LAN)", and the "Active DHCP Leases (WLAN)".



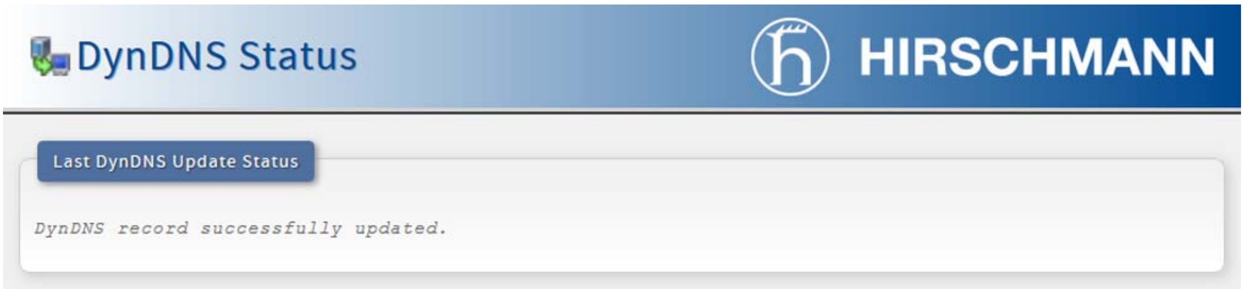
```
lease 192.168.1.2 {
        starts 1 2011/01/17 08:08:37;
        ends 1 2011/01/17 08:18:37;
        hardware ethernet 00:1D:92:25:72:33;
        uid 01:00:1D:92:25:72:33;
        client-hostname "User_Name";
}
```

DHCP server is disabled.

Figure 4: DHCP Status

DynDNS status

The router supports DynamicDNS using a DNS server on www.dyndns.org. If you configure the Dynamic DNS function, then the router displays the status in the "DynDNS" dialog. Refer to www.dyndns.org for more information on how to configure a Dynamic DNS client.



DynDNS record successfully updated.

Figure 5: DynDNS Status

When the router detects a DynDNS record update, the dialog displays one or more of the following messages:

- `DynDNS client is disabled.`
- `Invalid user name or password.`
- `Specified hostname does not exist.`
- `Invalid hostname format.`
- `Hostname exists, but not under the specified user name.`
- `No update performed yet.`
- `DynDNS record is already up to date.`
- `DynDNS record successfully updated.`
- `DNS error encountered.`
- `DynDNS server failure.`

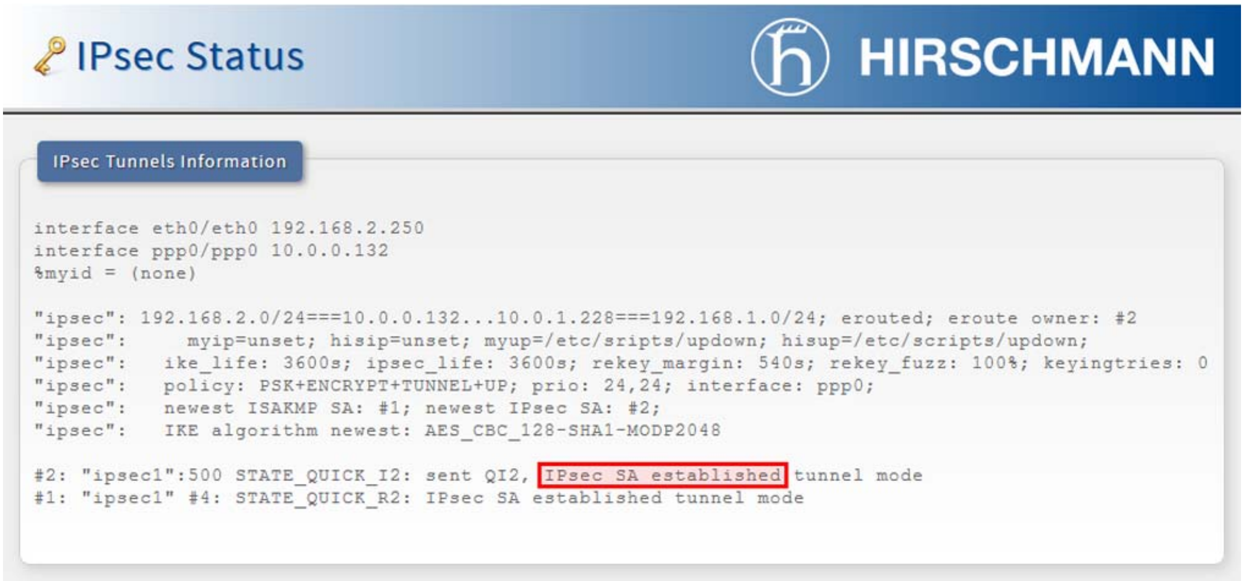
Note: In order for the DynDNS function to perform correctly, purchase a public IP address from your provider or have your provider assign you a public IP address.

1.2.4 Virtual Private Network

IPsec

In the "IPsec" dialog, you can view information about the current IPsec tunnel status. Up to 4 IPsec tunnels can be created. If no IPsec tunnels are configured, the dialog displays the IPsec as disabled.

If the IPsec tunnel is successfully established, the dialog displays `IPsec SA established`. Other information located in this dialog pertains only to the internal characteristics of the IPsec tunnel.



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

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

#2: "ipsec1":500 STATE_QUICK_I2: sent QI2, IPsec SA established tunnel mode
#1: "ipsec1" #4: STATE_QUICK_R2: IPsec SA established tunnel mode
```

Figure 6: IPsec Status

1.2.5 System Log

The router displays connection problems in the "System Log" dialog. The dialog displays detailed reports from individual applications. The dialog displays recent information. You can view older log entries by saving the system log to a file and opening it with a text editor. Use the "Save Log" button to save the system log to a connected computer. The router saves a text file with the `log` extension. You use the second button, "Save Report" for creating a detailed report. The report is a text file with a `txt` format. The report contains the following information which the technical support uses to assist you:

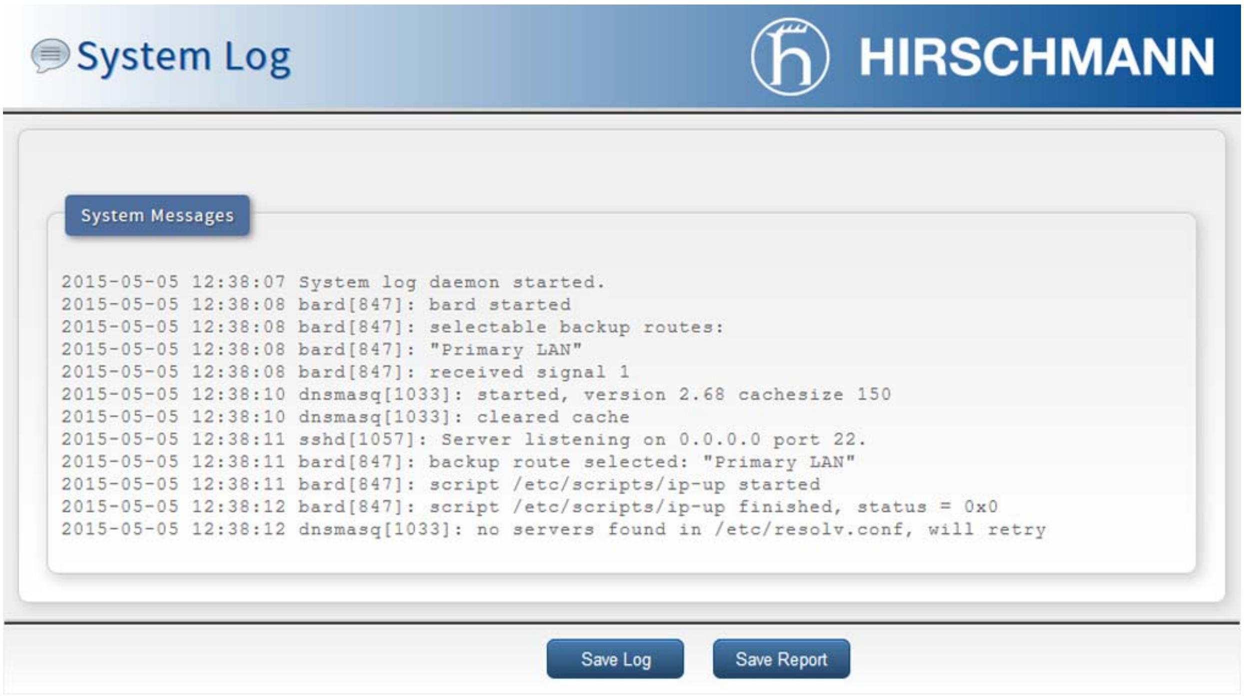
- statistical data
- routing and process tables
- the system log
- the configuration file

The default length of the system log is 1000 lines. After reaching 1000 lines a new file is created for storing the system log. After completion of 1000 lines in the second file, the first file is overwritten with a new file.

The router creates the output of the system log using the Syslogd application. You can start the Syslogd application with 2 options. The options modify the behavior of the system log as follows:

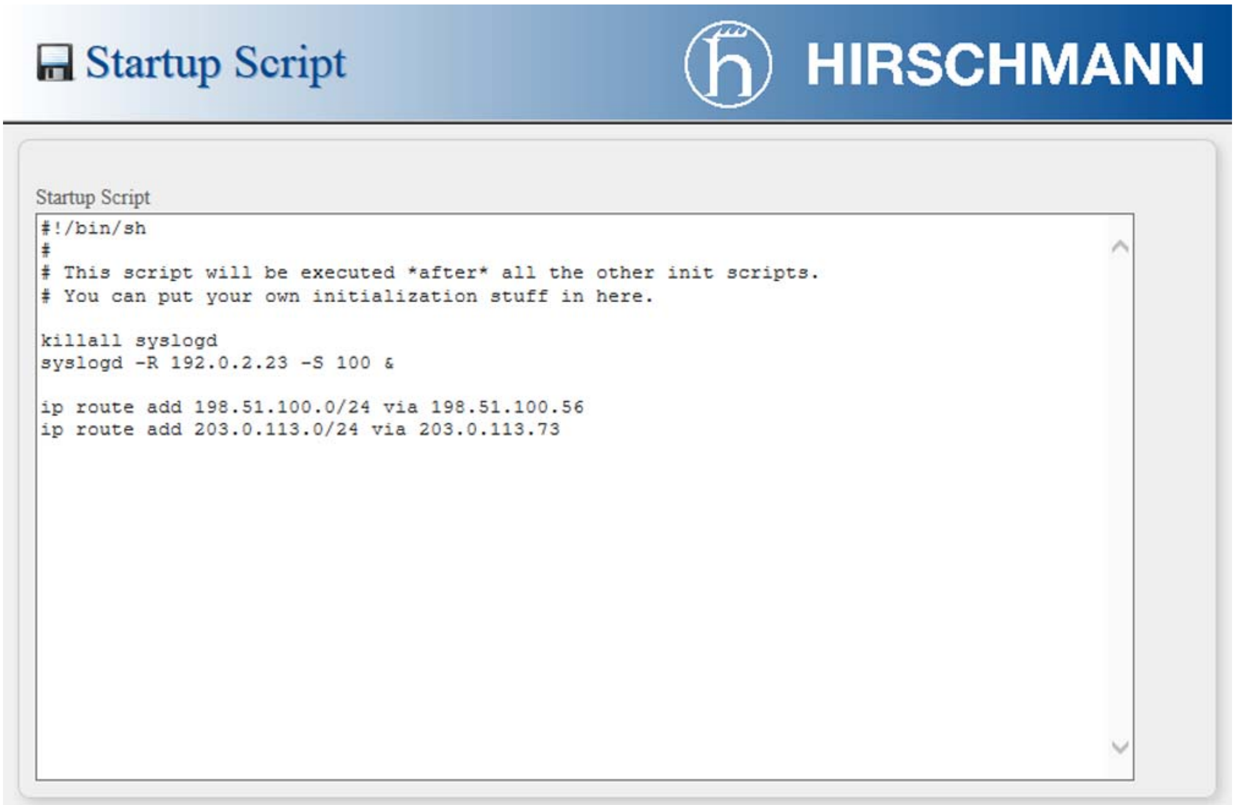
- Option "-S" followed by a decimal number sets the maximal number of lines in one log file.
- Option "-R" followed by a hostname or an IP address enables logging to a remote syslog daemon.

If the remote syslog deamon uses a Linux OS, then enable remote logging using the "syslogd -R &" command. If remote syslog deamon uses a Windows OS, install a syslog server application for example, Syslog Watcher. To start the Syslogd application with these options, modify the "/etc/init.d/syslog" script using SSH.



```
2015-05-05 12:38:07 System log daemon started.
2015-05-05 12:38:08 bard[847]: bard started
2015-05-05 12:38:08 bard[847]: selectable backup routes:
2015-05-05 12:38:08 bard[847]: "Primary LAN"
2015-05-05 12:38:08 bard[847]: received signal 1
2015-05-05 12:38:10 dnsmasq[1033]: started, version 2.68 cachesize 150
2015-05-05 12:38:10 dnsmasq[1033]: cleared cache
2015-05-05 12:38:11 sshd[1057]: Server listening on 0.0.0.0 port 22.
2015-05-05 12:38:11 bard[847]: backup route selected: "Primary LAN"
2015-05-05 12:38:11 bard[847]: script /etc/scripts/ip-up started
2015-05-05 12:38:12 bard[847]: script /etc/scripts/ip-up finished, status = 0x0
2015-05-05 12:38:12 dnsmasq[1033]: no servers found in /etc/resolv.conf, will retry
```

Figure 7: System Log



```
#!/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 192.0.2.23 -S 100 &

ip route add 198.51.100.0/24 via 198.51.100.56
ip route add 203.0.113.0/24 via 203.0.113.73
```

Figure 8: Example program syslogd start with the parameter -R

1.3 Configuration

1.3.1 Basic Settings

Backup Configuration

You can save the configuration of the router using the "Backup Configuration" function. If you click on "Backup Configuration" in the "Configuration> Basic Settings" section of the main menu, then the router allows you to select a directory in which the router saves the configuration file.

Restore Configuration

You can restore a configuration of the router using the "Restore Configuration" dialog. To navigate to the directory containing the configuration file (.cfg) you wish to load on the router, use the "Browse" button.

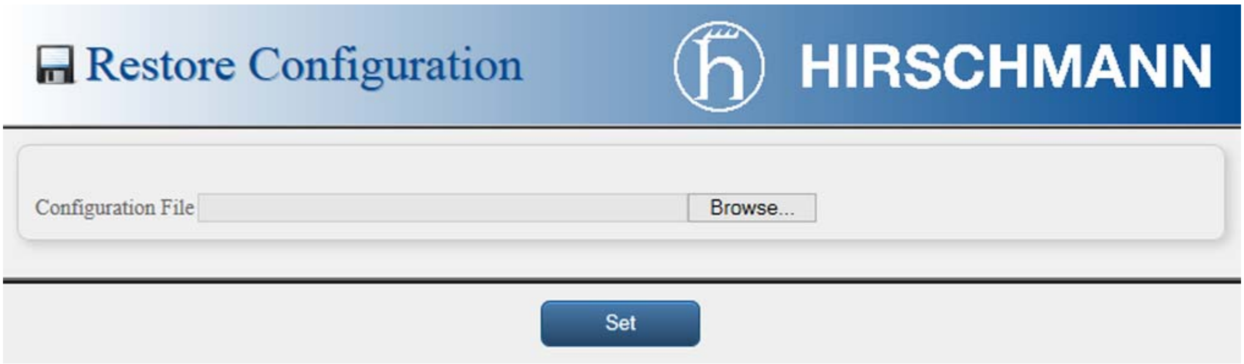


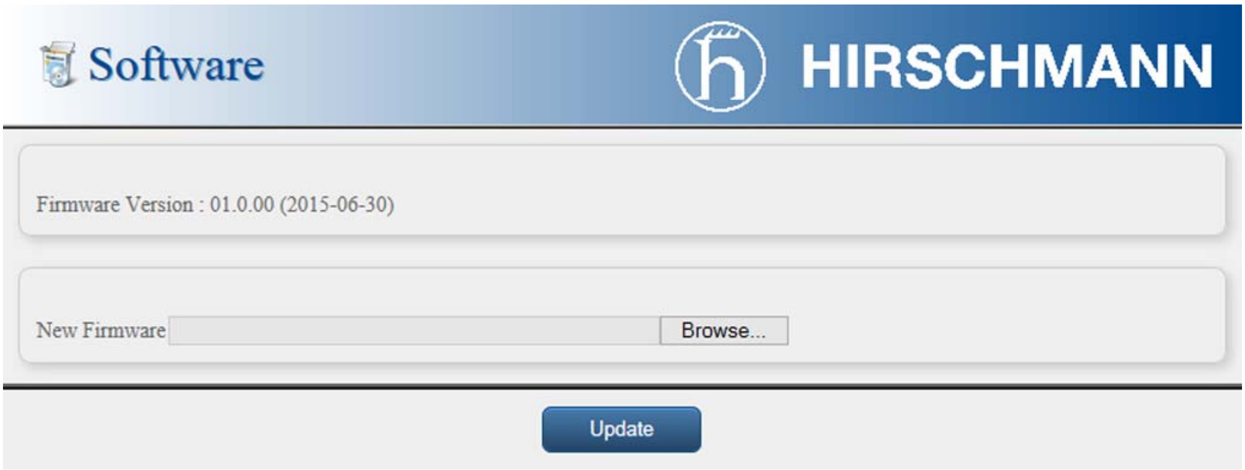
Figure 9: Restore Configuration

Software

You can find information about the firmware version in the "Software" dialog.

□ To navigate to the directory containing the firmware file you wish to upload to the router, use the "Browse" button.

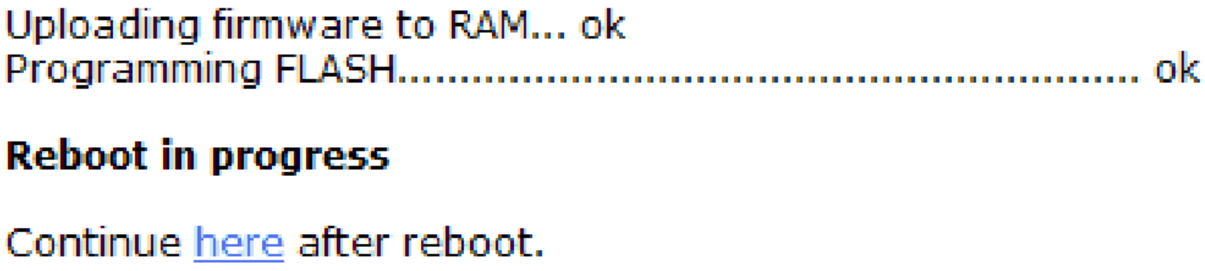
□ To upload the firmware to the router, click the "Update" button.



Firmware Version : 01.0.00 (2015-06-30)

Figure 10: Software

Information about programming the FLASH memory is displayed after a successful firmware update (see figure below):



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

Reboot in progress

Continue here after reboot.
```

Note: When you upload firmware intended for a different device you can cause damage of the router. Maintain a constant supply of power during a firmware update.

1.3.2 Network

LAN

To configuring the Ethernet ports for the Local Area Network (LAN), open the "LAN" dialog. To configure the first ETH interface (ETH0), use the "Primary LAN" parameters. To configure the second ETH interface (ETH1), use the "Secondary LAN" parameters.

Parameter	Description
DHCP Client	Enables/disables the DHCP client function. Possible values: ▶ `disabled` The router does not allow automatic allocation IP address from a DHCP server in LAN network. ▶ `enabled` The router allows automatic allocation IP address from a DHCP server in LAN network.
IP address	Specifies a fixed set of IP addresses for the network interfaces ETH.
Subnet Mask	Specifies a Subnet Mask for the IP address.
Bridged	Activates/deactivates the bridging function on the router. Possible values: ▶ `no` (default setting) The bridging function is inactive. ▶ `yes` The bridging function is active.
Media type	Specifies the type of duplex and speed used in the network. Possible values: ▶ `Auto-negation` (default setting) The router selects the speed of communication of network options. ▶ `100 Mbps Full Duplex` The router communicates at 100Mbps, in the full duplex mode. ▶ `100 Mbps Half Duplex` The router communicates at 100Mbps, in the half duplex mode. ▶ `10 Mbps Full Duplex` The router communicates at 10Mbps, in the full duplex mode. ▶ `10 Mbps Half Duplex` The router communicates at 10Mbps, in the half duplex mode.

Table 11: Configuration of Network Interface

Parameter	Description
Default Gateway	Specifies the IP address of default gateway. When entering the IP address of default gateway, every packet for which the destination IP address was not found in the routing table, is sent to this IP address.
DNS server	Specifies the IP address of the DNS server. When the IP address is not found the Routing Table, the router forwards an IP address requests to the DNS server.

Table 11: Configuration of Network Interface

You use the "Default Gateway" and "DNS Server" parameters only if the "DHCP Client" parameter is set to the value `disabled`, and if the "Backup routes" function selects the `Primary` or `Secondary` LAN as a default route. For a description of the selection algorithm. See “Backup Routes” on page 54.

The router supports only 1 active bridge. Use only the "DHCP Client", "IP address" and "Subnet Mask" parameters to configure the bridge. When you add both interfaces, eth0 and eth1, to the bridge. The Primary LAN has the higher priority. You can add or delete other interfaces to or from the existing bridge.

The DHCP server assigns the IP address, the gateway IP address and the IP address of the DNS server to the connected clients. If you enter the values manually in the dialog, then the router retains the values.

The DHCP server supports static and dynamic assignment of IP addresses. Using the dynamic function, the DHCP server assigns the client IP addresses from a defined address range. Using the static function, the DHCP server assigns the IP addresses that correspond to the MAC addresses of the connected clients.

Parameter	Description
Enable dynamic DHCP leases	Activates/deactivates the dynamic DHCP server function on the router. Possible values: ▶ `marked` The dynamic DHCP server function is active. ▶ `unmarked` (default setting) The dynamic DHCP server function is inactive.
IP Pool Start	Specifies the start of IP addresses allocated to the DHCP clients.
IP Pool End	Specifies the end of IP addresses allocated to the DHCP clients.
Lease time	Specifies the amount of time in seconds that the client can use the IP address.

Table 12: Configuration of Dynamic DHCP Server

Parameter	Description
Enable static DHCP leases	Activates/deactivates the static DHCP server function on the router. Possible values: ▶ `marked` The static DHCP server function is active. ▶ `unmarked` (default setting) The static DHCP server function is inactive.
MAC Address	Specifies the MAC address of a DHCP client.
IP Address	Specifies the assigned IP address.

Table 13: Configuration of Static DHCP Server

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

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

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

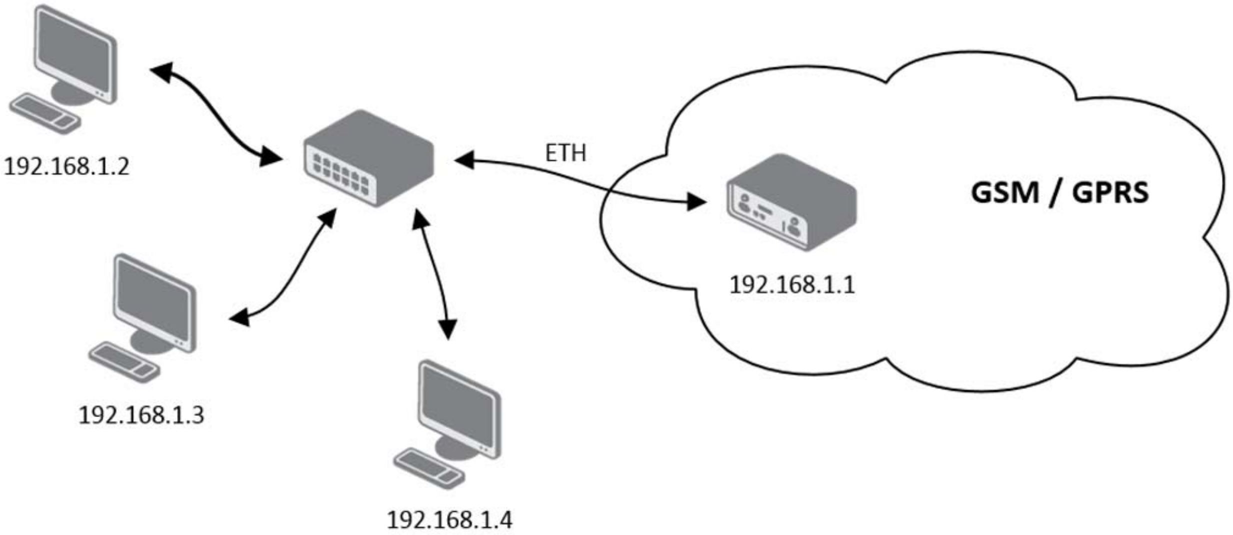
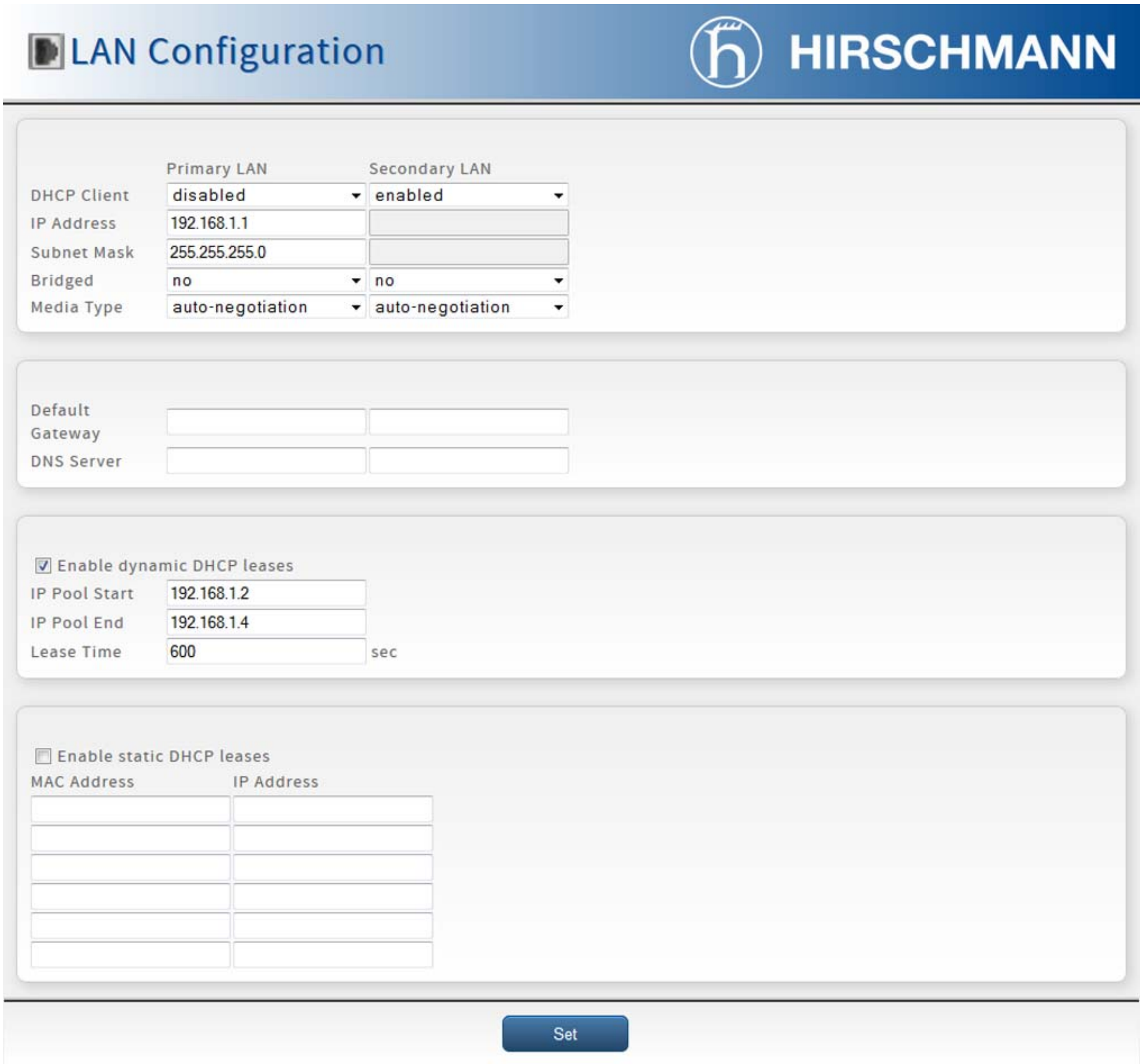


Figure 11: Topology of LAN Configuration Example 1



LAN Configuration

	Primary LAN	Secondary LAN
DHCP Client	disabled	enabled
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 12: LAN Configuration Example 1

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

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

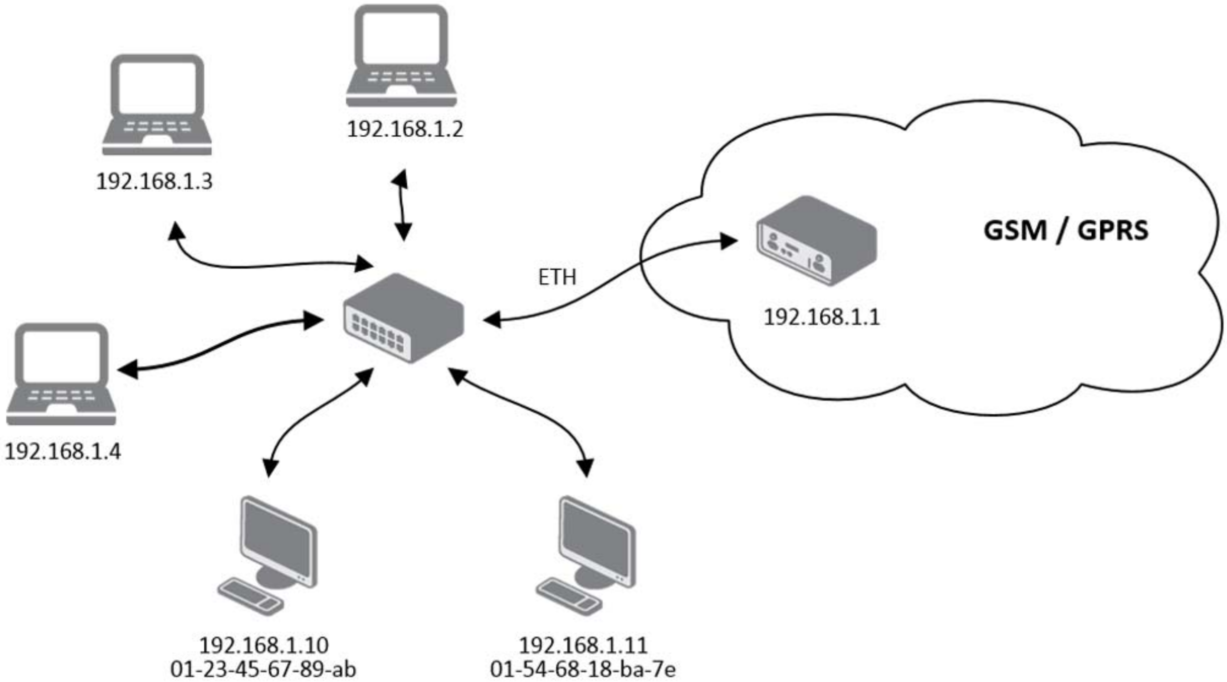
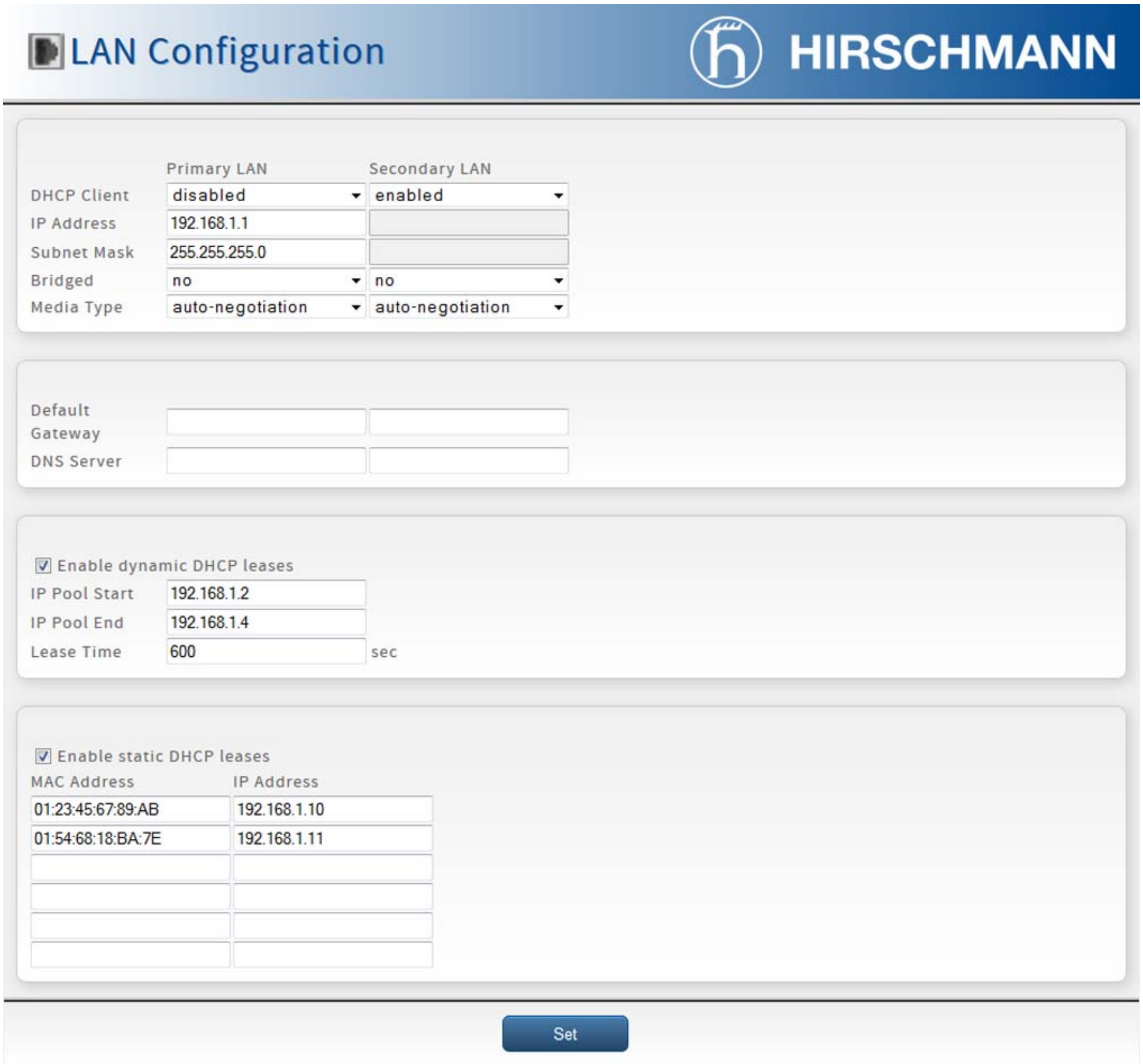


Figure 13: Topology of LAN Configuration Example 2



	Primary LAN	Secondary LAN
DHCP Client	disabled	enabled
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 14: LAN Configuration Example 2

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

- ▶ The Default gateway IP address is `192.168.1.20`.
- ▶ The DNS server IP address is `192.168.1.20`.

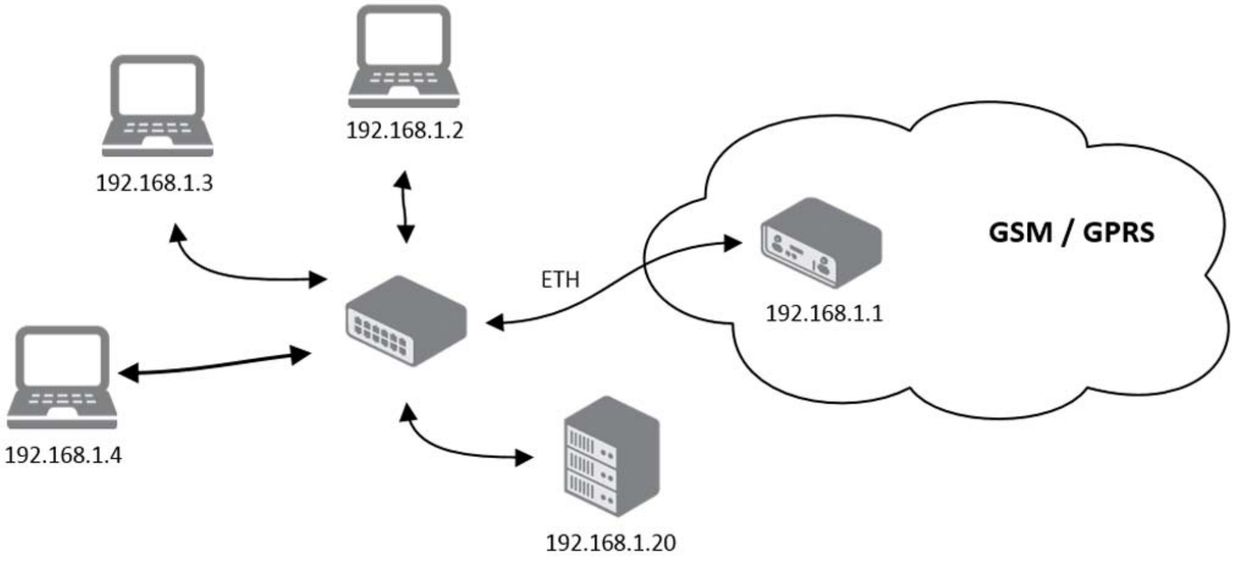
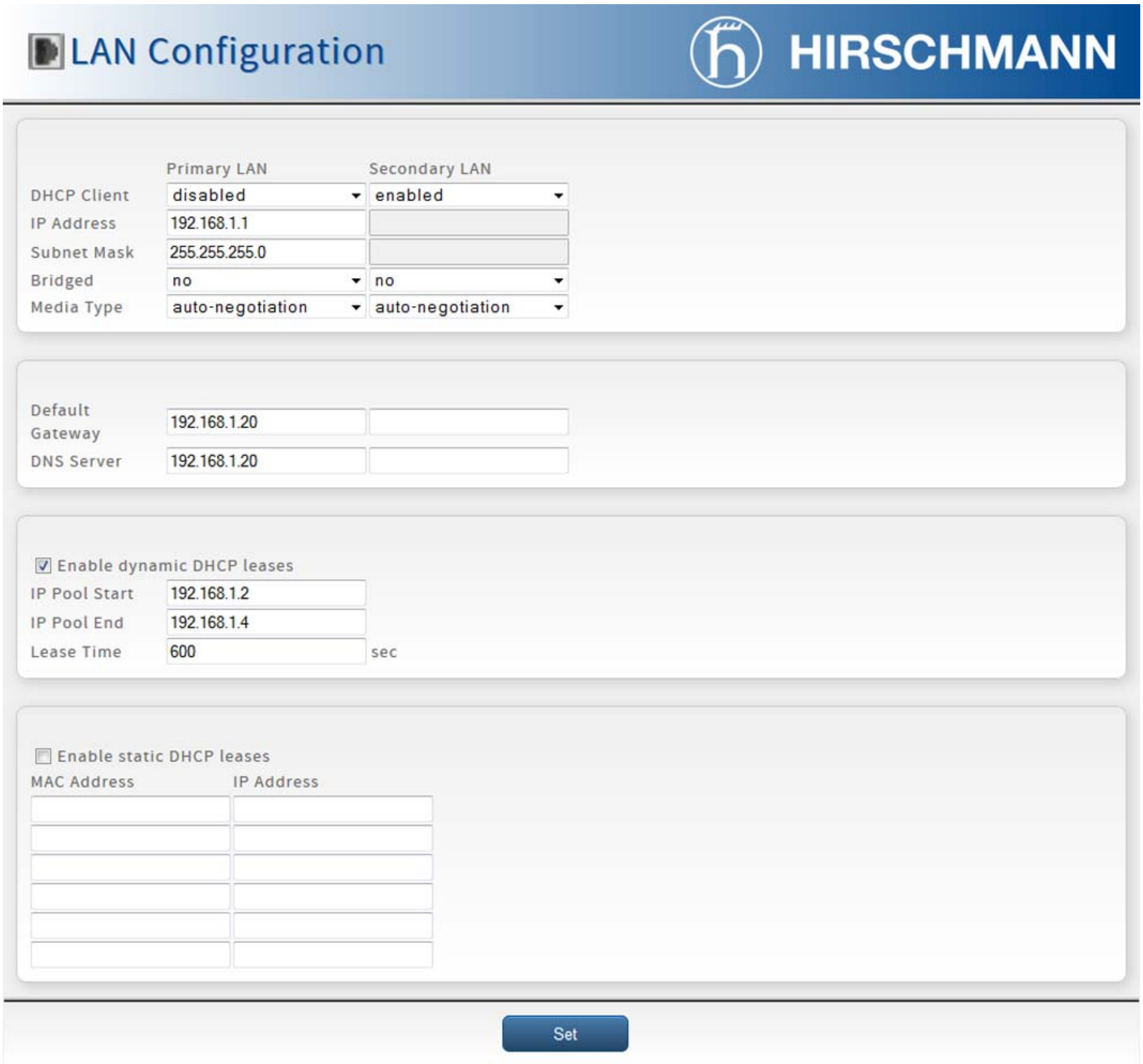


Figure 15: Topology of LAN Configuration Example 3



	Primary LAN	Secondary LAN
DHCP Client	disabled	enabled
IP Address	192.168.1.1	
Subnet Mask	255.255.255.0	
Bridged	no	no
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 16: LAN Configuration Example 3

Mobile WAN

To configuring an interface for a mobile network connection, open the "Mobile LAN" dialog in the "Configuration" section.

■ Connection to Mobile Network

If you mark the "Create connection to mobile network" checkbox, then the router automatically attempts to establish a connection after booting up. You can specify the following parameters for each SIM card separately, or to toggle between the SIM cards, specify 2 different APNs.

Parameter	Description
APN	Specifies the network identifier (Access Point Name).
Username	Specifies the user name for logging into the GSM network.
Password	Specifies the Password for logging into the GSM network.
Authentication	Specifies the authentication protocol in the GSM network. Possible values: ▶ `PAP or CHAP` The router selects the authentication method. ▶ `PAP` The router uses the PAP authentication method. ▶ `CHAP` The router uses the CHAP authentication method.
IP Address	Specifies the IP address of SIM card. You manually enter the IP address, only when mobile network carrier assigned the IP address.
Phone Number	Specifies the telephone number the router dials for a GPRS or CSD connection. The router uses a default telephone number `*99***1 #`.
Operator	Specifies the carrier code. You can specify the parameter as the PLNM preferred carrier code.
Network type	Specifies the type of protocol used in the mobile network. Possible values: ▶ `automatic selection` The router automatically selects the transmission method according to the availability of transmission technology. ▶ `GPRS/EDGE` ▶ `UMTS/HSPA` ▶ `LTE`
PIN	Specifies the PIN used to unlock the SIM card. Use a PIN parameter only if the network requires a SIM card router. The SIM card is blocked after several failed attempts to enter the PIN.
MRU	Specifies the Maximum Receive Unit which is the maximum size of a packet that the router can receive in a given environment. The default value is `1500 B`. Other settings can cause the router to incorrectly transmit data.
MTU	Specifies the Maximum Transmission Unit which is the maximum size of a packet that the router can transmit in a given environment. The default value is `1500 B`. Other settings can cause the router to incorrectly transmit data.

Table 14: Mobile WAN Connection Configuration

The following list contains tips for working with the Mobile WAN dialog:

- If the MTU size is set incorrectly, then the router does not exceed the data transfer. When you set the MTU value low, more frequent fragmentation of data occurs. More frequent fragmentation means a higher overhead and also the possibility of packet damage during defragmentation. On the contrary, a higher MTU value can cause the network to drop the packet.
- If the IP address field is left blank, when the router establishes a connection, then the mobile network carrier automatically assigns an IP address. If you assign an IP address, then the router accesses the network quicker.
- If the APN field is left blank, then the router automatically selects the APN using the IMSI code of the SIM card. If the PLMN (operator number format) is not in the APN list, then the router uses the default APN "internet". The mobile network carrier defines the APN.
- If you enter the word `blank` in the APN field, then the router interprets the APN as blank.

Note: If only 1 SIM card is installed, then the router toggles between the APNs. A router with 2 SIM cards toggles between both SIM cards.

Note: Enter a correct PIN. Use the same PIN for SIM cards with 2 APNs. Otherwise, entering the wrong PIN blocks the SIM card.

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

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

■ DNS Address Configuration

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

Check Connection to Mobile Network Configuration

If the "Check Connection" parameter is set to `enabled` or `enabled + bind`, the router checks the mobile network connection. The router automatically sends ping requests to the domain or IP address specified in the "Ping IP Address" field. The router sends ping requests at regular intervals as specified in the "Ping Interval" field. In case of an unsuccessful ping, the router sends a new ping after 10 seconds. If the ping fails 3 times in a row, the router terminates the current connection and attempts to establish a new connection. You can set the network verification separately for each SIM card or for 2 APNs. Use an IP address that you are certain is still functional and you are able to send ICMP pings to for example, the DNS server of mobile network carrier.

When you select the `enabled` option, the router sends the ping requests based on the routing table. The requests can be sent through any available interface. If you require the router to send each ping request through the network interface, which was created to connect to the mobile network carrier, set the "Check Connection" parameter to `enabled + bind`. The `disabled` option deactivates checking the connection to mobile network.

Parameter	Description
Ping IP Address	Specifies the destination IP address or domain name for ping queries.
Ping Interval	Specifies the time intervals between the outgoing pings.

Table 15: Check Connection to Mobile Network Configuration

If you mark the "Enable Traffic Monitoring" checkbox, then the router stops sending ping request to the "Ping IP Address" and it monitors the data stream on the connection to mobile network. If this connection is without data longer than the "Ping Interval", then the router sends a ping request to the "Ping IP Address".

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

Data Limit Configuration

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

Table 16: Data Limit Configuration

Toggle between SIM Card Configurations

At the bottom of this configuration form you can specify the rules for toggling between the 2 APNs, a single SIM card, or between the 2 SIM cards if you have inserted 2 SIM cards. The router can automatically toggle between the network setups in the following cases:

- the active connection to mobile network is lost
- the data limit is exceeded
- the binary input on the front panel is activated

Parameter	Description
Default SIM card	Specifies the default APN or SIM card. The router attempts to establish a connection to mobile network using the default. If you specify this parameter as none, then the router boots up in the off line mode and it is necessary to establish a connection to the mobile network using an SMS message.
Backup SIM card	Specifies the backup APN or SIM card.

Table 17: Default and Backup SIM Configuration

If you select `none` from the "Backup SIM card" drop down list, then the following parameters cause the router to go into the off line mode:

- "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"

Parameter	Description
Switch to other SIM card when connection fails	Activates/deactivates toggling to the secondary SIM card or secondary APN of the SIM card. Possible values: ▶ `marked` Toggling to the secondary is active. ▶ `unmarked` (default setting) Toggling to the secondary is inactive. Failure to connect to mobile network can occur in two ways. ▶ When you start the router, and it registers 3 failed attempts to establish a connection to mobile network. ▶ If you enable the "Check Connection" function and the router indicates a loss of the mobile network connection
Switch to backup SIM card when roaming is detected and switch to default SIM card when home network is detected	Activates/deactivates toggling to the secondary SIM card or secondary APN of the SIM card when the router detects that roaming is active. Possible values: ▶ `marked` Toggling to the secondary is active. ▶ `unmarked` (default setting) Toggling to the secondary is inactive. If the router detects the home network, this parameter allows the router to change back to the default SIM card. **Note:** For proper operation, enable roaming on your SIM card.
Switch to backup SIM card when data limit is exceeded and switch to default SIM card when data limit isn't exceeded	Activates/deactivates toggling to the secondary SIM card or secondary APN of the SIM card when the data limit of default APN is exceeded. Possible values: ▶ `marked` Toggling to the secondary is active. ▶ `unmarked` (default setting) Toggling to the secondary is inactive. When the data limit is under the allotted limit, the router returns to the default SIM card.
Switch to backup SIM card when binary input is active and switch to default SIM card when binary input isn’t active	Activates/deactivates toggling to the secondary SIM card or secondary APN of the SIM card when the binary input ‘bin0’ is active. Possible values: ▶ `marked` Toggling to the secondary is active. ▶ `unmarked` (default setting) Toggling to the secondary is inactive. The router returns to the default SIM card.
Switch to default SIM card after timeout	Specifies the method in which the router attempts to change back to the default SIM card or the default APN.

Table 18: Toggle between SIM Card Configurations

The following parameters specifies the length of time that the router waits before attempting to change back to the default SIM card or APN.

Parameter	Description
Initial timeout	Specifies the length of time that the router waits before the first attempt to change back to the primary SIM card or APN, the range of this parameter is from 1 to 10000 minutes.
Subsequent Timeout	Specifies the length of time that the router waits after an unsuccessful attempt to change to the default SIM card, the range is from 1 to 10000 min.
Additional constants	Specifies the length of time that the router waits for any further attempts to change back to the primary SIM card or APN. The length time is the sum of the time specified in the "Subsequent Timeout" parameter and the time specified in this parameter, the range is from 1 to 10000 minutes.

Table 19: Timeout Configuration

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

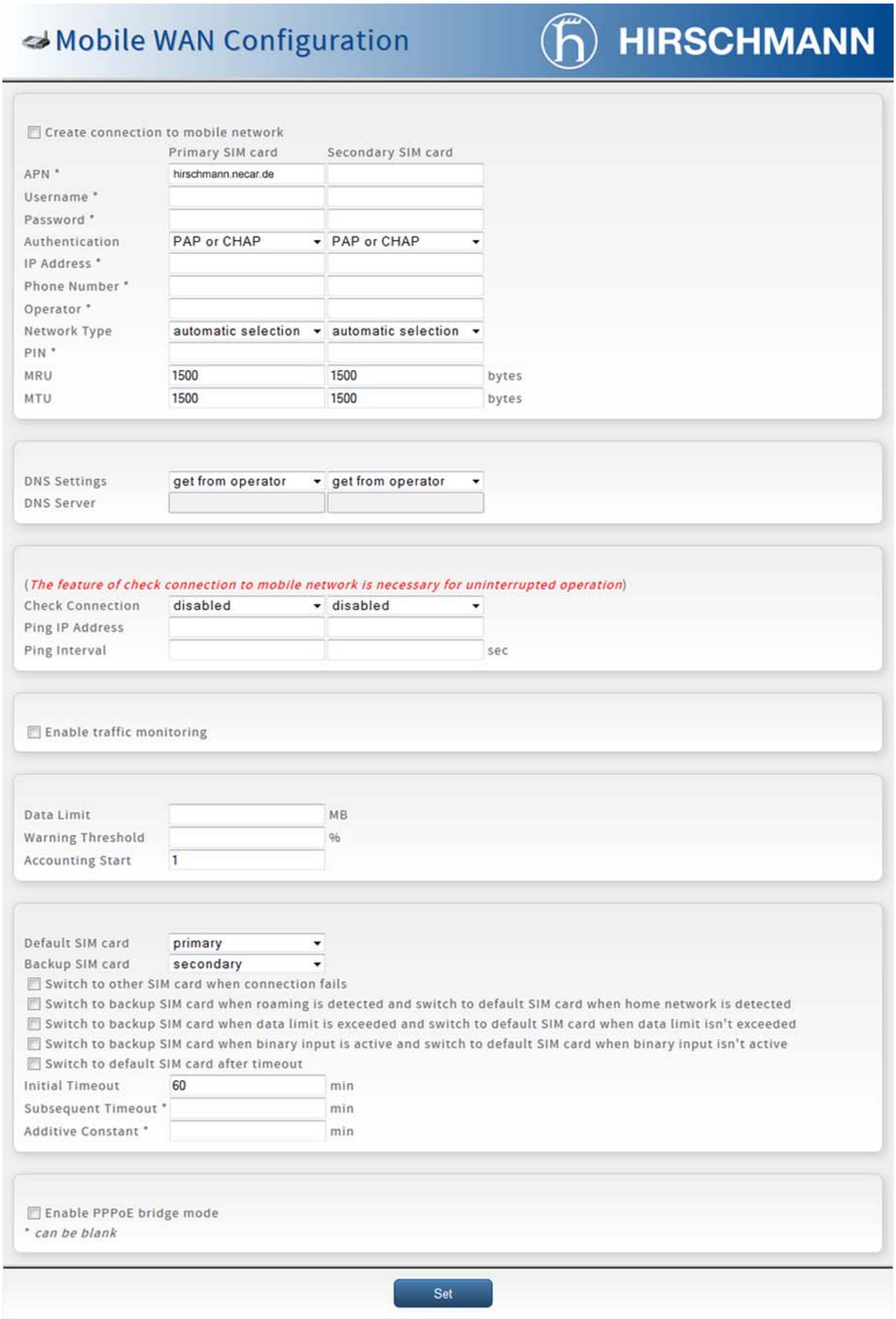
- Initial Timeout - 60 min
- Subsequent Timeout 30 min
- Additional Timeout - 20 min

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

PPPoE Bridge Mode Configuration

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

The changes in the dialog apply after clicking the "Set" button.



Mobile WAN Configuration

□ Create connection to mobile network

	Primary SIM card	Secondary SIM card	
APN *	hirschmann.necar.de		
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

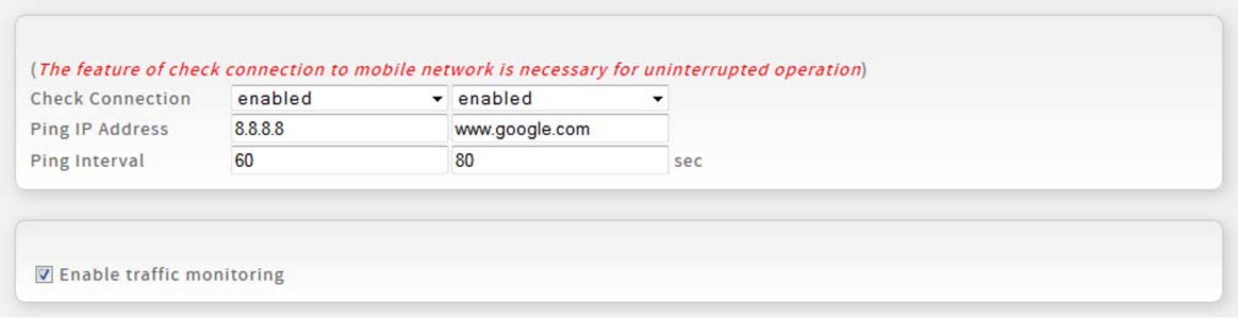
Initial Timeout	60	min
Subsequent Timeout *		min
Additive Constant *		min

□ Enable PPPoE bridge mode

* *can be blank*

Figure 17: Mobile WAN Configuration

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



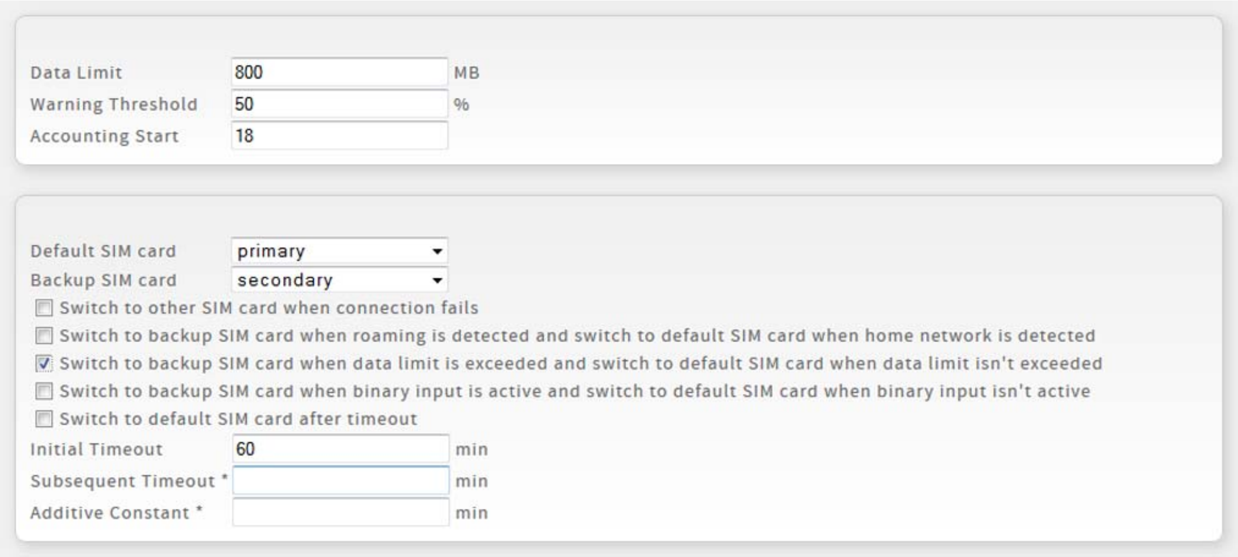
(*The feature of check connection to mobile network is necessary for uninterrupted operation*)

Check Connection	enabled	enabled	
Ping IP Address	8.8.8.8	www.google.com	
Ping Interval	60	80	sec

☑ Enable traffic monitoring

Figure 18: Mobile WAN Configuration Example 1

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



Data Limit	800	MB
Warning Threshold	50	%
Accounting Start	18	

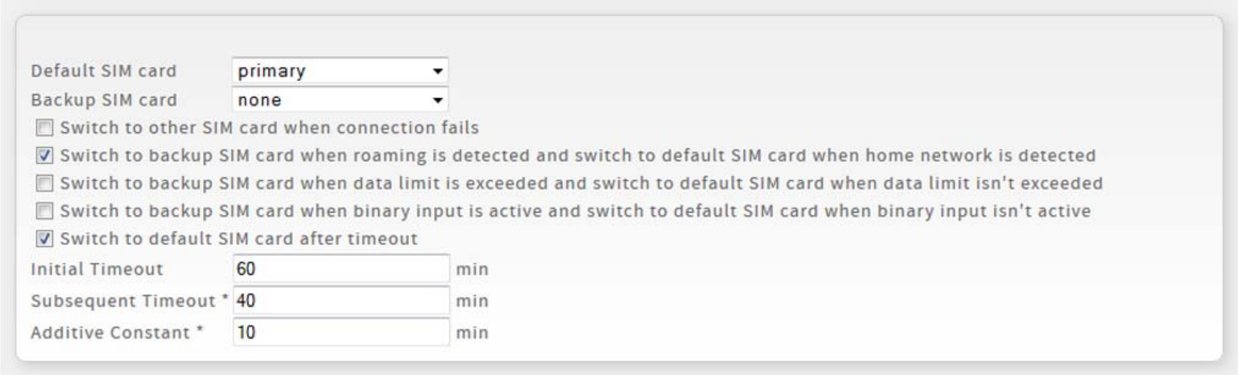
Default SIM card	primary
Backup SIM card	secondary

☐ 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 19: Mobile WAN Configuration Example 2

Example 3: The Primary SIM card changes to the off line mode after the router detects roaming. The first attempt to change back to the default SIM card is executed after `60` minutes, the second attempt is executed after `40` minutes, the third attempt is executed 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 20: Mobile WAN Configuration Example 3

L3-Redundancy

To configure the VRRP protocol, open the "L3-Redundancy" dialog in the "Configuration" section of the main menu. The Virtual Router Redundancy Protocol (VRRP) is a technique that is used to overcome a failure detected in a Gateway router. When the backup Gateway router detects a failure in the main router, the backup router automatically replaces the main router. The backup router uses the same IP and MAC address as the main router. To activate this protocol, mark the "Enable VRRP" check box. The table below describes the meaning of the other parameters:

Parameter	Description
Virtual Server IP Address	Specifies the virtual server IP address. Assign this address to both routers. A connected device sends its data through this virtual address.

Table 20: VRRP Configuration

Parameter	Description
Virtual Server ID	Specifies the virtual router identification number for a virtual router instance. The parameter distinguishes one virtual router on the network from others. Assign the value to both the main and backup routers.
Host Priority	Specifies the priority for the router in an VRRP instance. The master router is the router with the highest priority. You can install more than 2 routers in a VRRP instance. The routers elect a master router based on the "Host Priority" and when the "Host Priority" of the routers are the same, the routers elect the router with the higher IP address as the master. The priority 255 as described in the RFC, is reserved for the IP address owner. The IP address owner is the device that has the same IP address as the Virtual Server. The Host Priority of 255 is only allowed for the IP address owner.

Table 20: VRRP Configuration

To enable automatic test messages for the cellular network, mark the "Check connection" check box in the second part of the dialog.

In some cases, the mobile WAN connection is still active, but the router does not send data over the cellular network. You use the feature to verify that the router can send data over the PPP connection and supplements the normal VRRP message handling. The current active router (main/ backup) sends test messages to the "Ping IP Address" at periodic time intervals defined in "Ping Interval". The router then waits for a reply until the "Ping Timeout" timer expires. If the router does not receive a response to the ping command, then it again sends a ping. The router continues to send pings up to the number of times specified in the "Ping Probes" field. After that time, it assumes the role of the backup router until the PPP connection is restored.

Parameter	Description
Ping IP Address	Specifies the destination IP address for ping queries. Specify the address as an IP address only.
Ping Interval	Specifies the length of time between the consecutive outgoing pings.
Ping Timeout	Specifies the length of time to wait for ping response.
Ping Probes	Specifies the number of failed ping requests after which the route is considered to be impassable.

Table 21: Check Connection

Enter an IP address that you are certain is constantly available and you are able to send ICMP queries for example, the DNS server of the mobile network carrier.

You can use the "Enable traffic monitoring" function to reduce the number of messages that are sent to test the PPP connection. When this function is active, the router monitors the interface for any packets other than a ping. If the router receives a response to the packet before the "Ping Timeout" timer expires, then the router knows that the connection is still active. If the router does not receive a response within the timeout period, it attempts to test the mobile WAN connection using standard ping commands.

Example of the VRRP protocol:

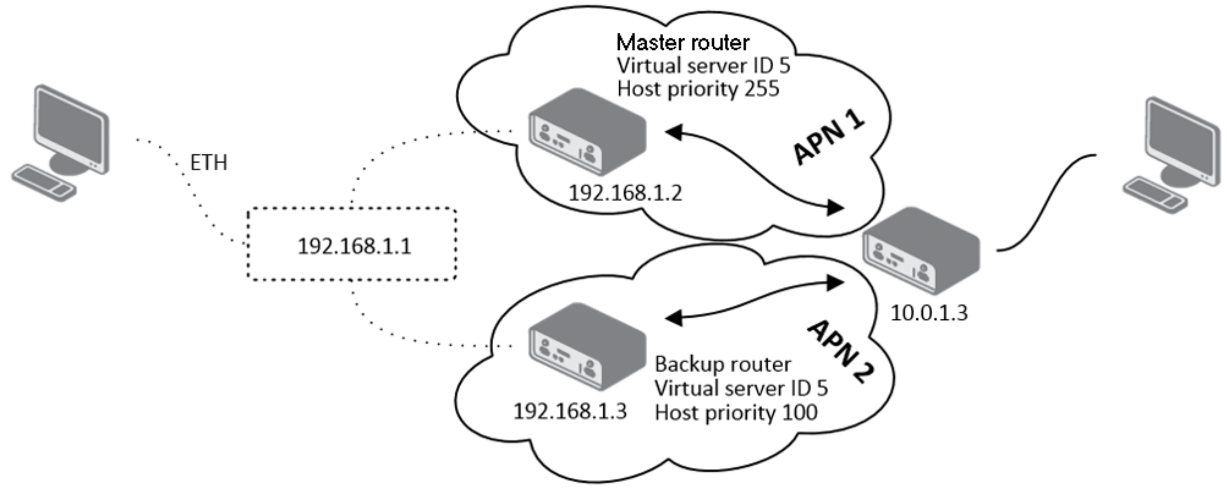
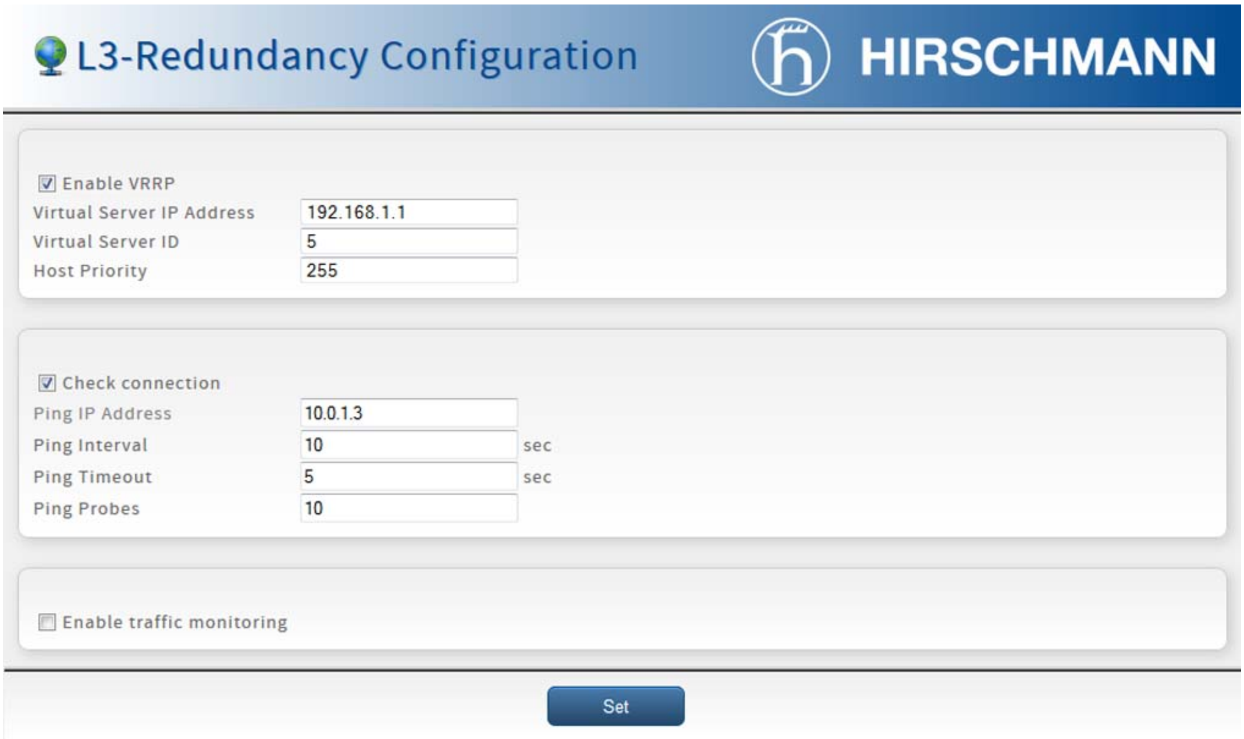


Figure 21: Topology of VRRP Configuration Example



☑ Enable VRRP

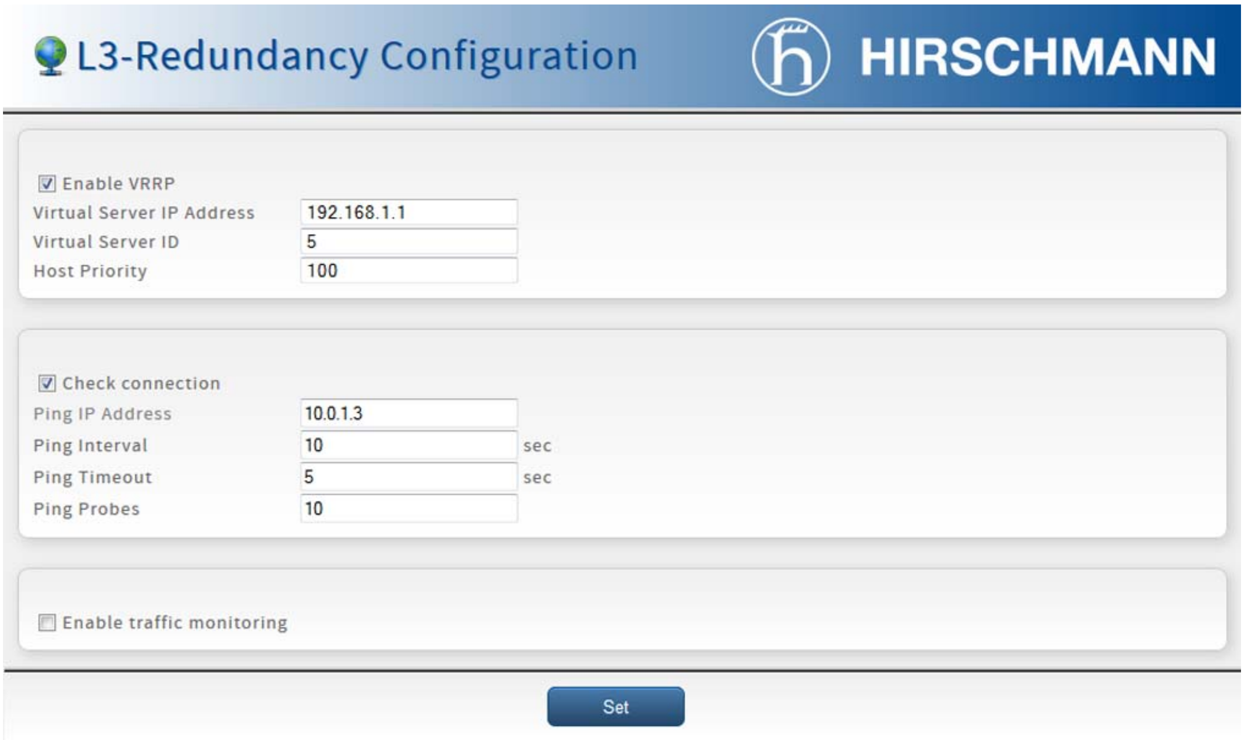
Virtual Server IP Address	192.168.1.1
Virtual Server ID	5
Host Priority	255

☑ Check connection

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

☐ Enable traffic monitoring

Figure 22: VRRP Configuration Example - Master Router



☑ Enable VRRP

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

☑ Check connection

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

☐ Enable traffic monitoring

Figure 23: VRRP Configuration Example - Backup Router

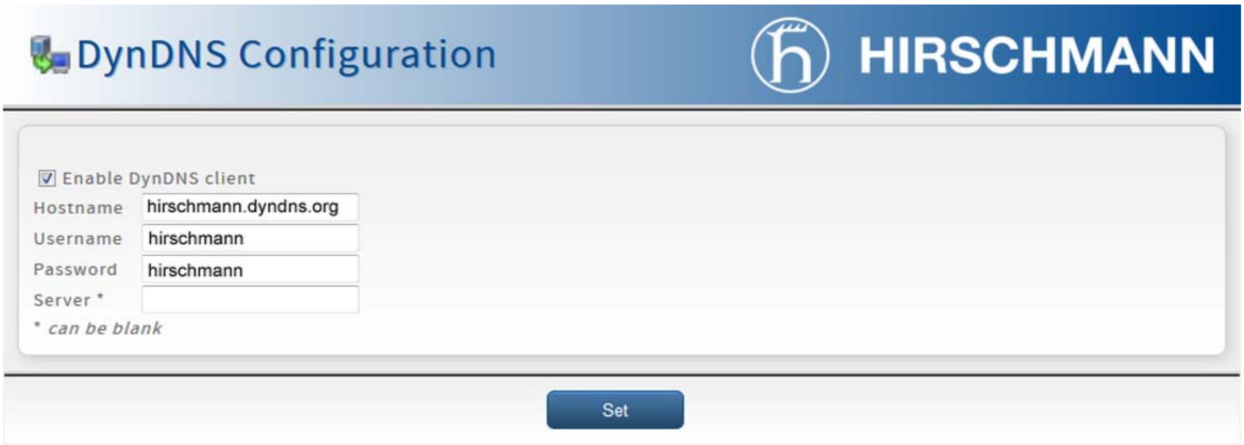
DynDNS

The DynDNS function allows you to access the router remotely using an easy to remember custom hostname. This DynDNS client monitors the IP address of the router and updates the address whenever it changes. In order for DynDNS to function, you require a public IP address, either static or dynamic, and an active Remote Access service account at www.dyndns.org. Registered the custom domain (third-level) and account information specified in the configuration form. To open the "DynDNS Configuration" dialog, click "DynDNS" in the main menu.

Parameter	Description
Hostname	Specifies the third order domain registered on the www.dyndns.org server.
Username	Specifies the username for logging into the DynDNS server.
Password	Specifies the password for logging into the DynDNS server.
Server	Specifies a DynDNS service other than the `www.dyndns.org`. Enter the update server service information in this field. If you leave this field blank, then the router uses the default server, `members.dyndns.org`.

Table 22: DynDNS configuration

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



☑ Enable DynDNS client

Hostname: hirschmann.dyndns.org

Username: hirschmann

Password: hirschmann

Server *:

* can be blank

Figure 24: DynDNS Configuration Example

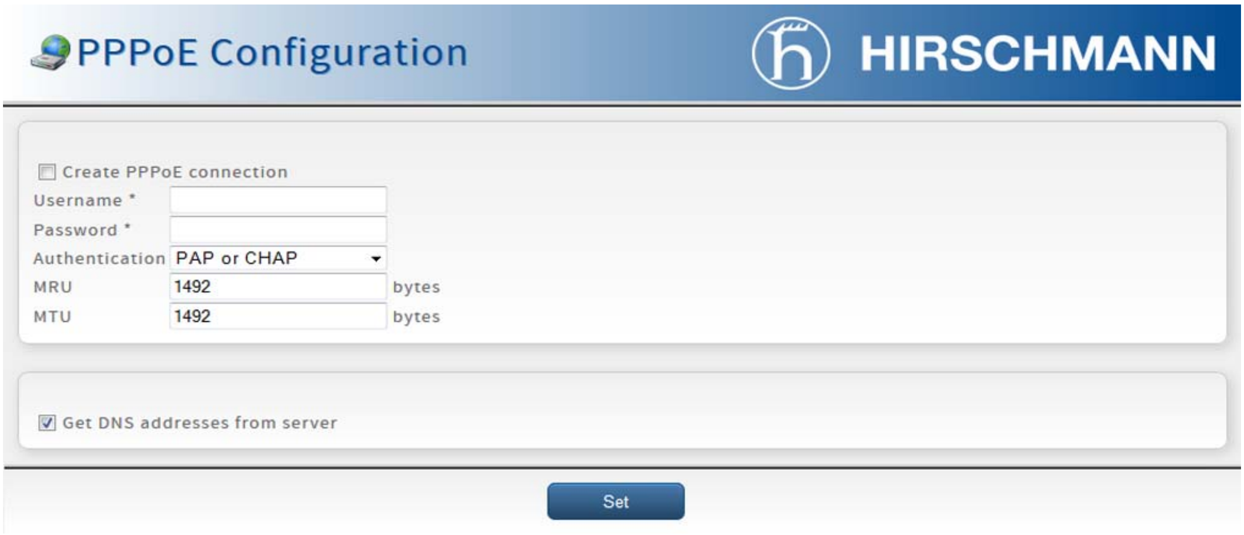
PPPoE

To open the "PPPoE Configuration" dialog, click on "PPPoE" in the "Configuration" section in the main menu. If you mark the "Create PPPoE connection" check box, then the router attempts to establish a PPPoE connection after boot up.

PPPoE (Point-to-Point over Ethernet) is a network protocol which encapsulates PPPoE frames into Ethernet frames. The router uses the PPPoE client to connect to devices supporting a PPPoE bridge or server. The bridge or server is typically an ADSL router. After connecting, the router obtains the IP address of the device to which it is connected. The communications from a device behind the PPPoE server is forwarded to the router.

Parameter	Description
Username	Specifies the username for secure access to PPPoE
Password	Specifies the password for secure access to PPPoE
Authentication	Specifies the authentication protocol in GSM network: Possible values: ▶ `PAP or CHAP` The router selects the authentication method. ▶ `PAP` The router uses the PAP authentication method. ▶ `CHAP` The router uses the CHAP authentication method.
MRU	Specifies the Maximum Receiving Unit. The MRU identifies the maximum packet size, that the router can receive in a given environment. The default value is 1492 bytes. Other settings can cause incorrect data transmission.
MTU	Specifies the Maximum Transmission Unit. The MTU identifies the maximum packet size, that the router can transfer in a given environment. The default value is 1492 bytes. Other settings can cause incorrect data transmission.

Table 23: PPPoE Configuration



PPPoE Configuration

☐ Create PPPoE connection

Username *

Password *

Authentication PAP or CHAP

MRU 1492 bytes

MTU 1492 bytes

☑ Get DNS addresses from server

Figure 25: PPPoE Configuration

Backup Routes

You can use the parameters in the "Backup Routes" dialog to specify a back up route for the primary connection or mobile connection. Back up routes are other connections to the Internet and/or mobile networks. You specify a priority for each back up connection. Changing from the Primary LAN to the Secondary LAN and back is done based on a set of priorities and the state of the connection.

If you mark the "Enable backup routes switching" checkbox, then the router selects the back up route according to the settings specified in this dialog. Namely, according to parameters of each enabled backup route function for example:

- Enable backup routes switching for Mobile WAN
- Enable backup routes switching for PPPoE
- Enable backup routes switching for Primary LAN
- Enable backup routes switching for Secondary LAN
- according to explicitly set priorities
- according to status of connection check, when enabled

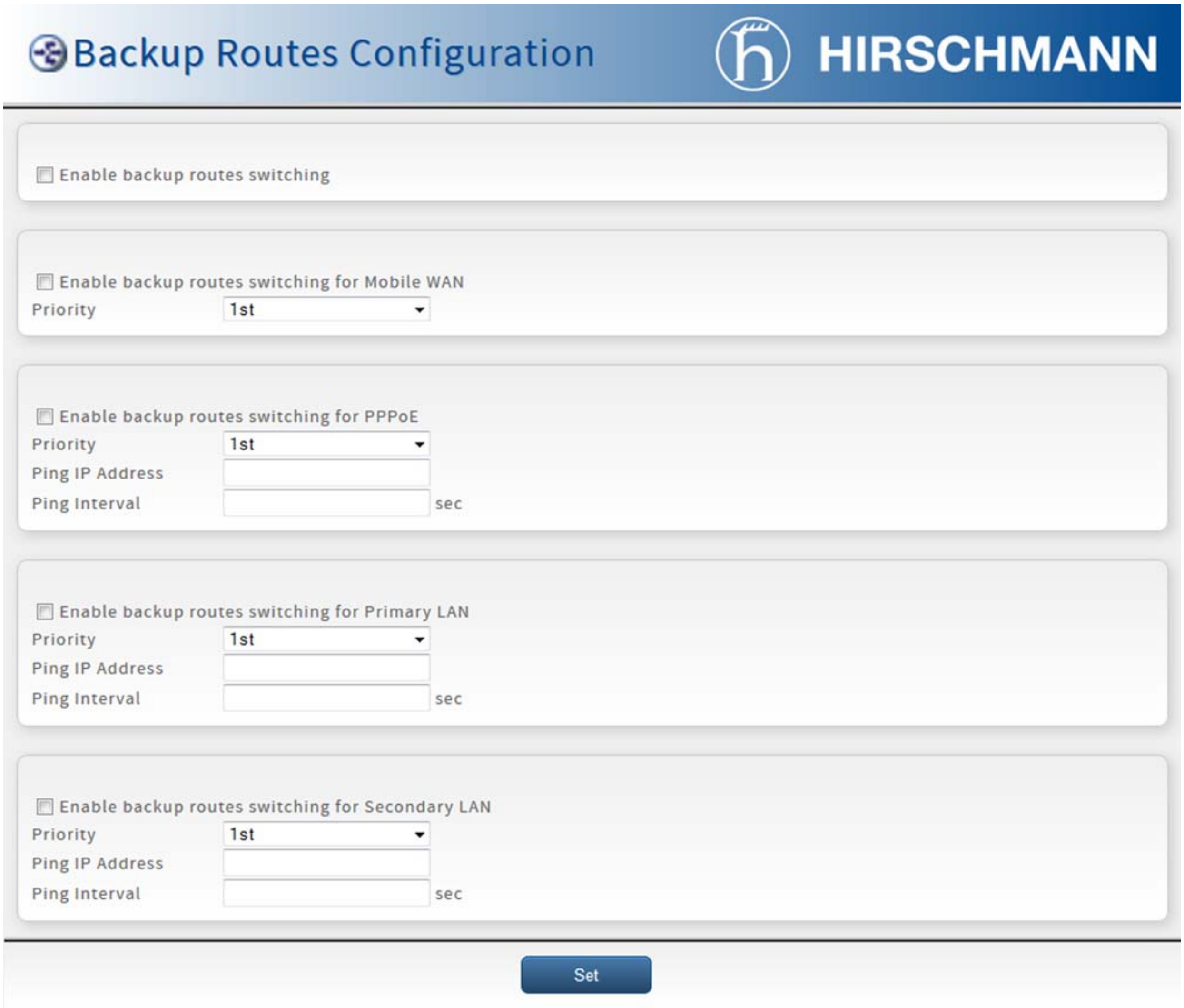
In addition, the router allows you to verify the status of the network interfaces assigned to individual backup routes.

☐ Open the "Status"> "Device Information" dialog.

☐ Click on "More Information" in the "Primary LAN" frame.

☐ Verify that the "Flags" parameter value is `Running`.

Note: If you want to use a mobile WAN connection as a backup route, then mark the "Check Connection" check box, and in the "Mobile WAN Configuration" dialog, select the `enable + bind` option, see “Mobile WAN” on page 39.



Backup Routes Configuration

□ Enable backup routes switching

□ Enable backup routes switching for Mobile WAN
Priority: 1st

□ Enable backup routes switching for PPPoE
Priority: 1st
Ping IP Address:
Ping Interval: sec

□ 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 26: Backup Routes

If you unmark the "Enable backup routes switching" check box, The backup routes system operates in the backward compatibility mode. The router selects the default route based on implicit priorities of the enabled settings for each of the network interfaces, as the case may be enabling services that set these network interfaces. The following list contains the names of backup routes and corresponding network interfaces in order of implicit priorities:

- Mobile WAN (usb0)
- PPPoE (ppp0)

- Secondary LAN (eth1)
- Primary LAN (eth0)

Example: The router selects the Secondary LAN as the default route only if you unmark the "Create connection to mobile network" check box in the "Mobile WAN" dialog. Alternatively, if you unmark the "Create PPPoE connection" check box in the "PPPoE" dialog. To select the Primary LAN, delete the IP address for the Secondary LAN and disabled the DHCP Client for the Secondary LAN.

Parameter	Description
Priority	Specifies the priority for the type of connection.
Ping IP Address	Specifies the destination IP address of ping queries to check the connection. The address cannot be specified as a domain name.
Ping Interval	Specifies the time intervals between consecutive ping queries.

Table 24: Backup Routes

The router uses the changed settings after you click the "Set" button.

1.3.3 Security

Firewall

The first security element which incoming packets pass is a check of the enabled source IP addresses and destination ports. You can specify the IP addresses as an IP address from which you can remotely access the router and the internal network connected behind a router. To enable this function, marking the "Enable filtering of incoming packets" check box located at the top of the "Firewall Configuration" dialog. Accessibility is checked against the IP address table. This means that access is permitted only to addresses specified in the table. It is possible to specify up to eight remote IP addresses for access. You can specify the following parameters:

Parameter	Description
Source	Specifies the IP address from which access to the router is allowed.
Protocol	Specifies the protocol used for remote access: Possible values: ▶ `all` Access for all protocols is active. ▶ `TCP` Access for the TCP protocol is active. ▶ `UDP` Access for the UDP protocol is active. ▶ `ICMP` Access for the ICMP protocol is active.
Target Port	Specifies the port number on which access to the router is allowed.
Action	Specifies the type of action the router performs: Possible values: ▶ allow The router allows the packets to enter the network. ▶ deny The router denies the packets from entering the network

Table 25: Filtering of Incoming Packets

The next section of the configuration form specifies the forwarding policy. If you unmark the "Enabled filtering of forwarded packets" check box, then packets are automatically accepted. If you activate this function, and a packet is addressed to another network interface, then the router sends the packet to the FORWARD chain. When the FORWARD chain accepts the packet and there is a rule for forwarding it, the router sends the packet. If a forwarding rule is unavailable, then the router drops the packet.

The dialog also contains a table for specifying the filter rules. It is possible to create a rule to allow data with the selected protocol by specifying only the protocol, or to create stricter rules by specifying values for source IP addresses, destination IP addresses, and ports.

Parameter	Description
Source	Specifies the IP address from which access to the router is allowed.
Destination	Specifies the IP address of destination device.

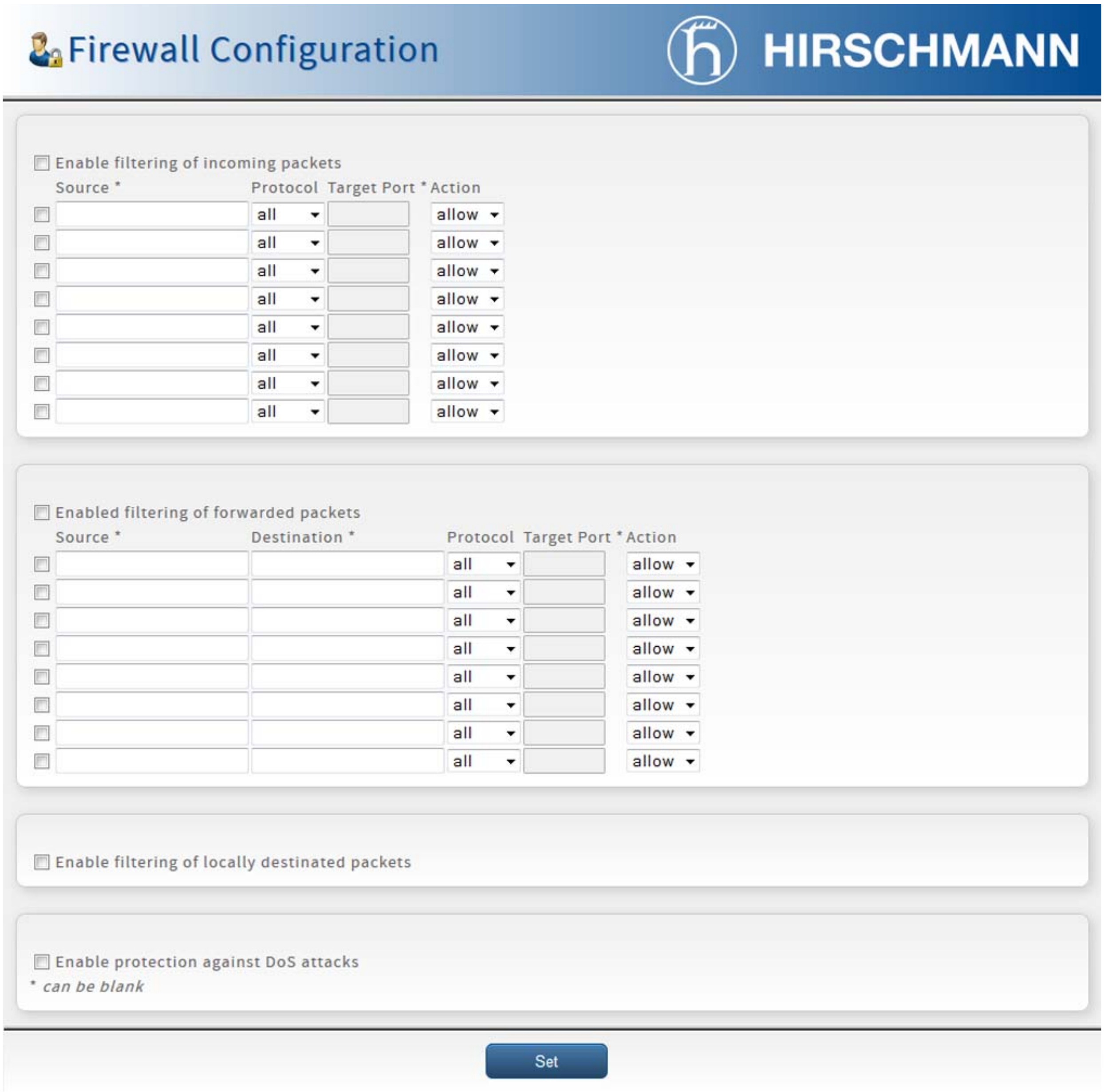
Table 26: Forward Filtering

Parameter	Description
Protocol	Specifies the protocol used for remote access: Possible values: ▶ `all` Access for all protocols is active. ▶ `TCP` Access for the TCP protocol is active. ▶ `UDP` Access for the UDP protocol is active. ▶ `ICMP` Access for the ICMP protocol is active.
Target Port	Specifies the port number on which access to the router is allowed.
Action	Specifies the type of action the router performs: Possible values: ▶ allow The router allows the packets to enter the network. ▶ deny The router denies the packets from entering the network

Table 26: Forward Filtering

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

As a protection against DoS attacks, the "Enable protection against DoS attacks" limits the number of allowed connections per second to 5. The DoS attack floods the target system with meaningless requirements.



Firewall Configuration

☐ Enable filtering of incoming packets

	Source *	Protocol	Target Port *	Action
☐		all		allow
☐		all		allow
☐		all		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*

Figure 27: Firewall Configuration

■ Example of the firewall configuration:

The router allows the following access:

- ▶ from IP address 171.92.5.45 using any protocol
- ▶ from IP address 10.0.2.123 using the TCP protocol on port 1000
- ▶ from IP address 142.2.26.54 using the ICMP protocol

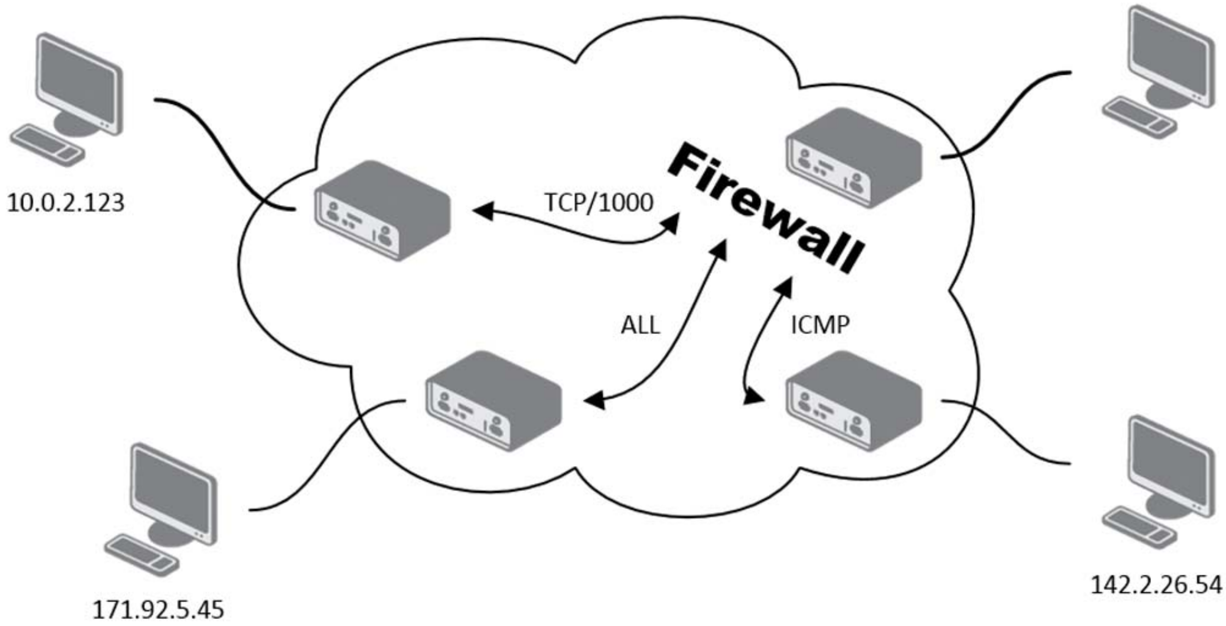
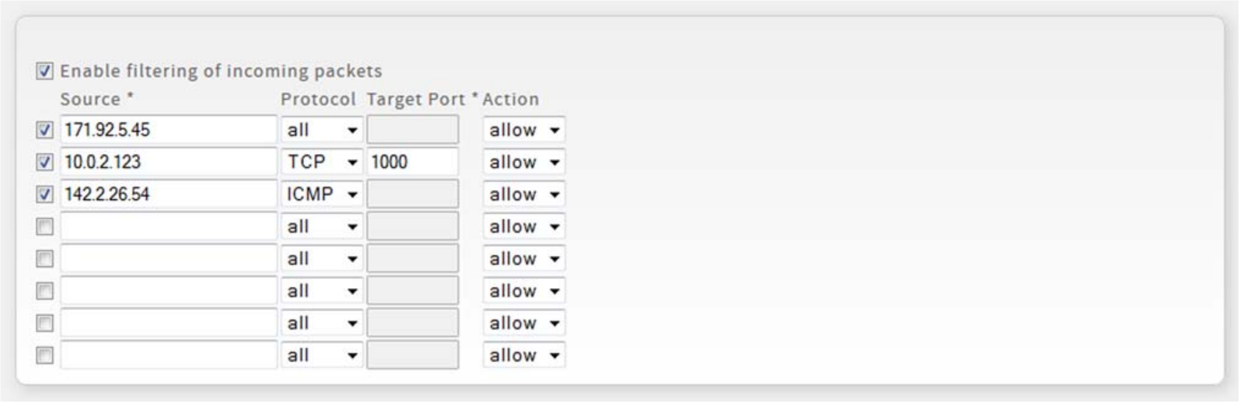


Figure 28: Topology for the Firewall Configuration Example



☑ 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 29: Firewall Configuration Example

■ NAT

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

Parameter	Description
Public Port	Specifies the public port
Private Port	Specifies the private port
Type	Specifies the protocol type
Server IP address	Specifies the IP address where the router forwards incoming data.

Table 27: NAT configuration

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

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

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

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

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

Table 28: Configuration of send all incoming packets

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

Note: Activate only the HTTPS function or HTTPS and HTTP functions together. The "Enable remote HTTP access on port" function only activates a redirect from HTTP to HTTPS protocol. The router does not allow an unsecured HTTP protocol to access the GUI dialogs. To access the GUI dialogs, mark the "Enable remote HTTPS access on port" check box.

Parameter	Description
Enable remote HTTP access on port	Activates/deactivates a redirect from HTTP to HTTPS. The default setting is disabled.
Enable remote HTTPS access on port	Activates/deactivates access to the router using HTTPS. If you enter the field and the port number, then the router allows you to configure the parameters router over web interface. The default setting is disabled.
Enable remote SSH access on port	Activates/deactivates access to the router using SSH - Secure Shell The default setting is disabled.
Enable remote SNMP access on port	Activates/deactivates access to the SNMP agent. The default setting is disabled.
Masquerade outgoing packets	Activates/deactivates the network address translation (PAT) function.

Table 29: Remote Access Configuration

Example1: NAT configuration with 1 connection to the router:

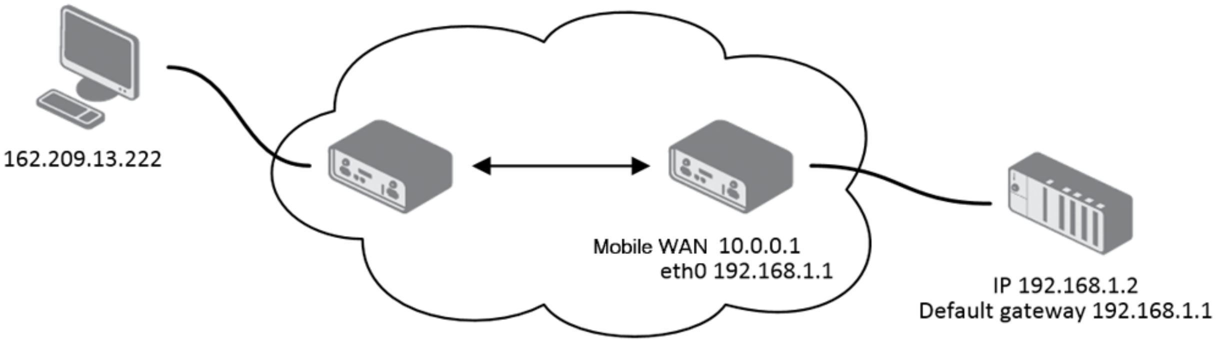
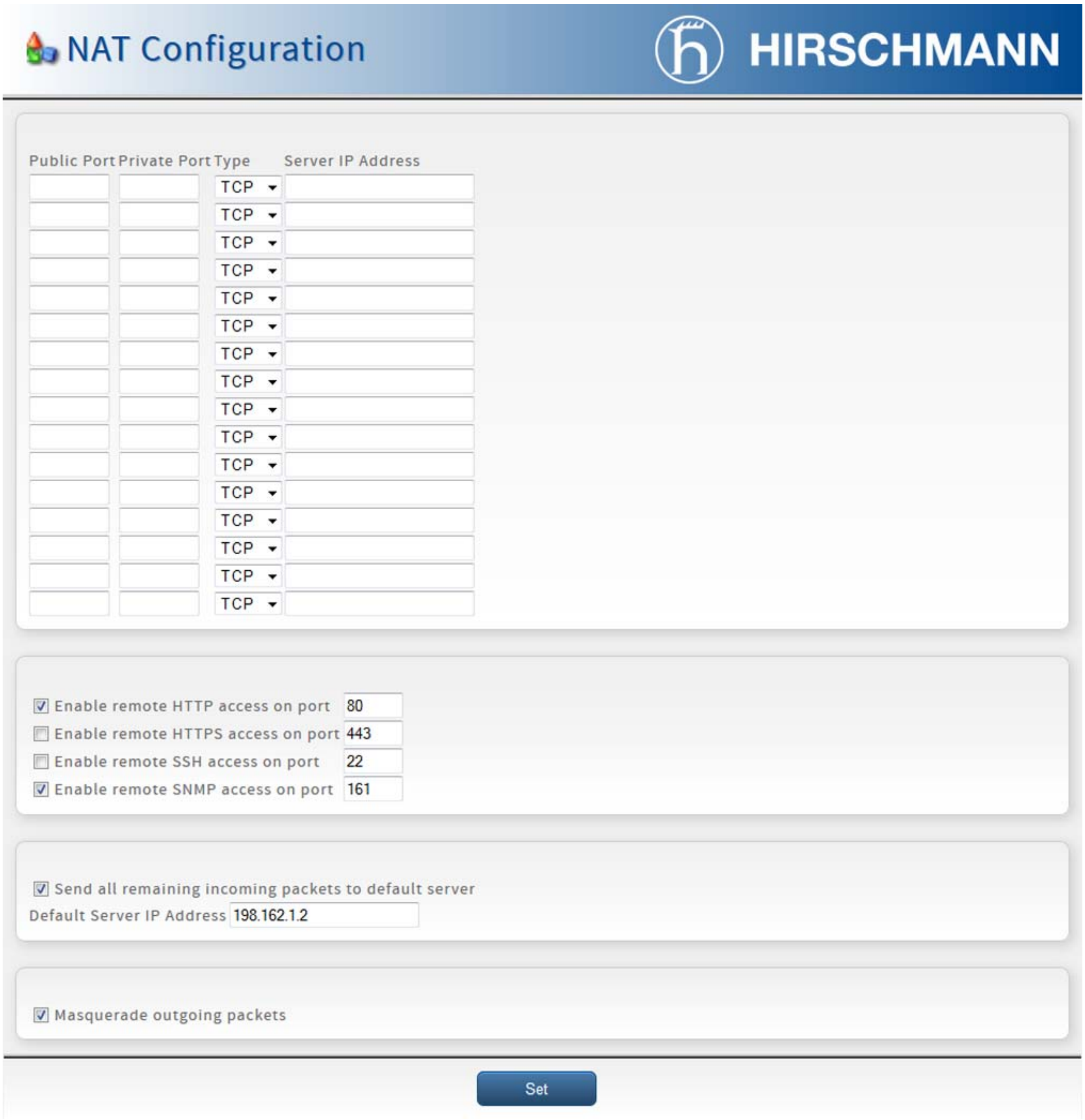


Figure 30: Topology of NAT configuration Example 1



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 HTTPS access on port 443

☐ Enable remote SSH access on port 22

☑ Enable remote SNMP access on port 161

☑ Send all remaining incoming packets to default server

Default Server IP Address 198.162.1.2

☑ Masquerade outgoing packets

Figure 31: NAT Configuration Example 1

It is important to mark the "Send all remaining incoming packets to default server" check box for this configuration. The IP address in this example is the address of the device behind the router. The default gateway of the devices in the subnetwork connected to router is the same IP address as displayed in the "Default Server IP Address" field. The connected device replies if a PING is sent to the IP address of the SIM card.

Example2: Configuration with more equipment connected:

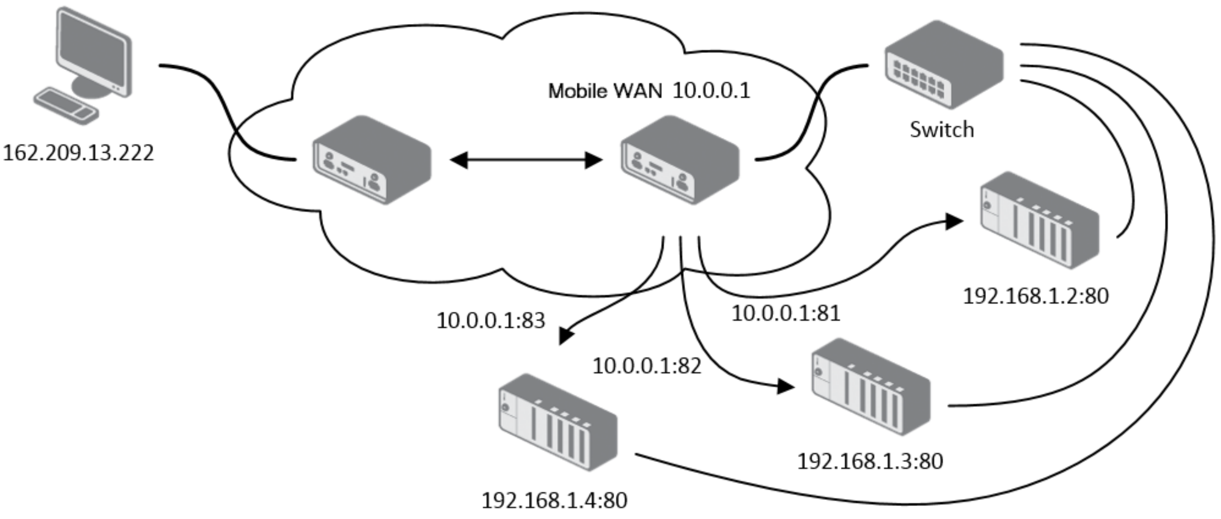
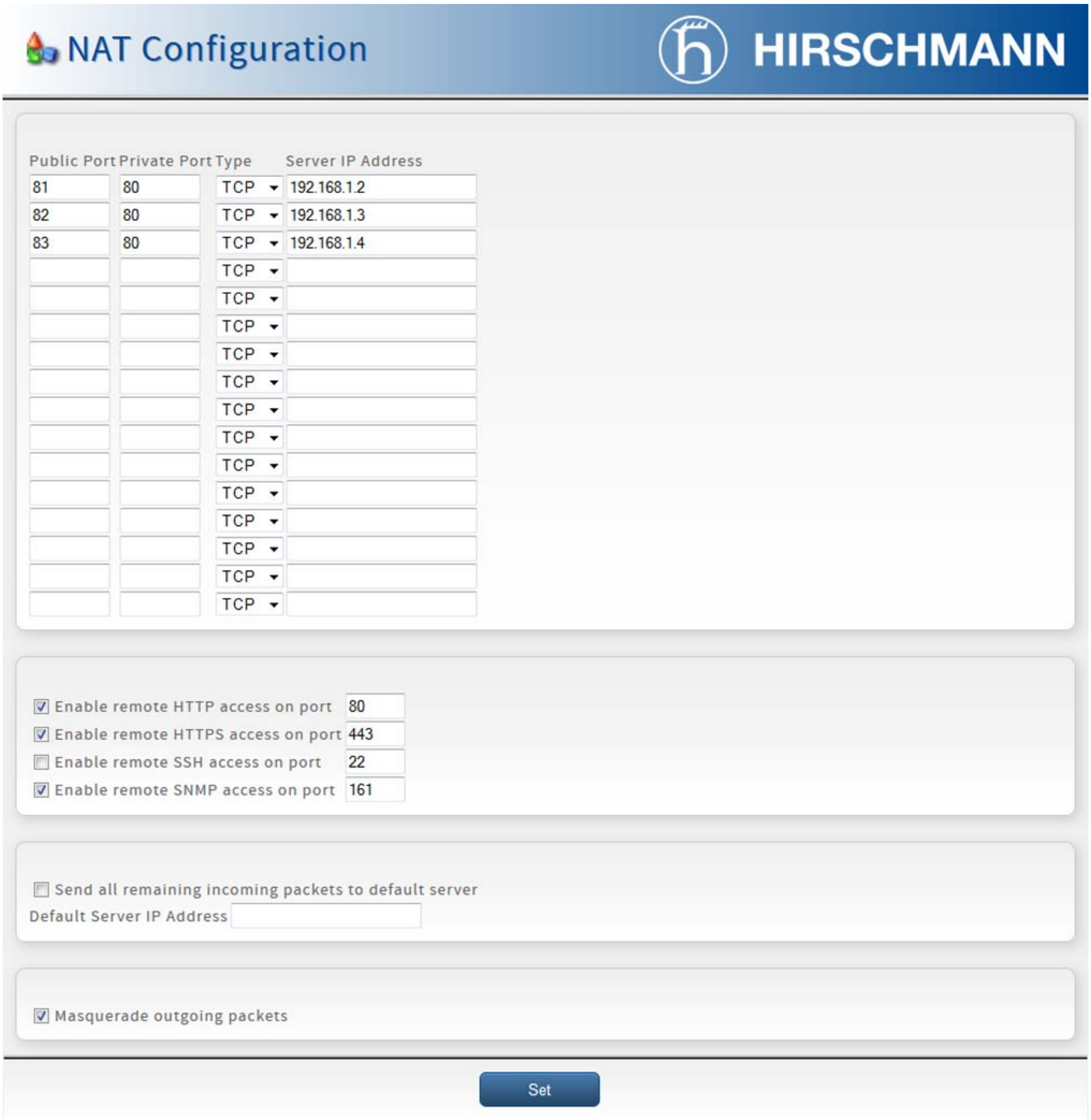


Figure 32: Topology of NAT Configuration Example 2

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



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 SSH access on port 22

☑ Enable remote SNMP access on port 161

☐ Send all remaining incoming packets to default server

Default Server IP Address

☑ Masquerade outgoing packets

Figure 33: NAT Configuration Example 2

Services

The "Services Configuration" dialog is only available for users with the admin role.

You can perform SSH service configurations in the "Services Configuration" dialog. The default settings of the sshd daemon, which provides the connection, is inactive. Until a user activates the service access in this dialog, using the "Enable SSH service" checkbox, the router denies service access. Also, when the access is deactivated, the router stops the ssh daemon and discards new login attempts.

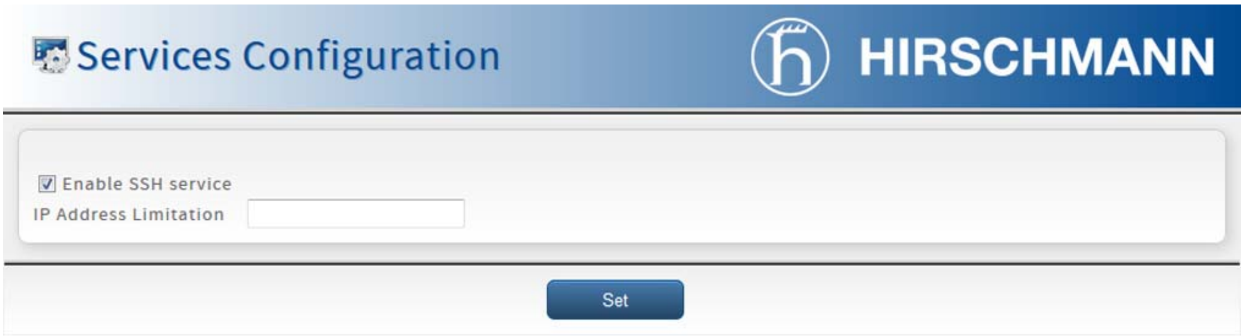
To provide fine grade access limitation to the service access, a user is able to limit access to the ssh service/port to a particular IP address. This is possible using the "IP Address Limitation" field in this dialog.

Note: This limitation applies only when the service access is enabled.

This field allows you to enter the following values:

- Single IP address – only the specified address is allowed to connect to ssh service
- IP/netmask notation (for example, 10.0.0.0/24) – only IP addresses from this segment are allowed to connect to the ssh service
- Left empty – access limitation is disabled, any IP address can connect

Note: Changing the IP address requires you to restart the device. After restarting the device re-establish the ssh connection.


Services Configuration

☑ Enable SSH service

IP Address Limitation

Figure 34: Services

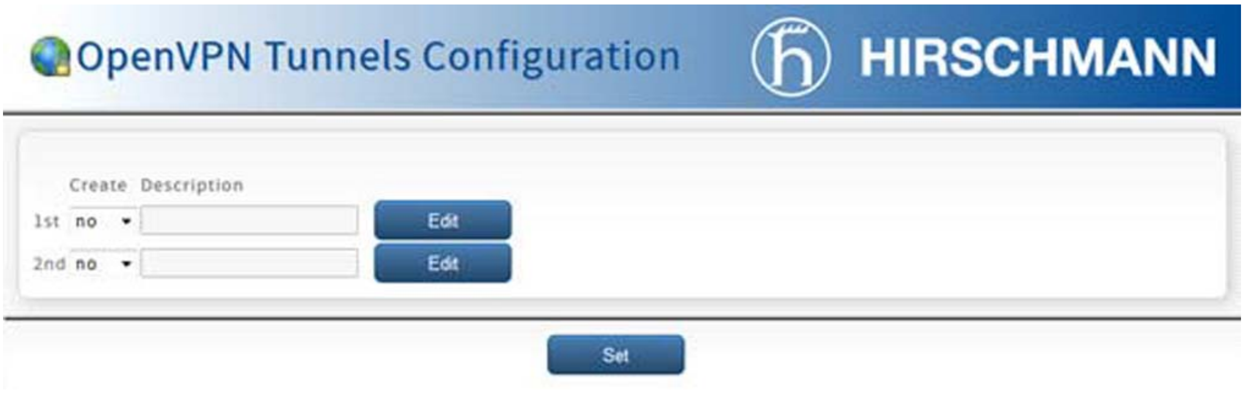
1.3.4 Virtual Private Network

OpenVPN

To open the "OpenVPN Tunnel Configuration" dialog, click "OpenVPN" in the "Configuration> Virtual Private Network" section of the main menu. The OpenVPN tunnel function allows you to create a secure connection between 2 separate LAN networks. The router allows you to create up to 2 OpenVPN tunnels.

Parameter	Description
Create	Activates/deactivates the individual tunnel configurations.
Description	Displays the name of the tunnel specified in the configuration form.
Edit	Opens the OpenVPN tunnel configuration form.

Table 30: OpenVPN Tunnels Overview


OpenVPN Tunnels Configuration

	Create	Description	
1st	no		Edit
2nd	no		Edit

Figure 35: OpenVPN Tunnels List

Parameter	Description
Description	Specifies the description or name of tunnel
Protocol	Specifies the communication protocol. Possible values: ▶ `UDP` (default setting) The OpenVPN communicates using UDP. ▶ `TCP server` The OpenVPN communicates using TCP in server mode. ▶ `TCP client` The OpenVPN communicates using TCP in client mode.
UDP/TCP port	Specifies the port of the relevant protocol (UDP or TCP)

Table 31: OpenVPN Tunnels Overview

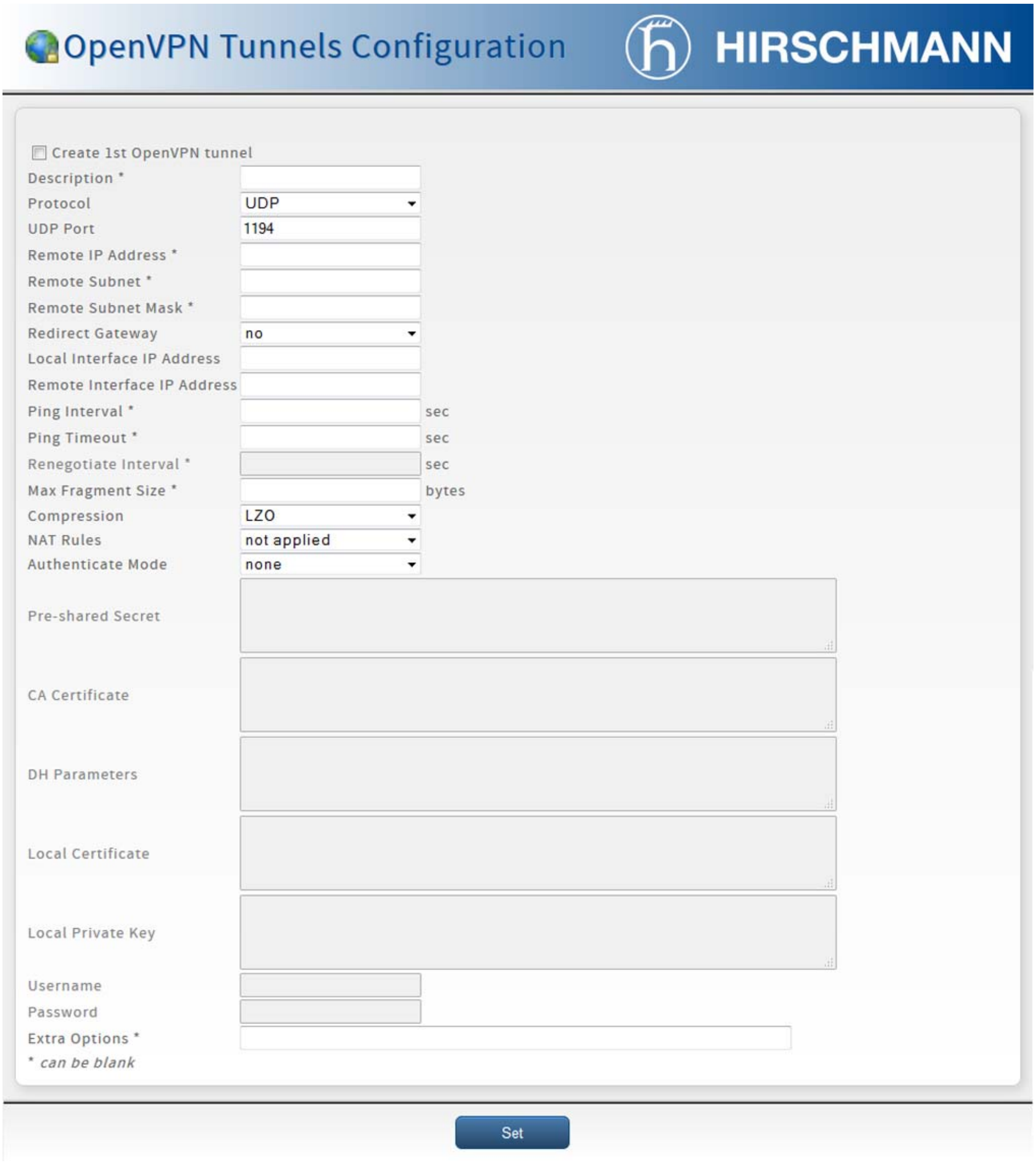
Parameter	Description
Remote IP Address	Specifies the IP address of opposite tunnel side. You can also use the domain name.
Remote Subnet	Specifies the IP address of a network behind opposite side of the tunnel.
Remote Subnet Mask	Specifies the subnet mask of a network behind opposite side of the tunnel
Redirect Gateway	Activates/deactivates redirection of data on Layer 2.
Local Interface IP Address	Specifies the IP address of a local interface
Remote Interface IP Address	Specifies the IP address of the interface of opposite side of the tunnel
Ping Interval	Specifies the time interval after which the router sends a message to opposite side of tunnel to verify the existence of the tunnel.
Ping Timeout	Specifies the time interval during which the router waits for a message sent by the opposite side. For proper verification of the OpenVPN tunnel, set the Ping Timeout to greater than the Ping Interval.
Renegotiate Interval	Specifies the renegotiate period (reauthorization) of the OpenVPN tunnel. You can only set this parameter when the "Authenticate Mode" is set to `username/password` or `X.509 certificate`. After this time period, the router changes the tunnel encryption to help provide the continues safety of the tunnel.
Max Fragment Size	Specifies the maximum size of a sent packet
Compression	Specifies the compression of the data sent. Possible values: ▶ `none` No compression is used. ▶ `LZO` (default setting) A lossless compression is used, use the same setting on both sides of the tunnel.
NAT Rules	Activates/deactivates the NAT rules for the OpenVPN tunnel. Possible values: ▶ `not applied` (default setting) NAT rules are not applied to the OpenVPN tunnel. ▶ `applied` NAT rules are applied to the OpenVPN tunnel.

Table 31: OpenVPN Tunnels Overview

Parameter	Description
Authenticate Mode	Specifies the authentication mode: Possible values: ▶ `none` No authentication is set. ▶ `pre-shared secret` Specifies the shared key function for both sides of the tunnel. ▶ `username/password` Specifies authentication using a CA Certificate, Username and Password. ▶ `X.509 cert. (multiclient)` Activates the X.509 authentication in multi-client mode. ▶ `X.509 cert. (client)` Activates the X.509 authentication in client mode. ▶ `X.509 cert. (server)` Activates the X.509 authentication in server mode.
Pre-shared Secret	Specifies the pre-shared secret which you can use for every authentication mode.
CA Certificate	Specifies the CA Certificate which you can use for the `username/password` and X.509 Certificate authentication modes.
DH Parameters	Specifies the protocol for the DH parameters key exchange which you can use for X.509 Certificate authentication in the server mode.
Local Certificate	Specifies the certificate used in the local device. You can use this authentication certificate for the X.509 Certificate authentication mode.
Local Private Key	Specifies the key used in the local device. You can use the key for the X.509 Certificate authentication mode.
Username	Specifies a login name which you can use for authentication in the username/password mode.
Password	Specifies a password which you can use for authentication in the username/password mode.
Extra Options	Specifies additional parameters for the OpenVPN tunnel, such as DHCP options. The parameters are proceeded by 2 dashes.For possible parameters see the help text in the router using SSH - run the openvpnd --help command.

Table 31: OpenVPN Tunnels Overview

The changes in the dialog apply after clicking the "Set" button.



OpenVPN Tunnels Configuration

HIRSCHMANN

□ 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 36: OpenVPN Tunnel Configuration

Example of the OpenVPN tunnel configuration:

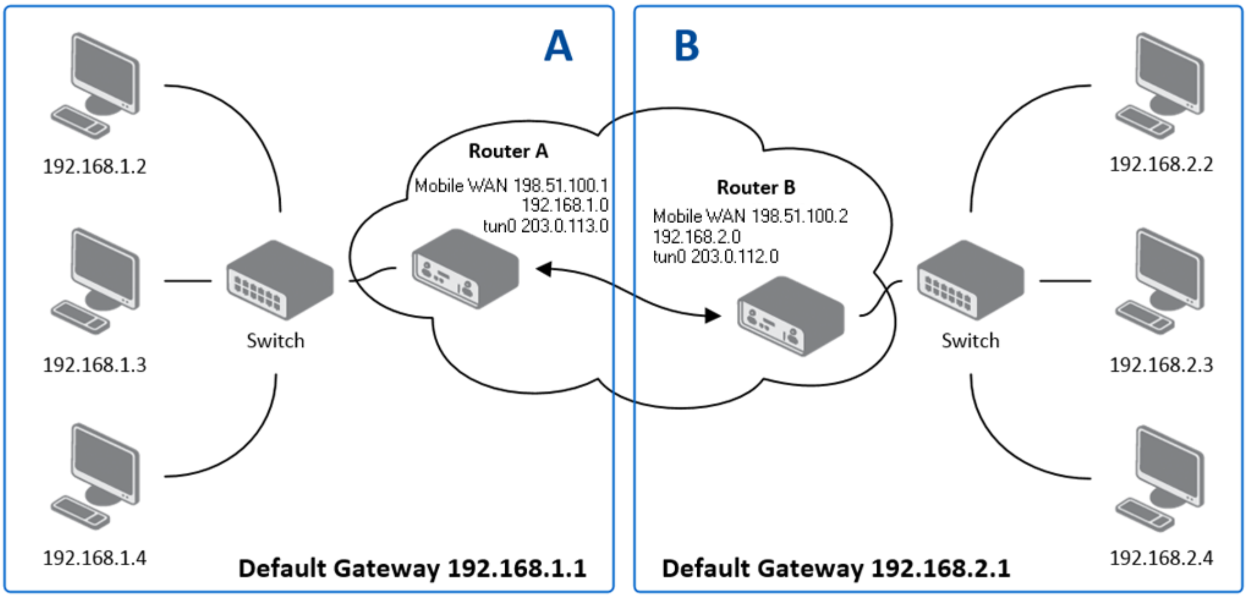


Figure 37: Topology of OpenVPN Configuration Example

OpenVPN tunnel configuration:

Configuration	A	B
Protocol	UDP	UDP
UDP Port	1194	1194
Remote IP Address	198.51.100.2	198.51.100.1
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	203.0.113.0	203.0.112.0
Remote Interface IP Address	203.0.112.0	203.0.113.0
Compression	LZO	LZO
Authenticate mode	none	none

Table 32: OpenVPN Configuration Example

For examples of different OpenVPN tunnel configuration and authentication options:
See “OpenVPN protocol” on page 117.

IPsec

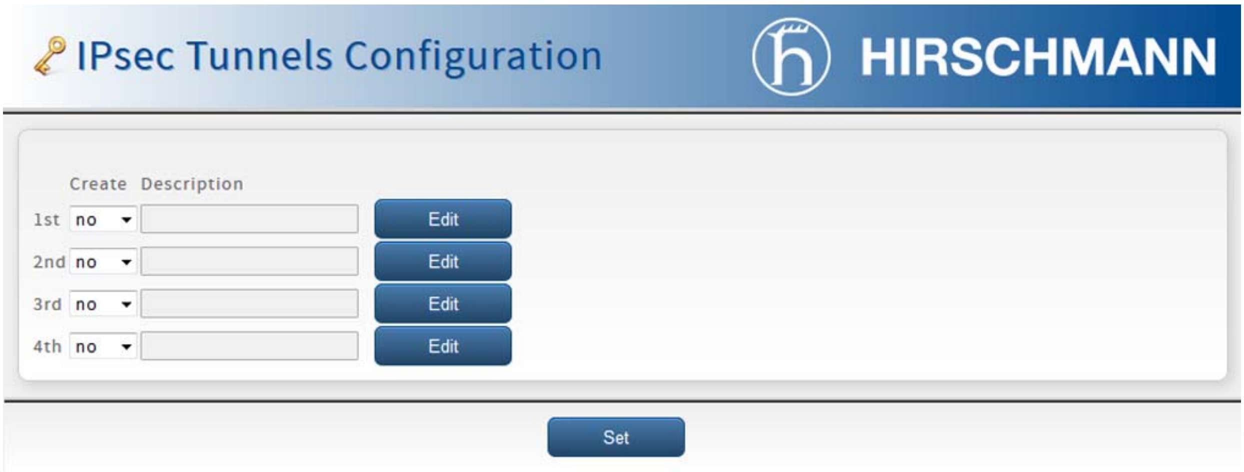
To open the "IPsec Tunnel Configuration" dialog, click "IPsec" in the "Configuration" section of the main menu. The IPsec tunnel function allows you to create a secured connection between 2 separate LAN networks. The router allows you to create up to 4 IPsec tunnels.

Note: To encrypt data between the local and remote subnets, specify the appropriate values in the subnet fields on both routers. To encrypt the data stream between the routers only, leave the local and remote subnets fields blank.

Note: If you specify the protocol and port information in the "Local Protocol/Port" field, then the router encapsulates only the packets matching the settings.

Parameter	Description
Create	Activates/deactivates the individual IPsec tunnels.
Description	Displays the name of the tunnel specified in the configuration of the tunnel.
Edit	Opens the IPsec tunnel configuration form.

Table 33: IPsec Tunnels Overview



IPsec Tunnels Configuration

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

Set

Figure 38: IPsec Tunnels List

Parameter	Description
Description	Specifies the name or description of the tunnel
Remote IP Address	Specifies the IP address of remote side of the tunnel. It is also possible to enter the domain name.
Remote ID	Specifies the identifier (ID) of remote side of the tunnel. It consists of 2 parts: a hostname and a domain-name.
Remote Subnet	Specifies the IP address of a network behind remote side of the tunnel
Remote Subnet Mask	Specifies the Subnet mask of a network behind remote side of the tunnel
Remote Protocol/Port	Specifies the protocol and port of the remote side of the tunnel. The general form is protocol/port, for example 17/1701 for UDP (protocol 17) and port 1701. It is also possible to enter only the number of protocol, however, the above mentioned format is preferred.
Local ID	Specifies the identifier (ID) of local side of the tunnel. It consists of 2 parts: a hostname and a domain-name.
Local Subnet	Specifies the IP address of a local network
Local Subnet Mask	Specifies the subnet mask of a local network
Local Protocol/Port	Specifies the protocol and port of a local network. The general form is protocol/port, for example 17/1702 for UDP (protocol 17) and port 1702. It is also possible to enter only the number of protocol, however, the above mentioned format is preferred.
Encapsulation Mode	Specifies the IPsec mode, according to the method of encapsulation. You can select the `tunnel` mode in which the entire IP datagram is encapsulated or the `transport` mode in which only IP header is encapsulated.
NAT traversal	Enable/disables NAT address translation on the tunnel. If you use NAT between the end points of the tunnel, then enable this parameter.
IKE Mode	Specifies the mode for establishing a connection (`main` or `aggressive`). If you select the aggressive mode, then the router establishes the IPsec tunnel faster, but the encryption is permanently set to 3DES-MD5. We recommend that you not use the aggressive mode due to lower security.
IKE Algorithm	Specifies the means by which the router selects the algorithm. Possible values: ▶ `auto` The encryption and hash alg. are selected automatically. ▶ `manual` The encryption and hash alg. are defined by the user.
IKE Encryption	Specifies the encryption algorithm. Possible values: ▶ `3DES` ▶ `AES128` ▶ `AES192` ▶ `AES256`

Table 34: IPsec Tunnels Overview

Parameter	Description
IKE Hash	Specifies the hash algorithm. Possible values are: Possible values: ▶ `MD5` ▶ `SHA1` ▶ `SHA256` ▶ `SHA384` ▶ `SHA512`
IKE DH Group	Specifies the Diffie-Hellman groups which determine the strength of the key used in the key exchange process. Higher group numbers are more secure, but require additional time to compute the key.
ESP Algorithm	Specifies the means by which the router selects the algorithm: Possible values: ▶ `auto` The encryption and hash algorithm are selected automatically. ▶ `manual` The encryption and hash algorithm are defined by the user.
ESP Encryption	Specifies the encryption algorithm. Possible values are: Possible values: ▶ `DES` ▶ `3DES` ▶ `AES128` ▶ `AES192` ▶ `AES256`
ESP Hash	Specifies the hash algorithm. Possible values are: Possible values: ▶ `MD5` ▶ `SHA1` ▶ `SHA256` ▶ `SHA384` ▶ `SHA512`
PFS	Enables/disables the Perfect Forward Secrecy function. The function ensures that derived session keys are not compromised if one of the private keys is compromised in the future
PFS DH Group	Specifies the Diffie-Hellman group number (see IKE DH Group)
Key Lifetime	Specifies the lifetime key data part of tunnel. The minimum value of this parameter is `60s`. The maximum value is `86400s`.
IKE Lifetime	Specifies the 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 a connection expires that the router attempts to negotiate a replacement. Specify a maximum value that is less than half of IKE and Key Lifetime parameters.
Rekey Fuzz	Specifies the percentage of time for the Rekey Margin extension.
DPD Delay	Specifies the time after which the IPsec tunnel functionality is tested
DPD Timeout	Specifies the period during which device waits for a response

Table 34: IPsec Tunnels Overview

Parameter	Description
Authenticate Mode	Specifies the means by which the router authenticates: Possible values: ▶ `pre-shared key` Sets the shared key for both sides of the tunnel. ▶ `X.509 certificate` Allows X.509 authentication in multiclient mode
Pre-shared Key	Specifies the shared key for both sides of the tunnel. The prerequisite for entering a key is that you select `pre-shared key` as the authentication mode
CA Certificate	Specifies the certificate for X.509 authentication.
Remote Certificate	Specifies the certificate for X.509 authentication.
Local Certificate	Specifies the certificate for X.509 authentication.
Local Private Key	Specifies the private key for X.509 authentication.
Local Passphrase	Specifies the passphrase used during private key generation.
Extra Options	Specifies the additional parameters of the IPsec tunnel for example, secure parameters.

Table 34: IPsec Tunnels Overview

The IPsec function supports the following types of identifiers (ID) for both sides of the tunnel, Remote ID and Local ID parameters:

- IP address (for example, 192.168.1.1)
- DN (for example, C=DE,O=Hirschmann Automation and Control GmbH,OU=TP,CN=A)
- FQDN (for example, @director.hirschmann.de) – the “@” symbol proceeds the FQDN.
- User FQDN (for example, director@hirschmann.de)

The certificates and private keys have to be in the PEM format. Use only certificates containing start and stop tags.

The random time, after which the router re-exchanges new keys is defined as follows:

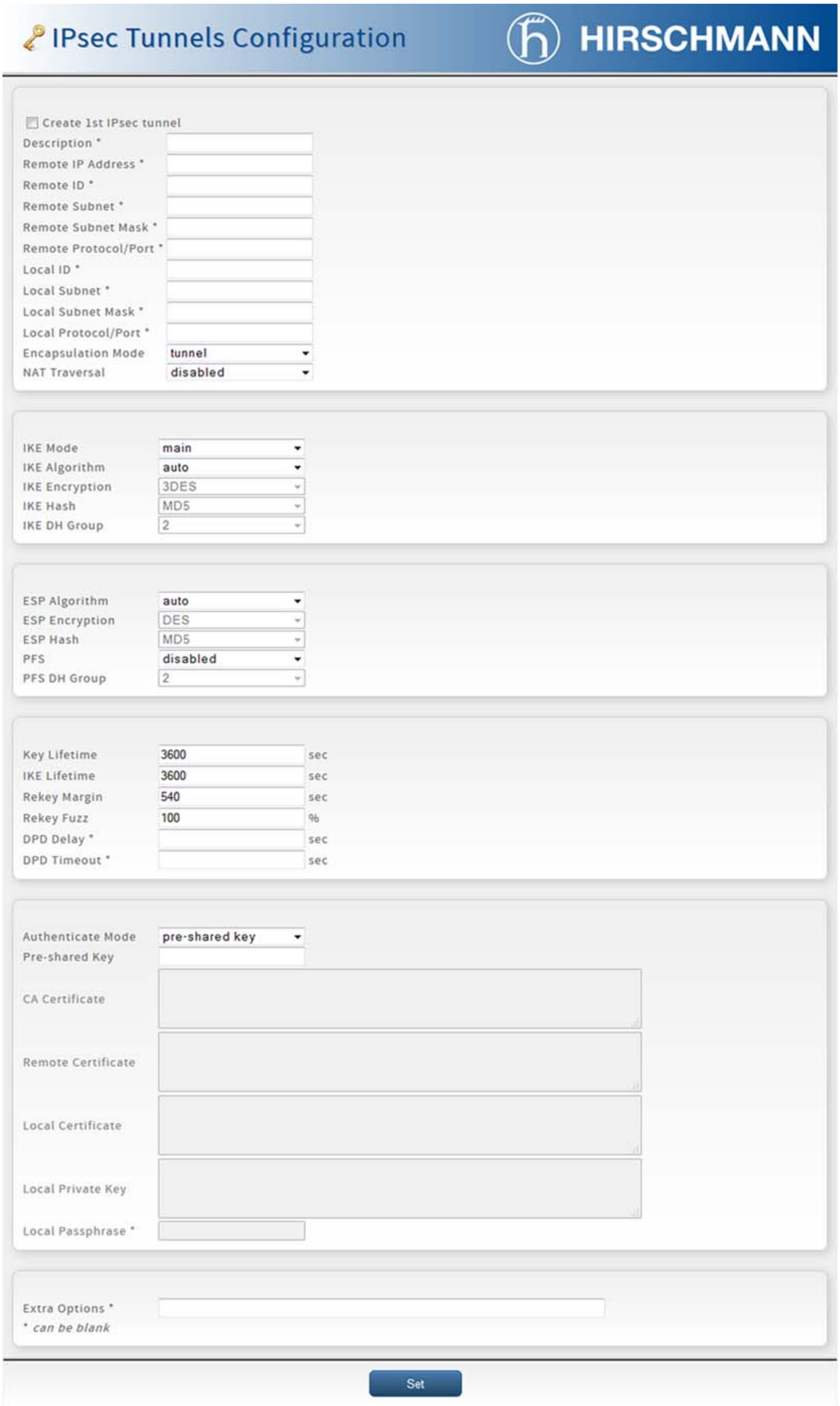
Lifetime = (Rekey margin + random value in range (from 0 to Rekey margin * Rekey Fuzz/100))

The default exchange of keys is in the following time range:

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

We recommend that you maintain the default settings. When you set key exchange times higher, the tunnel produces lower operating costs, but the setting also provides less security. Conversely, when you reducing the time, the tunnel produces higher operating costs, but provides for higher security.

The changes in the dialog apply after clicking the "Set" button.



IPsec Tunnels Configuration

□ Create 1st IPsec tunnel

Description *	
Remote IP Address *	
Remote ID *	
Remote Subnet *	
Remote Subnet Mask *	
Remote Protocol/Port *	
Local ID *	
Local Subnet *	
Local Subnet Mask *	
Local Protocol/Port *	
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 39: IPsec Tunnels Configuration

Example of the IPSec Tunnel configuration.

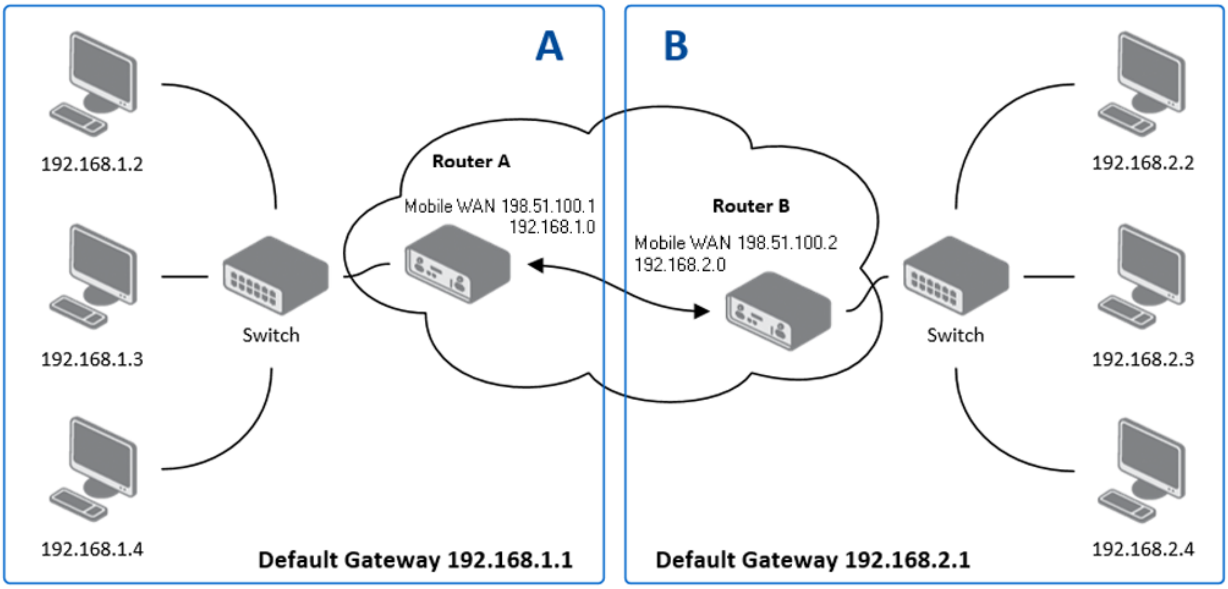


Figure 40: Topology of IPsec Configuration Example

IPsec tunnel configuration:

Configuration	A	B
Remote IP Address	198.51.100.2	198.51.100.1
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

Table 35: IPsec Configuration Example

You can find examples of different IPsec tunnel configurations and authentication options in the User Manual “IPsec Tunnel Application Note”.

GRE

GRE is an unencrypted protocol.

To open the "GRE Tunnel Configuration" dialog, click "GRE" in the "Configuration" section of the main menu. The GRE tunnel function allows you to create an unencrypted connection between 2 separate LAN networks. The router allows you to create 4 GRE tunnels.

Parameter	Description
Create	Activates/deactivates the individual GRE tunnels
Description	Displays the name of the tunnel specified in the configuration form.
Edit	Opens the GRE tunnel configuration form.

Table 36: GRE Tunnels Overview

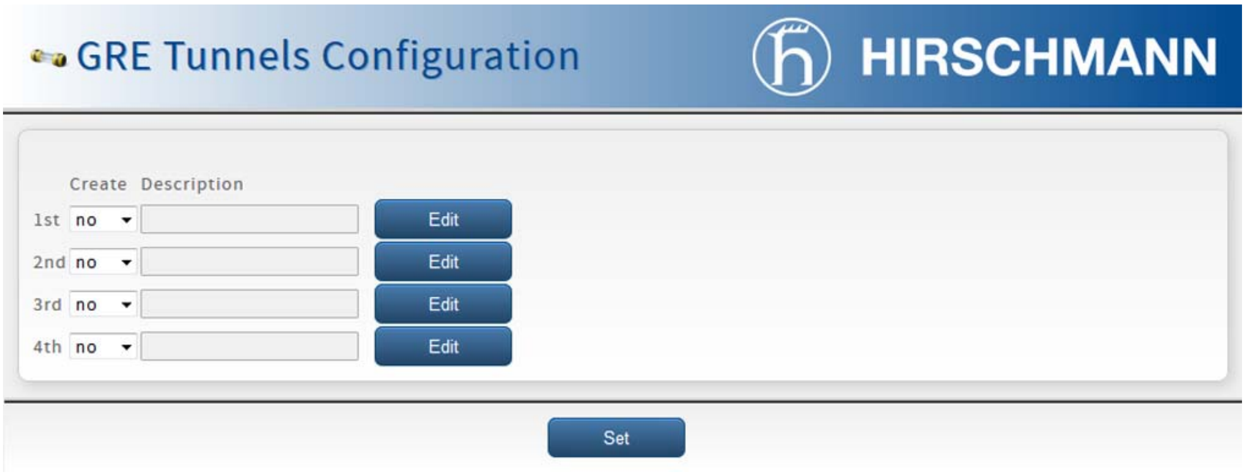


Figure 41: GRE Tunnels List

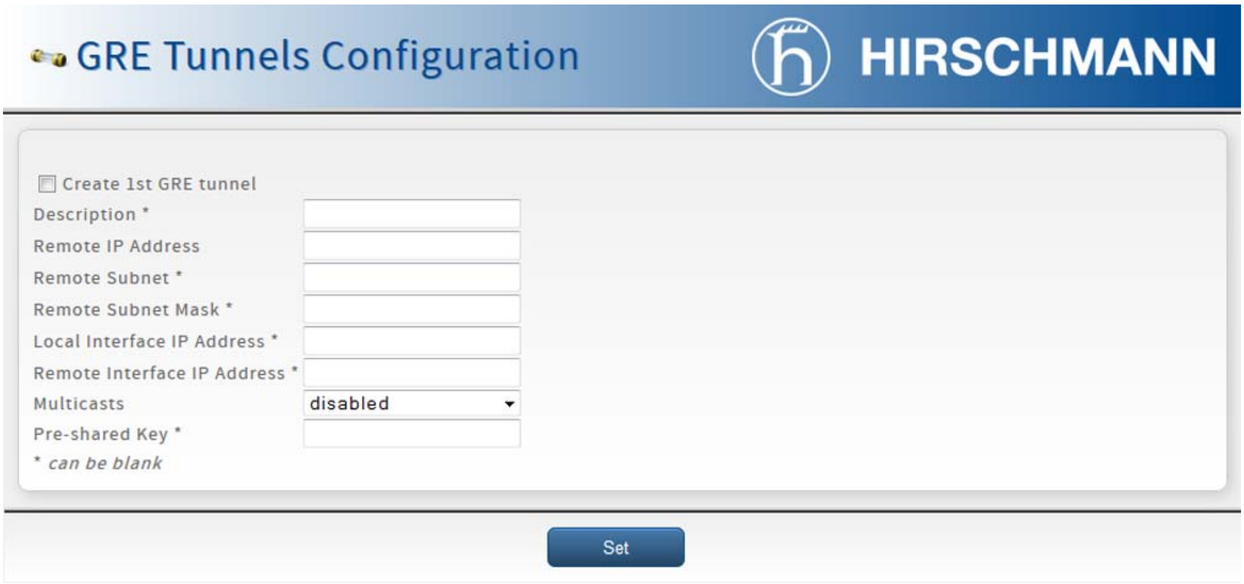
Parameter	Description
Description	Specifies the description of the GRE tunnel.
Remote IP Address	Specifies the IP address of the remote side of the tunnel.
Remote Subnet	Specifies the IP address of the network behind the remote side of the tunnel.
Remote Subnet Mask	Specifies the mask of the network behind the remote side of the tunnel.
Local Interface IP Address	Specifies the IP address of the local side of the tunnel.
Remote Interface IP Address	Specifies the IP address of the remote side of the tunnel.

Table 37: GRE Tunnel Configuration dialog

Parameter	Description
Multicasts	Activates/deactivates sending multicast into the GRE tunnel. Possible values: ▶ disabled Sending multicast into the tunnel is inactive. ▶ enabled Sending multicast into the tunnel is active.
Pre-shared Key	Specifies an optional value for the 32 bit shared key in numeric format, with this key the router sends the filtered data through the tunnel. Specify the same key on both routers, otherwise the router drops received packets.

Table 37: GRE Tunnel Configuration dialog

Note: The GRE tunnel does not pass through NAT.


GRE Tunnels Configuration

□ Create 1st GRE tunnel

Description *	
Remote IP Address	
Remote Subnet *	
Remote Subnet Mask *	
Local Interface IP Address *	
Remote Interface IP Address *	
Multicasts	disabled
Pre-shared Key *	

* *can be blank*

Figure 42: GRE Tunnel Configuration dialog

Example of the GRE Tunnel configuration:

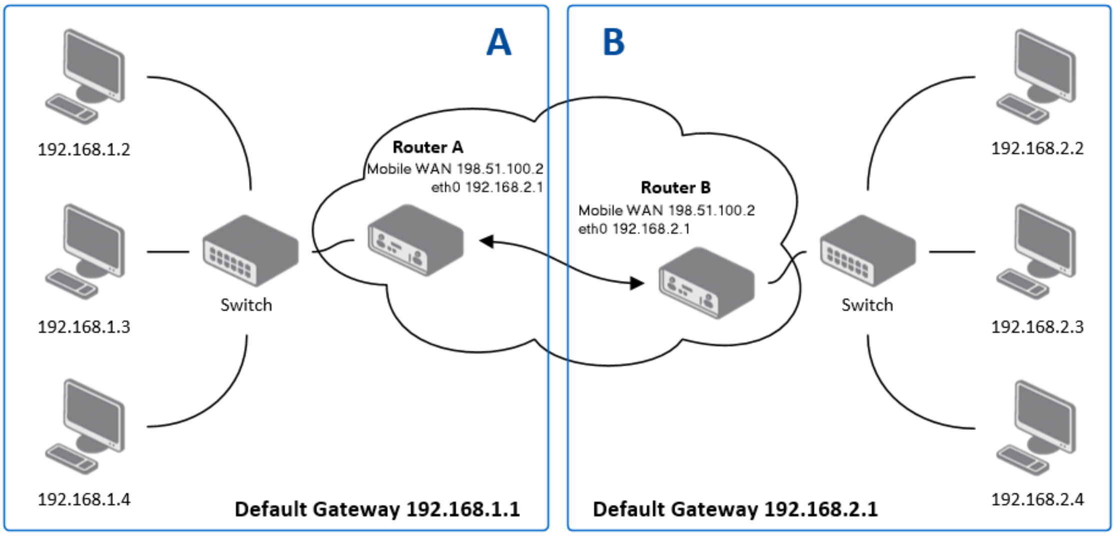


Figure 43: Topology of GRE Tunnel Configuration Example

GRE tunnel Configuration:

Configuration	A	B
Remote IP Address	198.51.100.2	198.51.100.1
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0

Table 38: GRE Tunnel Configuration Example

For examples of different GRE tunnel configurations and authentication options:
See “GRE Protocol” on page 221.

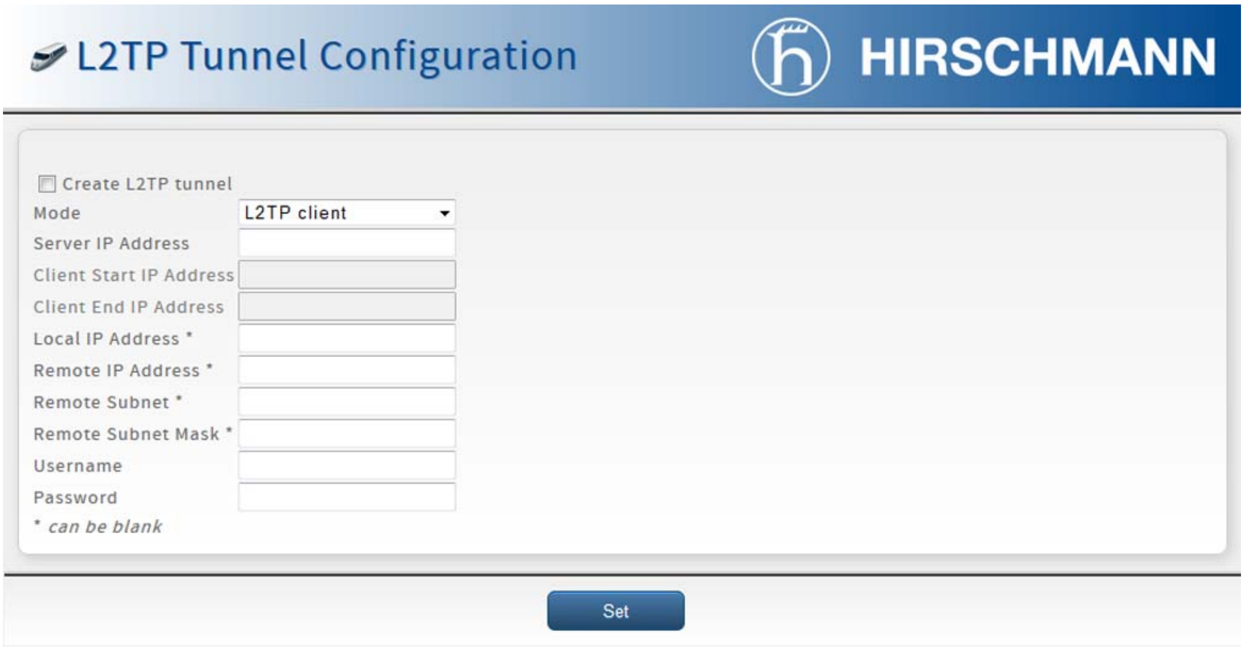
■ L2TP

L2TP is an unencrypted protocol.

To open the "L2TP Tunnel Configuration" dialog, click "L2TP" in the "Configuration" section of the main menu. The L2TP tunnel function allows you to create a password protected connection between 2 LAN networks. The router activates the tunnels after you mark the "Create L2TP tunnel" check box.

Parameter	Description
Mode	Specifies the L2TP tunnel mode on the router side: Possible values: ▶ `L2TP server` Specify an IP address range offered by the server. ▶ `L2TP client` Specify the IP address of the server.
Server IP Address	Specifies the IP address of the server.
Client Start IP Address	Specifies the IP address to start with in the address range. The range is offered by the server to the clients.
Client End IP Address	Specifies the last IP address in the address range. The range is offered by the server to the clients.
Local IP Address	Specifies the IP address of the local side of the tunnel.
Remote IP Address	Specifies the IP address of the remote side of the tunnel.
Remote Subnet	Specifies the address of the network behind the remote side of the tunnel.
Remote Subnet Mask	Specifies the mask of the network behind the remote side of the tunnel.
Username	Specifies the username for the L2TP tunnel login.
Password	Specifies the password for the L2TP tunnel login.

Table 39: GRE 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 44: L2TP Tunnel Configuration

Example of the L2TP tunnel configuration:

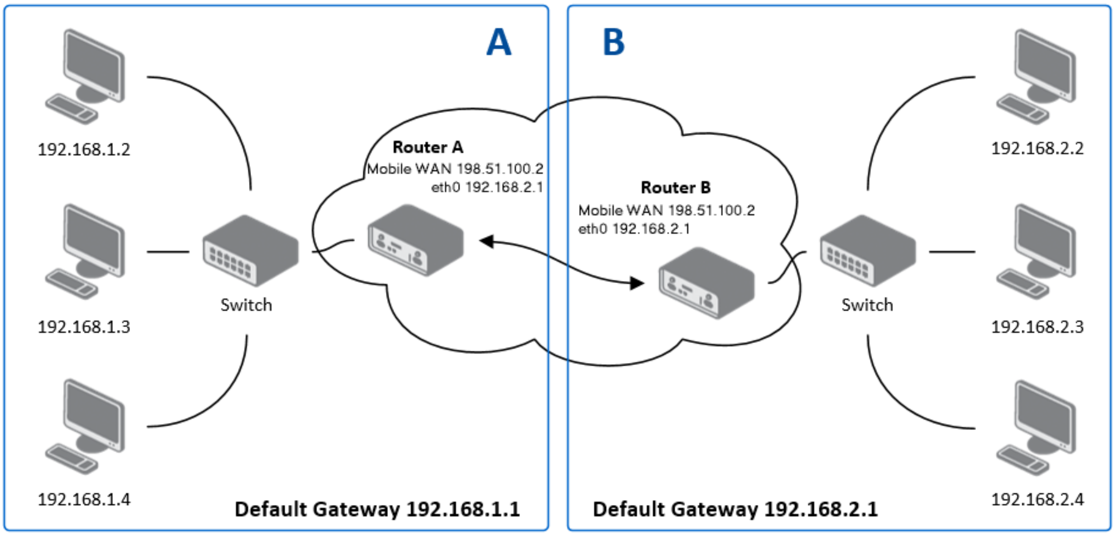


Figure 45: Topology of L2TP Tunnel Configuration Example

Configuration of the L2TP tunnel:

Configuration	A	B
Mode	L2TP Server	L2TP Client
Server IP Address	-	10.0.0.1
Client Start IP Address	192.168.1.2	-
Client End IP Address	192.168.1.254	-
Local IP Address	192.168.1.1	-
Remote IP Address	-	-
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Username	username	username
Password	password	password

Table 40: L2TP Tunnel Configuration Example

1.3.5 Device Configuration

■ Time

The "Time" dialog allows you to configure the NTP client. To open the "Time" dialog, click "Time" in the "Configuration" section of the main menu. NTP (Network Time Protocol) allows you to periodically set the internal clock of the router. The time is set from servers that provide the exact time to network devices.

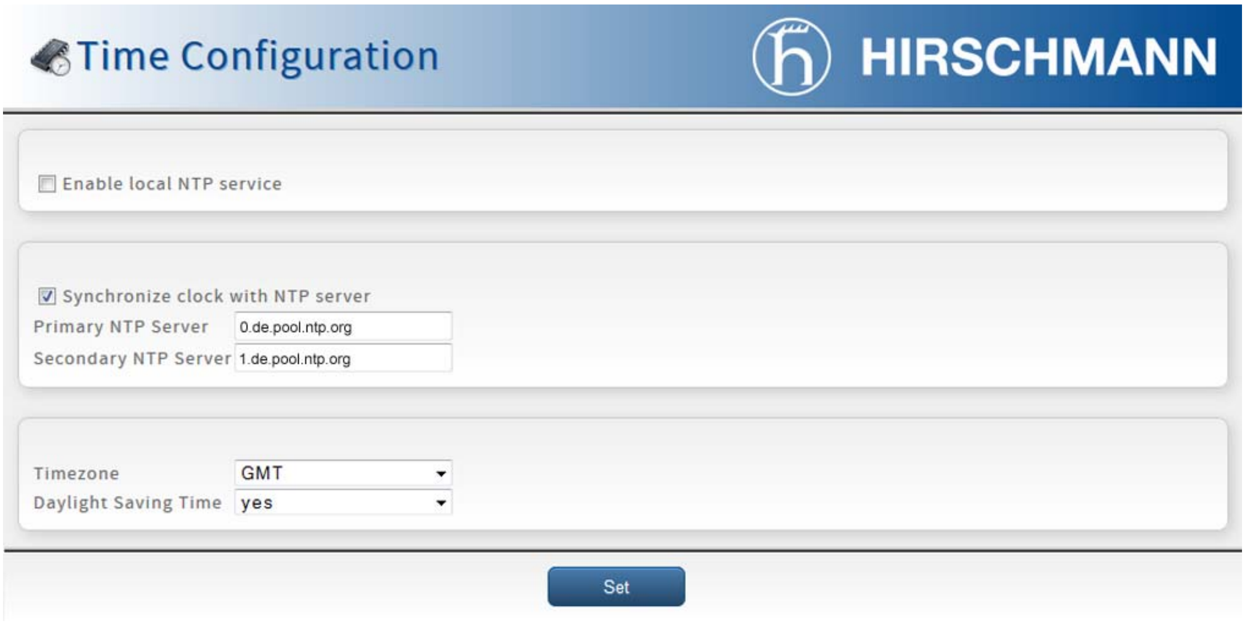
- ▶ If you mark the "Enable local NTP service" check box, then the router acts as a NTP server for other devices in the local network (LAN).
- ▶ If you mark the "Synchronize clock with NTP server" check box, then the router acts as a NTP client. This means that the router automatically adjusts the internal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

Parameter	Description
Primary NTP Server Address	Specifies the IP or domain address of primary NTP server.
Secondary NTP Server Address	Specifies the IP or domain address of secondary NTP server.
Timezone	Specifies the time zone where you installed the router.

Daylight Saving Time	Activates/deactivates the DST shift.
	Possible value:
	▶ `no`
	`The time shift is inactive.`
	▶ `yes`
	`The time shift is active.`

Table 41: NTP Configuration

The figure below displays an example of a Time configuration with the primary server set to `0.de.pool.ntp.org` and the secondary server set to `1.de.pool.ntp.org` and with the automatic change for daylight saving time enabled.



Time Configuration

□ Enable local NTP service

☑ Synchronize clock with NTP server

Primary NTP Server: 0.de.pool.ntp.org

Secondary NTP Server: 1.de.pool.ntp.org

Timezone: GMT

Daylight Saving Time: yes

Figure 46: Example of Time Configuration

SNMP

The "SNMP" dialog allows you to configure the SNMP v1/v2 or v3 agent which sends information about the router to a management station. To open the "SNMP" dialog, click "SNMP" in the "Configuration" section of the main menu. SNMP (Simple Network Management Protocol) provides status information about the network elements such as routers or endpoint computers. In the version v3, the communication is secured (encrypted). To enable the SNMP service, mark the "Enable the SNMP agent" check box.

Parameter	Description
Name	Specifies the designation of the router
Location	Specifies the location of where you installed the router.
Contact	Specifies the person who manages the router together with information how to contact this person.

Table 42: SNMP Agent Configuration

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

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

To enable the SNMPv3 function, mark the "Enable SNMPv3 access" checkbox, then specify the following parameters:

Parameter	Description
Username	Specify the user name.
Password	Specify the password used to generate the key used for authentication.
Authentication	Specify the encryption algorithm on the Authentication Protocol that is used to verify the identity of the users.
Privacy	Specify the encryption algorithm on the Privacy Protocol that is used to ensure confidentiality of data

Table 43: SNMPv3 Configuration

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

Each monitored value is uniquely identified using a numerical identifier "OID – Object Identifier". This identifier consists of a progression of numbers separated by a point. The shape of each OID is determined by the identifier value of the parent element and then this value is complemented by a point and current number. So it is obvious that there is a tree structure. The following figure displays the basic tree structure that is used for creating the OIDs.

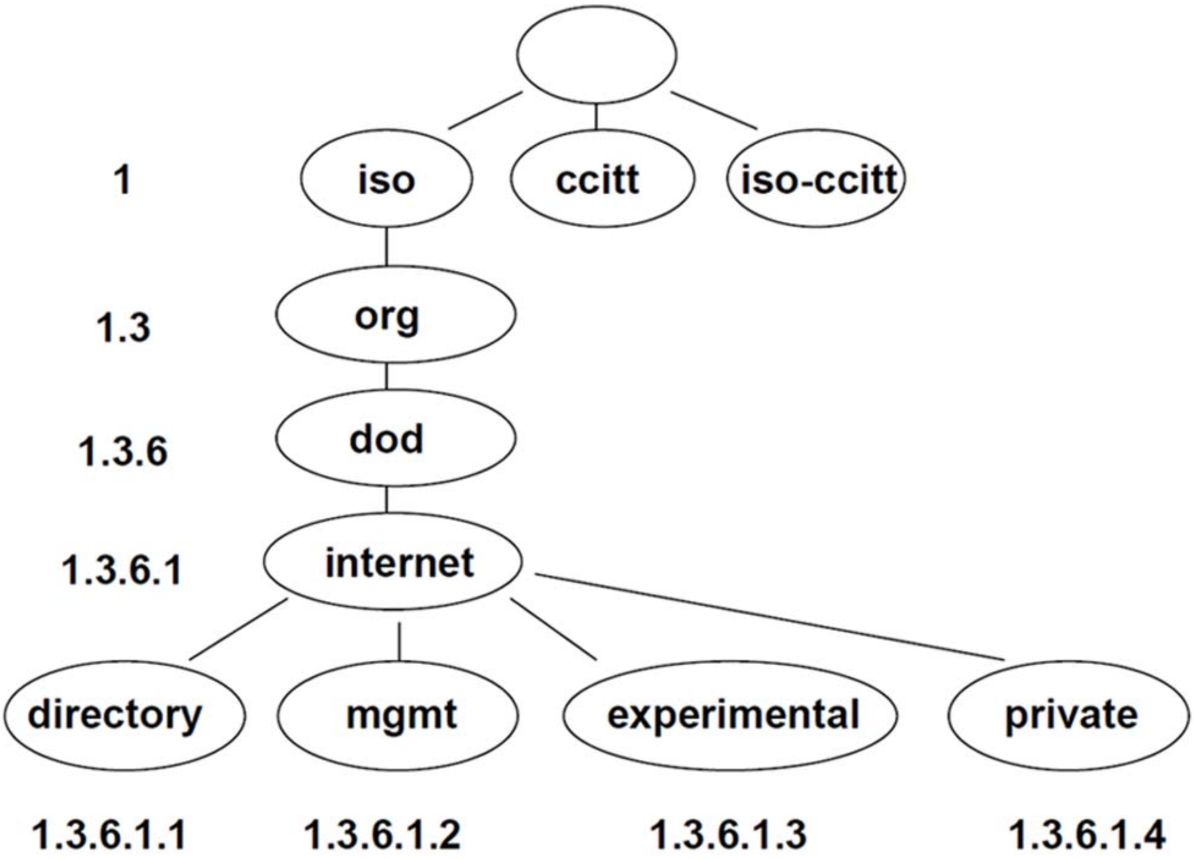


Figure 47: OID Basic Structure

The SNMP values that are specific for Hirschmann routers create the tree starting at OID = 1.3.6.1.4.1.248.40.1. You interpret the OID in the following manner:

iso.org.dod.internet.private.enterprises.hirschmann

The following figure displays the tree used for creating Hirschmann OIDs.

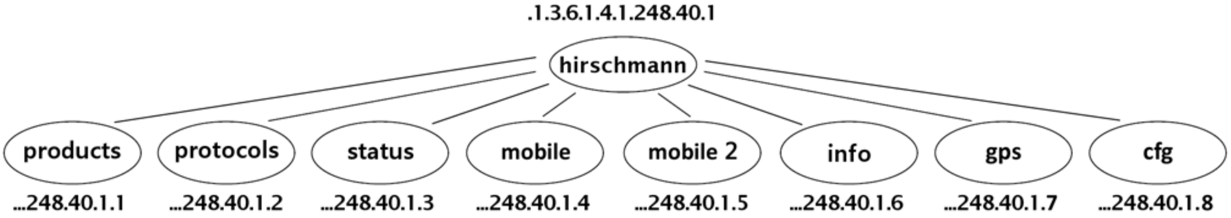
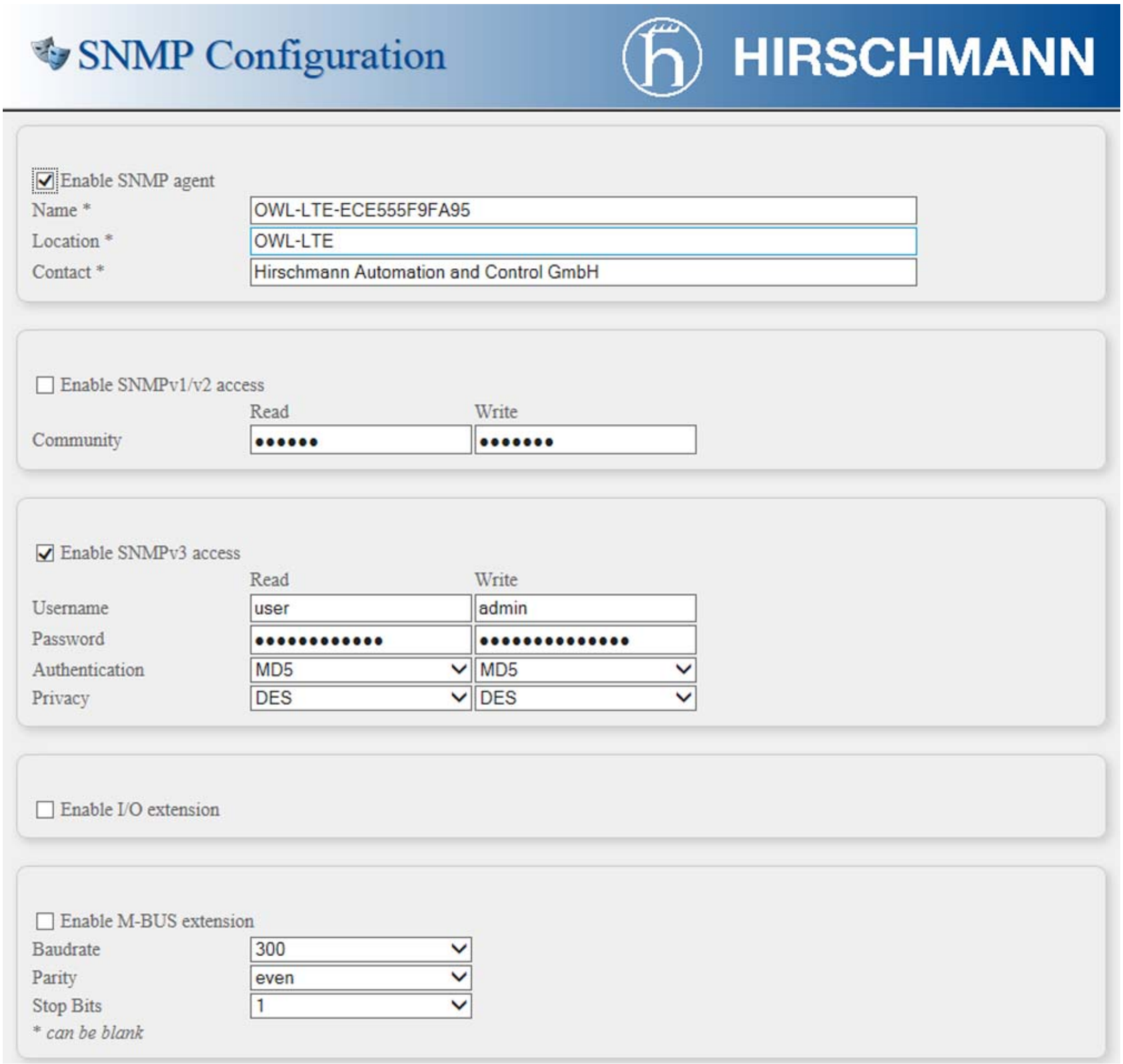


Figure 48: Hirschmann OID Tree

This means that the router provides for example, information about the internal temperature of the device (OID 1.3.6.1.4.1.248.40.1.3.3) or about the power voltage (OID 1.3.6.1.4.1.248.40.1.3.4). For the description of the OID values:
See “SNMP OID” on page 255.

Example of SNMP settings:



SNMP Configuration

☑ Enable SNMP agent

Name *	OWL-LTE-ECE555F9FA95
Location *	OWL-LTE
Contact *	Hirschmann Automation and Control GmbH

☐ Enable SNMPv1/v2 access

	Read	Write
Community	••••••	•••••••

☑ Enable SNMPv3 access

	Read	Write
Username	user	admin
Password	••••••••••••	••••••••••••••
Authentication	MD5	MD5
Privacy	DES	DES

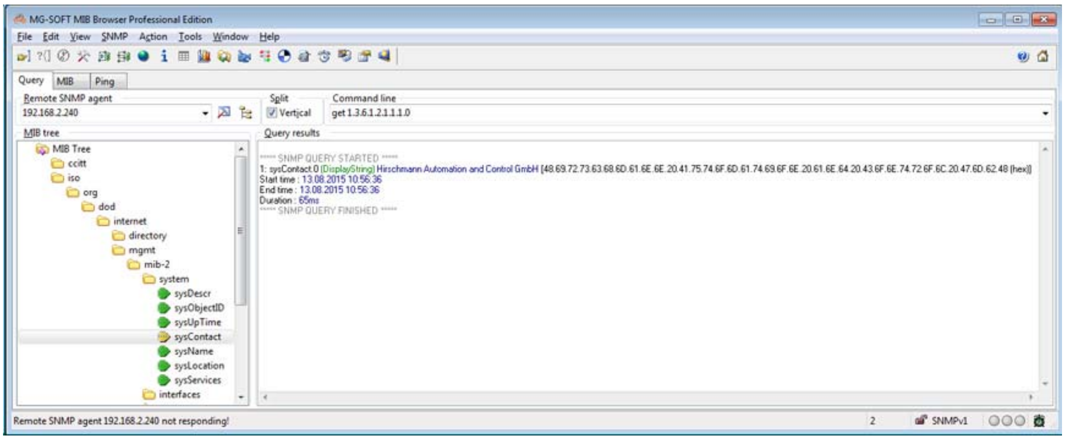
☐ Enable I/O extension

☐ Enable M-BUS extension

Baudrate	300
Parity	even
Stop Bits	1

* *can be blank*

Figure 49: SNMP Configuration Example



Remote SNMP agent: 192.168.2.240

Command line: get 1.3.6.1.2.1.1.1.0

```
***** SNMP QUERY STARTED *****
1: sysContact.0 (DisplayString) Hirschmann Automation and Control GmbH [48.69.72.73.63.68.6D.61.6E.6E.20.41.75.74.6F.6D.61.74.69.6F.6E.20.61.6E.64.20.43.6F.6E.74.72.6F.6C.20.47.6D.62.48 (hex)]
Start time : 13.08.2015 10:56:36
End time : 13.08.2015 10:56:36
Duration : 65ms
***** SNMP QUERY FINISHED *****
```

Remote SNMP agent 192.168.2.240 not responding!

Figure 50: MIB Browser Example

In order to access a particular device enter the IP address of the SNMP agent which is the router, in the "Remote SNMP agent" field. The dialog displayed the internal variables in the MIB tree after entering the IP address. Furthermore, you can find the status of the internal variables by entering their OID.

The path to the objects is:

iso -> org -> dod -> internet -> private -> enterprises -> hirschmann -> protocols

The path to information about the router is:

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

■ SMTP Configuration

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

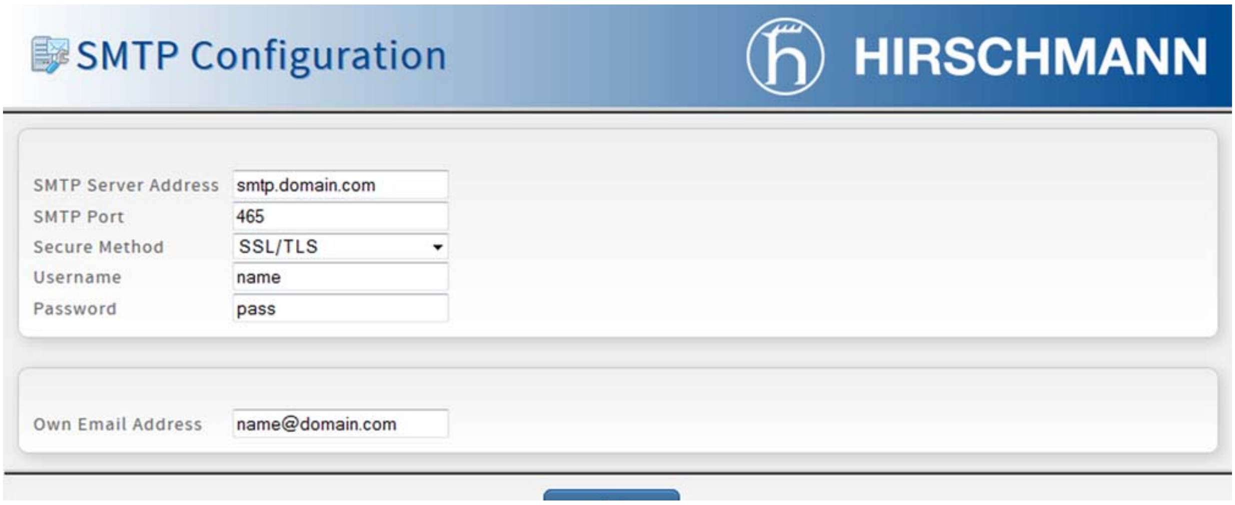
Parameter	Description
SMTP Server Address	IP or domain address of the mail server.
SMTP Port	Port the SMTP server is listening on
Secure Method	none, SSL/TLS, or STARTTLS. Secure method has to be supported by the SMTP server.
Username	E-mail account.

Table 44: SNMP Client Configuration

Parameter	Description
Password	Password for the e-mail account. The password can contain the following special characters:* + , - . / : = ? ! # % [ ] _ { } ~The following special characters are not allowed: “ $ & ’ ( ) ; < >
Own E-mail Address	Address of the sender.

Table 44: SNMP Client Configuration

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



SMTP Server Address smtp.domain.com
SMTP Port 465
Secure Method SSL/TLS
Username name
Password pass
Own Email Address name@domain.com

Figure 51: Example of the SMTP client configuration

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

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

You enter commands and parameters in lowercase. Example of sending an e-mail:email –t name@domain.com –s “`subject`” –m “`message`” –a `/mnt/abc.doc` –r `5`

The command above sends an e-mail address to, name@domain.com with the subject, body message, and attachment “abc.doc” directly from the directory /mnt/abc.doc. The router attempts to send the message 5 times.

SMS

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

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

Table 45: SMS Configuration

After you enter a phone number in the "Phone Number 1" field, the router allows you to configure the control of the device using an SMS message. You can configure up to 3 numbers for incoming SMS messages. To enable the function, mark the "Enable remote control via SMS" check box. The default setting of the remote control function is active.

Parameter	Description
Phone Number 1	Specifies the first phone number allowed to access the router using an SMS.
Phone Number 2	Specifies the second phone number allowed to access the router using an SMS.
Phone Number 3	Specifies the third phone number allowed to access the router using an SMS.

Table 46: Control via SMS

Note:
- If you leave the phone number field blank, then you can restart the router using an SMS Reboot message from any phone number.
- If you enter one or more phone numbers, then you can control the router using SMS messages sent only from the specified phone numbers.
- If you enter the wild card character `*`, then you can control the router using SMS messages sent from any phone number.

Control SMS messages do not change the router configuration. For example, if the router is changed to the off line mode using an SMS message, then the router remains in this mode.To return the router to the on-line mode, reboot or power cycle the device. The behavior is the same for every SMS control message.

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

Parameter	Description
go online sim 1	The router changes to SIM1 (APN1)
go online sim 2	The router changes to SIM2 (APN2)
go online	Changes the router to the online mode
go off line	Changes the router to the off line mode
set profile std	Sets the standard profile
set profile alt1	Sets the alternative profile 1
set profile alt2	Sets the alternative profile 2
set profile alt3	Sets the alternative profile 3
reboot	The router reboots
get ip	The router responds with the IP address of the SIM card.

Table 47: Control SMS

Setting the parameters in the "Enable AT-SMS protocol over TCP" frame, you can enable the router to send and receive SMS messages on a TCP port. This function requires you to specify a TCP port number. The router sends SMS messages using a standard AT command.

Parameter	Description
TCP Port	TCP port the sending/receiving SMS messages will be allowed on.

Table 48: Send SMS on Ethernet PORT1 configuration

Working with SMS messages

If you establish a connection to the router using a serial interface or Ethernet, then you can use AT commands to manage SMS messages. The following table lists only the commands that the router supports. For other AT commands the router sends an OK response. The router sends an ERROR response for complex AT commands.

For a detailed description and examples of these AT commands: See “AT Commands” on page 241.

Parameter	Description
AT+CGMI	Returns the specific identity of the manufacturer
AT+CGMM	Returns the specific model identity of the manufacturer
AT+CGMR	Returns the specific model revision identity of the manufacturer
AT+CGPADDR	Displays the IP address of the usb0 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 for 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 a specific phone number
AT+CMGW	Writes a short message to the SIM storage
AT+CMSS	Sends a message from the SIM storage location
AT+COPS?	Identifies the mobile networks available
AT+CPIN	Used to query and enter a PIN code
AT+CPMS	Selects the SMS memory storage types, to be used for the short message operations
AT+CREG	Displays the network registration status
AT+CSCA	Sets the short message service center (SMSC) number

Table 49: List of AT Commands

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

Table 49: List of AT Commands

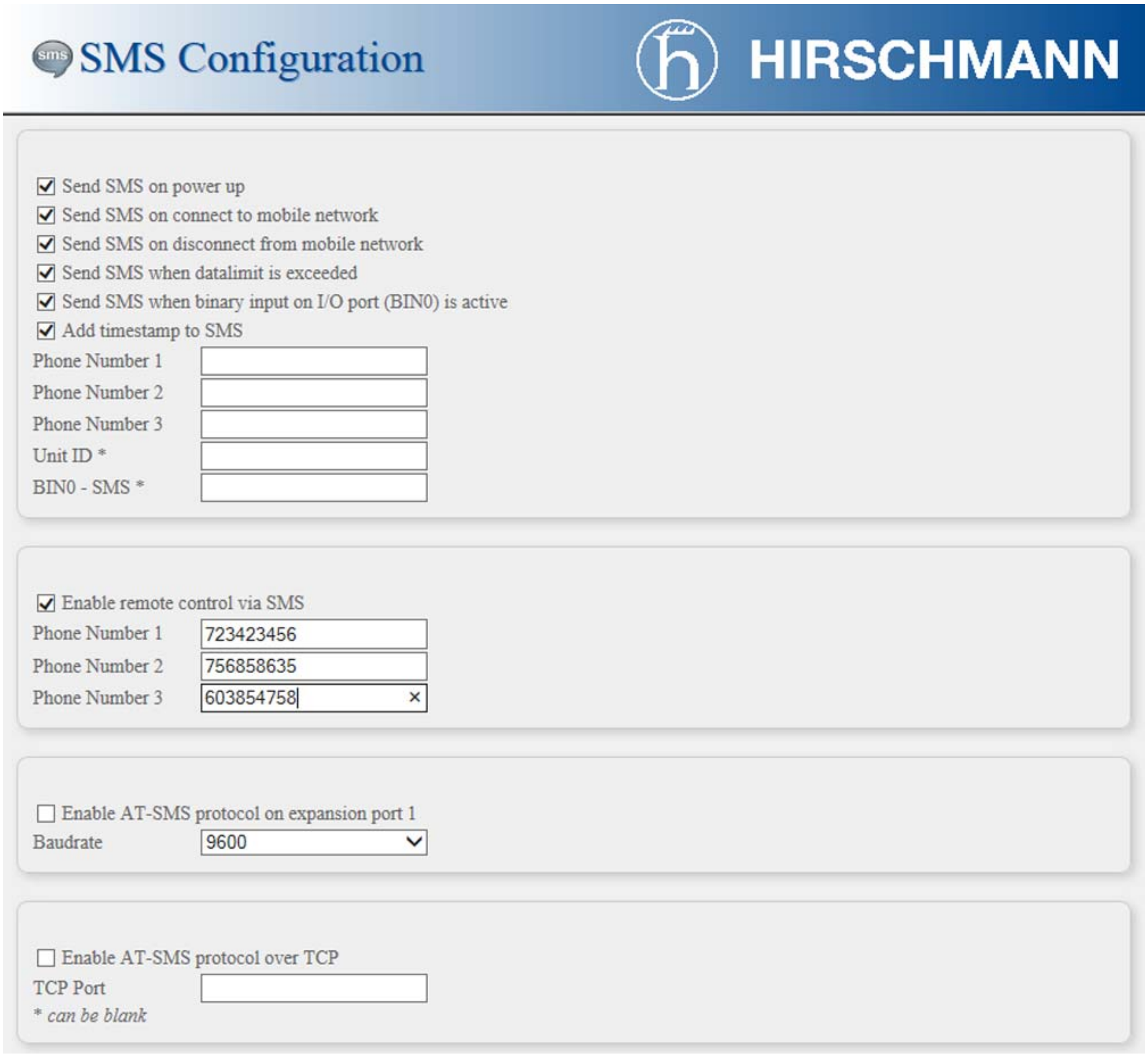
■ Example 1:

SMS sending configuration.

After powering up the router, the phone with the number entered in the dialog receives an SMS in the following form:
Router (Unit ID) has been powered up. Signal strength –xx dBm.

After connecting to mobile network, the phone with the number entered in the dialog receives an SMS in the following form:
Router (Unit ID) has established a connection to a mobile network. IP address xxx.xxx.xxx.xxx

After disconnecting from the mobile network, the phone with the number entered in the dialog receives an SMS in the following form:
Router (Unit ID) has lost connection to the mobile network. IP address xxx.xxx.xxx.xxx



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

Phone Number 1	
Phone Number 2	
Phone Number 3	
Unit ID *	
BIN0 - SMS *	

☑ Enable remote control via SMS

Phone Number 1	723423456
Phone Number 2	756858635
Phone Number 3	603854758

□ Enable AT-SMS protocol on expansion port 1

Baudrate	9600

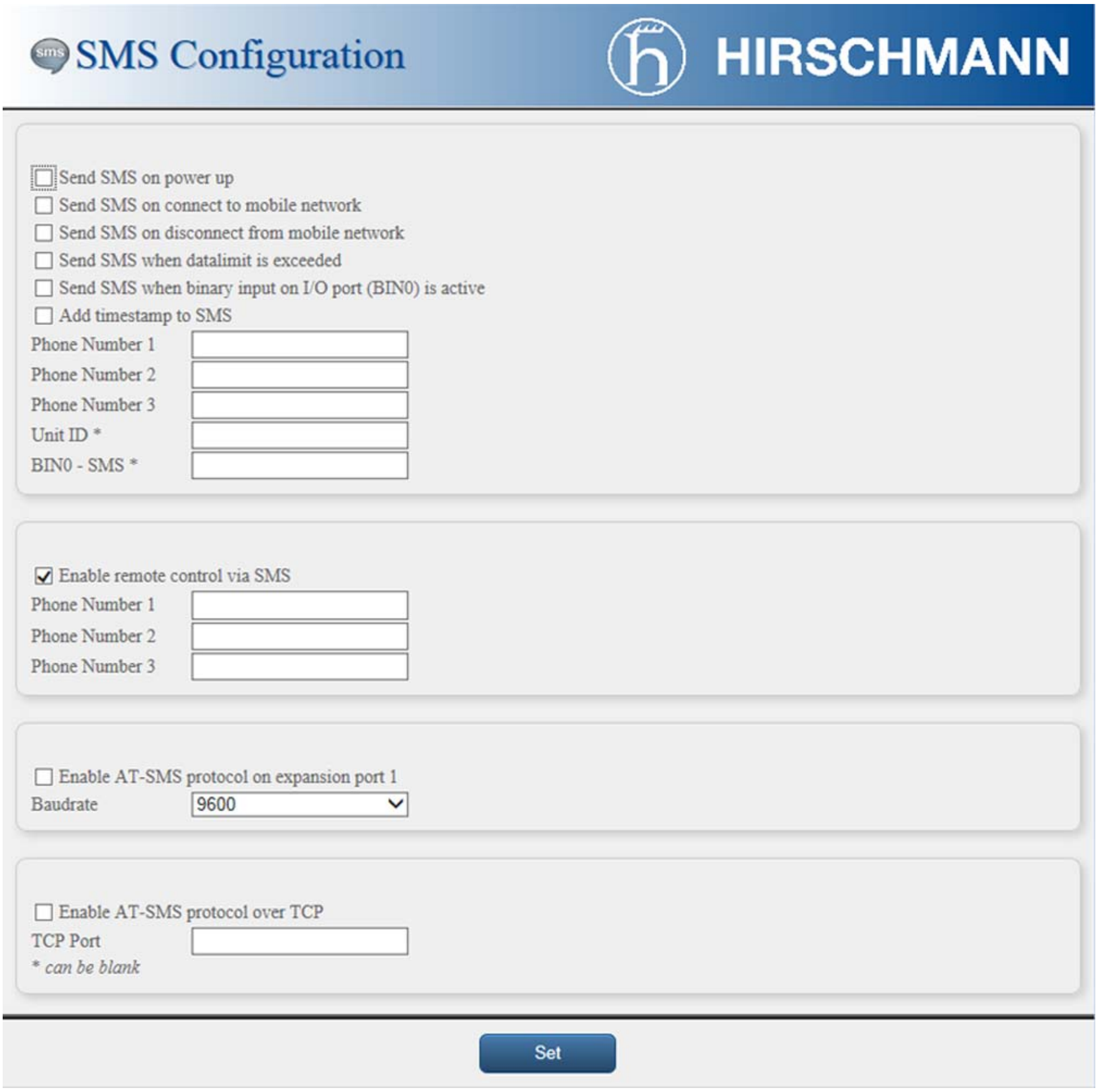
□ Enable AT-SMS protocol over TCP

TCP Port	

** can be blank*

Figure 52: Example 1 – SMS configuration

- **Example 2:**
  Control the router using an SMS from any phone number.



SMS Configuration

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

Phone Number 1
Phone Number 2
Phone Number 3
Unit ID *
BIN0 - 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 over TCP

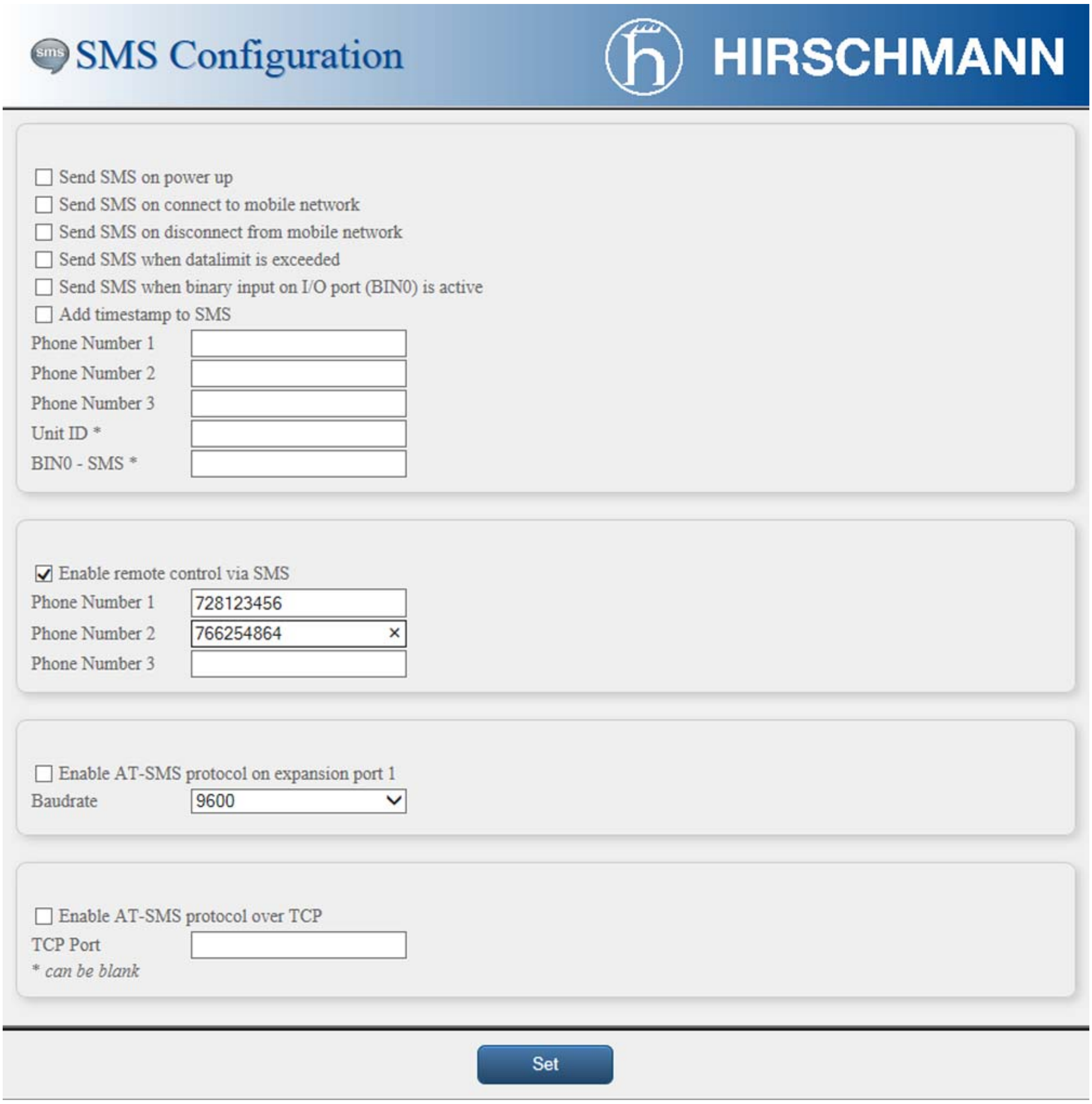
TCP Port

** can be blank*

Figure 53: Example 2 – SMS configuration

- **Example 3:**

  Control the router using an SMS from 2 phone numbers.



SMS Configuration

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

Phone Number 1	
Phone Number 2	
Phone Number 3	
Unit ID *	
BIN0 - 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 over TCP

TCP Port	

** can be blank*

Figure 54: Example 3 – SMS configuration

USB Port Configuration

You can use a USB to RS-232 converter to send data out of the serial port from the Ethernet network in the same manner as the RS-232 expansion port function. To specify the values for the USB port parameters, click "USB Port" in the "Configuration" section of the main menu. The following tables describe the parameters available in the dialog.

Parameter	Description
Baudrate	Specifies the applied communication speed.
Data Bits	Specifies the data Bits Number of data bits.
Parity	Specifies the control parity bit• none – will be sent without parity• even – will be sent with even parity• odd – will be sent with odd parity
Stop Bits	Specifies the number of stop bits.
Split Timeout	Specifies the time, in milliseconds, to rupture reports. If the gap between consecutive characters exceeds the specifies parameter, the router sends any buffered characters over the Ethernet port.
Protocol	Specifies the communications protocol:• TCP – communication using a linked protocol TCP• UDP – communication using a unlinked protocol UDP
Mode	Specifies the mode of connection:• TCP server – router listens to incoming requests about TCP connection• TCP client – router connects to a TCP server on the specified IP address and TCP port
Server Address	Specifies the server address. When you configure the router as a TCP client, enter the Server IP address.
TCP Port	Specifies the TCP/UDP port used for communications. The router uses the value for both the server and client modes.
Inactivity Timeout	Specifies the time period after which the TCP/UDP connection is interrupted in case of inactivity.

Table 50: USB port configuration

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

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

Parameter	Description
Keepalive Time	Specifies the time after which the router verifies the connection.
Keepalive Interval	Specifies the length of time that the router waits on an answer.
Keepalive Probes	Specifies the number of tests that the router performs.

Table 51: USB PORT configuration 2

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

CD	Description
Activated	The TCP connection is enabled.
Inactive	The TCP connection is disabled.

Table 52: CD signal description

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

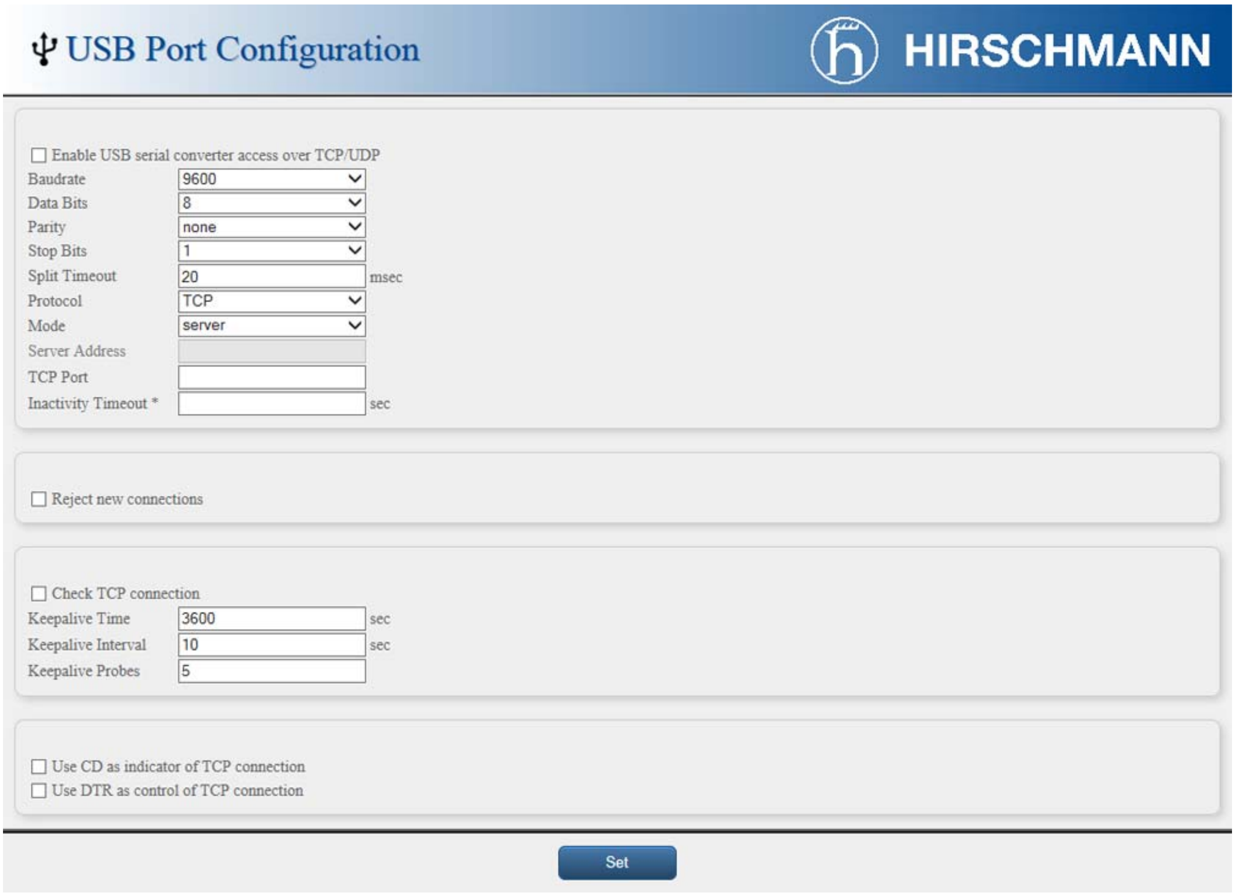
Parameter	Server Description	Client Description
Activated	The router allows the establishment of TCP connections.	The router initiates a TCP connection
Inactive	The router denies the establishment of TCP connections.	The router terminates the TCP connection.

Table 53: DTR signal description

The router supports the following USB/RS232 converters:

- FTDI
- Prolific PL2303
- Silicon Laboratories CP210×

The changes in the dialog apply after clicking the "Set" button.



□ 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		
Inactivity Timeout *		sec

□ Reject new connections

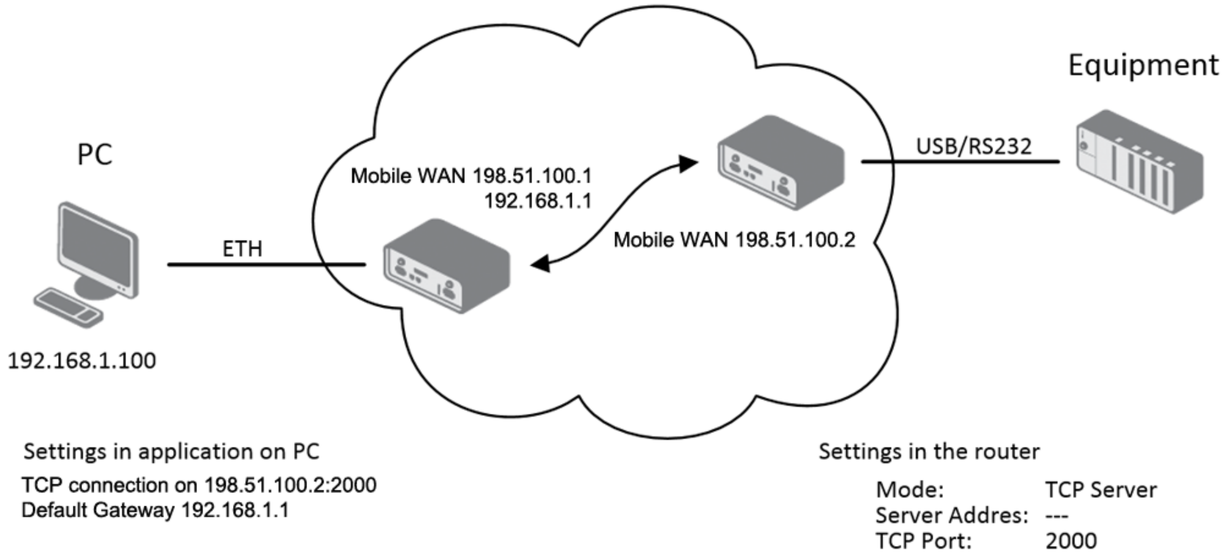
□ Check TCP connection

Keepalive Time	3600	sec
Keepalive Interval	10	sec
Keepalive Probes	5	

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

Figure 55: USB configuration dialog

Examples of the USB port configurations:



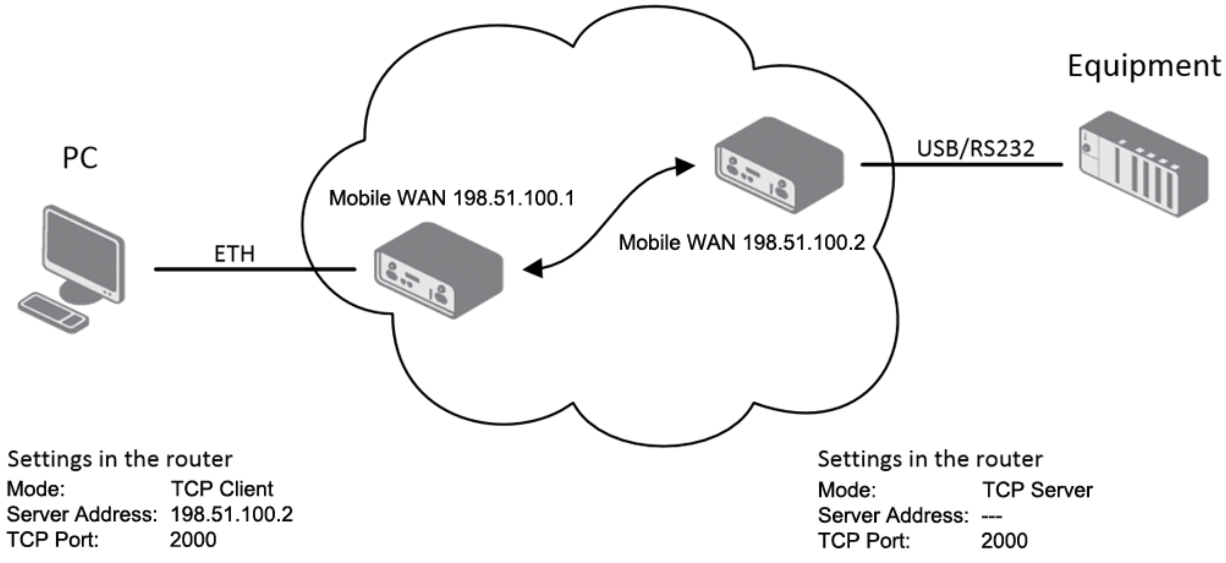
Settings in application on PC

TCP connection on 198.51.100.2:2000
Default Gateway 192.168.1.1

Settings in the router

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

Figure 56: Example 1 – USB port configuration



Settings in the router

Mode:	TCP Client
Server Address:	198.51.100.2
TCP Port:	2000

Settings in the router

Mode:	TCP Server
Server Address:	---
TCP Port:	2000

Figure 57: Example 2 – USB port configuration

■ Automatic update

To specify automatic configuration and firmware updates, use the "Automatic update" dialog in the "Configuration" section of the main menu. The dialog allows the router to automatically download the configuration and the newest firmware from a server. To prevent possible unwanted manipulation of the files, the router verifies that the downloaded file is in the tar.gz format. Then the router verifies the type of architecture and that each file in the archive is a tar.gz file.

If you mark the "Enable automatic update of configuration" check box, then the router automatically downloads the configuration files from the server.

If you mark the "Enable automatic update of firmware" check box, then the router automatically downloads the firmware files from the server.

Note: The router displays the link to the server as an HTTPS connection, but the router performs the automatic configuration and firmware update without first verifying the certificate of the server. Downloading files from a server without a verification process leaves the network open for an attack.

Parameter	Description
Source	Specifies the location of the firmware and configuration file: ▶ HTTP(S)/FTP(S) server – the router downloads updates from the Base URL address below. You specify the protocol that the router uses in the address for example: HTTP, HTTPS, FTP or FTPS. ▶ USB flash drive – The router finds the current firmware or configuration in the root directory of the connected USB device. ▶ Both – the router searches both sources for the current firmware or configuration.
Base URL	Specifies the base part of the domain or IP address of the server from which the router downloads the configuration or firmware file. Also specifies the communication protocol for example: HTTP, HTTPS, FTP or FTPS.

Table 54: Automatic Update Configuration

Parameter	Description
Unit ID	Specifies the name of configuration and/or firmware file without an extension. If you leave the field blank, then the MAC address of the router is used as the filename where the delimiter colon is used instead of a dot.
Update Hour	Specifies the hour, within the range 1-24, that the router performs the automatic update every day. If you leave the field blank, then the router performs the automatic update five minutes after boot up and every 24 hours thereafter. If router detects that the configuration file is different from the running configuration, then the router downloads the file from the server and reboot automatically which loads the new configuration file.

Table 54: Automatic Update Configuration

The name of configuration file consists of the Base URL parameter, the MAC address of eth0 interface, and a cfg extension. The router adds the MAC address and cfg extension automatically. The Unit ID parameter allows the user to specify the name of the downloaded file. This means that if you enter the parameter, the router uses the Unit ID instead of the MAC address.

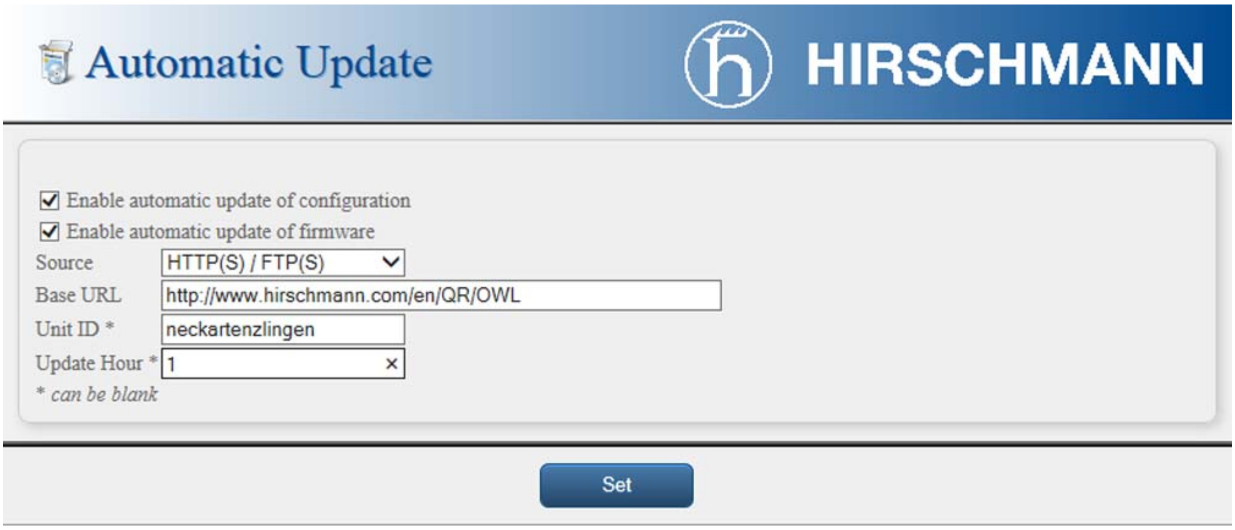
The name of the firmware file consists of Base URL parameter, router type and bin extension.

Note: The router requires a .bin file and a .ver file to be uploaded to the HTTP(S)/FTP(S) server. If you only have the .bin file uploaded and the HTTP server sends a 200 OK answer, instead of expected 404 Not Found, then the device attempts to download the nonexistent .ver file. The router can attempt to download the .bin file over and over again.

■ Example 1:

The router checks whether a new firmware and configuration file is available every day at 1:00 in the morning. The Unit ID parameter is specified.

- Firmware: http://www.hirschmann.com/en/QR/OWL/OWL-LTE.bin
- Configuration file: http://www.hirschmann.com/en/QR/OWL/neckartenzlingen.cfg



Automatic Update

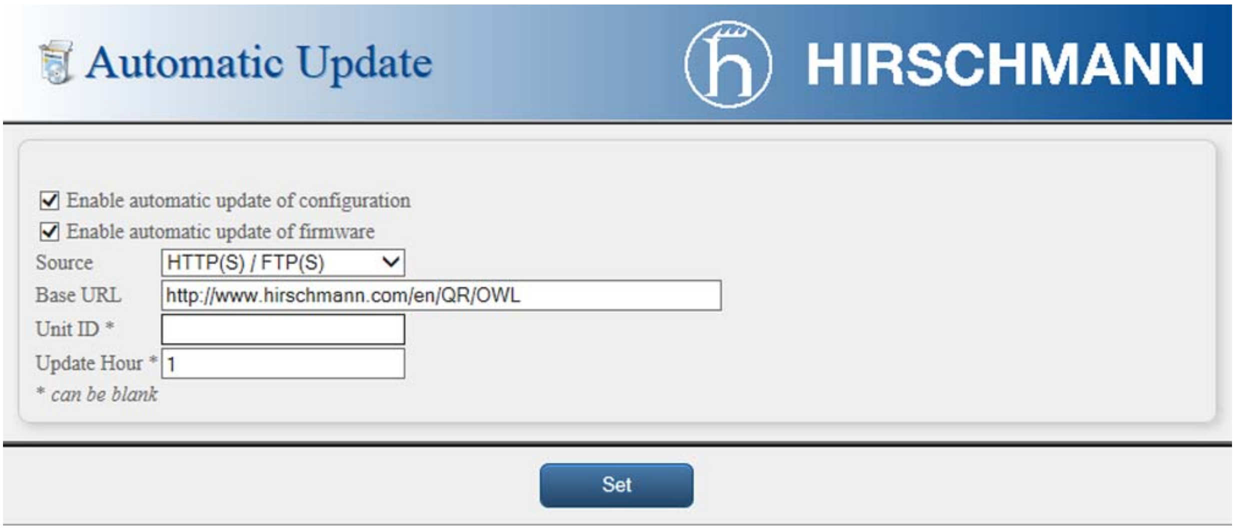
☑ Enable automatic update of configuration
☑ Enable automatic update of firmware

Source	HTTP(S) / FTP(S)
Base URL	http://www.hirschmann.com/en/QR/OWL
Unit ID *	neckartenzlingen
Update Hour *	1

** can be blank*

Figure 58: Automatic Update Example 1

- **Example 2:**
  The router checks whether a new firmware and configuration file is available every day at 1:00 in the morning. The router has MAC address 00:11:22:33:44:55.
  - ▶ Firmware: http://www.hirschmann.com/en/QR/OWL/OWL-LTE.bin
  - ▶ Configuration file: http://www.hirschmann.com/en/QR/OWL/00.11.22.33.44.55.cfg



Automatic Update

☑ Enable automatic update of configuration
☑ Enable automatic update of firmware

Source	HTTP(S) / FTP(S)
Base URL	http://www.hirschmann.com/en/QR/OWL
Unit ID *	
Update Hour *	1

** can be blank*

Figure 59: Automatic Update Example 2

1.4 Administration

1.4.1 Users

This configuration function is only available for users assigned the admin role.

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

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

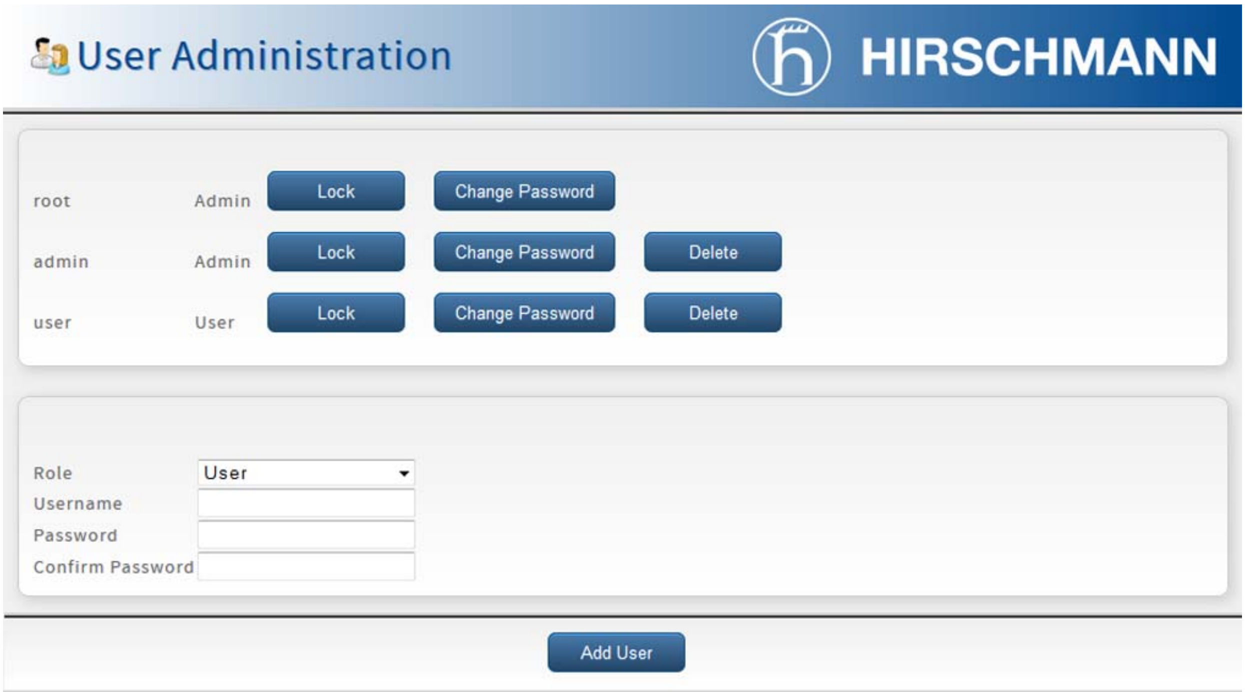
Table 55: Users overview

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

In the second frame you can add a new user. You can find detail descriptions to the parameters the table below.

Parameter	Description
Role	Specifies the type of user account ▶ `User` - user with basic permissions ▶ `Admin` - user with full permissions
Username	Specifies the name of the user allowed to log in the device.
Password	Specifies the password for the corresponding user.
Confirm Password	Confirms the password you specified above

Table 56: Add User



root	Admin	Lock	Change Password	
admin	Admin	Lock	Change Password	Delete
user	User	Lock	Change Password	Delete

Role: User
Username
Password
Confirm Password

Figure 60: Users

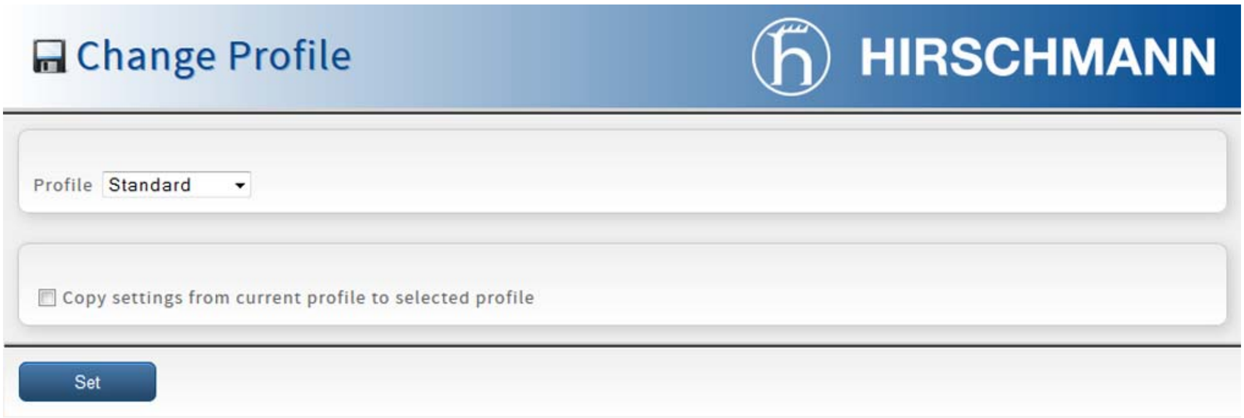
1.4.2 Change Profile

Using profiles you can change between different router configurations. You can change the profile using an SMS message or the GUI interface of the router.

Use the "Change Profile" dialog in the "Administration" section of the main menu to exchange the profiles. The selected profile is applied after clicking the "Set" button. Changes take effect after you reboot the router. The router allows you to specify 4 different profiles:

- `Standard`
- `Alternative 1`
- `Alternative 2`
- `Alternative 3`

It is also possible to copy the current configuration to a profile, using the "Copy settings from the current profile" check box.



Profile Standard

□ Copy settings from current profile to selected profile

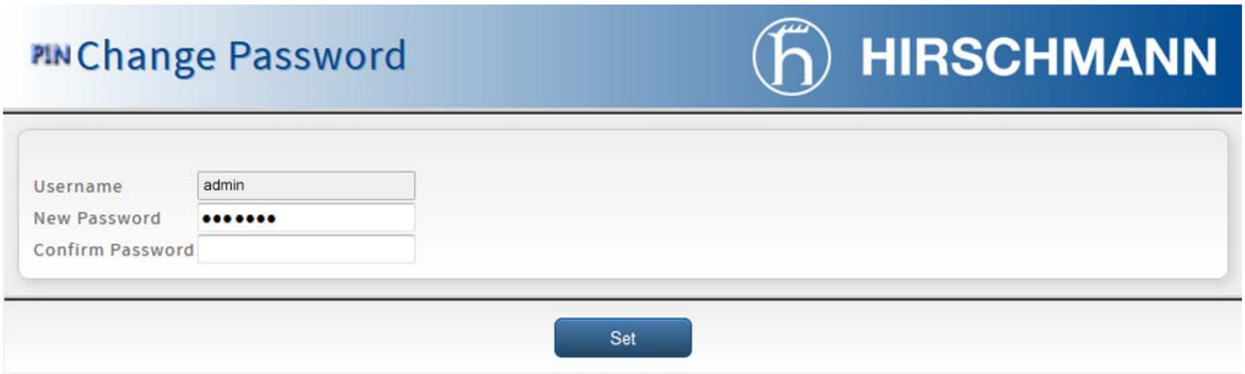
Figure 61: Change Profile

1.4.3 Change Password

Use the "Change Password" dialog in the "Administration" section of the main menu for changing your password used to log on the device. Enter the new password in the "New Password" field, confirm the password using the "Confirm Password" field, and press the "Set" button.

Note: The default password of the router is `private` for the `admin` user. To maintain the security of your network change the default password.

You can not enable remote access to the router for example, in NAT, until you change the password.



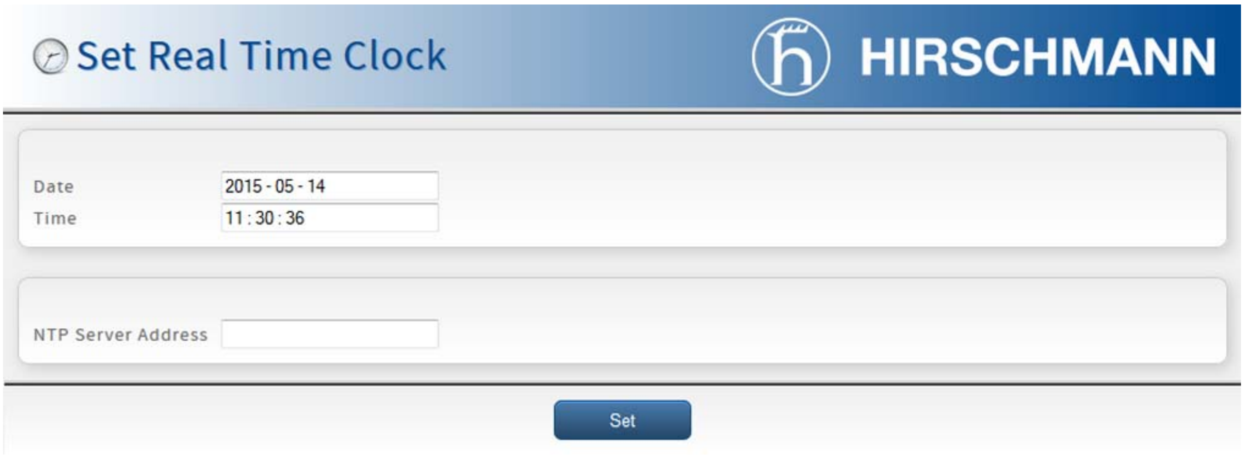
Username: admin
New Password: •••••••
Confirm Password:

Figure 62: Change Password

1.4.4 Set Real Time Clock

This configuration function is only available for users with the admin role.

You can set the internal clock directly using the "Set Real Time Clock" dialog in the "Administration" section of in the main menu. You can set the "Date" and "Time" manually. When entering the values manually use the format yyyy-mm-dd as seen in the figure below. You can also adjust the clock using the specified NTP server. After you enter the appropriate values, click the "Set" button.



Set Real Time Clock

Date 2015 - 05 - 14

Time 11 : 30 : 36

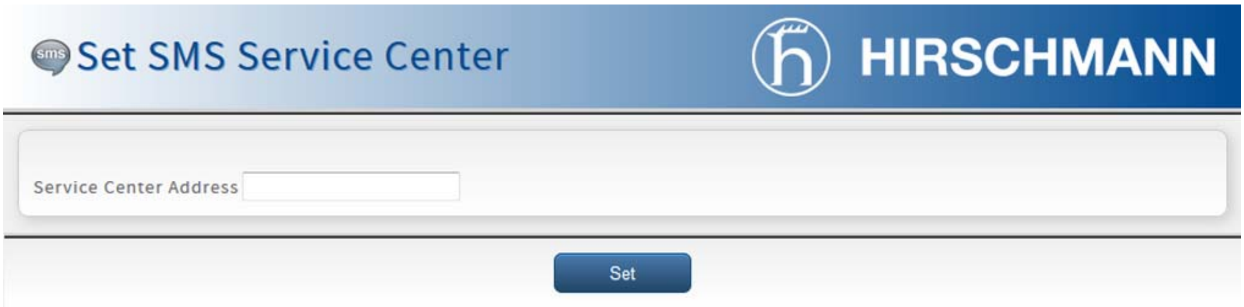
NTP Server Address

Figure 63: Set Real Time Clock

1.4.5 Set SMS Service Center

This configuration function is only available for users with the admin role.

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



Set SMS Service Center

Service Center Address

Figure 64: Set SMS service center address

1.4.6 Unlock SIM Card

This configuration function is only available for users with the admin role.

If your SIM card is protected using a 4 - 8 digit PIN number, open the "Unlock SIM Card" dialog in the "Administration" section of the main menu and enter the PIN number in the "SIM PIN" field, then click the "Set" button. The router requires you to enter the PIN code each time that you power up the SIM card.

Note: The SIM card is blocked after 3 failed attempts to enter the PIN code. Contact your SIM card carrier if it has been blocked.

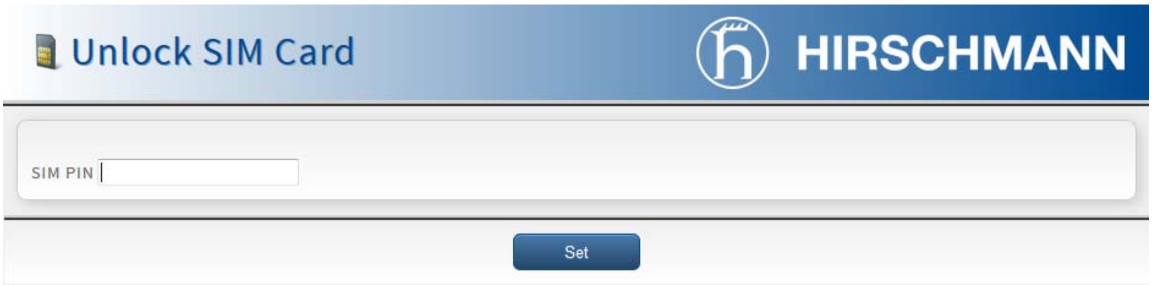
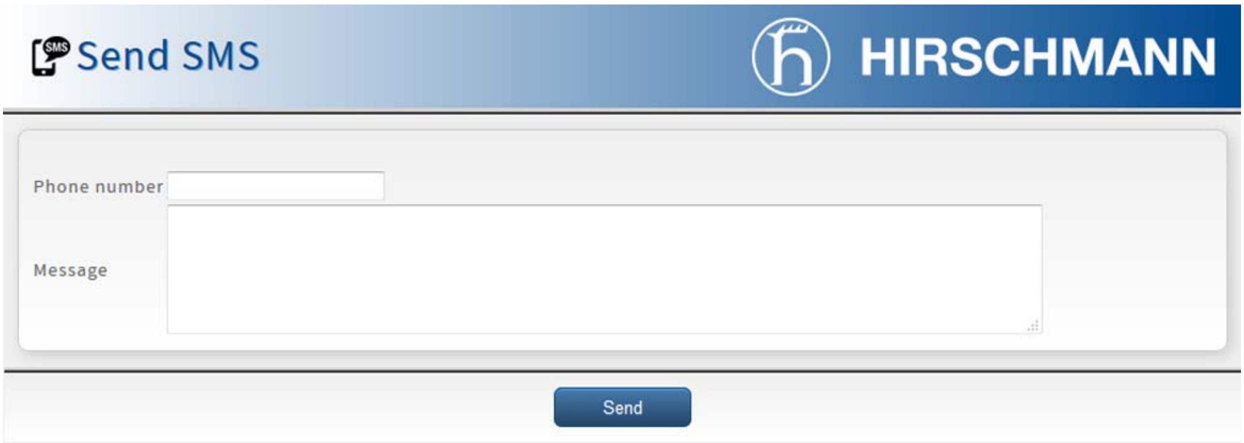


Figure 65: Unlock SIM Card

1.4.7 Send SMS

This configuration function is only available for users with the admin role.

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



Send SMS

Phone number

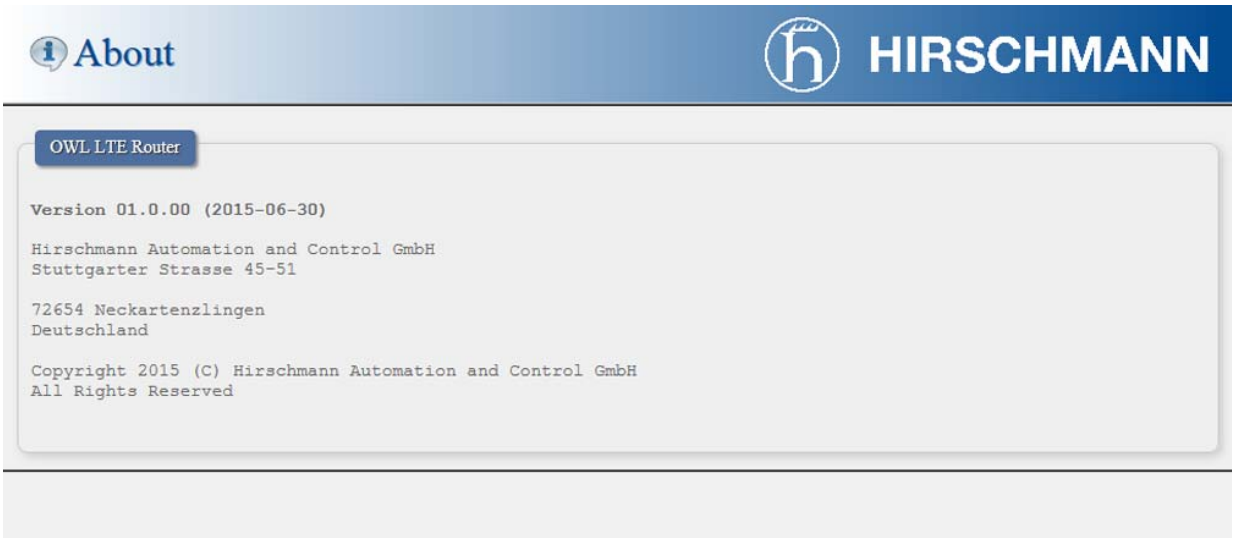
Message

Figure 66: Send SMS

1.5 Help

1.5.1 About

The "About" dialog displays information about the firmware version and basic information about the Hirschmann Automation and Control GmbH.

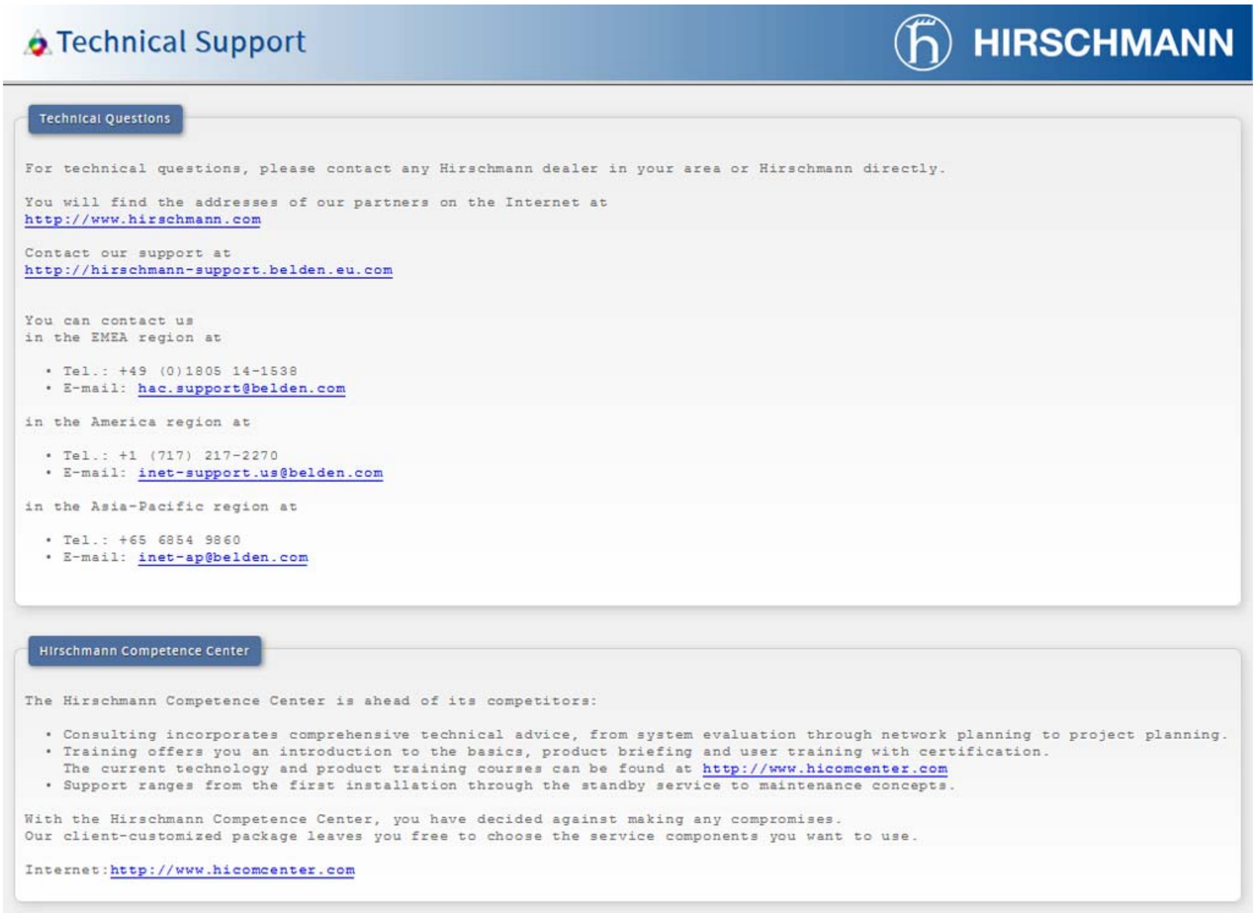


```
Version 01.0.00 (2015-06-30)

Hirschmann Automation and Control GmbH
Stuttgarter Strasse 45-51

72654 Neckartenzlingen
Deutschland

Copyright 2015 (C) Hirschmann Automation and Control GmbH
All Rights Reserved
```

Figure 67: About

1.5.2 Technical Support

You can find basic information about the Hirschmann Automation and Control GmbH technical support in the "Technical Support" dialog. You can also find information about the Hirschmann Automation and Control GmbH Competence Center.



Technical Support

Technical Questions

For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly.

You will find the addresses of our partners on the Internet at
http://www.hirschmann.com

Contact our support at
http://hirschmann-support.belden.eu.com

You can contact us
in the EMEA region at

- Tel.: +49 (0)1805 14-1538
- E-mail: hac.support@belden.com

in the America region at

- Tel.: +1 (717) 217-2270
- E-mail: inet-support.us@belden.com

in the Asia-Pacific region at

- Tel.: +65 6854 9860
- E-mail: inet-ap@belden.com

Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- Training offers you an introduction to the basics, product briefing and user training with certification.
  The current technology and product training courses can be found at http://www.hicomcenter.com
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you have decided against making any compromises.
Our client-customized package leaves you free to choose the service components you want to use.

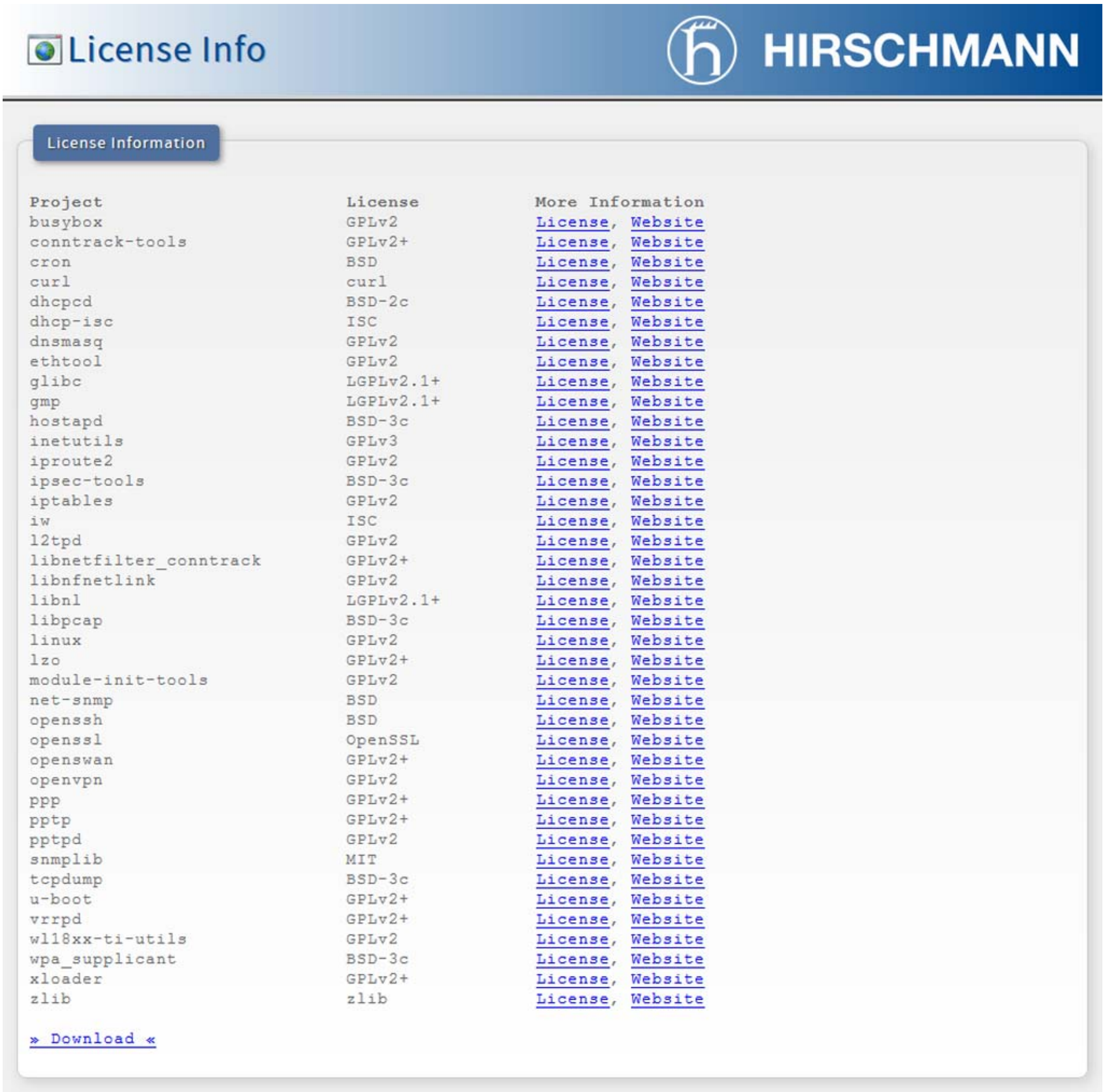
Internet:http://www.hicomcenter.com

Figure 68: Technical Support

1.5.3 License Info

The "License Info" dialog lists license information about every project relating to the router. There are 3 columns in this dialog:

- "Project" – name of the project
- "License" – type of the license
- "More Information" – the "License" and a link to "Website" of the project



Project	License	More Information
busybox	GPLv2	License, Website
conntrack-tools	GPLv2+	License, Website
cron	BSD	License, Website
curl	curl	License, Website
dhcpcd	BSD-2c	License, Website
dhcp-isc	ISC	License, Website
dnsmasq	GPLv2	License, Website
ethtool	GPLv2	License, Website
glibc	LGPLv2.1+	License, Website
gmp	LGPLv2.1+	License, Website
hostapd	BSD-3c	License, Website
inetutils	GPLv3	License, Website
iproute2	GPLv2	License, Website
ipsec-tools	BSD-3c	License, Website
iptables	GPLv2	License, Website
iw	ISC	License, Website
l2tpd	GPLv2	License, Website
libnetfilter_conntrack	GPLv2+	License, Website
libnfnetlink	GPLv2	License, Website
libnl	LGPLv2.1+	License, Website
libpcap	BSD-3c	License, Website
linux	GPLv2	License, Website
lzo	GPLv2+	License, Website
module-init-tools	GPLv2	License, Website
net-snmp	BSD	License, Website
openssh	BSD	License, Website
openssl	OpenSSL	License, Website
openswan	GPLv2+	License, Website
openvpn	GPLv2	License, Website
ppp	GPLv2+	License, Website
pptp	GPLv2+	License, Website
pptpd	GPLv2	License, Website
snmplib	MIT	License, Website
tcpdump	BSD-3c	License, Website
u-boot	GPLv2+	License, Website
vrrpd	GPLv2+	License, Website
wl18xx-ti-utils	GPLv2	License, Website
wpa_supplicant	BSD-3c	License, Website
xloader	GPLv2+	License, Website
zlib	zlib	License, Website

» Download «

Figure 69: License Info

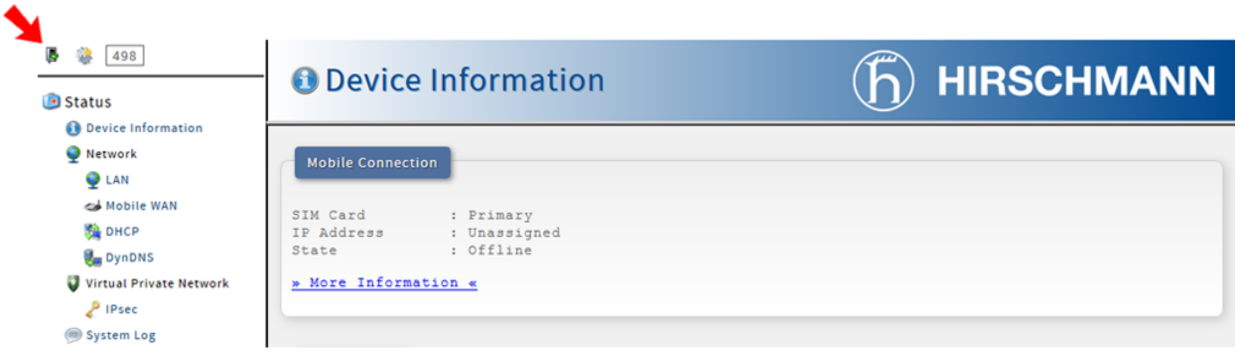
1.6 Icon Bar

This chapter describes meaning of each icon on the bar located in the upper left corner of the dialog.

1.6.1 Logout

The first icon on the bar, the open door with the green arrow, allows you to logout of the router.

When you click on the icon, the router discards any unsaved changes to the configuration.



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

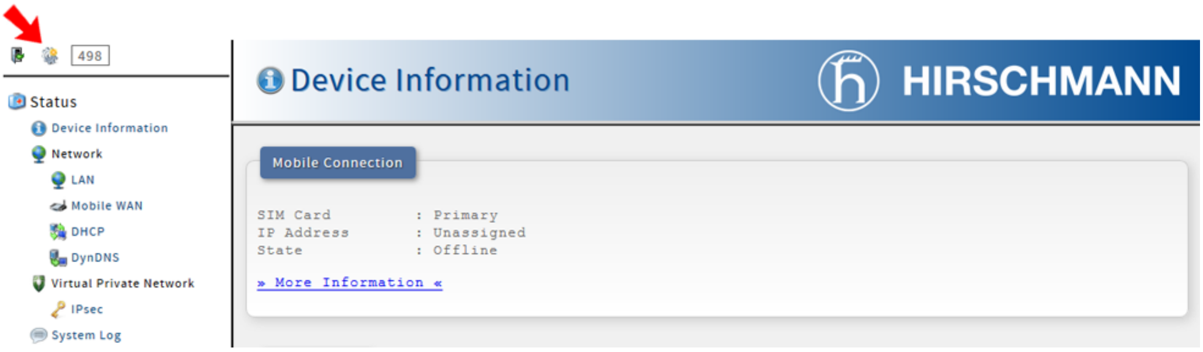
Figure 70: Logout

1.6.2 Reboot

This configuration function is only available for users with the admin role.

The second icon on the icon bar, the gearwheel, allows you to reboot the router.

When you click on the icon, the router discards any unsaved changes to the configuration.



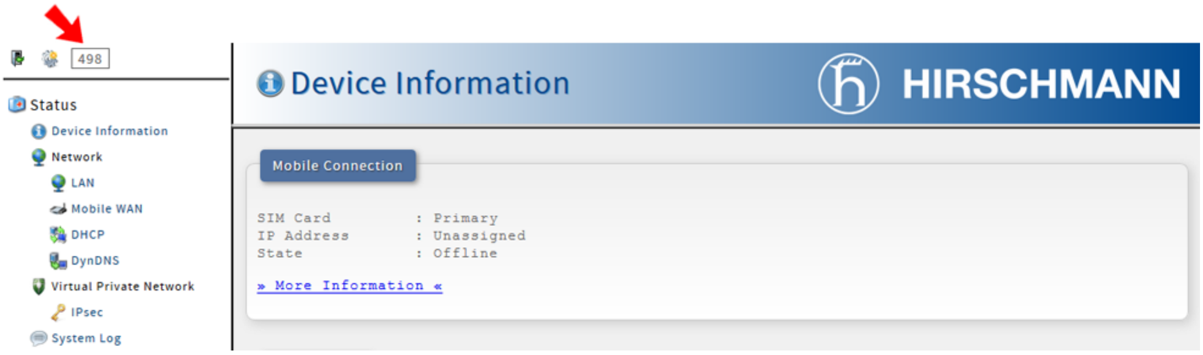
```
SIM Card        : Primary
IP Address      : Unassigned
State           : Offline
```

» More Information «

Figure 71: Reboot

1.6.3 Timeout Counter

The last icon, the number in a grey field, displays time remaining until the router automatically logs out an inactive user. The counter begins at `500`s. The counter restarts every time you open a different dialog.



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

» More Information «

Figure 72: Timeout Counter

2 OpenVPN protocol

The OpenVPN (Open Virtual Private Network) program is a means of interconnecting several computers through an untrusted public network. It is possible for connected computers to communicate with each other as if they were connected in a single closed private network. The closed private network is consequently trusted. Using the client-server architecture, The OpenVPN program is capable of establishing a direct connection between computers behind NAT (Network Address Translation) without any need to configure NAT. The OpenVPN program has a few ways to authenticate clients for example, a pre-shared key, an X.509 certificate, or a username and password.

The OpenVPN program uses the officially assigned UDP port 1194, which is applied as the default in newer versions. The OpenVPN program offers 2 types of network interfaces, the Universal TUN and the TAP driver. The drivers allow you to create an IP tunnel (TUN) on layer 3 of the ISO/OSI or an Ethernet TAP on layer 2. The Universal TUN and the Ethernet TAP are able to transmit any type of data. The OpenVPN program uses the common network protocols (TCP and UDP) and thus creates an alternative to the IPsec protocol.

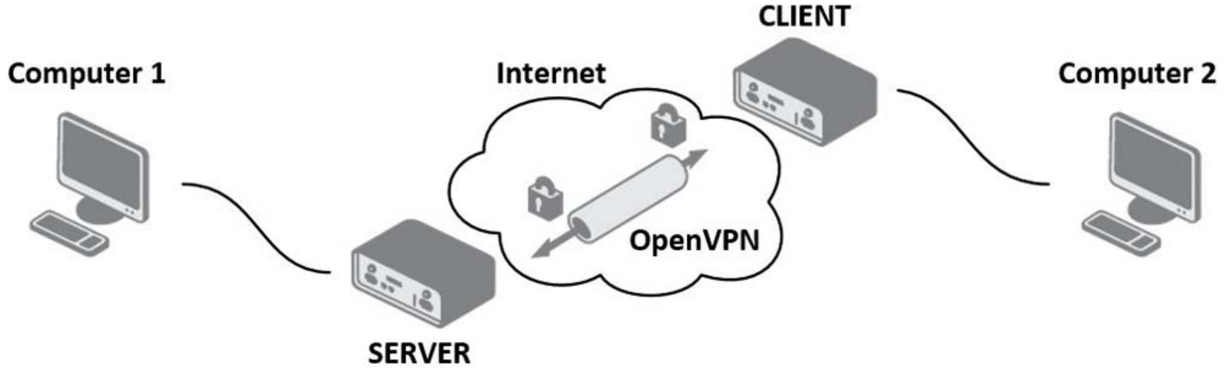


Figure 73: Basic scheme

2.1 Restrictions in Hirschmann routers

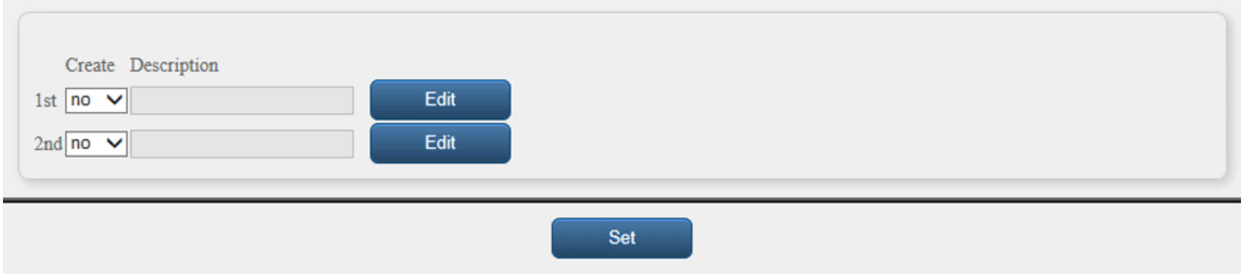
- The router allows you to create only 2 OpenVPN tunnels simultaneously.
- The router only supports a TUN adapter.
- The router can not be used as a multi-client server.

2.2 Configuration of an OpenVPN tunnel

The OpenVPN tunnel function allows you to protect the connection of 2 LAN networks so that the networks resemble a single homogenous LAN. You can configure an OpenVPN tunnel by clicking on `OpenVPN` in the menu tree of the graphical user interface. The `OpenVPN Tunnels Configuration` dialog contains 2 rows. You use each row to configure 1 OpenVPN tunnel. The following table contains the description of the individual parameters:

Item	Description
Create	Enables the individual VPN tunnels.
Description	Displays the name or description of the tunnel, specified in the second configuration dialog. The information displayed in this field is specified in the second configuration dialog.
Edit	Opens the second of 2 `OpenVPN Tunnel Configuration` dialogs. You use this dialog to specify the parameters of the tunnel.

Table 57: Overview of OpenVPN tunnels



	Create	Description	
1st	no		Edit
2nd	no		Edit

Figure 74: Overview of OpenVPN tunnels

After clicking the `Edit` button for a tunnel, the router opens the second of 2 `OpenVPN Tunnel Configuration` dialogs. The dialog contains a form that you use to set specific OpenVPN tunnel parameters. The following table contains the description of the individual parameters:

Item	Description
Description	Specifies the description or name of the VPN tunnel.
Protocol	Specifies the communication protocol that the tunnel uses: ▶ UDP – The OpenVPN uses UDP to communicate. ▶ TCP server – The OpenVPN uses TCP to communicate in server mode ▶ TCP client – The OpenVPN uses TCP to communicate in client mode
UDP/TCP port	Specifies the port for the relevant UDP or TCP protocol.
Remote IP Address	Specifies the IP address for the opposite side of the tunnel. You can use a domain name.
Remote Subnet	Specifies the IP address of a network behind the opposite side of the tunnel.
Remote Subnet Mask	Specifies the subnet mask of a network behind the opposite side of the tunnel.
Redirect Gateway	Specifies whether the router uses a gateway to redirect the Ethernet data stream.
Local Interface IP Address	Specifies the IP address of a local interface.
Remote Interface IP Address	Specifies the IP address of the interface on opposite side of the tunnel.
Ping Interval	Specifies the time interval between consecutive messages. The router sends a ICMP ping message to opposite side of the tunnel to verify the existence of the tunnel.
Ping Timeout	Specifies the time interval that the router waits for a message sent by the opposite side. For proper verification of the OpenVPN tunnel, set the Ping Timeout to a value greater than Ping Interval.
Renegotiate Interval	Specifies the renegotiation period used for reauthorization of the OpenVPN tunnel. After the specified time period, the router changes the tunnel encryption to verify the continues security of the tunnel. The prerequisite for this parameter is that you specify the `Authenticate Mode` value as `username/password` or an `X.509 certificate`.
Max Fragment Size	Specifies the maximum size of a sent packet
Compression	Specifies whether the device compresses the data transmitted. Specify the same value on both sides of the tunnel. ▶ none – no compression is used. ▶ LZO – a lossless compression is used.
NAT Rules	Specifies whether the device applies the NAT rules to the OpenVPN tunnel: ▶ applied – NAT rules are applied to the OpenVPN tunnel ▶ not applied – NAT rules are not applied to the OpenVPN tunnel You specify the NAT rules in the `Security> NAT` dialog.

Table 58: Configuration of OpenVPN tunnel

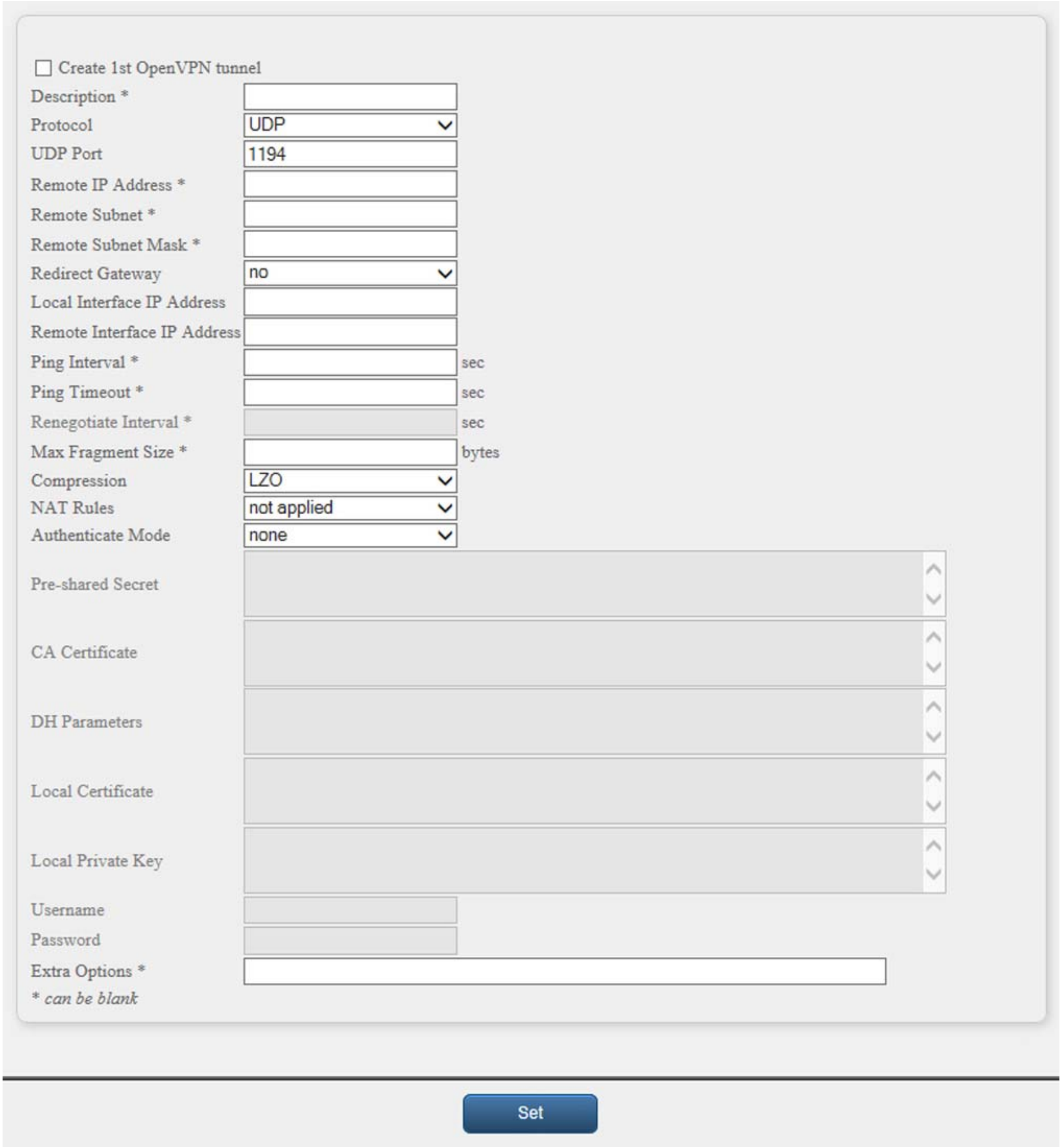
Item	Description
Authenticate Mode	Specifies the authentication mode that the router uses: ▶ none – no authentication is required ▶ Pre-shared secret – specifies the shared key for both sides of the tunnel. ▶ Username/password – enables authentication using a CA Certificate, Username and Password. ▶ X.509 Certificate (multi-client) – enables X.509 authentication in the multi-client mode. ▶ X.509 Certificate (client) – enables X.509 authentication in the client mode. ▶ X.509 Certificate (server) – enables X.509 authentication in the server mode.
Pre-shared Secret	Specifies the pre-shared secret used for authentication. The router uses the pre-shared secret for every authentication mode.
CA Certificate	Specifies the CA Certificate that the router uses for authentication. The prerequisite for this parameter is that you specify the `Authenticate Mode` value as `username/password` or an `X.509 certificate`.
DH Parameters	Specifies the protocol used for the exchange key DH parameters. The prerequisite for this parameter is that you specify the `Authenticate Mode` value as `X.509 cert. (server)`.
Local Certificate	Specifies the local certificate used for authentication. The prerequisite for this parameter is that you specify the `Authenticate Mode` value as an `X.509 certificate`.
Local Private Key	Specifies the local private key used for authentication. The prerequisite for this parameter is that you specify the `Authenticate Mode` value as an `X.509 certificate`.
Username	Specifies the login name of a user. The prerequisite for this parameter is that you specify the `Authenticate Mode` value as `username/password`.
Password	Specifies the login password of a user. The prerequisite for this parameter is that you specify the `Authenticate Mode` value as `username/password`.
Extra Options	Specifies the additional parameters of the OpenVPN tunnel for example, the DHCP options.

Table 58: Configuration of OpenVPN tunnel

The router applies the changes made to the parameters in this dialog after you click the `Set` button.

Tips for working with the configuration form:
- Assign a remote IP address, the server IP address to the CLIENT routers.
- For SERVER routers, we recommend that you leave the Remote IP Address parameter blank.

- If you connect 2 routers, configure a router as a CLIENT and the other as a SERVER.
- We recommend that you set the Ping Interval and the Ping Timeout parameters.



☐ 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 75: OpenVPN tunnel Configuration dialog

2.3 Router on both sides of tunnel

The figure below displays a network where a Hirschmann router is installed on both sides of the OpenVPN tunnel. The IP address of the SIM cards in the routers can be configured as either static or dynamic.

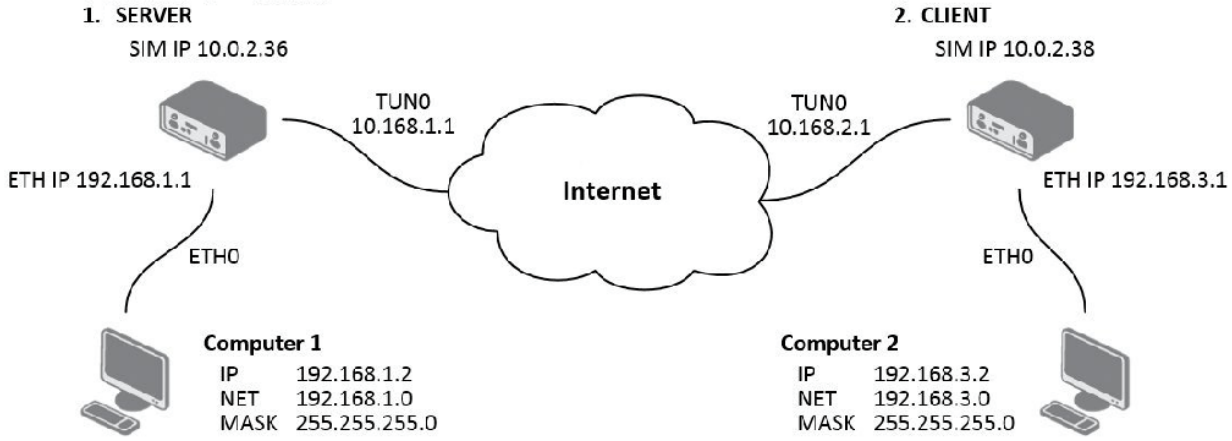


Figure 76: Router on both sides of a tunnel

2.3.1 OpenVPN tunnel without authentication

Enter the following parameters in the configuration of the first router. This router is the SERVER:

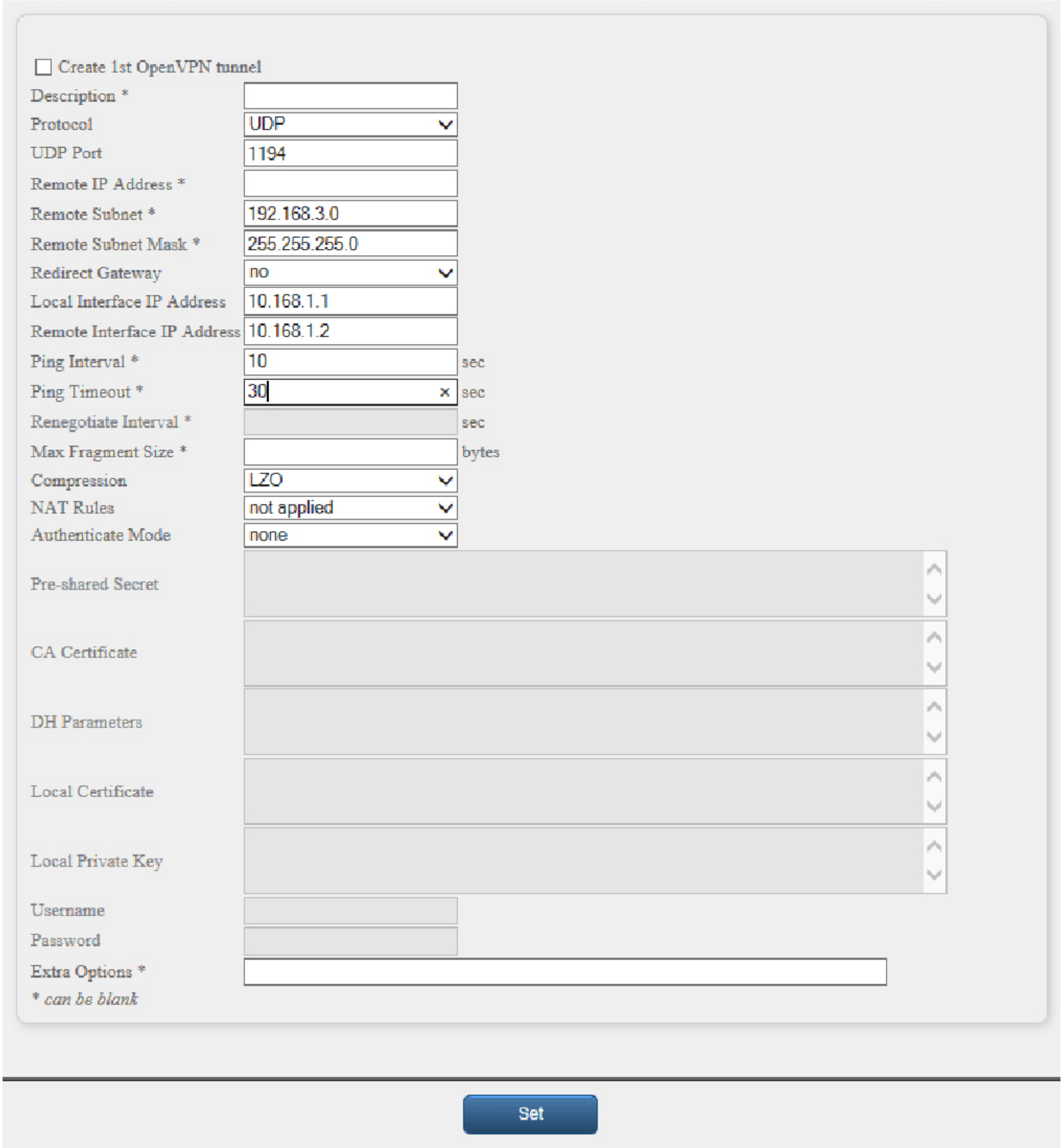
Item	Value
Remote Subnet	192.168.3.0
Remote Subnet Mask	255.255.255.0
Local Interface IP Address	10.168.1.1
Remote Interface IP Address	10.168.1.2

Table 59: Configuration of the first router (no authentication)

Enter the following parameters in the configuration of the second router. This router is the CLIENT:

Item	Value
Remote IP Address	10.0.2.36
Remote Subnet	192.168.1.0
Remote Subnet Mask	255.255.255.0
Local Interface IP Address	10.168.1.2
Remote Interface IP Address	10.168.1.1

Table 60: Configuration of the second router (no authentication)



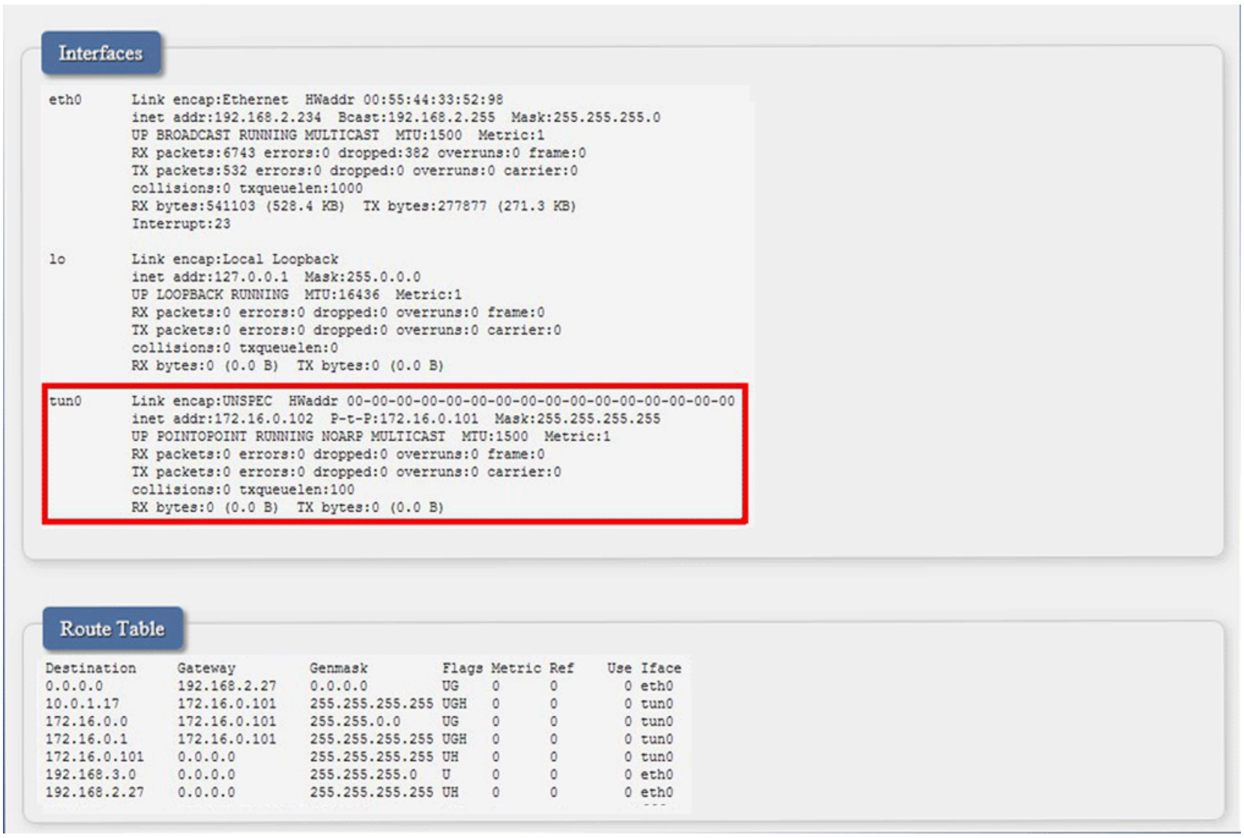
☐ Create 1st OpenVPN tunnel		
Description *		
Protocol	UDP	
UDP Port	1194	
Remote IP Address *		
Remote Subnet *	192.168.3.0	
Remote Subnet Mask *	255.255.255.0	
Redirect Gateway	no	
Local Interface IP Address	10.168.1.1	
Remote Interface IP Address	10.168.1.2	
Ping Interval *	10	sec
Ping Timeout *	30	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 77: Configuration of the first router (no authentication)

Note: The configuration of the second router is similar to the first router. See table 60 on page 124. If you select ”applied” from the NAT Rules drop down menu, then the router applies the rules specified in the Security> NAT dialog to the OpenVPN tunnel.

After establishing an OpenVPN tunnel, the `Network> LAN Status` dialog displays the tun0 interface in the Interface section, and the associated route in the Route Table section.

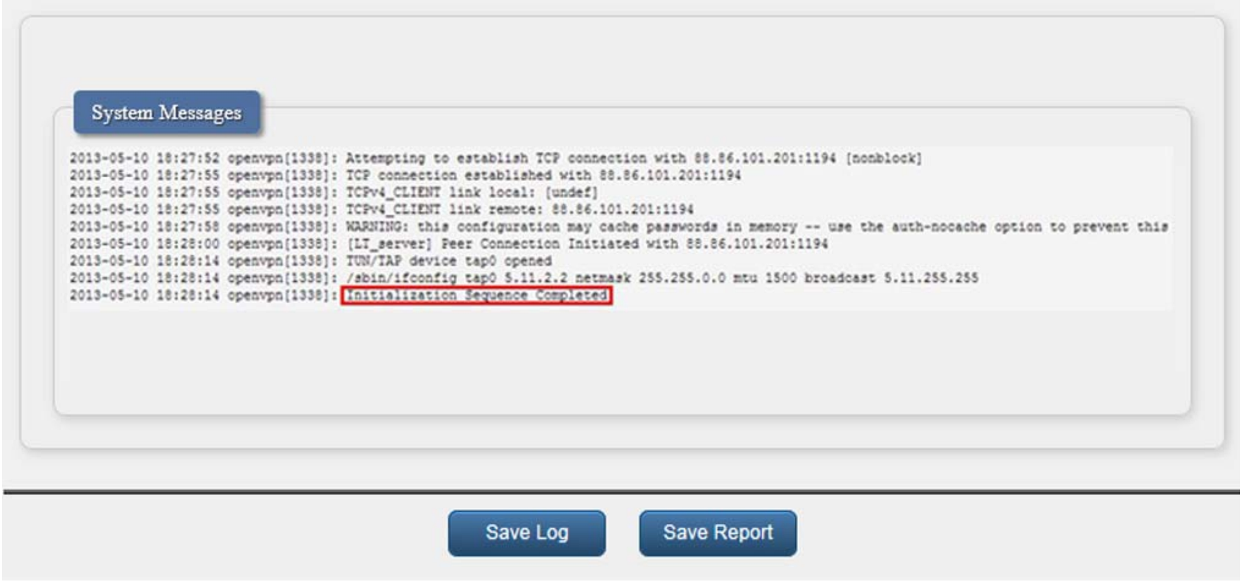


```
eth0      Link encap:Ethernet  HWaddr 00:55:44:33:52:98
          inet addr:192.168.2.234  Bcast:192.168.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6743 errors:0 dropped:382 overruns:0 frame:0
          TX packets:532 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:541103 (528.4 KB)  TX bytes:277877 (271.3 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)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:172.16.0.102  P-t-P:172.16.0.101  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP 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:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.2.27    0.0.0.0         UG    0      0        0 eth0
10.0.1.17       172.16.0.101    255.255.255.255 UGH   0      0        0 tun0
172.16.0.0      172.16.0.101    255.255.0.0     UG    0      0        0 tun0
172.16.0.1      172.16.0.101    255.255.255.255 UGH   0      0        0 tun0
172.16.0.101    0.0.0.0         255.255.255.255 UH    0      0        0 tun0
192.168.3.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.2.27    0.0.0.0         255.255.255.255 UH    0      0        0 eth0
```

Figure 78: Network Status

It is also possible to verify a successful establishment of the OpenVPN tunnel in the system log, click `System Log` in menu tree. After the router establishes an OpenVPN tunnel, the log displays the “Initialization Sequence Completed” entry.



```
2013-05-10 18:27:52 openvpn[1338]: Attempting to establish TCP connection with 88.86.101.201:1194 [nonblock]
2013-05-10 18:27:55 openvpn[1338]: TCP connection established with 88.86.101.201:1194
2013-05-10 18:27:55 openvpn[1338]: TCPv4_CLIENT link local: [undef]
2013-05-10 18:27:55 openvpn[1338]: TCPv4_CLIENT link remote: 88.86.101.201:1194
2013-05-10 18:27:58 openvpn[1338]: WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2013-05-10 18:28:00 openvpn[1338]: [LT_server] Peer Connection Initiated with 88.86.101.201:1194
2013-05-10 18:28:14 openvpn[1338]: TUN/TAP device tap0 opened
2013-05-10 18:28:14 openvpn[1338]: /sbin/ifconfig tap0 5.11.2.2 netmask 255.255.0.0 mtu 1500 broadcast 5.11.255.255
2013-05-10 18:28:14 openvpn[1338]: Initialization Sequence Completed
```

Figure 79: System log

2.3.2 OpenVPN tunnel with pre-shared secret authentication

Enter the following parameters in the configuration of the first router. This router is the SERVER:

Item	Value
Remote Subnet	192.168.3.0
Remote Subnet Mask	255.255.255.0
Local Interface IP Address	10.168.1.1
Remote Interface IP Address	10.168.1.2
Authenticate Mode	pre-shared secret
Pre-shared Secret	shared key for both of routers

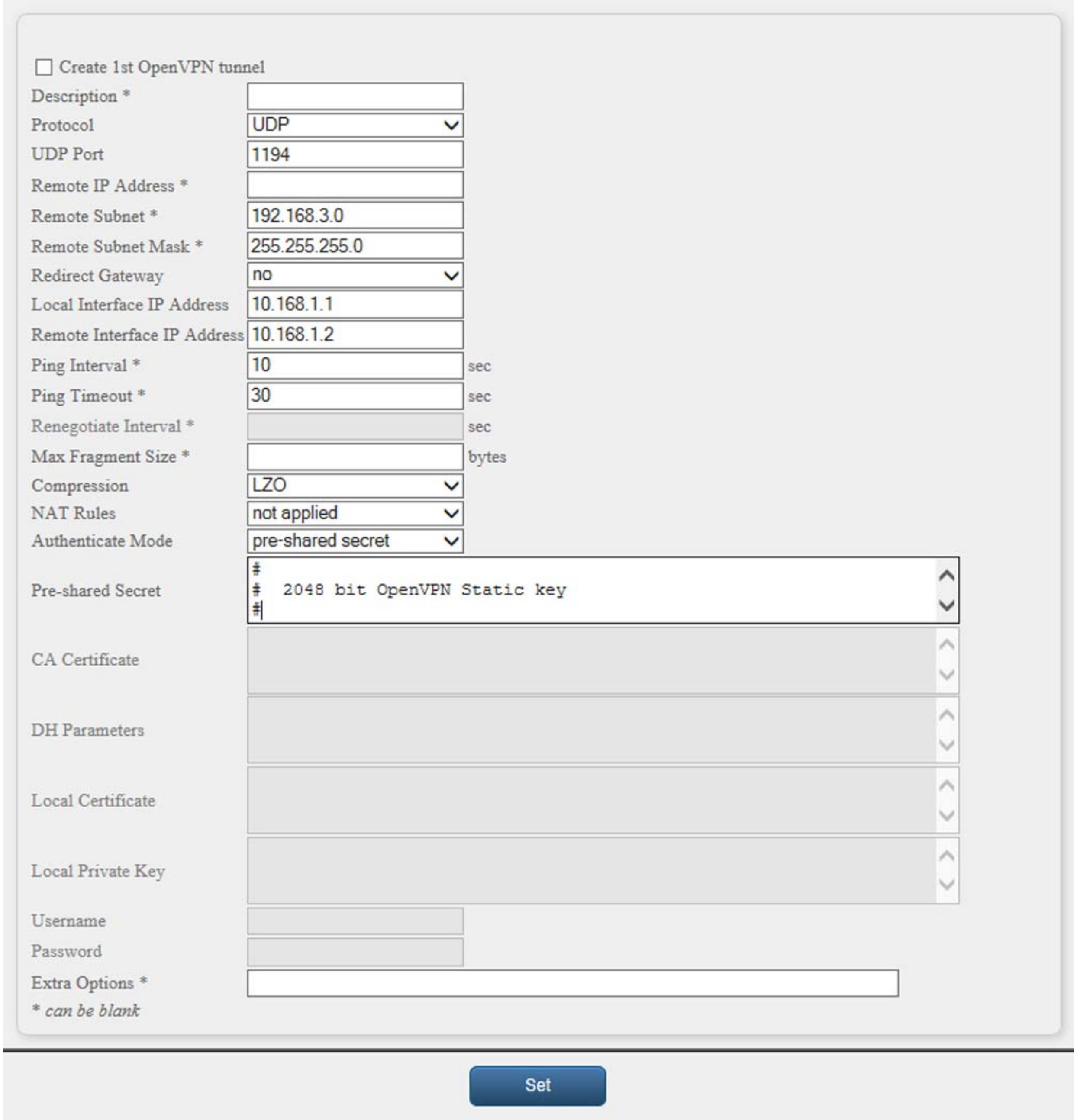
Table 61: Configuration of the first router (pre-shared secret)

Enter the following parameters in the configuration of the second router. This router is the CLIENT:

Item	Value
Remote IP Address	10.0.2.36
Remote Subnet	192.168.1.0
Remote Subnet Mask	255.255.255.0
Local Interface IP Address	10.168.1.2
Remote Interface IP Address	10.168.1.1
Authenticate Mode	pre-shared secret
Pre-shared Secret	shared key for both of routers

Table 62: Configuration of the second router (pre-shared secret)

The procedure of creating the pre-shared key is described in the pre-key chapter. See “Creation of pre-shared key” on page 157.



☐ Create 1st OpenVPN tunnel

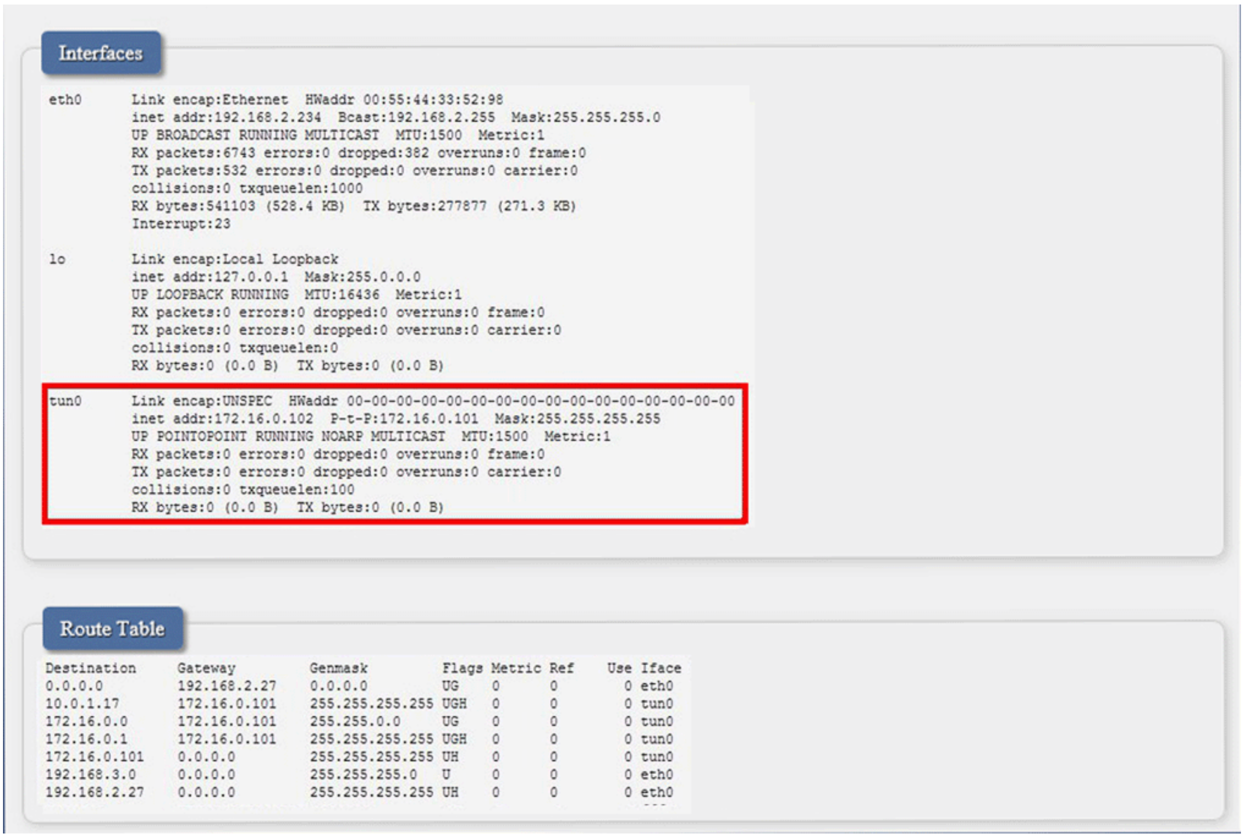
Description *		
Protocol	UDP	
UDP Port	1194	
Remote IP Address *		
Remote Subnet *	192.168.3.0	
Remote Subnet Mask *	255.255.255.0	
Redirect Gateway	no	
Local Interface IP Address	10.168.1.1	
Remote Interface IP Address	10.168.1.2	
Ping Interval *	10	sec
Ping Timeout *	30	sec
Renegotiate Interval *		sec
Max Fragment Size *		bytes
Compression	LZO	
NAT Rules	not applied	
Authenticate Mode	pre-shared secret	
Pre-shared Secret	# # 2048 bit OpenVPN Static key #	
CA Certificate		
DH Parameters		
Local Certificate		
Local Private Key		
Username		
Password		
Extra Options *		

** can be blank*

Figure 80: Configuration of the first router (pre-shared secret)

Note: The configuration of the second router is similar to the first router. See table 62 on page 128. If you select ″applied″ from the NAT Rules drop down menu, then the router applies the rules specified in the Security> NAT dialog to the OpenVPN tunnel.

After establishing an OpenVPN tunnel, the `Network> LAN Status` dialog displays the tun0 interface in the Interface section, and the associated route in the Route Table section.



Interfaces

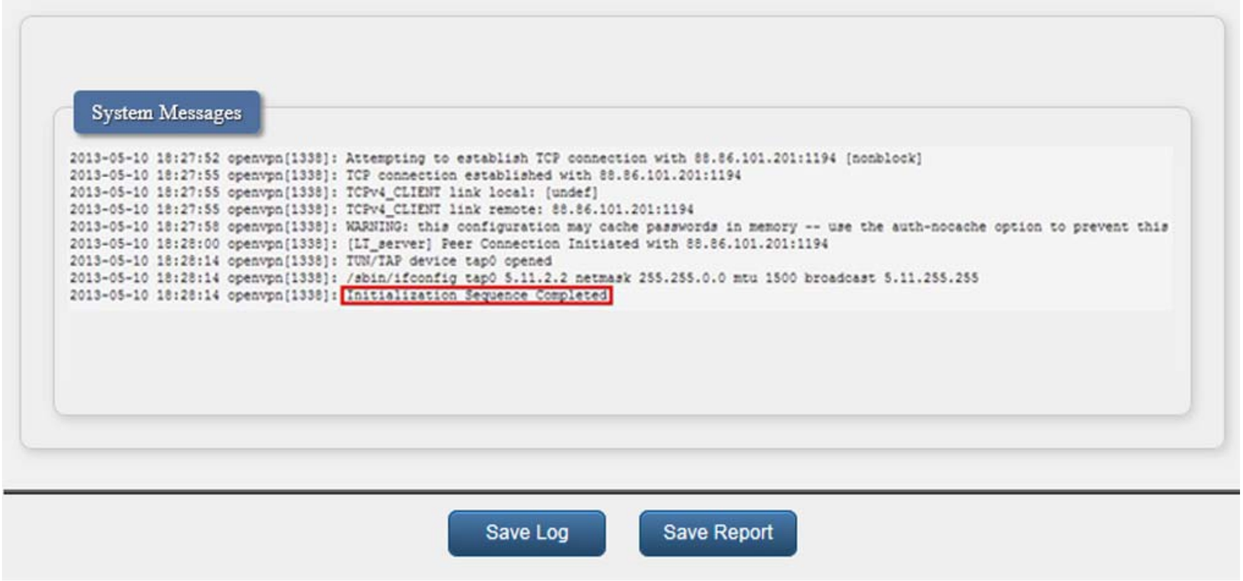
```
eth0      Link encap:Ethernet  HWaddr 00:55:44:33:52:98
          inet addr:192.168.2.234  Bcast:192.168.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6743 errors:0 dropped:382 overruns:0 frame:0
          TX packets:532 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:541103 (528.4 KB)  TX bytes:277877 (271.3 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)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:172.16.0.102  P-t-P:172.16.0.101  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP 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:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Route Table

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.2.27    0.0.0.0         UG    0      0        0 eth0
10.0.1.17       172.16.0.101    255.255.255.255 UGH   0      0        0 tun0
172.16.0.0      172.16.0.101    255.255.0.0     UG    0      0        0 tun0
172.16.0.1      172.16.0.101    255.255.255.255 UGH   0      0        0 tun0
172.16.0.101    0.0.0.0         255.255.255.255 UH    0      0        0 tun0
192.168.3.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.2.27    0.0.0.0         255.255.255.255 UH    0      0        0 eth0
```

Figure 81: Network Status

It is also possible to verify a successful establishment of the OpenVPN tunnel in the system log, click `System Log` in menu tree. After the router establishes an OpenVPN tunnel, the log displays the “Initialization Sequence Completed” entry.



```
2013-05-10 18:27:52 openvpn[1338]: Attempting to establish TCP connection with 88.86.101.201:1194 [nonblock]
2013-05-10 18:27:55 openvpn[1338]: TCP connection established with 88.86.101.201:1194
2013-05-10 18:27:55 openvpn[1338]: TCPv4_CLIENT link local: [undef]
2013-05-10 18:27:55 openvpn[1338]: TCPv4_CLIENT link remote: 88.86.101.201:1194
2013-05-10 18:27:58 openvpn[1338]: WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2013-05-10 18:28:00 openvpn[1338]: [LT_server] Peer Connection Initiated with 88.86.101.201:1194
2013-05-10 18:28:14 openvpn[1338]: TUN/TAP device tap0 opened
2013-05-10 18:28:14 openvpn[1338]: /sbin/ifconfig tap0 5.11.2.2 netmask 255.255.0.0 mtu 1500 broadcast 5.11.255.255
2013-05-10 18:28:14 openvpn[1338]: Initialization Sequence Completed
```

Figure 82: System log

2.3.3 OpenVPN tunnel with username/password authentication

Enter the following parameters in the configuration of the first router. This router is the SERVER:

Item	Value
Remote Subnet	192.168.3.0
Remote Subnet Mask	255.255.255.0
Authenticate Mode	username/password
CA Certificate	generated certificate from VPN server
Username	username assigned by the VPN server
Password	password assigned by the VPN server

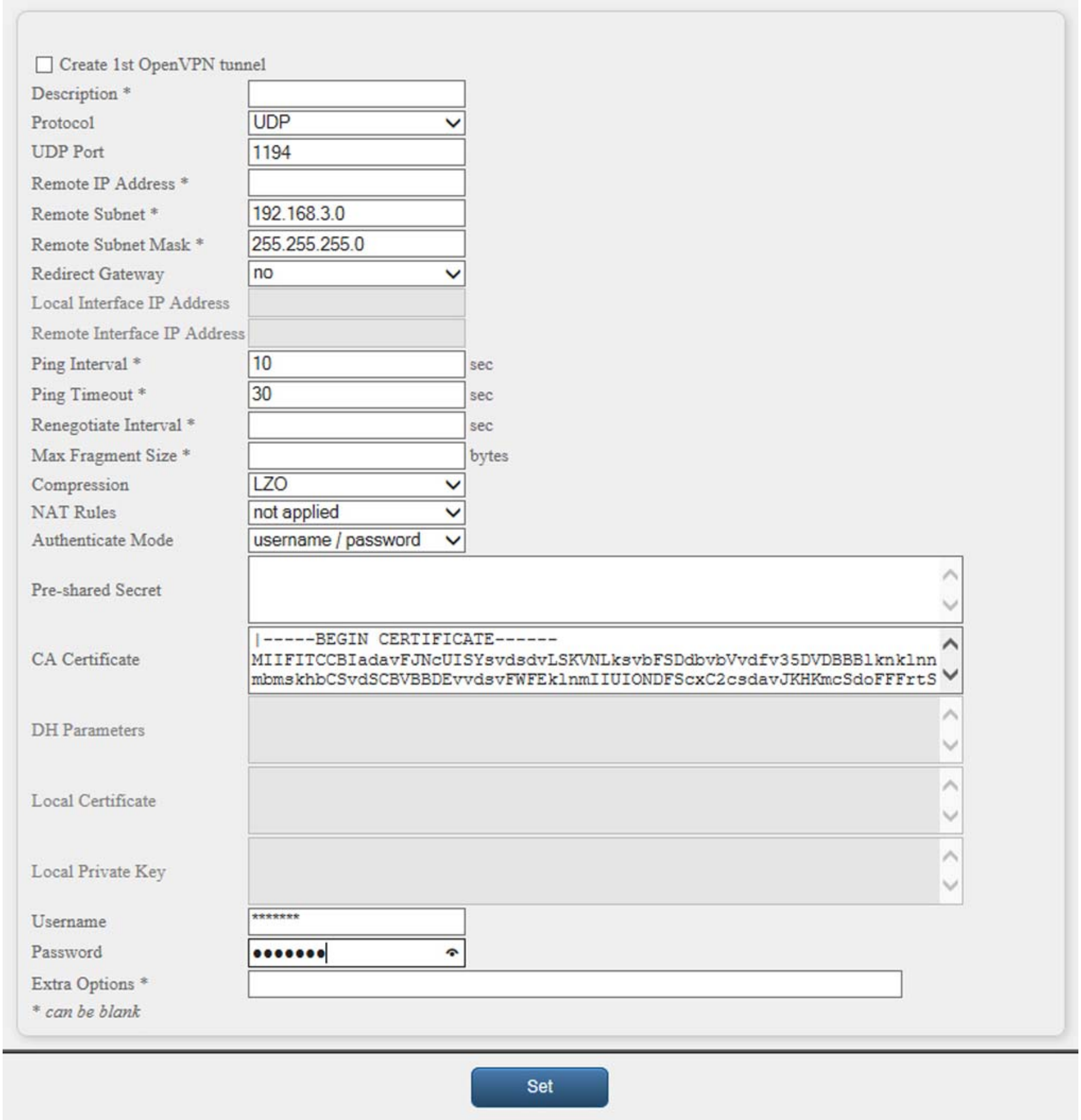
Table 63: Configuration of the first router (username/password)

Enter the following parameters in the configuration of the second router. This router is the CLIENT:

Item	Value
Remote IP Address	10.0.2.36
Remote Subnet	192.168.1.0
Remote Subnet Mask	255.255.255.0
Authenticate Mode	username/password
CA Certificate	generated certificate from VPN server
Username	username assigned by the VPN server
Password	password assigned by the VPN server

Table 64: Configuration of the second router (username/password)

The procedure of creating certificate is described in the certificate chapter. See “Creation of certificates” on page 158.



☐ Create 1st OpenVPN tunnel

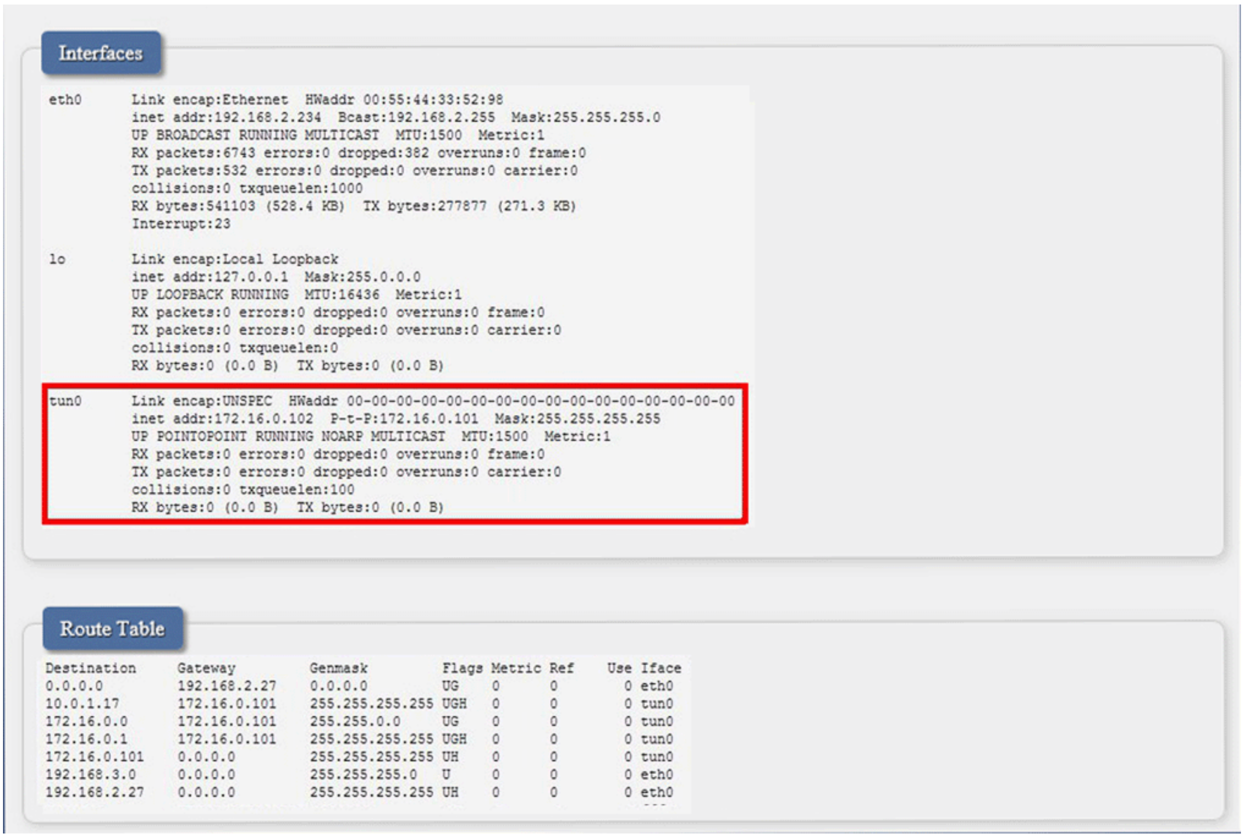
Description *		
Protocol	UDP	
UDP Port	1194	
Remote IP Address *		
Remote Subnet *	192.168.3.0	
Remote Subnet Mask *	255.255.255.0	
Redirect Gateway	no	
Local Interface IP Address		
Remote Interface IP Address		
Ping Interval *	10	sec
Ping Timeout *	30	sec
Renegotiate Interval *		sec
Max Fragment Size *		bytes
Compression	LZO	
NAT Rules	not applied	
Authenticate Mode	username / password	
Pre-shared Secret		
CA Certificate	-----BEGIN CERTIFICATE------ MIIFITCCBIadavFJNcUISYsvdsdvLSKVNLksvbFSDdbvbVvdfv35DVDBBBlknklnn mbmskhbCSvdSCBVBBDEvvdsvFWFEklnmIIUIONDFScxC2csdavJKHKmcSdoFFFrtS	
DH Parameters		
Local Certificate		
Local Private Key		
Username	*******	
Password	•••••••	
Extra Options *		

** can be blank*

Figure 83: Configuration of the first router (username/password)

Note: The configuration of the second router is similar to the first router. See table 64 on page 132. If you select ”applied” from the NAT Rules drop down menu, then the router applies the rules specified in the Security> NAT dialog to the OpenVPN tunnel.

After establishing an OpenVPN tunnel, the `Network> LAN Status` dialog displays the tun0 interface in the Interface section, and the associated route in the Route Table section.

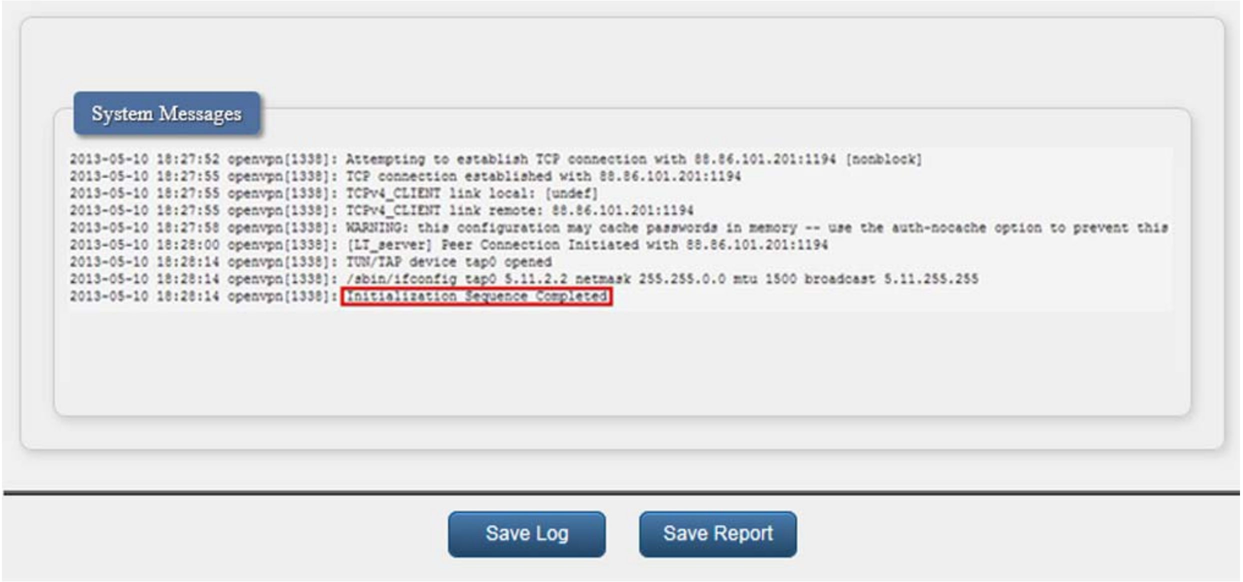


```
eth0      Link encap:Ethernet  HWaddr 00:55:44:33:52:98
          inet addr:192.168.2.234  Bcast:192.168.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6743 errors:0 dropped:382 overruns:0 frame:0
          TX packets:532 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:541103 (528.4 KB)  TX bytes:277877 (271.3 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)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:172.16.0.102  P-t-P:172.16.0.101  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP 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:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.2.27    0.0.0.0         UG    0      0        0 eth0
10.0.1.17       172.16.0.101    255.255.255.255 UGH   0      0        0 tun0
172.16.0.0      172.16.0.101    255.255.0.0     UG    0      0        0 tun0
172.16.0.1      172.16.0.101    255.255.255.255 UGH   0      0        0 tun0
172.16.0.101    0.0.0.0         255.255.255.255 UH    0      0        0 tun0
192.168.3.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.2.27    0.0.0.0         255.255.255.255 UH    0      0        0 eth0
```

Figure 84: Network Status

It is also possible to verify a successful establishment of the OpenVPN tunnel in the system log, click `System Log` in menu tree. After the router establishes an OpenVPN tunnel, the log displays the “Initialization Sequence Completed” entry.



```
2013-05-10 18:27:52 openvpn[1338]: Attempting to establish TCP connection with 88.86.101.201:1194 [nonblock]
2013-05-10 18:27:55 openvpn[1338]: TCP connection established with 88.86.101.201:1194
2013-05-10 18:27:55 openvpn[1338]: TCPv4_CLIENT link local: [undef]
2013-05-10 18:27:55 openvpn[1338]: TCPv4_CLIENT link remote: 88.86.101.201:1194
2013-05-10 18:27:58 openvpn[1338]: WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2013-05-10 18:28:00 openvpn[1338]: [LT_server] Peer Connection Initiated with 88.86.101.201:1194
2013-05-10 18:28:14 openvpn[1338]: TUN/TAP device tap0 opened
2013-05-10 18:28:14 openvpn[1338]: /sbin/ifconfig tap0 5.11.2.2 netmask 255.255.0.0 mtu 1500 broadcast 5.11.255.255
2013-05-10 18:28:14 openvpn[1338]: Initialization Sequence Completed
```

Figure 85: System log

2.3.4 OpenVPN tunnel with X.509 certificate authentication

Enter the following parameters in the configuration of the first router. This router is the SERVER:

Item	Value
Remote Subnet	192.168.3.0
Remote Subnet Mask	255.255.255.0
Local Interface IP Address	10.168.1.1
Remote Interface IP Address	10.168.1.2
Authenticate Mode	X.509 certificate (server)
CA Certificate	generated certificate from VPN server
DH Parameters	Diffie-Hellman protocol for key exchange
Local Certificate	local certificate assigned by the VPN server
Local Private Key	local private key assigned by the VPN server

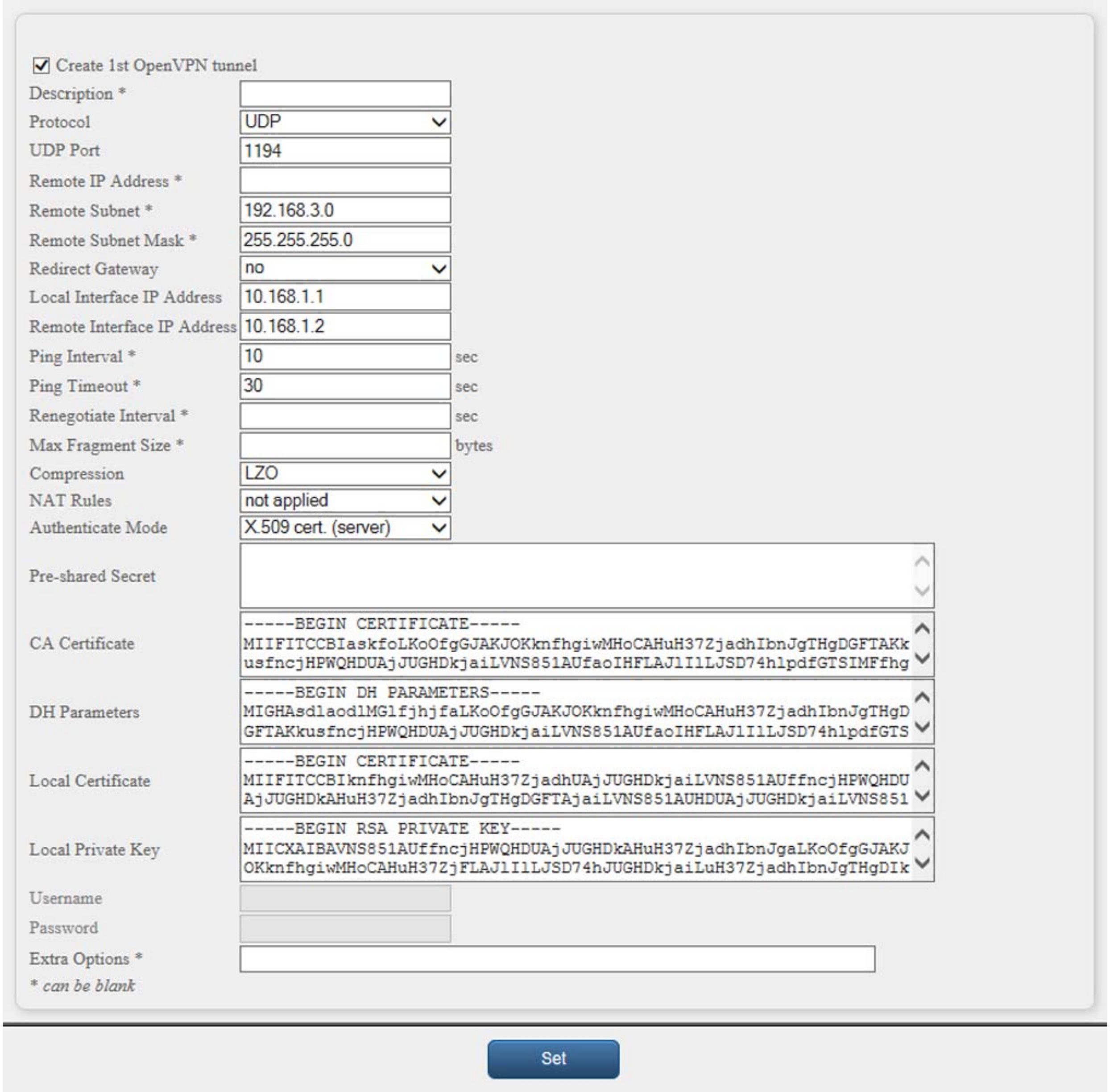
Table 65: Configuration of the first router (X.509 certificate)

Enter the following parameters in the configuration of the second router. This router is the CLIENT:

Item	Value
Remote IP Address	10.0.2.36
Remote Subnet	192.168.1.0
Remote Subnet Mask	255.255.255.0
Local Interface IP Address	10.168.1.2
Remote Interface IP Address	10.168.1.1
Authenticate Mode	X.509 certificate (client)
CA Certificate	generated certificate from VPN server
Local Certificate	local certificate assigned by the VPN server
Local Private Key	local private key assigned by the VPN server

Table 66: Configuration of the second router (X.509 certificate)

The procedure of creating certificate is described in the certificate chapter. See “Creation of certificates” on page 158.



☑ Create 1st OpenVPN tunnel

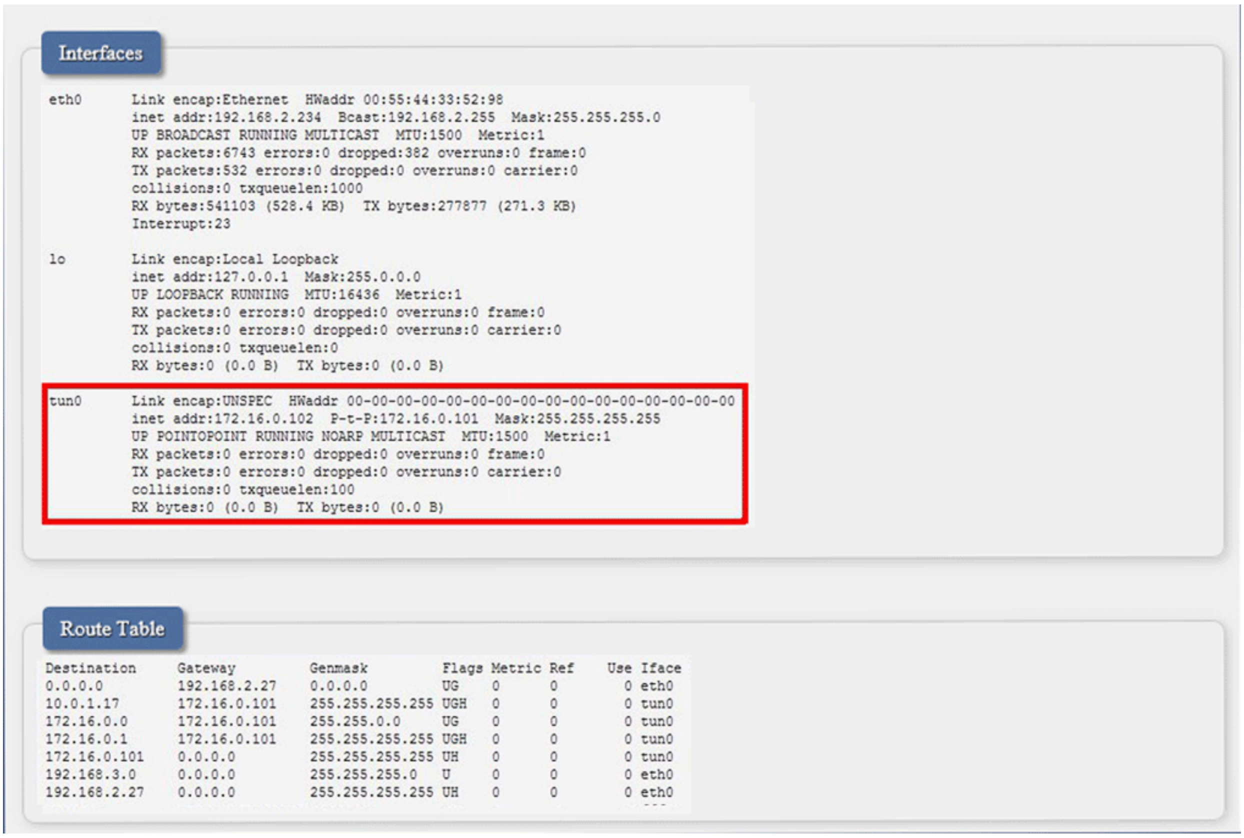
Description *		
Protocol	UDP	
UDP Port	1194	
Remote IP Address *		
Remote Subnet *	192.168.3.0	
Remote Subnet Mask *	255.255.255.0	
Redirect Gateway	no	
Local Interface IP Address	10.168.1.1	
Remote Interface IP Address	10.168.1.2	
Ping Interval *	10	sec
Ping Timeout *	30	sec
Renegotiate Interval *		sec
Max Fragment Size *		bytes
Compression	LZO	
NAT Rules	not applied	
Authenticate Mode	X.509 cert. (server)	
Pre-shared Secret		
CA Certificate	-----BEGIN CERTIFICATE----- MIIFITCCBIaskfoLKoOfgGJAKJOKknfhgiwMHoCAHuH37ZjadhIbnJgTHgDGFTAKk usfncjHPWQHDUAjJUGHDkjaiLVNS851AUfaoIHFLAJlIlLJSD74hlpdfGTSIMFfhg	
DH Parameters	-----BEGIN DH PARAMETERS----- MIGHAsdlaodlMGlfjhjfaLKoOfgGJAKJOKknfhgiwMHoCAHuH37ZjadhIbnJgTHgD GFTAKkusfncjHPWQHDUAjJUGHDkjaiLVNS851AUfaoIHFLAJlIlLJSD74hlpdfGTS	
Local Certificate	-----BEGIN CERTIFICATE----- MIIFITCCBIknfhgiwMHoCAHuH37ZjadhUAjJUGHDkjaiLVNS851AUffncjHPWQHDU AjJUGHDkAHuH37ZjadhIbnJgTHgDGFTAjaiLVNS851AUHDUAjJUGHDkjaiLVNS851	
Local Private Key	-----BEGIN RSA PRIVATE KEY----- MIICXAIBAVNS851AUffncjHPWQHDUAjJUGHDkAHuH37ZjadhIbnJgaLKoOfgGJAKJ OKknfhgiwMHoCAHuH37ZjFLAJlIlLJSD74hJUGHDkjaiLuH37ZjadhIbnJgTHgDIk	
Username		
Password		
Extra Options *		

** can be blank*

Figure 86: Configuration of the first router (X.509 certificate)

Note: The configuration of the second router is similar to the first router. See table 66 on page 136. If you select ”applied” from the NAT Rules drop down menu, then the router applies the rules specified in the Security> NAT dialog to the OpenVPN tunnel.

After establishing an OpenVPN tunnel, the `Network> LAN Status` dialog displays the tun0 interface in the Interface section, and the associated route in the Route Table section.

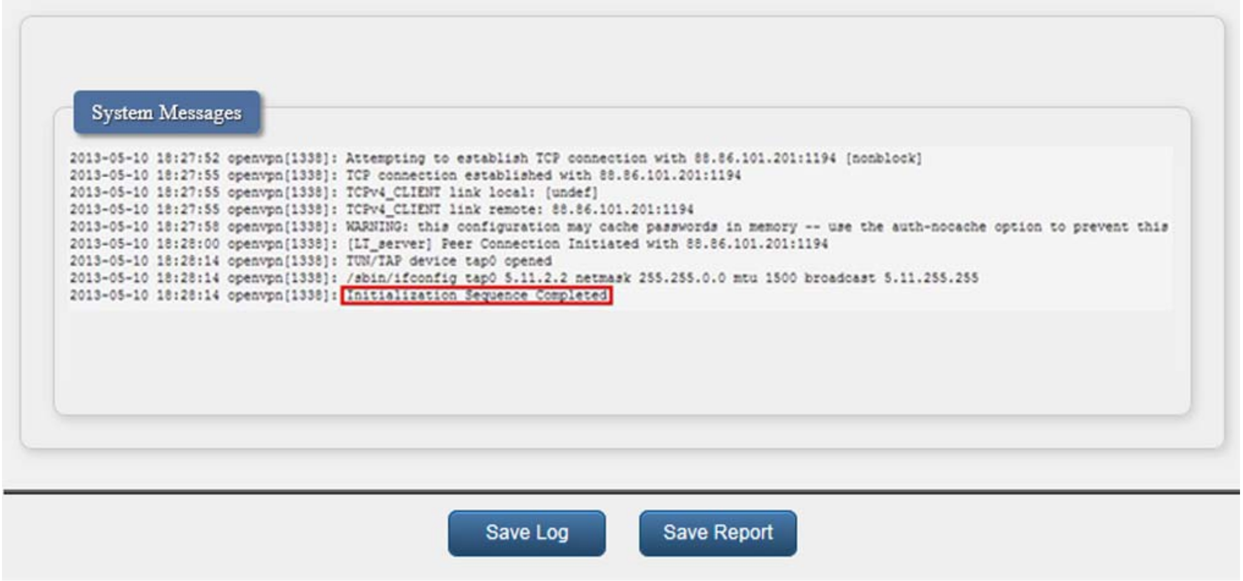


```
eth0      Link encap:Ethernet  HWaddr 00:55:44:33:52:98
          inet addr:192.168.2.234  Bcast:192.168.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6743 errors:0 dropped:382 overruns:0 frame:0
          TX packets:532 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:541103 (528.4 KB)  TX bytes:277877 (271.3 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)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:172.16.0.102  P-t-P:172.16.0.101  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP 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:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.2.27    0.0.0.0         UG    0      0        0 eth0
10.0.1.17       172.16.0.101    255.255.255.255 UGH   0      0        0 tun0
172.16.0.0      172.16.0.101    255.255.0.0     UG    0      0        0 tun0
172.16.0.1      172.16.0.101    255.255.255.255 UGH   0      0        0 tun0
172.16.0.101    0.0.0.0         255.255.255.255 UH    0      0        0 tun0
192.168.3.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.2.27    0.0.0.0         255.255.255.255 UH    0      0        0 eth0
```

Figure 87: Network Status

It is also possible to verify a successful establishment of the OpenVPN tunnel in the system log, click `System Log` in menu tree. After the router establishes an OpenVPN tunnel, the log displays the “Initialization Sequence Completed” entry.



```
2013-05-10 18:27:52 openvpn[1338]: Attempting to establish TCP connection with 88.86.101.201:1194 [nonblock]
2013-05-10 18:27:55 openvpn[1338]: TCP connection established with 88.86.101.201:1194
2013-05-10 18:27:55 openvpn[1338]: TCPv4_CLIENT link local: [undef]
2013-05-10 18:27:55 openvpn[1338]: TCPv4_CLIENT link remote: 88.86.101.201:1194
2013-05-10 18:27:58 openvpn[1338]: WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2013-05-10 18:28:00 openvpn[1338]: [LT_server] Peer Connection Initiated with 88.86.101.201:1194
2013-05-10 18:28:14 openvpn[1338]: TUN/TAP device tap0 opened
2013-05-10 18:28:14 openvpn[1338]: /sbin/ifconfig tap0 5.11.2.2 netmask 255.255.0.0 mtu 1500 broadcast 5.11.255.255
2013-05-10 18:28:14 openvpn[1338]: Initialization Sequence Completed
```

Figure 88: System log

2.4 Tunnel paired with a WIN/ Linux CLIENT

The figure below displays a network, where a Hirschmannn router is on one side of OpenVPN tunnel and device with a Windows/Linux operating system, in CLIENT mode, is on the other side. The IP address of the SIM card in the router can be static or dynamic.

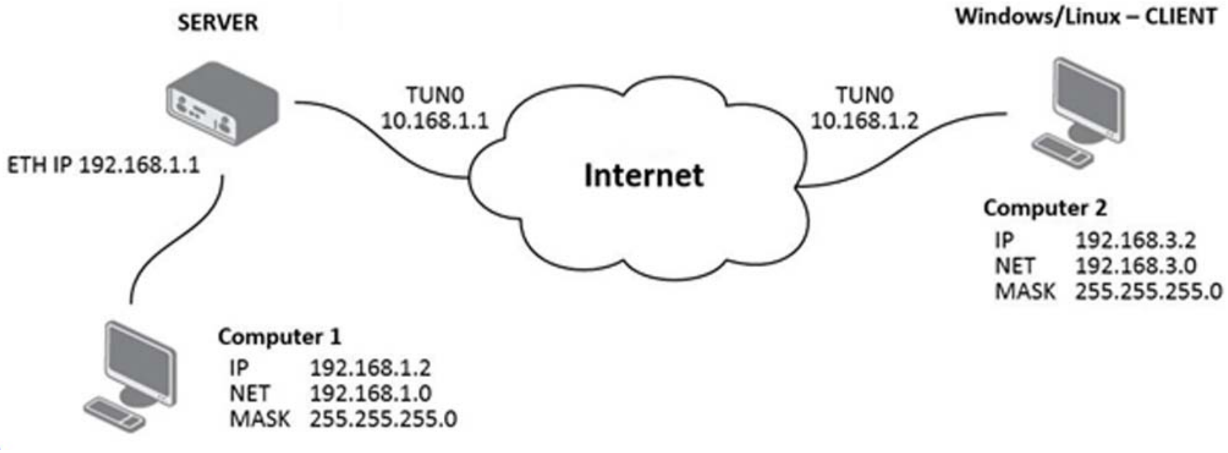
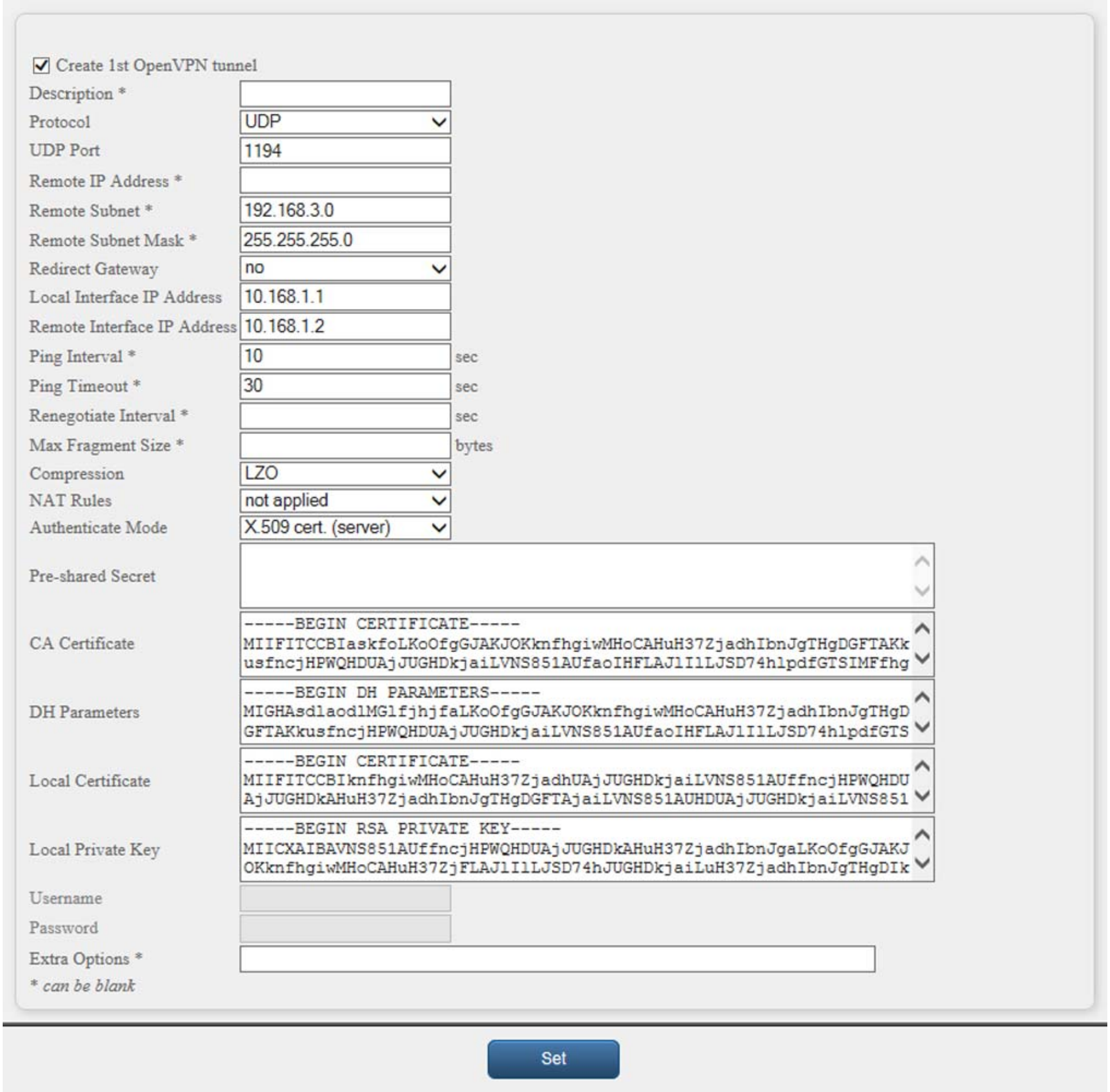


Figure 89: OpenVPN tunnel paired with a Windows/Linux CLIENT

2.4.1 OpenVPN tunnel configuration on the router

Item	Value
Remote Subnet	192.168.3.0
Remote Subnet Mask	255.255.255.0
Local Interface IP Address	10.168.1.1
Remote Interface IP Address	10.168.1.2
Authenticate Mode	X.509 certificate (server)
CA Certificate	generated certificate from router (SERVER)
DH Parameters	Diffie-Hellman protocol for key exchange
Local Certificate	local certificate assigned by router (SERVER)
Local Private Key	local private key assigned by router (SERVER)

Table 67: Router configuration



☑ Create 1st OpenVPN tunnel

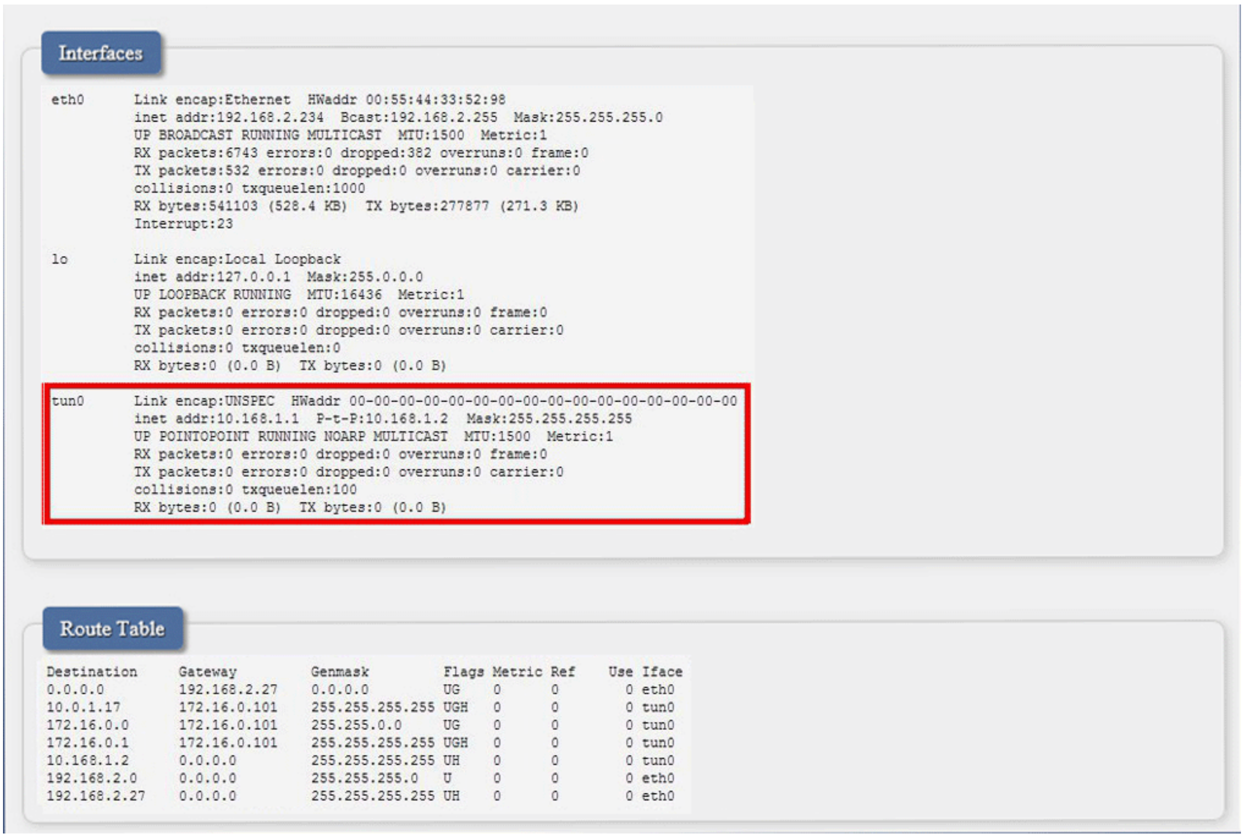
Description *		
Protocol	UDP	
UDP Port	1194	
Remote IP Address *		
Remote Subnet *	192.168.3.0	
Remote Subnet Mask *	255.255.255.0	
Redirect Gateway	no	
Local Interface IP Address	10.168.1.1	
Remote Interface IP Address	10.168.1.2	
Ping Interval *	10	sec
Ping Timeout *	30	sec
Renegotiate Interval *		sec
Max Fragment Size *		bytes
Compression	LZO	
NAT Rules	not applied	
Authenticate Mode	X.509 cert. (server)	
Pre-shared Secret		
CA Certificate	-----BEGIN CERTIFICATE----- MIIFITCCBIaskfoLKoOfgGJAKJOKknfhgiwMHoCAHuH37ZjadhIbnJgTHgDGFTAKk usfncjHPWQHDUAjJUGHDkjaiLVNS851AUfaoIHFLAJlIlLJSD74hlpdfGTSIMFfhg	
DH Parameters	-----BEGIN DH PARAMETERS----- MIGHAsdlaodlMGlfjhjfaLKoOfgGJAKJOKknfhgiwMHoCAHuH37ZjadhIbnJgTHgD GFTAKkusfncjHPWQHDUAjJUGHDkjaiLVNS851AUfaoIHFLAJlIlLJSD74hlpdfGTS	
Local Certificate	-----BEGIN CERTIFICATE----- MIIFITCCBIknfhgiwMHoCAHuH37ZjadhUAjJUGHDkjaiLVNS851AUffncjHPWQHDU AjJUGHDkAHuH37ZjadhIbnJgTHgDGFTAjaiLVNS851AUHDUAjJUGHDkjaiLVNS851	
Local Private Key	-----BEGIN RSA PRIVATE KEY----- MIICXAIBAVNS851AUffncjHPWQHDUAjJUGHDkAHuH37ZjadhIbnJgaLKoOfgGJAKJ OKknfhgiwMHoCAHuH37ZjFLAJlIlLJSD74hJUGHDkjaiLuH37ZjadhIbnJgTHgDIk	
Username		
Password		
Extra Options *		

** can be blank*

Figure 90: Router configuration

Note: If you select ”applied” from the `NAT Rules` drop down menu, then the router applies the rules specified in the `Security> NAT` dialog to the OpenVPN tunnel.

After establishing an OpenVPN tunnel, the `Network> LAN Status` dialog displays the tun0 interface in the Interface section, and the associated route in the Route Table section.

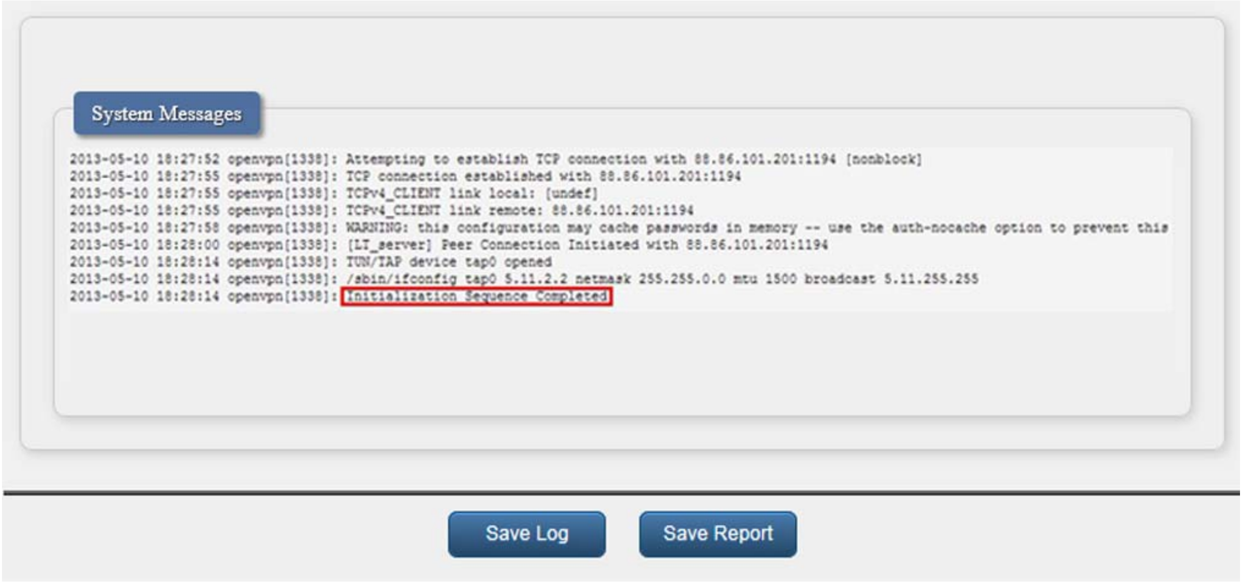


```
eth0      Link encap:Ethernet  HWaddr 00:55:44:33:52:98
          inet addr:192.168.2.234  Bcast:192.168.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6743 errors:0 dropped:382 overruns:0 frame:0
          TX packets:532 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:541103 (528.4 KB)  TX bytes:277877 (271.3 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)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.168.1.1  P-t-P:10.168.1.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP 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:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.2.27    0.0.0.0         UG    0      0        0 eth0
10.0.1.17       172.16.0.101    255.255.255.255 UGH   0      0        0 tun0
172.16.0.0      172.16.0.101    255.255.0.0     UG    0      0        0 tun0
172.16.0.1      172.16.0.101    255.255.255.255 UGH   0      0        0 tun0
10.168.1.2      0.0.0.0         255.255.255.255 UH    0      0        0 tun0
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.2.27    0.0.0.0         255.255.255.255 UH    0      0        0 eth0
```

Figure 91: Network Status

It is also possible to verify a successful establishment of the OpenVPN tunnel in the system log, click `System Log` in menu tree. After the router establishes an OpenVPN tunnel, the log displays the “Initialization Sequence Completed” entry.



```
2013-05-10 18:27:52 openvpn[1338]: Attempting to establish TCP connection with 88.86.101.201:1194 [nonblock]
2013-05-10 18:27:55 openvpn[1338]: TCP connection established with 88.86.101.201:1194
2013-05-10 18:27:55 openvpn[1338]: TCPv4_CLIENT link local: [undef]
2013-05-10 18:27:55 openvpn[1338]: TCPv4_CLIENT link remote: 88.86.101.201:1194
2013-05-10 18:27:58 openvpn[1338]: WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2013-05-10 18:28:00 openvpn[1338]: [LT_server] Peer Connection Initiated with 88.86.101.201:1194
2013-05-10 18:28:14 openvpn[1338]: TUN/TAP device tap0 opened
2013-05-10 18:28:14 openvpn[1338]: /sbin/ifconfig tap0 5.11.2.2 netmask 255.255.0.0 mtu 1500 broadcast 5.11.255.255
2013-05-10 18:28:14 openvpn[1338]: Initialization Sequence Completed
```

Figure 92: System log

2.4.2 OpenVPN tunnel configuration on Computer 1 with Windows

It is necessary to perform the following configuration on the computer, which is referred to as `Computer 1` in the figure at the beginning of this chapter. See figure 140 “OpenVPN tunnel paired with a Windows/Linux CLIENT”.

```
remote [SERVER_IP]tls-clientdev tunifconfig 10.168.1.2 10.168.1.1ns-
cert-type serverroute 192.168.2.0 255.255.255.0 10.168.1.2mute 10ca
cacert.pemcert client-cert.crt key client-key.keycomp-lzoverb 3
```

2.5 Tunnel paired with a WIN/ Linux SERVER

The figure below shows situation, where Hirschmann router is on one side of OpenVPN tunnel and device with an operating system Windows/Linux in SERVER mode is on the other side. IP address of the SIM card in the router can be static or dynamic.

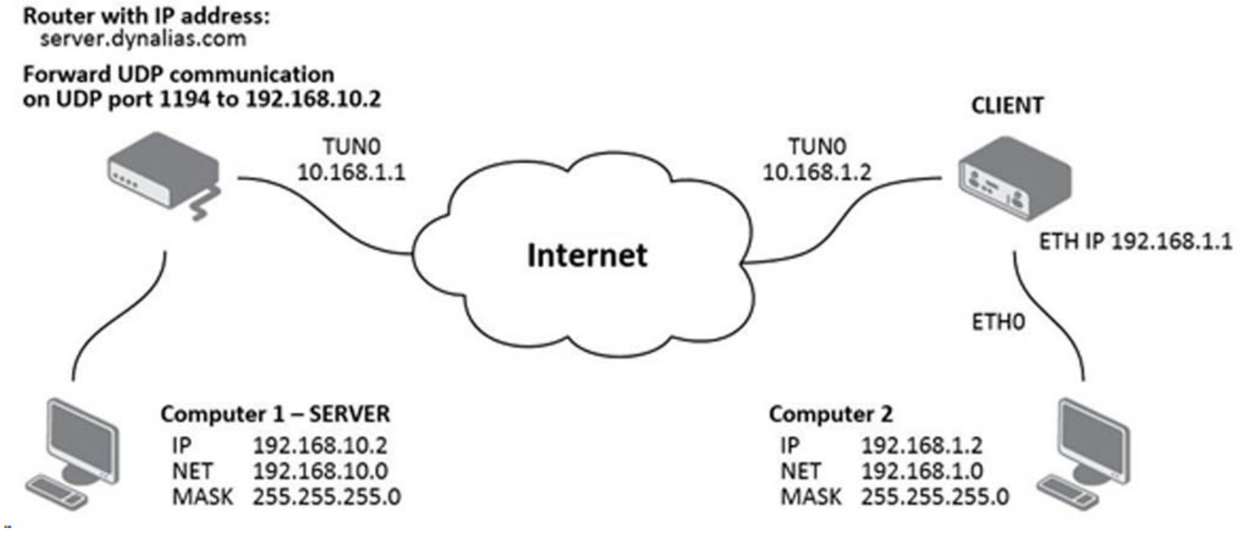
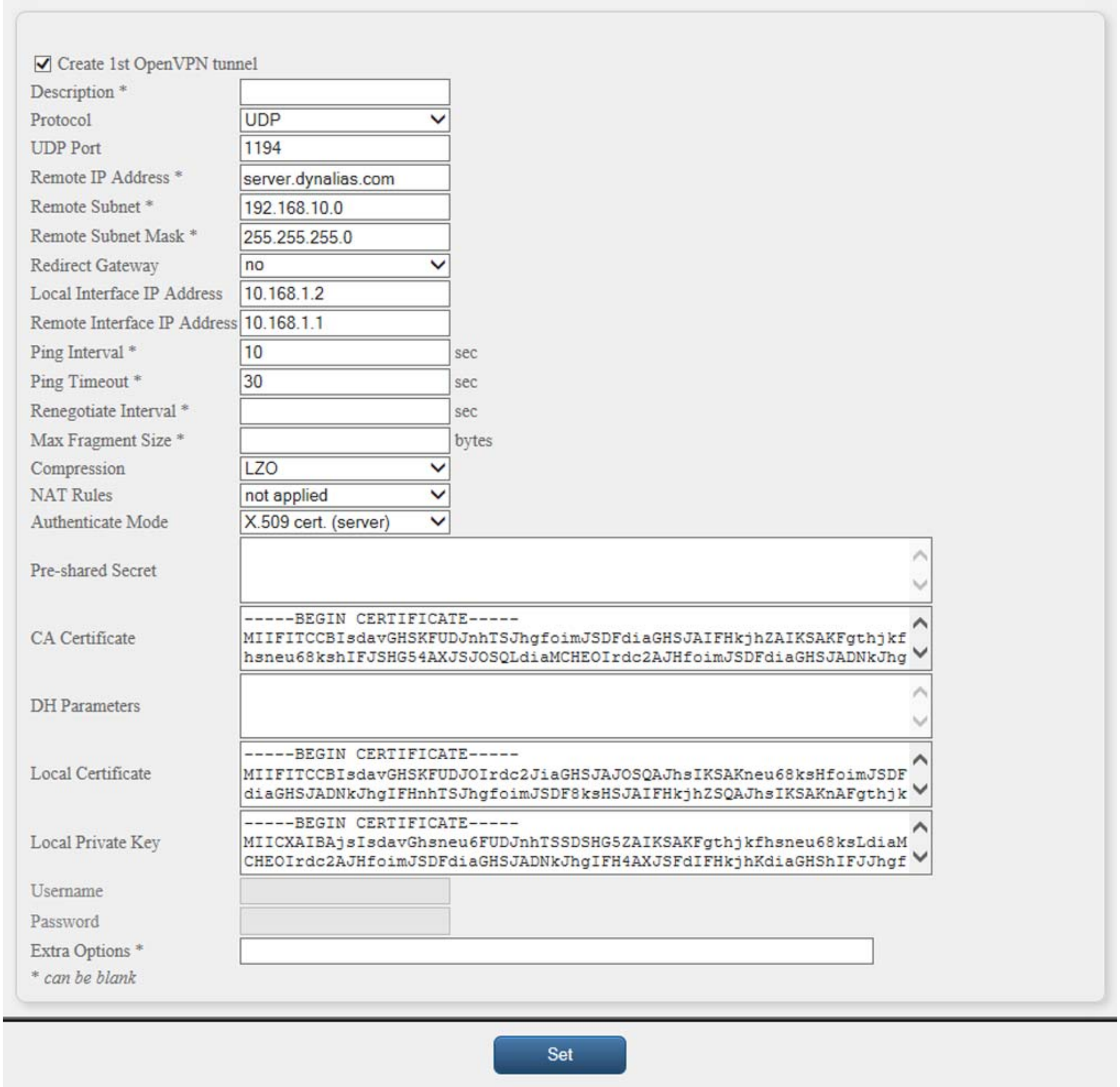


Figure 93: OpenVPN tunnel paired with a Windows/Linux Server

2.5.1 OpenVPN tunnel configuration on the router

Item	Value
Remote IP Address	server.dynalias.com
Remote Subnet	192.168.10.0
Remote Subnet Mask	255.255.255.0
Local Interface IP Address	10.168.1.2
Remote Interface IP Address	10.168.1.1
Authenticate Mode	X.509 certificate (client)
CA Certificate	generated certificate from router
DH Parameters	Diffie-Hellman protocol for key exchange
Local Certificate	local certificate assigned by router
Local Private Key	local private key assigned by router

Table 68: Router configuration



☑ Create 1st OpenVPN tunnel

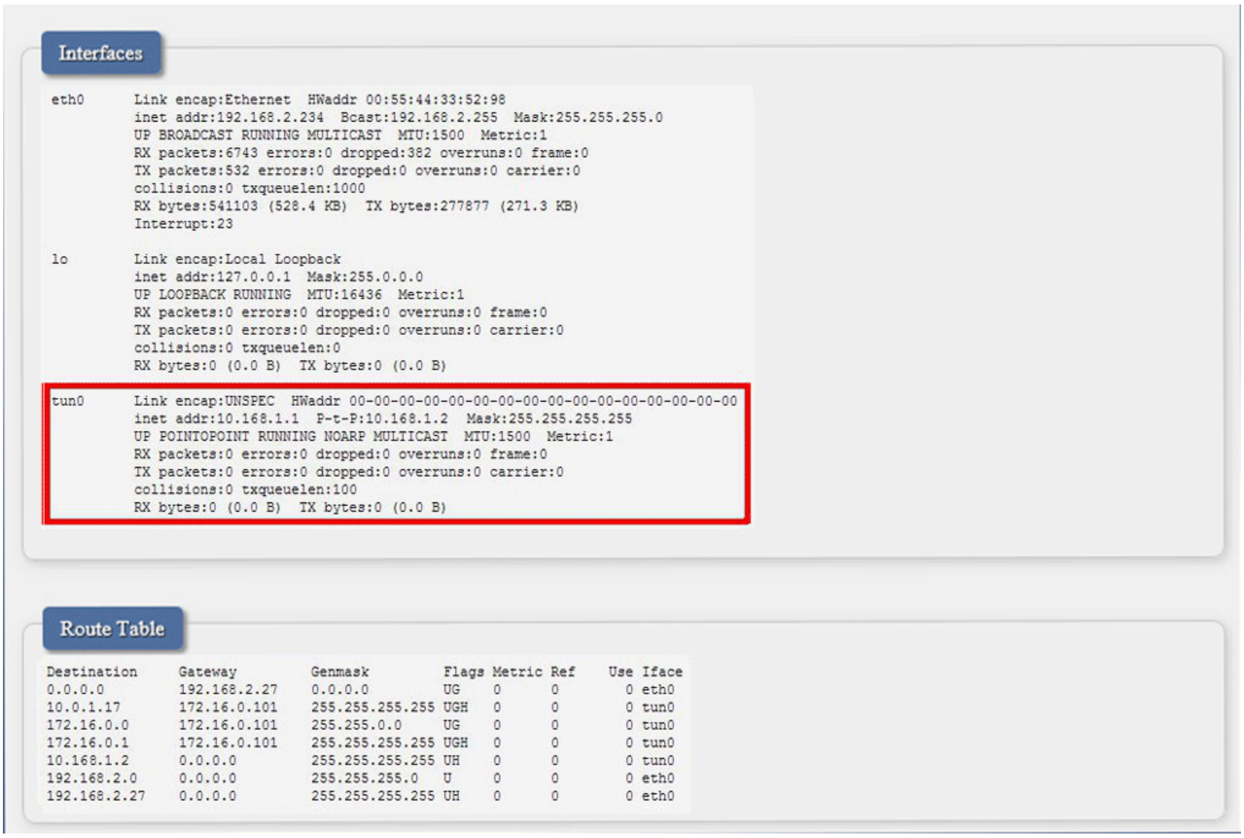
Description *		
Protocol	UDP	
UDP Port	1194	
Remote IP Address *	server.dynalias.com	
Remote Subnet *	192.168.10.0	
Remote Subnet Mask *	255.255.255.0	
Redirect Gateway	no	
Local Interface IP Address	10.168.1.2	
Remote Interface IP Address	10.168.1.1	
Ping Interval *	10	sec
Ping Timeout *	30	sec
Renegotiate Interval *		sec
Max Fragment Size *		bytes
Compression	LZO	
NAT Rules	not applied	
Authenticate Mode	X.509 cert. (server)	
Pre-shared Secret		
CA Certificate	-----BEGIN CERTIFICATE----- MIIFITCCBIsdavGHSKFUDJnhTSJhgfoimJSDFdiaGHSJAIFHkjhZAIKSAKFgthjkf hsneu68kshIFJSHG54AXJSJOSQLdiaMCHEOIrdc2AJHfoimJSDFdiaGHSJADNkJhg	
DH Parameters		
Local Certificate	-----BEGIN CERTIFICATE----- MIIFITCCBIsdavGHSKFUDJOIrdc2JiaGHSJAJOSQAJhsIKSAKneu68ksHfoimJSDF diaGHSJADNkJhgIFHnhTSJhgfoimJSDF8ksHSJAIFHkjhZSQAJhsIKSAKnAFgthjk	
Local Private Key	-----BEGIN CERTIFICATE----- MIICXAIBAjsIsdavGhsneu6FUDJnhTSSDSHG5ZAIKSAKFgthjkfhsneu68ksLdiaM CHEOIrdc2AJHfoimJSDFdiaGHSJADNkJhgIFH4AXJSFdIFHkjhKdiaGHShIFJJhgf	
Username		
Password		
Extra Options *		

** can be blank*

Figure 94: Router configuration

Note: If you select ”applied” from the NAT Rules drop down menu, then the router applies the rules specified in the Security> NAT dialog to the OpenVPN tunnel.

After establishing an OpenVPN tunnel, the `Network> LAN Status` dialog displays the tun0 interface in the Interface section, and the associated route in the Route Table section.



Interfaces

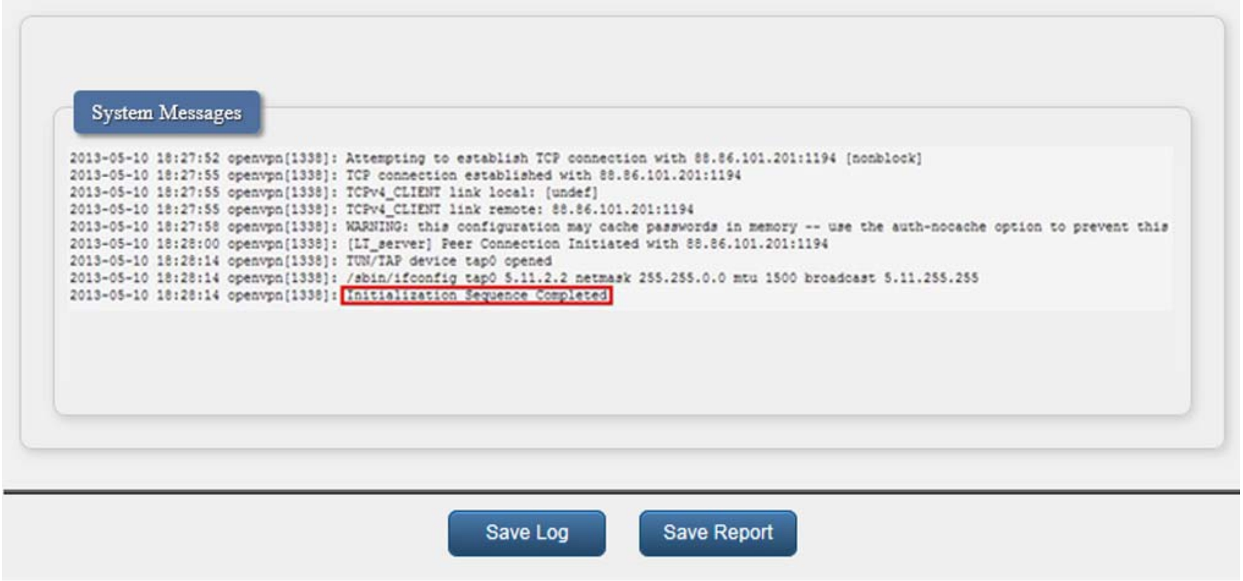
```
eth0      Link encap:Ethernet  HWaddr 00:55:44:33:52:98
          inet addr:192.168.2.234  Bcast:192.168.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6743 errors:0 dropped:382 overruns:0 frame:0
          TX packets:532 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:541103 (528.4 KB)  TX bytes:277877 (271.3 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)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.168.1.1  P-t-P:10.168.1.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP 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:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Route Table

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.2.27    0.0.0.0         UG    0      0        0 eth0
10.0.1.17       172.16.0.101    255.255.255.255 UGH   0      0        0 tun0
172.16.0.0      172.16.0.101    255.255.0.0     UG    0      0        0 tun0
172.16.0.1      172.16.0.101    255.255.255.255 UGH   0      0        0 tun0
10.168.1.2      0.0.0.0         255.255.255.255 UH    0      0        0 tun0
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.2.27    0.0.0.0         255.255.255.255 UH    0      0        0 eth0
```

Figure 95: Network Status

It is also possible to verify a successful establishment of the OpenVPN tunnel in the system log, click `System Log` in menu tree. After the router establishes an OpenVPN tunnel, the log displays the “Initialization Sequence Completed” entry.



```
2013-05-10 18:27:52 openvpn[1338]: Attempting to establish TCP connection with 88.86.101.201:1194 [nonblock]
2013-05-10 18:27:55 openvpn[1338]: TCP connection established with 88.86.101.201:1194
2013-05-10 18:27:55 openvpn[1338]: TCPv4_CLIENT link local: [undef]
2013-05-10 18:27:55 openvpn[1338]: TCPv4_CLIENT link remote: 88.86.101.201:1194
2013-05-10 18:27:58 openvpn[1338]: WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2013-05-10 18:28:00 openvpn[1338]: [LT_server] Peer Connection Initiated with 88.86.101.201:1194
2013-05-10 18:28:14 openvpn[1338]: TUN/TAP device tap0 opened
2013-05-10 18:28:14 openvpn[1338]: /sbin/ifconfig tap0 5.11.2.2 netmask 255.255.0.0 mtu 1500 broadcast 5.11.255.255
2013-05-10 18:28:14 openvpn[1338]: Initialization Sequence Completed
```

Figure 96: System log

2.5.2 Tunnel configuration on Computer 1 – Server

It is necessary to perform the following configuration on the computer, which is referred to as `Computer 1 – Server` in the figure at the beginning of this chapter. See figure 140 “OpenVPN tunnel paired with a Windows/Linux CLIENT”.

```
local 192.168.10.2
port 1194proto udptls-serverdev tunifconfig 10.168.1.1 10.168.1.2route
192.168.1.0 255.255.255.0 10.168.1.2mute 10dh dh1024.pemca ca.crtcert
server.crtkey server.keycomp-lzoverb 3
```

2.6 Multi-server – Hirschmann router (CLIENT)

The figure below displays a network, where an OpenVPN multi-server is on one side of an OpenVPN tunnel and several Hirschmann routers, three in this case, in the CLIENT mode are on the other side. The IP address of the SIM card in the routers can be static or dynamic.

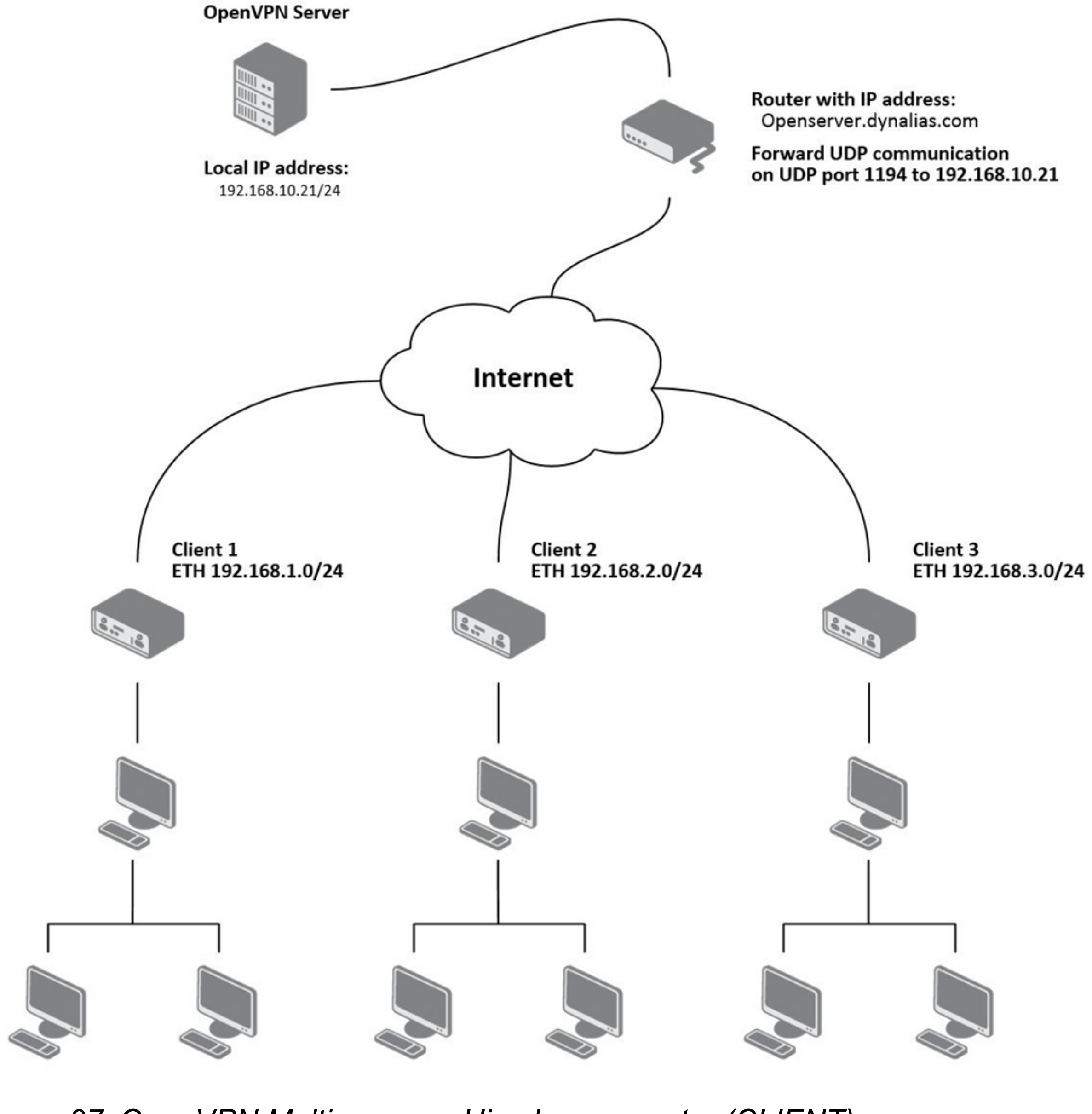
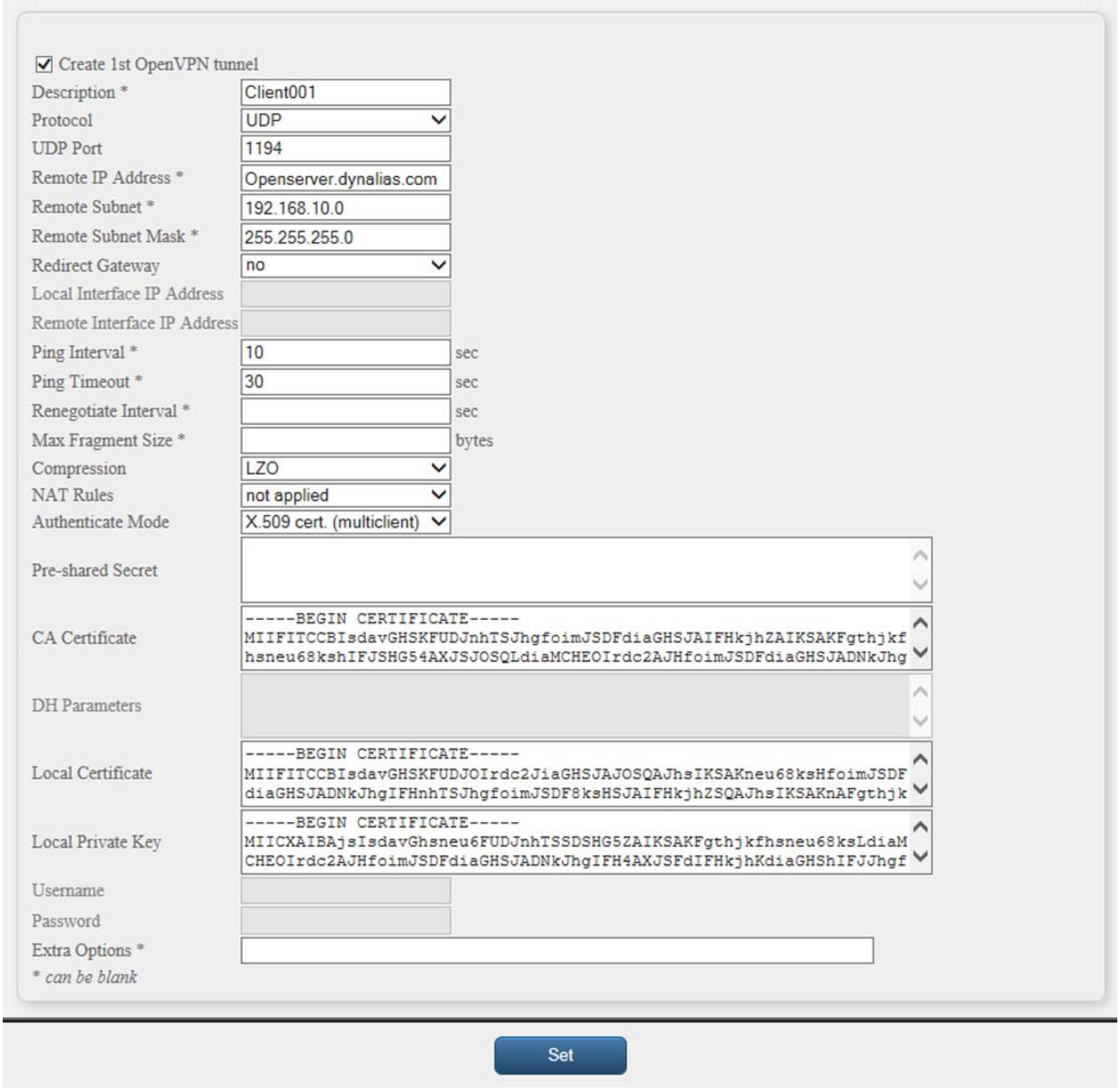


Figure 97: OpenVPN Multi-server – Hirschmann router (CLIENT)

2.6.1 OpenVPN tunnel configuration on Hirschmann routers



☑ Create 1st OpenVPN tunnel

Description *	Client001	
Protocol	UDP	
UDP Port	1194	
Remote IP Address *	Openserver.dynalias.com	
Remote Subnet *	192.168.10.0	
Remote Subnet Mask *	255.255.255.0	
Redirect Gateway	no	
Local Interface IP Address		
Remote Interface IP Address		
Ping Interval *	10	sec
Ping Timeout *	30	sec
Renegotiate Interval *		sec
Max Fragment Size *		bytes
Compression	LZO	
NAT Rules	not applied	
Authenticate Mode	X.509 cert. (multiclient)	
Pre-shared Secret		
CA Certificate	-----BEGIN CERTIFICATE----- MIIFITCCBIsdavGHSKFUDJnhTSJhgfoimJSDFdiaGHSJAIFHkjhZAIKSAKFgthjkf hsneu68kshIFJSHG54AXJSJOSQLdiaMCHEOIrdc2AJHfoimJSDFdiaGHSJADNkJhg	
DH Parameters		
Local Certificate	-----BEGIN CERTIFICATE----- MIIFITCCBIsdavGHSKFUDJOIrdc2JiaGHSJAJOSQAJhsIKSAKneu68ksHfoimJSDF diaGHSJADNkJhgIFHnhTSJhgfoimJSDF8ksHSJAIFHkjhZSQAJhsIKSAKnAFgthjk	
Local Private Key	-----BEGIN CERTIFICATE----- MIICXAIBAjsIsdavGhsneu6FUDJnhTSSDSHG5ZAIKSAKFgthjkfhsneu68ksLdiaM CHEOIrdc2AJHfoimJSDFdiaGHSJADNkJhgIFH4AXJSFdIFHkjhKdiaGHShIFJJhgf	
Username		
Password		
Extra Options *		

** can be blank*

Figure 98: Configuration of Hirschmann router

Note: Configuration of other routers is similar, the only difference is the “`Description`” parameter.

2.6.2 OpenVPN server configuration

```
Config Server:
server 10.8.0.0 255.255.255.0
port 1194
proto udp
dev tun
comp-lzo
keepalive 10 60
dh dh1024.pem
ca ca.crt
key server.key
cert server.crt
ifconfig-pool-persist ipp.txt
status openvpn-status.log
client-config-dir ccd
persist-key
persist-tun
verb 3
route 192.168.1.0 255.255.255.0
route 192.168.2.0 255.255.255.0
route 192.168.3.0 255.255.255.0
---------------------------------------
client-config-dir ccd
.\server\Client001
iroute 192.168.1.0 255.255.255.0
.\server\Client002
iroute 192.168.2.0 255.255.255.0
.\server\Client003
iroute 192.168.3.0 255.255.255.0
```

2.7 OpenVPN client to client

The figure below displays a network, where an OpenVPN server is on one side of an OpenVPN tunnel and several Hirschmann routers, three in this case, in the CLIENT mode are on the other side. The IP address of the SIM card in the routers can be static or dynamic.

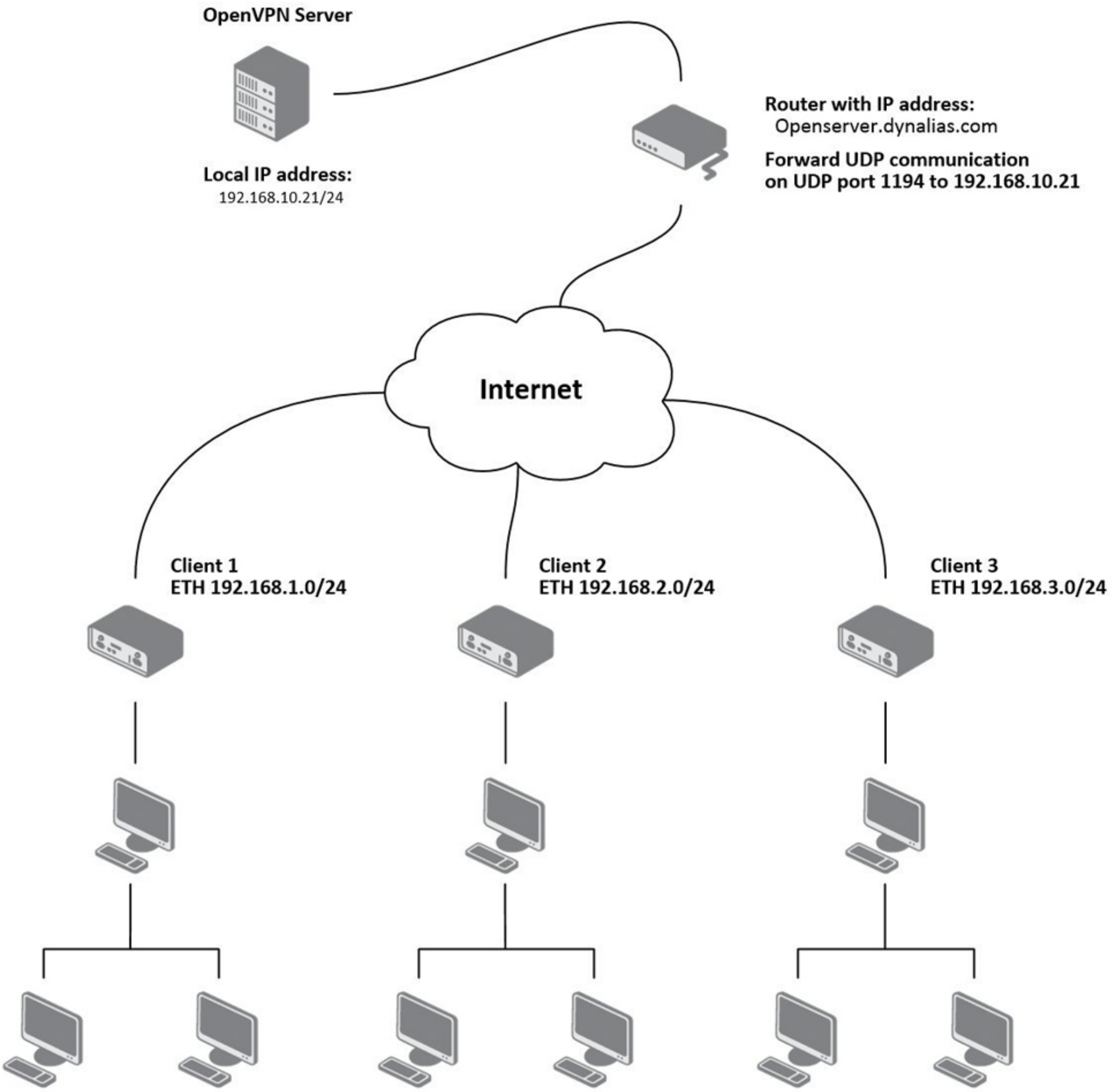
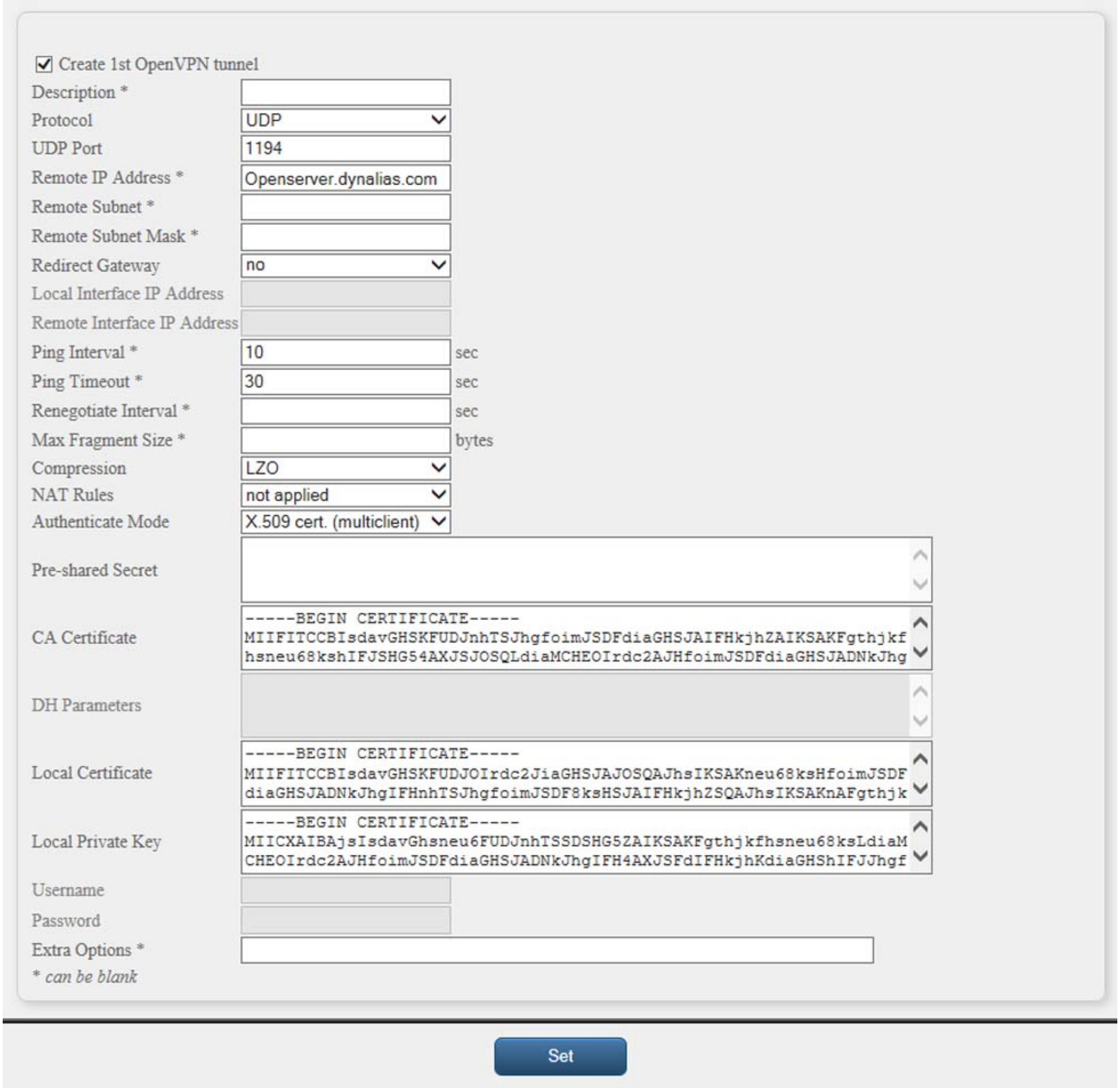


Figure 99: OpenVPN client to client

2.7.1 OpenVPN server configuration

```
server 10.8.0.0 255.255.255.0
port 1194
proto udp
dev tun
comp-lzo
keepalive 10 60
dh dh1024.pem
ca ca.crt
key server.key
cert server.crt
ifconfig-pool-persist ipp.txt
status openvpn-status.log
client-config-dir ccd
client-to-client
persist-key
persist-tun
verb 3
route 192.168.1.0 255.255.255.0
route 192.168.2.0 255.255.255.0
route 192.168.3.0 255.255.255.0
/ccd
/ccd/router1
iroute 192.168.1.0 255.255.255.0
push "route 192.168.2.0 255.255.255.0"
push "route 192.168.3.0 255.255.255.0"
push "route 192.168.10.0 255.255.255.0"
/ccd/router2
iroute 192.168.2.0 255.255.255.0
push "route 192.168.1.0 255.255.255.0"
push "route 192.168.3.0 255.255.255.0"
push "route 192.168.10.0 255.255.255.0"
/ccd/router3
iroute 192.168.3.0 255.255.255.0
push "route 192.168.1.0 255.255.255.0"
push "route 192.168.2.0 255.255.255.0"
push "route 192.168.10.0 255.255.255.0"
```

2.7.2 OpenVPN tunnel configuration on Hirschmann routers



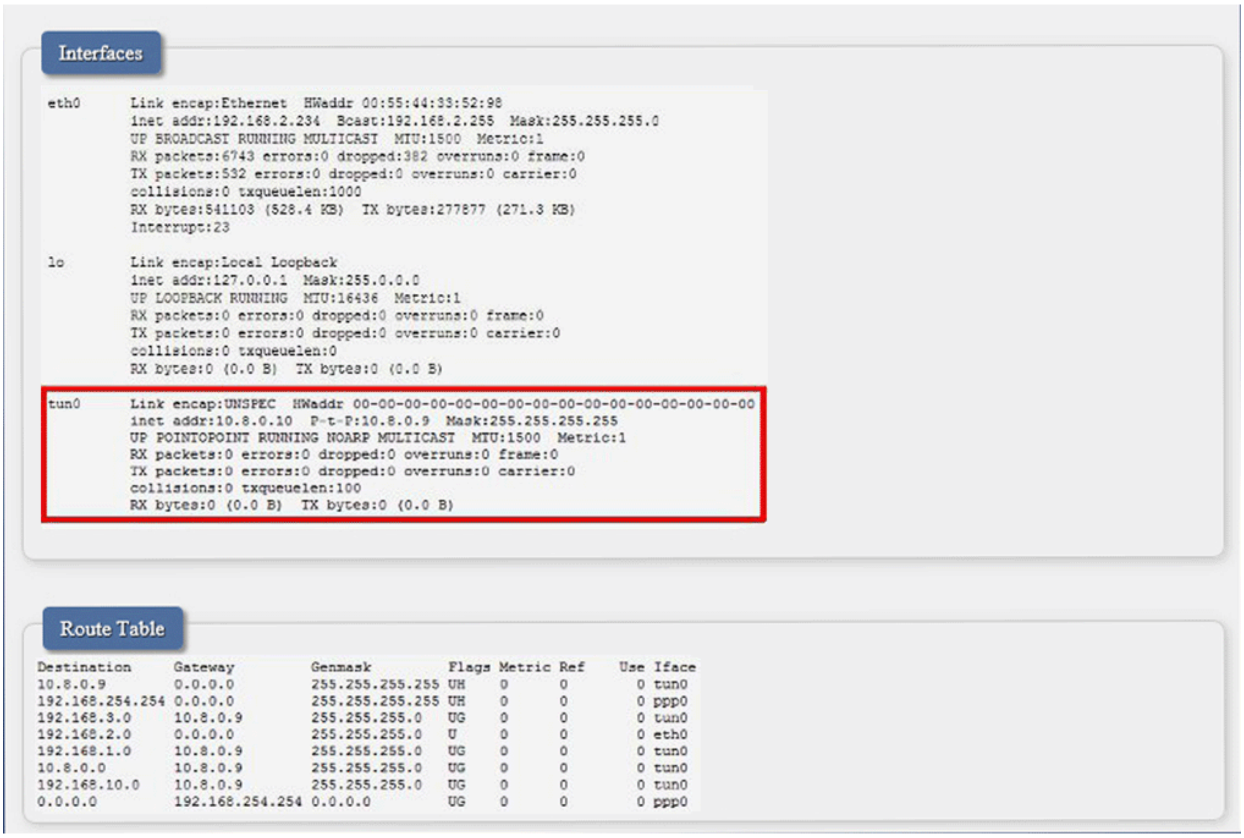
☑ Create 1st OpenVPN tunnel

Description *		
Protocol	UDP	
UDP Port	1194	
Remote IP Address *	Openserver.dynalias.com	
Remote Subnet *		
Remote Subnet Mask *		
Redirect Gateway	no	
Local Interface IP Address		
Remote Interface IP Address		
Ping Interval *	10	sec
Ping Timeout *	30	sec
Renegotiate Interval *		sec
Max Fragment Size *		bytes
Compression	LZO	
NAT Rules	not applied	
Authenticate Mode	X.509 cert. (multiclient)	
Pre-shared Secret		
CA Certificate	-----BEGIN CERTIFICATE----- MIIFITCCBIsdavGHSKFUDJnhTSJhgfoimJSDFdiaGHSJAIFHkjhZAIKSAKFgthjkf hsneu68kshIFJSHG54AXJSJOSQLdiaMCHEOIrdc2AJHfoimJSDFdiaGHSJADNkJhg	
DH Parameters		
Local Certificate	-----BEGIN CERTIFICATE----- MIIFITCCBIsdavGHSKFUDJOIrdc2JiaGHSJAJOSQAJhsIKSAKneu68ksHfoimJSDF diaGHSJADNkJhgIFHnhTSJhgfoimJSDF8ksHSJAIFHkjhZSQAJhsIKSAKnAFgthjk	
Local Private Key	-----BEGIN CERTIFICATE----- MIICXAIBAjsIsdavGhsneu6FUDJnhTSSDSHG5ZAIKSAKFgthjkfhsneu68ksLdiaM CHEOIrdc2AJHfoimJSDFdiaGHSJADNkJhgIFH4AXJSFdIFHkjhKdiaGHShIFJJhgf	
Username		
Password		
Extra Options *		

** can be blank*

Figure 100:Router configuration

After establishing an OpenVPN tunnel, the `Network> LAN Status` dialog displays the tun0 interface in the Interface section, and the associated route in the Route Table section.

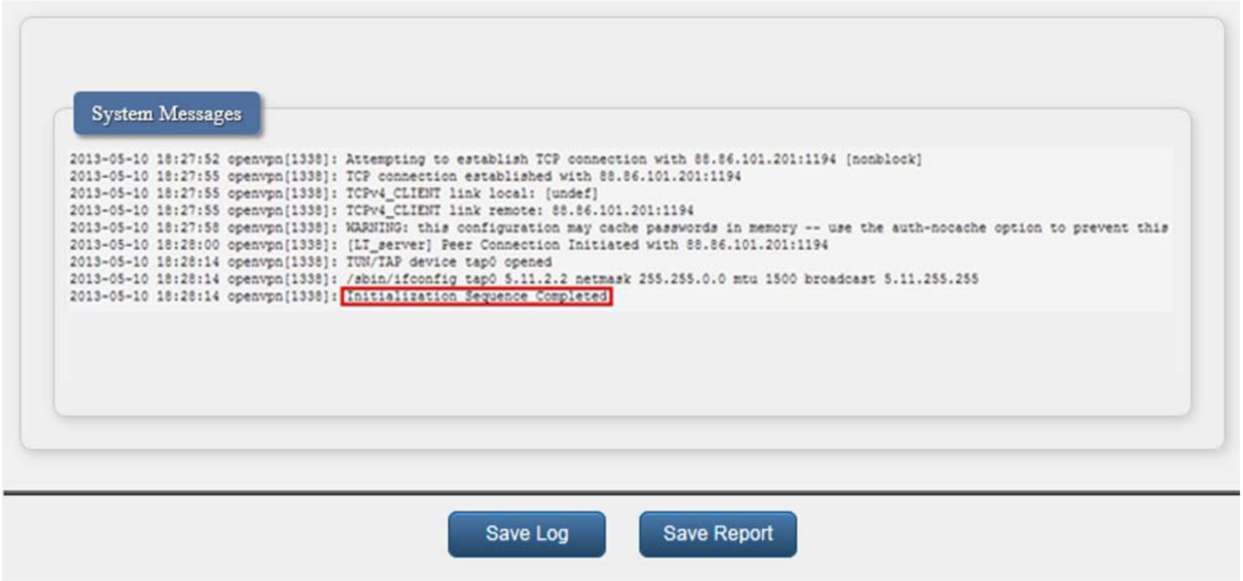


```
eth0      Link encap:Ethernet  HWaddr 00:55:44:33:52:98
          inet addr:192.168.2.234  Bcast:192.168.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6743 errors:0 dropped:382 overruns:0 frame:0
          TX packets:532 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:541103 (528.4 KB)  TX bytes:277877 (271.3 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)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.8.0.10  P-t-P:10.8.0.9  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP 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:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.8.0.9        0.0.0.0         255.255.255.255 UH    0      0        0 tun0
192.168.254.254 0.0.0.0         255.255.255.255 UH    0      0        0 ppp0
192.168.3.0     10.8.0.9        255.255.255.0   UG    0      0        0 tun0
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.1.0     10.8.0.9        255.255.255.0   UG    0      0        0 tun0
10.8.0.0        10.8.0.9        255.255.255.0   UG    0      0        0 tun0
192.168.10.0    10.8.0.9        255.255.255.0   UG    0      0        0 tun0
0.0.0.0         192.168.254.254 0.0.0.0         UG    0      0        0 ppp0
```

Figure 101:Network Status

It is also possible to verify a successful establishment of the OpenVPN tunnel in the system log, click `System Log` in menu tree. After the router establishes an OpenVPN tunnel, the log displays the “`Initialization Sequence Completed`” entry.



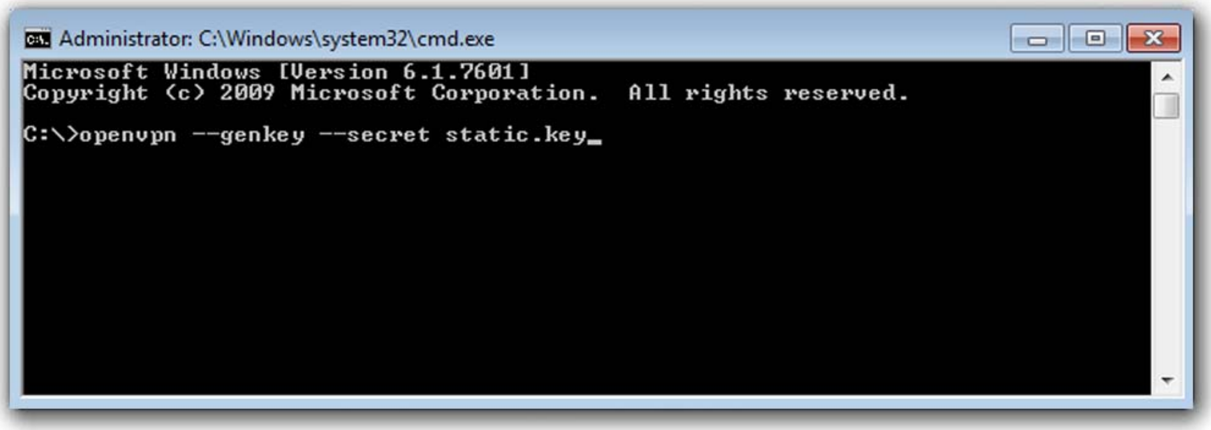
```
2013-05-10 18:27:52 openvpn[1338]: Attempting to establish TCP connection with 88.86.101.201:1194 [nonblock]
2013-05-10 18:27:55 openvpn[1338]: TCP connection established with 88.86.101.201:1194
2013-05-10 18:27:55 openvpn[1338]: TCPv4_CLIENT link local: [undef]
2013-05-10 18:27:55 openvpn[1338]: TCPv4_CLIENT link remote: 88.86.101.201:1194
2013-05-10 18:27:58 openvpn[1338]: WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2013-05-10 18:28:00 openvpn[1338]: [LT_server] Peer Connection Initiated with 88.86.101.201:1194
2013-05-10 18:28:14 openvpn[1338]: TUN/TAP device tap0 opened
2013-05-10 18:28:14 openvpn[1338]: /sbin/ifconfig tap0 5.11.2.2 netmask 255.255.0.0 mtu 1500 broadcast 5.11.255.255
2013-05-10 18:28:14 openvpn[1338]: Initialization Sequence Completed
```

Figure 102:System log

2.8 Creation of pre-shared key

For creating a pre-shared key it is needed to have installed the program OpenVPN. For description of the installation of OpenVPN: See “Installation of OpenVPN (Windows)” on page 273.

The figure below describes a way to easily generate a pre-shared key. It is then inserted into the Pre-shared Secret box in the form for configuration of OpenVPN tunnel.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>openvpn --genkey --secret static.key_
```

Figure 103:Generating a pre-shared key

Example of pre-shared key:

```
#
# 2048 bit OpenVPN static key
# -----BEGIN OpenVPN Static key V1-----

ac53ce6bf3ac2605bd3653fd66a113a4
373d57375763de58a38992f580efb97b
817e1b6d61ffbbf559ed9d2c927cef13
39baa06de34c7b4b05df6d4971aa97d0
ec72e4465af647a89e82b335db3dcbb8
a7dd9d190960215ac137e8e2456d2deb
4446b74b3360fe5bf0ac565d4a253a78
9823fd9891db70e190926dbf557c5ad9
cbdb7c0a649a1948b3e5dccce838fc4c
fd6e12b69b7d6bea95c87ee670e85fb1
8ac594f8a9a56921bb2e423dbcd3cbad
650d1543e486ffb956e7a9780925adfe
369e32c5913674bb655b414bde5eb6a0
184c6f2a51f648285f0ab91ea2fe8a20
a9bc715fe96301af90f41f17432e79e3
-----END OpenVPN Static key V1-----
```

2.9 Creation of certificates

For creating certificates it is needed to have installed the program OpenVPN. For description of the installation of OpenVPN:
See “Installation of OpenVPN (Windows)” on page 273.

2.9.1 Introduction

Digital certificates are digitally signed public encryption keys. They are issued by a certification authority (CA). Certificates are kept in X.509 format, which contains information such as the owner of the public key, the certificate issuer or the creator of the digital signature. Certificates are used to identify the counter party when creating a secure connection (HTTPS, VPN, etc.). On the basis of principle of a trust transfer, it is possible to trust unknown certificates signed by trusted certification authorities. It is typically used a hierarchical model.

2.9.2 Generating certificates

In the folder with the OpenVPN program (by default: C: Program Files OpenVPN) is easy-rsa directory in which vars.bat.sample file is saved.

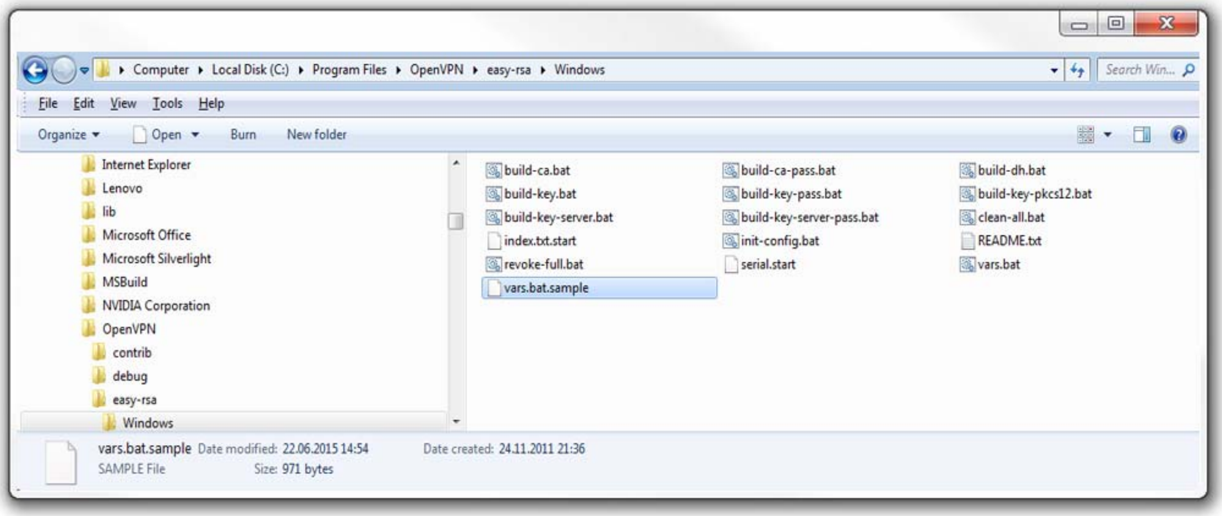


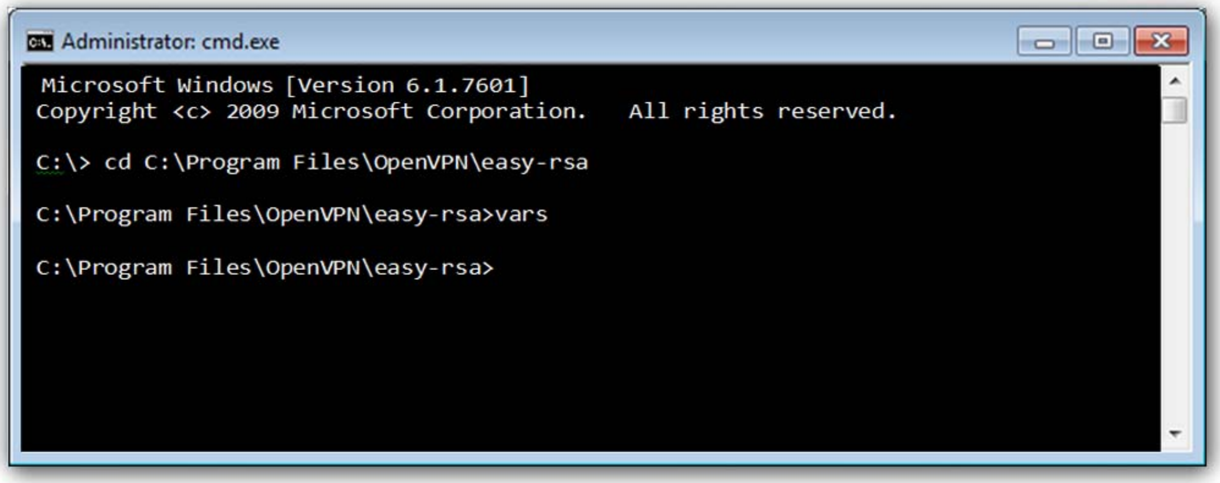
Figure 104:easy-rsa directory

This file needs to be opened using any text editor and filled in according to the instructions. It is recommended to enter values to all rows starting with the keyword set. After completing this file must be saved as vars.bat.

Example:

```
@echo off
set HOME=%ProgramFiles%\OpenVPN\easy-rsa set
KEY_CONFIG=openssl-1.0.0.cnf
set KEY_DIR=keys set KEY_SIZE=1024 set KEY_COUNTRY=DE set
KEY_PROVINCE=PA
set KEY_CITY=Neckartenzlingen set KEY_ORG=Hirschmann
set KEY_EMAIL=test@Hirschmann.de
```

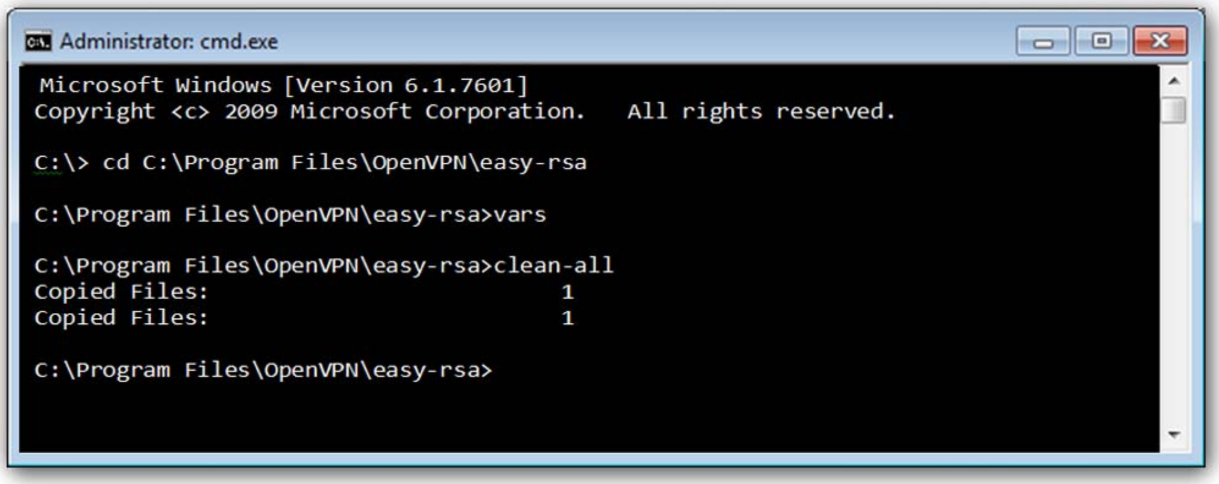
It is necessary to load the file vars.bat, which can be done using the command line:



```
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation.   All rights reserved.

C:\> cd C:\Program Files\OpenVPN\easy-rsa

C:\Program Files\OpenVPN\easy-rsa>vars

C:\Program Files\OpenVPN\easy-rsa>
```

Figure 105:vars.bat loading.

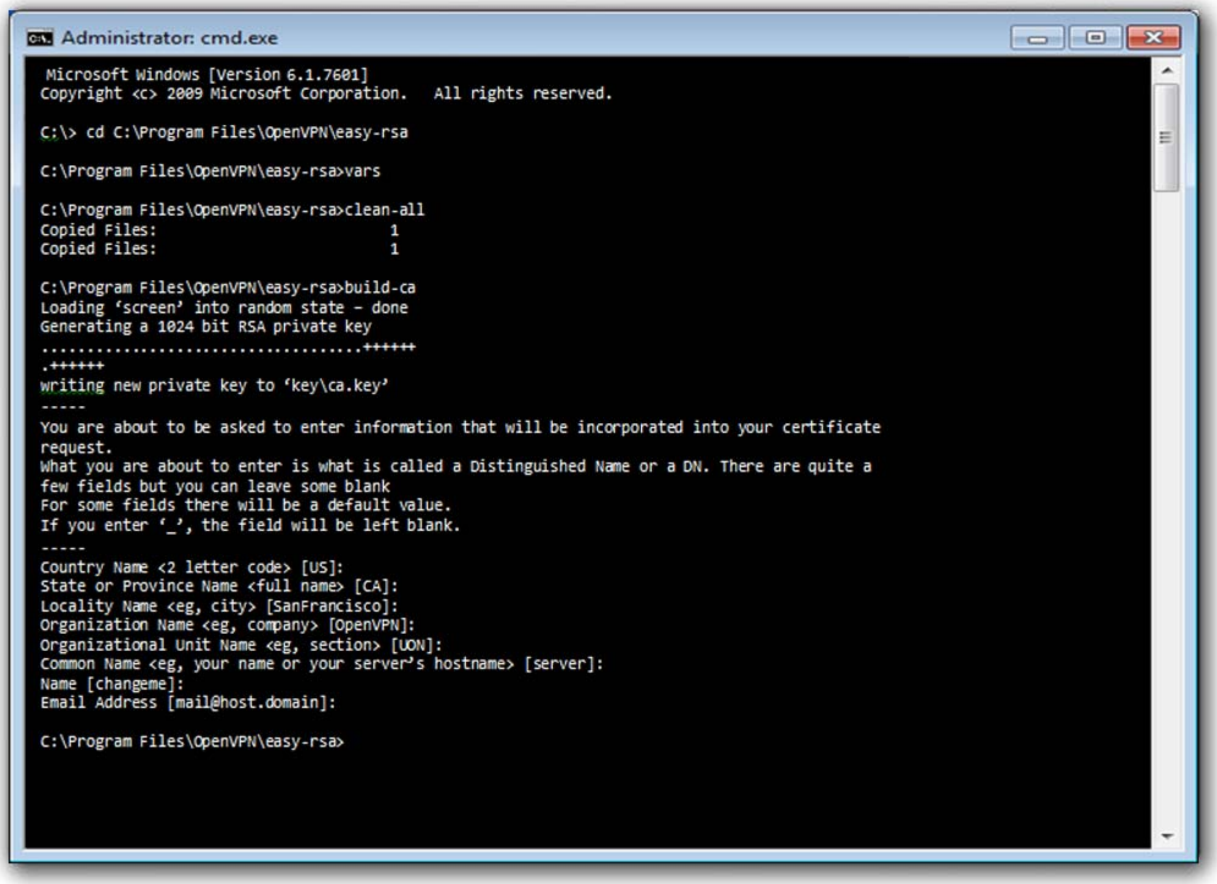
To delete the previously generated certificates that were saved in the directory, use the clean-all command:



```
 Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation.   All rights reserved.

C:\> cd C:\Program Files\OpenVPN\easy-rsa

C:\Program Files\OpenVPN\easy-rsa>vars

C:\Program Files\OpenVPN\easy-rsa>clean-all
Copied Files:                         1
Copied Files:                         1

C:\Program Files\OpenVPN\easy-rsa>
```

Figure 106:clean-all command.

To generate a certificate authority (CA), use the `build-ca` command:



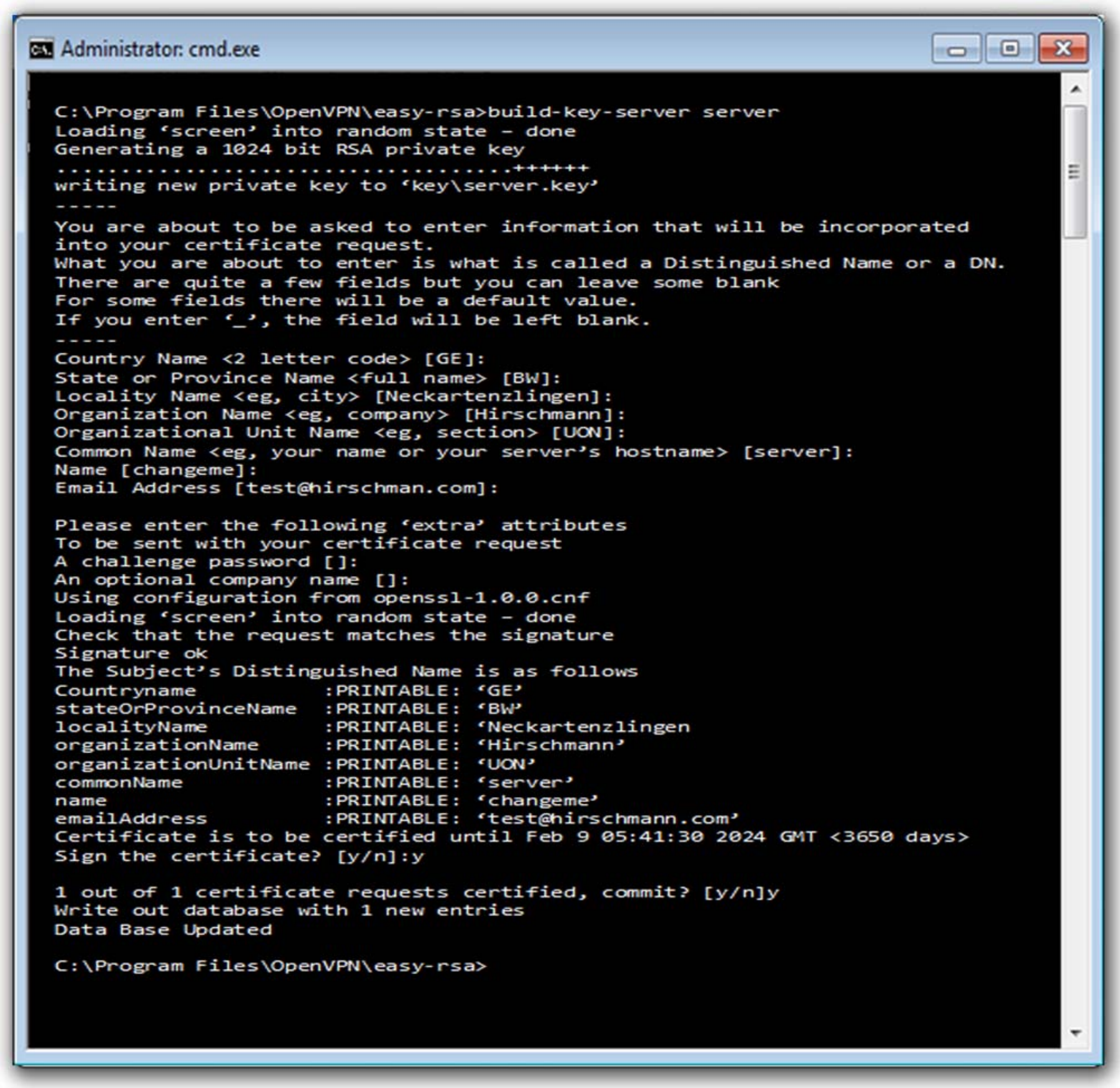
```
 Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation.   All rights reserved.

C:\> cd C:\Program Files\OpenVPN\easy-rsa

C:\Program Files\OpenVPN\easy-rsa>vars

C:\Program Files\OpenVPN\easy-rsa>clean-all
Copied Files:                         1
Copied Files:                         1

C:\Program Files\OpenVPN\easy-rsa>build-ca
Loading ‘screen’ into random state - done
Generating a 1024 bit RSA private key
..................................++++++
.++++++
writing new private key to ‘key\ca.key’
-----
You are about to be asked to enter information that will be incorporated into your certificate
request.
What you are about to enter is what is called a Distinguished Name or a DN. There are quite a
few fields but you can leave some blank
For some fields there will be a default value.
If you enter ‘_’, the field will be left blank.
-----
Country Name <2 letter code> [US]:
State or Province Name <full name> [CA]:
Locality Name <eg, city> [SanFrancisco]:
Organization Name <eg, company> [OpenVPN]:
Organizational Unit Name <eg, section> [UON]:
Common Name <eg, your name or your server’s hostname> [server]:
Name [changeme]:
Email Address [mail@host.domain]:

C:\Program Files\OpenVPN\easy-rsa>
```

Figure 107:Generating a certificate authority

Note: The `Common name` value must be filled in for servers and individual clients differently for example, server, client01, client02.

Now it is already possible to generate certificates and keys for elements in the network (server, client01, client02, …). For servers, use the `build-key-server server` command. For clients, use `build-key clientXY` command, where the clientXY term means a particular client (client01, client02, …). It follows that the certificates and keys must be generated for each element in the network separately.

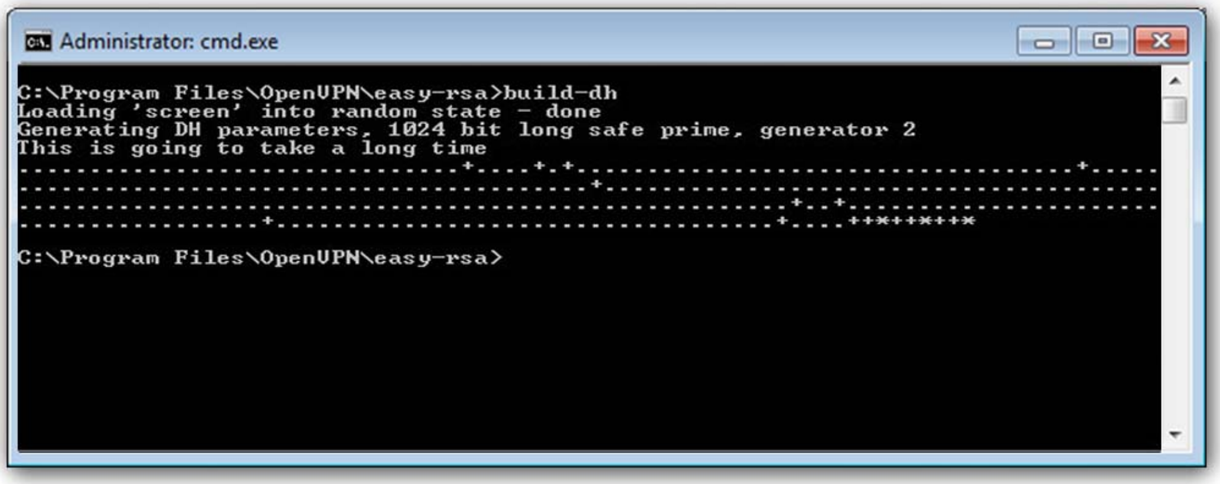
The following figure (on next page) shows the progress of generating certificates and keys for the server, which is called as server. A process for generating certificates and keys for each client is the same.



```
C:\Program Files\OpenVPN\easy-rsa>build-key-server server
Loading ‘screen’ into random state – done
Generating a 1024 bit RSA private key
....................................++++++
writing new private key to ‘key\server.key’
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value.
If you enter ‘_’, the field will be left blank.
-----
Country Name <2 letter code> [GE]:
State or Province Name <full name> [BW]:
Locality Name <eg, city> [Neckartenzlingen]:
Organization Name <eg, company> [Hirschmann]:
Organizational Unit Name <eg, section> [UON]:
Common Name <eg, your name or your server’s hostname> [server]:
Name [changeme]:
Email Address [test@hirschman.com]:

Please enter the following ‘extra’ attributes
To be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from openssl-1.0.0.cnf
Loading ‘screen’ into random state – done
Check that the request matches the signature
Signature ok
The Subject’s Distinguished Name is as follows
Countryname          :PRINTABLE: ‘GE’
stateOrProvinceName  :PRINTABLE: ‘BW’
localityName         :PRINTABLE: ‘Neckartenzlingen
organizationName     :PRINTABLE: ‘Hirschmann’
organizationUnitName :PRINTABLE: ‘UON’
commonName           :PRINTABLE: ‘server’
name                 :PRINTABLE: ‘changeme’
emailAddress         :PRINTABLE: ‘test@hirschmann.com’
Certificate is to be certified until Feb 9 05:41:30 2024 GMT <3650 days>
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

C:\Program Files\OpenVPN\easy-rsa>
```

Figure 108:generating certificates and keys

Finally, generate a Diffie-Hellman key (DH key) using the `build-dh` command (see figure below).



```
C:\Program Files\OpenVPN\easy-rsa>build-dh
Loading 'screen' into random state - done
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
...............................+....+.+...................................+.....
........................................+.......................................
......................................................+..+......................
.................+...................................+....++*++*++*

C:\Program Files\OpenVPN\easy-rsa>
```

Figure 109:generating DH key

2.9.3 Overview of the generated files

The following table describes the meaning of the generated files and their location (uploading to server or client).

File	Description	Location
server.crt	Signed certificate of VPN server	server
server.key	Personal RSA key of VPN server	server
server.csr	Request for signing	it's possible to delete it
client01.crt	Signed certificate of VPN client	client
client01.key	Personal RSA key of VPN client	client
client01.csr	Request for signing	it's possible to delete it
ca.crt	CA certificate	clients and server
ca.key	Key to k CA	secret and secure repository
dh1024.pem	Diffie-Hellmann key	only server

Table 69: Overview of the generated files

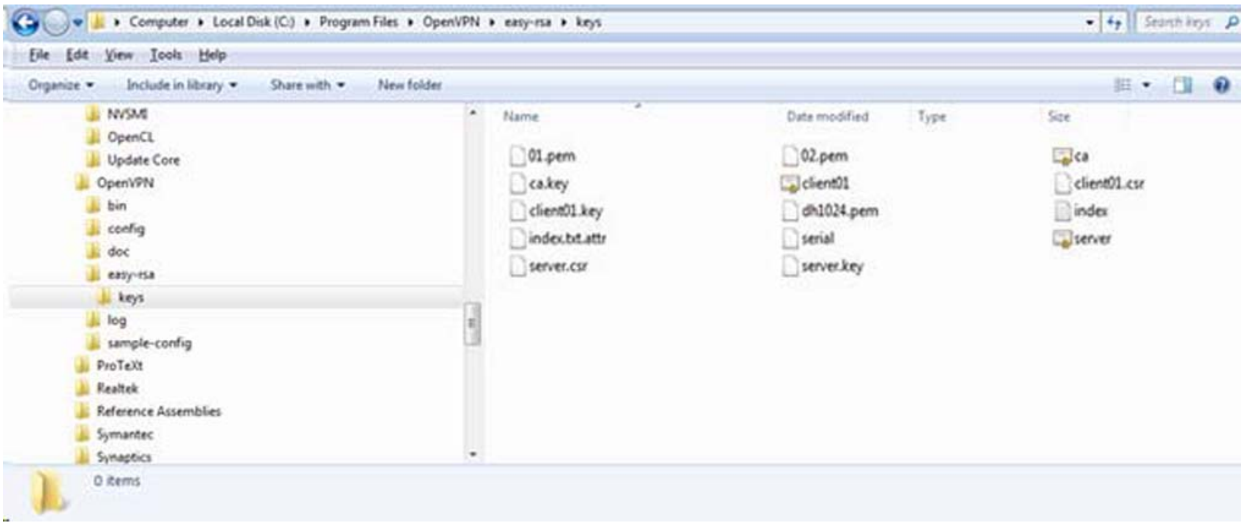


Figure 110:Overview of the generated files

3 Commands and Scripts

arp

The arp program displays and modifies the Internet-to-Ethernet address translation tables used by the address resolution protocol.

Synopsis:

```
arp [-a <hostname>] [-s <hostname> <hw_addr>] [-d <hostname>] [-v] [-n] [-
i <if>] [-D <hostname>] [-A ] [-f <filename>]
```

Options:

Option	Description
-a	The entries will be displayed in alternate (BSD) style.
-s	Manually create an ARP address mapping entry for hostname with hardware address set to hw_addr.
-d	Remove any entry for the specified host.
-v	Tell the user what is going on by being verbose.
-n	Shows numerical addresses instead of trying to determine symbolic host, port or user names.
-i	Select an interface.
-D	Use the interface if as hardware address.
-f	Similar to the -s option, only with this option the address info is taken from file filename set up. The name of the data file is very often /etc/ethers, but this is not official. If no filename is specified, /etc/ethers is used as default.The format of the file is simple; it only contains ASCII text lines with a hardware address and a hostname separated by whitespace. Additionally the pub, temp and netmask flags can be used

Table 70: arp options

With no flags, the program displays the current ARP entry for hostname. The host may be specified by name or by number, using Internet dot notation. For detail description of this command, visit Linux manual pages.

Examples:

View arp table without translating IP addresses to domain names

```
arp -n
```

■ awk

Awk scans each input file for lines that match any of a set of patterns specified literally in program-text or in one or more files specified as -f progfile.

Synopsis:

```
awk [-v] [-F] [-f] …[<program-text>] [<file> …]
```

Options:

Option	Description
-v	Assign the value `val` to the variable `var`, before execution of the program begins. Such variable values are available to the BEGIN block of an AWK program.
-F	Use for the input field separator (the value of the FS predefined variable).
-f	Read the AWK program source from the file program-file, instead of from the first command line argument. Multiple -f (or –file) options may be used.

Table 71: awk options

Examples:

Show IP address of Gateway

```
route -n | awk ’/^0 .0 .0 .0/ { print $2 }
```

brctl

The brctl command is used to set up, maintain, and inspect the Ethernet bridge configuration in the Linux kernel.

An Ethernet bridge is a device commonly used to connect different networks of Ethernets together, so that these Ethernets will appear as one Ethernet to the participants.

Each of the Ethernets being connected corresponds to one physical interface in the bridge. These individual Ethernets are bundled into one bigger (’logical’) Ethernet, this bigger Ethernet corresponds to the bridge network interface.

Synopsis:

```
brctl [<commands>]
```

Options:

Option	Parameters	Description
addbr	<bridge>	Add bridge
delbr	<bridge>	Delete bridge
addif	<bridge> <device>	Add interface to bridge
delif	<bridge> <device>	Delete interface from bridge
setageing	<bridge> <time>	Set aging time
setbridgepri	<bridge> <prio>	Set bridge priority
setfd	<bridge> <time>	Set bridge forward delay
sethello	<bridge> <time>	Set hello time
setmaxage	<bridge> <time>	Set max message age
setpathcost	<bridge> <port> <cost>	Set path cost
setportrpio	<bridge> <port> <prio>	Set port prioriy
show		Show list of bridges
showmacs	<bridge>	Show list of mac address
showstp	<bridge>	Show bridge stp info
stp	<bridge> {on | off}	Turn stp on/off

Table 72: brctl commands

Examples:

Create bridge between eth0 and eth1.

```
brctl addbr br0
brctl addif br0 eth0
brctl addif br0 eth1
```

■ cat

This command concatenates files and print on the standard output.

Synopsis:

```
cat [-u] [<file>] …
```

Options:

Option	Description
-u	Ignored since unbuffered I/O is always used.

Table 73: cat options

Examples:

View the contents of file /proc/tty/driver/spear_serial (info about serial ports of v2 routers).

```
cat /proc/tty/driver/spear_serial
```

Copy the contents of the router configuration files in /tmp/my.cfg.

```
cat /etc/settings.* > /tmp/my.cfg
```

■ cd

This command is used to change the current working directory.

Synopsis:

```
cd [-P] [-L] [<directory>]
```

Options:

Option	Description
-P	Do not follow symbolic links
-L	Follow symbolic links (default)

Table 74: cd options

Examples:

Move to home directory (/root).

```
cd
```

Move to directory /mnt.

```
cd /mmt
```

cdmaat

The program used for sending AT command to CDMA module if available (equivalent of the gsmat command, See “gsmat” on page 179.)

Synopsis:

```
cdmaat <AT command>
```

cdmapwr

The program used to control the supply of CDMA module if available (equivalent of the gsmpwr command, See “gsmpwr” on page 181.)

Synopsis:

```
cdmapwr [on | off]
```

chmod

This command is used to change file mode bits.

Synopsis:

```
chmod [-R] <mode> <filename>
```

Options:

Option	Description
-R	Change files and directories recursively

Table 75: chmod options

Examples:

Settings rights (permit execution) of script /tmp/script.

```
chmod 755 /tmp/script
```

conntrack

This program is user interface to netfilter connection tracking system.

Synopsis:

```
conntrack [commands] [option]
```

Options:

Command	Description
-L [table] [option]	List conntrack or expectation table
-G [table]	Get conntrack or expectation
-D [table]	Delete conntrack or expectation
-I [table]	Create a conntrack or expectation
-U [table]	Update a conntrack
-E [table]	Show events
-F [table]	Flush table

Table 76: conntrack comands

Table	Description
conntrack	This is the default table. It contains a list of all currently trackedconnections through the system.
expect	This is the table of expectations. Connection tracking expectationsare the mechanism used to "expect" RELATED connectionsto existing ones.

Table 77: conntrack tables

Option	Description
-n <ip>	Source NAT ip
-g <ip>	Destination NAT ip
-m <mark>	Set mark
-e <eventmask>	Event mask, eg. NEW,DESTROY
-z	Zero counters while listing
-o <type[...]>	Output format, eg. xml

Table 78: conntrack options

Option	Description
--tuple-src <ip>	Source address in expect tuple
--tuple-dst <ip>	Destination address in expect tuple
--mask-src <ip>	Source mask address
--mask-dst <ip>	Destination mask address

Table 79: expectation options

Option	Description
-s <ip>	Source address from original direction
-d <ip>	Destination address from original direction
-r <ip>	Source addres from reply direction
-q <ip>	Destination address from reply direction
-p <proto>	Layer 4 Protocol, eg. ’tcp’
-f <proto>	Layer 3 Protocol, eg. ’ipv6’
-t <timeout>	Set timeout
-u <status>	Set status, eg. ASSURED

Table 80: conntrack and expectation options

Examples:

Display content of conntrack table.

```
conntrack -L
```

Delete content of contrack table.

```
conntrack -F
```

cp

This command is used to copy files and directories.

Synopsis:

```
cp [<option>] <source> <dest>
```

Options:

Option	Description
-a	Preserve the all attributes
-d, -P	Never follow symbolic links
-H, -L	Follow command-line symbolic links
-p	Preserve the mode, ownership, timestamps attributes
-f	If an existing destination file cannot be opened, remove it and try again
-i	Prompt before overwrite
-R, -r	Copy directories recursively

Table 81: cp options

Examples:

Copy the system log to directory /mnt.

```
cp /var/log/messages* /mnt
```

Copy configuration profile "Alternative 1" to profile "Standard".

```
cp -r /etc/alt1/* /etc
```

curl

Curl (transfer a URL) is a tool to transfer data from or to a server, using one of the supported protocols (DICT, FILE, FTP, FTPS, GOPHER, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMTP, SMTPS, TELNET and TFTP). It is an alternative to wget .See “wget” on page 212.

Synopsis:

```
curl [options...] <url>
```

Options:

Type curl --help for options to show in the command line or visit online manual page at

```
http://curl.haxx.se/docs/manpage.html
```

date

This command is used to display the current time in the given FORMAT, or set the system date (and time).

Synopsis:

```
date [-R] [-d <string>] [-s] [-r <file>] [-u] [MMDDhhmm[[CC]YY][.ss]]
```

Options:

Option	Description
-R	Output date and time in RFC 2822 format
-d <string>	Display time described by STRING, not ’now’
-s	Set time described by STRING
-r <file>	Display the last modification time of FILE
-u	Print or set Coordinated Universal Time

Table 82: date options

Examples:

Display the current date and time.

```
date
```

Setting the date and time on December 24, 2011 20:00.

```
date 122420002011
```

defaults

The script is used to restore the default configuration.

Synopsis:

```
defaults
```

df

This command is used to view report file system disk space usage.

Synopsis:

```
df [-k] [<filesystem> …]
```

Options:

Option	Description
-k	Print sizes in kilobytes

Table 83: df options

dmesg

This command is used to print or control the kernel ring buffer.

Synopsis:

```
dmesg [-c] [-n <level>] [-s <size>]
```

Options:

Option	Description
-c	Clears the ring buffer’s contents after printing
-n <level>	Set the level at which logging of messages is done to the console
-s <size>	Use a buffer of size SIZE to query the kernel ring buffer. This is 16392 bydefault.

Table 84: dmesg options

Examples:

View the latest news and subsequent deletion of the kernel ring buffer.

```
dmesg -c
```

echo

This command prints the strings to standard output.

Synopsis:

```
echo [-n] [-e] [-E] [<string> ...]
```

Options:

Option	Description
-n	Do not output the trailing newline
-e <level>	Enable interpretation of backslash escapes
-E <size>	Disable interpretation of backslash escapes (default)

Table 85: echo options

Examples:

Switch profile to "Standard".

```
echo "PROFILE=" > /etc/settings
reboot
```

Switch profile to "Alternative 1".

```
echo "PROFILE=alt1" > /etc/settingsreboot
```

Send a sequence of bytes 0x41,0x54,0x0D,0x0A to serial line (write data in octal).

```
echo -n -e " 101 124 015 012" > /dev/ttyS0
```

■ email

The program used for sending email.

Synopsis:

```
email -t <to> [-s <subject>] [-m <message>] [-a <attachment>] [-r <retries>]
```

Options:

Option	Description
-t	Email of recipient
-s	Subject of email
-m	Message of email
-a	Attachment of email
-r	Number of retries

Table 86: email options

Examples:

Send system logs to the address john.doe@email.com.

```
email -t john.doe@email.com -s "System Log" -a /var/log/messages
```

■ ethtool

This command is used to display or change Ethernet card settings.

Synopsis:

```
ethtool [<option> …] <devname> [<commands>]
```

Options:

For detail description this command, visit Linux manual pages.

Examples:

View the status of the interface eth0.

```
ethtool eth0
```

Switch interface eth0 to mode 10 Mbit/s, half duplex.

```
ethtool -s eth0 speed 10 duplex half autoneg off
```

Turn on autonegacion on the interface eth0.

```
ethtool -s eth0 autoneg on
```

■ find

Command to search for files in a directory hierarchy.

Synopsis:
find [<path> …] [<expression>]

Options:
The default path is the current directory, default expression is ’-print’. Type find --help for help or look up online man page for more detailed description. Expression may consist of:

Option	Description
-follow	Dereference symbolic links
-name <pattern>	File name (leading directories removed) matches <pattern>
-print	Print (default and assumed)
-type X	Filetype matches X (where X is one of: f,d,l,b,c,…)
-perm <perms>	Permissions match any of (+NNN); all of (-NNN); or exactly (NNN)
-mtime <days>	Modified time is greater than (+N); less than (-N); or exactly (N) days
-mmin <mins>	Modified time is greater than (+N); less than (-N); or exactly (N) minutes
-exec <cmd>	Execute command with all instances of {} replaced by the files matching <expression>

Table 87: find expressions

Examples:

Search for files in your home directory which have been modified in the last twenty-four hours.

```
find $HOME -mtime 0
```

Search for files which have read and write permission for their owner, and group, but which other users can read but not write to. find

```
-perm 664
```

■ free

This command is used to display information about free and used memory.

Synopsis:

```
free
```

fwupdate

The program used for router’s firmware update.

Synopsis:
fwupdate [-i <filename> [-h] [-n]] [-f]

Options:

Option	Description
-i	File of the new firmware, filename has to be specified
-h	HTML output (used when called from web configuration)
-n	Do not reboot after firmware update
-f	finish update procedures, called by default

Table 88: fwupdate options

grep

Grep searches the named input FILEs (or standard input if no files are named, or the file name – is given) for lines containing a match to the given PATTERN. By default, grep prints the matching lines.

Synopsis:

```
grep [<options> …] <pattern> [<file> …]
```

Options:

Option	Description
-H	Print the filename for each match
-h	Suppress the prefixing of filenames on output when multiple files are searched
-i	Ignore case distinctions
-l	Suppress normal output; instead print the name of each input file from which output would normally have been printed
-L	Suppress normal output; instead print the name of each input file from which no output would normally have been printed
-n	Prefix each line of output with the line number within its input file
-q	Quiet; do not write anything to standard output. Exit immediately with zero status if any match is found, even if an error was detected. Also see the -s or --no-messages option.
-v	Invert the sense of matching, to select non-matching lines
-s	Suppress error messages about nonexistent or unreadable files
-c	Suppress normal output; instead print a count of matching lines for each input file
-f	Obtain patterns from FILE, one per line
-e	Use PATTERN as the pattern; useful to protect patterns beginning with –
-F	Interpret PATTERN as a list of fixed strings, separated by new lines, any of which is to be matched

Table 89: grep options

Examples:

See all lines of system log in which occurs the word "error".

```
grep error /var/log/messages
```

View all processes whose name the contents of the string "ppp".

```
ps | grep ppp
```

gsmat

The program used for sending AT command to GSM module.

Synopsis:

```
gsmat <AT command>
```

Examples:

Determine the type and firmware version of GSM module.

```
gsmat ATI
```

Determine the IMEI code of module.

```
gsmat "AT+GSN"
```

gsmat2

The program used for sending AT command to second GSM module if available.

Synopsis:

```
gsmat2 <AT command>
```

gsminfo

The program used to display information about the signal quality.

Synopsis:

Synopsis:
gsminfo

Options:

Option	Description
PLMN	Code of operator
Cell	The cell to which the router is connected
Channel	The channel on which the router communicates
Level	The signal quality of the selected cell
Neighbours	Signal quality of neighboring hearing cells
Uptime	Time to establish PPP connection

Table 90: Description of GSM information

■ gsmpwr

The program used to control the supply of GSM module.

Synopsis:

```
gsmpwr [on | off]
```

Examples:

Power of GSM module is turning on.

```
gsmpwr on
```

Power of GSM module is turning off.

```
gsmpwr off
```

■ gsmpwr2

The program used to control the supply of second GSM module if available.

Synopsis:

```
gsmpwr2 [on | off]
```

■ gsmsms

The program used to send SMS message.

Synopsis:

```
gsmsms <phone number> <text>
```

Examples:

Send SMS "Hello word" on telephone number +420123456789.

```
gsmsms +420123456789 "Hello word"
```

gunzip

This program is used to decompress FILE (or standard input if filename is '–').

Synopsis:

```
gunzip [-c] [-f] [-t] <filename>
```

Options:

Option	Description
-c	Write output on standard output
-f	Force decompression even if the file has multiple links or the corresp. filealready exists, or if the compressed data is read from or written to a terminal.
-t	Test. Check the compressed file integrity.

Table 91: gunzip options

Examples:

Decompression of file test.tar.gz (creates file test.tar).

```
gunzip test.tar.gz
```

gzip

This program is used to compress FILE with maximum compression.

Synopsis:

```
gzip [-c] [-d] [-f] <filename>
```

Options:

Option	Description
-c	Write output on standard output
-d	Decompress
-f	Force compression even if the file has multiple links or the corresponding file already exists, or if the compressed data is read from or written to a terminal

Table 92: gzip options

Examples:

Compression of file test.tar (creates file test.tar.gz).

```
gzip test.tar
```

hwclock

This program is used to query and set the hardware clock (RTC).

Synopsis:

```
hwclock [-r] [-s] [-w] [-u] [-l]
```

Options:

Option	Description
-r	Read hardware clock a print result
-s	Set the System Time from the Hardware Clock
-w	Set the Hardware Clock to the current System Time
-u	The hardware clock is kept in coordinated universal time
-l	The hardware clock is kept in local time

Table 93: hwclock options

Examples:

Set the hardware clock to the current system time.

```
hwclock -w -u
```

ifconfig

This command is used to configure a network interface.

Synopsis:

```
ifconfig [-a] <interface> [<option> …]
```

Options:

Option	Description
broadcast <addr.>	If the address argument is given, set the protocol broadcast addressfor this interface.
pointtopoint <ad.>	This keyword enables the point-to-point mode of an interface,meaning that it is a direct link between two machines with nobodyelse listening on it.
netmask <address>	Set the IP network mask for this interface.
dstaddr <address>	Set the remote IP address for a point-to-point link (such as PPP).
metric <NN>	This parameter sets the interface metric.
mtu <NN>	This parameter sets the Maximum Transfer Unit of an interface.
trailers	This flag used to cause a non-standard encapsulation of inet packets on certain link levels.
arp	Enable or disable the use of the ARP protocol on this interface.
allmulti	Enable or disable all-multicast mode. If selected, all multicastpackets on the network will be received by the interface.
multicast	Set the multicast flag on the interface. This should not normally be needed as the drivers set the flag correctly them-selves.
promisc	Enable or disable the promiscuous mode of the interface. If selected, all packets on the network will be received by the interface.
txqueuelen <NN>	Set the length of the transmit queue of the device.
up | down	This flag causes the interface to be activated. | This flag causes the driver for this interface to be shut down.

Table 94: ifconfig options

Examples:

View the status of all interfaces.

```
ifconfig
```

Activation of loopback with IP address 127.0.0.1/8.

```
ifconfig lo up
```

Activation of virtual interface eth0:0 with IP address

```
192.168.2.1/24.ifconfig eth0:0 192.168.2.1 netmask 255.255.255.0 up
```

io

The program is used to control outputs and read inputs. Supports reading state of binary outputs and setting state of counters.

Synopsis:

```
io [get <pin>] | [set <pin> <value>]
```

Options:

Option	Description
get	Set output
set	Determine state of input

Table 95: io options

Examples:

Set the state of binary output OUT0 to 1.

```
io set out0 1
```

Determine the state of digital input BIN0.

```
io get bin0
```

Note: The
Note: io get bin0
Note: command returns a logical `0` if the corresponding digital input is set to a logical `1`.

Determine the state of analog input AN1 on expansion port XC-CNT.

```
io get an1
```

Determine the state of counter input CNT1 on expansion port XC-CNT.

```
io get cnt1
```

ip

This command is used to configure a network interface or show the current configuration. Type ip --help for help in the terminal.

The OWL routers support more ip options and commands (options: -d[etails] , -t[imestamp , -b[atch] <filename> , -rc[vbuf] ; objects: addrlabel , ntable , tuntap , mrule , netns , l2tp , tcp_metrics , token). For information how to use, type ip <object> help , for detailed description of all options, visit Linux manual pages or look up them online.

Synopsis:

```
ip [ <options> ] <object> { <command> | help }
```

Options:

Option	Description
-V[ersion]	Print the version of the ip utility and exit
-s[tatistics]	Output more information. If the option appears twice or more, the amount of information increases.
-r[esolve]	use the system’s name resolver to print DNS names instead of host addresses
-f[amily] <family>	Specifies the protocol family to use. The protocol family identifier can be one of inet, inet6, bridge, ipx, dnet or link.
-o[neline]	output each record on a single line, replacing line feeds with the ’\’ character

Table 96: ip options

Object	Description
link	network device
addr	protocol (IP or IPv6) address on a device
route	routing table entry
rule	rule in routing policy database
neigh	manage ARP or NDISC cache entries
tunnel	tunnel over IP
maddr	multicast address
mroute	multicast routing cache entry
monitor	watch for netlink messages
xfrm	manage IPSec policies

Table 97: ip objects

Examples:

View the status of all interfaces.

```
ip link show
```

View the route table.

```
ip route list
```

Add routing networks 192.168.3.0/24 through interface eth0.

```
ip route add 192.168.3.0/24 dev eth0
```

Add routing IP address 192.168.3.1 trough gateway 192.168.1.2.

```
ip route add 192.168.3.1 via 192.168.1.2
```

Add default gateway 192.168.1.2.

```
ip route add default via 192.168.1.2
```

■ iptables

This command is used to administration tool for IP packet filtering and NAT.

Synopsis:

```
iptables [<options>]
```

Options:
For detail description of this command visit Linux manual pages.

Examples:

Redirect incoming TCP connections to port 8080 on IP address 192.168.1.2 and port 80.

```
iptables -t nat -A napt -p tcp --dport 8080 -j DNAT --to-destination
192.168.1.2:80
```

■ kill

This command is used to terminate process.

Synopsis:

```
kill [ -<signal> ] <process-id> [ <process-id> …]
kill -l
```

Options:

Option	Description
-l	Print a list of signal names. These are found in /usr/include/linux/signal.h
-q	Do not complain if no processes were killed

Table 98: kill options

Examples:

End the process with PID 1234 by sending signal SIGTERM.

```
kill 1234
```

End the process with PID 1234 by sending signal SIGKILL.

```
kill -9 1234
```

killall

This command is used to kill all process with process name.

Synopsis:

```
killall [ -q] [ -<signal> ] <process-name> [<process-name> …]
```

Options:

Option	Description
-l	Print a list of signal names. These are found in /usr/include/linux/signal.h
-q	Do not complain if no processes were killed

Table 99: killall options

Examples:

End the all processes with name pppd by sending signal SIGTERM.

```
killall pppd
```

End the all processes with name pppd by sending signal SIGKILL.

```
killall -9 pppd
```

led

The program used to control the USR LED on the front panel of the router.

Synopsis:

```
led [on | off]
```

Options:

Option	Description
on	User LED is on
off	User LED is off

Table 100:led options

Examples:

Turn on USR LED.

```
led on
```

Turn off USR LED.

```
led off
```

ln

The program used to make links between files.

Synopsis:

```
ln [ option ] < target > …< link_name > | < directory >
```

Options:

Option	Description
-s	Make symbolic links instead of hard links
-f	Remove existing destination files
-n	No dereference symlinks – treat like normal file
-b	Make a backup of the target (if exists) before link operation
-S	Use suffix instead of when making backup files

Table 101:ln options

Examples:

Creating a symbolic link to file /var/log/messages called my.log.

```
ln -s /var/log/messages my.log
```

■ logger

The program makes entries in the system log. It provides a shell command interface to the system log module.

Synopsis:

```
logger [ option ] [ message …]
```

Options:

Option	Description
-i	Log the process id of the logger process with each line
-s	Log the message to standard error, as well as the system log
-f <file>	Log the specified file
-p <priority>	Enter the message with the specified priority. The priority may be specified numerically or as a facility.level pair.
-t <tag>	Mark every line in the log with the specified tag
-u <socket>	Write to socket as specified with socket instead of builtin syslog routines
-d	Use a datagram instead of a stream connection to this socket

Table 102: logger options

Examples:

Send the message System rebooted to the syslogd daemon.

```
logger System rebooted
```

Send the message System going down immediately!!! to the syslog daemon, at the emerg level and user facility.

```
logger -p user.emerg "System going down immediately!!!
```

lpm

Put the router into the low power mode and wake up on events specified by parameters (binary input or time interval). Router will wake up on the first event coming when more parameters specified.

This command works on OWL routers only due to hardware support.

Synopsis:

Synopsis:
lpm [-b] [-i <interval>]

Options:

Option	Description
-b	Wake up the router on binary input In1
-i	Wake up the router after time interval specified in seconds

Table 103:lpm options

ls

The program used to list directory contents.

Synopsis:

```
ls [ option ] < filename > …
```

Options:

Option	Description
-1	List files in a single column
-A	Do not list implied . and ..
-a	Do not hide entries starting with .
-C	List entries by columns
-c	With -l: show ctime
-d	List directory entries instead of contents
-e	List both full date and full time
-i	List the i-node for each file
-l	Use a long listing form
-n	List numeric UIDs and GIDs instead of names
-L	List entries pointed to by symbolic links
-r	Sort the listing in reverse order
-S	Sort the listing by file size
-s	List the size of each file, in blocks
-t	With -l: show modification time
-u	With -l: show access time
-v	Sort the listing by version
-x	List entries by lines instead of by columns
-X	Sort the listing by extension

Table 104:ls options

Examples:

View list contents of actually directory.

```
ls
```

mac

The program used to display the MAC address of eth0.

Synopsis:

```
mac [<separator>]
```

Examples:

Display the MAC address of eth0. Will be used as the separator character "-" instead of ":".

```
mac -
```

mkdir

This program used to make directories.

Synopsis:

Synopsis:
mkdir [<option>] directory …

Options:

Option	Description
-m	Set permission mode (as in chmod), not rwxrwxrwx – umask
-p	No error if existing, make parent directories as needed

Table 105: mkdir options

Examples:

```
mkdir -p /tmp/test/example
```

mount

This program used to mount a file system.

Synopsis:

```
mount [-a] [-o] [-r] [-t] [-w] <DEVICE> <NODE> [ -o <option>, …]
```

Options:

Flag	Description
-a	Mount all filesystems in fstab
-o	One of many filesystem options, listed below
-r	Mount the filesystem read-only
-t	Specify the filesystem type
-w	Mount for reading and writing (default)

Table 106: mount flags

Option	Description
async/sync	Writes are asynchronous/synchronous
atime/noatime	Enable/disable updates to inode access times
dev/nodev	Allow use of special device files/disallow them
exec/noexec	Allow use of executable files/disallow them
suid/nosuid	Allow set-user-id-root programs/disallow them
remount	Re-mount a mounted filesystem, changing its flags
ro/rw	Mount for read-only/read-write
bind	Bind a directory to an additional location
move	Relocate an existing mount point

Table 107: mount options

For detail description this command, visit Linux manual pages.

Examples:

Connect a contents of USB flash drive to the directory /mnt.

```
mount -t vfat /dev/sda1 /mnt
```

■ mv

This program is used to move or rename files.

Synopsis:

```
mv [-f] [-i] <source> …<dest>
```

Options:

Option	Description
-f	Don’t prompt before overwriting
-i	Interactive, prompt before overwrite

Table 108: mv options

Examples:

Rename file abc.txt na def.txt.

```
mv abc.txt def.txt
```

Move all files with the extension txt to the directory /mnt.

```
mv *.txt /mnt
```

■ nc

This program Netcat opens a pipe to IP:port.

Synopsis:

```
nc [<options>] [<ip>] [<port>]
```

Options:

Option	Description
-l	listen mode, for inbound connects
-p <port>	local port number
-i <secs>	delay interval for lines sent
-w <secs>	timeout for connects and final net reads

Table 109: nc options

Examples:

Open a TCP connection to port 42 of 192.168.3.1, using port 31337 as the source port, with a timeout of 5 seconds:

```
nc -p 31337 -w 5 192.168.3.1 42
```

■ netstat

The program Netstat displays the networking information.

Synopsis:

```
netstat [<options>]
```

Options:

Option	Description
-l	display listening server sockets
-a	display all sockets (default: connected)
-e	display other/more information
-n	don’t resolve names
-r	display routing table
-t	tcp sockets
-u	udp sockets
-w	raw sockets
-x	unix sockets

Table 110: netstat options

■ ntpdate

The program is used to set the system time from NTP server.

Synopsis:

```
ntpdate [-p <probes>] [-t <timeout>] <server>
```

Options:

Option	Description
-p	Specify the number of samples to be acquired from each server as the integer samples, with values from 1 to 8 inclusive.
-t	Specify the maximum time waiting for a server response as the value timeout, in seconds and fraction.

Table 111: ntpdate options

Examples:

Set the system time according to the NTP server time.windows.com.

```
ntpdate time.windows.com
```

openssl

The openssl program is a command line tool for using the various cryptography functions of OpenSSL's crypto library from the shell. It can be used for:

- Creation of RSA, DH and DSA key parameters
- Creation of X.509 certificates, CSRs and CRLs
- Calculation of Message Digests
- Encryption and Decryption with Ciphers
- SSL/TLS Client and Server Tests
- Handling of S/MIME signed or encrypted mail

Synopsis:

```
openssl [<option> …]
```

Options:

For detail description this command, visit Linux manual pages.

Examples:

Generate a new key for the SSH server.

```
openssl genrsa -out /etc/certs/ssh_rsa_key 512
```

Generate a new certificate for the HTTPS server.

```
openssl req -new -out /tmp/csr -newkey rsa:1024 -nodes -keyout /etc/certs/
https_key
openssl x509 -req -setstart 700101000000Z -setend 400101000000Z -in /tmp/
csr -signkey /etc/certs/https_key -out /etc/certs/https_cert
```

passwd

This program is used to change password for user root.

Synopsis:

```
passwd
```

pidof

This program lists the PIDs of all processes with names that match the names on the command line.

Synopsis:

```
pidof <process-name> [<option>] [<process-name> ...]
```

Options:

Option	Description
-s	display only a single PID

Table 112: pidof options

ping

This program is used to send ICMP echo request to network host.

Synopsis:

```
ping [-c <count>] [-s <size>] [-q] <hosts>
```

Options:

Option	Description
-c	Send only COUNT pings
-s	Send SIZE data bytes in packets (default = 56)
-q	Quiet mode, only displays output at start and when finished
-I	Selects outgoing interface

Table 113: ping options

Examples:

Send one ICMP packet Echo Request with size 500 B on IP address 10.0.0.1.

```
ping -c 1 -s 500 10.0.0.1
```

portd

The program is used for transparent transfer of data from the serial line by TCP or UDP.

Synopsis:

```
[-l <split timeout>] [-4] [-h <hostname>] [-o <proto>] -t <port> [-k
<keepalive time>] [-i <keepalive interval>] [-r <keepalive probes>] [-x] [-
z]
portd -c <device> [-b <baudrate>] [-d <databits>] [-p <parity>] [-s
<stopbits>]
```

Options:

Option	Description
-c	Serial line device
-b	Baudrate
-d	Number of data bits
-p	Parity – even, odd or none
-s	Number of stop bits
-l	Split timeout
-4	Forced detection Expansion port 485
-h	Hostname
	Protocol TCP or UDP
-t	TCP or UDP port
-k	Keepalive time
-i	Keepalive interval
-r	Keepalive probes
-x	Use signal CD as indicator of the TCP connection
-z	Use DTR as control TCP connection

Table 114: portd options

Examples:

Running a TCP server listening on port 1000th After a TCP connection, the program transparently transmit data from the serial port settings 115200 bit/s, 8N1.

```
portd -c /dev/ttyS0 -b 115200 -t 1000 &
```

ps

This program is used to view report process status.

Synopsis:

```
ps
```

pwd

This program used to view current directory.

Synopsis:

```
pwd
```

reboot

This program is used to reboot the router.

Synopsis:

```
reboot [-d <delay>] [-n <nosync>] [-f <force>]
```

Options:

Option	Description
-d	Delay interval for rebooting
-n	No call to sync()
-f	Force reboot, do not call shutdown

Table 115: reboot options

Examples:

Reboot router after 10 second.

```
reboot -d 10
```

restore

This program is used to restore configuration from file.

Synopsis:

```
restore <filename>
```

Examples:

Restore configuration from file /tmp/my.cfg.

```
restore /tmp/my.cfg
```

rm

This program is used to remove files or directories.

Synopsis:

```
rm [-i] [-f] [-r] <file> …
```

Options:

Option	Description
-i	Always prompt before removing each destination
-f	Remove existing destinations, never prompt
-r	Remove the contents of directories recursively

Table 116: rm options

Examples:

Remove all files with extension txt in the current directory.

```
rm *.txt
```

Remove directory /tmp/test and all subdirectories.

```
rm -rf /tmp/test
```

rmdir

This program is used to remove empty directories.

Synopsis:

```
rmdir <filename>
```

Examples:

Remove empty directory /tmp/test.

```
rmdir /tmp/test
```

■ route

This program is used to show and manipulate the IP routing table.

Synopsis:

```
route [ -n ] [ -e ] [ -A ] [ add | del | delete ]
```

Options:

Option	Description
-n	Don’t resolve names
-e	Display other/more information
-A	Select address family

Table 117: route options

For detail description this command, visit Linux manual pages.

Examples:

View the routing table without translating IP addresses to domain names.

```
route -n
```

Add routing networks 192.168.3.0/24 through eth0.

```
route add -net 192.168.3.0/24 dev eth0
```

Add routing IP addresses 192.168.3.1 through 192.168.1.2 gateway.

```
route add -host 192.168.3.1 gw 192.168.1.2
```

Add default gateway 192.168.1.2

```
route add default gw 192.168.1.2
```

sed

This program is used for filtering and transforming text.

Synopsis:

```
sed [ -e ] [ -f ] [ -i ] [ -n ] [ -r ] pattern [ -files ]
```

Options:

Option	Description
-e	Add the script to the commands to be executed
-f	Add script-file contents to the commands to be executed
-i	Edit files in place (makes backup if extension supplied)
-n	Suppress automatic printing of pattern space
-r	Use extended regular expression syntax

Table 118: sed options

If no -e or -f is given, the first non-option argument is taken as the sed script to interpret. All remaining arguments are names of input files; if no input files are specified, then the standard input is read. Source files will not be modified unless -i option is given.

Examples:

Change parameter PPP_APN in file /etc/settings.ppp to value "internet".

```
sed -e "s/ (PPP_APN= ).*/ 1internet/" -i /etc/settings.ppp
```

service

This program is used to start, stop or restart specified service.

Synopsis:

```
service < service name > <start | stop | restart>
```

Examples:

Start service cron.

```
service cron start
```

Restart service ppp.

```
service ppp restart
```

sleep

This program is used to delay for a specified amount of time.

Synopsis:

```
sleep <time>
```

Examples:

Pause for 30 second.

```
pause 30
```

slog

This script used to show system log (file /var/log/message).

Synopsis:

```
slog [-n <number>] [-f]
```

Options:

Option	Description
-n	Print last N lines instead of last 10
-f	Output data as the file grows

Table 119: slog options

Examples:

Continuous listing the system log. Listing stops when reaching the maximum number of lines of log.

```
slog -
```

snmptrap

This program is used to sending SNMP trap.

Synopsis:

```
snmptrap [-c <community>] [-g <generic>] [-s <specific>] <hostname> [<oid>
<type> <value>]
```

Options:

Option	Description
-c	Community
-g	Specifies generic trap types: ▶ 0 – coldStart ▶ 1 – warmStart ▶ 2 – linkDown ▶ 3 – linkUp ▶ 4 – authenticationFailure ▶ 5 – egpNeighborLoss ▶ 6 – enterpriseSpecific
-r	Sends MAC address of eth0 interface
-s	Specifies user definition trap types in the enterpriseSpecific

Table 120: snmptrap options

Examples:

Send TRAP with info about the status of a digital input BIN0 to the IP address 192.168.1.2.

```
snmptrap 192.168.1.2 1.3.6.1.4.1.30140.2.3.1.0 u ’io get bin0’
```

Send TRAP "warm start" to the IP address 192.168.1.2

```
snmptrap -g 1 192.168.1.2
```

status

This program writes out the status of router’s interfaces or system. It is equivalent to General Status and Mobile WAN Status in router’s web administration.

Synopsis:

```
status [ -h ] [ -v ] [ lan | mobile | module | ports | ppp | sys | wifi ]
```

Options:

Option	Description
-h	Generates html output (used when called by web interface)
-v	Verbose – writes out more detailed informations
lan	Status of primary LAN. Can be lan 1, lan 2, etc. if available
mobile	Status of mobile WAN
module	Status of mobile module. Can be module 1, module 2, etc. if available
ports	Status of available peripheral ports
ppp	Status of mobile connection
sys	System information
wifi	Status of wlan interafce

Table 121: status options

Examples:

Show verbosed status of mobile connection.

```
status -v mobile
```

tail

This program is used to output the last part of files.

Synopsis:

```
tail [ -n <number>] [ -f ]
```

Options:

Option	Description
-n	Print last N lines instead of last 10
-f	Output data as the file grows

Table 122:tail options

Examples:

Show last 30 lines of /var/log/messages.

```
tail -n 30 /var/log/messages
```

tar

This program is used to create, extract or list files from a tar file.

Synopsis:

```
tar -[czxtv0] [ -f tarfile ] [ -C dir ] [ file ] …
```

Options:

Option	Description
c	Create
x	Extract
t	List
z	Filter the archive trough gzip
-f	Name of TARFILE or "-" for stdin
0	Extract to stdout
-C	Change to directory DIR before operation
v	Verbosely list files processed

Table 123:tar options

Examples:

Creating log.tar archive that contains files from the directory /var/log.

```
tar -cf log.tar /var/log
```

Extract files from the archive log.tar.

```
tar -xf log.tar
```

tcpdump

This program is used to dump traffic on a network.

Synopsis:

```
tcpdump [-AdDeflLnNOpqRStuUvxX] [-c <count>] [-C <file size>]
[-E algo:secret][-F <file>] [-i <interface>] [-r <file>]
[-s <snaplen>] [-T type] [-w <file>][-y <datalinktype>] [expression]
```

Options:

For detail description this command, visit Linux manual pages.

Examples:

View traffic on interface usb0.

```
tcpdump -n -i usb0
```

View traffic on interface eth0 except protocol Telnet.

```
tcpdump -n not tcp port 23
```

View UDP traffic on interface eth0.

```
tcpdump -n udp
```

View HTTP traffic on interface eth0.

```
tcpdump -n tcp port 80
```

View all traffic from/to IP address 192.168.1.2.

```
tcpdump -n host 192.168.1.2
```

View traffic from/to IP address 192.168.1.2 except protocol Telnet.

```
tcpdump -n host 192.168.1.2 and not tcp port 23
```

telnet

This program is used to establish interactive communication with another computer over a network using the TELNET protocol.

Synopsis:

```
telnet <host> [<port>]
```

Examples:

Connect to 192.168.1.2 by protocol Telnet.

```
telnet 192.168.1.2
```

touch

This program used to update timestamp of file.

Synopsis:

```
touch [-c] <file> [<file> …]
```

Options:

Option	Description
-c	Do not create any files

Table 124:touch options

Examples:

Create a file, respectively update timestamp of file /tmp/test.

```
touch /tmp/test
```

traceroute

This program is printed the route packets trace to network host.

Synopsis:

```
traceroute [-FIldnrv] [-f <1st_ttl>] [-m <max_ttl>] [-p <port#>] [-q
<nqueries>] [-s <src_addr>] [-t <tos>] [-w <wait>] [-g <gateway>] [-i
<iface>] [-z <pausemsecs>] host [data size]
```

Options:

Option	Description
-F	Set the don’t fragment bit
-I	Use ICMP ECHO instead of UDP datagrams
-l	Display the ttl value of the returned packet
-d	Enable socket level debugging
-n	Print hop addresses numerically rather than symbolically
-r	Bypass the normal routing tables and send directly to a host
-v	Verbose output
-m	Set the max time-to-live (max number of hops)
-p	Set the base UDP port number used in probes (default is 33434)
-q	Set the number of probes per "ttl" to nqueries (default is 3)
-s	Use the following IP address as the source address
-t	Set the type-of-service in probe packets to the following value (default 0)
-w	Set the time (in seconds) to wait for a response to a probe (default 3 sec)
-g	Specify a loose source route gateway (8 maximum)

Table 125:traceroute options

Examples:

Start traceroute on IP address 10.0.0.1 (without translation IP addresses to domain names).

■ umount

This program is used to umount file systems.

Synopsis:

```
umount [-a] [-r] [-l] [-f] <file system> | <directory>
```

Options:

Option	Description
-a	Unmount all file systems
-r	Try to remount devices as read-only if mount is busy
-l	Lazy umount (detach filesystem)
-f	Force umount (i.e. unreachable NFS server)

Table 126: umount options

Examples:

Disconnecting the disc connected to the directory /mnt.

```
umount /mnt
```

■ vi

This program is used to edit and read text file.

Synopsis:

```
vi [-R] [<file> …]
```

Options:

Option	Description
-R	Read only, do not write to the file

Table 127: vi options

Examples:

Open file /etc/rc.local in the text editor vi.

```
vi /etc/rc.local
```

wget

This program is used to retrieve files via HTTP or FTP.

Synopsis:

```
wget [-c] [-q] [-O <document file>] [--header 'header: value']
[-Y on/off] [-P <DIR>] <url>
```

Options:

Option	Description
-c	Continue retrieval of aborted transfers
-q	Quiet mode – do not print
-P	Set directory prefix to DIR
-O	Save to filename ('-' for stdout)
-Y	Use proxy ('on' or 'off')

Table 128: wget options

Examples:

Download a file my.cfg from HTTP server with IP address 10.0.0.1.

```
wget http://10.0.0.1/my.cfg
```

xargs

This program executes the command on every item given by standard input.

Synopsis:

```
xargs [<commands>] [<options>] [<args> ...]
```

Options:

Option	Description
-r	Do not run command for empty readed lines
-t	Print the command line on stderr before executing it

Table 129: xargs options

Examples:

Find files named core in or below the directory /tmp and delete them. Note that this will work incorrectly if there are any filenames containing newlines or spaces.

```
find /tmp -name core -type f -print | xargs /bin/rm -f
```

3.1 Examples of scripts

3.1.1 Send SMS

Send incoming SMS to the email.

Startup Script:

```
EMAIL=john.doe@email.com cat > /var/scripts/sms << EOF #!/bin/sh /usr/bin/
email -t \$EMAIL -s "Received SMS from \$2" -m "Authorized: \$1, Text: \$3
\$4 \$5 \$6 \$7 \$8" EOF
```

3.1.2 SMS command 1

Implementation of a new SMS command "IMPULSE", which activates binary output OUT0 for 5 seconds. SMS will be processed, if it comes from one of three numbers defined on the web interface or phone number +420123456789.

Startup Script:

```
PHONE=+420123456789 cat > /var/scripts/sms << EOF #!/bin/sh if [ "\$1" =
"1" ] || [ "\$2" = "$PHONE" ]; then if [ "\$3" = "IMPULSE" ]; then /usr/
bin/io set out0 1 sleep 5 /usr/bin/io set out0 0 fi fi EOF
```

3.1.3 SMS command 2

This script implements a new SMS command "PPP", which sets item Network type , Default SIM card and Backup SIM card . PPP command has the following structure:

PPP <AUTO/GPRS/UMTS> <1/2>

The first parameter sets network type. If the second parameter equals 1, Default SIM card will be set to primary SIM card. If this parameter equals 2, Default SIM card will be set to secondary SIM card.

Startup Script:

```
cat > /var/scripts/sms << EOF STARTUP=#!/bin/sh if [ "\$1" = "1" ]; then if
[ "\$3" = "PPP" ]; then if [ "\$4" = "AUTO" ]; then sed -e "s/
\(PPP_NETTYPE=\).*/\10/" -e "s/\(PPP_NETTYPE2=\).*/\10/" -i /etc/
settings.ppp elif [ "\$4" = "GPRS" ]; then sed -e "s/\(PPP_NETTYPE=\).*/
\11/" -e "s/\(PPP_NETTYPE2=\).*/\11/" -i /etc/settings.ppp elif [ "\$4" =
"UMTS" ]; then sed -e "s/\(PPP_NETTYPE=\).*/\12/" -e "s/
\(PPP_NETTYPE2=\).*/\12/" -i /etc/settings.ppp fi if [ "\$5" = "1" ]; then
sed -e "s/\(PPP_DEFAULT_SIM=\).*/\11/" -e "s/\(PPP_BACKUP_SIM=\).*/\12/" -
i /etc/settings.ppp elif [ "\$5" = "2" ]; then sed -e "s/
\(PPP_DEFAULT_SIM=\).*/\12/" -e "s/\(PPP_BACKUP_SIM=\).*/\11/" -i /etc/
settings.ppp fi reboot fi fi EOF
```

3.1.4 Send information email 1

Send information email about establishing of PPP connection.

Up Script:

```
EMAIL=john.doe@email.com /usr/bin/email -t $EMAIL -s "Router has
established PPP connection. IP address: $4"
```

3.1.5 Send information SNMP trap 1

Send information SNMP trap about establishing of PPP connection.

Up Script:

```
SNMP_MANAGER=192.168.1.2 /usr/bin/snmptrap -g 3 $SNMP_MANAGER
```

3.1.6 Send information email 2

Send information email about switch binary input BIN0.

Startup Script:

```
EMAIL=john.doe@email.com MESSAGE="BIN0 is active" while true do /usr/bin/
io get bin0 VAL=$? if [ "$VAL" != "$OLD" ]; then [ "$VAL" = "0" ] && /usr/
bin/email -t $EMAIL -s "$MESSAGE" OLD=$VAL fi sleep 1 done
```

3.1.7 Send information SNMP trap 2

Send information SNMP trap about change state of binary input BIN0.

Startup Script:

```
SNMP_MANAGER=192.168.1.2 while true do /usr/bin/io get bin0 VAL=$? if [
"$VAL" != "$OLD" ]; then /usr/bin/snmptrap $SNMP_MANAGER
1.3.6.1.4.1.30140.2.3.1.0 u $VAL OLD=$VAL fi sleep 1 done
```

3.1.8 Automatic reboot

Automatic reboot at the definition time. (23:55)

Startup Script:

```
echo "55 23 * * * root /sbin/reboot" > /etc/crontab service cron start
```

3.1.9 Switch between WAN and PPP

Switching between WAN and PPP. PPP connection is active, if PING on the defined IP address does not pass through.

Startup Script:

```
WAN_PING=192.168.2.1 WAN_GATEWAY=192.168.2.1 WAN_DNS=192.168.2.1 . /etc/
settings.eth /sbin/route add $WAN_PING gw $WAN_GATEWAY /sbin/iptables -t
nat -A PREROUTING -i eth1 -j napt /sbin/iptables -t nat -A POSTROUTING -o
eth1 -p ! esp -j MASQUERADE LAST=1 while true do ping -c 1 $WAN_PING PING=$?
if [ $PING != $LAST ]; then LAST=$PING if [ $PING = 0 ]; then /etc/init.d/
ppp stop sleep 3 /sbin/route add default gw $WAN_GATEWAY echo "nameserver
$WAN_DNS" > /etc/resolv.conf /usr/sbin/conntrack -F /etc/scripts/ip-up - -
- $ETH2_IPADDR else /etc/scripts/ip-down - - - $ETH2_IPADDR /usr/sbin/
conntrack -F /sbin/route del default gw $WAN_GATEWAY /etc/init.d/ppp start
fi fi sleep 1 done
```

3.1.10 Add more MAC addresses reservation to DHCP server

At first, it is necessary to edit eth file (/etc/rc.d/init.d/eth) in a way that is illustrated below (marked lines).

```
#!/bin/sh
. /etc/settings
. /etc/$PROFILE/settings.eth
. /etc/$PROFILE/settings.ppp
. /root/DHCP_MAC
case "$1" in start|restart) echo -n "Setting up network: "
.
:
fi
if [ "$ETH_DHCP_STAT_ENABLED" = "1" ]; then [ -n "$ETH_DHCP_STAT_MAC1" ]
     && [ -n "$ETH_DHCP_STAT_IPADDR1" ] && HOST1="\\nhost 1
     { hardware ethernet $ETH_DHCP_STAT_MAC1; fixed-address
     $ETH_DHCP_STAT_IPADDR1; }"
     [ -n "$ETH_DHCP_STAT_MAC2" ] && [ -n "$ETH_DHCP_STAT_IPADDR2" ]
     && HOST2="\\nhost 2
     { hardware ethernet $ETH_DHCP_STAT_MAC2; fixed-address
     $ETH_DHCP_STAT_IPADDR2; }"
     [ -n "$ETH_DHCP_STAT_MAC3" ] && [ -n "$ETH_DHCP_STAT_IPADDR3" ]
     && HOST3="\\nhost 3
     { hardware ethernet $ETH_DHCP_STAT_MAC3; fixed-address
     $ETH_DHCP_STAT_IPADDR3; }"
     [ -n "$ETH_DHCP_STAT_MAC4" ] && [ -n "$ETH_DHCP_STAT_IPADDR4" ]
     && HOST4="\\nhost 4
     { hardware ethernet $ETH_DHCP_STAT_MAC4; fixed-address
     $ETH_DHCP_STAT_IPADDR4; }"
     [ -n "$ETH_DHCP_STAT_MAC5" ] && [ -n "$ETH_DHCP_STAT_IPADDR5" ]
     && HOST5="\\nhost 5 { hardware ethernet $ETH_DHCP_STAT_MAC5;
     fixed-address $ETH_DHCP_STAT_IPADDR5; }"
     [ -n "$ETH_DHCP_STAT_MAC6" ] && [ -n "$ETH_DHCP_STAT_IPADDR6" ]
     && HOST6="\\nhost 6
     { hardware ethernet $ETH_DHCP_STAT_MAC6; fixed-address
     $ETH_DHCP_STAT_IPADDR6; }"
     [ -n "$ETH_DHCP_STAT_MAC7" ] && [ -n "$ETH_DHCP_STAT_IPADDR7" ]
     && HOST7="\\nhost 7    { hardware ethernet $ETH_DHCP_STAT_MAC7; fixed-
address
     $ETH_DHCP_STAT_IPADDR7; }"    [ -n "$ETH_DHCP_STAT_MAC8" ] && [ -n
"$ETH_DHCP_STAT_IPADDR8" ]
     && HOST8="\\nhost 8    { hardware ethernet $ETH_DHCP_STAT_MAC8; fixed-
address
     $ETH_DHCP_STAT_IPADDR8; }"    [ -n "$ETH_DHCP_STAT_MAC9" ] && [ -n
"$ETH_DHCP_STAT_IPADDR9" ]
     && HOST9="\\nhost 9    { hardware ethernet $ETH_DHCP_STAT_MAC9; fixed-
address
     $ETH_DHCP_STAT_IPADDR9; }"
.
:
fi
```

```
echo -e "option routers $ETH_IPADDR;" \
 "\\noption domain-name-servers $ETH_IPADDR;" \
 "\\ndefault-lease-time $ETH_DHCP_LEASE_TIME;" \
 "\\nmax-lease-time 86400;" \
 "\\nsubnet $ETH_NETWORK netmask $ETH_NETMASK { $POOL }" \
 "$HOST1$HOST2$HOST3$HOST4$HOST5$HOST6$HOST7$HOST8$HOST9" >
 /var/dhcp/dhcpd.conf
touch /var/dhcp/dhcpd.leases
 /usr/sbin/dhcpd -q -cf /var/dhcp/dhcpd.conf -lf
 /var/dhcp/dhcpd.leases $ETH_IFNAME 2>
 /dev/null & if [ $? = 0 ]; then echo
 "done"; else echo "failed"; fi exit 0
```

Create a file named DHCP_MAC and copy it to folder /root/. It is possible to edit this file (/root/DHCP_MAC) as you need (MAC addresses and IP addresses). Finally, reboot router or press Apply button on LAN page in the web interface of your router.

Example of DHCP_MAC file:

```
ETH_DHCP_STAT_MAC7=00:0A:14:80:92:2F ETH_DHCP_STAT_IPADDR7=192.168.1.55

ETH_DHCP_STAT_MAC8=00:0A:14:12:34:56 ETH_DHCP_STAT_IPADDR8=192.168.1.11

ETH_DHCP_STAT_MAC9=00:0A:14:F0:92:6A ETH_DHCP_STAT_IPADDR9=192.168.1.71
```

4 GRE Protocol

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of the network layer protocols inside a virtual point-to-point link over an Internet Protocol (IP) network. GRE tunnel creates a connection of the two LANs into one, looking from inside as a homogeneous. GRE is used when the IP packets are sent from the one network to the another, without being parsed or treated like IP packets by any intervening routers.

The GRE protocol encapsulates the original data, inner packet used to deliver the data to the remote network, into an outer packet. The router sends the packet through the GRE tunnel. The intervening routers forward the packet to the destination network where the outer packet is removed and the original packet is routed to the destination. Unlike IP-to-IP tunnel, the GRE tunnel is used for the transport of multi-cast and IPv6 packets between the connected networks.

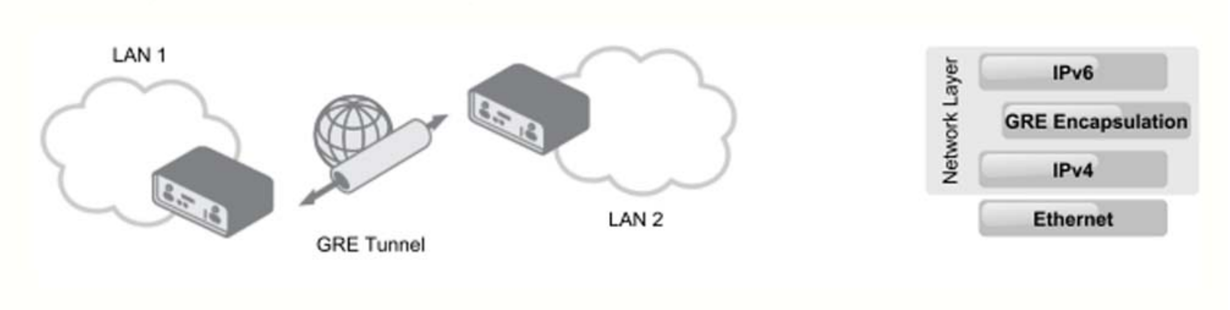


Figure 111:Left – the principle of the GRE tunnel. Right – encapsulation is done on the Network Layer, here encapsulation of IPv6 packets for transport through IPv4 network.

GRE protocol advantages:
GRE tunnels encase the multiple protocols over a single-protocol backbone, GRE tunnels provide the workarounds for the networks with limited hops, GRE tunnels connect the discontinuous sub-networks, GRE tunnels allow VPNs across the Wide Area Networks (WANs).

Examples of the GRE protocol usage:
In conjunction with PPTP to create VPNs, in conjunction with IPsec VPNs to allow passing of the routing information between the connected networks, in the Mobility protocols, Linux and BSD can establish ad-hoc IP over the GRE tunnels which are inter-operable with the Cisco equipment.

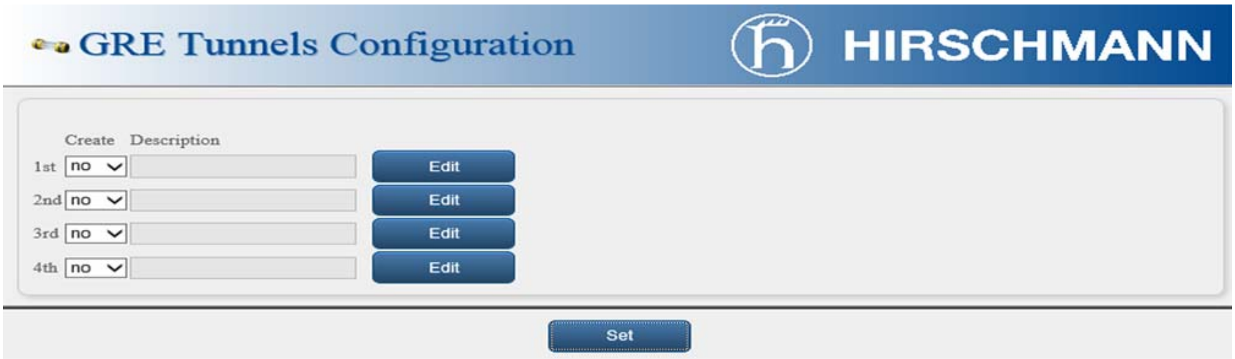
GRE protocol provides a stateless private connection, but is not an encrypted (secured) protocol. It doesn’t use any encryption like ESP (Encapsulating Security Payload) in the IPsec protocol. The GRE protocol is specified in RFC 2784 and RFC 2890. It is determined by number 47 in the Protocol field in the IP header.

4.1 GRE Tunnel Configuration

It is possible to configure up to the four GRE tunnels. To enter the GRE tunnels configuration, select the GRE menu item in the Configuration section. There are four rows in the window, representing the four possible tunnels.

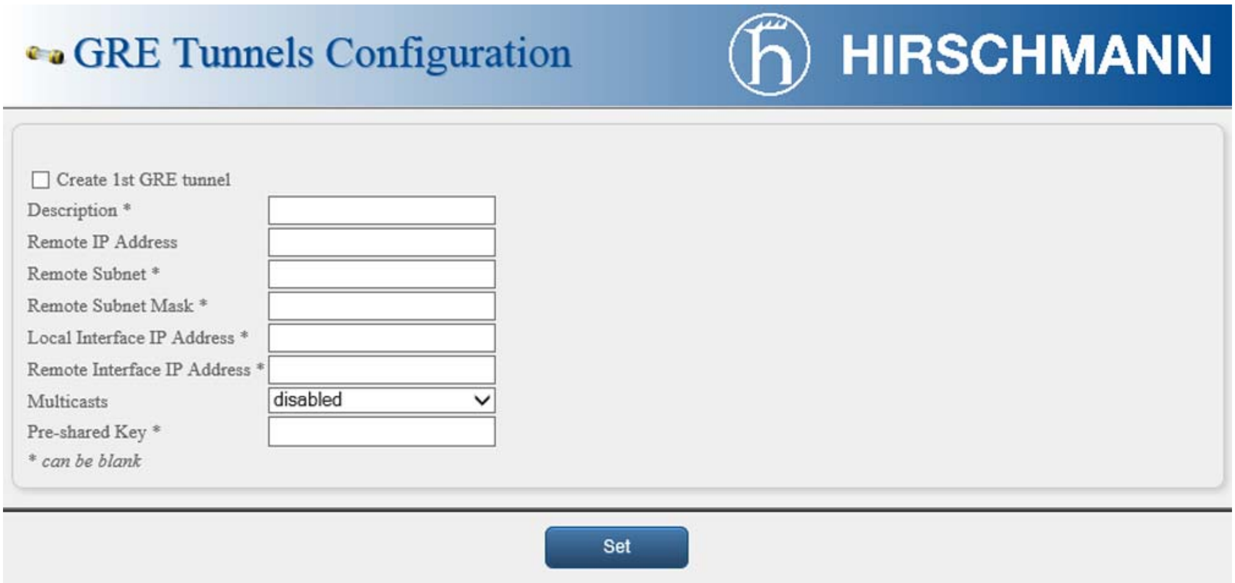
Item	Description
Create	Enables the individual tunnels
Description	Displays the name of the tunnel specified in the configuration form
Edit	Configuration of the GRE tunnel

Table 130:GRE tunnels overview



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

Figure 112:GRE tunnels overview



GRE Tunnels Configuration

□ Create 1st GRE tunnel

Description *	
Remote IP Address	
Remote Subnet *	
Remote Subnet Mask *	
Local Interface IP Address *	
Remote Interface IP Address *	
Multicasts	disabled
Pre-shared Key *	

* can be blank

Figure 113:GRE tunnel configuration (clicking the Edit button)

The tunnel can be activated by checking the Create 1st GRE tunnel box (equivalent of the Create item one level higher). The items of settings are following:

Item	Description
Description	Optional description of the 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	Mask of the network behind the remote side of the tunnel
Multicasts	Enables/disables multicast: ▶ disabled – multicast disabled ▶ enabled – multicast enabled
Pre-shared Key	Specifies the value of the pre-shared key. The pre-shared key is an optional value. The key is a numeric value containing 32 bits which allows the router to forward filtered data through the tunnel. Specify the same key on both routers, otherwise the router drops the received packets. Using the pre-shared key alone, does not provide a tunnel.

Table 131: GRE tunnels configuration

Attention, GRE tunnel does not connect itself using NAT. If you need to create tunnel through NAT, use IP-to-IP tunnel (IP packets encapsulated to IP packets) or GRE over IPsec (secured IPsec tunnel and then GRE encapsulation inside of the IPsec tunnel).

Press the `Set` button to implement all the changes in Settings.

4.2 GRE Configuration Examples

4.2.1 GRE Tunnel Between Hirschmann Routers

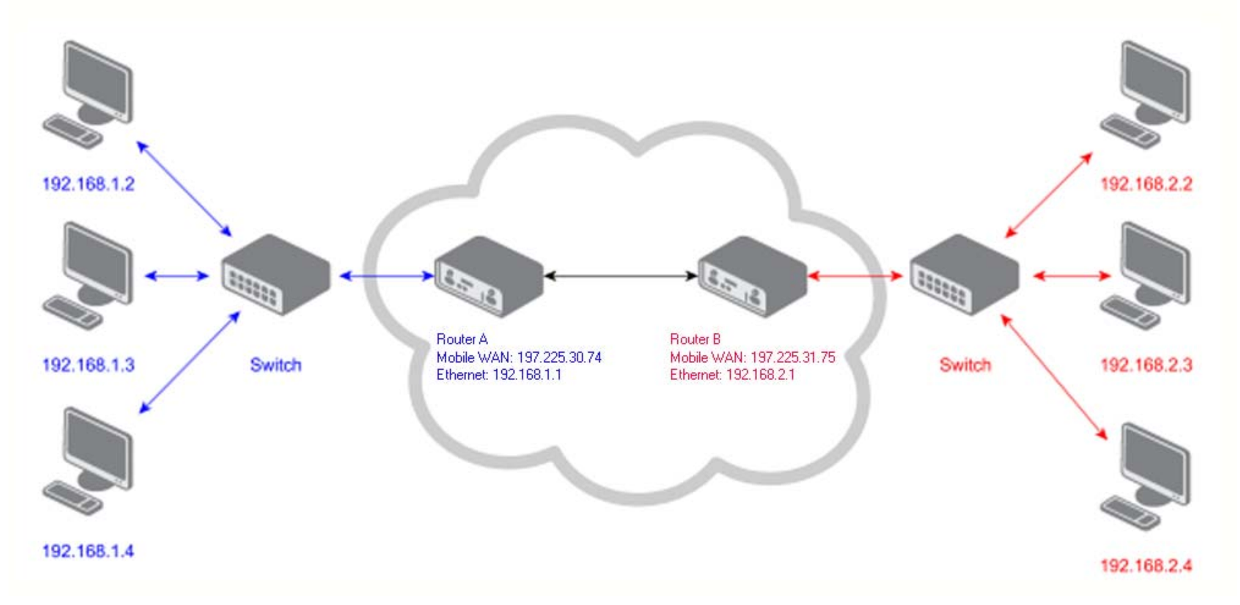
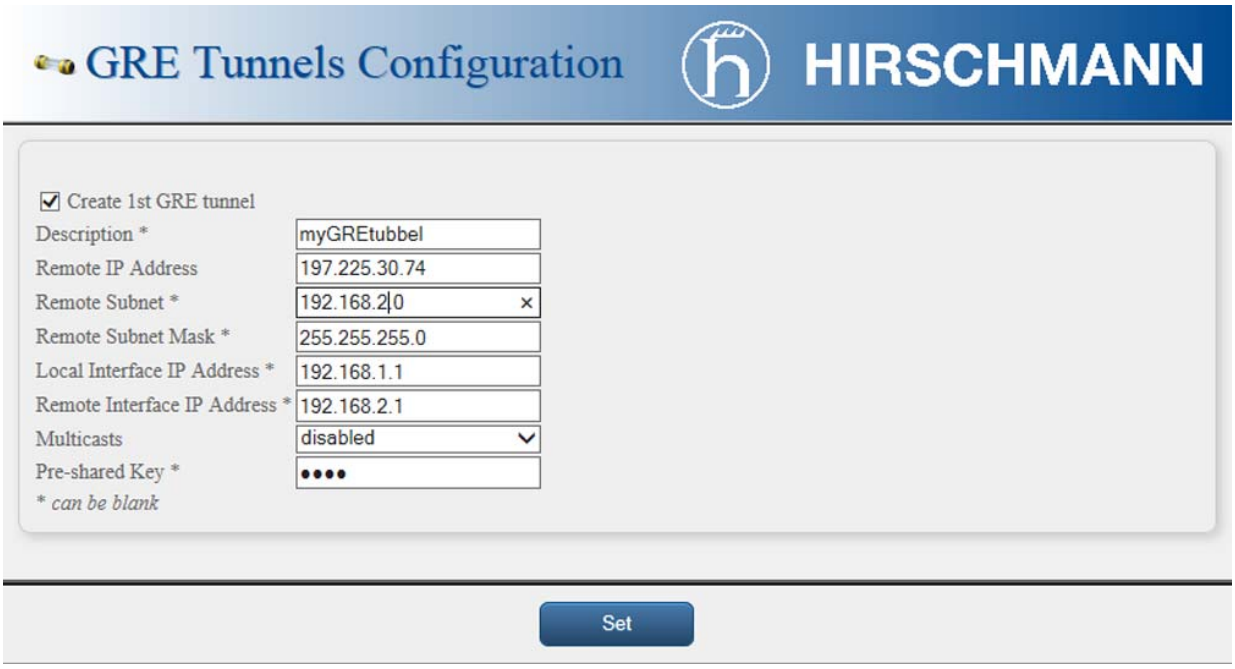


Figure 114:Topology of the Hirschmann to Hirschmann router configuration example

The figure above is an example of how to connect two LANs using GRE tunnel between the two Hirschmann routers. The default gateway for stations in the blue network is the Router A (192.168.1.1), for stations in the red network it is the Router B (192.168.2.1). GRE tunnel parameters set on both routers are shown on the next figures:



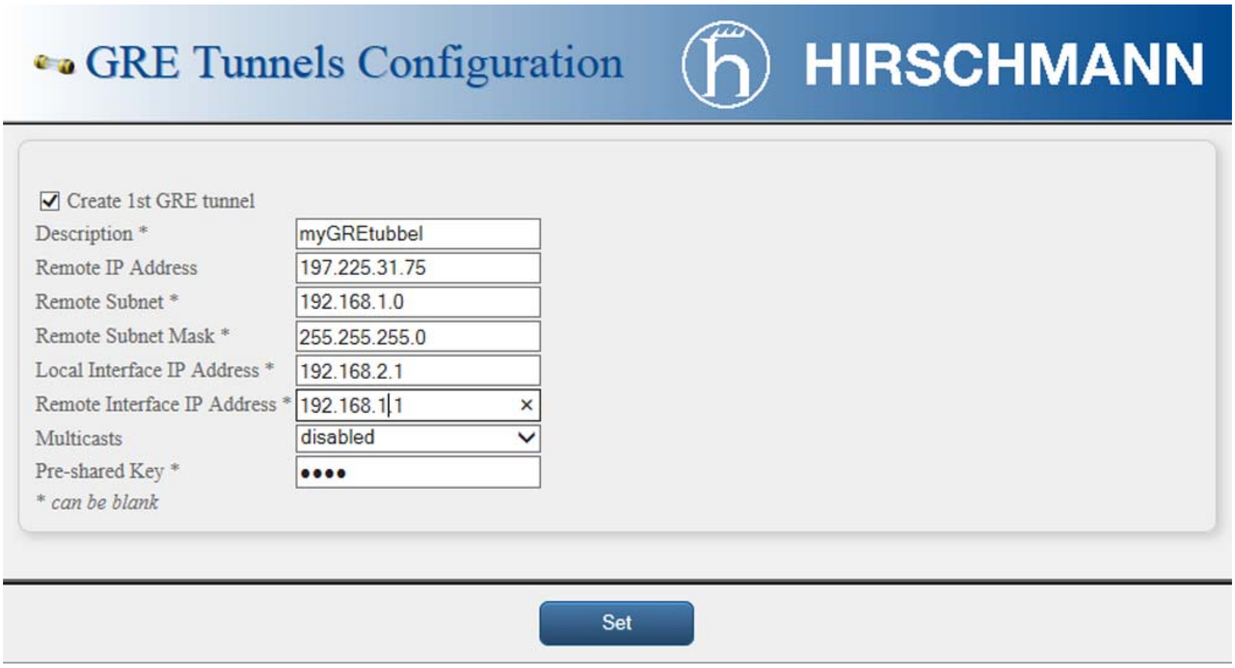
GRE Tunnels Configuration

☑ Create 1st GRE tunnel

Description *	myGREtubbel
Remote IP Address	197.225.30.74
Remote Subnet *	192.168.2.0
Remote Subnet Mask *	255.255.255.0
Local Interface IP Address *	192.168.1.1
Remote Interface IP Address *	192.168.2.1
Multicasts	disabled
Pre-shared Key *	••••

* *can be blank*

Figure 115:Router A (blue network) – GRE tunnel configuration



GRE Tunnels Configuration

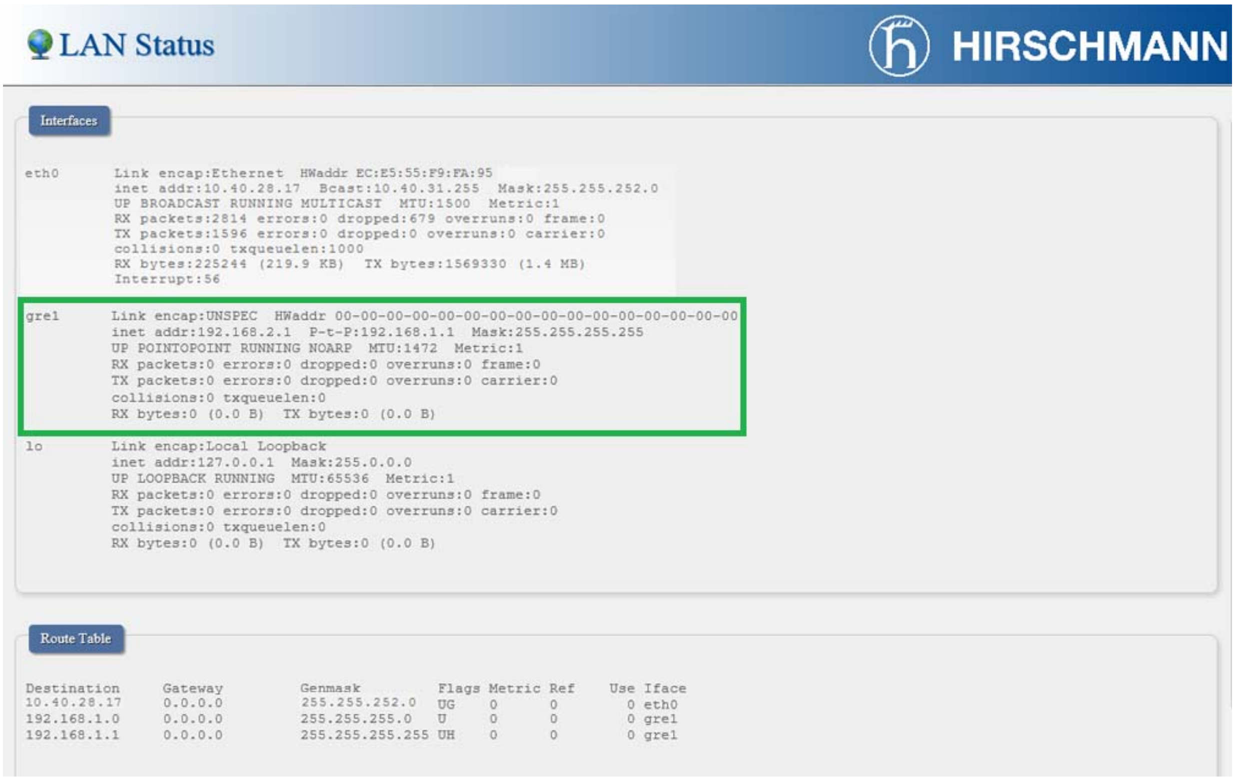
☑ Create 1st GRE tunnel

Description *	myGREtubbel
Remote IP Address	197.225.31.75
Remote Subnet *	192.168.1.0
Remote Subnet Mask *	255.255.255.0
Local Interface IP Address *	192.168.2.1
Remote Interface IP Address *	192.168.1.1
Multicasts	disabled
Pre-shared Key *	••••

* *can be blank*

Figure 116:Router B (red network) – GRE tunnel configuration

After you active the GRE tunnel, the router displays that a new network interface, “gre1”, created in every router. You can view in the "Network" dialog in the "Status" section, see the figure below:

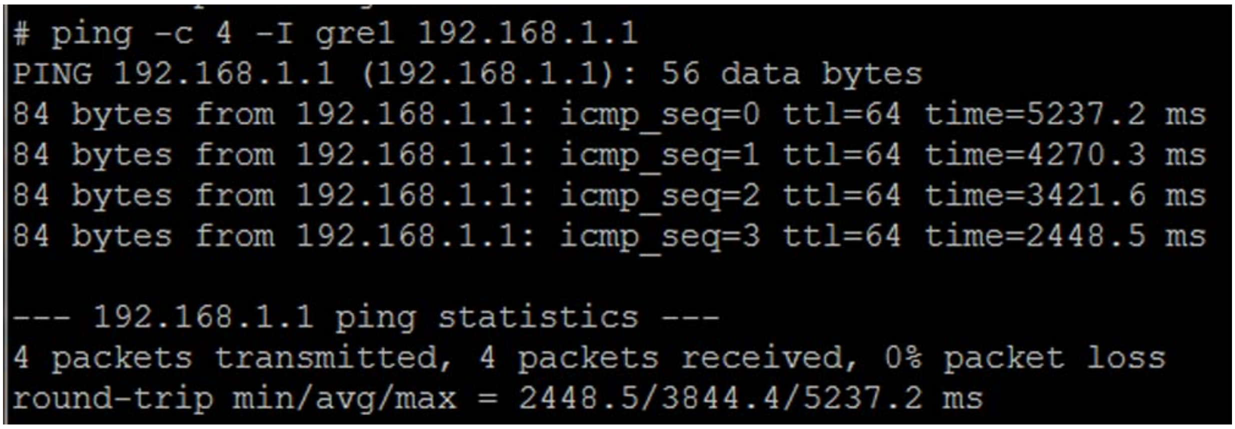


```
eth0      Link encap:Ethernet  HWaddr EC:E5:55:F9:FA:95
          inet addr:10.40.28.17  Bcast:10.40.31.255  Mask:255.255.252.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2814 errors:0 dropped:679 overruns:0 frame:0
          TX packets:1596 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:225244 (219.9 KB)  TX bytes:1569330 (1.4 MB)
          Interrupt:56

gre1      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:192.168.2.1  P-t-P:192.168.1.1  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP  MTU:1472  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)

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

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.40.28.17     0.0.0.0         255.255.252.0   UG    0      0        0 eth0
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 gre1
192.168.1.1     0.0.0.0         255.255.255.255 UH    0      0        0 gre1
```

Figure 117:Network Status – network interface gre1

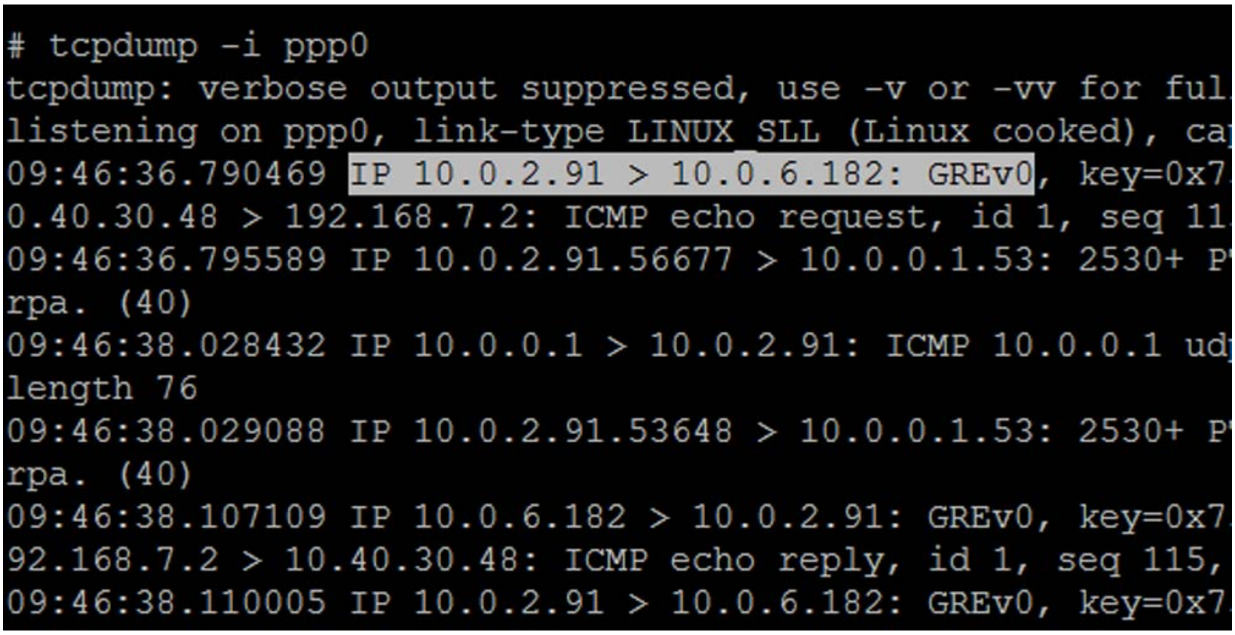
Now the connection between the networks using the GRE tunnel should work. You can verify it with the ping program after logging on to a router using SSH. In the Figure 8, there is a console of the Router B (192.168.2.1) with the program ping and its result shown. The -c switch tells the number of requests, the -I switch tells the interface used (gre1).



```
# ping -c 4 -I gre1 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
84 bytes from 192.168.1.1: icmp_seq=0 ttl=64 time=5237.2 ms
84 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=4270.3 ms
84 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=3421.6 ms
84 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=2448.5 ms

--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 2448.5/3844.4/5237.2 ms
```

Figure 118:Program ping using gre1 network interface

To verify the usage of the GRE protocol, you can run the `tcpdump` program for packet analysis in one of the routers. See the marked row in the next figure (GREv0). Here the `tcpdump` program runs with the -i switch telling which network interface listen on (ppp0 for watching the Mobile WAN communication running on this interface).



```
# tcpdump -i ppp0
tcpdump: verbose output suppressed, use -v or -vv for ful
listening on ppp0, link-type LINUX_SLL (Linux cooked), ca
09:46:36.790469 IP 10.0.2.91 > 10.0.6.182: GREv0, key=0x7
0.40.30.48 > 192.168.7.2: ICMP echo request, id 1, seq 11
09:46:36.795589 IP 10.0.2.91.56677 > 10.0.0.1.53: 2530+ P
rpa. (40)
09:46:38.028432 IP 10.0.0.1 > 10.0.2.91: ICMP 10.0.0.1 ud
length 76
09:46:38.029088 IP 10.0.2.91.53648 > 10.0.0.1.53: 2530+ P
rpa. (40)
09:46:38.107109 IP 10.0.6.182 > 10.0.2.91: GREv0, key=0x7
92.168.7.2 > 10.40.30.48: ICMP echo reply, id 1, seq 115,
09:46:38.110005 IP 10.0.2.91 > 10.0.6.182: GREv0, key=0x7
```

Figure 119:Tcpdump program for the packet analysis – verifying the GRE communication

4.2.2 GRE Tunnel Between Hirschmann Router and a Linux System

The example of the GRE tunnel between Hirschmann Router and a Linux system is shown here. Linux is running on the Hirschmann router, so it is a simple example to configure.

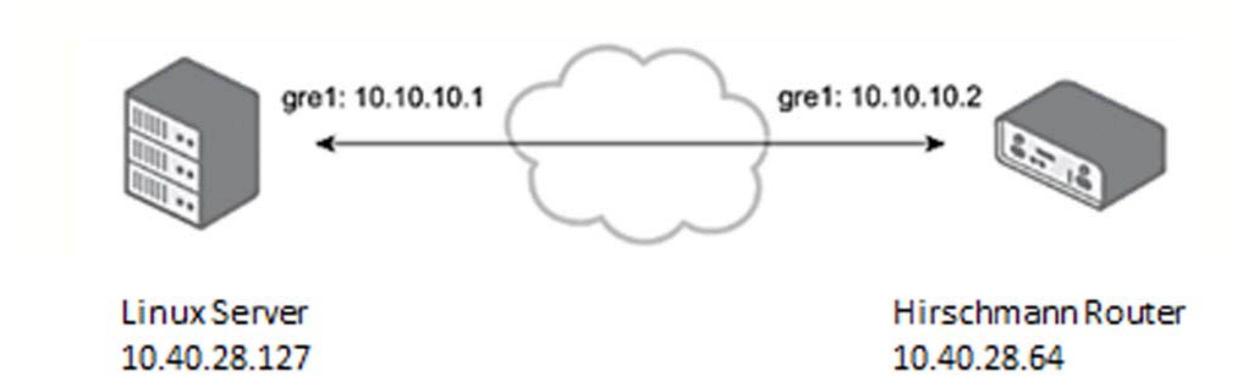
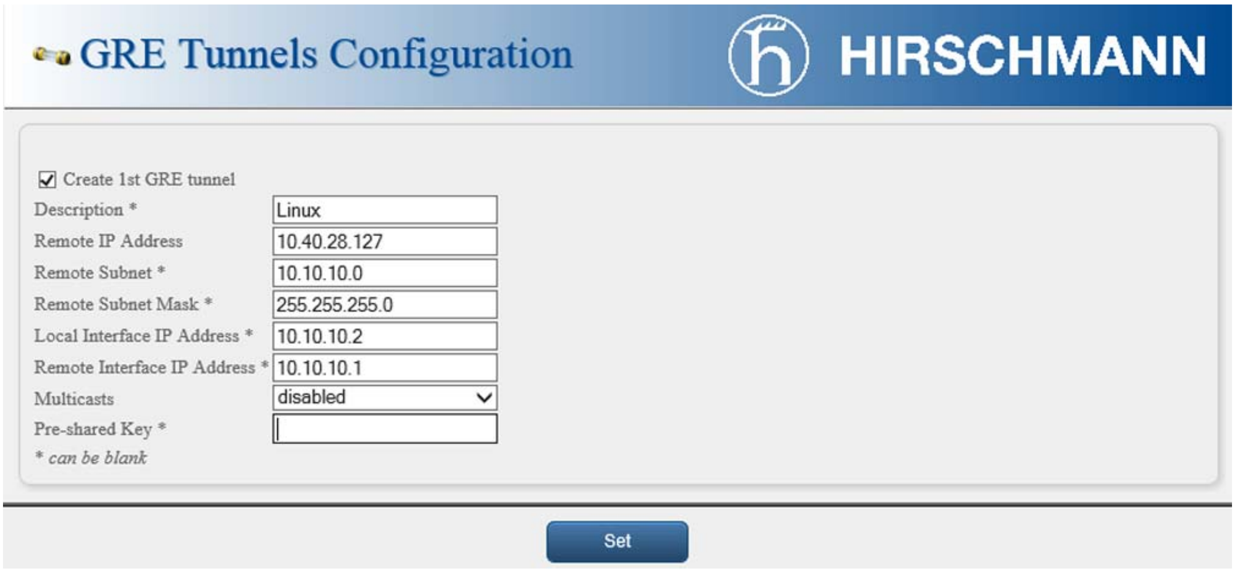


Figure 120:Example – GRE tunnel between Hirschmann router and OS Linux

For the topology and the IP addresses in this example, the GRE tunnel in the Hirschmann router is set up in the following way:



☑ Create 1st GRE tunnel

Description *	Linux
Remote IP Address	10.40.28.127
Remote Subnet *	10.10.10.0
Remote Subnet Mask *	255.255.255.0
Local Interface IP Address *	10.10.10.2
Remote Interface IP Address *	10.10.10.1
Multicasts	disabled
Pre-shared Key *	

** can be blank*

Figure 121:GRE tunnel configuration in the Hirschmann router

In the Linux system, run the terminal and create the other side of the GRE tunnel in the following way:

First, verify the Linux kernel module allowing the GRE tunnel is present. You can do this by running these commands on the Hirschmann OWL Router:

Command
$ sudo modprobe ip_gre

Command
$ lsmod | grep gre

When you enter the commands above the router displays the output in the table below:

Command	
ip_gre	22432 0
gre	12989 1 ip_gre

Now it is possible to create the GRE tunnel using the following commands:

Command
$ sudo ip tunnel add gre1 mode gre remote 10.40.28.64 local 10.40.28.127 ttl 255
$ sudo ip link set gre1 up
$ sudo ip addr add 10.10.10.124 dev gre1

It is possible to verify the creation of the tunnel by typing the `ip route show` command. The routing rules for the newly created network interface `gre1` are shown. Also, after running the `ifconfig` program showing the information about network interfaces, you see the newly created interface. For shutting down or deleting the GRE interface, use these commands:

Command
$ sudo ip link set gre1 down
$ sudo ip tunnel del gre1

The mentioned commands are used in the Hirschmann router (for example, using an SSH command line access), since the Linux OS is running on the Hirschmann routers and the `ip` program is available on these routers (see Commands and Scripts Application Note).

4.2.3 GRE Tunnel Between Hirschmann Router and Cisco Router

This is the example of the GRE tunnel configuration between the Hirschmann and the Cisco router. The topology and addresses are on the figure below:

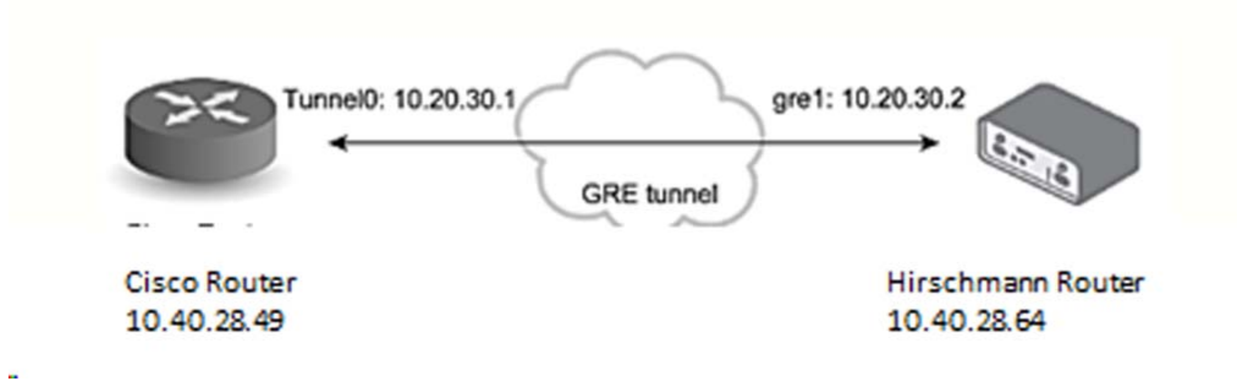
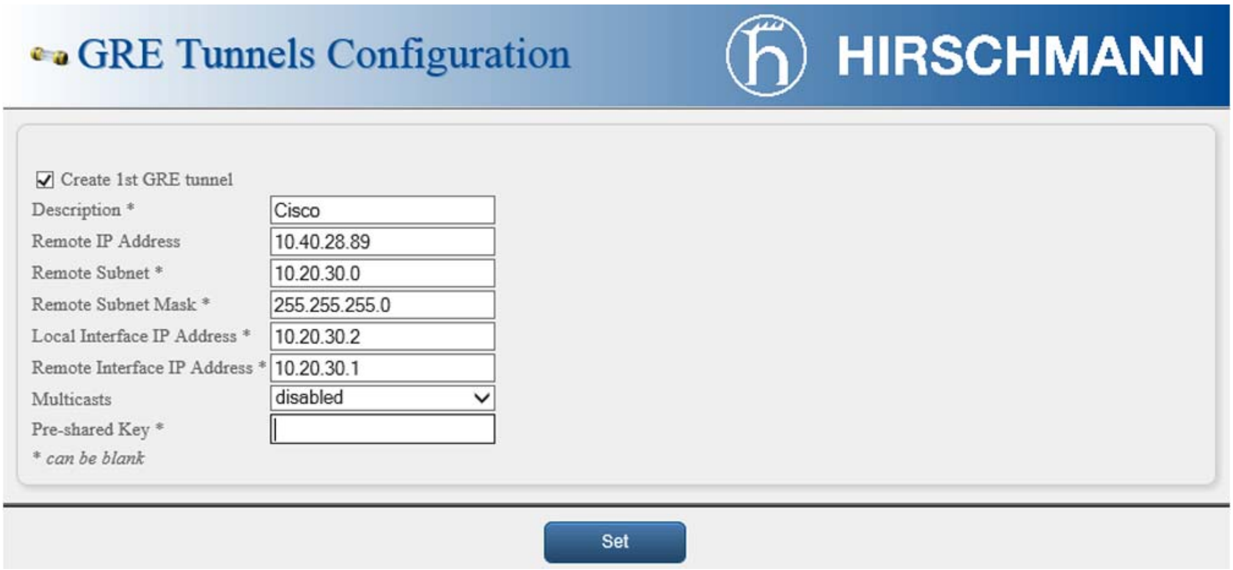


Figure 122:Example – GRE tunnel between Hirschmann router and Cisco router

Configure the Hirschmann router this way:



☑ Create 1st GRE tunnel

Description *	Cisco
Remote IP Address	10.40.28.89
Remote Subnet *	10.20.30.0
Remote Subnet Mask *	255.255.255.0
Local Interface IP Address *	10.20.30.2
Remote Interface IP Address *	10.20.30.1
Multicasts	disabled
Pre-shared Key *	

* can be blank

Figure 123:Hirschmann router – GRE tunnel configuration

Log into the console of the Cisco router (for example, using the telnet or serial line) and enter into the configuration terminal and type the `config terminal` command. Now you can create the GRE tunnel by using following commands:

Command
Router(config)# interface Tunnel0
Router(config-if)# ip address 10.20.30.1 255.255.255.0
Router(config-if)# tunnel source 10.40.28.89
Router(config-if)# tunnel destination 10.40.28.64
Router(config-if)# end

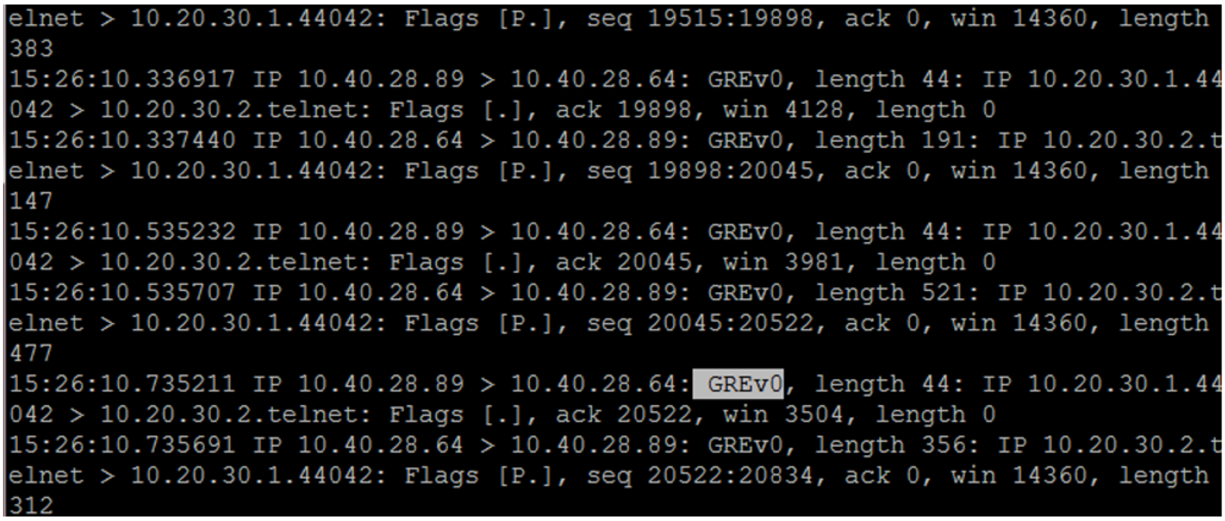
Optionally, adjust the packet length for the added overhead to prevent unnecessary packet fragmentation. You can add the route for stations connected behind the router.

Command
Router(config-if)# ip mtu 1400
Router(config-if)# ip tcp adjust-mss 1360

Command
Router(config)# ip route 192.168.1.0 255.255.255.0 10.20.30.1

You can view the running configuration typing the show `running-config` command (when out of the configuration terminal). There should be Tunnel0 network interface present and configured as done before. For deeper knowledge of Cisco router settings, see the Cisco documentation.

Now the `ping` program should work with the successful result (from the Cisco router to Hirschmann router using GRE tunnel – to the 10.20.30.2 address and vice versa). To verify the GRE encapsulation, you can, for example, from the Cisco router's console, log in to the Hirschmann router using SSH (`ssh admin@10.20.30.2`) and run there the `tcpdump` program for packet analysis. All the captured packets have a GRE protocol mark – see the next figure.



```
elnet > 10.20.30.1.44042: Flags [P.], seq 19515:19898, ack 0, win 14360, length
383
15:26:10.336917 IP 10.40.28.89 > 10.40.28.64: GREv0, length 44: IP 10.20.30.1.44
042 > 10.20.30.2.telnet: Flags [.], ack 19898, win 4128, length 0
15:26:10.337440 IP 10.40.28.64 > 10.40.28.89: GREv0, length 191: IP 10.20.30.2.t
elnet > 10.20.30.1.44042: Flags [P.], seq 19898:20045, ack 0, win 14360, length
147
15:26:10.535232 IP 10.40.28.89 > 10.40.28.64: GREv0, length 44: IP 10.20.30.1.44
042 > 10.20.30.2.telnet: Flags [.], ack 20045, win 3981, length 0
15:26:10.535707 IP 10.40.28.64 > 10.40.28.89: GREv0, length 521: IP 10.20.30.2.t
elnet > 10.20.30.1.44042: Flags [P.], seq 20045:20522, ack 0, win 14360, length
477
15:26:10.735211 IP 10.40.28.89 > 10.40.28.64: GREv0, length 44: IP 10.20.30.1.44
042 > 10.20.30.2.telnet: Flags [.], ack 20522, win 3504, length 0
15:26:10.735691 IP 10.40.28.64 > 10.40.28.89: GREv0, length 356: IP 10.20.30.2.t
elnet > 10.20.30.1.44042: Flags [P.], seq 20522:20834, ack 0, win 14360, length
312
```

Figure 124:Tcpdump program – GRE encapsulation check

4.2.4 GRE over IPsec tunnel

Example of creating the GRE tunnel inside of the IPsec tunnel between the two Hirschmann routers is shown here. This secured (encrypted) connection is used to transport the routing information (protocols) between the networks.

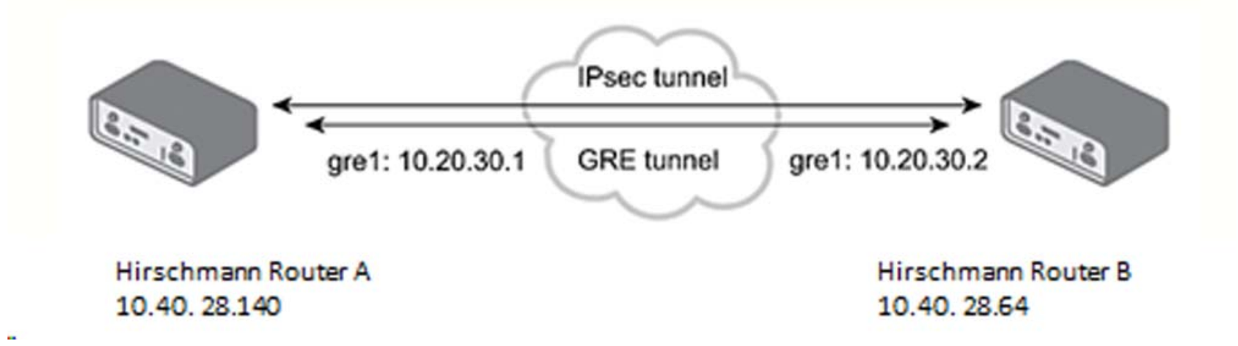
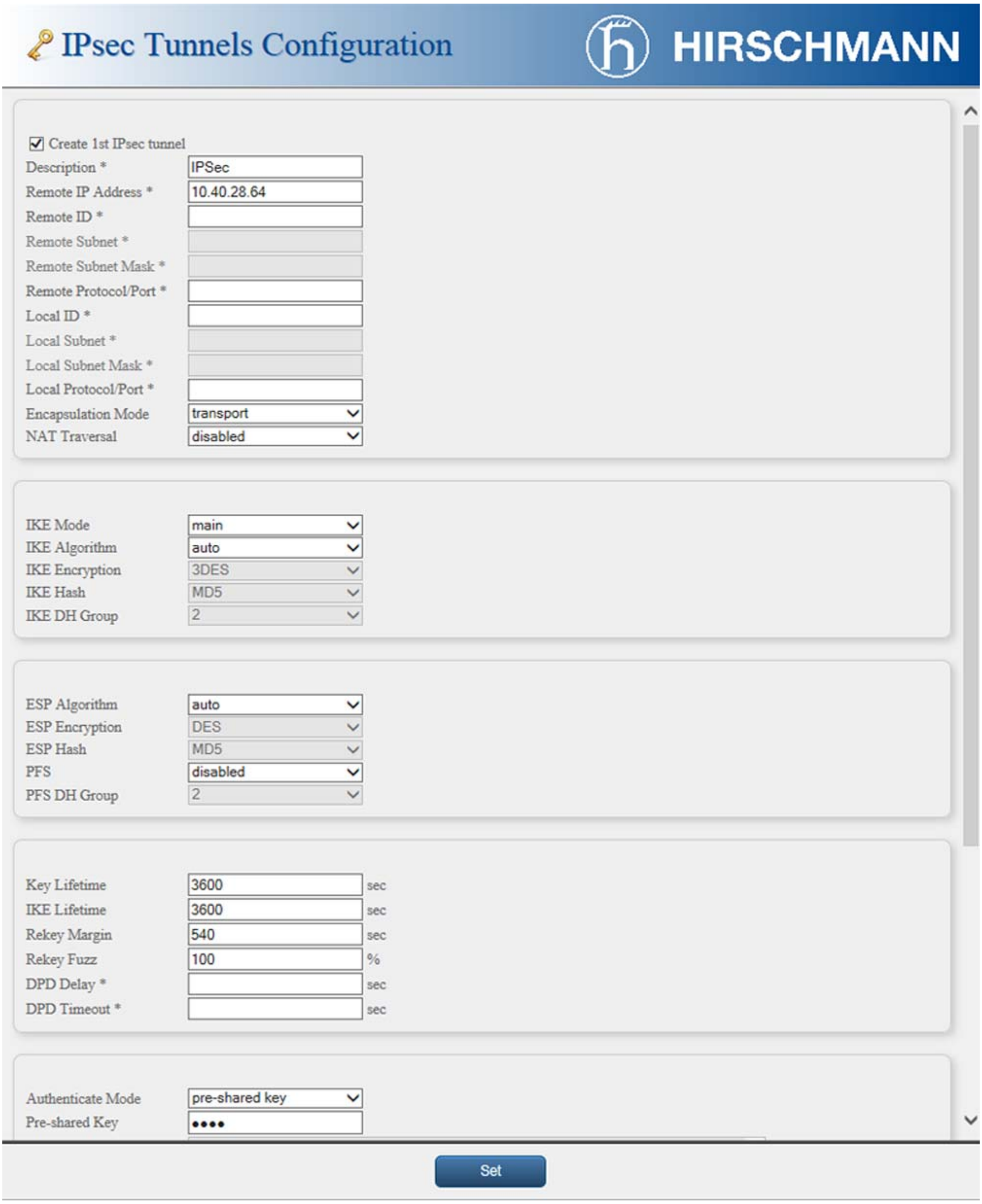


Figure 125:Topology of the GRE over IPsec example

For GRE over IPsec, make sure the IPsec connection is established and also GRE tunnel is set up on both the routers. There is the IPsec and GRE setup of the Router A and Router B on the following pictures:

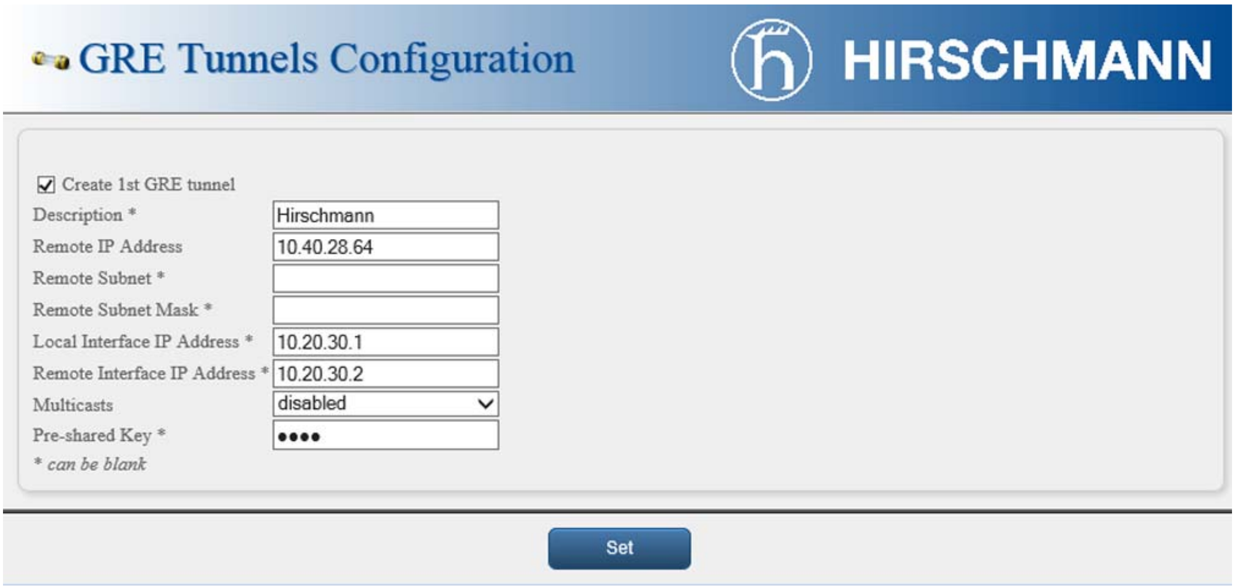


IPsec Tunnels Configuration

☑ Create 1st IPsec tunnel

Description *	IPSec	
Remote IP Address *	10.40.28.64	
Remote ID *		
Remote Subnet *		
Remote Subnet Mask *		
Remote Protocol/Port *		
Local ID *		
Local Subnet *		
Local Subnet Mask *		
Local Protocol/Port *		
Encapsulation Mode	transport	
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	••••	

Figure 126:Router A – IPsec configuration (IPsec item in the Customization section)

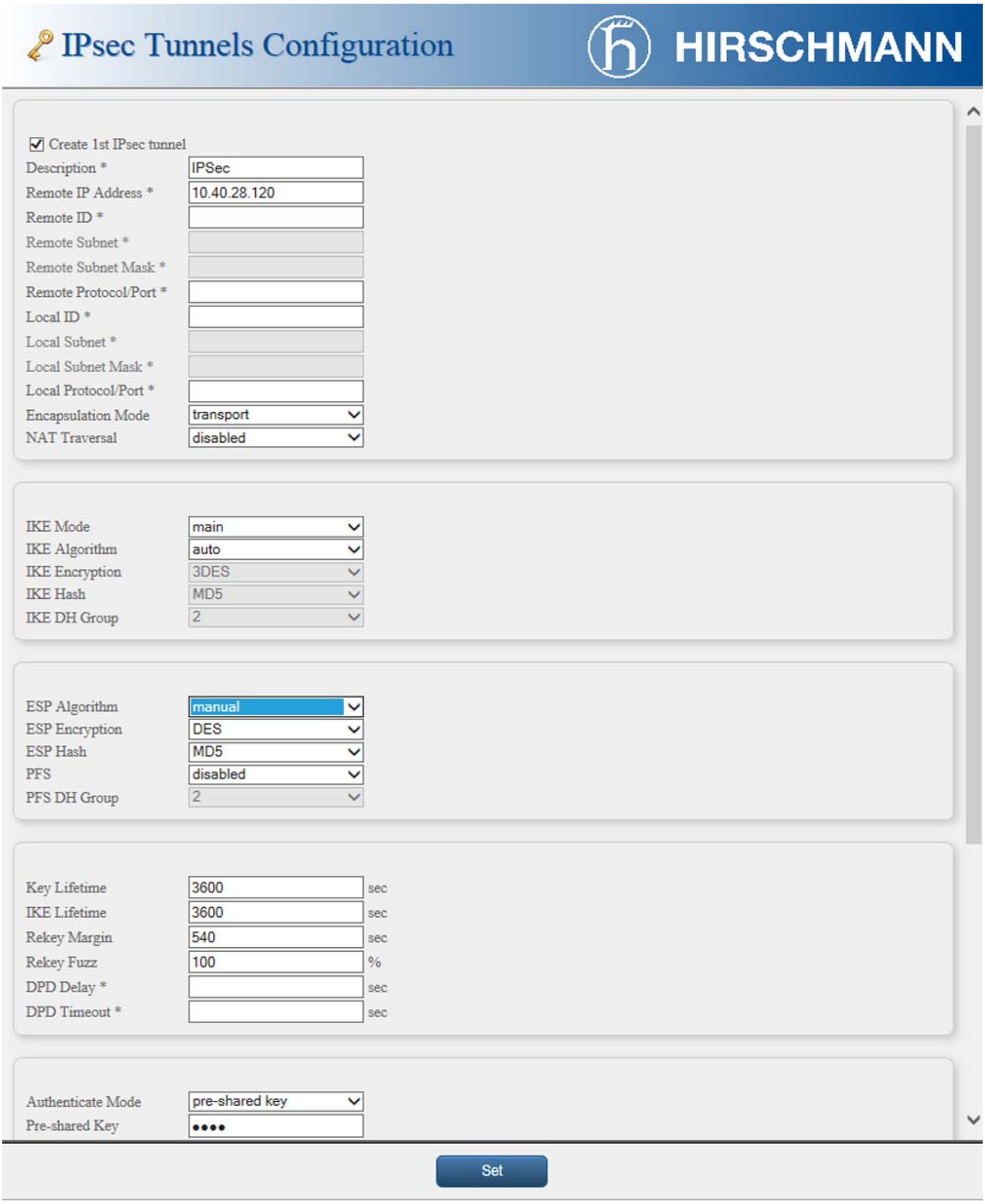


☑ Create 1st GRE tunnel

Description *	Hirschmann
Remote IP Address	10.40.28.64
Remote Subnet *	
Remote Subnet Mask *	
Local Interface IP Address *	10.20.30.1
Remote Interface IP Address *	10.20.30.2
Multicasts	disabled
Pre-shared Key *	••••

** can be blank*

Figure 127:Router A – GRE configuration

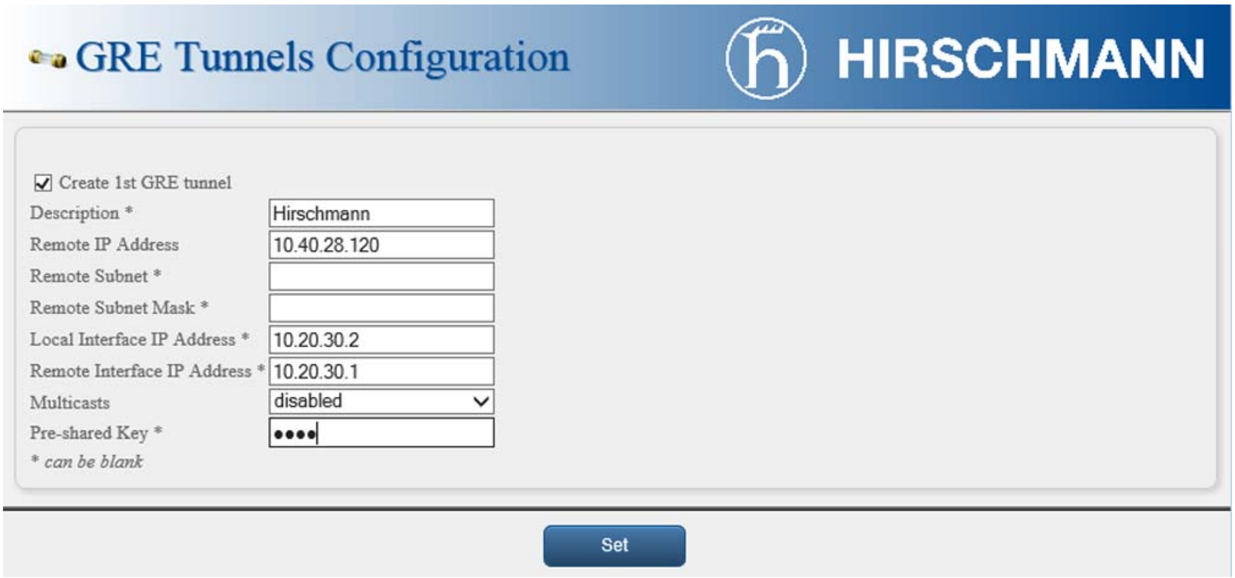


IPsec Tunnels Configuration

☑ Create 1st IPsec tunnel

Description *	IPSec
Remote IP Address *	10.40.28.120
Remote ID *	
Remote Subnet *	
Remote Subnet Mask *	
Remote Protocol/Port *	
Local ID *	
Local Subnet *	
Local Subnet Mask *	
Local Protocol/Port *	
Encapsulation Mode	transport
NAT Traversal	disabled
IKE Mode	main
IKE Algorithm	auto
IKE Encryption	3DES
IKE Hash	MD5
IKE DH Group	2
ESP Algorithm	manual
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	••••

Figure 128:Router B – IPsec configuration (IPsec item in the Customization section)



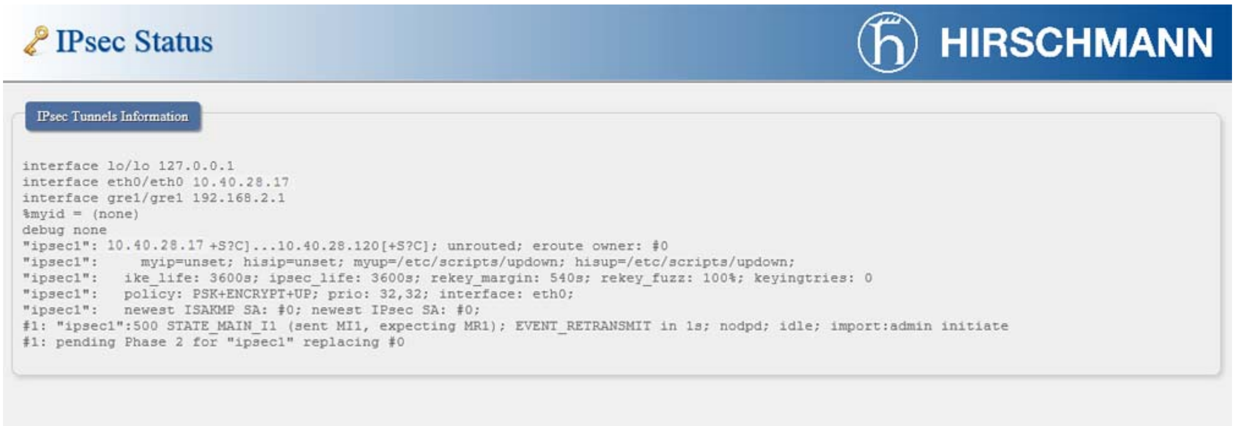
☑ Create 1st GRE tunnel

Description *	Hirschmann
Remote IP Address	10.40.28.120
Remote Subnet *	
Remote Subnet Mask *	
Local Interface IP Address *	10.20.30.2
Remote Interface IP Address *	10.20.30.1
Multicasts	disabled
Pre-shared Key *	••••

** can be blank*

Figure 129:Router B – GRE configuration

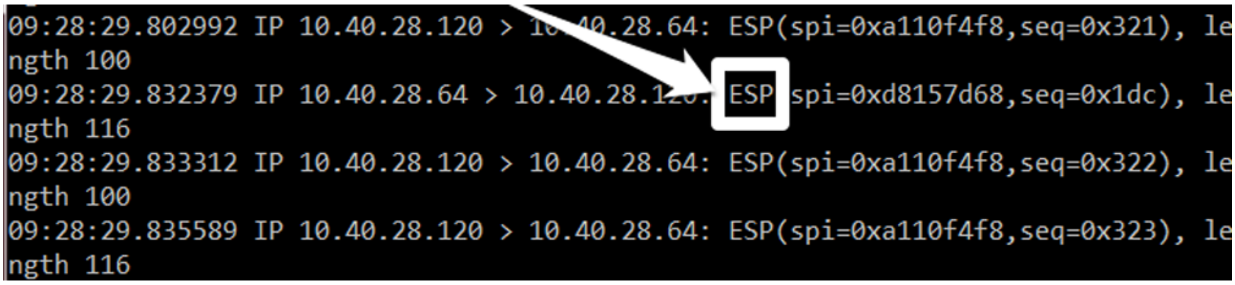
When right configured, both the routers have established information in the IPsec status – IPsec item in the Status section (see also the System Log).



```
interface lo/lo 127.0.0.1
interface eth0/eth0 10.40.28.17
interface gre1/gre1 192.168.2.1
%myid = (none)
debug none
"ipsec1": 10.40.28.17 +S?C]...10.40.28.120[+S?C]; unrouted; eroute owner: #0
"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+UP; prio: 32,32; interface: eth0;
"ipsec1":   newest ISAKMP SA: #0; newest IPsec SA: #0;
#1: "ipsec1":500 STATE_MAIN_I1 (sent MI1, expecting MR1); EVENT_RETRANSMIT in 1s; nodpd; idle; import:admin initiate
#1: pending Phase 2 for "ipsec1" replacing #0
```

Figure 130:Router B – IPsec Status, tunnel established

The encryption of GRE tunnel by IPsec is verified after logging in both the routers using telnet or SSH. For example, on the router B, run the `tcpdump` program with parameters for filtering the ESP protocol (IPsec): `tcpdump -s0 protochain 50`. From the console of router A, log in to the router B using telnet or SSH and via GRE tunnel – the 10.20.30.2 address – so that the captured communication is using the GRE tunnel. When writing in the console of router A, the `tcpdump` program on the router B captures the encrypted ESP packets. The communication is running using the GRE tunnel and is IPsec encrypted.



```
09:28:29.802992 IP 10.40.28.120 > 10.40.28.64: ESP(spi=0xa110f4f8,seq=0x321), le
ngth 100
09:28:29.832379 IP 10.40.28.64 > 10.40.28.120: ESP(spi=0xd8157d68,seq=0x1dc), le
ngth 116
09:28:29.833312 IP 10.40.28.120 > 10.40.28.64: ESP(spi=0xa110f4f8,seq=0x322), le
ngth 100
09:28:29.835589 IP 10.40.28.120 > 10.40.28.64: ESP(spi=0xa110f4f8,seq=0x323), le
ngth 116
```

Figure 131:Router B – ESP packets captured by tcpdump program

5 AT Commands

5.1 Description of AT commands

After establishing a connection with the router through a serial interface or an Ethernet it is possible to use AT commands to work with SMS messages.

This application not only lists commands that Hirschmann Automation and Control GmbH routers support. For other AT commands, the router sends an OK response. Treatment of complex AT command are unsupported, in such cases, the router sends an ERROR response.

5.1.1 ATE

The ATE <value> command determines whether or not the device echoes characters. By default this function is disabled, but may be useful for debugging purposes.

- <value> is 0 – characters are not echoed
- <value> is 1 – characters are echoed

Command	Action
ATE1	Enter
OK	

5.1.2 AT+CMGF

To set the presentation format of short messages use the AT+CMGF= <mode> command.

- <mode> is 0 – PDU mode
- <mode> is 1 – text mode

Command	Action
AT+CMGF=1	Enter
OK	

5.1.3 AT+CMGS

This command allows you to send a short message to the number that enters in the command. After sending the command AT+CMGS= “number” and pressing the `Enter` key, wait for the router to display the cursor character “>”. Enter your message behind the cursor. You terminate and send the text string using the `CTRL+Z` key combination. Transmitting the message takes some time. You can deactivate the SMS writing function by pressing the `Esc` key.

Command	Action
AT-CMGS=”465717171”	Enter
>Hello World!	CTRL+Z (shortcut key)
OK	

5.1.4 AT+CMGL

The AT+CMGL command lists the messages of a certain status from a message storage area. If you use this command in the form AT+CMGL=”ALL”, you get a list of all stored messages. If the status of a message is “received unread”, after being retrieved by the AT+CMGL command, the status changes to “received read”.

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

The Parameters have the following meaning:

- <index> – location of the message in the message storage area
- <status> – specifies the message status:
  - REC UNREAD – receives the unread messages
  - REC READ – receives the read messages
  - STO UNSENT – stores the unsent messages
  - STO SENT – stores the sent messages
  - ALL – lists all the messages
- <sender number> – the telephone number that sends the message
- <date> – the message receiving date
- <time> – the message receiving time

Command	Action
AT+CMGL=”ALL”	Enter
+CMGL: 1, “REC UNREAD”,“+420465717171, “08/02/02, 10:33:26+04”	
Hello World!	

5.1.5 AT+CMGR

The AT+CMGR command reads a message from the message storage area. The <index> number specifies the location of the next message from the message storage area. If the status of a message is “received unread”, once the AT+CMGR command retrieves it, the status changes to “received read”. Each message is displayed in this form (parameters are described in the previous command):

+CMGR: <index>, <status>, <sender number>, <date>, <time> SMS text

Command	Action
AT+CMGR=”ALL”	Enter
+CMGR: 1, “REC UNREAD”,“+420465717171, “08/01/12, 9:48:04+04”	
Hello World!	

5.1.6 AT+CMGD

This command deletes a message from the location <index>.

Command	Action
AT+CMGD=1	Enter
OK	

5.1.7 AT+CPMS

The AT+CPMS command performs a set of operation to select the SMS memory storage types for SMS reading, writing, deleting, sending or receiving. For SIM card, use “SM”. Expected response is a string in the following form:

+CPMS: <used1>,<max1>,<used2>,<max2>,<used3>,<max3>,

where the used items indicate the number of messages currently in this memory, the max items indicate the number of messages that are stored.

Command	Action
AT+CPMS=”SM”,”SM”	Enter
+CPMS: 1,10,1,10	
OK	

5.1.8 AT+CSCA

This command sets the Short Message Service Center (SMSC) number that sends the SMS text messages.

Command	Action
AT+CSCA=”+497170760000”	Enter
OK	

5.1.9 AT+CSCS

The AT+CSCS= <set> command changes the character set. If this command is in the form “AT+CSCS=?”, the response is a list of supported character sets.

Command	Action
AT+CSCS=?	Enter
+CSCS: (“GSM”,”IRA”,’HEX”)	

Command	Action
AT+CSCS=”HEX”	Enter
OK	

5.1.10 AT+CPIN

The AT+CPIN? command inquires whether the PIN code is expected. If the response is +CPIN: READ, the SIM card requires no PIN code and is ready for use. In case that the SIM card requires PIN code the response is +CPIN: SIM PIN, enter the PIN using command AT+CPIN=<PIN>. If you enter the wrong PIN code for more than three times, the SIM card gets block and you require the PUK code (response is +CPIN: SIM PUK).

Command	Action
AT+CPIN=”2654”	Enter
OK	

5.1.11 AT+CREG

The AT+CREG? command displays network registration status and returns the response in this form:

CREG: <`n`>, <`stat`>,

where <`n`> corresponds to one of the following values:

- 0 – disable network registration unsolicited result code
- 1 – enable network registration unsolicited result code

and <`stat`> (registration status) corresponds to one of the following values:

- 0 – not registered, not searching a new operator
- 1 – registered, home network
- 2 – not registered, currently searching a new operator
- 3 – registration denied
- 4 – unknown
- 5 – registered, roaming

Use the AT+CREG= <`n`> command to enable or disable network registration unsolicited result code.

Command	Action
AT+CREG=1	Enter
OK	

5.1.12 AT+CSQ

This command returns the signal strength of the registered network. The response is in the form +CSQ: <`rssi`>, <`ber`>, where <`rssi`> is the received signal strength indication and has value from 0 (-113 dBm and lower) to 31 (-51 dBm and higher), or 99 if the signal strength is not known or not detectable. The <`ber`> parameter is the channel bit error rate. It is detected only during a call, in other cases has a value 0 or 99 according to the SIM card. If this error rate is measured, its value is from 0 to 7.

Command	Action
AT+CSQ=1	Enter
+CSQ: 28,99	

5.1.13 AT+CGMM

The AT+CGMM command causes the device to return the manufacturer specific model identity.

Command	Action
AT+CGMM	Enter
+CGMM: “UCR11 V2”	

5.1.14 AT+CGMM

See the previous command AT+CGMM…

5.1.15 AT+GSN

The AT+GSN command returns the device to the product serial number.

Command	Action
AT+GSN	Enter
+GSN: “5700001”	

5.1.16 AT+CIMI

The AT+CIMI command returns the device to the International Mobile Subscriber Identity number (IMSI). It is an unique identification assigned to a SIM card by a mobile operator. An IMSI is usually presented as a 15 digit long number. The first 3 digits are the Mobile Country Code (MCC), and is followed by the Mobile Network Code (MNC), either 2 digits (European standard) or 3 digits (North American standard). The length of the MNC depends on the value of the MCC. The remaining digits are the Mobile Subscription Identification Number (MSIN) within the network of the customer base.

5.1.17 ATI

Use the ATI <`value`> command to transmit the manufacturer specific information about the device. The <`value`> parameter selects between multiple types of identification information. The value of this parameter starts at zero (0 corresponds to AT+GMM).

5.1.18 AT+CGPADDR

The command AT+CGPADDR displays the IP address of the ppp0 interface.

5.1.19 AT+CMGW

This command allows you to write a short message to SIM storage. After sending the command AT+CMGW= “length” and pressing the `Enter` key, wait for the router to display the cursor character “`>`”. Enter your message behind the cursor.You terminate and send the text string using the `CTRL+Z` key combination.Transmitting the message takes some time. You can deactivate the SMS writing function by pressing the `Esc` key. The response for this command is information about position, where the message was stored.

Command	Action
AT+CMGW=”140”	Enter
>Hello World!	CTRL+Z (shortcut key)
+CMGW: 2	

5.1.20 AT+CMSS

The AT+CMSS command sends a message from a SIM storage location value <`index`>. The location corresponds to the value that is returned by AT+CMGW command. The response is a reference value.

Command	Action
AT+CMSS=2	Enter
+CMSS: 12	

5.1.21 AT+COPS?

The AT+COPS command identifies the available mobile networks. When you press the `Enter` key, the command displays the response in the following form:

+COPS: <`mode`> <`format`> <`operator`>,

where the <`mode`> parameter specifies the registration mode:
- 0 – automatic
- 1 – manual
- 2 – de-register from network
- 4 – manual/automatic (if manual selection fails, automatic mode is entered)

and the <`operator`> parameter shows the operator identity, within the speech marks, in the format set by <`format`>:
- 0 – long alphanumeric format
- 1 – short alphanumeric format
- 2 – numeric format

Command	**Action**
AT+COPS?	Enter
+COPS: 0,0,”02 - CZ”	

5.1.22 AT+GMI

The AT+GMI command returns the device to the manufacturer specific identity.

Command	**Action**
AT+GMI	Enter
+GMI: HIRSCHMANN	

5.1.23 AT+CGMI

See the previous command AT+GMI…

5.1.24 AT+GMR

The AT+GMR command returns the device to the manufacturer specific model revision identity.

5.1.25 AT+CGMR

See the previous command AT+GMR…

5.1.26 AT+CGSN

See the command AT+CGSN…

5.2 List of AT commands

The commands are listed in alphabetical order.

AT Command	Description
AT+CGMI	Returns the manufacturer specific identity
AT+CGMM	Returns the manufacturer specific model identity
AT+CGMR	Returns the manufacturer specific model revision identity
AT+CGPADDR	Displays the IP address of the 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

Table 132: List of AT commands

6 SNMP OID

OID (Object Identifier) is the designation for a numeric identifier that unambiguously identifies each value in SNMP. This identifier consists of a progression of numbers separated by a point. The shape of the each OID is determined by the identifier value of the parent element and then this value is complemented by a point and a current number. So it is obvious that there is a tree structure. It is stored in the MIB (Management Information Base) that contains names and descriptions of the numeric identifiers.

6.1 Tree structure

The following figure shows the basic tree structure used for creating all of OIDs.

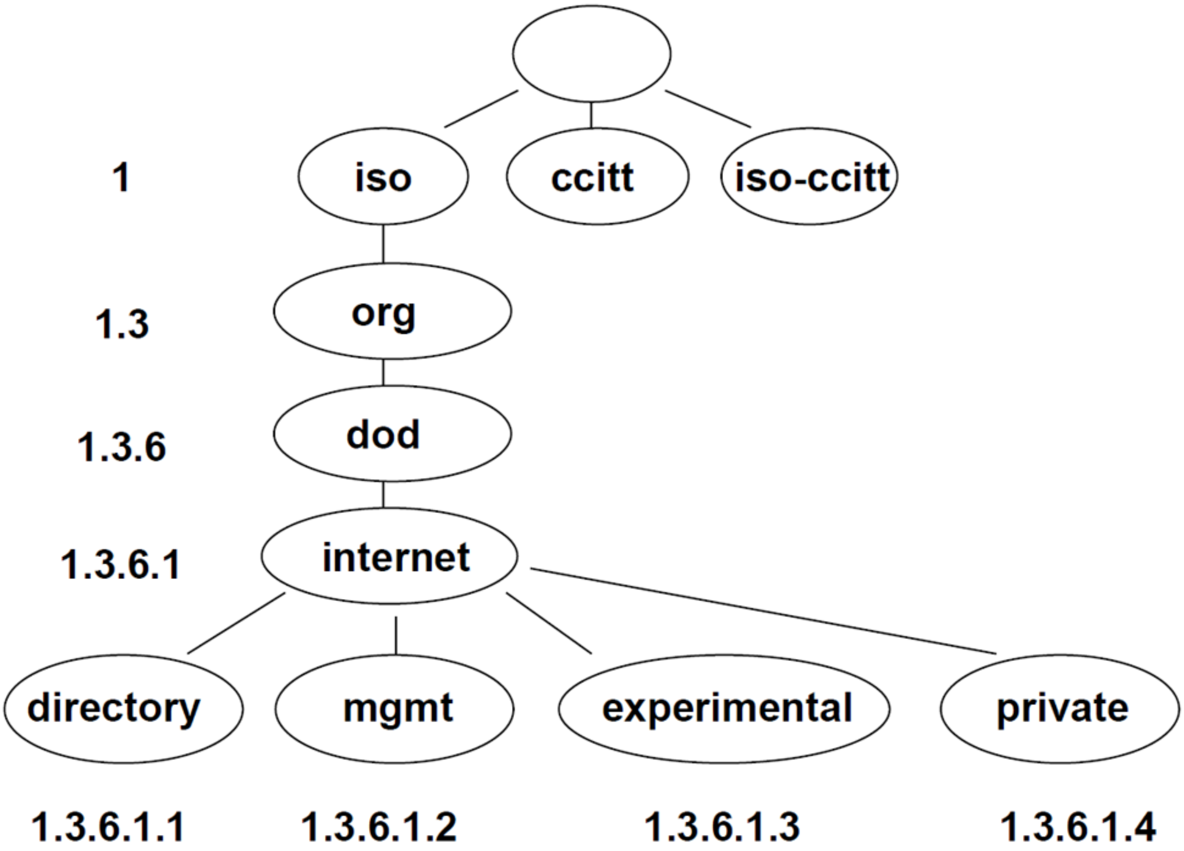


Figure 132:Basic structure

In the standard MIB table, the `mgmt` item is further divided into the following groups:

OID	Group Name	Note
.1.3.6.1.2.1.1	system	For more information see section 1.2
.1.3.6.1.2.1.2	interfaces	For more information see section 1.3
.1.3.6.1.2.1.3	at	Not supported by OWL routers
.1.3.6.1.2.1.4	ip	For more information see section 1.4
.1.3.6.1.2.1.5	icmp	For more information see section 1.5
.1.3.6.1.2.1.6	tcp	For more information see section 1.6
.1.3.6.1.2.1.7	udp	For more information see section 1.7
.1.3.6.1.2.1.8	egp	Not supported by OWL routers

Table 133: Basic groups

OID	Group Name	Note
.1.3.6.1.2.1.9	transmission	Not supported by OWL routers
.1.3.6.1.2.1.10	snmp	Not supported by OWL routers

Table 133: Basic groups

An example of OID value can be.1.3.6.1.2.1.4. This value corresponds to the text version of the MIB `iso.org.dod.internet.mgmt.mib-2.ip` (provides information about IP addresses).

6.2 System

OID	Object	Description
.1.3.6.1.2.1.1.1	sysDescr	A textual description of the entity.
.1.3.6.1.2.1.1.2	sysObjectID	Identification of the network management subsystem contained in the entity.
.1.3.6.1.2.1.1.3	sysUpTime	The time (in hundredth of a second) since the network management portion of the system was last reinitialized.
.1.3.6.1.2.1.1.4	sysContact	The textual identification of the contact person. If it is unknown, the value is a zero-length string.
.1.3.6.1.2.1.1.5	sysName	System name. If it is unknown, the value is a zero-length string.
..1.3.6.1.2.1.1.6	sysLocation	The physical location (for example, second floor). If it is unknown, the value is a zero-length string.
.1.3.6.1.2.1.1.7	sysServices	A value which indicates the set of services that this entity primarily offers.
.1.3.6.1.2.1.8	egp	Not supported by Hirschmann routers

Table 134: System

6.3 Interfaces

OID	Table	Description
.1.3.6.1.2.1.2.1	ifNumber	The number of network interfaces (regardless of their current state).
.1.3.6.1.2.1.2.2	ifTable	A list of interface entries. The number of entries isgiven by the value of ifNumber.

Table 135: Interfaces

`IfTable` is the parent element for a group `ifEntry` (OID.1.3.6.1.2.1.2.2.1). This group includes scalar objects that store information relating to a particular interface.

6.4 IP

OID	Object	Description
.1.3.6.1.2.1.4.1	ipForwarding	The indication of whether this entity is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to this entity.
.1.3.6.1.2.1.4.2	ipDefaultTTL	The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol.
.1.3.6.1.2.1.4.3	ipInReceives	The total number of input datagrams received from interfaces, including those received in error.
.1.3.6.1.2.1.4.4	ipInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, etc.
.1.3.6.1.2.1.4.5	ipInAddrErrors	The number of input datagrams discarded because the IP address in their IP header’s destination field was not a valid address to be received at this entity.
.1.3.6.1.2.1.4.6	ipForwDatagrams	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination.
.1.3.6.1.2.1.4.7	ipInUnknownProtos	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
.1.3.6.1.2.1.4.8	ipInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space).
.1.3.6.1.2.1.4.9	ipInDelivers	The total number of input datagrams successfully delivered to the IP user-protocols (including ICMP).
.1.3.6.1.2.1.4.10	ipOutRequests	The total number of IP datagrams which the local IP user protocols (including ICMP) supplied to the IP that requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.
.1.3.6.1.2.1.4.11	ipOutDiscards	The number of output IP datagrams for which no problem is encountered to prevent their transmission to their destination, but which were discarded (for example, the lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.

Table 136: IP

OID	Object	Description
.1.3.6.1.2.1.4.12	ipOutNoRoutes	The number of IP datagrams discarded because no route are available to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this “no-route” criterion.
.1.3.6.1.2.1.4.13	ipReasmTimeout	The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.
.1.3.6.1.2.1.4.14	ipReasmReqds	The number of IP fragments received which needed to be reassembled at this entity.
.1.3.6.1.2.1.4.15	ipReasmOKs	The number of IP datagrams successfully reassembled.
.1.3.6.1.2.1.4.16	ipReasmFails	The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, or errors).
.1.3.6.1.2.1.4.17	ipFragOKs	The number of IP datagrams that have been successfully fragmented at this entity.
.1.3.6.1.2.1.4.18	ipFragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be.
.1.3.6.1.2.1.4.19	ipFragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
.1.3.6.1.2.1.4.20	ipAddrTable	The table of addressing information relevant to this entity’s IP addresses.
.1.3.6.1.2.1.4.21	ipRouteTable	This entity’s IP Routing table.
.1.3.6.1.2.1.4.22	ipNetToMediaTable	The IP Address Translation table used for mapping from IP addresses to physical addresses.
.1.3.6.1.2.1.4.23	ipRoutingDiscards	The number of routing entries that are selected to discard even though they are valid.

Table 136: IP

6.5 ICMP

OID	Object	Description
.1.3.6.1.2.1.5.1	icmpInMsgs	The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.
.1.3.6.1.2.1.5.2	icmpInErrors	The number of ICMP messages which the entity receives but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
.1.3.6.1.2.1.5.3	icmpInDestUnreachs	The number of ICMP Destination Unreachable messages received.
.1.3.6.1.2.1.5.4	icmpInTimeExcds	The number of ICMP Time Exceeded messages received.
.1.3.6.1.2.1.5.5	icmpInParmProbs	The number of ICMP Parameter Problem messages received.
.1.3.6.1.2.1.5.6	icmpInSrcQuenchs	The number of ICMP Source Quench messages received.
.1.3.6.1.2.1.5.7	icmpInRedirects	The number of ICMP Redirect messages received.
.1.3.6.1.2.1.5.8	icmpInEchos	The number of ICMP Echo (request) messages received.
.1.3.6.1.2.1.5.9	icmpInEchoReps	The number of ICMP Echo Reply messages received.
.1.3.6.1.2.1.5.10	icmpInTimestamps	The number of ICMP Timestamp (request) messages received.
.1.3.6.1.2.1.5.11	icmpInTimestampReps	The number of ICMP Timestamped Reply messages received.
.1.3.6.1.2.1.5.12	icmpInAddrMasks	The number of ICMP Address Mask Request messages received.
.1.3.6.1.2.1.5.13	icmpInAddrMaskReps	The number of ICMP Address Mask Reply messages received.
.1.3.6.1.2.1.5.14	icmpOutMsgs	The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.
.1.3.6.1.2.1.5.15	icmpOutErrors	The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers.
.1.3.6.1.2.1.5.16	icmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
.1.3.6.1.2.1.5.17	icmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.
.1.3.6.1.2.1.5.18	icmpOutParmProbs	The number of ICMP Parameter Problem messages sent.

Table 137: ICMP

OID	Object	Description
.1.3.6.1.2.1.5.19	icmpOutSrcQuenchs	The number of ICMP Source Quench messages sent.
.1.3.6.1.2.1.5.20	icmpOutRedirects	The number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
.1.3.6.1.2.1.5.21	icmpOutEchos	The number of ICMP Echo (request) messages sent.
.1.3.6.1.2.1.5.22	icmpOutEchoReps	The number of ICMP Echo Reply messages sent
.1.3.6.1.2.1.5.23	icmpOutTimestamps	The number of ICMP Timestamp (request) messages sent.
.1.3.6.1.2.1.5.24	icmpOutTimestampReps	The number of ICMP Timestamp Reply messages sent.
.1.3.6.1.2.1.5.25	icmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.
.1.3.6.1.2.1.5.26	icmpOutAddrMaskReps	The number of ICMP Address Mask Reply messages sent

Table 137: ICMP

6.6 TCP

OID	Object	Description
.1.3.6.1.2.1.6.1	tcpRtoAlgorithm	The algorithm used to determine the timeout value used for retransmitting unacknowledged octets
.1.3.6.1.2.1.6.2	tcpRtoMin	The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds.
.1.3.6.1.2.1.6.3	tcpRtoMax	The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds.
.1.3.6.1.2.1.6.4	tcpMaxConn	The limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain -1.
.1.3.6.1.2.1.6.5	tcpActiveOpens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
.1.3.6.1.2.1.6.6	tcpPassiveOpens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
.1.3.6.1.2.1.6.7	tcpAttemptFails	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYNRCVD state.
.1.3.6.1.2.1.6.8	tcpEstabResets	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
.1.3.6.1.2.1.6.9	tcpCurrEstab	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
.1.3.6.1.2.1.6.10	tcpInSegs	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
.1.3.6.1.2.1.6.11	tcpOutSegs	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.

Table 138: TCP

OID	Object	Description
.1.3.6.1.2.1.6.12	tcpRetransSegs	The total number of segments retransmitted – that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
.1.3.6.1.2.1.6.13	tcpInErrs	The total number of segments received in error (e.g.,bad TCP checksums).
.1.3.6.1.2.1.6.14	tcpOutRsts	The number of TCP segments sent containing the RST flag.

Table 138: TCP

TCP also includes `tcpConnTable` table (.1.3.6.1.2.1.6.13) that is the parent element for the `tcpConnEntry` table. It is a table containing information about existing TCP connections and TCP listeners. This table is considered to be outdated and now is usually replaced by the `tcpConnectionTable` and `tcpListenerTable` tables.

6.7 UDP

OID	Object	Description
.1.3.6.1.2.1.7.1	udpInDatagram	The total number of UDP datagrams delivered to UDP users.
.1.3.6.1.2.1.7.2	udpNoPorts	The total number of received UDP datagrams for which there was no application at the destination port.
.1.3.6.1.2.1.7.3	udpInErrors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
.1.3.6.1.2.1.7.4	udpOutDatagrams	The total number of UDP datagrams sent from this entity.

Table 139: UDP

This group also includes `udpTable` table that is the parent element for `udpEntry` table. It is a table containing information about a particular current UDP listener. There are two scalar objects `udpLocalAddress` (.1.3.6.1.2.1.7.5.1.1) and `udpLocalPort` (.1.3.6.1.2.1.7.5.1.2). The first gives the local address for UDP listener and the second gives the local port number for UDP listener.

7 Management Information Base (MIB)

The Management Information Base (MIB) is designed in the form of an abstract tree structure.
The branching points are the object classes. The "leaves" of the MIB are called generic object classes.
If this is required for unique identification, the generic object classes are instantiated, i.e. the abstract structure is mapped onto reality, by specifying the port or the source address.
Values (integers, time ticks, counters or octet strings) are assigned to these instances; these values can be read and, in some cases, modified. The object description or object ID (OID) identifies the object class. The subidentifier (SID) is used to instantiate them.

Example:
The generic object class
`hm2PSState (OID = 1.3.6.1.4.1.248.11.11.1.1.1.1.2)`
is the description of the abstract information "power supply status". However, it is not possible to read any information from this, as the system does not know which power supply is meant.
Specifying the subidentifier (2) maps this abstract information onto reality (instantiates it), thus indicating the operating status of power supply 2. A value is assigned to this instance and can then be read. The instance "`get 1.3.6.1.4.1.248.11.11.1.1.1.1.2.1`“ returns the response "1", which means that the power supply is ready for operation.

Definition of the syntax terms used:	
Integer	An integer in the range -2^{31} - 2^{31}-1
IP Address	xxx.xxx.xxx.xxx (xxx = integer in the range 0-255)
MAC Address	12-digit hexadecimal number in accordance with ISO/IEC 8802-3
Object identifier	x.x.x.x… (e.g. 1.3.6.1.4.1.248...)
Octet string	ASCII character string
PSID	Power supply identifier (number of the power supply unit)

Definition of the syntax terms used:	
TimeTicks	Stopwatch, Elapsed time (in seconds) = numerical value / 100 Numerical value = integer in range 0-2^{32}-1
Timeout	Time value in hundredths of a second Time value = integer in range 0-2^{32}-1
Type field	4-digit hexadecimal number in accordance with ISO/IEC 8802-3
Counter	Integer (0-2^{32-1}), whose value is increased by 1 when certain events occur.

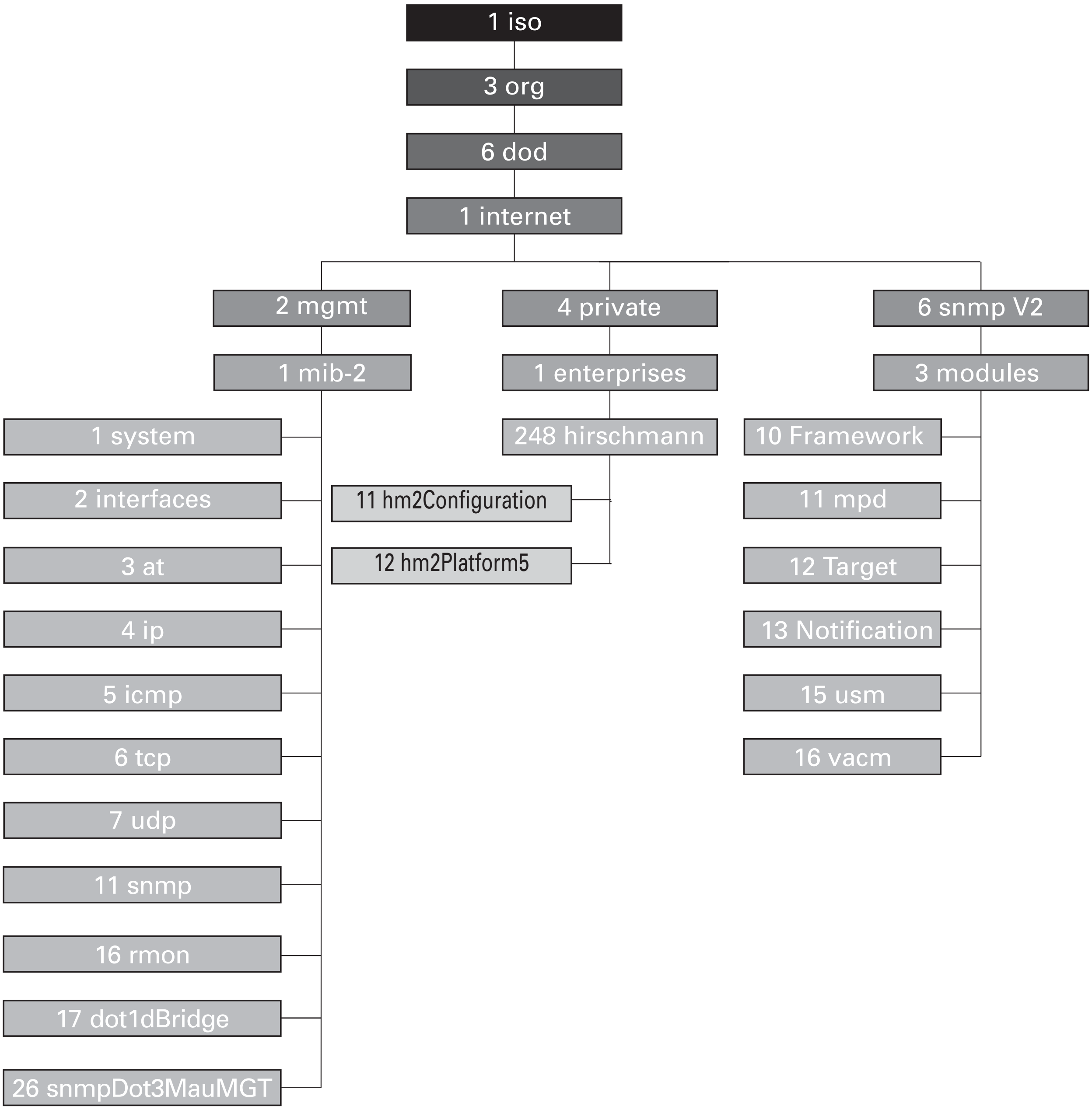
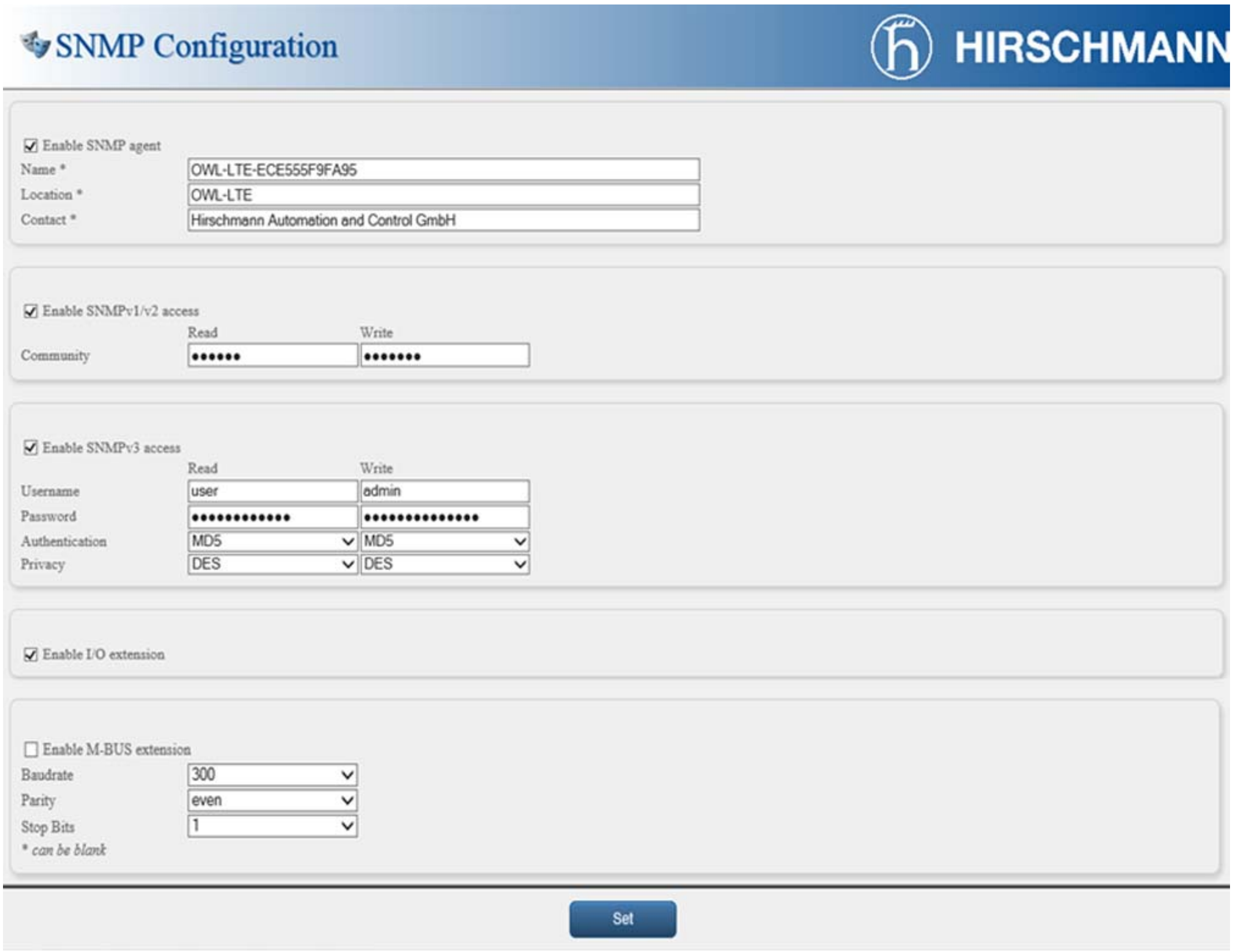


Figure 133:Tree structure of the Hirschmann MIB

8 Sample settings and readout:



☑ Enable SNMP agent

Name *	OWL-LTE-ECE555F9FA95
Location *	OWL-LTE
Contact *	Hirschmann Automation and Control GmbH

☑ Enable SNMPv1/v2 access

	Read	Write
Community	••••••	•••••••

☑ Enable SNMPv3 access

	Read	Write
Username	user	admin
Password	•••••••••••••	••••••••••••••
Authentication	MD5	MD5
Privacy	DES	DES

☑ Enable I/O extension

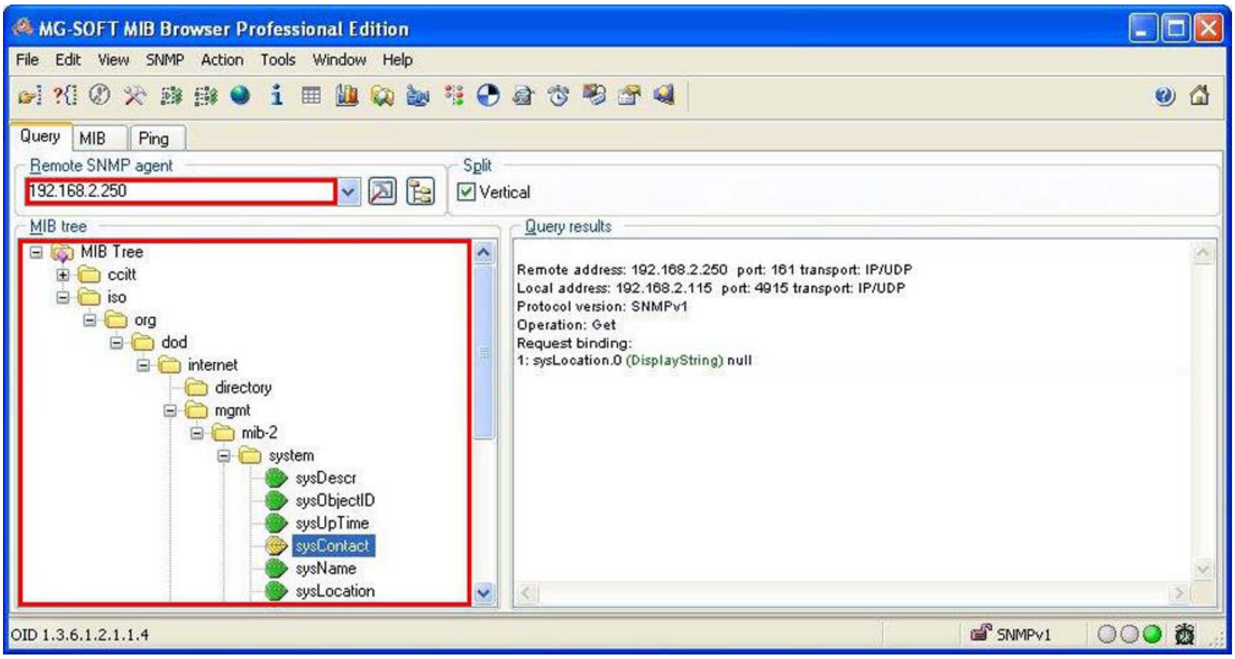
□ Enable M-BUS extension

Baudrate	300
Parity	even
Stop Bits	1

** can be blank*

Figure 134:Example of SNMP configuration

Sample settings and readout:



192.168.2.250

```
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
```

Figure 135:Example of MIB browser

It is important to set the IP address of the SNMP agent (router) in the `Remote SNMP agent` field. After entering the IP address the OIDs, the browser displays the OIDs in the MIB tree. To display the state of object identifier, enter the OID number.

The path to objects is:

iso.org.dod.internet.private.enterprises.hirschmann.protocols

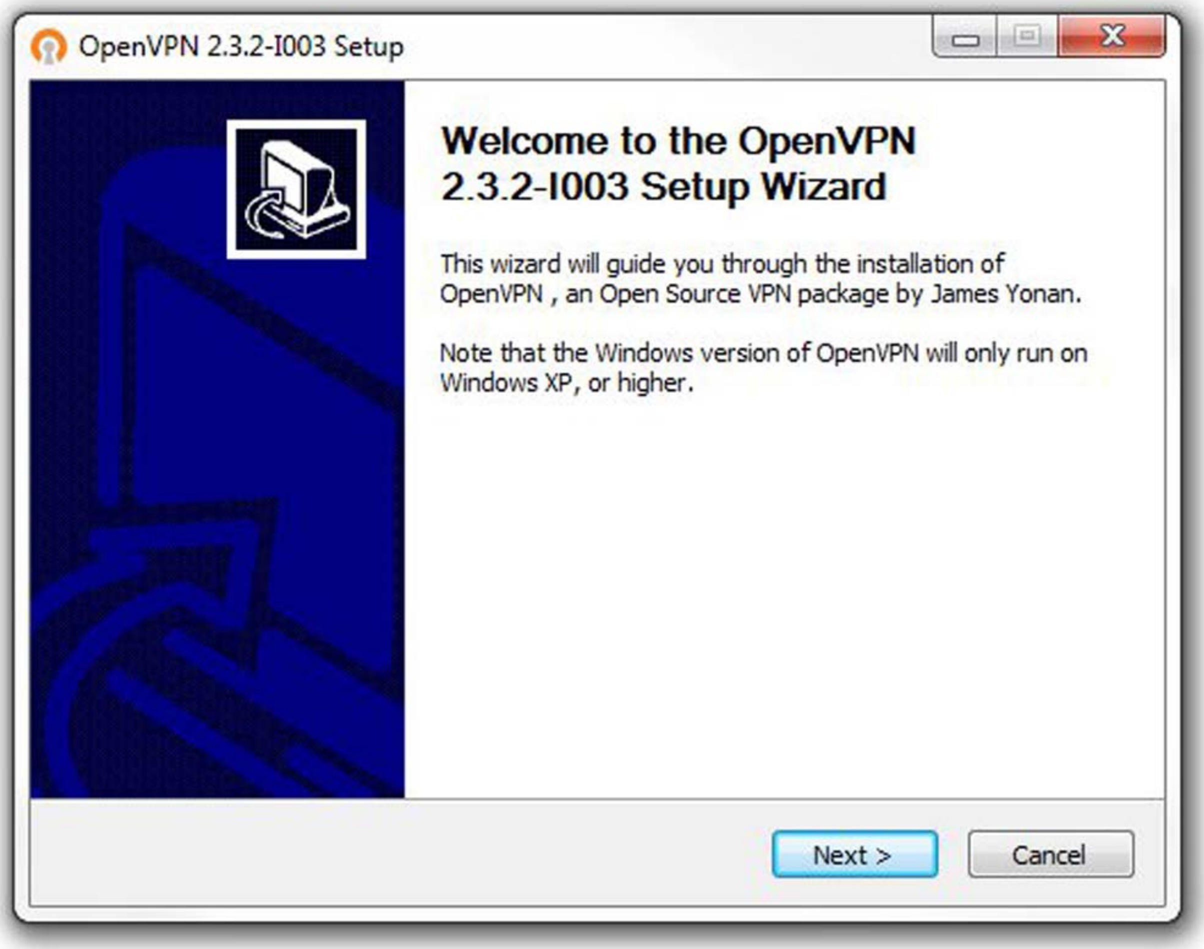
The path to basic information about the router is:

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

A Installation of OpenVPN (Windows)

Download the installation file from http://swupdate.openvpn.org/community/releases/ and run it. After opening the appropriate file the following dialog is displayed.

Procedures described in this manual require the installation file version 2.2.2 or older. Newer versions do not include easy-rsa directory.



OpenVPN 2.3.2-I003 Setup

Welcome to the OpenVPN 2.3.2-I003 Setup Wizard

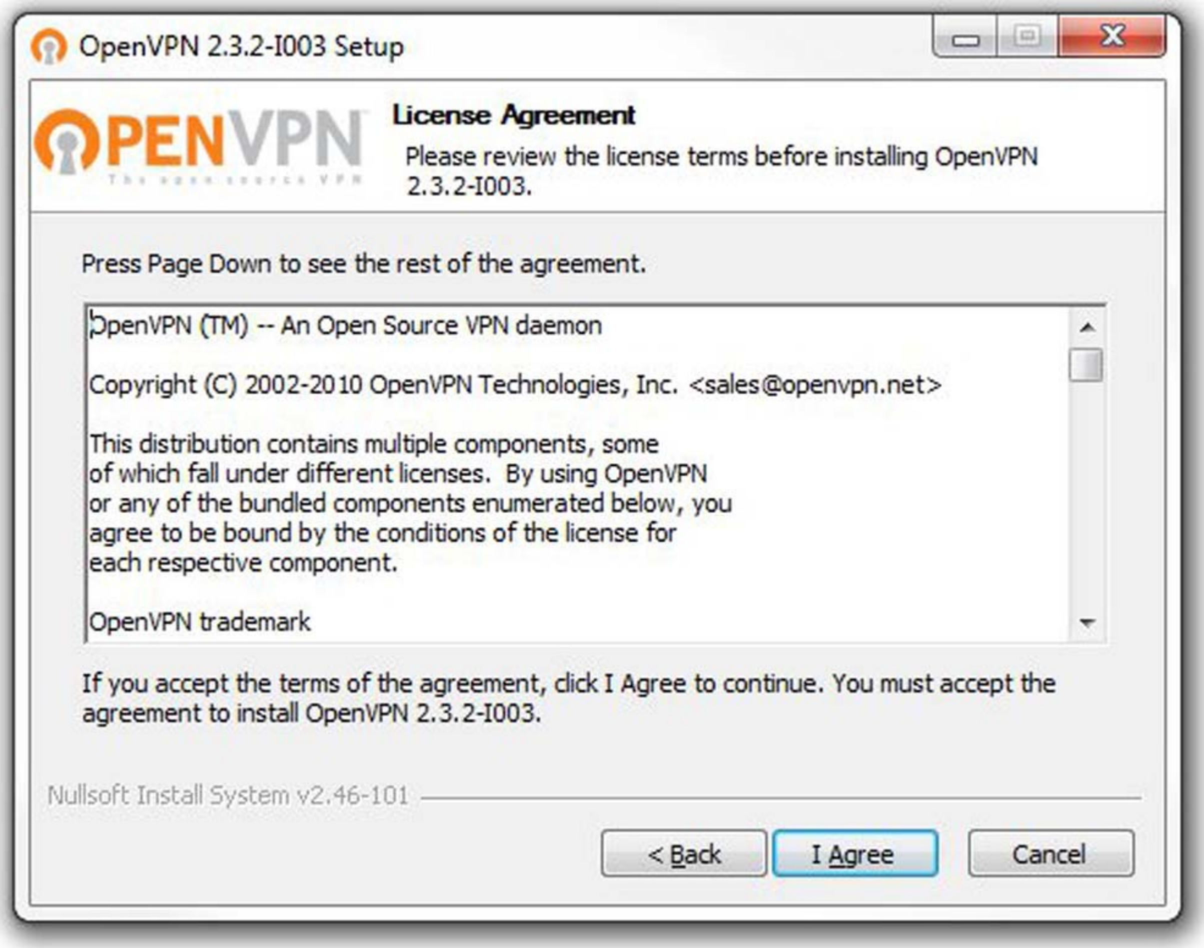
This wizard will guide you through the installation of OpenVPN , an Open Source VPN package by James Yonan.

Note that the Windows version of OpenVPN will only run on Windows XP, or higher.

Figure 136:Installation of OpenVPN – basic information

To install the OpenVPN program, use the following work steps:

- □ Press the "`Next`" button.
- □ Read the license agreement, then click the "`Next`" button.
- □ The next dialog that opens allows you to select the components of the OpenVPN program that you want to include in installation.
  See figure 137 on page 274.



License Agreement

Please review the license terms before installing OpenVPN 2.3.2-I003.

Press Page Down to see the rest of the agreement.

OpenVPN (TM) -- An Open Source VPN daemon

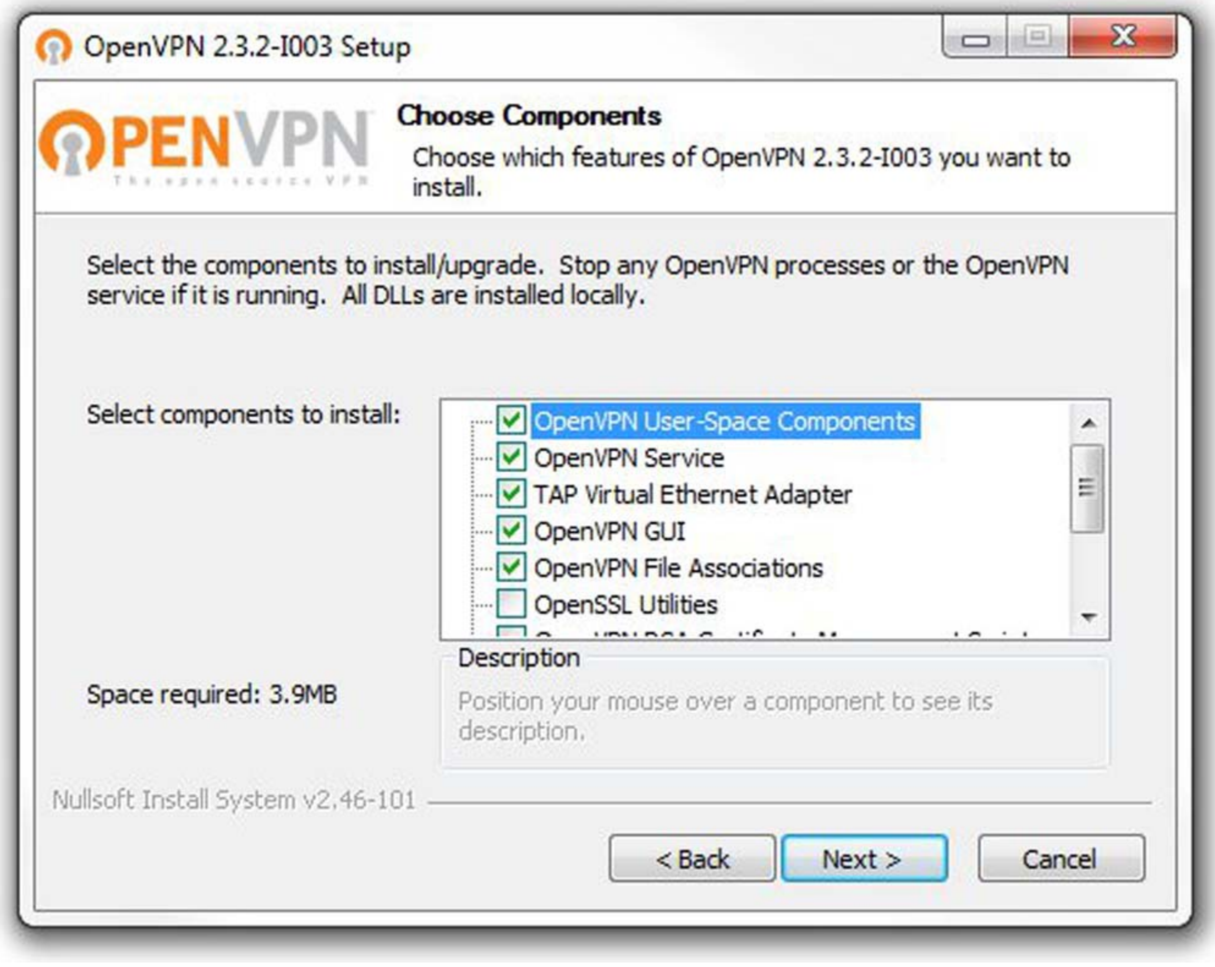
Copyright (C) 2002-2010 OpenVPN Technologies, Inc. <sales@openvpn.net>

This distribution contains multiple components, some
of which fall under different licenses. By using OpenVPN
or any of the bundled components enumerated below, you
agree to be bound by the conditions of the license for
each respective component.

OpenVPN trademark

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install OpenVPN 2.3.2-I003.

Figure 137:Installation of OpenVPN - license agreement



OpenVPN 2.3.2-I003 Setup

Choose Components

Choose which features of OpenVPN 2.3.2-I003 you want to install.

Select the components to install/upgrade. Stop any OpenVPN processes or the OpenVPN service if it is running. All DLLs are installed locally.

Select components to install:

- ☑ OpenVPN User-Space Components
- ☑ OpenVPN Service
- ☑ TAP Virtual Ethernet Adapter
- ☑ OpenVPN GUI
- ☑ OpenVPN File Associations
- □ OpenSSL Utilities

Space required: 3.9MB

Description

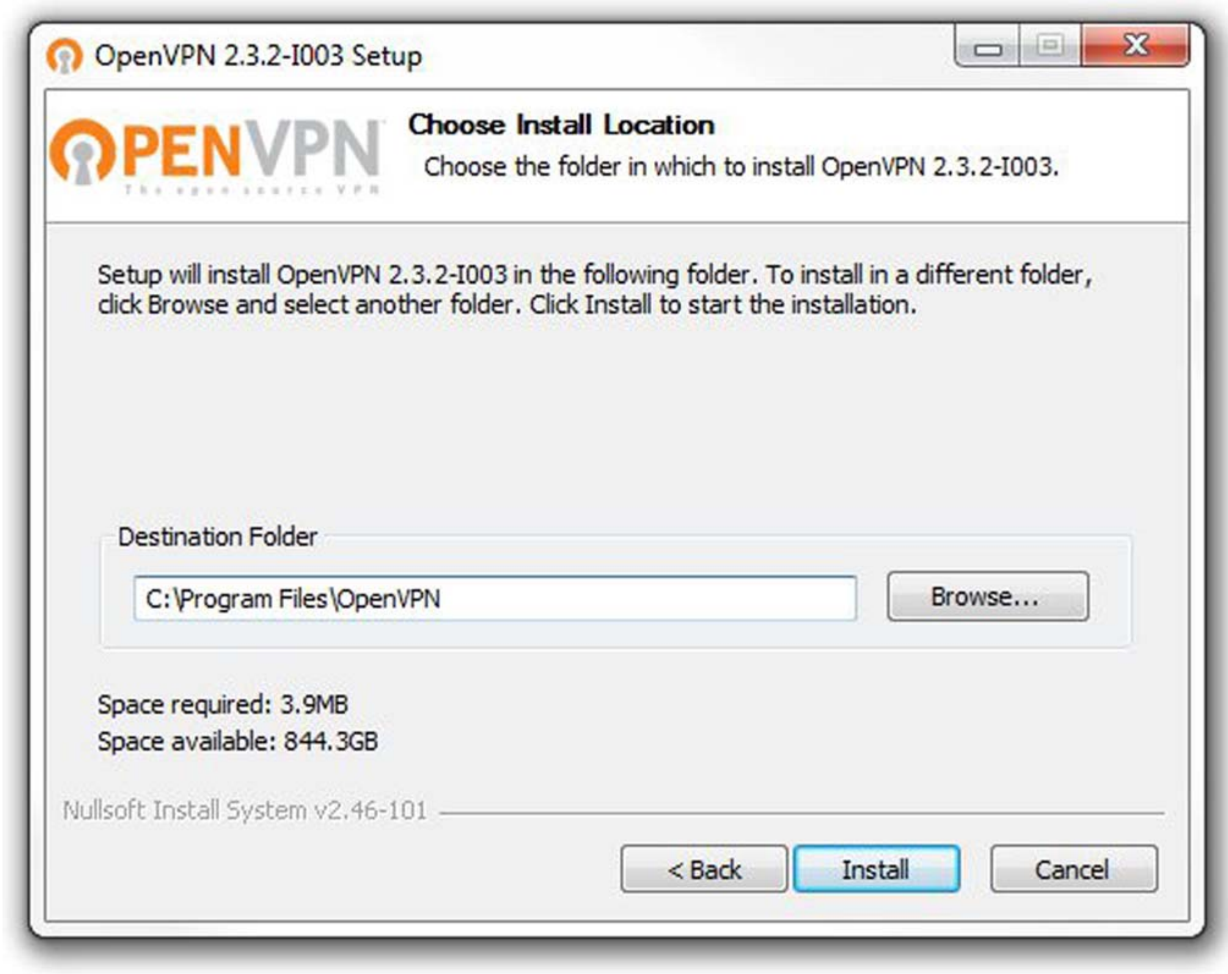
Position your mouse over a component to see its description.

Nullsoft Install System v2.46-101

Figure 138:Installation of OpenVPN - components

The installation wizard, as seen in figure 139 on page 276, allows you to select the directory in which you want to install the OpenVPN program. If you want to install the OpenVPN in a directory other than the default directory, use the following work steps:

□ Using the “`Browse`” button, navigate to the appropriate directory.
□ Start the installation, click the “`Install`” button and wait for the process to be completed.
□ Click the "`Next`" button.
□ Click the “`Finish`” button.



OpenVPN 2.3.2-I003 Setup

Choose Install Location

Choose the folder in which to install OpenVPN 2.3.2-I003.

Setup will install OpenVPN 2.3.2-I003 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder

C:\Program Files\OpenVPN

Space required: 3.9MB

Space available: 844.3GB

Nullsoft Install System v2.46-101

Figure 139:Installation of OpenVPN – location

B General Information

B.1 Abbreviations used

ACA	AutoConfiguration Adapter
ACL	Access Control List
BOOTP	Bootstrap Protocol
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
FDB	Forwarding Database
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IP	Internet Protocol
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
F/O	Optical Fiber
MAC	Media Access Control
MIB	Management Information Base
MRP	Media Redundancy Protocol
MSTP	Multiple Spanning Tree Protocol
NMS	Network Management System
NTP	Network Time Protocol
PC	Personal Computer
PTP	Precision Time Protocol
QoS	Quality of Service
RFC	Request For Comment
RM	Redundancy Manager
RSTP	Rapid Spanning Tree Protocol
SCP	Secure Copy
SFP	Small Form-factor Pluggable
SFTP	SSH File Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TP	Twisted Pair
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTC	Coordinated Universal Time

VLAN	Virtual Local Area Network

B.2 Technical Data

You will find the technical data in the document “User Manual Installation”.

B.3 Maintenance

Hirschmann is continually working on improving and developing their software. Check regularly whether there is an updated version of the software that provides you with additional benefits. You find information and software downloads on the Hirschmann product pages on the Internet (http://www.hirschmann.com).

C Index

D Further support

Technical questions

For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly.

You find the addresses of our partners on the Internet at http://www.hirschmann.com.

A list of local telephone numbers and email addresses for technical support directly from Hirschmann is available at https://hirschmann-support.belden.com.

This site also includes a free of charge knowledge base and a software download section.

Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors on three counts with its complete range of innovative services:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- Training offers you an introduction to the basics, product briefing and user training with certification.
  You find the training courses on technology and products currently available at http://www.hicomcenter.com.
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.

Internet:
http://www.hicomcenter.com

HIRSCHMANN

A BELDEN BRAND