HIRSCHMANN
A BELDEN BRAND

User Manual

Configuration
OWL3G (Industrial Cellular Router)

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
Tel.: +49 1805 141538

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.

The "Installation" user manual contains a device description, safety instructions, a description of the display, and the other information that you need to install the device.

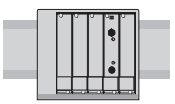
Key

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 Instruction

General safety instructions

You operate this device with electricity. The safe operation of the device depends on proper handling during transportation, storage and assembly, and proper use of operation and maintenance procedures. Improper use of this device can cause injury or property damage.

- ☐ Read this documentation, safety instructions and warnings before connecting any cables.
- ☐ Never start an operation with damaged components.
- ☐ The device does not contain any service components. If the device is not functioning correctly, or if it is damaged, turn off the power supply and return the device to Hirschmann for inspection.

⚠ 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.

Qualification requirements for personnel

- ☐ Allow qualified personnel to work on the device who have the following characteristics:
  - ▶ Properly trained personnel who have practical knowledge and experience. This is the prerequisite for grounding and labeling circuits, devices, and systems in accordance with current technology safety standards.
  - ▶ Qualified personnel are aware of the dangers that exist in their work.

- Qualified personnel are familiar with appropriate measures against these hazards in order to reduce the risk for themselves and others.
- Qualified personnel receive training on a regular basis.

Intended usage

- ☐ Use the product only for the application cases described in the Hirschmann product information, including this manual.
- ☐ Operate the product according to the technical parameters. See chapter 6 for details.
- ☐ Connect components which are suitable for the requirements of the specific application case to the product.

National and international safety regulations

Verify that the electrical installation meets local or nationally applicable safety regulations.

Working voltage

- ☐ Connect only a working voltage that corresponds to the type plate of your device.
- ☐ Make sure the following requirements are met every time you connect the electrical conductors:
  - The power supply conforms to overvoltage category I or II.
  - The power supply has an easily accessible disconnecting device (such as a switch or a plug) which is clearly identified. So in case of an emergency, it is clear which disconnecting device belongs to which power supply cable.
  - The electrical wires are voltage-free.
  - The power supply is Class 2 compliant.
  - The working voltage inputs are designed for operation with safety extra-low voltage. Connect only SELV circuits with voltage restrictions in line with IEC/EN 60950-1 to the working voltage connections.

- The wire diameter of the power supply cable is at least 1 mm² (North America: AWG16) on the working voltage input.
- The wire diameter of the ground conductor is at least 1 mm² (North America: AWG16).
- The power supply cables used are permitted for the temperature range required by the application case.
  The power cords are suitable for ambient air temperatures of at least 167 °F (75 °C). The power cord wires are made of copper.

Switch on the operating voltage for the device only when the following requirements are fulfilled:

- The housing is closed
- The terminal block is wired correctly
- The terminal block for the operating supply is connected

Installation site requirements

☐ Verify that there is at least 4 in (10 cm) of space above and below the device.
☐ Verify that there is at least 0.8 in (2 cm) of space on the right and left sides of the device.

Housing

The router cannot be opened.
☐ Never insert pointed objects (narrow screwdrivers, wires, etc.) into the device or into the connection terminals for electric conductors. Do not touch the connection terminals.

Please, observe the following instructions:

Note: Keep the SIM card away from small children as it can be easily swallowed.

☐ Before handling the SIM card, turn off the router and disconnect it from the power supply.
☐ The SIM card must not exceed the maximum voltage 30 V DC power connector on the router.

- ☐ Do not expose the router to extreme ambient conditions. Protect the router against dust, moisture and high temperature.
- ☐ The router should not be used at the petrol stations and around flammable and explosive materials. We remind the users of the duty to observe restrictions concerning the utilization of radio devices at petrol stations, in chemical plants, or in the course of blasting works in which explosives are used.
- ☐ When using the router in the close proximity of personal medical devices, such as cardiac pacemakers or hearing aids, you must proceed with heightened caution.
- ☐ If the router is in the proximity of TV sets, radio receivers, personal computers, and telephone it may cause interference.
- ☐ It is recommended that you should create an appropriate copy or backup of the important settings that are stored in the memory of the device.

1 Basic Information

Hirschmann Automation and Control GmbH designed the OWL Industrial Cellular Router for wireless communication in mobile networks using HSPA+, UMTS, EDGE or GPRS technology. Due to the high speed of data transfer up to 14.4 Mbit/s (download) and up to 5.76 Mbit/s (upload). This 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.

You can configure the router using either a web browser or Secure Shell (SSH). The Hirschmann Automation and Control GmbH Technical Support also uses the Secure Shell to help you locate problems with your device. Configuring the functions in the router using a web browser is described in this Configuration Manual. The technical parameters of your router can be found in UM-Installation Manual.

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

Diagnostic functions, which provide for continuous communication, include an automatic inspection of a PPP connection, offering an automatic restart feature in case of an unexpected termination of the connection. Another diagnostic function is the hardware watchdog, which monitors the status of the router.

Automatic check of PPP connection offering an automatic restart function in case the connection fails, hardware watchdog monitoring the status of the router.

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 Web Configuration

Note: Wireless transmission 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.

For monitoring, configuring and managing the router, use the GUI interface which can be accessed 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.

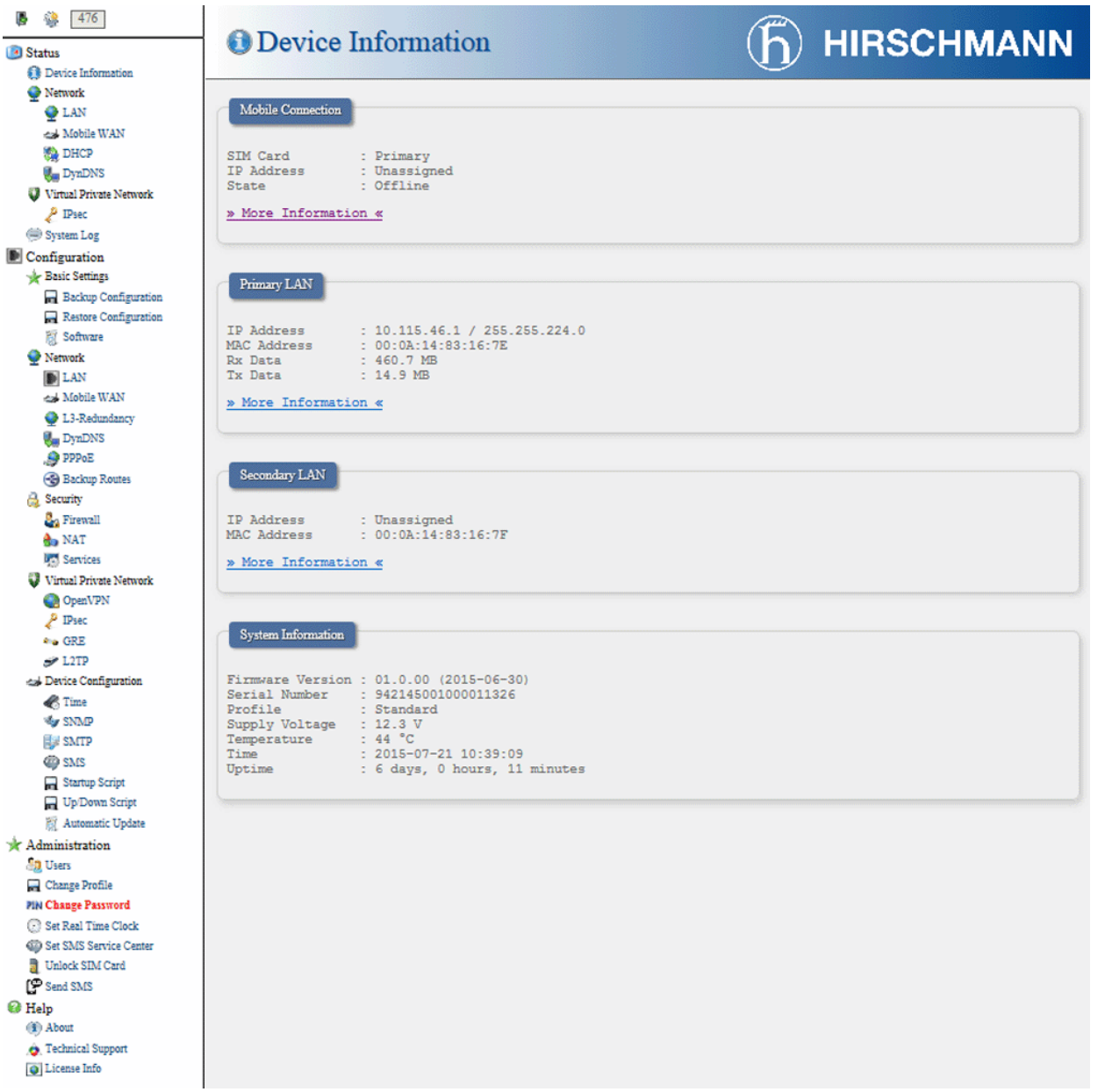


Figure 1: Example of the Web Configuration

The left part of the GUI interface contains the menu with sections for monitoring (Status), configuration (Configuration), and administration (Administration) of the router.

Note: For increased security of the network being managed by the router, change the default router password. When the default password of the router is set, the "Change password" menu item is highlighted in red.

After the green LED illuminates, it is possible to restore the initial settings of the router by pressing the "RST" button on the front panel. If you press the "RST" button, the configuration is restored 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 web configuration using the secure 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 install a security certificate. If your browser reports a disagreement in the domain, you can prevent this message by using the following procedure.

Since the domain name in the certificate is the given MAC address of the router, it is necessary to access the router via this domain name (use dash separators instead of colons). To enable this, add a DNS record in your DNS system:

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

To access the router with MAC address 00:11:22:33:44:55 securely, type the address https://00-11-22-33-44-55 into the web browser.

1.2 Status

1.2.1 Device Information

A summary of basic router information and its activities can be accessed by selecting the "Device Information" menu item. This dialog is the first 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
- System Information

Mobile Connection

Parameter	Description
SIM Card	Identification of the SIM card (Primary or Secondary)
Interface	Defines the interface
Flags	Displays network interface flags
IP Address	IP address of the interface
MTU	Maximum packet size that the equipment is able to transmit
Rx Data	Total number of received bytes
Rx Packets	Received packets
Rx Errors	Erroneous received packets
Rx Dropped	Dropped received packets
Rx Overruns	Lost received packets because of overload
Tx Data	Total number of sent bytes
Tx Packets	Sent packets
Tx Errors	Erroneous sent packets
Tx Dropped	Dropped sent packets
Tx Overruns	Lost sent packets because of overload
Uptime	Indicates how long the connection to mob. network is established

Table 1: Mobile Connection

1.2.2 LAN 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 router displays information divided into the following frames:

- The "Primary LAN" frame displays information about the eth0 interface.
- The "Secondary LAN" frame displays information about the eth1 interface.
- The "System Information" frame displays information about the hardware and firmware of the router.

The information that the router displays depends on the router configuration, see “LAN” on page 34.

System Information

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

Table 2: System Information

1.2.3 Network

LAN

To view information about the interfaces and the routing table, select the "LAN" menu item. 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.
ppp0	Displays the active PPP connection status to the mobile network (GSM module is connected)
tun0	Displays the OpenVPN tunnel interface status.
ipsec0	Displays the IPSec tunnel interface status.
gre1	Displays the GRE tunnel interface status
lo	Displays the Local loopback interface status.

Table 3: Description of Interfaces in LAN Status

Each of the interfaces displays the following information:

Parameter	Description
HWaddr	Hardware (unique) address of networks interface
inet	IP address of interface
P-t-P	IP address second ends connection
Bcast	Broadcast address
Mask	Mask of network
MTU	Maximum packet size that the equipment is able to transmit
Metric	Number of routers, over which packet must go trough
RX	packets - received packetserrors - number of errorsdropped - dropped packetsoverruns - incoming packets lost because of overloadframe - wrong incoming packets because of incorrect packet size
TX	packets - transmit packetserrors - number of errorsdropped - dropped packetsoverruns - outgoing packets lost because of overloadcarrier - wrong outgoing packets with errors resulting from the physical layer
collisions	Number of collisions on physical layer
txqueuelen	Displays the Transmit Queue Length. This parameter is the number of packets in the buffer of the router waiting for transmission.

Table 4: Description of Information in LAN Status

Parameter	Description
RX bytes	Total number of received bytes
TX bytes	Total number of transmitted bytes

Table 4: Description of Information in LAN Status

You can view the status of the connection to mobile network from the network information. If the connection to a mobile network is active, it is displayed in the "Interfaces" frame as a `ppp0` interface. At the bottom of the dialog, the router displays a Route Table.

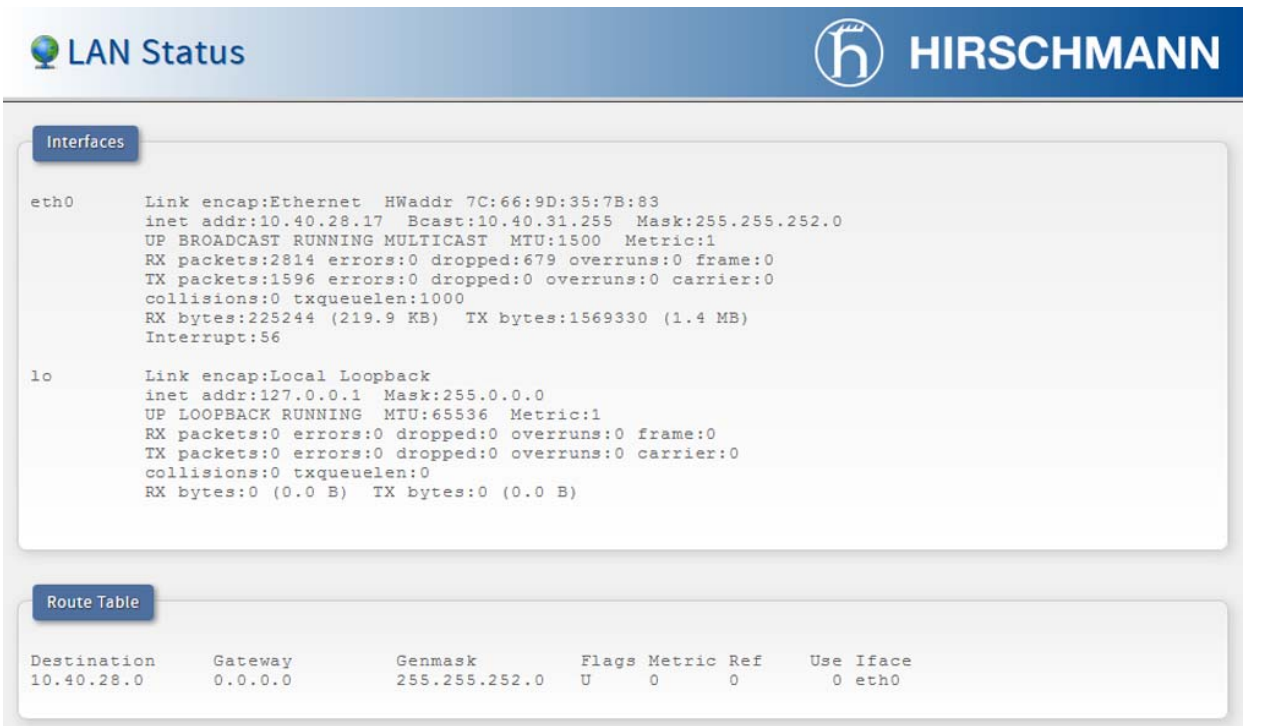


Figure 2: LAN Status

Mobile WAN

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

The first part of this 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	State of the network registration
Operator	Specifies the mobile network provider in whose network the router is installed
Technology	Transmission technology
PLMN	Code of mobile network provider
Cell	Cell to which the router is connected
LAC	Location Area Code - unique number assigned to each location area
Channel	Channel on which the router communicates
Signal Strength	Signal strength of the selected cell
CSQ	Cell Signal Quality, relative value is given by RSSI (dBm). 2-9 range means Marginal, 10-14 range means OK, 15-16 range means Good, 20-30 range means excellent.
Manufacturer	Module manufacturer
Model	Type of module
Revision	Revision of module
IMEI	IMEI (International Mobile Equipment Identity) number of module
ICCID	Integrated Circuit Card Identifier is international and unique serial number of the SIM card.

Table 5: Mobile Network Information

The adjacent cells, highlighted in red, have a close signal quality, which means that there is evidence of frequent changing between the current and the highlighted cell.

The next frames of this dialog display information about the quality of the connection in each period.

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

Table 6: Description of Period

Parameter	Description
Signal Min	Minimal signal strength
Signal Avg	Average signal strength
Signal Max	Maximal signal strength

Table 7: Mobile Network Statistics

Parameter	Description
Cells	Number of switch between cells
Availability	Availability of the router via the mobile network (expressed as a percentage)

Table 7: Mobile Network Statistics

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

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

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, number of connections for both SIM cards.

Parameter	Description
RX data	Total volume of received data
TX data	Total volume of sent data
Connections	Number of connection established to mobile network

Table 8: Traffic Statistics

The last frame of the dialog, the "Mobile Network Connection Log", informs you about the mobile network connection and connection problems.

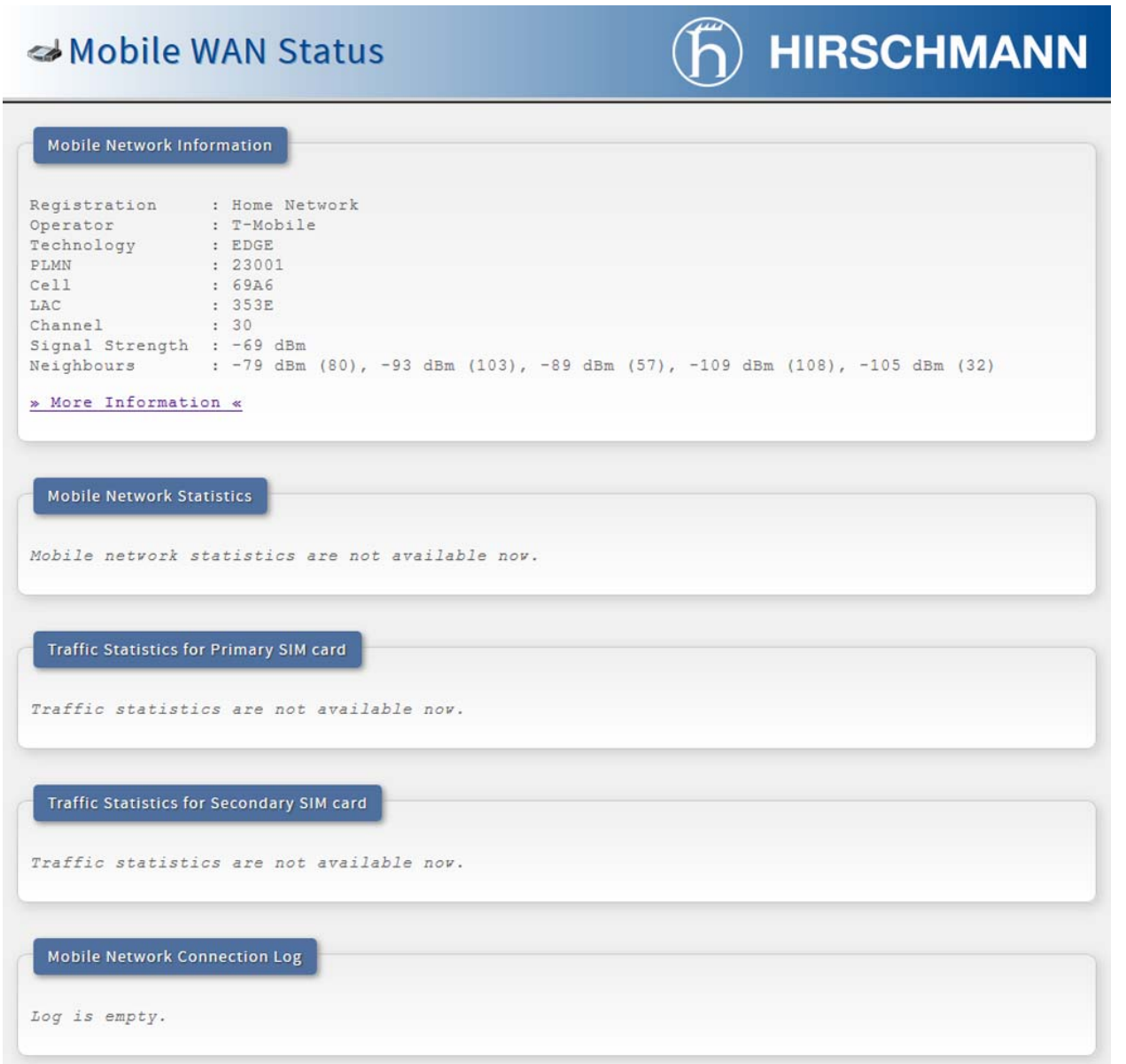


Figure 3: Mobile WAN Status

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, the IP address of the DNS server.

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

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

Table 9: 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)".

Figure 4: DHCP Status

DynDNS status

The router displays the result of a DynDNS record update, from the www.dyndns.org server, in the "DynDNS" dialog.

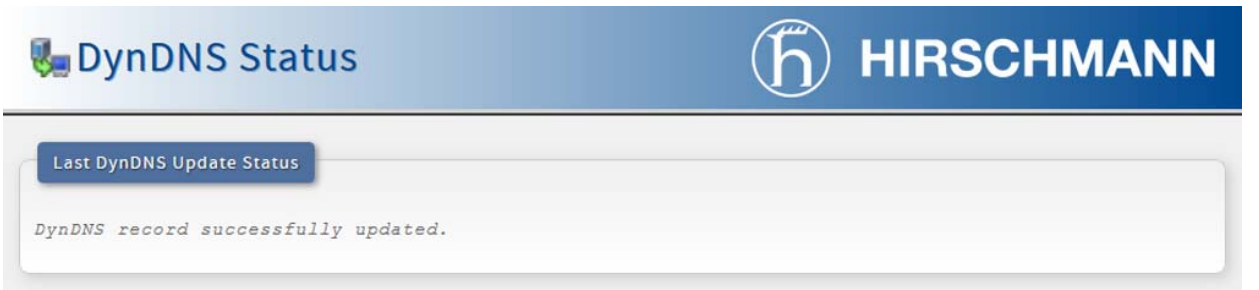


Figure 5: DynDNS Status

When the router detects a DynDNS record update, the router can display the following possible 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, assign a public IP address to the SIM card inserted into your router.

1.2.4 Virtual Private Network

IPsec

In the "IPsec" dialog, you can view information about the current IPsec tunnel status. 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.

Figure 6: IPsec Status

1.2.5 System Log

The router displays connection problems, in the "System Log" dialog. The router displays detailed reports from individual applications. 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, the "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 the new file is created for storing the system log. After completion of 1000 lines in the second file, the first file is overwritten with the 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 decimal number sets the maximal number of lines in one log file.
- Option "-R" followed by hostname or IP address enables logging to a remote syslog daemon.

If the remote syslog deamon uses a Linux OS, then enable remote logging, typically by 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.

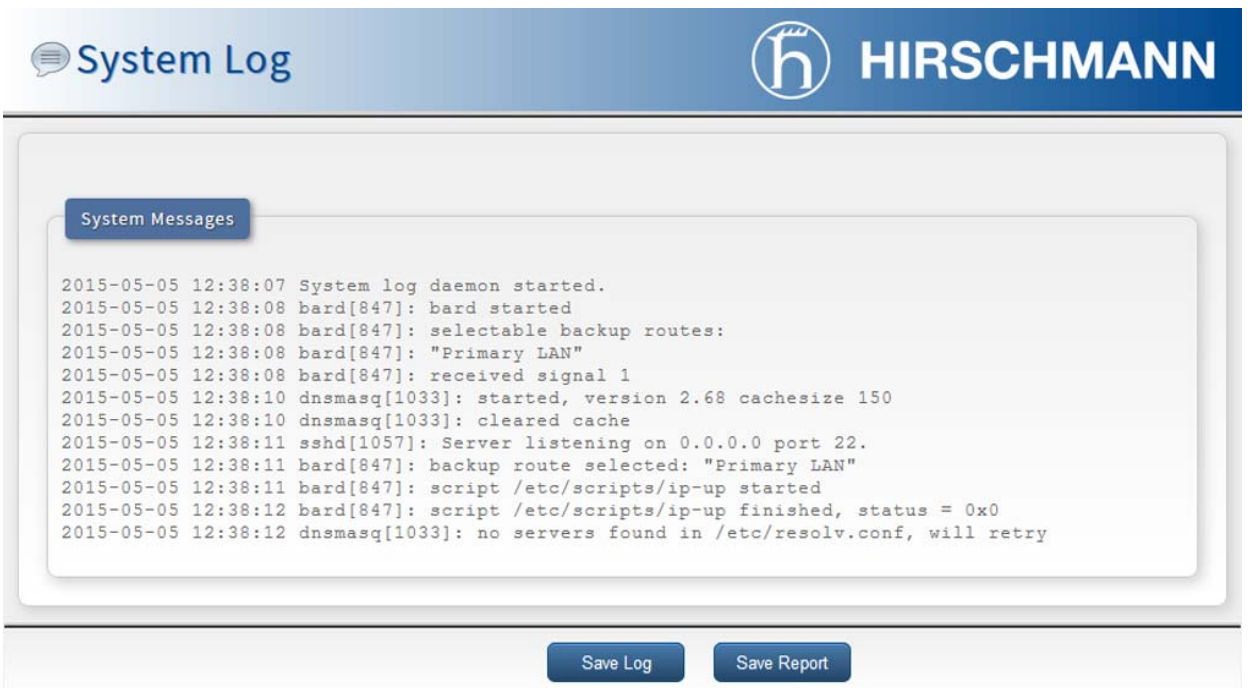


Figure 7: System Log

Example of logging into the remote daemon at 192.168.2.115:

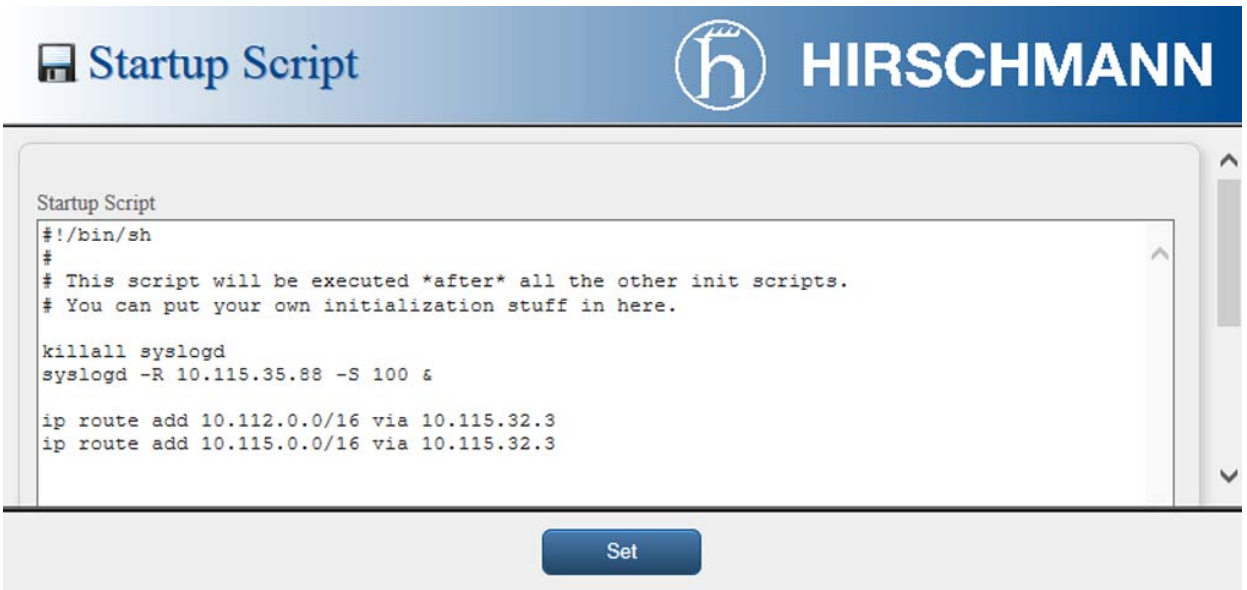


Figure 8: Example program syslogd start with the parameter -r

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. Use the "Browse" button to navigate to the directory containing the configuration file you wish to load on the router (.cfg).

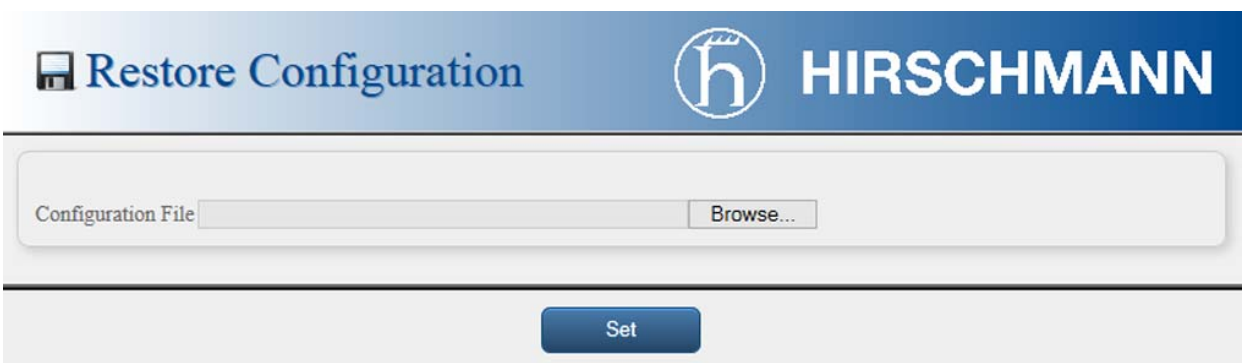


Figure 9: Restore Configuration

Software

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

- ☐ Use the "Browse" button to navigate to the directory containing the firmware file you wish to upload to the router.
- ☐ Then press the "Update" button.

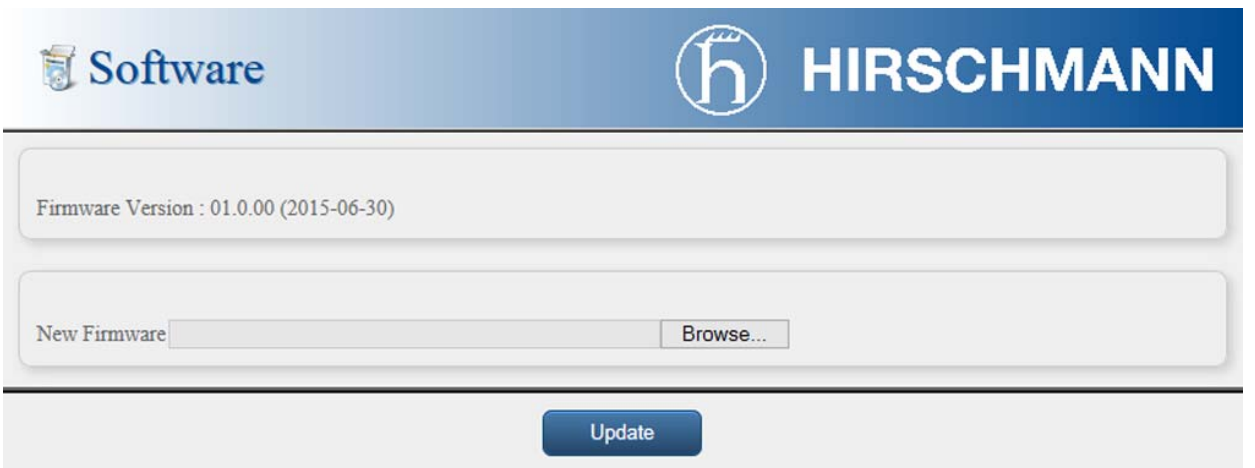
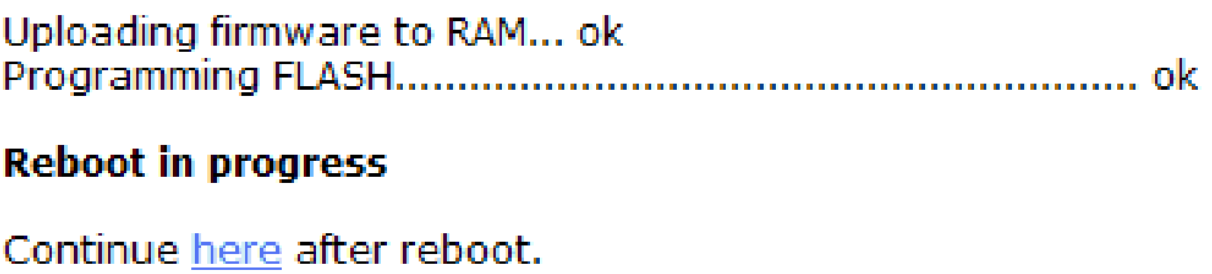


Figure 10: Software

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



Note: When you upload firmware intended for a different device you can cause damage of the router. A constant supply of power has to be maintained during updating of the firmware.

1.3.2 Network

LAN

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

Parameter	Description
DHCP Client	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	Fixed set IP address of network interface ETH.
Subnet Mask	IP address of Subnet Mask.
Bridged	no - router is not used as a bridge (default) yes - router is used as a bridge
Media type	Auto-negation - 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.
Default Gateway	IP address of router default gateway. When entering IP address of default gateway, all packets for which the record was not found in the routing table, sent to this address.
DNS server	IP address of DNS server of router. Address where they are forwarded to all DNS questions on the router.

Table 10: 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 56.

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/from the existing bridge.

The DHCP server assigns the IP address, the gateway IP address (IP address of the router) and the IP address of the DNS server (IP address of the router) to the connected clients. If the user enters these values in manually 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 clients 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	If checked, dynamic DHCP server enabled.
IP Pool Start	Start of IP addresses allocated to the DHCP clients.
IP Pool End	End of IP addresses allocated to the DHCP clients.
Lease time	Client can use the IP address for this amount of time in seconds.

Table 11: Configuration of Dynamic DHCP Server

Parameter	Description
Enable static DHCP leases	If checked, static DHCP server enabled.
MAC Address	MAC address of a DHCP client.
IP Address	Assigned IP address.

Table 12: 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 may occur if the network administrator overlaps the ranges.

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

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

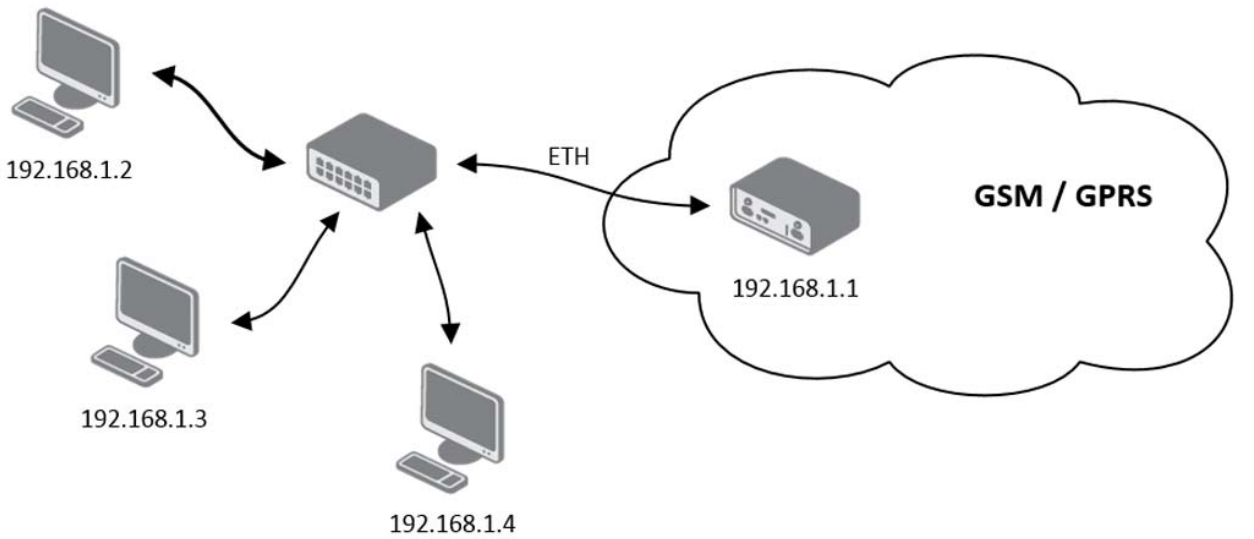


Figure 11: Topology of LAN Configuration Example 1

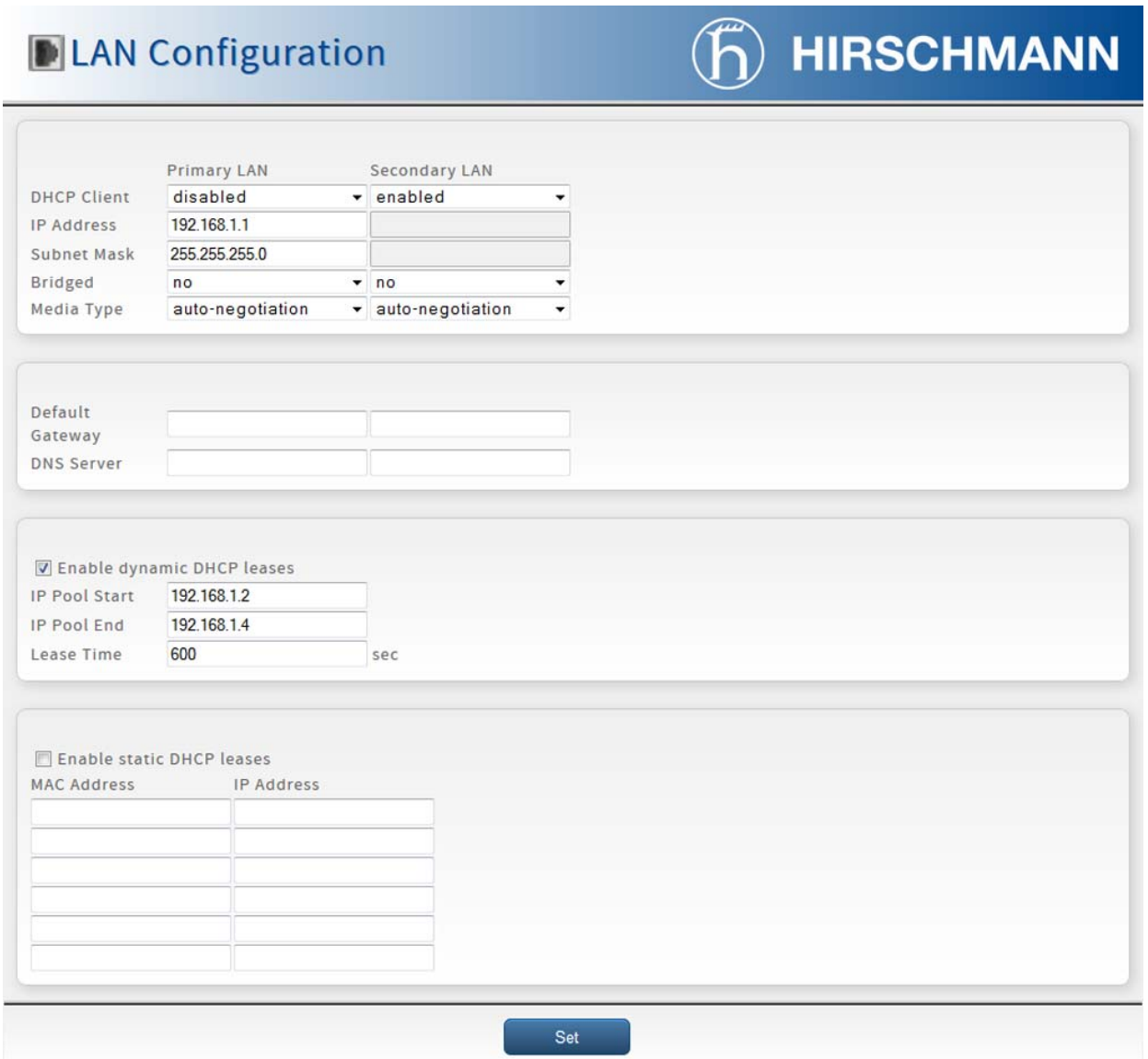


Figure 12: LAN Configuration Example 1

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

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

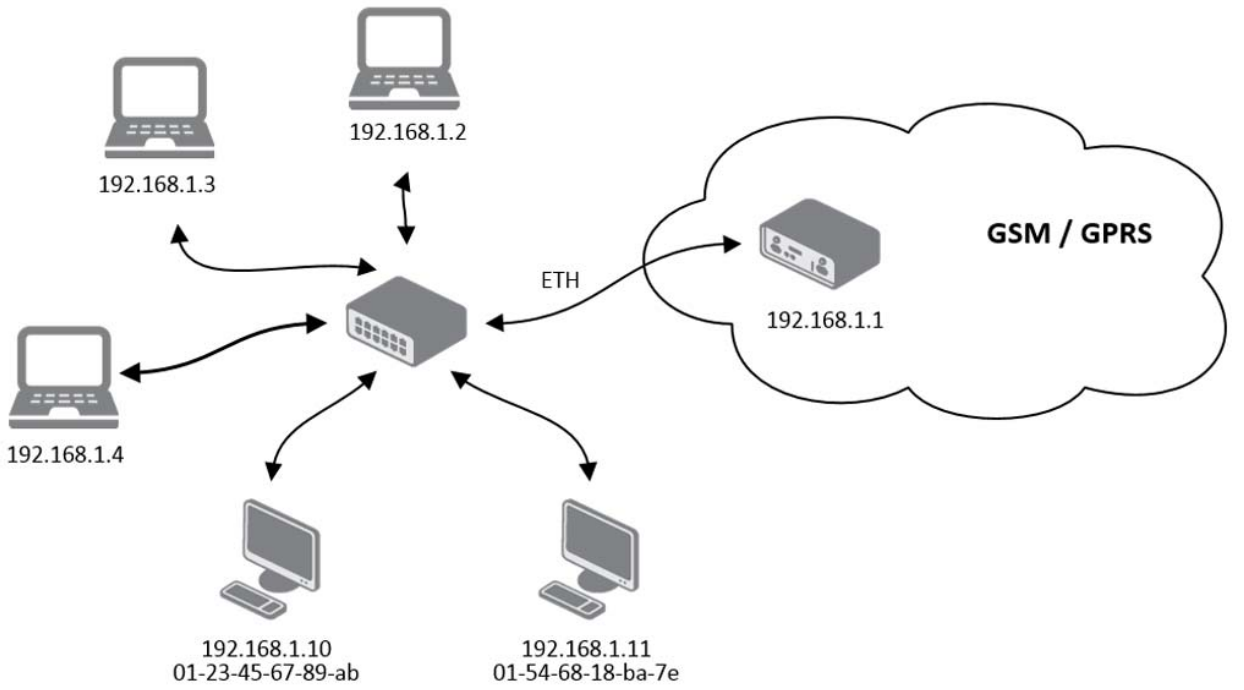


Figure 13: Topology of LAN Configuration Example 2

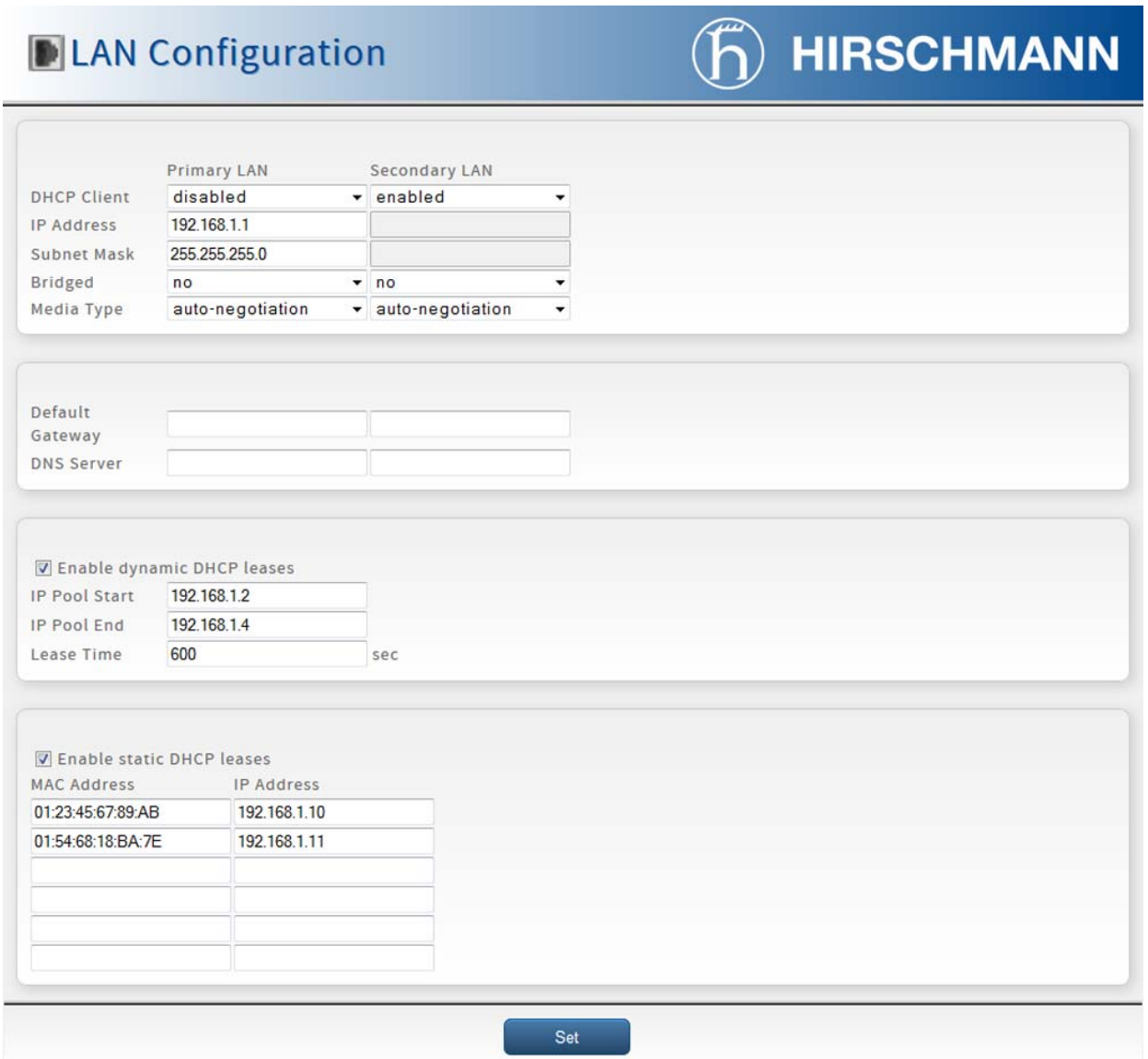


Figure 14: LAN Configuration Example 2

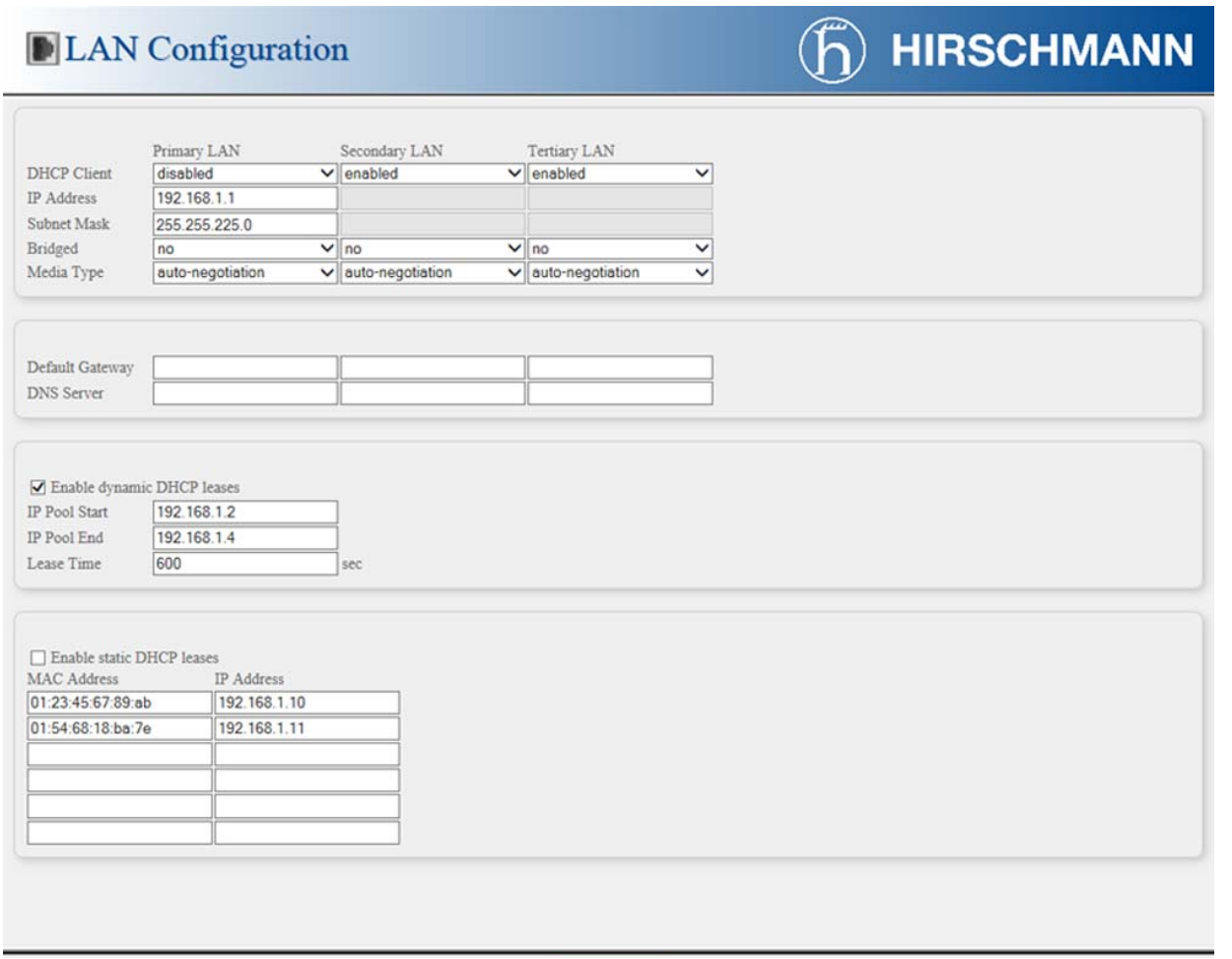


Figure 15: LAN Configuration Example 2

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

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

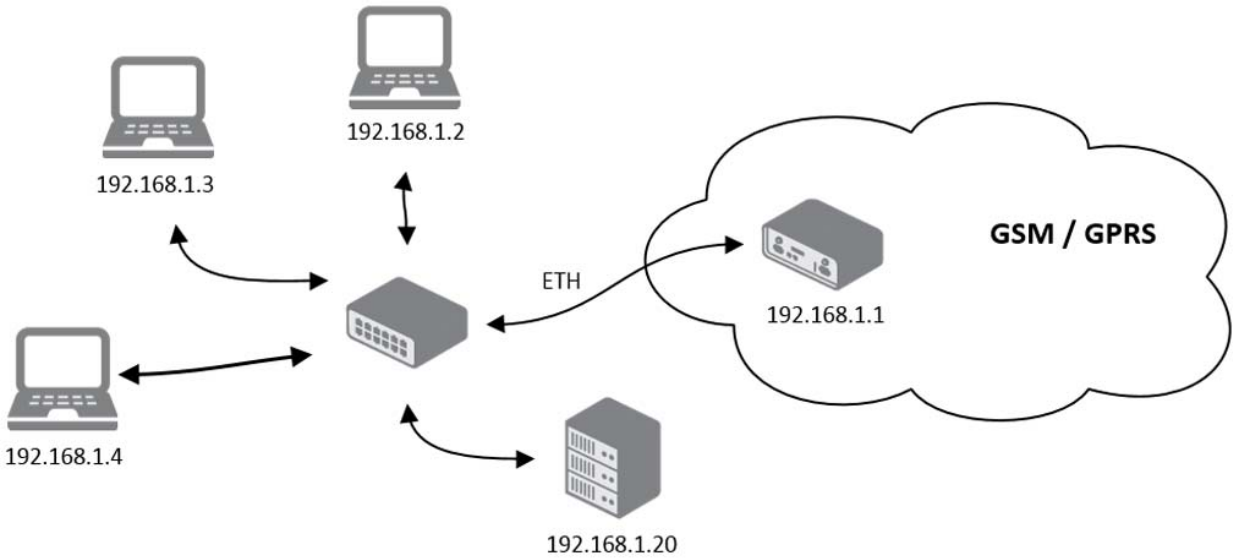


Figure 16: Topology of LAN Configuration Example 3

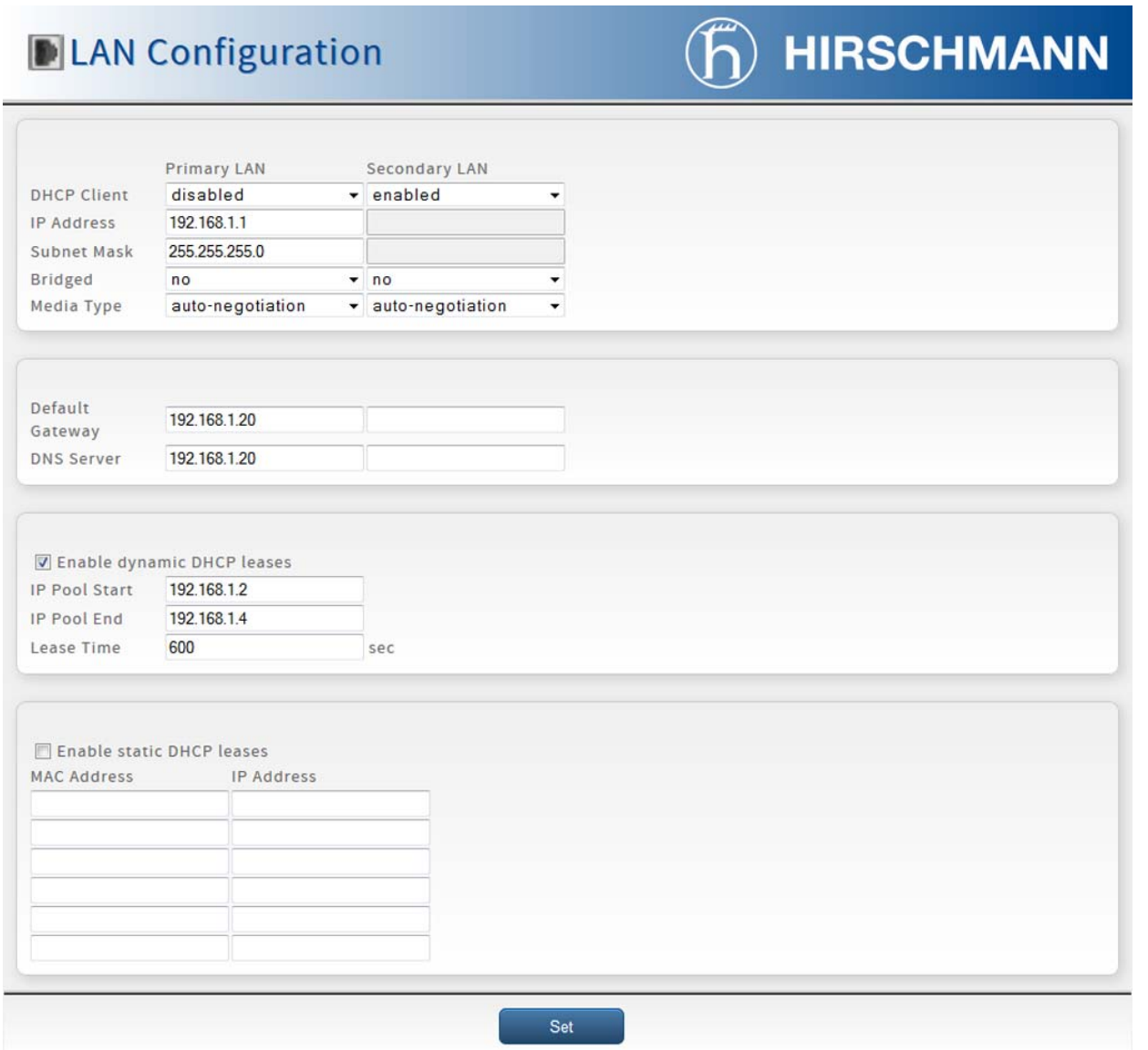


Figure 17: LAN Configuration Example 3

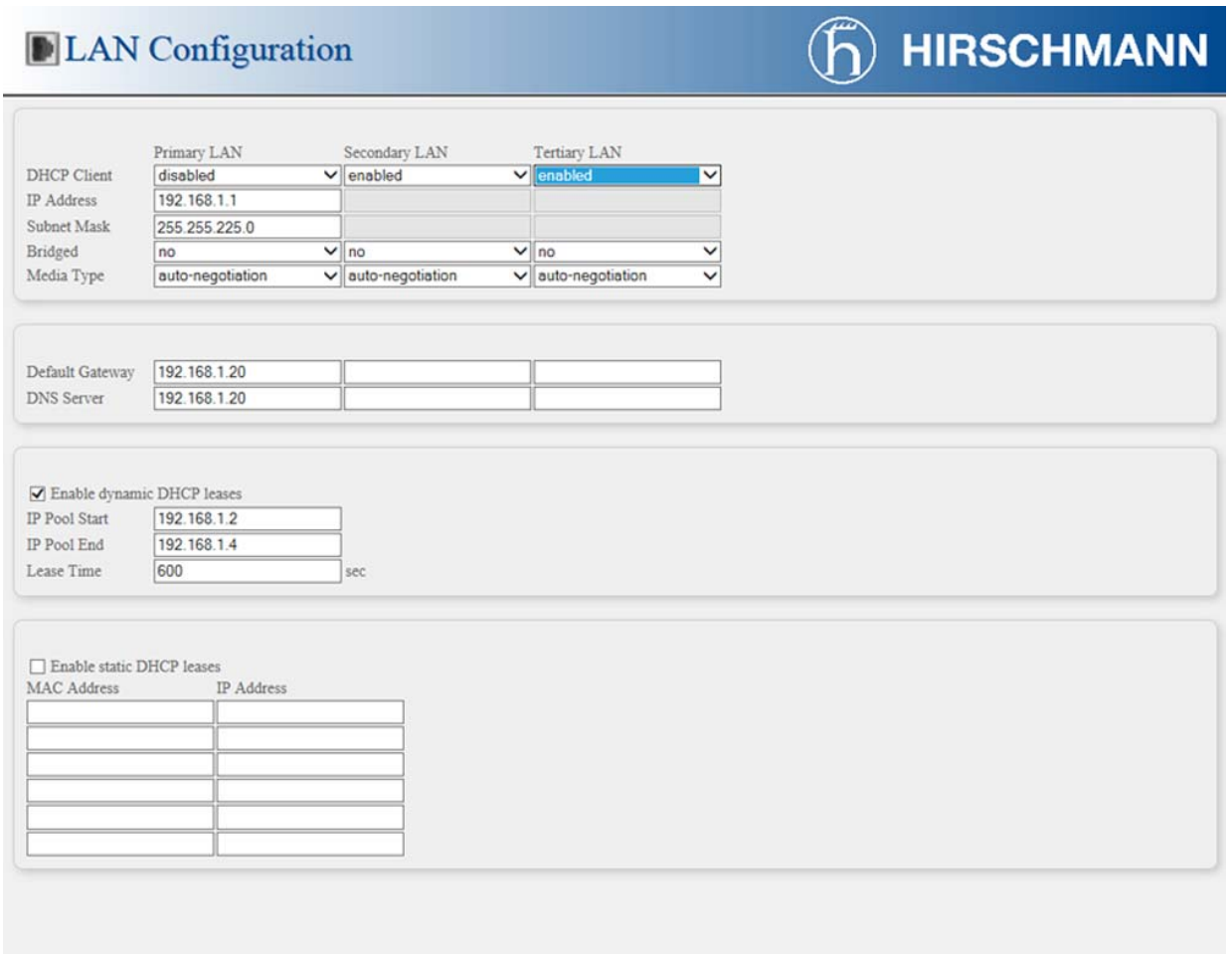


Figure 18: LAN Configuration Example 3

Mobile WAN

To configuring an interface to connect to the mobile network, 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	Network identifier (Access Point Name)
Username	User name for logging into the GSM network
Password	Password for logging into the GSM network
Authentication	Authentication protocol in GSM network: ▶ PAP or CHAP - authentication method is chosen by router ▶ PAP - it is used PAP authentication method ▶ CHAP - it is used CHAP authentication method
IP Address	IP address of SIM card. The user manually enters the IP address, only in the case the IP address was assigned of the mobile network provider.
Phone Number	Telephone number to dial GPRS or CSD connection. Router as a default telephone number used *99***1 #.
Operator	This item can be defined PLNM preferred carrier code
Network type	▶ Automatic selection - router automatically selects transmission method according to the availability of transmission technology ▶ Furthermore, according to the type of router - it's also possible to select a specific method of data transmission (GPRS, UMTS)
PIN	PIN parameter should be set only if it requires a SIM card router. SIM card is blocked in case of several bad attempts to enter the PIN.
MRU	Maximum Receiving Unit - It's an identifier of maximum size of packet, which is possible to receive in a given environment. Default value is 1500 B. Other settings may cause incorrect transmission of data.
MTU	Maximum Transmission Unit - It's an identifier of max. size of packet, which is possible to transfer in a given environment. Default value is 1500 B. Other settings may cause incorrect transmission of data.

Table 13: Mobile WAN Connection Configuration

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 not filled in, the mobile network provider automatically assigns an IP address when the router establishes a connection. If you assign an IP address, then the router accesses the network quicker.
- If the APN field is not filled in, the router automatically selects the APN using the IMSI code of the SIM card. If the PLMN (operator number format) is not in the list of APN, then the router uses the default APN "internet". The mobile network provider defines the APN.
- If the word `blank` is entered 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 provider.

When the router is unsuccessfully 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 provider. Setting the option to `set manually` allows you to specify the IP addresses of the Primary DNS servers manually in the "DNS Server" field.

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, at regular time 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 check 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 ping for example, the DNS server of mobile network provider.

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 provider, set the "Check Connection" parameter to `enabled + bind`. The `disabled` option deactivates checking the connection to mobile network.

Parameter	Description
Ping IP Address	Destinations IP address or domain name of ping queries.
Ping Interval	Time intervals between the outgoing pings.

Table 14: 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 requests 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	With this parameter you can set the maximum expected amount of data transmitted (sent and received) over GPRS in one billing period (month).
Warning Threshold	This parameter determines 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	This parameter sets the day of the month in which the billing cycle starts for the SIM card used. When the billing period starts is defined by the service provider that issued the SIM card. The router begins to count the amount of transferred data starting on this day.

Table 15: Data Limit Configuration

Switch between SIM Cards Configuration

At the bottom of this configuration form is possible to 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.

Parameter	Description
Default SIM card	This parameter 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 connection to mobile network using an SMS message.
Backup SIM card	Specifies the backup APN or SIM card, that the router uses in accordance with the specified rules.

Table 16: Default and Backup SIM Configuration

If you select none from the "Backup SIM card" drop down menu, then the parameters "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" cause the router to go into the off line mode.

Parameter	Description
Switch to other SIM card when connection fails	If the connection to mobile network fails, then this parameter enables the router to toggle to the secondary SIM card or secondary APN of the SIM card. Failure of the connection 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	When the router detects roaming, this parameter allows the router change to the secondary SIM card or secondary APN of the SIM card. 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	This parameter allows the router to change to the secondary SIM card or secondary APN of the SIM card, when the data limit of default APN is exceeded. This parameter also enables changing back to the default SIM card, when the data limit is not exceeded.
Switch to default SIM card after timeout	This parameter specifies the method, of how the router attempts to change back to the default SIM card or the default APN.

Table 17: Switch 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 18: 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, from a PC which is connected to the ETH port of the router. The IP address of the SIM card is assigned to the PC.

The changes in settings will apply after pressing the "Set" button.

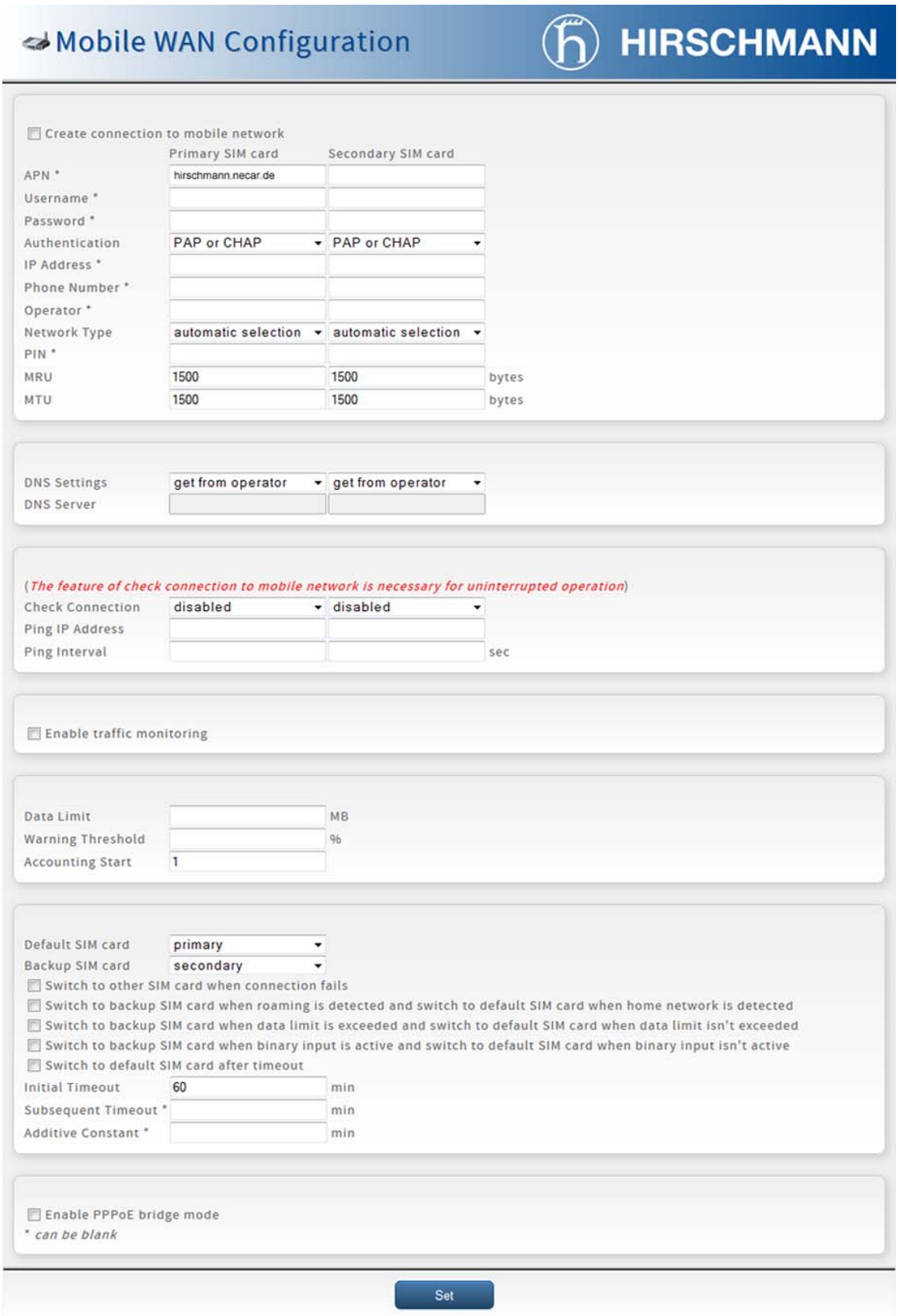


Figure 19: Mobile WAN Configuration

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 60s for the primary SIM card and on the address www.google.com with the time interval 80 s for the secondary SIM card. In the case of data stream on the router the control pings are not sent, but the data stream is monitored.

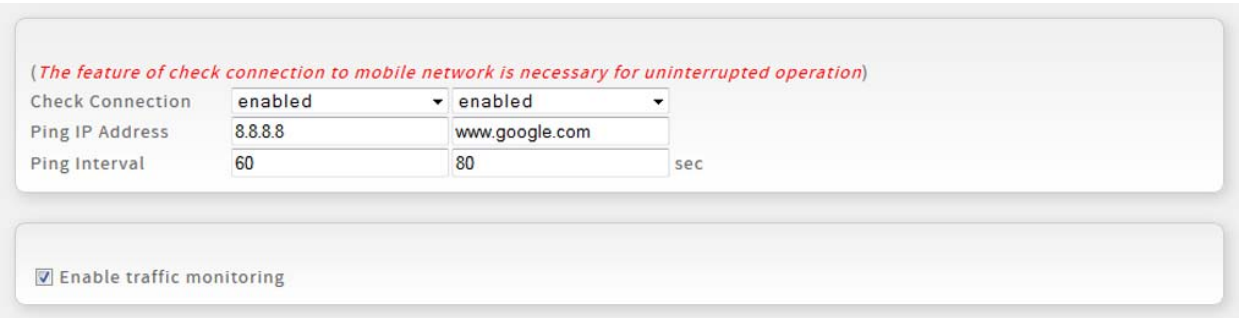


Figure 20: Mobile WAN Configuration Example 1

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

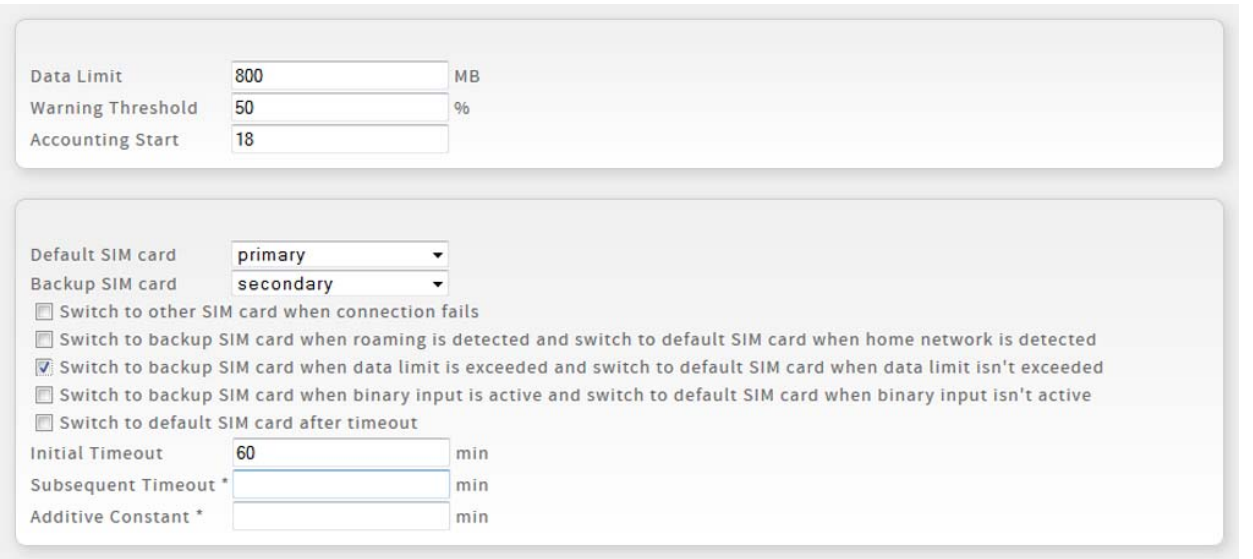


Figure 21: Mobile WAN Configuration Example 2

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).

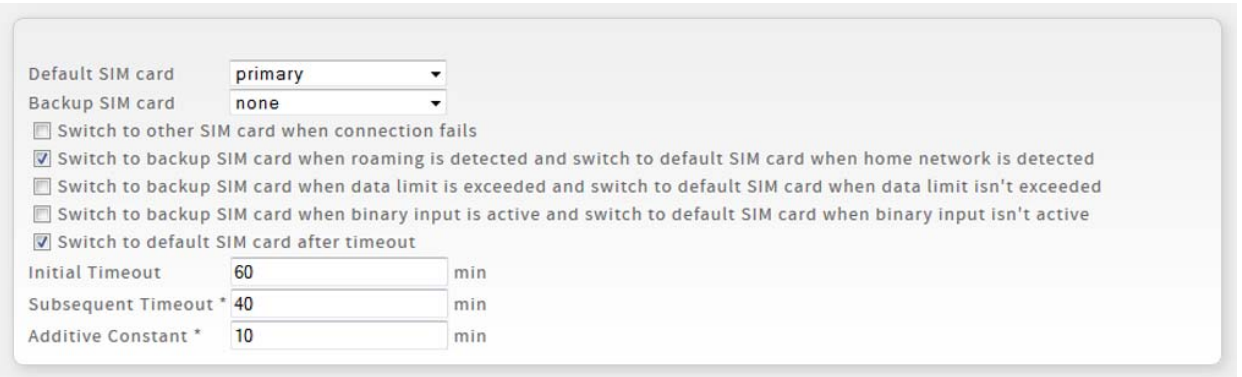


Figure 22: Mobile WAN Configuration Example 3

L3-Redundancy

To configure the VRRP protocol, open the "L3-Redundancy" dialog in the "Configuration" section of the main menu. The VRRP protocol (Virtual Router Redundancy Protocol) is a technique that you use to delegate routing from the main router to another (backup) router in case of the main router families. To activate this protocol, mark the check box of the first parameter in this dialog, "Enable VRRP". The table below describes the meaning of other parameters:

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

Table 19: VRRP Configuration

Parameter	Description
Virtual Server ID	This parameter distinguishes one virtual router on the network from others. Assign the value to both the main and backup routers.
Host Priority	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 19: VRRP Configuration

If you mark the "Check connection" check box, then the currently active router (main/backup) sends test messages (ping requests). The "Check connection" function is intended to evaluate the throughput of the route based on the role of the router when changed from the main to backup or backup to main.

Parameter	Description
Ping IP Address	Specifies the destinations 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 20: 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 provider.

The router has another function to evaluate the state of the active route, the "Enable traffic monitoring" check box. When you enable this function, the router monitors the route for any packet, other than a ping, before the "Ping Timeout" timer expires. If the "Ping Timeout" timer expires with no response received, the original message is considered to be a test message and accelerated testing using ping messages follows. The router sends the messages in the interval specified in the "Ping Interval" field. The router considers the first ping message sent to be the second test message in a series of probes. The router limits the number of probes to the value specified in the "Ping Probes" field.

Example of the VRRP protocol:

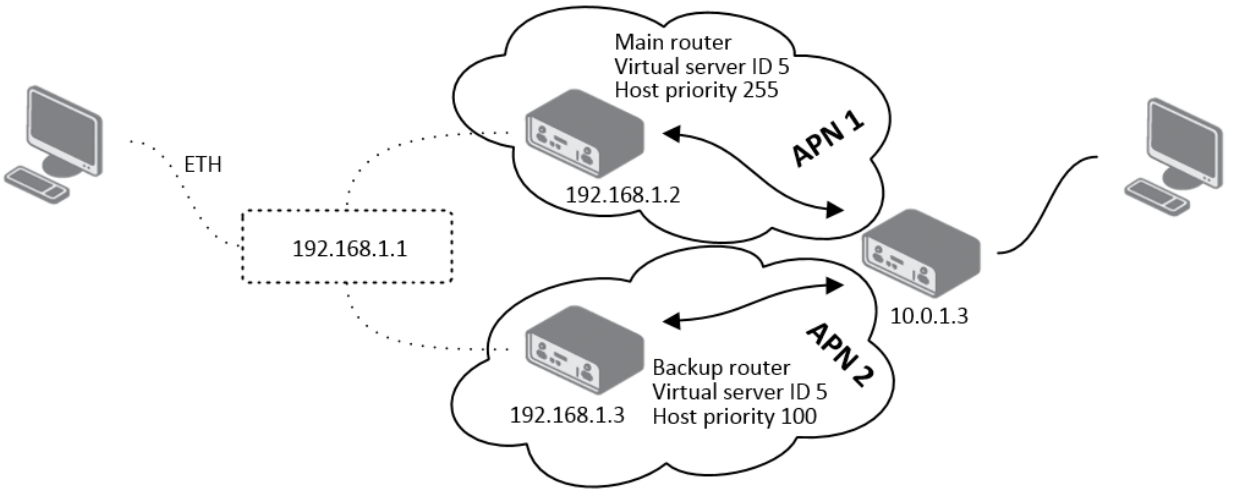


Figure 23: Topology of VRRP Configuration Example

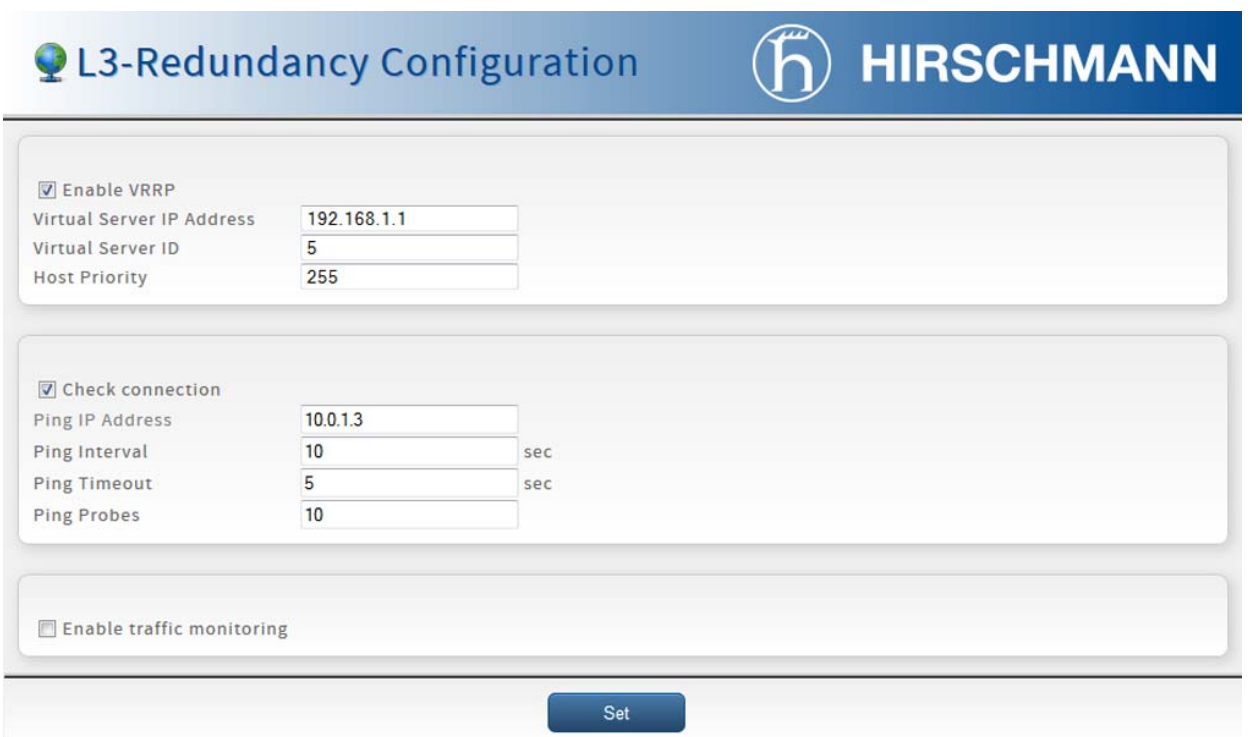


Figure 24: VRRP Configuration Example - Main Router

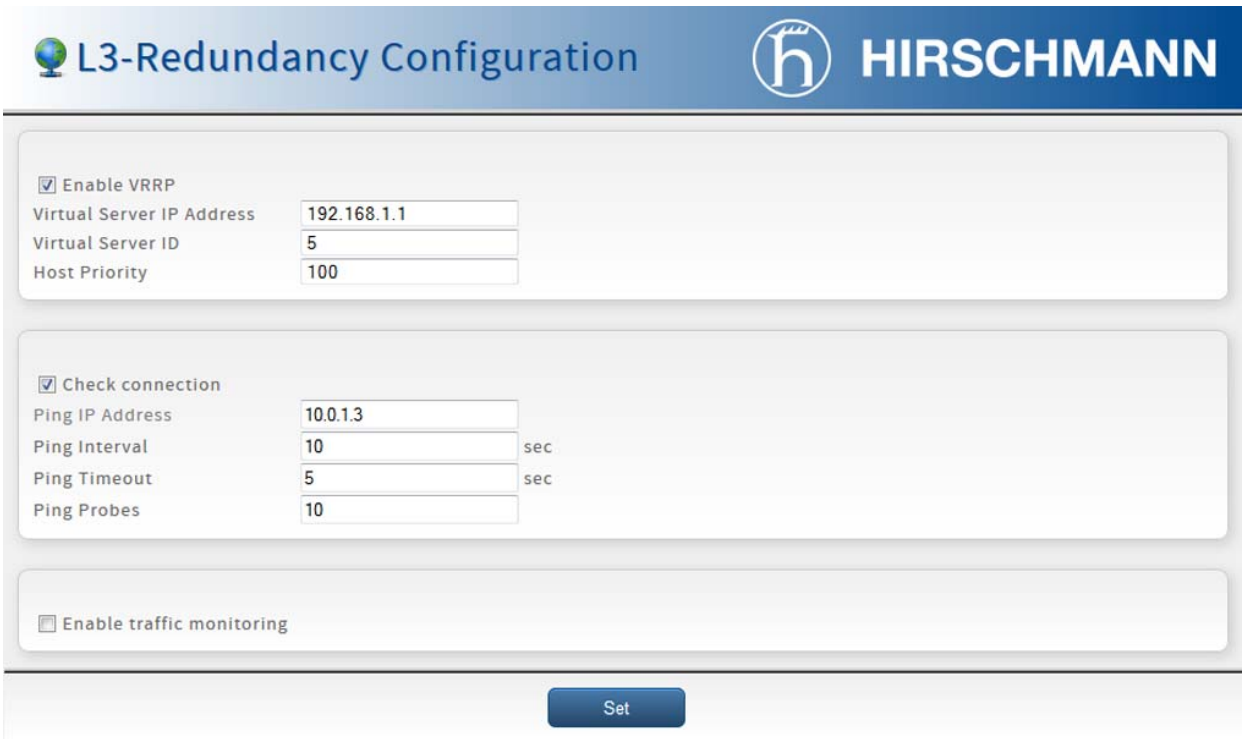


Figure 25: VRRP Configuration Example - Backup Router

DynDNS

With the DynDNS service you can 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.

Table 21:

Parameter	Description
Password	Specifies the password for logging into the DynDNS server.
Server	If you want to use a DynDNS service other than the `www.dyndns.org`, then 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 21:

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

Figure 26: 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 PPPoE client is used to connect devices supporting a PPPoE bridge or server this 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: ▶ PAP or CHAP - authentication method is chosen by the router ▶ PAP - is used PAP authentication method ▶ CHAP - it is used 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 22: PPPoE Configuration

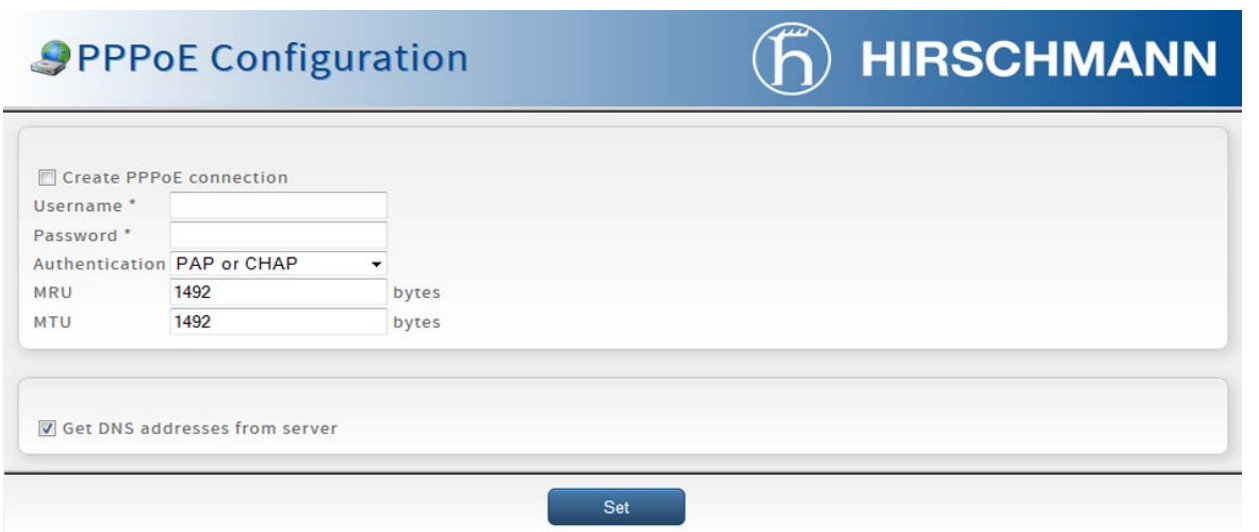


Figure 27: PPPoE Configuration

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 can be other connections to the Internet and/or mobile networks. You can 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 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, mark the "Check Connection" check box, and in the "Mobile WAN Configuration" dialog, select the `enable + bind` option, see “Mobile WAN” on page 43.

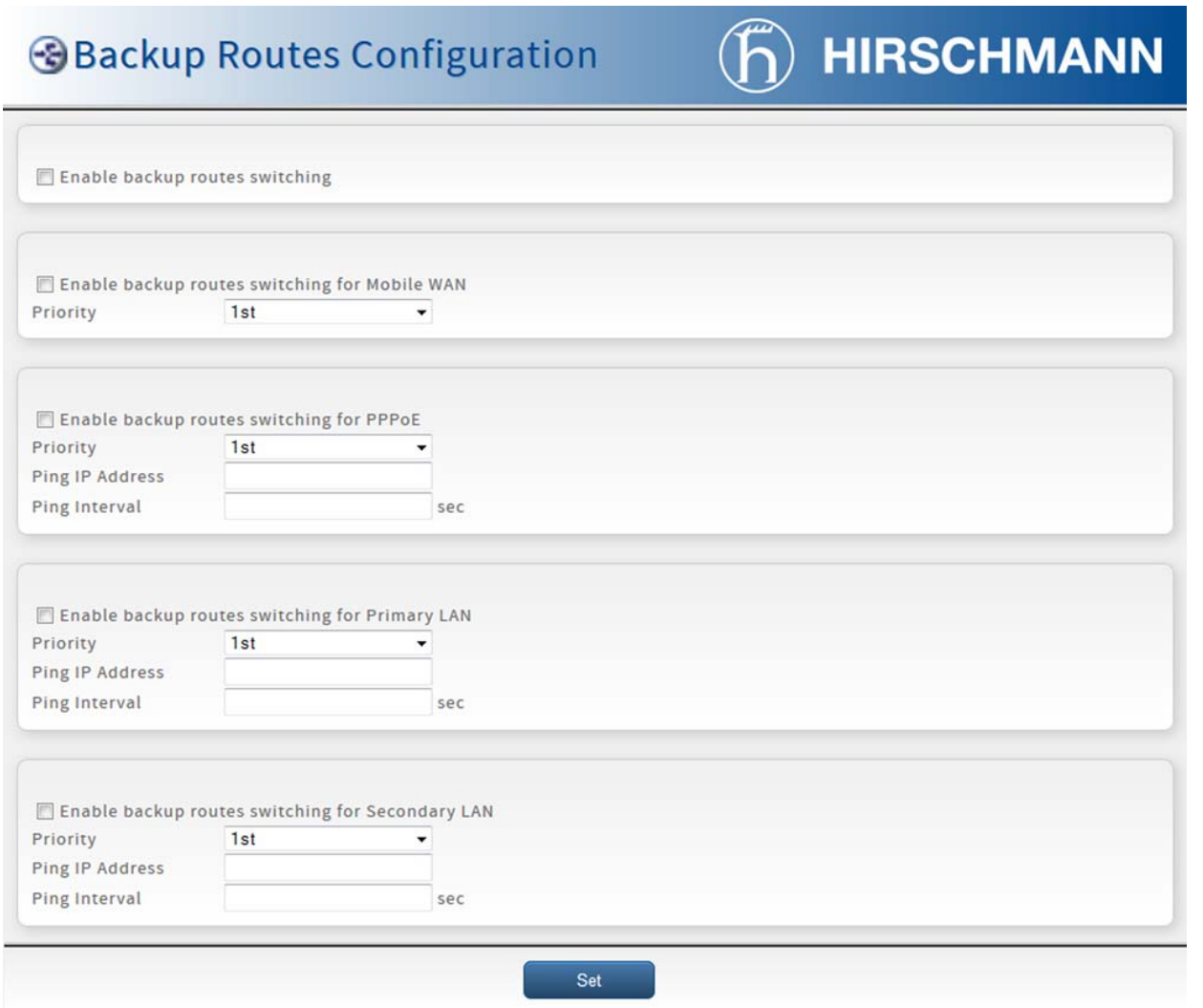


Figure 28: Backup Routes

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 (pppX)
- 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 23: 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 must 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: ▶ all - access is enabled for all protocols ▶ TCP - access is enabled for TCP protocol ▶ UDP - access is enabled for UDP protocol ▶ ICMP - access is enabled for ICMP protocol
Target Port	Specifies the port number on which access to the router is allowed.
Action	Specifies the type of action the router performs: ▶ allow - access is allowed ▶ deny - access is denied

Table 24: Filtering of Incoming Packets

The following 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.
Protocol	Specifies the protocol for remote access: ▶ all - access is enabled for every protocol ▶ TCP - access is enabled for TCP protocol ▶ UDP - access is enabled for UDP protocol ▶ ICMP - access is enabled for ICMP protocol
Target Port	Specifies the port number on which access to the router is allowed.
Action	Specifies the type of action the router performs: ▶ allow - access is allowed ▶ deny - access is denied

Table 25: Forwarding Filtering

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

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

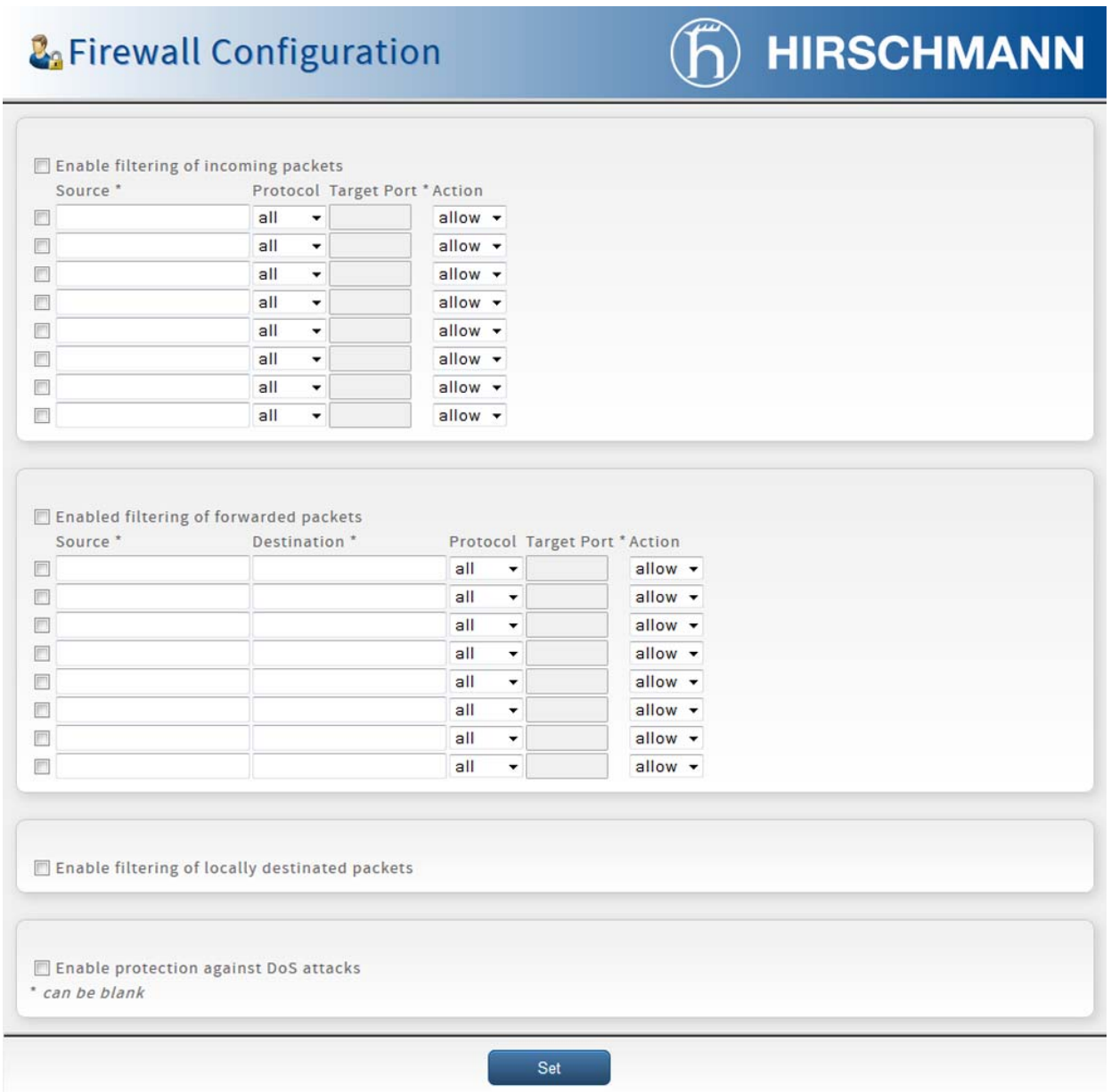


Figure 29: Firewall Configuration

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

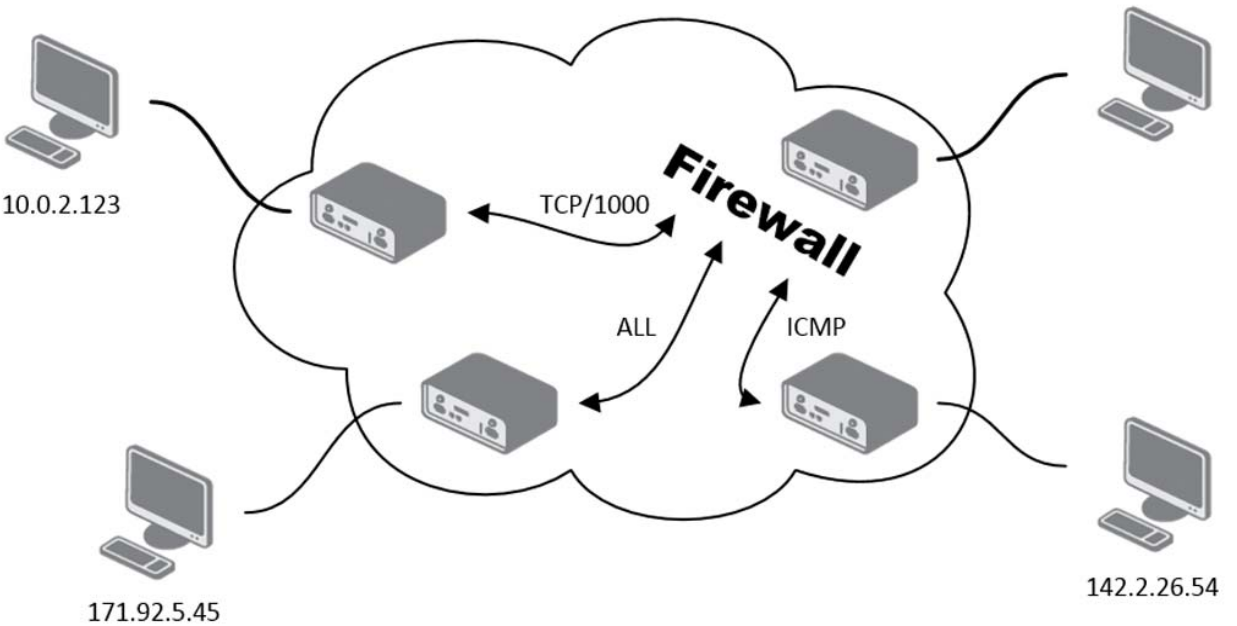


Figure 30: Topology for the Firewall Configuration Example

Figure 31: 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 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 26: NAT configuration

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

Parameter	Description
Send all remaining incoming packets to default server	Activating this function and specifying a "Default Server IP Address" can make the router forward incoming data from a GPRS to a computer with the assigned IP address.
Default Server IP Address	The router sends incoming packets to this IP address.

Table 27: 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. 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 address translation (PAT) function. Masquerade is a function used in the NAT protocol.

Table 28: Remote Access Configuration

Example of a configuration with 1 connection to the router:

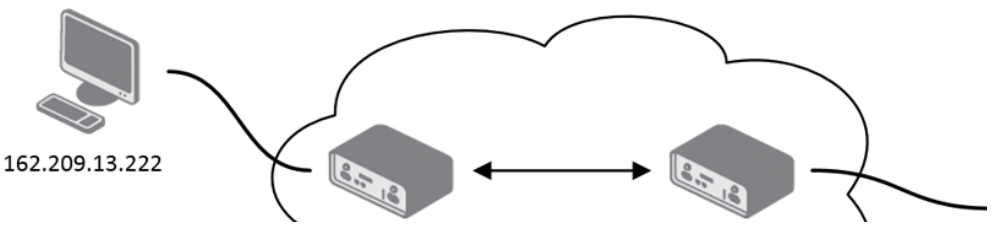


Figure 32: Topology of NAT configuration Example 1

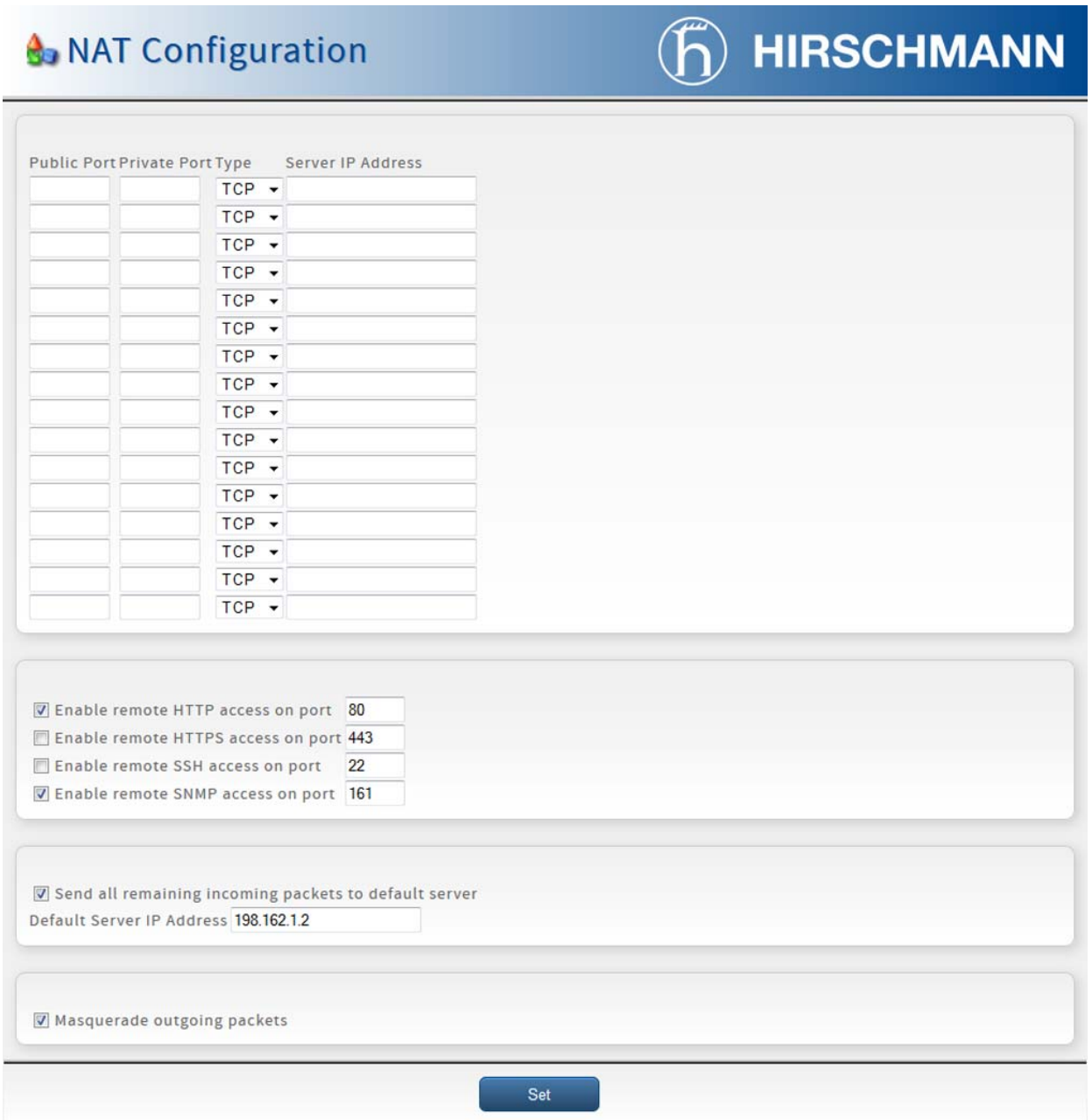


Figure 33: NAT Configuration Example 1

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.

Example of the configuration with more equipment connected:

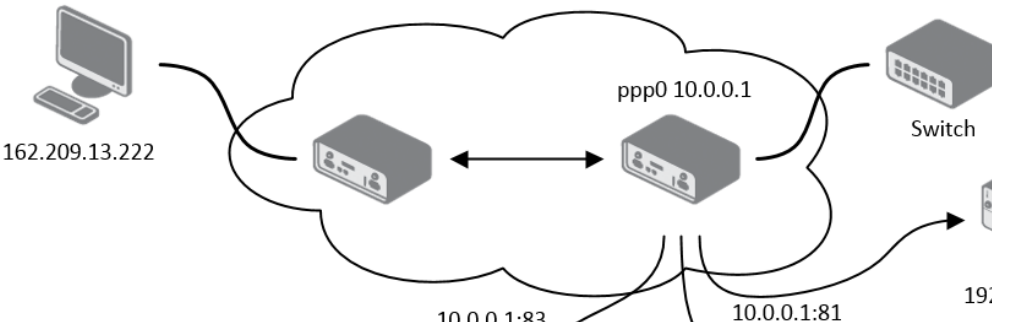


Figure 34: Topology of NAT Configuration Example 2

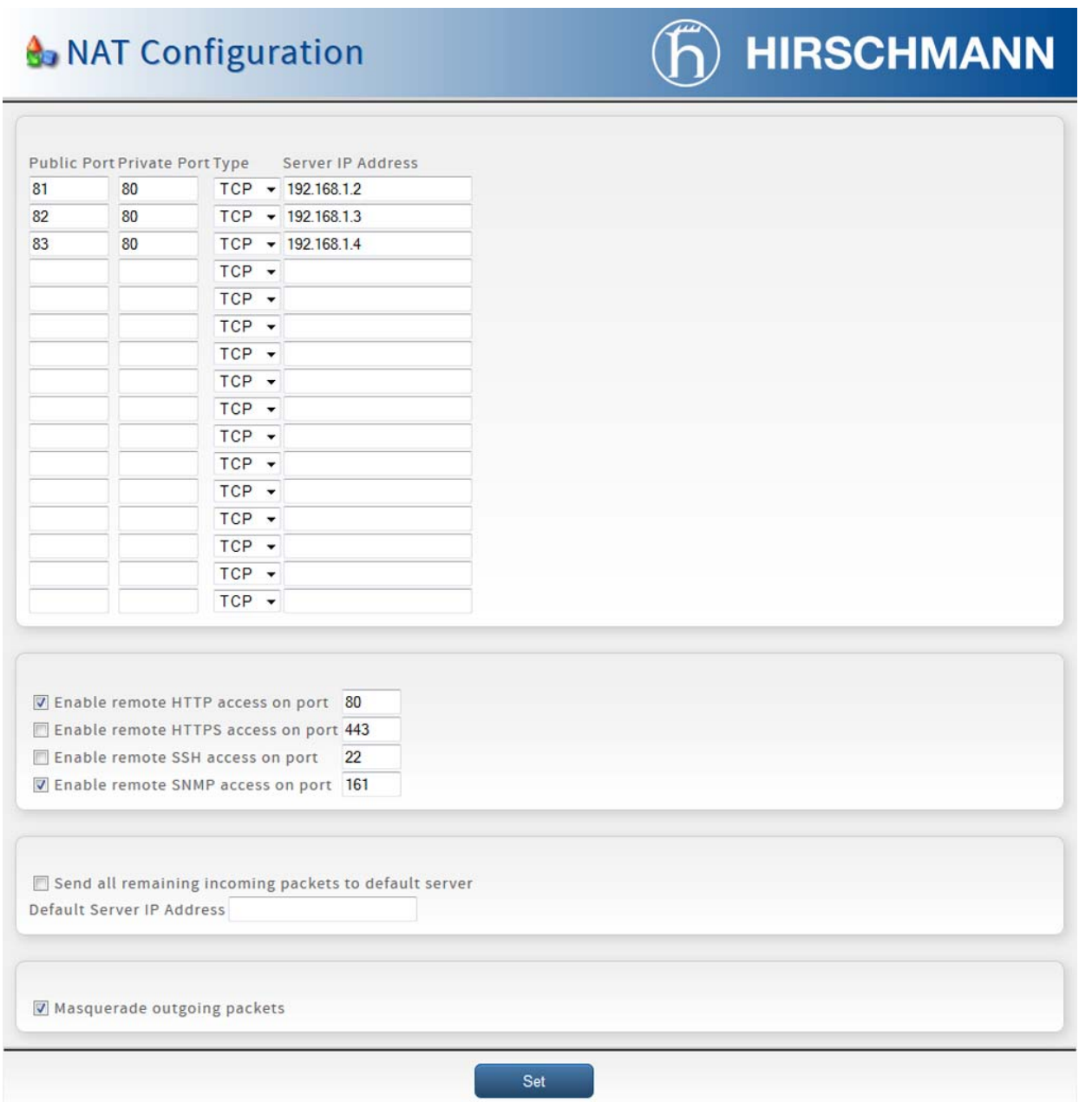


Figure 35: NAT Configuration Example 2

In this example, using ppp0 switch there is more equipment connected behind the router. Every device connected behind the router has its own IP address. This is the address entered in the "Server IP Address" field in the "NAT" dialog. These devices are communicating on the 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.

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 disabled. 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:

- 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.

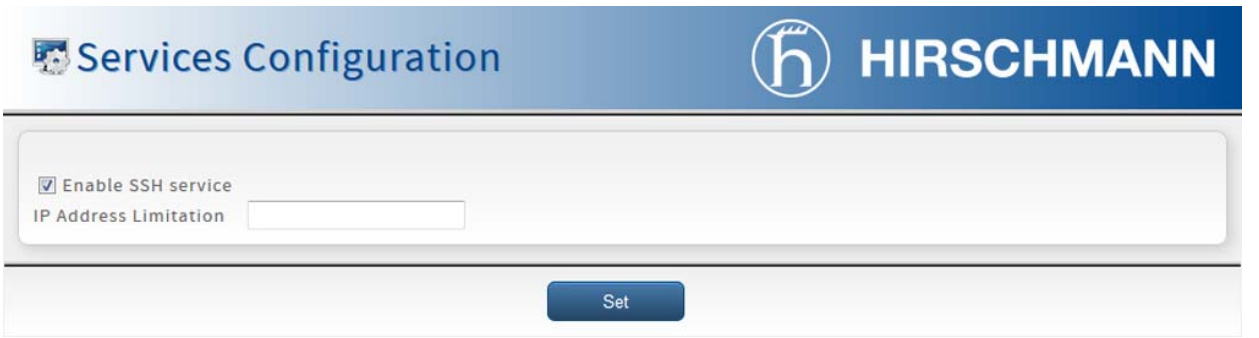


Figure 36: Services

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 protect the connection of 2 separate LAN networks, so that it looks like a single homogenous network. There are 2 rows in the OpenVPN dialog. Each row corresponds to a single OpenVPN tunnel configuration.

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 wizard

Table 29: OpenVPN Tunnels Overview

Figure 37: OpenVPN Tunnels List

Parameter	Description
Description	Specifies the description or name of tunnel
Protocol	Specifies the communication protocol: ▶ UDP - OpenVPN communicates using UDP ▶ TCP server - OpenVPN communicates using TCP in server mode ▶ TCP client - OpenVPN communicates using TCP in client mode
UDP/TCP port	Specifies the port of the relevant protocol (UDP or TCP)
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	Allows to redirect data on the Ethernet
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: ▶ `none` - no compression is used ▶ `LZO` - a lossless compression is used, use the same setting on both sides of the tunnel

Table 30: OpenVPN Tunnels Overview

Parameter	Description
NAT Rules	Activates/deactivates the NAT rules for the OpenVPN tunnel: ▶ `not applied` - NAT rules are not applied to the OpenVPN tunnel ▶ `applied` - NAT rules are applied to the OpenVPN tunnel
Authenticate Mode	Specifies the authentication mode: ▶ `none` - no authentication is set ▶ `pre-shared secret` - sets the shared key for both sides of the tunnel ▶ `username/password` - enables authentication using a CA Certificate, Username and Password ▶ `X.509 cert. (multiclient)` - enables X.509 authentication in multi-client mode ▶ `X.509 cert. (client)` - enables X.509 authentication in client mode ▶ `X.509 cert. (server)` - enables 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 30: OpenVPN Tunnels Overview

The changes in the settings take effect after clicking the "Set" button.

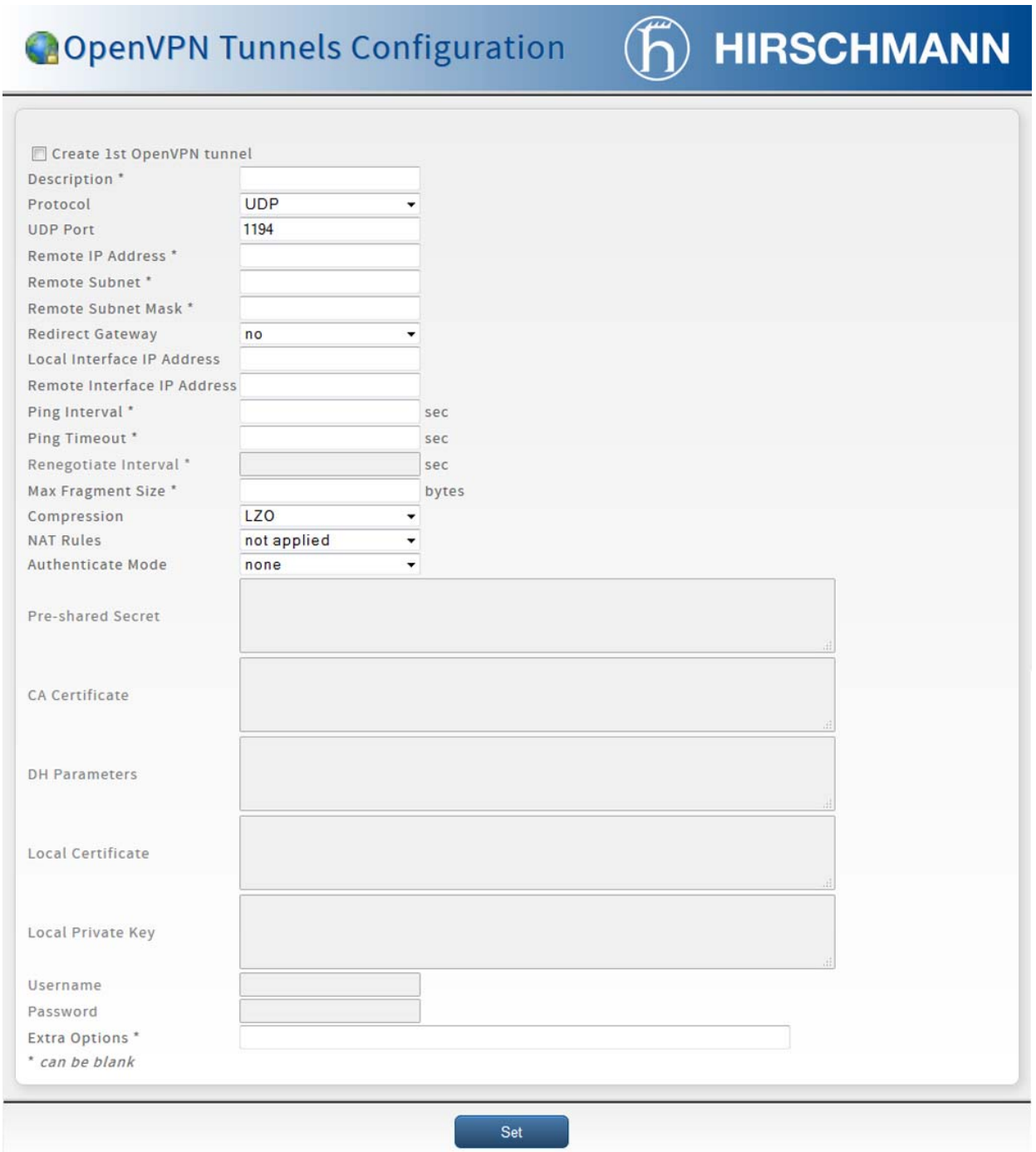


Figure 38: OpenVPN Tunnel Configuration

Example of the OpenVPN tunnel configuration:

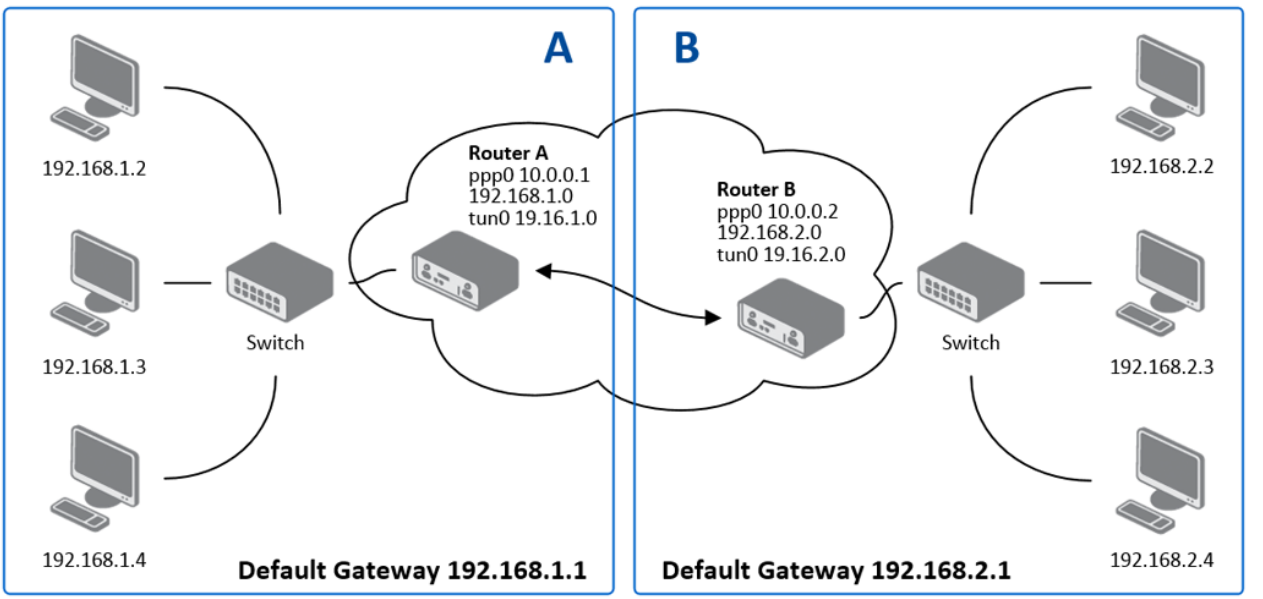


Figure 39: Topology of OpenVPN Configuration Example

OpenVPN tunnel configuration:

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

Table 31: OpenVPN Configuration Example

You can find examples of different OpenVPN tunnel configuration and authentication options in the OpenVPN appendix.

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 protect the connection of 2 separate LAN networks, so that it looks like a single homogenous network. There are 4 rows in the IPsec dialog. Each row corresponds to a single IPsec tunnel configuration.

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 wizard.

Table 32: IPsec Tunnels Overview

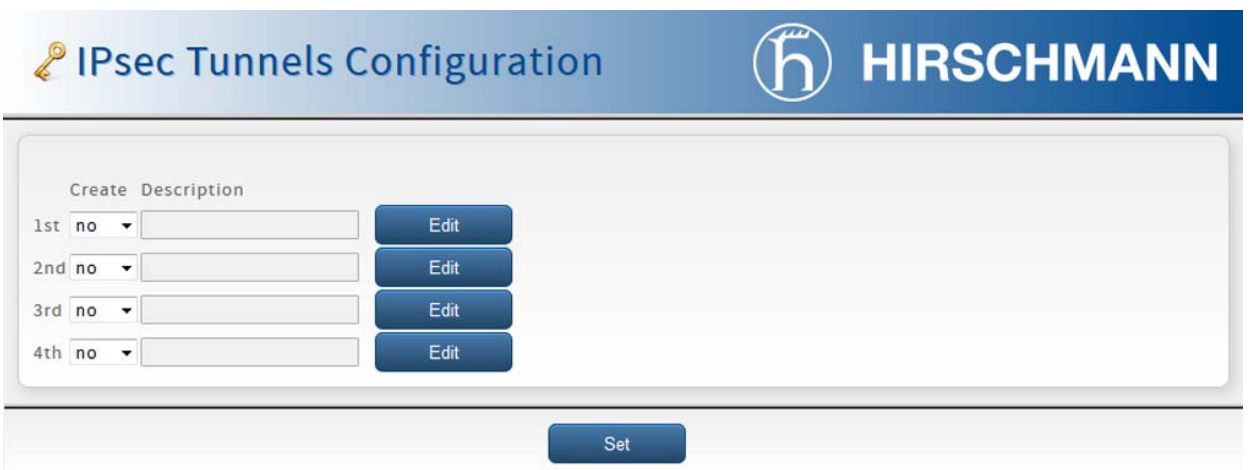


Figure 40: IPsec Tunnels List

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

Table 33: IPsec Tunnels Overview

Parameter	Description
Remote Protocol/Port	Specifies the Protocol/Port of remote side of the tunnel. The general form is protocol/port, for example 17/1701 for UDP (protocol 17) and port 1701. It is also possible to enter only the number of protocol, however, the above mentioned format is preferred
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/Port of a local network. The general form is protocol/port, for example 17/1701 for UDP (protocol 17) and port 1701. It is also possible to enter only the number of protocol, however, the above mentioned format is preferred.
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: ▶ `auto` - encryption and hash alg. are selected automatically ▶ `manual` - encryption and hash alg. are defined by the user
IKE Encryption	Specifies the encryption algorithm. Possible values are: `3DES`, `AES128`, `AES192`, `AES256`
IKE Hash	Specifies the hash algorithm. Possible values are: `MD5`, `SHA1`, `SHA256`, `SHA384` or `SHA512`
IKE DH Group	Specifies the Diffie-Hellman groups which determine the strength of the key used in the key exchange process. Higher group numbers are more secure, but require additional time to compute the key. A group with a higher number provides more security, but requires more processing time.
ESP Algorithm	Specifies the means by which the router selects the algorithm: ▶ `auto` - encryption and hash algorithm are selected automatically ▶ `manual` - encryption and hash algorithm are defined by the user
ESP Encryption	Specifies the encryption algorithm. Possible values are: `DES`, `3DES`, `AES128`, `AES192`, `AES256`
ESP Hash	Specifies the hash algorithm. Possible values are: `MD5`, `SHA1`, `SHA256`, `SHA384` or `SHA512`
PFS	Enables/disables the Perfect Forward Secrecy function. The function ensures that derived session keys are not compromised if one of the private keys is compromised in the future
PFS DH Group	Specifies the Diffie-Hellman group number (see IKE DH Group)

Table 33: IPsec Tunnels Overview

Parameter	Description
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
Authenticate Mode	Specifies the means by which the router authenticates: ▶ `pre-shared key` - sets the shared key for both sides of the tunnel ▶ `X.509 certificate`- allows X.509 authentication in multiclient mode
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 for X.509 authentication
Extra Options	Specifies the additional parameters of the IPsec tunnel for example, secure parameters.

Table 33: 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

When setting the key exchange times, we recommend that you maintain the default setting. 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 settings take effect after clicking the "Set" button.

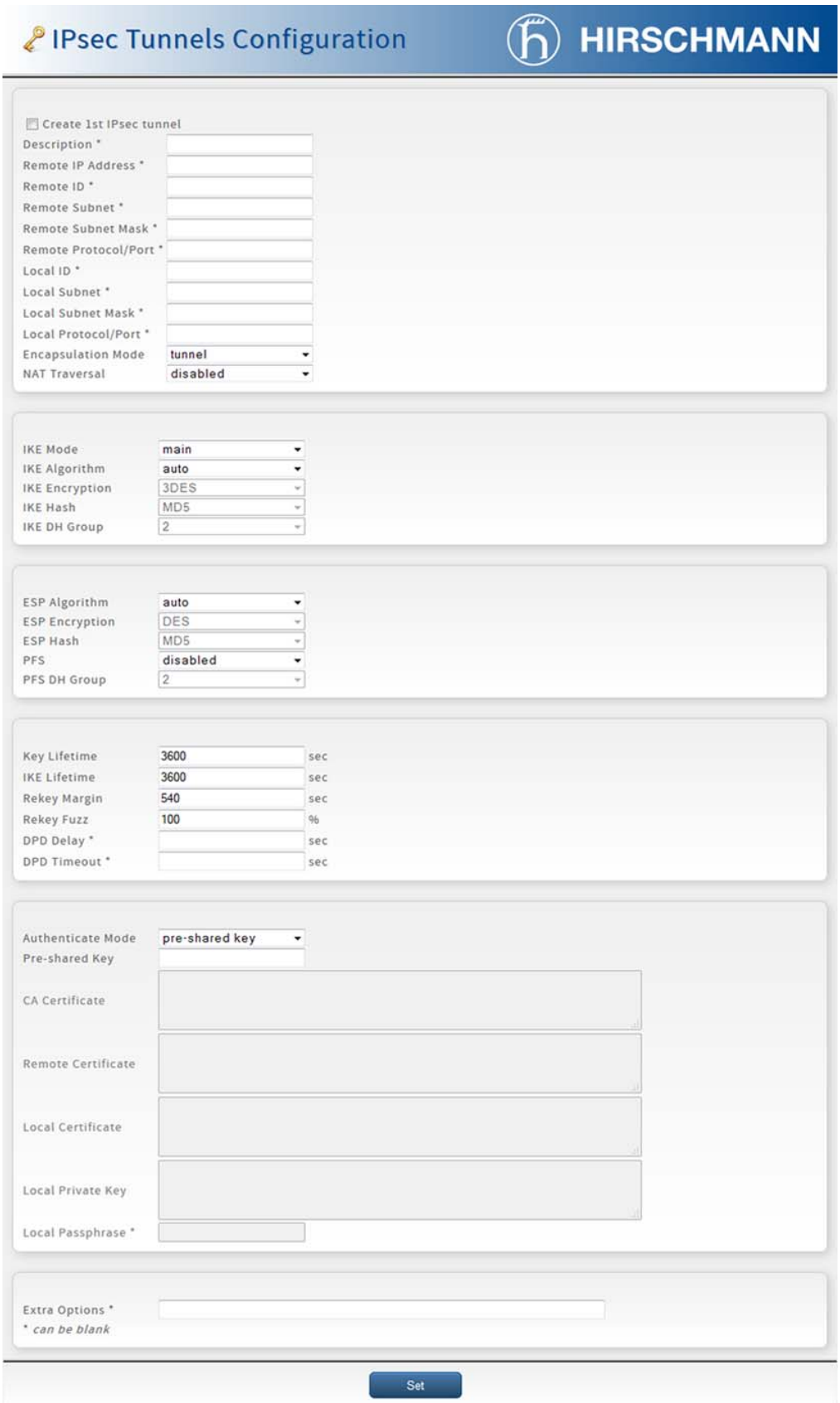


Figure 41: IPsec Tunnels Configuration

Example of the IPSec Tunnel configuration.

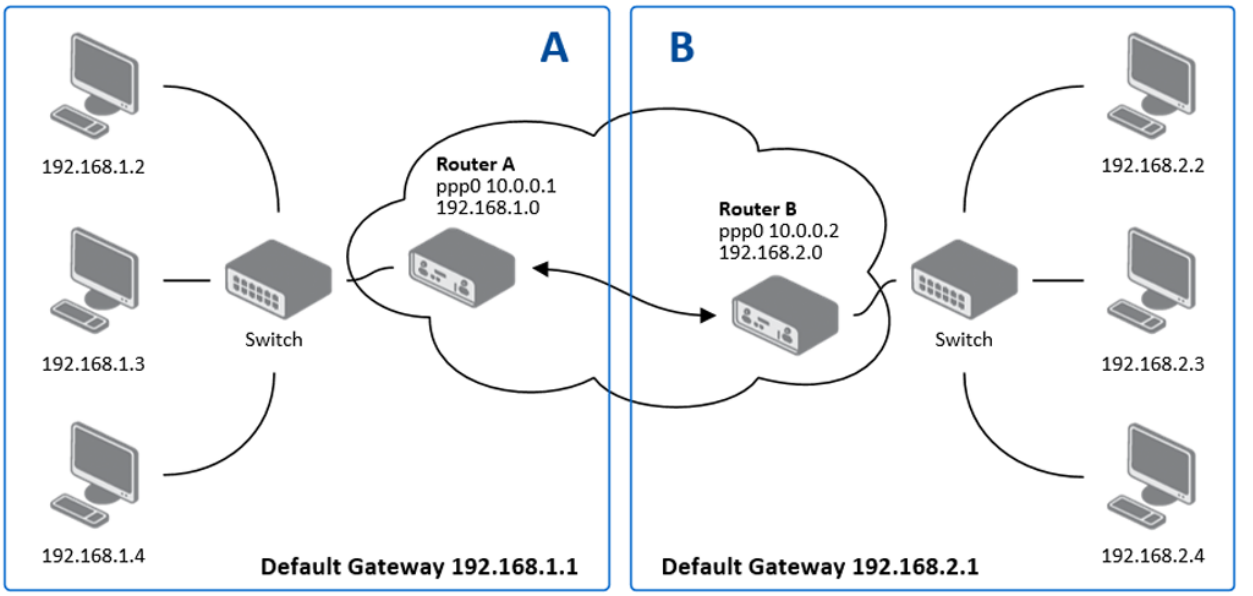


Figure 42: Topology of IPsec Configuration Example

IPsec tunnel configuration:

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

Table 34: IPsec Configuration Example

You can find examples of different IPsec tunnel configuration and authentication options in the IPsec appendix.

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 connect 2 separate LAN networks, so that it looks like a single homogenous network. There are 4 rows in the GRE dialog. Each row corresponds to a single GRE tunnel configuration.

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 wizard.

Table 35: GRE Tunnels Overview

Figure 43: GRE Tunnels List

Parameter	Description
Description	Description of GRE tunnel
Remote 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
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

Table 36: GRE Tunnel Configuration dialog

Parameter	Description
Multicasts	Enables/disables multicast: ▶ disabled - multicast disabled ▶ enabled - multicast enabled
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 36: GRE Tunnel Configuration dialog

Note: The GRE tunnel does not pass through NAT.

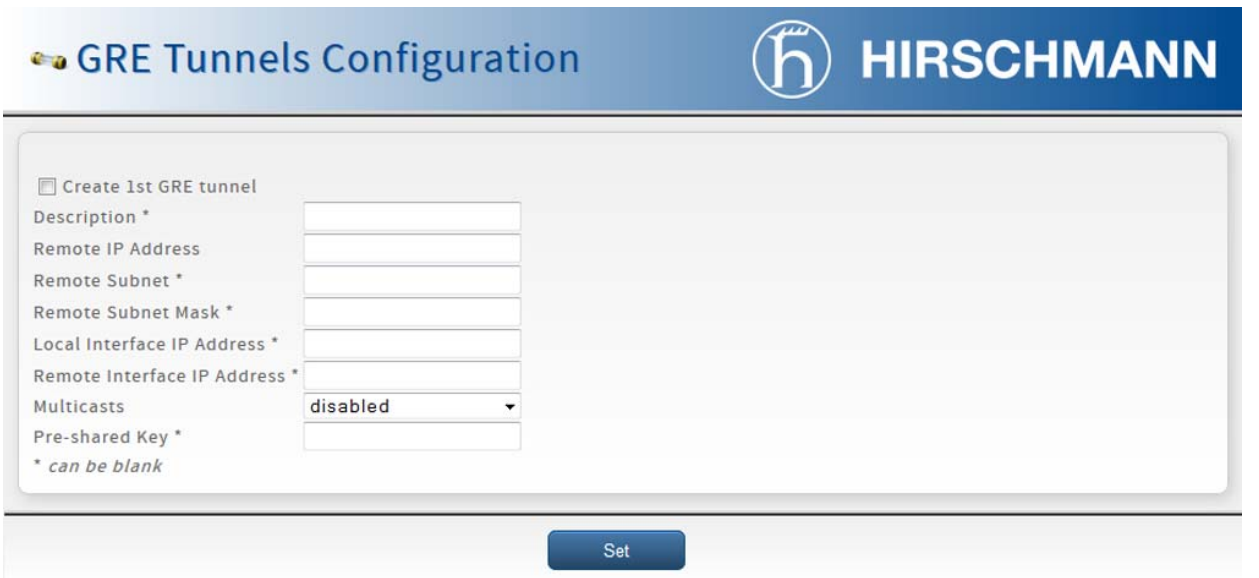


Figure 44: GRE Tunnel Configuration dialog

Example of the GRE Tunnel configuration:

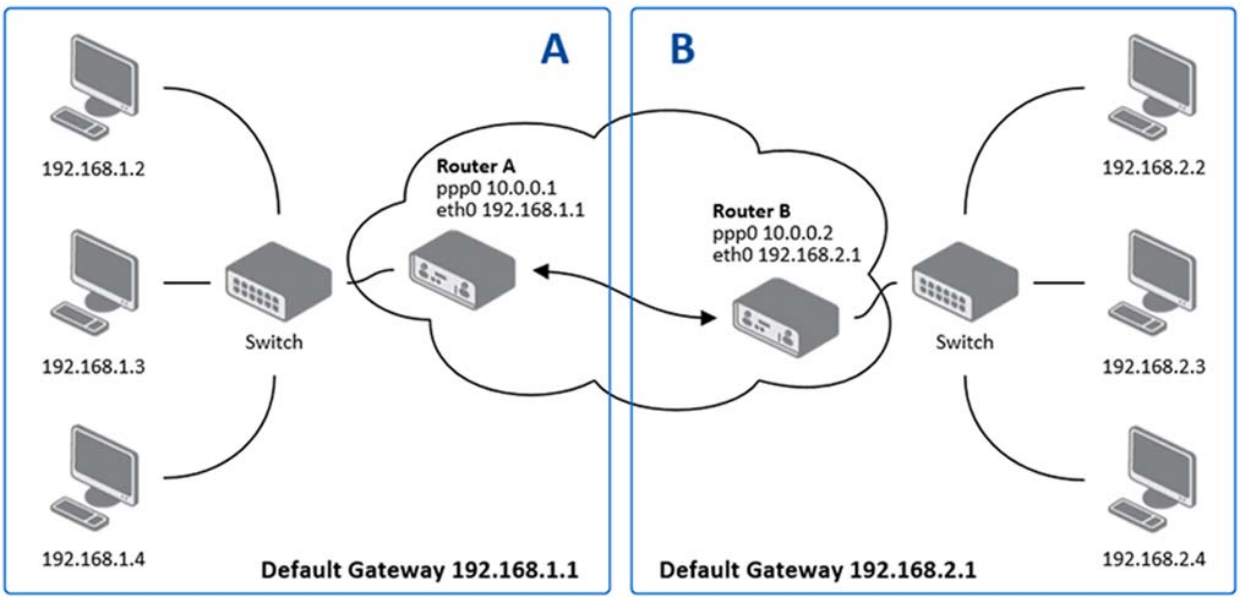


Figure 45: Topology of GRE Tunnel Configuration Example

GRE tunnel Configuration:

Configuration	A	B
Remote IP Address	10.0.0.2	10.0.0.1
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0

Table 37: GRE Tunnel Configuration Example

You can find examples of different GRE tunnel configuration and authentication options in the GRE Tunnel appendix.

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 connect 2 separate LAN networks, so that it looks like a single homogenous network. When you mark the "Create L2TP tunnel" check box, the router creates the tunnel as specified in the dialog.

Parameter	Description
Mode	Specifies the L2TP tunnel mode on the router side: ▶ `L2TP server` - specify an IP address range offered by the server ▶ `L2TP client` - specify the IP address of the server
Server IP Address	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 38: GRE Tunnel Configuration

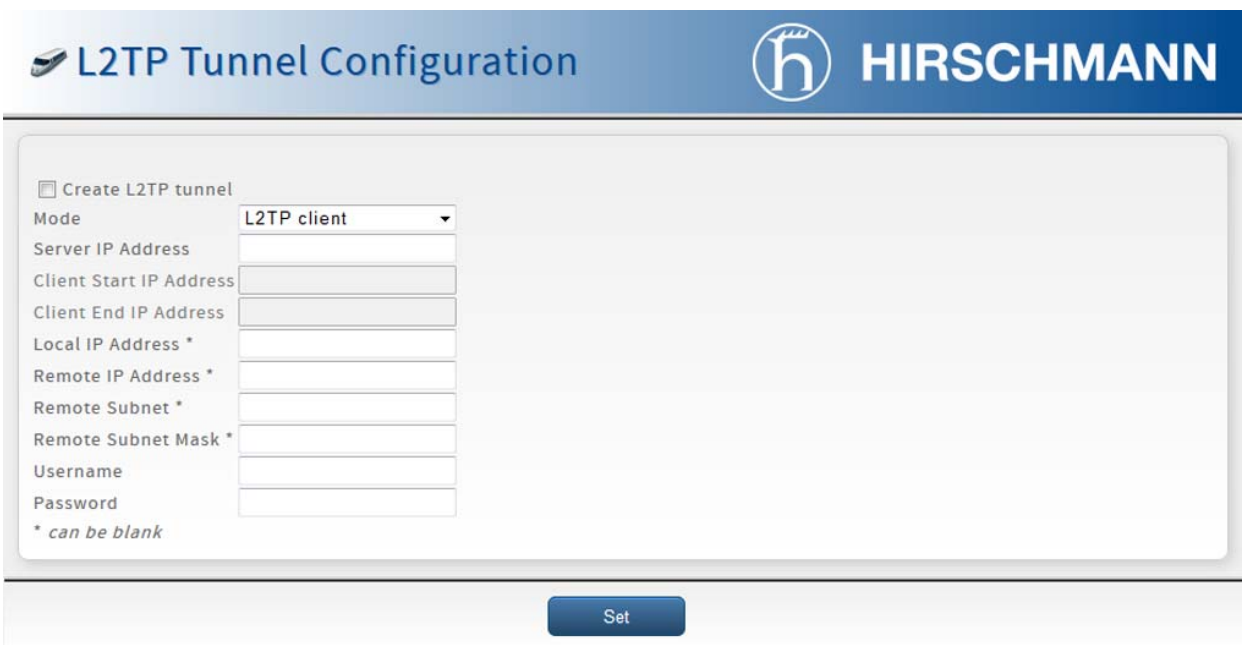


Figure 46: L2TP Tunnel Configuration

Example of the L2TP tunnel configuration:

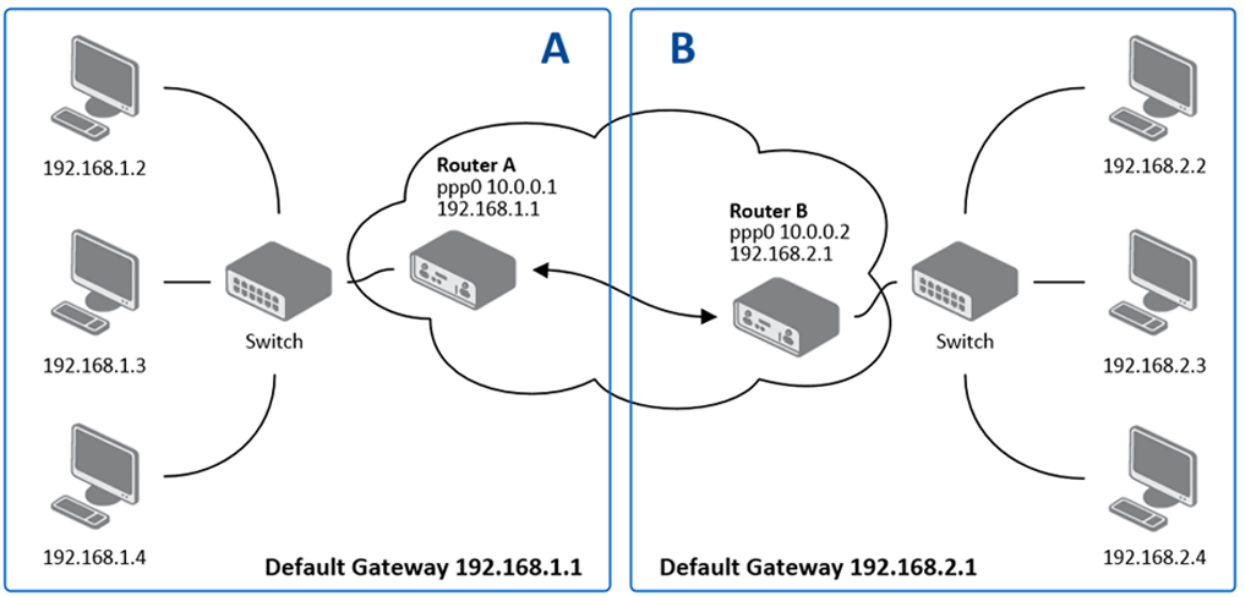


Figure 47: Topology of L2TP Tunnel Configuration Example

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 39: 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 exact time in 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) behind the router.
- 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: ▶ no - time shift is disabled ▶ yes - time shift is allowed

Table 40: 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.

Figure 48: 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 41: 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 "Read" default setting is `public` the "Write" password is `private`.

To enable SNMPv3, mark the "Enable SNMPv3 access" checkbox. Then you 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 42: SNMPv3 Configuration

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.

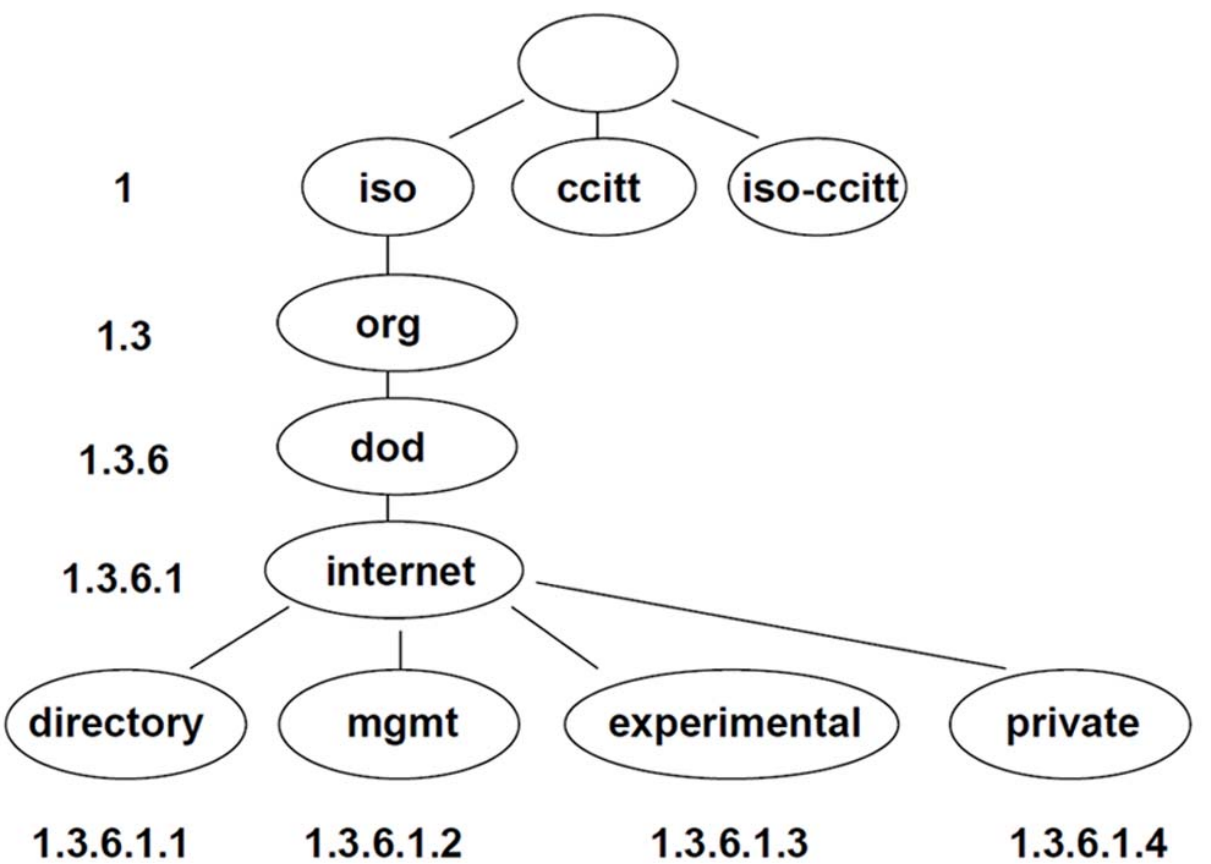


Figure 49: OID Basic Structure

SNMP values that are specific for Hirschmann routers create the tree starting at OID = 1.3.6.1.4.1.248.40.1. It can be interpreted as

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

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

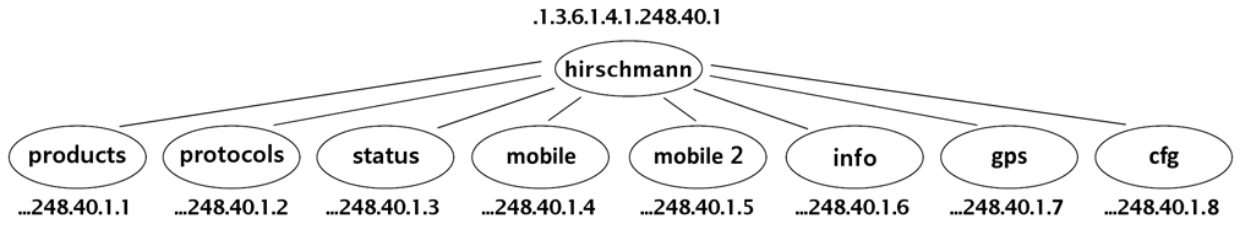


Figure 50: Hirschmann OID Tree

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). You can find a description of the OID values in SNMP OID appendix.

Example of SNMP settings:

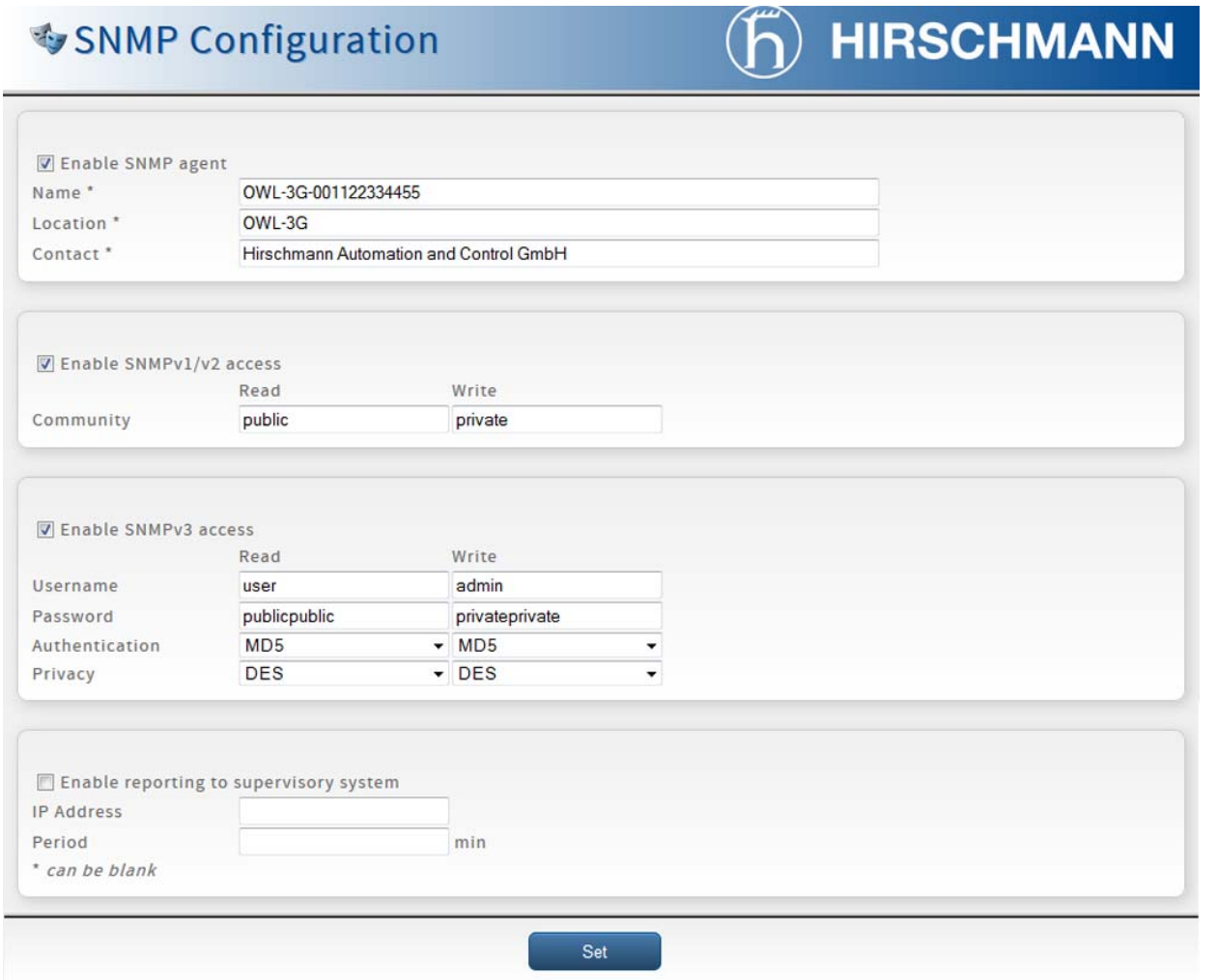


Figure 51: SNMP Configuration Example

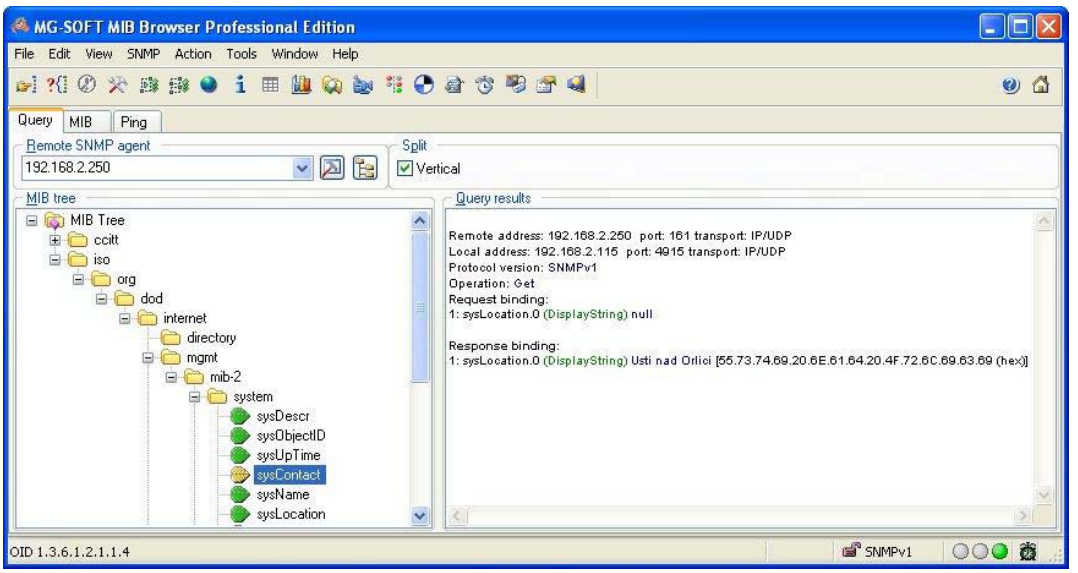


Figure 52: MIB Browser Example

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

The item SMTP is used for configuring SMTP (Simple Mail Transfer Protocol) client 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

Table 43: SNMPv3 Configuration

Parameter	Description
Secure Method	none, SSL/TLS, or STARTTLS. Secure method has to be supported by the SMTP server.
Username	E-mail account.
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 43: SNMPv3 Configuration

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

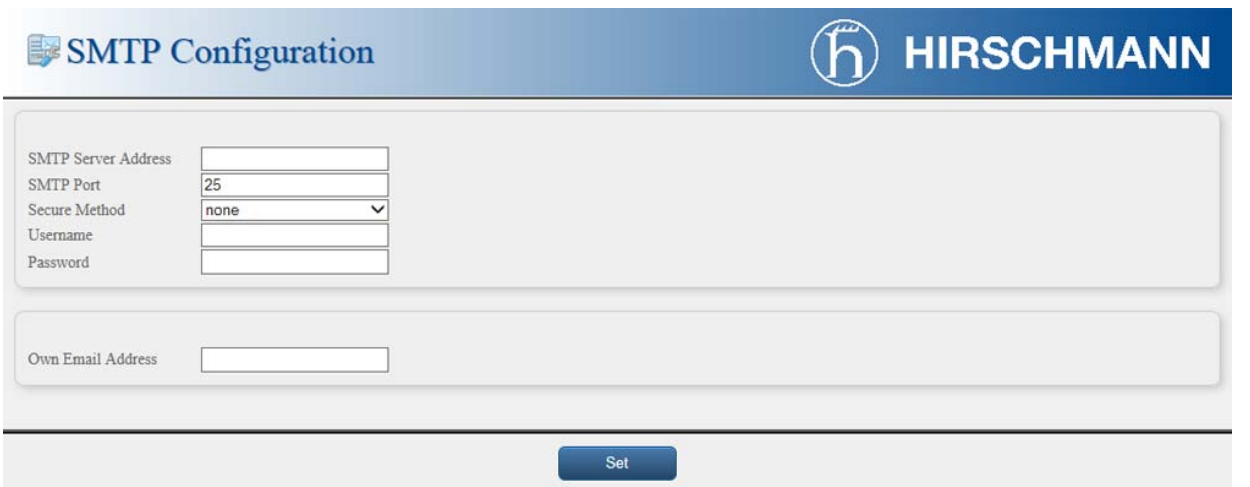


Figure 53: Example of the SMTP client configuration

E-mail can be sent from the Startup script (Startup Script item in the Configuration section) or via SSH connection. The command email is can be used with the following parameters:

- -t receiver’s E-mail address
- -s subject (has to be in quotation marks)
- -m message (has to be in quotation marks)
- -a attachment file
- -r number of attempts to send email (default 2 attempts set)

You can enter commands and parameters only in lowercase. Example of sending an e-mail:email –t name@domain.com –s "subject" –m "message" –a c:\directory\abc.doc –r 5

This command sends an e-mail address name@domain.com with the subject "subject", body message "message" and attachment "abc.doc" right from the directory c:\directory\. 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 device allows you to send SMS messages for various events and states of the router. You can configure which SMS messages the router sends in the top frame of the dialog.

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.
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.

Table 44: SMS Configuration

Then it is possible to configure control of the router via SMS. You can enable this function using the Enable remote control via SMS box. It is enabled by default.

Parameter	Description
Phone Number 1	This control can be configured for up to three numbers. If Enable remote control via SMS is enabled (this box is ticked), all incoming SMS are processed and deleted.
Phone Number 2	This control can be configured for up to three numbers. If Enable remote control via SMS is enabled (this box is ticked), all incoming SMS are processed and deleted.
Phone Number 3	This control can be configured for up to three numbers. If Enable remote control via SMS is enabled (this box is ticked), all incoming SMS are processed and deleted.

Table 45: 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 these phone numbers.
- If you enter characters, 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 until reboot. The behavior is the same for every SMS control message.

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 46: 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 47: 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.

You can find a detailed description and examples of these AT commands in the AT commands appendix.

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 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 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 48: 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 48: List of AT Commands

Example 1:

Sending a configuration using an SMS.

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

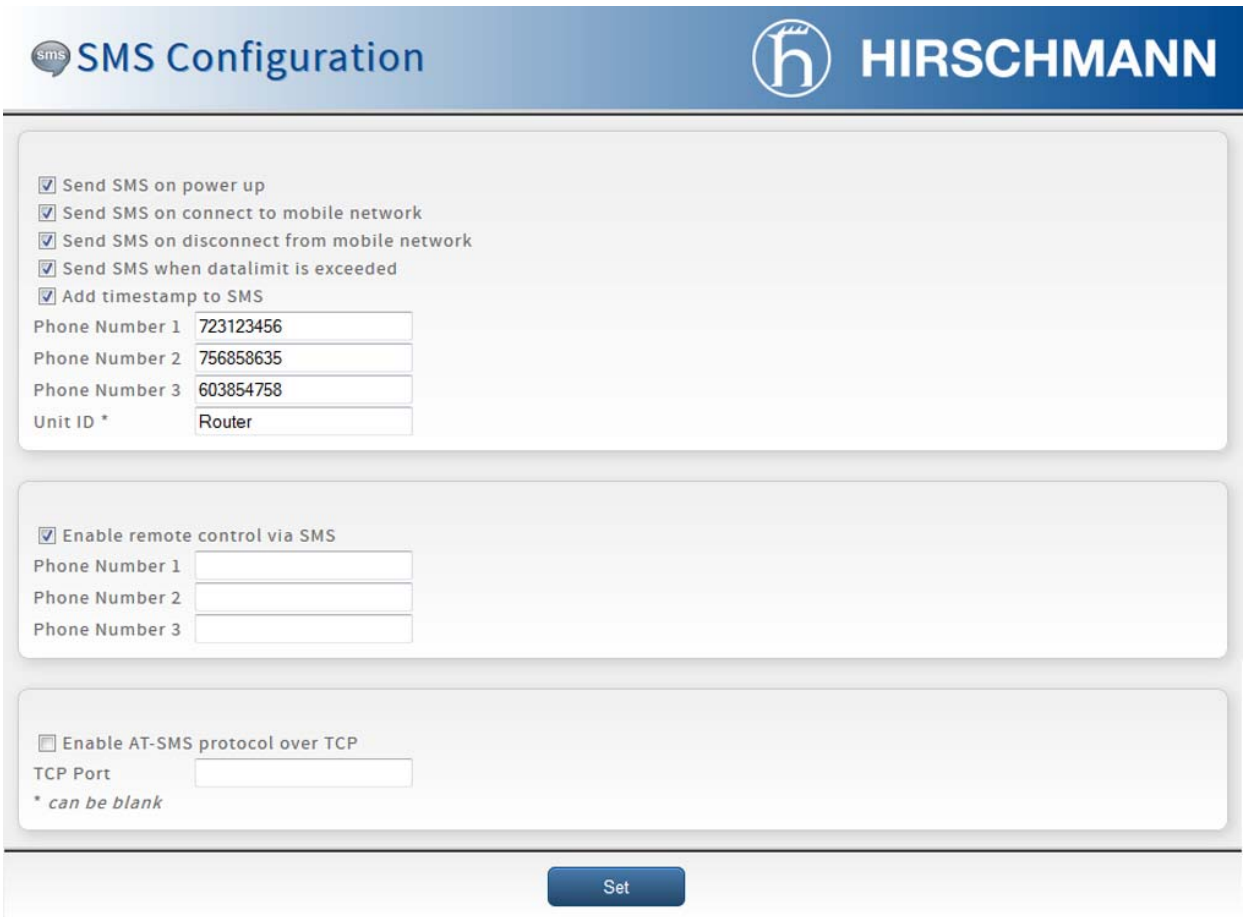


Figure 54: Example 1 – SMS configuration

- Example 2:
  Configuration to control the router using an SMS from any phone number.

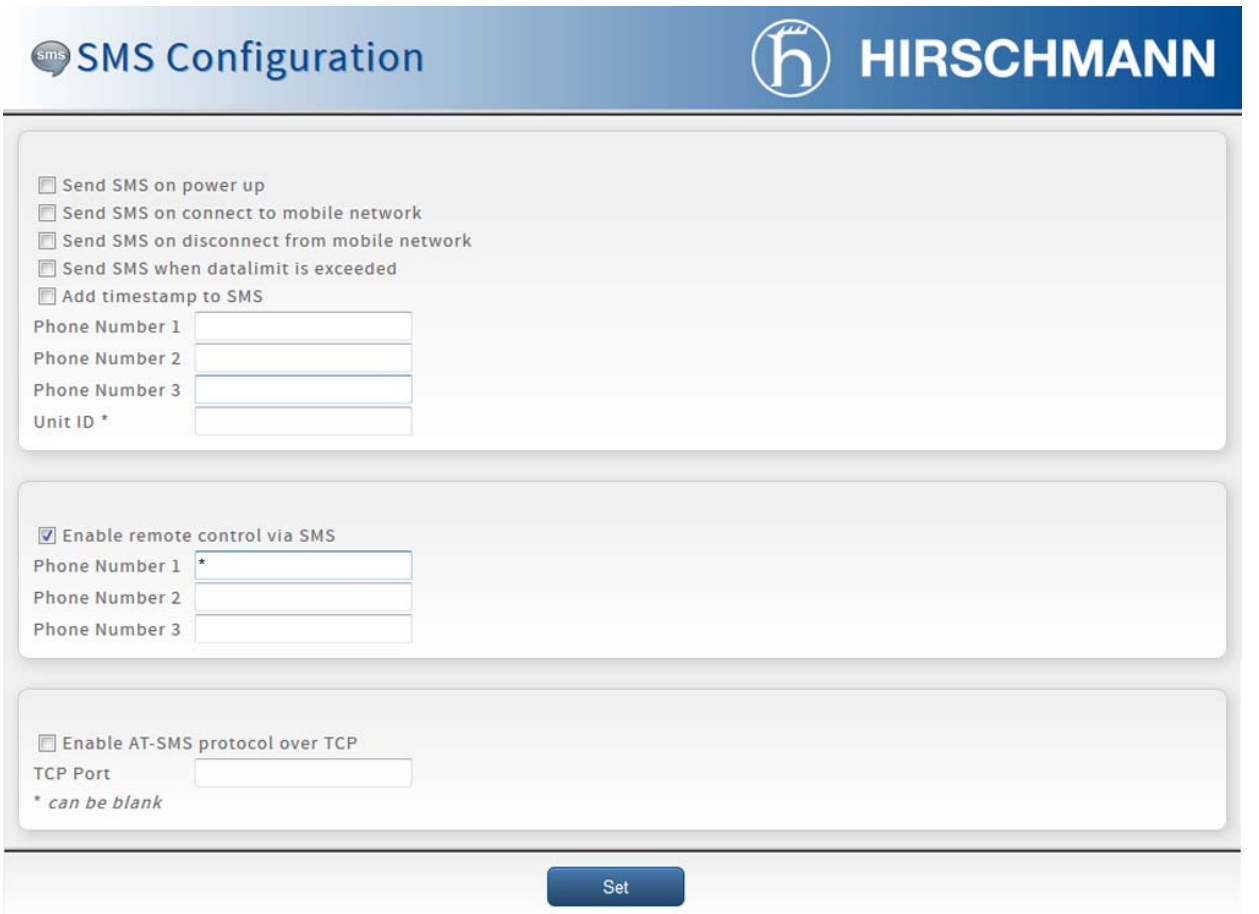


Figure 55: Example 2 – SMS configuration

Example 3:

Configuration to control the router using an SMS from 2 phone numbers.

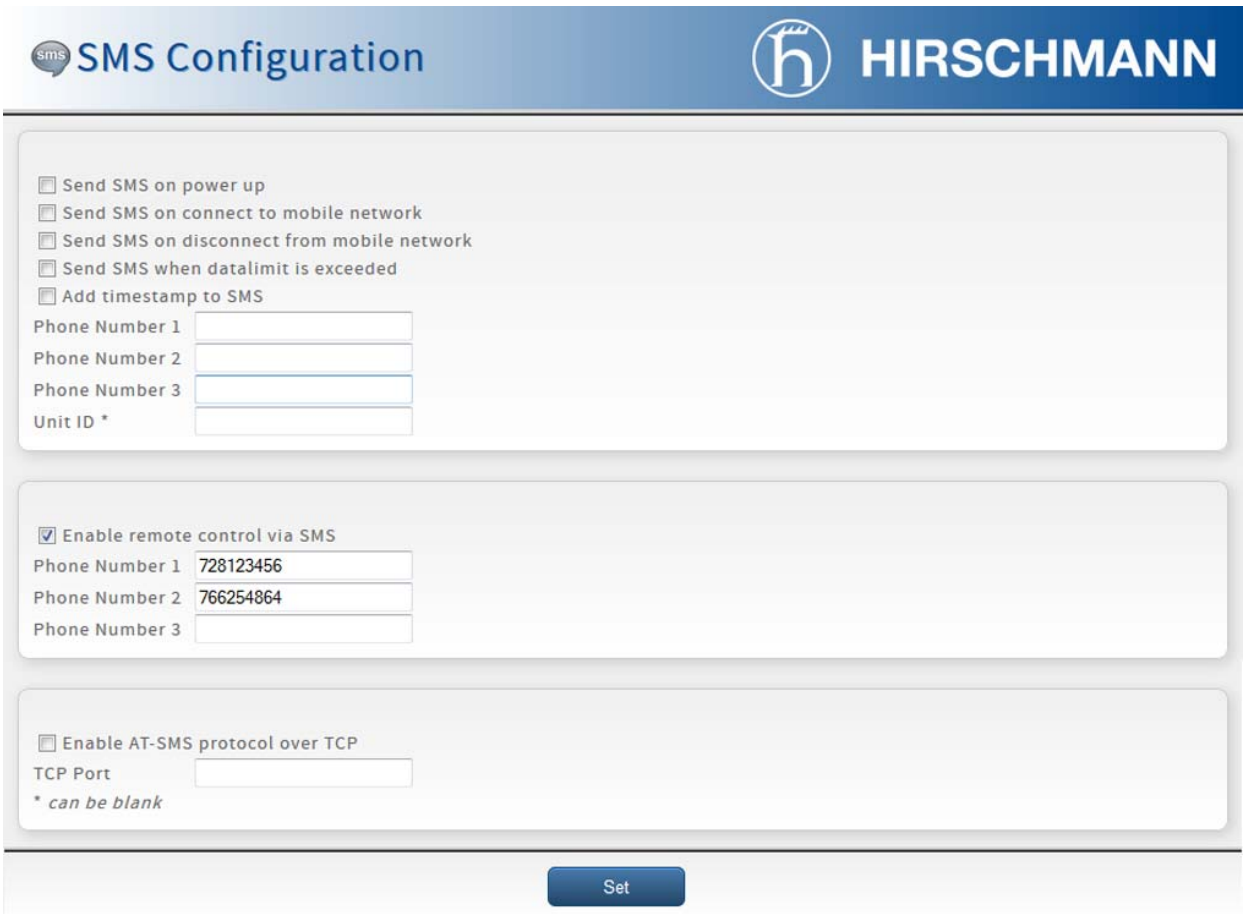


Figure 56: Example 3 – SMS configuration

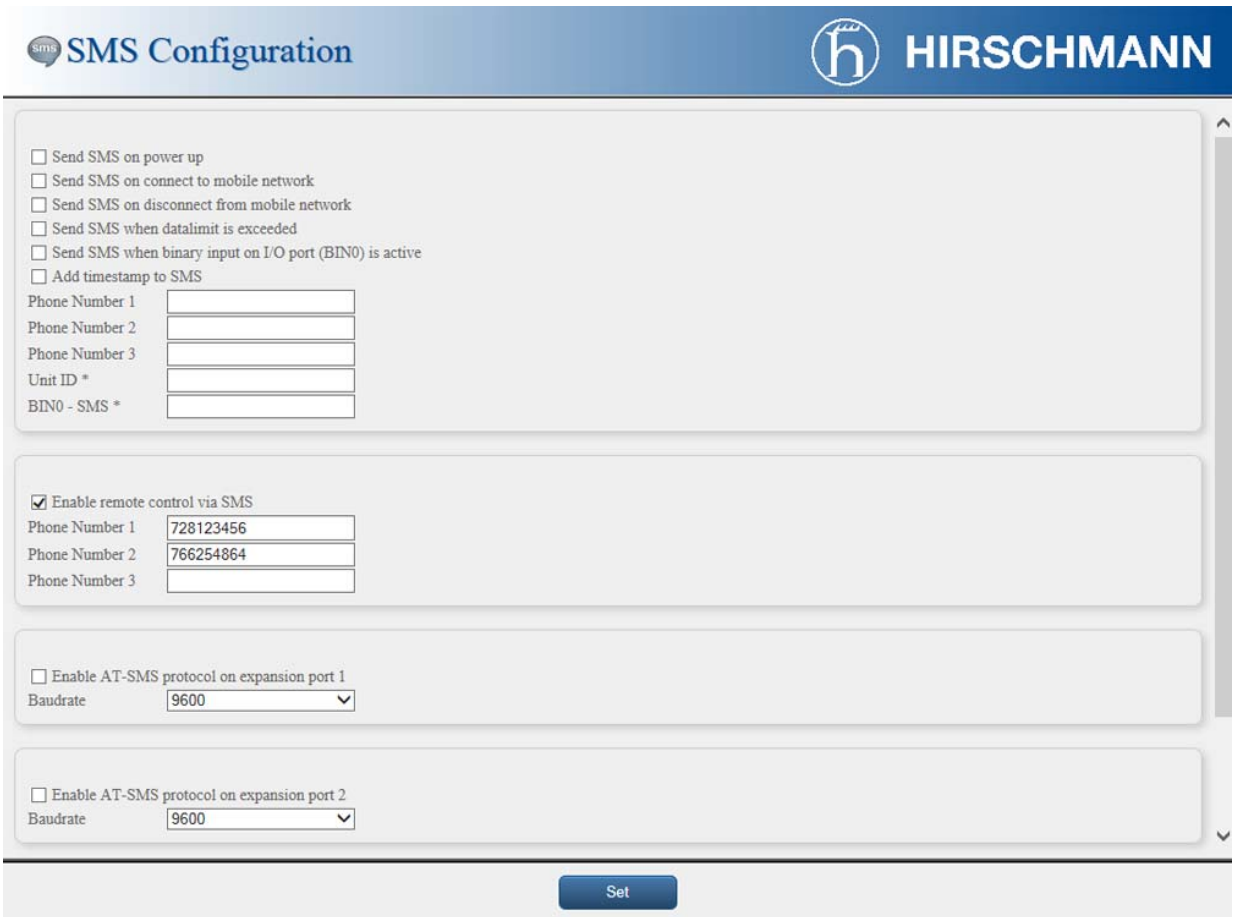


Figure 57: Example 3 – SMS configuration

Startup Script

The "Startup Script" dialog allows you to create your own scripts which the router executes after running the initial scripts.

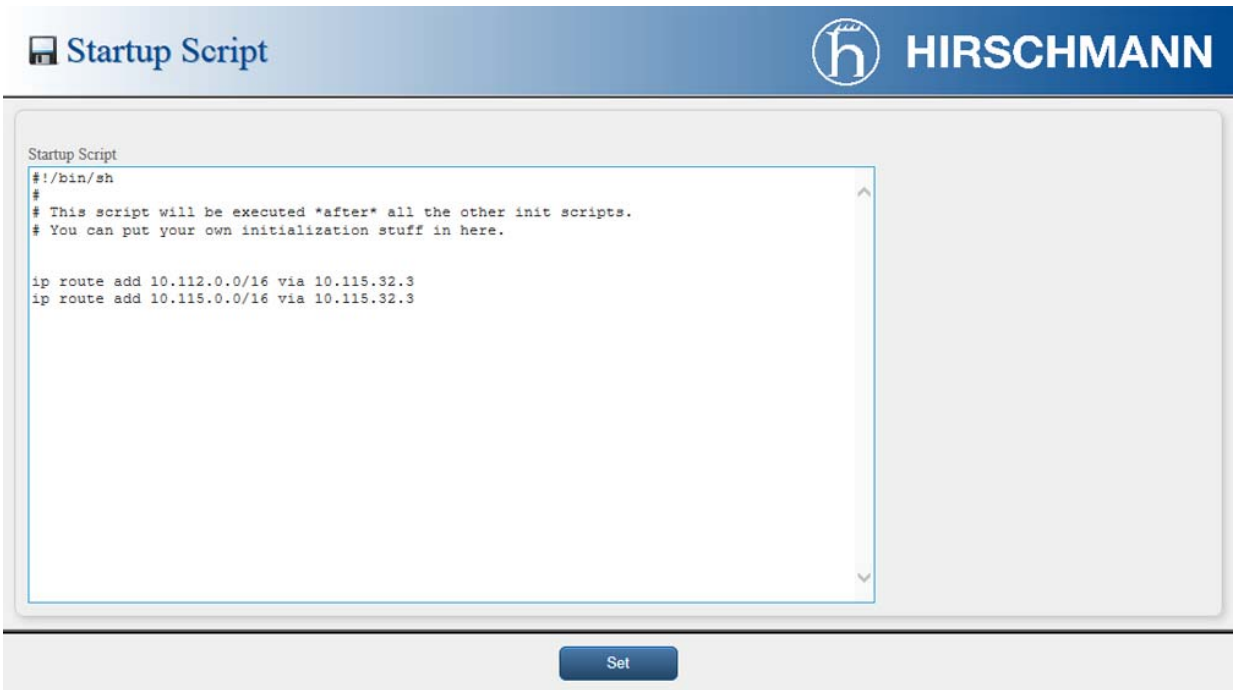


Figure 58: Startup script

The changes in the dialog take effect after you remove the power from the router, then connect the power again. To power cycling the router click the "Reboot" icon on the tool bar, or use an SMS message See “SMS” on page 91.

The following figure displays an example of a Startup script. After a reboot the router, it stops the syslogd program, and then restarts the syslogd program with remote logging on a device assigned the IP address 192.168.2.115. The script also limits the maximum number of entries to 100.

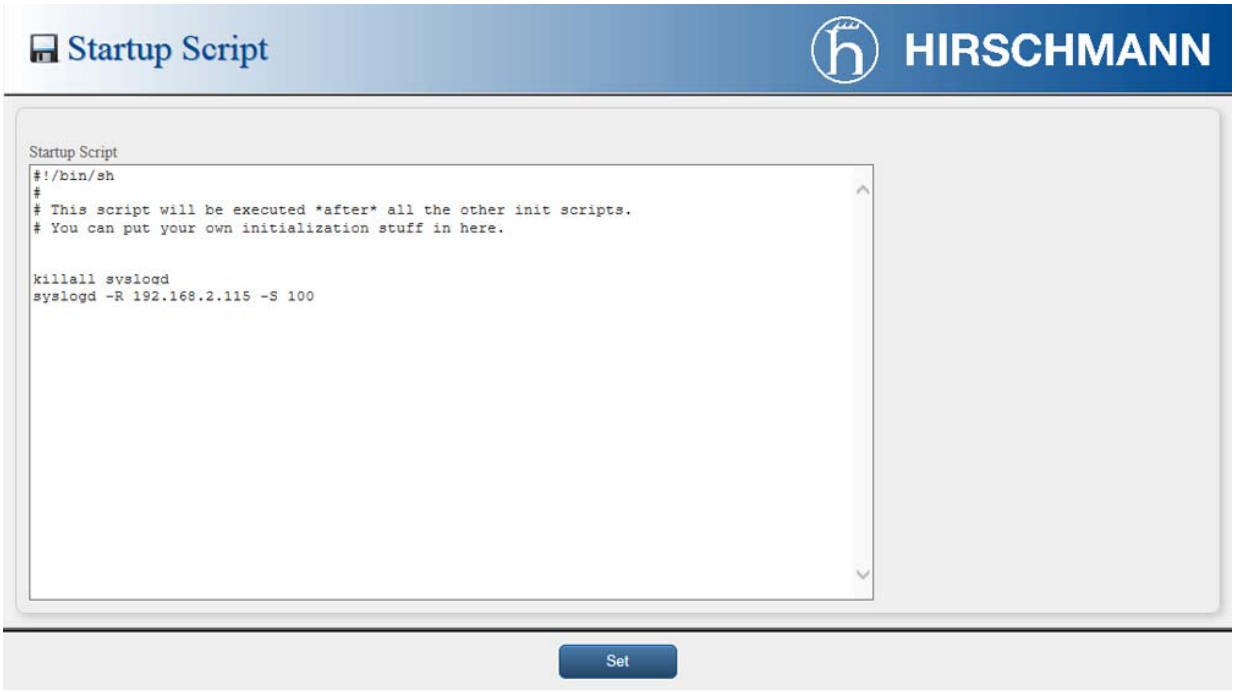


Figure 59: Example of Startup script

Up/Down Script

In the window Up/Down Script it is possible to create own scripts. In the item Up script is defined a script, which begins after establishing a PPP/WAN connection. In the item Down Script is defined script, which begins after lost a PPP/WAN connection.

The changes in the settings take effect after clicking the "Set" button. The router also requires a reboot.

Figure 60: Up/Down script

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

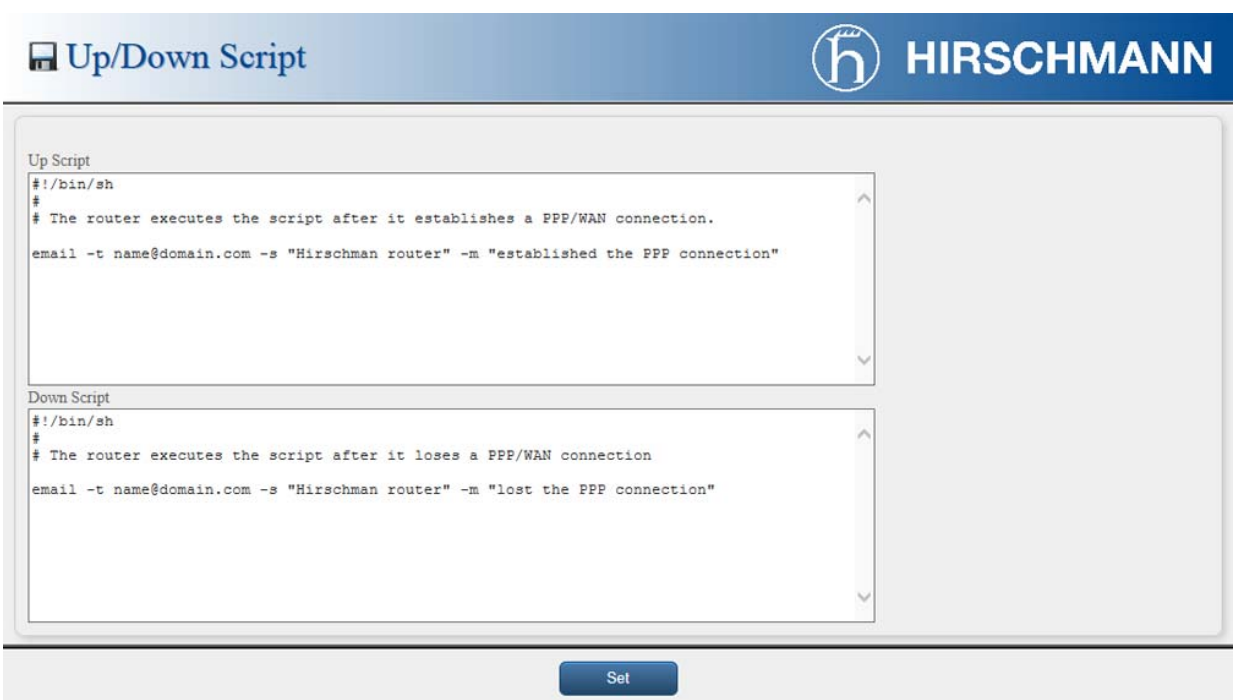


Figure 61: Example of Up/Down script

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.

Parameter	Description
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.
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 49: 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, so it is not necessary to enter it in the field. The Unit ID parameter allows the user to specify the name of the downloaded file. This means that if the parameter is filled in, 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://router/OWL-3G.bin
  - Configuration file: http://router/00.11.22.33.44.55.cfg

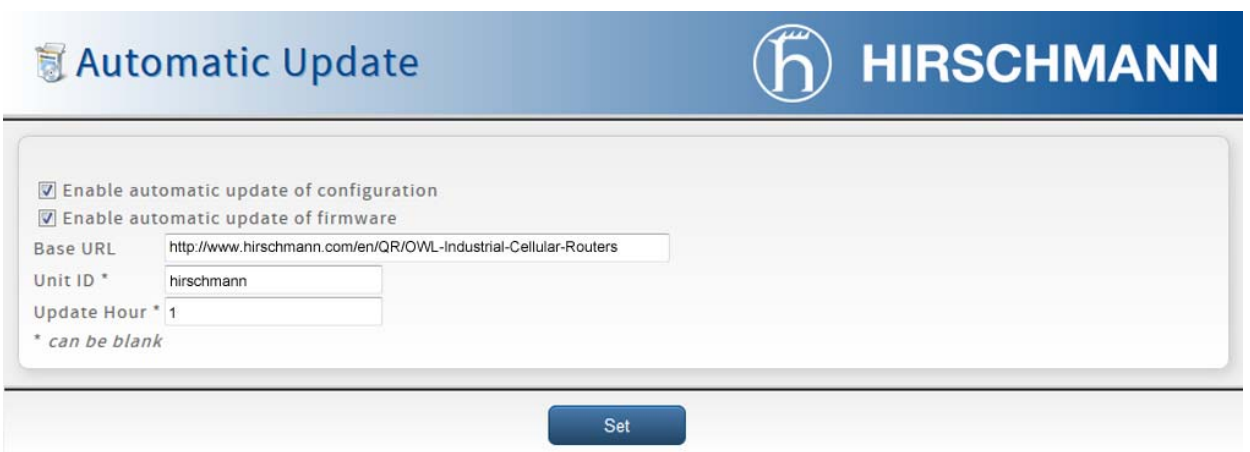


Figure 62: Automatic Update Example 1

- 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://router/OWL-3G.bin
  - Configuration file: http://router/00.11.22.33.44.55.cfg

Figure 63: 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 50: 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 51: Add User

Figure 64: Users

1.4.2 Change Profile

Using profiles you can change between different router configurations. You can for example change between different modes of router operation, router has established connection, the router has not established connection and the router creates a tunnel to the service center. 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 four 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.

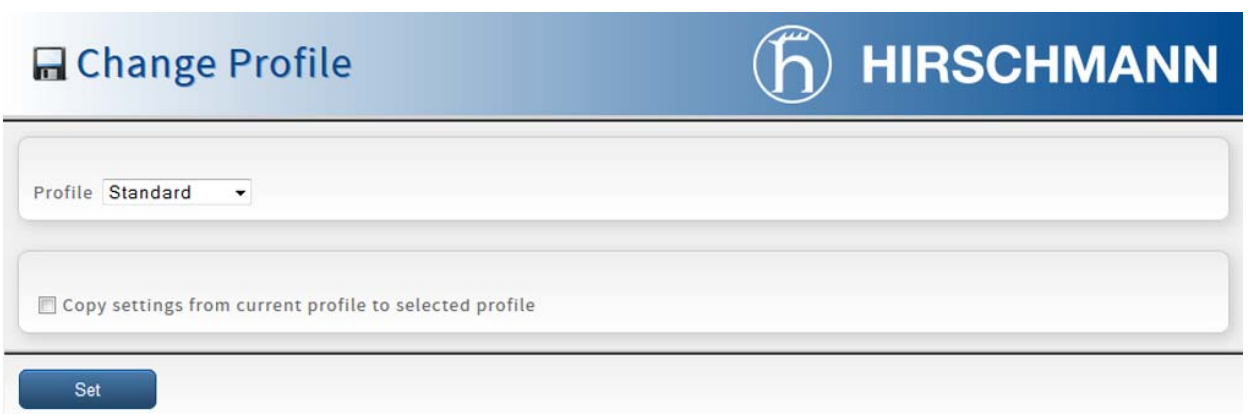


Figure 65: Change Profile

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.

Figure 66: 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 yyy-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.

Figure 67: 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 in some cases. 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).

Figure 68: 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 PIN number, open the "Unlock SIM Card" dialog in the "Administration" section of the main menu and enter your PIN number to the "SIM PIN" field. Then click the "Set" button.

Note: The SIM card is blocked after 3 failed attempts to enter the PIN code.

Figure 69: Unlock SIM Card

1.4.7 Send SMS

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

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.

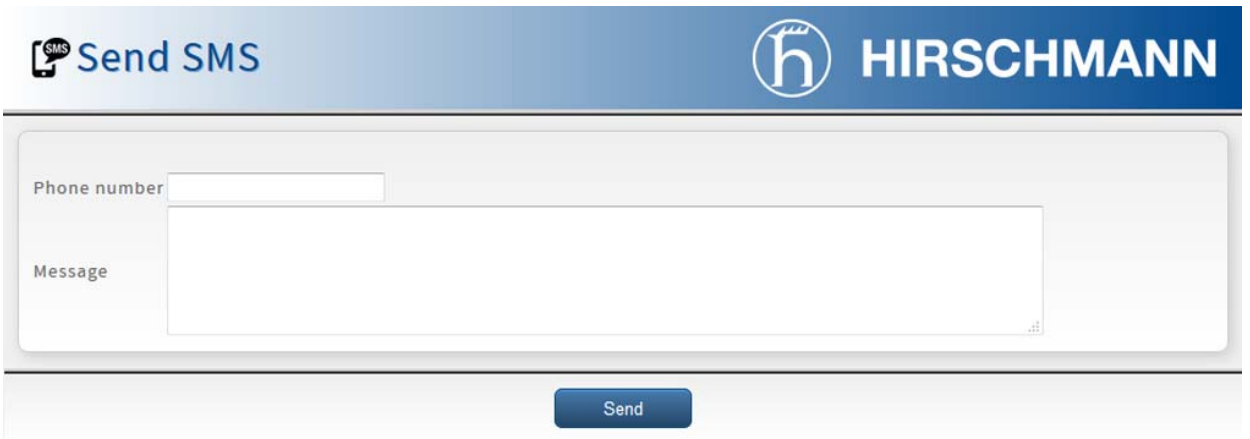


Figure 70: Send SMS

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 company.

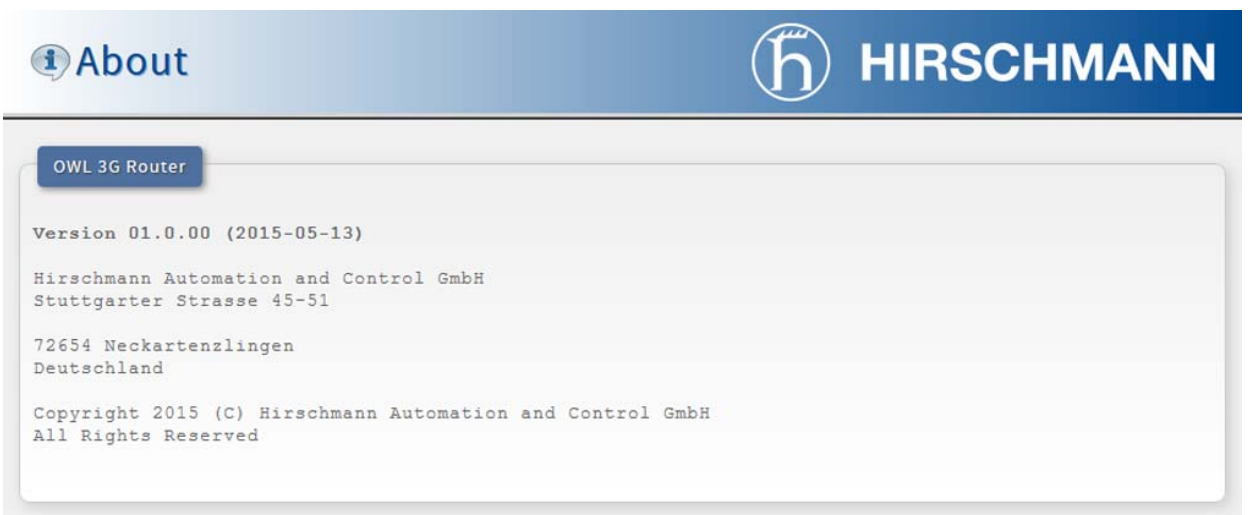


Figure 71: About

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.

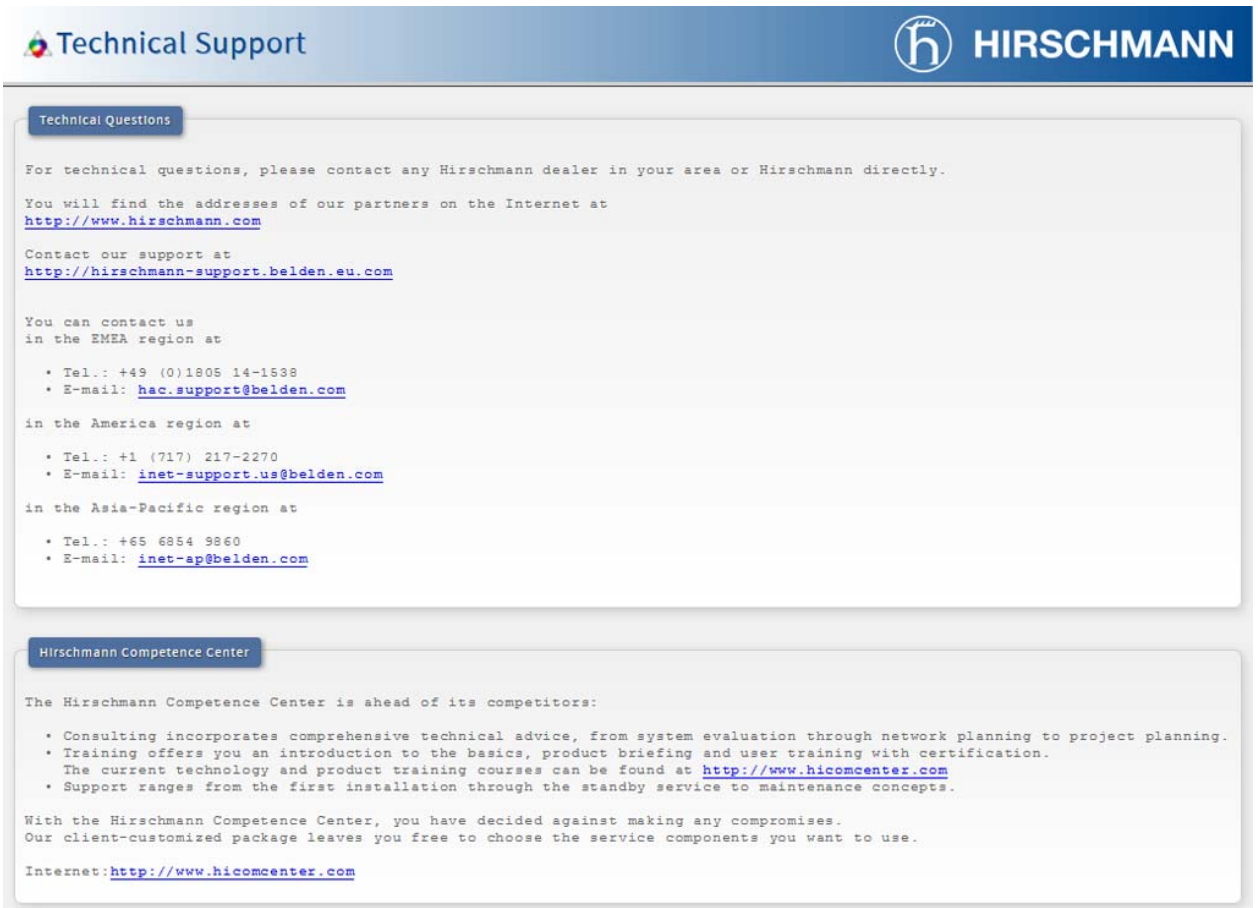
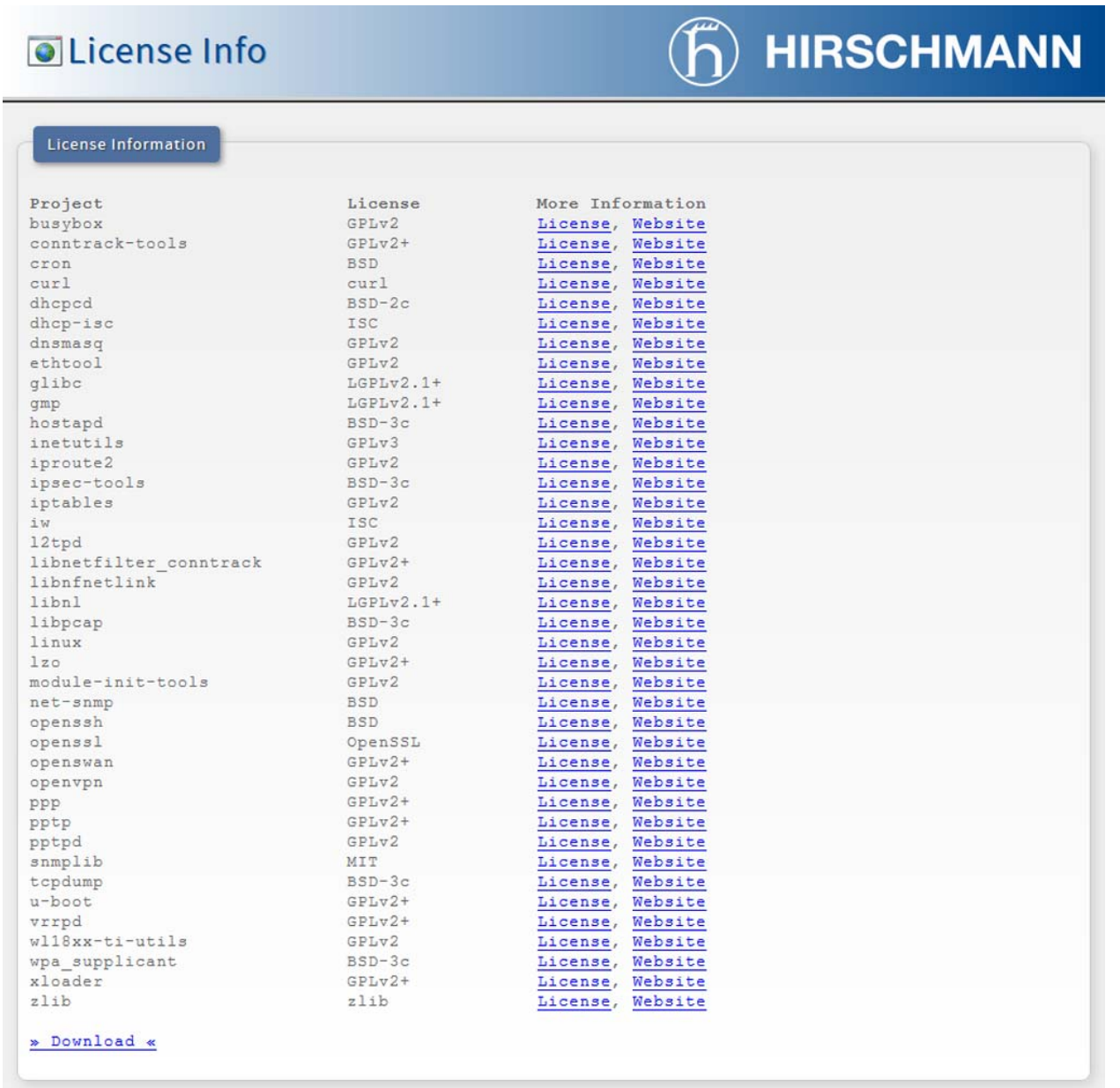


Figure 72: Technical Support

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

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

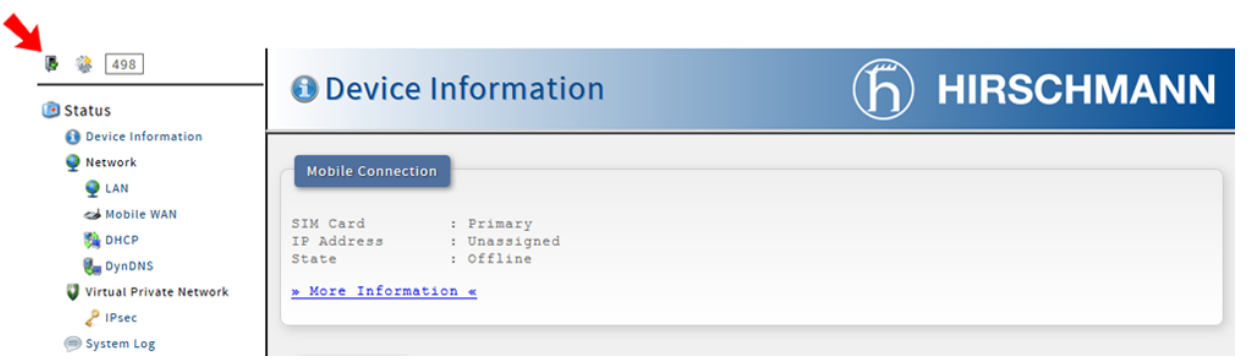


Figure 74: Logout

1.6.2 Reboot

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

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

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

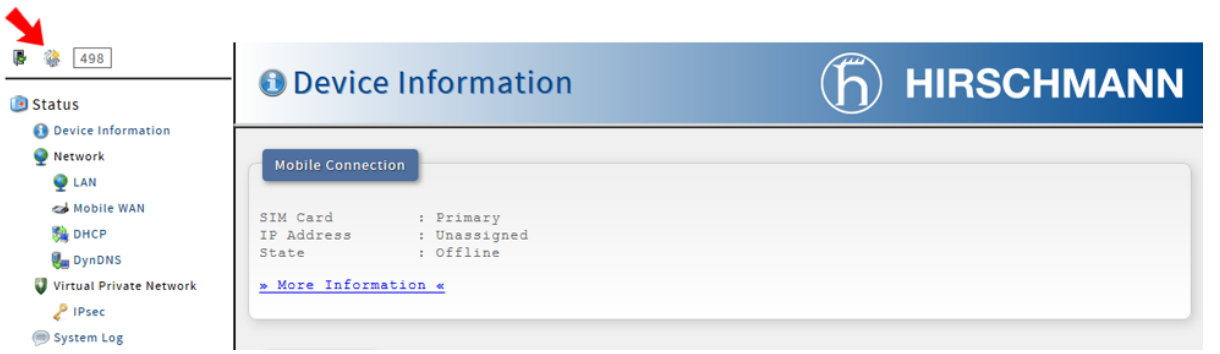


Figure 75: Reboot

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 500s. The counter restarts every time you open a dialog.

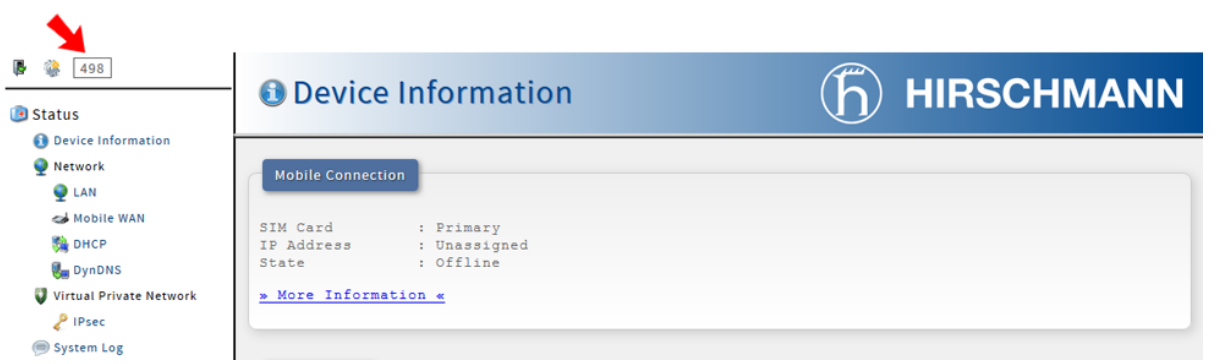


Figure 76: Timeout Counter

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.

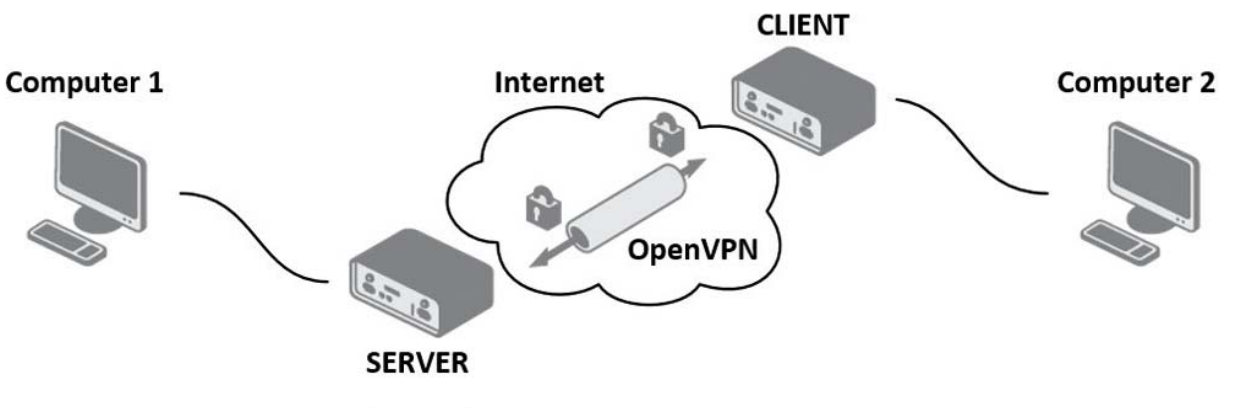


Figure 77: Basic scheme

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 52: Overview of OpenVPN tunnels

Figure 78: 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 53: 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 53: 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.

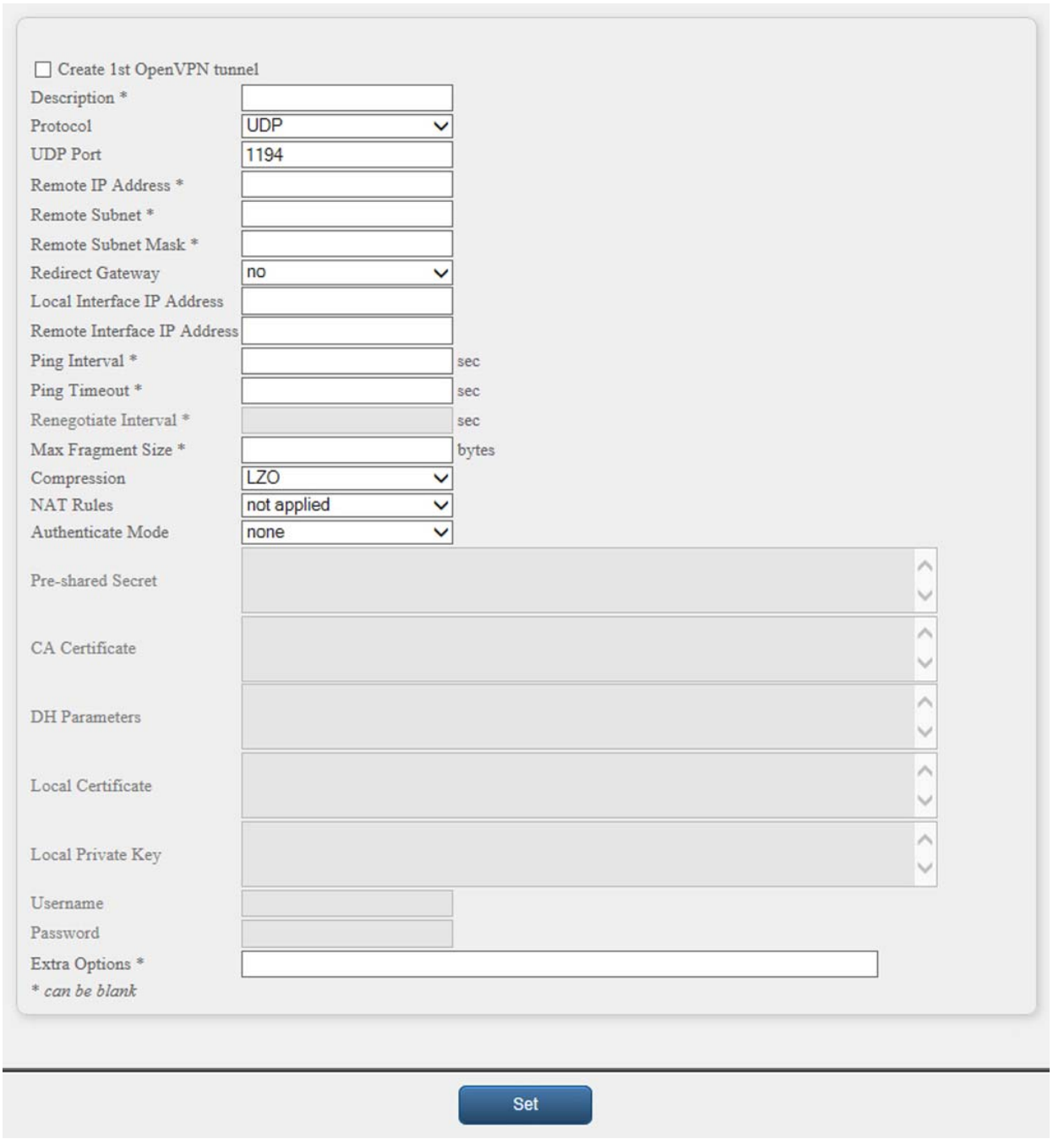


Figure 79: OpenVPN tunnel Configuration dialog

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.

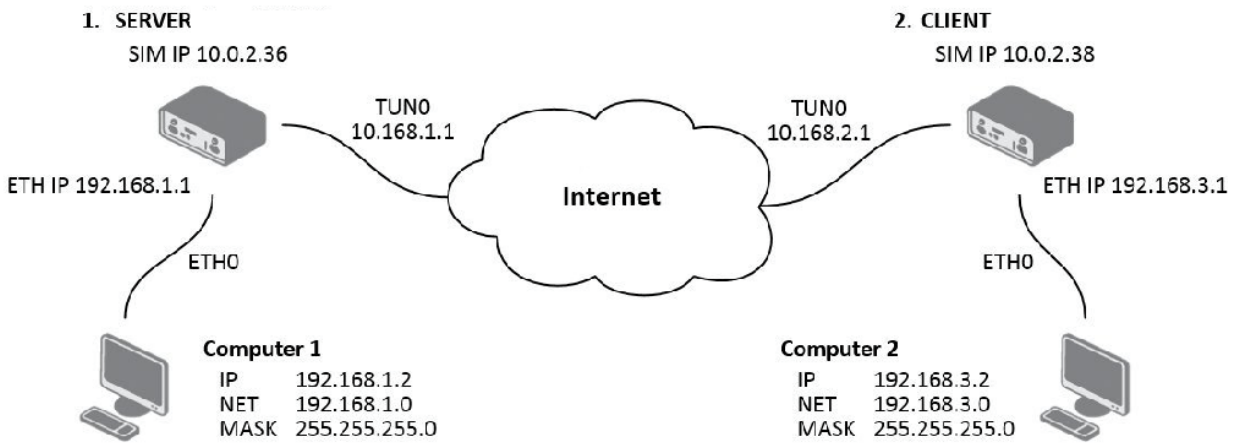


Figure 80: Router on both sides of a tunnel

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 54: 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 55: Configuration of the second router (no authentication)

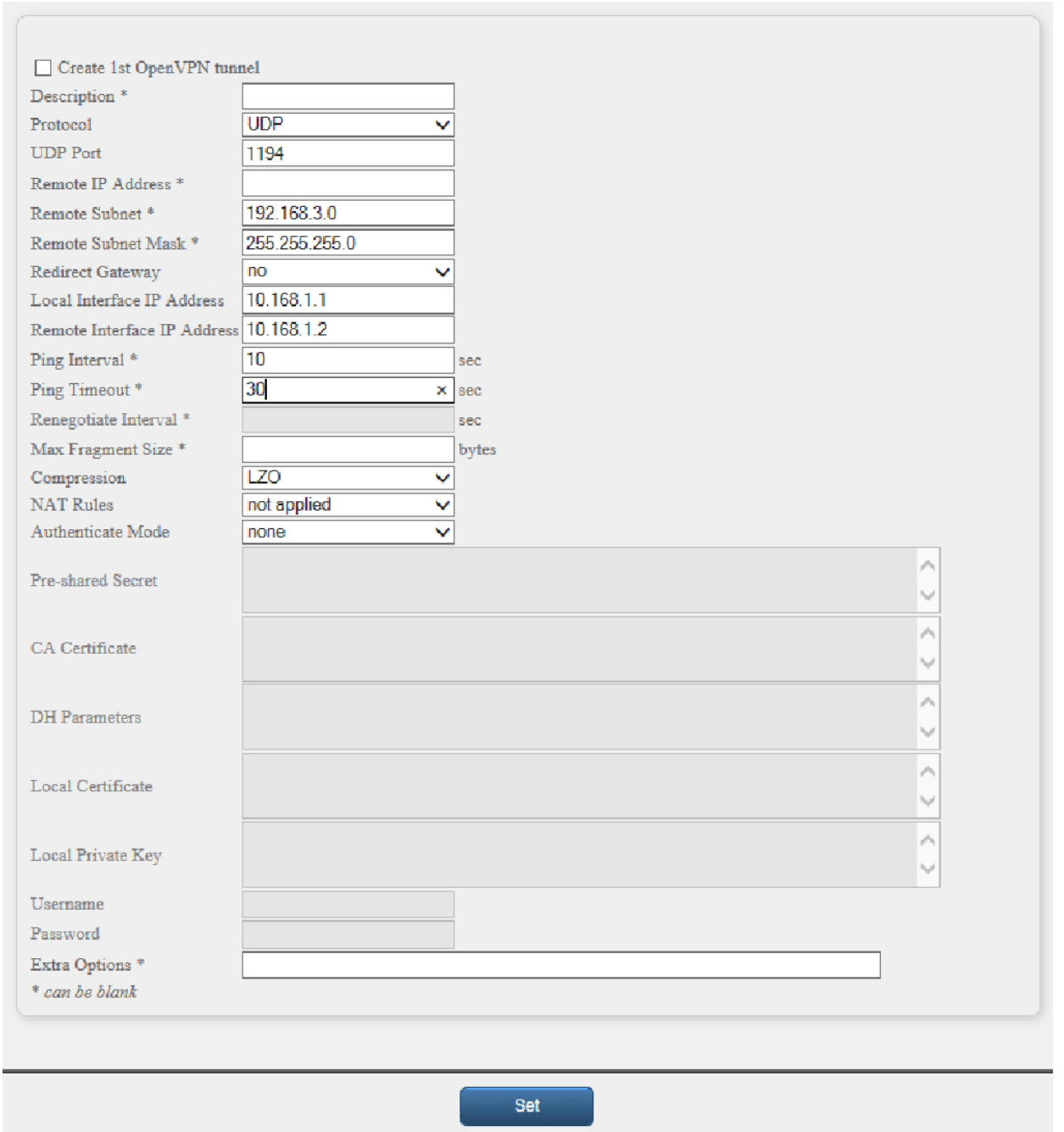


Figure 81: Configuration of the first router (no authentication)

Note: The configuration of the second router is similar to the first router. See table 55 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.

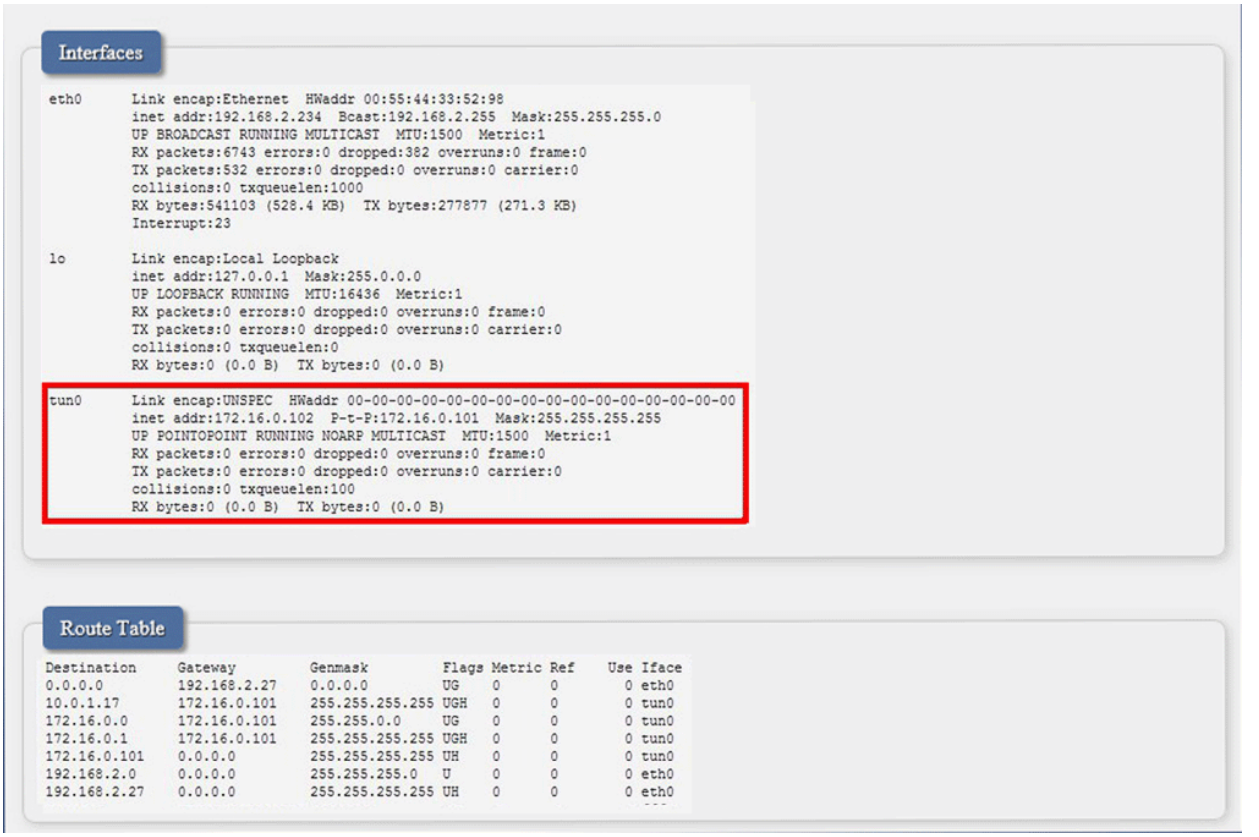


Figure 82: Network Status

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.

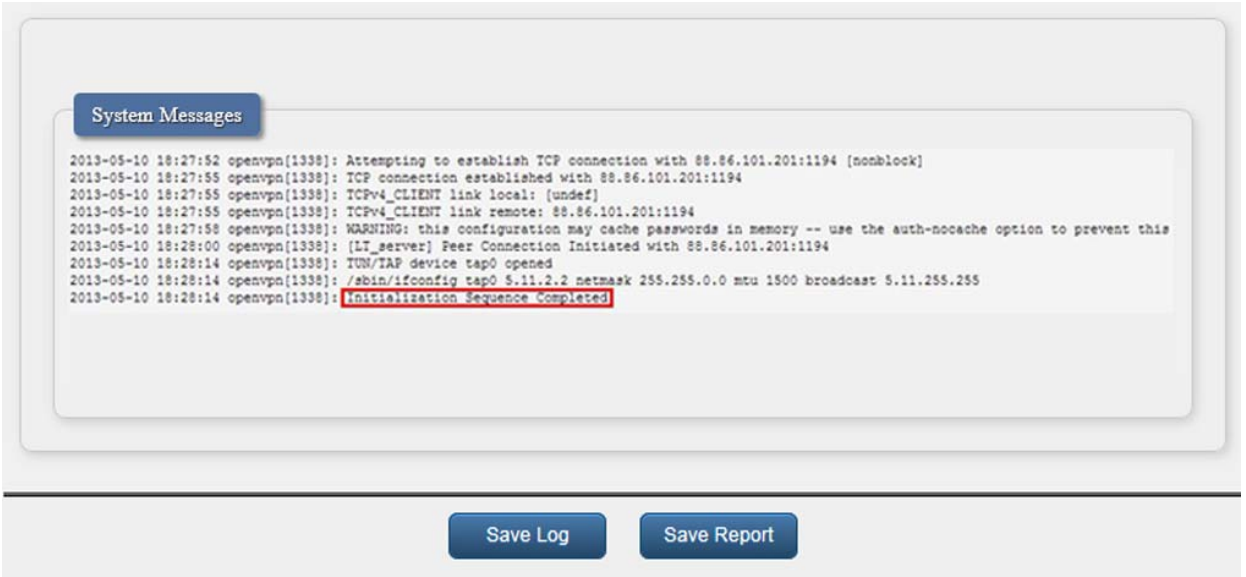


Figure 83: System log

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 56: 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 57: 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.

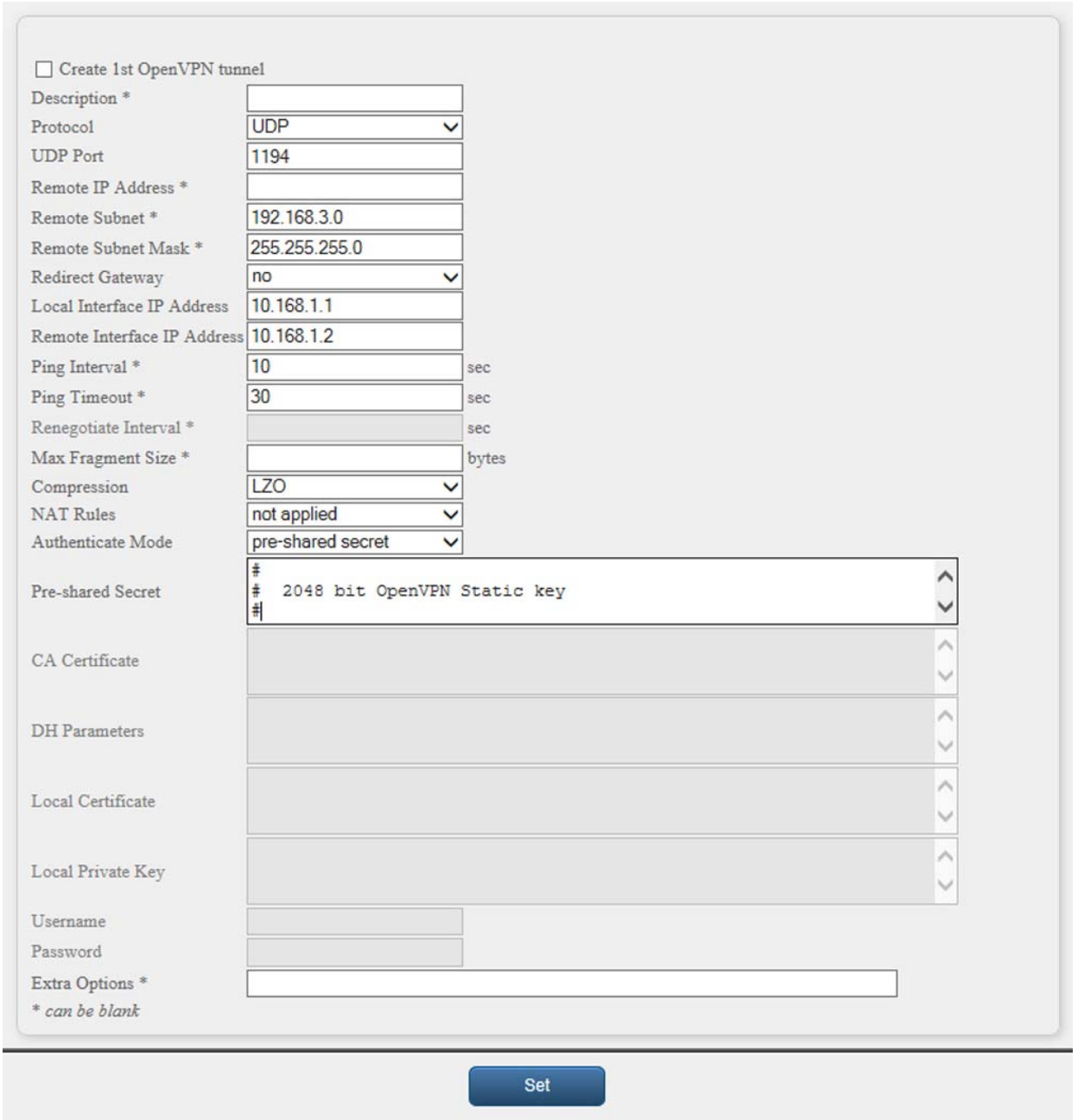


Figure 84: Configuration of the first router (pre-shared secret)

Note: The configuration of the second router is similar to the first router. See table 57 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.

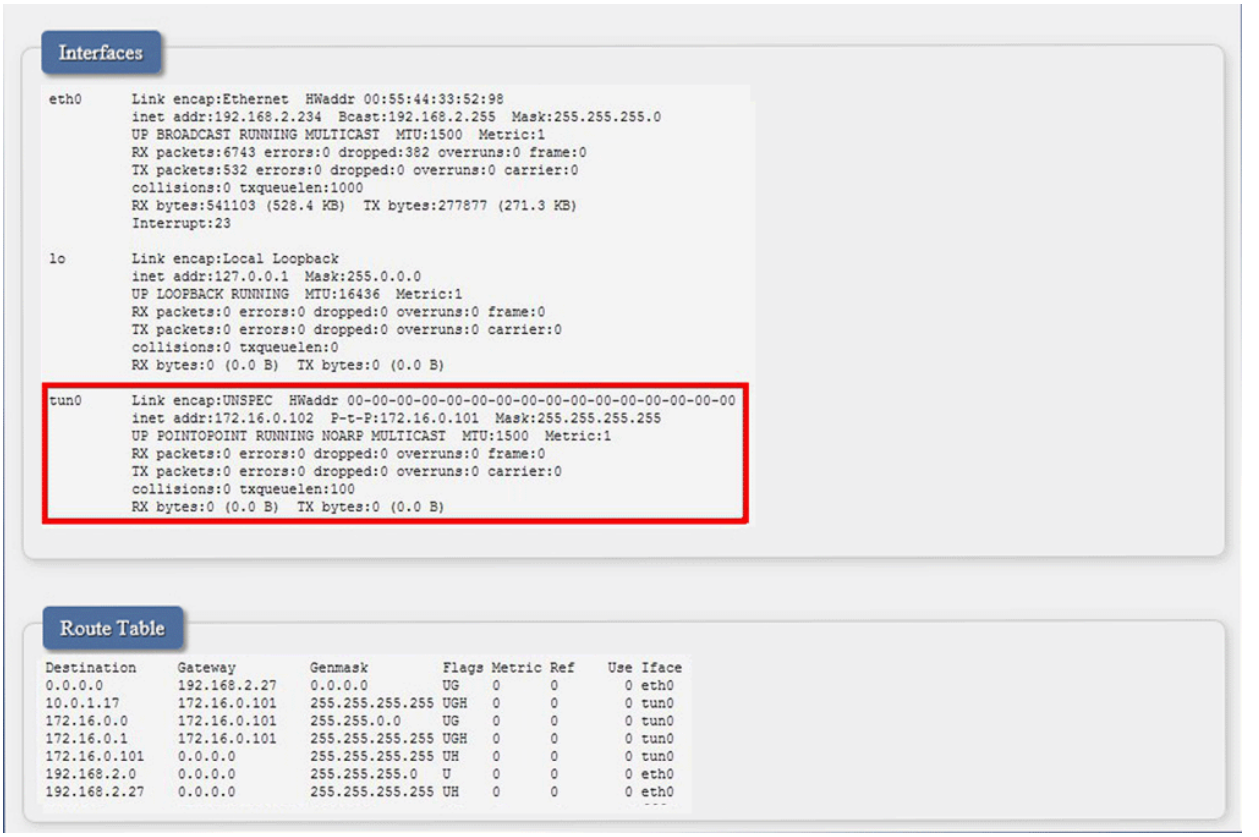


Figure 85: Network Status

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.

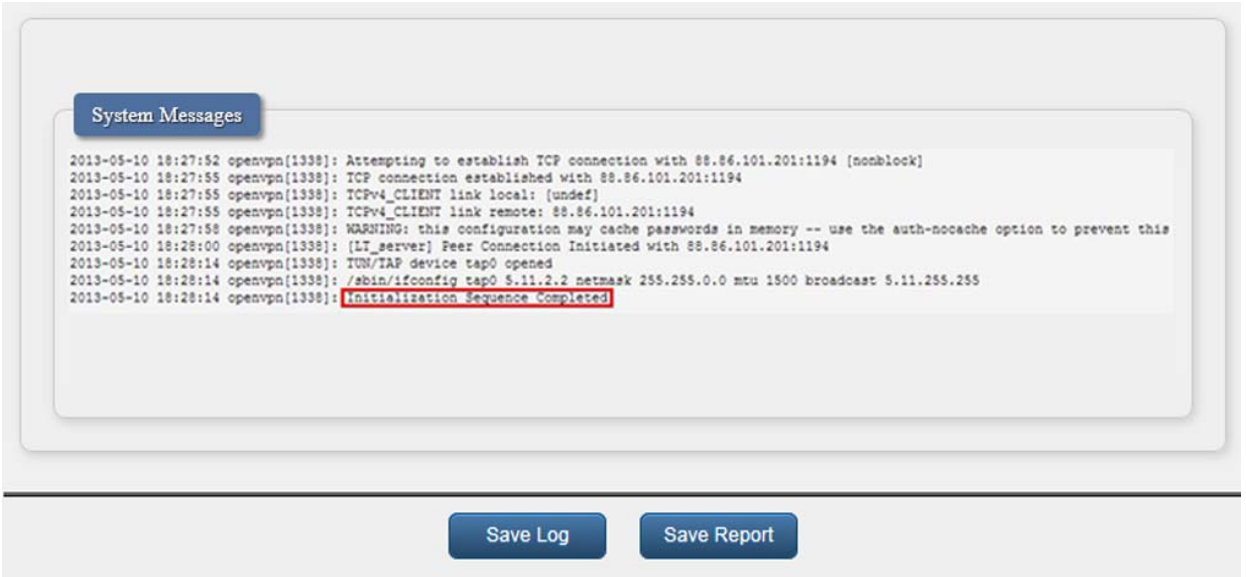


Figure 86: System log

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 58: 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 59: 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.

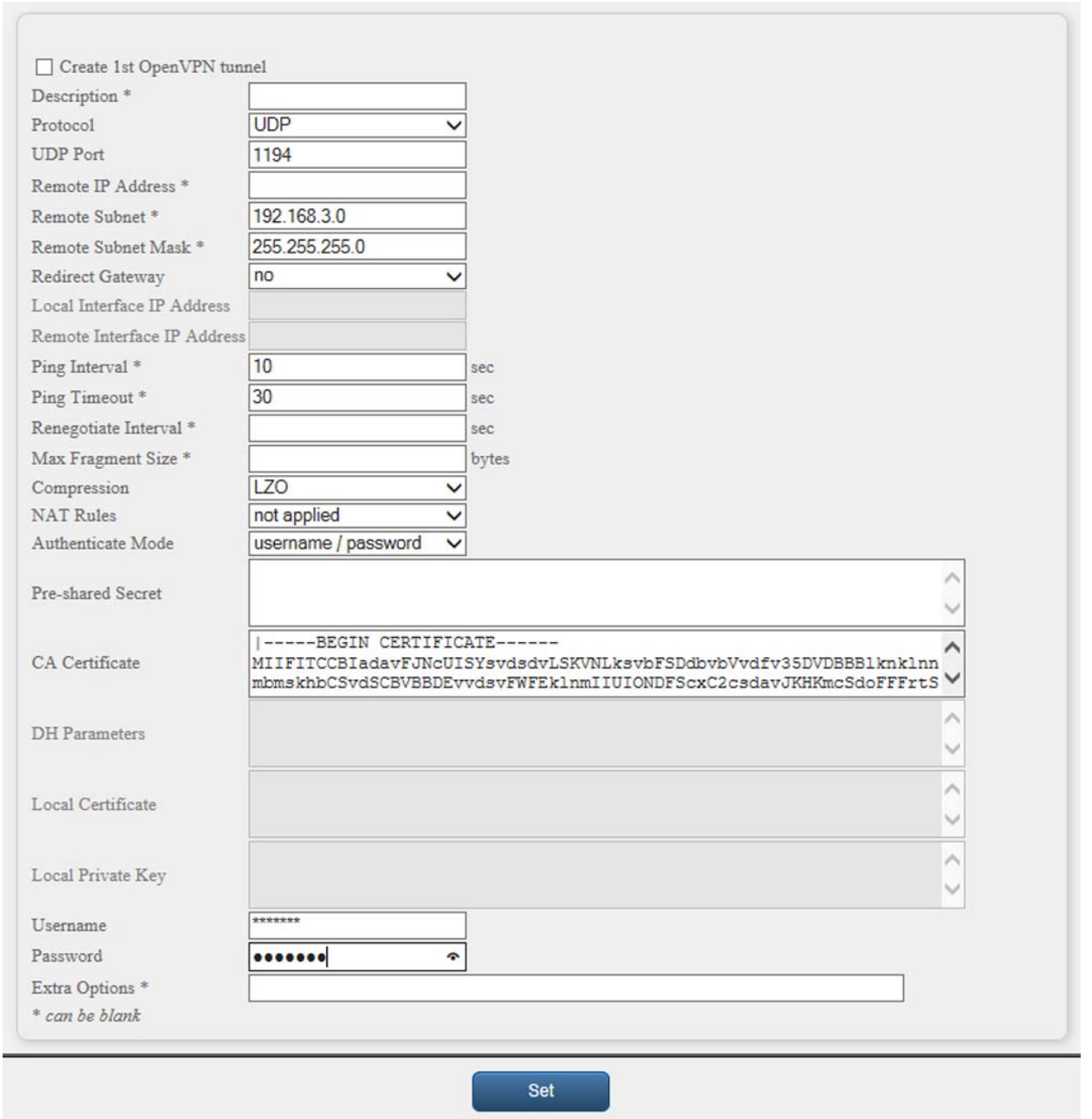


Figure 87: Configuration of the first router (username/password)

Note: The configuration of the second router is similar to the first router. See table 59 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.

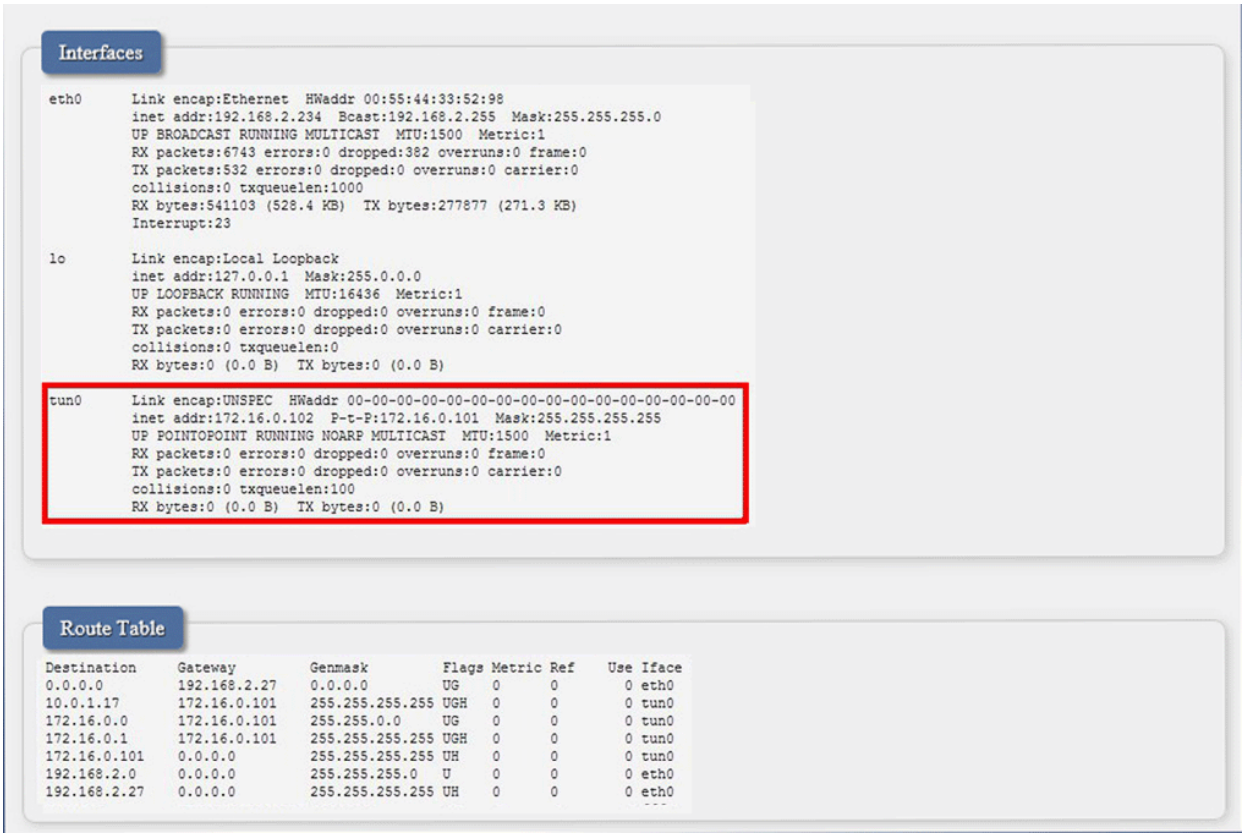


Figure 88: Network Status

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.

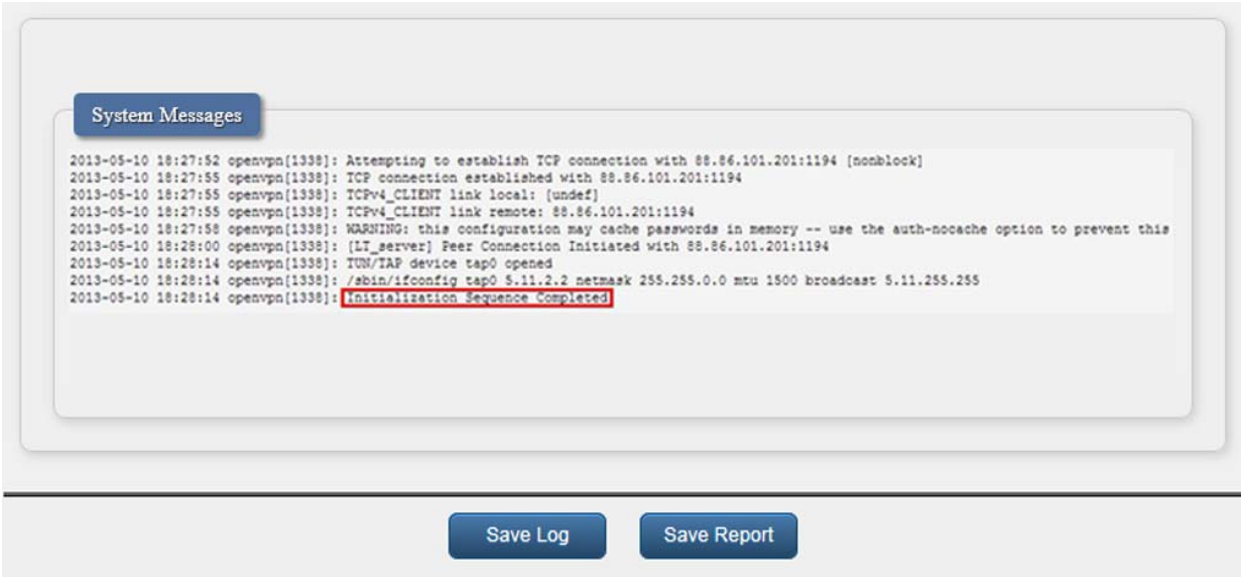


Figure 89: System log

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 60: 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 61: 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.

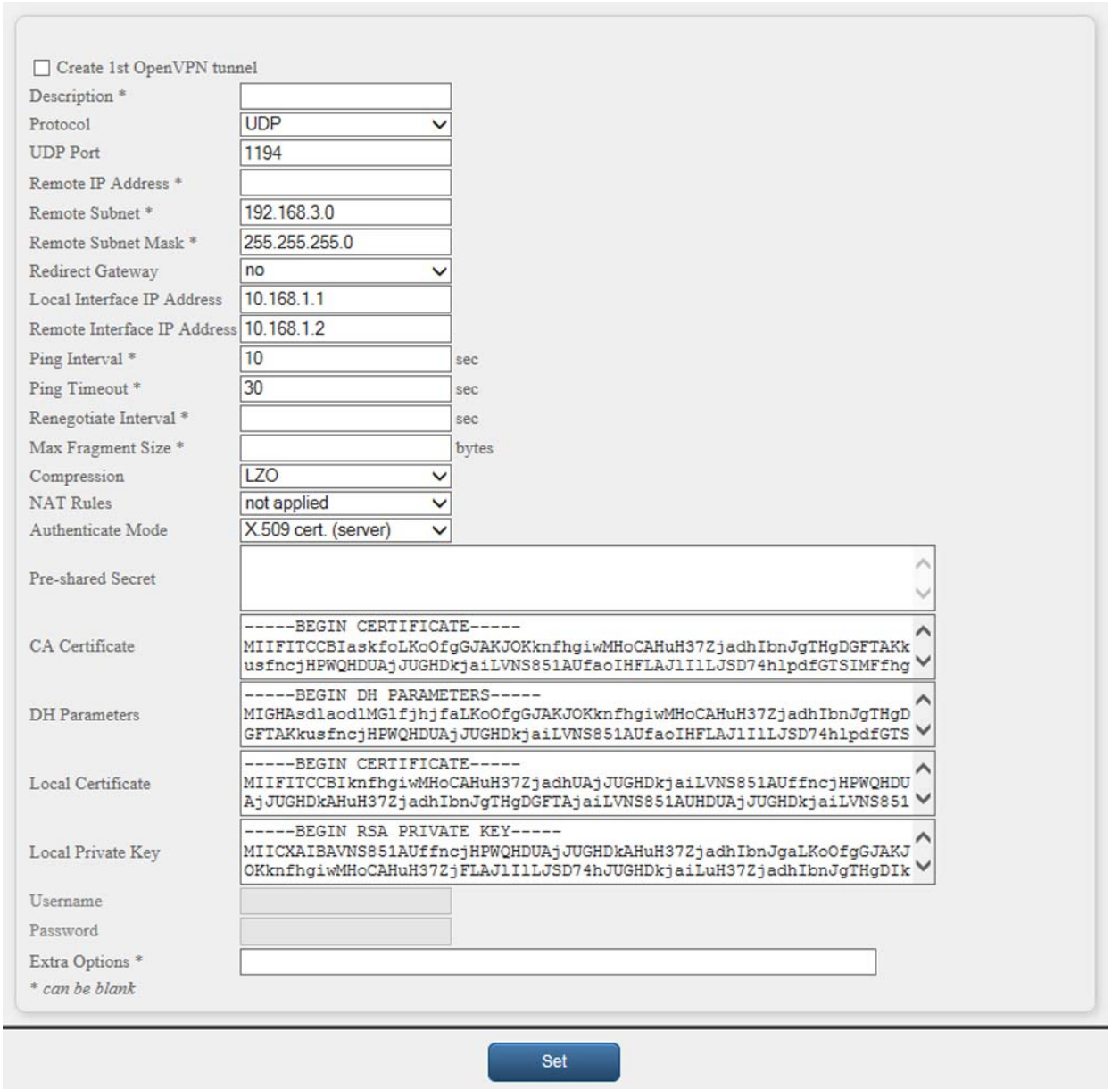


Figure 90: Configuration of the first router (X.509 certificate)

Note: The configuration of the second router is similar to the first router. See table 61 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.

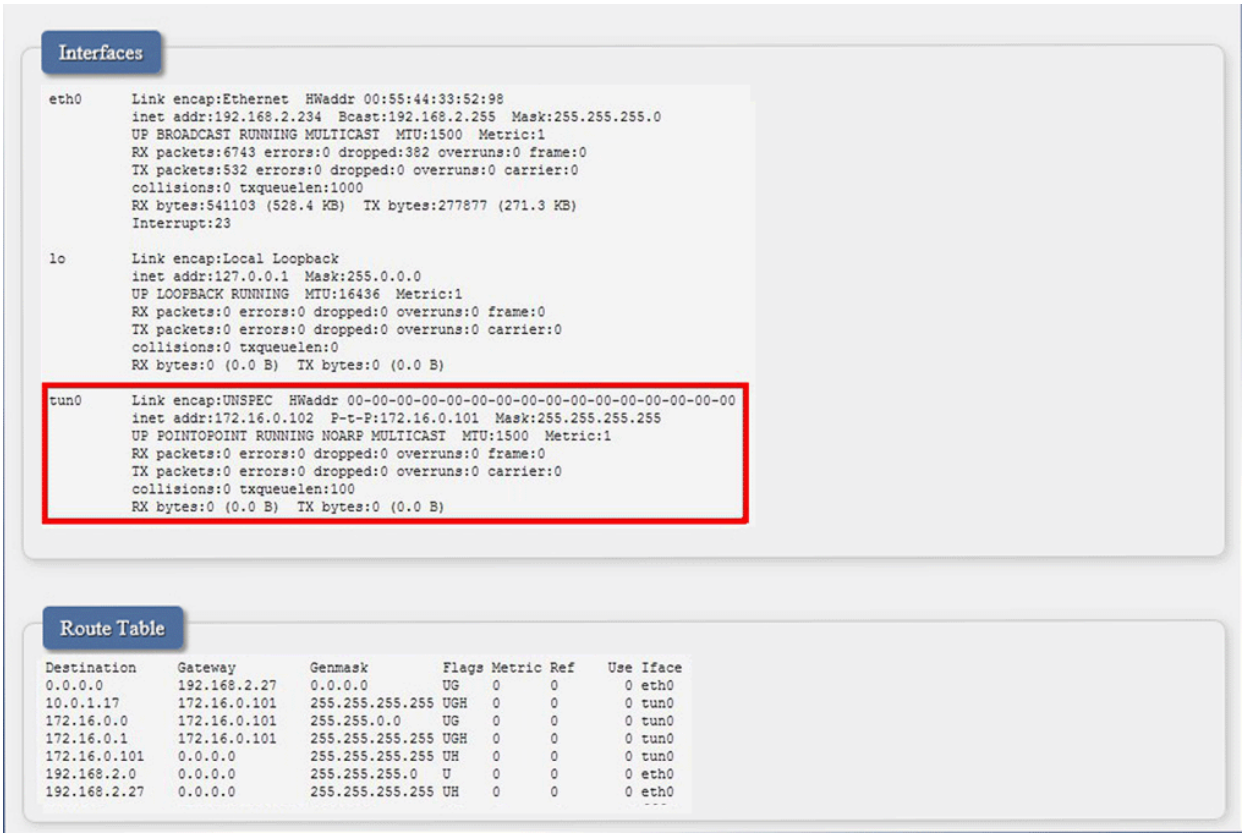


Figure 91: Network Status

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.

Figure 92: 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.

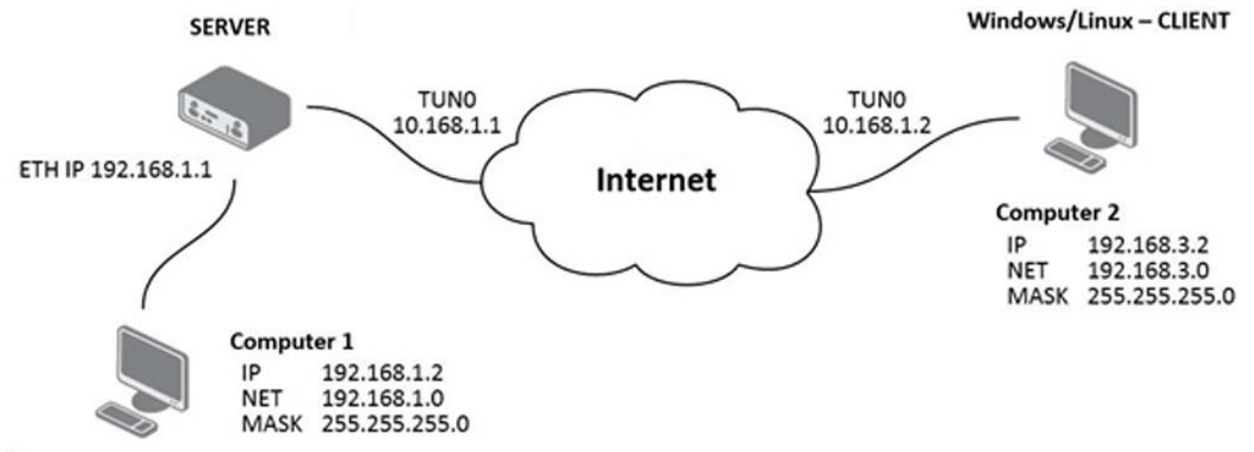


Figure 93: OpenVPN tunnel paired with a Windows/Linux CLIENT

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 62: Router configuration

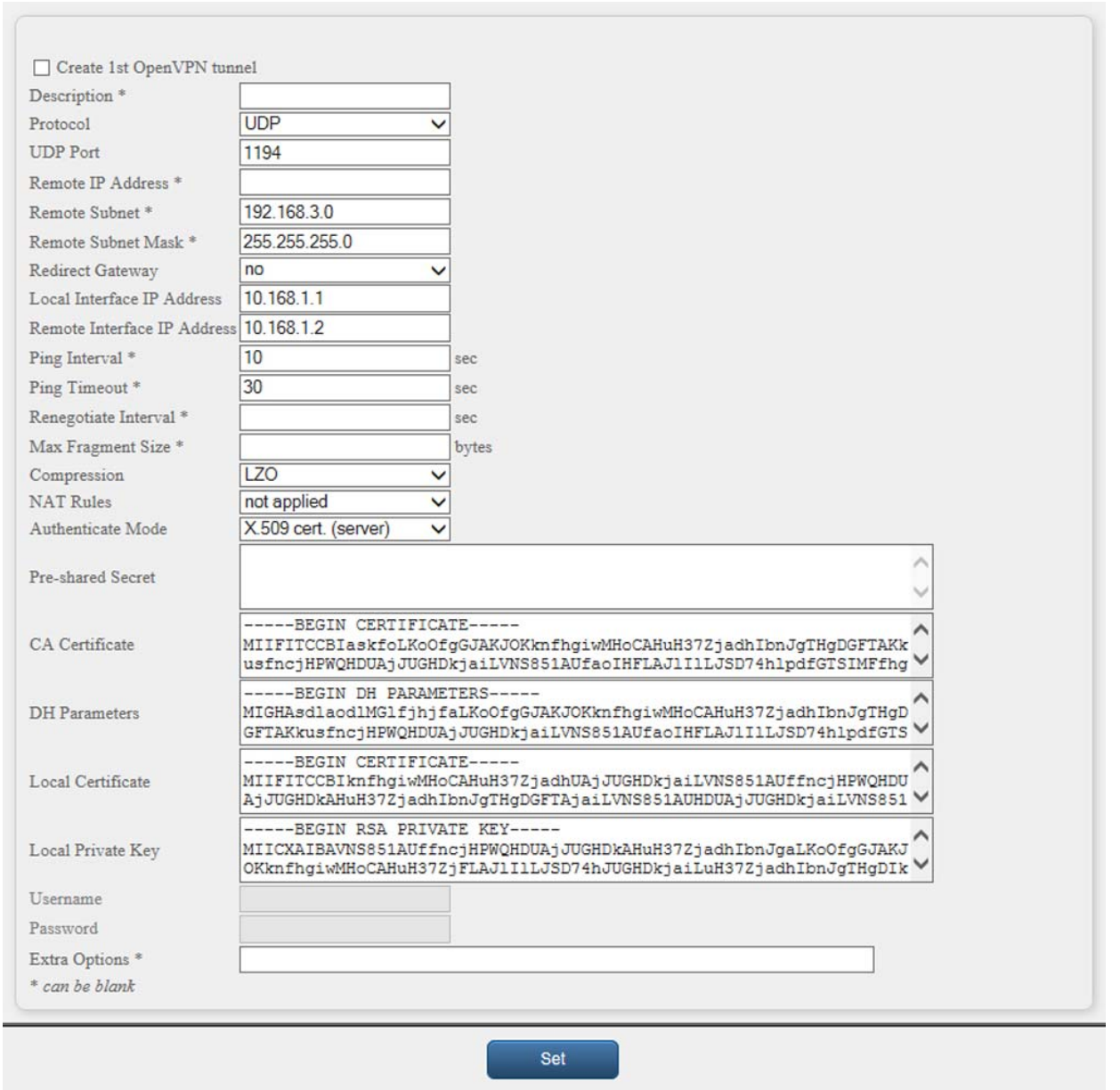


Figure 94: Router configuration

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.

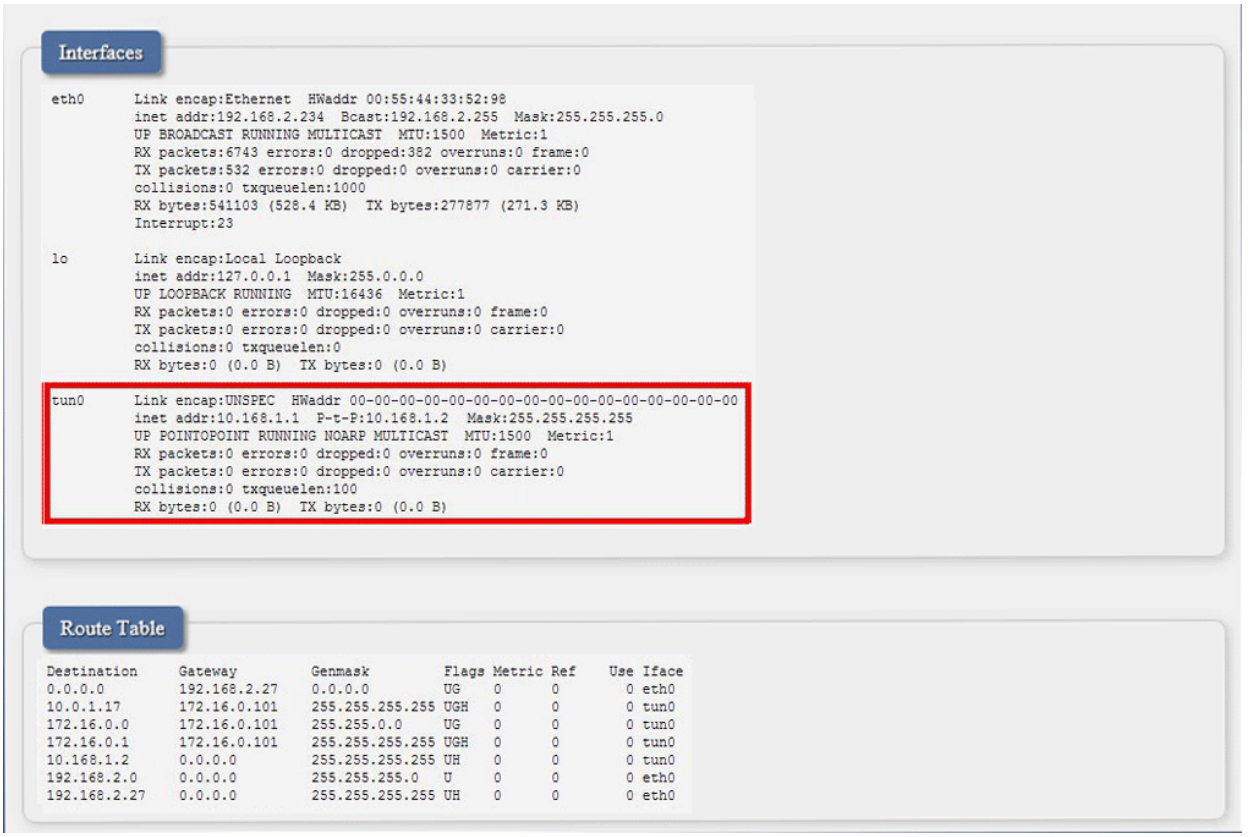


Figure 95: Network Status

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.

Figure 96: 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 10.0.2.36 tls-client

dev tun pull
ifconfig 10.168.1.2 10.168.1.1
route 192.168.2.0 255.255.255.0 10.168.1.2

mute 10

ca cacert.pem
cert client-cert.pem key client-key2.pem

comp-lzo verb 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.

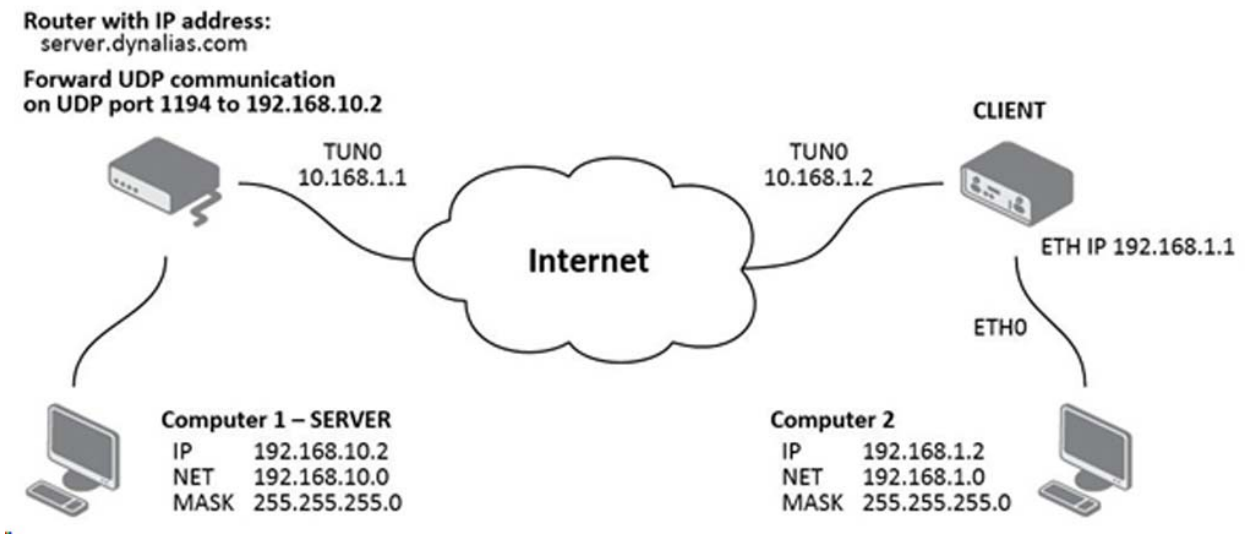


Figure 97: OpenVPN tunnel paired with a Windows/Linux Server

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 63: Router configuration

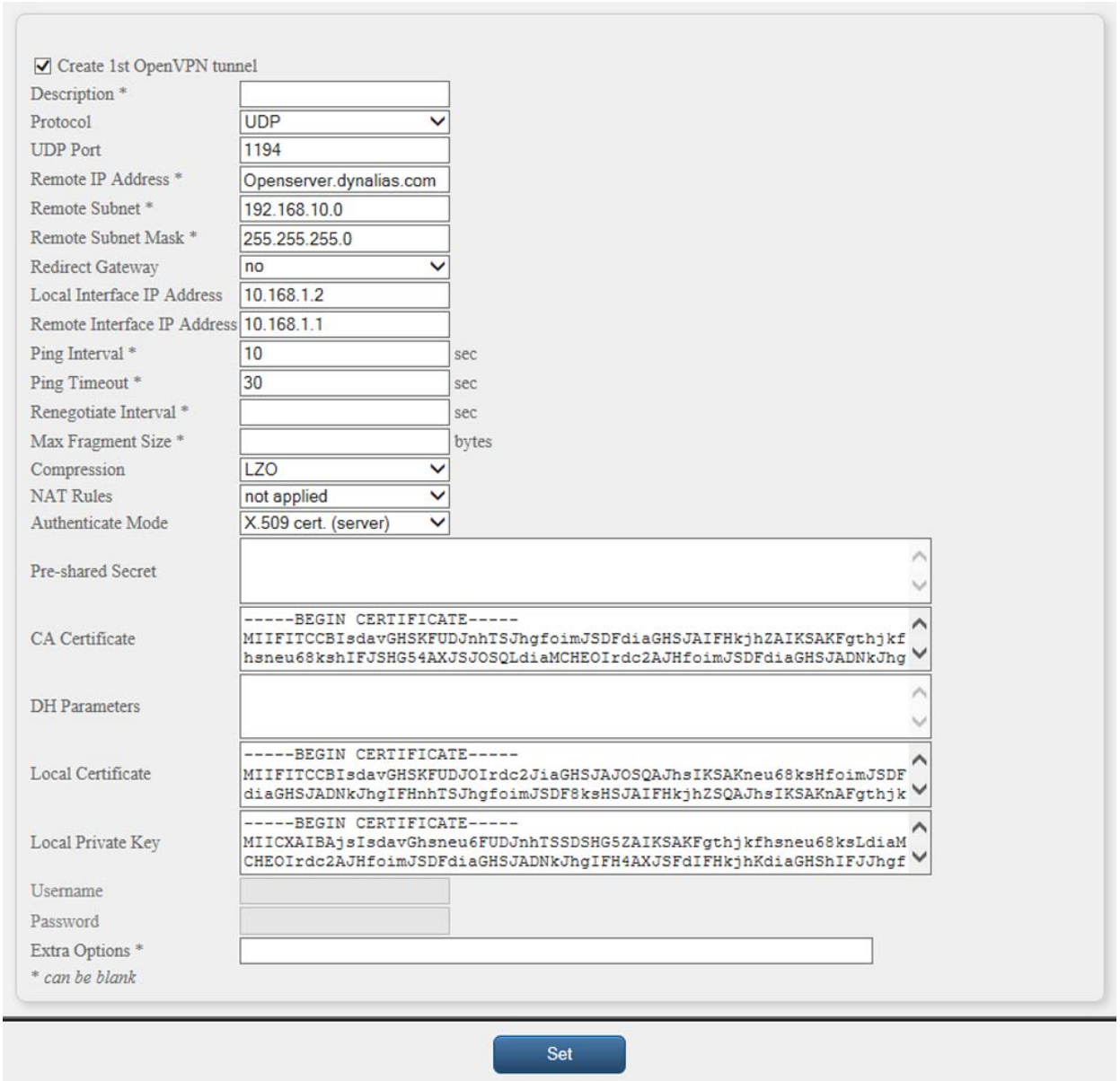


Figure 98: Router configuration

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.

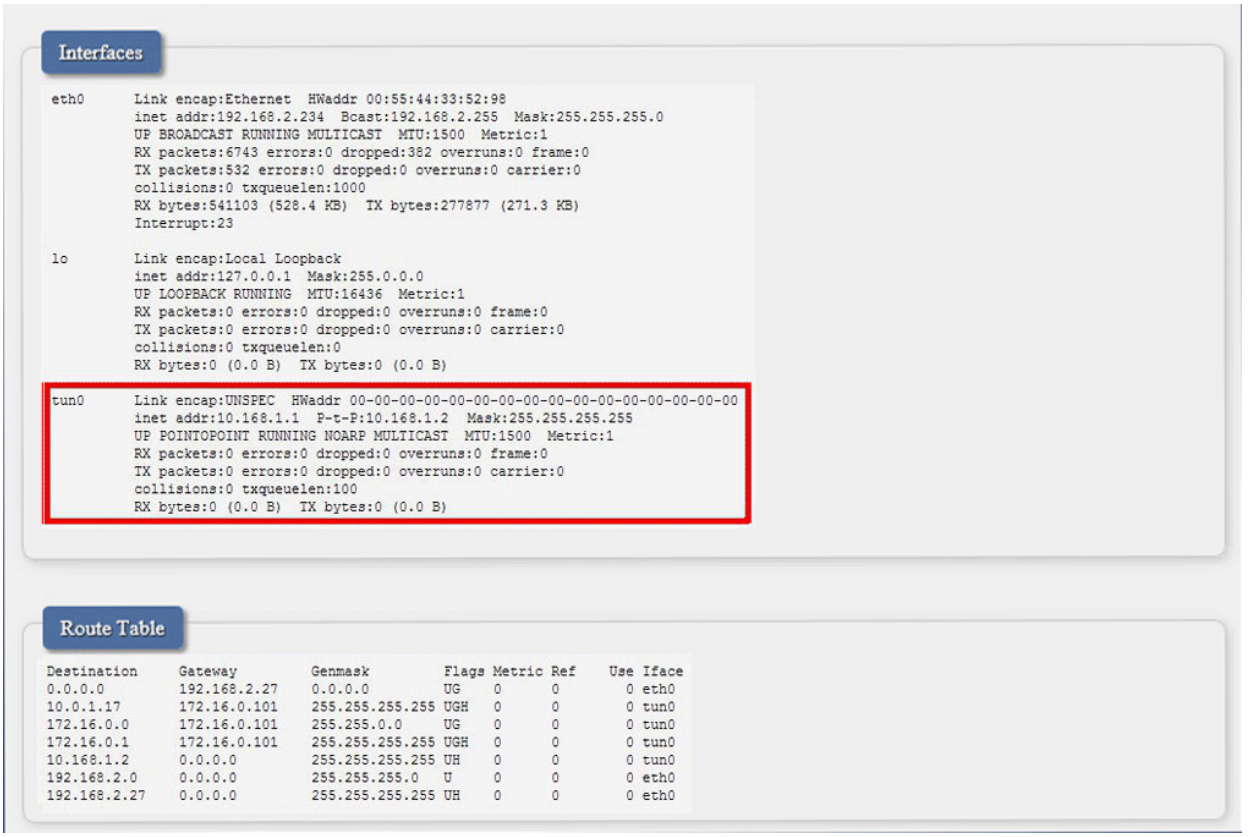


Figure 99: Network Status

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.

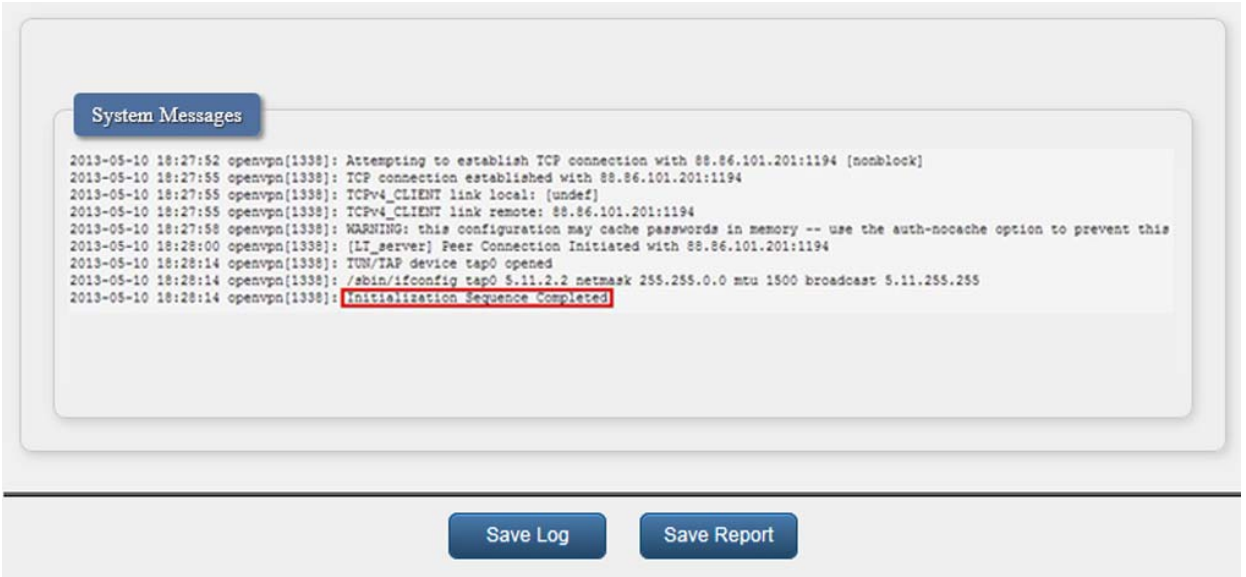


Figure 100:System log

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 tls-server

dev tun pull
ifconfig 10.168.1.1 10.168.1.2
route 192.168.1.0 255.255.255.0 10.168.1.2

mute 10

ca cacert.pem
cert client-cert.pem key client-key2.pem

comp-lzo verb 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.

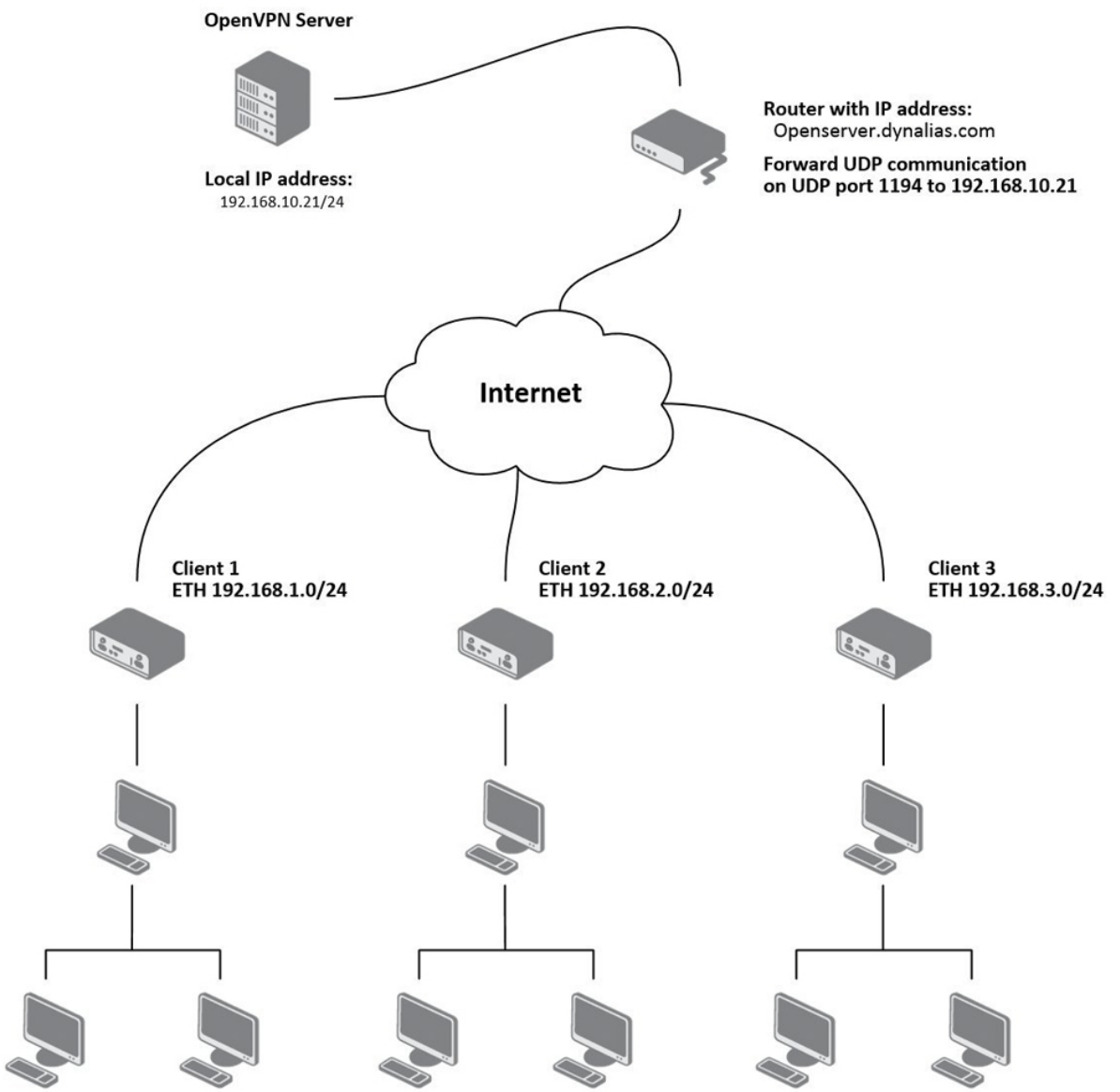


Figure 101:OpenVPN Multi-server – Hirschmann router (CLIENT)

2.6.1 OpenVPN tunnel configuration on Hirschmann routers

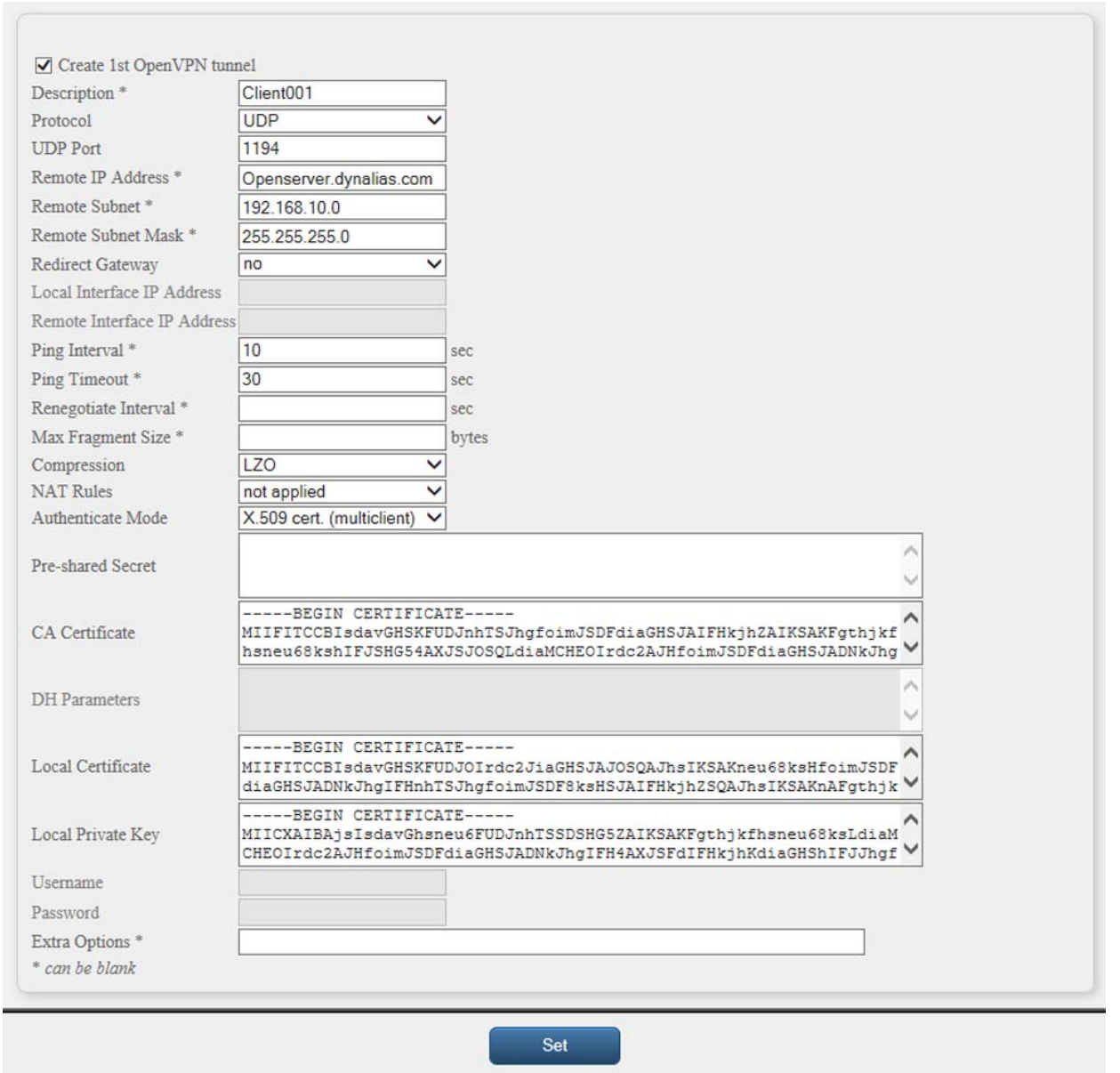


Figure 102:Configuration of Hirschmann router

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.

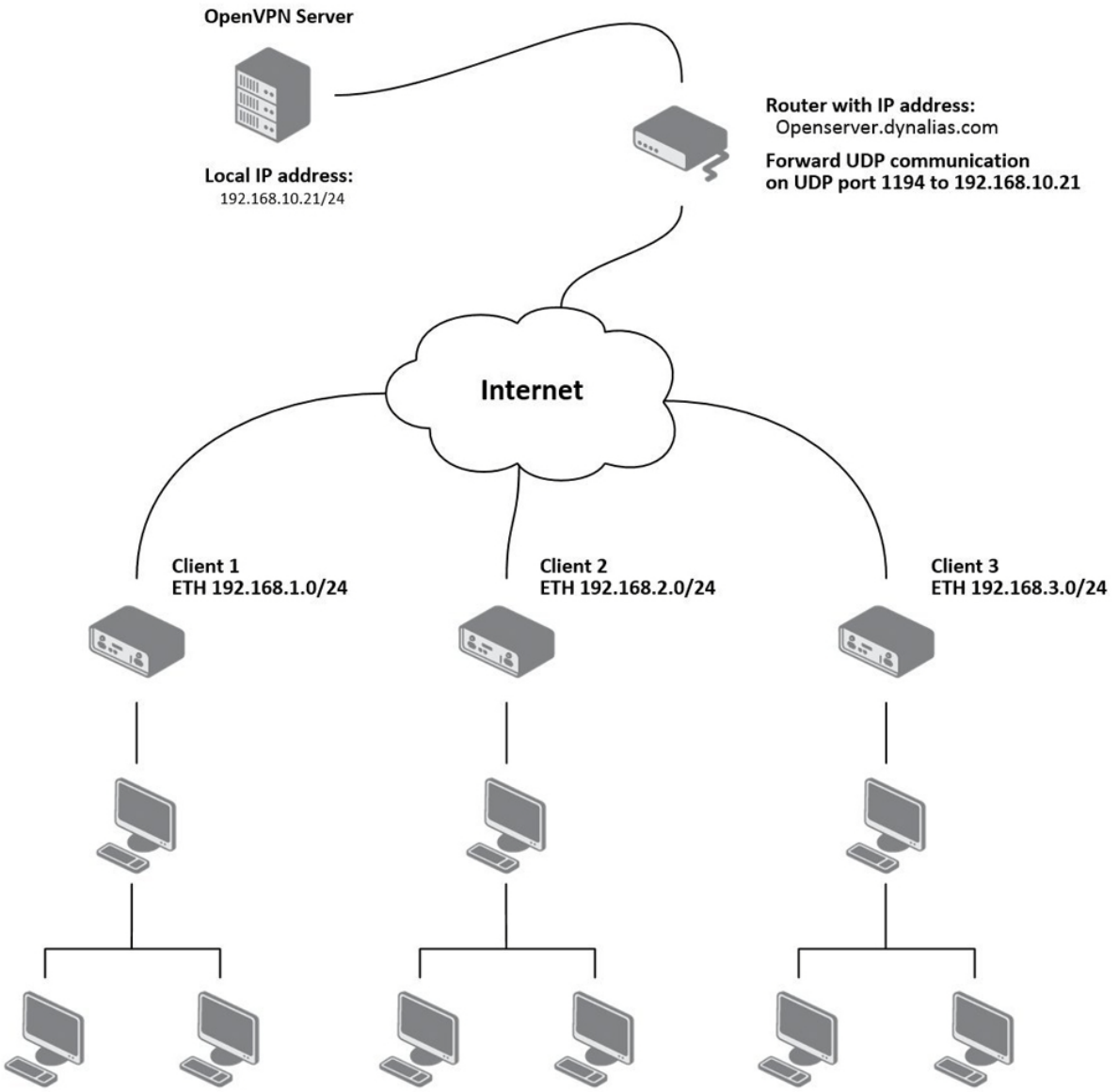


Figure 103:OpenVPN client to client

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

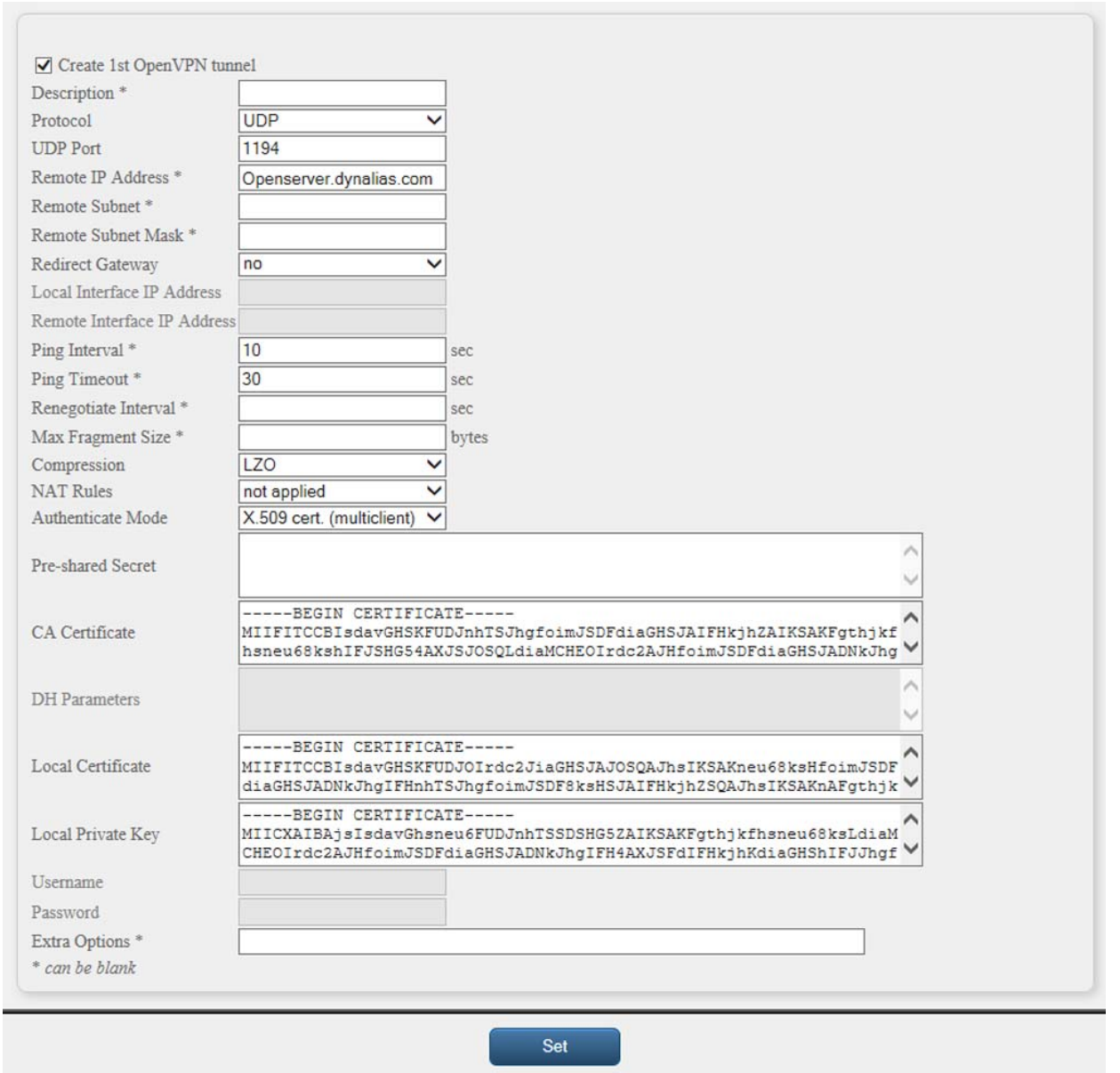


Figure 104:Router configuration

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.

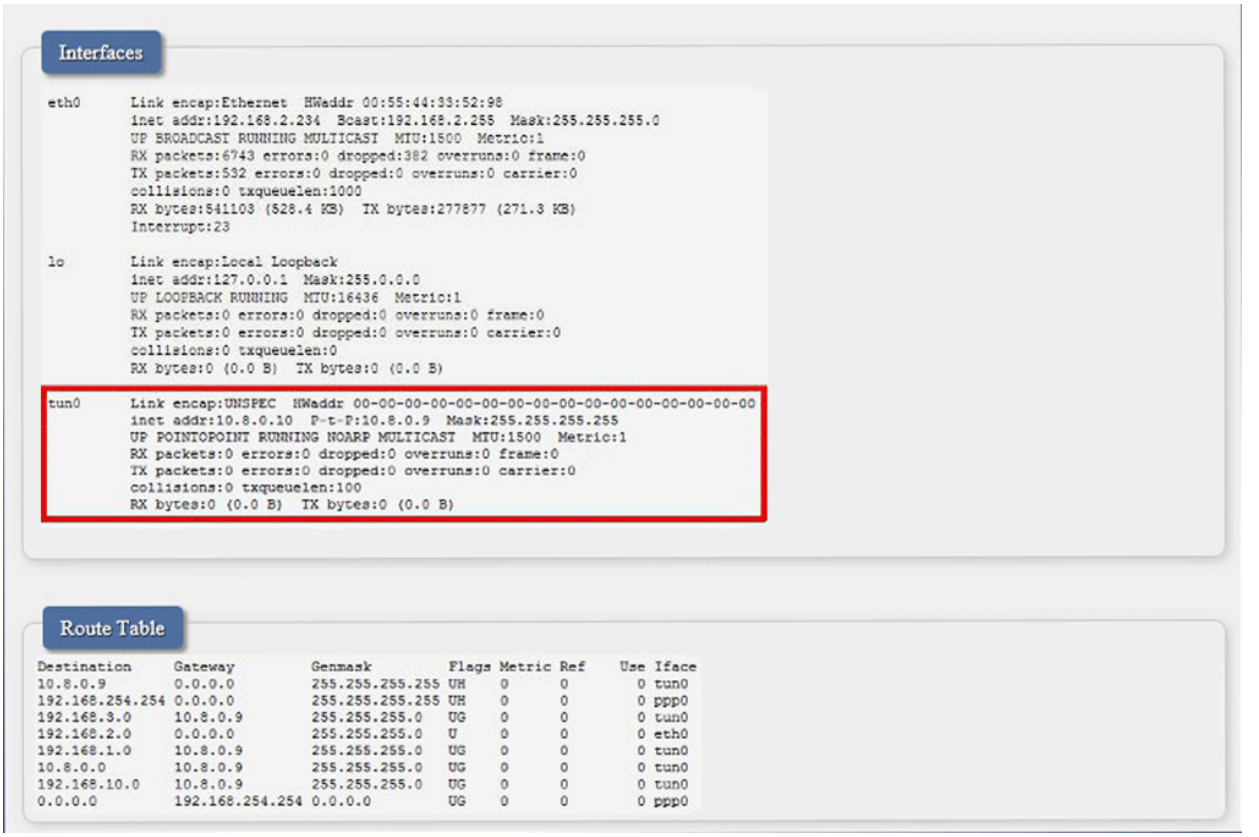


Figure 105:Network Status

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.

Figure 106:System log

2.8 Creation of pre-shared key

For creating pre-shared key is needed to have installed OpenVPN program (description of installation can be found in appendix A: Installation of OpenVPN (Windows) on page).

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.

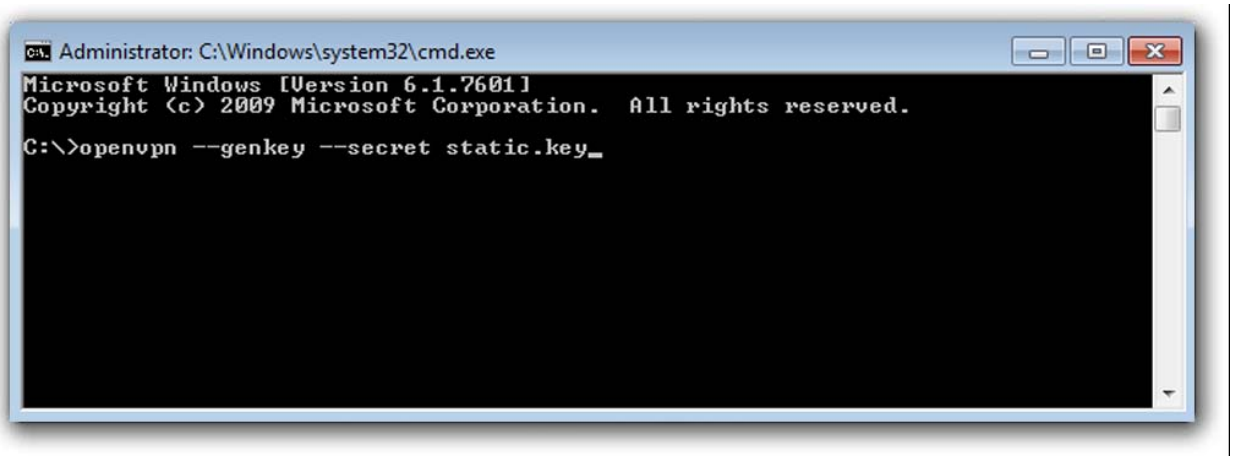


Figure 107:Generating a pre-shared key

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 is needed to have installed OpenVPN program (description of installation can be found in appendix A: Installation of OpenVPN (Windows) on page).

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.

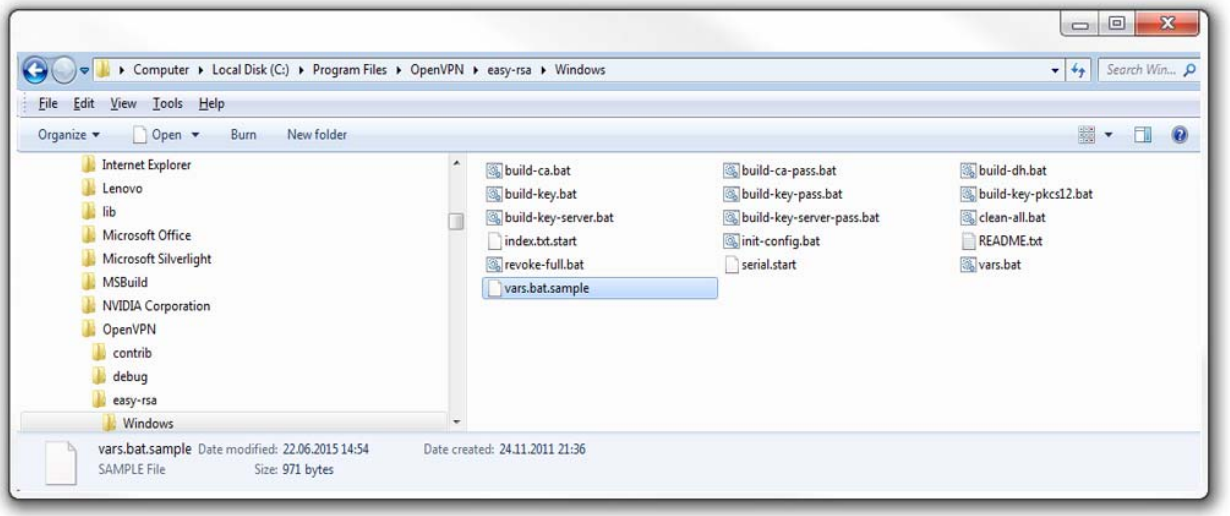


Figure 108:easy-rsa directory

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:

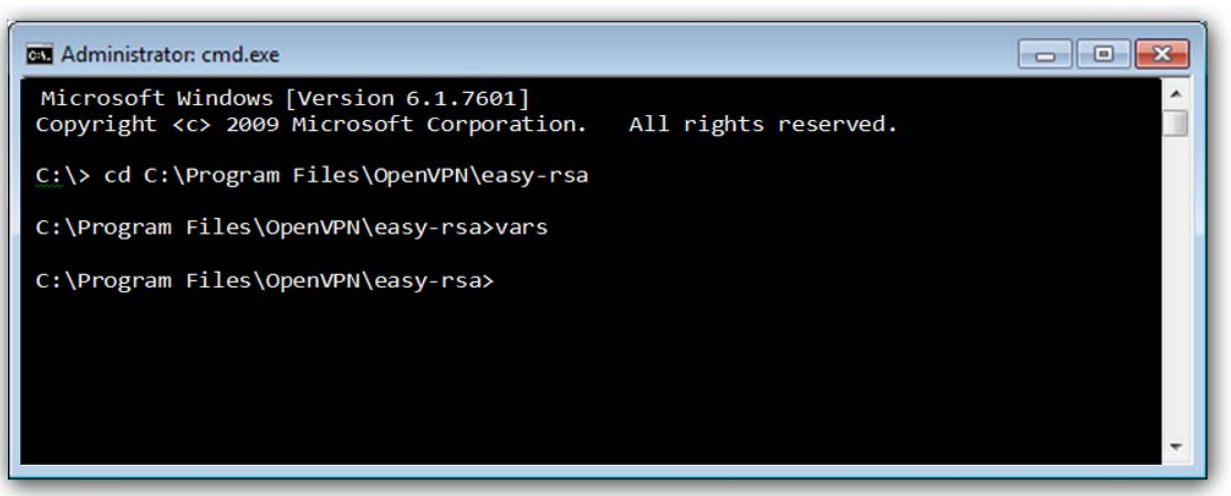


Figure 109:vars.bat loading.

Use the clean-all command to delete the old certificates from the directory.

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

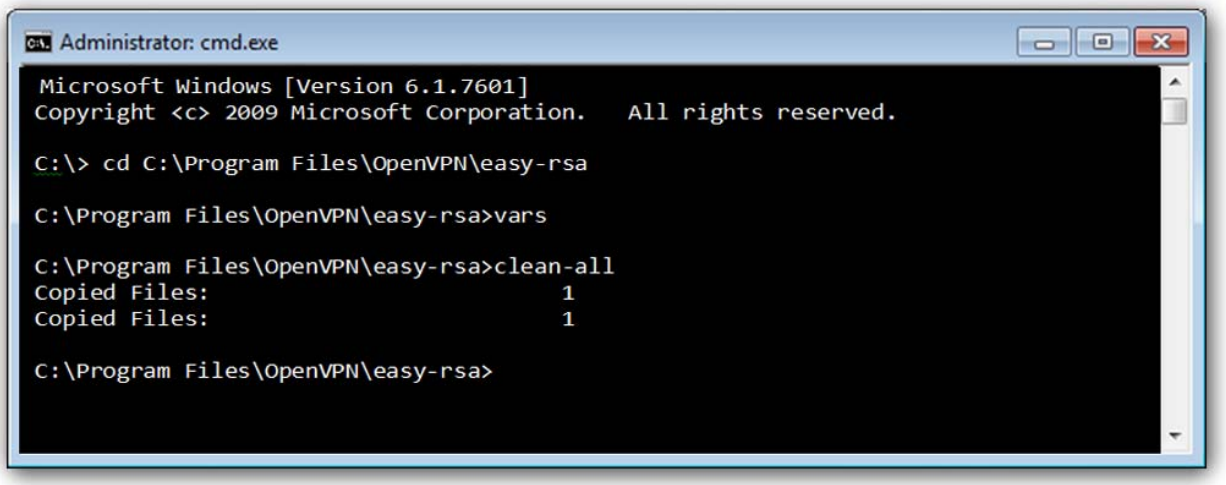


Figure 110:clean-all command.

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

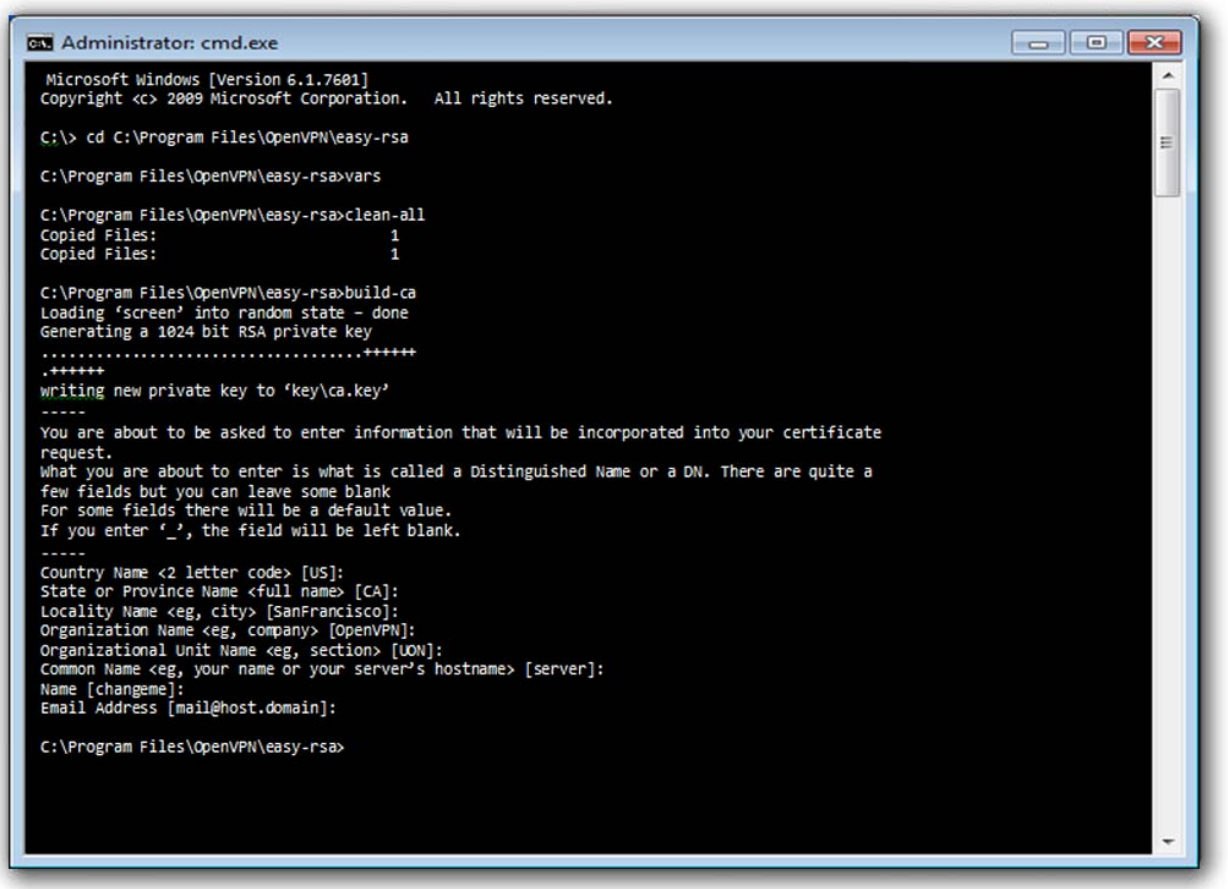


Figure 111:Generating a certificate authority

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.

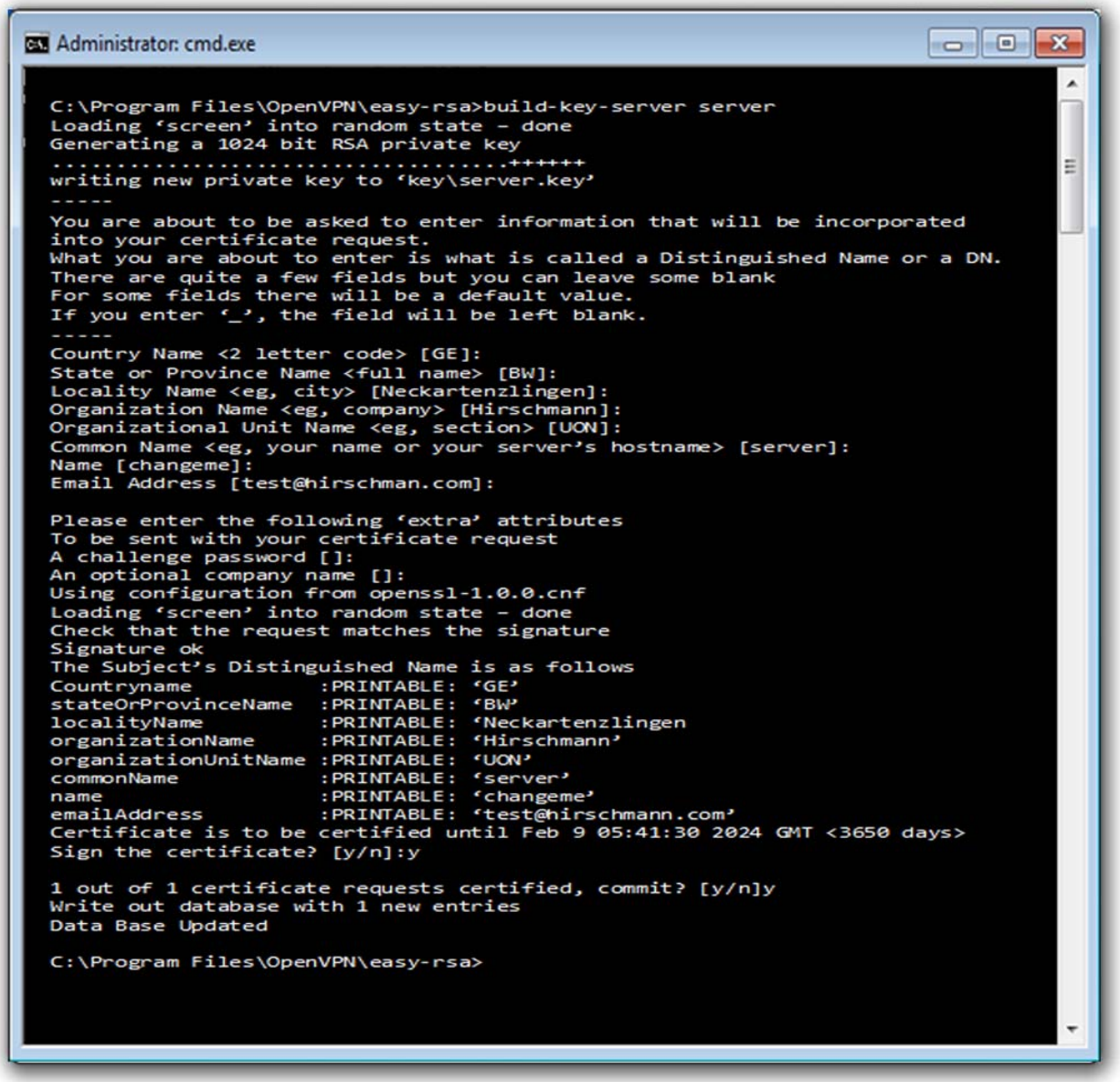


Figure 112:generating certificates and keys

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

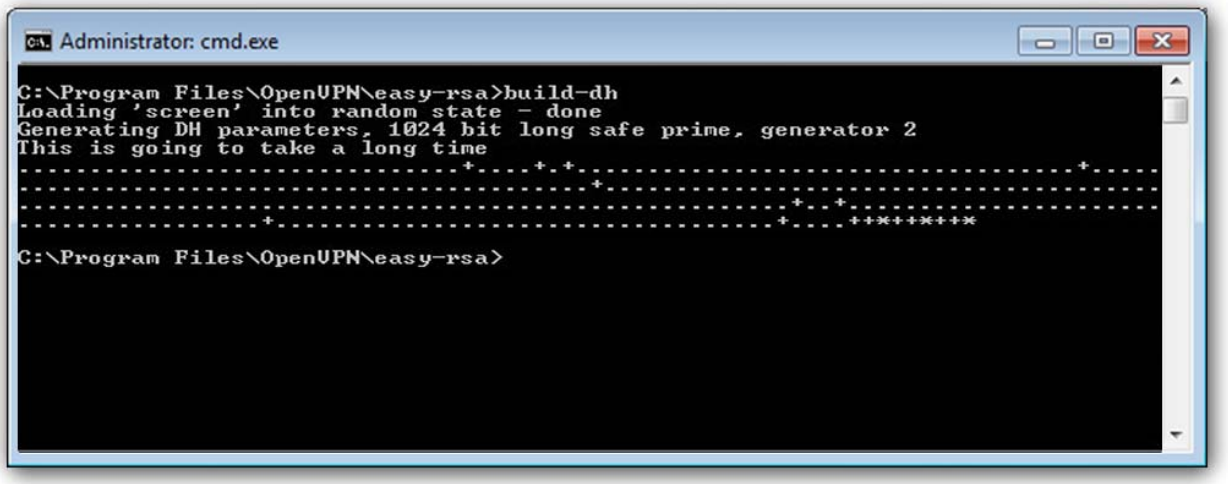


Figure 113:generating DH key

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 64: Overview of the generated files

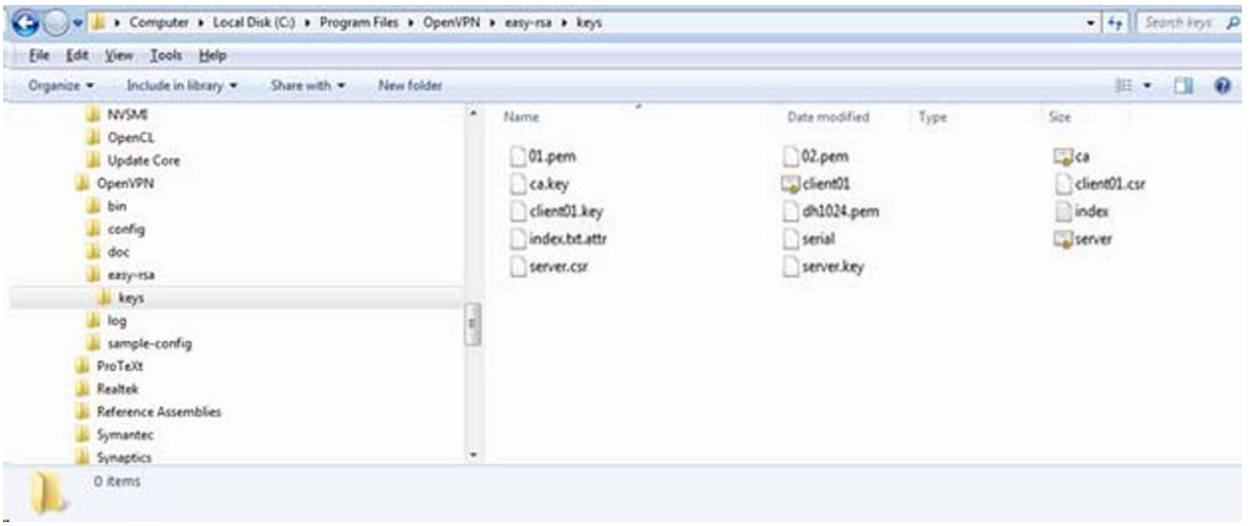


Figure 114:Overview of the generated files

2.10 Recommended literature

Hirschmann:Configuration manual for OWL routers

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 65: 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 66: 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 67: 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 68: 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 69: 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 181.)

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 183.)

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 70: 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 71: 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 72: 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 73: 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 74: 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 75: 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 76: 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 214.

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 77: 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 78: 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 79: 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 80: 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 81: 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 82: 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 83: 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 84: 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 85: 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 86: 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 87: 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 88: 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 89: 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 90: 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
```

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 v3 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 91: 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 92: 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 93: 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 94: 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 95: 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 96: 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 97: 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 v3 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 98: 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 99: 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 100: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 101: 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 102: 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 103: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 104: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 105: 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 106: 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 107: 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 108: 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 109: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 110: 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 111: 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 112: 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 113: 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 114: 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 115: 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 116: 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 117: 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 118: 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 ppp0.

```
tcpdump -n -i ppp0
```

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 119: 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 120: 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 121: 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 122: 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 123: 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 124: 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 SMNP 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 SMNP 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
```

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.

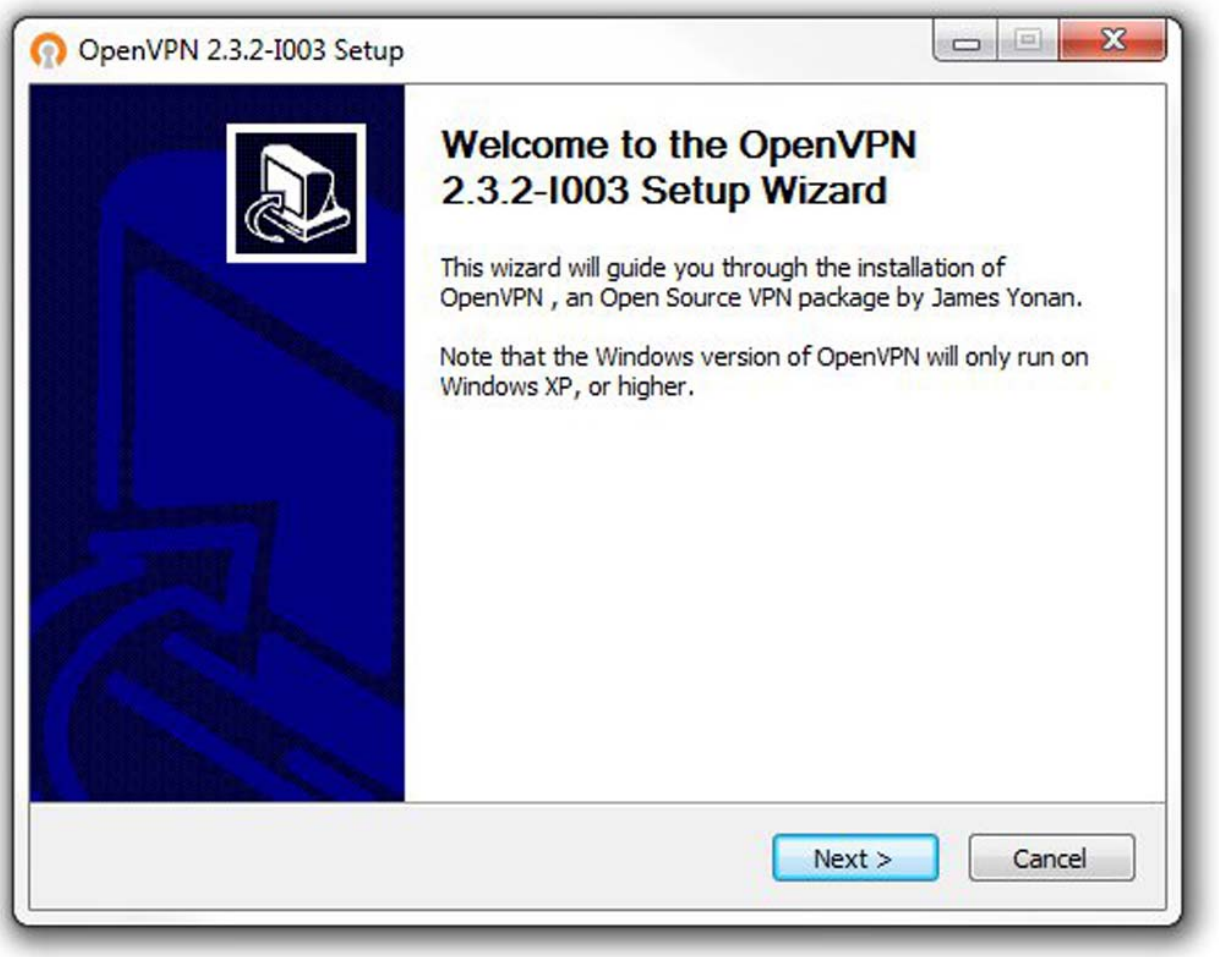


Figure 115:Installation of OpenVPN – basic information

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 116 on page 224.

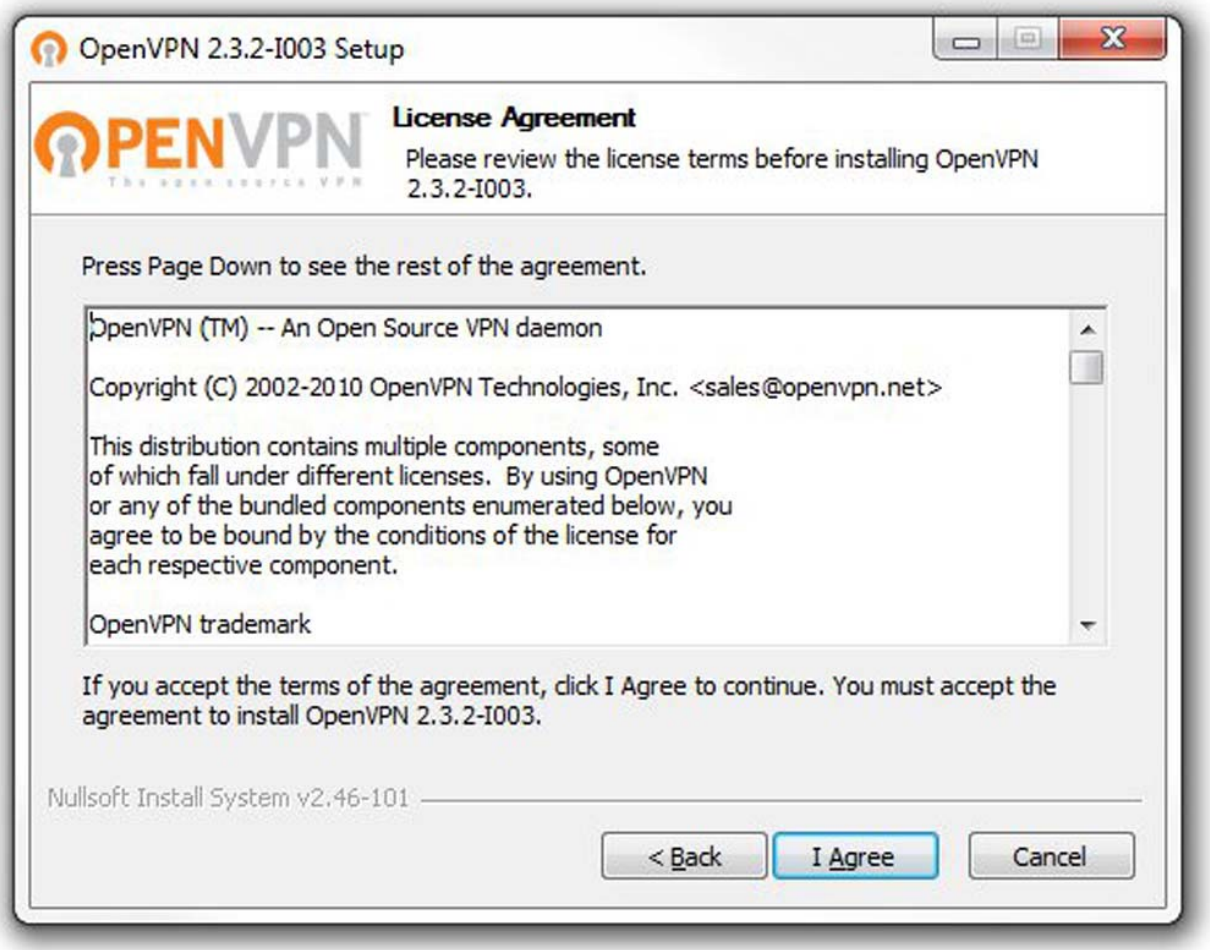


Figure 116:Installation of OpenVPN - license agreement

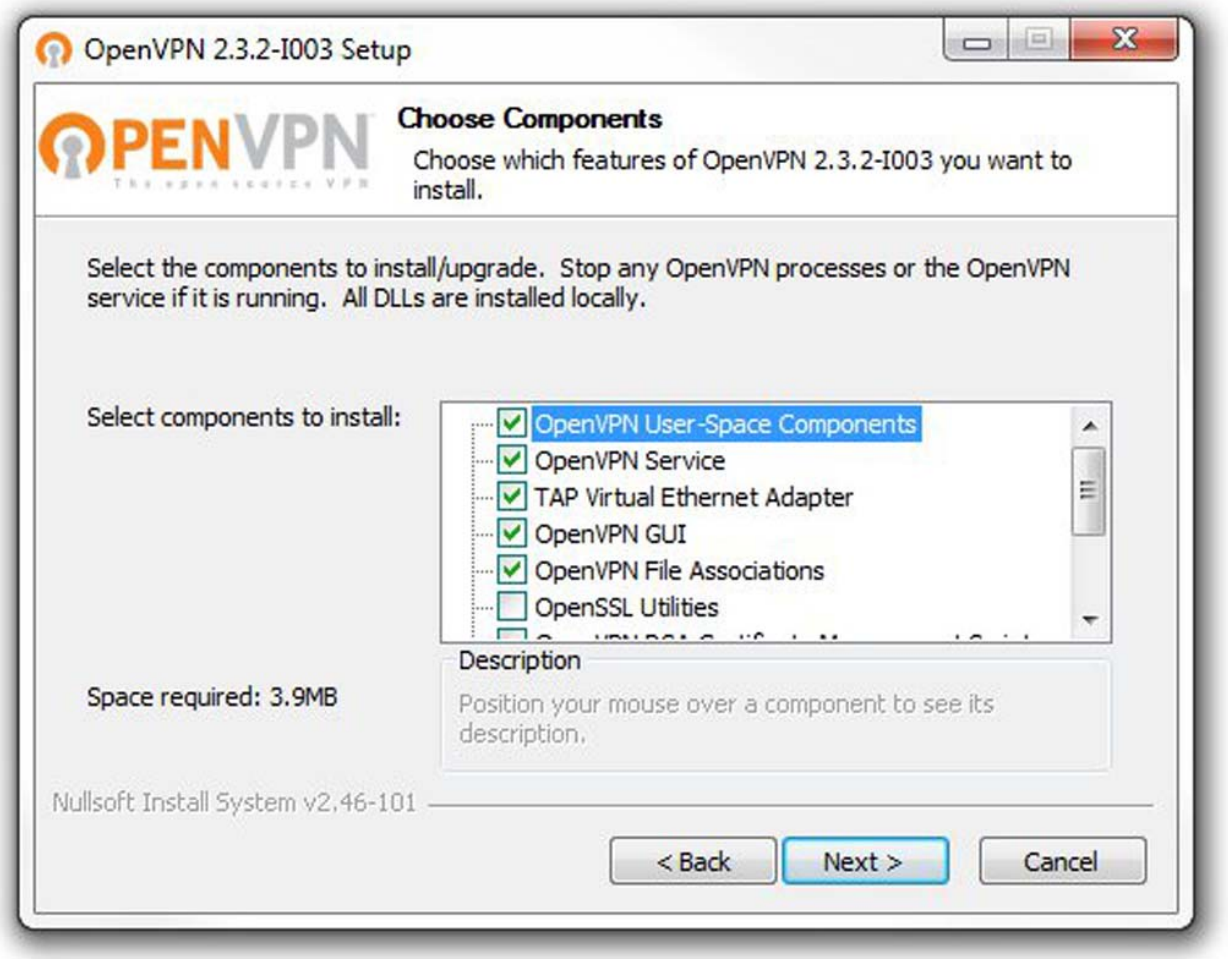


Figure 117:Installation of OpenVPN - components

The installation wizard, as seen in figure 118 on page 226, 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.

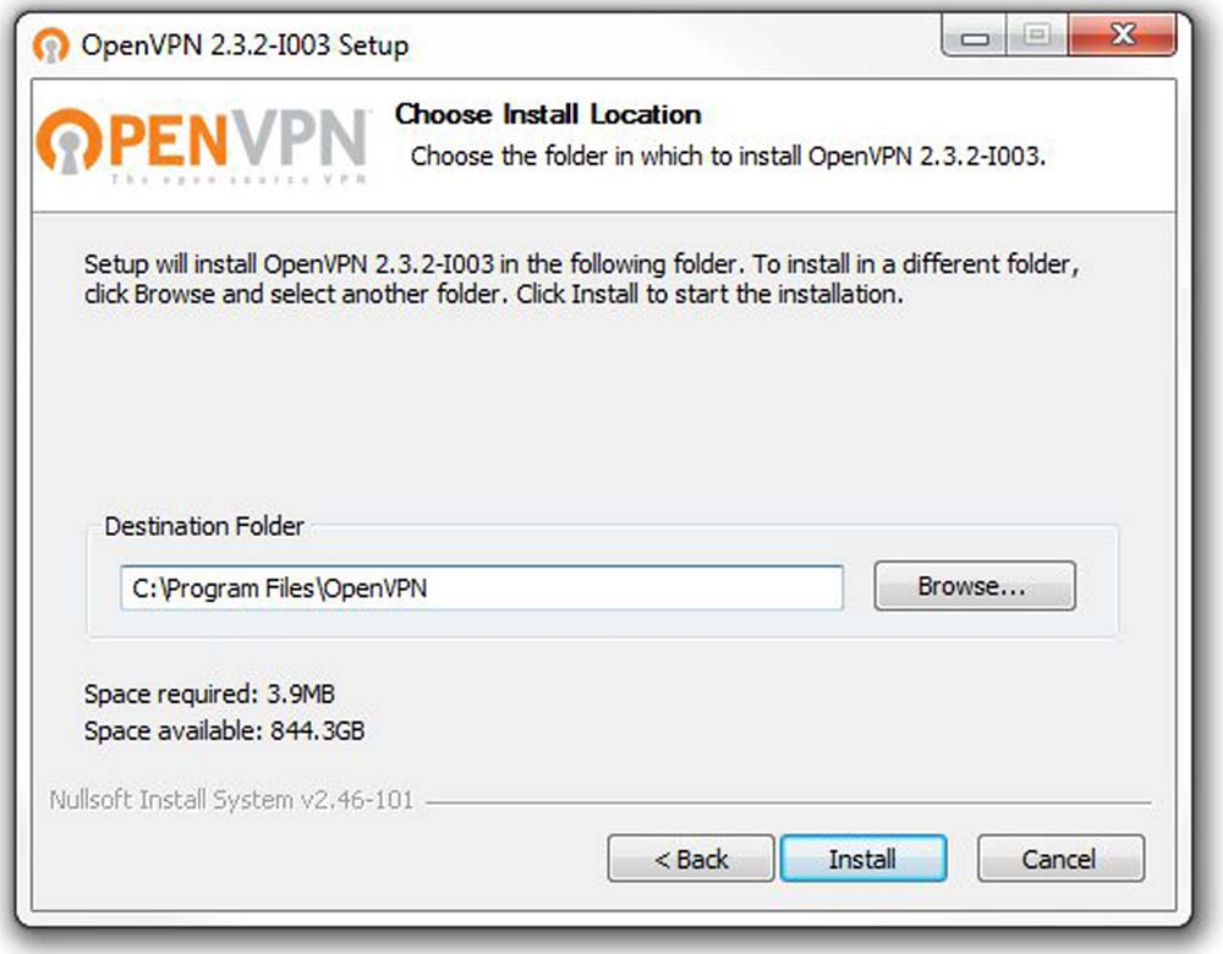


Figure 118:Installation of OpenVPN – location

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 “GUI Reference Manual”.

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).

B.4 Readers' Comments

What is your opinion of this manual? We are constantly striving to provide as comprehensive a description of our product as possible, as well as important information to assist you in the operation of this product. Your comments and suggestions help us to further improve the quality of our documentation.

Your assessment of this manual:

	Very Good	Good	Satisfactory	Mediocre	Poor
Precise description	O	O	O	O	O
Readability	O	O	O	O	O
Understandability	O	O	O	O	O
Examples	O	O	O	O	O
Structure	O	O	O	O	O
Comprehensive	O	O	O	O	O
Graphics	O	O	O	O	O
Drawings	O	O	O	O	O
Tables	O	O	O	O	O

Did you discover any errors in this manual?
If so, on what page?

Suggestions for improvement and additional information:

General comments:

Sender:

Company / Department:

Name / Telephone number:

Street:

Zip code / City:

E-mail:

Date / Signature:

Dear User,

Please fill out and return this page

- as a fax to the number +49 (0)7127/14-1600 or
- per mail to

  Hirschmann Automation and Control GmbH
  Department 01RD-NT
  Stuttgarter Str. 45-51
  72654 Neckartenzlingen

C Index

D Further 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 https://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

HIRSCHMANN

A BELDEN BRAND