

Industriefunkuhren



Technical Manual

NTP Time Client Module with two LAN Interfaces

Model 8030NTC

ENGLISH

Version: 02.01 - 14.11.2016

	SET	IMAGE (8030)	FIRMWARE (8030)
Valid for	Version: 02.xx	Version: 02.xx	Version: 02.xx

Version Numbers (Firmware / Description)

THE TERM **SET** DEFINES THE FIXED RELATIONSHIP BETWEEN THE IMAGE VERSION AND THE ASSOCIATED H8 FIRMWARE VERSION.

THE FIRST TWO DIGITS OF THE TECHNICAL DESCRIPTION VERSION NUMBER, THE **SET** VERSION AND THE IMAGE VERSION **MUST BE THE SAME!** THEY DESIGNATE THE SHARED FUNCTIONAL IDENTITY BETWEEN DEVICE, SOFTWARE AND TECHNICAL DESCRIPTION.

THE VERSION NUMBER OF THE IMAGE AND THE H8 SOFTWARE CAN BE READ IN THE WEBGUI OF THE TIME CLIENT 8030NTC (SEE **CHAPTER 6.3.6.1 DEVICE INFORMATION AND CHAPTER 6.3.6.2 HARDWARE INFORMATION**).

THE TWO DIGITS AFTER THE DOT IN THE VERSION NUMBER DESIGNATES CORRECTIONS TO THE FIRMWARE AND/OR DESCRIPTION WHICH HAVE NO EFFECT ON FUNCTIONALITY.

Downloading Technical Manuals

All current manuals of our products are available free of charge via our homepage on the Internet.

Homepage: <http://www.hopf.com>

E-mail: info@hopf.com

Symbols and Characters



Operational Reliability

Disregard may cause damages to persons or material.



Functionality

Disregard may impact function of system/device.



Information

Notes and Information.



Safety regulations

The safety regulations and observance of the technical data serve to ensure trouble-free operation of the device and protection of persons and material. It is therefore of utmost importance to observe and compliance with these regulations.

If these are not complied with, then no claims may be made under the terms of the warranty. No liability will be assumed for any ensuing damage.



Safety of the device

This device has been manufactured in accordance with the latest technological standards and approved safety regulations

The device should only be put into operation by trained and qualified staff. Care must be taken that all cable connections are laid and fixed in position correctly. The device should only be operated with the voltage supply indicated on the identification label.

The device should only be operated by qualified staff or employees who have received specific instruction.

If a device must be opened for repair, this should only be carried out by employees with appropriate qualifications or by **hopf** Elektronik GmbH.

Before a device is opened or a fuse is changed all power supplies must be disconnected.

If there are reasons to believe that the operational safety can no longer be guaranteed the device must be taken out of service and labelled accordingly.

The safety may be impaired when the device does not operate properly or if it is obviously damaged.

CE-Conformity



This device fulfils the requirements of the EU directive 2014/30/EU "Electromagnetic Compatibility" and 2014/35/EU "Low Voltage Equipment".

Therefore the device bears the CE identification marking
(CE = Communautés Européennes = European communities)

The CE indicates to the controlling bodies that the product complies with the requirements of the EU directive - especially with regard to protection of health and safety for the operator and the user - and may be released for sale within the common markets.

Contents	Page
1 NTP Time Client Module 8030NTC	7
2 Module Description.....	9
2.1 Installation Variants (Examples)	9
2.2 Installation and Removal of the Module	10
2.3 Functional Overview of the Front Panel Elements	10
2.3.1 Reset Button	10
2.3.2 Status LEDs (NTP/Stratum/Accuracy)	10
2.3.3 USB-Port	11
2.3.4 LAN Interface ETH0/ETH1	11
2.3.4.1 MAC-Address for ETH0/ETH1	11
3 Function Principle.....	12
4 Module Behaviour	13
4.1 Boot Phase.....	13
4.2 NTP Adjustment Process (NTP/Stratum/Accuracy)	13
4.3 Reset Button.....	13
4.4 Firmware Update	14
4.5 Activation of Functions by Activation Keys.....	16
5 Commissioning	17
5.1 General Procedure	17
5.2 Switching on the Operating Voltage.....	18
5.3 Establish the Network Connection via Web Browser	18
5.4 Network Configuration for ETH0 via LAN through <i>hmc</i>	18
6 HTTP WebGUI – Web Browser Configuration Interface	22
6.1 Quick Configuration	22
6.1.1 Requirements.....	22
6.1.2 Configuration Steps.....	22
6.2 General – Introduction	23
6.2.1 LOGIN and LOGOUT as User	24
6.2.2 Navigation via the Web Interface	25
6.2.3 Enter or Changing Data	26
6.3 Description of the Tabs.....	27
6.3.1 GENERAL Tab.....	27
6.3.2 TIME Tab	29
6.3.2.1 Time Zone Offset	29
6.3.2.2 Configuration of Summer Time (Daylight Saving Time)	30
6.3.3 NETWORK Tab.....	31
6.3.3.1 Host / Name Service	31
6.3.3.2 Network Interface ETH0/ETH1	32
6.3.3.3 Network Interface Bonding/Teaming (Activation Key necessary)	36
6.3.3.4 Network Interface PRP (Activation Key necessary)	40
6.3.3.5 Routing (Activation Key necessary)	43
6.3.3.6 Management (Management-Protocols – HTTP, SNMP, SNMP-Traps, etc.).....	44
6.3.3.7 Time (Time Protocols – NTP, DAYTIME etc.).....	47
6.3.4 NTP Tab	48
6.3.4.1 System Info.....	49
6.3.4.2 Kernel Info	50
6.3.4.3 Peers	50
6.3.4.4 Server Configuration	51

6.3.4.5	Extended Configuration	52
6.3.4.6	Restart NTP	55
6.3.4.7	Access Restrictions / Configuring the NTP Service Restrictions.....	55
6.3.4.8	Symmetric Key.....	60
6.3.4.9	Autokey / Public Key Cryptography	61
6.3.5	ALARM Tab.....	62
6.3.5.1	Syslog Configuration.....	62
6.3.5.2	E-mail Configuration	63
6.3.5.3	SNMP Configuration / TRAP Configuration	64
6.3.5.4	Alarm Messages	65
6.3.6	DEVICE Tab.....	66
6.3.6.1	Device Information	66
6.3.6.2	Hardware Information	66
6.3.6.3	Restoring Factory-Settings (Factory Defaults)	67
6.3.6.4	Reboot Device	67
6.3.6.5	Image Update & H8 Firmware Update	68
6.3.6.6	Customized Security Banner	69
6.3.6.7	Product Activation.....	70
6.3.6.8	Diagnostics Function	71
6.3.6.9	Passwords Master / Device	71
6.3.6.10	Downloading SNMP MIB / Configuration Files.....	72
6.3.7	OUTPUT Tab	73
6.3.7.1	PPS (Optional Hardware necessary)	73
6.3.7.2	DCF77 (Optional Hardware necessary).....	75
6.3.7.3	IRIG-B (Optional Hardware necessary)	77
6.3.7.4	Cyclic Pulse (Optional Hardware necessary).....	79
6.3.7.5	Serial Interface (Optional Hardware necessary)	82
7	SSH and Telnet Basic Configuration	98
8	Technical Data	99
9	Factory Defaults.....	101
9.1	Network	101
9.2	NTP.....	102
9.3	ALARM.....	102
9.4	DEVICE	102
10	Glossary and Abbreviations	103
10.1	NTP-specific Terminology.....	103
10.2	Tally Codes (NTP-specific)	103
10.2.1	Time-specific expressions.....	104
10.3	Abbreviations.....	105
10.4	Definitions	106
10.4.1	DHCP (Dynamic Host Configuration Protocol)	106
10.4.2	NTP (Network Time Protocol)	106
10.4.3	SNMP (Simple Network Management Protocol).....	107
10.4.4	TCP/IP (Transmission Control Protocol / Internet Protocol)	107
10.5	Accuracy & NTP Basic Principles	107
11	List of RFCs.....	109
12	List of Open Source Packages used	110

1 NTP Time Client Module 8030NTC

Module 8030NTC is a compact **Network Time Client** (*abbreviation* NTC) for the integration into Clock Systems or rather Signal Converters.

For the network connection the module is equipped with two Ethernet interface (ETH0/ETH1) 10/100/1000 Base-T (autosensing).

The Time Client Module 8030NTC is synchronized with the **UTC time** by the worldwide used time **NTP (Network Time Protocol)** via one or more NTP Time Servers.

The module can either be synchronized by a **NTP Timer Server** but also by a **SNTP Time Server**, if needed. However, this usually results in a considerably limited accuracy of the time information.

The time basis of the module synchronized via NTP is converted into a format that allows the synchronization of further **hopf** devices and components.

For the operation of Module 8030NTC it is required to supply it with power and a network connection. The power supply is usually carried out via the device/system the module is integrated in. The output of the synchronized time information is performed at the module internal outputs.

The respective **total status** of the module is indicated via three LEDs in the front panel. This allows an easy identification of the current operation status or any fault.

Due to its compact size, the NTP Time Client Module 8030NTC is easy to integrate and characterized by its easy and simple operation, although it offers a **broad range of functions**. Some of the practice-oriented functionalities are for example:

- **Complete parameterisation via protected WebGUI access**
All required settings for operation can be executed via a password protected WebGUI also giving an overview of the status of the module 8030NTC.
- **Automatic handling of the leap second**
Should a leap second in the UTC time be announced by the Time Server, this is recognized by the Time Client Module 8030NTC and the leap second automatically inserted into the time information.
- **Superior Security**
A superior security is guaranteed via available coding procedures such as symmetric keys, autokey and access restrictions and deactivation of non-used protocols.
- **Management and Monitoring Functions**
Different functions are available for this purpose (e.g. SNMP, SNMP-Traps, E-mail notification, Syslog-messages including MIB II and private Enterprise MIB).

A few other basic functions of the Time Client Module 8030NTC:

- Easy operation via **WebGUI**
- **NTP Status LEDs** on the front panel
- Completely **maintenance-free** system

Software supplied:

- **hmc (hopf Management Console)** Software

Overview of the functions of the network Time Client Module 8030NTC:

Two Ethernet Interfaces

- Auto negotiate
- 10 Mbps half-/full duplex
- 100 Mbps half-/full duplex
- 1 Gbps full duplex

Time Protocols

- RFC-5905 NTPv4 Server
 - NTP Broadcast Mode
 - NTP Multicast Mode
 - NTP Client for additional NTP Servers (redundancy)
 - SNTP Server
 - NTP Symmetric Key Encryption
 - NTP Autokey Encryption
 - NTP Access Restrictions
- SINEC H1 time datagram (**Activation Key necessary**)
- RFC-867 DAYTIME Server
- RFC-868 TIME Server

Network Configuration (Activation Key necessary)

- Routing
- Bonding (NIC Teaming) Link aggregation according to IEEE 802.1ad
- VLAN support according to IEEE 802.1q
- PRP (Parallel Redundancy Protocol) according to IEC62439-3

System Management (Activation Key necessary)

- E-mail notification
- Syslog messages to external syslog server
- SNMPv2c/v3, SNMP Traps (MIB II, Private Enterprise MIB)

Configuration Channel

- HTTP WebGUI (browser-based)
- Telnet
- SSH
- External LAN configuration tool (**hmc** - Network-Configuration-Assistant)

Additionally Features

- Firmware Update via TCP/IP
- Failsafe
- Watchdog circuit
- Customizable security banner
- NTP local time support

2 Module Description

The NTP Time Client Module 8030NTC is a complete multi-processor embedded-linux system.

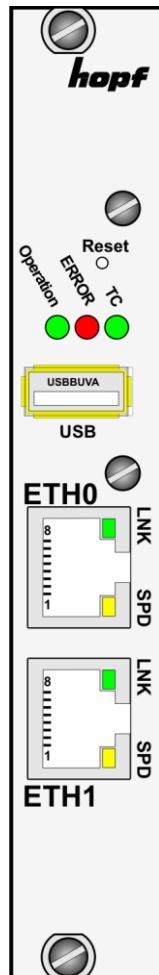
Usually the module is integrated as a NTP Time Client extension in **hopf** clock systems and converters at the factory.

The module is supplied with power via an internal plug-in connector. The output of the synchronized time information based on NTP also takes place via this connector.

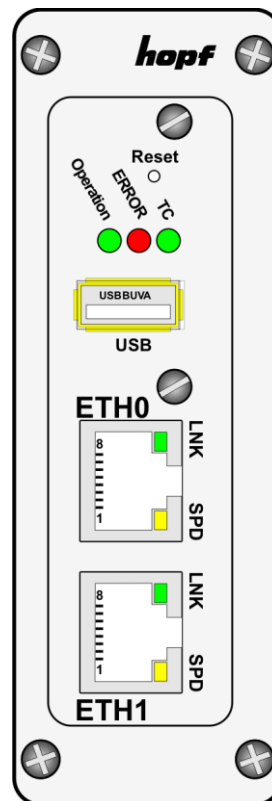
2.1 Installation Variants (Examples)

The module can be equipped with panels for the integration in different housings and system variants.

**Module 8030NTC
for the integration
in 19" systems
with 3U/4HP panels**



**Module 8030NTC
with front panel
for the integration in
DIN Rail housings (example)**



2.2 Installation and Removal of the Module

The module is supplied with power via an internal plug-in connection that also provides the output of the time information based on NTP and the system reset if any.

For service and repair purposes the module can be removed from the device.



The module does not support HOT-PLUG

In case an installation or removal of the module should be necessary the device in which the module is integrated in must be disconnected from power.

2.3 Functional Overview of the Front Panel Elements

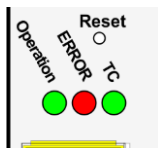
This chapter describes the individual front panel elements and their functions.

2.3.1 Reset Button



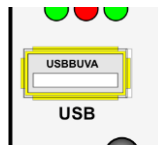
The Reset Button is accessible with a thin objective through the small drilling in the front panel next to the "Reset" inscription" (see **Chapter 4.3 Reset Button**).

2.3.2 Status LEDs (NTP/Stratum/Accuracy)



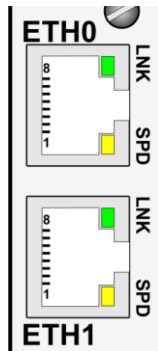
TS-LED (Green)	Time service of the Time Server 8030NTC
On	Standard , running
Off	Not or partially not running
ERROR-LED (Red)	Description
Off	Standard case , module 8030NTC is working.
3Hz flashing	Fail-safe basic parameterization is not available (emergency operation mode)
On	Primary CPU of module 8030NTC does not show any activity.
Operation-LED (Green)	Description
On	Standard case , module 8030NTC is working
1Hz flashing	Module 8030NTC is booting the operating system.
3Hz flashing	A firmware update (image) of module 8030NTC is being implemented.
Off	Module 8030NTC is not ready for operation.

2.3.3 USB-Port



On specific problems the USB connection can be used for a system recovery after consulting the **hopf** Support.

2.3.4 LAN Interface ETH0/ETH1



LNK LED (Green)	Description
Off	10 MBit Ethernet detected
On	100 MBit / 1 GBit Ethernet detected

SPD LED (Yellow)	Description
Off	No LAN connection to a network
On	LAN connection available
Flashes	Network activity (transmission / reception)

Pin No.	Assignment
1	TX_DA+
2	TX_DA-
3	RX_DB+
4	BI_DC+
5	BI_DC-
6	RX_DB-
7	BI_DD+
8	BI_DD-

2.3.4.1 MAC-Address for ETH0/ETH1

Each LAN interface is clearly identifiable on the Ethernet via a unique MAC Address (hardware address).

The MAC addresses given for the LAN interfaces can be read in the WebGUI of the appropriate board or be evaluated via the **hmc Network Configuration Assistant**.

The MAC address for ETH1 is incremented hexadecimal by 1 to the MAC address of ETH0.

Example:

- MAC address ETH0 = 00:03:C7:12:34:59
- MAC address ETH1 = 00:03:C7:12:34:5A

The MAC address is uniquely assigned for each LAN interface by the company **hopf** Elektronik GmbH.



The factory set MAC address for the Time Client 8030NTC is stated on a sticker directly placed on the module.



hopf Elektronik GmbH MAC addresses begin with **00:03:C7:xx:xx:xx**.

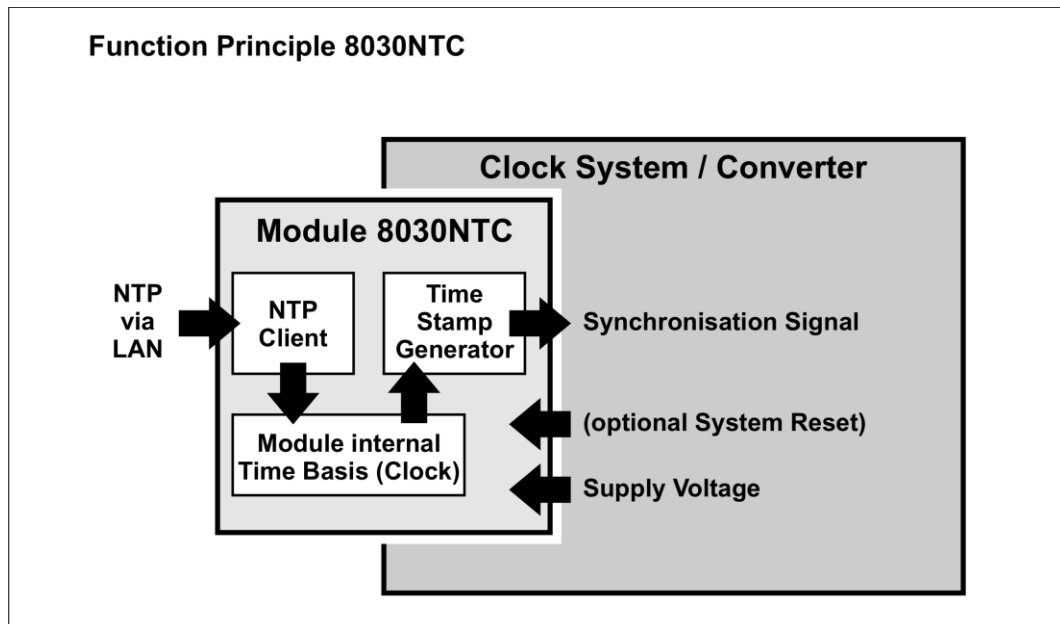
3 Function Principle

This chapter describes the functional principle of the Time Client Module 8030NTC and the internal relations between the individual function groups.

The Time Client Module 8030NTC is a multi-processor system.

The structure allows the following mode of operation:

The NTP service on the module is synchronized by a NTP Server via the network. With this time information the internal time basis of the module is synchronized with high precision. The time is then transformed into outputs with time information allowing further processing in the respective clock system.



4 Module Behaviour

This chapter describes the behaviour of the module in special operational phases and conditions.

4.1 Boot Phase

The boot process of the Time Client 8030NTC starts after turning on the system or a reset.

During the boot process the Module 8030NTC boots its LINUX operation system and is therefore not available via LAN.

The end of the boot process is reached when the LED test of the Status-LEDs in the front panel has been finished.



Boot phase takes approx. 35 seconds by using static IP-addresses for ETH0 and ETH1. Boot phase can be extended, depending on the network configuration in use (e.g. DHCP).

4.2 NTP Adjustment Process (NTP/Stratum/Accuracy)

NTP is a regulation process. After start of the NTP services, automatically processed during booting, the Time Client 8030NTC requires approximately 5-10 minutes depending on the accuracy and accessibility of the NTP Server parameterized in the module.

After a successful adoption of time by the NTP Server the module usually takes on a Stratum value one less than the respective NTP Server (e.g. Server = Stratum 1 \Rightarrow Stratum of the Client Module = 2).

For an output of time via the module, the NTP service needs to be regulated to an accuracy value = HIGH. The duration of the regulation process depends on factors such as accessibility and accuracy of the respective NTP Server (System Peer).

4.3 Reset Button

The Time Client 8030NTC can be reset by the Reset-(Default) Button behind the front panel of the board. The Reset-(Default) Button is accessible with a thin objective through the small drilling in the front panel.

The button triggers different functions depending on how long it is pressed:

Duration	Function
< 1 sec.	No action
1 - 9 sec.	After releasing a hardware reset is triggered in the module
10 - 19 sec.	After releasing a CUSTOM DEFAULT followed by a REBOOT is triggered after approx. 10 seconds.
≥ 20 sec.	After releasing a FACTORY DEFAULT followed by a REBOOT is triggered after approx. 10 seconds



If the user saves **no** CUSTOM DEFAULT via the WebGUI, a FACTORY DEFAULT is triggered instead.

4.4 Firmware Update

The Time Client 8030NTC is a multi-processor system. For this reason a firmware update always consists of a so called Software SET including two (2) program releases defined by the SET version needed to be loaded into the board.

Module 8030NTC:

1x Image Update	upgrade_8030gen_rel_vXXXX.img
1x H8 Update	H8_8030NTC_vXXXX_128.mot



An update is a critical process.
The device must not be turned off during the update and the network connection to the device not be interrupted.



All programs of a SET needed to be uploaded to ensure a defined operation condition.



The program releases assigned to a SET version may be taken from the release notes of the software SETs of the Time Client 8030NTC.

The general process of a software update of Module 8030NTC is described below:



For selection of the correct update set the identifier **8030NTC** has to be observed obligatory.

8030NTC can be recognized:

- By the label on the housing cover "**8030NTC**"
- In WebGUI at the Web-banner "**8030NTC**"

The firmware update 8030NTC has to be performed as a SET.

The software package contained in the file package hopf8030NTC_GPS_SET_vXXXX.zip has to be unpacked. The following steps have to be executed in the following sequence:

1. **Image Update 8030NTC**
2. **H8 Firmware Update 8030NTC**

Image Update

1. Log in as Master in WebGUI of the board.
2. Select in **Device** tab the menu item **Image Update**.
3. Select the file with the file **.img** via the selection window (Exapmle: **upgrade_8030gen_rel_vXXXX.img**).
4. The selected file is shown in the selection window.
5. The update process is started with the button **Upload now**.
6. In WebGUI the successful file transfer and writing to the Module is indicated.
7. In WebGUI the successful update is indicated after 2-3 minutes with the request to release a reboot of the board.
8. After activation and successful reboot of the board the image update process is finished.

H8 Firmware Update

1. Log in as Master in WebGUI of the board.
2. Select in the **Device** tab the menu item **H8 Firmware Update**.
3. Select the file with the file extension **.mot for Module 8030NTC** via the selection window (Example: **H8_8030NTC_vXXXX_128.mot**).
4. The selected file is shown in the selection window.
5. The update process is started with the button **Upload now**.
6. In WebGUI the successful file transfer to the Module is indicated.
7. Now the update of the board automatically starts after a few seconds.
8. After successful update the board automatically reboots.
9. After approx. 2 minutes the H8 update process is finished and the board is again accessible via WebGUI.

4.5 Activation of Functions by Activation Keys

Currently the Time Client 8030NTC offers three functions that require an "Activation Key".

These functions are only available after entering a valid activation key related to the serial number of the Module 8030NTC (not the serial number of the overall system). The serial number can be found in the WebGUI via Device / Serial Number: 8030xxxxxx.

The activation of such function(s) can be done by default and also later by the user if required.



The input and display is done in the tab "Device" under the menu item "Product Activation".

Please find an overview of the above mentioned functions here:

- **Network interface Bonding/Teaming**
By activating this function the LAN interfaces ETH0 and ETH1 can be bundled to a logical network interface. This feature plays a key role in redundantly structured networks to increase fail-safety of the NTP time service.
- **Virtual LAN (VLAN)**
By activating this function network interfaces can be configured with additional VLANs (Virtual Bridged Local Area Networks) according to IEEE 802.1q.
- **Routing**
This function is suitable for configuring static routes based on special network configuration requirements in the Time Client 8030NTC.
- **PRP (Parallel Redundancy Protocol)**
The PRP functionality enables to bundle the physical network interfaces ETH0 and ETH1 to one logical network interface using the Parallel Redundancy Protocol (PRP).
- **Alarming**
This function enables to use **SNMP (SNMPv2c, SNMPv3), Syslog and Email notification** to monitor the system status. Together with the assets provided in the MIB II by default, the **hopf** Private Enterprise MIB is also made available. By using the **hopf** Private Enterprise MIB numerous product-specific assets for realizing extended management and control functions are available.
- **SINEC H1 time datagram**
By activating this function SINEC H1 time datagram can be parameterized and issued via the LAN interface.



The settings for activation keys (e.g. an entered activation key) are neither modified nor influenced by the functions FACTORY DEFAULTS and CUSTOM DEFAULTS.

5 Commissioning

This chapter describes commissioning of the Time Client 8030NTC.

5.1 General Procedure

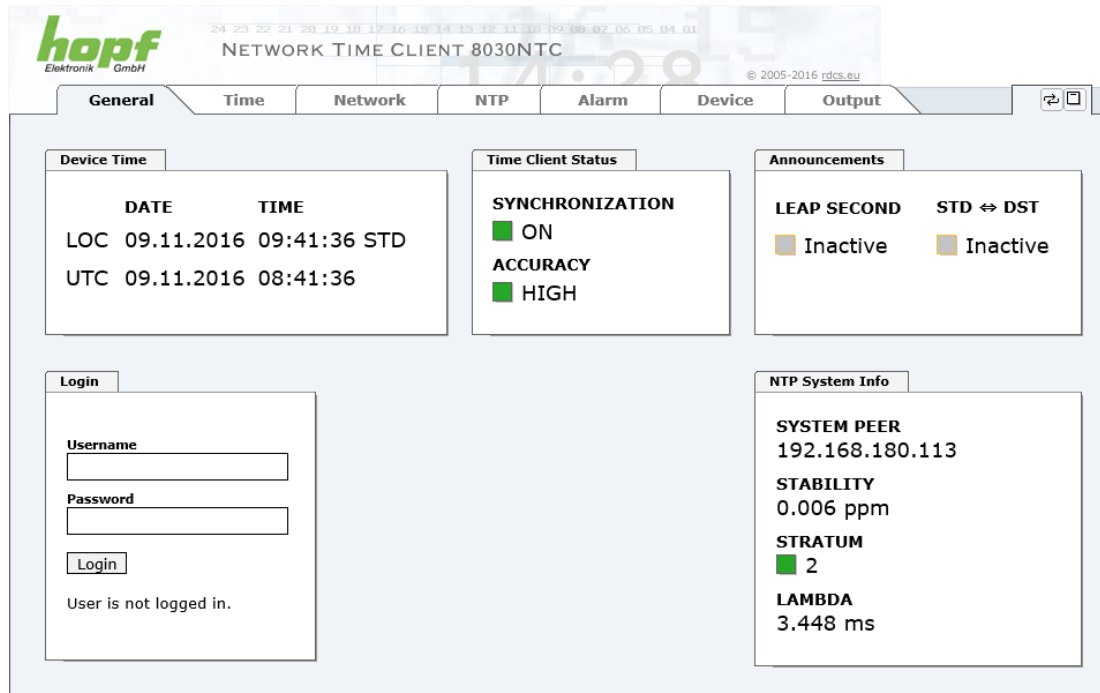
Overview of the general commissioning procedure:

- Finish the installation process completely
- Switch on the device
- Wait until the booting phase is finished (see **chapter 4.1 Boot Phase**)
- Using the SEARCH Function of the **hmc** Software (Network Configuration Assistant) in order to access the Time Client 8030NTC and set the basis LAN parameters (e.g. DHCP). Afterwards connect to the WebGUI of the Time Client 8030NTC via Web browser

OR

connect directly with the factory default IP-address (192.168.0.1) to the WebGUI via a Web browser

- Log in as "**master**"
- Change default passwords for "**master**" and "**device**" In the **DEVICE** tab
- Set all required LAN parameters (e.g. entry of DNS server) in **NETWORK** tab if necessary
- Check current settings in **NTP** tab and modify according to individual needs as necessary (e.g. entry of the NTP Time Server used for synchronization)
- Parameterize optional functions e.g. SNMP if necessary
- If all base settings are carried out correctly and the set NTP Time Server supplies the time information with the appropriate accuracy, the **GENERAL** tab should look like this after approx. 30 min. (usually considerably faster):



The screenshot shows the WebGUI of the hopf NETWORK TIME CLIENT 8030NTC. The interface has a top navigation bar with tabs: General, Time, Network, NTP, Alarm, Device, and Output. The 'General' tab is selected. Below the navigation bar, there are several sections:

- Device Time**: A table showing local and UTC times.

	DATE	TIME
LOC	09.11.2016	09:41:36 STD
UTC	09.11.2016	08:41:36
- Time Client Status**: Shows synchronization and accuracy status.

SYNCHRONIZATION	<input checked="" type="checkbox"/> ON
ACCURACY	<input checked="" type="checkbox"/> HIGH
- Announcements**: Shows leap second and DST status.

LEAP SECOND	STD ↔ DST
<input type="checkbox"/> Inactive	<input type="checkbox"/> Inactive
- Login**: A form with fields for Username and Password, a Login button, and a message 'User is not logged in.'.
- NTP System Info**: Shows system parameters.

SYSTEM PEER	192.168.180.113
STABILITY	0.006 ppm
STRATUM	<input checked="" type="checkbox"/> 2
LAMBDA	3.448 ms

5.2 Switching on the Operating Voltage

The Time Client 8030NTC has no own switch for the power supply. The Time Client 8030NTC is activated by switching on the device in which it is integrated in.

5.3 Establish the Network Connection via Web Browser



Ensure that the network parameters of the Time Client 8030NTC are configured in accordance with the local network before connecting the device to the network.



Connecting a network to an incorrectly configured Time Client 8030NTC (e.g. duplicate IP address) may cause interference on the network.



The Time Server 8030NTC is supplied with:

ETH0 with static IP-address

IP-address: 192.168.0.1
Network mask: 255.255.255.0
Gateway: not set

ETH1 with DHCP



In case it is not known whether the Time Client 8030NTC with a Factory Default setting causes problems in the network, the basis network parameterization should be executed via a "Peer to Peer" network connection.



Request the required network parameters from your network administrator if those are unknown.

The network connection is made via a LAN cable and RJ45 plug (recommended cable type: CAT5 or better).

5.4 Network Configuration for ETH0 via LAN through *hmc*

After connecting the system to the power supply and creating the physical network connection to LAN interface of the Time Client 8030NTC, the device can be searched for on the network via the ***hmc*** (***hopf*** Management Console). Then the base LAN parameters (IP address, netmask and gateway or DHCP) may be adjusted in order to allow accessibility of the Time Client 8030NTC for other systems on the network.



The SEARCH Function of the ***hmc*** - Network Configuration Assistant requires for location and recognition of the wished Time Client 8030NTC that both the ***hmc***-computer and Time Client 8030NTC are in the same SUB Net.

The base LAN parameters can be set via the **hmc** integrated **Network Configuration Assistant**.



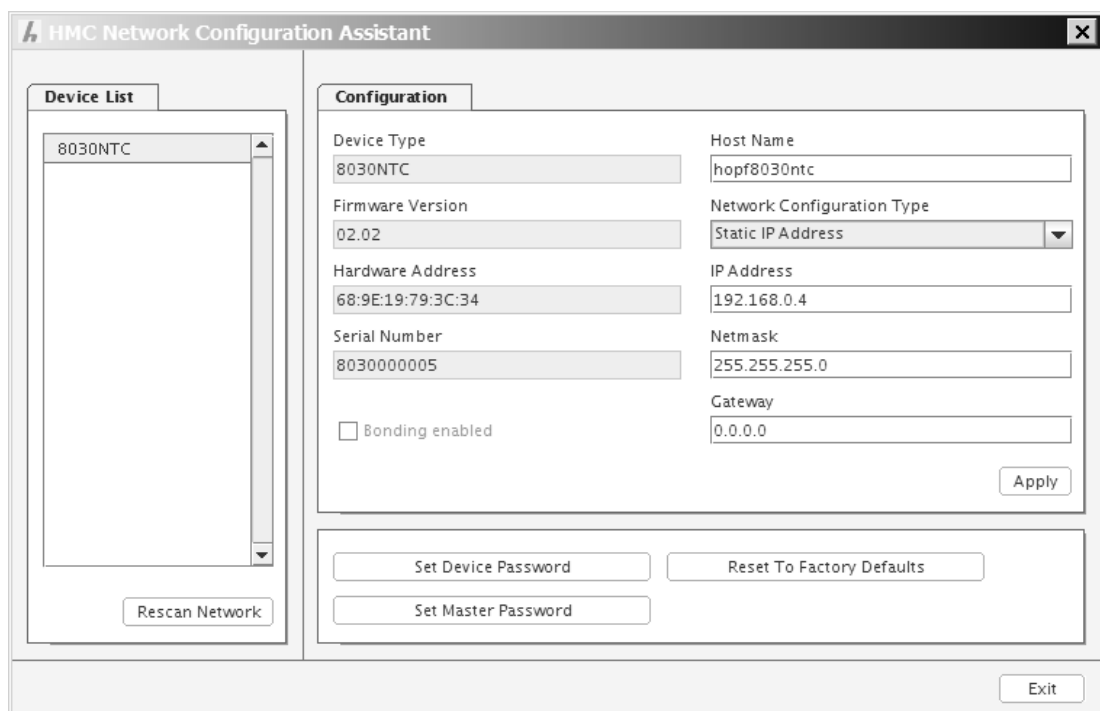
After a successful start of the **hmc Network Configuration Assistant** and completed search of the **hopf** LAN devices, the configuration of the base LAN parameters can be done.

The Time Client 8030NTC is stated as **8030NTC** in the Device List.

The determination of different Time Clients 8030NTC (or other products variants) is made via **Hardware Address** (MAC Address).



The factory set MAC address for the Time Client 8030NTC is stated on a sticker laterally positioned on the exterior of the housing of the device.



For an extended configuration of the Time Client 8030NTC through a browser via WebGUI the following base parameters are required:

- **Host Name** ⇒ e.g. hopf8030ntc
- **Network Configuration Type** ⇒ e.g. Static IP Address or DHCP
- **IP Address** ⇒ e.g. 192.168.0.4
- **Netmask** ⇒ e.g. 255.255.255.0
- **Gateway** ⇒ e.g. 0.0.0.0



The **hostname** must meet the following conditions:

- The hostname may only contain the characters 'A'-'Z', '0'-'9', '-' and '.'. There should be no distinction between upper-and lower-case letters.
- The character '.' may only appear as a separator between labels in domain names.
- The sign '-' must not appear as first or last character of a label.



The network parameters being assigned should be pre-determined with the network administrator in order to avoid problems on the network (e.g. duplicate IP address).

IP Address (IPv4)

An IP address is a 32 bit value divided into four 8 bit numbers. The standard presentation is 4 decimal numbers (in the range 0...255) separated from each other by dots (dotted quad notation).

Example: 192.002.001.123

The IP address consists of a leading network ID followed by the host ID. Four common network classes were defined in order to cover different requirements. Depending on the network class, the last one, two or three bytes define the host while the rest define the network (network ID) in each case.

In the following text the "x" stands for the host part of the IP address.

Class A Networks

IP addresses 001.xxx.xxx.xxx to 127.xxx.xxx.xxx

There is a maximum of 127 different networks in this class. This allows the possibility to connect a very high number of devices (max. 16.777.216)

Example: 100.000.000.001, (Network 100, Host 000.000.001)

Class B Networks

IP addresses 128.000.xxx.xxx to 191.255.xxx.xxx

Each of these networks can consist of up to 65534 devices.

Example: 172.001.003.002 (Network 172.001, Host 003.002)

Class C Networks

IP addresses 192.000.000.xx to 223.255.255.xxx

These network addresses are the most commonly used. Up to 254 devices can be connected.

Class D Networks

The addresses from 224.xxx.xxx.xxx - 239.xxx.xxx.xxx are used as multicast addresses.

Class E Networks

The addresses from 240.xxx.xxx.xxx - 254.xxx.xxx.xxx are designated as "Class E" and are reserved.

Gateway Address

The gateway or router address is required in order to be able to communicate with other network segments. The standard gateway must be set to the router address which connects these segments. This address must be within the local network.

After entering the above mentioned LAN parameters, they needed to be transferred to the Time Client 8030NTC via the **Apply** button. Afterwards the entry of the **Device Password** is requested:



The Time Client 8030NTC is supplied with the default device password **<device>** on delivery. After entry click on the **OK** button to confirm.

The LAN parameters thus set are directly adopted (without reboot) by the Time Client 8030NTC and are immediately active.

6 HTTP WebGUI – Web Browser Configuration Interface



For the correct display and function of the WebGUI, JavaScript and Cookies must be enabled in the browser.

6.1 Quick Configuration

This chapter gives a brief description of the basic operation of the WebGUI installed on the module.

6.1.1 Requirements

- Ready-for-operation **hopf** NTP Time Client 8030NTC
- PC with installed web browser (e.g. Internet Explorer) in the sub-network of Time Client 8030NTC

6.1.2 Configuration Steps

- Create the connection to the Time Client with a web browser
- Login as a '**master**' user (default password <**master**> is set by delivery)
- Switch to "Network" tab if available and enter the DNS Server (required for NTP and the alarm messages depending of network)
- Save the configuration
- Switch to "Device" tab and restart Network Time Client via "Reboot Device"
- NTP Service is now available with the standard settings
- NTP specified settings can be done in the "NTP" tab (e.g. entry of the NTP Time Server used for synchronization).
- Alarm messages via Syslog/SNMP/Email can be configured in "Alarm" tab – only if this function is enabled by an activation key



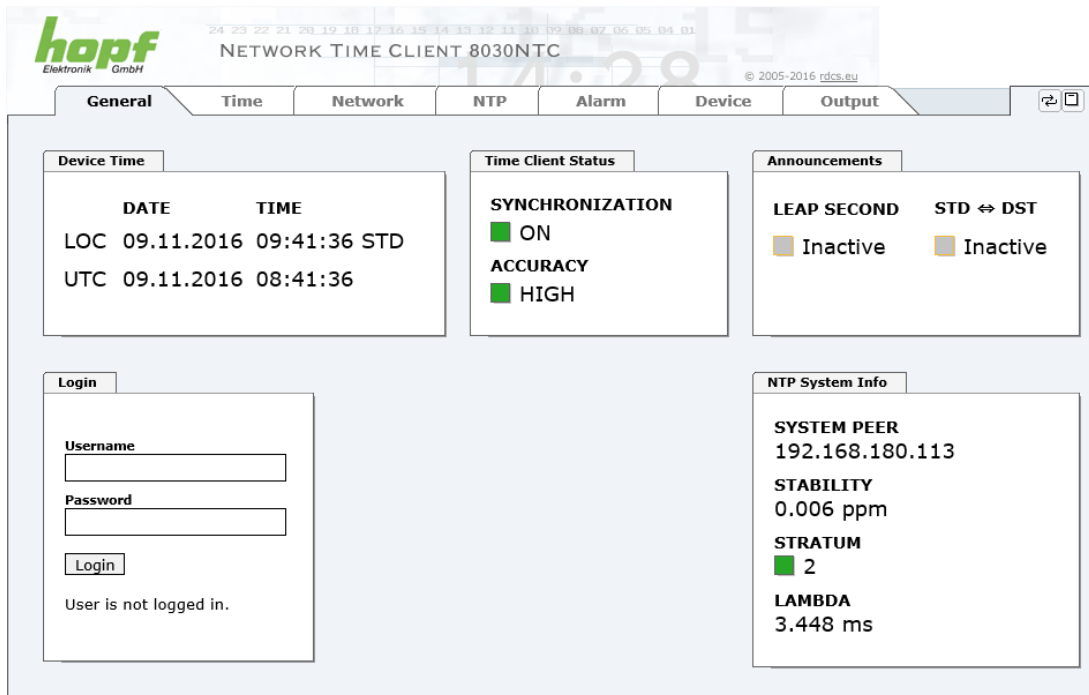
The following detailed explanatory information should be read if anything is unclear while executing the configuration steps.

6.2 General – Introduction

The Time Client 8030NTC should be accessible to a web browser if it has been set up correctly. Enter the IP address - as set up in the Time Client 8030NTC earlier - or the DNS name on the address line <<http://xxx.xxx.xxx.xxx>> and the following screen should appear.



The complete configuration can only be completed via the modules WebGUI!



The screenshot shows the WebGUI interface for the hopf NETWORK TIME CLIENT 8030NTC. The interface has a top navigation bar with tabs: General, Time, Network, NTP, Alarm, Device, and Output. The 'General' tab is selected. Below the navigation bar, there are several sections:

- Device Time:** A table showing the current date and time for both Local (LOC) and Universal Time (UTC).

	DATE	TIME
LOC	09.11.2016	09:41:36 STD
UTC	09.11.2016	08:41:36
- Time Client Status:** Shows synchronization and accuracy status.
 - SYNCHRONIZATION: ☒ ON
 - ACCURACY: ☒ HIGH
- Announcements:** Shows leap second and DST status.
 - LEAP SECOND: ☐ Inactive
 - STD ⇌ DST: ☐ Inactive
- Login:** A form with fields for Username and Password, and a Login button. Below the button, it says "User is not logged in."
- NTP System Info:** Shows system parameters.
 - SYSTEM PEER: 192.168.180.113
 - STABILITY: 0.006 ppm
 - STRATUM: ☒ 2
 - LAMBDA: 3.448 ms



The WebGUI was developed for multi-user read access but not for multi-user write access. It is the responsibility of the user to pay attention to this issue.

6.2.1 LOGIN and LOGOUT as User

All of the modules data can be read without being logged on as a special user. However, the configuration and modification of settings and data can only be carried out by an authorised user! Two types of user are defined:

- "master" user (default password on delivery: <master>)
- "device" user (default password on delivery: <device>)

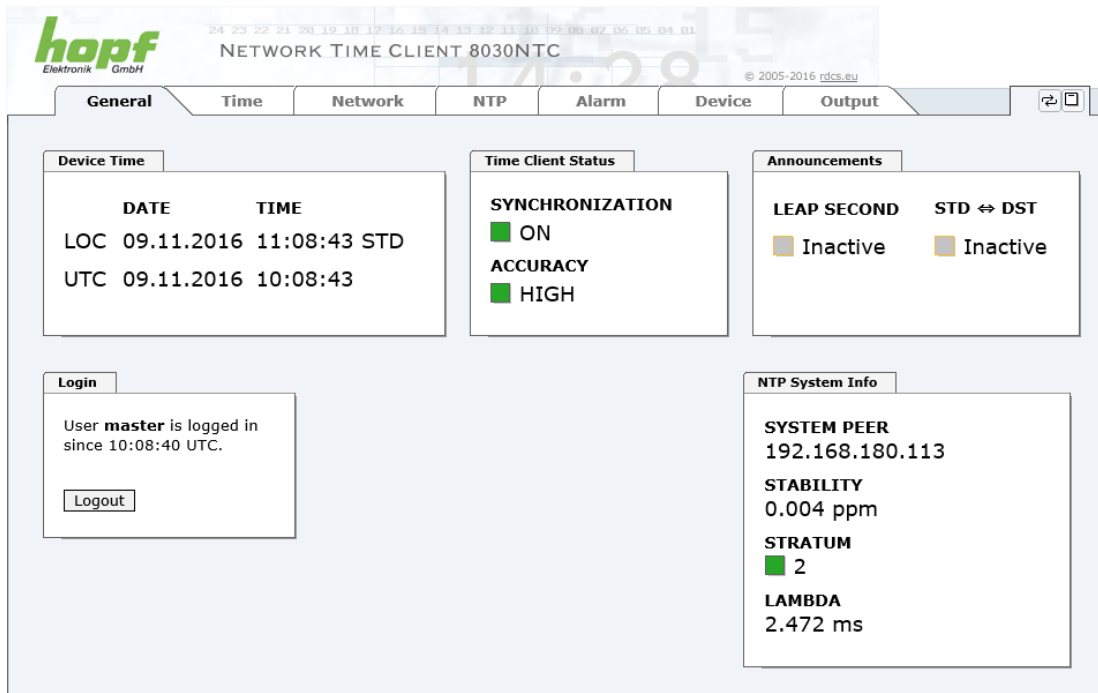


Differentiation is made between **upper and lower case** characters in the password. Alphanumeric characters and the following symbols can be used: [] () * - _ ! \$ % & / = ?



The password should be changed after the first login for security reasons.

The following screen should be visible after logging in as a "master" user:



hopf Elektronik GmbH
NETWORK TIME CLIENT 8030NTC
© 2005-2016 rdcs.eu

General | Time | Network | NTP | Alarm | Device | Output

Device Time

DATE	TIME
LOC 09.11.2016	11:08:43 STD
UTC 09.11.2016	10:08:43

Time Client Status

SYNCHRONIZATION
☒ ON
ACCURACY
☒ HIGH

Announcements

LEAP SECOND ☐ Inactive
STD ↔ DST ☐ Inactive

Login

User **master** is logged in since 10:08:40 UTC.

NTP System Info

SYSTEM PEER
192.168.180.113
STABILITY
0.004 ppm
STRATUM
☒ 2
LAMBDA
2.472 ms

Click on the **Logout** button to log out.

The WebGUI is equipped with a session management. If the user does not conduct a logout, the logout is automatically made after 10 minutes of inactivity (idle time).

After successful login, depending on the access level (device or master user), changes can be made to the configuration and saved.

Users logged in as "master" have all access rights to the Time Client 8030NTC.

Users logged in as "**device**" do **not** have access to:

- Trigger reboot
- Trigger factory defaults
- Carry out image update
- Carry out H8 firmware update
- Change master password
- Download configuration files

6.2.2 Navigation via the Web Interface

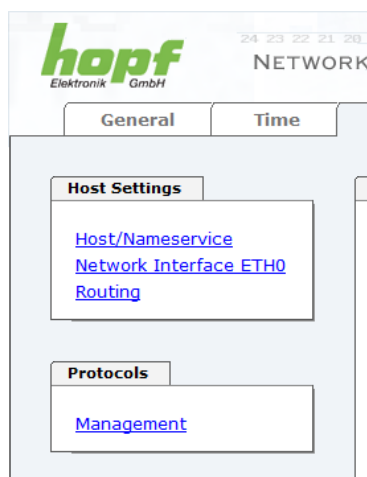
The WebGUI is divided into functional tabs. Click on one of these tabs to navigate through the board. The selected tab is identified by a darker background colour - see the following image (General in this case).



User login is not required in order to navigate through the board configuration options.



JavaScript and Cookies should be enabled in the browser in order to guarantee the correct operation of the web interface.



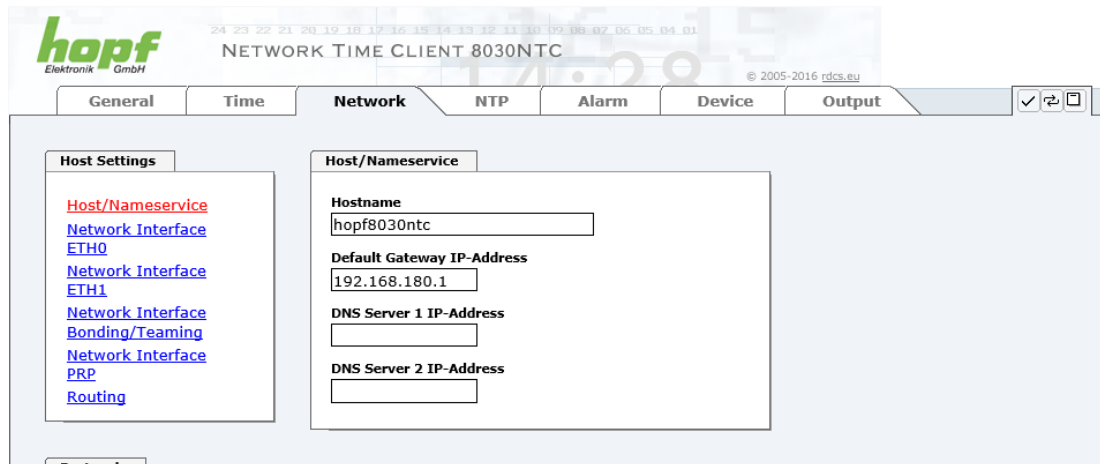
All the links within the tabs on the left hand side lead to corresponding detailed display or setting options.

6.2.3 Enter or Changing Data

It is necessary to be logged on as one of the users described above in order to enter or change data.

All changeable data, are saved in Module 8030NTC. For these data the value saving is divided into two steps.

For a permanent saving the modified value **must** first be accepted with **Apply** from the module and then be stored with **Save**. Otherwise the modifications get lost after a reboot of the module or switching the system off.



After an entry with **Apply** is made, the configured field is marked with a star ' * '. This means that a value has been entered or changed but not yet been stored in the flash memory.



Meaning of the symbols from left to right:

No.	Symbol	Description
1	Apply	Acceptance of changes and entered data
2	Reload	Restoring the saved data
3	Save	Fail-save storage of the data in the flash configuration

If the data should only be tested it is sufficient to accept the changes with **Apply**.



Changing Network Parameters

Modifications of the network parameters (e.g. IP address) are immediately effective clicking on **Apply** to confirm.

However, the modifications are not permanently saved yet. This requires to access the WebGUI with the new network parameters again and to save the data with **Save** permanently.



For adopting changes and entering values only the respective buttons in the WebGUI can be used.

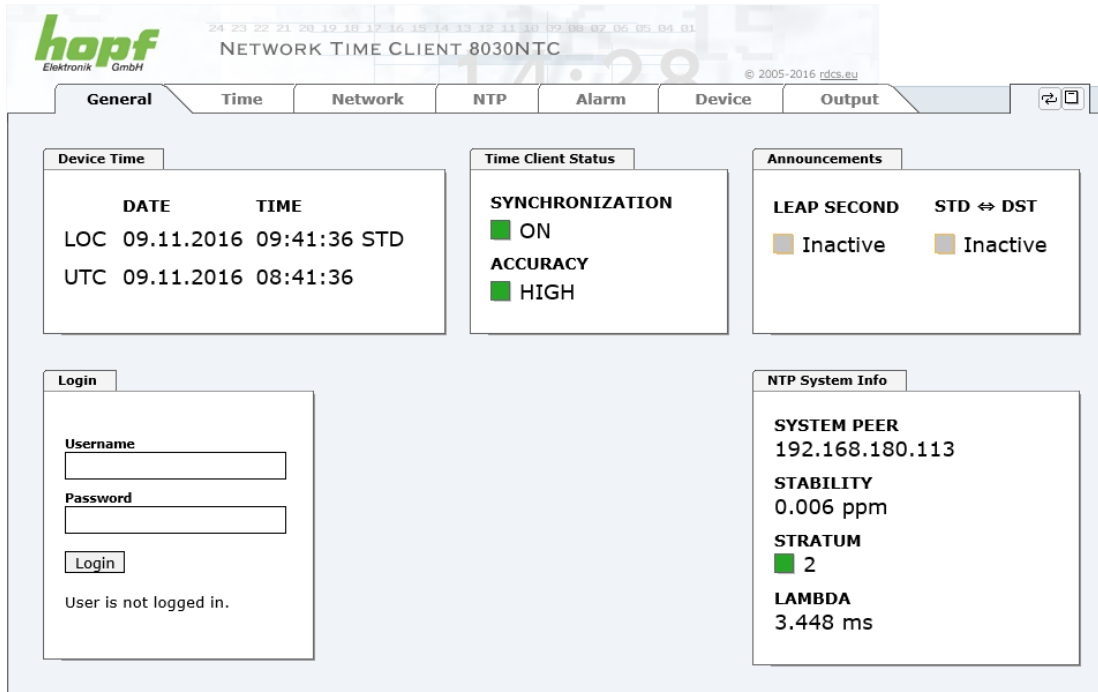
6.3 Description of the Tabs

The WebGUI is divided into the following tabs:

- General
- Time
- Network
- NTP
- Alarm
- Device

6.3.1 GENERAL Tab

This is the first tab which is displayed when using the web interface. This shows the current time and the synchronization state of the Module 8030NTC, furthermore a Login is possible (enter username and password), which is necessary to configure the Module 8030NTC via WebGUI.



The screenshot displays the 'General' tab of the hopf WebGUI for the 'NETWORK TIME CLIENT 8030NTC'. The interface includes a top navigation bar with tabs: General, Time, Network, NTP, Alarm, Device, and Output. Below the navigation bar, there are several status boxes:

- Device Time:** Shows DATE and TIME for LOC (09.11.2016 09:41:36 STD) and UTC (09.11.2016 08:41:36).
- Time Client Status:** Shows SYNCHRONIZATION (ON) and ACCURACY (HIGH).
- Announcements:** Shows LEAP SECOND (Inactive) and STD ↔ DST (Inactive).
- Login:** Includes fields for Username and Password, a Login button, and a message 'User is not logged in.'
- NTP System Info:** Shows SYSTEM PEER (192.168.180.113), STABILITY (0.006 ppm), STRATUM (2), and LAMBDA (3.448 ms).

Login

The **Login** box is used in accordance with **Chapter 6.2.1 LOGIN and LOGOUT as User**

Device Time

This sector displays the current time and date of Module 8030NTC, used for the output of time information. This time corresponds with the UTC time (UTC) received by NTP and the resulting local time (LOC). The local time is created by the parameters configured under the tab TIME (see **Chapter 6.3.2 TIME Tab**). In addition to the local time the daylight saving time (DST) / and standard time (STD) is indicated.

Time Client Status

SYNCHRONIZATION

Indicates the synchronization status of the internal time output. This value describes whether the connected components/devices can use the time information of Module 8030NTC for their own synchronization.

ON: The time information put out by the module can be used by connected components/devices for their own synchronization.

OFF: The time information put out by the module **cannot** be used by connected components/devices for their own synchronization.

ACCURACY

The **ACCURACY** field (accuracy of NTP) can include the possible values LOW - MEDIUM - HIGH. The meaning of those values is explained in **Chapter 10.5 Accuracy & NTP Basic Principles**.



By default the accuracy of NTP must be at least HIGH so that the module supplies time information for synchronization. This value can be set by the user if required.

Announcements

LEAP SECOND

announcement for inserting a leap second

Inactive: No announcement exists

Active: There is an announcement. A leap second is inserted on the next hour.

STD ⇔ DST

Announcement for adjustment for daylight saving time / standard time

Inactive: No announcement exists

Active: There is an announcement. An adjustment for daylight saving time / standard time is made on the next hour.

NTP System Info

SYSTEM PEER

Indicates the currently used NTP Time Server for the synchronisation.

STABILITY

Indicates the current NTP stability value of Module 8030NTC in ppm.

STRATUM

Indicates the current NTP stratum value of Module 8030NTC in the value range of 1-16.



By default the stratum value of the Module 8030NTC is always one lower than the stratum of the SYSTEM PEER. The Module 8030NTC can only be synchronized on a SYSTEM PEER that it is at least **STRATUM 14 or better**.

LAMBDA

Indicates the current calculated NTP-LAMBDA value of Module 8030NTC in milliseconds.

6.3.2 TIME Tab

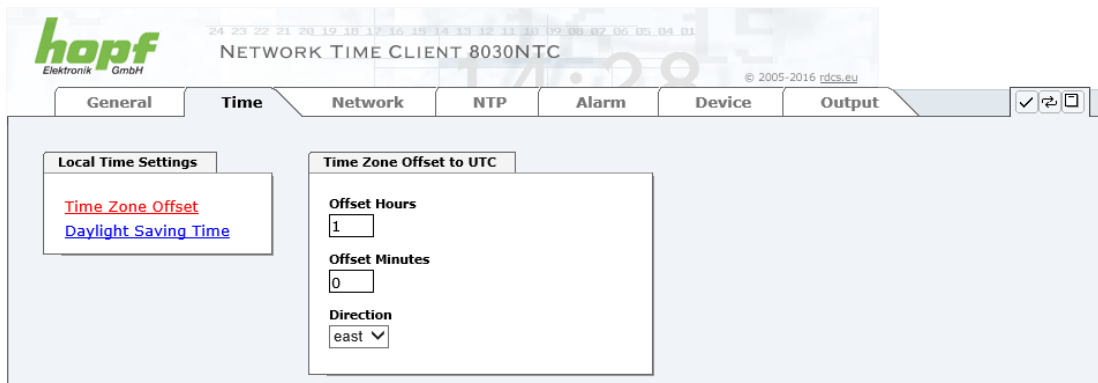
Generally NTP transfers the time information with the time basis UTC. The configuration of difference time (**Time Zone Offset to UTC**) is required for calculating the local standard time (winter time).

6.3.2.1 Time Zone Offset

Setting of the difference time (Time Zone Offset) from UTC to the local standard time (winter time).



The difference time to be entered **always** relates to **the local standard time (winter time)** even though the commissioning or rather the input of the difference time takes place during daylight saving time.



- **Offset Hours** Time Zone Offset input of the full hour (0-13)
- **Offset Minutes** Time Zone Offset input of minutes (0-59)

Example:

Time Offset for Germany ⇒ East, 1 hour and 0 minutes (+ 01:00)
 Time Offset for Peru ⇒ West, 5 hours and 0 minutes (- 05:00)

Direction relating to Prime Meridian – Direction of the Difference Time

Entering the direction the local time deviates from world time:

'East' corresponds to east,
 'West' corresponds to west of the Prime-Meridian (Greenwich)

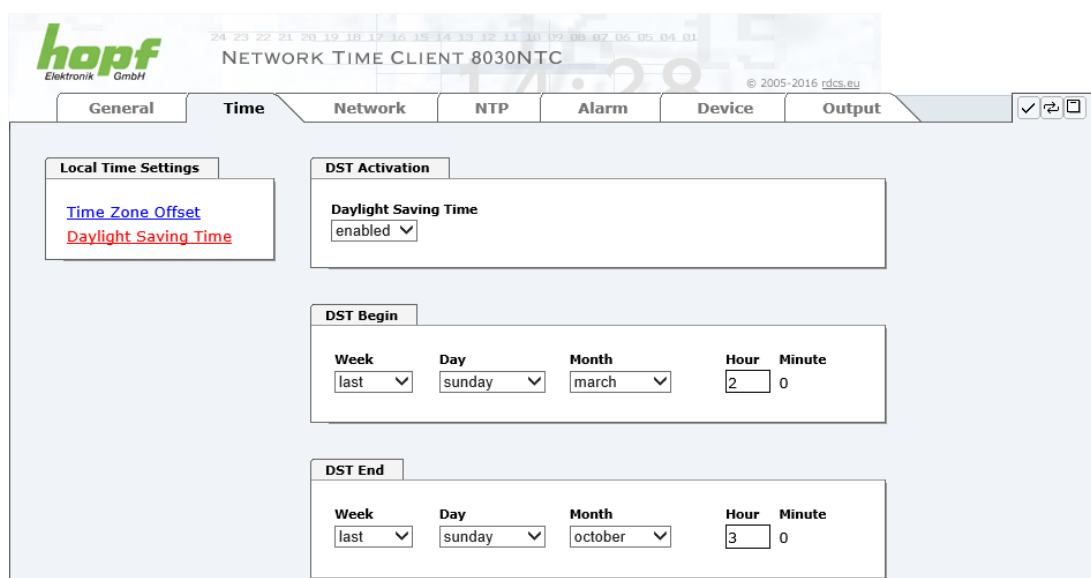
6.3.2.2 Configuration of Summer Time (Daylight Saving Time)

This input is used to define the point of time at which the changeover to Daylight Saving Time or winter time occurs during the course of the year. The hour, day of the week, week of the month and month at which the Daylight Saving Time begins and ends are determined.

So the exact times are automatically calculated for the running year.



After the turn of the year the changeover times for summer/winter time are **automatically** recalculated, without any user intervention.



- **DST Activation (enabled/disabled)** – Changeover times for summer/winter time
- **DST Begin** – Changeover time for standard time to Daylight Saving Time
- **DST End** – Changeover time for Daylight Saving Time to standard time

The individual items have the following meanings:

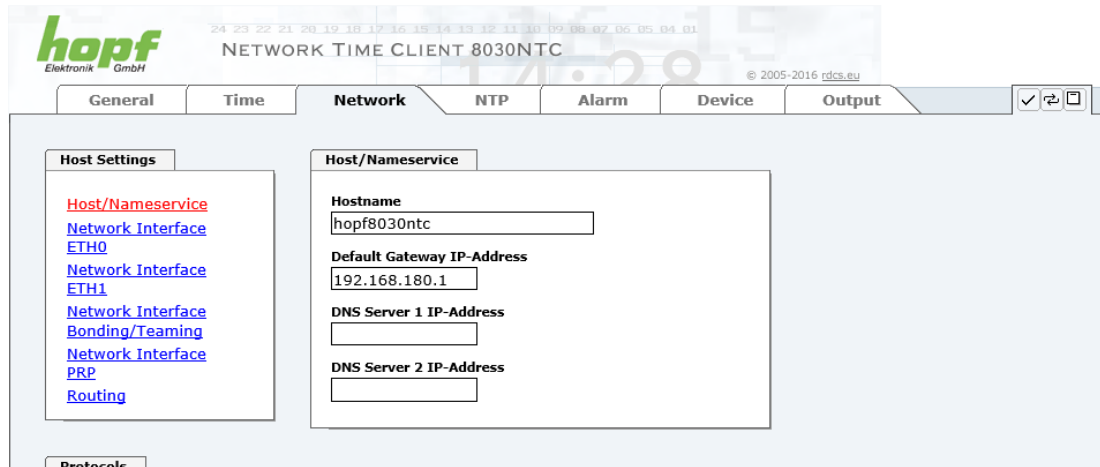
Week	How often the changeover should be processed per day of the week in the month	First - 1st week Second - 2nd week Third - 3th week Fourth - 4th week Last - last week
Day	The day of the week when the changeover should be processed	Sunday, Monday ... Saturday
Month	the month when the changeover should be processed	January, February ... December
Hour Minute	The time in hour and minute when the changeover should be processed	00h ... 23h 00min ... 59min



The data are entered on the basis of the local time.

6.3.3 NETWORK Tab

All the links within the tab on the left hand side lead to corresponding detailed setting options.




Changing Network Parameters

Modifications of the network parameters (e.g. IP address) are immediately effective clicking on **Apply** to confirm.

However, the modifications are not permanently saved yet. This requires to access the WebGUI with the new network parameters again and to save the data with **Save** permanently.

6.3.3.1 Host / Name Service

Setting for the unique network identification.

6.3.3.1.1 Hostname

The standard setting for the Hostname is "**hopf8030ntc**". This name should also be adapted to the respective network infrastructure.

If in doubt, simply leave the standard value in place or ask your network administrator.



The **hostname** must meet the following conditions:

- The hostname may only contain the characters 'A'-'Z', '0'-'9', '-' and '.'. There should be no distinction between upper-and lower-case letters.
- The character '.' may only appear as a separator between labels in domain names.
- The sign '-' must not appear as first or last character of a label.



For a correct operation a hostname is required. The field for the hostname **must not** be left blank.

6.3.3.1.2 Default Gateway

Contact your network administrator for details of the standard gateway if not known. If no standard gateway is available (special case), enter 0.0.0.0 in the input field or leave the field blank.

6.3.3.1.3 DNS Server 1 & 2

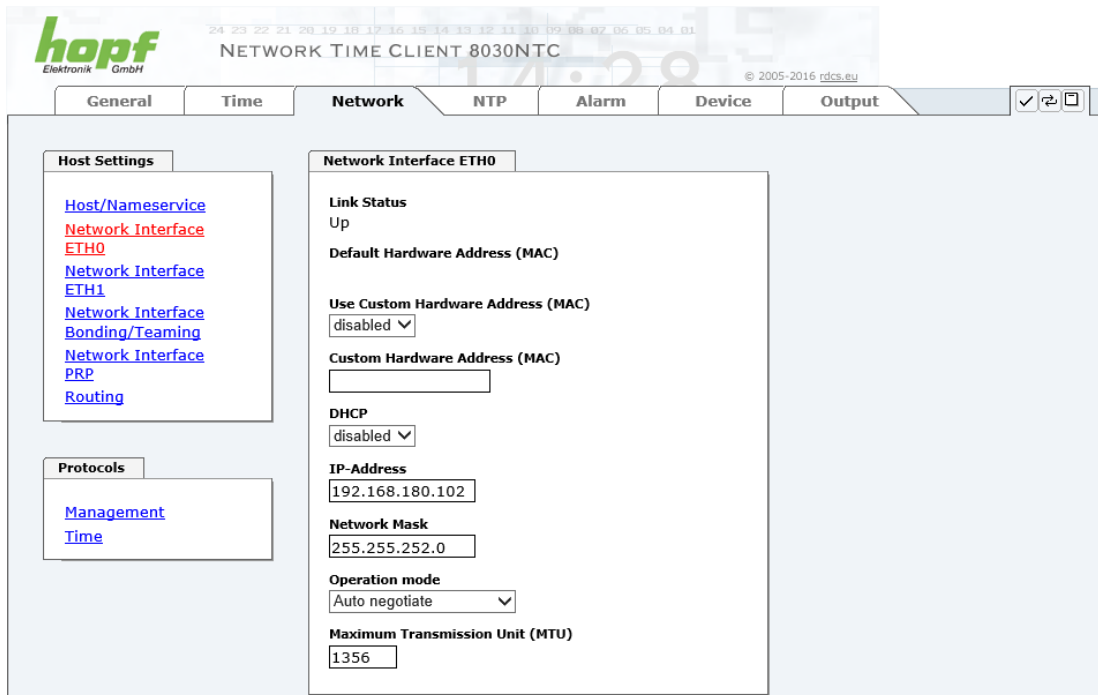
The IP address of the DNS server should be entered if you wish to use complete Hostnames (hostname.domainname) or work with reverse lookup.

Contact your network administrator for details of the DNS server if not known.

If no DNS server is available (special case), enter 0.0.0.0 in the input field or leave the field blank.

6.3.3.2 Network Interface ETH0/ETH1

Configuration of the Ethernet interface ETH0/ETH1 of the Time Client 8030NTC



The screenshot shows the web interface for the Hopf Network Time Client 8030NTC. The top navigation bar includes tabs for General, Time, Network (selected), NTP, Alarm, Device, and Output. The main content area is divided into two sections: Host Settings and Network Interface ETH0. The Host Settings section contains links for Host/Nameservice, Network Interface ETH0, Network Interface ETH1, Network Interface Bonding/Teaming, Network Interface PRP, and Routing. The Network Interface ETH0 section contains the following configuration options:

- Link Status: Up
- Default Hardware Address (MAC):
- Use Custom Hardware Address (MAC): disabled
- Custom Hardware Address (MAC):
- DHCP: disabled
- IP-Address: 192.168.180.102
- Network Mask: 255.255.252.0
- Operation mode: Auto negotiate
- Maximum Transmission Unit (MTU): 1356



ETH1 must not be located in the same sub net as ETH0!

6.3.3.2.1 Default Hardware Address (MAC)

The factory default MAC address can only be read and cannot be changed by the user. It is assigned once only by **hopf** Elektronik GmbH for each Ethernet interface.

For further information about the MAC address refer to **Chapter 2.3.4.1 MAC-Address for ETH0/ETH1** for the Time Client 8030NTC.



hopf Elektronik GmbH MAC addresses begin with **00:03:C7:xx:xx:xx**.

6.3.3.2.2 Customer Hardware Address (MAC)

The MAC address assigned from **hopf** can be changed to any user-defined MAC address. The board identifies itself with the user-defined MAC address to the network. The default hardware address shown in WebGUI remains unchanged.



Double assignment of MAC addresses on the Ethernet referring to customers MAC addresses should be avoided.
If the MAC address is not known, please contact your network administrator.

The use of customers MAC address needs to be activated by the function **Use Custom Hardware Address (MAC)** with **enable** and subsequently save it with **Apply** and **Save**.

Afterwards the customers MAC address has to be entered in hexadecimal form with a colon to separate as described in the below example, e.g. **00:03:c7:55:55:02**



The MAC address assigned by **hopf** can be activated at any time by disabling this function.



There are no MAC multicast addresses allowed!

Finally, the Time Client 8030NTC has to be restarted via "Device" ⇒ "Reboot Device" (see **Chapter 6.3.6.4 Reboot Device**).

6.3.3.2.3 DHCP

If DHCP is to be used, activate this with **enabled**.

6.3.3.2.4 IP Address

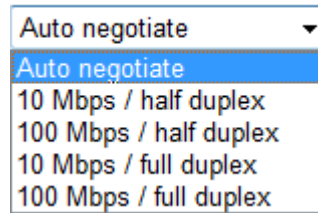
If DHCP is not used, the IP address needed to be entered here. Contact your network administrator for details of the used IP address if not known.

6.3.3.2.5 Network Mask

If DHCP is not used, the network mask needed to be entered here. Contact your network administrator for details of the used network mask if not known.

6.3.3.2.6 Operation Mode

Operation mode



The screenshot shows a dropdown menu with the following options: Auto negotiate (selected), Auto negotiate, 10 Mbps / half duplex, 100 Mbps / half duplex, 10 Mbps / full duplex, and 100 Mbps / full duplex.

The network device usually adjusts the data stream and duplex mode to the device to which it is connected (e.g. HUB, SWITCH) automatically. If the network device requires a certain speed or duplex mode, this can be configured via the web interface. The value should only be changed in special cases. The automatic setting is normally used.



In individual cases an enabled "Auto negotiate" might lead to problems between the network components and the adjustment process fails.

In such cases it is recommended to set the network speed of the Time Client 8030NTC **and** the connected network components manually to the same value.

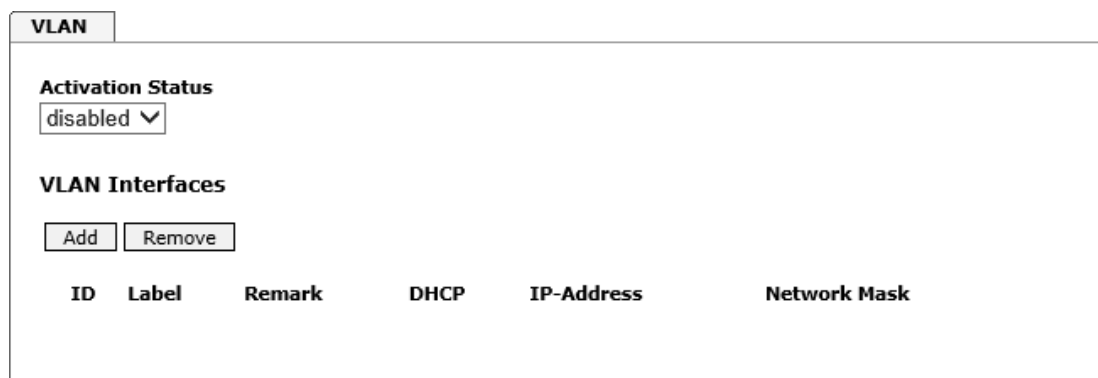
6.3.3.2.7 Maximum Transmission Unit (MTU)

The Maximum Transmission Unit describes the maximum size of a data packet of a protocol of the network layer (layer 3 of OSI model), measured in octets which can be transferred into the frame of a net of the security layer (layer 2 of OSI model) without fragmentation.

Time Client 8030NTC is going to be delivered with default setting 1356.

6.3.3.2.8 VLAN (Activation Key necessary)

A VLAN (Virtual Local Area Network) is a logical sub-network within a network switch or a whole physical network. VLANs are used to separate the logical network infrastructure from the physical wiring, thus to virtualize the Local Area Network. The technology of VLAN is standardized by IEEE Standard 802.1q. Network applications like Time Client 8030NTC, implementing the standard IEEE 802.1q, are able to allocate individual network interfaces to specific VLANs. To transfer data packets of several VLANs via a single network interface the data packets are marked with a related VLAN ID. This method is called VLAN-Tagging. The network application at the other end of the line (e.g. network switch, router etc.) can allocate the data packet to the correct VLAN by checking the marking / tag.



The screenshot shows the VLAN configuration interface. It has a tab labeled 'VLAN'. Below the tab, there is a section 'Activation Status' with a dropdown menu set to 'disabled'. Below that is a section 'VLAN Interfaces' with 'Add' and 'Remove' buttons. At the bottom, there is a table with the following headers: ID, Label, Remark, DHCP, IP-Address, and Network Mask.

WebGUI with activated VLAN

To be able to configure VLANs the activation status must be set to "enabled" first. Afterwards up to 32 different VLANs per network interface can be configured by clicking the button "Add".

An explicit VLAN ID must be configured for each VLAN interface.

The boxes "Label" and "Remark" can be filled out with a designation or a comment to easily keep the configured VLANs apart.

Determination of the IP-address for the configured VLAN interface can either be done automatically via DHCP or by filling out the boxes "IP-Address" and "Network Mask".

VLAN

Activation Status

enabled ▼

VLAN Interfaces

ID	Label	Remark	DHCP	IP-Address	Network Mask
<input type="checkbox"/> 10	DEV	Development	disabled ▼	192.168.180.30	255.255.255.0



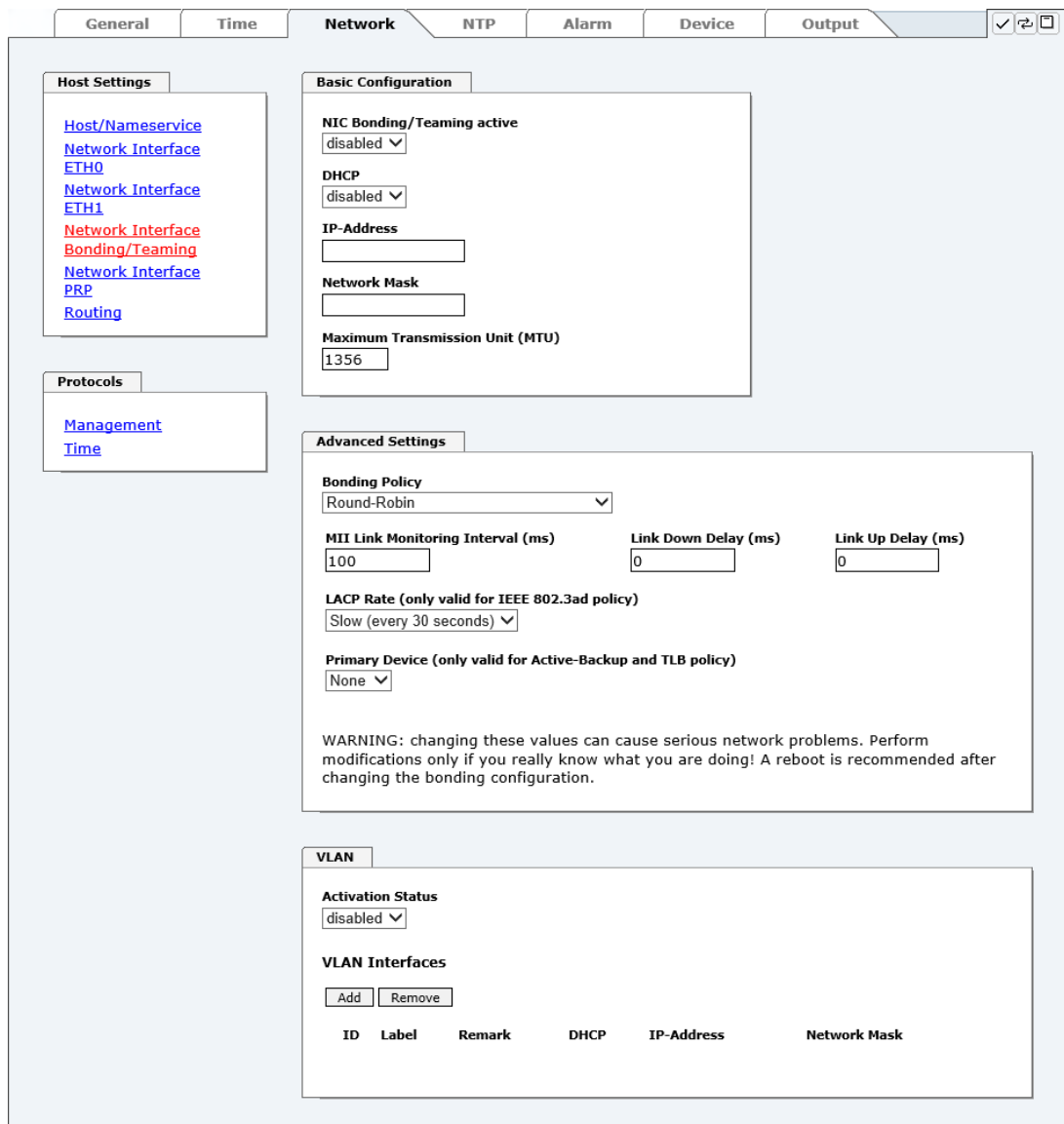
To ensure the correct function the network appliance must be connected with Time Client 8030NTC via the network interface. Furthermore it must be ensured that the network appliance is accurately configured with the same VLANs.



VLAN ID one (1) and two (2) are reserved and are therefore not permitted!

6.3.3.3 Network Interface Bonding/Teaming (Activation Key necessary)

The function Network Interface Bonding/Teaming (also known as NIC Bonding, NIC Teaming, Link Bundling, EtherChannel) enables to bundle the physical network interfaces ETH0 and ETH1 to one logical network interface.



This function is used for the distribution of load as well as to increase fail-safety in computer networks.



Making settings without profound knowledge of Bonding/Teaming can lead to serious network problems!

An incorrect configuration can lead to a loss of the network connection so that the Ethernet access to Time Client 8030NTC is going to be refused.

In this case settings of Time Client 8030NTC must be set back to default settings!



If function Bonding has been activated, parameters for ETH0 and ETH1 cannot be changed any more. The parameters are not displayed in the host setting menu as long as Bonding will be deactivated.

6.3.3.3.1 Basic Configuration

Determination of the basic network configuration with activated function Bonding/Teaming.

Basic Configuration

NIC Bonding/Teaming active

DHCP

IP-Address

Network Mask

Maximum Transmission Unit (MTU)

NIC Bonding/Teaming active

Activation of function NIC Bonding/Teaming

DHCP

Activation of DHCP of the "Bonding interface".



A change of the IP-address or activating of DHCP do have an immediate effect after confirming the settings – the connection to the web interface must be adapted and renewed.

IP address

Input of IP address of the "Bonding interface".

If you do not know the IP address, please contact your network administrator.



A change of the IP-address or activating of DHCP do have an immediate effect after confirming the settings – the connection to the web interface must be adapted and renewed.

Network Mask

Input of the network mask of the "Bonding interface".



A change of the IP-address or activating of DHCP do have an immediate effect after confirming the settings – the connection to the web interface must be adapted and renewed.

6.3.3.3.2 Advanced Settings

Advanced Settings

Bonding Policy

Active-Backup

MII Link Monitoring Interval (ms)

100

Link Down Delay (ms)

0

Link Up Delay (ms)

0

LACP Rate (only valid for IEEE 802.3ad policy)

Slow (every 30 seconds)

Primary Device (only valid for Active-Backup and TLB policy)

None

WARNING: changing these values can cause serious network problems. Perform modifications only if you really know what you are doing! A reboot is recommended after changing the bonding configuration.

Bonding Policy

- Round-Robin:**
 In this case the network interfaces, starting with ETH0, are transmitting sequentially whereby a distribution of load and a higher tolerance for errors are achieved. In that mode the network interfaces must be connected to the same network switch.
- Active Backup:**
 Only one of two network interfaces is sending and receiving. If an error occurs, the other network interface assumes responsibility for the process. The network interfaces do not have to be connected to the same network switch. From the outside the MAC address of the association is only visible on one network interface to avoid a mix-up. This mode supports tolerance for errors.
- Balance XOR:**
 Source and target are permanently assigned with one another via the MAC address of the network interfaces ETH0 and ETH1. The network interfaces must be connected to the same network switch. This mode supports distribution of load and tolerance for errors.
- Broadcast:**
 In this mode the computer sends its data via all available network interfaces which enables the use of several network switches. This fact leads to a high tolerance for errors, but this mode does not enable distribution of load.
- IEEE 802.3ad Dynamic Link Aggregation:**
 The network interfaces ETH0 and ETH1 are going to be bundled (Trunking) in this mode. It is mandatory that the network interfaces are configured with the same transmission rate and duplex setting. Bundling is made dynamically via the Link Aggregation Control Protocol (LACP). This mode supports distribution of load as well as tolerance for errors.



The network switch on which the network interfaces ETH0 and ETH1 of Time Client 8030NTC are connected also needs to be configured correctly! A wrong configuration can lead to a loss of availability of Time Client 8030NTC!

- **Adaptive Transmit Load Balancing (TLB):**
Outbound data traffic is split on both network interfaces ETH0 and ETH1 in accordance with the current load, depending on the interface speed adjusted.
The network interfaces do not have to be connected on the same network switch.
This mode supports distribution of load and tolerance for errors.

MII link monitoring interval (ms)

Indicates the interval in milliseconds for observing the MII-connection. A value of zero deactivates monitoring. The default value is 100ms.

link down delay (ms)

Determines the delay time in milliseconds to deactivate a connection after a link error is detected. This value needs to be a multiple of the MII link monitoring interval.

link up delay (ms)

Determines the delay time in milliseconds to enable a conjunction after a connection is detected. This value needs to be a multiple of the MII link monitoring interval.

LACP rate (only available for IEEE 802.3ad directive)

Indicates the link partner's request frequency to transfer LACP packets in IEEE 802.3ad mode.

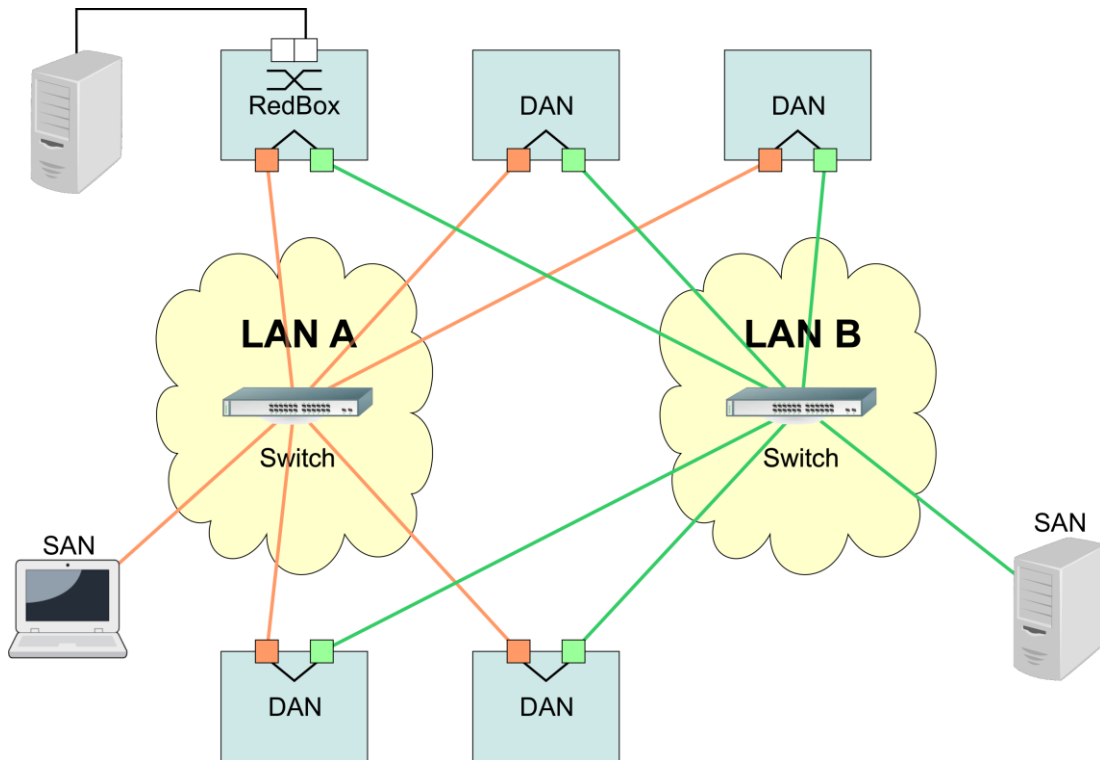
Primary Device (only valid for active backup and TLB directive)

If this asset is configured and the network interface is active, the adjusted network interface is going to be used. Only if the network interface is inactive, mode is changed to the second network interface.

6.3.3.4 Network Interface PRP (Activation Key necessary)

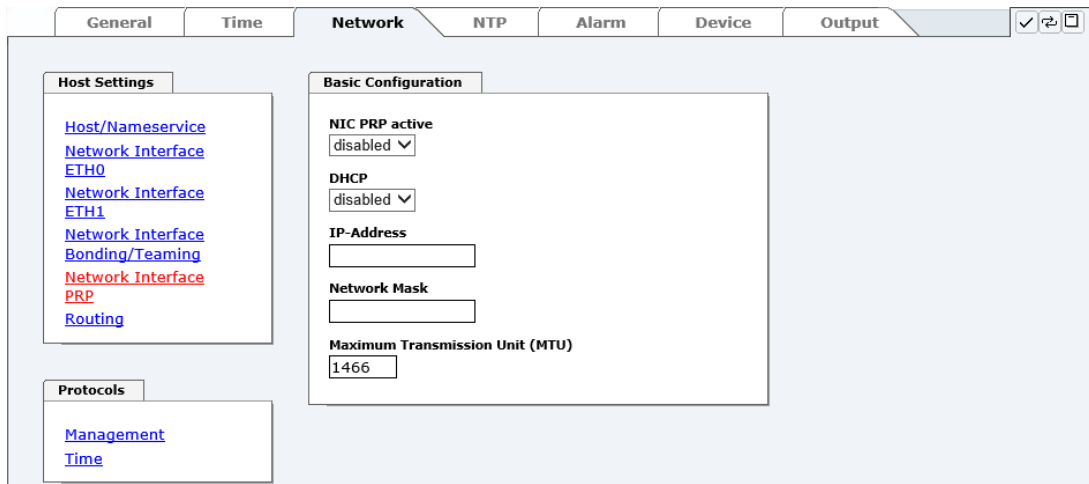
The PRP (Parallel Redundancy Protocol) functionality is specified in standard IEC 62439-3:2011 and enables to bundle the physical network interfaces ETH0 and ETH1 to one logical network interface. Each network interface is connected to an independent LAN (Local Area Network). If one of the two LANs has got a failure, usage of PRP ensures that the network connection between the PRP terminal devices is going to be maintained via the second, independent LAN. PRP standard was developed for very high demanding and critical applications in the field of automation of substations.

The following illustration shows an example of a PRP network:



PRP-suitable applications are known as DAN (Dual Attached Node) and are going to be connected to the independent networks "LAN A" and "LAN B". The advantage of PRP is that cost-efficient and common network switches can be used which do not have to support the PRP standard. Applications which do not need to be redundantly available and which do not have to support PRP can be connected without problems in one of the two LANs - they are then called SAN (Single Attached Node). If it is necessary to redundantly connect non-PRP-supporting applications to the PRP network, a so-called RedBox (Redundancy Box) can be used.

Time Client 8030NTC supports PRP as DAN and can therefore directly be integrated into a PRP network without using a RedBox.



To use PRP the following settings must be carried out:

NIC PRP active

Activation of the PRP functionality

DHCP

Activation of DHCP for the "PRP interface".



A change of the IP address or activation of DHCP will have an immediate effect after applying the settings - the connection to the web interface must be adapted and renewed.

IP address

Input of the IP address for the "PRP interface". If unknown the IP address needs to be obtained by the network administrator.



A change of the IP address or activation of DHCP will have an immediate effect after applying the settings - the connection to the web interface must be adapted and renewed.

Network Mask

Input of the network mask for the "PRP interface".



A change of the IP address or activation of DHCP will have an immediate effect after applying the settings - the connection to the web interface must be adapted and renewed.

Maximum Transmission Unit (MTU)

Input of the MTU to be used for the „PRP interface“.

The network interface ETH0 of Time Client 8030NTC need to be connected to PRP network "LAN A", network interface ETH1 need to be connected to PRP network "LAN B"!



Changing of the MTU default setting with value 1466 should not be necessary by default.

If settings are done without profound knowledge of PRP, severe network problems can occur.

An incorrect configuration can lead to a loss of the network connection which refuses the Ethernet access to Time Client 8030NTC.

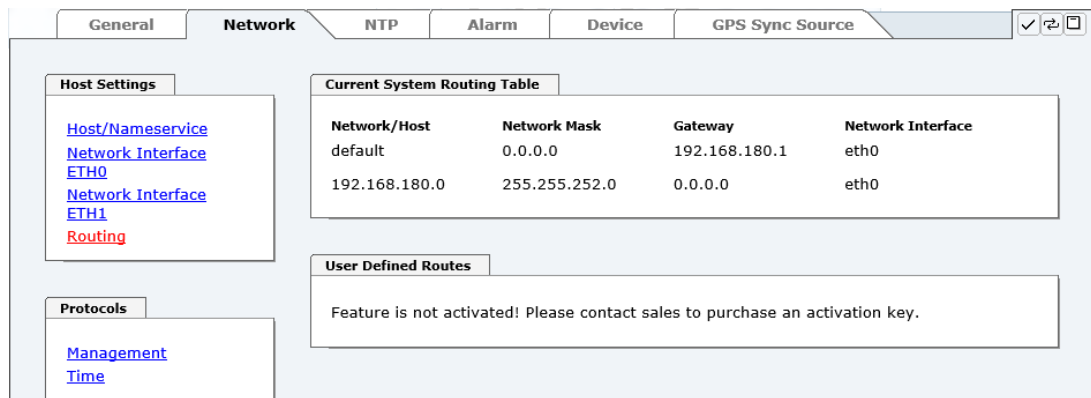
In that case the settings of Time Client 8030NTC need to be set to "factory default"!



If the functionality PRP was activated, parameters for ETH0 and ETH1 can no longer be adapted. The parameters will not be displayed in the host settings menu as long as PRP is going to be deactivated.

6.3.3.5 Routing (Activation Key necessary)

Additional static routes can be configured if the module is not only used in the local sub net and if connection cannot be established via the configured standard gateway.



The screenshot shows the 'Network' tab in the WebGUI. The 'Current System Routing Table' is displayed with the following data:

Network/Host	Network Mask	Gateway	Network Interface
default	0.0.0.0	192.168.180.1	eth0
192.168.180.0	255.255.252.0	0.0.0.0	eth0

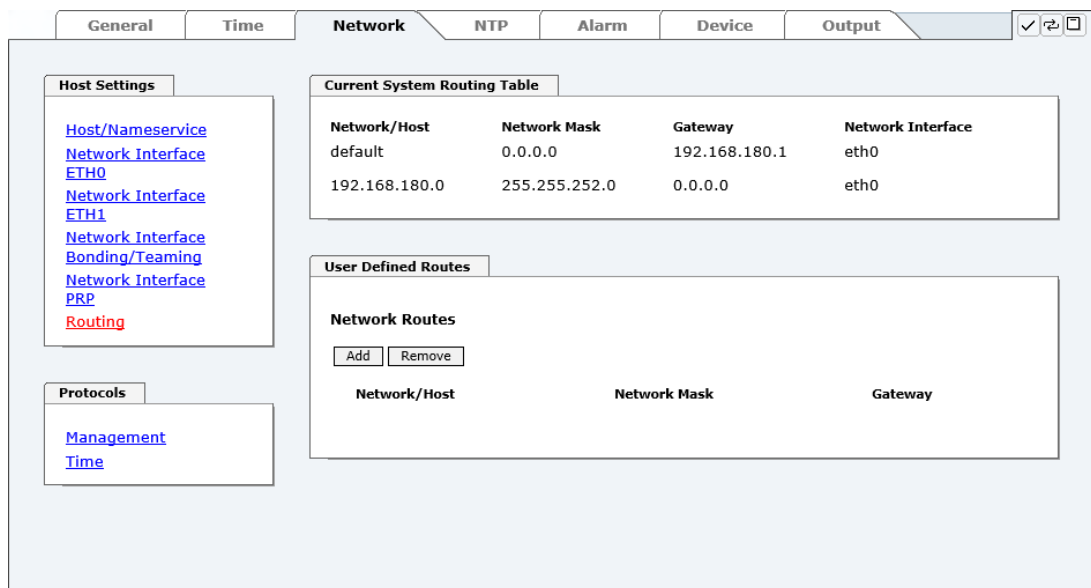
The 'User Defined Routes' section shows a message: "Feature is not activated! Please contact sales to purchase an activation key."

The gateway / gateway host need to be in the local sub-network range of the module in order to use the static routes.



The parameterization of this feature is a critical process as an incorrect configuration may lead to considerable problems on the network!

WebGUI with Routing activated



The screenshot shows the 'Network' tab in the WebGUI with 'Routing' activated. The 'Current System Routing Table' is the same as in the previous screenshot. The 'User Defined Routes' section now shows a table for 'Network Routes' with columns for 'Network/Host', 'Network Mask', and 'Gateway'. There are 'Add' and 'Remove' buttons above the table.

The image above shows every configured route of the base system routing table as well as the user's defined static routes.



The module cannot be used as a router!

6.3.3.6 Management (Management-Protocols – HTTP, SNMP, SNMP-Traps, etc.)

Protocols that are not required should be disabled for security reasons. A correctly configured module is always accessible via the web interface.

Changes to the availability of a protocol (enable/disable) take effect immediately.



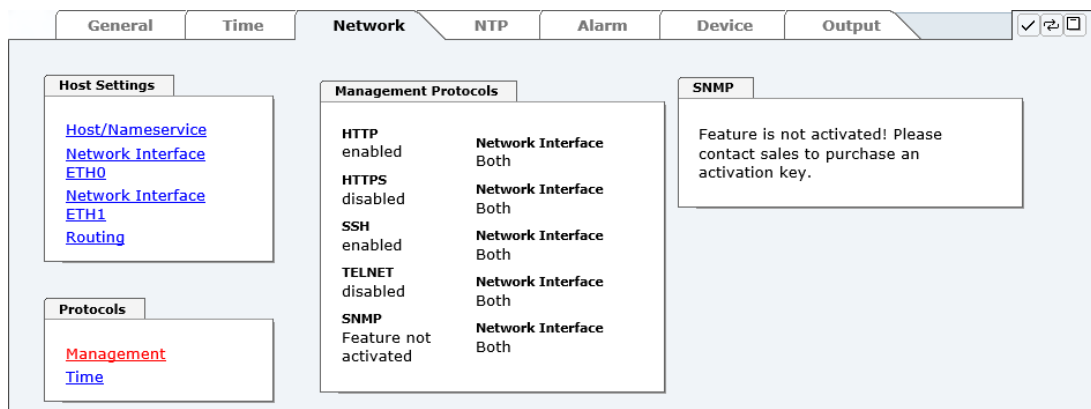
For SNMP functionality an activation key is necessary.



If by mistake all protocol channels become "disabled", the SSH channel is automatically "enabled" after the attempt to save.



After a Factory Default the HTTP and SSH channels are "enabled".



The screenshot shows the 'Network' tab in the web interface. It contains three main sections: 'Host Settings', 'Management Protocols', and 'SNMP'. 'Host Settings' includes links for Host/Nameservice, Network Interface (ETH0, ETH1), and Routing. 'Management Protocols' lists HTTP (enabled), HTTPS (disabled), SSH (enabled), TELNET (disabled), and SNMP (Feature not activated), each with a 'Network Interface' of 'Both'. The 'SNMP' section displays a message: 'Feature is not activated! Please contact sales to purchase an activation key.'



These service settings are valid globally! "Disabled" Services are not externally accessible and are not made externally available by the module!

WebGUI with Alarming activated

General	Time	Network	NTP	Alarm	Device	Output										
<div> <div> Host Settings Host/Nameservice Network Interface ETH0 Network Interface ETH1 Network Interface Bonding/Teaming Network Interface PRP Routing </div> <div> Protocols Management Time </div> </div> <div> Management Protocols <table> <tr> <td>HTTP enabled ▼</td> <td>Network Interface Both ▼</td> </tr> <tr> <td>HTTPS disabled ▼</td> <td>Network Interface Both ▼</td> </tr> <tr> <td>SSH enabled ▼</td> <td>Network Interface Both ▼</td> </tr> <tr> <td>TELNET disabled ▼</td> <td>Network Interface Both ▼</td> </tr> <tr> <td>SNMP disabled ▼</td> <td>Network Interface Both ▼</td> </tr> </table> </div> <div> SNMP <div> System Location <input type="text"/> </div> <div> System Contact <input type="text"/> </div> <div> SNMPv2 Read Only Community <input type="text" value="public"/> </div> <div> SNMPv2 Read Write Community <input type="text" value="secret"/> </div> <div> SNMPv3 Security Name <input type="text"/> </div> <div> SNMPv3 Access Rights <input type="text" value="Readonly"/> ▼ </div> <div> SNMPv3 Authentication Protocol <input type="text" value="MD5"/> ▼ </div> <div> SNMPv3 Authentication Passphrase <input type="text"/> </div> <div> SNMPv3 Privacy Protocol <input type="text" value="DES"/> ▼ </div> <div> SNMPv3 Privacy Passphrase <input type="text"/> </div> </div>							HTTP enabled ▼	Network Interface Both ▼	HTTPS disabled ▼	Network Interface Both ▼	SSH enabled ▼	Network Interface Both ▼	TELNET disabled ▼	Network Interface Both ▼	SNMP disabled ▼	Network Interface Both ▼
HTTP enabled ▼	Network Interface Both ▼															
HTTPS disabled ▼	Network Interface Both ▼															
SSH enabled ▼	Network Interface Both ▼															
TELNET disabled ▼	Network Interface Both ▼															
SNMP disabled ▼	Network Interface Both ▼															

Using SNMP and SNMP- traps the protocol SNMP should be enabled.

6.3.3.6.1 SNMPv2c / SNMPv3 (Activation Key required)

Both protocols SNMPv2c and SNMPv3 are supported and can be configured and enabled independently from each other.

System Location and System Contact are global settings and are valid for both protocols (SNMPv2c / SNMPv3).

In order to disable SNMPv2c both fields **SNMP Read Only Community** and **SNMP Read Write Community** must remain empty.

SNMPv2c	SNMPv2c enabled	SNMPv2c disabled
Read Only Community:	set (e.g. public)	empty
Read/Write Community:	set (e.g. secret)	empty

In order to enable SNMPv3 the following fields must be set:

SNMPv3	Description
Security Name:	SNMPv3 is enabled (identical to the username)
Access Rights:	Equivalent to the Read/Write Communities in SNMPv2c
Authentication Protocol:	Authentication (MD5 or SHA Hash)
Privacy Protocol:	Encryption (DES or AES Algorithm)

There are three security levels in SNMPv3 that can be adjusted by the removal of the pass-phrases:

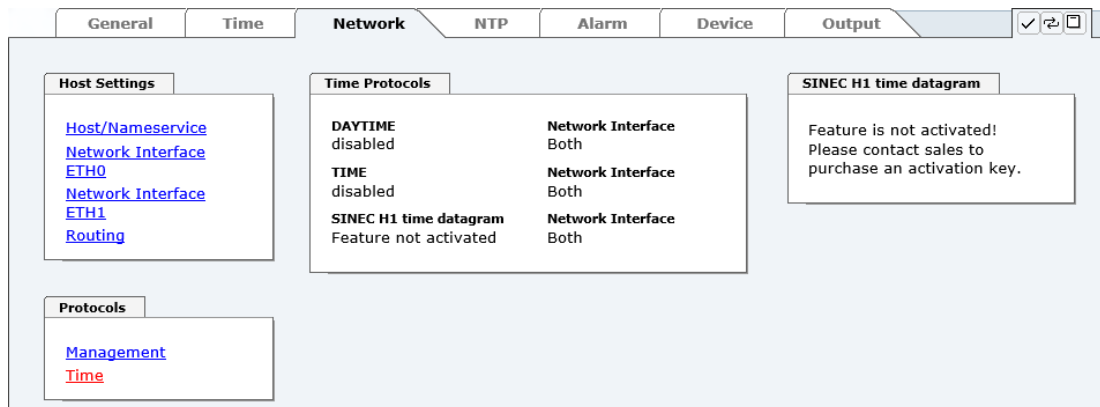
SNMPv3	noAuthNoPriv	authNoPriv	authPriv
Authentication Passphrase:	empty	set	set
Privacy Passphrase:	empty	empty	set



Right now only one user is supported.

6.3.3.7 Time (Time Protocols – NTP, DAYTIME etc.)

Activation and configuration of different synchronization protocols




All protocols can be enabled at the same time.

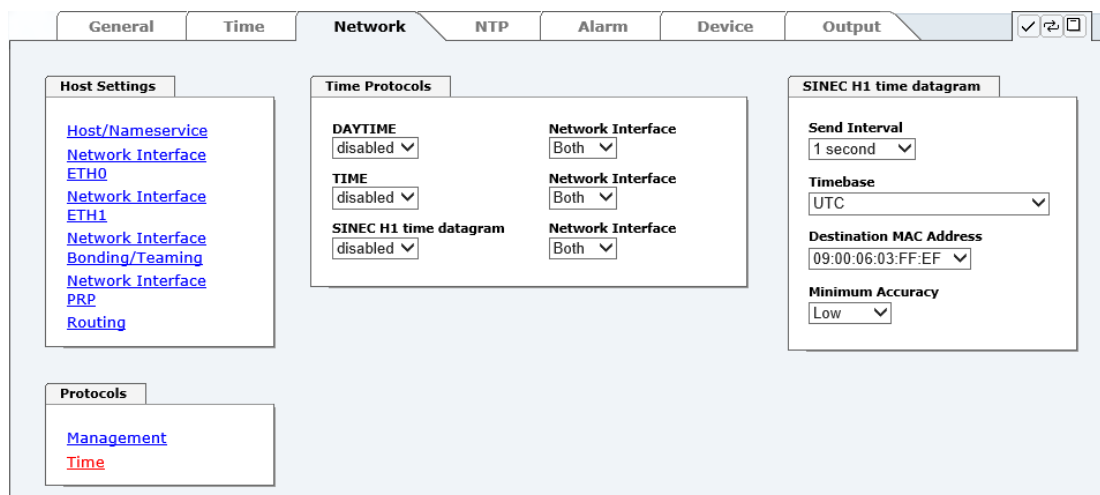
6.3.3.7.1 Synchronization Protocols (Time Protocols – NTP, SNTP etc.)

Needed time protocols can be enabled here.

- NTP (incl. SNTP)
- DAYTIME
- TIME
- SINEC H1 time datagram (Activation Key necessary)

6.3.3.7.2 SINEC H1 time datagram (Activation Key necessary)

Configuration of the SINEC H1 time datagram



Broadcast transmission intervals of the SINEC H1 time datagram (Send Interval)

- every second
- every 10 second
- every 60 second

Time base see also *Chapter 10.2.1 Time-specific expressions*

- Local time
- UTC
- Standard time
- Standard time with daylight / standard time status

Destination MAC Address

- 09:00:06:03:FF:EF
- 09:00:06:01:FF:EF
- FF:FF:FF:FF:FF:FF

Starting Transmission based on Synchronization Status (Minimum Accuracy)

This setting defines at which internal accuracy status the SINEC H1 time datagram should be transmitted (see **Chapter 10.5 Accuracy & NTP Basic Principles** and **Chapter 8 Technical Data**):

- LOW
- MEDIUM
- HIGH



The setting Minimum Accuracy = LOW may lead to the output of non-synchronised (thus possibly wrong) time information.

6.3.4 NTP Tab

This tab shows information and adjustment possibilities of the NTP services of the Time Client 8030NTC. The NTP service is the significant main service of the Time Client 8030NTC.

If you are not familiar with the subject of NTP you can find a short description in the Glossary. More details are also available at <http://www.ntp.org/>.

NTP functionality is provided by an NTP-Demon running on the embedded Linux of the Time Client 8030NTC.

Depending on the receiving conditions and under unfavourable circumstances it may take several hours until long-term accuracy is obtained (normally 5-10 minutes). During this time the NTP algorithm adjusts the internal accuracy parameters.



The NTP time protocol must be enabled in order to use NTP (see **Chapter 6.3.3.7 Time**)



After all changes relating to NTP a restart of the NTP service must be performed (see **Chapter 6.3.4.6 Restart NTP**).



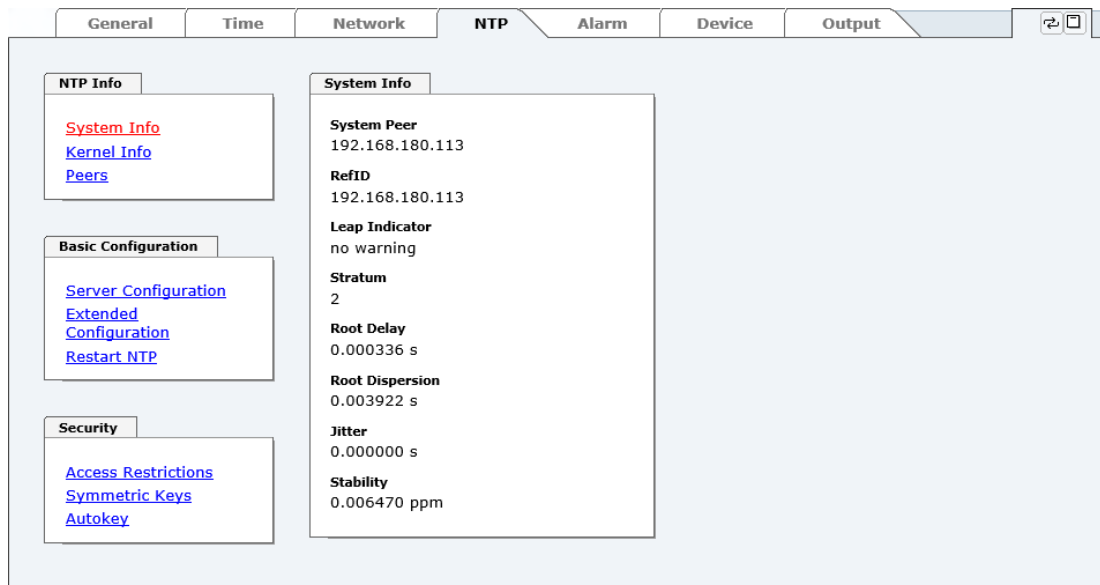
Via the NTP protocol SNTP Clients can also be synchronized. In contrast to NTP in SNTP Clients delay times are not evaluated on the network. For this reason the accuracy reached in SNTP Clients is lower than in NTP Clients.

6.3.4.1 System Info

In the window "System Info" the current NTP values of the NTP service running on the embedded Linux of the Time Client 8030NTC are indicated. In addition to the NTP calculated values for root delay, root dispersion, jitter, and stability the stratum value of the Time Client 8030NTC, the status to the leap second, and the current system peer are also found here.

The NTP version used adjusts the leap second correctly.

In case the used NTP Server (System PEER) works with Stratum 1 the NTP Client reaches max. Stratum 2.



The screenshot shows the NTP configuration web interface with the 'NTP' tab selected. The 'System Info' sub-tab is active, displaying the following data:

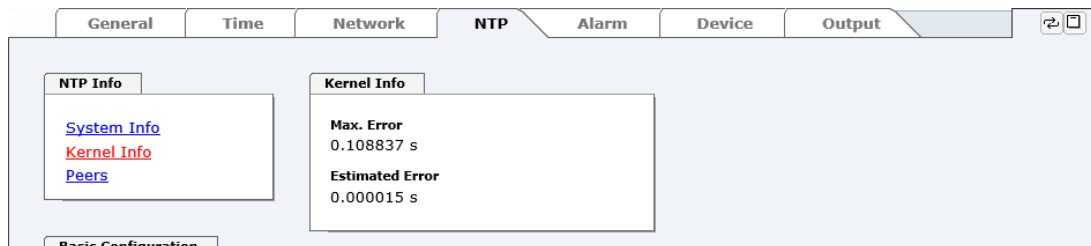
System Info	
System Peer	192.168.180.113
RefID	192.168.180.113
Leap Indicator	no warning
Stratum	2
Root Delay	0.000336 s
Root Dispersion	0.003922 s
Jitter	0.000000 s
Stability	0.006470 ppm

On the left side of the interface, there are three expandable sections:

- NTP Info**: Contains links for [System Info](#), [Kernel Info](#), and [Peers](#).
- Basic Configuration**: Contains links for [Server Configuration](#), [Extended Configuration](#), and [Restart NTP](#).
- Security**: Contains links for [Access Restrictions](#), [Symmetric Keys](#), and [Autokey](#).

6.3.4.2 Kernel Info

The “Kernel Info” overview shows the current error values of the internal embedded Linux clock. Both values are internally updated every second.



This screenshot shows a maximum kernel clock error of 108.837 msec (milliseconds). The estimated error value is 15 µs (microseconds).

The values indicated here are based on the calculation of the NTP service and have no significance for the accuracy of the Sync Source.

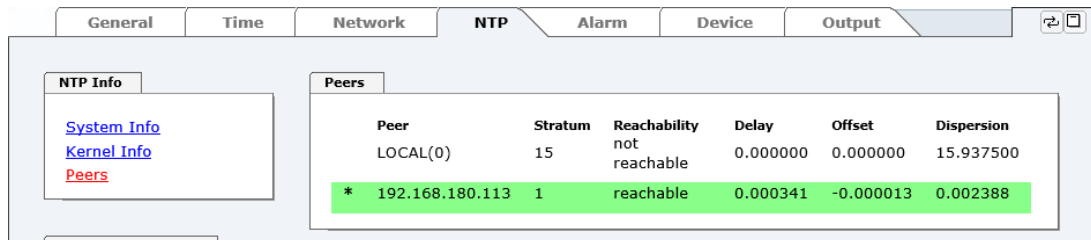
6.3.4.3 Peers

The “Peers summary” is used to track the performance of the configured NTP server/driver and the NTP algorithm itself.

The information displayed is identical with the information available via NTPQ or NTPDC programs.

Each NTP server/driver that has been set up in the NTP server configuration is displayed in the peer information.

The connection status is displayed in the reachability column (not reachable, bad, medium, and reachable).



Peer	Stratum	Reachability	Delay	Offset	Dispersion
LOCAL(0)	15	not reachable	0.000000	0.000000	15.937500
* 192.168.180.113	1	reachable	0.000341	-0.000013	0.002388

The first line displays the **hopf - refclock ntp driver** that gets the time information directly from the Sync Source.

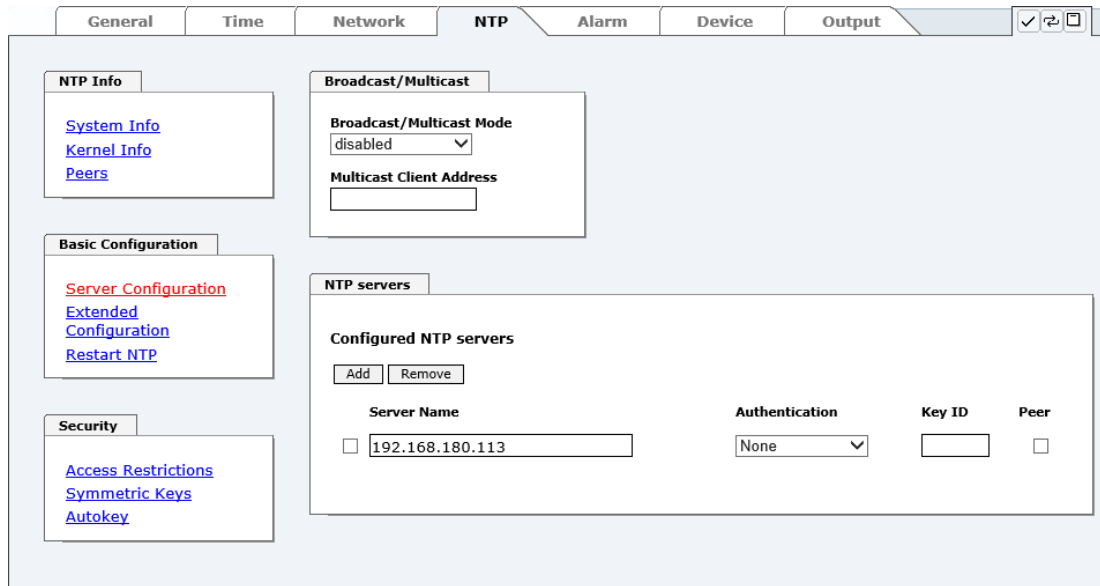
The second and third line display external NTP server that can be additionally added to the internal **hopf - refclock ntp driver** in the menu server configuration.

A short explanation and definition of the displayed values can be found in **Chapter 10.5 Accuracy & NTP Basic Principles**.

The character in the first column on the left presents the current status of the NTP association in the NTP selection algorithm. A list and description of possible characters can be found in the Glossary (see **Chapter 10.2 Tally Codes (NTP-specific)**).

6.3.4.4 Server Configuration

The basic settings for NTP base functionality are displayed when the "Server Configuration" link is selected.



6.3.4.4.1 Broadcast / Multicast

This section is used to configure the Time Client 8030NTC as a broadcast or multicast server.

The broadcast mode in NTPv3 and NTPv4 is limited to clients on the same sub-network and Ethernets which support broadcast technology.

This technology does not generally extend beyond the first hop (network node - such as router or gateway).

The broadcast mode is provided for configurations which are designed to facilitate one or more servers and as many clients as possible in a sub-network. The server continuously generates broadcast messages at defined intervals, corresponding to 16 seconds (minpoll 4) for Time Client 8030NTC. Care should be taken to ensure that the correct broadcast address is used for the sub-network, usually xxx.xxx.xxx.255 (e.g. 192.168.1.255). If the broadcast address is not known, this can be requested from the network administrator.

This section can also be used to configure the Time Client 8030NTC as a multicast server. The configuration of a multicast server is similar to that of a broadcast server. However, a multicast group address (class D) is used instead of the broadcast address.

An explanation of multicast technology goes beyond the scope of this document.

In principle, a host or router sends a message to an IPv4 multicast group address and expects all hosts and routers to receive this message. In doing so, there is no limit to the number of senders and receivers and a sender may also be a receiver and vice-versa. The IANA has assigned the multicast group address IPv4 224.0.1.1 to the NTP, however this should only be used if the multicast range can be safely limited in order to protect neighbouring networks. As a basic principle, administratively manageable IPv4 group addresses should be used as described in RFC-2365 or GLOP group addresses as described in RFC-2770.

6.3.4.4.2 NTP SERVERS for Synchronisation

Server Name

In this field the NTP Server, used for the synchronisation of Module 8030NTC, should be registered. Adding further NTP servers provides the option to implement a safety system for the time service. However, this influences the accuracy and stability of the module.

Detailed information on this subject can be found in the NTP documentation (<http://www.ntp.org/>).

Authentication / Key ID

Broadcast packets can be protected by authentication for security reasons.

If a security method is selected here this must be configured ADDITIONALLY in the security settings of the NTP tab. A key must be defined if the "Symmetric Key" is selected.

6.3.4.5 Extended Configuration

The synchronisation behaviour of Module 8030NTC can be adjusted following the link "**Extended Configuration**". This function allows by reference to the associated system properties Module 8030NTC to use NTP Server for synchronization and thus for the output of time information for the synchronization of connected devices and components with inaccurate NTP server. Reasons for inaccurate NTP server could be e.g. poor network performance, poor own accuracy or bad availability resulting in an insufficiently accurate synchronization of the module with the standard settings.

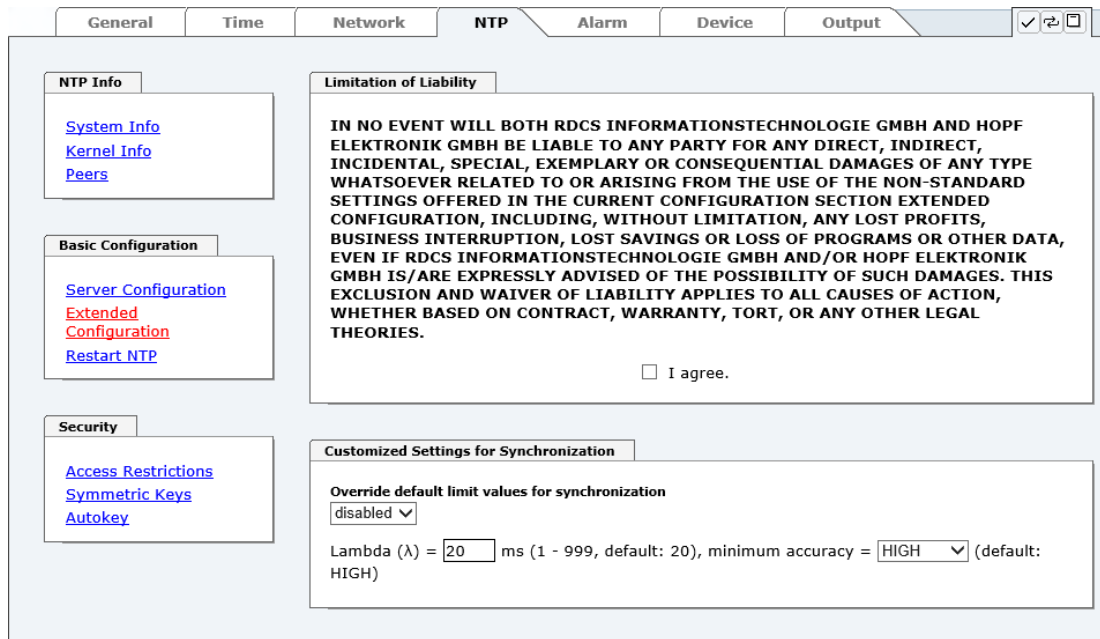
This function should be disabled by default.



When using this function the specified accuracy of Module 8030NTC and thus the accuracy of devices and components synchronized by the module may be worsened.



When using this function the specified data of NTP accuracy stated in the technical data of Module 8030NTC are not valid anymore.

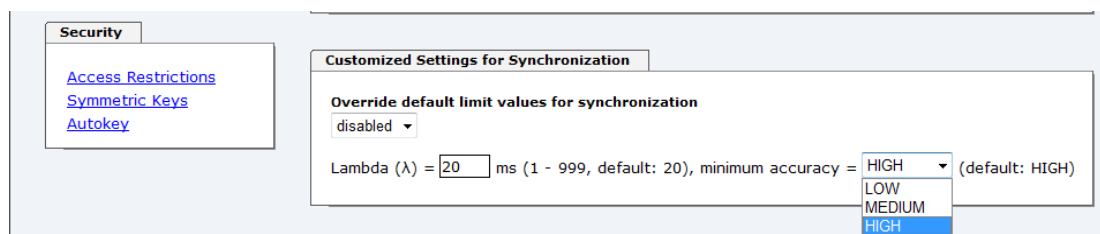


These functions are only unlocked with the declaration of consent "**I agree**" of the disclaimer "**Limitation of Liability**".



Safety Guidelines

The use of these functions should only be used by qualified users.
hopf is not liable for any damage caused by these.



Override default limit values for synchronization

For standard operation this function is disabled and should only be used by qualified users.

Lambda (λ)

For observance of specified accuracy of Module 8030NTC, it uses only accurate NTP server for synchronisation which have an accuracy value for lambda better 20ms.

In case it is required that Module 8030NTC should be synchronized on a more inaccurate NTP server the threshold accuracy value for lambda can be adjusted by this function.

The actually calculated lambda value is shown in the General tab.

Therefore, the function "**Override default limit values for synchronisation**" needs to be activated and to configure the required accuracy value for lambda (1-999ms).



When using this function the specified accuracy of Module 8030NTC and thus the accuracy of devices and components synchronized by the module may be worsened.

Minimum Accuracy

Only with the accuracy status **accuracy = high** Module 8030NTC synchronizes.

This function can be used for NTP server not being able to synchronize Module 8030NTC with the required accuracy. It allows the adjustment of the accuracy value (**accuracy = high / medium / low**) and the accuracy of the connected devices and components for the synchronization.



Modification of values do not cause an immediate effect when clicking on the apply symbol. In addition the NTP service **must** be restarted (see **Chapter 6.3.6.4 Reboot Device**).

6.3.4.5.1 Definition Accuracy (Low / Medium / High)

Calculation

$$\text{LAMBDA} = ((\text{root delay} / 2) + \text{Rootdispersion}) * 1000$$

LOW =

LAMBDA > Accuracy-value
or
 No system peer available
or
 Stratum = 16
or
 Internal NTP clock = not sync
or
 Clock hardware fault = ERROR

MEDIUM =

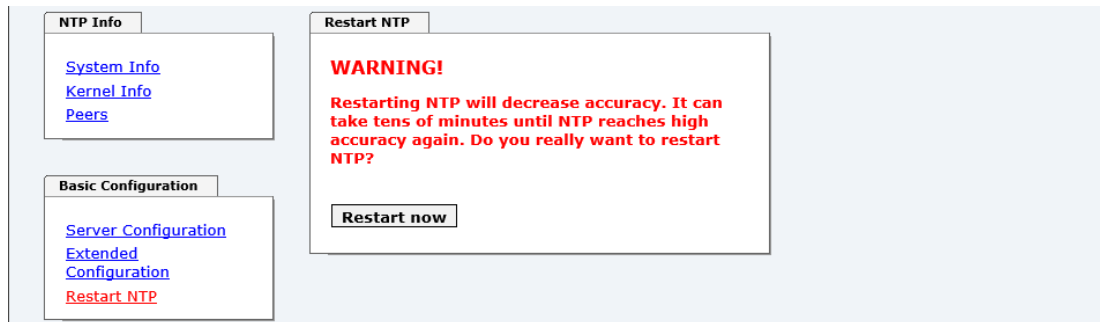
LAMBDA < Accuracy-value **and** System_Peer_Offset >= 0,001s
or
 LAMBDA < Accuracy-value **and** Stability > 2,0

HIGH =

LAMBDA < **Accuracy**-value **and** Stability < 0,2
or
 LAMBDA < Accuracy-value **and** Stability <= 2,0 **and** System_Peer_Offset < 0,001s

6.3.4.6 Restart NTP

The following screen appears after clicking on the Restart NTP function:



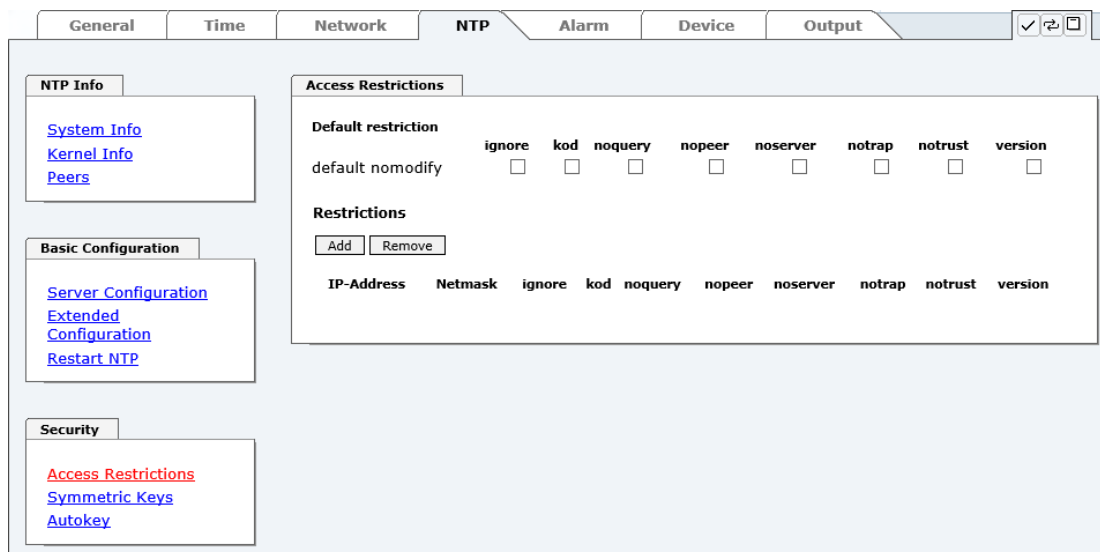
The screenshot shows the 'Restart NTP' tab in the web interface. On the left, there are navigation links for 'NTP Info' (System Info, Kernel Info, Peers) and 'Basic Configuration' (Server Configuration, Extended Configuration, Restart NTP). The main area displays a red 'WARNING!' message: 'Restarting NTP will decrease accuracy. It can take tens of minutes until NTP reaches high accuracy again. Do you really want to restart NTP?'. Below the warning is a 'Restart now' button.

Restarting NTP Services is the only possibility of making NTP changes effective without having to restart the entire Module 8030NTC. As can be seen from the warning message, the currently reachable stability and accuracy are lost due to this restart.

After a restart of the NTP service it takes a few minutes until the NTP service on Module 8030NTC is adjusted on an available NTP Server again.

6.3.4.7 Access Restrictions / Configuring the NTP Service Restrictions

One of the extended configuration options for NTP is the "Access Restrictions" (NTP access restrictions).



The screenshot shows the 'NTP' tab in the web interface. The 'Access Restrictions' sub-tab is active. It features a 'Default restriction' section with checkboxes for 'ignore', 'kod', 'noquery', 'nopeer', 'noserver', 'notrap', 'notrust', and 'version'. Below this is a 'Restrictions' section with 'Add' and 'Remove' buttons, and a table for configuring individual restrictions. The table has columns for 'IP-Address', 'Netmask', and the same restriction options as the default section.

Restrictions are used in order to control access to the System's NTP service and these are regrettably the most misunderstood options of the NTP configuration.

If you are not familiar with these options, a detailed explanation can be found at <http://www.ntp.org/>.



IP addresses should be used when configuring the restrictions – no Host-names!

The following steps show how restrictions can be configured - should these not be required it is sufficient to retain the standard settings.

The standard restrictions tell the NTP service how to handle packets of hosts (including remote time servers) and sub-network which otherwise have no special restrictions.

The NTP configuration can simplify the selection of the correct standard restrictions while making the required security available.

Before beginning the configuration the points **6.3.4.7.1** to **6.3.4.7.4** must be checked by the user:

6.3.4.7.1 NAT or Firewall

Are incoming connections to the NTP Service blocked by NAT or a Stateful Inspection Firewall?	
No	Proceed to Chapter 6.3.4.7.2 Blocking Unauthorised Access
Yes	No restrictions are required in this case. Proceed further to Chapter 6.3.4.7.4 Internal Client Protection / Local Network Threat Level

6.3.4.7.2 Blocking Unauthorised Access

Is it really necessary to block all connections from unauthorised hosts if the NTP Service is openly accessible?	
No	Proceed to Chapter 6.3.4.7.3 Allowing Client Requests
Yes	<p>In this case the following restrictions are to be used:</p> <p>ignore in the default restrictions <input checked="" type="checkbox"/></p> <p>If a standard restriction is selected in this area, exceptions can be declared in separate lines for each authorised server, client or sub-network. See Chapter 6.3.4.7.5 Addition of Exceptions to Standard</p>

6.3.4.7.3 Allowing Client Requests

Are clients to be allowed to see the server status information when they receive the time information from the NTP service (even if this is information about the module, operating system and NTPD version)?	
No	<p>In this case select from the following standard restrictions: See Chapter 6.3.4.7.6 Access Control Options</p> <p> <input checked="" type="checkbox"/> kod <input checked="" type="checkbox"/> notrap <input checked="" type="checkbox"/> nopeer <input checked="" type="checkbox"/> noquery. </p>
Yes	<p>In this case select from the following standard restrictions: See Chapter 6.3.4.7.6 Access Control Options:</p> <p> <input checked="" type="checkbox"/> kod <input checked="" type="checkbox"/> notrap <input checked="" type="checkbox"/> nopeer </p> <p>If a standard restriction is selected in this area, exceptions can be declared in separate lines for each authorised server, client or sub-network. See Chapter 6.3.4.7.5 Addition of Exceptions to Standard.</p>

6.3.4.7.4 Internal Client Protection / Local Network Threat Level

How much protection from internal network clients is required?	
Yes	<p>The following restrictions can be enabled if greater security settings than the installed authentication are required in order to protect the NTP service from the clients see Chapter 6.3.4.7.6 Access Control Options.</p> <p> <input checked="" type="checkbox"/> kod <input checked="" type="checkbox"/> notrap <input checked="" type="checkbox"/> nopeer </p>

6.3.4.7.5 Addition of Exceptions to Standard Restrictions

After the standard restrictions have been set once, certain exceptions may be necessary for special hosts/sub-networks in order to allow remote time servers and client hosts/sub-networks to contact the NTP service.

These standard restrictions are to be added in the form of restriction lines.

Access Restrictions

Default restriction
 default nomodify ☒ ignore ☒ kod ☒ noquery ☒ nopeer ☒ noserver ☒ notrap ☒ notrust ☐ version ☐

Restrictions

Add Remove

IP-Address	Netmask	ignore	kod	noquery	nopeer	noserver	notrap	notrust	version
<input type="checkbox"/> 192.168.233.199	255.255.224.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



An unrestricted access of the Time Client 8030NTC to its own NTP service is always allowed, irrespective of whether standard restrictions are ignored or not. This is necessary in order to be able to display NTP data on the web interface.

Add restriction exception: (for each remote time server)

Restrictions:

Press **ADD**

Enter the IP address of the remote time server.

Enable restrictions: e.g.

notrap / nopeer / noquery ☒

Allow **unrestricted access** to a special host (e.g. System administrator's workstation):

Restrictions:

Press **ADD**

IP address 192.168.1.101

Do not enable any restrictions

Allow a **sub-network** to receive time server and query server statistics:

Restrictions:

Press **ADD**

IP address 192.168.1.0

Network mask 255.255.255.0

notrap / nopeer ☒

6.3.4.7.6 Access Control Options

The official documentation concerning the current implementation of the restriction instructions can be found on the "Access Control Options" page at <http://www.ntp.org/>.

Numerous access control options are used. The most important of these are described in detail here.

nomodify – "Do not allow this host/sub-network to modify the NTPD settings unless it has the correct key."



Default Settings:

Always active. Can't be modified by the user.

As standard, NTP requires authentication with a symmetric key in order to carry out modifications with NTPDC. If a symmetric key is not configured for the NTP service, or if this is kept in a safe place, it is not necessary to use the nomodify option unless the authentication procedure appears to be unsafe.

noserver – "Do not transmit time to this host/sub-network."

This option is used if a host/sub-network is only allowed access to the NTP service in order to monitor or remotely configure the service.

notrust – "Ignore all NTP packets which are not encrypted."

This option tells the NTP service that all NTP packets which are not encrypted should be ignored (it should be noted that this is a change from ntp-4.1.x). The notrust option **MUST** NOT be used unless NTP Crypto (e.g. symmetric key or Autokey) has been correctly configured on both sides of the NTP connection (e.g. NTP service and remote time server, NTP service and client).

noquery – "Do not allow this host/sub-network to request the NTP service status."

The ntpd status request function, provided by ntpd/ntpd, declassifies certain information over the running ntpd Base System (e.g. operating system version, ntpd version) which under certain circumstances ought not to be made known to others. It must be decided whether it is more important to hide this information or to give clients the possibility of seeing synchronization information over ntpd.

ignore – "In this case ALL packets are refused, including ntpq and ntpdc requests".

kod – "A kiss-o'-death (KoD) packet is transmitted if this option is enabled in the case of an access error."

KoD packets are limited. They cannot be transmitted more frequently than once per second. Any KoD packet which occurs within one second from the last packet is removed.

notrap – "Denies support for the mode 6 control message trap service in order to synchronise hosts."

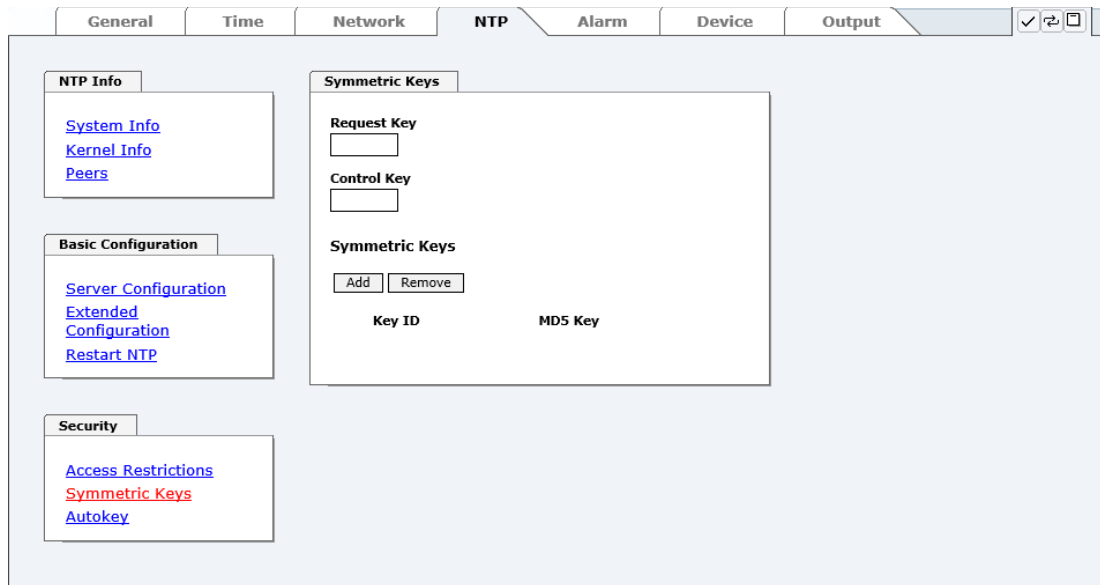
The trap service is a sub-system of the ntpq control message protocols. This service logs remote events in programmes.

version – "Denies packets which do not correspond to the current NTP version."



Changes in data do not take effect immediately after clicking on the "Apply" symbol. The NTP service **MUST** also be restarted (see **Chapter 6.3.4.6 Restart NTP**).

6.3.4.8 Symmetric Key



The screenshot shows the Hopf NTP configuration web interface. At the top, there are tabs for General, Time, Network, NTP (selected), Alarm, Device, and Output. Below the tabs, there are three main sections: NTP Info, Basic Configuration, and Security. The NTP Info section contains links for System Info, Kernel Info, and Peers. The Basic Configuration section contains links for Server Configuration, Extended Configuration, and Restart NTP. The Security section contains links for Access Restrictions, Symmetric Keys (highlighted in red), and Autokey. The Symmetric Keys section is expanded, showing fields for Request Key and Control Key, and a table for Symmetric Keys with columns for Key ID and MD5 Key. There are Add and Remove buttons for the Symmetric Keys table.

6.3.4.8.1 Why Authentication?

Most NTP users do not require authentication as the protocol contains several filters (for bad time).

Despite this, however, the use of authentication is common. There are certain reasons for this:

- Time should only be used from safe sources
- An attacker broadcasts false time signals
- An attacker poses as another time server

6.3.4.8.2 How is Authentication used in the NTP Service?

Client and server can execute an authentication whereby a code word is used on the client side and a restriction on the server side.

NTP uses keys to implement the authentication. These keys are used when data are exchanged between two machines.

In principle both sides must know this key. The key can generally be found in the `"*/etc/ntp.keys"` directory. It is unencrypted and hidden from public view. This means that the key has to be distributed on a safe route to all communication partners. The key can be downloaded for distribution under "Downloads / Configuration Files" on the DEVICE tab. It is necessary to be logged in as "Master" in order to access this.

The keyword `key` of a client's `ntp.conf` determines the key that is used to communicate with the designated server (e.g. the **hopf** NTP Time Server 8030NTS/GPS). The key must be reliable if time is to be synchronised. Authentication causes a delay. This delay is automatically taken into account and adjusted in the current versions.

6.3.4.8.3 How is a key created?

A key is a sequence of up to 31 ASCII characters. Some characters with special significance cannot be used (alphanumeric characters and the following symbols can be used: [] () * - _ ! \$ % & / = ?).

A new line can be inserted by pressing the **ADD** key. The key which is stored in the key file is entered on this line. The key ID is used to identify the key and is in the range from 1 – 65534. This means that 65534 different keys can be defined.

Duplicate key ID's are not allowed. Having now explained the principles of keys, it should be possible to use a key in practically the same way as a password.

The value of the request key field is used as the password for the ntpdc tool while the value of the control key field is used as the password for the ntpq tool.

More information is available at <http://www.ntp.org/>.

6.3.4.8.4 How does authentication work?

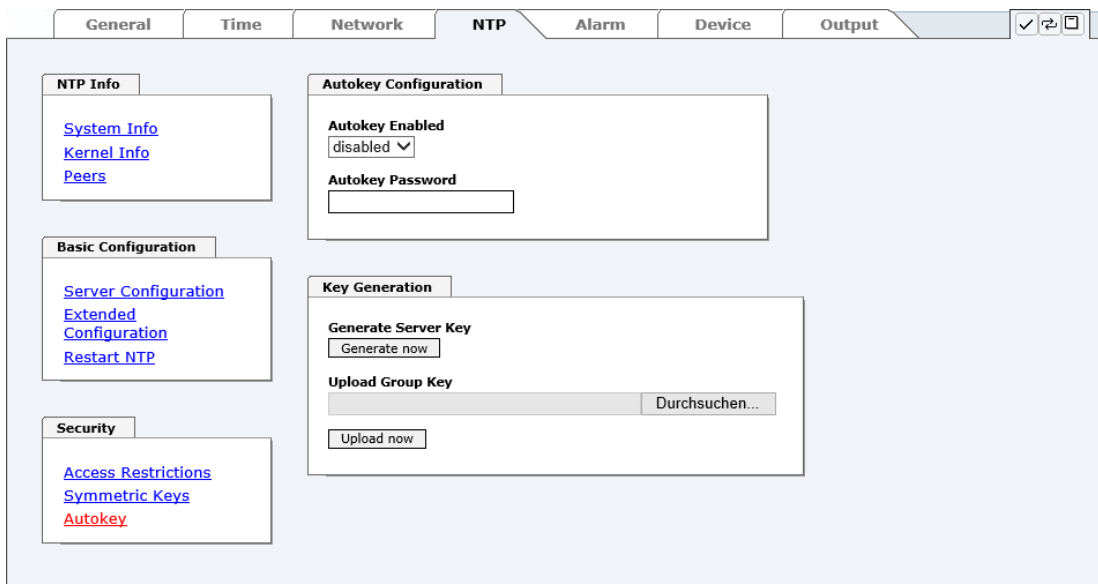
The basic authentication is a digital signature and no data encryption (if there are any differences between the two). The data packet and the key are used to create a non-reversible number which is attached to the packet.

The receiver (which has the same key) carries out the same calculation and compares the results. Authentication has been successful if the results agree.

6.3.4.9 Autokey / Public Key Cryptography

NTPv4 offers a new Autokey scheme based on **public key cryptography**.

As a basic principle, **public key cryptography** is safer than **symmetric key cryptography** as protection is based on a private value which is generated by each host and is never visible.



The screenshot shows the NTP configuration web interface. At the top, there are tabs for General, Time, Network, NTP, Alarm, Device, and Output. The NTP tab is selected. On the left, there are links for NTP Info (System Info, Kernel Info, Peers), Basic Configuration (Server Configuration, Extended Configuration, Restart NTP), and Security (Access Restrictions, Symmetric Keys, Autokey). The main content area is divided into two sections: Autokey Configuration and Key Generation. In the Autokey Configuration section, 'Autokey Enabled' is set to 'disabled' and 'Autokey Password' is empty. In the Key Generation section, there are buttons for 'Generate now', 'Upload now', and a search button labeled 'Durchsuchen...'.

In order to enable Autokey v2 authentication, the "Autokey Enabled" option must be set to "enabled" and a password specified (may not be blank).

A new server key and certificate can be generated by pressing the "Generate now" button.



Generate now

This should be carried out regularly as these keys are only valid for one year.

If the Time Client 8030NTC is to form part of an NTP trust group, a group key can be defined and uploaded with the "Upload now" button.

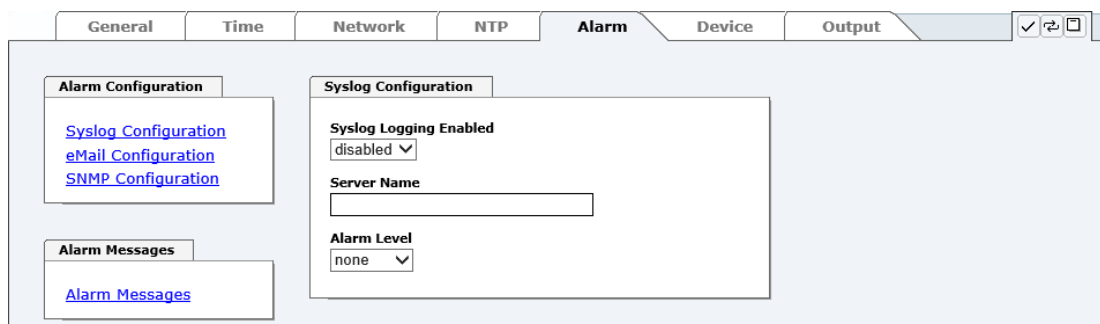
Detailed information about the NTP Autokey scheme can be found in the NTP documentation (<http://www.ntp.org/>).



Changes in data do not take effect immediately after clicking on the "Apply" symbol. The NTP service **MUST** also be restarted (see **Chapter 6.3.4.6 Restart NTP**).

6.3.5 ALARM Tab

All the links within the tabs on the left hand side lead to corresponding detailed setting options.



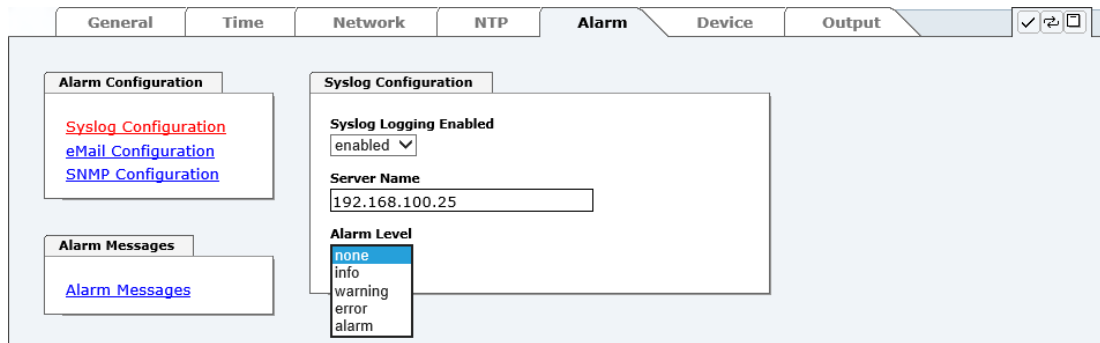
6.3.5.1 Syslog Configuration

It is necessary to enter the name or IP address of a Syslog server in order to store every configured alarm situation which occurs on the Board in a Linux/Unix Syslog. If everything is configured correctly and enabled (dependent on the Syslog level), every message is transmitted to the Syslog server and stored in the Syslog file there.

Syslog uses Port 514.

Co-logging on the Board itself is not possible as the flash memory is not of sufficient size.

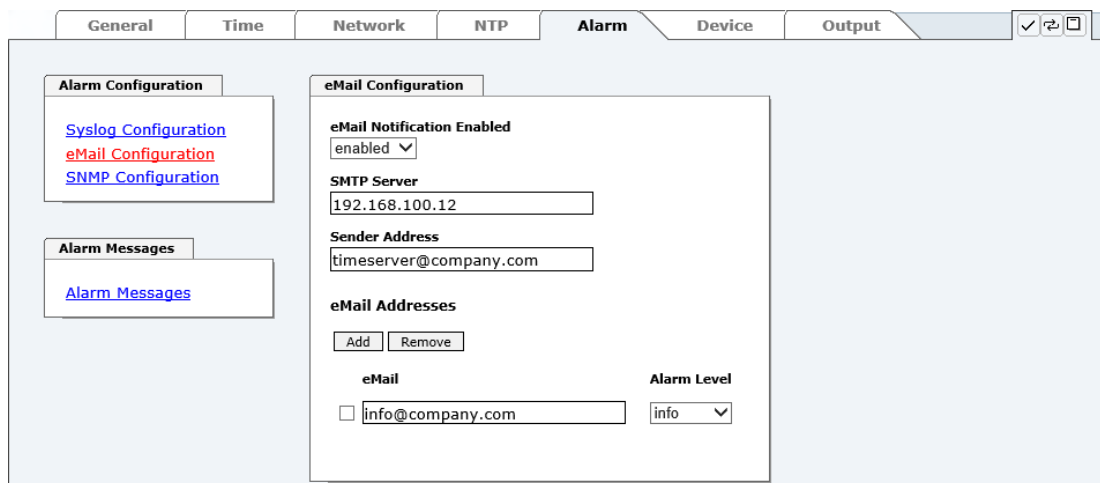
It should be noted that the standard Linux/Unix Syslog mechanism is used for this functionality. This is not the same as the Windows System Event mechanism!



The alarm level designates the priority level of the messages to be transmitted and the level from which transmission is to take place (see **Chapter 6.3.5.4 Alarm**).

Alarm Level	Transmitted Messages
none	no messages
info	info / warning / error / alarm
warning	warning / error / alarm
error	error / alarm
alarm	alarm

6.3.5.2 E-mail Configuration



E-mail notification is one of the important features of this device which offer technical personnel the opportunity to monitor and/or control the IT environment.

It is possible to configure various, independent E-mail addresses which each have different alarm levels.

Dependent on the configured level, an E-mail is sent after an error has occurred on the respective receiver.

A valid E-mail server (SMTP server) must be entered for the purpose of correct configuration.

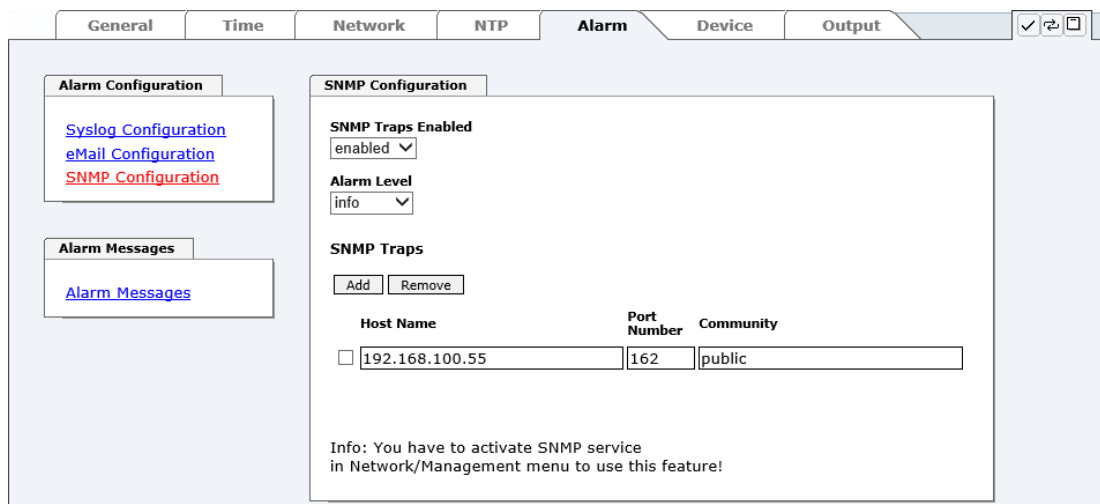
Some E-mail servers only accept messages if the sender address entered is valid (spam protection). This can be inserted in the "Sender Address" field.

The Alarm Level designates the priority level of the messages to be sent and the level from which they are to be sent (see **Chapter 6.3.5.4 Alarm**).

Alarm Level	Transmitted Messages
none	no messages
info	info / warning / error / alarm
warning	warning / error / alarm
error	error / alarm
alarm	alarm

6.3.5.3 SNMP Configuration / TRAP Configuration

It is possible to use an SNMP agent (with MIB) or to configure SNMP traps in order to monitor the Board over SNMP.



SNMP traps are sent to the configured hosts over the network. It should be noted that these are based on UDP and therefore it is not certain that they will reach the configured host!

Several hosts can be configured. However, all have the same alarm level.

The private **hopf** enterprise MIB is also available over the web (see **Chapter 6.3.6.10 Downloading SNMP MIB / Configuration Files**).

The "Alarm Level" designates the priority level of the messages to be sent and the level from which they are to be sent (see **Chapter 6.3.5.4 Alarm**).

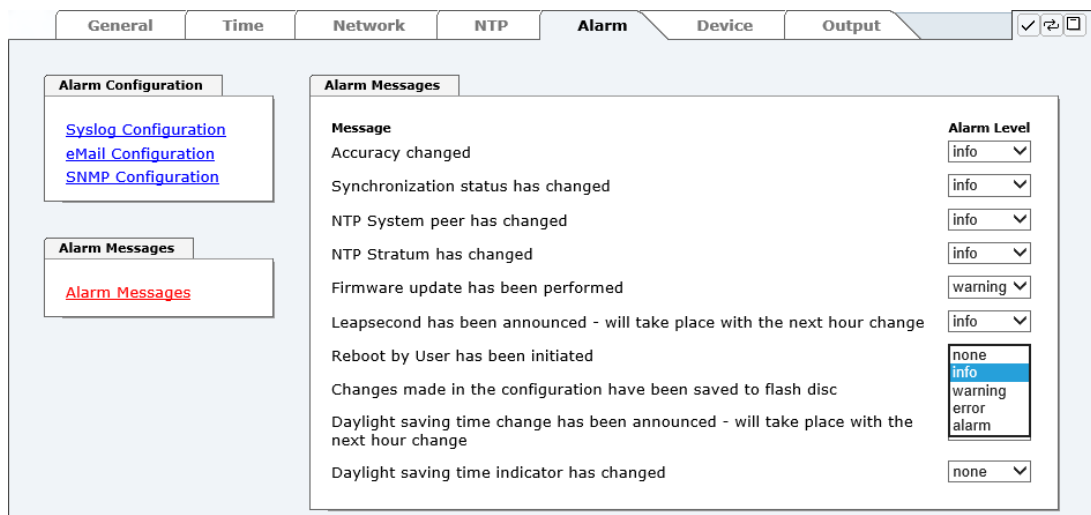
Alarm Level	Transmitted Messages
none	no messages
info	info / warning / error / alarm
warning	warning / error / alarm
error	error / alarm
alarm	alarm



SNMP protocol must be enabled in order to use SNMP (see **Chapter 6.3.3.6 Management (Management-Protocols – HTTP, SNMP, SNMP-Traps, etc.)**).

6.3.5.4 Alarm Messages

Every message shown in the image can be configured with the displayed alarm levels. If level NONE is selected this means that this message is completely ignored.



Message	Alarm Level
Accuracy changed	info
Synchronization status has changed	info
NTP System peer has changed	info
NTP Stratum has changed	info
Firmware update has been performed	warning
Leapsecond has been announced - will take place with the next hour change	info
Reboot by User has been initiated	none
Changes made in the configuration have been saved to flash disc	info
Daylight saving time change has been announced - will take place with the next hour change	warning
Daylight saving time indicator has changed	none

A corresponding action is carried out if an event occurs, depending on the messages, their configured levels and the configured notification levels of the E-mails.



Modified settings are failsafe stored after **Apply** and **Save** only.

6.3.6 DEVICE Tab

All the links within the tabs on the left hand side lead to corresponding detailed setting options.

This tab provides the basic information about the module hardware and software/firmware. Password administration and the update services for the module are also made accessible via this website. The complete download zone is also a component of this site.

6.3.6.1 Device Information

All information is available exclusively in write-protected and read-only form. Information about the Board type, serial number and current software versions is provided to the user for service and enquiry purposes.

General	Time	Network	NTP	Alarm	Device	Output
<div><div>Device</div><div>Device Info Hardware Info Factory Defaults Custom Defaults Reboot Device Hardware Reset Image Update H8 Firmware Update Upload Certificate Customized Security Banner Product Activation Diagnostics</div></div> <div><div>Device Info</div><div><p>Device Type 8030NTC</p><p>Device Uptime 0 days 23 hours 38 minutes</p><p>Serial Number 8030019992</p><p>Image Version 02.02 (P1) Build 0821 (Development)</p><p>Image Program Date 03.11.2016 08:37 UTC</p></div></div>						

6.3.6.2 Hardware Information

Read-only access is provided here in the same way as for device information.

The user requires this information in the case of service requests, e.g. MACH version, hardware status etc.

[illegible]

6.3.6.3 Restoring Factory-Settings (Factory Defaults)

In some cases it might be wished to restore all settings of the Module 8030NTC to their factory-settings (factory defaults).



This function enables the restoring of all settings from the flash memory to their factory default values. This also affects passwords (see **Chapter 9 Factory Defaults**).

The registration is conducted as Master user according to the manual, **Chapter 6.2.1 LOGIN and LOGOUT as User**.

By pressing "Reset now" factory default values are set.

There is NO chance to restore the deleted configuration once this process is triggered.



After a **Factory Default** a complete verification and a possibly new configuration of the Module 8030NTC are required. Especially the default MASTER and DEVICE passwords should be reset.

6.3.6.4 Reboot Device



All settings not saved with "Save" are lost on reset (see **Chapter 6.2.3 Enter or Changing Data**).

In broad terms, the **NTP service** implemented on the Board is restarted. This leads to a renewed alignment phase with the loss of the stability and accuracy reached up to this point.

Please log in as a "Master" user in accordance with the description in **Chapter 6.2.1 LOGIN and LOGOUT as User**.

Press the "Reset now" button and wait until the restart has been completed.

This procedure can take up to one minute. The website is not automatically updated.

6.3.6.5 Image Update & H8 Firmware Update

Patches and error recovery are provided for the individual modules by means of updates.

Both the embedded image and the H8 firmware can only be downloaded to the Board via the web interface (login as "Master" user required). See also **Chapter 4.4 Firmware Update**.



The following points should be noted regarding updates:

- Only experienced users or trained technical personnel should carry out an update after checking all necessary preconditions.
- Important: **Faulty updates** or **update attempts** may under certain circumstances require the Board to be returned to the factory for rectification at the owner's expense.
- Check that the update on hand is suitable for your Board. If in doubt please consult the support of the **hopf** company.
- In order to guarantee a correct update, the "**New version of saved site**" function must be set to "**On each access to the site**" in the Internet browser used.
- During the update procedure, the device **must not be switched off** and **settings must not be saved to the flash memory!**
- Updates are **always** executed as software set. I.e. H8 firmware update + image update. Unless specifically defined otherwise in the SET, it is absolutely essential to complete the H8 firmware update first, followed by the image update.
- For the Update please pay attention to the points in **Chapter 4.4 Firmware Update**.

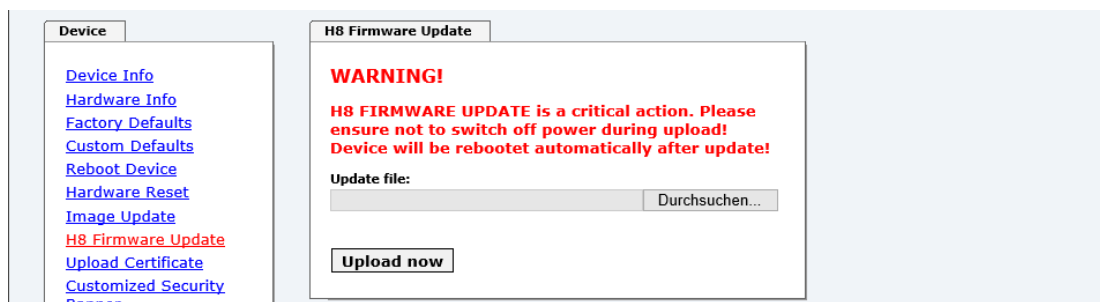
In order to carry out an update, enter the name and the folder in which the update / firmware image is located in the text field or open the file selection dialogue by pressing the "Browse" button.

Correct firmware and image designations are (e.g.):

H8-8030NTC_v0100_128.mot for the **H8 firmware**
(update takes approx. 1-1.5 minutes)

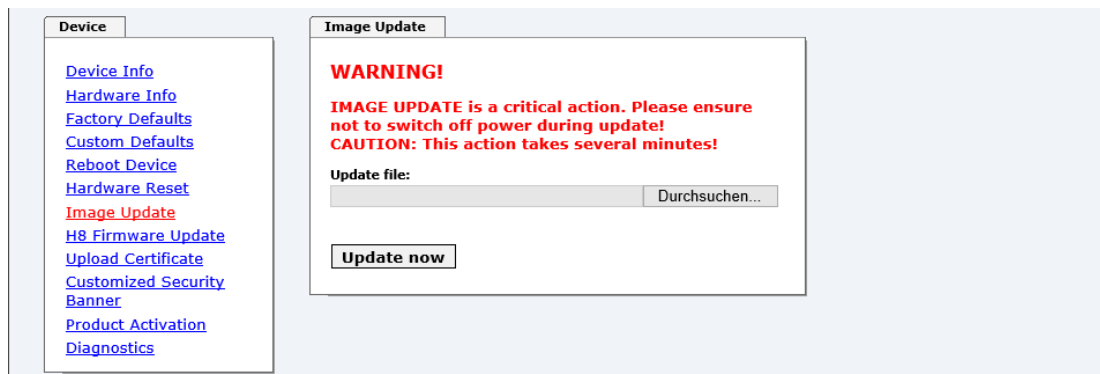
upgrade_8030_v0200_Release.img for the **embedded image**
(update takes approx. 7-8 minutes)

The update process is started by pressing the "**Update now**" button. The update is installed if the transfer and checksum test are successful. A success page is displayed and shows the number of bytes that have been transferred and installed.



A restart of the Board with the new Firmware is done automatically after the H8-Firmware update.

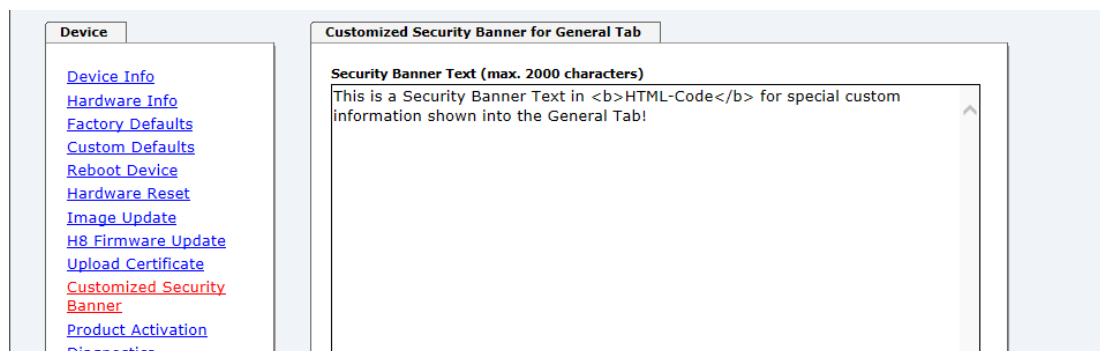
The procedure for the **Image update** differs only in how the module is restarted.



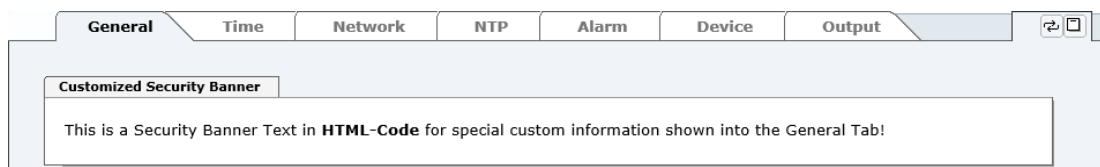
After the image-update the WebGUI displays a window to confirm the restart (reboot) of the board.

6.3.6.6 Customized Security Banner

Special security information displayed in the General tab can be entered here by the user.



The security information can be written as 'unformatted' text as well as in HTML format. There are 2000 characters available to write failsafe into the Time Client 8030NTC.



After a successful storage the "Customized Security Banner" with the saved security information is displayed in the General-Tab.

To delete the "Customized Security Banner" the inserted text must be deleted and saved again.

6.3.6.7 Product Activation

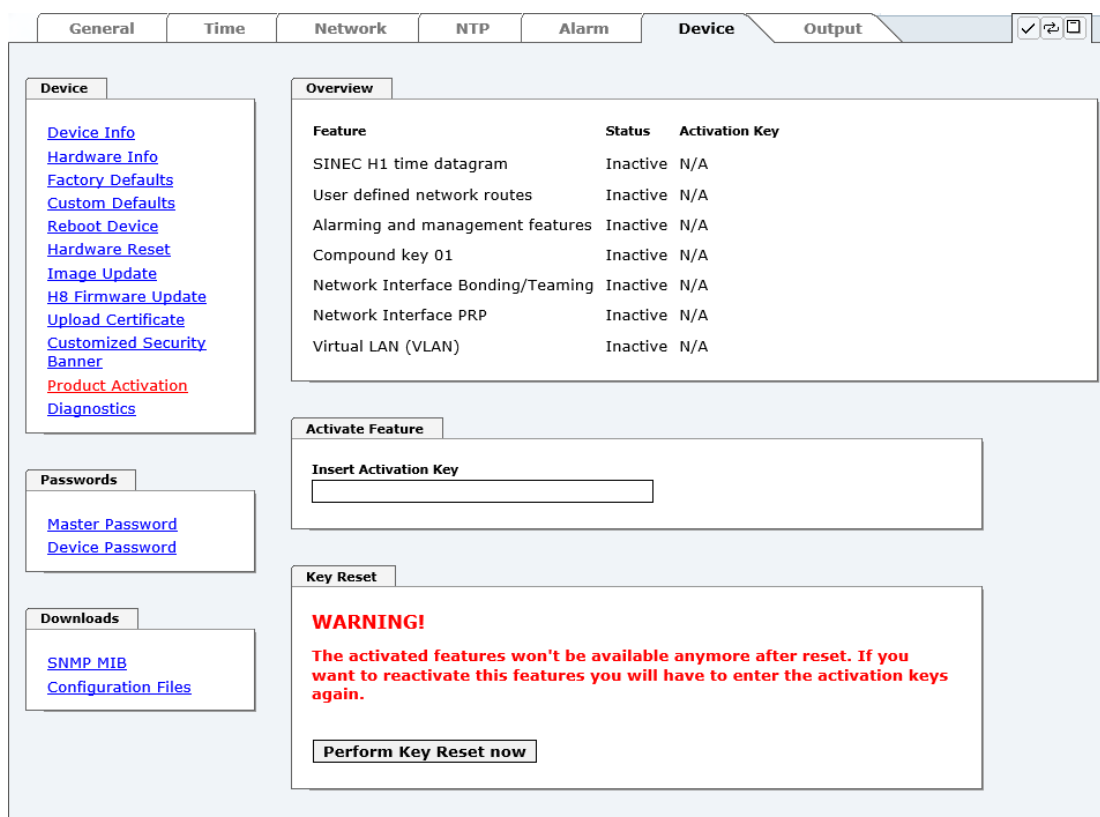
For the activation of optional functions, e.g. "alarming" or "SINEC H1 time datagram", a special activation key is required for which an order with the **hopf** Elektronik GmbH can be placed. Each activation key is related to a special board with an appropriate serial number and cannot be used for several boards.



For a subsequent order of an activation key the serial number of the Module 8030NTC (device) needs to be provided. The serial number can be found under the tab DEVICE – Device info (serial number 8030...).



The settings for activation keys (e.g. an entered activation key) are neither deleted nor restored via the functions FACTORY DEFAULTS and CUSTOM DEFAULTS.



The screenshot shows the 'Device' tab in the web interface. It includes a sidebar with links like 'Device Info', 'Hardware Info', 'Factory Defaults', 'Custom Defaults', 'Reboot Device', 'Hardware Reset', 'Image Update', 'H8 Firmware Update', 'Upload Certificate', 'Customized Security Banner', 'Product Activation', and 'Diagnostics'. The main area has an 'Overview' section with a table of features and their activation status.

Feature	Status	Activation Key
SINEC H1 time datagram	Inactive	N/A
User defined network routes	Inactive	N/A
Alarming and management features	Inactive	N/A
Compound key 01	Inactive	N/A
Network Interface Bonding/Teaming	Inactive	N/A
Network Interface PRP	Inactive	N/A
Virtual LAN (VLAN)	Inactive	N/A

Below the table, there is an 'Activate Feature' section with an 'Insert Activation Key' input field. At the bottom, there is a 'Key Reset' section with a red 'WARNING!' message: 'The activated features won't be available anymore after reset. If you want to reactivate this features you will have to enter the activation keys again.' and a 'Perform Key Reset now' button.

Overview

Full listing of all optional functions with the current activation status and stored activation key

Activate Feature

Input field to enter a new activation key. After entering the feature is activated by pressing the ☒ Apply button.

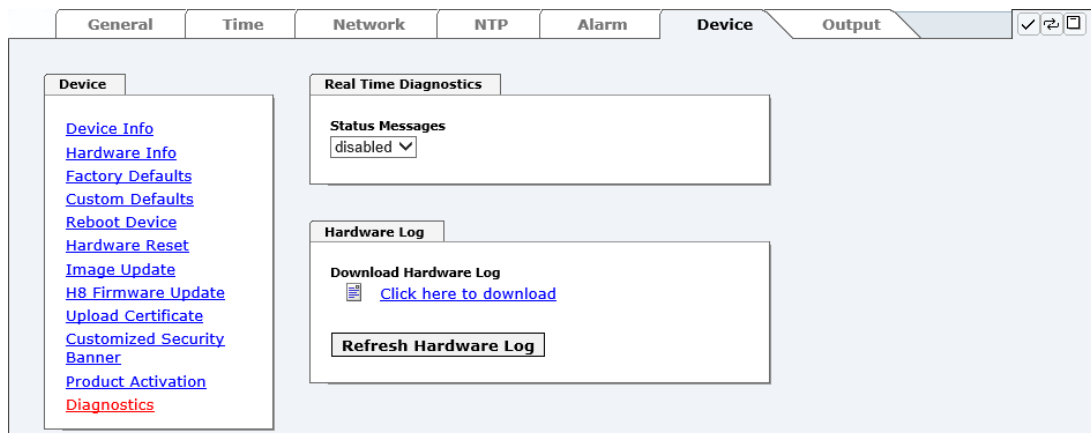
If the activation was successful the new feature is listed in the overview with status "Active" and can be used immediately.

Key Reset

Clears all activation keys and sets all optional features to status “Inactive”. All other non-optional features are still available after performing the key reset. If an optional feature is enabled again, the last stored configuration for this feature is restored.

6.3.6.8 Diagnostics Function

If "status messages" is enabled the output is processed as SYSLOG message. This function should only be used/enabled in case a problem arises and after consulting the **hopf** support.



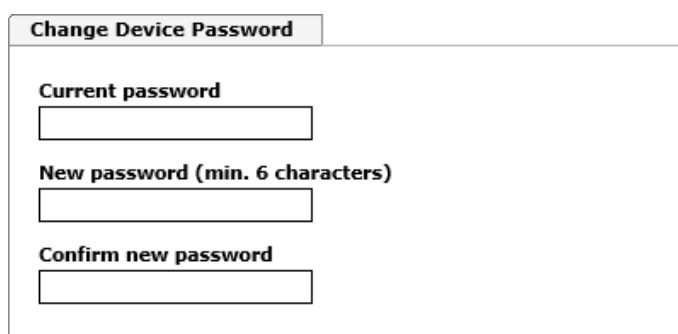
The screenshot shows the 'Device' tab in the Hopf WebGUI. On the left, a sidebar lists various configuration options: Device Info, Hardware Info, Factory Defaults, Custom Defaults, Reboot Device, Hardware Reset, Image Update, H8 Firmware Update, Upload Certificate, Customized Security Banner, Product Activation, and Diagnostics (highlighted in red). The main content area is titled 'Real Time Diagnostics'. It contains a 'Status Messages' section with a dropdown menu currently set to 'disabled'. Below this is a 'Hardware Log' section with a 'Download Hardware Log' button and a link 'Click here to download'. At the bottom of the Hardware Log section is a 'Refresh Hardware Log' button.

6.3.6.9 Passwords Master / Device

Differentiation is made between upper and lower case characters in passwords. In principle, all alphanumeric characters and the following symbols are allowed in passwords:

[] () * - _ ! \$ % & / = ?

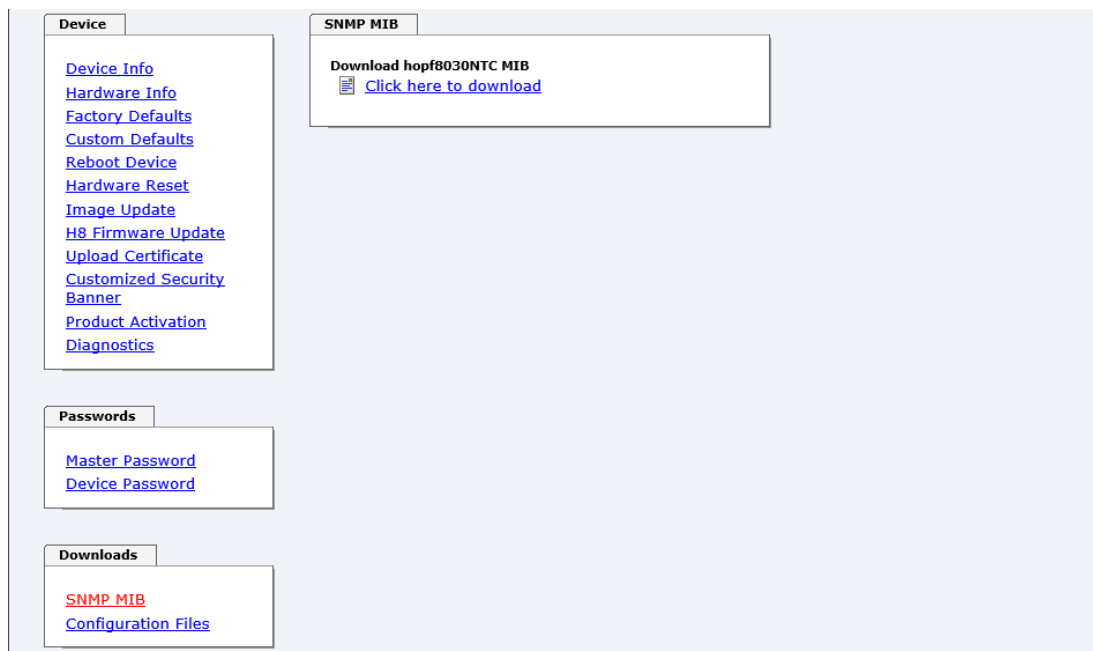
(See also **Chapter 6.2.1 LOGIN and LOGOUT as User**)



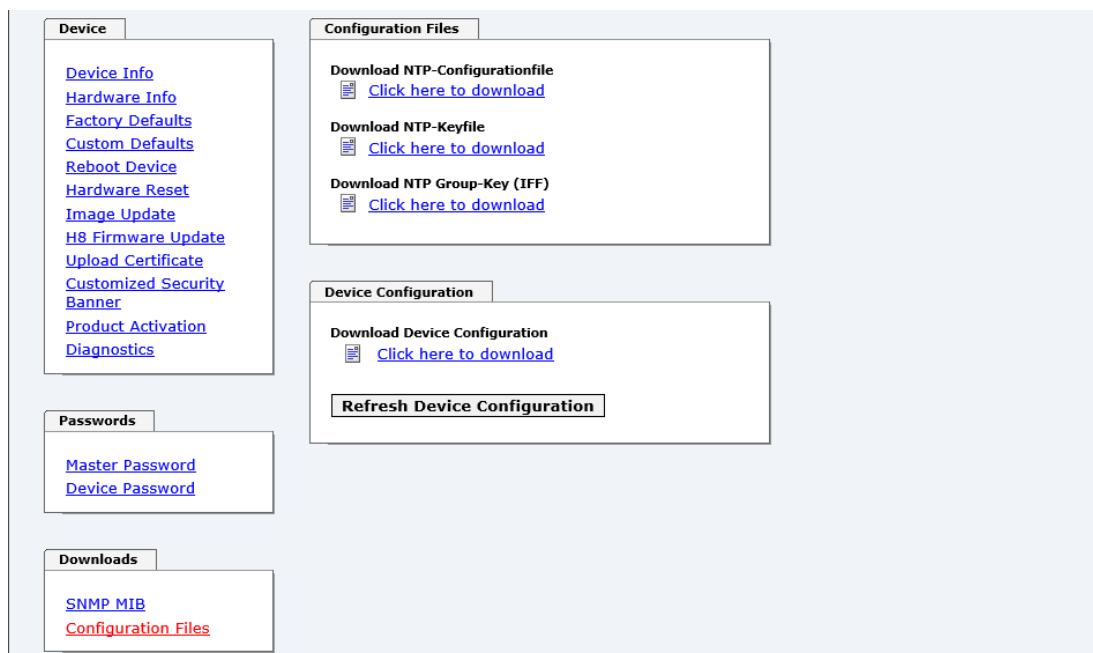
The screenshot shows the 'Change Device Password' form. It has three input fields: 'Current password', 'New password (min. 6 characters)', and 'Confirm new password'. Each field is represented by a text box with a label above it.

6.3.6.10 Downloading SNMP MIB / Configuration Files

The "private **hopf** enterprise MIB" is available via the WebGUI in this area.



In order to be able to download certain configuration files via the web interface it is necessary to be logged on as a "Master" user.



6.3.7 OUTPUT Tab

This Chapter describes the additional functions of the Time Client 8030NTC.

The WebGUI identifies the actual available device specific signal generators and only displays the corresponding tabs like (PPS / DCF77 / IRIG-B / ...).

The delivery status of the customer specific device can be found in the accompanying configuration documentation.



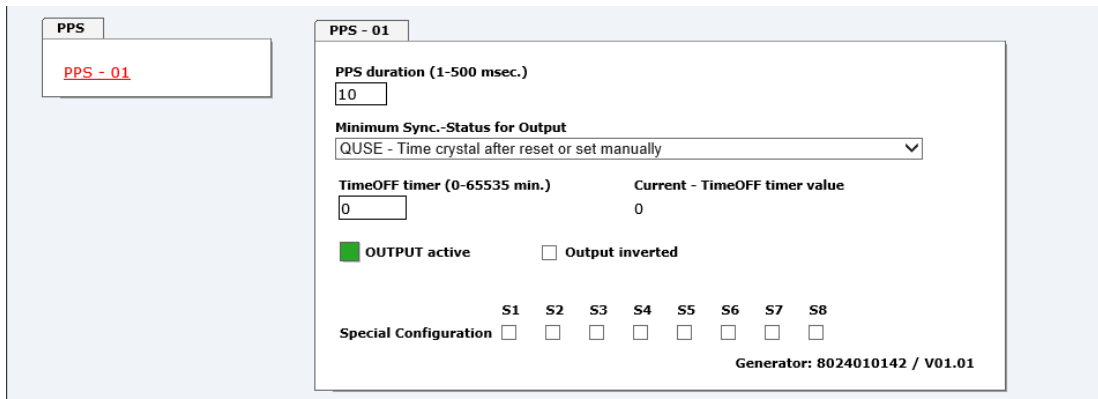
Subsequent activation of the Output functionality is **not** possible on site.

6.3.7.1 PPS (Optional Hardware necessary)

The signal generation for the output of a PPS pulse (1Hz) may be configured in this panel.



For the output of this signal additional hardware (at system level) is required (see system manual if applicable).



The screenshot shows the PPS configuration interface. On the left, a sidebar has a 'PPS' tab selected, with 'PPS - 01' listed below it. The main panel is titled 'PPS - 01' and contains the following settings:

- PPS duration (1-500 msec.):** A text input field containing '10'.
- Minimum Sync.-Status for Output:** A dropdown menu showing 'QUSE - Time crystal after reset or set manually'.
- TimeOFF timer (0-65535 min.):** A text input field containing '0'.
- Current - TimeOFF timer value:** A text input field containing '0'.
- OUTPUT active:** A green square checkbox that is checked.
- Output inverted:** An unchecked checkbox.
- Special Configuration:** A row of eight checkboxes labeled S1 through S8, all of which are unchecked.
- Generator:** A label at the bottom right indicating '8024010142 / V01.01'.

6.3.7.1.1 PPS duration

This section serves to select the pulse width to be transmitted. Basically it is possible to specify the pulse width in milliseconds.

Possible values for the **pulse duration**:

- Minimum: 1 msec
- Maximum: 500 msec

6.3.7.1.2 Minimum Sync.-Status for Output

Signal output can be configured only to be generated when the Time Client 8030NTC has reached a minimum synchronization status. As soon as this minimum synchronization status drops below this value during operation, the signal output stops unless the TimeOFF Timer has been set greater than 0. In this case the output is done for the duration of the TimeOFF Timer despite the minimum synchronization status for the output falls below the configured value.

Range of Sync.-Status

The synchronization status is represented from the bottom of the following table up with increasing quality.

Synchronisation Status	SYNC	Time synchronized + quartz control started/running
	SYOF	Time synchronized + SyncOFF running
	SYSI	Time synchronized as simulation mode (with no actual GPS reception)
	QUON	Quartz/crystal time + SyncON running
	QUEX	Quartz/crystal time (in freewheel after synchronization failure ⇒ Board was already synchronized)
	QUSE	Quartz/crystal time after reset or manually set
	INVA	Invalid time

Value range TimeOFF timer = 0 to 65635min.

6.3.7.1.3 Status of the Signal Output

The status of the output is stated via a display element with the following color and text indications:

GREEN	OUTPUT active	There is a signal output
YELLOW	OUTPUT + TimeOFF active	There is a signal output for the duration of the TimeOFF Timer
RED	OUTPUT blocked	There is no signal output

6.3.7.1.4 Output inverted

All outputs stated in the system manuals of the according devices are related to the DEFAULT setting: Output not inverted.

If nevertheless the inverting of the output signal has to be configured the "Output inverted" checkbox has to be enabled.

6.3.7.1.5 Special Configuration

If used, the correct settings are described in the additional system manual of the customer-specific device.

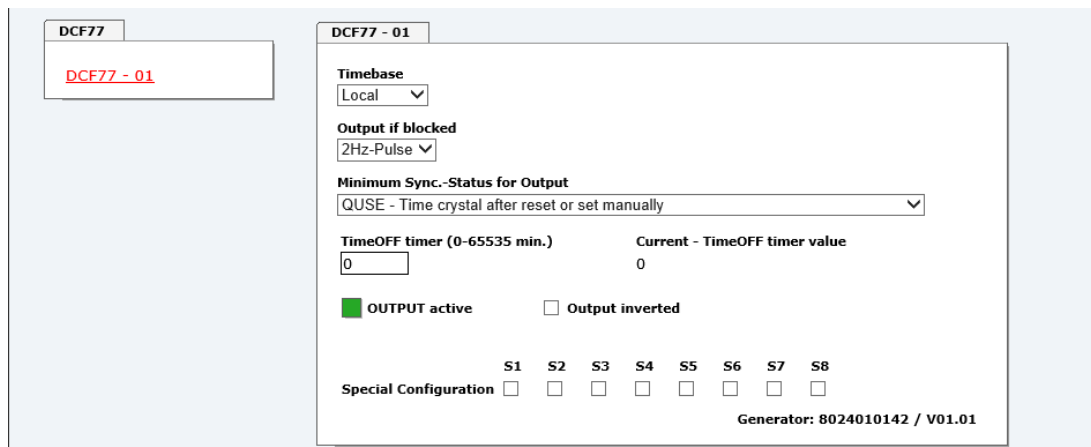
Otherwise for S1-S8 the DEFAULT-setting (all checkboxes disabled) should not be changed due to compatibility reasons.

6.3.7.2 DCF77 (Optional Hardware necessary)

The signal generation for the output of a DCF77 pulse (1Hz) may be configured in this panel.



For the output of this signal additional hardware (at system level) is required (see system manual if applicable).



6.3.7.2.1 Timebase

Timebase	Local Time
	Standard Time
	UTC Time

In general the local time is set as the base. This time leaps forward/back 1 hour every daylight saving time changeover. The standard or UTC time must be selected as the base if automatic daylight saving time changeover shall be suppressed.

When setting standard time (winter time), the time offset to local summer time is minus 1 hour. Standard time runs continuously (without time leap) throughout the whole year.

When setting UTC, the world time (formerly GMT) is used as the time base. This time base also runs continuously (without time leap) throughout the whole year.

6.3.7.2.2 Output if blocked

Using this menu item the interference reaction of the DCF77 pulse can be controlled unless the system status is lower than the reference value.

Fault signal	2 Hz Pulse: If the system status is lower than the reference value, a 2Hz pulse instead of the DCF77 pulse is provided.
	No Signal If the system status is lower than the reference value there is <u>no</u> signal output.



Transmission of a 2Hz pulse in the event of a fault allows the connected devices to monitor for line breakage.

6.3.7.2.3 Minimum Sync.-Status for Output

The signal output can be adjusted only to be generated when the Sync Module has reached a minimum synchronization status. As soon as this minimum synchronization status drops below this value during operation, the signal output stops unless the TimeOFF Timer has been set greater than 0. In this case the output is done for the duration of the TimeOFF Timer despite the minimum synchronization status for the output falls below the set value.

Range of Sync.-Status

The synchronization status is represented from the bottom of the following table up with increasing quality.

Synchronisation Status	SYNC	Time synchronized + quartz control started/running
	SYOF	Time synchronized + SyncOFF running
	SYSI	Time synchronized as simulation mode (with no actual GPS reception)
	QUON	Quartz/crystal time + SyncON running
	QUEX	Quartz/crystal time (in freewheel after synchronization failure ⇒ Board was already synchronized)
	QUSE	Quartz/crystal time after reset or manually set
	INVA	Invalid time

Value range TimeOFF timer = 0 to 65635min.

6.3.7.2.4 Status of the Signal Output

The status of the output is stated via a display element with the following color and text indications:

GREEN	OUTPUT active	There is a signal output
YELLOW	OUTPUT + TimeOFF active	There is a signal output for the duration of the TimeOFF Timer
RED	OUTPUT blocked	There is no signal output

6.3.7.2.5 Output inverted

All outputs stated in the system manuals of the according devices are related to the DEFAULT setting: Output not inverted.

If nevertheless the inverting of the output signal has to be configured the "Output inverted" checkbox has to be enabled.

6.3.7.2.6 Special Configuration

If used, the correct settings are described in the additional system manual of the customer-specific device.

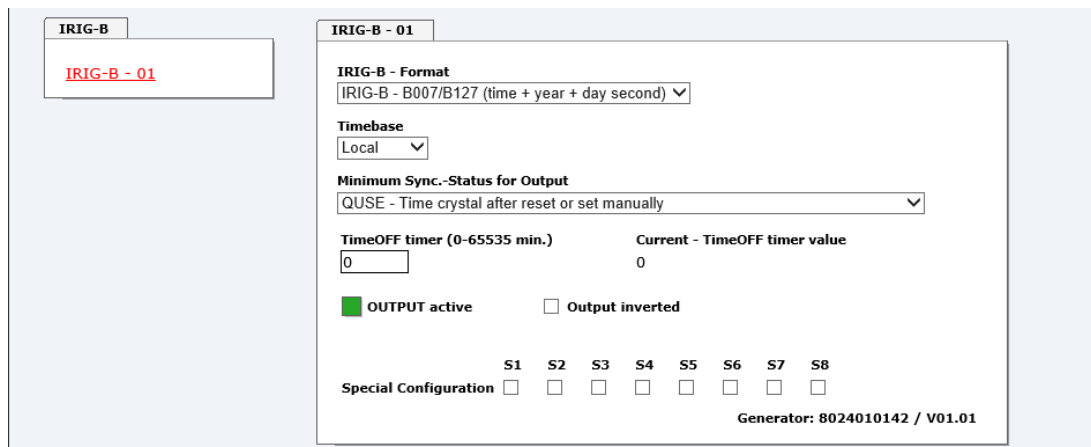
Otherwise for S1-S8 the DEFAULT-setting (all checkboxes disabled) should not be changed due to compatibility reasons.

6.3.7.3 IRIG-B (Optional Hardware necessary)

The signal generation for the output of an IRIG-B signal may be configured in this panel.



For the output of this signal additional hardware (at system level) is required (see system manual if applicable).



6.3.7.3.1 IRIG-B - Format

Following IRIG-B output formats are available:

Selection of Output Format IRIG-B / IEEE C37.118 / AFNOR
IRIG-B / B007+B127 (time, year, second of the day)
IRIG-B / B003+B123(time, second of the day)
IRIG-B / B006+B126 (time, year)
IRIG-B / B002+B122 (time)
IEEE C37.118 (previously IEEE 1344)
AFNOR NF S87-500

6.3.7.3.2 Timebase

Timebase	Local Time
	Standard Time
	UTC Time

In general the local time is set as the base. This time leaps forward/back 1 hour every daylight saving time changeover. The standard or UTC time must be selected as the base if automatic daylight saving time changeover shall be suppressed.

When setting standard time (winter time), the time offset to local summer time is minus 1 hour. Standard time runs continuously (without time leap) throughout the whole year.

When setting UTC, the world time (formerly GMT) is used as the time base. This time base also runs continuously (without time leap) throughout the whole year.

6.3.7.3.3 Minimum Sync.-Status for Output

The signal output can be adjusted only to be generated when the Sync Module has reached a minimum synchronization status. As soon as this minimum synchronization status drops below this value during operation, the signal output stops unless the TimeOFF Timer has been

set greater than 0. In this case the output is done for the duration of the TimeOFF Timer despite the minimum synchronization status for the output falls below the set value.

Range of Sync.-Status

The synchronization status is represented from the bottom of the following table up with increasing quality.

Synchronisation Status	SYNC	Time synchronized + quartz control started/running
	SYOF	Time synchronized + SyncOFF running
	SYSI	Time synchronized as simulation mode (with no actual GPS reception)
	QUON	Quartz/crystal time + SyncON running
	QUEX	Quartz/crystal time (in freewheel after synchronization failure ⇒ Board was already synchronized)
	QUSE	Quartz/crystal time after reset or manually set
	INVA	Invalid time

Value range TimeOFF timer = 0 to 65635min.

6.3.7.3.4 Status of the Signal Output

The status of the output is stated via a display element with the following color and text indications:

GREEN	OUTPUT active	There is a signal output
YELLOW	OUTPUT + TimeOFF active	There is a signal output for the duration of the TimeOFF Timer
RED	OUTPUT blocked	There is no signal output

6.3.7.3.5 Output inverted

All outputs stated in the system manuals of the according devices are related to the DEFAULT setting: Output not inverted.

If nevertheless the inverting of the output signal has to be configured the "Output inverted" checkbox has to be enabled.

6.3.7.3.6 Special Configuration

If used, the correct settings are described in the additional system manual of the customer-specific device.

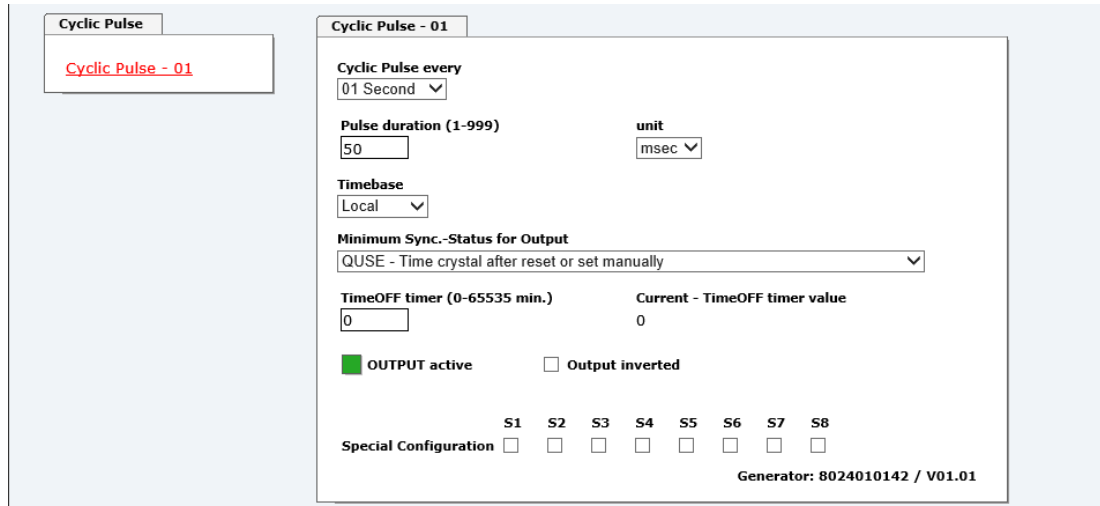
Otherwise for S1-S8 the DEFAULT-setting (all checkboxes disabled) should not be changed due to compatibility reasons.

6.3.7.4 Cyclic Pulse (Optional Hardware necessary)

The signal generation for the output of cyclic pulses may be configured in this panel.



For the output of this signal additional hardware (at system level) is required (see system manual if applicable).



The screenshot shows the 'Cyclic Pulse' configuration panel. On the left, a sidebar lists 'Cyclic Pulse' and 'Cyclic Pulse - 01'. The main panel is titled 'Cyclic Pulse - 01' and contains the following settings:

- Cyclic Pulse every:** 01 Second (dropdown)
- Pulse duration (1-999):** 50 (input field)
- unit:** msec (dropdown)
- Timebase:** Local (dropdown)
- Minimum Sync.-Status for Output:** QUSE - Time crystal after reset or set manually (dropdown)
- TimeOFF timer (0-65535 min.):** 0 (input field)
- Current - TimeOFF timer value:** 0 (display)
- OUTPUT active:** ☒ (checkbox)
- Output inverted:** ☐ (checkbox)
- Special Configuration:** S1, S2, S3, S4, S5, S6, S7, S8 (checkboxes)
- Generator:** 8024010142 / V01.01

6.3.7.4.1 Cyclic Pulse every

This section is used to select the pulse to be transmitted. Possible pulses are:

- Pulses every second: every 1, 2, 3, 4, 5, 6, 10, 12, 15, 20 or 30 seconds
- Pulses every minute: every 1, 2, 3, 4, 5, 6, 10, 12, 15, 20 or 30 minutes
- Pulses every hour: every 1, 2, 3, 4, 6, 8, 12 or 24 hours

6.3.7.4.2 Pulse duration (1-999)

This section is used to select the pulse width to be transmitted. Basically it is possible to specify the pulse width in milliseconds or seconds.

Possible values for the **pulse duration**:

- Minimum: 1
- Maximum: 999

Possible values for the **pulse duration unit**:

- Second (sec)
- Millisecond (msec)



Certain inputs are automatically corrected:

- Value > 999 are automatically corrected to 999.
- The pulse lengths must be at least 20msec shorter than the pulse interval.

6.3.7.4.3 Timebase

Timebase	Local Time
	Standard Time
	UTC Time

In general the local time is set as the base. This time leaps forward/back 1 hour every daylight saving time changeover. The standard or UTC time must be selected as the base if automatic daylight saving time changeover shall be suppressed.

When setting standard time (winter time), the time offset to local summer time is minus 1 hour. Standard time runs continuously (without time leap) throughout the whole year.

When setting UTC, the world time (formerly GMT) is used as the time base. This time base also runs continuously (without time leap) throughout the whole year.

6.3.7.4.1 Minimum Sync.-Status for Output

The signal output can be adjusted only to be generated when the Sync Module has reached a minimum synchronization status. As soon as this minimum synchronization status drops below this value during operation, the signal output stops unless the TimeOFF Timer has been set greater than 0. In this case the output is done for the duration of the TimeOFF Timer despite the minimum synchronization status for the output falls below the set value.

Range of Sync.-Status

The synchronization status is represented from the bottom of the following table up with increasing quality.

Synchronisation Status	SYNC	Time synchronized + quartz control started/running
	SYOF	Time synchronized + SyncOFF running
	SYSI	Time synchronized as simulation mode (with no actual GPS reception)
	QUON	Quartz/crystal time + SyncON running
	QUEX	Quartz/crystal time (in freewheel after synchronization failure ⇒ Board was already synchronized)
	QUSE	Quartz/crystal time after reset or manually set
	INVA	Invalid time

Value range TimeOFF timer = 0 to 65635min.

6.3.7.4.2 Status of the Signal Output

The status of the output is stated via a display element with the following color and text indications:

GREEN	OUTPUT active	There is a signal output
YELLOW	OUTPUT + TimeOFF active	There is a signal output for the duration of the TimeOFF Timer
RED	OUTPUT blocked	There is no signal output

6.3.7.4.3 Output inverted

All outputs stated in the system manuals of the according devices are related to the DEFAULT setting: Output not inverted.

If nevertheless the inverting of the output signal has to be configured the "Output inverted" checkbox has to be enabled.

6.3.7.4.4 Special Configuration

If used, the correct settings are described in the additional system manual of the customer-specific device.

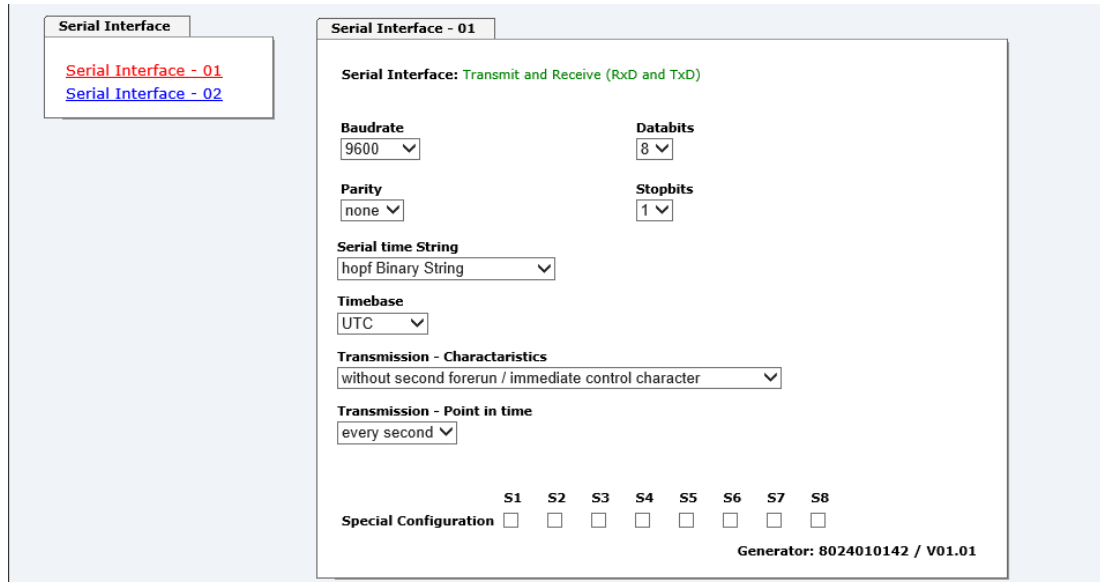
Otherwise for S1-S8 the DEFAULT-setting (all checkboxes disabled) should not be changed due to compatibility reasons.

6.3.7.5 Serial Interface (Optional Hardware necessary)

The serial data string generation may be configured in this panel.



For the output of serial data string additional hardware (at system level) is required (see system manual if applicable).



The screenshot shows the 'Serial Interface' configuration panel. On the left, there are links for 'Serial Interface - 01' and 'Serial Interface - 02'. The main panel is titled 'Serial Interface - 01' and contains the following settings:

- Serial Interface:** Transmit and Receive (Rx/D and Tx/D)
- Baudrate:** 9600
- Databits:** 8
- Parity:** none
- Stopbits:** 1
- Serial time String:** hopf Binary String
- Timebase:** UTC
- Transmission - Characteristics:** without second forerun / immediate control character
- Transmission - Point in time:** every second
- Special Configuration:** S1, S2, S3, S4, S5, S6, S7, S8 (all checkboxes are unchecked)
- Generator:** 8024010142 / V01.01

6.3.7.5.1 Serial Interface



Data strings are available by selection to change automatically the serial parameter.

Baud Rate

- 9600 baud
- 1200 baud
- 4800 baud
- 9600 baud
- 19200 baud
- 38400 baud
- 57600 baud
- 115000 baud

Databits

Possible settings are:

- 8 for 8 databits
- 7 for 7 databits

Parity

Possible settings are:

- No Parity
- Even Parity
- Odd Parity

Stopbits

Possible settings are:

- 1 for 1 stopbit
- 2 for 2 stopbits

6.3.7.5.2 Timebase

Timebase	Local Time
	Standard Time
	UTC Time

In general the local time is set as the base. This time leaps forward/back 1 hour every daylight saving time changeover. The standard or UTC time must be selected as the base if automatic daylight saving time changeover shall be suppressed.

When setting standard time (winter time), the time offset to local summer time is minus 1 hour. Standard time runs continuously (without time leap) throughout the whole year.

When setting UTC, the world time (formerly GMT) is used as the time base. This time base also runs continuously (without time leap) throughout the whole year.

6.3.7.5.3 Output scheme

The output scheme for the transmission must be selected here:

- Without second forerun / immediate control character
- With second forerun / immediate control character
- With second forerun / control character every second
- With second forerun / control character delayed every second

6.3.7.5.4 Transmission Time

- Every Second
- EveryMinute
- Every Hour
- Remote

6.3.7.5.5 Special Configuration

If used, the correct settings are described in the additional system manual of the customer-specific device.

Otherwise for S1-S8 the DEFAULT-setting (all checkboxes disabled) should not be changed due to compatibility reasons.

6.3.7.5.6 Serial time String

The string output for the transmission must be selected here:

- **hopf** Binäre String
- **hopf** time Universal
- **hopf** Master/Slave-String
- **hopf** Standard String (6021)
- Trimble Time String (TSIP)
- SINEC H1 Extended
- SAT 1703 Time String
- ABB Melody (CR/LF)
- ABB Melody (LF/CR)

6.3.7.5.6.1 **hopf** Binary String

The **hopf** Binary String can be used to synchronize slave systems with the time data of the master system.

Required:	<ul style="list-style-type: none"> • Transmission Time every second • With second forerun / control character every second • UTC time • 9600 baud, 8 bit, 1 stop bit, no parity
------------------	---

Example:

(STX):TIME:80;0233D88F08;07E0;003C;F4108014*6B(CR)(LF) (ETX)

6.3.7.5.6.2 **hopf** time Universal

The **hopf** time Universal String can be used to synchronize slave systems with the time data of the master system.

Required:	<ul style="list-style-type: none"> • Transmission Time every second • With second forerun / control character every second • 9600 baud, 8 bit, 1 stop bit, no parity
------------------	---

Example:

(STX)731144501904201602+0000FFFF*23(CR)(LF) (ETX)

6.3.7.5.6.3 **hopf** Master/Slave-String

The **hopf** Master/Slave-String can be used to synchronize slave systems with the time data of the master system.

The **hopf** Master/Slave-String transmits:

- the full time information (hour, minute, second)
- the date (day, month, year [2 digits])
- the difference time local to UTC (hour, minute)
- the day of the week
- status information (announcement of DST changeover, announcement of a leap second and the status of reception of the **hopf** Master/Slave-String source)

6.3.7.5.6.3.1 Specified Settings

Required:	<p>The following settings are required for the synchronization of the hopf slave-systems:</p> <ul style="list-style-type: none"> • output second forerun • ETX on the second change; selectable: data string at the beginning or at the end of the 59. second. • local time • 9600 baud, 8 bit, 1 stop bit, no parity
------------------	--



Received data on the serial interface that are not specified in the pertinent data string might disturb and interrupt the cyclic string output. The receiving synchronization interface should be set to "transmitting on request" for Sub-Master (Slave) Systems.

6.3.7.5.6.3.2 Structure

Character No.	Meaning	Hex-Value
1	STX (start of text)	\$02
2	status	\$30-39, \$41-46
3	day of the week	\$31-37
4	tens hour	\$30-32
5	unit hour	\$30-39
6	tens minute	\$30-35
7	unit minute	\$30-39
8	tens second	\$30-36
9	unit second	\$30-39
10	tens day	\$30-33
11	unit day	\$30-39
12	tens month	\$30-31
13	unit month	\$30-39
14	tens year	\$30-39
15	unit year	\$30-39
16	difference time tens hour / operational sign	\$30-31, \$38-39
17	difference time unit hour	\$30-39
18	difference time tens minutes	\$30-35
19	difference time unit minutes	\$30-39
20	LF (line feed)	\$0A
21	CR (carriage Return)	\$0D
22	ETX (end of text)	\$03

The difference time (time zone offset) is transmitted in hours and minutes following the year. The transmission is done in BCD. The difference time may be up to $\pm 14.00h$.

The operational sign is shown as the highest bit in the hours.

logic **1** = local time before UTC

logic **0** = local time after UTC

Example:

Data String	Tens Difference Time Nibble	Difference Time
(STX)83123456030196 <u>0</u> 300(LF)(CR)(ETX)	<u>0000</u>	- 03:00h
(STX)83123456030196 <u>1</u> 100(LF)(CR)(ETX)	<u>0001</u>	- 11:00h
(STX)83123456030196 <u>8</u> 230(LF)(CR)(ETX)	<u>1000</u>	+ 02:30h
(STX)83123456030196 <u>9</u> 100(LF)(CR)(ETX)	<u>1001</u>	+ 11:00h

6.3.7.5.6.3.3 Status

	b3	b2	b1	b0	Meaning
Status:	x	x	x	0	no announcement hour
	x	x	x	1	announcement (DST changeover)
	x	x	0	x	standard time
	x	x	1	x	daylight saving time (DST)
	x	0	x	x	no announcement leap second
	x	1	x	x	announcement leap second
	0	x	x	x	synchronization status code: INVA / QUSE / QUEX / QUON
	1	x	x	x	synchronization status code: SYOF / SYNC
Day of the Week:	0	0	0	1	Monday
	0	0	1	0	Tuesday
	0	0	1	1	Wednesday
	0	1	0	0	Thursday
	0	1	0	1	Friday
	0	1	1	0	Saturday
	0	1	1	1	Sunday

Status	Operating Mode	Time	DST changeover	Leap Second
0 = 0000	INVA / QUSE / QUEX / QUON	standard time	no announcement	no announcement
1 = 0001	INVA / QUSE / QUEX / QUON	standard time	announcement	no announcement
2 = 0010	INVA / QUSE / QUEX / QUON	DST	no announcement	no announcement
3 = 0011	INVA / QUSE / QUEX / QUON	DST	announcement	no announcement
4 = 0100	INVA / QUSE / QUEX / QUON	standard time	no announcement	announcement
5 = 0101	INVA / QUSE / QUEX / QUON	standard time	announcement	announcement
6 = 0110	INVA / QUSE / QUEX / QUON	DST	no announcement	announcement
7 = 0111	INVA / QUSE / QUEX / QUON	DST	announcement	announcement
8 = 1000	SYOF / SYNC	standard time	no announcement	no announcement
9 = 1001	SYOF / SYNC	standard time	announcement	no announcement
A = 1010	SYOF / SYNC	DST	no announcement	no announcement
B = 1011	SYOF / SYNC	DST	announcement	no announcement
C = 1100	SYOF / SYNC	standard time	no announcement	announcement
D = 1101	SYOF / SYNC	standard time	announcement	announcement
E = 1110	SYOF / SYNC	DST	no announcement	announcement
F = 1111	SYOF / SYNC	DST	announcement	announcement

DST = daylight saving time

6.3.7.5.6.3.4 Example

(STX)841234561807028230(LF)(CR)(ETX)

- It is Thursday 18.07.2002 - 12:34:56 o'clock
- synchronization status code: SYNC
- no announcement of a changeover
- The difference time to UTC is +2.30 h

6.3.7.5.6.4 **hopf** Standard String (6021)

Below the **hopf** Standard String is described.

6.3.7.5.6.4.1 Specified Settings

Required:	no
------------------	-----------

6.3.7.5.6.4.2 Structure

Character No.	Meaning	Hex-Value
1	STX (start of text)	\$02
2	status (internal clock status)	\$30-39, \$41-46
3	day of the week (1=Monday ... 7=Sunday) for UTC time bit 3 is set to 1 in the day of the week	\$31-37
4	tens hour	\$30-32
5	unit hour	\$30-39
6	tens minute	\$30-35
7	unit minute	\$30-39
8	tens second	\$30-36
9	unit second	\$30-39
10	tens day	\$30-33
11	unit day	\$30-39
12	tens month	\$30-31
13	unit month	\$30-39
14	tens year	\$30-39
15	unit year	\$30-39
16	LF (line feed)	\$0A
17	CR (carriage return)	\$0D
18	ETX (end of text)	\$03

6.3.7.5.6.4.3 Status

The second and the third ASCII-character contain the status and the day of the week.
The status is decoded binary.

	b3	b2	b1	b0	Meaning
Status:	x	x	x	0	no announcement hour
	x	x	x	1	announcement (DST changeover)
	x	x	0	x	standard time
	x	x	1	x	daylight saving time (DST)
	0	0	x	x	synchronization status code: INVA
	0	1	x	x	synchronization status code: QUSE / QUEX / QUON
	1	0	x	x	synchronization status code: SYOF
	1	1	x	x	synchronization status code: SYNC
Day of the Week:	0	x	x	x	CEST / CET
	1	x	x	x	UTC - time
	x	0	0	1	Monday
	x	0	1	0	Tuesday
	x	0	1	1	Wednesday
	x	1	0	0	Thursday
	x	1	0	1	Friday
	x	1	1	0	Saturday
	x	1	1	1	Sunday

Status	operation mode	time	announcement SZ-WZ-SZ
0 = 0000	INVA	winter	no announcement
1 = 0001	INVA	winter	announcement
2 = 0010	INVA	summer	no announcement
3 = 0011	INVA	summer	announcement
4 = 0100	QUSE / QUEX / QUON	winter	no announcement
5 = 0101	QUSE / QUEX / QUON	winter	announcement
6 = 0110	QUSE / QUEX / QUON	summer	no announcement
7 = 0111	QUSE / QUEX / QUON	summer	announcement
8 = 1000	SYOF	winter	no announcement
9 = 1001	SYOF	winter	announcement
A = 1010	SYOF	summer	no announcement
B = 1011	SYOF	summer	announcement
C = 1100	SYNC	winter	no announcement
D = 1101	SYNC	winter	announcement
E = 1110	SYNC	summer	no announcement
F = 1111	SYNC	summer	announcement

6.3.7.5.6.4.4 Example

(STX)E4123456180702(LF)(CR)(ETX)

- It is Thursday 18.07.2002 - 12:34:56 o'clock.
- synchronization status code: SYNC
- daylight saving time
- no announcement of a changeover
- () - ASCII-control characters e.g. (STX)

6.3.7.5.6.5 Trimble Time String (TSIP)

The Trimble Time String (TSIP) can be used to synchronize slave systems with the time data of the master system.

Example in Hex description (not ASCII):

[illegible]

6.3.7.5.6.6 SINEC H1 Extended

Below the data string SINEC H1 Extended is described.

String request

The data string SINEC H1 Extended can also be sent by request. The time of output shall be configured to "send only by request" and the string will be requested with the ASCII character "?".

6.3.7.5.6.6.1 Specified Settings

Required:	no
------------------	-----------

6.3.7.5.6.6.2 Structure

Character No.	Meaning	Hex-Value
1	STX (start of text)	\$02
2	"D" ASCII D	\$44
3	":" colon	\$3A
4	tens day	\$30-33
5	unit day	\$30-39
6	":" point	\$2E
7	tens month	\$30-31
8	unit month	\$30-39
9	":" point	\$2E
10	tens year	\$30-39
11	unit year	\$30-39
12	"," semicolon	\$3B
13	"T" ASCII T	\$54
14	":" colon	\$3A
15	day of the week	\$31-37
16	"," semicolon	\$3B
17	"U" ASCII U	\$55
18	":" colon	\$3A
19	tens hour	\$30-32
20	unit hour	\$30-39
21	":" point	\$2E
22	tens minute	\$30-35
23	unit minutes	\$30-39
24	":" point	\$2E
25	tens second	\$30-36
26	unit second	\$30-39
27	"," semicolon	\$3B
28	"#" or " " (space)	\$23 / \$20
29	"*" or " " (space)	\$2A / \$20
30	"S", "U" or " " (space)	\$53 / \$55 / \$20
31	!", "A" or " " (space)	\$21 / \$41 / \$20
32	ETX (end of text)	\$03

6.3.7.5.6.6.3 Status

The characters 28-31 in the data string SINEC H1 Extended tell the synchronization status of the Time Client 8030NTC.

The characters mean the following:

character no. 28 = "#"	no synchronisation after reset, time invalid "synchronization status code: INVA"
" " (space)	synchronisation after reset, clock in crystal operation "synchronization status code: QUSE / QUEX / QUON / SYOF / SYNC"
character no. 29 = "**"	time from internal crystal in the clock "synch. status code: INVA / QUSE / QUEX / QUON"
" " (space)	time by synchronisation "synchronization status code: SYOF / SYNC"
character no. 30 = "S"	daylight saving time
"U"	UTC
" " (space)	standard time
character no. 31 = "!"	announcement of a DST or standard time changeover
"A"	announcement of a leap second
" " (space)	no announcement

6.3.7.5.6.6.4 Example

(STX)D:18.07.02;T:4;U:12.34.56; _ _ _ _ (ETX) (_) = Space

- It is Thursday 18.07.02 - 12:34:56 o'clock
- The clock is synchronous (synchronization status code: SYNC)
- standard time (winter time)
- no announcement of a changeover

6.3.7.5.6.7 SAT 1703 Time String

All modes can be transmitted with the SAT 1703 Time String (e.g. with forerun or end character at second change).

The SAT 1703 Time String can also be sent on request. The point of transmission shall be set to "transmission on request". The SAT 1703 Time String may be requested with ASCII-character "?".

6.3.7.5.6.7.1 Specified Settings

Required:	no
------------------	-----------

6.3.7.5.6.7.2 Structure

Character No.	Meaning	Hex-Value	
1	STX (start of text)	\$02	
2	tens day	\$30-33	
3	unit day	\$30-39	
4	". "	\$2E	
5	tens month	\$30-31	
6	unit month	\$30-39	
7	". "	\$2E	
8	tens year	\$30-39	
9	unit year	\$30-39	
10	"/"	\$2F	
11	unit day of the week	\$31-37	
12	"/"	\$2F	
13	tens hours	\$30-32	
14	unit hours	\$30-39	
15	". "	\$3A	
16	tens minutes	\$30-35	
17	unit minutes	\$30-39	
18	". "	\$3A	
19	tens seconds	\$30-35	
20	unit seconds	\$30-39	
21	"M" or "M" or "U"	(Standard time, Daylight saving time or UTC)	\$4D, \$4D, \$55
22	"E" or "E" or "T"		\$45, \$45, \$54
23	"Z" or "S" or "C"		\$5A, \$53, \$43
24	" " or "Z" or " "		\$20, \$5A, \$20
25	" " (\$20 ⇨ synchronous) or "*" (\$2A ⇨ not synchronous)	\$20 \$2A	
26	" " (\$20 ⇨ no announcement) or "! " (\$21 ⇨ announcement of a DST or standard time changeover)	\$20 \$21	
27	CR (carriage return)	\$0D	
28	LF (line feed)	\$0A	
29	ETX	\$03	

6.3.7.5.6.7.3 Status

The characters 21-26 in the SAT 1703 Time String indicate the synchronisation status of the Time Client 8030NTC.

The characters mean the following:

Character no. 21-24 =	"MESZ"	Central European Summertime (Daylight Saving Time)
	"MEZ "	Central European Time (standard time / winter time)
	"UTC "	Coordinated Universal Time
Character no. 25 =	"*"	time from internal crystal in the clock
	" " (space)	time by synchronisation
		"synchronization status code: INVA / QUSE / QUEX / QUON"
		"synchronization status code: SYOF / SYNC"
Character no. 26 =	"!"	announcement of a DST or standard time changeover
	" " (space)	no announcement

6.3.7.5.6.7.4 Example

(STX)18.07.02/4/02:34:45UTC_ _ _ (CR)(LF)(ETX)

- It is Thursday 18.07.02 - 02:34:45 o'clock UTC
- The clock is synchronous (synchronization status code: SYNC)

6.3.7.5.6.8 ABB Melody (CR/LF)

Below the ABB Melody DataString is described.

6.3.7.5.6.8.1 Specified Settings

Required:	<p>The following settings are required for the synchronization:</p> <ul style="list-style-type: none"> • Output every minute • Output without second forerun • Output without ETX on the second change • UTC time • 9600 baud, 8 bit, 2 stop bit, parity even
------------------	--

6.3.7.5.6.8.2 Structure

Character No.	Meaning	Hex-Value
1	STX (start of text)	\$02
2	status (internal clock status)	\$30-39, \$41-46
3	day of the week (1=Monday ... 7=Sunday) for UTC time bit 3 is set to 1 in the day of the week	\$31-37
4	tens hour	\$30-32
5	unit hour	\$30-39
6	tens minute	\$30-35
7	unit minute	\$30-39
8	tens second	\$30-36
9	unit second	\$30-39
10	tens day	\$30-33
11	unit day	\$30-39
12	tens month	\$30-31
13	unit month	\$30-39
14	tens year	\$30-39
15	unit year	\$30-39
16	CR (carriage return)	\$0D
17	LF (line feed)	\$0A
18	ETX (end of text)	\$03

6.3.7.5.6.8.3 Status

The second and the third ASCII-character contain the status and the day of the week.
The status is decoded binary.

	b3	b2	b1	b0	Meaning
Status:	x	x	x	0	no announcement hour
	x	x	x	1	announcement (DST changeover)
	x	x	0	x	standard time
	x	x	1	x	daylight saving time (DST)
	0	0	x	x	synchronization status code: INVA
	0	1	x	x	synchronization status code: QUSE / QUEX / QUON
	1	0	x	x	synchronization status code: SYOF
	1	1	x	x	synchronization status code: SYNC
Day of the Week:	0	x	x	x	CEST / CET
	1	x	x	x	UTC - time
	x	0	0	1	Monday
	x	0	1	0	Tuesday
	x	0	1	1	Wednesday
	x	1	0	0	Thursday
	x	1	0	1	Friday
	x	1	1	0	Saturday
	x	1	1	1	Sunday

Status	operation mode	time	announcement SZ-WZ-SZ
0 = 0000	INVA	winter	no announcement
1 = 0001	INVA	winter	announcement
2 = 0010	INVA	summer	no announcement
3 = 0011	INVA	summer	announcement
4 = 0100	QUSE / QUEX / QUON	winter	no announcement
5 = 0101	QUSE / QUEX / QUON	winter	announcement
6 = 0110	QUSE / QUEX / QUON	summer	no announcement
7 = 0111	QUSE / QUEX / QUON	summer	announcement
8 = 1000	SYOF	winter	no announcement
9 = 1001	SYOF	winter	announcement
A = 1010	SYOF	summer	no announcement
B = 1011	SYOF	summer	announcement
C = 1100	SYNC	winter	no announcement
D = 1101	SYNC	winter	announcement
E = 1110	SYNC	summer	no announcement
F = 1111	SYNC	summer	announcement

6.3.7.5.6.8.4 Example

(STX)CC123456210416(CR)(LF)(ETX)

- It is Thursday 21.04.2016 - 12:34:56 o'clock.
- synchronization status code: SYNC
- UTC
- no announcement of a changeover
- () - ASCII-control characters e.g. (STX)

6.3.7.5.6.9 ABB Melody (LF/CR)

Below the ABB Melody DataString is described.

6.3.7.5.6.9.1 Specified Settings

Required:	<p>The following settings are required for the synchronization:</p> <ul style="list-style-type: none"> • Output every minute • Output without second forerun • Output without ETX on the second change • UTC time • 9600 baud, 8 bit, 2 stop bit, parity even
------------------	--

6.3.7.5.6.9.2 Structure

Character No.	Meaning	Hex-Value
1	STX (start of text)	\$02
2	status (internal clock status)	\$30-39, \$41-46
3	day of the week (1=Monday ... 7=Sunday) for UTC time bit 3 is set to 1 in the day of the week	\$31-37
4	tens hour	\$30-32
5	unit hour	\$30-39
6	tens minute	\$30-35
7	unit minute	\$30-39
8	tens second	\$30-36
9	unit second	\$30-39
10	tens day	\$30-33
11	unit day	\$30-39
12	tens month	\$30-31
13	unit month	\$30-39
14	tens year	\$30-39
15	unit year	\$30-39
16	LF (line feed)	\$0A
17	CR (carriage return)	\$0D
18	ETX (end of text)	\$03

6.3.7.5.6.9.3 Status

The second and the third ASCII-character contain the status and the day of the week.
The status is decoded binary.

	b3	b2	b1	b0	Meaning
Status:	x	x	x	0	no announcement hour
	x	x	x	1	announcement (DST changeover)
	x	x	0	x	standard time
	x	x	1	x	daylight saving time (DST)
	0	0	x	x	synchronization status code: INVA
	0	1	x	x	synchronization status code: QUSE / QUEX / QUON
	1	0	x	x	synchronization status code: SYOF
	1	1	x	x	synchronization status code: SYNC
Day of the Week:	0	x	x	x	CEST / CET
	1	x	x	x	UTC - time
	x	0	0	1	Monday
	x	0	1	0	Tuesday
	x	0	1	1	Wednesday
	x	1	0	0	Thursday
	x	1	0	1	Friday
	x	1	1	0	Saturday
	x	1	1	1	Sunday

Status	operation mode	time	announcement SZ-WZ-SZ
0 = 0000	INVA	winter	no announcement
1 = 0001	INVA	winter	announcement
2 = 0010	INVA	summer	no announcement
3 = 0011	INVA	summer	announcement
4 = 0100	QUSE / QUEX / QUON	winter	no announcement
5 = 0101	QUSE / QUEX / QUON	winter	announcement
6 = 0110	QUSE / QUEX / QUON	summer	no announcement
7 = 0111	QUSE / QUEX / QUON	summer	announcement
8 = 1000	SYOF	winter	no announcement
9 = 1001	SYOF	winter	announcement
A = 1010	SYOF	summer	no announcement
B = 1011	SYOF	summer	announcement
C = 1100	SYNC	winter	no announcement
D = 1101	SYNC	winter	announcement
E = 1110	SYNC	summer	no announcement
F = 1111	SYNC	summer	announcement

6.3.7.5.6.9.4 Example

(STX)CD123456220416(LF)(CR)(ETX)

- It is Friday 22.04.2016 - 12:34:56 o'clock.
- synchronization status code: SYNC
- UTC
- no announcement of a changeover
- () - ASCII-control characters e.g. (STX)

7 SSH and Telnet Basic Configuration



Only basic configuration is possible via SSH or Telnet. The complete configuration of the Module 8030NTC takes place exclusively via the WebGUI.

It is just as easy to use SSH (Port 22) or Telnet (Port 23) as the WebGUI. Both protocols use the same user interface and menu structure.

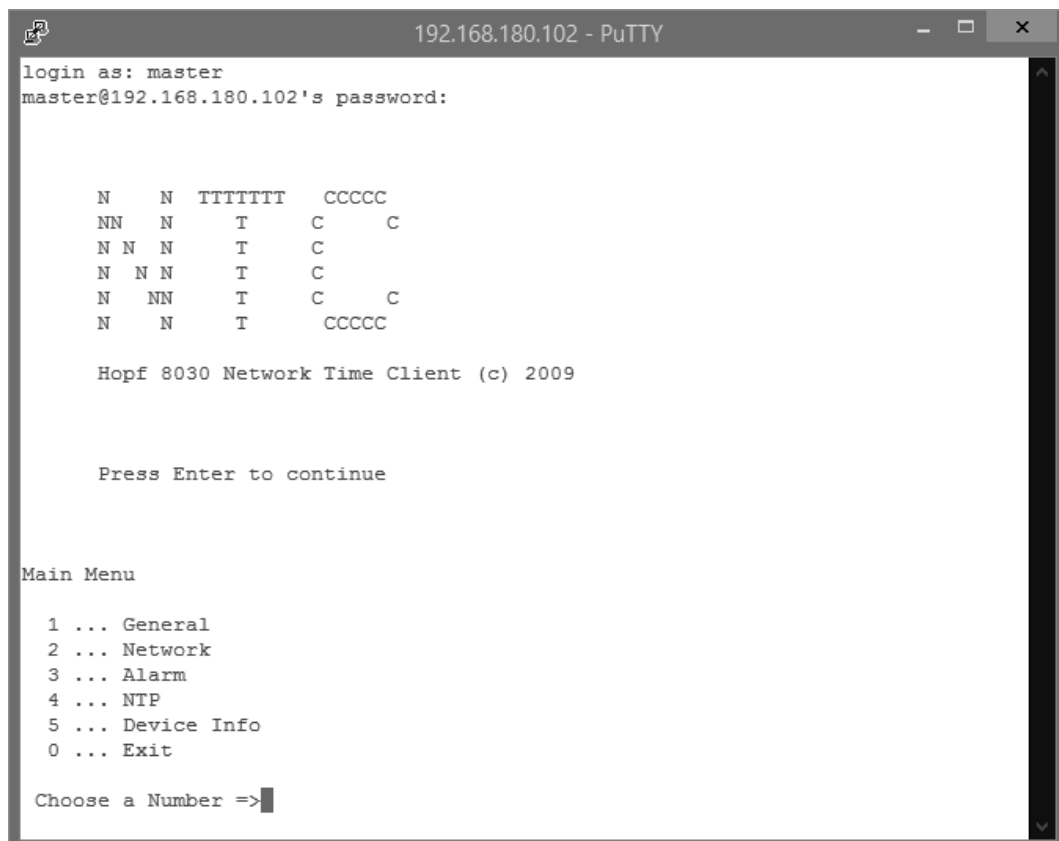
The user names and passwords are the same as on the WebGUI and are kept in alignment (see **Chapter 6.3.6.9 Passwords** Master / Device).



SSH does not allow blank passwords for safety reasons.



The corresponding protocols should be enabled for the use of Telnet or SSH (see **Chapter 6.3.3.6 Management (Management-Protocols – HTTP, SNMP, SNMP-Traps, etc.)**)).



```

192.168.180.102 - PuTTY
login as: master
master@192.168.180.102's password:

      N   N   TTTTTT   CCCCC
     NN   N       T    C    C
    N N   N       T    C
   N  N  N       T    C
  N   NN   T    C    C
 N    N    T    CCCCC

Hopf 8030 Network Time Client (c) 2009

Press Enter to continue

Main Menu

1 ... General
2 ... Network
3 ... Alarm
4 ... NTP
5 ... Device Info
0 ... Exit

Choose a Number =>
  
```

The navigation through the menu takes place by entering the respective number associated with the menu option (as can be seen in the above image).

8 Technical Data



The company **hopf** reserves the right to hardware and software alterations at any time.

General	
Operation	via WebGUI
Installation Position	any position
Protection Type of Board	IP00
Dimensions of Module	Multi-layer board 80mm x 60mm
Power Supply	5V DC \pm 5% (via internal plug-in connectors)
Power Consumption	Type 230mA / max. 300mA
MTBF	> 1,250,000h
Weight	Approx. 0.1kg

Temperature Range	
Operation	0° C to +50° C
Storage	-20° C to +75° C
Humidity	max. 90%, non condensing

LAN - ETH0/ETH1	
Network connection	Via a LAN cable with RJ45 connector, male (recommended cable type CAT5 or better)
Request per second	Max. 3,000 requests (during operation in GigaBit networks under optimum network conditions)
Number of connectable Clients	Theoretically unlimited
Network interface ETH0	10/100/1000 Base-T
Ethernet compatibility	Version 2.0 / IEEE 802.3
Isolation voltage (Network- to system side)	1500 Vrms
Boot time:	typ.: 35 seconds - When using static IP addresses for ETH0 and ETH1. Depending on the network configuration in use (e.g. DHCP) an extension of the boot phase can occur.

CE Conformity	
EMV Directive 2004/108/EC	
EN 55022 : 2006 + A1 : 2007	
EN 61000-3-2 : 2006 + A2 : 2009, EN 61000-3-3 : 2008	
EN 55024 : 1998+A1 : 2001+A2 : 2003	
Low Voltage Directive 2006/95/EC	
EN 60950-1 : 2006	

NTP Accuracy	Accuracy Value
LOW	Lambda > 20 msec
MEDIUM	Lambda < 20 msec
HIGH	Lambda < 20 msec AND stability < 0.8 pp

Time Protocols

- NTPv4 Server
- NTP Broadcast Mode
- NTP Multicast Mode
- NTP Client for additional NTP Servers (Redundancy)
- SNTP Server
- NTP Symmetric Key Encryption
- NTP Autokey Encryption
- NTP Access Restrictions

TCP/IP Network Protocols

- HTTP
- FTP
- Telnet
- SSH
- SNMP
- NTP

Configuration

- HTTP WebGUI (Browser Based)
- Telnet
- SSH
- External LAN configuration tool
- **hopf** system keypad and display

Features

- HTTP (status, control)
- SNMPv2c, SNMP Traps (MIB-II, Private Enterprise MIB)
- E-mail Notification
- Syslog Messages to External Syslog Server
- Update over TCP/IP
- Fail-safe
- Watchdog
- Power Management
- System Management

9 Factory Defaults

Usually the delivery status of the Module 8030NTC corresponds with the factory-defaults.

9.1 Network

Host/Name Service	Setting	WebGUI Presentation
Hostname	hopf8030ntc	hopf8030ntc
Default Gateway	Blank	---
DNS 1	Blank	---
DNS 2	Blank	---
Network Interface ETH0	Setting	WebGUI
Use Custom Hardware Address (MAC)	Disabled	Disabled
Custom Hardware Address (MAC)	Blank	---
DHCP	Disabled	Disabled
IP	192.168.0.1	192.168.0.1
Netmask	255.255.255.0	255.255.255.0
Operation mode	Auto negotiate	Auto negotiate
VLAN Interfaces	Disabled	Disabled
Network Interface ETH1	Setting	WebGUI
Use Custom Hardware Address (MAC)	Disabled	Disabled
Custom Hardware Address (MAC)	Blank	---
DHCP	Enabled	Enabled
IP	Blank	---
Netmask	Blank	---
Operation mode	Auto negotiate	Auto negotiate
VLAN Interfaces	Disabled	Disabled
Bonding	Setting	WebGUI
Network Interface Bonding/Teaming	Disabled	Disabled
Routing	Setting	WebGUI
User Defined Routes	Blank	---
Management	Setting	WebGUI
HTTP	Enabled	Enabled
HTTPS	Disabled	Disabled
SSH	Enabled	Enabled
TELNET	Disabled	Disabled
SNMP	Disabled	Disabled
System Location	Blank	---
System Contact	Blank	---
Read Only Community	public	public
Read/Write Community	secret	secret
Security Name	Blank	---
Access Rights	Readonly	Readonly
Authentication Protocol	MD5	MD5
Authentication Passphrase	Blank	---
Privacy Protocol	DES	DES
Privacy Passphrase	Blank	---
Time	Setting	WebGUI
NTP	Enabled	Enabled
DAYTIME	Disabled	Disabled
TIME	Disabled	Disabled
SINEC H1 time datagram	Setting	WebGUI
Send Interval	Every second	1 second
Time base	UTC	UTC
Destination MAC Address	09:00:06:03:FF:EF	09:00:06:03:FF:EF
Minimum Accuracy	LOW	LOW

9.2 NTP

NTP Server Configuration	Setting	WebGUI
Additional NTP Servers	Blank	---
Authentication	Disabled	None
Key ID	Blank	---
Peer	Blank	---
Broadcast/Multicast Mode	Disabled	Disabled
Multicast Client address	Blank	---
NTP Client Configuration	Setting	WebGUI
Lambda	20ms	20ms
Accuracy	HIGH	HIGH
NTP Access Restrictions	Setting	WebGUI
Access Restrictions		Default no modify
NTP Symmetric Keys	Setting	WebGUI
Request Key	Blank	---
Control Key	Blank	---
Symmetric Keys	Blank	---
NTP Autokey	Setting	WebGUI
Autokey	Disabled	Disabled
Password	Blank	---

9.3 ALARM

Syslog Configuration	Setting	WebGUI
Syslog	Disabled	Disabled
Server Name	Blank	---
Alarm Level	Disabled	None
E-mail Configuration	Setting	WebGUI
E-mail Notifications	Disabled	Disabled
SMTP Server	Blank	---
Sender Address	Blank	---
E-mail Addresses	Blank	---
SNMP Traps Configuration	Setting	WebGUI
SNMP Traps	Disabled	Disabled
Alarm Level	Disabled	None
SNMP Trap Receivers	Blank	---
Alarm Messages	Setting	WebGUI
Alarms	All disabled	All none

9.4 DEVICE

User Passwords	Setting	WebGUI
Master Password	master	---
Device Password	device	---

10 Glossary and Abbreviations

10.1 NTP-specific Terminology

Stability	The average frequency stability of the clock system.
Accuracy	Specifies the accuracy in comparison to other clocks.
Precision of a clock	Specifies how precisely the stability and accuracy of a clock system can be maintained.
Offset	This value represents the time difference between two clocks. It is the offset by which the local time would have to be adjusted in order to keep it congruent with the reference clock.
Clock skew	The frequency difference between two clocks (first derivative of offset over time).
Drift	Real clocks vary in frequency difference (second derivative of offset over time). This variation is known as drift.
Roundtrip delay	Roundtrip delay of an NTP message to the reference and back.
Dispersion	Represents the maximum error of the local clock relative to the reference clock.
Jitter	The estimated time error of the system clock measured as the average exponential value of the time offset.

10.2 Tally Codes (NTP-specific)

space	reject	Rejected peer – either the peer is not reachable or its synchronization distance is too great.
x	false tick	The peer was picked out by the NTP intersection algorithm as a false time supplier.
.	excess	The peer was picked out by the NTP sort algorithm as a weak time supplier on the basis of synchronization distance (concerns the first 10 peers).
-	outlier	The peer was picked out by the NTP clustering algorithm as an outlier.
+	candidate	The peer was selected as a candidate for the NTP combining algorithm.
#	selected	The peer is of good quality but not among the first six peers selected by the sort algorithm on the basis of synchronization distance.
*	sys.peer	The peer was selected as a system peer. Its characteristics are transferred to the Base System.
o	pps.peer	The peer was selected as a system peer. Its characteristics are transferred to the Base System. The current synchronization is derived from a PPS (pulse-per-second) signal either indirectly via PPS reference clock driver or directly via kernel interface.

10.2.1 Time-specific expressions

UTC	UTC Time (Universal Time Coordinated) was depending on the Greenwich Mean Time (GMT) definition of the zero meridian. While GMT follows astrological calculations, UTC is based on the stability and accuracy of the Caesium standard. The leap second was defined in order to cover this deviation.
Time Zone	The globe was originally divided into 24 longitudinal segments or time zones. Today, however, there are a number of time zones which in part apply specifically to certain individual countries only. In relation to the time zones, consideration was given to the fact that local daylight and sunlight coincide at different times in the individual time zones. The zero meridian runs through the British city of Greenwich.
Time Offset	This is the difference between UTC and the valid standard time of the current time zone. The Time Offset will be commit from the local time zone.
Local Standard Time (winter time)	Standard Time = UTC + Time Offset The time offset is defined by the local time zone and the local political regulations.
Daylight Saving Time (summer time)	Offset of Daylight Saving Time = + 1h Daylight Saving Time was introduced to reduce the energy requirement in some countries. In this case one hour is added to the standard time during the summer months.
Local Time	Local Time = Standard Time if exists with summer / winter time changeover
Leap Second	A leap second is a second which is added to the official time (UTC) in order to synchronise this with Greenwich Mean Time when required. Leap seconds are defined internationally by the International Earth Rotation and Reference Systems Service (IERS) .

10.3 Abbreviations

D, DST	Daylight Saving Time
ETH0	Ethernet Interface 0
ETH1	Ethernet Interface 1
FW	Firmware
GPS	Global Positioning System
HW	Hardware
IF	Interface
IP	Internet Protocol
LAN	Local Area Network
LED	Light Emitting Diode
NTP	Network Time Protocol
NE	Network Element
OEM	Original Equipment Manufacturer
OS	Operating System
RFC	Request for Comments
SNMP	Simple Network Management Protocol (handled by more than 60 RFCs)
SNTP	Simple Network Time Protocol
S, STD	Standard Time
TCP	Transmission Control Protocol http://de.wikipedia.org/wiki/User_Datagram_Protocol
ToD	Time of Day
UDP	User Datagram Protocol http://de.wikipedia.org/wiki/User_Datagram_Protocol
UTC	Universal Time Coordinated
WAN	Wide Area Network
msec	millisecond (10^{-3} seconds)
µsec	microsecond (10^{-6} seconds)
ppm	parts per million (10^{-6})

10.4 Definitions

An explanation of the terms used in this document.

10.4.1 DHCP (Dynamic Host Configuration Protocol)

DHCP makes it possible to integrate a new computer into an existing network with no additional configuration. It is only necessary to set the automatic reference of the IP address on the client. Without DHCP, relatively complex settings need to be made. Beside the IP address, further parameters such as network mask, gateway and DNS server have to be entered. A DHCP server can assign these parameters automatically by DHCP when starting a new computer (DHCP client).

DHCP is an extension of the BOOTP protocol. A valid IP address is allocated automatically if a DHCP server is available on the network and DHCP is enabled.



See RFC 2131 Dynamic Host Configuration Protocol for further information.

10.4.2 NTP (Network Time Protocol)

Network Time Protocol (NTP) is a standard for the synchronization of clocks in computer systems via packet-based communication networks. Although it is processed mainly over UDP, it can also be transported by other layer 4 protocols such as TCP. It was specially developed to facilitate reliable timing via networks with variable packet runtime.

NTP uses the Marzullo algorithm (devised by Keith Marzullo of the San Diego University in his dissertation) with a UTC timescale and supports leap seconds from Version 4.0. NTP. It is one of the oldest TCP/IP protocols still in use. It was developed by David Mills of the University of Delaware and published in 1985. The protocol and UNIX implementation continue to be developed under his direction. Version 4 is the up to date version of the protocol. This uses UDP Port 123.

NTPv4 can maintain the local time of a system to an accuracy of some 10 milliseconds via the public Internet. Accuracies of 500 microseconds and better are possible under ideal conditions on local networks.

With a sufficiently stable, local clock generator (oven-stabilised quartz, rubidium oscillator, etc.) and using the kernel PLL (see above), the phase error between reference clock generator and local clock can be reduced to something of the order of a few hundred microseconds. NTP automatically compensates for the drift of the local clock.

NTP can be installed over firewalls and offers a range of security functions.



See RFC 5905 for further information.

10.4.3 SNMP (Simple Network Management Protocol)

Simple Network Management Protocol (SNMP) is a network protocol which was developed by the IETF in order to be able to monitor and control network elements from a central station. This protocol regulates the communication between the monitored devices and the monitoring station. SNMP describes the composition of the data packets which can be transmitted and the communication procedure. SNMP was designed in such a way that can be provided by SNMP include:

- Monitoring of network components
- Remote control and configuration of network components
- Fault detection and notification

Due to its simplicity, SNMP has become the standard which is supported by most management programmes. SNMP Versions 1 and 2c hardly offer any safety mechanisms. The safety mechanisms have been significantly expanded in the current Version 3.

Using description files, so-called MIB's (Management Information Base), the management programmes are able to represent the hierarchical structure of the data of any SNMP agent and to request data from them. In addition to the MIB's defined in the RFC's, every software and hardware manufacturer can define his own so-called private MIB's which reflect the special characteristics of his product.

10.4.4 TCP/IP (Transmission Control Protocol / Internet Protocol)

TCP and IP are generally used concurrently and thus the term TCP/IP has become established as the standard for both protocols.

IP is based on network layer 3 (layer 3) in the OSI Layer Model whereas TCP is based on layer 4, the transport layer. In other words, the expression TCP/IP signifies network communication in which the TCP transport mechanism is used to distribute or deliver data over IP networks. As a simple example: Web browsers use TCP/IP to communicate with web servers.

10.5 Accuracy & NTP Basic Principles



NTP is based on the Internet protocol. Transmission delays and errors as well as the loss of data packets can lead to unpredictable accuracy data and time synchronization effects.



NTP protocol neither defines nor guarantees the accuracy or correctness of the time server.

Thus the QoS (Quality of Service) used for direct synchronization with GPS or serial interface does not apply to synchronization via NTP.

In simplified terms, accuracies of between 1msec and 1sec can be expected, depending on the accuracies of the servers used.

The accuracy of IP-based time synchronization is depending on the following criteria:

- Characteristics and accuracy of the time server / time signal used
- Characteristics of the sub-network
- Characteristics and quality of the synchronization client
- The algorithm used

NTP has a variety of algorithms to equalise the possible characteristics of IP networks. Algorithms also exist to equalise the offset between reference time source and the local clock.

However, under some circumstances it is not possible to provide an algorithmic solution.

For example:

1. Time servers which do not deliver any correct time cannot be detected at all. The only option available to NTP is to mark these time servers as FALSETICKERS in comparison to other time servers and to disregard them. However, this means that if only 2 time servers are configured, NTP has no way of determining the correctness of the individual times and clearly identifying which time is incorrect.
2. Asymmetries in the transmission between NTP servers and NTP clients can neither be measured nor calculated by NTP. NTP works on the assumption that the transmission path to the NTP server is exactly as long as the return path. The NTP algorithm can only filter out changes on a statistical basis. The use of several servers makes it possible for the combining algorithm to pick up and filter out any such errors. However, there is no possibility of filtering if this asymmetry is present on all or most of the NTP servers (faulty routing etc).
3. It goes without saying that the accuracy of the synchronised time cannot be better than the accuracy resolution of the local clock on the NTP server and NTP client.

With reference to the above mentioned error circumstances, the delivered **time offset** of the NTP should be considered to be at best the most favourable case and in no way to be a value that takes account of all possible errors.

In order to resolve this problem, NTP delivers the maximum possible error in relation to the offset. This value is designated as the synchronization distance ("**LAMBDA**") and is the sum of the **Root Dispersion** and half of the **Root Delay** of all NTP servers used. This value describes the worst possible case and thus the maximum error that can be expected.

Finally, please note that the user of the Time Server is responsible for the network conditions between the Time Server and the NTP clients.

As an example, we mention the case where a network has a delay of 500msec and an accuracy shift (asynchronization) of 50msec occurs. The synchronised clients will therefore NEVER achieve accuracy values of one millisecond or even microseconds!

The accuracy value in the GENERAL tab of the WebGUI is designed to help the user to estimate the accuracy.

11 List of RFCs

- IPv4:
Dynamic Host Configuration Protocol - DHCP (RFC 2131)
- Network Time Protocol (NTP):
NTP v2 (RFC 1119), NTP v3 (RFC 1305), NTP v4 (no RFC)
- Symmetric Key and Autokey Authentication
- Simple Network Time Protocol (SNTP):
SNTP v3 (RFC 1769), SNTP v4 (RFC 2030)
- Time Protocol (TIME):
Time Protocol (RFC 868)
- Daytime Protocol (DAYTIME):
Daytime Protocol (RFC 867)
- Hypertext Transfer Protocol (HTTP):
HTTP (RFC 2616)
- Secure Shell (SSH):
SSH v1.3, SSH v1.5, SSH v2 (OpenSSH)
- Telnet:
(RFC 854-RFC 861)
- Simple Network Management Protocol (SNMP):
SNMPv1 (RFC 1157), SNMPv2c (RFC 1901-1908)
- Simple Mail Transfer Protocol (RFC 2821)

12 List of Open Source Packages used

Third Party Software

The **hopf** Time Client 8030NTC includes a numerous of software packages subject to other license conditions. In case the use of such a software package might violate the licence conditions immediately after written notice it is ensured that the underlying licence conditions are met again.

If the underlying licence conditions relating to a specific software package require availability of the source code the package is provided electronically (email, download etc.) on requested.

The following table includes all used software packages with the applicable underlying software license conditions:

Paketname	Version	Lizenz	Lizenzdetails	Patches
boost	1.60.0		http://www.boost.org/LICENSE_1_0.txt	No
busybox	1.24.1	GPL	v2	No
bzip2	1.0.6	BSD		No
can-utils	f0abaaacb0a 3f620f73dd6 fd716d7daa 3c36a8e3	GPL	v2	No
cifs-utils	6.4	GPL	v3	No
dhcpcd	6.10.1	BSD		No
dhcpcdump	1.8		<p>Copyright 2001, 2002 by Edwin Groothuis, edwin@mavetju.org All rights reserved.</p> <p>Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:</p> <ol style="list-style-type: none"> 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. <p>THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.</p>	No

Paketname	Version	Lizenz	Lizenzdetails	Patches
dosfstools	3.0.28	GPL	v3	No
eeprog	0.7.6	GPL	v2+	No
ethtool	4.2	GPL	v2	No
exfat	1.2.3	GPL	v2+	No
exfat-utils	1.2.3	GPL	v2+	No
freetype	2.6.2	GPL	v2	No
gd	2.1.1	BSD		No
genext2fs	1.4.1	-		No
gzip	1.6	GPL	v2	No
hwdata	0.267	GPL	v2	No
i2c-tools	3.1.2	GPL	v2	No
igmpproxy	0.1	GPL	v2	No
ipkg	0.99.163	GPL	v2	No
iproute2	4.4.0	GPL	v2	No
iptables	1.6.0	GPL		No
iputils	2.4.10	GPL	v2	No
latencytop	0.5	GPL	v2	No
libarchive	3.1.2	BSD		No
libevent	2.0.22	3-clause BSD	http://libevent.org/LICENSE.txt	No
libffi	3.2.1	MIT License		No
libfuse	2.9.5	GPL		No
libglib2	2.46.2	LGPL	v2+	No
libnl	3.2.27	GPL		No
linux	4.1.13- g8dc6617	GPL	v2	Yes
libpcap	1.7.4	2-clause BSD		No
libpng	1.6.21		http://www.libpng.org/pub/png/src/libpng-LICENSE.txt	No
libserial	0.6.0rc2	GPL	v3	No
libserialport	0.1.1	GPL	v3	No
libsocketcan	0.0.1	LGPL	v2.1	No
libsysfs	2.1.0	LGPL	v2.1	No
libusb	1.0.19	LGPL	v2	No
libxml2	2.9.3	MIT License		No
libzip	0.11.2	BSD		No
lighttpd	1.6.39	3-clause BSD		No
lm-sensors	3.4.0	LGPL	v2.1	No
lshw	B.02.17	GPL	v2	No
lua	5.3.2	MIT License		No
lzo	2.09	GPL	v2	No
lzop	1.03	GPL	v2	No
memstat	1.0	MIT License		No
mii-diag	2.11	GPL		No
minicom	2.7	GPL	v2	No
mmc-utils		GPL	v2	No

Paketname	Version	Lizenz	Lizenzdetails	Patches
mtt	1.5.2	GPL	v2	No
nano	2.5.1	GPL		No
nanocom	1.0	GPL		No
ncftp	3.2.5		http://www.ncftp.com/ncftp/doc/LICENSE.txt	No
ncurses	5.9	Permissive free software licence	<p>Copyright (c) 1998-2004,2006 Free Software Foundation, Inc.</p> <p>Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, distribute with modifications, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:</p> <p>The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.</p> <p>THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.</p> <p>Except as contained in this notice, the name(s) of the above copyright holders shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization.</p>	No
netsnmp	5.7.3	BSD (mehrere)	http://net-snmp.sourceforge.net/about/license.html	No
netstat-nat	1.4.10	GPL		No
ntp	4.2.8p2	NTP	<p>Copyright (c) University of Delaware 1992-2011</p> <p>Permission to use, copy, modify, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided "as is" without express or implied warranty.</p>	Yes (6)
openssh	7.1p2	BSD		No
openssl	1.0.2g	Dual	http://www.openssl.org/source/license.html	No
opkg	0.3.1	GPL	v2	No

Paketname	Version	Lizenz	Lizenzdetails	Patches
pcrc	8.38	BSD		No
popt	1.16	GNU Free Documentation License	V1.3	No
pps-tools	0deb9c7e135e9380a6d09e9d2e938a146bb698c8	GPL	v2	No
rsync	3.1.2	GPL		No
setserial	2.17	GPL		No
spidev_test	V3.0	GPL	v2	No
sqlite	3100200	Public domain		No
sshpas	1.05	GPL		No
start-stop-daemon	1.18.4	GPL	v2	No
statserial	1.1	GPL		No
sudo	1.8.15	ISC-style	http://www.sudo.ws/sudo/license.html	No
sysstat	11.2.0	GPL	v2	No
uboot	2010.06	GPL	v2	No
uboot-tools	2016.01	GPL	v2	No
usb_mode-switch	2.2.5	GPL	v2	No
usb_mode-switch_data	20151101	GPL	v2	No
util-linux	2.27.1	GPL	v2	No
zlib	1.2.8	Permissive free software licence	http://www.gzip.org/zlib/zlib_license.html	No