Industriefunkuhren

hopf

Elektronik GmbH

_____

Technical Manual

NTP Time Server Module with 2x 10/100/1000 MBit LAN Interfaces

Model 8030NTS/M

ENGLISH

Version: 05.00   –   22.11.2018

_____

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 TIME SERVER 8030NTS/M (SEE *CHAPTER 7.3.6.1 DEVICE INFORMATION* AND *CHAPTER 7.3.6.2 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

NTP Time Server Module with 2x 10/100/1000 MBit LAN Interfaces 8030NTS/M - V05.00

1 NTP Time Server Module 8030NTS/M

Module 8030NTS/M is a compact NTP Time Server for the integration in clock systems or rather in signal converters. Based on the fed time information the module turns into a high-accurate **NTP Stratum 1** Time Server for the worldwide used time protocol **NTP (Network Time Protocol).** This Time Server Module is usded for the synchronization of computes and industrial networks.

The NTP Time Server module supports the following network synchronization protocols:

- NTP (incl. SNTP)
- Daytime
- Time
- SINEC H1 time datagram (**Activation Key necessary**)
- IEEE 1588 Precision Time Protocol (PTP) (**Activation Key necessary**)

Its operation is guaranteed by just supplying the Module 8030NTS/M with power and providing appropriate time information from the internal synchronization. Both are usually carried out in the basis system the Module 8030NTS/M is integrated in. However, the module can also be used in an independent signal converter.

> **i** The Module 8030NTS/M requires approx. 2-3 minutes for a successful and module's internal time synchronization, depending on the fed synchronization signal. As the module has no internal back-up clock and in order to receive an internal time for the time generation, it is required to synchronize the module after a reset or a power failure again.

The respective NTP 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 Time Server 8030NTS/M 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:

- **Complete parameterisation via protected WebGUI access**
  All required settings for operation can be executed via a password proteded WebGUI also giving an overview of the status of the Time Server 8030NTS/M.

- **Automatic switch-over of summer/winter time** (initial setting required)
  After initial commissioning there is no user intervention for a correct summer/winter time changeover for the following years required.

- **Automatic handling of the leap second**
  Insertion of a leap second in UTC time is automatically recognised and executed by the the Time Sever 8030NTS/M.

A superior security is guaranteed via available coding procedures such as symmetric keys, autokey and access restrictions and deactivation of non-used protocols.

Diffferent **Managemenet and Monitoring Functions** are availabe **as options** (e.g. SNMP, SNMP Traps, E-mail notification, Syslog-messages including MIB II and private Enterprise MIB).

The Time Server 8030NTS/M currently has unlockable features that are described in *Chapter 4.5 Activation of Functions by Activation Keys*:

- SINEC H1 time datagram
- Static Routing Table
- Alarming and management features
- Network Interface Bonding/Teaming
- IEC 62439-3 Parallel Redundancy Protocol (PRP)
- IEEE 802.1Q Tagged VLAN
- IEEE 1588 Precision Time Protocol (PTP)

A few other basic functions of the Time Server 8030NTS/M:

- The Time Server 8030NTS/M operates as **NTP Server with Stratum 1**
- Easy operation via **WebGUI**
- **NTP Status LEDs** on the front panel
- Completely **maintance-free** system

Software supplied:

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

Overview of the functions of the network Time Server 8030NTS/M:

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
- Precision Time Protocol (PTP) according to IEEE Std 1588™-2008 **(Activation Key necessary)**
  - IEEE Standard Profile for Use of IEEE 1588™ Precision Time Protocol in Power System Applications (Power Profile) according to IEEE Std C37.238™-2011

Network Configuration (Activation Key necessary)
- Routing
- Bonding (NIC Teaming) Link aggregation according toIEEE 802.1ad
- VLAN support according toIEEE 802.1q
- PRP (Parallel Redundancy Protocol) support 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/HTTPS WebGUI (browser-based)
- Telnet
- SSH
- External LAN configuration tool (*hmc* – **Network-Configuration-Assistant**)

Additional Features
- Firmware Update via TCP/IP
- Fail-safe
- Watchdog circuit
- Customizable security banner
- NTP local time support

2 Module Description

The NTP Time Server Module 8030NTS/M is a complete multi-processor embedded-linux system.

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

The module is supplied with power, the necessary time information for its synchronisation with the system time and with the system reset, if any, via an internal plug-in connection.

2.1 Installation Variants (Examples)

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

<table>
<tr>
<td align="center">Module 8030NTS/M
for the integration
in 19" systems
with 3U/4HP panels</td>
<td align="center">Module 8030NTS/M
with front panel
for the integration in
DIN Rail housings (example)</td>
</tr>
</table>
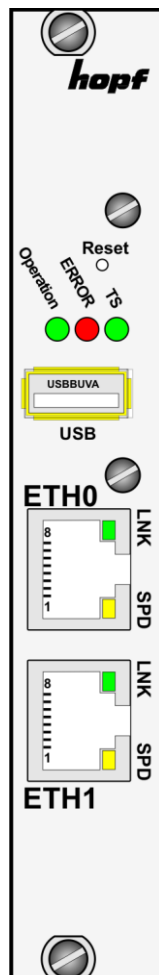
NTP Time Server Module with 2x 10/100/1000 MBit LAN Interfaces 8030NTS/M - V05.00
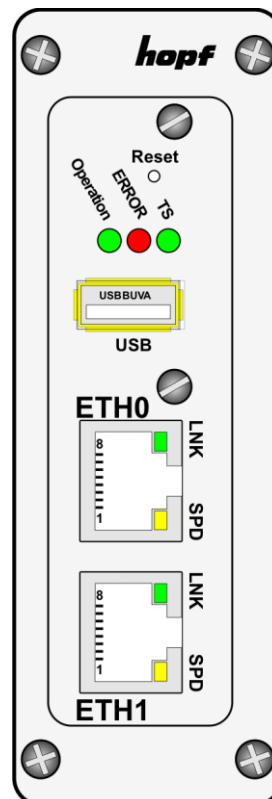
2.2 Installation and Removal of the Module

The module is supplied with power, the necessary time information for its synchronisation with the system time and with the system reset, if any, via an internal plug-in connection.

For service and reapir 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 moule 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-(Default) Button

The Reset-(Default) 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-(Default) Button*).

2.3.2 Status LEDs (TS/Error/Operation)

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

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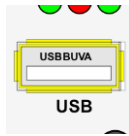
On specific problems the USB connection can be used for a system recovery after consulting the **hopf** Support.

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 at ETH0 (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 WebGUI of the appropriate module 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.

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

NTP Time Server Module with 2x 10/100/1000 MBit LAN Interfaces 8030NTS/M - V05.00

3   Function Principle

This chapter describes the functional principle of the Time Server 8030NTS/M and the internal relations between the individual function groups.

The Time Server Modul 8030NTS/M is a multi-processor system.

The structrue allows the following mode of operation:

The module receives evaluabe time information within the complete system (clock system). The time basis of the module is synchronized with high precision onto this time information.

Based on this internal time information standardized time information is supplied to the NTP service enabling the module to operate as a high-precises Stratum 1 - NTP Time Server.

Function Principle 8030NTS/M
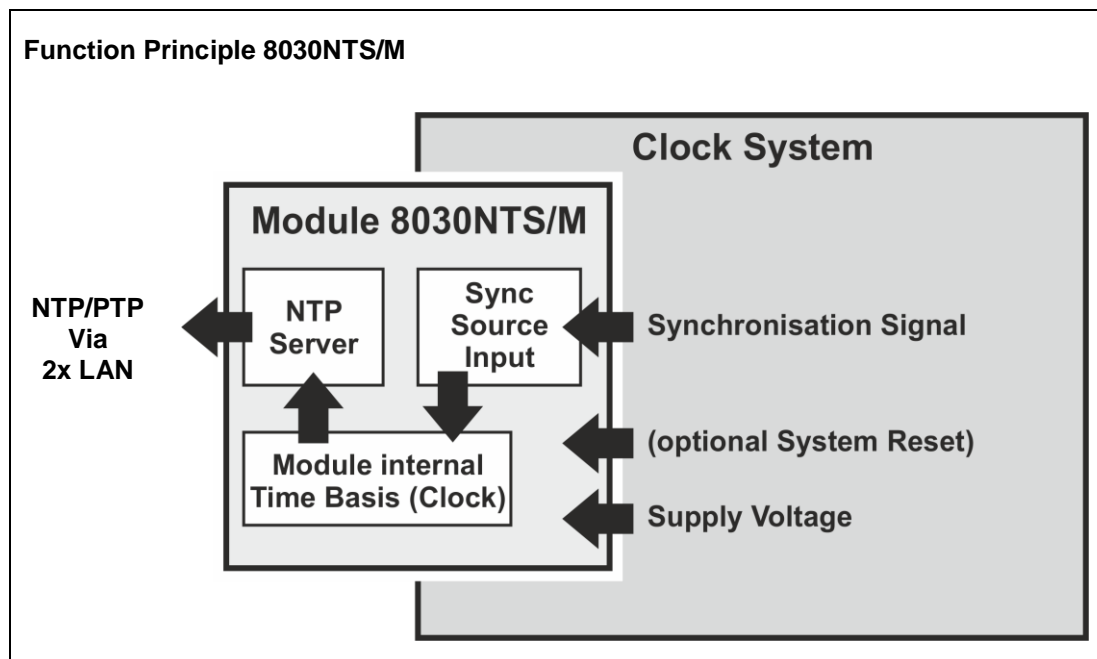
i   In this module Sync Source describes the time information provided to the module as well as the module- internal evaluation up to the successful snychornization of its internal time basis.

External Synchronization Signal (Sync Source Input)

Usually the status of the respective Sync Source is supplied in the synchronization signal as well.

Synchronisation of the Module (Clock)

Based on the system-internal provided synchronization signal and the status information contained therein the module is self-synchronized.

This synchronization status is indicatedin in the Web-GUI

(**GENERAL - SYNC SOURCE STATUS**).

NTP Adjustment

Based on the time information synchronized in the module the NTP service is supplied and controlled with standardized time information.

The status of the NTP service (time, date, stratum and accuracy) is indicated in the WebGUI (**GENERAL - NTP TIME STATUS**).

Modul Status

All information of the module required for an optimum operating state are recorded and evaluated centrally (**GENERAL - MODULE OVERVIEW**).

This concept allows the use of different synchronization signals to provide the module with time information. The format supplied to the module needs to be parameterized in the WebGUI of the module.

Although the fed synchronization signal might fail the module can continuously and independently snychronize the NTP service based on the internal time information. A differential setting of this behaviour can be parameterized in the WebGUI.

The module offers a variety of furhter settings in order to adopt the behaviour of the Time Server to the respective requirements.

NTP Time Server Module with 2x 10/100/1000 MBit LAN Interfaces 8030NTS/M - V05.00

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 Server 8030NTS/M starts after turning on the system or a reset.

During the boot process the Module 8030NTS/M 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.

> **i** Boot phase takes approx. 35 seconds by using static IPv4-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 Server 8030NTS/M requires approximately 5-10 minutes after synchronization of the Sync Source until NTP is set to the high accuracy of the Sync Source and reaches the optimized operation condition of **STRATUM = 1** and **ACCURACY = High**.

The decisive factors here are accuracy of the Sync Source (Accuracy) and the appropriate synchronization condition of the Sync Source.

4.3 Reset-(Default) Button

The Time Server 8030NTS/M 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 sec.	After releasing a **FACTORY DEFAULT** followd by a **REBOOT** is triggered after approx. 10 seconds

4.4 Firmware Update

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

Module 8030NTS/M:

> 1x Image Update
> 1x H8 Update

An update is a critical process.
The device should 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 progam releases assigned to a SET version may be taken from the release notes of the software SETs of the Time Sever 8030NTS/M.

The general process of a software update of Module 8030NTS/M is described below:

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.
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 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 8030NTS/M** via the selection window.
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.

NTP Time Server Module with 2x 10/100/1000 MBit LAN Interfaces 8030NTS/M - V05.00

4.5 Activation of Functions by Activation Keys

Currently the Time Server 8030NTS/M offers six 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 8030NTS/M (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.

> **i** 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.

- **IEEE 802.1Q Tagged VLAN**
  By activating this function network interfaces can be configured with additional VLANs (Virtual Bridged Local Area Networks) according to IEEE 802.1q.

- **Static Routing Table**
  This function is suitable for configuring static routes based on special network configuration requirements.

- **IEC 62439-3 Parallel Redundancy Protocol (PRP)**
  The PRP functionality enables to bundle the physical network interfaces ETH0 and ETH1 to one logical network interface using the Parallel Redundancy Protocol (PRP).

- **IEEE 1588 Precision Time Protocol (PTP)**
  By activating this function Precision Time Protocol (PTP) according to IEEE Std 1588™-2008 can be configured.

- **Alarming and management features**
  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.

5 Connection 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 at ETH0 (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-

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

NTP Time Server Module with 2x 10/100/1000 MBit LAN Interfaces 8030NTS/M - V05.00

6 Commissioning

This chapter describes commissioning of the Time Server 8030NTS/M.

6.1 General Procedure

Overview of the general commissioning procedure:

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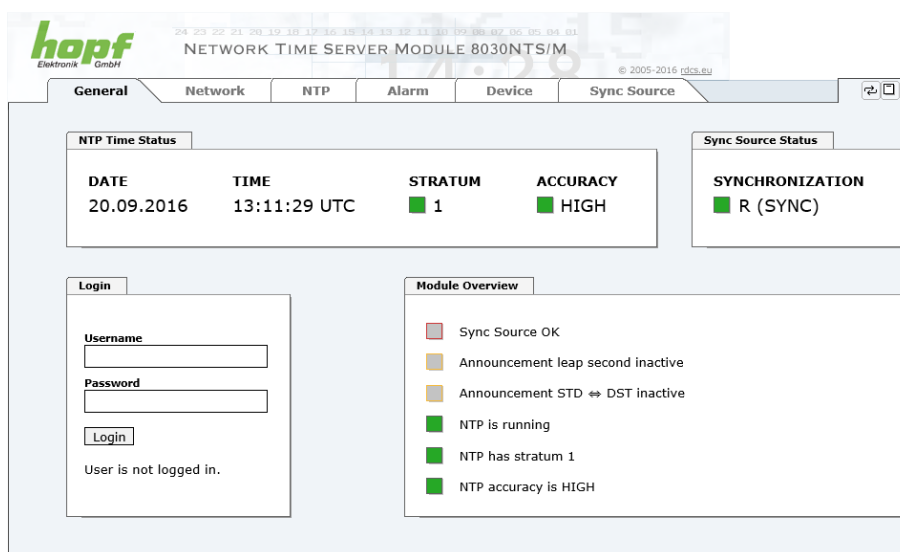
  OR

  connect directly with the factory default IPv4 address (192.168.0.1) to the WebGUI of the Time Server 8030NTS/M via 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
- Verify respectively Parametrize following values of the Sync Source in **SYNC SOURCE** tab:
  - o Used Sync Source
  - o Set the local difference time to UTC

For modules, integrated in clock systems in the factory, these settings were already performed by the *hopf* company.

- Check for **Sync Source Error** in tab **SYNC SOURCE**
- Parametrize optional functions e.g. SNMP or SINEC H1 time datagram
- If all base settings are carried out correctly and the set Sync Source supplies the time information with the appropriate accuracy, the **GENERAL** tab should look like this after approx. 30 min. (usually considerably faster):

6.2 Switching on the Operating Voltage

The Time Server 8030NTS/M has no own switch for the power supply. The Time Server 8030NTS/M is activated by switching on the device in which it is integrated in.

6.3 Establish the Network Connection via Web Browser

Ensure that the network parameters of the Time Server 8030NTS/M are configured in accordance with the local network before connecting the device to the network.

Connecting a network to an incorrectly configured Time Server 8030NTS/M (e.g. duplicate IP address) may cause interference on the network.

The Time Server 8030NTS/M is supplied with:

ETH0 with static IPv4 address
IPv4 address: 192.168.0.1
IPv4 network mask: 255.255.255.0
Gateway: not set

ETH1 with DHCP

In case it is not known whether the Time Server 8030NTS/M 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).

6.4 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 Server 8030NTS/M, 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 Server 8030NTS/M for other systems on the network.

The SEACH Function of the *hmc* - **Network Configuration Assistant requires** for location and recognition of the wished Time Server 8030NTS/M the *hmc*-computer **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 Server 8030NTS/M is stated as **8030NTS/M in the Device List.**

The determination of different Time Server 8030NTS/M (or other products variants) is made via **Hardware Address** (MAC Address).

> **i** The factory set MAC address for the Time Server 8030NTS/M is stated on a sticker laterally positioned on the exterior of the housing of the device.
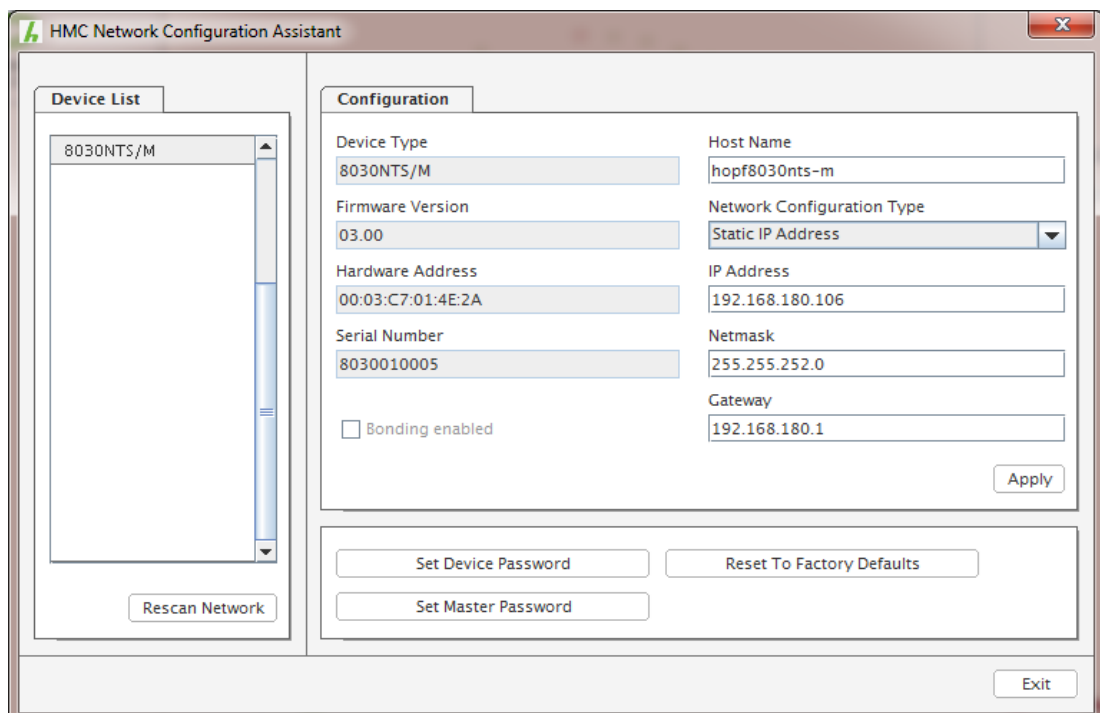
For an extended configuration of the Time Server 8030NTS/M through a browser via WebGUI the following base parameters are required:

- **Host Name**   ⇨ e.g. hopf8030nts-m
- **Network Configuration Type**   ⇨ e.g. Static IP Address or DHCP
- **IP Address**   ⇨ e.g. 192.168.180.106
- **Netmask**   ⇨ e.g. 255.255.252.0
- **Gateway**   ⇨ e.g. 192.168.180.1

!	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.
i	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 Server 8030NTS/M via the **Apply** button. Afterwards the entry of the **Device Password** is requested:

The Time Server 8030NTS/M 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 Server 8030NTS/M and are immediately active.

7   HTTP/HTTPS WebGUI – Web Browser Configuration Interface

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

7.1   Quick Configuration

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

7.1.1   Requirements

- Ready-for-operation *hopf* NTP Time Server 8030NTS/M

- PC with installed web browser (e.g. Internet Explorer) in the sub-network of Time Server 8030NTS/M

7.1.2   Configuration Steps

- Create the connection to the Time Server 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 Server via "Reboot Device"

- NTP Service is now available with the standard settings

- NTP specified settings can be done in the "NTP" tab

- 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.

7.2 General – Introduction
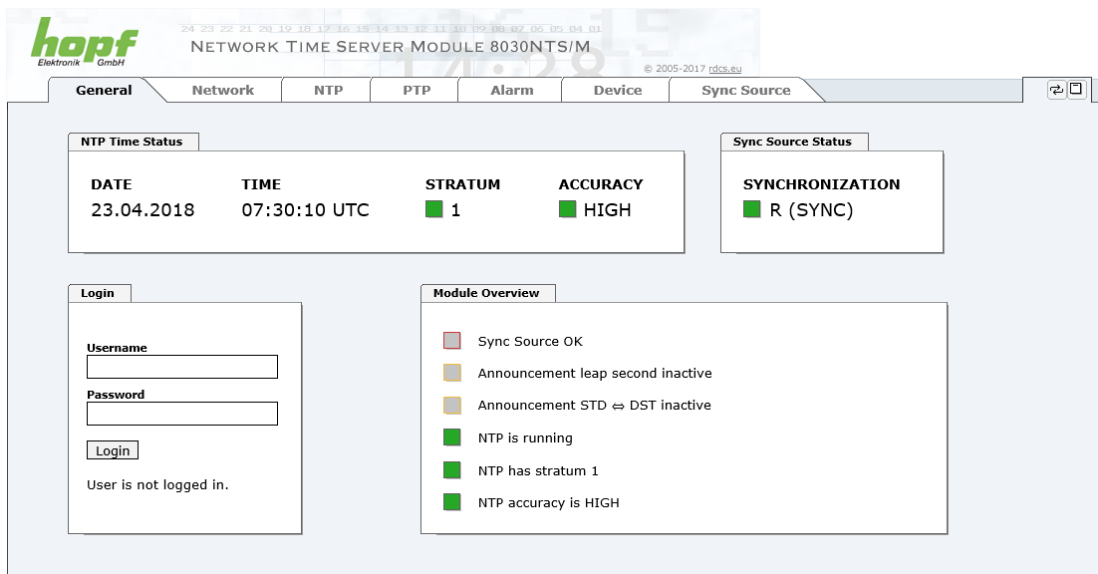
The Time Server 8030NTS/M should be accessible to a web browser if it has been set up correctly. Enter the IPv4 address - as set up in the Time Server 8030NTS/M earlier - or the DNS name on the address line <http://xxx.xxx.xxx.xxx> and the following screen should appear.

When using IPv6, it is mandatory to enclose the IPv6 address with [ ]
e.g..: http://[2001:0db8:85a3:08d3::0370:7344]/

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

> ⚠ 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.

7.2.1   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**>)
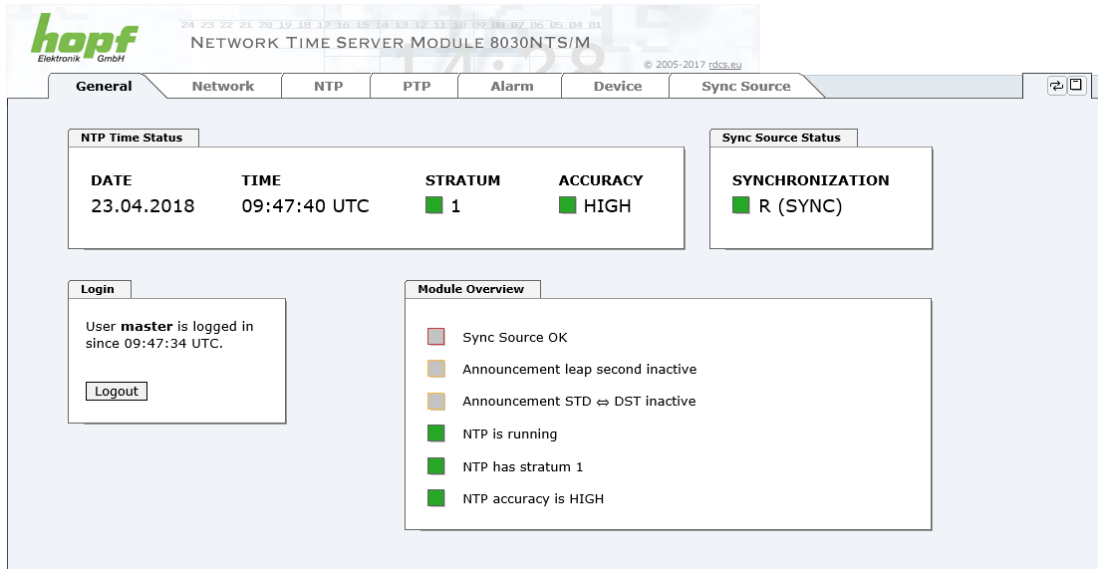
> **i** Differentiation is made between **upper and lower case** characters in the password. Alphanumeric characters and the following symbols can be used: **[ ] ( ) * - _ ! $ % & / = ?**

> **i** 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:

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

> **i** 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 in-activity (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 Server 8030NTS/M.

NTP Time Server Module with 2x 10/100/1000 MBit LAN Interfaces 8030NTS/M - V05.00

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

- Trigger reboot

- Trigger factory defaults

- Carry out image update

- Carry out H8 firmware update

- Upload certificate

- Change master password

- Diagnostics

- Download configuration files

7.2.2 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.
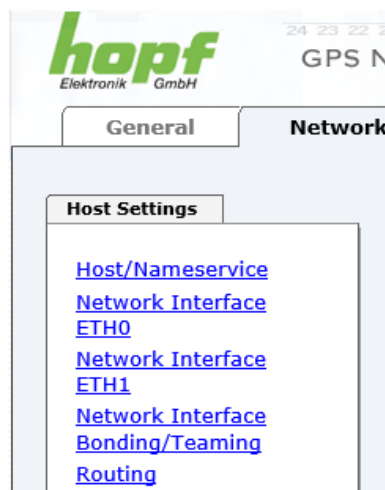
All the links within the tabs on the left hand side lead to corresponding detailed display or setting options.
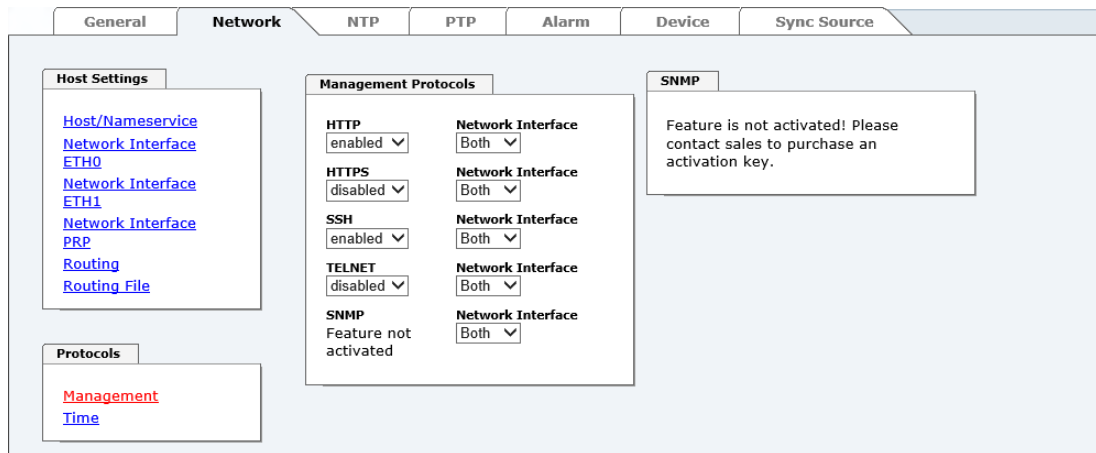
7.2.3 Enter or Changing Data

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 8030NTS/M. 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.

Only in the tab Sync Source the values are failsafe stored or rather adopted with **Apply**.

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.
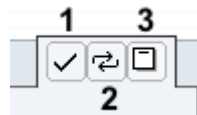
Meaning of the symbols from left to right:

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 paramters again and to save the data with **Save** permanently.
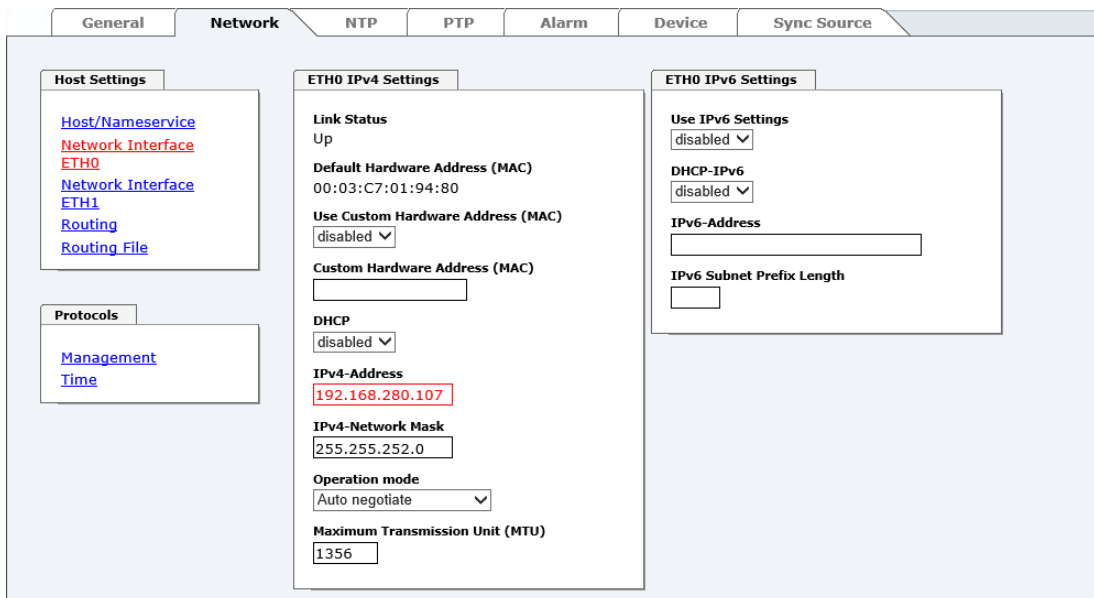
> For adopting changes and entering values only the respective buttons in the WebGUI can be used.

7.2.4   Plausibility Check during Input

A plausibility check is generally carried out during input.

As illustrated in the above image, an invalid value (e.g. text where a number should be entered, IP address not within the range etc.) is identified by a red border when an attempt is made to accept these settings. It should be noted here that this is only a semantic check and not to test whether an entered IP address can be used on the own network or in the configuration! As long as an error message is displayed it is not possible to save the configuration in the flash memory.

> The error check only verifies semantics and the validity of ranges. It is **NOT a logic or network check** for entered data.

7.3   Description of the Tabs

The WebGUI is divided into the following tabs:

- General
- Network
- NTP
- PTP
- Alarm
- Device
- Sync Source

7.3.1   GENERAL Tab

This is the first tab displayed when using the web interface.
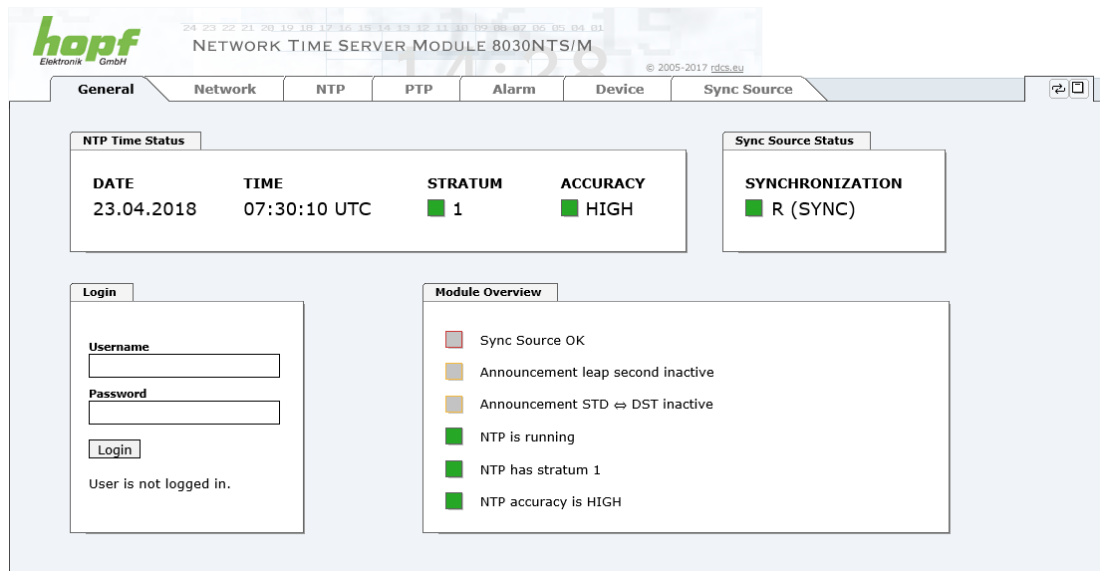
NTP Time Status

This area shows basic information about the current time and date of the Time Server 8030NTS/M. The time **always** corresponds to UTC. The reason for this is that NTP always works with UTC and not with local time.

Stratum displays the actual NTP stratum value of the Time Server 8030NTS/M with the value range from 1-16.

The **ACCURACY** field (accuracy of NTP) can contain the values LOW - MEDIUM - HIGH. The meaning of these values is explained in *Chapter 13.5 Accuracy & NTP Basic Principles*.

Sync Source Status

Display of the actual internal synchronization status of the module's internal time basis achieved by the adjusted and fed Sync Source:

SYNC	Time synchronized + Quartz regulation started/running
SYOF	Time synchronized + SyncOFF running
SYSI	Time synchronized as simulation mode (without 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 manual setting
INVA	Invalid time

Login

The login box is described in *Chapter 7.2.1 LOGIN and LOGOUT as User*.

Module Overview
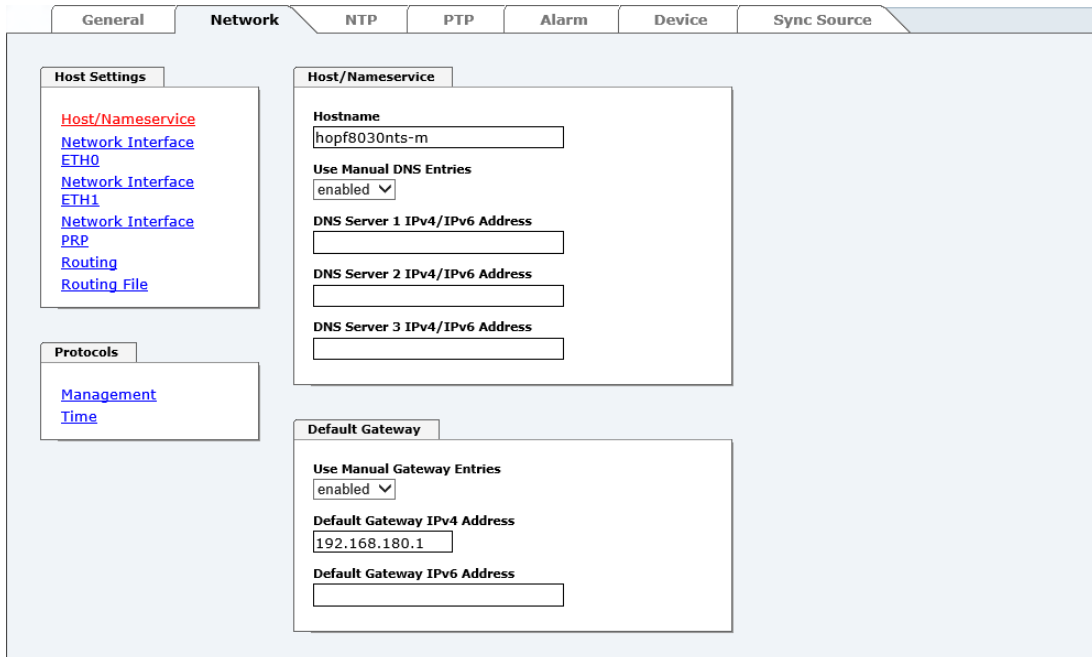
This table gives a direct overview of the Time Server's 8028NTS/M current operating states.

WebGUI	Description
Sync Source OK	When active (RED) there is a failure in the field of the Sync Souce or its evaluation. For details please go to **SYNC SOURCE** tab **– Sync Source Errors.**
Announcement leap second inactive	When active (ORANGE) there is an announcement for a leap-second.
Announcement STD ⇔ DST inactive	When active (ORANGE) there is an announcement for a summer / winter time change-over.
NTP is running	The NTP process on Module 8030NTS/M is running
NTP has stratum 1	Shows the appropriate stratum the NTP process works with.
NTP Accuracy is High	Shows the appropriate accuracy the NTP process works with.

The display fields LEAP SECOND and STD ⇔ DST announce a corrosponding event to the next hour (insertion of a leap-second or rather switchover of summer/winter time).

7.3.2   NETWORK Tab

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

| General | Network | NTP | PTP | Alarm | Device | Sync Source |

Host Settings

Host/Nameservice
Network Interface ETH0
Network Interface ETH1
Network Interface PRP
Routing
Routing File

Protocols

Management
Time

Host/Nameservice

Hostname
hopf8030nts-m

Use Manual DNS Entries
enabled ▾

DNS Server 1 IPv4/IPv6 Address

DNS Server 2 IPv4/IPv6 Address

DNS Server 3 IPv4/IPv6 Address

Default Gateway

Use Manual Gateway Entries
enabled ▾

Default Gateway IPv4 Address
192.168.180.1

Default Gateway IPv6 Address

⚠ **Changing Network Paramaters**

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 paramters again and to save the data with **Save** permanently.

7.3.2.1 Host/Nameservice

Setting for the clear network detection.

7.3.2.1.1 Hostname

The standard setting for the Hostname is "**hopf8030nts-m**". 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.

7.3.2.1.2 Use Manual DNS Entries

With this setting you can select whether the manually entered DNS servers (DNS servers 1 to 3) should be used.

If "enabled" is selected here, the entries in DNS Server 1 to 3 are used.

If "disabled" is selected, the entries in DNS Server 1 to 3 are ignored.

> If a DHCP server is used to distribute the network configuration and if this also distributes the DNS servers used in the network, then **Use Manual DNS Entries** should be set to disabled.

7.3.2.1.3 DNS Server 1 to 3

The IP address (IPv4 or IPv6) of the DNS server should be entered if you wish to use the Fully-Qualified Host Name (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.

7.3.2.1.4 Use Manual Gateway Entries

With this setting, you can select whether the manually entered gateways (Default Gateway IPv4 and Default Gateway IPv6) should be used.

If "enabled" is selected here, the entries in Default Gateway IPv4 and Default Gateway IPv6 are used.

If "disabled" is selected, the entries in Default Gateway IPv4 and Default Gateway IPv6 are ignored.

> If a DHCP server is used to distribute the network configuration and if this also distributes the address of the default gateway used in the network, then Use Manual Gateway Entries should be set to disabled.

7.3.2.1.5 Default Gateway IPv4

If the IPv4 default gateway is not known, it must be requested by the network administrator. If no standard gateway is available (special case), enter 0.0.0.0 in the input field or leave the field blank.

7.3.2.1.6 Default Gateway IPv6

If the Ipv6 default gateway is not known, it must be requested by the network administrator. If no standard gateway is available (special case), enter :: in the input field or leave the field blank.

7.3.2.2 Network Interface ETH0/ETH1

Configuration of the Ethernet interface ETH0/ETH1 of the Time Server 8030NTS/M.

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

7.3.2.2.1 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 Server 8030NTS/M.

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

7.3.2.2.2 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**

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

!	There are no MAC multicast addresses allowed!

7.3.2.2.3 DHCP

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

7.3.2.2.4 IPv4 Address

If DHCP is not used, the IPv4 address needed to be entered here. Contact your network administrator for details of the used IPv4 address if not known.

7.3.2.2.5 IPv4 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.

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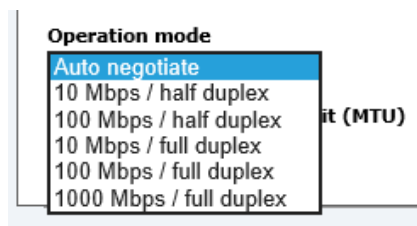
The network device usually adjusts the data stream and duplex mode to the device to which it is connected (e.g. HUB, SWITCH) automatically. If the network device requires a certain speed or duplex mode, this can be configured via the web interface. The value should only be changed in special cases. The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

> **i**
>
> 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 Server 8030NTS/M **and** the connected network components manually to the same value.

7.3.2.2.7 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 Server 8030NTS/M is going to be delivered with default setting 1356.

7.3.2.2.8 IPv6

The module can also be operated in an IPv6 network.

To enable IPv6, **Use IPv6 Settings** must be set to **enable**.

IPv6 addresses are 128 bits long and they are recorded in eight 4-character hexadecimal blocks. For example: **2001:0db8:0000:08d3:1319:8a2e:0370:7344**

Leading zeroes in a 4-character hexadecimal block can be omitted. For the above example, this results in the notation: **2001:db8:0:8d3:1319:8a2e:370:7344**

In addition, **once** per IPv6 address a consecutive sequence of blocks containing all zeros may be omitted. But this must be recorded with two consecutive colons. For the above example, this gives the notation: **2001:db8::8d3:1319:8a2e:370:7344**

Another example: **2001:0:0:0:1319:8a2e:0:7344** may be represented

>   as   **2001::1319:8a2e:0:7344**
>
>   or   **2001:0:0:0:1319:8a2e::7344**

7.3.2.2.9 DHCP-IPv6

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

7.3.2.2.10 IPv6 Address

If DHCP is not used, enter the IPv6 address here. If the IPv6 address to be used is unknown, it must be requested by the network administrator.

7.3.2.2.11   IPv6 Subnet Prefix Lengh

If no DHCP is used, the length of the network address must be entered here. If the length of the network address is not known, it must be requested by the network administrator.

7.3.2.2.12   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 Server 8030NTS/M, 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.

```
VLAN

Activation Status
disabled ▾

VLAN Interfaces

[ Add ]  [ Remove ]

  ID   Label   Remark     DHCP     IPv4-Address        IPv4-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 IPv4 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

Add   Remove

ID	Label	Remark	DHCP	IPv4-Address	IPv4-Network Mask
10	DEV	Development	disabled	192.168.180.30	255.255.255.0

---

i To ensure the correct function the network appliance must be connected with Time Server 8030NTS/M via the network interface. Furthermore it must be ensured that the network appliance is accurately configured with the same VLANs.
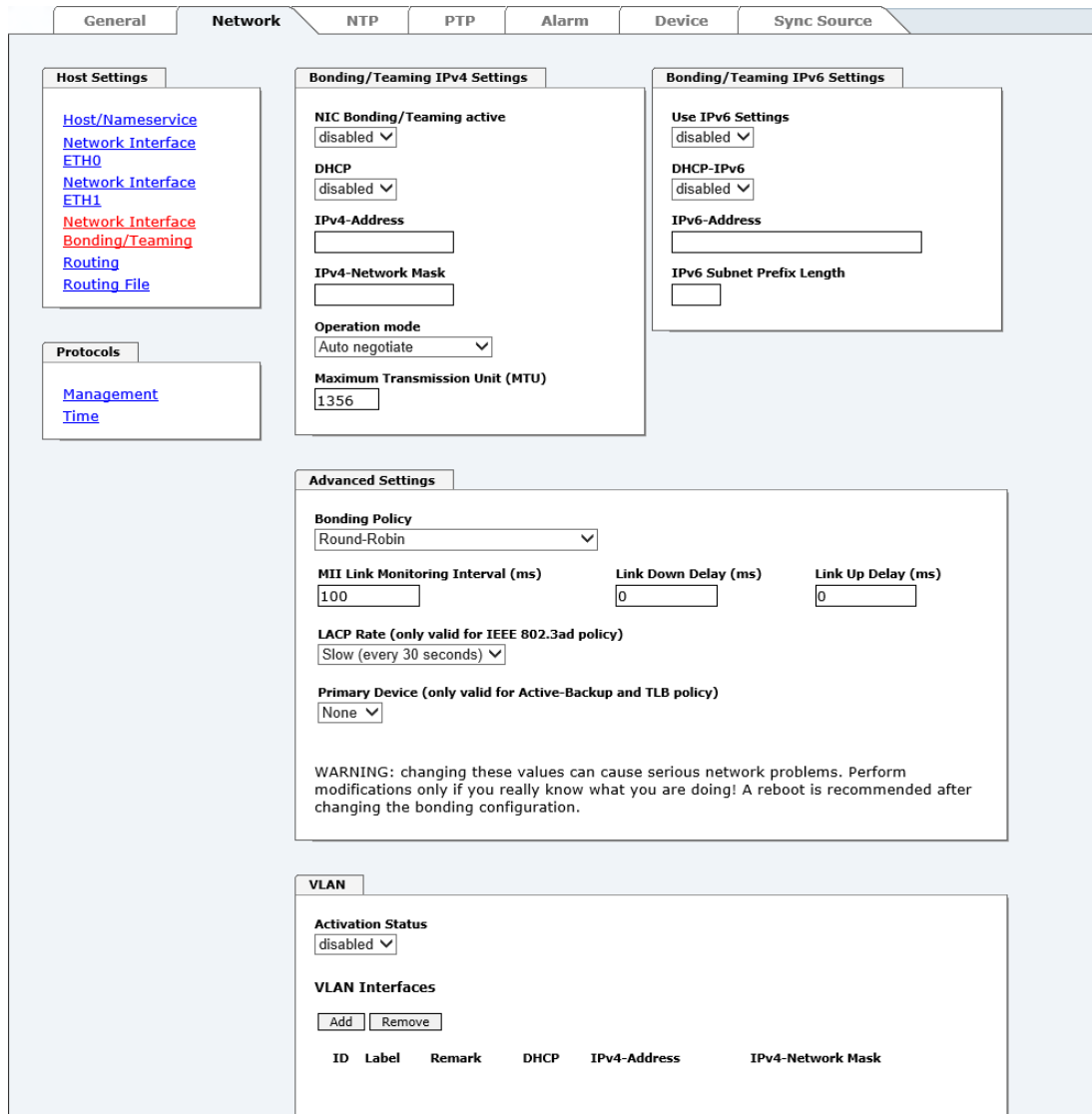
! VLAN ID one (1) and two (2) are reserved and are therefore not permitted!

7.3.2.3 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 a 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 Server 8030NTS/M is going to be refused.
>
> In this case settings of Time Server 8030NTS/M must be set back to default settings!

> ℹ 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.

7.3.2.3.1.1 Basic Configuration

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

```
┌─────────────────────────────────────┐
│ Bonding/Teaming IPv4 Settings        │
│                                      │
│ NIC Bonding/Teaming active           │
│ [disabled ▼]                         │
│                                      │
│ DHCP                                 │
│ [disabled ▼]                         │
│                                      │
│ IPv4-Address                         │
│ [                    ]               │
│                                      │
│ IPv4-Network Mask                    │
│ [                    ]               │
│                                      │
│ Operation mode                       │
│ [Auto negotiate         ▼]           │
│                                      │
│ Maximum Transmission Unit (MTU)      │
│ [1356  ]                             │
└─────────────────────────────────────┘
```

NIC Bonding/Teaming active

Activation of function NIC Bonding/Teaming

DHCP

Activation of DHCP of the "Bonding interface".

> ⚠ A change of the IPv4 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.

IPv4 address

Input of IP address of the "Bonding interface". If you do not know the IPv4 address, please contact your network administrator.

> ⚠ A change of the IPv4 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.

IPv4 Network Mask

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

> ⚠ A change of the IPv4 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.

NTP Time Server Module with 2x 10/100/1000 MBit LAN Interfaces 8030NTS/M - V05.00

7.3.2.3.2 IPv6 Network Configuration

Defining the IPv6 network configuration with the Bonding/Teaming function activated.

```
┌─────────────────────────────────────┐
│ Bonding/Teaming IPv6 Settings        │
├─────────────────────────────────────┤
│                                      │
│  Use IPv6 Settings                   │
│  [disabled ▼]                        │
│                                      │
│  DHCP-IPv6                           │
│  [disabled ▼]                        │
│                                      │
│  IPv6-Address                        │
│  [                            ]      │
│                                      │
│  IPv6 Subnet Prefix Length           │
│  [        ]                          │
│                                      │
└─────────────────────────────────────┘
```

Use IPv6 Settings
Activation of IPv6 function

DHCP IPv6
Activation of IPv6 DHCP for the "Bonding interface"

IPv6 address
Input of the IPv6 address for the " Bonding interface".
If the IPv6 address is not known, it must be requested by the network administrator.

IPv6 Subnet Prefix Length
Input of the IPv6 network length for the " Bonding interface".

7.3.2.3.2.1 Advanced Settings

```
Advanced Settings

Bonding Policy
Round-Robin                              ∨

MII Link Monitoring Interval (ms)    Link Down Delay (ms)    Link Up Delay (ms)
100                                  0                       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 Server 8030NTS/M are connected also needs to be configured correctly! A wrong configuration can lead to a loss of availability of Time Server 8030NTS/M!

- **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.

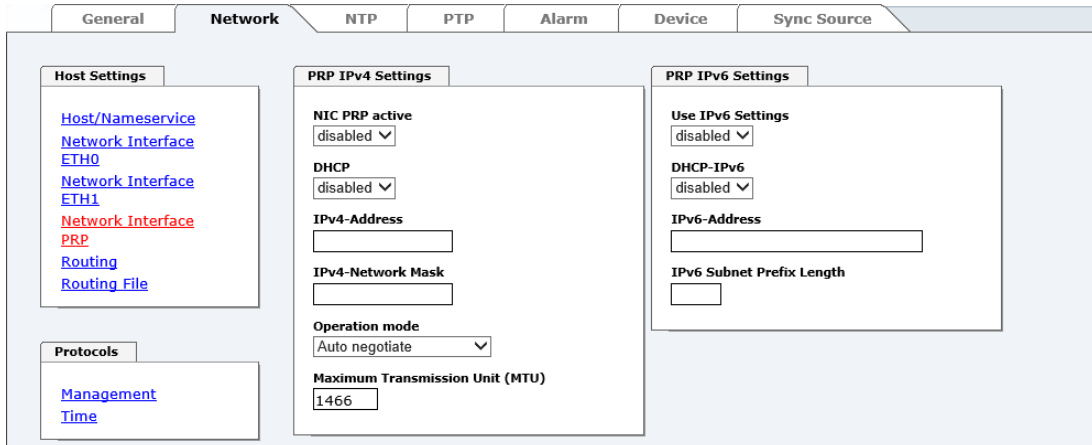### 7.3.2.4 Network Interface PRP (Activation Key necessary)

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:
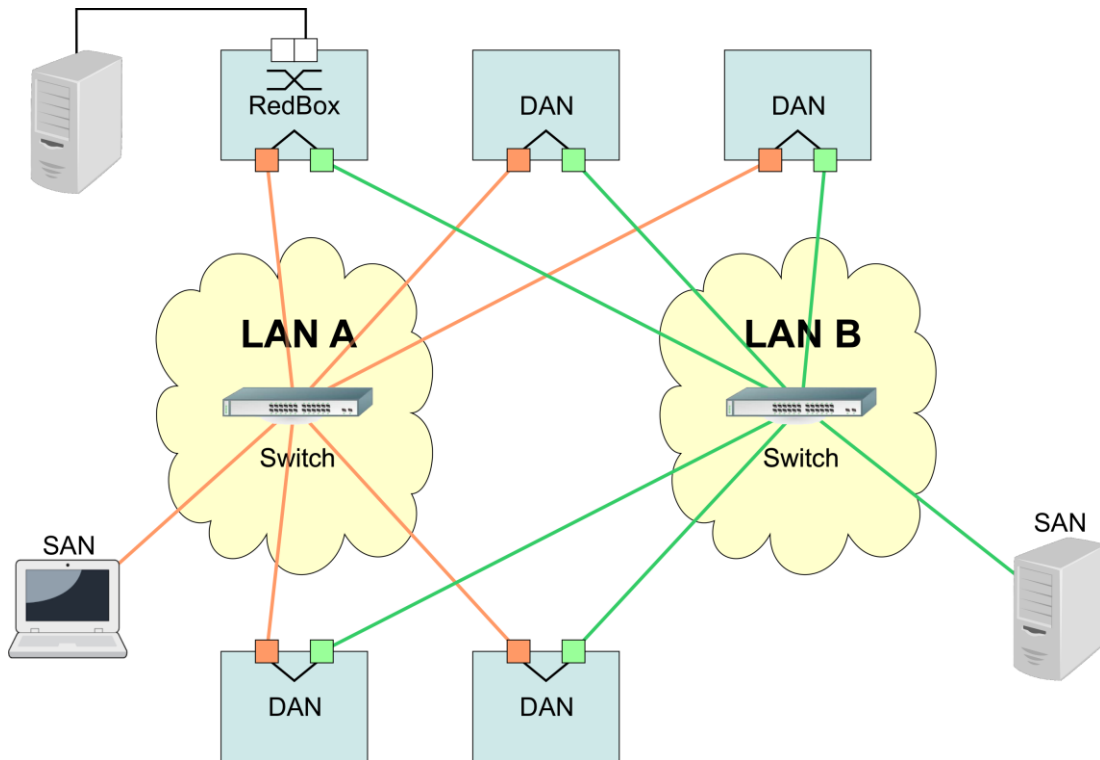
PRP-suitable applications are known as DAN (Dual Attached Node) and are going to be connected to the independent networks "LAN A" and "LAN B". The advantage of PRP is that cost-efficient and common network switches can be used which do not have to support the PRP standard. Applications which do not need 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 Server 8030NTS/M supports PRP as DAN and can therefore directly be integrated into a PRP network without using a RedBox.

NTP Time Server Module with 2x 10/100/1000 MBit LAN Interfaces 8030NTS/M - V05.00

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 IPv4 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.

IPv4 address

Input of the IPv4 address for the "PRP interface". If unknown the IPv4 address needs to be obtained by the network administrator.

> ⚠ A change of the IPv4 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.

IPv4 Network Mask

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

> ⚠ A change of the IPv4 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 Server 8030NTS/M 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 Server 8030NTS/M.
>
> In that case the settings of Time Server 8030NTS/M 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.

7.3.2.4.1 IPv6 Network Configuration

Defining the IPv6 network configuration for the PRP interface.

Use IPv6 Settings
Activation of IPv6 function

DHCP IPv6
Activation of IPv6 DHCP for the "PRP interface"

IPv6 address
Input of the IPv6 address for the " PRP interface".
If the IPv6 address is not known, it must be requested by the network administrator.

IPv6 Subnet Prefix Length
Input of the IPv6 network length for the " PRP interface".

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

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

WebGUI with Routing activated

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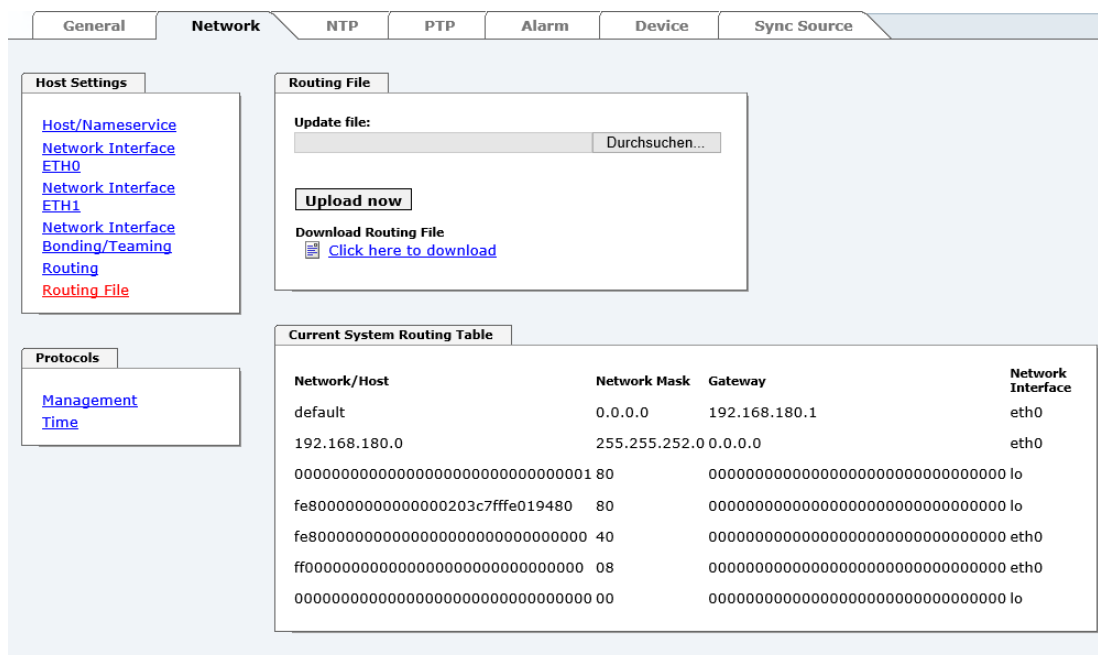

The module cannot be used as a router!

Select **Use Route File** to set whether the routing configuration set under **User Defined Routes** should be used, or routing configuration using a routing file.

If IPv6 routes are required, the routes must be made using the settings in *Chapter 7.3.2.6 Routing File*
.

7.3.2.6 Routing File

In order to activate this function, **Use Route File** must be set to **enabled** on the Routing Page.

The routing file also makes it possible to configure IPv6 routes.

General	Network	NTP	PTP	Alarm	Device	Sync Source

Host Settings

Host/Nameservice
Network Interface ETH0
Network Interface ETH1
Network Interface Bonding/Teaming
Routing
Routing File

Protocols

Management
Time

Routing File

Update file:

[Durchsuchen...]

[**Upload now**]

Download Routing File
Click here to download

Current System Routing Table

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
00000000000000000000000000000001	80	00000000000000000000000000000000	lo
fe800000000000000203c7fffe019480	80	00000000000000000000000000000000	lo
fe800000000000000000000000000000	40	00000000000000000000000000000000	eth0
ff000000000000000000000000000000	08	00000000000000000000000000000000	eth0
00000000000000000000000000000000	00	00000000000000000000000000000000	lo

Via the selection window under Update file and the button Upload now a new routing file can be uploaded. When uploading the file is checked whether the file is error-free and only then it is used.

If a routing file has already been uploaded, the uploaded routing file can be downloaded under **Download Routing File**.

Routing File Syntax

Each line of the routing file must be either a valid routing line or a comment line. A comment line starts with a hash sign (#) and can contain any text behind it.

A routing line has the format [destination address] [tab] [length of the destination mask in bits] [tab] [gateway address for the specified destination].

If the host 192.168.20.11 is to be reached using the gateway 192.168.0.2, then the routing file must look like this:

```
192.168.20.11   32   192.168.0.2
```

Example of a Routing File:

```
# Host 192.168.20.11 via Gateway 192.168.0.2
192.168.20.11   32   192.168.0.2
#Net 192.168.180.0 Netmask 255.255.255.0 via Gateway 192.168.0.2
192.168.180.0   24   192.168.0.2
#Net 2001:0db8:0:f102:: Subnet Prefix Length 64 via Gateway 2001:0db8:0:f101::1
2001:0db8:0:f102::   64    2000::1
```

Current **System Routing Table**

This table shows all active IPv4 and IPv6 routes.

For IPv6 routes, the colons of the destination and gateway addresses are not displayed, and the **Network Mask** column displays the length in hexadecimal

7.3.2.7 Management (Management-Protocols – HTTP, SNMP 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.

The **HMC NCA** field deactivates or activates the interface to the HMC network configuration wizard.
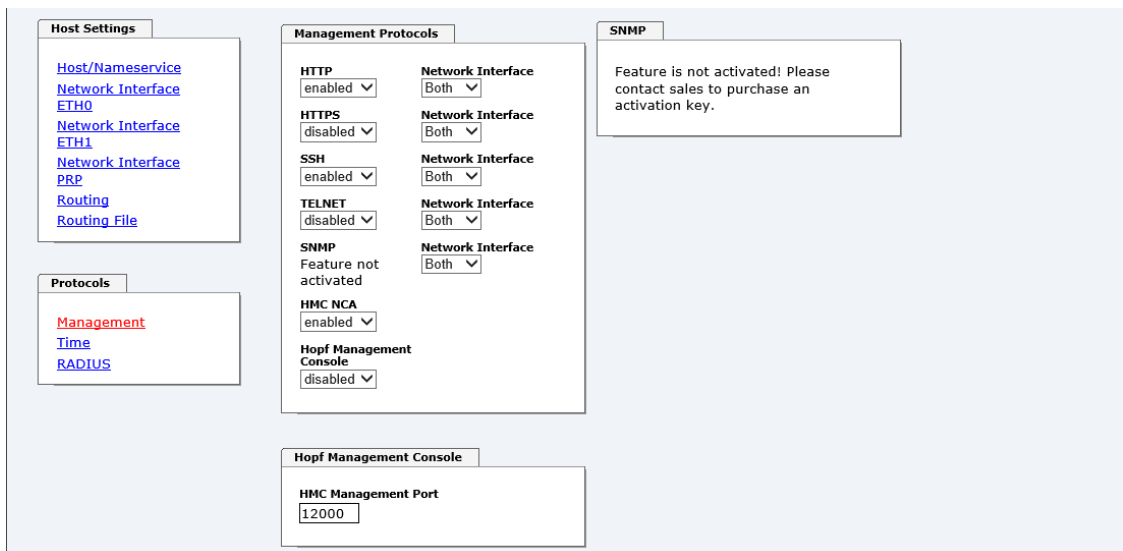
!	For SNMP functionality an activation key is necessary.

!	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".

i	These service settings are valid globally! Services with "disabled" status are not externally accessible and are not made externally available by the module!

WebGUI with Alarming activated

Using SNMP and SNMP traps the protocol SNMP should be enabled. All fields must be filled in for a correct operation of SNMP. Contact your network administrator for details of data not known.

NTP Time Server Module with 2x 10/100/1000 MBit LAN Interfaces 8030NTS/M - V05.00

7.3.2.7.1 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:
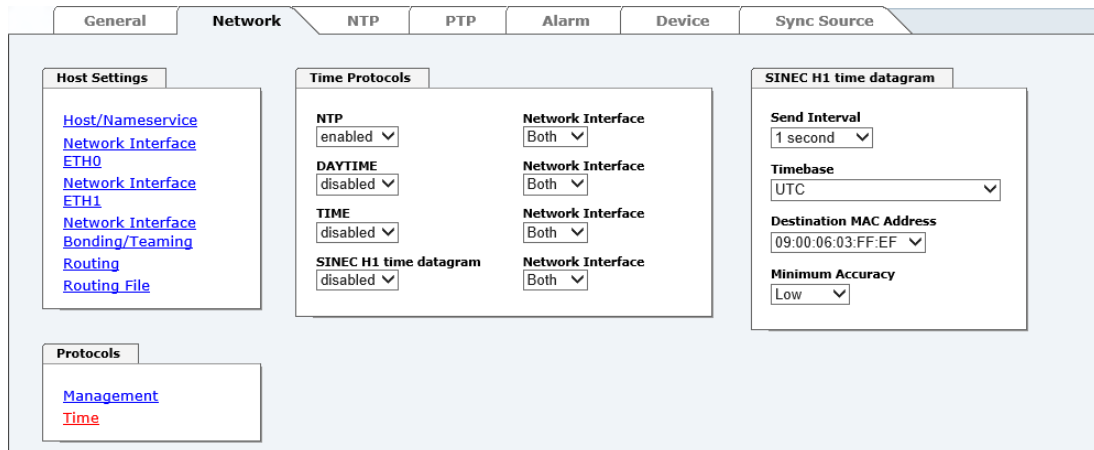
SNMPv3	noAuthNoPriv	authNoPriv	authPriv
Authentication Passphrase:	empty	set	set
Privacy Passphrase:	empty	empty	set

> ⚠ Right now only one user is supported.

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

Activation and configuration of different synchronization protocols

All protocols can be enabled at the same time.

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

Needed time protocols can be enabeld here.

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

7.3.2.8.2 SINEC H1 time datagram (Activation Key necessary)

Configuration of the SINEC H1 time datagram

SINEC H1 time datagram
Send Interval
1 second ▾
Timebase
UTC ▾
Destination MAC Address
09:00:06:03:FF:EF ▾
Minimum Accuracy
Low ▾

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

- every second
- every 10 second
- every 60 second

Timebase see also *Chapter 13.2.1 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

Synchronization Status based on Starting Transmission (Minimum Accuracy)

This setting defines at which internal accuracy status the SINEC H1 time datagram should be transmitted (see ***Chapter 13.5 Accuracy & NTP Basic Principles*** and ***Chapter 11 Technical Data***):

- LOW
- MEDIUM
- HIGH

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

7.3.2.9 RADIUS

This page allows the configuration of the RADIUS service (Remote Authentication Dial-In User Service).

In order to use this service, a correspondingly configured RADIUS server must exist.

7.3.2.9.1 RADIUS Server Configuration under Windows Server 2016

Prepare Active Directory Users and Computers

The RADIUS server must support two user groups.

Under 'Active Directory Users and Computers' create two groups of authorized users to authenticate with RADIUS - e.g. RADIUS-master and RADIUS-device.

Then you have to add authorized users to these groups.

Master users have full access to the system, device users have limited access to the system.

Installation of the function Network Policy and Access Service

In menu item 'Server-Manager' / 'Dashboard' / 'Manage' / 'Add Roles and Features' add server role 'Network Policy and Access Services' and restart server if required.

Configuration of RADIUS service

Open the Network Policy Server via 'Server Manager' / 'Dashboard' / 'Tools' / 'Network Policy Server'.

Register your RADIUS server on ActiveDirectory so that it can make queries to the users and groups database.

With the right mouse button click on the NPS (Local) button of the Network Policy Server and 'Register server in ActiveDirectory'.

Create RADIUS Clients

After configuring the RADIUS server service, the *hopf* device must be entered as RADIUS client.

The required menu can be found on the Network Policy Server 'NPS (Local)' / 'RADIUS Clients and Server' / 'RADIUS Clients'. With the right mouse button click on 'New'.

Type in 'Friendly name' (e.g. HOPF Device), Client-'Address' (e.g. 192.168.1.123) and a 'Shared secret' key (***).

The address typed in must match the address of the *hopf* device.

The shared secret key can be chosen freely. It must be repeated in the confirm field. The chosen key will be required as a secret key during configuration at the *hopf* device.

NTP Time Server Module with 2x 10/100/1000 MBit LAN Interfaces 8030NTS/M - V05.00

Create a Connection Request Policy

Open the menu item 'NPS (Local)' / 'Policies' / 'Connection Request Policy' in the Network Policy Server – then click on 'New' with the right mouse button.

Type in a 'Policy name' (e.g. TEST) => 'NEXT'

In the menu item 'Condition description' click on 'Add ...'

Select 'Client Friendly Name' and type in => 'Add ...'

Type in a name (e.g. TEST) => 'OK'

Click on 'NEXT' => 'NEXT' => 'NEXT'

In 'Configure Settings' select Attribute 'User-Name' and click 'NEXT' => 'FINISH'

Create a Network Policy

Subsequently the two network policies for the MASTER and DEVICE access to the *hopf* device must be created.

With the right mouse button click on menu item 'New' of the Network Policy Server menu 'NPS (Local)' / Policies / Network Policies

Type in a 'Policy name' (e.g. HOPF-master) => NEXT

In the menu item 'Condition description' click on 'Add ...'

Select the menu item 'User Groups' and click 'Add ...'

Click 'Add Groups ...' and select the previous created group e.g. RADIUS-master => 'OK' => 'Next'

In 'Specify Access permission' select **'Access granted'** => 'NEXT'

In 'Configure Authentication Methods' select **'Unencrypted authentication (PAP, SPAP)'** => NEXT

Click on 'Next' to open a note that needs to be confirmed with **'No'** to proceed with the next screen.

Click on 'Next' for the 'Configure settings' window.

In this window the attribute 'Tunnel password' must be set under 'RADIUS attributes' / 'Standard' with the button 'Add'. All other attributes must be cleared using the Remove button.

When adding the tunnel password attribute, make sure that Hexadecimal is selected for "Enter attribute value as". Now you have to select a password that must be entered into the tunnel password input field in the following way:

1. Six zeros must be entered at the beginning of the password.

2. As a two-digit hexadecimal number, the length of the selected password must be added. If as password, e.g. master is selected, then 06 must be added since master is six characters long.

3. Now, the ASCII value of each character of the selected password must be added as a two-digit hexadecimal number. For the password **master**, **6D6173746572** would have to be specified.

4. Finally, the tunnel password must be confirmed with OK.

Here are some password examples and the tunnel passwords to be given:

Password Example	Tunnel Password Input
Test123	0000000754657374313233
MySecret	000000084D79536563726574
ABCDEFGHIJKLMNOPQRST	00000014414243444546474849494a4b4c4d4e4f5051525354

After confirming the chosen password continue by clicking on 'Next'.

Use the 'Finish' button to complete the configuration of the new network policy.

Two network policies must be set up. One of the network policies regulates access to the *hopf* device with the MASTER user rights, the other regulates the access with DEVICE user rights. The tunnel passwords of the two network policies must be different.

If both network policies have been created, the Network Policy page must contain at least the two newly created policies.

7.3.2.9.2 RADIUS Configuration on the *hopf* Device

On the RADIUS page, the data required for the RADIUS configuration can be entered by the MASTER user or, if the RADIUS service is already activated, by a user who is in the MASTER group of the RADIUS server.

All other users see the following message:

RADIUS

You must be logged in as master user to perform this action.

Use the **Enable** field to enable and disable the RADIUS service. If the RADIUS service is disabled, the MASTER and the DEVICE users are used for logging into the web interface. If the RADIUS service is activated, the RADIUS service is used to log in to the web interface.

The **Server Address** field must specify the network address of the RADIUS server.

The **Secret Key** field must display the 'shared secret key' specified on the RADIUS server for this *hopf* device.

In the field **Master User Secret** the 'Tunnel password' must be entered, which has been specified in the *hopf* Master network policy.

In the field **Device User Secret** the 'Tunnel password' must be entered, which has been specified in the *hopf* Device network policy.

NTP Time Server Module with 2x 10/100/1000 MBit LAN Interfaces 8030NTS/M - V05.00

The following picture shows the RADIUS configuration on the **hopf** device, for a RADIUS server with the address 192.168.1.124 and the shared secret key **MySecret**.

7.3.2.9.3 Notes

The RADIUS service is only used for the web interface.

> ⚠ If other protocols than http and https are activated in the management section of **Chapter 7.3.2.7 Management (Management-Protocols – HTTP, SNMP etc.)**, they continue to use the master and the device user; therefore the other protocols should be deactivated when using the RADIUS service.

If the RADIUS service is activated after logging in with a user of the master group on the general page, you will be logged in as **master** user.

Users who are in the device group will see that they are logged in as **device** users.

7.3.3   NTP Tab

This tab shows information and adjustment possiblities of the NTP services of the Time Server 8030NTS/M. The NTP service is the significant main service of the Time Server 8030NTS/M.

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 Server 8030NTS/M.

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 7.3.2.8 Time (Time Protocols – NTP, DAYTIME etc.)**)

> After all changes relating to NTP a restart of the NTP service must be performed (see **Chapter 7.3.3.6 Restart NTP**).
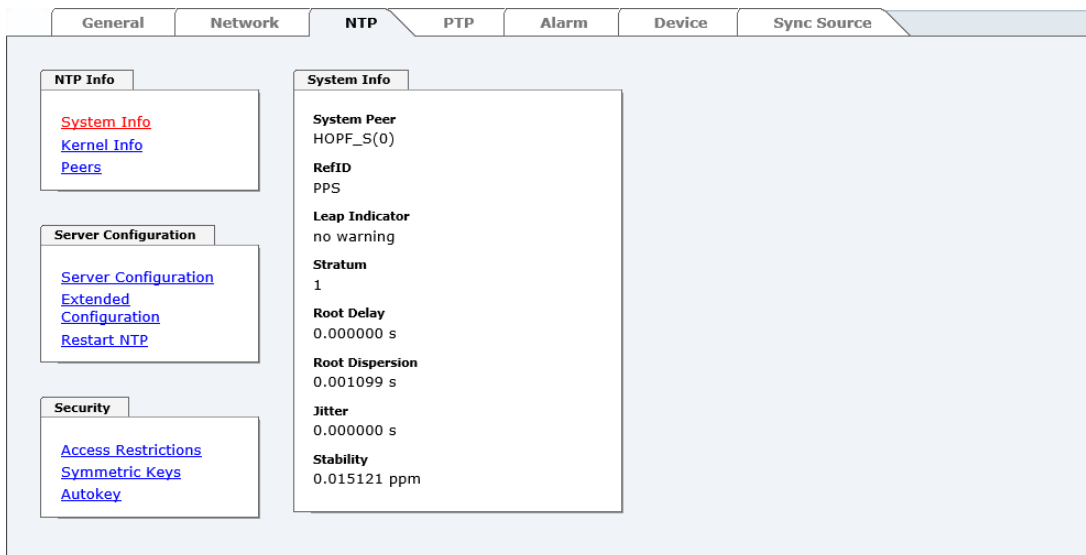
> Via the NTP protocol SNTP Clients can also be synchronized. In contrast to NTP in SNTP Clients delay times are not evaluated on the network. For this reason the accuracy reached in SNTP Clients is lower than in NTP Clients.

7.3.3.1 System Info

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

The NTP version used adjusts the leap second correctly.

The Time Server 8030NTS/M works as NTP Server with stratum 1 and belongs to the best available class of NTP server, as it has a reference clock with direct access.

General	Network	**NTP**	PTP	Alarm	Device	Sync Source

NTP Info

System Info
Kernel Info
Peers

Server Configuration

Server Configuration
Extended Configuration
Restart NTP

Security

Access Restrictions
Symmetric Keys
Autokey

System Info

System Peer
HOPF_S(0)

RefID
PPS

Leap Indicator
no warning

Stratum
1

Root Delay
0.000000 s

Root Dispersion
0.001099 s

Jitter
0.000000 s

Stability
0.015121 ppm

7.3.3.2 Kernel Info

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

General	Network	**NTP**	PTP	Alarm	Device	Sync Source

NTP Info

System Info
Kernel Info
Peers

Server Configuration

Kernel Info

Max. Error
16.000000 s

Estimated Error
0.005500 s

This screenshot shows a maximum kernel clock error of 16.000 msec (milliseconds). The estimated error value is 5.5 ms (milliseconds).

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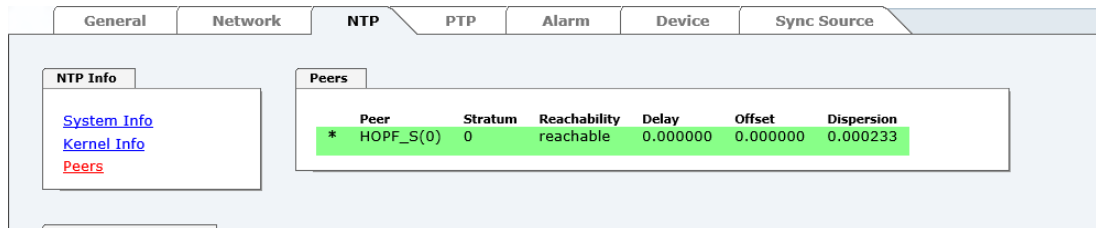
7.3.3.3 Peers

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 programes.

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).
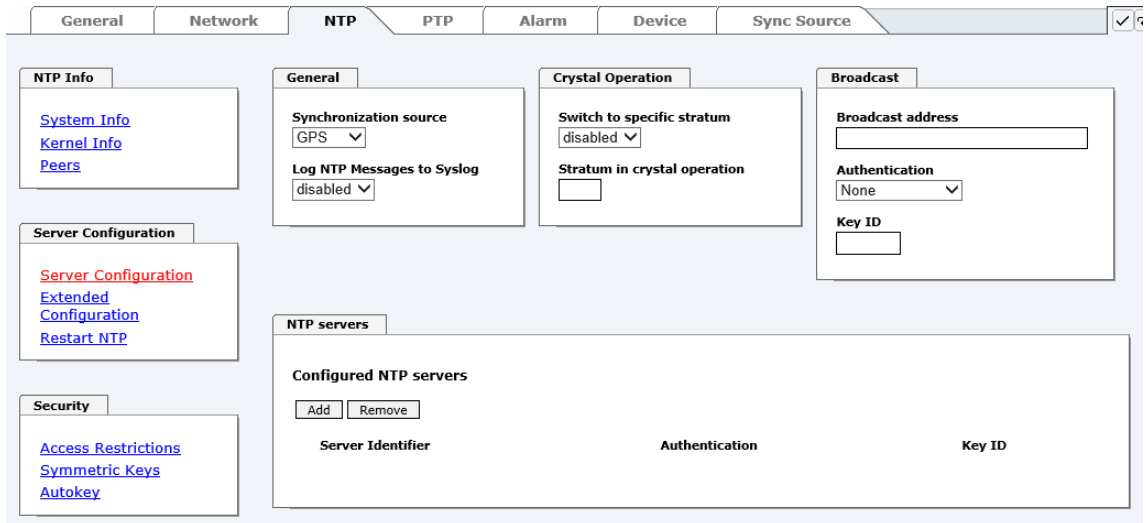
Three lines can be seen in the above image. The first line displays the *hopf* **- refclock ntp driver** that gets the time information directly from the Sync Source.

A short explanation and definition of the displayed values can be found in ***Chapter 13.5 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 13.2 Tally Codes (NTP-specific)***).

7.3.3.4 Server Configuration

The basic settings for NTP base functionality are displayed selecting the "Server Configuration" link.

The NTP-hopf-refclock driver is already configured as standard (127.127.38.0 in the "Peers Summary") and is not explicitly displayed here.

7.3.3.4.1 Synchronization Source (General / Synchronization source)

As *"Synchronization source"* either GPS or DCF77, depending on the appropriate Sync Source, has to be selected. This is reuiqred in order to align the NTP algorithm for the calculation of the accuracy with the synchronization source.

> Based on the selection of GPS, even though GPS is not the source of the Sync Source (different product option) the value **HIGH** for **Accuracy** may never be reached.

7.3.3.4.2 NTP Syslog Messages (General / Log NTP Messages to Syslog)

This option enables or disables Syslog messages which are generated from the NTP service.

This value has no effect if Syslog is not configured in the ALARM tab (see ***Chapter 7.3.5.1 Syslog Configuration***).

7.3.3.4.3 Crystal Operation

Crystal Operation / Switch to Specific Stratum

If the Sync Source connected to the module supplies an inadequate or no time information required for the time synchronization of the Module the NTP service of the Time Server 8030NTS/M usually behaves in the way that the receipt of time information is stopped from the Sync Source and the stratum value reset to 16 (defined as invalid in NTP).

> ⚠ NTP Clients do not accept time information from a NTP Time Server with stratum 16 (invalid). Briefly, as long as the Time Server 8030NTS/M indicates the stratum value 16, NTP Clients are not synchronized.

This behaviour of NTP during crystal operation of the Sync Source can be changed. Therefore the function "*Switch to specific stratum*" should be enabled by setting the value to "*enabled*" and the so-called downgrading stratum (= stratum value of the Time Server 8030NTS/M during crystal operation of the Sync Source).

For the sychronization of NTP Clients during crystal operation of the Sync Source or for testing the system without connected synchronization source, in the setting "*enabled*" any stratum value between 1 and 15 can be set.

Crystal Operation / Stratum in Crystal Operation

The value defined here (range 1-15) designates the transmitted fallback NTP stratum level of the module in "*Quartz*" synchronization status. Stratum 1 should be configured if downgrading is not desired in status "Quartz".

> ⚠ The NTP service MUST also be restarted (see **Chapter 7.3.3.6 Restart NTP**).

> ⚠ Using the option "*Switch to specific stratum*" the NTP Clients are synchronized with time information indicated in the general menu of the WebGUI of the Sync Source during crystal operating. Whether this time information (e.g. through drift) is imprecise or the time is manually set (wrong) cannot be detected by the NTP Client!

> ⚠ In case the value 1 is used for *"Stratum in crystal operation"*, the NTP Client cannot not verify whether the Time Server 8030NTS/M is synchronised or runs in crystal operation. Should a differentiation be wished between synchronized and crystal operation the downgrading stratum needs to be set to a value between 2 and 15.

The value is only adjustable if the "*Switch to specific stratum*" function is enabled.

7.3.3.4.4 Broadcast / Broadcast Address

This section is used to configure the Time Server 8030NTS/M 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 Server 8030NTS/M. 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 Server 8030NTS/M 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.

7.3.3.4.5 Broadcast / 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.
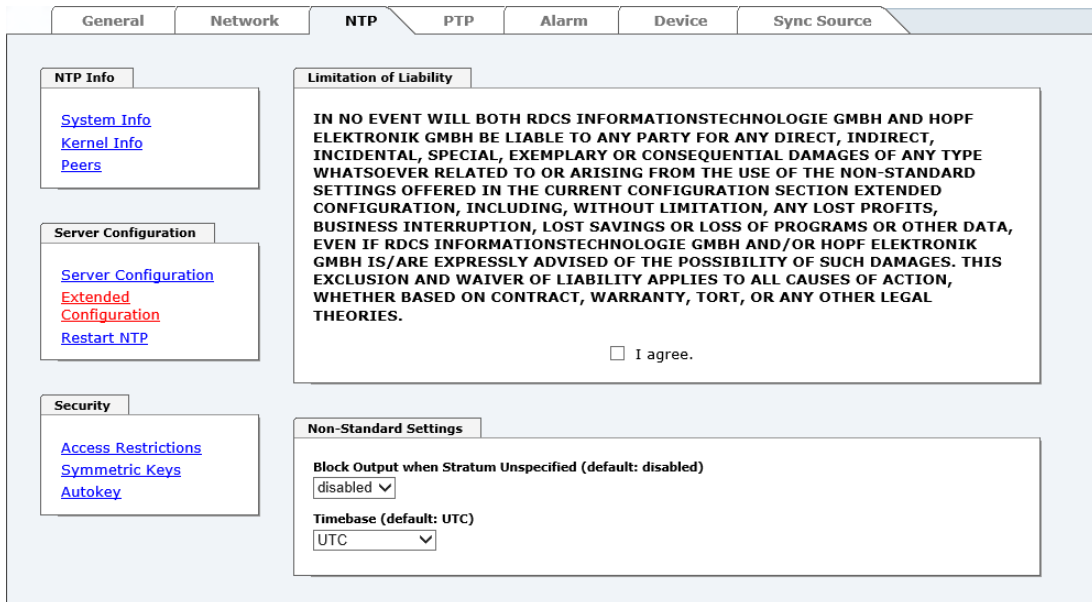
7.3.3.4.6 Additional NTP SERVERS

Adding further NTP servers provides the opportunity to implement a security system for the time service. However, this affects the accuracy and stability of the Time Server 8030NTS/M.

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

7.3.3.5 Extended NTP Configuration

NTP is a protocol for synchronising clocks of computer systems over packet-switched data networks. For special applications the NTP time base of the Time Server 8030NTS/M can be configured to local and standard time via the base system.

For activation of this special NTP output, the customer's approval shown in the WebGUI needed to be declared by checking the field "I agree".

7.3.3.5.1 Suppression of unspecified NTP outputs (Block Output when Stratum Unspecified)

Unspecified NTP outputs that e.g. are generated by NTP at re-start, are suppressed when this function is activated.

7.3.3.5.2 NTP Timebase

For custom applications this function enables adjustment of the time base of the NTP output.

Entering this function the transmitted time protocol of the Time Server 8030NTS/M is not conform to the NTP standard anymore.
According to the NTP standard NTP uses only the UTC time base. The NTP time protocol does not allow any leaps in time.

This function is only allowed for the Output of NTP
In case of activated function the output of the Time Server 8030NTS/M for *SINEC H1 TIME DATAGRAM / TIME / DAYTIME* is released with a wrong time basis. Therefore this datagram should be deactivated for security reasons.

<table>
<tr><td>⚠️</td><td>

Following configuration steps for the activation of the NTP time basis are required:

- Select the wished NTP time base.

- Transfer the setting with **Apply Changes** to the Time Server 8030NTS/M.

- Fail-save storage of the configuration by pressing **Save to Flash within 10 seconds**.
Depending on the activated time base leap a board reset might be released after transfer with Apply Changes eliminating non saved configurations.

</td></tr>
</table>

UTC - NTP with Time Basis UTC

According to the RFC standard NTP uses only the UTC time base.

NTP with the Time Base Standard Time

Using the NTP time protocol with the standard time base the released time information correspond with UTC plus the time difference, adjusted in the base system **without** considering the daylight saving time changeover.

NTP with the Time Base Local Time

Output of the NTP time protocol with the local time base the released time information correspond with UTC plus the time difference and the additional offset for the possible summer time, adjusted in the base system.

NTP does not allow any leaps in time. Using the NTP time protocol with the local time base the internal NTP process of a board is restarted based on a summer-/winter time adjustment.

<table>
<tr><td>⚠️</td><td>

Using the NTP time protocol with the local time base the summer-/winter time adjustment is released one to two minutes belated.

Afterwards the local time is correctly available in the NTP time protocol. Therefore, within this transition period a requested NTP time protocol is replied by the former time base.

</td></tr>
</table>

<table>
<tr><td>⚠️</td><td>

Changing the time base for the output of the protocol for NTP is only designed for customized applications and does not correspond with the standard of NTP. The synchronisation of a standard NTP-Client with a time basis deviating from UTC results in a wrong time information in the standard NTP-Client and might cause time leaps!

</td></tr>
</table>

7.3.3.6 Restart NTP

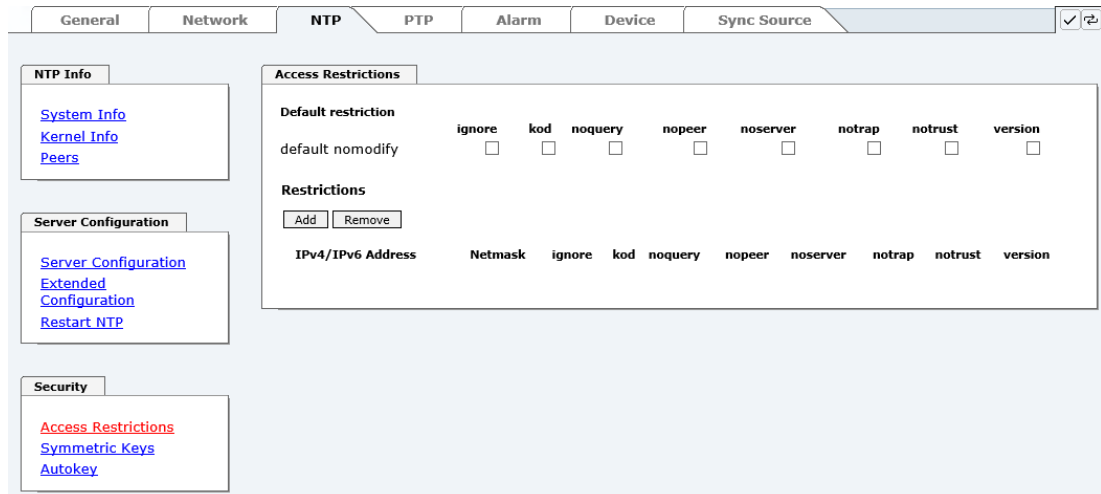The following screen appears after clicking on the Restart NTP option:
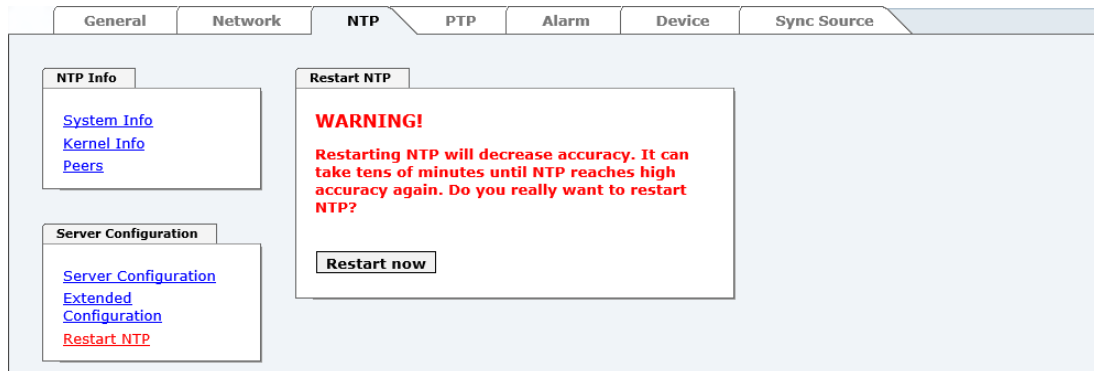
Restarting NTP services is the only possibility of making NTP changes effective without having to restart the entire Time Server 8030NTS/M. As can be seen from the warning message, the currently reachable stability and accuracy get lost caused by this restart.

> After a restart of the NTP service it takes up to 10 minutes until the NTP service on the Time Server 8030NTS/M is completely adjusted.

7.3.3.7 Configuring the NTP Access Restrictions

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

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 **7.3.3.7.1** to **7.3.3.7.4** must be checked by the user:

7.3.3.7.1 NAT or Firewall

Are incoming connections to the NTP Service blocked by NAT or a Stateful Inspection Firewall?	
No	Proceed to *Chapter 7.3.3.7.2 Blocking Unauthorised Access*
Yes	No restrictions are required in this case. Proceed further to *Chapter 7.3.3.7.4 Internal Client Protection / Local Network Threat Level*

7.3.3.7.2 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 7.3.3.7.3 Allowing Client Requests*
Yes	In this case the following restrictions are to be used: **ignore in the default restrictions** ☑ 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 7.3.3.7.5 Addition of Exceptions to Standard*

7.3.3.7.3 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	In this case select from the following standard restrictions: See *Chapter 7.3.3.7.6 Access Control Options* **kod** ☑ **notrap** ☑ **nopeer** ☑ **noquery**. ☑
Yes	In this case select from the following standard restrictions: See *Chapter 7.3.3.7.6 Access Control* Options: **kod** ☑ **notrap** ☑ **nopeer** ☑ 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 7.3.3.7.5 Addition of Exceptions to Standard .*

7.3.3.7.4 Internal Client Protection / Local Network Threat Level

How much protection from internal network clients is required?	
Yes	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 7.3.3.7.6 Access Control Options.* **kod** ☑ **notrap** ☑ **nopeer** ☑

7.3.3.7.5 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.

 An unrestricted access of the Time Server 8030NTS/M 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 ☑

The entry of exceptions also works for IPv6 addresses. For this, the IPv6 address must be entered in the column IPv4/IPv6 Address and the length of the IPv6 net mask must be entered in the Netmask column.

7.3.3.7.6 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/ntpdc, 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 7.3.3.6 Restart NTP***).

NTP Time Server Module with 2x 10/100/1000 MBit LAN Interfaces 8030NTS/M - V05.00

7.3.3.8 Symmetric Key

7.3.3.8.1 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

7.3.3.8.2 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 Time Server 8030NTS/M). 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.

7.3.3.8.3 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/.

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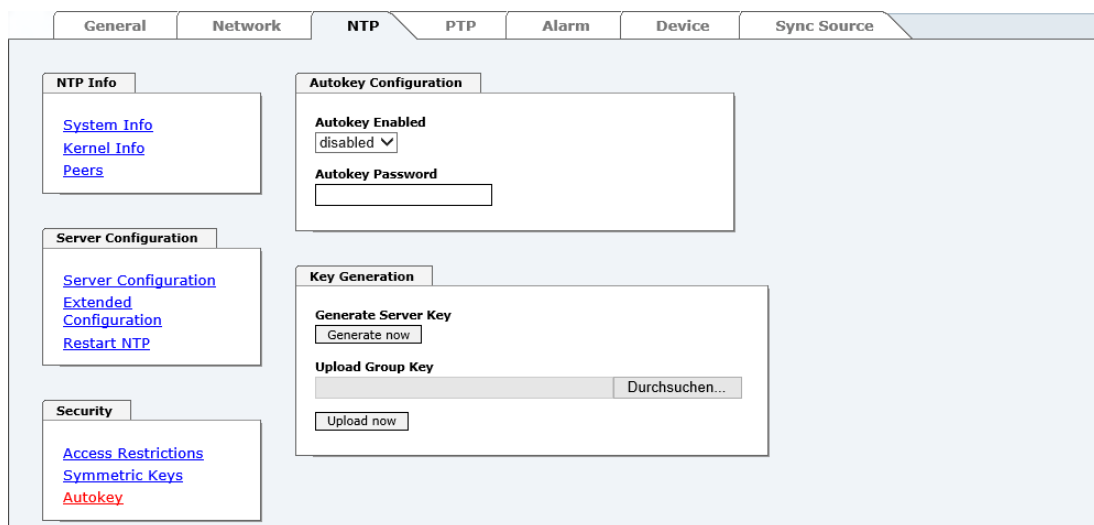
The basic authentication is a digital signature and no data encryption (if there are any differences between the two). The data packet and the key are used to create a non-reversible number which is attached to the packet.

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

7.3.3.9 Autokey

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.

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 Server 8030NTS/M 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 7.3.3.6 Restart NTP**).

7.3.4 PTP Tab

This Tab shows information and adjustment possibilities of the PTP service of the Time Server 8030NTS/M.
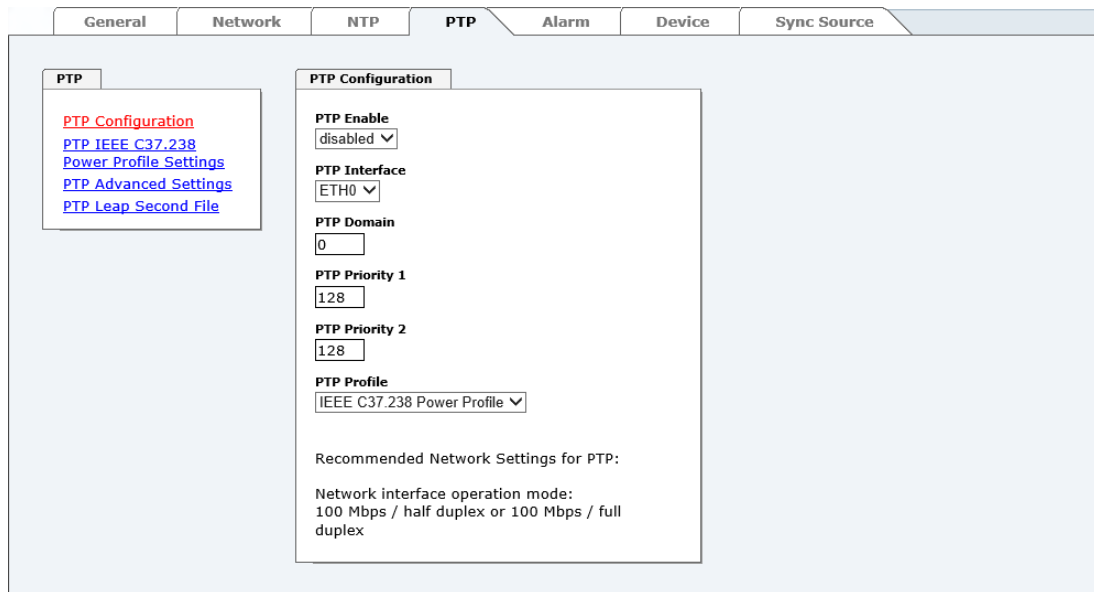
PTP functionality is provided by a PTP-Demon running on the embedded Linux of the Time Server 8030NTS/M.

Depending on the receiving conditions and under unfavourable circumstances it may take several hours until long-term accuracy is obtained (normally 5-10 minutes).

The PTP-Demon is implemented according to standard IEEE 1588-2008. More detailed description of the adjustable value in the PTP tab and their effects on the PTP-Demon can be found in this standard.

7.3.4.1 PTP Configuration

The "PTP Configuration" window provides basic settings of the PTP service.

PTP Enable

This option activates or deactivates the PTP service.

Remark: Changes in the "Network Interface …" settings in the "NETWORK" tab, can lead to the deactivation of "PTP Enable".

PTP Interface

This option sets the network interface that is used by the PTP service.

The content of the drop down depends on the settings in the "NETWORK" tab.

If "NIC Bonding / Teaming active" is active, only "BOND0" can be chosen.

If "NIC PRP active" is active, only "PRP0" can be chosen.

If "NIC Bonding / Teaming active" and "NIC PRP active" are inactive, "ETH0" or "ETH1" can be chosen.

PTP Domain

This option controls the PTP domain.

- Value-range: 0 to 255

PTP Priority 1

This option controls the PTP priority 1.

- Value-range: 0 to 255

PTP Priority 2

This option controls the PTP priority 2.

- Value-range: 0 to 255

PTP Profile

This option supports the selection of predefined profiles. Either "None" or "IEEE C37.238 Power Profile" can be selected.

If "IEEE C37.238 Power Profile" is selected, all settings in the "PTP Advanced Settings" window are set according to the standard IEEE C37.238 and all the settings in that window cannot be modified. The options in the "PTP IEEE C37.238 Power Profile Settings" window are only used by the PTP service when this profile is selected.

If "None" is selected, the settings in the "PTP Advanced Settings" window can be modified and the settings in the "PTP IEEE C37.238 Power Profile Settings" window are not used by the PTP service.

7.3.4.2 PTP IEEE C37.238 Power Profile Settings

The "PTP IEEE C37.238 Power Profile Settings" window supplies settings for the IEEE C37.238 standard. They only affect the PTP service if the "IEEE C37.238 Power Profile" profile is selected in the "PTP Configuration" window.

PTP Grandmaster ID

This option controls the PTP Grandmaster ID.

- Value-range: 3 to 254

Time Zone Name
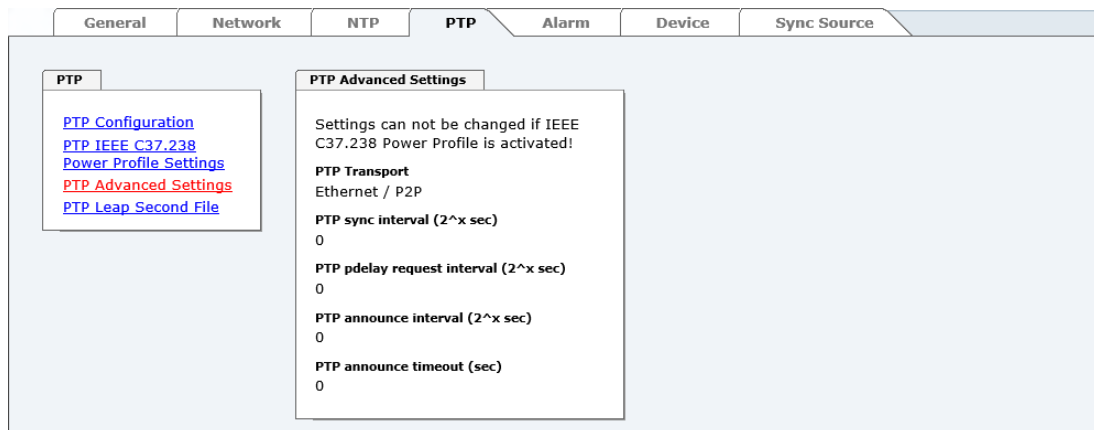
This option controls the time zone name.

- String length: 10 characters

This setting is used as "display name" in the "ALTERNATE_TIME_OFFSET_INDICATOR TLV". The other parameters that are needed by this TLV are taken from the system settings.

7.3.4.3 PTP Advanced Settings

The "PTP Advanced Settings" window supplies settings for the communication of the PTP service. These settings can be only changed, if the "PTP Profile" is set to "None" in the "PTP Configuration" window.

PTP Transport

This setting determines the network protocol that is used by the PTP service.

Possible choices: "Ethernet / P2P", "Ethernet / E2E" and "IPv4 / E2E"

PTP sync interval (2^x sec)

This setting determines the sending interval of SYNC messages of the PTP service.

The sending interval is calculated in the following way:

- x … selected value in the WebGUI
- Sending interval = 2^x
- Value-range: -7 to 6

The sending interval can be chosen between 0.0078125 seconds up to 64 seconds.

PTP pdelay request interval (2^x sec)

This setting determines the sending interval of Path Delay or Delay messages of the PTP service.

The sending interval is calculated in the following way:

- x … selected value in the WebGUI
- Sending interval = 2^x
- Value-range: -7 to 6

The sending interval can be chosen between 0.0078125 seconds up to 64 seconds.

PTP announce interval (2^x sec)

This setting determines the sending interval of Announce messages of the PTP service.

The sending interval is calculated in the following way:

- x … selected value in the WebGUI
- Sending interval = 2^x
- Value-range: -4 to 6

The sending interval can be chosen between 0. 0625 seconds up to 64 seconds.

PTP announce timeout

This setting determines how many seconds the PTP service stays in the LISTENING state.

- Value-range: 2 to 255

The value entered corresponds to the seconds that the PTP service spends in the LISTENING state.

7.3.4.4 PTP Leap Second File

The "PTP Leap Second File" window supplies a functionality to upload a Leap-Second-File to the Time Server 8030NTS/M.

This file informs the PTP service, how many seconds UTC and TAI time differs.

In case of announcing a leap second by the synchronization source the leap second file will automatically be updated.

If time server 8030NTS/M is not in operation during the whole announcing time, it is not possible for the application to update its leap second file. The leap second file needs to be updated next time when time server is put in operation.

> On the following website
> https://www.ietf.org/timezones/data/leap-seconds.list
> a current version of the leap second file can be downloaded.

UTC-TAI offset

This field shows the actual value, that the PTP service uses, for the difference of UTC and TAI time.

Date of Next Leap Second

This box shows if and if yes when the next leap second is going to be inserted.

NTP Time Server Module with 2x 10/100/1000 MBit LAN Interfaces 8030NTS/M - V05.00

7.3.5 ALARM Tab (Activation Key necessary)

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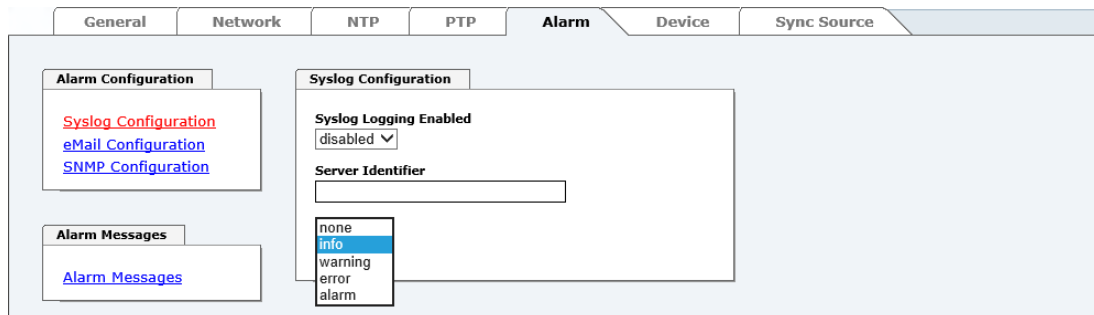
7.3.5.1 Syslog Configuration

It is necessary to enter the name or IPv4 or IPv6 address of a Syslog server in order to store every configured alarm situation which occurs on the module in a Linux/Unix Syslog. If everything is configured correctly and enabled (depending 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 in the system itself is not possible as therefore the internal 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!
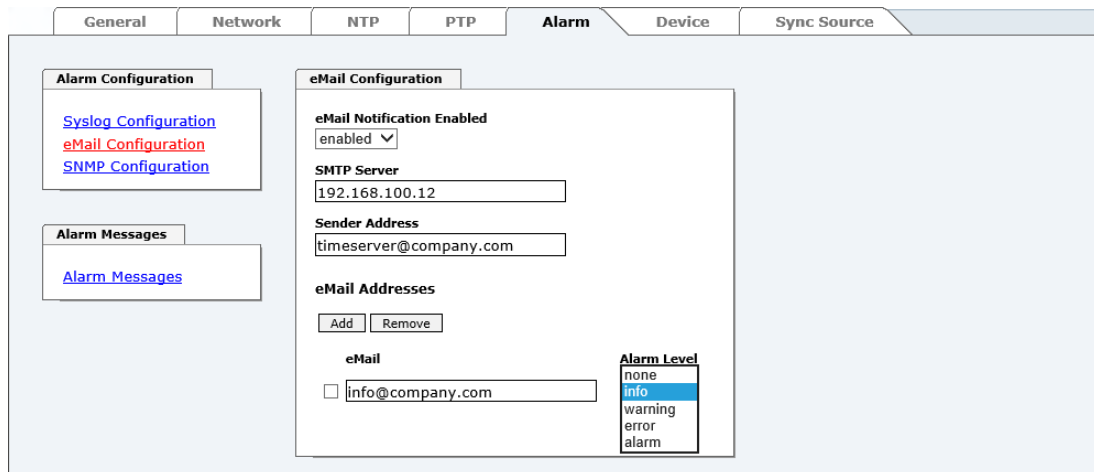
The alarm level designates the priority level of the messages to be transmitted and the level from which transmission should take place (see *Chapter 7.3.5.4 Alarm Messages*).

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

The NTP service implemented in the system can transmit its own Syslog messages (see *Chapter 7.3.3.4.2 NTP Syslog Messages (General / Log NTP Messages to Syslog)*).

7.3.5.2 E-mail Configuration

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

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

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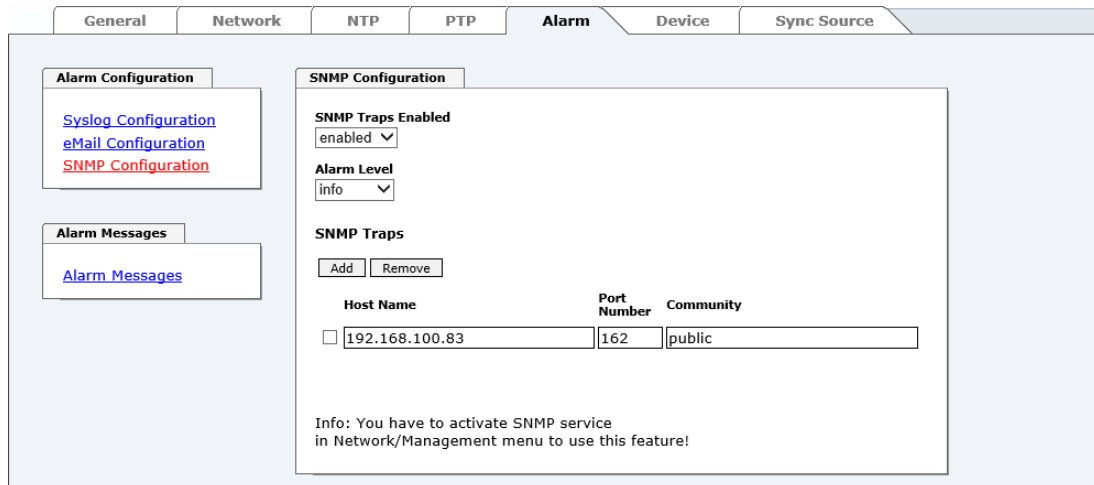
Some E-mail servers only accept messages if the sender address entered is valid (spam protection). This can be inserted in the "Sender Address" field.

The Alarm Level designates the priority level of the messages to be sent and determines from which level the message should be sent (see **Chapter 7.3.5.4 Alarm Messages**).

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

7.3.5.3 SNMP Configuration / TRAP Configuration

It is possible to use an SNMP agent (with MIB) or to configure SNMP traps in order to monitor the module 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 7.3.6.11 Downloading Configuration Files / SNMP MIB*).

The Alarm Level designates the priority level of the messages to be sent and determines from which level the message should be sent (see *Chapter 7.3.5.4 Alarm Messages*).
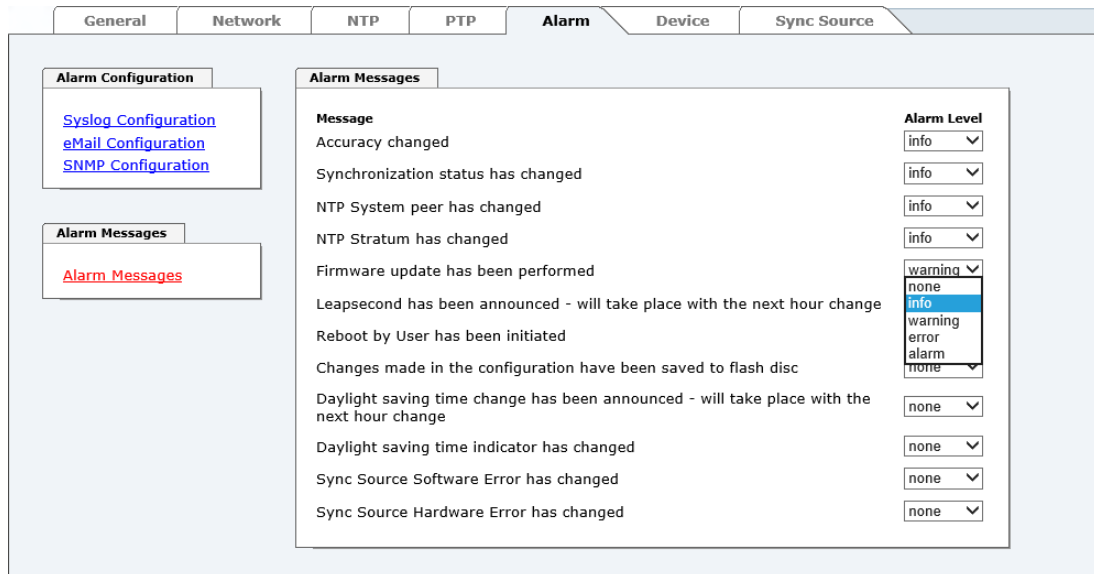
Alarm Level	Transmitted Messages
none	no messages
info	info / warning / error / alarm
warning	warning / error / alarm
error	error / alarm
alarm	alarm

! The SNMP protocol must be enabled in order to use SNMP (see *Chapter 7.3.2.7 Management (Management-Protocols – HTTP, SNMP)*).

7.3.5.4 Alarm Messages

Every message shown in the image can be configured with the displayed alarm levels. Selection of the level NONE means that this message is completely ignored.
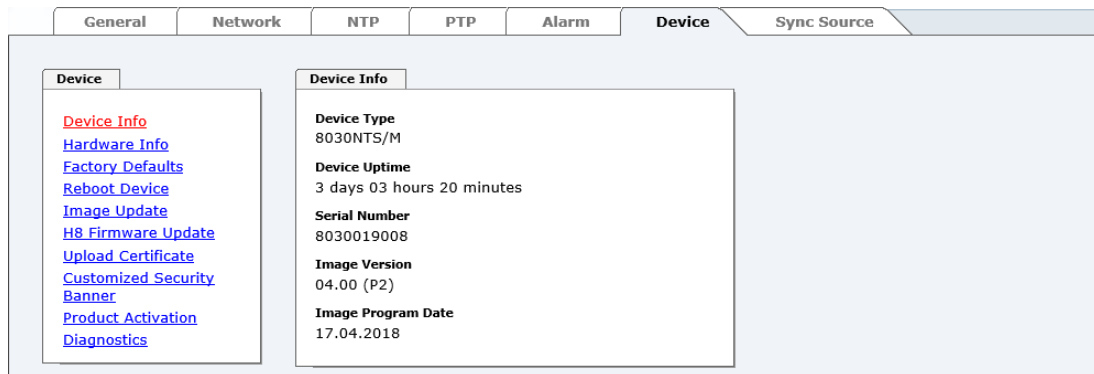
Depending on the messages, their configured levels and notifications levels of the E-mails, a corresponding action is carried out if an event occurs.

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

NTP Time Server Module with 2x 10/100/1000 MBit LAN Interfaces 8030NTS/M - V05.00

7.3.6 DEVICE Tab

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

This tab provides the basic information about the hardware of Module 8030NTS/M as well as 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.
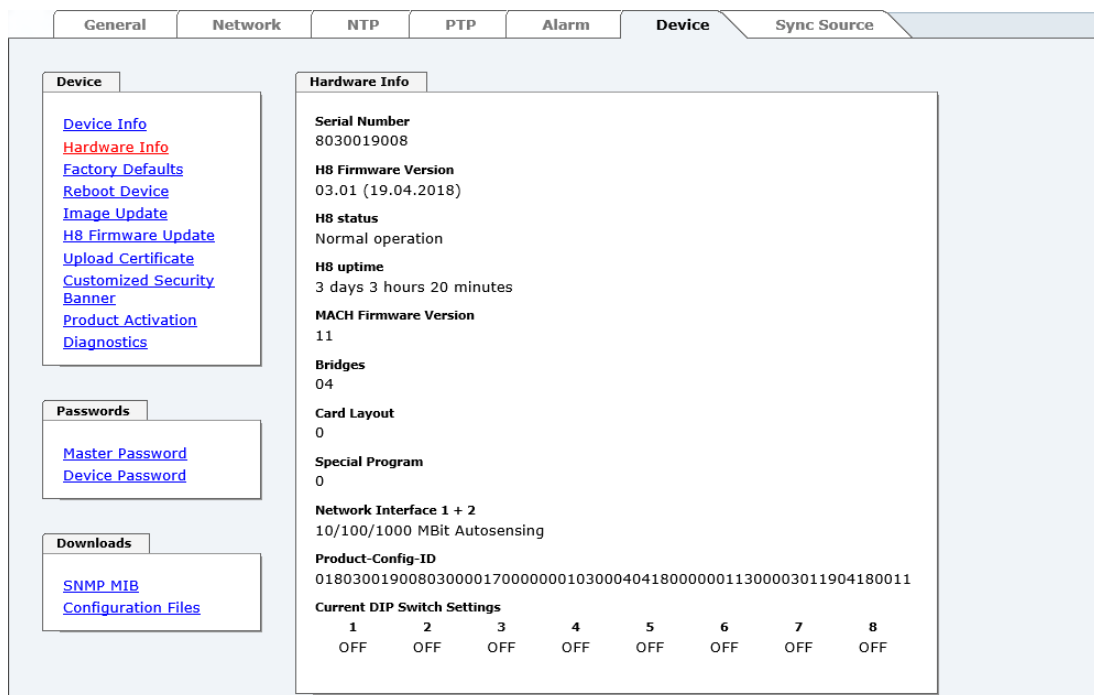
7.3.6.1 Device Information

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

7.3.6.2 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.

The display "Current DIP Switch Settings" is not applicable for this device.

7.3.6.3 Restoring the Factory Defaults Settings

In some cases it may be necessary or wished to reset all settings of module 8030NTS/M to factory settings (factory defaults).
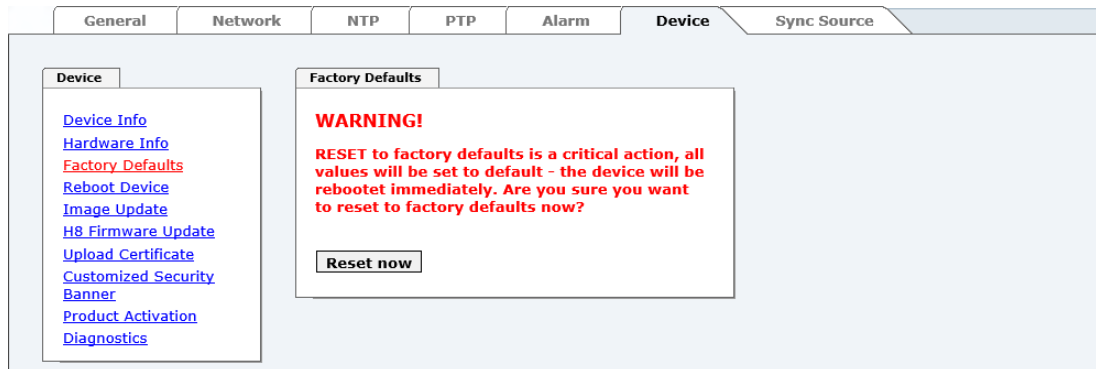
This function serves to reset all values in the flash memory to their factory default values. This also includes passwords (see **Chapter 12 Factory Defaults of Time Server 8030NTS/M**).

Please log in as a "Master" user in accordance with the description in **Chapter 7.2.1 LOGIN and LOGOUT as User**

Pressing the "**Reset now**" button releases setting of the factory default values.

Once this procedure has been triggered there is NO possibility of restoring the deleted configuration.
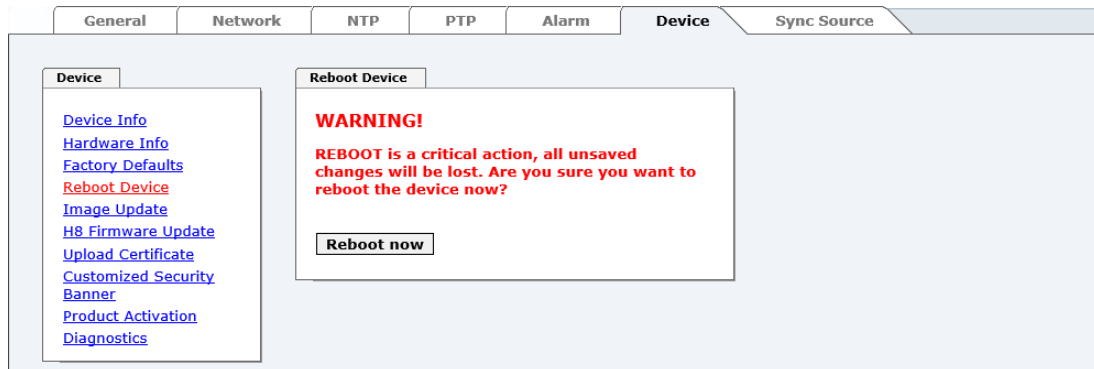
> **i** A **Factory Default** requires a complete check and optionally a new configuration of the Module 8030NTS/M. In particulary the default MASTER and DEVICE passwords should be reset.

7.3.6.4 Restarting the Module (Reboot Device)

> ⚠ The restart concerns the Module 8030NTS/M only but **not** the Sync Source.

> ⚠ All settings **not** saved with "**Save**" are lost on reboot (see *Chapter 7.2.3 Enter or Changing Data*).

Moreover the **NTP service** implemented in the system is restarted. This leads to a renewed alignment phase with the loss of the stability and accuracy reached up to this point.
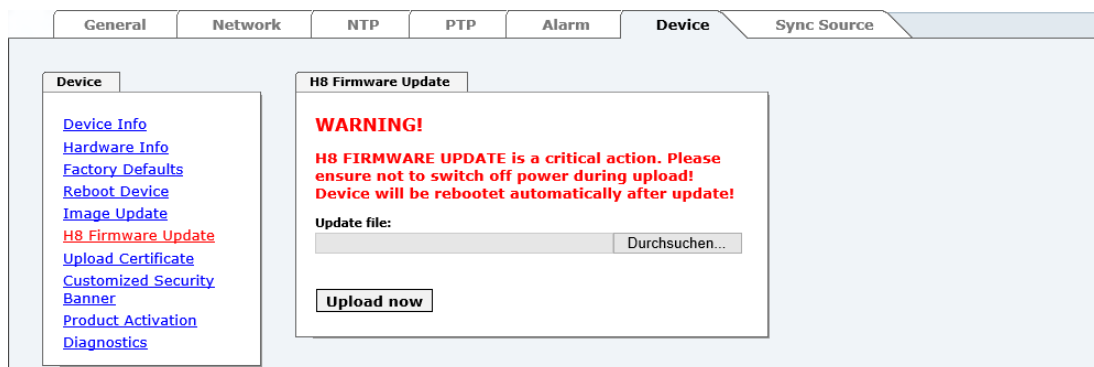
Log in is carried out as "Master" user in accordance with the description in *Chapter 7.2.1 LOGIN and LOGOUT as User*.

Press the "**Reboot now**" button and wait until the restart has been perfomed.

7.3.6.5 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.):
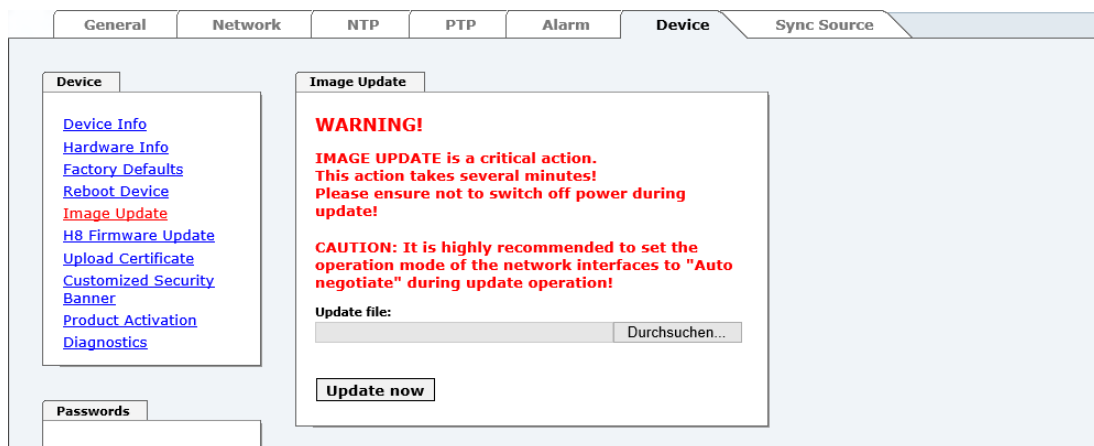
H8-8030NTS-M_v0100_128.**mot**   for the **H8 firmware**
(update takes approx. 1-1.5 minutes)

upgrade_8030gen_v0300.**img**   for the **embedded image**
(update takes approx. 2-3 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.
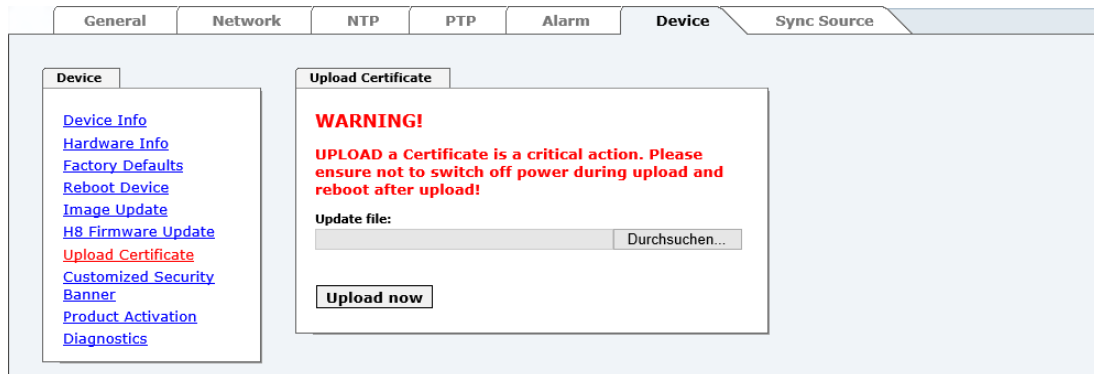
After the image-update the WebGUI displays a window to confirm the restart (reboot) of the board.
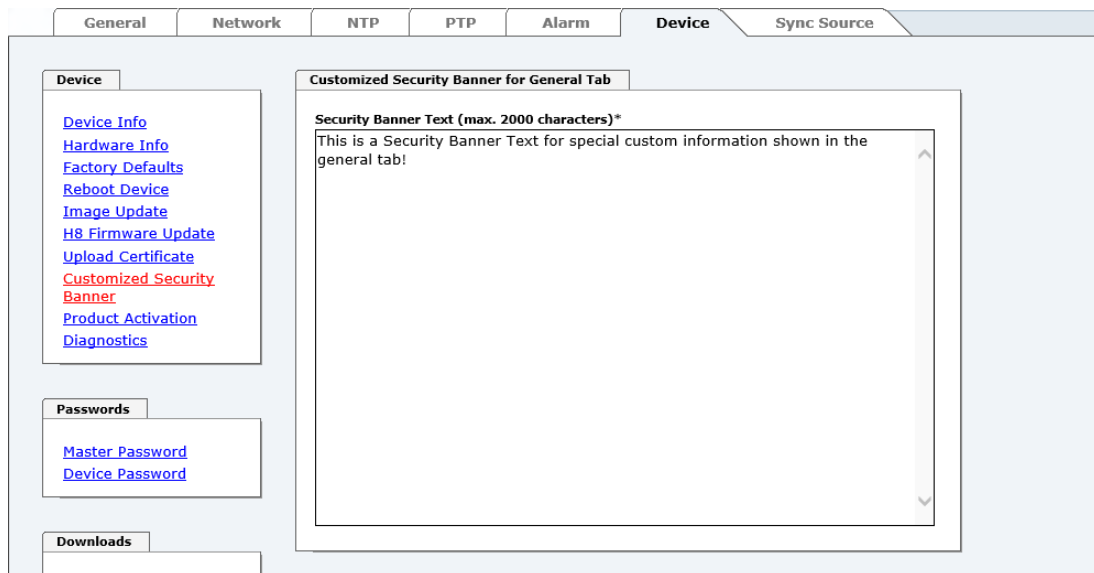
7.3.6.6 Upload of User SSL-Server-Certificate (Upload Certificate)

This offers the possibility to encrypt the https connections to the module with a user-provided SSL server certificate.

7.3.6.7 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. There are 2000 characters available to write failsafe into the device.

When saving the text, only the following characters are accepted (all other characters are discarded and therefore not displayed on the General page!):

- Capital letters (A…Z)

- Lowercase letters (a…z)

- Numbers (0…9)

- The following special characters: space (" "), exclamation mark ("**!**"), Comma ("**,**"), dot ("**.**"), Colon ("**:**"), question mark ("**?**")
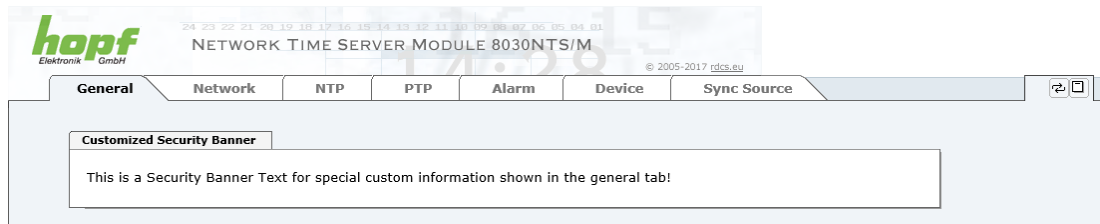
After a successful storage the "Customized Security Banner" with the saved security information is displayed in the General-Tab.

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

7.3.6.8 Product Activation by means of Activation Keys

For the activation of optional functions, e.g "Network Interface Bonding/Teaming", 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 8030NTS/M 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 function FACTORY DEFAULTS.

NTP Time Server Module with 2x 10/100/1000 MBit LAN Interfaces 8030NTS/M - V05.00
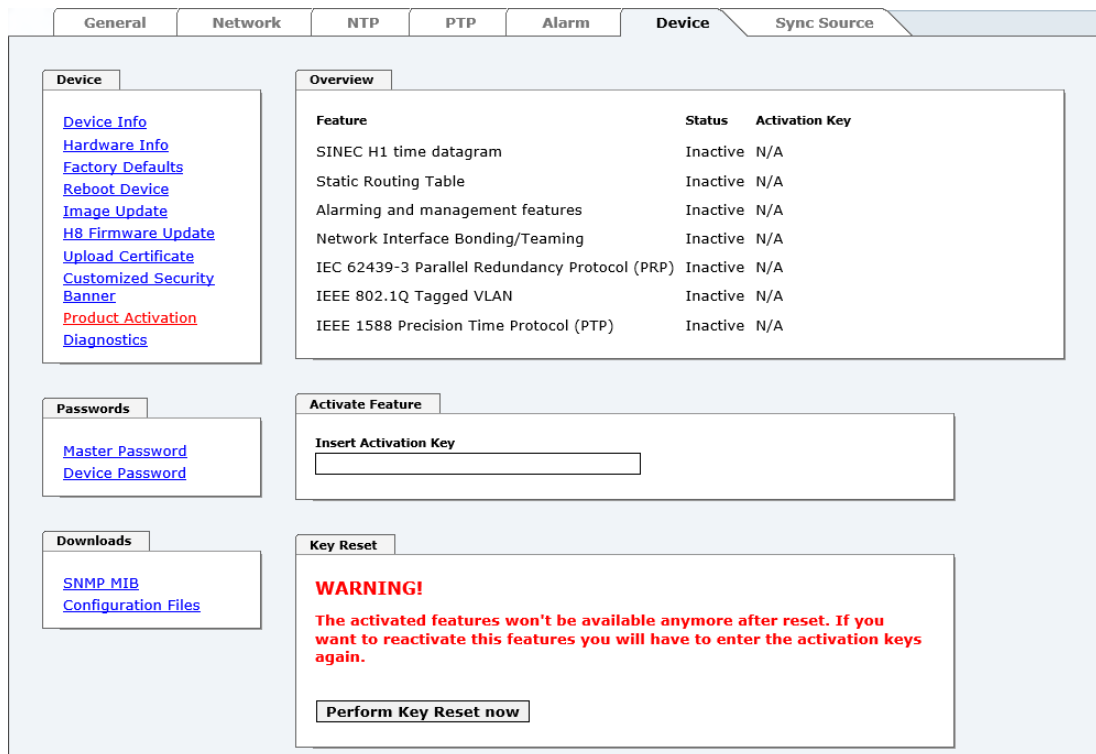
Overview

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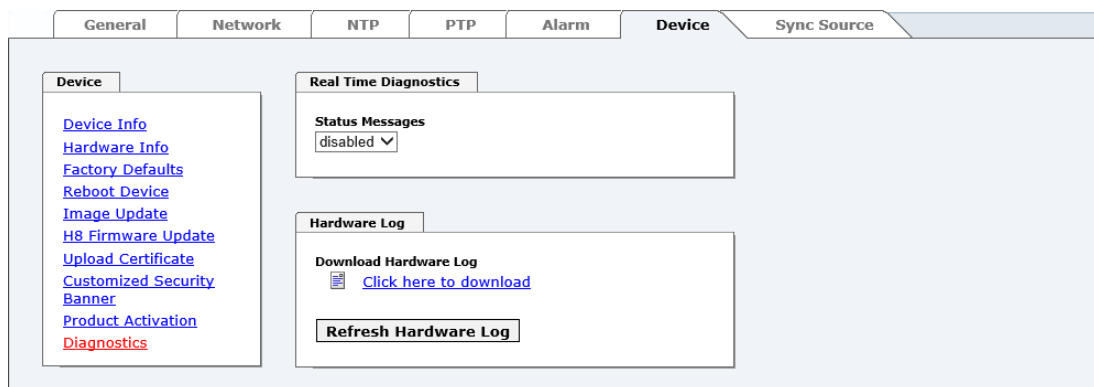
If the activation was successful the new feature is listed in the overview with status "Active" and can be used immediately.

Key Reset

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

7.3.6.9 Diagnostics Function

It "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.

7.3.6.10 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:

[ ] ( ) * - _ ! $ % & / = ?
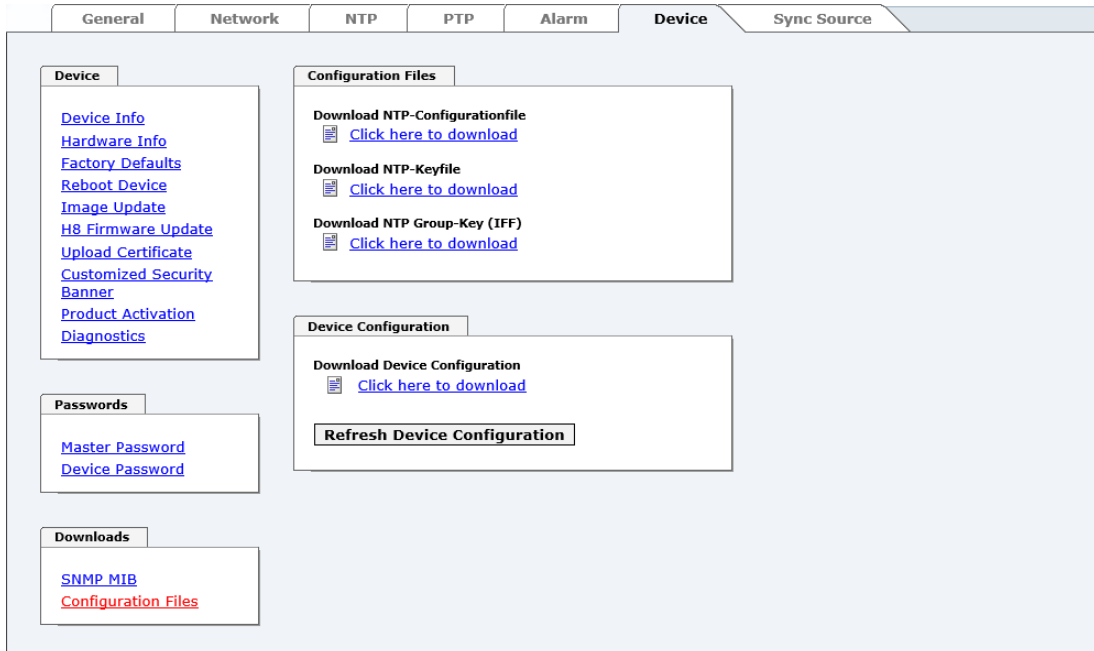
(See also *Chapter 7.2.1 LOGIN and LOGOUT as User*)

⚠ A new password must contain at least one capital letter and lowercase letter, a number, and six characters.

7.3.6.11 Downloading Configuration Files / SNMP MIB

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.

---

i	The loaded file **System Configuration** from the module is only used for support purposes and cannot be reloaded for adjusting the settings in the Time Server 8030NTS/M.

!	For the download of the file **System Configuration** the following process is mandatory: 1. Pressing the button **SAVE** 2. Pressing the button `Refresh System Configuration` 3. Perform the download of the file

The "private _hopf_ enterprise MIB" is also available via the WebGUI in this area.

NTP Time Server Module with 2x 10/100/1000 MBit LAN Interfaces 8030NTS/M - V05.00

7.3.7 SYNC SOURCE Tab

The complete display and parameterization of the synchronization of the module by the respectively fed Sync Source takes place in this tab.

The modified values in the tab SYNC SOURCE are directly adopted by pressing the button 1 and failsafe stored. This behaviour is indicated on the modified display of the Apply button. The buttons 2 and 3 are without function in the tab SYNC SOURCE and are not required.
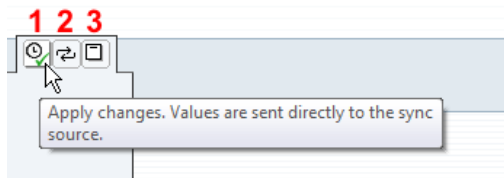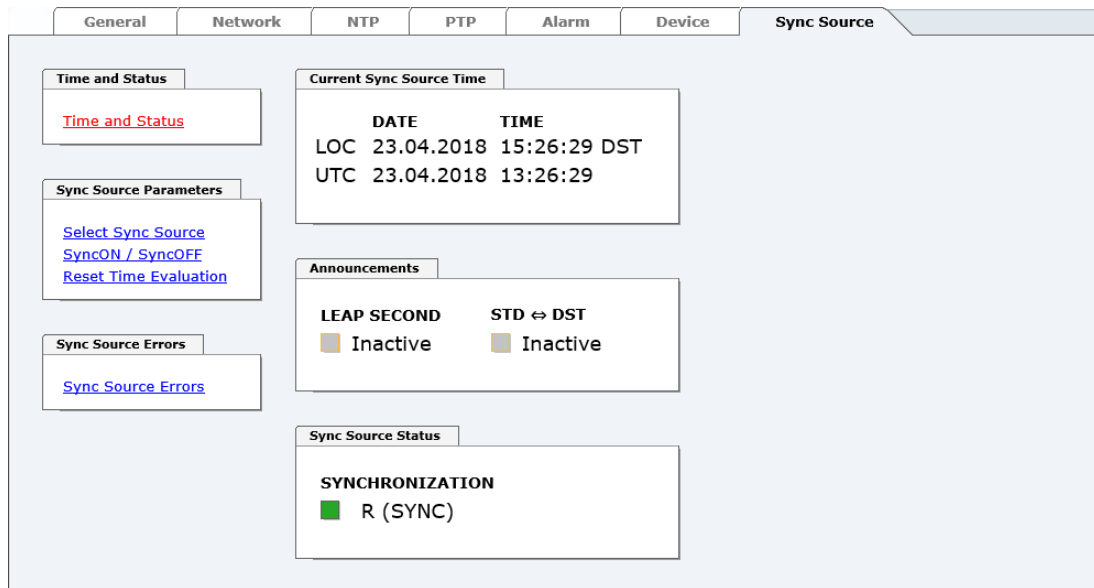
| ! | After the data transfer it can take up to 30 seconds until the modified data are modul-internally reapplied for the WebGUI indication. |

| ! | Generally it is recommended to activate the function **Reset Time Evaluation** after peforming modifications of the Sync Source settings (e.g. using the module in a stand-alone converter). This ensures that the modul-internal time information is really provided by the reset Sync Source. |

7.3.7.1 Time and Status

Current Sync Source Time

This area indicates the curent time and date of the Sync Source. Both the local and UTC time are displayed.

> ⚠ In theory, depending on the synchronization status of the Sync Source, the time displayed here can differ from the NTP time since two independent time systems are involved.

Announcements
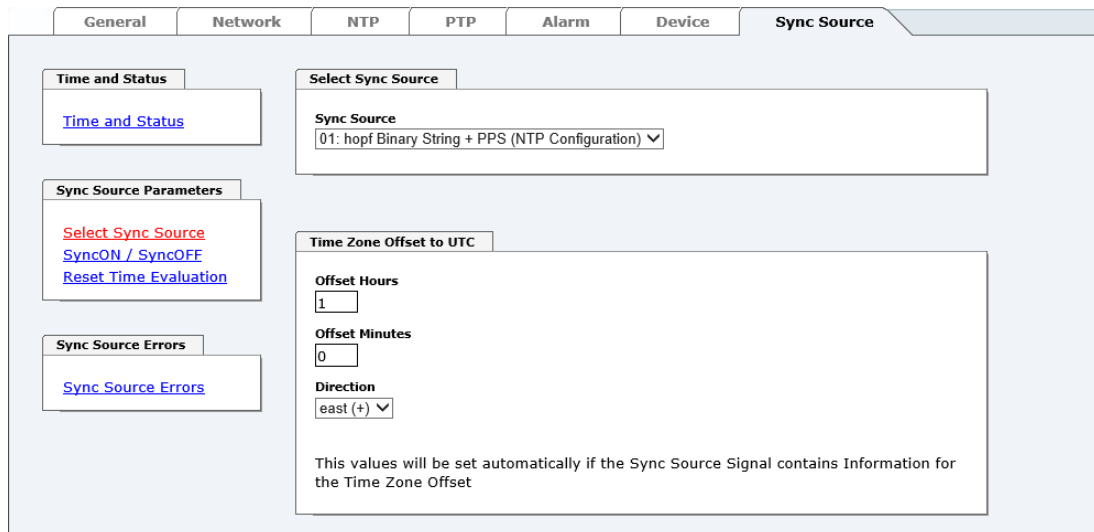
The display fields LEAP SECOND and STD ⇔ DST announce a corrosponding event to the next hour (insertion of a leap-second or rather switch-over of summer/winter time).

Sync Source Status

Display of the actual status of synchronization of the Sync Source with these possible values:

SYNC	Time synchronized + Quartz regulation started/running
SYOF	Time synchronized + SyncOFF running
SYSI	Time synchronized as simulation mode (without 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 manual setting
INVA	Invalid time

7.3.7.2 Select Sync Source

The Module 8030NTS/M can be synchronized by different time information. Using these modules in *hopf* basis systems the necessary settings are performed by default.

Using the module in converter units the settings may be required by the customer.

This selection determines what kind of time information should be evaluated by the module.

Currently *hopf* specific time formats as well as the DCF77 pulse (1Hz) with local time are available for the synchronization.

01: *hopf* Binary string with PPS (NTP configuration)
02: *hopf* System-BUS 6000 with PPS
03: *hopf* System-BUS 7001 with PPS
04: *hopf* Master/Slave-String – Transmission cycle: Every minute
05: *hopf* Master/Slave-String – Transmission cycle: Every second
06: *hopf* Master/Slave-String with PPS – Transmission cycle: Every min.
07: *hopf* Master/Slave-String with PPS – Transmission cycle: Every sec.
08: DCF77 Pulse (1Hz) – Local time (MEZ)

⚠ There is no synchronization of the Module and also no generation of the signal for the output in case of an incorrect setting.

7.3.7.2.1 Difference Time (Time Zone Offset to UTC)

The input of the difference time (Time Zone Offset to UTC) by the user is only necessary for Sync Source time information that donot include the current difference time.
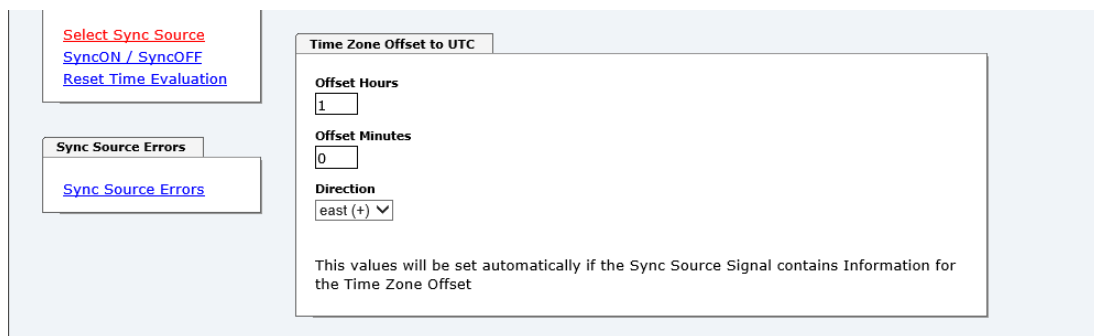
It is currently required for the synchronization by DCF77 pulse with local time.

> ⚠ The difference time to be entered **always** relates to **UTC** to **local time standard time (winter time)** although commissioning or the input of difference time takes place during summer time.

> ⚠ If the respectively set Sync Source supplies the current difference time with its time information the user's entered values are automatically overwritten with the information of the Sync Source after a successful synchronization.

- **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 Ttime

Entering the direction the local time deviates from world time:

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

7.3.7.3 SyncON / SyncOFF Timer

SyncON Timer

The SyncON timer is used to delay the sync-status "SYNC" by the set time although the module is already synchronous.

This function is enabled when adjustment processes should be terminated as defined before the sync status is "SYNC".

This function is not required for this module and should always be set to 0.

SyncOFF Timer

This value is used to provide reception failure bypassing resulting from the Sync Source. This timer shall allow an error-message free operation even if there are temporary problems with the Sync Source.

In the event of a reception failure of the Sync Soure, the re-synchronization of the Sync Source to **quartz** status is delayed by the set value. The module continues to run in synchronization status on the internally regulated, highly accurate quartz base during this period.

This timer is of special significance when certain system outputs are linked to a specific system status.

The Timer can be set from 2min. to 1440min.

Current Timer values

In case of an active Timer the appropriate value of the timer is displayed here.

7.3.7.4 Reset Time Evaluation

This function "Reset Time Evaluation" allows a setting back of the total internal evaluation of the module fed time information including any announcements for the summer/winter time switchover or rather insertion of a leap second.

> ⚠ The NTP service has its own and independent time. After processing this function, hence the NTP service receives time information unless the module-internal time basis has successfully been re-synchronized.

7.3.7.5 Sync Source Errors

This tab indicates the current failure status of the Sync Source or rather the components involved in the evaluatoon of the signals of the Sync Source.

> ℹ Sync Source describes in this module the supplied time information to the module as well as the modul-internal evaluation up to the successful synchronization of the modul-internal time basis.

> ℹ If collected error messages are displayed in the tab GENERAL (Sync Source Error) there is at least one error.
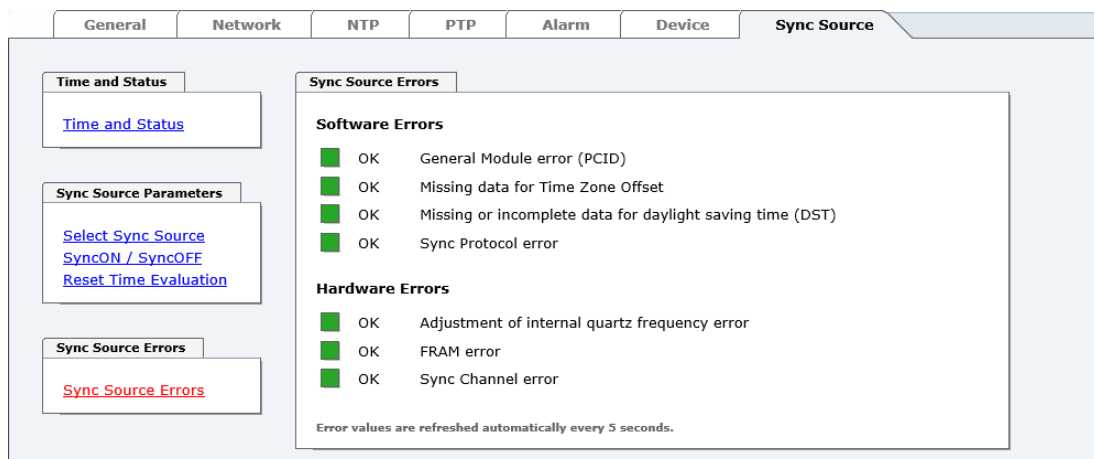
> ℹ This page is updated automatically every 5 seconds.

Overview Software Errors

- **General Module error (PCID)**

    If this error occurs even after a Power reset, the device is damaged.

- **Missing data for Time Zone Offset**

    Difference time (Time Zone Offset) shall be, where necessary, initially set by the user.

- **Missing or incomplete data for daylight saving time (DST)**

    The switchover times for summer/winter time shall be, where necessary, initially set / disabled by the user.

- **Sync Protocol error**

    The protocol being read or rather the time information of the Sync Source can neither be evaluated nor used.

Overview Hardware Errors

- **Adjustment of internal quartz frequency error**

    Problems with the internal quartz regulation of the Module 8030NTS/M have been occured. So the specified accuracy of the Sync Source cannot be guaranteed anymore.

- **FRAM error**

    If this error occurs even after a voltage reset, the support team of company *hopf* needs to be contacted for further actions.

- **Sync Channel error**

    No singal is detected on the module-internal inputs for the the time information.

7.3.7.5.1 Sync Protocol error

The protocol being read or rather the time information of the Sync Source can neither be evaluated nor used.

By default the "Sync Protocol error " is always set after a system reset. After start of the module the failure is set or rather be cancelled according to the received Sync Source protocol. This error is separately operated for each time format of the respective Sync Source. All used time protocols of the respective Sync Source may cause the setting of this failure.

Below the behaviour of the quality counter and the single formats of the Sync Source are described:

The respective quality counter evaluates the protocol of the time information received **every second** according to the following scheme:

Value range of the quality counter: 0-60

Quality counter +1 ⇨ all verifications are POSITIVE
Quality counter -5 ⇨ at least one verification is NEGATIVE

After a system reset:
    Initial value of the quality counter = 0
    Value of the quality counter = 0-30   ⇨ **Error "Sync Protocol error"**

If the quality counter has been >30 one time during operation:
    Quality counter = 0   ⇨ **Error "Sync Protocol error"**
    Quality counter ≠ 0   ⇨ **No error**

Sync Source with Output of SERIAL STRING and PPS

Serial String (Interval = every second or minute)

The internal string is controlled once per second or minute for:

- Plausibility of the strings structure
- Plausibility of the time information

If all the criteria of the string are met, the quality counter is incremented;
at least one not met criteria decrements the counter.

The protocols per minute **do not use a quality counter**. Here the error can be set or cancelled every minute depending on the result of the verification.

PPS (Interval = every second)

The PPS is controlled once per second for:

- The reception cycle is within 1000msec ±10msec
- Max. deviation of the pulse width ±40msec
- Pulse width max. 800msec

If all the criteria of the string are met, the quality counter is incremented;
at least one not met criteria decrements the counter.

NTP Time Server Module with 2x 10/100/1000 MBit LAN Interfaces 8030NTS/M - V05.00

Sync Source with Output of SERIAL STRING

Serial String (Interval = every second or minute)

The internalserial string is controlled once per second for:

- Plausibility of the strings structure
- Plausibility of the time information

If all the criteria of the string are met, the quality counter is incremented;
at least one not met criteria decrements the counter.

> **!** Protocols per minute **do not use a quality counter**. Here the error can be set or cancelled every minute depending on the result of the verification.

Sync Source with Output of DCF77 Pulse

DCF77 pulse (Interval = every minute)

The DCF77 time telegram is controlled once per minute for:

- Plausibility of the strings structure
- Plausibility of the time information
- Plausibility of pulse length
    - DCF77 pulse   low = 100msec. ±20msec.
    - DCF77 pulse   high = 200msec. ±20msec.

> **!** Protocols per minute **do not use a quality counter**. Here the error can be set or cancelled very minute depending on the result of the verification.

7.3.7.5.2 Sync Channel error

On the input of the adjusted Sync Source no signal nor activity is detected.

By default the error "Sync Channel" is **not** set after a System reset. After system start the error is set or rather be cancelled according to the activity on the signal input. This error is separately operated for each signal input. All used signal inputs of the respective Sync Source may cause the setting of a failure independently.

Based on no activity on a used signal input, the error "Sync Channel" is set at the end of the signal input **- Time OUT**. Each detected activity on this signal input sets the signal inputl - TimeOUT and thus resets the error.

Sync Source	Signal Input	Signal Input - TimeOUT
Serial String with PPS	Serial String	181 seconds
	PPS	61 seconds
Serial String	Serial String	181 seconds
DCF77 pulse	DCF77 Pulse	25 seconds

8   SSH and Telnet Basic Configuration

> ⚠ Only basic configuration is possible via SSH or Telnet. The complete configuration of the Time Server 8030NTS/M 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.
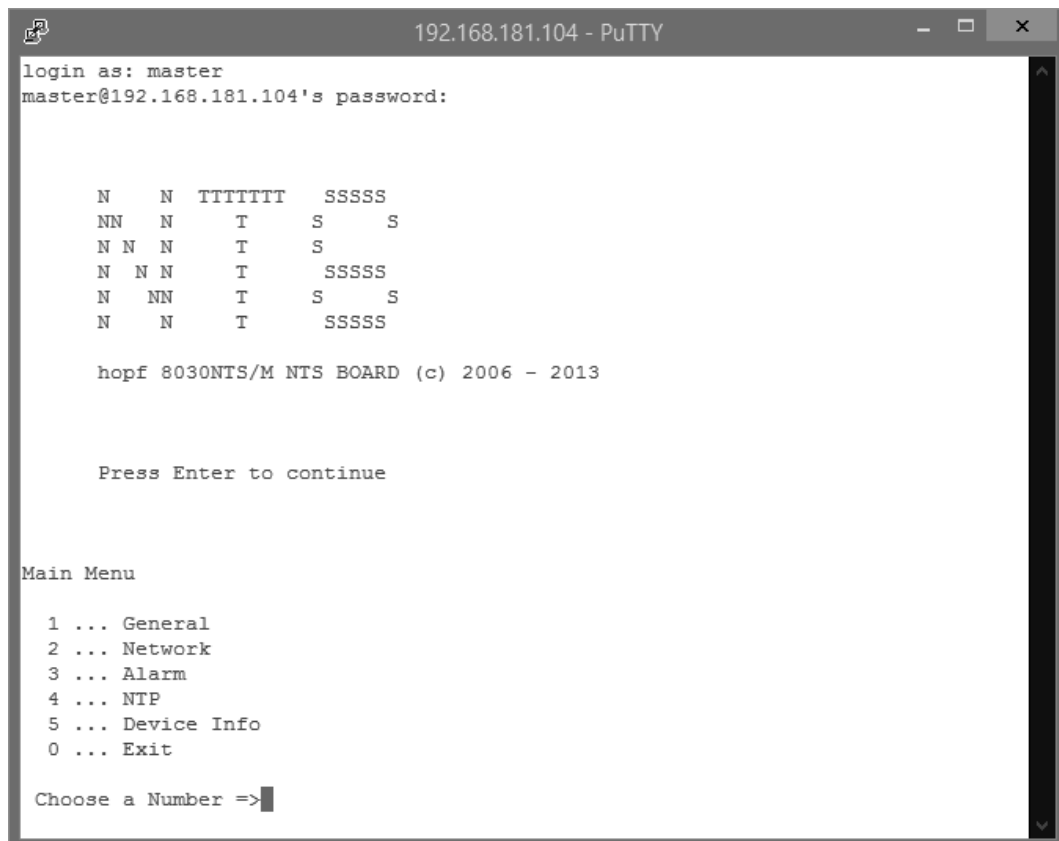
The user names and passwords are the same as on the WebGUI and are kept in alignment (see *Chapter 7.3.6.10 Passwords (Master/Device)*).

> ⚠ SSH does not allow blank passwords for safety reasons.

> ⚠ The corresponding protocols should be enabled for the use of Telnet or SSH (see *Chapter 7.3.2.7 Management (Management-Protocols – HTTP, SNMP)*).

```
                                    192.168.181.104 - PuTTY          _  □  ×
login as: master
master@192.168.181.104's password:


        N    N  TTTTTTT   SSSSS
        NN   N     T     S     S
        N N  N     T     S
        N  N N     T      SSSSS
        N   NN     T     S     S
        N    N     T      SSSSS

        hopf 8030NTS/M NTS BOARD (c) 2006 - 2013



        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).

9 Support from the *hopf* Company

Should the System show an undefined operating state or other error conditions arise, please contact the Support at *hopf* Elektronik GmbH with an exact description of the fault and the following information:

- If a WebGUI access is possible, download the according configuration files in the tab "DEVICE" and e-mail those to *hopf*
- If an access to the device is not possible please note the serial number of the system
- Occurrence of the error: During commissioning or operation
- Exact error description

Please write to the following E-mail address with the above information:

support@hopf.com

> ! Providing a detailed description of the error and the information listed above avoids the need for additional clarification and leads to faster processing by our Support team.

10 Maintenance

The Time Server 8030NTS/M is generally maintenance-free.

11   Technical Data

> ℹ The company **hopf** reserves the right to hardware and software altera-
> tions at any time.

General	
Operation	via WebGUI
Installation Position	any position
Protection Type of Module	IP00
Dimensions of Module	Multi-layer board 80mm x 60mm
Power Supply	5V DC ± 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. 6.250 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 compliant to EMC Directive 89/336/EC and Low Voltage Directive 73/23/EC	
Safety / Low Voltage Directive	DIN EN 60950-1:2001 + A11 + Corrigendum
EN 61000-6-4	
EMC (Electromagnetic Compatibility) / Interference Immunity	EN 610000-4-2 /-3/-4/-5/-6/-11
EN 61000-6-2	EN 61000-3-2 /-3
Radio Interference Voltage EN 55022	EN 55022 Klasse B
Radio Interference Emission EN 55022	EN 55022 Klasse B

GPS-System - Accuracy		
Lambda < 15ms	Stability < 0.2ppm	HIGH
Lambda < 15ms	Stability >= 0.2ppm and <= 2ppm, Offset < 1ms	HIGH
Lambda < 15ms	Stability > 2ppm or Offset >= 1ms	MEDIUM
DCF77-System - Accuracy		
Lambda < 15ms	Stability < 0.6ppm	HIGH
Lambda < 15ms	Stability >= 0.6ppm and <= 2ppm, Offset < 2ms	HIGH
Lambda < 15ms	Stability > 2ppm or Offset >= 2ms	MEDIUM

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
- PPS Time Source
- RFC-867 DAYTIME Server
- RFC-868 TIME Server
- SINEC H1 time datagram (Activation key required)

TCP/IP Network Protocols

- HTTP/ HTTPS
- DHCP
- Telnet
- SSH
- SNMP (Activation Key required)
- NTP (incl. SNTP)
- SINEC H1 time datagram (Activation key required)

Configuration Channels

- HTTP/HTTPS-WebGUI (Browser Based)
- Telnet
- SSH
- *hmc* Network Configuration Assistent

12 Factory Defaults of Time Server 8030NTS/M

This chapter lists the factory default values of the individual components integrated in the Time Server 8030NTS/M.

The default delivery status of the Time Server 8030NTS/M meets the factory default values when using GPS synchronization sources. In case of synchronization of the module by DCF77 based time information the function **"NTP / General / Sync Source"** is factrory-set to **"DCF77"** on delivery.

> **!** Using the board in DCF77 sytems (different product variant) the setting for **NTP / General / Sync Source"** needs to be re-configured to **"DCF77"** after a factory default.

NTP Server Configuration	Setting	WebGUI
Sync Source	DCF77	DCF77

12.1.1 Network

Host/Nameservice	Setting	WebGUI
Hostname	hopf8030nts-m	hopf8030nts-m
Use Manual DNS Entries	Enabled	Enabled
DNS Server 1 IPv4/IPv6 Address	Blank	---
DNS Server 2 IPv4/IPv6 Address	Blank	---
DNS Server 3 IPv4/IPv6 Address	Blank	---
Use Manual Gateway Entries	Enabled	Enabled
Default Gateway IPv4 Address	Blank	---
Default Gateway IPv6 Address	Blank	---
Network Interface ETH0	**Setting**	**WebGUI**
Use Custom Hardware Address (MAC)	Disabled	Disabled
Custom Hardware Address (MAC)	Blank	---
DHCP	Disabled	Disabled
IPv4	192.168.0.1	192.168.0.1
IPv4-Netmask	255.255.255.0	255.255.255.0
Operation mode	Auto negotiate	Auto negotiate
VLAN Interfaces	Disabled	Disabled
IPv6 Settings	Disabled	Disabled
Network Interface ETH1	**Setting**	**WebGUI**
Use Custom Hardware Address (MAC)	Disabled	Disabled
Custom Hardware Address (MAC)	Blank	---
DHCP	Enabled	Enabled
IPv4	Blank	---
IPv4-Netmask	Blank	---
Operation mode	Auto negotiate	Auto negotiate
VLAN Interfaces	Disabled	Disabled
IPv6 Settings	Disabled	Disabled
Bonding	**Setting**	**WebGUI**
Network Interface Bonding/Teaming	Disabled	Disabled

PRP	Setting	WebGUI
Network Interface PRP	Disabled	Disabled
Routing	**Setting**	**WebGUI**
Use Route File	Disabled	Disabled
User Defined Routes	Blank	---
Management	**Setting**	**WebGUI**
HTTP	Enabled	Enabled
HTTPS	Disabled	Disabled
SSH	Enabled	Enabled
TELNET	Disabled	Disabled
SNMP	Disabled	Disabled
HMC NCA	Enabled	Enabled
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	sekündlich	1 second
Timebase	UTC	UTC
Destination MAC Address	09:00:06:03:FF:EF	09:00:06:03:FF:EF
Minimum Accuracy	LOW	LOW
RADIUS	**Setting**	**WebGUI**
Enable	Disabled	Disabled
Server Address	Blank	---
Secret Key	Blank	---
Master User Secret	Blank	---
Device User Secret	Blank	---

12.1.2 NTP

NTP Server Configuration	Setting	WebGUI
Sync Source	GPS	GPS
NTP to Syslog	Disabled	Disabled
Switch to specific stratum	Disabled	Disabled
Stratum in crystal operation	Blank	---
Broadcast address	Blank	---
Authentication	Disabled	None
Key ID	Blank	---
Additional NTP Servers	Blank	---
NTP Extended Configuration	**Setting**	**WebGUI**
Limitation of Liability	Blank	---
Block Output when Stratum Unspecified	Disabled	Disabled
NTP Access Restrictions	**Setting**	**WebGUI**
Access Restrictions		Default nomodify
NTP Symmetric Keys	**Setting**	**WebGUI**
Request Key	Blank	---
Control Key	Blank	---
Symmetric Keys	Blank	---
NTP Autokey	**Setting**	**WebGUI**
Autokey	Disabled	Disabled
Password	Blank	---

12.1.3 PTP

PTP Configuration	Setting	WebGUI
PTP Enabled	disabled	disabled
PTP Interface	ETH0	ETH0
PTP Domain	0	0
PTP Priority 1	128	128
PTP Priority 2	128	128
PTP Profile	IEEE C37.238 Power Profile	IEEE C37.238 Power Profile
PTP IEEE C37.238 Power Profile Settings	**Setting**	**WebGUI**
PTP Grandmaster ID	3	3
Time Zone Name	UTC	UTC
PTP Advanced Settings	**Setting**	**WebGUI**
PTP Transport	Ethernet / P2P	Ethernet / P2P
PTP sync interval (2^x sec)	1 second	0
PTP pdelay request interval (2^x sec)	1 second	0
PTP announce interval (2^x sec)	1 second	0
PTP announce timeout (sec)	2 seconds	2

12.1.4 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

12.1.5 DEVICE

User Passwords	Settings	WebGUI
Master Password	master	---
Device Password	device	---
Diagnostic	**Settings**	**WebGUI**
Real Time Diagnostics	Disabled	Disabled
Product Activation	**Settings**	**WebGUI**
Activate Feature	No changes	No changes

12.1.6 Sync Source

All Sync Source settings shall not be affected by a factory- and custom-default.

13   Glossary and Abbreviations

13.1   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.

13.2   Tally Codes (NTP-specific)

space	**reject**	Rejected peer – either the peer is not reachable or its synchronization distance is too great.
x	**falsetick**	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).
-	**outlyer**	The peer was picked out by the NTP clustering algorithm as an outlyer.
+	**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.

13.2.1 Time-specific expressions

UTC	**UTC Time** (**U**niversal **T**ime **C**oordinated) 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)**.

13.3   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
PTP	Precision Time Protocol
PRP	Parallel Redundancy Protocol
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
VLAN	Virtual Local Area Network
WAN	Wide Area Network
msec	millisecond (10^{-3} seconds)
µsec	microsecond (10^{-6} seconds)
ppm	parts per million (10^{-6})

NTP Time Server Module with 2x 10/100/1000 MBit LAN Interfaces 8030NTS/M - V05.00

13.4   Definitions

An explanation of the terms used in this document.

13.4.1 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.

> **i**   See RFC 2131 Dynamic Host Configuration Protocol for further information.

13.4.2 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.

> **i**   See RFC 5905 for further information.

13.4.3 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.

13.4.4 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.

13.4.5 PTP (Precision Time Protocol)

The Precision Time Protocol (PTP) is a standard for synchronising clocks in computer networks. Unlike NTP it focuses on a higher accuracy and local networks.

In a network with several PTP-devices, every PTP-device executes the Best Master Clock-algorithm, to determine which PTP-device has the highest accuracy. That PTP-device serves as reference clock and is called Grandmaster Clock.

The Grandmaster Clock sends SYNC messages periodically to distribute the actual time to the slaves. The slaves periodically send Delay Request- or Path Delay Request-messages to the Grandmaster Clock. The Grandmaster Clock replies to those messages with a Delay Respond or Path Delay Respond message. The PTP-devices take sending and reception timestamps of those messages and attach those timestamps to the messages. These timestamps allow the slave to calculate the network delay and the exact actual time. For calculating the network delay the slave assumes, that the network delay in both directions is the same.

The PTP-devices use either Ethernet or UDP for their network communication. UDP uses the Ports 319 and 320.

13.5 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.

> ℹ 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.

14 List of RFCs

- NTPv4 - Protocol and Algorithms Specification (RFC 5905)
- NTPv4 - Autokey Specification (RFC 5906)
- PPS API (RFC 2783)
- DHCP (RFC 2131)
- Time Protocol (RFC 868)
- Daytime Protocol (RFC 867)
- HTTP (RFC 2616)
- HTTPS (RFC 2818)
- SSH-2 (RFC 4250-4256, 4335, 4344, 4345, 4419, 4432, 4716, 5656)
- TELNET (RFC 854-861)
- SNMPv2c (RFC 1213, RFC1901-1908)
- SNMPv3 (RFC 3410-3418)
- SYSLOG (RFC 5424)
- SMTP (RFC 5321)

15 List of Open Source Packages Used

Third Party Software

The *hopf* Time Server 8030NTS/M 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 availibility 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:

Package name	Version	Licence	Licence details	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	f0abaaacb 0a3f620f7 3dd6fd716 d7daa3c3 6a8e3	GPL	v2	no
cifs-utils	6.4	GPL	v3	no
dhcpcd	6.10.1	BSD		no
dhcpdump	1.8		Copyright 2001, 2002 by Edwin Groothuis, edwin@ma-vetju.org All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 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. 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.	no
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
freeradius-client	1.1.7	BSD		yes

freetype	2.6.2	GPL	v2	no
gd	2.1.1	BSD		no
genext2fs	**1.4.1**	**-**		**no**
gzip	1.6	GPL	v2	no
host-auto-conf	**2.69**	**GPL**	**v3**	**no**
host-automake	1.15	GPL	v2	no
host-bison	**3.0.4**	**GPL**	**v3**	**no**
host-dos2unix	7.3.1	BSD		no
host-e2fsprogs	1.42.13	GPL	v2	no
host-flex	2.5.37		Flex carries the copyright used for BSD software, slightly modified because it originated at the Lawrence Berkeley (not Livermore!) Laboratory, which operates under a contract with the Department of Energy: Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006, 2007 The Flex Project. Copyright (c) 1990, 1997 The Regents of the University of California. All rights reserved. This code is derived from software contributed to Berkeley by Vern Paxson. The United States Government has rights in this work pursuant to contract no. DE-AC03-76SF00098 between the United States Department of Energy and the University of California. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 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. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. This basically says "do whatever you please with this software except remove this notice or take advantage of the University's (or the flex authors') name". Note that the "flex.skl" scanner skeleton carries no copyright notice. You are free to do whatever you please with scanners generated using flex; for them, you are not even bound by the above copyright.	no
host-gen-ext2fs	1.4.1	GPL	v2	no
host-gettext	0.19.7	GPL	v3	no
host-kmod	22	LGPL	v2.1	no
host-libffi	3.2.1		libffi - Copyright (c) 1996-2014 Anthony Green, Red Hat, Inc and others. See source files for details. 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,	no

			copy, modify, merge, publish, distribute, 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: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. 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 AUTHORS OR 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.	
host-lib-glib2	2.46.2	LGPL	v2	no
host-libtool	2.46	GPL	v2	no
host-libxml2	2.9.3		Copyright (C) 1998-2012 Daniel Veillard All Rights Reserved. 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, 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: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. 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 AUTHORS OR 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.	no
host-lzo	2.09	GPL	v2	no
host-m4	1.4.17	GPL	v3	no
host-mtd	1.5.2	GPL	v2	no
host-ncurses	5.9		Copyright (c) 1998-2010,2011 Free Software Foundation, Inc. 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: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. 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,	no

			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. 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.	
host-omap-u-boot-utils	0.2.1	GPL	v2	no
host-pkgconf	0.9.12		Copyright (c) 2011, 2012, 2013, 2014, 2015 pkgconf authors (see AUTHORS). Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies. This software is provided 'as is' and without any warranty, express or implied. In no event shall the authors be liable for any damages arising from the use of this software.	no
host-uboot-tools	2016.01	GPL	v2+	no
host-zlib	1.2.8		Copyright (C) 1995-2017 Jean-loup Gailly and Mark Adler This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions: 1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required. 2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software. 3. This notice may not be removed or altered from any source distribution.	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
linuxptp	1.8	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
libselinux	2.1.13			
libsepol	2.1.9	LGPL	v2.1	
libserial	0.6.0rc2	GPL	v3	no
libserial-port	0.1.1	GPL	v3	no

libsock-etcan	0.0.10	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	1.4.39	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
mtd	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	Copyright (c) 1998-2004,2006 Free Software Foundation, Inc. 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: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. 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. 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.	no
netsnmp	5.7.3	BSD (mehrere)	http://net-snmp.sourceforge.net/about/license.html	no
netstat-nat	1.4.10	GPL		no
ntp	4.2.8p11	NTP	Copyright (c) University of Delaware 1992-2011 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.	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
pcre	8.38	BSD		no
popt	1.16	GNU Free Documentation License	V1.3	no
pps-tools	0deb9c7e 135e9380 a6d09e9d 2e938a14 6bb698c8	GPL	v2	no
prp	1.4	Permissive free software licence	Copyright (c) 2007, Institute of Embedded Systems at Zurich University of Applied Sciences (http://ines.zhaw.ch) Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: - Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. - 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. - Neither the name of the Zurich University of Applied Sciences nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.	yes
rsync	3.1.2	GPL		no
setools	3.3.8	GPLv2, LGPLv2.1		no
setserial	2.17	GPL		no
spidev_test	V3.0	GPL	v2	no
sqlite	3100200	Public domain		no
sshpass	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
ti-tools	06dbdb27 27354b5f3 ad7c7238 97f40051f ddee49		Copyright(c) 1998 - 2010 Texas Instruments. All rights reserved. All rights reserved. Base on code from Copyright (c) 2007, 2008, Johannes Berg johannes@sipsolutions.net Copyright (c) 2007, Andy Lutomirski Copyright (c) 2007, Mike Kershaw Copyright (c) 2008-2009, Luis R. Rodriguez mcgrof@gmail.com Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. * 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. * Neither the name Texas Instruments nor the names of its	no

NTP Time Server Module with 2x 10/100/1000 MBit LAN Interfaces 8030NTS/M - V05.00

			contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS 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 COPYRIGHT OWNER 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. | |
uboot	2010.06	GPL	v2	no
uboot-tools	2016.01	GPL	v2	no
usb_modeswitch	2.2.6	GPL	v2	no
usb_modeswitch_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