

Industriefunkuhren



Technical Manual

GPS - NTP Time Server with LAN Interface

Model 8029HEPTA-V2/GPS

ENGLISH

Version: 08.01 - 15.01.2019

	SET	IMAGE (8029)	FIRMWARE (8024)
Valid for	Version: 08.xx	Version: 08.xx	Version: 01.xx

Version number (Firmware / Manual)

THE FIRST TWO DIGITS OF THE VERSION NUMBER OF THE TECHNICAL MANUAL AND THE FIRST TWO DIGITS OF THE FIRMWARE VERSION MUST **COMPLY WITH EACH OTHER**. THEY INDICATE THE FUNCTIONAL CORRELATION BETWEEN DEVICE AND TECHNICAL MANUAL.

THE DIGITS AFTER THE POINT IN THE VERSION NUMBER INDICATE CORRECTIONS IN THE FIRMWARE / MANUAL THAT ARE OF NO SIGNIFICANCE FOR THE FUNCTION.

Downloading Technical Manuals

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

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

E-mail: info@hopf.com

Symbols and Characters



Operational Reliability

Disregard may cause damages to persons or material.



Functionality

Disregard may impact function of system/device.



Information

Notes and Information.



Safety regulations

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

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



Safety of the device

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

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

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

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

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

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

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

CE-Conformity



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

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

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

Contents	Page
1 GPS - NTP Time Server 8029HEPTA/GPS	9
2 System Structure	12
2.1 19 inch Rack 1U/84HP (Slim Line)	13
2.2 Functional Overview of the Front Panel Elements	13
2.2.1 LCD-Display with Pushbutton	13
2.2.2 Status-LEDs – System (& Extension)	14
2.2.3 Reset-(Default) Button	15
2.2.4 NTP Status LEDs (NTP/Stratum/Accuracy)	15
2.2.5 USB-Port (Host)	15
2.2.6 LAN Interface ETH0	16
2.2.6.1 MAC-Address for ETH0	16
2.2.7 Sync Status Optical Coupler	16
2.2.8 Sync Status LEDs	17
2.2.9 GPS Antenna Input	17
2.2.10 Extension Modules 1 – 6 (Option)	17
3 Function Principle	18
3.1 Block Diagram	18
3.2 Function 8029HEPTA (WebGUI: Device)	19
3.3 Function 8024GPS (WebGUI: Sync Source)	19
3.4 LCD-Display with Pushbutton	19
3.5 System EXTENSION 1 - 6 (Option)	20
4 System Behaviour	21
4.1 Boot Phase	21
4.2 NTP Adjustment Process (NTP/Stratum/Accuracy)	21
4.3 Reset-(Default) Button	21
4.4 Firmware Update	22
4.4.1 Firmware Update 8029HEPTA (WebGUI: Device)	22
4.4.2 Firmware Update 8024GPS (WebGUI: Sync Source)	23
4.5 Activation of Functions (Activation Key)	24
5 Installation	25
5.1 System 8029HEPTA/GPS in 1U Slim Line Housing	25
5.1.1 Installation of the 19 Inch Rack	25
5.1.2 Earthing	25
5.1.3 AC Power Supply	25
5.1.3.1 Safety and Warning Instructions	26
5.1.3.2 Power Supply Unit Specifications	26
5.1.3.3 Fusing	26
5.1.4 DC Power Supply (Option)	27
5.1.4.1 Power Supply Unit Specifications	27
5.1.4.2 Fusing	27
5.1.4.3 Reverse Voltage Protection	27
5.2 Connection GPS Antenna System	28

5.3	Connection LAN Interface ETH0.....	28
5.4	Connection Sync Status Optical Coupler	29
6	Commissioning.....	30
6.1	General Procedure	30
6.2	Switching the Operating Voltage on.....	31
6.3	LCD-Display after Switch On / Reset (Boot Phase)	31
6.4	Establish the Network Connection via Web Browser	32
6.5	Network Configuration for ETH0 via LAN through <i>hmc</i>	32
7	LCD-Display with Pushbutton – Function	36
7.1	Pushbutton Function (Light / Scroll).....	36
7.2	Standard Display Image	36
7.2.1	Standard Display Image without valid Time	36
7.2.2	Standard Display Image with valid Time.....	37
7.2.3	Standard Display with Additional Information	38
7.3	GENERAL ERROR	38
7.4	LAN Parameter.....	38
7.5	Local Time Parameter	39
7.6	GPS Satellite Display	40
7.7	Position	40
7.8	Receiver Status	40
7.9	Sync Source ERROR	41
7.10	Announcements (Summertime / Leap Second)	41
7.11	System-Info	42
8	HTTP/HTTPS WebGUI – Web Browser Configuration Interface.....	43
8.1	Quick Configuration	43
8.1.1	Requirements.....	43
8.1.2	Configuration Steps.....	43
8.2	General – Introduction	44
8.2.1	LOGIN and LOGOUT as User	45
8.2.2	Navigation via the Web Interface	46
8.2.3	Enter or Changing Data	47
8.2.3.1	Changing of Data in 8029HEPTA (WebGUI: Device)	47
8.2.3.2	Changing of Data in 8024GPS (WebGUI: GPS Sync Source).....	48
8.2.4	Plausibility Check during Input.....	49
8.3	Description of the Tabs.....	50
8.3.1	GENERAL Tab.....	50
8.3.2	NETWORK Tab.....	52
8.3.2.1	Host/Name Service.....	52
8.3.2.2	Network Interface ETH0.....	54
8.3.2.3	Routing (Activation Key necessary)	59
8.3.2.4	Routing File.....	60
8.3.2.5	Management (Management-Protocols – HTTP, SNMP, SNMP-Traps, etc.).....	61

8.3.2.6 Time (Time Protocols – NTP, DAYTIME etc.)	64
8.3.3 NTP Tab	66
8.3.3.1 System Info	66
8.3.3.2 Kernel Info	67
8.3.3.3 Peers	67
8.3.3.4 Server Configuration	68
8.3.3.5 Extended NTP Configuration	71
8.3.3.6 Restart NTP	73
8.3.3.7 Configuring the NTP Access Restrictions	74
8.3.3.8 Symmetric Key	78
8.3.3.9 Autokey	79
8.3.4 ALARM Tab (Activation Key necessary)	81
8.3.4.1 Syslog Configuration	81
8.3.4.2 E-mail Configuration	82
8.3.4.3 SNMP Configuration / TRAP Configuration	83
8.3.4.4 Alarm Messages	84
8.3.5 DEVICE Tab	85
8.3.5.1 Device Information	85
8.3.5.2 Hardware Information	85
8.3.5.3 Restoring the Factory Defaults Settings	86
8.3.5.4 Restarting the Module (Reboot Device)	87
8.3.5.5 Image Update for Module 8029HEPTA (WebGUI: Device)	88
8.3.5.6 Upload von Anwender SSL-Server-Zertifikat (Upload Certificate)	90
8.3.5.7 Customized Security Banner	91
8.3.5.8 Product Activation	92
8.3.5.9 Diagnostics Function	93
8.3.5.10 Passwords (Master/Device)	93
8.3.5.11 Downloading Configuration Files / SNMP MIB	94
8.3.6 GPS SYNC SOURCE Tab	95
8.3.6.1 Time and Status	95
8.3.6.2 Set Sync Source Time	96
8.3.6.3 Time Zone Offset	97
8.3.6.4 Daylight Saving Time (DST)	98
8.3.6.5 Reception Quality	99
8.3.6.6 Reception Mode	100
8.3.6.7 Receiver Position	100
8.3.6.8 SyncON / SyncOFF	101
8.3.6.9 Module Info	102
8.3.6.10 Module Reset	103
8.3.6.11 Factory Default	103
8.3.6.12 H8 Firmware Update (Sync Source)	104
8.3.6.13 Module Errors	105
8.3.6.14 Sync Status OC	107
9 SSH and Telnet Basic Configuration	108
10 Fault Analysis / Troubleshooting	109
10.1 Error Patterns	109
10.1.1 Complete Failure	109
10.1.2 No GPS Reception / No Synchronization	109
10.1.3 No Daylight Saving Time / Summer Time Switchover	111
10.2 Support by Company hopf	111
11 Maintenance	112
11.1 General Guidelines for Cleaning	112
11.2 Cleaning the Housing	112

11.3 Cleaning the Display and Front Panel.....	112
12 Technical Data	113
12.1 General – 8029HEPTA/GPS	113
12.2 Module 8029HEPTA.....	115
12.3 Module 8024GPS	116
13 Factory Defaults of Time Server 8029HEPTA/GPS	117
13.1 Factory Default Values of Module 8029HEPTA (Device)	117
13.1.1 Network	117
13.1.2 NTP	118
13.1.3 ALARM	119
13.1.4 DEVICE	119
13.2 Factory Default Values of Module 8024GPS (Sync Source)	120
14 Glossary and Abbreviations	121
14.1 NTP-specific Terminology.....	121
14.2 Tally Codes (NTP-specific)	121
14.2.1 Time-Specific Expressions.....	122
14.3 Abbreviations.....	123
14.4 Definitions	124
14.4.1 DHCP (Dynamic Host Configuration Protocol)	124
14.4.2 NTP (Network Time Protocol)	124
14.4.3 SNMP (Simple Network Management Protocol).....	125
14.4.4 TCP/IP (Transmission Control Protocol / Internet Protocol)	125
14.5 Accuracy & NTP Basic Principles	125
15 List of RFCs.....	127
16 List of Open Source Packages Used.....	128

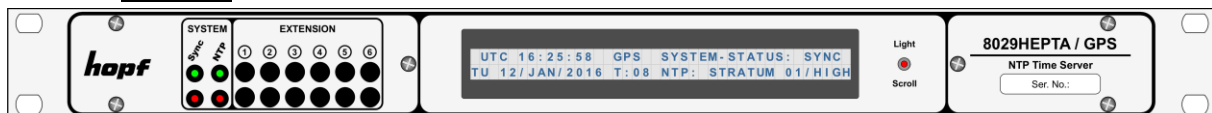
1 GPS - NTP Time Server 8029HEPTA/GPS

By GPS time synchronization and the worldwide used time protocol **NTP (Network Time Protocol)** the Time Server 8029HEPTA/GPS turns into a highly accurate **NTP Stratum 1** Time Server. It is used for the synchronization of computers and industrial networks.

The Time Server supports the following synchronization protocols:

- NTP (incl. SNTP)
- Daytime
- Time
- SINEC H1 time datagram (**Activation Key necessary**)

Front Side



Rear Side



The Time Server 8029HEPTA/GPS is integrated into a 1U/84HP 19" rack and characterized by its easy and simple operation. Some of these practice-oriented functionalities are e.g.:

- **Complete parameterisation via protected WebGUI access**
All required settings for operation can be executed via a password protected WebGUI also giving an overview of the status of the Time Server 8029HEPTA/GPS.
- **LCD-Display and Status-LEDs in the front panel**
The LCD-Display and the Status-LEDs make rapidly and easily substantial information for commissioning, on the operating status and for support matters available if a problem occurs, even without WebGUI access.
- **Monitoring of GPS antenna circuit**
An error message is generated when there is a short circuit in the GPS antenna circuit or an open antenna input.
- **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**
Should a leap second be inserted in the UTC time, it is recognized by the Time Server 8029HEPTA/GPS via the GPS signal and the leap second is automatically inserted in the time information.
- **Customized extensions possible**
The new designed housing concept allows customized system extensions for additional signal outputs (processed ex-works) easily and fast.

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

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

Currently the Time Server 8029HEPTA/GPS offers following unlockable functions:

- SINEC H1 time datagram
- Static Routing Table
- Alarming and management features
- IEEE 802.1Q Tagged VLAN

A few other basic functions of the Time Server 8029HEPTA/GPS:

- The Time Server 8029HEPTA/GPS operates as **NTP Server with Stratum 1**
- Easy operation via **WebGUI**
- **LCD-Display (2x40) and Status LEDs on the front panel**
- **Sync status output** via optical coupler
- **High freewheel accuracy** provided by GPS-supported regulation of the internal quartz basis
- Completely **maintenance-free** system
- **SyncOFF Timer** (reception failure bypassing) for operation free of fault messages even based on difficult reception conditions
- Redundant **multiple validation** of the synchronization signal for an error-free and leap free signal evaluation
- Maintenance-free, buffered **backup clock** for at least three days

Software supplied:

- **hmc** Remote Software for the operating systems:
 - Microsoft® Windows® NT/2000/XP/VISTA/7 (32/64 Bit)
 - Microsoft® Windows® Server 2003/2008 (32/64 Bit)
 - Linux® (32/64 Bit)
 - Oracle® Solaris SPARC/x86
 - IBM AIX® (from Version 5.2)
 - HP-UX 11i (RS232 support only for PA-RISC architecture)

Overview of the functions of the network Time Server 8029HEPTA/GPS:**Ethernet Interface**

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

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
- SINEC H1 time datagram (**Activation Key necessary**)
- RFC-867 DAYTIME Server
- RFC-868 TIME Server

Network Protocols

- HTTP/ HTTPS
- DHCP
- Telnet
- SSH
- SNMPv3, SNMP Traps (MIB II, Private Enterprise MIB) (**Activation Key necessary**)
- NTP (including SNTP)
- SINEC H1 time datagram (**Activation Key necessary**)

Configuration Channel

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

Additional Features

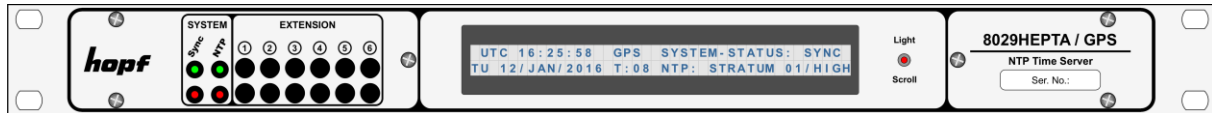
- E-mail notification (**Activation Key necessary**)
- Syslog messages to external syslog server (**Activation Key necessary**)
- Routing (**Activation Key necessary**)
- Update via TCP/IP
- Fail-safe
- Watchdog circuit
- System management
- Customized security banner

2 System Structure

The system 8029HEPTA/GPS consists of the following:

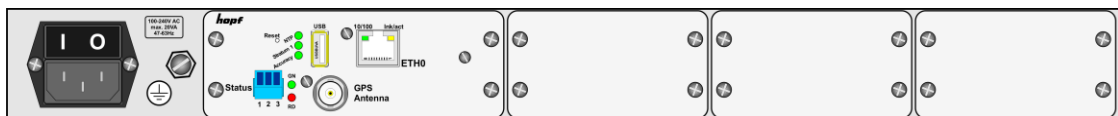
- 1/1 19" module rack 1U/84HP (Slim Line)
- System front panel with LCD-Display (2x40), pushbutton and status LEDs

System front view:



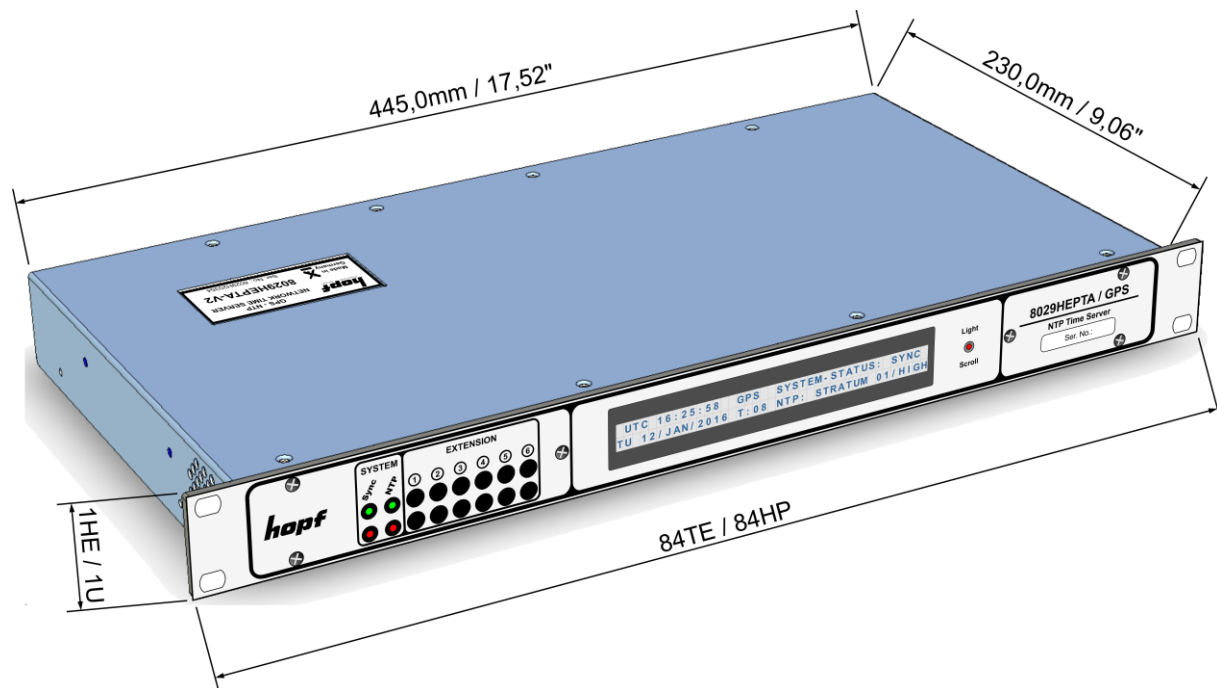
- Wide-ranging power supply unit from 100-240V AC / 20VA (47-63Hz)
Other input voltages available
- Voltage feed with power switch with connections in accordance with IEC/EN60320/C14 including EMI line filter
- Connection for protection earth (PE) cables up to 16mm²
- Module 8029HEPTA
- Module 8024GPS
- Space for up to 6 additional output modules

System rear side:



The new designed housing concept allows customized system extensions for additional signal outputs (processed ex-works) easily and fast.

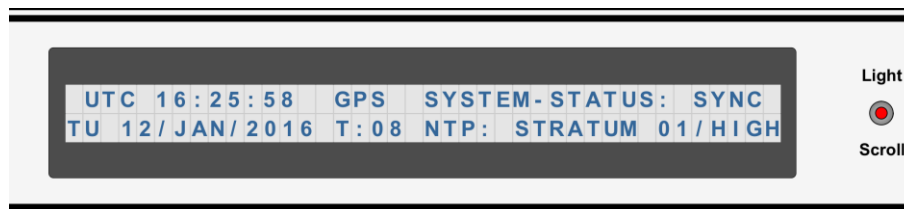
2.1 19 inch Rack 1U/84HP (Slim Line)



2.2 Functional Overview of the Front Panel Elements

This chapter describes the individual function elements of the front and rear panel.

2.2.1 LCD-Display with Pushbutton



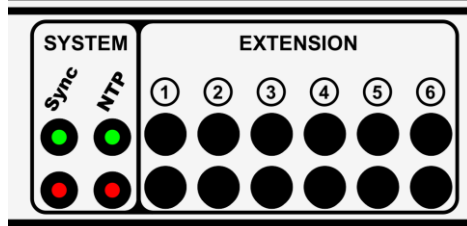
The background illumination of the LCD-Display is activated or rather controlled by the pushbutton Light/Scroll.

The 2x40 LCD-Display enables reading out the time and further essential information for the commissioning, the operation status, and for support even without WebGUI access.

The operation and function of the pushbutton and the display are described in **Chapter 7 LCD-Display with Pushbutton – Function**.

2.2.2 Status-LEDs – System (& Extension)

The Status LEDs on the front panel indicate the current synchronization and operation status of the System 8029HEPTA/GPS. Meanings of the LEDs are the following:



During the boot process, all LEDs are flashing in a test sequence. The boot process lasts approx. 30 seconds.

System - Sync			
Status LEDs		Sync-Status	Status Code
Green	Red		
ON	Off	Sync (radio-synchronous) with quartz regulation	SYNC
Flashes	Off	Sync (radio-synchronous) - SyncOFF timer running	SYOF
ON	Flashes	Sync (radio-synchronous) - simulation mode	SYSI
Flashes	Flashes	Quarz - SyncON timer running	QUON
ON	ON	Quarz - time was set via synchronization source	QUEX
Flashes	ON	Quarz - time set manually or after reset	QUSE
Off	ON	No valid time	INVA
Off	Off	No operating voltage / faulty	---

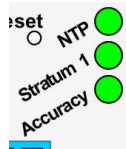
System - NTP				
Status LEDs		NTP Service	NTP-Status	
Green	Red		STRATUM	ACCURACY
Off	On	Not Active	---	Low
Flashes 1Hz 50%	On	Active	16	Low
Flashes 1Hz 10%	Flashes 1Hz 50%	Active	2-15	Low
Flashes 1Hz 50%	Flashes 1Hz 50%	Active	2-15	Medium
On	Flashes 1Hz 50%	Active	2-15	High
Flashes 1Hz 10%	Off	Active	1	Low
Flashes 1Hz 50%	Off	Active	1	Medium
On	Off	Active	1	High
Flashes 2Hz 50%	Off	Module loading Operating System		
Off	Flashes 4Hz 50%	Module CPU not ready for operation (ERROR)		

2.2.3 Reset-(Default) Button



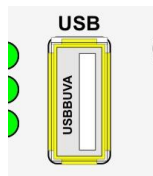
The Reset-(Default) Button is accessible with a thin object through the small drilling in the front panel next to the "Reset" inscription" (see **Chapter 4.3 Reset-(Default) Button**).

2.2.4 NTP Status LEDs (NTP/Stratum/Accuracy)



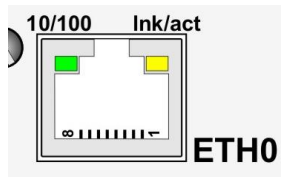
NTP-LED (Green)	NTP service of the Time Server 8029HEPTA/GPS
On	Standard, running
Off	Not running
Stratum1-LED (Green)	The NTP service of the Time Server 8029HEPTA/GPS works with:
On	Stratum 1
Flashes	Stratum 2-15
Off	Stratum 16 (no synchronization of NTP Clients)
Accuracy-LED (Green)	The NTP service of the Time Server 8029HEPTA/GPS works with accuracy of:
On	high
Flashes	medium
Off	low

2.2.5 USB-Port (Host)



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

2.2.6 LAN Interface ETH0



10/100-LED (Green)	Description
Off	10 MBit Ethernet detected
On	100 MBit Ethernet detected

Ink/act-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+
2	Tx–
3	Rx+
4	Not in use
5	Not in use
6	Rx–
7	Not in use
8	Not in use

2.2.6.1 MAC-Address for ETH0

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

The MAC address given for the LAN interface ETH0 can be read in WebGUI of the appropriate board or be evaluated via the **hmc Network Configuration Assistant**. The MAC address is uniquely assigned for each LAN interface by the company **hopf** Elektronik GmbH.

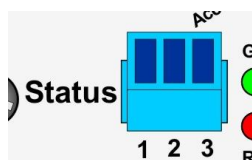


The factory set MAC address for the Time Server 8029HEPTA/GPS can also be read out via the LCD-Display.



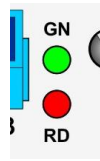
hopf Elektronik GmbH MAC addresses begin with **00:03:C7:xx:xx:xx**.

2.2.7 Sync Status Optical Coupler



Sync Status Optical Coupler	
3-pole pluggable Connector	
Pin	Signal
1	Collector
2	n.c.
3	Emitter

2.2.8 Sync Status LEDs



Sync Status LEDs	
LED	Meaning
RD	Status LED red
GN	Status LED green

The Status LEDs on the front panel signal the current (synchronization) status of the Sync Source (here Module 8024GPS). The meanings of the LEDs are as follows:

LED RD - Red	LED GN - Green	Status	STATUS Code
Off	ON	Sync (radio-synchronous) with quartz regulation	SYNC
Off	Flashes	Sync (radio-synchronous) - SyncOFF timer running	SYOF
Flashes	ON	Sync (radio-synchronous) - simulation mode	SYSI
Flashes	Flashes	Quarz - SyncON timer running	QUON
ON	ON	Quarz - time was set via synchronization source	QUEX
ON	Flashes	Quarz - time set manually or after reset	QUSE
ON	Off	No valid time	INVA
Off	Off	No operating voltage / faulty	---
3Hz	Off	General Module Error (PCID)	INVA
3Hz	Invert 3Hz	User settings missing (Difference time / ST-WT Changeover)	INVA

2.2.9 GPS Antenna Input



GPS Antenna	
BNC connector	
GPS	Antenna input



The antenna input provides an internal monitoring for "short-circuit" and "open input".

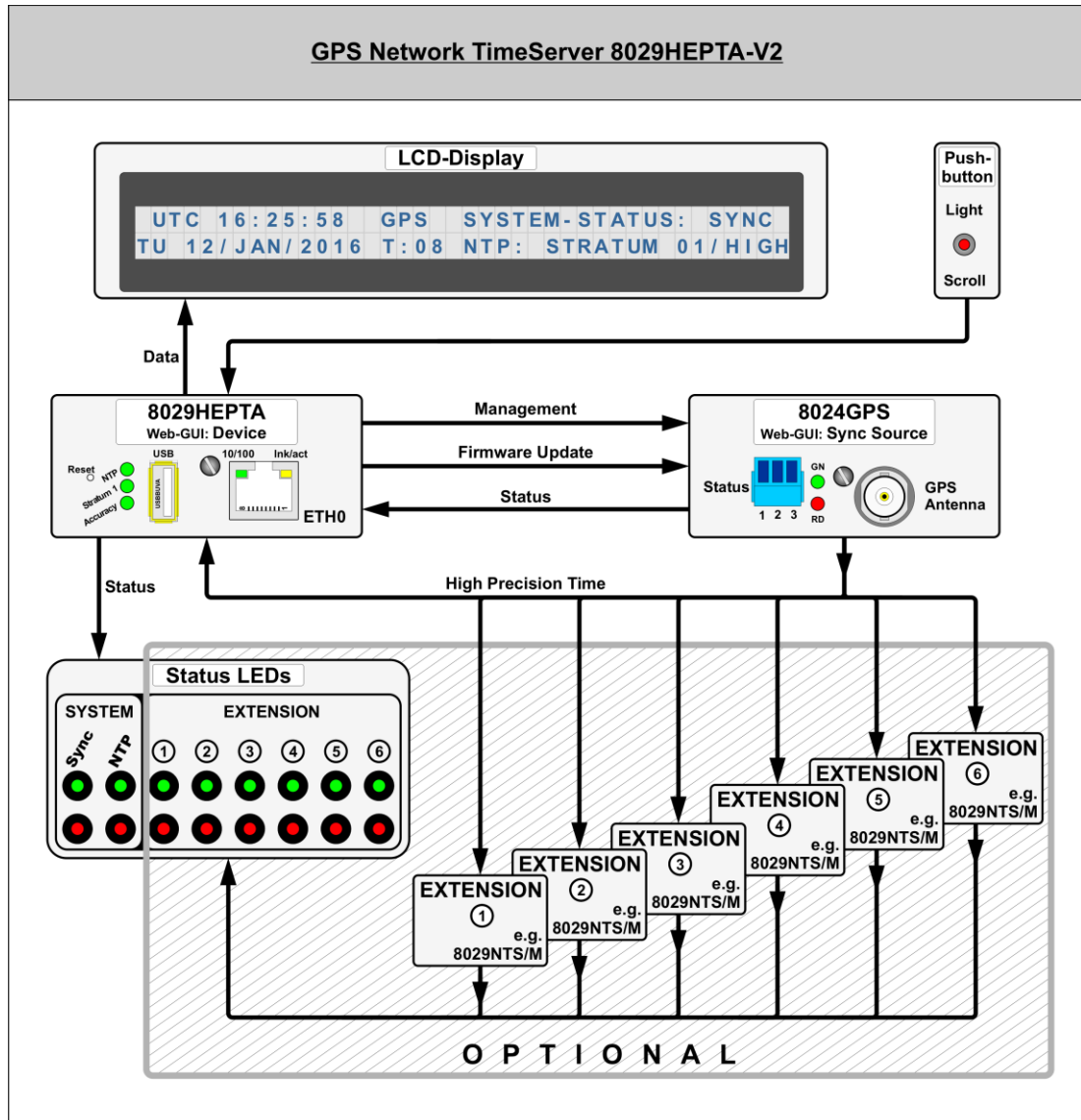
2.2.10 Extension Modules 1 – 6 (Option)

All installed system extensions deviating from the standard system 8029HEPTA/GPS including the pertinent Status LEDs are documented and described in a device-specific supplementary instruction.

3 Function Principle

This chapter describes the function principle of the Time Server 8029HEPTA/GPS and the internal relations between the different functional groups.

3.1 Block Diagram



- **Firmware Update**

A H8 firmware update of the Sync Source (here Module 8024GPS) is completely controlled by Module 8029HEPTA.

The update file for Module 8024GPS is loaded into Module 8029HEPTA via LAN through the WebGUI. Then Module 8029HEPTA performs the update of the Sync Source (here Module 8024GPS) independently.

- **Management**

The entire control of the Sync Source (here Module 8024GPS) is done by Module 8029HEPTA. All data of the Sync Source, indicated via WebGUI, are demanded cyclically by Module 8029HEPTA from the Sync Source (here Module 8024GPS) or if necessary. These data are then prepared for the display in WebGUI. After activation settings for the Sync Source are transferred to the Sync Source immediately.

- **High Precision Time**

The Sync Source provides a high-precision time information and the according synchronization status to Module 8029HEPTA. This time and status information is used for synchronization of the NTP service and if applicable other signal generations running on 8029HEPTA.

3.2 Function 8029HEPTA (WebGUI: Device)

The Module 8029HEPTA is the "heart" of the Time Server 8029HEPTA/GPS. A complete LINUX operating system is running on this Module providing all functions such as NTP, WebGUI etc. The Module also controls the connected Sync Source (here Module 8024GPS). Using the high-precise time information of Module 8024GPS the NTP service running on Module 8029HEPTA is also adjusted with high-precision. Thus the Module 8029HEPTA is a very precise **NTP STRATUM 1 - Time Server**.

3.3 Function 8024GPS (WebGUI: Sync Source)

The Module 8024GPS is in principle an independent Module with GPS receiver and its own μ Processor. In synchronous status it provides a high-precise time information to the Module 8029HEPTA. The control of Module 8024GPS in this system is completely done via Module 8029HEPTA. Parameters required by Module 8024GPS or provided are entered into WebGUI of Module 8029HEPTA or rather be output.

The Module 8024GPS has an own failsafe memory in which all required data for operation after generation via WebGUI are stored.

As the data of the Sync Source for the WebGUI indication need to be received by the Module 8029HEPTA at first, it is **no real-time indication** in **WebGUI**.

3.4 LCD-Display with Pushbutton

System settings cannot be changed via the pushbutton nor the display. The display allows the readout of important system and operation parameters directly at the device, even without WebGUI access.

The data indicated in the display are applicable to updating-cycles such as the WebGUI. An on-going process is indicated via the display.

3.5 System EXTENSION 1 - 6 (Option)

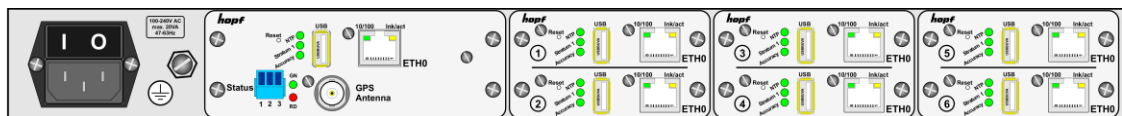
The system 8029HEPTA/GPS can be equipped with autonomous extension modules for complex functions (e.g. NTP Time Server Module 8029NTS/M) but also with additional output hardware for signals generated by the system 8029HEPTA/GPS itself and parameterized by its WebGUI.

Autonomous extension modules that are only provided with the high-precise time information for its own function/signal generation by the system have two Status LEDs in the front panel. Those are assigned via the EXTENSION numbers. These LEDs indicate the according operation status of the extension module.

System front view:



System rear side / plug-in side:



All installed system extensions deviating from the standard system 8029HEPTA/GPS including the pertinent Status LEDs are documented and described in a device-specific supplementary instruction.

4 System Behaviour

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

4.1 Boot Phase

The boot process of the Time Server 8029HEPTA/GPS starts after turning on the system or a reset.

This phase can be recognized by the LCD-Display and activated LED test of the Status LEDs in the front panel.

During the boot process the Module 8029HEPTA boots its LINUX operation system and is therefore not available via LAN.

The end of the boot process is reached when the LCD-Display changes to the standard picture and the LED test of the Status-LEDs in the front panel has been finished.



The boot process lasts approx. 30 seconds.

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 8029HEPTA/GPS requires approximately 5-10 minutes after synchronization of the Sync Source (Status "SYNC") until NTP is set to the high accuracy of the Sync Source (here Module 8024GPS) and reaches the optimized operation condition of **STRATUM = 1** and **ACCURACY = High**.

The decisive factors here are accuracy of the synchronization source and the appropriate synchronization condition of the Sync Source.

4.3 Reset-(Default) Button

The Time Server 8029HEPTA/GPS can be reset by the Reset-(Default) Button behind the front panel of the board. The Reset-(Default) Button is accessible with a thin object 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 system wide hardware reset is triggered
>= 10 sec.	After releasing a FACTORY DEFAULT followed by a REBOOT is triggered after approx. 10 seconds

4.4 Firmware Update

The Time Server 8029HEPTA/GPS is a multi-processor system. For this reason a firmware update always consists of a so called Software SET including three (3) program releases defined by the SET version needed to be loaded into the board.



ATTENTION

In order to select the correct image update, *Chapter 8.3.5.5.1 Select Image Update* must be checked!



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 program releases assigned to a SET version may be taken from the release notes of the software SETs of the Time Sever 8029HEPTA/GPS.

4.4.1 Firmware Update 8029HEPTA (WebGUI: Device)

The general process of a software update of Module 8029HEPTA is described below:



For selection of the correct update set the identifier **8029HEPTA-V2** has to be observed obligatory. The extension V2 describes a hardware version of 8029HEPTA.

8029HEPTA-V2 can be recognized:

- By the serial number stated on the front panel "**8029H2xxxx V2**"
- By the label on the housing cover "**8029HEPTA-V2**"
- In WebGUI at the Web-banner "**8029HEPTA-V2**"

The firmware update 8029HEPTA-V2 has to be performed as a SET.

The software package contained in the ZIP archive has to be unpacked. The following steps have to be executed in the following sequence:

1. **Image Update 8029HEPTA-V2**
2. **H8 Firmware Update 8029HEPTA-V2**
3. **H8 Firmware Update 8024GPS**

Image Update 8029HEPTA-V2

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 Firmware Update 8029HEPTA-V2

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 8029** 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.

4.4.2 Firmware Update 8024GPS (WebGUI: Sync Source)

H8 Firmware Update 8024GPS

1. Log in as Master in WebGUI of the board.
2. Select in the **GPS SYNC SOURCE** tab the menu item **H8 Firmware Update**.
3. Select the file with the file extension **.mot for Module 8024** 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.

4.5 Activation of Functions (Activation Key)

The Time Server 8029HEPTA/GPS offers several 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 8029HEPTA (not the serial number of the overall system).

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

These functions are:

- **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.
- **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 function FACTORY DEFAULTS.

5 Installation

The installation of the Time Server 8029HEPTA/GPS is described below.

5.1 System 8029HEPTA/GPS in 1U Slim Line Housing

5.1.1 Installation of the 19 Inch Rack

The System is assembled in a 1U/84HP 19" housing for control cabinet installation (measurement see **Chapter 2.1 19 inch Rack 1U/84HP (Slim Line)**).

The following steps are to be carried out:

- Place the rack in the control panel and fix to the mounting brackets on the front side of the rack using 4 screws.



The side ventilation apertures on the right and left hand sides must not be covered. Otherwise ventilation will not be effective and lack of convection and / or thermal coupling with surrounding equipment may give rise to an excessive equipment operating temperature.

- Ensure that there is sufficient space between the back of the rack and the control panel to allow connection and data lines with the system

5.1.2 Earthing

The Time Server 8029HEPTA/GPS is usually earthed via the PE cable of the power supply.

An additional earth cable for surge protection purposes can be connected by means of the earth screw located on the rear side of the System housing.

5.1.3 AC Power Supply

The Systems' standard AC power supply unit is described here. However, the connection data on the nameplate of the respective unit is always applicable.

Attention should be paid to the following when connecting the power supply:

- Correct voltage type (AC or DC)
- Voltage level

The power feed is via an input connector with EMI filter compliant with IEC/EN 60320-1/C14



- Check that the mains power switch is in position "0" (= off).
- Plug the input connector into the System's mains power inlet.
- Connect the input connector to the mains power supply and switch the line circuit breaker on.



The Time Server 8029HEPTA/GPS can be damaged if incorrect voltage is connected.

5.1.3.1 Safety and Warning Instructions

Please read these instructions fully in order to guarantee safe operation of the equipment and to be able to use all the functions.



Caution: Never work on an open unit when voltage is applied!
Danger to life!

The Time Server 8029HEPTA/GPS is an installation device. Installation and commissioning may only be carried out by suitably qualified specialist personnel. In doing so the respective country-specific specifications must be observed (e.g. VDE, DIN).

Before commissioning ensure that:

- The power supply has been connected correctly and electrical shock protection is in place
- The earth wire is connected
- All supply cables are correctly sized and fused
- All output cables are suitably sized or specially fused for the max. output current of the equipment
- Sufficient convection is guaranteed

The equipment contains life-threatening components and a high level of stored energy.

5.1.3.2 Power Supply Unit Specifications

All AC power supply specifications are described in **Chapter 12 Technical Data**.

5.1.3.3 Fusing

Pay attention to the correct fusing of the power supply when connecting the Time Server 8029HEPTA/GPS.

The corresponding performance data can be taken from the equipment nameplate. The Time Server 8029HEPTA/GPS is currently fitted with a power supply unit with a power consumption of max. 20VA.

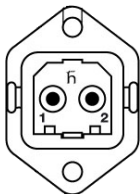


If the internal fuse (device protection) trips it is highly probable that the equipment is faulty. In this case the device should be checked in the factory.

5.1.4 DC Power Supply (Option)



Ensure that the external power supply is switched off. When connecting the supply cable make sure that the polarity is correct and the equipment is earthed.



- The cable of the power supply is connected using a 2-pole plug connector with additional earth connection and interlocked with the Time Server 8029HEPTA/GPS:

+V_{in}: Positive pole (contact 1)
-V_{in}: Negative pole (contact 2)
PE: Earth



The Time Server 8029HEPTA/GPS can be damaged if incorrect voltage is connected.



Earthing:

By default the minus pole (-V_{in}) and earthing (PE) are connected system-sided.

5.1.4.1 Power Supply Unit Specifications

All DC power supply specifications are described in **Chapter 12 Technical Data**.

5.1.4.2 Fusing

Pay attention to the correct fusing of the power supply when connecting the Time Server 8029HEPTA/GPS.

The corresponding performance data can be taken from the equipment nameplate. The Time Server 8029HEPTA/GPS is currently fitted with a power supply unit with a power consumption of max. 20VA.



If the internal fuse (device protection) trips it is highly probable that the equipment is faulty. In this case the device should be checked in the factory.

5.1.4.3 Reverse Voltage Protection

The version of Time Server 8029HEPTA/GPS with DC supply has reverse voltage protection. This protection prevents damage to the equipment due to an incorrectly connected DC power supply.

Protection is effected by means of a self-resetting fuse. In the case of reverse polarity, it is necessary to switch the equipment off for approx. 20 seconds after this fuse has tripped. The power supply can then be connected with the correct polarity.

5.2 Connection GPS Antenna System

The coaxial line of the GPS antenna system is placed on the BNC female connector with the "GPS Antenna" inscription on the rear side of the Time Server 8029HEPTA/GPS. More detailed descriptions referring to the installation of the antenna system, for example, cable lengths and cable types, are described in the document "Antenna System GPS".

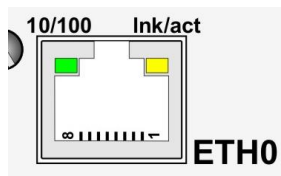


GPS Antenna	
BNC connector	
GPS	Antenna input



There is an antenna input monitoring for "open" and "short-circuit" on the system side.

5.3 Connection LAN Interface ETH0



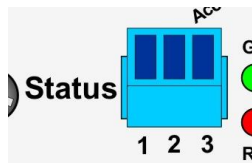
10/100-LED (Green)	Description
Off	10 MBit Ethernet detected
On	100 MBit Ethernet detected

Ink/act-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+
2	Tx-
3	Rx+
4	Not in use
5	Not in use
6	Rx-
7	Not in use
8	Not in use

5.4 Connection Sync Status Optical Coupler

The Sync Status Optical Coupler connection is a 3-pole pluggable screw terminal.



Sync Status Optical Coupler	
3-pole pluggable Connector	
Pin	Signal
1	Collector
2	n.c.
3	Emitter

6 Commissioning

This chapter describes commissioning of the Time Server 8029HEPTA/GPS.

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 finished (Duration approx. 30 seconds – see **Chapter 4.1 Boot Phase**)
- Using the SEARCH Function of the **hmc - Network Configuration Assistant** in order to access the Time Server 8029HEPTA/GPS and set the basis LAN parameters (e.g. DHCP). Afterwards connect to the WebGUI of the Time Server 8029HEPTA/GPS via Web browser

OR

Connect directly with the factory default IP-address (192.168.0.1) to the WebGUI of the Time Server 8029HEPTA/GPS 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
- Parameterize following values of the Sync Source (here Module 8024GPS) in **GPS SYNC SOURCE tab**:
 - Set current UTC time
 - Set the local difference time to UTC
 - Set or deactivate the changeover times for summer/winter time
 - Set local position (if not known as 0)
 - Check values for reception mode, SyncON/SyncOFF Timer and status OC

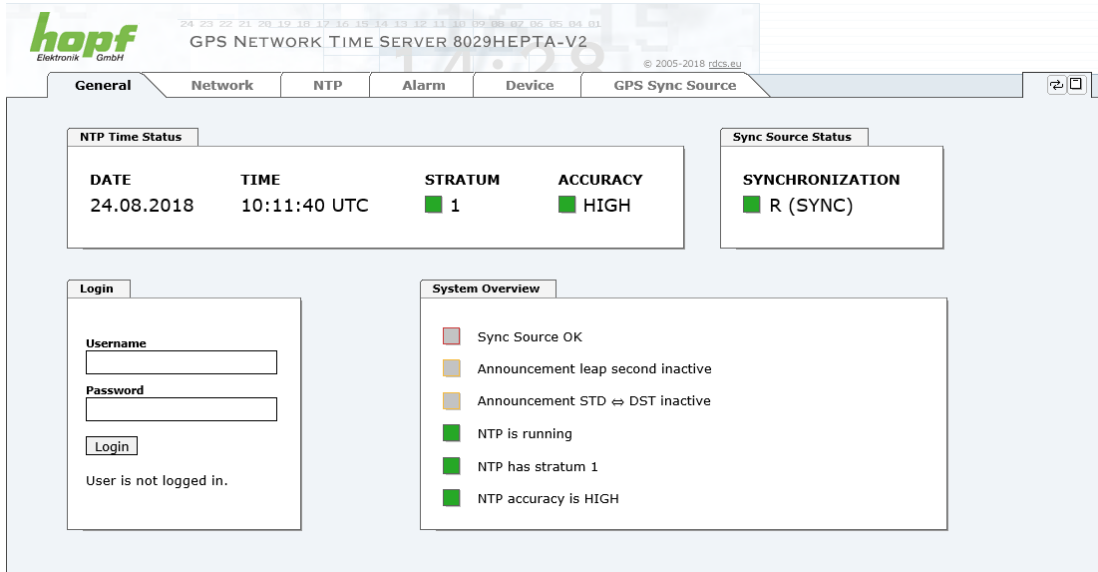
Trigger a **Module Reset** after the above mentioned entries



During first commissioning it is mandatory required to configure the difference time to UTC and the changeover times for summer/winter time respectively to deactivate them one time. Otherwise synchronization via GPS will not be possible and a "Sync Source Error" is indicated.

- Check for **Module Error** in register **GPS SYNC SOURCE**
- Parameterize optional functions e.g. SNMP or SINEC H1 time datagram

- If all base settings are carried out correctly and there is GPS reception, the **GENERAL** tab should look like this after approx. 30 min.:



The screenshot shows the web interface of the hopf GPS NETWORK TIME SERVER 8029HEPTA-V2. The 'General' tab is selected. The interface includes a navigation bar with tabs: General, Network, NTP, Alarm, Device, and GPS Sync Source. The main content area is divided into several sections:

- NTP Time Status:**

DATE	TIME	STRATUM	ACCURACY
24.08.2018	10:11:40 UTC	1	HIGH
- Sync Source Status:**

SYNCHRONIZATION
R (SYNC)
- Login:**

Username:

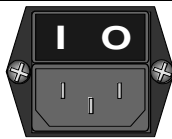
Password:

Login

User is not logged in.
- System Overview:**
 - Sync Source OK
 - Announcement leap second inactive
 - Announcement STD \leftrightarrow DST inactive
 - NTP is running
 - NTP has stratum 1
 - NTP accuracy is HIGH

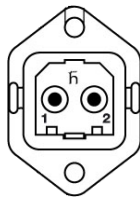
6.2 Switching the Operating Voltage on

AC power supply:



Put the mains power switch into position "I" (on).
The Time Server 8029HEPTA/GPS starts running with the boot process indicated in the display (see **Chapter 6.3 LCD-Display after Switch On / Reset (Boot Phase)**).

DC power supply:



Switch on external power supply source.
The Time Server 8029HEPTA/GPS starts running with the boot process indicated in the display (see **Chapter 6.3 LCD-Display after Switch On / Reset (Boot Phase)**).

The green Power LED resp. the power supply LED light up for both power supplies.

6.3 LCD-Display after Switch On / Reset (Boot Phase)

In the 2x40digit LCD-Display the following start-up picture appears for approx. 30 seconds after switching on or a reset:

```

hopf 8029HEPTA_V2/GPS : Booting...
Status-LEDs (Front): LED-Test active
  
```

6.4 Establish the Network Connection via Web Browser



Ensure that the network parameters of the Time Server 8029HEPTA/GPS are configured in accordance with the local network before connecting the device to the network.



Connecting a network to an incorrectly configured Time Server 8029HEPTA/GPS (e.g. duplicate IP address) may cause interference on the network.



The Time Server 8029HEPTA/GPS is supplied with a static IP-address (equivalent to the factory default setting).

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



In case it is not known whether the Time Server 8029HEPTA/GPS 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).

6.5 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 8029HEPTA/GPS, 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 8029HEPTA/GPS for other systems on the network.



The SEARCH Function of the ***hmc*** - Network Configuration Assistant requires for location and recognition of the wished Time Server 8029HEPTA/GPS that the ***hmc***-computer and the Time Server 8029HEPTA/GPS are in the same SUB Net.

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



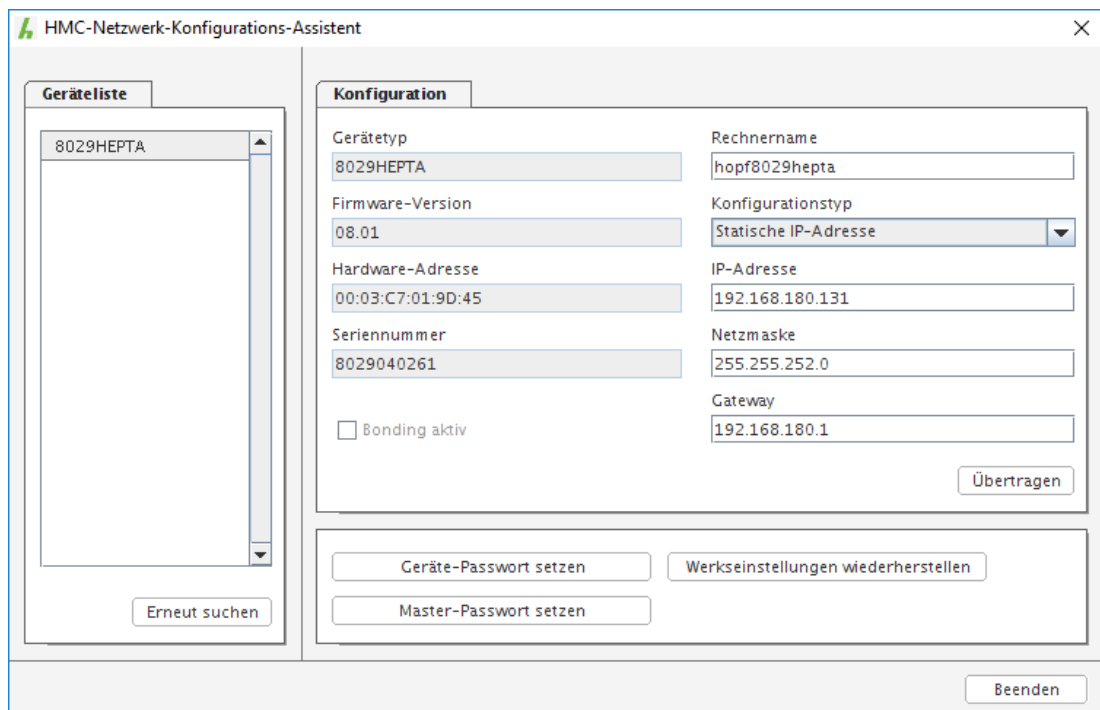
After a successful start of the **hmc Network Configuration Assistant** and completed search of the **hopf** LAN devices, the configuration of the base LAN parameters can be done.

The Time Server 8029HEPTA/GPS is stated as **8029HEPTA** in the **Device List**.

The determination of different Time Server 8029HEPTA/GPS (or other products variants) is made via **Hardware Address** (MAC Address).



The factory set MAC address for the Time Server 8029HEPTA/GPS can also be read out via the LCD-Display.



For an extended configuration of the Time Server 8029HEPTA/GPS through a browser via WebGUI the following base parameters are required:

- **Host Name** ⇒ e.g. hopf8029HEPTA
- **Network Configuration Type** ⇒ e.g. Static IP Address or DHCP
- **IP Address** ⇒ e.g. 192.168.100.149
- **Netmask** ⇒ e.g. 255.255.255.0
- **Gateway** ⇒ e.g. 192.168.100.1



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.



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 8029HEPTA/GPS via the **Apply** button. Afterwards the entry of the **Device Password** is requested:



The Time Server 8029NTP/GPS 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 8029HEPTA/GPS and are immediately active.

7.2.2 Standard Display Image with valid Time

Example image for the standard display after a system start with valid backup information or after manual input of the time information via the WebGUI:

UTC	16:25:58	GPS	SYSTEM-STATUS: SYNC
TU	12/JAN/2016	T:07	NTP: STRATUM 01/HIGH

Time Information:

LOC 10:25:19 /D	Display with the setting: local time . <ul style="list-style-type: none"> • D for summertime (Daylight-Saving Time) • S for standard time (wintertime)
UTC 08:25:19	Display with the setting: UTC time .
MO - TU - WE - TH - FR - SA - SU	Display with the Weekday in abbreviations: complies with MONDAY – SUNDAY
12/JAN/2016	Display of date: Day / Abbr. of Month / Year



It can be switched between UTC and local time as time basis for the display by using the button.
Therefore the pushbutton must be pressed for 5 seconds.

GPS Information:

The number of the currently and actually received satellites is shown here. If the value drops under "04" the value starts flashing.



In the GPS reception mode "3D" at least 4 satellites for the synchronization need to be received.

System-Status:

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

NTP-Status:

The current Stratum and accuracy value of the NTP service is shown here.

7.2.3 Standard Display with Additional Information

In the standard display further systemically significant information/conditions are displayed as soon as they occur.

UTC 16:25:58	GPS	SYSTEM-STATUS:			
TU 12/JAN/2016	T:00	Sync	Source-ERROR		

Active additional information automatically leads to the activation of the backlight.

Supplementary information is indicated alternating to the standard content of the display. Such additional information include following details/conditions:

1. Announcement active (see **Chapter 7.10 Announcements (Summertime / Leap Second)**)
2. Sync Source ERROR active (see **Chapter 7.9 Sync Source ERROR**)
3. An Image-Update of Module 8029HEPTA is active
4. A H8-Update of the Sync Source is active

7.3 GENERAL ERROR

Should a failure occur within the system not ensuring a defined and safe operation of the Time Server 8029HEPTA/GPS anymore this is indicated via the LCD-Display.

If there is an active GENERAL ERROR, the backlight is activated.

If such an error occurs it is recommended to disconnect the system from power for 30 seconds and then turn it on and put it into operation again. If the failure occurs again after this process, the system needs to be sent for repair or rather contact the **hopf** Support with the appropriate failure report (see **Chapter 10.2 Support by Company hopf**).

Example:

GENERAL-ERROR: NO DATA FROM SYNC-SOURCE
Turn OFF/ON power may solve the problem

7.4 LAN Parameter

The 3 display pictures of the LAN parameter indicate essential information on the LAN interface.

For more detailed information see **Chapter 8.3.2 NETWORK Tab.**

In the display picture LAN-Para-01 the currently valid values of the IP address, netmask and gateway are shown and whether the values are statically assigned via the WebGUI or via DHCP.

Example:

LAN-Para-01: STATIC	IP: 192.168.010.099
GW: 192.168.010.001	NM: 255.255.255.000

In the display picture LAN-Para-02 the **hopf** set MAC address and hostname (max. 30 characters – the balance is cut in the display) for the LAN interface are stated.

Example:

```
LAN-Para-02:  MAC 00:03:C7:01:27:D7
Hostname:  hopf8029hepta
```

In the display picture LAN-Para-03 it is indicated whether the LAN interface disposes of an active link to another network and with which transmission speed it is communicated (network operation mode).

Example:

```
LAN-Para-03: Link status: Up
Network operation mode: Auto negotiate
```

7.5 Local Time Parameter

Provided a local time via the input of difference time to UTC and/or switching points for the summertime is parameterized, these values can be read in the display.

Example:

Time-Zone	S->D	02:00	SU	28/04/2013
Offset:+01:00	D->S	03:00	SU	27/10/2013

The difference time to UTC was set to +1h in the above example. Based on the general parameters for the summer-/wintertime changeover set in the WebGUI, the following switching points are calculated for the current year (2013) by the system:

- Start of summertime (S \square D) on Sunday, 28 April 2013 at 2.00 o'clock
- End of summertime (D \square S) on Sunday, 27 October 2013 at 3.00 o'clock

Without valid time (System-Status INVA) the real values for the ST/WT changeover cannot be calculated.

Missing	Data
Missing	Data

Should the ST/WT changeover be disabled, it is shown in the display as follows:

Time-Zone	S->D	changeover	disabled
Offset:+01:00	D->S	changeover	disabled

Should the difference time and/or ST/WT changeover not be initially set by the user (in this case at least one Sync Source ERROR is active), the following picture is displayed:

Time-Zone Offset and/or DST Changeover
not initially set by USER

7.6 GPS Satellite Display

V:xx - Satellites in View

Number of available satellites detected by the GPS receiver.

T:xx - Satellites Tracked

Effective number of received satellites used for synchronization.

yy:zzz - Satellites Number : S/N Ratio

Overview of actually received GPS satellites with their number and reception quality and the pertinent interpretation.

≥ 48	Good reception quality
31-47	Sufficient reception quality
0-30	Poor reception quality

Example:

GPS	V:12	11:099	12:098	13:097	14:096
SAT	T:09	15:095	16:094	17:093	18:092



Maximal 8 satellites are shown in the display regardless from the actually received number.

7.7 Position

In this picture the position determined by the GPS receiver or rather set via the WebGUI is displayed.

Example:

GPS	Latitude :	51°12,6861'	North
POS	Longitude:	007°39,8195'	East

The above example shows the indication of the position data of the company **hopf**.

7.8 Receiver Status

This image displays the reception status information determined by the GPS receiver.

Example:

Receiver	PDOP: 2.46	Noise-Level: 133
Status	AGC: 18.7%	JAM: 13.9% -> Critical

Receiver	PDOP: 9.99	Noise-Level: 112
Status	AGC: 18.7%	JAM: 3.9% -> OK

Receiver	PDOP: 9.99	Noise-Level: 98
Status	AGC: 7.7%	JAM: 9.9% -> Warning

7.9 Sync Source ERROR

In the display the same Sync Source Errors messages are stated as in WebGUI (see **Chapter 8.3.6.13 Module Errors**).

If there is more than one error, the different error messages are continuously indicated once a second.



Should a Sync Source ERROR occur, this is signaled in the standard image.

SYNC - SOURCE ERROR:	No error
----------------------	----------

Example for a Sync Source ERROR:

SYNC - SOURCE ERROR:	01 ERROR ACTIVE
HW ->	Antenna circuit open

In the above picture no antenna has been connected to the system or rather the cable to the antenna is interrupted.

7.10 Announcements (Summertime / Leap Second)

In this picture the availability of an announcement for a summer-/wintertime changeover (DST-Announcement) or for inserting a leap second (Leap Second Announcement) is indicated.



Should an announcement be available, this is signaled in the standard image.

Example:

DST - Announcement:	ACTIVE
Leapsecond - Announcement:	Not active

In the above picture a summer-/wintertime changeover is processed on the next hour change.

7.11 System-Info

In the pictures with the system info, the uptime of the system, program versions and the serial numbers of the components are indicated.

In the display picture SYS-Info 01 the uptime and the image version of the Module 8029HEPTA are stated.

Example:

SYS - Info:	Uptime:0001-Day/02-Hour/53-Min
01/04	Image:06.00P Date:16.02.2016

In the display image SYS-Info 02 the serial number and the H8 processor version of the Module 8029HEPTA are shown in the first line, whereas in the second line the serial number of the Sync Source and its H8 processor version are stated.

Example:

SYS - Info:	8029-010133 P06.00 -16.02.2016
02/04	8024-010310 P01.00 -16.02.2016

The display images SYS-Info 03 and 04 indicate device information exclusively required by the **hopf** Support.

Example:

SYS - Info:	011511B4001899999999A00010806
03/04	1300000001383F00080210130002

SYS - Info:	010403B0000199999999A04012709
04/04	1200000010000304012709120011

8 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.

8.1 Quick Configuration

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

8.1.1 Requirements

- Ready-for-operation **hopf** NTP Time Server 8029HEPTA/GPS
- PC with installed web browser (e.g. Internet Explorer) in the sub-network of Time Server 8029HEPTA/GPS

8.1.2 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 and if available 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.

8.2 General – Introduction

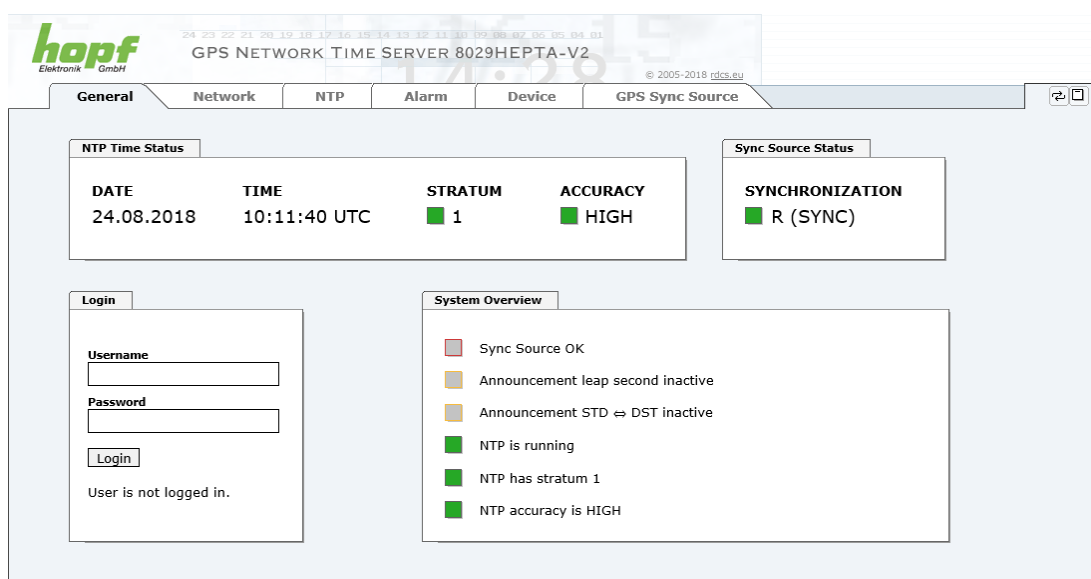
The Time Server 8029HEPTA/GPS should be accessible to a web browser if it has been set up correctly. Enter the IP address <http://xxx.xxx.xxx.xxx> - as set up in the Time Server 8029HEPTA/GPS earlier - or the DNS name on the address line and the following screen should appear.

When using IPv6, it is mandatory to enclose the IPv6 address with []

e.g.: [http://\[2001:0db8:85a3:08d3::0370:7344\]/](http://[2001:0db8:85a3:08d3::0370:7344]/)



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



The screenshot shows the WebGUI interface for the hopf GPS NETWORK TIME SERVER 8029HEPTA-V2. The interface has a top navigation bar with tabs: General, Network, NTP, Alarm, Device, and GPS Sync Source. The 'General' tab is active. Below the navigation bar, there are several status boxes:

- NTP Time Status:**

DATE	TIME	STRATUM	ACCURACY
24.08.2018	10:11:40 UTC	1	HIGH
- Sync Source Status:**

SYNCHRONIZATION
R (SYNC)
- Login:**

Username:

Password:

User is not logged in.
- System Overview:**
 - Sync Source OK
 - Announcement leap second inactive
 - Announcement STD ⇌ DST inactive
 - NTP is running
 - NTP has stratum 1
 - NTP accuracy is HIGH



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.

8.2.1 LOGIN and LOGOUT as User

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

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



Differentiation is made between **upper and lower case** characters in the password. Alphanumeric characters and the following symbols can be used: . , ! " \$ % & / { } [] () = ? \ + - @ * ~ # ' < > | ; : _

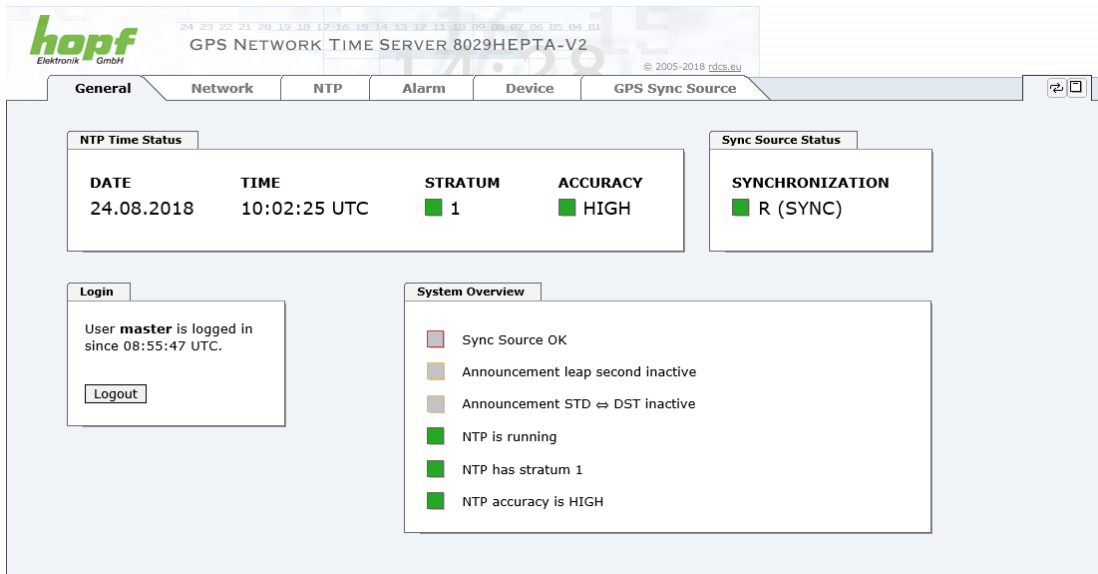


The password must be between 6 and 20 characters long and contain at least one uppercase letter, one lowercase letter and one digit!



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.

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

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

Users logged in as "master" have all access rights to the Time Server 8029HEPTA/GPS.

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

8.2.2 Navigation via the Web Interface

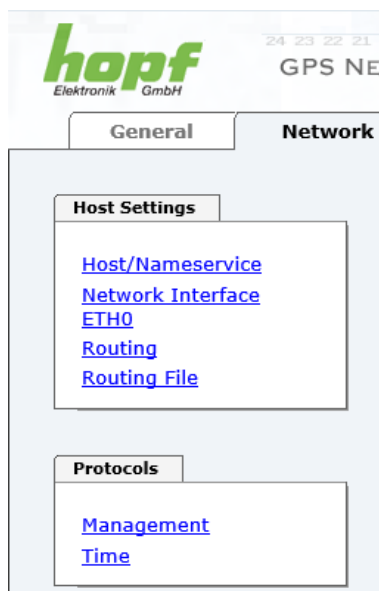
The WebGUI is divided into functional tabs. Click on one of these tabs to navigate through the board. The selected tab is identified by a darker background colour, see the following image (General in this case).



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.

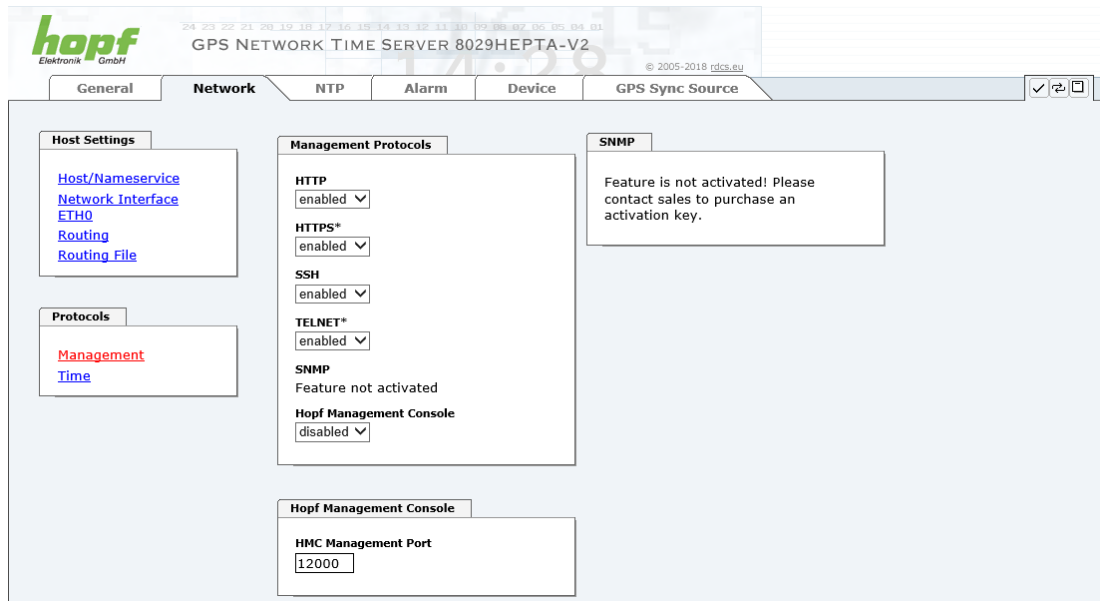
8.2.3 Enter or Changing Data

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

8.2.3.1 Changing of Data in 8029HEPTA (WebGUI: Device)

All changeable data, except those in GPS SYNC SOURCE tab, are saved in Module 8029HEPTA. For these data the value saving is divided into two steps.

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



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



Meaning of the symbols from left to right:

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

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



Changing Network Parameters

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

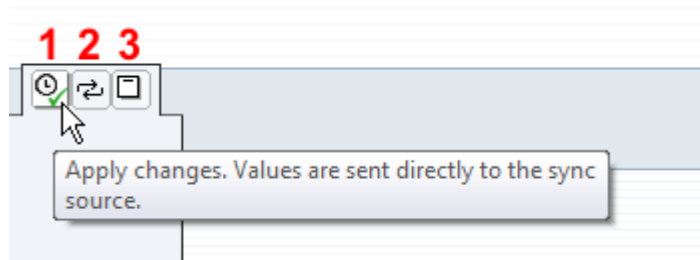
However, the modifications are not permanently saved yet. This requires to access the WebGUI with the new network parameters again and to save the data with **Save** permanently.



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

8.2.3.2 Changing of Data in 8024GPS (WebGUI: GPS Sync Source)

The modified data in the GPS SYNC SOURCE tab are directly transferred to the Module 8024GPS by pushing the button 1 and stored failsafe in Module 8024GPS. Tabs with settings and values modified in this manner can also be recognized by the modified display of the **Apply** button. The buttons 2 and 3 in GPS SYNC SOURCE tab are disabled and are not required.

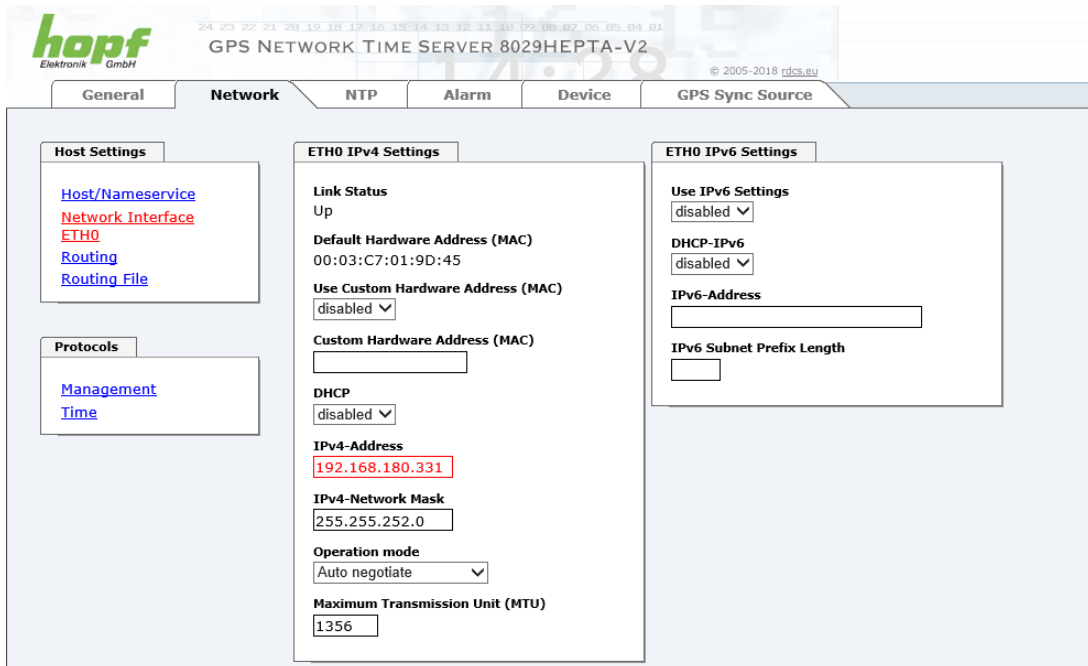


The new reading of the modified data from Module 8029HEPTA for the WebGUI indication can take up to 30 seconds after data transfer to Module 8024GPS.

However, this has no effect on the function of the appropriate setting/value.

8.2.4 Plausibility Check during Input

A plausibility check is generally carried out during input.



The screenshot shows the web interface for the hopf GPS NETWORK TIME SERVER 8029HEPTA-V2. The 'Network' tab is selected, showing settings for the 'ETH0' interface. The 'IPv4-Address' field contains the value '192.168.180.331', which is highlighted with a red border, indicating an invalid value. Other fields like 'IPv4-Network Mask' (255.255.252.0) and 'Maximum Transmission Unit (MTU)' (1356) are also visible. The 'IPv6' settings are currently disabled.

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.

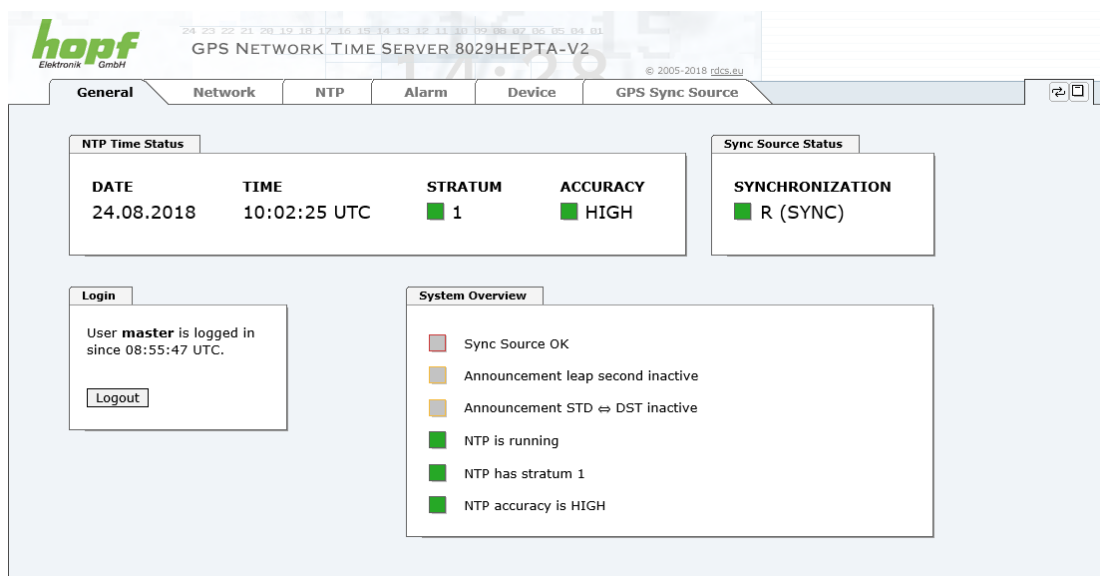
8.3 Description of the Tabs

The WebGUI is divided into the following tabs:

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

8.3.1 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 8029HEPTA/GPS. 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 8029HEPTA/GPS 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 14.5 Accuracy & NTP Basic Principles**.

Sync Source Status

Display of the actual status of synchronization of the Sync Source (here Module 8024GPS) 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

Login

The login box is described in **Chapter 8.2.1 LOGIN and LOGOUT as User**

System Overview

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

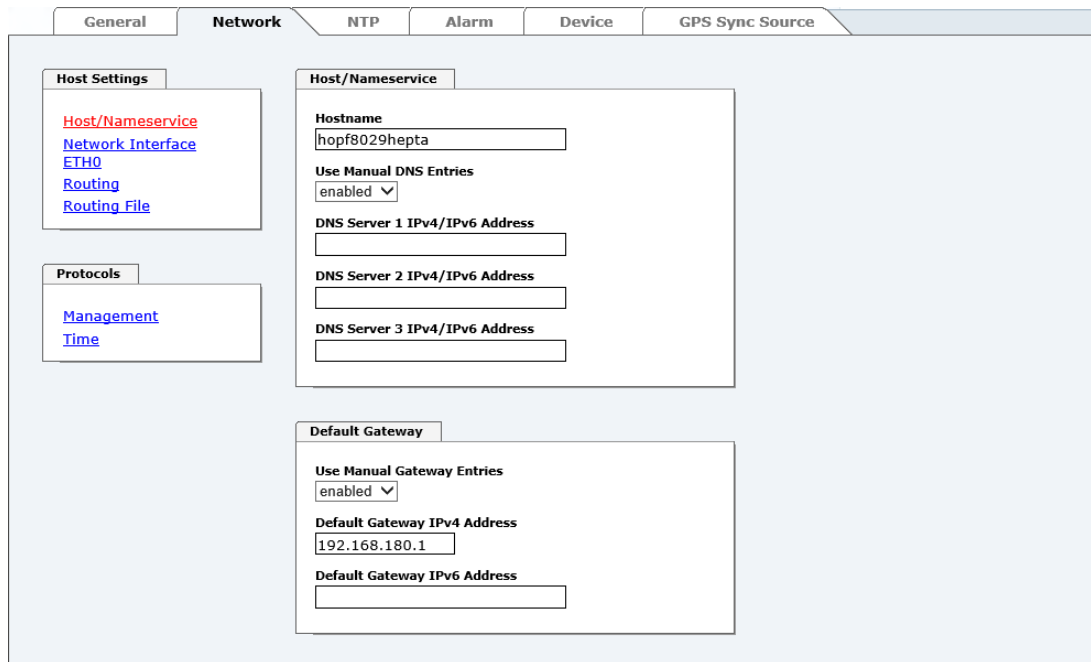
WebGUI	Description
Sync Source OK	When active (RED) there is a Sync Source failure. For details please go to GPS SYNC SOURCE tab - Module Errors .
Announcement leap second inactive	When active (ORANGE) there is an announcement for a leap-second.
Announcement STD ⇔ DST inactive	When active (ORANGE) there is an announcement for a summer / winter time change-over.
NTP is running	The NTP process on Module 8029HEPTA 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.

Announcements

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

8.3.2 NETWORK Tab

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




Changing Network Parameters

Modifications of the network parameters (e.g. IP address) are immediately effective clicking on **Apply** to confirm. However, the modifications are not permanently saved yet. This requires to access the WebGUI with the new network parameters again and to save the data with **Save** permanently.

8.3.2.1 Host/Name Service

Setting for the explicit network detection.

8.3.2.1.1 Hostname

The standard setting for the Hostname is "**hopf8029hepta**". 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.

8.3.2.1.1 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.

8.3.2.1.2 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.

8.3.2.1.3 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.

8.3.2.1.4 Default Gateway IPv4

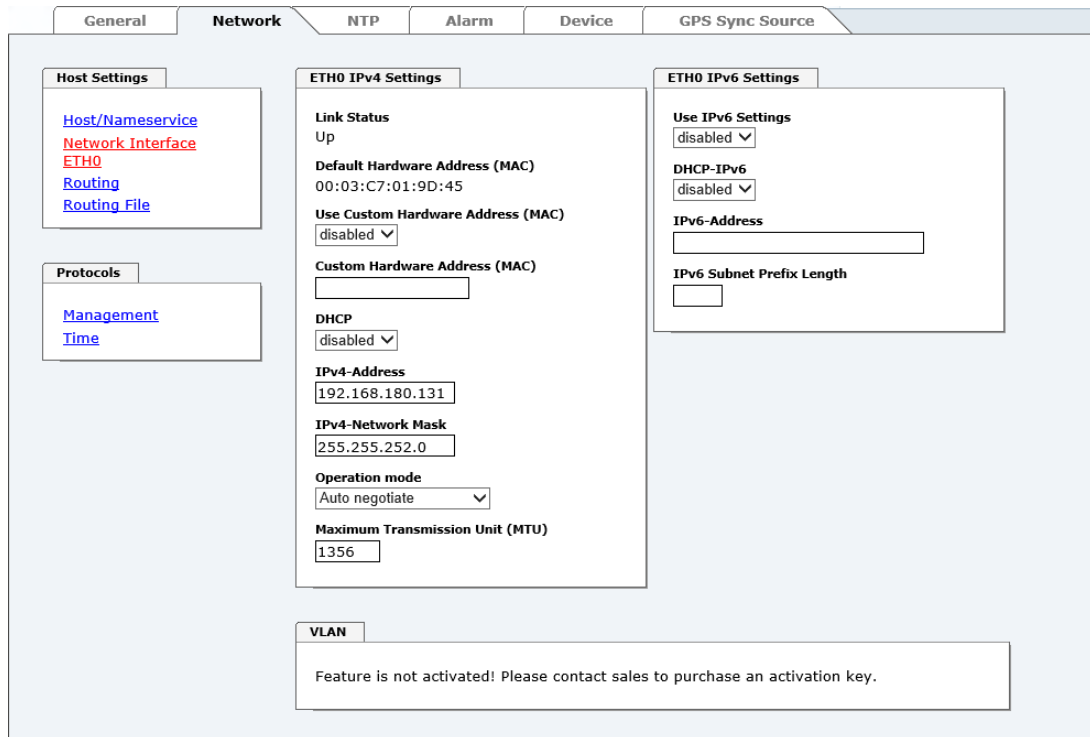
If the IPv4 default gateway is not known, it must be requested by the network administrator. If no standard gateway is available (special case), enter 0.0.0.0 in the input field or leave the field blank.

8.3.2.1.5 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.

8.3.2.2 Network Interface ETH0

Configuration of the Ethernet interface ETH0 of the Time Server 8029HEPTA/GPS.



8.3.2.2.1 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 2.2.6.1 MAC-Address for ETH0** for the Time Server 8029HEPTA/GPS.



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

8.3.2.2.2 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**



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



There are no MAC multicast addresses allowed!

Finally, the module 8029HEPTA has to be restarted via "Device" -> "Reboot Device" (see **Chapter 8.3.5.4 Restarting the Module (Reboot Device)**).

8.3.2.2.3 DHCP

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

8.3.2.2.4 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.

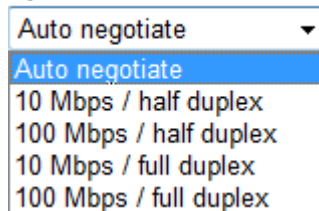
8.3.2.2.5 IPv4 Network Mask

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.

8.3.2.2.6 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.

Operation mode




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 8029HEPTA/GPS **and** the connected network components manually to the same value.

8.3.2.2.7 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.

The Time Server 8029HEPTA/GPS is going to be delivered with default setting 1356.

8.3.2.2.8 IPv6

The Time Server 8029HEPTA/GPS 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**

8.3.2.2.9 DHCP-IPv6

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

8.3.2.2.10 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.

8.3.2.2.11 IPv6 Subnet Prefix Length

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.

8.3.2.2.12 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 8029HEPTA/GPS, 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

VLAN Interfaces

ID	Label	Remark	DHCP	IPv4-Address	IPv4-Network Mask
<input type="checkbox"/> 10	DEV	Development	<input type="text" value="disabled"/>	192.168.180.30	255.255.255.0



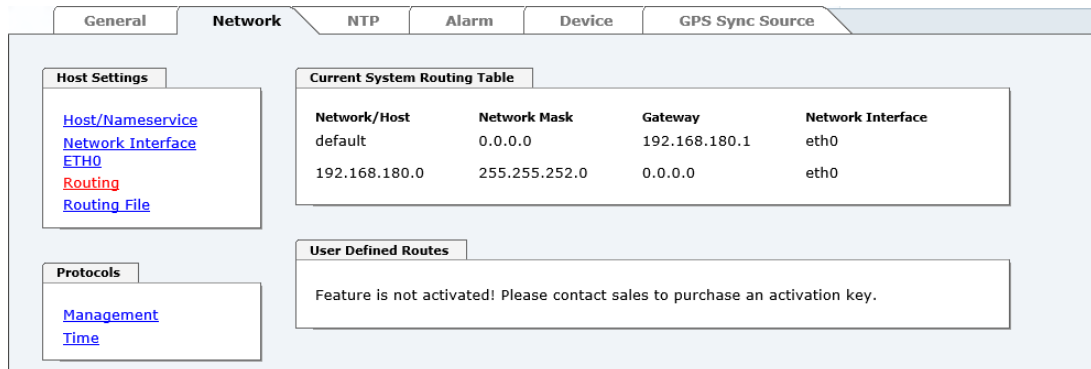
To ensure the correct function the network appliance must be connected with Time Server 8029HEPTA/GPS via the network interface. Furthermore it must be ensured that the network appliance is accurately configured with the same VLANs.



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

8.3.2.3 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.

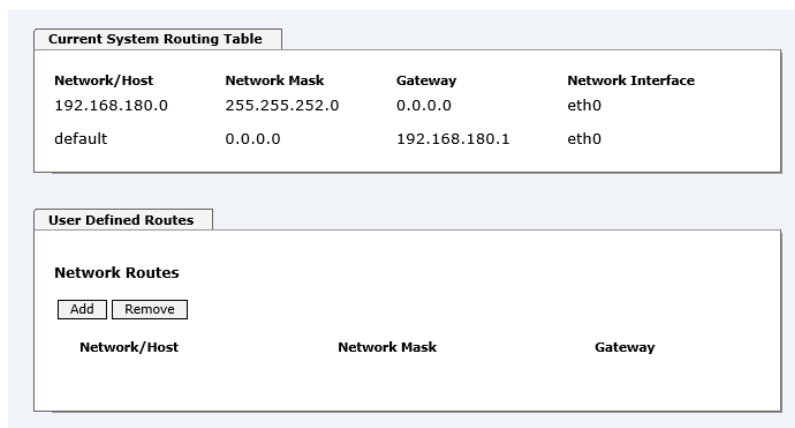


The gateway / gateway host need to be in the local sub-network range of the module in order to use the static routes.



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

WebGUI with Routing activated



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



The module cannot be used as a router!

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 8.3.2.4 Routing File**.

8.3.2.4 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.


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
00000000000000000000000000000000 80		00000000000000000000000000000000	lo
fe80000000000000000203c7fffe01947e 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

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

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

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



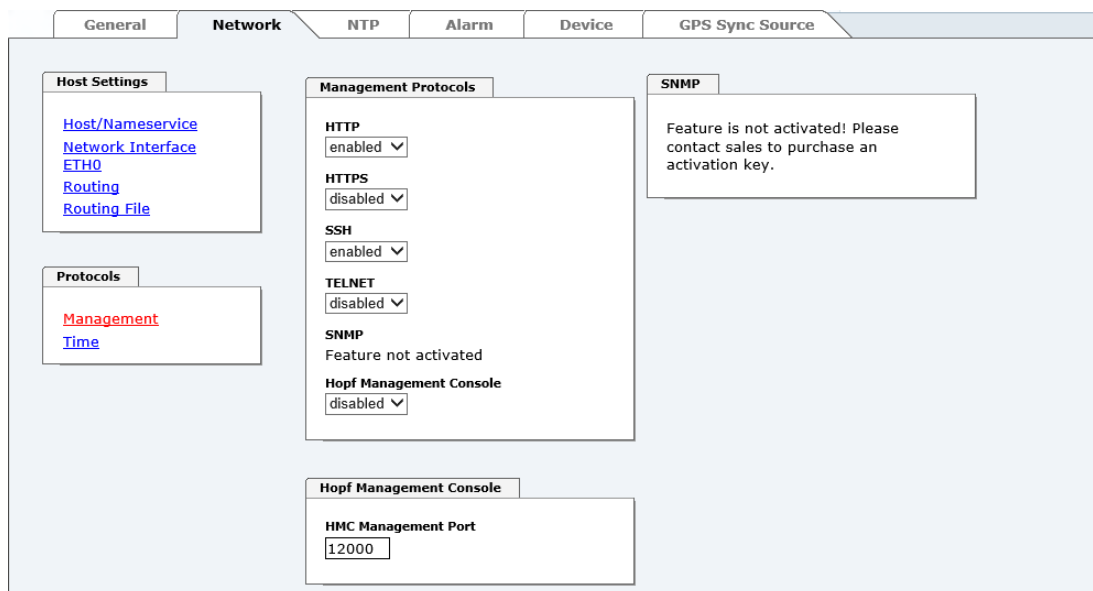
For SNMP functionality an activation key is necessary.



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



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



The screenshot shows the 'Management Protocols' configuration page in the Hopf Management Console. The page has a top navigation bar with tabs: General, Network, NTP, Alarm, Device, and GPS Sync Source. The 'Network' tab is active. On the left, there are two sub-sections: 'Host Settings' with links for Host/Nameservice, Network Interface, ETH0, Routing, and Routing File; and 'Protocols' with links for Management and Time. The main content area is divided into three panels. The 'Management Protocols' panel contains settings for HTTP (enabled), HTTPS (disabled), SSH (enabled), TELNET (disabled), and SNMP (Feature not activated). Below this is the 'Hopf Management Console' panel with the 'HMC Management Port' set to 12000. The 'SNMP' panel on the right displays a message: 'Feature is not activated! Please contact sales to purchase an activation key.'



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

WebGUI with Alarming activated

Management Protocols		SNMP
HTTP enabled ▼	Network Interface Both ▼	System Location <input type="text"/>
HTTPS disabled ▼	Network Interface Both ▼	System Contact <input type="text"/>
SSH enabled ▼	Network Interface Both ▼	SNMPv2 Read Only Community <input type="text" value="public"/>
TELNET disabled ▼	Network Interface Both ▼	SNMPv2 Read Write Community <input type="text" value="secret"/>
SNMP disabled ▼	Network Interface Both ▼	SNMPv3 Security Name <input type="text"/>
		SNMPv3 Access Rights Readonly ▼
		SNMPv3 Authentication Protocol MD5 ▼
		SNMPv3 Authentication Passphrase <input type="text"/>
		SNMPv3 Privacy Protocol DES ▼
		SNMPv3 Privacy Passphrase <input type="text"/>

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

8.3.2.5.1 SNMPv2 / SNMPv3 (Activation Key required)

Both protocols SNMPv2 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 (SNMPv2 / SNMPv3).

In order to disable SNMPv2 both fields **SNMP Read Only Community** and **SNMP Read Write Community** must remain empty.

SNMPv2	SNMPv2 enabled	SNMPv2 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 SNMPv2
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 passphrases:

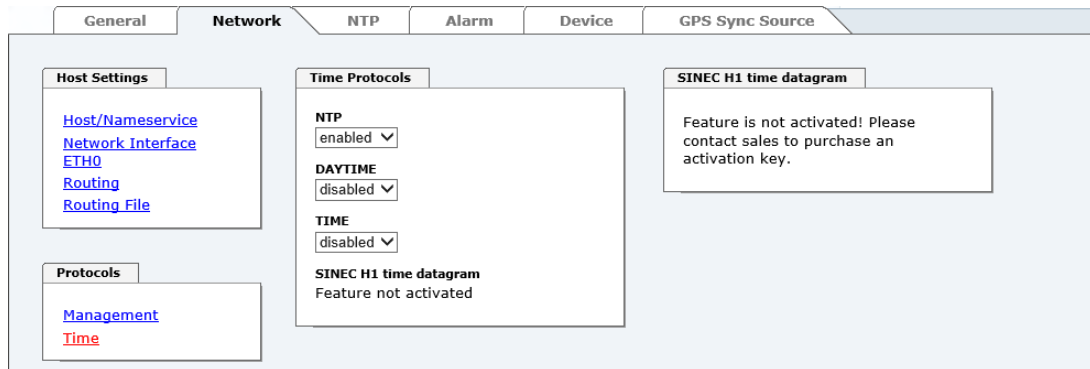
SNMPv3	noAuthNoPriv	authNoPriv	authPriv
Authentication Passphrase:	empty	set	set
Privacy Passphrase:	empty	empty	set



Right now only one user is supported.

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

Activation and configuration of different synchronization protocols




All protocols can be enabled at the same time.

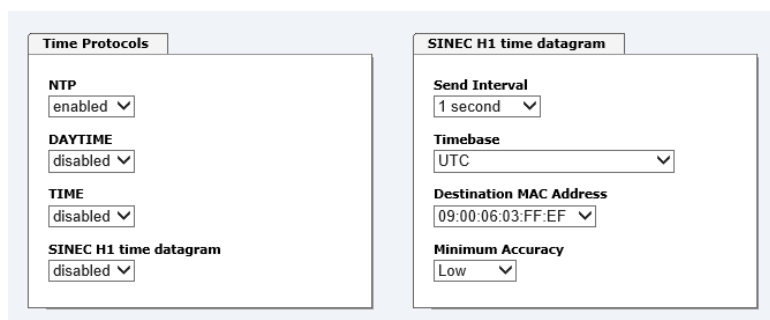
8.3.2.6.1 Synchronization Protocols (Time Protocols – NTP, SNTP etc.)

Needed time protocols can be enabled here.

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

8.3.2.6.2 SINEC H1 Time Datagram (Activation Key necessary)

Configuration of the SINEC H1 time datagram



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

- every second
- every 10 second
- every 60 second

Time base see also *Chapter 14.2.1 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 14.5 Accuracy & NTP Basic Principles*** and ***Chapter 12 Technical Data***):

- LOW
- MEDIUM
- HIGH



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

8.3.3 NTP Tab

This tab shows information and adjustment possibilities of the NTP services of the Time Server 8029HEPTA/GPS. The NTP service is the significant main service of the Time Server 8029HEPTA/GPS.

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 8029HEPTA/GPS.

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 8.3.2.6 Time**)



After all changes relating to NTP a restart of the NTP service must be performed (see **Chapter 8.3.3.6 Restart NTP**).



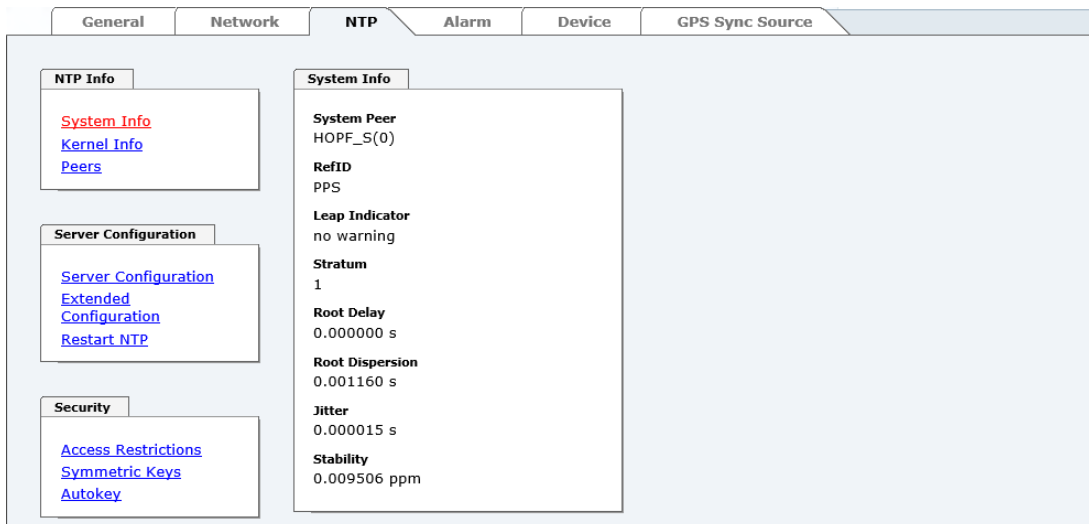
Via the NTP protocol SNTP Clients can also be synchronized. In contrast to NTP in SNTP Clients delay times are not evaluated on the network. For this reason the accuracy reached in SNTP Clients is lower than in NTP Clients.

8.3.3.1 System Info

In the window "System Info" the current NTP values of the NTP service running on the embedded Linux of the Time Server 8029HEPTA/GPS are indicated. In addition to the NTP calculated values for root delay, root dispersion, jitter, and stability the stratum value of the Time Server 8029HEPTA/GPS, 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 8029HEPTA/GPS 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.



8.3.3.2 Kernel Info

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



This screenshot shows a maximum kernel clock error of 4.500 msec (milliseconds). The estimated error value is 5 μ s (microseconds).

The values indicated here are based on the calculation of the NTP service and have no significance for the accuracy of the Sync Source (here Module 8024GPS).

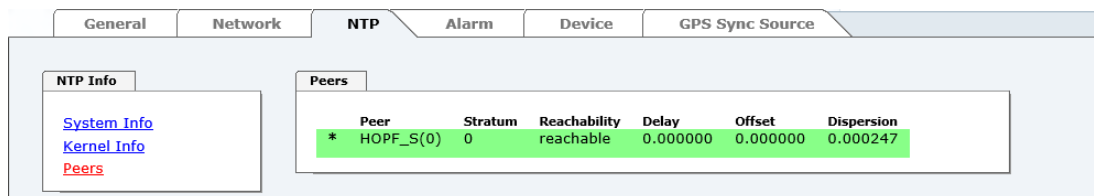
8.3.3.3 Peers

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 programs.

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

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



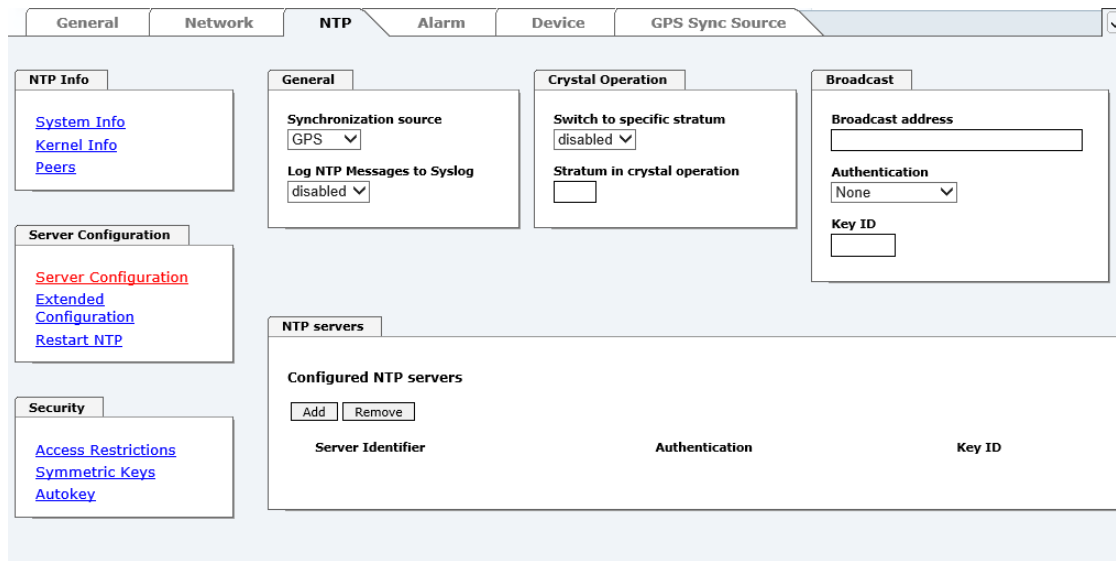
The first line displays the **hopf - refclock ntp driver** that gets the time information directly from the Sync Source.

A short explanation and definition of the displayed values can be found in **Chapter 14.5 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 14.2 Tally Codes (NTP-specific)**).

8.3.3.4 Server Configuration

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



The **hopf – refclock ntp driver** is already configured as standard (127.127.38.0 in the “Peers Summary”) and is not explicitly displayed here.

8.3.3.4.1 Synchronization Source (General / Synchronization source)

As “Synchronization source” either GPS or DCF77, depending on the appropriate Sync Source, has to be selected. This is required 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.

8.3.3.4.2 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 8.3.4.1 Syslog Configuration**).

8.3.3.4.3 Crystal Operation

Crystal Operation / Switch to Specific Stratum

If the Sync Source (here Module 8024GPS) runs in crystal operation (status "crystal") the NTP service of the Time Server 8029HEPTA/GPS 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 8029HEPTA/GPS 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 8029HEPTA/GPS during crystal operation of the Sync Source).

For the synchronization 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 fall back 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 8.3.3.6 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 (here Module 80121GPS) 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 8029HEPTA/GPS 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.

8.3.3.4.4 Broadcast / Broadcast Address

This section is used to configure the Time Server 8029HEPTA/GPS 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 8029HEPTA/GPS. 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 8029HEPTA/GPS 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.

8.3.3.4.5 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.

8.3.3.4.6 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 8029HEPTA/GPS.

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

8.3.3.5 Extended NTP Configuration

NTP is a standard for synchronising clocks in computer systems via packet-based communication networks. For special applications a NON standard setting can be configured.

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

8.3.3.5.1 Suppression of unspecified NTP Outputs (Block Output when Stratum Unspecified)

Unspecified NTP outputs that e.g. are generated by NTP at a restart are suppressed when this function is enabled.

8.3.3.5.2 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 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 for *SINEC H1 TIME DATAGRAM / TIME / DAYTIME* is released with a wrong time basis. Therefore this datagram should be deactivated for security reasons.



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

- Select the desired NTP time base.
- Transfer the setting with **Apply Changes** to the Time Server.
- 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.

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.



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

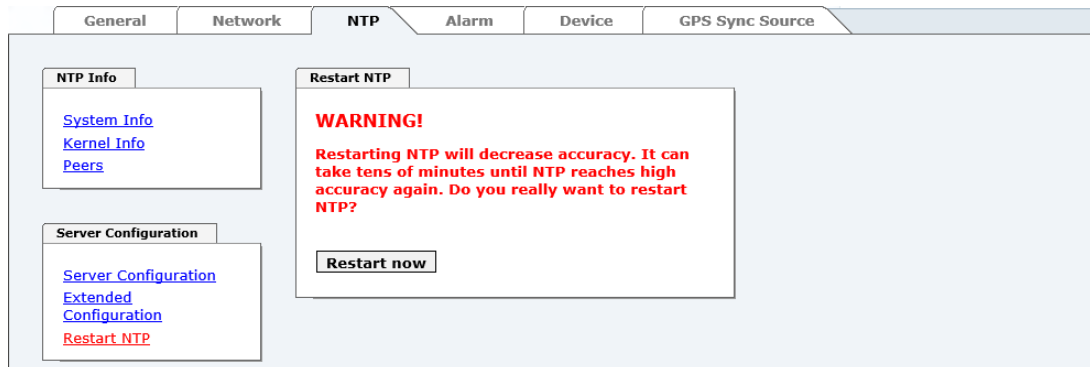
Afterwards the local time is correctly available in the NTP time protocol. Therefore, within this transition period a requested NTP time protocol is replied by the former time base.



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!

8.3.3.6 Restart NTP

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



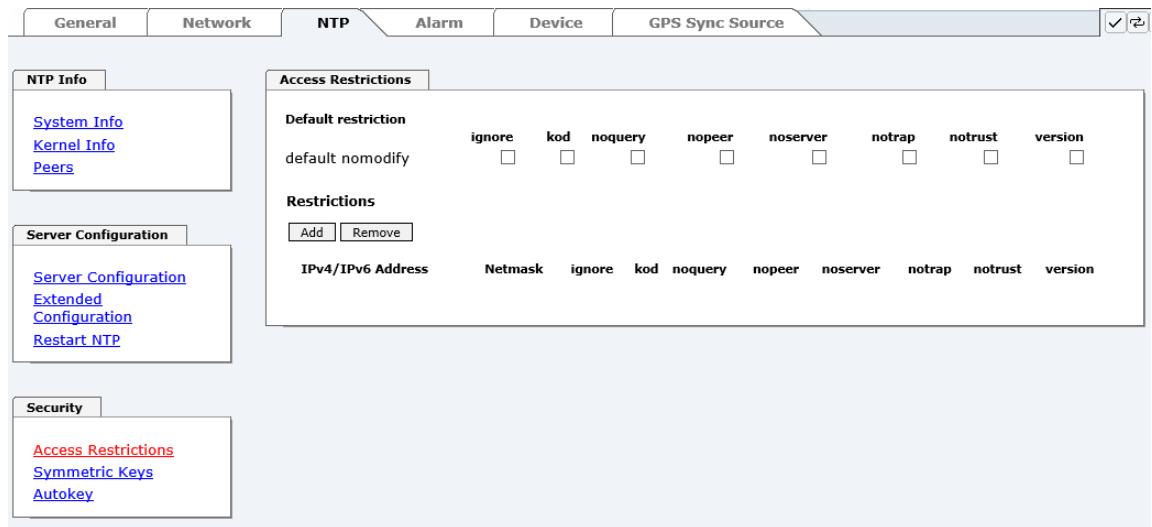
Restarting NTP services is the only possibility of making NTP changes effective without having to restart the entire Time Server 8029HEPTA/GPS. As can be seen from the warning message, the currently reachable stability and accuracy get lost caused by this restart.



After a restart of the NTP service it takes up to 10 minutes until the NTP service on the Time Server 8029HEPTA/GPS is completely adjusted.

8.3.3.7 Configuring the NTP Access Restrictions

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



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 Hostnames!

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 **8.3.3.7.1** to **8.3.3.7.4** must be checked by the user:

8.3.3.7.1 NAT or Firewall

Are incoming connections to the NTP Service blocked by NAT or a Stateful Inspection Firewall?	
No	Proceed to Chapter 8.3.3.7.2 Blocking Unauthorised Access
Yes	No restrictions are required in this case. Proceed further to Chapter 8.3.3.7.4 Internal Client Protection / Local Network Threat Level

8.3.3.7.2 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 8.3.3.7.3 Allowing Client Requests
Yes	<p>In this case the following restrictions are to be used:</p> <p style="text-align: center;">ignore in the default restrictions <input checked="" type="checkbox"/></p> <p>If a standard restriction is selected in this area, exceptions can be declared in separate lines for each authorised server, client or sub-network. See Chapter 8.3.3.7.5 Addition of Exceptions to Standard Restrictions</p>

8.3.3.7.3 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	<p>In this case select from the following standard restrictions: See Chapter 8.3.3.7.6 Access Control Options</p> <table> <tr><td>kod</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>notrap</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>nopeer</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>noquery.</td><td><input checked="" type="checkbox"/></td></tr> </table>	kod	<input checked="" type="checkbox"/>	notrap	<input checked="" type="checkbox"/>	nopeer	<input checked="" type="checkbox"/>	noquery.	<input checked="" type="checkbox"/>
kod	<input checked="" type="checkbox"/>								
notrap	<input checked="" type="checkbox"/>								
nopeer	<input checked="" type="checkbox"/>								
noquery.	<input checked="" type="checkbox"/>								
Yes	<p>In this case select from the following standard restrictions: See Chapter 8.3.3.7.6 Access Control Options</p> <table> <tr><td>kod</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>notrap</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>nopeer</td><td><input checked="" type="checkbox"/></td></tr> </table> <p>If a standard restriction is selected in this area, exceptions can be declared in separate lines for each authorised server, client or sub-network. See Chapter 8.3.3.7.5 Addition of Exceptions to Standard Restrictions</p>	kod	<input checked="" type="checkbox"/>	notrap	<input checked="" type="checkbox"/>	nopeer	<input checked="" type="checkbox"/>		
kod	<input checked="" type="checkbox"/>								
notrap	<input checked="" type="checkbox"/>								
nopeer	<input checked="" type="checkbox"/>								

8.3.3.7.4 Internal Client Protection / Local Network Threat Level

How much protection from internal network clients is required?							
Yes	<p>The following restrictions can be enabled if greater security settings than the installed authentication are required in order to protect the NTP service from the clients see Chapter 8.3.3.7.6 Access Control Options</p> <table> <tr><td>kod</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>notrap</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>nopeer</td><td><input checked="" type="checkbox"/></td></tr> </table>	kod	<input checked="" type="checkbox"/>	notrap	<input checked="" type="checkbox"/>	nopeer	<input checked="" type="checkbox"/>
kod	<input checked="" type="checkbox"/>						
notrap	<input checked="" type="checkbox"/>						
nopeer	<input checked="" type="checkbox"/>						

8.3.3.7.5 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.

Access Restrictions																													
Default restriction <div> <div>ignore</div> <div>kod</div> <div>noquery</div> <div>nopeer</div> <div>noserver</div> <div>notrap</div> <div>notrust</div> <div>version</div> </div> <div> <div>default nomodify</div> <div><input checked="" type="checkbox"/></div> <div><input checked="" type="checkbox"/></div> <div><input checked="" type="checkbox"/></div> <div><input checked="" type="checkbox"/></div> <div><input checked="" type="checkbox"/></div> <div><input checked="" type="checkbox"/></div> <div><input type="checkbox"/></div> <div><input type="checkbox"/></div> </div>																													
Restrictions <div> <div>Add</div> <div>Remove</div> </div>																													
<table> <thead> <tr> <th>IPv4/IPv6 Address</th> <th>Netmask</th> <th>ignore</th> <th>kod</th> <th>noquery</th> <th>nopeer</th> <th>noserver</th> <th>notrap</th> <th>notrust</th> <th>version</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> 192.168.233.199</td> <td>255.255.224.0</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>										IPv4/IPv6 Address	Netmask	ignore	kod	noquery	nopeer	noserver	notrap	notrust	version	<input type="checkbox"/> 192.168.233.199	255.255.224.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IPv4/IPv6 Address	Netmask	ignore	kod	noquery	nopeer	noserver	notrap	notrust	version																				
<input type="checkbox"/> 192.168.233.199	255.255.224.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																				



An unrestricted access of the Time Server 8029HEPTA/GPS 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.

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

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

kod – "A kiss-o'-death (KoD) packet is transmitted if this option is enabled in the case of an access error." KoD packets are limited. They cannot be transmitted more frequently than once per second. Any KoD packet which occurs within one second from the last packet is removed.

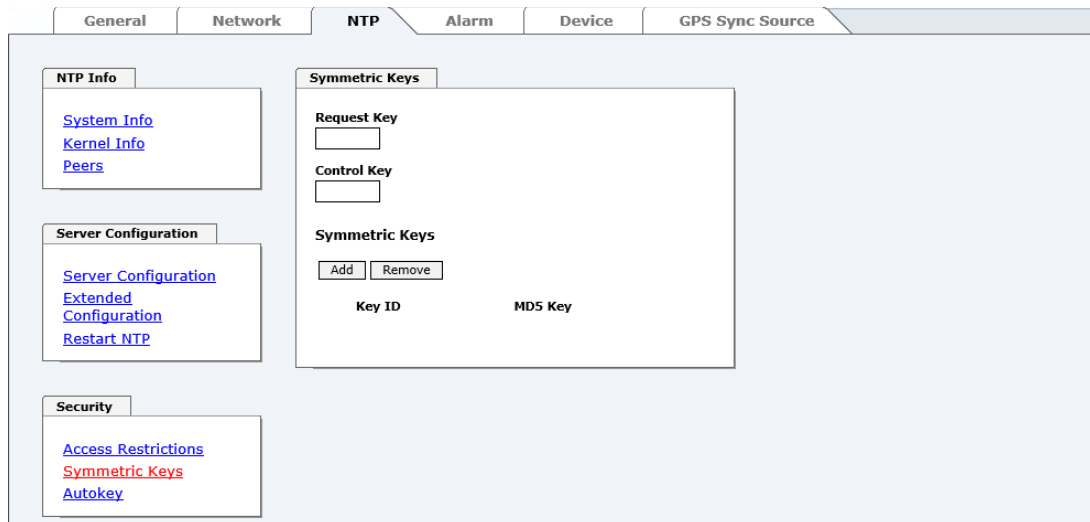
notrap – "Denies support for the mode 6 control message trap service in order to equalize hosts." The trap service is a sub-system of the ntpq control message protocols. This service logs remote events in programmes.

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 8.3.3.6 Restart NTP**).

8.3.3.8 Symmetric Key



8.3.3.8.1 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

8.3.3.8.2 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 8029HEPTA/GPS). The key must be reliable if time is to be synchronised. Authentication causes a delay. This delay is automatically taken into account and adjusted in the current versions.

8.3.3.8.3 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/>.

8.3.3.8.4 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.

8.3.3.9 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.



The screenshot shows the NTP configuration web interface. The top navigation bar includes tabs for General, Network, NTP, Alarm, Device, and GPS Sync Source. The NTP tab is active. On the left, there are links for NTP Info (System Info, Kernel Info, Peers), Server Configuration (Server Configuration, Extended Configuration, Restart NTP), and Security (Access Restrictions, Symmetric Keys, Autokey). The main content area is divided into two sections: Autokey Configuration and Key Generation. The Autokey Configuration section has a dropdown menu for 'Autokey Enabled' set to 'disabled' and a text input field for 'Autokey Password'. The Key Generation section has a 'Generate now' button, an 'Upload Group Key' section with a file upload area and a 'Durchsuchen...' button, and an 'Upload now' button.

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 8029HEPTA/GPS is to form part of an NTP trust group, a group key can be defined and uploaded with the "Upload now" button.

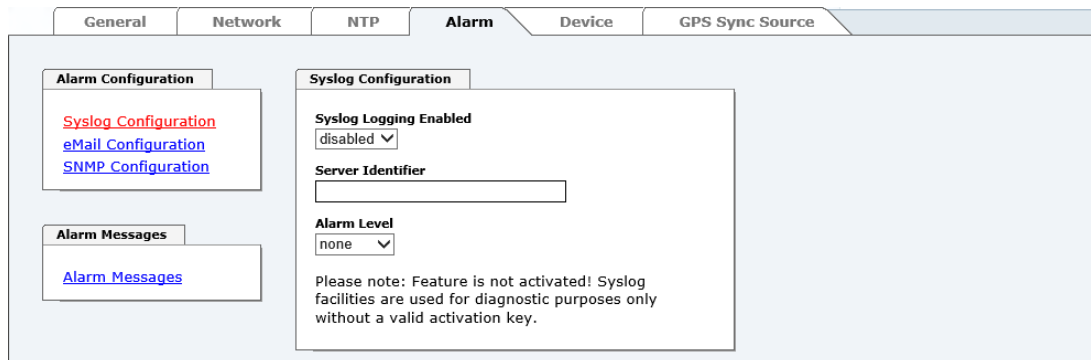
Detailed information about the NTP Autokey scheme can be found in the NTP documentation (<http://www.ntp.org/>).



Changes in data do not take effect immediately after clicking on the "Apply" symbol. The NTP service **MUST** also be restarted (see **Chapter 8.3.3.6 Restart NTP**).

8.3.4 ALARM Tab (Activation Key necessary)

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



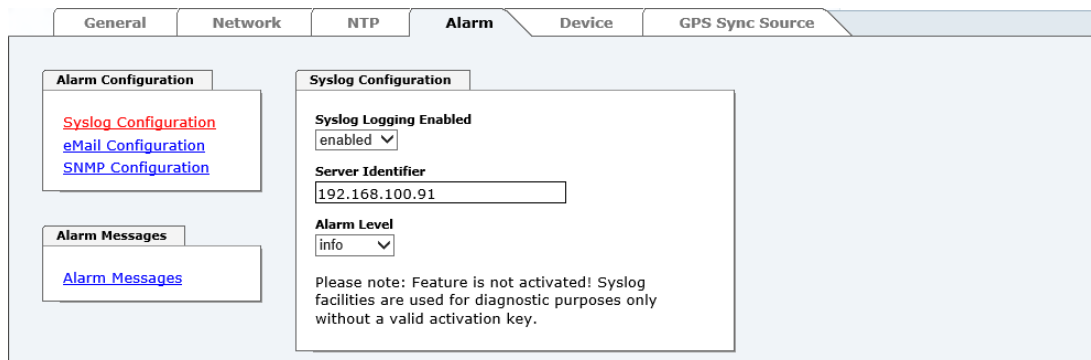
8.3.4.1 Syslog Configuration

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!

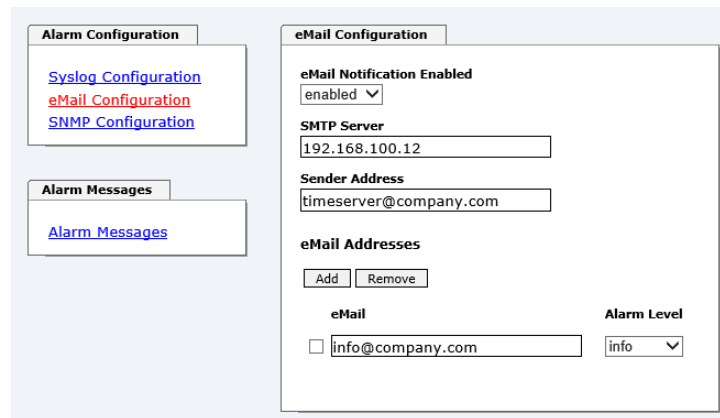


The alarm level designates the priority level of the messages to be transmitted and the level from which transmission should take place (see **Chapter 8.3.4.4 Alarm Messages**).

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 8.3.3.4.2 NTP Syslog Messages (General / Log NTP Messages to Syslog)**).

8.3.4.2 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, independent E-mail addresses which each have different alarm levels.

Depending 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.

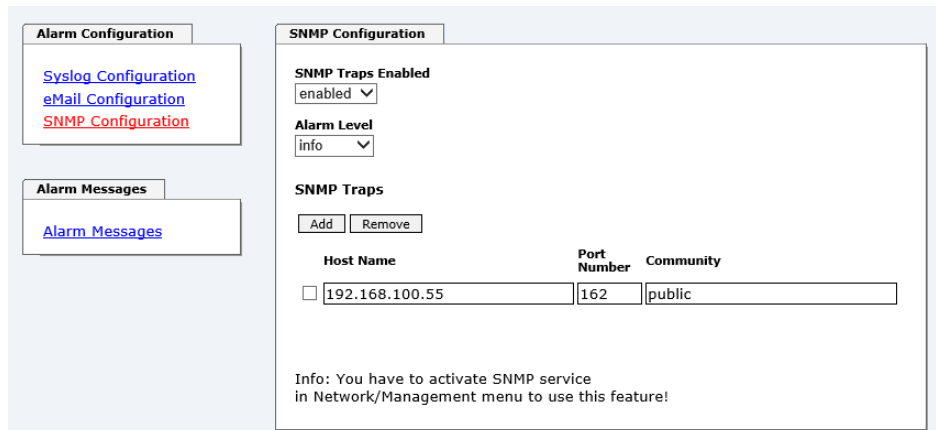
Some E-mail servers only accept messages if the sender address entered is valid (spam protection). This can be inserted in the "Sender Address" field.

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 8.3.4.4 Alarm Messages**).

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

8.3.4.3 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 8.3.5.11 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 8.3.4.4 Alarm Messages**).

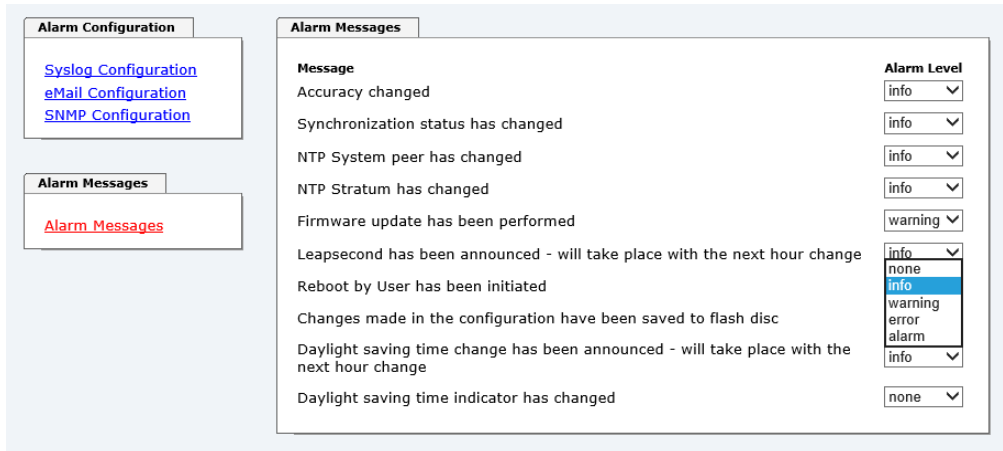
Alarm Level	Transmitted Messages
none	no messages
info	info / warning / error / alarm
warning	warning / error / alarm
error	error / alarm
alarm	alarm



The SNMP protocol must be enabled in order to use SNMP (see **Chapter 8.3.2.5 Management (Management-Protocols – HTTP, SNMP)**).

8.3.4.4 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.



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

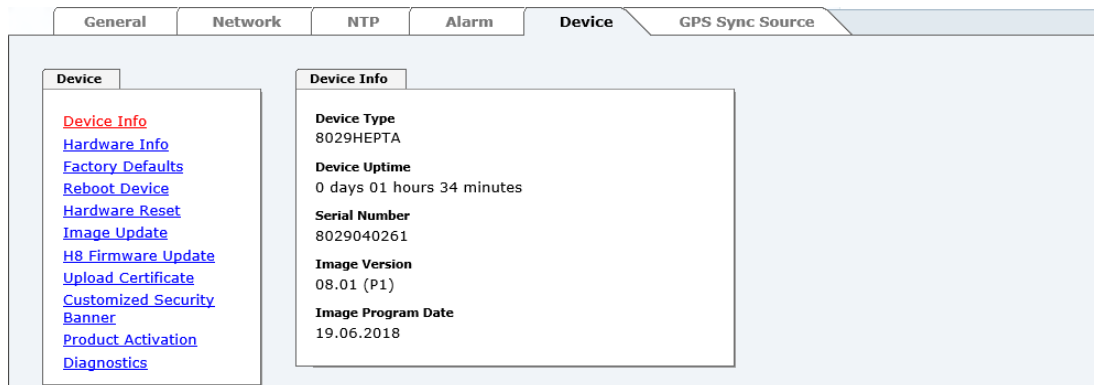
Depending on the messages, their configured levels and notifications levels of the E-mails, a corresponding action is carried out if an event occurs.



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

8.3.5 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 8029HEPTA 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.

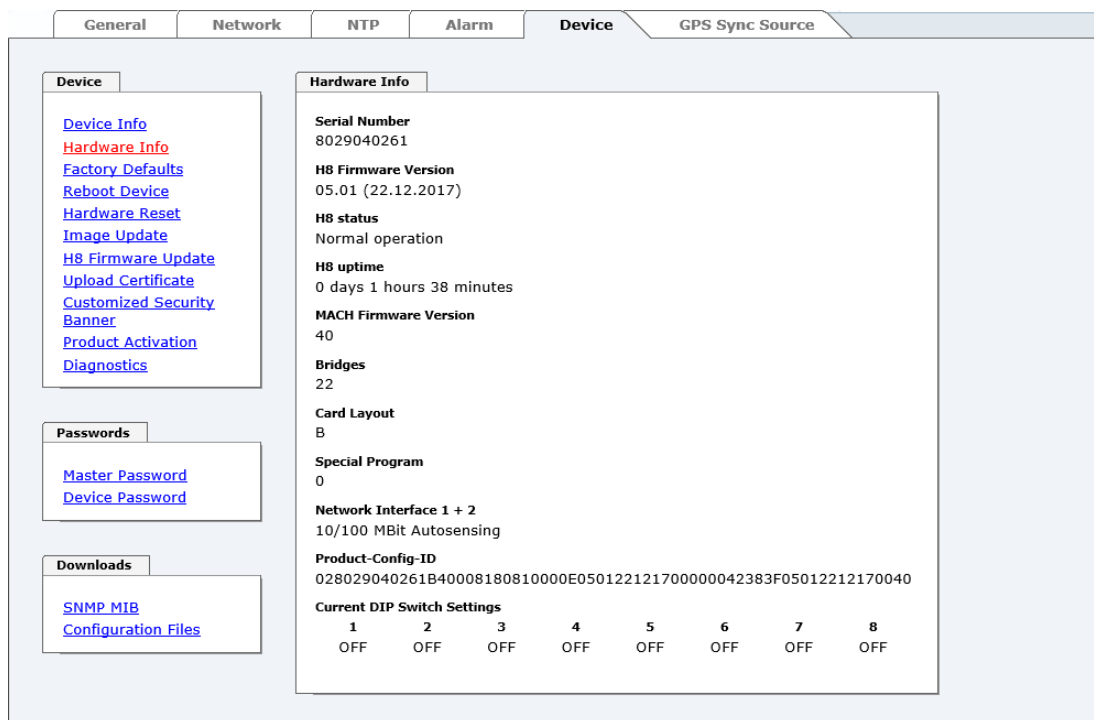
8.3.5.1 Device Information

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.

8.3.5.2 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.

8.3.5.3 Restoring the Factory Defaults Settings

In some cases it may be necessary or wished to reset all settings of module 8029HEPTA to factory settings (factory defaults).

Factory Defaults

WARNING!
RESET to factory defaults is a critical action, all values will be set to default - the device will be rebooted immediately. Are you sure you want to reset to factory defaults now?

Reset now

This function serves to reset all values in the flash memory to their factory default values.

This also includes passwords (see **Chapter 13.1 Factory Default Values of Module 8029HEPTA (Device)**).

Please log in as a "Master" user in accordance with the description in **Chapter 8.2.1 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.



A **Factory Default** requires a complete check and optionally a new configuration of the Module 8029HEPTA. In particularly the default MASTER and DEVICE passwords should be reset.

8.3.5.4 Restarting the Module (Reboot Device)



The restart concerns the Module 8029HEPTA and the Sync Source (here Module 8024GPS).

Reboot Device

WARNING!

REBOOT is a critical action, all unsaved changes will be lost. Are you sure you want to reboot the device now?

Reboot now



All settings **not** saved with "Save" are lost on reboot (see **Chapter 8.2.3 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 8.2.1 LOGIN and LOGOUT as User**.

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

8.3.5.5 Image Update for Module 8029HEPTA (WebGUI: Device)

Patches and Bug Fixes are provided for the individual boards by means of updates.

The embedded image is loaded only via the web interface in the Time Server 8029HEPTA/GPS (log in as “master” user required). See also **Chapter 4.4 Firmware Update**.



The following points should be considered regarding updates:

- Only experienced users or trained technical personnel should carry out a board update after checking all necessary preconditions.
- Important: **Faulty updates** or **update attempts** may, under certain circumstances, require the module to be returned to the factory for repair at customer's expense.
- Is the update on hand suitable for the module? If there are any doubts 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**" on the Internet browser used.
- During the update procedure, the device **must not be switched off** nor **settings be saved to the flash memory!**
- Updates are **always** carried out as Software SETs. That means that all programmes included in the SET must be downloaded to the system.
- For the update pay attention to point described 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.):

8024A_128_v0100.mot

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

upgrade_8029-SER1_gen_rel_v0600.img

or upgrade_8029-NAND_gen_rel_v0800.img

for the **embedded image** (update takes approx. 2-3 minutes)

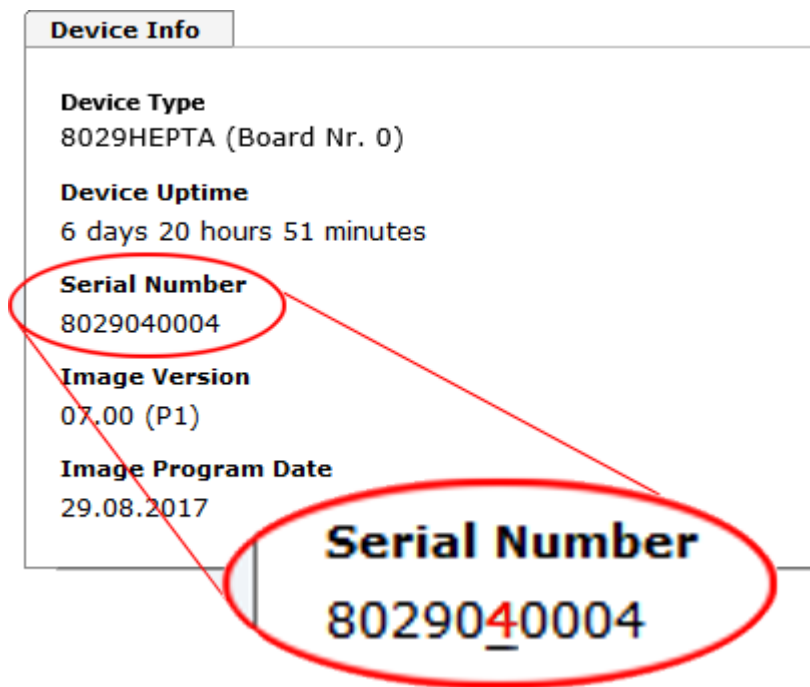
8.3.5.5.1 Select Image Update



ATTENTION

Important note for the identification of the required image update!

In order to select the correct image update, the **digit marked red** of the serial number must be checked!



Required ZIP archive for the Image Update:

Red marked digit = 1

Red marked digit = 4

hopf8029HEPTA-V2-SERI_GPS_SET_v06xx.zip

hopf8029HEPTA-V2-NAND_GPS_SET_v08xx.zip

Content of the ZIP archive

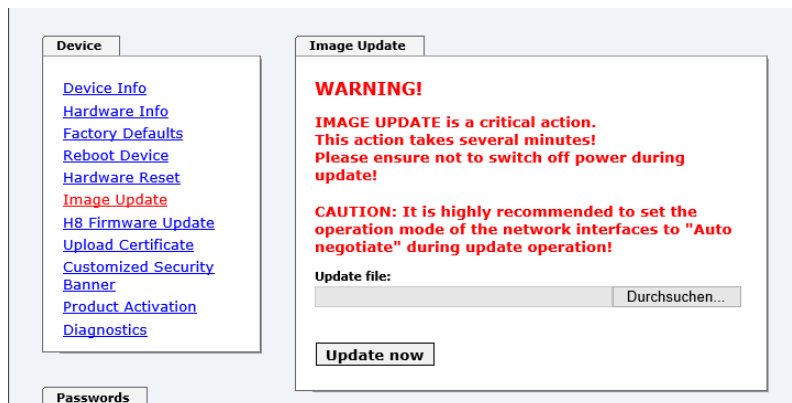
- 8024A_128_v01xx.mot
- 8029HEPTA-V2_128_v05xx.mot
- readme_8029HEPTA-V2-SERI_GPS.txt
- release-notes_8029HEPTA-V2-SERI_GPS.html
- upgrade_8029-SERI_gen_rel_v06xx.img

Content of the ZIP archive

- 8024A_128_v01xx.mot
- 8029HEPTA-V2_128_v05xx.mot
- readme_8029HEPTA-V2-NAND_GPS.txt
- release-notes_8029HEPTA-V2-NAND_GPS.html
- upgrade_8029-NAND_gen_rel_v08xx.img

8.3.5.5.2 Installation Image Update

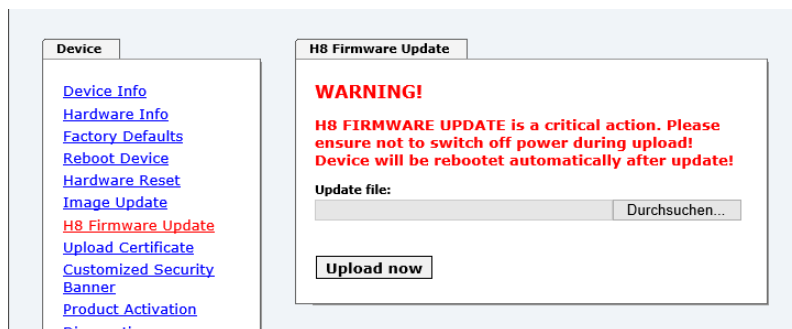
The update process is started by pressing the "**Update now**" button. The update is installed if the transfer and checksum test are successful. A success page is displayed and shows the number of bytes that have been transferred and installed.



After the image-update the WebGUI displays a window to confirm the reboot of the Time Server 8029HEPTA/GPS.

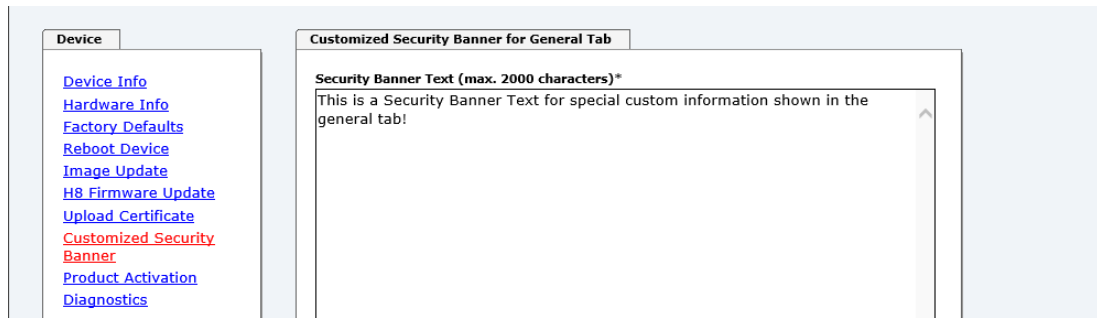
8.3.5.6 Upload von Anwender SSL-Server-Zertifikat (Upload Certificate)

Hiermit besteht die Möglichkeit die https-Verbindungen zum Gerät mit einem vom Anwender zur Verfügung gestellten SSL-Server-Zertifikat zu verschlüsseln.



8.3.5.7 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.

8.3.5.8 Product Activation

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



For a subsequent order of an activation key the serial number of the Module 8029HEPTA (device) needs to be provided. The serial number can be found under the tab DEVICE – Device info (serial number 8029...).



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

General
Network
NTP
Alarm
Device
GPS Sync Source

Device

[Device Info](#)
[Hardware Info](#)
[Factory Defaults](#)
[Reboot Device](#)
[Hardware Reset](#)
[Image Update](#)
[H8 Firmware Update](#)
[Upload Certificate](#)
[Customized Security Banner](#)
[Product Activation](#)
[Diagnostics](#)

Passwords

[Master Password](#)
[Device Password](#)

Downloads

[SNMP MIB](#)
[Configuration Files](#)

Overview

Feature	Status	Activation Key
SINEC H1 time datagram	Inactive	N/A
Static Routing Table	Inactive	N/A
Alarming and management features	Inactive	N/A
IEEE 802.1Q Tagged VLAN	Inactive	N/A

Activate Feature

Insert Activation Key

Key Reset

WARNING!

The activated features won't be available anymore after reset. If you want to reactivate this features you will have to enter the activation keys again.

Perform Key Reset now

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.

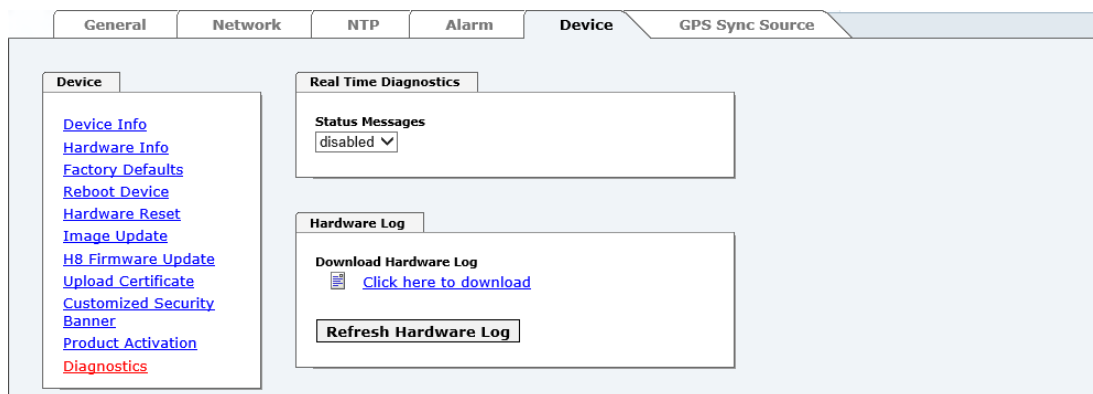
If the activation was successful the new feature is listed in the overview with status "Active" and can be used immediately.

Key Reset

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

8.3.5.9 Diagnostics Function

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



8.3.5.10 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 8.2.1 LOGIN and LOGOUT as User**)





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


8.3.5.11 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.


Configuration Files

Download NTP-Configurationfile
 [Click here to download](#)

Download NTP-Keyfile
 [Click here to download](#)

Download NTP Group-Key (IFF)
 [Click here to download](#)

Device Configuration

Download Device Configuration
 [Click here to download](#)

Download Sync Module Log
Sync Module Log not (yet) available

Refresh Device Configuration



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 8029HEPTA/GPS.




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. After approximately 30 seconds, the files are available for the download
4. Press on the link Configuration Files to update the web site
5. Perform the download of the file

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

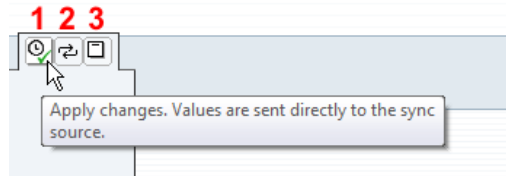
SNMP MIB

Download hopf8029HEPTA MIB
 [Click here to download](#)

8.3.6 GPS SYNC SOURCE Tab

The complete display and parameterization of the Sync Source (here Module 8024GPS) takes place in this tab.

The modified values in the tab GPS SYNC SOURCE are directly transferred to the Module 8024GPS (Sync Source) by pressing the button 1 and failsafe stored in Module 8024GPS. This behaviour is indicated on the modified display of the Apply button. The buttons 2 and 3 are without function in the tab GPS SYNC SOURCE and are not required.



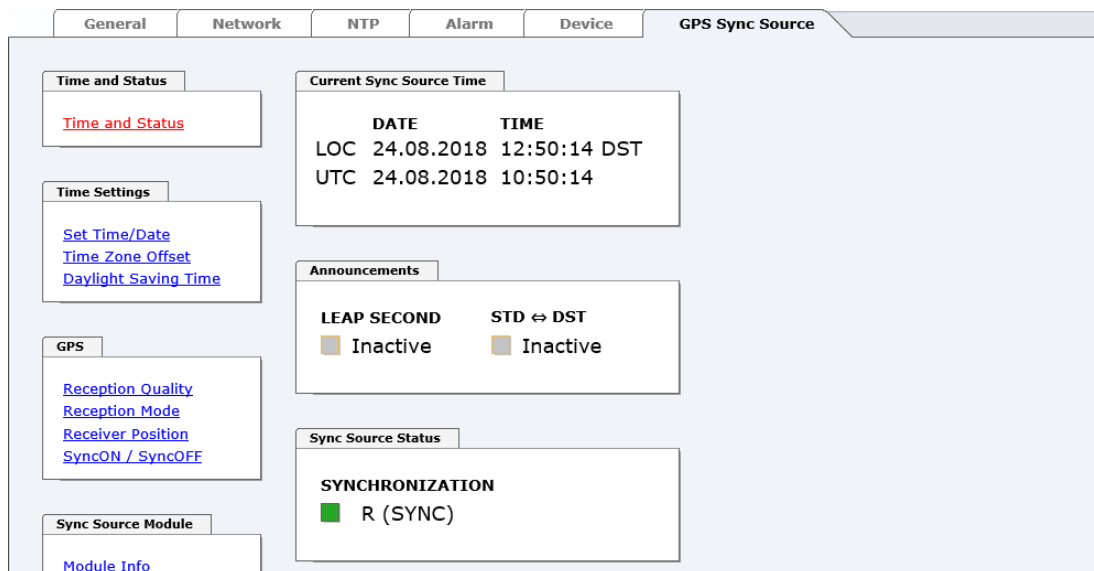
After the data transfer to 8024GPS it can take up to 30 seconds until the modified data are re-read from 8029HEPTA for the WebGUI indication.

This delayed indication has no effect on the functionality.



Generally it is recommended to perform a restart of the the Sync Source (here Module 8024GPS) with a **Module Reset** after performing all modifications. This ensures that the Module 8024GPS will be operated with the new and failsafe stored data.

8.3.6.1 Time and Status



The screenshot shows the 'GPS Sync Source' tab in the web GUI. The page is divided into several sections:

- General** (selected): Contains 'Time and Status' (with a red 'Time and Status' link), 'Time Settings' (with links for 'Set Time/Date', 'Time Zone Offset', and 'Daylight Saving Time'), 'GPS' (with links for 'Reception Quality', 'Reception Mode', 'Receiver Position', and 'SyncON / SyncOFF'), and 'Sync Source Module' (with a 'Module Info' link).
- Current Sync Source Time**: Displays the current time for LOC (24.08.2018 12:50:14 DST) and UTC (24.08.2018 10:50:14).
- Announcements**: Shows 'LEAP SECOND' and 'STD ⇌ DST' both as 'Inactive'.
- Sync Source Status**: Shows 'SYNCHRONIZATION' status as 'R (SYNC)' with a green square icon.

Current Sync Source Time

This area indicates the current 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 corresponding 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

8.3.6.2 Set Sync Source Time

Adjustment of UTC including the date in the Sync Source (here Module 8024GPS)

After entering the plausibility of these values are directly checked by clicking on the **Apply** button and then sent to the Sync Source (here Module 8024GPS).



Always the UTC time must be set. The local time is internally calculated from the difference time (Time Zone Offset) and the summer / winter time changeover (Daylight Saving Time).

General

Network

NTP

Alarm

Device

GPS Sync Source

Time and Status

Time Settings

Time and Status

[Set Time/Date](#)
[Time Zone Offset](#)
[Daylight Saving Time](#)

Set UTC Time/Date

Year (YYYY)

Month (MM)

Day (dd)

Hour (hh)

Minute (mm)

Second (ss)

- **Year** Input of the current UTC year (2000-2099)
- **Month** Input of the current UTC month (01-12)
- **Day** Input of the current UTC day (01-31)
- **Hour** Input of the current UTC hour (00-23)
- **Minute** Input of the current UTC minute (00-59)
- **Second** Input of the current UTC second (00-59)



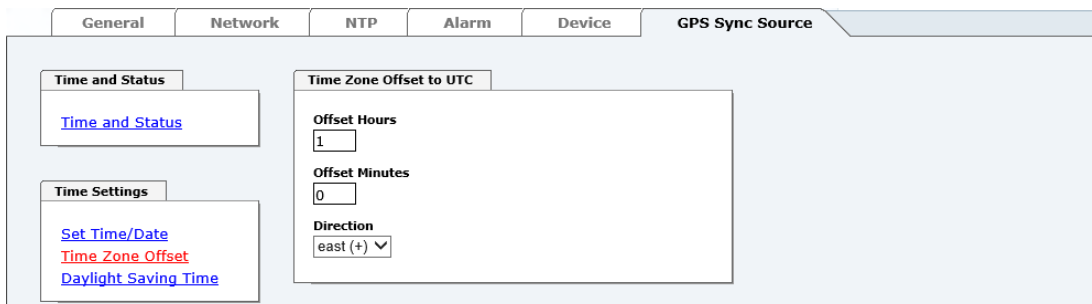
The input must be complete and according to the stated format.

8.3.6.3 Time Zone Offset

Setting of the difference time (Time Zone Offset) from UTC to the local standard time (winter time) in the Sync Source (here Module 8024GPS)



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



The screenshot shows the 'GPS Sync Source' configuration page. On the left, there are two sections: 'Time and Status' with a link 'Time and Status', and 'Time Settings' with links 'Set Time/Date', 'Time Zone Offset', and 'Daylight Saving Time'. The main area is titled 'Time Zone Offset to UTC' and contains three input fields: 'Offset Hours' with the value '1', 'Offset Minutes' with the value '0', and a 'Direction' dropdown menu currently showing 'east (+)'.

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

Example:

Time Offset for Germany ⇒ East, 1 hour and 0 minutes (+ 01:00)

Time Offset for Peru ⇒ West, 5 hours and 0 minutes (- 05:00)

Direction relating to Prime Meridian – Direction of the Difference Time

Entering the direction the local time deviates from world time:

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

8.3.6.4 Daylight Saving Time (DST)

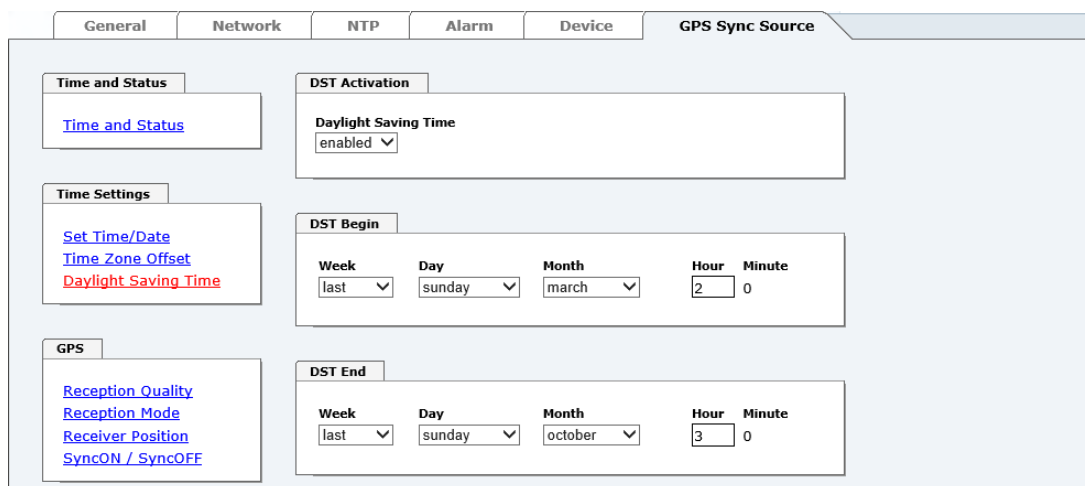
Setting of the changeover times for summer/winter time in the Sync Source (here Module 8024GPS).

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

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



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



The screenshot shows the 'GPS Sync Source' configuration page with tabs for General, Network, NTP, Alarm, Device, and GPS Sync Source. The 'GPS Sync Source' tab is active, showing sections for Time and Status, Time Settings, and GPS. The 'DST Activation' section has a dropdown set to 'enabled'. The 'DST Begin' section shows settings for Week (last), Day (sunday), Month (march), Hour (2), and Minute (0). The 'DST End' section shows settings for Week (last), Day (sunday), Month (october), Hour (3), and Minute (0).

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

The individual items have the following meanings:

Week	At which occurrence of that particular weekday in that month the changeover is going to take place.	First - 1st week Second - 2nd week Third - 3th week Fourth - 4th week Last - last week
Day	The day of the week when the changeover should be processed	Sunday, Monday ... Saturday
Month	the month when the changeover should be processed	January, February ... December
Hour Minute	The time in hour and minute when the changeover should be processed	00h ... 23h 00min ... 59min



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

8.3.6.5 Reception Quality

In this tab following information is indicated with read-only access:

Satellites in View

Number of available satellites detected by the GPS receiver.

Satellites Tracked

Effective number of received satellites used for synchronization.

Satellites Number – S/N Ratio

Overview of actually received GPS satellites with their number and reception quality and the pertinent interpretation.

Green	≥ 48	Good reception quality
Yellow	31-47	Sufficient reception quality
Red	0-30	Poor reception quality

Receiver Status

Display of the actual GPS receiver values. For analysing the GPS receiver in case of support.

General
Network
NTP
Alarm
Device
GPS Sync Source
Output

Time and Status
[Time and Status](#)

Time Settings
[Set Sync Source Time](#)
[Time Zone Offset](#)
[Daylight Saving Time](#)

GPS
[Reception Quality](#)
[Reception Mode](#)
[Receiver Position](#)
[SyncON / SyncOFF](#)

Sync Source Module
[Module Info](#)
[Module Reset](#)
[Factory Default](#)
[H8 Firmware Update](#)
[Sync Source Errors](#)

Sync Status OC
[Sync Status OC](#)

Reception Quality

Satellites in View
12
Satellites Tracked
9

SAT	S/N RATIO	BAD	SUFFICIENT	GOOD
5	87	██████████	██████████	██████████
7	87	██████████	██████████	██████████
30	84	██████████	██████████	██████████
2	75	██████████	██████████	██████████
13	75	██████████	██████████	██████████
9	66	██████████	██████████	██████████
20	57	██████████	██████████	██████████
6	36	██████████	██████████	
16	30	██████████		

GPS reception quality values are refreshed automatically every 5 seconds.

Receiver Status

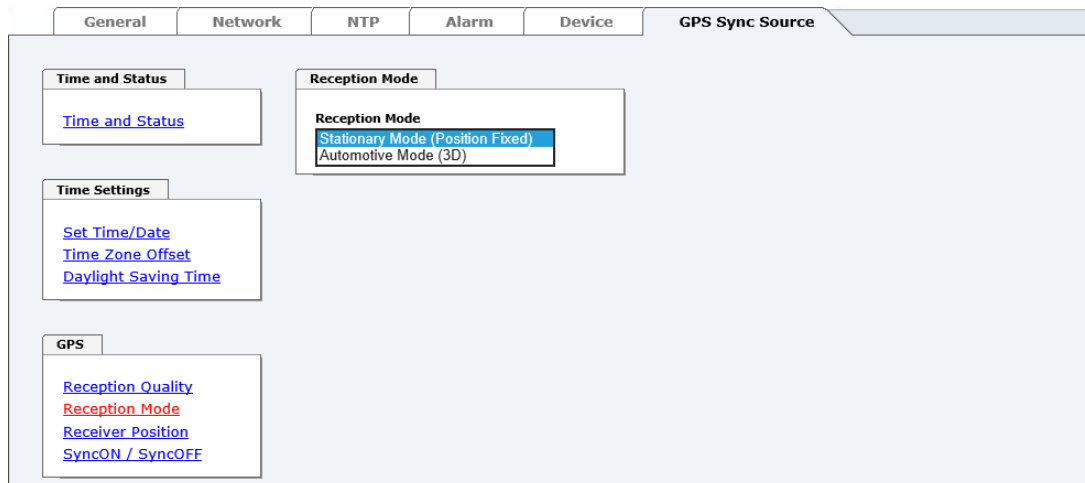
AGC Monitor
16.9 %
Noise Level
132
CW Jamming Indicator
5.9 %
Jamming Status
ok
PDOP
1.63



This page is updated automatically every 5 seconds.

8.3.6.6 Reception Mode

In this tab the GPS reception mode is adjusted and displayed. The accuracy of the time evaluation is defined by the exact position calculation of the installation site. For this calculation (3D evaluation) it is necessary to receive information from at least four (4) satellites. The signal runtime to several satellites is determined from the calculated position and the precise second mark is generated from their mean value.



The screenshot shows the 'GPS Sync Source' configuration page with the 'Reception Mode' tab selected. The 'Reception Mode' section contains two options: 'Stationary Mode (Position Fixed)' and 'Automotive Mode (3D)'. The 'Stationary Mode (Position Fixed)' option is currently selected and highlighted in blue. The left sidebar contains links for 'Time and Status', 'Time Settings', and 'GPS'.

Stationary Mode (Position Fixed) – Standard operation

In Stationary Mode (Fixed position), the GPS receiver calculates its accuracy based on a fixed position. If four or more satellites are received in this mode, the exact location is updated automatically.

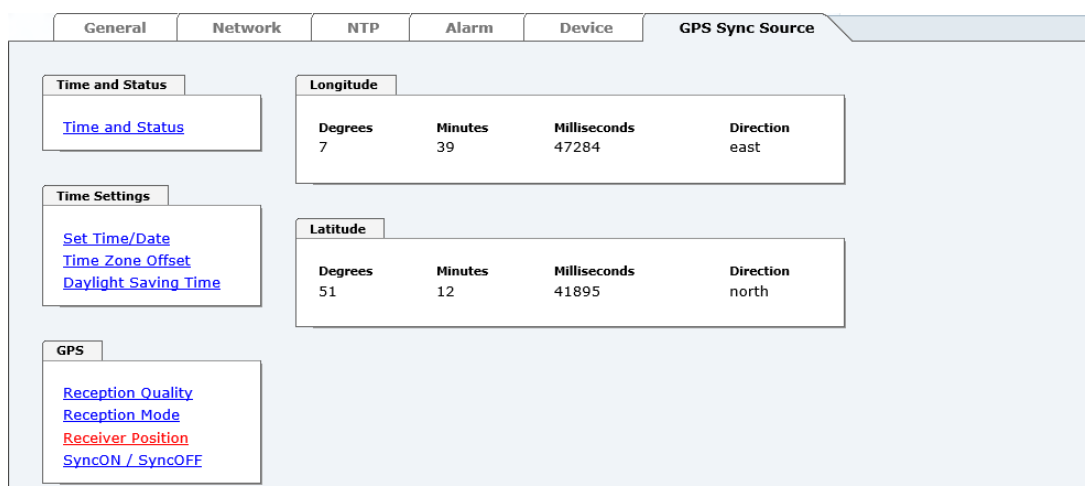
In this mode, a synchronization with a changing position is not possible.

Automotive (3D)

The automotive (3D) mode allows the use of system 8029NTS at mobile locations (except aircraft).

8.3.6.7 Receiver Position

In this tab the current position is adjusted and displayed.



The screenshot shows the 'GPS Sync Source' configuration page with the 'Receiver Position' tab selected. The 'Longitude' and 'Latitude' sections display the current position. The 'Longitude' section shows: Degrees 7, Minutes 39, Milliseconds 47284, and Direction east. The 'Latitude' section shows: Degrees 51, Minutes 12, Milliseconds 41895, and Direction north. The left sidebar contains links for 'Time and Status', 'Time Settings', and 'GPS'.

Longitude / Latitude – Current Position with Longitude and Latitude

Display of the actual position calculated by the GPS receiver.

8.3.6.8 SyncON / SyncOFF

General	Network	NTP	Alarm	Device	GPS Sync Source				
<div> <div> Time and Status Time and Status </div> <div> Time Settings Set Time/Date Time Zone Offset Daylight Saving Time </div> <div> GPS Reception Quality Reception Mode Receiver Position SyncON / SyncOFF </div> </div>									
<div> SyncON / SyncOFF Timer <table border="1"> <tbody> <tr> <td> SyncON timer (0-30 min) <input type="text" value="0"/> </td> <td> Current SyncON timer value 0 </td> </tr> <tr> <td> SyncOFF timer (2-1440 min) <input type="text" value="55"/> </td> <td> Current SyncOFF timer value 0 </td> </tr> </tbody> </table> <p>Please note: Current Sync Timer values are not refreshed automatically!</p> </div>						SyncON timer (0-30 min) <input type="text" value="0"/>	Current SyncON timer value 0	SyncOFF timer (2-1440 min) <input type="text" value="55"/>	Current SyncOFF timer value 0
SyncON timer (0-30 min) <input type="text" value="0"/>	Current SyncON timer value 0								
SyncOFF timer (2-1440 min) <input type="text" value="55"/>	Current SyncOFF timer value 0								

SyncON Timer

The SyncON timer is used to delay the sync-status “SYNC” by the set time although the GPS receiver is 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 device and should always be set to 0.

SyncOFF Timer

This value is used to provide reception failure bypassing for an error-message free operation even under poor reception conditions.

In the event of a reception failure of the Sync Source (here Module 8024GPS), the decrease of the Sync Source to **quartz** status is delayed by the set value. The system continues to run in synchronization status on the internally regulated, highly accurate quartz base during this period with sync status '**SYOF**'.

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.

8.3.6.9 Module Info

General	Network	NTP	Alarm	Device	GPS Sync Source
<div> <div> Time and Status Time and Status </div> <div> Time Settings Set Time/Date Time Zone Offset Daylight Saving Time </div> <div> GPS Reception Quality Reception Mode Receiver Position SyncON / SyncOFF </div> <div> Sync Source Module Module Info Module Reset Factory Default H8 Firmware Update Sync Source Errors </div> </div> <div> Module Info <p>Device Type 8024</p> <p>Device Version 0</p> <p>Card Layout 0</p> <p>Serial Number 8024010372</p> <p>Com. No. 9999999999</p> <p>H8 Firmware Version 01.01 (27.04.16)</p> <p>MACH Firmware Version 10</p> <p>Special Program 0</p> <p>Unlocked Features FE01</p> <p>Product-Config-ID 01802401037200000029999999999010127041600000010FE0101012704160010</p> </div>					

This tab indicates information about the hardware and software of the Module 8024GPS (Sync Source) implemented in the Time Server 8029HEPTA/GPS.



These details might be provided for service and support purposes.

8.3.6.10 Module Reset

Module Reset

WARNING!

MODULE RESET is a critical action, synchronization will be lost. Are you sure you want to reset the module now?

Perform Reset now

This function triggers a hardware reset of (just) the Sync Source (here Module 8024GPS).



This function has no effect on the failsafe stored data.

8.3.6.11 Factory Default

Factory Default

WARNING!

RESET to factory defaults is a critical action, all synchronization settings will be lost. Are you sure you want to reset the system to factory defaults now?

Perform Reset now



After setting the Sync Source to factory default values the GPS receiver needs up to 13 minutes of satellite reception in order to generate the correct information on the leap second from the GPS data. Only then the Sync Source (here Module 8024GPS) can be synchronized.

During this time (however only when the GPS receiver really receives satellites) the following message is displayed in the tab **Module Errors**:

GPS Receiver in raw data mode - no synchronisation



If the changeover times for summer/winter time and the difference time are not initial set after a factory default of the Sync Source (here Module 8024GPS) the following message is displayed in the tab **Module Errors**:

Missing data for Time Zone Offset

and/or

Missing or incomplete data for daylight saving time (DST)

8.3.6.12 H8 Firmware Update (Sync Source)

Patches and Bug Fixes are provided for the Time Server 8029HEPTA/GPS by means of updates.

The H8 update of the Sync Source is loaded only via the web interface in the Time Server 8029HEPTA/GPS (log in as "master" user required). See also **Chapter 4.4 Firmware Update**.



The following points should be considered regarding updates:

- Only experienced users or trained technical personnel should carry out a board update after checking all necessary preconditions.
- Important: **Faulty updates** or **update attempts** may, under certain circumstances, require the module to be returned to the factory for repair at customer's expense.
- Is the update on hand suitable for the module? If there are any doubts 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**" on the Internet browser used.
- During the update procedure, the device **must not be switched off** nor **settings be saved to the flash memory!**
- Updates are **always** carried out as Software SETs. That means that all programmes included in the SET must be downloaded to the system.
- For the update pay attention to point described 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.

A correct image designation is (e.g.):

8024_128_v0400.mot

for **H8 Firmware**

(Update takes approx. 1-1.5 minutes)

H8 Firmware Update

WARNING!
H8 FIRMWARE UPDATE is a critical action. Please ensure not to switch off power during upload!
Device will be rebooted automatically after update!

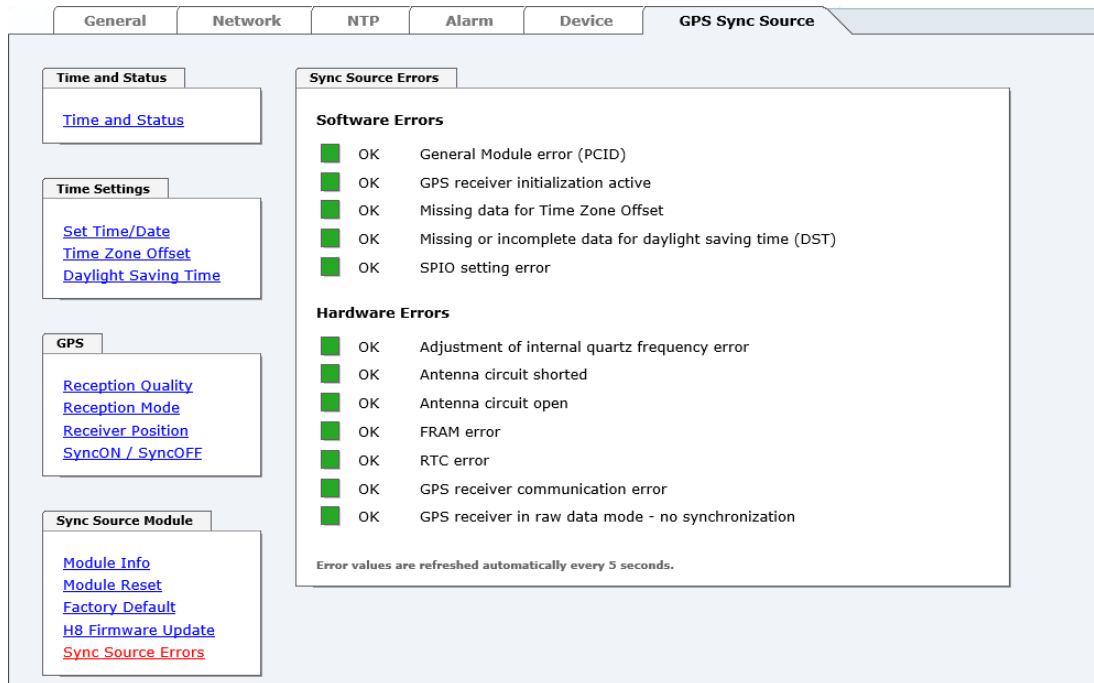
Update file:

8.3.6.13 Module Errors

This tab displays the current failure status of the Sync Source (here Module 8024GPS):



If a collected error message is displayed in the GENERAL tab, there is at least one error (Sync Source Error).



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

Time and Status
[Time and Status](#)

Time Settings
[Set Time/Date](#)
[Time Zone Offset](#)
[Daylight Saving Time](#)

GPS
[Reception Quality](#)
[Reception Mode](#)
[Receiver Position](#)
[SyncON / SyncOFF](#)

Sync Source Module
[Module Info](#)
[Module Reset](#)
[Factory Default](#)
[H8 Firmware Update](#)
[Sync Source Errors](#)

Sync Source Errors

Software Errors

- OK General Module error (PCID)
- OK GPS receiver initialization active
- OK Missing data for Time Zone Offset
- OK Missing or incomplete data for daylight saving time (DST)
- OK SPIO setting error

Hardware Errors

- OK Adjustment of internal quartz frequency error
- OK Antenna circuit shorted
- OK Antenna circuit open
- OK FRAM error
- OK RTC error
- OK GPS receiver communication error
- OK GPS receiver in raw data mode - no synchronization

Error values are refreshed automatically every 5 seconds.



This page is updated automatically every 5 seconds.

Overview Software Errors

- **General Module error (PCID)**
If this error occurs even after a Power down, the device is damaged.
- **GPS receiver initialization active**
This condition might last for max. 1 minute after particular actions.
- **Missing data for Time Zone Offset**
Difference time (Time Zone Offset) must be an initial entry by the user.
Otherwise there is no synchronization of the Sync Source (here Module 8024GPS).

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

The switchover times for summer/winter time must be initially set / disabled by the user.

Otherwise there is no synchronization of the Sync Source (here Module 8024GPS).

- **SPIO setting error**

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

Overview Hardware Errors

- **Adjustment of internal quartz frequency error**

Problems with the internal quartz regulation of the Sync Source (here Module 8024GPS) have occurred. So the specified accuracy of the Sync Source cannot be guaranteed anymore.

- **Antenna circuit shorted**

The Sync Source (here Module 8024GPS) has detected a short circuit in the antenna system. The antenna system should be checked.

- **Antenna circuit open**

The Sync Source (here Module 8024GPS) has detected an open antenna input. The antenna system should be checked.

- **FRAM error**

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

- **RTC error**

If this error with set or synchronized time (not sync.-status INVA) and a successive reset of the sync. source still maintains the internal backup clock may be defective.

- **GPS receiver communication error**

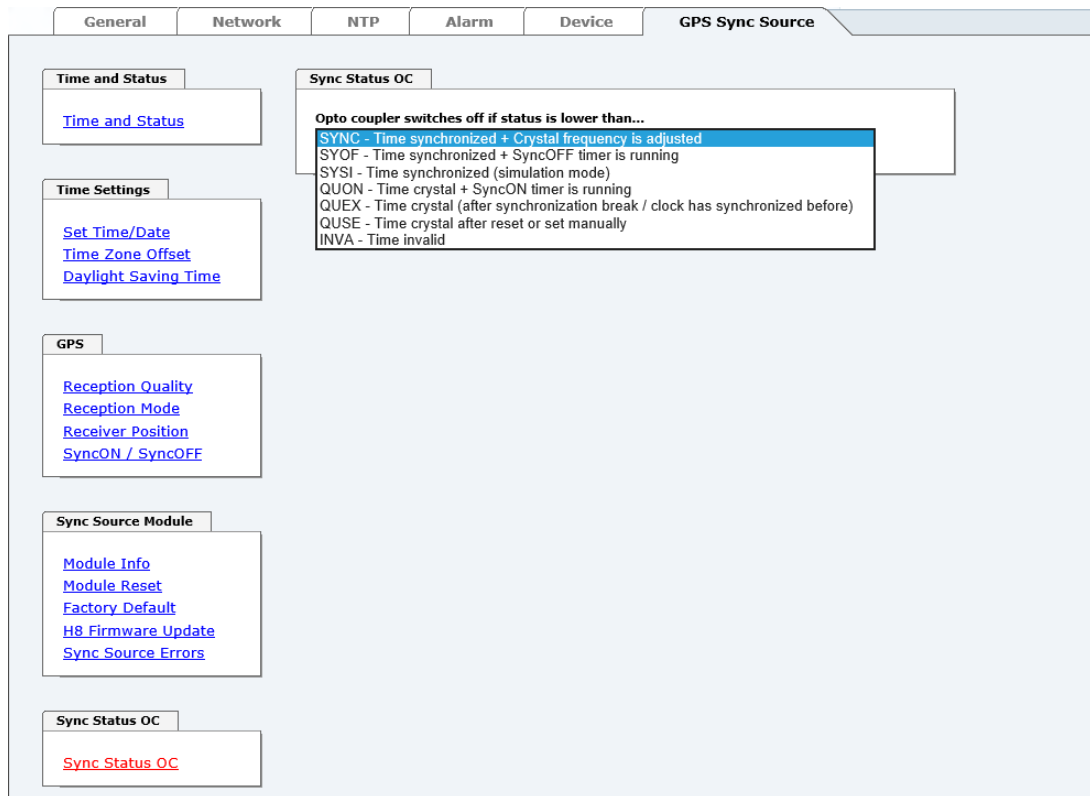
If this error occurs even after a Power-Reset, the support team of company **hopf** needs to be contacted for further actions.

- **GPS receiver in raw data mode – no synchronization**

If this condition is indicated, the GPS receiver requires special data from the GPS signal for which it needs up to 13 minutes signal reception of satellites. Only then the Sync Source (here Module 8024GPS) can be synchronized.

This happens e.g. after resetting the Sync Source parameters to factory default values.

8.3.6.14 Sync Status OC



The output of the status optical coupler (on the back panel of the Time Server 8029HEPTA/GPS) can be configured by the use of this function.

The Sync states are listed in this selection window in rising quality from the bottom to the top (**SYNC** = optimal condition).

Behaviour of Optical Coupler:

- Selected status achieved or better – Optical coupler switched through
- Selected status not achieved – Optical coupler blocked

Value range

Optical Coupler Status	SYNC	Time synchronized + Quartz regulation started/running
	SYOF	Time synchronized + SyncOFF running
	YSI	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

9 SSH and Telnet Basic Configuration



Only basic configuration is possible via SSH or Telnet. The complete configuration of the Time Server 8029NTS/GPS 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.

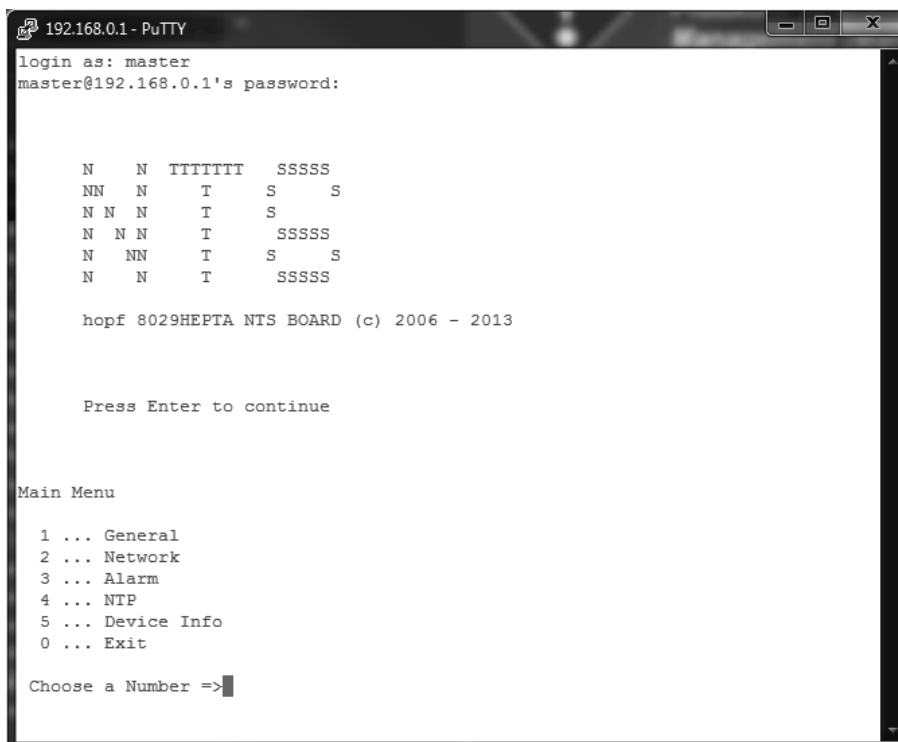
The user names and passwords are the same as on the WebGUI and are kept in alignment (see **Chapter 8.3.5.10 Passwords (Master/Device)**).



SSH does not allow blank passwords for safety reasons.



The corresponding protocols should be enabled for the use of Telnet or SSH (see **Chapter 8.3.2.5 Management (Management-Protocols – HTTP, SNMP)**).



```

192.168.0.1 - PuTTY
login as: master
master@192.168.0.1's password:

  N  N  TTTTTT  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 8029HEPTA 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).

10 Fault Analysis / Troubleshooting

This chapter explains different error patterns and the process to contact the **hopf** support team.

10.1 Error Patterns

This chapter describes various error patterns which enable the customer to make a preliminary problem analysis. In addition they also provide assistance in describing the error when contacting the **hopf** support.



If possible, for each problem the entire status in the tabs **GENERAL** and **GPS SYNC SOURCE** page "**Module Errors**" via WebGUI should always be checked.

10.1.1 Complete Failure

Description

- The Status LEDs on the front panel are off

Cause / Problem Solution

- Device is switched off
- Voltage supply failure
- Power supply defective

10.1.2 No GPS Reception / No Synchronization

Description

- In WebGUI the status of the SYNC SOURCE is **not** displayed with **SYNC** or **SYOF**
- The Status LEDs of Module 8024GPS on the front panel do not indicate **SYNC** or **SYOF** status

Cause / Problem Solution

- System was not correctly/completely initialized

The following describes various effects and their possible causes on a non-synchronizing system:

Case 1:

Effect: After the first installation, no satellite appears on the display after several hours and **0** is displayed under **Satellites in View**.

Possible Errors:

- The antenna cable is too long
- An incorrect cable type was used for the length of the antenna equipment
- The antenna cable is faulty
- The antenna cable is not connected
- The antenna is defective
- The indirect lightning protection is defective

Case 2:

Effect: There are 7 satellites in the visibility range (**V=07**) but a maximum of 2 appear on the display frame. However, the value of these satellites is 30 or above.

Possible Errors:

- The visibility range of the antenna to the sky is limited.

Case 3:

Effect: There are 9 satellites in the visibility range (**V=09**) and 6 appear on the display frame. The signal/noise ratios are all below 30. The equipment is not synchronized.

Possible Errors:

- The cable is too long
- An incorrect cable type was used for the length of the antenna equipment
- The BNC connectors are poorly mounted
- The cable is bent or crimped
- Indirect lightning protection was irreversibly damaged by overvoltage
- The antenna is defective

Case 4:

Effect: The equipment was working perfectly but has not been receiving for several days. 7 satellites appear in the visibility range (**V=07**) but no satellite is displayed.

Possible Errors:

- The cable has been damaged
- There was excess voltage on the antenna equipment and the indirect lightning protector is defective
- The antenna is defective
- The GPS receiver of Module 8024GPS is defective
- A building change has had an effect on the antenna equipment (e.g. shading of the antenna caused by subsequent building installation, or the laying of cables with a high electrical alternating field in the immediate vicinity of the GPS antenna cable)
- Electronic equipment with an interference effect on the GPS signal has been put into operation in the vicinity of the GPS antenna equipment / GPS receiver (e.g. transmitter for pagers)

Further information on the subject of the GPS antenna system can be consulted in the manual "Antenna Equipment GPS".

10.1.3 No Daylight Saving Time / Summer Time Switchover

Description

- There is no "DST" for "daylight saving time" (summer time) displayed in the Sync Source time in WebGUI
- Summer time is not considered in outputs working with it and even in case of availability.

Cause / Problem Solution

- Changeover times are not set
- Parameterization failure

10.2 Support by Company **hopf**

Should the system show any other failures than listed in **Chapter 10.1 Error Patterns**, please contact the support of company **hopf** Elektronik GmbH by providing an exact failure description and the following information:



If possible, for each problem the **Configuration File** in the tab **DEVICE** should be downloaded from the device and be sent to the **hopf** support (see **Chapter 8.3.5.11 Downloading Configuration Files / SNMP MIB**).

- With the file **System Configuration** or if not possible with the serial number of the System
- When does the error occur: During commissioning or operation
- Exact error description
- In the case of GPS reception/synchronization problems ⇒ description of the antenna equipment used:
 - Components used (antenna, indirect lightning protection, etc.)
 - Cable type used
 - Total length of the antenna system
 - Sequence of components and cable lengths between the components
 - Antenna installation site (e.g. signal shading by building)

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

support@hopf.com



Providing a detailed error description and above listed information avoid the need for additional clarification and leads to a faster processing by the support team.

11 Maintenance

The Time Server 8029HEPTA/GPS is generally maintenance-free. The following points should be observed if a cleaning of the system might be necessary.

11.1 General Guidelines for Cleaning

The following **must not** be used to clean the Time Server 8029HEPTA/GPS:

- Fluids
- Cleaning agents containing solvents
- Cleaning agents containing acids
- Abrasive media

The use of such cleaning agents or media could damage the Time Server 8029HEPTA/GPS.



Do not use a wet cloth to clean the Time Server 8029HEPTA/GPS.

There is the danger of an electric shock.

To clean the Time Server 8029HEPTA/GPS use a cloth that is:

- Antistatic
- Soft
- Non-fabric
- Damp

11.2 Cleaning the Housing



Make sure that connections or cables are not loosened while cleaning the housing of the Time Server 8029HEPTA/GPS. There is the danger of damage and functionality loss.

11.3 Cleaning the Display and Front Panel

Minimum pressure should be exerted when cleaning the display and push button. Excessive pressure may cause mechanical damage.

12 Technical Data



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

12.1 General – 8029HEPTA/GPS

General Data – System 8029HEPTA/GPS	
Housing design:	Sheet steel / Aluminium, closed
Housing dimensions:	See Chapter 2.1 19 inch Rack 1U/84HP (Slim Line)
Protection type of the housing:	IP20
Protection class:	I, with PE connection. Additional earth screw for cables up to 16mm ²
Cooling:	Passive, ventilation slots left / right
Weight:	Approx. 3kg

AC Power Supply (with wide input range)	
Nominal input voltage:	100-240V AC / 47-63Hz Connection via input connector compliant with IEC/EN 60320-1/C14 with EMI line filter and switch
Input voltage range:	85-264V AC
Frequency:	47-63Hz
Current consumption (at nominal values):	Approx. 0.37A (120V AC) / 0.23A (230V AC)
Starting current:	Typ. 15A (I _o = 100%) 120V AC Typ. 30A (I _o = 100%) 230V AC
Mains failure bridging at nominal load:	> 20msec. (> 100V AC)
Turn-on time after application of mains voltage:	< 500msec.
Transient overvoltage protection:	Overvoltage category II (EN 60664-1)
Input fuse - internal:	2A (equipment protection)
Recommended pre-fuse:	Line protection switch 6A, 10A characteristic B (EN 60898)
PE leakage current:	< 0.75mA (60Hz, compliant with EN 60950)
Insulation voltage input / PE:	2000V AC, 1 minute, residual current = 10mA, 500V DC, 50MΩ at least (at room temperature)
Output Data (internal only)	
Internal nominal output voltage:	5V DC
Nominal output current I _N 0°C .. +55°C:	3A (U _{OUT} = 5V DC)
Efficiency:	> 74% (at 230V AC and nominal values)

DC Power Supply (Option)			
Nominal input voltage:	24V DC	48V DC	110/220V DC
Input voltage range:	18-36V DC	36-76V DC	100-250V DC
Current consumption (at nominal values):	0.69A	0.35A	0.40A
Turn-on time after application of mains voltage:	< 200msec.	< 200msec.	< 500msec.
Input fuse - internal (equipment protection):	2A fast-acting	1A fast-acting	2A
Insulation voltage input / output:	1.500V DC 1 minute, 500V DC 50M Ω at least (20°C \pm 15°C)	1.500V DC 1 minute, 500V DC 50M Ω at least (20°C \pm 15°C)	2000V AC, 1 Minute, residual current = 10mA, 500V DC, 50M Ω at least (at room temp.)

Output Data (internal only)			
Internal nominal output voltage:	5V DC	5V DC	5V DC
Nominal output current I _N 0°C ... +55°C	3A (U _{OUT} = 5V DC)	3A (U _{OUT} = 5V DC)	3A (U _{OUT} = 5V DC)
Efficiency:	> 90%	> 90%	> 74%

Ambient Conditions		
Temperature range:	Operation:	0°C to +55°C
	Storage:	-20°C to +75°C
Humidity:	max. 95%, non condensing	

CE Conformity	
EMV Directive 2014/30/EU	
EN 55022 : 2010 / AC : 2011	
EN 61000-3-2 : 2006 / A2 : 2009, EN 61000-3-3 : 2013	
EN 55024 : 2010	
Low Voltage Directive 2014/35/EU	
EN 60950-1 : 2006 / AC : 2011	

MTBF	
MTBF	> 250,000h

Power Consumption - internal	
Normal operation	Typical: 750mA (max. 1000mA) at 5V DC
Boot phase	Typical: 750mA (max. 1000mA) at 5V DC

12.2 Module 8029HEPTA

LAN - ETH0	
Network connection	Via a LAN cable with RJ45 connector, male (recommended cable type CAT5 or better)
Request per second	Max. 1000 requests
Number of connectable Clients	Theoretically unlimited
Network interface ETH0	10/100 Base-T
Ethernet compatibility	Version 2.0 / IEEE 802.3
Isolation voltage (Network- to system side)	1500 Vrms

GPS-System - Accuracy		
Lambda < 15ms and Stratum 1-15	Stability: < 0,2ppm	HIGH
Lambda < 15ms and Stratum 1-15	Stability: 0,2ppm to 2ppm, Offset < 1ms	HIGH
Lambda < 15ms and Stratum 1-15	Stability: > 2ppm or Offset >= 1ms	MEDIUM
Lambda >= 15ms or Stratum 16	---	LOW
DCF77-System – Accuracy		
Lambda < 15ms and Stratum 1-15	Stability: < 0,6ppm	HIGH
Lambda < 15ms and Stratum 1-15	Stability: 0,6ppm to 2ppm, Offset < 2ms	HIGH
Lambda < 15ms and Stratum 1-15	Stability: > 2ppm or Offset >= 2ms	MEDIUM
Lambda >= 15ms or Stratum 16	---	LOW

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
- External LAN configuration tool (**hmc – Network-Configuration-Assistant**)

12.3 Module 8024GPS

Accuracy	
Internal PPS pulse on GPS reception (after 5min. continuous GPS reception):	<u>Standard Quartz:</u> < $\pm 30\text{ns}$ <u>VCTCXO:</u> < $\pm 15\text{ns}$
VCO control of the internal quartz base (after 5 min continuous GPS reception):	<u>Standard Quartz:</u> < $\pm 0.030\text{ppm}$ <u>VCTCXO:</u> < $\pm 0.015\text{ppm}$
Freewheel accuracy:	Standard Quartz: < $\pm 0.1\text{ppm}$ after at least 5min. GPS reception/ $T = +20^\circ\text{C}$ Drift for $T = +20^\circ\text{C}$ (constant): - after 1h: 0.36msec. - after 24h: 8.64msec. <u>VCTCXO:</u> < $\pm 0.02\text{ppm}$ after at least 5min. GPS reception/ $T = +20^\circ\text{C}$ Drift for $T = +20^\circ\text{C}$ (constant): - after 1h: 0.72msec. - after 24h: 1.73msec.
Internal back-up clock (RTC):	$\pm 25\text{ppm}$ / for $T = +10^\circ\text{C}$ to $+50^\circ\text{C}$

GPS Data	
Receiver type:	22 channel phase tracking receiver, C/A code
Evaluation:	L1 frequency (1575.42MHz)
Sensitivity:	Tracking: -161dB Cold Start: -148dBm
Synchronization time TTF (Time to First Fix):	<ul style="list-style-type: none"> • Warm start: < 1min. • Cold start: < 5min • first installation < 12.5 min (without valid leap second information)
Antenna connection:	<ul style="list-style-type: none"> • Via BNC connector, female • For active antennas, $U_b = 5\text{V DC}$ • Antenna power feed via BNC connector, female of Module 8024GPS

Signal Outputs	
Status optical coupler:	Via 3-pole pluggable screw terminal Resistive circuit-breaking capacity: max. 50mA / 80V DC

Special production:

Modifications can be made to hardware and software in accordance with customer specifications.



The **hopf** Company reserves the right to modify hardware and software at any time.

13 Factory Defaults of Time Server 8029HEPTA/GPS

This chapter lists the factory default values of the individual components integrated in the Time Server 8029HEPTA/GPS.

13.1 Factory Default Values of Module 8029HEPTA (Device)

The default delivery status of the Time Server 8029HEPTA/GPS meets the factory default values when using GPS synchronization sources. In case of DCF77 synchronization (different product variant) the function **"NTP / General / Sync Source"** is factory-set to **"DCF77"** on delivery.



Using the board in DCF77 systems (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	GPS	GPS

13.1.1 Network

Host/Name Service	Setting	WebGUI
Hostname	hopf8029HEPTA	hopf8029HEPTA
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
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
System Location	Blank	---
System Contact	Blank	---

Read Only Community	public	public
Read/Write Community	secret	secret
Security Name	Blank	---
Access Rights	Readonly	Readonly
Authentication Protocol	MD5	MD5
Authentication Passphrase	Blank	---
Privacy Protocol	DES	DES
Privacy Passphrase	Blank	---
Time	Setting	WebGUI
NTP	Enabled	Enabled
DAYTIME	Disabled	Disabled
TIME	Disabled	Disabled
SINEC H1 time datagram	Setting	WebGUI
Send Interval	Every second	1 second
Time base	UTC	UTC
Destination MAC Address	09:00:06:03:FF:EF	09:00:06:03:FF:EF
Minimum Accuracy	LOW	LOW

13.1.2 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 no modify
NTP Symmetric Keys	Setting	WebGUI
Request Key	Blank	---
Control Key	Blank	---
Symmetric Keys	Blank	---
NTP Autokey	Setting	WebGUI
Autokey	Disabled	Disabled
Password	Blank	---

13.1.3 ALARM

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

13.1.4 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

13.2 Factory Default Values of Module 8024GPS (Sync Source)

After triggering a factory default of Module 8024GPS two steps are carried out.

1. Deleting the current leap second information in the GPS receiver

2. Following parameters are set to default values:

Difference time	00h 00min east
Changeover times: Begin of Daylight Saving Time:	disabled Week <input type="checkbox"/> first Day <input type="checkbox"/> Monday Month <input type="checkbox"/> January Hour <input type="checkbox"/> 0
End of Daylight Saving Time:	Week <input type="checkbox"/> first Day <input type="checkbox"/> Monday Month <input type="checkbox"/> January Hour <input type="checkbox"/> 0
SyncON / SyncOFF Timeout:	0000 / 0055 (minutes)
GPS Position: Longitude: Latitude:	E 000° 00' 0000 N 00° 00' 0000
GPS reception mode:	Position Fixed
Sync Status OC:	SYNC

14 Glossary and Abbreviations

14.1 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.

14.2 Tally Codes (NTP-specific)

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

14.2.1 Time-Specific Expressions

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

14.3 Abbreviations

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

14.4 Definitions

An explanation of the terms used in this document.

14.4.1 DHCP (Dynamic Host Configuration Protocol)

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

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



See RFC 2131 Dynamic Host Configuration Protocol for further information.

14.4.2 NTP (Network Time Protocol)

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

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

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

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

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



See RFC 5905 for further information.

14.4.3 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 every network-compatible device can be integrated into the monitoring. Functions of the network management which 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.

14.4.4 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.

14.5 Accuracy & NTP Basic Principles



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



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

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

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

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

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

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

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

For example:

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

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

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

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

As an example, we mention the case where a network has a delay of 500msec and an accuracy shift (asynchronous) 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.

15 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)
- SNMPv2 (RFC 1213, RFC1901-1908)
- SNMPv3 (RFC 3410)
- SYSLOG (RFC 5424)
- SMTP (RFC 5321)

16 List of Open Source Packages Used

Third Party Software

The **hopf** Time Server 8029HEPTA/GPS includes a numerous of software packages subject to other license conditions. In case the use of such a software package might violate the licence conditions immediately after written notice it is ensured that the underlying licence conditions are met again.

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

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

Package name	Version	License	License details	Patches
arp-scan	1.9	GPL	v3	no
arptables	0.0.4			no
at91bootstrap 3	3.8.7			no
busybox	1.28.1	GPL	v2	no
bzip2	1.0.6	BSD		no
cifs-utils	6.7	GPL	v3	no
ethtool	4.13	GPL	v2	no
libevent	2.1.8-stable	3-clause BSD		no
libopenssl	1.0.2n	Dual	http://www.openssl.org/source/license.html	no
libpcap	1.8.1	BSD		no
libzlib	1.2.11		<p>Copyright (C) 1995-2017 Jean-loup Gailly and Mark Adler</p> <p>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.</p> <p>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:</p> <ol style="list-style-type: none"> 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
lighttpd	1.4.48		<p>Copyright (c) 2004, Jan Kneschke, incremental All rights reserved.</p> <p>Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:</p> <ul style="list-style-type: none"> - Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 	no

Package name	Version	License	License details	Patches
			<p>- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.</p> <p>- Neither the name of the 'incremental' nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.</p> <p>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.</p>	
linux	4.8.6	GPL	v2	no
linux-headers	4.8.6	GPL	v2	no
lzo	2.10	GPL	v2	no
mtdev	2.0.1	GPL	v2	no
net-snmp	5.7.3	BSD (mehrere)	http://net-snmp.sourceforge.net/about/license.html	no
ntp	4.2.8p11		<p>Copyright (c) University of Delaware 1992-2011</p> <p>Permission to use, copy, modify, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or Publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided "as is" without express or implied warranty.</p>	yes
openssh	7.6p1	BSD		no
pcrc	8.41	BSD		no
pps-tools	47333f24af878f67ce48022e8af16419713aa1ac	GPL	v2	no
uboot	2016.09.01	GPL	v2+	no
uboot-tools	2018.01	GPL	v2+	no
uclibc	1.0.28	GPL	v2	no

Package name	Version	License	License details	Patches
util-linux	2.31.1	GPLv2+ GPLv2 LGPLv2+ BSD		no
zip	3.0		<p>Copyright (c) 1990-2007 Info-ZIP. All rights reserved.</p> <p>For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:</p> <p>Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborh, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White.</p> <p>This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.</p> <p>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 above disclaimer and the following restrictions:</p> <ol style="list-style-type: none"> 1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions. 2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled. 3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions. 4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases. 	no