

Industriefunkuhren



Technical Manual

NTP Time Client Module with LAN Interface

Model 8029NTC

ENGLISH

Version: 02.04 - 30.08.2016

SET	IMAGE (8029)	FIRMWARE (8029)
Valid for	Version: 02.xx	Version: 01.xx

Version Numbers (Firmware / Description)

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

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

THE VERSION NUMBER OF THE IMAGE AND THE H8 SOFTWARE CAN BE READ IN THE WEBGUI OF THE TIME CLIENT 8029NTC (SEE **CHAPTER 7.3.6.1 DEVICE INFORMATION AND CHAPTER 7.3.6.2 HARDWARE INFORMATION**).

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

Downloading Technical Manuals

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

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

E-mail: info@hopf.com

Symbols and Characters



Operational Reliability

Disregard may cause damages to persons or material.



Functionality

Disregard may impact function of system/device.



Information

Notes and Information.



Safety regulations

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

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



Safety of the device

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

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

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

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

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

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

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

CE-Conformity



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

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

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

Contents	Page
1 NTP Time Client Module 8029NTC	7
2 Module Description.....	10
2.1 Installation Variants (Examples)	10
2.2 Installation and Removal of the Module	11
2.3 Functional Overview of the Front Panel Elements	11
2.3.1 Reset Button	11
2.3.2 NTP Status LEDs (NTP/Stratum/Accuracy)	11
2.3.3 USB-Port	12
2.3.4 LAN Interface ETH0	12
2.3.4.1 MAC-Address for ETH0	12
3 Function Principle.....	13
4 Module Behaviour	14
4.1 Boot Phase.....	14
4.2 NTP Adjustment Process (NTP/Stratum/Accuracy)	14
4.3 Reset Button.....	14
4.4 Firmware Update	14
5 Connection LAN Interface ETH0	16
6 Commissioning	17
6.1 General Procedure	17
6.2 Switching on the Operating Voltage.....	18
6.3 Establish the Network Connection via Web Browser	18
6.4 Network Configuration for ETH0 via LAN through <i>hmc</i>	18
7 HTTP WebGUI – Web Browser Configuration Interface	22
7.1 Quick Configuration	22
7.1.1 Requirements.....	22
7.1.2 Configuration Steps.....	22
7.2 General – Introduction	23
7.2.1 LOGIN and LOGOUT as User	24
7.2.2 Navigation via the Web Interface	25
7.2.3 Enter or Changing Data	26
7.3 Description of the Tabs.....	27
7.3.1 GENERAL Tab.....	28
7.3.2 TIME Tab	30
7.3.2.1 Time Zone Offset	30
7.3.2.2 Configuration of Summer Time (Daylight Saving Time)	31
7.3.3 NETWORK Tab.....	32
7.3.3.1 Host / Name Service	32
7.3.3.2 Network Interface ETH0.....	33
7.3.3.3 Routing	34
7.3.3.4 Management-Protocols / SNMP	35

7.3.4	NTP Tab	35
7.3.4.1	System Info	35
7.3.4.2	Peers	36
7.3.4.3	Server Configuration	37
7.3.4.4	Client Configuration	38
7.3.4.5	Restart NTP	41
7.3.4.6	Access Restrictions / Configuring the NTP Service Restrictions	41
7.3.4.7	Symmetric Key	46
7.3.4.8	Autokey / Public Key Cryptography	47
7.3.5	ALARM Tab	48
7.3.5.1	Syslog Configuration	48
7.3.5.2	E-mail Configuration	49
7.3.5.3	SNMP Configuration / TRAP Configuration	50
7.3.5.4	Alarm Messages	51
7.3.6	DEVICE Tab	52
7.3.6.1	Device Information	52
7.3.6.2	Hardware Information	52
7.3.6.3	Restoring Factory-Settings (Factory Defaults)	53
7.3.6.4	Reboot Device	53
7.3.6.5	Image Update & H8 Firmware Update	54
7.3.6.6	Passwords	55
7.3.6.7	Downloading SNMP MIB / Configuration Files	56
8	SSH and Telnet Basic Configuration	57
9	Technical Data	58
10	Factory Defaults	60
10.1	Network	60
10.2	NTP	60
10.3	ALARM	61
10.4	DEVICE	61
11	Glossary and Abbreviations	62
11.1	NTP-specific Terminology	62
11.2	Tally Codes (NTP-specific)	62
11.2.1	Time-specific expressions	63
11.3	Abbreviations	64
11.4	Definitions	65
11.4.1	DHCP (Dynamic Host Configuration Protocol)	65
11.4.2	NTP (Network Time Protocol)	65
11.4.3	SNMP (Simple Network Management Protocol)	66
11.4.4	TCP/IP (Transmission Control Protocol / Internet Protocol)	66
11.5	Accuracy & NTP Basic Principles	66
12	List of RFCs	68
13	List of Open Source Packages used	69

1 NTP Time Client Module 8029NTC

Module 8029NTC is a compact **Network Time Client** (*abbreviation* NTC) for the integration into Clock Systems or rather Signal Converters.

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

The Time Client Module 8029NTC is synchronized with the **UTC time** by the worldwide used time **NTP (Network Time Protocol)** via one or more NTP Time Servers.

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

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

For the operation of Module 8029NTC it is required to supply it with power and a network connection. The power supply is usually carried out via the device/system the module is integrated in. The output of the synchronized time information is performed at the module internal outputs.

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

Due to its compact size, the NTP Time Client Module 8029NTC is easy to integrate and characterized by its easy and simple operation, although it offers a **broad range of functions**. Some of the practice-oriented functionalities are for example:

- **Complete parameterisation via protected WebGUI access**
All required settings for operation can be executed via a password protected WebGUI also giving an overview of the status of the module 8029NTC.
- **Automatic handling of the leap second**
Should a leap second in the UTC time be announced by the Time Server, this is recognized by the Time Client Module 8029NTC and the leap second automatically inserted into the time information.
- **Superior Security**
A superior security is guaranteed via available coding procedures such as symmetric keys, autokey and access restrictions and deactivation of non-used protocols.
- **Management and Monitoring Functions**
Different functions are available for this purpose (e.g. SNMP, SNMP-Traps, E-mail notification, Syslog-messages including MIB II and private Enterprise MIB).

A few other basic functions of the Time Client Module 8029NTC:

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

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® (Version 5.2 and higher)
 - HP-UX 11i (RS232 support only for PA-RISC architecture)

Overview of the functions of the network Time Client Module 8029NTC:

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

Network Protocols

- HTTP
- DHCP
- Telnet
- SSH
- SNMPv2c, SNMP Traps (MIB II, Private Enterprise MIB)
- NTP (including SNTP)

Configuration Channel

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

Additionally Features

- E-mail notification
- Syslog messages to external syslog server
- Routing
- Update via TCP/IP
- Failsafe
- Watchdog circuit
- System management

2 Module Description

The NTP Time Client Module 8029NTC is a complete multi-processor embedded-linux system.

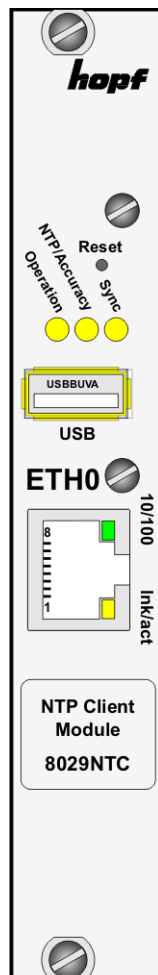
Usually the module is integrated as a NTP Time Client extension in **hopf** clock systems and converters at the factory.

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

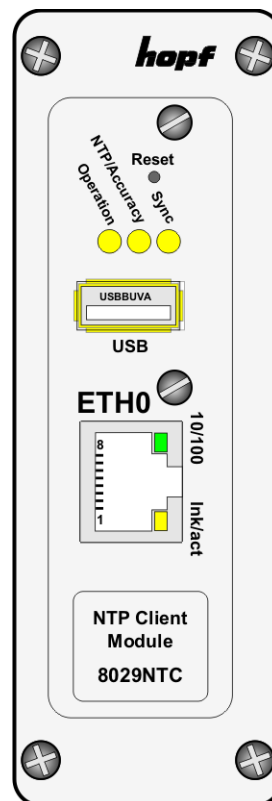
2.1 Installation Variants (Examples)

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

**Module 8029NTC
for the integration
in 19" systems
with 3U/4HP panels**



**Module 8029NTC
with front panel
for the integration in
DIN Rail housings (example)**



2.2 Installation and Removal of the Module

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

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



The module does not support HOT-PLUG

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

2.3 Functional Overview of the Front Panel Elements

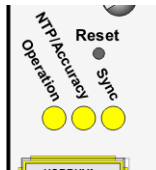
This chapter describes the individual front panel elements and their functions.

2.3.1 Reset Button



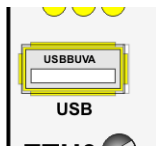
The Reset Button is accessible with a thin objective through the small drilling in the front panel next to the "Reset" inscription" (see **Chapter 4.3 Reset Button**).

2.3.2 NTP Status LEDs (NTP/Stratum/Accuracy)



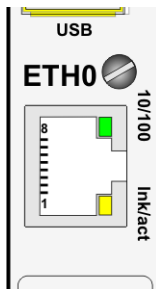
Operation-LED (Yellow)	Operating Mode of the Time Client Module 8029NTC
On	Module is operational
Flashes	Module boots
Off	Module is switched of or defective
NTP/Accuracy-LED (Yellow)	Synchronisation of the Time Client Module 8029NTC via NTP:
On	Accuracy "HIGH" – The module-time base is synchronized successfully with sufficient accuracy by a NTP time server (peer system)
Flashes	Accuracy "LOW" or "MEDIUM" – Not sufficiently accurate synchronization of module-time basis by a NTP time server (peer system)
Off	No NTP Time Server with stratum 14 or better accessible via LAN (module Stratum = 16)
Sync-LED (Yellow)	Status of Time Output of the Time Client Module 8029NTC:
On	The time information put out by the module can be used by connected components/devices for their own synchronization.
Off	The time information put out by the module cannot be used by connected components/devices for their own synchronization.

2.3.3 USB-Port



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

2.3.4 LAN Interface ETH0



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

2.3.4.1 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 the WebGUI of the appropriate board or be determined 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 Client 8029NTC is stated on a sticker directly placed on the module.



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

3 Function Principle

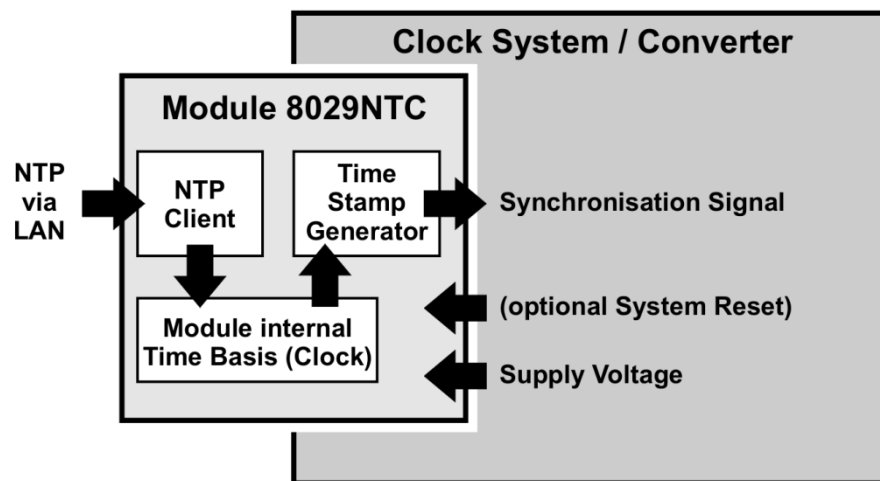
This chapter describes the functional principle of the Time Client Module 8029NTC and the internal relations between the individual function groups.

The Time Client Module 8029NTC is a multi-processor system.

The structure allows the following mode of operation:

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

Function Principle 8029NTC



4 Module Behaviour

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

4.1 Boot Phase

The boot process of the Time Client 8029NTC starts after turning on the system or a reset.

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

The end of the boot process is reached when the operation LED (yellow) is shining and thereby indicates that the NTP service on Module 8029NTC has been started and enabled. The boot process lasts approx. 1-1.5 minutes.

4.2 NTP Adjustment Process (NTP/Stratum/Accuracy)

NTP is a regulation process. After start of the NTP services, automatically processed during booting, the Time Client 8029NTC requires approximately 5-10 minutes depending on the accuracy and accessibility of the NTP Server parameterized in the module.

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

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

4.3 Reset Button

The Time Client 8029NTC can be reset by the Reset Button behind the front panel. The Reset Button is accessible with a thin objective through the small drilling in the front panel.

The button triggers a reset immediately:

4.4 Firmware Update

The Time Client 8029NTC is a multiprocessor system. For this reason a firmware update always consists of a so called Software SET including up to two (2) program releases defined by the SET version needed to be loaded into the board.

Module 8029NTC:

1x Image Update

1x H8 Update



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



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



The program releases assigned to a SET version may be taken from the release notes of the software SETs of the Time Client 8029NTC.

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

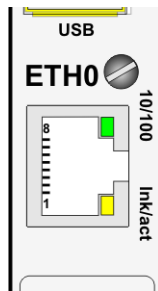
H8 Update

1. Log in as Master in WebGUI of the board.
2. Select in the **Device** tab the menu item **H8 Firmware Update**.
3. Select the file with the file extension **.mot for Module 8029NTC** 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.

Image Update

10. Log in as Master in WebGUI of the board.
11. Select in **Device** tab the menu item **Image Update**.
12. Select the file with the file **.img** via the selection window.
13. The selected file is shown in the selection window.
14. The update process is started with the button **Upload now**.
15. In WebGUI the successful file transfer and writing to the Module is indicated.
16. In WebGUI the successful update is indicated after 7-8 minutes with the request to release a reboot of the board.
17. After activation and successful reboot of the board the image update process is finished.

5 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

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

6 Commissioning

This chapter describes commissioning of the Time Client 8029NTC.

6.1 General Procedure

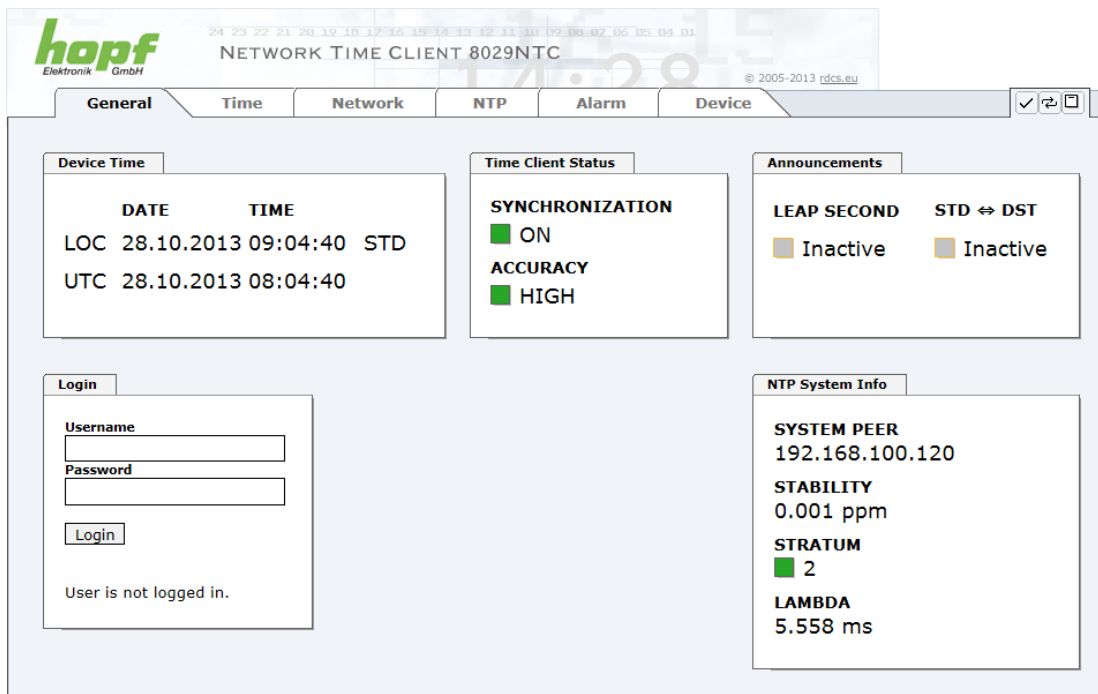
Overview of the general commissioning procedure:

- Finish the installation process completely
- Switch on the device
- Wait until the booting phase is finished (Duration approx. 2 min. – finished when the yellow Operation LED is lit on)
- Using the SEARCH Function of the **hmc - Network Configuration Assistant** in order to access the Time Client 8029NTC and set the basis LAN parameters (e.g. DHCP). Afterwards connect to the WebGUI of the Time Client 8029NTC via Web browser

OR

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

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



The screenshot displays the WebGUI of the hopf NETWORK TIME CLIENT 8029NTC. The interface features a top navigation bar with tabs: General, Time, Network, NTP, Alarm, and Device. The 'General' tab is active, showing several status panels:

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

	DATE	TIME	STD
LOC	28.10.2013	09:04:40	STD
UTC	28.10.2013	08:04:40	
- Time Client Status:** Shows synchronization status as 'ON' and accuracy as 'HIGH', both indicated by green status icons.
- Announcements:** Shows 'LEAP SECOND' and 'STD ⇌ DST' as 'Inactive'.
- Login:** A section with fields for 'Username' and 'Password', a 'Login' button, and a message stating 'User is not logged in.'
- NTP System Info:** Displays system parameters: SYSTEM PEER (192.168.100.120), STABILITY (0.001 ppm), STRATUM (2), and LAMBDA (5.558 ms).

6.2 Switching on the Operating Voltage

The Time Client 8029NTC has no own switch for the power supply. The Time Client 8029NTC is activated by switching on the device in which it is integrated in.

6.3 Establish the Network Connection via Web Browser



Ensure that the network parameters of the Time Client 8029NTC are configured in accordance with the local network before connecting the device to the network.



Connecting a network to an incorrectly configured Time Client 8029NTC (e.g. duplicate IP address) may cause interference on the network.



The Time Client 8029NTC 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 Client 8029NTC with a Factory Default setting causes problems in the network, the basis network parameterization should be executed via a "Peer to Peer" network connection.



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

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

6.4 Network Configuration for ETH0 via LAN through *hmc*

After connecting the system to the power supply and creating the physical network connection to LAN interface of the Time Client 8029NTC, the device can be searched for on the network via the ***hmc*** (***hopf*** Management Console). Then the base LAN parameters (IP address, netmask and gateway or DHCP) may be adjusted in order to allow accessibility of the Time Client 8029NTC for other systems on the network.



The SEARCH Function of the ***hmc*** - Network Configuration Assistant requires for location and recognition of the wished Time Client 8029NTC that both the ***hmc***-computer and Time Client 8029NTC are in the same SUB Net.

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



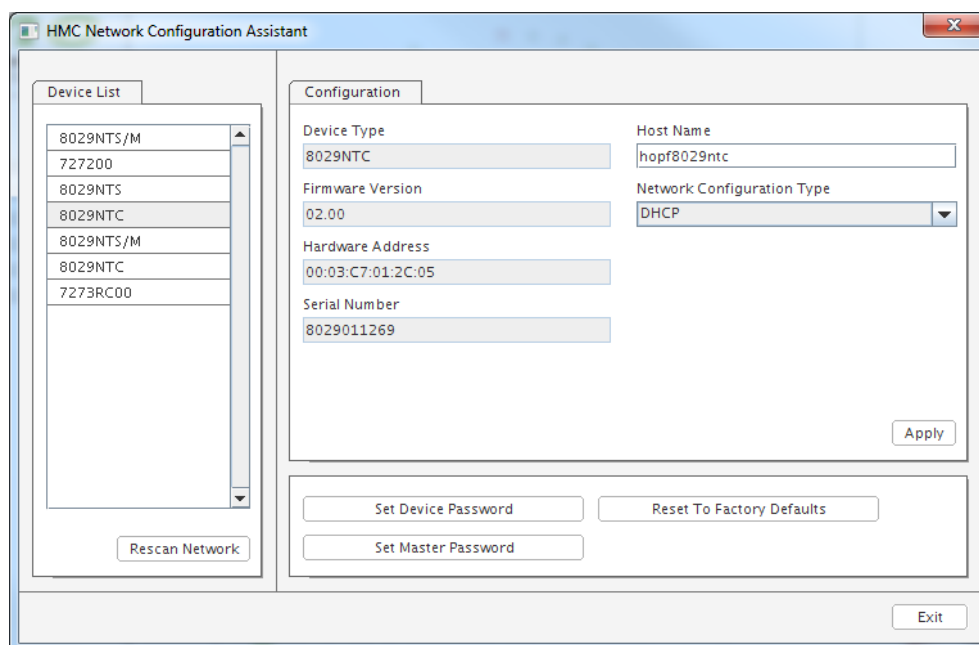
After a successful start of the **hmc Network Configuration Assistant** and completed search of the **hopf** LAN devices, the configuration of the base LAN parameters can be done.

The Time Client 8029NTC is stated as **8029NTC** in the Device List.

The determination of different Time Client 8029NTC (or other products variants) is made via **Hardware Address** (MAC Address).



The factory set MAC address for the Time Client 8029NTC is stated on a sticker laterally positioned on the exterior of the housing of the device.



For an extended configuration of the Time Client 8029NTC through a browser via WebGUI the following base parameters are required:

- **Host Name** ⇒ e.g. hopf8029ntc
- **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 Client 8029NTC via the **Apply** button. Afterwards the entry of the **Device Password** is requested:



The Time Client 8029NTC is supplied with the default device password <device> on delivery. After entry click on the **OK** button to confirm.

The LAN parameters thus set are directly adopted (without reboot) by the Time Client 8029NTC and are immediately active.

7 HTTP WebGUI – Web Browser Configuration Interface



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



The correct function & display of the WebGUI were verified on Windows XP and Windows 7 using the browsers MS Internet Explorer 8 and Mozilla Firefox, version 6.0.2 and 14.0.1

7.1 Quick Configuration

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

7.1.1 Requirements

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

7.1.2 Configuration Steps

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



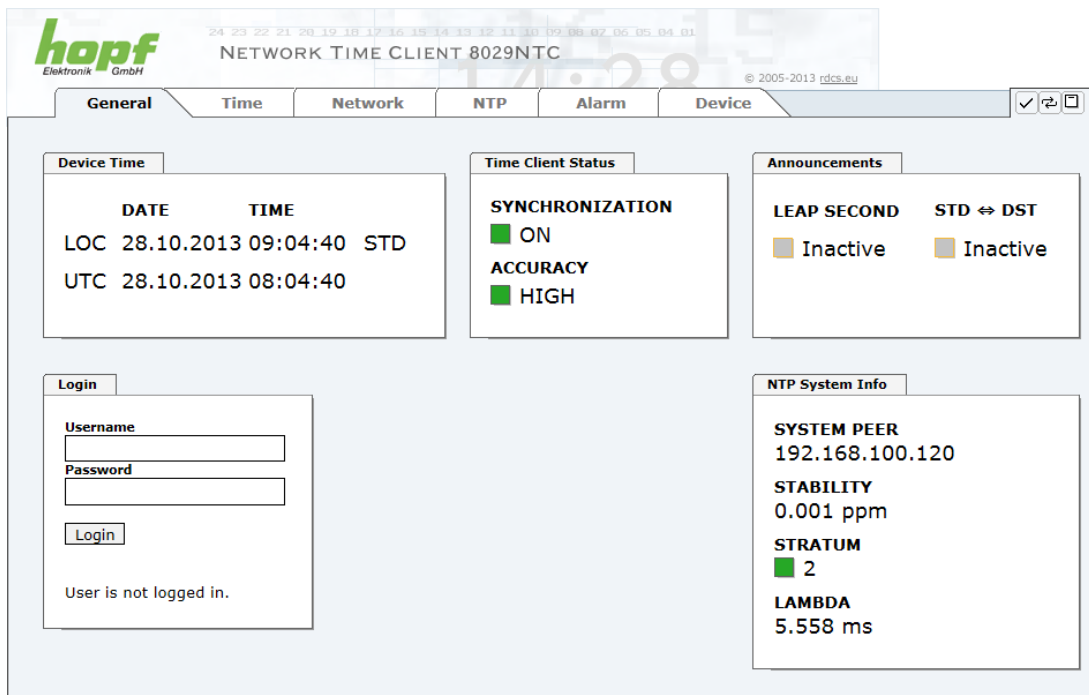
The following detailed explanatory information should be read if anything is unclear while executing the configuration steps.

7.2 General – Introduction

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



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



hopf Elektronik GmbH
NETWORK TIME CLIENT 8029NTC
© 2005-2013 rdcg.eu

General | Time | Network | NTP | Alarm | Device

Device Time

DATE	TIME	STD
LOC 28.10.2013	09:04:40	STD
UTC 28.10.2013	08:04:40	

Time Client Status

SYNCHRONIZATION
☒ ON
ACCURACY
☒ HIGH

Announcements

LEAP SECOND ☐ Inactive
STD ⇌ DST ☐ Inactive

Login

Username:
 Password:

 User is not logged in.

NTP System Info

SYSTEM PEER
192.168.100.120
STABILITY
0.001 ppm
STRATUM
☒ 2
LAMBDA
5.558 ms



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

7.2.1 LOGIN and LOGOUT as User

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

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

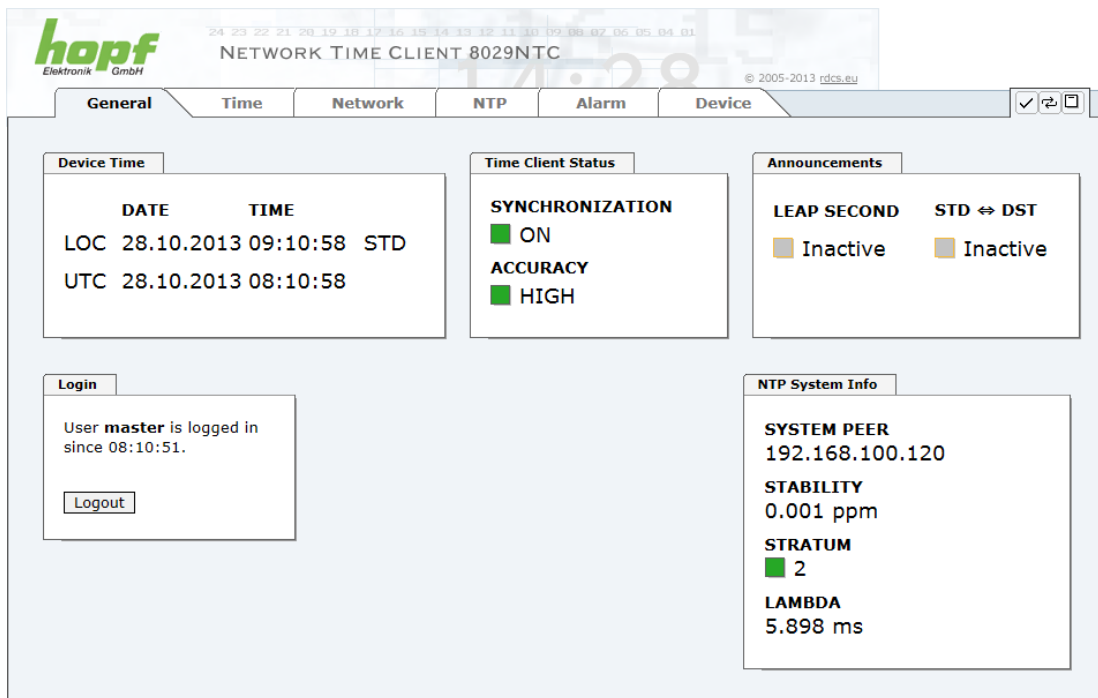


Differentiation is made between **upper and lower case** characters in the password. Alphanumeric characters and the following symbols can be used: [] () * - _ ! \$ % & / = ?



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

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



hopf Elektronik GmbH
NETWORK TIME CLIENT 8029NTC
© 2005-2013 rdcs.eu

General | Time | Network | NTP | Alarm | Device

Device Time

DATE	TIME
LOC 28.10.2013 09:10:58	STD
UTC 28.10.2013 08:10:58	

Time Client Status

SYNCHRONIZATION
☒ ON
ACCURACY
☒ HIGH

Announcements

LEAP SECOND ☐ Inactive
STD ⇌ DST ☐ Inactive

Login

User **master** is logged in since 08:10:51.

NTP System Info

SYSTEM PEER
192.168.100.120
STABILITY
0.001 ppm
STRATUM
☒ 2
LAMBDA
5.898 ms

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



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

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

Users logged in as **"master"** have all access rights to the Time Client 8029NTC.

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

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

7.2.2 Navigation via the Web Interface

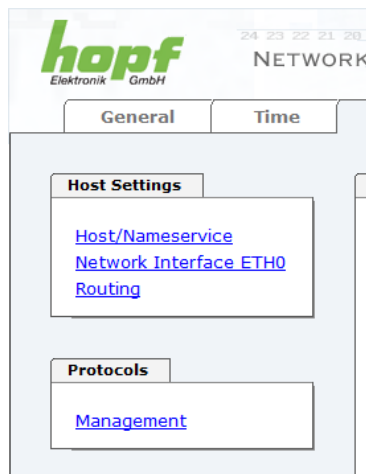
The WebGUI is divided into functional tabs. Click on one of these tabs to navigate through the board. The selected tab is identified by a darker background colour - see the following image (General in this case).



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



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



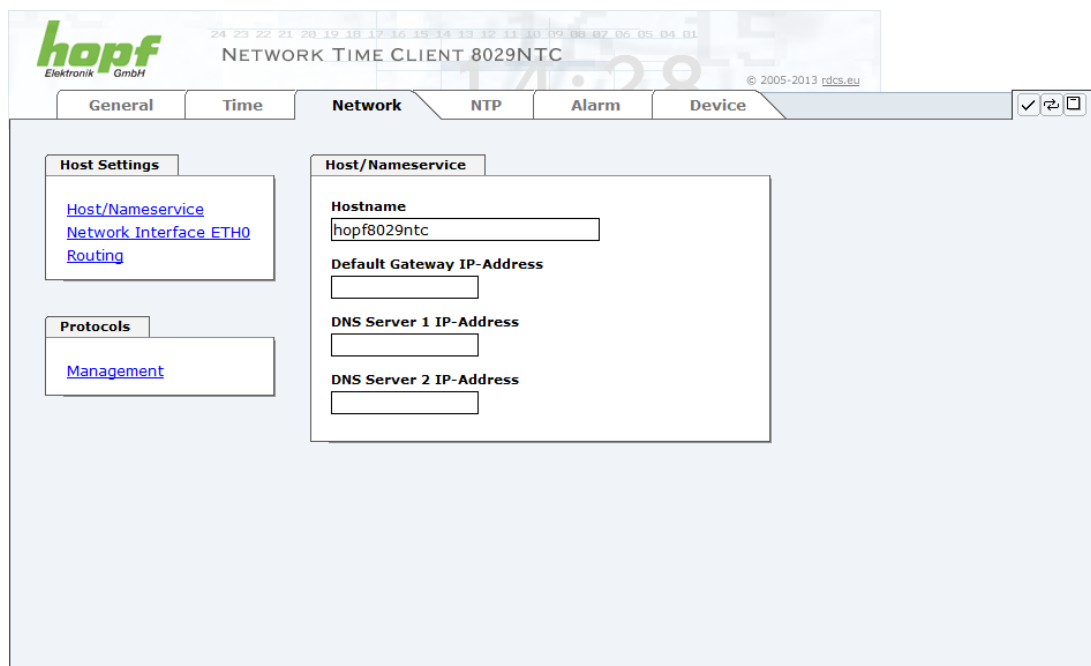
All the links within the tabs on the left hand side lead to corresponding detailed display or setting options.

7.2.3 Enter or Changing Data

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

All changeable data, are saved in Module 8029NTC. 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.

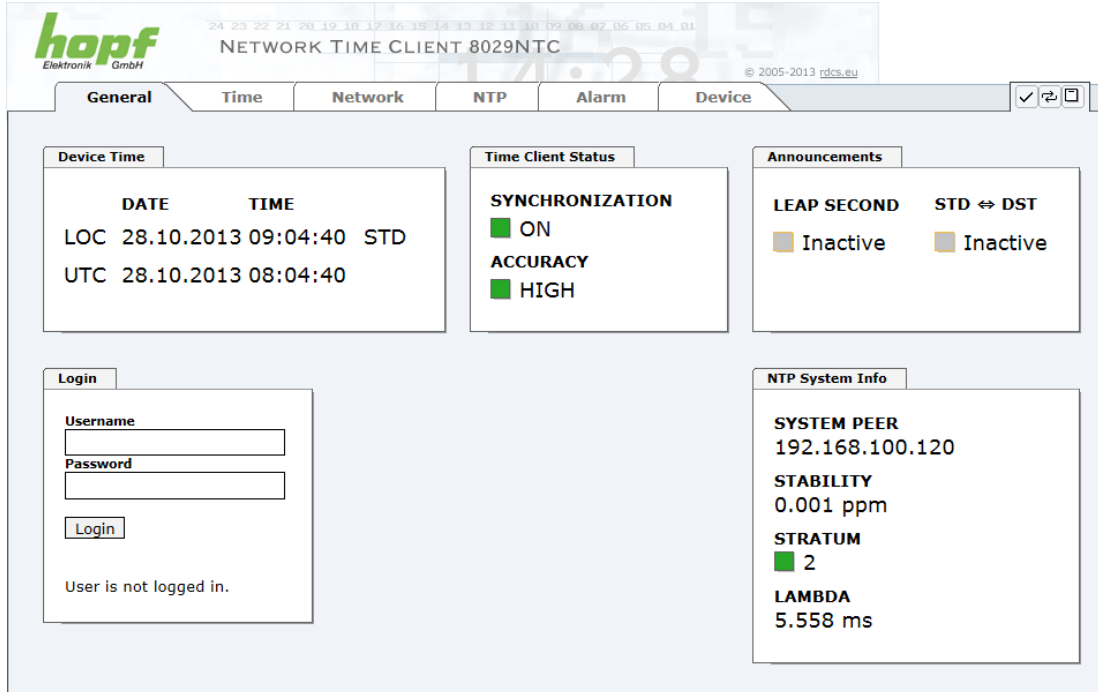
7.3 Description of the Tabs

The WebGUI is divided into the following tabs:

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

7.3.1 GENERAL Tab

This is the first tab which is displayed when using the web interface. This shows the current time and the synchronization state of the Module 8029NTC, furthermore a Login is possible (enter username and password), which is necessary to configure the Module 8029NTC via WebGUI.



The screenshot shows the 'General' tab of the 'hopf NETWORK TIME CLIENT 8029NTC' web interface. The interface includes a navigation bar with tabs: General, Time, Network, NTP, Alarm, and Device. The main content area is divided into several sections:

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

DATE	TIME
LOC 28.10.2013	09:04:40 STD
UTC 28.10.2013	08:04:40
- Time Client Status:** Displays synchronization and accuracy status.
 - SYNCHRONIZATION: ☒ ON
 - ACCURACY: ☒ HIGH
- Announcements:** Shows the status of LEAP SECOND and STD ⇌ DST. Both are currently 'Inactive'.
- Login:** A section for user authentication with fields for Username and Password, a Login button, and a message stating 'User is not logged in.'.
- NTP System Info:** Provides details about the NTP system.
 - SYSTEM PEER: 192.168.100.120
 - STABILITY: 0.001 ppm
 - STRATUM: ☒ 2
 - LAMBDA: 5.558 ms

Login

The **Login** box is used in accordance with **Chapter 7.2.1 LOGIN and LOGOUT as User**

Device Time

This sector displays the current time and date of Module 8029NTC, used for the output of time information. This time corresponds with the UTC time (UTC) received by NTP and the resulting local time (LOC). The local time is created by the parameters configured under the tab TIME (see **Chapter 7.3.2 TIME Tab**). In addition to the local time the daylight saving time (DST) / and standard time (STD) is indicated.

Time Client Status

SYNCHRONIZATION

Indicates the synchronization status of the internal time output. This value describes whether the connected components/devices use the time information of Module 8029NTC for their own synchronization.

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

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

ACCURACY

The **ACCURACY** field (accuracy of NTP) can include the possible values LOW - MEDIUM - HIGH. The meaning of those values is explained in **Chapter 11.5 Accuracy & NTP Basic Principles**.



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

Announcements

LEAP SECOND

announcement for inserting a leap second

Inactive: No announcement exists

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

STD ⇌ DST Announcement for adjustment for daylight saving time / standard time

Inactive: No announcement exists

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

NTP System Info

SYSTEM PEER

Indicates the currently used NTP Time Server for the synchronisation.

STABILITY

Indicates the current NTP stability value of Module 8029NTC in ppm.

STRATUM

Indicates the current NTP stratum value of Module 8029NTC in the value range of 1-16.



By default the stratum value of the Module 8029NTC is always one lower than the stratum of the SYSTEM PEER. The Module 8029NTC can only be synchronized on a SYSTEM PEER that it is at least **STRATUM 14 or better**.

LAMBDA

Indicates the current calculated NTP-LAMBDA value of Module 8029NTC in milliseconds.

7.3.2 TIME Tab

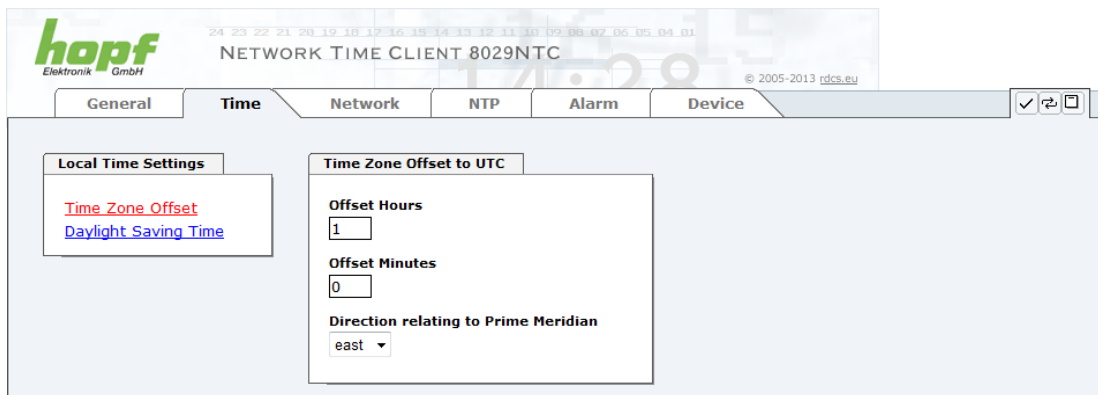
Generally NTP transfers the time information with the time basis UTC. The configuration of difference time (**Time Zone Offset to UTC**) is required for calculating the local standard time (winter time).

7.3.2.1 Time Zone Offset

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



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



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

Example:

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

Direction relating to Prime Meridian – Direction of the Difference Time

Entering the direction the local time deviates from world time:

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

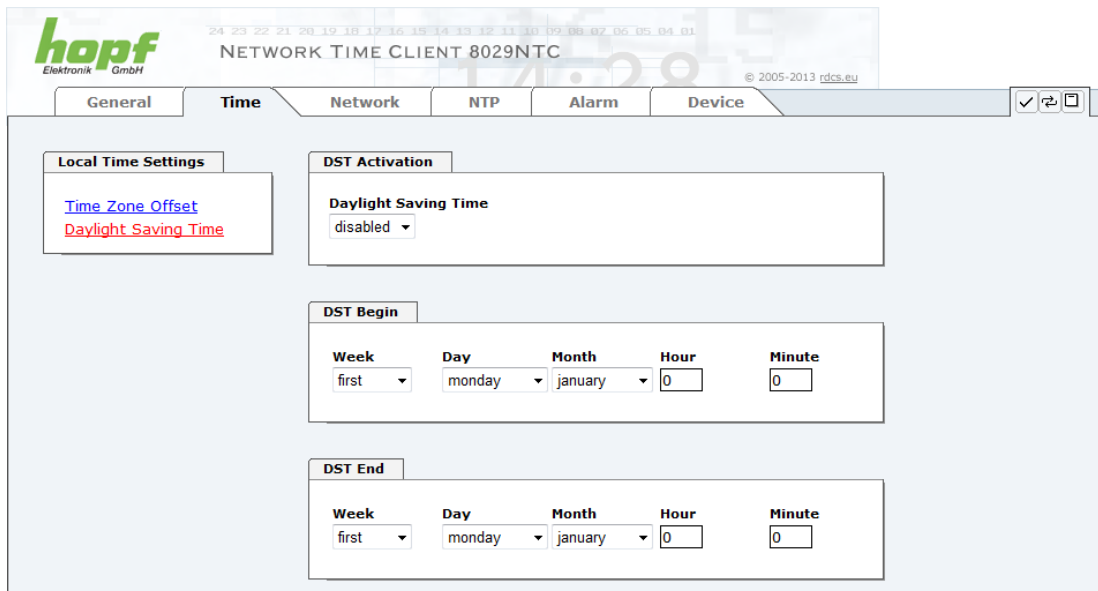
7.3.2.2 Configuration of Summer Time (Daylight Saving Time)

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

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



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



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

The individual items have the following meanings:

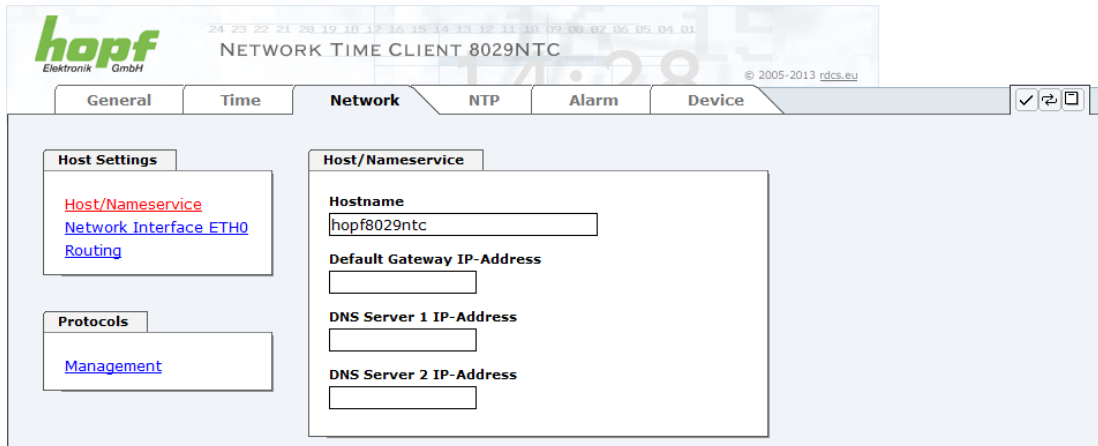
Week	How often the changeover should be processed per day of the week in the month	First - 1st week Second - 2nd week Third - 3th week Fourth - 4th week Last - last week
Day	The day of the week when the changeover should be processed	Sunday, Monday ... Saturday
Month	the month when the changeover should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



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

7.3.3 NETWORK Tab

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




Changing Network Parameters

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

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

7.3.3.1 Host / Name Service

Setting for the unique network identification.

7.3.3.1.1 Hostname

The standard setting for the Hostname is "**hopf8029ntc**". This name should also be adapted to the respective network infrastructure.

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



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

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



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

7.3.3.1.2 Default Gateway

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

7.3.3.1.3 DNS Server 1 & 2

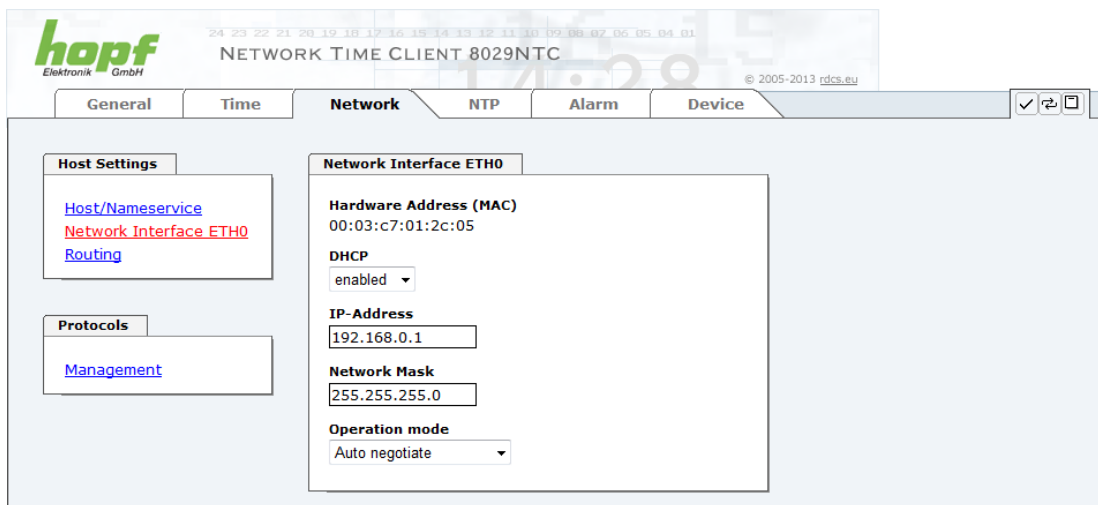
The IP address of the DNS server should be entered if you wish to use complete Hostnames (hostname.domainname) or work with reverse lookup.

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

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

7.3.3.2 Network Interface ETH0

Configuration of the Ethernet interface ETH0 of the Module 8029NTC



The screenshot shows the web interface for the hopf NETWORK TIME CLIENT 8029NTC. The 'Network' tab is selected, and the 'Network Interface ETH0' configuration page is displayed. The interface includes a sidebar with links for Host Settings (Host/Nameservice, Network Interface ETH0, Routing) and Protocols (Management). The main configuration area for ETH0 shows the Hardware Address (MAC) as 00:03:c7:01:2c:05, DHCP set to 'enabled', IP-Address as 192.168.0.1, Network Mask as 255.255.255.0, and Operation mode set to 'Auto negotiate'.

7.3.3.2.1 Default Hardware Address (MAC)

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

For further information about the MAC address refer to **Chapter 2.3.4.1 MAC-Address for ETH0** for the Time Client 8029NTC.



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

7.3.3.2.2 DHCP

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

7.3.3.2.3 IP Address

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

7.3.3.2.4 Network Mask

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

7.3.3.2.5 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

Auto negotiate ▼

Auto negotiate

10 Mbps / half duplex

100 Mbps / half duplex

10 Mbps / full duplex

100 Mbps / full duplex

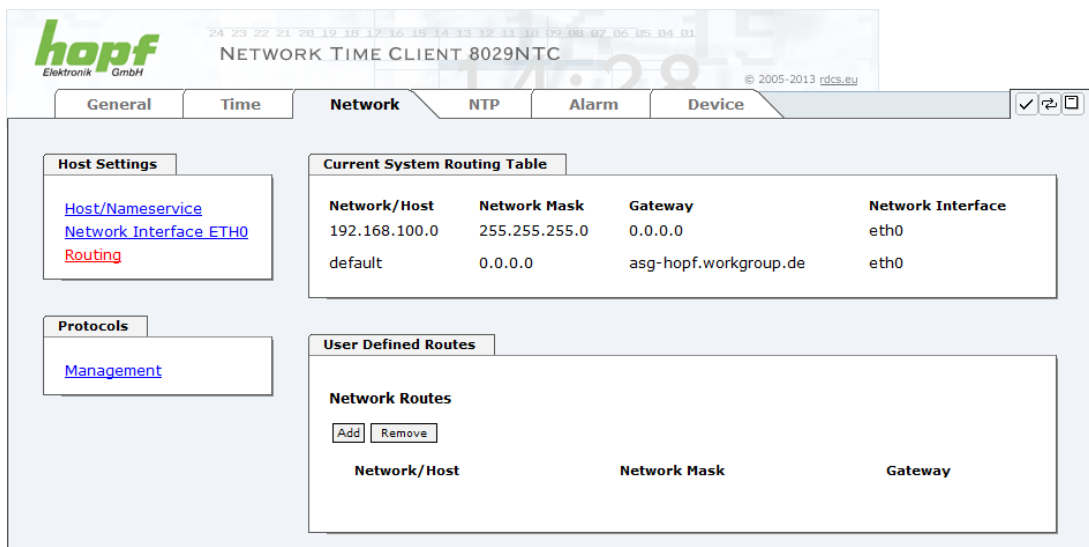
7.3.3.3 Routing

A route must be configured if the module is not only be used in the local sub-network.

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



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



Current System Routing Table

Network/Host	Network Mask	Gateway	Network Interface
192.168.100.0	255.255.255.0	0.0.0.0	eth0
default	0.0.0.0	asg-hopf.workgroup.de	eth0

User Defined Routes

Network Routes

Add Remove

Network/Host	Network Mask	Gateway
--------------	--------------	---------

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

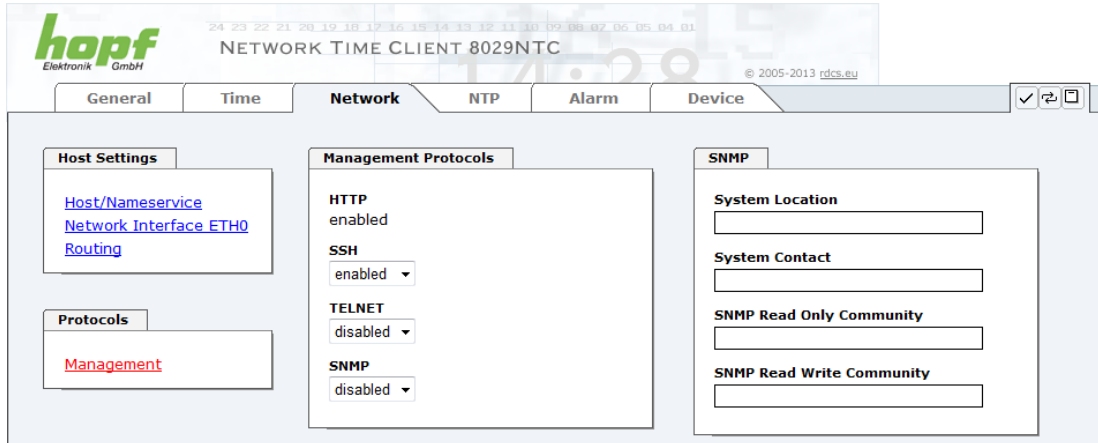


The module cannot be used as a router!

7.3.3.4 Management-Protocols / SNMP

Protocols that are not required should be disabled for security reasons. The only protocol that cannot be disabled is the HTTP. A correctly configured Board is always accessible via the web interface.

Changes to the security for a protocol (enable/disable) take effect immediately.



The screenshot shows the hopf web interface for the '8029NTC' module. The 'Network' tab is selected, and the 'Management Protocols' sub-tab is active. It shows settings for HTTP (enabled), SSH (enabled), TELNET (disabled), and SNMP (disabled). To the right, the 'SNMP' tab is also visible, showing fields for System Location, System Contact, and Read/Write Communities. The interface includes a top navigation bar with tabs for General, Time, Network, NTP, Alarm, and Device.

All fields must be completed for the SNMP to operate correctly. Contact your network administrator if you do not have all the data.

The SNMP protocol should be enabled when using SNMP Traps.



These service settings are applicable across the board! Services with "disabled" status are not externally accessible and are not made externally available by the Board!

7.3.4 NTP Tab

This tab shows values and settings for all of the NTP services. NTP is the module's main service.

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

The NTP functionality is provided by a NTP daemon running on the embedded-Linux of the module.



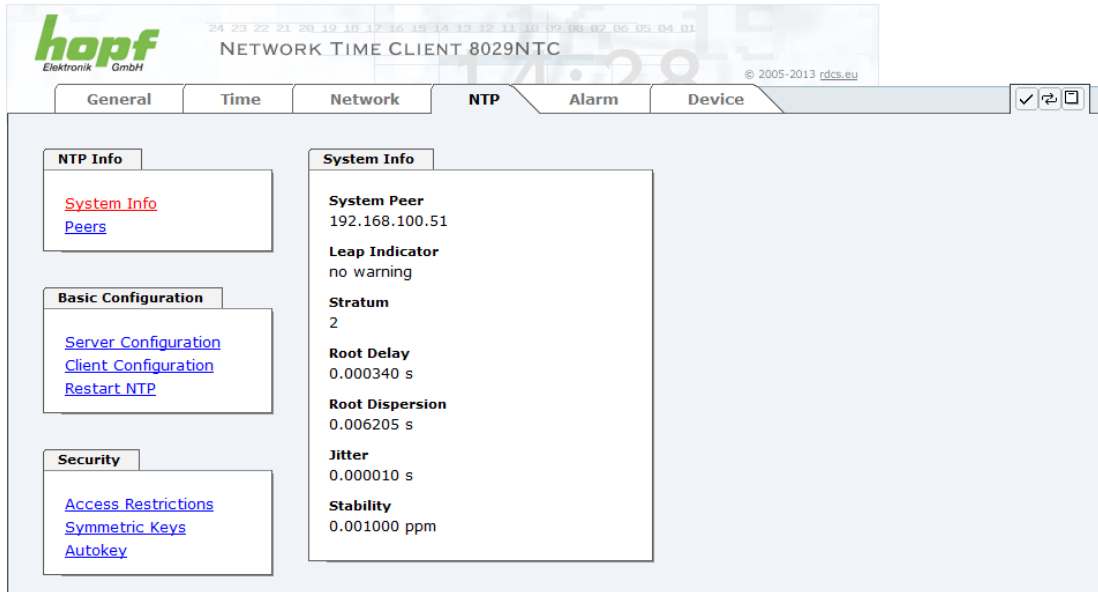
After all changes (according to NTP) have been done a restart of the NTP service of the module is necessary (see **Chapter 7.3.4.5 Restart NTP**).

7.3.4.1 System Info

The System "System Info" summary displays the momentary NTP data of the embedded Linux and provides additional information about stratum, leap second, current Base System peer, jitter and the stability of the time information.

The NTP version used correctly adjusts the leap second.

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



The screenshot shows the 'NTP' tab of the 'NETWORK TIME CLIENT 8029NTC' web interface. The left sidebar contains links for 'NTP Info' (System Info, Peers), 'Basic Configuration' (Server Configuration, Client Configuration, Restart NTP), and 'Security' (Access Restrictions, Symmetric Keys, Autokey). The main content area displays 'System Info' with the following details:

- System Peer:** 192.168.100.51
- Leap Indicator:** no warning
- Stratum:** 2
- Root Delay:** 0.000340 s
- Root Dispersion:** 0.006205 s
- Jitter:** 0.000010 s
- Stability:** 0.001000 ppm

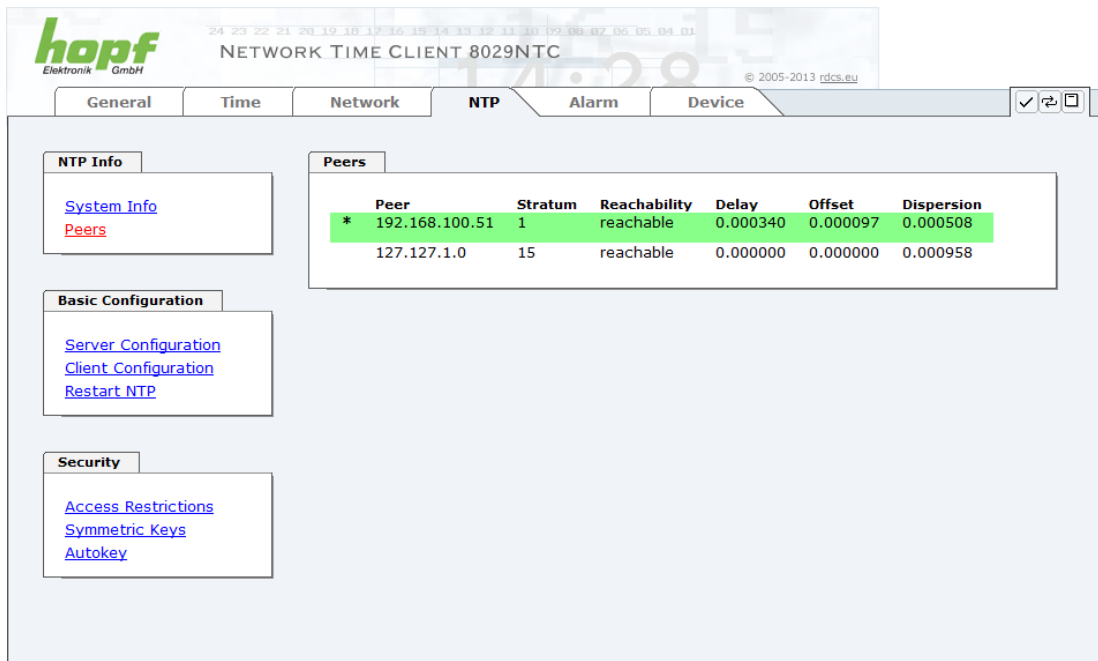
7.3.4.2 Peers

The overview of the Peers is used to monitor the behaviour and the properties of the configured NTP Server and the NTP algorithm.

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

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

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



The screenshot shows the 'Peers' tab of the 'NETWORK TIME CLIENT 8029NTC' web interface. The left sidebar is identical to the previous screenshot. The main content area displays a table with the following data:

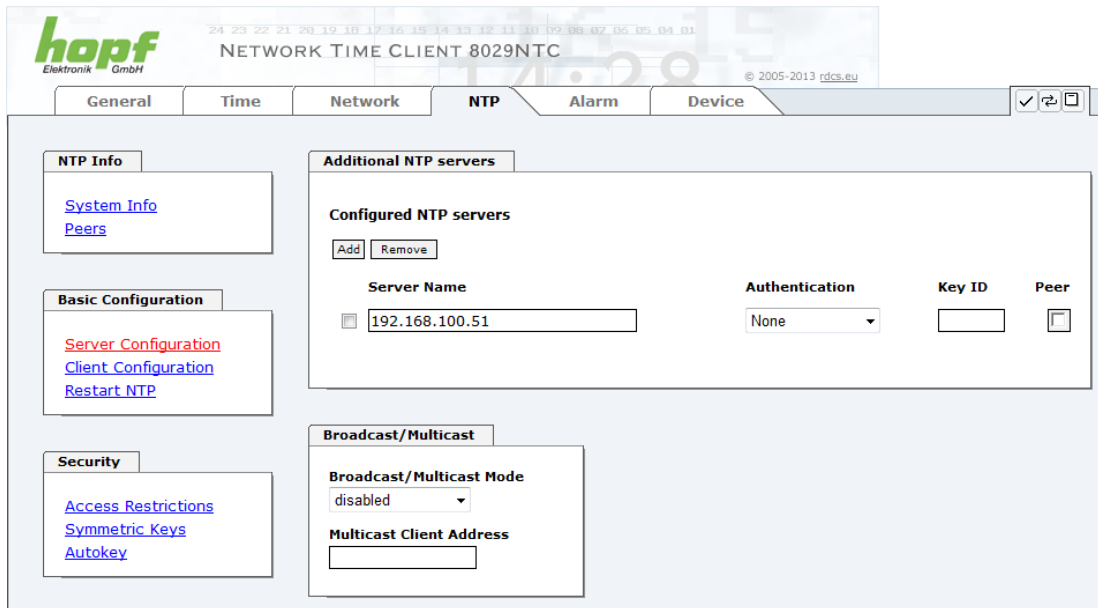
Peer	Stratum	Reachability	Delay	Offset	Dispersion
* 192.168.100.51	1	reachable	0.000340	0.000097	0.000508
127.127.1.0	15	reachable	0.000000	0.000000	0.000958

To synchronise the Module 8029NTC further external NTP servers are configured in the lines.

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 11.2 Tally Codes (NTP-specific)**).

7.3.4.3 Server Configuration

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



7.3.4.3.1 NTP SERVERS for Synchronisation

Server Name

In this field the NTP Server, used for the synchronisation of Module 8029NTC, should be registered. Adding further NTP servers provides the option to implement a safety system for the time service. However, this influences the accuracy and stability of the module.

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

Authentication / Key ID

Broadcast packets can be protected by authentication for security reasons.

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

7.3.4.3.2 Broadcast / Multicast

This section is used to synchronize the Module 8029NTC with a broadcast or multicast server.

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

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

The server continuously generates broadcast messages at defined intervals, corresponding to 16 seconds (minpoll 4) on the LAN Board. 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 LAN Board as a multicast server. The configuration of a multicast server is similar to that of a broadcast server. However, a multicast group address (class D) is used instead of the broadcast address.

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

In principle, a host or router sends a message to an Ipv4 multicast group address and expects all hosts and routers to receive this message. In doing so, there is no limit to the number of senders and receivers and a sender may also be a receiver and vice-versa. The IANA has assigned the multicast group address IPv4 224.0.1.1 to the NTP, however this should only be used if the multicast range can be safely limited in order to protect neighbouring networks. As a basic principle, administratively manageable IPv4 group addresses should be used as described in RFC-2365 or GLOP group addresses as described in RFC-2770.

7.3.4.4 Client Configuration

The synchronisation behaviour of Module 8029NTC can be adjusted following the link "**Client Configuration**". This function allows by reference to the associated system properties Module 8029NTC to use NTP Server for synchronization and thus for the output of time information for the synchronization of connected devices and components with inaccurate NTP server. Reasons for inaccurate NTP server could be e.g. poor network performance, poor own accuracy or bad availability resulting in an insufficiently accurate synchronization of the module with the standard settings.

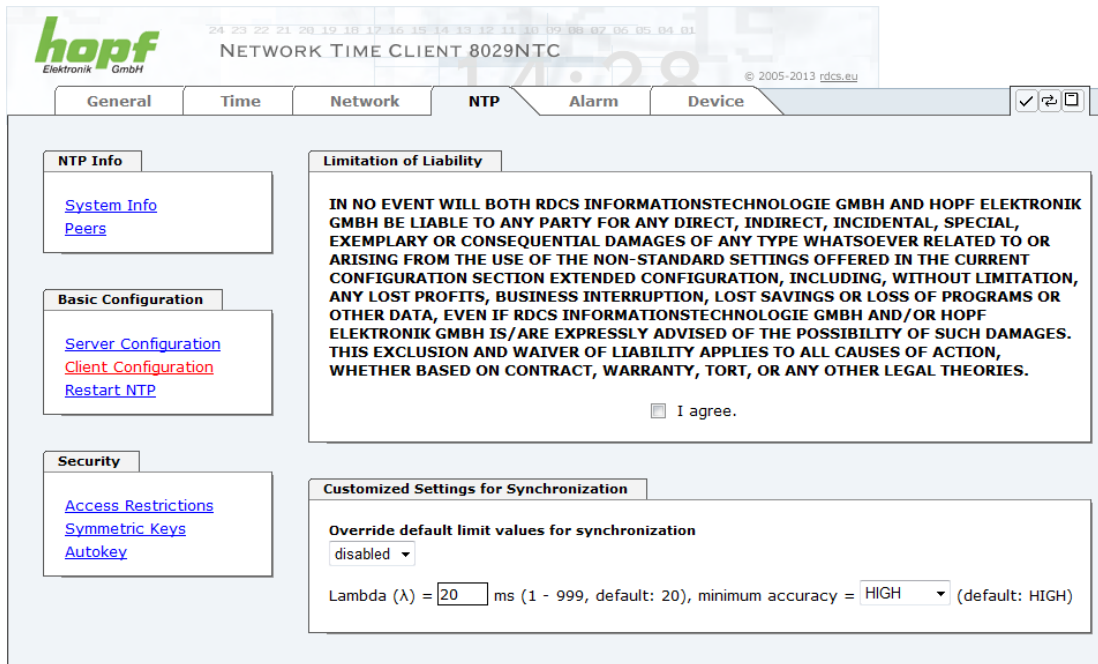
This function should be disabled by default.



When using this function the specified accuracy of Module 8029NTC and thus the accuracy of devices and components synchronized by the module may be worsened.



When using this function the specified data of NTP accuracy stated in the technical data of Module 8029NTC are not valid anymore.

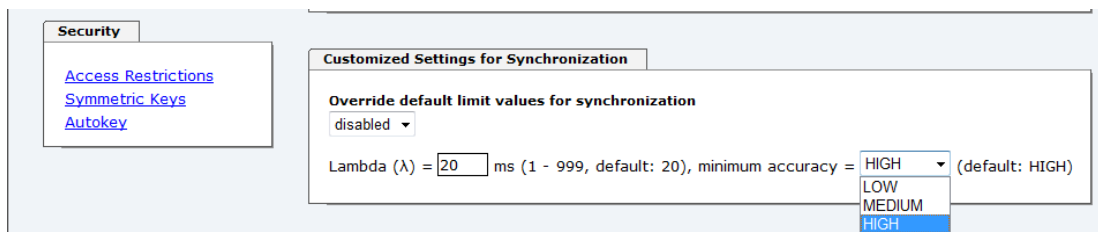


These functions are only unlocked with the declaration of consent "I agree" of the disclaimer "Limitation of Liability".



Safety Guidelines

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



Override default limit values for synchronization

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

Lambda (λ)

For observance of specified accuracy of Module 8029NTC, it uses only accurate NTP server for synchronisation which have an accuracy value for lambda better 20ms.

In case it is required that Module 8029NTC should be synchronized on a more inaccurate NTP server the threshold accuracy value for lambda can be adjusted by this function.

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

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



When using this function the specified accuracy of Module 8029NTC and thus the accuracy of devices and components synchronized by the module may be worsened.

Minimum Accuracy

Only with the accuracy status **accuracy = high** Module 8029NTC synchronizes.

This function can be used for NTP server not being able to synchronize Module 8029NTC with the required accuracy. It allows the adjustment of the accuracy value (**accuracy = high / medium / low**) and the accuracy of the connected devices and components for the synchronization.



Modification of values do not cause an immediate effect when clicking on the apply symbol. In addition the NTP service **must** be restarted (see **Chapter 7.3.6.4 Reboot Device**).

7.3.4.4.1 Definition Accuracy (Low / Medium / High)

Calculation

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

LOW =

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

MEDIUM =

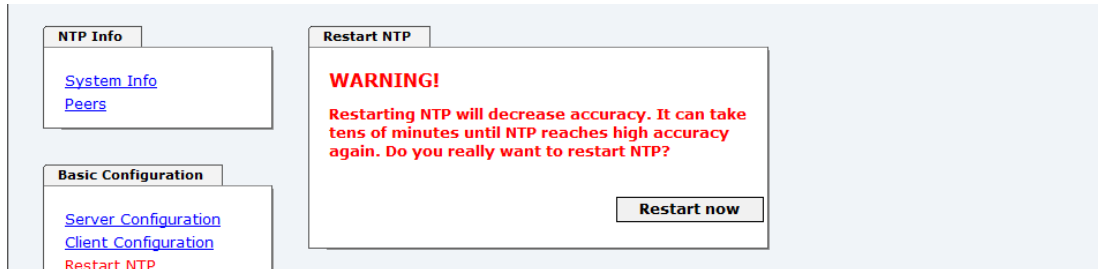
LAMBDA < Accuracy-value **and** System_Peer_Offset >= 0,001s
or
 LAMBDA < Accuracy-value **and** Stability > 2,0

HIGH =

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

7.3.4.5 Restart NTP

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



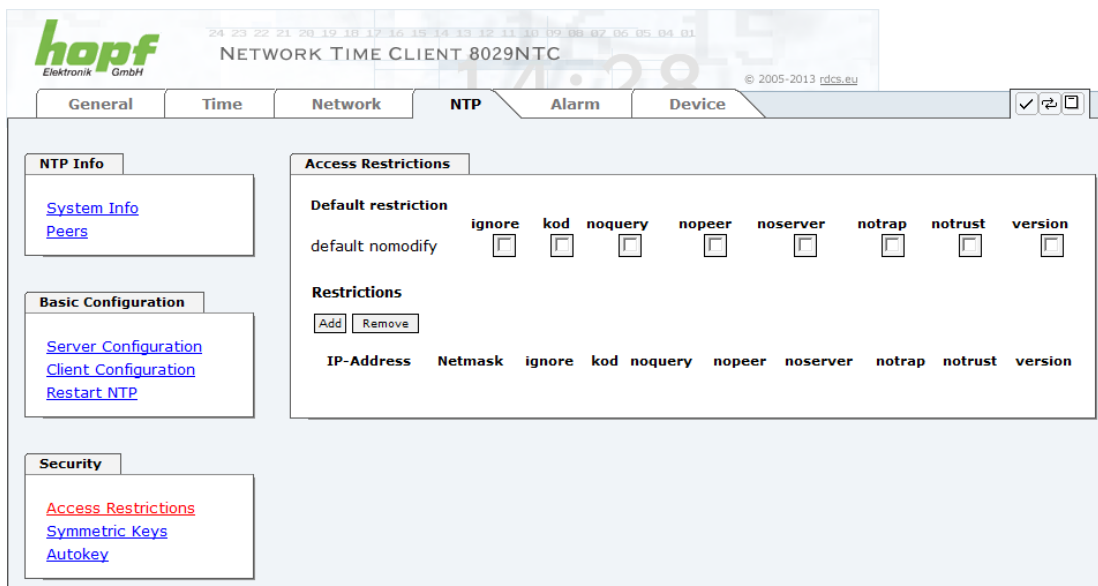
The screenshot shows a web interface with a sidebar on the left containing links for 'NTP Info' (System Info, Peers), 'Basic Configuration' (Server Configuration, Client Configuration, Restart NTP), and 'Security' (Access Restrictions, Symmetric Keys, Autokey). The main area displays a 'Restart NTP' dialog with a red 'WARNING!' header. The text reads: 'Restarting NTP will decrease accuracy. It can take tens of minutes until NTP reaches high accuracy again. Do you really want to restart NTP?'. A 'Restart now' button is located at the bottom right of the dialog.

Restarting NTP Services is the only possibility of making NTP changes effective without having to restart the entire Module 8029NTC. As can be seen from the warning message, the currently reachable stability and accuracy are lost due to this restart.

After a restart of the NTP service it takes a few minutes until the NTP service on Module 8029NTC is adjusted on an available NTP Server again.

7.3.4.6 Access Restrictions / Configuring the NTP Service Restrictions

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



The screenshot shows the 'NTP' configuration page for the 'NETWORK TIME CLIENT 8029NTC'. The sidebar on the left has links for 'NTP Info' (System Info, Peers), 'Basic Configuration' (Server Configuration, Client Configuration, Restart NTP), and 'Security' (Access Restrictions, Symmetric Keys, Autokey). The main area is titled 'Access Restrictions' and contains a 'Default restriction' section with checkboxes for 'ignore', 'kod', 'noquery', 'nopeer', 'noserver', 'notrap', 'notrust', and 'version'. Below this is a 'Restrictions' section with 'Add' and 'Remove' buttons, followed by a table with columns: 'IP-Address', 'Netmask', 'ignore', 'kod', 'noquery', 'nopeer', 'noserver', 'notrap', 'notrust', and 'version'.

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

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



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

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

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

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

Before beginning the configuration the points **7.3.4.6.1** to **7.3.4.6.4** must be checked by the user:

7.3.4.6.1 NAT or Firewall

Are incoming connections to the NTP Service blocked by NAT or a Stateful Inspection Firewall?	
No	Proceed to Chapter 7.3.4.6.2 Blocking Unauthorised Access
Yes	No restrictions are required in this case. Proceed further to Chapter 7.3.4.6.4 Internal Client Protection / Local Network Threat Level

7.3.4.6.2 Blocking Unauthorised Access

Is it really necessary to block all connections from unauthorised hosts if the NTP Service is openly accessible?	
No	Proceed to Chapter 7.3.4.6.3 Allowing Client Requests
Yes	<p>In this case the following restrictions are to be used:</p> <p>ignore in the default restrictions <input checked="" type="checkbox"/></p> <p>If a standard restriction is selected in this area, exceptions can be declared in separate lines for each authorised server, client or sub-network. See Chapter 7.3.4.6.5 Addition of Exceptions to Standard</p>

7.3.4.6.3 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 7.3.4.6.6 Access Control Options</p> <p> <input checked="" type="checkbox"/> kod <input checked="" type="checkbox"/> notrap <input checked="" type="checkbox"/> nopeer <input checked="" type="checkbox"/> noquery. </p>
Yes	<p>In this case select from the following standard restrictions: See Chapter 7.3.4.6.6 Access Control Options:</p> <p> <input checked="" type="checkbox"/> kod <input checked="" type="checkbox"/> notrap <input checked="" type="checkbox"/> nopeer </p> <p>If a standard restriction is selected in this area, exceptions can be declared in separate lines for each authorised server, client or sub-network. See Chapter 7.3.4.6.5 Addition of Exceptions to Standard.</p>

7.3.4.6.4 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 7.3.4.6.6 Access Control Options.</p> <p> <input checked="" type="checkbox"/> kod <input checked="" type="checkbox"/> notrap <input checked="" type="checkbox"/> nopeer </p>

7.3.4.6.5 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

ignore

kod

noquery

nopeer

noserver

notrap

notrust

version

default nomodify

☒

☒

☒

☒

☒

☒

☐

☐

Restrictions

Add

Remove

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



An unrestricted access of the Time Client 8029NTC 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 ☒

7.3.4.6.6 Access Control Options

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

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

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



Default Settings:

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

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

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

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

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

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

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

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

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

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

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

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

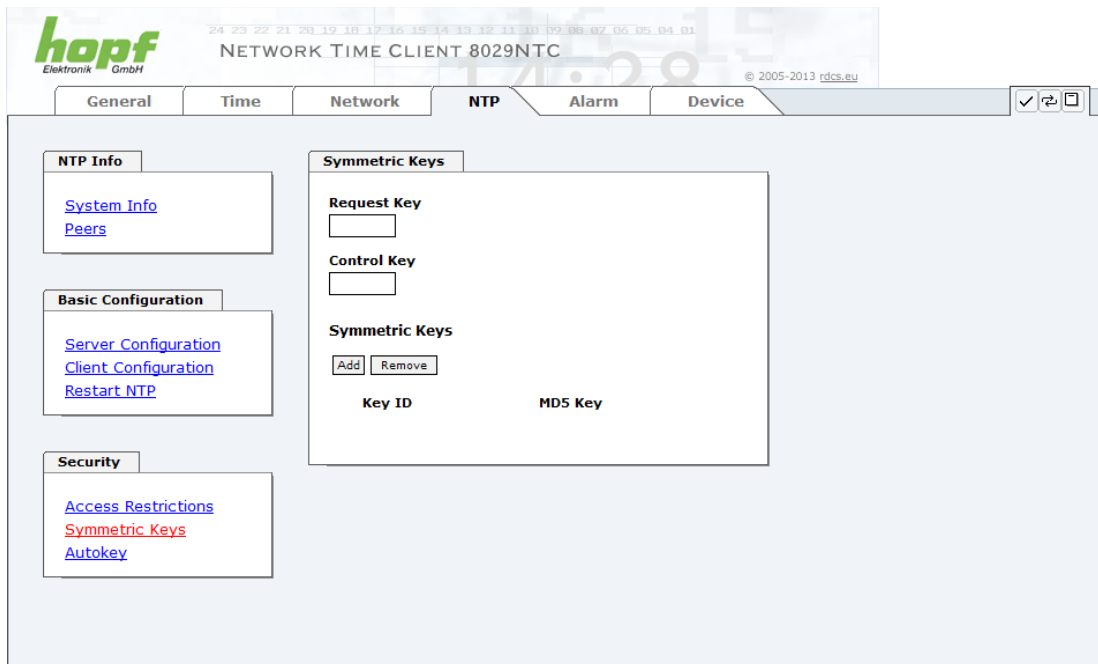
The trap service is a sub-system of the ntpq control message protocols. This service logs remote events in programmes.

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



Changes in data do not take effect immediately after clicking on the "Apply" symbol. The NTP service **MUST** also be restarted (see **Chapter 7.3.4.5 Restart NTP**).

7.3.4.7 Symmetric Key



hopf Elektronik GmbH NETWORK TIME CLIENT 8029NTC © 2005-2013 rdcs.eu

General Time Network **NTP** Alarm Device

NTP Info

[System Info](#)
[Peers](#)

Basic Configuration

[Server Configuration](#)
[Client Configuration](#)
[Restart NTP](#)

Security

[Access Restrictions](#)
[Symmetric Keys](#)
[Autokey](#)

Symmetric Keys

Request Key

Control Key

Symmetric Keys

Key ID	MD5 Key
--------	---------

7.3.4.7.1 Why Authentication?

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

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

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

7.3.4.7.2 How is Authentication used in the NTP Service?

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

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

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

The keyword key of a client's `ntp.conf` determines the key that is used to communicate with the designated server (e.g. the **hopf** NTP Time Server 8029NTS/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.

7.3.4.7.3 How is a key created?

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

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

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

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

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

7.3.4.7.4 How does authentication work?

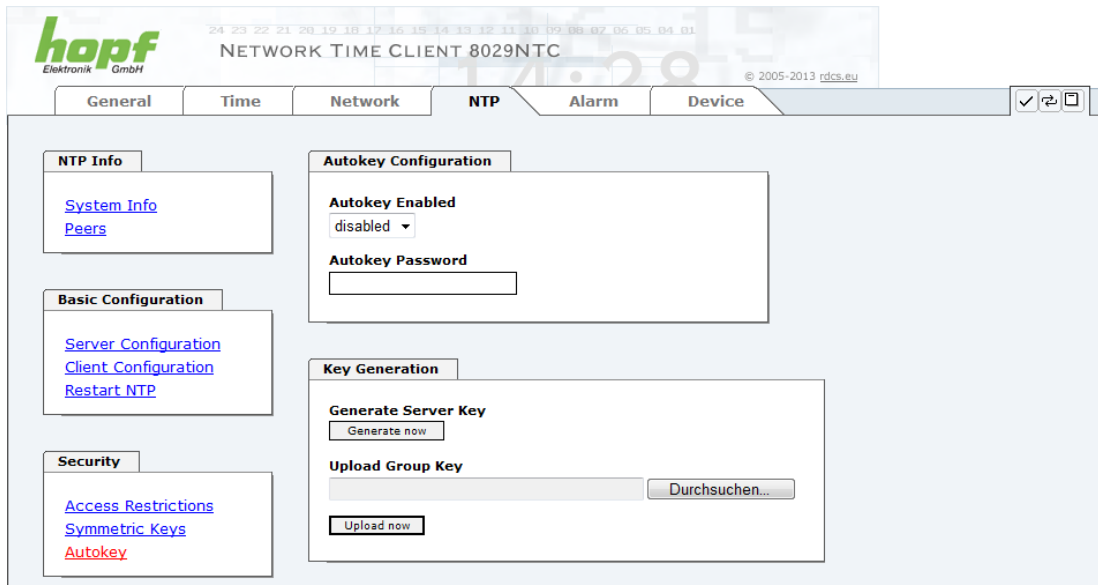
The basic authentication is a digital signature and no data encryption (if there are any differences between the two). The data packet and the key are used to create a non-reversible number which is attached to the packet.

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

7.3.4.8 Autokey / Public Key Cryptography

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

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



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

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



Generate now

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

If the Time Client 8029NTC is to form part of an NTP trust group, a group key can be defined and uploaded with the "Upload now" button.

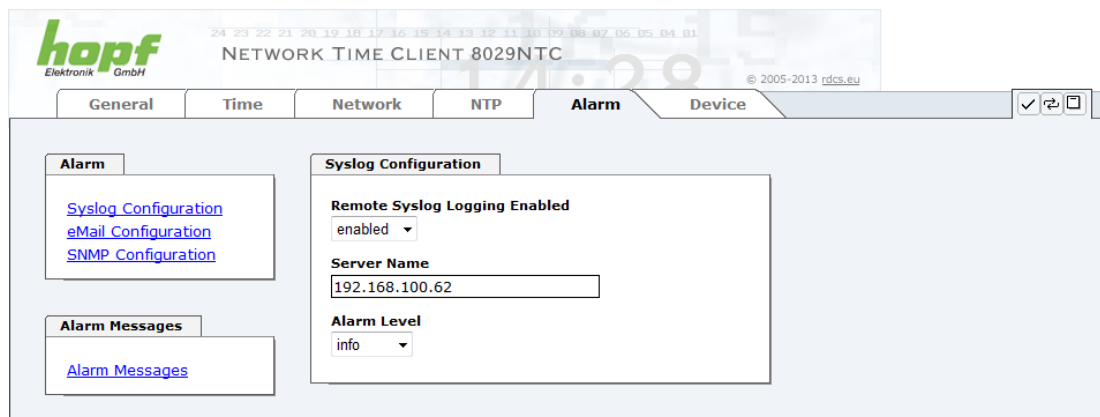
Detailed information about the NTP Autokey scheme can be found in the NTP documentation (<http://www.ntp.org/>).



Changes in data do not take effect immediately after clicking on the "Apply" symbol. The NTP service **MUST** also be restarted (see **Chapter 7.3.4.5 Restart NTP**).

7.3.5 ALARM Tab

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



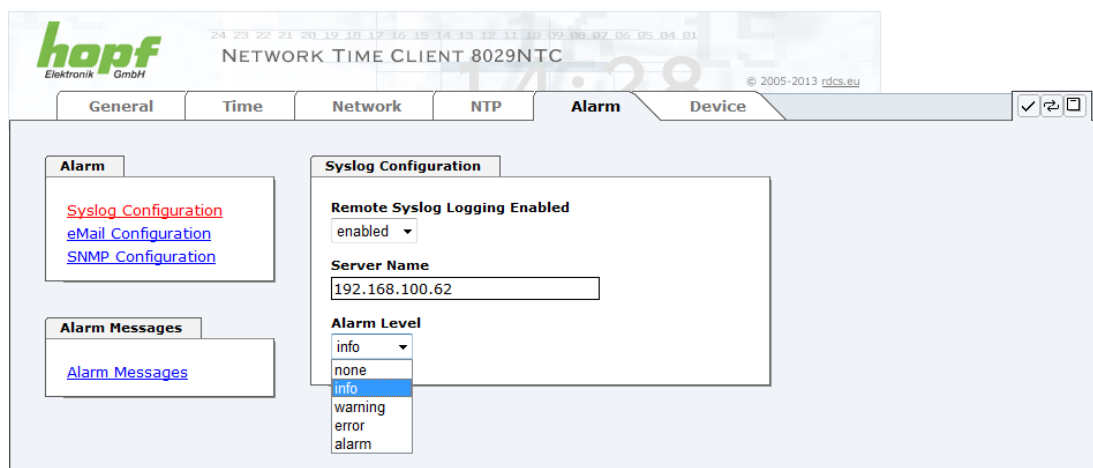
7.3.5.1 Syslog Configuration

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

Syslog uses Port 514.

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

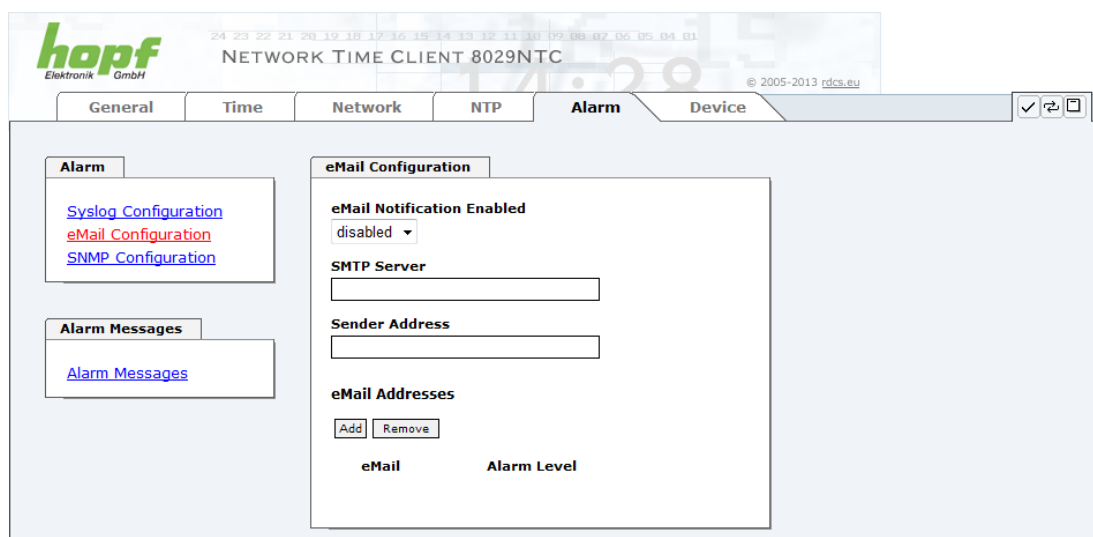
It should be noted that the standard Linux/Unix Syslog mechanism is used for this functionality. This is not the same as the Windows System Event mechanism!



The alarm level designates the priority level of the messages to be transmitted and the level from which transmission is to take place (see **Chapter 7.3.5.4 Alarm**).

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

7.3.5.2 E-mail Configuration



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

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

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

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

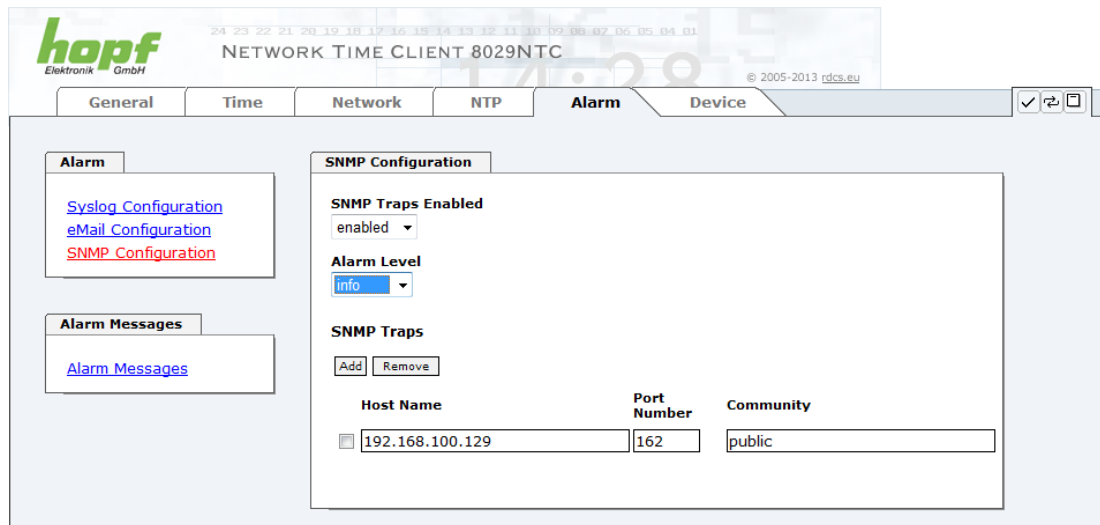
Some E-mail servers only accept messages if the sender address entered is valid (spam protection). This can be inserted in the "Sender Address" field.

The Alarm Level designates the priority level of the messages to be sent and the level from which they are to be sent (see **Chapter 7.3.5.4 Alarm**).

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

7.3.5.3 SNMP Configuration / TRAP Configuration

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



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

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

The private **hopf** enterprise MIB is also available over the web (see **Chapter 7.3.6.7 Downloading SNMP MIB / Configuration Files**).

The "Alarm Level" designates the priority level of the messages to be sent and the level from which they are to be sent (see **Chapter 7.3.5.4 Alarm**).

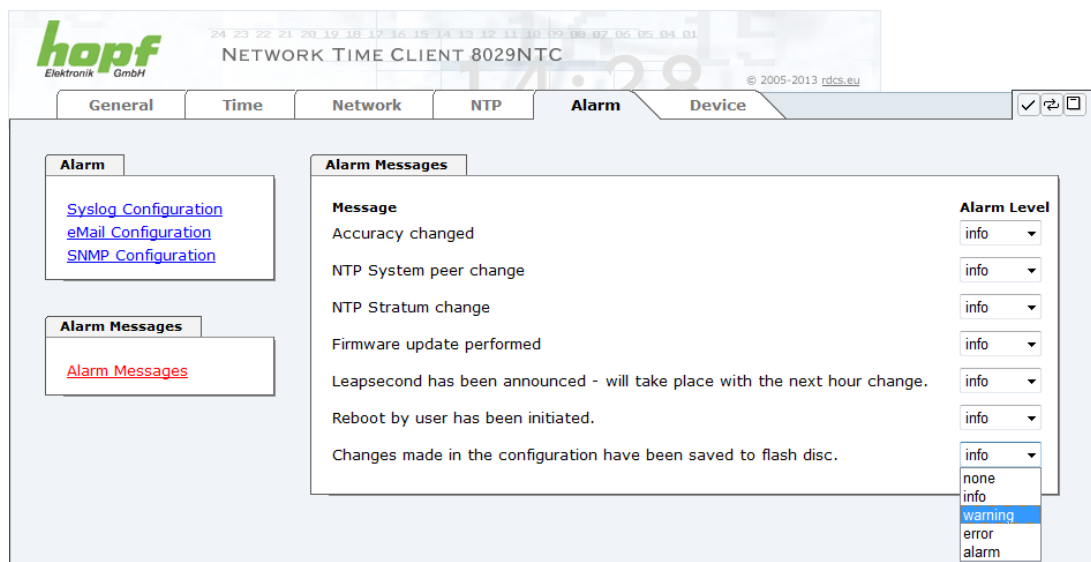
Alarm Level	Transmitted Messages
none	no messages
info	info / warning / error / alarm
warning	warning / error / alarm
error	error / alarm
alarm	alarm



SNMP protocol must be enabled in order to use SNMP (see **Chapter 7.3.3.4 Management-Protocols / SNMP**).

7.3.5.4 Alarm Messages

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



The screenshot shows the 'Alarm' configuration page in the hopf WEBGUI. The page has tabs for General, Time, Network, NTP, Alarm, and Device. The 'Alarm' tab is active. On the left, there are links for Syslog Configuration, eMail Configuration, and SNMP Configuration. Below these is a section for Alarm Messages with a link to Alarm Messages. The main area is titled 'Alarm Messages' and contains a table with columns 'Message' and 'Alarm Level'. The messages listed are: Accuracy changed, NTP System peer change, NTP Stratum change, Firmware update performed, Leapsecond has been announced - will take place with the next hour change., Reboot by user has been initiated., and Changes made in the configuration have been saved to flash disc.. The 'Alarm Level' dropdown menu is open, showing options: none, info, warning (selected), error, and alarm.

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



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

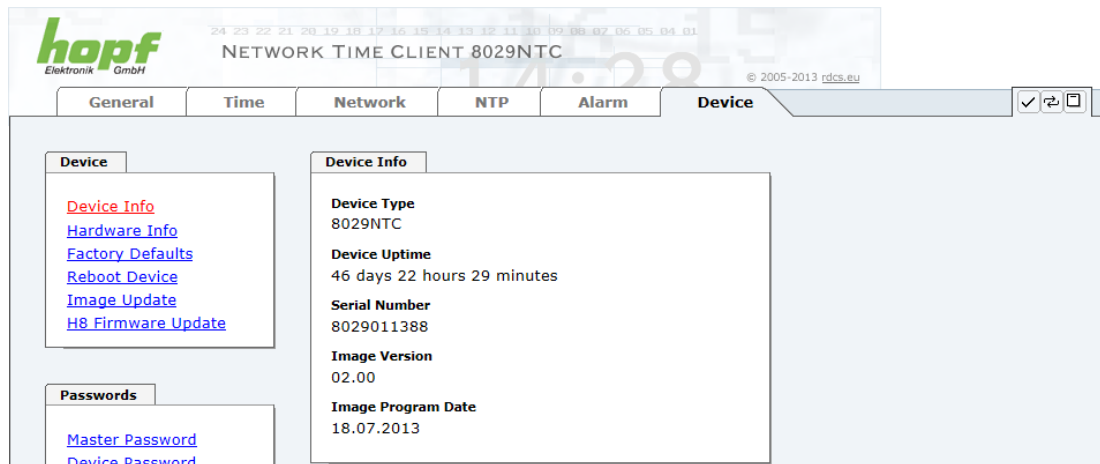
7.3.6 DEVICE Tab

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

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

7.3.6.1 Device Information

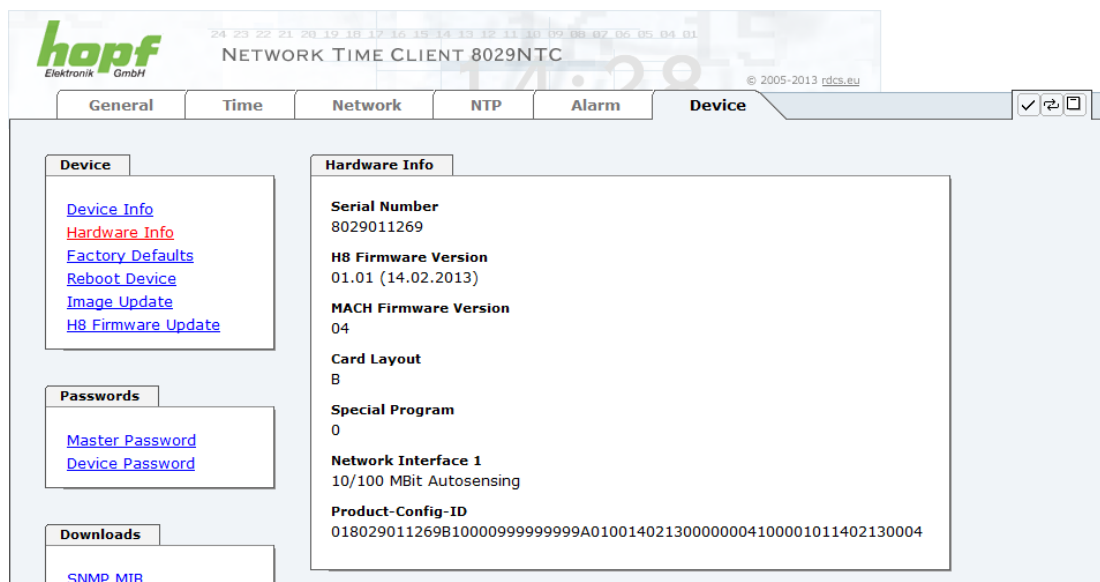
All information is available exclusively in write-protected and read-only form. Information about the Board type, serial number and current software versions is provided to the user for service and enquiry purposes.



7.3.6.2 Hardware Information

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

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



7.3.6.3 Restoring Factory-Settings (Factory Defaults)

In some cases it might be wished to restore all settings of the Module 8029NTC to their factory-settings (factory defaults).



This function enables the restoring of all settings from the flash memory to their factory default values. This also affects passwords (see **Chapter 10 Factory Defaults**).

The registration is conducted as Master user according to the manual, **Chapter 7.2.1 LOGIN and LOGOUT as User**.

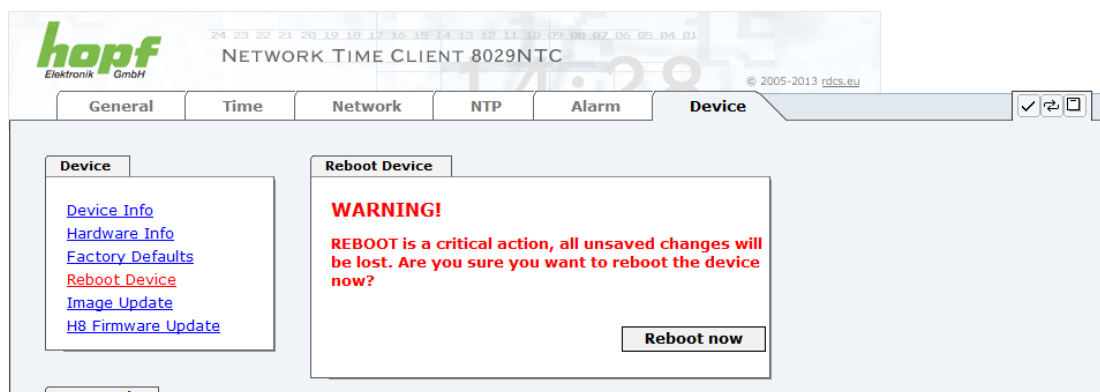
By pressing "**Reset now**" factory default values are set.

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



After a **Factory Default** a complete verification and a possibly new configuration of the Module 8029NTC are required. Especially the default MASTER and DEVICE passwords should be reset.

7.3.6.4 Reboot Device



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

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

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

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

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

7.3.6.5 Image Update & H8 Firmware Update

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

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



The following points should be noted regarding updates:

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

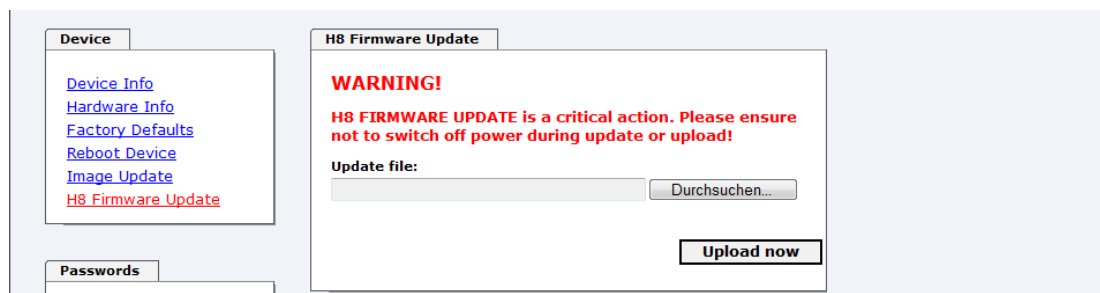
In order to carry out an update, enter the name and the folder in which the update / firmware image is located in the text field or open the file selection dialogue by pressing the "Browse" button.

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

H8-8029NTC_v0100_128.mot for the **H8 firmware**
(update takes approx. 1-1.5 minutes)

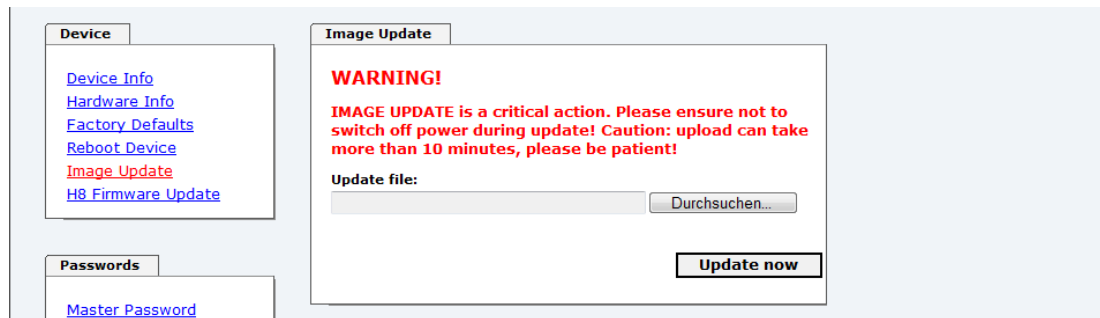
upgrade_8029_v0200_Release.img for the **embedded image**
(update takes approx. 7-8 minutes)

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



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

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



Device

- [Device Info](#)
- [Hardware Info](#)
- [Factory Defaults](#)
- [Reboot Device](#)
- [Image Update](#)
- [H8 Firmware Update](#)

Passwords

- [Master Password](#)

Image Update

WARNING!

IMAGE UPDATE is a critical action. Please ensure not to switch off power during update! Caution: upload can take more than 10 minutes, please be patient!

Update file:

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

7.3.6.6 Passwords

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

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

(See also **Chapter 7.2.1 LOGIN and LOGOUT as User**)



Device

- [Device Info](#)
- [Hardware Info](#)
- [Factory Defaults](#)
- [Reboot Device](#)
- [Image Update](#)
- [H8 Firmware Update](#)

Passwords

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

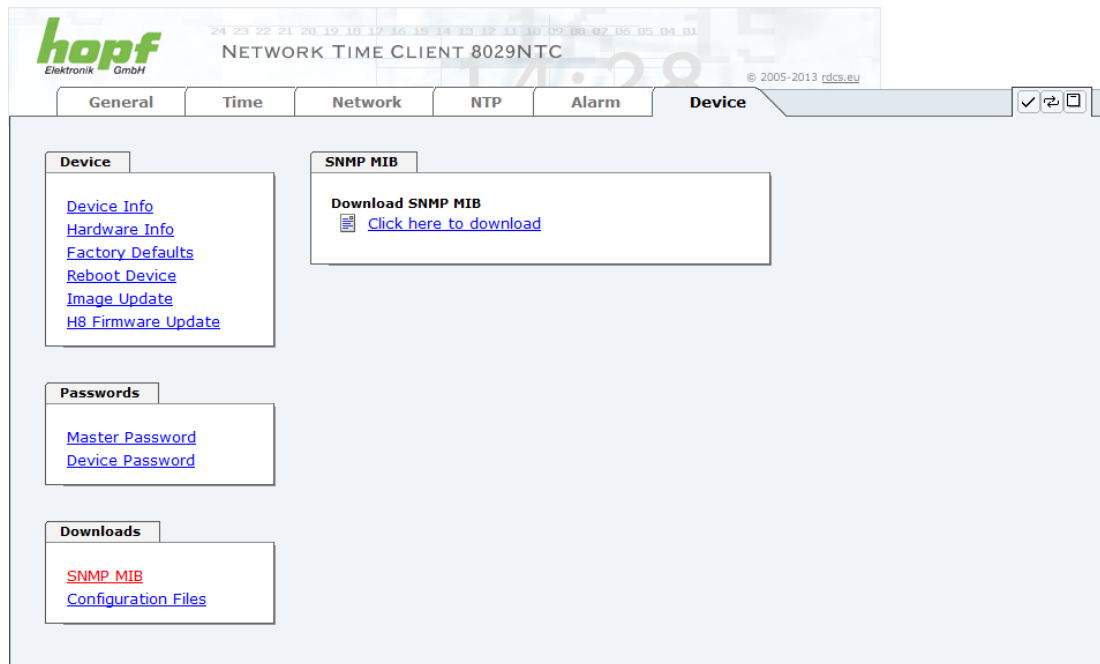
Change Device Password

New password (min. 6 characters)

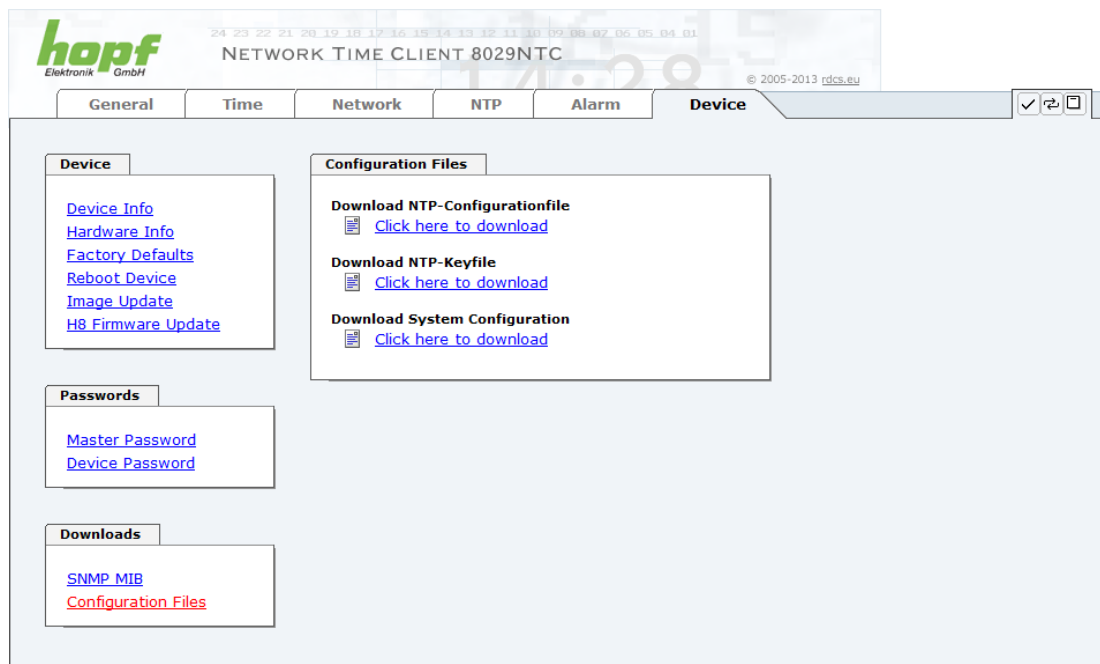
Confirm new password

7.3.6.7 Downloading SNMP MIB / Configuration Files

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



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



8 SSH and Telnet Basic Configuration



Only basic configuration is possible via SSH or Telnet. The complete configuration of the Module 8029NTC takes place exclusively via the WebGUI.

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

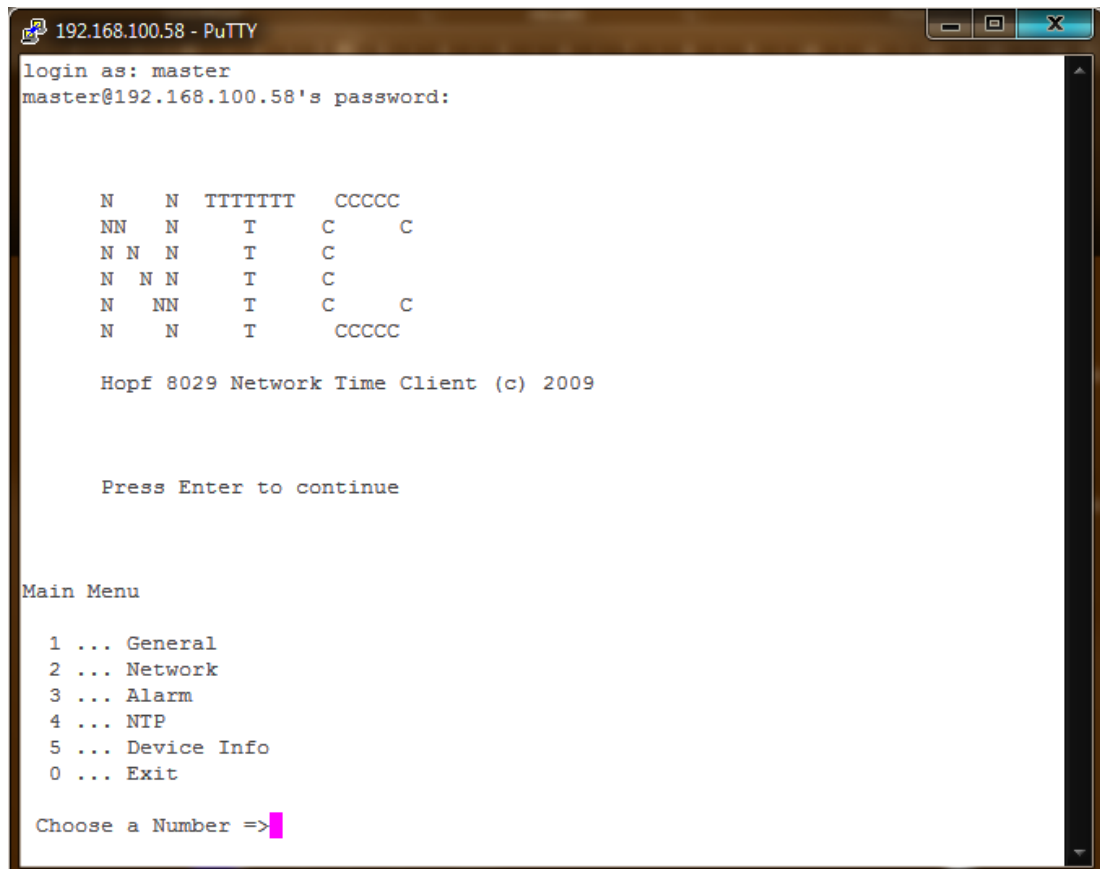
The user names and passwords are the same as on the WebGUI and are kept in alignment (see **Chapter 7.3.6.6 Passwords**).



SSH does not allow blank passwords for safety reasons.



The corresponding protocols should be enabled for the use of Telnet or SSH (see **Chapter 7.3.3.4 Management-Protocols / SNMP**).



```

192.168.100.58 - PuTTY
login as: master
master@192.168.100.58's password:

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

Hopf 8029 Network Time Client (c) 2009

Press Enter to continue

Main Menu

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

Choose a Number =>
```

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

9 Technical Data



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

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

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

LAN	
Network Connection	Via a LAN cable with RJ45 connector, male (recommended cable type CAT5 or better)
Requests 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

CE compliant to EMC Directive 89/336/EC and Low Voltage Directive 73/23/EC	
Safety / Low Voltage Directive	DIN EN 60950-1:2001 + A11 + Corrigendum
EN 61000-6-4	
EMC (Electromagnetic Compatibility) / Interference Immunity	EN 610000-4-2 /-3/-4/-5/-6/-11
EN 61000-6-2	EN 61000-3-2 /-3
Radio Interference Voltage EN 55022	EN 55022 Class B
Radio Interference Emission EN 55022	EN 55022 Class B

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

Time Protocols

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

TCP/IP Network Protocols

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

Configuration

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

Features

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

10 Factory Defaults

Usually the delivery status of the Module 8029NTC corresponds with the factory-defaults.

10.1 Network

Host/Name Service	Setting	WebGUI Presentation
Hostname	hopf8029ntc	hopf8029ntc
Default Gateway	Blank	---
DNS 1	Blank	---
DNS 2	Blank	---
Network Interface ETH0	Setting	WebGUI
DHCP	Disabled	Disabled
IP	192.168.0.1	192.168.0.1
Netmask	255.255.255.0	255.255.255.0
Operation mode	Auto negotiate	Auto negotiate
Routing	Setting	WebGUI
User Defined Routes	Blank	---
Management	Setting	WebGUI
HTTP	Enabled	Enabled
SSH	Enabled	Enabled
TELNET	Disabled	Disabled
SNMP	Disabled	Disabled
System Location	Blank	---
System Contact	Blank	---
Read Community	Blank	---
Read/Write Community	Blank	---

10.2 NTP

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

10.3 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

10.4 DEVICE

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

11 Glossary and Abbreviations

11.1 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.

11.2 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.

11.2.1 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) .

11.3 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})

11.4 Definitions

An explanation of the terms used in this document.

11.4.1 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.

11.4.2 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.

11.4.3 SNMP (Simple Network Management Protocol)

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

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

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

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

11.4.4 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.

11.5 Accuracy & NTP Basic Principles



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



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

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

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

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

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

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

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

For example:

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

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

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

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

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

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

12 List of RFCs

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

13 List of Open Source Packages used

Third Party Software

The **hopf** Time Client 8029NTC 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
boa	0.94.14rc21	GPL	V2	nein
busybox	1.13.2	GPL		nein
dosfstools	2.11	GPL	V2	nein
eeprog	0.7.6	GPL	V2	nein
ethtool	6	GPL	V2	nein
fakeroot	1.9.5	GPL	V2	nein
gettext	0.16.1	GPL	V2	nein
gmp	4.2.2	LGPL		nein
i2c-tools	3.0.2	GPL		nein
libelf	0.8.10	LGPL		nein
libevent	1.2	3-clause BSD	http://libevent.org/LICENSE.txt	nein
libblockfile	1.06.1	LGPL		nein
libtool	1.5.24	GPL	V2	nein
libusb	0.1.12	LGPL	v2	nein
lockfile-progs	0.1.11	GPL	v2	nein
lzo	2.03	GPL	v2	nein
linux	2.6.27	GPL	v2	ja
microcom	1.02	GPL	v2	nein
mpfr	2.3.2	GPL	v2	nein
ncurses	5.6	Permissive free software licence	Copyright (c) 1998-2004,2006 Free Software Foundation, Inc. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation Copyright (c) 1998-2004,2006 Free Software Foundation, Inc. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, dis-tribute with modifications, sublicense,	nein

and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT

WARRANTY OF ANY KIND, EXPRESS OR IMPLIED,

INCLUDING BUT NOT LIMITED TO THE WARRANTIES

OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN

NO

EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE

LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF

CONTRACT,

TORT OR OTHERWISE, ARISING FROM, OUT OF OR

IN CONNECTION WITH THE SOFTWARE OR THE USE

OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name(s) of the above copyright holders shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization.

ntp	4.2.4p5	NTP	Copyright (c) University of Delaware 1992-2011 Permission to use, copy, modify, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of	nein
openssh	5.1p1	BSD		nein
openssl	0.9.8g	Dual	http://www.openssl.org/source/license.html	
pkg-config	0.23	GPL	V2	nein
sysfsutils	2.1.0	GPL	V2	nein
tftp-hpa	0.40	GPL	V2	nein
udev	114	GPL	V2	nein
usbutils	0.72	GPL	V2	nein
u-boot	2009.01-rc1	GPL	V2	nein
zlib	1.2.3	Permissive free software licence	http://www.gzip.org/zlib/zlib_license.html	nein