

Industriefunkuhren



---

## **Technical Manual**

Large Matrix Display 4985  
with integrated LAN Interface

**Model 4985LAN**

**ENGLISH**

**Version: 08.01 - 25.03.2019**

---

Valid for Devices **4985LAN** with FIRMWARE Version: **08.xx**  
and REMOTE-SOFTWARE (HMC) Version: **01.13**



## **Version number (Firmware / Manual)**

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

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

## **Downloading Technical Manuals**

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

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

E-mail: [info@hopf.com](mailto: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.

<b>Contents</b>	<b>Page</b>
<b>1 Functions .....</b>	<b>9</b>
1.1 Function Principle .....	9
1.2 Housing .....	9
1.3 Initial Operation .....	10
1.3.1 Opening and Closing of Housing .....	10
1.3.2 Wall Mounting and Cable Entry .....	12
<b>2 hopf Management Console Software .....</b>	<b>13</b>
2.1 Remote-Software-Connection with large matrix display 4985LAN .....	13
2.2 Adjustment options .....	14
2.2.1 Time and Date .....	15
2.2.2 In General .....	15
2.2.3 System .....	16
2.2.4 DCF77 .....	16
2.2.5 Outputs .....	17
<b>3 Output Diagrams – Matrix Display .....</b>	<b>18</b>
3.1 Connection Failure .....	18
3.2 System and Grid Time .....	18
3.2.1 System and Grid Time small (42mm) .....	18
3.2.2 Grid and System Time (42mm) .....	18
3.2.3 System Time large (84mm) .....	18
3.2.4 Grid Time large (84mm) .....	18
3.3 Difference Time .....	19
3.3.1 Difference Time (42mm) .....	19
3.3.2 Difference Time (84mm) .....	19
3.4 Frequency/Difference Frequency .....	19
3.4.1 Frequency/Difference Frequency (42mm) .....	19
3.4.2 Frequency/Difference Frequency (42mm) .....	19
3.4.3 Frequency (84mm) .....	19
3.4.4 Difference Frequency (F3 with 84mm) .....	19
<b>4 Module Behaviour Network Time Client 8029NTC .....</b>	<b>20</b>
4.1 Boot Phase .....	20
4.2 Regulating Phase .....	20
4.2.1 NTP Adjustment Process (NTP/Stratum/Accuracy) .....	20
4.3 Reset Button .....	20
4.4 Firmware Update .....	21
4.5 Activation of Functions by Activation Keys .....	23
<b>5 HTTP WebGUI – Web Browser Configuration Interface .....</b>	<b>24</b>
5.1 Quick Configuration .....	24
5.1.1 Requirements .....	24
5.1.2 Configuration Steps .....	24

5.2 General – Introduction .....	25
5.2.1 LOGIN and LOGOUT as User .....	26
5.2.2 Navigation via the Web Interface .....	27
5.2.3 Enter or Changing Data .....	28
5.3 Description of the Tabs.....	29
5.3.1 GENERAL Tab.....	29
5.3.2 Time/Date Tab .....	31
5.3.2.1 Time Zone Offset.....	31
5.3.2.2 Configuration of Summer Time (Daylight Saving Time).....	32
5.3.3 NETWORK Tab.....	33
5.3.3.1 Host / Name Service.....	33
5.3.3.1.1 Hostname .....	33
5.3.3.1.2 Use Manual DNS Entries.....	34
5.3.3.1.3 DNS Server 1 to 3 .....	34
5.3.3.1.4 Use Manual Gateway Entries .....	34
5.3.3.1.5 Default Gateway IPv4.....	34
5.3.3.1.6 Default Gateway IPv6.....	34
5.3.3.2 Network Interface ETH0.....	35
5.3.3.2.1 Default Hardware Address (MAC) .....	35
5.3.3.2.2 Customer Hardware Address (MAC).....	36
5.3.3.2.3 DHCP .....	36
5.3.3.2.4 IPv4 Address.....	36
5.3.3.2.5 IPv4 Network Mask .....	36
5.3.3.2.6 Operation Mode.....	36
5.3.3.2.7 Maximum Transmission Unit (MTU) .....	37
5.3.3.2.8 IPv6.....	37
5.3.3.2.9 DHCP-IPv6.....	37
5.3.3.2.10 IPv6 Address .....	37
5.3.3.2.11 IPv6 Subnet Prefix Length.....	37
5.3.3.2.12 VLAN (Activation Key necessary).....	38
5.3.3.3 Routing (Activation Key necessary) .....	39
5.3.3.4 Routing File.....	40
5.3.3.5 Management (Management-Protocols – HTTP, SNMP, SNMP-Traps, etc.).....	41
5.3.3.5.1 SNMPv2c / SNMPv3 (Activation Key required) .....	43
5.3.3.6 Display.....	44
5.3.4 NTP Tab.....	46
5.3.4.1 System Info.....	46
5.3.4.2 Kernel Info .....	47
5.3.4.3 Peers .....	47
5.3.4.4 Server Configuration.....	48
5.3.4.4.1 Broadcast / Multicast.....	48
5.3.4.4.2 NTP Servers for Synchronisation .....	49
5.3.4.5 Extended Configuration .....	49
5.3.4.5.1 Definition Accuracy (Low / Medium / High).....	51
5.3.4.6 Restart NTP .....	52
5.3.4.7 Access Restrictions / Configuring the NTP Service Restrictions.....	52
5.3.4.7.1 NAT or Firewall.....	53
5.3.4.7.2 Blocking Unauthorised Access .....	53
5.3.4.7.3 Allowing Client Requests.....	54
5.3.4.7.4 Internal Client Protection / Local Network Threat Level.....	54
5.3.4.7.5 Addition of Exceptions to Standard Restrictions.....	55
5.3.4.7.6 Access Control Options .....	56
5.3.4.8 Symmetric Key.....	57
5.3.4.8.1 Why Authentication? .....	57
5.3.4.8.2 How is Authentication used in the NTP Service? .....	57
5.3.4.8.3 How is a key created? .....	57
5.3.4.8.4 How does authentication work?.....	58
5.3.4.9 Autokey / Public Key Cryptography .....	58

5.3.5	ALARM Tab.....	59
5.3.5.1	Syslog Configuration.....	59
5.3.5.2	E-mail Configuration .....	60
5.3.5.3	SNMP Configuration / TRAP Configuration .....	61
5.3.5.4	Alarm Messages .....	62
5.3.6	DEVICE Tab.....	63
5.3.6.1	Device Information .....	63
5.3.6.2	Hardware Information .....	63
5.3.6.3	Restoring Factory-Settings (Factory Defaults) .....	64
5.3.6.4	Reboot Device .....	64
5.3.6.5	Image Update & H8 Firmware Update .....	65
5.3.6.6	Upload Certificate (SSL-Server-Certificate) .....	66
5.3.6.7	Customized Security Banner .....	67
5.3.6.8	Product Activation.....	68
5.3.6.9	Diagnostics Function .....	69
5.3.6.10	Passwords Master / Device .....	69
5.3.6.11	Downloading SNMP MIB / Configuration Files.....	70
<b>6</b>	<b>SSH and Telnet Basic Configuration .....</b>	<b>71</b>
<b>7</b>	<b>Technical Data Large Matrix Display 4985 .....</b>	<b>72</b>
<b>8</b>	<b>Factory Defaults.....</b>	<b>73</b>
8.1	Network.....	73
8.2	NTP .....	74
8.3	ALARM.....	74
8.4	DEVICE.....	74
<b>9</b>	<b>Glossary and Abbreviations .....</b>	<b>75</b>
9.1	NTP-specific Terminology.....	75
9.2	Tally Codes (NTP-specific) .....	75
9.2.1	Time-specific expressions.....	76
9.3	Abbreviations.....	77
9.4	Definitions .....	78
9.4.1	DHCP (Dynamic Host Configuration Protocol) .....	78
9.4.2	NTP (Network Time Protocol) .....	78
9.4.3	SNMP (Simple Network Management Protocol).....	79
9.4.4	TCP/IP (Transmission Control Protocol / Internet Protocol) .....	79
9.5	Accuracy & NTP Basic Principles .....	79
<b>10</b>	<b>List of RFCs.....</b>	<b>81</b>
<b>11</b>	<b>List of Open Source Packages used .....</b>	<b>82</b>





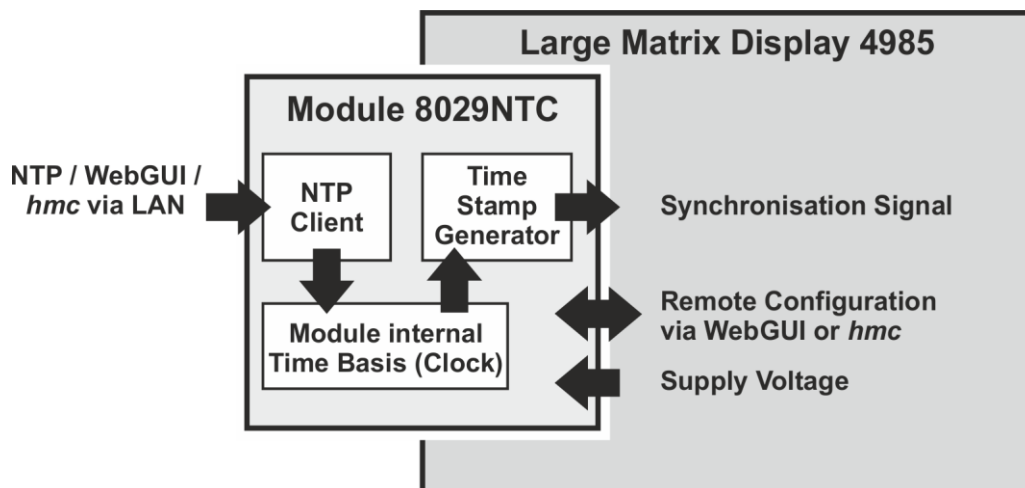
# 1 Functions

The large matrix display 4985LAN consists of a large display with a matrix measuring 16x64 LED and a NTP Time Client Module 8029NTC.

Two lines of 42 mm or one line of 84 mm alphanumeric characters can be displayed on this matrix.

Time and date can be displayed in different formats.

## 1.1 Function Principle



## 1.2 Housing

The large display is set up in a black lacquered aluminium housing for wall installation.

The front panel is of red and of coated acrylic glass and fixed into guiding rails of the housing.

For installation and configuration of the large display the right-side panel of the housing and the front panel should be pulled to the right. The side panel of housing is mounted into guiding rails with spring locks.



## 1.3 Initial Operation

The large display 4985 is delivered in its casing ready for operation. It is now only necessary to install the connections required for operation.

### 1.3.1 Opening and Closing of Housing

For installation of the display the right-side panel of the housing needs to be removed. The right-side panel is fixed into the housing by spring locks.

#### Opening of housing

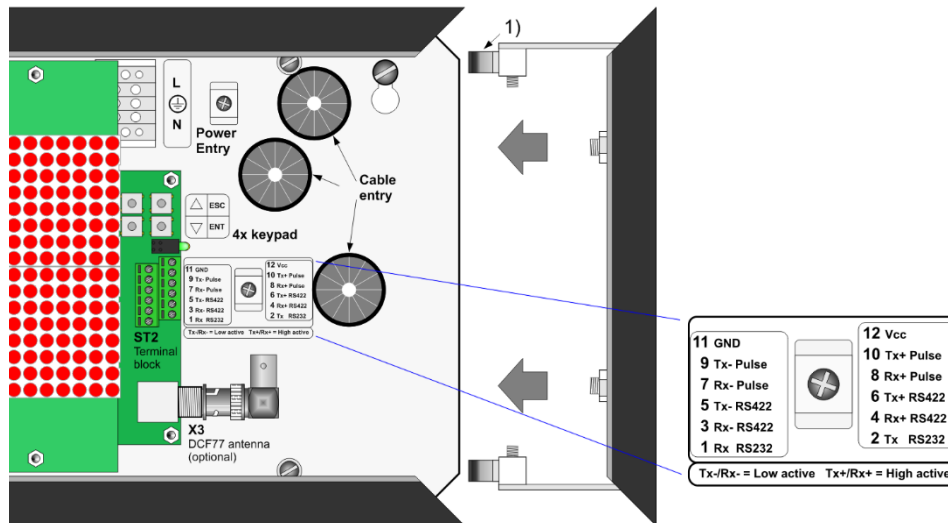


- Pull the right-side panel to the right out of the housing  
(ATTENTION: DO NO JAM)
- When pulling out, override the pressure point of the spring locks **at the top** first and then **at the bottom** (traction approximately 50N – corresponding with at driving power of approximately 5kg)
- Pull the front panel to the right out of the housing



Pay attention to a secure hold when opening the large display.

### Closing the housing



No signals may be connected to terminal block ST2 of the large matrix display 4985LAN since these signals are controlled by the NTP Time Client module 8029NTC.

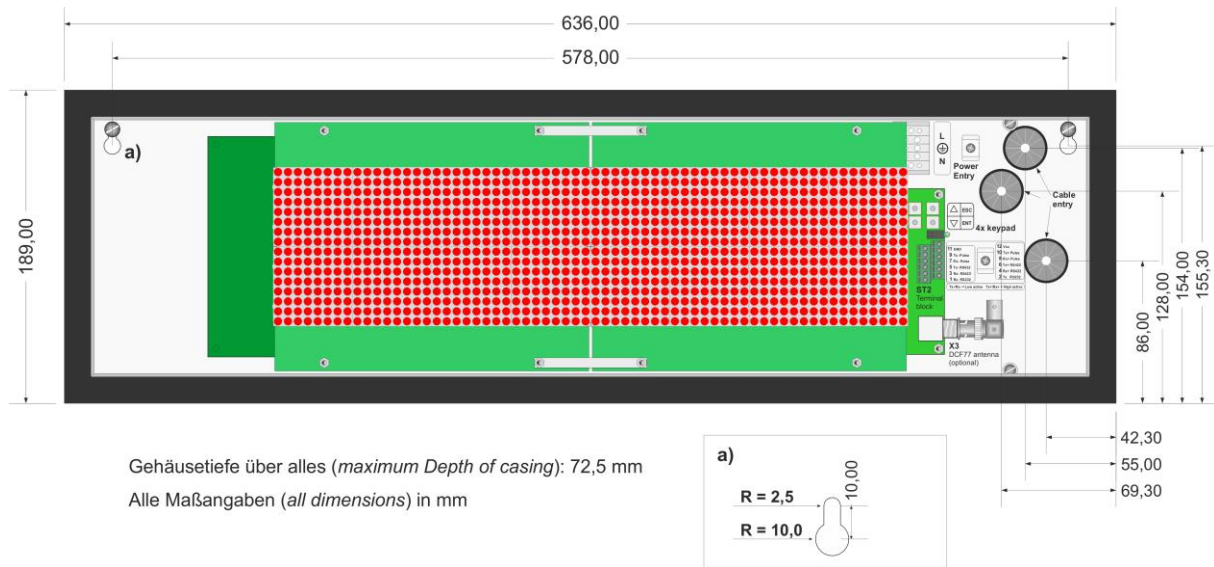
- Push the front panel in the front guiding rails of the housing (coated side of front panel outside)
- Insert the fixing brackets of the side panel in the appropriate guiding rails of the housing at the top and bottom (ATTENTION: DO NO JAM)
- When snapping the side panel into the housing pay attention to the fact that the front panel and the rear panel are placed in the appropriate guiding rails of the side panel
- When snapping in, the pressure point of the spring locks (1) must be overridden



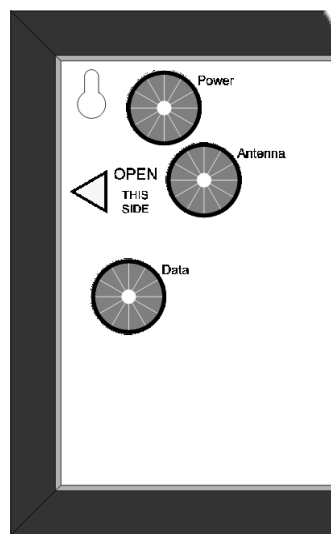
Pay attention to a secure hold when closing the large display.

### 1.3.2 Wall Mounting and Cable Entry

The large display is mounted at the wall by fixing apertures (a) in the rear panel.

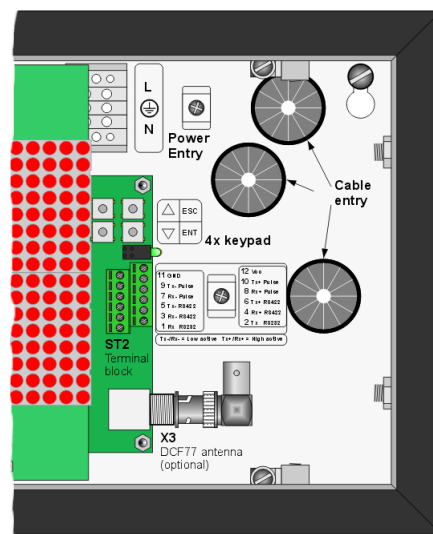


For cable entry (power supply, antenna cable and data cable) there are three marked openings available.



Backside Housing

After connection, the cables should be fixed with the according strain relief into the housing.



Installation and commissioning may only be carried out by suitable specialist personnel. In doing so the respective country-specific regulations (e.g. VDE, DIN) are to be observed.

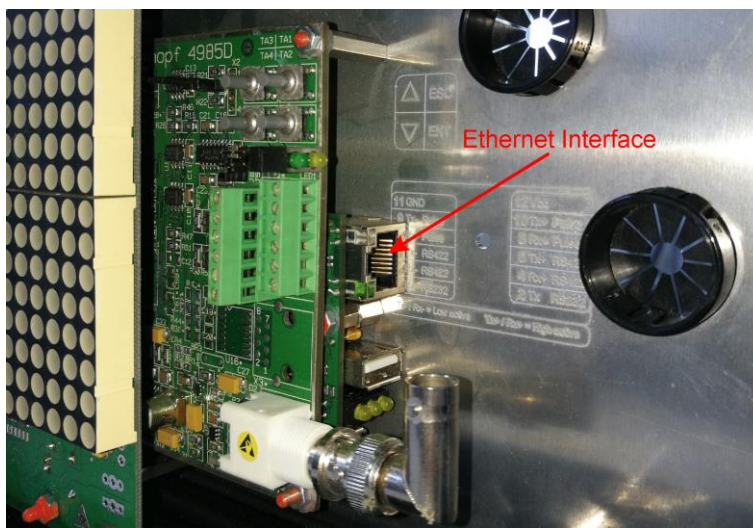
## 2 **hopf** Management Console Software

The **hmc** (**hopf** management console) is the remote software to setup the board 4985 and can be found on the **hopf** CD or in our download area [https://www.hopf.com/hmc\\_en.html](https://www.hopf.com/hmc_en.html).

Please look at the description of the **hmc** remote software for the minimum system requirements for the client PC.

### 2.1 Remote-Software-Connection with large matrix display 4985LAN

The large matrix display 4985LAN will be connected with a suitable computer via the ethernet interface of the 8029NTC module. After connecting please switch on both appliances and start the remote software.

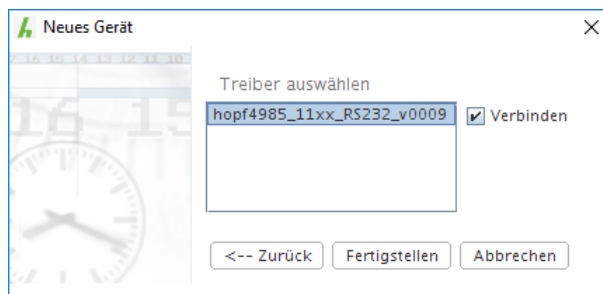


When installing the new device in the remote software the communication canal **RS232 / TCP/IP** needs to be chosen. State the host name respectively the IP address of large matrix display 4985LAN and make sure that the port matches to the details that have been adjusted in the WebGUI (as described in **Chapter 5.3.3.5 Management (Management-Protocols – HTTP, SNMP, SNMP-Traps, etc.)**).

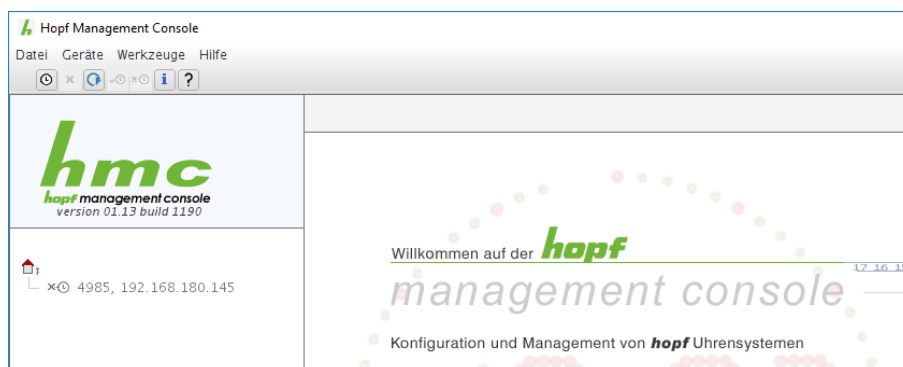
Subsequently make a request about the device name and the firmware of the large matrix display via these settings.



Afterwards choose the appropriate driver and click „Connect“.



The large matrix display is now connected with the **hopf** management console (**hmc**).

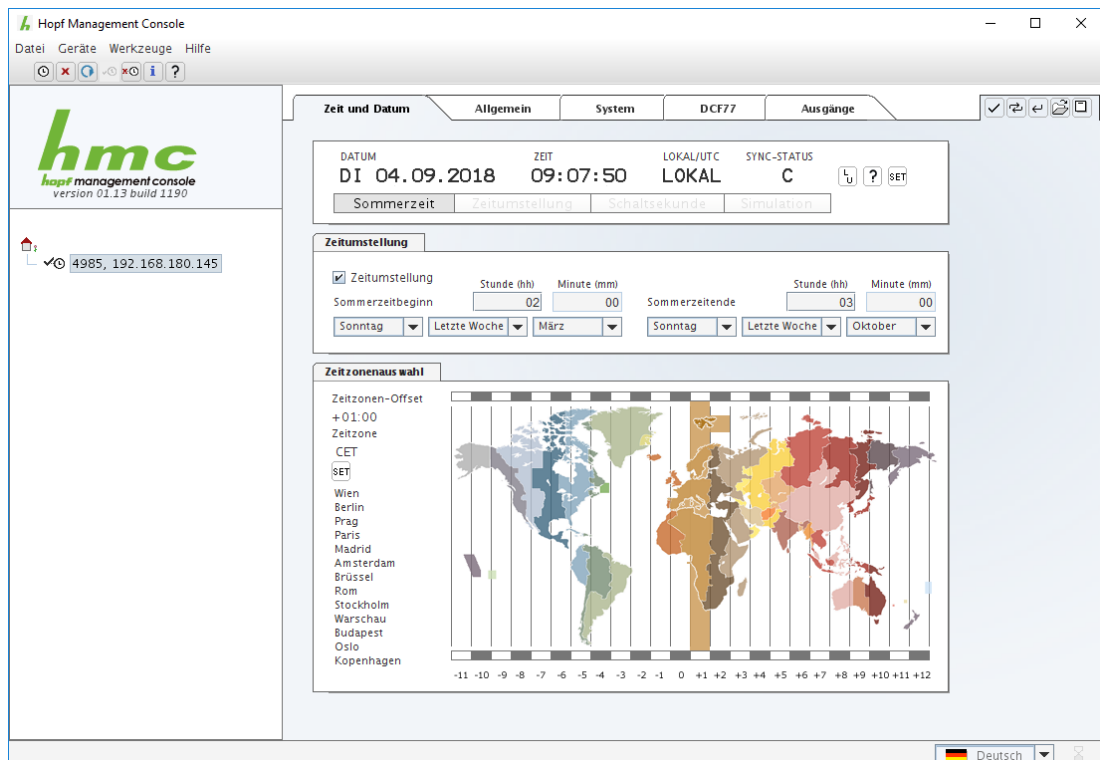


## 2.2 Adjustment options

After successful connection of large matrix display 4985LAN with the **hopf** Management Console Software, various settings for the large matrix display can be carried out by using the **hmc** software. Furthermore various status information can be queried.

Data will be shown in several tabs of the remote software which will be described in the following chapters.

## 2.2.1 Time and Date

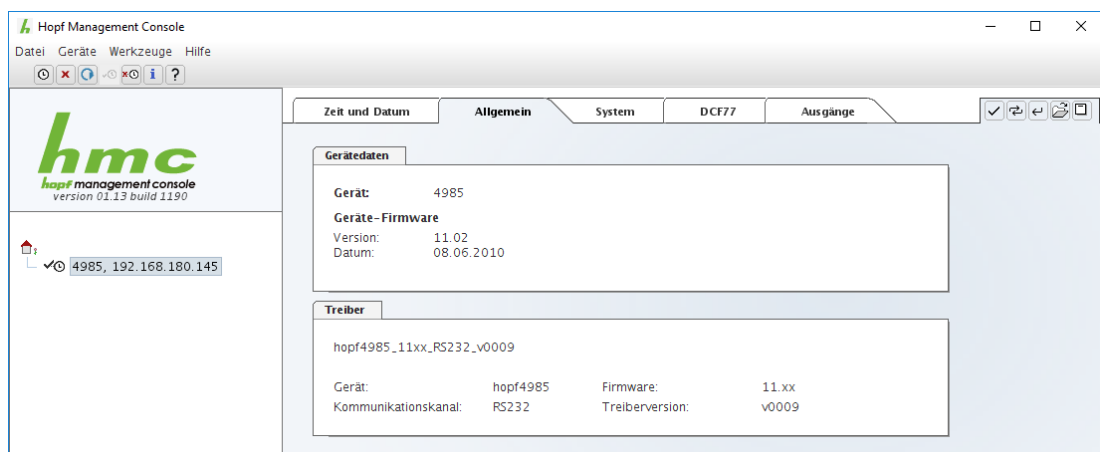


This page is necessary for adjusting and displaying the time zone, summer and winter time, points of time changeovers and the current time.



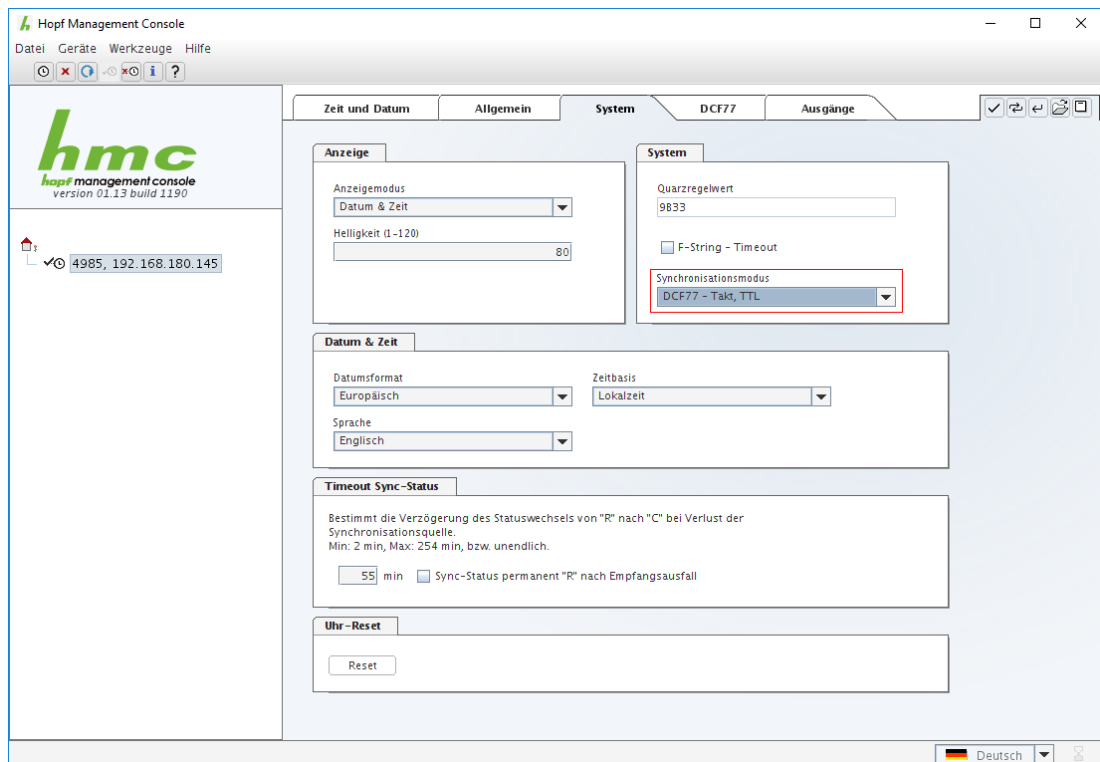
To enable a correct functionality it is necessary to make these adjustments via the WebGUI of large matrix display 4985LAN.

## 2.2.2 In General



This page shows several device data of the large matrix display as well as the version data of the remote software driver in use.

## 2.2.3 System



On this page you can adjust which information of the large matrix display should be outputted. Furthermore you can configure the synchronization behaviour of the large matrix display and you trigger a reset of the large matrix display.



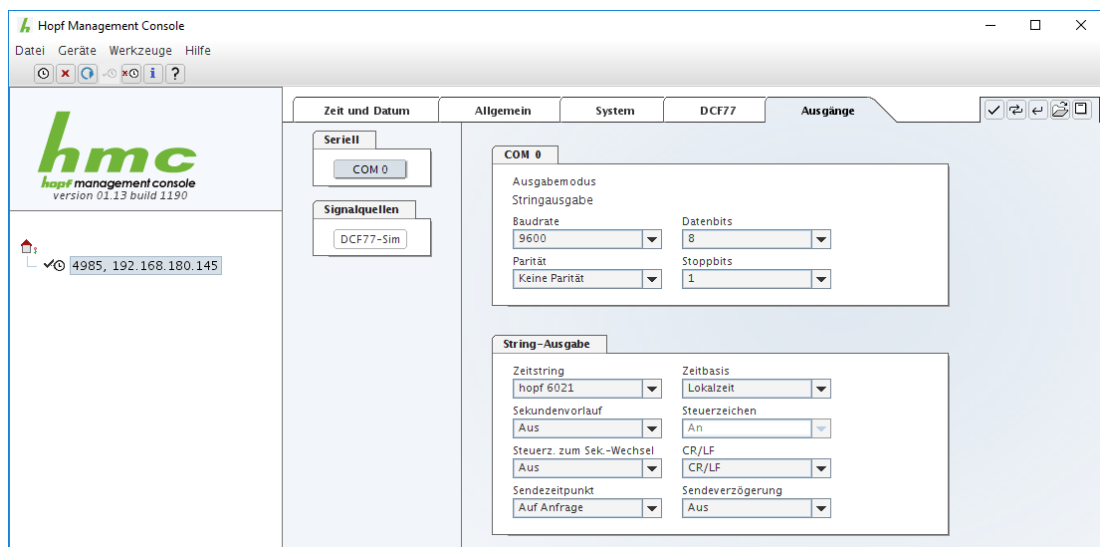
The synchronization mode for system 4985LAN needs to be adjusted to **"DCF77-pulse, TTL"**.

## 2.2.4 DCF77

This register is not necessary for operating the 4985LAN.



## 2.2.5 Outputs



This page enables to configure the output interfaces.



A serial output will not be supported by the large matrix display 4985LAN.

### 3 Output Diagrams – Matrix Display

Unless otherwise indicated all values are given in 2 digits without operational sign.

#### 3.1 Connection Failure

The behaviour of display 4985 in case connection failure to board 7515(RC) can parameterized via Remote Software / System Tab).

Timeout for F-string activated: 5 seconds after F-string failure the message CONNECTION LOST appears.

Timeout for F-string disabled: The last indicated display is permanently shown.

#### 3.2 System and Grid Time

##### 3.2.1 System and Grid Time small (42mm)

1<sup>st</sup> line: "Sy" hour:minute:second (system time)

2<sup>nd</sup> line: "N1" hour:minute:second (grid time)

Example:      **Sy 12:34:56**  
                 **N1 12:34:57**

##### 3.2.2 Grid and System Time (42mm)

1<sup>st</sup> line: "N1" hour:minute:second (grid time)

2<sup>nd</sup> line: "Sy" hour:minute:second (system time)

Example:      **N1 12:34:57**  
                 **Sy 12:34:56**

##### 3.2.3 System Time large (84mm)

One line: hour:minute:second (system time)

Example:      **12:34:56**

##### 3.2.4 Grid Time large (84mm)

One line: hour:minute:second (grid time)

Example:      **12:34:57**

### 3.3 Difference Time

#### 3.3.1 Difference Time (42mm)

1<sup>st</sup> line: "t" operational sign hour:minute:second

2<sup>nd</sup> line: milliseconds

Example:      **t + 00:00:06**  
                         **447**

#### 3.3.2 Difference Time (84mm)

One line: operational sign seconds, milliseconds

Example:      **+ 06,447**



Display up to  $\pm 99,999$ . In case of overflow  $\pm 99,999$  is displayed.

### 3.4 Frequency/Difference Frequency

#### 3.4.1 Frequency/Difference Frequency (42mm)

1<sup>st</sup> line: "f1" frequency with 2 pre- and 3 post-comma digits "Hz"

2<sup>nd</sup> line: "df" difference frequency with 2 pre- and 3 post-comma digits "Hz"

Example:      **f1 49,998 Hz**  
                         **df -00,002 Hz**

#### 3.4.2 Frequency/Difference Frequency (42mm)

1<sup>st</sup> line: "df" difference frequency with 2 pre- and 3 post-comma digits "Hz"

2<sup>nd</sup> line: "f1" frequency with 2 pre- and 3 post-comma digits "Hz"

Example:      **df +00,002 Hz**  
                         **f1 50,002 Hz**

#### 3.4.3 Frequency (84mm)

One line: frequency with 2 pre- and 3 post-comma digits

Example:      **49,998**

#### 3.4.4 Difference Frequency (F3 with 84mm)

One line: operational sign and frequency with 2 pre- and 3 post-comma digits

Example:      **+00,002**

## 4 Module Behaviour Network Time Client 8029NTC

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

### 4.1 Boot Phase

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

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

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



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

### 4.2 Regulating Phase

After the boot phase, the NTP service is started automatically.

After starting the NTP service, the device will take about 5-10 minutes, depending on the accuracy and availability of the time servers configured in the card, to regulate the internal clock.

#### 4.2.1 NTP Adjustment Process (NTP/Stratum/Accuracy)

NTP is a regulation process. After starting the NTP services, automatically processed during booting, the Network 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 Network Time Client 8029NTC can be reset by the Reset-(Default) Button behind the front panel of the board. The Reset-(Default) Button is accessible with a thin objective through the small drilling in the front panel.

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

Duration	Function
< 1 sec.	No action
1 - 9 sec.	After releasing a <b>hardware reset</b> is triggered in the module
$\geq 10$ sec.	After releasing a <b>FACTORY DEFAULT</b> followed by a <b>REBOOT</b> is triggered after approx. 10 seconds

## 4.4 Firmware Update

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

### Module 8029NTC:

1x Image Update	upgrade_8029NTC_vXXXX.img
1x H8 Update	8029NTC_128.mot



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



All programs of a SET need 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:



For selection of the correct update set the identifier **8029NTC** has to be observed obligatory.

8029NTC can be recognized:

- By the label on the housing cover "**8029NTC**"
- In WebGUI at the Web-banner "**8029NTC**"

The firmware update 8029NTC has to be performed as a SET.

The software package contained in the file package hopf8029NTC\_SET\_vXXXX.zip has to be unpacked. The following steps have to be executed in the following sequence:

1. **Image Update 8029NTC**
2. **H8 Firmware Update 8029NTC**

### Image Update

1. Log in as Master in WebGUI of the board.
2. Select in **Device** tab the menu item **Image Update**.
3. Select the file with the file **.img** via the selection window (Example: **upgrade\_8029NTC\_vXXXX.img**).
4. The selected file is shown in the selection window.
5. The update process is started with the button **Upload now**.
6. In WebGUI the successful file transfer and writing to the Module is indicated.
7. In WebGUI the successful update is indicated after 2-3 minutes with the request to release a reboot of the board.
8. After activation and successful reboot of the board the image update process is finished.

### H8 Firmware Update

1. Log in as Master in WebGUI of the board.
2. Select in the **Device** tab the menu item **H8 Firmware Update**.
3. Select the file with the file extension **.mot for Module 8029NTC** via the selection window (Example: **8029NTC\_128.mot**).
4. The selected file is shown in the selection window.
5. The update process is started with the button **Upload now**.
6. In WebGUI the successful file transfer to the Module is indicated.
7. Now the update of the board automatically starts after a few seconds.
8. After successful update the board automatically reboots.
9. After approx. 2 minutes the H8 update process is finished and the board is again accessible via WebGUI.

## 4.5 Activation of Functions by Activation Keys

The Network Time Client 8029NTC offers several functions that require an "Activation Key".

These functions are only available after entering a valid activation key related to the serial number of the Module 8029NTC (not the serial number of the overall system). The serial number can be found in the WebGUI via Device / Serial Number: 8029xxxxxx.

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



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

Please find an overview of the above mentioned functions here:

- **Static Routing Tables**

This function is suitable for configuring static routes based on special network configuration requirements in the Network Time Client 8029NTC.

- **Alarming and Management features**

This function enables to use **SNMP (SNMPv2c, SNMPv3), Syslog and Email notification** to monitor the system status. Together with the assets provided in the MIB II by default, the **hopf** Private Enterprise MIB is also made available. By using the **hopf** Private Enterprise MIB numerous product-specific assets for realizing extended management and control functions are available.

- **IEEE 802.1QTagged VLAN**

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



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

## 5 HTTP WebGUI – Web Browser Configuration Interface



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

### 5.1 Quick Configuration

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

#### 5.1.1 Requirements

- Ready-for-operation **hopf** Large Scale Display 4985LAN
- PC with installed web browser (e.g. Internet Explorer) in the sub-network of Large Scale Display 4985LAN

#### 5.1.2 Configuration Steps

- Create the connection to the Large Scale Display 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 Large Scale Display 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.



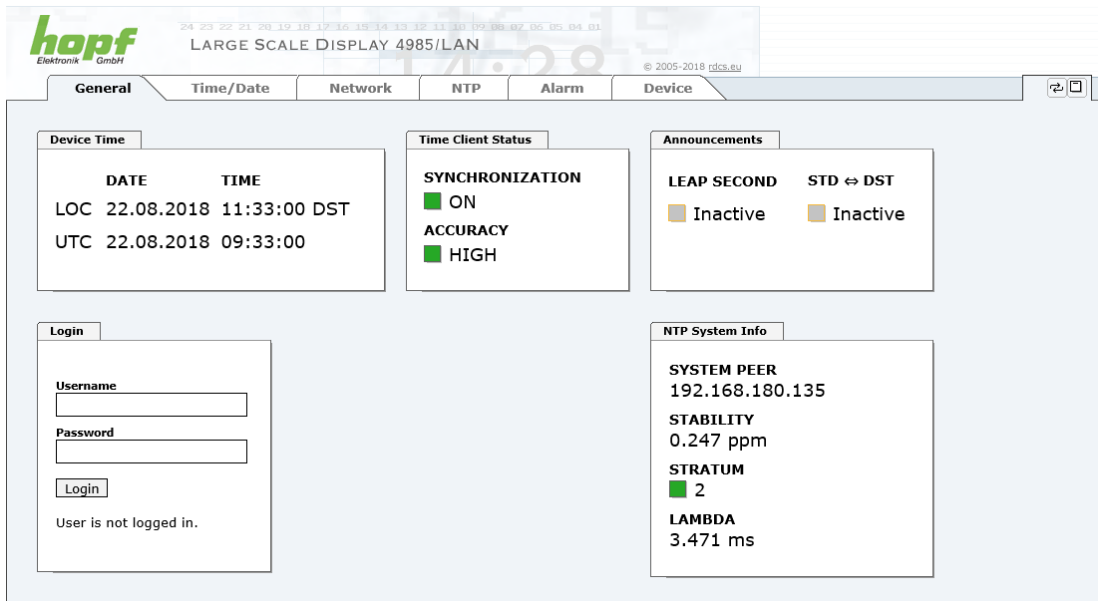
## 5.2 General – Introduction

The Large Scale Display 4985LAN should be accessible to a web browser if it has been set up correctly. Enter the IP address - as set up in the Large Scale Display earlier - or the DNS name on the address line <<http://xxx.xxx.xxx.xxx>> and the following screen should appear.

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



The complete configuration can only be done via the modules in WebGUI!



The screenshot shows the WebGUI interface for the Large Scale Display 4985/LAN. The interface has a header with the hopf logo and a navigation bar with tabs: General, Time/Date, 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	22.08.2018	11:33:00 DST
UTC	22.08.2018	09:33:00
- Time Client Status:** Shows synchronization status (ON) and accuracy (HIGH).
 

SYNCHRONIZATION
ON

ACCURACY
HIGH
- Announcements:** Shows the status of LEAP SECOND and STD ⇌ DST. Both are currently Inactive.
 

LEAP SECOND	STD ⇌ DST
Inactive	Inactive
- Login:** A section with fields for Username and Password, a Login button, and a message stating "User is not logged in."
 

Username:   
 Password:   
 Login  
 User is not logged in.
- NTP System Info:** Shows system peer information, stability, stratum, and lambda.
 

SYSTEM PEER	192.168.180.135
STABILITY	0.247 ppm
STRATUM	2
LAMBDA	3.471 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.

## 5.2.1 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> )

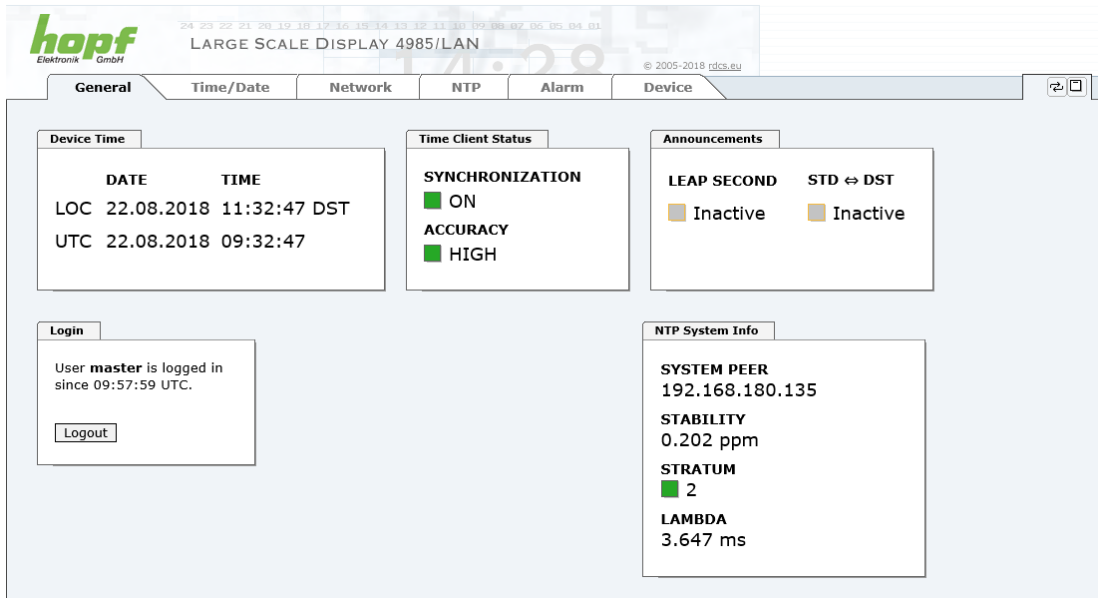


Differentiation is made between **upper and lower case** characters in the password. Alphanumeric characters and the following symbols can be used: . , ! " \$ % & / { } [ ] ( ) = ? \ + - @ \* ~ # ' < > | ; : \_



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:



The screenshot displays the Hopf WebGUI interface for the 'LARGE SCALE DISPLAY 4985/LAN'. The top navigation bar includes tabs for General, Time/Date, Network, NTP, Alarm, and Device. The main content area is divided into several panels:

- Device Time:** Shows the current date and time for both the device (LOC) and the network (UTC).
 

	DATE	TIME
LOC	22.08.2018	11:32:47 DST
UTC	22.08.2018	09:32:47
- Time Client Status:** Shows the synchronization status.
 

SYNCHRONIZATION
ON

ACCURACY
HIGH
- Announcements:** Shows the status of leap seconds and DST.
 

LEAP SECOND	STD ⇌ DST
Inactive	Inactive
- Login:** Shows the user 'master' is logged in since 09:57:59 UTC. A 'Logout' button is visible.
- NTP System Info:** Shows system parameters.
 

SYSTEM PEER
192.168.180.135

STABILITY
0.202 ppm

STRATUM
2

LAMBDA
3.647 ms

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

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

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

Users logged in as "master" have all access rights to the Large Scale Display 4985LAN.

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

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

## 5.2.2 Navigation via the Web Interface

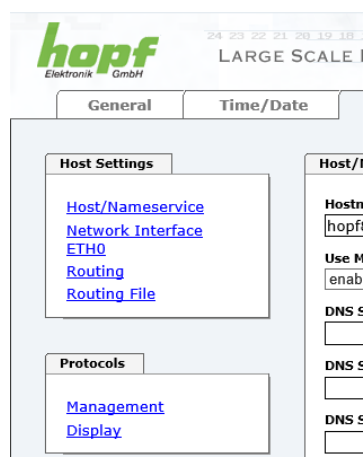
The WebGUI is divided into functional tabs. Click on one of these tabs to navigate through the board. The selected tab is identified by a darker background colour - see the following image (General in this case).



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.



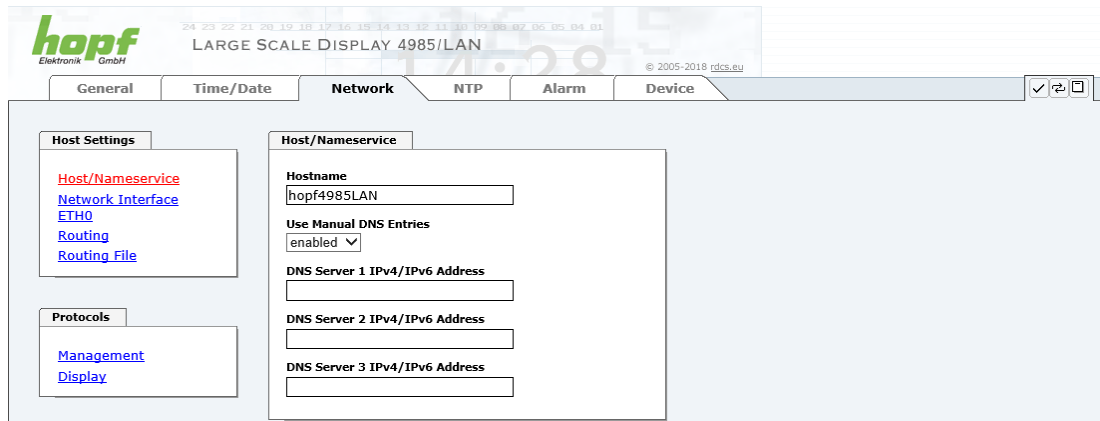
All the links within the tabs on the left hand side lead to corresponding detailed display or setting options.

### 5.2.3 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	<b>Apply</b>	Acceptance of changes and entered data
2	<b>Reload</b>	Restoring the saved data
3	<b>Save</b>	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.

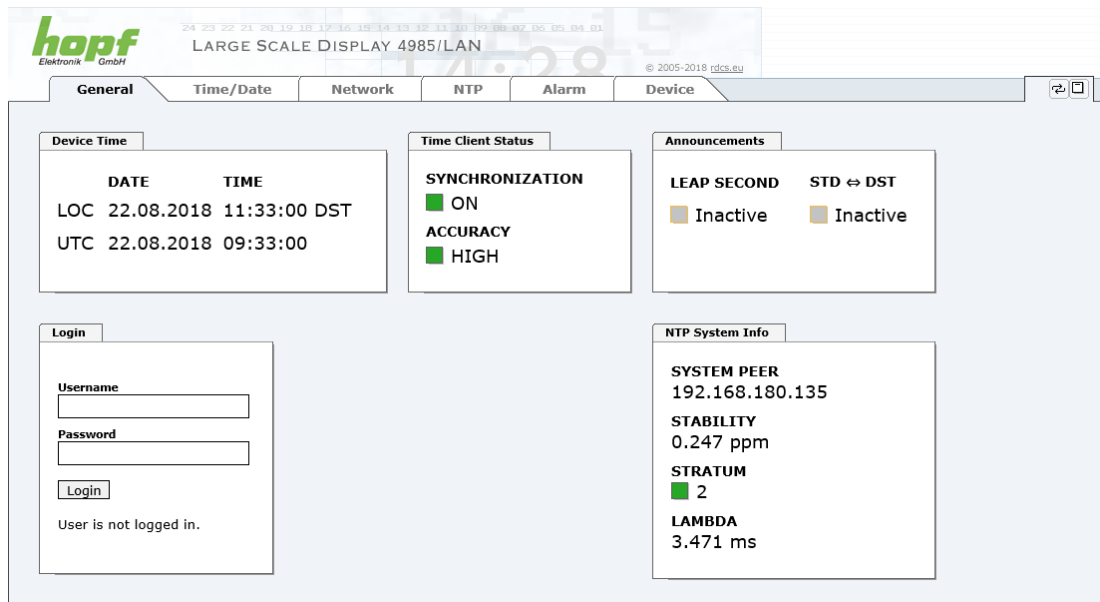
## 5.3 Description of the Tabs

The WebGUI is divided into the following tabs:

- General
- Time/Date
- Network
- NTP
- Alarm
- Device

### 5.3.1 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 and the Large Matrix Display 4985 via WebGUI.



The screenshot shows the 'General' tab of the hopf WebGUI. At the top, there is a header with the hopf logo, a large digital display showing '24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 09 08 07 06 05 04 03', and the text 'LARGE SCALE DISPLAY 4985/LAN' and '© 2005-2018 rdcs.eu'. Below the header is a navigation bar with tabs: General, Time/Date, 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	22.08.2018	11:33:00 DST
UTC	22.08.2018	09:33:00
- Time Client Status:** A section showing the synchronization and accuracy status.
 

SYNCHRONIZATION	<input checked="" type="checkbox"/> ON
ACCURACY	<input checked="" type="checkbox"/> HIGH
- Announcements:** A section showing the status of leap seconds and standard time (STD) to daylight saving time (DST) transitions.
 

LEAP SECOND	<input type="checkbox"/> Inactive
STD ⇌ DST	<input type="checkbox"/> Inactive
- Login:** A section with a login form.
 

Username	<input type="text"/>
Password	<input type="password"/>
<input type="button" value="Login"/>	
User is not logged in.	
- NTP System Info:** A section showing NTP system information.
 

SYSTEM PEER	192.168.180.135
STABILITY	0.247 ppm
STRATUM	<input checked="" type="checkbox"/> 2
LAMBDA	3.471 ms

#### Login

The **Login** box is used in accordance with **Chapter 5.2.1 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 5.3.2 Time/Date Tab**). In addition to the local time the daylight saving time (DST) / and standard time (STD) is indicated.

### Time Client Status

#### SYNCHRONIZATION

Indicates the synchronization status of the internal time output. This value describes whether the connected components/devices can use the time information of Module 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 Network Time Client) can include the possible values LOW - MEDIUM - HIGH. The meaning of those values is explained in **Chapter 9.5 Accuracy & NTP Basic Principles**.



By default the accuracy 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 (with NTP activated)

#### 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.

### 5.3.2 Time/Date Tab

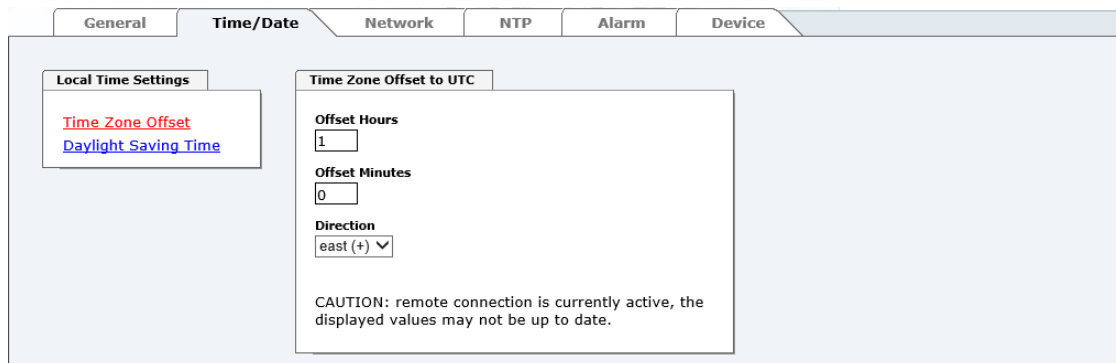
Generally, Module 8029NTC uses the time basis UTC. The configuration of difference time (**Time Zone Offset to UTC**) is required for calculating the local standard time (winter time).

#### 5.3.2.1 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)

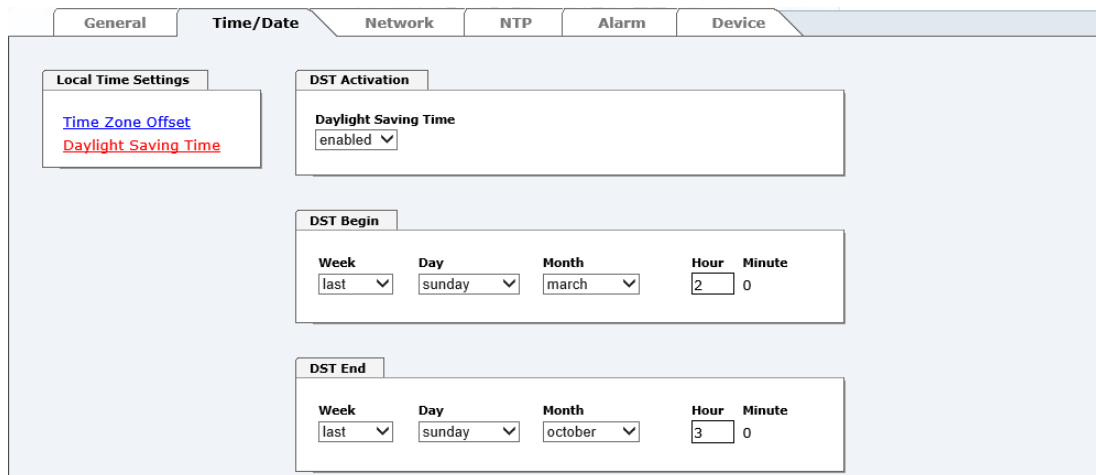
### 5.3.2.2 Configuration of Summer Time (Daylight Saving Time)

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.



The screenshot shows the 'Time/Date' tab in the configuration interface. Under 'Local Time Settings', there are links for 'Time Zone Offset' and 'Daylight Saving Time'. The 'DST Activation' section has a dropdown set to 'enabled'. The 'DST Begin' section shows settings for Week (last), Day (sunday), Month (march), Hour (2), and Minute (0). The 'DST End' section shows settings for Week (last), Day (sunday), Month (october), Hour (3), and Minute (0).

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

The individual items have the following meanings:

<b>Week</b>	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
<b>Day</b>	The day of the week when the changeover should be processed	Sunday, Monday ... Saturday
<b>Month</b>	the month when the changeover should be processed	January, February ... December
<b>Hour Minute</b>	The time in hour and minute when the changeover should be processed	00h ... 23h 00min ... 59min

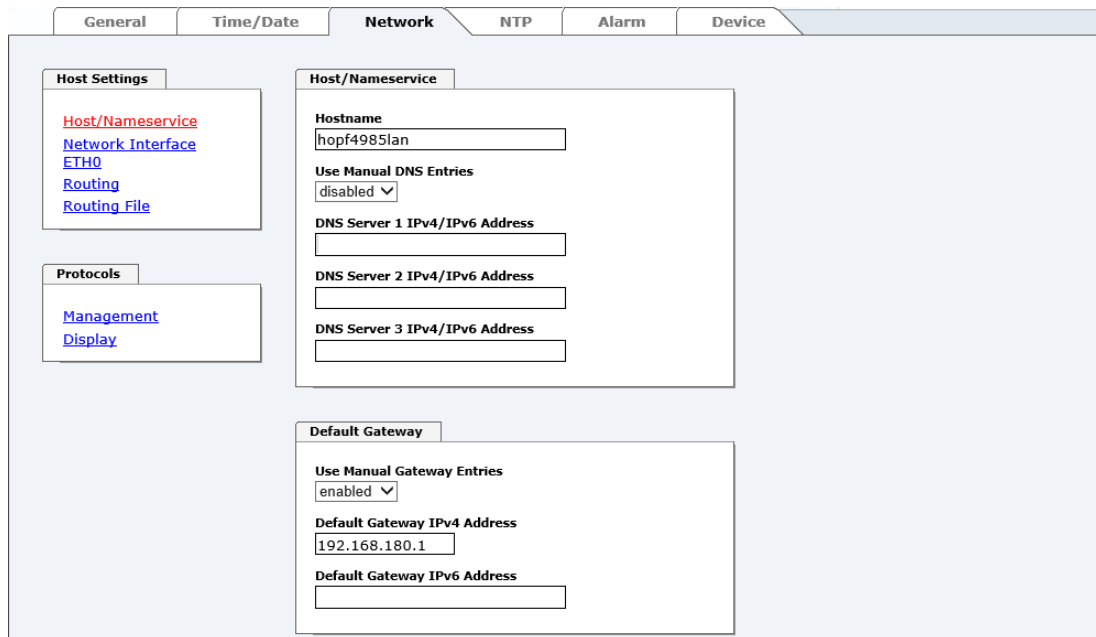


The data are entered on the basis of the local time.



### 5.3.3 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.

#### 5.3.3.1 Host / Name Service

Setting for the unique network identification.

##### 5.3.3.1.1 Hostname

The standard setting for the Hostname is "**hopf4985lan**". 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.

### 5.3.3.1.2 Use Manual DNS Entries

With this setting you can select if the manually entered DNS servers of the Network Time Client 8029NTC (DNS servers 1 to 3) should be used.

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

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



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

### 5.3.3.1.3 DNS Server 1 to 3

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

### 5.3.3.1.4 Use Manual Gateway Entries

With this setting, you can select if the manually entered gateways of the Network Time Client 8029NTC (Default Gateway IPv4 and Default Gateway IPv6) should be used.

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

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



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

### 5.3.3.1.5 Default Gateway IPv4

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

### 5.3.3.1.6 Default Gateway IPv6

If the IPv6 default gateway is not known, it must be requested from the network administrator.  
If no standard gateway is available (special case), enter :: in the input field or leave the field blank.

### 5.3.3.2 Network Interface ETH0

Configuration of the Ethernet interface ETH0 of the Time Client 8029NTC

General	Time/Date	Network	NTP	Alarm	Device
<div> <div> <b>Host Settings</b>  <a href="#">Host/Nameservice</a>  <a href="#">Network Interface</a>  <b>ETH0</b>  <a href="#">Routing</a>  <a href="#">Routing File</a> </div> <div> <b>Protocols</b>  <a href="#">Management</a>  <a href="#">Display</a> </div> </div>					
<div> <div> <b>ETH0 IPv4 Settings</b>  <b>Link Status</b>  Up  <b>Default Hardware Address (MAC)</b>  00:03:C7:01:9E:C2  <b>Use Custom Hardware Address (MAC)</b>  disabled  <b>Custom Hardware Address (MAC)</b>    <b>DHCP</b>  disabled  <b>IPv4-Address</b>  192.168.180.145  <b>IPv4-Network Mask</b>  255.255.252.0  <b>Operation mode</b>  Auto negotiate  <b>Maximum Transmission Unit (MTU)</b>  1356 </div> <div> <b>ETH0 IPv6 Settings</b>  <b>Use IPv6 Settings</b>  disabled  <b>DHCP-IPv6</b>  disabled  <b>IPv6-Address</b>    <b>IPv6 Subnet Prefix Length</b>    </div> </div>					
<div> <b>VLAN</b>  Feature is not activated! Please contact sales to purchase an activation key. </div>					

#### 5.3.3.2.1 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.



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

### 5.3.3.2.2 Customer Hardware Address (MAC)

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



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

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

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



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



There are no MAC multicast addresses allowed!

Finally, the Network Time Client 8029NTC has to be restarted via "Device" / "Reboot Device" (see **Chapter 5.3.6.4 Reboot Device**).

### 5.3.3.2.3 DHCP

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

### 5.3.3.2.4 IPv4 Address

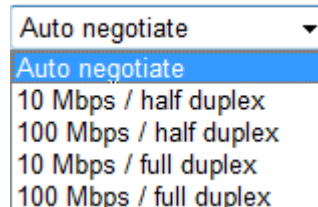
If DHCP is not used, the IPv4 address needed to be entered here. Contact your network administrator for details of the used IPv4 address if not known.

### 5.3.3.2.5 IPv4 Network Mask

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

### 5.3.3.2.6 Operation Mode

#### 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.



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

In such cases it is recommended to set the network speed of the Time Client 8029NTC **and** the connected network components manually to the same value.

#### 5.3.3.2.7 Maximum Transmission Unit (MTU)

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

Network Time Client 8029NTC is going to be delivered with default setting 1356.

#### 5.3.3.2.8 IPv6

The Network Time Client 8029NTC can also be operated in an IPv6 network.

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

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

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

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

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

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

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

#### 5.3.3.2.9 DHCP-IPv6

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

#### 5.3.3.2.10 IPv6 Address

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

#### 5.3.3.2.11 IPv6 Subnet Prefix Length

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

#### 5.3.3.2.12 VLAN (Activation Key necessary)

A VLAN (Virtual Local Area Network) is a logical sub-network within a network switch or a whole physical network. VLANs are used to separate the logical network infrastructure from the physical wiring, thus to virtualize the Local Area Network. The technology of VLAN is standardized by IEEE Standard 802.1q. Network applications like Network Time Client 8029NTC, implementing the standard IEEE 802.1q, are able to allocate individual network interfaces to specific VLANs. To transfer data packets of several VLANs via a single network interface the data packets are marked with a related VLAN ID. This method is called VLAN-Tagging. The network application at the other end of the line (e.g. network switch, router etc.) can allocate the data packet to the correct VLAN by checking the marking / tag.

VLAN

Activation Status

disabled ▾

VLAN Interfaces

Add

Remove

ID	Label	Remark	DHCP	IPv4-Address	IPv4-Network Mask
----	-------	--------	------	--------------	-------------------

### WebGUI with activated VLAN

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

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

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

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

VLAN

Activation Status

enabled ▾

VLAN Interfaces

Add

Remove

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



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



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

### 5.3.3.3 Routing (Activation Key necessary)

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

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



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

#### WebGUI with Routing activated

Current System Routing Table

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

User Defined Routes

Use Route File

disabled ▾

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 static routes.



The module cannot be used as a router!

By selecting **Use Route File** you can set up whether the under **User Defined Routes** set routing configuration should be used, or if routing configuration should take place by using a routing file.



If IPv6 routes are required, the routes must be made using the settings in **Chapter 5.3.3.4 Routing File**

#### 5.3.3.4 Routing File

In order to activate this function, **Use Route File** must be set to **enabled** on the Routing Page (see **Chapter 5.3.3.3 Routing (Activation Key necessary)**).

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


Routing File

Update file:

Durchsuchen...

Upload now

Download Routing File


[Click here to download](#)

Current System Routing Table

Network/Host	Network Mask	Gateway	Network Interface
default	0.0.0.0	192.168.180.1	eth0
192.168.180.0	255.255.252.0	0.0.0.0	eth0
00000000000000000000000000000000 80		00000000000000000000000000000000	lo
fe8000000000000000203c7ffe01947e 80		00000000000000000000000000000000	lo
fe800000000000000000000000000000 40		00000000000000000000000000000000	eth0
ff000000000000000000000000000000 08		00000000000000000000000000000000	eth0
00000000000000000000000000000000 00		00000000000000000000000000000000	lo

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

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

## Routing File Syntax

Each line of the routing file must be either a valid routing line or a comment line.

A comment line starts with a hash sign (#) and can contain any text behind it.

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

Should the host 192.168.20.11 be reached by using the gateway 192.168.0.2, then the routing file must look like this:

```
192.168.20.11    32    192.168.0.2
```

### Example of a Routing File:

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

### Current System Routing Table

This table shows all active IPv4 and IPv6 routes.

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



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

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

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



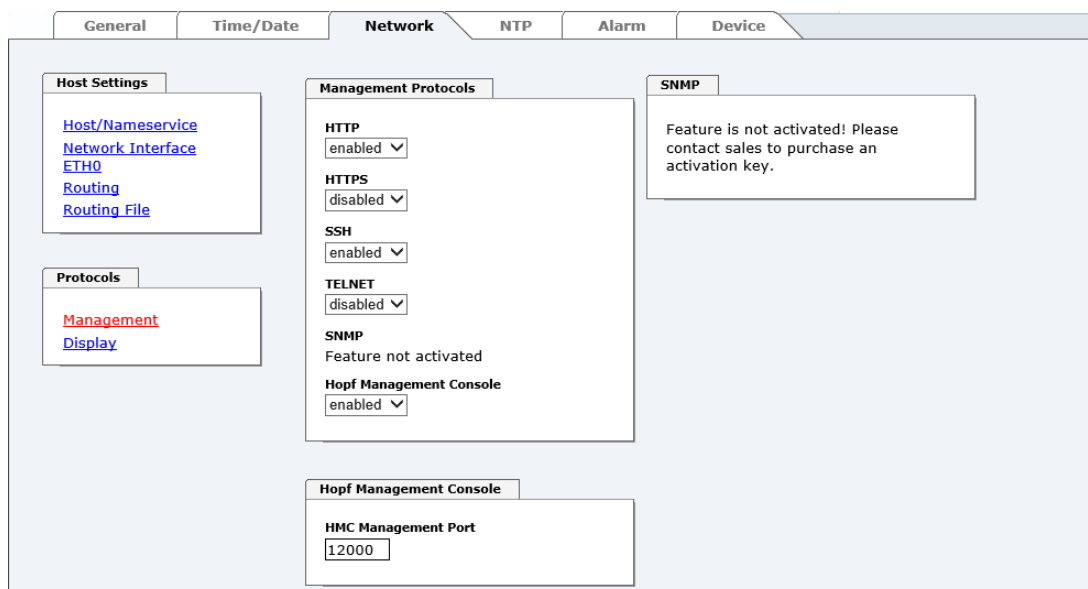
For SNMP functionality an activation key is necessary.



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



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



The screenshot shows the 'Network' tab in the Hopf web interface. It contains three main sections: 'Host Settings', 'Management Protocols', and 'SNMP'. The 'Host Settings' section includes links for 'Host/Nameservice', 'Network Interface', 'ETH0', 'Routing', and 'Routing File'. The 'Management Protocols' section lists several protocols with their status: HTTP (enabled), HTTPS (disabled), SSH (enabled), TELNET (disabled), and SNMP (Feature not activated). Below this, the 'Hopf Management Console' section shows the 'HMC Management Port' set to 12000. A warning message in the 'SNMP' section states: 'Feature is not activated! Please contact sales to purchase an activation key.'



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

**WebGUI with Alarming activated**

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

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

### 5.3.3.5.1 SNMPv2c / SNMPv3 (Activation Key required)

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

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

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

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

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

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

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

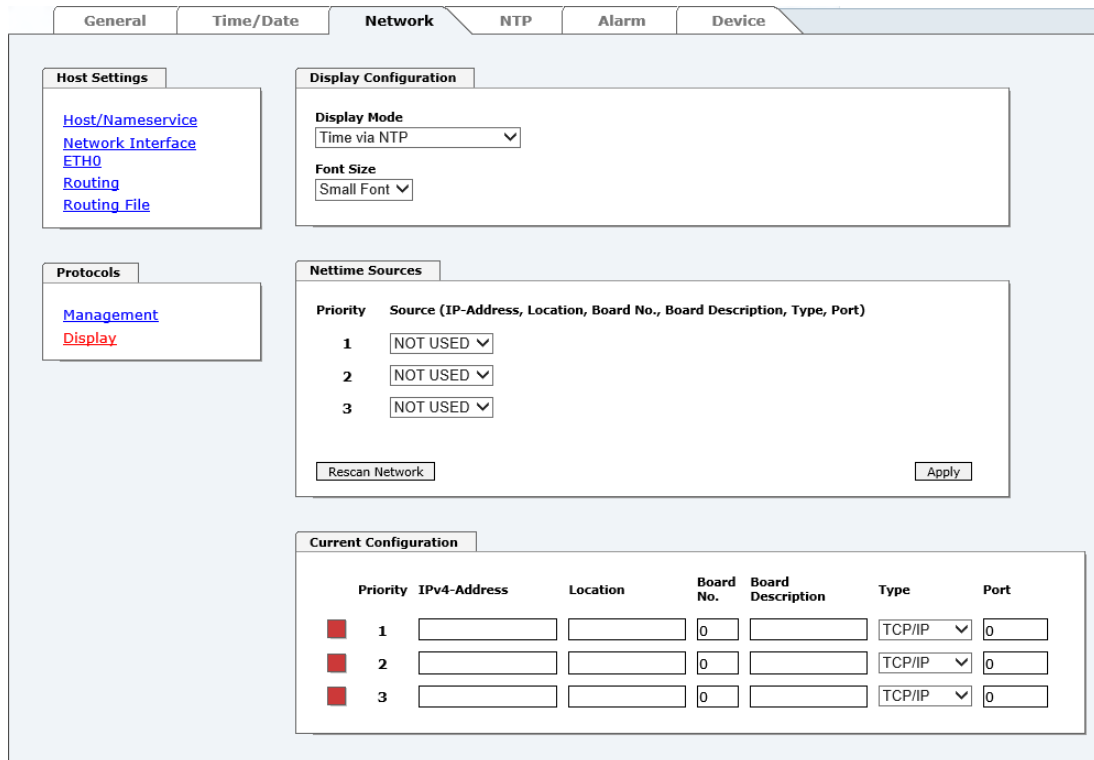
SNMPv3	noAuthNoPriv	authNoPriv	authPriv
Authentication Passphrase:	empty	set	set
Privacy Passphrase:	empty	empty	set



Right now only one user is supported.

### 5.3.3.6 Display

On this page you can adjust the information displayed by the large matrix display 4985.



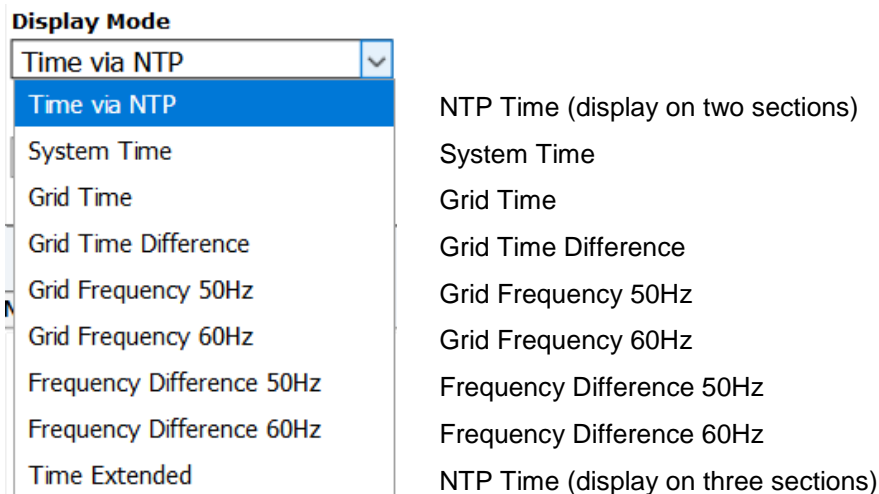
The screenshot shows the 'Display' configuration page with the following sections:

- Host Settings:** Links to Host/Nameservice, Network Interface, ETH0, Routing, and Routing File.
- Protocols:** Links to Management and Display.
- Display Configuration:**
  - Display Mode:** A dropdown menu currently set to 'Time via NTP'.
  - Font Size:** A dropdown menu currently set to 'Small Font'.
- Nettime Sources:**
  - Priority 1: NOT USED
  - Priority 2: NOT USED
  - Priority 3: NOT USED
  - Buttons: Rescan Network, Apply
- Current Configuration:**

Priority	IPv4-Address	Location	Board No.	Board Description	Type	Port
1			0		TCP/IP	0
2			0		TCP/IP	0
3			0		TCP/IP	0

#### Display Mode

With this drop-down menu you can adjust which data should be outputted by the large matrix display 4985.



The screenshot shows the 'Display Mode' dropdown menu with the following options:

- Time via NTP (selected)
- System Time
- Grid Time
- Grid Time Difference
- Grid Frequency 50Hz
- Grid Frequency 60Hz
- Frequency Difference 50Hz
- Frequency Difference 60Hz
- Time Extended

Descriptions for the options:

- Time via NTP:** NTP Time (display on two sections)
- System Time:** System Time
- Grid Time:** Grid Time
- Grid Time Difference:** Grid Time Difference
- Grid Frequency 50Hz:** Grid Frequency 50Hz
- Grid Frequency 60Hz:** Grid Frequency 60Hz
- Frequency Difference 50Hz:** Frequency Difference 50Hz
- Frequency Difference 60Hz:** Frequency Difference 60Hz
- Time Extended:** NTP Time (display on three sections)



For all entries except "**Time via NTP**" and "**Time Extended**" data shown will be provided by boards 7515. Data for boards 7515 will be provided via network by boards 7274RC with activation "**7515RC mains frequency data**".

### Font Size

This drop-down menu enables the font choice for the data adjusted by display mode.

### Nettime Sources

With the elements in this box 7274RC boards which have been activated with "7515RC mains frequency data" (please have a look at **chapter product activation of technical description 7274**) can be searched in the network.

By pushing the **Rescan Network** Button you can search for 7274RC boards with activated "7515RC mains frequency data" function. Afterwards detected 7274RC boards can be chosen via three drop-down menus.

In the drop-down menus you can select **priority levels 1 to 3** whereby 1 means highest priority.

If you push the **apply** button, data of the three drop-down menus will be registered in the fields of the **current configuration** box. Thereby data won't be saved, this proceeding solely avoids to enter the data in the fields of the current configuration box manually.

### Current Configuration

In this table the currently configured communication canals for net time information will be shown. Furthermore you can also change the communication canals in this table.

The fields **Location** and **Board Description** can be chosen freely to enable an easier identification of the data source of the net time information.

The remaining fields define the communication canal to the data source.

### 5.3.4 NTP Tab

This tab shows information and adjustment possibilities of the NTP services of the Network Time Client 8029NTC. The NTP service is the significant main service of the Network Time Client 8029NTC.

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

NTP functionality is provided by an NTP-Demon running on the embedded Linux of the Network Time Client 8029NTC.

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



After all changes relating to NTP a restart of the NTP service must be performed (see **Chapter 5.3.4.6 Restart NTP**).



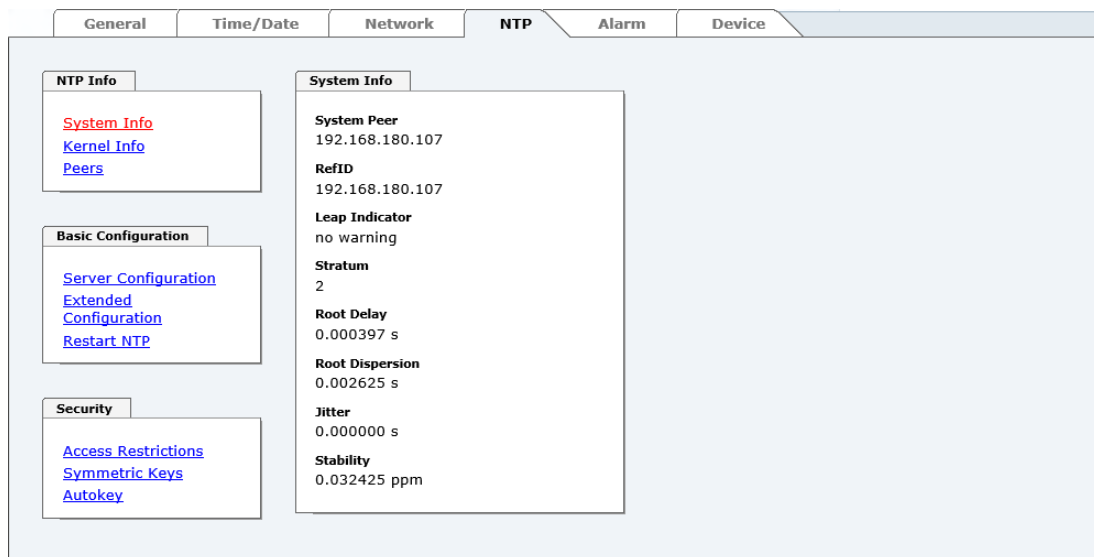
Via the NTP protocol SNTP Clients can also be synchronized. In contrast to NTP in SNTP Clients delay times are not evaluated on the network. For this reason the accuracy reached in SNTP Clients is lower than in NTP Clients.

#### 5.3.4.1 System Info

In the window "System Info" the current NTP values of the NTP service running on the embedded Linux of the Network Time Client 8029NTC are indicated. In addition to the NTP calculated values for root delay, root dispersion, jitter, and stability the stratum value of the Time Client 8029NTC, the status to the leap second, and the current system peer are also found here.

The NTP version used adjusts the leap second correctly.

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



The screenshot shows the 'NTP' tab selected in the top navigation bar. The interface is divided into three main sections: 'NTP Info', 'Basic Configuration', and 'Security'. The 'System Info' sub-tab is active, displaying the following data:

<b>System Peer</b>	192.168.180.107
<b>RefID</b>	192.168.180.107
<b>Leap Indicator</b>	no warning
<b>Stratum</b>	2
<b>Root Delay</b>	0.000397 s
<b>Root Dispersion</b>	0.002625 s
<b>Jitter</b>	0.000000 s
<b>Stability</b>	0.032425 ppm

### 5.3.4.2 Kernel Info

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



This screenshot shows a maximum kernel clock error of 23.081 msec (milliseconds). The estimated error value is 32 µs (microseconds).

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

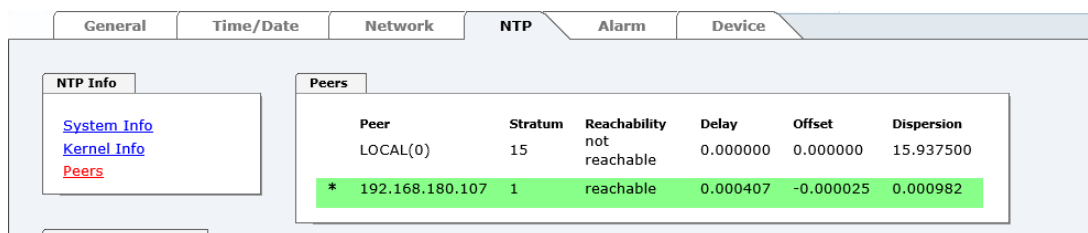
### 5.3.4.3 Peers

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

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

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

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



Peer	Stratum	Reachability	Delay	Offset	Dispersion
LOCAL(0)	15	not reachable	0.000000	0.000000	15.937500
* 192.168.180.107	1	reachable	0.000407	-0.000025	0.000982

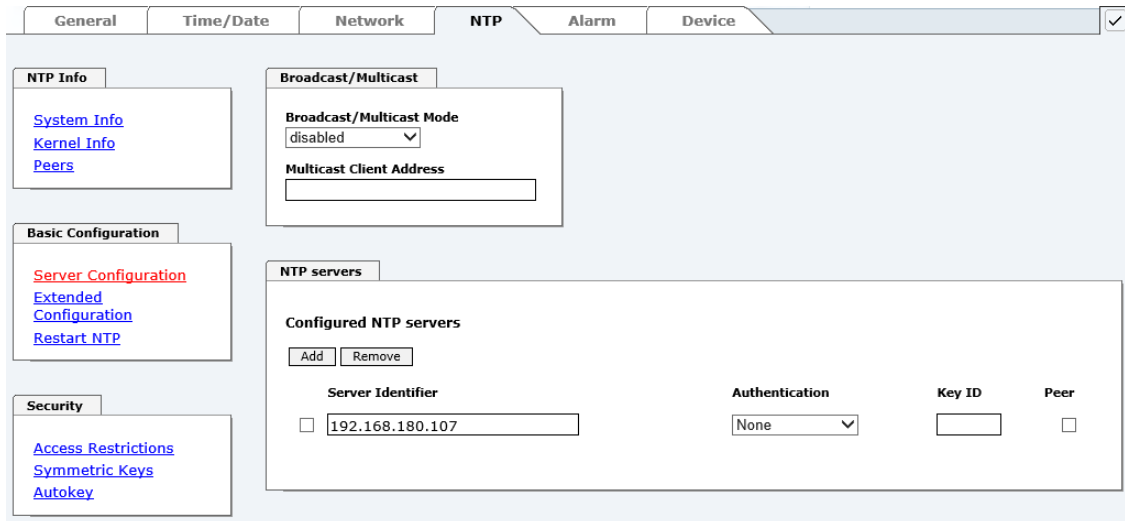
The upper picture shows the external NTP server (192.168.180.107) used for synchronization.

A short explanation and definition of the displayed values can be found in **Chapter 9.5 Accuracy & NTP Basic Principles**.

The character in the first column on the left presents the current status of the NTP association in the NTP selection algorithm. A list and description of possible characters can be found in the Glossary (see **Chapter 9.2 Tally Codes (NTP-specific)**).

### 5.3.4.4 Server Configuration

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



The screenshot shows the NTP configuration page. The 'NTP' tab is active. On the left, there are links for 'System Info', 'Kernel Info', 'Peers', 'Server Configuration' (highlighted in red), 'Extended Configuration', 'Restart NTP', 'Access Restrictions', 'Symmetric Keys', and 'Autokey'. The main area has sections for 'Broadcast/Multicast' (mode: disabled, multicast client address field) and 'NTP servers'. Under 'NTP servers', there is a table titled 'Configured NTP servers' with columns for 'Server Identifier', 'Authentication', 'Key ID', and 'Peer'. One server is listed with identifier '192.168.180.107', authentication 'None', and the peer checkbox is unchecked.

#### 5.3.4.4.1 Broadcast / Multicast

This section is used to configure the Network Time Client 8029NTC as a broadcast or multicast server.

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

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

The broadcast mode is provided for configurations which are designed to facilitate one or more servers and as many clients as possible in a sub-network. The server continuously generates broadcast messages at defined intervals, corresponding to 16 seconds (minpoll 4) for Network Time Client 8029NTC. 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 Network Time Client 8029NTC 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.



### 5.3.4.4.2 NTP Servers for Synchronisation

#### Server Identifier

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/>).

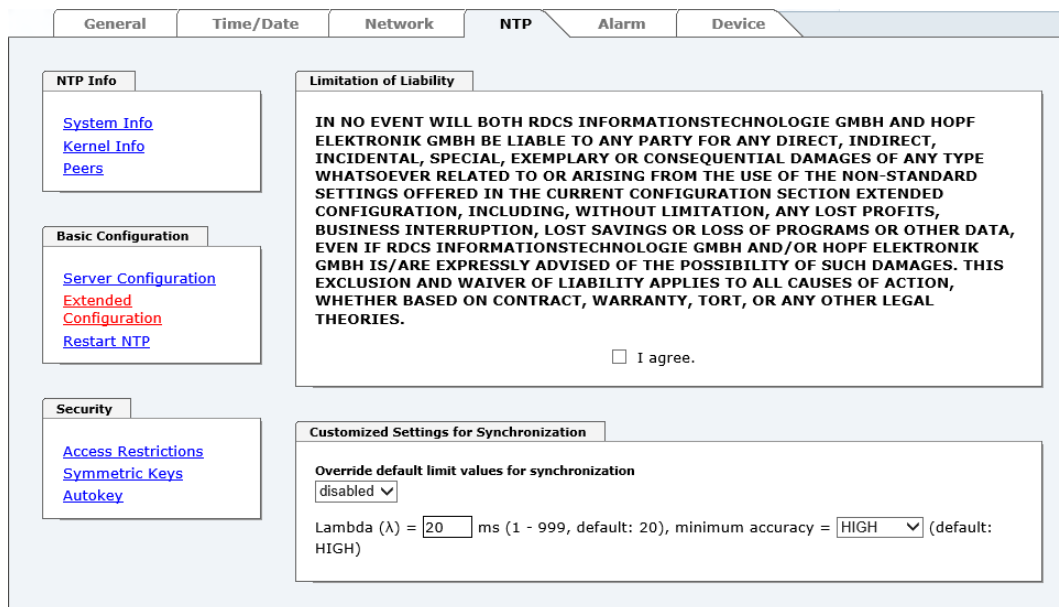
#### Authentication / Key ID

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.

### 5.3.4.5 Extended Configuration

The synchronisation behaviour of Module 8029NTC can be adjusted following the link "**Extended 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.



The screenshot shows the NTP configuration interface. The 'NTP' tab is selected. On the left, there are three sections: 'NTP Info' with links for System Info, Kernel Info, and Peers; 'Basic Configuration' with links for Server Configuration, Extended Configuration, and Restart NTP; and 'Security' with links for Access Restrictions, Symmetric Keys, and Autokey. The main area contains a 'Limitation of Liability' section with a disclaimer text and an 'I agree' checkbox. Below that is the 'Customized Settings for Synchronization' section, which includes a dropdown for 'Override default limit values for synchronization' (currently set to 'disabled'), and a field for 'Lambda (λ)' set to '20' ms, with a note '(1 - 999, default: 20), minimum accuracy = HIGH' (default: HIGH).

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.

Customized Settings for Synchronization

Override default limit values for synchronization

Lambda ( $\lambda$ ) =  ms (1 - 999, default: 20), minimum accuracy =  (default: HIGH)

#### **Override default limit values for synchronization**

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

##### **Lambda ( $\lambda$ )**

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 5.3.6.4 Reboot Device**).

### 5.3.4.5.1 Definition Accuracy (Low / Medium / High)

#### Calculation

<b>LAMBDA</b>	<b>=</b>	<b>((root delay / 2) + Rootdispersion) * 1000</b>
---------------	----------	---

#### **LOW =**

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

#### **MEDIUM =**

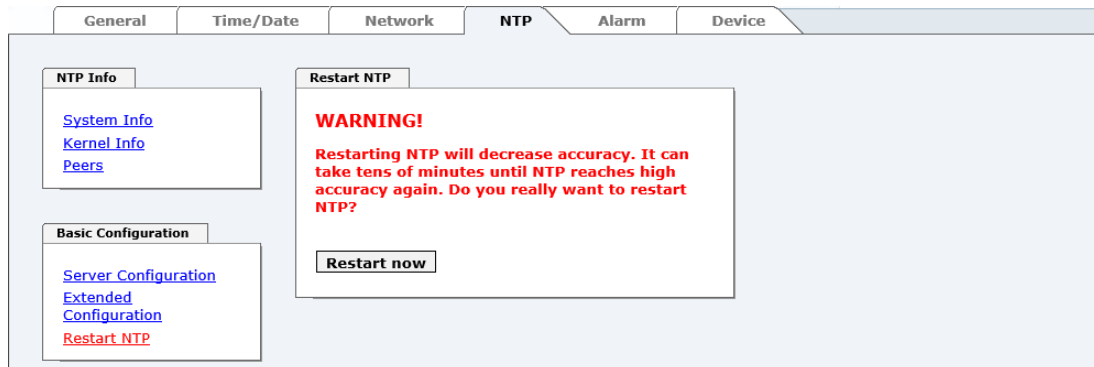
LAMBDA < Accuracy-value **and** System\_Peer\_Offset >= 0,001s  
**or**  
LAMBDA < Accuracy-value **and** Stability > 2,0

#### **HIGH =**

LAMBDA < **Accuracy**-value **and** Stability < 0,2  
**or**  
LAMBDA < Accuracy-value **and** Stability <= 2,0 **and** System\_Peer\_Offset < 0,001s

### 5.3.4.6 Restart NTP

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



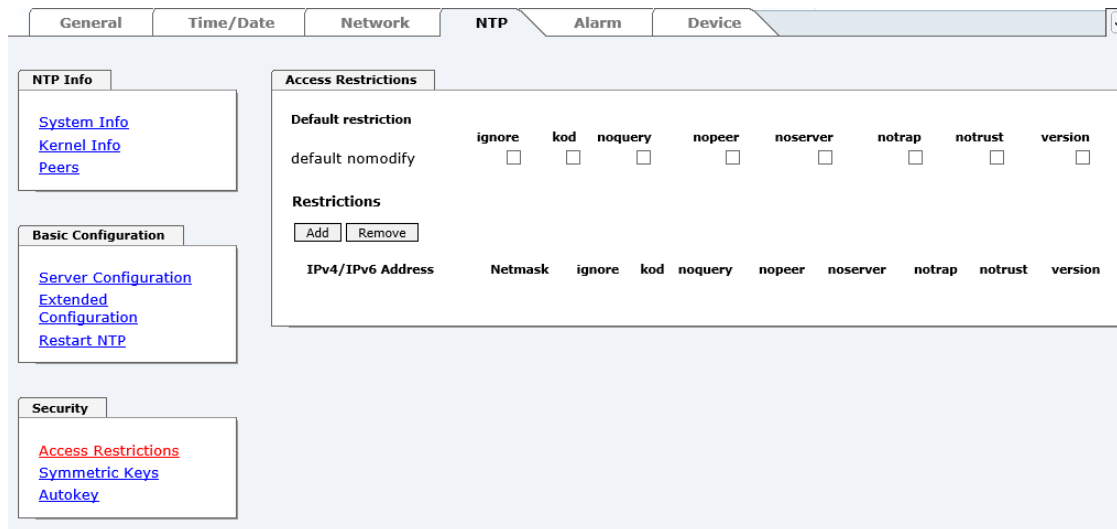
The screenshot shows the 'NTP' tab selected in the top navigation bar. On the left, there are two panels: 'NTP Info' with links for 'System Info', 'Kernel Info', and 'Peers'; and 'Basic Configuration' with links for 'Server Configuration', 'Extended Configuration', and 'Restart NTP'. The main area displays a 'Restart NTP' dialog with a red 'WARNING!' header. The warning text states: 'Restarting NTP will decrease accuracy. It can take tens of minutes until NTP reaches high accuracy again. Do you really want to restart NTP?'. At the bottom of the dialog is a 'Restart now' button.

Restarting NTP Services is the only possibility of making NTP changes effective without having to restart the entire Module 8029NTC. As you can see at 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.

### 5.3.4.7 Access Restrictions / Configuring the NTP Service Restrictions

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



The screenshot shows the 'NTP' tab selected. On the left, the 'Security' panel is active, showing links for 'Access Restrictions', 'Symmetric Keys', and 'Autokey'. The main area displays the 'Access Restrictions' configuration. It includes 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. A table lists the configuration options for each restriction: 'IPv4/IPv6 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 Hostnames!

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

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

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

Before beginning the configuration, the points **5.3.4.7.1** to **5.3.4.7.4** must be checked by the user:

#### 5.3.4.7.1 NAT or Firewall

Are incoming connections to the NTP Service blocked by NAT or a Stateful Inspection Firewall?	
<b>No</b>	Proceed to <b>Chapter 5.3.4.7.2 Blocking Unauthorised Access</b>
<b>Yes</b>	No restrictions are required in this case. Proceed further to <b>Chapter 5.3.4.7.4 Internal Client Protection / Local Network Threat Level</b>

#### 5.3.4.7.2 Blocking Unauthorised Access

Is it really necessary to block all connections from unauthorised hosts if the NTP Service is openly accessible?	
<b>No</b>	Proceed to <b>Chapter 5.3.4.7.3 Allowing Client Requests</b>
<b>Yes</b>	<p>In this case the following restrictions are to be used:</p> <p style="text-align: center;"><b>ignore in the default restrictions</b> <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 <b>Chapter 5.3.4.7.5 Addition of Exceptions to Standard</b></p>

### 5.3.4.7.3 Allowing Client Requests

Are clients to be allowed to see the server status information when they receive the time information from the NTP service (even if this is information about the module, operating system and NTPD version)?									
No	<p>In this case select from the following standard restrictions: See <b>Chapter 5.3.4.7.6 Access Control Options</b></p> <table> <tr> <td>kod</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>notrap</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>nopeer</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>noquery.</td> <td><input checked="" type="checkbox"/></td> </tr> </table>	kod	<input checked="" type="checkbox"/>	notrap	<input checked="" type="checkbox"/>	nopeer	<input checked="" type="checkbox"/>	noquery.	<input checked="" type="checkbox"/>
kod	<input checked="" type="checkbox"/>								
notrap	<input checked="" type="checkbox"/>								
nopeer	<input checked="" type="checkbox"/>								
noquery.	<input checked="" type="checkbox"/>								
Yes	<p>In this case select from the following standard restrictions: See <b>Chapter 5.3.4.7.6 Access Control Options</b>:</p> <table> <tr> <td>kod</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>notrap</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>nopeer</td> <td><input checked="" type="checkbox"/></td> </tr> </table> <p>If a standard restriction is selected in this area, exceptions can be declared in separate lines for each authorised server, client or sub-network. See <b>Chapter 5.3.4.7.5 Addition of Exceptions to Standard</b>.</p>	kod	<input checked="" type="checkbox"/>	notrap	<input checked="" type="checkbox"/>	nopeer	<input checked="" type="checkbox"/>		
kod	<input checked="" type="checkbox"/>								
notrap	<input checked="" type="checkbox"/>								
nopeer	<input checked="" type="checkbox"/>								

### 5.3.4.7.4 Internal Client Protection / Local Network Threat Level

How much protection from internal network clients is required?							
Yes	<p>The following restrictions can be enabled if greater security settings than the installed authentication are required in order to protect the NTP service from the clients see <b>Chapter 5.3.4.7.6 Access Control Options</b>.</p> <table> <tr> <td>kod</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>notrap</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>nopeer</td> <td><input checked="" type="checkbox"/></td> </tr> </table>	kod	<input checked="" type="checkbox"/>	notrap	<input checked="" type="checkbox"/>	nopeer	<input checked="" type="checkbox"/>
kod	<input checked="" type="checkbox"/>						
notrap	<input checked="" type="checkbox"/>						
nopeer	<input checked="" type="checkbox"/>						

### 5.3.4.7.5 Addition of Exceptions to Standard Restrictions

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

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

Access Restrictions

Default restriction

ignore

kod

noquery

nopeer

noserver

notrap

notrust

version

default nomodify

☒

☒

☒

☒

☒

☒

☐

☐

Restrictions

Add

Remove

IPv4/IPv6 Address

Netmask

ignore

kod

noquery

nopeer

noserver

notrap

notrust

version

☐

☒

☐

☐

☐

☒

☒

☐

☐



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** ☒

### 5.3.4.7.6 Access Control Options

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

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

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



**Default Settings:**

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

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

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

This option is used if a host/sub-network is only allowed to access 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.

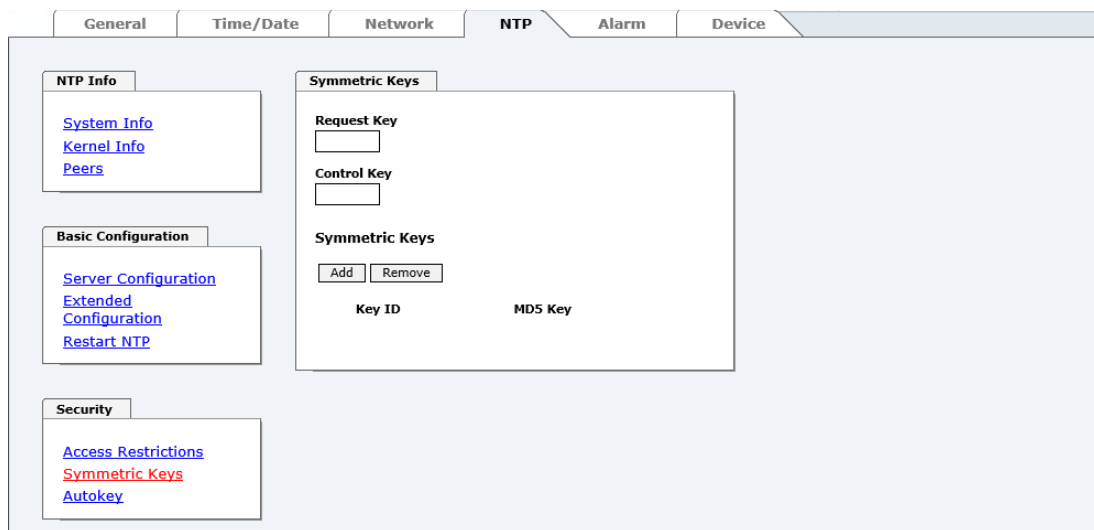
**version** – "Denies packets which do not correspond to the current NTP version."



Changes in data do not take effect immediately after clicking on the "Apply" symbol. The NTP service **MUST** also be restarted (see **Chapter 5.3.4.6 Restart NTP**).



### 5.3.4.8 Symmetric Key



#### 5.3.4.8.1 Why Authentication?

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

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

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

#### 5.3.4.8.2 How is Authentication used in the NTP Service?

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

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

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

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

#### 5.3.4.8.3 How is a key created?

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

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

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

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

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

#### 5.3.4.8.4 How does authentication work?

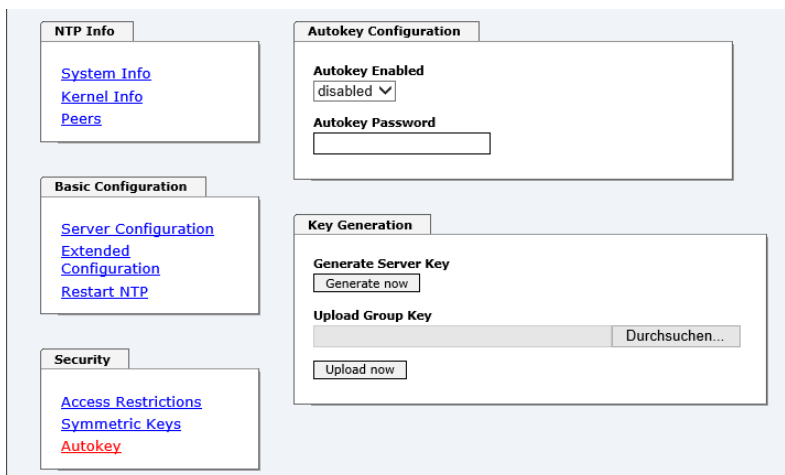
The basic authentication is a digital signature and no data encryption (if there are any differences between the two). The data packet and the key are used to create a non-reversible number which is attached to the packet.

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

#### 5.3.4.9 Autokey / Public Key Cryptography

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

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



The screenshot shows the NTP WebGUI configuration interface. On the left, there are three main sections: 'NTP Info' with links for 'System Info', 'Kernel Info', and 'Peers'; 'Basic Configuration' with links for 'Server Configuration', 'Extended Configuration', and 'Restart NTP'; and 'Security' with links for 'Access Restrictions', 'Symmetric Keys', and 'Autokey'. The 'Autokey' link is highlighted in red. On the right, the 'Autokey Configuration' section is active, showing 'Autokey Enabled' set to 'disabled' with a dropdown arrow, and an empty 'Autokey Password' field. Below this, the 'Key Generation' section is visible, containing a 'Generate Server Key' button labeled 'Generate now', an 'Upload Group Key' section with a file input field and a 'Durchsuchen...' button, and an 'Upload now' button.

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

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



#### Generate now

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

If the Network 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.

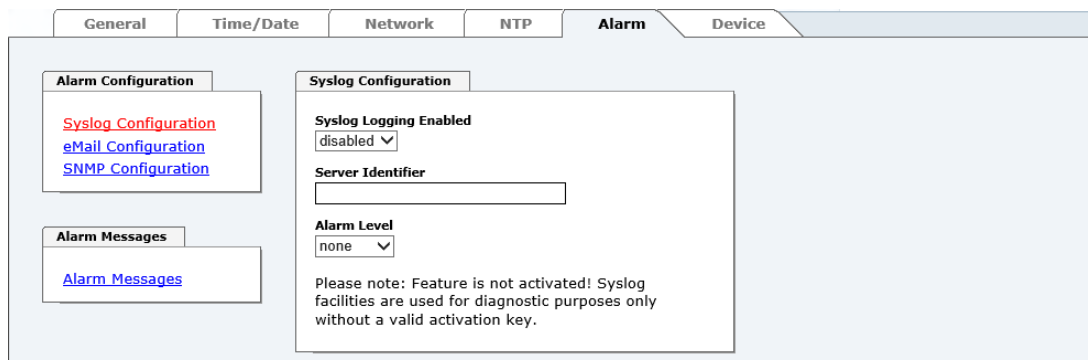
Detailed information about the NTP Autokey scheme can be found in the NTP documentation (<http://www.ntp.org/>).



Changes in data do not take effect immediately after clicking on the "Apply" symbol. The NTP service **MUST** also be restarted (see **Chapter 5.3.4.6 Restart NTP**).

## 5.3.5 ALARM Tab

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



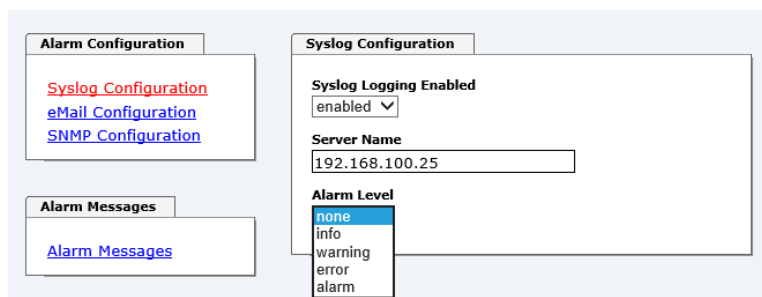
### 5.3.5.1 Syslog Configuration

It is necessary to enter the name or IPv4 or IPv6 address of a Syslog server in order to store every configured alarm situation which occurs on the 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 5.3.5 ALARM Tab**).

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

### 5.3.5.2 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 5.3.5 ALARM Tab**).

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

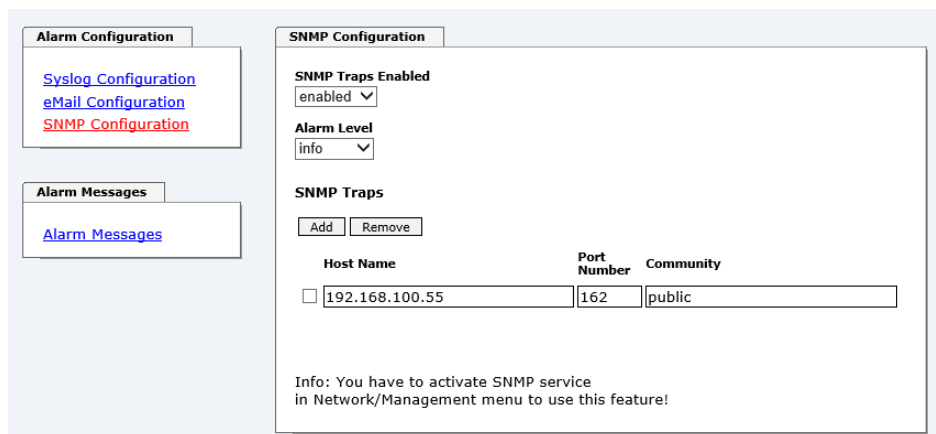
### 5.3.5.3 SNMP Configuration / TRAP Configuration

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 5.3.6.11 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 5.3.5 ALARM Tab**).

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

### 5.3.5.4 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.

Alarm Configuration	
<a href="#">Syslog Configuration</a> <a href="#">eMail Configuration</a> <a href="#">SNMP Configuration</a>	
<b>Alarm Messages</b> <a href="#">Alarm Messages</a>	

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

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



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

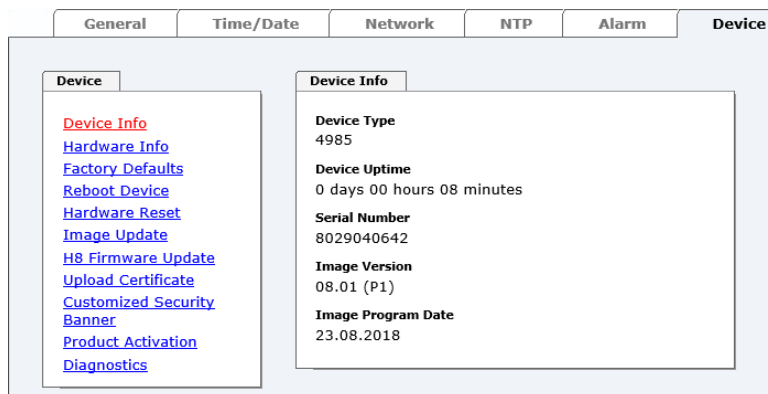
### 5.3.6 DEVICE Tab

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.

#### 5.3.6.1 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.



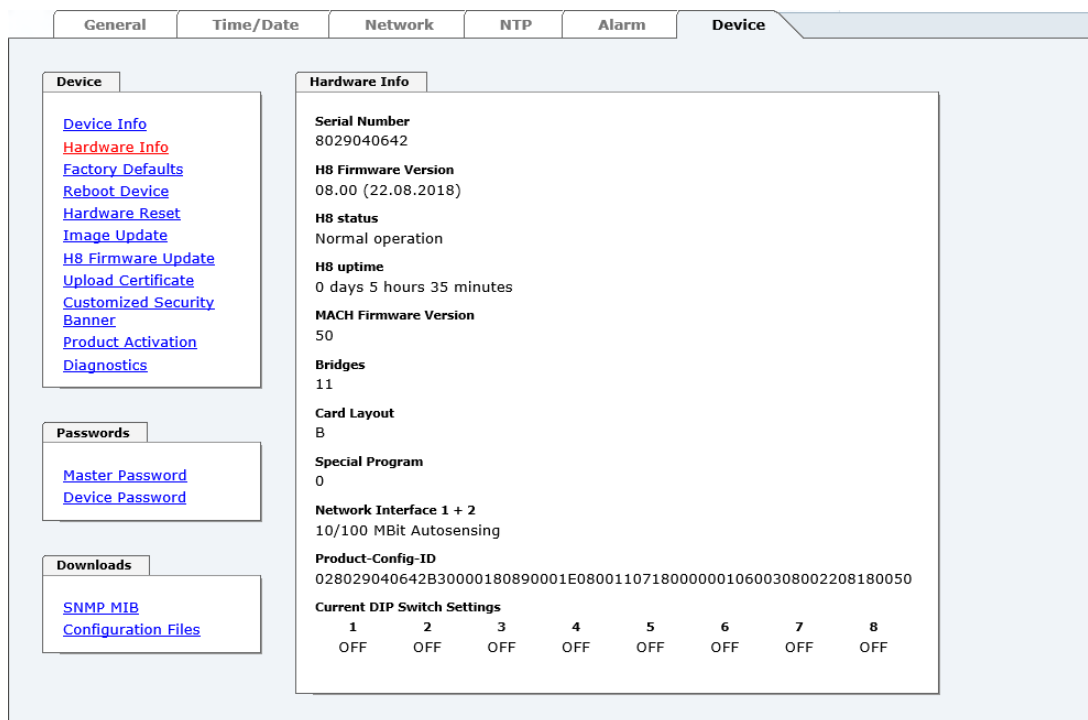
The screenshot shows the 'Device' tab selected in the top navigation bar. On the left, a sidebar contains a list of links: Device Info, Hardware Info, Factory Defaults, Reboot Device, Hardware Reset, Image Update, H8 Firmware Update, Upload Certificate, Customized Security Banner, Product Activation, and Diagnostics. The main content area is titled 'Device Info' and displays the following information:

- Device Type:** 4985
- Device Uptime:** 0 days 00 hours 08 minutes
- Serial Number:** 8029040642
- Image Version:** 08.01 (P1)
- Image Program Date:** 23.08.2018

#### 5.3.6.2 Hardware Information

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

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



The screenshot shows the 'Device' tab selected in the top navigation bar. On the left, a sidebar contains a list of links: Device Info, Hardware Info, Factory Defaults, Reboot Device, Hardware Reset, Image Update, H8 Firmware Update, Upload Certificate, Customized Security Banner, Product Activation, and Diagnostics. The main content area is titled 'Hardware Info' and displays the following information:

- Serial Number:** 8029040642
- H8 Firmware Version:** 08.00 (22.08.2018)
- H8 status:** Normal operation
- H8 uptime:** 0 days 5 hours 35 minutes
- MACH Firmware Version:** 50
- Bridges:** 11
- Card Layout:** B
- Special Program:** 0
- Network Interface 1 + 2:** 10/100 MBit Autosensing
- Product-Config-ID:** 028029040642B30000180890001E080011071800000010600308002208180050
- Current DIP Switch Settings:**

1	2	3	4	5	6	7	8
OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF

Below the 'Hardware Info' section, there are two additional sections in the sidebar:

- Passwords:** Master Password, Device Password
- Downloads:** SNMP MIB, Configuration Files

### 5.3.6.3 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 8 Factory Defaults**).

The registration is conducted as Master user according to the manual, **Chapter 5.2.1 LOGIN and LOGOUT as User**.

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

**Factory Defaults**

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

**Reset now**

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.

### 5.3.6.4 Reboot Device

All settings not saved with "**Save**" are lost on reset (see **Chapter 5.2.3 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 5.2.1 LOGIN and LOGOUT as User**.

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

**Reboot Device**

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

**Reboot now**

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



### 5.3.6.5 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**.

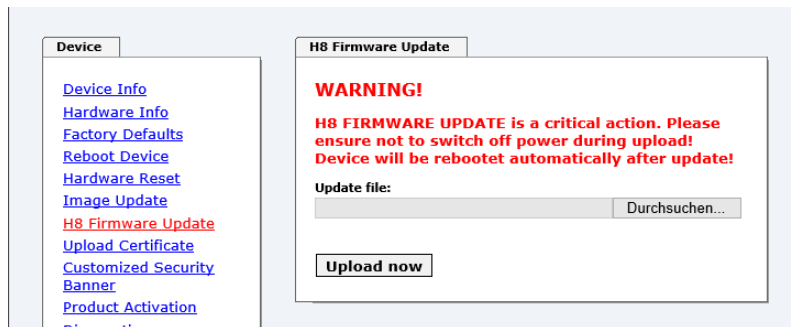
In order to carry out an update, enter the name and the folder in which the update / firmware image is located in the text field or open the file selection dialogue by pressing the "Browse" button.

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

8029NTC\_v0100\_128.mot                      for the **H8 firmware**  
(update takes approx. 1-1.5 minutes)

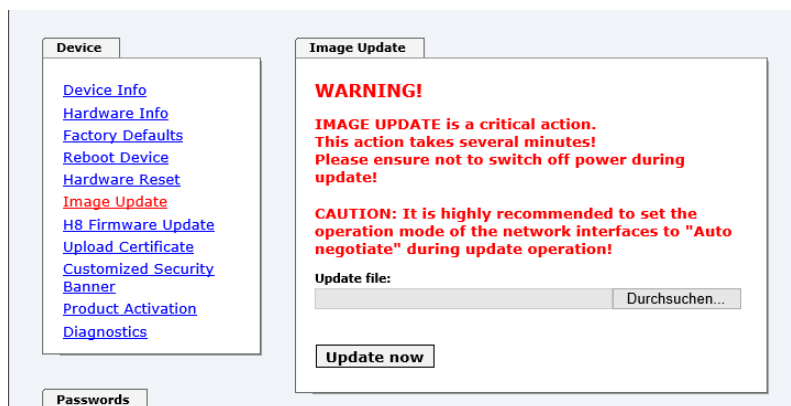
upgrade\_8029NTC\_v0201.img                  for the **embedded image**  
(update takes approx. 7-8 minutes)

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



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

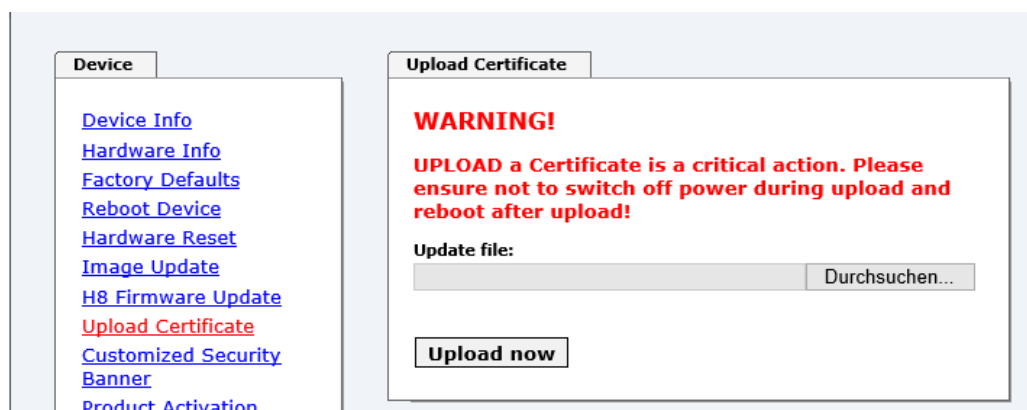
The procedure for the **Image update** differs only in how the module is restarted.



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

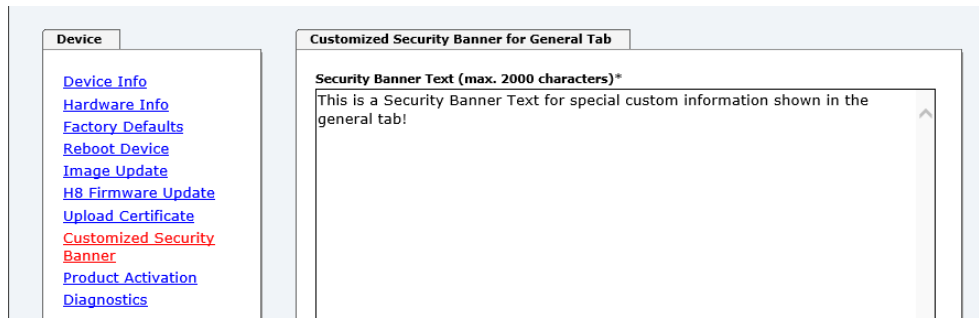
### 5.3.6.6 Upload Certificate (SSL-Server-Certificate)

It is possible to encrypt the https connections to the Network Time Client Module 8029NTC with a user-supplied SSL server certificate.



### 5.3.6.7 Customized Security Banner

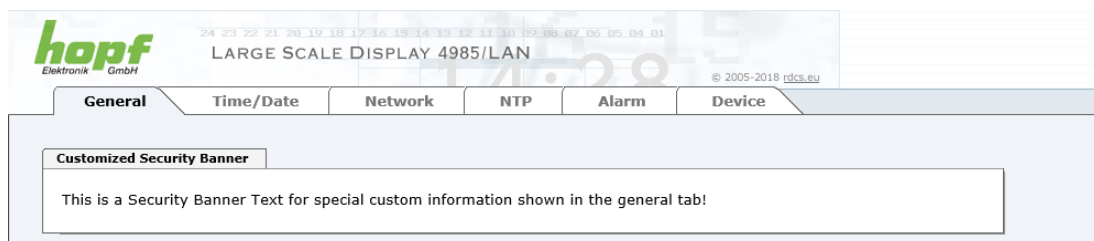
Special security information displayed in the General tab can be entered here by the user.



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

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

- Capital letters (A...Z)
- Lowercase letters (a...z)
- Numbers (0...9)
- The following special characters: space (" "), exclamation mark ("!"), Comma (","), dot ("."), Colon (":"), question mark ("?" )



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

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

### 5.3.6.8 Product Activation

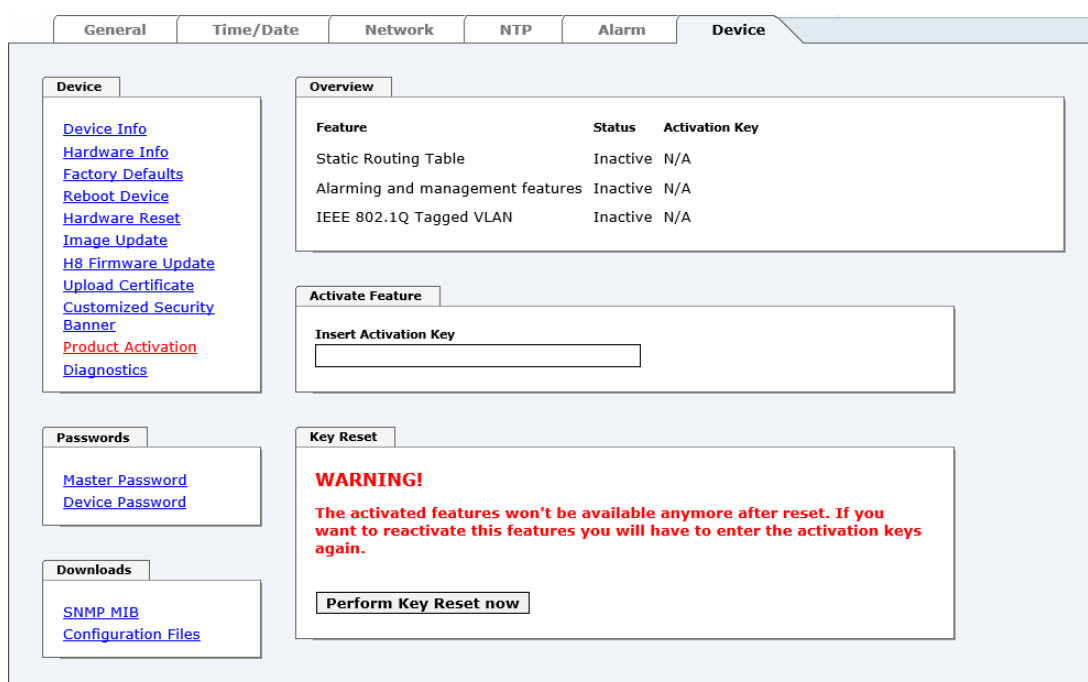
For the activation of optional functions, e.g. "Network Interface Bonding/Teaming", a special activation key is required for which an order with the **hopf** Elektronik GmbH can be placed. Each activation key is related to a special board with an appropriate serial number and cannot be used for several boards.



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



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



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

**Activate Feature**

Insert Activation Key

**Key Reset**

**WARNING!**

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

Perform Key Reset now

#### Overview

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

#### Activate Feature

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

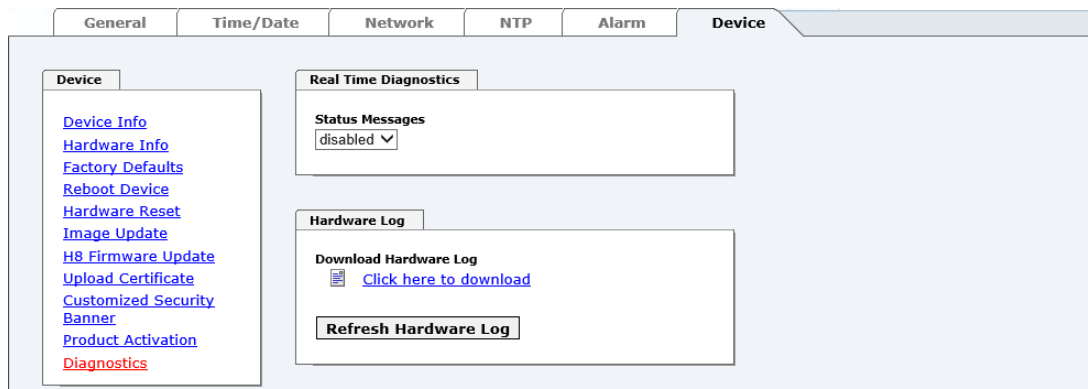
If the activation was successful the new feature is listed in the overview with status "Active" and can be used immediately.

#### Key Reset

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

### 5.3.6.9 Diagnostics Function

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

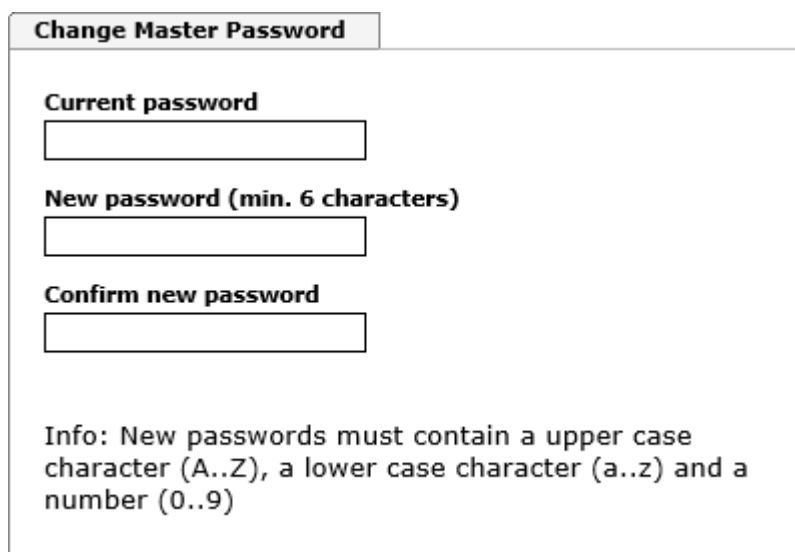


### 5.3.6.10 Passwords Master / Device

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

. , ! " \$ % & / { } [ ] ( ) = ? \ + - @ \* ~ # ' < > | ; : \_

(See also **Chapter 5.2.1 LOGIN and LOGOUT as User**)





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

### 5.3.6.11 Downloading SNMP MIB / Configuration Files


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


**SNMP MIB**


**Download hopf8029NTC MIB**  
 [Click here to download](#)

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

**Configuration Files**

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

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

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

**Device Configuration**

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

**Refresh Device Configuration**

## 6 SSH and Telnet Basic Configuration



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

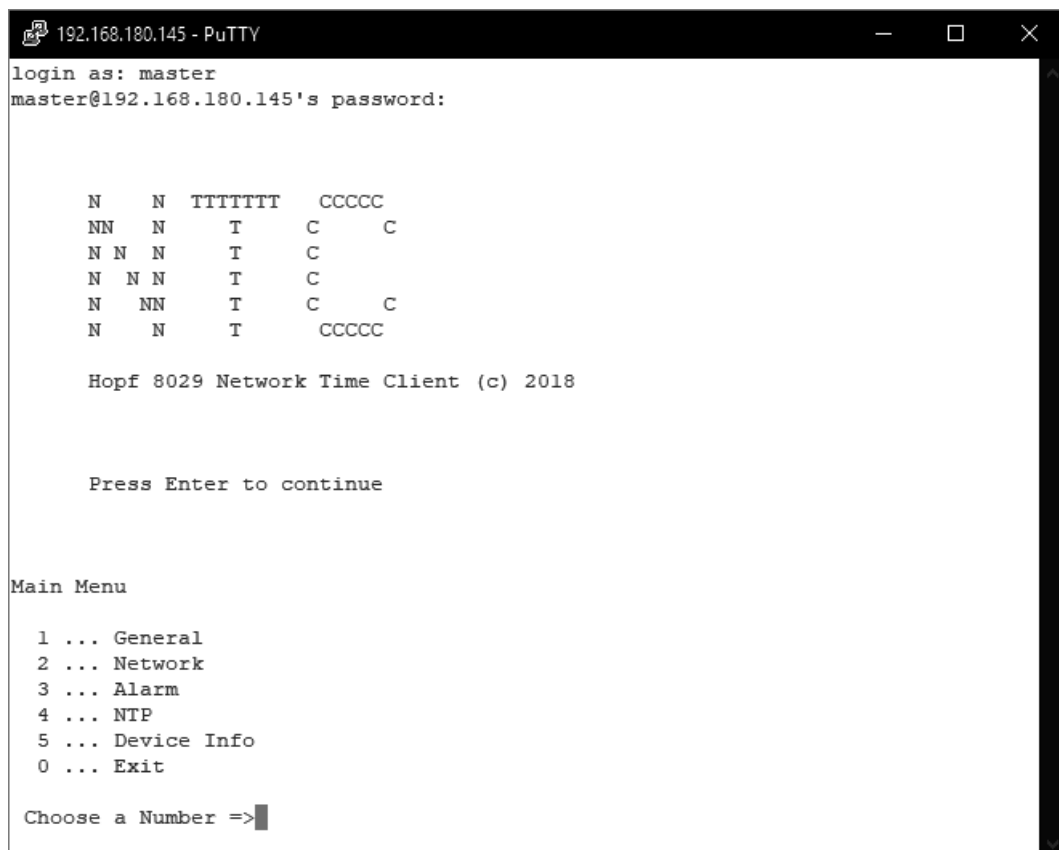
The user names and passwords are the same as on the WebGUI and are kept in alignment (see **Chapter 5.3.6.10 Passwords Master / Device**).



SSH does not allow blank passwords for safety reasons.



The corresponding protocols should be enabled for the use of Telnet or SSH (see **Chapter 5.3.3.5 Management (Management-Protocols – HTTP, SNMP, SNMP-Traps, etc.)**).



```

192.168.180.145 - PuTTY
login as: master
master@192.168.180.145'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) 2018

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).

## 7 Technical Data Large Matrix Display 4985

Technical Data	Board 4985
Voltage supply:	85-250V AC (47-440Hz) or 110-250V DC
Housing dimensions:	see <b>Chapter 1.3.2 Wall Mounting and Cable Entry</b>
Temperature range:	Operating: 0° to +55° C Storage: -20° to +75° C
Readability:	in 2 lines each with 42mm high characters ⇒ 20m in 1 line each with 84mm high characters ⇒ 40m
Humidity:	Max. 95%, not condensed
LED colour:	Red
Protection:	IP40 for indoor mounting
Housing:	Housing for wall mounting Material: aluminium, black
Weight:	Approx. 3.7kg
Backup-Clock Accuracy:	± 25 ppm at constant temperature in a range of +10° to +50° C
Backup-Clock Buffering (maintenance-free):	3 days
Operation:	Via WebGUI or with <b>hmc</b> ( <b>hopf</b> Management Console) via LAN interface
Custom-made products:	Hard- and software solutions according to customer specifications



**hopf** reserves the right to make any modifications to the hard- and software at any time.



## 8 Factory Defaults

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

### 8.1 Network

Host/Name Service	Setting	WebGUI Presentation
Hostname	hopf4985lan	hopf4985lan
Use Manual DNS Entries	Enabled	Enabled
DNS Server 1 IPv4/IPv6 Address	Blank	---
DNS Server 2 IPv4/IPv6 Address	Blank	---
DNS Server 3 IPv4/IPv6 Address	Blank	---
Use Manual Gateway Entries	Enabled	Enabled
Default Gateway IPv4-Adresse	Blank	---
Default Gateway IPv6-Adresse	Blank	---
Network Interface ETH0	Setting	WebGUI
Use Custom Hardware Address (MAC)	Disabled	Disabled
Custom Hardware Address (MAC)	Blank	---
DHCP	Disabled	Disabled
IPv4	192.168.0.1	192.168.0.1
IPv4-Netmask	255.255.255.0	255.255.255.0
Operation mode	Auto negotiate	Auto negotiate
VLAN Interfaces	Disabled	Disabled
IPv6 Settings	Disabled	Disabled
Routing	Setting	WebGUI
Use Route File	Disabled	Disabled
User Defined Routes	Disabled	Disabled
Management	Setting	WebGUI
HTTP	Enabled	Enabled
HTTPS	Disabled	Disabled
SSH	Enabled	Enabled
TELNET	Disabled	Disabled
SNMP	Disabled	Disabled
System Location	Blank	---
System Contact	Blank	---
Read Only Community	public	public
Read/Write Community	secret	secret
Security Name	Blank	---
Access Rights	Readonly	Readonly
Authentication Protocol	MD5	MD5
Authentication Passphrase	Blank	---
Privacy Protocol	DES	DES
Privacy Passphrase	Blank	---

## 8.2 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	---

## 8.3 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

## 8.4 DEVICE

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

## 9 Glossary and Abbreviations

### 9.1 NTP-specific Terminology

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

### 9.2 Tally Codes (NTP-specific)

<b>space</b>	<b>reject</b>	Rejected peer – either the peer is not reachable or its synchronization distance is too great.
<b>x</b>	<b>false tick</b>	The peer was picked out by the NTP intersection algorithm as a false time supplier.
<b>.</b>	<b>excess</b>	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).
<b>-</b>	<b>outlier</b>	The peer was picked out by the NTP clustering algorithm as an outlier.
<b>+</b>	<b>candidate</b>	The peer was selected as a candidate for the NTP combining algorithm.
<b>#</b>	<b>selected</b>	The peer is of good quality but not among the first six peers selected by the sort algorithm on the basis of synchronization distance.
<b>*</b>	<b>sys.peer</b>	The peer was selected as a system peer. Its characteristics are transferred to the Base System.
<b>o</b>	<b>pps.peer</b>	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.

## 9.2.1 Time-specific expressions

<b>UTC</b>	<b>UTC Time (Universal Time Coordinated)</b> 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.
<b>Time Zone</b>	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.
<b>Time Offset</b>	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.
<b>Local Standard Time (winter time)</b>	<b>Standard Time = UTC + Time Offset</b> The time offset is defined by the local time zone and the local political regulations.
<b>Daylight Saving Time (summer time)</b>	<b>Offset of Daylight Saving Time = + 1h</b> 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.
<b>Local Time</b>	Local Time = Standard Time if exists with summer / winter time changeover
<b>Leap Second</b>	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 <b>International Earth Rotation and Reference Systems Service (IERS)</b> .

## 9.3 Abbreviations

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

## 9.4 Definitions

An explanation of the terms used in this document.

### 9.4.1 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.

### 9.4.2 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.

### 9.4.3 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.

### 9.4.4 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.

## 9.5 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.



## 10 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)

## 11 List of Open Source Packages used

### Third Party Software

The **hopf** Network 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
arp-scan	1.9	GPL	v3	no
arptables	0.0.4			no
at91bootstrap 3	3.8.7			no
busybox	1.28.1	GPL	v2	no
bzip2	1.0.6	BSD		no
cifs-utils	6.7	GPL	v3	no
ethtool	4.13	GPL	v2	no
libevent	2.1.8-stable	3-clause BSD		no
libopenssl	1.0.2n	Dual	<a href="http://www.openssl.org/source/license.html">http://www.openssl.org/source/license.html</a>	no
libpcap	1.8.1	BSD		no
libzlib	1.2.11		Copyright (C) 1995-2017 Jean-loup Gailly and Mark Adler  This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.  Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:  1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required. 2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software. 3. This notice may not be removed or altered from any source distribution.	no
lighttpd	1.4.48		Copyright (c) 2004, Jan Kneschke, incremental All rights reserved.  Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:  - Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.	no

Package name	Version	License	License details	Patches
			<p>- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.</p> <p>- Neither the name of the 'incremental' nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.</p> <p>THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.</p>	
linux	4.8.6	GPL	v2	no
linux-headers	4.8.6	GPL	v2	no
lzo	2.10	GPL	v2	no
mtd	2.0.1	GPL	v2	no
netcat	0.7.1	GPL	v2	no
netsnmp	5.7.3	BSD (mehrere)	<a href="http://net-snmp.sourceforge.net/about/license.html">http://net-snmp.sourceforge.net/about/license.html</a>	no
ntp	4.2.8p11		<p>Copyright (c) University of Delaware 1992-2011</p> <p>Permission to use, copy, modify, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or Publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided "as is" without express or implied warranty.</p>	yes
openssh	7.6p1	BSD		no
pcrc	8.41	BSD		no
pps-tools	47333f24af878f67ce48022e8af16419713aa1ac	GPL	v2	no
uboot	2016.09.01	GPL	v2+	no
uboot-tools	2018.01	GPL	v2+	no

Package name	Version	License	License details	Patches
uclibc	1.0.28	GPL	v2	no
util-linux	2.31.1	GPLv2+ GPLv2 LGPLv2+ BSD		no
zip	3.0		<p>Copyright (c) 1990-2007 Info-ZIP. All rights reserved.</p> <p>For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:</p> <p>Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White.</p> <p>This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.</p> <p>Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:</p> <ol style="list-style-type: none"> <li>1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.</li> <li>2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.</li> <li>3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.</li> <li>4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.</li> </ol>	no