

Industriefunkuhren



---

## **Technical Manual**

NTP/SINEC H1 LAN Board

**Model 7271RC and 7272RC**

**ENGLISH**

**Version: 06.02 – 15.09.2011**

---

	<b>SET</b>	<b>IMAGE</b>	<b>FIRMWARE</b>
Valid for Board 7271	Version: <b>06.xx</b>	Version: <b>06.xx</b>	Version: <b>06.xx</b>
Valid for Board 7272	Version: <b>13.xx</b>	Version: <b>13.xx</b>	Version: <b>13.xx</b>



## **Version Numbers (SET / Firmware / Description)**

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

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

THE VERSION NUMBER OF THE IMAGE AND THE H8 SOFTWARE CAN BE READ IN THE WEBGUI OF BOARD 7271RC/7272RC (SEE **CHAPTER 8.3.5.1 Device Information** AND **CHAPTER 8.3.5.2 Hardware Information**).

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

## **Downloading Technical Manuals**

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

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

E-mail: [info@hopf.com](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 89/336/EEG "Electromagnetic compatibility" and 73/23/EEG "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 General .....</b>	<b>9</b>
<b>2 Board 7271RC/7272RC Basic Functions .....</b>	<b>10</b>
<b>3 Board 7271RC Construction .....</b>	<b>12</b>
3.1 Board 7271RC Front Panel .....	12
3.1.1 Status LEDs of the Board 7271RC .....	13
3.1.2 RJ45 Socket (ETH0) .....	14
3.1.3 Reset / Default Button .....	14
3.2 Overview of Board 7271RC (3U/4HP) Assembly .....	15
3.2.1 DIP Switch DS1 .....	15
3.2.2 MAC Address for ETH0 .....	16
3.2.3 Heat Sink .....	16
<b>4 Board 7272RC Construction .....</b>	<b>17</b>
4.1 Board 7272RC Front Panel .....	17
4.1.1 Status LEDs of the Board 7272RC .....	18
4.1.2 RJ45 Socket (ETH0 / ETH1) .....	19
4.1.3 Reset / Default Button .....	19
4.2 Overview of Board 7272RC (3U/4HP) Assembly .....	20
4.2.1 DIP Switch DS1 .....	20
4.2.2 MAC Address for ETH0 / ETH1 .....	21
4.2.3 Heat Sink .....	21
<b>5 Board 7271RC/7272RC System Performance .....</b>	<b>22</b>
5.1 Delayed Readiness for Operation after Switch-on / Reset .....	22
5.2 Reset / Default Button .....	22
5.2.1 Board Reset .....	23
5.2.2 Place LAN Parameters in Default Status .....	24
<b>6 Implementing Board 7271RC/7272RC in a <i>hopf</i> Base System .....</b>	<b>25</b>
6.1 Setting the System Board Number .....	25
6.1.1 Setting the Board Number for Base System 7001RC .....	26
6.2 NTP Accuracy Message for Status- and Error Messages in System 7001RC .....	27
6.3 Creating the Network Connection .....	27
<b>7 Network Configuration for ETH0 via the Base System .....</b>	<b>28</b>
7.1 Input Functions of Base Systems 7001RC .....	30
7.1.1 Inputting the Static IPv4 Address / DHCP Mode .....	30
7.1.2 Inputting the Gateway Address .....	31
7.1.3 Inputting the Network Mask .....	31
7.1.4 Inputting the Control-Byte .....	31
7.1.4.1 Bit 7-1 - No Function at Present .....	31
7.1.4.2 Bit 0 - Restoring Factory Settings .....	32
7.1.5 Inputting the Parameterbyte 01 (no function at present) .....	32

7.1.6 Inputting the Parameterbyte 02 (no function at present) .....	32
<b>8 HTTP/HTTPS WebGUI – Web Browser Configuration Interface.....</b>	<b>33</b>
8.1 Quick Configuration .....	33
8.1.1 Requirements.....	33
8.1.2 Configuration Steps.....	33
8.2 General – Introduction .....	34
8.2.1 LOGIN and LOGOUT as a User .....	35
8.2.2 Navigation via the Web Interface .....	36
8.2.3 Inputting or Changing Data .....	37
8.2.4 Plausibility Check during Input.....	38
8.3 Description of the Tabs.....	39
8.3.1 GENERAL Tab.....	39
8.3.2 NETWORK Tab.....	40
8.3.2.1 Host/Nameservice .....	41
8.3.2.1.1 Hostname .....	41
8.3.2.1.2 Default Gateway .....	41
8.3.2.1.3 DNS Server 1 & 2 .....	41
8.3.2.2 Network Interface ETH0 / ETH1 .....	42
8.3.2.2.1 Default Hardware Address (MAC) .....	43
8.3.2.2.2 Customer Hardware Address (MAC) .....	43
8.3.2.2.3 DHCP .....	43
8.3.2.2.4 IP Address .....	44
8.3.2.2.5 Network Mask .....	44
8.3.2.2.6 Operation Mode .....	44
8.3.2.3 Option: Network Interface Bonding / Teaming .....	45
8.3.2.3.1 Basic Configuration.....	45
8.3.2.3.2 Basic Configuration.....	46
8.3.2.3.3 Advanced Configuration Parameters .....	47
8.3.2.4 Routing .....	49
8.3.2.5 Management-Protocols / SNMP .....	50
8.3.2.6 Time.....	51
8.3.2.6.1 Time Protocols.....	51
8.3.2.6.2 SINEC H1 time datagram .....	52
8.3.2.6.3 Transmission point of SINEC H1 time datagram .....	52
8.3.2.7 Option: Mains Frequency / Nettime Distribution.....	53
8.3.3 NTP Tab.....	55
8.3.3.1 System Info.....	56
8.3.3.2 Kernel Info .....	57
8.3.3.3 Peers .....	58
8.3.3.4 Server Configuration.....	59
8.3.3.4.1 General / Synchronization Source .....	59
8.3.3.4.2 General / Log NTP Messages to Syslog.....	60
8.3.3.4.3 Crystal Operation.....	60
8.3.3.4.4 Broadcast / Broadcast Address .....	60
8.3.3.4.5 Broadcast / Authentication / Key ID .....	61
8.3.3.4.6 Additional NTP SERVERS.....	61
8.3.3.5 Extended NTP Configuration .....	62
8.3.3.5.1 Suppression of unspecified NTP outputs (Block Output when Stratum Unspecified) .....	62
8.3.3.5.2 NTP Timebase.....	62
8.3.3.6 Restart NTP .....	63
8.3.3.7 Access Restrictions / Configuring the NTP Service Restrictions.....	64
8.3.3.7.1 NAT or Firewall .....	65
8.3.3.7.2 Blocking Unauthorised Access .....	65
8.3.3.7.3 Allow Client Requests .....	65
8.3.3.7.4 Internal Client Protection / Local Network Threat Level .....	66
8.3.3.7.5 Addition of Exceptions to Standard Restrictions .....	66
8.3.3.7.6 Access Control Options .....	67
8.3.3.8 Symmetric Key and Autokey.....	68
8.3.3.8.1 Why Authentication? .....	69

8.3.3.8.2	How is Authentication used in the NTP Service?	69
8.3.3.8.3	How is a key created?	69
8.3.3.8.4	How does authentication work?	69
8.3.3.9	Autokey / Public Key Cryptography	70
8.3.4	ALARM Tab	71
8.3.4.1	Syslog Configuration	71
8.3.4.2	E-mail Configuration	72
8.3.4.3	SNMP Configuration / TRAP Configuration	73
8.3.4.4	Alarm Messages	74
8.3.5	DEVICE Tab	75
8.3.5.1	Device Information	75
8.3.5.2	Hardware Information	76
8.3.5.3	Restoring the Factory Settings - Factory Defaults	77
8.3.5.4	Restarting (Rebooting) the Board	77
8.3.5.5	Image Update & H8 Firmware Update	78
8.3.5.6	Customized Security Banner	80
8.3.5.7	Option FG7271/PPM: Minute Pulse Length (PPM)	81
8.3.5.8	Product Activation	82
8.3.5.9	Passwords (Master/Device)	83
8.3.5.10	Downloading Configurations / SNMP MIB	83
<b>9</b>	<b>SSH and Telnet Basic Configuration</b>	<b>84</b>
<b>10</b>	<b>Technical Data</b>	<b>85</b>
10.1	General	85
10.1.1	Design	85
10.1.2	Ambient conditions	85
10.1.3	CE compliant	85
10.1.4	NTP Accuracy	85
10.1.5	Time Protocols	86
10.1.6	TCP/IP Network Protocols	86
10.1.7	Configuration	86
10.1.8	Features	86
10.2	Special Technical Data of Board 7271RC	87
10.2.1	Board 7271RC with Option FG7271/PPM (Output Minute Pulse)	87
10.3	Special Technical Data of Board 7272RC	87
<b>11</b>	<b>Factory Defaults</b>	<b>88</b>
11.1	Network	88
11.2	NTP	89
11.3	ALARM	89
11.4	DEVICE	89
<b>12</b>	<b>Glossary and Abbreviations</b>	<b>90</b>
12.1	NTP-specific terminology	90
12.2	Tally Codes (NTP-specific)	90
12.2.1	Time-specific expressions	91
12.3	Abbreviations	92
12.4	Definitions	93
12.4.1	DHCP (Dynamic Host Configuration Protocol)	93
12.4.2	NTP (Network Time Protocol)	93

---

12.4.3 SNMP (Simple Network Management Protocol).....	94
12.4.4 TCP/IP (Transmission Control Protocol / Internet Protocol) .....	94
12.5 Syslog Messages .....	95
12.6 Accuracy & NTP Basic Principles .....	95
<b>13 List of RFCs.....</b>	<b>98</b>
<b>14 List of Open Source Packages used .....</b>	<b>99</b>



# 1 General

LAN Board 7271RC/7272RC is a **Network Time Server** (NTS) for the **hopf** 7001RC System in 19" (3U) racks.

Board 7271RC is equipped with 10/100 Base-T (auto-sensing) Ethernet interface (ETH0).

Board 7272RC is equipped with one or two Ethernet interfaces (ETH0 + ETH1) and can be used in different Sub-Networks with respectively 10/100/1000 Base-T (autosensing). Both interfaces allow the configuration of the board 7272RC.

Board 7271RC/7272RC can be used by networks for highly accurate synchronisation over **NTP (Network Time Protocol)**, which is available worldwide. The following synchronisations protocols are available:

- NTP
- SINEC H1 time data string
- Daytime
- Time

The network connection of the LAN Board 7271RC/7272RC can be installed at any desired point on the network.

Up to 31 of these LAN Boards can be implemented independently from each other in the Base System 7001RC on a modular basis (depending on the system configuration).

Due to its **hot-plug capability**, the Board 7271RC/7272RC can be removed from and re-connected to the running 7001RC system at any time and at any point, without affecting the function of other system boards.

A variety of management and monitoring functions are available (e.g. SNMP traps, E-mail notification, Syslog messages).

Increased security is freely available via optional encryption methods such as symmetric keys, Autokey and access restrictions and the disabling of unused protocols.

Extensive parameters are provided to suit the conditions of individual applications by means of a variety of access / configuration channels.

- The accessibility of the LAN Board 7271RC/7272RC in the network can be established via the **hopf** Base System menu or remote software.
- The Board is configured over Ethernet:
  - HTTP/HTTPS WebGUI (**G**raphical **U**ser **I**nterface) by means of a web browser
  - Or text-based menus over Telnet and SSH
- Various protocols (e.g. IPv4, http, https, Telnet etc.) are available for the Ethernet connection.

## 2 Board 7271RC/7272RC Basic Functions

### Time Protocols

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

### Network Protocols

- HTTP/ HTTPS
- DHCP
- Telnet
- SSH
- SNMP
- NTP
- SINEC H1 time datagram

### Configuration Channel

- HTTP/HTTPS WebGUI (browser-based)
- Telnet
- SSH
- External LAN configuration tool
- **hopf** 7001RC system keypad and display

### Ethernet Interface 7271RC

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

### Additionally on Board 7272RC

- 1000 Mbps half-/full duplex

## Features

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

## Internal to the Board

An embedded Linux is responsible for the correct operation of the Board. The following Linux operating system version is in use:

7271: Linux hopf727x 2.4.21-NANO (Linux Kernel 2.4.21 with Nano Kernel extension).

7272: Linux-2.6.22.1 with LINUXPPS Kit

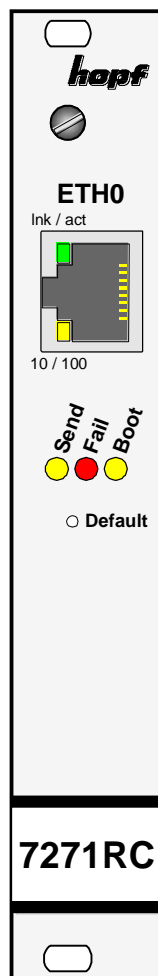
### 3 Board 7271RC Construction

This Chapter describes the hardware components of Board 7271RC.

#### 3.1 Board 7271RC Front Panel

Board 7271RC has a 3U/4HP front panel for 19" systems. It is equipped with the following components:

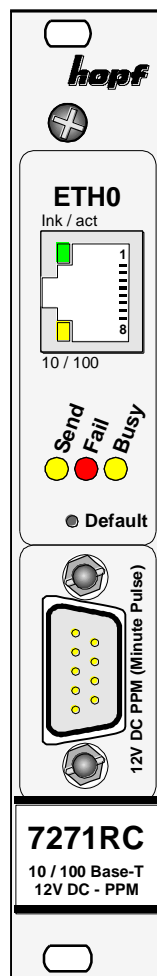
##### 3U/4HP Front Panel



##### 3U/4HP Front Panel

with Option

##### FG7271/PPM



**ETH0-RJ45 socket** - Ethernet LAN Interface

**Ink/act LED** - Activity with the Ethernet

**10/100 LED** - 10/100 MBit Ethernet

**Send/system bus LED** - Access to the Internal System Bus

**Fail LED** - Readiness for Operation

**Boot LED** - Boot Status

**Default Button** - Board Reset / Default Setting

**SUB-D male connector (9-pole)**

Pin-No.	Assignment
1	Minute pulse of defined duration (isolated, reference potential GND1)
2	reserved
3	reserved
4	reserved
5	GND
6	+12V DC (isolated, reference potential GND1)
7	reserved
8	reserved
9	GND1 (isolated for minute pulse / +12V DC)

Optionally (FG7271/PPM) the Board 7271RC is assembled with a SUB-D male connector to put out a minute pulse (PPM).

### 3.1.1 Status LEDs of the Board 7271RC

Board 7271RC has Status LEDs on the front panel. These facilitate detection of the operating status of installed boards.

The LEDs represent the following board conditions:

SEND LED (yellow)	Description
Flashing / flickering	<b>Normal case</b> – indicates access to the system bus. Board 7271RC is correctly integrated into System 7001RC or 68xx.
Off	Board 7271RC is not ready for operation.
On	Fault on Board 7271RC.

Fail LED (red)	Description
Off	<b>Normal case</b> – Board 7271RC is not detecting any operating failure.
On	Board 7271RC is not ready for operation or booting of the Board is delayed (see <b>Chapter 5.1 Delayed Readiness for Operation after Switch-on / Reset</b> ).
Flashing (every second)	Default button activated for less than 5 seconds.

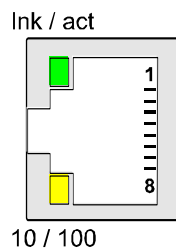
Boot LED (yellow)	Description
Off	<b>Normal case</b> – Board 7271RC is in operation.
On	Board 7271RC is booting its operating system (duration approx. 1 minute).

Ink/act LED (green)	Description
Off	There is no LAN connection to a network.
On	LAN connection available.
Flashing	Activity (send / receive) on network.

10/100 LED (yellow)	Description
Off	10 MBit Ethernet detected.
On	100 MBit Ethernet detected.

### 3.1.2 RJ45 Socket (ETH0)

#### ETH0



Pin No.	Assignment
1	Tx+
2	Tx-
3	Rx+
4	Not in use
5	Not in use
6	Rx-
7	Not in use
8	Not in use
9	Not in use

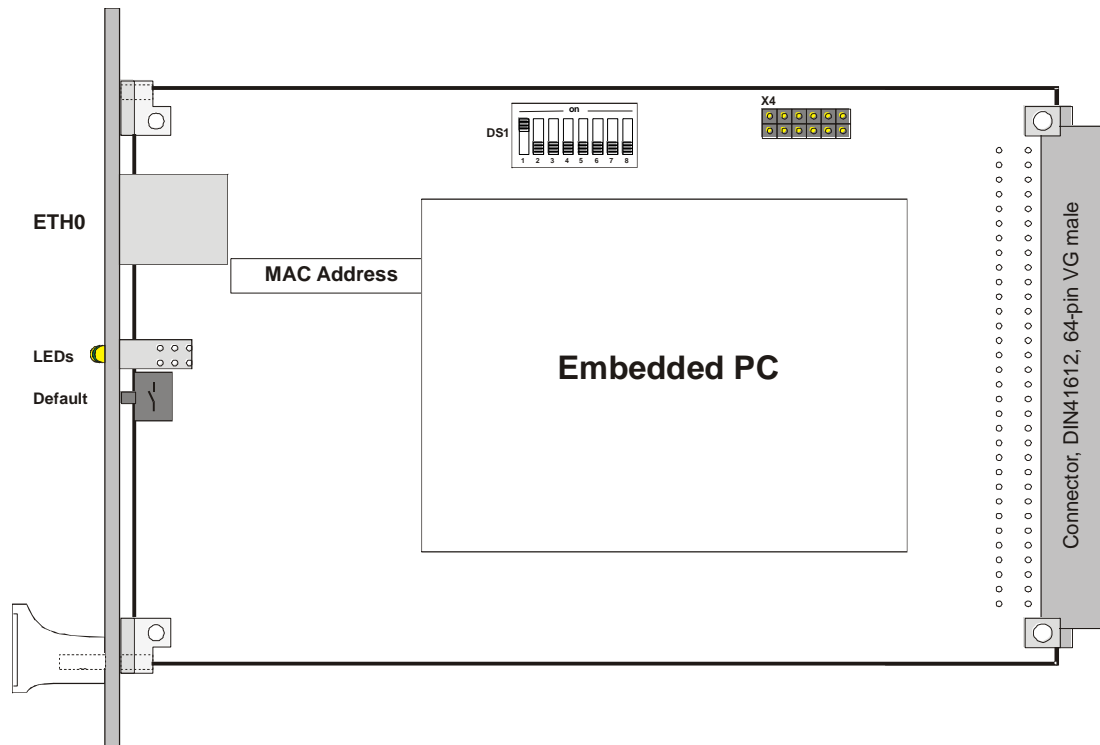


The meanings of the RJ45 socket LEDs are described in **Chapter 3.1.1 Status LEDs of the Board 7271RC**.

### 3.1.3 Reset / Default Button

The default button is activated by means of a thin object through the hole in the front panel next to the "Default" inscription (see **Chapter 5.2 Reset / Default**).

## 3.2 Overview of Board 7271RC (3U/4HP) Assembly



### 3.2.1 DIP Switch DS1

The Board number in the Base System is set here.

DIP Switch DS1	Function
8	No function at present
7	<b>Accuracy of the NTP</b> message 7271RC 7272RC is used in the system 7001RC for the generation of status and error messages (see <b>chapter 6.2 NTP Accuracy Message for Status- and Error Messages in System 7001RC</b> )
6	Transmissions point of SINEC H1 time datagram (see <b>chapter 8.3.2.6.3 Transmission point of SINEC H1 time datagram</b> )
5	Board number in System 7001RC (see <b>chapter 6.1 Setting the System Board Number</b> )
4	
3	
2	
1	

### 3.2.2 MAC Address for ETH0

Each LAN interface is uniquely identifiable in the Ethernet by means of a MAC address (hardware address).

The MAC address assigned to the respective LAN interface ETH0 can be found on the label assigned to the board 7271RC. A unique MAC address is assigned by **hopf** Elektronik GmbH for each LAN interface.



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

### 3.2.3 Heat Sink

Due to the installation height, care should be taken to ensure that the heat sink does not make contact with surrounding system components when removing or inserting Board 7271RC.



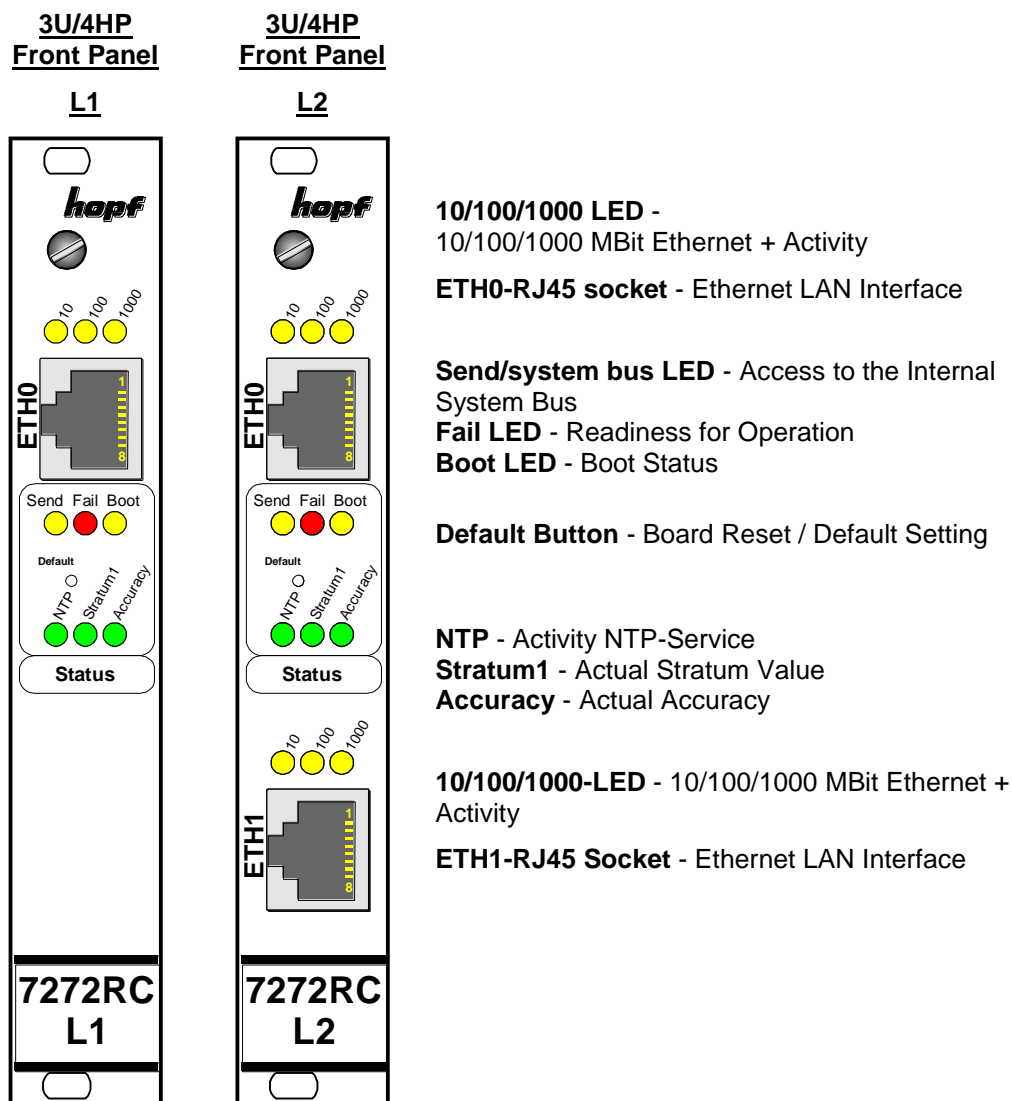
## 4 Board 7272RC Construction

This Chapter describes the hardware components of Board 7272RC.

The board 7272RC is actually available in two different versions. Version L1 has one Ethernet Interface and Version L2 has two Ethernet Interfaces for two independent subnets.

### 4.1 Board 7272RC Front Panel

Board 7272RC has a 3U/4HP front panel for 19" systems or 1U front panel for 1U systems. It is equipped with the following components.



#### 4.1.1 Status LEDs of the Board 7272RC

Board 7272RC has Status LEDs on the front panel. These facilitate detection of the operating status of installed boards.

The LEDs represent the following board conditions:

##### Board Status LEDs

<b>SEND LED (yellow)</b>	<b>Description</b>
Flashing / flickering	<b>Normal case</b> – indicates access to the system bus. Board 7272RC is correctly integrated into System 7001 or 68xx.
Off	Board 7272RC is not ready for operation.
On	Fault on Board 7272RC.
<b>Fail LED (red)</b>	<b>Description</b>
Off	<b>Normal case</b> – Board 7272RC is not detecting any operating failure.
On	Board 7272RC is not ready for operation or booting of the Board is delayed (see <b>Chapter 5.1 Delayed Readiness for Operation after Switch-on / Reset</b> ).
Flashing (every second)	Default button activated for less than 5 seconds.
<b>Boot LED (yellow)</b>	<b>Description</b>
Off	<b>Normal case</b> – Board 7272RC is in operation.
On	Board 7272RC is booting its operating system (duration approx. 1 minute).

##### NTP Status LEDs

<b>NTP-LED (Green)</b>	<b>NTP Service of the Board 7272RC</b>
On	<b>Normal case</b> , is started
Off	is started
<b>Stratum1-LED (Green)</b>	<b>NTP Service of the Board 7272RC works with:</b>
On	Stratum 1
Flashing	Stratum 2-15
Off	Stratum16
<b>Accuracy-LED (Yellow)</b>	<b>NTP Service of the Board 7272RC works with:</b>
On	High accuracy
Flashing	Medium accuracy
Off	Low accuracy

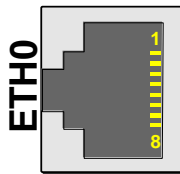


The board internal NTP service works with the highest accuracy if all NTP Status LED are lighted.

### LAN Status LEDs

LAN LED ETH0/ETH1 (Yellow)			Description
10	100	1000	
Flashes	Off	Off	10MBit link with activity
	On	Off	100MBit link with activity
	Off	On	1000MBit link with activity
Off	---	---	no activity LAN

### 4.1.2 RJ45 Socket (ETH0 / ETH1)



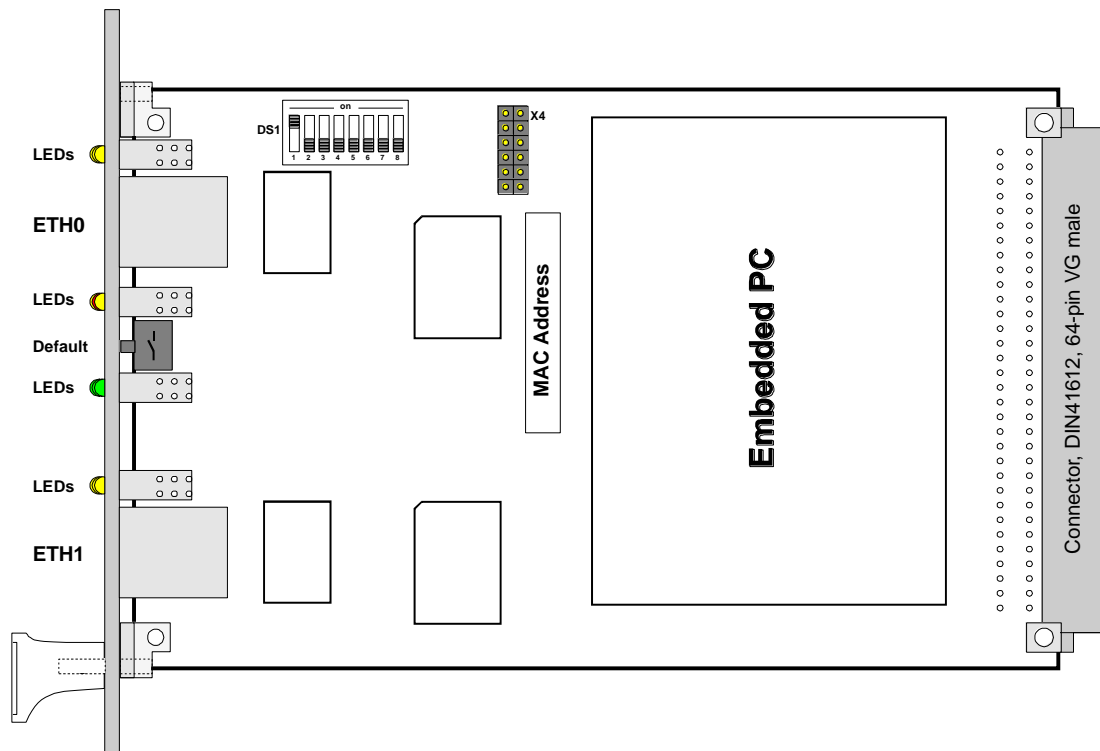
Pin No.	Assignment
1	Tx+
2	Tx-
3	Rx+
4	Not in use
5	Not in use
6	Rx-
7	Not in use
8	Not in use
9	Not in use

### 4.1.3 Reset / Default Button

The default button is activated by means of a thin object through the hole in the front panel next to the "Default" inscription (see **Chapter 5.2 Reset / Default**).

## 4.2 Overview of Board 7272RC (3U/4HP) Assembly

Version L2:



### 4.2.1 DIP Switch DS1

The Board number in the Base System is set via DIP switch DS1.

DIP Switch DS1	Function
8	No function at present
7	<b>Accuracy of the NTP</b> message 7271RC 7272RC is used in the system 7001RC for the generation of status and error messages (see <b>chapter 6.2 NTP Accuracy Message for Status- and Error Messages in System 7001RC</b> )
6	Transmissions point of SINEC H1 time datagram (see <b>chapter 8.3.2.6.3 Transmission point of SINEC H1 time datagram</b> )
5	Board number in System 7001RC (see <b>chapter 6.1 Setting the System Board Number</b> )
4	
3	
2	
1	

#### 4.2.2 MAC Address for ETH0 / ETH1

Each LAN interface is uniquely identifiable in the Ethernet by means of a MAC address (hardware address).

The MAC address assigned to the respective LAN interface ETH0 can be found on the label assigned to the board 7272RC. If exists the MAC address for ETH1 is incremented hexadecimal by 1 to the MAC address of ETH0.

Example:

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

The MAC address is assigned once-only by **hopf** Elektronik GmbH for each Ethernet interface.



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

#### 4.2.3 Heat Sink

Due to the installation height, care should be taken to ensure that the heat sink does not make contact with surrounding system components when removing or inserting Board 7272RC.

## 5 Board 7271RC/7272RC System Performance

Behaviour of Board 7271RC/7272RC when switching on and resetting the Base System and when activating the default button on the front panel.

### 5.1 Delayed Readiness for Operation after Switch-on / Reset

Board 7271RC/7272RC requires an increased supply current during the boot procedure (Board start-up). In order to guarantee the power management of the system, booting of the Board is delayed dependent on the set System Board number.

The red Fail LED on the front panel lights up during the delay phase.



Booting delay = Board number x 30 seconds

### 5.2 Reset / Default Button

Board 7271RC/7272RC can be reset or placed in default status with the aid of the default button which is located behind the Board's front panel. The default button can be accessed by means of a thin object through a small hole in the front panel.

Default Button	Description
Press for approx. 1 second	Trigger Board reset (see <b>Chapter 5.2.1 Board Reset</b> )
Press for more than 5 seconds	Place Board in default status (see <b>Chapter 5.2.2 Place LAN Parameters in Default Status</b> )

### 5.2.1 Board Reset

A reset is triggered on Board 7271RC/7272RC by briefly pressing the default button (approx. 1-2 seconds). This reset does not affect the Base System and its other functions.

Trigger Board reset with the default button:

1. Briefly press default button (approx. 1-2 seconds).
2. Board reset takes place maximum 5 seconds after releasing the default button.
3. Red Fail LED lights up  $\Rightarrow$  Board 7271RC/7272RC is not yet ready for operation.
4. Yellow Send LED flickers  $\Rightarrow$  Board 7271RC/7272RC is integrated into the Base System.
5. Red Fail LED goes out and yellow Boot LED lights up  $\Rightarrow$  the Board 7271RC/7272RC begins to boot depending on the set Board number (the boot process can take up to one minute).
6. Full operating status is obtained when:
  - Send LED flickers
  - Fail LED is not lit
  - Boot LED is not lit



Board 7271RC/7272RC is not immediately accessible following a reset (see **Chapter 5.1 Delayed Readiness for Operation after Switch-on / Reset**).



There run an embedded Linux-System and a  $\mu$ -processor-system on board 7271RC/7272RC for implementation of high-precision processes in real-time environment. These processes require an exact coordination of such two systems, monitored by a so-called alive-handling. Thus the detection of just a minimal deviation or rather recognizing of a problem in the network the board 7271RC/7272RC automatically performs a reboot that resets the board into a defined and correct condition.

This process lasts approximately 60 seconds and can occur at different intervals depending on the diverse ambient conditions.

During this time the board 7271RC/7272RC is not available in the net. In conjunction with NTP though this period is not critical and does not impact the time synchronisation through NTP. This is an intra-board process and does not impact the remaining clock system.

This behaviour of the board can not be influenced by the user.

## 5.2.2 Place LAN Parameters in Default Status

Board 7271RC/7272RC can be placed in default status by means of the default button in the event that the Board is no longer reachable on the Ethernet following incorrect configuration (e.g. over the Ethernet).

If the default button is pressed for longer than 5 seconds, the following LAN parameters which are stored on the Board are set in the DHCP mode:

- IP 000.000.000.000
- Gateway 000.000.000.000
- Network mask 000.000.000.000



The LAN parameter like IP address, Netmask and Gateway are not changed in the system 7001RC. After a default they will be assumed from the board 7271RC/7272RC.



All other configurations can only be set to default status via the Ethernet interface (see **Chapter 8.3.5.3 Restoring the Factory Settings - Factory Defaults**).

### Set Board 7271RC/7272RC to default status.

1. Press the default button
2. Red Fail LED flashes every second until "Trigger Default" is reached (after approx. 5 seconds)
3. Release the default button
4. Board 7271RC/7272RC takes over the default settings
5. Board 7271RC/7272RC triggers a Board reset
6. Create accessibility to the Ethernet ETH0 via the Base System (reset the IP address, gateway and network mask via the Base System menu)
7. Check all configurations in the WebGUI and reset if necessary



## 6 Implementing Board 7271RC/7272RC in a *hopf* Base System

All Function Boards are parameterised individually from within the Base System.



Each Function Board is uniquely identified in a *hopf* Base System via the Board type and an assigned Board number

The following steps are required for the purpose of implementation:

- Free slot available in the Base System
- Not more than 30 LAN boards already implemented in the system
- Set a Board number that is not yet assigned in the Base System via the DIP switch on Board 7271RC/7272RC
- Insert the LAN Board
- Select the LAN Board setting menu in the Base System (LAN x / x = set Board number)
- Set the desired LAN parameters (IP address, network mask and gateway) via the menu or remote software
- Configure LAN Board 7271RC/7272RC over WebGUI and Ethernet

### 6.1 Setting the System Board Number

The boards must be coded to a System Board number in order to enable the various LAN Boards to be administered and configured in the Base System.



**Under no circumstances** may two LAN Boards 7271RC/7272RC with the same Board number be integrated into one Base System. This leads to unspecified faults on these two Boards!

The coding of the Board number takes place on Board 7271RC/7272RC via DIP switch bank (DS1).

### 6.1.1 Setting the Board Number for Base System 7001RC

A maximum of 31 LAN Boards 7271RC/7272RC can be configured in System 7001RC. The Board number is set via the DIP switch bank (**DS1 / SW1-5**) for unique identification in the Base System.

SW5	SW4	SW3	SW2	SW1	System Board No.:
off	off	off	off	off	-
off	off	off	off	on	Board Nr. 01
off	off	off	on	off	Board Nr. 02
off	off	off	on	on	Board Nr. 03
off	off	on	off	off	Board Nr. 04
off	off	on	off	on	Board Nr. 05
off	off	on	on	off	Board Nr. 06
off	off	on	on	on	Board Nr. 07
off	on	off	off	off	Board Nr. 08
off	on	off	off	on	Board Nr. 09
off	on	off	on	off	Board Nr. 10
off	on	off	on	on	Board Nr. 11
off	on	on	off	off	Board Nr. 12
off	on	on	off	on	Board Nr. 13
off	on	on	on	off	Board Nr. 14
off	on	on	on	on	Board Nr. 15
on	off	off	off	off	Board Nr. 16
on	off	off	off	on	Board Nr. 17
on	off	off	on	off	Board Nr. 18
on	off	off	on	on	Board Nr. 19
on	off	on	off	off	Board Nr. 20
on	off	on	off	on	Board Nr. 21
on	off	on	on	off	Board Nr. 22
on	off	on	on	on	Board Nr. 23
on	on	off	off	off	Board Nr. 24
on	on	off	off	on	Board Nr. 25
on	on	off	on	off	Board Nr. 26
on	on	off	on	on	Board Nr. 27
on	on	on	off	off	Board Nr. 28
on	on	on	off	on	Board Nr. 29
on	on	on	on	off	Board Nr. 30
on	on	on	on	on	Board Nr. 31



Only these Board numbers set with the DIP switch are allowable in System 7001RC.  
System 7001RC is unable to configure Board numbers which are set outside the range of the system (31).

## 6.2 NTP Accuracy Message for Status- and Error Messages in System 7001RC



The evaluation of NTP Accuracy message is available from version 07.00 of 7020RC.

The evaluation of the **NTP Accuracy message** for the generation of status and error messages can be allowed / suppressed for the base system 7001RC by each board 7271RC/7272RC with DIP switch DS1 – SW7.

DIP Switch DS1- SW7	Function
ON	Evaluation of NTP Status in System 7020RC allowed
OFF	Evaluation of NTP-Status in System 7020RC not allowed

The status messages of the system 7020RC are described in the base manual in the chapter status and error messages.

## 6.3 Creating the Network Connection



Ensure that the network parameters of the LAN Board are configured in accordance with the local network before connecting the LAN Board to the network (see **Chapter 7 Network Configuration for ETH0 via the Base System**).



Connecting a network to an incorrectly configured LAN Board (e.g. duplicated IP address) may cause interference in the network.



Request the required network parameters from your network administrator if you do not know them.

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

## 7 Network Configuration for ETH0 via the Base System

The only configuration that is carried out on Board 7271RC/7272RC via the Base System is to enable it to be reachable on the network via **ETH0**. All other configurations on the Board are carried out over the WebGUI.

Configuring the network can only be done via the WebGUI but not via the base system.

Setting-up the boards 7271RC/7272RC via the base system is identical. For this reason only board 7271RC is described in the following examples.

LAN Board 7271RC/7272RC is configured via the keyboard of the respective Base System. The necessary network parameters are configured such as IP address, gateway address, network mask and a general control byte.

The Technical Description of the respective Base System is the basis for configuration.



After they have been entered fully, the LAN parameters configured through the system menu are transferred to the control board by pressing the **ENT** key. From here the parameters are transferred to the LAN board.



The Base System accept LAN parameters which are subsequently changed via the WebGUI.

### IP Address (IPv4)

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

**Example: 192.002.001.123**

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

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

#### Class A Networks

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

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

**Example: 100.000.000.001, (Network 100, Host 000.000.001)**

#### Class B Networks

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

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

**Example: 172.001.003.002 (Network 172.001, Host 003.002)**

### Class C Networks

IP addresses 192.000.000.xx to 223.255.255.xxx

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

### Class D Networks

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

### Class E Networks

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

### Gateway Address

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

### Network Mask

The network mask is used to partition IP addresses outside of network classes A, B and C. When entering the network mask it is possible to designate the number of bits of the IP address to be used as the network part and the number to be used as the host part, e.g.:

Network Class	Network Part	Host Part	Network Mask Binary	Network Mask Decimal
A	8 Bit	24 Bit	11111111.00000000.00000000.00000000	255.0.0.0
B	16 Bit	16 Bit	11111111.11111111.00000000.00000000	255.255.0.0
C	24 Bit	8 Bit	11111111.11111111.11111111.00000000	255.255.255.0

The number of bits for the host part is entered in order to calculate the network mask:

Network Mask	Host Bits
255.255.255.252	2
255.255.255.248	3
255.255.255.240	4
255.255.255.224	5
255.255.255.192	6
255.255.255.128	7
255.255.255.000	8
255.255.254.000	9
255.255.252.000	10
255.255.248.000	11
.	.
.	.
255.128.000.000	23
255.000.000.000	24

### Example:

Desired network mask:

**255.255.255.128**

Value to be entered:

**7**

## 7.1 Input Functions of Base Systems 7001RC



After they have been entered fully, the LAN parameters configured through the system menu are transferred to the control board by pressing the **ENT** key. From here the parameters are transferred to the LAN board.

The input and display functions of the board parameters are polled in the menu heading **BOARD-SETUP: 4**

with **ENT** key      ⇒ Main menu  
with **4** key          ⇒ Board setup  
with **N** key          ⇒ Scroll to menu heading:

[illegible]

Select with key **y**

Search for board to be parameterized with key **N** and select with key **Y**.

Example:

PARAMETER	BOARD 03 OF 25	7271 NO.:01
STATUS:M/-	BOARDNAME:"ETHERNET"	SET>Y/N

<b>PARAMETER BOARD 03 OF 25</b>	⇒ board <b>03</b> of <b>25</b> implemented
<b>7271RC NO.: 01</b>	⇒ board type <b>7271RC</b> with board number <b>01</b>
<b>STATUS: M (I)/- (E)</b>	⇒ <b>M or I</b> = monitoring <b>or</b> no monitoring
	⇒ <b>E or -</b> = without error operating <b>or</b> board error
<b>BOARDNAME:"ETHERNET "</b>	⇒ <b>ETHERNET</b> board name freely selected by customer, up to 8 characters

### 7.1.1 Inputting the Static IPv4 Address / DHCP Mode

## Static IPv4 Address

In the upper line the selected board appears with its board number and IPv4 address of the LAN interface ETH0. For configuration of a new IPv4 address the complete entry of the 4 groups of digits is necessary.

The IPv4 address is entered in 4 groups of digits configurable from 000 to 255. They are separated by a dot ( . ). Input must be in the form of 3 digits (e.g.: 2 ⇒ 002).

An example of a complete entry would be as follows:

B.7271	NO. : 01	IP-ADR	>192.168.017.001<
	NEW	IP-ADDRESS	>~~~,~~~,~~~,~~~<

In the case of an implausible entry (such as 265), an INPUT ERROR is sent and the complete entry is rejected.

### DHCP / Static IP Address Assignment

For the use of DHCP, the IP address, gateway address and network mask are all to be fully set to **>000.000.000.000<** (invalid IP address).

All other addresses are interpreted as static IP addresses.

## 7.1.2 Inputting the Gateway Address

The gateway address can be entered via the selection screen.

```
B . 7 2 7 1  NO . : 0 1  GW - ADR  > 2 5 5 . 0 0 0 . 0 0 0 . 0 0 0 <
NEW GW - ADDRESS  > ~ ~ ~ . ~ ~ ~ . ~ ~ ~ . ~ ~ ~ <
```

The Gateway address can now be entered in the same way as the IP address, as described in **Chapter 7.1.1 Inputting the Static IPv4 Address / DHCP Mode**.

## 7.1.3 Inputting the Network Mask

The network mask can be entered via the selection screen.

```
B . 7 2 7 1  NO . : 0 1  NETMASC  > 2 5 5 . 2 5 5 . 0 0 0 . 0 0 0 <
NEW NETMASC  > ~ ~ ~ . ~ ~ ~ . ~ ~ ~ . ~ ~ ~ <
```

The network mask for LAN interface ETH0 can now be entered in the same way as the IP address, as described in **Chapter 7.1.1 Inputting the Static IPv4 Address / DHCP Mode**.

## 7.1.4 Inputting the Control-Byte

The Control-Byte is shown on the top line with the currently set values.

```
B . 7 2 7 1  NR . : 0 1  CONTROL-BYTE  0 0 0 0 0 0 1 0
NEW CONTROL-BYTE  > ~ ~ ~ ~ ~ ~ ~ ~ <
```

For the purposes of manipulation, the individual bits of the new byte are to be entered on the second line using "0" and "1". The complete Control Byte must always be recorded and confirmed with the **ENT** key.

The bits of the Control Byte are numbered in descending order:

```
CONTROL-BYTE  > 7 6 5 4 3 2 1 0 <
```

### 7.1.4.1 Bit 7-1 - No Function at Present

Bits 7-1	No function at present
0	These bits should always be set to "0" for reasons of compatibility.

### 7.1.4.2 Bit 0 - Restoring Factory Settings

Bit 0	Restoring Factory Settings
0	Board 7271RC/7272RC is ready for use
1	Restoring factory settings followed by a reboot (see <b>Chapter 11 Factory Defaults</b> ).



Bit 0 must be set back to 0 after performing a factory default, so that a default is not performed again.

1. Set Control Byte Bit 0 = 1 ⇒ performing a default
2. Wait until Board 7271RC/7272RC is performing a reboot (visible by the shining Fail-LED). Afterwards the Boot-LED is shining for a reboot.
3. Set Control Byte Bit 0 = 0 ⇒ prevent performing a default.  
The fully operation status is reached when the Send-LED is flickering and the Fail-LED and the Boot-LED is not shining.

### 7.1.5 Inputting the Parameterbyte 01 (no function at present)

Parameter of Parameter-Byte 01 is shown on the top line with the currently set values.

```

B . 7 2 7 1  N O . : 0 1      O L D :   B Y T E   0 1  > 0 0 0 0 0 0 0 0 <
B Y T E   =   B I T   7 . . 0  N E W :   B Y T E   0 1  > ~ ~ ~ ~ ~ ~ ~ ~ <
    
```

For the purposes of manipulation, the individual bits of the new byte are to be entered on the second line using "0" and "1". The complete Parameter Byte must always be recorded and confirmed with the **ENT** key.

The bits of the Parameter Byte are numbered in descending order:

```

B Y T E   0 1  > 7 6 5 4 3 2 1 0 <
    
```

Bits 7-0	No function at present
0	These bits should always be set to "0" for reasons of compatibility.

### 7.1.6 Inputting the Parameterbyte 02 (no function at present)

Parameter of Parameterbyte 02 is shown on the top line with the currently set values.

```

B . 7 2 7 1  N O . : 0 1      O L D :   B Y T E   0 2  > 0 0 0 0 0 0 0 0 <
B Y T E   =   B I T   7 . . 0  N E W :   B Y T E   0 2  > ~ ~ ~ ~ ~ ~ ~ ~ <
    
```

For the purposes of manipulation, the individual bits of the new byte are to be entered on the second line using "0" and "1". The complete Parameter Byte must always be recorded and confirmed with the **ENT** key.

The bits of the Parameter Byte are numbered in descending order:

```

B Y T E   0 2  > 7 6 5 4 3 2 1 0 <
    
```

Bits 7-0	No function at present
0	These bits should always be set to "0" for reasons of compatibility.



## 8 HTTP/HTTPS WebGUI – Web Browser Configuration Interface

If there is no functional difference to board 7272RC the WebGUI screenshots displayed in this description refer to the board 7271RC.

Only the fully configurable Ethernet interface ETH1 of board 7272RC makes a difference.



JavaScript and Cookies must be enabled in the browser in order for the WebGUI to display and function correctly.



The WebGUI has been tested with the following browsers: MOZILLA 1.x, Netscape 7.x and IE 6.x – some functions do not run on older versions.

### 8.1 Quick Configuration

This Chapter briefly describes the basic operation of the WebGUI installed on the Board.

#### 8.1.1 Requirements

- Ready-for-operation **hopf** Base System with implemented Board 7271RC/7272RC
- Board configured for network operation (see **Chapter 7 Network Configuration for ETH0 via the Base System**)
- PC with installed web browser (e.g. Internet Explorer) in the sub-network of Board 7271RC/7272RC

#### 8.1.2 Configuration Steps

- Create the connection to the Board with a web browser
- Login as a '**master**' user (no password is set initially)
- Switch to "Network" tab and enter the DNS Server (required for NTP and the alarm)
- Save the configuration
- Switch to "Device" tab and restart Network Time Server via "Reboot Device"
- NTP Service is now available with the standard settings



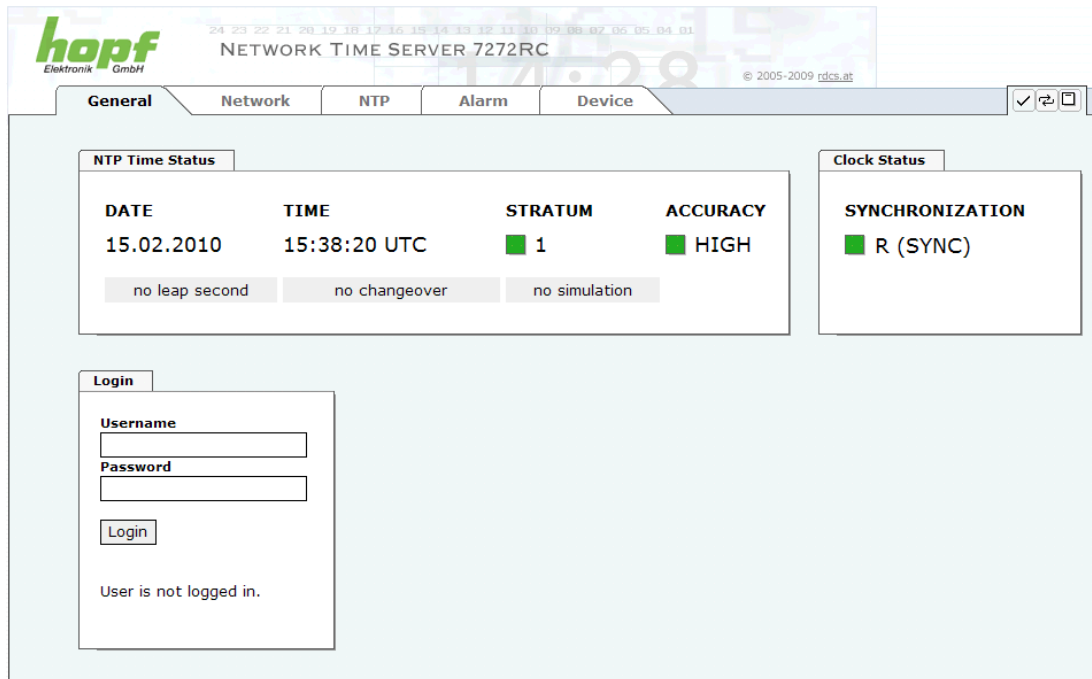
The following detailed explanatory information should be read if anything is unclear while executing the configuration steps.

## 8.2 General – Introduction

Board 7271RC/7272RC should be accessible to a web browser if it has been set up correctly. Enter the IP address - as set up on the Board earlier - or the DNS name on the address line <<http://xxx.xxx.xxx.xxx>> and the following screen should appear.



Configuration can only be completed via the Board's WebGUI!



The screenshot shows the WebGUI interface for the hopf NETWORK TIME SERVER 7272RC. The interface has a header with the hopf logo, a navigation bar with tabs for General, Network, NTP, Alarm, and Device, and a status bar at the top showing IP addresses and a copyright notice. The main content area is divided into two sections: NTP Time Status and Clock Status. The NTP Time Status section displays the current date (15.02.2010), time (15:38:20 UTC), stratum (1), and accuracy (HIGH). It also includes status indicators for leap second, changeover, and simulation. The Clock Status section shows the synchronization status (R (SYNC)). Below these sections is a Login form with fields for Username and Password, a Login button, and a message indicating the user is not logged in.



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

## 8.2.1 LOGIN and LOGOUT as a User

All of the Board's data can be read without being logged on as a special user. However, the Board data can only be configured or modified by an authorised user! Two types of user are defined:

- "master" user (user name <master> no password is set on delivery)
- "device" user (user name <device> no password is set on delivery)

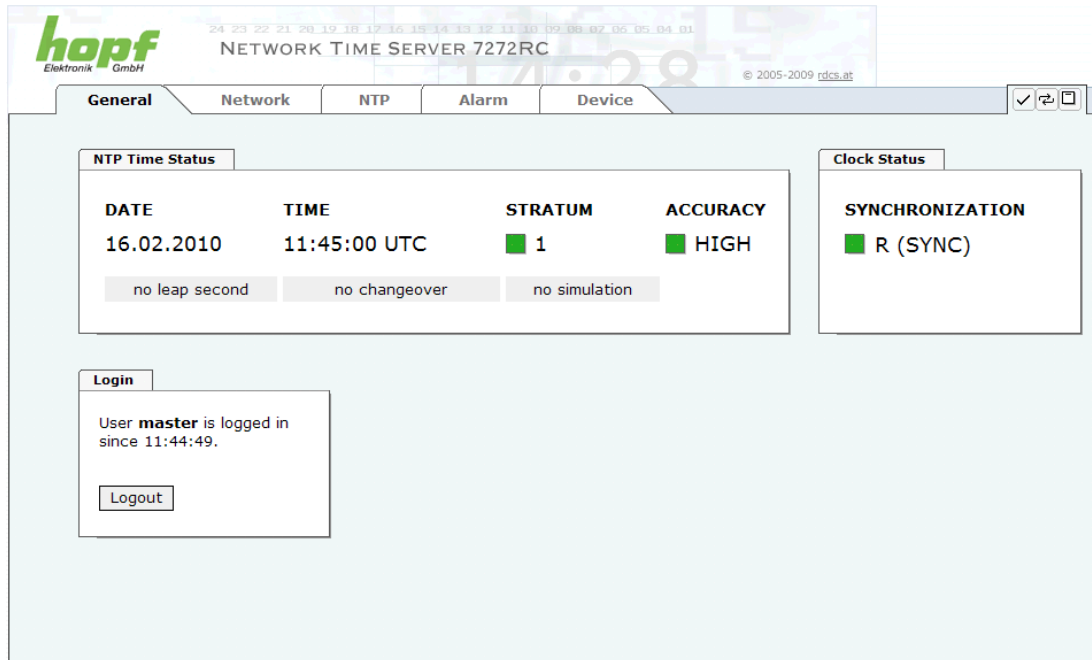


Differentiation is made between **upper and lower case** characters in the password. Alphanumeric characters and the following symbols can be used: `[]()*-_!$%&/=?`



The password should be changed after the first login for security reasons (see **chapter 8.3.5.9 Passwords**).

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



The screenshot shows the WebGUI interface for the hopf Elektronik GmbH. The top navigation bar includes tabs for General, Network, NTP, Alarm, and Device. The main content area is divided into two sections: NTP Time Status and Clock Status.

**NTP Time Status**

DATE	TIME	STRATUM	ACCURACY
16.02.2010	11:45:00 UTC	1	HIGH

Below the table, there are three status indicators: "no leap second", "no changeover", and "no simulation".

**Clock Status**

SYNCHRONIZATION
R (SYNC)

**Login**

User **master** is logged in since 11:44:49.

Logout

Click on the **Logout** button to log out. WebGUI is equipped with session management. If a user does not log out, he or she is automatically logged off 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.

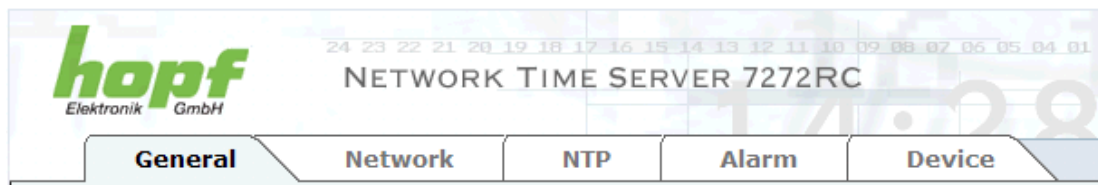
Users logged in as **Master** have all access rights to Board 7271RC.

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 certification
- Change master password
- Download configuration files

## 8.2.2 Navigation via the Web Interface

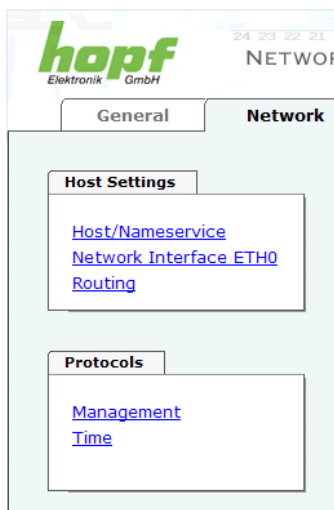
The WebGUI is divided into function tabs. Click on one of these tabs to navigate through the Board. The selected tab is identified by a darker background colour, see the following image (General in this case).



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



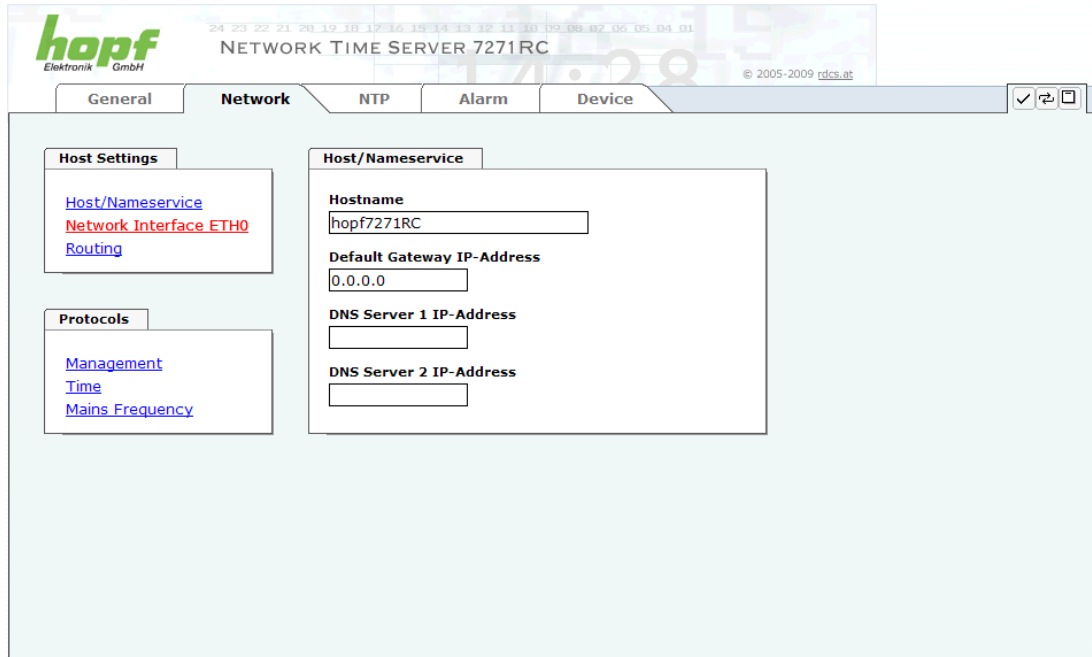
JavaScript should be enabled in the browser in order to guarantee the correct operation of the web interface.



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

### 8.2.3 Inputting or Changing Data

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



After an entry has been made the configured field is marked with a star ' \* '. This means that a value has been entered or changed but is not yet stored in the flash memory. It is necessary to be acquainted with the symbols shown below in order to be able to save the configuration or the changed value.



Meaning of the symbols from left to right:

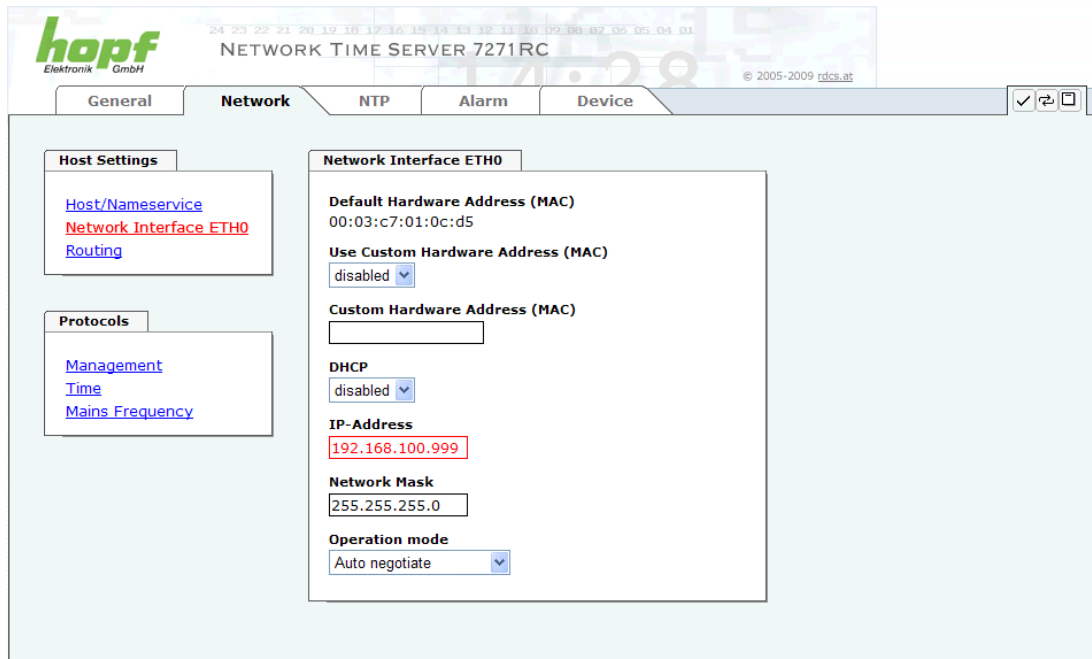
No.	Symbol	Description
1	<b>Apply</b>	Acceptance of changes and entered data
2	<b>Reload</b>	Restoring the saved data
3	<b>Save</b>	Permanent storage of the data in the flash configuration

For permanent storage the value **MUST** be accepted by the Board with **Apply** and then saved with **Save**.

If the data is only to be tested it is sufficient to accept the changes with **Apply**. However, this data is then lost when the **hopf** Base System is switched off or restarted.

## 8.2.4 Plausibility Check during Input

A plausibility check is generally carried out during input.



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



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

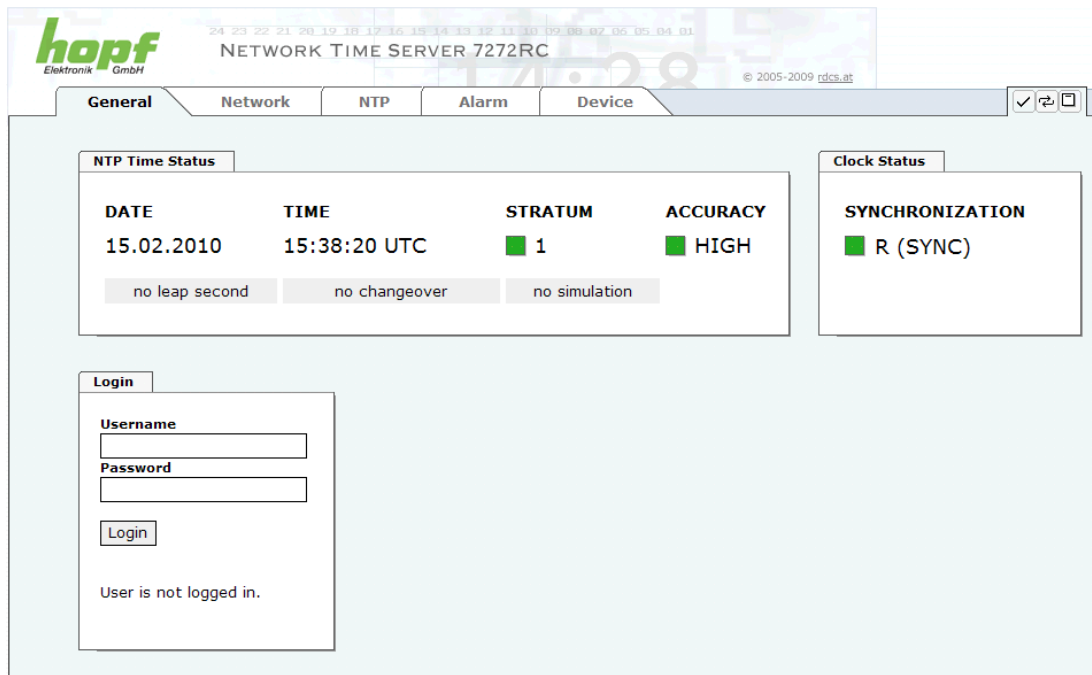
## 8.3 Description of the Tabs

The WebGUI is divided into the following tabs:

- General
- Network
- NTP
- Alarm
- Device

### 8.3.1 GENERAL Tab

This is the first tab which is displayed when using the web interface.



The screenshot shows the 'General' tab of the hopf WebGUI. At the top, there is a header bar with the hopf logo, a digital clock 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 'NETWORK TIME SERVER 7272RC'. Below the header, there are five tabs: 'General', 'Network', 'NTP', 'Alarm', and 'Device'. The 'General' tab is selected. The main content area is divided into two sections: 'NTP Time Status' and 'Clock Status'. The 'NTP Time Status' section contains a table with columns 'DATE', 'TIME', 'STRATUM', and 'ACCURACY'. The 'DATE' is '15.02.2010', 'TIME' is '15:38:20 UTC', 'STRATUM' is '1' (indicated by a green square), and 'ACCURACY' is 'HIGH' (indicated by a green square). Below the table, there are three buttons: 'no leap second', 'no changeover', and 'no simulation'. The 'Clock Status' section contains a 'SYNCHRONIZATION' status 'R (SYNC)' (indicated by a green square). At the bottom left, there is a 'Login' section with fields for 'Username' and 'Password', a 'Login' button, and a message 'User is not logged in.'

#### NTP Time Status

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

Stratum displays the actual NTP stratum value of the board 7271RC/7272RC (value range from 1-16).

The **ACCURACY** (accuracy of NTP) field contains the values LOW, MEDIUM and HIGH. The meaning of these values is explained in **Chapter 12.6 Accuracy & NTP**.

The **Leapsecond** and **Changeover** display fields announce that such an event is to take place on the next hour change.

The **Simulation display** is used if the system time of the **hopf** Base System is marked as a simulated time (not currently available).

### Clock Status

Display of the actual status of synchronisation of **hopf** Base system with this possible values:

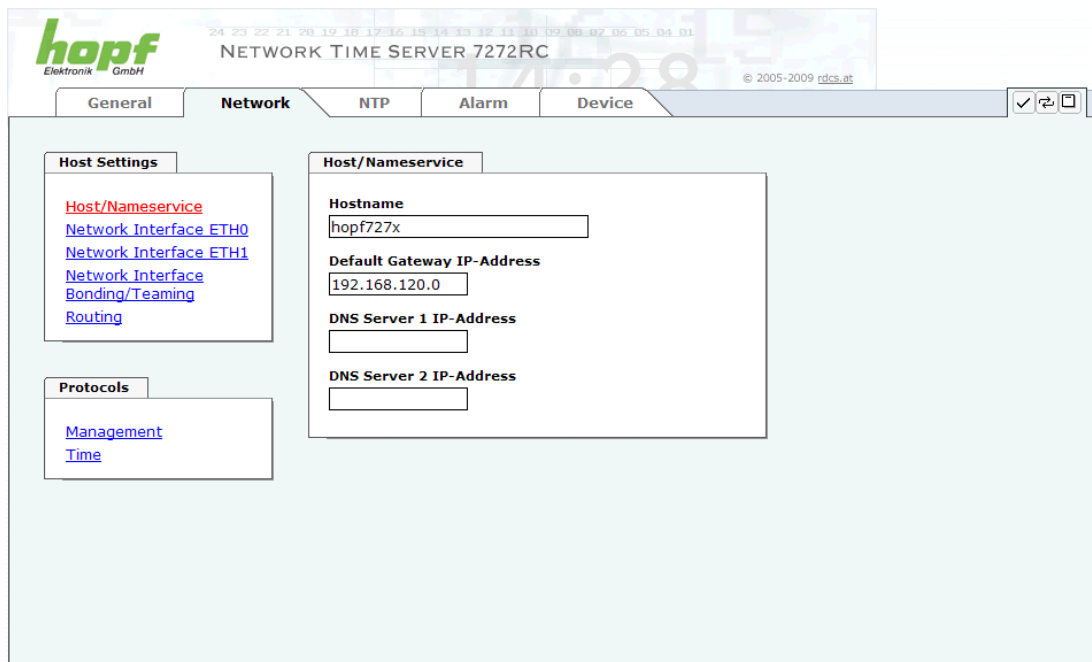
- invalid** Invalid time
- C** The system is in crystal mode (C = Crystal)
- r** The system is synchronous to the synchronization source but without regulating the internal crystal generator
- R** The system is synchronous to the synchronization source and the crystal generator will be regulated

### Login

The **Login** box is used in accordance with **Chapter 8.2.1 LOGIN and LOGOUT as a User.**

## 8.3.2 NETWORK Tab

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



The screenshot shows the 'hopf' web interface for a 'NETWORK TIME SERVER 7272RC'. The top navigation bar includes tabs for 'General', 'Network' (selected), 'NTP', 'Alarm', and 'Device'. Below the navigation bar, there are two main sections: 'Host Settings' and 'Host/Nameservice'. The 'Host Settings' section contains links for 'Host/Nameservice', 'Network Interface ETH0', 'Network Interface ETH1', 'Network Interface Bonding/Teaming', and 'Routing'. The 'Host/Nameservice' section contains input fields for 'Hostname' (filled with 'hopf727x'), 'Default Gateway IP-Address' (filled with '192.168.120.0'), 'DNS Server 1 IP-Address', and 'DNS Server 2 IP-Address'. The 'Protocols' section contains links for 'Management' and 'Time'.



### 8.3.2.1 Host/Nameservice

Setting for the unique network identification.

#### 8.3.2.1.1 Hostname

The standard setting for the Hostname is "**hopf727x**". 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.



A BLANK Hostname is not a valid name and can cause the Board to malfunction.

#### 8.3.2.1.2 Default Gateway

The standard gateway is generally configured via the Base System menu. However it can also be changed via the web interface.

Contact your network administrator for details of the standard gateway if not known.

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

#### 8.3.2.1.3 DNS Server 1 & 2

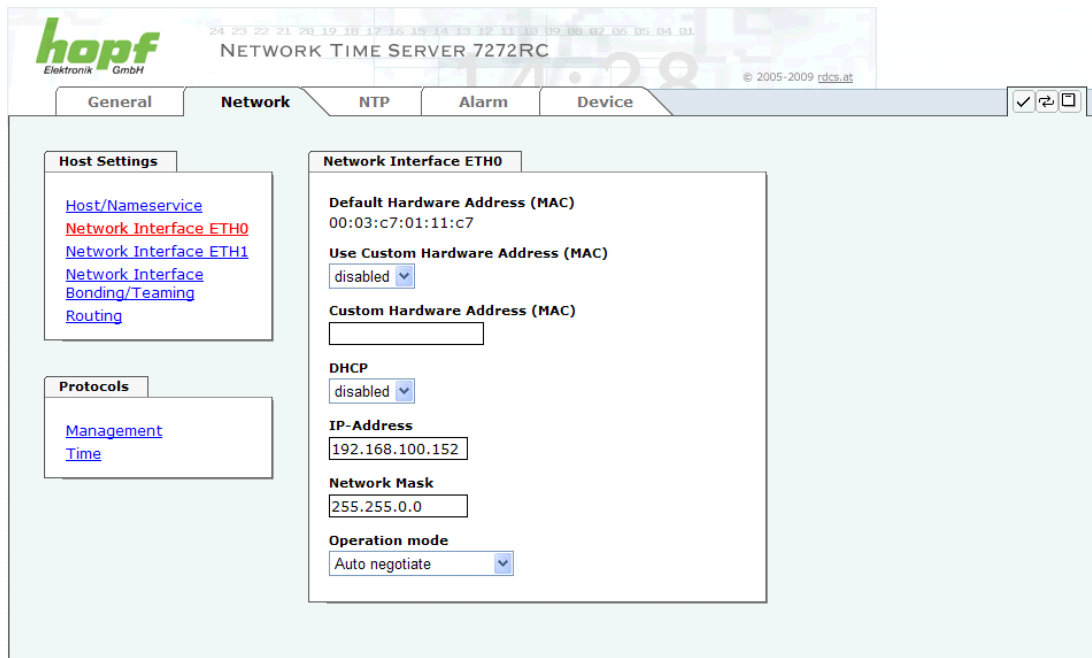
The IP address of the DNS server should be entered if you wish to use complete Hostnames (hostname.domainname) or work with reverse lookup.

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

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

### 8.3.2.2 Network Interface ETH0 / ETH1

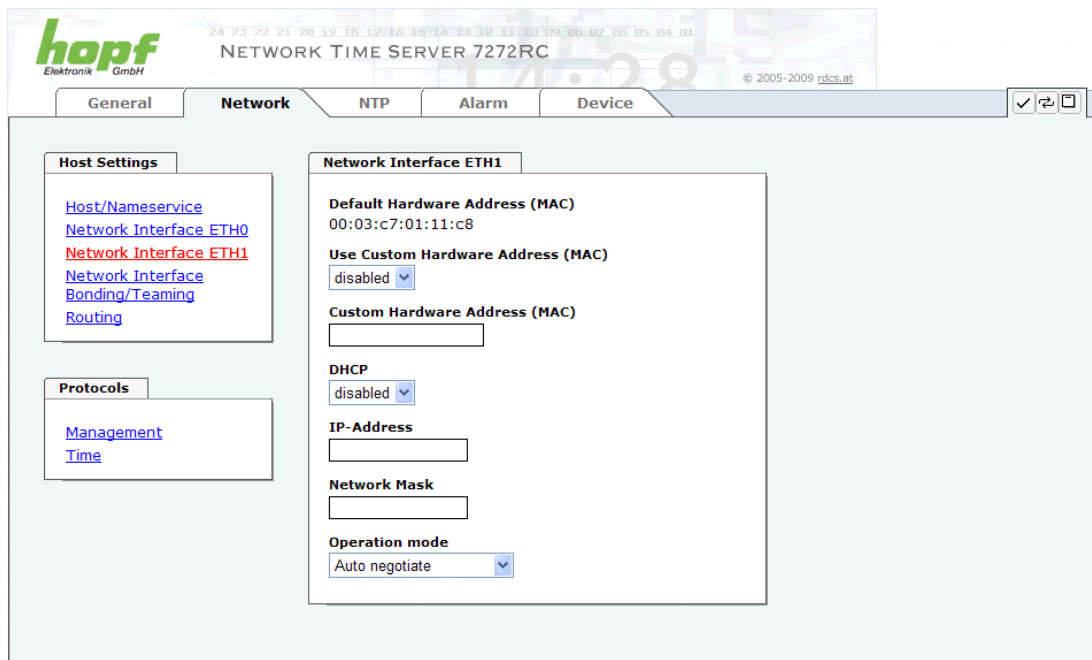
Configuration of the Ethernet interface ETH0 of the board 7271RC.



The screenshot shows the 'Network' tab of the WEBGUI. The 'Host Settings' sidebar contains links for Host/Nameservice, Network Interface ETH0 (highlighted in red), Network Interface ETH1, Bonding/Teaming, and Routing. The 'Protocols' sidebar contains links for Management and Time. The main configuration area is titled 'Network Interface ETH0' and includes the following fields:

- Default Hardware Address (MAC):** 00:03:c7:01:11:c7
- Use Custom Hardware Address (MAC):** disabled (dropdown)
- Custom Hardware Address (MAC):** (empty text field)
- DHCP:** disabled (dropdown)
- IP-Address:** 192.168.100.152
- Network Mask:** 255.255.0.0
- Operation mode:** Auto negotiate (dropdown)

Configuration of the Ethernet interface ETH0 + ETH1 of the board 7272RC



The screenshot shows the 'Network' tab of the WEBGUI. The 'Host Settings' sidebar contains links for Host/Nameservice, Network Interface ETH0, Network Interface ETH1 (highlighted in red), Bonding/Teaming, and Routing. The 'Protocols' sidebar contains links for Management and Time. The main configuration area is titled 'Network Interface ETH1' and includes the following fields:

- Default Hardware Address (MAC):** 00:03:c7:01:11:c8
- Use Custom Hardware Address (MAC):** disabled (dropdown)
- Custom Hardware Address (MAC):** (empty text field)
- DHCP:** disabled (dropdown)
- IP-Address:** (empty text field)
- Network Mask:** (empty text field)
- Operation mode:** Auto negotiate (dropdown)

### 8.3.2.2.1 Default Hardware Address (MAC)

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

For further information about the MAC address refer to **chapter 3.2.2 MAC Address for ETH0** for board 7271RC and refer to **chapter 4.2.2 MAC Address for ETH0 / ETH1** for board 7272RC.



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

### 8.3.2.2.2 Customer Hardware Address (MAC)

The MAC address assigned from **hopf** can be changed to a user-defined MAC address.



Please avoid a double of customer MAC address in the Ethernet.  
If the MAC address is not known please contact your network administrator.

To use the 'customers MAC address function' you have to activate it by setting the function '**Use Custom Hardware Address (MAC)**' to **enable**.

You have to enter the customers MAC address in hexadecimal form with a colon to separate (e.g. **00:03:c7:55:55:02**).



The MAC address assigned by **hopf** can be activated consistently.



There are no MAC multicast addresses allowed!

### 8.3.2.2.3 DHCP

If DHCP is to be used, 0.0.0.0 should be entered as the IP address via the **hopf** Base System menu (likewise for gateway and network mask). This change can also be made via the web interface by enabling the DHCP.



Changes to the IP address or the enabling of DHCP take immediate effect when the settings are accepted. The connection to the web interface must be adapted and regenerated.

#### 8.3.2.2.4 IP Address

The IP address is generally configured via the **hopf** Base System menu. However it can also be changed via the web interface.

Contact your network administrator for details of the IP address if not known.

#### 8.3.2.2.5 Network Mask

The network mask is generally configured via the **hopf** Base System menu. However it can also be changed via the web interface.

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

#### 8.3.2.2.6 Operation Mode

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

7271RC

**Operation mode**

Auto negotiate

Auto negotiate

10 Mbps / half duplex

100 Mbps / half duplex

10 Mbps / full duplex

100 Mbps / full duplex

7272RC

**Operation mode**

Auto negotiate

Auto negotiate

10 Mbps / half duplex

100 Mbps / half duplex

10 Mbps / full duplex

100 Mbps / full duplex

1000 Mbps / full duplex

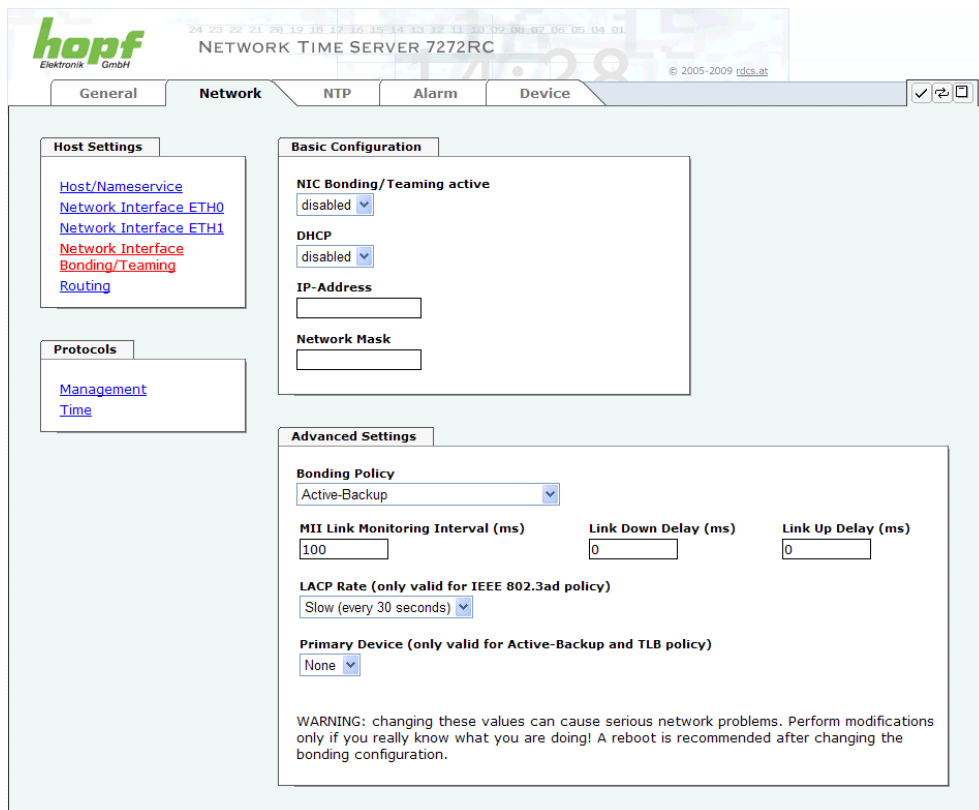
### 8.3.2.3 Option: Network Interface Bonding / Teaming

#### 8.3.2.3.1 Basic Configuration

Network Interface Bonding (also called Teaming) describes the use of multiple network cables/ports in parallel to increase the link speed beyond the limits of a single port to increase the redundancy and/or the availability.

This functionality is optionally available with SET0504 or above.

It can be used only with boards having more than one physical network interface (e.g. Board 7272RC) and has to be activated with a special activation key (how to activate see **Chapter 8.3.5.8 Product Activation**). If this feature isn't activated it isn't shown in the menu 'Network / Host Settings' at all.




Changing these settings without knowledge in Bonding/Teaming functionality may result in serious network troubles. Some of the operation modes are working only if they are supported by the attached network equipment. Misconfiguration can result in a lock out with no further access to the card 7272RC via Ethernet.

In this case you will have to reset the card settings to factory defaults!

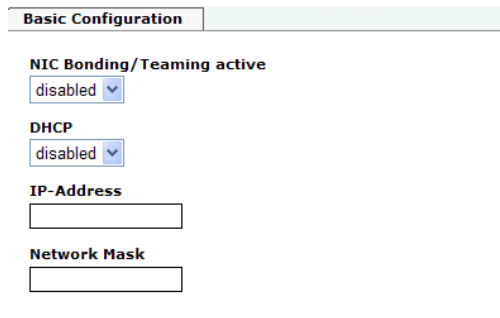


If NIC Bonding is enabled the Network Interface parameters for ETH0 and ETH1 are not applicable anymore and therefore cannot be changed. They are not shown in the Host Settings sub menu at all until NIC Bonding is disabled again.

In most setups the default settings for Bonding can be applied (Active-Backup policy, 100 ms MII Link Monitoring Interval). If the default configuration isn't suitable for your environment, these settings can be changed in the *Advanced Settings* area.

### 8.3.2.3.2 Basic Configuration

Basic network configuration function with activated bonding / teaming function.



#### NIC Bonding/Teaming active

Activating the NIC Bonding/Teaming function

#### DHCP

Activation of DHCP of the "Bonding Interface".



A change of the IP address or the activation of the DHCP have an immediate impact after takeover of settings. The connection to the Web interface needs to be modified and reconnected.

#### IP Address

Entering the IP address of the "Bonding Interface". The network administrator needs to be contacted if the IP address is not known.



A change of the IP address or the activation of the DHCP have an immediate impact after takeover of settings. The connection to the Web interface needs to be modified and reconnected.

#### Network Mask

Eingabe der Netzmaske der "Bonding-Schnittstelle".



A change of the IP address or the activation of the DHCP have an immediate impact after takeover of settings. The connection to the Web interface needs to be modified and reconnected.

### 8.3.2.3.3 Advanced Configuration Parameters

Advanced Settings

Bonding Policy

Active-Backup

MII Link Monitoring Interval (ms)

100

Link Down Delay (ms)

0

Link Up Delay (ms)

0

LACP Rate (only valid for IEEE 802.3ad policy)

Slow (every 30 seconds)

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

None

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

#### Bonding Policy

- Round-robin policy:**  
 Transmit in a sequential order from the first available slave through the last. This mode provides load balancing and fault tolerance.
- Active-backup policy (default):**  
 Only one slave in the bond is active. A different slave becomes active only if the active slave fails. The bond's MAC address is externally visible on only one port (network adapter) to avoid confusing the switch. This mode provides fault tolerance.
- Balance XOR policy:**  
 Transmit based on: [(source MAC address XOR'd with destination MAC address) modulo slave count]. This selects the same slave for each destination MAC address. This mode provides load balancing and fault tolerance.
- Broadcast policy:**  
 Transmits everything on all slave interfaces. This mode provides fault tolerance.
- IEEE 802.3ad Dynamic link aggregation:**  
 Creates aggregation groups that share the same speed and duplex settings. Transmits and receives on all slaves in the active aggregator.
- Adaptive transmit load balancing (TLB):**  
 Channel bonding that does not require any special switch support. The outgoing traffic is distributed according to the current load (computed relative to the speed) on each slave. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed receiving slave.

**MII Link Monitoring Interval (ms)**

Specifies the interval in milliseconds that MII link monitoring will occur. A value of zero disables MII link monitoring. Default value: 100 ms

**Link Down Delay (ms)**

Specifies the delay time in milliseconds to disable a link after a link failure has been detected. This must be a multiple of the MII Link Monitoring Interval value.

**Link Up Delay (ms)**

Specifies the delay time in milliseconds to enable a link after a link up status has been detected. This must be a multiple of the MII Link Monitoring Interval value.

**LACP Rate (only valid for IEEE 802.3ad policy)**

Specifies the rate in which the board will ask it's link partner to transmit LACPDU packets in 802.3ad mode.

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

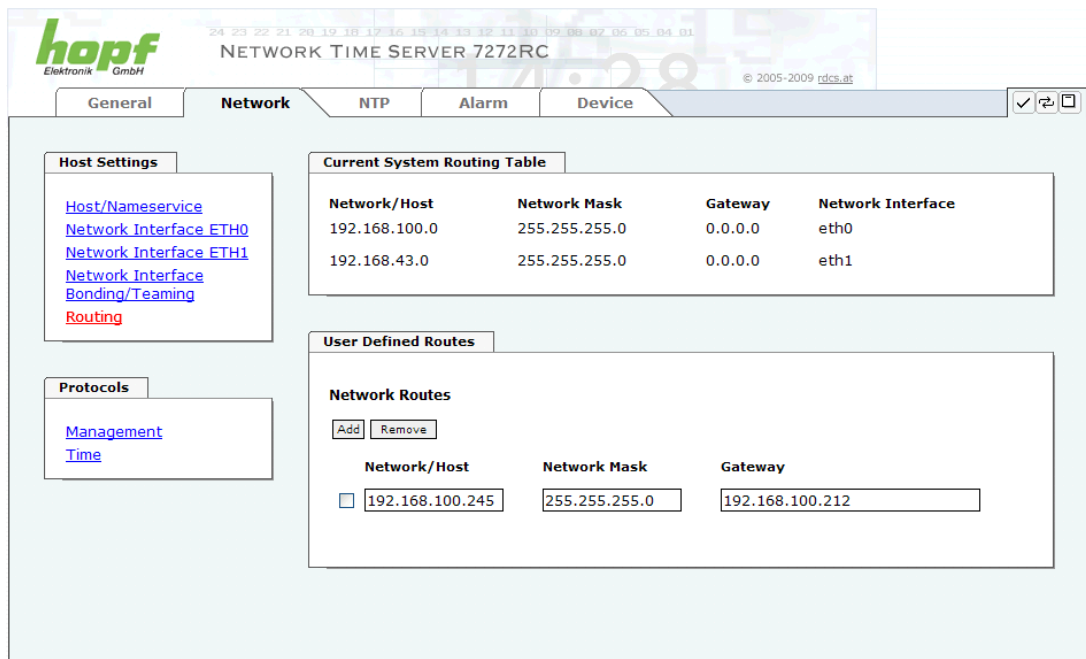
If this value is configured and the device is online, it will be used first as the output media. Only when this device is offline, alternate devices will be used.

Otherwise, once a failover is detected and a new default output is chosen, it will remain the output media until it fails too.



### 8.3.2.4 Routing

A route must be configured if the Board is to be used in more than the local sub-network.



The screenshot shows the 'Network' tab of the hopf WEBGUI. It includes a sidebar with links for Host Settings, Protocols, and a main content area with sections for Host Settings, Current System Routing Table, and User Defined Routes.

**Host Settings**

- [Host/Nameservice](#)
- [Network Interface ETH0](#)
- [Network Interface ETH1](#)
- [Network Interface](#)
- [Bonding/Teaming](#)
- [Routing](#)

**Current System Routing Table**

Network/Host	Network Mask	Gateway	Network Interface
192.168.100.0	255.255.255.0	0.0.0.0	eth0
192.168.43.0	255.255.255.0	0.0.0.0	eth1

**User Defined Routes**

**Network Routes**

Network/Host	Network Mask	Gateway
<input type="checkbox"/> 192.168.100.245	255.255.255.0	192.168.100.212

Routes cannot be used where the gateway / gateway host is not in the local sub-network range of the Board.



This feature is an extended option and can cause problems in the network if it is not configured correctly!

The image above shows every configured route of the Base System Routing Table as well as the User Defined Routes.

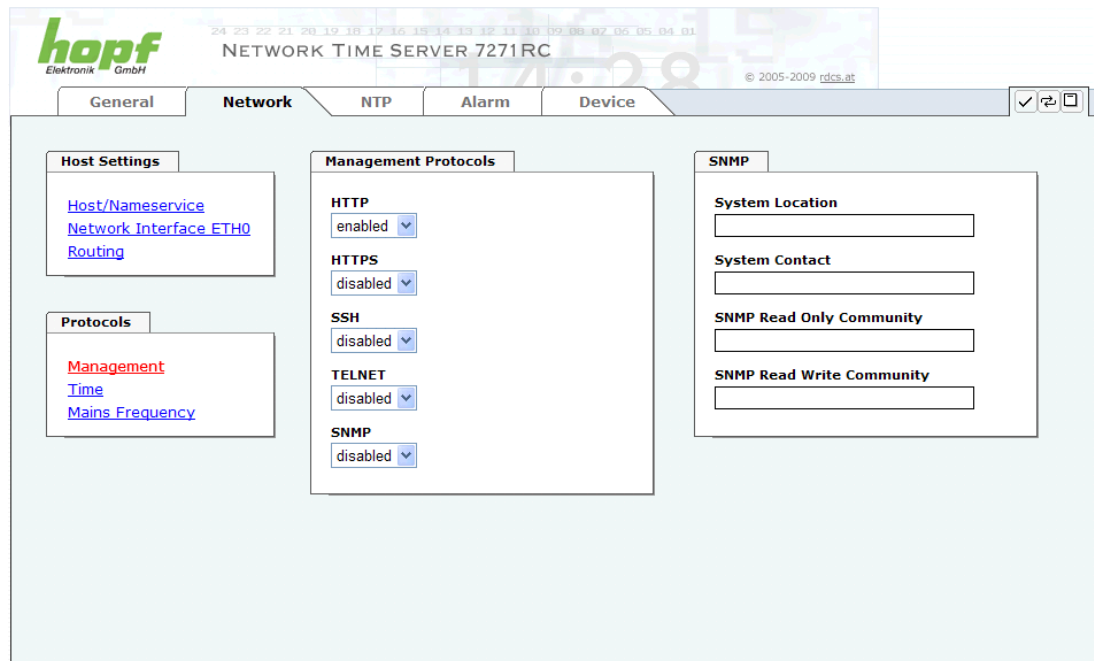


The Board cannot be used as a router!

### 8.3.2.5 Management-Protocols / SNMP

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

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



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

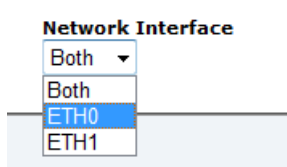
The SNMP protocol should be enabled when using SNMP Traps.



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

#### 7272RC

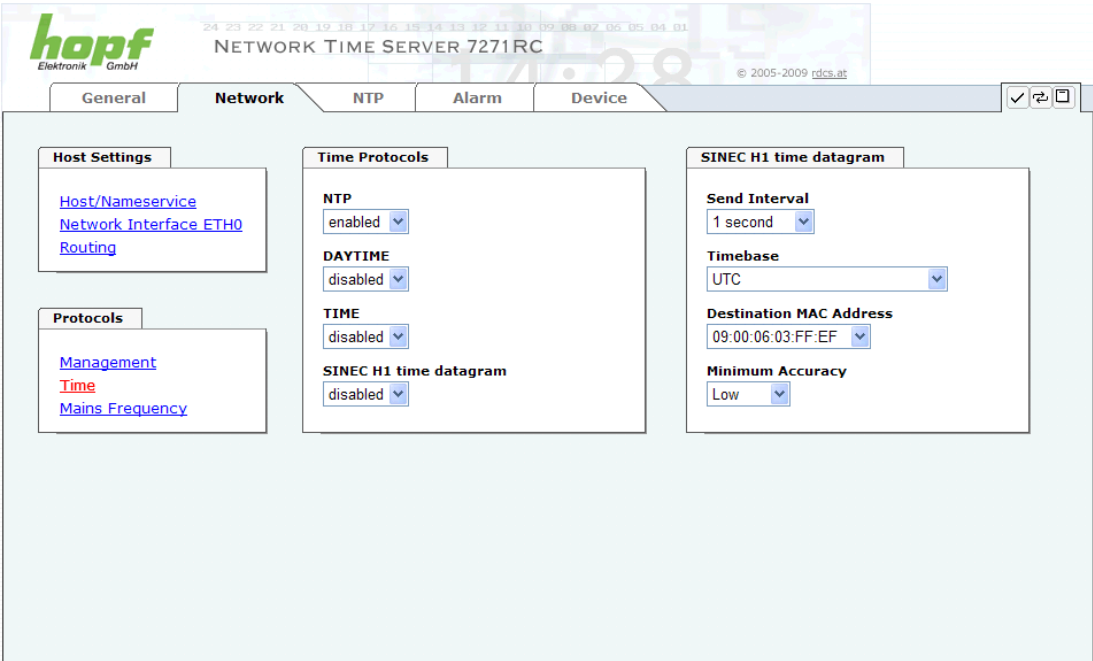
For both interfaces ETH0/ETH1 the management protocols can be activated respectively deactivated separately.



Network Interface	Meaning
Both	Output at interface ETH0 and ETH1
ETH0	Output at interface ETH0 only
ETH1	Output at interface ETH1 only

8.3.2.6 Time

Activation and configuration of different time protocols



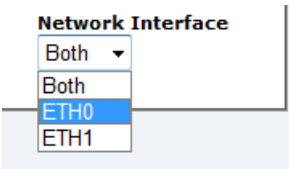
8.3.2.6.1 Time Protocols

Needed time protocols can be activated here.

- NTP
- DAYTIME
- TIME
- SINEC H1 time datagram

7272RC

For both interfaces ETH0/ETH1 the synchronization protocols can be activated respectively deactivated separately.



Network Interface	Meaning
Both	Output at interface ETH0 and ETH1
ETH0	Output at interface ETH0 only
ETH1	Output at interface ETH1 only

#### 8.3.2.6.2 SINEC H1 time datagram

### Configuration of SINEC H1 time datagram.

### Configuration of the broadcast transmission intervals SINEC H1 time datagram (Send Interval):

- every second
- 10 second
- 60 second

**Timebase:**

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

**Destination MAC Address:**

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

**Minimum Accuracy for starting transmission:**

This setting defines the internal minimum accuracy for starting transmission of the SINEC H1 time datagram (see **Chapter 12.6 Accuracy & NTP Basic Principles**):

- low
- medium
- high

#### 8.3.2.6.3 Transmission point of SINEC H1 time datagram

DIP Switch **DS1 switch SW6** sets the transmission point of the SINEC H1 time datagram.

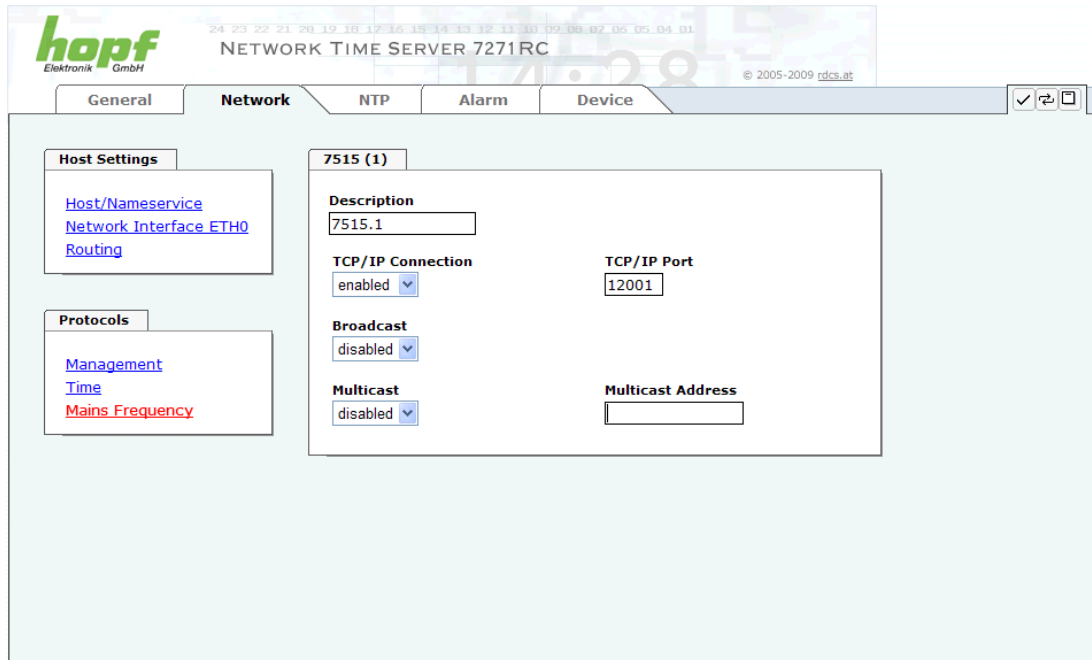
DS1 SW6	Transmission point of the SINEC H1 time datagram	
off	based on the time information of its transmission point. (Default)	
	e.g.: transmission point (UTC, absolute): 12:33:00,001	with time information: 12:33:00,000
on	<b>ONE second delayed.</b> e.g.: transmission point (UTC, absolute): 12:33:01,002	
		with time information: 12:33:00,000

### 8.3.2.7 Option: Mains Frequency / Nettime Distribution

This option allows the distribution of Nettime and Frequency over Ethernet from a board 7515RC in a 7001RC system.

The large scale display 4985-NTP may use this information from the Ethernet for display of network information.

It can be used only if activated with a special activation key (how to activate see **Chapter 8.3.5.8 Product Activation**). If this feature isn't activated it isn't shown in the 'Protocols' sub menu at all.



After activation of this feature you will find an additional link in the 'Protocols' sub menu called 'Mains Frequency'.

As you can see in the screenshot you can configure the method for distribution for every board applied into the system 7001RC. The board number of board 7515RC is shown in brackets in the Tab heading, e.g. 7515 (1).

### **Description**

An additional description can be entered for every board 7515RC for easier identification at the consumers.

Several distribution types can be configured in any combination:

### **Broadcast**

For connectionless distribution you can choose and enable the broadcast mode (UDP) at port 5010.

### **TCP/IP Connection**

For distribution via an explicit connection you can choose and enable the TCP/IP Connection. The port number must be between 1025 and 65535 except port 5010 which is used by the broadcast mode.

### **Multicast**

Multicast is not often used and should be used carefully entering a valid multicast address. Wrong settings for multicast may flood your network and may cause network troubles.

After configuration it is recommended to save the settings of board 7271RC/7272RC using the "Save to flash" button and reboot the board. After reboot the new configuration will be ready for use.

Consumer configuration has to be done in the "client" device (e.g. 4985-NTP Large Scale Display).

### 8.3.3 NTP Tab

This tab shows the options for all of the NTP services, which can also be configured here. This is the Board's main service.

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

NTP functionality is provided by an NTP-Demon (product version ntp-4.2.0), which runs on the embedded Linux of the Board. The Linux system is equipped with a NANO kernel extension (PPS kit 2.1.2) in order to achieve the highest possible accuracy as well as nanosecond resolution in the kernel.

Depending on the **hopf** Base System it may take several hours until long-term accuracy is obtained. During this time the NTP algorithm adjusts the internal accuracy parameters.



NTP time protocol must be enabled in order to use NTP  
(see **Chapter 8.3.2.5 Management-Protocols / SNMP**)



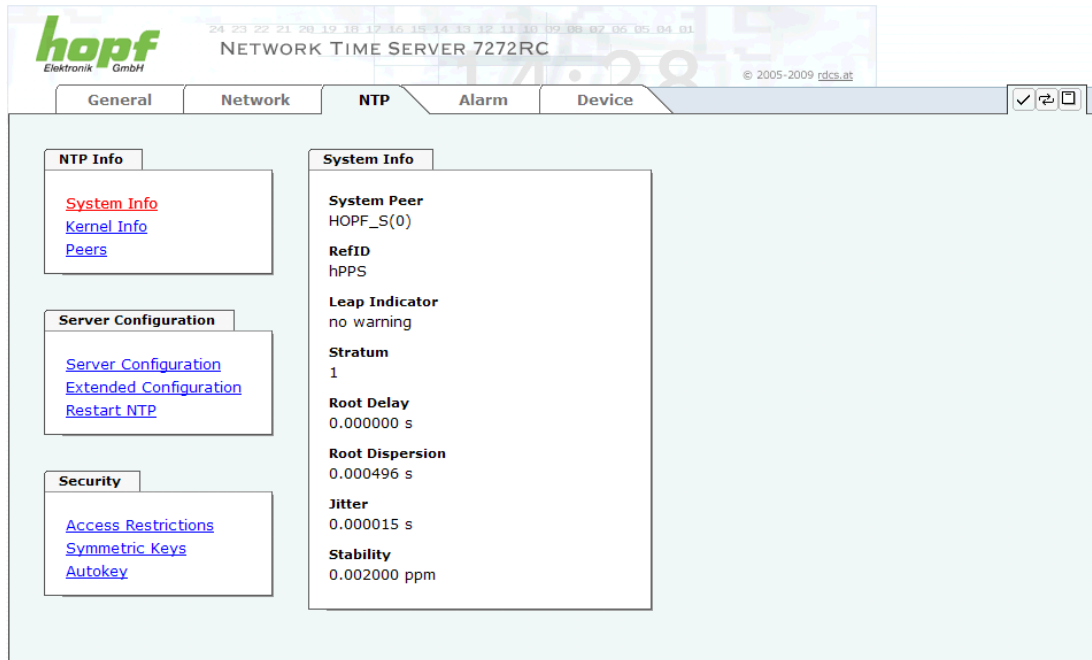
After all changes (according to NTP) have been done a restart of the NTP service on the board is necessary (see **Chapter 8.3.3.6 Restart NTP**).

### 8.3.3.1 System Info

The Base System “System Info” summary, which is shown in the image below, displays the momentary NTP data of the embedded Linux and provides additional information about stratum, leap second, current Base System peer, jitter and the stability of the time information.

The NTP version used correctly adjusts the leap second.

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



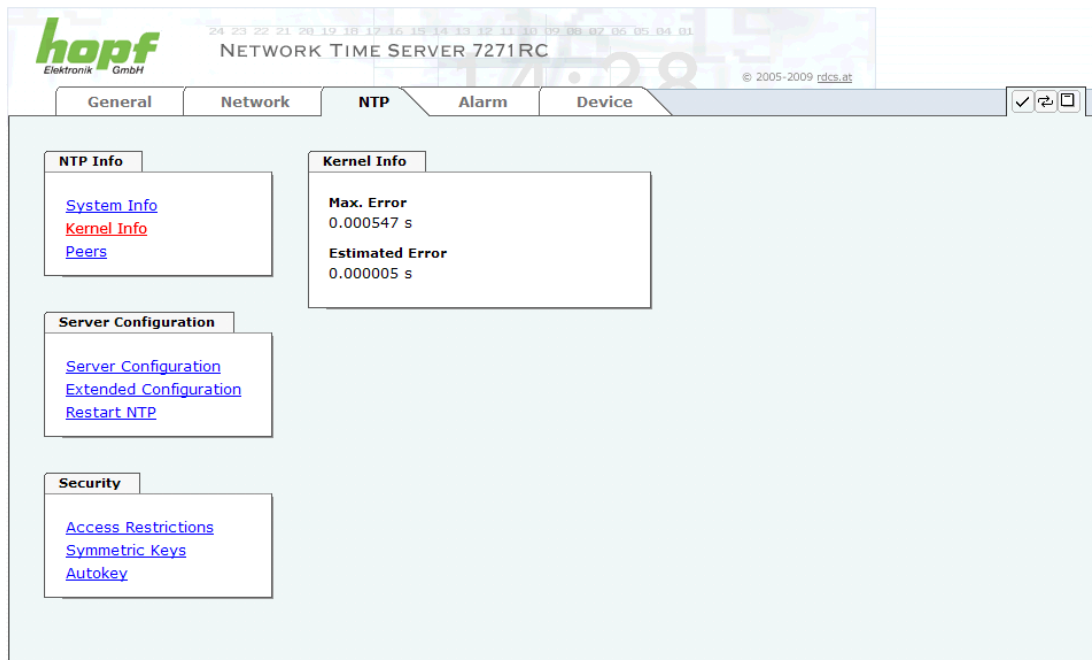
The screenshot shows the web interface for the Hopf Network Time Server 7272RC. The top navigation bar includes tabs for General, Network, NTP (selected), Alarm, and Device. The main content area is divided into two columns. The left column contains links for NTP Info (System Info, Kernel Info, Peers), Server Configuration (Server Configuration, Extended Configuration, Restart NTP), and Security (Access Restrictions, Symmetric Keys, Autokey). The right column displays the System Info summary with the following data:

System Info	
<b>System Peer</b>	HOPF_S(0)
<b>RefID</b>	hPPS
<b>Leap Indicator</b>	no warning
<b>Stratum</b>	1
<b>Root Delay</b>	0.000000 s
<b>Root Dispersion</b>	0.000496 s
<b>Jitter</b>	0.000015 s
<b>Stability</b>	0.002000 ppm



### 8.3.3.2 Kernel Info

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



This screenshot shows a maximum kernel clock error of 0.582 msec (milliseconds). The estimated error value is 5µs (microseconds).

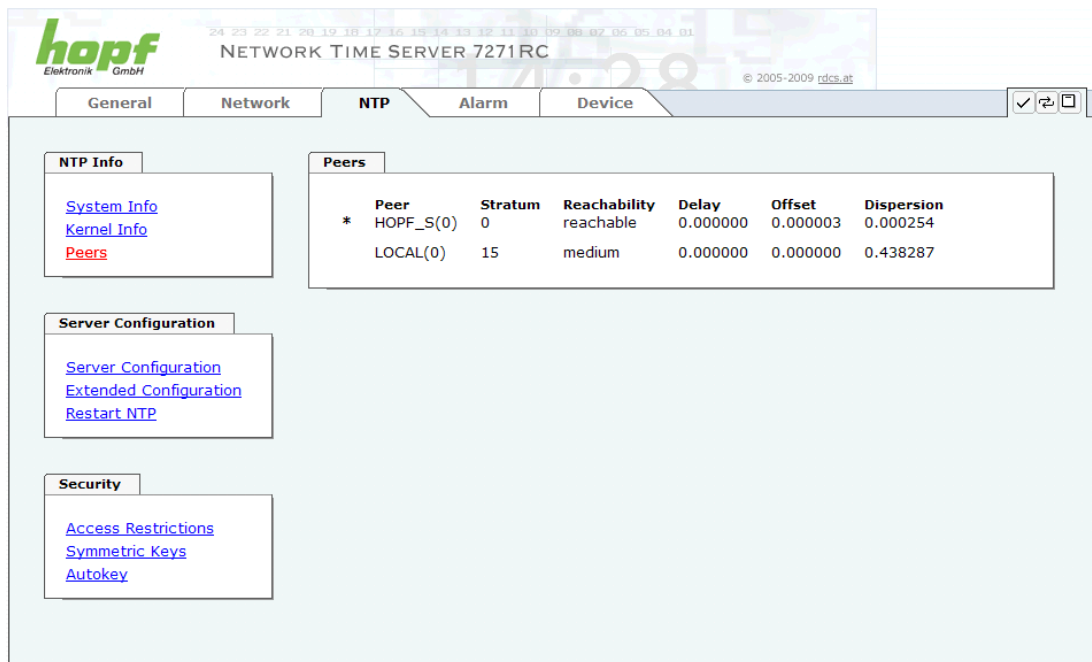
### 8.3.3.3 Peers

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

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

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, reachable).



Peer	Stratum	Reachability	Delay	Offset	Dispersion
* HOPF_S(0)	0	reachable	0.000000	0.000003	0.000254
LOCAL(0)	15	medium	0.000000	0.000000	0.438287

Three lines can be seen in the above image. The first line is **always displayed**, as this concerns the **hopf refclock ntp driver** with pps interface (127.127.38.0), which gets its time information directly from the **hopf** Base System.

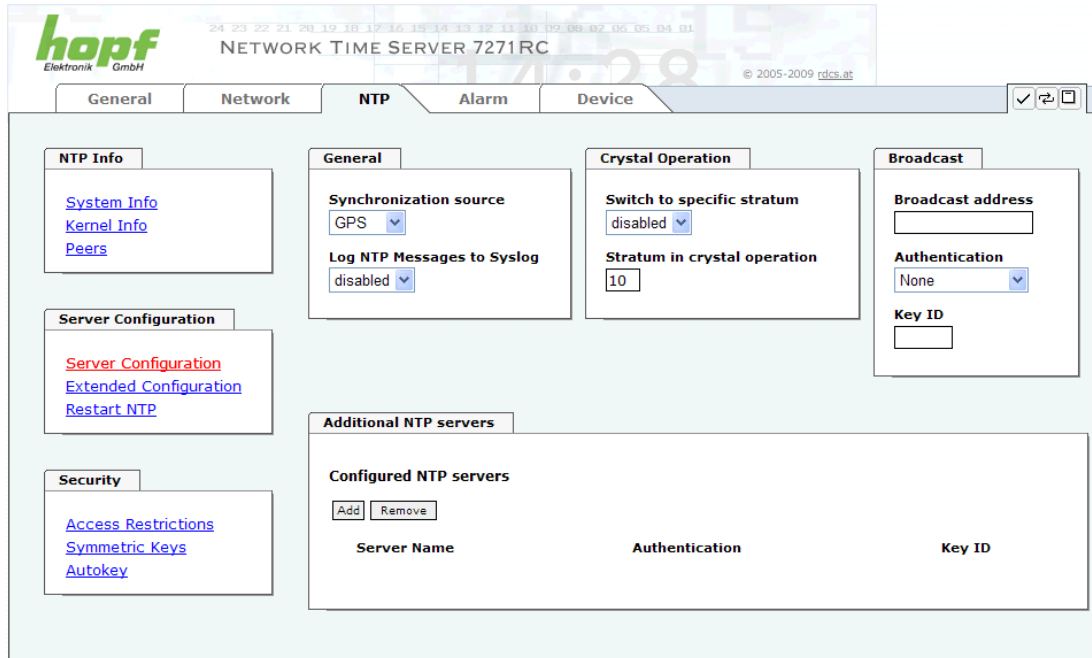
Further external NTP servers are configured in the second and third lines.

A short explanation and definition of the displayed values can be found in **Chapter 12 Glossary and Abbreviations**.

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

### 8.3.3.4 Server Configuration

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



The screenshot shows the web interface for the hopf NETWORK TIME SERVER 7271RC. The top navigation bar includes tabs for General, Network, NTP (selected), Alarm, and Device. The main content area is divided into several sections:

- NTP Info:** Contains links for System Info, Kernel Info, and Peers.
- Server Configuration:** Contains links for Server Configuration (highlighted in red), Extended Configuration, and Restart NTP.
- Security:** Contains links for Access Restrictions, Symmetric Keys, and Autokey.
- General:**
  - Synchronization source:** A dropdown menu set to GPS.
  - Log NTP Messages to Syslog:** A dropdown menu set to disabled.
- Crystal Operation:**
  - Switch to specific stratum:** A dropdown menu set to disabled.
  - Stratum in crystal operation:** A text input field containing the value 10.
- Broadcast:**
  - Broadcast address:** A text input field.
  - Authentication:** A dropdown menu set to None.
  - Key ID:** A text input field.
- Additional NTP servers:**
  - Configured NTP servers:** A table with columns for Server Name, Authentication, and Key ID. It includes 'Add' and 'Remove' buttons.

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

#### 8.3.3.4.1 General / Synchronization Source

The two possible options, GPS and DCF77, must be configured in order to align the accuracy and the algorithm, dependent on the selected synchronisation source of the **hopf** Base System.

If the GPS setting is selected though it is no GPS-based Base System it is possible that HIGH accuracy status may never be achieved.

#### 8.3.3.4.2 General / Log NTP Messages to Syslog

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

This value has no effect if this option is disabled or Syslog is not configured in the ALARM tab (see Chapter 8.3.4.1 Syslog Configuration).

#### 8.3.3.4.3 Crystal Operation

##### Crystal Operation / Switch to specific stratum

If the **hopf** Base System is running in quartz mode, NTP on Board 7271RC/7272RC generally performs in such a way that it stops time transfer from the **hopf** Base System, changes its own stratum level to 16 (illegal level) and neither transmits time signals nor responds to network requests, which leads to the loss of service for connected clients.

This NTP performance can be changed in **hopf** Base Systems with stabilised quartz (OCXO) or rubidium oscillator, which guarantee a stable and precise time over a specified period of time while loss of synchronisation. The "*Switch to specific stratum*" function must be enabled here by setting the value to "*enabled*". This sets the so-called downgrading stratum.

This function is often used when **hopf** Base Systems are tested in an environment without synchronisation sources. In this case it should be noted that from the viewpoint of NTP the synchronisation status of the **hopf** Base System (quartz) is ignored and thus permanent operation in quartz mode is not detected under certain circumstances (only via the high stratum value selected).

##### Crystal Operation / Stratum in crystal operation

The value defined here (range 1-15) designates the transmitted fallback NTP stratum level of the Board in "*Quartz*" synchronisation status and should be in the range 5-15. This value is generally set to 10 or higher and therefore a lower Stratum. Stratum 1 should be configured if downgrading is not desired.



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

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

#### 8.3.3.4.4 Broadcast / Broadcast Address

This section is used to configure the Board as a broadcast or multicast server.

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

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

The 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) on the LAN Board. Care should be taken to ensure that the correct broadcast address is used for the sub-network, usually xxx.xxx.xxx.255 (e.g. 192.168.1.255). If the broadcast address is not known, this can be requested from the network administrator.

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

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

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

#### **8.3.3.4.5 Broadcast / Authentication / Key ID**

Broadcast packets can be protected by authentication for security reasons.

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


#### **8.3.3.4.6 Additional NTP SERVERS**

The addition of further NTP servers provides the opportunity to implement a security system for the time service. However, this has an effect on the accuracy and stability of the Board.

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

### 8.3.3.5 Extended NTP Configuration

NTP is a protocol (**RFC 1305**) for synchronising clocks of computer systems over packet-switched data networks. For special applications the NTP time base of board 7271RC can be configured to local and standard time via the base system.



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

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

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

#### 8.3.3.5.2 NTP Timebase

This function enables adjustment of the time base of the NTP output.



Entering this function the transmitted time protocol of the board 7271RC is not conform to RFC 1305 anymore. According to RFC 1305 NTP uses only the UTC time base. The NTP time protocol does not allow any leaps in time.



#### **This function is only allowed for the Output of NTP**

The output of all further time protocols of board 7271RC (*SINEC H1 TIME DATAGRAM / TIME / DAYTIME*) are guaranteed with the entered function, however with a wrong time base and are therefore not available to the user.

#### UTC - NTP with Time Basis UTC

According to RFC 1305 NTP uses only the UTC time base.

#### NTP with the Time Base Standard Time

Using the NTP time protocol with the standard time base the released time information correspond with UTC plus the time difference, adjusted in the base system.

#### NTP with the Time Base Local Time

Using the NTP time protocol with the local time base the released time information correspond with UTC plus the time difference including possible summer time, adjusted in the base system.

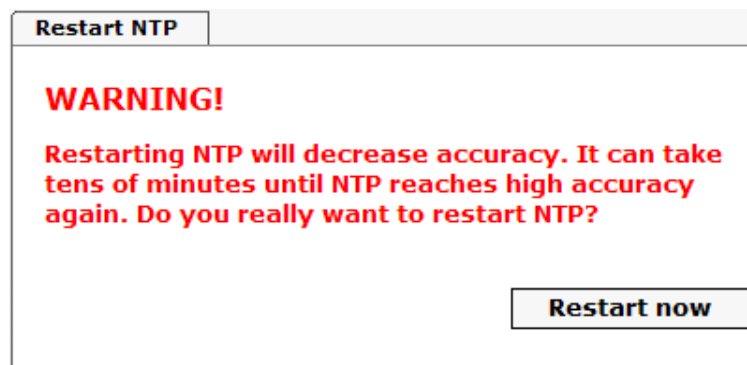
NTP does not allow any leaps in time. Using the NTP time protocol with the local time base the internal NTP process of a board is restarted based on a summer-/winter time adjustment.



Using the NTP time protocol with the local time base the summer-/winter time adjustment is released one to two minutes belated. Afterwards the local time is correctly available in the NTP time protocol. Therefore, within this transition period a requested NTP time protocol is replied by the former time base.

### 8.3.3.6 Restart NTP

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

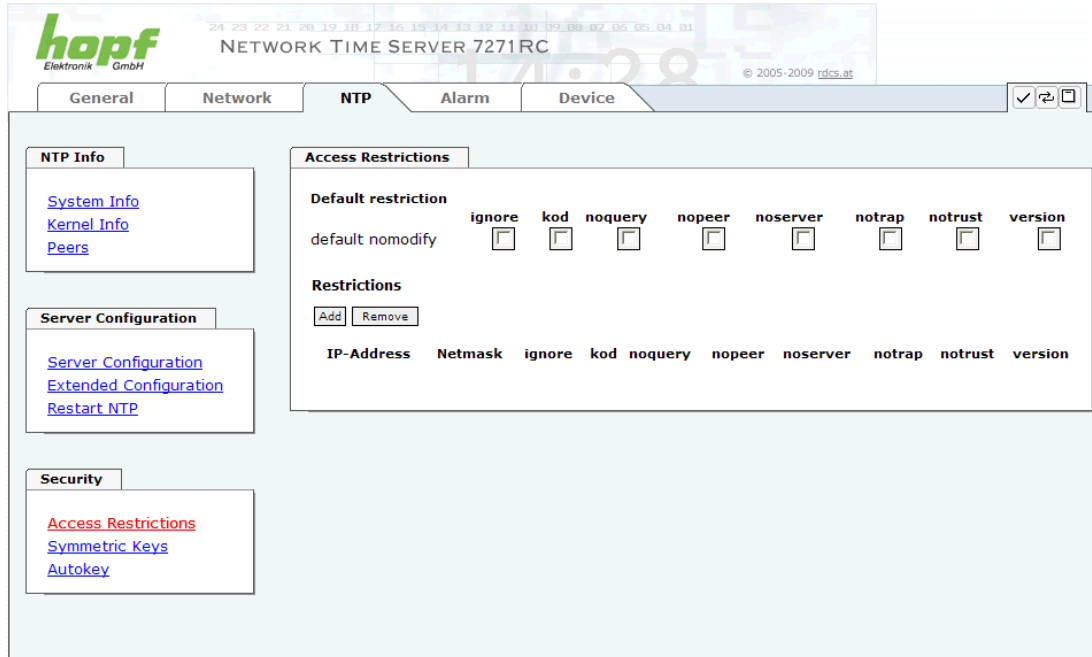


Restarting NTP Services is the only possibility of making NTP changes effective without having to restart the entire Board 7271RC/7272RC. As can be seen from the warning message, the currently reachable stability and accuracy are lost due to this restart.

After a restart of the NTP service it takes a few minutes until the NTP service on the board 7271RC/7272RC is completely adjusted and synchronised with the system time of the base system again.

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

One of the extended configuration options for NTP is “NTP Access Restrictions”.



The screenshot shows the NTP configuration web interface for a NETWORK TIME SERVER 7271RC. The interface has a top navigation bar with tabs: General, Network, NTP (selected), Alarm, and Device. Below the tabs, there are three main sections on the left: NTP Info (with links for System Info, Kernel Info, and Peers), Server Configuration (with links for Server Configuration, Extended Configuration, and Restart NTP), and Security (with links for Access Restrictions, Symmetric Keys, and Autokey). The main content area is titled 'Access Restrictions' and contains two sections: 'Default restriction' and 'Restrictions'. The 'Default restriction' section has a row of checkboxes for: ignore, kod, noquery, nopeer, noserver, notrap, notrust, and version. Below this is a 'Restrictions' section with 'Add' and 'Remove' buttons, followed by a table with columns: IP-Address, Netmask, ignore, kod, noquery, nopeer, noserver, notrap, notrust, and version.

Restrictions are used in order to control access to the Board'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 from hosts (including remote time servers) and sub-networks which otherwise have no special restrictions.

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

Before beginning the configuration you should ask yourself the following questions:



### 8.3.3.7.1 NAT or Firewall

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

### 8.3.3.7.2 Blocking Unauthorised Access

Is it really necessary to block all connections from unauthorised hosts if the NTP Service is openly accessible?	
No	Proceed to <b>Chapter 8.3.3.7.3 Allow Client Requests</b>
Yes	<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 8.3.3.7.5 Addition of Exceptions to Standard</b></p>

### 8.3.3.7.3 Allow 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 LAN Board, operating system and NTPD version)?									
No	<p>In this case select from the following standard restrictions: <b>See Chapter 8.3.3.7.6 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: <b>See Chapter 8.3.3.7.6 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 8.3.3.7.5 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"/>								

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

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

### 8.3.3.7.5 Addition of Exceptions to Standard Restrictions

After the standard restrictions have been set, 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										
<b>Default restriction</b>										
	ignore	kod	noquery	nopeer	noserver	notrap	notrust	version		
default nomodify	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
<b>Restrictions</b>										
<input type="button" value="Add"/> <input type="button" value="Remove"/>										
	IP-Address	Netmask	ignore	kod	noquery	nopeer	noserver	notrap	notrust	version
<input type="checkbox"/>	192.168.017.123		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	192.168.001.101		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	192.168.001.000	255.255.255.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



Unrestricted access of Board 7271RC/7272RC 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

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

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

IP address 192.168.1.0

Network mask 255.255.255.0

**notrap / nopeer** ☒

### 8.3.3.7.6 Access Control Options

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

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

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



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

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

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

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

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

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

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

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

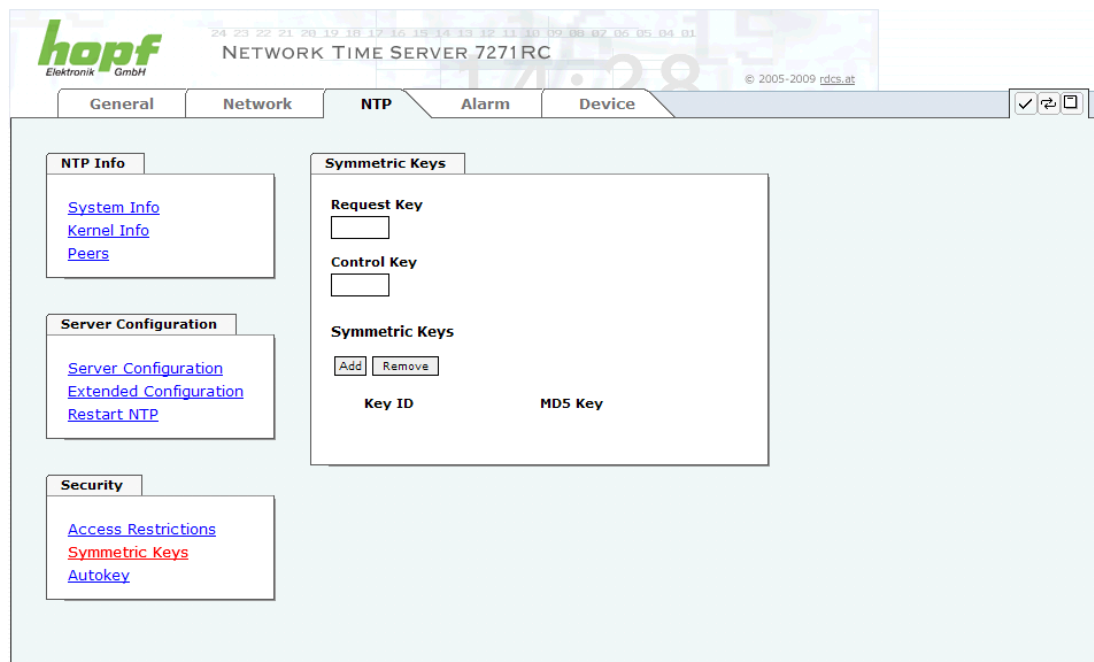
The trap service is a sub-system of the ntpq control message protocols. This service logs remote events in programmes.

**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 8.3.3.6 Restart NTP**).

### 8.3.3.8 Symmetric Key and Autokey



The screenshot shows the web interface for the hopf NETWORK TIME SERVER 7271RC. The top navigation bar includes tabs for General, Network, NTP (selected), Alarm, and Device. The main content area is divided into three sections:

- NTP Info:** Contains links for System Info, Kernel Info, and Peers.
- Server Configuration:** Contains links for Server Configuration, Extended Configuration, and Restart NTP.
- Security:** Contains links for Access Restrictions, Symmetric Keys (highlighted in red), and Autokey.

The **Symmetric Keys** section is expanded, showing fields for Request Key and Control Key, each with an input box. Below these are buttons for Add and Remove. A table with two columns, Key ID and MD5 Key, is also visible.

#### 8.3.3.8.1 Why Authentication?

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

Despite this, however, the use of authentication is common.

There are certain reasons for this:

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

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

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

NTP uses keys to implement the authentication. These keys are used when data is 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” on the DEVICE tab. It is necessary to be logged in as “Master” in order to access this.

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

#### 8.3.3.8.3 How is a key created?

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

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

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

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

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

#### 8.3.3.8.4 How does authentication work?

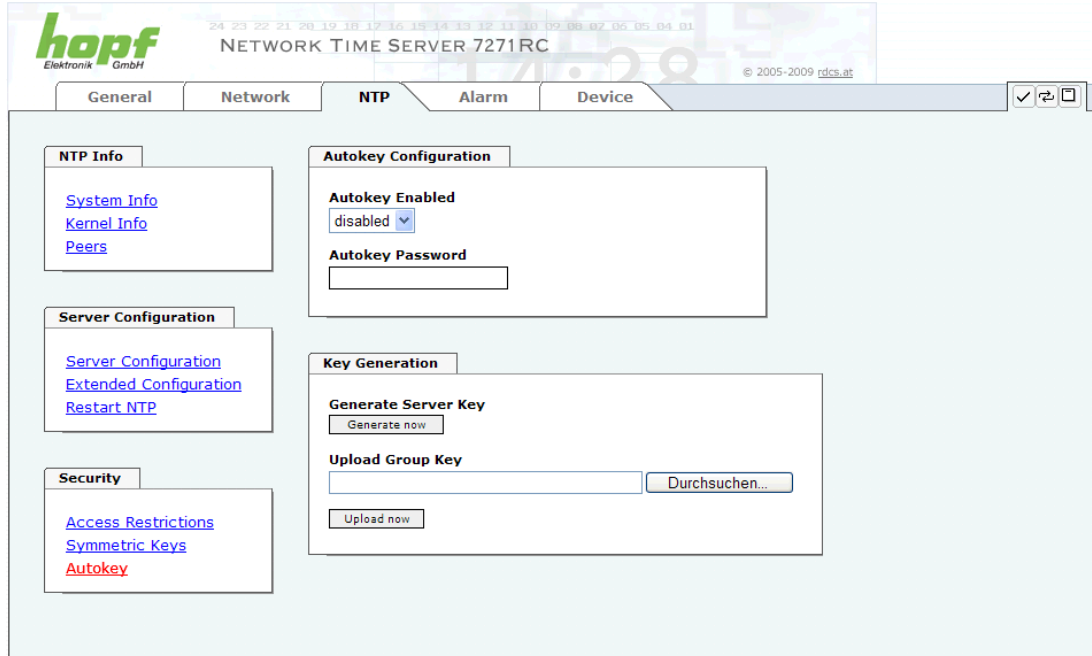
Basic authentication is a digital signature and not data encryption (if there is any difference between the two). The data packet and the key are used to create a non-reversible number which is attached to the packet.

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

### 8.3.3.9 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 web interface for the hopf NETWORK TIME SERVER 7271RC. The top navigation bar includes tabs for General, Network, NTP (selected), Alarm, and Device. The main content area is divided into several sections:

- NTP Info:** Contains links for System Info, Kernel Info, and Peers.
- Server Configuration:** Contains links for Server Configuration, Extended Configuration, and Restart NTP.
- Security:** Contains links for Access Restrictions, Symmetric Keys, and Autokey (highlighted in red).
- Autokey Configuration:** Contains a dropdown menu for "Autokey Enabled" (currently set to "disabled") and a text input field for "Autokey Password".
- Key Generation:** Contains a "Generate Server Key" section with a "Generate now" button, and an "Upload Group Key" section with a text input field, 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 NTS board is to form part of an NTP trust group, a group key can be defined and uploaded with the "Upload now" button.

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



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

### 8.3.4 ALARM Tab

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

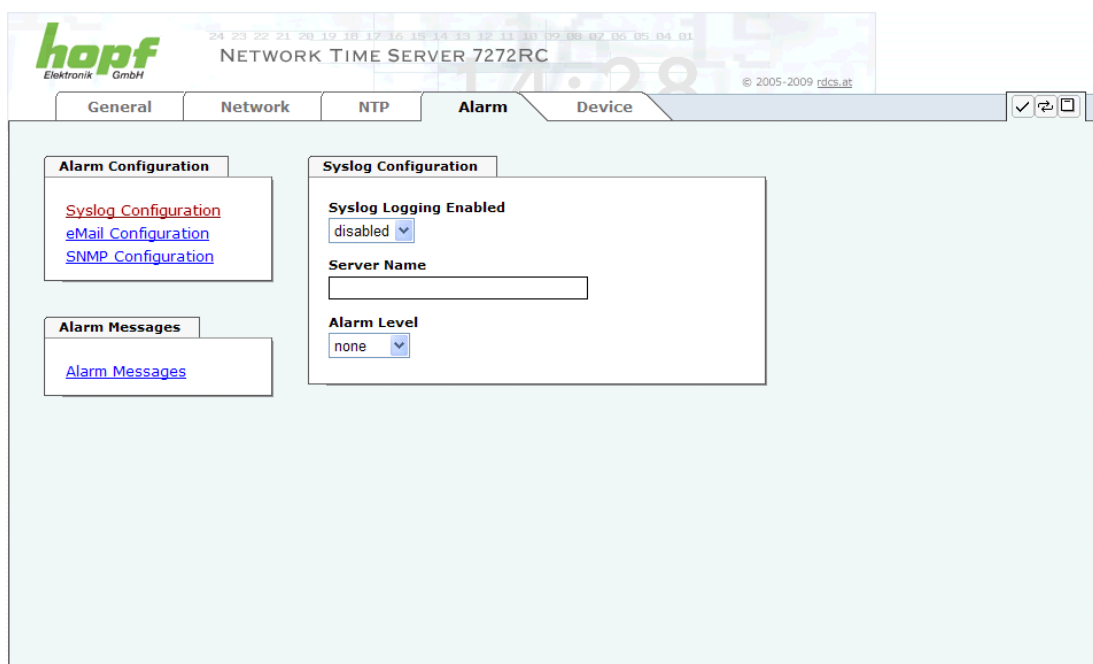
#### 8.3.4.1 Syslog Configuration

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

**Syslog uses Port 514.**

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

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



The screenshot shows the Hopf WebGUI interface for the Alarm tab. At the top, there's a header with the Hopf logo, a network time server status bar, and navigation tabs: General, Network, NTP, Alarm (selected), and Device. Below the tabs, there are two main configuration sections. On the left, under 'Alarm Configuration', there are links for 'Syslog Configuration', 'eMail Configuration', and 'SNMP Configuration'. Below that, under 'Alarm Messages', there is a link for 'Alarm Messages'. On the right, under 'Syslog Configuration', there are two settings: 'Syslog Logging Enabled' set to 'disabled' and 'Server Name' with an empty text input field. Below these, 'Alarm Level' is set to 'none'.

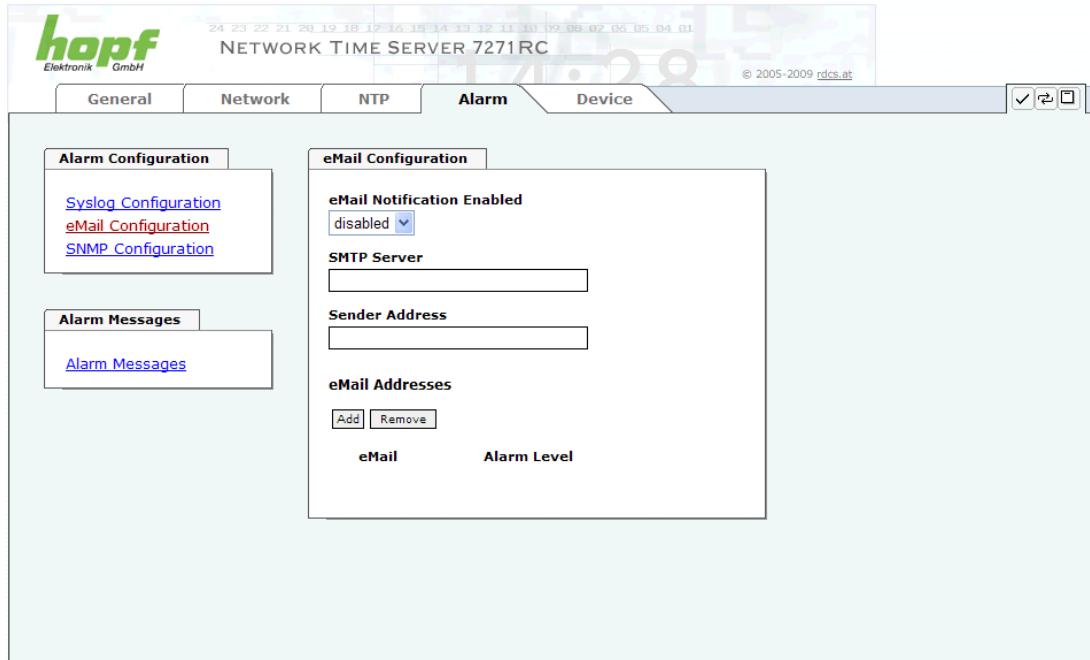
The alarm level designates the priority level of the messages to be transmitted and the level from which transmission is to take place (see **Chapter 8.3.4.4 Alarm**).

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

The NTP service implemented on this Board can transmit its own Syslog messages (see **Chapter 8.3.3.4.2 General / Log NTP Messages to Syslog**).

Generated Syslog messages of board 7271/7272 are described in **Chapter 12.5 Syslog Messages**.

### 8.3.4.2 E-mail Configuration



The screenshot shows the web interface for the hopf NETWORK TIME SERVER 7271RC. The 'Alarm' tab is selected, and within it, the 'eMail Configuration' sub-tab is active. The interface includes a navigation bar with tabs for General, Network, NTP, Alarm, and Device. On the left, there are links for Syslog Configuration, eMail Configuration, and SNMP Configuration. The main configuration area for eMail includes a dropdown for 'eMail Notification Enabled' (currently set to 'disabled'), input fields for 'SMTP Server' and 'Sender Address', and a section for 'eMail Addresses' with 'Add' and 'Remove' buttons. Below this is a table with columns for 'eMail' and 'Alarm Level'.

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.

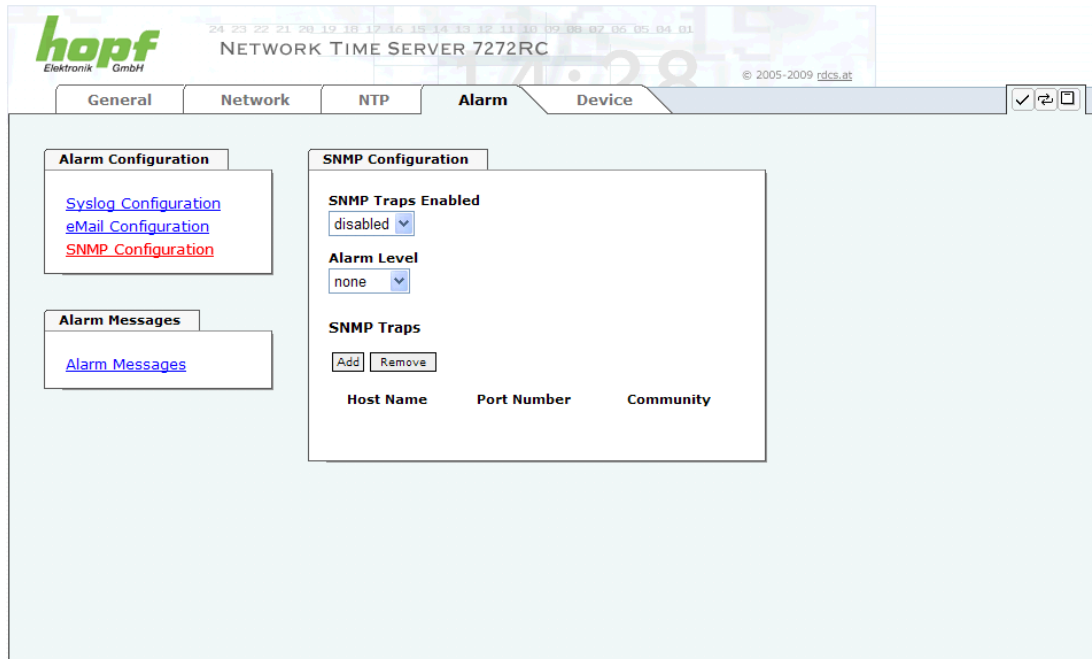
The Alarm Level designates the priority level of the messages to be sent and the level from which they are to be sent (see **Chapter 8.3.4.4 Alarm Messages**).

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



### 8.3.4.3 SNMP Configuration / TRAP Configuration

It is possible to use an SNMP agent (with MIB) or to configure SNMP traps in order to monitor the 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 8.3.5.10 Downloading Configurations / SNMP MIB**).

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 8.3.4.4 Alarm**).

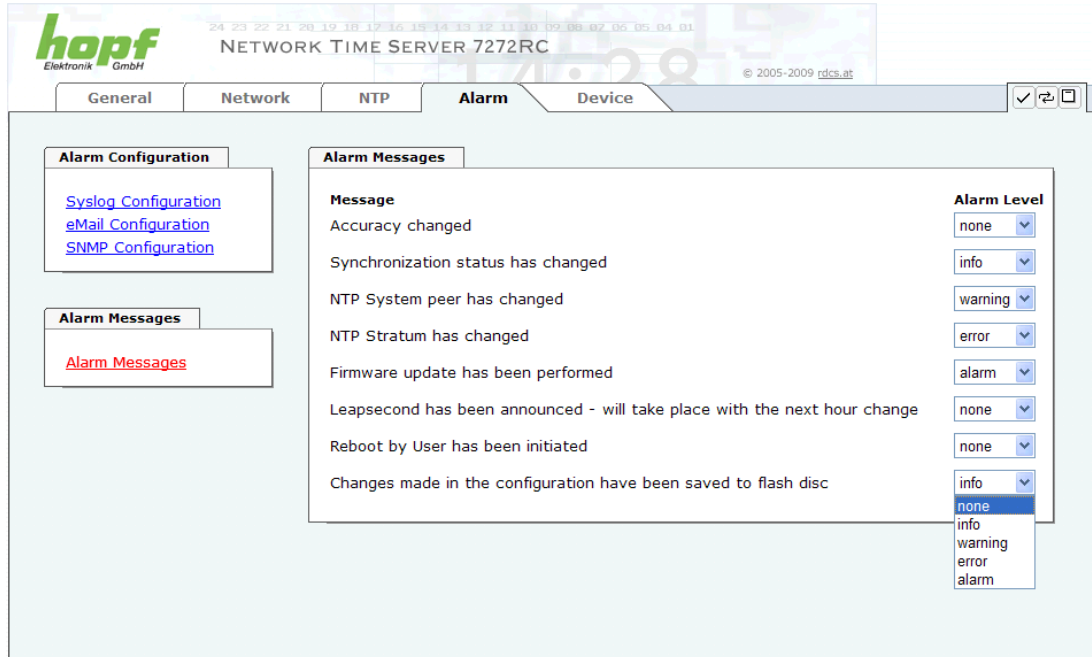
Alarm Level	Transmitted Messages
none	no messages
info	info / warning / error / alarm
warning	warning / error / alarm
error	error / alarm
alarm	alarm



SNMP protocol must be enabled in order to use SNMP (see **Chapter 8.3.2.5 Management-Protocols / SNMP**).

### 8.3.4.4 Alarm Messages

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



The screenshot shows the 'Alarm Messages' configuration page for the 'hopf NETWORK TIME SERVER 7272RC'. The interface includes a top navigation bar with tabs for General, Network, NTP, Alarm, and Device. The 'Alarm' tab is active. On the left, there are links for 'Syslog Configuration', 'eMail Configuration', and 'SNMP Configuration'. The main area is divided into two sections: 'Alarm Configuration' and 'Alarm Messages'. The 'Alarm Messages' section contains a table with the following messages and their corresponding alarm levels:

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

A dropdown menu is open for the 'Changes made in the configuration have been saved to flash disc' message, showing the following options: none, info, warning, error, alarm.

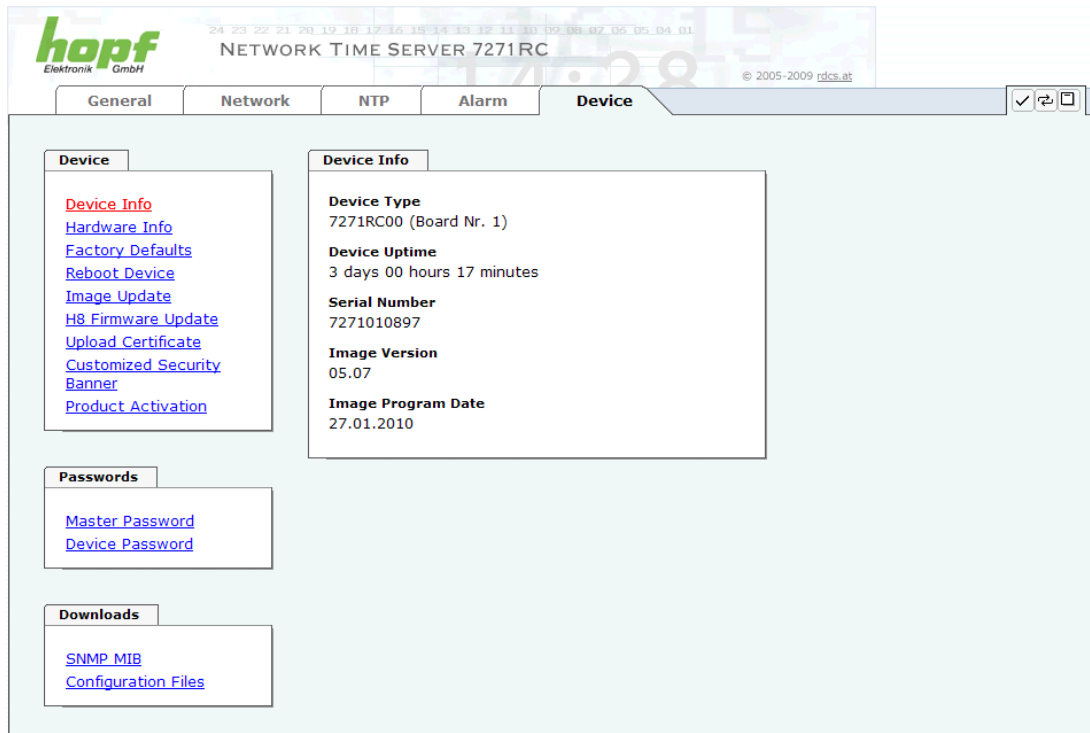
A corresponding action is carried out if an event occurs, depending on the messages, their configured levels and the configured notification levels of the E-mails.



Always remember to save any changed value to the flash disc in order to store this permanently, otherwise this will be lost in the event of a restart!

### 8.3.5 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 Board hardware and software/firmware. Password administration and the update services for the Board are also made accessible via this website. The complete download zone is also a component of this site.

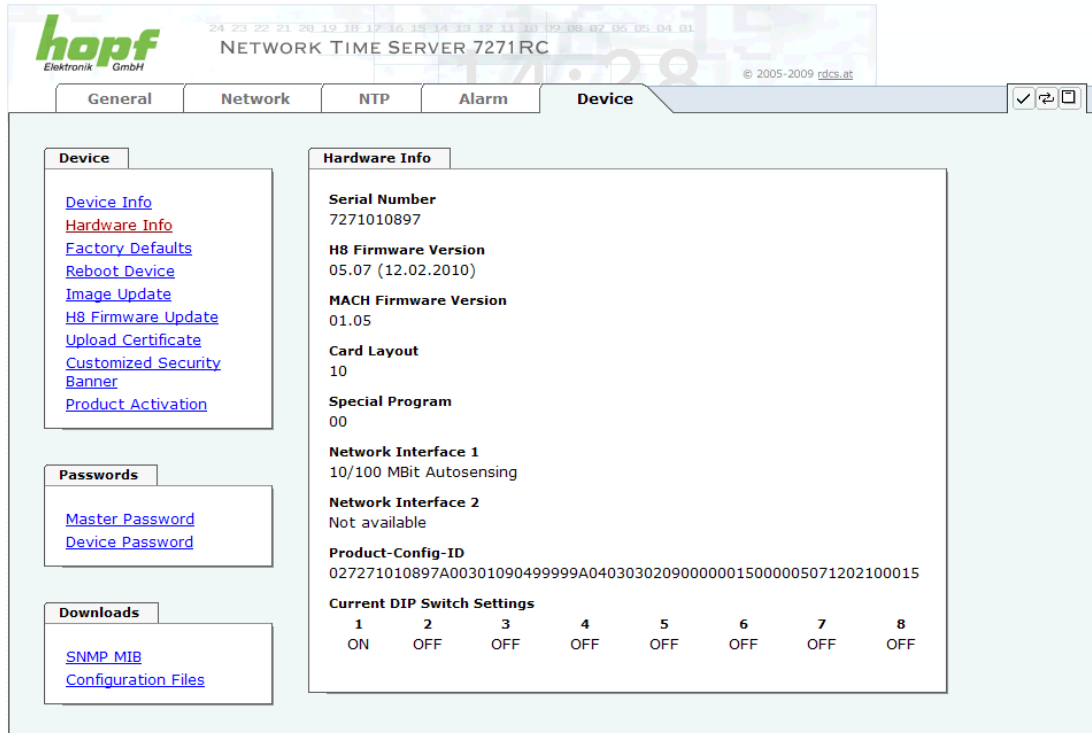
#### 8.3.5.1 Device Information

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

### 8.3.5.2 Hardware Information

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

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



The screenshot shows the Hopf WebGUI interface for a 'NETWORK TIME SERVER 7271RC'. The 'Device' tab is selected, and the 'Hardware Info' section is expanded. The left sidebar contains links for 'Device Info', 'Hardware Info', 'Factory Defaults', 'Reboot Device', 'Image Update', 'H8 Firmware Update', 'Upload Certificate', 'Customized Security Banner', and 'Product Activation'. Below these are sections for 'Passwords' (Master Password, Device Password) and 'Downloads' (SNMP MIB, Configuration Files). The main content area displays the following hardware information:

- Serial Number:** 7271010897
- H8 Firmware Version:** 05.07 (12.02.2010)
- MACH Firmware Version:** 01.05
- Card Layout:** 10
- Special Program:** 00
- Network Interface 1:** 10/100 MBit Autosensing
- Network Interface 2:** Not available
- Product-Config-ID:** 027271010897A00301090499999A040303020900000015000005071202100015
- Current DIP Switch Settings:**

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

The settings of the DIP-switch on the board 7271RC/7272RC will be shown under the point "Current DIP Switch Settings"

### 8.3.5.3 Restoring the Factory Settings - Factory Defaults

In some cases it may be necessary or desirable to restore all of the Board's settings to their delivered condition (factory defaults).

**Factory Defaults**

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

**Reset now**

This function serves to restore all values in the flash memory to their default values. This also includes passwords. (See **Chapter 11 Factory Default**).

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

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

Once this procedure has been triggered there is NO possibility of restoring the deleted configuration.



A complete check (and reconfiguration of the Board where appropriate) is required after every **Factory Default** procedure. In particular, the MASTER and DEVICE passwords must be reset.

### 8.3.5.4 Restarting (Rebooting) the Board

**Reboot Device**

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

**Reboot now**

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

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

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

### 8.3.5.5 Image Update & H8 Firmware Update

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

Both the embedded software and the H8 firmware can only be downloaded to the Board via the web interface (login as "Master" user required).



#### 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 a **hopf** engineer.
- 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.
- A restart is absolutely essential prior to downloading an update (see **Chapter 8.3.5.4 Restarting (Rebooting) the Board**).
- During the update procedure, the device **must not be switched off** and **settings must not be saved to the flash memory!**
- Updates are usually executed as a 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.

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 image designations are (e.g.):

20060222_727x.bin	for the <b>H8 firmware</b> and	(update takes 3-5 minutes)
20050821_upgrade.img	for the <b>embedded image</b>	(update takes 3-5 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.

The screenshot shows a web browser window titled "H8 Firmware Update". Inside, there is a red "WARNING!" heading followed by a red text block: "H8 FIRMWARE UPDATE is a critical action. Please ensure not to switch off power during upload and reboot after upload! In 6xxx and 7001 Systems the rest of the System will go in AUTORESET MODE!". Below this, there is a label "Update file:" followed by a text input field and a "Durchsuchen..." button. At the bottom right, there is a large "Upload now" button.

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

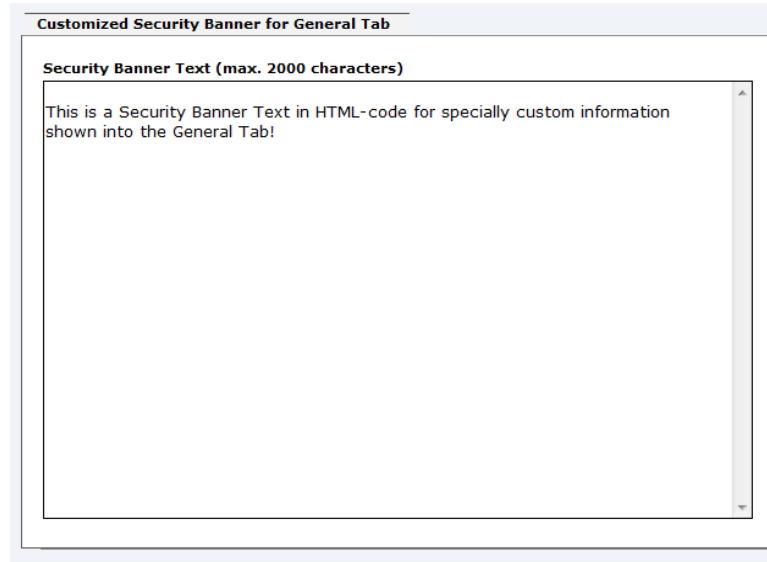
The procedure for the **Image update** differs only in how the Board 7271RC is restarted.

The screenshot shows a web browser window titled "Image Update". Inside, there is a red "WARNING!" heading followed by a red text block: "IMAGE UPDATE is a critical action. Please ensure not to switch off power during update!". Below this, there is a label "Update file:" followed by a text input field and a "Durchsuchen..." button. At the bottom right, there is a large "Update now" button.

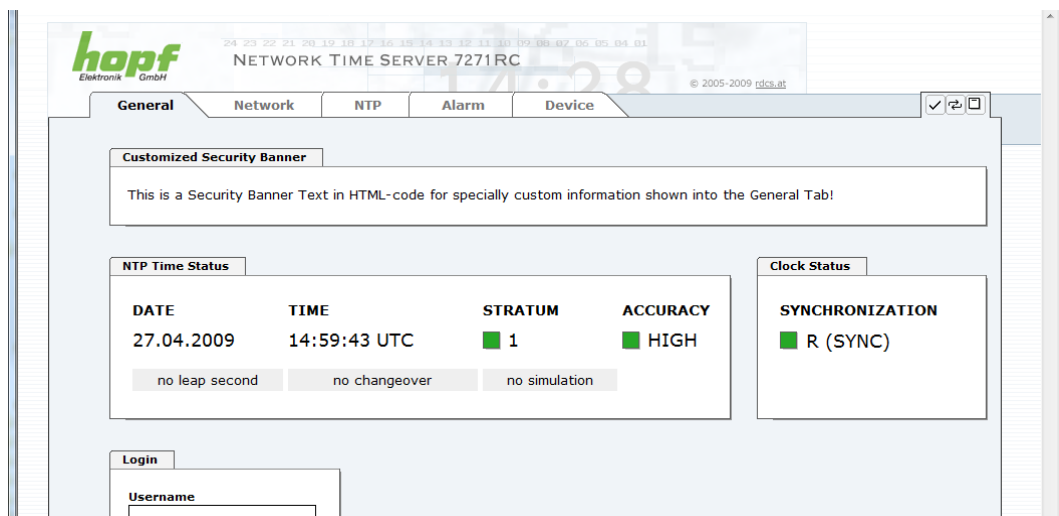
After the image-update the Web-GUI displays a window to confirm the restart (reboot) of the board.

### 8.3.5.6 Customized Security Banner

Special security information which are displayed in the General-Tab can be entered here by the user.



The security information can be written as 'unformatted' text as well as HTML formatted text. 2000 characters are available to write failsafe into the board 7271RC/7272RC.



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

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



### 8.3.5.7 Option FG7271/PPM: Minute Pulse Length (PPM)

With this option FG7271/PPM a high active isolated minute pulse of +12V DC is distributed on the 9-pole SUB-D male connector. Further technical data can be found in **Chapter 10.2.1 Board 7271RC with Option FG7271/PPM (Output Minute Pulse)**.

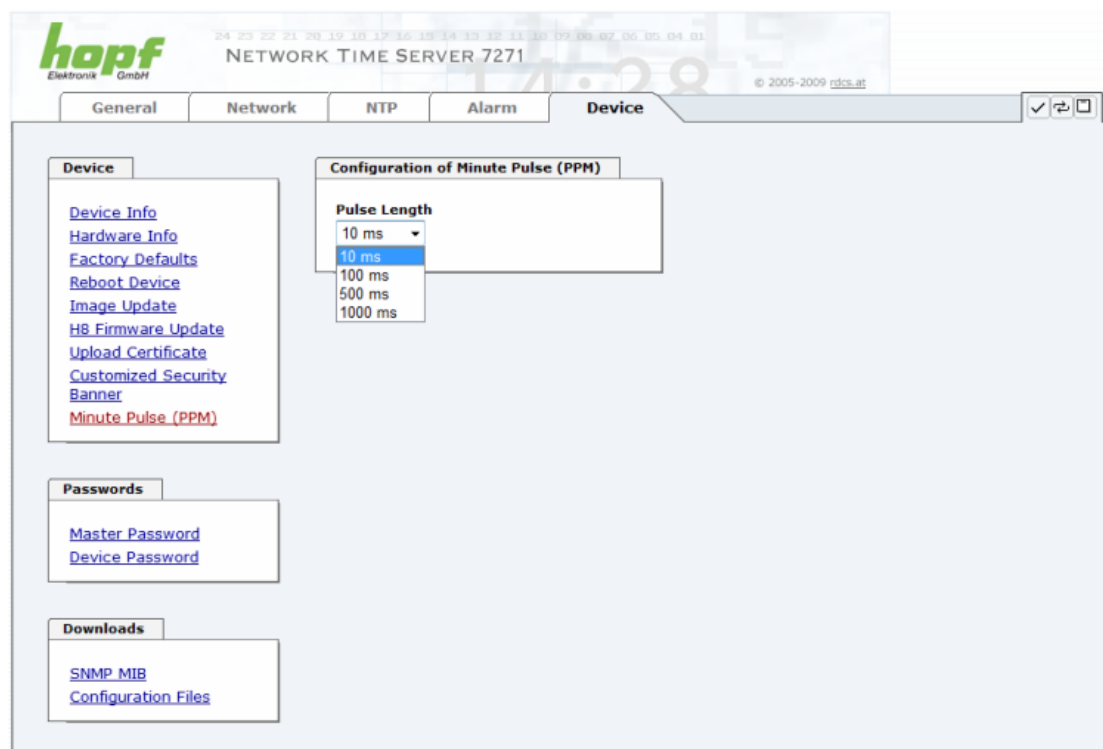
The output is an "open collector" with a current limiter.



This minute pulse is fully compatible to the minute pulse of the hopf board 7270 (the assignment of the 9-pole SUB-D connector as well as the electrical properties and the adjustable parameters).

The length of the pulse can be adjusted in 4 steps.

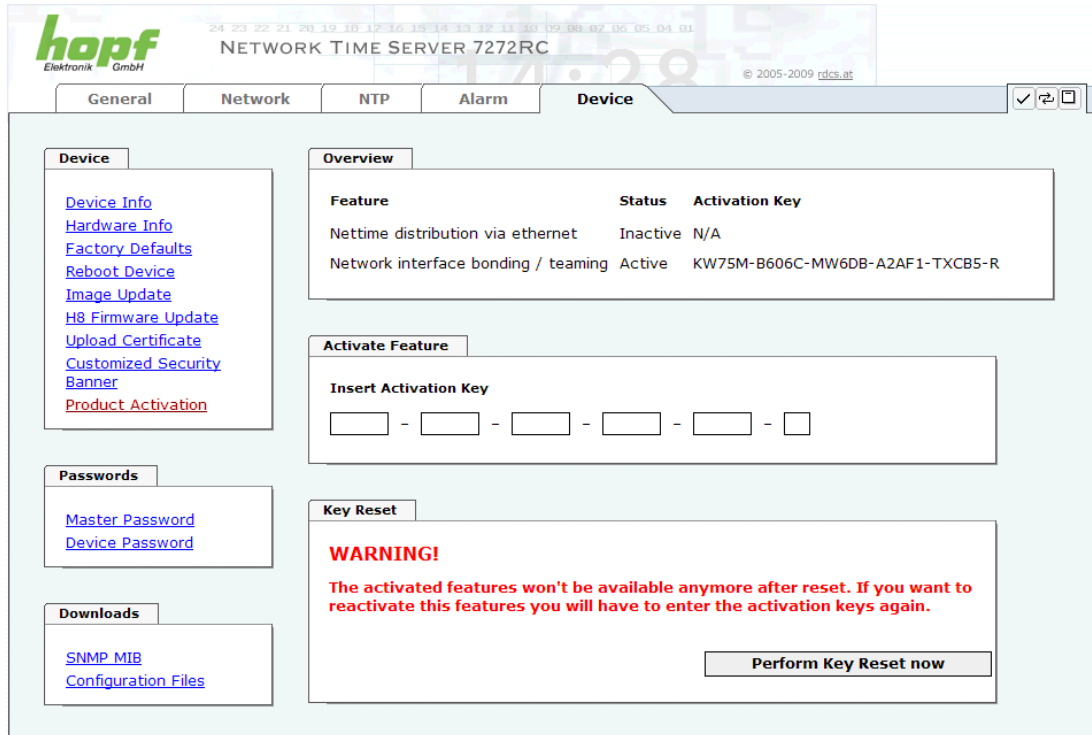
Pulse Length of the Minute Pulse (high active)
10 msec
100 msec
500 msec
1000 msec



### 8.3.5.8 Product Activation

Optional features (e.g. NIC Bonding/Teaming) can be activated using a special activation key which can be requested from **hopf** Elektronik GmbH.

Each activation key is bound to a specific board and cannot be shared between several boards.



**hopf** Elektronik GmbH  
NETWORK TIME SERVER 7272RC  
© 2005-2009 rdc.at

General Network NTP Alarm **Device**

**Device**

- Device Info
- Hardware Info
- Factory Defaults
- Reboot Device
- Image Update
- H8 Firmware Update
- Upload Certificate
- Customized Security Banner
- Product Activation

**Overview**

Feature	Status	Activation Key
Nettime distribution via ethernet	Inactive	N/A
Network interface bonding / teaming	Active	KW75M-B606C-MW6DB-A2AF1-TXCB5-R

**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

List of all options with its current activation status and the stored activation key.

#### Activate Feature

Input fields to enter a new activation key. The activation key has 26 characters and can be entered case insensitive without hyphens (-). After entering a key the feature can be activated by pressing the ☒ Apply button. If 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”. No optional feature is available anymore after performing the Key Reset. If the option is enabled again, the last configuration for the optional feature is restored.

### 8.3.5.9 Passwords (Master/Device)

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




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

(See also **Chapter 8.2.1 LOGIN and LOGOUT as a User**)


Change Master Password
<b>Current password</b> <input type="password"/>
<b>New password (min. 6 characters)</b> <input type="password"/>
<b>Confirm new password</b> <input type="password"/>

### 8.3.5.10 Downloading Configurations / SNMP MIB

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

Configuration Files
<b>Download NTP-Configurationfile</b>  <a href="#">Click here to download</a>
<b>Download NTP-Keyfile</b>  <a href="#">Click here to download</a>
<b>Download System Configuration</b>  <a href="#">Click here to download</a>

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

SNMP MIB
<b>Download hopf727x MIB</b>  <a href="#">Click here to download</a>

## 9 SSH and Telnet Basic Configuration



Only basic configuration is possible via SSH or Telnet. The complete configuration of Board 7271RC/7272RC takes place exclusively via the WebGUI.

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

The user names and passwords are the same as on the web and are kept in alignment. (See **Chapter 8.2.1 LOGIN and LOGOUT as a User and 8.3.5.9 Passwords**)



SSH does not allow blank passwords for safety reasons (however this is the condition as delivered). Therefore, in order to use SSH, a password must have been pre-set via Telnet or the WebGUI.



The corresponding service is to be enabled for the use of Telnet or SSH (see **Chapter 8.3.2.5 Management-Protocols / SNMP**)

```
kaw@paris:~/Entwicklung/workspace/727x/src
[kaw@paris src]$ telnet 192.168.1.211
Trying 192.168.1.211...
Connected to 192.168.1.211.
Escape character is '^]'.
Username: master
Password:
Login successful.

      N   N   TTTTTT  SSSSS
     NN  N   T       S   S
    N N  N   T       S
   N N N   T       SSSSS
  N  NN   T       S   S
 N   N   T       SSSSS

Hopf 727x NTS CARD (c) 2006

Press Enter to continue

Main Menu
1 ... General
2 ... Network
3 ... Alarm
4 ... NTP
5 ... Device Info
0 ... Exit
Choose a Number =>
```

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

## 10 Technical Data

### 10.1 General

General technical Data of the Boards 7271RC and 7272RC

#### 10.1.1 Design

<b>Assembly</b>	
<b>Model</b>	Euro-board 160 x 100 mm
<b>Carrier</b>	19" 3U racks with 3U/4HP front panel
<b>Power supply</b>	
internal system voltage Vcc	5V DC $\pm$ 5% via system bus

#### 10.1.2 Ambient conditions

<b>Temperature range</b>	
Operating	0°C to +40°C
Storage	-20°C to +75°C
Cooling	passive cooling (heat sink) - external active cooling / ventilation is recommended
Humidity	max. 95%, not condensed

#### 10.1.3 CE compliant

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

#### 10.1.4 NTP Accuracy

<b>GPS System - Accuracy</b>	
Internal Kernel Accuracy	Better than 5 $\mu$ sec depending on the long-term accuracy of the synchronisation system
LOW – Lambda	> 15 msec
MEDIUM – Lambda	< 15 msec
HIGH – Lambda	< 15 msec <b>AND</b> stability < 0.05 ppm
<b>DCF77 System - Accuracy</b>	
Internal Kernel Accuracy	Better than 200 $\mu$ sec depending on the long-term accuracy of the synchronisation system
LOW – Lambda	> 15 msec
MEDIUM – Lambda	< 15 msec
HIGH – Lambda	< 15 msec <b>AND</b> stability < 0.3 ppm
<b>Other Signal Sources - Accuracy</b>	
	with quartz synchronisation status configured with additional NTP servers
LOW – Lambda	> 15 msec
MEDIUM – Lambda	< 15 msec
HIGH – Lambda	< 15 msec <b>AND</b> stability < 0.8 ppm

### 10.1.5 Time Protocols

- NTPv4 Server
- NTP Broadcast Mode
- NTP Multicast Mode
- NTP Client for additional NTP Servers (Redundancy)
- SNTP Server
- NTP Symmetric Key Encryption
- NTP Autokey Encryption
- NTP Access Restrictions
- PPS Time Source
- RFC-867 DAYTIME Server
- RFC-868 TIME Server
- SINEC H1 time datagram

### 10.1.6 TCP/IP Network Protocols

- HTTP/ HTTPS
- FTP
- Telnet
- SSH
- SNMP
- NTP
- SINEC H1 time datagram

### 10.1.7 Configuration

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

### 10.1.8 Features

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

## 10.2 Special Technical Data of Board 7271RC

<b>Power consumption</b>	
Normal operation	approx. 700 mA
Boot phase	approx. 1200 mA
<b>LAN</b>	
Network Connection	Takes place via a LAN cable with RJ45 plug (recommended cable type CAT5 or better).
Requests per second	max. 1000 requests
Number of connectable clients	Theoretically unlimited
<b>Network interface ETH0</b>	10/100 Base-T
<b>Ethernet compatibility</b>	Version 2.0 / IEEE 802.3
<b>Isolation voltage</b> (network to system side)	1500 Vrms
<b>MTBF</b>	
MTBF	> 285,000 hours

### 10.2.1 Board 7271RC with Option FG7271/PPM (Output Minute Pulse)

<b>Minute Pulse</b>	<b>12V DC, potential isolated via an 'open collector unit'</b>
Current Source	typical: 20mA (max. 30 mA) The output load should be ( $R_L < 600 \text{ Ohm}$ ), because of a too small edge steepness.
Activity	high active
<b>ext. 12V DC Voltage</b>	12V DC, max. 100mA, potential isolated
Isolation	min. 1000V DC

## 10.3 Special Technical Data of Board 7272RC

<b>Power consumption</b>	
Normal operation	approx. 600 mA (with ETH0+ETH1 10/100MBit) approx. 1200 mA (with ETH0+ETH1 1000MBit)
Boot phase	approx. 1200 mA
<b>LAN</b>	
Network Connection	Takes place via a LAN cable with RJ45 plug (recommended cable type CAT5 or better).
Requests per second	max. 1000 requests
Number of connectable clients	Theoretically unlimited
<b>Network interface ETH0</b>	10/100/1000 Base-T
<b>Ethernet compatibility</b>	Version 2.0 / IEEE 802.3
<b>Isolation voltage</b> (network to system side)	1500 Vrms
<b>MTBF</b>	
MTBF	> 285,000 hours

## 11 Factory Defaults

Board 7271RC/7272RC is generally delivered in accordance with the factory defaults.

At DCF77 systems the "NTP / General / Sync. Source" to "DCF77" function is configured.

NTP Server Configuration	Setting	WebGUI
Sync. Source	DCF77	DCF77

### 11.1 Network

Host/Name Service	Setting	WebGUI Presentation
Hostname	hopf727x	hopf727x
Default Gateway	No change	---
DNS 1	Blank	---
DNS 2	Blank	---
Network Interface ETH0	Setting	WebGUI
Use Custom Hardware Address (MAC)	Disabled	Disabled
Custom Hardware Address (MAC)	Blank	---
DHCP	Enabled	Enabled
IP	No change	No change
Netmask	No change	No change
Operation mode	Auto negotiate	Auto negotiate
Network Interface ETH1 (7272)	Setting	WebGUI
Use Custom Hardware Address (MAC)	Disabled	Disabled
Custom Hardware Address (MAC)	Blank	---
DHCP	Disabled	Disabled
IP	Blank	---
Netmask	Blank	---
Operation mode	Auto negotiate	Auto negotiate
Routing	Setting	WebGUI
User Defined Routes	Blank	---
Management	Setting	WebGUI
HTTP	Enabled	Enabled
HTTPS	Disabled	Disabled
SSH	Disabled	Disabled
TELNET	Disabled	Disabled
SNMP	Disabled	Disabled
System Location	Blank	---
System Contact	Blank	---
Read Community	Blank	---
Read/Write Community	Blank	---
Time	Setting	WebGUI
NTP	Enabled	Enabled
DAYTIME	Disabled	Disabled
TIME	Disabled	Disabled
SINEC H1 time datagram	Setting	WebGUI
Send Interval	every second	1 second
Timebase	UTC	UTC
Destination MAC Address	09:00:06:03:FF:EF	09:00:06:03:FF:EF
Minimum Accuracy	LOW	LOW

DIP-Switch DS1 SW6	Setting	WebGUI Presentation
Transmission point of the SINEC H1 time datagram	off (every second)	off



## 11.2 NTP

NTP Server Configuration	Setting	WebGUI
Sync. source	GPS	GPS
NTP to Syslog	Disabled	Disabled
Switch to specific stratum	Disabled	Disabled
Stratum in crystal operation	10	10
Broadcast address	Blank	---
Authentication	Disabled	None
Key ID	Blank	---
Additional NTP Servers	Blank	---
NTP Access Restrictions	Setting	WebGUI
Access Restrictions		Default nomodify
NTP Symmetric Keys	Setting	WebGUI
Request Key	Blank	---
Control Key	Blank	---
Symmetric Keys	Blank	---
NTP Autokey	Setting	WebGUI
Autokey	Disabled	Disabled
Password	Blank	---

## 11.3 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

## 11.4 DEVICE

User Passwords	Setting	WebGUI
Master Password	Blank	---
Device Password	Blank	---

## 12 Glossary and Abbreviations

### 12.1 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.

### 12.2 Tally Codes (NTP-specific)

<b>space</b>	<b>reject</b>	Rejected peer – either the peer is not reachable or its synchronisation 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 synchronisation 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 synchronisation 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 synchronisation is derived from a PPS (pulse-per-second) signal either indirectly via PPS reference clock driver or directly via kernel interface.

## 12.2.1 Time-specific expressions

<b>UTC</b>	<b>UTC Time (Universal Time Coordinated)</b> was dependent 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>	<p>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.</p> <p>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.</p> <p>The zero meridian runs through the British city of Greenwich.</p>
<b>Time Offset</b>	<p>This is the difference between UTC and the valid standard time of the current time zone.</p> <p>The Time Offset will be commit from the local time zone.</p>
<b>Local Standard Time (winter time)</b>	<p><b>Standard Time = UTC + Time Offset</b></p> <p>The time offset is defined by the local time zone and the local political regulations.</p>
<b>Daylight Saving Time (summer time)</b>	<p><b>Offset of Daylight Saving Time = + 1h</b></p> <p>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.</p>
<b>Local Time</b>	Local Time = Standard Time if exists with summer / winter time changeover
<b>Leap Second</b>	<p>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.</p> <p>Leap seconds are defined internationally by the <b>International Earth Rotation and Reference Systems Service (IERS)</b>.</p>

## 12.3 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 (version 3: RFC 1305)
<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 (version 4: RFC 2030)
<b>S, STD</b>	Standard Time
<b>TCP</b>	Transmission Control Protocol
<b>ToD</b>	Time of Day
<b>UDP</b>	User Datagram Protocol
<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 ( $10^{-6}$ )

## 12.4 Definitions

An explanation of the terms used in this document.

### 12.4.1 DHCP (Dynamic Host Configuration Protocol)

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

The Board is supplied from the factory with DHCP enabled.



See RFC 2131 Dynamic Host Configuration Protocol for further information

### 12.4.2 NTP (Network Time Protocol)

Network Time Protocol (NTP) is a standard for the synchronisation of clocks in computer systems over 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 roundtrip times.

NTP uses the Marzullo algorithm (devised by Keith Marzullo of San Diego University in his dissertation) with a UTC timescale and which 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 in 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 1305 for further information.

### 12.4.3 SNMP (Simple Network Management Protocol)

Simple Network Management Protocol (SNMP) is a network protocol which was developed by the IETF in order to be able to monitor and control network elements from a central station. This protocol regulates the communication between the monitored devices and the monitoring station. SNMP describes the composition of the data packets which can be transmitted and the communication procedure. SNMP was designed in such a way that every network-compatible device can be monitored. The network management tasks which are possible with 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 offer hardly any safety mechanisms. The safety mechanisms have been significantly expanded in the current Version 3.

With the aid of description files known as MIB's (Management Information Base), the management programmes are in a position to represent the hierarchical structure of the data of any desired 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.

### 12.4.4 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 while 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.

## 12.5 Syslog Messages

Description of the Syslog messages of the board 7271RC/7272RC configured by the alarm messages. Further Syslog messages generated by the operating system (e.g. NTP, Syslog-Deamon, ...) are not described here.

Type	Message	Values %1, %2
G	NTP Accuracy change - <b>Accuracy changed to %1 !</b>	LOW, MEDIUM, HIGH
G	Synchronization status change - <b>Syncstatus changed from %1 to %2</b>	I, C, r, R
G	NTP System peer change - <b>System peer changed from %1 to %2</b>	HOPF_S(0) <i>hopf-System</i> " " no peer, IP-Address, DNS-Name
G	NTP Stratum change - <b>Stratum changed from %1 to %2</b>	0, 1, 2,... 16
E	Firmware <b>Firmware update performed</b>	-
E	Announcement of leap second <b>Leap second has been announced - will take place with the next hour change</b>	-
E	Reboot <b>Reboot by user has been initiated</b>	-
E	Changes of configuration <b>Changes made in the configuration have been saved to flash disc</b>	-

Type of message ( E : single-point information ; G : group information )

## 12.6 Accuracy & NTP Basic Principles



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



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

Thus the QOS (Quality of Service) used for direct synchronisation with GPS or serial interface does not apply to synchronisation 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 synchronisation is dependent on the following criteria:

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

In order to guarantee the highest possible quality for the time synchronisation of the Board, an embedded Linux with NANO kernel extension is used as the operating system.

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 greater 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 synchronisation 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.



For further information see Appendix H (Analysis of Errors and Correctness Principles) of RFC1305 [1].

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

As an example, we mention the case where a network has a delay of 500msec and an accuracy shift (asynchronisation.) 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 web interface is designed to help the user to estimate the accuracy.



**GPS signal sources** with radio-synchronous synchronisation status:

<b>Lambda</b>	<b>Accuracy</b>
LOW	> 15 msec
MEDIUM	< 15 msec
HIGH	< 15msec AND Stability < 0.05 ppm

**DCF77 signal sources** with radio-synchronous synchronisation status:

<b>Lambda</b>	<b>Accuracy</b>
LOW	> 15 msec
MEDIUM	< 15 msec
HIGH	< 15msec AND Stability < 0.3 ppm

**Other signal sources** with quartz synchronisation status, configured with additional NTP servers:

<b>Lambda</b>	<b>Accuracy</b>
LOW	> 15 msec
MEDIUM	< 15 msec
HIGH	< 15msec AND Stability < 0.8 ppm

## 13 List of RFCs

## 13 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/HTTPS (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)

## 14 List of Open Source Packages used

Open-Source Package	7271	7272
boa-0.94.13.tar.gz	X	
boa-0.94.14rc21		X
busybox-1.00-pre5.tar.bz2	X	
busybox-1.14.4		X
e100-2.3.43.tar.gz	X	X
ethtool-3.tar.gz	X	X
gmp-4.1.2.tar.bz2	X	X
liboop-1.0.tar.gz	X	X
linux-2.4.21.tar.bz2	X	
linux-2.6.22.1 mit LINUXPPS Kit		X
lsh-1.5.3.tar.gz	X	
lsh-2.0.4		X
mini_httpd-1.19.tar.gz	X	
mini_httpd-1.19		X
mtd-snapshot-20040303.tar.bz2	X	
mtd-utils-1.0.0		X
net-snmp-5.2.1.2.tar.gz		X
ntp-4.2.0.tar.gz	X	
ntp-4.2.4p6		X
openssl-0.9.6l.tar.gz	X	
openssl-0.9.6l		X
passwd.tar.gz	X	X
PPSkit-2.1.2.tar.bz2	X	
setserial-2.17		X
smc91111.tar.bz2	X	X
net-snmp-5.2.1.2		X
sysklogd-1.4.1.tar.gz	X	
sysklogd-1.4.1		X
tinylogin-1.4.tar.bz2	X	X
uClibc-0.9.26.tar.bz2	X	
uClibc-0.9.29		X
udhcp-0.9.8.tar.gz	X	
udhcp-0.9.8		X
zlib-1.2.1.tar.bz2	X	
zlib-1.2.3		X