



MANUAL

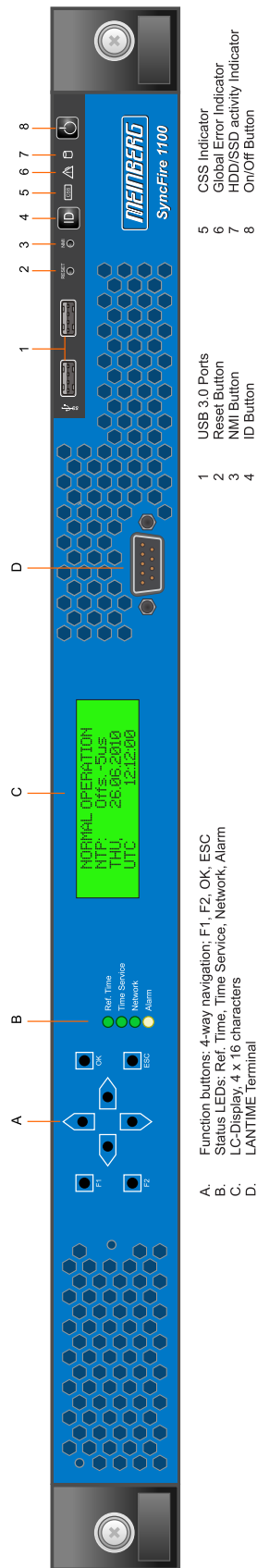
SyncFire 1100

High performant NTP Server

14th April 2016

Meinberg Radio Clocks GmbH & Co. KG

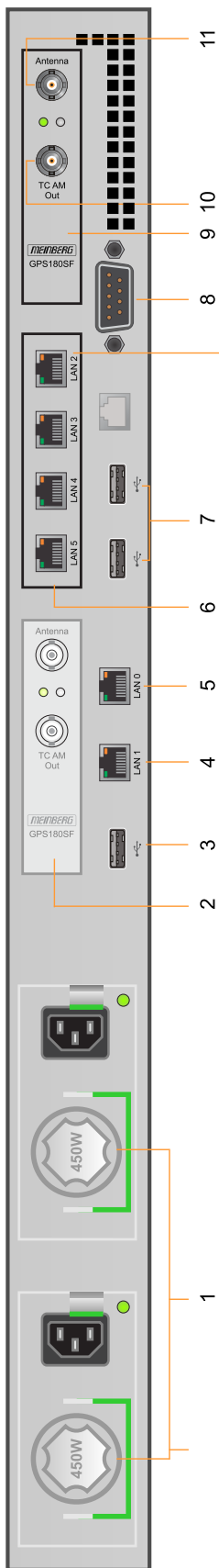
Front view (Frontansicht) SyncFire 1100



- A: Function buttons; 4-way navigation; F1, F2, OK, ESC
- B: Status LEDs: Ref. Time, Time Service, Network, Alarm
- C: LC-Display, 4 x 16 characters
- D: LANTIME Terminal

- 1: USB 3.0 Ports
- 2: Reset Button
- 3: NMI Button
- 4: ID Button
- 5: CSS Indicator
- 6: Global Error Indicator
- 7: HDD/SSD activity Indicator
- 8: On/Off Button

Rear view (Rückansicht) SyncFire 1100



- 1. Power supply (redundant power supplies)
- 2. Option: second receiver (Clock 2 - GPS or GLN)
- 3. USB connector
- 4. LAN 1 network connector
- 5. LAN 0 network management port
- 6. Option: four additional network ports 10/100/1000BASE-T or two additional network ports 10GBASE SFP

- 7. USB connectors
- 8. Video connector (standard operation)
- 9. GPS or GLN receiver - Clock 1
- 10. TC-AM - modulated time code output, BNC
- 11. Antenna input Clock 1, BNC female

Option: additional network ports 10GBASE SFP

Table of Contents

1	Imprint	1
2	Used Symbols	2
3	Safety instructions for building-in equipment	3
4	The Modular System SyncFire 1100	5
4.1	Network Configuration Concept	6
4.2	Why to use a Network Time Server?	7
5	Installation	8
6	Mounting the GPS Antenna	9
6.1	Example:	9
6.2	Antenna Assembly with Surge Voltage Protection	10
6.3	Antenna Short-Circuit	11
7	Quick Start	12
8	Booting the GPS180 receiver	13
9	Introduction: Configuration LANTIME	14
10	Front Panel of SyncFire 1100	15
10.1	Control Elements	16
10.2	Indicators on the control panel	17
10.3	Indicators on the Drives	17
11	The Menus in Detail	18
11.1	Root Menu	18
11.2	Menü: Reference Time	20
11.2.1	Menu: Info Receiver	20
11.2.2	Menu: Setup GPS180	22
11.2.3	Setup Time Zone	22
11.2.4	Setup GPS Outputs	23
11.2.5	Enable Outputs	23
11.2.6	TIME CODE (IRIG)	23
11.3	Menu: Reference Time (RDT Option)	24
11.4	Menu: Time Service	25
11.4.1	Menu: external NTP	25
11.4.2	Menu: Stratum of local clock	25
11.4.3	Menu: Restart NTP	25
11.5	Menu: Network	26
11.5.1	Menu: Global Configuration	27
11.5.2	Menu: Setup Network Interfaces	27
11.5.3	Menu: Setup IPv4 LAN Parameter	28
11.5.4	Menu: Setup IPv6 Parameter	28
11.5.5	Menu: Link Mode	28
11.5.6	Menu: Network Services	29
11.6	Menu: System	30
11.6.1	Menu: Set time zone	30
11.6.2	Menu Restart	31
11.6.3	Menu: System Info	32
12	The graphical user interfaces	33

13 The WEB Interface	34
13.1 Configuration: Main Menu	34
13.2 Configuration: Network	36
13.2.1 Network interface specific configuration	36
13.2.2 IPv4 addresses and DHCP	41
13.2.3 IPv6 addresses and autoconf	42
13.2.4 High Availability Bonding	43
13.3 Configuration: Notification	44
13.3.1 SYSLOG Server	44
13.3.2 E-mail messages	45
13.3.3 Windows Messenger Information	45
13.3.4 SNMP-TRAP messages	46
13.3.5 VP100/NET wall mount display	46
13.3.6 User defined Alarm scripts	47
13.3.7 Miscellaneous	48
13.3.8 Alarm events	49
13.4 Configuration: Security	51
13.4.1 HTTP Access Control	51
13.4.2 Front Panel	51
13.4.3 SSH Secure Shell Login	51
13.4.4 Generate SSL Certificate for HTTPS	52
13.4.5 SNMP Parameter	55
13.4.6 SHS Configuration	56
13.5 Configuration: NTP	57
13.5.1 General Settings	57
13.5.2 External NTP Server	58
13.5.3 NTP Local Clock	59
13.5.4 NTP Broadcast	60
13.5.5 Show NTP Configuration	62
13.5.6 NTP Restrictions	63
13.5.7 NTP Authentication	64
13.5.8 NTP Autokey Settings	66
13.5.9 NTP Leap Second Handling	69
13.6 Configuration: PTP V2	70
13.6.1 PTP Status Information	71
13.6.2 PTP Configuration Menu	75
13.7 FDM - Frequency Deviation Monitoring	85
13.7.1 FDM - Current State	85
13.7.2 FDM Configuration	85
13.7.3 Manual FDM Configuration	87
13.8 Configuration: System	88
13.8.1 Common Configuration	88
13.8.2 Web interface language	88
13.8.3 Services and Functions	89
13.8.4 User Management	91
13.8.5 System Information	95
13.8.6 Show System Messages	95
13.8.7 Firmware/Software Update	100
13.8.8 Download Diagnostic File	100
13.8.9 Configuration and Firmware Management	101
13.8.10 Display	102
13.8.11 Option: Fan Control	102
13.9 Configuration: Statistics	103
13.9.1 Statistical Information	106
13.10 Configuration: Receiver	107
13.10.1 MRS Settings	108
13.10.2 IRIG Settings	109
13.10.3 Serial Ports	110
13.10.4 Synthesiser	111
13.10.5 Time Zone	111
13.10.6 Enable Outputs	111

13.10.7 Miscellaneous	112
13.10.8 Receiver Information	114
13.11 I/O Configuration	115
13.11.1 Configuration: Input	115
13.11.2 Configuration: Output	118
13.12 NTP Monitoring	119
13.13 Configuration: Documentation	120
14 Attachment: Technical Information	121
14.1 Skilled/Service-Personnel only: Replacing the Lithium Battery	121
14.2 Technical Specifications SyncFire 1100	122
14.3 Front/Rear Panel Connectors	123
14.4 TERMINAL (Console)	124
14.5 USB Connector	124
14.6 10/100/1000base-T Gigabit Ethernet (IEEE 802.3-2008)	125
14.7 10 Gigabit SFP+	125
14.8 GPS Antenna	125
14.9 GLN Antenna	126
14.10 Time Code AM Output	126
15 Declaration of Conformity	127

1 Imprint








Meinberg Funkuhren GmbH & Co. KG
Lange Wand 9, 31812 Bad Pyrmont - Germany

Phone: + 49 (0) 52 81 / 93 09 - 0
Fax: + 49 (0) 52 81 / 93 09 - 30

Internet:<http://www.meinberg.de>
Mail: info@meinberg.de

Date: 2015-11-01

2 Used Symbols

Nr.	Symbol	Beschreibung / Description
1		IEC 60417-5031 Gleichstrom / <i>Direct current</i>
2		IEC 60417-5032 Wechselstrom / <i>Alternating current</i>
3		IEC 60417-5017 Erdungsanschluss / <i>Earth (ground) Terminal</i>
4		IEC 60417-5019 Schutzleiterklemme / <i>Protective Conductor Terminal</i>
5		Vorsicht, Risiko eines elektrischen Schlages / <i>Caution, possibility of electric shock</i>
6		ISO 7000-0434 Vorsicht, Risiko einer Gefahr / <i>Caution, Danger</i>
7		2002/96/EC Dieses Produkt fällt unter die B2B Kategorie. Zur Entsorgung muss es an den Hersteller übergeben werden. <i>This product is handled as a B2B category product. In order to secure a WEEE compliant waste disposal it has to be returned to the manufacturer.</i>

CE marking

This device follows the provisions of the directives 93/68/EEC



3 Safety instructions for building-in equipment

This building-in equipment has been designed and tested in accordance with the requirements of Standard IEC60950-1 "Safety of Information Technology Equipment, including Electrical Business Equipment".

During installation of the building-in equipment in an end application (i.e. rack) additional requirements in accordance with Standard IEC60950-1 have to be taken into account.

- The building-in equipment is a class 1 - equipment and must be connected to an earthed outlet (TN Power System).
- The building-in equipment has been evaluated for use in office environment (pollution degree 2) and may be only used in this environment. For use in rooms with a higher pollution degree more stringent requirements are applicable.
- The building-in equipment may not be opened.
- Protection against fire must be assured in the end application.
- The ventilation opening may not be covered.
- The equipment/building-in equipment was evaluated for use in a maximum ambient temperature of 40°C.
- For safe operation the building-in equipment must be protected by max 16 A fuse in the power installation system.
- Disconnection of the equipment from mains is done by pulling the mains plug.
- Do not expose the server to extreme environmental conditions.



Note: The SyncFire 1100 cannot operate as a standard server. Meinberg's SyncFire 1100 was developed to operate as a powerful NTP time server and does not provide the needed operation system to be deployed as a standard server.

Make sure that the server is acclimatized for the time indicated in this table before putting it into operation:

Temperature difference (°C)	Minimum acclimatization time
5	3
10	5
15	7
20	8
25	9
30	10

4 The Modular System SyncFire 1100

The SyncFire 1100 is a time server system based on a Primergy Fujitsu Server with an integral Meinberg GPS or combined GPS/GLONASS reference clock all installed in a 19 inch rackmount case and ready to operate. The interfaces provided by SyncFire 1100 are accessible via connectors in the rear panel and front panel of the case. Details of the components are described below.

Please Note: The SyncFire 1100 is also available as RDT variant. In that case, the time server does not include a built-in receiver and the reference time will be provided by another available NTP server in the network.



The implemented NTPD distributes the reference time from the used receiver cyclic in the network. Information on the NTPD is monitored on the LC-Display or can be inquired via the network.

The installation of system is very easy for the system/network administrator. The network address, the netmask and the default gateway have to be configured from the front panel of SyncFire 1100. The network address or the equivalent name of system has to be shown to all NTP clients in the TCP/IP network.

As well as NTP the Linux system also supports a number of further network protocols: HTTP(S), FTP, SSH and Telnet. Because of this remote configuration or status requests can come from any WEB browser. This access via the network can be deactivated. Changes in the receiver status, errors or other important events are logged either on the local Linux system or on an external SYSLOG-Server. In addition messages can be sent to a data center via SNMP traps or automatically generated e-mails where they can be recorded. Furthermore all alarm messages can be displayed by the large display VP100/20/NET that is accessed via network connection. In order to avoid a service interruption several Meinberg NTP servers can be installed in the same network to obtain redundancy.

4.1 Network Configuration Concept

The LANTIME system supports a wide range of different network environments due to its flexible and powerful network configuration concept. A separation between physical and logical ("virtual") interface configurations covers almost all possible requirements for datacenters, telecommunication backhaul networks and industrial network environments.

Each LANTIME server has at least one physical ethernet interface which is provided by the CPU module (lan0). Additional network interfaces can be provided by network expansion cards (LNE or TSU cards) or on backplanes (depending on model). These additional physical interfaces can be used to provide synchronization services to multiple physical network segments, to separate management and synchronization networks or to combine multiple ethernet interfaces to form redundant connections ("bonding"). The 6th generation of LANTIME firmware (LTOS6) can manage up to 99 physical network interfaces as a theoretical maximum.

Configuration of IPv4 and IPv6 addresses is done based on logical interface configurations. Each logical interface is assigned to one physical ethernet port and can be configured to use one IEEE 802.1q VLAN ID. The current firmware version supports up to 99 logical interfaces per server and all of those could be theoretically assigned to a single physical port.

The network ports of TSU modules (for PTP and Hardware-NTP) are not providing this logical interface functionality and are limited, at least in the current firmware version, to one IPv4/IPv6 address and one VLAN ID per physical interface. Redundancy and connectivity to multiple network segments and VLANs can be achieved by adding multiple TSU cards in a system.

For each logical interface the available network services for synchronization (NTP, TIME, ..) and management (HTTP, HTTPS, SSH, SNMP, TELNET, ...) can be enabled/disabled individually. This allows to only provide synchronization on one IP address and remote access the unit for management tasks over a different IP address.

4.2 Why to use a Network Time Server?

In principle it is possible to synchronize your computers with time servers on the internet. However, a lot of our customers rely on their own time server in their network environment for security and/or maintainability reasons.

- Particularly in the case of our NTP SERVER you or a responsible person can be notified by mail or SNMP trap if there is a malfunction in your time synchronization.
- The clients on the network do not depend on an active internet connection.
- The clients on the network do not depend on the availability of an external time server.
- A test of other freely available time servers reported that many NTP servers distributed a significantly wrong time, although they were classified as stratum-1 time servers. This is the responsibility of the server's administrators.
- If an internet connection is working properly then NTP can determine and account for the packet transmission delays quite reliable. However, if the internet connection is at its capacity limit, time synchronization can be significantly degraded due to high dispersion in packet transmission delays. Reasons for this may be hacker attacks, which must not address your own network, or new viruses causing a huge flood of emails, like it has already happened in the past.

In the United States the U.S. Naval Observatory (USNO) has a similar function to spread the legal time as the PTB in Germany, and also operates publicly available NTP servers for a long time. Those NTP servers are more and more constrained by "bad" clients, which makes the future of the public service questionable. There are already precautions to limit the affect of such clients. Dave Mills, the originator of NTP, cooperates with the USNO and has already adverted this in the NTP news group.

The topics outlined above should provide some arguments to install an own time server, if an accurate time is a requirement for the reliable operation of a local network.

5 Installation



First of all, carefully read the safety instructions in this chapter!

- Transport the server to the place where you want to set it up.
- Unpack the system, check the contents of the package for visible transport damage and check whether the items delivered match the details on the packing list.
- Mount the server into the rack.
- Wire the server. Follow the instructions in sections "Connecting devices to the server".
- Connect the server to the mains.
- Familiarize yourself with the controls and indicators on the front and rear of the server (see section "Controls and indicators").
- Configure the server: the following options are available:
 - Remote configuration via the HTTP interface
 - Basic configuration via function Keys and LE-Display

6 Mounting the GPS Antenna

The GPS satellites are not stationary, but circle round the globe with a period of about 12 hours. They can only be received if no building is in the line-of-sight from the antenna to the satellite, so the antenna/downconverter unit must be installed in a location that has as clear a view of the sky as possible. The best reception is achieved when the antenna has a free view of 8° angular elevation above the horizon. If this is not possible, the antenna should be installed with the clearest free view to the equator, because the satellite orbits are located between latitudes 55° North and 55° South. If this is not possible, you may experience difficulty receiving the four satellites necessary to complete the receiver's position solution.

The antenna/converter unit can be mounted on a wall, or on a pole up to 60 mm in diameter. A 50 cm plastic tube, two wall-mount brackets, and clamps for pole mounting are included. A standard RG58 coaxial cable should be used to connect the antenna/downconverter unit to the receiver. The maximum length of cable between antenna and receiver depends on the attenuation factor of the coaxial cable.

Up to four GPS180 receivers can be run with one antenna/downconverter unit by using an optional antenna splitter. The total length of an antenna line from antenna to receiver must not be longer than the max. length shown in the table below. The position of the splitter in the antenna line does not matter.

The optional delivered MBG S-PRO protection kit can also be used for outdoor installation (degree of protection: IP55).

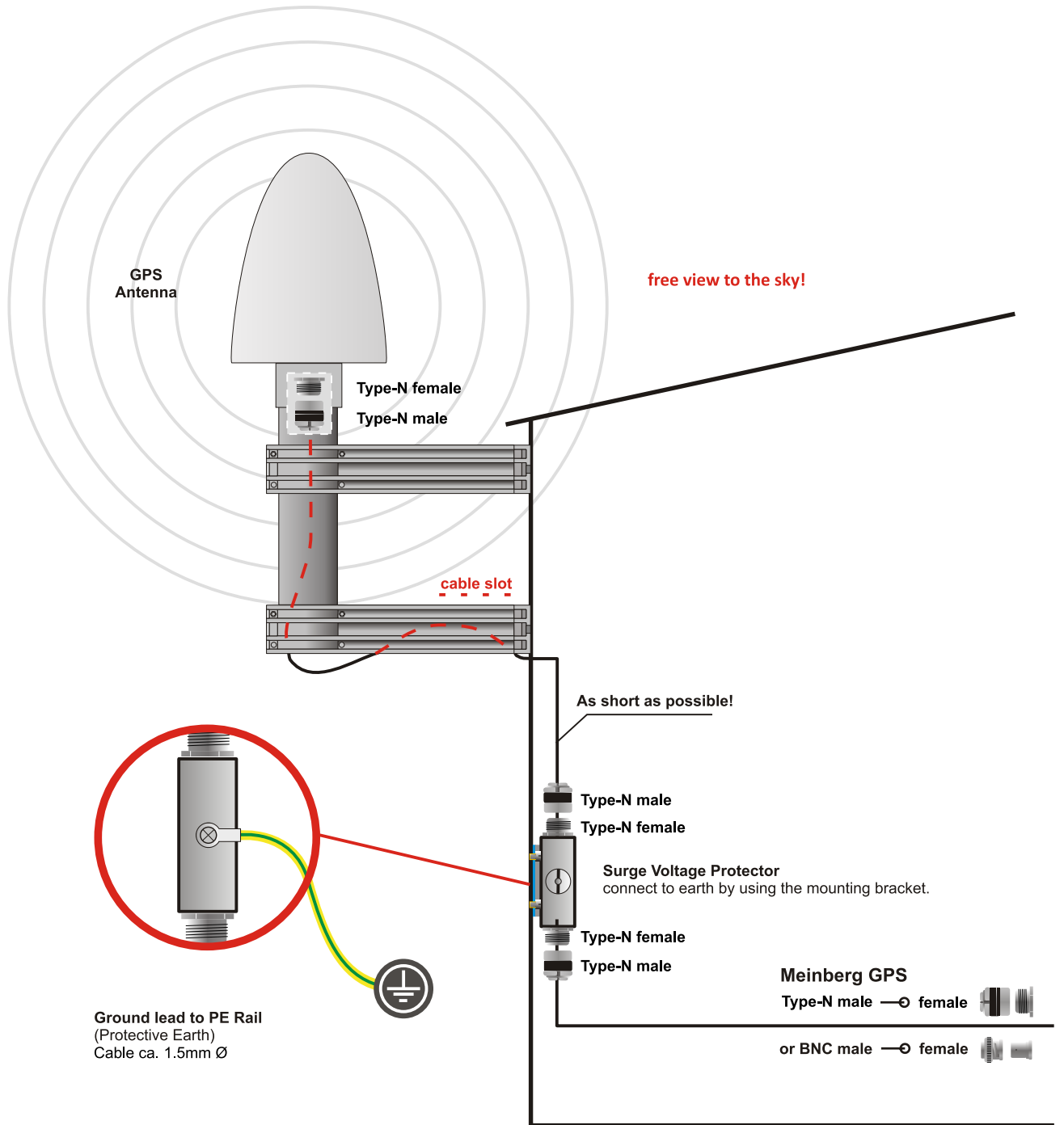
6.1 Example:

Type of cable	diameter \varnothing [mm]	Attenuation at 100MHz [dB]/100m	max lenght. [m]
RG58/CU	5mm	17	300 ⁽¹⁾
RG213	10.5mm	7	700 ⁽¹⁾

(1)This specifications are made for antenna/converter units produced after January, 2005
The values are typically ones; the exact ones are to find out from the data sheet of the used cable

6.2 Antenna Assembly with Surge Voltage Protection

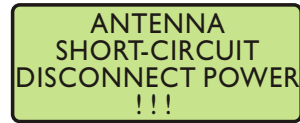
Optional a surge voltage protector for coaxial lines is available. The shield has to be connected to earth as short as possible by using the included mounting bracket. Normally you connect the antenna converter directly with the antenna cable to the system.



6.3 Antenna Short-Circuit

(systems with front display only)

In case of an antenna line short-circuit the following message appears in the display:



ANTENNA
SHORT-CIRCUIT
DISCONNECT POWER
!!!

A rectangular box with a light green background and a black border containing the text: ANTENNA SHORT-CIRCUIT DISCONNECT POWER !!!

If this message appears the clock has to be disconnected from the mains and the defect eliminated. After that the clock can be powered-up again. The antenna supply voltage must be 15V_{DC} .

7 Quick Start

When booting the system the following message will be displayed while dots will be counted up in the lower line:

```
Starting up
please wait ...
.....
```

Main Menu will be displayed with some important status informations after booting has finished:

```
NORMAL OPERATION
NTP: Offs. 2ms
Thu, 01.01.2008
UTC 12:00:00
```

If the GPS receiver remains asynchronous (Refclock LED is still red after 12 minutes) the number of satellites in view and the good satellites are to check (press buttons ↓, →, ↓ from main menu). The antenna has to be installed without any obstructions to the sky.

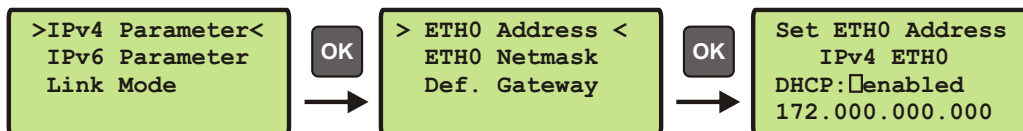
```
SV CONSTELLATION
SV in view: 10
Good Svs   : 9
Sel:01 21 16 22
```

For first time installation enter TCP/IP address, netmask and default gateway. To get an overview of the current configuration press F2 from main menu. Press F2 again to enter SETUP configuration page. Please ask your administrator for proper TCP/IP configuration:



Then press 3 times the OK button to change to IPV4 ETH0 configuration page to enter the IP address, netmask and the default gateway:

NOTE: These settings are related to the first Ethernet connection (ETH0).



After this all further settings can be done via network interface, either by using a WEB browser or a Telnet Session.

Default user: root
 Default password: timeserver

8 Booting the GPS180 receiver

If both the antenna and the power supply have been connected, the system is ready to operate. About 2 minutes after power-up the receiver's oscillator has warmed up and operates with the required accuracy. If the receiver finds valid almanac and ephemeris data in its battery buffered memory and the receiver's position has not changed significantly since its last operation, the receiver can determine which satellites are presently in view. Only a single satellite must be received to synchronize and generate output pulses, so synchronization can be achieved within one minute after power-up.

If the receiver position has changed by more than one hundred kilometers since last operation, the satellites' real elevation and Doppler might not match those values expected by the receiver, and this will force the receiver to start scanning for satellites. This mode is called **Warm Boot** because the receiver can obtain ID numbers of existing satellites from the valid almanac. When the receiver has found four satellites in view it can update its new position and switch to **Normal Operation**. If the almanac has been lost (because the battery has been disconnected) the receiver has to scan for a satellite and read in the current almanac. This mode is called **Cold Boot**. It takes 12 minutes until the new almanac is complete and the system switches to Warm Boot mode, scanning for other satellites.

9 Introduction: Configuration LANTIME

There are several ways to configure the LANTIME parameters:

- TELNET
- SSH
- HTTP Interface
- Secure HTTP Interface (HTTPS)
- Terminal in front panel (38400/8N1/VT100)
- Front panel LCD/VFD Interface
- SNMP Management

In order to be able to configure the time server via the web interface or a telnet/SSH connection, an IP address has to be assigned via the front panel keys and LC/VF display (for automatic assignment possibilities please refer to: DHCP IPv4 or AUTOCONF IPv6). Once the IPv4 address, net mask and IPv4 GATEWAY have been set up or the network interface has been automatically configured with DHCP/Autoconf, further configuration changes can be done via a network connection:

Note: If the system doesn't has a display feature (e.g. LANTIME M100), goto chapter LANTIME Setup Wizard in this manual.

To set up a TELNET connection the following commands are entered:

```
telnet 198.168.10.10 // LANTIME IP  
Default User: root  
Default Password: timeserver
```

To set up a SSH connection the following commands are entered:

```
ssh root@198.168.10.10 // LANTIME IP  
Default Password: timeserver
```

To set up a HTTP connection the following address is to enter in a web browser:

```
http://198.168.10.10 // LANTIME IP  
Default User: root  
Default Password: timeserver
```

To set up a Secure HTTP (HTTPS) connection the following address is entered in a web browser:

```
https://198.168.10.10 // LANTIME IP  
Default User: root  
Default Password: timeserver
```

10 Front Panel of SyncFire 1100



LC-Display, 4 x 20 characters

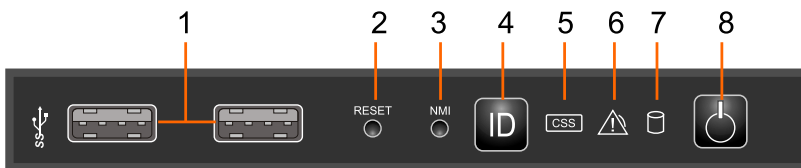
Eight push buttons to set up basic network parameters and to change receiver settings

Four bicolor LEDs

showing status of:

- Reference time
- Time service
- Network
- Alarm

Indicators and Function Keys on the Front Panel



1 USB 3.0 Ports

2 Reset Button

3 NMI Button

4 ID Button

5 CSS Indicator

6 Global Error Indicator

7 HDD/SSD activity Indicator

8 On/Off Button

10.1 Control Elements

7: On/Off Button:

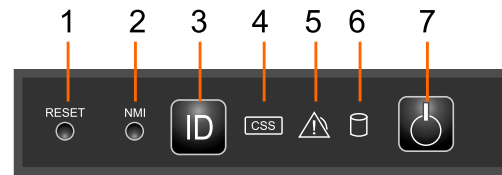
When the system is switched off, it can be switched on again by pressing the On/Off button.

When the system is operating, pressing the On/Off button will switch off the system.

4: CSS indicator (yellow) - „Customer Self Service“

Lights up yellow if a prefailure event was detected for a CSS component that you can fix yourself (for reasons of precaution) with the CSS concept. Flashes yellow if an error was detected that you can fix yourself with the CSS concept.

Does not light up when the system is OK. If the event is still acute after a power cycle, the indicator is activated after the restart. The indicator also lights up in standby mode.



Risk of loss of data!

The On/Off button does not disconnect the server from the mains voltage. To disconnect from the mains completely, remove the power plug(s).



2: NMI Button

Do not press!

Risk of loss of data!

The NMI button may only be used by service personnel.



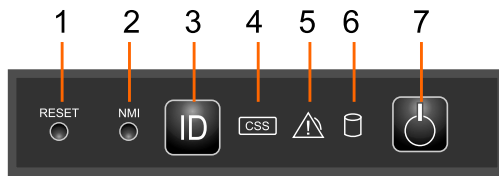
1: RESET Button

Risk of loss of data!

Pressing the reset button reboots the system.



10.2 Indicators on the control panel



5: Global Error indicator (orange)

Lights up orange if a prefailure event has been detected that requires (precautionary) service intervention. Flashes orange if an error was detected that requires service intervention.

Does not light up if there is no critical event. If the event is still acute after a power cycle, the indicator is activated after the restart. The indicator also lights up in standby mode.

7: Power-on indicator (three colors)

Lights orange when the server is switched off but mains voltage is present.

Lights up yellow during power up delay. If the server is switched off and then immediately switched on again, a server is only restarted after a power up delay.

This prevents a current overload, for example:

Lights up green when the server is switched ON. Flashes green if the server has been switched on and is in standby mode or if the server is in a sleep state.

10.3 Indicators on the Drives

4: CSS indicator (yellow) - „Customer Self Service“

Lights up yellow if a prefailure event was detected for a CSS component that you can fix yourself (for reasons of precaution) with the CSS concept.

Flashes yellow if an error was detected that you can fix yourself with the CSS concept.

Does not light up when the system is OK. If the event is still acute after a power cycle, the indicator is activated after the restart. The indicator also lights up in standby mode.

3: ID indicator (blue)

Lights up blue when the system has been selected by pressing the ID button. To deactivate, press the button again.

6: Global Error indicator

Lights up orange if a prefailure event has been detected that requires (precautionary) service intervention. Flashes orange if an error was detected that requires service intervention.

Does not light up if there is no critical event. If the event is still acute after a power cycle, the indicator is activated after the restart.

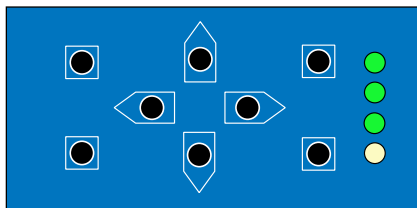
11 The Menus in Detail

11.1 Root Menu

The root menu is shown when the receiver has completed initialization after power-up. With the four arrow buttons and the buttons „OK“, „ESC“, „F1“ and „F2“ the navigation and setting of parameters can be managed. Main menu can be reached by pressing „ESC“ some times. The main menu reflect some of the main parameters of the time server. First line shows the name of the device and the status of the Reference Clock (GPS). The text "GPS: NORMAL MODE" might be replaced by "COLD BOOT", "WARM BOOT" or "UPDATE ALMANAC". If the antenna is disconnected or not working properly, the text "ANTENNA FAU" is displayed instead.



Current time and date of the timeserver with the name of the time zone (NTP uses UTC time zone) will be monitored in the bottom line. If the "IGNORE LOCK" option is enabled an "*" will be shown behind the time.



The multicolor LEDs will reflect the current state of the device.

„Ref. Time“

green: the reference clock (e.g. integrated GPS) produce valid time.

red: the reference clock produce no valid time (e.g. not synchronized)

„Time Service“

green: NTP has been synchronized to reference clock.

red: NTP is not synchronous to reference clock or sync to „local clock“

„Network“

green: all watched network ports has been "link up" detected

red: at least one of the watched network ports (look at „Setup Device Parameter / Check Network Linkup“) is not connected

„Alarm“

off: no error at moment

red: general error – more information will be shown on display.

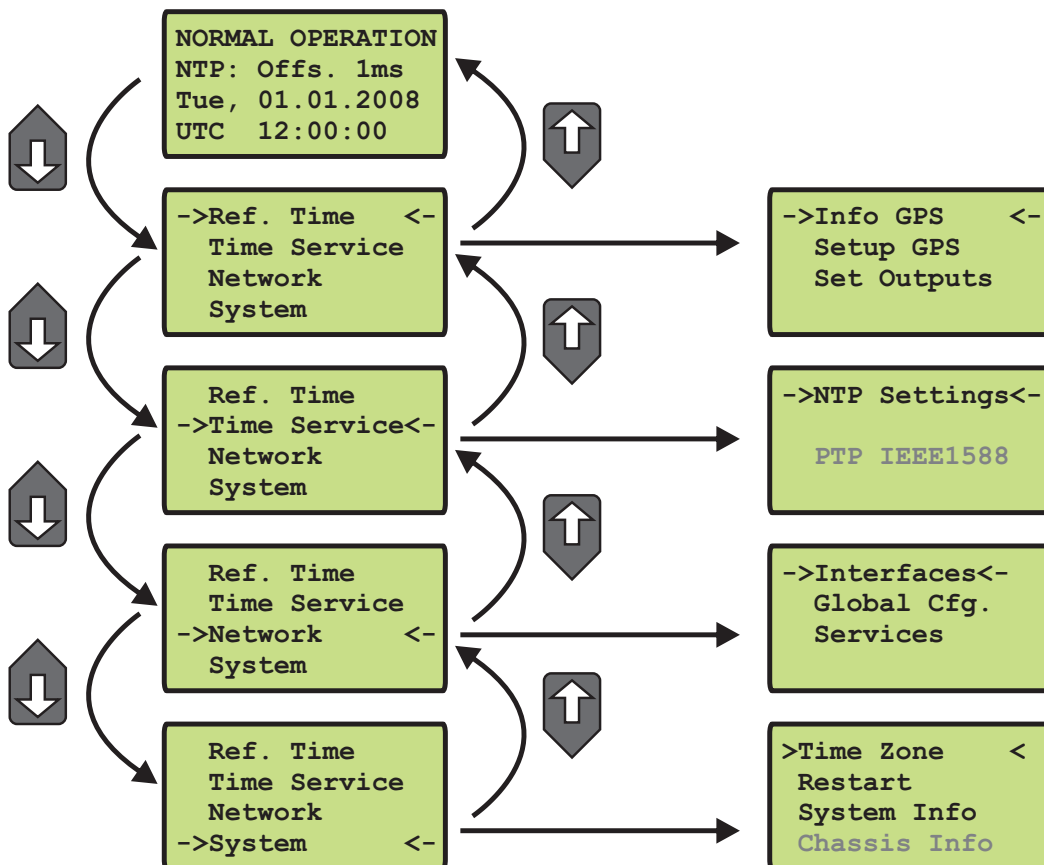
If the symbol „F1“ will be shown in the upper right corner a help page can be displayed when pressing the „F1“ button. When pressing „F1“ from main menu a short description for menu navigation will be displayed:

Use → and ← to select different main menus. Use ↑ and ↓ to enter

When pressing the „OK“ button from main menu the version of the LANTIME software, the NTP and the LINUX kernel version will be displayed.

```
ELX800    VX.XXx
SN: 000000000000
NTP: X.X.Xx@X.X
Krn.: X.X.XX.X
```

The following main menus will be displayed when pressing the „UP“ and „DOWN“ arrow buttons:



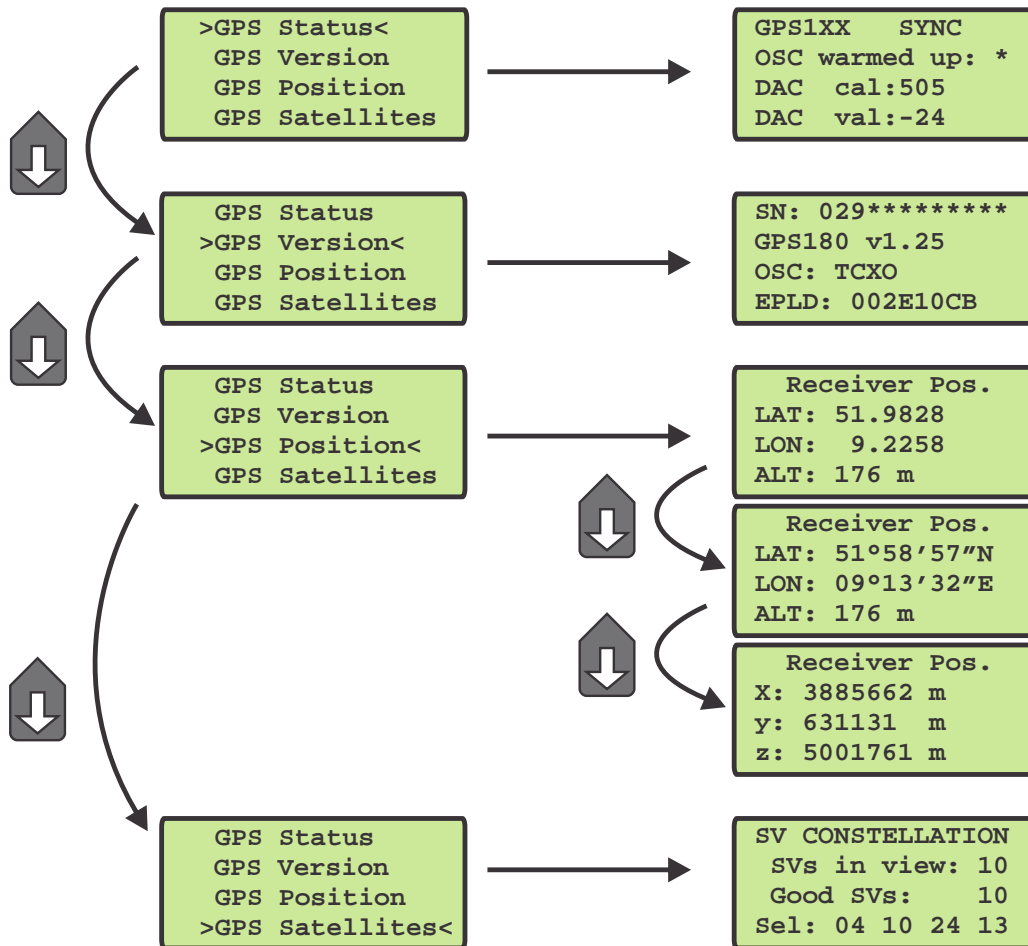
11.2 Menü: Reference Time

The Reference Clock menu and all its sub menus will manage all status information and parameters of the reference clock.



To enter the following sub menus press the „OK“ or right arrow button.

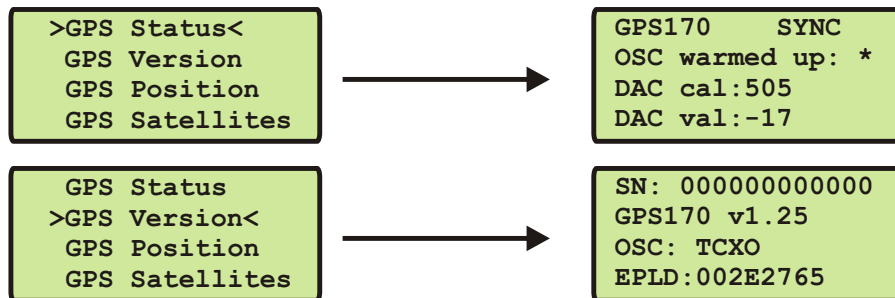
11.2.1 Menu: Info Receiver



In this menu all relevant information about the GPS radio clock, the internal oscillator and the GPS satellites will be shown.

GPS180 Status and Version

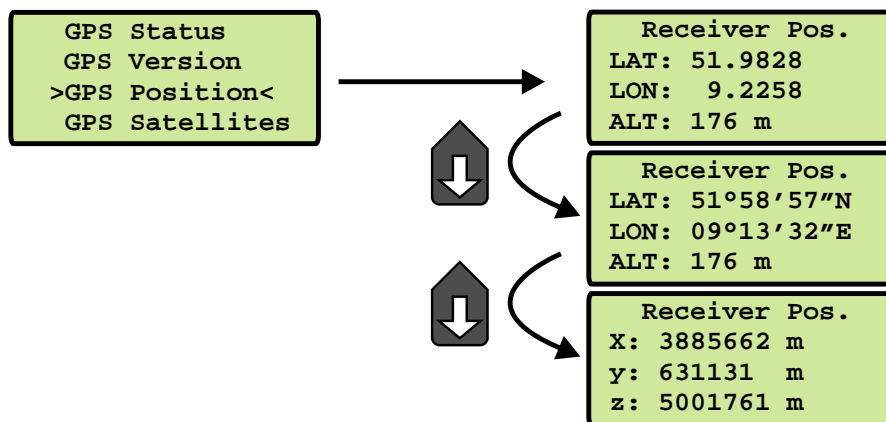
This page will monitor the current state („SYNC“ or „ASYNCL“) and the version of the reference clock.



The second line of "GPS Version" will reflect the version number of the GPS reference clock and the oscillator type. In the bottom line the serial number of the receiver will be shown.

GPS180 - Receiver Position

This menu shows the current receiver position. The „OK“ key lets the user select one of three formats. The default format is geographic latitude, longitude and altitude with latitude and longitude displayed in degrees, minutes and seconds. The next format is geographic too, with latitude and longitude displayed in degrees with fractions of degrees. The third format displays the receiver position in earth centred, earth fixed coordinates (ECEF coordinates).

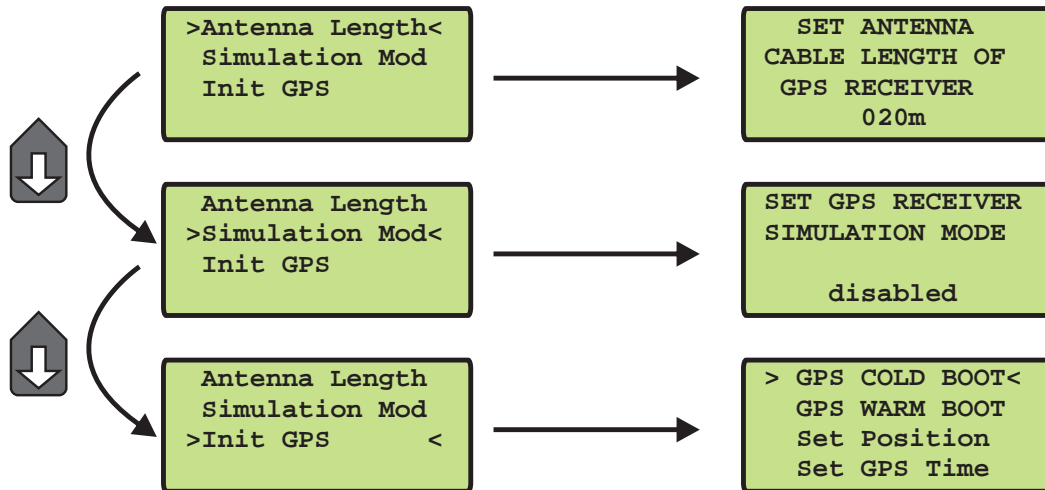


GPS180 - Satellite Constellation

The SV constellation menu gives an overview of the current satellites (SVs) in view. The display shows the number of satellites with an elevation of 5° or more (In view), the number of satellites that can be used for navigation (Good) and the selected set of satellites which are used to update the receiver position (Sel).



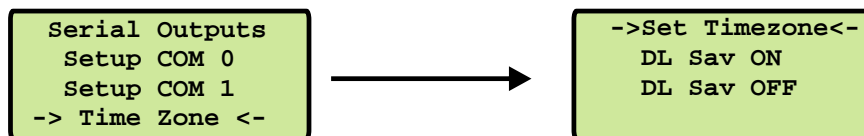
11.2.2 Menu: Setup GPS180



11.2.3 Setup Time Zone

The time zone of the GPS receiver can be set up. These parameters will affect the serial output lines and the timecode (IRIG) outputs. The internal time zone of the timeserver and the time of NTP will always be UTC. The time monitored in the main menu will be the time of the NTP.

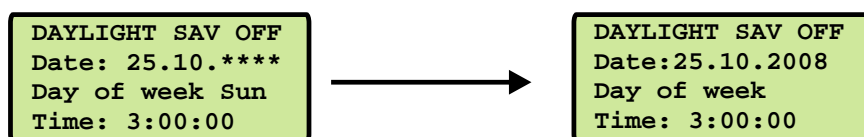
This menu lets the user enter the names of the local time zone with daylight saving disabled and enabled, together with the zones' time offsets from UTC. These parameters are used to convert UTC to local time, e.g. MEZ = UTC + 1h and MESZ = UTC + 2h for central Europe. The range of date daylight saving comes in effect can be entered using the next two pages of the setup menu.



Beginning and ending of daylight saving may either be defined by exact dates for a single year or using an algorithm which allows the receiver to re-compute the effective dates year by year. The figures below show how to enter parameters in both cases. If the number of the year is displayed as wildcards ('*'), a day-of-week must be specified. Then, starting from the configured date, daylight saving changes the first day which matches the configured day-of-week. In the figure below October 25th, 2008 is a Saturday, so the next Sunday is October 26th, 2008.

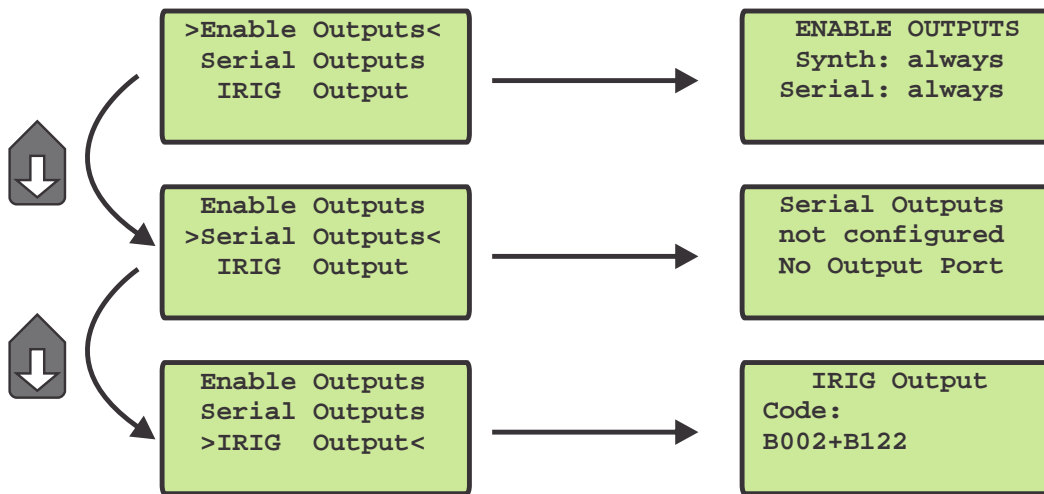
All changeover rules for the daylight saving like "the first/the second/the second to last/the last Sunday/-Monday etc. in the x-th month," can be described by the used format "first specified day-of-week after a defined date".

If the number of the year is not displayed as wildcards the complete date exactly determines the day daylight saving has to change (October 26th, 2008 in the figures below), so the day-of-week does not need to be specified and therefore is displayed as wildcards.



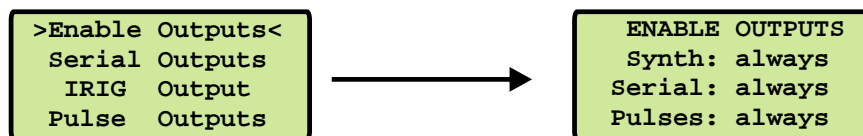
If no changeover in daylight saving is wanted, identical dates and times must be entered in both of the submenus (DAYLIGHT SAV ON/OFF). After this a restart should be done.

11.2.4 Setup GPS Outputs



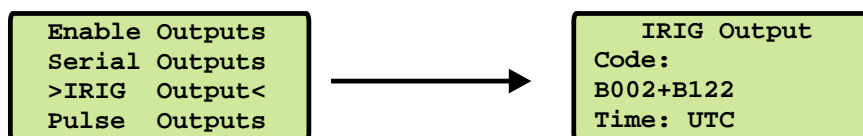
11.2.5 Enable Outputs

This menu lets the user configure at which time after power up the serial ports, pulse outputs, and frequency synthesizer output are to be enabled. Outputs which are shown to be enabled always will be enabled immediately after power-up. Outputs which are shown to be enabled if sync will be enabled after the receiver has decoded the signals from the satellites and has checked or corrected its on-board clock. The default setting for all outputs is if sync.



11.2.6 TIME CODE (IRIG)

This menu lets the user select the Timecodes to be generated by GPS180. Most IRIG-Codes do not carry any time zone information, hence UTC is selected for output by default. If desired, the clocks local time can be output by selecting "TIME: LOCAL".



Refer to chapter Timecode for details.

11.3 Menu: Reference Time (RDT Option)

The SyncFire 1100 can operate without integrated reference clock. In this case its reference source is provided by another available NTP server in the network.



You can adjust all relevant settings in the Submenu
Time Service -> NTP Settings -> NTP Setup -> external NTP.

11.4 Menu: Time Service

The NTP configuration page is used to set up the additional NTP parameters needed for a more specific configuration of the NTP subsystem.



11.4.1 Menu: external NTP

The default configuration of the timeserver consists of a local clock, which represents the hardware clock of your time server system and the GPS reference clock. The local clock is only chosen as the NTP time reference after the GPS clock lost its synchronization. The stratum level of this local clock is set to 12, this ensures that clients recognize the switchover to the local clock and are able to eventually take further actions. The local clock can be disabled if the timeserver should not answer anymore when the reference clock is out of order.



Additional external NTP servers can be set up to provide a high grade of redundancy for the internal reference clock.

11.4.2 Menu: Stratum of local clock

The local clock is only chosen as the NTP time reference after the GPS clock lost its synchronization. The stratum level of this local clock is set to 12, this ensures that clients recognize the switchover to the local clock and are able to eventually take further actions. The local clock can be disabled if the timeserver should not answer anymore when the reference clock is out of order. The field "Stratum of local clock" is used to change the stratum level of the local clock (see above), default is 12.

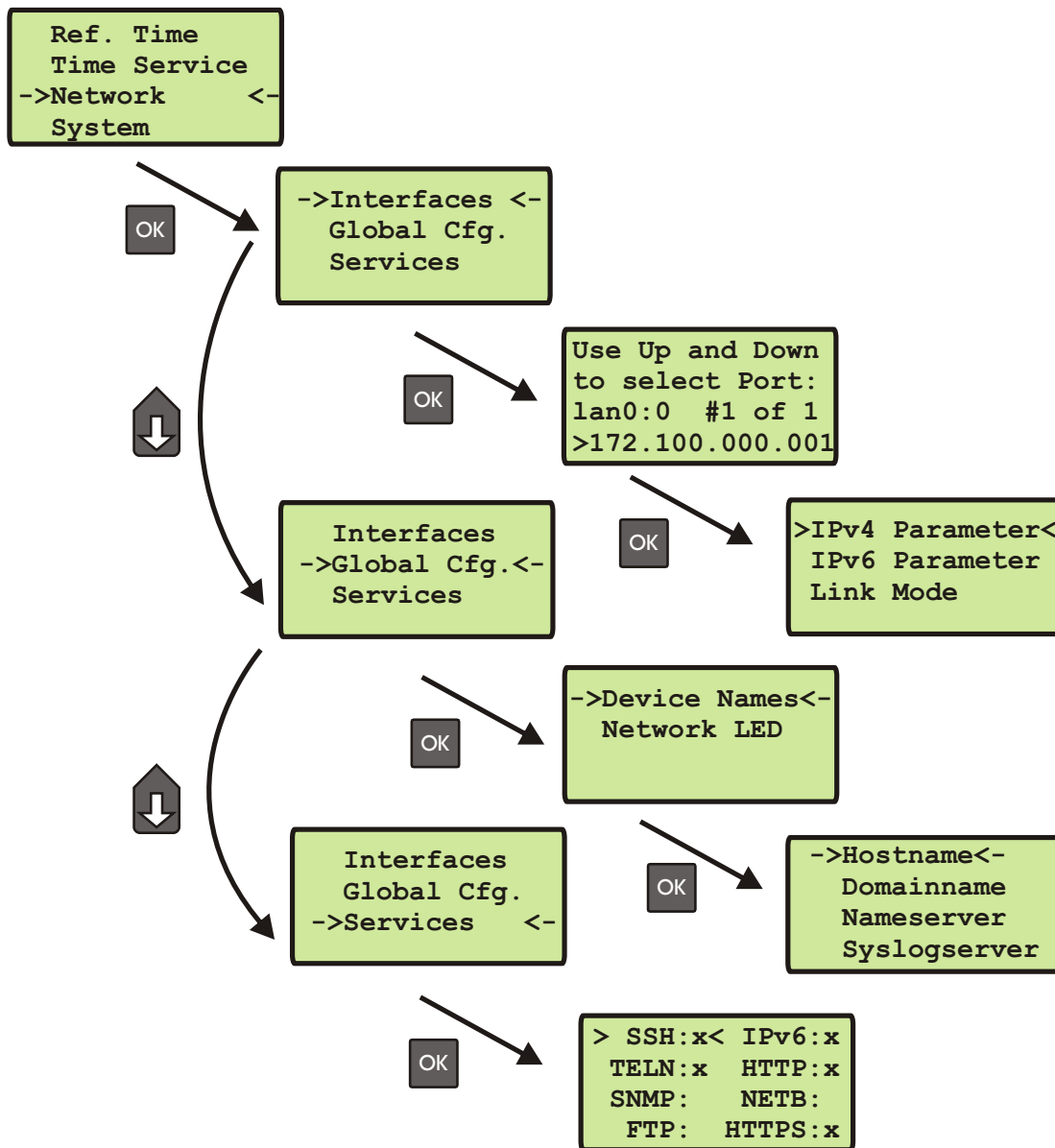


11.4.3 Menu: Restart NTP

The system time is setup, together with the reference time and the NTP service is rebooting.



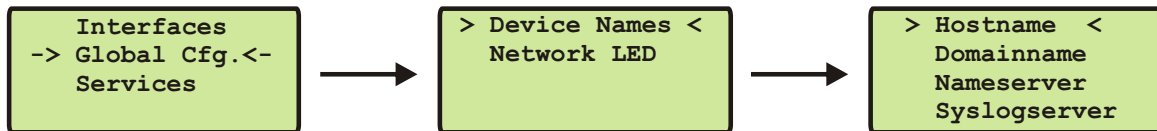
11.5 Menu: Network



In this submenu the network configuration parameters related to the network interfaces can be changed. The submenus can be selected with the arrow keys and the "OK" button:

As soon as an IP address is configured, additional network configuration can be done via network connection with TELNET, SSH or the WEB interface. Ask your network administrator for network specific parameters. Every change of the network parameters will restart the NTP. All network specific parameters will be saved on the flash disk (/mnt/flash/config/global_configuration) and will be reloaded after reboot. It is highly recommended not to edit this file manually but to configure the parameters via the several configuration interfaces (HTTP, CLI or SNMP). If this file is not present, an empty file will be created. See Appendix for the default settings of this file.

11.5.1 Menu: Global Configuration



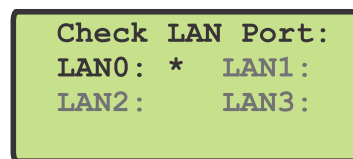
In this sub menu you can change the global network settings like host and domain name, nameserver and syslog server. Further name- or syslog servers can be set up via HTTP interface or CLI Setup. In the nameserver and syslog server fields you have to enter an Ipv4 address.

All information written to the LANTIME SYSLOG (/var/log/messages) can be forwarded to one or two remote SYSLOG servers. The SYSLOG daemon of this remote SYSLOG needs to be configured to allow remote systems to create entries. A Linux SYSLOG daemon can be told to do so by using the command "syslogd -r" when starting the daemon.

If you enter nothing in the SYSLOG server fields or specify 0 .0.0.0 as the SYSLOG servers addresses, the remote SYSLOG service is not used on your LANTIME.

Please be aware of the fact that all SYSLOG entries of the timeserver are stored in „/var/log/messages“ and will be deleted when you power off or reboot the timeserver. A daily CRON job is checking for the size of the LANTIME SYSLOG and deletes it automatically if the log size is exceeding a certain limit.

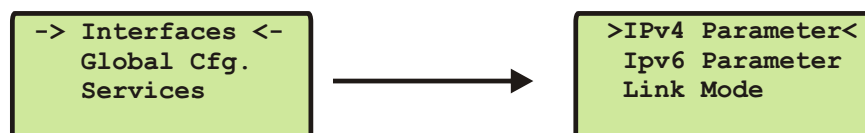
By specifying one or two remote SYSLOG servers, you can preserve the SYSLOG information even when you need to reboot or switch off the LANTIME.



The submenu „Netw. LED“ will monitor the network ports, which will be checked continuously if the network port is „LINKED UP“. If one of these ports has no link up, the network LED on the front panel will change to red. An „L“ for „LED“ indicates if the port is checked. Please navigate through the list of ports with the LEFT/RIGHT buttons and change the setting with the UP/DOWN buttons.

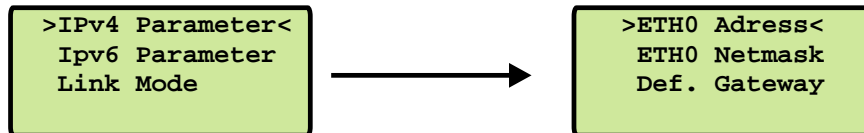
11.5.2 Menu: Setup Network Interfaces

In the network configuration parameters related to the network interfaces can be changed. The following sub-menus can be selected with the arrow keys and the "OK" button:



When configured an IP address once additionally network configuration can be done via network connection with TELNET, SSH or the WEB interface. Ask your network administrator for network specific parameters. Every change of the network parameters will restart the NTP. All network specific parameters will be saved on the flash disk (/mnt/flash/config/global_configuration) and will be reloaded after reboot.

11.5.3 Menu: Setup IPv4 LAN Parameter



There is a separate configuration submenu for every physical network interface. If there is no DHCP client mode activated a static IP address for each interface can be entered. IPv4 addresses are built of 32 bits which are grouped in four octets, each containing 8 bits. You can specify an IP address in this mask by entering four decimal numbers, separated by a point ".".

Example: 192.168.10.2

Additionally you can specify the IPv4 netmask and your default gateway address.

Please contact your network administrator, who can provide you with the settings suitable for your specific network.

If there is a DHCP (Dynamic Host Configuration Protocol) server available in your network, the time server system can obtain its IPv4 settings automatically from this server. If you want to use this feature (again, you should ask your network administrator whether this is applicable in your network), you can change the DHCP Client parameter to "ENABLED". Using DHCP is the default factory setting.

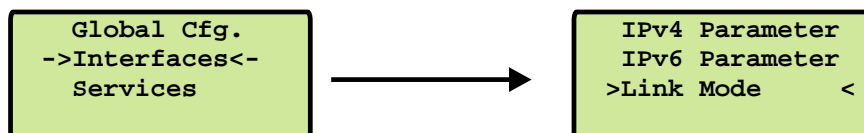
If the DHCP client has been activated, the automatically obtained parameters are shown in the appropriate fields (IPv4 address, netmask, gateway).

11.5.4 Menu: Setup IPv6 Parameter

The IPV6 parameter can be configured via the front panel display for the first ethernet port (ETH0) only. Additionally IPV6 configuration can be done via network connection with TELNET, SSH or the WEB interface. You can specify up to three IPv6 addresses for your time server. Additionally you can switch off the IPv6 autoconf feature. IPv6 addresses are 128 bits in length and written as a chain of 16 bit numbers in hexadecimal notation, separated with colons. A sequence of zeros can be substituted with "::" once.

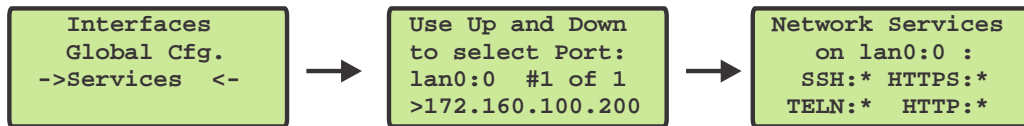
If you enabled the IPv6 protocol, the system always gets a link local address in the format "fe80:: ...", which is based upon the MAC address of the interface. If a IPv6 router advertiser is available in your network and if you enabled the IPv6 autoconf feature, your ntp server will be set up with up to three link global addresses automatically.

11.5.5 Menu: Link Mode



With the Link Mode submenu the parameters for link speed and duplex mode of the first ethernet interface (ETH0) can be configured. There are 5 modes available: Autosensing, 10 Mbit/Half Duplex, 100 Mbit/Half-Duplex, 10MBit/Full-Duplex, 100 Mbit/Full-Duplex. The interfaces are configured with „Autosensing“ by default.

11.5.6 Menu: Network Services



The possible network protocols and access methods can be configured. After pressing the OK button you can enable/disable SSH, TELNET, SNMP, FTP, IPV6, HTTP, HTTPS and NETBIOS by using the UP/DOWN Keys and navigate through the list with the LEFT/RIGHT keys. After you saved your settings with the "OK" button, all these subsystems are stopped and eventually restarted (only if they are enabled, of course).

11.6 Menu: System



In this submenu system specific parameters can be configured.

11.6.1 Menu: Set time zone



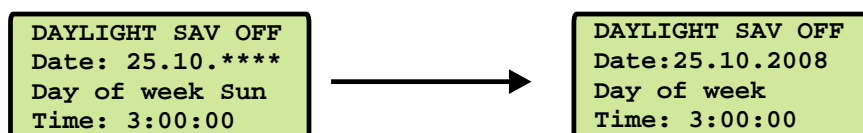
The time zone of the time that is shown on the front panel display can be set up here. The internal time zone of the timeserver and the time of NTP will always be UTC. These parameters will not affect the serial output lines and the timecode (IRIG) outputs. These parameters have to be configured in another menu - (**Reference Time->Setup Outputs**).

This menu lets the user enter the names of the local time zone with daylight saving disabled and enabled, together with the zones' time offsets from UTC. These parameters are used to convert UTC to local time, e.g. MEZ = UTC + 1h and MESZ = UTC + 2h for central Europe. The range of date daylight saving comes in effect can be entered using the next two pages of the setup menu.

Beginning and ending of daylight saving may either be defined by exact dates for a single year or using an algorithm which allows the receiver to re-compute the effective dates year by year. The figures below show how to enter parameters in both cases. If the number of the year is displayed as wildcards ('*'), a day-of-week must be specified. Then, starting from the configured date, daylight saving changes the first day which matches the configured day-of-week. In the figure below October 25th, 2008 is a Saturday, so the next Sunday is October 26th, 2008.

All changeover rules for the daylight saving like "the first/the second/the second to last/the last Sunday/Monday etc. in the x-th month," can be described by the used format "first specified day-of-week after a defined date".

If the number of the year is not displayed as wildcards the complete date exactly determines the day daylight saving has to change (October 26th, 2008 in the figures below), so the day-of-week does not need to be specified and therefore is displayed as wildcards.



If no changeover in daylight saving is wanted, identical dates and times must be entered in both of the submenus (DAYLIGHT SAV ON/OFF).

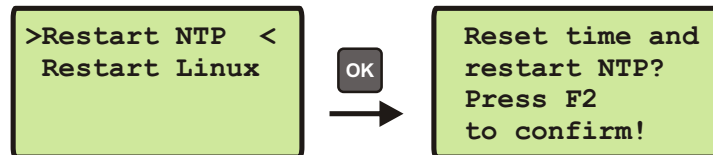
11.6.2 Menu Restart



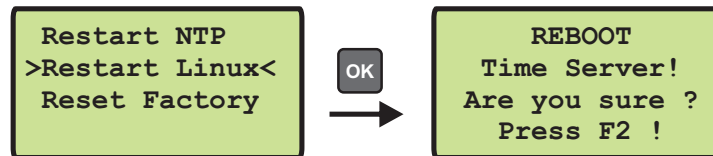
With the menu item **Restart** you can open the submenus *Restart NTP*, *Restart Linux* and *Factory Reset*.

Menu: Restart NTP

If the time of the reference clock has changed (e.g. while testing with different times) the system time has to be set with the time of the reference clock and the NTP has to be restarted.

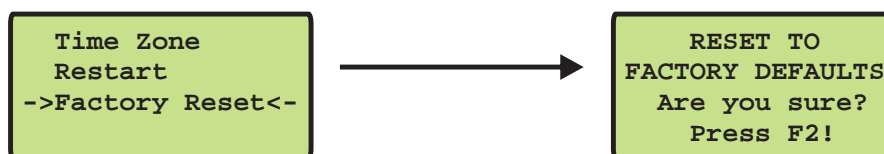


Menu Reboot System



The command **Reboot time server** reboots the Linux operating system – the build-in reference clock will not be restarted.

Menu Factory Reset



When **Reset to factory defaults** is called, all system parameters will be reset to initial values. However the parameters of each network interface do not change.

11.6.3 Menu: System Info



This submenu shows system specific information (e.g. CPU temperature).

12 The graphical user interfaces

The LANTIME offers two different options for configuration and status management: An extensive and powerful web interface and SNMP. In order to use the SNMP features of your LANTIME, you need special software like management systems or SNMP clients. In order to use the web interface, all you need is a web browser (LANTIME supports a broad range of browsers, we recommend Mozilla Firefox).

The screenshot displays the LANTIME Web Interface with the following sections:

- General Information:**

LANTIME	M3000/REDUNDANT (ELX)	Serial Number	000012323432
Contact	Unconfigured (Configure Now)	Location	Unconfigured (Configure Now)
Uptime	4 days, 17:22		
- Network Information:**

Hostname	lt-udo	Domain	
LAN IPv4 (IF 1 - lan0:0)	172.16.100.250/16	IPv6 (IF 1)	Not assigned
LAN IPv4 (IF 2 - lan1:1)	172.29.9.177/24	IPv6 (IF 2)	Not assigned
PTP IPv4 (Slot: MRI2)	192.168.100.10/24	PTP IPv6 (Slot: MRI2)	Not assigned
PTP IPv4 (Slot: IO5)	192.168.100.11/24	PTP IPv6 (Slot: IO5)	Not assigned
- Receiver Information:**

MRS Status	sync to GPS	Receiver information	sync; 51.9823 9.2258 170m; 9/9SVs; normal operation
MRS Status	sync to GGR	Receiver information	sync to GGR; 51.9823 9.2258 169m; GPS: 9/13SVs, GLONASS: 0/6SVs
SHS Status	Redundant Mode (Diff= +0.0ns)	RSC Information	Automatic Mode (Selected Refclock: CLK2)
- NTP Information:**

NTP Status	Offs. 0us	Date/Time	UTC 08:20:04 Mon, 06/22/2015
------------	-----------	-----------	------------------------------
- PTP Information:**

Port State 1 (Slot: MRI2)	SLAVE	PTP Mode 1 (Slot: MRI2)	Multicast Slave
Port State 2 (Slot: IO5)	MASTER	PTP Mode 2 (Slot: IO5)	Multicast Master
- Last messages:**

```

2015-06-21 15:27:20 UTC: LANTIME -> Fan OK [Fan Module: 1 ]
2015-06-19 08:40:08 UTC: LANTIME -> Oscillator Adjusted [CLK: 1 ]
2015-06-19 08:21:37 UTC: LANTIME -> Normal Operation
2015-06-19 08:21:35 UTC: LANTIME -> CLK1 Sync
2015-06-19 08:21:15 UTC: LANTIME -> XMR Reference Detected [Reference Source: 1 (CLK1 GPS)]
2015-06-19 08:21:15 UTC: LANTIME -> XMR Reference Changed [Reference Source: 1 (CLK1 new source GPS(0))]
2015-06-19 08:21:04 UTC: LANTIME -> GPS Normal Operation
2015-06-19 08:21:04 UTC: LANTIME -> Antenna Reconnect [CLK: 1 ]
2015-06-19 07:18:19 UTC: LANTIME -> XMR Reference Detected [Reference Source: 17 (CLK2 PPS(5)3)]
2015-06-19 07:17:15 UTC: LANTIME -> XMR Reference Disconnected [Reference Source: 17 (CLK2 PPS(5)3)]
2015-06-19 08:29:15 UTC: LANTIME -> XMR Reference Detected [Reference Source: 17 (CLK2 PPS(5)3)]
2015-06-19 08:28:24 UTC: LANTIME -> XMR Reference Detected [Reference Source: 16 (CLK2 PPS(5)2)]

```

The WEB Interface

The web interface can be used by more than one user in parallel, but the two or more running sessions may influence each other. We explicitly do not recommend the parallel usage of the configuration interfaces.

Connect to the web interface by entering the following address into the address field of your web browser: <http://198.168.10.10> (You need to replace 198.168.10.10 with the IP address of your LANTIME).

Default Login

User: root
Password: timeserver

13 The WEB Interface

Connect to the web interface by entering the IP address of the corresponding time server into the address field of your web browser:

13.1 Configuration: Main Menu

The screenshot shows the LANTIME Web Interface Main Menu. The page is titled "LANTIME - Main Menu" and contains several sections of information:

- General Information:**

LANTIME	M3000/REDUNDANT (ELX)	Serial Number	000012323432
Contact	Unconfigured (Configure Now)	Location	Unconfigured (Configure Now)
Uptime	4 days, 17:22		
- Network Information:**

Hostname	lt-udo	Domain	
LAN IPv4 (IF 1 - lan0:0)	172.16.100.250/16	IPv6 (IF 1)	Not assigned
LAN IPv4 (IF 2 - lan1:1)	172.29.9.177/24	IPv6 (IF 2)	Not assigned
PTP IPv4 (Slot: MRI2)	192.168.100.10/24	PTP IPv6 (Slot: MRI2)	Not assigned
PTP IPv4 (Slot: IO5)	192.168.100.11/24	PTP IPv6 (Slot: IO5)	Not assigned
- Receiver Information:**

MRS Status	sync to GPS	Receiver information	sync; 51.9823 9.2258 170m; 9/9SVs; normal operation
MRS Status	sync to GGR	Receiver information	sync to GGR; 51.9823 9.2258 169m; GPS: 9/13SVs, GLONASS: 0/6SVs
SHS Status	Redundant Mode (Diff= +0.0ns)	RSC Information	Automatic Mode (Selected Refclock: CLK2)
- NTP Information:**

NTP Status	Offs. 0us	Date/Time	UTC 08:20:04 Mon, 06/22/2015
------------	-----------	-----------	------------------------------
- PTP Information:**

Port State 1 (Slot: MRI2)	SLAVE	PTP Mode 1 (Slot: MRI2)	Multicast Slave
Port State 2 (Slot: IO5)	MASTER	PTP Mode 2 (Slot: IO5)	Multicast Master
- Last messages:**

```

2015-06-21 15:27:20 UTC: LANTIME -> Fan OK [Fan Module: 1 ]
2015-06-19 08:40:08 UTC: LANTIME -> Oscillator Adjusted [CLK: 1 ]
2015-06-19 08:21:37 UTC: LANTIME -> Normal Operation
2015-06-19 08:21:35 UTC: LANTIME -> CLK1 Sync
2015-06-19 08:21:15 UTC: LANTIME -> XMR Reference Detected [Reference Source: 1 (CLK1 GPS)]
2015-06-19 08:21:15 UTC: LANTIME -> XMR Reference Changed [Reference Source: 1 (CLK1 new source GPS(0|0))]
2015-06-19 08:21:04 UTC: LANTIME -> GPS Normal Operation
2015-06-19 08:21:04 UTC: LANTIME -> Antenna Reconnect (CLK: 1 )
2015-06-19 07:18:19 UTC: LANTIME -> XMR Reference Detected [Reference Source: 17 (CLK2 PPS(5|3))]
2015-06-19 07:17:15 UTC: LANTIME -> XMR Reference Disconnected [Reference Source: 17 (CLK2 PPS(5|3))]
2015-06-18 08:29:15 UTC: LANTIME -> XMR Reference Detected [Reference Source: 17 (CLK2 PPS(5|3))]
2015-06-18 08:28:24 UTC: LANTIME -> XMR Reference Detected [Reference Source: 16 (CLK2 PPS(5|2))]

```

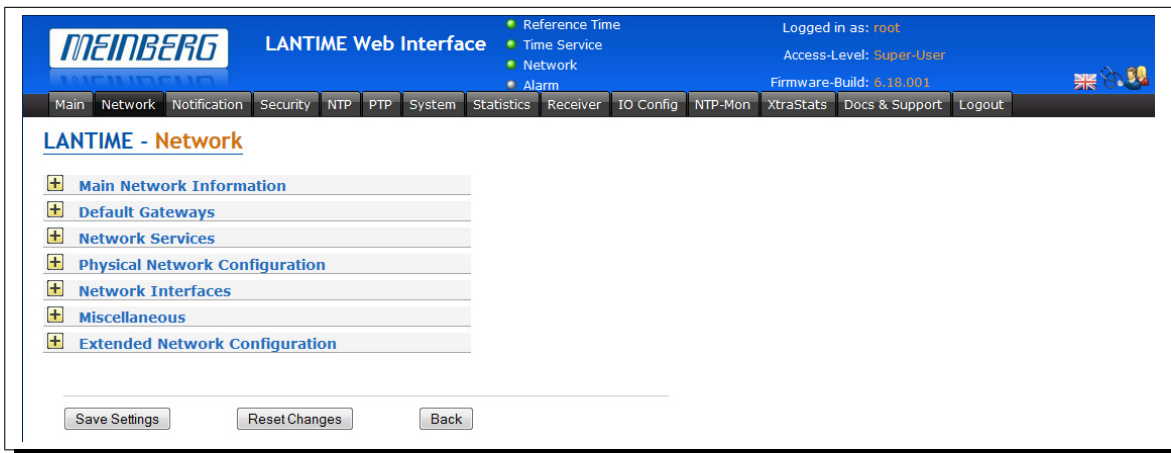
After entering the right password, the main menu page shows up. This page contains an overview of the most important configuration and status parameters for the system.

- Information about LANTIME model and software
- Network information
- Receiver status
- NTP status
- PTP status (option)
- Last messages
- Statistics (NTP/MRS Performance, NTP Access ...)
- Extended Statistics (MRS - external reference input signals)
- Documentation (Manuals), support information

The field in the lower section shows the last messages of the system with a timestamp added. The newest messages are on top of the list. This is the content of the file `/var/log/messages`, which is created after every start of the system (and is lost after a power off or reboot).

By using the navigation on top of the page you can reach a number of configuration menus, which are described in the following chapters.

13.2 Configuration: Network



In the network configuration all parameters related to the network interfaces can be changed. In the first section you can edit the hostname and domain name. You can also specify two nameserver - in the nameserver field you may enter an IPv4 or IPv6 address.

13.2.1 Network interface specific configuration

Standard Gateways:



In this Subsection you can enter a Default Gateway for IPv4 and IPv6

Network Services

Service	NTP	HTTP	HTTPS	TELNET	SSH	SNMP	FTP	TIME	DAYTIME	FPC	WEBSHELL
Interface 01:	<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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Interface 02:	<input checked="" 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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Interface 03:	<input checked="" 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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Interface 04:	<input checked="" 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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Interface 05:	<input checked="" 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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Current Status:											

In the second section the possible network protocols and access methods can be configured. You can enable/disable NTP, HTTP, HTTPS, TELNET, SSH, SNMP, FTP, TIME, DAYTIME, FPC and WEBSHELL by checking/unchecking the appropriate check boxes. After you saved your settings with the "Save Settings" button, all these subsystems are stopped and eventually restarted (if they are enabled).

Physical Network Configuration

The screenshot shows a configuration window titled "Physical Network Configuration". It contains a table with two columns for network interfaces: LAN0 and LAN1. The settings for each interface are as follows:

Interface	LAN0	LAN1
Net Link Mode	AUTO	AUTO
Indicate Link on Front Panel LED	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Bonding	Single Connection	Single Connection
IPv6 Mode	Deactivated	Deactivated
MAC Address	00:13:95:0a:c2:c2	00:13:95:0a:c2:c2
Assigned Virtual Interfaces	01	02

A dropdown menu is open for the LAN1 Net Link Mode, showing the following options: AUTO, 10 MBIT HALF DUPLEX, 10 MBIT FULL DUPLEX, 100 MBIT HALF DUPLEX, 100 MBIT FULL DUPLEX, 1000 MBIT HALF DUPLEX, and 1000 MBIT FULL DUPLEX.

The "Net Link Mode" controls the port speed and duplex mode of the selected Ethernet port. Under normal circumstances, you should leave the default setting (AUTO) untouched, until your network administrator tells you to change it.

Possible values are:

AUTO Autonegotiation or Autosensing – the link mode is set up automatically..

10 MBIT HALF DUPLEX Transmission of information in both direction of the channel –
 100 MBIT HALF DUPLEX but not at the same time, only alternate.
 1000 MBIT HALF DUPLEX

10 MBIT FULL DUPLEX The simultaneous transmission of data in both directions is possible
 100 MBIT FULL DUPLEX in Full Duplex mode.
 1000 MBIT FULL DUPLEX

Further configurations:

With the checkbox you can activate the Network LED at the front panel of your LANTIME for the corresponding physical network interface and you can activate/deactivate IPv6 mode in the drop down list.

Network Interfaces:

Here you can edit/select parameters for IPv4 and IPv6. In this version the IPv4 protocol is mandatory and cannot be disabled, but as a workaround a standalone IPv6 mode can be achieved by entering an IPv4 address "0.0.0.0" and disabling the DHCP client option for every network interface of your LANTIME. By doing so, you ensure that the timeserver cannot be reached with IPv4. Please note that TELNET and FTP cannot be used over IPv6 in this version. It is no problem to use IPv4 and IPv6 in a mixed mode environment on your LANTIME.

For each physical network interface you find a separate submenu after first start of the device. The parameters of the interfaces are editable with the context menu (see chapter "IPv4 addresses and DHCP").

Network Interfaces

Add Interface

Interface 01: IPv4 IPv6 Misc VLAN Cluster

IPv4:

TCP/IP address

Netmask

Enable DHCP-Client

IP-Address from DHCP 172.16.100.167

Netmask from DHCP 255.255.0.0

Broadcast from DHCP 172.16.255.255

Gateway from DHCP 172.16.3.1

DNS from DHCP 172.16.3.1

Domain from DHCP py.meinberg.de

Interface 02: IPv4 IPv6 Misc VLAN Cluster

Interface 03: IPv4 IPv6 Misc VLAN Cluster

Interface 04: IPv4 IPv6 Misc VLAN Cluster

Interface 05: IPv4 IPv6 Misc VLAN Cluster

NTP Cluster

To enable NTP redundancy for network clients, which can only communicate with one time server, multiple time servers can be assigned to a cluster.

For this purpose, the selected interfaces of the involved time servers are assigned to a common cluster-IP. The NTP-clients can send their NTP-requests to this cluster-IP. The current master sends its NTP packets via this IP to the clients.

Network Interfaces

Add Interface

Interface 01 - lan0:0 IPv4 IPv6 Misc VLAN Cluster

Cluster:

Enable Cluster Option

TCP/IP address 172.28.22.16

Netmask 255.255.0.0.000

Priority 0

Cluster Status:

Mode LISTENING (Reconfiguration in progress: SLAVE=>MASTER)

Interface 02 - lan1:1 IPv4 IPv6 Misc VLAN Cluster

In our example, we will choose the virtual port 01 (assigned to the physical interface LAN 0 of this time server) as cluster port. The cluster tag of this interface is selected and the corresponding fields are filled with the cluster-IP and subnet-mask, as shown in the dialog screen above.

The same cluster IP configuration is entered on all involved NTP servers in the cluster. If you want to set the priority of a particular server as master, then the priority value in the list must be set to a smaller value than the value of the other servers in the cluster.

The MASTER server is chosen according to parameters in the following order:

1. NTP status (sync, not sync);
2. Priority (user configurable, the lower value the higher priority, default value is 0)
3. Ref Clock Type - GNSS receiver has the highest rating
4. Ref Clock Status (sync, not sync)

Extended Network Configuration

With the submenu "Extended Network Configuration" you can configure additional network parameter like special network routes or alias definitions. For this you will edit a script file which will be activated every time after the network configuration will run.

Edit Additional Network Configuration:

```
#!/bin/bash
#Example how to setup an additional route
#route add -net 172.16.6.0 netmask 255.255.255.0 eth0
```

13.2.2 IPv4 addresses and DHCP

IPv4 addresses are built of 32 bits, which are grouped in four octets, each containing 8 bits. You can specify an IP address in this mask by entering four decimal numbers, separated by a point “.”.

Example: 192.168.10.2

Additionally you can specify the IPv4 netmask and your default gateway address. Please contact your network administrator, who can provide you with the settings suitable for your specific network.

If there is a DHCP (Dynamic Host Configuration Protocol) server available in your network, the LANTIME system can obtain its IPv4 settings automatically from this server. If you want to use this feature (again, you should ask your network administrator whether this is applicable in your network), you can change the DHCP Client parameter to “ENABLED”. In order to activate the DHCP client functionality, you can also enter the IP address “000.000.000.000” in the LCD menu by using the front panel buttons of the LANTIME. Using DHCP is the default factory setting.

The MAC address of your timeserver can be read in the LCD menu by pressing the NEXT button on the front panel twice. This value is often needed by the network administrator when setting up the DHCP parameters for your LANTIME at the DHCP server.

The screenshot displays the 'Network Interfaces' configuration page. At the top, there is a 'Network Interfaces' header with a small German flag icon. Below it is an 'Add Interface' button. The main content area shows five interface configurations, each with a header and a set of tabs: 'Interface 01:', 'Interface 02:', 'Interface 03:', 'Interface 04:', and 'Interface 05:'. Each interface has tabs for 'IPv4', 'IPv6', 'Misc', 'VLAN', and 'Cluster'. The 'IPv4' tab for 'Interface 01:' is selected, revealing the following settings:

- TCP/IP address: [Empty text box]
- Netmask: [Empty text box]
- Enable DHCP-Client:
- IP-Address from DHCP: 172.16.100.167
- Netmask from DHCP: 255.255.0.0
- Broadcast from DHCP: 172.16.255.255
- Gateway from DHCP: 172.16.3.1
- DNS from DHCP: 172.16.3.1
- Domain from DHCP: py.meinberg.de

If the DHCP client has been activated, the automatically obtained parameters are shown in the appropriate fields (IPv4 address, netmask, gateway).

13.2.3 IPv6 addresses and autoconf

You can specify up to three IPv6 addresses for your LANTIME timeserver. Additionally you can switch off the IPv6 autoconf feature. IPv6 addresses are 128 bits in length and written as a chain of 16bit numbers in hexadecimal notation, separated with colons. A sequence of zeros can be substituted with "::" once.

Examples:

"::" is the address, which simply consists of zeros
 ":::1" is the address, which only consists of zeros and a 1 as the last bit. This is the so-called host local address of IPv6 and is the equivalent to 127.0.0.1 in the IPv4 world

"fe80::0211:22FF:FE33:4455" is a typical so-called link local address, because it uses the "fe80" prefix.

In URLs the colon interferes with the port section, therefore IPv6-IP-addresses are written in brackets in an URL.
 ("http://[1080::8:800:200C:417A]:80/" ;
 the last ":80" simply sets the port to 80, the default http port)

The screenshot shows the configuration page for 'Interface 01'. The 'IPv6' tab is selected. Under the 'IPv6:' section, there are four fields:

- TCP/IP address:** An empty text input field.
- Enable DHCP-Client:** A checkbox that is currently unchecked.
- IP by Router Advertisement:** A text input field containing the value '3fe:302:11:2:213:95ff:fe02:c2fa/64'.
- Link Local:** A text input field containing the value 'fe80::213:95ff:fe02:c2fa/64'.

Below this section, the 'Interface 02:' configuration area is visible, with tabs for IPv4, IPv6, Misc, VLAN, and Cluster.

If you enabled the IPv6 protocol, the LANTIME always gets a link local address in the format "fe80: ...", which is based upon the MAC address of the interface. If a IPv6 router advertiser is available in your network and if you enabled the IPv6 autoconf feature, your LANTIME will be set up with up to three link global addresses automatically.

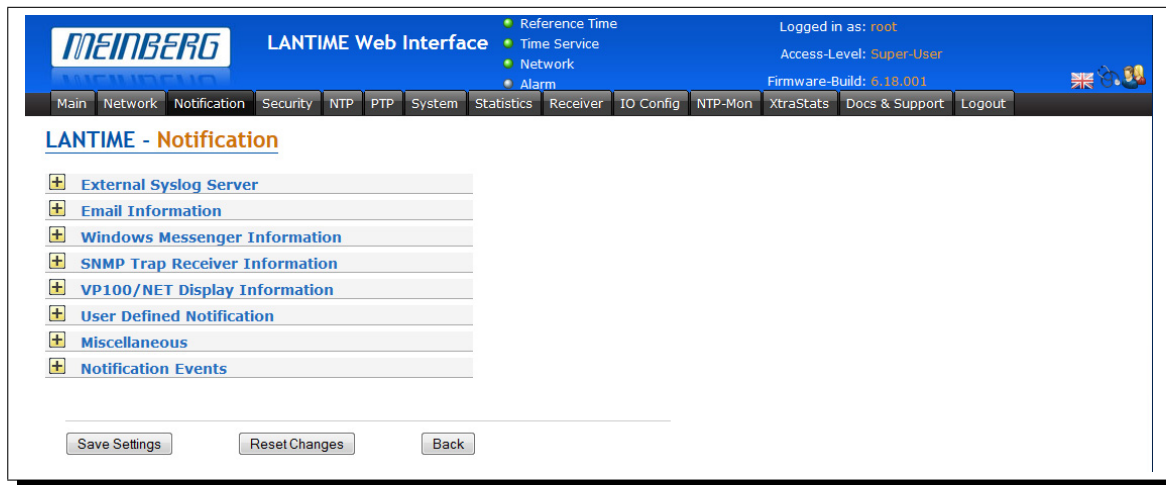
13.2.4 High Availability Bonding

The standard moniker for this technology is IEEE 802.3ad, although it is known by the common names of trunking, port trunking, teaming and link aggregation. The conventional use of bonding under Linux is an implementation of this link aggregation.

Interface	LAN0	LAN1	LAN2
Net Link Mode	100 MBIT FULL DUPLEX	AUTO	AUTO
Indicate Link on Front Panel LED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bonding	Single Connection	Single Connection	Single Connection
IPv6 Mode	Single Connection	Deactivated	Deactivated
MAC Address	Assigned to Group 1	00:60:6e:7b:e1:66	00:60:6e:7b:e1:67
Assigned Virtual Interfaces	Assigned to Group 2		
	Assigned to Group 3		
	Assigned to Group 4		
	Assigned to Group 5		

Only one link is used at any given time. At least two physical Ethernet ports must be linked to one bonding group to activate this feature. The first Ethernet Port in one bonding group provides the IP-Address and the net mask of this new virtual device. The implementation of the LANTIME Bonding feature will not replace the MAC address of the active ethernet port. Depending on the LINK state of the ETH-port the IP address of the first port in the bonding group will be set to the next ethernet port. All services will be restarted automatically.

13.3 Configuration: Notification



13.3.1 SYSLOG Server

All information written to the LANTIME SYSLOG (/var/log/messages) can be forwarded to one or two remote SYSLOG servers. The SYSLOG daemon of this remote SYSLOG needs to be configured to allow remote systems to create entries. A Linux SYSLOGD can be told to do so by using the command “syslogd -r” when starting the daemon.

If you enter nothing in the SYSLOG server fields or specify 0.0.0 as the SYSLOG servers addresses, the remote SYSLOG service is not used on your LANTIME.

Please be aware of the fact that all SYSLOG entries of the timeserver are stored in /var/log/messages and will be deleted when you power off or reboot the timeserver. A daily CRON job is checking for the size of the LANTIME SYSLOG and deletes it automatically, if the log size is exceeding a certain limit.

By specifying one or two remote SYSLOG servers, you can preserve the SYSLOG information even when you need to reboot or switch off the LANTIME.

13.3.2 E-mail messages

You can specify the e-mail address which is used as the senders address of the notification e-mail (From: address), the e-mail address of the receiver (To: address) and a SMTP smarthost, that is a mail server forwarding your mail to the receiver's mail server. If your LANTIME system is connected to the internet, it can deliver those e-mails itself by directly connecting to the receivers mail server. Additional e-mail addresses can be specified via the CC-recipients button.

The screenshot shows the 'Email Information' configuration page. It features several input fields and a checkbox:

- Recipient**: A text input field.
- Sender**: A text input field.
- Smarthost**: A text input field.
- Port**: A text input field containing the value '25'.
- Enable Authentication**: A checkbox that is currently unchecked.
- User**: A text input field.
- Password**: A text input field.
- Additional Email Recipient**: A text input field with an **Add** button next to it.

At the bottom of the form, there are two tabs: **Additional Email Recipients** and **Options**. The **Additional Email Recipients** tab is active, showing a blue bar with the text: **Currently no additional Email recipients configured**.

These settings cannot be altered with the LC display buttons of the front panel. Please note the following:

- The host name and domain name should be known to the SMTP smarthost
- A valid nameserver entry is needed
- The domain part of the "From:" address has to be valid

13.3.3 Windows Messenger Information

The screenshot shows the 'Windows Messenger Information' configuration page. It features two input fields:

- Mail Address 1**: A text input field.
- Mail Address 2**: A text input field.

13.3.4 SNMP-TRAP messages

SNMP Trap Receiver Information

SNMP Trap Receiver 1 Community
 Version (dropdown menu showing SNMP v1, v2, v3)

SNMP Trap Receiver 2 Community
 Version

SNMP Trap Receiver 3 Community
 Version

SNMP Trap Receiver 4 Community
 Version

Up to four independent SNMP trap receiver hosts can be configured in this subsection, you may use IPv4 or IPv6 addresses or specify a hostname. Additionally you have to enter a valid SNMP community string for your trap receiving community. These can be unrelated to the SNMP community strings used for status monitoring and configuration access (see SNMP configuration on the “Security” page).

13.3.5 VP100/NET wall mount display

The VP100/NET wall display is an optional accessory for the LANTIME timeserver, it has an own integrated Ethernet port (10/100 Mbit) and a SNTP client. The time for the display can be received from any NTP server using the SNTP protocol (like your LANTIME), additionally the display is capable of showing text messages, which are sent by using a special utility. The LANTIME can send an alarm message to one or two VP100/NET displays over the network, whenever an event occurs for which you selected the display notification type. If this happens, a scrolling alarm message is shown three times on the display.

Just enter the display’s IP address and its serial number (this is used for authorisation), which can be found by pressing the SET button on the back of the display four times. The serial number consists of 8 characters, representing four bytes in hexadecimal notation.

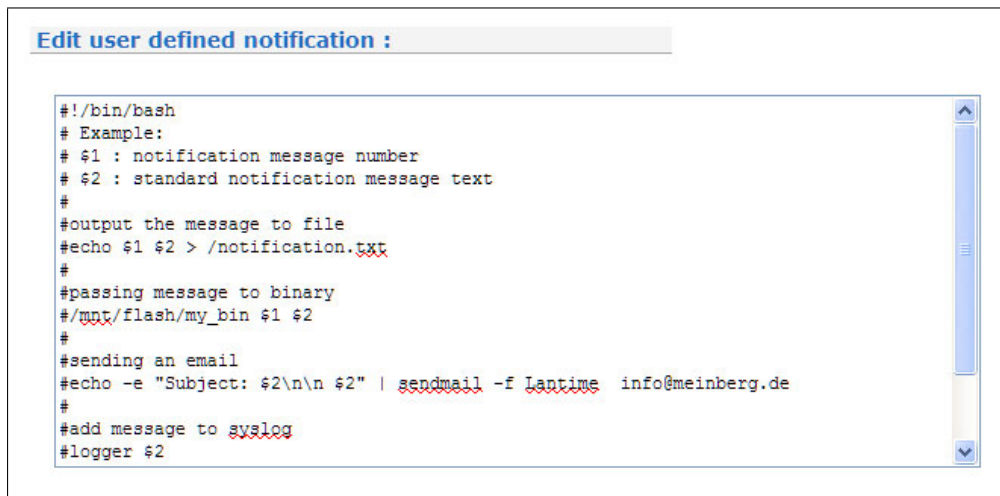
VP100/NET Display Information

Display 1 Serial Number
 Display 2 Serial Number

If you want to use the display for other purposes, you can send text messages to it by using our command line tool `send2display`, which can be found on the LANTIME. This allows you to use the display by CRON jobs or your own shell scripts etc. If you run the tool without parameters, a short usage screen is shown, explaining all parameters it may understand. See appendix for a printout of this usage screen.

13.3.6 User defined Alarm scripts

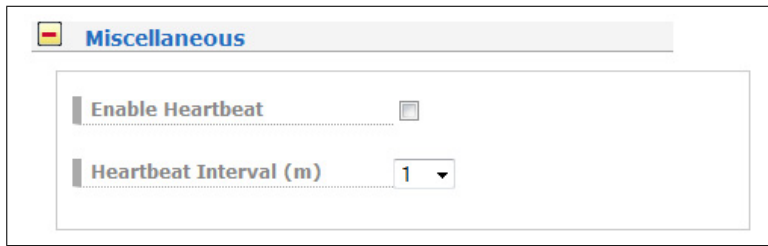
You can define your own alarm script for every event by using the “Edit user defined notification script”. This script will be called automatically if one of the selected events occurs.



```
#!/bin/bash
# Example:
# $1 : notification message number
# $2 : standard notification message text
#
#output the message to file
#echo $1 $2 > /notification.txt
#
#passing message to binary
#/mnt/flash/my_bin $1 $2
#
#sending an email
#echo -e "Subject: $2\n\n $2" | sendmail -f lantime info@meinberg.de
#
#add message to syslog
#logger $2
```

This user alarm script will be stored on the Flash-Disk at “/mnt/flash/user_defined_notification”. This script will be called with index and the alarm message as text. The index value of the test message is 0.

13.3.7 Miscellaneous



The image shows a configuration window titled "Miscellaneous". Inside the window, there are two settings:

- Enable Heartbeat**: A checkbox that is currently unchecked.
- Heartbeat Interval (m)**: A dropdown menu currently set to "1".

A heartbeat is a periodic signal generated by hardware or software to indicate normal operation or to synchronize other parts of a system. Usually a heartbeat is sent between machines at a regular interval on the order of seconds. If a heartbeat isn't received for a time - usually a few heartbeat intervals - the machine that should have sent the heartbeat is assumed to have failed.

13.3.8 Alarm events

Notification Events

Event	Status	Triggers								
		EMAIL	WMAIL	SNMP	DISP	USER	ALED	RELAY		
NORMAL OPERATION	since 22h 02m 01s	<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 checked="" type="checkbox"/>
NTP NOT SYNC		<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 checked="" type="checkbox"/>
NTP SYNC	since 22h 02m 59s	<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 checked="" type="checkbox"/>
NTP STOPPED		<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 checked="" type="checkbox"/>
SYSTEM REBOOT	Last: Wed Oct 15 10:25:52 2014	<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 checked="" type="checkbox"/>
1. REFCLOCK NOT RESPONDING		<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 checked="" type="checkbox"/>
1. REFCLOCK NOT SYNC	Last: Wed Mar 16 00:02:09 2011	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1. REFCLOCK SYNC	since 22h 03m 01s	<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 checked="" type="checkbox"/>
ANTENNA FAULTY		<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 checked="" type="checkbox"/>
ANTENNA RECONNECT	since 22h 03m 02s	<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 checked="" type="checkbox"/>
ANTENNA SHORT CIRCUIT		<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 checked="" type="checkbox"/>
DEVICE CONFIGURATION CHANGED	Last: Wed Oct 15 10:27:06 2014	<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 checked="" type="checkbox"/>
LEAP SECOND ANNOUNCED		<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 checked="" type="checkbox"/>
POWER SUPPLY FAILURE		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
POWER SUPPLY OK	since 22h 03m 04s	<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 checked="" type="checkbox"/>
NTP CLIENT LIMIT EXCEEDED		<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 checked="" type="checkbox"/>
NETWORK LINK DOWN	Last: Wed Mar 16 00:02:07 2011	<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 checked="" type="checkbox"/>
NETWORK LINK UP	since 22h 02m 05s	<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 checked="" type="checkbox"/>
LOW SYSTEM RESSOURCES		<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 checked="" type="checkbox"/>
SUFFICIENT SYSTEM RESSOURCES		<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 checked="" type="checkbox"/>
CERTIFICATE EXPIRED		<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 checked="" type="checkbox"/>
OSCILLATOR ADJUSTED	since 21h 59m 57s	<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 checked="" type="checkbox"/>
OSCILLATOR NOT ADJUSTED	Last: Wed Oct 15 10:26:53 2014	<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 checked="" type="checkbox"/>
CLUSTER MASTER CHANGED		<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 checked="" type="checkbox"/>
CLUSTER FALSETICKER DETECTED		<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 checked="" type="checkbox"/>
CLUSTER FALSETICKER CLEARED		<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 checked="" type="checkbox"/>

Autorepeat Event Never

Max. Number of Repetition 0

On this page you can set up different notification types for a number of events. This is an important feature because of the nature of a timeserver: running unobserved in the background. If an error or problem occurs, the timeserver is able to notify an administrator by using a number of different notification types.

The LANTIME timeserver offers different ways of informing the administrator or a responsible person about nine different events: EMAIL sends an e-mail message to a specified e-mail account, SNMP-TRAP sends a SNMP trap to one or two SNMP trap receivers, WINDOWS POPUP MESSAGE sends a winpopup message to one or two different computers. DISPLAY shows the alarm message on a wall mount display model VP100/NET, which is an optional accessory you can obtain for your LANTIME. You also can use user defined scripts (read section "User defined Alarm scripts") and the error relay out.

Attention: mbgLtTrapNormalOperation clears everything! It is a master trap to show that the LANTIME is running in full state!

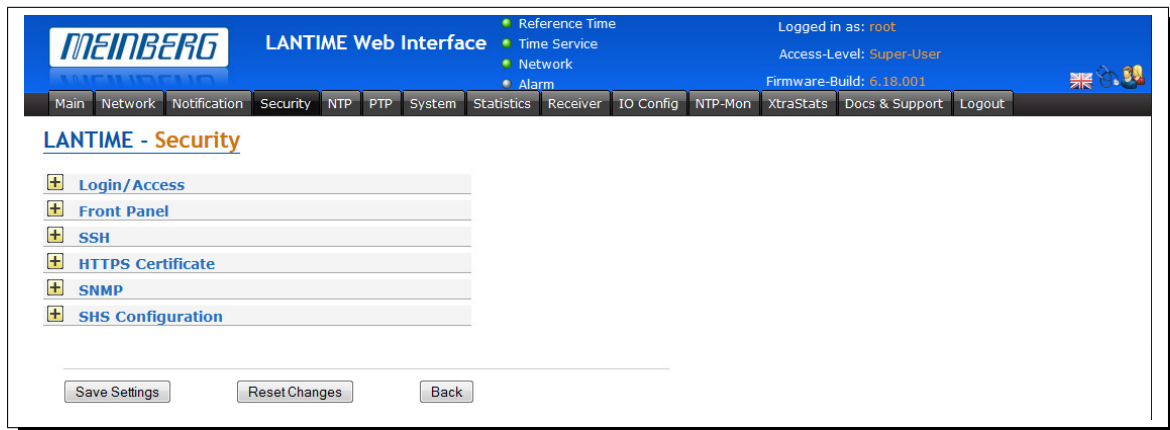
Trapname	Cleared By
NTPStopped	NTPNotSync or NTP Sync
NTPNotSync	NTPSync
ReceiverNotResponding	ReceiverNotSync or ReceiverSync
ReceiverNotSync	ReceiverSync
AntennaFaulty	AntennaReconnect
SecondaryRecNotSync	SecondaryRecSync
PowerSupplyFailure	PowerSupplyUp
NetworkDown	NetworkUp
SecondaryRecNotResp	RecNotSync or RecSync

The following traps are notifications that do not have a "clearing" trap:

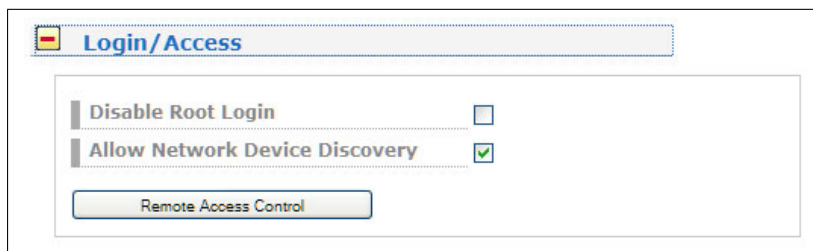
- mbgLtTrapConfigChanged
- mbgLtTrapLeapSecondAnnounced
- mbgLtTrapServerBoot

Every event can use a combination of those four notification types, of course you can disable notification for an event (by just disabling all notification types for this event). The configuration of the four notification types can be changed in the upper section of the page, you can control which notification is used for which event in the lower part of the page.

13.4 Configuration: Security



13.4.1 HTTP Access Control



With this function you can restrict the access to the web interface and allow only a few hosts to login. Only the hosts you entered in the list are able to login to the HTTP/HTTPS server of your LANTIME.

13.4.2 Front Panel



With the checkboxes the frontpanel and USB port of the LANTIME can be locked.

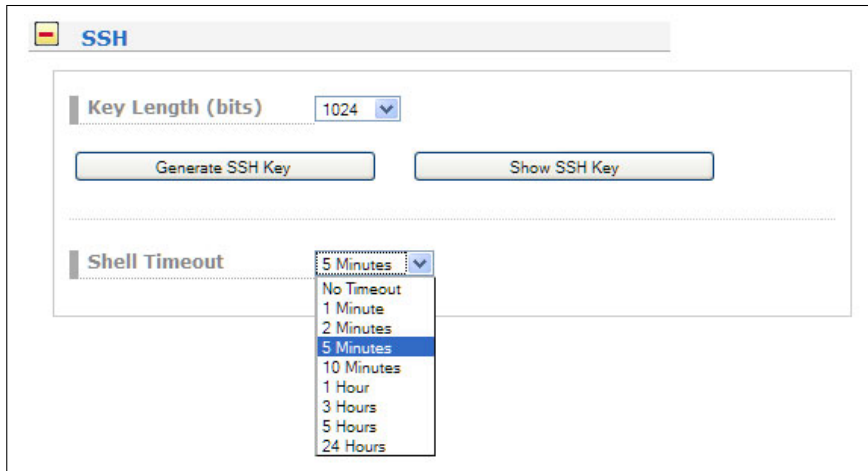
13.4.3 SSH Secure Shell Login

The SSH provides you with a secure shell access to your timeserver. The connection is encrypted, so no readable passwords are transmitted over your network. The actual LANTIME version supports SSH1 and SSH2 over IPv4 and IPv6. In order to use this feature, you have to enable the SSHD subsystem and a security key has to be generated on the timeserver by using the "Generate SSH key" button. Afterwards, a SSH client can connect to the timeserver and opens a secure shell: `ssh root @ 192.168.16.111`

The first time you connect to a SSH server with an unknown certificate, you have to accept the certificate, afterwards you are prompted for your password (which is configured in the first section of this page).

Default Password: timeserver

If you generate a new SSH key, you can copy and paste it into your SSH client configuration afterwards in order to allow you to login without being prompted for a password. We strongly recommend to use SSH for shell access, TELNET is a very insecure protocol (transmitting passwords in plain text over your network).

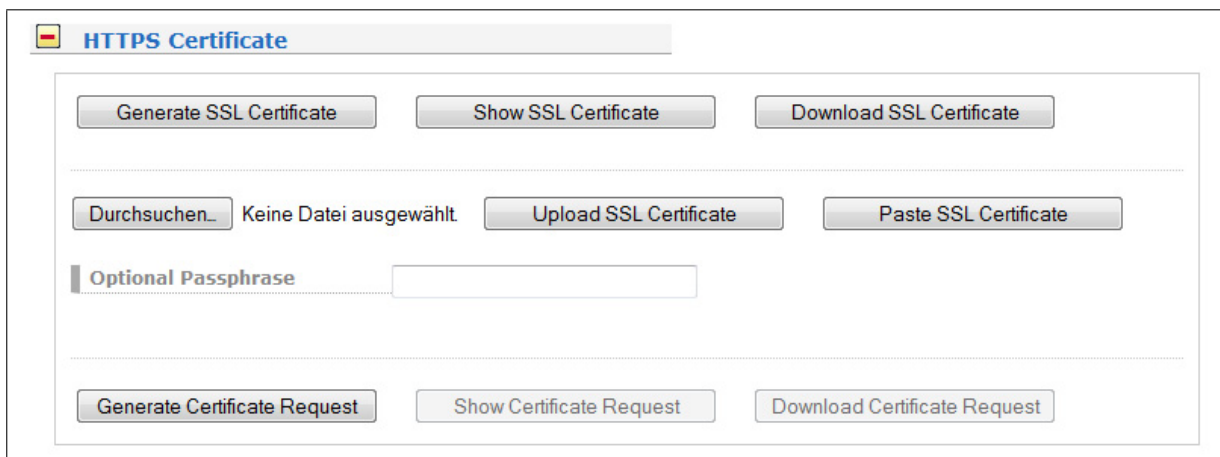


The screenshot shows the SSH configuration page. At the top, there is a 'Key Length (bits)' dropdown set to '1024'. Below it are two buttons: 'Generate SSH Key' and 'Show SSH Key'. Further down, the 'Shell Timeout' dropdown menu is open, displaying a list of options: '5 Minutes', 'No Timeout', '1 Minute', '2 Minutes', '5 Minutes' (which is highlighted in blue), '10 Minutes', '1 Hour', '3 Hours', '5 Hours', and '24 Hours'.

If you enabled SSH, your LANTIME automatically is able to use secure file transfer with SCP or SFTP protocol. The usage of FTP as a file transfer protocol is as insecure as using TELNET for shell access.

13.4.4 Generate SSL Certificate for HTTPS

HTTPS is the standard for encrypted transmission of data between web browser and web server. It relies on X.509 certificates and asymmetric crypto procedures. The timeserver uses these certificates to authenticate itself to the client (web browser). The first time a web browser connects to the HTTPS web server of your LANTIME, you are asked to accept the certificate of the web server. To make sure that you are talking to your known timeserver, check the certificate and accept it, if it matches the one stored on the LANTIME. All further connections are comparing the certificate with this one, which is saved in your web browser configuration. Afterwards you are prompted to verify the certificate only when it changed.



The screenshot shows the HTTPS Certificate configuration page. At the top, there are three buttons: 'Generate SSL Certificate', 'Show SSL Certificate', and 'Download SSL Certificate'. Below these, there is a 'Durchsuchen...' button followed by the text 'Keine Datei ausgewählt', and two more buttons: 'Upload SSL Certificate' and 'Paste SSL Certificate'. In the middle, there is an 'Optional Passphrase' label and an empty text input field. At the bottom, there are three buttons: 'Generate Certificate Request', 'Show Certificate Request', and 'Download Certificate Request'.

By using the button "Generate SSL certificate for HTTP" you can create a new certificate. Please enter your organisation, name, mail address and the location in the upcoming form and press "Generate SSL certificate" to finally generate it.

Generate SSL Certificate

Country Name (2 letter code)	<input type="text" value="DE"/>
Locality Name	<input type="text" value="BAD PYRMONT"/>
Organization Name	<input type="text" value="MEINBERG"/>
Organizational Unit	<input type="text" value="SOFTWARE"/>
Common Name	<input type="text" value="SWD"/>
Email Address	<input type="text" value="info@meinberg.de"/>

After the successful generation of the certificate and with the button "SSL..." the certificate is shown to you in the textarea:

Show SSL Certificate:

```

Certificate information:
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      d1:78:76:50:88:da:c6:83
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=DE, ST=Some-State, L=Bad Pyrmont, O=Meinberg Funkuhren GmbH & Co. KG, OU=Software
    Development, CN=Meinberg LANTIME/emailAddress=info@meinberg.de
    Validity
      Not Before: Nov  2 13:44:23 2010 GMT
      Not After : Oct 30 13:44:23 2020 GMT
    Subject: C=DE, ST=Some-State, L=Bad Pyrmont, O=Meinberg Funkuhren GmbH & Co. KG, OU=Software
    Development, CN=Meinberg LANTIME/emailAddress=info@meinberg.de
    Subject Public Key Info:

```

It is also possible to upload your own HTTPS certification. If you upload a non valid certification HTTPS will not work.

Uploading certified SSL Certificates

A certificate which is certified by a certification authority (CA) can be installed using the "Upload SSL Certificate" button. This certificate must be in PEM file format, it must contain a private key and the certificate itself.

The content of the private key starts with

"—BEGIN RSA PRIVATE KEY—"

and ends with

"—END RSA PRIVATE KEY—"

the certificate itself starts with

"—BEGIN CERTIFICATE—"

and ends with

"—END CERTIFICATE—".

This example is an excerpt from a PEM file:

```
---BEGIN RSA PRIVATE KEY---
MIICXQIBAAKBgQC6FkGxyJ6+Bqxyzfp3bNtEYyiRIAbQAIshblYPG7aQk+8XbIXWB
...
aiLbmu7N3TEdWVDgro8kMuQC/Ugkttx7TdJJbqJoVsF5
---END RSA PRIVATE KEY---
---BEGIN CERTIFICATE---
MIIEJTCCA46gAwIBAgIJANF4d1CI2saDMA0GCSqGSIb3DQEBBQUAMIG+MQswCQYD
...
ekZ970dAaPca
---END CERTIFICATE---
```

IMPORTANT: The certificate should not be protected with a password, otherwise the web server cannot start automatically.

Uploading certified Multi-Level / chained Certificates

Steps below require an SSH access to your timeserver.

In addition to SSL certificates, also multi-level / chained certificates are supported. In this case, a private key and a certificate chain are divided into two files, which are both in a PEM format. The actual PEM file contains the private key which is enclosed between BEGIN RSA PRIVATE KEY and END RSA PRIVATE KEY line as shown above. The CA-file on the other hand contains the certificate chain, where each single certificate is enclosed between BEGIN and END CERTIFICATE line as shown above.

The PEM file that contains the private key should be copied manually to `/etc/https.pem` and the CA to `/etc/https_cert.pem`.

Subsequently, the line `'ssl.ca-file = "/etc/https_cert.pem"'` should be added in a server configuration file `/etc/httpd.conf`.

Running the command `"saveconfig"` saves the settings persistently, the command `"restart https"` applies the settings.

Please Note: the certificates should not be protected with a password for the reasons stated above.

13.4.5 SNMP Parameter

In the last Section all parameters for SNMP can be configured. More information you can find in the chapter "SNMP Configuration" in this manual.

SNMP

General Information

SNMP Contact SNMP Location
Please edit these values on the system page (General Settings).

Number of Retries Timeout (seconds)

Activated Protocol Versions

V1 & V2C Parameter

Read Community Write Community

V3 Parameter

Security Name Security Level

Engine-ID

Rights

Authentication Protocol

Authentication Passphrase Re-Enter Passphrase

Privacy Protocol

Privacy Passphrase Re-Enter Passphrase

13.4.6 SHS Configuration

The screenshot displays the 'SHS Configuration' web interface. It features a title bar with a German flag icon and the text 'SHS Configuration'. Below the title bar, there are four configuration items:

- SHS-Mode**: A dropdown menu set to 'Disabled' with a help icon (question mark) to its right.
- Time Limit Warning Level (ms)**: A text input field containing the value '10'.
- Time Limit Critical Level (ms)**: A text input field containing the value '25'.
- Stop NTP Service on Time Limit Error**: A checkbox that is checked.

SHS Parameter

SHS is the abbreviation of Secure Hybrid Systems and is available on systems with two reference clocks. It provides a plausibility mode where the incoming times of both time signals are continuously compared against each other. Only if the time difference between those reference times does not exceed a certain limit (configurable) will it give over the time to the NTP service. Otherwise the time output is stopped immediately.

SHS-Mode

This parameter is used to activate the SHS feature and with it the comparison of time. If the SHS mode is disabled the times of both receivers are passed directly to the NTP service. The NTP service decides autonomously which reference time will be used. In case of the master reference time got unavailable the NTP service just switches over to the other time source.

Time Limit Warning Level(ms)

This value indicates at which calculated time difference between the two reference times an alarm is generated over the built-in notification system. The warning level indicates that the reference times are no longer equal and that a time error may be imminent. The NTP service is still receiving the time from the SHS system.

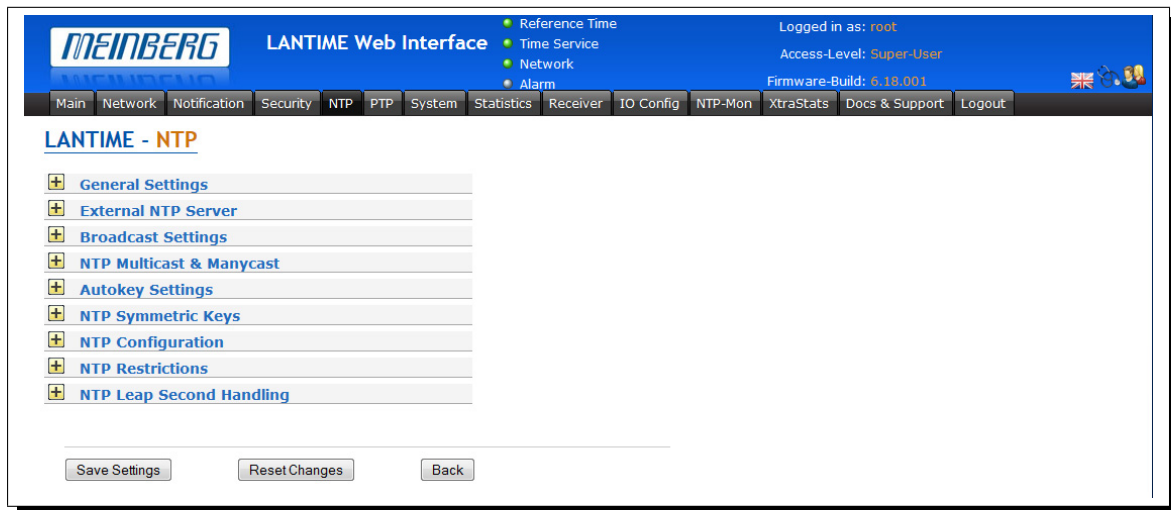
Time Limit Error Level(ms)

This value indicates at which difference the time output to NTP is stopped and an appropriate alarm is generated over the built-in notification system. If the SHS error was triggered an administrator action is needed to bring the NTP service back to normal operation. The administrator must check the times of both receiver and confirm that everything is ok. An appropriate dialog is shown on the web interface. After affirmation the handover of time to the NTP service is resumed and NTP will resynchronize.

Stop NTP Service on Time Limit Error

This parameter is used to decide whether the NTP service is stopped directly in case of a time limit error. In this case no NTP client gets an answer anymore from the time server.

13.5 Configuration: NTP



The NTP configuration page is used to set up the additional NTP parameters needed for a more specific configuration of the NTP subsystem.

13.5.1 General Settings

The “Local trusted key” field holds a list of all trusted symmetric keys (comma or space separated), which have to be accepted by the NTPD of your LANTIME.

13.5.2 External NTP Server

External NTP Server

External Server Address 1	<input type="text"/>	Symmetric Key	<input type="text"/>	Use Autokey	<input type="checkbox"/>
Minpoll	Default <input type="button" value="v"/> Seconds	Maxpoll	Default <input type="button" value="v"/> Seconds	Use iburst	<input type="checkbox"/>
...					
External Server Address 7	<input type="text"/>	Symmetric Key	<input type="text"/>	Use Autokey	<input type="checkbox"/>
Minpoll	Default <input type="button" value="v"/> Seconds	Maxpoll	Default <input type="button" value="v"/> Seconds	Use iburst	<input type="checkbox"/>

By using the NTP configuration page, a number of additional parameters can be added to this default `ntp.conf`. In the upper section up to seven external NTP servers can be set up to provide a high grade of redundancy for the internal reference clock. For each of these external NTP servers the AUTOKEY or symmetric key feature of NTP can be used to ensure the authentic of these time sources.

13.5.3 NTP Local Clock

The default configuration of the timeserver consists of a local clock, which represents the hardware clock of your LANTIME system and the reference clock. The local clock is only chosen as the NTP time reference after the receiver's clock lost its synchronisation. The stratum level of this local clock is set to 12, this ensures that clients recognise the switchover to the local clock and are able to eventually take further actions. The local clock can be disabled if the timeserver should not answer any more when the reference clock is out of order.

Because the reference clock is internally connected to the LANTIME system by using a serial connection, the accuracy using this way of synchronisation is around 1 ms. The high accuracy of the LANTIME timeserver (around 10 microseconds) is available by using the PPS (PulsePerSecond) of the reference clock (GPS), which is evaluated by the operating system. The default configuration looks like this:

```
# *** lantime ***
# NTP.CONF for GPS167 with UNI ERLANGEN

server 127.127.1.0          # local clock
fudge 127.127.1.0 stratum 12 # local stratum

server 127.127.8.0 mode 135 prefer# GPS167 UNI Erlangen PPS
fudge 127.127.8.0 time1 0.0042 # relative to PPS
server 127.127.22.0        # ATOM (PPS)
fudge 127.127.22.0 flag3 1 # enable PPS API
enable stats
statsdir /var/log/
statistics loopstats
driftfile /etc/ntp.drift

# Edit /mnt/flash/ntpconf.add to add additional NTP parameters
```

13.5.4 NTP Broadcast

If you want to use your LANTIME timeserver to send NTP broadcast packets to your network, you have to enter a valid broadcast address in "NTP broadcast address". If you want to use IPv6 multicast mode, you have to enter a valid IPv6 multicast address in this field. Please note that NTP Version 4, which is used by the LANTIME timeserver, only permits authenticated broadcast mode. Therefore you have to set up the AUTOKEY feature or a symmetric key if you use a NTPv4 client and want to broadcast / multicast your time. A sample configuration of the NTP client for broadcast with symmetric keys looks like:

```
broadcastclient yes
broadcastdelay 0.05 # depends on your network
keys /etc/ntp/keys
trustedkey 6 15
requestkey 15
controlkey 15
```

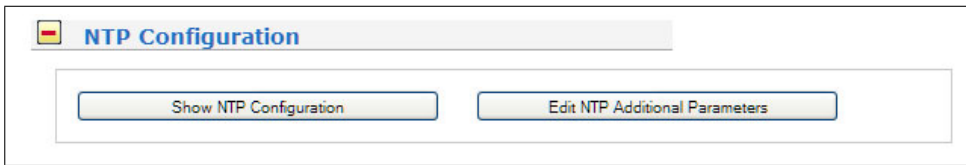
In the next section you can enable the AUTOKEY feature for your LANTIME timeserver and the PPS mode (which is enabled in default settings), see above for a description.

The NTP Trusttime will specify the time how long the NTP will trust the reference time if this is not synchronized (free running). This time will be set in seconds or minutes or hours. The value 0 will be select the default value for the specific reference clock. The default values are:

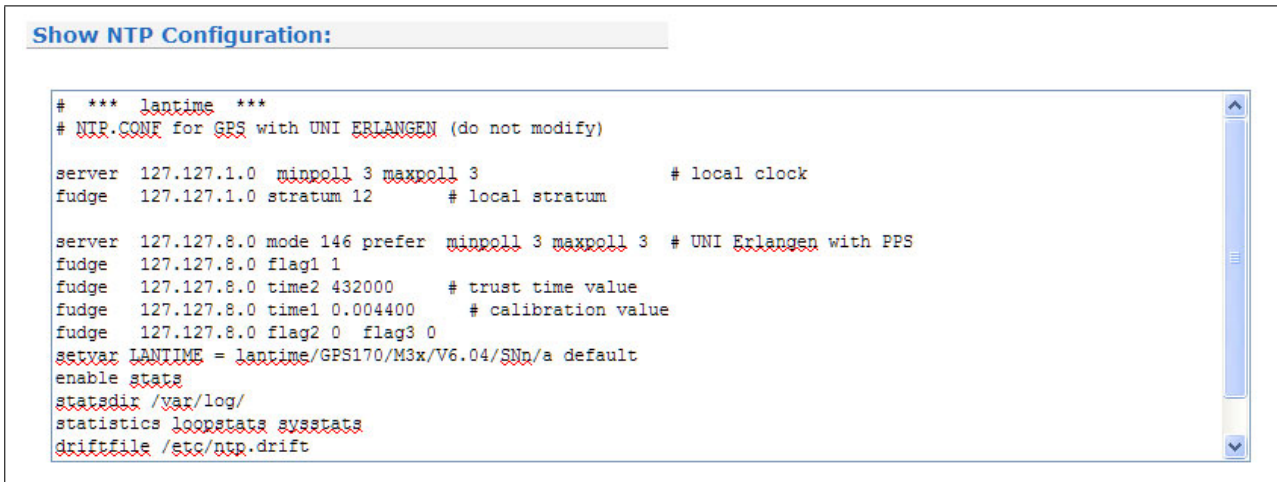
```
LANTIME/GPS:      96 h
LANTIME/PZF:      0,5 h
LANTIME/RDT:      0,5 h
LANTIME/MRS:      96 h
```

After each restart and after any change of configuration a new `/etc/ntp.conf` file is generated by the LANTIME software. Any changes you made to this file are lost. In order to use your custom `ntp.conf` (your LANTIME is using a standard version of the NTP software suite, therefore all configuration parameters of the NTP software are fully supported), you have to edit the file `/mnt/flash/ntpconf.add`, which is automatically appended to the `/etc/ntp.conf` file generated at boot time or when reloading configuration after a change. You can edit this file by using the button "Edit additional NTP parameter".

13.5.5 Show NTP Configuration



By choosing "Show NTP configuration", you can review the actual state of the `/etc/ntp.conf` file. The file cannot be changed on this page, see above for a description why editing this file is not reasonable.



The screenshot shows a window titled "Show NTP Configuration:" displaying the contents of the `/etc/ntp.conf` file. The text is as follows:

```
# *** lantime ***
# NTP.CONF for GPS with UNI ERLANGEN (do not modify)

server 127.127.1.0 minpoll 3 maxpoll 3          # local clock
fudge 127.127.1.0 stratum 12                # local stratum

server 127.127.8.0 mode 146 prefer minpoll 3 maxpoll 3 # UNI Erlangen with PPS
fudge 127.127.8.0 flag1 1
fudge 127.127.8.0 time2 432000             # trust time value
fudge 127.127.8.0 time1 0.004400          # calibration value
fudge 127.127.8.0 flag2 0 flag3 0
setvar LANTIME = lantime/GPS170/M3x/V6.04/SNp/a default
enable stats
statsdir /var/log/
statistics loopstats sysstats
driftfile /etc/ntp.drift
```

13.5.6 NTP Restrictions

With "Edit NTP Restrictions" you can allow access to specified NTP clients. Enter the IP address and the netmask as shown in the section below. All other IP address are invalid if an entry in the restriction list is made. Only the users from the list have NTP access on this time server.

The following lines are written automatically in the NTP configuration file:
#NTP RESTRICTION SECTION - LAST MODIFIED: Wed Jan 5 07:47:58 2011
restrict 0.0.0.0 mask 0.0.0.0 ignore # block IPv4 completely
restrict 127.0.0.1 mask 255.255.255.255# allow localhost
restrict ::0 ignore # block IPv6 completely

#USER DEFINED RESTRICTIONS
restrict 172.16.3.13 mask 255.255.255.255
restrict 172.16.5.0 mask 255.255.255.0

The address 172.16.3.13 and all IPs from the subnet 172.16.5.xx have access to all NTP services.

Add NTP Restrictions

IP Address	<input type="text"/>
Netmask	<input type="text"/>
<input type="button" value="Add Restriction"/>	

Current NTP Restrictions

Currently no NTP Restrictions saved.

13.5.7 NTP Authentication

NTP version 2 and version 3 support an authentication method using symmetric keys. If a packet is sent by the NTPD while using this authentication mode, every packet is provided with a 32 bit key ID and a cryptographic 64/128 bit checksum of the packet. This checksum is built with MD5 or DES, both algorithms offer a sufficient protection against manipulation of data.

Please note that the distribution of DES in the United States of America and Canada is subject to restrictions, while MD5 is not affected by that. With any of these algorithms the receiving NTP clients validate the checksum. Both parties (server and client) need to have the same crypto key with the same key ID.

In the authentication mode a party is marked “untrusted” and not suitable for synchronisation, whenever unauthorised packets or authorised packets with a wrong key are used. Please note that a server may recognise a lot of keys but uses only a few of them. This allows a timeserver to serve a client, who is demanding an authenticated time information, without “trusting” the client.

Some additional parameters are used to specify the key IDs used for validating the authentic of each partner. The configuration file `/etc/ntp.conf` of a server using this authentication mode may look like this:

```
# peer configuration for 128.100.100.7
# (expected to operate at stratum 2)
# fully authenticated this time

peer 128.100.49.105 key 22# suzuki.ccie.utoronto.ca
peer 128.8.10.1 key 4 # umd1.umd.edu
peer 192.35.82.50 key 6 # lilben.tn.cornell.edu

keys /mnt/flash/ntp.keys # path for key file
trustedkey 1 2 14 15 # define trusted keys
requestkey 15 # key (mode 6) for accessing server variables
controlkey 15 # key (mode 7) for accessing server variables
```

The “keys” parameter indicates the location of the file, in which all symmetric keys are stored. The “trustedkey” line identifies all key IDs, which have to be considered “trusted” or “uncompromised”. All other keys defined in the keyfile are considered “compromised”. This allows to re-use already owned keys by just adding their respective key ID to the “trustedkey” parameter. If a key needs to be “switched off”, it can be removed from this line without actually removing it from the system. This ensures an easy way to re-activate it later without actually transferring the key again.

The line “requestkey 15” declares the key ID for mode-6 control messages (as described in RFC-1305), which are used by the `ntpq` utility for example. The “controlkey” parameter is specifying the key used for mode-7 private control messages, for example used by the `ntpd` utility. These keys protect the `ntpd` variables against unauthorised modification.

The `ntp.keys` file mentioned above holds a list of all keys and their respective ID known by the server. This file should not be world-readable (only root should be able to look into this) and it may look like this:

```
# ntp keys file (ntp.keys)
```

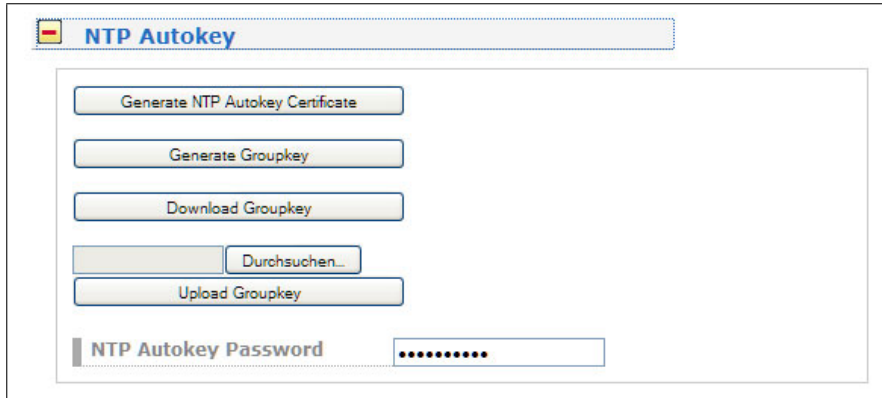
```
1      N 29233E0461ECD6AE # des key in NTP format
2      M Rlrop8KPPvQvYotM # md5 key as an ASCII random string
14     M sundial # md5 key as an ASCII string
15     A sundial # des key as an ASCII string
# the following 3 keys are identical
10     A SeCReT
10     N d3e54352e5548080
10     S a7cb86a4cba80101
```

The first column holds the key ID (used in the `ntp.conf` file), the second column defines the format of the key, which is following in column three. There are four different key formats:

- **"A"** means DES key with up to eight 7-bit ASCII characters, where each character is standing for a key octet (this is used by Unix passwords, too).
- **"S"** is a DES key written in hexadecimal notation, where the lowest bit (LSB) of each octet is used as the odd parity bit.
- If the key format is specified as **"N"**, it also consists of a hexadecimal string, but in NTP standard format by using the highest bit (HSB) of each octet used as the odd parity bit.
- A key defined as **"M"** is a MD5 key with up to 31 ASCII characters.
- The LANTIME supports MD5 authentication only.
- Please be aware of the following restrictions: No **"#"**, **"t" (tab)**, **"n" (newline)** and **"0"** (null) are allowed in a DES or MD5 ASCII key. The key ID 0 is reserved for special purposes and should not appear in the keys file.

13.5.8 NTP Autokey Settings

NTP Version 4 supports symmetric keys and additionally provides the so-called AUTOKEY feature. The authentic of received time at the NTP clients is sufficiently ensured by the symmetric key technique. In order to achieve a higher security, e.g. against so-called replay attacks, it is important to change the used crypto keys from time to time.



In networks with a lot of clients, this can lead to a logistic problem, because the server key has to be changed on every single client. To help the administrator to reduce this work (or even eliminate it completely), the NTP developers invented the AUTOKEY feature, which works with a combination of group keys and public keys. All NTP clients are able to verify the authentic of the time they received from the NTP servers of their own AUTOKEY group by using this AUTOKEY technique.

The AUTOKEY features works by creating so-called secure groups, in which NTP servers and clients are combined. There are three different kinds of members in such a group:

a) Trusted Host

One or more trusted NTP servers. In order to become a “trusted” server, a NTP server must own a self-signed certificate marked as “trusted”. It is good practice to operate the trusted hosts of a secure group at the lowest stratum level (of this group).

b) Host

One or more NTP servers, which do not own a “trusted” certificate, but only a self-signed certificate without this “trusted” mark.

c) Client

One or more NTP client systems, which in contrast to the above mentioned servers do not provide accurate time to other systems in the secure group. They only receive time.

All members of this group (trusted hosts, hosts and clients) have to have the same group key. This group key is generated by a so-called trusted authority (TA) and has to be deployed manually to all members of the group by secure means (e.g. with the UNIX SCP command). The role of a TA can be fulfilled by one of the trusted hosts of the group, but an external TA can be used, too.

The used public keys can be periodically re-created (there are menu functions for this available in the web interface and also in the CLI setup program, see “Generate NTP Autokey Certificate” in section “NTP Autokey Settings” of the “Security Management” page) and then distributed automatically to all members of the secure group. The group key remains unchanged, therefore the manual update process for crypto keys for the secure group is eliminated.

A LANTIME can be a trusted authority / trusted host combination and also a “non-trusted” host in such a secure group.

To configure the LANTIME as a TA / trusted host, enable the AUTOKEY feature and initialise the group key via the HTTPS web interface (“Generate groupkey”) or CLI setup program. In order to create such a group key, a crypto password has to be used in order to encrypt / decrypt the certificate. This crypto password is

shared between all group members and can be entered in the web interface and CLI setup program, too. After generating the group key, you have to distribute it to all members of your secure group (and setup these systems to use AUTOKEY, too). In the ntp.conf file of all group members you have to add the following lines (or change them, if they are already included):

```
crypto pw cryptosecret
keysdir /etc/ntp/
```

In the above example “cryptosecret” is the crypto password, that has been used to create the group key and the public key. Please note that the crypto password is included as a plain text password in the ntp.conf, therefore this file should not be world-readable (only root should have read access to it).

On the clients, the server entries must be altered to enable the AUTOKEY feature for the connections to the NTP servers of the group. This looks like:

```
server time.meinberg.de autokey version 4
server time2.meinberg.de
```

You find the server time.meinberg.de which is using the AUTOKEY feature, while time2.meinberg.de is used without any authentic checks.

If you want to setup the LANTIME server as a trusted host, but need to use a different trusted authority, please create your own group key with this TA and include it with the web interface of your LANTIME (on page “Security Management” see section “NTP autokey” , function “Upload groupkey”).

If you want to setup the LANTIME as a “non-trusted” NTP server, you have to upload the group key of your secure group (“Security Management” / “NTP autokey” / “Upload groupkey”) and create your own, self-signed certificate (without marking it as “trusted”). Because every certificate which is creating by using the web interface and/or CLI setup is marked “trusted”, you have to execute the tool “ntp-keygen” manually on your LANTIME by using shell access (via SSH).

```
LantimeGpsV4:/etc/ntp # ntp-keygen -q cryptosecret
```

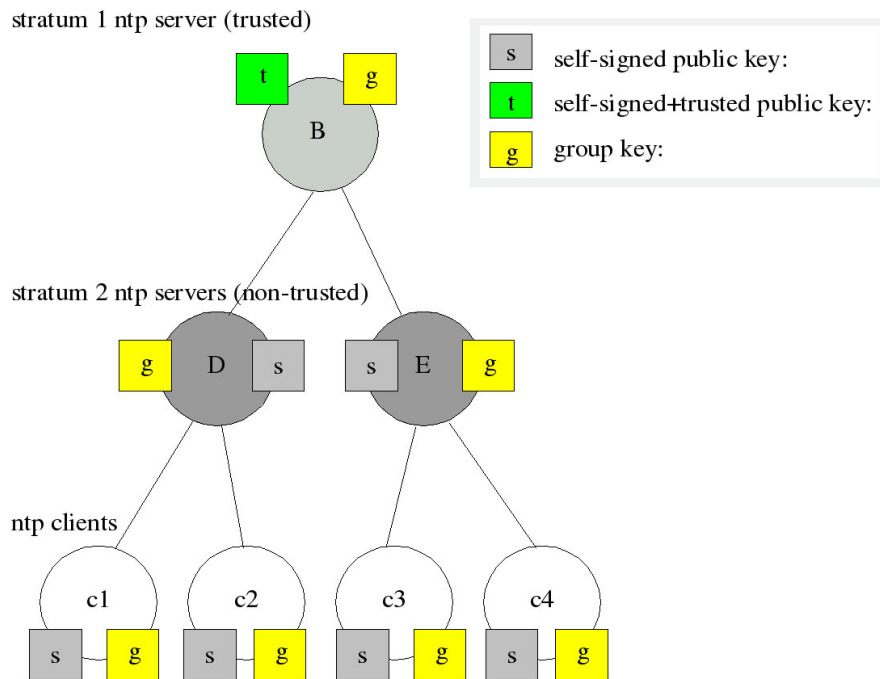
Here, too, “cryptosecret” is the crypto password used in the ntp.conf entry. Then you have to copy the new ntpkeys to the flash disk with:

```
cp /etc/ntp/ntpkey_* /mnt/flash/config/ntp/uploaded_groupkeys
```

A detailed description about ntp-keygen can be found on the NTP website (<http://www.ntp.org>).

Example:

This autokey group is formed by one Stratum-1-server (B), two Stratum-2-servers (D and E) and a number of clients (in the diagram there are 4 clients shown, c1 – c4). B is the trusted host, he holds the group key and a self-signed certificate marked as “trusted”.



D and E are NTP servers, which are “non-trusted” hosts of the group, they hold the group key and a self-signed certificate which lacks the “trusted” mark. The clients also hold the group key and a self-signed certificate. In order to distribute new public keys to the whole group, the administrator only has to generate a new “t” key, which will be distributed automatically to the two hosts D and E. Because these two servers can now present a unbroken chain of certificates to a trusted host, they can be considered “trusted” by the clients as well.

More about the technical background and detailed processes of the AUTOKEY technique can be found at the official NTP website (<http://www.ntp.org>).

13.5.9 NTP Leap Second Handling

GPS system time differs from the universal time scale (UTC) by the number of leap seconds which have been inserted into the UTC time scale since GPS was initiated in 1980. The current number of leap seconds is part of the navigation message supplied by the satellites or radio transmitters, so the internal real time of the clock is based on UTC.

In this menu you can select an available "Leap Second File" from the Meinberg or NTP web server. Of course you can enter your own download link or you can upload your own file for leap second handling.

Available Download Sources

Meinberg: https://www.meinberg.de/download/ntp/leap_second

NTP.ORG: <ftp://time.nist.gov/pub/> (leap-seconds.xxxxxxxx)

13.6 Configuration: PTP V2

TSU-GbE card - optional functionalities: SyncE* / Hardware NTP Interface*

The screenshot displays the LANTIME Web Interface. At the top, the MEINBERG logo is on the left, and the title 'LANTIME Web Interface' is in the center. On the right, it shows 'Logged in as: root', 'Access-Level: Super-User', and 'Firmware-Build: 6.18.001'. A navigation menu below the header includes: Main, Network, Notification, Security, NTP, PTP, System, Statistics, Receiver, IO Config, NTP-Mon, XtraStats, Docs & Support, and Logout. The main content area is titled 'LANTIME - PTP' and is divided into two sections: 'PTP V2 Status' and 'PTP V2 Configuration'. The 'PTP V2 Status' section shows two interfaces: 'Interface 01 (Slot: MRI2)' with buttons for 'Network', 'Global', and 'SyncE'; and 'Interface 02 (Slot: IO5)' with buttons for 'Network' and 'Global'. The 'PTP V2 Configuration' section shows 'Interface 01 (Slot: MRI2):' with buttons for 'Network', 'Global', 'SyncE', 'Misc', and 'Outputs'; and 'Interface 02 (Slot: IO5):' with buttons for 'Network', 'Global', and 'Misc'. At the bottom of the configuration area, there are three buttons: 'Save Settings', 'Reset Changes', and 'Back'.

All parameters for proper PTP functionality can be configured in a clear and user friendly Web GUI. The set of parameters which can be configured in the Web GUI corresponds to the PTP card version currently installed in the system. Some features are available with TSU-GbE cards and above only and these are marked as optional (*) in this manual.

When you log in to the Web GUI, please follow to the PTP dialog. In the main menu the following sub-menus are listed:

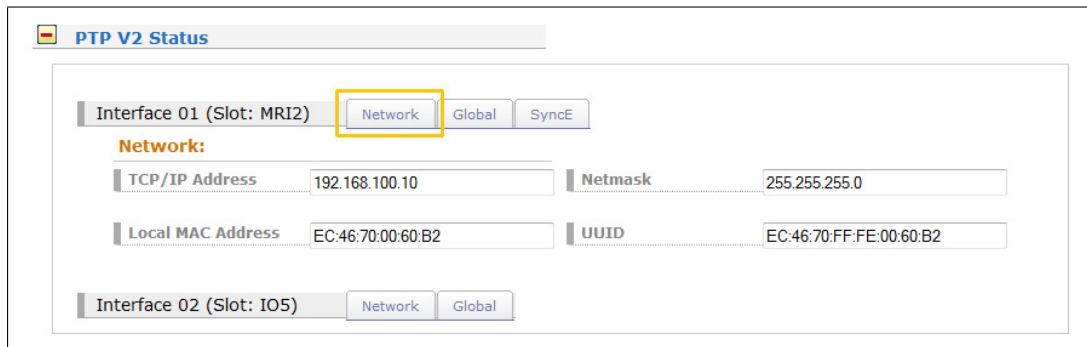
- PTPv2 Status
- PTPv2 Configuration

If more than one PTP unit (PTP ports) is built into the system, then the status and configuration for each port can be edited separately and will be listed on this page.

13.6.1 PTP Status Information

The PTPv2 status dialogue shows all current status information of the selected PTP card according to its settings configured in the configuration submenu.

PTP Network Status



The screenshot shows the 'PTP V2 Status' dialog box. At the top, there is a tab for 'Interface 01 (Slot: MRI2)' with sub-tabs for 'Network', 'Global', and 'SyncE'. The 'Network' tab is selected and highlighted with a yellow box. Below the tabs, the 'Network:' section contains four input fields: 'TCP/IP Address' (192.168.100.10), 'Netmask' (255.255.255.0), 'Local MAC Address' (EC:46:70:00:60:B2), and 'UUID' (EC:46:70:FF:FE:00:60:B2). At the bottom, there is a section for 'Interface 02 (Slot: IO5)' with sub-tabs for 'Network' and 'Global'.

In the Network tab you can check if network settings of the PTP card are valid.

Local MAC Address of the PTP unit

If the PTP card operates currently as a Grandmaster (GM) its local MAC Address is shown in the status of PTP slaves which are currently synchronized to this GM.

UUID

The UUID is the unique identifier of the PTP port which is based on the MAC address of the PTP port.

PTP Global Status

In the Global submenu the current operation mode of the selected PTP port (interface) is shown. The appearance of this page depends on the mode of the PTP card operation. Different states of a PTP port are possible. For example, if the unit is configured as a PTP master clock, then this page shows "Master" state. In MRS (Multi Reference Source) devices, the PTP mode "Slave" may be displayed here.

PTP V2 Status

Interface 01 (Slot: MRI2) Network **Global** SyncE

Global:

PTP Mode	Multicast Slave	Domain Number	0
Port State	SLAVE	Port Link up	Yes
Grandmaster MAC	EC:46:70:00:51:BD	Delay Asymmetry	-0.0ns
Offset from Master	+0.000000007s	Path Delay	0.000000006s
Clock accuracy	< 100 ns	Clock class	6
PTP Seconds	1435220689	Time Source	GPS
UTC Offset	35s	Leapsecond	Not Announced
TSU Time: TAI:25.06.15 08:24:49.591465;			

Interface 02 (Slot: IO5) Network Global

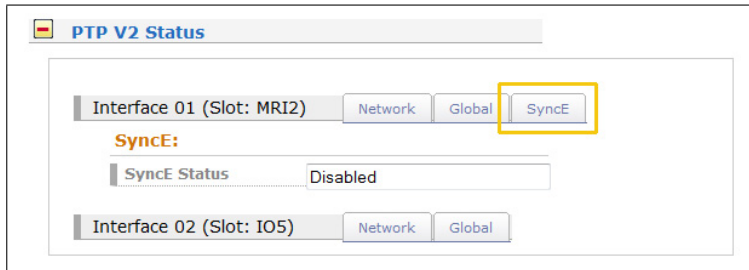
PTP Port States

- uninitialized: The PTP module is booting up, the software daemon has not yet started, the IP address is not yet assigned.
- initializing: In this state the port initializes its data sets, hardware, and communication facilities.
- faulty: Not defined in LANTIME systems.
- stopped: The PTP service has been stopped or it has not started due to a missing link on the PTP port or a not-synchronized master clock after a startup.
- disabled: Not defined in LANTIME systems.
- listening: The port is waiting for the announceReceiptTimeout to expire or to receive an Announce message from a master.
- preMaster: A short transitional state while the port is becoming a master.
- master: The port is a current master.
- passive: The port is in passive mode, meaning there is another master clock active in the PTP domain. The port can enter master state when it wins the BMCA (Best Master Clock Algorithm) due to a failure/service degradation of the current master.
- uncalibrated: The port wants to become a slave in the PTP domain and has already detected a suitable grandmaster. The TSU is waiting to calculate the path delay to a Grandmaster.

slave:	The port has successfully subscribed to a master and receives all expected messages. It also successfully measured the path delay using delay request messages.
Grandmaster MAC	The MAC Address of the current Grandmaster.
Clock Accuracy	The clock accuracy of the active grandmaster. This value is used in the Best Master Clock Algorithm to select the best master.
PTP Seconds	Current value of the raw PTP seconds value (seconds since 1970).
UTC Offset	This value represent the current Offset to the PTP time based on TAI to calculate UTC.
Domain Number	A PTP domain is a logical group of PTP devices within a physical network which is defined by the same domain number. Slave devices that should sync to a certain master in the network must be configured with a unique domain number which is the same as for the master.
Port Link up	Status 0: the port is down, check the link LED and the connection to the link partner. If faulty, the network card should be replaced. Status 1: the port is in normal operation.
Delay Asymmetry	If a static asymmetry offset in the network is known, this value may be entered (in ns) to compensate it before the PTP start.
Clock Class	PTP Clock class of the currently selected PTP grandmaster. This value is used in the Best Master Clock Algorithm.
Time Source	The type of a time source as used by the Grandmaster (informative only).
Leap Second	Leap second announcement flag, set up to 24 hours prior the leap second event, depending on the GM implementation.
TSU Time	Displayed time of day in the selected PTP timescale.

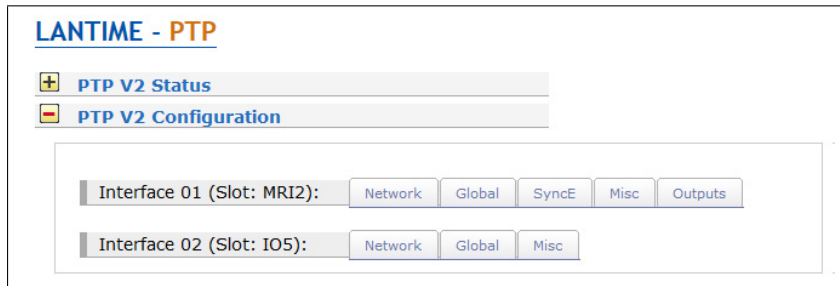
SyncE Status

You can check if SyncE functionality is activated on the card or not (if supported by the PTP module).



13.6.2 PTP Configuration Menu

All parameters for proper operation of each PTP port (interface) which are built into the system should be configured separately according to its function in the PTP network. Whenever a change should be applied, it needs to be saved by confirming the “Save Settings” button at the bottom of the page.



The configuration parameters are grouped in the submenus as follows. Submenus marked with * are available in TSU-GbE (and higher version) cards only.

- Network
- Global
- SyncE*
- Misc*
- Outputs*

PTP Network Configuration

PTP V2 Configuration

Interface 01 (Slot: MRI2): **Network** Global SyncE Misc Outputs

Network:

Hostname: PTPv2 Domainname:

Nameserver 1: 0.0.0.0 Nameserver 2: 0.0.0.0

Enable DHCP-Client: No

TCP/IP Address: 192.168.100.10 Netmask: 255.255.255.0

Default Gateway: 192.168.100.1

IPv6 Mode: Static

IPv6 Address:

IPv6 Multicast Scope: FF01 - Interface-Local Scope

Enable VLAN Option:

VLAN-Tag (1-4094): 0 Priority: 0

Disable SSH Service:

DSCP PTP Classification: CUSTOM 00 (HEX: 00)

Multicast TTL: 5

Interface 02 (Slot: IO5): Network Global Misc

Network Configuration

Hostname	Hostname for the selected PTP port can be entered.
Domainname	Domainname for the selected PTP can be assigned.
Nameserver1	Nameserver1 can be entered if it is used in a network.
Nameserver2	Nameserver2 can be entered if it is used in a network.
Enable DHCP-Client	Activation / deactivation of DHCP service. If a DHCP Client is activated the field for static IP configuration is deactivated. The opposite is the case when DHCP Client is deactivated.
IP-Address from DHCP	If DHCP service is found in the network, a valid IP for a PTP port will be assigned automatically and displayed here.
Netmask from DHCP	If DHCP service is found in the network, a valid Netmask for a PTP port will be assigned automatically.
Gateway from DHCP	If DHCP service is found in the network, a valid Gateway for a PTP port will be assigned

	automatically.
TCP / IP Address	If the DHCP Client is deactivated, this field can be edited to assign a valid static IP address for the selected PTP interface.
Netmask	If the DHCP Client is deactivated, this field can be edited to assign a netmask for the selected PTP interface.
Default Gateway	If the DHCP Client is deactivated, this field can be edited to assign a default gateway for the selected PTP interface.
IPv6 Mode	IPv6 addressing via DHCPv6 / Static assignment / Router Advertisement are available.
IPv6 Address	Ipv6 Address assigned to the selected PTP port. If Static option is activated for Ipv6 Mode, then a valid static IP address can be configured in this field.
IPv6 Multicast Scope	The prefix of IPv6 multicast addresses specifies their scope. A specific scope in case of multicast mode can be selected here.
Enable VLAN Option	Activation / deactivation of Virtual LAN (IEEE 802.1Q) service on the PTP interface.
VLAN-Tag (1-4094)	A 12-bit value specifying a VLAN ID to which a PTP port belongs.
Priority	Values 0 (default, lowest priority) to 7 (highest priority) which can be used to prioritize network traffic for different types of data.
Disable SSH Service	If checked then SSH Access for this PTP port is deactivated.
DCSP PTP Classification	Differentiated Services Code Point. This is a QoS parameter within the IP header of the PTP packet to prioritize the traffic.
Multicast TTL	Time-To-Live. By default, the PTP multicast traffic is not routed and this value is defined as "1" by the PTP standard. However a user defined configuration of the TTL value can be entered here to change the default value.

PTP - Global Configuration

PTP V2 Configuration

Interface 01 (Slot: MRI2): Network **Global** SyncE Misc Outputs

Global:

Operating Mode PTP NTP

Select Profile Custom

PTP Mode Multicast Slave Hybrid-Mode

Unicast Master Address 172.29.9.210

Delay Mechanism E2E Domain Number 0

Network Protocol UDP/IPv4 (L3) Timescale PTP Standard (TAI)

Priority1 128 Default Asymmetry Offset [ns] 0

Priority2 128

Announce Interval 1 announce message every 2 seconds

Sync Interval 1 sync message per second HQ-Filter No

Delay Request Interval 1 request message every 2 seconds

Interval Duration [s] 60 Announce Receipt Timeout 3

Profile Specific Configuration: Power IEEE C37.238 Telecom ITU-T G.8265.1 Telecom ITU-T G.8275.1 SMPTE ST 2059-2

Interface 02 (Slot: IO5): Network Global Misc

Operating Mode: If supported, there is an option to run a NTP service in Server mode with hardware timestamp support. Select between PTP and NTP mode at this step. It is not possible to run both modes at the same time on one TSU card.

Select Profile: User can choose among preselected sets of PTP parameters defined in profiles usually used in different industries. If the default setting "Custom" is selected, the user can select any parameter combination available in the global configuration section as long as the PTP standard allows it. Depending on the selected profile, there might be profile specific parameters available which can be found in the "Profile Specific Parameters" section below the standard PTP parameters sections.

There are six different presets currently supported on PTP cards:

Default E2E IEEE 1588-2008

Default Profile with End-To-End Delay Mechanism as defined by the IEEE 1588-2008 standard, available in Multicast and Unicast mode.

- Ann Msg Rate: 2 sec
- Sync Msg Rate: 1/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: "E2E"

Default P2P IEEE 1588-2008

Default Profile with P2P delay mechanism as defined by the IEEE 1588-2008 standard, available in Multicast mode.

- Ann. Msg Rate: 2 sec
- Sync Msg Rate: 1/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: "P2P"
- Network Prot. "Layer 3 (UDP/IPv4)"

Power IEEE C37.238

- Ann Msg Rate: 1/sec
- Sync Msg Rate: 1/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: "P2P"
- Network Prot. "Layer 2 (IEEE 802.3)"
- VLAN (802.1Q) enabled (VLAN ID:0, Prio:4)
- Power Profile TLVs enabled

Telecom ITU-T G.8275.1

- Ann Msg. Rate: 8/sec
- Sync Msg. Rate: 16/sec
- Del Req Rate: 16/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: "E2E"
- Network Prot. "Layer 2 (IEEE 802.3)"

In Unicast Master / Slave Mode:

Telecom ITU-T G.8265.1

- Ann Msg. Rate: 1/sec
- Sync Msg. Rate: 16/sec
- Del Req Rate: 16/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: "E2E"
- Network Prot. "Layer 3 (UDP/IPv4)"

In Unicast or Multicast Master / Slave Mode:

SMPTE ST 2059-2

- Ann Msg. Rate: 4/sec
- Sync Msg. Rate: 8/sec
- Del Req Rate: 8/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: "E2E" or "P2P"

- PTP Mode:** A PTP port can operate in one mode only: master or slave. When the mode is selected the user can choose between multicast or unicast-only protocol. In the newest firmware a combined unicast multicast master mode of operation is also supported.
- Hybrid Mode:** In this mode PTP messages Sync, FollowUp and Announce are sent in Multicast whereas the DelayRequest and DelayResponse Messages are sent in Unicast.
- Delay Mechanism:** Two options possible:
E2E (End-to-end) where delay measurement messages are sent directly from a slave to the master (two end nodes).

P2P (Peer-to-peer): each device (a peer) in the network exchanges peer-delay measurement messages. This way each node can keep a track of the delays between itself and its immediately connected neighbour. P2P mechanism can be used in 1588 PTP-capable networks only.
- Network Protocol:** Two options for network protocol are possible:
ETH-IEEE 802.3 / Ethernet (Layer 2): Ethernet frames including MAC addresses of a slave and master.

UDP-UDP/IPv4/IPv6 (Layer 3): User Data Protocol one of the main protocols used for the Internet.
- Priority 1:** The attribute is used in the execution of the best master clock algorithm (BMCA). Lower values take precedence.

Configurable range: 0..255. The operation of the BMCA selects clocks from a set with a lower value of priority1 over clocks from a set with a greater value of priority1.
- Priority 2:** The attribute is used in the execution of the BMCA. Lower values take precedence.

Configurable range: 0..255.

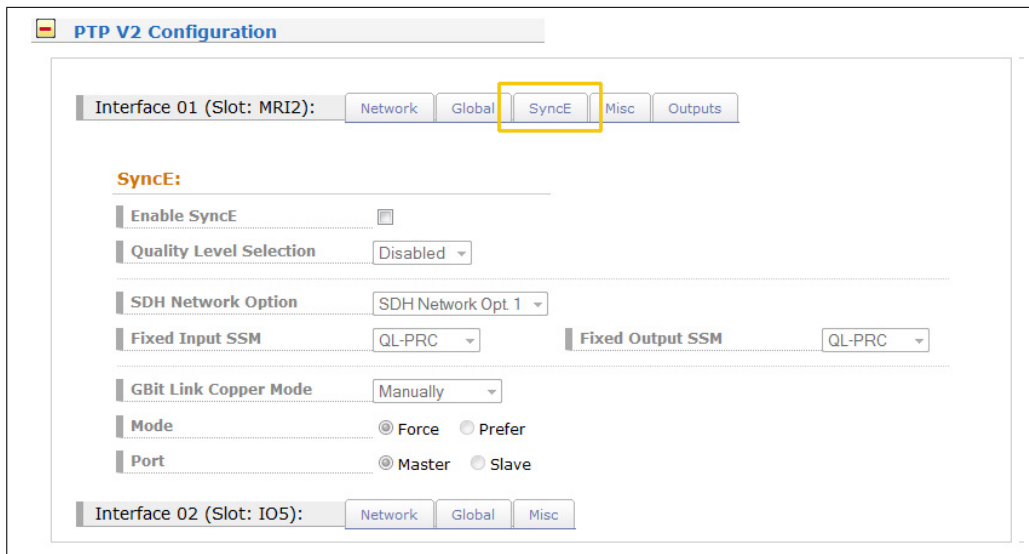
In the event that the operation of the BMCA fails to order the clocks based on the values of priority1, clockClass, clockAccuracy, and scaledOffsetLogVariance, the priority2 attribute allows the creation of up to 256 priorities to be evaluated before the tiebreaker. The tiebreaker is based on the clockIdentity. The values clockClass, clockAccuracy, and scaledOffsetLogVariance depend on the internal state of the grandmaster and cannot be configured.
- Msg. Intervals:** Specify the settings for PTP message rates.
- Announce Interval:** Specifies the rate for sending announce messages between masters in order to select the current Grand Master.

Available settings are: 16/s, 8/s, 4/s ... 2s, 4s, 8s, 16s with a default value 2 seconds.
- Sync Interval:** Specifies the rate for sending sync messages from a master to slave.

Available settings are: 128/s, 64/s ... 64s, 128s, with a default value 1 second.
- Delay Request Interval** Specifies the rate how often delay request messages are sent from a slave to the master. Delay request messages intervals 128/s, 64/s,... 64s, 128s, with a default value 2 seconds.

Announce Receipt Timeout:	Specifies the rate for announce receipt timeout messages which is generally 2–10 times the Announce Interval rate, with a default value of 3. In this time the BMCA procedure should select the current Grand Master.
Interval Duration [s]:	Requested duration until timeout / renewal.
Domain Number:	A PTP domain is a logical group of PTP devices within a physical network which is defined by the same domain number. Slave devices that should sync to a certain master in the network must be configured with a unique domain number which is the same as for the master.
Timescale:	<p>Two options are possible:</p> <p>PTP: As per default TAI timescale is used in PTP timing. TAI is a linear timescale without discontinuities such as inserted leap seconds in the UTC timescale. A time unit is based on SI second. The TAI timescale started with 1 January 1970 00:00:00.</p> <p>ARB as arbitrary: In normal operation, the epoch is set by an administrative procedure.</p>
Fixed / Asymmetry Offset [ns]:	User defined network asymmetry / known offset compared to the Reference Time. Possible value [0 – 1000000 ns].
HQ Filter:	In heavy loaded networks when using non-PTP compliant switches, the "HQ Filter" can be activated to reduce the jitter.

Option SyncE Configuration



This submenu allows all relevant settings for the Synchronous Ethernet functionality. SyncE is an ITU-T standard for computer networking that facilitates the transference of clock signals over the Ethernet physical layer.

Note: The SyncE signal can only be used as a reference input signal, when a TSU-GbE card operates in an MRI Slot (see menu - "Configuration Receiver -> MRS Settings").

Enable SyncE:	Activation / Deactivation of SyncE signal on a PTP port. SyncE runs on the PHY network layer therefore it does not disturb PTP on Layer 2 or Layer 3. They both can run in parallel on the same port.
Quality Level Selection	If enabled, the Quality Levels as transported once per second within the ESMC (Ethernet Synchronization Message channel) and are determined automatically depending on the clock status in master mode or used as they are received as an input in slave mode. IF this mode is disabled, then the settings chosen below in Fixed Input SSM and Fixed Output SSM are used permanently as static values.
SDH Network Option	The selectable values for the Quality levels depend on the SDH network options which reflect to Option 1 (for SDH, E1 based systems) or Option 2 (for SONET, T1 based systems).
Fixed Input SSM	Fixed Quality level of the SyncE input signal.
Fixed Output SSM	Fixed Quality level of the SyncE output signal.
Gbit Link Copper Mode	If the copper port is used for SyncE in GBit mode then the Clock Master or Clock Slave needs to be defined. This is not necessary if optical connections via SFP are used as this is determined automatically there.
Mode	User can select if the copper port should be forced to act as the clock master or clock slave depending on the role (Master/Slave) that this SyncE port should have. Misconfiguration can lead to link loss, so the user needs to take care about the proper configuration of the link partners.
Port	The port can operate in a SyncE clock master or clock slave mode. A configuration is only necessary for the copper port but not for Fibre Optic connections.

Option Misc. Configuration



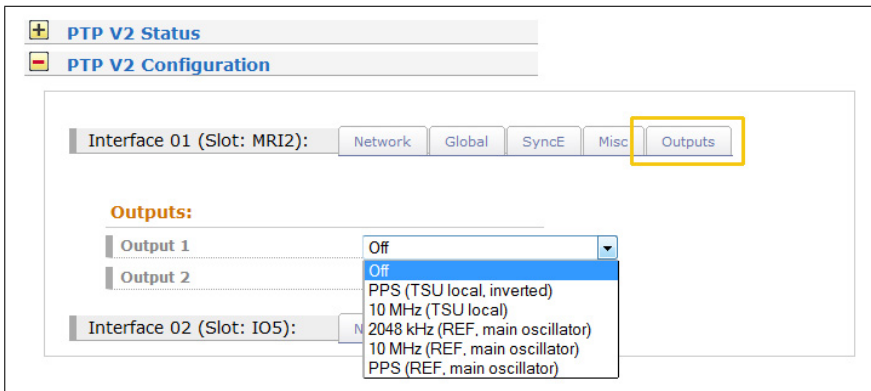
Activate PTP One Step: Per default Two Step approach is active.

Two Step approach: The PTP protocol requires the master to periodically send SYNC messages to slave devices. The hardware time stamping approach of PTP requires that the master records the exact time when such a SYNC packet is going on the network wire and needs to communicate this time stamp to the slaves. This can be achieved by sending this time stamp in a separate packet (a so-called FOLLOW-UP message).

One Step operation enabled: the SYNC message itself is time stamped on-the-fly just before it leaves the network port. Therefore, not FOLLOW-UP message is needed.

Disable PTP Management Messages: A protocol within PTP used to query and update the PTP data sets maintained by master clocks. These messages are also used to customize a PTP system and for initialization and fault management. Management messages are used between management nodes and clocks. This feature is enabled per default.

Option: Output Configuration



TSU-GbE card comprises one Gigabit Ethernet SFP/RJ45 Combo Port for network synchronization and two female BNC output interfaces with a list of available signals as follows:

- PPS (generated locally on the TSU, inverted)
- 10 MHz (generated locally on the TSU)
- 2.048 MHz (taken from the active internal clock module)
- 10 MHz (taken from the active internal clock module)
- PPS (taken from the active internal clock module)

Per default no output signal is active on both outputs.

13.7 FDM - Frequency Deviation Monitoring

MEINBERG LANTIME Web Configuration Utility

Logged in as: root
Access-Level: Super-User
Build: 6.16.009

Main Network Notification Security NTP System Statistics Documentation Receiver FDM XtraStats Logout

LANTIME - FDM

Actual FDM Stats

Frequency	49.999000	Referencetime	13:51:38
Frequencydifference	-0.001000	Powerlinetime	13:51:19.862
		Timedifference	-18.138000

[FDM Configuration Form](#)
[Manual FDM Configuration](#)

13.7.1 FDM - Current State

Actual FDM Stats

Frequency	49.999000	Referencetime	13:51:38
Frequencydifference	-0.001000	Powerlinetime	13:51:19.862
		Timedifference	-18.138000

13.7.2 FDM Configuration

FDM Configuration

FDM - Frequency Deviation Monitor 1 [Chassis 0, Slot ESI2]:

Interface 01

General:

Line Frequency	50 Hz	
Min Frequenz Deviation	45000	mHz
Max Frequenz Deviation	55000	mHz
Min Time Deviation	-100000	ms
Max Time Deviation	100000	ms

The frequency deviation monitor FDM is suitable for 50Hz power networks as well as for 60Hz networks. Selection is made with nominal frequency. After power-up, the PL time is reset to the REF time and therefore the time deviation is set to +00.000s. However, if a different start value is required because of any reason, a time deviation preset value in the range between -99.999s (Lower Limit) and +99.999s (Upper Limit) can be entered in this submenu. The PL time is calculated according to the new value of the time deviation.

Analog Outputs

The screenshot shows the 'FDM Configuration' window for 'FDM - Frequency Deviation Monitor 1 [Chassis 0, Slot ES12]'. The 'Interface 01' tab is active, and the 'Analog Outputs' sub-tab is selected. Under 'Analog Outputs:', there are two sections: 'Analog Output 1' and 'Analog Output 2'. Each section has a 'Mode' dropdown menu currently set to 'Frequency Deviation'.

The FDM provides two analog outputs for longtime-recording. These outputs have a range of $-2.5V \dots +2.5V$, divided in 65536 steps. Either the frequency deviation or the time deviation can be selected for monitoring via one of these analog outputs.

Serial Interfaces

The screenshot shows the 'FDM Configuration' window for 'FDM - Frequency Deviation Monitor 1 [Chassis 0, Slot ES12]'. The 'Interface 01' tab is active, and the 'Serial Port' sub-tab is selected. Under 'Serial Port:', there are two sections: 'COM 1' and 'COM 2'. Each section has four dropdown menus: 'Baud Rate', 'Framing', 'String Type', and 'Mode'. The 'Mode' dropdown for both COM 1 and COM 2 is set to 'on request '?' only'.

The parameters of both serial RS-232 interfaces COM0 and COM1 can be configured. Baudrate, framing and the string type can be set according to the users requirements.

Note: Make sure that the configuration of COM1 corresponds with the COM parameter of the preconnected reference clock! This is mandatory, because the input of COM1 is used to read in the REF time.

The output sends a serial output string once per second. This applies for COM1 as well as for COM0. The format of the available output strings is described in chapter "Serial Output Strings".

FDM Configuration

FDM - Frequency Deviation Monitor 1 [Chassis 0, Slot ESI2]:

Interface 01 General Serial Port Analog Outputs New Receiver Receiver 1

New Receiver:

Receiver Type: Standard

Address:

Port:

Transport Protocol: TCP

Prefix:

String:

Suffix:

Add Receiver

FDM Configuration

FDM - Frequency Deviation Monitor 1 [Chassis 0, Slot ESI2]:

Interface 01 General Serial Port Analog Outputs New Receiver Receiver 1

Receiver 1:

Receiver Type: Standard

Address: 172.16.84.15

Port: 10001

Transport Protocol: TCP

Prefix:

String: F:%PLFRQ FD:%FRQDEV REF:%REFTIME PLT:%POWERLNTIME TD:%PLTDEV

Suffix:

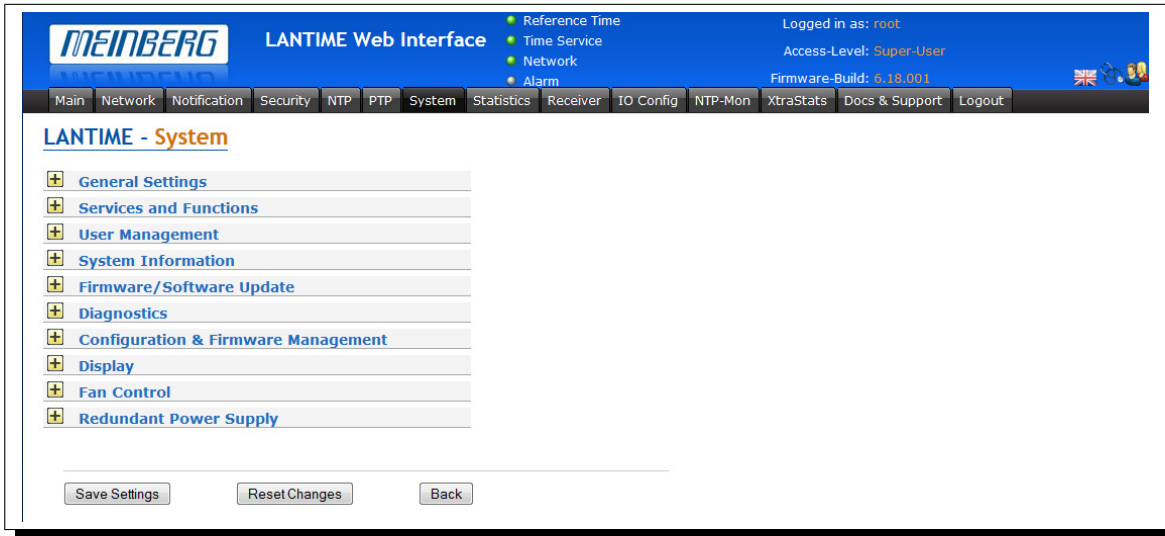
Delete Receiver

13.7.3 Manual FDM Configuration

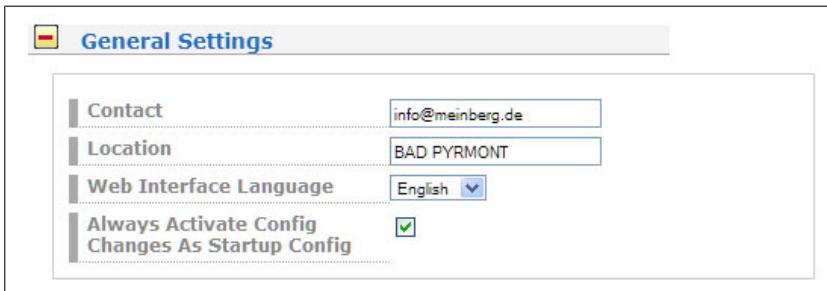
Manual FDM Configuration

Show FDM Configuration Edit FDM Configuration

13.8 Configuration: System



13.8.1 Common Configuration



You can enter a contact address, the location of the LANTIME and the language of the web interface. If the checkbox is activated then all changes during the last session will be stored as new startup configuration.

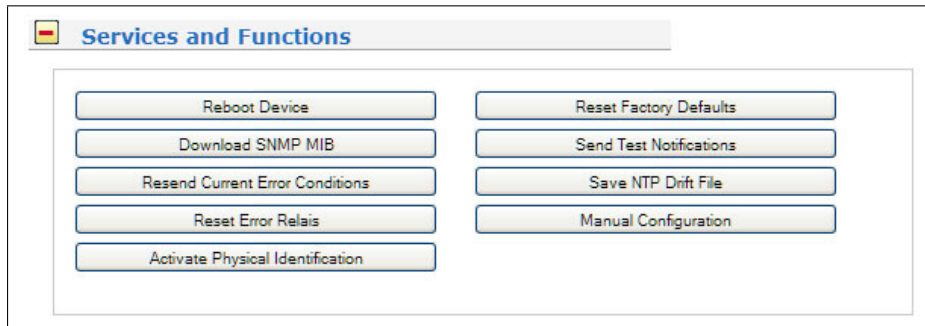
13.8.2 Web interface language



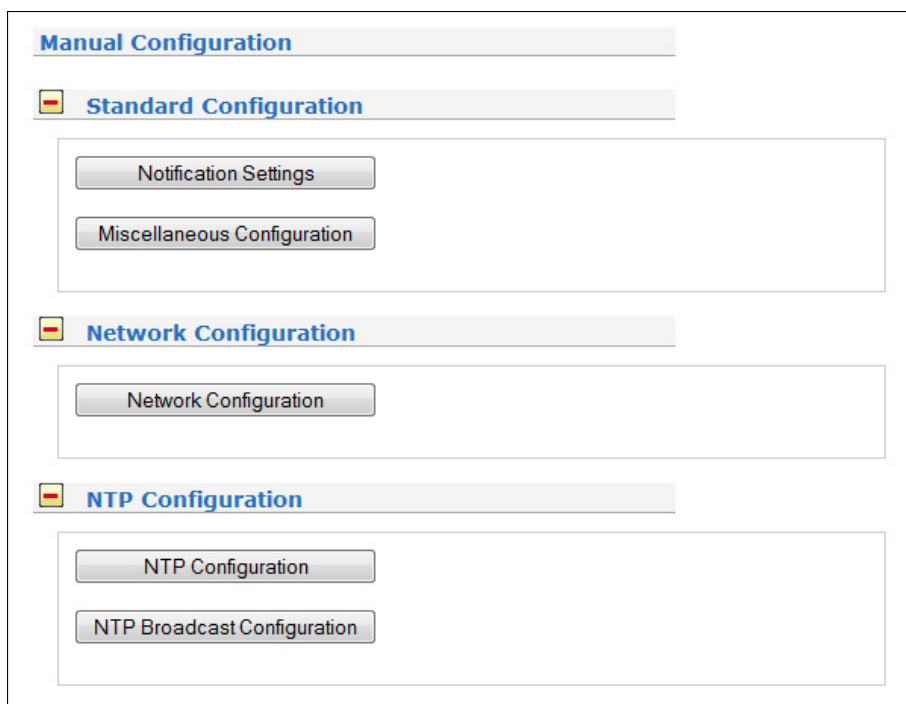
With the selector box "Web interface language" you can change the displayed language of the WEB interface.

13.8.3 Services and Functions

In the first section there are several functions which may be used by the administrator. The button “Reboot Device” is restarting the system, the built-in reference clock is not affected by this, only the included computer system is rebooted, which may take up to 30 seconds.



With “Manual configuration” you are able to change the main configuration by editing the configuration file by hand. After editing, press the “Save file” button to preserve your changes, afterwards you are asked if your changes should be activated by reloading the configuration (this results in reloading several subsystems like NTPD, HTTPD etc.).



The function “Send test notification” is generating a test alarm message and sends it using all configured notify possibilities (e-mail, WMail, SNMP-Traps, wall mount display).

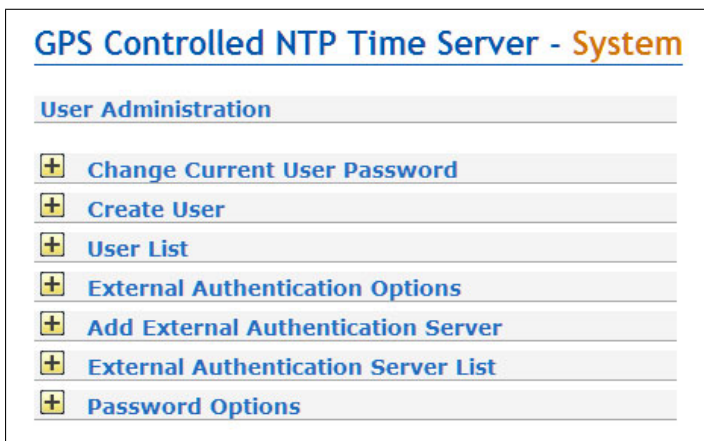
You can use the function “Save NTP drift file” to copy the file `/etc/ntp.drift` to the internal flash disc of your LANTIME. NTP is using this file to have the parameters for compensation of the incorrectness of the system clock available directly after a restart. This results in a faster synchronisation process of the NTPD subsystem after a system restart. You should use this function only, if the NTPD has been synchronized to the internal reference clock for more than one day. This is done here at Meinberg directly before shipping the LANTIME unit to our customers, so you do not need to use this function during normal operation. It may be applicable after a software update.

The function "Reset to factory defaults" is setting all configuration parameters back to default values. The regular file /mnt/flash/global_configuration will be replaced with the file /mnt/flash/factory.conf, but first a copy of the configuration is saved under /mnt/flash/global_configuration.old for backup reasons. The default password "timeserver" is replacing the actual password, too. After using this function, all certificates should be recreated because of the change of the unit's hostname.

Please be aware of the fact that the default configuration is not activated instantly. If you want to avoid setting up the IP address of your unit by locally configuring it on site with the buttons of the front panel (meaning physical presence of someone directly at the location of the LANTIME), you have to configure the network parameters of your LANTIME immediately after using the "reset to factory defaults" button. So, please proceed directly to the Ethernet page and check/change the IP address and the possible access subsystems (HTTP for example) of the LANTIME. The first usage of "Save settings" will load the configuration from flash into memory and activate it.

The point "Download SNMP MIB files" can be used to download all Meinberg specific SNMP MIB files to your workstation. They can be distributed to all SNMP management clients afterwards.

13.8.4 User Management



It is possible to create multiple user accounts on a LANTIME system, each account can be assigned one of three access levels: the Super-User level has full read-write access to the configuration of the LANTIME system, it can modify all parameters and has full shell access to the system when logging in via Telnet, SSH or serial console port.

Administrator level accounts can only modify parameters via the WEB interface but does not have shell access. The access level "Info" can only review status and configuration options but is not allowed to modify any parameters or configuration files.

The screenshot shows two forms:

Change Current User Password

New Password

Confirm Password

Create User

User Name

Password

Confirm Password

Group Membership

The "User Management" menu allows you to set up different users with password and the access level. To change the properties of an user you have to delete the old user and set up a new one. The user "root" cannot be deleted and has always the membership of Super-User. The password of the user "root" can be set on the security page.

User Name	Group Membership	Option
root	Super-User	<input type="button" value="Delete User"/>
MaxMuster	Admin-User	<input type="button" value="Delete User"/>
MaxiMusterfrau	Info-User	<input type="button" value="Delete User"/>

Authentication Options

You can choose between several Authentication Methods:

TACACS: Terminal Access Controller Access-Control System (TACACS) is a remote authentication protocol that is used to communicate with an authentication server commonly used in UNIX networks.

The LANTIME TACACS authentication feature requires that each account that should be able to login to the LANTIME needs a special attribute called „priv-lvl“. This attribute has to be configured on the TACACS Server. In addition to that, you need to assign a value of 100 (=Super User), 200 (=Admin User) or 300 (=Info User) for this attribute to each TACACS user account that should be able to login to a LANTIME.

Please note that you have to define the attribute for the service "lantime_mgmt", for example:

```
service = lantime_mgmt {
    priv-lvl = 100
}
```

RADIUS: Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication for MEINBERG Time Servers to connect and use the network services. RADIUS is a client/server protocol that runs in the application layer, using UDP as transport.

The LANTIME RADIUS authentication feature requires that each account that should be able to login to the LANTIME needs a Vendor Specific Attribute (VSA) called MBG-Management-Privilege-Level. This VSA has to be defined in the so-called dictionary of the RADIUS Server.

In addition to that file, you need to assign a value of 100 (=Super User), 200 (=Admin User) or 300 (=Info User) for this attribute to each RADIUS user account that should be able to login to a LANTIME.

Password-Options

In this section you can activate special options to enhance security features of the user passwords.

Minimum Password Length

This parameter set the minimum number of characters of a password before it is accepted by the system as a valid password. This value is used when creating a new user as well as when you change a current user password.

Allow Secure Passwords Only

The password must contain at least one lower character [a-z], one upper character [A-Z], one number [0-9] and one special character.

List of valid special characters:

```
- _ . ! " [ ] @ \ $ % & ,  
( ) = ? * + ' # ~ { / : ; ^ °
```

User must change password periodically

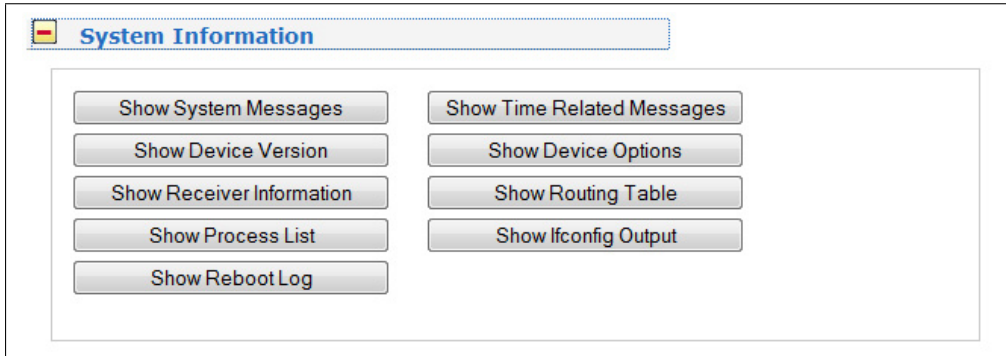
Users will be forced to change there passwords at regular intervals. If a password is expired the user can't log in to the unit before changing his current password.

Available intervals:

Monthly	= Every 30 Days
Half-Yearly	= Every 180 Days
Yearly	= Every 360 Days

13.8.5 System Information

The button “System Information” displays the SYSLOG of the LANTIME completely. In this log all subsystems create their entries, even the OS (upper case) kernel. The SYSLOG file /var/log/messages is only stored in the system’s ram disk, therefore it is lost after a power off or restart. If you configured an external SYSLOG server, all LANTIME syslog entries will be duplicated on this remote system and can be saved permanently this way.



13.8.6 Show System Messages

Show System Messages:

1-200 201-400 401-600 601-800 801-1000 1001-1200 1201-1400 1401-1600 1601-1800 1801-2000 2001-2126

Text:

Show Entries: 1-200

Date	Time	Host	Process	Message
Mar, 19	00:06:45	timeserver	crontab[4698]:	(root) REPLACE (root)
Mar, 19	00:06:45	timeserver	crond[4699]:	(CRON) INFO (pidfile fd = 3)
Mar, 19	00:06:45	timeserver	crond[4700]:	(CRON) STARTUP (fork ok)
Mar, 19	00:06:45	timeserver	crond[4700]:	(CRON) INFO (Running @reboot jobs)
Mar, 19		timeserver	ifplugd(lan0)[4764]:	ifplugd 0.28 initializing, using NETLINK device monitoring.

Show Time Related Messages:

Show Time Related Messages:

1-15

Text:

Show Entries: 1-200

Date	Time	Process	Message
2011-03-30	09:13:55 UTC:	lantime	-> Config changed
2011-03-30	09:02:29 UTC:	lantime	-> Config changed
2011-03-30	07:58:10 UTC:	lantime	-> Config changed
2011-03-30	07:12:24 UTC:	lantime	-> Config changed
2011-03-30	06:26:31 UTC:	lantime	-> Config changed
2011-03-29	13:09:52 UTC:	lantime	-> Normal Operation
2011-03-29	13:09:50 UTC:	lantime	-> NTP sync to MRS
2011-03-29	13:09:50 UTC:	lantime	-> NTP sync
2011-03-29	13:09:23 UTC:	lantime	-> NTP sync to local
2011-03-29	13:09:07 UTC:	lantime	-> NTP sync to MRS
2011-03-29	13:09:07 UTC:	lantime	-> NTP sync
2011-03-29	13:08:52 UTC:	lantime	-> XMR Ref reconnect at Reference Source GPS
2011-03-29	13:08:34 UTC:	lantime	-> Receiver sync
2011-03-29	13:08:23 UTC:	lantime	-> MRS changed to mode "NORMAL OPERATION"
2011-03-29	13:08:19 UTC:	lantime	-> Server boot

Number of entries: 15

A list of time related messages appears which are registered by certain events like reboot of the system, change of configuration settings and so on. After a restart this list is overwritten!

Show Device Version

With "Show Device Version" a number of version numbers (including LANTIME software, operating system and NTPD) are shown in a textbox.

Show Device Version:

```

ID: lantime ELX800 GPS170 M3x V6.04
S/N: n/a
GPS170 :1.19 S/N: 10012290
Oscillator type: TCXO
EPCID: 002E10CB
NTP Version: 4.2.6p3@1.2290-o Fri Feb 4 12:59:24 UTC 2011 (8)
Kernel Version: 2.6.37
System Version: 604
LAN0: HWaddr 00:13:95:02:C2:FA
Built Version:
    
```

Show Device Options

The function “Show Device Options” shows the hardware options installed in your LANTIME.

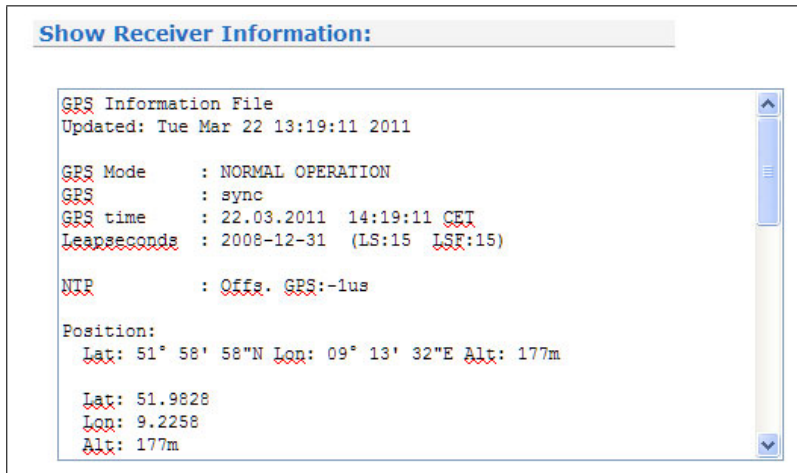
```
Show Device Options:

#GLOBAL OPTIONS

NUMBER ETHERNET INTERFACES: 1
SYSTEM LAYOUT: 0
SYSTEM ADV LAYOUT: 0
SYSTEM LANGUAGE: 0
SYSTEM PARAMETER: server
SYSTEM DESIGN: 0
PIR PARAMETER:
REDUNDANT POWER SUPPLY:
NOTIFICATIONS:
ADV HTTP OPTION:
```


Show Receiver Information

Using the button "Show Receiver Information" gives you the possibility to check detailed receiver status information. The first parameter indicates the time and date of the last update of the shown parameters. Next you find the receiver status and the NTP status.



```

Show Receiver Information:

GPS Information File
Updated: Tue Mar 22 13:19:11 2011

GPS Mode      : NORMAL OPERATION
GPS           : sync
GPS time      : 22.03.2011 14:19:11 CET
Leapseconds   : 2008-12-31 (LS:15 LSF:15)

NTP           : Offs. GPS:-1us

Position:
  Lat: 51° 58' 58"N Lon: 09° 13' 32"E Alt: 177m

  Lat: 51.9828
  Lon: 9.2258
  Alt: 177m
  
```

In case of a GPS receiver you can find GPS position data in this file. The position uses the Latitude / Longitude / Altitude format. Latitude and Longitude are shown in degrees, minutes and seconds, Altitude is shown in meters above WGS84 ellipsoid. The satellite section shows the numbers of satellites in view and the number of usable satellites ("good SV"). Additionally, the selected set of the four used satellites can be read.

The accuracy of the calculated receiver position and time deviation is dependent on the constellation of the four selected satellites. Using the position of the receiver and the satellites, a number of values can be calculated, which allow a rating of the selected constellation. These values are called "Dilutions of Precision (DOP)". PDOP is the abbreviation for "Position Dilution of Precision", TDOP means "Time Dilution of Precision" and GDOP stands for "General Dilution of Precision". Lower values are indicating better accuracy.

The next section "Satellite Info" shows information about all the satellites, which are in view momentarily. The satellite ID, elevation, Azimuth and distance to the receiver reveal the position of the satellite in the sky. The Doppler shows whether the satellite is ascending (positive values) or descending (negative value).

MRS Systems: The configured external NTP servers can be found under:

List of external NTP server:

```

server 172.160.100.000, stratum 1, offset -0.000020, delay 0.02599
server 172.160.100.001, stratum 1, offset 0.000026, delay 0.02603
server 172.160.100.002, stratum 0, offset 0.000000, delay 0.00000
28 Aug 10:58:56 ntpdate[12367]: adjust time server 172.160.100.000 offset -0.000020 sec
  
```

The list shows also the currently used external NTP server (adjust).

Show Routing Table:**Show Routing Table:**

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
169.254.100.0	*	255.255.255.0	U	0	0	0	tsu100
172.16.0.0	*	255.255.0.0	U	0	0	0	lan0
default	meinberg.py.mei	0.0.0.0	UG	0	0	0	lan0

The table shows all available and configured network routes.

Show Process List**Show Process List:**

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
7502	root	20	0	3916	1796	1460	R	23.1	1.8	0:00.12	ssh
5306	root	20	0	88672	2860	1020	S	3.8	2.8	41:31.17	lntimed
7499	root	20	0	2256	940	736	R	1.9	0.9	0:00.02	top
1	root	20	0	1740	576	504	S	0.0	0.6	0:01.58	init
2	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kthreadd

A list of all active processes (CPU performance, used memory, runtime...) of the LAN-CPU is indicated with this table.

Show Ifconfig Output**Show Ifconfig Output:**

```

bond0    Link encap:Ethernet HWaddr 00:00:00:00:00:00
          BROADCAST MASTER MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

bond1    Link encap:Ethernet HWaddr 00:00:00:00:00:00
          BROADCAST MASTER MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

bond2    Link encap:Ethernet HWaddr 00:00:00:00:00:00
          BROADCAST MASTER MULTICAST MTU:1500 Metric:1

```

Show Reboot Log**Show Reboot Log :**

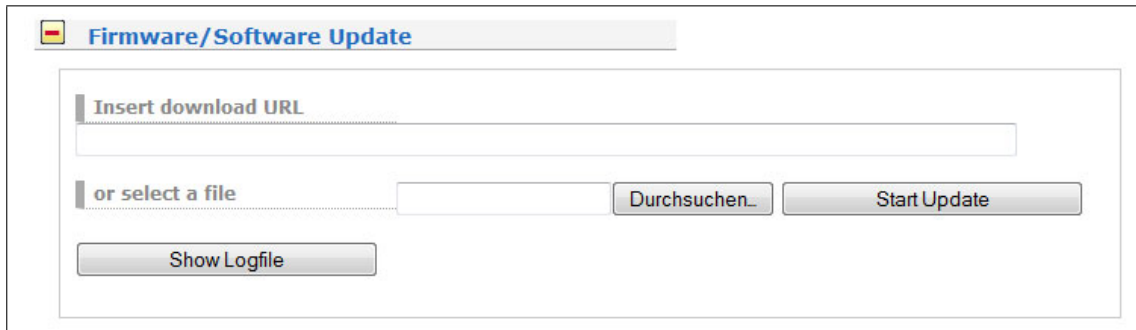
```

Fri Apr 19 07:17:45 UTC 2013 reboot initiated: TTY=PID 21319 USER=root PID=21319 REASON=Autoreboot by install-
release REMOTEHOST= REMOTEUSER=
Mon Apr 22 09:54:39 UTC 2013 reboot initiated: TTY=PID 8517 USER=root PID=8517 REASON=- REMOTEHOST= REMOTEUSER=
Tue Apr 23 08:39:44 UTC 2013 reboot initiated: TTY=PID 17245 USER=root PID=17245 REASON=Manual Reboot
REMOTEHOST=172.16.100.34 REMOTEUSER=
Tue Apr 23 08:49:01 UTC 2013 reboot initiated: TTY=PID 23577 USER=root PID=23577 REASON=Manual Reboot
REMOTEHOST=172.16.100.34 REMOTEUSER=

```

13.8.7 Firmware/Software Update

If you need to update the software of your LANTIME, you need a special file from Meinberg, which can be uploaded to the LANTIME by first choosing the file on your local computer with the "Browse" button and then press "Start Update".



The screenshot shows a web interface titled "Firmware/Software Update". It features a text input field labeled "Insert download URL". Below this is a radio button labeled "or select a file" next to a file selection button labeled "Durchsuchen...". To the right of the "Durchsuchen..." button is a "Start Update" button. Below these elements is a "Show Logfile" button.

The chosen file will be uploaded to the LANTIME, afterwards you are prompted to confirm the start of the update process. The scope of the update only depends on the chosen file.

13.8.8 Download Diagnostic File

A diagnostic file which includes all status data of a LANTIME system logged since the last reboot can be downloaded from all LANTIME Time servers. The file format of the diagnostic file is a tgz-archive. The archive contains all the important configuration and logfiles. In most support cases it is the first action to ask the customer to download the diagnostic file, because it is very helpful to identify the current state of the LANTIME and to find possible errors.



The screenshot shows a web interface titled "Diagnostics". It contains a single button labeled "Download Diagnostic File".

Download via Web Interface

1. Open the "System" page and the submenu "Diagnostics".
2. Press the "Download Diagnostic File" button.
3. Send the tgz-archive with a short description of your problem to our technical support: techsupport@meinberg.de

13.8.9 Configuration and Firmware Management

With this menu you can save the current configuration on the flash memory of the LANTIME. On this way it is possible to save different configuration files on the system. Later you can activate a stored configuration as startup file.

Additionally more than one Firmware version can be archived on the LANTIME. If a updated version is not correspond correctly in the environment, then it is possible to reload an established version on the LANTIME.

Configuration & Firmware Management

Configuration Management

Save Current Configuration As:

Upload Configuration:

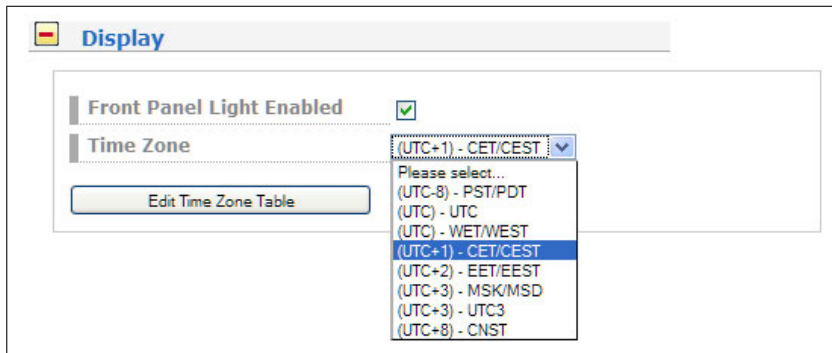
Available Configurations	Options		
startup	<input type="button" value="Activate"/>	<input type="button" value="Delete"/>	<input type="button" value="Download"/>
preupdate	<input type="button" value="Activate"/>	<input type="button" value="Delete"/>	<input type="button" value="Download"/>

Firmware Management

Running Firmware fw_6.14.013
 Scheduled Firmware fw_6.14.013

Available Firmware Files	Version	Type	Options	
OSV (Original Shipped Version)	6.14.012		<input type="button" value="Activate"/>	<input type="button" value="Delete"/>
fw_6.14.013	6.14.013		<input type="button" value="Activate"/>	<input type="button" value="Delete"/>

13.8.10 Display



Time Table:

Here you can edit the Time Table directly. You can add a new timezone with daylight savings and the app. parameters. So you can show the local time on the LC Display of the LANTIME.

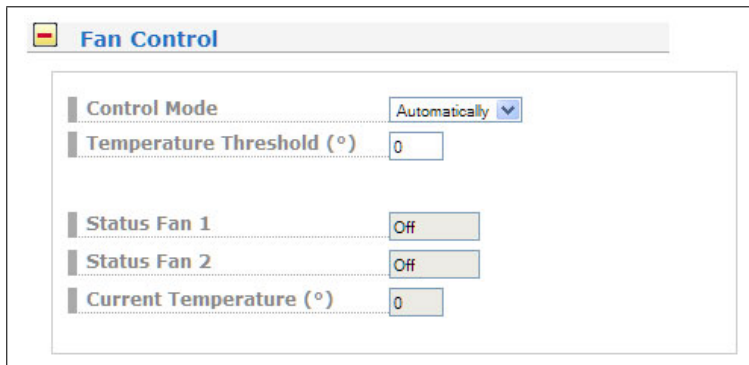
Example:

```
(UTC+1) - CET/CEST,CEST,0,25.03.****,+,02:00,02:00:00,CET,0,25.10.****,+,01:00,03:00:00
```

The string above is the local time zone of middle europe. The offset from UTC is +1 hour. Daylight saving ON with an offset of +2 hours on 25th of march at 2:00 am and OFF at 3:00 am at 25th of october.

The first part of the character string (the Komma is delimiter), you can see as option in the dropdown selection list.

13.8.11 Option: Fan Control



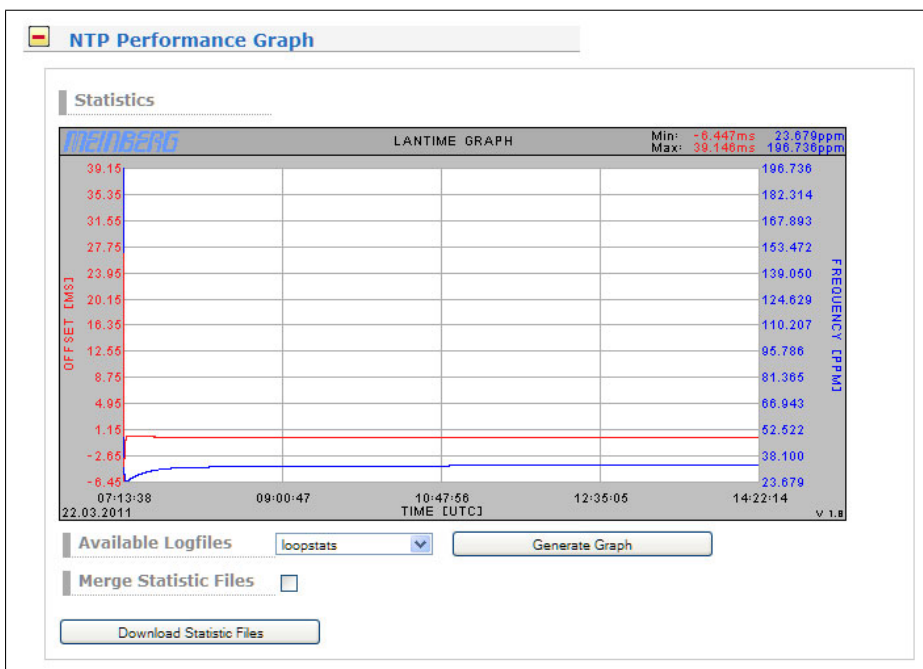
With the optional fan control menu the current status of the operational temperature and the fans can be displayed on the systems interface. The mode of the fans can be selected here:

- On the ventilators are always running
- Off the ventilators are off
- Automatically the ventilation runs from the temperature, which is specified by the "Temperature Threshold" parameter. This value is only editable, if the operation mode "Automatically" is selected. If the temperature of the device is less than 7 degrees (Celsius) as the specified value, the fan control turns off automatically.

13.9 Configuration: Statistics

The screenshot shows the MEINBERG LANTIME Web Interface. The top navigation bar includes: Main, Network, Notification, Security, NTP, PTP, System, Statistics, Receiver, IO Config, NTP-Mon, XtraStats, Docs & Support, and Logout. The user is logged in as 'root' with Super-User access level. The firmware build is 6.18.001. The 'Statistics' menu is expanded, showing options: NTP Performance Graph, PTP V2 Statistics, NTP Status, NTP Monlist, NTP Debug, NTP Access Graph, NTP Client List, and MRS Performance Graph. At the bottom, there are buttons for 'Save Settings', 'Reset Changes', and 'Back'.

NTP Performance Graph



In the first section a graphical diagram shows the running synchronisation process. NTP is storing this statistical information in so-called “loopstats” files, which are used here to draw the curves. The red line is describing the offset between the internal reference clock (GPS) and the system clock. The blue line shows the frequency errors of the system time (in PPM, parts per million). In the upper right corner of the diagram you will find the measurement range of the red and blue curve. The last 24 hours are shown initially, but you are able to select the last 10 days (or fewer days, depending on the system uptime) or switch to a “merge loopstats” diagram, which shows all available days in one diagram (with a maximum of 10 days). All time data is using UTC.

NTP Status

After that a list of all actually reflocks of the internal NTP server will be shown. The last section will show some NTP specific informations about the reflock.

Remote	RefID	Stratum	Type	When	Poll	Reach	Delay	Offset	Jitter
LOCAL(0)	.LOCL.	12	I	7h	8	0	0.000	0.000	0.000
oGENERIC(0)	.GPS.	0	I	6	8	377	0.000	0.000	0.002

with the following meaning:

- remote: list of all valid time servers (ntp.conf)
- refid: reference number
- st: actual stratum value (hierarchy level)
- when: last request (seconds)
- poll: period of requesting the time server (seconds)
- reach: octal notation of the successful requests, shifted left
- delay: delay of the network transmission (milliseconds)
- offset: difference between system time and reference time (milliseconds)
- jitter: variance of the offsets (milliseconds)

NTP Monitor

Remote Address	Port	Local Address	Count	M	Version	Code	Avg Length	First/Last
172.16.100.124	123	172.16.100.167	367	3	4	0	69	53

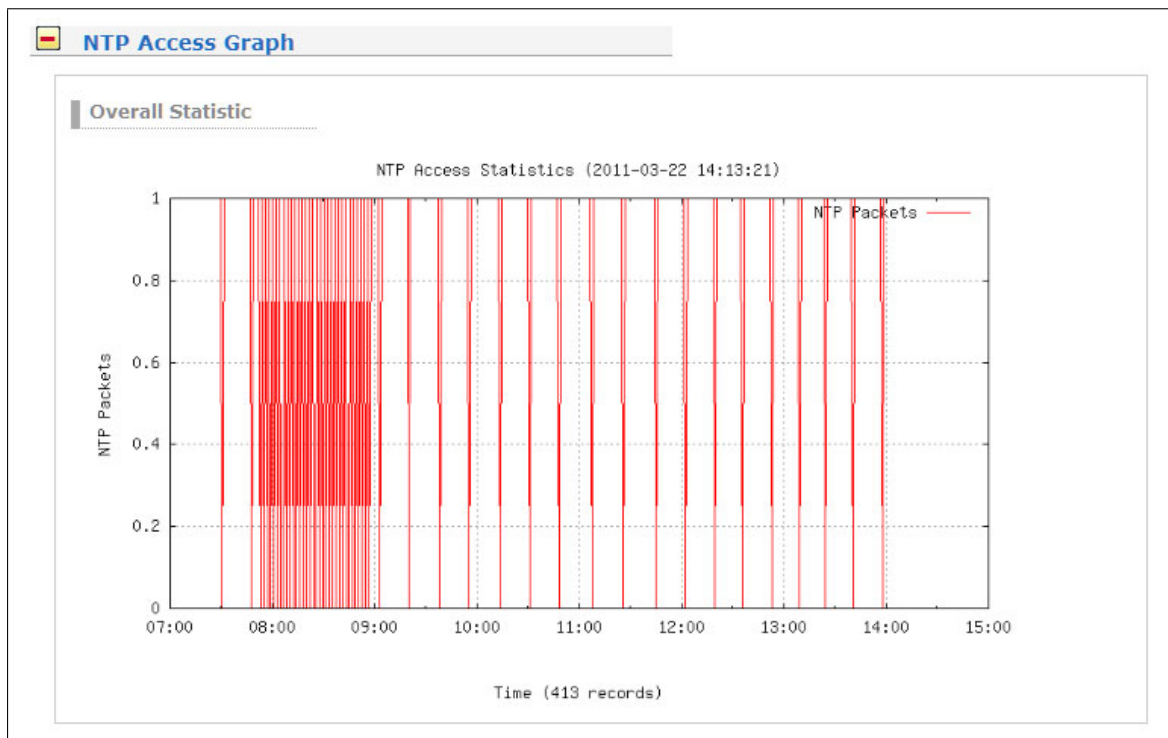
NTP Debug

Index	assID	Status	Conf	Reach	Auth	Condition	Last Event	Count
1	37751	8033	yes	no	none	reject	unreachable	3
2	37752	973a	yes	yes	none	pps.peer	sys_peer	3

assID: 0	Sysvars
assID: 37751	Clockvars Readvars
assID: 37752	Clockvars Readvars

NTP Access Graph

In the next section all NTP clients accessing the NTP server are listed. This list is maintained internally by NTPD, clients who did not access the NTPD for a longer period are automatically removed. This section can grow very long in large networks. There are no further information found about the parameters "code,



avglen and first. The name resolution of the IP address in the first column will take too much time; so its disabled.

13.9.1 Statistical Information

In the first section a graphical diagram shows the running synchronisation process. NTP is storing this statistical information in so-called "loopstats" files, which are used here to draw the curves. The red line is describing the offset between the internal reference clock (GPS) and the system clock. The blue line shows the frequency errors of the system time (in PPM, parts per million). In the upper right corner of the diagram you will find the measurement range of the red and blue curve. The last 24 hours are shown initially, but you are able to select the last 10 days (or fewer days, depending on the system uptime) or switch to a "merge loopstats" diagram, which shows all available days in one diagram (with a maximum of 10 days). All time data is using UTC.

The next sections shows version information for a number of subsystems, including the OS kernel version, NTPD version and the GPS firmware revision of the internal reference clock. Additionally, the MAC address of the first Ethernet interface can be found here. The "Mem free" value is indicating the free memory available to the system, the Disk free value is related to the ram disk of the LANTIME. Both system memory and ram disk have a total capacity of 32 MB (each). The Uptime parameter displays the time since the last boot process of the unit.

In the next section all NTP clients accessing the NTP server are listed. This list is maintained internally by NTPD, clients who did not access the NTPD for a longer period are automatically removed. This section can grow very long in large networks. There are no further information found about the parameters "code, avglen and first. The name resolution of the IP address in the first column will take too much time; so its disabled. After that a list of all actually refclocks of the internal NTP server will be shown.

remote	refid	st	t	when	poll	reach	delay	offset	jitter
LOCAL(0)	LOCAL(0)	3	l	36	64	3	0.00	0.000	7885
lantime	.GPS.	0	l	36	64	1	0.00	60.1	15875

with the following meaning:

-
- remote: list of all valid time servers (ntp.conf)
 - refid: reference number
 - st: actual stratum value (hierarchy level)
 - when: last request (seconds)
 - poll: period of requesting the time server (seconds)
 - reach: octal notation of the successful requests, shifted left
 - delay: delay of the network transmission (milliseconds)
 - offset: difference between system time and reference time (milliseconds)
 - jitter: variance of the offsets (milliseconds)

The last section will show some NTP specific informations about the refclock.

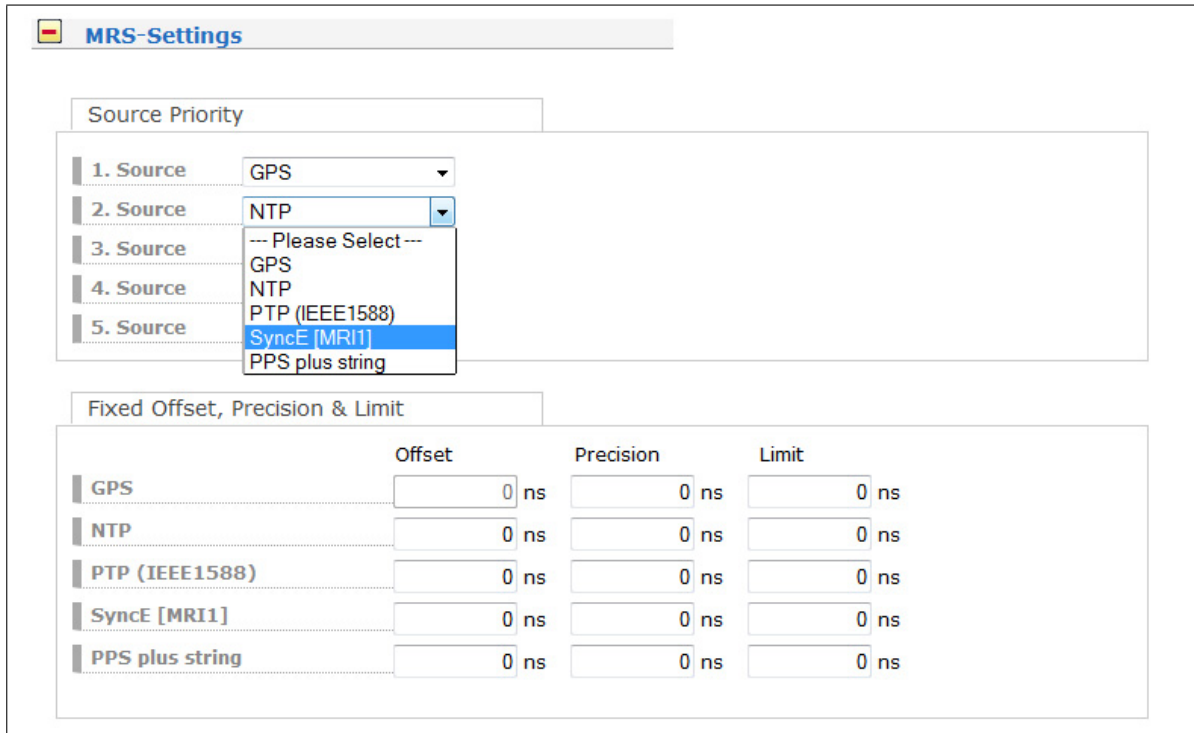
13.10 Configuration: Receiver

The screenshot displays the MEINBERG LANTIME Web Interface. The top navigation bar includes links for Main, Network, Notification, Security, NTP, PTP, System, Statistics, Receiver, IO Config, NTP-Mon, XtraStats, Docs & Support, and Logout. The user is logged in as 'root' with Super-User access level. The firmware build is 6.18.001. The main content area is titled 'LANTIME - Receiver' and is divided into two columns. The left column contains sections for 'GPS Receiver' and 'GLN Receiver', each with expandable options: MRS Status, MRS-Settings, IRIG Settings, Serial Ports, Miscellaneous, Initialize Receiver, and Receiver Information. The right column is titled 'Switch Card' and contains expandable options: Time Zone, Enable Outputs, Programmable Pulses, Initialize Receiver, and Receiver Information. At the bottom of the page, there are three buttons: 'Save Settings', 'Reset Changes', and 'Back'.

On this page you can edit the important receiver settings like "Serial Ports" or "Time Zone" and you can get an overview about the information of your LANTIME's internal receiver.

13.10.1 MRS Settings

With this submenu you can setup some important parameters of the selected systems reference time:



In the next menu the user can define in which order the references will be used to control the internal oscillator. The reference clock with the highest priority will be used always if this is available. You can set a fixed offset for the available references in the next sub menu. By default this value is 0 ns. The bias of the internal GPS receiver can not be set up – indirectly this can be done via the antenna cable length.

Possible values for reference input signals:

- GPS GPS signal of internal receiver
- PPS in PulsePerSecond input reference
- IRIG IRIG Time Code (DCLS/AM)
- NTP external NTP time server
- PTP (IEEE1588) IEEE 1588 (Slave mode)
- SyncE TSUv3 Time Stamp Unit in MRI Slot (Slave Mode)
- Fixed Freq. in Frequency input

Each reference clock can be assigned a specific precision which will reflect the accuracy of the reference clock. This precision value will determine the hold over time when switching to the next reference clock if the current master is not available anymore. If the precision is 0 the next reference clock will be switched at once. If the precision value is greater than 0 the time for switching to the next reference (hold over time) will be calculated by the following formula: (precision of next reference) / (precision of current master) * constant [s]

The parameter „constant“ depends on the quality of the internal oscillator!

Example: the external PPS with an precision of 100ns is the current master. If this master is no longer available it will switch to the next reference source of the priority order – in this case the IRIG input with an precision of 10us. With the formula ((10000ns/100ns)*11.4) we get hold over time of 19min. The online display of the MRS status will show the remaining time and the calculated time. The hold over time will be recalculated if the status of the reference clocks will change.

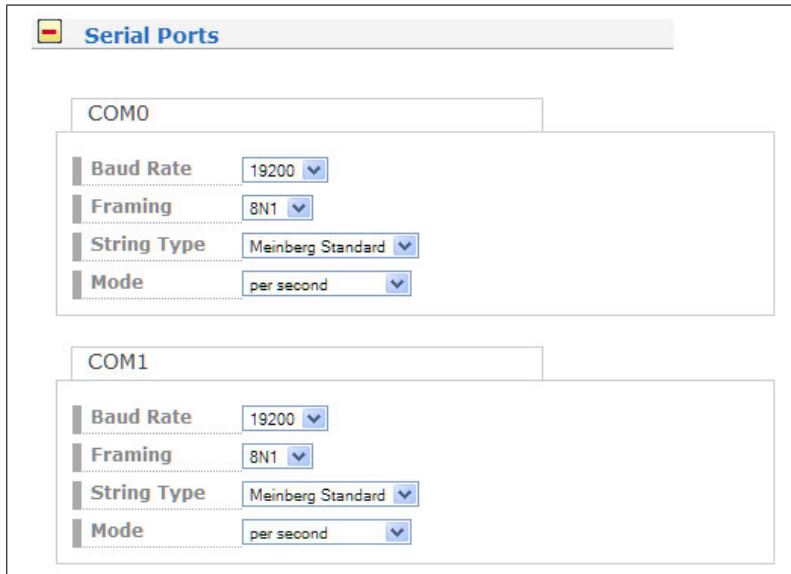
13.10.2 IRIG Settings

With IRIG Settings you can adjust the IRIG/AFNOR outputs of the device:

B002+B122	IRIG-B 100PPS: DC Level Shift (DCLS), No carrier(DCLS), coding of time (HH,MM,SS,DDD) + modulated, 1 kHz / 1 millisecond resolution, coding of time (HH,MM,SS,DDD), Control Functions
B003+B123	like B002+B122, with second of day (0...86400)
AFNOR NF S87-500	AFNOR NFS 87-500 is a standardized french time code similar to IRIG-B but contains additional day, day-of-month and year information.
IEEE1344	Additional extensions to the IRIG-B time code: year, time quality, daylight savings time, local time offset and leap second information

13.10.3 Serial Ports

This menu lets the user configure the baud rate, the framing and the string type of the serial RS232 port to one of the following values:



The screenshot shows a configuration window titled "Serial Ports" with a German flag icon. It contains two sections for COM0 and COM1. Each section has four dropdown menus: Baud Rate (set to 19200), Framing (set to 8N1), String Type (set to Meinberg Standard), and Mode (set to per second).

Baud Rate: 300 to 19200

Framing: 7E1, 7E2, 7N2, 7O1, 7O2, 8E1, 8N1, 8N2, 8O1

Selectable Telegrams

- Meinberg Standard
- SAT
- NMEA RMC
- Uni Erlangen
- Comptime
- Sysplex 1
- Meinberg Capture
- SPA
- RACAL
- Meinberg GPS
- NMEA GGA
- NMEA RMC GGA
- NMEA ZDA
- ION

COM provides a time string once per second, once per minute or on request. If the "on request" is activated you have to send the character "?" to get the time string.

Default settings: COM:19200 baud, 8N1, per second, Meinberg Standard Time String

13.10.4 Synthesiser

Here you can edit the frequency and phase to be generated by the on-board synthesizer. Frequencies from 1/8 Hz up to 10 MHz can be entered using four digits and a range. If frequency is set to 0 the synthesizer is disabled.

With "Phase" you can enter the phase of the generated frequency from -360° to $+360^\circ$ with a resolution of 0.1° . Increasing the phase lets the signal come out later. Phase affects frequencies less than 10.00 kHz only!

13.10.5 Time Zone

With the dropdown list you can select the local time zone. You can add more values to the list with the menu you find in "System -> Display -> Edit Time Zone Table".

13.10.6 Enable Outputs

This menu lets the user configure at which time after power up the serial ports are enabled. Outputs which are enabled "always" will be enabled immediately after power up. Outputs which are enabled "if sync" will be enabled after the integrated receiver is running in normal operation mode.

13.10.7 Miscellaneous

GPS Receiver:

1. Antenna Cable Length:

Enter the length of the antenna cable here. The received time frame is delayed by approx. 5 ns per meter antenna cable. The receiver is able to compensate this delay if the exact cable length is given. The default value is 20 m. The maximum value you can enter in this field is 500m. In case of longer cable runs you have to use an amplifier or a fiber optic connection.

2. GPS Simulation Mode (GPS Receiver)

Enabling this menu lets the user run the LANTIME without antenna. Normally the NTPD loses synchronisation with the GPS when the antenna is disconnected or the GPS did not receive enough satellites (red FAIL LED is turned on). So it is possible to set the NTPD with any other time. If this option is enabled an "*" will be shown behind the time string in the root menu of the display.

3. GPS Time Scale (GPS Receiver)

You can select between the following values:

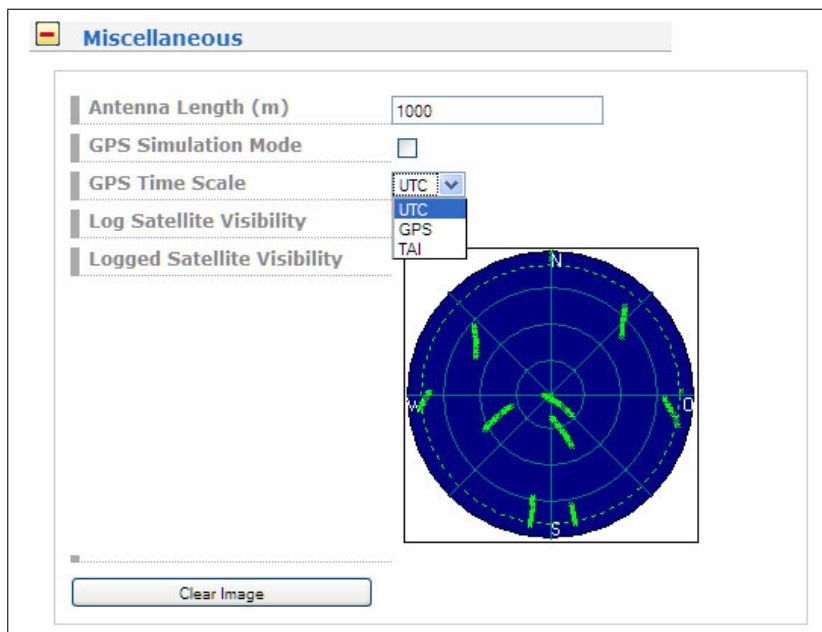
UTC - Coordinated Universal Time (including leap seconds)

GPS - since 1th of January 1980 - equivalent to TAI Time Scale with the difference from a constant value of 19 seconds (this time scale includes the leap seconds from 1980 until today).

TAI - since 1968, 1th of January 1900 as reference start time - International Atomic Time (without Leap Seconds)

4. Logged Satellite Visibility (GPS Receiver)

If this checkbox is activated, the system generates a graphic from the constellation of the visible satellites.



Init Receiver (GPS Receiver)

The screenshot shows a web interface titled "Initialize Receiver". It contains the following elements:

- Two buttons: "Warm Boot Mode" and "Cold Boot Mode".
- Input fields for "Time (hh:mm:ss)" with the value "11:23:28" and "Date (dd.mm.yyyy)" with the value "16.10.2014".
- An "Initialize Date/Time" button.
- Input fields for "Latitude" (51° 58' 58" N), "Longitude" (9° 13' 34" E), and "Altitude" (184 m).
- An "Initialize Position" button.

Warm Boot Mode (GPS Receiver)

You can force the receiver into the Boot Mode. This may be necessary when the satellite data in the memory are too old or the receiver position has changed by some hundred kilometres since last operation. Synchronisation time may be reduced significantly. If there is valid satellite data in the memory the system starts in the WARM BOOT mode, otherwise the system changes into COLD BOOT to read new data.

Cold Boot Mode (GPS Receiver)

With this button you can initialize all GPS data, i.e. all saved satellite data will be cleared. You have to confirm this operation before the initialisation starts. The system starts operating in the COLD BOOT mode and seeks for a satellite to read its actual parameters. Please note, that the GPS receiver needs approximately 15 minutes for the initiated COLD BOOT!

Long Wave Receiver (DCF77, MSF, WWVB):

The screenshot shows a web interface titled "Miscellaneous". It contains the following elements:

- A text input field for "Distance To Transmitter (km)" with the value "250".
- A checkbox for "PZF Simulation Mode" which is currently unchecked.

Distance to Transmitter


In this submenu the distance to the transmitter is entered for compensating the propagation delay of the received pseudo-random code. This setting should be done as exact as possible because the absolute precision of the time frame is influenced by this value.

Simulation Mode

With "Simulation Mode" the user enable or disable the SYNC simulation mode. If you want to use the receiver without connecting an antenna this mode will simulate a valid output for the NTP daemon. This is only for test purposes. "Simulation Mode" should be disabled under normal operating conditions.

13.10.8 Receiver Information

Here you can indicate all important and relevant information about the used receiver and its internal oscillator

 **Receiver Information**

Common Receiver Information

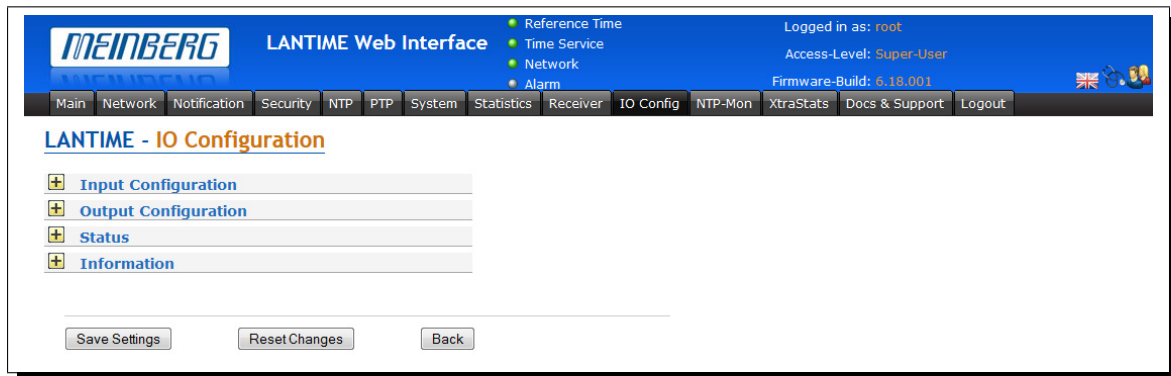
Name	Value
Model:	GPS170
Serial Number:	029010012290
Software Revision:	ext. PPS sync
Oscillator Type:	TCXO
Supported Features:	Pulse Per Second, Pulse Per Minute, DCF77 Time Marks, Ignore Lock
Number of Programmable Pulse Outputs:	0
Number of Serial Ports:	4

Special Receiver Information

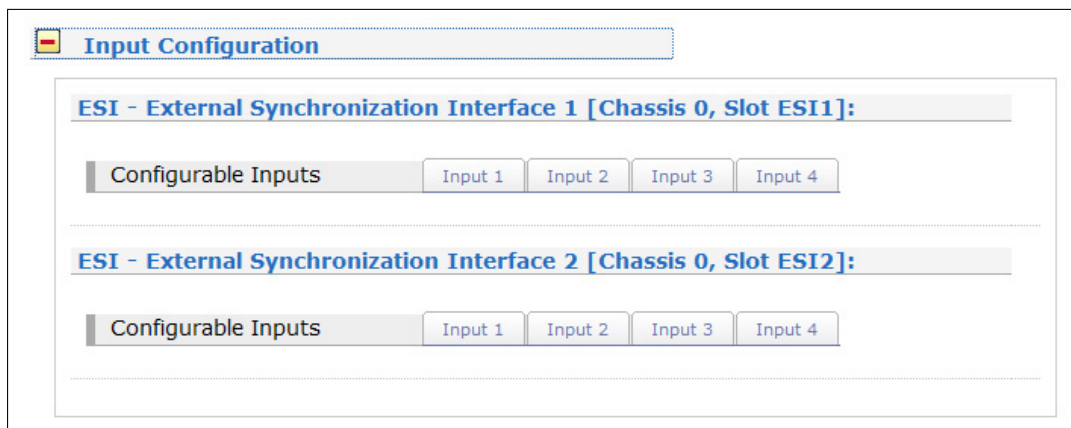
Name	Value
GPS Status:	NORMAL OPERATION
GPS Position LLA:	Lat: 51.9828 Lon: 9.2258 Alt: 166m
GPS Position XYZ:	X:3885651m Y: 631133m Z:5001753m
Number Satellite In View:	9
Number Good Satellites:	9
Selected Satellite Set:	13 20 31 04

13.11 I/O Configuration

This menu occurs in the case of a MRS system



13.11.1 Configuration: Input



Configurable Inputs Input 1 Input 2 Input 3 Input 4

Input 1:

Type PPS in ▾

Configurable Inputs Input 1 Input 2 Input 3 Input 4

Input 2:

Type Freq. In ▾

Frequency 10 MHz ▾

Maximum Slip 1.5 ▾ Cycles

Fixed Frequency T1 framed ▾

Quality 00000 ▾ Maximum BOC

Configurable Inputs

Input 3:

Type

Frequency

Maximum Slip Cycles

Fixed Frequency

Quality

Configurable Inputs

Input 4:

Type

Frequency

Maximum Slip Cycles

Fixed Frequency

Quality

13.11.2 Configuration: Output

With the pull-down menu "Output Configuration" the available outputs of the I/O slots can be configured:

Output Configuration of a LIU module (Line Interface Unit):

In this menu one can select between E1 or T1 mode for the LIU outputs. The selected mode is the same for all outputs.

T1 or E1?

T1 is a digital carrier signal that transmits the DS - 1 signal. It has a data rate of about 1.544 Mbit/second. It contains 24 digital channels and therefore requires a device that has a digital connection.

E1 is the european equivalent to T1. T1 is the North American term whereas E1 is a European term for digital transmission. The data rate of E1 is about 2 Mbit/second. It has 32 channels at the speed of 64 Kbit/second. 2 channels among 32 are already reserved. One channel is used for signaling while the other is used for controlling. The difference between T1 and E1 lies in the number of channels here.

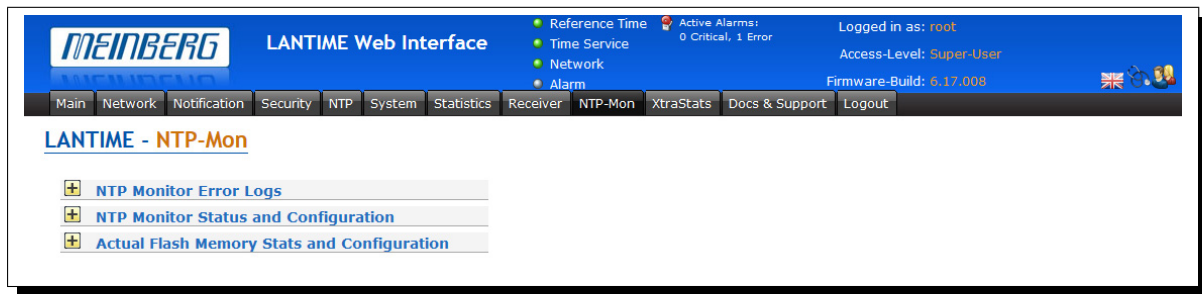
Sa Bits

ITU-T Recommendations allow for bits Sa4 to Sa8 to be used in specific point-to-point applications (e.g. transcoder equipment) within national borders. When these bits are not used and on links crossing an international border they should be set to 1.

Bit Sa4 may be used as a message-based data link for operations, maintenance and performance monitoring. This channel originates at the point where the frame is generated and terminates where the frame is split up.

Bit Sa4 kann hier als nachrichtenbasierte Datenverbindung für den Betrieb, die Wartung und für Performanceüberwachung verwendet werden. Im Webinterface kann das SSM Bit (Synchronisation Status Message) für die Übertragung der Qualität ausgewählt werden. Standardeinstellung ist hier Sa4.

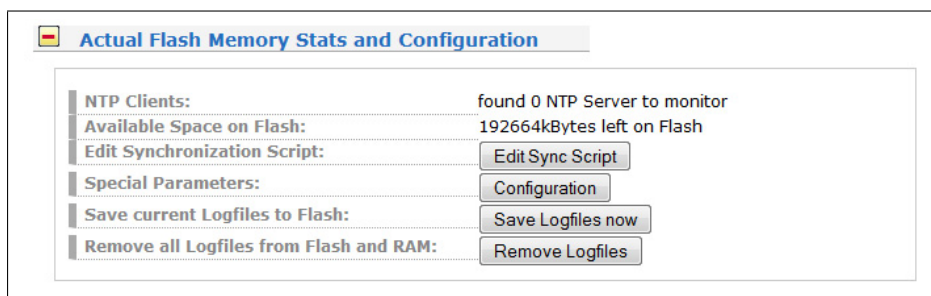
13.12 NTP Monitoring



In this NTP-Mon menu the following points can be monitored or executed:

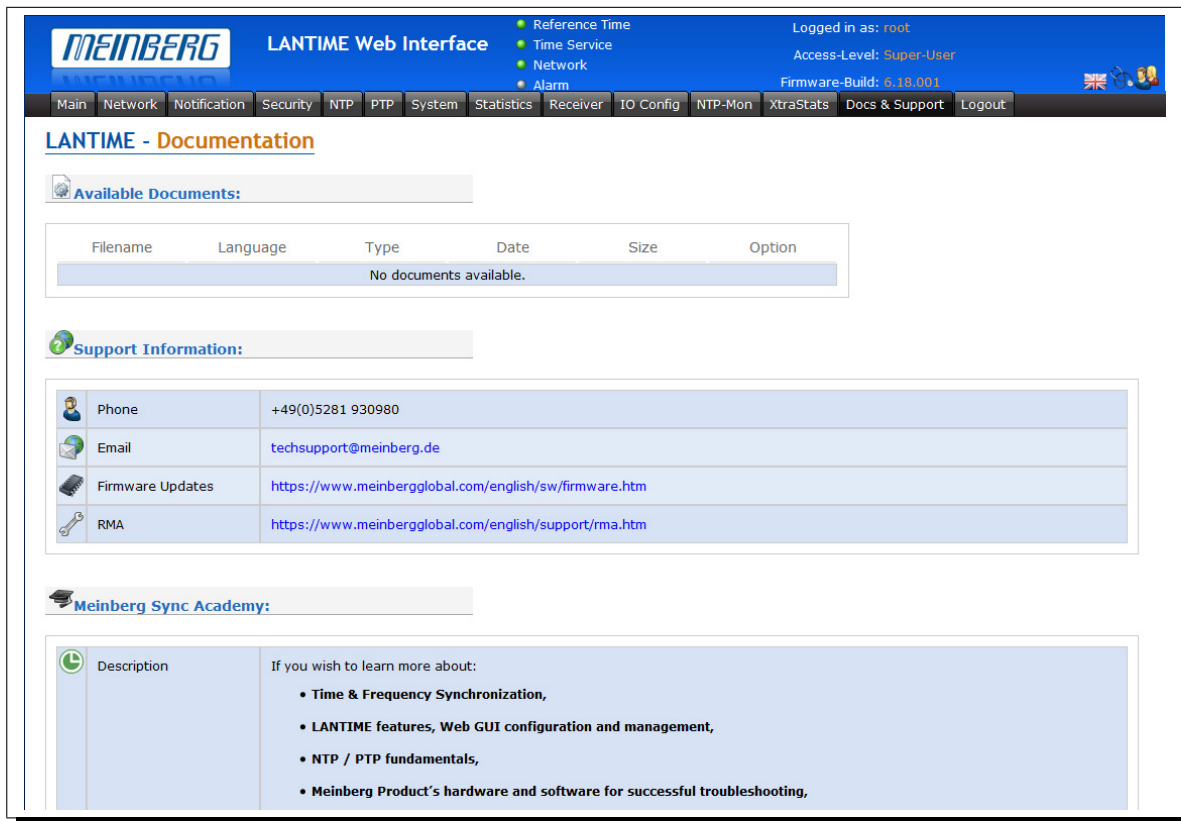
- NTP Monitor Error Logs
- Open Box NTP Monitor Status and Configuration
- Open Box Actual Flash Memory Stats and Configuration

Menu Open Box Actual Flash Memory Stats and Configuration



- A list of detected clients in the network.
- Available free space on the flash card of the time server.
- Editor window for your own synchronization scripts.
- Special parameters: SRC port for outgoing packets, Base Path for log files.
- The current log files can be stored on the flash card.
- All log files can be removed from the flash card.

13.13 Configuration: Documentation



LANTIME Web Interface

Reference Time
Time Service
Network
Alarm

Logged in as: root
Access-Level: Super-User
Firmware-Build: 6.18.001

Main Network Notification Security NTP PTP System Statistics Receiver IO Config NTP-Mon XtraStats Docs & Support Logout

LANTIME - Documentation

Available Documents:

Filename	Language	Type	Date	Size	Option
No documents available.					

Support Information:

Phone	+49(0)5281 930980
Email	techsupport@meinberg.de
Firmware Updates	https://www.meinbergglobal.com/english/sw/firmware.htm
RMA	https://www.meinbergglobal.com/english/support/rma.htm

Meinberg Sync Academy:

Description

If you wish to learn more about:

- Time & Frequency Synchronization,
- LANTIME features, Web GUI configuration and management,
- NTP / PTP fundamentals,
- Meinberg Product's hardware and software for successful troubleshooting,

This page gives you access to the documents stored on your LANTIME, especially the manuals and your own notes. The two lists include filename, language, file type, date and size of the documents/notes.

Available Documents:

Filename	Language	Type	Date	Size	Option
m600_mrs_ptpv2	english	pdf	2011-12-07	5265.91kb	View
m600_mrs_ptpv2	german	pdf	2011-12-07	5869.14kb	View
2 Documents available					

The LANTIME documents can be downloaded from here in order to read / print them on your workstation. The customer notes are a way of storing small pieces of information on your LANTIME, for example if you want to keep track of configuration changes and want to comment them, you can create a note called "config_changes" and show or edit it from here. If you want to get rid of one of your notes, you are able to delete it by choosing the appropriate button.

If you want to add a note (you can maintain more than one note on your LANTIME), after choosing the button "add note" you have to enter a filename (without a directory path, all notes are stored in a fixed directory on the flash disk of your LANTIME) and the language of your note first. After you confirmed these parameters with "Add document", you are able to edit the text of your new note.

14 Attachment: Technical Information

14.1 Skilled/Service-Personnel only: Replacing the Lithium Battery

The life time of the lithium battery on the board is at least 10 years. If the need arises to replace the battery, the following should be noted:

ATTENTION!

There is a Danger of explosion if the lithium battery is replaced incorrectly. Only identical batteries or batteries recommended by the manufacturer must be used for replacement.

The waste battery has to be disposed as proposed by the manufacturer of the battery.



14.2 Technical Specifications SyncFire 1100

Dimensions / Weight

Rack (W x D x H)	483 mm (bezel) /435 mm (body) x 768 mm (bezel) /770.7 mm x 43 mm
Mounting depth rack	748.2 mm
Height unit rack	1 U
19" rackmount	Yes
Mounting cable depth rack	200 mm (1000 mm rack recommended)
Weight	16 kg

Electrical data (hot-plug power supply unit)

Rated voltage range	100-240 V
Frequency	50 / 60Hz
Effective power	450 W
Rated current	8.5 A (100 V) / 3.5 A (240 V)

Power supply configuration 2 x hot-plug power supply for redundancy

Environment

Temperature:	Operation: 5°C ... 40°C
Humidity	10% ... 85% (non condensing)

14.3 Front/Rear Panel Connectors

Name	Type	Signal	Cable
Front panel			
TERM (LANTIME)	9pin. D-SUB	RS-232	shielded data line
2 x USB	3.0	USB connector	
Rear panel			
1-2 Power supply	100 V - 240V / 450 W		power cord receptacle
GPS Receiver			
Antenna	BNC	10 MHz / 35.4 MHz	shielded coaxial line
or			
combined GPS/GLONASS Receiver			
L1 Antenna	SMA	1575.42 +- 10 MHz 1602-1615 MHz	shielded coaxial line
IRIG Time Code (AM) BNC		3Vpp into 50 Ohm	shielded coaxial line
VGA	9pin. D-SUB		shielded data line
2 x USB 3.0	USB connector		
1 x USB 2.0	USB connector		
2 x LAN Port	RJ45	10/100/1000 Mbit/s	shielded data line
Optional			
4 x LAN Ports (add.)	RJ45	10/100/1000 Mbit/s	shielded data line
or			
2 x LAN Ports (add.)	SFP Slot	10GBASE	shielded coax line
Second Receiver			
GPS Antenna	BNC	10 MHz / 35.4 MHz	shielded coaxial line
or			
combined GPS/GLONASS			
L1 Antenna	SMA	1575.42 +- 10 MHz 1602-1615 MHz	shielded coaxial line
IRIG Time Code (AM) BNC		3Vpp into 50 Ohm	shielded coaxial line

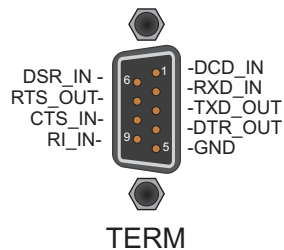
Information for ensuring electromagnetic compatibility

All data and signal cables must have sufficient shielding. The use of cable type S/FTP Cat5 or better is recommended. Use of unshielded or badly shielded cables may lead to increased emission of interference and/or reduced fault-tolerance of the device.



14.4 TERMINAL (Console)

To connect a serial terminal use 9 pin SUBD RS232 connector in the front panel. Via the serial terminal connection it is possible to configure parameters with the command line interface. You have to use a NULL-MODEM cable connecting to your PC or Laptop computer. You can use e.g. the standard Hyperterminal program shipped with your Windows operating system. Configure your terminal program with 38400 Baud, 8 Databits, no parity and 1 Stopbit. The terminal emulation have to set to VT100. After connecting to the timeserver there will be displayed the login message (press RETURN for first connection; default user: root password: timeserver).



14.5 USB Connector

Most LANTIME M-Series products come with a USB interface for connecting a USB storage device, e.g. a USB stick. This USB stick can be used for different tasks in combination with the LANTIME:

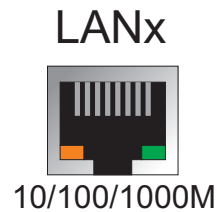


USB

- Transfer configuration parameters
- between different LANTIMEs
- Keypad locking for secure
- using the keypad of the LCD
- Transfer of log files
- Install Software Updates
- Upload and download secure certificates
- (SSL, SSH) and passwords

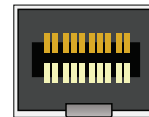
14.6 10/100/1000base-T Gigabit Ethernet (IEEE 802.3-2008)

Link speed:	10/100/1000 Mbit
Connector Type:	8P8C (RJ45)
Cable:	CAT 5.0
Duplex Modes:	Half/Full/Autonegotiaton



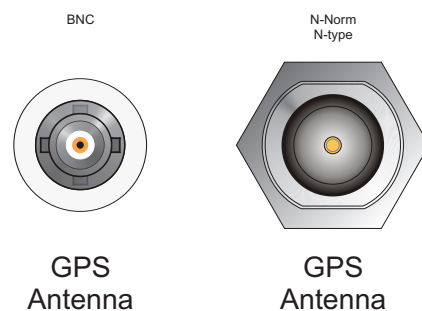
14.7 10 Gigabit SFP+

Transceiver Interface Type	SFP+
Bus Interface:	PCI Express v1.1, x8
Network:	10 Gigabit Ethernet
Power consumption:	Dual Port 10GBase-SR, typ. 10 W, max. 10.7 W Dual Port SFP+ Twinax typ. 7.9 W, max. 8.6 W
Operating Temperature:	0 - 55 °C



14.8 GPS Antenna

Cable:	shielded coax
Cablelength:	max. 300m to RG58, max. 700m to RG213
Connector:	BNC female or N-type female
Input GPS:	Antenna circuit 1000 V DC insulated
Local Oscillator to Converter Frequency:	10 MHz ¹
First IF Frequency:	35.4 MHz ¹



1) these frequencys are transfered via the antenna cable.

Power Requirements: 12V ... 18V, 100mA (via antenna cable)

14.9 GLN Antenna

Cable: shielded coaxial line

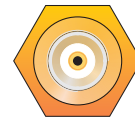
Cablelength: max. 50m to RG58

Connector: SMA female

**Type of receiver
GLN/GPS:** Number of channels: 24
Frequency band: L1

Type of antenna: 40 dB GPS L1/GLONASS L1
Antenna with Integrated Lightning Protection

Frequency Band: 1575.42 +- 10 MHz / 1602-1615 MHz
Antenna Gain: ≥ 3.5 dBic / ≥ 3 dBic
Nominal Impedance: 50 ohms



GLN
Antenna

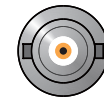
14.10 Time Code AM Output

Carrier frequency: 1 kHz (IRIG-B)

Signal outputs: Unbalanced sine wave-signal:
3 Vpp (MARK) / 1 Vpp (SPACE) into 50 Ohm

Connector: BNC, female

Cable: shielded coax line



TC AM Out

15 Declaration of Conformity

Konformitätserklärung

Doc ID: SyncFire 1100-2015-11-01

Hersteller Meinberg Funkuhren GmbH & Co. KG
Manufacturer Lange Wand 9, D-31812 Bad Pyrmont

erklärt in alleiniger Verantwortung, dass das Produkt,
declares under its sole responsibility, that the product

Produktbezeichnung SyncFire 1100
Product Designation

auf das sich diese Erklärung bezieht, mit den folgenden Normen übereinstimmt
to which this declaration relates is in conformity with the following standards

EN55022:2010, Class B Limits and methods of measurement of radio interference characteristics
of information technology equipment

EN55024:2010 Limits and methods of measurement of Immunity characteristics of information
technology equipment

EN 60950-1:2006 Safety of information technology equipment
(+A11:2009 +A12:2011)

EN 50581:2012 Technical documentation for the assessment of electrical and electronic products
with respect to the restriction of hazardous substances

gemäß den Richtlinien 2014/30/EU (Elektromagnetische Verträglichkeit), 2014/35/EU (Niederspannungsrichtlinie),
2011/65/EU (Beschränkung der Verwendung bestimmter gefährlicher Stoffe) und 93/68/EWG (CE Kennzeichnung)
sowie deren Ergänzungen.
*following the provisions of the directives 2014/30/EU (electromagnetic compatibility), 2014/35/EU (low voltage
directive), 2011/65/EU (restriction of the use of certain hazardous substances) and 93/68/EEC (CE marking) and
its amendments.*

Bad Pyrmont, 2015-11-01



Günter Meinberg
Managing Director



SyncFire-1100_011215